BRIVO ONSITE SERVER ADMINISTRATOR'S MANUAL

06/25/2020

brivo®
simply better security

Legal Disclaimers

Canada-Underwriters Laboratories (C-UL) Compliancy

For C-UL Listed applications, the unit shall be installed in accordance with Part 1 of the Canadian Electrical Code.

Documentation Disclaimer and Restrictions

Information in this document is subject to change without notice and does not represent a commitment on the part of Brivo Systems LLC. For the most up-to-date information, visit www.brivo.com.

This document and the data herein shall not be duplicated, used or disclosed to others for procurement or manufacturing, except as authorized with the written permission of Brivo Systems LLC. The information contained within this document or within the product itself is considered the exclusive property of Brivo Systems LLC. All information in this document or within the hardware and software product themselves is protected by the copyright and/or other intellectual property laws of the United States.

Product Support

All support for this product is provided by the third-party dealer. Please contact the dealer who installed the product with questions and support requests.

Brivo® is a registered trademark of Brivo Systems LLC. Brivo Systems LLC, 7700 Old Georgetown Road, Suite 300, Bethesda, MD 20814.

Table of Contents

1. Getting Started 11

System Overview: Brivo Onsite Server Software Application 12
Brivo Onsite Server System Architecture 13
Brivo ACS5000-S control panels in Client Mode 14
Browser Requirements 15
Main Features of the Brivo Onsite Server 16

2. Network Environment 17

Networking Requirements 18
Adding a Brivo Control Panel to Brivo Onsite Server 20
Accessing Brivo Onsite Server 22

3. Home 24

4. Status 25

Browsing the Dashboard 26
Managing the Dashboard 29
What is Alarm Text? 33
Using Display Filters 38
Live Map/Floorplan 40

5. History 41

What is Activity? 42
Browsing the System Activity Log 43
Index of Events 45
Generating an Activity Report 48
Exporting the Activity Log 50
What is Reporting? 51
Browsing the Reports List 52
Creating a New Report 53
Managing Reports 54
Browsing the Scheduled Reports List 57
Creating a New Scheduled Report 58
Managing Scheduled Reports 60
Running a Muster Report 62
Browsing the Administrative Journal 63

6. Users & Groups 64

What are Users, User Aliases, and Groups? 65
Browsing the Users List 66
Viewing User Details 67
Creating a User 69
Managing Users 73
Browsing the Groups List 75
Viewing Group Details 76
Creating a Group 78
Creating a Group Enabled Schedule 80
Managing Groups 82

Managing Custom Fields 84

7. Cards 87

What is a Card? 88
Browsing the Cards List 89
Adding Cards 91
Managing Card Formats 93
Managing Card Assignments 99
Managing Cards 100

8. Badging 102

What are Badges? 103
Badge Templates 104

9. Accounts 113

What is an Account? 114
Defining the Initial System Account Administrator 115
Viewing Account Details 119
Creating Tenant Accounts 121
Managing Account Contact Information 124

10. Email Notifications 125

What are Email Notifications? 126
Browsing the Notifications List 127
Creating Notification Rules 128
Managing Notification Rules 129
Sample Email Notifications 130

11. Administrators and Administrator Roles 131

Administrator Roles 135
Definitions of Permissions 136

12. Threat Levels 140

Who Can Change Threat Levels? 141
Threat Level Influence 142
Threat Level Configuration 144
Threat Level Severity 146
Editing Permissions for Threat Levels 148
Editing Devices for Threat Levels 149
Editing Schedules for Threat Levels 150
Threat Levels and Shared Devices 151

13. Antipassback 152

Antipassback Zones 153
Antipassback Definitions 154
Hard Antipassback 154
Soft Antipassback Reset Interval 154
Antipassback Immunity 154
Important Antipassback Considerations 155

Managing Antipassback Controls 156

14. Devices 160

Managing Multiple Control Panels 162
Programmable Devices 163
Special Options for Devices: Floors and Elevators 164
Special Options for Devices: Cameras 167
Special Options for Devices: DVRs 169
Special Options for Devices: Muster Points 172
Special Options for Devices: Keypad Commands 174
Special Options for Devices: Guard Tour 176
Special Options for Devices: Salto Routers and Salto Door Locks 178
Special Options for Devices: DEDs (Data Entry Devices) 182
Special Options for Devices: IPAC Devices 184
Special Options for Devices: NDE Gateways and Locks 186
Viewing Video 190
Viewing Panel and Board Details 192
Update and/or Configure a Control Panel 195
Control Panel Options 196
Adding Control Boards 199
Managing Control Boards 200
Browsing the Devices List 203
Viewing Device Details 204
Creating Devices 207
Device Profiles 208
Live Status 210
Managing Devices 212

15. Schedules and Holidays 219

What are Schedules? 220
What are Holidays? 221
Browsing the Schedules List 222
Viewing Schedule Details 223
Creating a Schedule 224
Managing Schedules 227
Browsing the Holidays List 228
Creating a Holiday 229
Managing Holidays 230

16. Maps/Floorplans 231

Maps/Floorplans Definitions 232
Browsing Maps/Floorplans 233
Managing Maps/Floorplans 234
Live Map 240

17. System Management 243

Maintenance Mode 244
Browsing the System Status Page/Using Maintenance Mode 245
Browsing the System Logs 247
Using System Tools 248
Panel Comms Monitoring 249

Session Management 250
Manage Running Reports 251
Fetch Panel Logs 252
Diagnostic 255
Setting System Date and Time 257
SNMP Agent Settings 258
Upgrading Your Firmware 259
Upgrading Panels 261
License Keys 262
Manage Branding 264
Security Settings 266
Importing User Data 267
Backing up Your Database 269
Backup Server 271
Report Service 273
Configuring the Network 274
Configuring Network Routing 276
Configuring the SMTP Server 277
Panel Discovery 278
Custom Server Certificates 281
ES IP Pool Configuration 282

18. Tenant Accounts 284

Changes in System Account Administrator Access 285
Tenant Administrator Access 289

19. Appendices 291

Appendix 1: Glossary 292
Appendix 2: Use of Report Service 297
Appendix 3: Salto Equipment 300
Appendix 4: Obix Integration 316
Appendix 5: DVR Installation Notes 320

Table of Figures

Figure 1. Brivo Onsite Server System Architecture 13
Figure 2. Brivo ACS5000-S Client Mode 14
Figure 3. Brivo Onsite Server on a single LAN 18
Figure 4. Brivo Onsite Server with Multiple Panels on Multiple LANs 19
Figure 5. Brivo ACS5000-S Client Mode Settings 20
Figure 6. Back of Brivo Onsite Server appliance 22
Figure 7. Brivo Onsite Server direct console static IP setup 23
Figure 8. Home Page for Brivo Onsite Server 24
Figure 9. View Dashboard and Live Status 26
Figure 10. Dashboard Activity List – Pulse Event Entry 29
Figure 11. Dashboard Activity List – Latch Event Entry 29
Figure 12. Dashboard Activity List – Unlatch Event Entry 30
Figure 13. Dashboard Activity List – Door Locked Event Entry 30
Figure 14. Dashboard Activity List – Door Unlocked Event Entry 30
Figure 15. Dashboard Activity List: Door Returned to Unlock Schedule 31
Figure 16. Dashboard Display Filter 31
Figure 17. Alarm Console Settings 32
Figure 18. Creating an Alarm Text Message 33
Figure 19. Alarm Update/Acknowledgement 34
Figure 20. Alarm Clear 34
Figure 21. Alarm Console Settings for Doors, Valid Credential Devices, and Elevators 35
Figure 22. Settings for Event Triggers, Input Switches, Etc. 36
Figure 23. Swipe & Show display 37
Figure 24. Filters 38
Figure 25. Filter Details 38
Figure 26. Create New Filter 39
Figure 27. View Live Map 40
Figure 28. View System Activity Log 43
Figure 29. Generate Activity Report 48
Figure 30. View Activity Report 49
Figure 31. Export Activity Log 50
Figure 32. View Reports List 52
Figure 33. Create New Report 53
Figure 34. View a Report 54
Figure 35. Edit a Report 55
Figure 36. View Scheduled Reports List 57
Figure 37. Create New Scheduled Report 58
Figure 38. View a Scheduled Report 60
Figure 39. Edit a Scheduled Report 61
Figure 40. Generating a Muster Report 62
Figure 41. View Administrative Journal 63
Figure 42. View Users List 66
Figure 43. View User Details 67
Figure 44. Create a New User 69
Figure 45. Select a Card Popup List 70
Figure 46. Create a User Alias 71
Figure 47. Aliased User 71
Figure 48. Rehoming a User Alias 72
Figure 49. Edit a User 73
Figure 50. View Groups List 75

Figure 51. View Group Details 76
Figure 52. Create New Group 78
Figure 53. Edit a Group 82
Figure 54. View Custom Fields List 84
Figure 55. Create a Custom Field 85
Figure 56. Rename a Custom Field 85
Figure 57. Viewing Cards List 89
Figure 58. Add New Cards 91
Figure 59. Add Card by Value 92
Figure 60. View Card Formats 93
Figure 61. View Card Format Details 94
Figure 62. Create New Card Format 95
Figure 63. Copy Card Format 97
Figure 64. Edit Card Format 98
Figure 65. Delete Multiple Cards 100
Figure 66. Create Badge Template 104
Figure 67. Template Properties 105
Figure 68. Field Properties 105
Figure 69. Choose Color 106
Figure 70. Examples of Standard Text Objects 107
Figure 71. User Photo Icon 108
Figure 72. User Photo Properties 108
Figure 73. Static Image Icon 109
Figure 74. Static Image Properties 109
Figure 75. Print Preview 111
Figure 76. Print Badge 111
Figure 77. Log In 115
Figure 78. System Account Administrator Creation Page 116
Figure 79. Set up System Account 117
Figure 80. View Account Details 119
Figure 81. Create Tenant Account 121
Figure 82. View Active Account 122
Figure 83. Edit Account Details 124
Figure 84. View Email Notifications List 127
Figure 85. Create Notification Rule 128
Figure 86. Edit Email Notification Rule 129
Figure 87. View Current Administrators 132
Figure 88. Create New Administrator 132
Figure 89. View Administrator Details 133
Figure 90. View Administrator Roles 135
Figure 91. Create New Administrator Role 138
Figure 92. Threat Level engaged 143
Figure 93. Create a Threat Level 145
Figure 94. Edit Threat Level 145
Figure 95. Threat Level Severity 146
Figure 96. Change Threat Level Icon 147
Figure 97. Change Threat Level Popup 147
Figure 98. Setting threat level permissions for a group 148
Figure 99. Setting threat level permissions for a device 149
Figure 100. Setting threat level permissions for a schedule 150
Figure 101. Enabling threat levels 151
Figure 102. Create Antipassback Zone 156
Figure 103. Create New Floor 164

Figure 104. Create New Elevator 165
Figure 105. List of Devices 167
Figure 106. Create Cameras 168
Figure 107. DVR Driver Details 169
Figure 108. Install DVR Driver 170
Figure 109. Create New DVR 170
Figure 110. Create Muster Point 173
Figure 111. Create Keypad Command Device 175
Figure 112. Create Guard Tour 177
Figure 113. Create Salto Router 179
Figure 114. Create Salto Door Lock 181
Figure 115. Create a Data Entry Device (DED) 183
Figure 116. Create an NDE Gateway Device 186
Figure 117. Create an NDE Lock Device 188
Figure 118. Viewing Live Video 190
Figure 119. Event Based Video Playback 191
Figure 120. Control Panel Details 193
Figure 121. Configure Brivo Control Panel 195
Figure 122. Add a Control Panel 196
Figure 123. Devices: Control Panels 197
Figure 124. Devices: Edit Control Panel Details 197
Figure 125. Add New Board 199
Figure 126. Define Door Board Settings 200
Figure 127. Define IO Board Settings 202
Figure 128. View Devices List 203
Figure 129. Device Details: Valid Credential Device 205
Figure 130. Create a Device 207
Figure 131. Customize Live Status Message 210
Figure 132. Configure a Door 213
Figure 133. View Schedules List 222
Figure 134. View Schedule Details 223
Figure 135. Create New Schedule 224
Figure 136. Edit Schedule 227
Figure 137. View Holidays List 228
Figure 138. Create a Holiday 229
Figure 139. Edit a Holiday 230
Figure 140. Create a Map 234
Figure 141. Add an Icon 236
Figure 142. Add a Region 238
Figure 143. View Live Map 241
Figure 144. Maintenance Mode Warning Message 244
Figure 145. System Status 245
Figure 146. View System Log: Application 247
Figure 147. Enter System Command 248
Figure 148. Panel Comms Monitoring 249
Figure 149. System: Active Sessions 250
Figure 150. Managing Reports 251
Figure 151. Fetch Panel Logs Display Page 252
Figure 152. Individual List of Panel Logs Display Page 253
Figure 153. Viewing Individual Panel Log Details 254
Figure 154. Diagnostic Display 256
Figure 155. Set System Date and Time 257
Figure 156. System: SNMP Agent Settings 258

Figure 157. Upgrade System Firmware 259
Figure 158. Upgrading a Panel 261
Figure 159. Upload License File 263
Figure 160. Manage Branding 264
Figure 161. Security Settings Page 266
Figure 162. Import User Data, Step One 267
Figure 163. Import User Data, Step Two 268
Figure 164. Backup and Restore the Database 269
Figure 165. Backup Server Settings 271
Figure 166. Activating Report Service 273
Figure 167. Configure the Network 274
Figure 168. Configure Network Routing 276
Figure 169. Configure SMTP Server 277
Figure 170. Panel Discovery 278
Figure 171. Panel Scan 279
Figure 172. Discovered Panels 279
Figure 173. Configuring Panel 280
Figure 174. Custom Server Certificates 281
Figure 175. Elevator System IP Pool Configuration 282
Figure 176. Active Account 285
Figure 177. Select Active Account 285
Figure 178. View Accounts List 286
Figure 179. Share a Door or Valid Credential Device 288

1. Getting Started

System Overview: Brivo Onsite Server Software Application

Brivo Onsite Server is a standalone access control system. With the use of the Brivo Onsite Server appliance, it can also span multiple facilities, with the master server residing at one of those facilities, as determined by the end user. All Brivo Onsite Server appliances are fully browser-managed, and accessible via the Internet with appropriate network configuration.

The Brivo Onsite Server's software application interface is accessible via a web browser and is divided into six sections. When you scroll over a section link, a corresponding dropdown menu displays, providing access to data maintained in that section.

The Home section provides links to common tasks based on the level of access of the Account Administrator.

The Status section lets the System Account Administrator access the Dashboard which provides a three-fold administrative functionality for monitoring and controlling the output behavior of programmable system devices, and Maps/Floorplans which allows the administration of maps/floorplans

The History section provides access to Activity, which includes System Activity log, Activity Reporting, and Activity Export; Reporting, which includes Reports, Scheduled Reports, and Muster Reports; and the Administrative Journal. The System Activity log tracks access-related events, such as doors being opened and closed, and devices being switched on and off. Activity Reporting allows Account Administrators to gather information based on certain events, for specific devices, or for certain groups and users. Activity Export allows for the creation of a tab separated file for events during a given timeframe. The Administrative Journal tracks actions performed by Account Administrators of Brivo Onsite Server such as the creation or deletion of an access schedule.

The Users section allows Administrators to manage the set of users to be given access to the facility. Groups are managed from this section. Card inventory is also managed from this section.

The Configuration section provides Administrators to ability to set up various areas of the account. The Account section shows the Account Details as well as permits the creation of the System Account as well as any additional Tenant Accounts. This section also allows you to define rules for automatically emailing select individuals when specific security events occur, to establish alarm text for alarm events, and to define custom fields for maintaining additional information on users who have access to a facility. New Administrators as well as additional Administrator Roles are managed from this section. Threat level management, if active, is controlled from this section. The Cards section manages card formats and badging. The Devices section lets System Account Administrators manage doors, devices, control panels, and DVRs associated with the building, as well as antipassback administration. The Scheduling section provides Administrators the ability to manage specific periods of time during which a device might be accessed or operated. The Dashboard section allows the creation of maps/floorplans and for the display and creation of filters.

The System section is used to configure and monitor system operations, including licensing, database backups, firmware upgrades, and data imports.

At the top of each page you will also find:

- A Help link that transfers you to Brivo's help documentation.
- A Log Out button at the end of the section menu bar that allows you to exit Brivo Onsite Server in a secure manner.
- A Threat Level icon that allows the user to change the threat level of the account, provided the individual logged in has the privilege to use this function.

	***NOTE:*** *Individuals with access to Brivo Onsite Server are referred to as Administrators. Administrators have varying levels of control as described in the Administrator Roles section.* *Individuals with access to a facility who cannot log in to Brivo Onsite Server are referred to as Users.*

Brivo Onsite Server System Architecture

Brivo Onsite Server is an access control *appliance* and software interface that is compatible with ACS6000-A, ACS5000-A, ACS300-A, and ACS-IPDC-1A or ACS-IPDC-2A.

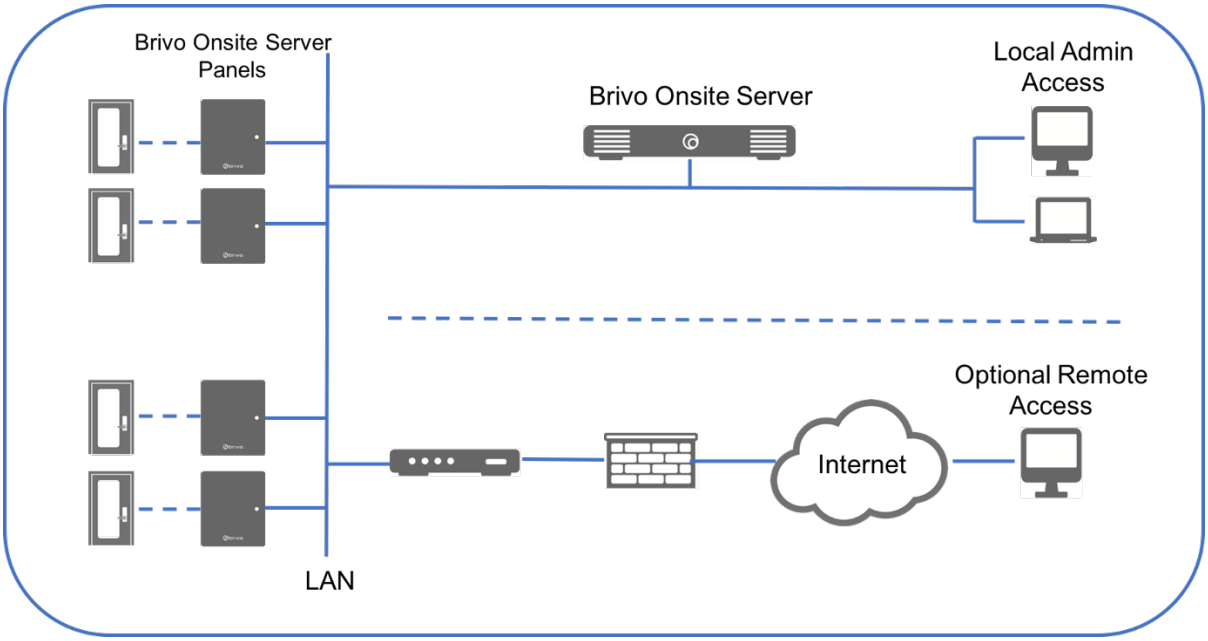


Figure 1. Brivo Onsite Server System Architecture

Brivo ACS5000-S control panels in Client Mode

A Brivo ACS5000-S panel is in Client Mode when it has been connected to a Brivo Onsite Server appliance and therefore becomes integrated into the Brivo Onsite Server system.

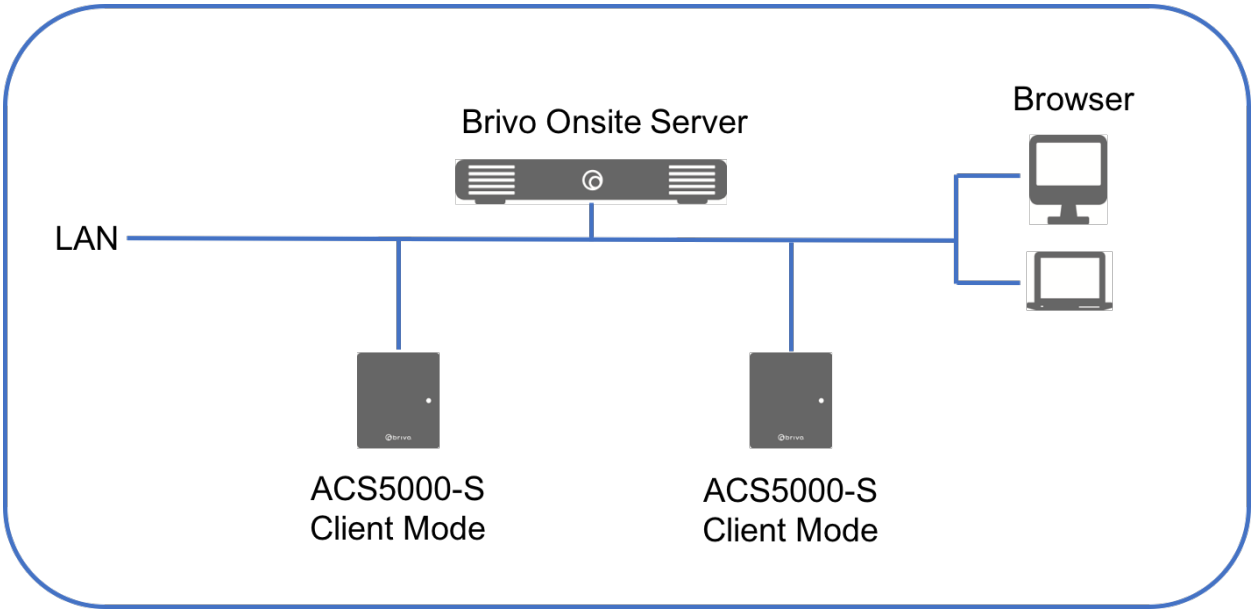


Figure 2. Brivo ACS5000-S Client Mode

	***WARNING: Brivo ACS5000-S Firmware Changes*** *Once a Brivo ACS5000-S panel has been connected to a Brivo Onsite Server appliance, its firmware is replaced and it can no longer function as an independent panel.*

	*NOTE:* *The majority of this document assumes you have a single System Account. For a description of how Brivo Onsite Server operates differently when Tenant Accounts are defined, see the* Tenant Accounts *Section.* *In situations where only one business occupies a building, security is managed via a single System Account. If, however, there are multiple businesses leasing portions of a building, the System Account can be used to manage building-wide security, while individual Tenant Accounts are created for each business, enabling them to manage their own internal security.*

Browser Requirements

You can use any standard Web browser to access the interface. Note that video playback functionality may vary by DVR type. Please see specific DVR driver documentation for more information.

The interface uses *cookies* to preserve session information. If your browser disallows cookies, the interface will not function properly.

The interface uses JavaScript to validate form data, control navigation and display images. If your browser has *scripting* disabled, the interface will not function properly.

Some functional elements appear in pop-up windows. If you have installed software that blocks pop-up windows, the interface will not function properly.

Main Features of the Brivo Onsite Server

Application runs locally on the Brivo Onsite Server access control appliance

Up to 500,002 users

Up to 1,000 readers/doors

Customizable administrator roles

Supports the ability to add control panels and Edge devices

Supports Digital Video Playback with supported DVRs

Supports an integrated badging application

Supports interactive maps and floorplans

Supports varied threat levels for increased security

Supports global antipassback

Supports mustering

Supports reporting

Supports guard tours

2. Network Environment

This section describes the basic operation of the Brivo Onsite Server series in an IP network environment.

First, the network requirements are identified. Next, the steps for accessing Brivo Onsite Server are outlined.

Networking Requirements

Brivo Onsite Server with multiple Brivo panels on a single LAN

The following network requirements are applicable to a system in which a Brivo Onsite Server appliance is managing one or more Brivo ACS5000-A, ACS6000-A, ACS300-A, ACS-IPDC-1A, or ACS-IPDC-2A control panels on a single LAN (i.e., a single IP subnet or address space), as shown in the figure below.

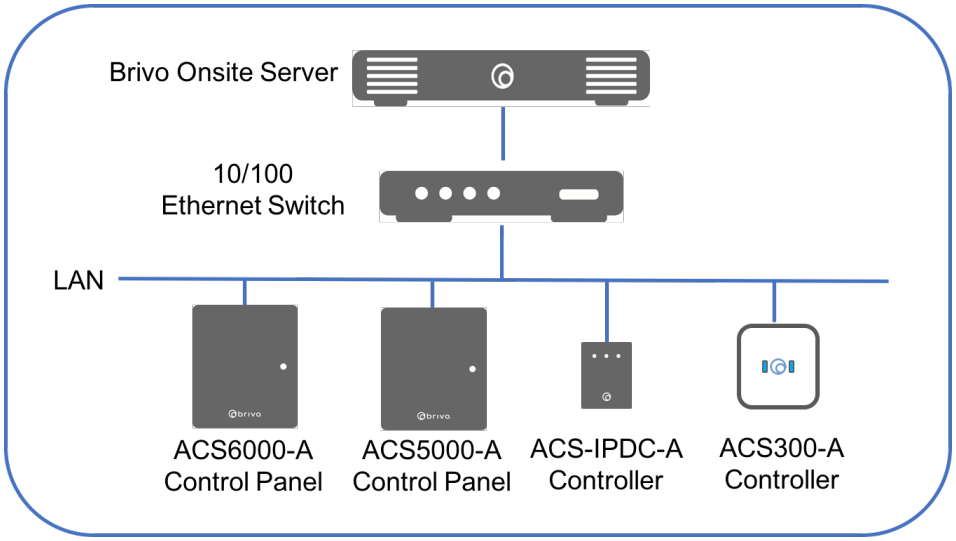


Figure 3. Brivo Onsite Server on a single LAN

Requirements	Comment
Ethernet 10/100 Base T LAN	CAT5 Cabling with RJ45 Connectors
Ethernet Hub/Switch set to Auto-Negotiate	Most hubs and switches default to auto-negotiate, which is the preferred setting.
IP Addressing – Brivo Onsite Server	A static IP address is required for the Brivo Onsite Server appliance. Consult your local network administrator for a suitable static IP address for the appliance.
IP Addressing – ACS5000-A, ACS6000-A, ACS300-A, ACS-IPDC-1A or ACS-IPDC-2A	The Brivo ACS5000-A, ACS6000-A, ACS300-A, ACS-IPDC-1A, or ACS-IPDC-2A panels being controlled by the Brivo Onsite Server appliance may be configured with either DHCP or a static IP address. Please see the local network administrator for a preferred configuration for these settings.
Proxy (not required)	The existence of a proxy on the LAN is not relevant to the Brivo Onsite Server because it is a Web server; however, outside access to the appliance may require the end user to be aware of proxy settings for proper behavior of his/her browser. Consult your local network administrator for further information about proxy settings.

Brivo Onsite Server with multiple Brivo panels on multiple LANs

The following network requirements are applicable to a system in which a Brivo Onsite Server appliance is managing one or more Brivo ACS5000-A, ACS6000-A, ACS300-A, ACS-IPDC-1A, or ACS-IPDC-2A control panels on multiple LANs (i.e., typically multiple sites, each with their own connection to the Internet or a corporate WAN) as shown in the figure below.

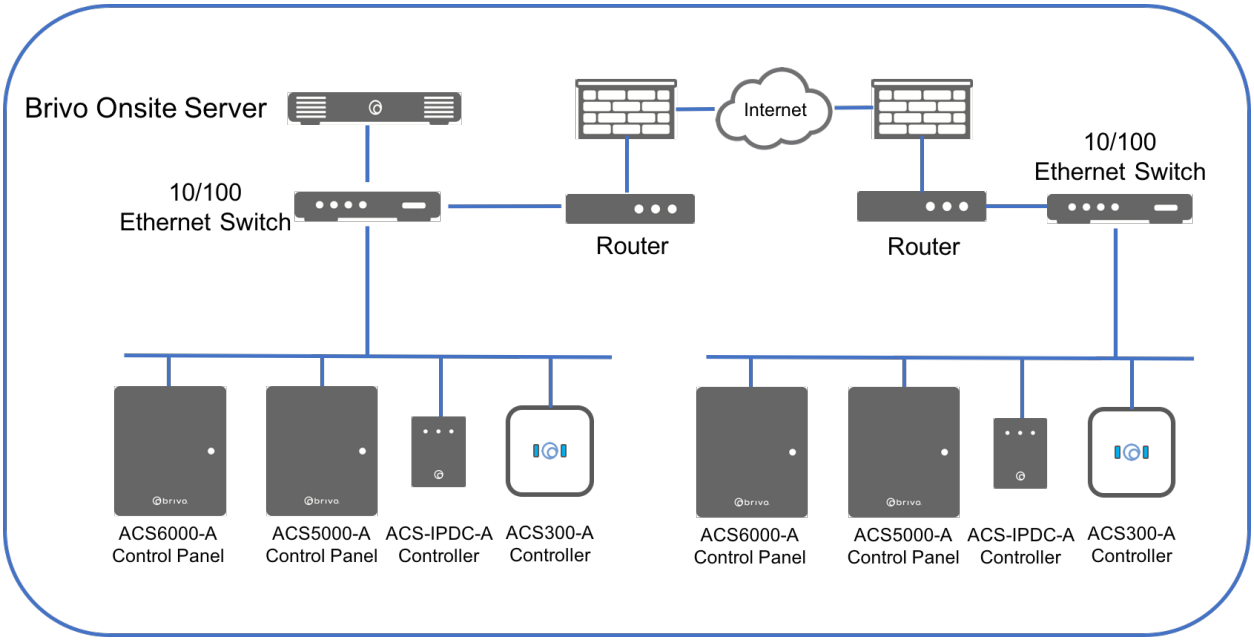


Figure 4. Brivo Onsite Server with Multiple Panels on Multiple LANs

The following requirements for a multi-site Brivo Onsite Server network are in addition to the requirements for a single LAN.

Requirements	Comment
Site-to-site (LAN-to-LAN) connectivity	The sites where the Brivo Onsite Server and Brivo ACS5000-A, ACS6000-A, ACS300-A, ACS-IPDC-1A, or ACS-IPDC-2A equipment is located must all be able to connect to a common networking environment such as the Internet or a corporate WAN.
IP routing	There must be an IP route established between the sites where the Brivo Onsite Server equipment is located. This must be performed by the network administrator for those sites. Typical approaches include VPNs, public IP addresses, port forwarding, etc. Contact the network administrator to determine the proper configuration.

Adding a Brivo Control Panel to Brivo Onsite Server

	NOTE: *Unless otherwise noted, the term "control panel" in this document refers to either ACS5000 or ACS6000 panels, ACS300 Controllers or IP Door Controllers (IPDC). While the general procedures for managing earlier versions of control panels may be similar, you should refer to the documentation for your specific Brivo Onsite Server product for instructions on creating, editing and deleting control panels.*

The Brivo Onsite Server appliance can support up to as many control panels as necessary for their full reader capacity. The panels can be a mix of Brivo ACS5000-A or ACS6000-A control panels with up to fourteen expansion boards each for a maximum total of 30 readers. Alternately, each ACS-IPDC-A or ACS300-A controllers can control up to a maximum of two readers.

In either case, the panels or controllers must be individually configured with the IP address of the Brivo Onsite Server appliance it will get data from.

In order to configure a panel or controller, you will need the following:

- A network connection to the panel or controller
- The IP address of the Brivo Onsite Server appliance

The IP address of the Brivo Onsite Server appliance is available from the System Administrator.

To configure the panel or device to connect to a Brivo Onsite panel or Edge device, do the following:

1. Open http://*ip-address*/cgi-bin/server.cgi in a browser, where *ip-address* is the address of the panel or device you are configuring.
2. In the Server IP Address box, enter the IP address of the Brivo Onsite Server appliance from where the panel or device will retrieve data.

Figure 5. Brivo ACS5000-S Client Mode Settings

3. Click Save.

The panel or device will connect to the server and retrieve whatever firmware/settings are necessary.

	***WARNING:** Do not interrupt the process once started. If you make a mistake, let the process finish before attempting to correct. Interrupting the installation of new firmware can damage the panel or device*

Adding a Brivo ACS5000-S panel using manual handshake mode

Usually, Panel Discovery is the primary method by which Brivo Onsite Server detects and adds new panels. However, there are times when complex networking setups (firewalls, WANs) do not allow for this. A secondary manual handshake process with instructions listed below allows for a panel to be added to Brivo Onsite Server in situations where Panel Discovery is not used. A laptop will be required for this process.

1. Plug the laptop into the ADMIN port on the main board of the Brivo ACS5000-S panel.
1. Power the laptop on.
2. The panel must use firmware version 1.1.1 or later. If the panel has 1.1.1 or later, proceed to step 4. If not, to upgrade:
   a) Open browser to "Onsite.brivo.com"
   b) Enter admin into the username field and click Login.
   c) Click the link that says "Click here if you have a Brivo Onsite backup file you wish to restore."
   d) Click the Upgrade Firmware option from the navigation menu on the left.
   e) Click the Export Data button, and click "Cancel" on the "Save As" dialog box that pops up.
   f) Click the Browse button and select the brivo-Onsite-1.1.1.bin file downloaded from www.brivo.com
   g) Click Upgrade. The upgrade process will take a few minutes.
3. Open your browser to http://Onsite.brivo.com/cgi-bin/server.cgi
4. Enter the IP Address of the appliance into the field on the page.
5. Click Save.
6. The system will take a few minutes to handshake with the Brivo Onsite Server appliance.

The Brivo ACS5000-S has now been configured to operate with the Brivo Onsite Server appliance.

Accessing Brivo Onsite Server

This section describes how to connect to the Brivo Onsite Server appliance.

In order to access Brivo Onsite Server you will need to:

- Connect a laptop to the Brivo Onsite Server appliance
- Set a static IP address

Alternately, you can use the Brivo Onsite Server Console Interface to configure a static IP address. To do this you will need to:

- Connect a monitor and keyboard to the Brivo Onsite Server appliance
- Set a static IP address

Connecting to the Brivo Onsite Server appliance from Laptop:

The Brivo Onsite Server will boot with a static IP address of: 169.254.242.207.

You will need to:

1. Connect your laptop to Ethernet Port 1 (clearly labeled) on the back of the appliance.

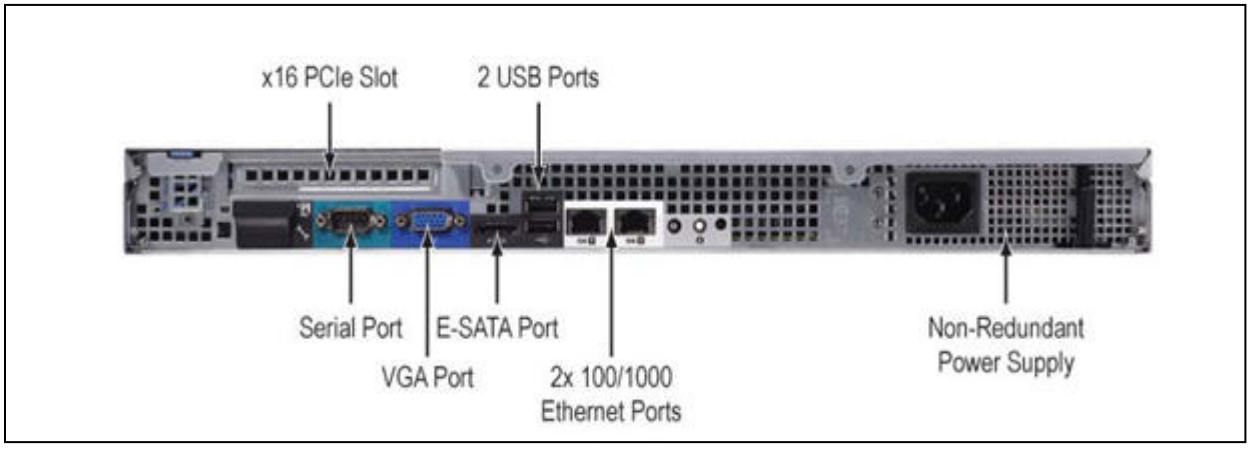


Figure 6. Back of Brivo Onsite Server appliance

2. Your laptop should default to an appropriate address on this same network (i.e., 169.254.xxx.xxx); if it does not, please use the manual networking settings tools on your laptop to configure it to an address on the 169.254.xxx.xxx network).
3. Log on to your laptop and open a browser to http://169.254.xxx.xxx to access Brivo Onsite Server.
4. See the *Configuring the Network* section for information on how to assign a static IP address for the LAN.

Direct console:

The Brivo Onsite Server appliance supports a USB keyboard and monitor to present a basic network configuration console-based interface. It is generally necessary to configure a static IP address for the Brivo Onsite Server appliance. The Network Settings dialog prompts for static address parameters.

	NOTE: *If DHCP is required, please use the initial static IP address for the appliance to log into the main application and select DHCP addressing.*

1. Connect a VGA monitor and keyboard to appropriate ports on the Brivo Onsite Server appliance
2. Log in with username "admin" and no password (for first login) or use the initially configured admin password.
3. To set a static IP address for the LAN, select Network Settings from the main menu.
4. Enter the appropriate IP address information.

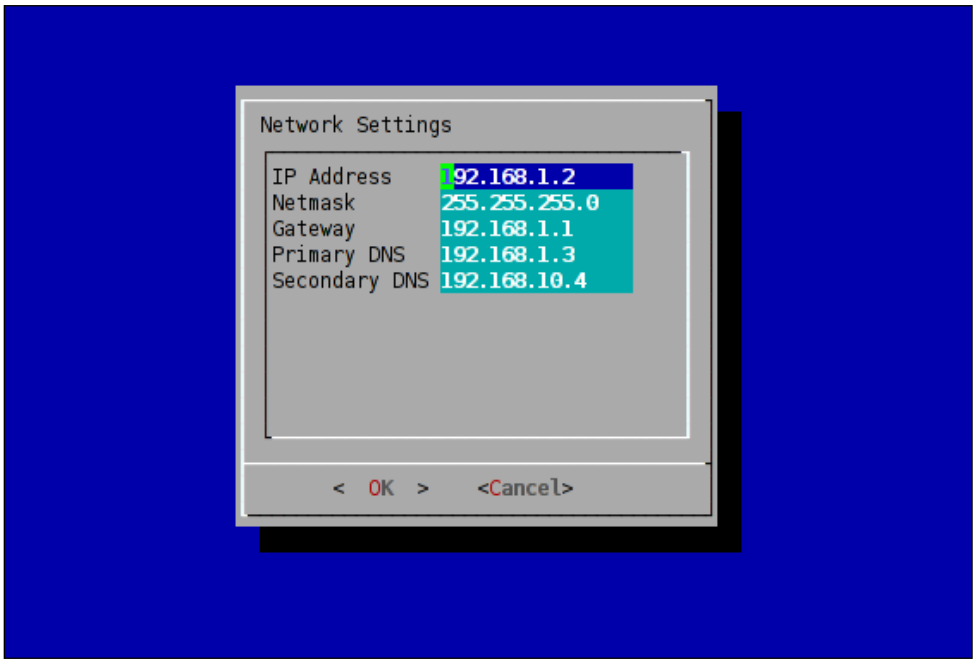


Figure 7. Brivo Onsite Server direct console static IP setup

5. Press Enter to save settings.

3. Home

The Home page is the initial page displayed after logging into the interface. The Home page provides a list of Common Tasks and Reports available to the Administrator. The contents of these lists can change dependent upon the permissions of the Administrator as defined by their Administrator Role. For example, if an administrator could not add new cards, the Add New Cards link would not appear in the Common Tasks list. For more information on the setup and defining of Administrators and Administrator Roles, see the Accounts chapter.

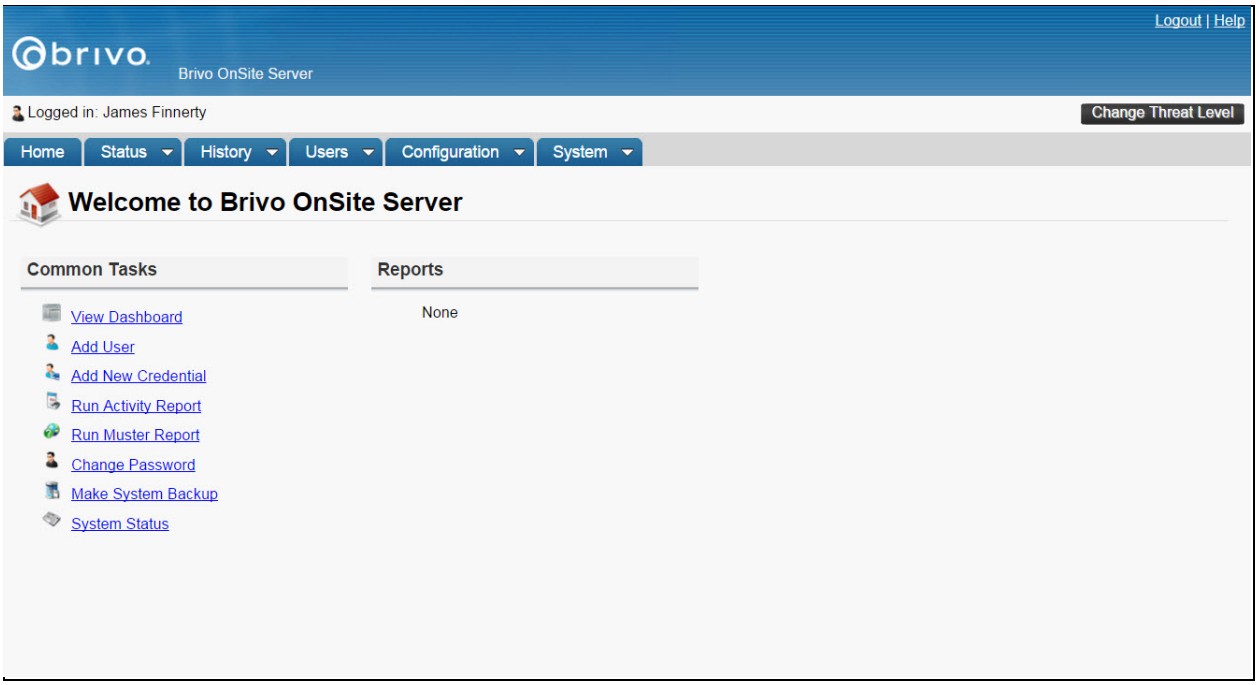


Figure 8. Home Page for Brivo Onsite Server

4. Status

The Status Page provides a two-fold administrative functionality for monitoring and controlling the output behavior of programmable system devices, as well as the monitoring of live device maps and floorplans.

On the Dashboard itself, the left side of the Dashboard page displays the Activity, Alarm Console (if enabled), and Swipe & Show tabs. The Activity tab is a dynamic system Activity Log that automatically refreshes in three seconds or less with the most recent events in reverse chronological order (i.e., most recent event at the top; earliest event at the bottom) and associates these events with a time-stamp and the name of the device involved. The Alarm Console tab (if enabled) shows the time and date stamp for any alarm events as well as the device linked to the alarm event and a button to acknowledge the alarm event. The Swipe & Show tab shows the last eight credentials swiped at a selected device along with any picture associated with the credential holder. The right side of the Dashboard page displays the Device Status, Hardware Status, and Schedule Status tabs. The Device Status tab lists system devices in alphabetical order, along with their lock/unlock status. The Hardware Status tab lists the connection status of control panels associated with the account. The Schedule Status tab lists schedules that are configured as group activated. For Administrators configured to use it, the Device Status and Schedule Status lists also provides corresponding command button mechanisms to control the output behaviors of specific devices or schedules.

On the Edit Device page, system devices *must* be configured for an output behavior of Pulse, Latch or Unlatch *and* have the Control from browser option checked to be controllable from the Device Status list on the Dashboard page. System devices configured for an output behavior of Follow are *not* controllable from the Dashboard page.

There is a Status feature on the Dashboard that allows the user to see the physical position of the door as open or closed, live video (if cameras and DVRs are configured), as well as customized, color-coded messages for programmable devices. Programmable devices are described in the section on Live Status in the chapter on *Devices*.

There is a Change Threat Level icon that enables certain Administrators to change the current threat level. For more information, see the chapter on *Threat Levels*.

Users can control which device status is displayed on the Device Status section of the Dashboard by creating Display Filters. For more information, see the section on *Using Activity Filters.*

Browsing the Dashboard

The Dashboard page provides a dynamic system activity log that automatically refreshes periodically with the most recent events (such as when a door is accessed or a device is activated), along with the corresponding time-stamp and device name. Administrators with appropriate permissions can view *all* system activity entries displayed on the Dashboard page.

To view the Dashboard page:

From any other page in the system, click the Status link from the dropdown menu and select Dashboard to access the Dashboard page.

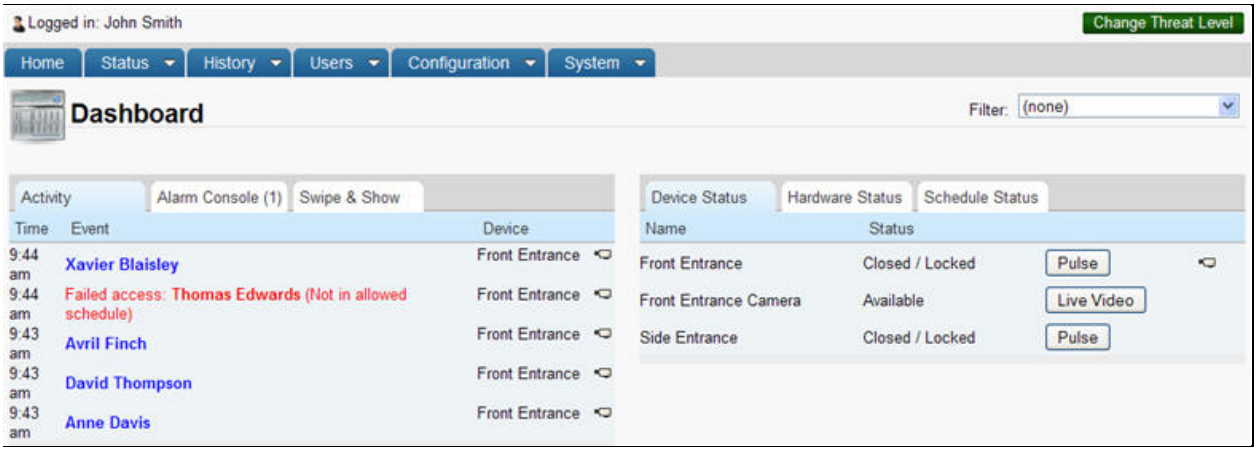


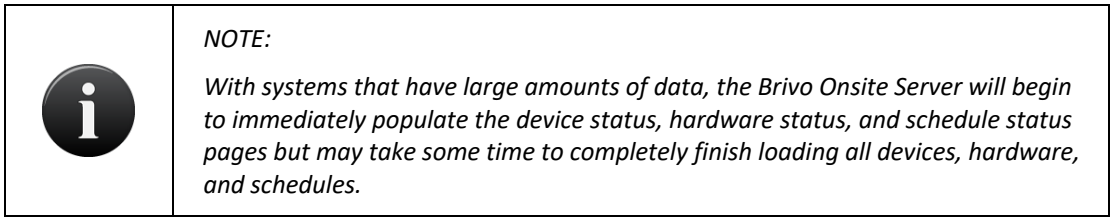
Figure 9. View Dashboard and Live Status

Details displayed include:

- Activity
  - Time. The time at which the event occurred.
  - Event. The type of system activity event. There are three types of events that may be listed.
    i. Standard device-related events are shown in black. This includes such occurrences as a door unlocking according to schedule or a timer-driven device turning itself on.
    ii. For user access events, such as an authorized user entering a valid PIN, the user's name is listed in blue. Clicking on a user name takes you to the corresponding User Detail page.
    iii. Alarms and alert events, such as Door Forced Open or Failed Access Attempt messages are displayed in red.
  - Device. The device at which the event occurred. Clicking the device name takes you to the corresponding Device Details page.
- Alarm Console
  - Bulk Alarm Acknowledge Checkbox. Located to the far left of the screen next to the Time header, this checkbox allows the administrator to select all current alarm events.
  - Alarm Acknowledge Checkbox. Located to the left of each alarm event, this checkbox allows the administrator to select an event(s).
  - Time. The time when the event occurred.

- Event. The alarm or alert system activity event, such as Door Forced Open or Failed Access Attempts.
- Details. The device where the alarm event occurred and if multiple alarms have occurred in the same location, the number of events will follow the location in parentheses.
- Acknowledge. Shows the number of selected alarm events and links to the Alarm Details popup window. At least one alarm must be selected for the Acknowledge link to work.
- Additional Information (+). This button calls up the Alarm Details popup window for a specific alarm event, discussed further in the Alarm Text section below.

- Swipe & Show
  - User. The user name as well as the date and time of the swipe event.
  - Device. A link to select which device to monitor in the upper right corner of the Swipe & Show display area.
  - Photo. A display of the photo on record pulled from the user profile. If no photo is available, the Default User Icon is presented.
  - Image Gallery. Shows the last eight valid credential reads displaying the user name, time and date stamp, and photo on record from the user profile. If no photo is available, the Default User Icon is presented.



NOTE:

With systems that have large amounts of data, the Brivo Onsite Server will begin to immediately populate the device status, hardware status, and schedule status pages but may take some time to completely finish loading all devices, hardware, and schedules.

Device Status

- Name. The name of the logical device configured for use at your installation. Clicking the device name takes you to the corresponding Device Details page. In the case of Guard Tours, clicking on the arrow icon will expand or close the details of the Guard Tour.
- Status. The current output behavior status of the logical device configured for use at your installation. (The status of devices configured for an output behavior of Follow will *not* be displayed.)
- If appropriate, buttons to control the state of the device will appear as well.
- If applicable, previously created Display Filters will be accessible via a dropdown list.

- Hardware Status
  - Name. The name of the control panel, or an indication that the panel has not been configured.
  - Panel ID. The unique identifier that separates this panel from all others in the system. Might be blank if a control panel has been configured, but has not yet been given a physical Panel ID to be associated with.
  - Status. The connection status of the panel and its IP address if connected.
  - Note: Additional information may appear in the event that a panel requires upgrade or other circumstances.

- Schedule Status

- Name. The name of the schedule. Clicking the schedule name takes you to the corresponding Schedule Details page.
- Status. The current status of the schedule, showing either not activated or activated until the date and time the schedule ends.
- Buttons to control the state of the schedule.

Administrators with appropriate permissions can:

Select a filter from the dropdown list in order to control which device status is displayed on Device Status section of the Dashboard.

View the most recent activity events in the Activity list on the Dashboard page.

Click a user name in the Activity list on the Dashboard page to access the corresponding User Details page.

Click a device name in the Device Status list on the Dashboard page to access the associated Device Details page.

View and acknowledge alarm events on the Alarm Console page of the Dashboard.

View the Swipe & Show gallery and see the last valid access event (with photo, time, and date) as well as click on a gallery photo image to call up that previous valid access event (with photo, time, and date).

Managing the Dashboard

Practically speaking, the Dashboard page is intended to give Administrators more immediate control over their installation environment. The Pulse feature provides a standard remote "buzz-through" access on doors for authorized users who may have forgotten their credential, entered a PIN incorrectly several times, or attempted entry out-of-schedule. The Latch/Unlatch toggle feature allows Administrators to intentionally latch or unlatch a programmable device that is configured for that output behavior. The Lock Early/Unlock Early/Follow Schedule feature allows Administrators to manually override a door locking schedule to allow/disallow access under certain special circumstances.

Using the Dashboard's Pulse Feature

The Dashboard's Pulse feature provides a standard remote "buzz-through" access on doors for authorized users.

1. To pulse a device, click the Pulse button associated with it on the Dashboard's Device Status list. The system displays the Device output pulsed dialog box.
2. Click OK to acknowledge the dialog. Within a few seconds, an event entry similar to the example shown below displays at the top of the Dashboard's Activity list.

Time	Event	Device
10:48 am	Device activated by admin: **Janet Viera**	front door

Figure 10. Dashboard Activity List – Pulse Event Entry

Using the Dashboard's Latch/Unlatch Feature

The Dashboard's Latch/Unlatch toggle feature allows Administrators to intentionally latch or unlatch a programmable device that is configured for that output behavior.

1. To latch a device, click the Latch button associated with it on the Dashboard's Device Status list. The system displays the Device output latched dialog box.
2. Click OK to acknowledge the dialog. Within a few seconds, an event entry similar to the example shown below is displayed at the top of the Dashboard's Activity list.

Time	Event	Device
10:35 am	Output latched by admin: **Lisa Dominci**	Server Room Temp Sensor

Figure 11. Dashboard Activity List – Latch Event Entry

3. To unlatch the device, click the Unlatch button associated with it on the Dashboard's Device Status list. The system displays the Device output unlatched dialog box.
4. Click OK to acknowledge the dialog. Within a few seconds an event entry similar to the example shown below display at the top of the Dashboard's Activity list.

Time	Event	Device
10:36 am	Output unlatched by admin: **Lisa Dominci**	Server Room Temp Sensor

Figure 12. Dashboard Activity List – Unlatch Event Entry

Using the Dashboard's Lock Early/Unlock Early/Follow Schedule Feature

The Dashboard's Lock Early/Unlock Early/Follow Schedule feature allows administrators to manually override a door timer schedule to allow/disallow access under certain special circumstances. When desired, the Administrator can then return the door device to its normal lock/unlock schedule.

NOTE:

Doors or devices that are overridden will only remain overridden until the next scheduled event in the schedule, either to engage (lock) or to disengage (unlock). The device or door still follows its schedule on the next appropriate schedule block.

1. To lock a door *before* its normal scheduled time, click the Lock Early button associated with it on the Dashboard's Device Status list. The system displays the Door locked ahead of schedule dialog box.
2. Click OK to acknowledge the dialog. Within a few seconds an event entry similar to the example shown below display at the top of the Dashboard's Activity list.

Time	Event	Device
10:36 am	Door locked ahead of schedule: **Lisa Dominci**	Front Door

Figure 13. Dashboard Activity List – Door Locked Event Entry

3. To unlock a door *before* its normal scheduled time, click the Unlock Early button associated with it on the Dashboard's Device Status list. The system displays the Door unlocked ahead of schedule dialog box.
4. Click OK to acknowledge the dialog. Within a few seconds an event entry similar to the example shown below display at the top of the Dashboard's Activity list.
5. The "Activate Devices" field does not default to appear checked. You must check this box to allow this Administrator to activate devices from the Dashboard.

Time	Event	Device
10:37 am	Door unlocked ahead of schedule: **Lisa Dominci**	Lobby Door

Figure 14. Dashboard Activity List – Door Unlocked Event Entry

6. To return a door to its normal lock/unlock schedule, click the Follow Schedule button associated with it on the Dashboard's Device Status list. The system displays the Door returned to following configured unlock schedule dialog box.
7. Click OK to acknowledge the dialog. Within a few seconds, an event entry similar to the example shown below display at the top of the Dashboard's Activity list.

Time	Event	Device
10:38 am	Door returned to following configured unlock schedule: **Lisa Dominci**	Front Door

Figure 15. Dashboard Activity List: Door Returned to Unlock Schedule

To select a filter for devices displayed on the Dashboard

1. From the Status link at the top of any page, click on the Dashboard link.
2. Select a filter from the dropdown list next to Filter.

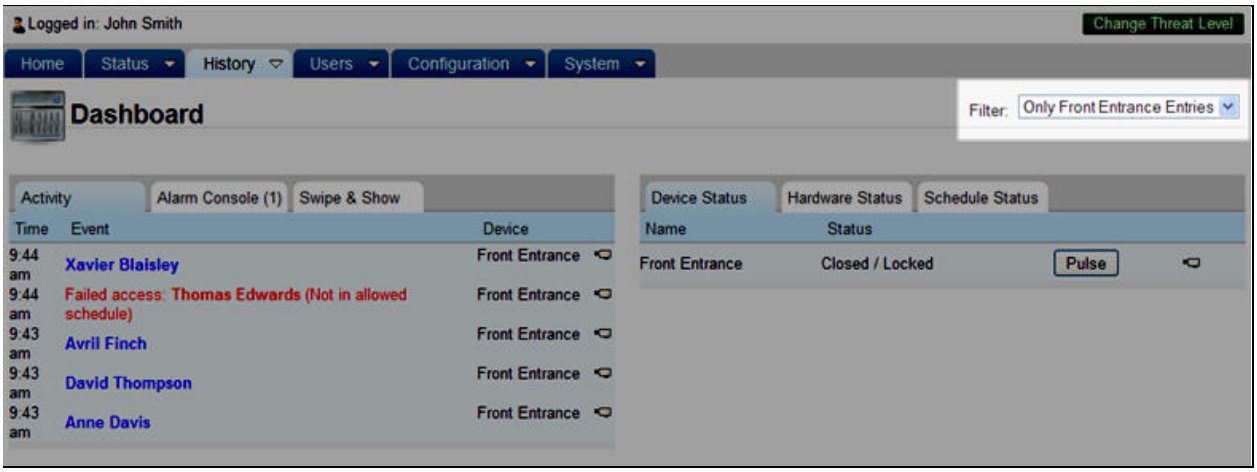


Figure 16. Dashboard Display Filter

3. The corresponding device status for the selected filter will display. For more information on how to create a filter, refer to the section on *Using Display Filters*.

Using the Dashboard's Alarm Console Feature

The Dashboard's Alarm Console feature allows administrators to view and acknowledge alarm events either individually or in bulk. When desired, the administrator can enter messages about alarm events on the alarm details page, acknowledging the alarm, updating it for future review, or clearing them from the alarm console depending upon the type of alarm event.

To enable the Alarm Console

1. From the Configuration dropdown menu, choose the Accounts tab and click on the Accounts link. The list of Accounts will appear.
2. Select the account where you want to activate Alarm Console. The Edit Account Details page appears.
3. Click Edit at the bottom of the Account Details page.
4. Check the Enable checkbox under Alarm Console Settings.
5. If you only want alarms generated during a specific schedule to appear on the alarm console and require acknowledgement, you may select a schedule from the dropdown menu next to Alarm Active Schedule.
6. If you wish to assign a priority system to alarm events, you may input an Alarm Priority Minimum and Alarm Priority Maximum as a numeric range.

7. You may ignore Threat Levels or select under what Threat level conditions the device will report alarm events.
8. Click Save.

To enable Alarm for Control Panels

1. From the Configuration dropdown menu, choose the Accounts tab and click on the Accounts link. The list of Accounts will appear.
2. Select the account where you want to activate Alarm Console. The Edit Account Details page appears.
3. Click Edit at the bottom of the Account Details page.
4. If you want specific instruction text to appear when an alarm event for a control panel occurs, select from the Instruction Text dropdown menu. See the Alarm Text section of the manual on how to create instruction text.
5. You may assign an Alarm Priority to alarm events for control panels.
6. Click Save.

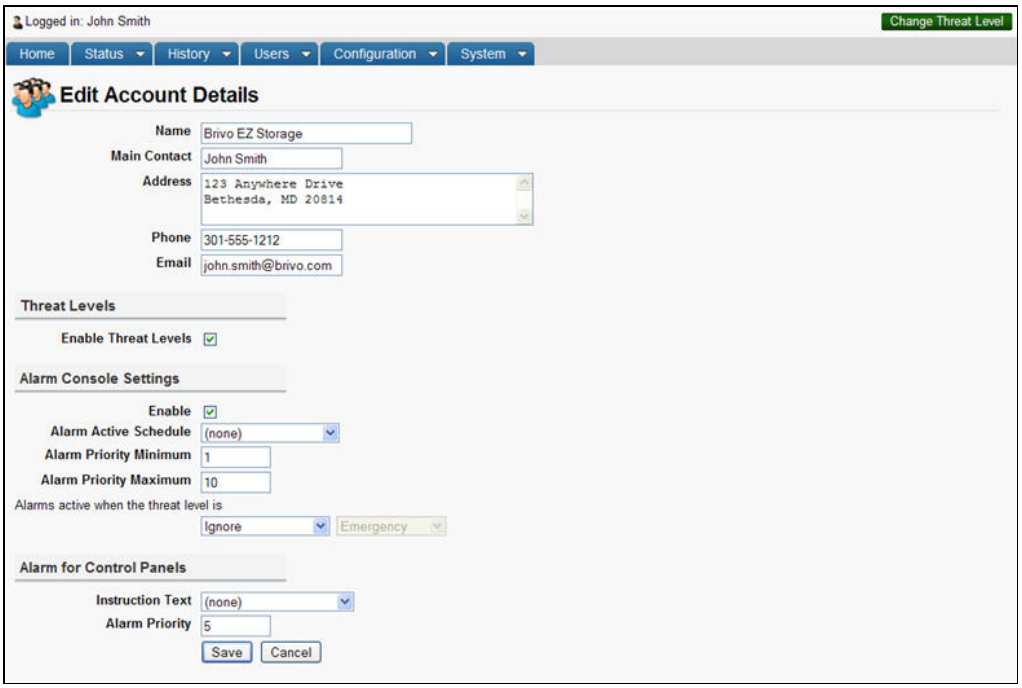


Figure 17. Alarm Console Settings

What is Alarm Text?

Alarm Text allows administrators with appropriate permissions to create instructions for alarm events and precanned acknowledgements for use when reviewing and acknowledging alarm events.

To create new Alarm Text

1. From the Configuration dropdown menu, choose the Accounts tab and click on the Alarm Text link. The Alarm Text list will appear.
2. Click on the Create New Alarm Text button.
3. Select the Type of alarm text you would like to generate from the dropdown menu.
4. Type in a Summary to describe the alarm text.
5. Enter the Text of the alarm text into the provided field.
6. Click Save.

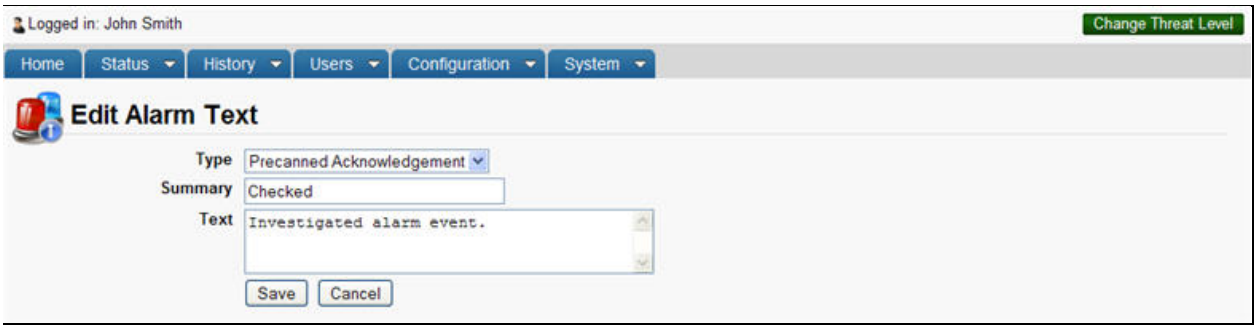


Figure 18. Creating an Alarm Text Message

To acknowledge, update, or clear an Alarm Event(s)

1. From the Dashboard, click on the Alarm Console tab. The Alarm Console section of the Dashboard displays all the listed alarm events.
2. Select a single alarm event by checking the checkbox on the left next to the single alarm event, or you may select all events by checking the checkbox next to Time at the top of the Alarm Console tab.
3. Click the + button or the Bulk link above it to take you to the Alarm Details popup window.
4. If desired, select a precanned acknowledgement from the Canned Message dropdown menu or simply enter information into the Message text field below.
5. To update an alarm event, click the Update Alarm button. This returns you to the Alarm Console dashboard, and an Alarm Updated message appears in the activity log along with any message entered into the Message text field.
6. To acknowledge an alarm event, click the Acknowledge Alarm button. You are returned to the Alarm Console dashboard, and an Alarm Acknowledged message appears in the activity log along with any message entered into the Message text field.
7. To clear an alarm event, click the Clear Alarm button. You are returned to the Alarm Console dashboard, and an Alarm Cleared message appears in red in the activity log, along with any message entered into the Message field.

	NOTE: Clearing Alarms *Clearing an alarm removes an alarm event that is still not in its normal state off the alarm console. For example, normally a door ajar alarm stays on the console until it is both acknowledged and the door is closed again. If you want to remove the alarm event before actually closing the door, you can acknowledge the alarm event, then bring up the Alarm Details popup window again and press the Clear Alarm button, which will forcibly remove the alarm event from the alarm console.*

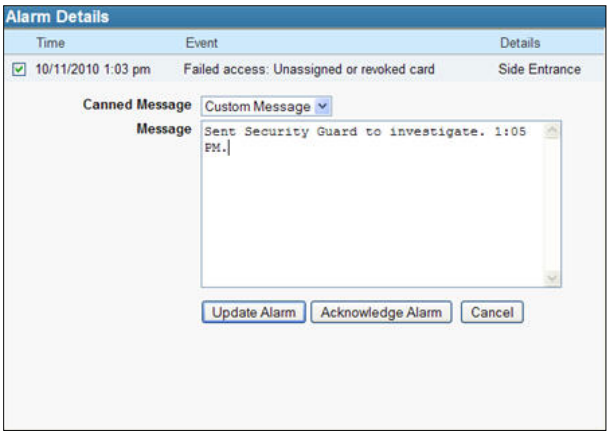


Figure 19. Alarm Update/Acknowledgement

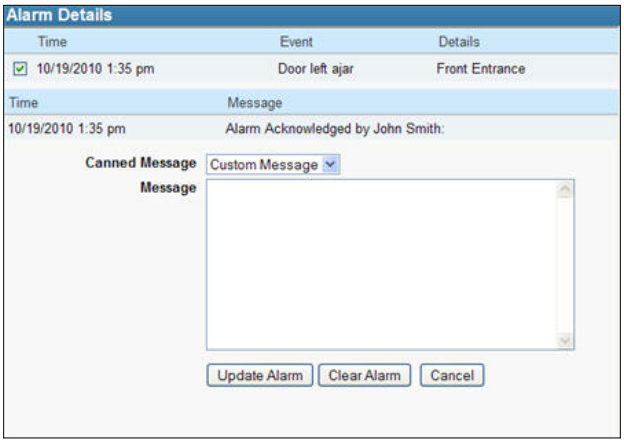


Figure 20. Alarm Clear

Enabling Alarm Events for Doors, Valid Credential Devices, and Elevators

An administrator with appropriate permissions can enable alarm events for doors, valid credential devices, and elevators by defining the privileges on the Edit Device page. This allows failed access events to appear as alarms, as well as allowing the combination of multiple alarm events of the same type into a single reported alarm event.

To enable alarm events for doors, valid credential devices, and elevators

1. From the Configuration dropdown menu, choose the Devices tab and then click on Devices. If you are enabling an existing device to use Alarm Console, simply click on the device you wish to enable and click Edit at the bottom of the Device Details page, then skip to step 5.
2. Click on the Create New Device button.
3. Select the Type of device from the dropdown menu, choosing Door, Valid Credential Device, or Elevator.
4. Select a Subtype if you wish to make this a device profile.
5. In the Alarm Console Settings section of the page, check the Include failed access as alarm checkbox if you wish to include failed access events as alarm events.
6. Check the Combine Alarms checkbox if you wish to combine multiple alarm events of the same type into a single reported alarm event.
7. Enter Instruction text if desired.
8. Enter an Alarm Priority if desired.
9. Select an Alarm Active Schedule from the dropdown menu if desired. If a schedule is selected here, the alarm events will appear during the selected schedule as well as during any selected schedule under the Alarm Console Settings for the entire account.
10. You may ignore Threat Levels or select under what Threat level conditions the device will report alarm events.
11. Click Save.

Figure 21. Alarm Console Settings for Doors, Valid Credential Devices, and Elevators

Enabling Alarm Events for Event Triggers, Input Switches, and Schedule Controlled Devices

An administrator with appropriate permissions can enable alarm events for event triggers, input switches, schedule controlled devices, and muster points by defining the privileges on the Edit Device page. This allows standard events to appear as alarms, as well as allowing the combination of multiple alarm events of the same type into a single reported alarm event.

To enable alarm events for event triggers, input switches, and schedule controlled devices

1. From the Configuration dropdown menu, choose the Devices tab then click on the Devices link. If you are enabling an existing device to use Alarm Console, simply click on the device you wish to enable and click Edit at the bottom of the Device Details page, then skip to step 5.
2. Click on the Create New Device button.
3. Select the Type of device from the dropdown menu, choosing event trigger, input switch, schedule controlled device, or muster point.
4. Select a Subtype if you want to make this a device profile.
5. In the Alarm Console Settings section of the page, check the Standard events as alarm checkbox if you wish to include standard events as alarm events.
6. Check the Combine Alarms checkbox if you wish to combine multiple alarm events of the same type into a single reported alarm event.
7. Enter Instruction text if desired.
8. Enter an Alarm Priority if desired.
9. Select an Alarm Active Schedule from the dropdown menu if desired. If a schedule is selected here, the alarm events will appear during the selected schedule as well as during any selected schedule under the Alarm Console Settings for the entire account.
10. You may ignore Threat Levels or select under what Threat level conditions the device will report alarm events.
11. Click Save.

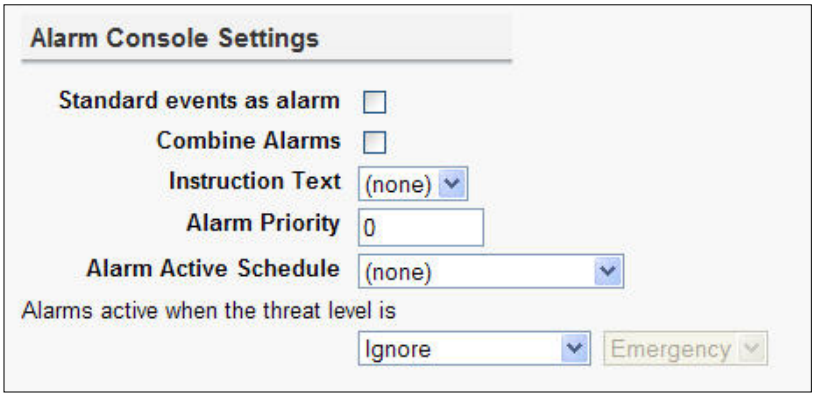


Figure 22. Settings for Event Triggers, Input Switches, Etc.

Using the Dashboard's Swipe & Show feature

The Dashboard's Swipe & Show feature allows administrators to view valid credential events at a selected device, seeing the current and the seven previous events. When desired, the administrator can select any of the photos in the gallery and call up the photo, time, and date of that particular valid credential event.

To use Swipe & Show

1. From the Status dropdown menu, select Dashboard.
2. Click on the Swipe & Show tab of the Dashboard.
3. Click on the Select Device link in the upper right hand corner of the Swipe & Show section. The Select Device popup window appears.
4. Choose a device from the available list by clicking on it. You are returned to the Swipe & Show page.
5. The last valid credential device read displays the user name, as well as the time and date stamp of the read, along with the photo image attached to the user profile.
6. The last eight valid credential device reads along with their respective photo images display along the bottom of the page. Selecting any of the images from the gallery at the bottom recalls the user photo and the time and date of last access.
7. As new valid credential reads occur, the oldest image is removed and the newest image is placed at the beginning of the line.

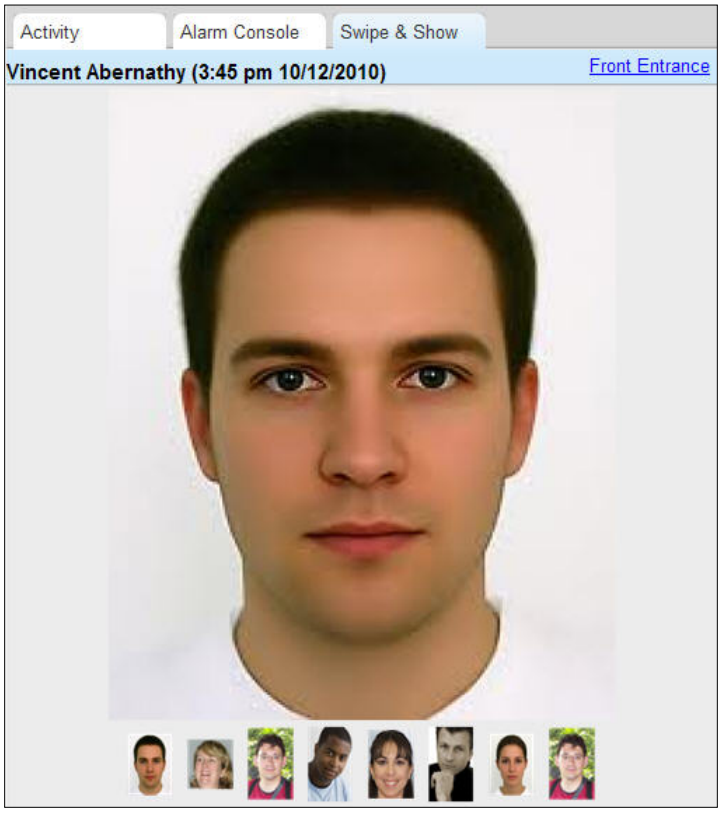


Figure 23. Swipe & Show display

Using Display Filters

Brivo Onsite Server allows users to control the devices for which status displayed on the Device Status section of Dashboard by creating Display Filters.

To view filters

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Dashboard link, click Display Filters. The Display Filters page displays.

Figure 24. Filters

3. To view the details for a particular filter, click on the filter's name. The Filter Details page displays.

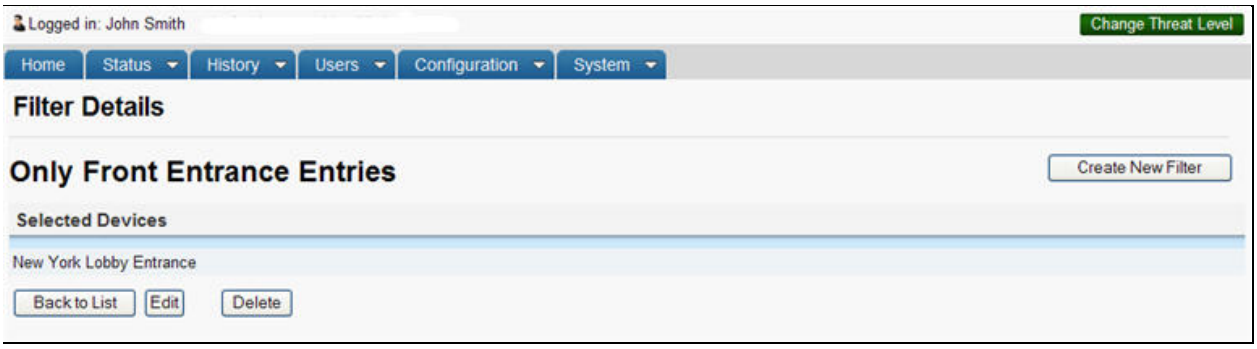


Figure 25. Filter Details

To create a filter

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Dashboard link, click Display Filters. The Display Filters page displays.
3. Click "Create New Filter" at the top of the page. The "Edit Filter" page will display.

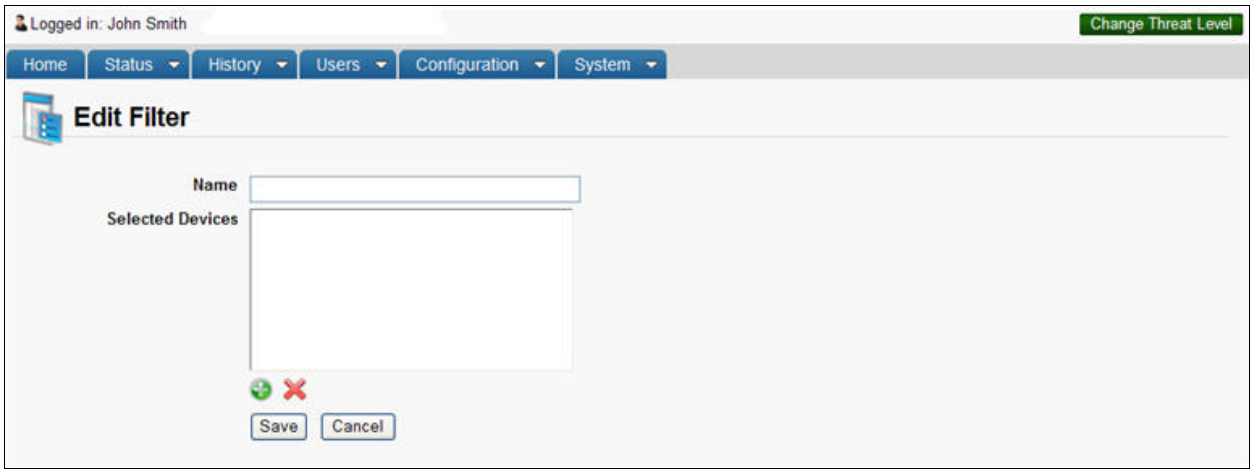


Figure 26. Create New Filter

4. In the field next to "Name," enter a name for the filter.
5. Click  to select which device(s) will appear in the filter. A popup list will appear. Select each new device to add to the filter which will then appear in the Selected Devices box.
6. Click Save. You are returned to the Filter Details page.

To edit a filter

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Dashboard link, click Display Filters. The Display Filters page displays.
3. Click the filter you wish to edit. The Filter Details page displays.
4. Click "Edit Filter" at the bottom of the page. The "Edit Filter" page will display.
5. When you have finished making changes to the filter, click Save. You are returned to the Filter Details page.

To delete a filter

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Dashboard link, click Display Filters. The Display Filters page displays.
3. Click the filter you wish to delete. The Filter Details page displays.
4. Click "Delete" at the bottom of the page. Click OK in the confirmation prompt. You are returned to the Filters page.

Live Map/Floorplan

Once a map/floorplan has been created, icons added, and regions established, then an administrator with appropriate permissions can utilize the Live Map feature under the Dashboard link.

To use the Live Map feature:

1. Scroll over the Status link. The sub-navigation menu displays.
2. From the sub-navigation menu, click the Maps/Floorplans link. A popup window with a list of map names appears. Select the map you wish to use.
3. The Live Map page will appear with the icons and regions in their current states (either normal or alarm).

	NOTE: *An icon representing a programmable device or door will appear as its normal color (default is green) if in a normal state (such as unlocked or locked). The icon will switch to its alarm color (default red) if in an alarm state such as door ajar or wire cut.*

4. To interact with a device, scroll over the icon representing that device. The name and current status of the device will appear in a popup window.
5. If the device can be controlled via the browser, if you click on the icon, a button will appear (for example, Pulse for a door).
6. Zoom – to zoom in, out, or reset the default size of the live map, there are three buttons in the upper right hand corner of the screen (+), (-), and (fit).
7. Choose Map – to choose a new map for live view, click on the Choose Map button and a popup window with available maps will appear. Select the map you wish to view live and you are returned to the Live Map page.

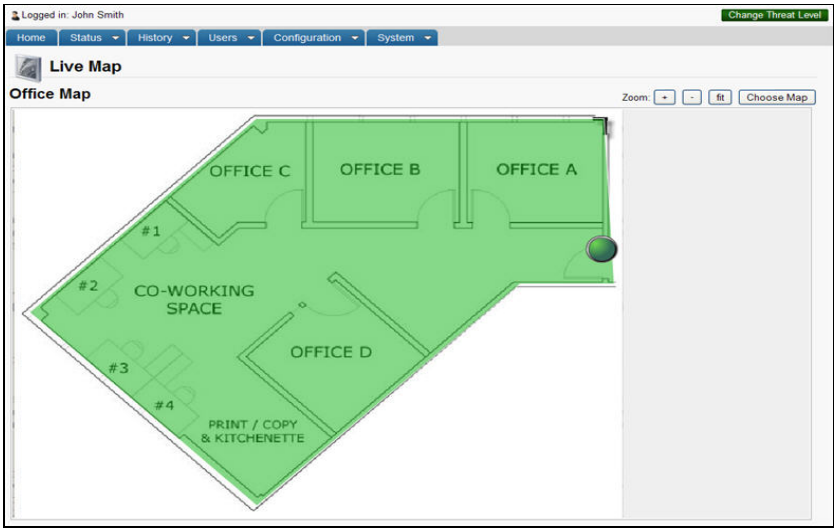


Figure 27. View Live Map

5. History

What is Activity?

Brivo Onsite Server tracks the operation of all system devices, such as when a door is unlocked or when a relay is engaged. It is also tracks the actions of all Administrators. For example, whenever a new account is created, or an Administrator is assigned to an account, these actions are recorded in the Administrative Journal. Likewise, whenever a new user, device or schedule is created, edited, or deleted in the system, those changes are recorded. In this way, Brivo Onsite Server lets you track what actions were performed by whom and when.

Browsing the System Activity Log

The System Activity provides a complete list of events for a given day, such as when a door is accessed or a device is activated. Administrators with appropriate permissions can view all activity entries.

To view the System Activity page:

From any other page in the system, scroll over the History link, and then the Activity link. Select System Activity from the sub-navigation menu to access the System Activity page.

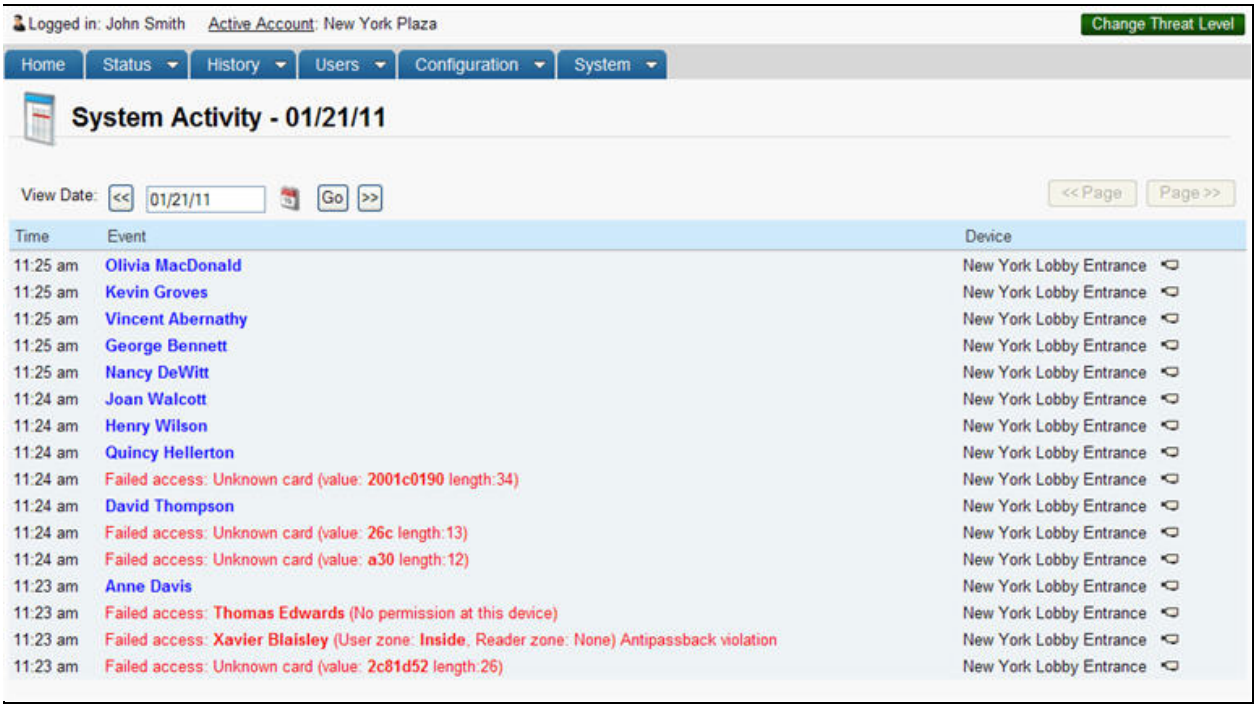


Figure 28. View System Activity Log

Details displayed include:

- Time. The time at which the event occurred.
- Event. The type of access events. There are three types of events that may be listed.
  - Standard device-related events are shown in black. This includes such occurrences as a door unlocking according to schedule or a timer-driven device turning itself on.
  - For user access events, such as an authorized user entering a valid PIN, the user's name is listed in blue. Clicking on a user name takes you to the corresponding User Detail page.
  - Alarms and alert events, such as Door Forced Open or Failed Access Attempt messages are displayed in red.
- Device. The device at which the event occurred. Clicking the device name takes you to the corresponding Details page.

Administrators with appropriate permissions can:

View events that occurred on a specific date

- Click << in the View Date section to scroll backwards day-by-day, to view past activity logs.
- Click the date field to select a specific date from a popup calendar, then click Go to view the activity log for that date.
- Click >> to scroll forward day-by-day.

Click <<Page or Page>> to scroll backward and forward through the complete list of events for the current day.

Click a user name to access the corresponding User Details page.

Click a device name to access either the Board Details page or the Device Details page.

Click Display Filters to access the filters for activity on that account.

Index of Events

The following events appear in the System Activity log.

