NLSS Unified Security Suite

User Manual

v4.0

© 2009-2014 by Next Level Security Systems, Inc.
All rights reserved.

2.00-UM-20140804

Next Level Security Systems® is a registered trademark of Next Level Security Systems, Inc. NextConnect™ is a trademark of Next Level Security Systems, Inc.

All content included in this document, including text, and graphics, is © 2009-2014 Next Level Security Systems, with all rights reserved, or is the property of Next Level Security Systems and/or third parties protected by intellectual property rights. Any use of materials in this document, including reproduction for purposes other than those noted above, modification, distribution, or replication, or other commercial exploitation of any kind, without prior written permission of an authorized officer of Next Level Security Systems is strictly prohibited.

Next Level Security Systems' trademarks may not be used in connection with any product or service that is not provided by Next Level Security Systems, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Next Level Security Systems.

All other trademarks displayed in this document are the trademarks of their respective owners, and constitute neither an endorsement nor a recommendation of those Vendors. In addition, such use of trademarks is not intended to imply, directly or indirectly, that those Vendors endorse or have any affiliation with Next Level Security Systems.

The contents of this manual are subject to change without notice.

Contents

Preface **16**

PART 1: GETTING STARTED 17

Chapter 1: Introduction 18

KEY FEATURES 18

COMPONENTS OF THE NLSS UNIFIED SECURITY PLATFORM 19
- NLSS Gateway 19
- NLSS Unified Security Suite 19
- Access Control Devices 19
- Cameras 19
- NLSS HD Decoder 20
- External Storage 20
- Generic Computers and Browsers 20
- Generic HD Monitors 20

Chapter 2: Installation 21

SYSTEM REQUIREMENTS 21
- Requirements for NLSS Discovery Utility 21
- Requirements for Configuration and Operation 21

CAMERA REQUIREMENTS 22

HARDWARE INSTALLATION 22

SOFTWARE INSTALLATION 22
- Install Security Certificate 22
- Install Cameras 24
- Install NLSS Gateways 24
  - *Finding the IP Address without the Web Interface* 26

Chapter 3: Using the NLSS Web Interface 28

LOG IN 28
- Local Login 28
  - *Automatic Log Off* 29
- Remote Login 29

USING THE NLSS WEB INTERFACE 29

MAIN MENU 30
- Operations 31
  - *System Health* 32
  - *Operations Windows* 33

Filtering Operations Lists 34
Searching a List 35
Configuration 35
Events 36
Full Screen Toggle 36
Log off 36
Help 36
Transcode 36

PART 2: OPERATIONS 37

Chapter 4: Controlling Cameras 38

SELECTING CAMERAS 38
Camera Icons 40
Filtering the Camera List 40
Video Player 41

MONITORING CAMERAS 42
Monitor Cameras from the Operations Menu 42
Using the Camera Toolbar 43
Video Information 43
Play/Pause 44
Live/Archive Toggle 44
Rewind and Fast Forward 44
Date & Time Selection 45
Camera Events Toggle 45
Event Bookmark 45
PTZ (Pan, Tilt, Zoom) 46
Video Analytics 49
Audio Analytics 50
Digital Zoom 50
Output Contact 50
Play Audio 50
Talkback (Local Microphone Control) 51
Volume / Mute 51
Export JPG 51
Export Video 51
Full Screen Toggle 53
Timelines 53
Additional Camera Controls 54
Select a Stream 54
Low Resolution/Native resolution 55
Camera Event Log 55
Camera Reports 57
Back 57

Chapter 5: Operations with Video Analytics 58

PARAMETERS 58

USING VIDEO ANALYTICS 59
Activity 61
Direction 62

© 2009-2014 Next Level Security Systems, Inc.

Dwell 63
Face Capture 64
Face Recognition 65
License Plate Capture and License Plate Recognition 66
Line Crossing 66
Object Moved 67
Object Taken 68
People Count 69
People Count Directional 70
Perimeter 71
Troubleshooting Video Analytics 71

VIDEO FORENSICS 72

Chapter 6: Operations with Doors 73

DOORS WINDOW 73

DOOR LIST 74
List Filters 74
Door Icons 74

UNLOCK 75

ADD CAMERA 75
Adding and Viewing Cameras with Doors 75
Remove Camera 75

PUSH TO TALK 76

EVENT LOG 76

REPORTS 76

Chapter 7: Operations with Cardholders & Users 77

CARDHOLDERS/USERS WINDOW 77
Filtering Cardholders/Users List 78

CARDHOLDERS/USERS DETAILS 78
Cardholder Information 78
User Information 78
Cardholder Photo 78
Activate / Deactivate Cardholders 79
Cardholders & Users Reports and Events 79

Chapter 8: Operations with Reports 80

GENERATING REPORTS 80
Reports Window 81
Event-Specific Reports 81
Device-Specific Reports 83

CATEGORIES OF EVENT-SPECIFIC REPORTS 84

CANNED REPORTS 85
Using the Table 85
Report Table Filters 87

© 2009-2014 Next Level Security Systems, Inc.

Search filter 87
Column Filters 87

Chapter 9: Displaying Video 88

CREATE, EDIT, AND DISPLAY VIEWS 88
Views Menu and Layout 89
Menu Options 89
Create Views 90
Edit Views 90
Filter Views List 90
Transport Control 91
Delete Views 92

CREATE, EDIT, AND DISPLAY SEQUENCES 93
Sequences Menu and Editor 93
Create New Sequences 94
Edit a Sequence 94
Delete Sequences 95
Display Sequences 95

PUSH MEDIA CLIPS, VIEWS AND SEQUENCES TO DECODERS 95
Decoder Window 96
Pushing a Media Clip 97
Pushing a View or Sequence 98

Chapter 10: Media Operations 99

MEDIA LIBRARY 100
Filter the Library 101
Searching the Media Library 101
Download a Video Clip 101
Stop a Camera Export 102
Lock a Media File 102
Delete a Media File 102
Replacing a Default Audio File 102

Chapter 11: Operations with Input Devices 103

INPUT DEVICES WINDOW 103

INPUT DEVICE LIST 104
Input Device Icons 104

ADD CAMERA 104
Adding and Viewing Cameras with Input Devices 104
Remove Camera 105

PUSH TO TALK 105

EVENT LOG 105

REPORTS 106

Chapter 12: Operations with Output Devices 107

OUTPUT DEVICES WINDOW 107

© 2009-2014 Next Level Security Systems, Inc.

OUTPUT DEVICE LIST 108
Output Device Icons 108
ACTIVATING AND DEACTIVATING A DEVICE 108
ADD CAMERA 109
Adding and Viewing Cameras with Output Devices 109
Remove Camera 109
PUSH TO TALK 109
EVENT LOG 110
REPORTS 110

Chapter 13: Using Floor Plans 111

Chapter 14: Using Groups 112
GROUPS WINDOW 113
LIST VIEW 113
Adding and Using Maps 114
Opening a Door from a Floor plan or Map 116
Viewing Video from a Floorplan or Map 116
Deactivating a Cardholder Information via a Floorplan or Map *117*
Activating and Deactivating an Output Device 117

Chapter 15: Monitoring and Handling Events 118
MONITORING EVENTS 118
EVENT LOG 119
Date & Time Range 119
Event Log Queues 120
Event Filters 120
Search Fields 121
Event List 121
List Actions 122
EVENT DETAILS 123
Event Details Actions 123
Event State 123
Shunt Toggle 124
Lock State Toggle 124
Written Note Editor 124
Recorded Event 124
Current Snapshot 124
Profile Picture 124
Exporting the Event Log 124
Close 125
Emergency Events 125
FACE RECOGNITION EVENTS 125
Events and Linkages 126

© 2009-2014 Next Level Security Systems, Inc.

PART 3: SYSTEM CONFIGURATION 127

Chapter 16: General Configuration Functions 128

SEARCHING TABLES 128

ADDING, EDITING AND DELETING ITEMS 129
- Adding Items 129
- Edit Items 129
- Delete Items 130

Chapter 17: Global Configurations 131

CONFIGURE SUBSCRIPTIONS 132
- Enabling RMS 133
- Enabling Other Premium Features 133

CONFIGURE CUSTOMER 134
- Customer Details 134
- Customer Configuration 134

CONFIGURE SITES 135
- Site Details 135
- Editing Site Details 135

CONFIGURE NLSS GATEWAYS 136
- General Tab 136
  - *General Tab Parameters* 136
  - *General Tab Buttons and Links* 137
- Wired Network Tab 142
- Email Tab 143
- Time Tab 144

CONFIGURE HOLIDAYS 145
- Holidays Table 145
- Holiday Details 145

CONFIGURE SCHEDULES 146
- Schedule Details 147
- Create New Schedules 147

CONFIGURE EVENT TYPES 148
- Event Type Table 148
- Event Type Details 149

CONFIGURE EVENT SEVERITY 149
- Event Severity Table 149
- Event Severity Details 150

CONFIGURE GROOMER SETTINGS 150

CONFIGURE ACTIONS 151
- Action Type 152
- Creating an Action 153

CONFIGURE EVENT LINKAGES 154
- Event Linkage Details 155

© 2009-2014 Next Level Security Systems, Inc.

Creating an Event Linkage 156

Chapter 18: Configure Identity and Credentials 157

CONFIGURE ACCESS LEVELS 157
Access Level Details 158
Create a New Access Level 158

CONFIGURE CARD TYPES 159
Card Types Table 159
Card Types Details 160

CONFIGURE CARDHOLDER TYPES 161
Cardholder Types Table 161
Cardholder Types Details 161

CONFIGURE CARDHOLDERS 162
Cardholders Table 162
Configuration Order 163
Cardholders Tabs 163
General Tab 163
Cards Tab 164
Access Levels Tab 166

Chapter 19: Configure Access Control 168

CONFIGURE CONTROLLERS 169
Controller Details 170
General Tab 170
Controller Details: Diagnostics Tab 172
Associating a Mercury Controller with an NLSS Gateway 173
Putting an Axis A1001 Network Door Controller In Service 173

CONFIGURE ELEVATOR CONTROL 174
Configuring Elevator Control 175

CONFIGURE READER INTERFACES 175
Reader Interface Details 176
General Tab 176
Aux Input Tab 178
Aux Output Tab 179
Adding and Deleting Reader Interfaces 180
Add Reader Interfaces Manually 180
Delete Reader Interfaces 180

CONFIGURE READERS 181
Reader Details 181

CONFIGURE DOORS 183
Gateway Capacities 183
Adding and Maintaining Doors 183
Door Details 184

CONFIGURE I/O INTERFACES 185
I/O Interface Details 186
I/O Interfaces: General Parameters 186
I/O Interface Details: Aux Input Tab 186
I/O Interface Details: Aux Output Tab 187

© 2009-2014 Next Level Security Systems, Inc.

CONFIGURE I/O LINKAGES 188
I/O Linkages Details 189

Chapter 20: Configure Video, & Storage, & Decoders 190

CONFIGURE EXTERNAL STORAGE DEVICES 190
Storage Table 191
Storage Details 191
Adding Storage Devices 192
USB Storage Devices 192
eSATA Storage Devices 192
iSCSI Storage Devices 192
NAS Storage Devices 193

CONFIGURE CAMERAS AND STREAMS 194
Camera Details General Tab 195
Editable Parameters 195
Read-Only Parameters 197
Camera Details Stream Tab 197
List of Streams 198
Video Stream Parameters 198
Audio Stream Parameters 199
Camera Details Recording Tab 199
Stream Settings *200*
Camera Settings 200
Cameras Actions 201
Connect to a Camera 201
Add RTSP and HTTP Streams 201

CONFIGURE NLSS HD DECODERS 202
Decoder Table 202
Decoder Details 203
Editable Parameters 203
Read-Only Parameters 203

Chapter 21: Configuring Permissions 204

APPLYING PERMISSIONS EXAMPLE 204

GROUPS 207
Example 207
Groups Window 208
Create a Group 208
Edit a Group 209
Delete a Group 209

ROLES 210
Roles Details 211
General Tab 211
Gateway Modules Tab 212
Gateway Groups 214
Gateway Functions 215
Cloning a Role 216
Delete a Role 216

USERS 217
User Details 218

© 2009-2014 Next Level Security Systems, Inc.

PART 4: PREMIUM FEATURES 219

Chapter 22: Configuring and Using Face Recognition 220

DATABASE SPECIFICATIONS 221
.csv File 221
Images Requirements 221

IMPORTING A DATABASE 222

FACE RECOGNITION GROUPS 223
Accessing Face Recognition Groups 224
Groups Table 224
Group Details 225
Creating a Group 225
Deleting a Group 225
Assigning People to Groups 226

MANAGEMENT 226
Management Table 227
Management Details 227
General Tab 227
Images Tab 228
Updating the Management List 230
Adding a Person 230
Editing a Person 230
Deleting a Person 231

RUNNING THE FACE RECOGNITION ANALYTIC 232

FACE CAPTURE AND RECOGNITION GUIDELINES 233
Configuration Notes 233
FAQs on the Face Capture and Face Recognition Video Analytic 234

Chapter 23: Configuring and Using License Plate Recognition 235

DATABASE SPECIFICATIONS 236
lpr.csv File 236
vehicles.csv 237
Images Requirements 237

IMPORTING A DATABASE 238

LICENSE PLATE RECOGNITION MANAGEMENT 239
Management Table 239
Management Details 240
General Tab 240
License Plate Tab 240
Updating the Management List 241
Adding a Person 241
Editing a Person *242*
Deleting a Person 242

LICENSE PLATE RECOGNITION GROUPS 242
Accessing License Plate Recognition Groups 243
Groups Table 243
Group Details 243

© 2009-2014 Next Level Security Systems, Inc.

Creating a Group 244
Deleting a Group 244
Assigning People to Groups 244
RUNNING LICENSE PLATE CAPTURE 245
RUNNING THE LICENSE PLATE RECOGNITION ANALYTIC 246
SEARCHING EVENTS FOR LICENSE PLATES 247
LICENSE PLATE CAPTURE AND RECOGNITION GUIDELINES 248

Chapter 24: Configuring Audio Analytics 249
CONFIGURING AN AUDIO ANALYTIC 249

Chapter 25: Configuring and Using Intrusion Detection 252
CONFIGURING INTRUSION 253
Panel 253
General Tab 254
Diagnostic Tab 255
Zones Tab 255
Outputs Tab 256
Adding an Intrusion Detection Panel 256
Areas 257
Devices *258*
Zones 259
INTRUSION OPERATIONS 260
Adding a Camera to a Zone or Area 260
Zones Window 261
Bypassing a Zone 262
Zone Alarm Status Indicator 262
Areas Window 262
Arming or Disarming an Area 263
Armed Setting Indicator 264

Chapter 26: Configuring and Using Point of Sale 265
OPERATIONS 265
Controlling the Video Player 267
Exporting Transactions 267
CONFIGURATION 268
Terminal Interface 268
Terminals 268

Chapter 27: NLSS Remote Management Services 269
EXAMPLE OF RMS DEPLOYMENT 269
RMS HIERARCHY 273
LOGGING IN TO THE NLSS RMS WEB INTERFACE 274
RMS MAIN MENU 274
VOLUME 275

© 2009-2014 Next Level Security Systems, Inc.

SITES 275
OPERATIONS 276
Media 276
Transferring a Video Clip to RMS 277
Export a Video Clip 277
Downloading a Video Clip 278
Multiview 279
Groups 280
CONFIGURATION 280
RMS Settings 280
Initial Registration 281
RMS Dependencies 282
Transferring RMS Settings 282
Transfer Status 283
Global 284
Customer 284
Sites 284
Holidays 287
Schedules 288
Event Type 288
Event Severity 289
Identity 290
Access Levels 290
Card Type 291
Cardholder Types 292
Cardholders 292
Permissions 295
Setting Up Groups in RMS 295
Setting Up Roles in RMS 295
Setting Up Users in RMS 296
EVENTS 297
RMS Event Log 297
FULL SCREEN 297
LOG OFF 298
HELP 298
TRANSCODE 298

Chapter 28: Next Level Mobile Application 299
SUPPORTED MOBILE DEVICES 300
GETTING STARTED 300
NAVIGATING THE NEXTMOBILE APP 303
RMS Options 305
Device Navigation 305
FAVORITES 308
SEARCHING A LIST 308
USING THE VIDEO PLAYER 309
REMOTE DOOR UNLOCK 312

© 2009-2014 Next Level Security Systems, Inc.

EVENTS 314
Event Details 316
MULTIVIEWS 318
CLOUD CLIPS 319
USING THE MOBILE APP WITH A DECODER 320
Check the Active Video 321
Setting a Channel to Active 321
Setting a View to Active 321
Setting a Sequence to Active 321

PART 5: APPENDICES 322

Appendix A: Performance and Setup Guidelines: Video Analytics, Face Recognition, and License Plate Recognition 323

VIDEO ANALYTICS METRICS 324
VIDEO ANALYTICS PERFORMANCE 325
SPECIFIC VIDEO ANALYTICS BEHAVIOR NOTES 325
FACE RECOGNITION 326
Face Capture and Face Recognition Guidelines for Best Results 326
Photograph Guidelines 326
IP Camera Guidelines 327
General Guidelines 327
Face Recognition Events and Actions 328
Event Linkage Examples 328
LICENSE PLATE RECOGNITION 329
License Plate Capture and License Plate Recognition Guidelines for Best Results 329
License Plate Recognition Events and Actions 330
Event Linkage Examples 330

Appendix B: Audio Analytics Guidelines 331

INTRODUCTION 331
GLASS BREAK ANALYTIC 332
Analytic Specifications 332
CAR ALARM ANALYTIC 332
Analytic Specifications 332
AGGRESSION ANALYTIC 333
Analytic Specifications 333
GUNSHOT ANALYTIC 333
Analytic Specifications 333
GENERAL SPECIFICATIONS 334
Environmental 334
Performance 334

© 2009-2014 Next Level Security Systems, Inc.

Configuration 334
SUPPORTED CAMERAS 335
USING AUDIO ANALYTICS 335

Appendix C: Contacting Support 336
GATEWAY INFORMATION 336
SYSTEM LOG 337
CONFIGURATION BACKUP 337
CONTACT INFORMATION 338

Index 339

© 2009-2014 Next Level Security Systems, Inc.

Preface

PURPOSE, SCOPE, AND AUDIENCE OF THIS MANUAL

This document explains how to install, configure, and operate the NLSS Unified Security Suite.

- **Part 1: Getting Started** highlights the features of the NLSS Unified Security Suite; provides installation instructions; and introduces the NLSS Web Interface.

Note: 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.**

- **Part 2: Operations** provides instructions for the day-to-day procedures for using the NLSS Security Suite Web Interface.

  The instructions in Part 1 and Part 2 are intended for anyone with basic familiarity with PCs, web browsers, and security concepts.

- **Part 3: System Configuration** provide procedures for setting up and maintaining the NLSS Unified Security Suite.

  These tasks require a slightly greater than average knowledge of these topics, and some IT knowledge in certain areas.

- **Part 4: Premium Features** provides instructions for configuring and using features that can be added to the NLSS Unified Security Suite.

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.

MORE INFORMATION

For more information about the NLSS Gateway, including release notes, a list of supported devices, and standalone product documents, see the NLSS Support website: **support.nlss.com**

© 2009-2014 Next Level Security Systems, Inc.

PART 1: GETTING STARTED

Getting Started includes:

- **Chapter 1: Introduction** - an introduction to the product,
- **Chapter 2: Installation** - installation instructions.
- **Chapter 3: Using the NLSS Web Interface** - introduction to the NLSS Web Interface.

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 NLSS Gateway or cloud camera, or to multiple Gateways and cloud cameras managed by *RMS* (*Remote Management 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.

© 2009-2014 Next Level Security Systems, Inc.

  - *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 **Chapter 5: Operations with 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 Services (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 a premium feature.)

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.

The NLSS Unified Security Suite comes installed on all NLSS Gateways.

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**.

© 2009-2014 Next Level Security Systems, Inc.

1.2.5 NLSS HD Decoder

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

NLSS strongly recommends the use of NLSS HD 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 (20.0 or above, Windows and Mac OS X only), Safari (5.1.10 for OS X v10.6, 6.1.4 for OS X 10.7-10.8), Internet Explorer (9.0 or later), or Chrome (26.0 or above).
- Adobe Flash Player 13.0 or above also must be installed. Check the Adobe web site for the latest version: **get.adobe.com/flashplayer**.

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.

© 2009-2014 Next Level Security Systems, Inc.

Chapter 2: Installation

This chapter provides instructions for using the NLSS Unified Security Suite software to discover your cameras and access control devices. (Installing the 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 NLSS HD Decoders installed on the same network.

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

- Access to the network on which the NLSS Gateway is installed.
- Multicore Intel processor.
- 2GB of RAM minimum. The 64-bit version of Windows requires 4 GB of RAM.
- Operating systems:
  - Windows 7 or Windows 8: 32-bit or 64-bit for both Windows versions
- 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 via the NLSS Gateway Web Interface.

- Minimum dual core processor
- Operating Systems:
  - Windows 7 or Windows 8: 32 bit or 64 bit for both Windows versions
  - Linux
  - Mac OS X v10.6 or above
- 2GB of RAM minimum

© 2009-2014 Next Level Security Systems, Inc.

- Access to the network on which the NLSS Gateway is installed.
- Supported browsers: Firefox (26 or above), Safari (6 or above), Internet Explorer (10 or above), Chrome (30 or above).
- Flash 13.0 or above also must be installed.

  Check the Adobe web site for the latest version: **get.adobe.com/flashplayer**. Check **adobe.com/software/flash/about/** for information on supported operating systems and Flash versions.

Important: Disable hardware acceleration for Flash in the browser.

2.2 CAMERA REQUIREMENTS

IP cameras must be installed on the same sub-network as the NLSS Gateway, for the Gateway to discover them. Cameras on other networks can be added via HTTP.

A list of supported cameras is located on the NLSS Support website: **support.nlss.com/customer/portal/articles/970656-cameras-and-encoders**

2.3 HARDWARE INSTALLATION

For instructions on physically installing NLSS Gateways and NLSS HD Decoders, see the *NLSS Gateway: Quick Start Guide*, which can be downloaded from **support.NLSS.com**.

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

2.4 SOFTWARE INSTALLATION

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

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

2.4.1 Install Security Certificate

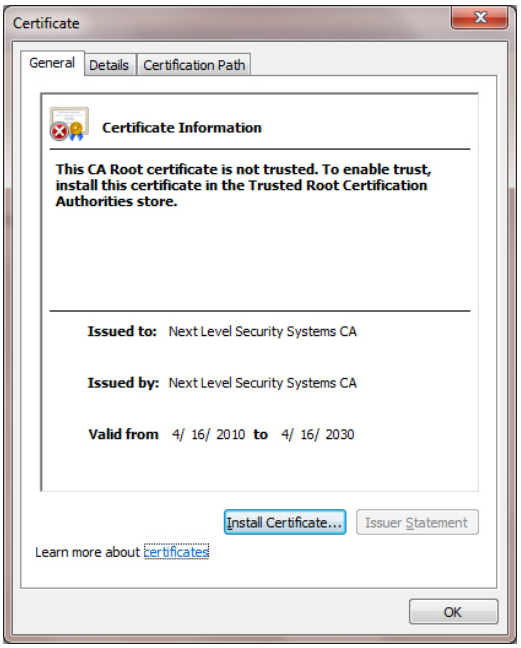
CA certificates are an important component of secure connections using the HTTPS protocol, which NLSS Gateways use for security purposes.

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.

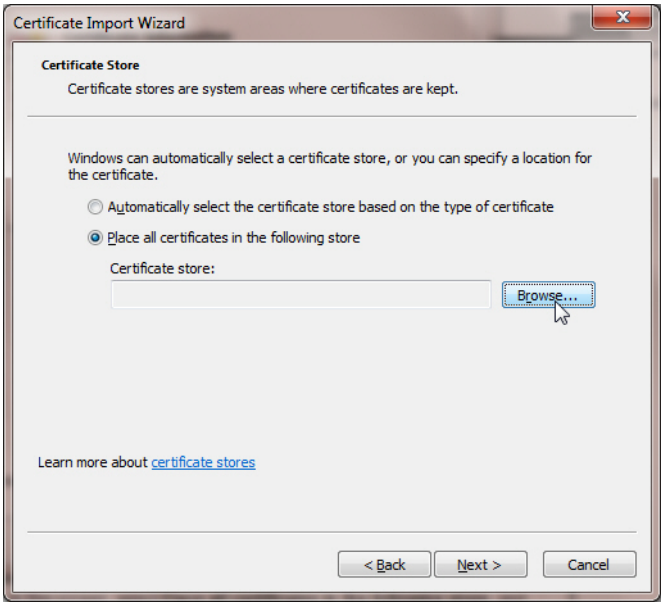
1. Using Internet Explorer, go to **http://support.nlss.com**.
2. Click the **Downloads** link to access the page for downloading NLSS CA certificates.

© 2009-2014 Next Level Security Systems, Inc.

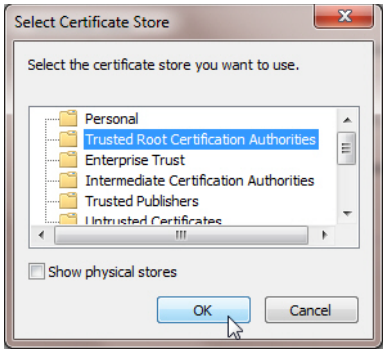
3. Download the **NLSS Certificate**, and save it to your desktop.
4. Double-click the certificate file on your desktop to display the Certificate dialog (see the figure below).



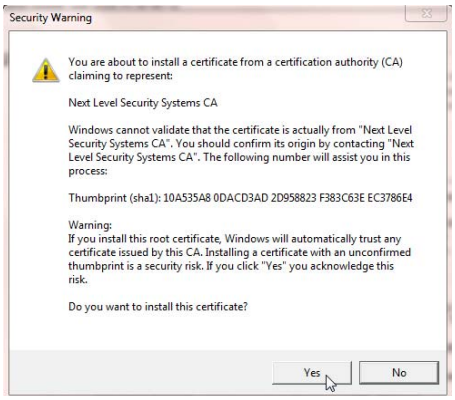
5. In the General tab of the Certificate dialog, click **Install Certificate**. The *Certificate Import Wizard* is displayed.
6. In the Wizard:
   a. Click **Next** to display the Certificate Store page.
   b. Select **Place all certificates in the following store**.
   c. Click **Browse** to display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



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



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



2.4.2 Install Cameras

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

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.

2.4.3 Install NLSS Gateways

1. Physically connect the 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 13.0 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.

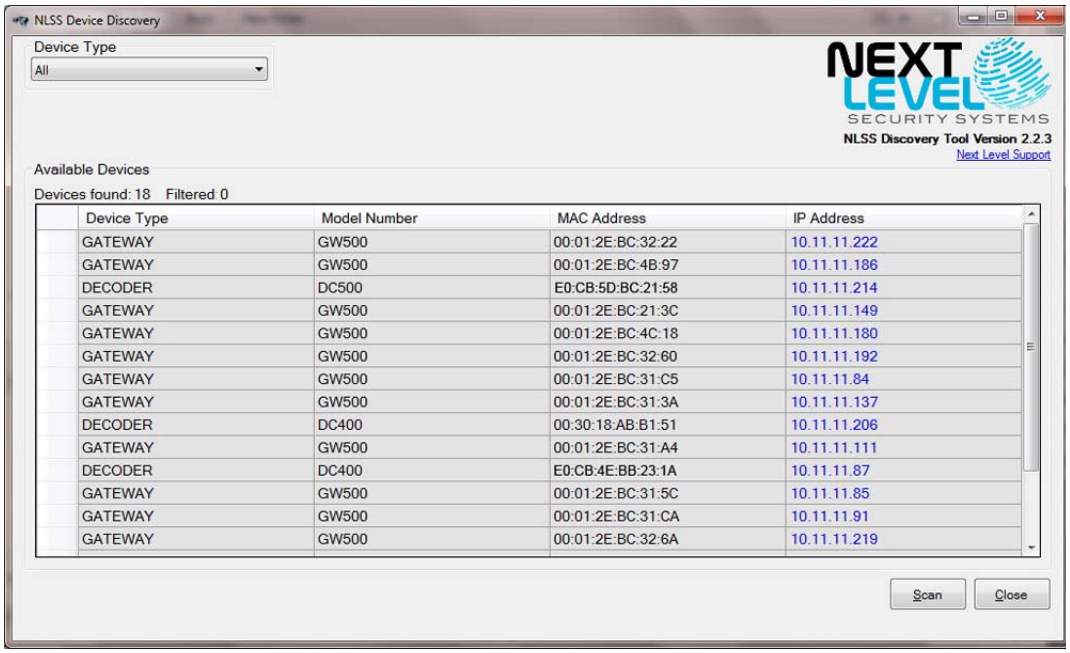
© 2009-2014 Next Level Security Systems, Inc.

2. Insert the supplied **NLSS Discovery Utility CD** into the computer's disc drive, or download the software from the NLSS web site (**support.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* window, click **Scan**. The Utility discovers all the NLSS Gateways, NLSS HD Decoders, and Cloud Cameras on the same LAN.



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

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

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

6. Click an IP address to open the NLSS Web Interface login window 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*.locall
(*note the removal of colons*)

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

© 2009-2014 Next Level Security Systems, Inc.

The NLSS Gateway's login window is displayed in the browser. This login window 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 *Configuration* > *Global* > *Gateways*, 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**.

2.4.3.1 Finding the IP Address without the Web Interface

If a problem occurs locating the Gateway with the Discovery Utility, and the MAC address is unavailable, the IP address can be discovered by directly connecting to the Gateway.

1. Ensure the Gateway is shutdown.
   – If the Gateway is running, *quickly press and release* the power button. This procedure allows the Gateway to shutdown properly.

Important: Do NOT press and hold the power button, or unplug the Gateway, as those actions can damage the Gateway by not allowing it to shut down properly.

2. Connect a monitor to the Gateway using an HDMI or DVI connection.
   – Do not use a VGA converter, as the Gateway's output signal is digital.
3. Connect a keyboard to a USB port on the Gateway.
4. Power up the Gateway.

   The Gateway takes about three minutes to boot up. A small, NLSS logo is displayed on the monitor when the boot up is complete.
5. Press **Ctrl**-**Alt**-**F6**.

   A login prompt is displayed.
6. Login with these credentials:
   – Username: **support**
   – Password: **nlss123**

   A menu is displayed.

```
==========================================

Please choose one of the following options:

1--Show local IP Address
2--Enable/disable ssh
3--FactoryReset
4--Display software version
5--Initiate Check Update
6--Initiate NLSS Support Session
7--Close all NLSS Support Sessions
Q--exit

==========================================
```

7. Enter **1**, and press **Enter**.

© 2009-2014 Next Level Security Systems, Inc.

The Gateway's IP address is displayed.

8. Enter **Q**, and press **Enter**.

   This option closes the menu.

9. Power down the monitor, and remove the monitor and keyboard.

10. In a browser on a computer connected to the same sub-network as the Gateway, log in as described in **Local Login**.

11. In the NLSS Web Interface, navigate to *Configuration* > *Global* > *Gateways*, 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**.

© 2009-2014 Next Level Security Systems, Inc.

Chapter 3: Using the NLSS Web Interface

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 21: 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.

Important: If the network is not using DHCP, then a *link-local address* is assigned to the decoder (*169.254.x.x*) when it is connected to the network. A static IP address must be entered in the IP Address field for the Gateway to communicate outside the local network. See **Wired Network Tab** in **Chapter 17: Global Configurations** in **Chapter 17: Global Configurations** for more information.

When the browser connects to the target Gateway, a login window 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.

© 2009-2014 Next Level Security Systems, Inc.

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 put into service with this Gateway. Devices are put into service by setting the **Administrative State** to **In Service** in the **Configuration** menu for the device type. See **Configure Cameras and Streams** in **Chapter 20: Configure Video, & Storage, & Decoders** for more information.

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 Off

If the NLSS Gateway detects no activity in the NLSS Web Interface for 60 minutes, then the system automatically logs off the user who logged in last. This security feature prevents unattended interfaces from being 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 USING THE NLSS WEB INTERFACE

After logging in, the NLSS Unified Security Suite Web Interface is opened. The Web Interface provides access to the Security Suite features. Access to each feature is determined by permissions set for the user who is logged in. Users with unlimited permissions can access all menu options. See **Roles** and **Users** in **Chapter 21: Configuring Permissions** for more information.

Mouse-over a button in the Web Interface to display a *Tool Tip*.

Features are accessed through the Main Menu at the bottom of the window. The bottom pane also contains two information boxes describing the current state of the system:

- **Current User**: the user logged into this NLSS Web Interface session.

© 2009-2014 Next Level Security Systems, Inc.

- **Latest Event**: the most recent event detected by the NLSS Gateway. The NLSS Web Interface can play an audio alert notification when an event is detected.

3.3 MAIN MENU

The Main Menu contains three modules for using the NLSS Web Interface:

Operations **Configuration** **Events**

Operations and Configuration provide options that are displayed in the left column of the Web Interface.These modules and options are discussed later in this chapter and in the following chapters.

The Main Menu contains these additional options:

Volume: opens a slider to set the volume for audio played locally through the Web Interface when events occur.

Full Screen: toggles between full-screen and windowed modes.

Log off: ends your session in the NLSS Web Interface.

© 2009-2014 Next Level Security Systems, Inc.

Help: opens the on-line help system.

Transcode: adjusts resolution of the video displayed in the Web Interface.

3.3.1 Operations

In the Operations menu in the left pane 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 under the Gateway's name.

- **Media**: a search-able catalog of audio and video files that the Gateway can play. See **Chapter 10: Media Operations** for more information.
- **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 Decoders for display on remote monitors. See **Push Media Clips, Views and Sequences to Decoders** in **Chapter 9: Displaying Video** for instructions.
- **Doors:** locking and unlocking doors manually, as well as running individual door reports. See **Chapter 6: Operations with Doors** for instructions.
- **Cardholders/Users**: tracing and deactivating individual cardholders, as well as running individual cardholder reports. See **Chapter 7: Operations with Cardholders & Users** for instructions.
- **Reporting**: run reports that summarize events, etc. See **Chapter 8: Operations with Reports** for instructions.
- **Views:** create custom video display layouts, using one or multiple cameras or video streams. See **Chapter 9: Displaying Video** for instructions.
- **Sequences**: create automated progression of views to display when launched. See **Chapter 9: Displaying Video** for instructions.
- **Groups**: access groups created in Configuration > Permissions > Groups. See **Chapter 14: Using Groups** for instructions.

© 2009-2014 Next Level Security Systems, Inc.

3.3.1.1 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** in **Chapter 4: Controlling Cameras** for more information.

1. Open the NLSS Gateway Web Interface.
2. Select **Operations in** the Main Menu.
3. Select the ***gateway's name*** or ***IP address***, at the top of the Operations options in the left column. For example, *GW4000-IP: 10.1.9.10*.

   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 readouts and colored gauges summarize the Gateway's health.

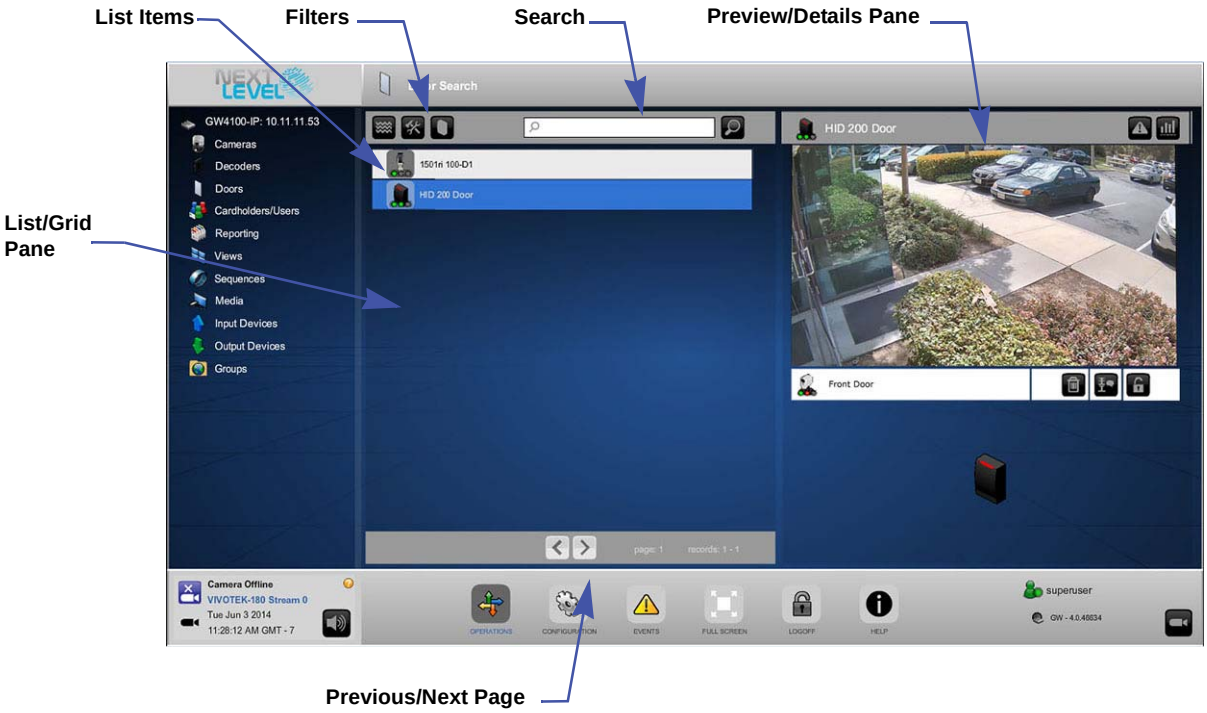
Color	Cause
Green	Operating within normal parameters.
Yellow	System is exceeding 70% of the RAM or processor capacity.
Orange	System is exceeding 80% of the RAM or processor capacity.
Red	System is exceeding 85% of the RAM or processor capacity.

- **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.

- **GPU Memory Usage**: the percentage of the graphics processor 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.

3.3.1.2 Operations Windows

When the Operations > Media, Doors, Decoders, or Cardholders/Users options are selected, List and Preview or Details panes are displayed. The Cameras and Reporting options display a single pane with a list to drill down to the camera or report. Views, Sequences and Groups display the item selected under that option. Each Operations menu option is discussed in the chapters in **Part 2: Operations**.



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 Media, Cameras and Cardholders/Users.

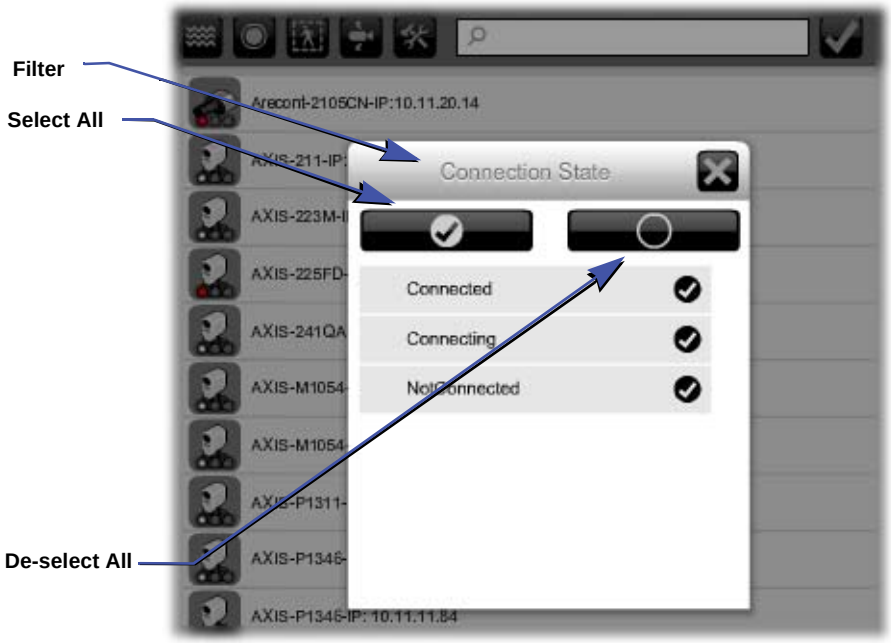
- **Previous/Next Page**: provides navigation through multiple pages of items. These buttons are grayed out if only one page of items is available.
- **List Item**: accesses the selected item. Click on a list item to display that item.

  Selected decoders and doors also display a mini-video player in the right pane, if video is available. Selected cameras, views, and sequences also display video.

3.3.1.3 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.
   - De-select an option to hide the matching items in the list.
   - Click **Select All** (check mark) to choose all options in the dialog.
   - Click **De-select 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**.

3.3.1.4 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**.

3.3.2 Configuration

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 options for configuring the Gateway, and events. See **Chapter 17: Global Configurations** for instructions.
- **Identity**: provides options for configuring cardholders and access levels. See **Chapter 18: Configure Identity and Credentials** for instructions.
- **Access Control**: a premium features that provides options for configuring access to doors and other entries that are monitored by your NLSS system. See **Chapter 19: Configure Access Control** for instructions.
- **Video**: provides options for configuring installed cameras, NLSS HD Decoders, and external storage devices. See **Chapter 20: Configure Video, & Storage, & Decoders** for instructions.
- **Permissions**: create *Groups*, *Roles*, and *Users*.
- **Intrusion**: configure the Gateway to work with Panels, Areas, Devices, and Zones. See **Chapter 11: Operations with Input Devices** and **Chapter 12: Operations with Output Devices** for more information.
- **Face Recognition**: set up for an add-on video analytic. See **Chapter 22: Configuring and Using Face Recognition** for instructions.
- **Licnese Plate Recognition**: set up for an add-on video analytic. See **Chapter 23: Configuring and Using License Plate Recognition** for instructions.

© 2009-2014 Next Level Security Systems, Inc.

3.3.3 Events

The Events menu provides a timeline of all system events in an Event Log view. Superusers and users with *Operator* permissions typically have access to everything under the Events menu. For details, see **Chapter 15: Monitoring and Handling Events**.

3.3.4 Full Screen Toggle

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 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.

3.3.5 Log off

Click **Logoff** in the Main Menu to close the current RMS session. The Login window is dis played.

3.3.6 Help

The NLSS Unified Security Suite includes a help system to provide detailed configuration and operation instructions for the local Gateway interface.

- Click **Help** in the Main Menu.

The help system is displayed in a new tab.

3.3.7 Transcode

All video displayed through the Web Interface can be set to a lower resolution if bandwidth usage becomes an issue. A maximum resolution of 1080p can be transcoded.

Note: This button is hidden when the video player is displayed.

- Click **Transcode** in the main menu before opening a video player.

The frame rate, bit rate and resolution are adjusted to alleviate bandwidth issues. Only the video being displayed reflects the setting. The setting does not impact recorded video.

The camera icon in the transcode button becomes smaller to reflect the lower resolution.

- Click **Transcode** again to return to the camera setting for the video.

Important: Selecting these settings at in the main menu impacts all video displayed in this session, but does not impact the video displayed in the Web Interface for other users.

© 2009-2014 Next Level Security Systems, Inc.

PART 2: OPERATIONS

Part 2: Operations includes instructions and background information for using the options under the Operations module.

A Web Interface User's access to these options is dependent on the permissions assigned to the role associated with the user. Permissions and roles are discussed in **Chapter 21: Configuring Permissions**.

- **Chapter 4: Controlling Cameras** - provides instructions for using the built-in video player, and the video analytics and forensics. Among the analytics are activity detection and face recognition.
- **Chapter 5: Operations with Video Analytics** - provides instructions for configuring and using video analytics available through the video player.
- **Chapter 6: Operations with Doors** - provides instructions for monitoring a door's status, remotely unlocking a door, and associating a camera with a door.
- **Chapter 7: Operations with Cardholders & Users** - provides instructions for viewing cardholder and user information, and activating and deactivating cardholders.
- **Chapter 8: Operations with Reports** - provides instructions for configuring, running reports, printing and saving.
- **Chapter 9: Displaying Video** - provides instructions for displaying video from multiple cameras using views and sequences.
- **Chapter 10: Media Operations** - provide instructions for using the Media Library, including how to download video clips to a local computer.
- **Chapter 11: Operations with Input Devices**: provides instructions for using input devices, and associating cameras to those devices.
- **Chapter 12: Operations with Output Devices**: provides instructions for using activating and deactivating output devices, and associating cameras to those devices.
- **Chapter 13: Using Floor Plans** - provides links to configuration instructions for floor plans.
- **Chapter 14: Using Groups** - provides an overview of how groups work, plus instructions for using groups, and creating and using maps and floor plans.
- **Chapter 15: Monitoring and Handling Events** - provides instructions for accessing events, and using the Event Log to review the incidents that triggered an event.

© 2009-2014 Next Level Security Systems, Inc.

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 a camera's operations and configurations, in general, is controlled by permissions. Access to specific, pre-configured cameras can be controlled by groups. See **Chapter 21: Configuring Permissions** for more information.

To be discovered, a camera or encoder:

- Must be physically attached to the same sub-network as the Gateway.
- Must be turned on.

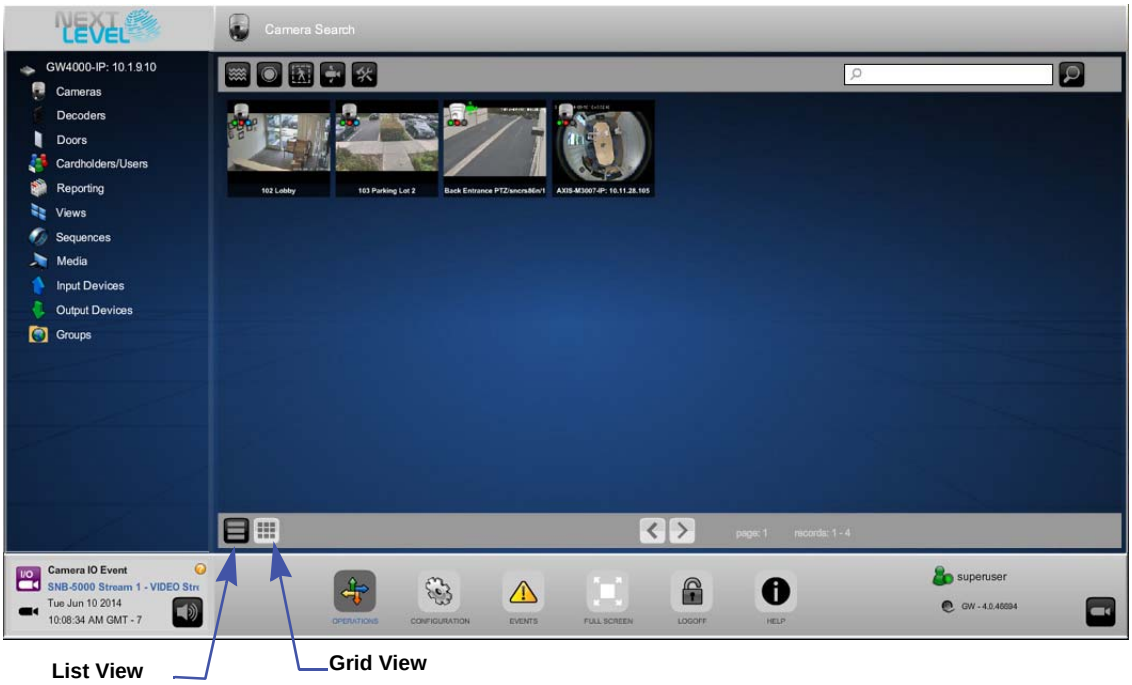
Starting with NLSS Security Suite v3.1 and later, Verint encoders are also automatically discovered, if the device is on the same LAN as the Gateway, and the default port setting is used. Each encoder stream is displayed separately.

Streams from cameras and Verint encoders on other networks can be added. See **Configure Cameras and Streams** in **Chapter 20: Configure Video, & Storage, & Decoders** for instructions on adding streams.

Important: Discovering a camera is not enough to view its video streams. To see video, the system must connect to the camera, which requires configuring the Gateway to use the camera's user name and password, and setting the Admin State to *In Service*. See **Configure Cameras and Streams** in **Chapter 20: Configure Video, & Storage, & Decoders** for configuration instructions.

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

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



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

The list has two viewing options:

- **Grid view**: displays a thumbnail of the camera's stream. The thumbnail updates automatically.
- **List view**: displays the camera's name and icon.

The NLSS Gateway supports many camera features, as listed in this chapter. However, some cameras do not 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: Only users with Superuser or the appropriate permissions can configure cameras. See **Chapter 21: Configuring Permissions** for more information.

In the Cameras list, the icon displayed next to each camera's name indicates the operational state of the camera.

© 2009-2014 Next Level Security Systems, Inc.

4.1.1 Camera Icons

Camera icons vary according to the camera model, such as these examples.

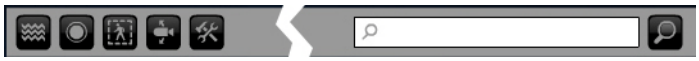
The Streaming symbol indicates an RTSP or HTTP video stream.

- Green LED: indicates the system is successfully connected to the camera.
- Yellow LED: not connected/off line.
- Red LED: indicates that the camera is currently recording.
- Blue LED: indicates that analytics are running.

  A blue LED in a window 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.

4.1.2 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.



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

Connection State: Connected, Connecting, Not Connected

Active Recording: All, Active, Inactive

Active Analytics: All, Active, Inactive

PTZ: All, Yes, No

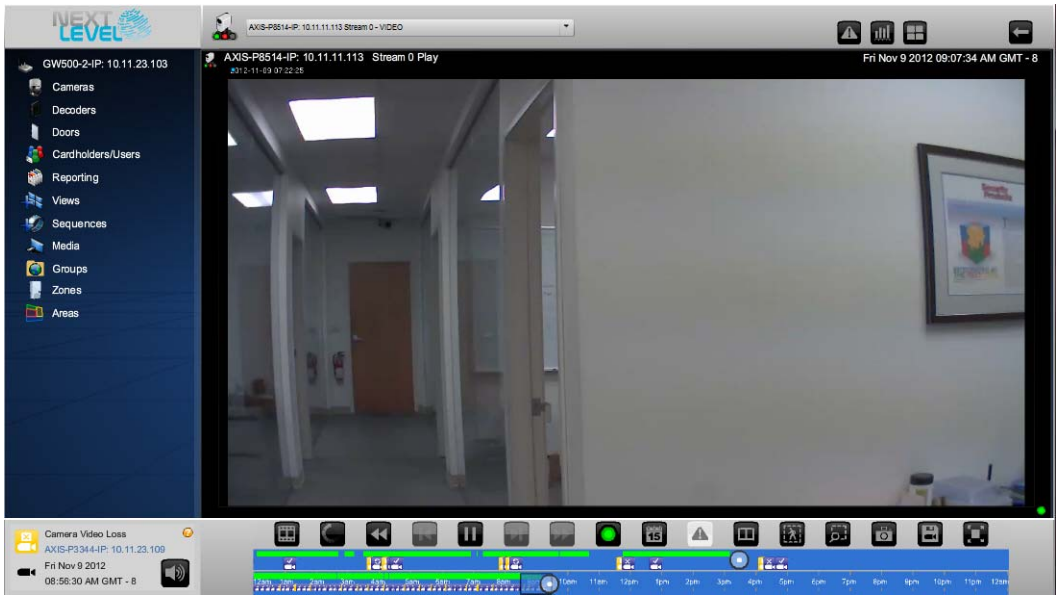
Admin State: In Service, Out of Service, Preprovisioned

© 2009-2014 Next Level Security Systems, Inc.

4.1.3 Video Player

The Video Player is used to operate the camera, and view recorded video.

- Click the corresponding link to select a camera or video stream.
  The NLSS Web Interface video player is displayed.
  The video player contains a series of fields and options.
  – The name of the camera or stream.
  – Links to Events and Reports for that camera or stream.
  – Buttons to control and configure the video and the player.
  See **Using the Camera Toolbar** for instructions on using the video player.



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 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

Camera streams can be displayed from three locations under the Operations menu in the NLSS Web Interface:

- **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 9: Displaying Video** for instructions on configuring and using Views and Sequences.

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

© 2009-2014 Next Level Security Systems, Inc.

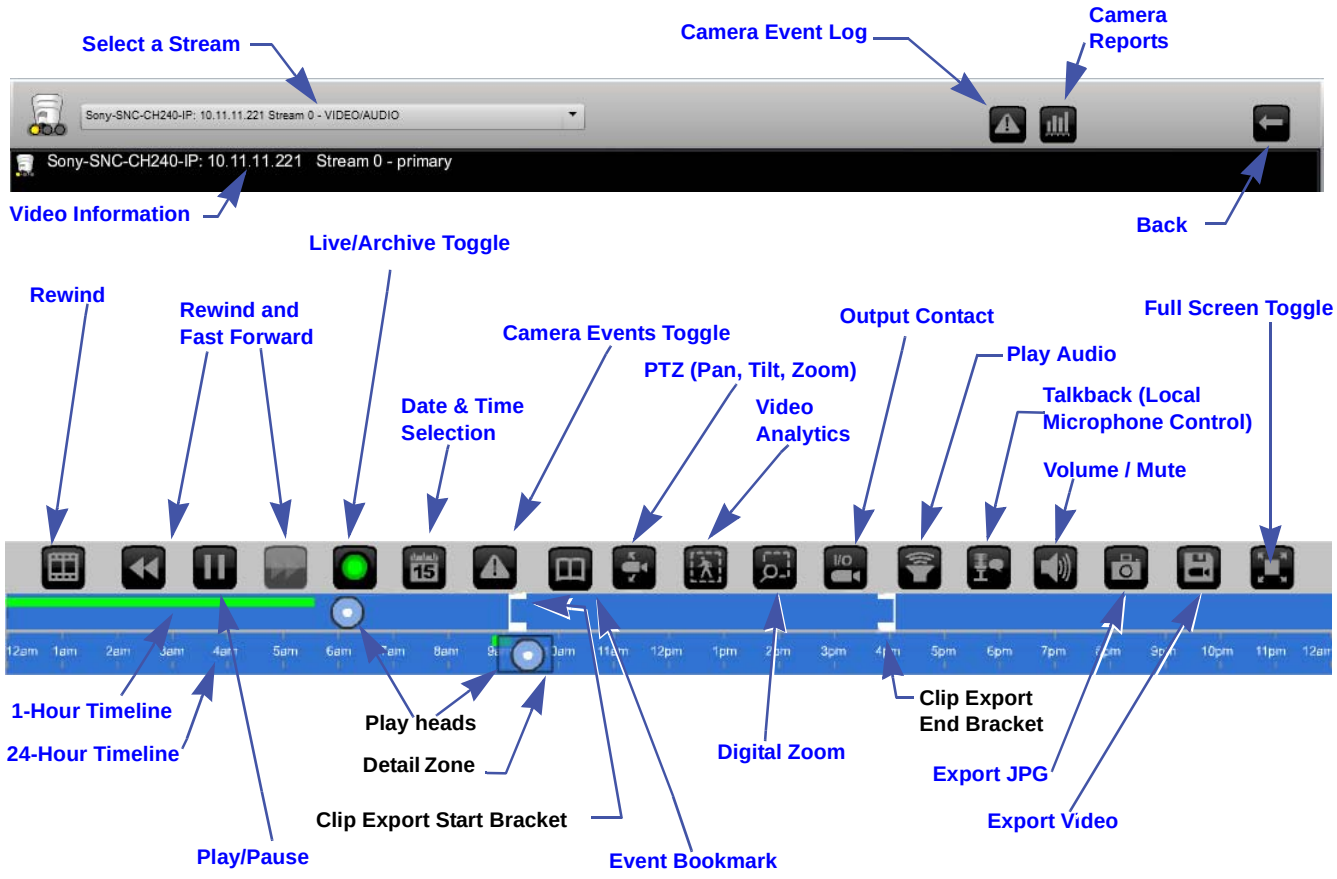
4.2.2 Using the Camera Toolbar

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 a thumbnail or item in the camera list.

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 can be controlled by permissions. See **Chapter 21: 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.

- **Device Name**: the name assigned to the camera or stream when it was configured. See **Camera Details General Tab** in **Chapter 20: Configure Video, & Storage, & Decoders**.

- **Stream**: the stream currently displayed, as selected from the drop-down list above the video player. See **Select a Stream** in **Chapter 20: Configure Video, & Storage, & Decoders**.

Note: Some cameras output multiple streams simultaneously. Each stream 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.

4.2.2.2 *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/Archive 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 **Timelines**, and the **Rewind and Fast Forward** buttons.
3. Toggle between **Play** and **Pause** to start and stop playback.

4.2.2.3 *Live/Archive* Toggle

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

The Live/Archive 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 **Timelines**, the **Rewind and Fast Forward** buttons, or **Rewind and Fast Forward** buttons.
3. Click **Play** and **Pause** to start and stop playback.
4. To return to the live video stream, click the **Live/Archive** toggle button.

4.2.2.4 Rewind and Fast Forward

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

1. Click **Play/Pause** in the toolbar to play recordings made from this camera.

2. In the toolbar, use the **Date & Time Selection** buttons, the **Timelines**, or both, to select the day and time to rewind to.
3. Use the **Rewind** and **Fast Forward** buttons to move through the video.

© 2009-2014 Next Level Security Systems, Inc.

Note: Click the **Rewind** and **Fast Forward** buttons repeatedly to cycle between 0.5x, 2x, 5x, 10x, and 50x speed. The amount of video that the play head moves depends on the frame rate at which the video was recorded.

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

4.2.2.5 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 requested. This setting allows selection of video for playback or export. See **Export Video** for instructions.

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 **Timelines** 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/Archive Toggle** to return to live video. The button turns green when live video is displayed.

4.2.2.6 Camera Events Toggle

Event markers can be displayed or hidden in the timeline.

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

4.2.2.7 Event Bookmark

A bookmark is a manually defined event.

1. To manually add an event to the timeline, click **Bookmark** 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 Event Log** window, open *Event Notes* for the book marked event that you just set, and enter notes about the event.

© 2009-2014 Next Level Security Systems, Inc.

4.2.2.8 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 **PTZ** 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 **Accessing Patrols** for more information.

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

4.2.2.8.1 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 **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

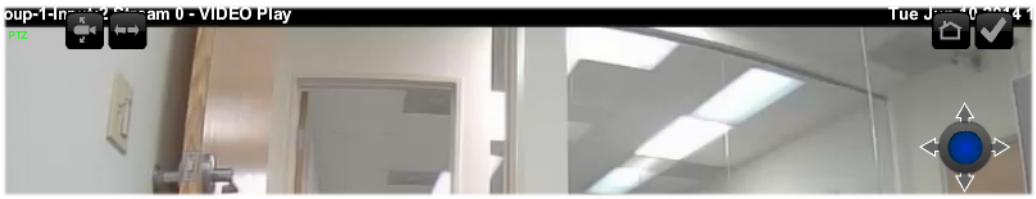
1. Move and zoom the camera to the desired position for a Home preset.
2. Click **Update** to set this position as the Home preset.

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 in the middle of the window).



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.

© 2009-2014 Next Level Security Systems, Inc.

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 setting to be deleted from the list.

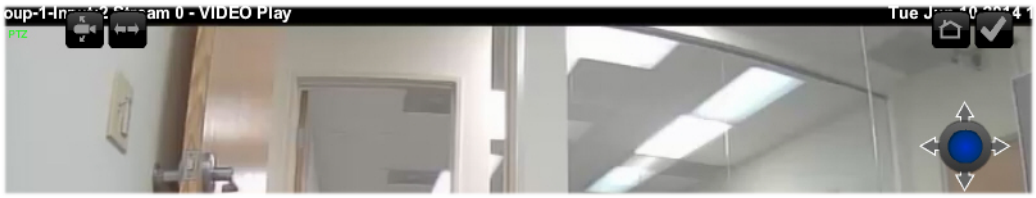
4.2.2.8.2 Accessing Patrols

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 **PTZ** in the toolbar to access the Patrol functionality.
   From the PTZ window, 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 in the middle of the window).



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.

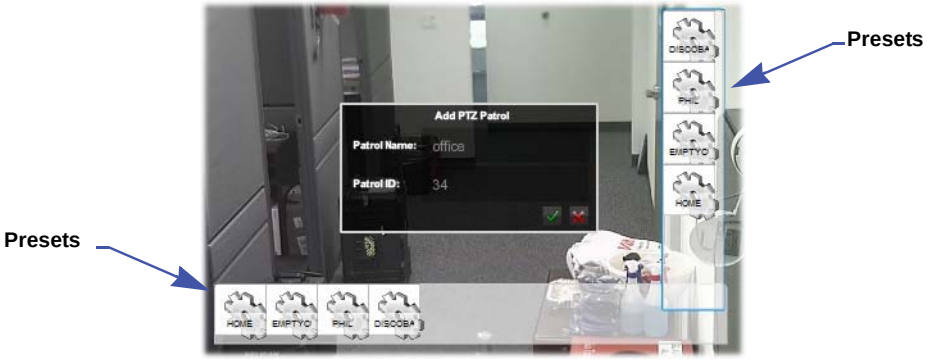
CONFIGURE AND EDIT PATROLS

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.

© 2009-2014 Next Level Security Systems, Inc.

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.



- 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.

4.2.2.9 VIDEO ANALYTICS

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

See **Chapter 5: Operations with Video Analytics** for instructions on configuring and using video analytics.

© 2009-2014 Next Level Security Systems, Inc.

4.2.2.10 Audio Analytics

If a camera has a built-in or attached microphone, audio analytics can be applied.

When an Audio Analytic is activated for a camera, the Gateway analyzes detected sounds, then compares it to sounds that can trigger an event. If a match is made, an event is generated.

By default, the NLSS Gateway includes an Audio Analytic for *glass break*.

Other audio analytics are available as a premium feature enabled by a token.

See **Chapter 24: Configuring Audio Analytics** for instructions on configuring and using audio analytics.

4.2.2.11 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 to move the display.
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.

4.2.2.12 Output Contact

Devices such as door locks, alarms, or flashing lights can be operated from a contact switch on a camera. This switch can be triggered from the video player.

- Click **Output Contact** 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.

4.2.2.13 Play Audio

Sound effects and audio warnings can be played through a speaker attached to a camera, if available. An audio file can be associated with a camera using Configuration >Global >Actions.

This audio can be triggered manually from the video player, or automatically using Event Linkages. See **Configure Actions** and **Configure Event Linkages** in **Chapter 17: Global Configurations** for instructions on automatic triggering.

Manual triggering is used when the user watching a camera observes an event or behavior that requires a warning.

1. Open a camera or stream in the video player.
2. Click **Play Audio**.

The audio files are included with the Web Interface. See **Chapter 10: Media Operations** for more information.

© 2009-2014 Next Level Security Systems, Inc.

4.2.2.14 Talkback (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 **Talkback** in the toolbar.
3. Drag the slider up and down to increase or decrease the local microphone's volume through the camera's speaker.

4.2.2.15 *Volume / Mute*

The NLSS Gateway supports full duplex audio. The toolbar contains a slider that controls the volume of the computer's speaker.

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

4.2.2.16 Export JPG

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

1. Select a camera and open the video player.
   – If you want an image of a recorded clip, navigate to the location in the timeline.
2. Click **Export JPG**.
   A dialog is displayed.
3. Follow the prompts to save the picture.

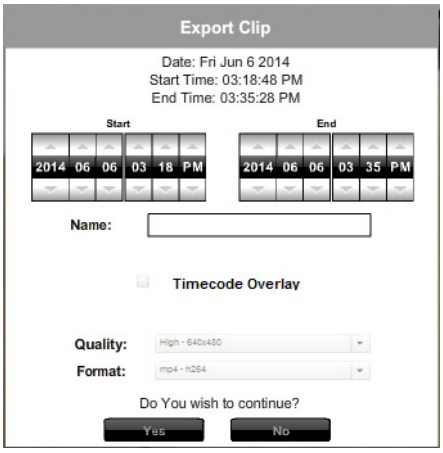
4.2.2.17 Export Video

A clip from a recording can be exported if the selected camera or stream is configured to record, and the target recording period has been saved. The file is sent to the Media Library. The file also can be saved to the local computer.

1. Select a camera and open the video player.
2. If the time and date of the clip are not known, use the **Date & Time Selection**, the **Timelines**, and the **1-Hour Timeline** to locate the clip.
3. Click **Export Video**.

© 2009-2014 Next Level Security Systems, Inc.

A dialog is displayed to set the date and time range of the clip to be exported.



If the time and date of the clip are not known, use the **Date & Time Selection**, the **Timelines**, and the **1-Hour Timeline** in the player to locate the clip.

4. Set the **Start** and **End** date and time.

Important: A maximum of four hours of video can be exported in one clip.

Although export can be simultaneously run on multiple cameras, exporting several large files at the same time can impact Gateway performance.

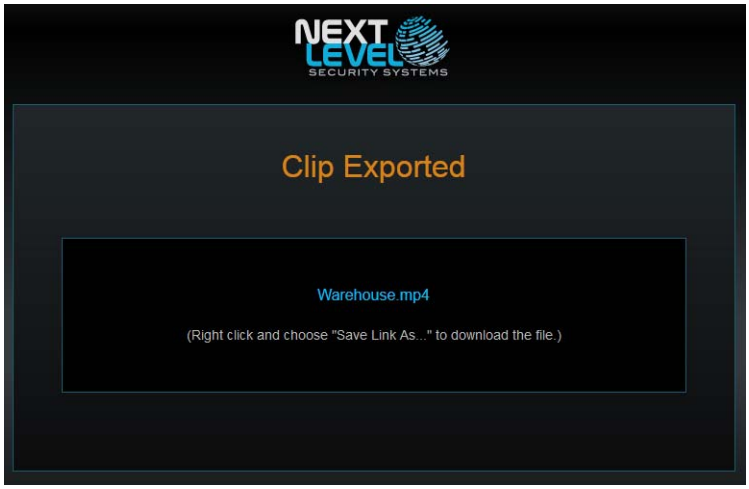
5. Enter a **Name** for the clip.

   The default file name is the name of the camera. Change the file name. If the default file name is used, it overwrites previous files with the same name.

6. In the Export dialog, click **Yes** to start the export.
   – Click **No** to cancel the export.

   An icon in the Main Menu indicates that the export in underway.

7. When the export is complete, the browser displays a pop-up window or dialog box, depending on the browser. The clip can be downloaded and saved locally. Follow the prompts to download the clip.



Note: If the Gateway is accessed via the RMS Sites map, the clip is placed in the Gateway's Media Library to be transferred to the RMS Media Library for exporting. See **Export a Video Clip** in **Chapter 27: NLSS Remote Management Services** for more information.

When the export is complete, the clip is automatically saved in the Gateway's Media Library. See **Chapter 10: Media Operations** for more information.