Access Events

Access by User

Exception Events

Communication with Node Lost

Communication with Node Restored

Critical Battery

Door Ajar

Door Ajar Cleared

Too Many Invalid PINs

Door Forced Open

Door Locked by Timer

Door Unlocked by Timer

Door Lock Intrusion Alarm

Door Lock Intrusion Alarm Cleared

Invalid Second Factor (by Known User): Invalid [Card/PIN value]

Invalid Second Factor (by Known User): Same PIN/Card Credential Presented Twice

Invalid Second Factor (by Known User): Second Credential Not Presented

Failed Access (by Unknown Person): Unknown card/PIN

Failed Access (by Unknown Person): Unassigned or revoked card

Failed Access (by Known User): Low Battery

Failed Access (by Known User): Card Rejected Offline

Failed Access (by Known User): User is out of effective date range

Failed Access (by Known User): User is at unauthorized door

Failed Access (by Known User): User is out of schedule

Failed Access (by Known User): Antipassback violation

Failed Access (by Known User): Access permission threat level violation

Failed Access (by Known User): No permission at this device

Failed Access (by Known User): Suspended User

Failed Access (by Known User): Invalid Credential Type

Failed Access: Invalid credential type

Low Battery

Open with Metallic Key (Forced Open)

Open with PPD (Forced Open)

Open with Memorized Code (Forced Open)

Salto Router Connection Dropped

Device Events

Device Engaged

Device Disengaged

Guard tour stop visited

Guard tour stop missed

Guard tour completed

Guard tour incomplete

Wire cut set

Wire cut cleared

Wire short set

Wire short cleared

Control Panel Events

AC Power Loss (Switch to Battery)

AC Power Restored

Panel Enclosure Opened

Panel Enclosure Closed

Expansion Board Chip Reset

Board Communication Failure Set

Board Communication Failure Cleared

Unauthorized IP Access

Failed Access Events

A *Failed Access Event* is an incident of an invalid credential being presented. The system logs Failed Access Events according to the following rules of precedence:

Failed Access by Unknown Persons:

- If the credential is unknown to the system: Failed Access: Unknown Credential [Card/PIN value]
- If the credential is known to the system but has never been issued to a user: Failed Access: Unassigned or revoked card: [Card value]
- If the credential is not the proper type of credential: Failed Access: Invalid credential type (Card required)

Failed Access by Known Users:

- If the credential belongs to a user who attempts access outside of his or her effective date range: Failed Access by [User Name]: Out of effective date range
- If the credential belongs to a user who attempts access at an unauthorized door: Failed Access by [User Name]: Unauthorized Door
- If the credential belongs to a user who attempts access at an authorized door, but at an unauthorized time: Failed Access by [User Name]: Out of Schedule
- If the credential belongs to a user who attempts to enter an antipassback zone they have already entered without exiting: Failed Access by [User Name] (User Zone: [Zone], Reader Zone [Zone]) Antipassback violation
- If the credential belongs to a user who attempts unauthorized access when a Threat Level has changed: Failed Access by [User Name]: Access permission threat level violation
- If the credential belongs to a user who does not have permission at a particular door: Failed Access by [User Name] (No permission at this device)
- If the credential belongs to a user who attempts unauthorized access when they are suspended: Failed Access: Suspended User [User Name]
- If the credential is valid but the wireless lock has a low battery: Failed Access by [User Name]: Low Battery
- If the credential is valid but the wireless lock router is offline: Failed Access by [User Name]: Card Rejected Offline
- If the credential belongs to a user who attempts to gain entry using an incorrect credential type: Failed Access by [User Name]: Invalid Credential Type

Unauthorized IP Access Events

An *Unauthorized IP Access* event is an incident where a control panel attempts to contact an IP address other than the approved Brivo Host Addresses. The system logs Unauthorized IP Access events as follows:

- Unauthorized IP Address: [IP Address] from [Control Panel Number]

Generating an Activity Report

A report is a printable query of the Activity Log, such as:

All Exception Events on the Main Control Board in the last month

All Access Events at Front Door by John Doe between 9:00 AM and 5:00 PM on February 1

All Device Events at Front Door by members of the Group "Staff" in the last three days

Administrators with appropriate permissions can generate an Activity Report.

To generate an activity report:

1. Scroll over the History link. The sub-navigation menu displays.
2. From the Activity link, click System Activity. The System Activity page displays.
3. Click Activity Reporting on the sidebar menu. The Activity Report page displays.

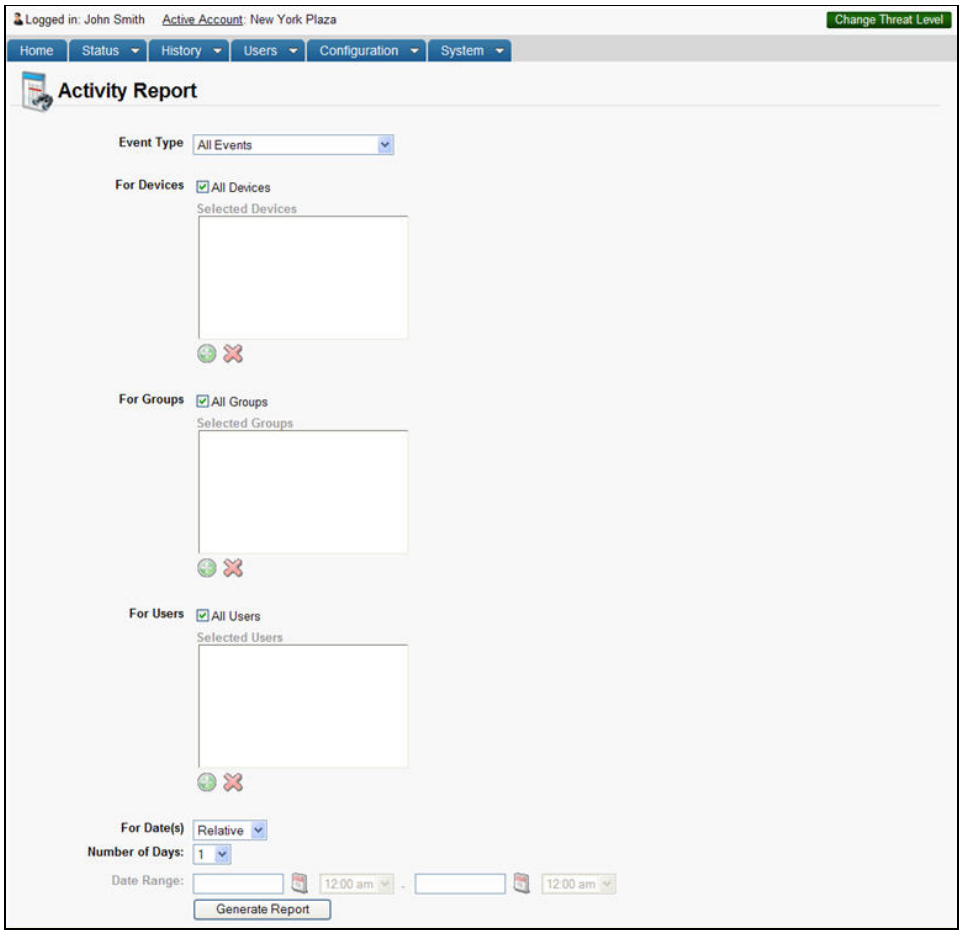


Figure 29. Generate Activity Report

4. From the Event Type drop-down list click the type of event(s) you want to include in the report.
5. Click the checkbox for All Devices to include activity related to all the currently defined doors and devices in your report, or select individual devices:
    - Click the button which will display a popup list of Available Devices on the left to highlight it.

- Click on the device you want to place in the Selected Devices field.
- To remove a device from the report, click to highlight it in the Selected Devices list, and then click Removed Selected button to remove it from the list.

6. Click the checkbox for All Groups to include activity related to all the currently defined groups in your report, or select individual groups using the procedure described above for devices.
7. Click the checkbox for All Users to include activity related to all the currently defined users in your report, or select individual users using the procedure described above for devices.
8. On the For Date(s) drop-down list choose Relative to specify the number of days to be included in the report, or Absolute to enter a specific date range.
    - If you select Relative, click the Number of Days on the drop-down list. For example, if you click 2, the Activity Report will include all the desired events for the previous two days.
    - If you select Absolute, you must specify a Date Range. Click in the first field of this section to choose a start date from the pop-up calendar, then select a start time on the associated drop-down list. Next, click on the second blank field to choose an end date from the pop-up calendar, then select an end time from the second drop-down list.
9. Click Generate Report. A copy of the report displays in a pop-up window.

Time	Event	Device
2007-04-10 15:22	Door returned to following configured unlock schedule: **Lisa Dominci**	Front Door
2007-04-10 15:22	Door unlocked on schedule	Front Door
2007-04-10 15:22	**Jane Brown**	Back Door
2007-04-10 15:22	Door unlocked ahead of schedule: **Lisa Dominci**	Front Door
2007-04-10 15:22	Door locked on schedule	Front Door
2007-04-10 15:21	**Jane Brown**	Back Door
2007-04-10 15:04	Door unlocked on schedule	Front Door
2007-04-10 15:04	Schedule Activated: **Mon - Fri 10AM-4PM** User: **Jane Brown**	Front Door
2007-04-10 15:04	**Jane Brown**	Front Door
2007-04-10 15:01	Door left ajar	Front Door
2007-04-10 14:59	Door returned to following configured unlock schedule: **Lisa Dominci**	Front Door
2007-04-10 14:59	Door locked on schedule	Front Door

Figure 30. View Activity Report

10. Use your browser's Print function to print a copy of the report.

Exporting the Activity Log

The Activity Log can be exported to a tab-separated file for use by other programs.

Administrators with appropriate permissions can export the Activity Log.

To export the Activity Log:

1. Scroll over the History link. The sub-navigation menu displays.
2. From the Activity link, click Activity Export. The Activity Export page displays.

Figure 31. Export Activity Log

3. Click anywhere in the Start Date field or click to specify the first date to be included in the log file.
4. Click anywhere in the End Date field or click to specify the last date to be included in the log file.
5. Click Export Activity File. Follow your browser's prompts for saving the file.

What is Reporting?

Brivo Onsite Server provides reporting capabilities on a variety of levels.

Activity Reporting is a customized query of the Activity Log, such as "All Access Events by John Doe at Front Door on February 1" or "All Exception Events at Server Room in the last month." This report is discussed in greater detail in Chapter 14: Activity.

Under the History tab, the Reporting tab also provides several reporting options:

Reports is a query tool for predefined commonly run reports, allowing these reports to be generated immediately depending upon administrator permissions. Reports also allows for the creation and generation of new reports.

Predefined reports have established data so they do not require user input. They can be edited, but it is recommended that the predefined reports be maintained as a baseline and copied into a new report if changes are desired.

These reports allow an administrator with appropriate permissions to run these reports for immediate consumption without requiring any additional set up.

Scheduled Reports allows either predefined or new reports to be run on a defined schedule. Administrators with appropriate permissions can create schedules for reports.

Finally, Muster Report allows administrators with appropriate permissions to use the normal antipassback functionality to track the presence of users in a facility.

Reporting uses two features that are defined below:

Relations – Relations are the data that you want to report on, and related data. For example, users have groups, which have permissions and thus are tied to devices. When building a report listing all users and the groups those users are in, you can start with the Users relation then select Groups. This makes various properties of Users as well as Groups available for both report criteria and outputs.

Criteria - Criteria are ways to specify what data appears in a report. Criteria are built by selecting a property of a relation, an operation and a value. For example, to constrain a report on users to only those that will be expiring in the next two weeks, add a criteria for 'User Expiration Date', an operation of 'within the next' and specify a value '14 days.' Note that all rows in the report will match all given criteria. Criteria properties are defined below.

- Equal – exactly matches the data selected/input into the field.
- Not Equal – does not match the data selected/input into the field.
- Is Empty – contains no data.
- Is Not Empty – contains any data.
- Is In – is within the criteria selected/input into the field (for example, is in Managers).
- Is Not In – is not within the criteria selected/input into the field. (for example, is not in Morning Shift).
- Begins With – starts with the data selected/input into the field.
- Contains – contains the data at any point selected/input into the field.
- Ends With – ends with the data selected/input into the field.
- Within The Last – prompts for a number and a unit (minutes, hours, days, weeks).
- Within the Next – prompts for a number and a unit (minutes, hours, days, weeks)

Browsing the Reports List

The Reports list displays a list of predefined reports for your account. The list displays reports listed alphabetically.

Administrators with appropriate permissions can view the Reports associated with their own accounts.

To view the list of reports for your account:

1. Scroll over the History link. The sub-navigation menu displays.
2. From the Reporting link, click Reports from the dropdown list. The Reports list displays.

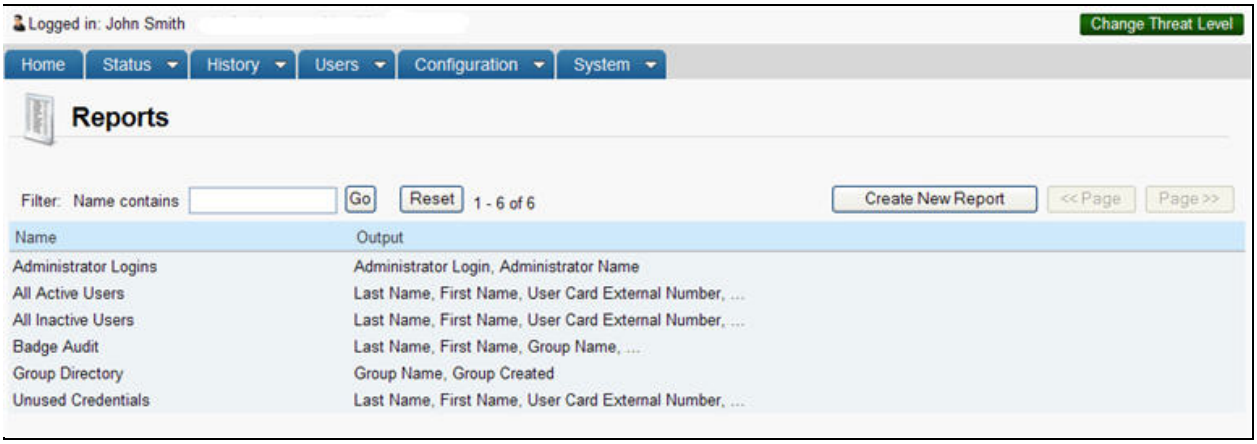


Figure 32. View Reports List

Details displayed include:

- Name. The name of the report, such as "Badge Audit" or "Unused Credentials."
- Output. The fields that appear in the report.

Administrators with appropriate permissions can:

Click the name of any report to access the corresponding Report Details page.

Click Create New Report to access the Edit Report page to create a new report for this account.

Creating a New Report

Administrators with appropriate permissions can create new reports.

To create a new report

1. Scroll over the History tab, the sub-navigation menu displays.
2. From the Reporting link, click Reports from the dropdown list. The Reports List displays.
3. Click on the Create New Report button. The Edit Report page displays.

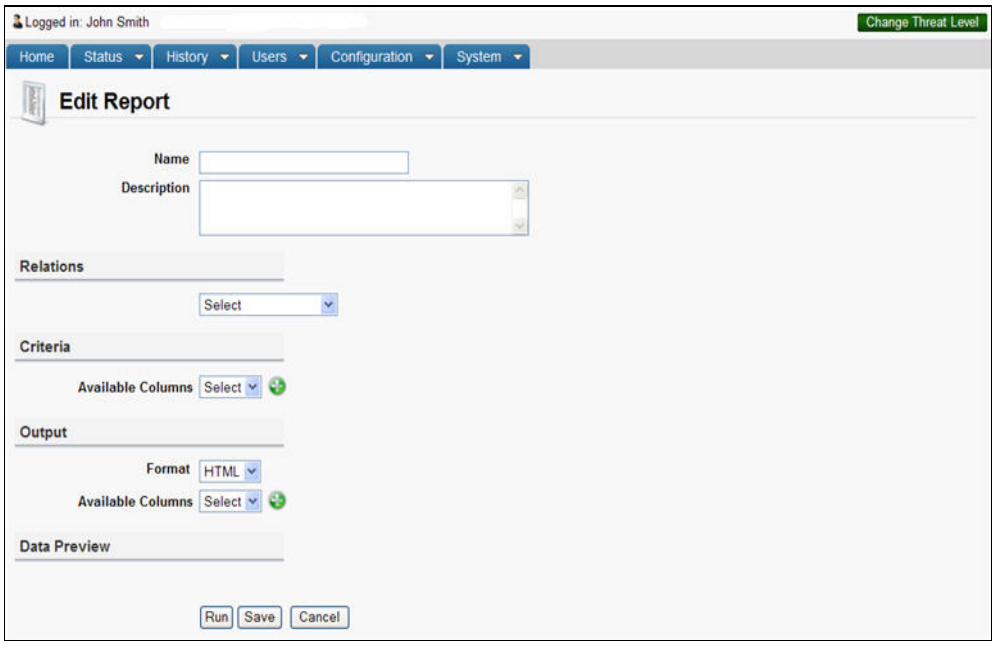


Figure 33. Create New Report

4. Enter a Name for the report.
5. Enter a Description of the report.
6. Select Relations from the dropdown list. When selecting a Relation, note that it loads other relations that are naturally associated with the already selected values. For example, Users belong in Groups, which have Permissions, and those Permissions are to Devices, which operate on Schedules.
7. Select any Criteria you want from the dropdown list. Use to add additional criteria.
8. Select the Format from the dropdown list.
9. Select the columns to appear in the report by selecting the Available Columns from the dropdown list. Use to add additional columns as needed. You may edit the name of the columns by simply replacing the information in the field.
10. As the report is created, the columns selected above under Available Columns will start to appear in the Data Preview section. Use to sort in ascending order, use to not sort, or use to sort in descending order, or click on to remove an output column. Also, columns in the Data Preview can be moved left or right to reorder where they appear when the report is generated. Simply click on the column and move it to the desired location.
11. To run the report immediately without saving, click Run. If you wish to save the report to run it again, click Save. You are returned to the Report Details page.

Managing Reports

Once a report is created, its details can be edited at any time. Reports can also be deleted.

Administrators with appropriate permissions can manage reports.

To view a report:

1. Scroll over the History link. The sub-navigation menu displays.
2. From the Reporting link, click Reports from the dropdown list. The Reports list displays.
3. Click the report you wish to view. The corresponding Report Details page displays.
4. To have the report appear on the Home Page under Reports as a hotlink, check the Show Link On Home Page checkbox.

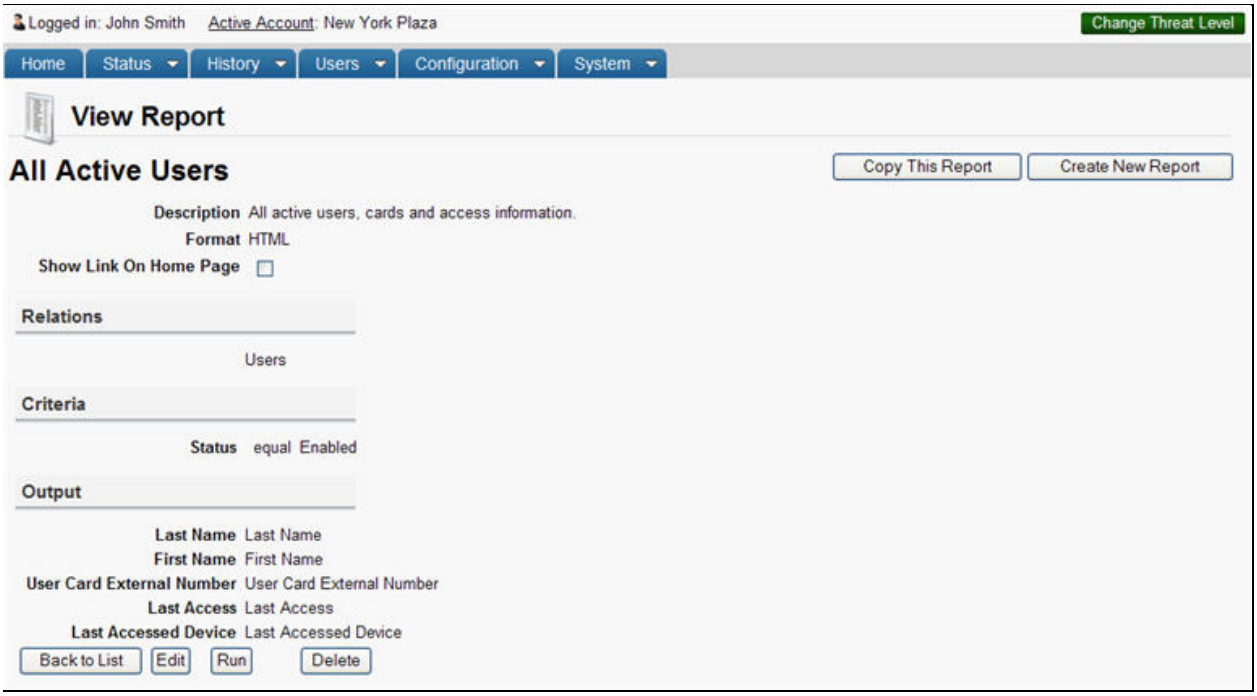


Figure 34. View a Report

To edit a report:

1. Scroll over the History link. The sub-navigation menu displays.
1. From the Reporting link, click Reports from the dropdown list. The Reports list displays.
2. Click the report you wish to edit. The corresponding Report Details page displays.
3. Click Edit. The Edit Report page displays.

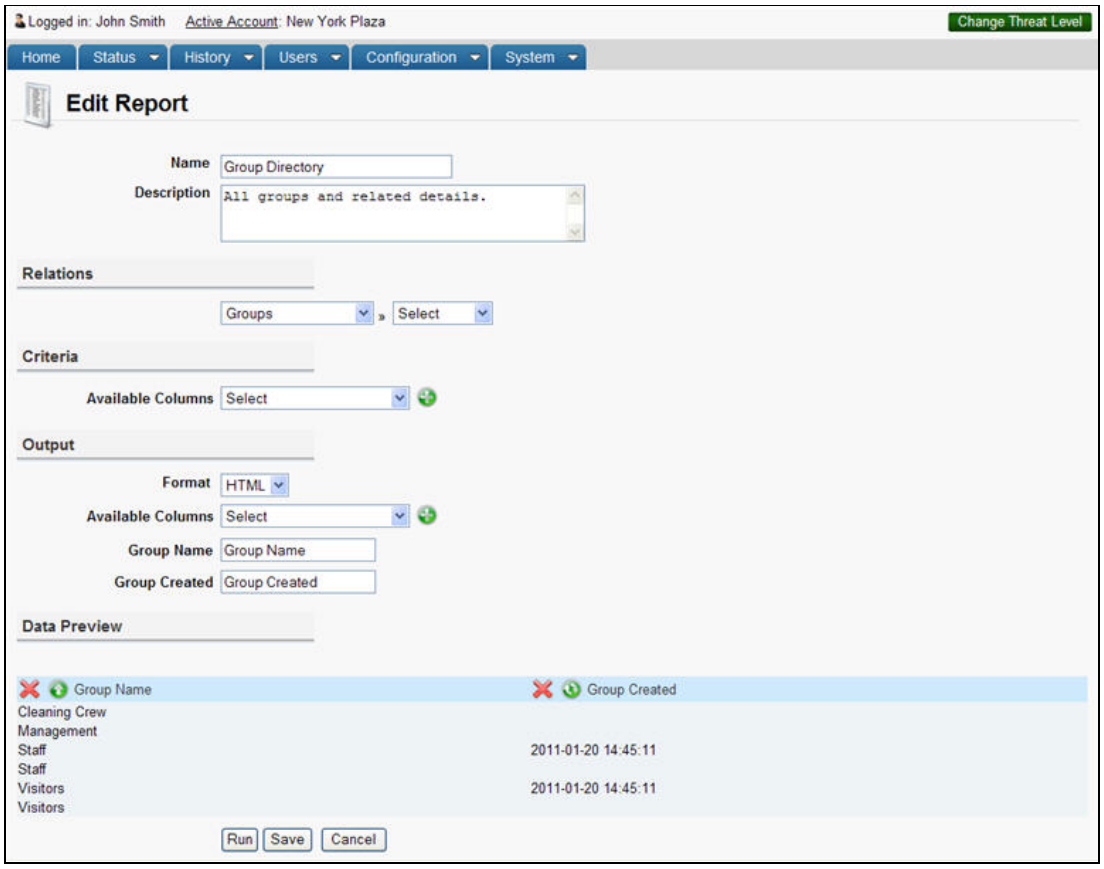


Figure 35. Edit a Report

4. To rename the report, enter a new value in the Name field.
5. To edit the description, enter a new value in the Description field.
6. To change the relations of the report, edit the Relations dropdown list as desired.
7. To edit the criteria of the report, edit the Available Columns from the dropdown menu. Use if more criteria are required.
8. To change the output format, select the new Format from the dropdown list.
9. To add additional Available Columns, use and select the new output from the dropdown list. You may edit the name of the columns by simply replacing the information in the field.
10. To edit the Data Preview, click on to remove an output column, or use to sort in ascending order, use to not sort, or use to sort in descending order. Also, columns in the Data Preview can be moved left or right to reorder where they appear when the report is generated. Simply click on the column and move it to the desired location.
11. Click Run to run the report without saving or Save to save the report. You are returned to Report Details page.

To copy a report:

1. Scroll over the History link. The sub-navigation menu displays.
2. From the Reporting link, click Reports from the dropdown list. The Reports list displays.

3. Click the name of the report you want to copy. The corresponding Report Details page displays.
4. Click the Copy This Report button. The Edit Report page displays with the Name field blank, but all other details filled in.
5. Fill in the new name of the report in the Name field and click Save. You are returned to the Reports list with the copied report added with its new name.

To delete a report:

1. Scroll over the History link. The sub-navigation menu displays.
2. From the Reporting link, click Reports from the dropdown list. The Reports list displays.
3. Click the name of the report you want to delete. The corresponding Report Details page displays.
4. Click Delete. A warning message asks you to confirm that you want to delete the report, and informs you that this operation cannot be undone.
5. Click OK. You are returned to the Reports list with the deleted report removed.

Browsing the Scheduled Reports List

The Scheduled Reports list displays a list of reports, when they are scheduled to run, and who the recipients are. The list displays reports listed alphabetically by schedule name.

Administrators with appropriate permissions can view the Scheduled Reports associated with their own accounts.

To view the list of scheduled reports for your account:

1. Scroll over the History link. The sub-navigation menu displays.
1. From the Reporting link, click Scheduled Reports from the dropdown list. The Scheduled Reports list displays.

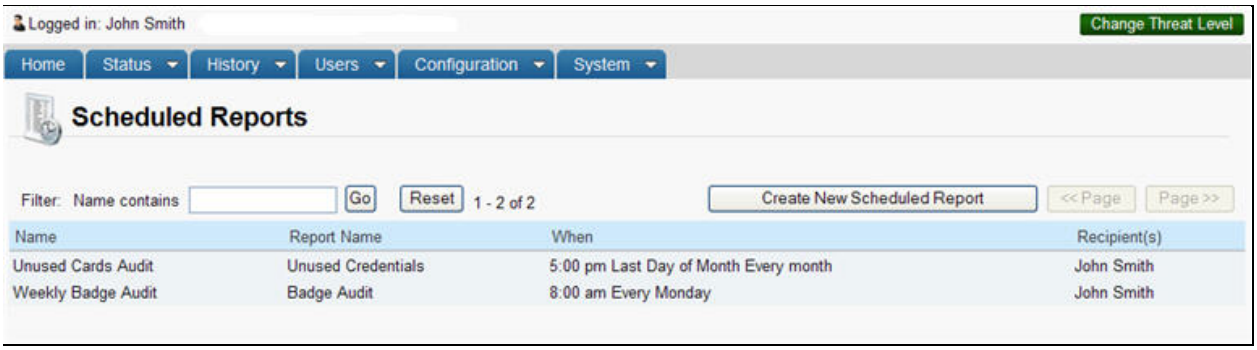


Figure 36. View Scheduled Reports List

Details displayed include:

- Name. The name of the scheduled report, such as "Weekly Badge Audit" or "Unused Cards Audit."
- Report Name. The name of the report being generated.
- When. The time and frequency of the scheduled report.
- Recipient. The administrator(s) that receive the scheduled report.

Administrators with appropriate permissions can:

Click the name of any scheduled report to access the corresponding Scheduled Report Details page.

Click Create New Scheduled Report to access the Edit Scheduled Report page to create a new report for this account.

Creating a New Scheduled Report

Administrators with appropriate permissions can create new scheduled reports.

To create a new scheduled report:

1. Scroll over the History tab, the sub-navigation menu displays.
2. From the Reporting link, click Scheduled Reports from the dropdown list. The Scheduled Reports List displays.
3. Click on the Create New Scheduled Report button. The Edit Scheduled Report page displays.

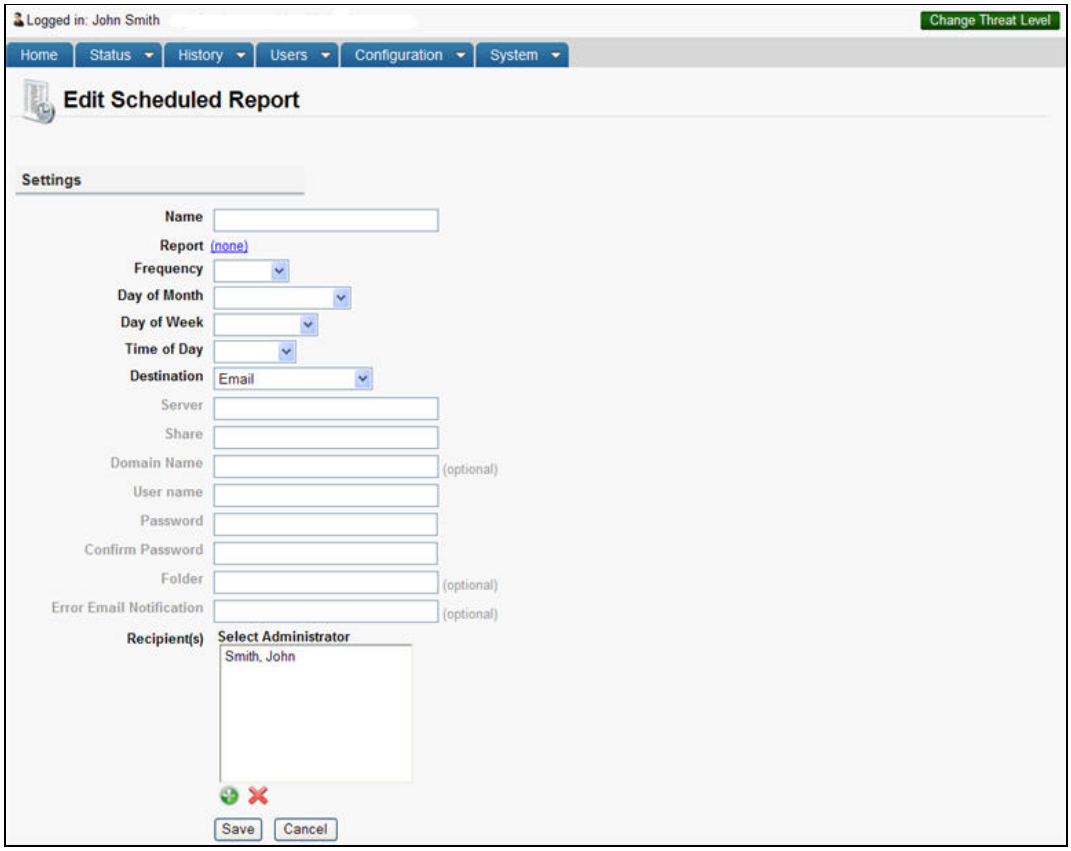


Figure 37. Create New Scheduled Report

4. Enter a Name for the scheduled report.
5. Click on the Report link to select which report will be scheduled.
6. Select the Frequency that the scheduled report will run from the dropdown list. Depending upon the frequency, select the Day of Month or Day of Week that the report will run. Finally, select the Time of Day the report will run.
7. Select the Destination for the scheduled report.
    - None (Disabled) – this is in case you want to keep the scheduled report information in place, but do not wish to currently generate it.
    - Email – this will send the scheduled report data to the email address of any selected administrators.

- Remote Server – this will send the schedule report data to a remote server. If selected, fill in the required fields.
  - Error Email Notification – this will send an email to the provided email address notifying the recipient of a failure to post the data to the requested location.
- Email/Remote Server – this will send the scheduled report data to both a remote server location and to the email address of any selected administrators.

8. If email is chosen as a delivery method, select the Recipient(s) from available administrators. Use to call up a popup window of available administrators. Click on the name of the administrator and you returned to the Edit Scheduled Report page and the administrator has been added to the Recipient(s) box.
9. Click Save. You are returned to the Scheduled Report Details page.

	NOTE: *Scheduled Reports have a maximum size of 20MB (megabytes) or the maximum attachment size limit established under the SMTP server settings, whichever is smaller.*

Managing Scheduled Reports

Once a scheduled report is created, its details can be edited at any time. Scheduled Reports can also be deleted.

Administrators with appropriate permissions can manage scheduled reports.

To view a scheduled report:

1. Scroll over the History link. The sub-navigation menu displays.
2. From the Reporting link, click Scheduled Reports from the dropdown list. The Scheduled Reports list displays.
3. Click the scheduled report you wish to view. The corresponding Scheduled Report Details page displays.

Figure 38. View a Scheduled Report

To edit a scheduled report:

1. Scroll over the History link. The sub-navigation menu displays.
2. From the Reporting link, click Scheduled Reports from the dropdown list. The Scheduled Reports list displays.
3. Click the scheduled report you wish to edit. The corresponding Scheduled Report Details page displays.
4. Click Edit. The Edit Scheduled Report page displays.

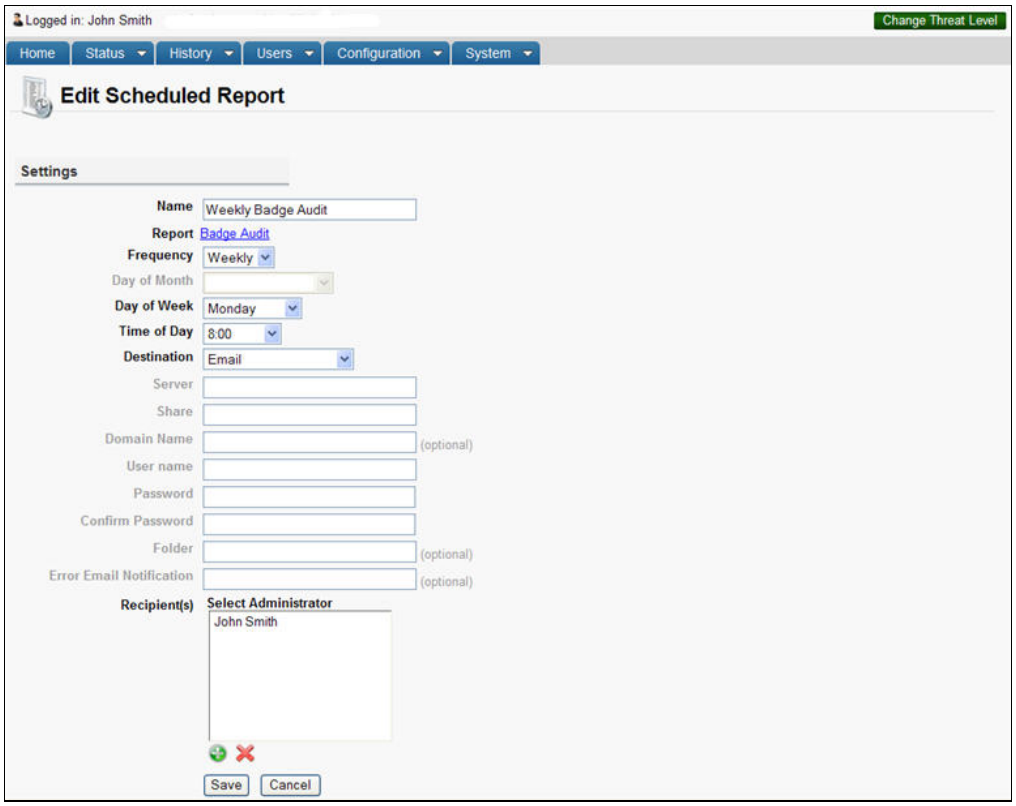


Figure 39. Edit a Scheduled Report

5. Make whatever edits are necessary.
6. Click Save to save the scheduled report. You are returned to Scheduled Report Details page.

To delete a report:

1. Scroll over the History link. The sub-navigation menu displays.
2. From the Reporting link, click Scheduled Reports from the dropdown list. The Scheduled Reports list displays.
3. Click the name of the scheduled report you want to delete. The corresponding Scheduled Report Details page displays.
4. Click Delete. A warning message asks you to confirm that you want to delete the scheduled report, and informs you that this operation cannot be undone.
5. Click OK. You are returned to the Scheduled Reports list with the deleted report removed.

Running a Muster Report

Once antipassback zones have been established, administrators with appropriate permissions can generate a muster report which allows them to view users and their current locations within specified (or all) antipassback zones.

To run a Muster Report (once antipassback zones have been established):

1. Scroll over the History link. The sub-navigation menu displays.
2. From the Reporting link, click Muster Report from the dropdown list. The Muster Reports page displays.
3. Select a zone. Available zones are listed in the right hand box. Click on the <- arrow to move the zone from available to selected. To select all zones, check the All Zones checkbox. To remove a selected zone, click on the -> arrow and move the zone from the selected zone box back to the available zone box.
4. To allow global visibility, check the Global Visibility checkbox.
5. When finished selecting zones, click Generate Report to generate a muster report.
6. The muster report will appear in a new window listing the selected zone, the users in that zone, and the total number of users in that zone.

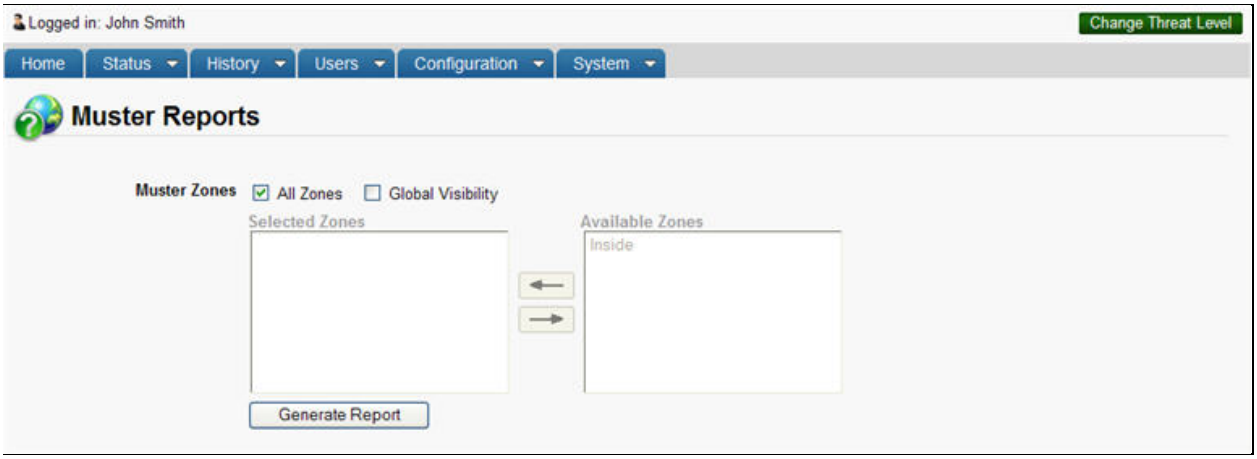


Figure 40. Generating a Muster Report

Browsing the Administrative Journal

The Administrative Journal tracks all Administrator actions in Brivo Onsite Server. For example, each time an Administrator creates, edits or deletes information in the interface, it is logged in the Administrative Journal.

All Administrators for the Account can view the Journal.

To view the Administrative Journal:

1. Scroll over the History link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Administrative Journal. The Administrative Journal for the current day displays.

Figure 41. View Administrative Journal

Details displayed include:

- Time. The time at which the Administrator performed the action.
- Administrator Name. The name of the Administrator who performed the action.
- Action. The action performed, including old and new values for changes to data or identification of created or deleted data.

Administrators with appropriate permissions can:

View actions that were performed on a specific date:

- Click << in the View Date section to scroll backwards day-by-day, to view past activity logs.
- Click to select a specific date from a popup calendar, then click Go to view the activity log for that date.
- Click >> to scroll forward day-by-day.

Click <<Page or Page>> to scroll backward and forward through the complete list of events for the current day.

6. Users & Groups

What are Users, User Aliases, and Groups?

A *user* is any person who requires access to one or more devices at the facility. A user has unique credentials, such as a card or PIN, that enable entry and exit at the specified doors. A user can belong to one or more groups.

A *user alias* is a way to place a user in multiple sub-accounts. The user name, user photo, credentials, and dates work across permissions granted in multiple sub-accounts. The advantage to this is that it allows each account to manage its own set of permissions on a given user. Note that suspending/expiring/deleting a primary identity affects all aliases. Also, the primary identity user name and user photo will propagate to all other accounts and cannot be changed except in the primary account.

A *group* is a set of users with the same access privileges to a facility. A group has a descriptive name, such as "Washington Staff." Access privileges are defined at the group level. A user inherits privileges from the group(s) to which he or she belongs. However, an individual user's privileges can be set to start and/or expire on specified dates.

Administrators vs. Users

The term *user* refers to an individual who has access privileges to some part of a building. It does not refer to end-users of the interface; users do not have direct access to the Brivo Onsite Server interface. Instead, Administrators add and manage user-related information.

The term *Administrator*, on the other hand, refers to an individual who has access permissions to the interface. Administrators manage the interface itself.

An Administrator is also a user, and is subject to the same rules of group assignments when determining access privileges to devices.

Browsing the Users List

The Users page displays a list of users for an account and identifies the group affiliation(s), if any, of each. Administrators with appropriate permissions can view the users associated with their account.

To view the list of users for your account:

1. Scroll over the Users link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Users from the dropdown list. The Users list displays.

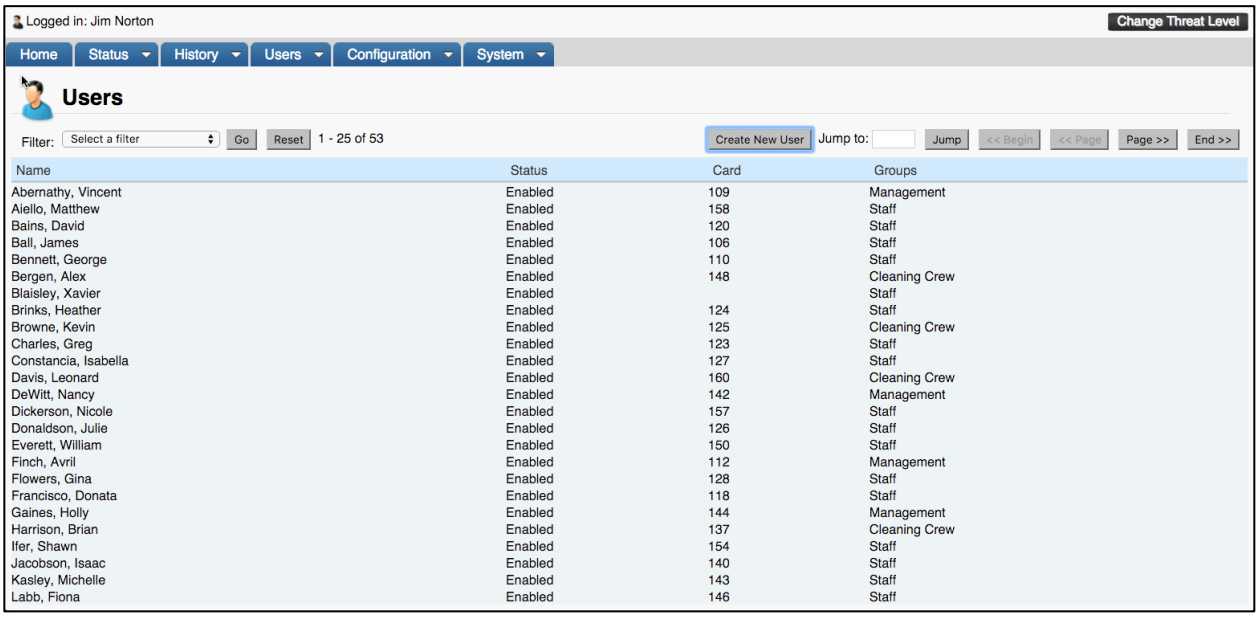


Figure 42. View Users List

Details displayed include:

- Name. The user's name.
- Status. The current status of the user.
- Card(s). The number(s) of the user's card(s).
- Groups. The list of groups with which the user is affiliated.

Administrators with appropriate permissions can:

Click the name of any user to access the corresponding User Details page.

Click a Filter from the drop-down list, then enter the associated parameter(s) and click Go to view a subset of the Users list. You can filter by any combination of Last Name, Group, Status, Current Zone, Aliased User, or any custom field.

Use the Jump field to move anywhere in the list of users by entering the number of the user record and clicking the Jump button.

Click <<Begin or End>> to travel to the beginning or end of the list of users.

Click <<Page or Page>> to scroll backward and forward through the list of users.

Click Create New User to access the Edit User page to create a new user for this account.

Viewing User Details

The User Details page displays information for an individual user.

To view details for a specific user:

1. Scroll over the Users link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Users from the dropdown list. The Users list displays.
3. Click the user you want to view. The corresponding User Details page displays.

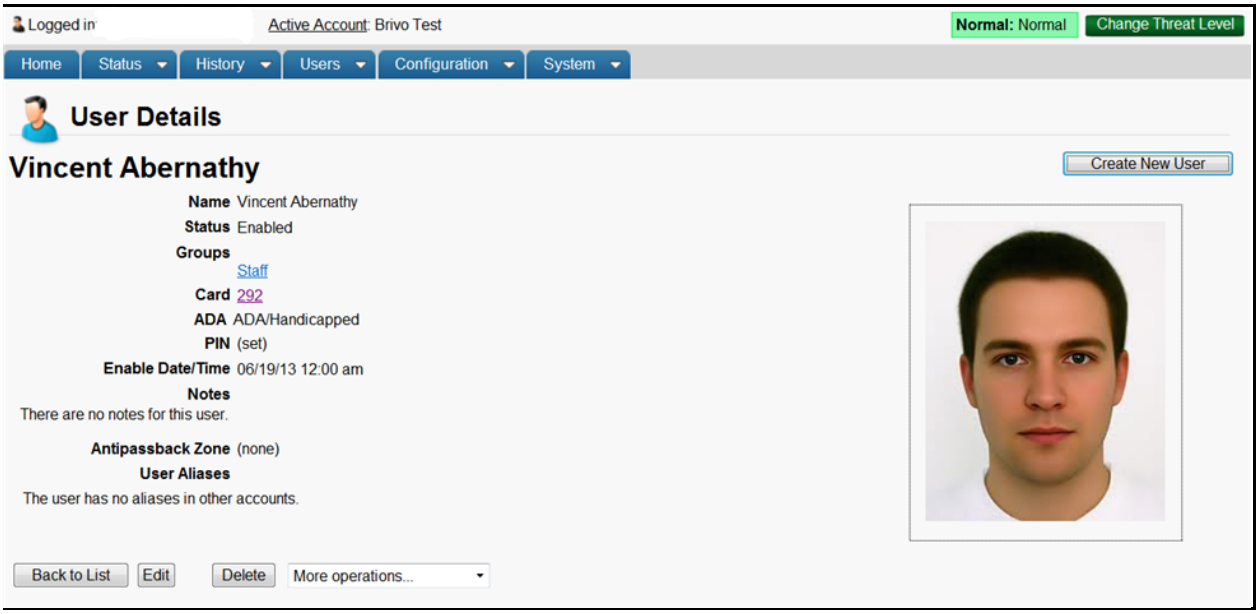


Figure 43. View User Details

Details displayed include:

- Name. The name of the user.
- Status. The current status of the user (enabled, suspended, or expired).
- Custom Fields. If there are any custom fields defined for this account, and if there have been values entered in these fields for the given user, that information displays at the top of this page.
- Groups. The list of groups with which the user is affiliated. If the user is not affiliated with any groups, this field does not display.
- Card. If the user has been assigned a card, that card number displays.
- ADA. If the account has a TKE license, this field shows if the user is ADA/Handicapped.
- PIN. If user has been assigned a PIN, the value (set) displays in this field; for security reasons the actual value is not displayed.
- Enable Date. If the user has been assigned a specific date on which his or her access is to become active, that date displays. Likewise, if an Expiration Date for the user's access has been set, that is also shown.
- Notes. If there are any notes concerning the user, they will be displayed here along with the time that those notes were entered into the system.

- Antipassback Zone. This field lists the current zone in which the user resides.
- Aliases in other account. This field lists any aliases the user has in other accounts.
- Last Access. This field lists the device where the last access occurred.
- Photo Image. If user has been assigned a photo image, it will display here.

Administrators with appropriate permissions can:

Click Back to List to return to the Users list for this account.

Click Create New User to create a new user for this account.

Click Edit to make changes to this user's information.

Click Delete to delete the user.

Click  to delete a user alias.

Under the More Operations dropdown list

- Click Suspend User to suspend a user. If suspended, the user status will change from enabled (or expired) to suspended. The Suspend User button will also change to Reinstate User. A suspended user's credential(s) will not work at any device. Changes are recorded in the administrative journal.
- Click Create User Alias to create a user alias for another account.
  - If a user alias exists, click Re-home User Alias to move a user from one account to another.
- Click Reset Antipassback Zone to place a user in an available zone.
- Click Print Badge to print a user badge.
- Click Clone User to create a new user profile with the same User Profile content as the Cloned User. The following fields will not be copied when a User is Cloned:
  - First Name
  - Middle Name
  - Last Name
  - Photo Image
  - Assigned Cards
  - PIN

Creating a User

Administrators with appropriate permissions can create users for their account.

To create a user:

1. Scroll over the Users link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Users from the dropdown list. The Users list displays.
3. Click Create New User. The Edit User page displays with blank fields.

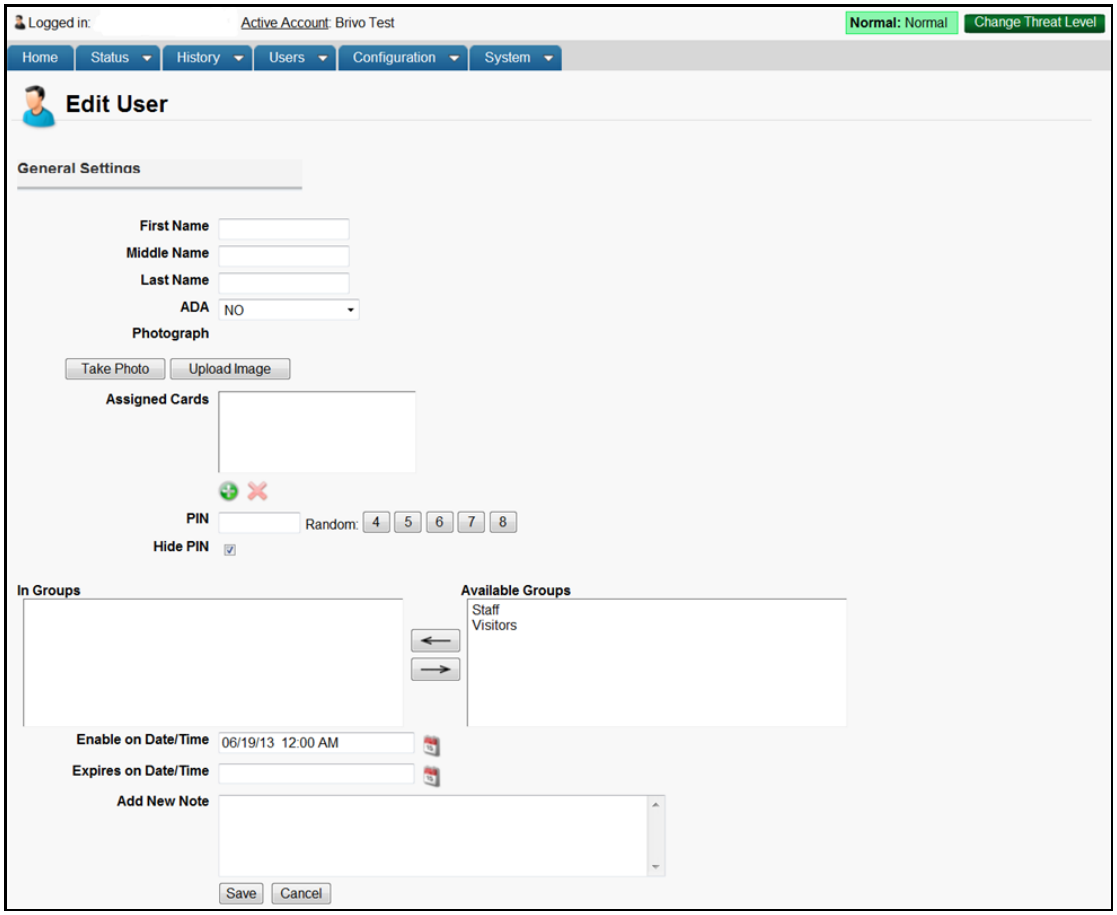


Figure 44. Create a New User

4. Enter the user's First Name, Middle Name, and Last Name. The First Name and Last Name fields are required.
5. If the account has a TKE license, the user may be noted as handicapped by toggling the ADA dropdown menu from No to Yes.
6. If you would like to import a photograph for the user, click Upload Image to locate the image from your hard drive. If your computer supports webcam usage, you make click Take Photo to capture and crop the image of the user instead.
7. Custom fields display to the right of the name fields. For any custom field, enter valid values for this user. These fields are optional.
8. If you would like to import a signature for the user, you may create an Image Custom Field and click Browse to locate the image from your hard drive.

9. If your doors have card readers, select a Card number by clicking the button to view a popup list of all currently unassigned cards. Each user may have a maximum of 16 cards assigned to them.

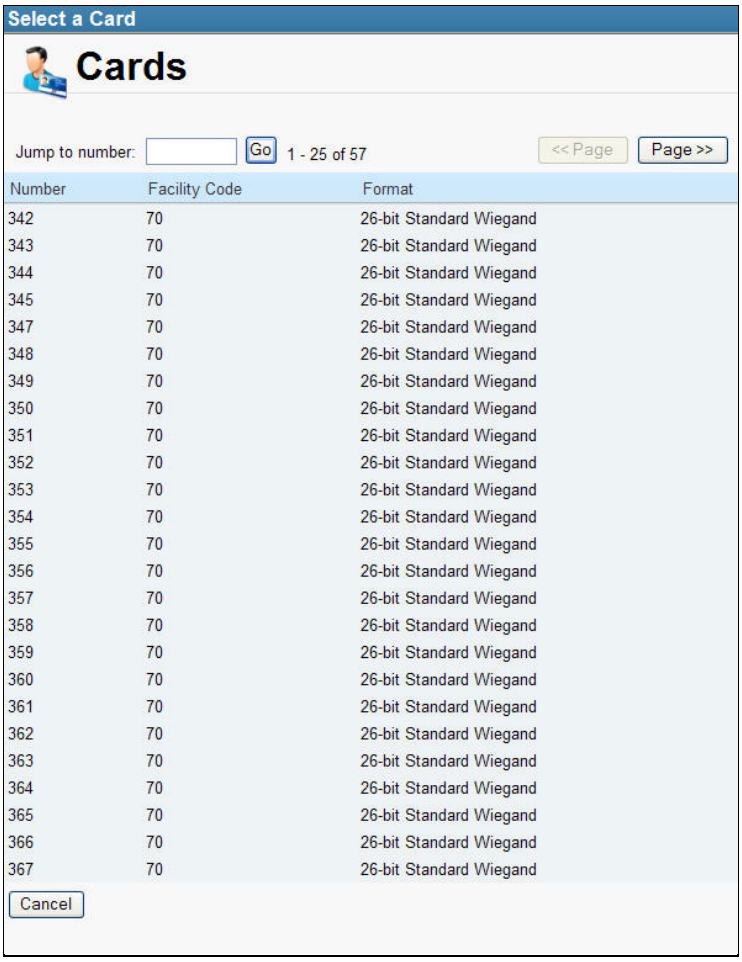


Figure 45. Select a Card Popup List

10. If your doors have keypads, enter a 4- to 8-digit number in the PIN field, or click one of the number buttons to generate a random PIN with 4, 5, 6, 7 or 8 digits. The number entered will only appear as asterisks by default. To see the number, uncheck the Hide PIN checkbox.
11. To assign a user to a group, select the desired group from the Available Groups list on the right and click the left arrow (←). The group name displays in the In Groups list. To remove a user from a group, select the group from the In Groups list and click the right arrow (→). Users can be assigned to up to 16 groups at a time. The user inherits access permissions from the groups to which he or she belongs. For users who belong to multiple groups, their access permissions are cumulative.
12. The Enable on Date defaults to today's date. Change the date if the user's access permissions should take effect on a later date. The Expire on Date field is empty by default. Enter a date if the user's access permissions should expire on a pre-determined date; otherwise leave the field blank.
13. The Add New Note field allows administrators to enter information specific to a user such as any medical conditions.
14. The Notes field shows any existing notes, if any, and when they were entered into the system.
15. Click Save to create the user. The User Details page for the new user displays.

To create a user alias:

1. Scroll over the Users link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Users from the dropdown list. The Users list displays.
3. Click the user you want to edit. The User Details page displays.
4. Click Edit. The Edit User page displays.

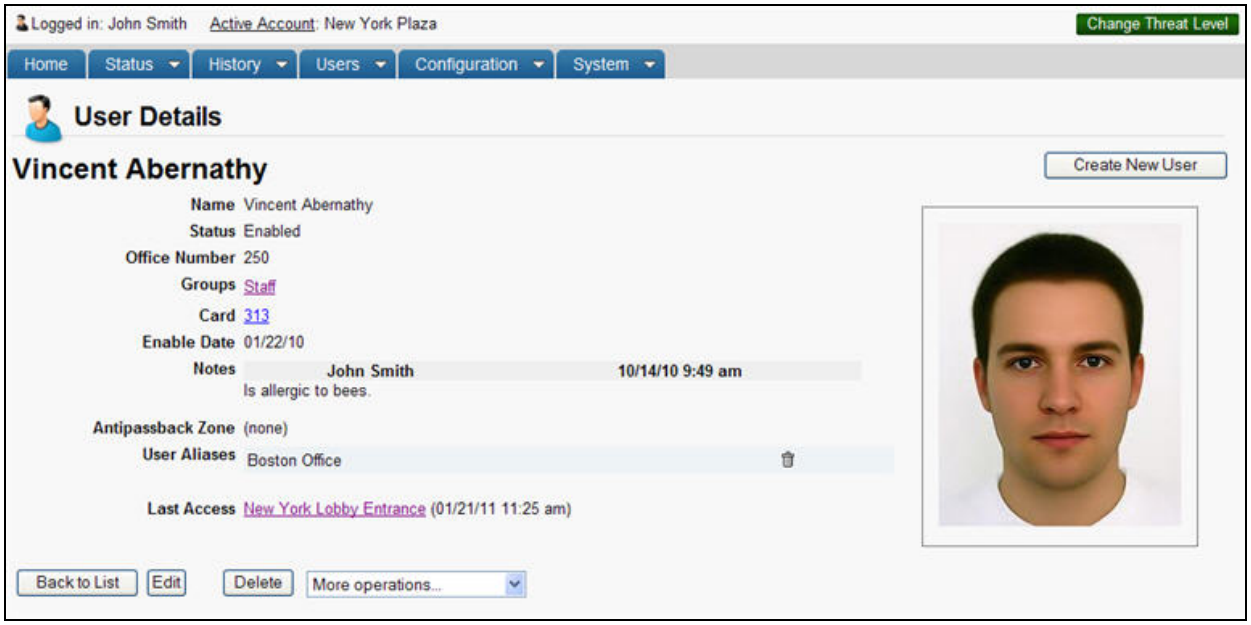


Figure 46. Create a User Alias

5. Under the More Operations dropdown menu, click Create User Alias. A popup window will appear asking in which Target Account you want to place the user alias. Click on the appropriate Target Account and you are returned to the User Details page. The Target Account will now appear next to User Aliases on the User Details page.
6. In the Target Account, the aliased user will appear with an icon next to their name denoting that it is an alias.

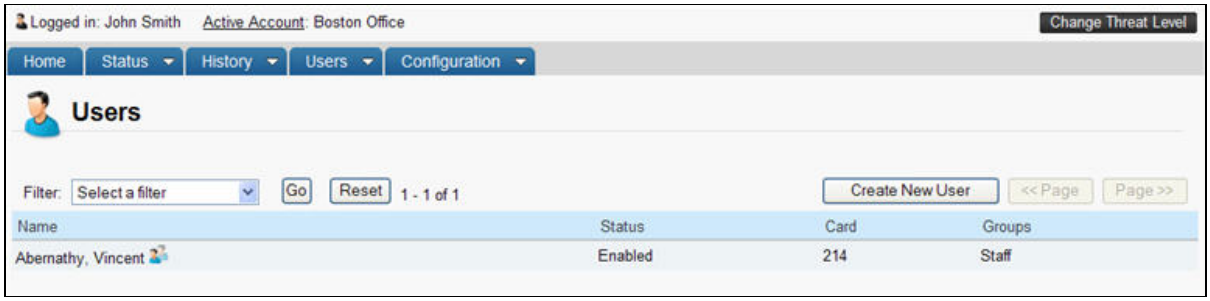


Figure 47. Aliased User

To rehome a user alias:

Rehoming is switching a user's primary account to a new target account, making the new target account the user's primary account.

1. Scroll over the Users link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Users from the dropdown list. The Users list displays.
3. Click the user you want to rehome. The User Details page displays.
4. From the dropdown list, select Rehome User Alias. A popup window with available target accounts appears. Select the target account you want. A warning window appears asking if you want to rehome the user. Click OK and you are returned to the User Details page. You will now see the user is listed as a user alias from the target account.

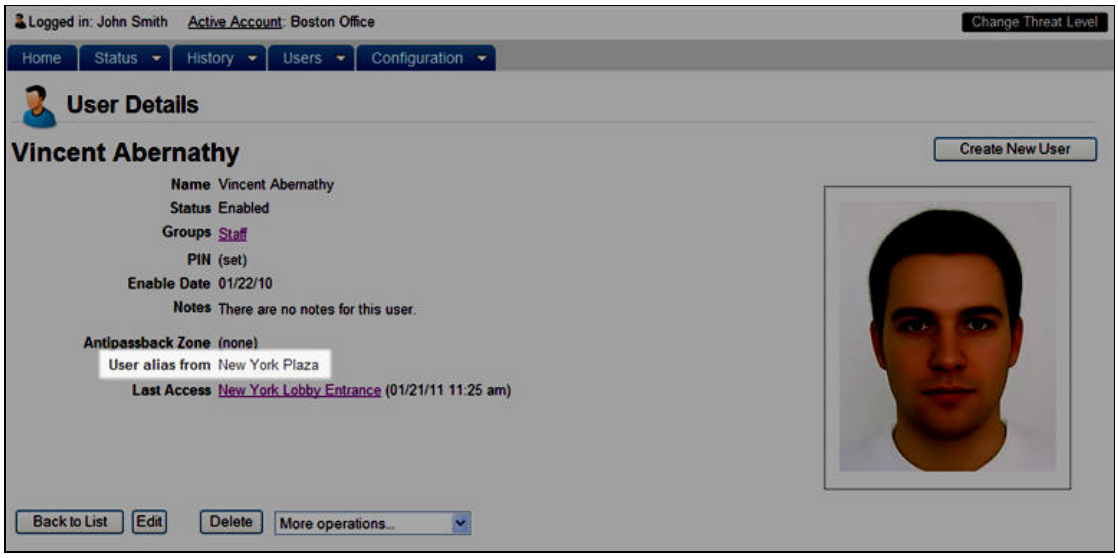


Figure 48. Rehoming a User Alias

	NOTE: *When a user is re-homed, the card assigned to that user moves to the new primary account, but if the user was assigned a PIN, the PIN remains with the original (now aliased) account. The user will have to be reassigned a new PIN number in the primary account.*

Managing Users

Once a user is created, his/her information can be updated at any time. Or, the user can be deleted completely from the system.

Administrators with read/write access can edit and delete users.

To edit a user:

1. Scroll over the Users link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Users from the dropdown list. The Users list displays.
3. Click the user you want to edit. The User Details page displays.
4. Click Edit. The Edit User page displays.

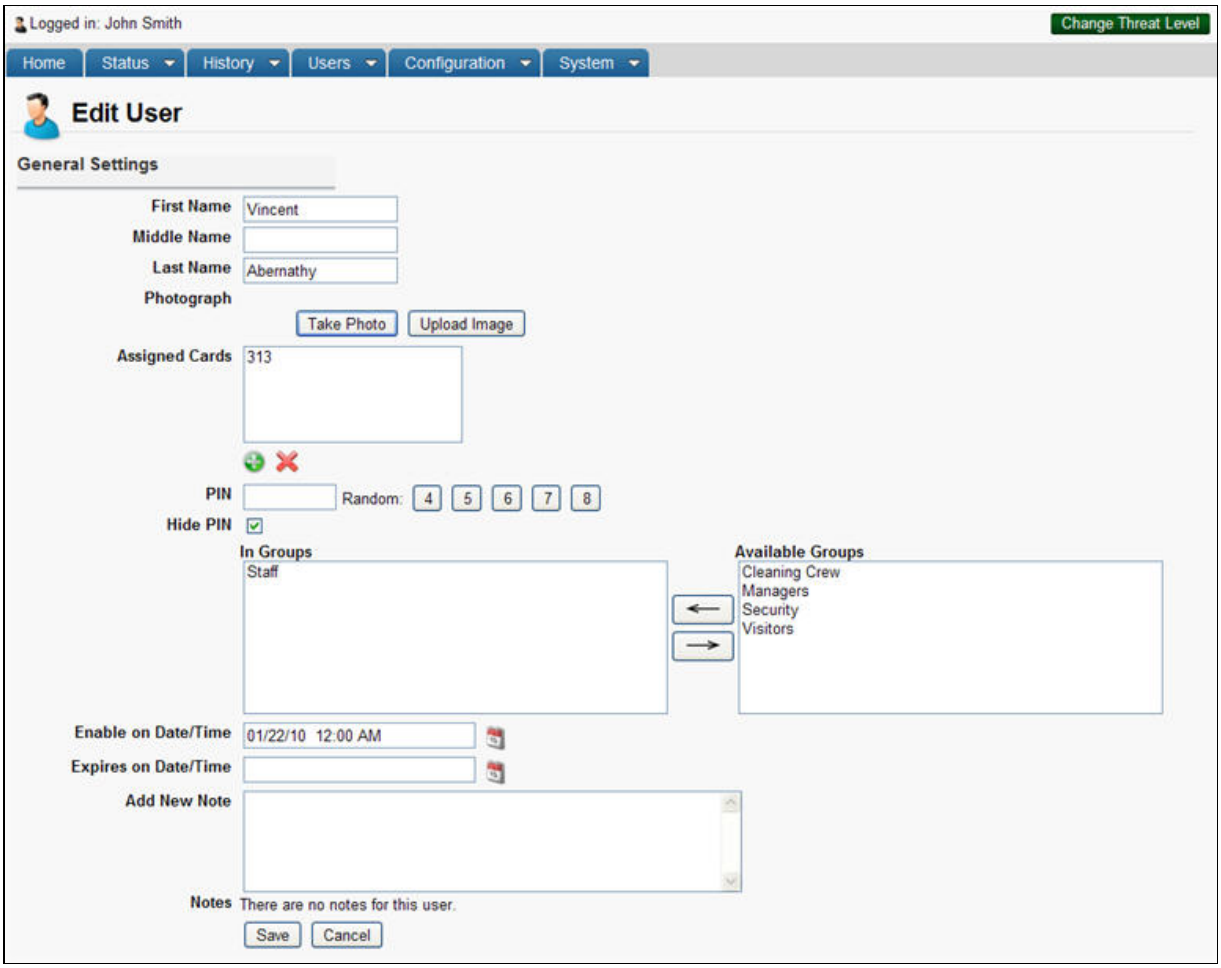


Figure 49. Edit a User

5. All fields on this page can be edited. Enter the desired changes using the guidelines for creating a user, described above.
6. You can edit or delete the values in the Card and PIN fields at any time. However, if you leave both of these fields blank, you revoke all access privileges for the user. Until a new card or PIN is entered, the user will have no access to the facility.
7. Click Save. You are returned to the User Details page with the updates displayed.

To delete a user:

1. Scroll over the Users link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Users from the dropdown list. The Users list displays.
3. Click the user you want to delete. The associated User Details page displays.
4. Click Delete. A warning message asks you to confirm that you want to delete the user.
5. Click OK. You are returned to the Users list with the deleted user removed.

WARNING: *Deleting Users*

When you delete a user, the user is removed from all groups to which he or she belongs and all aliases are deleted as well. Accordingly, all of the user's access privileges are revoked. If the user has a PIN, it will no longer be viable. If the user has a card, the card will become unassigned and can be assigned to another user at a later date.

Once a user is deleted, the user cannot be undeleted. To add the user back, he or she must be re-created as a new user.

If a user is also an administrator, when the user is deleted, the administrator login is also deleted.

To delete a user alias:

1. Scroll over the Users link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Users from the dropdown list. The Users list displays.
3. Click the user you wish to edit. The associated User Details page displays.
4. On the User Aliases line, a list of all accounts where there is an alias for this user is displayed. Next to each account name is a trash can icon. Simply click on the trash can icon and a warning popup window will appear. Click OK to delete the alias and you are returned to the User Details page.

Browsing the Groups List

The Groups list displays a list of groups defined for your account. The list displays groups listed alphabetically.

Administrators with appropriate permissions can view the Groups associated with their own accounts.

To view the list of groups for your account:

1. Scroll over the Users link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Groups from the dropdown list. The Groups list displays.

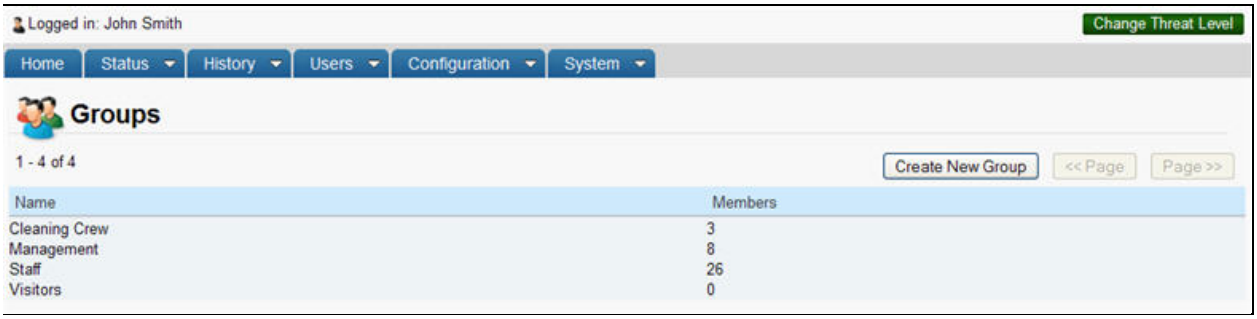


Figure 50. View Groups List

Details displayed include:

Name. The name given the group, such as "Managers" or "Cleaning Crew."

Members. The number of users currently associated with this group.

Administrators with appropriate permissions can:

Click the name of any group to access the corresponding Group Details page.

Click Create New Group to access the Edit Group page to create a new group for this account.

Viewing Group Details

The Group Details page displays the name and access information for a specific group.

To view the detail page for a group:

1. Scroll over the Users link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Groups from the dropdown list. The Groups list displays.
3. Click the name of the group you want to view. The corresponding Group Details page displays.

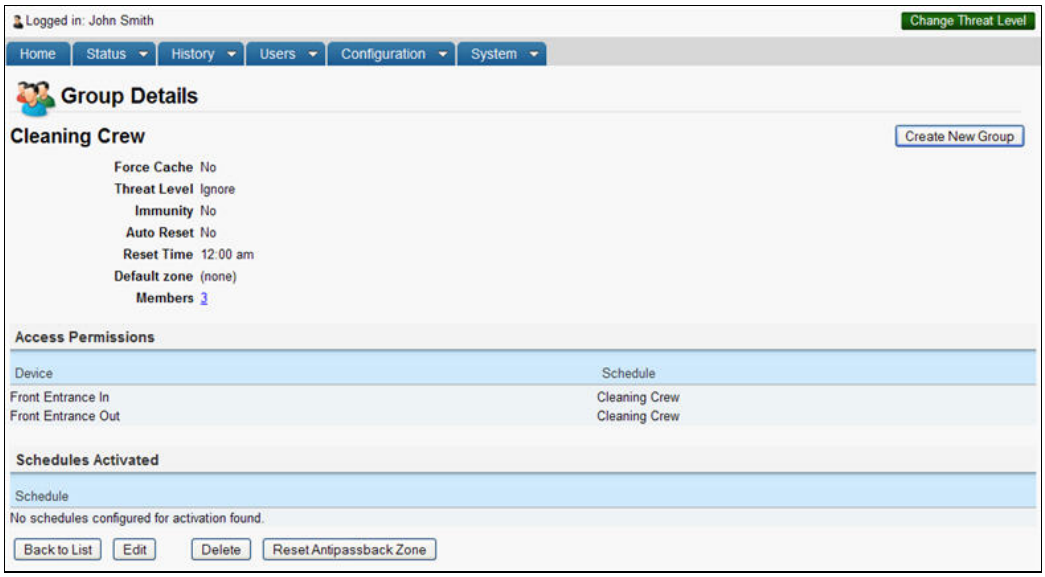


Figure 51. View Group Details

Details displayed include:

- Force Cache. If Force Cache is enabled, users in the group are pushed to all panels automatically. Certain users (security or emergency personnel) must be able to access doors/devices even if the server cannot be reached, for example during a network outage.
- Enable Date/Time. Shows ONLY if the group has Enable on Date/Time information entered. This is the date and time on which the group's permissions will begin to function.
- Expire Date/Time. Shows ONLY if the group has Expire on Date/Time information entered. This is the date and time after which the group's permissions will no longer function.
- Threat Level. Shows if the group ignores Threat Levels or at what Threat Level severity the group will have access.
- Immunity. Shows antipassback settings including if the group is immune, if auto reset is enabled, and what is the reset time. Finally, the default zone is shown.
- Members. Shows the number of users currently assigned to this group. Clicking on the number will call up a User List with all current members of this group.
- Access Permissions. All doors and Valid Credential Input Devices defined for the account are listed, along with the schedule, if any, during which the group has access to those doors and devices.
- Schedules Activated. If the group is responsible for activating a schedule, that schedule is identified. For more information see the section on *Creating a Schedule.*

Administrators with appropriate permissions can:

Click the name of a Device to access the Device Details page.

Click the name of a Schedule to access the Schedule Details page.

Click Back to List to return to the Groups list for this account.

Click on the Members link to see a list of users in that group.

Click Create New Group to access a blank Edit Group page in order to create a new group for the account.

Click Edit to make changes to the current group's access permissions.

Click Delete to remove the group from the account.

Creating a Group

A group is a set of users with the same access privileges.

For example, the account "Acme Megaplex" may have two doors. If all employees require the same level of access to both doors, then a single group, "Acme Staff," would be sufficient.

Or, the account might have three doors. If we say that the staff requires access to "Front Door" only while managers require access to all three doors, then it would make sense to create two groups, one called "Acme Staff" and one called "Acme Managers."

Administrators with read/write access can create groups for their own accounts.

To create a group:

1. Scroll over the Users link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Groups from the dropdown list. The Groups list displays.
3. Click Create New Group. The Edit Group page displays with blank fields.

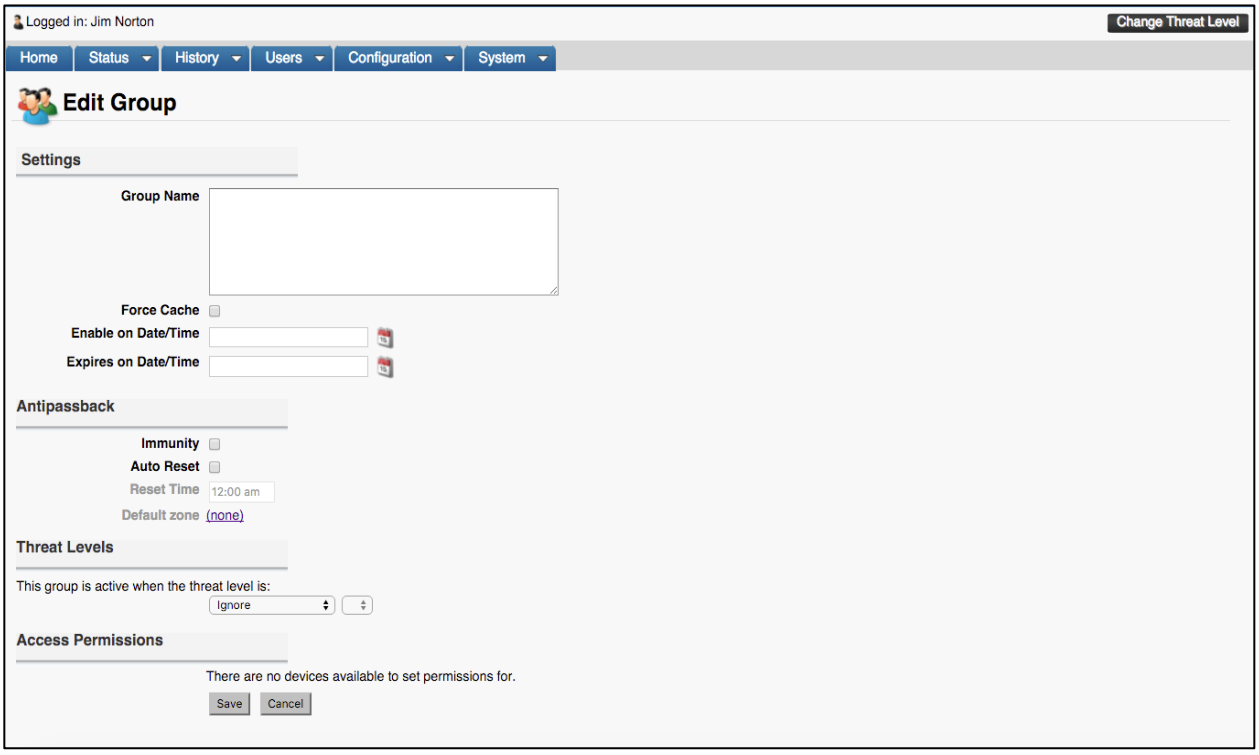


Figure 52. Create New Group

4. Enter a brief, descriptive Group Name.
5. If the users in this group need to be pushed down to the panels, check the Force Cache checkbox.
6. You may enable a group's permissions at a certain time and date by filling in the Enable on Date/Time field. You may disable a group's permissions at a certain time and date by filling in the Expires on Date/Time field. If these fields are left blank, the group is enabled immediately for an indefinite period of time.

7. For antipassback, you may check the Immunity checkbox to make the users in this group immune to antipassback. You may check the Auto Reset checkbox for soft antipassback and choose a reset time from the dropdown list. Finally, select a default zone to start by clicking on the (none) link and choosing from the popup window.
8. You may have the group ignore Threat Levels or select under what Threat Level conditions the group will operate. Note that this will affect all permissions this group has to devices.
9. For each device listed, define Access Permissions by selecting a schedule from the drop-down list associated with each device. This schedule determines the days and times the users in this group will have access to the device. If the group should have no access to a specific door or device, leave (no access) selected.
10. Click Save. You are returned to the Group Details page associated with the new group.

Creating a Group Enabled Schedule

WARNING: *Group Enabled Schedules and Time Zones*

Each schedule operates according to local time zones. It is recommended to make sure that if you are using a Group Enabled Schedule, do not use it across two different time zones.

The Brivo Onsite Server Group Enabled Schedule feature allows you to implement a First-Person-In, Supervisor-on-Site, or Input-Controlled Schedules functionality at your facility.

With First-Person-In, you stipulate that the schedule controlling a specific door cannot be activated until a member of the activating group accesses it. For example, you may have scheduled the front door of your building to be unlocked at 9:00AM, *but only if a security guard is present*. If no member of the Front Door Guard group arrives until 9:15, the door remains locked until that time and can only be accessed with a valid credential.

Supervisor-on-Site performs essentially the same function, but applies to a situation where you want to ensure that no other employees enter a designated building or area until a supervisor has arrived. Not only does the door remain locked until that time, but card readers and keypads also remain inactive.

Input-Controlled Schedules allow an input (i.e., input switch, valid credential) to activate a schedule. If the group enabled schedule has the Auto-Deactivate checkbox unchecked, unlike other group enabled schedules, such a schedule will not deactivate until the input changes state.

Implementing either of these features requires careful thought to ensure that you do not inadvertently bar your employees unintentionally, nor leave doors unlocked when they should not be. To ensure the security of your facility you must perform the following steps in the order indicated:

1. *Create a group that includes only those people you want to activate a specific schedule at a specific door or device*. Give the group an identifying name, such as "Openers." These users will almost certainly belong to at least one other group as well, a group that defines their overall access privileges; their membership in the group Openers means only that they can activate the schedule for a specific door. See the section on *Creating a Group* for procedural information.
2. *Associate a schedule with the activating group*. When you make this association, you are *NOT* indicating that members of the group will only have access privileges during that schedule's time period; it means that when the first member of the activating group accesses the designated door the schedule will then become active. See the section on *Creating a Schedule* for guidelines on associating a schedule with an activating group.

WARNING: *Activating Group Grace Periods*

When you assign an activating group to a schedule, you are prompted to specify a Grace Period. Without a grace period, the schedule only becomes active if a group member arrives at or after the schedule start time, not before. For example, if the schedule starts at 9:00 and a member of the activating group arrives at 8:55, the schedule will not become active at 9:00. With a grace period of ten minutes, a member of the activating group could arrive any time after 8:50 and the schedule would still become active at its 9:00 start time.

3. *Assign the activating group access privileges at the desired door.* By giving the activating group access privileges at a specific door according to a specific schedule you tell the system "This schedule does not allow access for any user until it enters an active period *and* is first accessed by a member of the activating group." See the instructions for *Managing Groups* in the following section for instructions on managing group privileges.

Managing Groups

Once a group is created, its name or access permissions can be edited at any time. Editing the access permissions changes the days and times during which the users in that group can access a device.

Groups can also be deleted. When a group is deleted, all access privileges assigned to its users are revoked.

Administrators with appropriate permissions can manage groups.

To edit a group:

1. Scroll over the Users link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Groups from the dropdown list. The Groups list displays.
3. Click the group whose permissions you want to change. The corresponding Group Details page displays.
4. Click Edit. The Edit Group page displays.

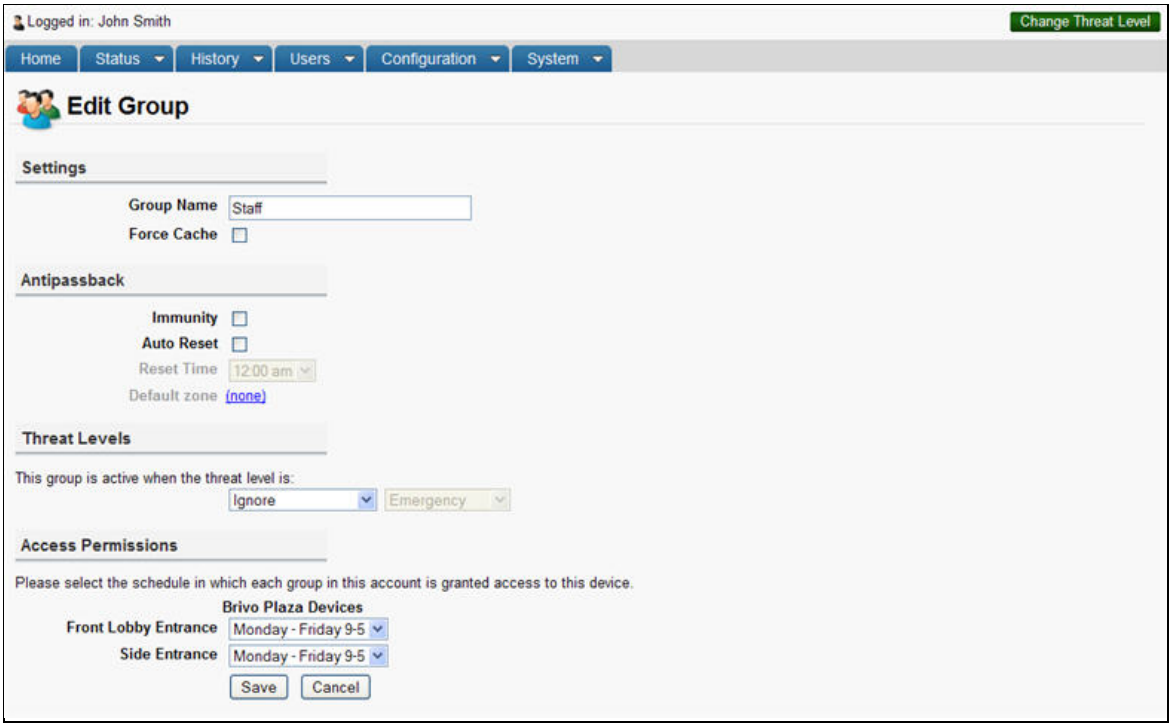


Figure 53. Edit a Group

5. To rename the group, enter a new value in the Group Name field.
6. To establish antipassback settings, check the Immunity checkbox if you wish the group to be immune to antipassback. To establish an auto reset time for returning the users in the group to their default zone, check the Auto Reset checkbox, select an appropriate time, and click on the Default Zone link and select the default zone you wish the users in the group to be returned to.
7. To edit the threat level of the group, choose from the dropdown menu whether or not the group will ignore or be subject to threat level conditions.
8. To update the access permissions for any device, select a new schedule from the drop-down list associated with that device or click (no access).
9. Click Save. You are returned to the Group Details page with the updates reflected.

To delete a group:

1. Scroll over the Users link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Groups from the dropdown list. The Groups list displays.
3. Click the name of the group you want to delete. The corresponding Group Details page displays.
4. Click Delete. A warning message asks you to confirm that you want to delete the group, and informs you that this operation cannot be undone.
5. Click OK. You are returned to the Groups list with the deleted group removed.

Managing Custom Fields

Custom fields store optional information about a user, such as department or parking space assignment. They also have the option of being a text object, such as a user's job title, or an image object, such as a user's signature. You can define an unlimited number of custom fields for an account, and each can hold up to 32 alpha-numeric characters. Custom field labels are the same throughout your account. For example, if you name a custom field "Department" it will appear as Department on all pages, for every user in the account.

Administrators with appropriate permissions can view, create, edit, and delete custom fields.

To view a list of custom fields for an account:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Account link, click Custom Fields from the dropdown list. The Custom Fields list displays with arrows that allow users to reorder items as desired.
3. The Custom Fields list displays with arrows that allow users to reorder items as desired.

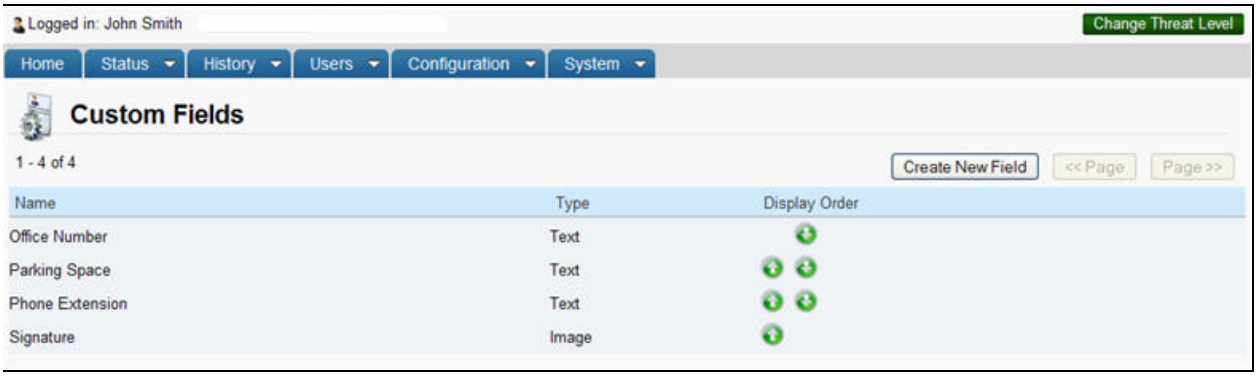


Figure 54. View Custom Fields List

Details displayed include:

- The Name of each custom field defined for the account.
- The Type of each custom field, either text or image.
- The Display Order of the custom fields and how they will appear on the User Details page.

Administrators with appropriate permissions can:

Click on the name of a custom field to access the Edit Custom Field page.

Click Create New Field to access a blank Edit Custom Field page in order to create a new custom field.

Change the Display Order of the custom fields by using the up and down arrows.

To create a new custom field:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Accounts link, click Custom Fields from the dropdown list. The Custom Fields list displays.
3. Click Create New Field. The Edit Custom Field page displays.

Figure 55. Create a Custom Field

4. Enter a brief, descriptive Name for the field, such as "Department" or "Office Number."
5. Select from the dropdown list whether you are creating a text object or an image as a custom field.
6. Select the display order from the dropdown list for where in the list the new custom field will appear.
7. Click Save. You are returned to the Custom Field page with the new field listed. This field now displays on the Edit User page for all users, and on the User Details page for all users who have a value defined for it.

To rename a custom field:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Accounts link, click Custom Fields from the dropdown list. The Custom Fields list displays.
3. Click the field you want to rename. The Edit Custom Field page displays.

Figure 56. Rename a Custom Field

4. Enter a new Name of the custom field.
5. Click Save. You are returned to the Custom Fields page, with the new field listed.

To delete a custom field:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Accounts link, click Custom Fields from the dropdown list. The Custom Fields list displays.
3. Click the field you want to delete. The Edit Custom Field page displays.
4. Click Delete. A warning message displays.
5. Click OK. You are returned to the Custom Fields page with the deleted field removed. This field and its contents are deleted for all users associated with the account.

7. Cards

What is a Card?

A *card* is a physical credential carried by a user, such as a proximity card, magnetic stripe card, or smart card. It has a number printed on its surface, such as "789" or "00789."

A user presents his or her card to a card reader — or "swipes" it — to enter a door. The card reader reads the card and sends the data to a control panel, which processes the request.

An example is that the card reader flashes green when a valid card is presented, and the door unlocks. If the card is rejected, the card reader flashes red and the door remains locked.

	*NOTE:* *For card readers without indicator lights, a valid card will still cause the door to unlock; there is just no green light to indicate success or red light to indicate failure.*

Browsing the Cards List

The Cards list is an inventory of cards associated with the system. It indicates which cards are assigned to users and which cards are unassigned. (Unassigned cards do not allow any type of access.)

Cards can be assigned, revoked or deleted. When a card is assigned, it allows a user to identify himself and request access to system devices and doors. When a card is revoked from a user, it becomes unassigned and can be assigned later to another user. When a card is deleted, it is erased from the system. If deemed appropriate (i.e. a card reported lost or destroyed is later recovered), deleted cards can be recreated.

To view the list of cards:

1. Scroll over the Users link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Cards from the dropdown list. The Cards list displays.

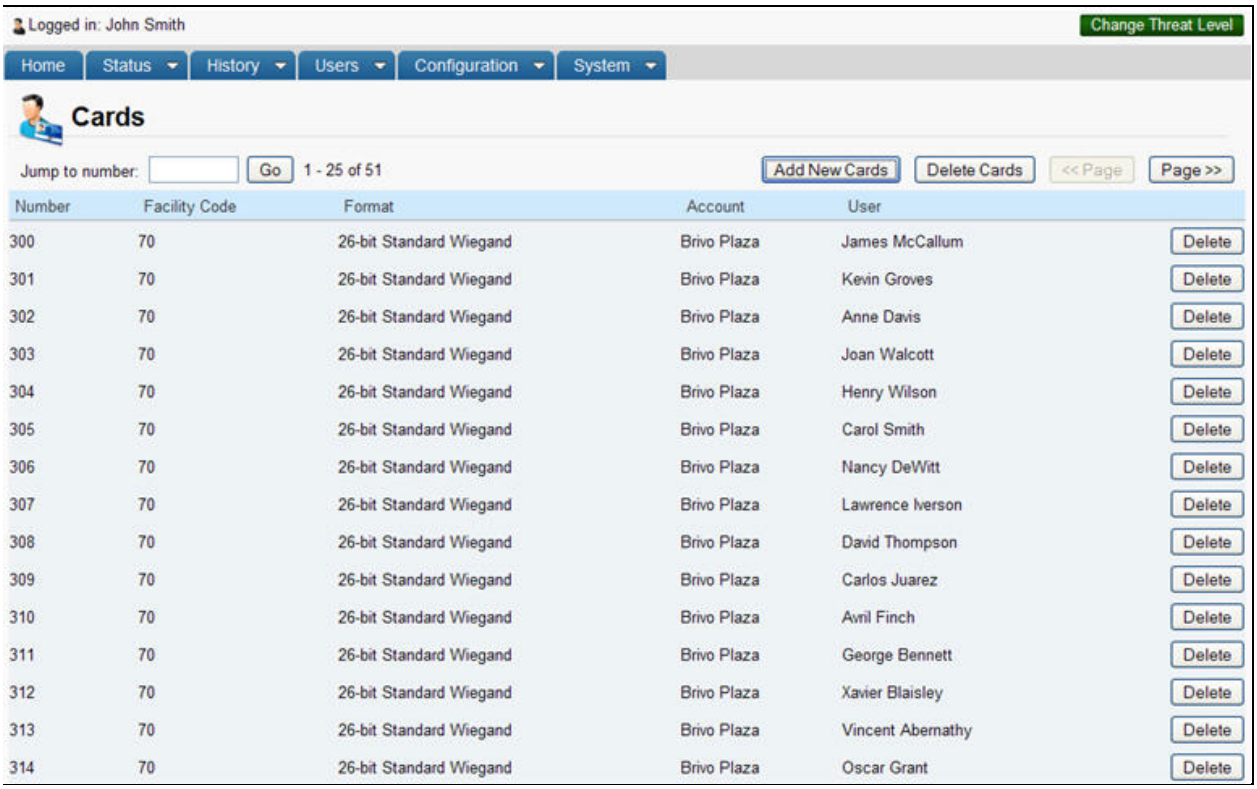


Figure 57. Viewing Cards List

Details displayed include:

- Number. The number displaying on the outside of the card
- Facility. This field is variable and may not appear for all card formats. The facility code assigned by the card manufacturer.
- Vendor/Agency. This field is variable and may not appear for all card formats. An embedded vendor/agency code for certain card formats that require this field.
- Format. The card format, for example "26-bit Standard Wiegand."
- Account. The account of the user to whom the card is assigned.

- User. The user to whom this card has been assigned, if any.

Administrators with appropriate permissions can:

Enter a number in the Jump to number field and click Go to jump to a specific point in the list of cards.

Click << Page to scroll backwards through the list of cards, or Page >> to scroll forward.

Click anywhere on a line with a defined User to access the corresponding User Details page. See *Users and Groups* for more information.

Click Add New Cards to define one or more new cards for the account.

Click Delete Cards to remove multiple cards from the account at one time.

Click the Delete button associated with any individual card to delete just that card.

	*NOTE:* *A card cannot be changed once it is created. If you add a card incorrectly, you must delete it and then re-add it to the account.*

Adding Cards

Administrators with appropriate permissions can add cards to the system.

There are two ways to add cards to your account. A set of cards can be added all at once by defining the first and last Internal Numbers for the set. For example, you can add 100 cards all at the same time by specifying the first card's Internal Number (e.g., 3000) and the last card's Internal Number (e.g., 3099). Administrators with appropriate permissions can add cards in this way. Alternatively, you can add individual cards on an as-needed basis through a process referred to as "swipe-to-enroll."

Procedures for both methods are described below.

To add one or more cards to the account:

1. Scroll over the Users link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Cards from the dropdown list. The Cards list displays.
3. Click Add New Cards. The Add Cards page displays.

Figure 58. Add New Cards

4. Click the appropriate Format on the drop-down list.
5. Enter the First External Number. The external number is the number printed on the card's surface. For example, card #200 will have "200" or "00200" printed on its corner. The external number is simply a reference to the card itself.

	NOTE: *The internal number and external number are often the same, in which case you only need to enter the external number. However, in some cases they are offset. For example, you can have a series of 100 cards in which the external numbers are 3001-3100 and the internal numbers are 5001-5100. When this happens you must enter both the first internal number as well as the corresponding external number.*

6. To add multiple cards at once, enter a Last External Number. A card is added for each number in the range defined by the first and last external numbers inclusively. If you enter a First External Number without also entering a Last External Number, then only a single card with the specified number is added.
7. Enter the First Card Number. The internal number is part of the card's embedded value. First Card Number is a required field only if the internal number is different from the external number.

	NOTE: *The maximum number of cards you can add at one time is 1000. In other words, the range defined by the first and last external numbers can be no greater than 1000.*

8. Enter the Facility Code if one came from the card manufacturer. Not all card formats have facility codes. In those cases, enter 0 for the facility code.
9. Click Save. You are returned to the Cards list with the new cards shown.

To add individual cards through swipe-to-enroll:

1. Using a card that has not yet been added to the Card Bank, swipe it through your card reader.
2. Scroll over the History link to view the System Activity log. The sub-navigation menu displays.
3. From the Activity link, click System Activity. The System Activity page displays, listing all activity events, including the unknown credential event just created. (See *Browsing the System Activity Log* for more information on the Activity Log.)
4. Click on the raw card value. The Add Card By Value page displays, with the Card Length and Card Internal Value fields filled in from the System Activity log entry.

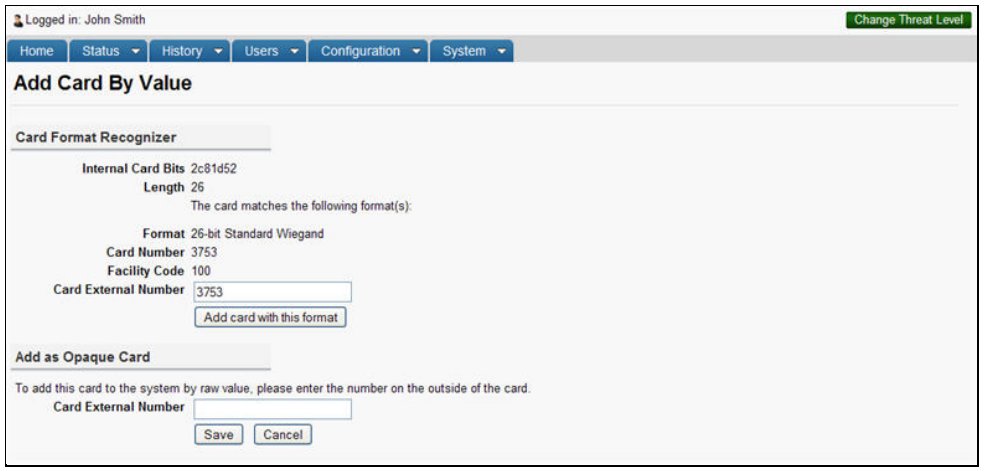


Figure 59. Add Card by Value

5. If the card is of a format recognized by the system, it will be listed as shown in Figure 53. If the format is unrecognized, the card can still be added as a simple opaque card. In either case, either the card's external number in the appropriate field.
6. Click Add Card with this Format to add as a known format, or simply click Save to add the card as an opaque. You are then returned to the Cards list with the new card shown.

	NOTE: *It is possible to add multiple cards with the same number. You may have cards with the same number but of different types. You may also have cards with the same number and of the same type, so long as the cards have different facility codes.*

Managing Card Formats

A pre-defined set of card formats is automatically generated when the System Account is first created. However, additional card formats can be defined by administrators with appropriate permissions.

	NOTE: *Administrators with appropriate permissions can edit or delete a card format until such time as a card with that format is added to the system.*

To view the list of card formats:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Cards link, click Card Formats from the dropdown list. The Card Formats list page displays.

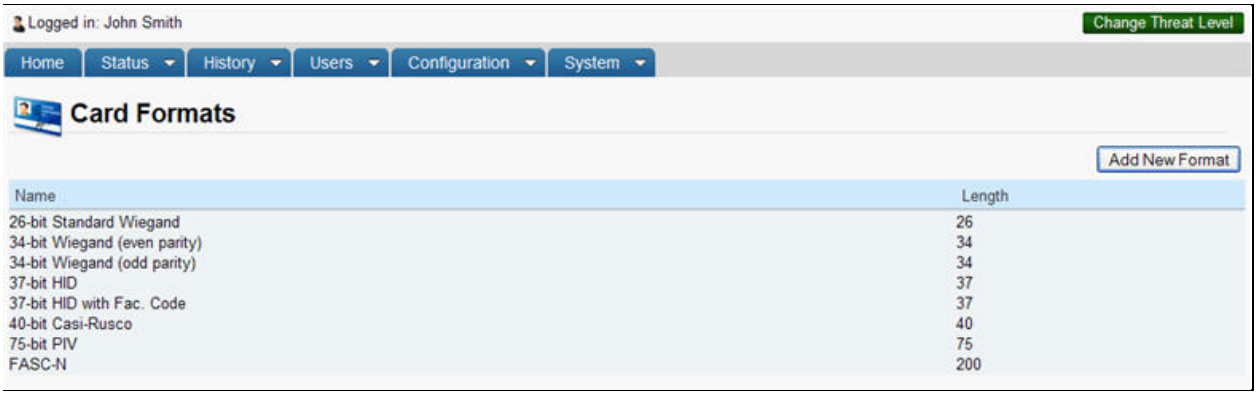


Figure 60. View Card Formats

Details displayed include:

- Name. The name assigned to the card format.
- Length. The number of bits in the card format.

Administrators with appropriate permissions can:

Click anywhere on a listed format to access the associated Card Format page.

Click Add New Format to add a new card format to the system.

To view the details for a specific card format:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Cards link, click Card Formats from the dropdown list. The Card Formats list displays.
3. Click the card format you want to view. The corresponding Card Format page displays.

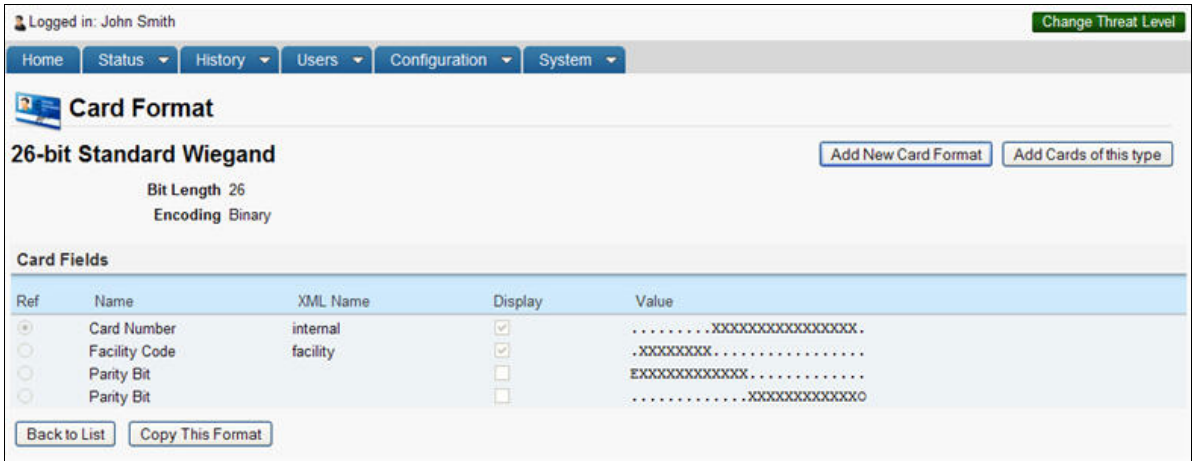


Figure 61. View Card Format Details

Details displayed may include some of the following:

- Bit Length. The length, in bit size, of the card format.
- Encoding. The style of encoding used on the card format.
- Card Number. The internal value that uniquely identifies the card.
- Facility Code. An internal value set at manufacturing to differentiate cards with the same external value.
- Agency Code. Some card formats have a hardwired set of bits unique to the card vendor, while other formats use an additional data field, depending on the format.
- Parity bit. Simple parity bit calculations are a common way to ensure the accuracy of the card read. This field provides space to inform the card engine how to calculate a single parity bit.
- Bit Mask. In some cases certain bits within a card should be ignored. Specifying a mask allows bits to be dropped out of incoming credentials of the same length as this format before being matched to the set of defined cards. Note that this causes a loss of information in creating card credentials, and should only be used if you fully understand the implications.
- Preset Value. Certain card formats that contain a "vendor bits" field or similar hardwired value that is present no matter what other fields exist on the card. This allows you to enter a template for values that will always be inserted into a card when encoded.

Administrators with appropriate permissions can:

Click Back to List to return to the Card Formats list.

Click Add New Card Format to add a new card format to the system.

Click Add Cards of this type to access the Add Cards page in order to add new cards of this type to the system.

Click Copy This Format to access the Edit Card Format page in order to create a new card format similar to the current one.

To create a new card format:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From Cards link, click Card Formats from the dropdown list. The Card Formats list displays.
3. Click Add New Format. The Edit Card Format page displays.

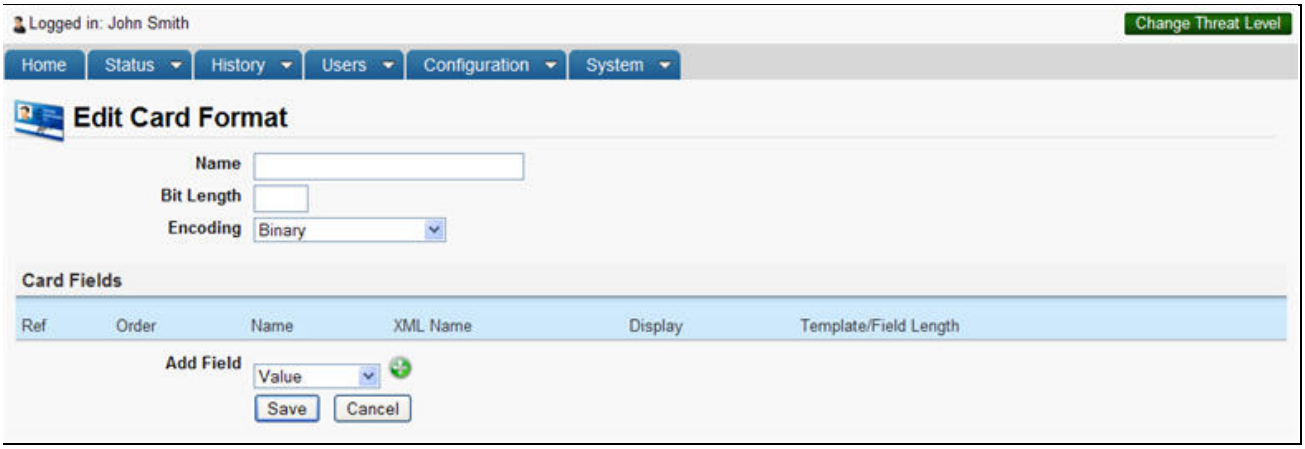


Figure 62. Create New Card Format

4. In the Name field enter a name for the new format. The name should indicate the bit length and the card maker. For example, 26-bit Standard Wiegand. This is a required field.
5. Enter the Bit Length, the number of bits in the card format. This is a required field.
6. Choose the appropriate Encoding from the dropdown list.
7. For the Card Fields, select the necessary fields from the dropdown list. Add and fill in the appropriate information.

	*NOTE:* *Some of the fields listed below may not appear when creating a new card format dependent upon factors like bit length or encoding style.*

8. The Value field is the usual field that is encoded into a card. For example, in the built-in 26 bit Wiegand format, the card number and facility code are both "value" fields in the format. Agency Code is also another example of a "value" field.
9. The XML Name field is a reference name used via the Brivo Datasync interface for creating cards of this format. Valid values only contain numbers, lower case letters, and _ (the underscore).
10. The Preset Value field is used for card formats that contain a "vendor bits" field or similar hardwired value that is present no matter what other fields exist on the card. This allows you to enter a template for values that will always be inserted into a card when encoded. This field is optional.
11. Bit Mask. This field is used to strip bits out of a card before processing. Masking is extremely dangerous and can result in seriously weakened security. The number of characters entered in this field must be the same as the bit length, and valid values include: . (period) to indicate a bit to strip out of the final card value, and X to indicate a bit to keep in the final card value. This field is optional.

12. Parity bit. The number of characters entered in each field must be the same as the bit length, and valid values include: . (period), to indicate bits ignored by this parity calculation, X to indicate a bit used by this parity calculation, and O and E to indicate the location of an Odd or Even parity bit. This field is optional.
13. Click Save. The Card Format page displays.

To copy a format from an existing format:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Cards link, click Card Formats from the dropdown list. The Card Formats list displays.
3. Click the format you want to use as the basis for the new card format. The associated Card Format page displays.

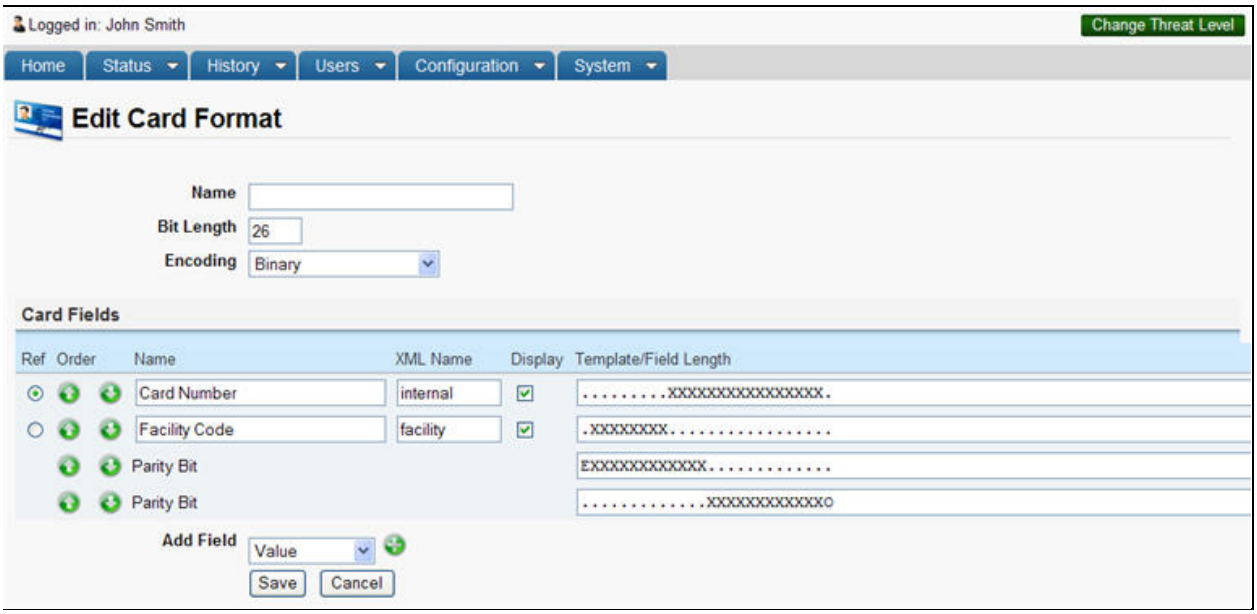


Figure 63. Copy Card Format

4. Click Copy This Format. The Edit Card Format page displays with all the fields filled in from the copied format. Only the Name field is blank.
5. Enter a unique Name for this new format. Do not use the same name as the format you copied.
6. Update the appropriate data fields according to the preceding guidelines for creating a new card format.
7. Click Save. The Card Format page displays.

To edit a card format:

1. Click the Configuration link. The sub-navigation menu displays.
2. From the Cards link, click Card Formats on the sidebar menu. The Card Formats page displays.
3. Click the format you want to edit. The associated Card Format page displays.
4. Click Edit. The Edit Card Format page displays.

	*NOTE:* *Only those card formats defined by an Administrator can be edited or deleted. The Edit and Delete buttons do not display on the Card Format page for system-defined card formats.*

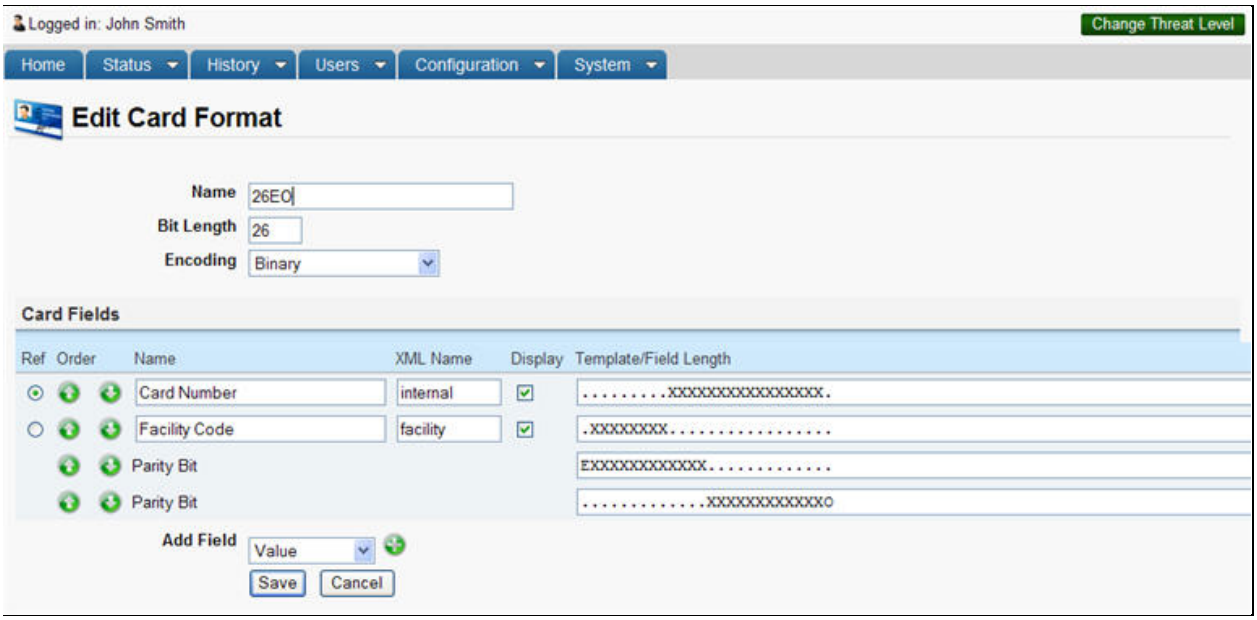


Figure 64. Edit Card Format

5. Update the appropriate data fields according to the preceding guidelines for creating a new card format.
6. Click Save. The Card Format page displays.

To delete a card format:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Cards link, click Card Formats from the dropdown list. The Card Formats list displays.
3. Click the format you want to delete. The associated Card Format page displays.

	*NOTE:* *Only those card formats defined by an Administrator can be edited or deleted. The Edit and Delete buttons do not display on the Edit Card Format page for system-defined card formats.*

4. Click Delete. A warning message indicates that by deleting this format you are also deleting all cards of this format, and that the operation cannot be undone.
5. Click OK. You are returned to the Card Formats page with the deleted format no longer listed.

Managing Card Assignments

Cards are assigned to users in order to provide them access to a facility. A card can be assigned when the user is first created, or it can be assigned at a later time. Likewise, it is possible to change a user's card assignment or delete it all together.

Card assignments are made on the Edit User page. See the section on *Creating a User* for guidelines on assigning a card when the user is first added to the account, or see the section on *Managing Users* for directions on adding, changing, or deleting a card assignment for an existing user.

Administrators with appropriate permissions can manage card assignments.

Managing Cards

Once created, a card cannot be edited. It can, however, be deleted from an account.

To delete a single card:

1. Scroll over the Users link. The sub-navigation menu displays.
2. Click Cards from the dropdown list. The Cards list displays.
3. Click Delete on the line of the card you want to delete. A warning message informs you that this operation cannot be undone.
4. Click OK in the confirmation prompt. You are returned to the Cards list with the deleted card removed. If the card had been assigned to a user, the assignment is removed.

To delete multiple cards:

1. Scroll over the Users link. The sub-navigation menu displays.
2. Click Cards from the dropdown list. The Cards list displays.
3. Click Delete Cards. The Delete Cards page displays.

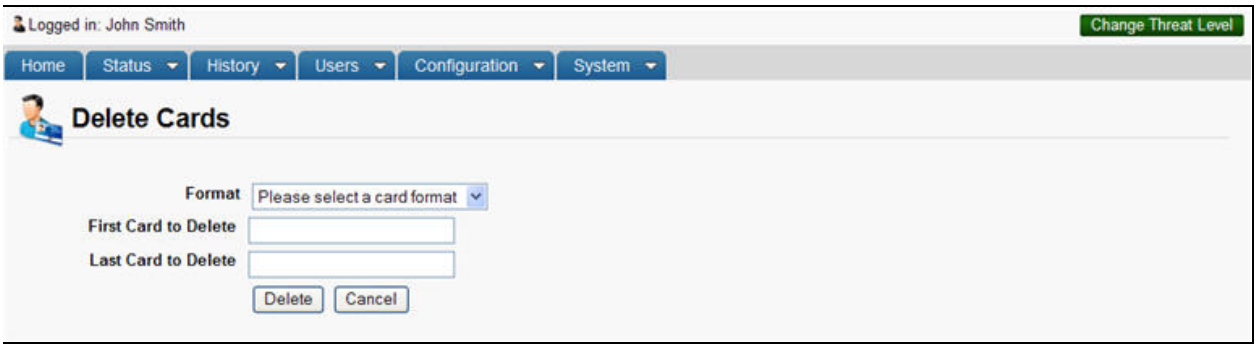


Figure 65. Delete Multiple Cards

4. From the drop-down list, click the Format of the cards you want to delete. This is a required field.
5. Enter the numbers of the First Card to Delete and the Last Card to Delete. These are both required fields.
6. Enter the Facility Code for the card range to be deleted.
7. Click Delete. A message asks you to confirm that you want to delete the specified cards.
8. Click OK. You are returned to the Cards list with the selected cards removed.

	NOTE: *If a card is lost, damaged or not returned, you can delete the card from the Card Bank. Deleted cards can be recreated if deemed appropriate.*

	NOTE: *If a user attempts to gain access to a door with a deleted card, the event will be logged as a* Failed Access Attempt: Unknown Card.

8. Badging

What are Badges?

Brivo Onsite Server's badging capability allows users to design custom badges with several options, including orientation of the badge, single or dual sided, customized background color and/or image, use of standard text objects (first name & last name; first name; last name) and custom text objects (such as Job Title), static text objects, user photo objects, static image objects, and custom image objects.

For more information regarding custom fields, see the section in *Users and Groups* on *Managing Custom Fields.*

Badge Templates

To create a badge template:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Cards link, click Badge Templates from the dropdown list. If there are preexisting badge templates, the page displays them.

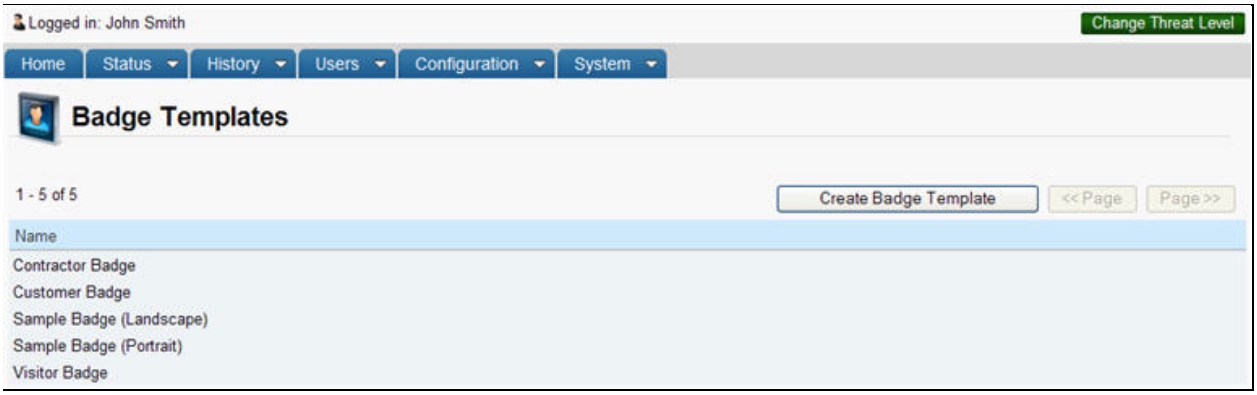


Figure 66. Create Badge Template

3. Click Create Badge Template. The Edit Badge Template page displays with an editable area for creating a badge template.
4. Under Template Properties, enter a name for the template you have created.
5. Select the orientation of the template from the dropdown list. The orientation of the card determines the scale of images and text objects.
6. Select whether or not the badge will be duplex (both sides) or not from the dropdown menu.
7. Select the Badge Size from the dropdown menu. The default is CR80.
8. The height and width (in inches) can be edited manually if that is required.

	*NOTE:* *Any changes made to the default settings can produce unexpected results if they are not supported by the printer driver.*

9. Choose from the list of items on the palette on the left and drag them to the open box in the middle to create your badge template.
10. Depending upon which items you dragged from the palette onto the badge template area, text will appear in the box next to the badge template area. Though the field may read "First Name", when the badge is actually created for a user, the user's actual first name will be entered into the field automatically.

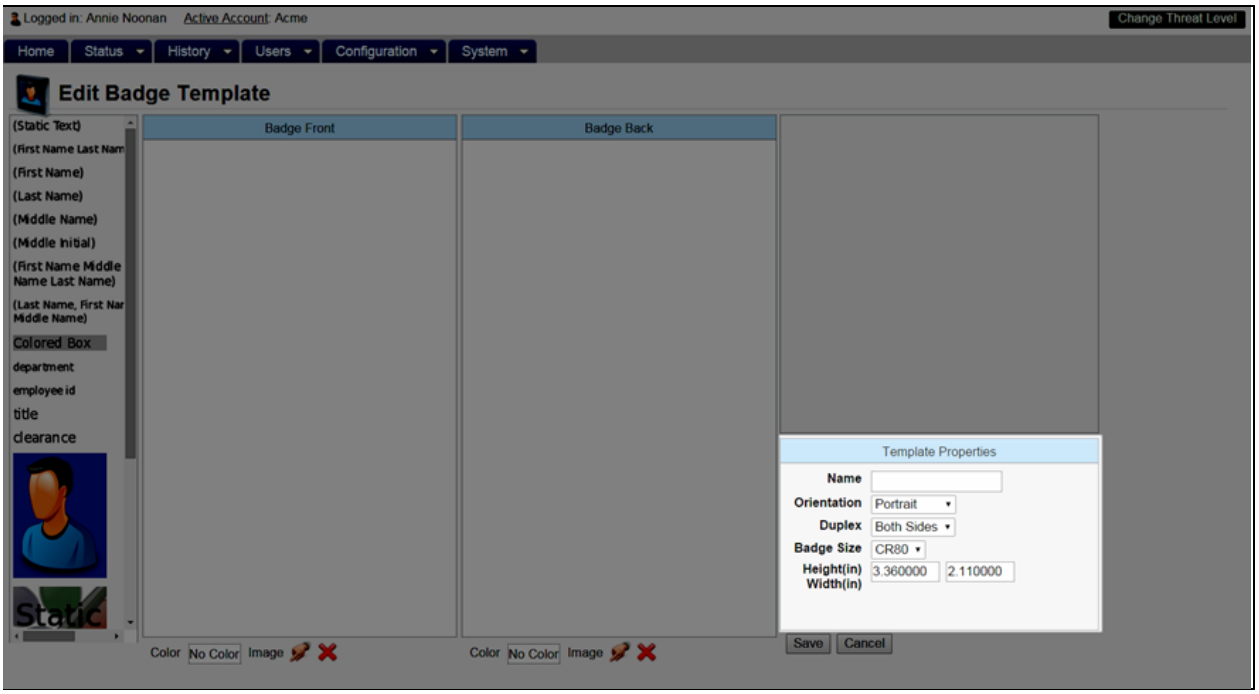


Figure 67. Template Properties

11. If you wish to select a background color for the badge, click No Color and a popup list will appear. Choose a color from the palette and click Save. To reject the color, click Cancel. For no color, select No Color.

12. To add an image as your background, click  to import an image. A popup window will appear. Select your image and click Upload. Click  to remove an image.

13. Once you have finished specifying the options for your template, select Apply to apply your options. If you wish to return to the default settings, click Revert. If you wish to delete the text box, click Delete.

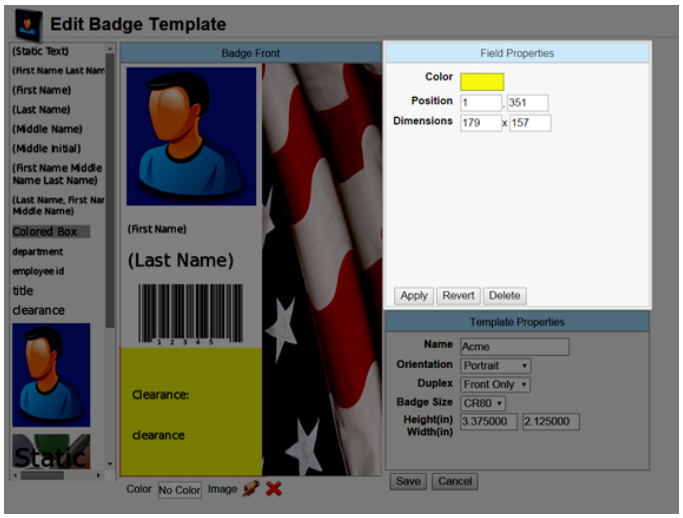


Figure 68. Field Properties

Badging options:

For Static Text Objects:

a) Drag the static text object from the palette to the editable box.

b) Specify the Text Properties:

a) Text: Enter the desired text in the static text field.

b) Color: Choose a color for the static text from the pop up color box. To keep the selected color, click Save. To cancel the selection, click Cancel. For no color, click No Color.

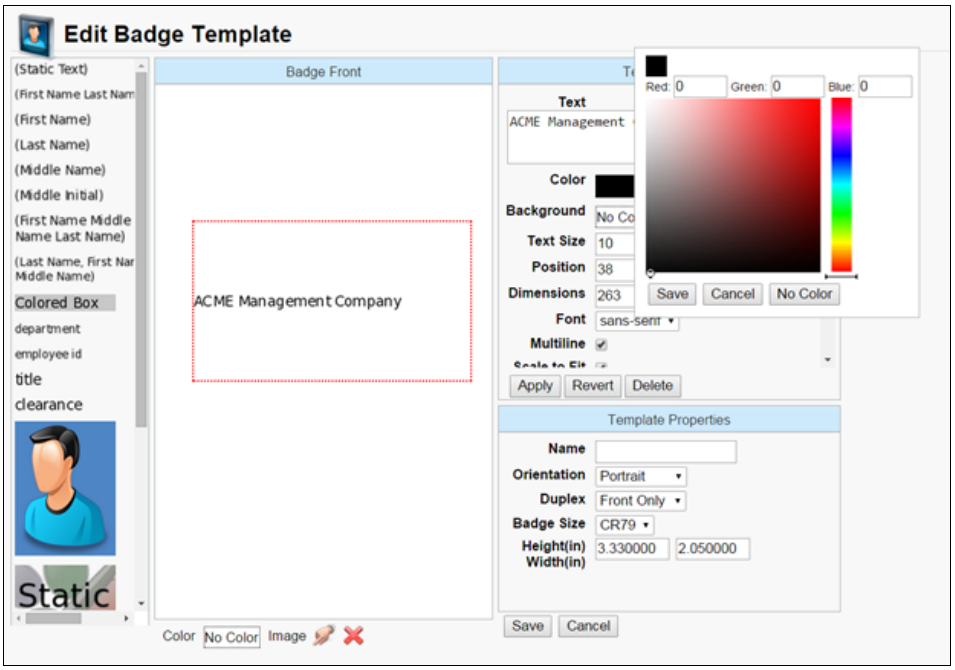


Figure 69. Choose Color

c) Background: Click on the Background field and select a background color for the text field. To accept the color you have selected, click Save. To reject the color, click Cancel. For no color, select No Color.

d) Text Size: Enter the desired font size for the text in the Size field, or click on a corner of the text box and drag to enlarge.

	NOTE: *Because of scaling and other factors, the font size may or may not correspond to the font point size.*

e) Position: You may either manually enter the position where you'd like the text, or you can simply drag the text to the desired area of the template.

f) Dimensions: You may either manually enter the desired dimensions for the text, or you can simply click on a corner of the text box and drag to increase or decrease the dimensions.

g) Font: select a font for the text from the dropdown list.

h) Multiline: Check the Multiline box if you wish to split the text across more than one line. If left unchecked, the text is only broken across multiple lines if a new line is embedded.

i) Scale to Fit: Check the Scale to Fit box if you wish for the text to correspond with the size of the box.

j) Alignment: Select the alignment from the dropdown list for the text.

k) Vertical Placement: Select the placement from the dropdown list for the text or image.

l) Orientation: Select the orientation of the text from the dropdown list.

For Standard Text Objects:

1. Drag a standard text icon from the palette to the editable box.

Figure 70. Examples of Standard Text Objects

2. Specify the Text Properties:

i. Color: Click on the Color field and select a color for the text.

ii. Background: Click on the Background field and select a background color for the text field. To accept the color you have selected, click Save. To reject the color, click Cancel. For no color, select No Color.

iii. Text Size: Enter the desired font size for the text in the Size field, or click on a corner of the text box and drag to enlarge.

iv. Position: You may either manually enter the position where you'd like the text, or you can simply drag the text to the desired area of the template.

v. Dimensions: You may either manually enter the desired dimensions for the text, or you can simply click on a corner of the text box and drag to increase or decrease the dimensions.

vi. Font: select a font for the text from the dropdown list.

vii. Multiline: Check the Multiline box if you wish to split the text across more than one line. If left unchecked, the text is only broken across multiple lines if a new line is embedded.

viii. Scale to Fit: Check the Scale to Fit box if you wish for the text to correspond with the size of the box.

ix. Alignment: Select the alignment from the dropdown list for the text.

x. Vertical Placement: Select the placement from the dropdown list for the text or image.

xi. Orientation: Select the orientation of the text from the dropdown list.

3. Once you have finished specifying the options for the text field, select Apply to apply your options. If you wish to return to the default settings, click Revert. If you wish to delete the text box, click Delete.

For User Photo Objects:

1. Drag the standard image icon from the palette to the editable box.

Figure 71. User Photo Icon

2. Specify the Image Properties:

   i. Position: You may either manually enter the position where you'd like the image, or you can simply drag the image to the desired area of the template.

   ii. Dimensions: You may either manually enter the desired dimensions for the image, or you can simply click on a corner of the image box and drag to increase or decrease the dimensions.

   iii. Background: Click on the Background field and select a background color for the image. Background color will only be available if there is enough room after the image is resized. To accept the color you have selected, click Save. To reject the color, click Cancel. For no color, select No Color.

   iv. Keep Aspect: Check the Keep Aspect box if you wish to resize the image as large as possible without distorting the image.

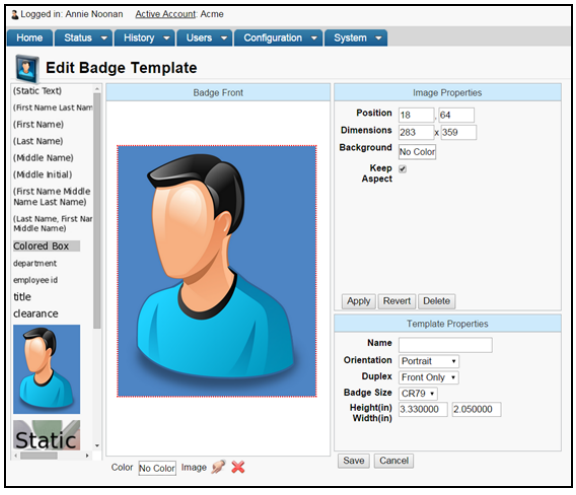


Figure 72. User Photo Properties

3. Once you have finished specifying the options for the image field, select Apply to apply your options. If you wish to return to the default settings, click Revert. If you wish to delete the user photo, click Delete.

For Static Image Objects:

1. Drag the Static Image icon from the palette to the editable box.

Figure 73. Static Image Icon

2. Specify the Image Properties:
   i. Filename: To import an image file, click Browse and select the file you wish to import.
   ii. Position: You may either manually enter the position where you'd like the image, or you can simply drag the image to the desired area of the template.
   iii. Dimensions: You may either manually enter the desired dimensions for the image, or you can simply click on a corner of the image box and drag to increase or decrease the dimensions.
   iv. Background: Click on the Background field and select a background color for the image and click Save. Background color will only be available if there is enough room after the image is resized.
   v. Keep Aspect: Check the Keep Aspect box if you wish to resize the image as large as possible without distorting the image.

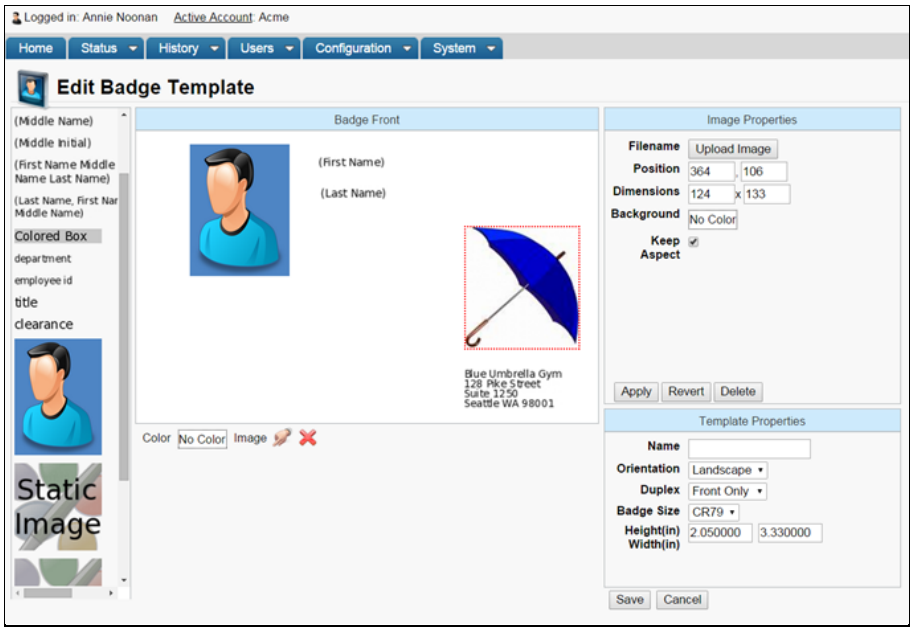


Figure 74. Static Image Properties

3. Once you have finished specifying the options for the image field, select Apply to apply your options. If you wish to return to the default settings, click Revert. If you wish to delete the static image, click Delete.

For Colored Boxes:

1. Drag the colored box icon from the palette to the editable box.
2. Select a color from the pop up list next to the Color field. To accept the color you have selected, click Save. To reject the color, click Cancel. For no color, select No Color.

For Barcodes:

1. Drag the barcode icon from the palette to the editable box.
2. Select the Barcode Properties.
   i. Encoding: Select a code style from the dropdown list.
   ii. Custom Field: If you wish to include a custom field along with your barcode, select one from the dropdown list.
   iii. Position: You may either manually enter the position where you'd like the image, or you can simply drag the image to the desired area of the template.
   iv. Dimensions: You may either manually enter the desired dimensions for the image, or you can simply click on a corner of the image box and drag to increase or decrease the dimensions.
   v. Orientation: Select the orientation of the text from the dropdown list.
   vi. Generate Checksum: Select this box to generate a number to verify that the barcode matches the code specified in the user's file.
   vii. Show Numbers: Check this box if you want numbers to be shown on the barcode.
3. Once you have finished specifying the options for the barcode field, select Apply to apply your options. If you wish to return to the default settings, click Revert. If you wish to delete the barcode, click Delete.

	***NOTE:*** *Because different barcodes specify particular formats, a red "X" may appear in the barcode field if the properties have not been entered correctly.*

To edit a badge template:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Cards link, click Badge Templates from the dropdown list. The Badge Templates list displays.
3. Choose from the list of templates the badge you would like to edit.
4. The "Badge Template Details" page displays. Click Edit.
5. When you are finished making changes to the badge template, click Save.

To print a badge:

1. Scroll over the Users link. The sub-navigation menu displays.
2. Click Users from the dropdown list. The Users list displays.
3. Choose from the list of users for whom you wish to print a badge.
4. The "User Details" page displays. Select Print Badge from the More Operations dropdown menu.
5. The "Print Badge" page displays. Select a previously created badge template from the dropdown list. The template is applied to the user's information.

Figure 75. Print Preview

Figure 76. Print Badge

6. Click Print Preview. The Print Preview page displays. If the badge is acceptable, click Print and the badge prints via your default printer.

	NOTE: *The badge printer must have dual sided printing enabled to print any two sided badges. If not enabled, the printer may not print properly. Some printers do not carry the settings from one print job to the next. Be sure to check any printer specific settings prior to printing a badge.*

To delete a badge template:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Cards link, click Badge Templates from the dropdown list. The Badge Templates list displays.
3. Click "Badge Templates." Choose the badge you would like to delete from the list of templates.
4. The "Badge Template Details" page displays. Click Delete. A warning pops up advising you that the action you are about to complete cannot be undone. Click Ok to proceed. The badge has successfully been deleted.

9. Accounts

What is an Account?

An *account* is essentially a "span of control." With the Brivo Onsite Server family of applications, there is usually only one account: the System Account. This is the account that manages the overall facility at which the system is installed. The control of all doors, exterior and interior, as well as all devices, is managed by this one account.

If sections of the facility are leased out, then there may also be one or more Tenant Accounts in addition to the System Account. In cases such as this, the System Account is used to manage the overall facility, such as access to lobby doors or a cafeteria. Tenant Accounts, on the other hand, are used to manage the access of user groups associated with the tenant organization.

NOTE:

Administration permissions to sub-accounts are controlled by the role-based administration settings. Roles can be granted permissions to sub-accounts, so system account administrators can be given as restricted as needed set of capabilities in sub-accounts.

Defining the Initial System Account Administrator

An Administrator with full permissions must be defined for the System Account before any other data is entered. When you first log in to the System Account, you are automatically taken to the Welcome page and prompted to create a System Account Administrator.

To log in for the first time:

1. In your web browser, enter the address for the Brivo Onsite Server.
2. The Log In page displays.

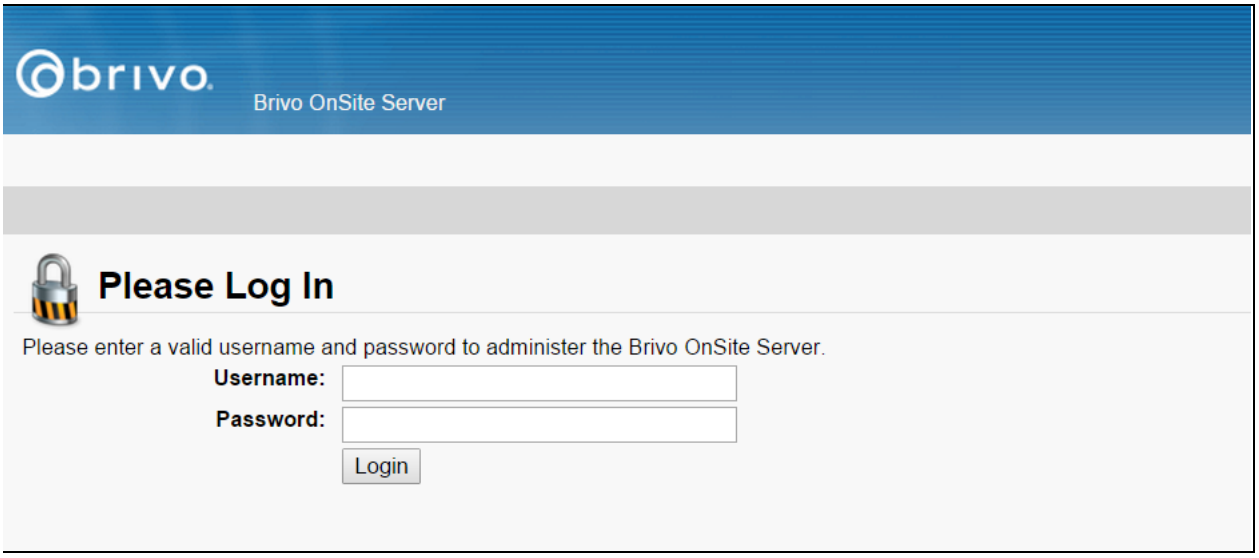


Figure 77. Log In

3. In the Username field, enter admin.
4. Leave the Password field blank.
5. Click Login. The Welcome page displays.

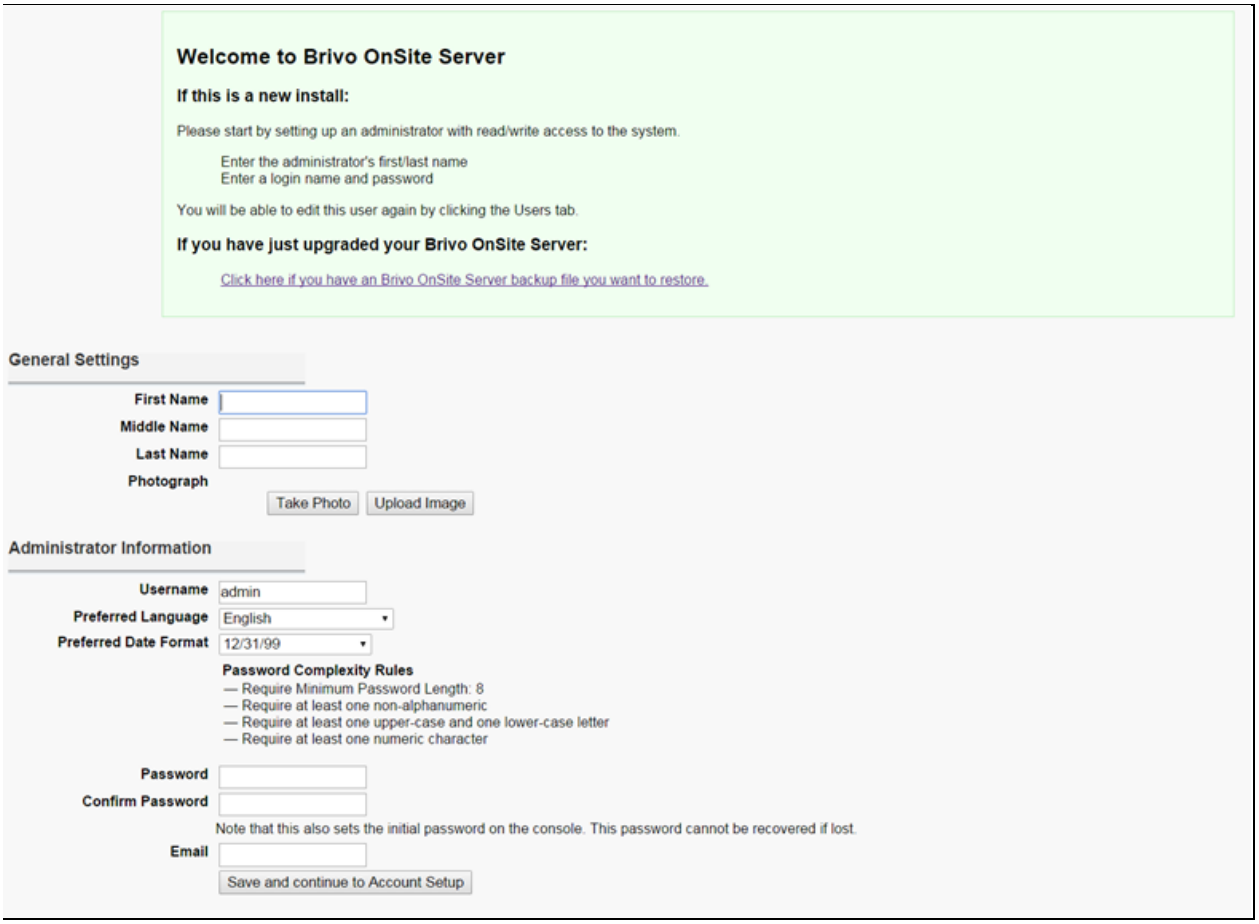


Figure 78. System Account Administrator Creation Page

To define the initial System Account Administrator

1. In the First Name, Middle Name and Last Name fields enter the first, middle, and last names of the Administrator for the System Account. The first name and last name are required fields.
2. If you want a photograph linked to this administrator, you may click on either the Take Photo button to use a webcam or the Upload Image to upload an already existing image.
3. The Username defaults to admin. For security reasons, you may want to change the Username of the System Account Administrator, but you are not required to do so.
4. Select a Preferred Language from the dropdown list.
5. Select a Preferred Date Format from the dropdown list.
6. In the Password field, enter a password for the Administrator. Re-enter the exact same password in the Confirm Password field. Both of these fields are required.
7. Select an Email for the System Account Administrator.

	NOTE: *The password that is set on this first page is used to control access to the console configuration for the Brivo Onsite Server. After setting up your initial Administrator, you will need to use that password with the username 'admin' to log into the console. The password may then be changed from the console if necessary.* *Do not lose this password, or you will not be able to log into the console interface in the future without it.*

	NOTE: *The Username and Password fields are required for all Administrators. The username and password combination determine the Administrator's access to the Brivo Onsite Server application, and must be entered the next time the Administrator logs in.*

8. Click Save and continue to Account Setup. The Edit Account Details page displays.

To set up the System Account:

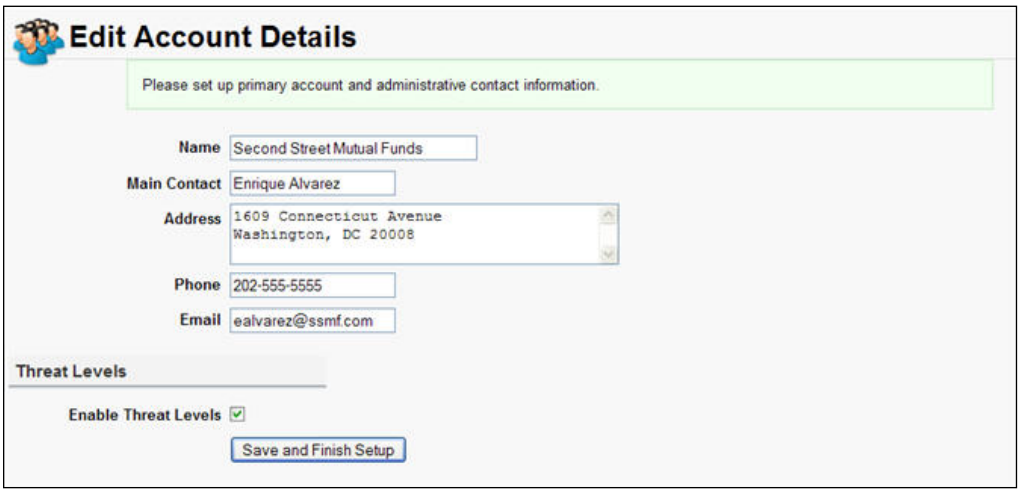


Figure 79. Set up System Account

1. After defining a System Account Administrator, you are prompted to name the System Account and identify a main contact for it. Other than Name, all of the fields on this page are optional.
2. Enter the Name for the System Account. If the facility is occupied by a single business, you probably want to use the name of that business. If the facility has more than one tenant, you may want to use the building name, the building address, or the landlord's name.
3. Enter the Main Contact for the System Account. This is the person primarily responsible for the operation of the Brivo Onsite Server at this facility. For Tenant Accounts, the main contact is the person who deals with the System Account management company.

4. Enter the complete Address for the main contact. The format of this address will vary depending on the location of the facility. For example, in the United States the address should include a street number and name on line, possibly a suite or office number on the second line, and the city, state and zip code on the last line.
5. Enter the complete Phone number for the main contact. The format of the phone number will vary depending on the location of the facility. For example, in the United States the phone number should include a 3-digit area code, a 7-digit number, and possibly an extension.
6. Enter an Email address for the main contact.
7. Enable Threat Level functionality. Check the "Enable Threat Levels" to be able to use Threat Level functionality.
8. Click Save and Finish Setup. The System Activity page displays. You are now ready to begin configuring the system. See the section on *System Management.*

Viewing Account Details

Administrators with appropriate permissions can view basic account information on the Account Details page. This overview displays contact information for the account as well as a list of Administrators and devices defined for the account.

To view details for a specific account:

1. Scroll over the Configuration link at the top of any page. The sub-navigation menu displays.
2. From the Account link, click Account Details. The Account Details page displays.

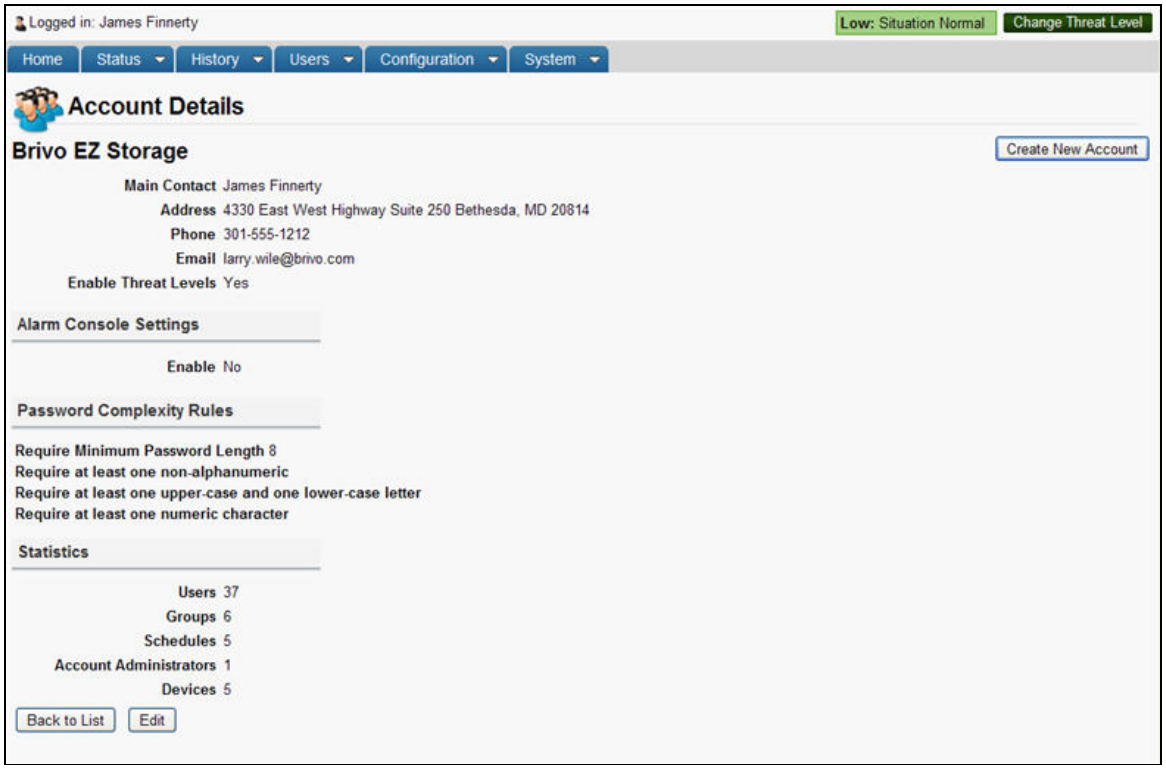


Figure 80. View Account Details

Details displayed include:

- Main Contact. The name of the person primarily responsible for the operation of the system at this facility
- Address. The complete mailing address for the main contact for the account.
- Phone. The phone number(s) for the main contact.
- Email. The email address for the main contact.
- Enable Threat Levels. Whether or not the account has Threat Level functionality enabled.
- Alarm Console Settings. Whether or not this account has Alarm Console functionality enabled, and if enabled, when alarms are active, any alarm priorities that have been set, and if alarms are linked to specific threat levels.
- Alarm for Control Panels. Whether or not there are any alarm texts for control panel alarm events and what the alarm priority is for those events.
- Password Complexity Rules. Whether or not the password rules for the account will follow:

- A minimum password length (the default is 8 characters).
- Requiring at least one non-alphanumeric character.
- Requiring at least one upper-case and one lower-case letter.
- Requiring at least one numeric character.

- Statistics. Shows the number of Users, Groups, Schedules, Account Administrators, and Devices for the selected account.

NOTE:

Administrator status is assigned to a user on the Administrators page. See Creating an Administrator for more information.

NOTE:

Doors and devices are defined in the Devices section. See the section on Managing Devices *for more information.*

Administrators with appropriate permissions can:

Click Back to List to return to the Accounts list.

Click Create New Account to access a blank Edit Account Details page in order to create a new Tenant Account.

Click Edit to access the Edit Account Details page associated with this account.

Creating Tenant Accounts

By default, the account you create when you first log in is automatically defined as the System Account. All subsequent accounts are automatically defined as Tenant Accounts.

Only Administrators with appropriate permissions can create new Tenant Accounts.

To create a Tenant Account:

1. Scroll over the Configuration link at the top of any page. The sub-navigation menu displays.
2. From the Account link, click Account Details. The Account Details page displays.
3. Click Create New Account. The Edit Account Details page displays with blank fields.

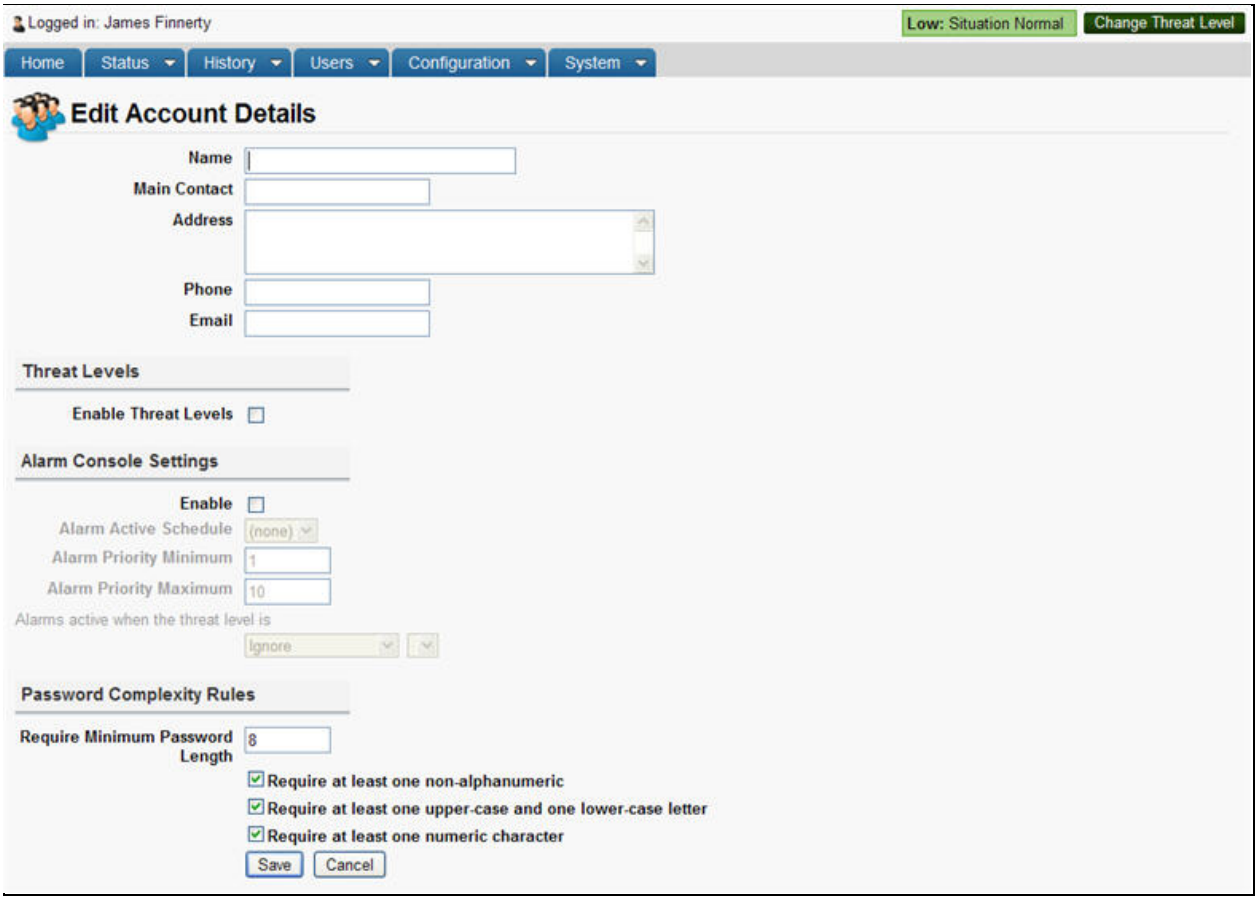


Figure 81. Create Tenant Account

4. In the Name field enter a descriptive name for the account, such as the name of the business. This is the only required field on this page
5. In the Main Contact field enter the name of the person primarily responsible for managing the interface for this account.
6. In the Address field enter the complete address for the person identified as the main contact. The format of this address will vary depending on the country in which the account is located. For example, in the United States the address should include the street number and name, office number, city, state, and zip code.

7. In the Phone field enter the complete phone number for the person identified as the main contact. As with the address, the format of the phone number will depend on the country. In the United States, this field would contain a three-digit area code, a seven-digit number, and possibly an extension.
8. In the Email field enter the email address for the main contact.
9. Enable Threat Level functionality for the account. Check the "Enable Threat Levels" to be able to use threat levels on the tenant account.
10. Enable Alarm Console Settings functionality for the account. Check the "Enable" checkbox to set scheduling, priority, and threat level functionality.
11. In the Password Complexity Rules section, enter the required minimum password length, and whether or not the password will require non-alphanumeric, upper-case and lower-case, and/or numeric characters.
12. Click Save. At the top of the page, the active account displays. To change the active account, click on the Active Account link and select the new Active Account from the list.

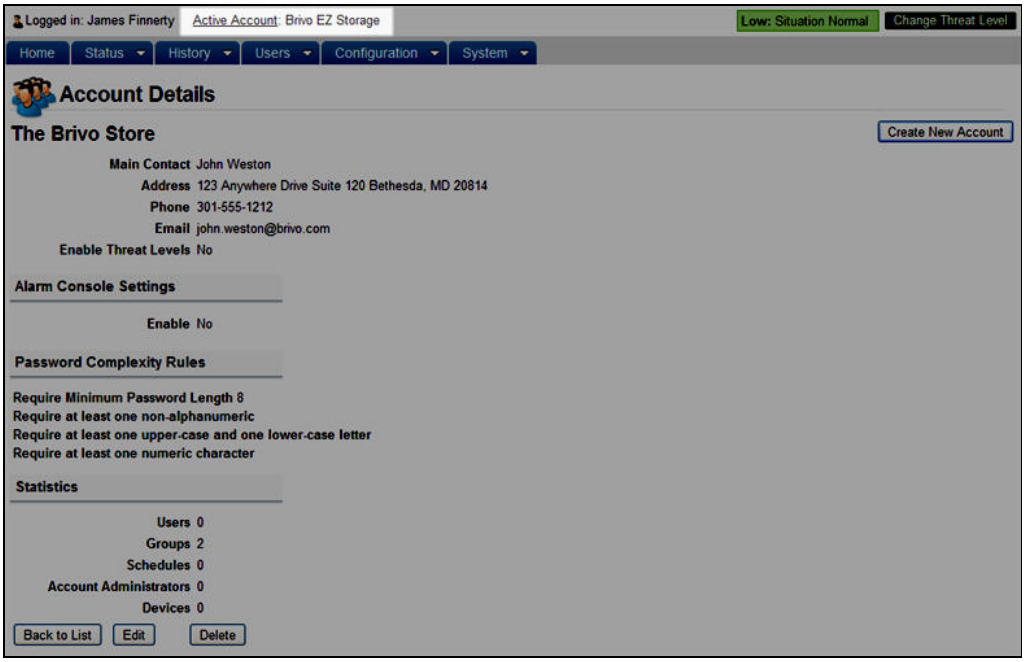


Figure 82. View Active Account

	NOTE: You now have a multi-account setup. See Tenant Accounts for guidelines on managing these accounts.

13. If you choose not to assign an Administrator to the new account, you can:
    - Click Create New Account to create another Tenant Account without first assigning an Administrator to this one. You can always assign an Administrator at a later time.

- Click Back to List to return to the Accounts list without first assigning an Administrator to this account. You can always assign an Administrator at a later time.
- Click Edit to access the Edit Account Details page to make changes to this account before first assigning an Administrator.
- Click Delete to remove the account from the system.

	*NOTE:* *If there are no Administrators with permissions to a Tenant Account, the tenant will not be able to log in to the account, and the account will remain under the complete control of the System Account until an Administrator is assigned.*

Managing Account Contact Information

Once an account is created, all contact information can be edited by any Account Administrator with appropriate permissions.

To edit account contact information:

1. Scroll over the Configuration link at the top of any page. The sub-navigation menu displays.
2. From the Account link, click Account Details. The Account Details page displays.
3. Click Edit. The Edit Account Details page displays.

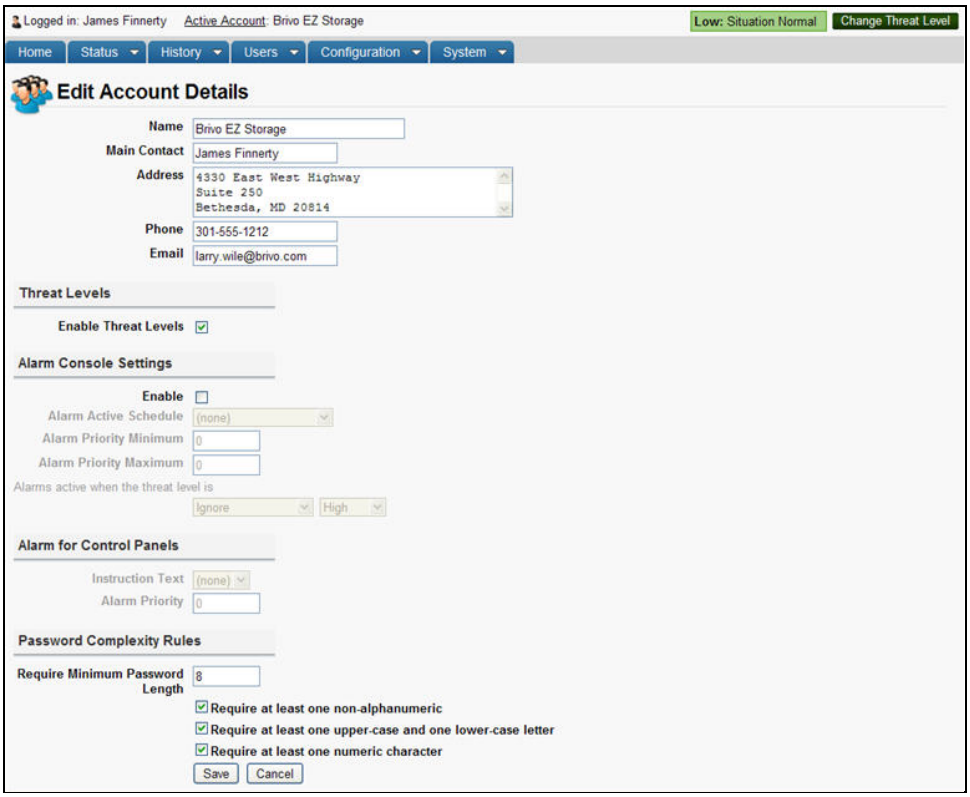


Figure 83. Edit Account Details

4. You can change the account Name, but you cannot delete it. This is the only required field on this page.
5. Update the remaining fields according to the procedures for creating tenant accounts.
6. Enable Threat Levels functionality for the account. If you choose to allow the account to be able to use Threat Levels, click the "Enable Threat Levels" box.
7. Enable Alarm Console Settings for the account. If you choose to allow the account to use Alarm Console Settings, click the "Enable" box.
8. Edit Password Complexity Rules for the account as needed.
9. Click Save. You are returned to the Account Details page with the updated information displayed.

10. Email Notifications

What are Email Notifications?

An *email notification* is an email message that corresponds to an Access Event (such as when a member of the group "Janitors" enters the "Main Office"), an Exception Event (such as when the "Front Door" is ajar for three minutes), a Device Event (such as when a motion sensor engages), or a Control Panel Event (such as when the control panel loses AC power).

Email notifications are sent to specific people under specific circumstances according to a set of notification rules that state those *who* should be notified about *what* events. Notifications are formatted in plain text. The time that the notification displays when it is sent corresponds with the time zone configured for the appliance. For more information on configuring control panels, see *Update and/or Configure a Control Panel.*

In order to use the Email Notification function in Brivo Onsite Server, you must first configure your SMTP Server. See the section on *Configuring the SMTP Server* for more information.

Browsing the Notifications List

Administrators with appropriate permissions can view, create, edit and delete notification rules.

To view the Notifications list for a specific account:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Account link, click Email Notifications. The Email Notifications page displays.
3. Click Email Notifications on the sidebar menu. The Email Notifications page displays.

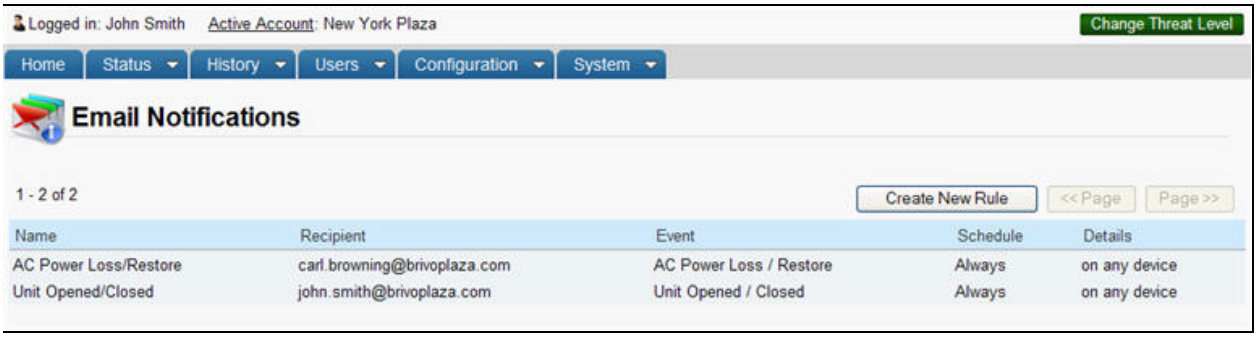


Figure 84. View Email Notifications List

Details displayed include:

- Name. The name assigned to the notification rule.
- Recipient. The email address for the individual that will receive the notification.
- Event. The event that, when it occurs, causes the email notification to be sent.
- Schedule. The schedule associated with the notification rule. See the section on *Schedules and Holidays* for more information.
- Details. The specific door or device at which the event occurred.

Administrators with appropriate permissions can:

Click Create New Rule to access a blank Edit Notification page in order to create a new notification rule.

Click anywhere on the line for a specific rule to access the associated Edit Notification page.

Creating Notification Rules

Administrators with appropriate permissions can create notification rules.

To create a notification rule:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Account link, click Email Notifications. The Email Notifications page displays.
3. Click Create New Rule. The Edit Notification page displays with all the fields blank.

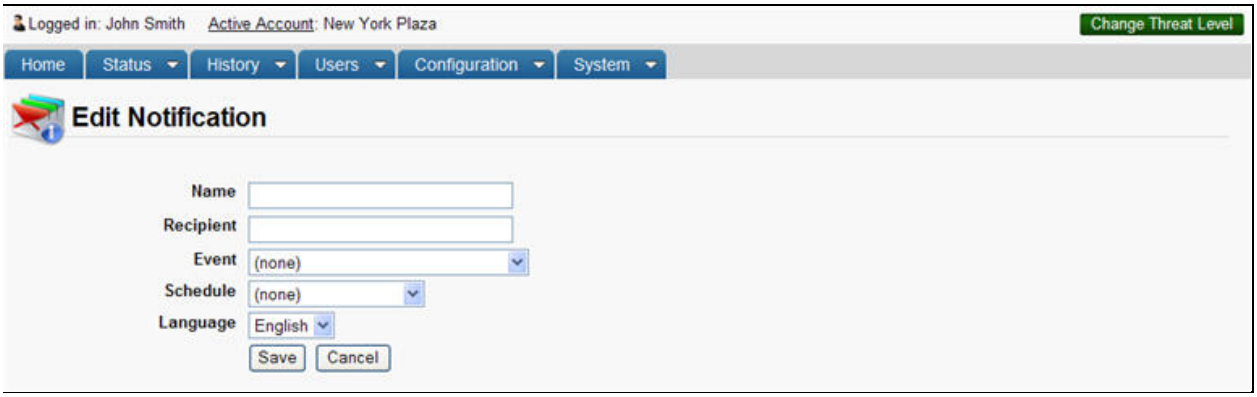


Figure 85. Create Notification Rule

4. Enter a brief, descriptive Name for the rule, such as "Lobby Door Ajar."
5. In the Recipient field, enter the email address of the individual to receive the email notification. Enter only one email address in this field.
6. From the drop-down list, select the Event for which you want a notification sent.
7. From the drop-down list, select the Schedule according to which you wish to monitor this event. The notification rule will only trigger the sending of an email if the specified event happens during an active block in the given schedule.
8. For some event types, you will need to specify a Device, a User, or a Group.
9. From the Language drop-down list select a language for the email message.
10. Click Save. The Email Notifications page displays with the new rule listed. From this point forward, each time the selected event occurs during the schedule selected, the specified recipient will receive an email notification.

Managing Notification Rules

Notification rules can be edited or deleted at any time by administrators with appropriate permissions.

To edit a notification rule:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Account link, click Email Notifications. The Email Notifications page displays.
3. Click anywhere on the line of information for the rule you want to edit. The corresponding Edit Notification page displays.