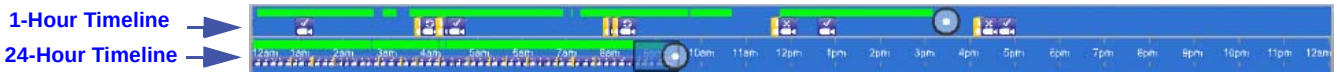
4.2.2.18 *Full Screen Toggle*

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 *Timelines*

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



4.2.2.19.1 24-Hour Timeline

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

The 24-hour timeline includes:

- A **Detail Zone** is a transparent 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 Timeline** in the top portion of the timeline.

  The brackets are not displayed unless the system contains recorded video for that camera.

- The **Time Indicator** is a cursor that can be moved to an earlier hour on the 24-hour timeline, 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 Timeline

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

- The exact start and end times of the 1-hour timeline are displayed at either end of the slider.
- Drag the **Time Indicator** 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 **Export Video**.

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 a Stream

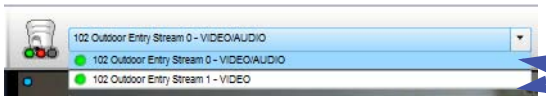
Some cameras simultaneously output more than one stream. Streams may have different codecs or resolution settings, or both. If a camera supports multiple streams, and the NLSS Web Interface is configured to handle more than one stream from that camera, then a stream can be selected to display in the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

A stream must be enabled in the Streams tab of the Configuration > Video > Cameras window. 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 LED next the menu item indicates the selected stream.



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

4.2.3.2 Low Resolution/Native resolution

If bandwidth becomes an issue for displaying video, the displayed video can be transcoded to display at a lower resolution.

Note: This button is hidden when the video player is displayed.

- Click **Transcode** in the main menu before opening a video player.

The Gateway adjusts the frame rate, bit rate and resolution to alleviate bandwidth issues. The quality of the video also reflects the setting.

The camera icon in the transcode button becomes smaller to reflect the lower resolution.

- Click **Transcode** again to return to the camera setting for the video.

Important: Selecting these settings impacts all displayed video from the Gateway.

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 Camera Event Log

1. Click **Operations >Cameras**.
2. Select a camera or video stream.
3. Click **Events** in the top bar of the video player.

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

   See **Chapter 15: Monitoring and Handling Events** for instructions on using events.
4. Click **Return** to go back to the video player.

4.2.3.3.1 Camera Events

The following types of events are associated with a camera or stream:

- **Video Analytics** that are set up for this camera or stream.
- **Event Bookmark** that is manually set up for this camera or stream.
- The *operational status* reported by this camera or stream, such as going online or offline, video or channel loss, video resumed or bookmarked, clip or video exported successfully or not.
- **Motion Event** as set up through the camera.
- **Input Port** as set up through the camera.

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

© 2009-2014 Next Level Security Systems, Inc.

4.2.3.3.2 Motion Event

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.

4.2.3.3.3 Input Port

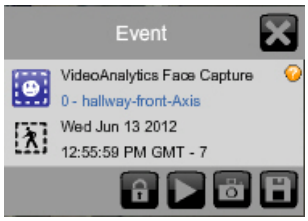
Some cameras contain an input port that generates an *I/O Event* when triggered. The NLSS Gateway can accept this event from many cameras, and lists that event with other events. This event is configured within the camera, not in through the NLSS Web Interface.

4.2.3.3.4 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. Click 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 window. The dialog appears in the same location when accessed for subsequent events.



3. In the dialog:

Click **Lock** to prevent the event from being groomed (deleted). The event is added to the *lock* queue in the Events module, and cannot be deleted until it is unlocked. See **Configure Groomer Settings** for more information about grooming stored video.

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 make a copy of the video for the event. The clip is downloaded to the local hard drive on which the web interface is being accessed.

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

4. Click the event marker.

   The timeline cursor is placed at that location, and recorded video is played, as indicated by the red **Live/Archive Toggle** in the timeline.

5. Click **Close** to exit the dialog.
6. Click the toggle again to return to live video, indicated by the green toggle.

© 2009-2014 Next Level Security Systems, Inc.

4.2.3.3.5 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.

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

4.2.3.4 Camera Reports

1. Click **Operations >Cameras**.
2. Select a camera or video stream.
3. Click **Reports** in the top bar of the video player.

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

   See **Chapter 8: Operations with Reports** for instructions on using reports.
4. Click **Back** to go back to the video player.

4.2.3.5 Back

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

© 2009-2014 Next Level Security Systems, Inc.

Chapter 5: Operations with Video Analytics

This chapter provides instructions for setting up and using video analytics.

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

5.1 PARAMETERS

The NLSS Unified Security Suite provides 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.

NLSS analytics can only be used if the video streams are no more than1080p.

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 License Plate Capture Line Crossing People Count People Count Direction Perimeter

Metric Level	Video Analytic
2	Dwell Face Recognition Forensics (except those noted below) License Plate Recognition Object Moved Object Taken
3	Forensic Face Recognition Forensic License Plate Recognition

The total number of *Metric 1* video analytics that can be supported is determined on a per platform (NLSS device) basis.

See **Appendix A: Performance and Setup Guidelines: Video Analytics, Face Recognition, and License Plate Recognition** for recommendations and performance guidelines for running Video Analytics.

Important: The optimal setting for Video Analytic success is 15 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 Event Log** in **Chapter 4: Controlling Cameras**.

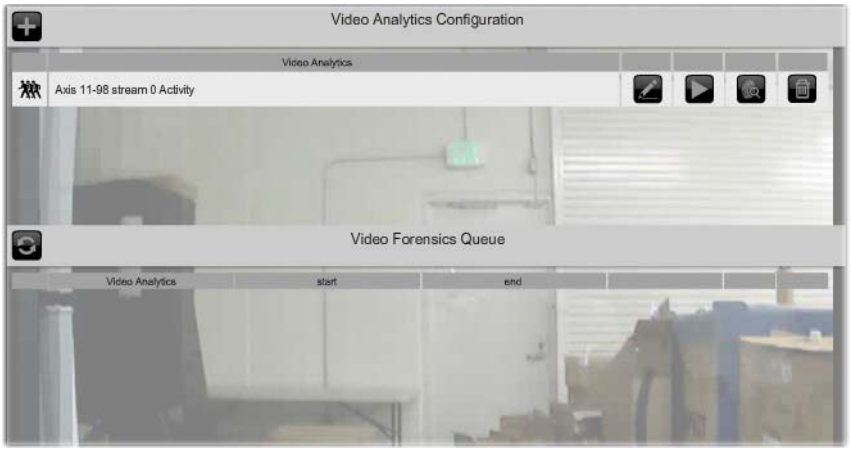
5.2 USING VIDEO ANALYTICS

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. Click **Analytics**.

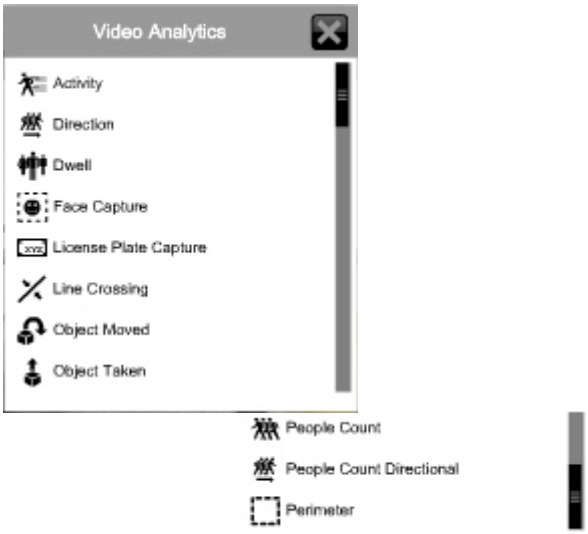
   The *Video Analytics Configuration* overlay is displayed with the *Video Analytics Configuration* list and *Video Forensics Queue*.
   - The *Video Analytics Configuration* list contains the analytics set for this camera. From this list, you can edit, play or pause, or delete an analytic. You can also 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**.

© 2009-2014 Next Level Security Systems, Inc.

– 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 sections.

   – **Activity**
   – **Direction**
   – **Dwell**
   – **Face Recognition**
   – **License Plate Capture and License Plate Recognition**
   – **Line Crossing**
   – **Object Moved**
   – **Object Taken**
   – **People Count**
   – **People Count Directional**
   – **Perimeter**

© 2009-2014 Next Level Security Systems, Inc.

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.

Note: The defined detection area for the following analytics needs to be bigger than 50% of the detected object size in order to trigger event. For example, if a person takes up 100 pixels on the screen, the Line Crossing detection line needs to be 50 pixels long when configured for the analytic.

- Activity
- Direction
- Dwell
- Line Crossing
- People Count
- Perimeter
- People Count Directional

5.2.1 Activity

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

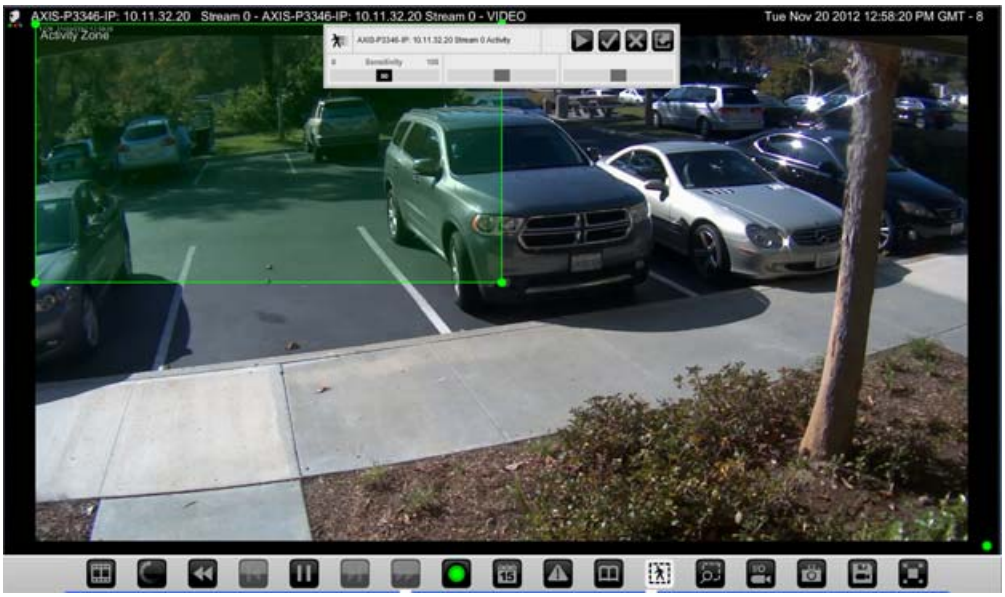
1. Click **Edit** for **Activity** in the Video Analytics Configuration list.

   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.

© 2009-2014 Next Level Security Systems, Inc.

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

5.2.2 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.

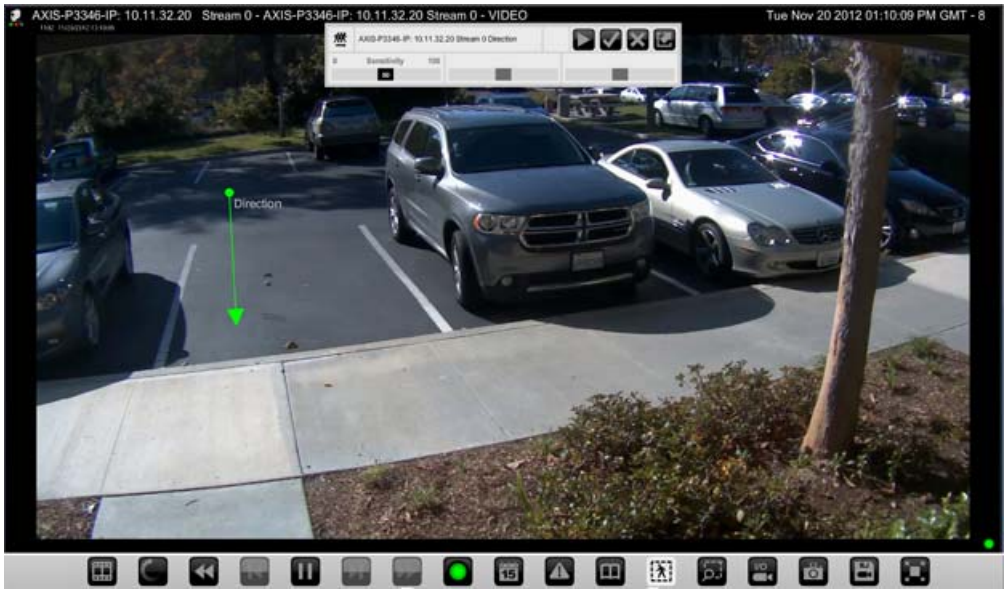
1. Click **Edit** for **Direction** in the Video Analytics Configuration list.

   The video player is displayed containing a line with an arrow indicating the direction in which movement is monitored.

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

© 2009-2014 Next Level Security Systems, Inc.

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



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

5.2.3 Dwell

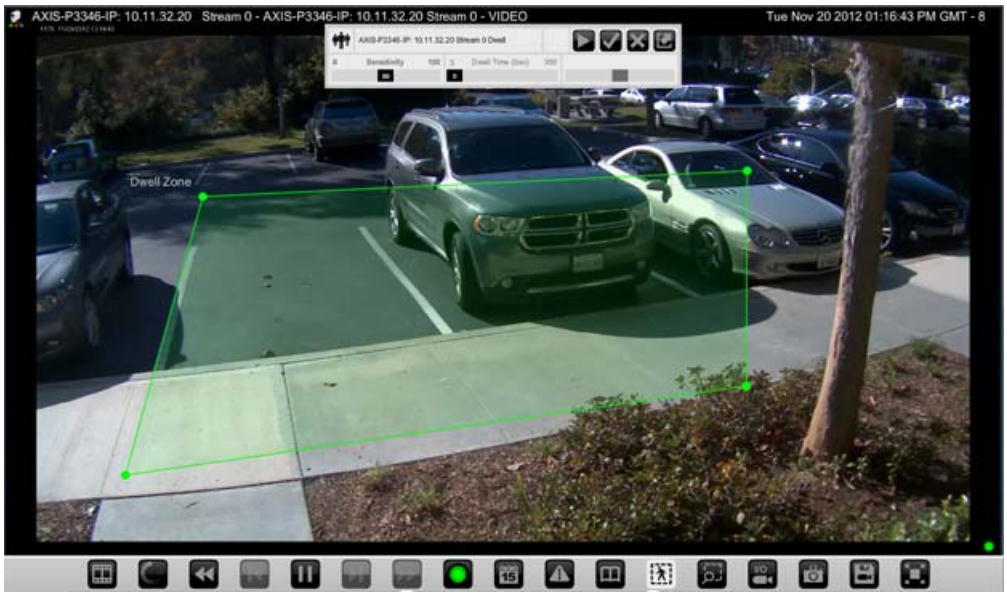
Dwell detects when an object or a person moves into a monitored location and stays longer than a designated time.

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

   The video player is displayed with a *Dwell Zone* highlighted, a rectangle by default.
2. Drag the rectangle to move the shape to the area that you want to monitor.

© 2009-2014 Next Level Security Systems, Inc.

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 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.

5.2.4 Face Capture

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

Face Capture is a standard Video Analytic included with the NLSS Unified Security Suite.

Face Recognition is a premium, add on feature. Face Capture does not need to be configured and launched if Face Recognition is running. When Face Recognition is running, a Face Capture event is generated before the Face Recognition event.

However, Face Capture can be run if Face Recognition is not running or enabled.

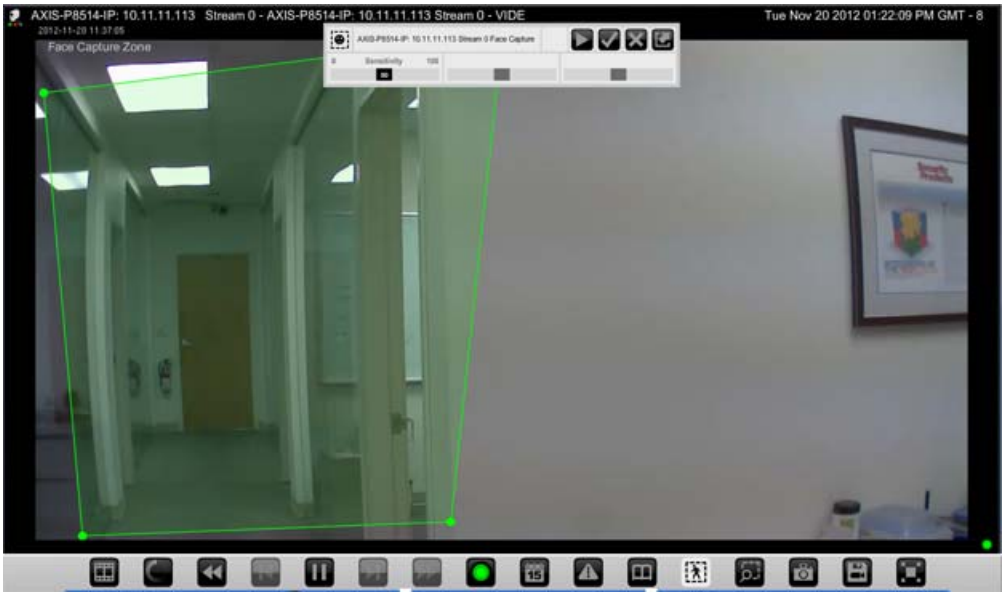
Face Capture is configured and run at the local Gateway level, on a per camera basis.

To get the best results, the proper settings are needed in configuring Face Capture. For details on optimizing face capture, see:

- **Face Capture and Recognition Guidelines** in **Chapter 22: Configuring and Using Face Recognition** for basic configuration notes.
- **Appendix A: Performance and Setup Guidelines: Video Analytics, Face Recognition, and License Plate Recognition** for more detailed guidelines.

© 2009-2014 Next Level Security Systems, Inc.

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. A higher sensitivity setting puts a lower threshold on the face capture. A higher sensitivity captures more face-like objects, but increases the false positive rate.
5. Click **Save** to keep the changes.
6. Click **Start** to activate this video analytic.
   A square, labeled *Minimum Face Size*, is displayed to indicate the minimum size that face must be on the screen to be recognized by the system. 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.

5.2.5 Face Recognition

Face Recognition is premium Video Analytic that can be added to the NLSS Unified Security Suite. When the Face Recognition Video Analytic is activated for a camera, it captures a face, then compares the image to uploaded images in a database. If a match is made, an event is generated. The capture and recognition features generate an event.

See **Chapter 22: Configuring and Using Face Recognition** for instructions on setting up and using the Face Recognition Analytic.

© 2009-2014 Next Level Security Systems, Inc.

5.2.6 License Plate Capture and License Plate Recognition

License Plate Recognition is a premium Video Analytics that can be added to the NLSS Unified Security Suite. When the License Plate Recognition Video Analytic is activated for a camera, it captures a license plate from video, reads it, and then compares the number to license plates in a database. The capture and recognition features generate an event.

See **Chapter 23: Configuring and Using License Plate Recognition** for instructions on setting up and using the Face Recognition Analytic.

5.2.7 Line Crossing

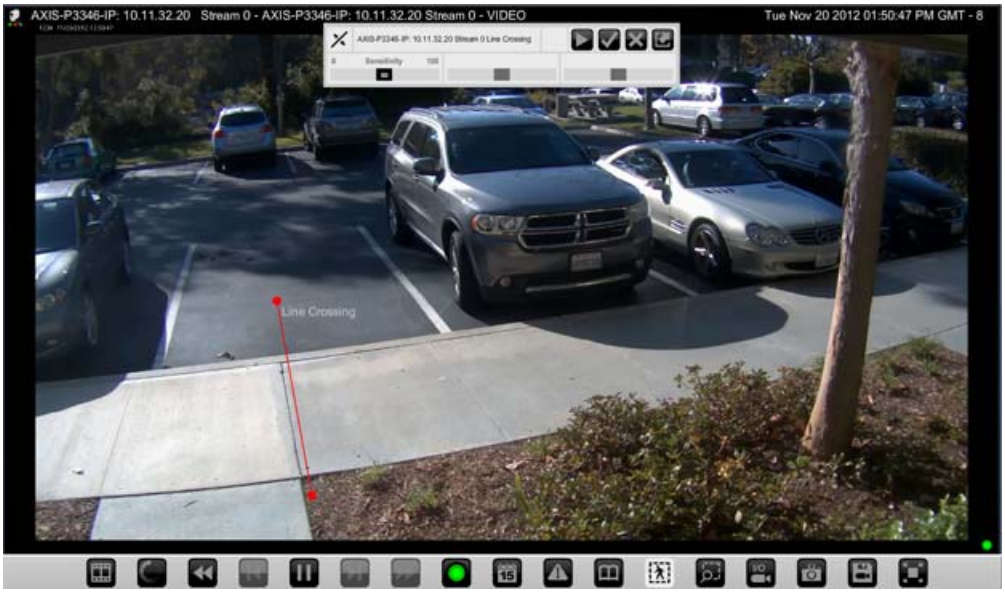
Line Crossing monitors movement that crosses a line drawn in the area being monitored.

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.



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.

© 2009-2014 Next Level Security Systems, Inc.

5.2.8 Object Moved

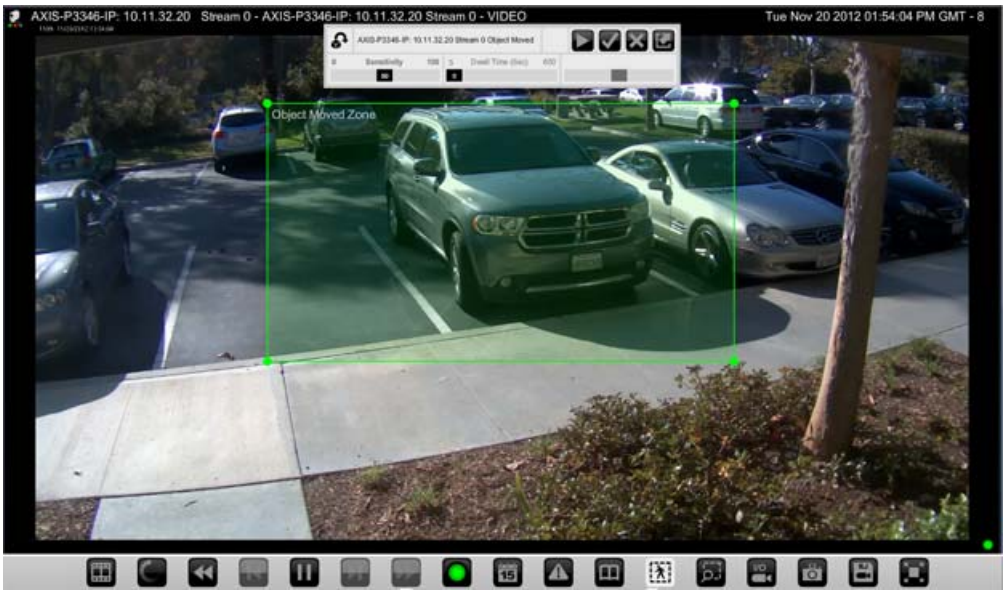
Object Taken monitors for objects that are placed in or removed from an area.

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.



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.

© 2009-2014 Next Level Security Systems, Inc.

5.2.9 Object Taken

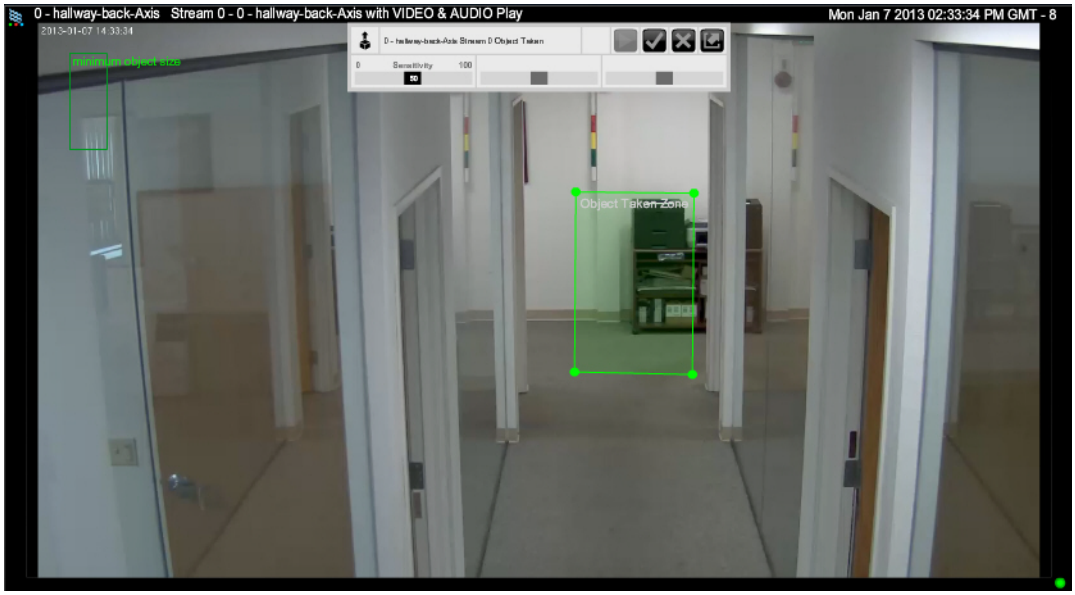
Object Taken monitors for objects removed from a selected area.

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

© 2009-2014 Next Level Security Systems, Inc.

5.2.10 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.

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.

© 2009-2014 Next Level Security Systems, Inc.

5.2.11 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.

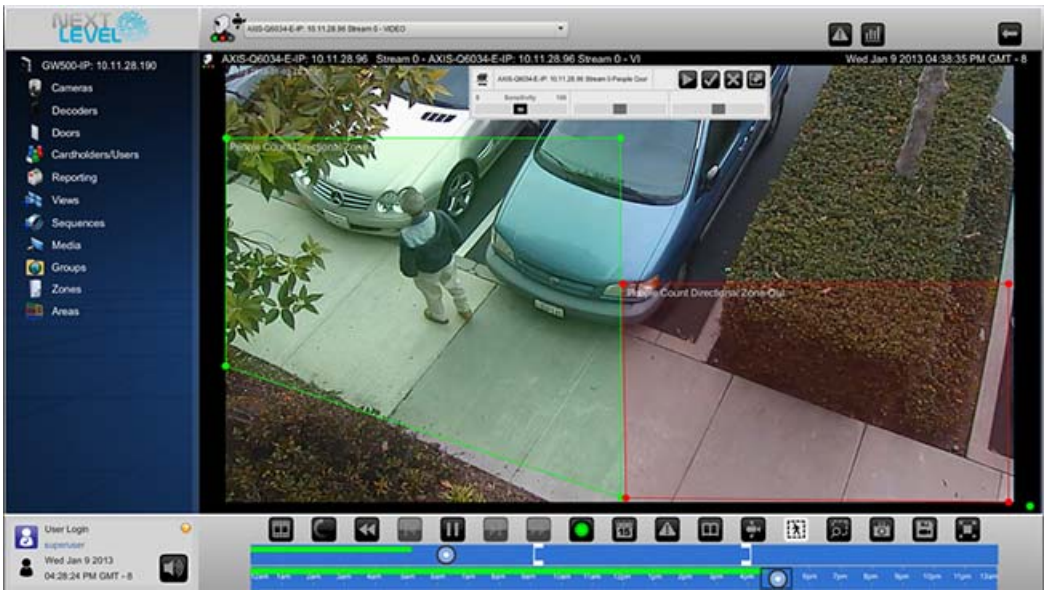
1. Click **Edit** for **People Count Directional** in the Video Analytics Configuration list.

   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.



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.

© 2009-2014 Next Level Security Systems, Inc.

5.2.12 Perimeter

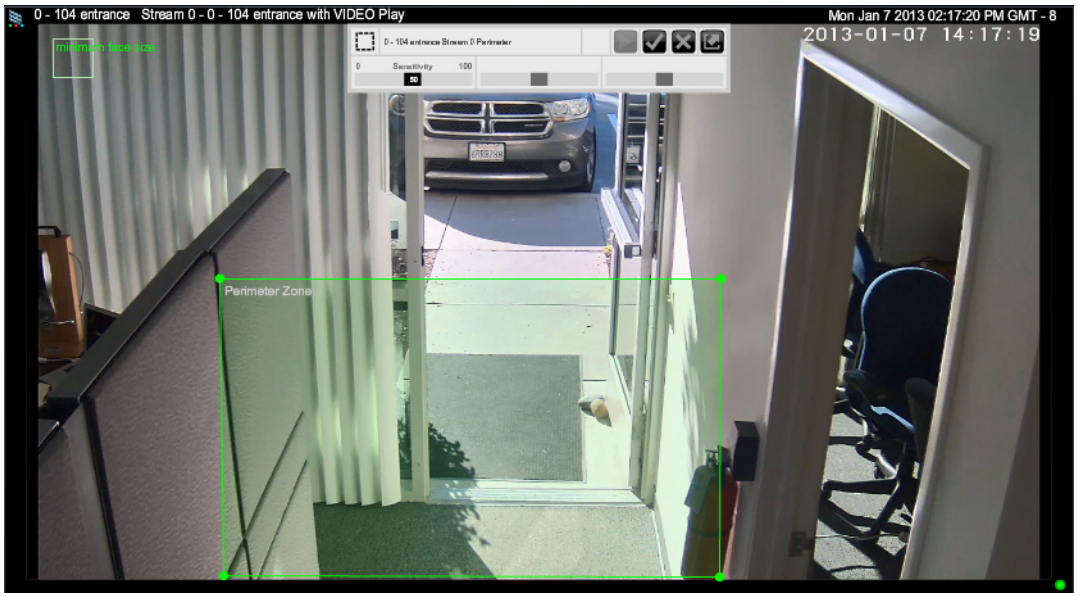
The Perimeter analytic functions similar to the Line Crossing analytic, but encompasses a four sides boundary. Any person or object that enters the Perimeter Zone from any direction is counted as an event.

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.



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.

5.2.13 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.

© 2009-2014 Next Level Security Systems, Inc.

- **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.

5.3 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** to remove the result from the queue.

Chapter 6: Operations with Doors

Configured doors are listed under the **Operations > Doors** menu. Four features are available with doors:

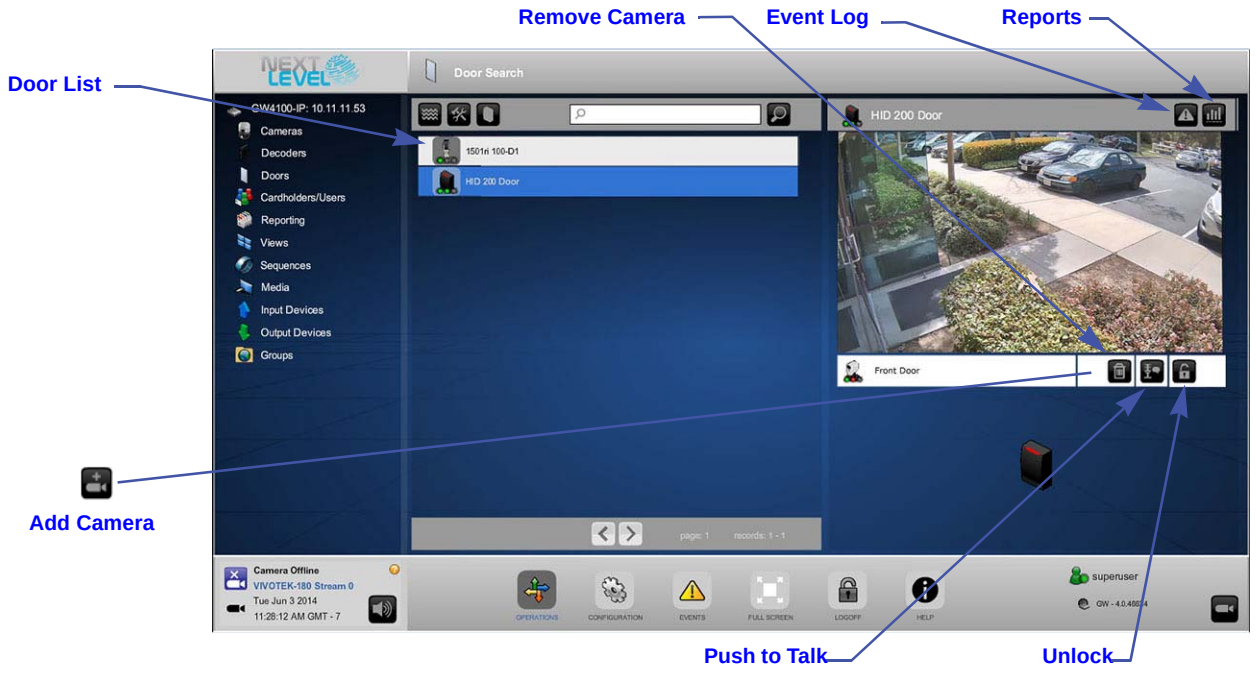
- **Unlock**
- **Add Camera**
- **Push to Talk**
- **Event Log**

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

Operations > Doors is not available if access control is not enabled for the Gateway.

6.1 DOORS WINDOW

Select **Operations > Doors** to display the *Doors* window. The left pane includes a list of doors discovered by the Gateway. The right pane provides the option to associate a camera or video stream with the selected door. If a camera and door are associated, a video stream is displayed with, talk back (if available), remove, and unlock buttons. A video player also can be launched from this pane.



6.2 DOOR LIST

The Door list contains the doors discovered by the NLSS Unified Security Suite and set up in Configuration > Access Control > Doors. See **Configure Doors** in **Chapter 19: Configure Access Control** for more information. The Doors list can be filtered and searched. See **Operations Windows** in **Chapter 3: Using the NLSS Web Interface** for more information on using a list and its functions.

See **Searching a List** in **Chapter 3: Using the NLSS Web Interface** for instructions on searching a list.

6.2.1 List Filters

The Door list can be filtered by:

Connection State **Admin State** **Controller Type**

These filters can be combined to narrow the results.

1. Click a filter button.
   The filter dialog box is opened.
2. Select or deselect the desired filter items.
   - *Connection State*: **Connected** or **Not Connected**.
   - *Admin State*: **In Service** or **Out of Service**.
   - *Controller Type*: lists the controller models supported by the Gateway.
3. Close the dialog.

The list displays the doors meeting the search criteria.

6.2.2 Door Icons

Each door icon includes three LEDs to indicate status.

Door Connection Status	Door Secured Status (Mercury only)	Strike Energized Status
• Green = InService/Online • Yellow = InService/Offline • Red = OutOfService/Offline • Gray = Preprovisioned	• Green = Secured • Gray = Unsecured (Off)	• Red = Strike energized • Gray = Strike is not energized (Off)

© 2009-2014 Next Level Security Systems, Inc.

6.3 UNLOCK

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* window is displayed.
3. Click **Open** to unlock the door for its configured *strike time*. See **General Tab** in **Chapter 19: Configure Access Control** 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.

6.4 ADD CAMERA

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

6.4.1 Adding 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 **Add Camera** to display the Camera list in the right pane. See **Selecting Cameras** in **Chapter 4: Controlling Cameras** for more information.
4. Select a camera or video stream.

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

6.4.2 Remove Camera

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

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

© 2009-2014 Next Level Security Systems, Inc.

6.5 PUSH TO TALK

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 **Push to Talk** to speak.
4. Click Talk again to cancel the microphone feed to the camera.

6.6 EVENT LOG

The Event Log for the selected door can be accessed from the Doors window.

1. Click **Operations >Doors**.
2. Select a door.
3. Click **Event Log** in the mini-pane.
   The Reports or Events pane for the door is displayed.
   See **Chapter 15: Monitoring and Handling Events** for instructions.
4. Click **Return** to go back to the Doors window.

6.7 REPORTS

Reports for the selected door can be accessed from the Doors window.

1. Click **Operations >Doors**.
2. Select a door.
3. Click **Reports** in the mini-pane.
   The Reports or Events pane for the door is displayed.
   See **Chapter 8: Operations with Reports** for instructions.
4. Click **Return** to go back to the Doors window.

© 2009-2014 Next Level Security Systems, Inc.

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 18: Configure Identity and Credentials** for instructions on configuring cards and adding cardholders. Cardholders work with the add-on Access Control module.

See **Chapter 21: Configuring Permissions** for instructions on configuring users.

7.1 CARDHOLDERS/USERS WINDOW

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

Cardholders are the people whose access to doors is controlled by the system. A cardholder's card can be *Activated* or *Deactivated* from the record pane.

Users are the people operating the system through the NLSS Web Interface. No actions can be taken on a user record from this window.

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 21: Configuring Permissions** for more information.

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 21: Configuring Permissions** for instructions on creating and configuring User Types.

7.2 CARDHOLDERS/USERS DETAILS

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

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

Note: *Five* access cards can be active per cardholder.

7.2.1 Cardholder Information

These fields are populated in the Configuration > Identity > Cardholders window. See **Cardholders Tabs** in **Chapter 18: 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 window. See **Users** in **Chapter 21: 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, the photo is displayed in the Configuration pane. See **Cards Tab** in **Chapter 18: Configure Identity and Credentials** for instructions on uploading a photo.

© 2009-2014 Next Level Security Systems, Inc.

7.2.4 Activate / Deactivate Cardholders

Cardholder access can be activated or deactivated from the Configuration pane.

1. Click **Cardholder Status** in the Configuration pane.
   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 Configuration pane.

   Reports

   Events

   The Reports or Events page for the cardholder or user is displayed.

   See **Chapter 8: Operations with Reports** and **Chapter 15: Monitoring and Handling Events** for more instructions.
4. Click **Back** to go back to the Cardholders/Users window.

© 2009-2014 Next Level Security Systems, Inc.

Chapter 8: 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. Reports are displayed as graphs in the NLSS Web Interface. Reports also can be displayed in a table format using **Canned Reports**.

8.1 GENERATING REPORTS

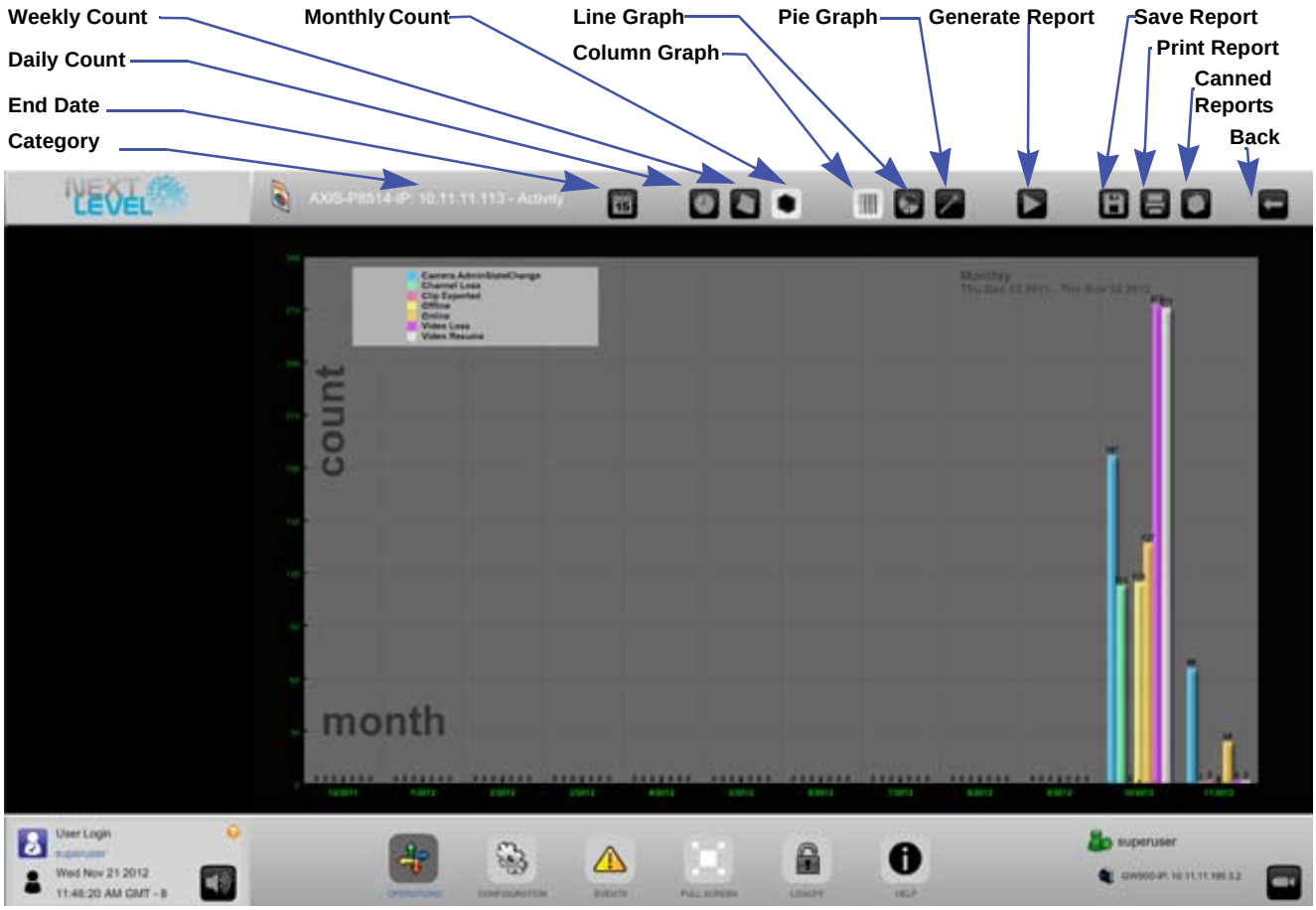
Two types of reports are available.

- **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 video player or the Preview/Details panes for Cameras, Doors, or Cardholders & Users.

© 2009-2014 Next Level Security Systems, Inc.

8.1.1 Reports Window

Most features are the same for all types of reports on the Reports window.



8.1.2 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.

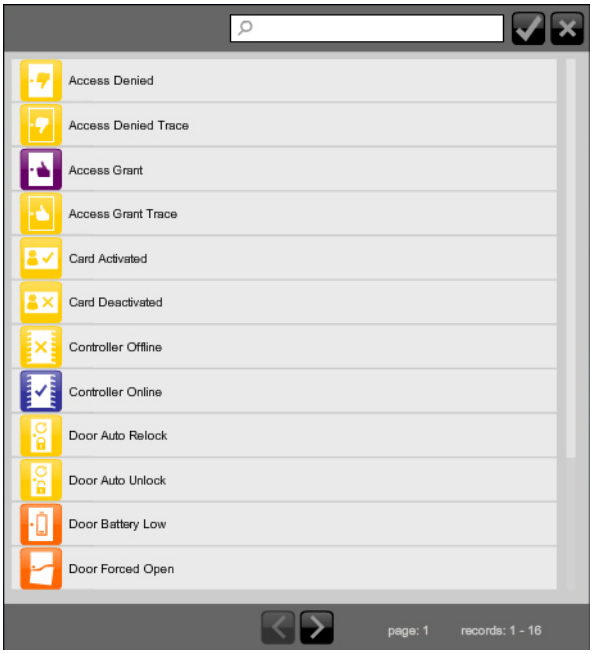
1. Select **Operations > Reporting** from the Main Menu.

   The Reports window is displayed.

The Reports window is opened with a report category list.

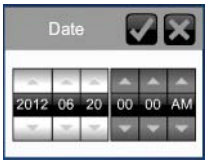
2. Select a category (Event Filter).

   The *Event Type* list is displayed for the category.



3. Select an Event Type from the list.
   – Click **Event Filters** to return to Category list.

4. Click **Date/Time**. 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.

Hourly: 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**, **Pie Chart**, or **Line Graph**.

8. Click **Run Report** to create the report.
   – Click **Print Report** to print the report.
   – Click **Save .csv file** to keep a .csv spreadsheet of the report.

   If a message is displayed stating: *No records to display*, widen the search time using the Date and Time dialog and run the report again.

Any of the report settings be clicked at any time to run a different report. A new report must be run after any change to update the data.

8.1.3 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**.
4. Click **End Date**. The Date dialog box is displayed.

© 2009-2014 Next Level Security Systems, Inc.

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. The start time and date are dependent on the time period selected for the report

– Click **Save** to set the date and time.

5. 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.
6. Select a graph type for the report: **Column**, **Line**, or **Pie**.
7. Click **Generate Report** to create the report.
   – Click **Print** to print the report.
   – Click **Save** to keep a .csv version of the report.

The report settings be clicked at any time to run a different report for the selected device. A new report must be run after any change to update the data.

8.2 CATEGORIES OF EVENT-SPECIFIC REPORTS

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

- **Access Control Reports**: Access Control reports provide the status of key access control hardware in your system.
- **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.
- **Decoder Reports**: Decoder reports provide off-line and on-line reports for NLSS decoders discovered by the Gateway.
- **System Reports**: Reports on external storage and recording events.
- **User Reports**: User reports lists when specific users have logged in or out of the system.
- **Video Analytics Reports**: Video Analytics reports list how many times the cameras in the system have detected a video analytic event.

© 2009-2014 Next Level Security Systems, Inc.

8.3 CANNED REPORTS

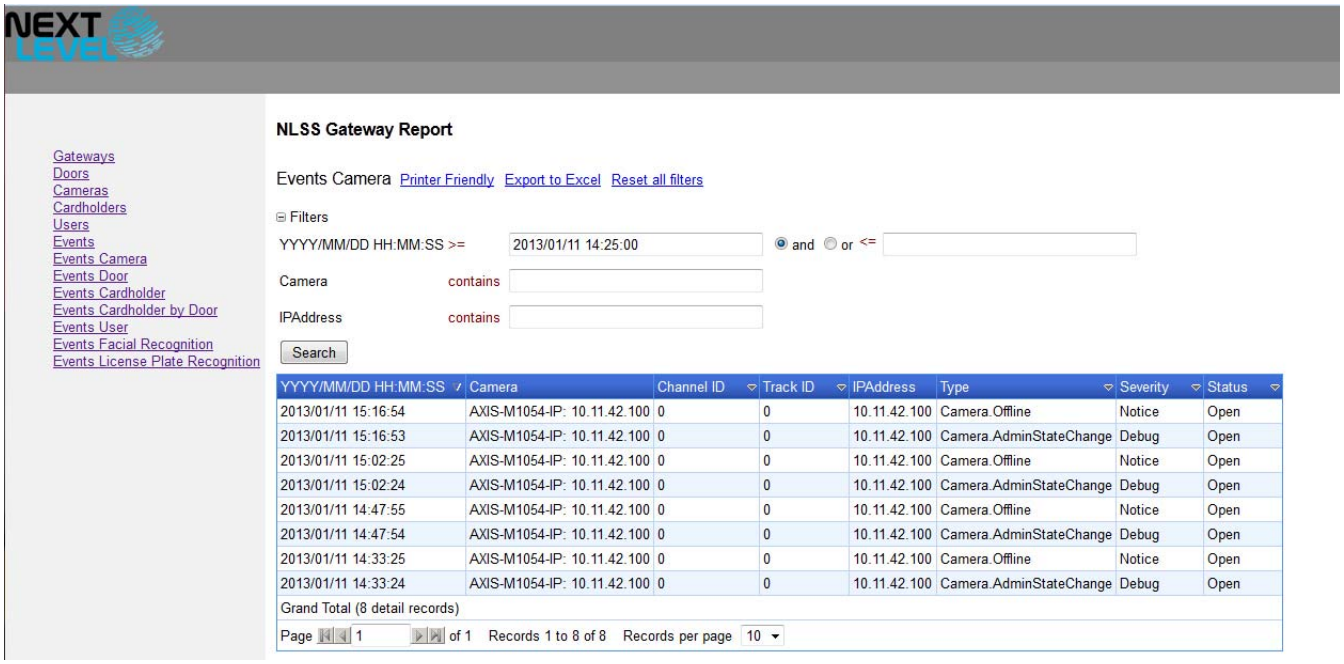
Besides graphs, reports can be displayed in tables that can be filtered and sorted. These tables also can be printed and exported to a formatted spreadsheet in .xls format.

8.3.1 Using the Table

Tables can be sorted and filtered.

1. Click **Canned Reports** in the Reports window to display report tables.

   The tables are displayed in a separate window or tab than the NLSS Web Interface.



2. Select a report from the left column.
   - **Doors**: provides a summary of configuration information set in *Configuration* > *Access Control* > *Doors*, plus **Strike** and **Opened** counts.

     See **Door Details** in **Chapter 19: Configure Access Control** for field definitions.
   - **Cameras**: provides a summary of configuration information set in *Configuration* > *Video*> *Cameras*, plus video parameters set directly on the camera.

     See **Configure Cameras and Streams** in **Chapter 20: Configure Video, & Storage, & Decoders** for field definitions.
   - **Cardholders**: provides a summary of cardholder information, as set in Con*figure* > *Identity* > *Cardholders* and plus the Facility Code set in *Card Profiles*.

     See **Configure Cardholders** and **Configure Cardholder Types** in **Chapter 18: Configure Identity and Credentials** for field definitions.
   - **Users**: lists the users' first and last names, User ID, Type and Group, as set in Configuration > Permissions > Users.

     See **User Details** in **Chapter 21: Configuring Permissions** for field definitions.

© 2009-2014 Next Level Security Systems, Inc.

– **Events**: provides a summary of events recorded by the Gateway. This summary contains all event types.

  The reports are available for the following Event Categories

  » Camera
  » Cardholder
  » User
  » License Plate Recognition
  » Door
  » Cardholder by Door
  » Facial Recognition

  Each event table lists the time of the event, plus identifies the item (door, camera, etc.) that triggered the event. The Event Type, Severity, and Status are also listed.

  See **Chapter 15: Monitoring and Handling Events** for more information on events.

– The Event reports can be filtered by specific category details, such as a name, or IP address, or by time and date.

  The time and date filter is set in the YYYY/MM/DD HH:MM:SS format.

  » To search after a date and time, enter the starting point in the *greater than or equal to* field (**>=**).
  » To narrow the search, enter an end point date and time in the less than or equal to field (**<=**).
  » Select **and** or **or** to define the end point.

3. Click on a column header to sort a table.
4. Use the page navigation at the bottom of the table to:
   – Go the previous or next page.
   – Go to the first or last page.
   – Select the number of records to be displayed on a page.

   The total number of records in the report also is displayed below the table.
5. From the drop-down list, select the number of items (*Groups*) to display per page.
6. Click **Printer Friendly** to open a page formatted for printing.
   – Use the browser's print options to print the page.
   – Use the browser's **Back** button to return to the full Canned Reports page.
7. Click **Export to Excel** to generate an .xls file.
   – Follow the prompts to save and open the file.

© 2009-2014 Next Level Security Systems, Inc.

8.3.2 Report Table Filters

Report tables can be filtered using the search feature, or directly from the column header.

8.3.2.1 Search Filter

1. Select a report type.
2. Click the plus (**+**) to display the **Filters** fields, if they are not displayed.
   - The fields vary, depending on the selected report type.
   - Each filter provides a field to search on the item name and ID.
   - Cameras and doors can be searched by IP address.
   - Events can be searched by greater than, or equal to (**>=**) a time stamp (*hh:mm:ss*) and date (*yyyy/mm/dd*), with an **and/or** option.

Note: If a search by time is configured, a date must be included.

3. Click **Search** to display the items matching the search criteria.
4. Click **Reset** and click **Search** again to restore all records.

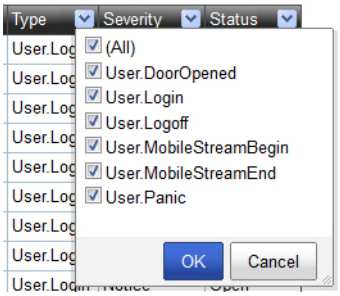
8.3.2.2 Column Filters

Tables also can be filtered by columns.

1. Select a report type.
2. Click **Column Filter**.

   A drop-down dialog is displayed with the current entries contained in that column.

   For example, this graphic shows the filter dialog for the event type in a Events User report. Only event types in the report are listed. If an event is triggered with a different type, it is added to subsequent reports, but not to this report.



3. Check the items on which to filter the table.
4. Click **OK**.
5. To remove the filter, open the drop-down and check **All**.

Chapter 9: Displaying Video

In the NLSS Web Interface, video streams from IP cameras, and RTSP, HTTP, and encoder 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 Media Clips, 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 Decoders* to the system. The NLSS Web Interface can **Push Media Clips, 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.

9.1 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.

© 2009-2014 Next Level Security Systems, Inc.

9.1.1 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.

9.1.1.1 Menu Options

Use the menu options to configure the View.

- **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.
- **View Layout**: displays the selected cameras and streams, depending on the layout selected. Cameras and video streams are assigned from the pane.
- **Selected Monitor**: a light, gray frame highlights the selected pane.
- **Transport Control**: provides control of synchronized playback of video in each monitor pane in the view. See **Transport Control** for instructions.

© 2009-2014 Next Level Security Systems, Inc.

9.1.2 Create Views

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

1. Select **Operations > Views** from the Main Menu.
2. Click **Add** to display a *New View* window.
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 **Close** 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.

9.1.3 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.

9.1.4 Filter Views List

The Views list can be filtered by view types, such as 1x1, 2x4, etc.

1. Click **View Type**.
2. Select the desired formats to display in the list.

See**Filtering Operations Lists** in **Chapter 3: Using the NLSS Web Interface** for more information on filtering lists.

© 2009-2014 Next Level Security Systems, Inc.

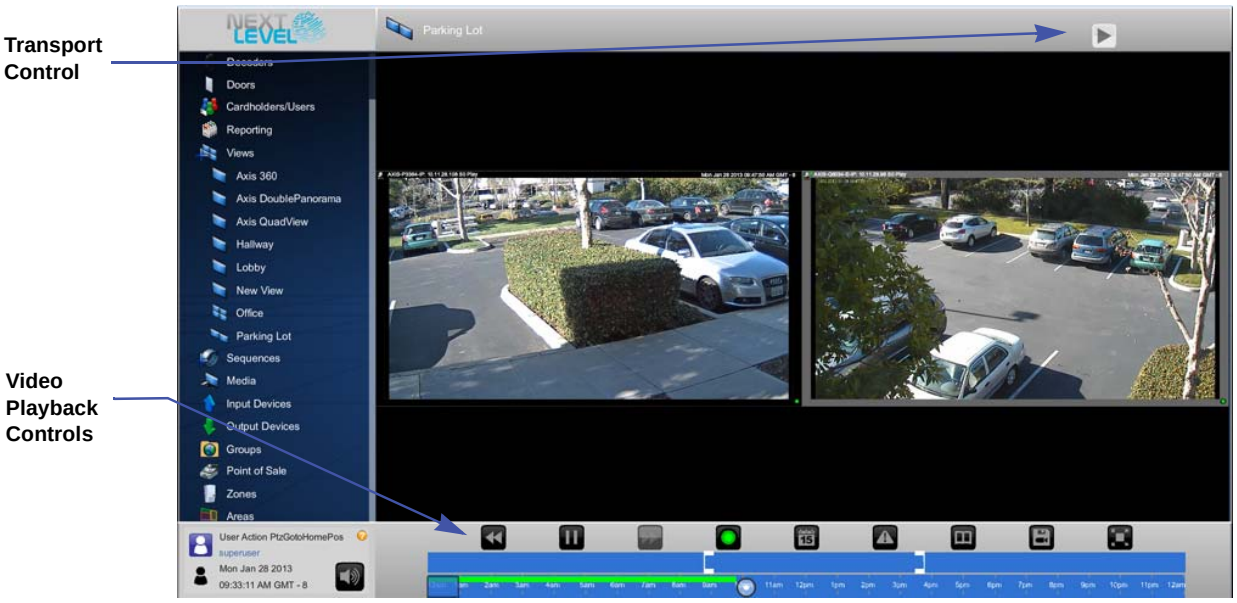
9.1.5 Transport Control

Besides displaying live video from multiple cameras, synchronized recorded video can be played back from each camera in the View. If recorded video of an event is displayed for a selected camera, Transport Control can be used to synchronize the other playback of the other cameras in the view to the same time.

The Transport Control feature displays video player controls in the Views window.

1. Click **Transport Control** in the top of the Views page.

   Video player controls are displayed, and the view edit buttons are hidden.



Note: If a video stream is not configured for recording, the current video continues to display while other monitors show recorded video.

The selected monitor must be configured for recording to access recorded video from other monitors.

2. Use the video player controls to control playback for all monitors.
   - These controls are applied the selected monitor, and then simultaneously applied to video streams in the other monitors.
   - Complete camera controls are only available if the camera is accessed through Operations > Cameras.

   See **Using the Camera Toolbar** in **Chapter 4: Controlling Cameras** for more information on the video player controls.

3. Select the time period for playback:
   - Click **Date & Time**.

     - or -
   - Drag the **play head** in the timeline the desired time.

   The Live/Archive toggle turns red when playing a recorded stream.

4. Click **Play/Pause** to start or pause the playback.

5. Use the **Rewind** and **Fast Forward** buttons to move through the video.

Note: Click the **Rewind** and **Fast Forward** buttons repeatedly to cycle between 0.5x, 2x, 5x, 10x, and 50x speed. The amount of video that the play head moves depends on the frame rate at which the video was recorded.

6. Click the **Camera Events Toggle** to display or hide events markers.
7. Click **Bookmark** to manually add an event to the timeline. A marker is added in the timelines for each camera in the view.
8. Click **Export Video** to save synchronized video clips from all monitors.
   Video clips from the same time period are exported to the Media Library.
9. Click **Full Screen** to hide the Operations menu options, and expand the view to full screen.
10. Click **Play/Pause** at any time to start and pause playback.
11. Click the **Live/Archive** toggle to return to live video.
    The toggle button turns green when the displayed video is live.
12. Click **Transport Control** again to return to the Views edit mode.

Note: If the Transport Control is closed while recorded video is playing, the recorded video continues to play.

9.1.6 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.

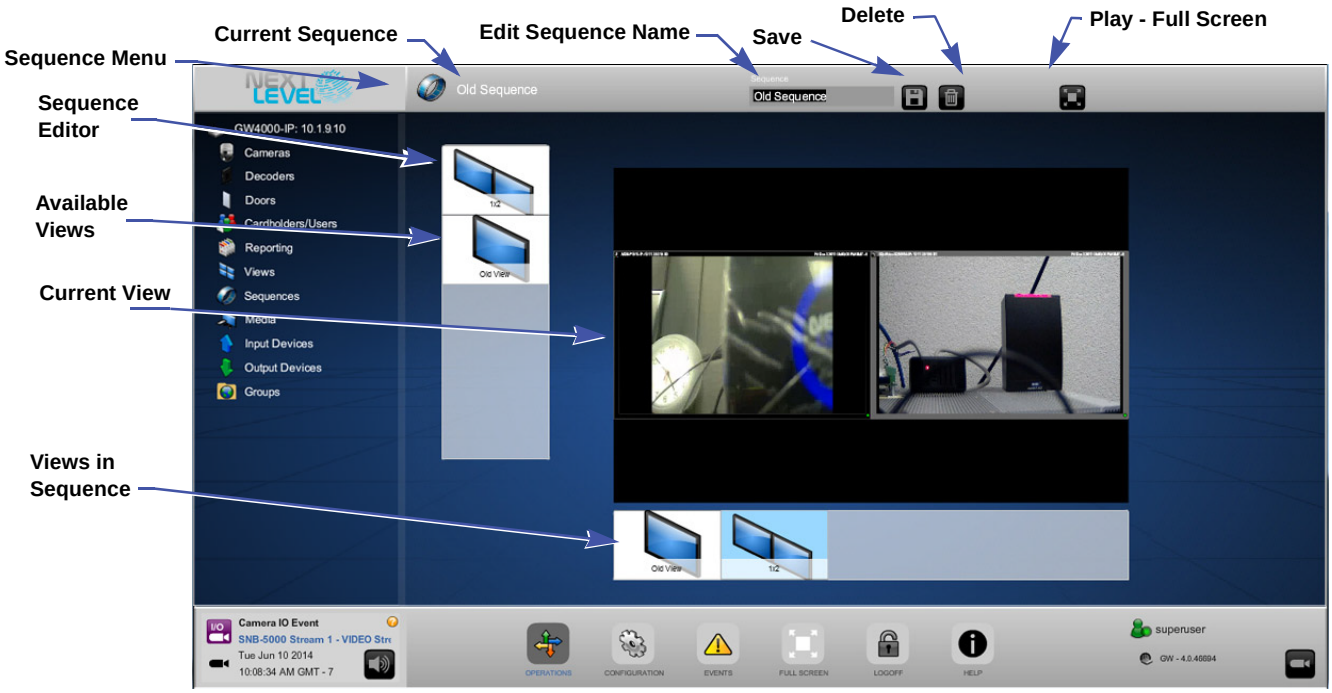
1. Select **Operations > Views** from the Main Menu.
2. Select a View.
3. Click **Delete** in the Views menu.

© 2009-2014 Next Level Security Systems, Inc.

9.2 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.

9.2.1 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 **9.1 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.

9.2.2 Create New Sequences

1. Select **Operations > Sequence**.
2. Click **Add**. 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.

9.2.2.1 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.

© 2009-2014 Next Level Security Systems, Inc.

9.2.2.2 DELETE SEQUENCES

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

9.2.2.3 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 window.

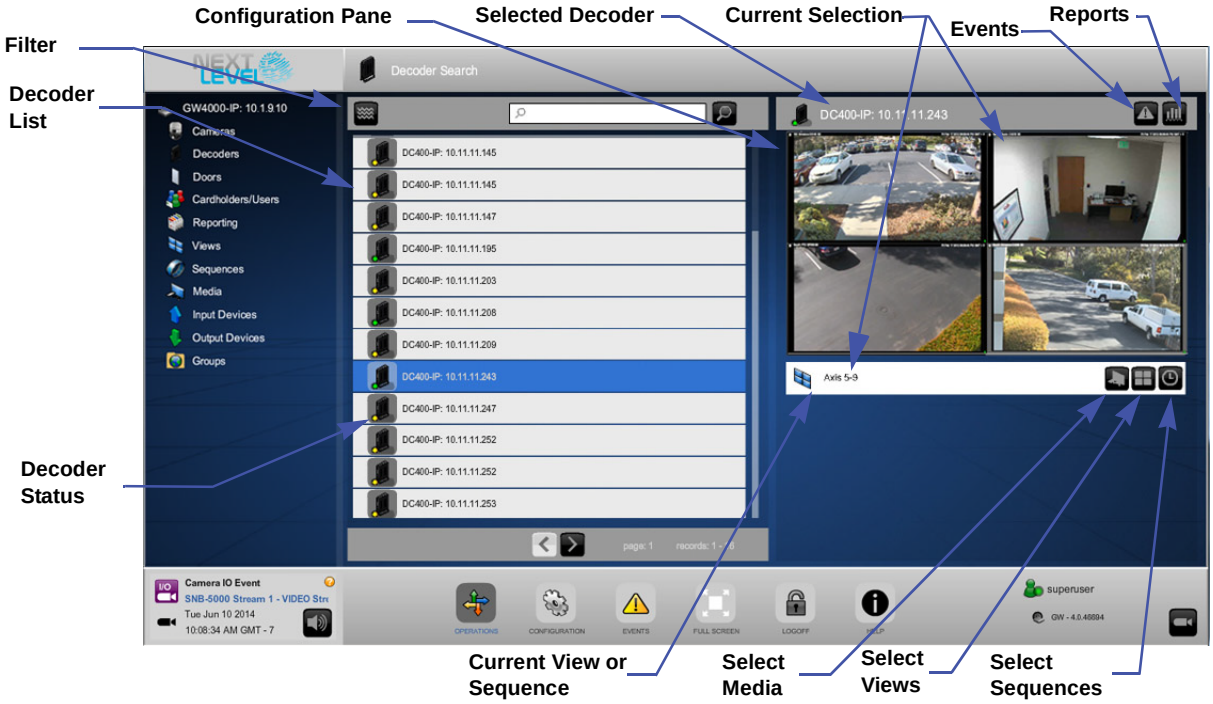
9.3 PUSH MEDIA CLIPS, VIEWS AND SEQUENCES TO DECODERS

A selected Media clip, View, or Sequences can be pushed from the Gateway to NLSS HD Decoders for display. The selected View and Sequence, or Media clip is pushed to a decoder as a stream from this page. See the *NLSS HD Decoder User Manual* for more information on configuring that device.

© 2009-2014 Next Level Security Systems, Inc.

9.3.1 Decoder Window

Select **Operations > Decoders** to display the *Decoder* window.



The left pane lists all decoders discovered by the Gateway.

A right pane contains configuration options to push a Media clip, View or Sequence from the Gateway to the decoder. The video for the selection is also displayed.

- **Decoder List**:
  - **Decoder Name**: the name assigned under Configuration > Video > Decoders in this interface. The selected Decoder Name is displayed above the configuration pane.
  - **Device Status**: colored LED under the Decoder icon that indicates if the decoder is on line. Green indicates the decoder is *connected*; yellow indicates that the decoder is *not connected*.
  - **Filter**: the list can be filtered on *Connection State*: **Connected** or **Not Connected**.
  - **Search**: locate a decoder in the list.

- **Configuration Pane**: displays the Media clip, 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 Selection**: the Media clip, View or Sequence being pushed to the decoder. The video is displayed in the player and the name is listed below the media player.
  - **Events**: opens the Events Log to list the events associated with the selected decoder. See **Event Log** in **Chapter 15: Monitoring and Handling Events** for more information.

- **Reports**: opens the Reports window to create reports for the selected decoder. See **Generating Reports** in **Chapter 8: Operations with Reports** for more information.
- **Media**: opens the Media Library list containing clips that can be pushed to the decoder from the Gateway. See **Media Library** in **Chapter 10: Media Operations** for more information.
- **Views**: accesses a list of Views on this Gateway.

  When a view is *pushed* from the Gateway to a Decoder, each pane of video in the decoder display counts as a stream. For example, if a 2x2 view is sent from the Gateway to a Decoder, it counts as four (4) streams.

  The decoder cannot display 3x3 views in sequences created on the decoder.
- **Sequences**: accesses a list of Sequences on this Gateway.

Access to Operations > Decoders is controlled by permissions. Access to specific decoders can be controlled by groups. See **Chapter 21: Configuring Permissions** for more information.

9.3.2 Pushing a Media Clip

1. Click **Operations > Decoders** from the Main Menu.
2. Select a decoder.
3. Click **Media**. A list of saved video files is displayed.

Note: This list does not contain the sound effects files shipped with the Media Library.

- Use the Search feature, if necessary, to locate the desired decoder.
- The Views list can be filtered by layout type, such as 1x1, 2x2, etc.