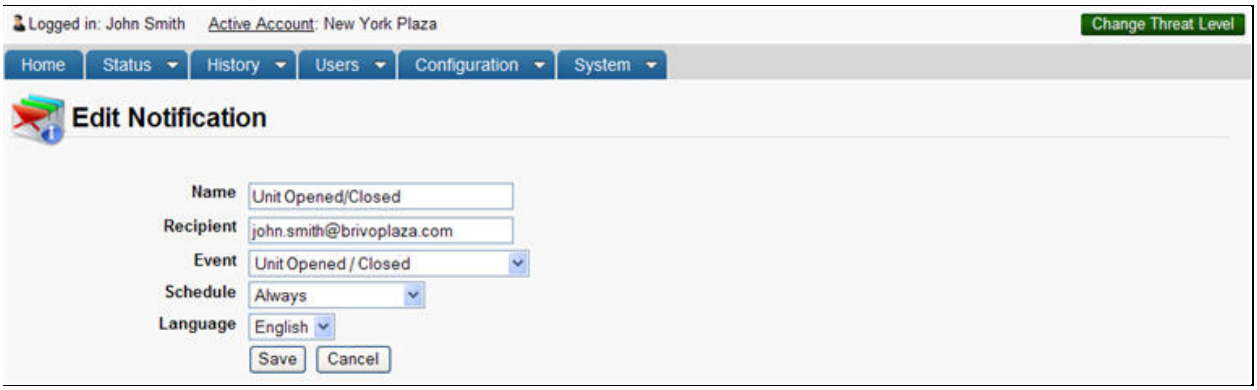


Figure 86. Edit Email Notification Rule

4. Update the fields according to the guidelines provided for creating notification rules.
5. Click Save. You are returned to the Email Notifications list with the updated information displayed.

To delete a rule:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Account link, click Email Notifications. The Email Notifications page displays.
3. Click the name of the notification rule you wish to delete. The corresponding Notification Details page displays.
4. Click Delete This Rule. The Notifications page displays and the deleted rule is no longer listed. The rule is removed from the system and will no longer cause email messages to be sent.

Sample Email Notifications

Following are several sample email notification messages. Please see the section on *Index of Events* for more information.

Access by User

Subject: Valid Credential Presented
To: jack@acme.com

Valid Credential Presented
When: Mon Mar 20 06:32:53 2006
Device: Acme Megaplex Front Door
User: Emily Bennett

Door Ajar

Subject: Door left ajar
To: jamie@acme.com

Door left ajar
When: Tue Mar 21 18:02:06 2006
Device: Acme Megaplex Front Door

Door Forced Open

Subject: Door forced open
To: jamie@acme.com

Door forced open
When: Tue Mar 21 18:00:06 2006
Device: Acme Megaplex Front Door

Locked or Unlocked on Schedule

Subject: Unlocked on schedule
To: jack@acme.com

Unlocked on schedule
When: Mon Mar 20 09:00:00 2006
Device: Acme Megaplex Front Door

Failed Access by Unknown Person (Unknown card)

Subject: Failed access attempt: Unknown card
To: bobby@acme.com

Failed access attempt: Unknown card
When: Thu Mar 23 07:17:05 2006
Device: Acme Megaplex Front Door

Failed Access by Known User (Unassigned or revoked card)

Subject: Failed access attempt: Unassigned or revoked card
To: bobby@acme.com

Failed access attempt: Unassigned or revoked card
When: Thu Mar 23 20:17:05 2006
Device: Acme Megaplex Front Door

11. Administrators and Administrator Roles

Administrators are people with access to Brivo Onsite Server, the web-based interface. These permissions are defined by the administrator roles feature, which details very specifically what sections of the interface an administrator has access to as well as what processes an administrator is allowed to use.

The creation of the first administrator, or System Administrator, is detailed in the previous chapter.

To view current administrators:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Account link, select Administrators. The Administrators List page displays.

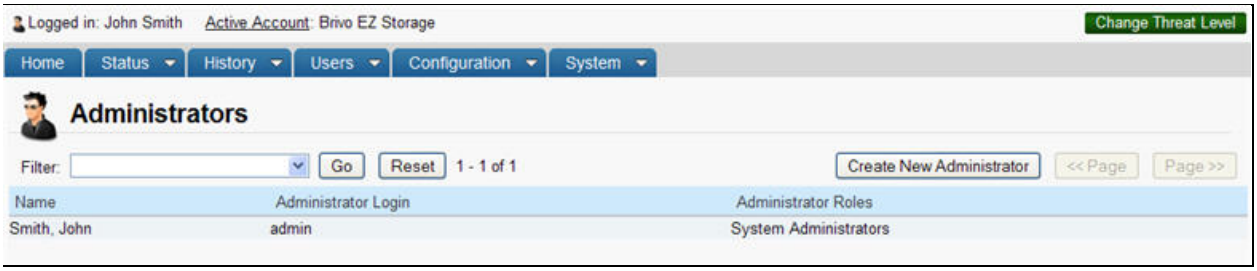


Figure 87. View Current Administrators

To create a new administrator:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Account link, select Administrators. The Administrators List page displays.
3. Click on the Create New Administrator button.

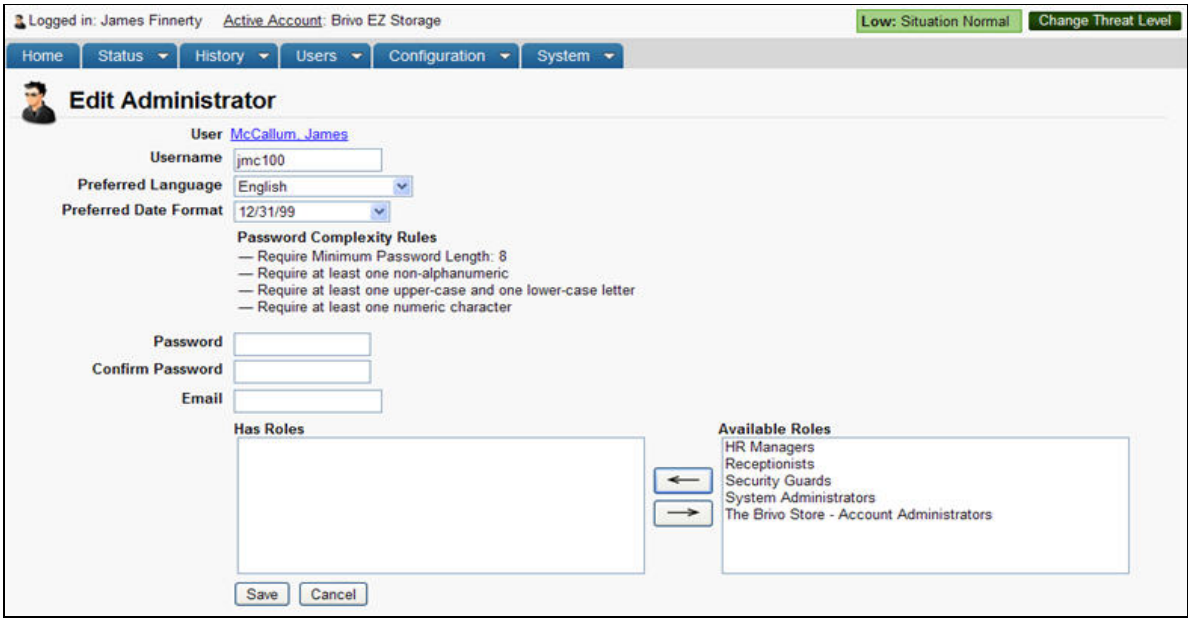


Figure 88. Create New Administrator

4. Click on the User link. The Select User popup window will appear. Select the user to link to this administrator or click the None (Leave selection blank) button. If you click the None (Leave selection blank) button, you are not able to save the administrator.
5. Select a Username for this administrator.
6. Select a Preferred Language from the dropdown list.

7. Select a Preferred Date Format from the dropdown list.
8. Select a Password for the new administrator and enter it again in the Confirm Password field. The required Password Complexity Rules are listed above the Password field.
9. Select one or more Available Roles and click on the left arrow to move the administrator roles from the right box to the left.
10. Click Save. You are returned to the Administrator Details page.

Figure 89. View Administrator Details

To edit an administrator:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Account link, select Administrators. The Administrators List page displays.
3. Click on the administrator you wish to edit. The Administrator Details page displays.
4. Click Edit. The Edit Administrator page displays.
5. Update the necessary fields and click Save. You are returned to the Administrator Details page.

To delete an administrator:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Account link, select Administrators. The Administrators List page displays.
3. Click on the administrator you wish to delete. The Administrator Details page displays.
4. Click Delete and click OK in the confirmation popup window. You are returned to the Administrators List page.

	***WARNING: Deleting Administrators*** *Deleting an administrator cannot be undone. Do not delete an administrator without being fully aware of the consequences.*

WARNING: No Administrators Left!

"Warning: There are no administrators on this account with full access. Please create an administrator login with full access to this account before performing any other user operations."

If you get this message while deleting a user or administrator, you have attempted to disable the last administrator with full access to this system. Please make sure another administrator has full access before disabling this one.

Administrator Roles

Administrator roles are an assigned set of permissions that allow an administrator access to the various sections of the Brivo Onsite Server. For example, the Brivo Onsite Server provides a few preloaded administrator roles, one of which is called Receptionist. An administrator who has been given the role of receptionist has the capability to view and modify device status and to view activity. If additional permissions are desired, a new administrator role can be created or an existing administrator role can be edited to add new permissions.

Administrators can be assigned a number of different roles, all granting different permissions. If any action is granted by a role, an administrator with that role is allowed that action regardless of other roles the administrator may have.

Each account in the system has a reserved role, called System Administrator or Account Administrator (for the system and sub-accounts respectively). These roles cannot be modified or deleted, and have certain permissions that cannot be granted to other roles. For example, the ability to create and edit new administrator roles is restricted to the reserved role only. As a special case, the System Administrator role must always be assigned to at least one administrator. This protects against accidental complete system lock-out.

To view administrator roles:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Account link, select Administrator Roles. The Administrator Roles List page displays.

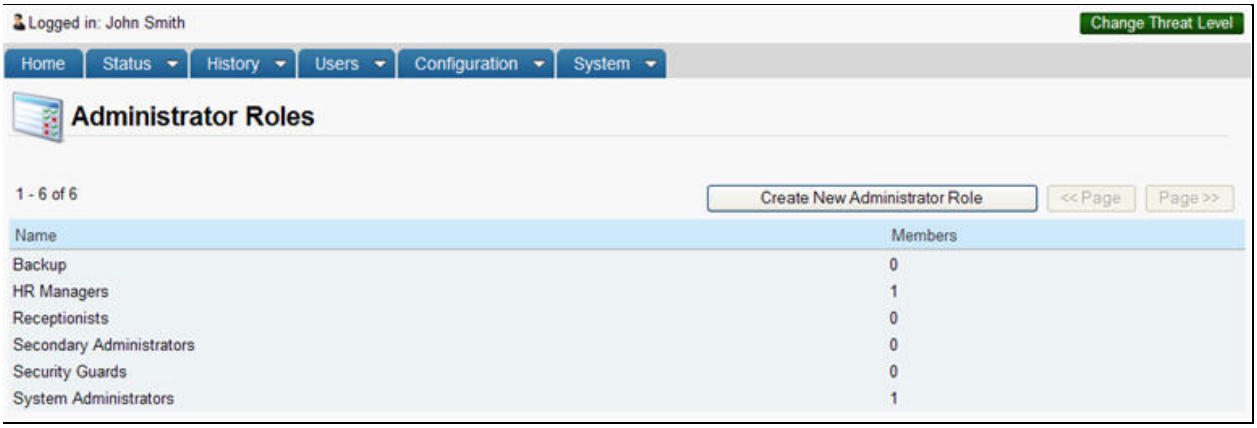


Figure 90. View Administrator Roles

Definitions of Permissions

Below is a list of definitions for each of the various permissions allowed when setting up or editing an administrator role.

Administrator Controls

- View – allows an administrator to view content for a particular permission.
- Modify – allows an administrator the ability to modify data in relation to a particular permission.
- Create – allows an administrator the ability to create new data in relation to a particular permission.
- Delete – allows an administrator to delete data in relation to a particular permission.
- Allow – allows an administrator the right to perform an action in regards to a particular permission.
- Targets – refers to the entities within an account that this permission will be affecting.

Permissions:

- Make System Backup – allows an administrator with this permission to perform a system backup of the Brivo Onsite Server.
- System Settings – allows an administrator to view and/or modify the system settings of the Brivo Onsite Server, including things like system date/time, upgrading the firmware, and license keys.
- Network Settings – allows an administrator to view and/or modify the network settings of the Brivo Onsite Server, including things like network configuration or panel discovery.
- Database – allows an administrator to view and/or modify the database of the Brivo Onsite Server. This includes such activities as bulk user imports, and backing up and restoring the full application database.
- Accounts - allows an administrator to view and/or modify information related to one or more accounts of the Brivo Onsite Server.
- Administrators – allows an administrator to view, modify, create, and/or delete administrators on the Brivo Onsite Server.
- Administrator Roles – allows an administrator to view administrator roles.
- Users – allows an administrator to view, modify, create, and/or delete users in the Brivo Onsite Server database.
- Residents – allows an administrator to view, modify, create, and/or delete residents in the Brivo Onsite server database. This functionality is only usable if the Brivo Onsite Server has an IPAC license.
- Manage User Group Memberships – allows an administrator to view and/or modify the group members of users in the Brivo Onsite Server database for one or more accounts.
- Custom Field Definitions – allows an administrator to view, modify, create, and/or delete custom fields of the Brivo Onsite Server for one or more accounts.
- Custom Field Data – allows an administrator to view and/or modify the data in custom fields in the Brivo Onsite Server database for one or more accounts.
- Cards – allows an administrator to view, create, and/or delete cards in the Brivo Onsite Server.
- Card Formats – allows an administrator to view, modify, create, and/or delete card formats in the Brivo Onsite Server.
- Badge Templates – allows an administrator to view, modify, create, and/or delete badge templates in the Brivo Onsite Server.

- Print Badge – allows an administrator to print badges in from a given set of badge templates on the Brivo Onsite Server.
- Control Panels – allows an administrator to view, modify, create, and/or delete control panels associated with the Brivo Onsite Server.
- Devices – allows an administrator to view, modify, create, and/or delete devices in the Brivo Onsite Server.
- Device Status – allows an administrator to view and/or modify the status of devices associated with the Brivo Onsite Server for a given set of devices.
- DVR Drivers – allows an administrator to view, create, and/or delete DVR drivers for the Brivo Onsite Server.
- Filters – allows an administrator to view, modify, create, and/or delete filters in the Brivo Onsite Server.
- Groups – allows an administrator to view, modify, create, and/or delete groups in the Brivo Onsite Server.
- Holidays – allows an administrator to view, modify, create, and/or delete groups in the Brivo Onsite Server.
- Maps – allows an administrator to view, modify, create, and/or delete maps in the Brivo Onsite Server.
- Email Notifications – allows an administrator to view, modify, create, and/or delete email notifications in the Brivo Onsite Server.
- Schedules – allows an administrator to view, modify, create, and/or delete schedules in the Brivo Onsite Server.
- Threat Levels – allows an administrator to view, modify, create, and/or delete threat levels in the Brivo Onsite Server.
- Antipassback Zones – allows an administrator to view, modify, create, and/or delete antipassback zones in the Brivo Onsite Server.
- Activity – allows an administrator to view activity in the Brivo Onsite Server.
- Administrative Journal – allows an administrator to view the Administrative Journal in the Brivo Onsite Server.
- Change Threat Level – allows an administrator to change the threat level in the Brivo Onsite Server for one or more accounts.
- Schedules Status – allows an administrator to view and/or modify the status of schedules in the Brivo Onsite Server for one or more accounts.
- Reset Antipassback Zones – allows an administrator to reset antipassback zones in the Brivo Onsite Server for one or more accounts.
- View Live Video – allows an administrator to view live video in the Brivo Onsite Server for one or more accounts.
- View Archive Video – allows an administrator to view archive video in the Brivo Onsite Server for one or more accounts.
- Alarm Console Settings – allows an administrator to view, modify, create, and delete the alarm console settings in the Brivo Onsite Server for one or more accounts.
- Alarm Console – allows an administrator to acknowledge the alarm console for one or more accounts.
- Alarm Bulk Acknowledge – allows an administrator the right to bulk acknowledge alarm events on the alarm console.

- Reports – allows an administrator the right to view, modify, create, and delete reports.
- Scheduled Reports – allows an administrator the right to view, modify, create, and delete scheduled reports.

To create an administrator role:

1. Scroll over the Configuration link at the top of any page. The sub-navigation menu displays.
2. From the Account link, click Administrator Roles from the dropdown list. The Administrator Roles list displays.
3. Click Create New Administrator Role. The Edit Administrator Role page displays.

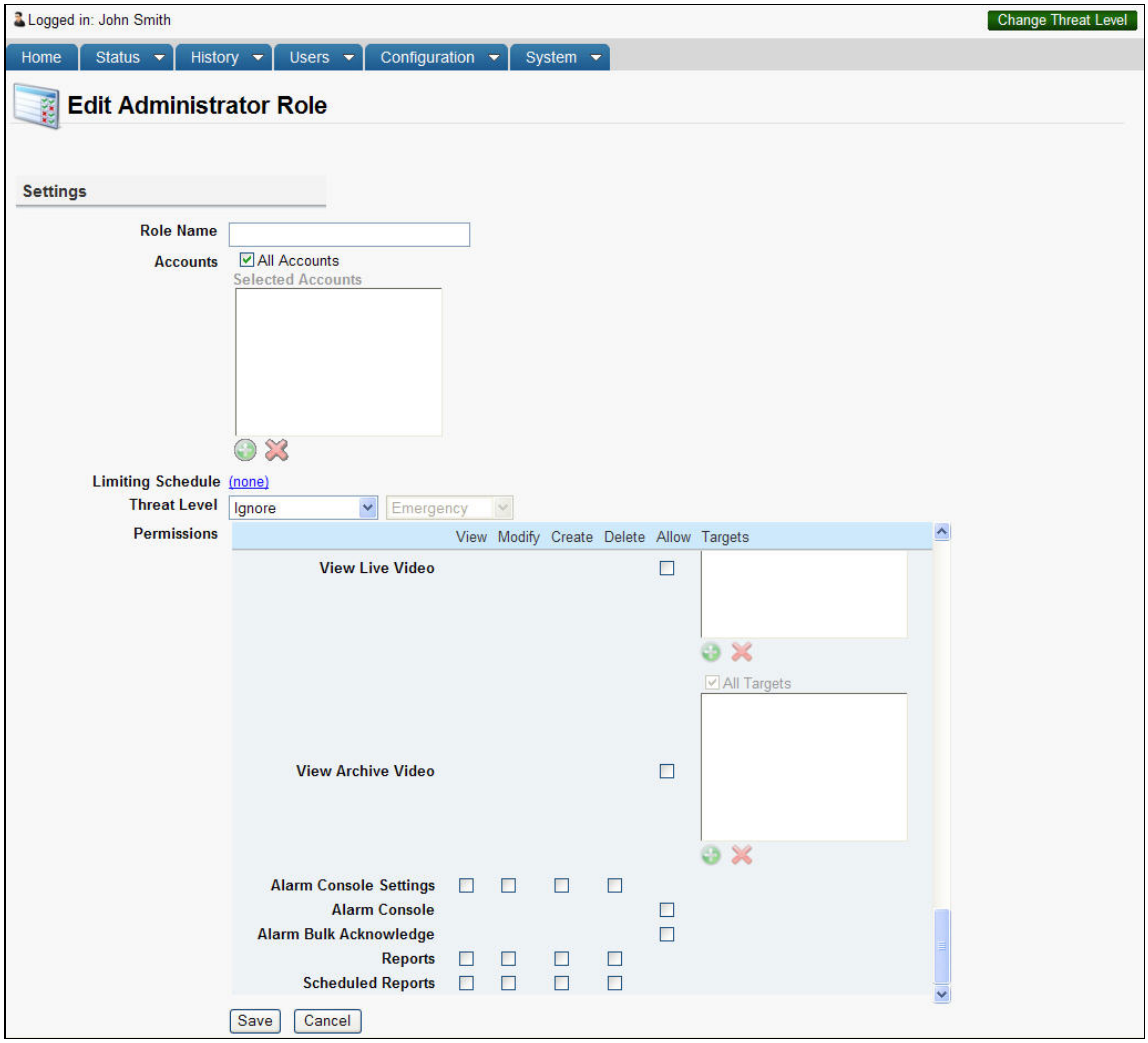


Figure 91. Create New Administrator Role

4. Enter a Role Name for the new Administrator Role.
5. Select which Accounts in which you wish this Administrator Role to be used. If you wish it to be used in all accounts, simply check the All Accounts checkbox.
6. If you wish this administrator role to be limited by a specific schedule, click on the Limiting Schedule link and select the appropriate schedule from the popup window.

7. You may have the administrator role ignore the Threat Level, or select under what threat level condition the administrator role will function.
8. Select which Permissions this administrator role will have. See Definitions of Permissions above for details on each permission.
9. When finished, click Save. You are returned to the Administrator Role List page.

To edit an administrator role:

1. Scroll over the Configuration link at the top of any page. The sub-navigation menu displays.
2. From the Account link, click Administrator Roles from the dropdown list. The Administrator Roles list displays.
3. Click on the administrator role you wish to edit. The Administrator Role Details page displays.
4. Click Edit. The Edit Administrator Role page displays.
5. When you have finished making changes to the administrator role, click Save. You are returned to the Administrator Role Details page.

To delete an administrator role:

1. Scroll over the Configuration link at the top of any page. The sub-navigation menu displays.
2. From the Account link, click Administrator Roles from the dropdown list. The Administrator Roles list displays.
3. Click on the administrator role you wish to delete. The Administrator Role Details page displays.
4. Click Delete. A popup box appears warning you this action is permanent. Click OK. You are returned to the Administrator Roles list page.

	*NOTE:* *Any administrators using a deleted role will simply lose any permissions that role allowed them to use, unless duplicated by another role that they also have assigned. If the deleted administrator role was the only role assigned to them, their admin login will still work, but they will have no ability to use the system other than to change their password.*

To copy an administrator role:

For ease of use, administrator roles can be duplicated using a copy feature. This allows, for example, a certain set of permissions to be used multiple times for different accounts without having to recreate the role manually every single time.

1. Scroll over the Configuration link at the top of any page. The sub-navigation menu displays.
2. From the Account link, click Administrator Roles from the dropdown list. The Administrator Roles list displays.
3. Click on the administrator role you wish to copy. The Administrator Role Details page displays.
4. Click Copy This Role. The Edit Administrator Role page displays with all of the details of the copied role.
5. Enter a new Role Name for the new role.
6. Make any addition changes as needed. When finished, click Save. You are returned to the Administrator Role Details page.

12.Threat Levels

Threat Levels represent different operational modes for the entire system, which can, for example, allow an Administrator to rapidly secure all unlocked doors and restrict access to specific groups. These modes may have different rules for which users can access which resources, what devices do (or don't do), and whether measures that normally relax system security (e.g. doors unlocking on a schedule) continue to do so. An important distinction about Threat Levels is that Threat Levels are usually tied to a range. An example of this would be that if your system had 5 threat levels with 1 being normal and 5 being the most severe, threat levels allow you to create scenarios where certain events occur at 'threat level 3 or lower'. Thus, threat levels are not as distinct and compartmentalized as simple modes as a concept.

Once a threat level is changed, it will remain in effect until manually changed again. Changing a threat levels is displayed on the Dashboard page. It is also tracked in the Activity Log, reflecting the time and Administrator who made the change.

Who Can Change Threat Levels?

Any authorized administrator with appropriate permissions can change Threat Levels for their account. Threat Levels can be optionally configured on a per-account basis. Authorized administrators can only change Threat Levels for their own account.

Certain Threat Levels may limit access to credential-based devices, such as doors and floors in an elevator. Only those groups with the appropriate permissions will continue to be able to use such devices. If a System Account Administrator changes a Threat Level, all access to devices that are shared by other accounts is subject to the conditions of the new Threat Level for the groups belonging to those accounts.

If you do not wish to have Threat Levels available on an account, you may choose to omit this option when configuring the account.

Threat Level Influence

NOTE:

The default setting for permissions, devices, and schedules concerning threat levels is Ignore. This means that unless the administrator edits it, the permission, device, or schedule will continue to function as programmed even if the threat level is changed. If an administrator wants a permission, device, or schedule to respond to a change in threat level, the administrator must edit it to do so.

Change of a Threat Level may affect the following:

- Schedules can be set to be active at, at or more severe, or at or less severe than a given threat level.
- Permissions to devices (configured on the Edit Group Permissions page) can be set to be active at, at or more severe, or at or less severe, than a given threat level.
- Floors and doors owned by the account that use the threat level can be set to ignore their unlocked schedules at, at or more severe, or at or less severe than a given threat level.
- Programmable devices can be configured to be only active at, at or more severe, or at or less severe than a given threat level (in addition to their configured schedule).
- Elevators, valid credential devices, and doors owned by the account that use the threat level can be configured to require 2-factor authentication at, at or more severe, or at or less severe than a given threat level.
- Muster points owned by the account that use the threat level can be configured to be active at, at or more severe, or at or less severe than a given threat level.
- Every page of the application will display a large, colored banner that contains a pre-configured message notifying the owner that a threat level has been changed, unless the threat level has been changed to the default threat level which shows no banner message. The message is customized when either a new account is created or an existing account is edited.
- The Activity Log reflects the date and time the threat level was changed, as well as the Administrator who made the change.
- Email notifications can be configured to alert administrators to changes in threat level.
- Administrator Roles can be configured to function at, at or more severe, or at or less severe than a given threat level.

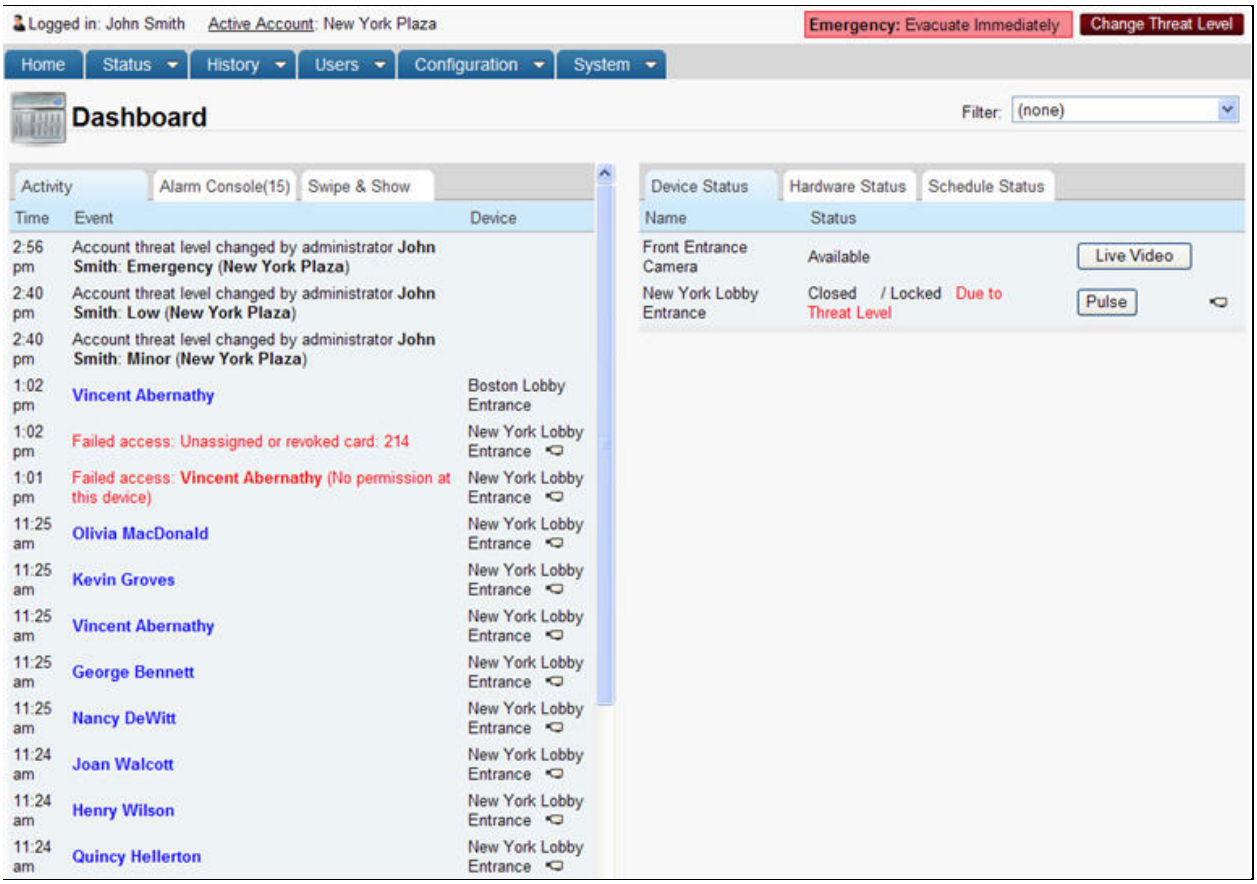


Figure 92. Threat Level engaged

Threat Level Configuration

The Brivo Onsite Server, rather than strict imposition of arbitrary numbers, allows a user defined set of rules to be implemented to suit the needs of the user. Threat Levels can be created and arranged in any severity desired by the administrator.

Each threat level has the following properties:

Property	Type	Description
Name	Text	What to call the threat level
Description	Text	Allows the user to specify what this threat level means
Color	Color (chosen from palette)	Color used in the user interface to represent the condition
Message	Text	Message that will display in the user interface when the threat level is invoked
Default Level	Radio button	To determine if this is the default state for the system (no special displays occur when the system is at default)
Password	Checkbox	Whether to prompt for an administrator's password when setting the system to this new threat level

To Create a Threat Level:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. Select Threat Levels from the Account dropdown list.
3. Click on the Create New Threat Level button.
4. Enter a Name for the new threat level.
5. Click on the Select button and choose a color from the palette.
6. Enter a Description of the threat level. This message will appear on the Change Threat Level popup page when a threat level is changed.
7. Enter the Banner information that will appear next to the Change Threat Level button when the threat level is engaged. This field will not appear when the default threat level is engaged.
8. Check the Prompt for password checkbox if you want a password to be required to activate this threat level.
9. When finished, click Save. This will return you to the Threat Level Details page.
10. If you wish for this threat level to be the default threat level, return to the Threat Levels list page and choose the Default radio button for this threat level.

NOTE:

Even though a threat level has been created, until such time as any threat level is actually activated, the system will continue to operate as if there are no threat levels in place.

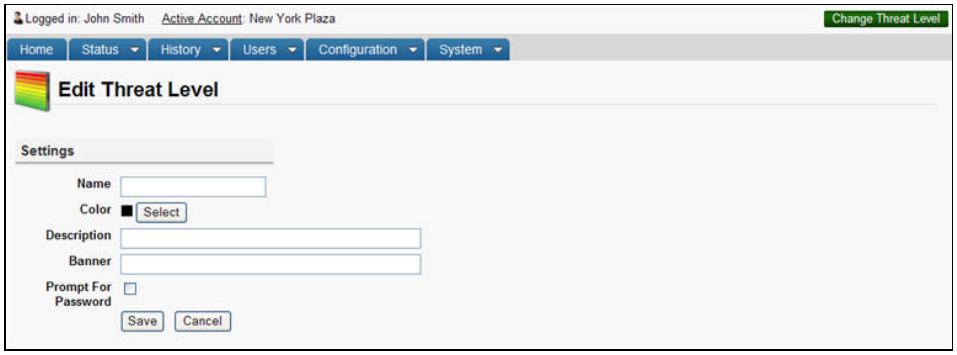


Figure 93. Create a Threat Level

To Edit a Threat Level:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. Select Threat Levels from the Account dropdown list.
3. Click on the threat level you want to edit. The Threat Level Details page displays.
4. Click Edit. The Edit Threat Level page displays.
5. Enter the desired changes and click Save. You are returned to the Threat Level Details page.

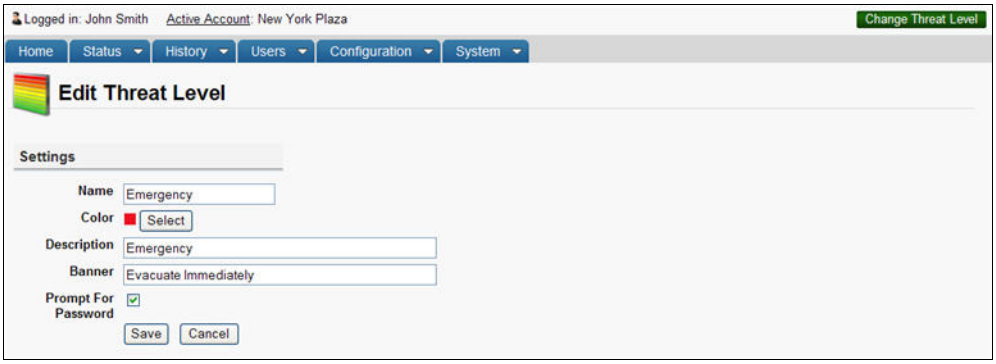


Figure 94. Edit Threat Level

To Delete a Threat Level:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Account link, click Threat Levels.
3. Click on the threat level you want to delete.

	***WARNING:** Deleting Threat Levels* *Deleting a threat level will also remove any restrictions on any devices, permissions, or schedules that rely on this threat level. It will also remove any restrictions that include this Threat Level in a range. This operation cannot be undone.*

4. Click Delete. On the popup window, click OK. The Threat Levels list page displays.

Threat Level Severity

Once more than one threat level has been created, the severity of each new threat level can be modified.

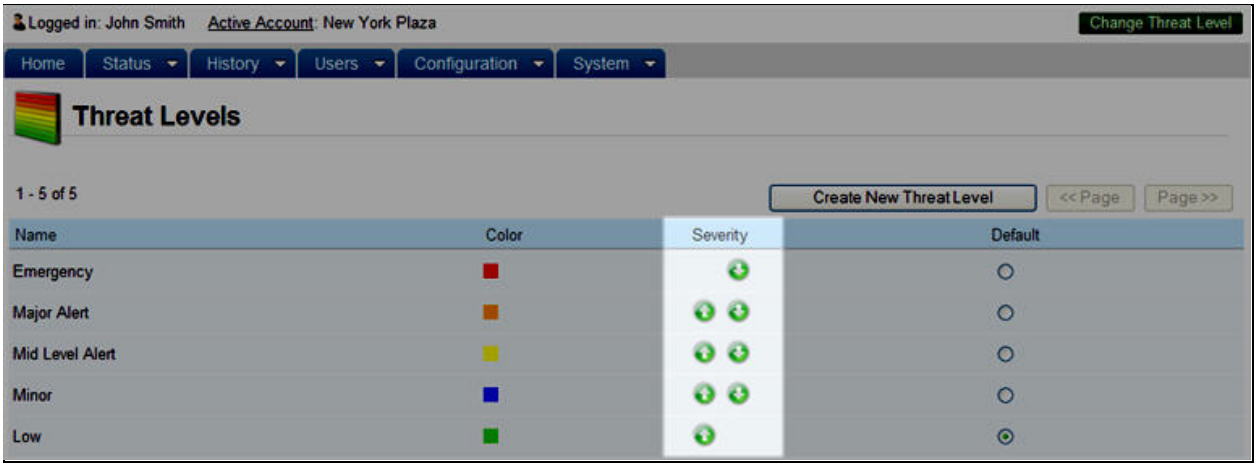


Figure 95. Threat Level Severity

The threat level severity chart functions on a top-down approach. The top most threat levels are the most severe. The lower the threat levels on the list, the less severe it is considered. An administrator with appropriate permissions can adjust the severity of a particular threat level by clicking on the blue up arrow to increase the severity of the threat level or by clicking on the blue down arrow to decrease the severity of the threat level.

New threat levels always begin at the top of the list, being considered most severe, and may be moved down in severity as needed.

To Change a Threat Level:

1. The Change Threat Level icon at the top right of any screen must be clicked to change a threat level.

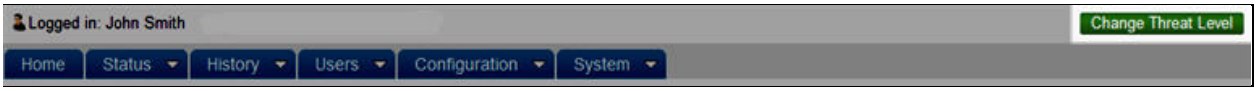


Figure 96. Change Threat Level Icon

2. A Change Threat Level box will display, showing the current threat level, showing the available threat levels from a dropdown menu, and an Administrator Password field if necessary.

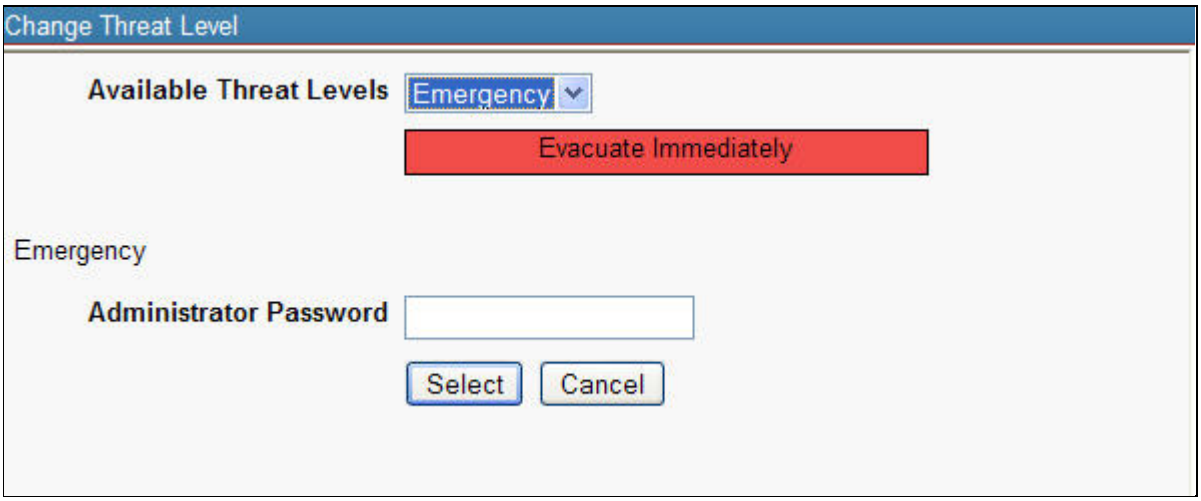


Figure 97. Change Threat Level Popup

3. Select the new threat level from the Available Threat Levels dropdown menu.
4. Enter the Administrator Password if required.
5. Click Select.
6. The threat level will change and the message banner will appear next to the Change Threat Level icon.

Editing Permissions for Threat Levels

An administrator with appropriate permissions can determined whether or not groups can have access during, above, or below certain threat levels by defining the privileges on the Edit Group page.

To set a threat level for a permission:

1. Scroll over the Users link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Groups. The Groups page displays.
3. Select the group you wish to edit or click the Create New Group button.
4. Under the threat levels section, choose when this group is active from the dropdown menu. Options are to ignore threat levels entirely, or to have the group be active at, above (more severe), or below (less severe) a selected threat level.

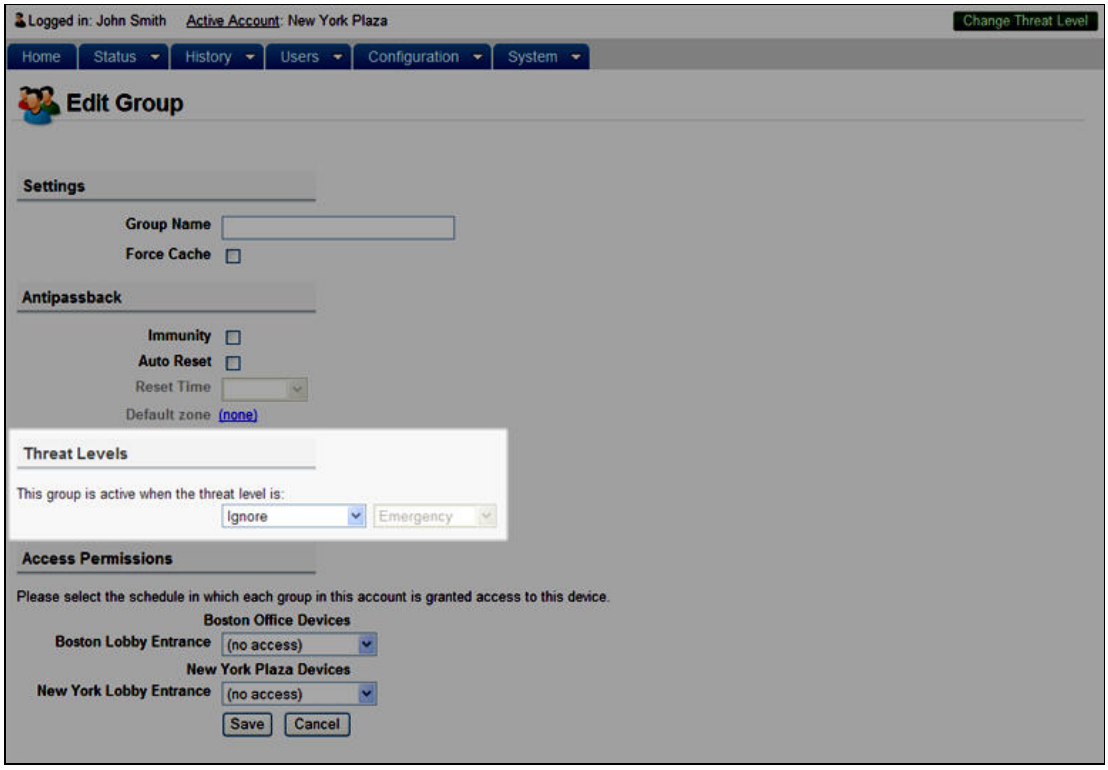


Figure 98. Setting threat level permissions for a group

5. Click Save.

Editing Devices for Threat Levels

An administrator with appropriate permissions can determine whether or not a device can be active at, above, or below certain threat levels by defining the privileges on the Edit Device page.

To set a threat level for a device:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices. The Devices page displays.
3. Select the device you wish to edit or click the Create New Device button.
4. Under the threat levels section, choose when this device is active from the dropdown menu. Options are to ignore threat levels entirely, or to have the device be active at, at or more severe, or at or less severe than a selected threat level.
5. Optionally, an administrator may select if the device will also require two-factor authentication. Options are to ignore threat levels entirely, or to have the device be active at, at or more severe, or at or less severe than a selected threat level.

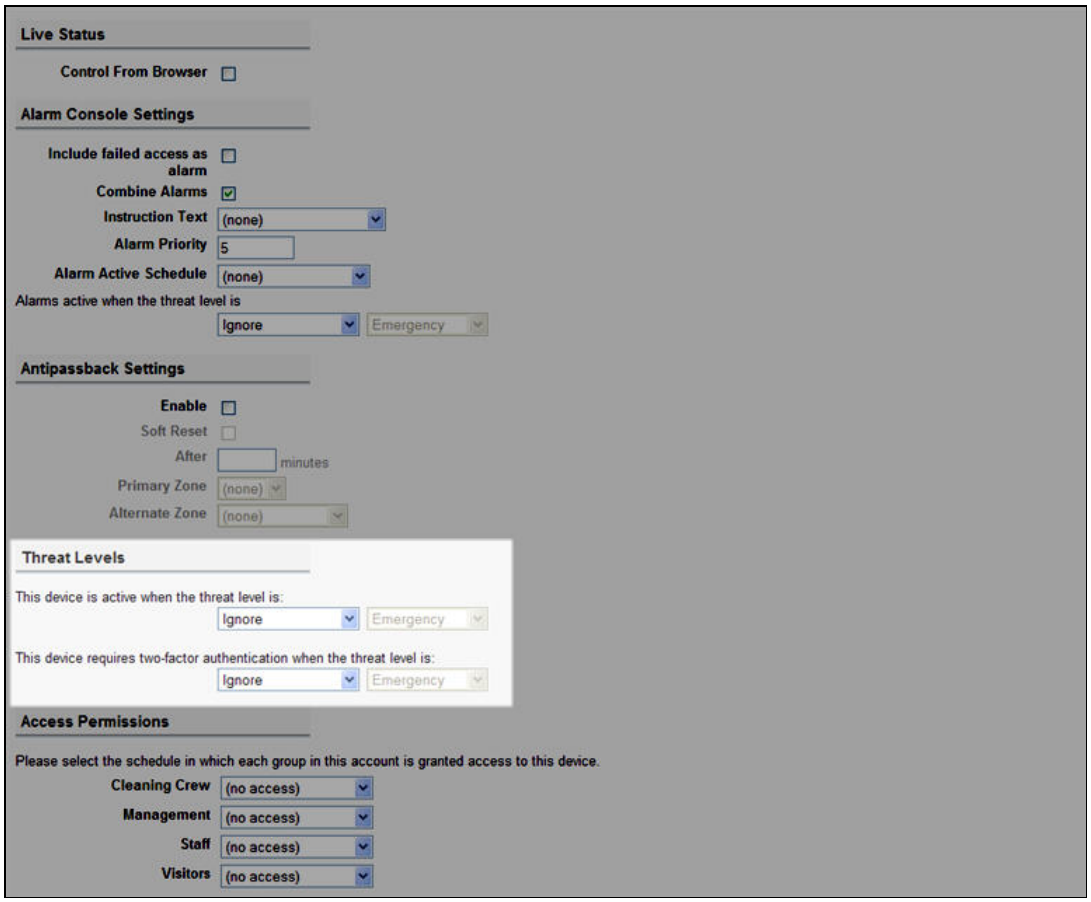


Figure 99. Setting threat level permissions for a device

6. Click Save.

Editing Schedules for Threat Levels

An administrator with appropriate permissions can determine whether or not a schedule can be active at, above, or below certain threat levels by defining the privileges on the Edit Schedule page.

To set a threat level for a schedule:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Scheduling link, click Schedules. The Schedules page displays.
3. Select the schedule you wish to edit or click the Create New Schedule button.
4. Under the threat levels section, choose when this schedule is active from the dropdown menu. Options are to ignore threat levels entirely, or to have the schedule be active at, at or more severe, or at or less severe than a selected threat level.

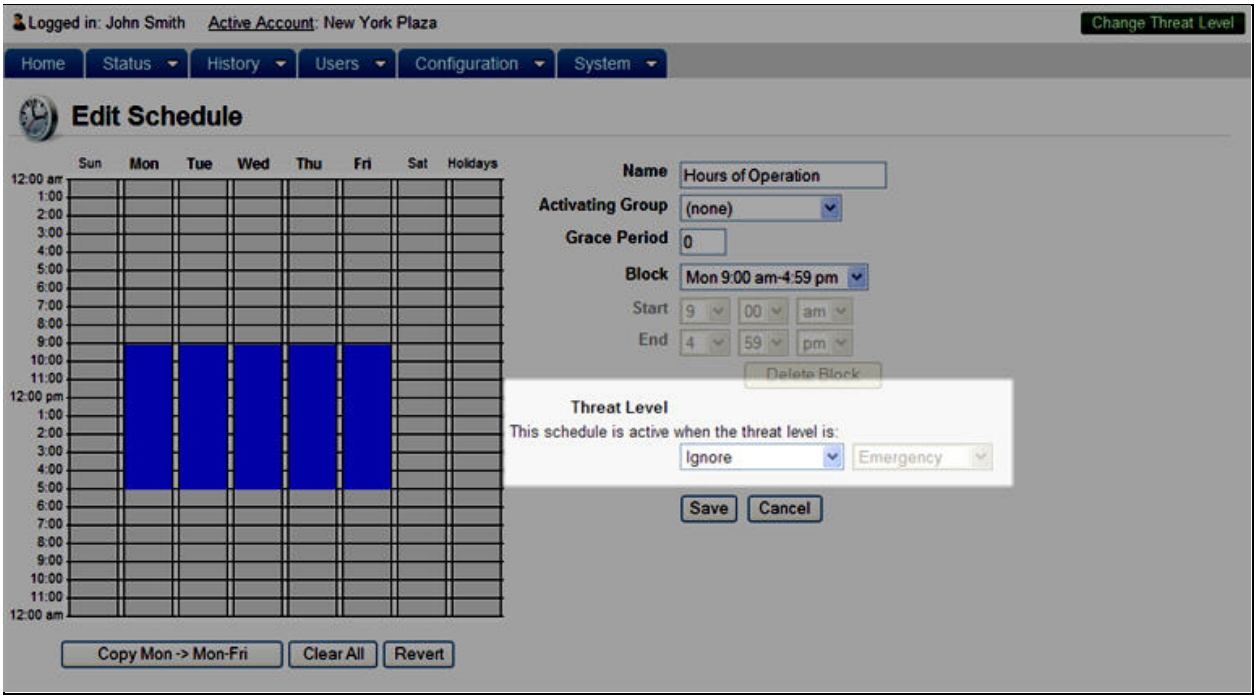


Figure 100. Setting threat level permissions for a schedule

5. Click Save.

Threat Levels and Shared Devices

Devices that are shared to sub-accounts are mapped only to a schedule. Threat level definitions are confined to individual accounts. Assigning ownership of a device (as opposed to sharing the device) allows a sub-account to assign its own threat levels to that device. A device can only be owned by one account at a time, but may be shared between multiple sub-accounts.

Note that this means that threat levels on group permissions to shared devices are already set for sub-account access to those shared devices, so group permissions on shared devices in sub-accounts do not have access to threat level selections.

To enable threat levels on an account:

1. Threat levels must be enabled at an account level in order to function. Sub-accounts can also have independent threat levels for their own (non-shared) devices.
2. Scroll over the Configuration link. The sub-navigation menu displays.
3. From the Account link, click Account Details.
4. Click on the account in which you wish to enable threat levels.
5. Click Edit and the Edit Account Details page displays.
6. Check the Enable Threat Levels checkbox.
7. Click Save. You are returned to the Account Details page.

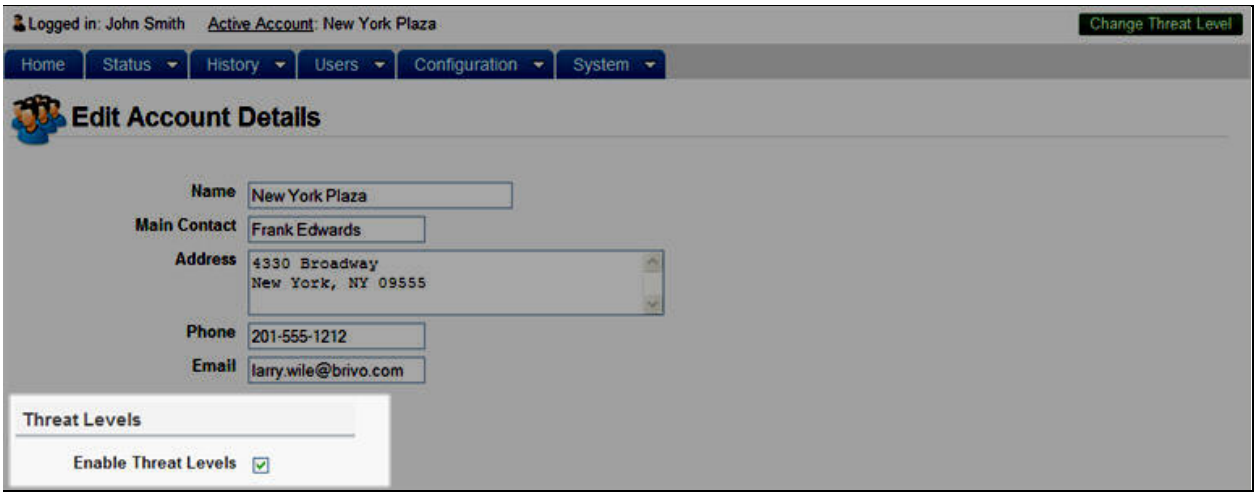


Figure 101. Enabling threat levels

13.Antipassback

Antipassback prevents an authorized user from presenting a credential to access an area, and then "passing back" that credential to another individual, who then uses the same credential to access the building.

An example of antipassback is sealed labatory where two credential readers are installed, one on an entry and one on an egress, at particular doors. Users must present their card to enter, and also to exit the door. The Activity Log documents when individuals enter and exit.

Another example of antipassback is a parking garage where an ingress reader is installed, allowing users to enter an antipassback zone, and then to have the zone reset after a certain period of time, allowing users to return if they have left the zone (driven home for the night).

When Antipassback is enabled, and an individual enters and passes back his or her credential to another, the unauthorized user will not be allowed to enter, because the system recognizes that the credential has already been used to enter the building.

All Antipassback violations are recorded in the Activity Log.

NOTE:

Antipassback functionality relies on the connection between control panels and the server. If the panels are not connected to the appliance, Antipassback will not function.

NOTE:

Salto Door Locks are not capable of supporting anti-passback functionality.

Antipassback settings can easily be disabled by administrators with appropriate permissions, allowing them to control entry and exit in the case of an emergency. Additionally, Antipassback provides an important employee management feature, as the access system can provide information regarding how many people are within a building or access controlled area at a specific time, as well as their identities.

Antipassback Zones

While antipassback can be employed on a system-wide basis, it often is used within an overall access control system for specific zones, such as server rooms, data storage facilities, and other high-security areas.

NOTE:

If an individual enters a door configured within an Antipassback zone without showing his credential, he will not be able to exit that zone when he presents his credential. Similarly, individuals who exit a door in an Antipassback zone without presenting a credential will not be allowed to reenter until the Antipassback Reset Interval has elapsed.

Devices may have both a Primary and Alternate zone:

The Primary Zone is the location of the primary (or only) reader associated with a device.

Alternate Zones indicate the location of a secondary (or alternate) reader that is applied to Antipassback configurations, if one is configured for that device.

Antipassback Definitions

Hard Antipassback

Hard Antipassback controls keep individuals from using their card to enter a zone if they are already inside, or exiting if they are already outside. With Hard Antipassback implemented, once a user presents his or her credential, Brivo Onsite Server recognizes the entry to a zone and will not allow the user re-enter unless he or she first exits that zone.

Soft Antipassback Reset Interval

Soft Antipassback design allows administrators to specify an interval after which users are free to re-enter a zone without having properly exited that zone. This can also be described as a "forgiveness interval" after which an Antipassback violation can be "forgiven" and a valid user granted access. The Soft Reset Interval range for Antipassback is from 1 to 999 minutes.

Antipassback Immunity

The Antipassback Immunity feature is ideal for administrators who wish for only one individual to bypass Antipassback settings for an account. Immunity is granted to a particular user by creating a group that will only include the individual with immunity to Antipassback.

Important Antipassback Considerations

Users start out in the (none) zone when created.

Administrators with appropriate permissions to activate devices can reset a group's or user's Antipassback zone to whichever zone the administrator desires.

When a user's or group's zone is reset, the action is noted in the activity log.

With Hard Antipassback, once a user has entered a zone, he or she will not be allowed back into this zone until exiting that zone.

Tenant account may use system Antipassback zones in their zone configuration if the Global Visibility option is checked.

Administrators can set the device's Antipassback zone from the Devices list page or from the Edit Antipassback Zone page.

WARNING: Antipassback and deleting doors

It is very important to note that any doors that have antipassback in use can still be deleted. However, this will cause severe problems for antipassback functionality. Do NOT delete any doors on a system using antipassback without first being aware of the effects of how deleting that door will affect your antipassback setup.

Groups who are immune to Antipassback controls do not follow the same Antipassback controls as those who are not immune. These users are free to enter or exit a door even if the Antipassback Reset Interval has not elapsed.

Alternate readers can be set up without Antipassback enabled

If device is using a device profile, the device follows the profile's configured settings for Antipassback.

All devices with readers can be configured for Antipassback.

Administrators with appropriate permissions can select a zone for a group to be automatically reset to once a day.

Antipassback functionality can work across multiple panels.

User Aliases are universally affected by antipassback actions taken in the primary account. For example, if the primary account resets the antipassback settings for the user's group, the user (and its alias) will be affected.

Managing Antipassback Controls

To create an Antipassback zone:

1. Scroll over the Configuration section. The sub-navigation menu displays.
2. From the Devices link, click the Antipassback link. The Antipassback Zones list page displays.
3. Click Create New Antipassback Zone. The Edit Antipassback Zone page displays.

Figure 102. Create Antipassback Zone

4. Enter the name for the Antipassback Zone you wish to create.
5. If you wish for the Antipassback Zone to be visible across accounts, check the Global Visibility box.
6. To add the preferred available device into the For Readers box, click the Add New button. A popup window will appear with a list of available readers. Click on the reader you wish to select. The reader now appears in the For Readers box.
7. Once finished, click Save. You are returned to the Antipassback Zones list page.

To edit an Antipassback zone:

1. Scroll over the Configuration section. The sub-navigation menu displays.
2. From the Devices link, click the Antipassback link. The Antipassback Zones list page displays.
3. Click the Antipassback Zone that you wish to edit. The Antipassback Details page displays.
4. Click Edit. The Edit Antipassback Zone page displays.
5. After you have finished making changes to the Antipassback zone, click Save. You are returned to the Antipassback Zones list page.

To delete an Antipassback zone:

1. Scroll over the Configuration section. The sub-navigation menu displays.
2. From the Devices link, click the Antipassback link. The Antipassback Zones list page displays.
3. Click the Antipassback Zone that you wish to delete. The Antipassback Details page displays.
4. Click Delete. Click OK in the confirmation prompt. You are returned to the Antipassback Zones list page.

To configure Antipassback settings for a device:

	*NOTE:* *All devices with readers can be configured for antipassback, and alternate readers can be set up without antipassback enabled.* *If device is using a device profile, the device follows the profile's configured settings for antipassback.* *If you are not planning on using the antipassback functionality of the Brivo Onsite Server for a specific device, do not check the Enable checkbox under Antipassback Settings during device creation.*

1. Scroll over the Configuration section. The sub-navigation menu displays.
2. From the Devices link, click the Devices link. The Devices list page displays.
3. To apply Antipassback controls to a preexisting device, click on that device. The Device Details page displays. (To configure the Antipassback controls for a new device, see the section on Creating Devices.)
4. At the bottom of the Device Details page, click Edit. The Edit Device page displays.
5. To activate Antipassback, check the Enable box under the Antipassback Settings heading.
6. The Antipassback controls are automatically configured for Hard Antipassback, with the default reset interval set at 0 minutes. To configure Soft Antipassback, enter the number of minutes from 1 to 999.
7. Select from the Primary Zone dropdown list which zone you would like to configure Antipassback for use with your primary reader. Users start out in the (none) zone when created.
8. Select from the Alternate Zone dropdown list which zone you would like to configure Antipassback for use with your alternate reader, if one is configured. Users presenting a credential at the primary reader will be transferred into this zone.
9. If you would like the door to be controlled by two readers, you may configure Antipassback controls for an alternate reader by selecting a zone from the Alternate Reader dropdown list.
10. Click Save. You are returned to the Device List page.

To configure Antipassback Settings for a group:

1. Scroll over the Users link. The sub-navigation menu displays.
2. From the sub-navigation menu, click the Group link. The group directory displays.
3. Click on the group for which you would like to configure Antipassaback. The group details page displays.
4. Click Edit. The Edit Group page displays.
5. Under the Antipassback heading, check "Immunity" if you wish for the group to be immune to Antipassback settings.

	*NOTE:* *Groups who are immune to Antipassback controls do not follow the same Antipassback controls as those who are not immune. These users are free to cross zone boundaries without restrictions.*

6. To configure the group's Antipassback settings to reset automatically, check the "Auto Reset" box.

7. Select the time you wish for the Antipassback controls to be reset from the dropdown list.
8. Click on the link next to Default to select the default Antipassback zone for the group.
9. When you have finished configuring the group's Antipassback settings, click Save. You are returned to the Group Details page.

To configure a time to automatically reset the Antipassback zone for all users in a group:

	*NOTE:* *If a user is in multiple groups that have automatic zone resets, the resets will each be applied to that user with the last reset being the final zone setting for that user. If multiple groups reset their zone at the same time, a user in those groups ends up with one of the zones arbitrarily.*

1. Scroll over the Users link. The sub-navigation menu displays.
2. From the sub-navigation menu, click the Groups link. The group directory displays.
3. Click on the group for which you wish to configure the Antipassback Reset Time. The page displays the group details.
4. Click Edit. The Edit Group page displays.
5. If you would like the group to remain immune from Antipassback, check the "Immunity" box underneath the Antipassback heading. To configure the Antipassback zone for all users in that group to be reset automatically, check the Auto Reset box.
6. Select the reset time from the dropdown menu.
7. Click on the default zone link and select a default zone from the popup window.
8. Click Save. You are returned to the group details page.

To manually reset an Antipassback zone for a user:

	*NOTE:* *When a user's or group's zone is reset by an administrator, the action is noted in the activity log.*

1. Scroll over the Users link. The sub-navigation menu displays.
2. From the sub-navigation menu, click the Users link. The user directory displays.
3. Click the user whose Antipassback zone you would like to reset. The Users Details page displays.
4. Choose Reset Antipassback Zone from the dropdown menu. A popup window displays.
5. Select from the popup window which Antipassback zone you would like to reset for the user. You are returned to the Users Details page.

To manually reset an Antipassback zone for a group:

1. Scroll over the Users link. The sub-navigation menu displays.
2. From the sub-navigation menu, click the Groups link. The group directory displays.
3. Click the group whose Antipassback zone you would like to reset. The Group Details page displays.

4. Click Reset Antipassback Zone. A popup window displays.
5. Select from the popup window which Antipassback zone you would like to reset for the group. You are returned to the Group Details page.

To manually reset an Antipassback zone:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click the Antipassback link. The group directory displays.
3. Click the antipassback zone you would like to reset. The Antipassback Details page displays.
4. Click Reset Antipassback Zone. A popup window displays.
5. Select from the popup window into which new antipassback zone you would like to move any users in the current antipassback zone.
6. Click OK in the popup window. You are returned to the Antipassback Details page.

14. Devices

The Brivo ACS5000-A and ACS6000-A control panels consist of one or more control boards used to manage the doors and devices defined for an account. A *control board* is either a Door Board or an Input Output (IO) Board. Each control board has a number of input and output *points*, which are actual connections wired to switches, relays and readers. In the case of Door Boards, the points are grouped into two *door nodes* per board, each node containing all of the inputs and outputs necessary to control a single door. Door boards can therefore be configured to drive two doors (one per node). Or, they can be used to control one door and multiple devices, since the input and output points of the second door node can be used to drive devices.

The Brivo ACS300-A controller, a single HID E/ERW-400 Edge device, Brivo ACS-IPDC-1 or Brivo ACS-IPDC-2 controllers. The Brivo ACS300-A and Brivo ACS-IPDC-2 control two readers, and the Edge device or the Brivo ACS-IPDC-1 controls one reader.

	*NOTE:* *Although it is labeled DOOR BOARD, the Brivo ACS5000-A/ACS6000-A Door Board can be used to drive any type of device that can be wired to close contacts or driven by a relay; it does not have to be used to control just a door.*

	*NOTE:* *Keep in mind, when configuring the input and output points on the control boards, that the configuration must match the actual physical wiring of the panel. Consult your dealer to ensure that the configuration in Brivo Onsite Server matches the actual control panel wiring.*

For the ACS5000 and ACS6000, a *control panel* is a complete system of chassis, control boards, power supplies, and associated interconnected wiring referred to as a common Control Panel ID number. This includes the Main Board and up to 14 additional control boards (Door Boards and/or Input Output Boards). While each control panel can have a maximum of only 15 control boards (including the Main Board), an account can manage multiple control panels.

For the ACS300, a *control panel* is a complete system of the ACS300 unit, power supply (if needed) and associated interconnected wiring referred to as a common Control Panel ID number.

For the IPDC, a *control panel* is a complete system of the IPDC unit, power supply (if needed), and associated interconnected wiring referred to as a common Control Panel ID number. For configuration instructions for the IPDC unit, please consult the *IPDC-A Configuration Guide* on our website.

A *control board* is either a Door Board or an Input Output Board (I/O Board). Each control board has a number of input and output *points*, which are actual connections wired to switches, relays and Wiegand readers. In the case of Door Boards, the points are grouped into two *door nodes* per board, each node containing all of the inputs and outputs necessary to control a single door. Door boards can therefore be configured to drive two doors (one per node). Or, they can be used to control one door and multiple devices, since the input and output points of the second door node can be used to drive devices such as elevators.

Control boards are accessible from the System Account only, as is all hardware-related information.

With the Brivo ACS5000-A or ACS6000-A panel, control boards can be used to manage the following devices:

Doors, both external and internal.

Switch Input Devices, such as a manual switch or any device that can create a contact closure.

Valid Credential Input Devices, such as a Wiegand card reader.

Schedule Controlled Devices, such as a light switch trigger.

Event Triggered Devices, such as a door forced open event.

Elevators

Floors

DVRs

Cameras

Muster Points

Guard Tours

Keypad Commands

Salto Router Devices

Salto Door Locks

DED (Data Entry) Devices

The Devices tab also allows users to define Antipassback zones and create device profiles in order to expedite the creation of multiple similar devices.

Managing Multiple Control Panels

The Brivo Onsite Server appliance offers the option of adding more than one control panel, upgrading a control panel through the Brivo Onsite Server interface, and configuring a panel through the web interface.

For configuration purposes, a Brivo ACS5000-A or ACS6000-A panel in Client Mode and its attached expansion boards is considered a control panel, as are the Brivo ACS300-A controller, a single HID E/ERW-400 Edge device, Brivo ACS-IPDC-1A or Brivo ACS-IPDC-2A controllers. Brivo ACS5000-A or ACS6000-A panels are capable of controlling up to 30 readers, while the Brivo ACS300-A and Brivo ACS-IPDC-2A control two readers, and the Edge device or the Brivo ACS-IPDC-1A controls one reader.

The input/output points on boards may be utilized to control devices attached to any control panel used by the Brivo Onsite Server appliance. This cross-panel setup can allow a more efficient use of all of the system's input and output points.

Programmable Devices

The following devices produce messages indicating their live status, which is then shown on the Dashboard:

Switch Input Device: A device with one input point and an optional output that has the state of On or Off. The device can have the following behaviors: Toggle, Latch, Unlatch, Pulse, or Follow. A schedule associated with the device causes it to be available for activation via its input point during the selected times for the schedule.

Schedule Controlled Device: A device whose input is a schedule and that has an optional output associated with it. The timer's state is On during the times selected in its schedule; otherwise it is Off. The device can have these behaviors: Toggle, Latch, Unlatch, Pulse, or Follow.

Valid Credential Input Device: A device whose input is a card reader and that has an optional output associated with it. A valid credential device has no state, so its behaviors are limited to: Toggle, Latch, Unlatch, and Pulse. Valid credential devices have permissions associated with them and appear in the group permissions area. Valid credential devices do not have Disengage messages because they do not have On or Off states, nor do they have schedules.

Event Triggered Device: A device whose input is the specific event associated with it from the door that the event triggered device is created to watch. An event triggered device can have an optional output associated with it. The device can always have these behaviors: Toggle, Latch, Unlatch, or Pulse. If an event triggered device is watching for Door Ajar events, then it has a state and can have a Follow behavior. If the Follow behavior is selected, then the device can have a Disengage message. The schedule associated with an event triggered device defines when it is active because a client might want to respond to the event differently during business hours than during non-business hours.

The device types above all allow the following types of Target Output:

Relay: When this type of output is targeted, the selected relay will obey the prescribed output behavior.

Schedule: When this type of output is targeted, the selected Group Activated Schedule obeys the prescribed output behavior.

Threat Level: When this type of output is targeted, the selected Target Threat Level is changed to correspond with the prescribed output behavior.

Special Options for Devices: Floors and Elevators

In order to create an elevator that provides access to a certain floor, you may want to create the floor first.

To Create a Floor:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device List page displays.
3. Click Create New Device.
4. From the device type dropdown list, select "Floor."
5. Enter the name of the floor.

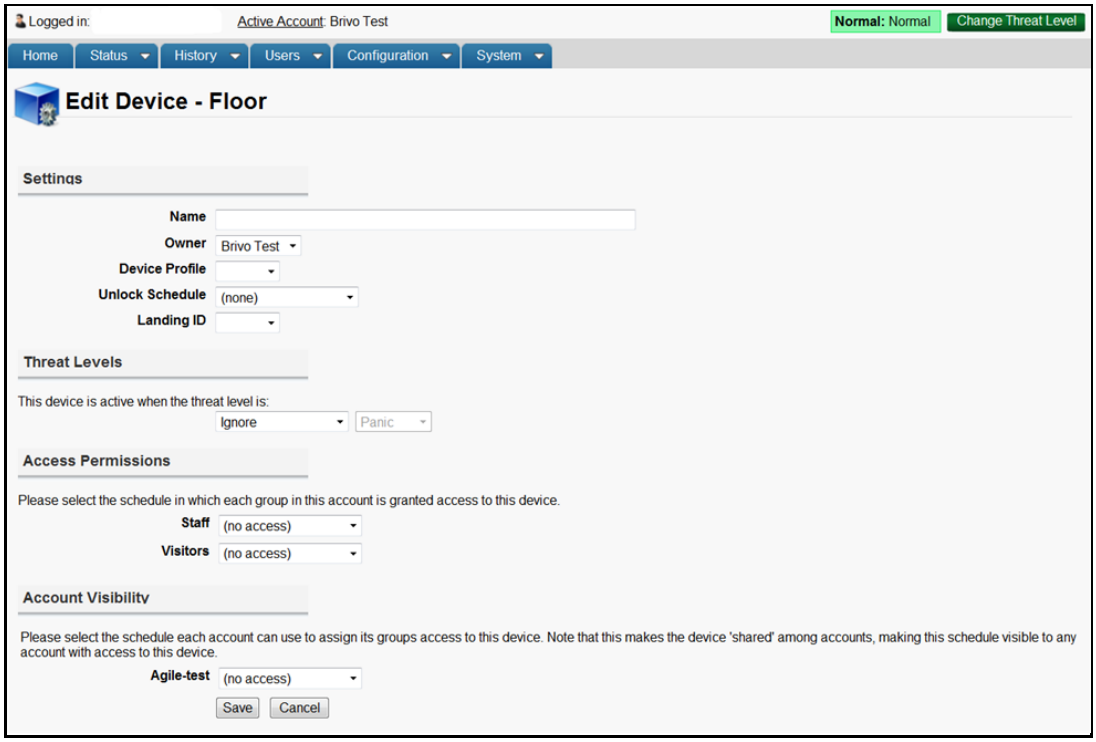


Figure 103. Create New Floor

6. Choose the owner of the floor from the dropdown list.
7. If you have created a Device Profile, you may select it from the dropdown list.
8. If you wish for the floor to remain unlocked during certain hours, choose a schedule during which you would like it to remain open from the Unlock Schedule dropdown list. If you wish for the floor to remain locked, choose "none" from the dropdown list.
9. If the account has a TKE license, the Landing ID may be selected from the dropdown list.
10. You may have the floor ignore Threat Levels or select under what Threat Level conditions the floor will operate.
11. Assign schedules for when select groups can access the floor by choosing a schedule from the dropdown list of next to each group. If you do not want a certain group to access that floor, choose "no access."

12. If you want other accounts to be able to assign access permissions to this floor, choose the schedule during which other groups may assign these permissions from the dropdown list.
13. Click Save.

To create an Elevator:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device list displays.
3. Click Create New Device.
4. From the device type dropdown list, select "Elevator."
5. Enter the name of the elevator.

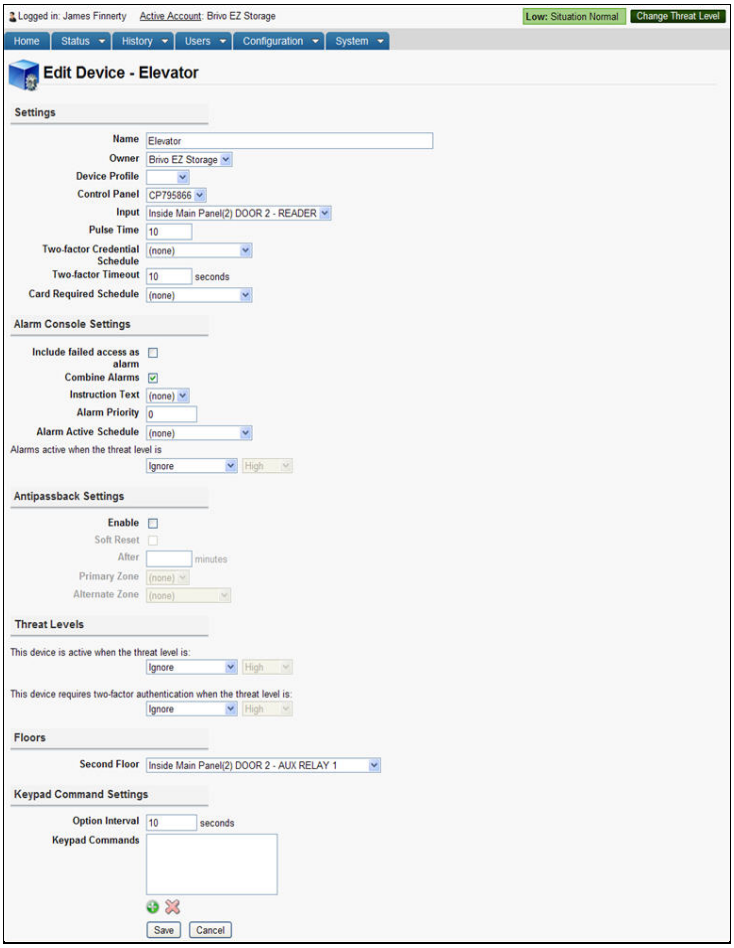


Figure 104. Create New Elevator

6. Choose the owner of the elevator from the dropdown list.
7. If you have created a Device Profile, you may select it from the dropdown list.
8. Under the Control Panel dropdown menu, select the control panel that corresponds to your elevator.
9. Select the input.
10. Enter (in seconds) the amount of time for the device to pulse when provided with a valid credential.

11. If you wish to require the display of two credentials in order to permit access, enable a two-factor credential schedule from the dropdown list. If you do not wish to require two-factor credentials, choose "none."
12. Enter (in seconds) the amount of time allowed before the option to display two credentials expires.
13. If you wish to enable alarm console settings, check the "include failed access as alarms" checkbox. You may also combine alarms, provide instruction text, set alarm priority, schedule when the alarm will function, and whether or not an elevator will function during certain threat levels.
14. If you wish to enable antipassback, check the enable box. You may also enable soft reset with a given number of minutes and determine which antipassback zones will be primary or alternative.
15. You may have the elevator ignore Threat Levels or select under what Threat Level conditions the elevator will operate and if the elevator will require two factor credentialing.
16. If you want to control access to a particular floor, match the relay to the corresponding floor by selecting from the dropdown list.
17. If you wish to apply any Keypad Commands to this elevator, click on the  icon and select the Keypad Command from the popup window.
18. Click Save.

Special Options for Devices: Cameras

Brivo Onsite Server provides Live Video from the dashboard to users with previously defined permission. The cameras are configured on the Devices page. Users can add a camera or a DVR in any order; however, in order for the Dashboard to display Live Video, the Camera must be linked to the DVR.

To create a camera

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device list displays.
3. Click the "Create New Device" button.

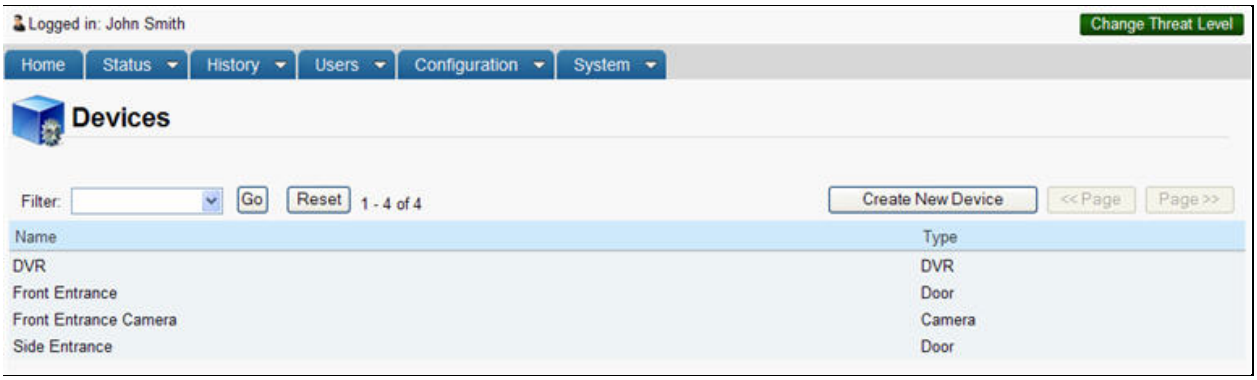


Figure 105. List of Devices

4. Select "camera" from the dropdown list and click "Next." The "Edit Device" page displays.
5. Enter the name of the camera in the field next to Name.
6. If you have already installed a DVR driver, select a DVR from the dropdown list. For more on installing DVR drivers, see *Special Options for Devices: DVRs*.
7. Click the Select button, and if your DVR supports listing cameras, you may choose a camera from the available list. Otherwise, please enter the appropriate camera number in the field provided.

	NOTE: *Depending upon the security settings of your particular browser, a Security Warning popup box may appear. If it does, press No and continue with the operation.*

8. If you wish the photo attached the user profile to display when a card swipe occurs, check the Display Photo checkbox.
9. In the Devices field, use the arrows to move devices from the "Available Devices" box to the "Monitored Devices" box in order to choose which devices you would like the camera to monitor.
10. In the Account Visibility field, use the arrows to determine which accounts have permission to access the camera and Live Video. Use the arrows to move an account from "Available Accounts" to "Permitted Accounts."

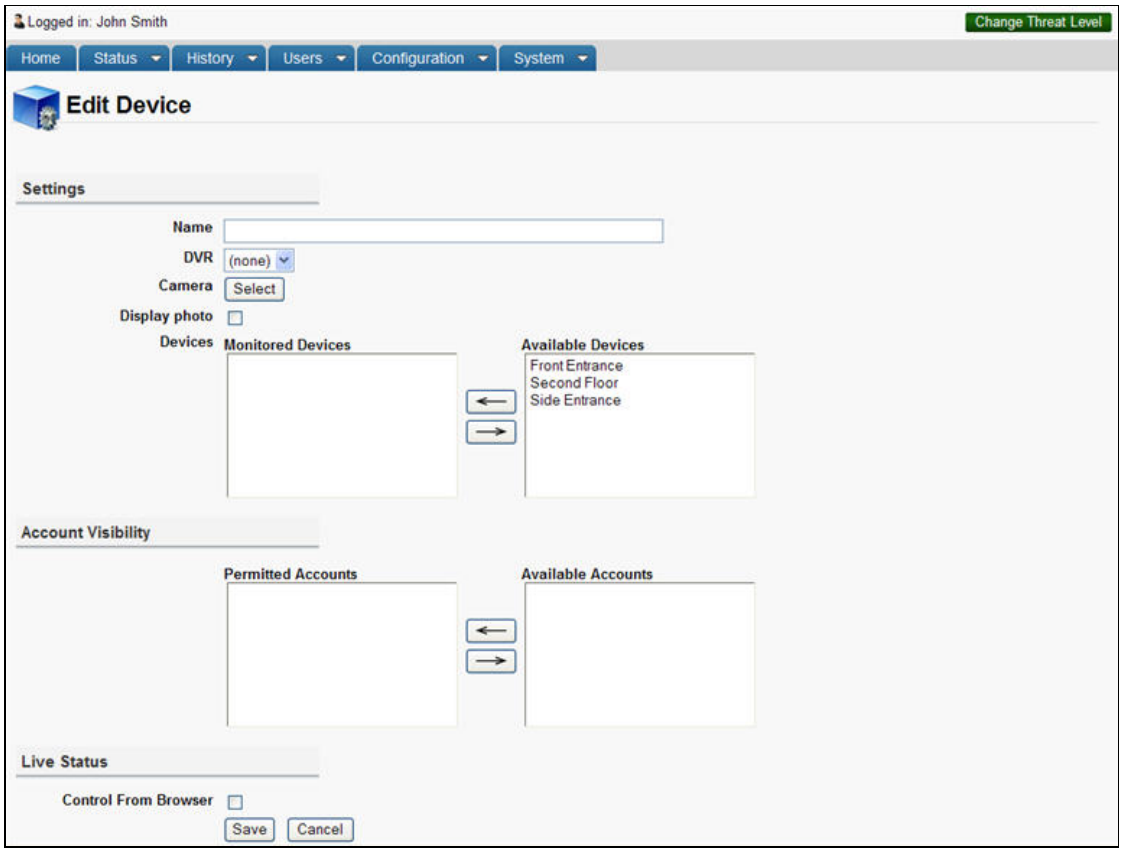


Figure 106. Create Cameras

11. To allow users to view Live Video and the status of the camera from the Dashboard, check the box next to "Control from Browser" under the Live Status field.
12. Click Save.

To edit a camera

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device list displays.
3. Click on the Camera you wish to edit. The device's details display.
4. Click "Edit Device." The Edit Device page displays.
5. When you have finished making changes to the camera, click Save. You are returned to the list of Devices.

To delete a camera

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device list displays.
3. Click on the camera you wish to delete. The device's details display.
4. Click "Delete." A pop-up box appears warning you that this action is permanent. Click OK. You are returned to the list of devices.

Special Options for Devices: DVRs

In order to create a DVR for usage with a camera, you must first install the DVR driver.

	NOTE: *The Xtralis DVR requires a plug-in to be loaded on your local machine in order to function properly. This plug-in may be downloaded from the Brivo website under the Support/Manuals & Downloads/3rd party support section.*

	NOTE: *DVRs require a license key. Without the license key, the DVRs functionality will be disabled.*

To view the list of installed drivers

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device list displays.
3. Click the DVR Drivers link. The DVR Drivers page displays.
4. Click on the driver whose information you wish to view. The details for the driver displays.

Figure 107. DVR Driver Details

To install a DVR driver

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device list displays.
3. Click the DVR Drivers link. The DVR Drivers page displays.
4. Click on the Install New Driver button on the right.

Figure 108. Install DVR Driver

5. Click the Browse button to locate the DVR driver file on your computer. Once you have found it, click Add. You are returned to the DVR Drivers page with the newly-installed driver listed.

To create a DVR

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device list displays.
3. Click the Create New Device button.
4. Select DVR from the dropdown list and click Next. The Edit Device page displays.

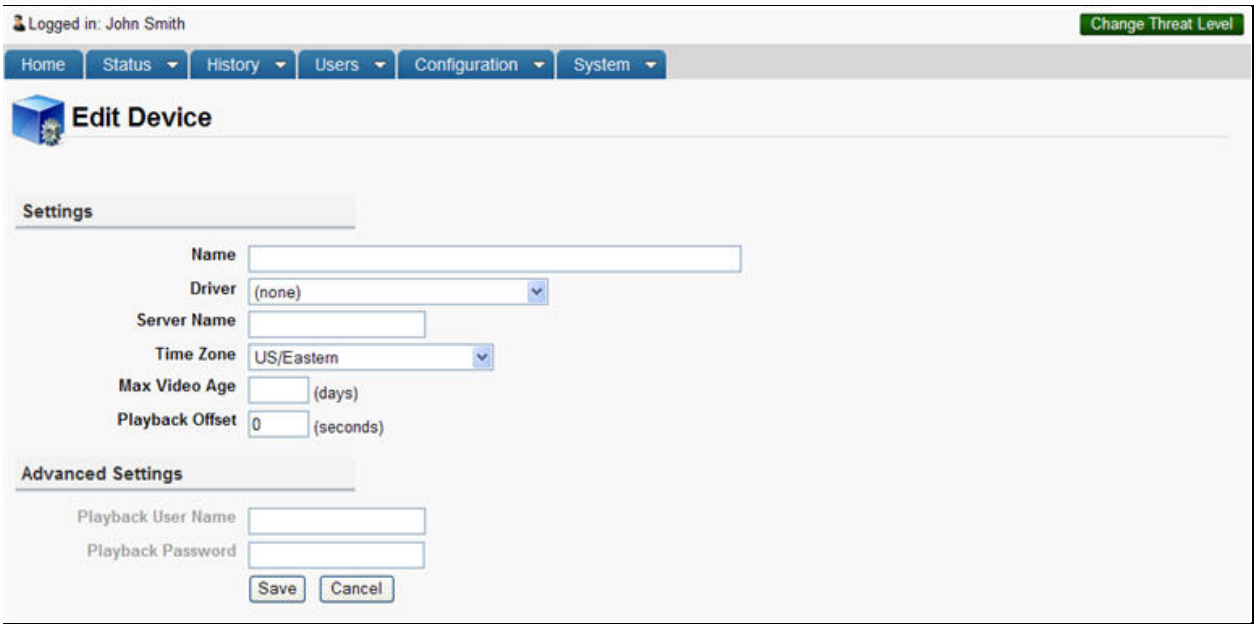


Figure 109. Create New DVR

5. Enter the name of the DVR in the field next to Name.
6. Select a driver from the dropdown list. For more information on installing DVR drivers, refer to the previous section.
7. Enter the Server Name. If you do not know the name of the server, contact your network administrator.
8. Select the Time Zone where the DVR will be installed.
9. Enter the Max Video Age in days to determine the day range of videos logged.

10. Enter the number of seconds next to Playback Offset to specify if there is a lag in connection or not.
11. If your DVR requires a user name and password to play the video, the Advanced Settings field will become active. Enter the user name and password in the respective fields.
12. If your DVR requires that you specify the DVR port number, a DVR Port field will appear for you to enter the number. If your DVR does not require a specific port, this option will not appear.
13. Click Save. You are returned to the list of Devices.

To edit a DVR

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device list displays.
3. Click on the DVR whose information you wish to edit. The Edit Device page displays.
4. When you have finished making changes to the DVR, click Save. You are returned to the list of devices.