4. Select a View or Sequence.

   See **Create, Edit, and Display Views** and **Create, Edit, and Display Sequences** for more information on Views and Sequences.

Note: A sequence containing a 3x3 view should not be pushed to a decoder.

5. Close the list.

   The selected clip is displayed in the Current View pane, and is now available to the decoder. The pane contains a media player with play/pause, stop and volume controls, same as in the Operations > Media window.

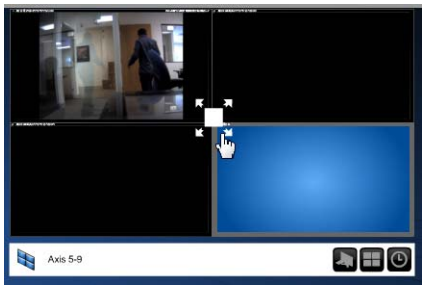
© 2009-2014 Next Level Security Systems, Inc.

9.3.3 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.

   See **Create, Edit, and Display Views** and **Create, Edit, and Display Sequences** for more information on Views and Sequences.
5. Close the list.

   The selected View or Sequence is displayed in the Current View. This View or Sequence is now available to the decoder.
6. Mouse-over the pane and click the **Full Screen** button to fill the window with the View or Sequence.



   – Click **Back** to return to the default display.

Chapter 10: Media Operations

The NLSS Web Interface contains a Media Library to store audio and video files. *Operations* > *Media* includes a searchable library of sound effects that are included with the Gateway. The library also holds the video exported from a camera.

Note: The sound effects files included with the system cannot be deleted or unlocked. However, the files can be replaced with an imported audio file. See **Replacing a Default Audio File**.

Use the NLSS Web Interface to play selected audio through a speaker attached to camera. The audio can either be triggered automatically by an event, or manually from the NLSS Web Interface video player. See **Using the Camera Toolbar** in **Chapter 4: Controlling Cameras** for more information.

The audio is associated to a camera as an *Action*. An event is associated with the action through *Event Linkages*. When the event occurs, the Action triggers the audio to play. See **Configure Actions** and **Configure Event Linkages** in **Chapter 17: Global Configurations** for instructions.

Video clips up to four hours long can be stored in the Media Library. See **Export Video** in **Chapter 4: Controlling Cameras** for instructions. The video is deleted (groomed) from the library after a set period if the file is not locked. See **Configure Groomer Settings** in **Global Configurations** for more information.

© 2009-2014 Next Level Security Systems, Inc.

10.1 MEDIA LIBRARY

From the Media Library, files can be sorted, searched, sampled, and downloaded.

1. Select **Operations > Media**.

   The Media Library opens with a list of files in the left pane. These files can be filtered and searched in this pane, as described later in this chapter.

2. Select a media file.

   These files can be previewed, downloaded, locked and deleted in using the tools in the right pane.

3. The player function in the Preview pane on the right depends on the file type.
   – *Audio*: click the **Speaker** to open the slider to adjust the playback volume.

   – *Video*: use the player to view the video. The player contains the standard play, pause, stop, volume, and mute controls.

See **Operations Windows** in **Chapter 3: Using the NLSS Web Interface** for instructions on other window features.

10.1.1 Filter the Library

The Media Library can be filtered by three types:

Video Audio Lock

1. Select a filter type.

   A dialog is displayed with three choices. The choices vary between filter types.

   – **all**: shows all files.
   – **no audio**: do not display audio files.
   – **with audio**: only display audio files.
   – **no video**: do not display video files.
   – **with video**: only display video files.
   – **unlocked**: only display unlocked files.
   – **locked**: only display locked files.

   The Lock filters can be combined with the audio or video filters to further refine the list.

2. Click **Close** (**X**) to exit the dialog and display the filtered list.
3. To remove the filter, reopen the dialogs and select **all**.

10.1.2 Searching the Media Library

Use the Search tool in the left pane to locate a specific file or group of files. See **Searching a List** in **Chapter 3: Using the NLSS Web Interface** for instructions on searching.

10.1.3 Download a Video Clip

A clip exported from a camera can be downloaded to the local computer.

See **Export Video** in **Chapter 4: Controlling Cameras** for instructions on exporting a video clip form a camera.

1. Select a video clip in the Media Library.
2. In the right pane, click **Download File**.
3. Follow the prompts in the dialog box to save the file in a new location.

Note: If the Gateway is subscribed to RMS, the clips in the Gateway's Media Library must be transferred to RMS for export. The Download File option is replaced by Transfer to RMS.

1. Select the clip.
2. Click **Transfer to RMS**.

The clip can then be exported from the RMS Media Library.

© 2009-2014 Next Level Security Systems, Inc.

10.1.4 Stop a Camera Export

If a large file is being exported to the Media Library from a camera, the process can be stopped if desired. This action may be needed if multiple large files are simultaneously exported, and slowing down the system.

Note: The **Stop** button is only displayed if the selected media file is being downloaded.

1. Select a file in the library.
2. Click **Stop**.

10.1.5 Lock a Media File

A video file can be locked to prevent it from being accidentally deleted. The lock on a video file exported from a camera also prevents the file from being groomed.

Note that the default audio files cannot be unlocked.

1. Select a file in the library.
2. In the right pane, click **Lock**.

   The Lock button changes to **Unlock**.

   – Click the **Unlock** to unlock the file.

10.1.6 Delete a Media File

Unlocked media files can be deleted from the library.

Note that the default audio files cannot be deleted, but can be replaced. See **Replacing a Default Audio File**.

1. Select a file in the library.
2. In the right pane, click **Delete**.

Important: No warning or confirmation is displayed before a file is deleted.

10.1.7 Replacing a Default Audio File

The default audio files installed on the NLSS Gateway cannot be deleted, but can be replaced.

1. Select an audio file.

Note: The file does not need to be unlocked to be replaced.

2. Click **Upload**.
3. Click **Browse** to locate a new file in the *File Uploader* dialog box.
4. Follow the prompts to select and upload the file.

Note: If the audio file is linked to an action, the Gateway plays the new audio when the action is triggered. No reconfiguration of the action is required.

© 2009-2014 Next Level Security Systems, Inc.

Chapter 11: Operations with Input Devices

Input devices connected the NLSS Unified Security Suite are listed under **Operations > Input Devices**. Devices such as motion detectors, power or battery failure detectors, electronic switches, etc., can be connected to reader interfaces and I/O interfaces.

These devices are added to the Unified Security Suite under Configuration > Access Control. See **Configure Reader Interfaces** and **Configure I/O Interfaces** in **Chapter 19: Configure Access Control** for configuration instructions.

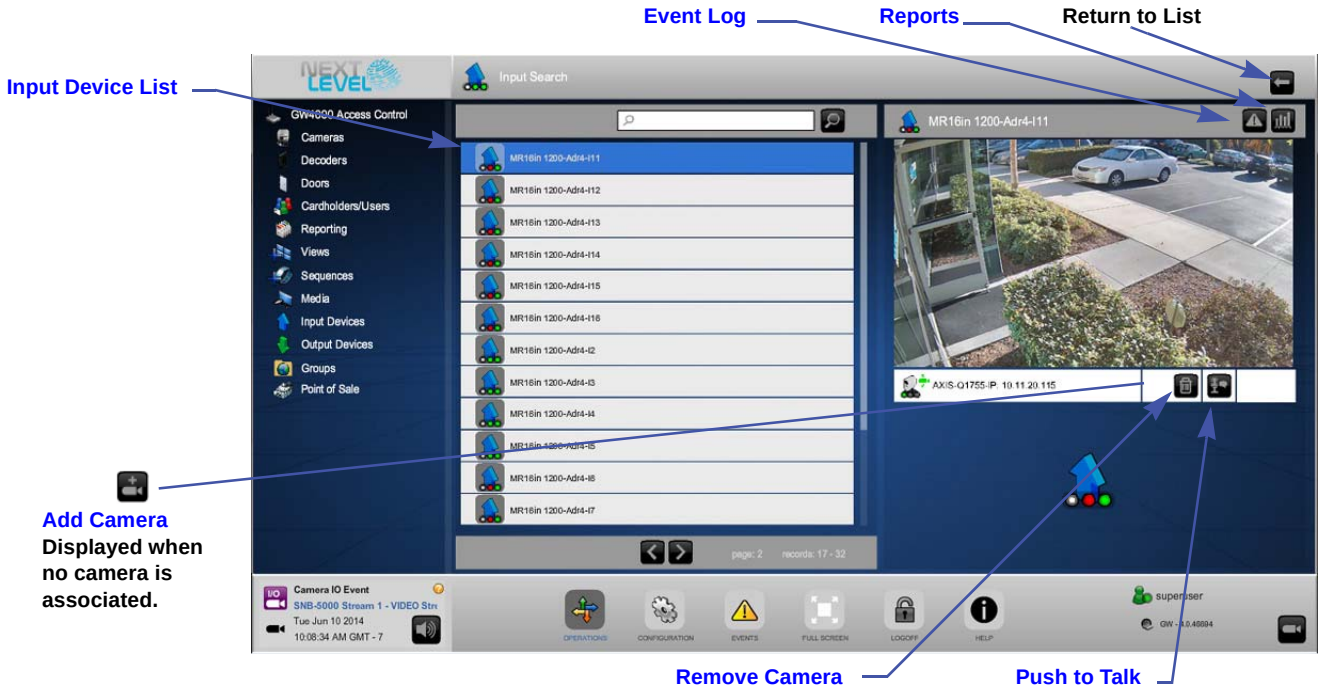
Access to input device operations and configurations is controlled by permissions.

11.1 INPUT DEVICES WINDOW

- Select **Operations > Input Devices** to display the *Input Devices* window.

The left pane includes a list of input devices added through Configuration > Access Control > Reader Interfaces or I/O Interfaces.

The right pane provides the option to associate a camera or video stream with the selected device. If a camera and device are associated, the video stream is displayed with Remove Camera and Talk Back (if available) buttons. The video player also can be launched by clicking on the video in this pane.



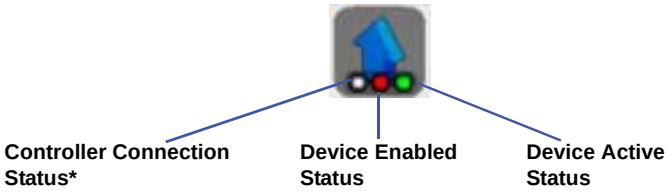
11.2 INPUT DEVICE LIST

The Input Device list contains the devices added under the Configuration > Access Control > Reader Interfaces and I/O Interfaces options. See **Configure Reader Interfaces** and **Configure I/O Interfaces** in **Chapter 19: Configure Access Control** for configuration instructions.

The Input Devices list can be filtered and searched. See **Operations Windows** in **Chapter 3: Using the NLSS Web Interface** for more information on using a list and its functions. See **Searching a List** in **Chapter 3: Using the NLSS Web Interface** for instructions on searching a list.

11.2.1 Input Device Icons

Each input device icon includes three LEDs to indicate status.



Controller Connection Status*	Device Enabled Status	Device Active Status
• Green = In Service/Online • Yellow = Not in Service/ Online • Red = Offline • Gray = Preprovisioned	• Green = Enabled • Red = Disabled	• Red = Active (signal sent) • Green = Not active

* *Controller Connection Status*: status of the controller to which the input device is connected.

11.3 ADD CAMERA

A camera can be associated with an input device. The camera's stream can be viewed directly from the right pane in the Input Devices window.

11.3.1 Adding and Viewing Cameras with Input Devices

By default, input devices do not have cameras associated with them.

1. Click **Operations > Input Devices**.
2. Select an input device from the list.
3. Click **Associate Camera** to display the Camera list in the right pane. See **Selecting Cameras** in **Chapter 4: Controlling Cameras** for more information.
4. Select a camera or video stream.

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

© 2009-2014 Next Level Security Systems, Inc.

11.3.2 Remove Camera

The association between a camera and an input device can be removed.

1. Click **Operations > Input Devices**.
2. Select an input device from the list.
3. Click **Remove Camera** to remove the link between the camera and the input device.

Note: This removal only impacts this connection, and does not effect camera or video streams connection to other devices, or availability in the camera list.

11.4 PUSH TO TALK

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 > Input Devices**.
2. Select an input device.
3. Click **Push to Talk** to speak.
4. Click **Push to Talk** again to cancel the microphone feed to the camera.

11.5 EVENT LOG

The Event Log for the selected input device can be accessed from the Input Devices window.

1. Click **Operations >Input**.
2. Select an input device.
3. Click **Event Log** in the mini-pane.
   The Reports or Events pane for the input device is displayed.
   See **Chapter 15: Monitoring and Handling Events** for instructions.
4. Click **Back** to go back to the Input Devices window.

© 2009-2014 Next Level Security Systems, Inc.

11.6 REPORTS

Reports for the selected input device can be accessed from the Input Devices window.

1. Click **Operations >Input Devices**.
2. Select an input device.
3. Click **Reports** in the mini-pane.
   The Reports or Events pane for the input device is displayed.
   See **Chapter 8: Operations with Reports** for instructions.
4. Click **Back** to go back to the Input Devices window.

© 2009-2014 Next Level Security Systems, Inc.

Chapter 12: Operations with Output Devices

Output devices connected the NLSS Unified Security Suite are listed under **Operations > Output Devices**. Devices such as alarms, warning lights, door unlock or lock electronic switches, etc., can be connected to relays on reader interface and I/O interface boards.

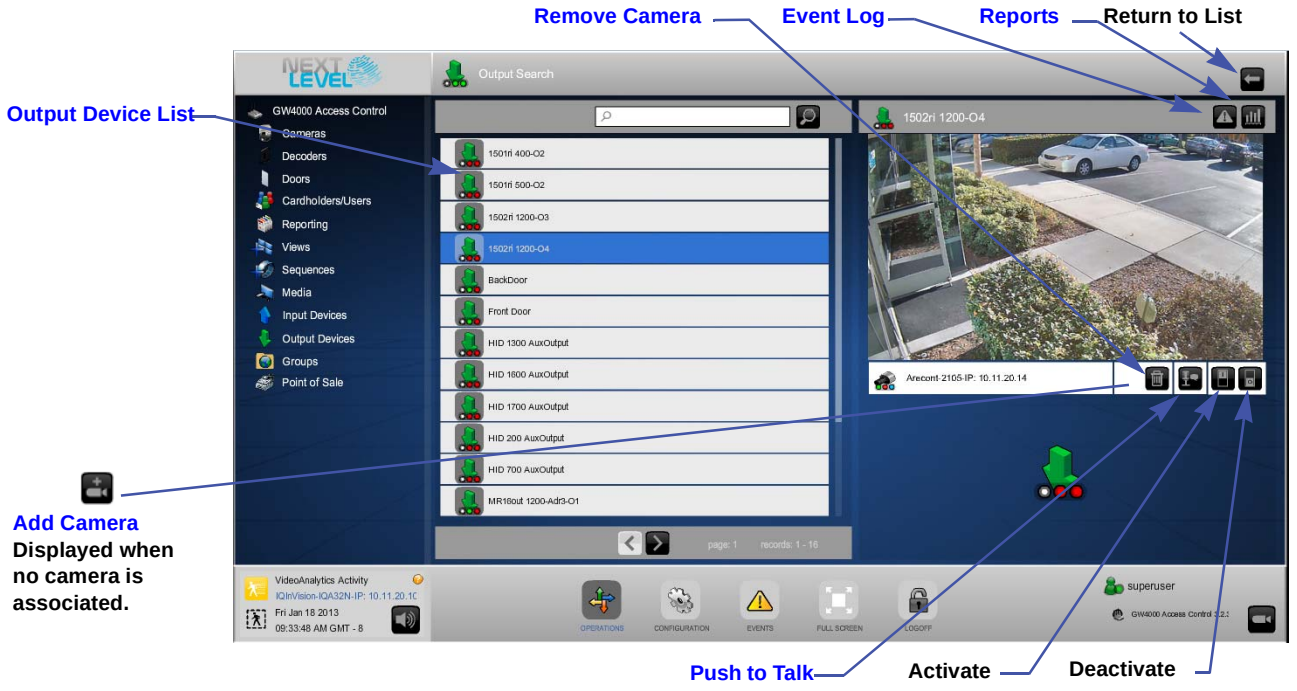
These devices are added to the Unified Security Suite under Configuration > Access Control. See **Configure Reader Interfaces** and **Configure I/O Interfaces** in **Chapter 19: Configure Access Control** for configuration instructions. Access to output device operations and configurations is controlled by permissions. See **Chapter 21: Configuring Permissions** for more information.

12.1 OUTPUT DEVICES WINDOW

- Select **Operations > Output Devices** to display the *Output Devices* window.

The left pane includes a list of output devices added through Configuration > Access Control > Reader Interfaces or I/O Interfaces.

The right pane provides the option to associate a camera or video stream with the selected device. If a camera and device are associated, a video stream is displayed with Remove Camera, Talk Back (if available), Activate, and Deactivate buttons. The video player also can be launched by clicking on the video in this pane.



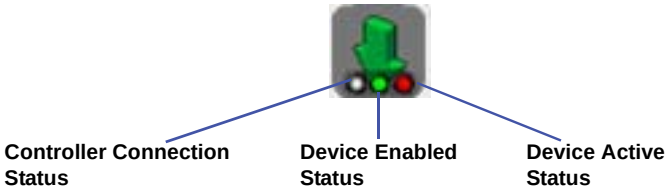
12.2 OUTPUT DEVICE LIST

The Output Device list contains the devices added under the Configuration > Access Control > Reader Interfaces and I/O Interfaces options. See **Configure Reader Interfaces** and **Configure I/O Interfaces** in **Chapter 19: Configure Access Control** for configuration instructions.

The Output Devices list can be filtered and searched. See **Operations Windows** and **Searching a List**, in **Chapter 3: Using the NLSS Web Interface** for more information on using a list and its functions, searching a list, respectively.

12.2.1 Output Device Icons

Each output device icon includes three LEDs to indicate status.



Controller Connection Status*	Device Enabled Status	Device Active Status
• Green = In Service/Online • Yellow = Not in Service/ Online • Red = Offline • Gray = Preprovisioned	• Green = Enabled • Red = Disabled	• Red = Active (signal sent) • Green = Not active

* *Controller Connection Status*: status of the controller to which the output device is connected. This includes MR16Out: the connection status is of the 1502 that controls it.

12.3 ACTIVATING AND DEACTIVATING A DEVICE

An output device can be activated from the Operations > Output Device window. The output signal toggles a relay on a reader interface and I/O interface board. The signal closes or opens the circuit, depending on if its normally open or normally closed.

The output remains active for the duration set in Configuration > Access Control. If no duration is set, the signal remains on until it is deactivated. See **Configure Reader Interfaces** and **Configure I/O Interfaces** in **Chapter 19: Configure Access Control** for output duration configuration instructions.

Activating and deactivating an out device is done from the right pane.

1. Select **Operations > Output Devices** from the Main Menu.
2. Select a device from the list.
3. Click **Activate**.
4. Click **Deactivate**. to stop a device before the duration expires, or no duration is set.

© 2009-2014 Next Level Security Systems, Inc.

12.4 ADD CAMERA

A camera can be associated with an output device. The camera's stream can be viewed directly from the right pane in the Output Devices window.

12.4.1 Adding and Viewing Cameras with Output Devices

By default, output devices do not have cameras associated with them.

1. Select **Operations > Output Devices** from the Main Menu.
2. Select an output device from the list.
3. Click **Associate Camera** to display the Camera list in the right pane. See **Selecting Cameras** in **Chapter 4: Controlling Cameras** for more information.
4. Select a camera or video stream.

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

12.4.2 Remove Camera

The association between a camera and an output device can be removed.

1. Click **Operations > Output Devices**.
2. Select an output device from the list.
3. Click **Remove Camera** to remove the link between the camera and the output device.

Note: This removal only impacts this connection, and does not effect camera or video streams connection to other devices, or availability in the camera list.

12.5 PUSH TO TALK

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 > Output Devices**.
2. Select an output device.
3. Click **Push to Talk** to speak.
4. Click **Push to Talk** again to cancel the microphone feed to the camera.

© 2009-2014 Next Level Security Systems, Inc.

12.6 EVENT LOG

The Event Log for the selected output device can be accessed from the Output Devices window.

1. Click **Operations >Output**.
2. Select an output device.
3. Click **Event Log** in the mini-pane.
   The Reports or Events pane for the output device is displayed.
   See **Chapter 15: Monitoring and Handling Events** for instructions.
4. Click **Back** to go back to the Output Devices window.

12.7 REPORTS

Reports for the selected output device can be accessed from the Output Devices window.

1. Click **Operations >Output Devices**.
2. Select an output device.
3. Click **Reports** in the mini-pane.
   The Reports or Events pane for the output device is displayed.
   See **Chapter 8: Operations with Reports** for instructions.
4. Click **Back** to go back to the Output Devices window.

© 2009-2014 Next Level Security Systems, Inc.

Chapter 13: 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 21: Configuring Permissions** for information on including floor plans or maps with a group.

See **Adding and Using Maps** in **Chapter 14: Using Groups** for instructions on uploading and using floor plans with a group.

Chapter 14: Using Groups

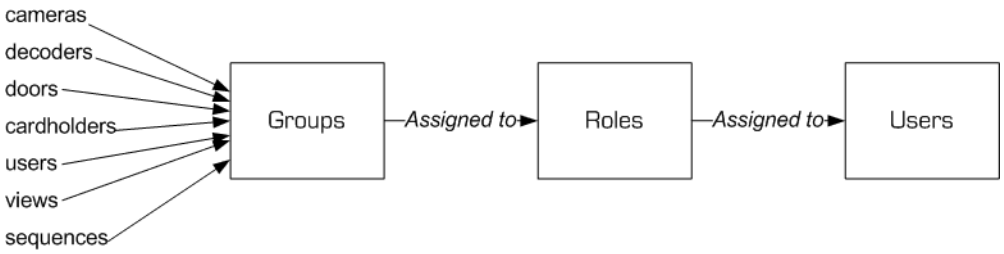
Groups are collections of cameras, decoders, doors, users, cardholders, views and sequences. In RMS, Groups consist of Gateways and Multiviews on the RMS Level. Groups can have different types of objects in the same group.

From the Operations module, groups are used to quickly access details or video for items in the group.

From the Configuration module, groups on a Gateway are used to enable and disable access to certain devices and operations for users. Groups are *not* for bulk configuration of like objects.

Using Configuration > Permissions, items are assigned to Groups. 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.

Groups also can include a floor plan or a map, if so configured. The items in the group can be moved on the graphic to show location of the item.

See **Chapter 21: Configuring Permissions** for more information on how permissions work together, and instructions on setting up groups and permissions.

14.1 GROUPS WINDOW

Groups are accessed under **Operations > Groups**.

When an item is selected in a group, the display and features are the same as if the item was selected from its respective Operations menu list.

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

- *List View*: a list of the grouped items is displayed. Click on an item to display details in the right pane, or video, depending on the device type of the item.

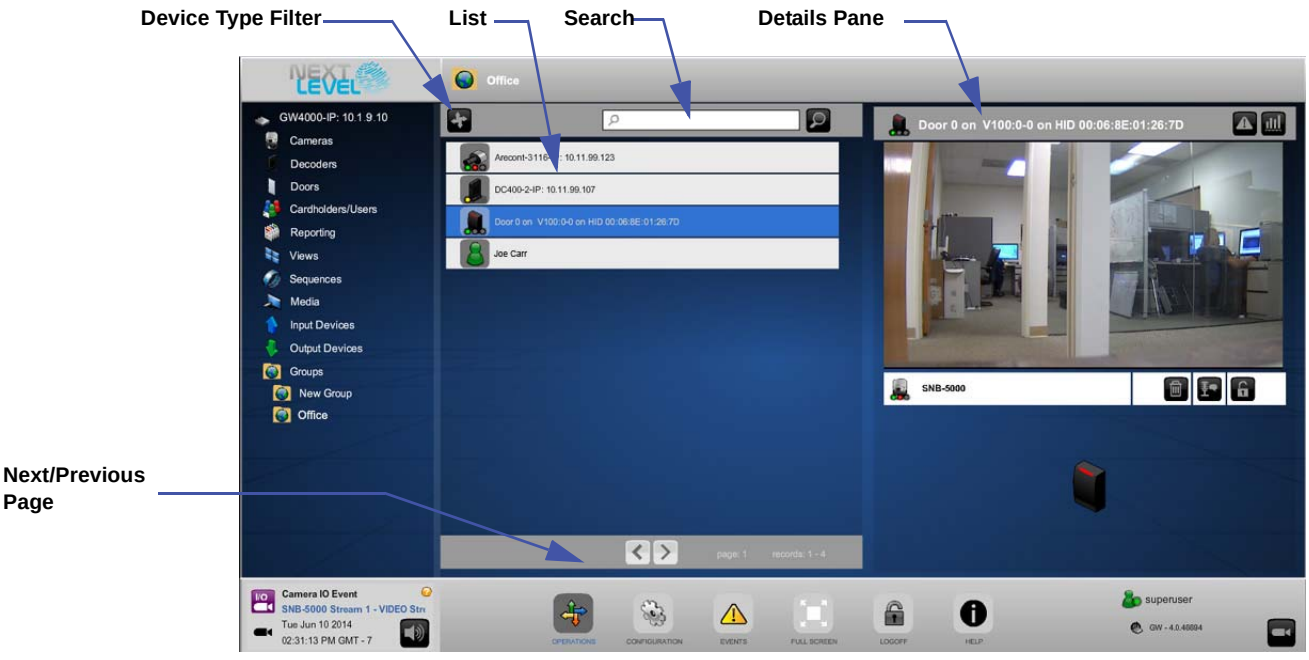
  See **Groups** in **Chapter 21: Configuring Permissions** for more information on creating and maintaining groups.

- *Map View*: if **Show Maps** was selected in Configuration > Permissions > Groups, a JPEG of a map, floor plan or graphic can be uploaded as a background graphic for the group. Click an icon to display details or a video, depending on the device type of the item.

  See **Adding and Using Maps** in this chapter, and **Create a Group** in **Chapter 21: Configuring Permissions** for more information.

14.2 LIST VIEW

1. Select **Operations > Groups > *group name***, where *group name* is the specific group.
2. Select a group with a globe on the folder for a List view.

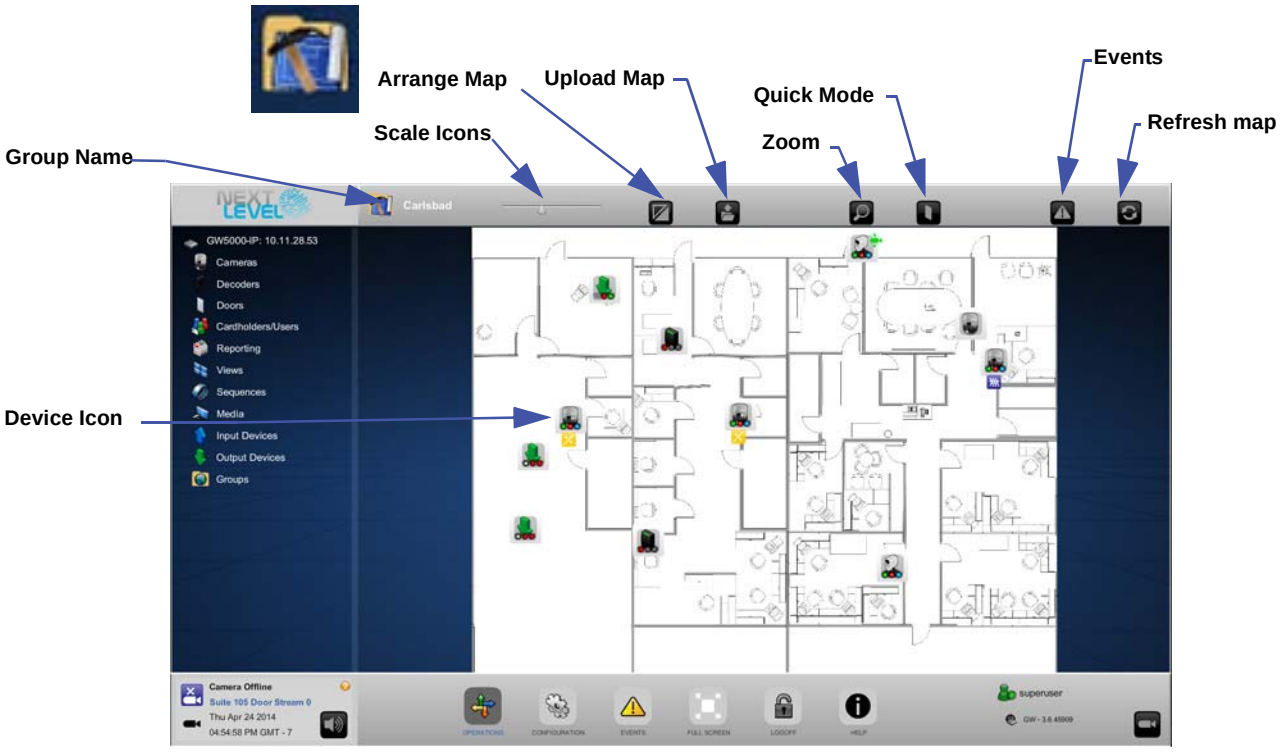


- **Device Type Filter**: displays the filter dialog. The list can be filtered on a device type, or multiple types, that make up the group. Options include: Cameras, Cardholders, Decoder, Door, Group, Sequence, User, and View.
- The **Group** option allows the filter to show or hide sub-groups of the selected group.
- **List**: the items are added under Configuration > Permissions >Groups. See **Groups** in **Chapter 21: 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.
- **Details Pane**: the display is dependent on the selected item's device type. Cameras, Views and Sequences display full screen video players. Doors display a mini-player, if a camera is associated with the door.

14.2.1 Adding and Using Maps

Maps allow a background image such as a map or a floor plan 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 floor plan to show a security layout for an office.

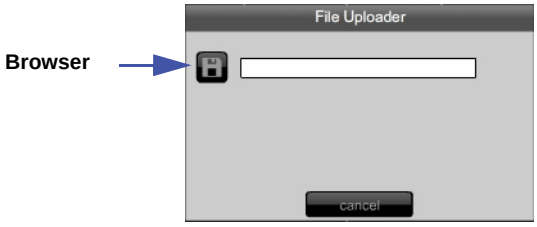
Select a group with a map on the folder for a Map view.



Note: The User must have the appropriate permissions to see and access the icons and associated functions. See **Chapter 21: Configuring Permissions** for more information.

Access control must be enabled for a system for the door controls to be available.

- **Scale Icons**: drag slider to increase and decrease icon size.
- **Arrange Map**: click to move icons. Click **Arrange Map** again to lock the icons in place.
- **Upload Map**: click to launch the *File Uploader* dialog to upload a new background.
  - The recommended size of the .jpeg is 1300x800 @ 72dpi
    - » The image can be larger or smaller, as it scales to fit the screen.
    - » The Web Interface provides a zoom tool. A larger the map provides better resolution when zoomed in. Smaller maps load quicker and are good for nesting groups.
  - 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.

    The Show Map option must be selected in **Configuration > Permissions > Groups**. See **Create a Group** in **Chapter 21: Configuring Permissions** for more information.

- **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.

- **Quick Mode**: click **Quick Mode** to enable a single click to unlock a door.
  - If Quick Mode is enabled, video for a selected door cannot be accessed from the icon.
  - This setting does not impact the other icons.
  - Click **Quick Mode** again to return to *Regular Mode*.
- **Refresh Map**: click **Refresh Map** to update the display.
- **Device icon**
  - Hover over an icon to expand it to display the device's name, and options, if applicable.

  - Click an icon to launch the video player or a Details pane for the device.
    - The Details pane is the same that is accessed from the respective Operations menu option for that device.
    - If a camera is associated with the device, the video player for that camera is displayed.
  - Where applicable, reports and events for the selected item can be accessed from the Details pane.
  - Launch the video player from a camera icon.
  - Lock or unlock a door from door icon.
  - Activate or deactivate output devices from an output device icon.

- **Open All Doors**: click **Open All Doors** to temporarily unlock all doors in the group.
- **Events**: click **Events** to open an Events Log for the devices in the group.

14.2.1.1 Opening a Door from a Floor plan or Map

A door can be temporarily unlocked using either Regular Mode or Quick Mode.

Using either of these modes, the door is temporarily unlocked, according to its strike time setting in Configuration > Access Control > Doors. See **Configure Doors** in **Chapter 19: Configure Access Control** for more information.

14.2.1.1.1 Regular Mode

To temporarily unlock a door from a floor plan or map in Regular Mode:

1. Hover over or click a door icon.

2. Click **Unlock** in the pop-up menu.
   - Talkback is also available in the pop-up menu.

14.2.1.1.2 Quick Mode

To temporarily unlock a door from a Floorplan or map in Quick Mode:

1. Ensure **Quick Mode** is enabled in the top menu.
2. Click the icon for the door.

14.2.1.2 Viewing Video from a Floorplan or Map

Video can be displayed from Cameras, Decoders, Views, and Sequences, from a floorplan or map.

- Click a **Camera**, **Door**, **Decoder**, **View** or **Sequence** icon.

The camera video player, view, or sequence window is displayed for those selections. A mini-pane is displayed if a decoder or door is selected.

© 2009-2014 Next Level Security Systems, Inc.

14.2.1.3 Deactivating a Cardholder Information via a Floorplan or Map

A Cardholder and User Details pane can be accessed from a floor plan or map. The name and other related information is displayed.

A cardholder's card also can be deactivated or activated from this window.

1. Click a **Cardholder** icon.

   The Details pane for the selected cardholder is displayed.

2. Click **Deactivate** in the Cardholder Details pane.
   – Click **Activate** to enable a card.

14.2.1.4 Activating and Deactivating an Output Device

Intrusion detection output devices can be enabled or disabled from a group.

1. Hover over a device from the list.

2. Click **Activate**.
3. Click **Deactivate**. to stop the device before the duration expires, or no duration is set.

See **Chapter 12: Operations with Output Devices** for more information about output devices.

Chapter 15: Monitoring and Handling Events

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

15.1 MONITORING EVENTS

The Events log displays events in real-time, as well as providing a list of recent events. The log can be customized by date and time, and a series of filters.

Access to Events is controlled by Permissions. See **Roles** in **Chapter 21: Configuring Permissions** for more information.

- Click **Events** in the Main Menu to access the Event Log for all Gateway features.

- Click **Events** in an Operations Preview pane or a video player for a selected item to access the Event Log only for that item. Event logs are available for cameras, decoders, doors, cardholders, and users.

The Event Log provides a list of the events detected in the system. Click on an event to get a more detailed view of the event, with options 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.

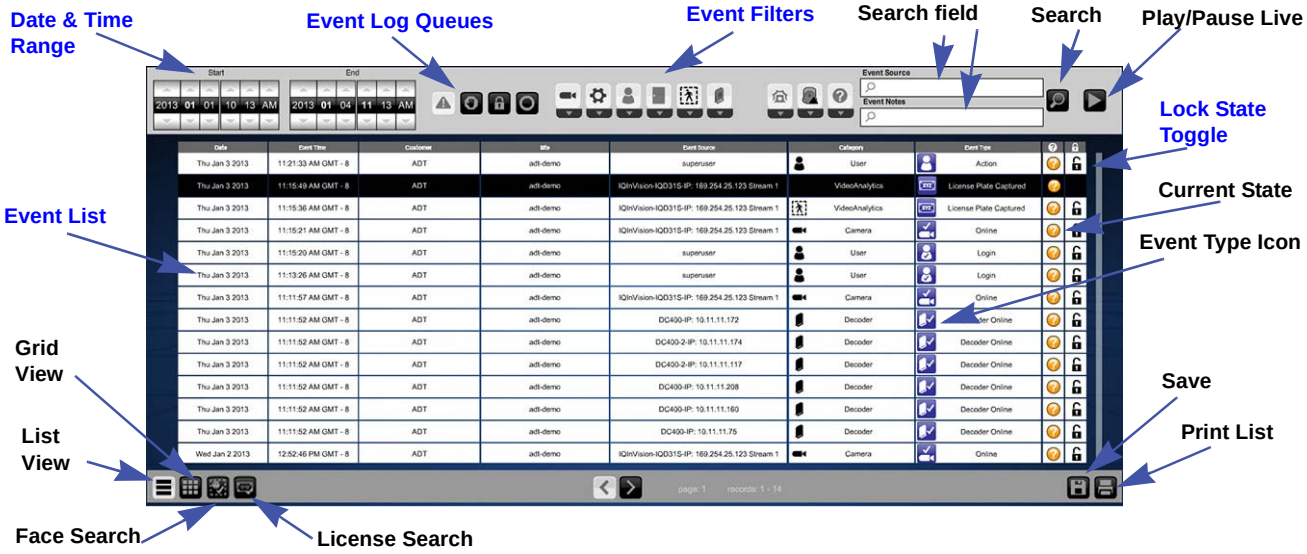
Important: If the Events button is pulsating, an Emergency event has been generated. See **Emergency Events** for instructions.

Event Type and Event Severity are set under Configuration > Global. See **Configure Event Types** and **Configure Event Severity** in **Chapter 17: Global Configurations** for instructions and more information.

15.2 EVENT LOG

When an Events button is clicked, the *Event Log* is displayed listing events over a specified time period. Click on an event to display the **Event Details**.
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. Click **Search**. *Do not* use the browser's refresh button, as that returns the window to the login window.



15.2.1 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.

15.2.2 Event Log Queues

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

Event Log: lists all events.

Shunt Queue: 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**.

Locked Queue: 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 (deleted), but video eventually may be groomed. Event video only is guaranteed to be saved if total disk usage remains below 90%.

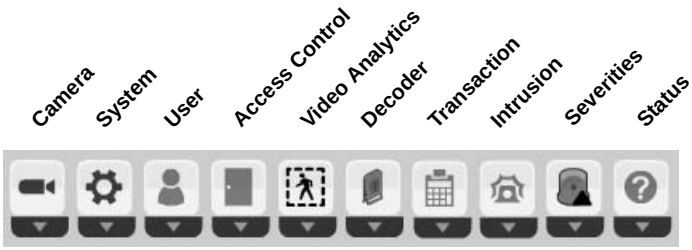
Emergency Queue: lists events with an emergency status. See **Emergency Events**.

15.2.3 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 changes to black when selected to filter out that category.

The filter can be set to a more granular level by selecting individual event types from a dialog box.

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 **Select All** to select all event types in the dialog and allow them in the Event Log list.

© 2009-2014 Next Level Security Systems, Inc.

– Click the **Selections None** button to deselect all event types and filter them out of the Event Log list.

3. Click the **Close** button to exit the dialog.
4. Click **Search** 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 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.

15.2.4 Search Fields

The Events log can be searched by the item triggering an event (Event Source), or by descriptive text (Event Notes).

1. Set the **Start** and **End** times and dates.
   – Event filters also can be set to further define the search.
2. Enter the search text in the Event Source or Event Notes field.
   – Text can be entered in both fields to further define the search.
   – Partial strings can be entered, such as part of a user's name.
3. Click **Search**.
4. The Start and End times and dates, filters, and search fields can be further defined to narrow the search results.

   Adjust these parameters and click **Search** again.

15.2.5 Event List

The Event Log provides high level information on each event.

- **Date** and **Event Time**: the date and time the event took place.
- **Customer**: the owner of the Gateway. This field only differs if the Event Log is accessed at the RMS level.
- **Site**: the Gateway on which the event occurred. This field only differs if the Event Log is accessed at the RMS level.
- **Event Source**: the device, user, cardholder, or other system resource that triggered this event.
- **Category**: the categories of events include Access Control, Camera, Cardholder, Door, System. These icons are the same as used for the filter buttons. See **Event Filters**.
- **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.

© 2009-2014 Next Level Security Systems, Inc.

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**.

- **Current State**: indicates whether the event is:

  Open

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

  Acknowledged

  Closed

  If an event requires acknowledgment, 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 Groomer Settings** in **Chapter 17: 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**.

15.2.6 List Actions

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

Pause/Play Live: 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 an update of the Event Log. 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.

© 2009-2014 Next Level Security Systems, Inc.

15.3 EVENT DETAILS

When an event is selected in the Event Log, 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.

15.3.1 Event Details Actions

The *Event Details* dialog allows a user to acknowledge an event, play it back, add notes, see linked events (if applicable), and save and print a record of the event.

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

15.3.1.1 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, click **Acknowledge** to indicate that someone has looked at the event. This status can be applied to events either marked as *Open* or is marked as *Needs Acknowledgment*.

  Events may be configured by the Superuser to require acknowledgment. See **Event Type Details**.

- If no further action is needed on the event, click **Closed**. This marks the event as resolved.
  - This button does not close the dialog. Use the **Close** to leave the dialog.

15.3.1.2 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 an event type is no longer shunted, the database resumes recording those events.

- 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.

15.3.1.3 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.

15.3.1.4 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 **Save** 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.

15.3.1.5 RECORDED EVENT

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

15.3.1.6 CURRENT SNAPSHOT

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

15.3.1.7 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.

15.3.1.8 EXPORTING THE EVENT LOG

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

Save CSV File: 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.

© 2009-2014 Next Level Security Systems, Inc.

15.3.1.9 CLOSE

The **Close** 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.

15.3.2 Emergency Events

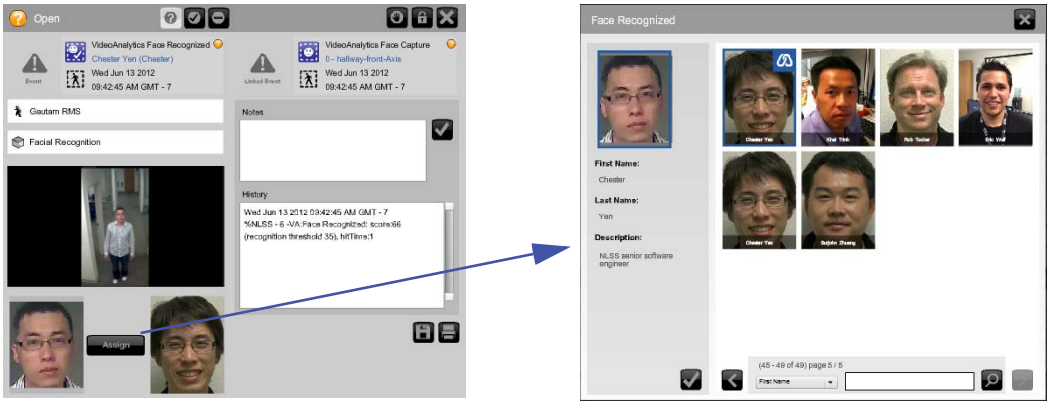
If the Events button is pulsating in the Main Menu, an Emergency event has been triggered. Emergency events are user configured by setting the severity of an event type. See **Configure Event Severity** for more information.

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 instructions.
6. Click the **Closed** to remove the event from the Emergency queue.

15.4 FACE RECOGNITION EVENTS

When a Face Recognition event occurs, the event displays the captured face, along with the matched face from the database. If the face match is not correct, a match can be manually assigned using a different image or person. The event is updated to reflect the correct match.

1. Open the *Events Details* dialog for a Face Recognition event.
   See **Event Details** for general instructions on using this dialog.
2. Click **Assign**.
   The *Face Recognized* dialog opens, and displays all of the pictures contained in the Face Recognition database. The pages can be scrolled and searched using the buttons and search field at the bottom of the dialog.



3. Select a new image to assign to the event.

4. Click **Save**.

The event now reflects the update.

15.4.1 Events and Linkages

Face Recognition triggers an event in the system. As with other events, any Face Recognition event can be linked to Actions via the Event Linkages feature.

When the event is linked to the email action, the snapshot of the face capture and the snapshot from the database are included in the message. The event is time-stamped, simplifying retrieval of the video using the NLSS Web Interface.

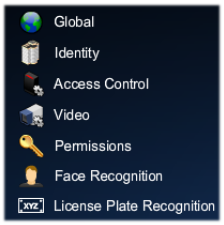
See **Configure Event Linkages** in **Chapter 17: Global Configurations** for instructions and more information on event linkages.

© 2009-2014 Next Level Security Systems, Inc.

PART 3: SYSTEM CONFIGURATION

System Configurations contains instructions for configuring the devices and data used by the NLSS Unified Security Suite. Configuration is done by users with appropriate permissions, such as Superusers, using the NLSS Web Interface generated by the NLSS Gateway.

Only users with the appropriate software *permissions* on 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 (*clone*) other user accounts with various permissions (including other superusers with unlimited permissions).



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

1. Review the common configuration functions in **Chapter 16: General Configuration Functions**.
2. Do global configurations, as described in **Chapter 17: Global Configurations**.
3. Configure identity related information, as described in **Chapter 18: Configure Identity and Credentials**.
4. Configure Access Control, as described in **Chapter 19: Configure Access Control**.
5. Configure video sources, as described in **Chapter 20: 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 21: Configuring Permissions**.

If Face Recognition or License Plate Recognition are added to the system, they must be configured prior to using it

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

Important: When entering data in a configuration field, only use alpha-numeric characters, as follows:

Letters: A-Z (upper or lower case)

Numbers: 0-9

A dash (-), or underscore (_).

No special characters (&, :, ., #, etc.)

© 2009-2014 Next Level Security Systems, Inc.

Chapter 16: 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.

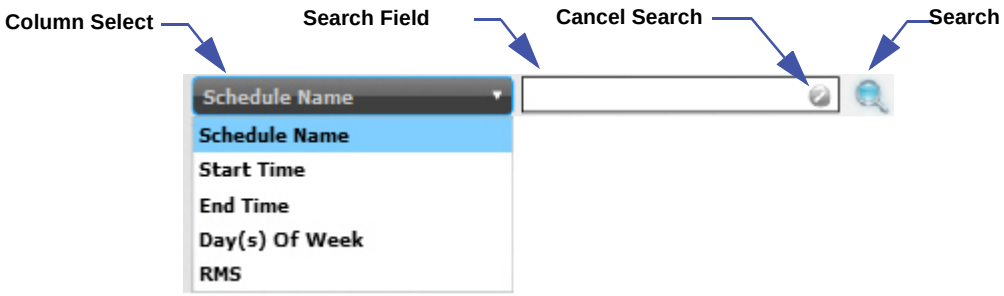
Sort: click a column header to sort the results in ascending (up arrow) or descending (down arrow) order.

Pages: pages for a table are accessed via the numbered buttons below the list. The current page is highlighted with the blue rectangle.
Click the double dashes (**--**) to return to the first page.
Click the double plus signs (**++**) to go to the last page.

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

16.1 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** 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.

16.2 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.

16.2.1 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 module to be configured, such as Global, Identity, Access Control, Video, Permissions, or Face Recognition. *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.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

4. Click **Save**

to keep the settings.

   – Click **Cancel**

to clear the fields, and revert to the default settings, if any.

16.2.2 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.

© 2009-2014 Next Level Security Systems, Inc.

16.2.3 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.

© 2009-2014 Next Level Security Systems, Inc.

Chapter 17: Global Configurations

NLSS recommends doing global configurations in the following order:

1. **Configure Subscriptions** (if applicable)
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 panes until a change is made. The Save button remains grayed out if a required field is blank.

Access to any Configuration category, in general, can be controlled by permissions. Permissions can be set to the view, add, edit and delete functions for an item. See **Chapter 21: Configuring Permissions** for more information.

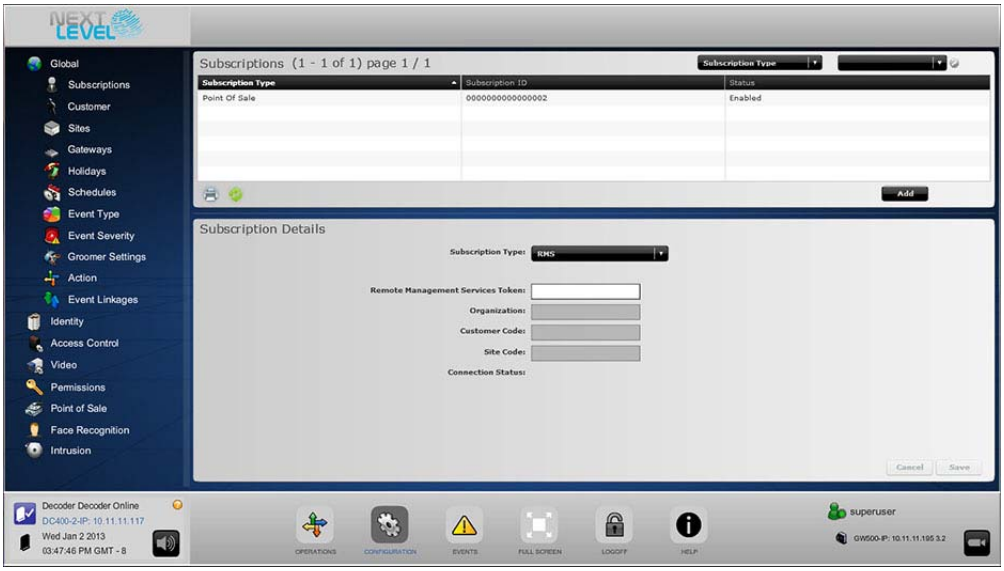
© 2009-2014 Next Level Security Systems, Inc.

17.1 CONFIGURE SUBSCRIPTIONS

Configuration > *Subscriptions* is the window where tokens are entered to enable *premium* options for a Gateway. These features are optional for a Gateway. The tokens are provided by NLSS or a partner.

- Select **Configurations > Global > Subscriptions** from the Main Menu.

The *Subscriptions* window is displayed.



The *Subscriptions* table lists the options for which tokens have been entered for the Gateway.

- **Subscription Type**: either *RMS*, *Face Recognition*, *Point of Sale*, *License Plate Capture*, *Intrusion*, or *Audio Analytics: Car Alarm/Aggression/Gun Shot*.
- **Token** (Subscription ID): the token entered for to enable the selected option.
- **Status**: whether the feature is enabled or not.

Subscriptions Details provides a field to enter a token to enable the feature.

See **Enabling RMS** for descriptions of additional fields, and the steps for enabling RMS.

Note: Once the token is saved and the feature is enabled, the fields in the Subscriptions Details pane cannot be edited.

© 2009-2014 Next Level Security Systems, Inc.

17.1.1 Enabling 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.

Note: *If no Gateway is registered with RMS*, *NLSS recommends configuring a Gateway locally before applying RMS across the system.* Settings can be tested on that Gateway, before applying those settings to multiple Gateways via 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. Select **Configurations > Global > Subscriptions** 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.
     - **Organization**: used by RMS to group Customers. This field is used when logging into RMS.
     - **Customer Code** and **Site Code**: identifiers generated by RMS.
     - **Connection Status**: indicates if the Gateway is connected to RMS.
3. Click **Save**

to record the token.
   - Click **Cancel**

to clear the token.

See **Chapter 27: NLSS Remote Management Services** for instructions on configuring and using RMS.

17.1.2 Enabling Other Premium Features

Other premium features are also added enabled using a token.

1. Select **Configurations > Global > Subscriptions** from the Main Menu.
2. Click **Add**.

3. Select a **Subscription Type** from the drop-down menu under *Subscription Details*:
   - **Access Control**: see **Chapter 18: Configure Identity and Credentials** and **Chapter 19: Configure Access Control** for more information.
   - **Face Recognition**: see **Chapter 22: Configuring and Using Face Recognition** for more information.
   - **Point of Sale**: see **Chapter 26: Configuring and Using Point of Sale** for more information.
   - **License Plate Capture**: see **Chapter 23: Configuring and Using License Plate Recognition** for more information.
   - **Intrusion**: see **Chapter 25: Configuring and Using Intrusion Detection** for more information.
   - **Audio Analytics: Car Alarm/Aggression/Gun Shot**: see **Chapter 24: Configuring Audio Analytics** for more information.

© 2009-2014 Next Level Security Systems, Inc.

4. In the **Token** field, enter the token from NLSS or the Partner.
5. Click **Save** to record the token.
   – Click **Cancel** to clear the token.

17.2 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.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

17.2.1 Customer Details

These parameters define the customer that is selected in the table in the top pane of the *Customer Details* window.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.

17.2.2 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.

© 2009-2014 Next Level Security Systems, Inc.

17.3 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* window accessed from the RMS level has additional tabs. See **Sites** in **Chapter 27: NLSS Remote Management Services** for more information.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

17.3.1 Site Details

The Site Details pane, in the *Configuration* > *Global* > *Sites* window, 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 27: NLSS Remote Management Services** for RMS instructions.

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

17.3.2 Editing Site Details

1. Select **Configuration > Global > Sites** from the Main Menu.
   The *Site Details* window 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.

© 2009-2014 Next Level Security Systems, Inc.

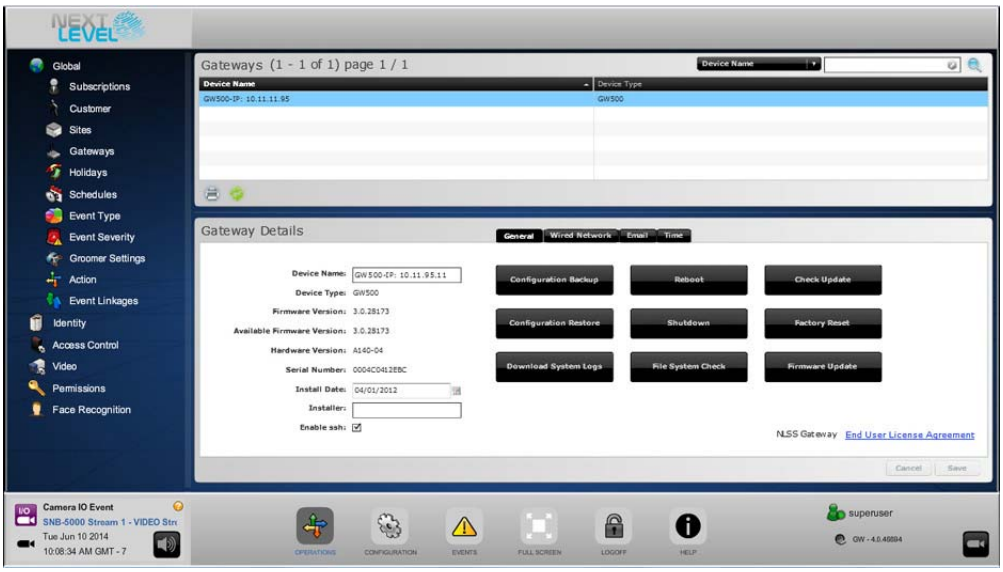
17.4 CONFIGURE NLSS GATEWAYS

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

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

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

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



17.4.1 General Tab

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

17.4.1.1 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.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

- **Device Type**: (read-only) the model of the selected NLSS Gateway.
- **Firmware Version**: (read-only) the firmware version running on the Gateway.

© 2009-2014 Next Level Security Systems, Inc.

- **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 user name and password. When they are finished, disable SSH to prevent further access.

Notes

  – Only Superusers can enable SSH.
  – As long as SSH is disabled, no one can log into the Gateway via SSH, even with the SSH password.

17.4.1.2 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**

© 2009-2014 Next Level Security Systems, Inc.

17.4.1.2.1 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 re-compressed before being used to restore system configurations.

17.4.1.2.2 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.

© 2009-2014 Next Level Security Systems, Inc.

17.4.1.2.3 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

17.4.1.2.4 Reboot

Important: The 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.

17.4.1.2.5 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.

© 2009-2014 Next Level Security Systems, Inc.

MANUAL SHUTDOWN

If the Local Interface is not available:

- *Quickly* press and release the power button on the Gateway to properly shut it down. The power lights go off to indicate that the device is powered down.

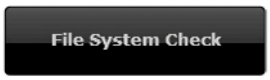
Important: Do not unplug the unit or hold down the power switch to shut it down, as these steps can cause an improper shutdown.

17.4.1.2.6 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.

17.4.1.2.7 Check Update

The value in the Available Firmware Version field blinks if a newer version is available. Selecting Check Update 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.

© 2009-2014 Next Level Security Systems, Inc.

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.

Note: If the Gateway is running an older version, then certain intermediate versions are installed to reach the current release: v3.0 > v3.3 > v3.6 > v4.0.

17.4.1.2.8 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.

Important: If the Gateway is running an older version, then certain intermediate versions must be installed to reach the current release: v3.0 > v3.3 > v3.6 > v4.0.

Not all versions between the current and older release have to be installed. For example, if the Gateway is running v3.0, then v3.1 and v3.2 can be skipped, and 3.3 is installed, then v3.6, then 4.0.

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.

17.4.1.2.9 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.

© 2009-2014 Next Level Security Systems, Inc.

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** in **Chapter 2: Installation**.

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.

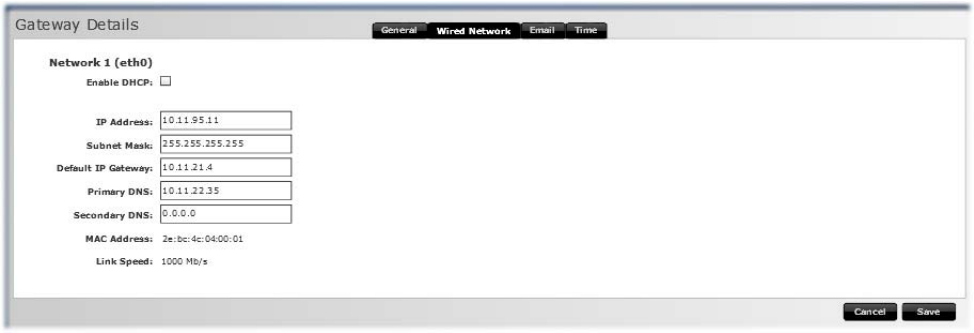
17.4.1.2.10 NLSS Gateway End User License Agreement

- 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

17.4.2 Wired Network Tab

The GW-3000, GW-4000, and the 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 can only be edited 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 that connects networks to each other, and to the Internet. It is a separate device from the NLSS Gateway.

- **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.

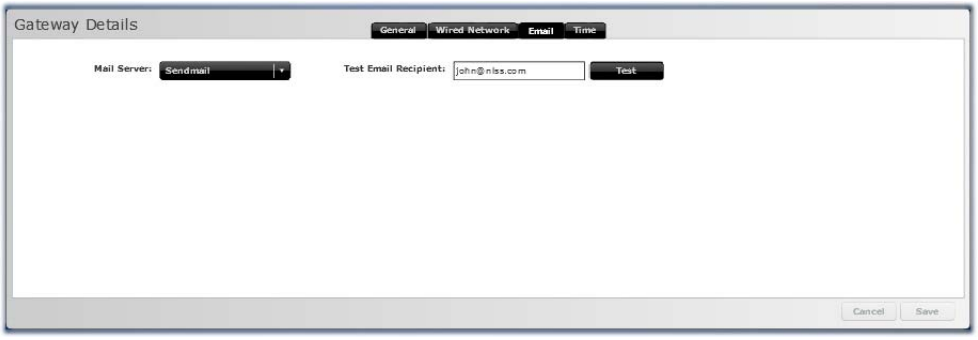
If any of the parameters are changed:

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

17.4.3 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 SMTP 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.

17.4.4 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:
  – **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.

© 2009-2014 Next Level Security Systems, Inc.

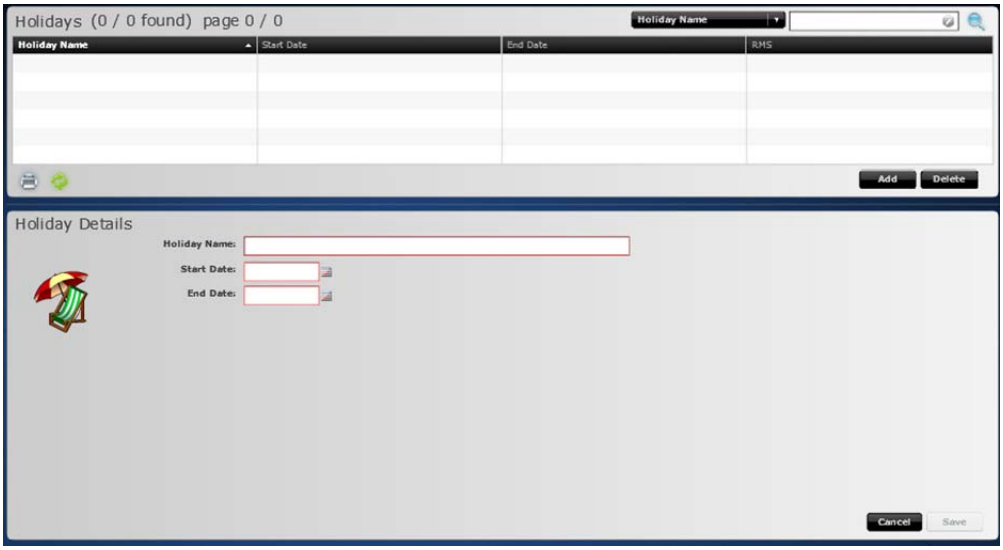
17.5 CONFIGURE HOLIDAYS

Holidays provide an exception to scheduled unlock settings for doors.

Up to 255 holidays can be configured for a Gateway.

In the *Configuration* > *Global* > *Holidays* window, the configured Holidays are listed. Initially, the window is empty. Holidays can be added, edited, searched and deleted. See **Adding, Editing and Deleting Items** and **Searching Tables** in **Chapter 16: General Configuration Functions** for instructions.

- Select **Configuration > Global > Holidays**.



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.

17.5.1 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.

17.5.2 Holiday Details

- **Name**: enter the Holiday's name.
- **Start Date**: click the **Calendar** to select a Holiday's start date. The time the Holiday begins is 12:01 a.m. on that date.
- **End Date**: click the **Calendar** to select the Holiday's end date. The end time is 11:59 p.m. on that date. For one day Holidays, the End Date and Start Date are the same.

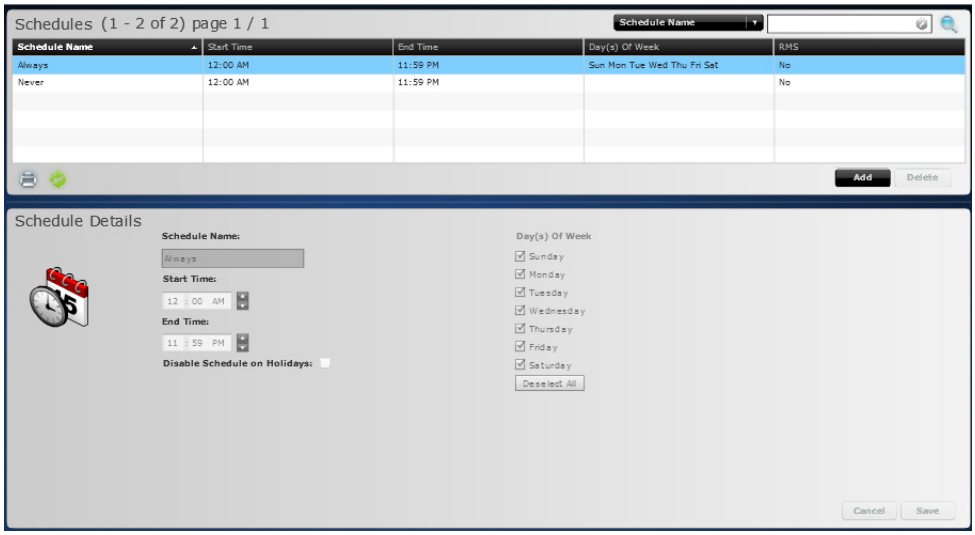
See **Adding, Editing and Deleting Items** and **Searching Tables** in **Chapter 16: General Configuration Functions** for add, edit, delete and search instructions.

© 2009-2014 Next Level Security Systems, Inc.

17.6 CONFIGURE SCHEDULES

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

- Select **Configuration > Global > Schedules**.



These settings cannot be modified at the site level if 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** window, 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** window, 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** window, 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* window 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.

© 2009-2014 Next Level Security Systems, Inc.

17.6.1 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.

17.6.2 Create New Schedules

Up to 255 schedules can be created for a Gateway.

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.

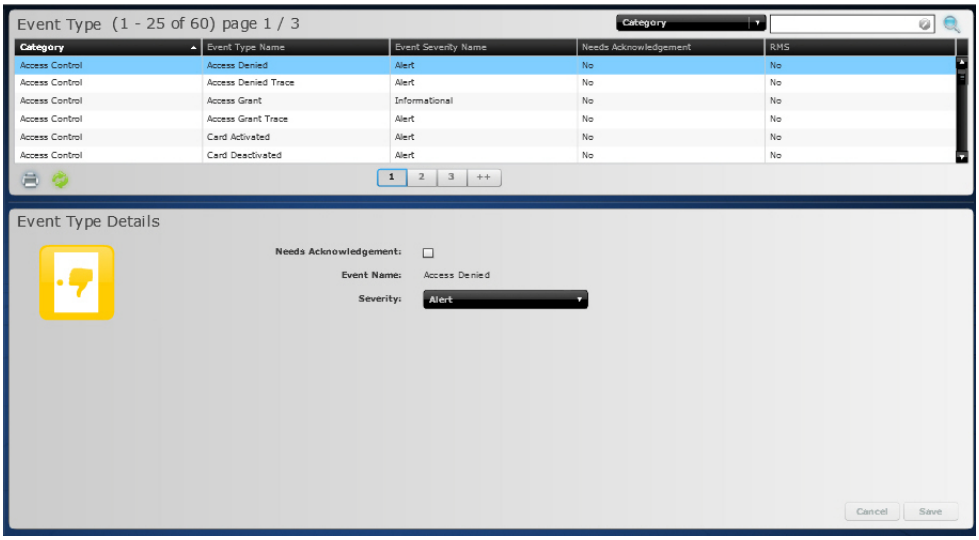
See **Adding, Editing and Deleting Items** and **Searching Tables** in **Chapter 16: General Configuration Functions** for edit, delete and search instructions.

© 2009-2014 Next Level Security Systems, Inc.

17.7 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* window.

- Select **Configuration > Global > Event Type**.



Event Types cannot be added or deleted, but can be edited and searched. See **Chapter 16: General Configuration Functions** for edit and search instructions.

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

17.7.1 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.
- **Severity**: the Severity level assigned in the *Event Type Details* pane.
- **Needs Acknowledgment**: if an event is checked with Needs Acknowledgment, it displays in the Event Table in the Open State, but the icon is Red, not Orange.

  This setting is cleared when the status is changed to *Acknowledged* in the Event dialog. The Events Table can be filtered on Needs Acknowledgment. See **Chapter 15: Monitoring and Handling Events** for more information.

© 2009-2014 Next Level Security Systems, Inc.

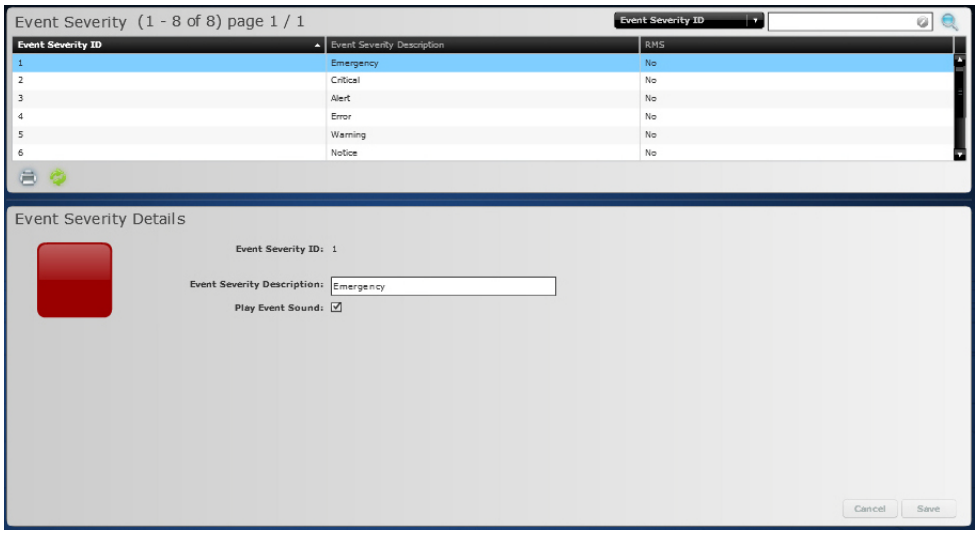
17.7.2 Event Type Details

- **Needs Acknowledgment**: select this box to require an acknowledgment of this Event Type; deselect to make an acknowledgment 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.

17.8 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* window. 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.

- Select **Configuration > Global > Event Severity**.



Event Severity can be searched. See **Searching Tables** in **Chapter 16: General Configuration Functions** for instructions.

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

17.8.1 Event Severity Table

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

17.8.2 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).

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

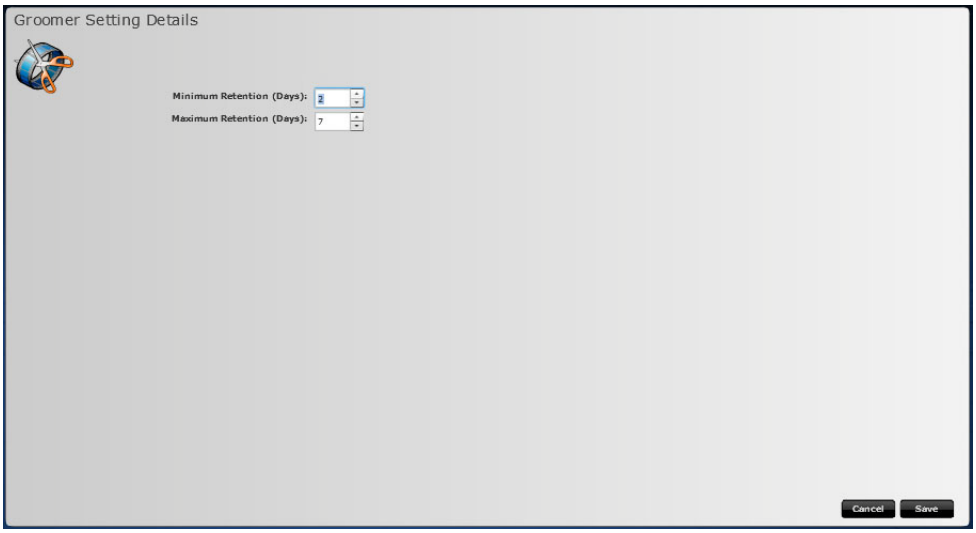
Note: Click **Save** after modifying the **Description**.

17.9 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* window 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.

     This setting is applicable only for non-event-based media.

     Event-based media is retained longer (on a best-effort basis).

     Non-event-based media is removed first, if it is older than the specified minimum days of retention.
   - **Maximum Retention (Days)**: the longest time (in days) that saved files are preserved, before being deleted by the groomer function.

© 2009-2014 Next Level Security Systems, Inc.

This setting applies to all media. Media older than the max days of retention is removed first when a disc reaches its capacity.

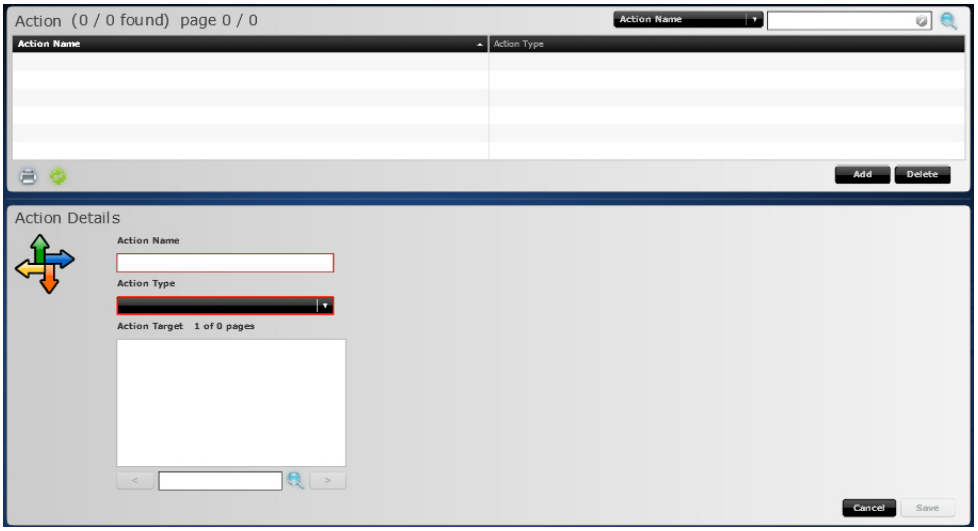
3. Click **Save** to keep the changes.
   – Click **Cancel** to return to the previous settings.

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

17.10 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. See **Configure Event Linkages** for instructions.

- Select **Configuration > Global > Action**.



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 16: General Configuration Functions** for instructions.

17.10.1 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.
CameraOutput	Enables the selected I/O output ona camera, if so configured.
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.
FaceRecognitionValidate Group	A face is compared to pictures in the database for a face recognition group. If a match is found, the action is triggered. A Face Match Group event can be tied to this action in Event Linkages.
InAreaArm	Arms an intrusion device for an area when triggered by the linked event. See **Arming or Disarming an Area** in **Chapter 25: Configuring and Using Intrusion Detection** for more information.
InAreaDisarm	Disarms an intrusion device for an area when triggered by the linked event. See **Arming or Disarming an Area** in **Chapter 25: Configuring and Using Intrusion Detection** for more information.
InOutputOff	Turns off an intrusion panel output when triggered by the linked event. See **Outputs Tab** in **Chapter 25: Configuring and Using Intrusion Detection** for more information.
InOutputOn	Turns on an intrusion panel output when triggered by the linked event. See **Outputs Tab** in **Chapter 25: Configuring and Using Intrusion Detection** for more information.
InZoneBypass	Sets an intrusion panel not to trigger an alarm when a linked event is detected. See **Bypassing a Zone** in **Chapter 25: Configuring and Using Intrusion Detection** for more information.
InZoneReset	Resets a zone alarm when a linked event is detected. See **Zone Alarm Status Indicator** in **Chapter 25: Configuring and Using Intrusion Detection** for more information.
LicensePlateRecognitionValidateGroup	A license plate is compared to license plates in the database for a LPR group. If a match is found, the action is triggered.

© 2009-2014 Next Level Security Systems, Inc.

Action Type	Definition
Play Audio	Triggers an audio file to play through the speaker connected to a selected camera and stream. Select a camera, stream, and audio file. See **Part 2: Operations** for more information.
PTZGoToHomePos	Returns a PTZ enabled camera to its home position. See **Using Presets** in **Chapter 4: Controlling Cameras**for more information.
PTZGoToPreset	Moves a PTZ enabled camera to a preset position. See **Using Presets** in **Chapter 4: Controlling Cameras** for more information.
PTZStartPatrol	Starts a Patrol sequence on a PTZ enabled camera. See **Accessing Patrols** in **Chapter 4: Controlling Cameras** for more information.
SequenceSetActive	Displays a camera sequence when triggered by the linked event. See **Create, Edit, and Display Sequences** in **Chapter 9: Displaying Video** for instructions on creating a sequence.
StreamRecordStart	Starts recording of a camera or video stream when triggered by an event. See **Camera Details Recording Tab** in **Chapter 20: Configure Video, & Storage, & Decoders** for more information.
StreamRecordStop	Stops recording of a camera or video stream when triggered by an event. See **Camera Details Recording Tab** in **Chapter 20: Configure Video, & Storage, & Decoders** 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** in **Chapter 4: Controlling Cameras** 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** in **Chapter 4: Controlling Cameras** 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.

17.10.2 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*.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

© 2009-2014 Next Level Security Systems, Inc.

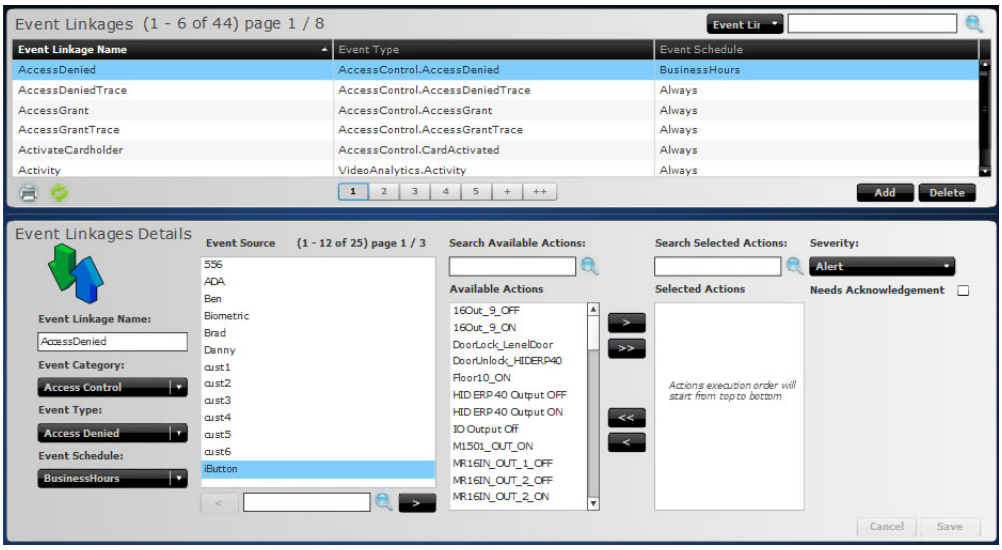
4. Select an **Action Type** from the drop-down list. See **Action Type** for more information.
   – If the Action Type applies to a door, camera or stream, or a decoder, a drop-down list shows the applicable devices.
   – **EmailSend** provides fields to enter a recipient, subject and body (message).
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 16: General Configuration Functions** for edit and deletion instructions.

17.11 CONFIGURE EVENT LINKAGES

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

- Select **Configuration > Global > Event Linkages**.



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

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

If Face Capture, Face Recognition, or License Plate Capture are linked to a email action, the message includes the captured image. A Face Recognition event also includes the image from the database to which the captured image is compared.

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 16: General Configuration Functions** for instructions

17.11.1 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 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, Audio Event Detected, Direction, Dwell, Face Capture, Face Match Group, Face Recognized, 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 item to apply the Event Linkage. The list is determined by the Event Category and 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**.

© 2009-2014 Next Level Security Systems, Inc.

- **Needs Acknowledgment**: when the linked event occurs, an acknowledgment is required from a user in the Events Log. This setting overrides the Needs Acknowledgment setting in Configuration > Event Types. See **Event Log** in **Monitoring and Handling Events**.

17.11.2 Creating an Event Linkage

1. Select **Configuration > Global > Event Linkages** from the Main Menu.
2. Click **Add**.

3. Enter a descriptive **Event Linkage Name**.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

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 16: General Configuration Functions** for edit and deletion instructions.

Chapter 18: Configure Identity and Credentials

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

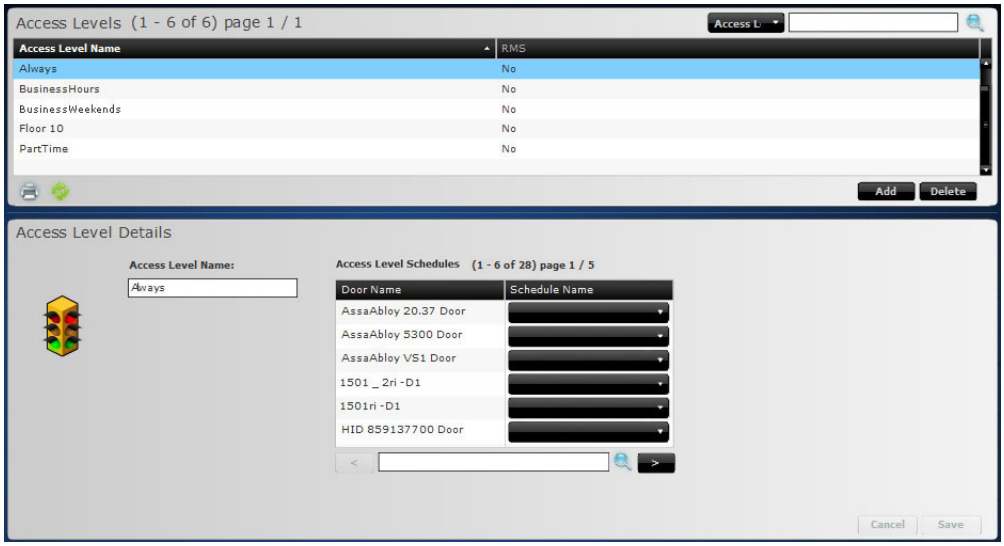
NLSS recommends Identity configuration be completed in the following order:

1. **Configure Access Levels**: required to provide access privileges to cardholders.
2. **Configure Card Types**: required to set up Cardholders, and to define the technical aspects of the card (such as Type, Bit Format and Facility Code).
3. **Configure Cardholder Types**: required to define the types of cardholders in your system, and to set up cardholders. Cardholder Types are also used to set default deactivation dates, orientation, and logos.
4. **Configure Cardholders**: requires that Access Levels, Card Types, and Cardholder Types are already configured.
5. **Users** of the NLSS Unified Security Suite software.

Configuration > Identity is not available if access control is not enabled for the Gateway.

18.1 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* window.



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 17: Global Configurations**.
- Access Levels are assigned to cardholders to grant access.
  - Use the Configuration > Identity > Cardholder > Access Level tab to assign an access level. See **Access Levels Tab**.
- Up to 128 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 128 levels.

To configure access 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.

18.1.1 Access Level Details

After an Access Level is selected 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 17: Global Configurations** for more information.

  No schedules are assigned to doors by default.

18.1.2 Create a New Access Level

Up to 8000 different access levels can be added to a Gateway.

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

3. Enter an **Access Level Name**.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

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

See **Adding, Editing and Deleting Items** in **Chapter 16: General Configuration Functions** for edit and deletion instructions.

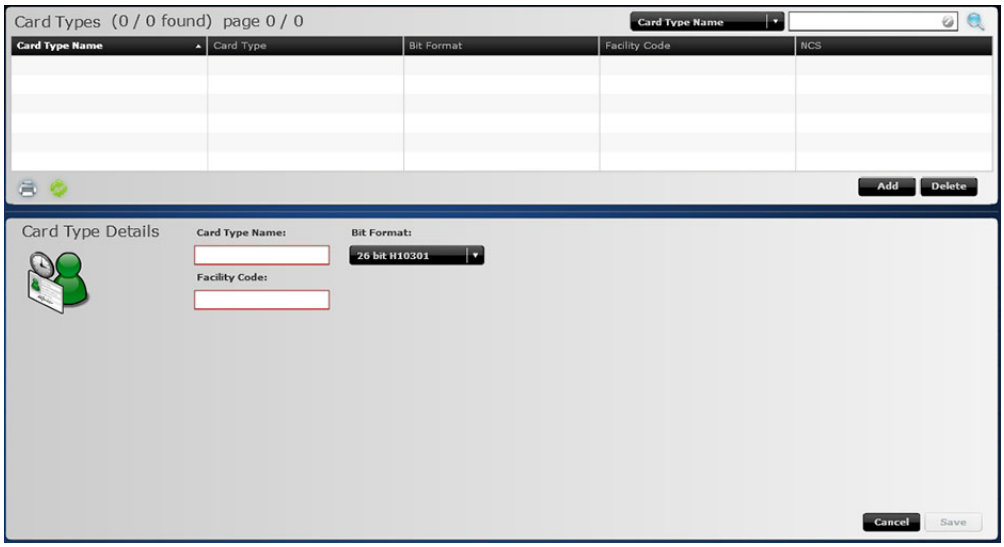
18.2 CONFIGURE CARD TYPES

Cardholders use cards to access one or more doors in the NLSS system. *Card Types* 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*.

Card Types can be added, configured, searched and deleted. See **Adding, Editing and Deleting Items** in **Chapter 16: General Configuration Functions** instructions.

18.2.1 Card Types Table

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



See **Searching Tables** for search instructions.

18.2.2 Card Types Details

- **Card Type Name**: a unique, editable field assigning a label to the profile.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

- **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.

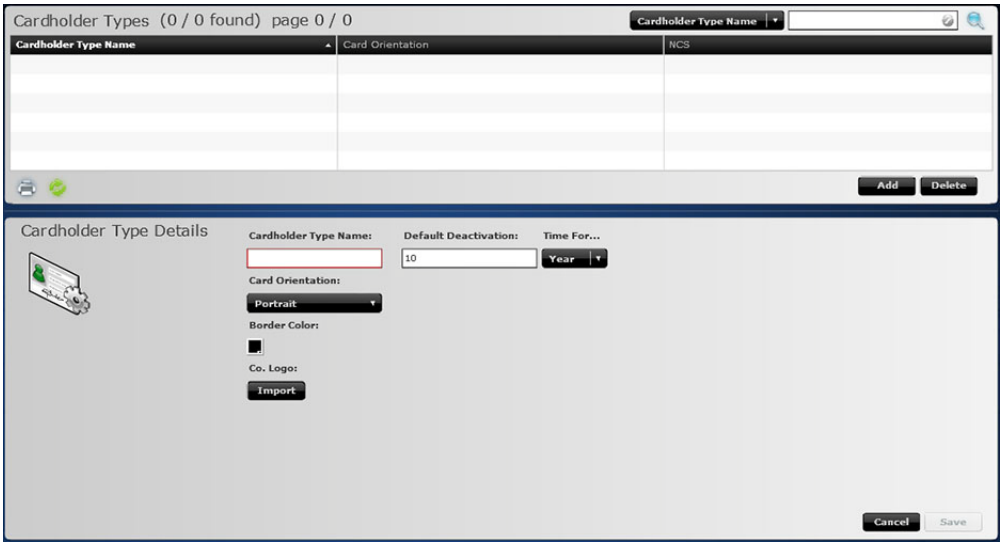
- **Bit Format**: use the drop-down list to select a data structure for this card type.
  - **26-bit: H10301**
    - » The industry standard *open* format.
    - » 255 possible facility codes.
    - » Each facility code has a total of 65,535 unique card numbers.
  - **37-bit: H10302**
    - » HID Proprietary 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**
    - » Configuration for more advanced users. For a card not covered by the other options, Unformatted is another option.
  - **ABA/ISO Track 2**
    - » A facility code is required.
  - **Unformatted**
    - » Enter the **Number of bits total**.
    - » This information can be gathered by swiping the card on an Omnikey card reader, or a reader attached to the Gateway. The later provides the information via the details for the *Access Denied* event generated by the card swipe. See **Event Details** in **Chapter 15: Monitoring and Handling Events** for more information.

© 2009-2014 Next Level Security Systems, Inc.

18.3 CONFIGURE CARDHOLDER TYPES

Configuration > *Identity* > *Cardholder Types* completes the generic information required for cardholder entries. Any additional information required to produce badges is unique to the each cardholder, and is entered in the Cardholder configuration windows.



Cardholder Types can be added, configured, searched and deleted. See **Adding, Editing and Deleting Items** in **Chapter 16: General Configuration Functions** instructions.

18.3.1 Cardholder Types Table

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

See **Searching Tables** for search instructions.

18.3.2 Cardholder Types Details

- **Cardholder Type Name**: an editable field with a unique identifier for the profile.
  - NLSS recommends creating a unique cardholder type 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.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

- **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 Cardholder Type.

© 2009-2014 Next Level Security Systems, Inc.

- **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 Cardholder Type automatically deactivate.
  - **Time Format**: a drop-down list to select either **Day**, **Month** or **Year** to set the units for the Default Deactivation.

18.4 CONFIGURE CARDHOLDERS

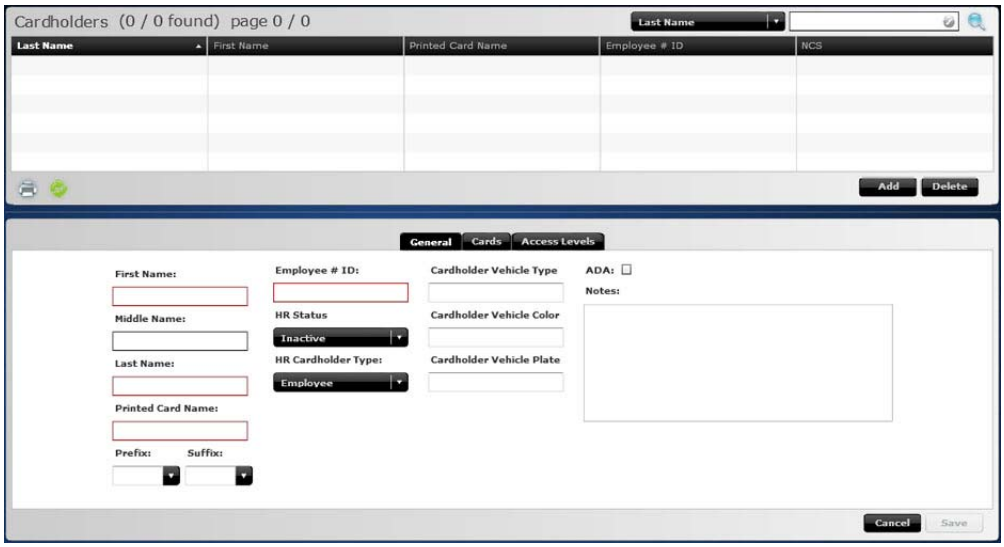
Configuration > *Identity* > *Cardholders* provides the fields needed to set up access and details for individuals with access badges.

Cardholders can access areas monitored by the 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.

Cardholders can be added individually using this menu option, or in bulk by uploading a .csv file. See **Uploading a Multiple Cardholders** in **Chapter 27: NLSS Remote Management Services** for instructions.

18.4.1 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.

18.4.2 Configuration Order

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

1. Click **Add** to create a new cardholder record, then configure the following parameters.
2. **General Tab**
3. **Cards Tab**
4. **Access Levels Tab**

Cardholders can be added, configured, searched and deleted. See **Adding, Editing and Deleting Items** in **Chapter 16: General Configuration Functions** instructions.

18.4.3 Cardholders Tabs

Cardholder parameters are configured through a series of tabs.

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

18.4.3.1 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.
- **HR 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 give it to the 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.
- **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 19: Configure Access Control**.
  - In the Controller Details window, the **DHO Time** (*Door Held Open*) is the time (in seconds) that a normally closed door can be held open before activating an alarm.

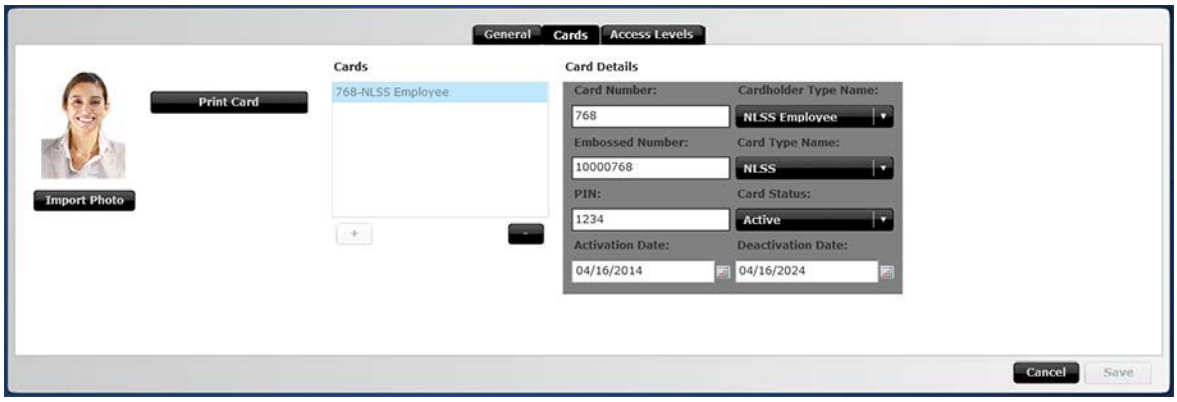
© 2009-2014 Next Level Security Systems, Inc.

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

- **Notes:** Optional comments.

18.4.3.2 CARDS TAB

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



- **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.
    - » Up to five (5) active cards can be assigned to a cardholder.
    - » Up to 100,000 access cards can issued for one Gateway.
  - Click **Delete Card** (**-**) below the list to remove a card for the selected cardholder.

  When Add is selected, additional fields are displayed.

- **Card Details**: aspects of the card used to define the card.
  - **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.
  - **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 19: 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.
  - **Activation Date**: sets the date on which this card become active. This date is set automatically when the Cardholder Type Name is selected, but can be manually changed using the Calendar tool next to the field.

© 2009-2014 Next Level Security Systems, Inc.

- **Deactivation Date**: the Cardholder Type sets the default deactivation date when this card automatically becomes inactive. This date is set automatically when the Cardholder Type Name is selected, but can be manually changed using the Calendar tool next to the field.
- **Cardholder Type Name**: a drop-down menu to select a Cardholder Type for this card. At least one Cardholder Type must created before cards can be created. See **Configure Cardholder Types** for more information.
- **Card Type Name**: a drop-down menu to select a Card Type for this card. At least one Cardholder Type must created before cards can be created. See **Configure Card Types** for more information.
- **Card Status**: the status of the selected card, not the cardholder: **Active**, **Inactive**, **Returned**, **Lost**, and **Damaged**.

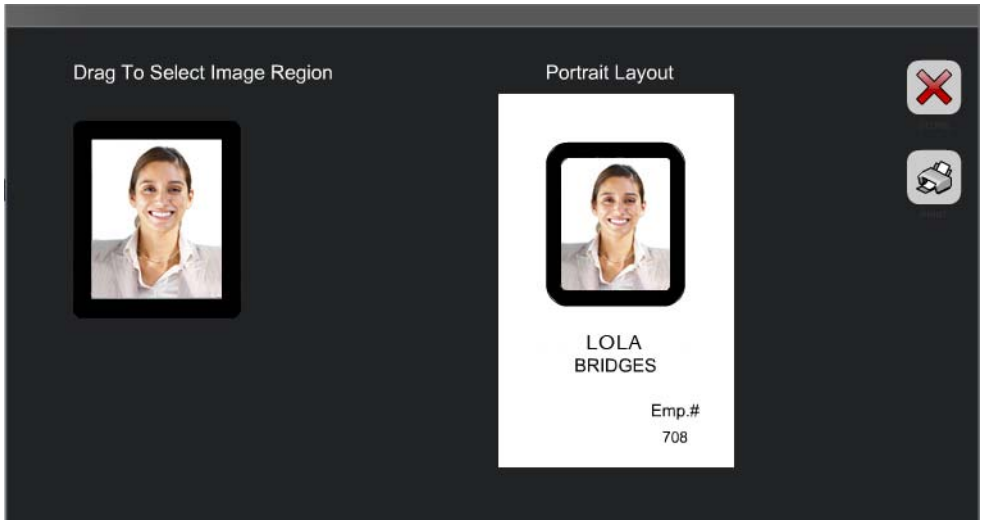
  When set to **Active**, the card can be used to open doors according to the access level assigned in the **Access Levels Tab**. All other designations disable the card.

Important: A cardholder can be active in the system and have deactivated cards.

A cardholder can have five (5) card can be active at one 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.

- **Import Photo**: brings up a file browser used to locate and load a JPEG photo of this cardholder. The recommended size is 640px high x 480px wide, with a preferred resolution of 300 dpi.
- **Print Card**: prints the selected card to a supported badge printer. Drag the border around the photo to center it properly.



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 **Cards 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 **Cards Tab**, click the plus (**+**) under the Cards list. Blank **Card Details** fields are displayed.
5. Select an existing **Cardholder Type 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 **Cards Tab**.
8. Click **Save**

to keep the changes.
   – Click **Cancel**

to restore the previous settings.

18.4.3.3 ACCESS LEVELS TAB

Up to 128 Access Levels can be assigned to a cardholder 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 window 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.

Important: Access Levels are assigned to the active card if a cardholder has multiple cards.

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.

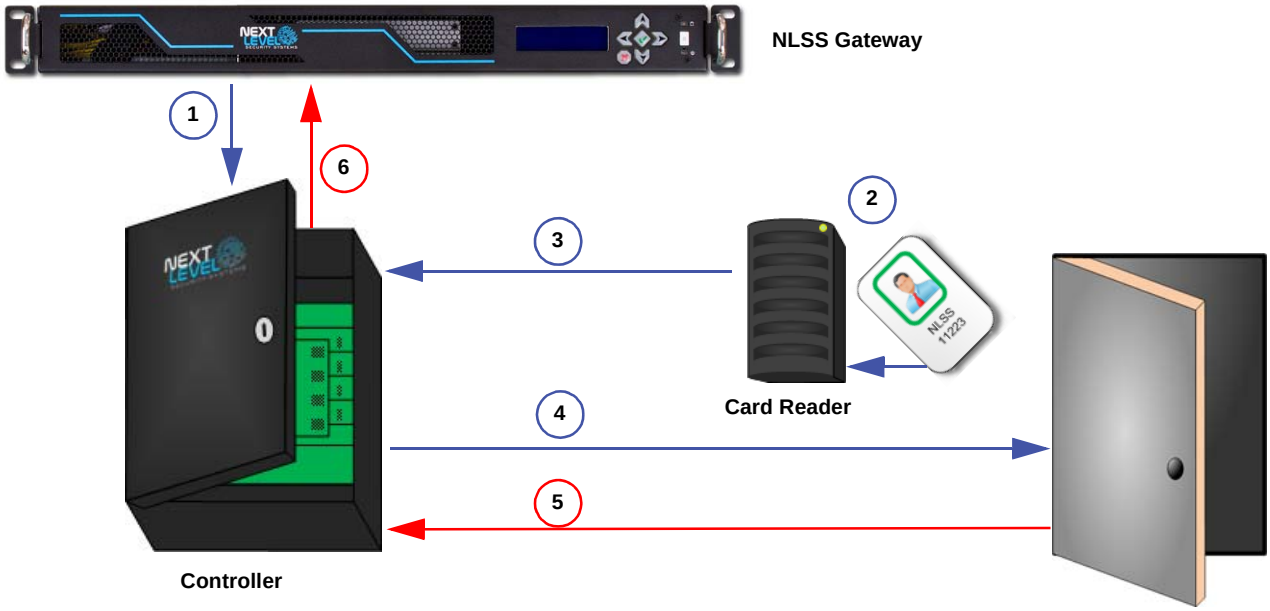
© 2009-2014 Next Level Security Systems, Inc.

Chapter 19: Configure Access Control

Access Control is a premium feature providing management of access devices and related hardware via the NLSS Gateway, and the Unified Web Interface.

Access Control is enabled via a Subscription ID. See **Configure Subscriptions** in **Chapter 17: Global Configurations** for instructions on enabling a premium feature.

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 18: 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 15: Monitoring and Handling Events**.

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

Access control devices must be configured in the following order.

1. **Configure Controllers**
   – **Configure Elevator Control** (if applicable)
2. **Configure Reader Interfaces**
3. **Configure Readers**
4. **Configure Doors**
5. **Configure I/O Interfaces**
6. **Configure I/O Linkages**

19.1 CONFIGURE CONTROLLERS

Each controller needs to be associated with one NLSS Gateway. The same controller can *not* be associated with multiple NLSS Gateways.

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 on-line, reader interfaces and readers and doors are added automatically to the Gateway. The controller, reader interfaces, reader, and door have 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.

  To set up an Assa Abloy/Sargent door lock, see the article on the NLSS Support website: **support.nlss.com**. Enter: *Programming an Assa Abloy/Sargent Door Lock* in the Search field.
- 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* window in the NLSS Web Interface.

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

© 2009-2014 Next Level Security Systems, Inc.

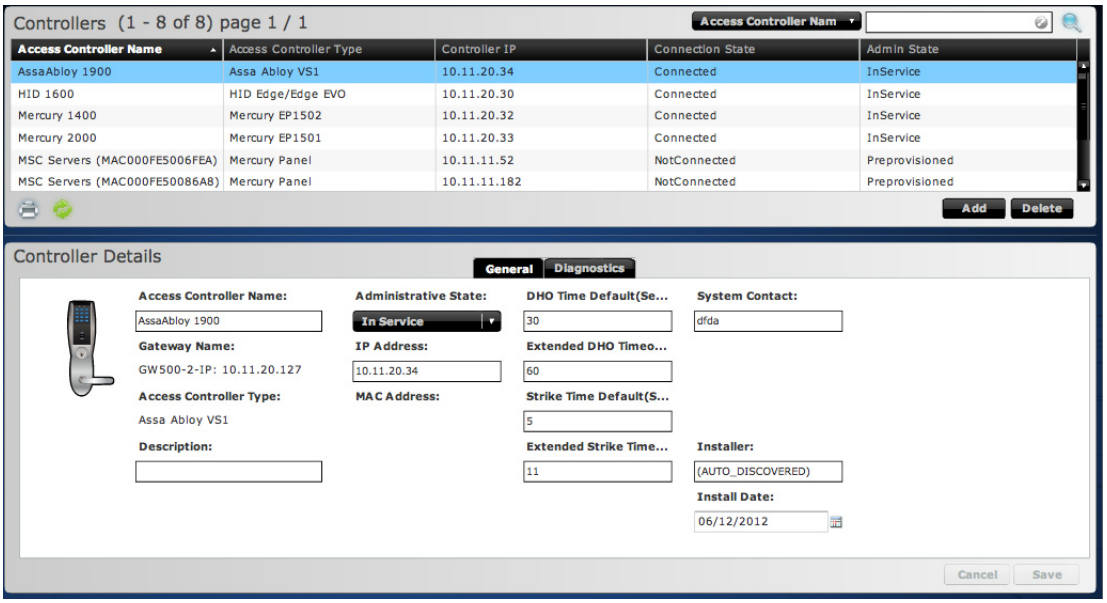
The *Controllers* window is displayed with a table listing the controllers in the system.

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 16: General Configuration Functions** for instructions.

19.1.1 Controller Details

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



19.1.1.1 General Tab

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

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

Note: Some fields 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 a controller, this drop-down list contains the 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.

© 2009-2014 Next Level Security Systems, Inc.

  - 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.
  - Axis A1001 requires the initial Username and Password to be entered in the General tab for the Gateway to establish a connection. The IP address must be entered manually.

    For instructions on setting the username and password on this device, see the Support tab on the Axis A1001 product page: **www.axis.com/techsup/access_control/a1001/index.htm**.

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 active service in the NLSS system, but does not delete its records from the system.
  - **Pre-provisioned** is the default setting when the controller has been discovered by the Gateway, but has not been placed in service.

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

1. Select the **Configuration > Access Control > Controllers >General** tab.
2. Select **Out of Service** under **Administrative State**.
3. **Save** the change.

- **IP Address**: shows the IP address of this controller. Do *not* change this value in this window.
- **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 user name 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.

© 2009-2014 Next Level Security Systems, Inc.

- **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' **General 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).

19.1.1.2 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.

© 2009-2014 Next Level Security Systems, Inc.

19.1.2 Associating a Mercury Controller with an NLSS Gateway

Mercury controllers are discovered automatically. To prevent multiple Gateways from competing over a Mercury controller, configure one Gateway to attach to that controller.

Note: These steps are also required for Mercury controllers if only one Gateway is installed in the system.

1. Log into the Web Interface for the NLSS Gateway to attached to 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. Check **Attach to Gateway** to complete the association of the controller with this NLSS Gateway.
6. 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.
7. Click **Save** to keep the changes.

   Attaching to the controller takes about *five* minutes. When done, an event message is states that the Mercury Controller is on-line and is ready to be placed *In Service*.
8. 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.
9. Click **Save** to keep the changes.

19.1.3 Putting an Axis A1001 Network Door Controller In Service

Although the Gateway automatically discovers the device, the Axis A1001 Network Door Controller's username and password must be manually to Gateway.

1. Log into the NLSS Web Interface for the NLSS Gateway to be associated with a Axis controller.
2. Select **Configuration > Access Control > Controllers** from the Main Menu.
3. Select the controller from the list at the top of the page.
4. Enter the Username and Password configured for the controller.

   See the Axis controller's documentation for instructions on setting its username, and password.
5. Click **Save** to keep the changes.

© 2009-2014 Next Level Security Systems, Inc.

19.2 CONFIGURE ELEVATOR CONTROL

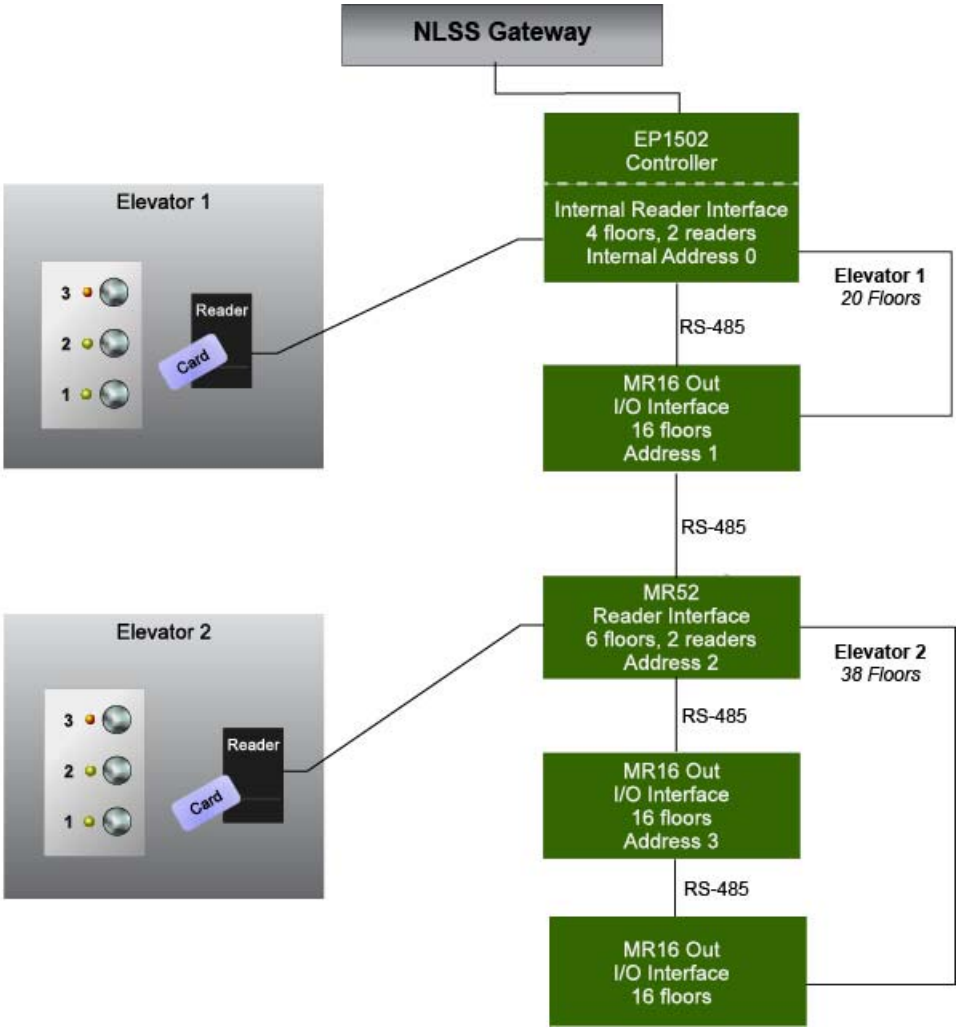
Elevator Control works similar to granting access to doors using the NLSS Gateway. Access to a floor is treated the same as setting up access to a door.

When a card is swiped in an elevator cab, and a floor button is pushed, the Gateway checks to see to which floors the cardholder is permitted access. Access is assigned through the Access Levels table in the NLSS Unified Security Suite. See **Configure Access Levels** in **Chapter 18: Configure Identity and Credentials** for more information.

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

Once a controller is on-line, reader interfaces, readers and floors are added automatically to the Gateway. The controller, reader interfaces, reader, and floors have names automatically assigned to them when they are discovered by the Gateway.

The reader in an elevator cab is connected to a reader interface. An I/O interface is connected to the reader interface via an RS-485 connection, each with its own address. The interfaces are connected to the floors to allow or deny access.



19.2.1 Configuring Elevator Control

While the Gateway automatically discovers the Controller, it must be configured for elevator control.

1. Open the NLSS Unified Security Suite interface.
2. Open **Configuration > Access Control > Controllers**.
3. Select the controller from the **Controllers** list in the top pane.
4. Select the **Special Function** drop-down menu in the **General** tab.
5. Select **Elevator Control** from the menu.
6. 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.
7. Click **Save**

to keep the changes.

   Attaching to the controller takes about *five* minutes. When done, an event message is states that the Mercury Controller is on-line and is ready to be placed *In Service*.
8. 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.
9. Click **Save**

to keep the changes.

No other settings need to be changed in this window.

19.3 CONFIGURE READER INTERFACES

When a reader interface is attached to a controller that is 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 HID and Assa Abloy interfaces are built into the controller and do not support external reader interfaces.

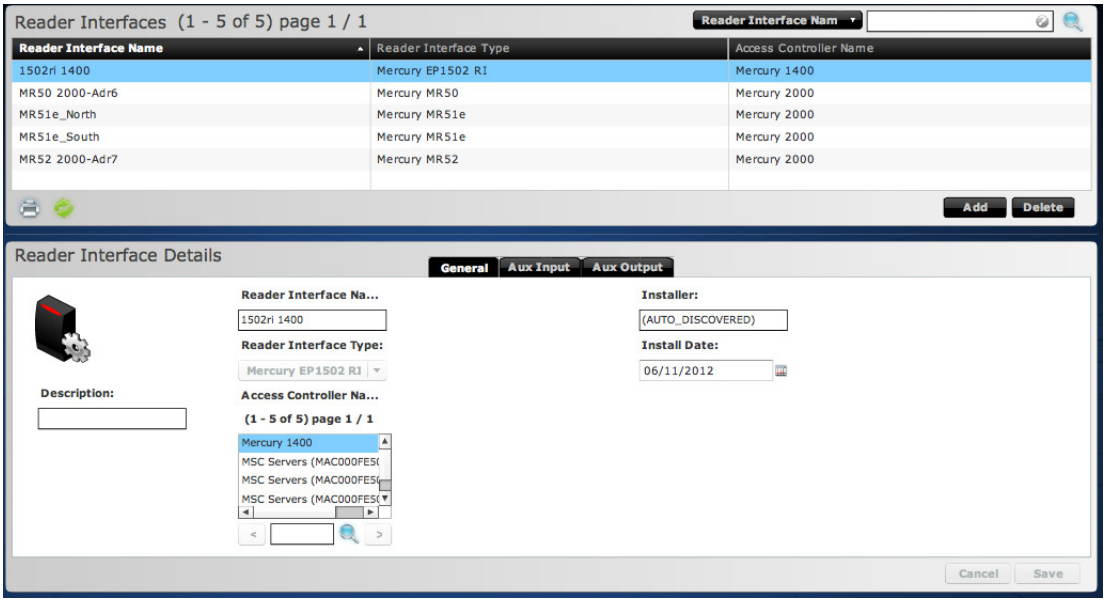
Reader Interfaces are configured from the *Reader Interfaces* window.

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

   The *Reader Interfaces* window is displayed with a list of Reader Interfaces in the system.
2. Select a Reader Interface.

© 2009-2014 Next Level Security Systems, Inc.

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 16: General Configuration Functions** for instructions.

19.3.1 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.

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.

19.3.1.1 General Tab

These parameters are applicable to Mercury reader interfaces only. Not all of these parameters are used by all Mercury controllers.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

- **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 to which this reader can 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 entered 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 these switches are set, 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:

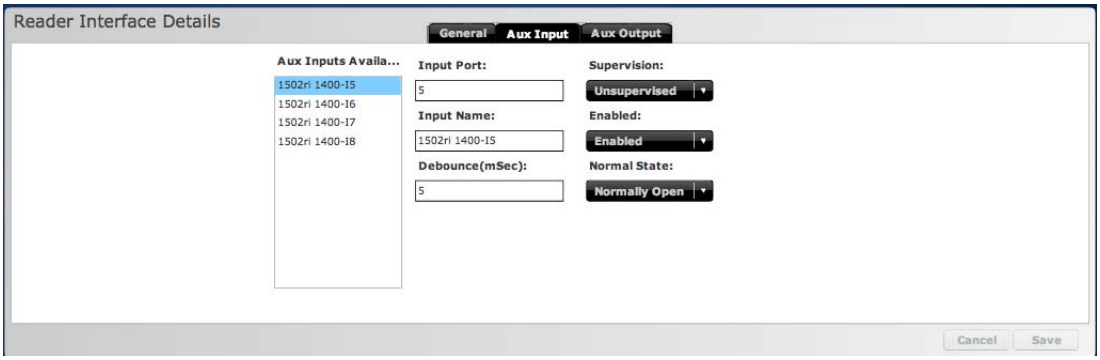
  - Inputs 1 and 3 are dedicated to the Door Contact for doors 1 & 2, respectively.
  - Inputs 2 and 4 are dedicated to doors 1 & 2, respectively.

    (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.

© 2009-2014 Next Level Security Systems, Inc.

19.3.1.2 AUX INPUT TAB

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

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

- **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).

19.3.1.2.1 Reader Interface Inputs

The inputs vary between reader interfaces. Supported reader interfaces include:

- **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.

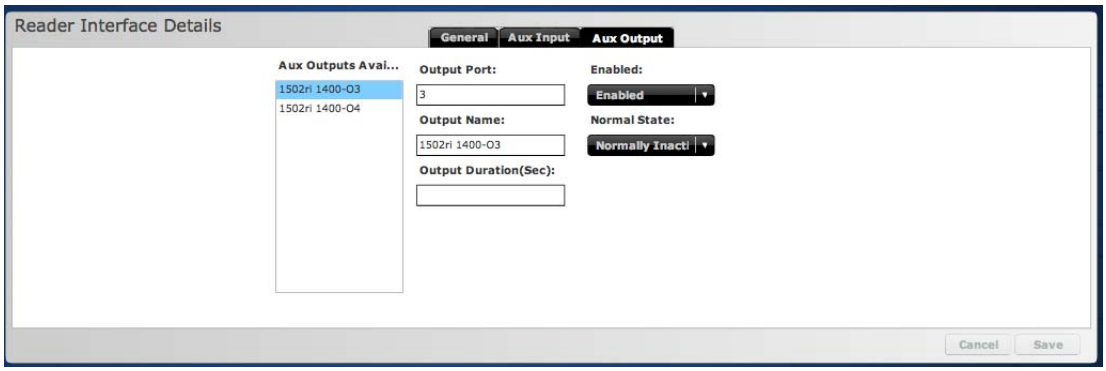
© 2009-2014 Next Level Security Systems, Inc.

- 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.

19.3.1.3 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**. Enter the port where the connection was made.
- **Output Name:** give this output device a unique name.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

- **Output Duration**: enter a length of the output signal, in seconds. If left blank, the signal remains on until it is deactivated in Operations > Output Devices.
- **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**.

19.3.1.3.1 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.

© 2009-2014 Next Level Security Systems, Inc.

– Outputs 3, 4 and 5, 6 are the spares for doors 1 & 2 respectively.

19.3.2 Adding and Deleting Reader Interfaces

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.

19.3.2.1 Add Reader Interfaces Manually

For the Mercury MR51e:

1. In the *Configuration* > *Access Control* > *Reader Interfaces* window, 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.

19.3.2.2 Delete Reader Interfaces

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

1. In the *Configuration* > *Access Control* > *Reader Interfaces* window, 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.

© 2009-2014 Next Level Security Systems, Inc.

19.4 CONFIGURE READERS

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

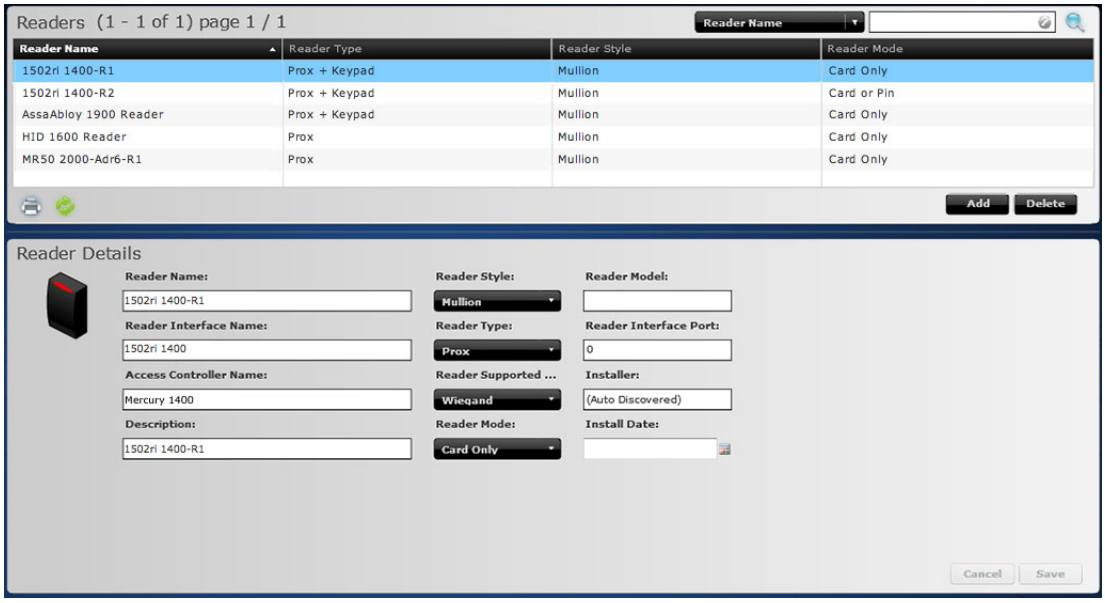
When a controller/reader interface is added to a system, the Readers table is automatically populated in the *Configuration* > *Access Control* > *Readers* window.

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

   The *Readers* window is displayed listing the readers in the system.

2. Select a Reader.

   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 16: 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.

19.4.1 Reader Details

The Reader Details pane fields differ slightly between different reader types. The Aux Output tab is only applies to HID readers.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

- **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.

© 2009-2014 Next Level Security Systems, Inc.

- **Access Controller Name**: select a controller from the drop-down list to associate with the reader.
- **Description**: optional description of this reader.
- **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 **Cards 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**: enter a port number 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. Click the **Calendar** to enter the reader's installation date.

© 2009-2014 Next Level Security Systems, Inc.

19.5 CONFIGURE DOORS

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

19.5.1 Gateway Capacities

The number of doors that can be connected to an NLSS Gateway depend on the Gateway being used.

NLSS Gateway	Sargent/Assa Abloy Wi-Fi	Sargent/Assa Abloy PoE	HID Edge EVO	Mercury
GW-500-2	0-16	0-16	0-16	0-16
GW-3000	16-64	16-64	16-64	16-64
GW-4000	64-256	64-256	64-256	64-256
GW-5000	-	-	256-1024	256-1024

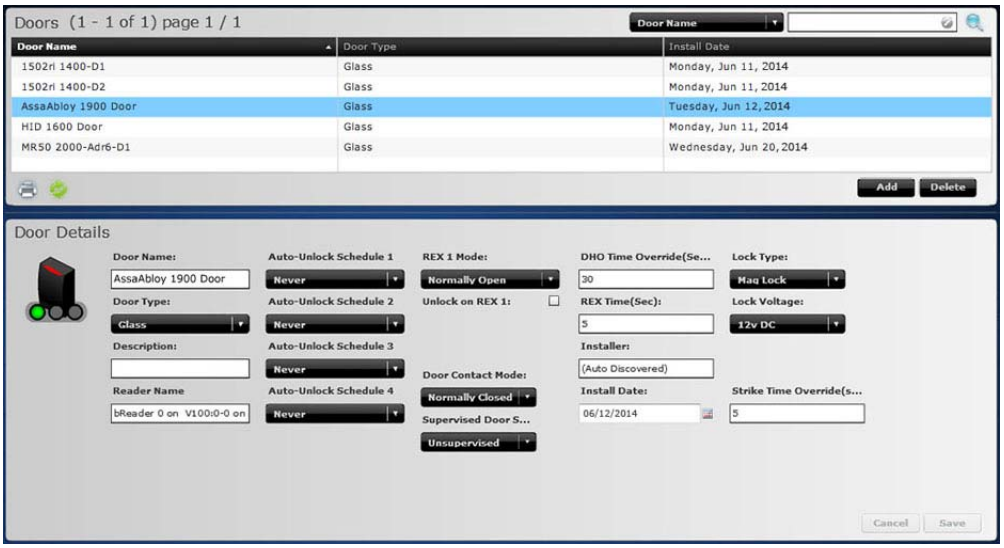
19.5.2 Adding and Maintaining Doors

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

   The *Doors* window 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 16: General Configuration Functions** for instructions.

© 2009-2014 Next Level Security Systems, Inc.

Notes:

- Configure schedules *before* associating schedules with doors or other items in the system that uses schedules. See **Configure Schedules** in **Chapter 17: Global Configurations** for instructions.
- Holidays can override schedules associated with doors. See **Configure Holidays** in **Chapter 17: 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.

19.5.3 Door Details

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

- **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**.
- **Description**: optional text box to enter a description of this door, such as its location.
- **Reader Name**: from the drop-down list of readers available in the system, select the reader that is physically associated with this door.
- **Auto Unlock Schedule 1/2/3/4**: a drop-down list of configured schedules. See **Configure Schedules** in **Chapter 17: Global Configurations** for more information.
- **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.
- **Door Contact Mode**: from the drop-down list, select whether the door is **Normally Open** or **Normally Closed**.
- **Supervised Door Setting**: a drop-down list with two options: **Supervised** or **Unsupervised**.
- **DHO Time Override (Sec)**: select a *door held open* value only to override the default DHO value set in the **Configure Controllers** window.
- **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.
- **Lock Type**: from the drop-down list, select the type of lock used on this door, such as **Mag Lock**, **Electric Lockset**, etc.

© 2009-2014 Next Level Security Systems, Inc.

- **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** window. *Strike Time* is the time, in seconds, that a door remains unlocked after receiving an unlock signal.
- **Failure Mode**: (AssaAbloy only) select either **Fail Safe** or **Fail Secure** from the drop-down list.
  - **Fail Safe**: if power is lost, the door is unlocked for entering and exiting.
  - **Fail Secure**: if power to the door is lost, the door is locked from the outside, but is unlocked inside to allow people to exit. Without power, a key must be used to unlock the door from the outside. Card or keypad access is disabled without power.

19.6 CONFIGURE I/O INTERFACES

I/O Interfaces boards extend the input and output capabilities of a controller. Mercury-based systems can be configured with multiple MR16 input and output interface boards. The MR16In allows 16 inputs and 2 outputs while the MR16Out has no inputs and allows 16 outputs.

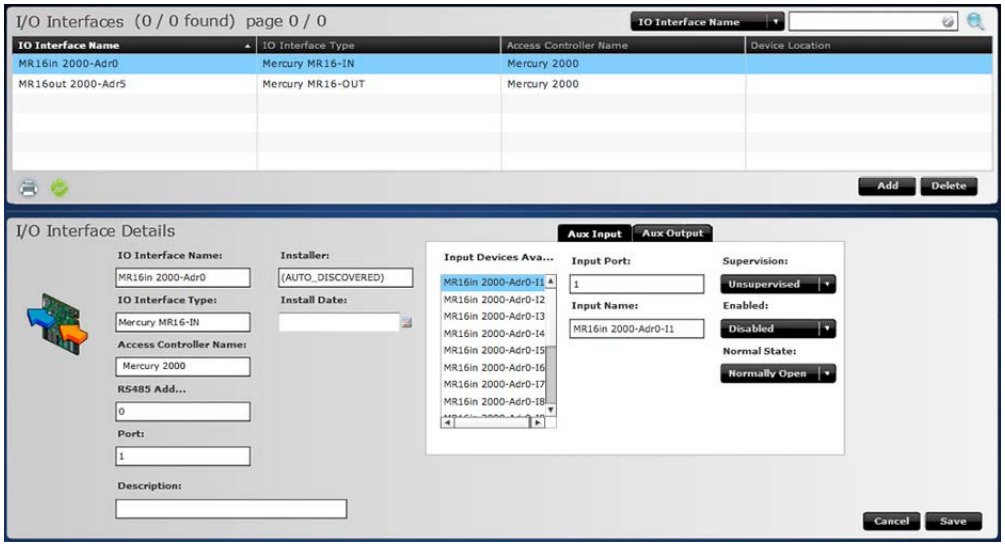
Some Mercury reader interfaces have extra inputs and outputs for general purpose use. Configuration of these I/O interfaces varies, based on the capabilities of the parent controller and the specific I/O device. This section includes general instructions for most configurations.

1. Select **Configuration > Access Control > I/O Interfaces** from the Main Menu.

   The *I/O Interfaces* window 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 16: General Configuration Functions** for instructions.

19.6.1 I/O Interface Details

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

19.6.1.1 I/O Interfaces: General Parameters

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

- **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.
- **Port**: this field is automatically populated.
- **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.

19.6.1.2 I/O Interface Details: Aux Input Tab

The Auxiliary Input tab lists the available input points. When an input device is selected, the remaining fields in the tab are used to configure that input.

The **I/O Interfaces: General Parameters** must be configured and saved before the input settings are configured.

- **Input Devices Available**: a list of physical input ports on the selected I/O device. External devices can be connected to these ports. After a port is selected, configure the remaining fields for that port.
- **Input Port**: a text field identifying the port selected in the list of **Input Devices Available**.

© 2009-2014 Next Level Security Systems, Inc.

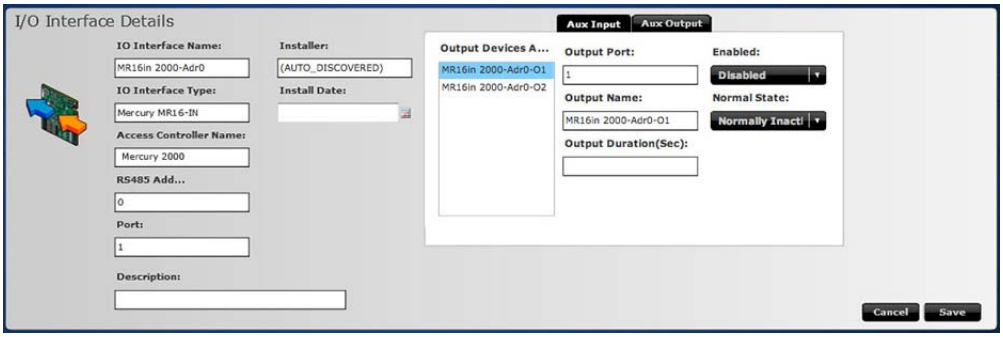
- **Input Name**: a text field to provide a descriptive name for the selected input port. The name can indicate the type of device to which the port is connected, such as a panic button, motion sensor, etc.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

- **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.

19.6.1.3 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.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

- **Output Duration**: length of time (in seconds) an output port changes state.
  - Output durations can be up to 65,000 seconds (18 hours) for Mercury.
  - Output durations can be up to 1500 second (25 minutes) with HID.
  - If left blank, the signal remains on until it is deactivated in Operations >Output Devices.

© 2009-2014 Next Level Security Systems, Inc.

- **Enabled**: a drop-down list to activate or deactivate the port for the Output Duration time. 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.

19.7 CONFIGURE I/O LINKAGES

After **Configure I/O Interfaces** are configured, then specific input ports can be linked or associated with particular output ports on the same I/O board, or any other board with I/O inputs that is in your NLSS system.

Outputs generally follow inputs with which they are associated.

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.

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.

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.

I/O Linkages are configured after I/O Interfaces. See **Configure I/O Interfaces**.

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.

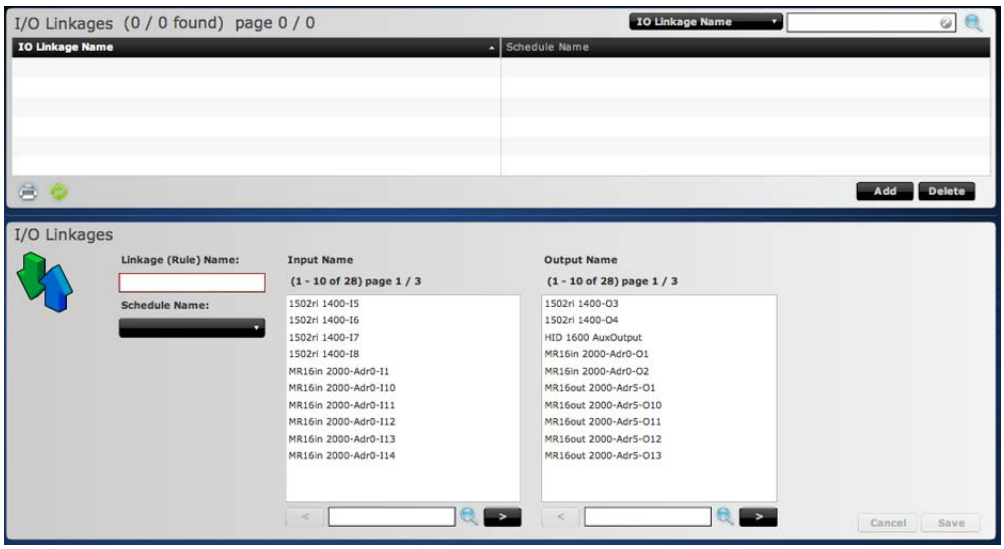
   The *I/O Linkages* window is displayed. The table at the top of the window is empty until an I/O Linkage is created.

   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.

© 2009-2014 Next Level Security Systems, Inc.

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 16: General Configuration Functions** for instructions.

19.7.1 I/O Linkages Details

- **Linkage Rule Name**: enter a unique name to identify the link.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

- **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 17: Global Configurations**.

- **Input Name**: select an input port from the 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 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.

© 2009-2014 Next Level Security Systems, Inc.

Chapter 20: Configure Video, & Storage, & Decoders

Configure video cameras and related devices in the following order:

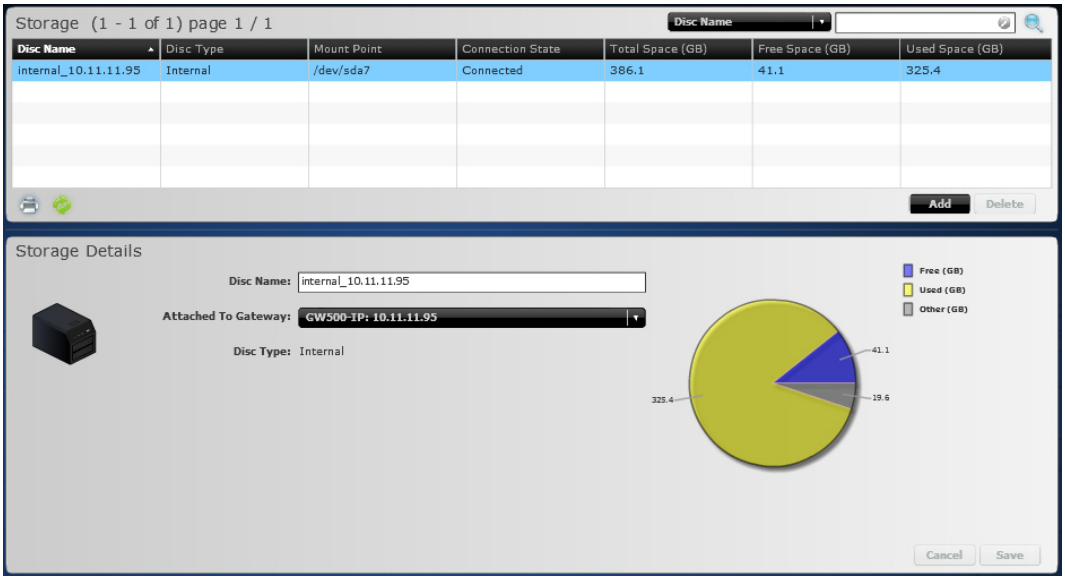
1. **Configure External Storage Devices**
2. **Configure Cameras and Streams**
3. **Configure NLSS HD Decoders**

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 level.

20.1 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* window. 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* window.

The NLSS Gateway supports: iSCSI and NFS.

20.1.1 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, Editing and Deleting Items** and **Searching Tables** in **Chapter 16: General Configuration Functions** for instructions.

20.1.2 Storage Details

- **Device Name**: a text field to enter a custom name for the device.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

- **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.

© 2009-2014 Next Level Security Systems, Inc.

20.1.3 Adding Storage Devices

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

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

20.1.3.1 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** Save to keep the change.
      » Click **Cancel** Cancel to restore the previous setting.

20.1.3.2 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, 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** Save to keep the change.
      » Click **Cancel** Cancel to restore the previous setting.