To uninstall a DVR driver

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device list displays.
3. Click on the DVR Driver you wish to uninstall. The device's details display.
4. Click "Uninstall Driver" at the bottom of the page. Click OK at the pop-up prompt. When the driver finishes the uninstall process, you are returned to the DVR Drivers page.

To delete a DVR

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device list displays.
3. Click on the DVR you wish to delete. The device's details display.
4. Click "Delete" and then click the OK button in the pop-up prompt. You are returned to the list of devices.

Special Options for Devices: Muster Points

The Muster Point feature allows administrators to use the normal antipassback functionality to track the presence of users in a facility. Antipassback zones are also used for mustering with the addition of a new muster point device type that is a dedicated way to move users into a different zone for tracking purposes.

Muster point devices are a device type that only requires a reader input and a zone configuration. Users that present a credential at a reader are moved into the zone. No permissions or other setup are required, as the mustering point does not actually control access to any resources. It accepts all credentials tied to a user as valid and shows up in the activity log as a valid read access. As with other Brivo Onsite Server antipassback functionality, panel boundaries have no effect on this feature.

To create a muster point:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device List page displays.
3. Click Create New Device.
4. From the device type dropdown list, select Muster Point. Click Next.

	*NOTE:* *Antipassback zones need to be pre-established before Muster Points can be functional.*

5. Enter the name of the muster point.
6. Choose the owner of the muster point from the dropdown list.
7. Choose the control panel from the dropdown list.
8. Choose the Input and Muster Zone from the dropdown list.
9. You may have the muster point ignore Threat Levels or select under what Threat Level conditions the muster point will operate.
10. If you wish to apply any Keypad Commands to the Muster Point, click on the  icon and select the Keypad Command from the popup window.
11. Click Save. You are returned to the Device Details page.

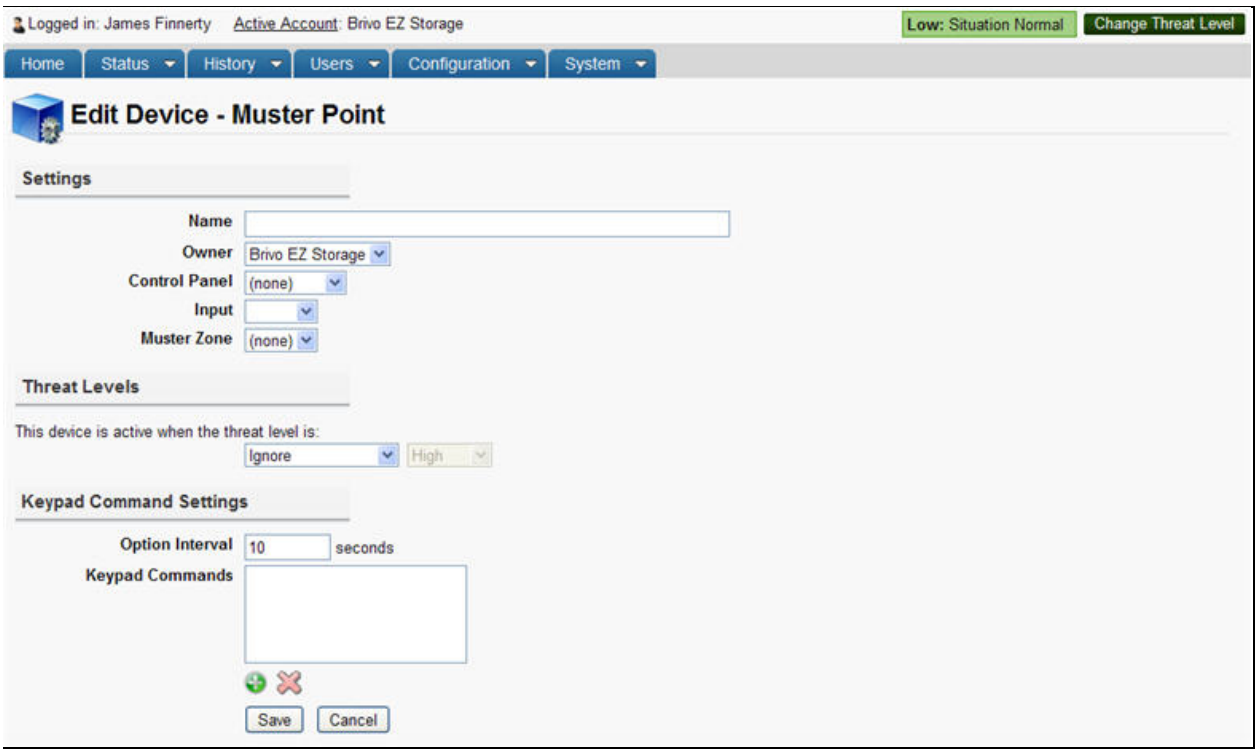


Figure 110. Create Muster Point

To edit a muster point:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Devices from the dropdown list. The Device List page displays.
3. Click on the muster point you wish to edit. The Device Details page displays.
4. Click Edit. The Edit Device page displays.
5. After you have finished making changes, click Save. You are returned to the Device Details page.

To delete a muster point:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device List page displays.
3. Click on the muster point you wish to delete. The Device Details page displays.
4. Click Delete. Click OK in the confirmation prompt. You are returned to the Device List page.

Special Options for Devices: Keypad Commands

The Keypad Command feature allows administrators to define a numeric sequence at a keypad to a specific output behavior. This Keypad Command has its own set of permissions that can be overseen by the administrator, and the Keypad Command functionality can tie to any reader-based device.

Keypad Command devices are a device type that only requires a keypad reader. Users that enter a preset numeric sequence will activate the specified keypad command. Be aware that these keypad command numeric sequences are not unique and that the same numeric sequence can be used at different devices for different output behaviors.

To create a keypad command:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device List page displays.
3. Click Create New Device.
4. From the device type dropdown list, select Keypad Command Device. Click Next.
5. Enter the name of the keypad command device.
6. Choose the owner of the keypad command device from the dropdown list.
7. Choose the control panel from the dropdown list.
8. Enter the Numeric Sequence for the keypad command device.
9. Choose the Target Output from the dropdown list.
10. Choose the Output Behavior from the dropdown list and any delay if desired.
11. Click the icon to choose the Output relay.
12. Under the Relay column, click on the (Click to select panel) area and the control panel list popup will appear. Select the appropriate control panel and then select which relay from the dropdown list.
13. Choose at which threat levels this device will operate.
14. Select which groups will have access to this keypad command device in the Access Permissions section.
15. Choose which devices to apply this keypad command to in the Apply On Devices section. Click the icon to call up a popup list of available devices. Click on the device and you are returned to the Edit Device page.
16. Click Save. You are returned to the Device Details page.

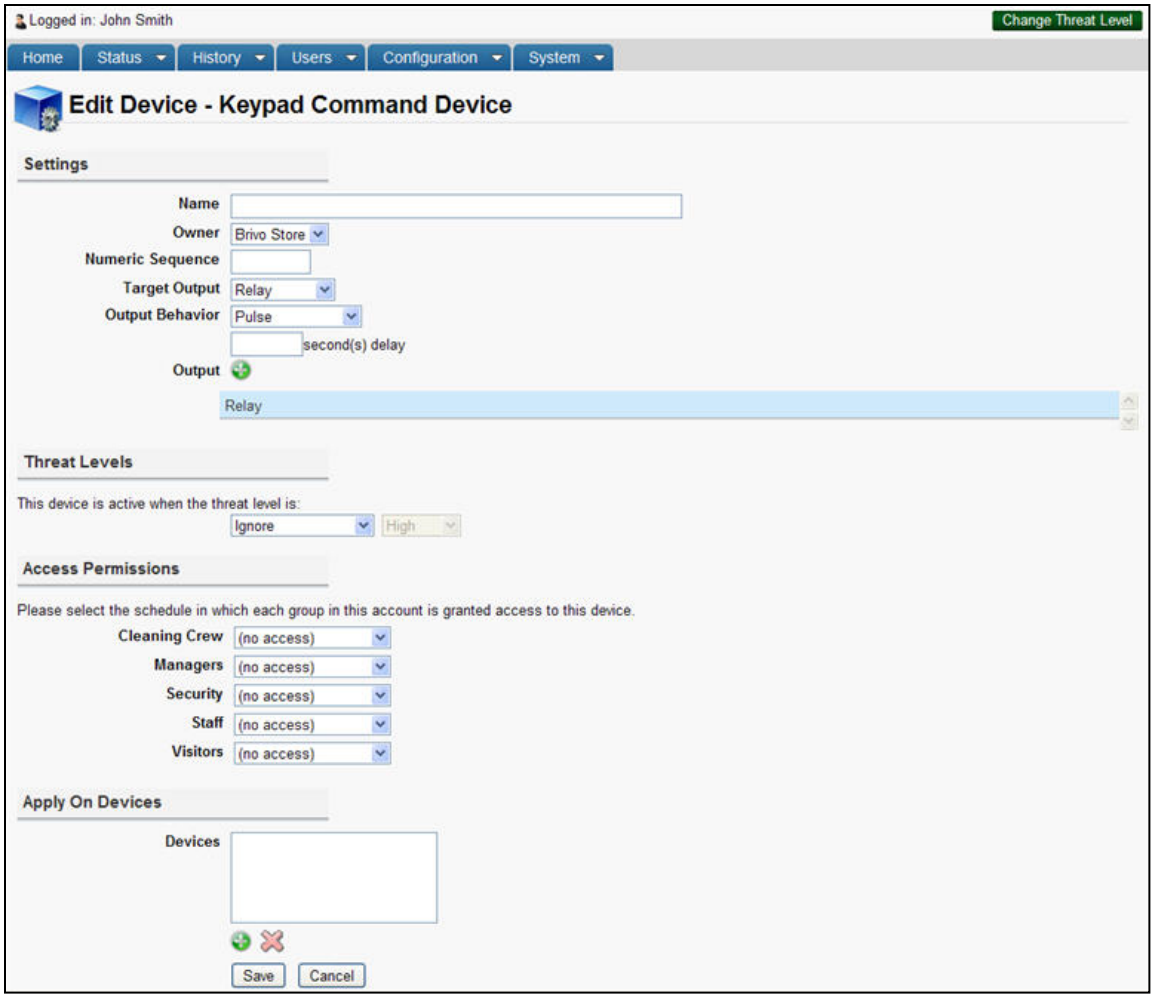


Figure 111. Create Keypad Command Device

To edit a keypad command:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Devices from the dropdown list. The Device List page displays.
3. Click on the keypad command device you wish to edit. The Device Details page displays.
4. Click Edit. The Edit Device page displays.
5. After you have finished making changes, click Save. You are returned to the Device Details page.

To delete a keypad command:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device List page displays.
3. Click on the keypad command device you wish to delete. The Device Details page displays.
4. Click Delete. Click OK in the confirmation prompt. You are returned to the Device List page.

Special Options for Devices: Guard Tour

	NOTE: *Guard Tour requires a license key. Without the license key, Guard Tour functionality will be disabled.*

The Guard Tour feature allows administrators to assign series of readers to act as tour stops that must be visited at an established interval. Guard Tour allows any reader from any device to be utilized in one or more tours. The Guard Tour feature sends alarm messages to the Dashboard if the tour is not successfully completed. Guard Tour also allows relays to be activated if a tour stop is overdue, which can be linked to, for example, a buzzer or flashing light.

Individual stops on a tour can be controlled and may be activated or deactivated as needed, and guard tours can be subject to both assigned schedules and threat levels.

To create a guard tour:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device List page displays.
3. Click Create New Device.
4. From the device type dropdown list, select Guard Tour. Click Next.
5. Enter the name of the guard tour.
6. Choose the owner of the keypad command device from the dropdown list.
7. Choose the Interval of the guard tour.
8. Select the group that is responsible for the guard tour.
9. Check the Control Individual Stops checkbox if you want them individually controlled. Enter the Active Stop Label and Inactive Stop Label if checked.
10. Select the Active Schedule for the guard tour from the dropdown list.
11. If you wish to enable alarm console settings, check the "Combine Alarms" checkbox. You may also provide instruction text, set alarm priority, schedule when the alarm will function, and whether or not the alarms will function during certain threat levels.
12. You may have the guard tour ignore Threat Levels or select under what Threat Level conditions the will operate.
13. Choose which devices to make Tour Stops for the guard tour. Click the icon to add a device to the Tour Stops list. Click on (Click to select device) to call up a popup list of available devices. Click on the device and you are returned to the Edit Device page.
14. If desired, you may (Click to select panel) to have the guard tour activate an Overdue Relay and/or an Active Relay. If selected, these relays will activate when the appropriate situation occurs.
15. Click Save. You are returned to the Device Details page.

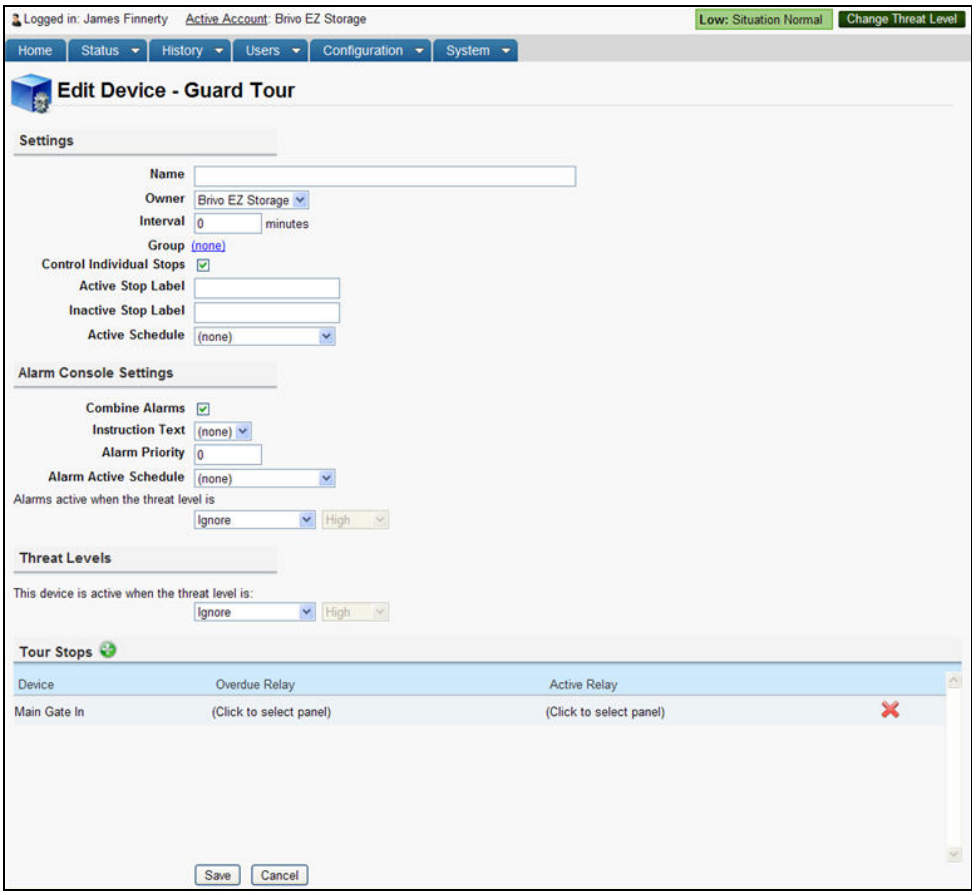


Figure 112. Create Guard Tour

To edit a guard tour:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Devices from the dropdown list. The Device List page displays.
3. Click on the guard tour you wish to edit. The Device Details page displays.
4. Click Edit. The Edit Device page displays.
5. After you have finished making changes, click Save. You are returned to the Device Details page.

To delete a guard tour:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device List page displays.
3. Click on the guard tour you wish to delete. The Device Details page displays.
4. Click Delete. Click OK in the confirmation prompt. You are returned to the Device List page.

Special Options for Devices: Salto Routers and Salto Door Locks

	*NOTE:* *Before the installation and configuration of any Salto products with the Brivo Onsite Server, please follow all preliminary instructions from Salto to ensure the Salto router or Salto door locks are properly configured. Please refer to the Salto Quick Start Guide on the Brivo website for further details.*

The following equipment is required to install and configure Salto equipment on the Brivo Onsite Server.

- A laptop running Windows Vista or later for use with the Salto executable file
- The PPD (Portable Programming Device) using firmware version 1.23 or later

Additionally, the Salto router MUST be configured along with any nodes prior to configuring any Salto door locks.

The Salto routers and door locks feature allows administrators to install and configure Salto wireless door locks.

To create a Salto Router:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Devices from the dropdown list. The Device List page displays.
3. Click Create New Device.
4. From the dropdown menu, select Salto Router Device and click Next.
5. Enter the Name of the router.
6. If available, select the Account Owner from the dropdown list.
7. Select the Control Panel the Salto Router will be linked to.
8. Enter the IP Address/MAC address for the Salto Router.
9. Enter the correct Service Port. This defaults to 1234.
10. If you wish to enable alarm console settings, check the "Combine Alarms" checkbox. You may also provide instruction text, set alarm priority, schedule when the alarm will function, and whether or not the alarms will function during certain threat levels.
11. Click Save.

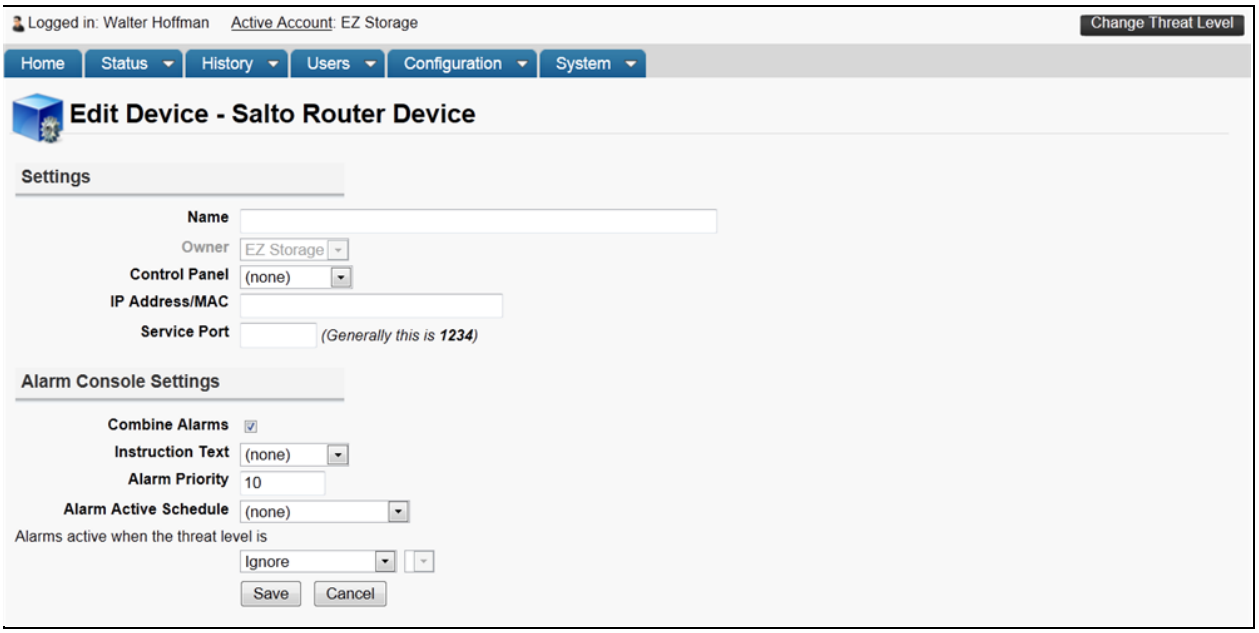


Figure 113. Create Salto Router

To create a Salto Door Lock:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Devices from the dropdown list. The Device List page displays.
3. Click Create New Device.
4. From the dropdown menu, select Salto Door Lock and click Next.
5. Select the Owner from the dropdown list.
6. Select the Salto Router and Lock ID from the dropdown lists.
7. Select an Unlock Schedule if any for the Salto Door Lock.
8. Select the Passthrough Period for the Salto Door Lock. The default is 10 seconds.
9. If desired, select the Offline Behavior (Cached Credentials) for the Salto Door Lock. The default is 0 days.
10. If you wish to control the Salto Door Lock from your browser, check the Control From Browser checkbox.
11. If you wish to enable alarm console settings, check the "Combine Alarms" checkbox. You may also provide instruction text, set alarm priority, schedule when the alarm will function, and whether or not the alarms will function during certain threat levels.
12. You may have the Salto Door Lock ignore Threat Levels or select under what Threat Level conditions the will operate.
13. You may select which groups have Access Permissions to the Salto Door Lock and under which schedules these permissions will operate.

14. If tenant accounts exist, under the Account Visibility section you may select the schedule each account can use to assign its groups access to this device as well as allowing the tenant account to activate the device by checking the Activate Devices checkbox. Note that this makes the device 'shared' among accounts, making this schedule visible to any account with access to this device.
15. To enable Privacy Mode, click the Privacy Mode Enable checkbox. Select the group which may override Privacy Mode by checking the box next to the group name.
16. Click Save.

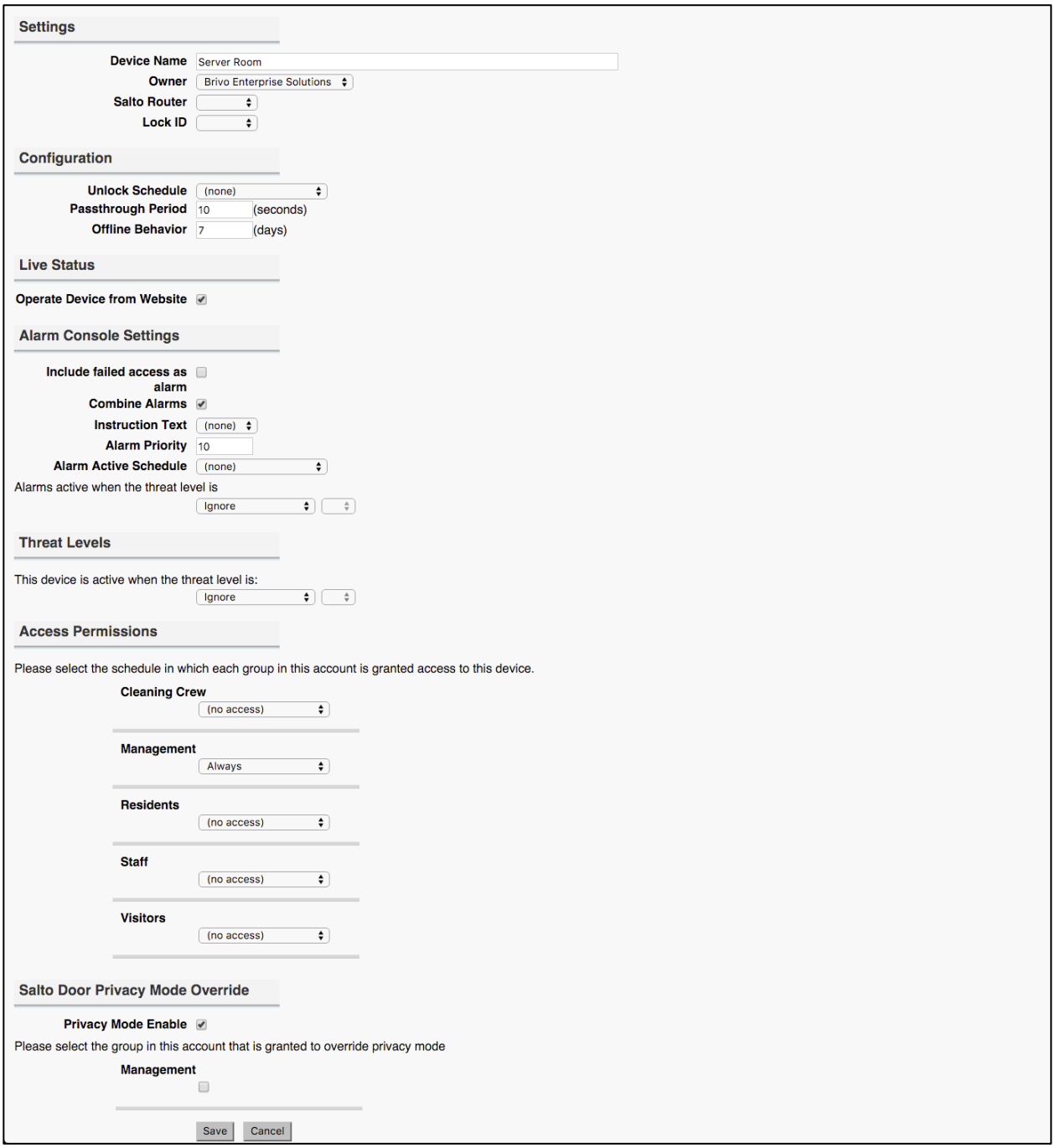


Figure 114. Create Salto Door Lock

To edit a Salto Router or Salto Door Lock:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Devices from the dropdown list. The Device List page displays.
3. Click on the Salto Router or Salto Door Lock you wish to edit. The Device Details page displays.
4. Click Edit. The Edit Device page displays.
5. After you have finished making changes, click Save. You are returned to the Device Details page.

To delete a Salto Router or Salto Door Lock:

WARNING: Salto Routers and Door Locks

If a Salto Router is deleted and has Salto Door Locks associated with it, the Salto Door Locks will automatically default to not having a link to any Salto Router and will stop functioning.

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device List page displays.
3. Click on the Salto Router or Salto Door Lock you wish to delete. The Device Details page displays.
4. Click Delete. Click OK in the confirmation prompt. You are returned to the Device List page.

Special Options for Devices: DEDs (Data Entry Devices)

The DED (Data Entry Device) feature allows administrators to assign and configure touchscreens or keypads to interact with the users of an elevator system attached to the Brivo Onsite Server.

	*NOTE:* *DED (Data Entry Device) functionality requires a license key. Without the license key, DED functionality will be disabled.*

To create a Data Entry Device:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Devices from the dropdown list. The Device List page displays.
3. Click Create New Device.
4. From the dropdown menu, select DED Device and click Next.
5. Enter the Name of the DED device.
6. If available, select the Account Owner from the dropdown list.
7. If available, select the Device Profile from the dropdown list.
8. Select the Control Panel from the dropdown list.
9. Select the Input from the dropdown list.
10. Enter the Group Number in the field provided (values from1-255).
11. Enter the Landing Number in the field provided (values from 1-255).
12. Enter the Object Number in the field provided (unique DED identifier).
13. Select Which Side (Front or Rear).
14. If you wish to require the display of two credentials in order to permit access, enable a two-factor credential schedule from the dropdown list. If you do not wish to require two-factor credentials, choose "none."
15. Enter (in seconds) the amount of time allowed before the option to display two credentials expires.
16. If you wish to require a card to be presented for entry, enable a card required schedule from the dropdown list. If you do not wish to require a card to be presented, choose "none".
17. If you wish to enable alarm console settings, check the "include failed access as alarms" checkbox. You may also combine alarms, provide instruction text, set alarm priority, schedule when the alarm will function, and whether or not an elevator will function during certain threat levels.
18. You may have the Data Entry Device ignore Threat Levels or select under what Threat Level conditions the Data Entry Device will operate and if the Data Entry Device will require two factor credentialing.
19. To associate floors with the Data Entry Device, select a floor in the Available Floors box and click on the  icon and move the selected floor to the Associated Floors box. To disassociate floors, simply select the floor and click on the  icon and move the Associated Floors to the Available Floors box.
20. When finished, click Save.

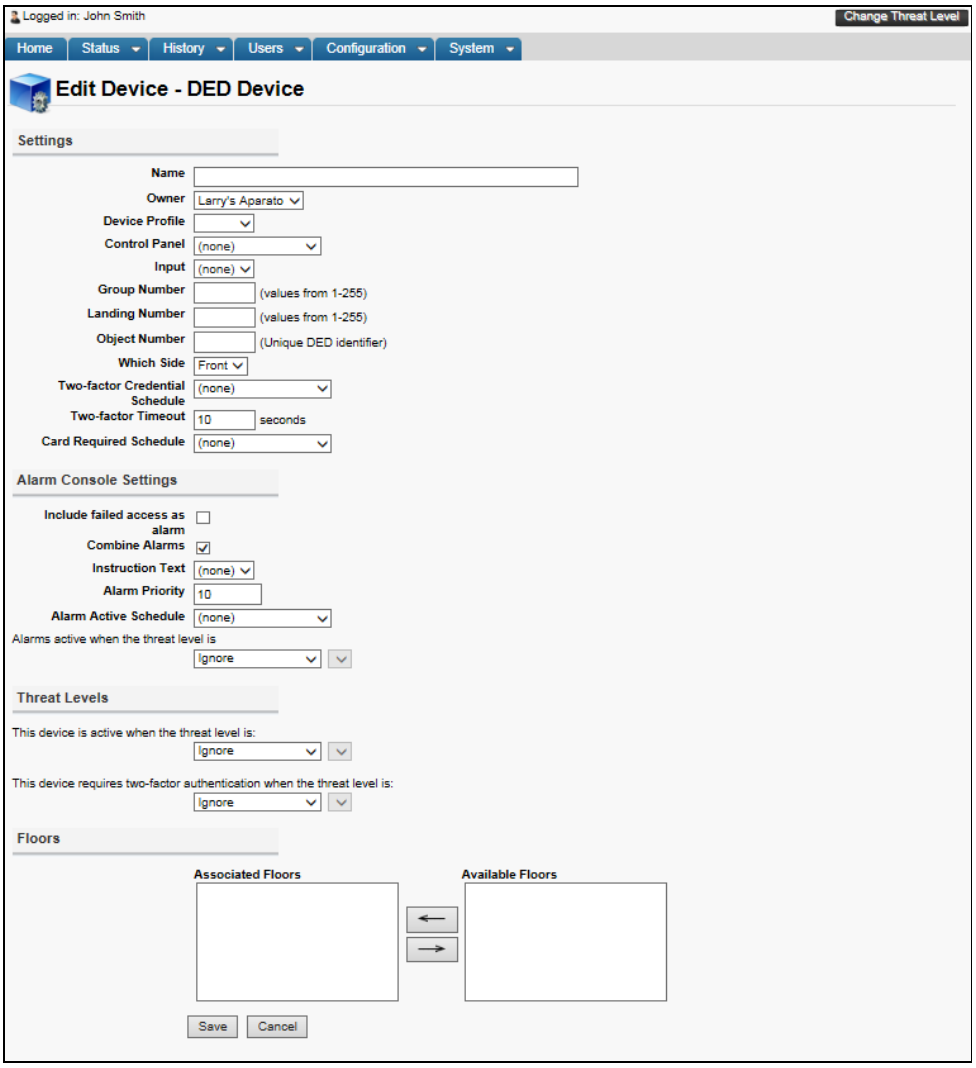


Figure 115. Create a Data Entry Device (DED)

To edit a Data Entry Device (DED):

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Devices from the dropdown list. The Device List page displays.
3. Click on the Data Entry Device you wish to edit. The Device Details page displays.
4. Click Edit. The Edit Device page displays.
5. After you have finished making changes, click Save. You are returned to the Device Details page.

To delete a Data Entry Device (DED):

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device List page displays.
3. Click on the Data Entry Device (DED) you wish to delete. The Device Details page displays.
4. Click Delete. Click OK in the confirmation prompt. You are returned to the Device List page.

Special Options for Devices: IPAC Devices

	*NOTE:* *Before the installation and configuration of the IPAC device with the Brivo Onsite Server, please follow all preliminary instructions from Liftmaster to ensure the IPAC device is properly configured. Please refer to the IPAC Quick Start Guide on the Brivo website for further details.*

	*NOTE:* *IPAC functionality requires a license key. Without the license key, IPAC functionality will be disabled.*

The IPAC feature allows administrators to integrate IPAC Devices with the Brivo Onsite Server and utilize IPAC functionality, which includes:

- Creating a Directory Code for Residents in the Account Setup screen.
    - Alternately, if this functionality is added after the account has been set up, this feature can be applied from the Account Details page.
- Residents under the Users dropdown list.
- Resident Directory under the Users dropdown list.
- The ability to select IPAC Device from the New Device Type dropdown list.

To create an IPAC device:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Devices from the dropdown list. The Device List page displays.
3. Click Create New Device.
4. From the dropdown menu, select IPAC Device and click Next.
5. Enter the Name of the IPAC device in the Device Name field.
6. If available, select the Account Owner from the dropdown list.
7. Select the Control Panel from the dropdown list.
8. Enter the SIP Domain information.
9. Enter the Username.
10. Enter the Authorization ID if required.
11. Enter the Password.
12. Enter the Server Port (the default is 5060) in the field provided.
13. If required, enter the Outbound Proxy and Stun Server information.
14. Choose the Max. Call Time (default is 60 seconds).
15. Choose the Max. waiting time for call establish (default is 20 seconds).
16. Enter the IPAC Greeting Message in the field provided.

17. Enter the Speaker Volume (value from 0-100) (the default is 80).
18. Enter the MIC Volume (value from 0-100) (the default is 80).
19. Select the IPAC Directory from the dropdown list.
20. Choose which Device to link to Gate (1) from the dropdown list. Select the DTMF Key from the dropdown list (default is 9). Finally, if the Gate can accept an access code to allow entry, check the checkbox to Accept Access Code.

	***NOTE:*** *The DTMF (Dual Tone Multi Frequency) Key is the number a tenant would push on the telephone keypad to grant entry to someone calling from outside.*

21. Complete step 20 again for Gate 2.
22. Check the checkbox for SIP Diagnostic when required. Default is to have the checkbox unchecked.
23. When finished, click Save.

To edit IPAC Device:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Devices from the dropdown list. The Device List page displays.
3. Click on the IPAC Device you wish to edit. The Device Details page displays.
4. Click Edit. The Edit Device page displays.
5. After you have finished making changes, click Save. You are returned to the Device Details page.

To delete a Data Entry Device (DED):

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device List page displays.
3. Click on the IPAC Device you wish to delete. The Device Details page displays.
4. Click Delete. Click OK in the confirmation prompt. You are returned to the Device List page.

Special Options for Devices: NDE Gateways and Locks

The NDE Gateway and NDE Lock Device features allow administrators to assign and configure Allegion NDE gateways and locks attached to the Brivo Onsite Server.

	NOTE: *Allegion NDE functionality requires a license key. Without the license key, NDE functionality will be disabled.*

To create an NDE Gateway Device:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Devices from the dropdown list. The Device List page displays.
3. Click Create New Device.
4. From the dropdown menu, select NDE Gateway Device and click Next.
5. Enter the Name of the NDE Gateway Device.
6. Select the Control Panel from the dropdown list.
7. Select the NDE Gateway Address from the dropdown list.
8. When finished, click Save.

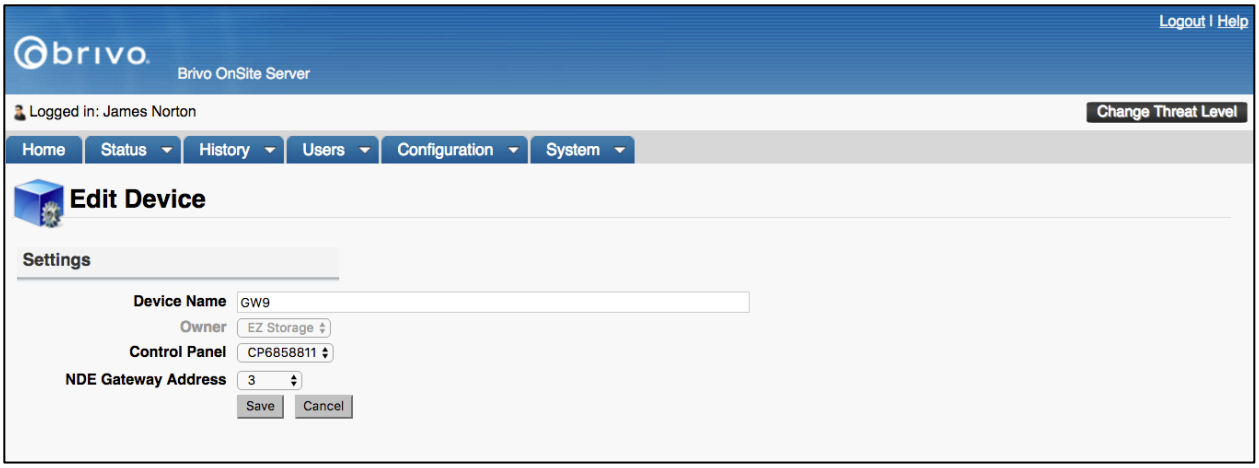


Figure 116. Create an NDE Gateway Device

To edit an NDE Gateway Device:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Devices from the dropdown list. The Device List page displays.
3. Click on the NDE Gateway Device you wish to edit. The Device Details page displays. If any NDE Lock Devices have been associated with the NDE Gateway, they will be displayed here under the Associated NDE Lock Device list.
4. Click Edit. The Edit Device page displays.
5. After you have finished making changes, click Save. You are returned to the Device Details page.

To delete an NDE Gateway Device:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device List page displays.
3. Click on the NDE Gateway Device you wish to delete. The Device Details page displays.
4. Click Delete. Click OK in the confirmation prompt. You are returned to the Device List page.

To create an NDE Lock Device:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Devices from the dropdown list. The Device List page displays.
3. Click Create New Device.
4. From the dropdown menu, select NDE Lock Device and click Next.
5. Enter the Name of the NDE Lock Device.
6. If available, select the Account Owner from the dropdown list.
7. Select the NDE Gateway Device from the dropdown list.
8. Select the NDE Gateway Address from the dropdown list.
9. Select an Unlock Schedule from the dropdown list.
10. Enter the Passthrough Period in seconds in the field provided (the default is 10).
11. If desired, check the Report Door Ajar checkbox to have the NDE Lock Device report door ajar events.
12. Enter the Ajar Delay in seconds in the field provided (the default is 120).
13. If desired, check the Cache Mode checkbox to have the NDE Lock Device use cache mode, allowing a certain number of credentials to be saved locally so that cached credentials continue to allow entry even with loss of communication.
14. When the Cache Mode checkbox is checked, if desired, check the Purge Unused Cached Credential After 5 Days to have any unused credentials older than five days purged from the system.
15. Enter the number of Maximum Cache Entries (from 0 – 1275) in increments of five.
16. To allow the NDE Lock Device to be operated from the website, check the Operate Device From Website checkbox.
17. When the Include failed access as alarm option is checked, system devices will be monitored from the Dashboard page. Instruction text, alarm priority, active scheduling, and threat level compliance may also be defined.
18. You may have the NDE Lock Device ignore Threat Levels or select under what Threat Level conditions the will operate.
19. You may select which groups have Access Permissions to the NDE Lock Device and under which schedules these permissions will operate.
20. For Allegion LE locks only, you may select to Enable Privacy Mode by checking the Enable Support For Privacy Mode checkbox. You may also select which group(s) have override privileges by checking the checkbox next to the group(s) name under the Override section.

	NOTE: *Allegion LE locks will blink three times at the 20, 40, 60, and 120 seconds and every 120 seconds thereafter when Privacy Mode is enabled.*

21. When finished, click Save.

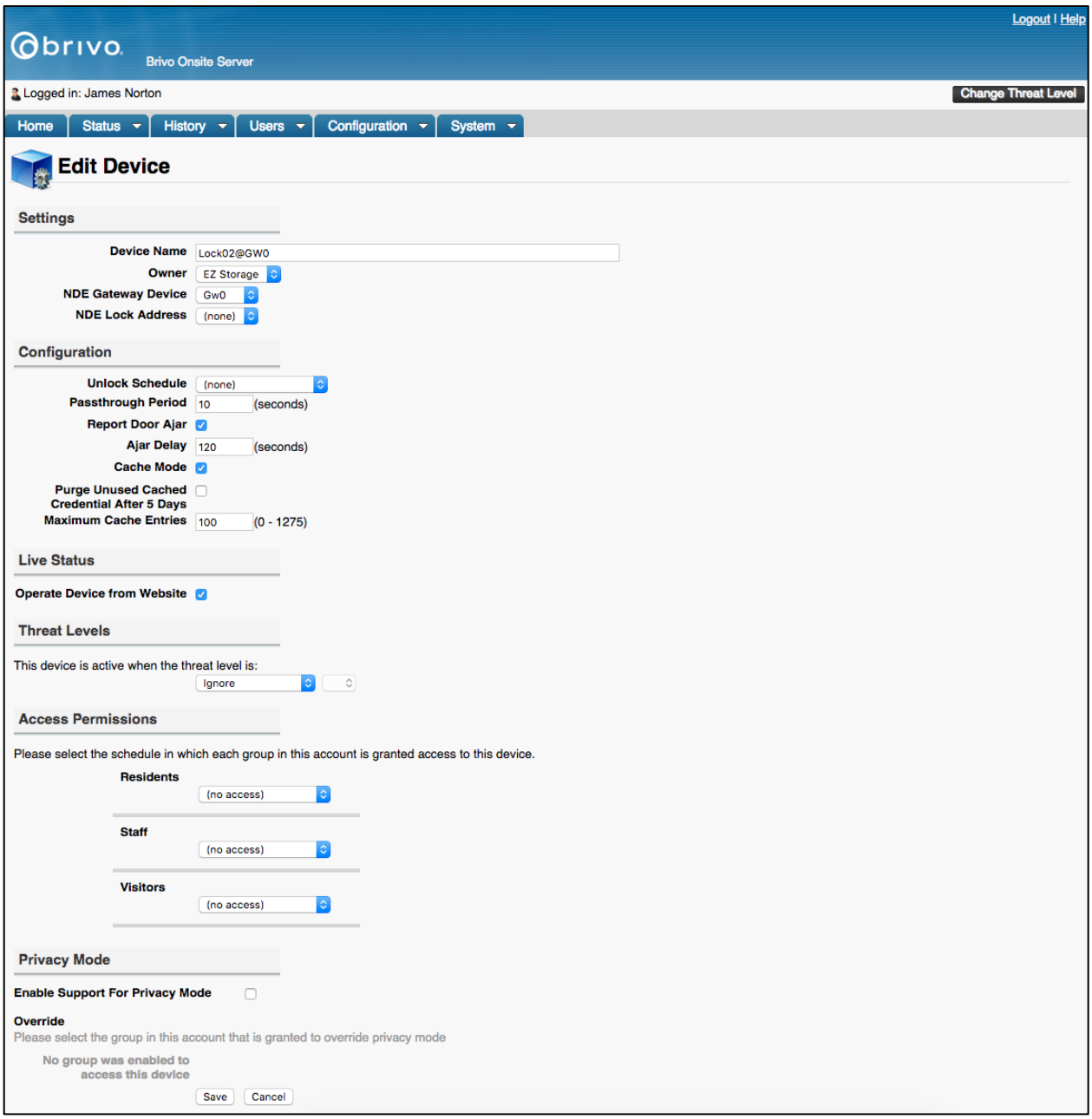


Figure 117. Create an NDE Lock Device

To edit an NDE Lock Device:

1. Scroll over the Configuration link. The sub-navigation menu displays.

2. From the sub-navigation menu, click Devices from the dropdown list. The Device List page displays.
3. Click on the NDE Lock Device you wish to edit. The Device Details page displays. If this NDE Lock Devices have been associated with any Groups, those permissions will be displayed here under the Access Permissions list. If there are any tenant accounts, if this NDE Lock Device has been made visible to any other accounts, those permissions will be listed under the Account Permissions list along with their Allowed Schedule.
4. Click Edit. The Edit Device page displays.
5. After you have finished making changes, click Save. You are returned to the Device Details page.

To delete an NDE Lock Device:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device List page displays.
3. Click on the NDE Lock Device you wish to delete. The Device Details page displays.
4. Click Delete. Click OK in the confirmation prompt. You are returned to the Device List page.

Viewing Video

When cameras and DVRs are in use, administrators with appropriate permissions have two options for viewing video. Administrators may watch live video via Live Status on the Dashboard (if the camera is set up to be controlled from the browser) or watch video related to specific access events under the Activity Log on the Dashboard.

	NOTE: *Live Video and Pulsing Doors/Devices* *In order to pulse a door/device using live video, the door/device being viewed must have the Control From Browser box checked under its device details. A device must also have its output set to Pulse.*

To view live video (with a Pulse button)

1. Scroll over the Status link. The sub-navigation menu displays.
2. Click on the Dashboard link. The Dashboard will display.
3. Under the Device Status tab of the Dashboard, locate the door at which you want to view live video.
4. Click the Camera Icon ( ) button next to door/device. The live video pop-up window will appear.

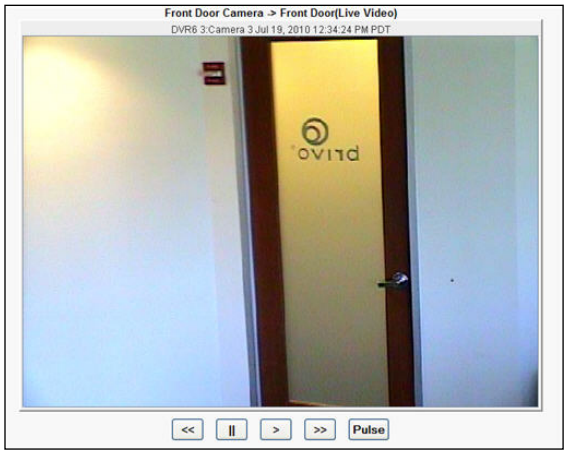


Figure 118. Viewing Live Video

	NOTE: *Playback Controls* *It is important to note that not all supported DVRs provide playback controls as shown above in Viewing Live Video.*

5. Use the buttons below the video to control play (if available).
   a) << to Rewind the video
   b) || to Pause or Stop the video
   c) > to Play the video
   d) >> to Fast Forward the video
   e) Pulse to pulse the door

To view live video (without a Pulse button)

1. Scroll over the Status link. The sub-navigation menu displays.
2. Click on the Dashboard link. The Dashboard will display.
3. Under the Device Status tab of the Dashboard, locate the camera you want to use to view live video.
4. Click the Live Video button next to the camera. The live video pop-up window will appear.
5. Use the buttons below the video to control play (if available).
   f) << to Rewind the video
   g) || to Pause or Stop the video
   h) > to Play the video
   i) >> to Fast Forward the video

To view event based video

1. Scroll over the Status link. The sub-navigation menu displays.
2. Click on the Dashboard link. The Dashboard will display.
3. Under the Activity tab of the Dashboard, choose the event you want to view.
4. Click the Camera Icon ( ) next to the device name. The event based video pop-up window will appear.

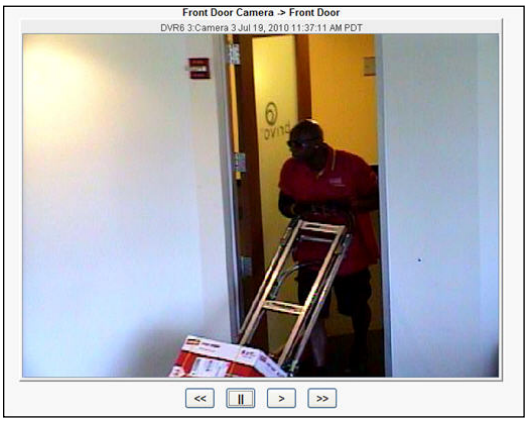


Figure 119. Event Based Video Playback

5. Use the buttons below the video to control play.
   j) << to Rewind the video
   k) || to Pause or Stop the video
   l) > to Play the video
   m) >> to Fast Forward the video

Viewing Panel and Board Details

Administrators with appropriate permissions can view the details for a control panel or control board.

To view details for a specific control panel and control board:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Control Panels from the dropdown list. The Control Panels list displays.
3. Click the control panel you want to view. The corresponding Control Panel Details page displays with details regarding the control boards on those panels.

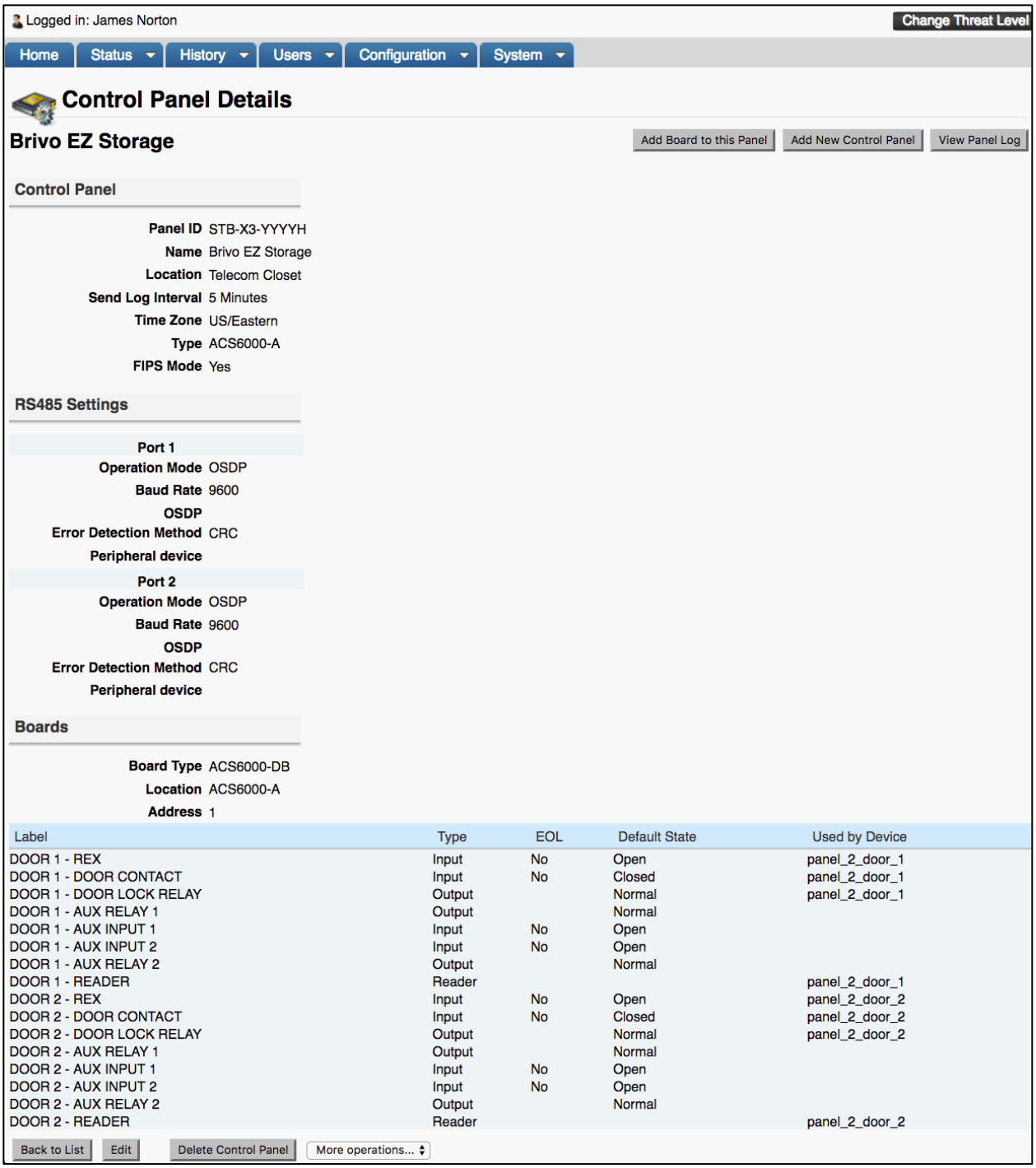


Figure 120. Control Panel Details

Details displayed include:

- Control Panel ID, Name, Location, Log Interval, Time Zone, Panel Type, and if FIPS mode is active.
- For ACS6000 (dual port) and ACS300 (single port) panels only, the RS485 Settings section details:
    - Port 1 and Port 2 lists:

- Operation Mode - Port 1 can be set to either Allegion RSI or OSDP Reader. Since Allegion NDE devices and OSDP use different protocols, the administrator needs to select the correct operation mode. For example, the administrator cannot set the Operation Mode to Allegion RSI and connect an OSDP reader. Port 2 will only accept OSDP readers (and is only available on ACS6000 panels).
- Baud Rate – This is the speed at which information is transferred over the line. The default is 9600.
- Error Detection Method – Allows the administrator to select either Checksum or Cyclic Redundancy Check (CRC) as the method used for error detection.
- Peripheral Device Address – Since RS485 is a bus and several devices can coexist on the same bus, there needs to be a method that different devices on the bus can be sent specific messages, and peripheral device addressing solves this problem.

- Label. For Door Boards, the label references a terminal node on the actual board. For IO Boards, this is a set of eight Input points and eight Output points.
- Type. Valid types include Input, Output and Reader. Reader is valid only for the Reader node on Door Boards.
- EOL. Indicates if the input point is wired for end-of-line supervision.
- Default State. Indicates if the point is normally open or normally closed.
- Used by Device. Indicates what device, if any, is currently wired to that point on the control board. Clicking the device name takes you to the corresponding Device Details page.

Administrators with appropriate permissions can:

Click Back to List to return to the Hardware list for this account.

Click Add New Control Panel to access a blank Add New Control Panel page in order to create a new control panel.

Click View Panel Log to access the Fetch Panel Log page to view or download the available panel logs for the control panel.

Click Edit on the Control Panel page to make changes to this control panel.

Click More Operations and perform the following three actions:

- Reboot Panel
- Reset Panel Data
- Reset Can Bus

	*NOTE: Use of any of the above three actions should only be performed at the request of Brivo Technical Support or by a certified Brivo technician.*

Click Delete Board to delete any control board.

Click Delete Control Panel to delete the control panel.

	*NOTE: On Brivo ACS5000-A panels, ACS6000-A panels, ACS300-A controllers, or ACS-IPDC controllers, since the Main Board cannot be deleted, the Delete button does not appear on the corresponding Board Details page.*

Update and/or Configure a Control Panel

The Hardware Status tab on the Dashboard allows you to configure the firmware in a given panel or panels, as well as choose whether you are configuring a control panel that is connected but not yet configured.

To configure your firmware on a control panel:

To upgrade and/or configure your firmware on a control panel, follow these steps:

1. To configure your panel, click the "Configure" tab next to the panel you wish to configure.

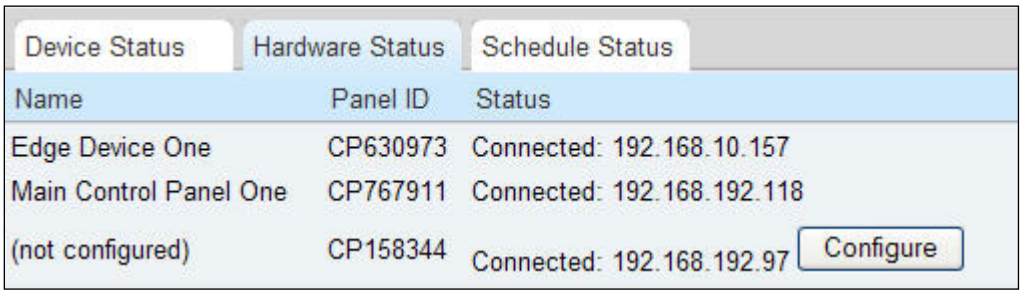


Figure 121. Configure Brivo Control Panel

2. A page will then display with the configuration options.
3. Enter the name of the panel.
4. Enter the panel's location.
5. Choose from the dropdown list the type of panel or device you are configuring. You may choose "ACS6000-A/Brivo Onsite", "ACS5000-A", "ACS5000-S", "ACS300-A", "ACS-IPDC-1A", "ACS-IPDC-2A", or "HID E-400/ERW-400."
6. Click Save.

Control Panel Options

To add a new control panel:

You may choose to add a new control panel that has not yet connected to the Brivo Onsite Server appliance by following these steps:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Control Panels from the dropdown list. The Control Panels list displays.
3. Click Add New Control Panel.
4. Enter the Panel ID Number. This is the number that begins with the letters "CP" and can be found printed on the packaging, inside the panel's cover, or on a sticker on the panel's main board.

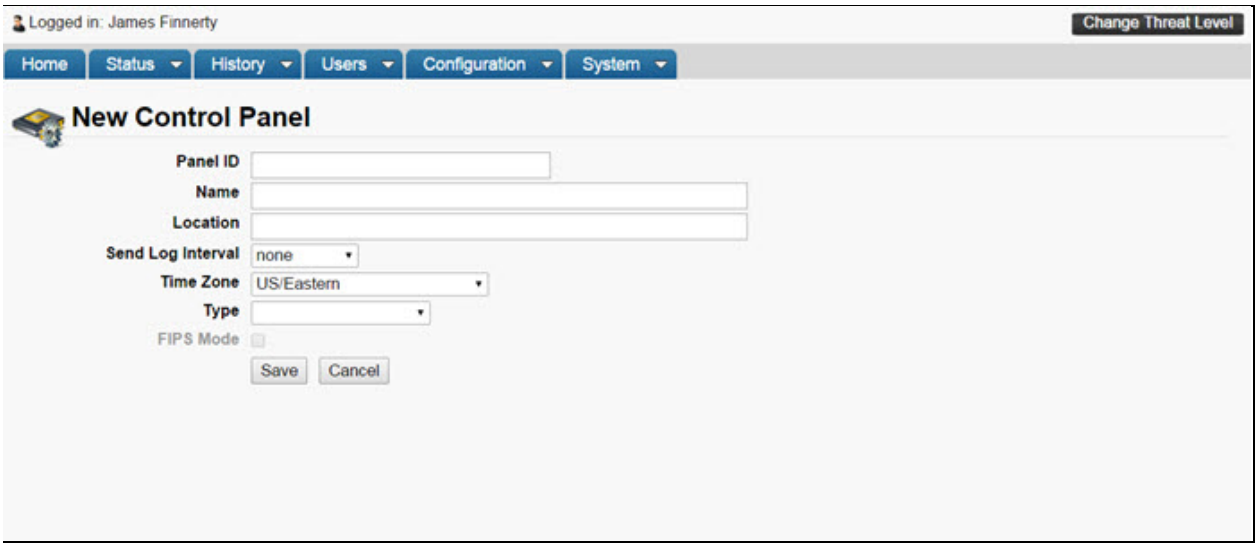


Figure 122. Add a Control Panel

5. Enter a name for the panel.
6. Enter the location of the panel.
7. If desired, enter the time interval when the control panel will upload a panel log file.
8. Enter the time zone for the panel.
9. Choose whether you are adding a Brivo ACS6000-A/Brivo Onsite panel, a ACS5000-A panel, a Brivo ACS5000-S panel, a Brivo ACS300-A controller, an HID E-400/ERW-400, a Brivo ACS-IPDC-1A controller, or a Brivo ACS-IPDC-2A controller.
10. Click Save.
11. For ACS6000 and ACS300 panels only, the RS485 settings default to OSDP for Port 1 and Port 2. To change these settings, click Edit at the bottom of the Control Panel Details page and follow the instructions in the Viewing Panel and Board Details above.

To edit a control panel:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Control Panels from the dropdown list. The Control Panels list displays.

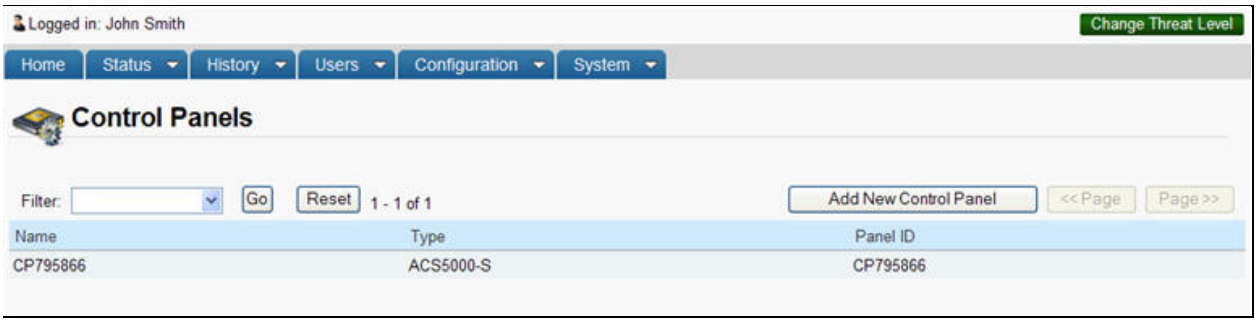


Figure 123. Devices: Control Panels

3. Click on the control panel you wish to edit. The Control Panel Details page displays.
4. At the bottom of the page, click Edit. The Edit Control Panel Details page displays.

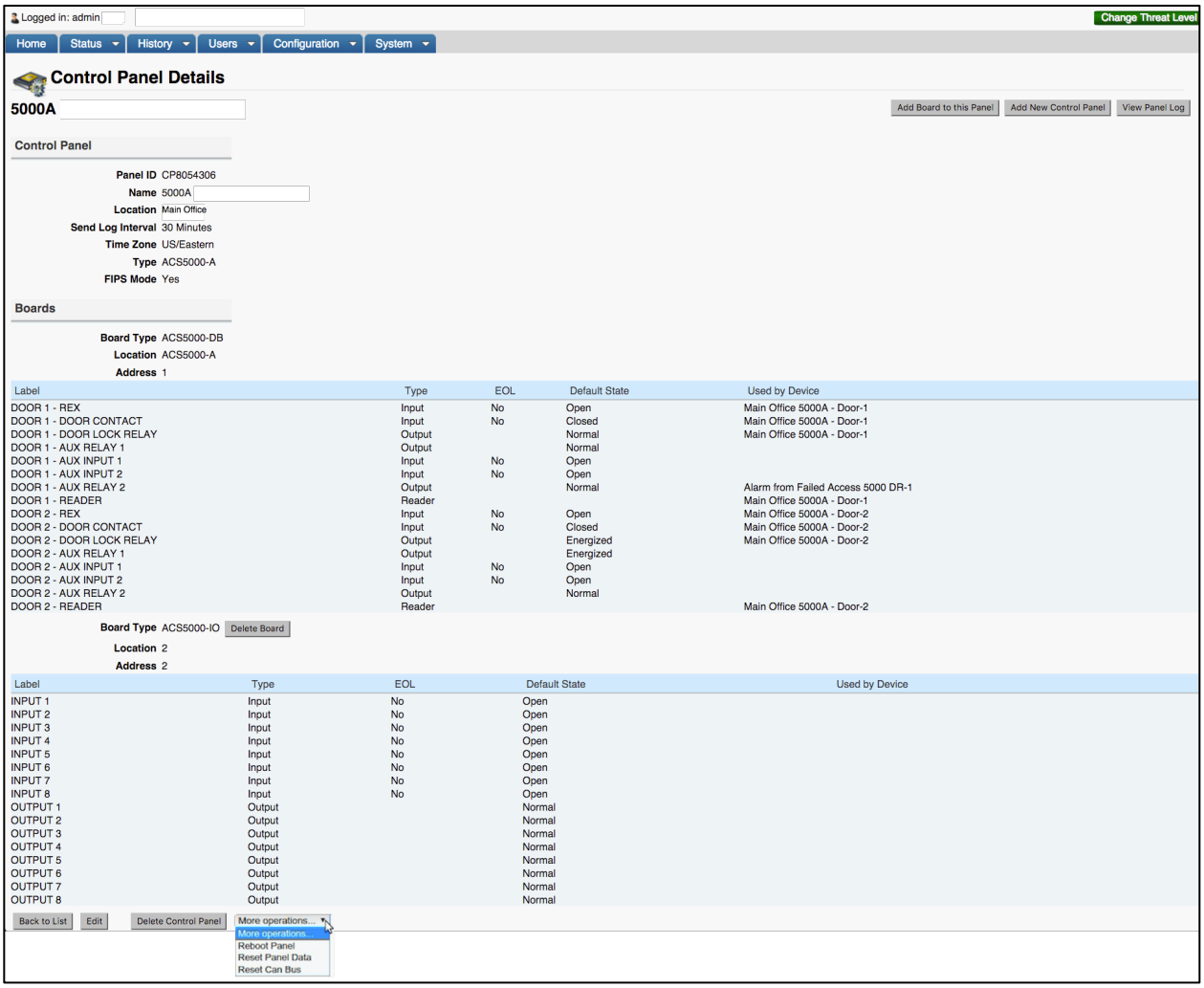


Figure 124. Devices: Edit Control Panel Details

5. After making changes to the control panel, click Save. You are returned to the list of control panels.

To perform a change to Panel communications (Reboot Panel, Reset Panel Data, or Reset Can Bus)

WARNING: PANEL REBOOT

This operation should only be performed if advised by Brivo Technical Support and should only be performed by a Certified Brivo Integrator.

Doors will be unresponsive and may be non-secure during a reboot. If the panel fails to boot after this operation is complete, doors will be left unresponsive and may be a sign of more severe issue.

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Control Panels from the dropdown list. The Control Panels list displays.
3. Click on the More Operations dropdown list at the bottom of the page.
4. Select which operation you wish to perform. You are returned to the Edit Control Panel page and the action you performed will appear in the Activity Log.

NOTE:

The Reset Can Bus function will not appear in the dropdown list for ACS-IPDC units.

To delete a control panel

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Control Panels from the dropdown list. The Control Panels list displays.
3. Click on the control panel you wish to delete. The Control Panel Details page displays.
4. At the bottom of the page, click Delete Control Panel. Click OK when at the confirmation prompt. You are then returned to the list of control panels.

Adding Control Boards

Administrators with appropriate permissions can add a control board.

To add a control board to an account:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Control Panels from the dropdown list. The Control Panels list displays.
3. Click on the panel where you would like to add a board. The Control Panel Details page displays.
4. Click Add Board to this Panel. The Add New Board page displays.

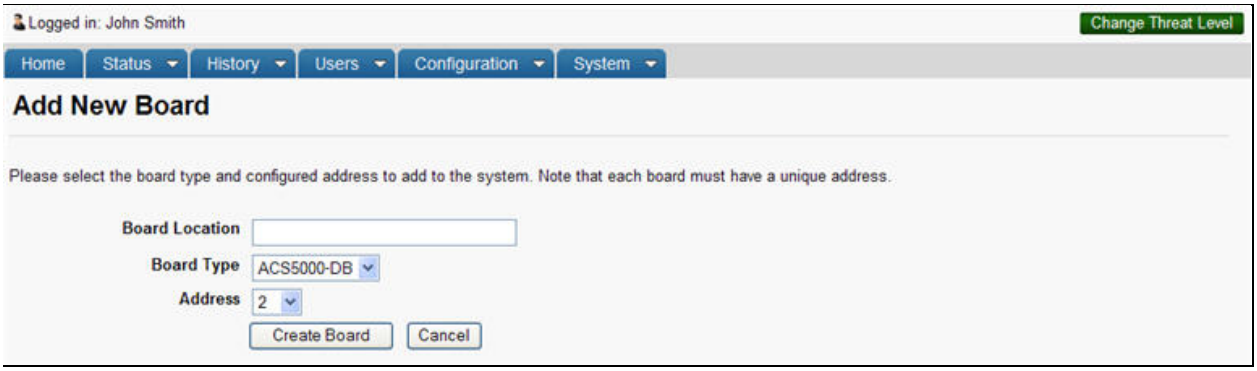


Figure 125. Add New Board

5. In the Board Location field, enter a brief description of the board's location, such as "Server Room."
6. Select the correct Board Type from the drop-down list.
7. In the Address field, assign a number to this board. The drop-down list includes all valid board numbers (2-15) not currently in use.

	NOTE: *When the Brivo Control Panel is first configured, one Door Control Board is automatically associated with it and assigned Address 1. This is the Main Board for the system, and it cannot be deleted.*

8. Click Create Board. The Control Panel Details page displays.

Managing Control Boards

Once the control board is created, you must configure it as part of the control panel it belongs to on the Edit Control Panel Details page.

Administrators with appropriate permissions can configure or delete control boards.

To edit a Door Board:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Control Panels from the dropdown list. The Control Panels list displays.
3. Click the control panel that contains the board you would like to edit. The Control Panels Details page displays.
4. Click Edit at the bottom of the page. The Edit Control Panel Details page displays.

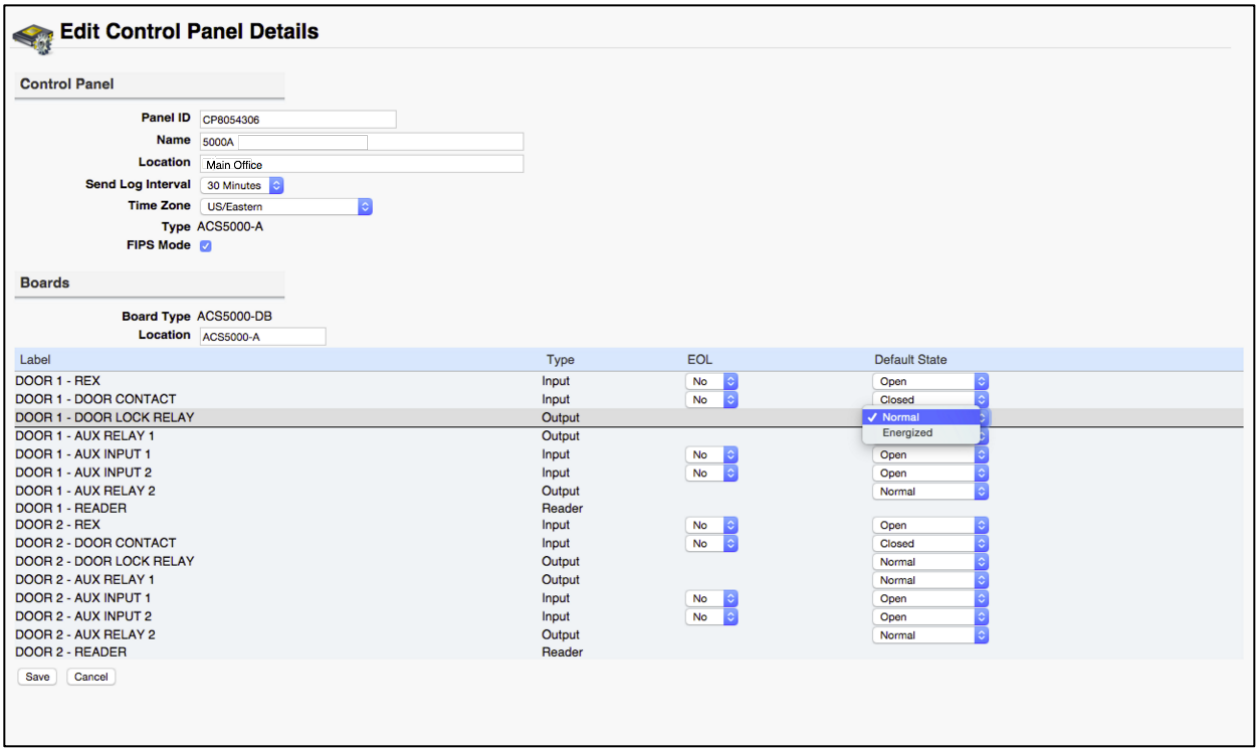


Figure 126. Define Door Board Settings

5. The Location field for each control board can be edited on this page.
6. Each Door Board contains two nodes, each of which can be used to control either one door or one door and multiple devices. On this page, these two nodes are identified as DOOR 1 and DOOR 2, and for each there is a set of input and output points that correspond to a block of terminals on the actual Door Board. All of the labels match the exact text silk-screened on the control board.

	NOTE: *A Door Board node does not have to be used to control a door; it can be used to control any number of devices. However, the following terminal blocks cannot be used by any other device if the node is to be used for a door: REX, DOOR CONTACT, and READER.*

7. For each input point, there is a set of fields used to define the operation of the associated terminals.
    - In the EOL field, click Yes or No to indicate if the input point is wired for end-of-line supervision.
    - In the Default State field, click Open to indicate that the input point is normally open, or Closed to indicate that it is normally closed.
8. For each output point, there is a set of fields used to define the operation of the associated terminals.
    - In the Default State field, click Normal to indicate that the output point operates in a fail-secure mode. Click Energized to indicate that the output point operates in a fail-open mode.

	*NOTE:* *The following three steps must be completed in order to utilize Fail-Open functionality in Brivo Onsite Server:* 1. *Mode set to Fail-Open* 2. *Correctly wired for Fail-Open* 3. *Fail-Open style door lock must be used* *Simply changing mode to Fail-Open from a system that had been configured for Fail-Secure operations is not sufficient to achieve Fail-Open operation.* *For more information on fail-open functionality, please review the Brivo Fail-Open Wiring Technical Note.*

9. Click Save. The Control Panel Details page displays.

To edit an IO Board:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Control Panels from the dropdown list. The Control Panels list displays.
3. Click the control panel whose IO board you would like to edit. The Control Panels Details page displays.
4. Click Edit at the bottom of the page. The Edit Control Panels Details page displays.
5. Edit the information in the corresponding fields of the IO board.

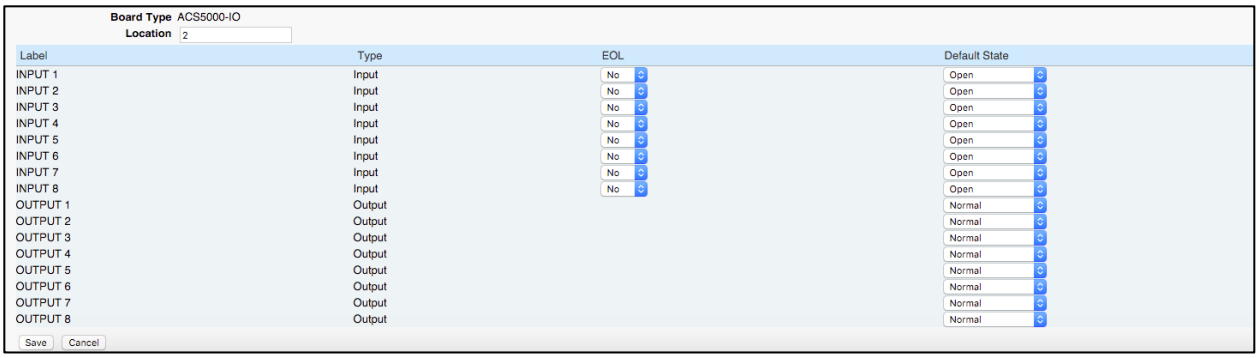


Figure 127. Define IO Board Settings

6. You can define up to eight inputs and eight outputs for each IO Board. Points can be shared by more than one device, and some devices use multiple points; therefore, the number of devices controlled by an IO Board is undefined.
7. For each input device, there is a set of fields used to define the operation of the associated terminals
    - In the EOL field, click Yes or No to indicate if the input point is wired for end-of-line supervision.
    - In the Default State field, click Open to indicate that the input point is normally open, or Closed to indicate that it is normally closed.
8. For each output point, there is a set of fields used to define the operation of the associated terminals.
    - In the Default State field, click Normal to indicate that the output point operates in a fail-secure mode. Click Energized to indicate that the output point operates in a fail-open mode.
9. Click Save. The Board Details page displays.

To delete a control board:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Control Panels from the dropdown list. The Control Panels list displays.
3. Click on the control panel whose board you wish to delete. The corresponding Control Panels Details page displays.
4. Next to the type of control board is a "Delete Board" button. Click Delete. A message displays warning that this operation cannot be undone.
5. Click OK to complete the deletion and return to the Control Panels Details page with the deleted control board no longer listed.

	NOTE: *When a control board is deleted, all dependent information is also removed from the system. For example, any device using points on that board will lose its hardware configuration and revert to a simple unconfigured state.*

Browsing the Devices List

All Administrators can view the complete list of devices for their account.

To view the devices associated with a specific account:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Control Panels from the dropdown list. The Control Panels list displays.

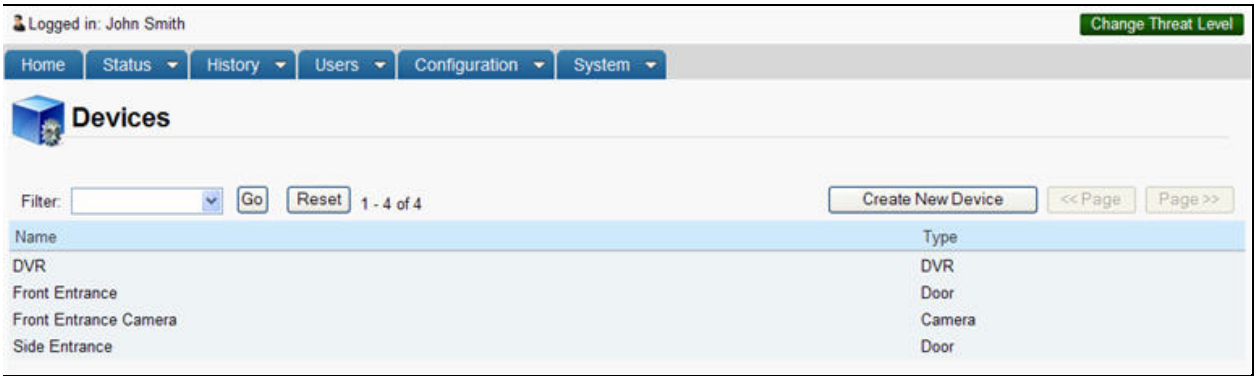


Figure 128. View Devices List

Details displayed include:

- This page lists all the devices currently defined for the account.

Administrators with appropriate permissions can:

Click a device to access the associated Device Details page.

Click Create New Device to access a blank Edit Device page in order to create a new device.

Viewing Device Details

All Administrators can view the details for any device associated with their account.

To view details for a specific device:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Control Panels from the dropdown list. The Control Panels list displays.
3. Click the device you want to view. The corresponding Device Details page displays. The layout of this page varies slightly depending on the type of device you are viewing.

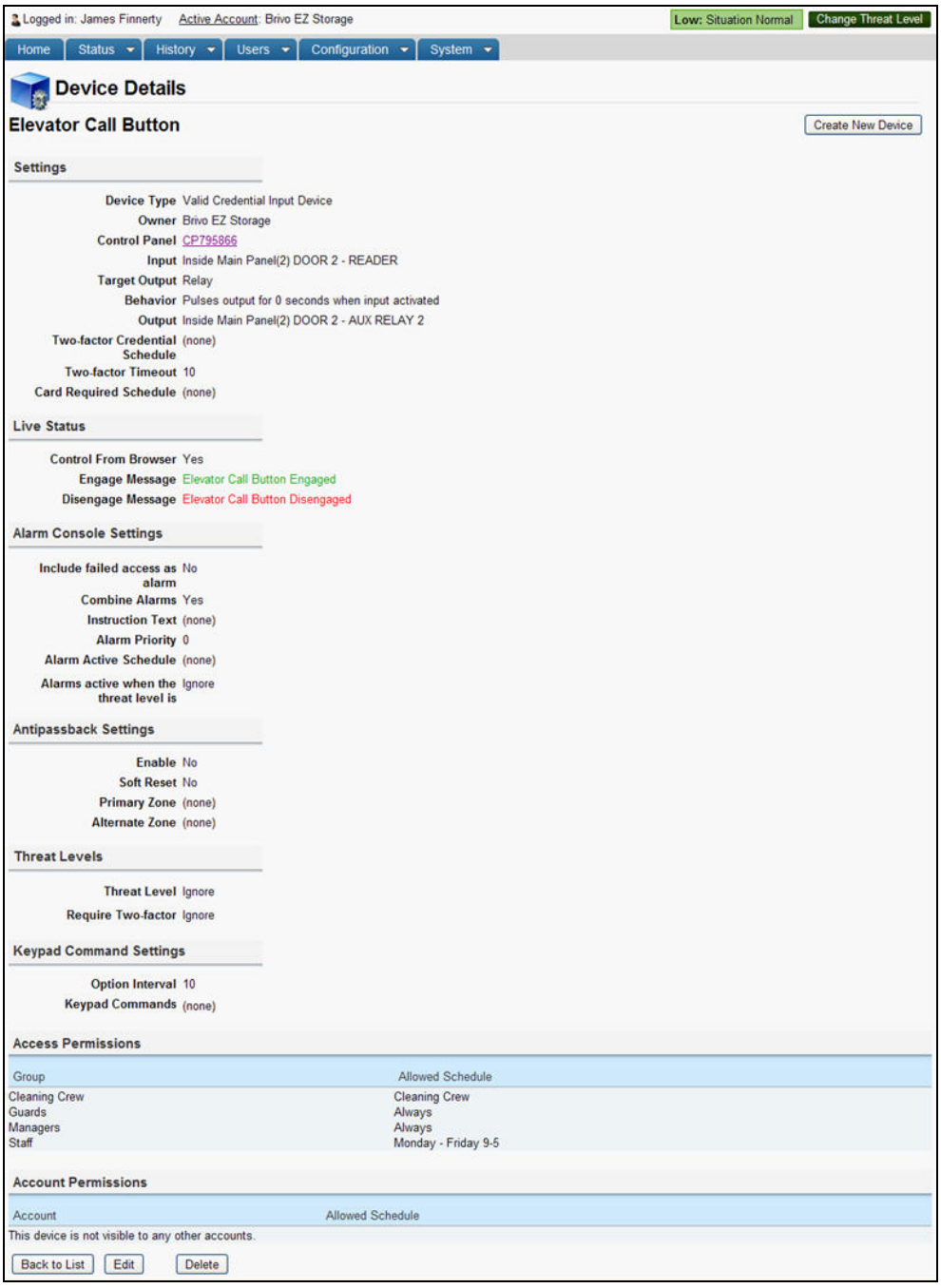


Figure 129. Device Details: Valid Credential Device

Details displayed include:

- Details displayed on this page vary depending on the device being viewed. See the following section, *Creating Devices,* for more information.

Administrators with appropriate permissions can:

Click the name of the Two-factor Credential Schedule or Card Required Schedule, if one is identified, to access the corresponding Schedule Details page.

Click a group name under Access Permissions to view the corresponding Group Details page.

Click Back to List to return to the Devices list for this account.

Click Create New Device to access a blank Edit Device page in order to create a new device.

Click Edit to access the Edit Device page.

Click Delete to delete the device.

Creating Devices

Administrators with appropriate permissions can create devices.

To create a device for an account:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Control Panels from the dropdown list. The Control Panels list displays.
3. Click Create New Device. The Edit Device page displays.

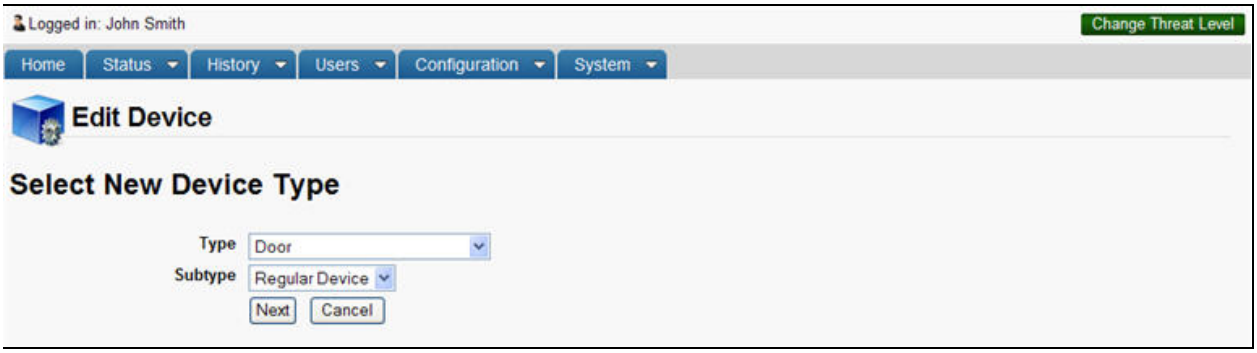


Figure 130. Create a Device

4. Select the Device type you want to create. See the *Glossary* at the end of this document for a brief description of each type.
5. Click Next. The Edit Device page displays. This page varies noticeably according to the device being created. Enter the appropriate fields for the device you have chosen. For editing devices, see the section on Configuring Devices for more details.

Device Profiles

The Device Profile feature allows for the creation of a profile that can be simultaneously assigned to multiple devices, giving all such devices identical settings. Hardware aspects of the device profile, like assigning a node or relay, must be chosen later at the time you create the actual device.

Features:

Creating a device profile allows users to differentiate between types of devices and device subtypes

Allows users to create devices with the same settings

To Create a Device Profile:

1. Scroll over the Configuration link at the top of any page. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device List page displays.
3. Click Create New Device. The Create New Device page displays.
4. From the device type dropdown list, select the device type you wish to create the profile for. From the device subtype dropdown list, select "Device Profile." Click Next.

	*NOTE:* *Cameras, DVRs, Muster Points, Keypad Command devices, and Guard Tour devices do not allow for the creation of device profiles.*

5. Enter the name of the Device Profile.
6. Choose the owner of the Device Profile from the dropdown list.
7. Assign the Device Profile the necessary configuration just like you would when creating a new device of the same type.
8. Click Save. You are returned to the Device Details page.

To Apply a Device Profile:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device List page displays.
3. Click Create New Device.
4. From the device type dropdown list, select the device type you wish to create. From the device subtype dropdown list, select "Regular Device." Click Next.
5. Enter the name of the device.
6. Choose the owner of the device from the dropdown list.
7. Choose the device profile from the dropdown list.
8. Click Save. You are returned to the Device Details page.

To Edit Settings on a Device Profile:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device List page displays.
3. Click on the device profile you wish to edit. The Device Details page displays.

	*NOTE:* *Under the section Devices Using This Profile, all devices currently using that device profile are listed.*

4. Click Edit. The Edit Device page displays.
5. After you have finished making changes, click Save. You are returned to the Device Details page.