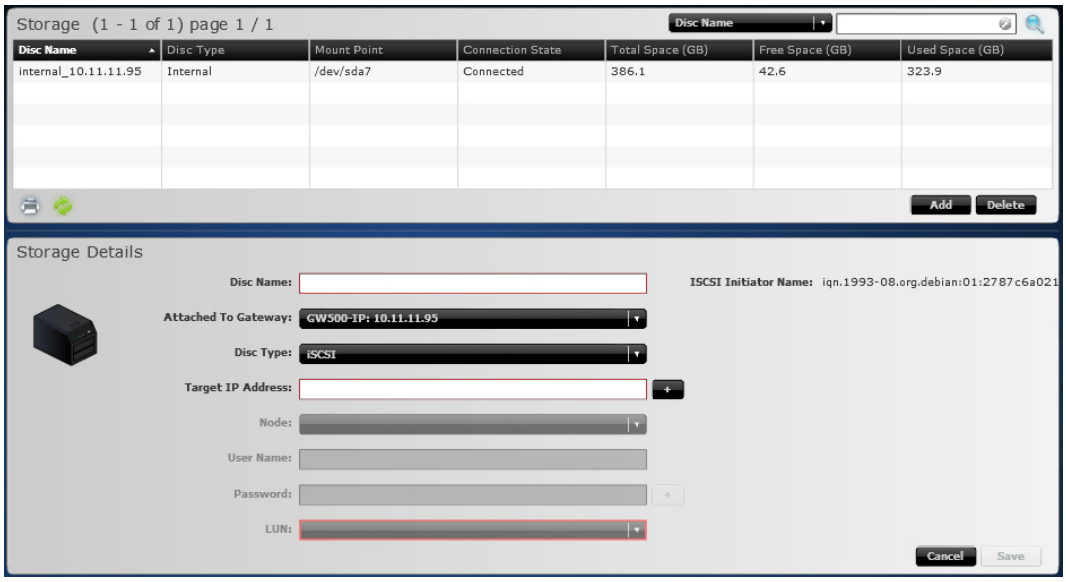
20.1.3.3 iSCSI Storage Devices

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

   A blank *Storage Details* pane is displayed.
2. Enter a **Disc Name**.

© 2009-2014 Next Level Security Systems, Inc.

3. Select **iSCSI** from the **Device Type** drop-down list. Additional fields are displayed.



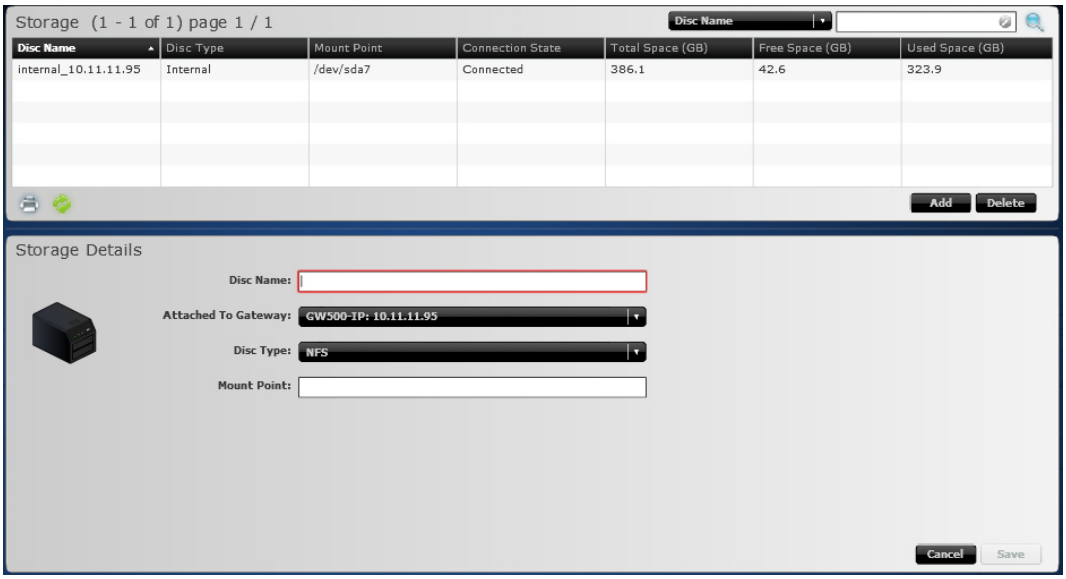
4. Enter the **Target IP Address**.
5. Click plus (**+**) next to the Target IP Address field.
   The Gateway locates the device on the network.
6. Select a **Node** from the drop-down list.
7. Enter a **User Name** and **Password** to access the disc.
   These credentials must have read-write access.
8. Select the **LUN** from the drop-down list.
9. Click **Save** to keep the change.
   – Click **Cancel** to restore the previous setting.

20.1.3.4 NAS Storage Devices

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

© 2009-2014 Next Level Security Systems, Inc.

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.

20.2 CONFIGURE CAMERAS AND STREAMS

The NLSS Gateway discovers cameras and lists them in the *Configuration* > *Video* > *Cameras* window.

Two dependencies must be configured before cameras and streams:

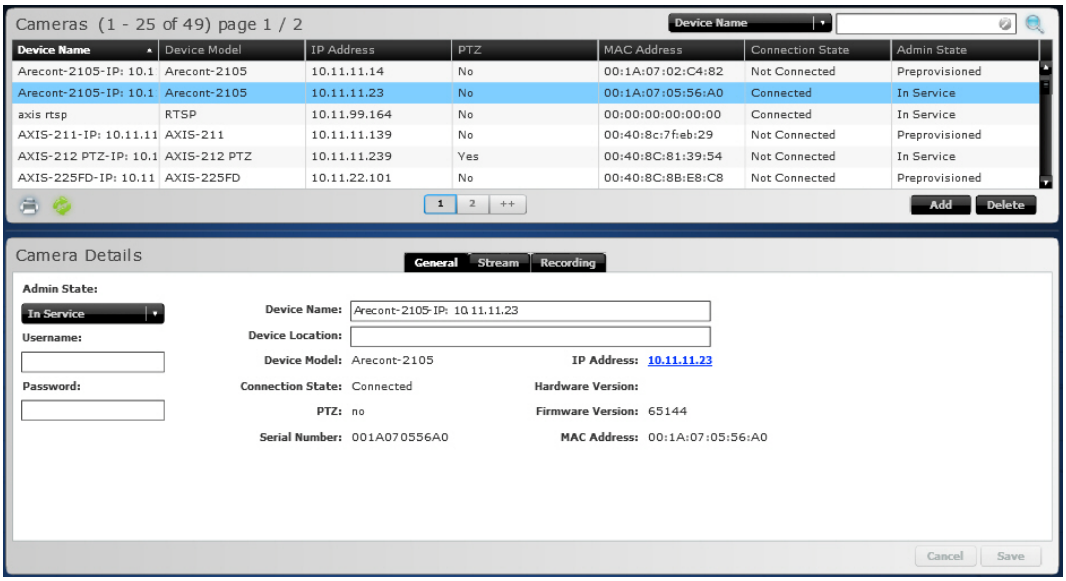
- Schedules must be configured before associating schedules with cameras streams or anything else in the system that uses schedules. See **Configure Schedules** in **Chapter 17: Global Configurations**.
- Holidays do *not* override schedules associated with cameras and other video streams.

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.

© 2009-2014 Next Level Security Systems, Inc.

The *Cameras* table is displayed.



2. Select a camera from the table.
3. To activate a camera for the Gateway, select **In Service** from the **Admin State** drop-down menu. See **Camera Details General Tab** for more information.

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 16: General Configuration Functions** for instructions.

20.2.1 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* window, a series of parameters appear in the Camera Details' General tab, even if the camera is not currently connected to the system.

20.2.1.1 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.

    The Admin State must be manually changed to *In Service* to connect the Gateway to the camera.

© 2009-2014 Next Level Security Systems, Inc.

  - **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.

    If a camera goes off line, its Admin State remains set to *In Service*, but its Connection State changes to *Not Connected*. If plans are to keep the camera off line, then change the Admin State to *Out of Service*. If a camera is physically removed, the camera can be deleted from the list.

  - **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 user name 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.

Important: The Username and Password *must* be entered in the NLSS Web Interface.

If that password has been changed on the camera, it must be updated in the interface to allow the Gateway to communicate with the camera.

Do *not* leave these fields blank.

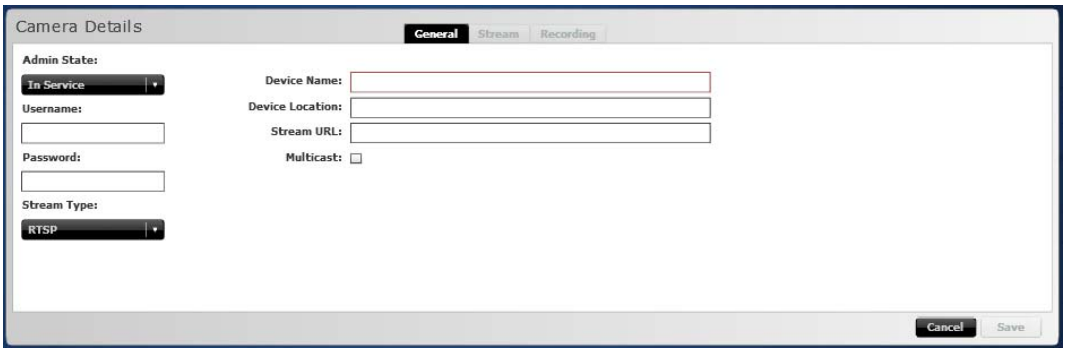
- **Device Name**: the system provides a default name, constructed when the camera is discovered. This default name includes the model and IP address of the selected camera. This default name can be kept or customized in this field.

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

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

20.2.1.1.1 Stream-only Parameters

If a stream is added or selected, additional fields must be configured.



- **Custom Stream Type**: a drop-down list with three options: RTSP, HTTP, Encoders.
  - **RTSP**: applies to remote streams using the Real-Time Streaming Protocol.
  - **HTTP**: applies to remote streams running over HTTP.

– **Encoders**: applies to streams running through a supported encoder.

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

- **Use Multicast**: (*RTSP only*) Enable for this stream to use multicast; disable to use unicast.
- **Stream URL**: (*HTTP and RTSP*) Enter the URL of the source for the stream.

Important: Without the URL, the stream cannot connect to the system.

A different set of fields is used to connect to an encoder:

- **IP Address**: the encoder's IP address.
- **Port**: the port to open on the Gateway to allow the stream.
- **Manufacturer**: select the maker of the encoder.
- **Device Model**: select the model number for the desired encoder.

20.2.1.2 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.

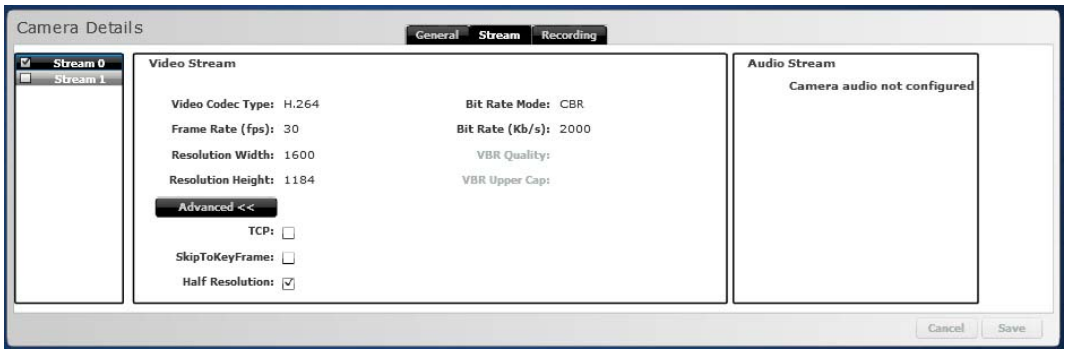
20.2.2 Camera Details Stream Tab

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.

© 2009-2014 Next Level Security Systems, Inc.

3. Open the **Stream** tab.



The Stream tab contains three sections:

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

20.2.2.1 List of Streams

Some cameras have multiple outputs, each with a different codec and/or resolution. For example: Stream 0 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**.

20.2.2.2 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.

© 2009-2014 Next Level Security Systems, Inc.

- **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 the 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- Variable Bit Rate)
- **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 Save any changes made to these settings.

20.2.2.3 Audio Stream Parameters

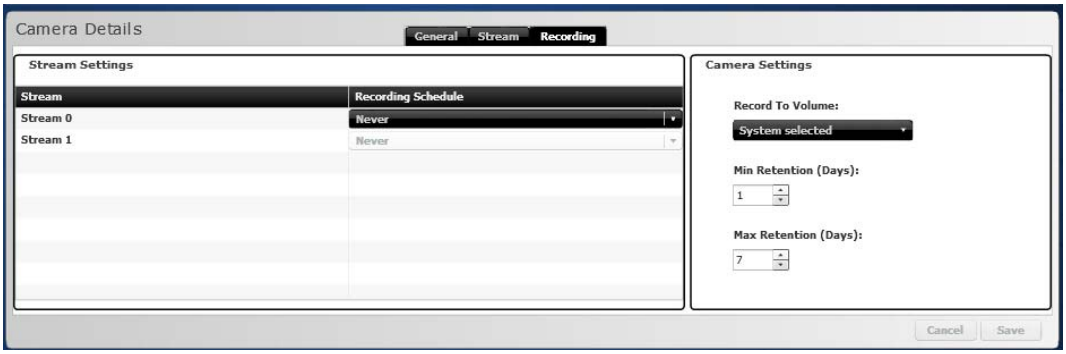
If a camera is capable of audio, then these read-only parameters are displayed.

- **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 between the camera and Gateway.

20.2.3 Camera Details Recording Tab

The Recording tab is available only after the 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.

20.2.3.1 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 17: Global Configurations** for more information on Schedules.

After a stream is enabled in the Stream tab, link 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.

20.2.3.2 Camera Settings

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

Note: These settings override the default Groomer settings. See **Configure Groomer Settings** in **Chapter 17: Global Configurations**.See**Configure Groomer Settings** in **Chapter 17: Global Configurations** for more information.

- **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. Select **Min Retention** and **Max Retention**, as described in **Camera Settings**.
2. 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.
3. Click **Save** to keep the settings.
   – Click **Cancel** to restore the previous settings.

© 2009-2014 Next Level Security Systems, Inc.

20.2.4 Cameras Actions

The *Configuration* > *Video* > *Cameras* window 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 16: General Configuration Functions** for instructions.

20.2.4.1 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.

Important: A camera's user names and passwords are set locally at the camera, *not from the NLSS Web Interface*. Check with the 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's Admin State to the *Out of Service*.
   - Click **Cancel** to abort the configuration and reset the fields to the previous values.

20.2.4.2 Add RTSP and HTTP Streams

Generic RTSP and HTTP video streams can be added to the system. Streams from encoders also can be added to the camera list.

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.

20.3 CONFIGURE NLSS HD DECODERS

NLSS HD Decoders in the same network are discovered when the NLSS Discovery Utility is run when installing the Gateway. These decoders are listed in the NLSS Web Interface. Decoders also can be added manually.

For details on NLSS decoders, see the *NLSS HD Decoder (DC-400, DC-400-2, DC-500): User Manual* available at **www.NLSS.com**.

20.3.1 Decoder Table

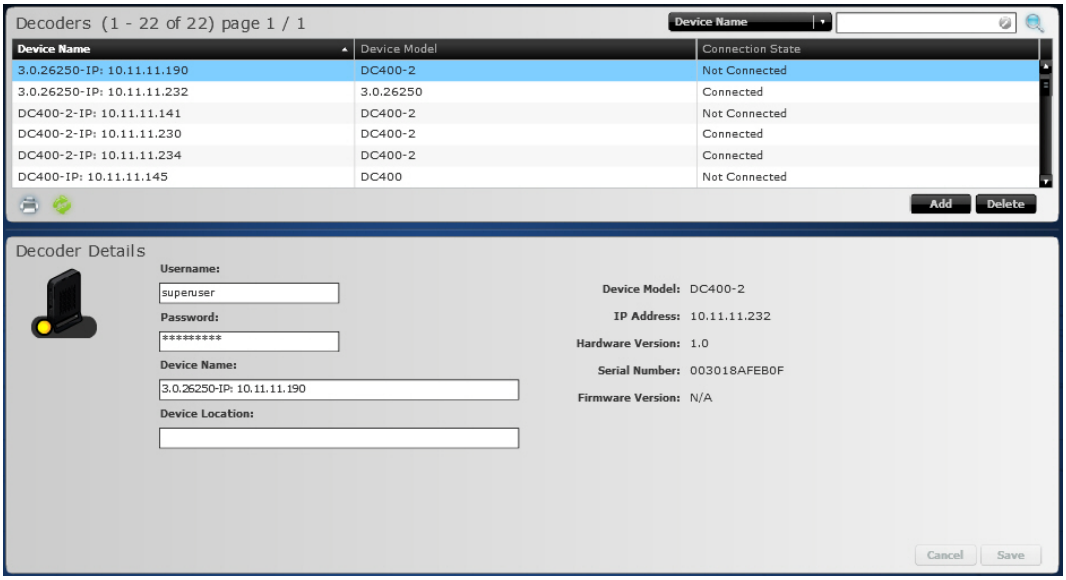
The Decoder table provides an overview of the decoder.

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 16: 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.

© 2009-2014 Next Level Security Systems, Inc.

20.3.2 Decoder Details

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

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

20.3.2.1 Editable Parameters

The decoder's user name and password are set on the decoder itself, via its own interface. See the *NLSS HD Decoder User Manual* for instructions.

- **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.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

- **Device Model**: select the model number of the NLSS HD 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.

20.3.2.2 Read-Only Parameters

- **Device Model**: the model of this decoder, such as GW-5000.
- **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.

© 2009-2014 Next Level Security Systems, Inc.

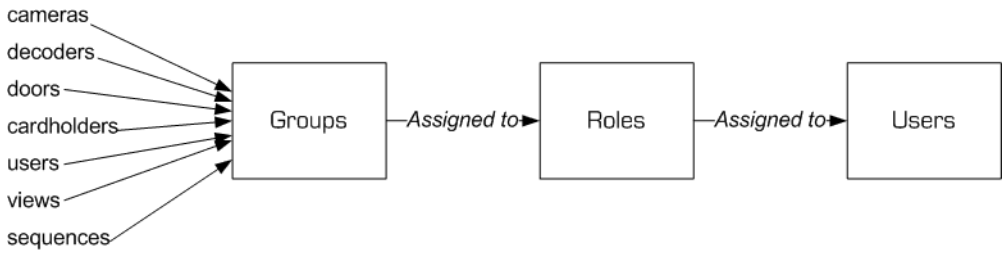
Chapter 21: Configuring Permissions

Permissions determine to which features an NLSS Web Interface user has access. 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.



21.1 APPLYING PERMISSIONS EXAMPLE

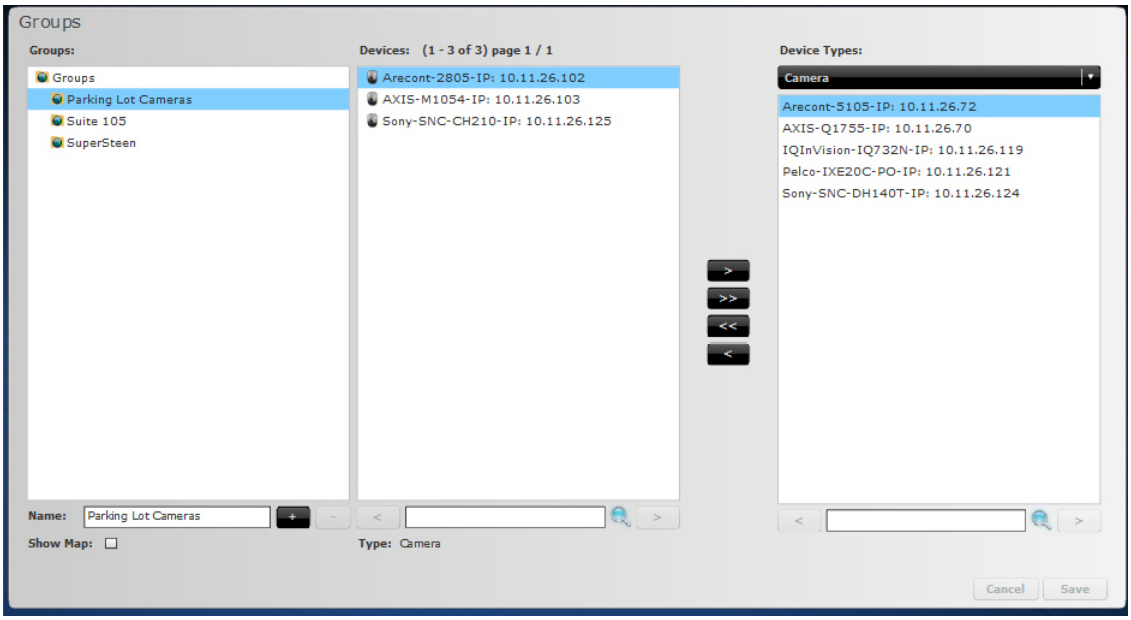
A parking lot security guard may only need to view video and related events covering the parking lot. However, this user does not need access to create Views or Sequences, or access to Doors, Cardholder/User, and Reporting windows.

Use the Configurations > Permissions options to set up this user.

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

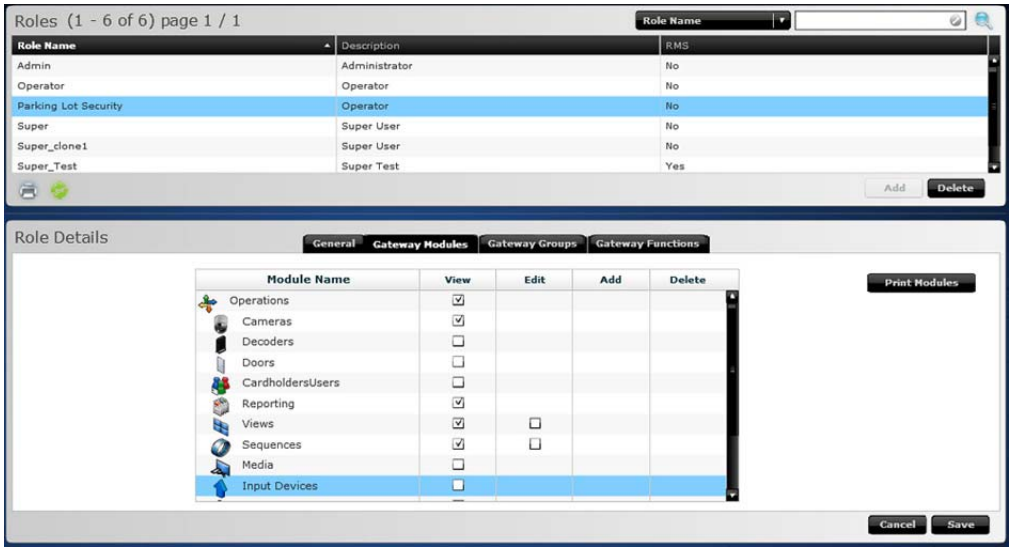
1. Open **Configuration > Permissions > Groups**.
   a. Create a group called *Parking Lot Cameras*.

b. Add the desired cameras, views and sequences.



See **Groups** for instructions.

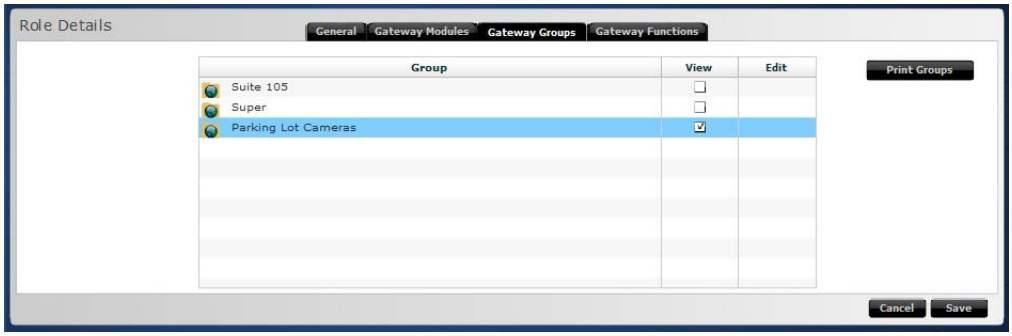
2. Open **Configuration > Permissions > Roles**.
   a. Create a clone of the Operator role, and name it *Parking Lot Security*.
   b. In the Gateway Modules tab for the cloned role, disable View permissions for all Operations options, *except* for Cameras, Views and Sequences.
   c. Disable Edit permissions for Views and Sequences. This steps also removes Add and Delete abilities from these options.



By default, the Operator has no Configuration permissions.

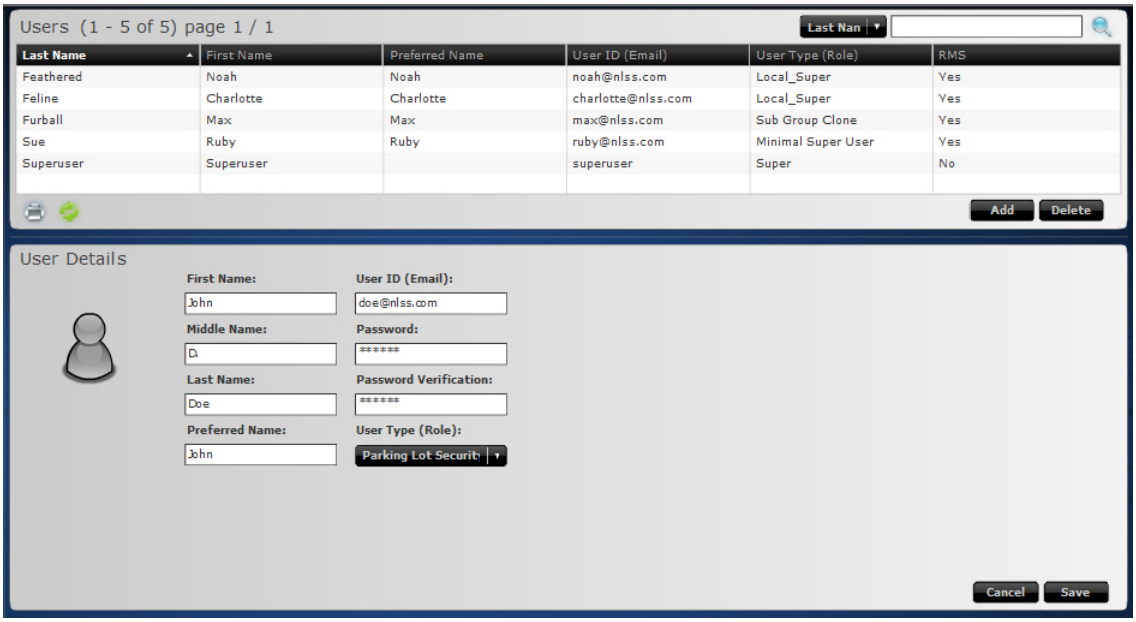
Top level permissions must be disabled before permissions configured by groups can be applied.

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



See **Roles** for instructions.

3. Open **Configuration > Permissions > Users**.
   a. Create a new user.
   b. Select the User Type (Role) of *Parking Lot Security*.



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 view the events associated with these cameras.

21.2 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 have different types of objects contained 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.

Groups can be created, edited and deleted. Maps or other JPEG images, such as floor plans, can be used as a background. The Device lists can be searched.

21.2.1 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.

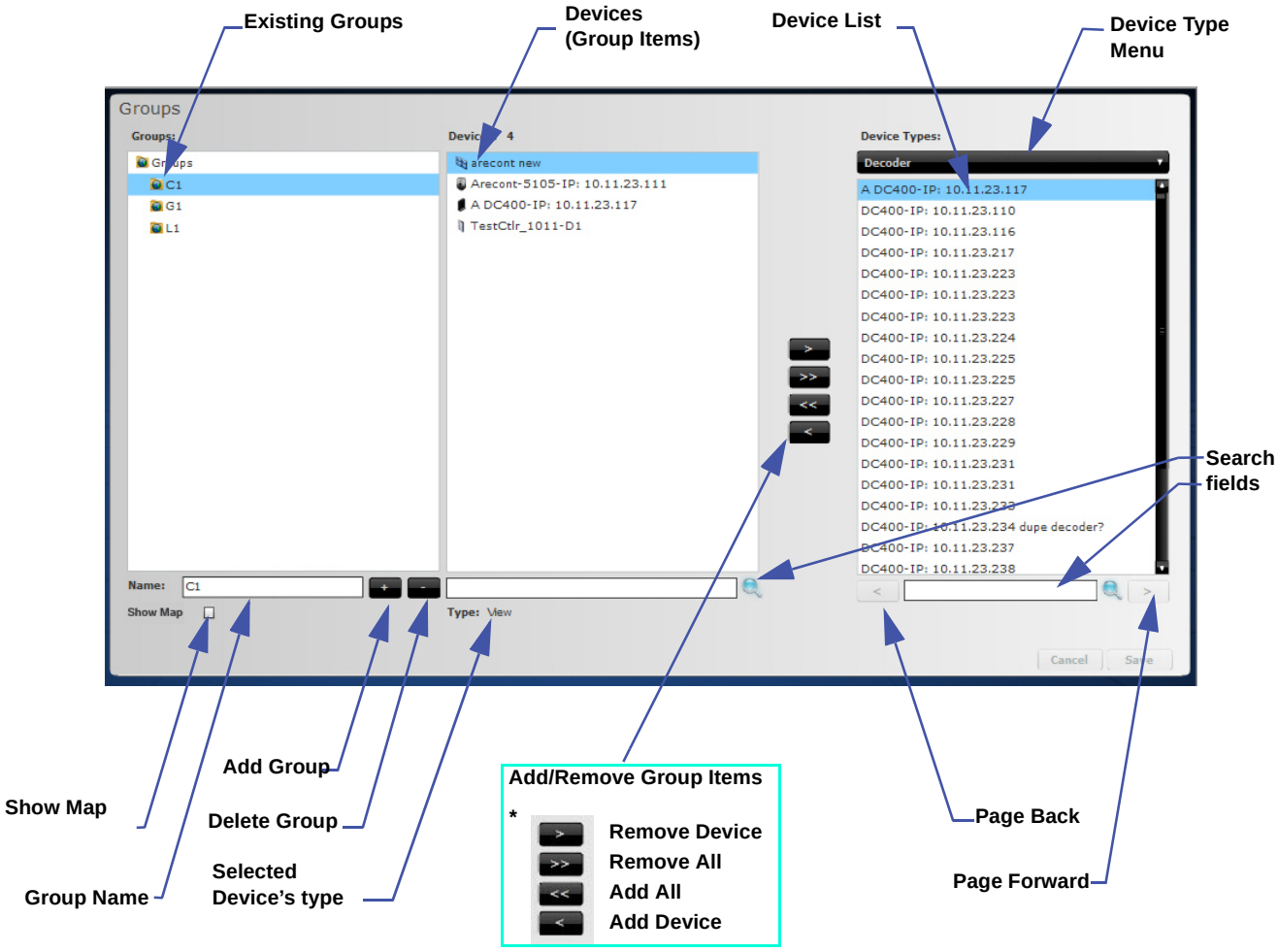
Users are then assigned that role.

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.

© 2009-2014 Next Level Security Systems, Inc.

21.2.2 Groups Window

Groups are created and maintained from **Configuration > Permissions > Groups**.



21.2.3 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**.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

© 2009-2014 Next Level Security Systems, Inc.

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 14: 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.

21.2.4 Edit a Group

1. Click **Configuration > Permissions > Groups**.
2. Select a **Group**.
3. Edit the **Group Name**, if desired.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

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.

21.2.5 Delete a Group

1. Click **Configuration > Permissions > Groups**.
2. Select a **Group**.
3. Click **Delete Group** (**-**).

© 2009-2014 Next Level Security Systems, Inc.

4. Click **Yes** to confirm the deletion when prompted.
   – Click **No** to stop the deletion and keep the group.

21.3 ROLES

Roles define the capabilities of the users operating the NLSS Gateway. The *Configuration > Permissions > Roles* window provides capabilities to manage roles.

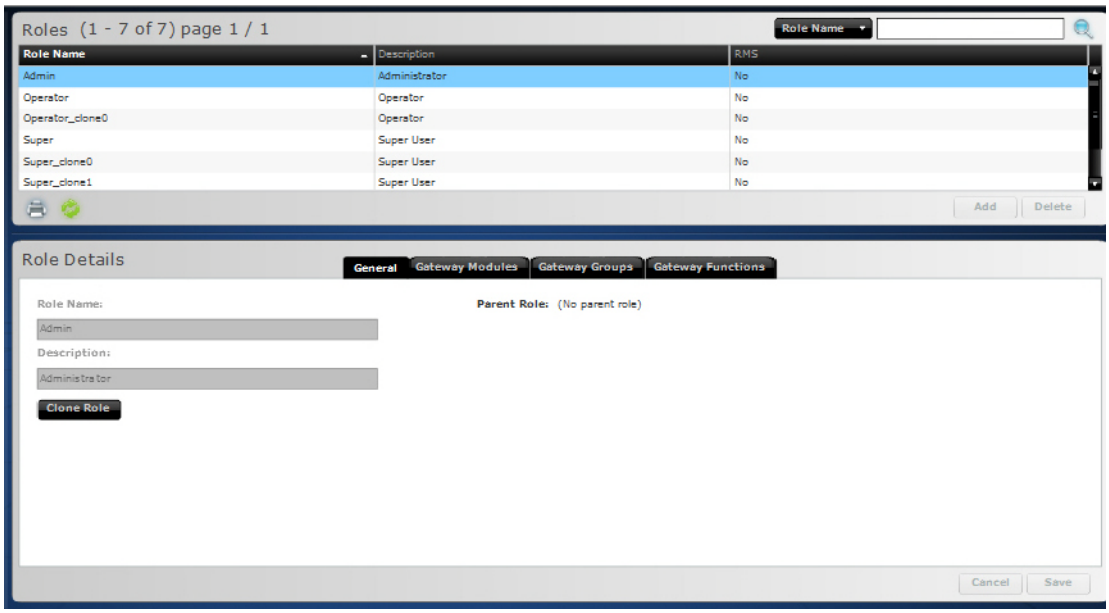
If a Gateway is managed via RMS, roles are configured at the RMS level, not at site level.

1. Select **Configuration > Permissions > Roles** from the Main Menu. Access the Configuration menu from the *Sites* window, if running RMS.

   The *Roles* window is displayed listing the default and created (cloned) roles.

2. Select a role.

   The *Roles Details* pane is displayed.



The NLSS Gateway has four pre-defined roles, three of which are available at the local Gateway level. These default roles cannot be edited or deleted.

- **Superuser**: the *root* or Primary User of the Gateway. The Superuser has full access to all menus and features in the NLSS Web Interface. This role can be cloned to create similar roles.
- **Administrator**: run and modify features under the Configuration menu. This role can be cloned to create similar roles.
- **Operator**: run and modify camera features under the Operations menu.This role can be cloned to create similar roles.
- **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.

© 2009-2014 Next Level Security Systems, Inc.

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 16: 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.

21.3.1 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.

Permissions to menu options are set in the **Gateway Modules Tab** for cloned (added) roles. Permissions cannot be changed for the default roles

- **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. If Delete is not checked, the Edit and Add options remain available.

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.

21.3.1.1 General Tab

The General tab allows a role to be identified and cloned.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

- **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.

© 2009-2014 Next Level Security Systems, Inc.

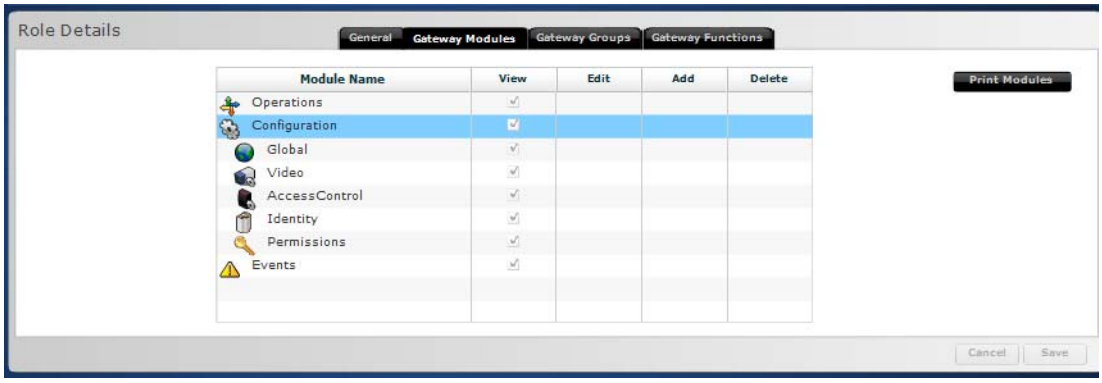
- **Clone Role**: click this button to create an editable copy of the selected role. Default and created roles can be cloned.
- **Parent Role**: the role from which the selected role was cloned.

Click **Save** to keep any changes to cloned roles, or **Cancel** to return the fields to their previous settings.

21.3.1.2 Gateway Modules Tab

Modules are the top level options selected from the Main Menu: Operations, Configuration, and Events. Cloned (added) role permissions for the modules are set in this tab. This tab is also accessed through the **Configuration > Permissions > Roles** window 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.



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.

© 2009-2014 Next Level Security Systems, Inc.

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 Types, Cardholder Types, 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*

© 2009-2014 Next Level Security Systems, Inc.

Default Role	Operations Module Options	Configuration Module Options	Events Module
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 Types, Cardholder Types, Cardholders: *View, Edit, Add, Delete* – Cardholder - User Defined: *View, Edit* – Permissions: *View, Edit, Add, Delete for all options*	*View*

21.3.1.3 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*

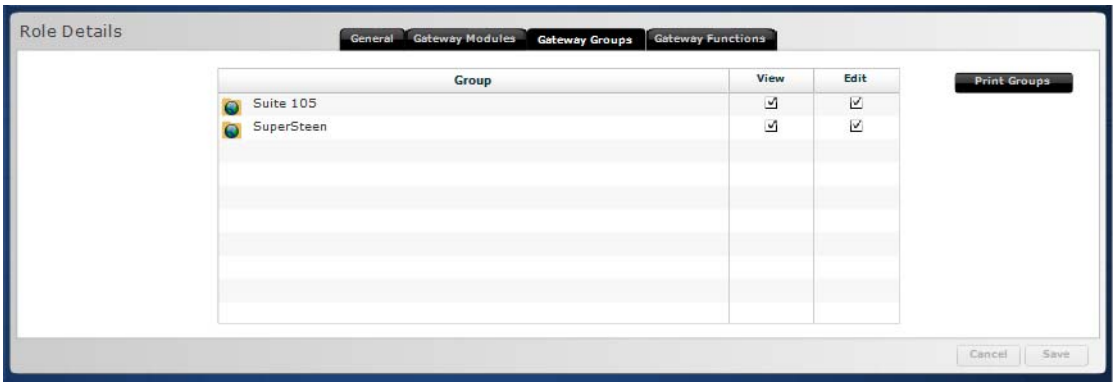
This tab is labeled as **RMS Groups** at the RMS level.

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.

© 2009-2014 Next Level Security Systems, Inc.

3. Open the **Gateway Groups** tab.



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.

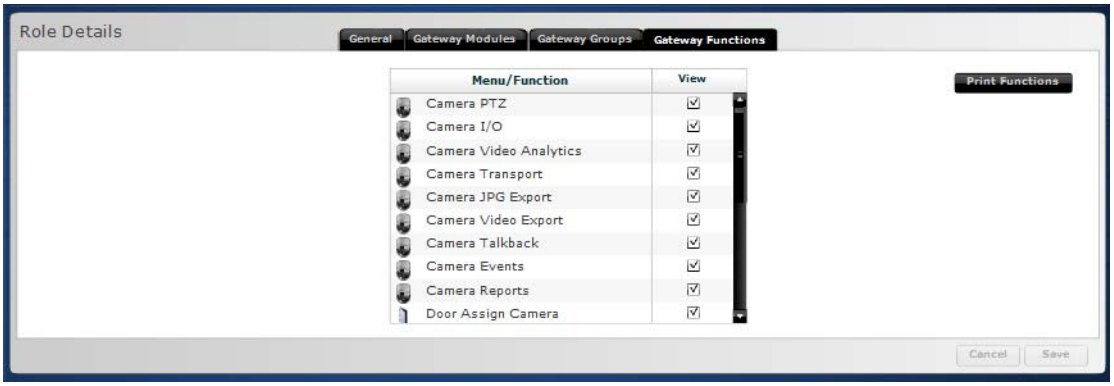
21.3.1.4 GATEWAY FUNCTIONS

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.



4. Click the **View** check box to enable (checked) or disable (unchecked) a desired permission.

Note: Enabling *Camera Talkback* also enables the ability to play audio through a camera

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.

21.3.2 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 Role**.
4. Edit the tabs, as needed.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

5. Click **Save** to keep the clone.
   – Click **Cancel** to delete the clone without saving.

21.3.3 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.

© 2009-2014 Next Level Security Systems, Inc.

21.4 USERS

Users are the people monitoring, administering, and maintaining the security system through the NLSS Web Interface.

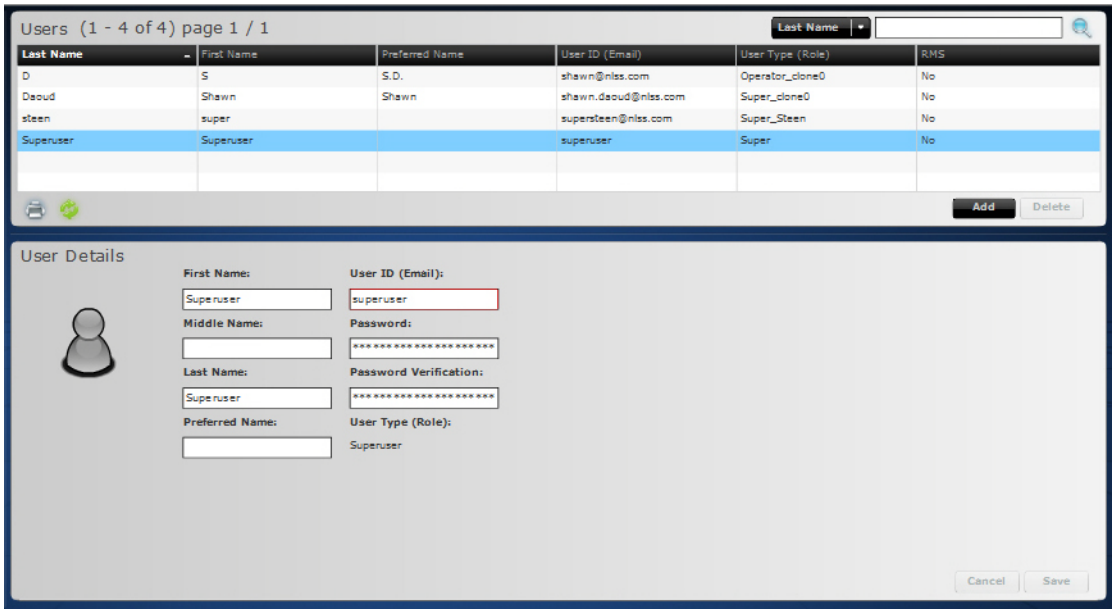
If a Gateway is managed via RMS, users are configured at the RMS level, not at the local Gateway level.

1. Select **Configuration > Permissions > Users** from the Main Menu. Access the Configuration menu from the *Sites* window, if running RMS.

   The *Users* window is displayed listing the users.

2. Select a user.

   The *User Details* pane is displayed.



Default users are included with the NLSS Gateway. The roles of the same name can only be applied to these users.

- **Superuser** (Gateway only): 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.

Users can be added, edited, searched and deleted. See **Adding, Editing and Deleting Items** and **Searching Tables** in **Chapter 16: General Configuration Functions** for instructions.

Note: The Master and Superuser *cannot* be deleted, and their roles cannot be changed. Their names, passwords, and email address can be edited.

21.4.1 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 a new user. The Superuser and Operator roles only are applied to the default users of the same name.

  See **Roles** for more information.

© 2009-2014 Next Level Security Systems, Inc.

PART 4: PREMIUM FEATURES

Additional features are available for accessing and managing NLSS Unified Security Suite.

- **Chapter 22: Configuring and Using Face Recognition** - captures faces from video and compares the image to those stored in a database on the NLSS Gateway.
- **Chapter 23: Configuring and Using License Plate Recognition** - provides instructions for configuring License Plate Capture and License Plate Recognition.
- **Chapter 24: Configuring Audio Analytics** - provides instructions for configuring audio analytics for cameras equipped with microphones.
- **Chapter 25: Configuring and Using Intrusion Detection** - provides instructions to configure the NLSS Unified Security Suite to gather information from intrusion detection systems.
- **Chapter 26: Configuring and Using Point of Sale** - records cash register transactions, and associates them as events with live and recorded video available through an NLSS Gateway.
- **Chapter 27: NLSS Remote Management Services** - provides configuration and operations instructions for RMS. If a Gateway is controlled through *Remote Management Services*, or *RMS*, many configuration settings are done at the RMS level.
- **Chapter 28: Next Level Mobile Application** - provides instructions for using the NLSS interface features available through a tablet or smartphone using the NLSS Mobile App.
- **Appendix A: Performance and Setup Guidelines: Video Analytics, Face Recognition, and License Plate Recognition** - provides additional information for optimizing the Video Analytics, Face Recognition, and License Plate *Recognition* features. Performance details are also discussed for these features.

© 2009-2014 Next Level Security Systems, Inc.

Chapter 22: Configuring and Using Face Recognition

Face Recognition is an add on Video Analytic. When the Face Recognition Video Analytic is activated for a camera, it grabs a picture of a face, and generates a *Face Captured* event.

The image is then compared to images stored in the *Face Pool*. The Face Pool images are either imported from external files or added from the cardholders database on the Gateway.

Each Gateway contains its own Face Recognition database. The database lists the people to be recognized, along the identifying pictures for matching.

People are grouped in the Face Recognition database. A group is assigned to a camera to enable Face Recognition for that camera.

Important: A group must be assigned to a camera. If a group is not assigned, Face Recognition defaults to run as Face Capture.

The *Face Captured*, *Face Recognized*, and *Face Match Group* events are displayed in the Event Log. Standard event functions are available, including filtering, playing the video clip of the event, acknowledgment, etc. See **Chapter 15: Monitoring and Handling Events** for more information.

These events can be linked to specific actions using an Event Linkage. See **Configure Event Linkages** in **Chapter 17: Global Configurations** for instructions.

Face Capture and Face Recognition are configured and run at the local Gateway level, on a per camera basis. Before using Face Recognition:

- Enter a token in *Configuration* > *Global* > *Subscriptions* to enable Face Recognition. See **Enabling Other Premium Features** in **Chapter 17: Global Configurations** for instructions.
- Configure Face Recognition for the Gateway from *Configuration* > *Face Recognition*, as described in this chapter.
- Configure and run the analytic for a camera or video stream. See **Running the Face Recognition Analytic** for instructions.

Note: Face Capture runs within Face Recognition. If Face Recognition is not running, Face Capture can be run on its own. See **Face Capture** in **Chapter 5: Operations with Video Analytics** for instructions.

The database is loaded into the Gateway through the Configuration module to speed configuration of Face Recognition. However, the files for the database must meet the following specifications.

22.1 DATABASE SPECIFICATIONS

The database is built from a zipped file containing a *.csv* file and an image folder. The zipped file is imported to the Gateway to create Face Recognition groups. See **Importing a Database** later in this chapter for instructions on downloading a template for the contents of the zip file, and adding database contents to the Face Recognition database.

22.1.1 .csv File

The *facialrecognition_configuration_template.csv* file lists the people for the database. Each instance of this file in the database defines a Face Recognition group. The .csv file must have the following columns, in this order, to identify the people in the database:

- **groupName**: one group per .csv file.
- **userSuppliedID**: the unique identifier for each person.

  Use only alpha-numeric characters, with no special characters (_, -, ., #, etc.) and no spaces.
- **firstName**
- **middleName**
- **lastName**
- **preferredName**
- **description**

Important: The .csv file is limited to 5000 entries. Any entries past 5000 are not processed when the file is imported into the Gateway.

Multiple .csv files can be imported with the same GroupName. However, when the database entries on the gateway for that group reach 5000, any additional entries in the imported .csv file are ignored.

Note: Cardholders are automatically added to the Face Pool, so they do not need to be added via a .csv file. Each time a new cardholder is added, that person's name and image are added to the Face Pool.

22.1.2 Images Requirements

The images must meet the following criteria to be used for Face Recognition.

- The images folder must contain JPEG (*.jpg)* images to be associated with the people in the database.
- Size: up to 5 MB

© 2009-2014 Next Level Security Systems, Inc.

- Limit: Up to 10 images can be associated with a person.
- Naming: *userSuppliedID.jpg*, with a *-x* to identify multiple pictures of the same person. For example, if the userSuppledID for a person is NLSS01, then that person's images would be labeled as NLSS01.jpg, NLSS01-1.jpg, NLSS01-2.jpg, etc.

Note: The file name extension, .jpg, must be in lower case.

Also, duplicate images are ignored and will not be uploaded, even if the image files have different names.

Important: Ensure that all images match up with a userSuppliedID. Persons listed in the .csv file without a matching primary image trigger an error during the upload.

- Frontal face image (face looking forward) with a neutral expression (regular expression).
- The eyebrows, eyes, nose and mouth must be uncovered. No sunglasses or hats.

See **Photograph Guidelines** in **Appendix A: Performance and Setup Guidelines: Video Analytics, Face Recognition, and License Plate Recognition** for more information.

22.2 IMPORTING A DATABASE

Import the zip file containing the database components through the Configuration module.

1. Log into the NLSS Unified Security Suite Web Interface for a local Gateway.
2. Select **Configuration > Face Recognition > Management**.

   The *Face Recognition Management* window is displayed.

3. Click **Import/Export**.

The *Import/Export Face Recognition* dialog box is displayed.

– A **Sample Template** of the .csv file can be downloaded from this dialog box by clicking **Download** under the Import button.

4. Click **Import**.

   The *File Uploader* dialog box is displayed.

5. **Browse** to select a zip file.

6. Click **Upload**.

Note: If an error occurs while importing a .zip file, check the **Import Log** by clicking **Download** at the top of the dialog box.

The contents of the .zip file are added to the Face Recognition database on the Gateway. The people in the .csv file are placed in the group listed in that file. The images named with their userSuppliedID are assigned to that person.

The people are placed in a Face Pool in the database. These people can belong to multiple groups. People listed in database can be added to other groups created within the *Configuration* > *Face Recognition* > *Groups* window.

Important: The Face Recognition video analytic must be restarted after the Face Pool is updated.

22.3 FACE RECOGNITION GROUPS

The Face Recognition database can be partitioned into specific groups. People can be assigned to Face Recognition Groups either in the *.csv* file imported in into the database, or manually from the *Configuration* > *Face Recognition* > *Groups* page.

Face Recognition Groups are assigned to cameras that are running that Video Analytic. A group assignment narrows the database search for a match when running the analytic.

A group must be assigned to a camera to run Face Recognition. See **Running the Face Recognition Analytic**.

Using groups improves management of the database, and provides the ability to recognize a specific group of people on a per camera or deployment basis. For example, groups can be created for employees, contractors, or VIP Customers.

Note: Face Recognition groups are configured and used separately from *Permissions Groups*. Face Recognition groups are *not* used with the Configuration > Permissions settings.

© 2009-2014 Next Level Security Systems, Inc.

Face Recognition groups can be in either an *open* or *closed* environment.

- A *closed* environment contains only the people whose images are already in the database. Closed environments identify known people, such as employees, and typically have higher face recognition accuracy.
- An *open* environment exists when most of the faces to be captured are not in the database. Open environments identify specific people from a large group of unknowns.

Open and closed groups are not specifically identified in the system. The concept is useful to understand the type of group or behavior that is desired for the video analytic.

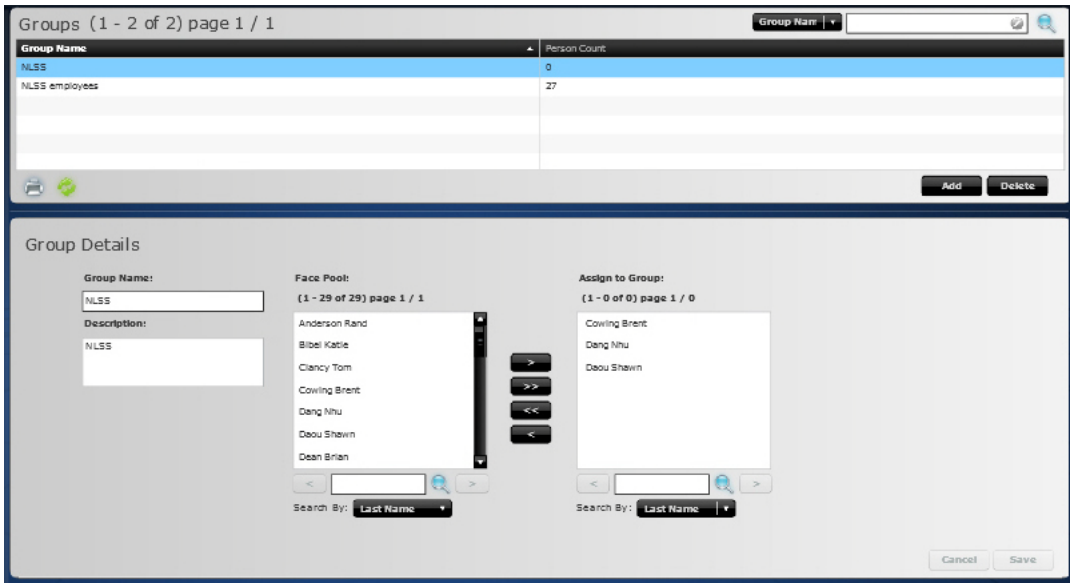
Important: Although cardholders are automatically added to the Face Pool, they must be manually added to a group to be included in Face Recognition searches.

22.3.1 Accessing Face Recognition Groups

Groups are listed and details are provided in the *Configuration > Face Recognition > Groups* window.

1. Log into the NLSS Unified Security Suite Web Interface.
2. Select **Configuration > Face Recognition > Groups**.

   The *Face Recognition Groups* window is displayed.



22.3.2 Groups Table

The Face Recognition groups are listed in the table in the top pane. The number of people in the groups is also listed in the **Person Count** field. This list can be searched and sorted by **Group Name** or **Person Count**.

22.3.3 Group Details

The bottom pane contains the Group Details for the selected group.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

- **Group Name**: editable field identifying the group.
- **Description**: optional text field.
- **Face Pool**: lists the people who have been imported into the database.
- **Assign to Group**: lists the people who can have been assigned to this group.

Note: The Face Pool and Assign to Group lists can be searched by First Name or Last Name.

When the mouse hovers over a name in the Face Pool or Assign to Group lists, a pop-up is displayed with that person's first and last name, along with a thumbnail of the person's Primary Image. See **Images Tab** for instructions on setting a Primary Image.

22.3.4 Creating a Group

1. Select **Configuration > Face Recognition > Groups**.

   The *Face Recognition Groups* window is displayed.

2. Click **Add**

in the top pane. A blank *Group Details* pane is displayed.

3. Enter a **Group Name**.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

4. Enter a **Description**.
5. Select a person in the **Face Pool**.
6. Use the right arrow (**>**) to move the person to the **Assign to Group** list.
   - Use the double right arrow (**>>**) to move all people in the Face Pool to the Assign to Group list. Remember, each group is limited to 5000 members.
   - Use the left arrows (**<**, **<<**) to remove people from the **Assign to Group** list.
7. Click **Save**

to keep the group settings.
   - Click **Cancel**

to discard the settings.

22.3.5 Deleting a Group

Deleting a group does not delete the people in that group from the Face Recognition database.

1. Select **Configuration > Face Recognition > Groups**.
2. Select a **Group** in the Groups table.

© 2009-2014 Next Level Security Systems, Inc.

3. Click **Delete** Delete in the top pane. A confirmation message is displayed.
4. Click **Yes** to delete the group.
   – Click **Cancel** to keep the group.

22.3.6 Assigning People to Groups

People can either be assigned to Face Recognition groups:

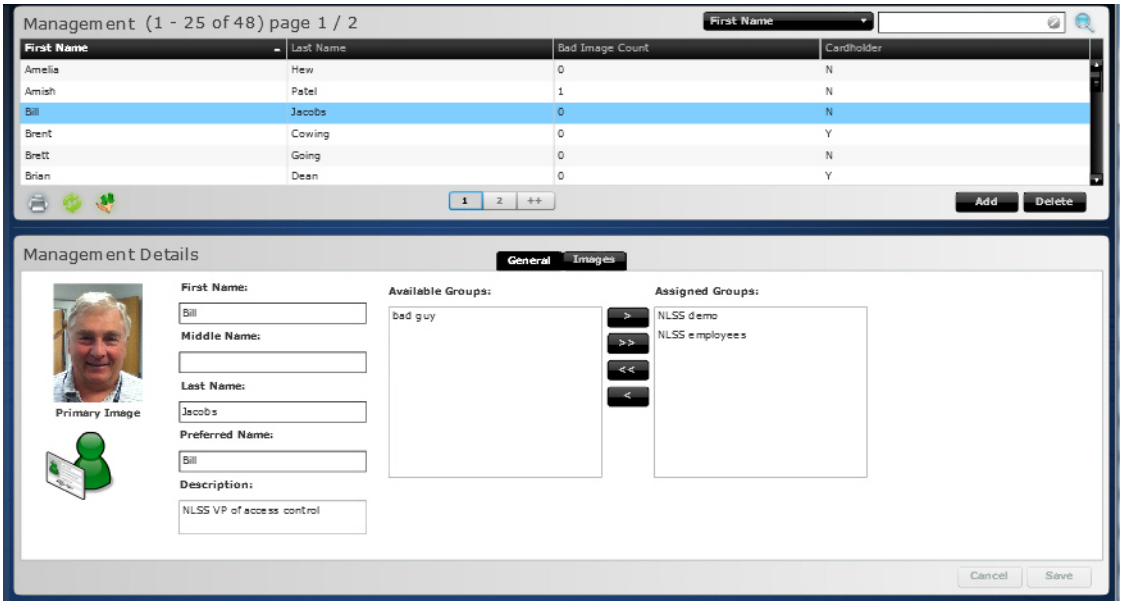
- In the .csv file.
- In the *Groups* window, as described in **Creating a Group**.
- In the *Management* window, when the person's record is edited or added. See **Updating the Management List**.

22.4 MANAGEMENT

The Management window lists the people included in the Face Recognition database. People can be either added through a database import, or individually in this window. Records also can be edited and deleted using this window.

1. Log into the NLSS Unified Security Suite Web Interface.
2. Select **Configuration > Face Recognition > Management**.

The *Face Recognition Management* window is displayed. Additional groups can be applied to people, and new images can be uploaded through this window



22.4.1 Management Table

The table in the top pane lists the people in the database. These records can be added, edited and deleted using this window. Sort the table using the column headers.

- **First Name**: The first name that was either included in the imported .csv file, or added in the Management Details pane.
- **Middle Name**: The middle name that was either included in the imported .csv file, or added in the Management Details pane.
- **Last Name**: The last name that was either included in the imported .csv file, or added in the Management Details pane.
- **Bad Image**: a count of the number of unusable images that have been imported for this person. The system can determine if the image contains a valid face for recognition, or if the image file is not in the proper format for recognition.
- **Cardholder**: Indicates if the person is a cardholder (**Y** or **N**). Cardholders are automatically added to the face recognition database. This field and the cardholder picture cannot be changed in this window. That picture can only be changed in the Credentials tab in Configuration > Identity > Cardholder. See **Cards Tab** in **Chapter 18: Configure Identity and Credentials** for more information.

  Additional pictures can be added to the face recognition database for a cardholder.

22.4.2 Management Details

The bottom pane contains the Management details to configure the records listed in the Face Recognition database.

This pane contains two tabs: **General** and **Images**.

22.4.2.1 General Tab

These editable fields contain the data entered in the .csv file that was imported. These fields can be edited when a person is selected in the Management table.

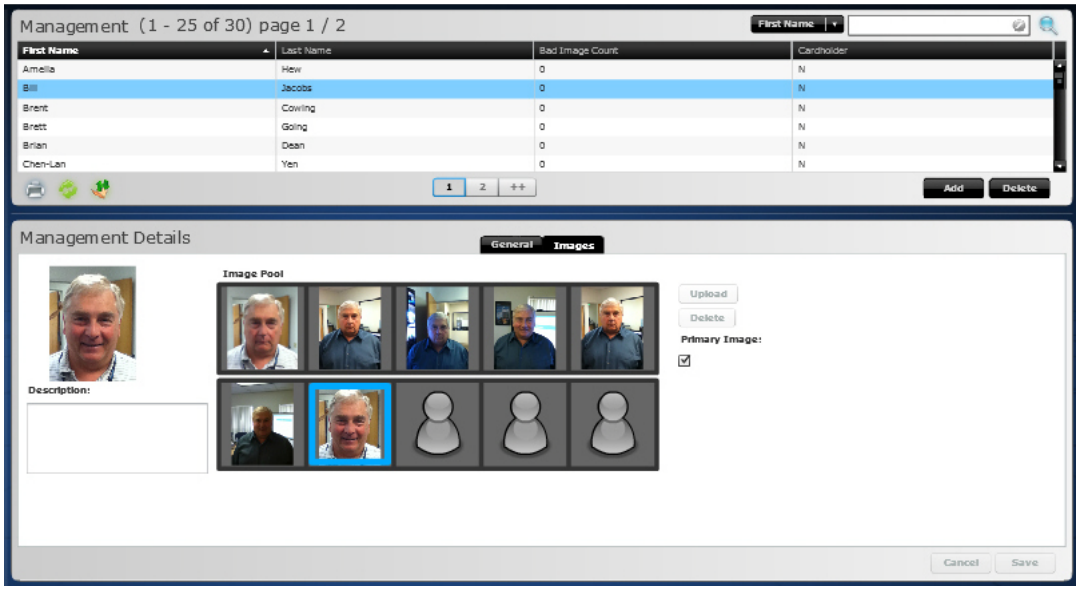
These fields are also used to create records for new people added through this window.

- **First Name**: The first name that was included in the imported .csv file, or added in this pane when an entry was added.
- **Middle Name**: (optional) The middle name, or initial, that was included in the imported .csv file, or added in this pane when an entry was added.
- **Last Name**: The last name that was included in the imported .csv file, or added in this pane when an entry was added.
- **Preferred Name**: (optional) The preferred name, such as a nickname, that was included in the imported .csv file, or added in this pane when an entry was added.
- **Description**: (optional) An text field to provided further information about the person.
- **Available Groups**: The existing groups in the Face Recognition database.
- **Assigned Groups**: The Face Recognition groups to which this person belongs.

© 2009-2014 Next Level Security Systems, Inc.

22.4.2.2 IMAGES TAB

The Images tab provides thumbnails of each image uploaded for the selected person. Images can either be uploaded in zip file with the .csv file, or added through this tab.



- **Image Pool**: up to 10 images can be uploaded for a person. The selected image is highlighted with a blue box. The gray icons are placeholders in the Image Pool.

  The Face Recognition video analytic starts with the Primary Image, then proceeds through the Image Pool for this person when a potential match is detected.

Important: Images must be the front of a face, with no hat or sunglasses, and the person's regular facial hair. By using more images, with a slightly different angle or with different lighting, result in an improved recognition rate.

- **Primary Image**: check this box to set an image as the Primary Image. The Primary Image is displayed with any Face Recognition events generated for this person.

- **Description**: an optional text field to provide more information about the selected image.

22.4.2.2.1 Upload an Image

Images can be uploaded to the Face Recognition database, but meet the system's requirements.

- To upload an image, it must be a JPEG (.jpg) file, no larger than 5 MB.

- The file name must contain only alpha-numeric characters, with no special characters (_, -, ., #, etc.) and no spaces.

Important: When importing a file through this pane, the name *must include the userSuppliedID*, as is required if the image is included in the Images folder in the .zip file imported into the database. See **Images Requirements** under **Importing a Database** for more information.

- Frontal face image (face looking forward) with a neutral expression (regular expression).
- No sunglasses or hats.
- The eyebrows, eyes, nose and mouth must be uncovered.

See **Photograph Guidelines** in **Appendix A: Performance and Setup Guidelines: Video Analytics, Face Recognition, and License Plate Recognition** for more information.

Snapshots taken by a camera in the NLSS system also can be imported into the Face Recognition Pool. For instructions on taking snapshots from the video player, see section **Export JPG** in **Chapter 4: Controlling Cameras**.

1. Open the **Images** tab in the *Configuration* > *Face Recognition* > *Management* window.
2. Select a box with a gray icon. The selected icon is highlighted with a blue box.

3. Click **Upload**.

The *File Uploader* dialog box is displayed.
4. **Browse** to select a an image file.
5. Click **Upload**.

A thumbnail of the image is added to the Image Pool.

   The Face Recognition feature analyzes the image. If the image does not contain usable facial features for recognition, or the image is not the correct format, the image is highlighted with a red box. Place the mouse over the thumbnail to display a message explaining why the image is not acceptable for Face Recognition. See **Images Requirements** for more information.
6. Add a **Description** if desired.

22.4.2.2.2 Delete an Image

If an image is bad or is not needed, it can be deleted from the Face Recognition database.

1. Open the **Images** tab in the *Configuration* > *Face Recognition* > *Management* window.
2. Select an image. The selected image is highlighted with a blue box.
3. Click **Delete**.

A confirmation message is displayed.
4. Click **Yes** to delete the image.
   – Click **Cancel** to keep the image.

Important: A Primary Image cannot be deleted. If the image needs to be deleted, first select a different image to be the Primary Image

22.4.3 Updating the Management List

People and their images can be added, edited and deleted.

22.4.3.1 Adding a Person

People can be added manually to the Face Recognition database.

Cardholders

1. Select **Configuration > Face Recognition > Management**.
2. Click **Add** in the top pane.
   A blank *Management Details* pane is displayed.
3. Enter a **First Name**, **Middle Name** (optional), **Last Name**, and **Preferred Name** (optional).
4. Enter a **Description** (optional).
5. Select an **Available Group**.
   – Use the single right arrow (**>**) to move the group to the **Assigned Groups** list.
   – Use the double right arrow (**>>**) to move all groups to the **Assigned Groups** list.
   – Use the left arrows (**<**, **<<**) to remove groups from the **Assigned Groups** list.

Note: A group does not need to be assigned to a person when the record is first created. For example, if the group to which this person will be assigned has not yet been created, that group can be added later. See **Creating a Group** instructions.

However, a group must be assigned for that person to be included when the Face Recognition video analytic is running.

6. Click **Save** to add the person to the database.
   – Click **Cancel** to discard the settings.
7. Open the **Images** tab.
8. Add images for the person, as described in **Upload an Image**.

Note: New cardholders are automatically added to the Face Pool. Additional images can be added, as described in **Editing a Person**.

22.4.3.2 Editing a Person

1. Select **Configuration > Face Recognition > Management**.
2. Select a person in the Management table.
3. Edit the **Name** fields or **Description**, if desired.
4. Update the settings for the **Available Groups** and **Assigned Groups**.
   Select a group.
   – Use the single right arrow (**>**) to move a selected group to the **Assigned Groups** list.
   – Use the double right arrow (**>>**) to move all groups to the **Assigned Groups** list.
   – Use the left arrows to remove a selected group from the **Assigned Groups** list.

© 2009-2014 Next Level Security Systems, Inc.

– Use the double left arrows (**<<**) to remove groups from the **Assigned Groups** list.

5. Click **Save** to update the record.
   – Click **Cancel** to discard the changes.
6. Open the **Images** tab.
7. Update the images as needed.
   a. Select a gray icon to **Upload** a new image.
   b. Select an image to **Delete**, or set it as a **Primary Image**.

   See **Images Requirements** for complete instructions.

22.4.3.3 Deleting a Person

1. Select **Configuration > Face Recognition > Management**.
2. Select a person in the Management table.
3. Click **Delete** in the top pane.
   A confirmation message is displayed.
4. Click **Yes** to delete the person.
   – Click **Cancel** to keep the person.

Deleting a person does not delete associated groups from the Face Recognition database.

Important: Cardholders cannot be deleted from the Face Pool. They are automatically deleted from the Face Pool if deleted from the Gateway.

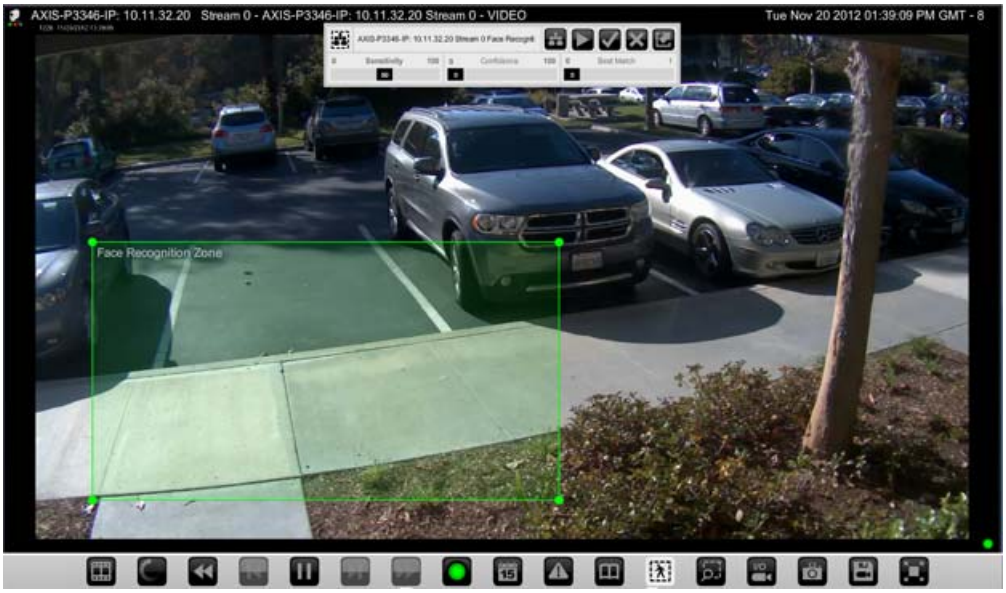
© 2009-2014 Next Level Security Systems, Inc.

22.5 RUNNING THE FACE RECOGNITION ANALYTIC

After Face Recognition is configured, the analytic can be used.

1. Click **Face Recognition** in the Video Analytics Configuration list.
2. Click **Edit**.

   The Face Recognition settings are displayed in the video player with a *Face Recognition Zone*.



3. Drag the slides to configure the analytic settings.
   a. **Sensitivity**: scale 0-100
      » A *higher* sensitivity results in a better detection rate, but also a higher false positive rate.
      » A *lower* sensitivity results in a lower detection rate, but also a lower false positive rate.
   b. **Confidence**: scale 0-100
      » A *higher* confidence setting results in fewer recognition results, but better accuracy.
      » A *lower* confidence setting results in more recognition results, but more false positives.
   c. **Best Match**: options 0 or 1
      » **1** = closest result generates an event. Enabling Best Match provides a higher recognition rate, but also higher false positive rate. A setting of 1 works best in a closed group environment where all of the people are in the Face Recognition database, such as an office.
      » **0** = generates an event if the analytic is absolutely sure of a match, per the Confidence setting. Disabling Best Match provides a lower false positive rate, but also a lower recognition rate. This setting is good for an open group or environment where not all of the people are in the database, such as an airport or train station.

© 2009-2014 Next Level Security Systems, Inc.

After the analytic is saved, a square, labeled *Minimum Face Size*, is displayed to indicate the minimum size that a face must be on the screen to be recognized by the system. This square is an indicator, and does not need to be moved.

A *Face Captured* event is generated if a valid face appears in the Face Recognition Zone. A face is considered valid if it is larger than minimum face size, is located inside the defined Face Recognition Zone, and meets the required sensitivity threshold.

4. Drag the corners of the *Face Recognition Zone* to match the area to be monitored. By default, the area is a rectangle.

Note: A *larger* Face Recognition Zone results in a *longer* detection time. Reduce the size of the Face Recognition Zone to reduce the detection time.

5. Click **Group**. This is a Face Recognition group, not a permissions group.
6. Check a circle in the pop-up list to select a group. Multiple groups can be selected.
7. Click **Save** to keep the analytic settings.
8. Click **Start** to launch the Face Recognition video analytic for this camera.
   – Click **Cancel** (**X**) to exit the edit mode without keeping the settings.

22.6 FACE CAPTURE AND RECOGNITION GUIDELINES

The following set of guidelines helps to optimize the face capture and recognition capabilities. See **Appendix A: Performance and Setup Guidelines: Video Analytics, Face Recognition, and License Plate Recognition** for more detailed instructions on setting up Face Capture and Face Recognition.

22.6.1 Configuration Notes

- A *larger* Face Capture or Face Recognition Zone results in a *longer* detection time. Reduce the size of the Face Capture Zone to reduce the detection time.
- A *higher* sensitivity results in a better detection rate, but also a higher false positive rate.
- A *lower* sensitivity results in a lower detection rate, but also lower false positive rate.

© 2009-2014 Next Level Security Systems, Inc.

22.6.2 FAQs on the Face Capture and Face Recognition 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 30 x 30 pixels within the Face Capture Zone. The sensitivity setting does not impact this setting. Only faces larger than minimum object size are detected.
- Basically, smaller activity zone (or bigger minimum face) results in better frame rate and also lower CPU usage, and vice versa.

© 2009-2014 Next Level Security Systems, Inc.

Chapter 23: Configuring and Using License Plate Recognition

License Plate Recognition (LPR) is an add-on Video Analytic. When the License Plate Recognition Video Analytic is activated for a camera, it grabs a picture of a license plate, and generates a *License Plate Captured* event.

License plates are read, and compared to the numbers in the LPR group assigned to the camera.

Each Gateway contains its own LPR database. The database lists the license plates and the people associated with those plates. Multiple license plates can be associated to a person.

All people and their associated plate numbers are stored in the *Personal Vehicle Pool.*

People are grouped in the License Plate Recognition database. A group is assigned to a camera to enable License Plate Recognition for that camera.

Important: A group must be assigned to a camera. If a group is not assigned, License Plate Recognition defaults to run as License Plate Capture.

The *License Plate Captured*, *License Plate Recognized*, and *License Plate Match Group* events are displayed in the Event Log. Standard event functions are available, including filtering, playing the video clip of the event, acknowledgment, etc. See **Chapter 15: Monitoring and Handling Events** for more information.See *Chapter 14: Monitoring and Handling Events* of the *NLSS Unified Security Suite User Manual* for more information.

These events can be linked to specific actions using an Event Linkage. See **Configure Event Linkages** in **Chapter 17: Global Configurations** for instructions.

These events can be linked to specific actions using an Event Linkage. See *Configure Event Linkages* in *Chapter 16: Global Configurations* of the *NLSS Unified Security Suite User Manual* for instructions.

License Plate Capture and License Plate Recognition is configured and run at the local Gateway level, on a per camera basis. Before using License Plate Recognition:

- Enter a token in *Configuration* > *Global* > *Subscriptions* to enable License Plate Recognition. See **Enabling Other Premium Features** in **Chapter 17: Global Configurations** for instructions.
- Configure and run the analytic for a camera or video stream. See **Running the License Plate Recognition Analytic** for instructions.

Note: License Plate Capture runs within License Plate Recognition. If License Plate Recognition is not running, License Plate Capture can be run on its own. See **Running License Plate Capture** for instructions.

The LPR database is loaded into the Gateway through the Configuration module to speed configuration of License Plate Recognition. However, the files for the database must meet the following specifications.

23.1 DATABASE SPECIFICATIONS

The database is built from a zipped file containing two *.csv* files, and an image folder.

- *lpr.csv*: lists the people associated with the license plates in the database.
- *vehicles.csv*: lists license plate numbers, the associated person, plus general information about the vehicle.

The zipped files are imported to the Gateway to create License Plate Recognition groups. See **Importing a Database** later in this chapter for instructions on downloading a template for the contents of the zip file, and adding database contents to the License Plate Recognition database.

23.1.1 lpr.csv File

The *lpr.csv* file lists the people to be associated with license plates. Each instance of this file in the database defines a License Plate Recognition group.

The .csv file must have the following columns, in this order, to identify the people in the database:

- **groupName**: one group per .csv file.
- **userSuppliedID**: the unique identifier for each person.

  Use only alpha-numeric characters, with no special characters (_, -, ., #, etc.) and no spaces.
- **firstName**
- **middleName**
- **lastName**
- **preferredName**
- **description**

Important: The .csv file is limited to 5000 entries. Any entries past 5000 are not processed when the file is imported into the Gateway.

Multiple .csv files can be imported with the same GroupName. However, when the database entries on the gateway for that group reach 5000, any additional entries in the imported .csv file are ignored.

© 2009-2014 Next Level Security Systems, Inc.

23.1.2 vehicles.csv

The *vehicles.csv* associates people with license plate numbers and their vehicles, plus general information about the vehicle.

- **userSuppliedID**: the unique identifier for each person, as defined in the lpr.csv.
- **licensePlate**: the license plate number.
- **make**: vehicle manufacturer
- **model**: vehicle name
- **state**: state where the plate is registered.
- **country**: country in which the vehicle is registered.
- **description**: optional field to provide additional information about the vehicle.

Important: The .csv file is limited to 5000 entries. Any entries past 5000 are not processed when the file is imported into the Gateway.

23.1.3 Images Requirements

The images must meet the following criteria to be used for License Plate Recognition.

- The images folder must contain JPEG (*.jpg)* images to be associated with the people in the database.
- Size: up to 5 MB
- Limit: One image can be associated with a person.
- Naming: *userSuppliedID.jpg*. For example, if the userSuppledID for a person is NLSS01, then that person's images would be labeled as NLSS01.jpg, etc.

Note: The file name extension, .jpg, must be in lower case.

Important: Ensure that all images match up with a userSuppliedID. Persons listed in the .csv file without a matching primary image trigger an error during the upload.

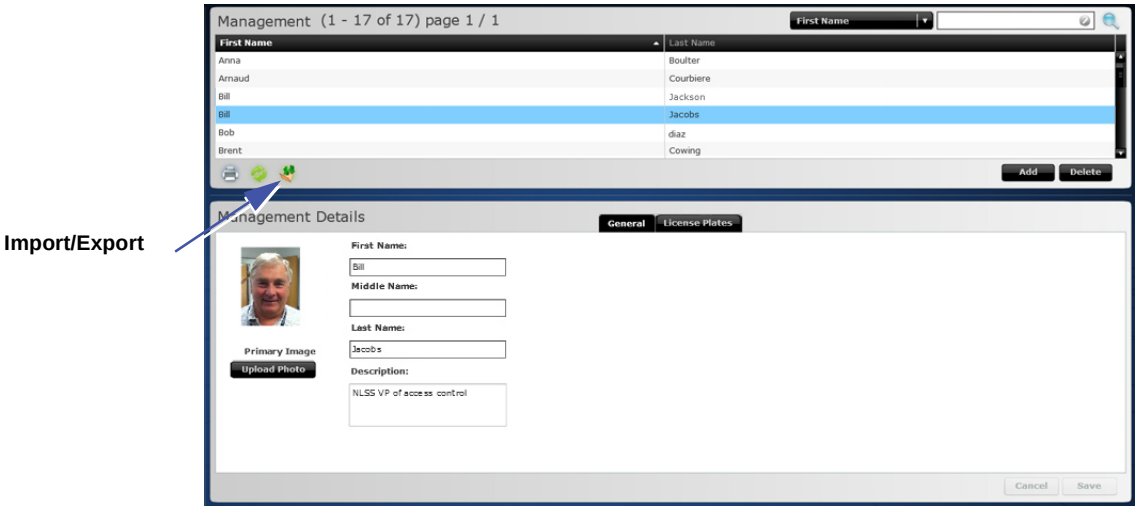
© 2009-2014 Next Level Security Systems, Inc.

23.2 IMPORTING A DATABASE

Import the zip file containing the database components through the Configuration module.

1. Log into the NLSS Unified Security Suite Web Interface for a local Gateway.
2. Select **Configuration > License Plate Recognition > Management**.

   The *License Plate Recognition Management* window is displayed.



3. Click **Import/Export**.

   The *Import/Export License Plate Recognition* dialog box is displayed.

   – A **Sample Template** of the .csv files can be downloaded from this dialog box by clicking **Download** under the Import button.

4. Click **Import**.

   The *File Uploader* dialog box is displayed.

5. **Browse** to select a zip file.
6. Click **Upload**.

Note: If an error occurs while importing a .zip file, check the **Import Log** by clicking **Download** at the top of the dialog box.

The contents of the .zip file are added to the License Plate Recognition database on the Gateway. The people in the .csv file are placed in the group listed in that file. The userSuppliedID is used to assign to a person to a license plate number and image.

© 2009-2014 Next Level Security Systems, Inc.

The people and license numbers are placed in a License Plate Pool in the database. These people can belong to multiple groups. People listed in database can be added to other groups created within the *Configuration > License Plate Recognition > Groups* window.

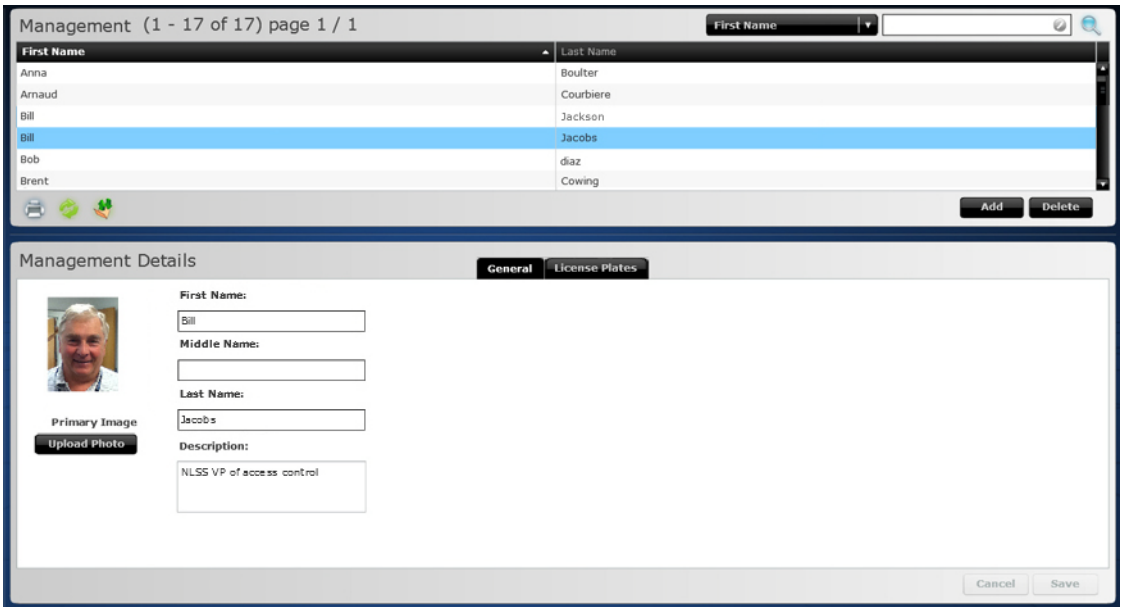
Important: The License Plate Recognition video analytic must be restarted after the License Plate Pool is updated.

23.3 LICENSE PLATE RECOGNITION MANAGEMENT

The Management window lists the people included in the License Plate Recognition database. People can be either added through a database import, or individually in this window. Records also can be edited and deleted using this window.

1. Log into the NLSS Unified Security Suite Web Interface.
2. Select **Configuration > License Plate Recognition > Management**.

The *License Plate Recognition Management* window is displayed. New images can be uploaded through this window



23.3.1 Management Table

- **First Name**: The first name that was either included in the imported .csv file, or added in the Management Details pane.
- **Last Name**: The last name that was either included in the imported .csv file, or added in the Management Details pane.

23.3.2 Management Details

The bottom pane contains the Management details to configure the records listed in the License Plate Recognition database.

This pane contains two tabs: **General** and **License Plates**.

23.3.2.1 General Tab

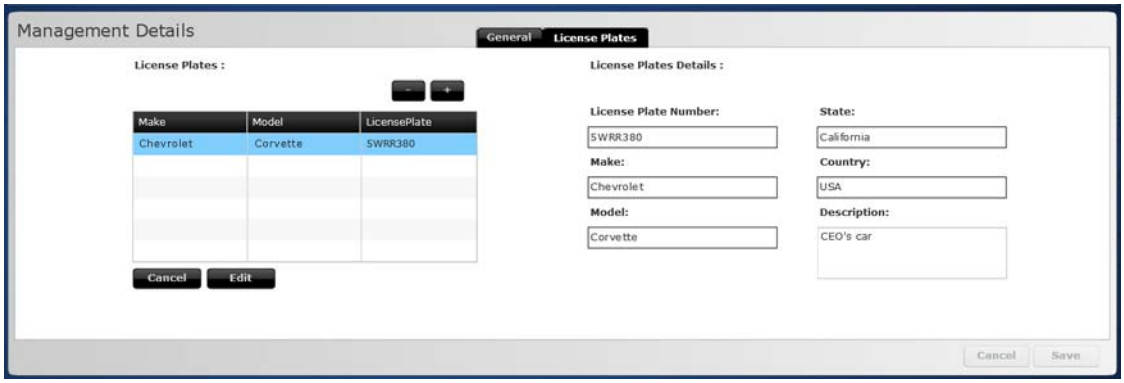
These editable fields contain the data entered in the .csv file that was imported. These fields can be edited when a person is selected in the Management table.

- **First Name**: The first name that was either included in the imported .csv file, or added in the Management Details pane.
- **Middle Name**: (optional) The middle name, or initial, that was included in the imported .csv file, or added in this pane when an entry was added.
- **Last Name**: The last name that was either included in the imported .csv file, or added in the Management Details pane.
- **Description**: (optional) An text field to provided further information about the person.

23.3.2.2 License Plate Tab

The License Plate tab provides details about the license plates associated with the selected user.

License plate information can be edited, and plates can be added or deleted in this tab.



The **License Plates** table lists the license plates associated with the selected person.

License Plates Details provides editable fields identifying the plate.

- **License Plate Number**: the license plate number.
- **Make**: vehicle manufacturer.
- **Model**: vehicle name.
- **State**: state where the plate is registered.
- **Country**: country in which the vehicle is registered.
- **Description**: optional field to provide additional information about the vehicle.

© 2009-2014 Next Level Security Systems, Inc.

23.3.2.2.1 Adding a License Plate

A plate can be added to the License Plate list in the Management Details pane.

1. Click **Add** by the License Plates list.
2. Enter the License Plate Details.
3. Click **Save** to add the license plate to the database and associate it with the selected person.
   – Click **Cancel** to discard the settings.

23.3.2.2.2 Deleting a License Plate

A plate can be deleted from the License Plate list in the Management Details pane.

1. Select a license plate from the list.
2. Click **Delete** by the list.

Important: No confirmation message is displayed. Ensure the desired license plate is selected before clicking delete.

23.3.3 Updating the Management List

People can be added, edited and deleted.

23.3.3.1 Adding a Person

1. Select **Configuration > License Plate Recognition > Management**.
2. Click **Add** in the top pane.
   A blank *Management Details* pane is displayed.
3. Enter a **First Name**, **Middle Name** (optional), **Last Name**, and **Preferred Name** (optional).
4. Enter a **Description** (optional).
5. Click **Upload**.
   The *File Uploader* dialog box is displayed.
6. **Browse** to select a an image file.
7. Click **Upload**.
   A thumbnail of the image is added to the License Plate Recognition database.
8. Click **Save** to add the person to the database.
   – Click **Cancel** to discard the settings.

© 2009-2014 Next Level Security Systems, Inc.

23.3.3.2 EDITING A PERSON

1. Select **Configuration > License Plate Recognition > Management**.
2. Select a person in the Management table.
3. Edit the **Name** fields or **Description**, if desired.
4. Update the image, if desire.
5. Click **Save** to update the record.
   – Click **Cancel** to discard the changes.

23.3.3.3 DELETING A PERSON

1. Select **Configuration > License Plate Recognition > Management**.
2. Select a person in the Management table.
3. Click **Delete** in the top pane.
   A confirmation message is displayed.
4. Click **Yes** to delete the person.
   – Click **Cancel** to keep the person.

Deleting a person does not delete associated groups from the License Plate Recognition database.

23.4 LICENSE PLATE RECOGNITION GROUPS

The License Plate Recognition database can be partitioned into specific groups. People can be assigned to License Plate Recognition Groups either in the *lpr.csv* file imported in into the database, or manually from the *Configuration* > *License Plate Recognition* > *Groups* page.

License Plate Recognition Groups are assigned to cameras that are running that Video Analytic. A group assignment narrows the database search for a match when running the analytic.

Using groups improves management of the database, and provides the ability to recognize a specific group of people on a per camera or deployment basis. For example, groups can be created for employees, contractors, or VIP Customers.

Note: License Plate Recognition groups are configured and used separately from *Permissions Groups*. License Plate Recognition groups are *not* used with the Configuration > Permissions settings.

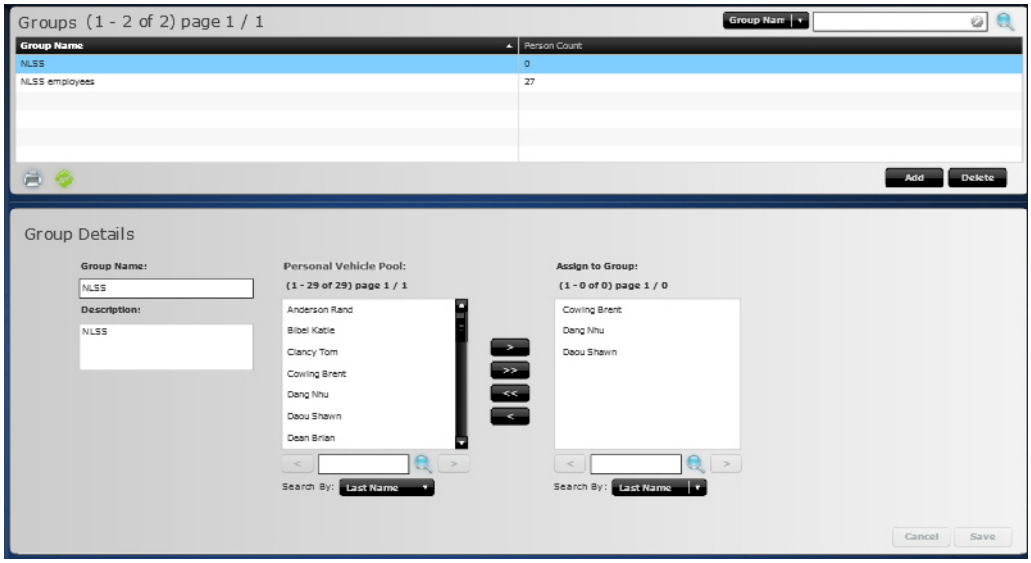
© 2009-2014 Next Level Security Systems, Inc.

23.4.1 Accessing License Plate Recognition Groups

Groups are listed and details are provided in the *Configuration > License Plate Recognition > Groups* window.

1. Log into the NLSS Unified Security Suite Web Interface.
2. Select **Configuration > License Plate Recognition > Groups**.

   The *License Plate Recognition Groups* window is displayed.



23.4.2 Groups Table

The License Plate Recognition groups are listed in the table in the top pane. The number of people in the groups is also listed in the **Person Count** field. This list can be searched and sorted by **Group Name** or **Person Count**.

23.4.3 Group Details

The bottom pane contains the Group Details for the selected group.

- **Group Name**: editable field identifying the group.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

- **Description**: optional text field.
- **Personal Vehicle Pool**: lists the people who have been imported into the database.
- **Assign to Group**: lists the people who can have been assigned to this group.

Note: The Personal Vehicle Pool and Assign to Group lists can be searched by First Name or Last Name.

© 2009-2014 Next Level Security Systems, Inc.

When the mouse hovers over a name in the License Plate Pool or Assign to Group lists, a pop-up is displayed with that person's first and last name, along with a thumbnail of the person's image, and the license plates associated with that person.

The image is assigned when the database content was created, and can be changed in the Management page. See **Management Details** later in this chapter for instructions on uploading a photo.

23.4.4 Creating a Group

1. Select **Configuration > License Plate Recognition > Groups**.

   The *License Plate Recognition Groups* window is displayed.

2. Click **Add** in the top pane. A blank *Group Details* pane is displayed.

3. Enter a **Group Name**.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

4. Enter a **Description**.

5. Select a person in the **Personal Vehicle Pool**.

6. Use the right arrow (**>**) to move the person to the **Assign to Group** list.
   - Use the double right arrow (**>>**) to move all people in the Personal Vehicle Pool to the Assign to Group list. Remember, each group is limited to 5000 members.
   - Use the left arrows (**<**, **<<**) to remove people from the **Assign to Group** list.

7. Click **Save** to keep the group settings.
   - Click **Cancel** to discard the settings.

23.4.5 Deleting a Group

Deleting a group does not delete the people in that group from the License Plate Recognition database.

1. Select **Configuration > License Plate Recognition > Groups**.

2. Select a **Group** in the Groups table.

3. Click **Delete** in the top pane. A confirmation message is displayed.

4. Click **Yes** to delete the group.
   - Click **Cancel** to keep the group.

23.4.6 Assigning People to Groups

People can either be assigned to License Plate Recognition groups in two locations:

- In the lpr.csv file.
- In the *Groups* window, as described in **Creating a Group**.

© 2009-2014 Next Level Security Systems, Inc.

23.5 RUNNING LICENSE PLATE CAPTURE

License Plate Capture records license plates, but does not have a database that compares the numbers, or associates the license plate with a person or vehicle.

License Plate Capture runs as part of License Plate Recognition, so it does not need to be configured and launched if License Plate Recognition is running. When License Plate Recognition is running, a License Plate Capture event is generated before the License Plate Recognition event.

License Plate Capture can be run if License Plate Recognition is not running. License Plate Capture is configured and run at the local Gateway level, on a per camera basis.

1. Select **Operations > Cameras**.
2. Select a camera or video stream.
3. Click **License Plate Capture** in the Video Analytics Configuration list.
4. Click **Edit**.

   The License Plate Capture settings are displayed in the video player with a *License Plate Capture Zone*.

5. Drag the slides to configure the analytic settings.
   a. **Sensitivity**: scale 0-100
      » A *higher* sensitivity results in a better detection rate, but also a higher false positive rate.

      A higher sensitivity captures license plates further away, but uses more system resources.

      » A *lower* sensitivity results in a lower detection rate, but also a lower false positive rate.

      A lower sensitivity requires license plates to be closer, but uses less system resources.

© 2009-2014 Next Level Security Systems, Inc.

After the analytic is saved, a square, labeled *Minimum License Plate Size*, is displayed to indicate the minimum size that a license plate must be on the screen to be recognized by the system. This square is a size indicator, and does not need to be moved.

An event is generated if a valid license plate appears in the License Plate Capture Zone.

A license plate is considered valid if:

» It is larger than minimum license plate size.

» Is located inside the defined License Plate Recognition Zone.

» Meets the required sensitivity threshold.

6. Drag the corners of the *License Plate Capture Zone* to match the area to be monitored. By default, the area is a rectangle.

Note: A *larger* License Plate Capture Zone results in a *longer* detection time. Reduce the size of the License Plate Capture Zone to reduce the detection time.

7. Click **Save** to keep the analytic settings.
8. Click **Start** to launch the License Plate Capture video analytic.
   – Click **Cancel** (**X**) to exit the edit mode without keeping the settings.

23.6 RUNNING THE LICENSE PLATE RECOGNITION ANALYTIC

After License Plate Recognition is configured, the analytic can be used.

1. Click **License Plate Recognition** in the Video Analytics Configuration list.
2. Click **Edit**.

   The License Plate Recognition settings are displayed in the video player with a *License Plate Recognition Zone*.

3. Drag the slides to configure the analytic settings.
   a. **Sensitivity**: scale 0-100
      » A *higher* sensitivity results in a better detection rate, but also a higher false positive rate.
      » A *lower* sensitivity results in a lower detection rate, but also a lower false positive rate.
   b. **Best Match**: options 0 or 1
      » **1** = closest result generates an event. Enabling Best Match provides a higher recognition rate, but also higher false positive rate.

      A setting of 1 works best in a closed group environment where all of the people are in the License Plate Recognition database, such as an office.
      » **0** = generates an event if the analytic determines an exact match. Disabling Best Match provides a lower false positive rate, but also a lower recognition rate.

      This setting is good for an open group or environment where not all of the people are in the database, such as an airport or train station.

© 2009-2014 Next Level Security Systems, Inc.

After the analytic is saved, a square, labeled **minimum plate size**, is displayed to indicate the minimum size that a License Plate must be on the screen to be recognized by the system. This square is a size indicator, and does not need to be moved.

A License Plate is considered valid if it is larger than minimum License Plate size, is located inside the defined License Plate Recognition Zone, and meets the required sensitivity threshold.

4. Drag the corners of the *License Plate Recognition Zone* to match the area to be monitored. By default, the area is a rectangle.

Note: A *larger* License Plate Recognition Zone results in a *longer* detection time. Reduce the size of the License Plate Recognition Zone to reduce the detection time.

5. Click **Group**. This is a License Plate Recognition group, not a permissions group.
6. Check a circle in the pop-up list to select a group. Multiple groups can be selected.
7. Click **Save** to keep the analytic settings.
8. Click **Start** to launch the License Plate Recognition video analytic for this camera.
   – Click **Cancel** (**X**) to exit the edit mode without keeping the settings.

23.7 SEARCHING EVENTS FOR LICENSE PLATES

The Events log can be searched for a captured license plate by the characters in the plate number. The license plate number is recorded as a string, translating the letters and numbers that are stored in an event record. Events can be searched for the whole string, or a partial string.

A *License Plate Captured* event is generated if a valid license plate appears in the License Plate Recognition Zone. If the plate is recognized, a *License Plate Recognized* event is generated. If the plate is part of the group being monitored, then a *License Plate Group Match* event is generated.

1. Open **Events**.
2. Set the **Start** and **End Date** and **Time**.
3. Enter the string or a partial string in the **Event Notes** field.
4. Click **Search**.
5. Select an event from the log.

The dialog displays the event details, plus the applicable parent and child events in this hierarchy: License Plate Capture > License Plate Recognition > License Plate Match Group.

See **Chapter 15: Monitoring and Handling Events** for more information on using Events.See *Chapter 14: Monitoring and Handling Events* of the NLSS Unified Security *Suite User Manual* for more information on using Events.

© 2009-2014 Next Level Security Systems, Inc.

If an email notice is set up for the LPR event, the message contains photos of the license plate and associated person, as shown in the Event Log.

23.8 LICENSE PLATE CAPTURE AND RECOGNITION GUIDELINES

The following set of basic guidelines helps to optimize the license plate capture and recognition capabilities.

For more detailed guidelines, see **Appendix A: Performance and Setup Guidelines: Video Analytics, Face Recognition, and License Plate Recognition**.

Image requirements:

- The license plate's image must be clear, with less than a 5 degree tilt.
- Any added borders or license plate frames must not cover the license plate number.

Processing time:

- The license plate must appear in front of the camera for at least two seconds before the analytic's bounding boxes can locate the license plate. Three seconds are needed to read the number. Then an event is generated.

Event search:

- The license string can be searched in events page by putting partial license text in the **Event Notes** field.

© 2009-2014 Next Level Security Systems, Inc.

Chapter 24: Configuring Audio Analytics

If a camera has a built-in or attached microphone, audio analytics can be applied.

When an Audio Analytic is activated for a camera, the Gateway analyzes detected sounds, then compares it to sounds that can trigger an event. If a match is made, an event is generated.

By default, the NLSS Gateway includes an Audio Analytic for *Glass Break*. This analytic can be applied up to four video streams on a Gateway.

Other audio analytics are available as premium features that are enabled via a token: *Car Alarm*, *Gun Shot*, and *Aggression*.

The Audio Analytic event is displayed in the Event table. Standard event functions are available, including filtering, playing the video clip of the event, acknowledgment, etc. Audio Analytic events can be linked to specific actions using an Event Linkage. See **Configure Event Linkages** in **Chapter 17: Global Configurations** for instructions.

Audio Analytics are configured and run at the local Gateway level, on a per camera basis. Before using Audio Analytics:

- Enter a token in *Configuration* > *Global* > *Subscriptions* to enable an the premium Audio Analytics. Each premium Audio Analytic requires a separate token. Glass Break does not require a token.

  See **Enabling Other Premium Features** in **Chapter 17: Global Configurations** for instructions.

- Configure and run the analytic for a camera or video stream. See **Configuring Audio Analytics** for instructions.

See **Appendix B: Audio Analytics Guidelines** for more information.

24.1 CONFIGURING AN AUDIO ANALYTIC

The audio must be configured on the camera before the analytic is enabled.

1. Access the camera's set up interface.
2. Enable audio.
3. Under audio input:
   a. Set the *sample rate* to **16KHz**.
   b. Set encoding to **AAC**.

c. Any audio signal process (such as AGC - Active gain control) applied by the camera or encoder should be turned off.

4. Save the changes.

Note: See the camera's documentation for specific instructions on using the setup.

5. In the NLSS Web Interface, select **Audio Analytics** from the Video Analytic options.

Note: If a video analytic will run simultaneously, configure that analytic before the audio analytic.

6. Click **Edit** for **Audio Analytics** in the Video Analytics Configuration list.
7. Select an audio analytic to run.
8. Ensure that the Audio Analytic is checked in the Edit dialog.
9. Set the **Sensitivity**: scale 0-100
   - » A *higher* sensitivity results in a better detection rate, but also a higher false positive rate.
   - » A *lower* sensitivity results in a lower detection rate, but also a lower false positive rate.
   - » The default for all audio analytic sensitivity settings is 50 and works well for most scenarios.
10. Click **Save** to keep the changes.
11. Click **Start** to activate this video analytic. If someone (or something large enough) moves through the rectangle, a video analytic event is generated.

Configuration Notes for Glass Break

- The audio analytic requires a microphone with a frequency response equal to at least 100 Hz - 8 kHz +/- 6dB. Most built-in camera microphones met these requirements.
- The microphone sensitivity settings on the camera or encoder should be set so that the audio does not clip or distort using a glass break simulator.
- The microphone sensitivity settings must provide a reasonable level of audio to the gateway and the analytic.

FAQ's on Audio Analytic for Glass Break

How to test the analytic and camera are setup and configured properly?

- Use a glass break simulator to test that the analytic and camera are properly configured. The glass break analytic works with the Risco RG65 industry standard glass break simulator.
  a. Set the simulator to plate glass mode.
  b. Use the simulator to test the analytic and microphone sensitivity have been configured properly with the simulator approximately one meter from the microphone.

What type of glass does the analytic detect breaking?

- Breakage of different thicknesses and sizes of office, shop and house window glass breaking are detected by this analytics.
  - Plate: 2.4 mm - 6.4 mm;
  - Tempered: 3.2 mm - 6.4 mm;
  - Wired: 6.4 mm; (only thickness wired glass comes in)
  - Laminated: 6.4 mm
  - Minimum glass size, all types of glass: 300 mm x 300 mm.

How far from the microphone will the analytic work?

- The analytic detects glass break up to 10 meters from the microphone based on a representative environment for intrusion detection applications.
- Effective range varies according to the physical and acoustic environment. The ranges are based on the types of microphones built into modern security cameras.
- Generally, the audio source needs to be at least 3 meters away from microphone in order to avoid distortion.
- The audio is ignored when distortion is detected in the input audio. This action prevents frequent false alarms.
- The distortion pattern can be seen in the audio volume bar in the manufacturer's camera interface.

How noisy an environment can the analytic work in?

- The analytic reliably detects glass break in typical intrusion detection scenarios up to at least 50 dB SNR (Signal to Noise Ratio).

© 2009-2014 Next Level Security Systems, Inc.

Chapter 25: Configuring and Using Intrusion Detection

Next Level Security Unified Security Suite works with *intrusion detection systems* to associate cameras with a monitored location, and provide events to NLSS users when an intrusion event is detected.

Intrusion detection systems associated with the NLSS Unified Security Suite monitor physical access to a location, as opposed to intrusion detection systems that monitor devices on a computer network.

Intrusion detection systems include sensors for detecting smoke, motion, fire, glass breakage, open doors, etc. These devices are configured and managed through the keypads and associated software. See that system's documentation for instructions on configuring zones and areas.

Intrusion panels are manually added to the NLSS Unified Security Suite. From this connection, the Security Suite gathers information about areas, zones, keypads and zone expanders.

The NLSS Unified Security Suite is connected to an intrusion detection panel, and monitors *Zones* and *Areas*.

- **Zone**: is a specific location where an intrusion sensor is installed, such as a door or a window. Intrusion devices include motion detectors and breakage sensors.
- **Area**: is a collection of zones that are grouped in the intrusion detection system.

For a list of supported intrusion detection systems, see the NLSS Support site: **nlss.com/support.html**.

The NLSS Unified Security Suite accepts alerts from the intrusion systems, and generates events from those alerts. As with other NLSS events, actions can be associated with the event. See **Configure Actions** in **Chapter 17: Global Configurations** for instructions.

From the NLSS Web Interface, an area can be armed, and zones can be bypassed. These features are discussed later in this chapter.

- Intrusion is a premium feature for the NLSS Gateway and is enabled by entering a token. See **Enabling Other Premium Features** in **Chapter 17: Global Configurations** for instructions.
- Configuration for the NLSS Web Interface, and information on the intrusion detection system devices is available from Configuration > Intrusion. See **Configuring Intrusion** for more information.

© 2009-2014 Next Level Security Systems, Inc.

25.1 CONFIGURING INTRUSION

- Select **Configuration > Intrusion** from the Main Menu.

  Four options are available:

  – **Panel**

  – **Areas**

  – **Devices**

  – **Zones**

Most of the data under thee options is informational, and is gathered from the intrusion detection system.

25.1.1 Panel

Intrusion Detection Panels are added manually to the NLSS Unified Security Suite. Identifying and access information is added through the NLSS Web Interface.

1. Select **Intrusion > Panel**.

   A Panel list is displayed in the top pane of the window, with Intrusion Panel details displayed in the bottom pane.

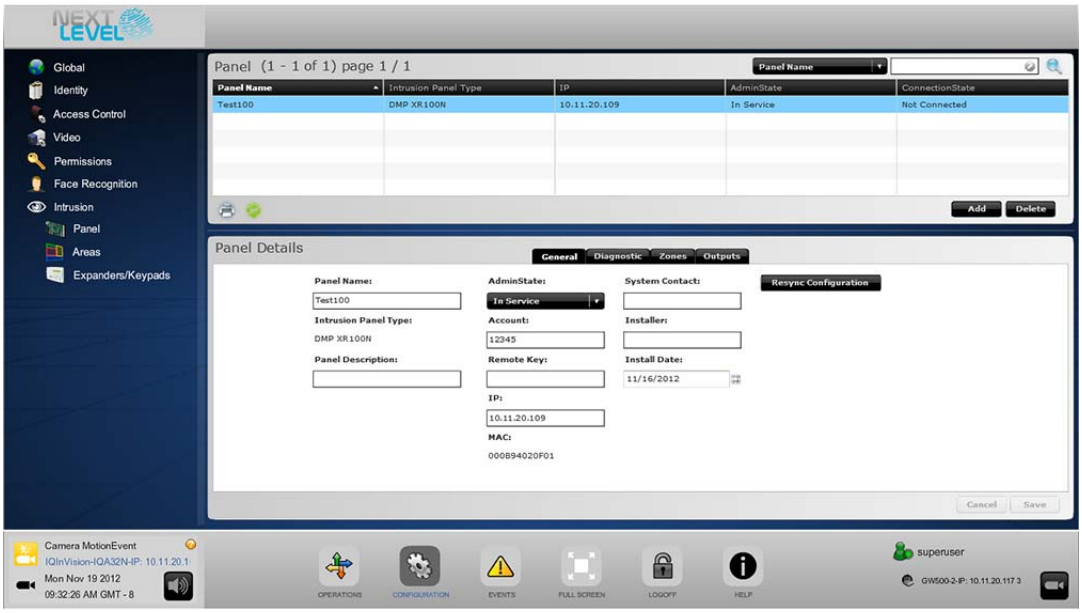
   The top pane has an additional field of **Connection State**. This field indicates where whether or not the Panel is connected to the Gateway.

2. Select a panel from the list.

   The Panel Details are displayed under four tabs in the bottom pane.

© 2009-2014 Next Level Security Systems, Inc.

The list includes the Panel Name, Intrusion Panel Type, IP address, and Admin State, as also listed in the **General Tab**.



If no panels listed, manually add them. See **Adding an Intrusion Detection Panel**.

Details for a selected panel are displayed in four tabs in the bottom pane:

- **General Tab**
- **Diagnostic Tab**
- **Zones Tab**
- **Outputs Tab**

25.1.1.1 General Tab

The General tab contains the only editable fields in the Intrusion Panel pane. These fields identify the panel and provide fields to enter access information to allow the NLSS Unified Security Suite to access the panel.

Important: Only use alpha-numeric characters,: A-Z (upper or lower case), 0-9, a dash (-), or underscore (_). No special characters (&, :, ., ., #, etc.)

- **Panel Name** (required): a unique name to identify the panel in the NLSS Unified Security Suite.
- **Intrusion Panel Type**: is selected when a panel is added.
- **Panel Description**: a text field used to further identify the panel.
- **Admin State**: a drop-down menu to place the panel **In Service** or **Out of Service** in the NLSS Unified Security Suite.

  A default setting of **Preprovisioned** is assigned when the panel is first added.

- **Account** (required): numeric user name required to allow the NLSS Unified Security Suite to access the panel.
- **Remote Key**: numeric password associated with the account.
- **IP** (required): the IP address assigned to the intrusion detection panel. A static IP address is recommended, as a DHCP assigned address can change, breaking the connection between the panel and the NLSS Unified Security Suite.
- **MAC**: the MAC address for the panel, detected when the panel's Admin State is changed to In Service.
- **System Contract**: the person responsible for maintaining the panel.
- **Installer**: the person who installed the panel.
- **Install Date**: when the panel was installed.
- **Resync Configuration**: click this button to synchronize the tabs with any updates that have been input through the intrusion detection system.

25.1.1.2 Diagnostic Tab

The data on this tab is gathered from the panel and is not editable.

- **Firmware Version**: the firmware release running on the panel.
- **Serial Number**: the serial number for the panel.
- **Firmware Release Date**: the date on which the installed firmware was released.

25.1.1.3 Zones Tab

Zones are defined on the panel using that intrusion detection system's keypad or software.

- **Zones**: lists the zones configured on the panel. A zone is a specific location where an intrusion sensor is installed, such as on a door or a window.
  - Select a zone to display its details in the tab.
- **Zone Name**: unique, descriptive name for the zone.
- **Number**: numerical identifier for the zone.
- **Type**: zone type, such as day, night, exit, fire, arming, emergency, etc.
- **Status**: current state of the panel.
- **Area Number**: the area to which this zone is assigned. An area is a collection of zones, tied together through the intrusion detection system.
- **Entry Delay**: time, in seconds, to enter an access code in a keypad after an entry is detected.
- **Exit Delay**: time, in seconds, to exit an area after arming the intrusion detection system from a keypad.

© 2009-2014 Next Level Security Systems, Inc.

25.1.1.4 Outputs Tab

The Outputs tab lists the output associated with specific events in the intrusion detection system. These outputs are triggered when the event is initiated by an associated sensor, such as a window breaking, or motion is detected.

This information is not editable, and is gathered when a panel is added to the NLSS Unified Security Suite.

- **Outputs**: lists the outputs configured for this panel.
  - Select an output to display its details in the tab.
- **Output Name**: unique, descriptive name for the selected output.
- **Number**: numerical identifier for the selected output.

25.1.1.5 Adding an Intrusion Detection Panel

Panels must be added manually to the NLSS Unified Security Suite.

1. Click **Add** in the Panel list.

   A blank Panel Details pane is displayed.

2. Select an **Intrusion Panel Type** from the drop down menu.
3. Enter the required fields: **Panel Name**, **Account**, and **IP** (address).
   - The other fields are optional.
4. Click **Save** to add the panel.

   The MAC address is added from the panel, and Admin State drop-down menu be becomes available.

   The fields in the other tabs are populated with data from the panel.
   - Click **Cancel** to clear the fields, without adding the panel.

   A default Admin State of **Preprovisioned** is assigned.
5. Select **In Service** from the **Admin State** drop down menu to be add the panel to the NLSS Unified Security Suite.
6. Click **Save** to keep the changes.
   - Click **Cancel** to return to the previous settings.

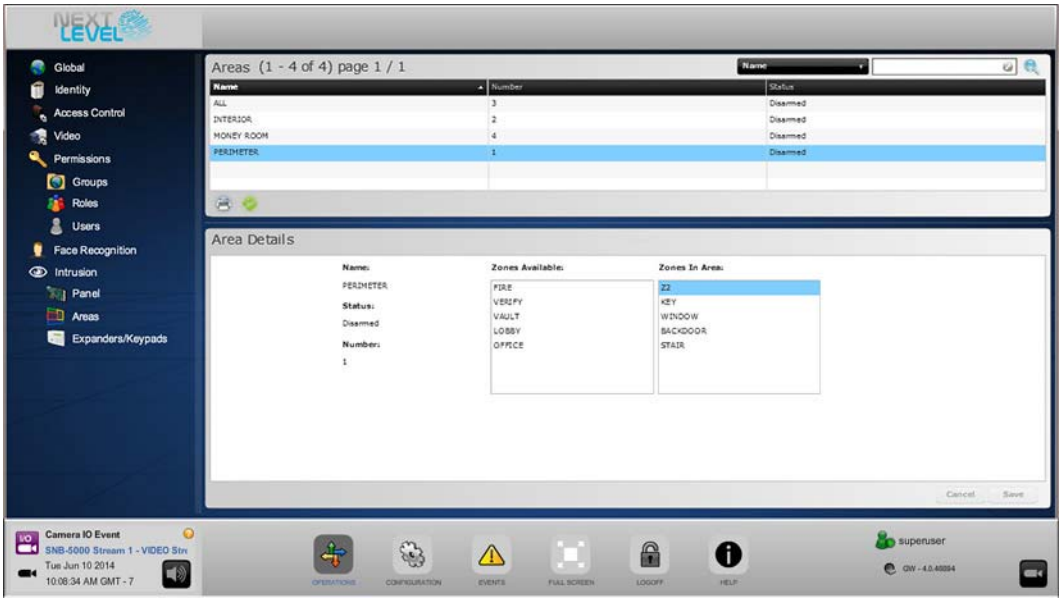
© 2009-2014 Next Level Security Systems, Inc.

25.1.2 Areas

Areas are collections of zones that are grouped in the intrusion detection system. The Areas window contains read-only fields describing each areas' configuration.

1. Select **Configuration > Intrusion > Areas** from the Main Menu.

   The Areas window lists the areas in the system, and provides configuration information about each area.



   The Areas list provides the:

   – **Name**: unique, descriptive name for the area.
   – **Number**: unique, numeric identifier for the area.
   – **Status**: indicates the state of the area, such as *Armed* or *Disarmed*.

2. Select an area from the list.

   Area Details are displayed in the bottom pane. Besides the Name, Status, and Number, as provided in the list, the details also include:

   – **Zones Available**: a list of zones in the system that are not included in this area.
   – **Zones In Area**: zones assigned to the area through the intrusion detection system.

© 2009-2014 Next Level Security Systems, Inc.

25.1.2.1 DEVICES

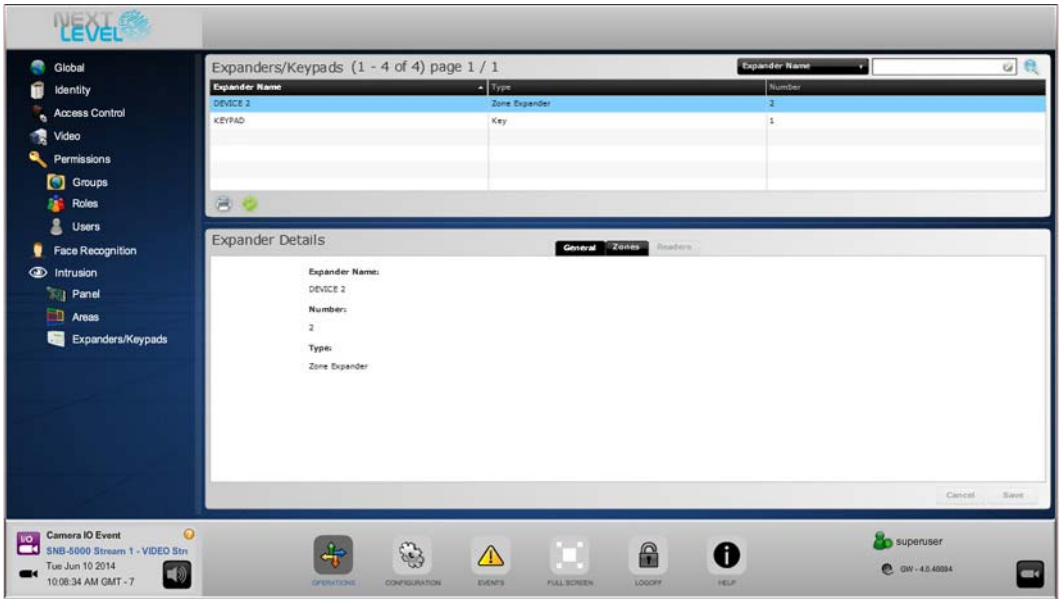
Two devices are detected by the NLSS Gateway:

- *Zone expander*: is a board added to an intrusion detection panel to provide more zone connections.
- *Keypad*: a physical interface to a panel. Keypads are used to arm or disarm a system, enter access codes, and configure and reset the system.

The *Devices* window provides read-only information about these devices, as gathered from the intrusion detection system. Other items may be listed, depending on devices connected to the panel.

1. Select **Configuration > Intrusion > Expanders/Keypads** from the Main Menu.

   The Expanders/Keypads window is displayed, with list of these devices in the system.



2. Select a device to display its details in the bottom pane.

   The **General** tab contains the same fields for both devices:

   – **Name**: unique, descriptive name for the expander or keypad.

   – **Number**: a unique, numeric identifier for the device.

   – **Type**: identifies what the device is, such as *Key* (for a keypad), or *Zone Expander*.

   If a zone expander is selected, a **Zones** tab is displayed. The information is the same as displayed in the **Zones Tab** available under Intrusion > Panel.

© 2009-2014 Next Level Security Systems, Inc.

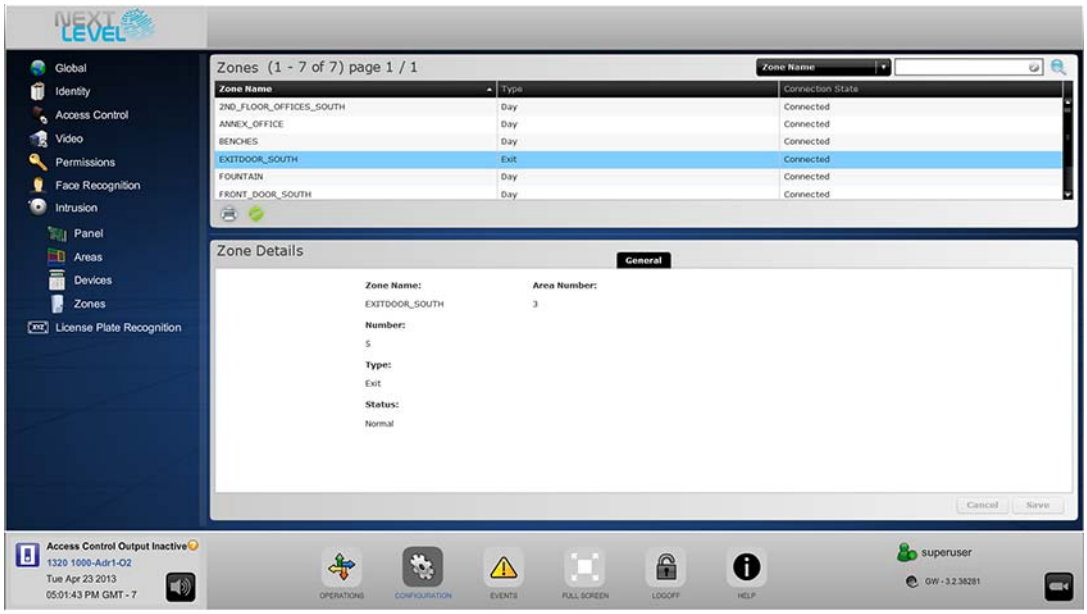
25.1.3 Zones

Zones are defined by the sensors connected to the intrusion panel. Zones are configured through the panel using its keypad or associated software. The NLSS Gateway downloads this configuration information when it is connected to an intrusion panel.

The Zones window contains read-only fields describing each zones' configuration.

1. Select **Configuration > Intrusion > Zones** from the Main Menu.

   The zones in the system are listed, with details about each zone.



   The Zones list provides the:

   – **Name**: unique, descriptive name for the zone.
   – **Type**: as defined through the intrusion panel.
   – **Connection State**: indicates the state of the area, such as **Connecting**, **Connecting**, or **Not Connected**.

2. Select an zone from the list.

   The *Zone Details* pane is displayed. The pane contains one tab: **General**.

   Besides the Name, and Type, as provided in the list, the details also include:

   – **Number**: unique, numeric identifier for the zone.
   – **Status**: indicates the current status of the sensor in the zone.
      » **Normal**: the sensor is on-line and active.
      » **Bypassed**: the intrusion panel is set not to trigger an alarm should the sensor detect an event.
      » **Low Battery**: the battery powering the device needs replacement.
      » **Missing**: the sensor is not being detected by the intrusion panel.
      » **Open**: the intrusion panel has detected a open circuit in the connection to the sensor.
      » **Short**: the intrusion panel has detected a short circuit in the connection to the sensor.
   – **Area Number**: the area to which this zone is assigned.

© 2009-2014 Next Level Security Systems, Inc.

25.2 INTRUSION OPERATIONS

Both Zones and Areas can be accessed from the Operations menu. These options display video from cameras associated with the selected zone or area.

A set of LEDs provide the admin and connection state for the zone or area. These LEDs are on the left of the zone or area icon:

- Green: In service/On line
- Yellow: In service/Off line
- Red: Out of service/Off line
- Gray: Preprovisioned/Off Line

Also, a camera can be associated with a zone or area.

25.2.0.1 ADDING A CAMERA TO A ZONE OR AREA

A camera can be associated with a zone to synchronize video with a sensor. Only one camera can be associated with a zone.

Note that if a camera covers multiple sensors, it can be associated with multiple zones. However, a more efficient method is grouping those sensors in an area, and assigning a camera to that area.

A camera also can be associated with an area, covering multiple zones. Only one camera can be associated with an area. However, one camera can be associated with multiple areas. Applying a camera to an area is more efficient than applying the same camera individually to multiple zones.

To add a camera to a selected zone or area:

1. Select a Zone or Area.
2. Click **Add Camera**.

   The available cameras are listed in the Details Pane. See **Selecting Cameras** in **Chapter 4: Controlling Cameras** for more information on this list.
3. Select a camera. The camera's video is displayed in the Details Pane.

   If the camera supports duplex audio, the Talkback button is displayed. See **Talkback (Local Microphone Control)** in **Chapter 4: Controlling Cameras** for more information.

Note: A camera assigned to an individual zone in Operations > Zones remains assigned to that zone, even if a different camera is assigned to an area containing that zone. Select the zone from the area's list to see that camera.

4. Click the video to open the video player for the camera.
   – Click **Back** in the video player to return to the Zone window.

© 2009-2014 Next Level Security Systems, Inc.

5. To remove a camera from zone, click **Remove Camera**.

25.2.1 Zones Window

The first level of intrusion detection is zones.

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

   A list of zones monitored by the NLSS Unified Security Suite is displayed. The list can be searched and filtered.

2. Select a zone.

   The Details Pane is displayed for that zone.

3. To filter the list, click the filter button:
   - **Connection State** : select either **Connected** or **Not Connected**.
   - **Admin State** : select either **In Service** or **Out of Service**.
4. Click **Event Log** to view the events associated with this zone.
5. Click **Reports** to view reports associated with this zone.
6. Click **Add Camera**. See **Adding a Camera to a Zone or Area**.

25.2.1.1 Bypassing a Zone

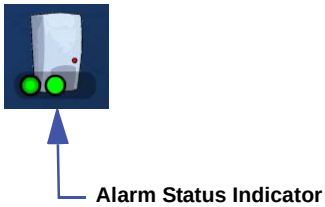
If an event is being triggered in a zone, that event can be bypassed if notification is not needed. For example, a door with a motion detector that is normally shut is propped open for a delivery. Instead of a constant stream of events, the intrusion panel is notified from the NLSS Web Interface to bypass, or ignore the event at this time.

- Click **Bypass** in the Detail Pane for the selected zone.

25.2.1.2 Zone Alarm Status Indicator

The right LED under the zone icon indicates the alarm status for the device in the zone.

- Green = Normal/Reset
- Orange = Trouble (potential event detected that could trigger an alarm)
- Red = Alarm
- White = Bypass



25.2.2 Areas Window

Zones can be grouped into areas. This grouping simplifies simultaneously monitoring multiple zones.

Areas are created though the intrusion detection system's tools. See the system's documentation for instructions on configuring areas.

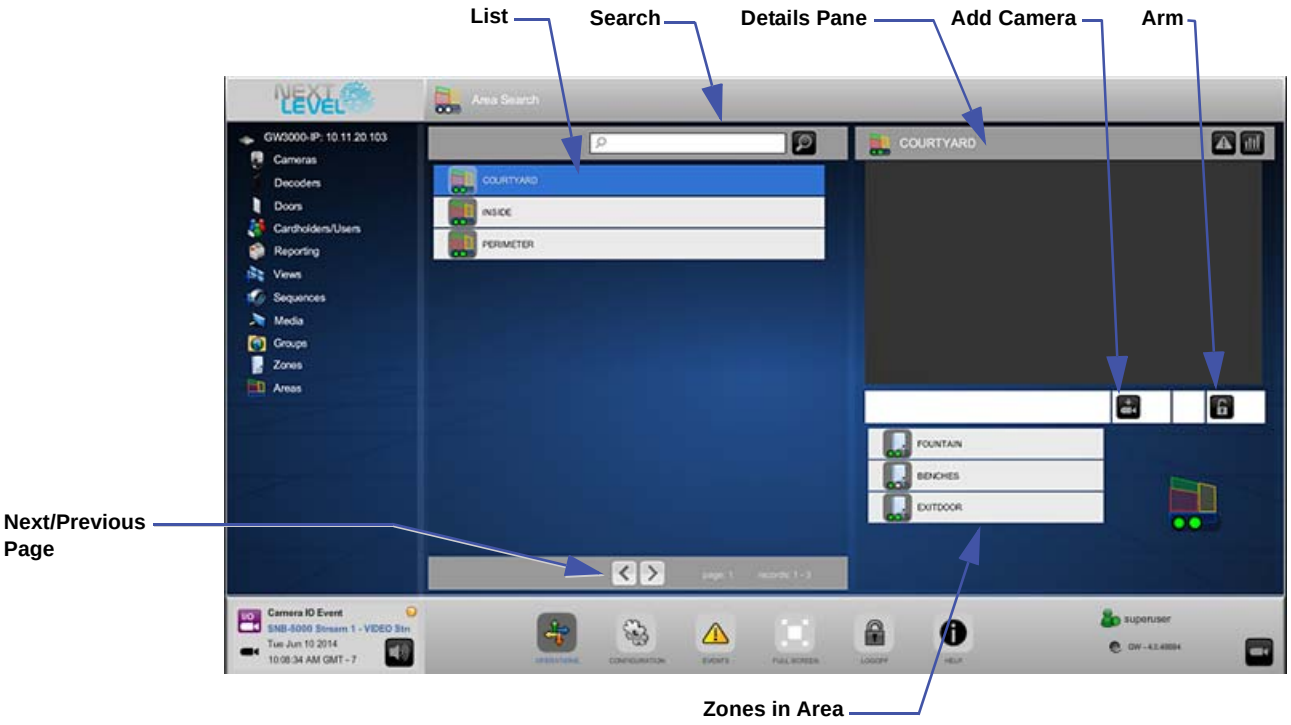
1. Select **Operations > Areas** from the Main Menu.

   A list of areas monitored by the NLSS Unified Security Suite is displayed. The list can be searched.

2. Select an area.

© 2009-2014 Next Level Security Systems, Inc.

The Details Pane is displayed for that area.



The zones included in the selected area are listed in the Detail Pane.

a. Select a zone to view the Detail Pane from that zone.

b. Click **Close** in the zone's detail pane to return to the selected area's Detail Pane.

3. Click **Event Log** to view the events associated with this zone.
4. Click **Reports** to view reports associated with this zone.
5. Click **Add Camera**. See **Adding a Camera to a Zone or Area**.

25.2.2.1 Arming or Disarming an Area

An alarm for the area can be armed or disarmed from the buttons in the details pane.

The zones remain active, but an alarm is not triggered when a zones' sensor detects something. Alarms are triggered when a connected device detects an event, such as glass breaking, smoke, unexpected motion, etc.

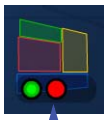
- Click **Bypass** in the Detail Pane for the selected area.
- Click **Disarm** to turn off the alarm for an area.

© 2009-2014 Next Level Security Systems, Inc.

25.2.2.2 Armed Setting Indicator

The right LED under the area icon indicates whether or not the area is armed.

- Red = Area is armed.
- Green = Area is not armed.



Armed setting indicator

Chapter 26: Configuring and Using Point of Sale

Point of Sale is an add-on features, that associates cash register transactions as events with live and recorded video available through an NLSS Gateway. Using the Point of Sale feature, users can monitor individual transactions and multiple cash registers from the NLSS Web Interface.

Note: The subscription for using Point of Sale must be enabled before using this feature. See **Enabling Other Premium Features** in **Chapter 17: Global Configurations**. After the subscription is enabled, the Point of Sale options are displayed in the NLSS Web Interface.

Using Point of Sale, each cash register transaction is recorded on the Gateway as an event. An associated camera or cameras records video of the transaction. Later, the transaction can be replayed, with the video synchronized to each purchase.

Transactions can be searched, filtered, and reviewed in the Events Log. See **Chapter 15: Monitoring and Handling Events** for instructions on using Events.

Transactions also can be monitored and reviewed from the Operations menu.

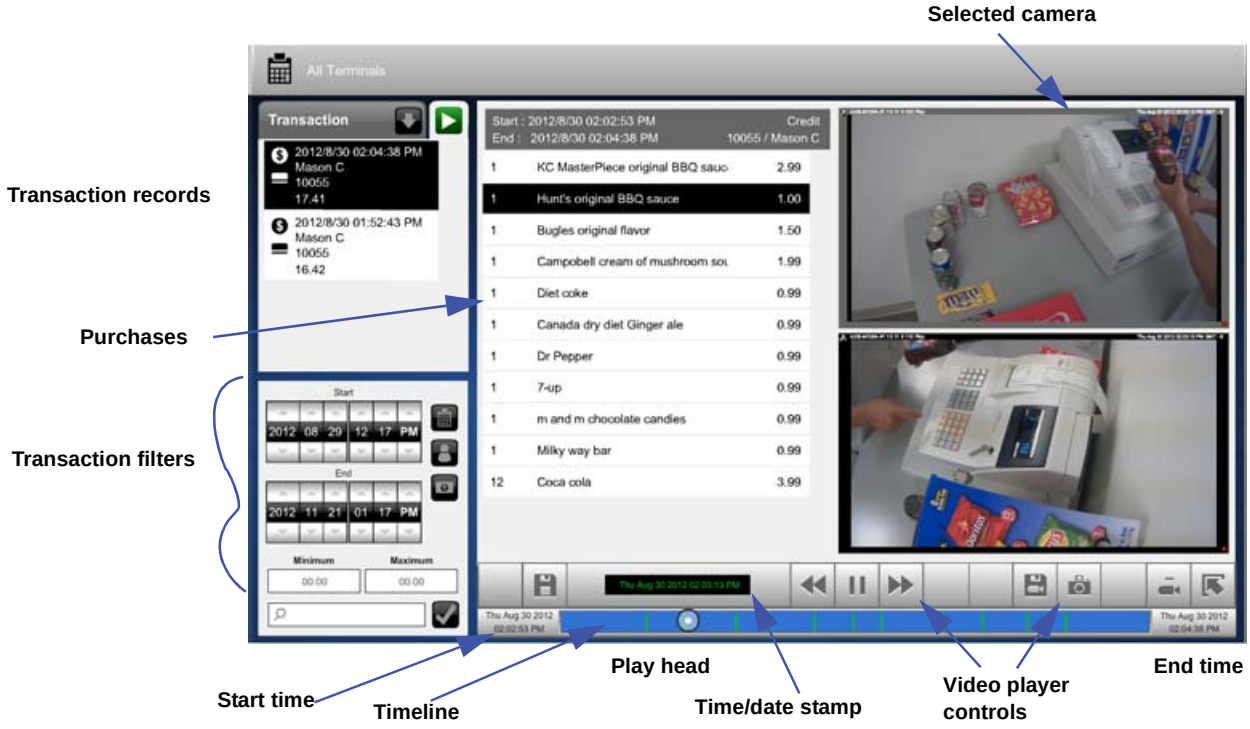
26.1 OPERATIONS

Point of Sale is accessed from the Operations menu. The Gateway's database is then searched for transactions.

1. Select **Operations > Point of Sale**.

© 2009-2014 Next Level Security Systems, Inc.

The Point of Sale window is displayed in the right pane.



2. Either live or recorded transactions can be displayed.
3. Current transactions are listed in the *Transaction* pane, with live video, as indicated by the **Pause Live** button.

   The Transactions list can be searched and filtered to locate previous transaction events.

   Several filters are available to locate the desired transaction.