To Delete a Device Profile:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices from the dropdown list. The Device List page displays.
3. Click on the device profile you wish to delete. The Device Details page displays.
4. Click Delete. Click OK in the confirmation prompt. You are returned to the Device List page.

Live Status

When logging into the Brivo interface, the Dashboard link displays the live status of a door or device on the right-hand side. For example, depending on its position, the status of a door will be displayed on the Dashboard under "Device Status" as "open" or "closed."

Under the "Device Status" heading, messages display in various colors the status of the device. You may choose to customize the message displayed for programmable devices. You can also select the color for the message you wish to display.

Programmable Devices

You can customize the live status message of the following devices:

- Switch Input Devices
- Event Triggered Devices
- Valid Credential Input Devices
- Schedule Controlled Device

To customize Live Status message

1. Scroll over the Configuration link at the top of any page. The sub-navigation menu displays.
2. From the Devices link, click Devices. The Device List page displays.
3. If you want to modify an existing device's message
4. Click on the device whose message you wish to modify.
5. At the bottom of the page, click Edit.
6. Under the "Live Status" heading, check the box "Control from browser." The "Engage Message" and "Disengage Message" fields will become active.
7. Enter the message you wish to be displayed on the Dashboard in the respective fields.
8. Click Save.

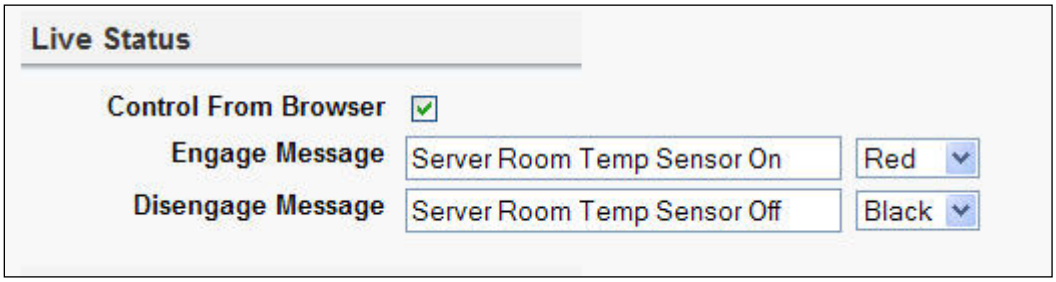


Figure 131. Customize Live Status Message

Color Coding the Status of a Programmable Device

You may also choose to select specific colors to indicate the status of a Programmable Device, such as a Switch Input Device, an Event Triggered Device, a Valid Credential Input Device, or a Schedule Controlled Device. This decreases the time it takes for you to search for a particular event on the Live Status page.

To customize the color of the Live Status message:

1. Scroll over the Configuration link at the top of any page. The sub-navigation menu displays.

2. From the Devices link, click Devices. The Device List page displays.
3. If you want to modify an existing device's message color:
4. Click on the device whose color you wish to modify.
5. At the bottom of the page, click Edit.
6. Under the "Live Status" heading, check the box "Control from browser."
7. The "Engage Message" and "Disengage Message" fields will become active.
8. Choose from the dropdown list the color you would like the message to be displayed in.
9. Click Save.

Managing Devices

Once a device is created, you must configure it on the Edit Device page. You are taken to this page automatically when you first add the device, but can return to it at any time to edit the device's settings.

To configure a device:

1. Scroll over the Configuration link at the top of any page. The sub-navigation menu displays.
2. From the Devices link, click Devices. The Device List page displays.
3. Click the device you want to configure. The corresponding Device Details page displays.
4. Click Edit. The Edit Device page displays.

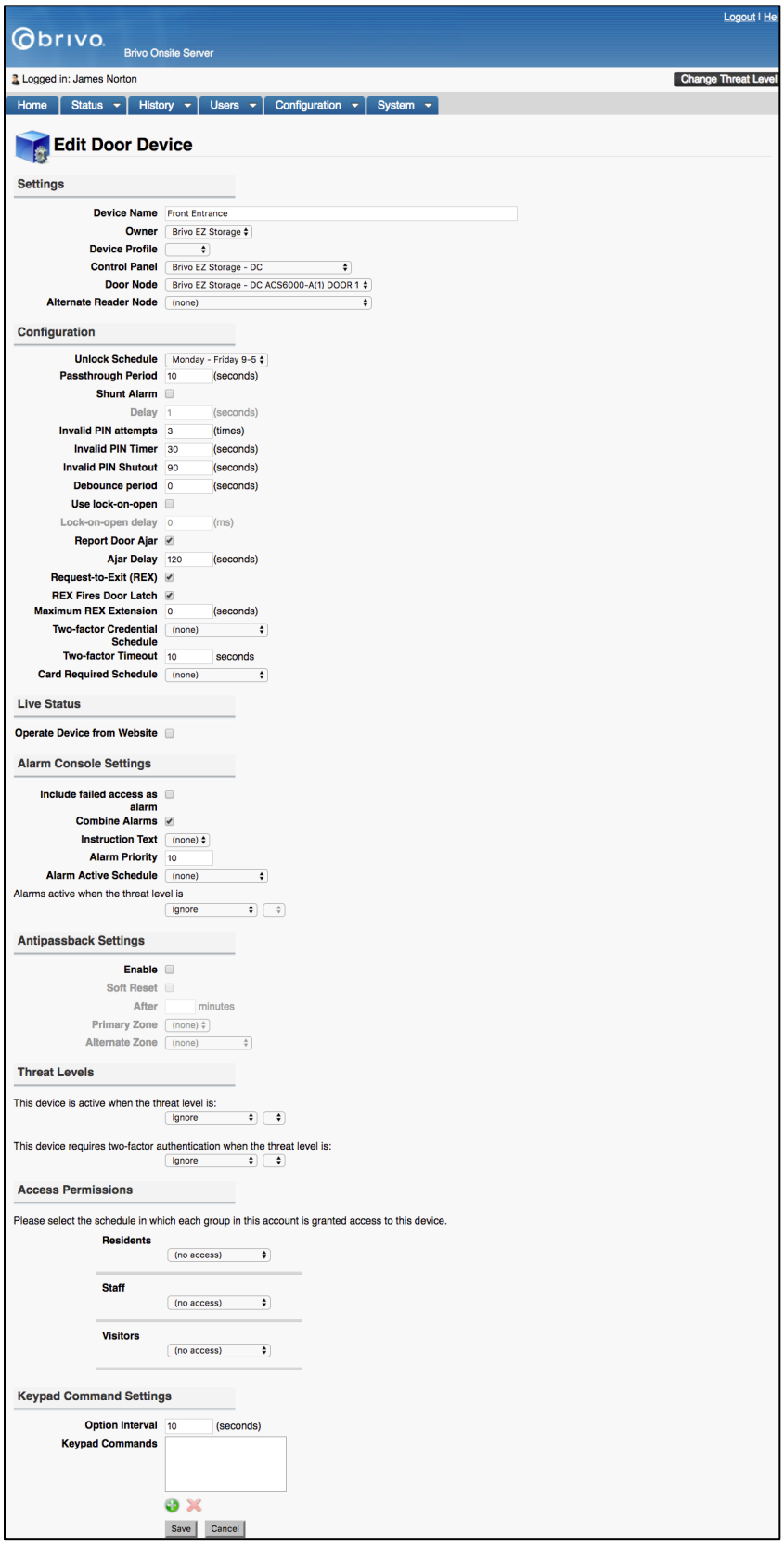


Figure 132. Configure a Door

A subset of the following fields displays on the Edit Device page, depending on the type of device you are configuring.

1. Name is a required field for any type of device. The name you enter should be brief, but descriptive.
2. Owner is also a required field for all device types and identifies the account responsible for the device. The default value in the drop-down list is the current account.
3. Device Profile is an optional field that allows a predefined device profile to be used instead of setting up the device manually.
4. Control Panel is a required field that identifies to which control panel the device will be assigned.
5. The Door Node field displays only when you are configuring a Door. Although this page does not require you to select a control board/point combination from the drop-down list, the door will not function until you do. The list includes all valid, available door nodes.
6. The Alternate Reader Node is used if you would like the door to be controlled by two readers. You may configure Antipassback controls for an alternate reader by selecting a Node from the Alternate Reader drop-down list.
7. The Input drop-down list displays only when you are configuring either an Input Switch or Valid Credential Input Device, and includes all valid, available input terminals.
8. The Input Device and Event dropdown lists are valid for Event Trigger devices only. The Input Device list includes all doors associated with this account, while the Event list lets you identify a specific access event, such as Door Forced Open that will cause the selected output behavior to occur.
9. The Target Output dropdown lists are valid for all device types. Relay will apply the selected Output Behavior, Schedule will apply the selected Output Behavior to the Target Schedule, and Threat Level sets the Target Threat Level.
10. The Output Behavior varies dependent upon which device type or target output is selected and include: Pulse, Follow, Latch, Unlatch, Toggle, Activate, Deactivate, and Set Threat Level.
11. Output Behavior is a valid field for all device types other than Door. From the drop-down list, select the behavior you want to occur in response to the identified input. See the *Glossary* at the end of this document for a brief description of each output behavior type.
12. When an output behavior of either Pulse or Follow is selected, the second(s) delay field becomes active. Enter the amount of time, in seconds, that should elapse between when the input is deactivated and the output released (for Follow) or the total amount of time the output should be engaged for each time the input goes to an activated state (for Pulse.)
13. The Unlock Schedule dropdown list displays only when you are configuring a Door, and is used to indicate the schedule period during which the door should be left unlocked.
14. The Output field displays when you are configuring an Input Switch, Valid Credential Input, or Event Trigger device. Click the  icon to choose the Output relay for any of these devices.
15. Under the Relay column, click on the (Click to select panel) area and the control panel list popup will appear. Select the appropriate control panel and then select which relay from the dropdown list.
16. The Active Schedule dropdown list displays when you are configuring any device other than a Door, and is used to indicate the schedule periods during which the device should operate.

	*NOTE:* *Devices and schedules must belong to the same account. When you change the Owner, any Schedule dropdown lists automatically reload to include all schedules defined for that account.*

17. For Doors, set Passthrough, Invalid PIN, Door Ajar, and Request-to-Exit parameters:

    - In the Passthrough Period field, enter the maximum length of time (1-99999 seconds) the door should remain unlocked after a user presents his or her credentials and is authenticated or presses a Request-to-Exit switch. For example, if this value is set to 15, the user has 15 seconds to pass through the door before it automatically re-locks. The default setting is 10.
    - Check the Shunt Alarm box if the door is connected to an alarm system that should be shunted (temporarily disabled) for a specified period of time after the pass-through period has expired. The shunt time is in addition to the passthrough period. For example, if Pass through Period is set to 10 seconds, and Shunt Alarm Delay is 1 second, the alarm will engage only if the door remains in an open state for more than 11 seconds after the user is authenticated.
    - When the Shunt Alarm box is checked, enter the length of time (1-99999 seconds) the alarm system should be shunted in the Delay field. The default and strongly recommended setting is one.

	***WARNING:*** Alarm Shunt Restrictions *If any device is connected to the AUX RELAY 1 terminal block on the Door Board, the Alarm Shunt feature cannot be enabled. Both the Shunt Alarm and Delay fields are inactive and a message displays indicating that there is no alarm shunt available for this door node.*

    - In the Invalid PIN attempts field, indicate the maximum number of consecutive invalid PINS that can be entered in the door's keypad (1-99) before it is considered a security risk and the keypad freezes. The default setting is three.
    - In the Invalid PIN timer field, specify the amount of time (1-99999 seconds) allowed for each attempted PIN entry. For example, if this field is set to 30, and Invalid PIN attempts is set to 3, a person would have 90 seconds total (30 seconds per attempt) to enter a valid PIN before the keypad freezes. The default is 30.
    - The Invalid PIN shutdown field lets you set the length of time (1-99999 seconds) the keypad should remain frozen if the maximum number of invalid PINs or the PIN timer is exceeded. The default setting is 90.
    - In the Debounce period field, specify the amount of time (1-255 seconds) that the device will delay after a door closure is detected, before triggering a door forced open message. The default setting is zero.

- Check the Lock-on-Open box to indicate that you want to enable the Lock-on-Open feature. In certain installation situations, it is desired that the lock re-enable upon detection of a door opening event. If you want a delay before Lock-on-open engages, specify the amount of time (in milliseconds) in the field provided.
- Check the Report Door Ajar box to indicate that you want to enable the Door Ajar feature. This feature controls how long a door can be left propped or held open before it is considered a security risk, causing the event to be recorded in the Activity Log. The default setting is checked.
- If the Door Ajar feature is enabled, use the Ajar delay field to indicate the maximum length of time (1-99999 seconds) the door can be left ajar without causing a security violation. The default setting is 120.
- Check the Request-to-Exit (REX) box to indicate that a Request-to-Exit (REX) motion sensor is in use for the door. With a REX switch, if the door is opened without a credential or a request to exit, the Activity Log records a Door Forced Open event and an optional email notification is sent. The default setting is checked.

	*NOTE:* *A Request-to-Exit motion sensor (as opposed to a wall-mounted button) can fail to engage if a person exits too quickly. Likewise, if a person engages the motion sensor, then waits for the sensor to disengage, then pushes the door open, the "request" will not be processed. In either case, the system will log a Door Forced Open event.*

- Check the REX fires door latch field to indicate that the REX switch causes the door to unlock. The default is checked.
- The Maximum REX Extension field lets you set the maximum length of time (1-99999 seconds) for the complete pass through period in the presence of continual REX triggers being received by the controller. If the REX trigger is stuck in an "active" state or is being triggered over and over, the total passthrough period will become the Maximum REX Extension plus the passthrough period. The default setting is zero.

18. For Doors and Valid Credential Input Devices, you can define a time during which two-factor credentials are required; i.e., a period of time during which a user must provide both a card and a PIN.
    - On the Two Factor Credential Schedule dropdown list, click the schedule during which you want this door to require two credentials. During the selected time period, users with privileges at this door will need scan a security card *and* enter a PIN to gain access.
    - In the Two Factor Timeout field, enter the amount of time (1-99999 seconds) the user will have to present both credentials. If the user takes more than the allotted time, access will be denied.
19. For Input Switch, Schedule Controlled, and Event Trigger devices set report engage and disengage parameters:

- Check the Report Engage box to indicate that engagement of this device should be reported in the Activity Log. The default is checked.
- If Report Engage is checked, enter a Message to be used in the Activity Log, such as "Motion detected."
- Check the Report Disengage box to indicate that disengagement of this device should be reported in the Activity Log. The default is checked. This field is not valid for Event Trigger devices.
- If Report Disengage is checked, enter a Message to be used in the Activity Log, such as "Motion subsided." This field is not valid for Event Trigger devices.

20. For Doors, Valid Credential Devices, Input Switches, Schedule Controlled Devices, and Event Triggers, you can select a schedule during which presentation of a card is required.
    - On the Card Required Schedule dropdown list, click the schedule during which you want this door to require the presentation of a card credentials. During the selected time period, users with privileges at this door will need scan a security card.

	*NOTE:* *If both Two-Factor and Card Required are selected, Two-Factor Credential Schedule takes precedence over Card Required and so a user will be required to present both a security card and a valid PIN to gain access.*

21. When the Operate Device from Website option is checked, system devices configured with an output behavior of Pulse, Latch or Unlatch will be monitored and controllable from the Dashboard page.

	*NOTE:* *This control mechanism does not apply to devices for which the Follow output behavior has been defined.*

22. When the Include failed access as alarm option is checked, system devices will be monitored from the Dashboard page. Instruction text, alarm priority, active scheduling, and threat level compliance may also be defined.
23. When the Enable option is checked, the Antipassback Settings are active, allowing for soft reset (if checked) after a number of minutes (1-99999). Primary and Alternate Zones may also be defined.
24. You may have the device ignore Threat Levels or select under what Threat Level conditions (including requiring two-factor authentication) the device will operate.
25. The Access Permissions section of the page displays only when a Door or Valid Credential Input device is being configured, and lists all user groups currently defined for the owner account. Two groups are defined automatically when the System Account is first created: "Staff" and "Visitors." For each group, select the schedule according to which the group has access to this door or Valid Credential device.
26. If tenant accounts exist, under the Account Visibility section you may select the schedule each account can use to assign its groups access to this device. Note that this makes the device 'shared' among accounts, making this schedule visible to any account with access to this device.

27. You may add a Keypad Commands by clicking on the icon and selecting an available keypad command from the popup window. Once selected, you are returned to the Device Details page.
28. Click Save. The Device Details page displays.

To delete a device:

1. Scroll over the Configuration link at the top of any page. The sub-navigation menu displays.
2. From the Devices link, click Devices. The Device List page displays.
3. Click the device you want to delete. The corresponding Device Details page displays.
4. Click Delete. A message displays warning that this operation cannot be undone.
5. Click OK to complete the deletion and return to the Devices page with the deleted device no longer listed.

	NOTE: *When a device is deleted, all permissions to it are revoked from all accounts and groups.*

15.Schedules and Holidays

What are Schedules?

A *schedule* is an editable, reusable time template that can be used to control such things as when a door is accessible or when a device is activated. A user's access privileges are the result of a three-way relationship that is created between: (1) a group of users, (2) a secured device, and (3) a schedule.

A group of users is permitted access to a device, such as a door, according to a predefined schedule. This access is granted on the Edit Group page. (Refer to the section on *Creating a Group*.) This page lets you define access to single door or device differently for individual groups of users. For example, the group "Staff" may have access to the "Front Door" according to the schedule "Work Day," which allows them to access the door, using a valid credential, between the hours of 7:00AM and 6:00PM. At the same door, the group "Cleaning Crew" may have access according to the "Night Shift" schedule, permitting them access only during the hours of 8:00PM and midnight.

Schedules also allow one-time active or inactive blocks to be defined. For example, if a training session will be taking place at 7:00 PM to 10:00 PM on the 1st of the month, the "Work Day" schedule can add a one-time change to the schedule allowing the "Staff" group to have access to the facility until 10:00 PM on that day. Additionally, monthly recurring schedule blocks can be defined as well, for example, if the training session were to become a monthly occurrence.

A door can also be assigned an Unlock Schedule, which specifies a period of time during which no credential is required to access the door; all users have free access during the Door Unlock Schedule period. Likewise, a device may be assigned an Active Schedule, a period during which the device is in operation. Before any of these devices are created, you must first define the schedule according to which they will operate. (For more information on devices, see the section on Managing Devices.)

What are Holidays?

An observed holiday is a specific time period during which schedules refer to their Holiday override columns instead of to the day of week. If a schedule's Holiday column is blank, the schedule will not be active during that time period.

Browsing the Schedules List

The Schedules list displays a list of all schedules currently defined for the account.

Administrators with appropriate permissions can view the schedules associated with their own accounts.

To view the list of schedules:

1. Scroll over the Configuration link at the top of any page. The sub-navigation menu displays.
2. From the Scheduling link, click Schedules. The Schedules list page displays.

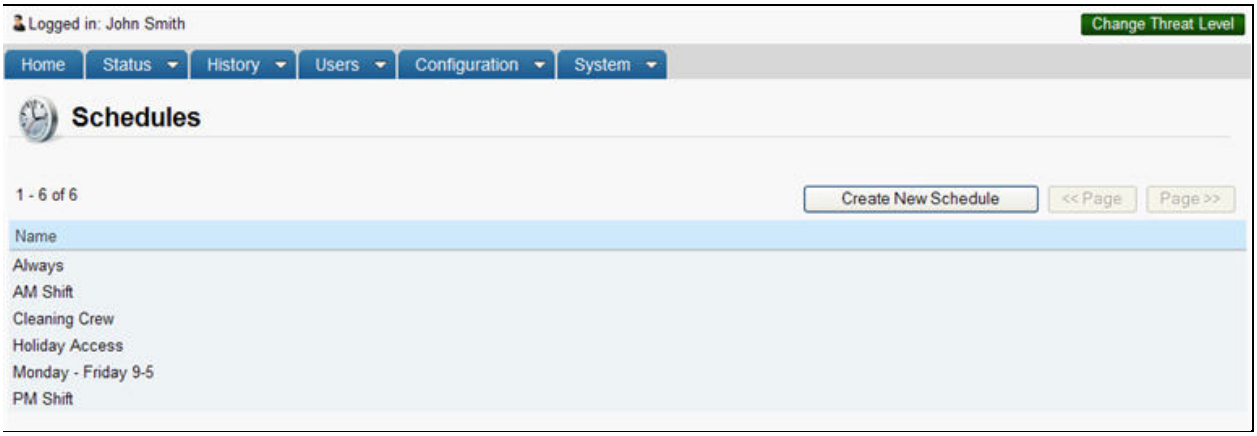


Figure 133. View Schedules List

Details displayed include:

- This page lists all the schedules currently defined for the account. Two schedules are defined automatically when the System Account is first created: "Always" and "Monday – Friday 9-5".

Administrators with appropriate permissions can:

Click a schedule to access the corresponding Schedule Details page.

Click Create New Schedule to access a blank Edit Schedule page in order to define a new schedule.

Viewing Schedule Details

Administrators with appropriate permissions can view basic schedule information on the Schedule Details page. This overview indicates the times during which the selected schedule is active.

To view details for a specific schedule:

1. Scroll over the Configuration link at the top of any page. The sub-navigation menu displays.
2. From the Scheduling link, click Schedules. The Schedules list page displays.
3. Click the schedule you want to view. The corresponding Schedule Details page displays.

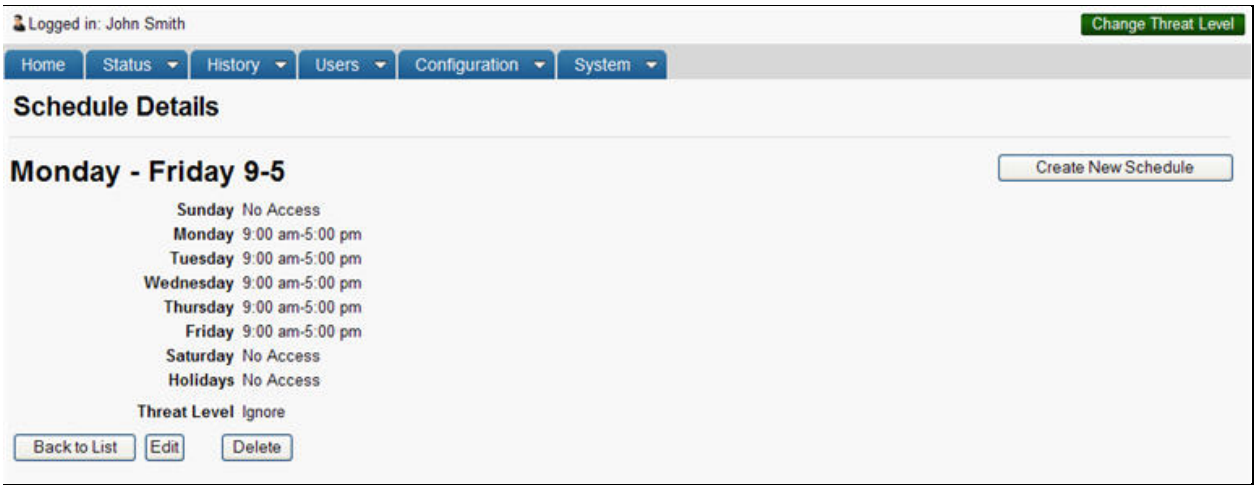


Figure 134. View Schedule Details

Details displayed include:

- For each day of the week, Sunday through Saturday, this page indicates the "on" periods for the selected schedule. In other words, when this schedule is assigned to a door, these are the periods during which the door is automatically unlocked. When it is assigned to a group, these are the periods during which users may access the device(s) for which they have privileges. Schedules may be affected by Threat Levels and the Threat Level indicator shows if a schedule is affected or if the schedule ignores Threat Levels (as above).

Administrators with appropriate permissions can:

Click the name of the Activating Group to access the associated Group Details page.

Click Back to List to return to the Schedules list.

Click Create New Schedule to access a blank Edit Schedule page in order to create a new schedule.

Click Edit to access the Edit Schedule page associated with this schedule.

Click Delete to remove the schedule from the system.

Creating a Schedule

Administrators with appropriate permissions can create new schedules.

	NOTE: *Please refer to the section on Creating a Group Enabled Schedule before assigning an activating group to any schedule or unchecking the Auto-Deactivate checkbox.*

To create a schedule:

1. Scroll over the Scheduling link at the top of any page. The sub-navigation menu displays.
2. From the sub-navigation menu, click Schedules. The Schedules list page displays.
3. Click Create New Schedule. The Edit Schedule page displays with blank fields.

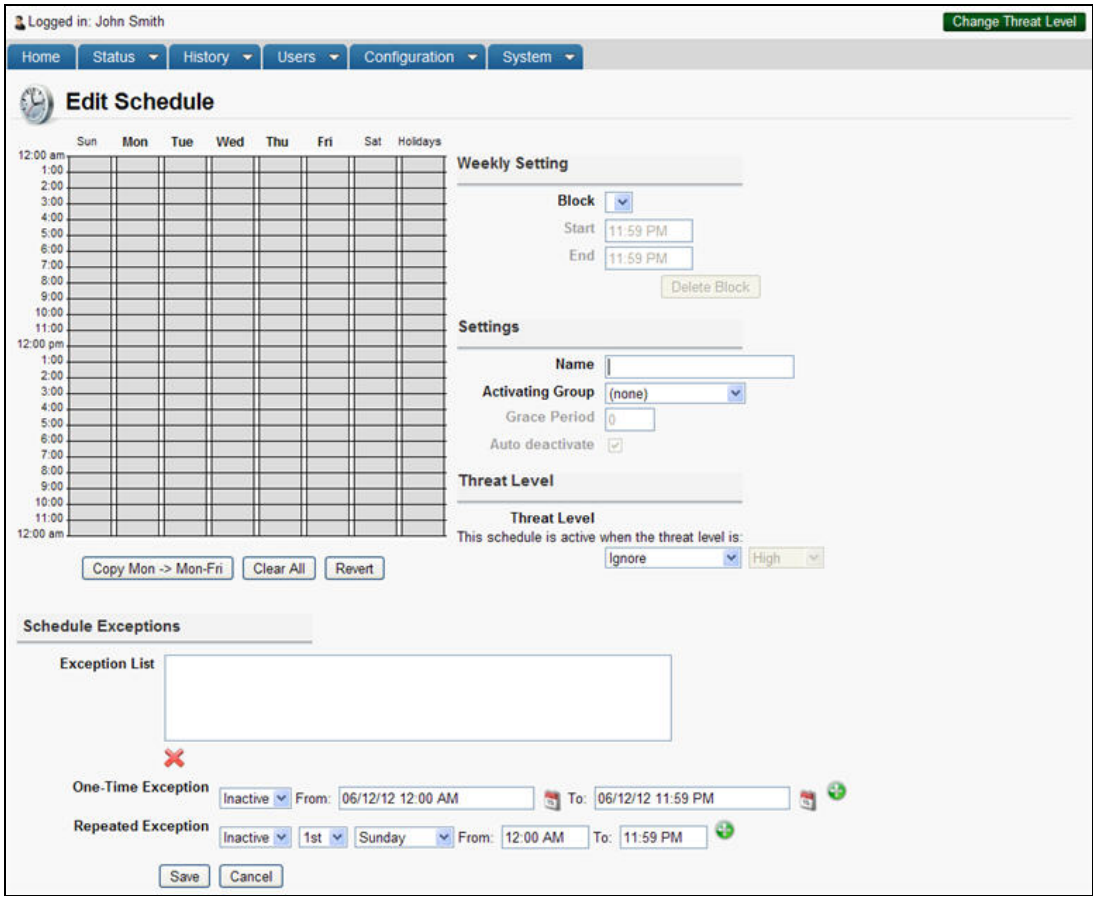


Figure 135. Create New Schedule

4. Enter a brief, descriptive Name for the schedule, such as "Night Shift" or "Cleaning Crew."
5. If this is a Group Enabled Schedule, select the Enabling Group from the drop-down list and enter an associated Grace Period. Please refer to the section on *Creating a Group Enabled Schedule* before assigning an activating group to any schedule. To turn off the auto-deactivate feature of group enabled schedules, uncheck the Auto Deactivate checkbox. Once this is done, this then treats the group enabled schedule like a normal schedule without requiring any further input from the enabling group until the device is deactivated manually.

	*WARNING: Turning off the Auto-Deactivation feature* *All panels attached to the Brivo Onsite Server appliance must have firmware 3.0.5 or later to be able to turn off the Auto-Deactivate functionality.*

	*WARNING: Group Enabled Schedules* *Group Enabled Schedules support the Brivo Onsite Server First-Person-In and Supervisor-on-Site functionality. If you assign an enabling activating group to a schedule without first understanding how this feature works you may inadvertently create a security risk. Refer to the section on Creating a Group Enabled Schedule before assigning an activating group to any schedule.*

6. For each day of the week, use the schedule graph to define a block of time during which the schedule is active. Active blocks determine when a group of users has access to a door or device or when a device is operational.
    - To define an active block, click on a gray column for any day (i.e., Mon). Click at the desired start point (e.g.., 8:00 AM) and drag the cursor down to the desired end point (e.g., 5:59 PM), and then release. Two things happen. First, this block of time is added to the Block drop-down list as a menu option (e.g., as Mon 8:00 am – 5:59 pm). Second, whenever the block is highlighted in the schedule graph, the start and end times display in the Start and End fields.
    - To edit a block of time once it is defined, click the block name on the Block drop-down list or click the highlighted block on the schedule graph, and then use the Start and End fields to change the time range.
    - To delete an access block, click inside the block to highlight it then click Delete Block. The block is cleared from the schedule graph, the associated menu option is removed from the Block drop-down list, and the Start and End fields become inactive.
    - To repeat an access period for the work week, fill in the Monday column, and then click Copy Mon -> Mon-Fri.
    - To clear all active blocks, click Clear.
    - To revert to the most recently saved settings, click Revert.
7. A schedule refers to its Holiday column during defined holiday periods. In the Holiday column, enter the time period during which the door or device can be accessed or a device can be activated during the holiday periods for this schedule. For example, you might have a schedule called "Cleaning Crew" that is active 6:00 pm through 2:00 am Monday through Friday. But on holidays, you want to limit access to 6:00 pm through 10:00 pm.

	*NOTE:* *If the Holiday column is left blank, no access will be permitted during holidays.*

8. Threat Level determines if a schedule is affected by Threat Levels, and if so, at what point. The default selection is to have a schedule ignore Threat Levels, but a schedule can be activated at a certain Threat Level and may include when Threat Levels are less or more severe than the selected Threat Level. For example, a schedule may be active at a Medium Threat Level and all less severe Threat Levels or perhaps a schedule may only activate when a High Threat Level or more severe Threat Levels are initiated.
9. Schedule Exceptions allow an administrator to create a One-Time Exception or Repeated Exceptions.
    - For One-Time Exceptions, select whether or not the exception will be to be active during a normally closed portion of the schedule or to be inactive during a normally open portion of the schedule. Then select the time and date from the calendar in the From: and To: fields. Once complete, click on the  icon to add the One-Time Exception to the Exception List.
    - For Repeated Exceptions, select whether or not the exception will be to be active during a normally closed portion of the schedule or to be inactive during a normally open portion of the schedule. Repeated exceptions are based on a weekly rotation, so select the 1st through the 5th , then the day of the week, and finally the time of day in the From: and To: fields. Once complete, click on the  icon to add the Repeated Exception to the Exception List.
10. Click Save. The Schedule Details page displays. This schedule can now be used to define access permissions and to control devices.

Managing Schedules

Administrators with appropriate permissions can edit and delete all schedules associated with an account.

To edit an existing schedule:

1. Scroll over the Configuration link at the top of any page. The sub-navigation menu displays.
2. From the Scheduling link, click Schedules. The Schedules page displays.
3. Click the schedule you want to edit. The corresponding Schedule Detail page displays.
4. Click Edit. The Edit Schedule page displays.

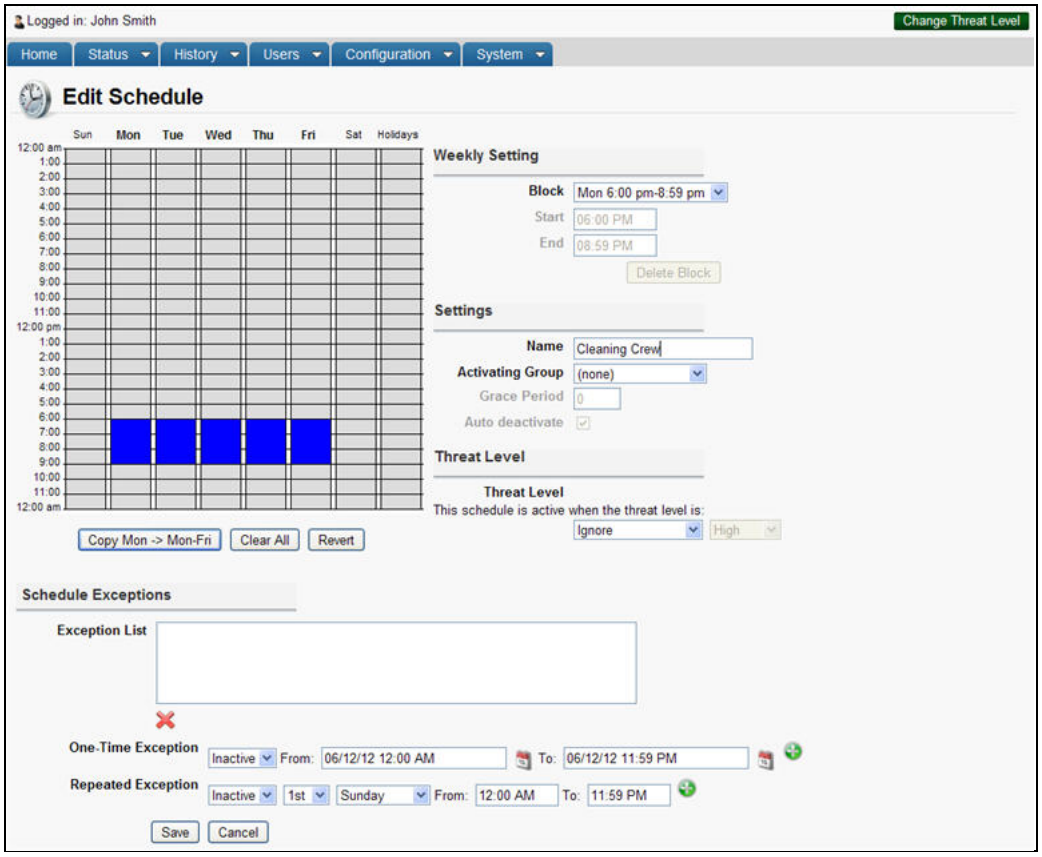


Figure 136. Edit Schedule

5. Edit the schedule according to the preceding guidelines for *Creating a Schedule*.
6. Click Save. You are returned to the Schedule detail page.

To delete a schedule:

1. Scroll over the Configuration link at the top of any page. The sub-navigation menu displays.
2. From the Scheduling link, click Schedules. The Schedules list page displays.
3. Click the name of the schedule you wish to delete. The corresponding Schedule Detail page displays
4. Click Delete. A confirmation prompt displays.
5. Click OK in the confirmation prompt. The Schedules page displays with the deleted schedule removed from the list.

Browsing the Holidays List

The Holidays list displays a list of all holidays currently defined for the account.

Administrators with appropriate permissions can view the holidays associated with their own accounts.

To view the list of holidays:

1. Scroll over the Configuration link at the top of any page. The sub-navigation menu displays.
2. From the Scheduling link, click Holidays. The Holidays list page displays.

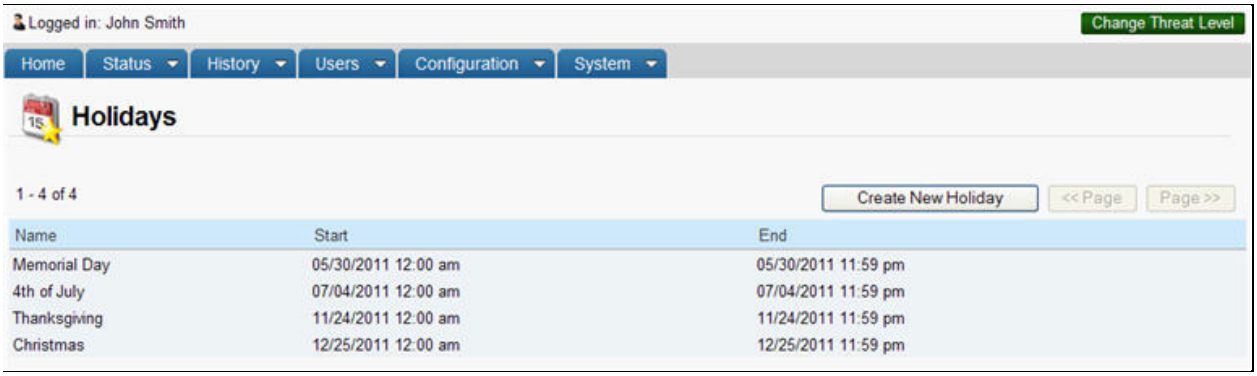


Figure 137. View Holidays List

Details displayed include:

- Name. The name of the holiday. Holidays are listed in chronological rather than alphabetical order.
- Time and Date. The calendar date and time on which this holiday is to be observed. At the listed time on the start date, all schedules will operate according to their Holidays hours, as indicated on the Schedule Details page.

Administrators with appropriate permissions can:

Click a holiday to access the corresponding Edit Holiday page.

Click Create New Holiday to access a blank Edit Holiday page in order to define a new holiday for the account.

Creating a Holiday

Administrators with appropriate permissions can create new holidays.

To create a holiday:

1. Scroll over the Configuration link at the top of any page. The sub-navigation menu displays.
2. From the Scheduling link, click Holidays. The Holidays list page displays.
3. Click Create New Holiday. The Edit Holiday page displays.

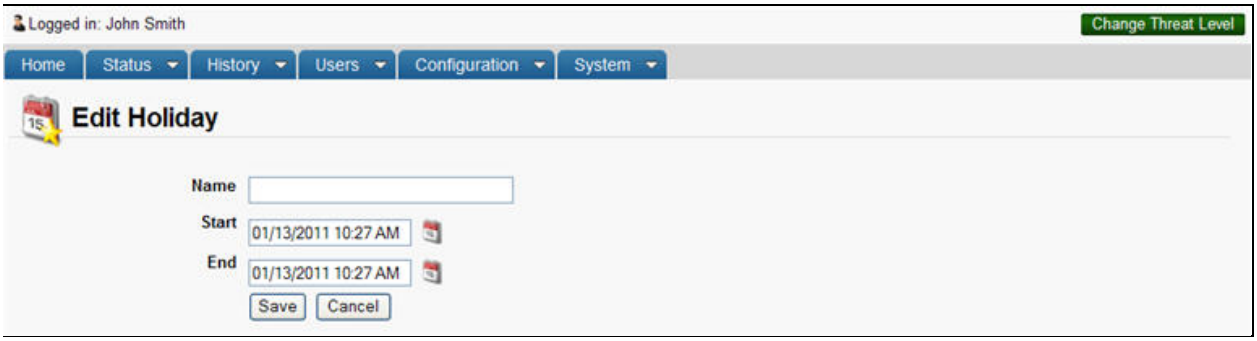


Figure 138. Create a Holiday

4. Enter a brief, meaningful Name for the holiday, such as "Memorial Day."
5. Click anywhere in the Start field and type in the date or click the calendar icon to open a pop-up calendar and select the date on which this holiday should be observed. Do the same for the End field.
6. Click Save. The Holidays page displays with the new holiday listed.

Managing Holidays

Administrators with appropriate permissions can edit or delete a holiday.

To edit a holiday:

1. Scroll over the Configuration link at the top of any page. The sub-navigation menu displays.
2. From the Scheduling link, click Holidays. The Holidays list page displays.
3. Click the name of the holiday you want to edit. The corresponding Edit Holiday page displays.

Figure 139. Edit a Holiday

4. Update the Name, Start, and End fields according to the preceding guidelines for *Creating a Holiday*.
5. Click Save. You are returned to the Holidays list with the changes reflected.

To delete a holiday:

1. Scroll over the Configuration link at the top of any page. The sub-navigation menu displays.
2. From the Scheduling link, click Holidays. The Holidays list page displays.
3. Click the holiday you want to delete. The corresponding Edit Holiday page displays.
4. Click Delete. A message displays warning that this operation cannot be undone.
5. Click OK. You are returned to the Holidays list with the deleted holiday removed from the list. Holiday schedules will no longer be observed on this day.

16.Maps/Floorplans

The Maps/Floorplans feature allows administrator with appropriate permissions to import and use floorplan graphics (campuses/complexes/buildings/offices) for both configuration and status monitoring. Using icons and regions, administrators can monitor linked devices and regions for changes in status or alarm.

Maps/Floorplans Definitions

Maps

Maps are imported images representing an area, for example, a building floorplan, business campus, or an individual office. Any suitable image (floorplan or otherwise) can be used for the basis for a map. Maps can have icons placed on them to represent devices, and maps can be detailed with regions linking them to other maps/floorplans.

Icons

Icons are graphics that represent the devices present on your site. Examples include doors, input switch devices, valid credential input devices, and elevators. Icons, representing devices, are placed on the map/floorplan for monitoring and control purposes. When a device changes state on your site, the icon linked to that device will change to match, for example showing that the door is open or closed.

When a device enters an alarm state, the icon representing the device will change to match the alarm state. A device will, for example, enter an alarm state due to a wire cut message or a door ajar message.

Regions

Regions are sections of a map/floorplan that a user selects by drawing a border around the area. Regions are primarily used to link multiple maps/floorplans together for monitoring purposes, like buildings on a campus or separate floors in an office building. Additionally, when a device enters an alarm state, the region where the device is will also enter an alarm state by changing color, and any other linked regions will also enter an alarm state.

Browsing Maps/Floorplans

The maps/floorplans list displays a list of all maps/floorplans currently defined by the account.

Administrators with appropriate permissions can view the maps/floorplans associated with their own accounts.

To display maps/floorplans:

1. Scroll over the Configuration section. The sub-navigation menu displays.
2. From the Dashboard link, click the Maps/Floorplans link. The Maps/Floorplans list page displays.

Details displayed include:

- This page lists all of the maps/floorplans currently defined for the account.

Administrators with appropriate permissions can:

Click maps/floorplans to access the corresponding View Map Details page.

Click Create New Map to access a blank Edit Map page in order to define new maps/floorplans.

Click Edit to edit currently defined maps/floorplans.

Control device states from the dashboard using the Live Map feature.

Managing Maps/Floorplans

To create a map:

1. Scroll over the Configuration section. The sub-navigation menu displays.
2. From the Dashboard link, click the Maps/Floorplans link. The Maps/Floorplans list page displays.
3. Click Create New Map. The Edit Map page displays.
4. Enter the name for the map/floorplan you wish to create in the Map Properties box.
5. Click on the Upload Image button to load your new Map/Floorplan.
6. Click Browse and select the image file you wish to upload. Once it is selected, click the Upload button. You are returned to the Edit Map page and your map/floorplan should now be displayed.

	NOTE: *File types supported for maps/floorplans are .jpg, .png, and .gif.*

7. Click Save. You are returned to the View Map Details page.

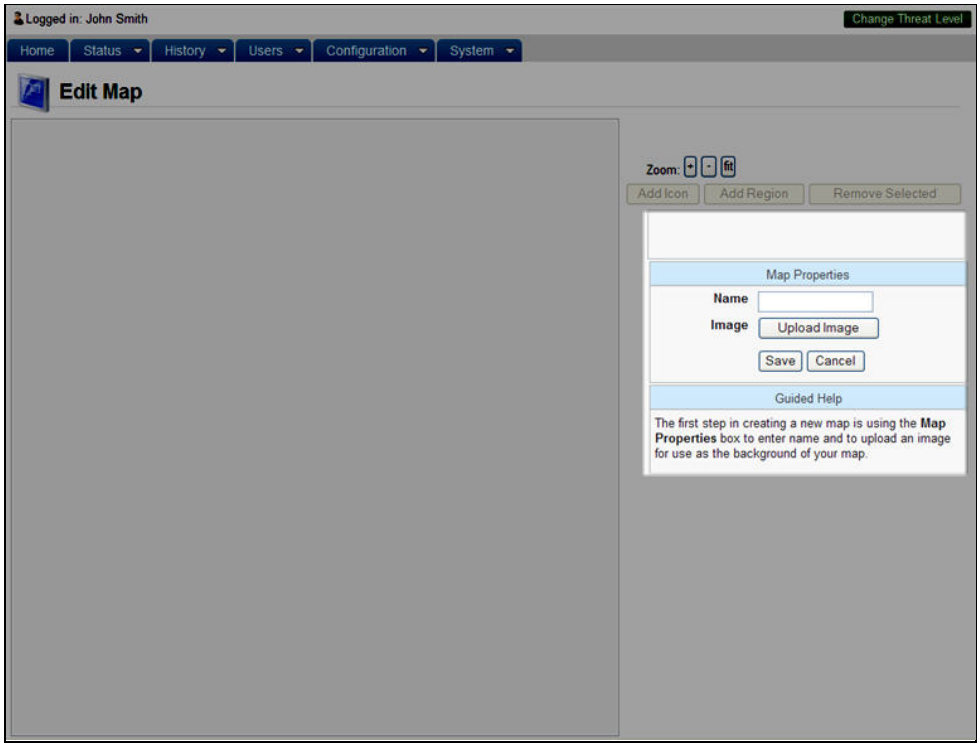


Figure 140. Create a Map

To edit a map:

1. Scroll over the Configuration section. The sub-navigation menu displays.
2. From the Dashboard link, click the Maps/Floorplans link. The Maps/Floorplans list page displays.
3. Click the map that you wish to edit. The Maps/Floorplans Details page displays.
4. Click Edit. The Edit Map page displays.

5. After you have finished making changes to the map, click Save. You are returned to the View Map Details page.

To delete a map:

1. Scroll over the Configuration section. The sub-navigation menu displays.
2. From the Dashboard link, click the Maps/Floorplans link. The Maps/Floorplans list page displays.
3. Click the map that you wish to delete. The Edit Map Details page displays.
4. Click Delete. Click OK in the confirmation prompt. You are returned to the View Map Details page.

To add an icon:

1. Scroll over the Configuration section. The sub-navigation menu displays.
2. From the Dashboard link, click the Maps/Floorplans link. The Maps/Floorplans list page displays.
3. Click on the map that you wish to edit. The View Map Details page displays.
4. At the bottom of the View Map Details page, click Edit. The Edit Map page displays.
5. To add an icon, click the Add Icon button. Move the mouse over the map area and a purple circle will appear. Place the purple circle where you want the icon to appear.
6. Scale the size of the icon to fit your map. You may move the icon around the map to its desired location.
7. In the Icon Properties box on the right, click the Select button to link the icon to a device at your site. The Select box will appear with a list of all devices. Select a device and you are returned to the Edit Map page.
8. In the Icon Properties box on the right, you may also select the shape of your icon from the dropdown menu.
9. Click Save. You are returned to the View Map Details page.

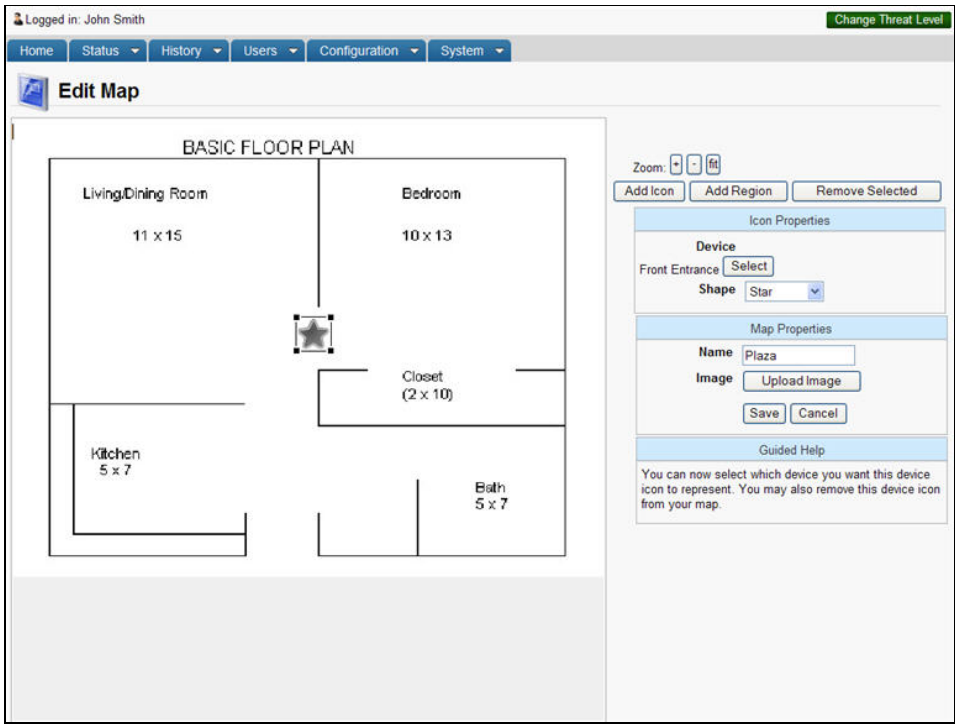


Figure 141. Add an Icon

To edit an icon to change the device:

1. Scroll over the Configuration section. The sub-navigation menu displays.
2. From the Dashboard link, click the Maps/Floorplans link. The Maps/Floorplans list page displays.
3. Click on the map you wish to edit. The View Map Details page displays.
4. At the bottom of the View Map Details page, click Edit. The Edit Map page displays.

5. Click on the icon you wish to edit.
6. From this page, you may move the icon around the map, or you may rescale the size of the icon.
7. To change the device your icon is linked to, click on the Select button in the Icon Properties box to the right. The Select box will appear with a list of all devices.
8. Select a different device from the dropdown list and you are returned to the Edit map page.
9. When you have finished, click Save. You are returned to the View Map Details page.

To delete an icon:

1. Scroll over the Configuration section. The sub-navigation menu displays.
2. From the Dashboard link, click the Maps/Floorplans link. The Maps/Floorplans list page displays.
3. Click on the map you wish to edit. The View Map Details page displays.
4. At the bottom of the View Map Details page, click Edit. The Edit Map page displays.
5. Click on the icon you wish to delete.
6. Click on the Remove Selected button on the right side of the screen. The icon will disappear from the screen.
7. When you have finished, click Save. You are returned to the View Map Details page.

To add a region:

1. Scroll over the Configuration section. The sub-navigation menu displays.
2. From the Dashboard link, click the Maps/Floorplans link. The Maps/Floorplans list page displays.
3. Click on the map you wish to edit. The View Map Details page displays.
4. At the bottom of the View Map Details page, click Edit. The Edit map page displays.
5. To add a region, click the Add Region button.
6. Click the starting point on the map where you want the region to be outlined. As you move the mouse, a line will appear stretching from the starting point to the mouse pointer. Select the points around the area so that it is defined as you want it to appear. Finally, click the starting point a second time and the region will be defined. The default color for regions is gray, so a gray box will appear as you have outlined.
7. In the Region Properties box on the right, click the Select button to link the region to a map. The Select box will appear with a list of all maps. Select a map and you are returned to the Edit Map page.
8. When you are finished, click Save. You are returned to the View Map Details page.

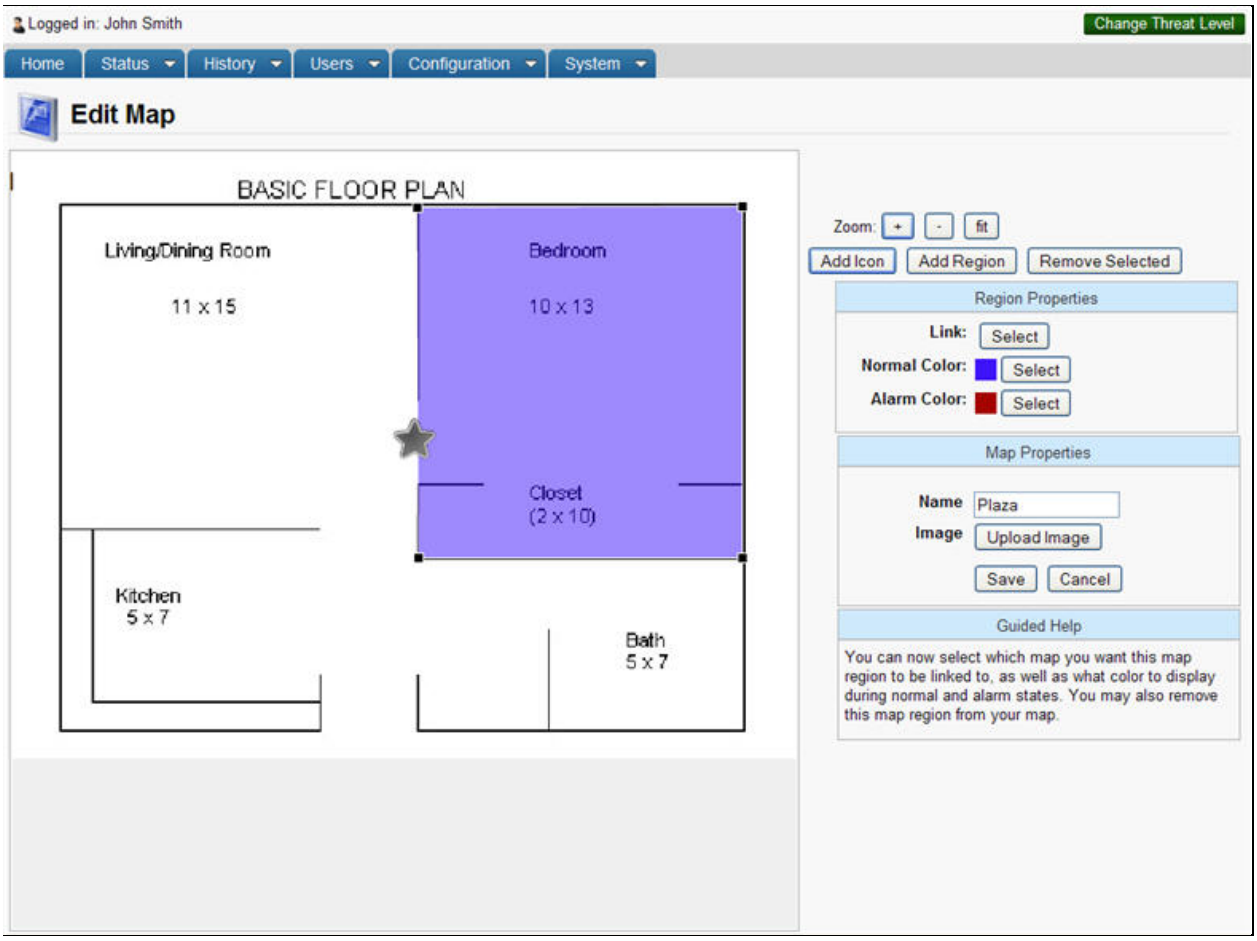


Figure 142. Add a Region

To edit a region:

1. Scroll over the Configuration section. The sub-navigation menu displays.
2. From the Dashboard link, click the Maps/Floorplans link. The Maps/Floorplans list page displays.
3. Click on the map you wish to edit. The View Map Details page displays.
4. At the bottom of the View Map Details page, click Edit. The Edit map page displays.
5. Click on the region you wish to edit. The defining points around the region will appear.

To edit the shape of a region:

n) You may move your mouse over any defining point and while holding the mouse button down drag the defining point anywhere on the map. You will see the shape of the region change as a result.

o) When you are finished, click Save. You are returned to the View Map Details page.

To edit the normal/alarm colors:

a) To change the normal color, click the middle Select button in the Region Properties box to the right. A color box will appear. You may change the color by selecting it from the main color box, using the vertical color bar on the right or by typing in the red, green, and blue numbers to match your chosen color.

b) To change the alarm color, click the lower Select button in the Region Properties box to the right. A color box will appear. You may change the color by selecting it from the main color box, the color bar on the right or by typing in the red, green, and blue numbers to match your chosen color.

c) When you are finished, click Save. You are returned to the View Map Details page.

To edit the link to the region:

a) To change the link to the region, click the upper Select button in the Region Properties box to the right. The Select box will appear with a list of all maps. Select a map and you are returned to the Edit Map page.

b) When you are finished, click Save. You are returned to the View Map Details page.

To delete a region:

1. Scroll over the Configuration section. The sub-navigation menu displays.
2. From the Dashboard link, click the Maps/Floorplans link. The Maps/Floorplans list page displays.
3. Click on the map you wish to edit. The View Map Details page displays.
4. At the bottom of the View Map Details page, click Edit. The Edit map page displays.
5. Click on the region you wish to edit. The defining points around the region will appear.
6. Click the Remove Selected button on the right. The region will disappear from the screen.
7. When you have finished, click Save. You are returned to the View Map Details page.

Live Map

Once a map/floorplan has been created, icons added, and regions established, then an administrator with appropriate permissions can utilize the Live Map feature under the Dashboard link.

To use the Live map feature:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Dashboard link, click the Maps/Floorplans link. A popup window with a list of map names appears. Select the map you wish to use.
3. The Live Map page will appear with the icons and regions in their current states (either normal or alarm).

NOTE:

An icon representing a programmable device or door will appear as its normal color (default is green) if in a normal state (such as unlocked or locked). The icon will switch to its alarm color (default red) if in an alarm state such as door ajar or wire cut.

4. To interact with a device, scroll over the icon representing that device. The name and current status of the device will appear in a popup window.
5. If the device can be controlled via the browser, if you click on the icon, a button will appear (for example, Pulse for a door).
6. Zoom – to zoom in, out, or reset the default size of the live map, there are three buttons in the upper right hand corner of the screen (+), (-), and (fit).
7. Choose Map – to choose a new map for live view, click on the Choose Map button and a popup window with available maps will appear. Select the map you wish to view live and you are returned to the Live Map page.

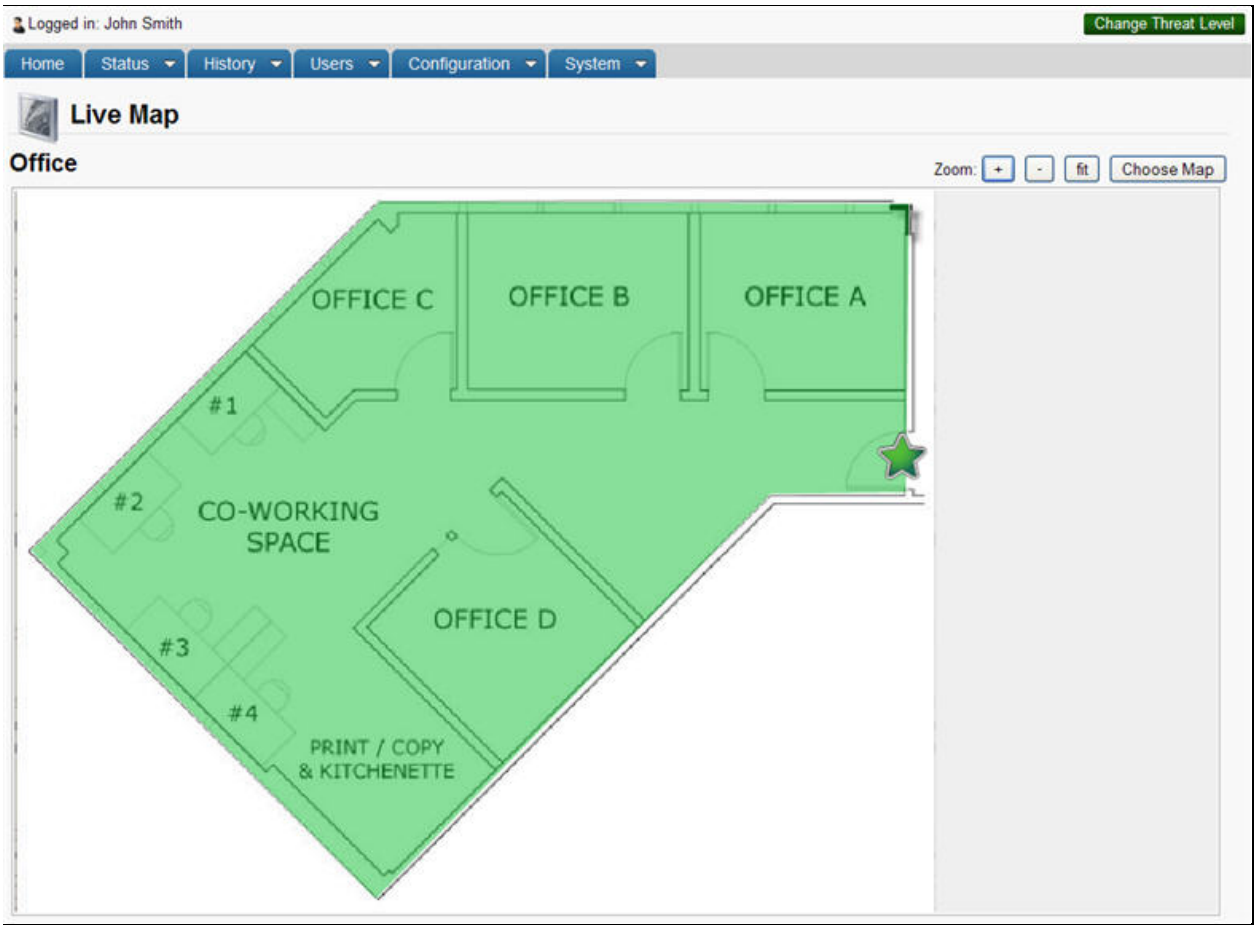


Figure 143. View Live Map

17.System Management

The System link only displays when you log in as an administrator with appropriate permissions. Tenant Account Administrators have no access to this section of Brivo Onsite Server. This is because, to a large extent, the System section deals with the networking aspects of the hardware. The steps described in the System chapter should be performed by your network administrator.

Maintenance Mode

Maintenance Mode is a system state that prevents the Brivo Onsite Server from accepting panel connections until it is ready. So long as the Brivo Onsite Server remains in maintenance mode, there will be no communication between the appliance and the panels. All panels will continue to function with their current dataset. The Brivo Onsite Server will enter maintenance mode if a firmware upgrade is started or if an administrator manually puts the appliance into maintenance mode. The Brivo Onsite Server will remain in maintenance mode until it is manually taken out of maintenance mode by an administrator with appropriate permissions. For more details on manually taking the Brivo Onsite Server in and out of maintenance mode, see *Browsing the System Status Page.*

So long as the Brivo Onsite Server is in maintenance mode, a red warning message will appear at the top of every page.

Figure 144. Maintenance Mode Warning Message

Browsing the System Status Page/Using Maintenance Mode

The System Status page displays when you click the System Status link from the Home page or via the instructions below. This page is where administrators can take the Brivo Onsite Server into and out of maintenance mode.

Account Administrators with modify permissions to the System tab can utilize the maintenance mode feature.

To access the system status page:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Status. The Status sub-navigation menu displays.
3. From the Status sub-navigation menu, click System Status. The System Status page displays.

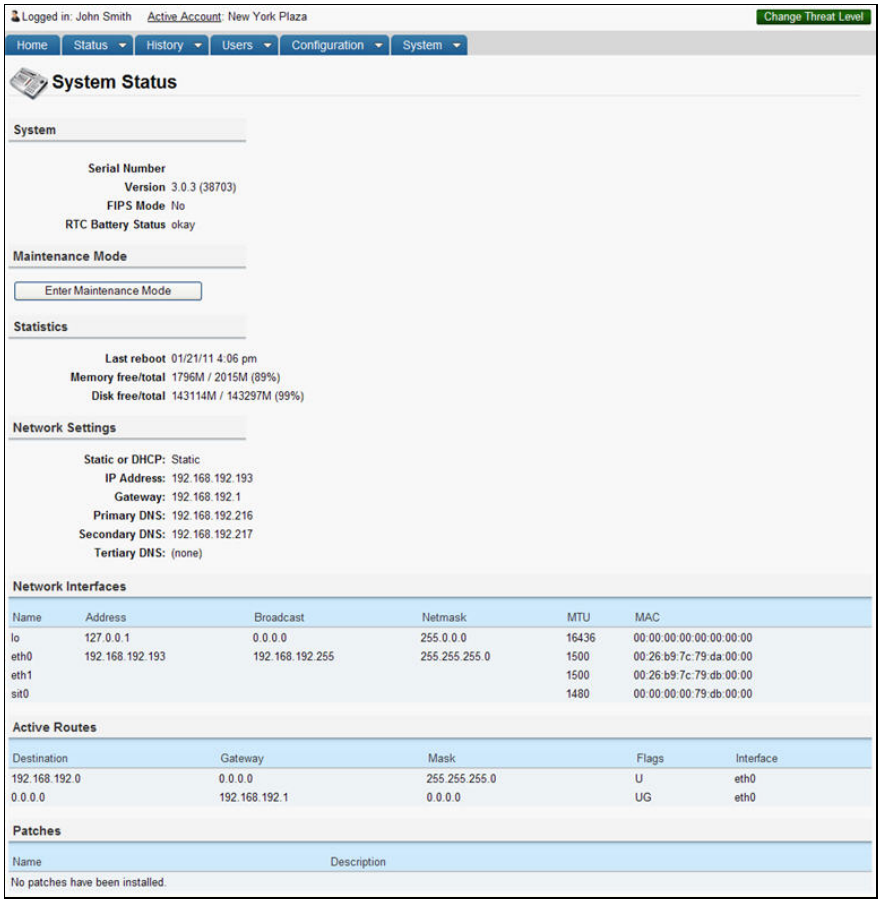


Figure 145. System Status

Details displayed include:

System

- Serial Number. The serial number of the Brivo Onsite Server.
- Version. The version of application firmware currently being run.
- FIPS Mode. Shows if the Brivo Onsite Server is using FIPS Mode or not.

Maintenance Mode

- Enter/Exit Maintenance Mode. This button allows the Brivo Onsite Server to enter or exit maintenance mode.

Statistics

- Last reboot. The date and time at which the Brivo Onsite Server panel was last rebooted.
- Memory free/total. The amount of free memory compared to total memory on the machine running Brivo Onsite Server.
- Disk free/total. The amount of free disk space compared to the total disk space.

Network Settings

- Static or DHCP. Indicates whether the network settings on this system were set by an automatic network service (DHCP) or set manually (Static).
- IP Address. The IP address of the system, distinguishing this from other nodes on the same network.
- Gateway. The address of the machine acting as a gateway between the local network and other networks, such as the internet.
- Primary DNS/Secondary DNS/Tertiary DNS. Tells the system which server(s) to use when converting the machine name (e.g., www.brivo.com) to the numeric IP address used on the internet. At least one (Primary) server is required, and a second (Secondary) is customary but not required.

Network Interfaces

- Name. A list of interfaces currently in use. Not all of the interfaces listed below are active on all systems.
- lo. Loopback. An interface used internally by the system. If the interface is not present, the network layer may not be active.
- eth0. Generally, the primary Ethernet interface, your connection to the outside world. When you change the IP address settings of the panel, this is the interface that you are manipulating.
- Address. IP address assigned to the interface.
- Broadcast. Mask of bits that specify broadcast packets on the network.
- Netmask. A mask used to separate a sub-network of machines; e.g., 255.255.255.0
- MTU. The Maximum Transmission Unit size.
- MAC. The Media Access Control address.

Active Routes

- Destination. The destination host or network.
- Gateway. The address of the machine acting as intermediary between networks or hosts.
- Mask. A mask of the address range covered by the routing rule.
- Flags. Displays the status of the route, i.e. U=Active, UG=Gateway.
- Interface. Routing specific flag values.

Patches

- Name. The name of any patches that have been installed.
- Description. The description of any patches that have been installed.

Browsing the System Logs

The System Logs page provides access to three different views of the system log:

System. Lists all system operations

Kernel. Lists only operations related to the system kernel.

Obix. Lists only operations related to Obix events.

	NOTE: *Obix Integration requires a license key. Without the license key, Obix Integration functionality will be disabled.*

Administrators with appropriate permissions can access this page.

To view a system log:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Status. The Status sub-navigation menu displays.
3. From the Status sub-navigation menu, click System Logs. The System Logs page displays.

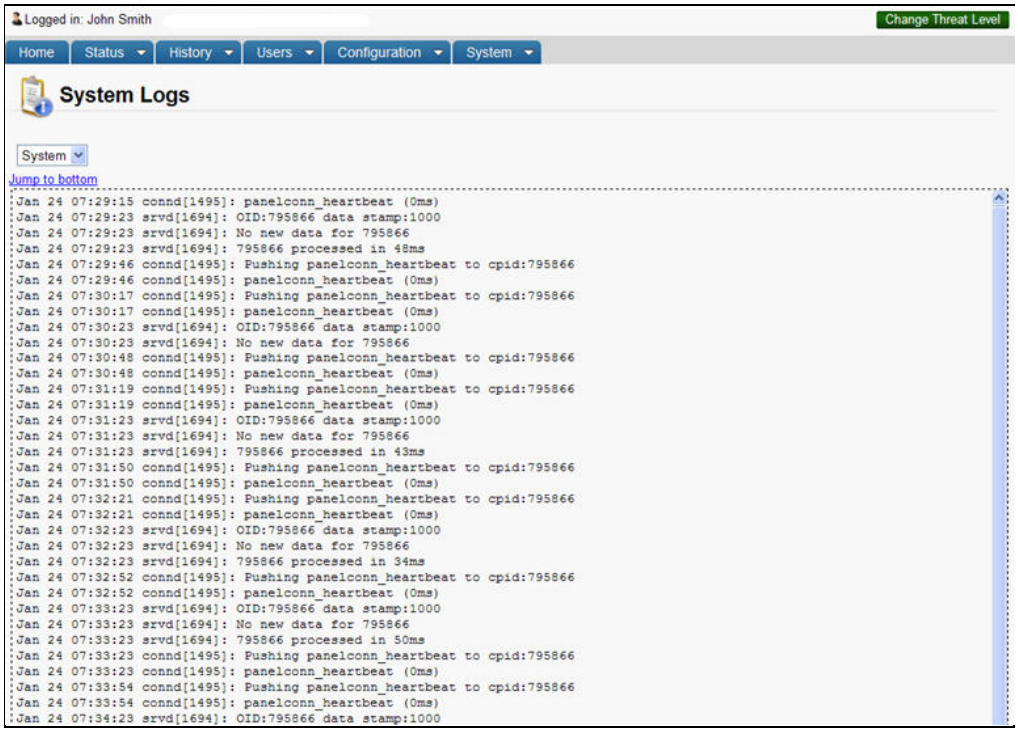


Figure 146. View System Log: Application

Administrators with appropriate permissions can:

Select the type of log to view, from the drop-down list.

Click Jump to bottom or Jump to top to move quickly between the top and bottom of the page.

Using System Tools

The application provides access to basic system commands via the Tools page in the System section.

Administrators with appropriate permissions can access or enter commands on the Tools page.

To use the system tools:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Status. The Status sub-navigation menu displays.
3. From the Status sub-navigation menu, click Tools. The Tools page displays.

Figure 147. Enter System Command

Administrators with appropriate permissions can:

Select a Command from the drop-down list.

Enter a parameter for that command in the adjoining data entry field.

Click Go to activate the command.

Valid command options include:

- ping. Provides a mechanism for determining whether the control panel can reach a particular IP address on the LAN or the internet. For example, the target of the ping command may be local to the network (e.g., trying to ping the local gateway to the internet first to see if the control panel can communicate with the LAN), or may be
- traceroute. Show the route a packet takes en route to its given destination. This command may take longer to execute than the others.
- nslookup. Attempt to resolve a host name, to make sure your DNS settings are valid.
- arp. Output low-level routing information.
- ifconfig. Output low-level network device configuration and status information.
- restart panel communications. Allows an administrator to restart data and command channels when they are not working properly.
- restart network. Reinitializes the network layer, potentially releasing DHCP leases and activating any outstanding changes to network configurations.
- reboot system. Performs a graceful restart of the system.

Panel Comms Monitoring

The application allows the system to send notification emails concerning panel connectivity to a list of specified recipients.

Administrators with appropriate permissions can access and assign details concerning panel communication with the appliance.

To use panel comms monitoring:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Status. The Status sub-navigation menu displays.
3. From the Status sub-navigation menu, click Panel Comms Monitoring. The Panel Comms Monitoring page displays.
4. Select the Minimum Disconnect Time in minutes. This is the number of minutes that a panel has to be out of contact with the Brivo Onsite Server appliance before a notification will be sent.
5. Select the Notification Repeat Interval in minutes. This is how often additional emails will be sent to the recipients after the initial email.
6. Enter the email addresses of the intended Recipients, using commas to separate the individual email addresses.
7. Select a Language in which the notifications will be sent.
8. Click Save.

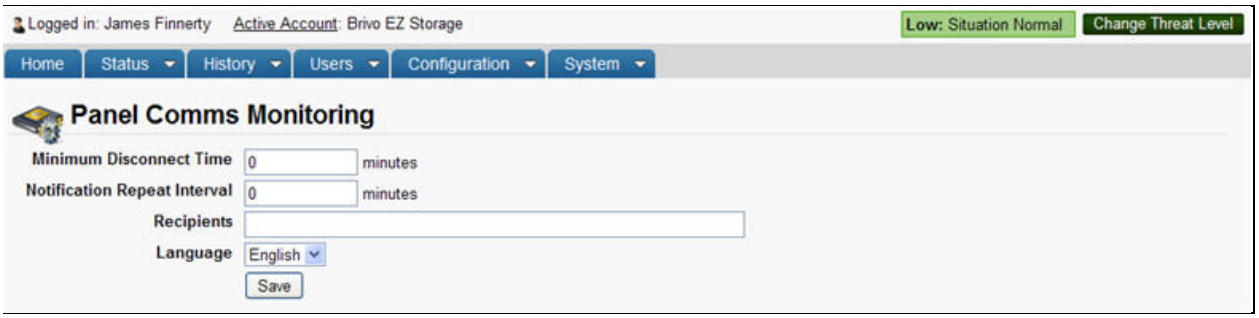


Figure 148. Panel Comms Monitoring

	NOTE: *In the case of multiple panels losing communication with the appliance, after the initial notification has been sent, any subsequent repeat notifications will be grouped together. For example, if you have a five panel system, if all five panels fail, you will receive individual notifications after the allotted time. However, when the repeat interval expires, you will receive a single email informing you that all five of your panels remain disconnected.*

Session Management

Brivo Onsite Server offers administrators the option to review the active sessions, and also enables the ability to force an administrator to logout. Brivo Onsite Server logs an administrator out after thirty minutes of inactivity. A pop-up window will appear 60 seconds prior to logout offering you the opportunity to resume your session. If you have a pop-up blocker enabled, this feature will not function.

	NOTE: Multiple Session Windows *It is important to note that if you have more than one session window open, when the pop-up window appears for one of your windows due to inactivity and you let the timeout expire, you will be logged out of your session entirely, including your current window.*

To manage account sessions

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Status. The Status sub-navigation menu displays.
3. From the Status sub-navigation menu, click Session Management. The Active Sessions page displays.

Figure 149. System: Active Sessions

Details displayed include:

- User Name
- Account Name
- IP Address
- Date and time since of user's login
- Force Logout. The Administrator has the option to force the user to logout.

Administrators with appropriate permissions can:

Force a user to logout.

To force a user to logout

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Status. The Status sub-navigation menu displays.
3. From the Status sub-navigation menu, click Session Management. The Active Sessions page displays.
4. Click the Force Logout button next to the user's name for whom you would like to force a logout. Once the user has been successfully logged out, you are returned to the Active Sessions page.

Manage Running Reports

Brivo Onsite Server offers administrators the option to manage reports that are currently running, and also enables the ability to force a report to stop running.

Details displayed include:

- Report – the name of the report that is running.
- Started – the time and date when the report was started.
- Administrator Name –the name of the administrator who started the report.
- Account – which account is generating the report.
- Stop Report The Administrator has the option to stop a report from running.

Administrators with appropriate permissions can:

Stop a report from running

To end a report:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Status. The Status sub-navigation menu displays.
3. From the Status sub-navigation menu, click Manage Running Reports. The Running Reports page displays showing all reports currently running.
4. Click the button to stop a report from running. Once the report has been successfully stopped, you are returned to the Running Reports page.

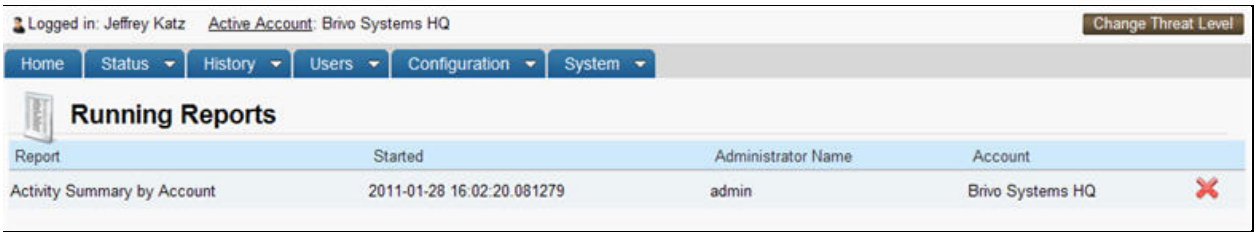


Figure 150. Managing Reports

	NOTE: *Ending reports prematurely is not something that should be done regularly. It is provided as a troubleshooting/diagnostic tool. If a report is ended prematurely, it may cause the person expecting the report to experience errors.*

Fetch Panel Logs

Brivo Onsite Server offers administrators the option to fetch panel logs from panels attached to the Brivo Onsite Server appliance.

Details Displayed Include:

- Panel Name - The name given to the control panel.
- Panel Type – The type of control panel.
- Panel ID - The control panel number assigned to the panel.
- Firmware Version – The version of firmware currently installed on the control panel.
- Connection Status – Indication of whether or not the control panel is connected to the Brivo Onsite Server appliance.

Administrators with appropriate permissions can:

Retrieve panel logs from control panels assigned to the Brivo Onsite Server appliance.

To View the Panel Logs Page:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Status. The Status sub-navigation menu displays.
3. From the Status sub-navigation menu, click Fetch Panel Log. The Fetch Panel Logs page displays.

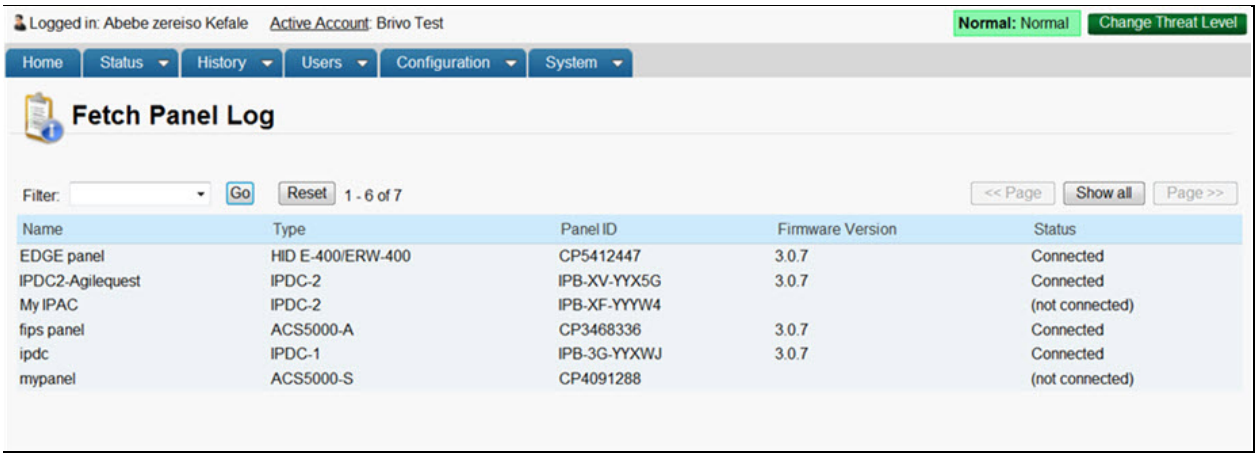


Figure 151. Fetch Panel Logs Display Page

Administrators with appropriate permissions can:

View individual panel logs.

Download individual panel logs.

Download all panel logs from a specific panel by clicking on the Download All link.

Generate a new panel log by clicking on the Fetch Panel Log link.

Navigate between pages using the <<Page and Page>> or return to the first page by clicking on the Go To First Page button.

To view a list of Panel Logs for a specific control panel:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Status. The Status sub-navigation menu displays.
3. From the Status sub-navigation menu, click Fetch Panel Log. The Fetch Panel Logs Control Panel List page displays.
4. To view the available panel log(s) of a specfic panel, click on the Panel Name of the panel whose logs you wish to view. The individual list of panel logs page displays.

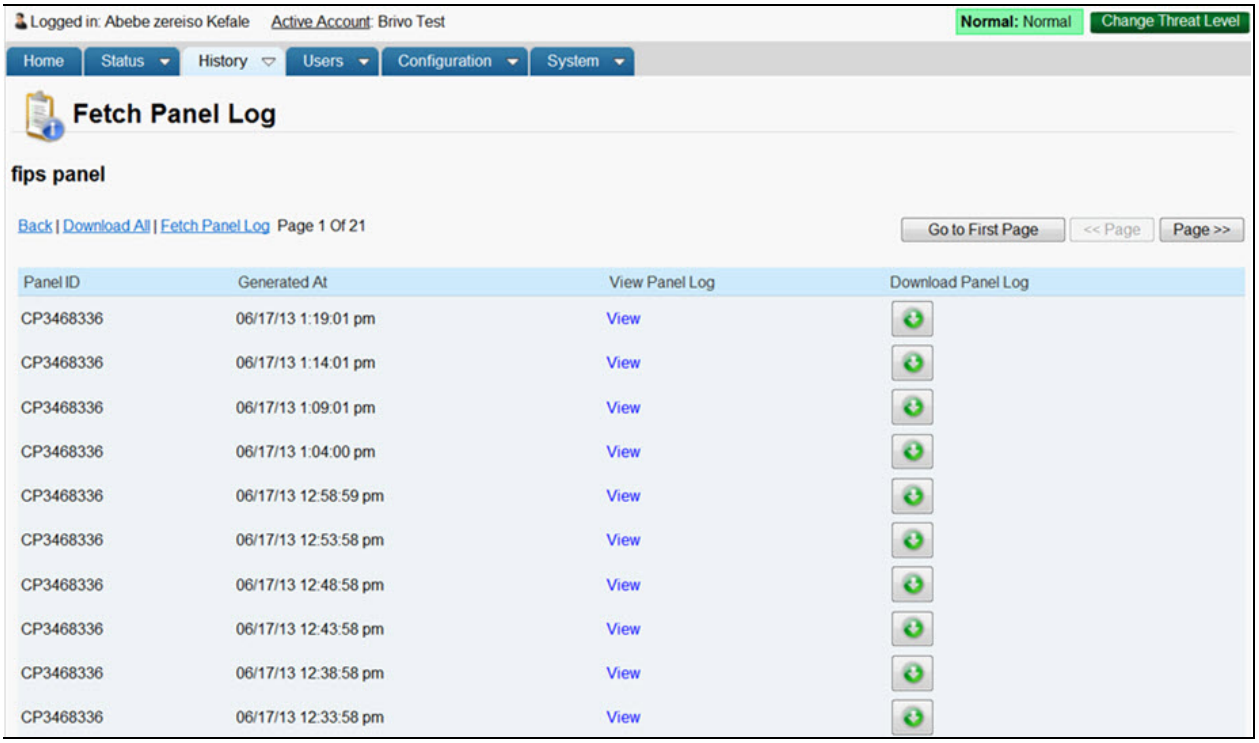


Figure 152. Individual List of Panel Logs Display Page

5. To download all available panel logs specific to the selected control panel, click on the Download All link and the logs will be downloaded in .bin format.
6. To generate a new panel log immediately, click on the Fetch Panel Log link and a new panel log will appear at the top of the log list.
7. To download a specific panel log, select the appropriate log and click on the  icon. The log will be downloaded in .bin format.
8. To view a specific panel log, select the appropriate log and click on View. The selected panel log displays.

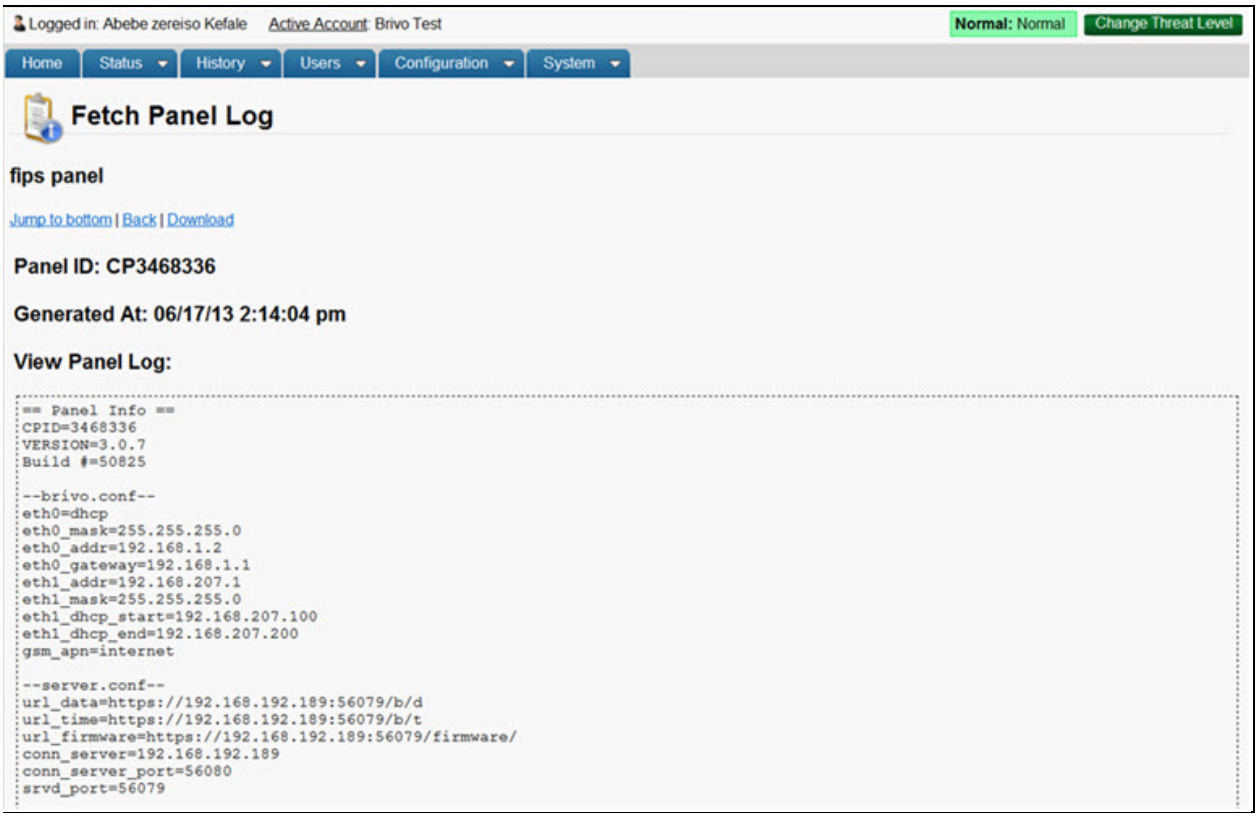


Figure 153. Viewing Individual Panel Log Details

9. To jump to the bottom of the log, click the Jump to Bottom link and likewise click the Jump to Top link to return to the top of the log.
10. Click Back to return to the Panel Log list.
11. Click Download to download this log in .bin format.

Diagnostic

	*NOTE:* *The Diagnostic dashboard should only be accessed by experienced administrators and in consultation with Brivo Technical Support.*

Brivo Onsite Server offers administrators an array of diagnostic tools as well as the ability to download a diagnostic dump and execute a tail log. The page also displays a System Detail log.

Details Displayed Include:

- Component – A feature or process used by the Brivo Onsite Server appliance.
- Description – The definition of the feature or process used by the Brivo Onsite Server appliance.
- Logging Level – The detail level of the logging of events. Quiet (minimal logs), Normal (standard logs), and Verbose (extremely detailed logs) are the three options.
- Send Signal – Allows an administrator to switch between logging levels on the corresponding component.
- Diagnostic Dump – a detailed log of processes occurring in the Brivo Onsite Server appliance.
- Tail Log – a live view of the current processes occurring in the Brivo Onsite Server appliance.

Administrators with appropriate permissions can:

Send a signal (change the logging level) for a specified component.

Download a diagnostic dump from the Brivo Onsite Server appliance.

Execute a Tail Log.

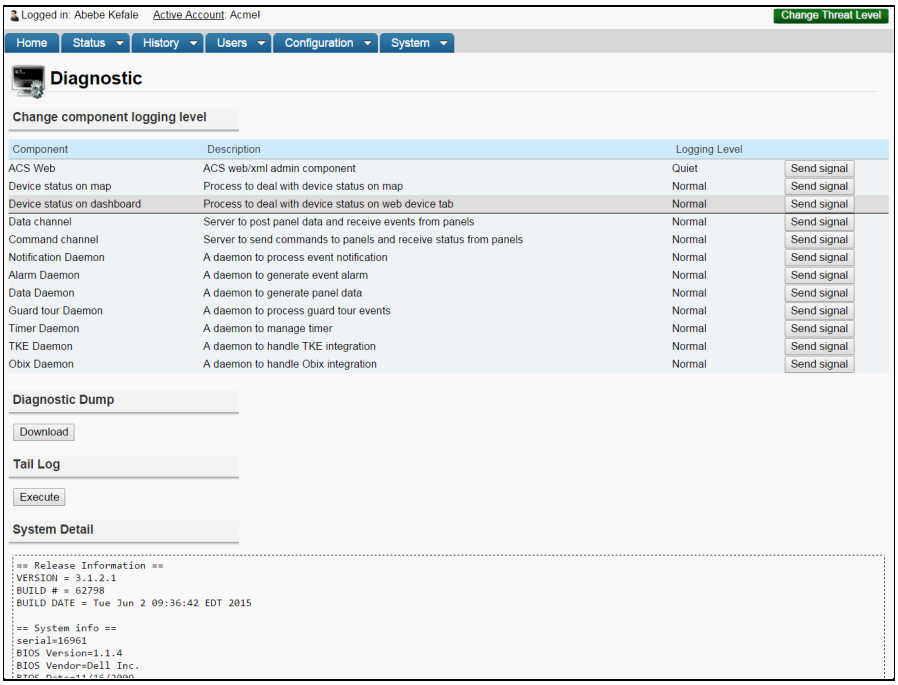


Figure 154. Diagnostic Display

To change a Logging Level

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Status. The Status sub-navigation menu displays.
3. From the Status sub-navigation menu, click Diagnostic. The Diagnostic page displays.
4. Select the Component whose logging level you wish to change and click on the **Send Signal** button. The default is Normal and each click of the Send Signal button will cycle through the three options (Quiet, Normal, Verbose).

To download a Diagnostic Dump

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Status. The Status sub-navigation menu displays.
3. From the Status sub-navigation menu, click Diagnostic. The Diagnostic page displays.
4. Click on the **Download** button under the Diagnostic Dump section of the page. The diagnostic file will automatically download to local storage in .bin format.

To execute a Tail Log

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Status. The Status sub-navigation menu displays.
3. From the Status sub-navigation menu, click Diagnostic. The Diagnostic page displays.
4. Click on the **Execute** button under the Tail Log section of the page. A pop-up window will display showing the live log of the Brivo Onsite Server appliance.
5. Simply close the pop-up window to end the Tail Log session.

Setting System Date and Time

The system normally synchronizes its system clock via NTP (Network Time Protocol) with servers over the Internet, to ensure accuracy. In case the system cannot reach an external server for time synchronization, such as when a firewall blocks access or the system is simply not on a network with Internet access, the system time must be set manually.

To set the date and time for your system:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Settings. The Settings sub-navigation menu displays.
3. From the Settings sub-navigation menu, click System Date/Time. The System Date/Time page displays.

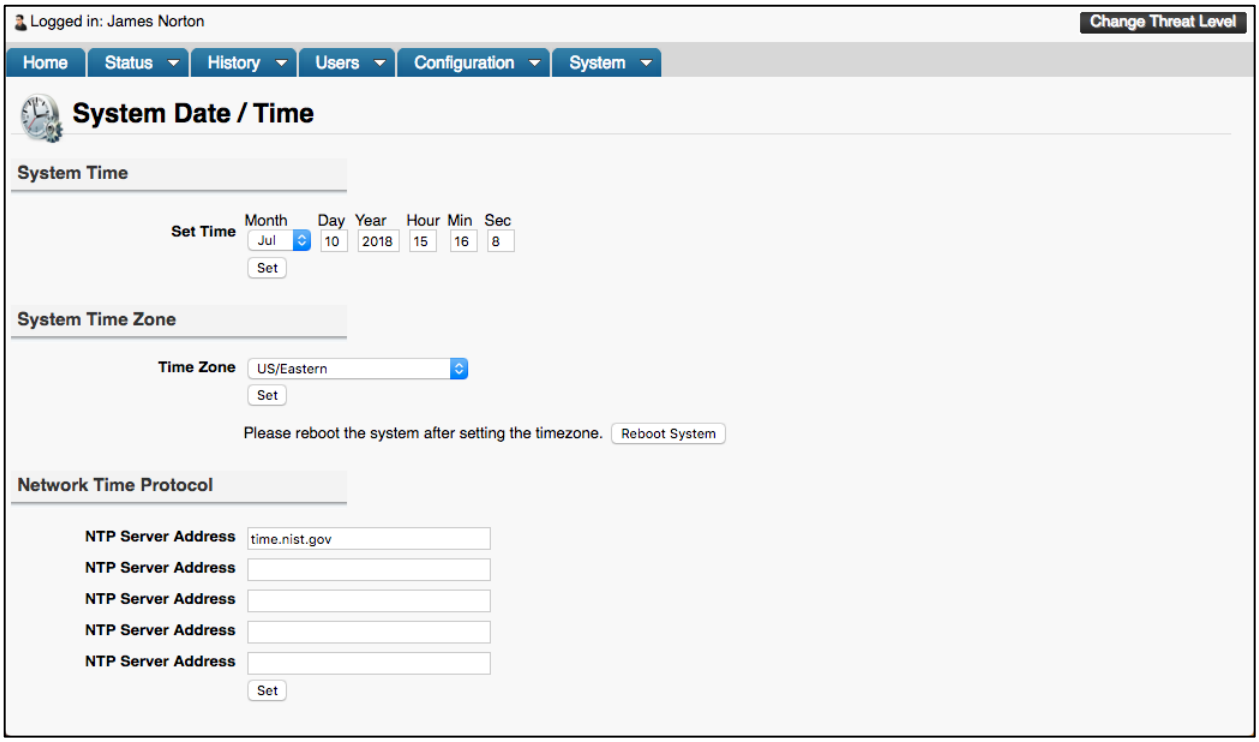


Figure 155. Set System Date and Time

4. Select a System Time Zone from the Time Zone drop-down list on the bottom half of the page, and then click the corresponding Set button.
5. To manually set the System Time, enter the current time using the Set Time fields, and then click the corresponding Set button.
6. The Network Time Protocol defaults to time.nist.gov. You may select up to five separate NTP server addresses with which the system can automatically synchronize. Simply enter the different Internet time server URLs into the associated NTP Server Address fields, and then click the corresponding Set button.

	*NOTE:* *If the System Time or System Time Zone is changed, it is highly recommended that you reboot the system in order for these changes to take effect.*

SNMP Agent Settings

These actions should only be performed by your network administrator.

To configure SNMP Agent Settings

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Settings. The Settings sub-navigation menu displays.
3. From the Settings sub-navigation menu, click SNMP Agent Settings. The SNMP Agent Settings page displays.

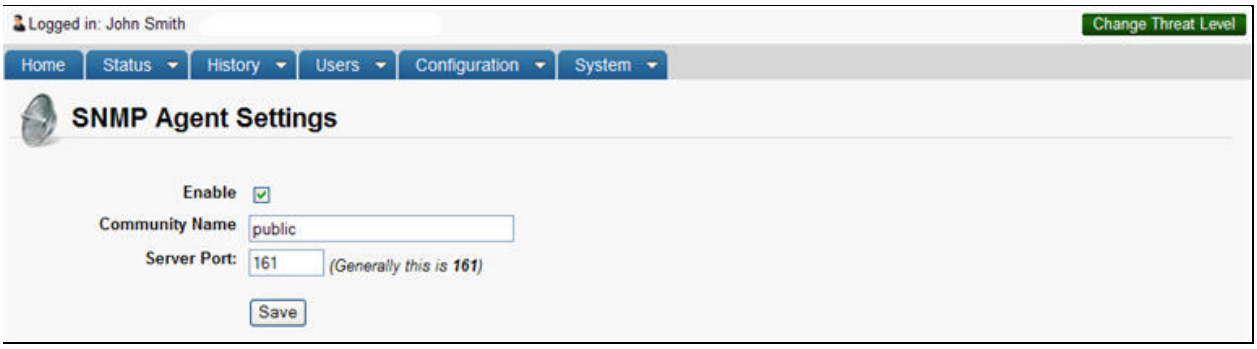


Figure 156. System: SNMP Agent Settings

4. Check the box next to "Enable." It is left unchecked by default.
5. Enter the community name.
6. Enter the server port next to the respective field.
7. Click Save. You are returned to the System page.

Upgrading Your Firmware

On occasion, Brivo will issue an upgrade of the Brivo Onsite Server firmware. When this occurs, you will need to contact Brivo Technical Support with the unit serial number for your Brivo Onsite Server to verify your support contract and request the firmware upgrade.

This operation is restricted to administrators with appropriate permissions.

	***WARNING:** Database Backups and Firmware Upgrades* *When performing a backup for the Brivo Onsite Server prior to upgrading firmware, it is important to allow the backup process to complete entirely before proceeding with firmware upgrades. This ensures the integrity of the backup process and prevents any interruptions that may cause future problems.*

	***WARNING:** Firmware Upgrades and Maintenance Mode* *When upgrading the firmware of the Brivo Onsite Server, the appliance will automatically enter maintenance mode.*

To upgrade the application firmware:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Settings. The Settings sub-navigation menu displays.
3. From the Settings sub-navigation menu, click Upgrade Firmware. The Upgrade Firmware page displays.

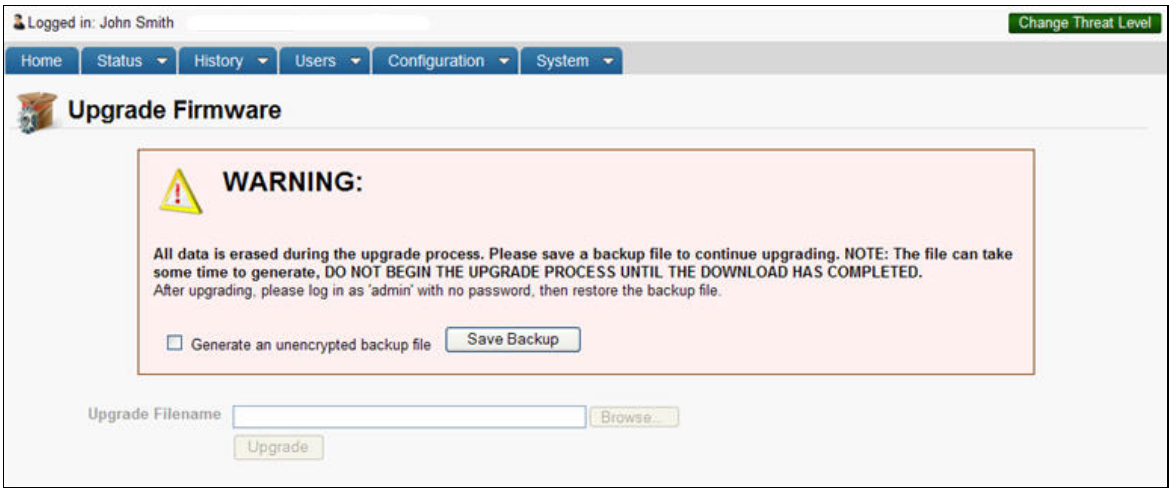


Figure 157. Upgrade System Firmware

4. If you want the backup file of your current database to be unencrypted, click the Generate an unencrypted backup file checkbox.
5. Create an encrypted backup of your current database by clicking Save Backup. Your operating system guides you through the procedures for saving the backup.
6. Enter the name of the upgrade file in the Upgrade Filename field, or click Browse to search your system for the appropriate file
7. Click Upgrade. The upgrade process runs, outputting its progress as it goes.

	***WARNING:*** *Do not interrupt upgrades!* *While the system takes every possible measure to ensure a graceful rollback in the event of failure, interrupting the upgrade process may render the system inoperative*

8. At the conclusion of the upgrade, the system will restart.
9. Log back into the application and follow instructions above to restore the database.

Upgrading Panels

Upgrading panels with the Brivo Onsite Server is handled through the Upgrade Panels page. Panels can be upgraded to the latest firmware version either individually or all at once.

This operation is restricted to administrators with appropriate permissions.

To upgrade a panel

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Settings. The Settings sub-navigation menu displays.
3. From the Settings sub-navigation menu, click Upgrade Panels. The Upgrade Panels page displays showing all the available panels and their current firmware version.

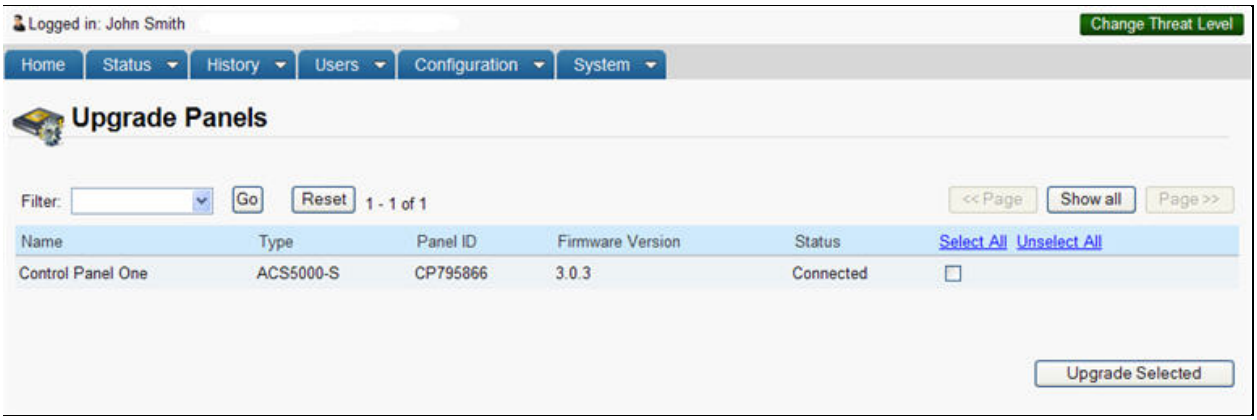


Figure 158. Upgrading a Panel

4. Select the panel you wish to upgrade individually by checking the checkbox or click on the Select All link to choose all panels for upgrade.
5. Once the panels are selected, click on the Upgrade Selected button in the bottom right corner of the page.
6. The upgrade process will begin. You will notice that the status of the panels being upgraded will change to Upgrading.
7. Once the process is complete, the panel being upgraded will show the new upgraded firmware version and the status will return to Connected.

License Keys

License keys are files that "unlock" and allow a certain number of parts of the Brivo Onsite Server to function. For example, a User Key allows a certain number of Users to be loaded into the Brivo Onsite Server. A list of active keys is shown on the License Key page under the System tab. In addition to types of license keys, there are also date ranges, so that certain license keys may be valid for a period of time, for example, one year, before a new license key must be entered.

Using the example above, if a 100 User Key was licensed to a Brivo Onsite Server and the administrator attempted to enter 101 users, the system would not allow any new users to be entered into the system until a larger license key was installed (for example 250 Users) or the 101st user was deleted from the system.

Types of Keys

User Key – allows the specified number of users to be entered into the system.

Reader Key – allows the specified number of readers to be entered into the system.

Input Key – allows the specified number of inputs to be entered into the system.

Output Key – allows the specified number of outputs to be entered into the system.

Session Key – allows the specified number of concurrent sessions to occur.

Account Key – allows the specified number of accounts to be created in the system.

DataSync Key – allows DataSync to occur on the Brivo Onsite Server.

DVR Driver – allows the specified DVR driver to be loaded into the Brivo Onsite Server.

Guard Tour Key – allows the account to utilize Guard Tour functionality on the Brivo Onsite Server.

Branding Key – allows the Brivo Onsite Server to install specific branding.

Salto Key – allows the Brivo Onsite Server to utilize Salto door locks and routers.

DED Key – allows the Brivo Onsite Server to use TKE elevator system functionality.

NDE Lock Device – allows the Brivo Onsite Server to use NDE Gateway and NDE Lock functionality.

The second section of the License Key page shows the Maximum Capacity of the current licenses.

Key Type – lists the type of license key, for example, Users or Accounts.

Allowed – the maximum number of the key type allowed in the Brivo Onsite Server or whether or not a process is allowed, for example, DataSync or use of DVR drivers.

Current – the current number of the key type in the Brivo Onsite Server.

To upload a license file:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Settings. The Settings sub-navigation menu displays.
3. From the Settings sub-navigation menu, click License Keys. The License Keys page displays.
4. Click Browse to locate the valid license file provided to you by Brivo.
5. Click Upload to upload the valid license file.

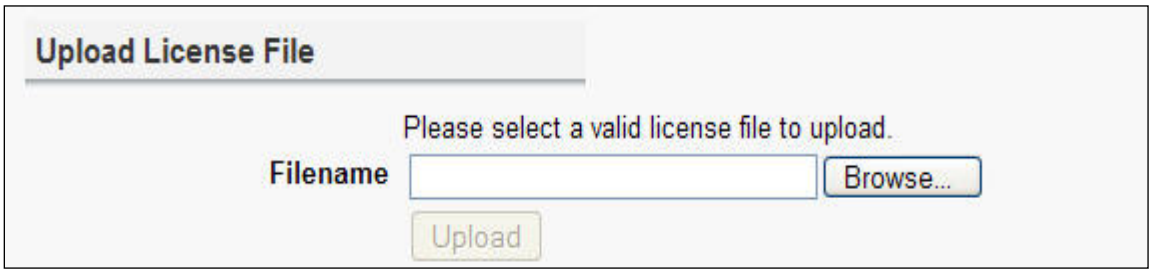


Figure 159. Upload License File

6. When a new license file is uploaded, the system must be rebooted. Click Reboot System and allow the process to complete.
7. Once complete, return to the License Key page and make certain the appropriate changes have occurred.

Manage Branding

The Branding section of the Brivo Onsite Server allows the administrator to make certain cosmetic changes to the interface of the Brivo Onsite Server.

To manage branding:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Settings. The Settings sub-navigation menu displays.
3. From the Settings sub-navigation menu, click Manage Branding. The Manage Branding page displays.

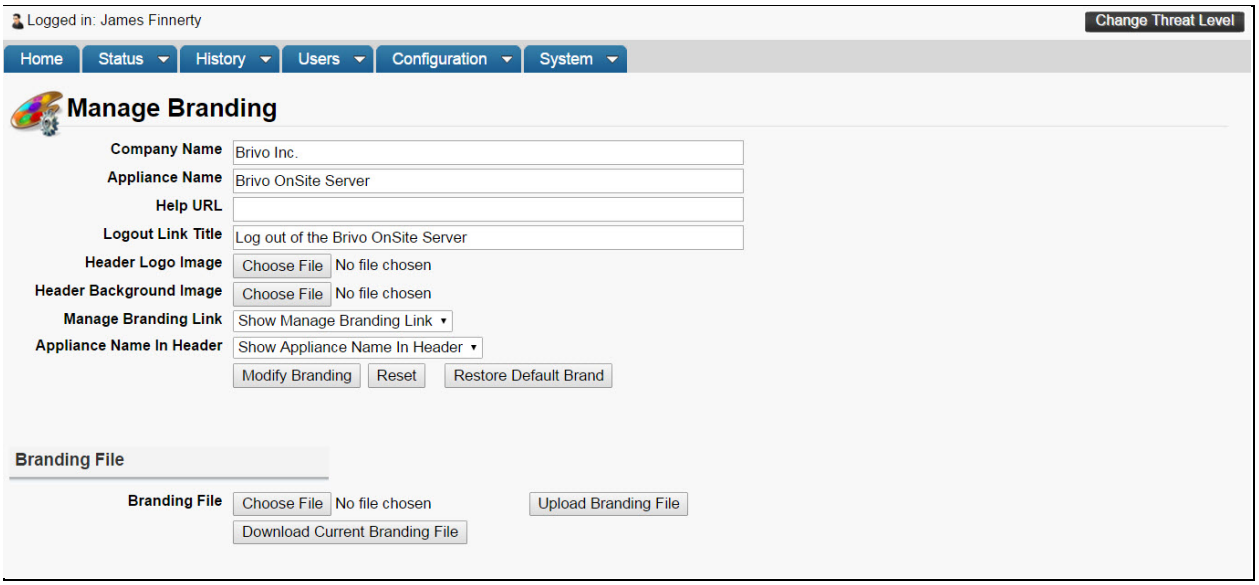


Figure 160. Manage Branding

4. Enter the Company Name you wish to use.
5. Enter the Appliance Name you wish to use.
6. Enter the Help URL you wish to link to.
7. Enter the Logout Link Title you wish to have appear when you mouse over the Logout link.
8. To upload a new Header Logo Image, click Browse and upload the file.
9. To upload a new Header Background Image, click Browse and upload the file.

	***NOTE:*** *Acceptable file formats for branding in the Brivo Onsite Server* *Any file uploaded for use as a Header Logo Image or as a Header Background image must be in .jpg, .png, or .gif format.*

10. To remove the Manage Branding link from the System link, choose Hide Manage Branding Link from the dropdown list.
11. To remove the Appliance Name from the header of the page, choose Hide Appliance Name In Header from the dropdown list.

12. To finalize any changes made above, click the Modify Branding button.
13. To reset any changes made to the fields in Manage Branding before saving, click Reset to restore the fields to their original entries. Once Modify Branding has been clicked, the Reset button will only restore back to the last time Modify Branding was clicked.
14. To restore the fields in Manage Branding to their original factory settings, click the Restore Default Brand button which will restore the original settings.
15. If a branding file is available for upload, click Browse to locate the file and Upload Branding File to upload the settings to the fields on the Manage Branding page.
16. To save a copy of the current branding file, click Download Current Branding File and click Save in the popup window.

Security Settings

The Security Settings page provides options for enhanced security of the Brivo ACS6000-A panels, ACS5000-A panels, ACS-IPDC-A or ACS300-A controllers by allowing administrators to enable FIPS Mode, enforce TLS 1.2, and enforce HTTP Strict Transport Security (HSTS) header.

FIPS mode specifies that the Brivo Onsite Server will use only FIPS 140-2 validated embedded encryption modules for all communication with Brivo ACS6000-A panels, ACS5000-A panels, ACS-IPDC-A or ACS300-A controllers. It is engaged by default.

To enable FIPS mode:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Settings. The Settings sub-navigation menu displays.
3. From the Settings sub-navigation menu, click Security Settings. The Security Settings page displays.
4. Click the FIPS Mode checkbox if you wish to have FIPS mode enabled. If you enable FIPS mode, a system reboot is required to activate changes.
5. Click the Enforce TLS 1.2 checkbox if you wish to have the control panel only utilize TLS 1.2 or higher when communicating.
6. Click the Enforce HTTP Strict Transport Security (HSTS) header checkbox if you wish to have the Brivo Onsite Server declare that web browsers should only interact with it using secure HTTPS connections.
7. Click Save. You are returned to the Security Settings page.

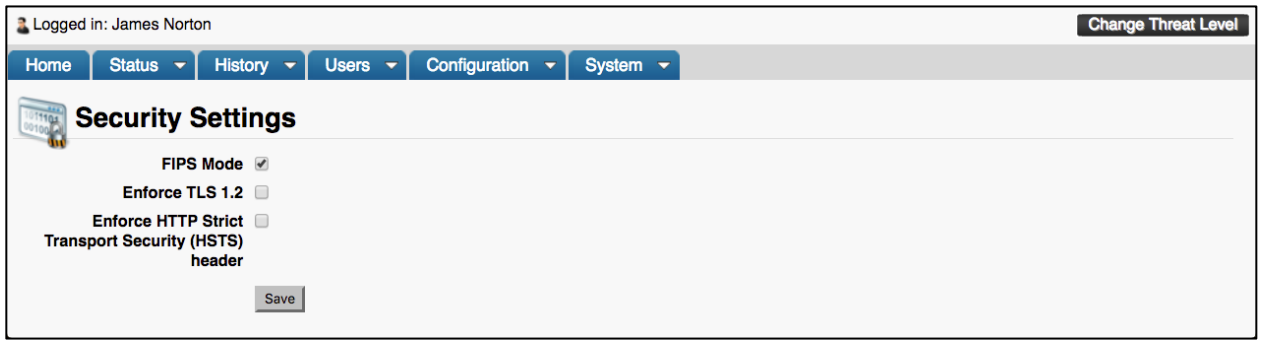


Figure 161. Security Settings Page

Importing User Data

Brivo Onsite Server provides a mechanism for importing user data from a flat file.

The systems support importing user data from tab-separated flat files, without quote characters. These files are easily created by many applications, including spreadsheet or simple database applications. Be sure to observe the following rules when exporting a file from another application or tool for import into Brivo Onsite Server:

Use tab characters as a field separator

Do not use any quoting or quote characters around fields

Embedded tabs are not supported on the input stream

Administrators with appropriate permissions can import user data.

To import user data from a flat file:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Database. The Database sub-navigation menu displays.
3. From the Database sub-navigation menu, click Import User Data. The Import User Data page displays.

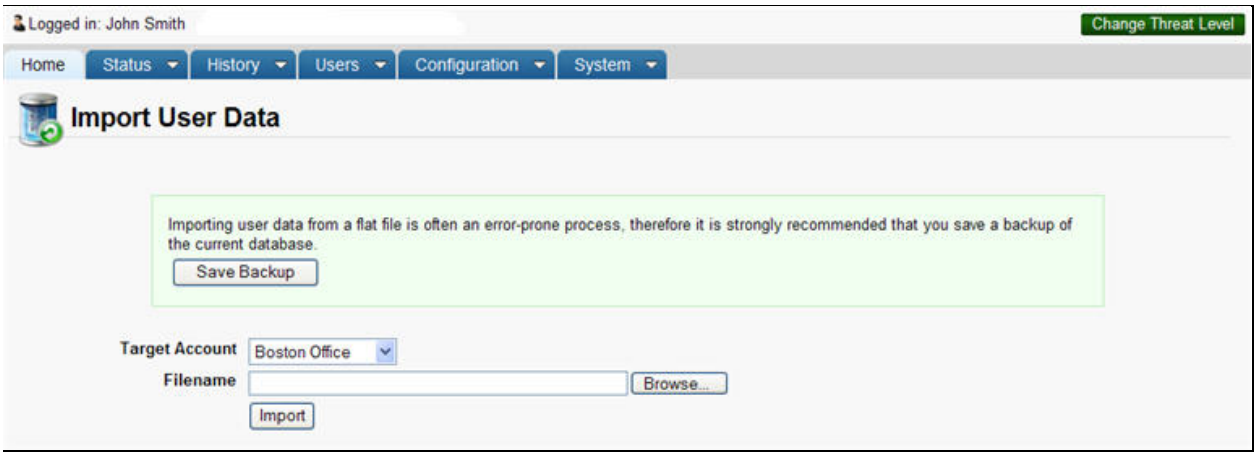


Figure 162. Import User Data, Step One

4. Create a backup of your current database by clicking Export backup file. Your operating system guides you through the procedures for saving the backup.

	***WARNING:** Make a backup!* *Importing data into a system has a tendency to magnify the smallest errors. If data is imported into the wrong fields, the easiest way to clean up is to restore the backup - if you've made one just before starting the import.*

5. After the database is successfully backed up, select the Target Account to which you want to import user data.
6. Enter the name of the file you want to import in the Filename field, or click Browse to search your system for the appropriate file.

7. Click Import. If you have entered a valid filename, the second portion of the Import User Data page displays.

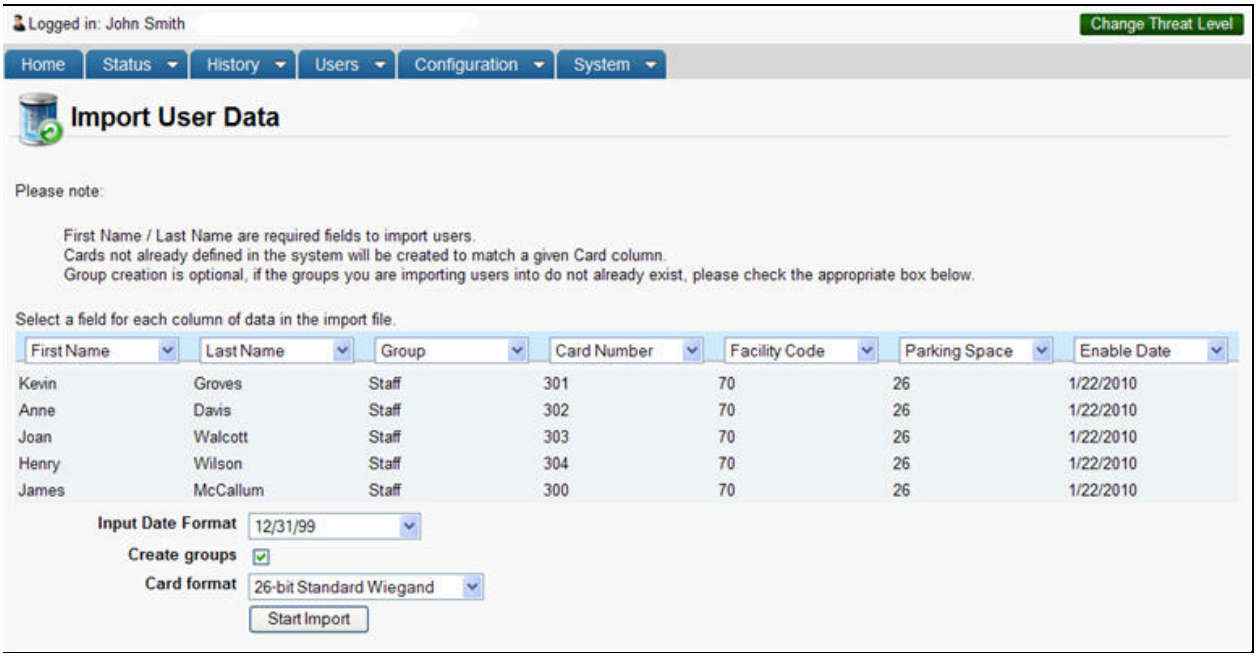


Figure 163. Import User Data, Step Two

8. You can import multiple columns of user data from a source file. Click which columns you want to include from the drop-down lists in the middle of the page. You must include First Name and Last Name as two of the columns. For the remaining columns you can select any of the information displayed on the User Detail page, such as Group, PIN or Card.
9. From the Input Date Format drop-down list, click the date format used in the input file.
10. The Create Group checkbox causes the system to create groups as necessary to satisfy relationships in the import file. If this box is not checked, any group values in the input file that are not a match to an existing group name will be output as an error and the user/group relationship will not be created.
11. If you are importing Card numbers, click a valid Card format from the drop-down list.

	NOTE: *It is important to make certain that if you are importing card numbers that have a facility code, that one of the columns being imported contains the Facility Code information. This will ensure that the cards function properly once imported.*

12. Click Start Import. The import process will report its progress and will output a message when the import has finished. Larger imports may take a while.

Backing up Your Database

Your database should be backed up on a regular basis. You must also back it up before upgrading the application firmware. Brivo Onsite Server facilitates the backup and restoration of your database, as well as the export of the System Activity Log.

The frequency of system backups depends on the amount and regularity of changes to the data in the Brivo Onsite Server. As a rule, it is strongly recommended that backups be taken, either manually or automatically, to preserve data against unintentional or catastrophic loss.

Administrators with appropriate permissions can make backups of the system.

To create a backup of your database:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Database. The Database sub-navigation menu displays.
3. From the Database sub-navigation menu, click Backup & Restore. The Backup & Restore page displays.

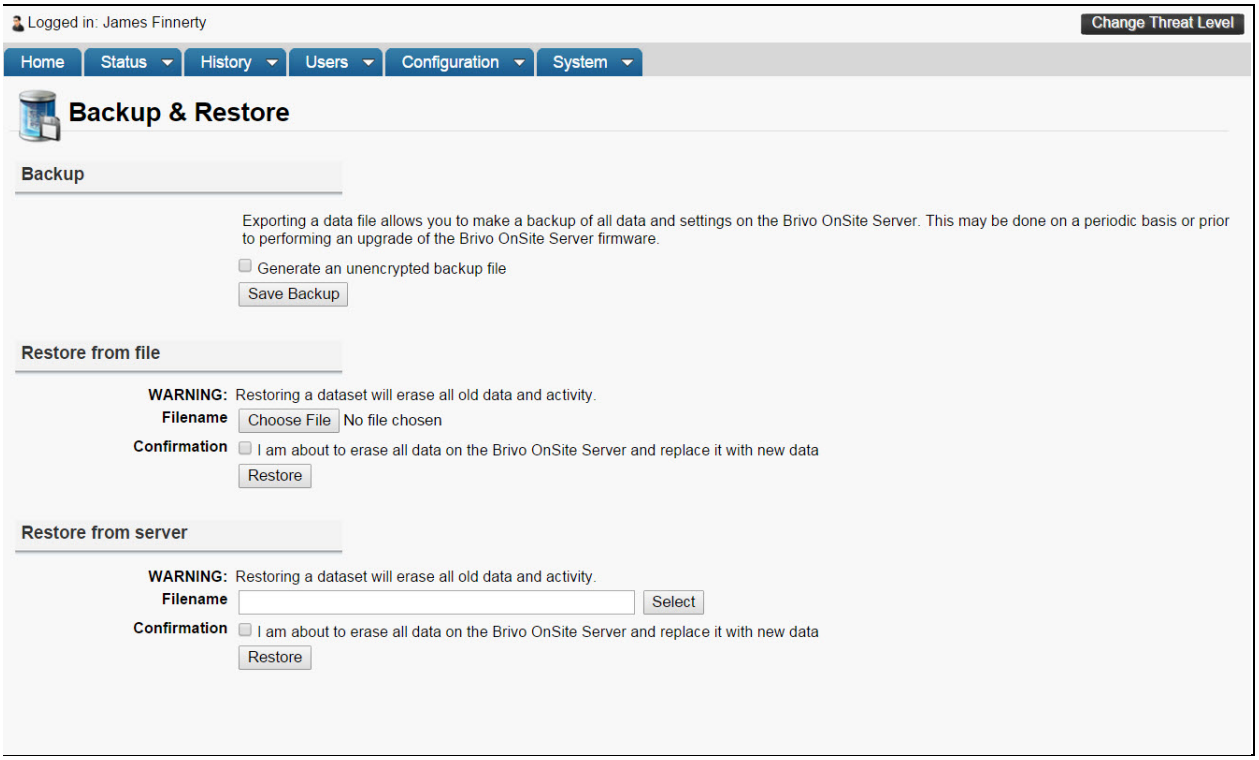


Figure 164. Backup and Restore the Database

4. All backup files are normally encrypted. If you desire that the backup file be unencrypted, check the Generate an unencrypted backup file checkbox.
5. Click Save Backup in the Backup section of the page. Your browser guides you through the procedures for saving the backup file. Progress is reported along every step of the way. Firmware updates are not available during this Database Backup process.

To restore a backed up database:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Database. The Database sub-navigation menu displays.
3. From the Database sub-navigation menu, click Backup & Restore. The Backup & Restore page displays.
4. In the Restore section of the page, enter the name of the file you want to restore in the Filename field, or click Browse to search your system for the appropriate file.

WARNING: *Database Restoration and network configuration*

When you restore your database file, you completely overwrite all existing data with the data from the restoration file. This includes possibly restoring a new set of network settings, which may affect your browser's ability to connect to the appliance.

For Brivo Onsite Server, it may be necessary to access the console to reset the network configuration if they've been overwritten by the restore.

5. Once you are certain that you want to complete the restoration, check the Confirmation box that reads I am about to erase all data on the system and replace it with new data.
6. Click Restore. The system restore can take a while to complete. Progress is reported along every step of the way.

To restore a database that was backed up to a server:

If you have a backup server configured, you can restore from a backup file stored on the server. For more information on backup servers, see the section, *Backup Server*.

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Database. The Database sub-navigation menu displays.
3. From the Database sub-navigation menu, click Backup & Restore. The Backup & Restore page displays.
4. In the Restore from Server section, click on the Select button. A window will appear with a list of backup files on the server.
5. Select a backup file from the list. The file name will appear in the box next to the Select button.
6. Once you are certain that you want to complete the restoration, check the Confirmation box that reads I am about to erase all the data on the system and replace it with new data.
7. Click the Restore button. The system restore can take a while to complete. Progress is reported along every step of the way.

Backup Server

Brivo Onsite Server enables administrators with appropriate permissions to configure their servers to back up automatically, and according to either a Windows share or SSH methods. These tasks should only be performed by a network administrator.

To configure Backup Server settings

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Database. The Database sub-navigation menu displays.
3. From the Database sub-navigation menu, click Backup Server. The Backup Server page displays.
4. In the Auto Backup section of the page, check the "Enable" box to enable automatic backup of your server.

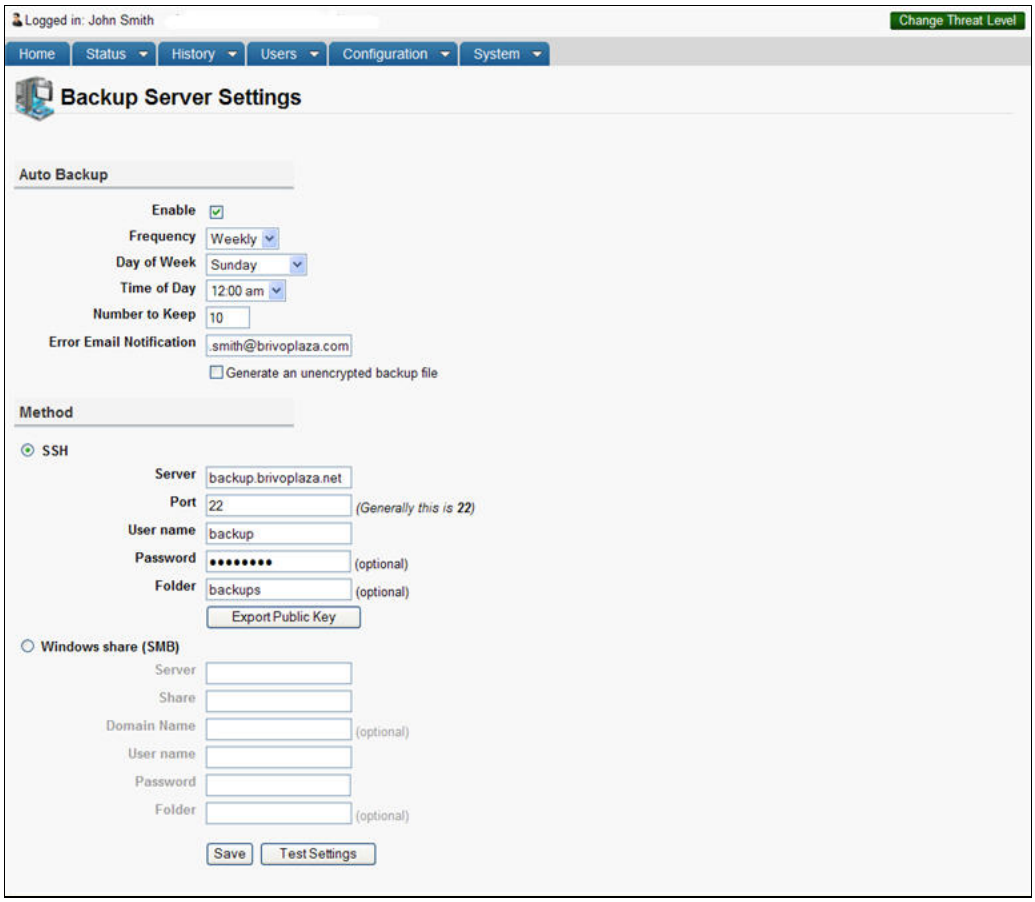


Figure 165. Backup Server Settings

5. Select the frequency of automatic backup from the dropdown list.
6. Select the day of the week from the dropdown list for your automatic backup.
7. Specify the time of day for your backup by selecting a time from the dropdown list.
8. Enter the number of backups to keep in the field next to Number to Keep.
9. Enter the email address for notification of an error with automatic backup.

10. To generate an unencrypted version of the backup file, fill in the checkbox next to Generate an unencrypted backup file.
11. In the Method section of the page, choose either SSH or Windows share. For SSH, enter the Server, Port, User name, Password and Folder (optional). For Windows share, enter the Server, Share, Domain Name (optional), User name, Password, and Folder (optional). For increased security, a public key may be obtained by clicking "Export Public Key" to allow password-less SSH connections.
12. Click Save. Or, if you would like to test these settings, click Test Settings.

Report Service

Brivo Onsite Server enables administrators with appropriate permissions to utilize the report service tool to export database information for use with external tools.

	NOTE: *Use of the Brivo Onsite Server Report Service* *An example of using Report Service can be found in the Appendices at the end of the Brivo Onsite Server Administrator's Manual.*

To activate report service:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Database. The Database sub-navigation menu displays.
3. From the Database sub-navigation menu, click Report Service. The Report Service page displays.
4. To activate report service, click the Report Service checkbox.
5. Enter a new password in the Password field. This is a new password, not your current administrator password.
6. Confirm the password in the Confirm Password field.
7. Click Save.

Figure 166. Activating Report Service

Configuring the Network

You can configure the network to use manually defined (static) network settings, or to use an automatic network service (DHCP).

Administrators with appropriate permissions can configure network settings.

To configure your network settings:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Network. The Network sub-navigation menu displays.
3. From the Network sub-navigation menu, click Network Configuration. The Network Configuration page displays.

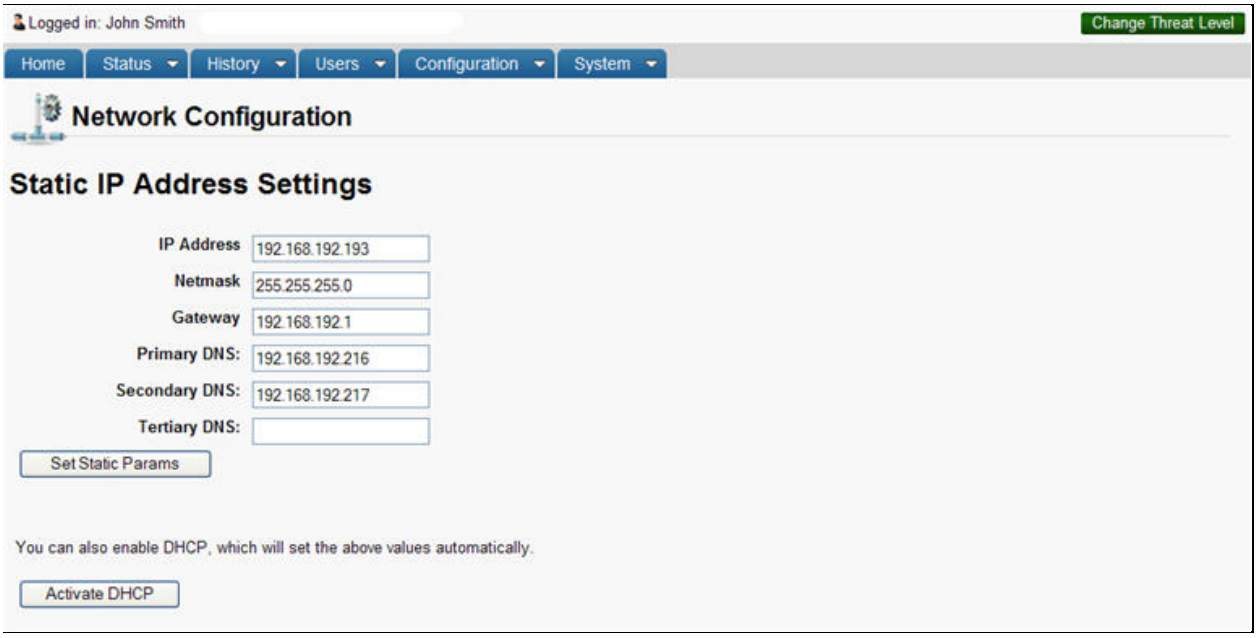


Figure 167. Configure the Network

4. To configure a static network:
    - Enter the IP Address of the system, distinguishing this from other nodes on the same network.
    - Enter the Netmask address, a mask used to separate a sub-network of machines; for example, 255.255.255.0
    - Enter the Gateway address, the address of the machine acting as a gateway between the local network and other networks, such as the internet.
    - Enter the Primary DNS, Secondary DNS, and, if appropriate, the Tertiary DNS. These numbers tell the system which server(s) to use when converting the machine name (e.g., www.brivo.com) to the numeric IP address used on the internet. At least one (Primary) server is required, and a second (Secondary) is customary but not required.
    - Click Set Static Params. The parameters are set, and you are returned to the Network Configuration page.

5. To enable DHCP, simply click Activate DHCP. DHCP becomes activated, possibly changing the IP address of the control panel, and you are returned to Network Configuration page.

	*NOTE:* *If DHCP is activated, this page simply displays a message to that effect*.

	***WARNING:*** *Changing Network Settings* *Be aware that when modifying the network settings, the IP address used by the system may change, forcing you to manually change the URL of the browser through which you are accessing the device.* *For Brivo Onsite Server, the admin console is the safest way to set network parameters.*

Configuring Network Routing

The Network Routing page provides utilities for configuring static routes that the control panel may need to use to reach other resources on the network, if required.

Only System Account Administrators with read/write access can configure static routes.

	***WARNING:** Static Routes* *Establishing static routes is rarely required, and should be done only with the advice of the network administrator for the site where the system is installed.*

To configure a network route:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Network. The Network sub-navigation menu displays.
3. From the Network sub-navigation menu, click Network Routing. The Network Routing page displays.

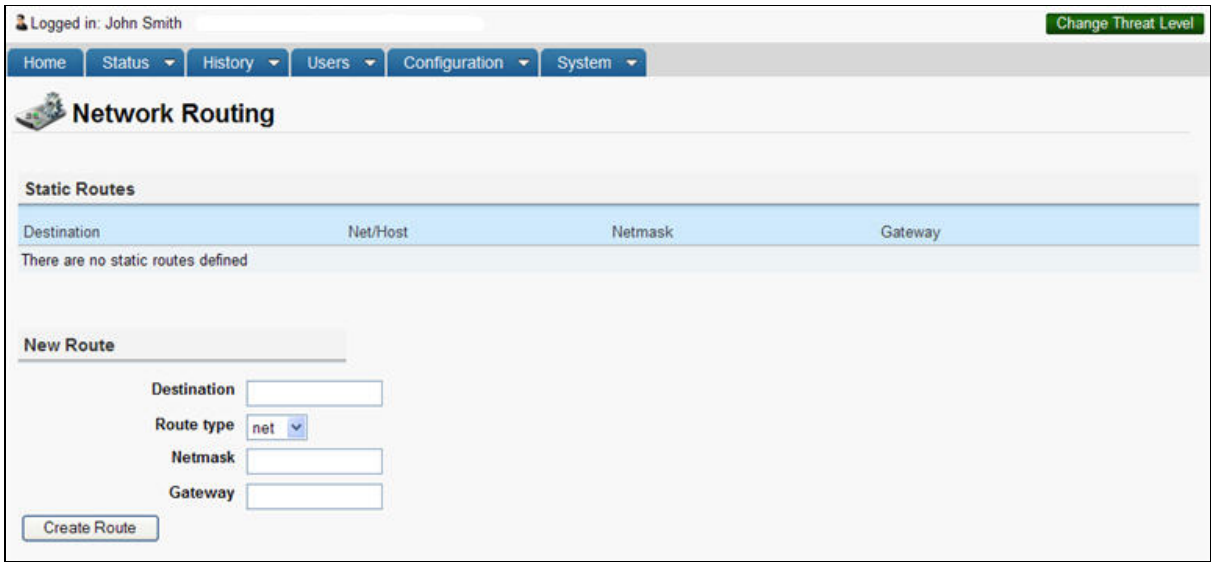


Figure 168. Configure Network Routing

4. On the bottom half of the page, enter a Destination IP Address or network.
5. Select a Route type from the drop-down list, either net or host.
6. Enter the Netmask address for the static route, a mask used to separate a sub-network of machines; for example, 255.255.255.0
7. Enter the Gateway address for the static route, the address of the machine acting as a gateway between the local network and other networks, such as the internet.
8. Click Create Route. The page reloads with the new route displayed in the table.

Configuring the SMTP Server

In order to use the Email Notification functionality, you must first configure your SMTP Server. SMTP (Simple Mail Transfer Protocol) is how email is sent between machines on the Internet.

Administrators with appropriate permissions can configure the SMTP server.

To configure your SMTP server:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Network. The Network sub-navigation menu displays.
3. From the Network sub-navigation menu, click SMTP Server Settings. The SMTP Server Settings page displays.

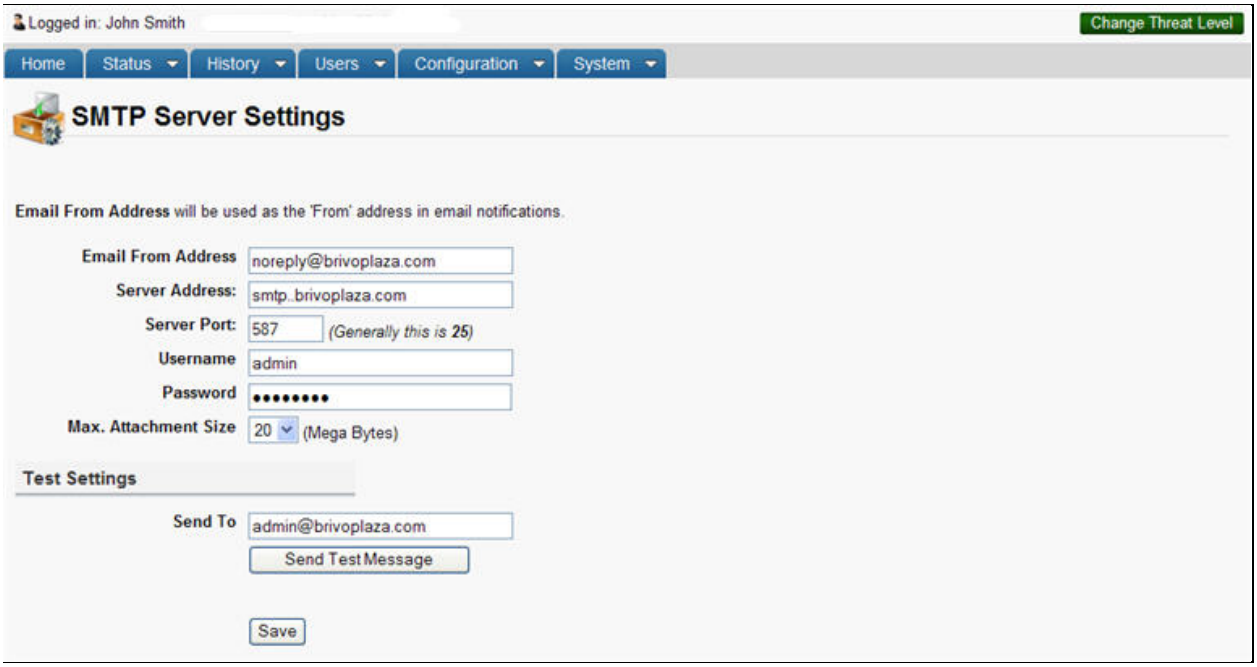


Figure 169. Configure SMTP Server

4. In the Email From Address field, enter the email address you would like to appear in the From field of email notifications.
5. Enter the address of your SMTP server in the Server Address field.
6. Enter the port of your SMTP server in the Server Port field. This value is usually 25.
7. Enter the Username and Password of the administrator configuring the SMTP server.
8. Choose the Maximum Attachment Size (1 to 20 megabytes) from the dropdown menu. This will affect files generated for scheduled reports. If the file size for the scheduled report exceeds the maximum attachment size, the file will not be sent.
9. To test your Email settings, enter an email address in the Send To field, and then click Send Test Message. The system attempts to send a simple message to the specified email address and reports the status of the interactions with the email server.
10. Click Save. Some internal applications may take a moment to restart automatically at this point.

Panel Discovery

Panel discovery is an automated process by which the Brivo Onsite Server scans a series of IP addresses for available devices. This process will find Brivo ACS6000-A, ACS300-A, ACS5000-A, ACS-IPDC-A panels as well as HID E-400 devices.

To use panel discovery:

	NOTE: *Using the Brivo Onsite Server's Panel Discovery feature will cause the Brivo Onsite Server to scan a range of IP addresses. This may trigger a false alarm on network intrusion detection systems.*

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Network. The Status sub-navigation menu displays.
3. From the Network sub-navigation menu, click Panel Discovery. The Panel Discovery page displays.

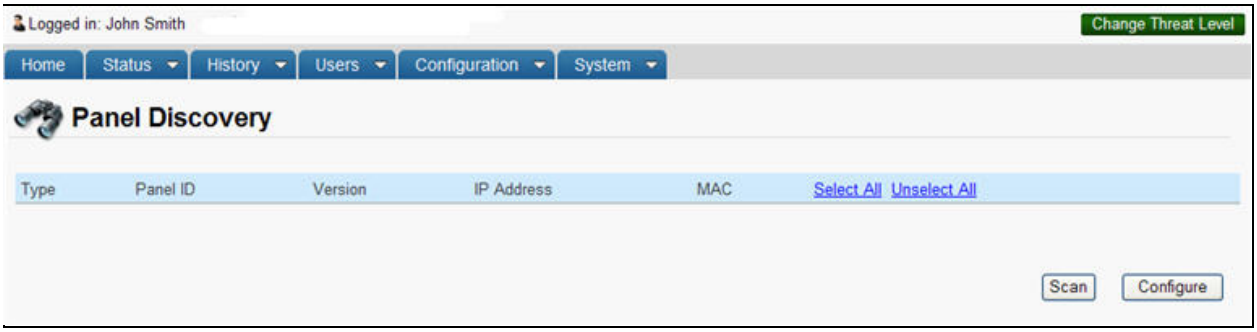


Figure 170. Panel Discovery

4. Click the Scan button. The Panel Scan popup window appears.
5. Enter the beginning IP address and the ending IP address to scan. When finished, click the Scan button. The **Brivo Onsite Server** will scan the IP range and report back any discovered panels.

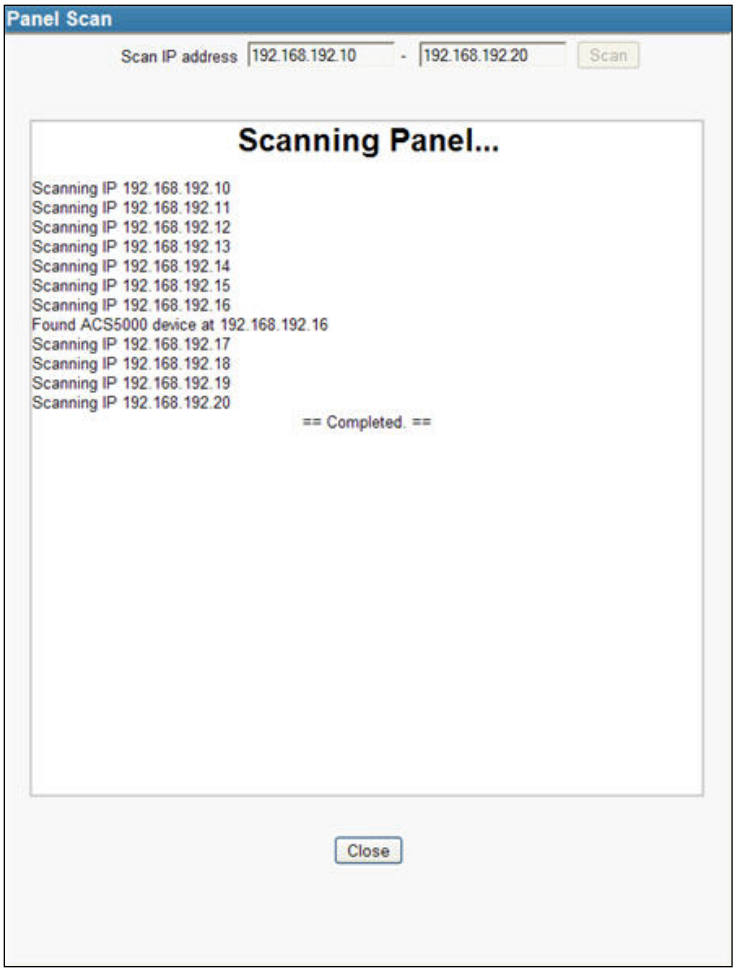


Figure 171. Panel Scan

6. Once the scan is complete, click Close. You are returned to the Panel Discovery page where any unassigned panels detected with be displayed.

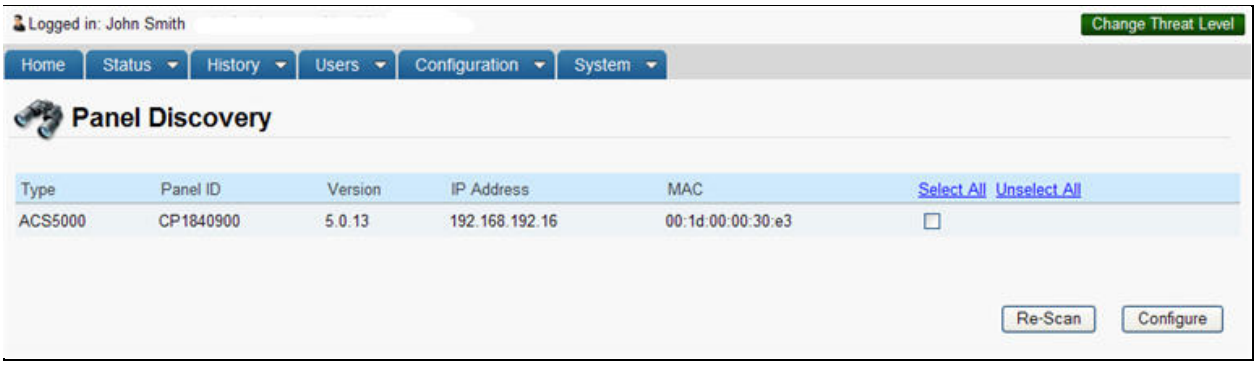


Figure 172. Discovered Panels

7. Discovered panels will display Type of panel, the CP number (Panel ID), the current Version of firmware, the assigned IP address, and the MAC Address to the discovered panel.

8. If multiple panels are discovered, the administrator may individually select each using the provided checkboxes or simply click Select All to select all discovered panels. Administrators may also click Unselect All to deselect all discovered panels.
9. Once a panel has been selected, click Configure. The Configure Panel popup window will appear.

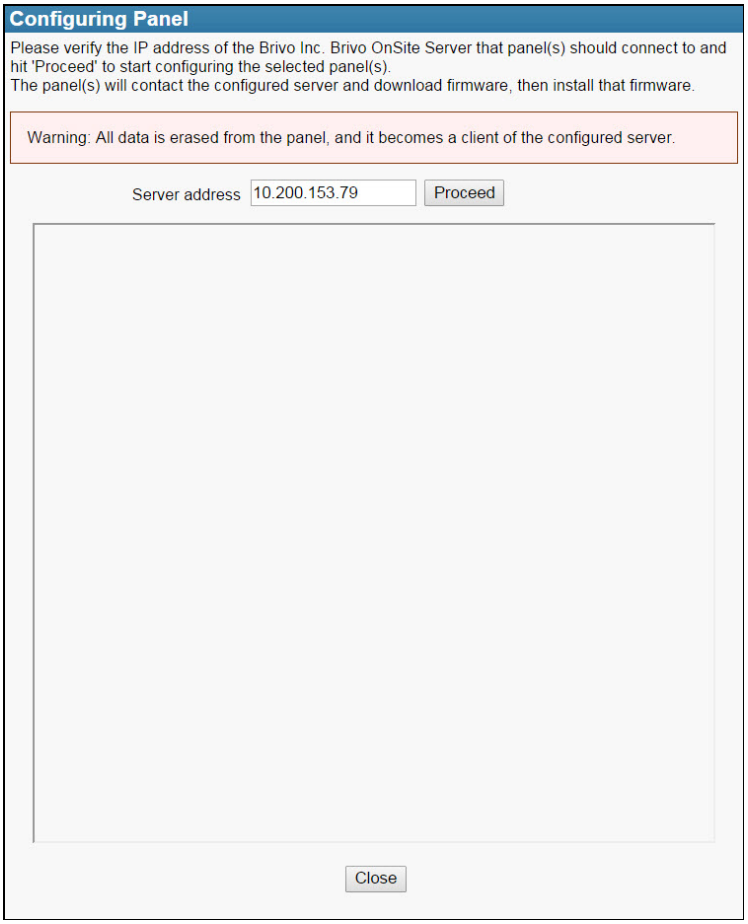


Figure 173. Configuring Panel

	***WARNING:*** *All data is erased from the panel, and it becomes a client of the configured server*

10. Verify the server address is accurate and click Proceed.

Custom Server Certificates

Custom Server Certificates displays the current active certificate in use and allows the administrator to upload a new certificate file.

To upload a new certificate file:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Network. The Status sub-navigation menu displays.
3. From the Network sub-navigation menu, click Custom Server Certificates. The Custom Server Certificates page displays.
4. Click on the Browse button and select the .PEM file you wish to upload.
5. Click on the Upload button to install your custom server certificate.
6. The Active Certificate information will change to denote the new Issuer and Validity.
7. For details on the active certificate, click on the Display Detail button and an expanded detailed version of the certificate will display.

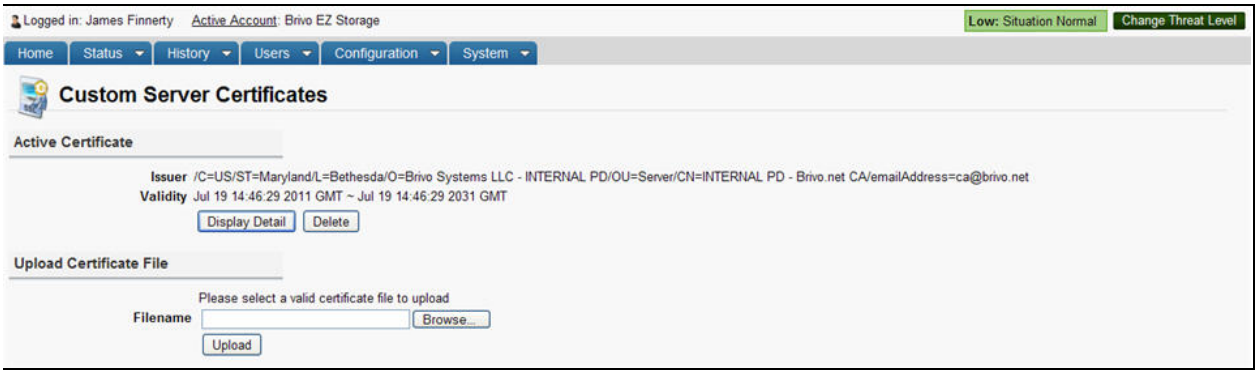


Figure 174. Custom Server Certificates

To delete a custom server certificate:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Network. The Status sub-navigation menu displays.
3. From the Network sub-navigation menu, click Custom Server Certificates. The Custom Server Certificates page displays.
4. Click on the Delete button. Click OK in the confirmation prompt. You are returned to the Custom Server Certificates page. The default self-signed certificate is loaded until a new custom server certificate is uploaded.

ES IP Pool Configuration

The ES (Elevator System) IP Pool Configuration allows an administrator to configure a specific pool of IP addresses that the Brivo Onsite Server will use to contact the elevator control system using destination dispatch instead of using general network broadcasting. For the Brivo Onsite Server, this functionality is for use with systems that work with ThyssenKrupp elevators (TKE).

Details include:

- Account Name – The account using the IP address to connect with the elevator system using destination dispatch.
- IP Address – The specific IP address used by the Brivo Onsite Server to connect to the elevator system using destination dispatch.
- Action – The  icon which allows an administrator to delete an already configured IP address from the IP pool.

Administrators with appropriate permissions can:

Add IP addresses to the elevator system IP pool.

Remove IP addresses from the elevator system IP pool.

To add an IP address to the ES IP Pool:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Network. The Status sub-navigation menu displays.
3. From the Network sub-navigation menu, click ES IP Pool Configuration. The ES IP Pool Configuration page displays.
4. Enter the desired IP address in the IP Address field and click the  icon.
5. Click Save. The IP address will appear under the List of Addresses.

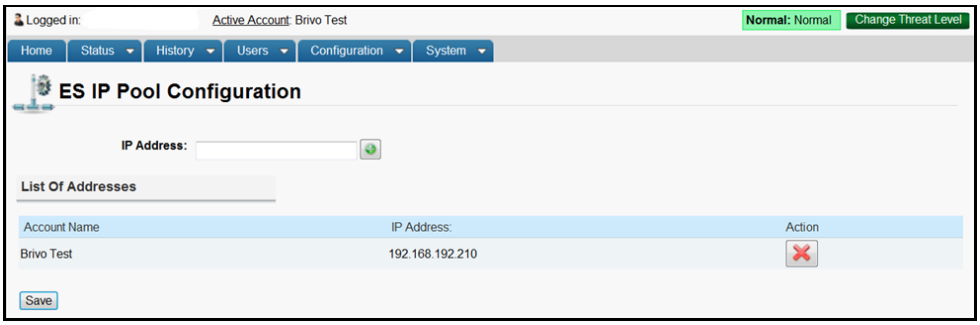


Figure 175. Elevator System IP Pool Configuration

To remove an IP address from the ES IP Pool:

1. Scroll over the System link. The sub-navigation menu displays.
2. From the sub-navigation menu, click Network. The Status sub-navigation menu displays.
3. From the Network sub-navigation menu, click ES IP Pool Configuration. The ES IP Pool Configuration page displays.

4. Find the IP address you want to remove from the ES IP Pool and click on the corresponding  icon. The selected IP address will disappear from the page.
5. Click Save. The IP address will be deleted from the ES IP Pool and you will be returned to the ES IP Pool Configuration page.

18.Tenant Accounts

Typically, there will be a single Account defined in Brivo Onsite Server, the System Account. However, if sections of a facility are leased out, there may also be one or more Tenant Accounts (see Appendix A for details). In such cases, the System Account is used to manage the overall facility, such as access to lobby doors or a cafeteria. Tenant Accounts, on the other hand, are used to manage the access of users, groups and devices associated with the tenant organization.

As with the System Account, Tenant Accounts have Administrators. Although there may be multiple Administrators defined for a single Tenant Account, each Tenant Account Administrator is associated with one and only one Tenant Account.

System Account Administrators have access to all Tenant Account data. All administrators with appropriate permissions can view, create, edit, and delete Tenant Account information.

This chapter explains how Brivo Onsite Server operates differently when Tenant Accounts exist. The first section describes the changes that affect a System Account Administrator's access. The second section provides an overview of how Brivo Onsite Server functions for Tenant Account Administrators.

NOTE:

The maximum number of Tenant Accounts is determined by the licensing agreement for a Brivo Onsite Server system.

Changes in System Account Administrator Access

For the most part, a System Account Administrator's access to Brivo Onsite Server does not change much whether there are Tenant Accounts defined or not. The few changes that do occur when one or more Tenant Accounts are defined are described below.

Active Account drop-down list

When a System Account Administrator creates the first Tenant Account a new item is automatically added above the menu. This is the current Active Account. If you click on the Active Account link, the Select New Active Account popup window appears and it lists all currently defined Accounts. Selecting a Tenant Account from the list allows a System Account Administrator to view the system from the perspective of a Tenant Account Administrator.

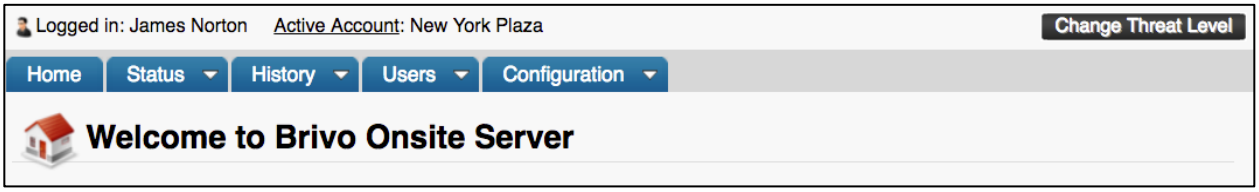


Figure 176. Active Account

When a Tenant Account is selected as the Active Account, the System Account Administrator is limited in what s/he can see or do in the system. For example, the System link disappears from the section menu since Tenant Account Administrators do not have access to this section. Also, all actions performed by this Administrator will be tracked on the Administrator Journal of the Tenant Account.

Although this Active Account link does not display when Tenant Account Administrators log in, since they can only see their own Account, it does remain visible for System Account Administrators even after they select a Tenant Account from the list. This allows the System Account Administrator to return to the System Account at any time. Additionally, the Administrator can select an Active Account and then display activity from the Dashboard according to a particular account.

To select an Active Account

1. Click on the Active Account link at the top of any page.
2. Select an account from the popup window.

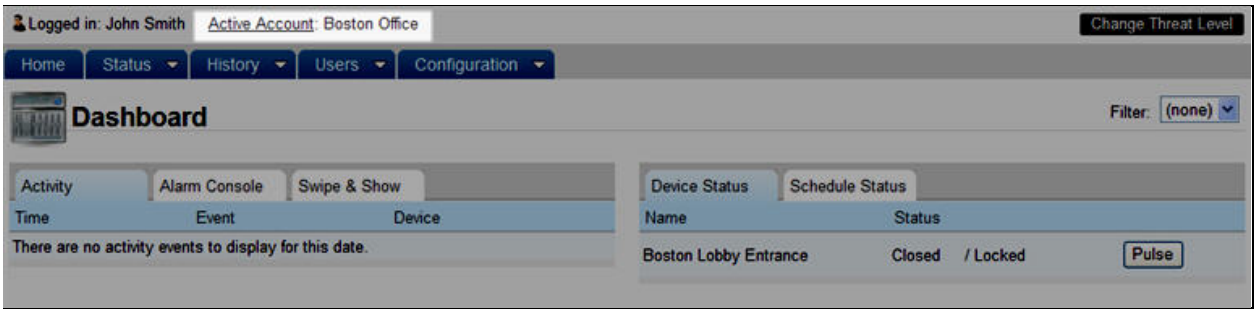


Figure 177. Select Active Account

3. The activity for the selected account will display.

	NOTE: *If a System Account Administrator accesses a page that is not visible to a Tenant Account Administrator and then selects a Tenant Account from the Active Account drop-down list, an error message will display. For example if a System Account Administrator accesses the System section and then selects a Tenant Account as the Active Account, the message:* Page Not Found *displays. Switch back to the System Account to continue working.*

Accounts list

Another change that occurs when a Tenant Account is created is that a new option is added to the Account dropdown menu. This is the Accounts option, which provides access to the Accounts list, a list of all currently defined Accounts.

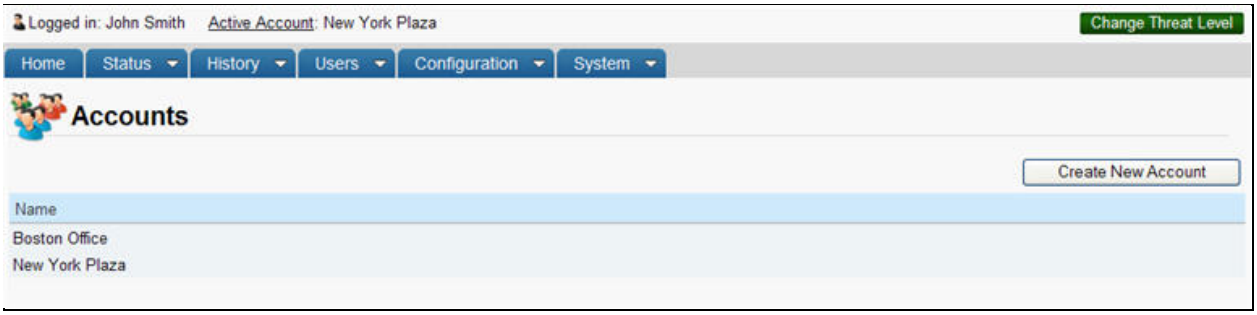


Figure 178. View Accounts List

Operations that can be performed on this page include:

Create New Account. This button appears for administrators with appropriate permissions. Click it to access a blank Edit Account page in order to create a new Tenant Account.

Name. Click the name of an account to access the corresponding Account Details page.

Deleting Tenant Accounts

Once it is created, the System Account cannot be deleted. However, System Account Administrators with read/write access can create Tenant Accounts at any time.

1. Log in as a System Account Administrator.
2. Scroll over the Configuration link. The sub-navigation menu displays.
3. From the Accounts link, click Accounts on the sidebar menu. The Accounts list displays.
4. Click the Tenant Account you want to delete. The corresponding Account Details page displays.
5. Click Delete. A warning message displays indicating that by deleting this account you will remove all its associated cards, users, schedules, and notification rules, and ownership of all Tenant Account devices is returned to the System Account.
6. Click OK to complete the deletion and return to the Accounts page with the deleted account no longer listed.

Tenant Account Devices

Tenant Accounts can be assigned 'ownership' of devices. This allows Tenant Administrators to manage all non-hardware related properties of the respective device. This also makes all activity events relating to that device visible to the Tenant Administrators.

By way of example, a Lobby Door in a building would be shared by multiple tenants, while the entrance to a particular tenant's suite would be owned by that tenant. Sharing a device between multiple tenants is done by setting the Account Visibility for the device. Multiple tenants may also activate a device, so long as the Activate Devices checkbox is checked under the Account Visibility section. However, a device cannot be both owned by a Tenant Account and shared with other Tenant Accounts at the same time.

Account Visibility

When Tenant Accounts are defined, there is an additional Account Visibility section that appears at the bottom of the Edit Device page when the Device type is Door or Valid Credential Device. The Account Visibility feature allows a door to be shared among Tenant Accounts. For example, a café located in a building may want to restrict access for certain parts of the day, but may want to grant access to all Tenant Accounts during meal hours.

To share a Door or Valid Credential Device with a Tenant Account:

1. Scroll over the Configuration link. The sub-navigation menu displays.
2. From the Devices link, click Devices. The Devices list page displays.
3. Access the Edit Device page:
    - To share an existing Door or Valid Credential Device, click that device to access the Device Details page then click Edit.
    - To share a new Door or Valid Credential Device, click Create New Device, select Door or Valid Credential Device from the Device type drop-down list, and then click Next.

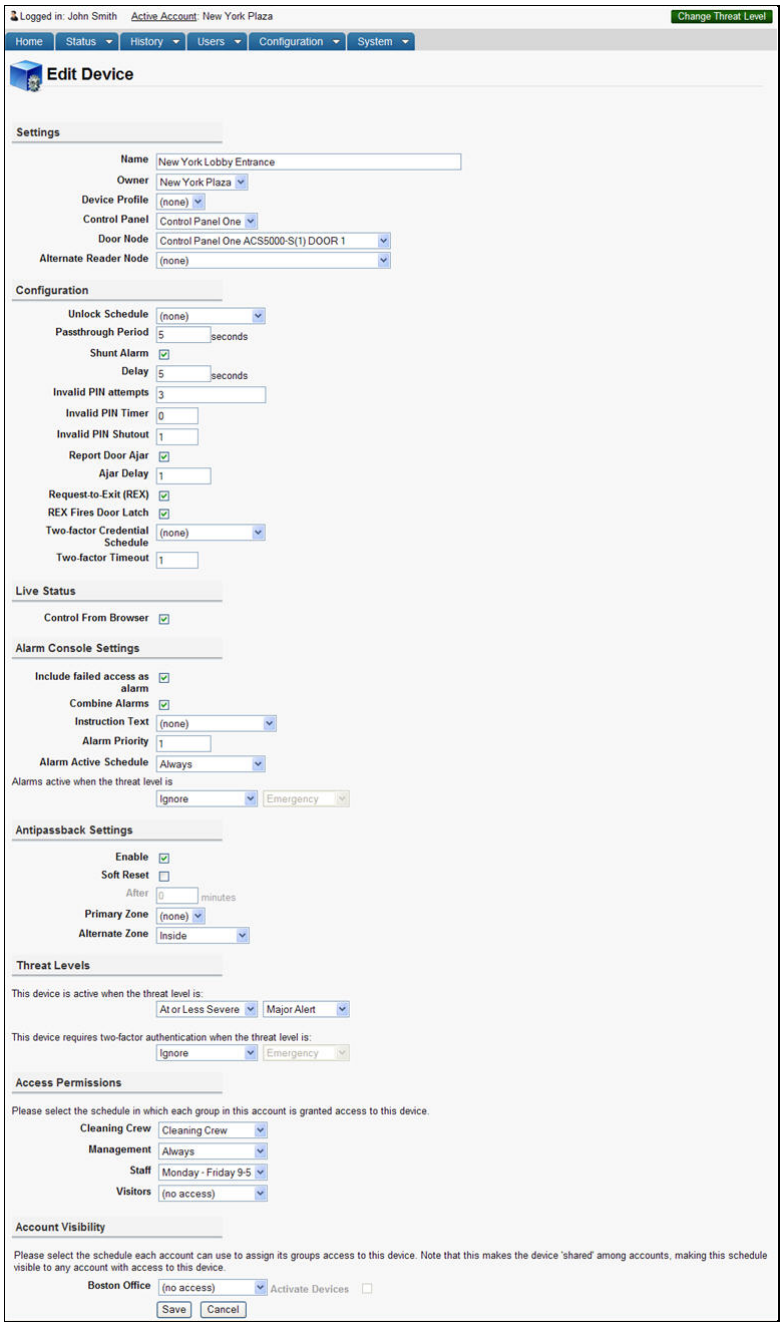


Figure 179. Share a Door or Valid Credential Device

4. For new devices, follow the procedures in the *Managing Devices* section for data entry guidelines *not* related to the Account Visibility section.

5. In the Account Visibility section, for each Tenant Account listed, select a schedule from the drop-down list to define when users of that Account have shared access to the device being configured. If you do not want a Tenant Account to have shared access, leave (no access) selected. Select the Activate Devices checkbox to allow the Tenant Administrators for the selected Tenant Accounts to be able to activate this device.

6. Click Save. The Device Details page displays with the shared status for each Tenant Account listed in the Account Permissions section at the bottom of the page.

Tenant Administrator Access

As with System Account Administrators, some Tenant Account Administrators have certain permissions while others do not. This distinction is the same for both types of Account Administrators. In other words, administrators with appropriate permissions manage (create, edit and delete) the data to which they have access, while other administrators with fewer permissions cannot.

Following is a list of all the ways in which Brivo Onsite Server functions differently for Tenant Account Administrators. The list is broken down into sections that parallel the chapters in this document. For example, the Account section below lists the ways in which a Tenant Account Administrator's access differs from the access described in the *Account* chapter. For each section, see the corresponding chapter for more information.

Account

Tenant Account Administrators:

- Cannot view the Accounts list.
- Can view the Account Details page for the Tenant Account only.
- Cannot create new Accounts.
- Can edit their own Account contact information if they have permissions.

Schedules and Holidays

- Tenant Account Administrators with appropriate permissions can view/edit/delete Schedules and Holidays, with the exception of the Holidays created by the System Account, which are inherited across all Tenant Accounts.

Devices

Tenant Account Administrators:

- Cannot view the Hardware list or any pages used in maintaining control boards, including Board Details, Add New Board, and Edit Board Details.
- Can view only those devices that have been shared by a System Account Administrator on the Devices list. See the *Account Visibility* topic in the *Changes in System Account Administrator Access* above for more information.
- Can activate only those devices which have Activate Devices checked under Account Visibility.
- Cannot create devices.
- Can edit non-hardware related characteristics of devices owned by the Tenant account, such as the Active Schedule on a device or the Passthrough Period on a door. All hardware settings are the domain of the System Administrators only.

Cards

Tenant Account Administrators:

- Cannot view the Card Formats list or any pages used in maintaining card formats, including Card Format and Edit Card Format.
- Cannot create, edit or delete cards.
- Can assign cards to user aliases that are only valid for the permissions in that account.

Users and Groups

Tenant Account Administrators:

- Cannot edit the name of a user alias.
- Cannot edit the photo of a user alias.
- Cannot edit the enable from and expires on fields for a user alias.
- Can perform all other user and group administration like a System Administrator.

Activity Logs

Tenant Account Administrators:

- Can view the System Activity log for the Tenant Account, which shows activity related to only those devices and users to which the Tenant Account has access.
- Can see if a user from a different Tenant Account has interacted with a device on the Administrator's own Tenant Account, but cannot see the user's name. For example, an Administrator for Tenant Account "A" can see if a user from Tenant Account "B" has attempted access at a Tenant "A" door, but cannot see the user's name. The name is not visible since that would represent a leak of data between Tenant Accounts. However, this information *is* available to System Administrators.
- Can view the Administrative Journal for the Tenant Account, which tracks the actions performed by all Tenant Account Administrators. This journal also shows actions performed by System Account Administrators when they had the Tenant Account selected as the Active Account.

Dashboard

- Can control devices owned by the Tenant Account.
- Can view devices that are shared by multiple Accounts.
- Can control devices that are shared by multiple accounts if Activate Devices has been selected.

Email Notifications

- Administration of email notifications is the same for Tenant Administrators and System Administrators.

System Management

- No access to the System link or any system management pages.

Threat Levels

- Can create new threat levels.
- Ability to change threat levels must be specified in the Account section.
- No access to shared devices when the device is out of its default threat level.

19.Appendices

Appendix 1: Glossary

Account
A span of access control which identifies who has access to what areas of a facility according to which schedule, as well as what devices are associated with the facility and how they operate.

Account, Active
System Account Administrators can access all data for all Accounts at a facility. They can also choose to act as an Account Administrator for a Tenant Account by selecting that Account from the Active Account drop-down list.

Account, System
The System Account is the primary Account for a facility. A facility must have one and only one System Account. System Account Administrators can access the data maintained for all Accounts.

Account, Tenant
If sections of a facility are leased out, the System Account may be used to manage security for the entire building while Tenant Accounts are created to manage security for individual organizations. While there can only be one System Account, a facility may have multiple Tenant Accounts. Tenant Account Administrators can access only that data associated with their account.