   – **Start**/**End**: use the arrow buttons to set the date and time range for the search.This field must be set to a wide enough range to include transactions covered by the other filters.
   – **Minimum**/**Maximum** (optional): set a search range for the transaction total.
   – **Terminals** : click to display a dialog listing the terminals connected to the Gateway.
      » Select a terminal and close the dialog.
   – **Cashiers** : click to display a dialog listing the cashiers authorized to use the terminals.
   – **Tender** : click to display a list of transaction types, including: **Cash**, **Credit**, **Debit/ATM/**, **Gift Card**, **Store Credit**, or **unknown**. The
   – **Text**: enter text in the search field to locate transactions containing a certain item.
4. Search stored transactions.
   a. Set the search filters.
   b. Click **Search**.

A list of matching transactions is displayed in the *Transaction* pane. Each listing contains the time and date of the transaction, the terminal, cashier, and then length of the corresponding video.

c. Click **Hide** to hide the search and filter options to display more transactions in the list.

5. Select a transaction.

   The detailed transaction record is displayed in the left pane. The record contains the Start and End time of the transaction, the Tender (transaction type), terminal, and cashier.

   The items are listed, with the quantity purchased, and the unit price.

   The video of the purchase is also displayed. The video player controls the playback.

6. Select an item to see the video for that particular purchase.
7. Click **Play Live** to return to monitoring of live transactions.

26.1.1 Controlling the Video Player

The Point of Sale video player operates similarly to the full video player available from Operations > Cameras. Cameras also can be added from the video player.

Play

Rewind, Pause, Fast Forward: available when video is playing.;

Add a camera to a selected pane.

Delete a camera from a selected pane.

26.1.2 Exporting Transactions

The transaction record, video, or a snapshot can be exported from the Point of Sale video player. The features function the same as the export functions elsewhere in the NLSS Web Interface. The selected record or video is exported.

1. Click on a transaction record to select it. The selected is highlighted with a black background and white lettering.
2. Click on a video pane to select the video. The selected frame is highlighted by a gray rectangle.
3. Click the button for the desired export.

© 2009-2014 Next Level Security Systems, Inc.

4. Follow the prompts to save the file.

Export to .csv.

Export video. Exports the selected video clip for the entire transaction.

Export JPG. Exports a snapshot of the selected video.

26.2 CONFIGURATION

The Point of Sale feature is enabled and terminals (cash registers) are added and set up through the Configuration menu.

- Select **Configuration > Point of Sale**.

Two windows are available: **Terminal Interface** and **Terminals**.

26.2.1 Terminal Interface

The Terminal Interface defines the communications between terminals and the NLSS Unified Security Suite,

- Select **Configuration > Point of Sale > Terminal Interface**.

The *Terminal Interface* page is displayed. The only action available is setting retention times for grooming transaction records.

Just as with recorded video, transaction records can be groomed from the NLSS Gateway database. If the Gateway's storage hits 90% of capacity, the groomer deletes older records first to make room for new transactions.

Transaction events cannot be groomed if the item is locked in the Events Log. See **Lock State Toggle** in **Monitoring and Handling Events** for more information.

Separate settings can be made for cash and credit/debit transactions.

1. Use the arrow buttons to edit the Groomer settings as desired for the transaction type, either **Cash** or **Credit/Debit**.
   - **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.
2. Click **Save**

to keep the changes.
   - Click **Cancel**

to return to the previous settings.

26.2.2 Terminals

The Terminals window lists the terminals created by the NLSS Default POS API. This window is informational, and no editable fields are available.

© 2009-2014 Next Level Security Systems, Inc.

Chapter 27: NLSS Remote Management Services

NLSS Remote Management Systems (*RMS*) provides centralized configuration and management for NLSS sites (Gateways). Also, 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 that 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, the Gateway can be operated from the RMS 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 that Gateway. Those settings can then be applied to other Gateways in RMS system, as needed.

Before RMS can be run an a Gateway, a subscription ID (token) must be entered in *Configuration > Global > Subscriptions*. See **Configure Subscriptions** in **Chapter 17: Global Configurations** for instructions.

27.1 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 using a single browser from the Security Office, or another local or remote 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 Configuration > 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 Configuration > 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.

© 2009-2014 Next Level Security Systems, Inc.

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.

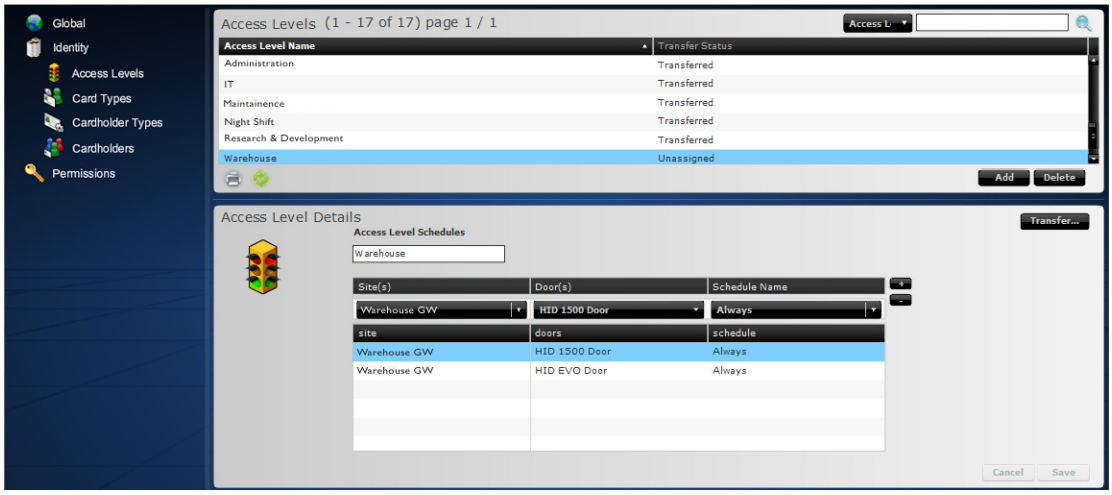
See **RMS Hierarchy** and **Logging In to the NLSS RMS Web Interface** for more information.

The RMS main window 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.

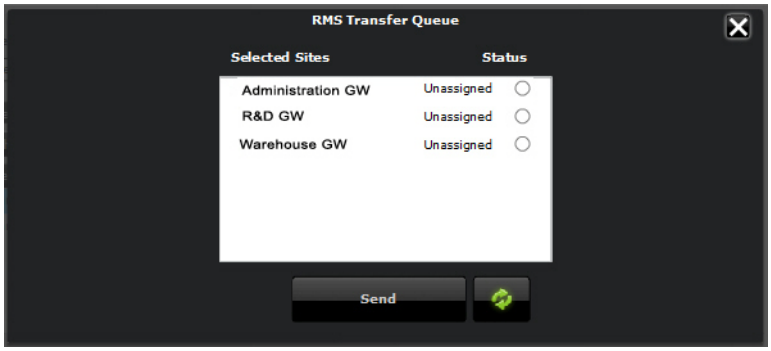
4. Create an Access Level called *Warehouse*, which only applies to the Warehouse doors.



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.

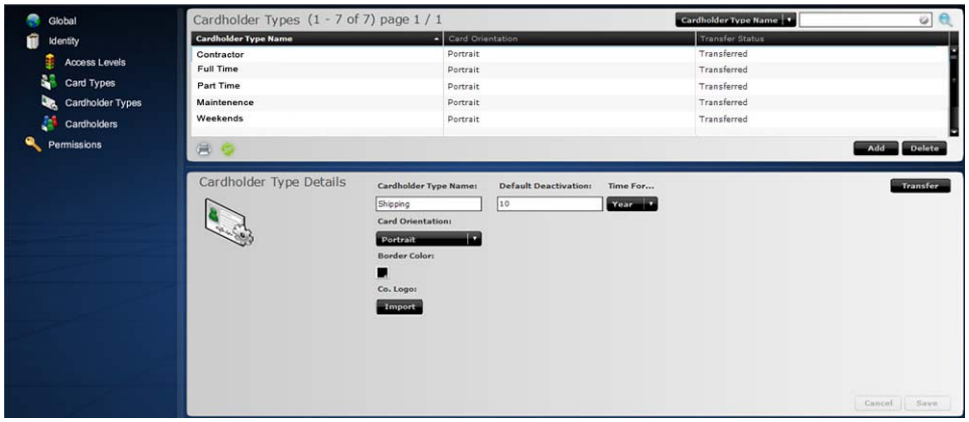


See **Transferring RMS Settings** for more information.

6. Create a Cardholder Type for the Warehouse employees. This cardholder type can be assigned to any Warehouse employee to provide access to the doors in that building.

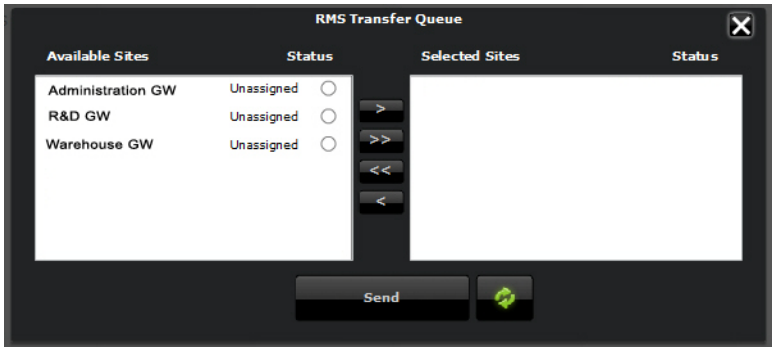
© 2009-2014 Next Level Security Systems, Inc.

Since Shipping and Receiving employees operate the Warehouse, create a Cardholder Type called *Shipping*, and apply the *Warehouse* access level. Any cardholder assigned the *Shipping* Cardholder Type receives access to the Warehouse doors.



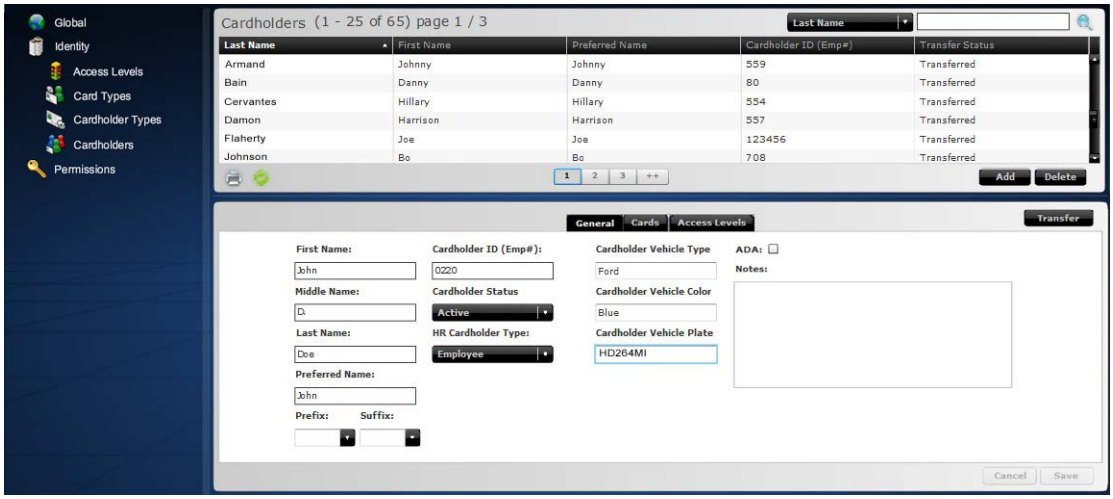
See **Cardholder Types** in for more instructions.

7. Transfer the *Shipping* Cardholder Type to the Warehouse Gateway. Cardholder Types are conditional, meaning the Gateways for transfer can be selected



See **Transferring RMS Settings** for more information.

8. Create a cardholder to print a badge for each employee in Shipping and Receiving.



9. Enter the Shipping Cardholder Type in the Credentials tab of the Cardholder window.
   See **Cardholders** for instructions.
10. Transfer the Cardholder settings to the Warehouse Gateway.
    See **Transferring RMS Settings** for more information.

27.2 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 for 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.

© 2009-2014 Next Level Security Systems, Inc.

27.3 LOGGING IN TO THE NLSS RMS WEB INTERFACE

The login for RMS is different than the login for locally accessing a Gateway.

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 window.
   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 reset from the login window.
      » Click Password Reset and follow the prompts.
   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.

27.4 RMS MAIN MENU

The RMS Main Menu contains seven options.

- **Volume**
- **Sites**
- **Operations**
- **Configuration**
- **Events**
- **Full Screen**
- **Log off**
- **Help**
- **Transcode**

© 2009-2014 Next Level Security Systems, Inc.

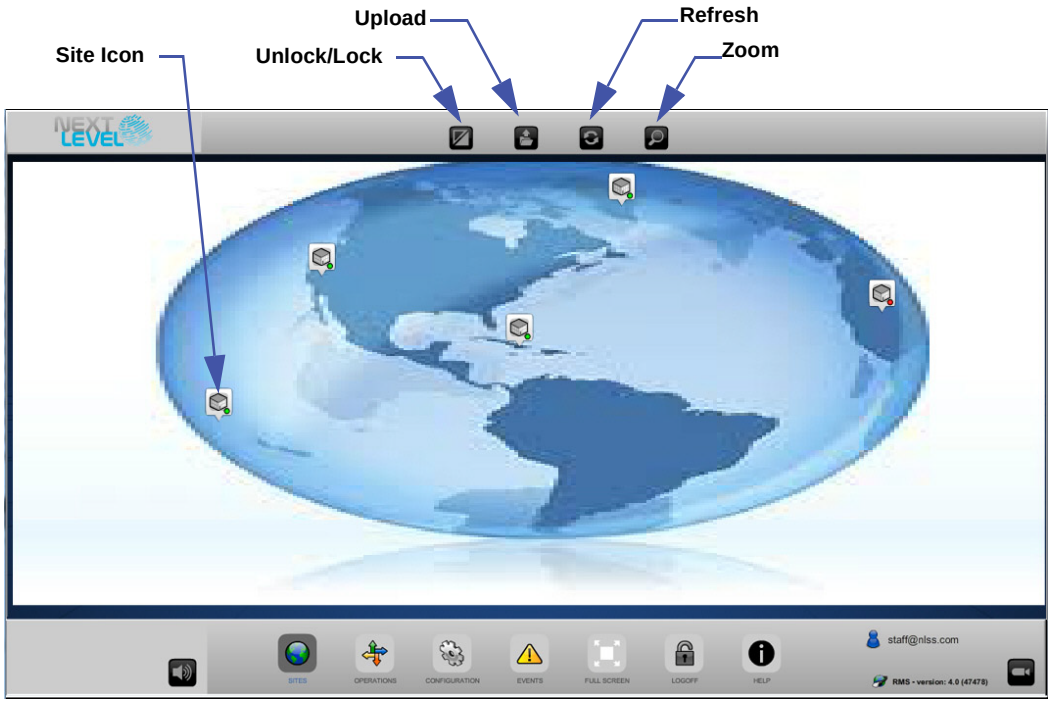
27.5 VOLUME

RMS can play an audio alert when an event occurs. Audio is associated with events using Actions and Event Linkages at the Gateway level. See **Configure Actions** and **Configure Event Linkages** in **Chapter 17: Global Configurations** for instructions.

- Click on **Volume** to open a slider to set the audio level for the alert that is played when events occur.

27.6 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.

  Image requirements: .png, 1300x800 @ 72dpi

- *Site icons* are automatically placed on the map when a site is added. A colored LED provides the status of the site.

  Mouse-over the icon to expand the label to display name of the site.

  – Green LED indicates that the site is accessible.

  – Red LED 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.

© 2009-2014 Next Level Security Systems, Inc.

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.
- **Refresh Map**: click **Refresh Map** to update the display.
- 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.

27.7 OPERATIONS

The RMS Web Interface Operations module has three options: **Media**, **Multiview** and **Groups**.

27.7.1 Media

Video clips exported from a camera to local Gateways are can be transferred to RMS for exporting. These clips then can be downloaded from the RMS Media Library to local storage.

- Select **Operations > Media** from the RMS Main Menu.

The video player in the right pane of the Media page operates the same as when accessing the Gateway directly. The RMS Media Library only contains files transferred from the Gateways.

Note: The default audio files are not automatically transferred to RMS.

- Video clips only can be downloaded at the RMS level. See **Download a Video Clip**.

- The Media Library for a Gateway accessed through RMS is slightly different than if the Gateway is accessed directly:
  - When a Gateway is accessed through RMS, a transfer option is available in place of the download option.
  - The transfer option is not available if a Gateway is accessed directly instead of through RMS, even if the Gateway is managed by RMS.
  - Delete and lock features are at the Gateway level for video exported from a camera. See **Chapter 10: Media Operations** for more information on delete and lock.
  - The player and download options are available in the RMS level Media Library. See **Chapter 10: Media Operations** for more information on the player.

Note: A transferred video clip remains in the RMS Media Library for 72 hours before it is automatically deleted from that library. The clip remains on the local Gateway until it is manually deleted, or groomed.

A clip deleted from RMS can be transferred again from the Gateway.

If the clip is deleted from the Gateway, a copy remains in the RMS Media Library for the designated 72 hours after it was transferred.

27.7.1.1 Transferring a Video Clip to RMS

When a clip is exported from a camera, it can transferred to RMS for viewing or exporting. Even though a video file is deleted automatically from RMS after 72 hours, it can be manually transferred to the RMS Media Library from the Gateway.

Note: Do not attempt to manually transfer a clip while it is being exported from a camera, as indicated by the icon with the rotating arrow. The clip is automatically transferred from the Gateway to the RMS Media Library.

When the transfer is complete, an email is sent to the logged in user.

The clip may be listed in the RMS Media Library before the transfer is complete. The video player displayed in the right pane if the clip is selected when the transfer is complete. Do not attempt a manual transfer if the automatic transfer is not complete.

1. Access a Gateway through the Sites map.
2. Select **Operations > Media**.
3. Select a video file.
4. In the right pane, click **Transfer to RMS**.

27.7.1.2 Export a Video Clip

When a Gateway is accessed through the RMS Sites map, video clips can be downloaded after transfer to the RMS Media Library.

When a clip is exported from a camera on a Gateway accessed through RMS, the video clip is exported to that Gateway's Media Library, and from which it can be transferred to the RMS Media Library. The clip then can be downloaded from the RMS Media Library. See **Downloading a Video Clip**.

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

© 2009-2014 Next Level Security Systems, Inc.

See **Export Video** in **Chapter 4: Controlling Cameras** for instructions on exporting video.

When a video clip is successfully exported to RMS, an email is sent to the user logged into RMS. See **Downloading a Video Clip**.

27.7.1.3 Downloading a Video Clip

When Gateways are accessed through RMS, clips are downloaded from the RMS media Library, not at the Gateway level. However, clips can downloaded from the Gateway's Media Library, if the Gateway is accessed through its local interface, not through RMS.

An email message is sent to the user logged into RMS, after the clip has successfully transferred to RMS. The email message contains a link to download the file.

For example:

On Aug 17, 2012, at 2:28 PM, info@nlss.com wrote:

Start Time: 08/17/2012 02:10:24 PM

End Time: 08/17/2012 02:15:48 PM

https://rms.site.com/export/c31/ab34e567-c8120-j56t-bb92-21db5db20128/SS7.mp4

- Click the link to in the email message to download the file.

27.7.1.3.1 Manually Downloading a Video Clip

A clip also can be downloaded from the NLSS RMS Web Interface, at the RMS level.

1. Select **Operations > Media** from the RMS Main Menu.
2. Select a clip.
3. In the right pane, click **Download File**.
4. Follow the prompts in the browser to download the file.

© 2009-2014 Next Level Security Systems, Inc.

27.7.2 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 cameras from multiple sites to be grouped together for quick access. By default, no Views are configured for the NLSS Web Interface.

1. Select **Operations > Multiviews** from the Main Menu.
2. Click **Add** to display a *New View* window.
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 sites.
   – A light gray frame highlights the selected pane.
6. Select a site to display a lists of cameras and streams available from that Gateway.
   – 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.
7. 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.

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

27.7.3 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. In 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, which can be displayed in a list or on a map or floor plan. See **Chapter 14: Using Groups** for instructions on using Operations > Groups.

27.8 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.

27.8.1 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 are added, edited, and deleted through the Gateway.

Parameter	RMS Controlled?	Transfer	RMS Configuration Options
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	—	—

© 2009-2014 Next Level Security Systems, Inc.

Parameter	RMS Controlled?	Transfer	RMS Configuration Options
Event Action Linkages	No	—	—
Actions	No	—	—
Identity			
Access Level	Yes	Multiple unique sites	Add/Delete/Edit
Cardholders	Yes	Conditional	Add/Delete/Edit
Card Types	Yes	Conditional	Add/Delete/Edit
Cardholder Types	Yes	Conditional	Add/Delete/Edit
User Defined	Yes	Unconditional	Edit only
Access Control	No	—	—
Video	No	—	—
Permissions			
Groups[a]	No	No	Add/Delete/Edit
Roles	Yes	Conditional	Add/Delete/Edit
Users	Yes	Conditional	Add/Delete/Edit

a. Groups can be created at the RMS level, but *only apply to the RMS level*. Site groups are separate, and created and configured at the site level.

27.8.1.1 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.

© 2009-2014 Next Level Security Systems, Inc.

27.8.2 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 initial setting.

Menu Option	Initial Setting	Dependent Setting
Global	Holidays	Schedules
	Event Severity	Event Type
Identity	Schedules	Access Levels
	Cardholder Type	Cardholders > Credentials
	Access Levels	Cardholders > Access Levels
	Access Levels, Card Types	Cardholder Types
	Cardholder-User Defined	Cardholders > User Defined
Permissions	Roles	Users

27.8.3 Transferring RMS Settings

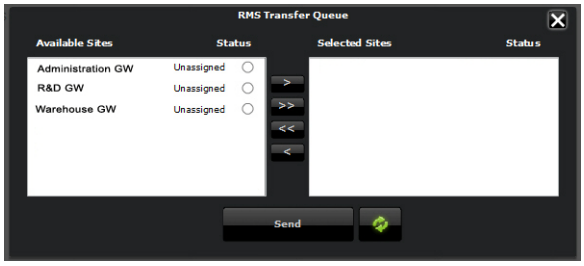
After a setting is added or edited in RMS, it must be transferred to the sites to be applied. Conditional settings can be transferred to selected sites, while unconditional settings only can be transferred to all sites. The transfer capability is indicated in the RMS Transfer Queue. The **Transfer Status** 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. Select the setting.
2. 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.

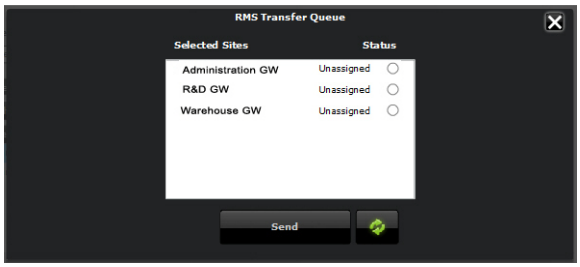


Important: Note that all sites to which the setting is applied must be placed in the **Selected Sites** (right) column, *even if the role has been previously applies to the site*.

This dialog configures to which sites a setting is applied. If a site remains in the Available Sites (left) column, the setting is not applied, and *it is removed from the site if it was previously applied*.

© 2009-2014 Next Level Security Systems, Inc.

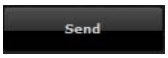
– If a setting is unconditional, a single column listing the sites is displayed. Skip to step 3.



3. 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**.

4. Click **Send** to confirm the transfer of this setting to the sites.



5. Click **Close** to exit the dialog.

27.8.3.1 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 all specified sites.
Processing	Yellow	At least one transfer is still processing, and there are no errors.
Error	Red	RMS reached the Gateways, but was unable to transfer the record successfully to at least one site.
Stopped	Red	The record is being transferred to the sites, 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.

© 2009-2014 Next Level Security Systems, Inc.

27.8.4 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 17: Global Configurations**.

27.8.4.1 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.

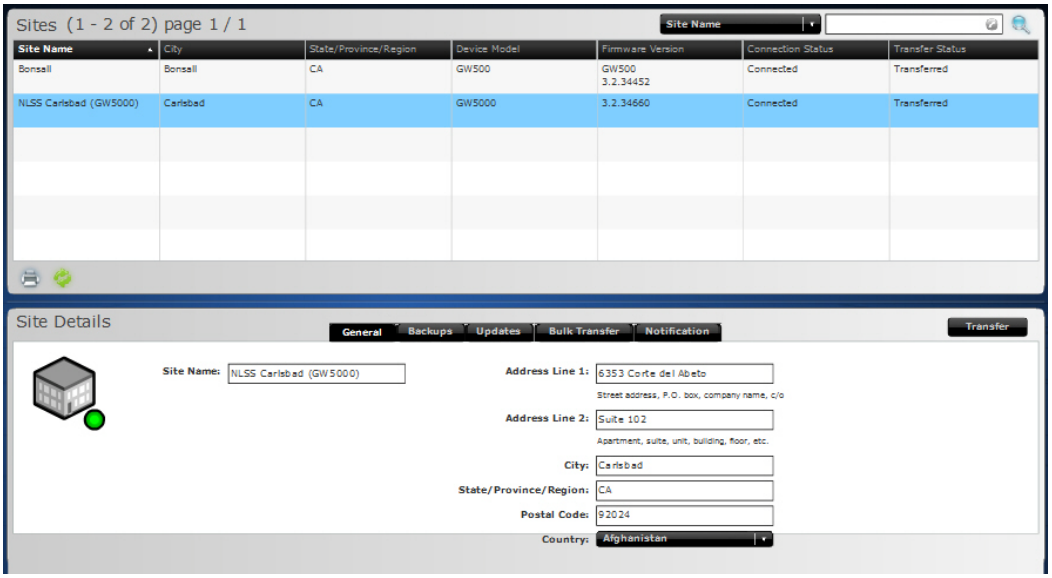
27.8.4.2 Sites

Site information is transferred from the RMS level to the local sites. At the RMS level, the *Configuration > Global > Sites* window lists the sites managed by RMS.

Sites cannot be added manually. Sites are discovered by RMS when the *RMS subscription ID* is entered in the *Configuration > Global > Subscriptions* window for a Gateway. See **Enabling RMS** in **Chapter 17: Global Configurations** for more information.

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

   The *Configuration > Global > RMS* window is displayed.



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 16: General Configuration Functions** for instructions.

Note: If a site is not appearing in the Sites list, ensure that the Gateway is registered with RMS. The listed sites have a subscription ID entered at the local Global > Sites window, and are managed by RMS. See **Enabling RMS** in **Chapter 17: Global Configurations**.

© 2009-2014 Next Level Security Systems, Inc.

27.8.4.2.1 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 settings can be reapplied easily from RMS. This tab is not available at the site level.

1. Select **Configuration > Global > Sites** from the Main Menu.
2. Select a **Site Name**.
3. Open the **Backup** tab.

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

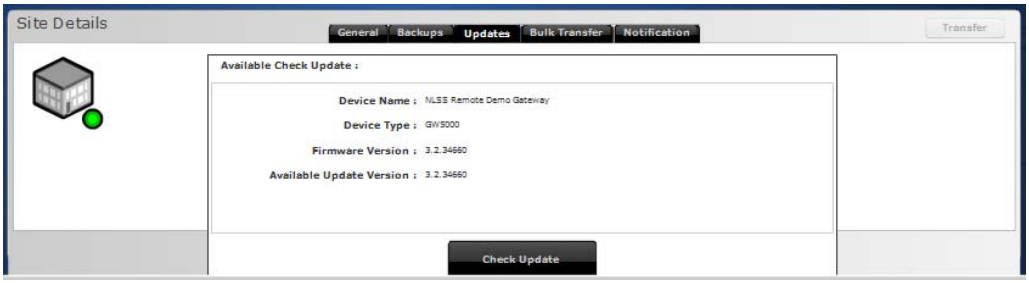
Remote Check Update allows the Check Update feature to be run for a selected Gateway at the RMS level, the same as running Check Update at the local level from *Configuration > Global > Gateways*.

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.

© 2009-2014 Next Level Security Systems, Inc.

3. Open the **Updates** tab.



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

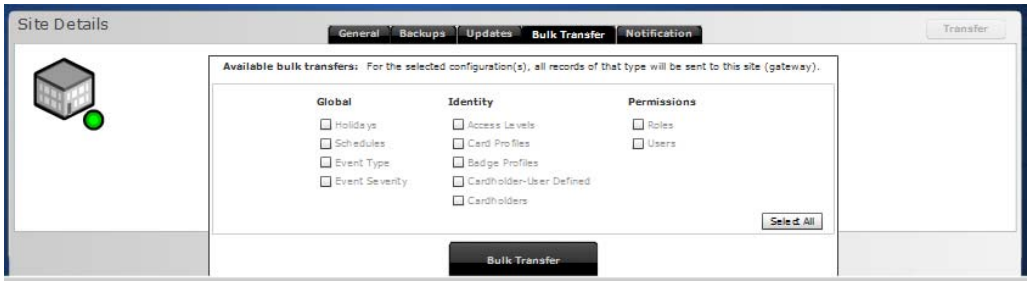
The Bulk Transfer tab simplifies the process of updating settings for a Gateway. Instead of running a Transfer for each setting, Bulk Transfer allows a group of settings to be pushed simultaneously to the selected Gateway.

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.



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 in 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 off line, the Bulk Transfer executes as soon as the site comes back on line.

NOTIFICATION TAB

The **Notification** tab provides configuration to prompt the system to send an email notification if the selected site goes off line.

1. Select **Configuration > Global > Sites** from the Main Menu.
2. Select a **Site Name**.
3. Open the **Notification** tab.

4. Check **Send Email Notification**.
5. Enter an **Recipient Email** address.
6. From the drop-down list, select an **Interval** to send the notification while the gateway remains off line.

27.8.4.3 HOLIDAYS

Holidays can be transferred to all sites simultaneously, or to selected sites.

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

   The *Holidays* window 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 17: Global Configurations** for descriptions of the Holidays fields.

Holidays can be added, edited, deleted and searched. See **Chapter 16: General Configuration Functions** for instructions.

© 2009-2014 Next Level Security Systems, Inc.

27.8.4.3.1 Dependencies

- Holiday settings must be transferred before Schedule settings can be transferred.

27.8.4.3.2 Transferring Holidays

Holidays are conditional settings. Settings can be applied to all or selected sites.

See **Transferring RMS Settings** for instructions.

27.8.4.4 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 17: 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 16: General Configuration Functions** for instructions.

27.8.4.4.1 Dependencies

- Holiday settings must be transferred before Schedule settings can be transferred.

27.8.4.4.2 Transferring a Schedule

Schedules are conditional settings. Settings can be applied to all or selected sites.

See **Transferring RMS Settings** for instructions.

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

27.8.4.5 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 all site to provide consistency.

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 17: Global Configurations** for descriptions of the fields.

See **Configure Event Types** in **Chapter 17: 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.

© 2009-2014 Next Level Security Systems, Inc.

Event Types cannot be added or deleted, but can be edited and searched. See **Chapter 16: General Configuration Functions** for more information.

27.8.4.5.1 Dependencies

- Event Severity settings must be transferred before Event Type settings are configured and transferred.

27.8.4.5.2 Transferring Event Types

Event Type settings are unconditional. Settings are transferred to *all* sites managed by RMS, and cannot be applied to selective sites.

See **Transferring RMS Settings** for instructions.

27.8.4.6 Event Severity

Event Severity allows names to be assigned to event levels. See **Configure Event Severity** in **Chapter 17: 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 16: General Configuration Functions** for instructions.

27.8.4.6.1 Dependencies

- Event Severity settings must be transferred before Event Type settings are configured and transferred.

27.8.4.6.2 Transferring Event Severity

Event Severity settings are unconditional. Settings are transferred to *all* sites managed by RMS, and cannot be applied to selective sites.

See **Transferring RMS Settings** for instructions.

© 2009-2014 Next Level Security Systems, Inc.

27.8.5 Identity

Configuration > *Identity* provides control of identity information and credentials for users and cardholders of each site. See **Chapter 18: Configure Identity and Credentials** for more information on Identity menu options.

27.8.5.1 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 an Access Level applied from RMS.

See **Configure Access Levels** in **Chapter 18: 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 18: 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 16: General Configuration Functions** for instructions.

27.8.5.1.1 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.

27.8.5.1.2 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* window.

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.

© 2009-2014 Next Level Security Systems, Inc.

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.

27.8.5.2 Card Type

Cardholders use cards to access one or more doors in the NLSS system. *Card Types* 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, Card Type can be transferred to all sites simultaneously, or to selected sites.

1. Select **Configuration > Identify > Card Type** from the Main Menu.
   The *Card Types* table lists the cardholders entered in the system.
2. Click on a **Card Type**.
   The *Card Type Details* are displayed. See **Card Types Details** in **Chapter 18: Configure Identity and Credentials** for a description of the fields.

Card Types can be added, edited, deleted and searched. See in **Chapter 16: General Configuration Functions** for instructions.

27.8.5.2.1 Dependency Notes

- Access Levels and Card Types settings must be transferred before Cardholder Type settings can be transferred.

27.8.5.2.2 Transferring Card Types

Card type settings are conditional. Settings can be applied to all or selected sites.

See **Transferring RMS Settings**.

© 2009-2014 Next Level Security Systems, Inc.

27.8.5.3 Cardholder Types

Configuration > Identity > Cardholder Type 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 windows. See **Configure Cardholder Types** in **Chapter 18: Configure Identity and Credentials** instructions.

In RMS, Cardholder Types can be applied to all sites simultaneously, or to selected sites.

1. Select **Configuration > Identify > Cardholder Types** from the Main Menu.

   The *Card Type* table lists the cardholders entered in the system.

2. Click on a **Cardholder Type**.

   The *Cardholder Type Details* pane is displayed. See **Cardholder Types Details** in **Configure Identity and Credentials** for a description of the fields.

Cardholder Types can be added and edited. See **Transferring Cardholder Types**. Card Types also can be deleted and searched. See **Delete Items** and **Searching Tables** in **Chapter 16: General Configuration Functions** for instructions.

27.8.5.3.1 Dependency Notes

- The Cardholder Type settings must be transferred before Cardholders Credentials settings can be transferred.
- Access Levels and Card Types settings must be transferred before Cardholder Type settings can be transferred.

27.8.5.3.2 Transferring Cardholder Types

Cardholder Type settings are conditional. Settings can be applied to all or selected sites.

See **Transferring RMS Settings**.

27.8.5.4 Cardholders

Configuration > Identity > Cardholders provides the fields needed to set up access and details for individuals with access badges. See **Configure Cardholders** in **Chapter 18: Configure Identity and Credentials** for more information.

In RMS, Cardholders can be applied to all sites simultaneously, or to selected sites. Lists of cardholders also can be imported from a .csv file

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 16: General Configuration Functions** for instructions.

© 2009-2014 Next Level Security Systems, Inc.

27.8.5.4.1 Dependencies

- The Cardholder Type 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.

27.8.5.4.2 Transferring Cardholders

Cardholder settings are conditional. Settings can be applied to all or selected sites.

See **Transferring RMS Settings**.

27.8.5.4.3 Uploading a Multiple Cardholders

A list of cardholders also can be uploaded from a .csv file. The *Cardholders.csv* file lists the cardholders for the database.

Important: The .csv file must be zipped before it is uploaded.

The column headers in the file represent the fields in the tabs in the Details pane of the *Configuration* > *Identity* > *Cardholders* screen. See **Cardholders Tabs** in **Chapter 18: Configure Identity and Credentials** for definitions of the fields.

The .csv file must have the columns listed below, in this order, to identify the cardholders in the database.

- The columns names for the .csv file are listed in order, by row, left to right, and down.
- Employee number (**p.employeeNumber**) is the *Primary Key* in the system for this cardholder. The system does not allow duplicates.
- Use only alpha-numeric characters, with no special characters (_, -, ., #, etc.) and no spaces.
- Complete as many columns as desired to simplify entering a large number of cardholders into the system.

p.employeeNumber	p.prefix	p.suffix	p.firstName
p.middleName	p.lastName	p.preferredName	p.title
p.location	p.department	p.supervisor	p.cardholderType
p.cardholderStatus	p.PIN	p.ADA	p.enableTrace
p.notes	cd1.embossedNumber	cd1.cardNumber	cd1.badgeProfile
cd1.cardStatus	cd1.activationDate	cd1.deactivationDate	cal1.accessLevel
cal2.accessLevel	cal3.accessLevel	pv.vehicleType	pv.vehicleColor
pv.vehicleLicensePlate	pe1.type	pe1.emailAddress	pp1.type
pp1.phoneNumber	sms1.smsNumber		

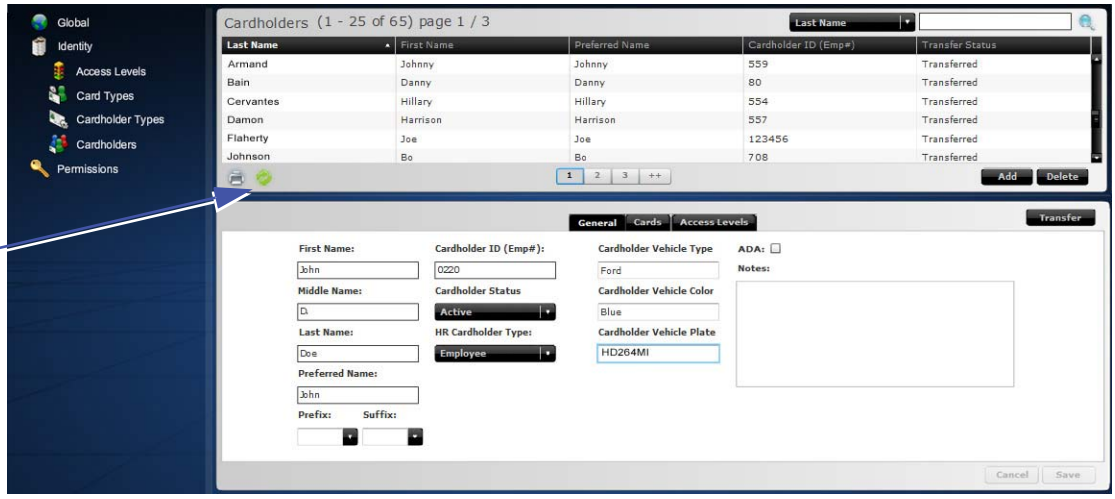
© 2009-2014 Next Level Security Systems, Inc.

IMPORTING A DATABASE

Import the zip file containing the database components through the Configuration module.

1. Log into RMS.
2. Select **Configuration > Identity> Cardholders**, from the Main Menu.

   The *Cardholders* window is displayed.



3. Click **Import/Export**.

   The *Import/Export Face Recognition* dialog box is displayed.

   – A **Sample Template** of the .csv file can be downloaded from this dialog box by clicking **Download** under the Import button.

4. Click **Import**.

   The *File Uploader* dialog box is displayed.

5. **Browse** to select a zip file.
6. Click **Upload**.

Note: If an error occurs while importing a .zip file, check the **Import Log** by clicking **Download** at the top of the dialog box.

The contents of the .zip file are added to the Cardholder database in RMS.

© 2009-2014 Next Level Security Systems, Inc.

27.8.6 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 the RMS level must be pushed down to the local Gateways if that user is allowed to access those Gateways.

See **Chapter 21: Configuring Permissions** for more information on Permissions, and instructions on creating, editing and deleting permissions.

27.8.6.1 Setting Up Groups in RMS

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 21: Configuring Permissions** for instructions on creating, editing, and deleting Groups.

See **Chapter 14: Using Groups** for instructions on using Groups.

27.8.6.2 Setting Up Roles in RMS

Roles define the capabilities of the users operating the NLSS Gateway. The *Configuration* > *Permissions* > *Roles* window provides capabilities to manage roles.

Roles can be applied to all sites simultaneously, or to selected sites.

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 21: Configuring Permissions** for more information and instructions on adding, editing and deleting roles.

© 2009-2014 Next Level Security Systems, Inc.

27.8.6.2.1 Role Details

See **Roles Details** in **Chapter 21: 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**: these modules are the top level modules available in the RMS Main Menu. These modules are Sites, Operations, Configuration, and Events.

Note: Access to these modules at the Gateway level is set in the Gateway Modules tab.

- **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.

27.8.6.2.2 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.

27.8.6.2.3 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**.

27.8.6.3 Setting Up Users in RMS

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 21: Configuring Permissions** for more information.

© 2009-2014 Next Level Security Systems, Inc.

27.8.6.3.1 Dependencies

- A Role assigned to a user must be transferred before the user is transferred.

27.8.6.3.2 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**.

27.9 EVENTS

Emergency and Critical Events at the Gateway level are propagated up to the RMS level.

Severity settings are assigned to an **Event Type** at the RMS level and unconditionally transferred to all sites. Emergency or Critical can be assigned to any Event Type. See **Event Type** earlier in this chapter for instructions.

Visibility of events is also dependent on the role assigned to the User who is logged into the Web Interface. Events must be selected in the RMS Modules tab of Configuration > Permissions > Roles. See **Setting Up Roles in RMS** earlier in this chapter and **Roles** in **Chapter 21: Configuring Permissions** for instructions.

27.9.1 RMS Event Log

The RMS Event Log and Event Details windows contain the same functions as available at the site level. See **Event Log** in **Chapter 15: Monitoring and Handling Events** for more instructions.

27.10 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 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.

© 2009-2014 Next Level Security Systems, Inc.

27.11 LOG OFF

Click **Logoff** in the Main Menu to close the current RMS session. The Login window is displayed.

Note that clicking the Back button in a browser also logs off the user from the NLSS Web Interface.

27.12 HELP

RMS includes a help system to provide detailed configuration and operation instructions for both the RMS interface, and the local Gateway interface.

- Click **Help** in the Main Menu.

The help system is displayed in a new tab.

27.13 TRANSCODE

Just as with the local Gateway, all video displayed in RMS can be set to a lower resolution if bandwidth usage becomes an issue.

Note: This button is hidden when the video player is displayed.

- Click **Transcode** in the RMS main menu before opening a video player.

The frame rate, bit rate and resolution are adjusted to alleviate bandwidth issues. The quality of the video also reflects the setting.

The camera icon in the transcode button becomes smaller to reflect the lower resolution.

- Click **Transcode** again to return to the camera setting for the video.

Important: Selecting these settings at the RMS level impacts all video through this RMS session.

If the transcode setting is changed at a 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.

The setting does not impact other users, when they log into RMS.

© 2009-2014 Next Level Security Systems, Inc.

Chapter 28: Next Level Mobile Application

The *Next Level Mobile Application*, or *NextMobile*™, provides smart phones and tablet computers with access to Remote Management Services (RMS), NLSS Gateways, and Decoders.

NextMobile provides access to devices managed by the local Gateway, plus cameras, and stored video clips.

NextMobile provides live video by accessing a camera, or a device associated with a camera, such as a door, input or output device, or an intrusion zone or area. If accessed via RMS, recorded video is also available.

Other app features include:

- Search and update events.
- Remotely open doors and view associated cameras.
- Stream video from a mobile device to an NLSS Gateway, via NextProtect®.

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.

NextMobile does not provide the Configuration options that are available in the NLSS Web Interface. Access these options though the Gateway, or RMS interface.

Important: To connect to a local NLSS Gateway, or Decoder, the mobile device must have a wireless connection to the network on which the device resides. The RMS connection requires wireless or Internet access.

Note: NLSS Gateways must be configured before the NextMobile app can be used. See the **Part 3: System Configuration** for instructions.

This chapter includes:

- **Supported Mobile Devices**
- **Navigating the NextMobile App**
- **Searching a List**
- **Using the Video Player**
- **Events**

© 2009-2014 Next Level Security Systems, Inc.

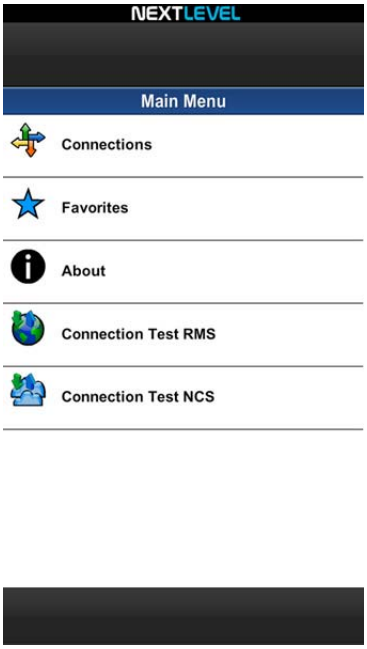
28.1 SUPPORTED MOBILE DEVICES

NextMobile supports the following mobile devices.

Platform	OS Version	Device
Apple	iOS 4.3 - 7.1	• iPhone 3S, 4, 4s, 5, 5s, 5c • iPad 1,2,3 • iPod 2nd gen and up
Android	Froyo (2.2 and up) Gingerbread (2.3 and up) Honeycomb (3.0 and up) Ice Cream Sandwich (4.0 and up) Jelly Bean (4.1 and up) KitKat (4.4 and up) **NOTE**: It is recommended that the latest level of a version be used. For example: 2.2.3 for Froyo, 4.3 for Jelly Bean, etc.	• Phones and tablets are supported.

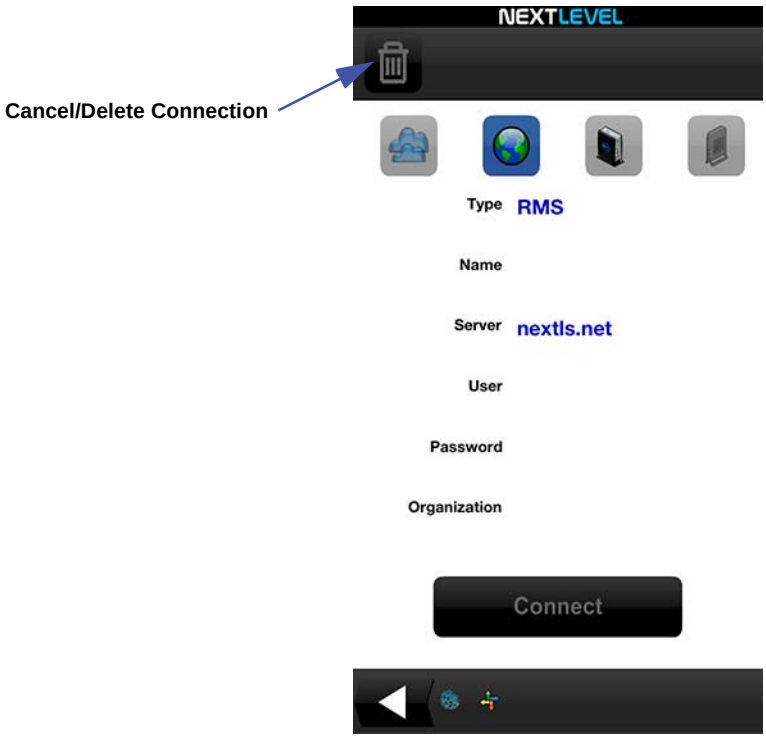
28.2 GETTING STARTED

1. Download the *NextLevel* app (*NextMobile*) from an app store. The download is free.
   – The app is available from the Apple App Store, or Google Play.
   – Search for **nextlevel**.
2. Install the app according to the standard installation procedures for the mobile device.
3. Launch the app. The *Main Menu* is displayed.



4. Tap **Connections**. The *connections* screen is displayed.
5. Tap **Add Connection** to create a connection for the mobile app.

A blank connection screen is displayed with options for the type of connection.



6. Select an option:
   – **RMS**: an Remote Management Services. The app accesses RMS from the top level.

   – **Gateway**: a local Gateway on the same network as the device.

   – **Decoder**: an NLSS Decoder on the same network as the device. The app allows video from Display, Channel, View, or Sequence to be set to active for a decoder.

Important: Be sure to set the decoder to *Enable HTTP* to allow NextMobile to access the decoder. See the *NLSS HD Decoder User Manual* for instructions. This manual is available from the NLSS Support web site: **support.nlss.com**.

7. Complete the fields to identify and verify the connection. The fields are the same for each connection, except for an added *Organization* field for RMS.

© 2009-2014 Next Level Security Systems, Inc.

a. **Name**: enter a unique name to identify the connection in NextMobile.

   The name is only assigned as an identifier for the mobile device, and is not propagated to the connected system.

   The remaining fields must be completed according to the user's settings configured in RMS, or through the local Gateway, or on the Users page on the decoder web interface.

   See **Users** in **Chapter 21: Configuring Permissions** for more information. Decoder information is contained in the NLSS Decoder User Guide.

b. **Server**: enter the URL for RMS, or an IP address for the Gateway, or Decoder to establish a connection.

   This field is the web address for the RMS portal, as provided by the partner who set up the RMS service, such as *rmscloud.com*.

Note: The full URL entered in a browser contains the organization name, as described below. That name *does not* need to be included in the Server URL when making a connection in the mobile app.

Note: Do not include **http://** in the Server field.

c. **User**: the user name required to log into the connection.

d. **Password**: the password required for this user name.

e. **Organization**: (RMS only) a name assigned to the collection of Gateways monitored remotely.

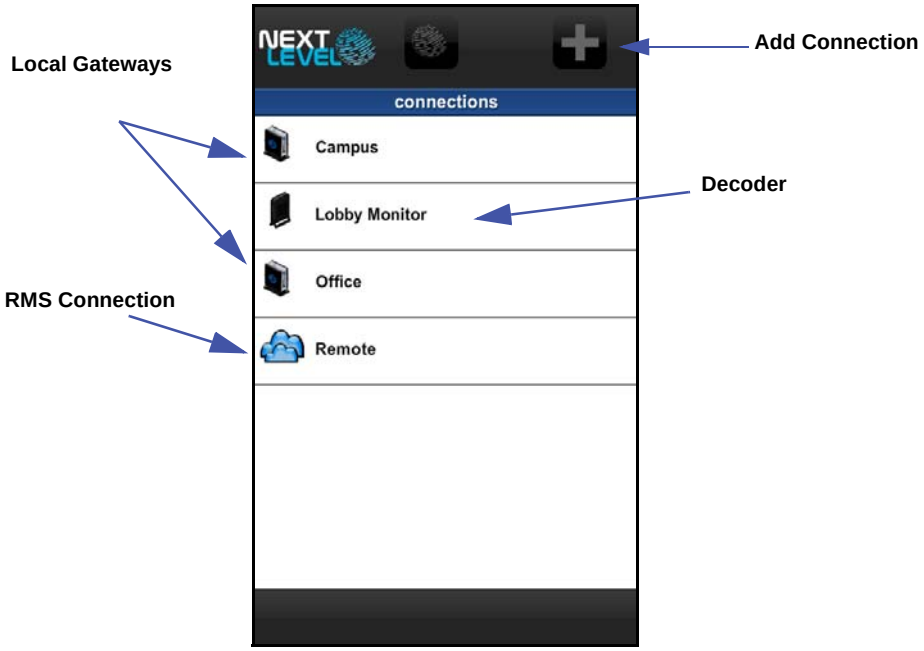
   The organization is defined in the RMS URL, such as *rmscloud.com/mycompany*, where *mycompany* is entered in the Organization field.

8. Tap **Connect**.

   » Tap **Cancel/Delete** in the top menu to exit the connection settings without saving. This button is also used to delete an existing connection.

© 2009-2014 Next Level Security Systems, Inc.

The connection is added to the list.



The user can only see features that have been assigned through RMS or the local Gateway using Configuration > Permissions. See **Chapter 20: Configuring Permissions** for instructions.

Multiple connections can be added the list. For example, if a device is managed by RMS, that Gateway, can be included, along with the RMS system to which the device is associated.

28.3 NAVIGATING THE NEXTMOBILE APP

1. Open **NextMobile**.
2. Tap **Connections**.
3. Select a **connection**.

   The login screen is displayed with the credentials already entered.
4. Tap **Connect**.

   Options are displayed according to the users permissions.

Navigation features include:

- As the screens are navigated, icons (*breadcrumbs*) are displayed at the bottom of the list screens to display the navigation path.

Breadcrumb icons

Breadcrumbs are not displayed when the full screen video player is displayed. Close the full screen view to access breadcrumbs again.

- Use the **Back** button to return to the previous screen.

- Lists can include multiple pages. Use the arrow buttons at the bottom of the screen to navigate between pages.

28.3.1 RMS Options

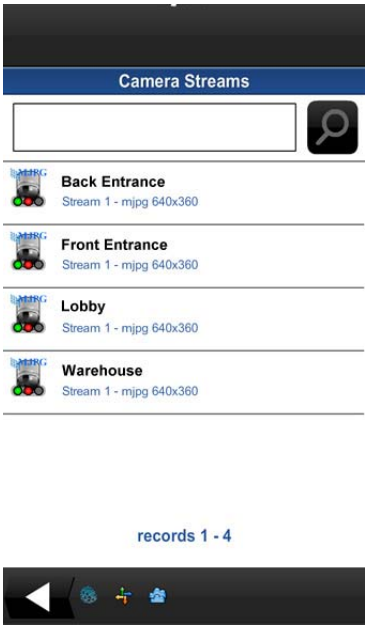
If using an RMS connection, four top level buttons are displayed.

	Sites: accesses a list of Gateways and Cloud Cameras registered with RMS.
	Multiview: accesses a list of views available at the top level of RMS. These views can be from one or multiple sites.
	Media: accesses a list of video clips exported from the registered Gateways.
	Groups: accesses a list of groups created for RMS. These groups include collections of Multiviews, Gateways and Cloud Cameras managed by RMS, plus site-based groups configured at the Gateway level.

28.3.2 Device Navigation

If a Gateway connection, or a Gateway under RMS, is selected, the local gateway Operations menu options are displayed. The list can be scrolled.

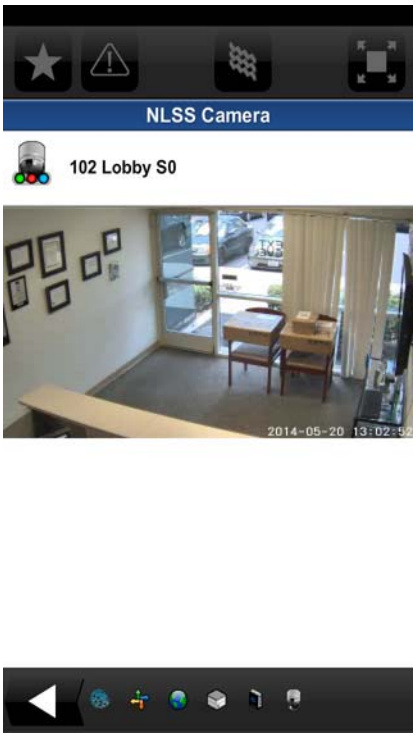
1. Tap the **Camera Streams** icon to open a list of video streams. All lists can be searched. Longer lists can be scrolled.



The path for each item is *option* > *list* > *item* > *video player* (if applicable).

2. Tap a stream to display its screen, and associated video, if available.

Camera viewer



Three options are available at the top of the page when a stream is selected in the local Gateway view:

Events

Favorites

Full Screen

These options are discussed later in this chapter.

Events are also displayed as in the Operations menu of the NLSS Web Interface. Access to Events are controlled by permissions set in the Web Interface's configuration menu. See **Chapter 20: Configuring Permissions** of the *NLSS Unified Security Suite User Manual* for more information.

The options vary in the item screen, depending on the type of item selected. The table below lists the options available for each menu item. See the respective sections earlier in this manual for instructions on using these options.

Icon	Options
	cameras: events

© 2009-2014 Next Level Security Systems, Inc.

Icon	Options
	decoders: events
	doors: events, open, unlock
	Cardholders/Users: events, card list
	Views
	Media: play , stop , volume/mute
	Input Devices: events
	Output Devices: events, activate , deactivate
	Groups: depends on items in group
	Areas: events, arm , disarm
	Zones: events, bypass , reset

- See **Using the Video Player** for instructions on using the video player.
  - If video is available for an stream, the **Transcode** option is displayed. **PTZ** presets also are available, if the camera is configured for that feature.
- Swipe a screen to go to the next or previous stream in the list. The list screen does not need to be accessed to go to a different stream.

© 2009-2014 Next Level Security Systems, Inc.

28.4 FAVORITES

Preferred locations in the app can be marked as a favorite for easier access.

1. Navigate to the desired page.
2. Tap the **Favorites** button at the top of the page.
   The preferred location is added to the *Favorites* list.
3. Return to the *Main Menu*.
4. Tap **Favorites**. The new location is displayed in the *Favorites* list.

28.5 SEARCHING A LIST

Lists can cover multiple pages. To simplify locating an item, a Search function is included.

1. Access a list.
2. Tap in the **Search** field.
3. Use the pop-up keyboard to enter the search criteria.

4. Tap **Search**.
5. Select the desired item.
6. To display all items in the list again:
   a. Tap **Clear** to reset the **Search** field.
   b. Tap **Search** again.

28.6 USING THE VIDEO PLAYER

Video can be viewed by selecting a camera from the Cameras list, or by selecting a menu option, such as a view or door, that has items with a camera or video stream assigned.

1. Open **NextMobile**.
2. Open a **connection**.

   See **Device Navigation** for more information.

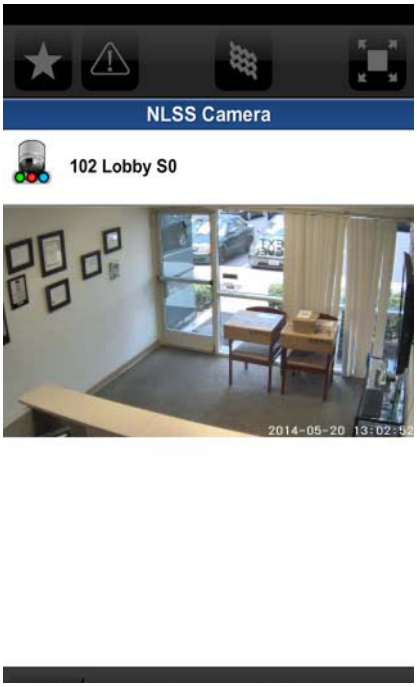
   – If using RMS, navigate down.

   » Select **sites** or **groups** to navigate to a site to access cameras.

   » Select **multiviews** to access customized displays for the system.

   See **RMS Options** for more information.
3. Select Cameras. Doors, Views, Sequences, Input Devices, Output Devices, and Groups can also be selected, if a camera is associated with the device.
4. Select a stream, or an item with an active camera or video stream assigned. Live video is displayed. The options in the screen vary slightly between devices, depending on the options available for that device, such as unlock for a door.

Camera video player

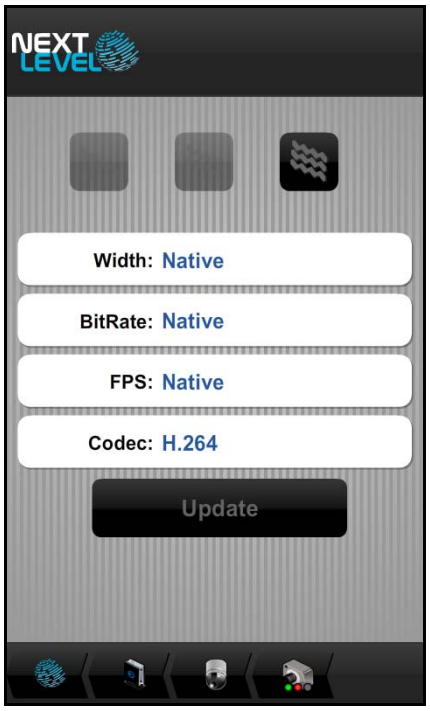


5. Use **Transcode** to change the resolution of the video display.

The transcode window has three settings, low (default), medium, and high. These settings adjust the frame rate, bit rate and resolution to alleviate bandwidth issues.

© 2009-2014 Next Level Security Systems, Inc.

The setting is indicated by the transcode icon at the top of the window.



Low

Medium

High

a. Select a resolution setting to change the resolution.

Note: This setting is applied to the video displayed for all connections in this session of NextMobile. When this session is exited, the setting reverts to the low setting the next time NextMobile is accessed.

b. Press **Update** to apply the change.

6. Tap **Full Screen**. The video is rotated to landscape view.

The video is displayed without any player controls. f

– 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.
– The breadcrumbs are hidden while the video player is in Full Screen mode.

Note: The camera must be in record mode for the recorded video to be played. A red LED under the camera icon indicates that the camera is recording.

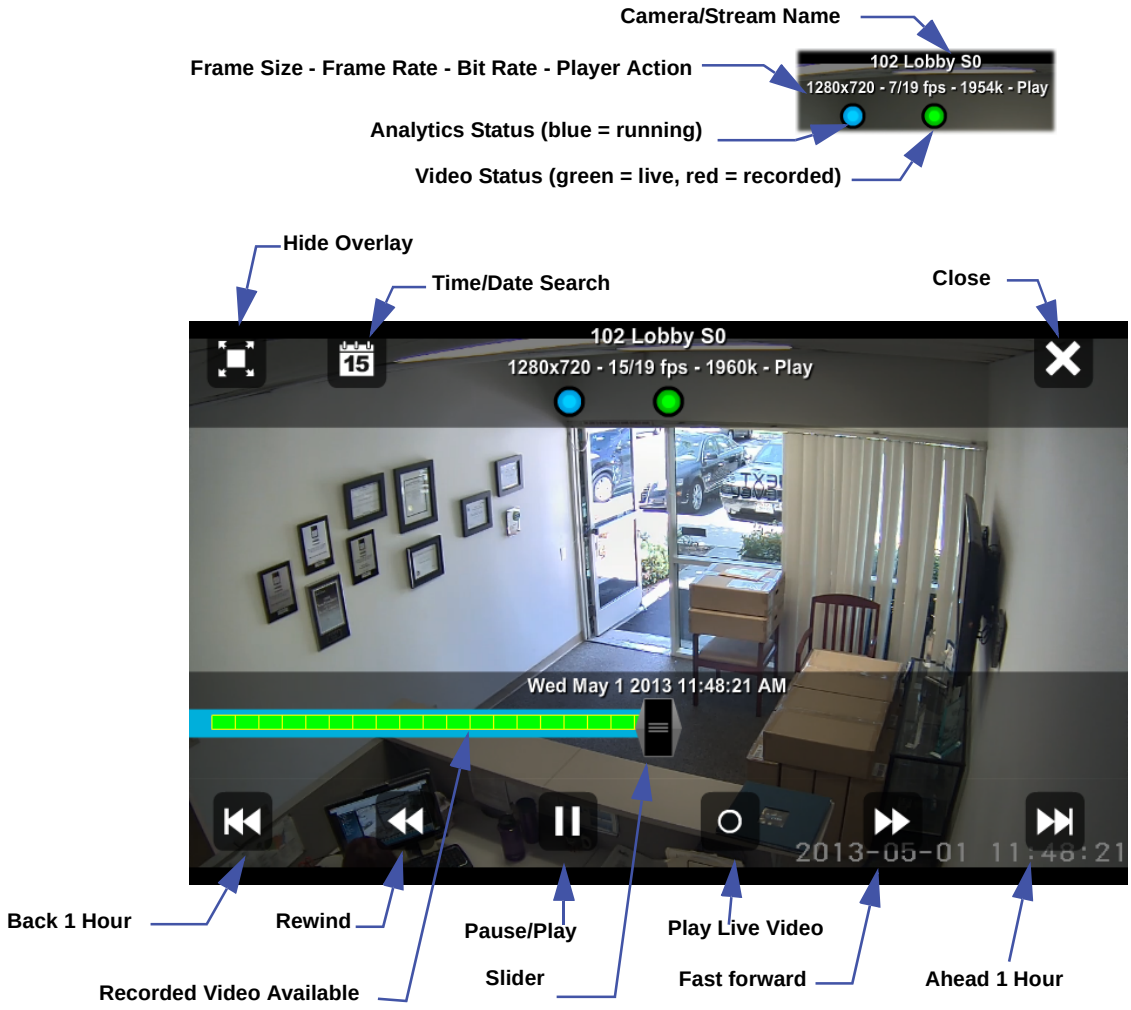
7. Tap the middle of the screen to display stream information, and player controls.These controls are only displayed if the camera is accessed via RMS.

   Specifications about the camera or steam are displayed in an overlay on top of the screen. The date and time are listed at the bottom.

   – If using a Local Gateway connection, the only controls displayed are the **Hide Overlay** and **Close** buttons.

   – If the camera has PTZ capabilities, tap the **PTZ** icon to display a list of Presets. Select a preset to move the camera.

   See **Using Presets** in **Chapter 4: Controlling Cameras** for more information on presets.



8. Recorded video can be searched and played back. A green line in the timeline indicates recorded video is available.

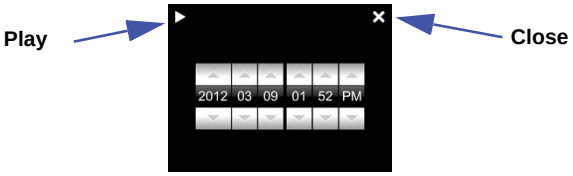
   To play a recorded video clip, drag the slider on the timeline.

Alternately, the clip can be located by entering the date and time.

a. Tap **Time/Date Search**.

» Use the arrow keys to select the time and date.

» Tap **Play** to locate a recorded video clip.



b. Tap **|<<** or **>>|** to move back or ahead an hour in recorded video.

c. Tap **<<** or **>>** to rewind or fast forward the playback.

d. Tap **O** to return to live video.

9. Tap **Hide Overlay** to display the video in the full screen.

10. Tap **Close** to return to the portrait view.

11. Tap **Back** to return to the Camera Streams list.

28.7 REMOTE DOOR UNLOCK

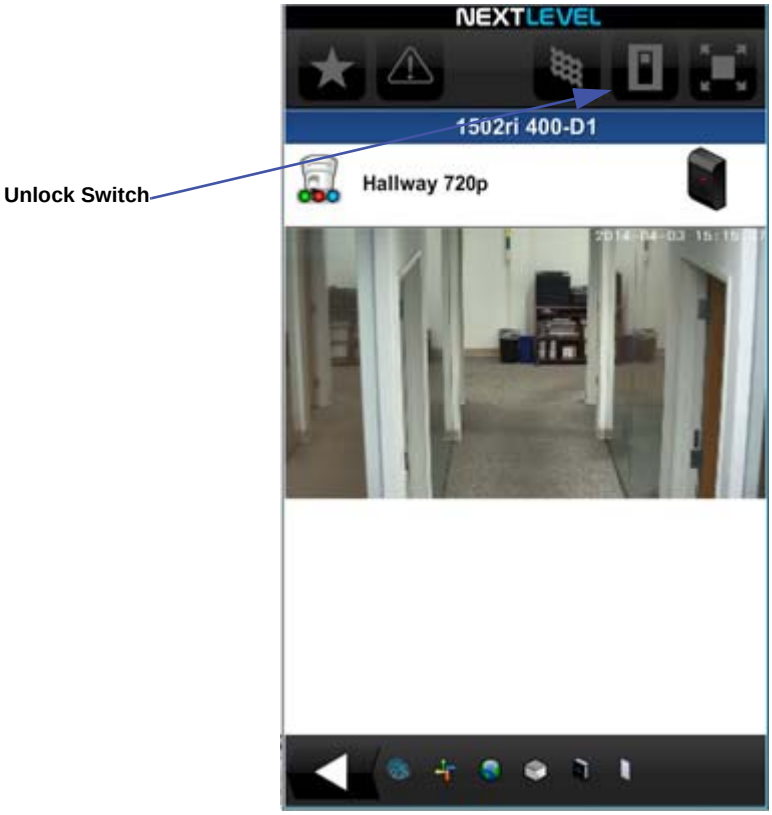
A door can be temporarily unlocked from a NextMobile.

1. Navigate to a Gateway, either through a local connection, or through RMS.
2. Select **Doors** from the options list.
3. Select a door from the Doors list.

   The door's screen is displayed. Video is also displayed, if a camera is assigned to the door, via the Gateway.
4. Touch the **Temporary Unlock** switch.

© 2009-2014 Next Level Security Systems, Inc.

A green indicator flashes briefly in the corner of the screen to indicate the door was successfully unlocked.



28.8 EVENTS

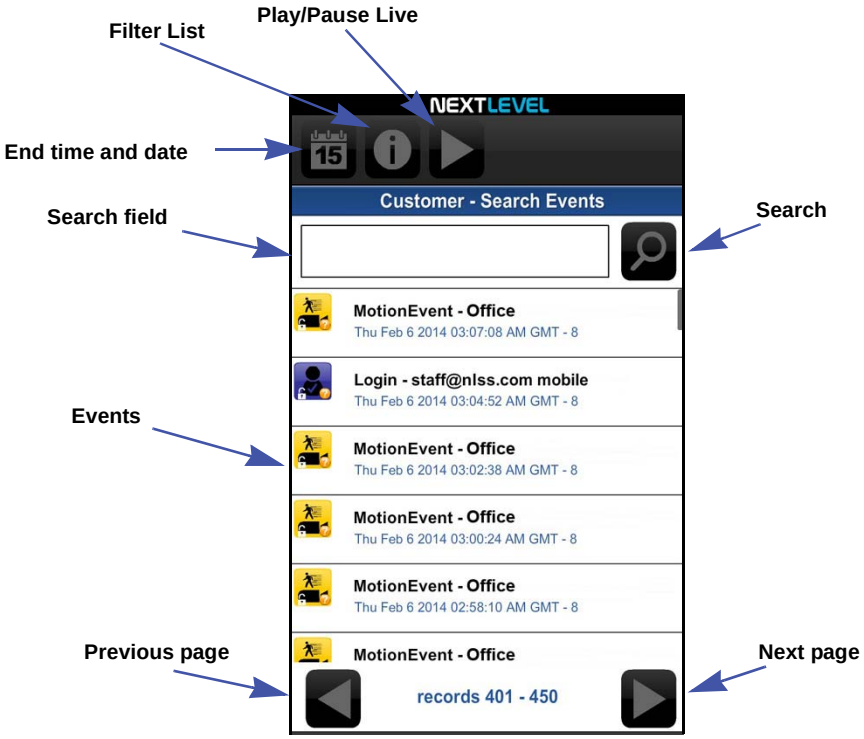
NextMobile provides access to the Event Log for a site, and associated items: cameras, access control, decoders, intrusion, system, users, and video analytics.

The Event Log can be accessed for the entire site, or from the menu for a selected item such as a camera.

See **Chapter 15: Monitoring and Handling Events** for more details about Events.

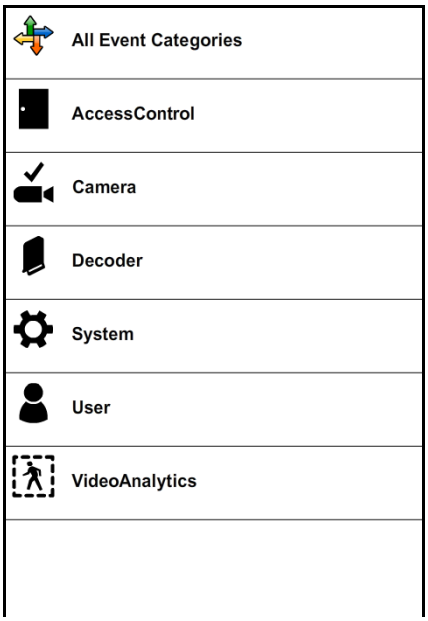
- Tap **Events** at the top of the screen.

The *Events Log* is displayed. The Event Log can be searched and filtered. Individual events can be accessed to see more details.



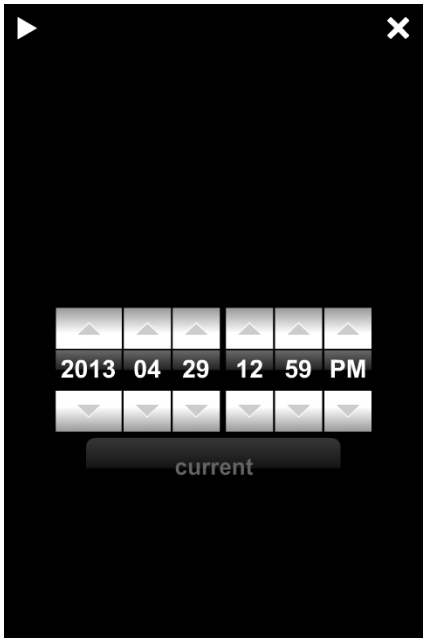
- **Play/Pause Live**: toggles between displaying a live list and pausing the list so new events are not displayed. When the live log is paused, the button turns blue, with a flashing green dot.
  - Click the button again to resume the live Events Log.

- **Filter List**: select a filter type to display only events in that category.



- **End Date and Time**: use the arrow buttons to set an end time and date for Events Log.
  - Tap **Play** to display the list with this time and date setting.
  - Tap **Close** to exit the dialog without applying the setting.

  Click **Current** to return the setting to the current time and date.

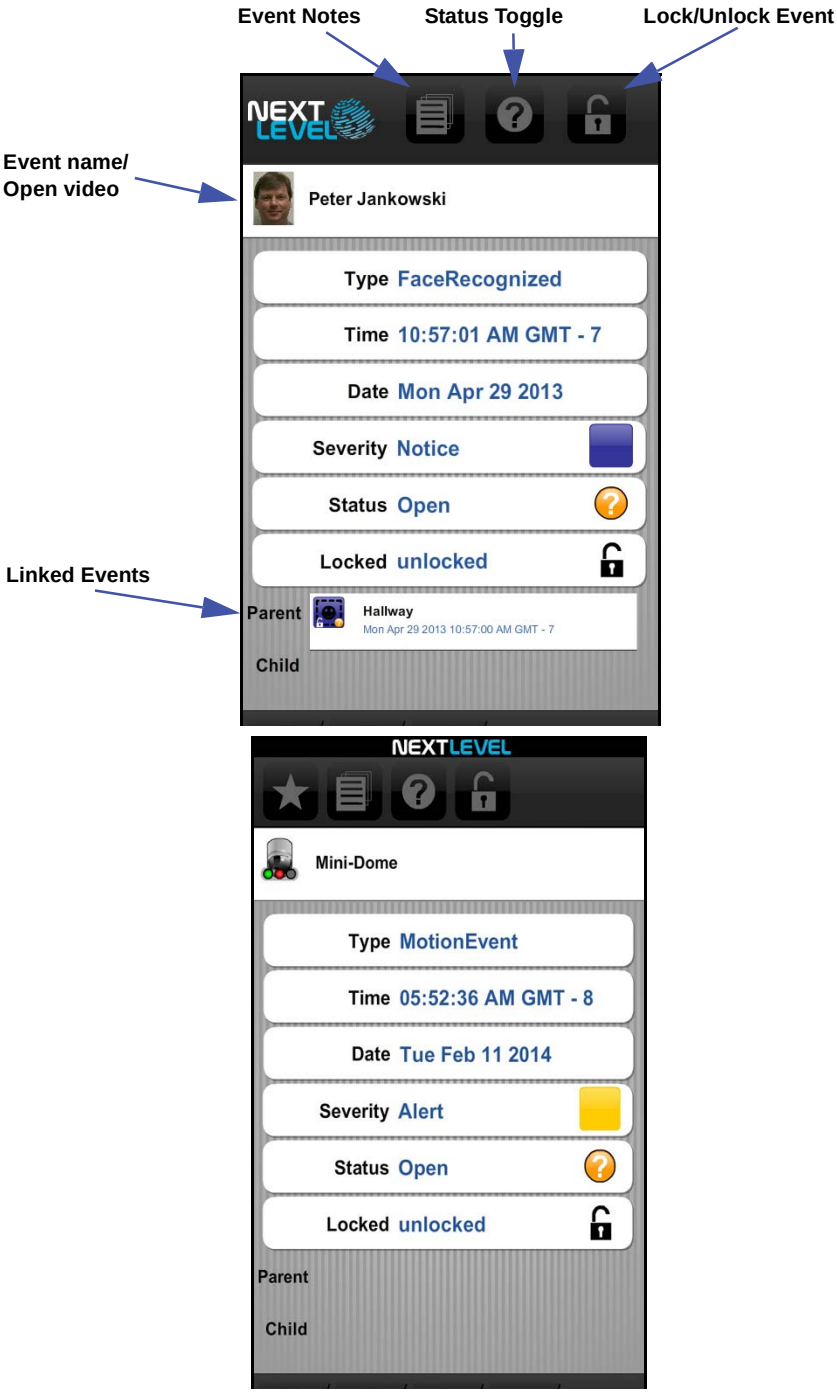


- **Search**: triggers an update of the Event Log. If a value is entered in the adjoining field, Search only checks the Event Source field for the value, and displays only the events that match that criteria. See **Searching a List** for more information.

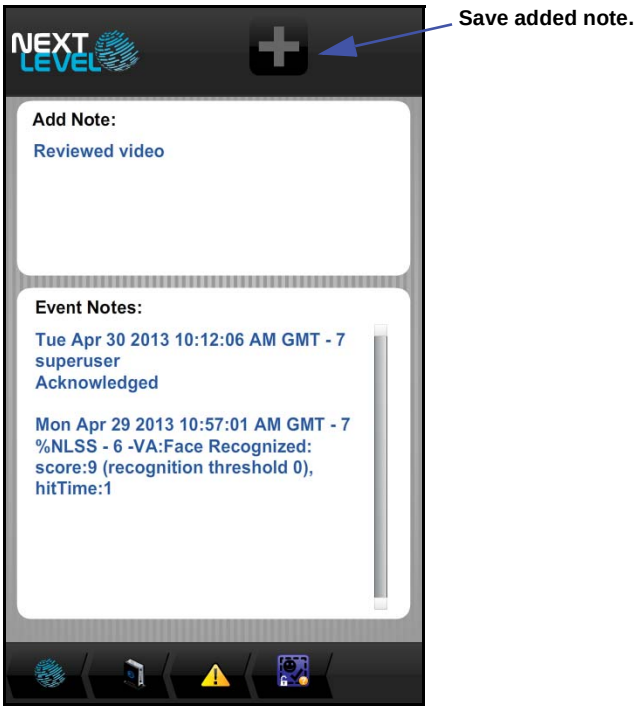
  - Enter a value and tap **Search** to locate matching events.
  - Clear the field and tap **Search** again to display the complete log.
- Use **Previous** and **Next** to scroll through the pages of events.
- Tap an event to see its details.

28.8.1 Event Details

Event details are accessed when an event is selected from the Events Log.



Event Notes: tap to open the *Event Notes* dialog. Past notes are displayed. Create new notes by tapping in the **Add Notes** section.



Add Note: after entering text in the Add note field, tap Add to save the new note.

Status: tap to toggle the status: *Open, Acknowledge*, *Closed*. A note is generated each time the status is changed.

Lock/Unlock: tap to lock an event so it cannot be groomed from the Event Log. Tap again to unlock the event.

- **Event Name**: tap the event name to play the video associated with the event, if any was recorded.
- **Parent/Child**: tap the item to display the details for the linked event.

See **Event Details** in **Chapter 15: Monitoring and Handling Events** for more information.

© 2009-2014 Next Level Security Systems, Inc.

28.9 MULTIVIEWS

Multiviews provide customized displays of multiple camera streams monitored by RMS. Streams from multiple devices can be grouped together in RMS, and displayed in NextMobile.

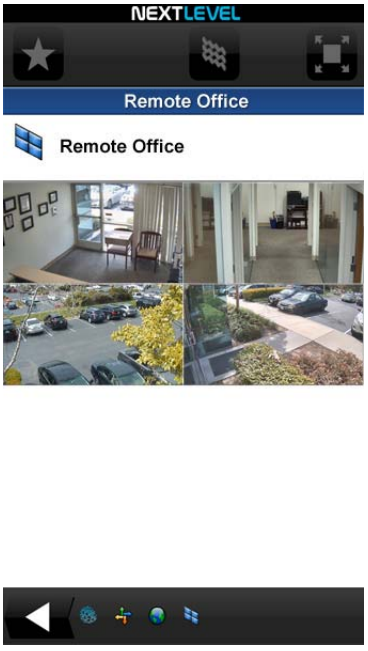
1. Connect to RMS.
2. Tap **Multiviews** in the menu.

   A list of multiviews configured in RMS are displayed.

3. Tap a Multiview setting from the list.

   The Multiview screen is displayed with three options: Favorites, Transcode, and Full Screen.

   The video for each stream is displayed in pane



4. Use **Transcode** to change the resolution of the video display.

5. Tap **Full Screen** to display a larger view of the multiview.

6. Tap anywhere on the screen to close the full screen mode.

28.10 CLOUD CLIPS

Video clips stored in the cloud can be accessed through NextMobile via RVS, or Cloud Clips exported by a Cloud Camera.

1. Tap **media** in the RMS main menu.

   The media list is displayed with clips recorded by cameras discovered by the Gateways subscribed to RMS. These clips were sent to RMS when they were exported from the local Gateway. See **Export Video** in **Chapter 4: Controlling Cameras** for more information.

2. Select a bridge.

   A clip library is displayed.

3. Select a clip. A video player is displayed.

   If desired, the clip can be marked as a favorite. See **Favorites** for more information.

4. Tap **Play**.

The video is played. The timeline allows the video to be scrubbed or paused.

5. Close the player.

28.11 USING THE MOBILE APP WITH A DECODER

The Mobile App provides many of the options available in the decoder interface.

Important: Be sure to set the decoder to *Enable HTTP* to allow NextMobile to access the decoder.

This setting is accessed in the Decoder web interface. In the Decoder menu, check the **Enable HTTP** box in the **Advanced** tab.

See the *NLSS HD Decoder User Manual* for detailed instructions on configuring and using the decoder. This manual is available from the NLSS Support web site: **support.nlss.com**.

To access a decoder:

1. Open the Connections list.
   – If a decoder is not listed, add it to the list. See **Supported Mobile Devices** for instructions.
2. Open a decoder:
   – Tap the decoder in the Connections list, if it was previously added.
   – Tap **Connect** is just adding the decoder,

As with other devices in the Mobile App, the **Favorites** and **Events** options are available. Lists also can be searched.

Other options allow the active video stream to be set and a snapshot to be viewed.

© 2009-2014 Next Level Security Systems, Inc.

28.11.1 Check the Active Video

A snapshot of the currently active video stream for the decoder can be viewed in the Mobile App.

1. Tap **Display** to see the snapshot.
2. Tap **Refresh** to update the snapshot.

28.11.2 Setting a Channel to Active

1. Tap **Channels**.
   The list is displayed of the channels set on the decoder.
2. Tap a channel to set it as the active display for the decoder.
3. Return to the Decoder menu.
4. Tap **Display** to see a snapshot of the selected channel.
5. Tap **Refresh** to update the snapshot.

28.11.3 Setting a View to Active

1. Tap **Views**.
   The list is displayed of the views set on the decoder.
2. Tap a view to set it as the active display for the decoder.
3. Return to the Decoder menu.
4. Tap **Display** to see a snapshot of the selected view.
5. Tap **Refresh** to update the snapshot.

28.11.4 Setting a Sequence to Active

1. Tap **Sequences**.
   The list is displayed of the sequences set on the decoder.
2. Tap a sequence to set it as the active display for the decoder.
3. Return to the Decoder menu.
4. Tap **Display** to see a snapshot of the selected sequence.
5. Tap **Refresh** to update the snapshot.

© 2009-2014 Next Level Security Systems, Inc.

PART 5: APPENDICES

- **Appendix A: Performance and Setup Guidelines: Video Analytics, Face Recognition, and License Plate Recognition** - provides additional information for optimizing the Video Analytics, Face Recognition, and License Plate *Recognition* features. Performance details are also discussed for these features.
- **Appendix B: Audio Analytics Guidelines** - provides guidelines and specifications for using audio analytics.
- **Appendix C: Contacting Support** - contact information and steps for contacting NLSS Technical Support.

© 2009-2014 Next Level Security Systems, Inc.

Appendix A: Performance and Setup Guidelines: Video Analytics, Face Recognition, and License Plate Recognition

This appendix provides additional information for optimizing the NLSS Unified Security Suite *Video Analytics*, *Face Recognition*, and *License Plate Recognition* features, and performance details for these features. See **Chapter 4: Controlling Cameras** for instructions on configuring these features.

Video Analytics (VA) is the single most processing intensive function in the system and therefore sets the performance limits of the Gateway. Different video analytics require different amounts of processing power. Video analytics processing and accuracy depends on the selected analytic's behavior, plus other factors that the Next Level Gateways cannot control, such as the scene, lighting, camera video quality.

Video analytics accuracy refers to both detection and false positives. Detection means that the desired video analytics event is detected by the system. False positives are events that are detected by the system, but do not capture the desired behavior.

For example, the Activity video analytic is enabled. If a car passes through the scene and the system detects it, that is desired behavior. But if a tree with leaves is blowing in the wind, the system may detect that activity as well. That detection is a false positive. Ideally, there is a very high detection rate for desired events and a very low false positive rate. High video analytics accuracy typically requires good camera placement, scene analysis, and adjustments based on trial run results.

Here are some basic guidelines for using video analytics.

- Optimum analytics performance per camera or stream is H.264, 720p, 15 fps, 2Mbps
- Video analytics resolution is limited to 1080p (1920x1080).
- A higher frame rate increases the load on the system, but does *not* increase video analytics accuracy.
- A higher resolution does not notably increase video analytics accuracy, except in some Face Recognition and License Plate Recognition cases.
- A lower frame rate significantly decreases video analytics accuracy.
- Gateway video analytics performance is platform dependent. See **Video Analytics Performance**.
- Transcodes do not generate events, but are part of the **Video Analytics Metrics** calculations.

© 2009-2014 Next Level Security Systems, Inc.

- Transcode include transcodes from the Operations > Cameras video player, display of MPEG4 stream in the NLSS Web Interface, and display of any stream on a mobile device.
- Only one forensic analytic can be run on a stream over a specific time period. If there is an overlap of time, the first forensic analytic *must be deleted* before running a second analytic.

A.1 VIDEO ANALYTICS METRICS

Each process has an impact on the Gateway. For reference, these processes are assigned a value to compare the impact of one process as compared to the others.

- Transcode = .5
- Live video analytic = 1
- Forensic video analytic = 2
- Face Recognition = 2
- Forensic Face Capture or Recognition = 3

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 License Plate Capture Line Crossing People Count People Count Direction Perimeter
2	Dwell Face Recognition Forensics (except those noted below) License Plate Recognition Object Moved Object Taken
3	Forensic Face Recognition Forensic License Plate Recognition

© 2009-2014 Next Level Security Systems, Inc.

A.2 VIDEO ANALYTICS PERFORMANCE

Guidelines: H.264, 720p, 15 fps, 2Mbps

The following table provides the capacities for running instances of video analytics and transcoding on each model of the Gateway.

NLSS Gateway	# Streams	Analytics & Transcode	Video Encoding	Video Resolution	Frame Rate	Bit Rate	Internal Storage
GW-500-2	8	2[a]	H.264	720p	15fps	2Mbps	500 GB
GW-3000	16	4	H.264	720p	15fps	2Mbps	4 TB
	32	2					
GW-4000	32	6	H.264	720p	15fps	2Mbps	8 TB
	64	3					
GW-5000[b]	64	6	H.264	720p	15fps	2Mbps	1.5 TB
	128	3					

a. No instances of Face Recognition or License Plate Recognition can be supported on the GW-500.
b. The GW-5000 contains dual GPUs.

A.3 SPECIFIC VIDEO ANALYTICS BEHAVIOR NOTES

Specific analytic behaviors require some specific parameters for best results.

- **Line crossing**: For a line crossing to trigger an event, the length of the line has to be at least twice as long as the object's width or height.
- **People Counting**: For best results, point the camera straight down, so that it is over the top of the people being counted.

© 2009-2014 Next Level Security Systems, Inc.

A.4 FACE RECOGNITION

The Face Recognition (FR) video analytic requires adjustment to achieve the best results.

To recognize a face, that face must be captured first. Face Recognition compares a captured face to the images stored in the system. The comparison images loaded into the system should be high quality for best results.

Using a good quality digital camera is the best tool to capture faces for comparison and storage on the Gateway. Cell phone cameras are not recommended. Ensure no special lenses, such as a fish-eye, are installed on the camera.

The *Face Capture* (FC) analytic typically requires the same adjustments as Face Recognition for best results. See the **Face Capture** and in **Chapter 5: Operations with Video Analytics**, and **Face Recognition** in **Chapter 22: Configuring and Using Face Recognition** for instructions on configuring Face Capture and Face Recognition, respectively.

A.4.1 Face Capture and Face Recognition Guidelines for Best Results

This section provides photograph, camera, and general guidelines.

A.4.1.1 PHOTOGRAPH GUIDELINES

The most important consideration for accurate face recognition is a good photo in the database.

- Photos must be in the JPEG format, no larger than 5 MB.
- Photos must meet the minimum requirement of 300x300 pixels of a complete facial photo.
- Facial photos of 900x900 pixels or better is recommended.
- NLSS recommends that higher resolution facial photos should be used over the minimum requirements.
- Position the camera at face level for a direct view of the person's face
- Take more than one photo, and from slightly different angles if possible.
- If the subject wears glasses, take a pictures with the glasses off, and with them on.
- The more reference photos the better the accuracy of the recognition system.
- Do not use blurry or unfocused pictures. These images cause the system to produce many false positive events.
- Do not use a wide angle lens, which can distort the image of the face.

One method to ensure excellent photos is to follow the guidelines set for US Passport Photos.

- Requirements are available at: **http://travel.state.gov/passport/pptphotoreq/pptphotoreq_5333.html**

© 2009-2014 Next Level Security Systems, Inc.

- Example photos are available at: **http://travel.state.gov/passport/pptphotoreq/photoexamples/photoexamples_5300.html**
- A free tool to crop and resize photos is available at: **http://travel.state.gov/_res/flash/cropper/FIG_cropper.html#**

A.4.1.2 IP Camera Guidelines

- Position the camera at face level for a direct view of the person's face
- Verify the camera lens and cover are clean.
- If possible, use a variable focus lens that can be focused on a face.
- Do not use a wide angle lens, which can distort the image of the face.
- Make sure the resolution is set for no higher than 1080p.
- For most applications, 720p resolution is sufficient for good Face Recognition accuracy, but 1080p is better.
- For wide area scenes, where the faces are a small part of the view, a 1080p resolution may provide better results.
- Set frame rate to a setting no lower than 15 fps.
- The angle of view for the face capture is no more than 15 degrees.
- Verify the background is not *washed out* due to lighting or sunlight. Using a wide, dynamic range camera typically improves results across a broad range of lighting.
- Verify that the subject face remains in the camera's view for at least two seconds.
- Verify that there are no shadows in the facial area
- Images with sunglasses and/or hats do not provide good results.
- Images with different facial hair from data base pictures do not provide good results.
- When possible, provide procedural instructions that help ensure that the above guidelines are met. For example, require people in a security line to remove their hats and sunglasses and look at the camera as they pass through a checkpoint.
- Use the video analytics forensic to adjust the Face Recognition parameters (sensitivity, confidence, best match) and verify the results based on different settings. See **Video Forensics** in **Chapter 22: Configuring and Using Face Recognition** for instructions.

A.4.1.3 General Guidelines

- Maximum number of people per Face Recognition group is 5000. As the number of people in the face recognition group decreases, the accuracy typically increases.

© 2009-2014 Next Level Security Systems, Inc.

- Use the video analytics forensic to adjust the Face Recognition parameters (sensitivity, confidence, best match) and verify the results based on different settings. See **Chapter 22: Configuring and Using Face Recognition** for instructions.

A.4.2 Face Recognition Events and Actions

Face Recognition events can be combined with other events to create sophisticated rules.

The events for Face Recognition are:

- Face Recognized
- Face Match Group

The action for Face Recognition is:

- FaceRecognitionValidateGroup

See **Configure Actions** in **Chapter 17: Global Configurations** for more information.

A.4.2.1 Event Linkage Examples

To create a rule where a Face Match in a particular group causes an action, create two Event Linkages using the following events and actions:

- Event: FaceRecognized-> Action: FaceRecognitionValidateGroup
- Event:FaceMatchGroup-> Action:SendEmail

See **Configure Event Linkages** in **Chapter 17: Global Configurations** for instructions and more information on event linkages.

© 2009-2014 Next Level Security Systems, Inc.

A.5 LICENSE PLATE RECOGNITION

The License Plate Recognition (LPR) video analytic requires adjustment to achieve the best results.

To recognize a license plate, that license plate must be captured first. The *License Plate Capture* (LPC) analytic typically requires the same adjustments as License Plate Recognition for best results. See **Chapter 23: Configuring and Using License Plate Recognition** for instructions on configuring License Plate Capture and License Plate Recognition.

License Plate Recognition compares a captured license plate to the images stored in the system. The comparison images loaded into the system should be high quality for best results.

A.5.1 License Plate Capture and License Plate Recognition Guidelines for Best Results

- Position the camera to capture a clear image of the license plate, with less than a 5 degree tilt.
- The camera time stamp must be turned off. See the camera's documentation for instructions.
- Any added borders or license plate frames must not cover the license plate number.
- Verify the camera lens and cover are clean.
- If possible, use a variable lens that can be focused on a license plate, rather than a wide angle lens.
- Verify the license plate is not *washed out* due to lighting or sunlight. Using a wide, dynamic range camera typically improves results across a broad range of lighting.
- For most applications, 720p resolution is sufficient for good License Plate Recognition accuracy.
- For wide area scenes, where the license plates are a smaller part of the view, a 1080p resolution may provide better results.
- The license plate must appear in front of the camera for at least two seconds before the analytic's bounding boxes can locate the license plate. Three seconds are needed to read the number. Then an event is generated.
- Use upper case letters when entering the alpha portion of a license plate either through the NLSS Web Interface or a .csv file.

© 2009-2014 Next Level Security Systems, Inc.

A.5.2 License Plate Recognition Events and Actions

License Plate Recognition events can be combined with other events to create sophisticated rules.

The events for License Plate Recognition are:

- License Plate Recognized
- License Plate Match Group

A.5.2.1 Event Linkage Examples

To create a rule where a License Plate Match in a particular group causes an action, create two Event Linkages using the following events and actions:

- Event: LicensePlateRecognized-> Action: LicensePlateRecognitionValidateGroup
- Event: LicensePlateMatchGroup-> Action:SendEmail

© 2009-2014 Next Level Security Systems, Inc.

Appendix B: Audio Analytics Guidelines

The NLSS Unified Security Suite provides optional audio analytics that monitor the audio from the cameras attached to the NLSS Gateway. This paper provides an overview of these analytics.

- **Introduction**
- **Glass Break Analytic**
- **Car Alarm Analytic**
- **Aggression Analytic**
- **Gunshot Analytic**
- **Supported Cameras**
- **General Specifications**
- **Using Audio Analytics**

B.1 INTRODUCTION

The NLSS Unified Security Suite's audio analytics recognize certain sounds within the audio from a camera or video stream. An event is generated when set thresholds are exceeded.

Audio events can be associated with a notification or alarm in the NLSS Web Interface, thereby alerting the proper personnel to a potential threat or problem.

Since the audio is associated with a camera or video stream, live audio and video can be viewed in the NLSS Web Interface to quickly ascertain if there is a threat or problem. Recorded audio and video also can be played back to analyze what triggered the event.

Audio analytics monitor audio for four types of events or behaviors.

- Glass Break
- Car Alarm
- Aggression
- Gunshot

Audio Analytics are a premium feature that are enabled by a token provided by an NLSS partner.

© 2009-2014 Next Level Security Systems, Inc.

B.2 GLASS BREAK ANALYTIC

The glass break analytic detects standard window glass being broken. Breakage of a range of different glass types can be detected, including laminate, plate, wired, and tempered glass, as are commonly found in commercial and residential buildings.

Breakage of different thicknesses and sizes of glass are characterized in the analytic, as well as a range of different *implements* used to break the glass.

The glass break analytic also works with one of the standard industry glass break simulators used in confirming successful system setup and configuration of the analytic.

B.2.1 Analytic Specifications

- Breakage of different thicknesses and sizes of office, shop and house window glass breaking are detected by this analytic.
  - *Plate*: 2.4 mm - 6.4 mm
  - *Tempered*: 3.2 mm - 6.4 mm
  - *Wired*: 6.4 mm (the only thickness wired glass comes in)
  - *Laminated*: 6.4 mm
  - *Minimum glass size, all types of glass*: 300 mm x 300 mm
- The analytic detects glass break up to 10 meters from the microphone, based on a representative environment for intrusion detection applications.
- The analytic reliably detects glass break in typical intrusion detection scenarios up to at least 50 dB SNR (Signal to Noise Ratio).
- A glass break simulator can be used to test that the analytic and camera are properly configured. An example is the Risco RG65 industry standard glass break simulator.

B.3 CAR ALARM ANALYTIC

The car alarm analytic detects the seven standard types of car alarms used by major car manufacturers in Europe and North America. The seven major car alarms are characterized by looping patterns.

Sample car alarm audio clips can be obtained from the NLSS web site, **nlss.com**

B.3.1 Analytic Specifications

- The analytic operates up to 50 meters from the microphone.
- The analytic can reliably detect car alarms up to at least 10 dB SNR (Signal to Noise Ratio).

© 2009-2014 Next Level Security Systems, Inc.

B.4 AGGRESSION ANALYTIC

The aggression analytic characterizes and detects the specific pitch, tone and intonation changes that occur in the voice patterns in response to someone getting aggressive.

B.4.1 Analytic Specifications

- The analytic operates up to 10 meters from the microphone.
- The analytic can reliably detect aggression up to at least 40 dB SNR (Signal to Noise Ratio).

B.5 GUNSHOT ANALYTIC

The gunshot analytic detects various types of firearms being discharged, covering the types of guns most commonly used in civilian gun crimes. Gunshots are characterized by the unique, un-silenced muzzle blast associated with a range of weapons typically used in crimes in the Americas, Europe, Middle East and Australasia.

- *Hand guns*, including: 9mm semi-automatics and revolvers with and without muzzle diffusers.
- *Shot guns*, including: 20-gauge, and12-gauge
- *Rifles* including: .22 and 7.62 mm bolt action
- *Automatic rifles*, including AK-47, and AR-15
- *Semi-automatic rifles*, including AR-15
- *Uzi submachine gun*

B.5.1 Analytic Specifications

- The analytic operates up to 100 - 200 meters from a gun shot.
- The analytic can reliably detect gunshots up to at least 50 dB SNR (Signal to Noise Ratio).

© 2009-2014 Next Level Security Systems, Inc.

B.6 GENERAL SPECIFICATIONS

Certain environmental, performance, and configuration specifications are required when using the audio analytics with an NLSS Gateway.

B.6.1 Environmental

- Audio analytics can be applied to both indoor and outdoor installations.

  The analytics can compensate for ambient sounds, including:

  – Traffic noise
  – Street noise.
  – Office and building noise.

- The analytics operate in various environmental conditions, including:
  – Day time or night time.
  – Various weather conditions. including rain, thunder and wind.

B.6.2 Performance

The system performance of audio analytics varies, based on:

- Background noise levels
- Microphone sensitivity settings (clipping/distorting/low-level)
- Any audio signal process that is applied to the audio by the capture device, such as AGC (auto gain control).

B.6.3 Configuration

- Audio analytics require an IP camera with a built-in or external microphone, or an encoder. The device must support an audio sampling rate of 16 KHz, 16 bits, using the AAC codec.
- The analytic's sensitivity can be adjusted for each channel, although the default setting works in most applications.
- The audio analytic requires a microphone with a frequency response equal to at least 100 Hz - 8 kHz +/- 6dB. Most camera's built-in microphones meet these requirements.
- To prevent clipping or distortion:
  – The microphone should be at least two meters from potential sound sources.
  – Adjust the microphone sensitivity settings on the camera or encoder.
- The microphone sensitivity settings must provide a reasonable level of audio to the NLSS Gateway and the analytic.
- The effective range for microphones quoted in this document are typical detection ranges in representative environments, in which the analytic is likely to be used. The effective range varies, according to the physical and acoustic environment.

© 2009-2014 Next Level Security Systems, Inc.

B.7 SUPPORTED CAMERAS

As mentioned earlier, to run audio analytics, the cameras must support a 16 KHz, 16 bit audio sampling rate, with the AAC codec.

Below is a list of cameras, with built-in microphones that support these audio settings. Additional cameras will be added to the list as they are tested.

Axis

- Axis M1031
- Axis M1054
- Axis P1343
- Axis P1344
- Axis P1346
- Axis P1347
- Axis P3343/-V
- Axis P3344/-V
- Axis P3346/-V
- Axis P3367-V
- Axis M501
- Axis M5014
- Axis Light Finder P3364

Sony[a]

- SNC-VB630
- SNC-VM600
- SNC-VM600B
- SNC-VM601
- SNC-VM601B
- SNC-VM630
- SNC-VM631

a. Sony cameras require firmware version 1.3 or later.

B.8 USING AUDIO ANALYTICS

The audio analytics are enabled and configured similar to the video analytics included with the NLSS Gateway.

- The Glass Break analytic can be run simultaneously on up to four channels (cameras or video streams) on an NLSS Gateway. This component is included as standard feature on every NLSS Gateway.
- The other audio analytics are purchased on a per stream basis.

© 2009-2014 Next Level Security Systems, Inc.

Appendix C: Contacting Support

Before contacting NLSS Support:

- Search the **NLSS Support Knowledgebase** for answers not found in the documentation: **support.nlss.com**
- If a call to NLSS Support is required to resolve an issue:
  - 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.

C.1 GATEWAY INFORMATION

Print this page and fill in the information below. This information is available in the NLSS Web Interface, from *Configuration* > *Global* > *Gateways*.

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.

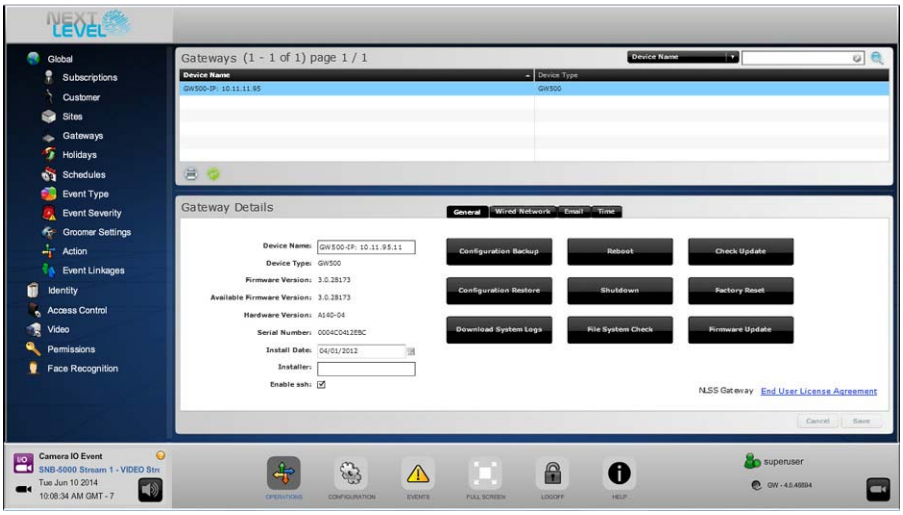
» See **Check Update** for instructions on updating the Gateway via an Internet connection.

» See **Firmware Update** for instructions on updating the Gateway if an Internet connection is not available or a manual update is preferred.

C.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

C.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.

© 2009-2014 Next Level Security Systems, Inc.

C.4 CONTACT INFORMATION

For support:

Call: 1-760-444-1410

Email: **support@nlss.com**

© 2009-2014 Next Level Security Systems, Inc.

Index

Symbols

.csv file
  Face Recognition 221, 293

Numerics

26-bit H10301 160

37-bit H10302 160

37-bit H10304 160

A

AAC 249

Access Control
  configuration order 169
  configuring controllers 169
  configuring reader interfaces 175
  devices 19
  I/O Interfaces 185
  I/O Linkages 188
  overview 168
  reports 84

Access Controller
  I/O interface usage 186

Access Level
  assigning to cardholders 166
  configuring
    local gateway 157
    local RMS 290
  creating 158
  doors 158
  schedules 146, 158

ACDoorMomentaryUnlock 152

ACDoorRelock 152

ACDoorUnlock 152

ACOutputOff 152

ACOutputOn 152

Actions
  configuring 151
  creating 153
  defined 151
  types 152
  use with Event Linkages 154

actions
  Face Recognition 328
  License Plate Recognition 330

activating cardholders 79, 163

Activation Date 164

Activity analytic 61

ADA 163

adding
  items to a configuration list 129
  permissions 211

Admin State
  cameras 195
  doors 74

Administrative State
  controllers 171

administrator 210
  gateway permissions 213

aggression
  defined 333
  specifications 333

agreement, end user license 142

analytics - see video analytics

Areas 257
  bypassing 263
  defined 252
  operations 262

Assa Abloy
  Call In Frequency 172
  controllers 169
  Sargent v.S1 170
  Sargent v.S2 170

assigning people
  Face Recognition groups 226
  License Plate Recognition groups 244

audio 50
  analytic 50, 249
  bit rate 199
  codec 199
  play by action 153
  sample rate 199
  stream parameters 199

audio analytics
  aggression

defined 333
specifications 333
car alarm
defined 332
specifications 332
encoding 249
glass break
defined 332
specifications 332
guidelines 331
gun shot
defined 333
specifications 333
sample rate 249
specifications 334
configuration 334
environmental 334
performance 334
supported cameras 335
using 335

Aux Input tab
I/O interfaces 186
readers 178

Aux Output tab
I/O interfaces 187
readers 179

Available Firmware Version 137

Axis
A1001 controller 171

B

back button 57

backing up Gateway configuration 138

Backups tab., RMS 285

Bad Image field 227

Badge Orientation 161

Badge Profiles
configuring
RMS 292
default deactivation 162

badges, printing 165

Baud Rate, controllers 172

Billing Address 134

Bit Format 160

bit rate
audio 199

Bit Rate (Kb/s) 199

Bit Rate Mode 199

bit rate, video 199

Border Color, badges 161

BulkTransfer tab, RMS 286

bypassing an area, intrusion 263

C

cameras
add video stream 201
adding to a zone 260
adding to doors 75
adding to input devices 104, 109
Admin State 195
audio analytic support 335
back button 57
bit rate
video 199
bit rate mode 199
configuring 194
connection state 197
custom preset 47
Custom Stream Type 196
date and time 45
digital zoom 50
event bookmark 45
event log 55
event types 55
events 45
playback 57
export a clip
local gateway 51
RMS 277
external storage 190
fast forward 44
filtering lists 40
firmware version 197
frame rate 198
full screen player 53
Home preset 47
I/O 50
icons 40
input port 56
In-Service 196
installation 24
IP address 197
live/archive toggle 44
MAC address 197
manual connection 201
manual output 50
monitoring 42
Motion Event 56
multicast 197
mute 51
off line settings 196
Out of Service 196
Patrols

© 2009-2014 Next Level Security Systems, Inc.

configure 48
create 48
delete 49
using 48, 49
pause 44
play 44
play audio 50
playback events 57
Pre-Provisioned 195
PTZ 46
PTZ presets 46
recording schedule 200
recording settings 200
removing
door 75
input device 105, 109
reports 57, 84
resolution 55
resolution height 198
resolution width 198
rewind 44
schedules 146
selecting 38
serial number 197
settings 200
SkipToKeyFrame 199
snapshot 51
stream selection 54
talkback 51
TCP 199
timeline events 56
timelines 53
1 hour 54
24 hour 53
toolbar 43
video information 43
UDP 199
unsupported, adding 201
VBR
quality 199
upper cap 199
video codec 198
video information 43
views 39
volume 51

car alarm
defined 332
specifications 332

Card Number 164

Card Profiles
Bit Format 160
configuring
RMS 291
details 160
Facility Code 160

Card Status 165

Card Types
cardholder configuration 165
configuring
local gateway 159

Cardholder ID (Emp#) 163

Cardholder Types
cardholder configuration 165
configuring
local gateway 161

Cardholder Vehicle 163

cardholders 79
activate 79, 163
Activation Date 164
ADA setting 163
assigning access levels 166
card number 164
card status 165
Card Types, applying 165
Cardholder Types, applying 165
Cards tab 164
photo import 165
configuration
order 163
configuring
local gateway 162
RMS 292
Credential tab
PIN 164
Print Badge 165
deactivate 79, 163
from maps & floorplans 117
deactivation Date 165
defined 77
Embossed Number 164
event picture 124
Face Recognition status 227
HR type 163
ID 163
information 78
OmniKey readers 166
photo 78
status 163
vehicle 163

Cardholders/User
cardholders
information 78
photo 78
users information 78
window overview 77

Cardholders/Users
defined 77
details 78
events 79
list 78
reports 79

© 2009-2014 Next Level Security Systems, Inc.

Cards tab 164
Import Photo 165
cashiers, listing 266
ChannelSetActive 152
Check Update 140
clock, Gateways 144
clone button 212
cloning roles 216
closed environment, Face Recognition 224
codec
audio 199
setting 198
Components 19
conditional settings, RMS 280
confidence
License Plate Capture 246
Configuration
Access Control 168
Doors 183
I/O Interfaces 185
I/O Linkages 188
Readers 181
adding items 129
deleting items 130
editing items 129
Face Recognition 220
Global
Actions 151
Customers 134
Event Linkages 154
Event Severity 149
Event Types 148
Gateways 136
Groomer Settings 150
Holidays
local gateway 145
RMS 287
local gateway 131
RMS 284
Schedules 146
RMS 288
Sites 135
Subscriptions 132, 133
Identity 157
Access Level
local gateway 157
RMS 290
Badge Profiles
RMS 292
Card Profiles
RMS 291
Card Types
local gateway 159
Cardholder Types
local gateway 161
Cardholders
local gateway 162
RMS 292
RMS 290
Intrusion 253
areas 257
devices 258
panels 253
License Plate Recognition 235
menu overview 35
order 127
overview 127
Permissions
Groups
local gateway 207
RMS 295
Roles 210
users
RMS 296
RMS 280
initials settings 281
settings 280
dependencies 282
table 280
transfer status 283
transferring 282
searching table 128
table options 128
user access permissions 127
Video 190
Cameras 194
Storage 190
Configuration Backup 138
for support 337
Configuration Restore 138
connecting to a camera 201
Connection State
cameras 197
decoders 203
connections screen 301
contact mode, doors 184
contacting support 336
controller
IP address 171
controllers
Administrative State 171
In Service 171
Out of Service 171
Pre-provisioned 171
Assa Abloy 169
ASSA Call In Frequency 172

© 2009-2014 Next Level Security Systems, Inc.

baud rate 172
configuring 169
DHO default setting 172
DHO extended timeout 172
extended time setting 172
firmware
release date 172
version 172
General tab 170
hardware version 172
HID 169
MAC address 171
Mercury 169
associating with NLSS Gateway 173
strike time default setting 172
types 170

Credential tab
PIN 164
Print Badge 165

csv file
Face Recognition 221, 293
LPR (License Plate Recognition) 236

Current Gateway Time 144

Custom preset, cameras 47

Custom Stream Type 196

Customer 134
configuration 134
details 134
RMS Global menu 284

customer, defined 273

D

database
importing for Face Recognition 222, 294
importing for License Plate Recognition 238

Days of Week 147

deactivating cardholders 163
Cardholders/Users 79, 117
maps & floorplans 117

Deactivation Date 165

Debounce 187

decoder
mobile app access 320

decoders 88, 98
configuring 202
connection state 203
editable parameters 203
firmware version 203
hardware version 203
IP address 203
listed 202
model 203
NextMobile 301
pushing a clip to 97
pushing a view to 98
reports 84
serial number 203
window 96

Default Deactivation 162

Default IP Gateway 143

Delete permission 211

deleting items from a configuration list 130

dependencies, RMS 282

Device Model, decoders 203

Device Name
decoders 203
gateway 136

Device Type
gateway 136

Devices, intrusion 258

DHCP, gateways 142

DHO (door held open)
extended timeout 172
Time Default 172
time override 184

digital zoom 50

Direction analytic 62

Disable Schedule on Holidays 147

Discovery Utility/Tool, running 25

doors
Access Level setting 158
adding cameras 75
Admin State 74
cameras
adding 75
removing 75
viewing 75
configuring 183
contact mode 184
controllers
default strike time 172
DHO (door held open) extended timeout 172
DHO (door held open) setting 172
extended strike time 172
DHO time override 184
event log 76
Fail Safe 185
Fail Secure 185
Failure Mode 185
holidays, disable unlock 147

© 2009-2014 Next Level Security Systems, Inc.

icon LEDs 74
icons 74
list 74
filters 74
Lock Type 184
lock voltage 185
Normally Closed 184
Normally Open 184
open from maps and floorplans 116
push to talk 76
reader name 184
reports 76
REX settings 184
schedules 146
Strike Time Override 185
type 184
unlock 75
window 73

downloading
video clip
email link (RMS only) 278
local gateway 101
RMS 278

Dwell analytic 63

E

Edit permission 211

editing items in a configuration list 129

Email notices, configuring 143

Email tab, Gateways 143

EmailSend 152

Embossed Number 164

employee number (Emp#) 163

Enable DHCP 142

Enable SSH 137

encoders
IP address 197
stream type 197

End Date
holidays 145
video export 52

End Time
video export 52

End Time, schedules 147

End User License Agreement 142

Error 283

eSATA storage 192

Ethernet
configuring 142
default network gateway 143
IP address, gateways 143
Link Speed 143
MAC address 143
primary DNS 143
secondary DNS 143
setting
subnet mask, gateways 143

event bookmark, cameras 45

Event Category
associated Event Types 155
defined 155

event details
NextMobile 316

Event Linkage
creating 156
Face Recognition 328
License Plate Recognition 330
Needs Acknowledgment setting 156

Event Linkages 154
configuring 154
defined 154
Face Recognition 126

event log
actions 122
filters 120
local gateway 119
NextMobile 314
overview 119
queues 120
RMS 297

Event Severity
configuring 149
RMS 289

Event Type
RMS 288
Severity 148
use in Event Linkages 154

Event Types 148
associated Event Category 155

event types
cameras 55

events 79
camera logs 55
camera playback 57
camera timeline 56
cameras 45
details dialog 123
described 123
event state 123
lock state toggle 124

© 2009-2014 Next Level Security Systems, Inc.

notes editor 124
profile picture 124
recorded event 124
shunt toggle 124
snapshot 124
doors 76
emergency 125
export 124
Face Match Group 220
Face Recognition 125
linkages 126
I/O, cameras 56
input devices 105, 110
License Plate Match Group 235
list defined 121
local gateway 119
logs 119
monitoring options
local gateway 118
motion 56
NextMobile 314
RMS 297
transactions 265

export
events 124
stopping video 102
video clip
local gateway 51
RMS 277

Extended Time Default, controllers 172

external storage
adding 192
configuring 190
eSATA 192
IP address 191
iSCSI 191, 192
listed 191
LUN 191
mount point 191
NAS 190
USB 192

external storage target 191

F

Face Capture
defined 64
guidelines 326

Face Capture analytic
configuration notes 233

Face Match Group 220

Face Pool 225

Face Recognition 220
.csv file 221, 293
actions 328
validate group 152
adding a person 230
bad image 227
Best Match 232
cardholder status 227
closed environment 224
confidence 232
database
construction 221
importing 222, 294
defined 64, 65, 220, 232
deleting a person 231
editing a person 230
event linkages 328
events 125
linkages 126
group name 221, 236
groups 223, 226
accessing 224
assigned 227
available 227
creating 225
deleting 225
Face Pool 225
guidelines 326
images
requirements 221
size 221
type 221
uploading 228
Images tab 228
images tab
image pool 228
primary image 228
importing a database 222, 294
management 226
updating 230
open environment 224
sample template 223, 294
sensitivity 232
userSuppliedID 221, 236

FaceRecognitionValidateGroup 152

Facility Code 160

Factory Reset 141

Fail Safe 185

Fail Secure, doors 185

Failure Mode, doors 185

Features 18

File System Check 140

firmware
camera version 197
controllers
release date 172

© 2009-2014 Next Level Security Systems, Inc.

version 172
restoring to factory settings 141
update
manual 141
via Internet 140
version
decoders 203
gateway 136

Firmware Update 141

floorplans 111
adding to groups 114
deactivating cardholders 117
opening a door 116
using 114
viewing video 116

forensics, video 72

FPS 44

Frame Rate 198

full screen
gateway 36
RMS 297

full screen toggle 36, 297

full screen video player 53

G

gateway clock 144

Gateway Groups tab 214

Gateway Module tab, roles 212

Gateways 36, 136
Check Update 140
Configuration Backup 138
Configuration Restore 138
downloading system logs 139
Email tab 143
End User License Agreement 142
Factory Reset 141
File System Check 140
Firmware Update 141
General tab 136
installation 24
logging in 28
menu permissions 212
port for streams 197
rebooting 139
setting time 144
shutting down 139
system logs 139
Time tab 144
Wired Network tab 142

General tab
controllers 170
Gateways 136
Intrusion
Panel 254

Generic Format 160

glass break
defined 332
specifications 332

Global menu
Actions 151
Customer 134
Event Linkages 154
Event Severity 149
Event Types 148
Gateways 136
Groomer Settings 150
Holidays
local gateway 145
RMS 287
local gateway 131
RMS 284
Customer 284
Sites 284
Schedules 146
RMS 288
Sites 135
Subscriptions 132
tokens 133

groomer
Maximum Retention 150, 268
Minimum Retention 150, 268
Point of Sale 268
settings 150

groups
assigning in Face Recognition database 221, 236
defined 112
local gateway 207
RMS 295
Face Recognition 223
accessing 224
assigned 227
assigning people 226
available 227
creating 225
deleting 225
Face Pool 225
hierarchy 112
License Plate Recognition
assigning people
License Plate Recognition
groups 244
creating 244
deleting 244
license plate recognition 242
accessing 243
License Plate Pool 243

list 113
local gateway
create 208
delete 209
edit 209
example 207
permissions 207
window 208
LPR 235
maps, adding 114
opening doors in maps & floorplans 116
Quick Mode 115
RMS
defined 280
roles, setting permissions 214
validation by face recognition 152
viewing video
maps & floorplans 116
window 113

gun shot
defined 333
specifications 333

H

Hardware Version
decoder 203
Gateway 137

HID 169
Edge/ EDGE EVO 171

holidays
defined 145
end date 145
local gateway 145
RMS 287
start date 145

Home preset, cameras 47

HR Cardholder Type 163

HTTP 196

I

I/O
camera event 56
cameras, manual output 50

I/O Interfaces
Aux Input tab 186
Aux Output tab 187
configuring 185
Debounce 187
Input Devices Available 186
Input Port 186
Normal State
input 187, 188
Output Devices Available 187
Output Duration 187
Output Port 187
RS485 address 186

I/O Linkages
configuring 188
defined 188
example 188
Linkage Rule name 189

iCLASS
readers 182

icons
doors 74
RMS sites 275

Identity 157
Access Level
local gateway 157
RMS 290
Badge Profiles
RMS 292
Card Profiles
RMS 291
Card Types
local gateway 159
Cardholder Types
local gateway 161
Cardholders
local gateway 162
RMS 292
configuration order 157
RMS 290

Image Pool 228

images
cardholder photo 165
Face Recognition
requirements 221
size 221
type 221
License Plate Recognition
requirements 237
size 237
type 237

Images tab, Face Recognition 228

In Service
cameras 196
controllers 171

input device
icon LEDs 104, 108

input devices
cameras
adding 104, 109
removing 105, 109
viewing 104, 109

© 2009-2014 Next Level Security Systems, Inc.

event log 105, 110
list 104, 108
push to talk 105, 109
reports 106, 110
window 103, 107

Input Devices Available 186

Input Port 186

Install Date 137

installation
cameras 24
gateways 24
hardware 22
security certificate 22
system requirements 21

Installer 137

Intrusion
add-on defined 252
Areas
configuration 257
defined 252
operations 262
configuring 253
devices 258
Operations 260
panel 253
Zones
configuration 255
defined 252
operations 261

IP address 191
cameras 197
controller 171
decoders 203
encoder 197
gateways 143
reader interface 177

iSCSI storage
adding 192
Node 191
supported 191

K

keypad 258

L

LEDs
doors 74
input devices 104, 108

License Plate Capture
confidence 246
configuring 245
defined 66
guidelines 233, 248, 329
sensitivity 245

License Plate Match Group 235

License Plate Pool 243

License Plate Recognition
actions 330
Best Match 246
confidence 246
defined 66, 246
event linkages 330
events generated 247
groups 235
creating 244
deleting 244
guidelines 329
images
requirements 237
size 237
type 237
importing a database 238
License Plate tab 240
Personal Vehicle Pool 235
plate capture requirements 246
sample template 238
sensitivity 246

license plate recognition 235
.csv file
lpr (License Plate Recognition) 236
database
construction 236
importing 238
defined 235
deleting a person 242
editing a person 242
groups 242
accessing 243
License Plate Pool 243
management
updating 241

License Plate tab 240

Line Crossing analytic 66

Link Speed 143

Linkage Rule Name 189

lists
cameras 40
doors 74
event log 121
filtering 34
groups 113
input devices 104, 108
searching 35

© 2009-2014 Next Level Security Systems, Inc.

live video indicator 44

live/archive toggle 44

local microphone control 51

lock a video clip 102

Lock Type 184

Lock Voltage 185

locking events 124

log off
  automatic 29
  RMS 298
  Web Interface 36

login 28
  local 28
  RMS 274
    organization 274

LPR
  defined 235
  group 235

LUN 191

M

MAC address 143
  cameras 197
  controller 171
  reader interface 177

Mailing Address 134

main menu
  introduction 30
  Operations options
    local gateway 31
    RMS 276
  RMS 274

manual output, cameras 50

manual shutdown 140

maps
  adding 114
  opening a door 116
  using 114
  viewing video 116

master 210

Max Retention 200

Maximum Retention 150, 268

Media Library
  defined 99
  delete clip 102
  downloading a video clip
    local gateway 101
    RMS 278
  filtering 101
  local gateway 99
  lock 102
  RMS 276
    differences from gateway 277
  stop export 102
  using 100

menu, setting permissions 212

Mercury 169
  associating with NLSS Gateway 173
  aux input settings (MR16IN) 178
  aux output settings (MR16OUT) 179
  configuring I/O interfaces 185
  EP1501 170
  EP1501 RI 177
  EP1502 171
    inputs and outputs 177
  EP1502 RI 177
  MR50 176, 179
  MR51e 176, 179, 180
  MR52 177, 179

metrics, Video Analytics 58

Min Retention 150, 200, 268

Mini-Reader 182

mobile app
  connecting 301
  decoder 320
  getting started 300
  navigating 303
  searching 308
  usage 299
  video player 309

Motion Event 56

Mount Point 191

Mullion 182

multicast 197

Multiview
  adding 279
  defined 279
  RMS groups 280

N

navigating a configuration table 128

Needs Acknowledgment 148
  Event Linkage 156

Network Attached Storage (NAS) 190

network gateway
  not NLSS Gateway 143

© 2009-2014 Next Level Security Systems, Inc.

setting for NLSS Gateway 143
NextMobile 299
connections 301
event details 316
event log 314
Gateway menu 305
navigating 303
RMS menu 305
searching lists 308
transcode settings 310
video player 309
NFS 191
NLSS Discovery Utility
requirements 21
running 25
NLSS Unified Security Suite, defined 19
NLSS Web Interface
overview 29
using 29
Node 191
Normal State
I/O interfaces
input 188
I/O interfaces, input 187
Normally Active
I/O interface output 188
Normally Closed
doors 184
I/O interfaces 187
Normally Inactive
I/O interface output 188
Normally Open
doors 184
I/O interfaces 187
notes, events 124
NTP Server 144

O

Object Moved analytic 67
Object taken analytic 68
off line camera settings 196
OmniKey Readers, configuring automatic input 166
open environment, Face Recognition 224
Operations
cameras 38
Cardholders/Users 77
decoders 96
doors 73
Groups 112
input devices 103, 107
Intrusion 260
lists
filtering 34
searching 35
monitor cameras 42
Reports 80
System Health 32
Views 89
window overview 33
operations
Media Library
RMS 276
Operations menu
configuring access 215
overview
local gateway 31
RMS 276
operator 210
gateway permissions 213
organization
defined 274
RMS login 274
Out of Service
cameras 196
controllers 171
Out of Sync 283
Output Devices Available 187
Output Duration 187
Output Port 187

P

Panel
adding 256
configuration 253
Diagnostic tab 255
General tab 254
Zones tab 255
partner
defined 273
Patrols
accessing 48
configure 48
create 48
delete 49
using 49
Perimeter analytic 71
Permissions

© 2009-2014 Next Level Security Systems, Inc.

example 204
permissions
administrator 210
clone button 212
delete 211
groups
local gateway 207
RMS 295
master 210
operator 210
roles
add 211
cloning 216
deleting 216
edit 211
Gateway Groups tab 214
Gateway module tab 212
setting groups permissions 214
settings 211
users 217
view 211
superuser 210
users
RMS 296
Personal Vehicle Pool 235
PIN 164
reader 182
Play Audio 153
play audio, via a camera 50
played via a camera 50
Point of Sale 265
Configuration 268
Terminal Interface 268
Terminals 268
groomer settings 268
list filters 266
Operations 265
Pre-Provisioned
cameras 195
Pre-provisioned
controllers 171
Primary Contact 134
Primary DNS 143
Primary Image 228
primary user
local gateway 210
RMS 210
printing
badges 165
printing a configuration list 128
Processing 283
Prox
readers 182
Prox + Keypad 182
PTZ
actions
go to home 153
go to preset 153
start patrol 153
Custom presets 47
defined 46
Home preset 47
Patrols
accessing 48
configure 48
create 48
delete 49
using 49
presets 46
PTZ presets
deleting 48
editing 47
using 47
PTZGoToHomePos 153
PTZGoToPreset 153
PTZStartPatrol 153
push to talk
doors 76
input devices 105, 109
pushing a sequence to 98

Q

queues, event log 120
Quick Mode 115

R

reader interfaces
adding 179
Aux Input tab 178
Aux Output tab 179
configuring 175
controllers 177
deleting 180
IP address 177
MAC address 177
manually adding an MR51e 180
outputs 179
Mercury MR50 179
Mercury MR51e 179
Mercury MR52 179

© 2009-2014 Next Level Security Systems, Inc.

RS 485 address 177
types 176

Reader Mode 182

readers
configuring 181
interface port 182
PIN 182
Reader Mode 182
style 182
type 182

rebooting a Gateway 139

record video indicator 44

recording
external storage 190
maximum retention 200
minimum retention 200
playback 44
schedule 200
storage location 200

Recording Schedule 200

refreshing a configuration list 128

Remote Check Update 285

Remote Management Systems, defined 269

repairing a Gateway's internal drive 140

reports
access control 84
cameras 57, 84
decoders 84
defined 80
device-specific
defined 80
using 83
doors 76
event-specific
categories 84
defined 80
using 81
generating 80
input devices 106, 110
system 84
users 79, 84
video analytics 84
window 81

requirements
NLSS Discovery Utility 21
NLSS Web Interface 21
system 21

resolution
native
gateway 36, 55
RMS 298
playback
gateway 55
gateways 36
RMS 298

Resolution Height 198

Resolution Width 198

restoring firmware to factory settings 141

restoring Gateway configuration 138

REX (Request to Exit) 184

RMS 277, 285, 297
cardholders 292
conditional settings 280
Configuration menu 280
initial settings 281
setting dependencies 282
settings 280
transfer status 283
transferring 282
settings table 280
customer
defined 273
defined 269
deployment example 269–273
enabling 133
Event Log 297
event severity 289
events 297
export
video clip 277
Global menu 284
Customer 284
Sites 284
groups
defined 280
groups (permissions) 295
hierarchy 273
log off 298
login 274
main menu 274
master role 210
Media Library
differences from local gateway access 277
Multiview 279
organization 274
partner, defined 273
permissions
groups 295
roles
configuring 295
site
defined 273
transferring settings 273
Site details 285
backups 285
bulk transfer 286

© 2009-2014 Next Level Security Systems, Inc.

updates 285
Site Map 275
background 275
icons 275
moving 275
zoom 276
token 133
unconditional settings 280
users 296

roles
administrator 210
cloning 216
configuring 210
defined 112, 210
details 213
deleting 216
menu permissions
administrator 213
operator 213
superuser 214
Operations menu access 215
operator 210
RMS, configuring 295
setting gateway permissions 212
settings 211
superuser 210
users 217

root user
local gateway 210
RMS 210

RS485 address
I/O interface 186
Mercury MR50 176
Mercury MR52 177
range 186
reader interfaces 177

RTSP 196
add unsupported cameras 201

S

sample rate
audio analytics 249
audio stream 199

sample template
License Plate Recognition 238

sample template, Face Recognition 223, 294

schedule
Access Level 158

Schedule Name 147

schedules
access levels 146
camera 146
configuring for Gateways 146
creating 147
Days of the Week 147
disable for holidays 147
doors 146
end time 147
events 155
I/O linkages 189
recording 200
RMS 288
start time 147

searching
configuration tables 128
mobile app 308

Secondary DNS 143

Security Certificate 22

Sensitivity 232, 245, 246

sensitivity
License Plate Capture 245

sequences 88
creating 94
deleting 95
displaying 95
editing 94
menu 93
push to decoder 98

Serial Number 137
decoder 203

serial number, camera 197

settings
gateway time 144
RMS bulk transfer 286
roles 210, 213

severity, Needs Acknowledgment 148

shunting events 124

shutting down a Gateway
local interface 139
manually 140

Site Address 135

Site Map 275
upload map or graphic 275

Site Name 135

sites
details
local gateway 135
RMS 285
icons 275
moving 275
local gateway 135
RMS 273

© 2009-2014 Next Level Security Systems, Inc.

backups 285
updates 285
RMS Global menu 284
RMS interface 275
SkipToKeyFrame 199
smart phone access 299
snapshot
event 124
video 51
sound effects, playing 50
specifications
audio analytics 334
configuration 334
environmental 334
performance 334
SSH 137
Start Date
holidays 145
video export 52
Start Time
schedules 147
video export 52
Stopped, transfer status 283
Stream URL 197
StreamRecordStart 153
StreamRecordStop 153
streams
adding to the cameras list 201
external storage 190
recording schedule 200
selecting 54
settings 200
types 196
URL source 197
Strike Time Default, controllers 172
Strike Time Override, doors 185
Subnet Mask, gateways 143
subscriptions
adding tokens 133
configuring 132
RMS 133
superuser 210
gateway permissions 214
support
configuration backup 337
contact information 338
contacting 336
system log 337
Switchplate 182
synchronized playback 91
System Health 32
system logs
downloading 139
for support 337
system logs, downloading 139
system reports 84
System Requirements 21

T

tablet access 299
talkback 51
cameras 51
doors 76
input devices 105, 109
TCP 199
terminal interface 268
terminals 268
Time Mode 144
Time tab 144
Time Zone 144
time, manually setting 144
tokens 133
RMS 133
toolbar
overview 43
using 43
transactions
events 265
searching 266
types 266
transcode
gateway 36, 55
NextMobile 310
RMS 298
Transferred 283
transferring RMS settings 282
status 283
transferring video clips 277
Transport Control 91
troubleshooting
video analytics 71
Type

© 2009-2014 Next Level Security Systems, Inc.

doors 184
lock 184

types
actions 152
reader interfaces 176
severity 148

U

UDP 199

Unassigned 283

unconditional settings, RMS 280

unlocking a door 75

Updates tab, RMS 285

uploading images
Face Recognition 228

URL
stream 197

USB storage 192

Use Multicast 197

use with actions 154

User ID 218

users
configuring 217
defined 77, 112, 217
RMS 296
details 218
information 78, 218
reports 84
selecting roles 218

userSuppliedID 221, 236

V

validate
group by face recognition 152

VAStart 153

VBR
quality 199
Upper Cap 199

version
controller hardware 172
decoder firmware 203
decoder hardware 203
updating
from web 140
manual 141

video
actions
record stream, start 153
record stream, stop 153
adding streams 201
external storage 190
information 43
live indicator 44
recorded indicator 44
recording schedule 200
stream parameters 198
viewing from floorplans & maps 116

video analytics
Activity 61
Audio 50, 249
defined 49
Direction 62
Dwell 63
Face Capture 64
Face Recognition 64, 65, 232
forensics 72
impact on processing 58
License Plate Capture 66
License Plate Recognition 66, 246
Line Crossing 66
Object Moved 67
Object Taken 68
People Count
People Count analytic 69
People Count Directional
People Count Directional analytic 70
performance 325
Perimeter 71
reports 84
start by action 153
stop by action 153
troubleshooting 71
using 59

video clip
delete 102
downloading
local gateway 101
RMS 278
lock 102
pushing to a decoder 97
stop export 102
transferring to RMS 277

Video Codec
setting 198

video forensics 72

Video menu 190

video player
cameras 43
mobile app 309
NextMobile 309

View permission 211

© 2009-2014 Next Level Security Systems, Inc.

views 88
creating 90
delete 92
edit 90
layout 89
menu 89
overview 88
push to decoder 98
set active by action 153
transport control 91

ViewSetActive 153

volume
camera mute 51
local gateway interface 30
RMS interface 275

W

Web Interface
log off 36
logging in 28
requirements 21

Wire Network Tab, Gateways 142

Z

Zone expander 258

Zones
adding a camera 260
defined 252
operations 261

zoom 50
Site Map (RMS) 276