ACS
Access control system.

Administrative Journal
A record of actions performed by Administrators, such as logging in and editing the properties of a user.

Administrator
A person with access to Brivo Onsite Server, the web-based interface. Administrators may have a variety of permissions including read only access to an account, or may have read/write access that allows them to add, change, and delete data in the system.

Administrator Role
Administrator roles are an assigned set of permissions that allow an administrator to potentially view, modify, create, delete, or allow access to the various sections of the Brivo Onsite Server.

Administrator, System Account
System Account Administrators have access to all data maintained via Brivo Onsite Server.

Administrator, Tenant Account
Tenant Account Administrators have access to only that data that is directly related to the Tenant Account with which they are associated.

Alarm Console
A tab on the Dashboard that allows administrators to view and acknowledge alarm events at devices that are configured to report alarm events.

Brivo ACS6000-A panel
The model of ACS6000 control panel that is compatible with the Brivo Onsite Server

Brivo ACS5000-A panel
The model of Brivo ACS5000 control panel that is compatible with the Brivo Onsite Server

Brivo ACS300-A controller
The model of Brivo ACS300 controller that is compatible with the Brivo Onsite Server.

Brivo Onsite
The software interface for the Brivo ACS5000-S panel when operated in its default mode.

Brivo Onsite Server
The software interface that runs on a dedicated appliance to drive multiple Brivo control panels or other compatible control panels.

Card Required Credential
A security feature that requires users to provide a card at a door, elevator, or valid credential device.

Client Mode
When a Brivo ACS5000-S has been configured to act as a client of a Brivo Onsite Server appliance, it is said to be in 'client mode'. In this mode, it has no application software of its own. The panel receives all configuration information from the Brivo Onsite Server appliance it is configured to work with.

Control Panel
A system consisting of 1-15 control boards: one Main Board and up to 14 Door Boards and/or Input Output Boards. A Brivo Onsite system consists of a single control panel, while a Brivo Onsite Server system consists of an appliance and a number of Control Panels.

Criteria
Criteria are ways to specify what data appears in a report. Criteria are built by selecting a property of a relation, an operation and a value. For example, to constrain a report on users to only those that will be expiring in the next two weeks, add a criteria for 'User Expiration Date', an operation of 'within the next' and specify a value '14 days.' Note that all rows in the report will match all given criteria.

Dashboard
The Dashboard page is the initial system form displayed after logging into Brivo Onsite Server. The Dashboard provides a two-fold functionality for monitoring and controlling the operation of system devices for authorized Administrators.

Data Entry Device (DED)
Touchscreens or keypads which are used to interact with the elevator user.

Device
A device is a logical definition of how a control panel interacts with the world. A motion detector, a temperature sensor, and an EAS pedestal are just a few examples of devices.

Device Profile
A feature that allows for the creation of a profile that can be simultaneously assigned to multiple devices, giving all such devices identical settings.

Device Type, Door
A door with an electronic means of entry, such as a keypad or card reader. A door has a descriptive name such as "Lobby Door" or "Server Room" and a number of configuration options that control its behavior.

Device Type, Input Switch
A device with one input point and one output point that has state (On or Off). The device can have these behaviors: Latch, Unlatch, Pulse, or Follow. A schedule associated with the device causes it to be available for activation via its input point during the selected times for the schedule.

Device Type, Schedule Controlled Device
A device whose input is a schedule and that has one output point associated with it. The timer's state is On during the times selected in its schedule; otherwise it is Off. The device can have these behaviors: Latch, Unlatch, Pulse, or Follow.

Device Type, Valid Credential Input Device
A device whose input is usually a card reader and that has one output point associated with it. A valid credential device has no state, so its behaviors are limited to: Latch, Unlatch, and Pulse. Valid credential input devices have permissions associated with them and appear in the group permissions area. They do not have Engage/Disengage messages because they do not have state, nor do they have schedules as their schedule behavior is defined by permissions, as with Doors.

Device Type, Event Trigger
A device whose input is the specific event associated with it from the door that the event track device is created to watch. An event track device can have one output point associated with it. The device can always have these

behaviors: Latch, Unlatch, or Pulse. If an event track device is watching for Door Ajar events, then it has state and can have a Follow behavior. If the Follow behavior is selected, then the device can have a Disengage message. The schedule associated with an event track device defines when it is active because a client might want to respond to the event differently during business hours than during non-business hours.

Email Notification
An email message that is sent in response to a set of rules including an event, a schedule and a possible target for the event.

First-Person-In
A security feature which prevents a door from unlocking until a specified period of time *and* until a member of the enabling group arrives. See *Group Enabled Schedule*.

Group
A group of users with the same access privileges for a facility. A group has a descriptive name such as "Washington Staff."

Group Enabled Schedule
A group of users responsible for activating a schedule. Until a member of this group accesses the door or device to which the schedule is linked, the schedule remains inactive and does not permit any type of access.

Guard Tour
A feature allows administrators to assign series of readers to act as tour stops that must be visited at an established interval.

Holiday
A period of time during which schedules refer to their Holiday override columns instead of to the day of week.

Keypad
A device that accepts numeric input (e.g. a PIN) from a User. A typical Keypad has 12 keys. A Keypad is connected to a control panel.

Keypad Command Device
A device feature that allows administrators to define a numeric sequence at a keypad to a specific output behavior.

Maintenance Mode
Maintenance Mode is a system state that prevents the Brivo Onsite Server from accepting panel connections. It is used during the firmware upgrade process. This allows for an upgrade and restore of the Brivo Onsite Server without interrupting the operation of the panels or causing the loss of any event data during the actual upgrade process.

Maps/Floorplans
Maps/Floorplans are imported images representing an area, for example, a building floorplan, business campus, or an individual office. Maps can have icons placed on them to represent devices, and maps can be detailed with regions linking them to other maps/floorplans.

Muster Report
A feature that allows administrators to use the normal antipassback functionality to track the presence of users in a facility.

Output Behavior
The behavior a device exhibits when it is activated.

Output Behavior, Follow
When the device is activated, the outputs are activated until the state that is being followed terminates and the delay period elapses. This behavior is only valid for devices that have state, such as switches, timers, or event trackers when Door Ajar is the selected event. Example: If you have an Event Track device set to watch Door Ajar

messages, you can set the output to *follow* the input, and it will engage its output when the door is left ajar. Likewise, when the Door Ajar condition is cleared, the Event Track device will disengage its output.

Output Behavior, Latch
When the device is activated, it causes the device's outputs to latch. Example: A buzzer is activated when a switch is turned on to call a service person.

Output Behavior, Pulse
When the device is activated, its outputs are activated for the amount of time defined in the second(s) delay field. Example: If a Valid Credential device controls access to a Copy Machine, the machine is only accessible, once a credential is verified, for the amount of time specified in the seconds(s) delay field.

Output Behavior, Toggle
When the device is activated, it causes the device's output to change to the opposite state. Example: A switch linked to the burglar alarm is toggled to deactivate during office hours, but after hours, the switch toggles back to being activated.

Output Behavior, Unlatch
When the device is activated, it causes the device's outputs to unlatch. Example: A buzzer is silenced when the switch is turned off by a service person.

Request-to-Exit (REX) Switch
A button or motion sensor that causes a Door latch to disengage, allowing a person to exit.

Relations
Relations are the data that you want to report on, and related data. For example, users have groups, which have permissions and thus are tied to devices. When building a report listing all users and the groups those users are in, you can start with the Users relation then select Groups. This makes various properties of Users as well as Groups available for both report criteria and outputs.

Rule
A set of conditions for routing email notifications.

Schedule
A *schedule* is an editable, reusable time template that can be used to control such things as when a door is accessible or when a device is activated. A Schedule has a descriptive name such as "Mon-Fri 7AM-7PM."

Schedule Exception
A *schedule exception* is an exception to a schedule, either once or on a repeating timetable, that determines if the exception will cause the schedule to be active during a normally closed portion of the schedule or to be inactive during a normally open portion of the schedule.

Supervisor-on-Site
A security feature that lets you define a schedule so that it does not become active unless or until a member of a specific group accesses the door to which that schedule is linked.

Swipe & Show
A tab on the Dashboard that allows an administrator to view the last eight valid credential reads at a selected device.

System Activity Log
A record of Access Events, Exception Events, Device Events and Control Panel Events.

Threat Level
Different operational modes that can allow or restrict access to certain portions of a facility, including doors, elevators, floors, or devices.

Two Factor Credential
A security feature that requires users to provide both forms of credentials, a card and a PIN, at a door, elevator, or valid credential device.

User
A person who requires access to one or more doors. A user has unique credentials, such as a Card or PIN, and belongs to one or more group

User Alias
A method to place a user in multiple sub-accounts. A user alias may only be created by an administrator who can see both the primary account and the account where the alias is being created. The user name, user photo, credentials, and dates work across permissions granted in multiple sub-accounts.

User Status – Enabled
A user who is currently active. This information appears on the View Users page.

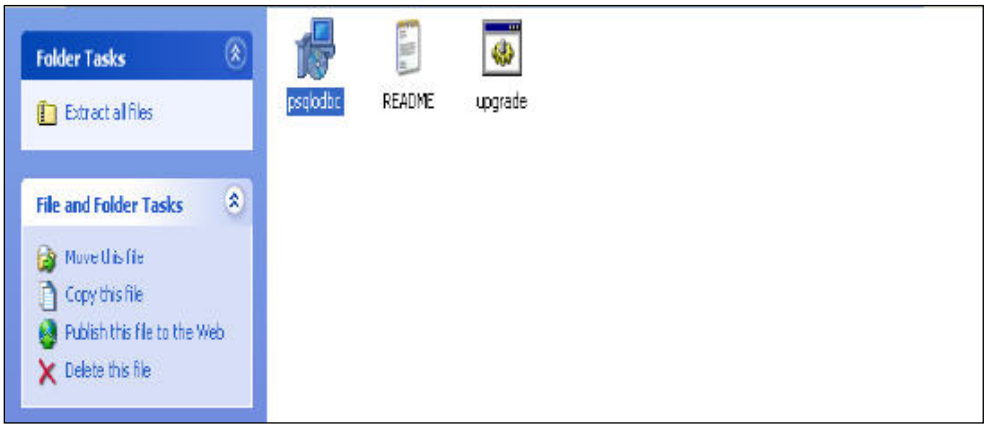
User Status – Expired
A user whose expiration date in their User Profile has passed. This information appears on the View Users page.

User Status - Suspended
A user who has been suspended. The user's credential(s) will not function at any device until the user is reinstated. This information appears on the View Users page.

Appendix 2: Use of Report Service

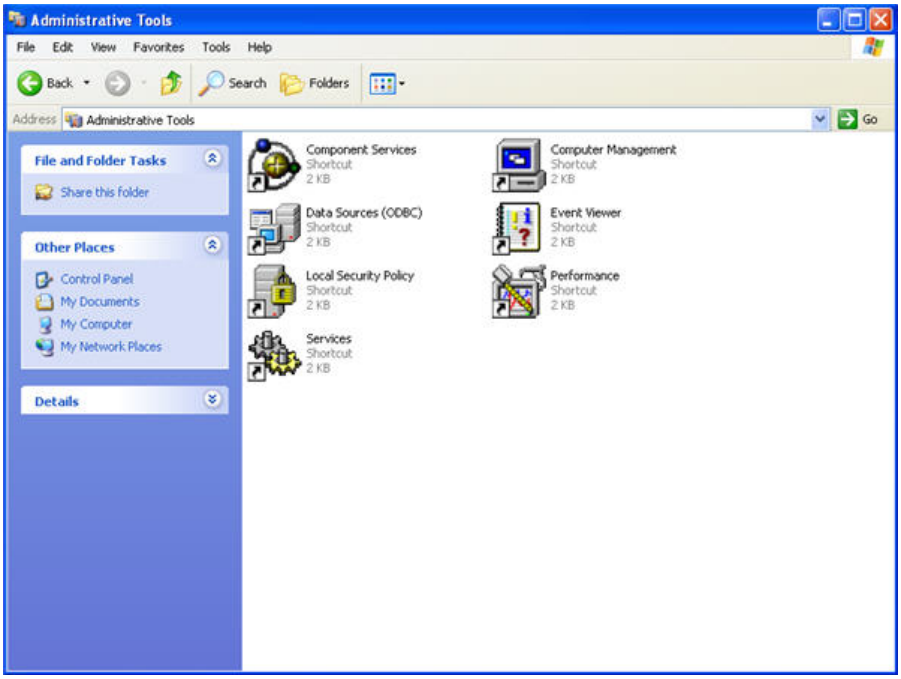
Below is a list of instructions for the use of the Brivo Onsite Server Report Service in Microsoft Windows.

1. Download driver from the following website: http://www.postgresql.org/ftp/odbc/versions/msi/
2. Install the driver by double clicking on psqlodbc.msi

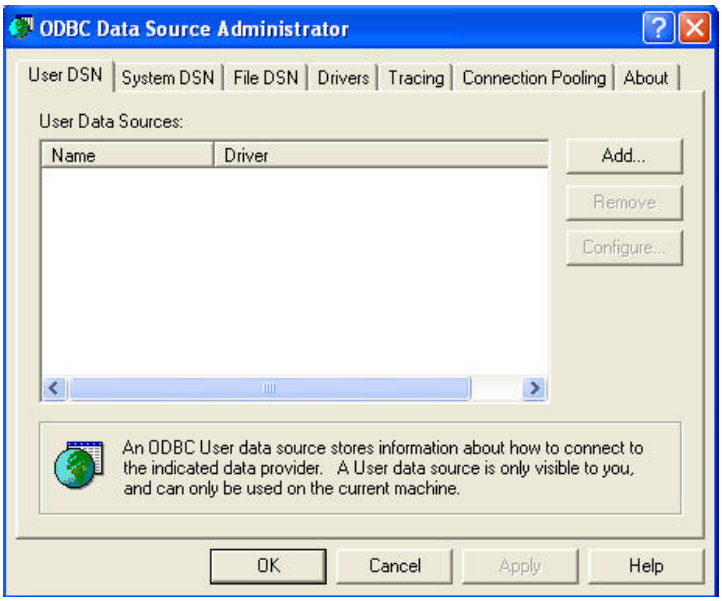


3. Configure system data source (ODBC)

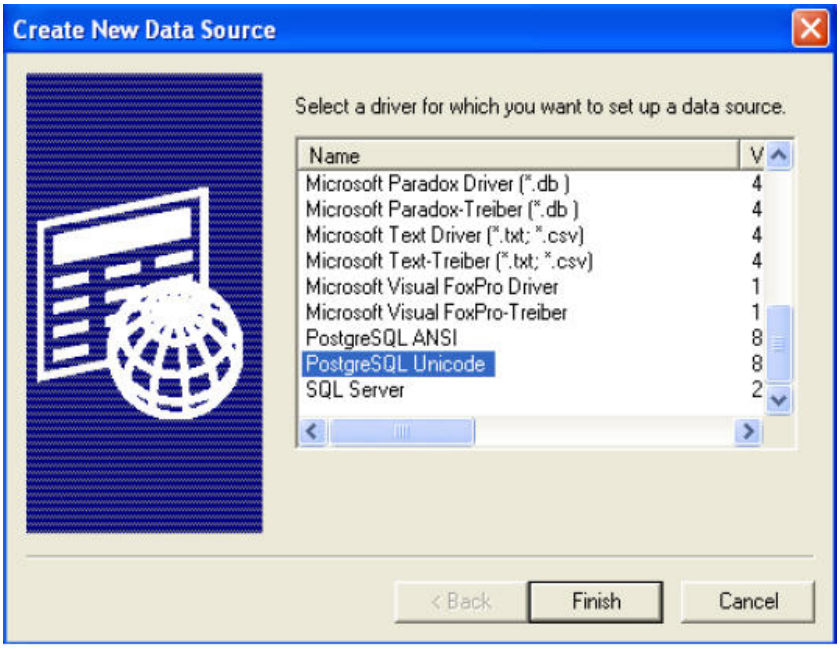
p) Control Panel -> Administrative tools -> Data Sources (ODBC)



q) Click on User DSN tab and then click Add.



r) Select PostgreSQL Unicode and click OK.



s) A popup setup window will appear. There are four essential parameters that must be configured. Fill in the fields as instructed below.

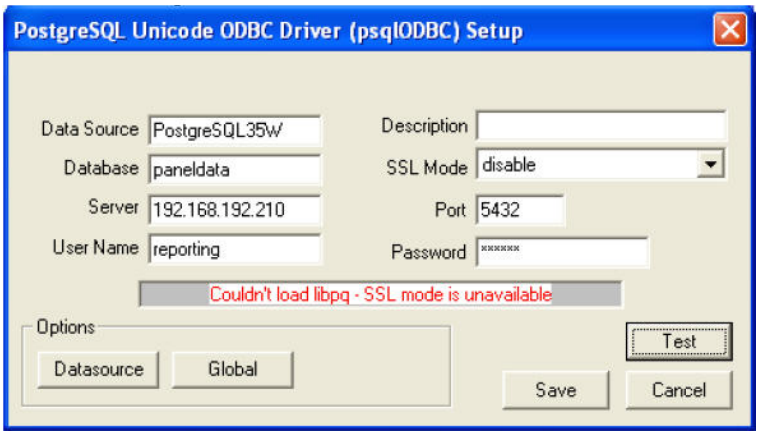
   a) Database: paneldata

   b) Server: This is the IP address or host name for your Brivo Onsite Server

   c) User Name: reporting

   d) Password: This password must match the password defined in the Brivo Onsite Server Report Service section.

t) When all four fields are entered properly, click Test to make certain it can connect to the Brivo Onsite Server.



u) If the above steps show Connection Successful, click on Save to save the settings.

4. Your internal setup is complete. At this point, please consult your product specific documentation for how to interface with an ODBC data source.

Appendix 3: Salto Equipment

Salto Maintenance Schedule

Batteries:

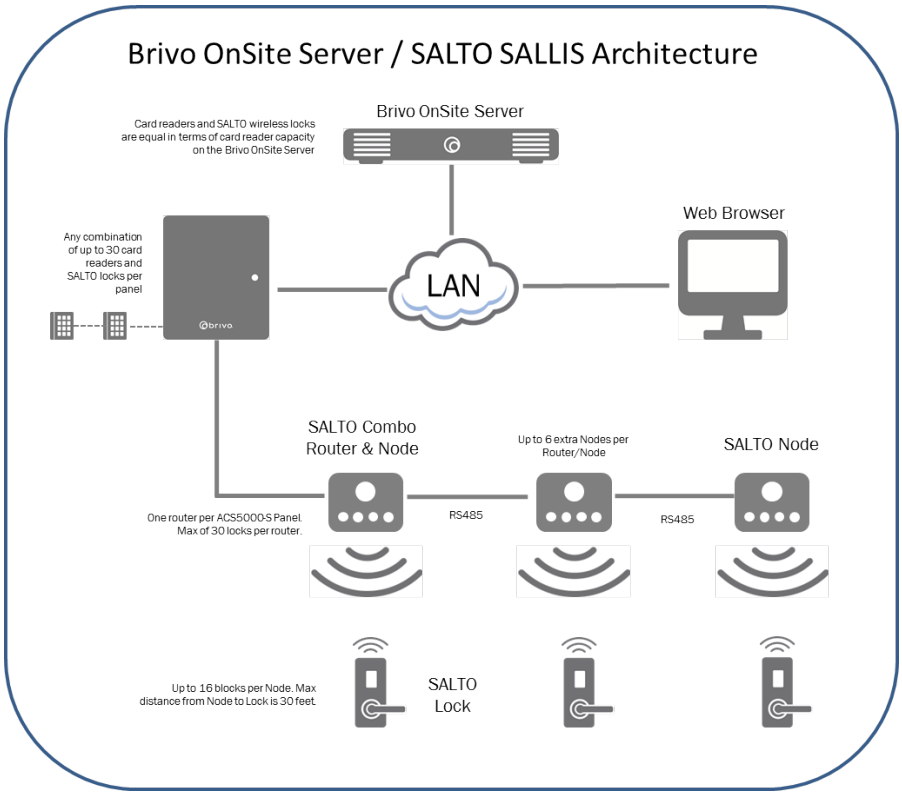
1. Battery life benchmarked to 65,000 Operations or 2.5- 3.0 years.
2. Shall be powered by standard off the shelf batteries (AAA).
3. Proprietary batteries or proprietary battery packs are not acceptable.

Salto Installation and Configuration

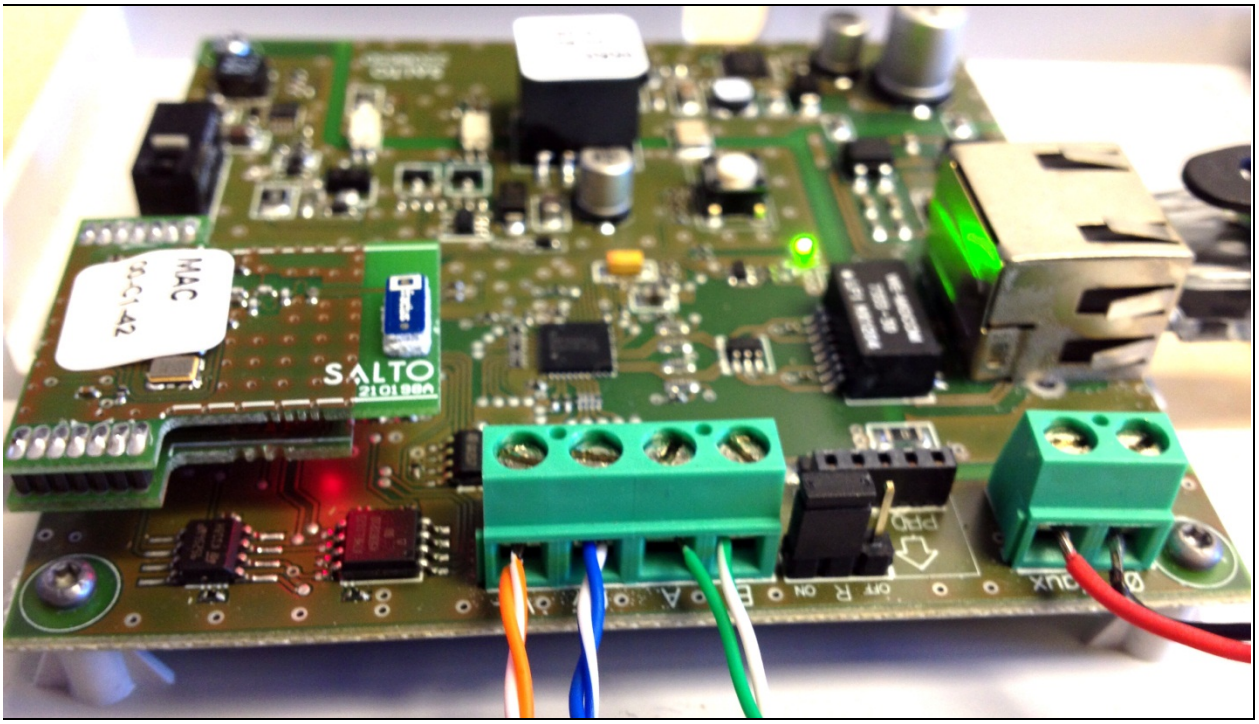
OVERVIEW

SALTO wireless locks can only communicate to a Brivo ACS access control system through the Brivo Sallis Router using Sallis technology. The router must first be associated to a maximum of 30 locks that will communicate to up to 7 nodes. Finally, the router is connected directly into the Admin Port of a Brivo ACS6000 control panel or Brivo ACS300 controller or the AEN Ethernet port of a Brivo control panel. This is a private network.

The diagram below illustrates an architectural structure view and the wire connections of the Brivo Sallis router. The figure below illustrates a combination of two hardwired readers and six wireless lock sets in a Brivo Onsite Server system. A total combination of 30 hardwired and/or wireless doors can be connected under a single Brivo ACS6000-A, Brivo ACS300-A, Brivo ACS5000-A or Brivo ACS5000-S control panel system.



Below the Brivo Sallis router wire connections are shown. The power adapter will be supplied when purchasing a router from an authorized Brivo dealer. The RS485 connection from router to node is to be wired using CAT5e twisted pair wire.



Be sure to have the following required hardware and firmware components supplied:

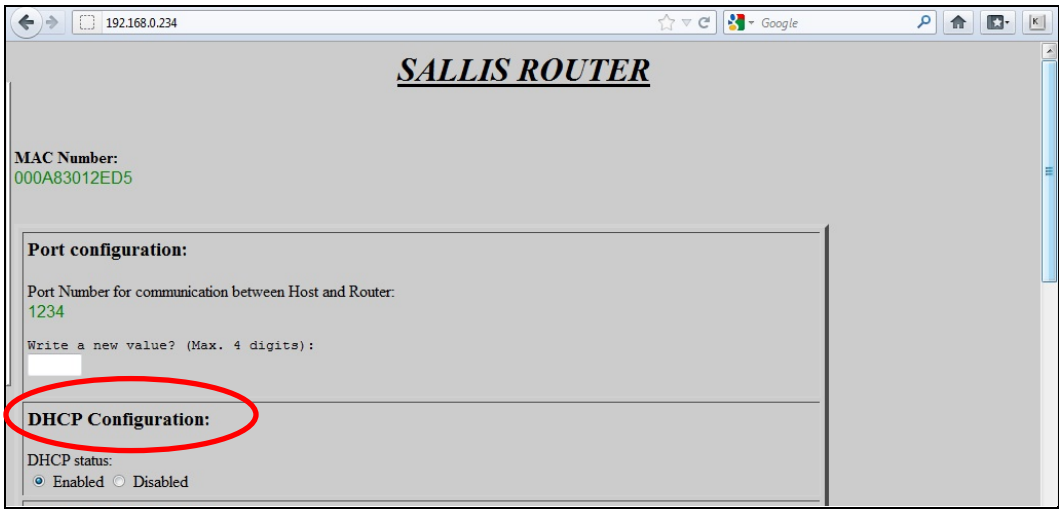
A. Brivo Sallis Ethernet Router (with or without built-in node). *Note: The Sallis RS485 Router is not compatible with Brivo IPDC controllers.*
B. Brivo Onsite Server Firmware 3.0.6 or higher
C. Sallis Router Configuration Software 3.1.06 or higher
D. Salto PPD programmer with firmware 1.23 or later

After going through the general step for updating the firmware on the Brivo Onsite Server to 3.0.6 and upgrading the associated panels, the Salto equipment can now be configured and connected.

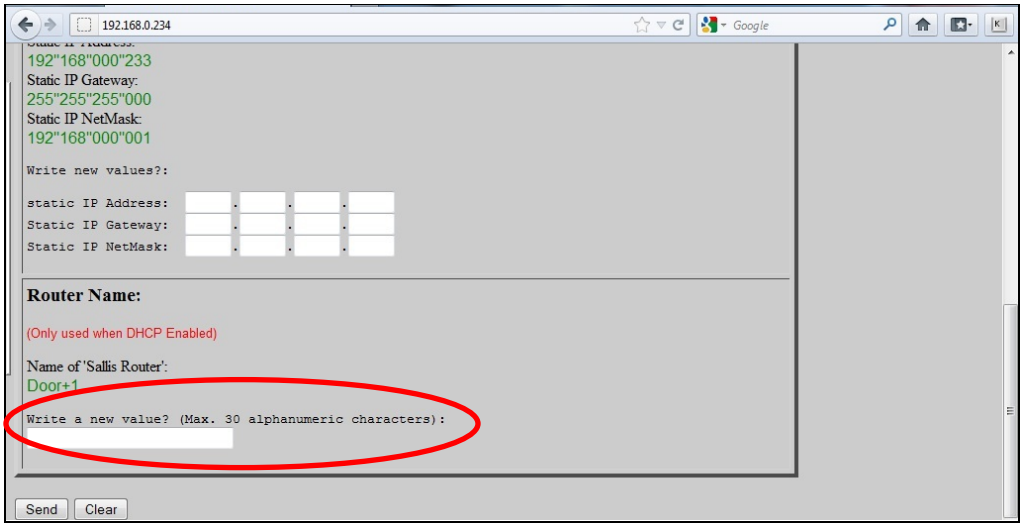
ROUTER CONFIGURATION

A. OVERVIEW
   All Brivo Sallis routers come from factory with DHCP enabled. When connecting an Ethernet cable between the Brivo Sallis Router and the Admin port for Brivo ACS6000 and Brivo ACS300 and the AEN port for Brivo control panel, the router will obtain an IP address from the Brivo control panel and connect automatically.
B. Follow the steps below to log into the router and confirm DHCP.
   a. Plug a laptop or PC directly into the Sallis router Ethernet port
   b. Confirm that the laptop or pc being used has its static IP configurations correct and open a standard internet browser

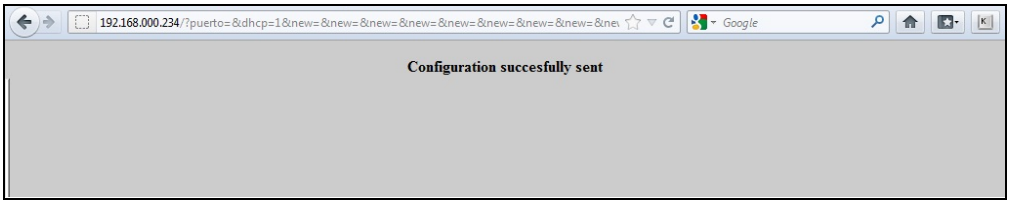
c. On the router find the CLR button and press down for 5 seconds, the LED should then turn orange. The router is now in "fabrication mode."
d. In the address bar type 192.168.0.234 to get to the Sallis router configuration screen (no login required)
e. The router configuration screen will confirm that DHCP is enabled (if it is not enable it by clicking on 'enabled'); also take note of the 'MAC Number' and 'Port Number' – they will be needed later.



f. Assign the router a specific name if necessary and click 'save'

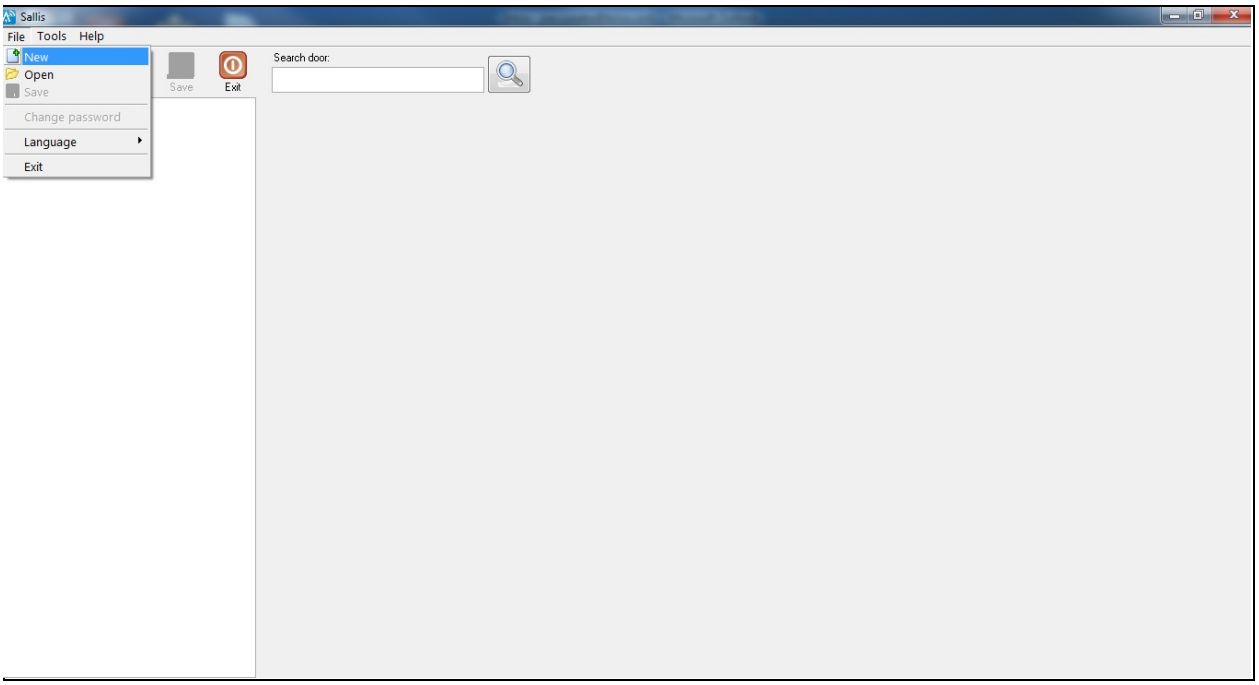


g. It will show that the configurations have successfully been saved

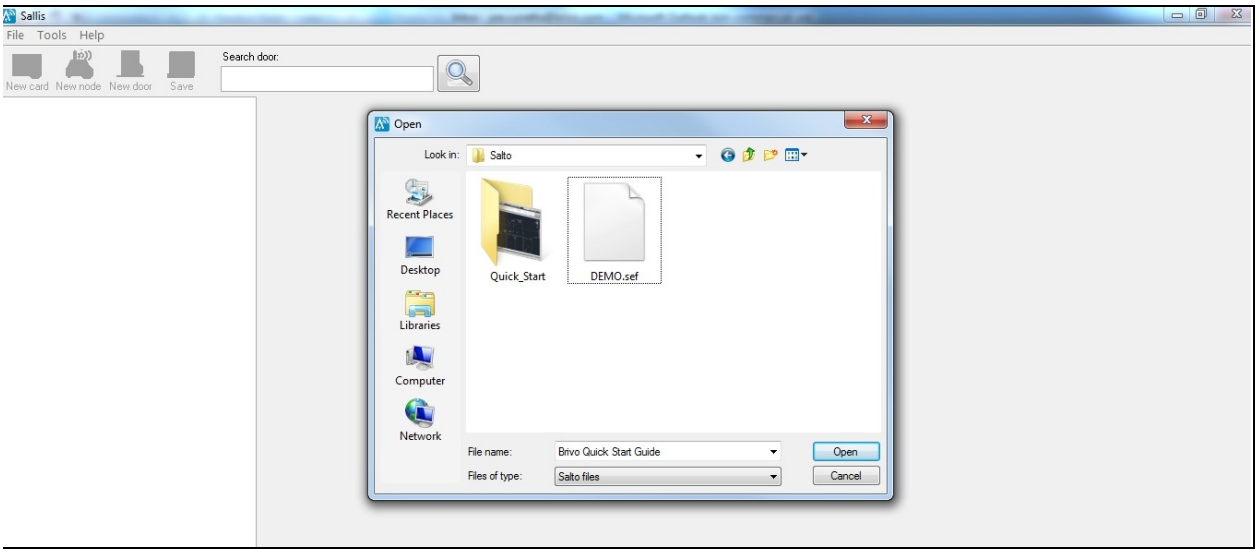


h. Now that the router has been configured, unplug the Ethernet cable from the laptop or PC and plug it into the Admin port on the Brivo ACS6000 and Brivo ACS300 or the AEN port of the Brivo control panel.
   1) The LED on the Brivo Sallis router will begin to blink red signaling that connection has been lost. Once the Brivo panel has begun its communication with the router the LED will turn green signaling communication has been restored.

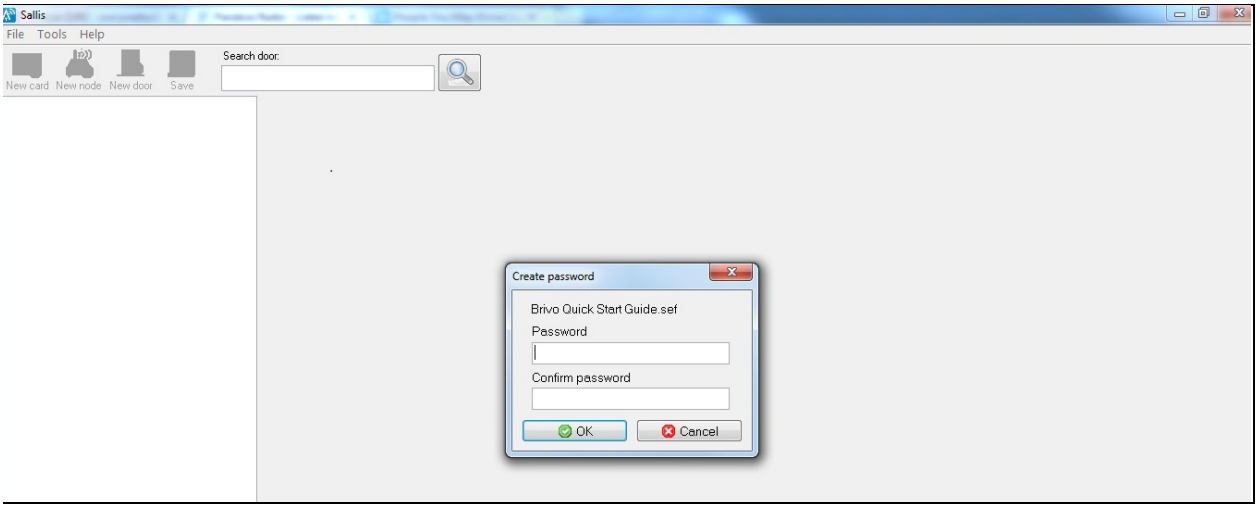
C. A router configuration file must now be configured in the Sallis Software. This data file being created will be uploaded to the router and lock in future steps.
   a. Install and open the Sallis software.
   b. After the installation is complete, open the Sallis software and click File ->New.



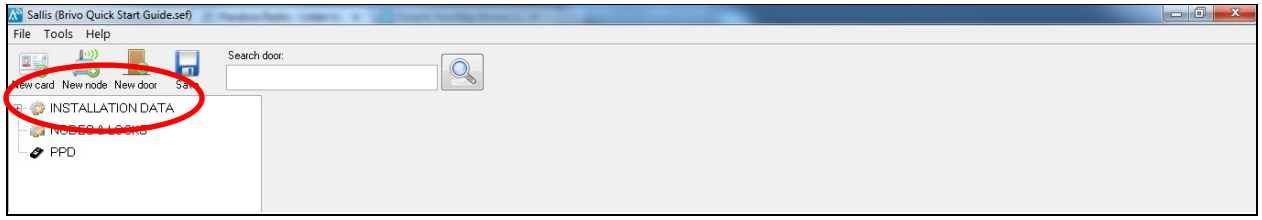
c. In the pop-up window, find the location in which the file will reside, type in the desired file name and click 'Open.'



d. A password can be set for file security if desired. If no password is desired leave the password fields blank and click 'OK.'



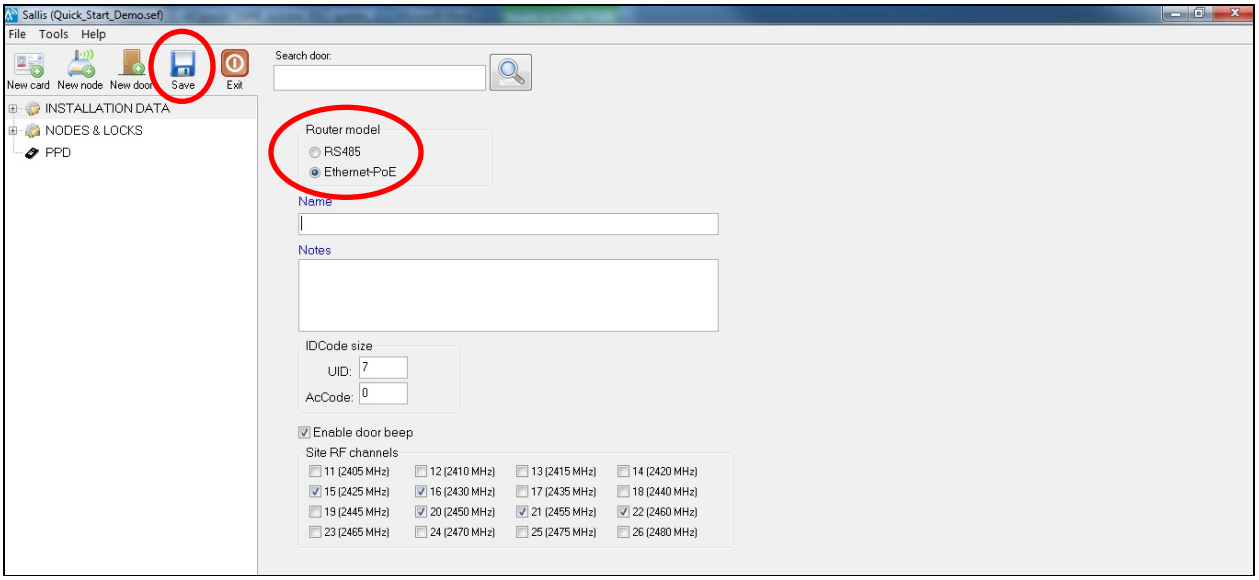
e. On the side tab click installation & data.



f. Select "Ethernet-PoE" under router model, which has been supplied to you by Brivo.

g. Click 

(found in the toolbar next to 'new door').



CARD TYPE CONFIGURATION

A. Do not use Salto's card type configuration. Please refer to the *Adding Cards* section of the Brivo Onsite Server manual for the proper method of adding cards.

NODE CONFIGURATION

A. Press the 

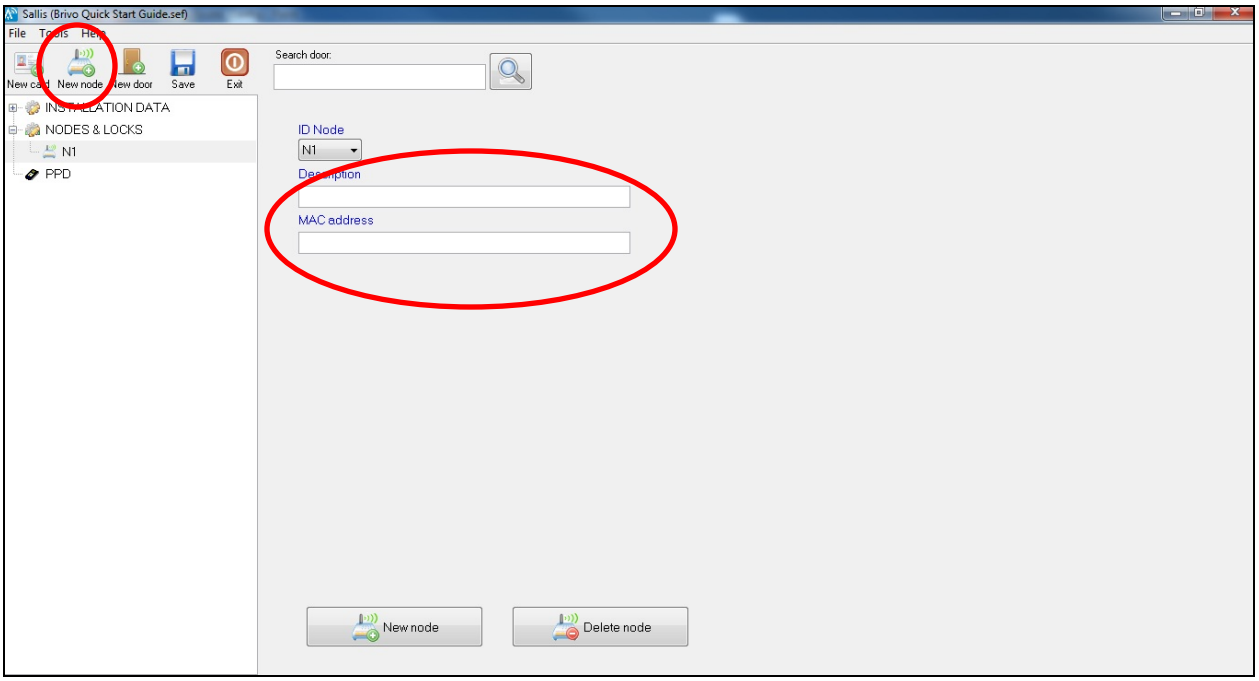
button in the toolbar to add a node to the router file. A new icon will be created under the 'NODES & LOCKS' icon.

B. Set the correct Node ID.
   a. For example if only 1 node will be installed, leave this setting at 'N1.'
   b. If 5 nodes will be installed, set each node, 'N1' to 'N5' accordingly.

C. Find the MAC of each node (on the backside of the node on the sticker labeled "MAC") and input the data for each node accordingly.

D. If adding more nodes click 'New Node' at the bottom of the screen, or else click the 

button.



DOOR CONFIGURATION

A. Press the 

button in the toolbar to add a door to the router file. A new icon will be created under the 'NODES & LOCKS' icon.

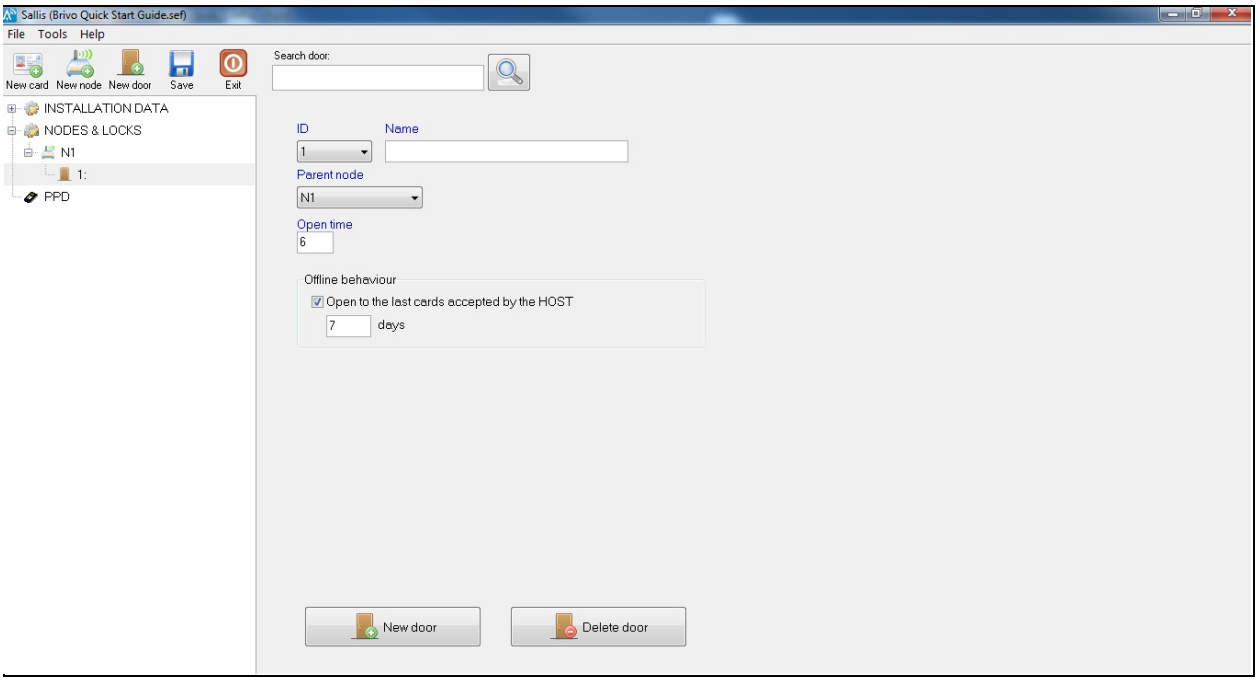
B. Set the desired ID for the lock being configured and pick the node it will be associated with under "Parent Node."

C. Set the desired "open time" (the length in time in seconds that the lock is unlocked after a valid unlocking event).

D. Leave "Offline Behaviour" as it is set from factory. This feature will have no effect on this setup.

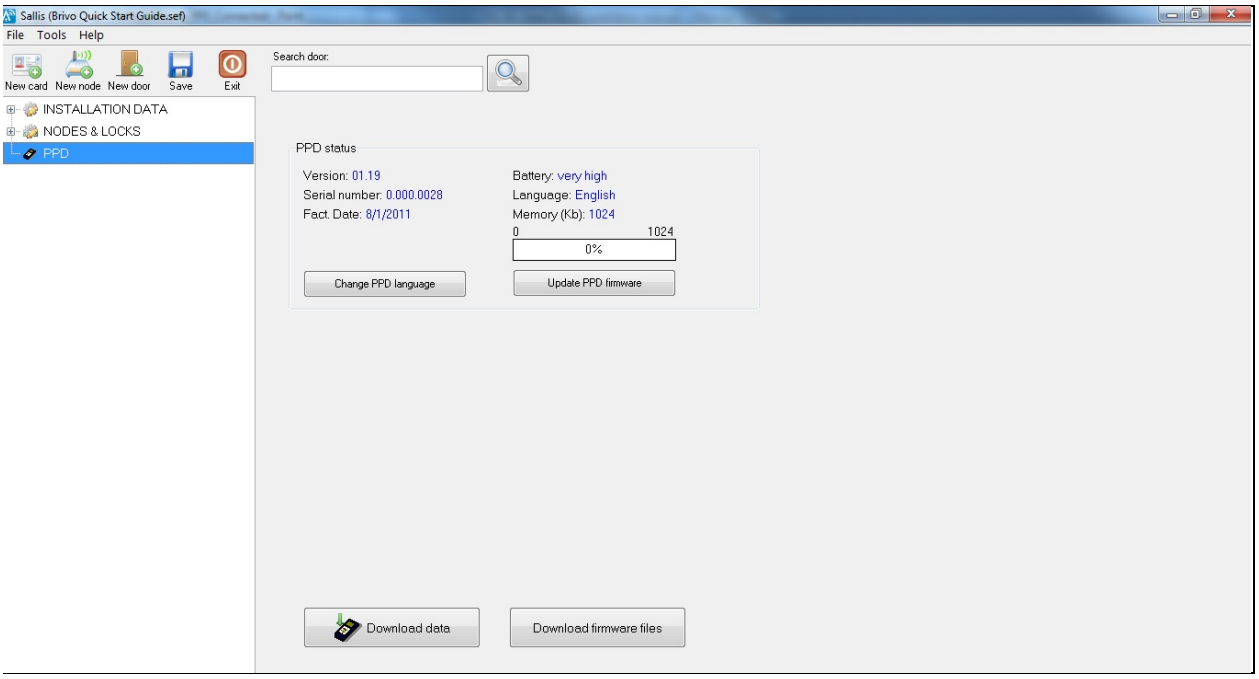
E. If adding more doors click 'New Door' at the bottom of the screen or else click the 

button.

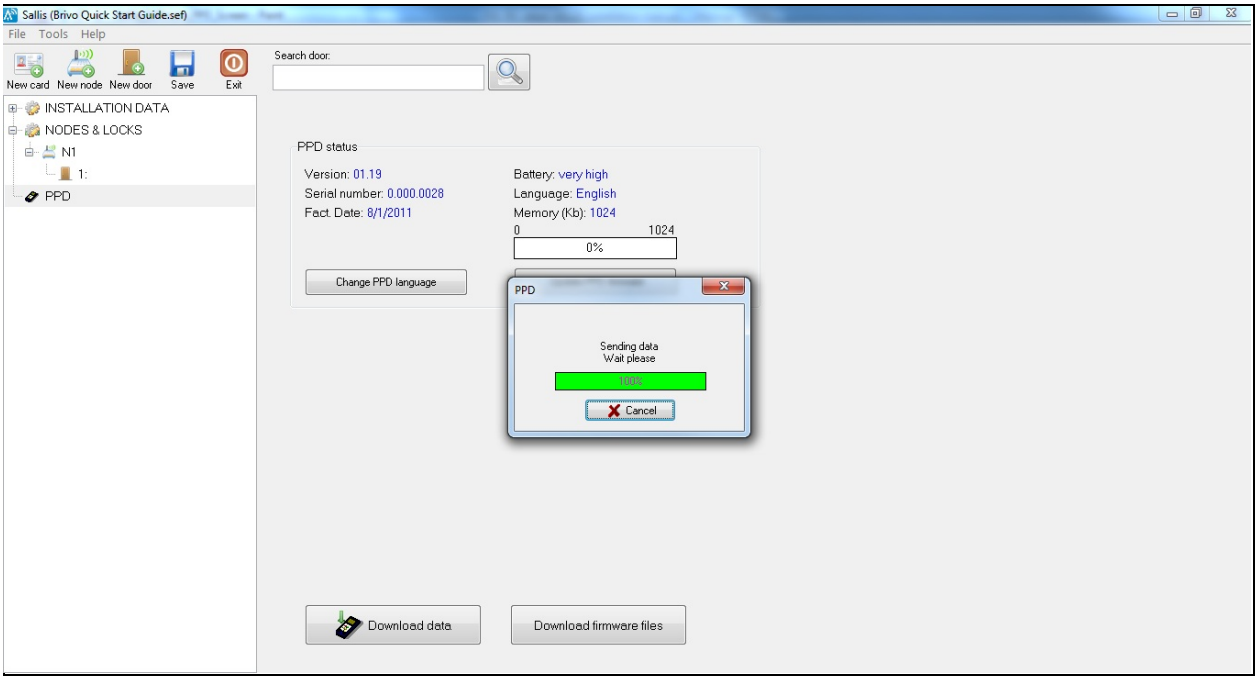


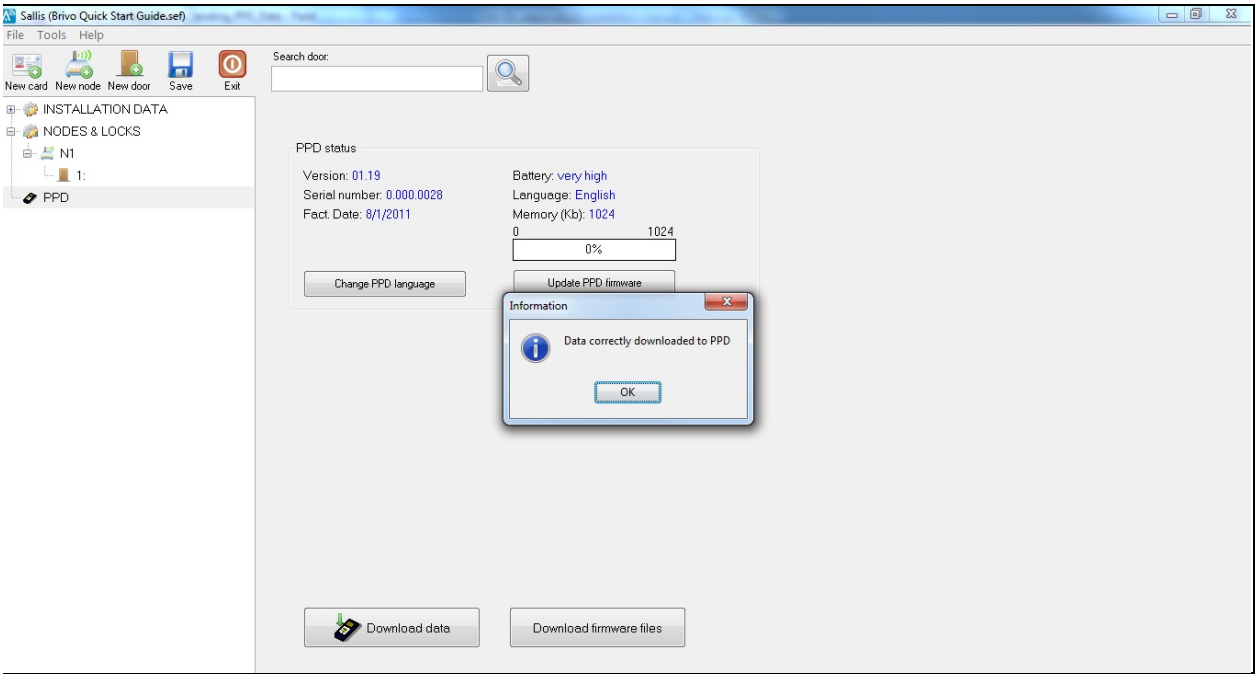
PPD DATA DOWNLOAD

A. Now that the Salto configuration is complete, the data must be downloaded to the PPD.
   a. Connect the PPD to the computer via USB
   b. Click 'Download Data' at the bottom of the screen



c. The pop-up task bar will show the data being transferred successfully

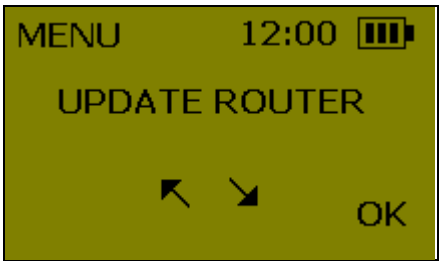




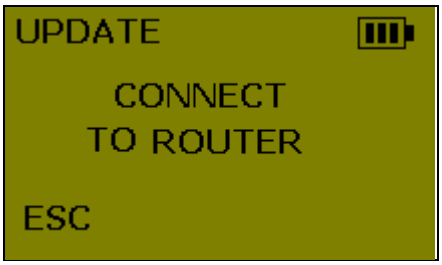
DATA UPLOAD/UPDATE ROUTER AND NODE DEVICES

ROUTER UPDATE

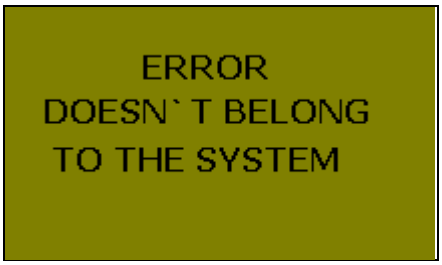
A. Turn on the PPD and select the 'Update Router' option.



B. When prompted, connect the PPD to the router and press 'OK.'



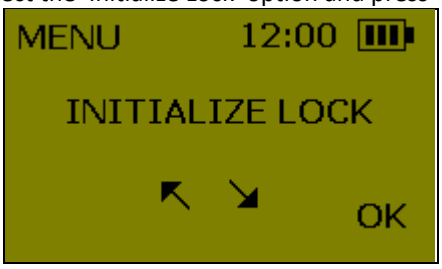
C. If the error message pops up: "ERROR DOESN'T BELONG TO THE SYSTEM," proceed again with step B keeping the 'CLR' pressed on the router.



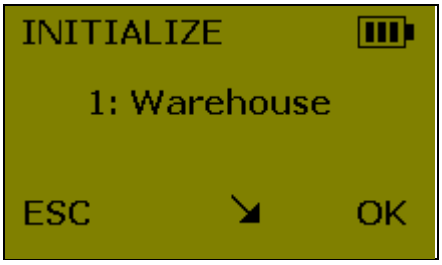
D. The configuration file has successfully been updated to the router when the PPD shows "UPDATED."

NODE UPDATE

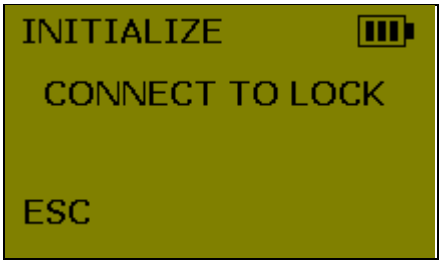
A. Turn on the PPD and select the 'Initialize Lock' option and press 'OK.'



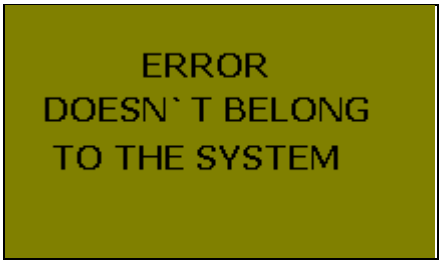
B. The list of configured doors will be displayed. Toggle through to find the correct door and press 'OK.'



C. When prompted connect the PPD into the PPD socket on the lock device.



D. If the error message pops up: "ERROR DOESN'T BELONG TO THE SYSTEM," proceed again with step C keeping the 'CLR' pressed on the back of the lock device (PPD MUST BE CONNECTED WITH CLR PRESSED AND AT THE SAME TIME THE LOCK DISPLAYS AN AMBER LED).



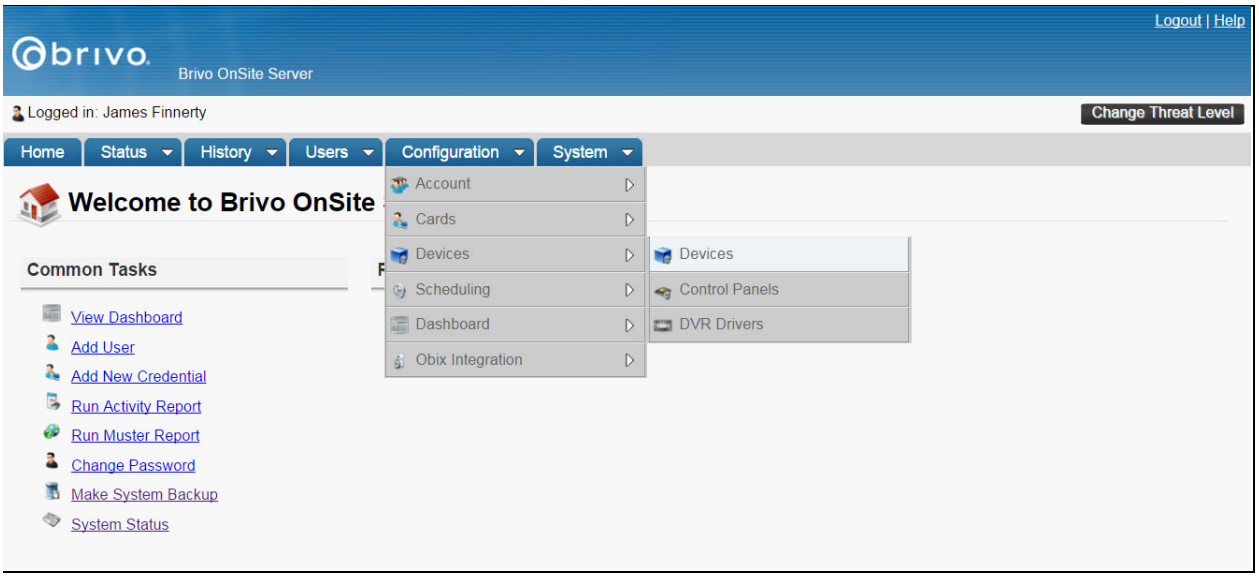
E. The configuration file has successfully been updated to the router when the PPD shows "UPDATED."

F. After the PPD finalizes the initialization process and the lock tries to connect with the assigned node. It will show a corresponding LED with tone.
   a. Green LED flash: the lock is successfully connected to the node.
   b. Red LED flash: the lock indicates a connection error. Re-check that the node is correctly installed and within range of the lock device.

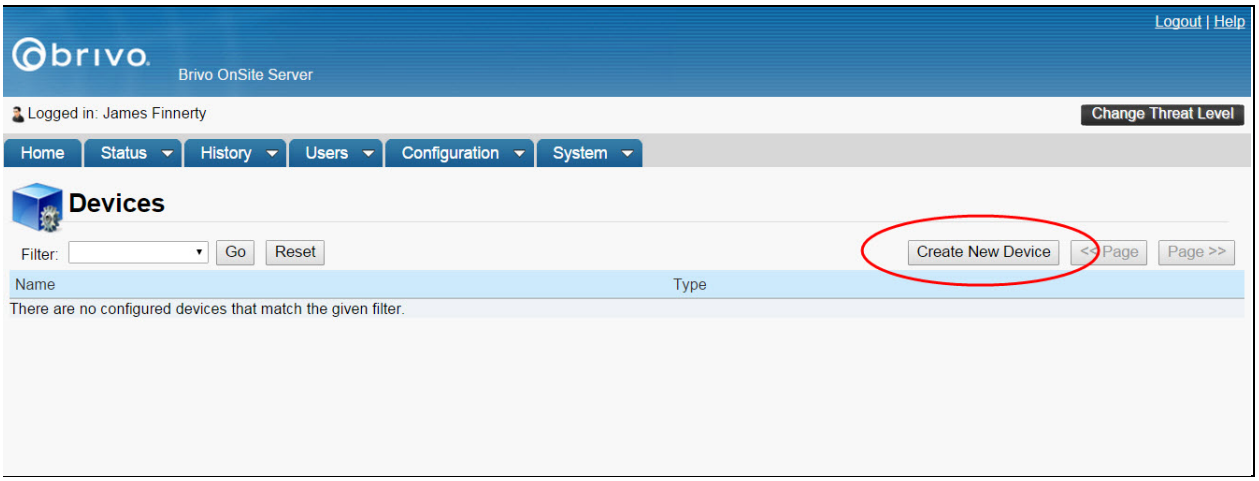
BRIVO SOFTWARE CONFIGURATION

DEVICE CONFIGURATION

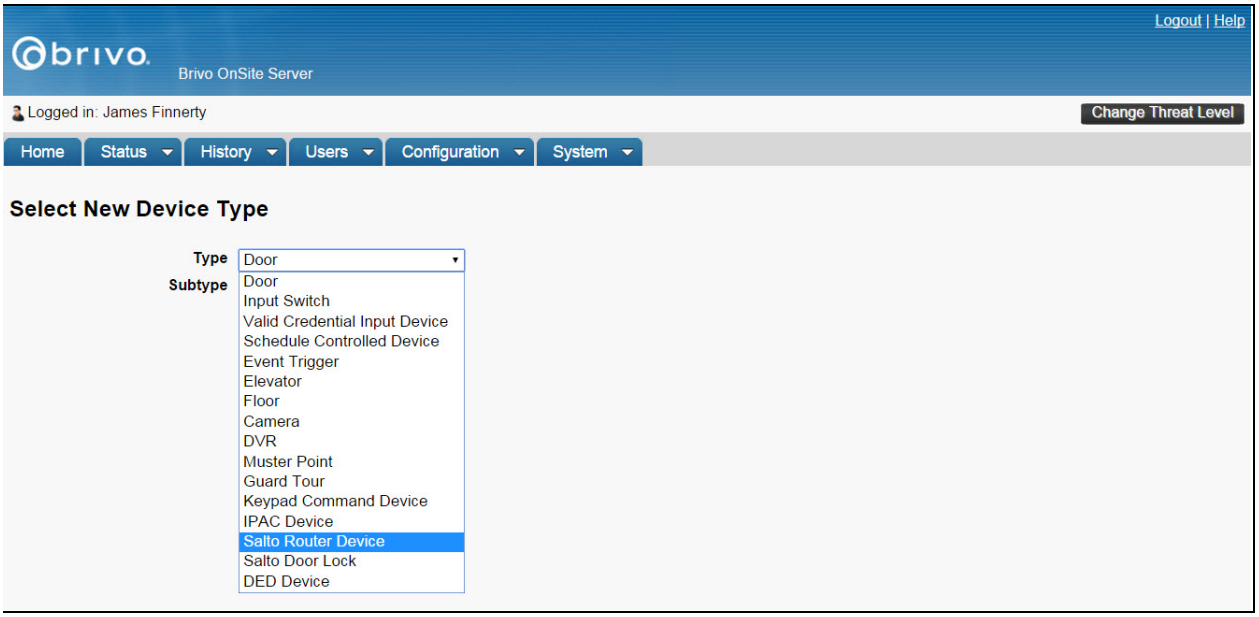
A. Log into the Brivo Onsite Server and go to Configuration->Devices->and select Devices.



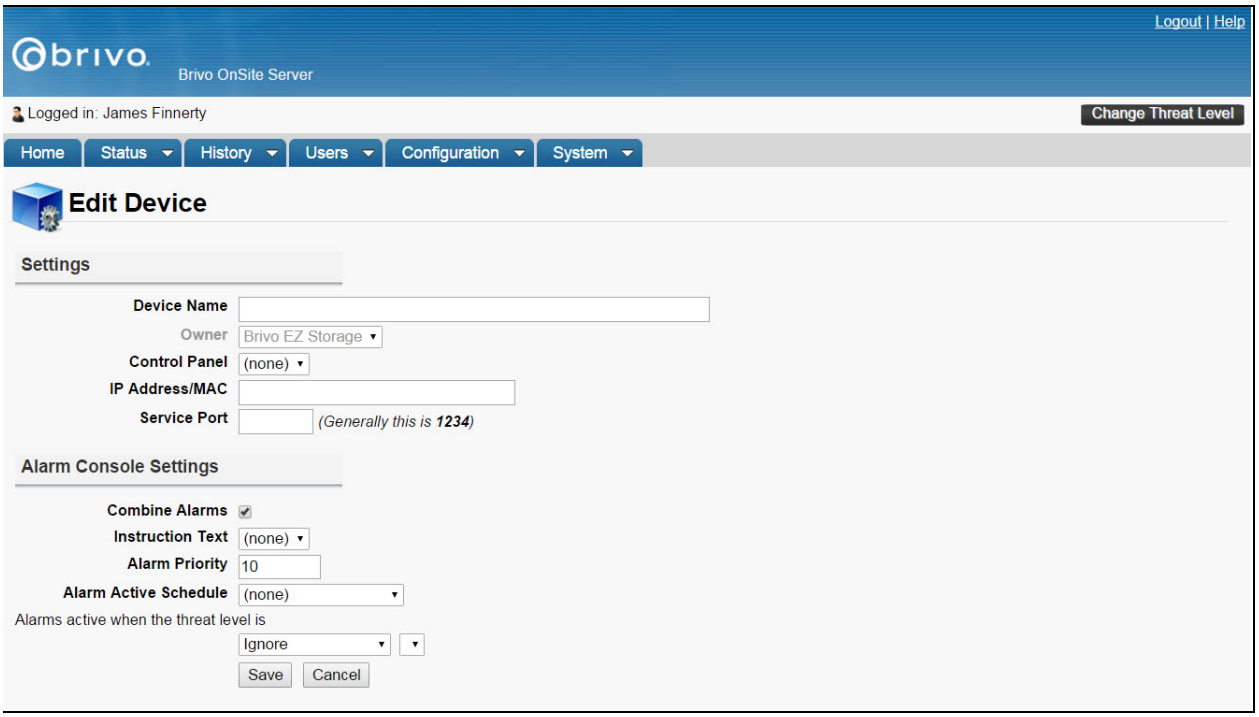
B. In the 'Devices' database page, click 'Create New Device.'



C. In the drop down menu select 'Salto Router Device' and click Next.

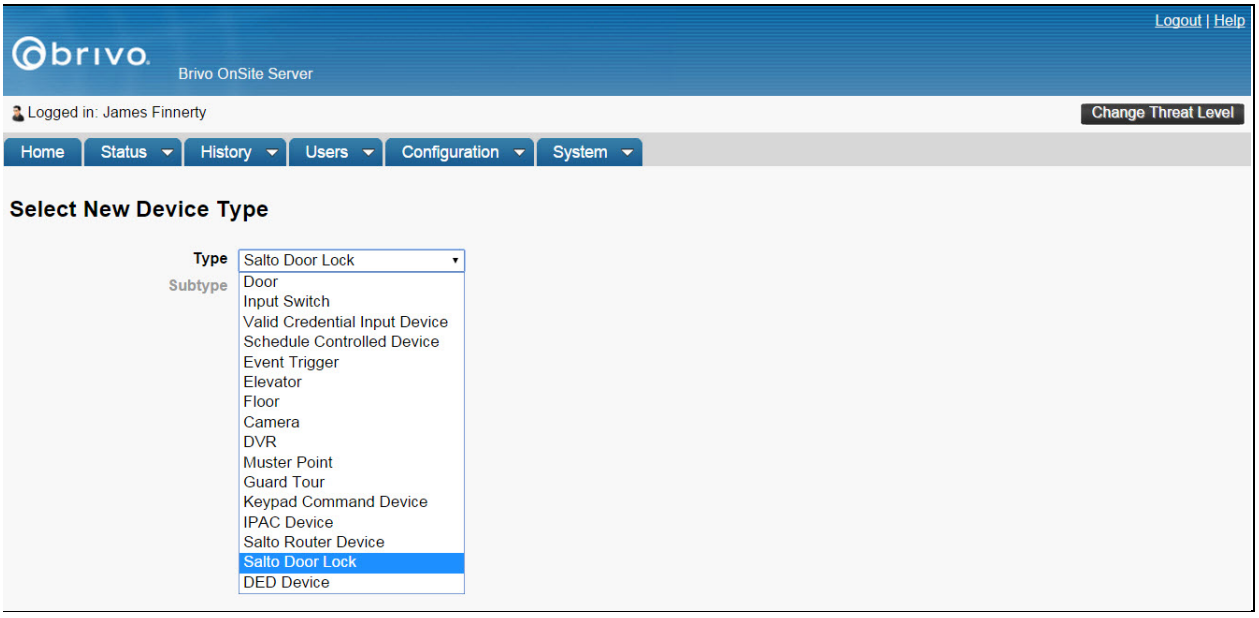


D. Input a desired name for the router along with the MAC and Service Port noted earlier then click Save. (MAC number can also be found on the sticker on the router labeled 'MAC')

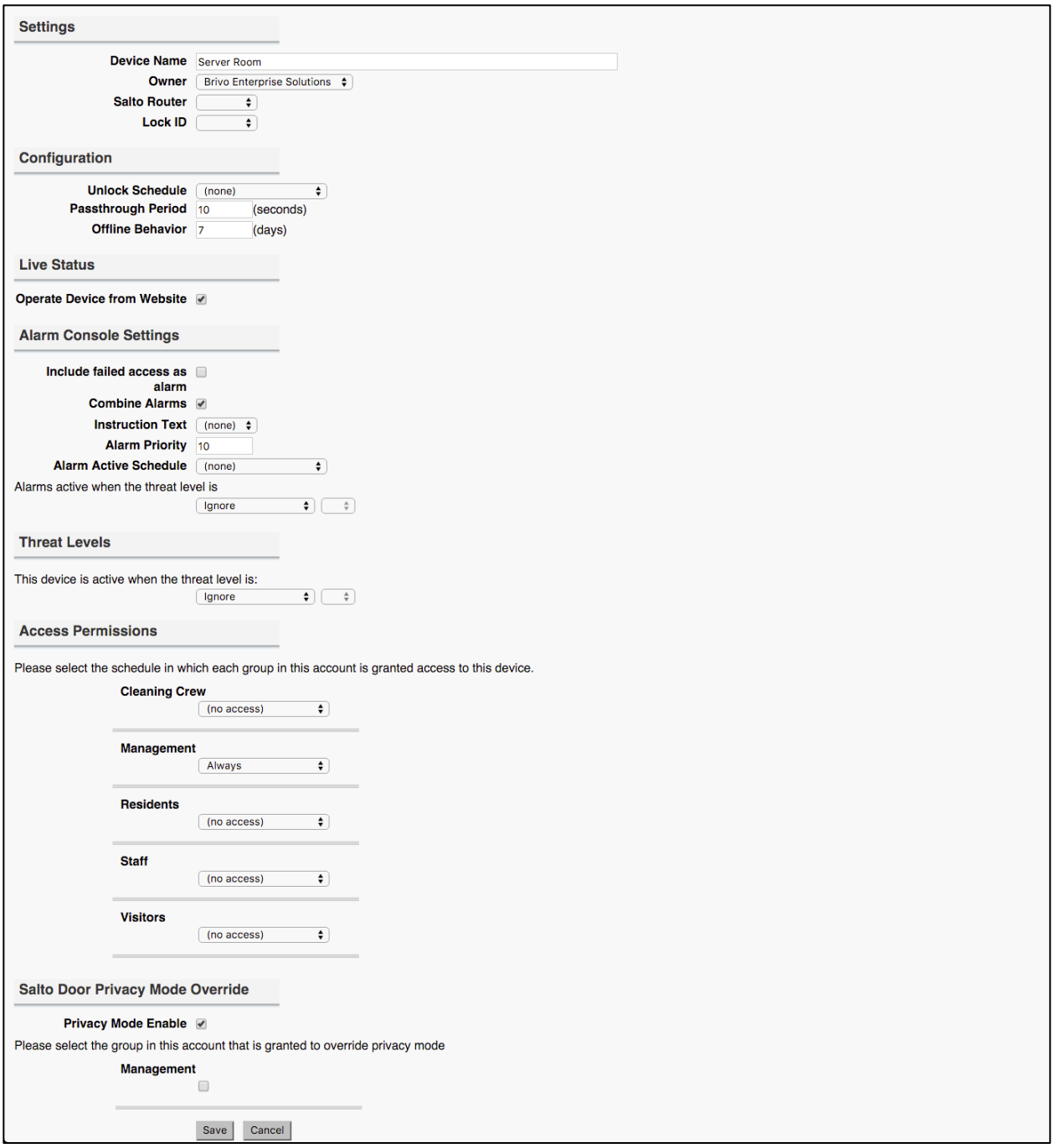


E. After a router has been configured, an associated lock device must be set. To do so, go back to the device database list and select 'Create New Device'

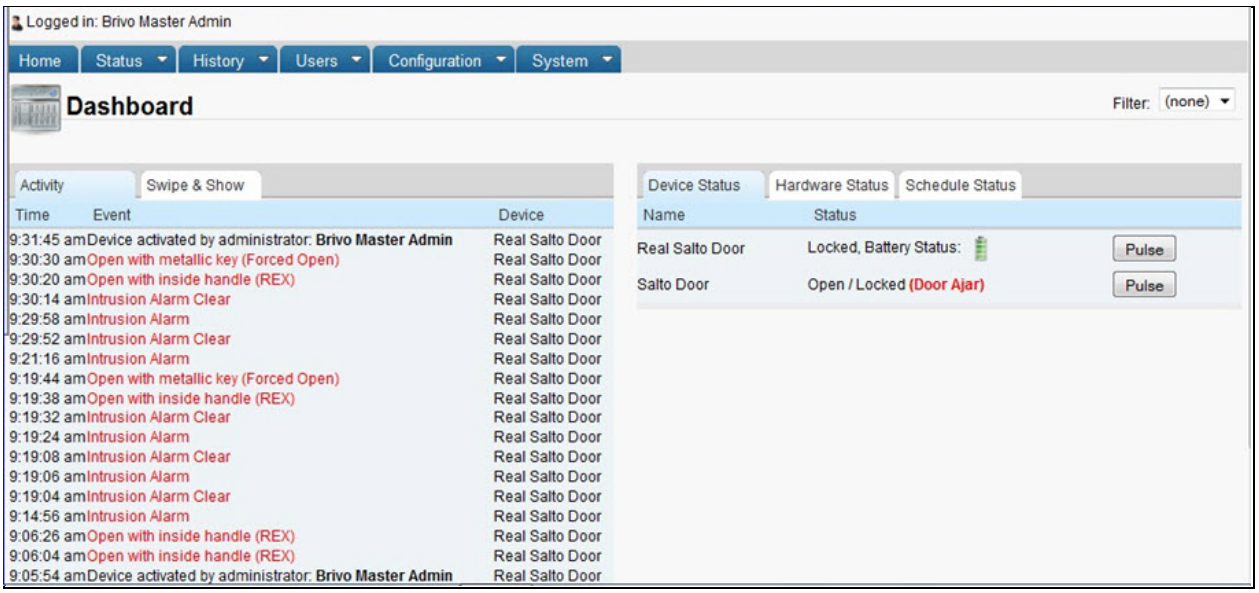
F. In the drop down select 'Salto Door Lock' and click Next.



G. Set the desired parameters and click Save.



The Salto devices are now configured to the Brivo Onsite Server device and can be used or controlled as any other device created in the Brivo Onsite Server setup.



Appendix 4: Obix Integration

Obix Integration is integrated event notification tool, allowing the Obix software to listen directly, rather than through Brivo DataSync API, to a defined set of events. These events are door ajar, door forced open, panel communication failure, and AC power loss.

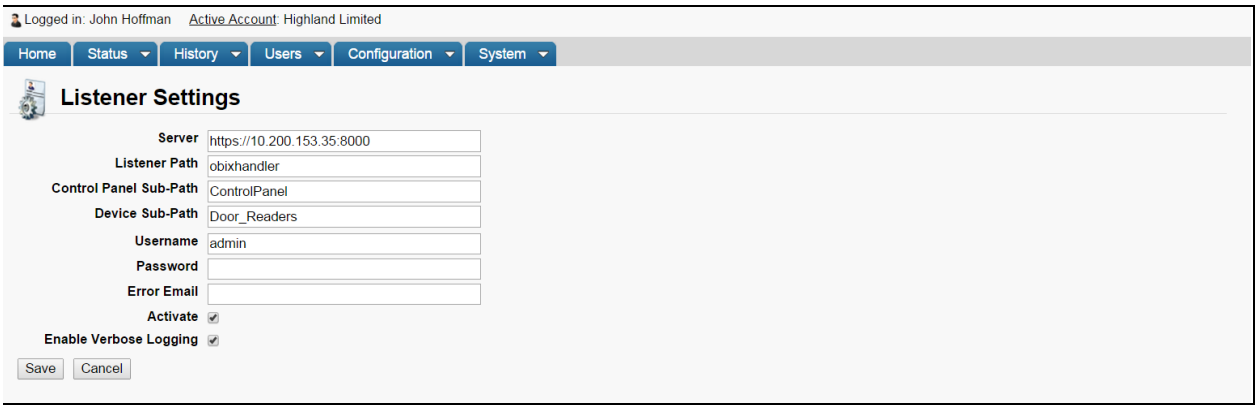
	*NOTE:* *Obix Integration requires a license key. Without the license key, Obix Integration functionality will be disabled.*

The Obix Integration setup is divided into three sections: Listener Settings, Control Panel Mapping, and Device Mapping.

Administrators with appropriate permissions can add, edit, or delete Listener Settings, Control Panel Mappings, and Device Mappings associated with their own accounts.

To create Listener Settings:

1. Scroll over the Configuration section. The sub-navigation menu displays.
2. From the Obix Integration link, click the Listener Settings link. The Listener Settings page displays.
3. Enter the Server name in the field provided (IP address of destination Obix server)
4. Enter the Listener Path in the field provided (optional). Defining this field allows you to push events directly a more defined URL destination. For example, in the screenshot below, the URL would appear as http://10.200.153.35:8000/obixhandler.
5. Enter the Control Panel Sub-Path in the field provided (optional). As above, defining this field allows you to push events to a more defined URL destination. To continue on the example above, a control panel event (i.e., panel communication failure) would appear as http://10.200.153.35:8000/obixhandler/ControlPanel/(Control Panel Mapping Name)
6. Enter the Device Sub-Path in the field provided (optional).). As above, defining this field allows you to push events to a more defined URL destination. To continue on the example above, a device event (i.e., door ajar or door forced open) would appear as http://10.200.153.35:8000/obixhandler/Door_Readers/(Device Mapping Name)
7. Enter the Username and Password in the fields provided.
8. Enter the email address to send any errors that occur to the provided email address in the Error Email field.
9. To activate Listener Settings, check the Activate checkbox.
10. To Enable Verbose Logging, check the Enable Verbose Logging checkbox.
11. Click Save.



Details displayed include:

- This page lists the Listener Settings currently defined for the account and whether or not the Listener Settings have been activated.

Administrators with appropriate permissions can:

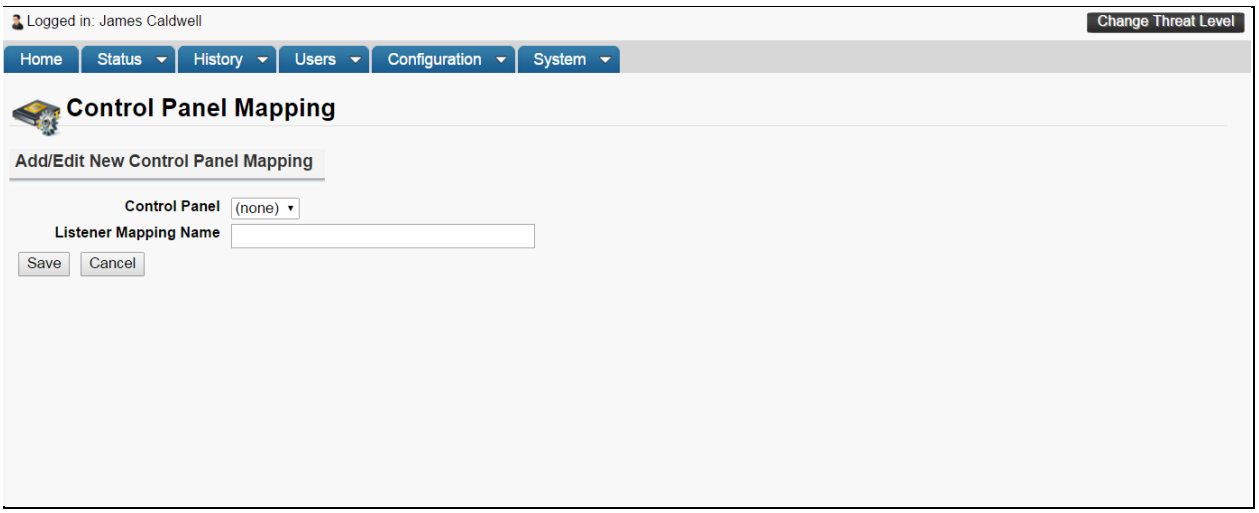
Click Save to save the Listener Settings page.

To create Control Panel Mapping:

1. Scroll over the Configuration section. The sub-navigation menu displays.
2. From the Obix Integration link, click the Control Panel Mapping link. The Control Panel Mapping list page displays.
3. Click on the Add New Control Panel Mapping button in the upper right hand corner.
4. Select the Control Panel from the dropdown menu.
5. Enter the Listener Mapping Name in field provided.

	NOTE: *The Listener Mapping Name selected must match the Obix name exactly or the notification push will not perform correctly.*

6. Click Save.



Details displayed include:

- This page lists all of the control panels and their corresponding listener mapping names for the account.

Administrators with appropriate permissions can:

Click on a Control Panel to access the corresponding Control Panel Mapping page.

Click Add New Control Panel Mapping to define new listener mapping names.

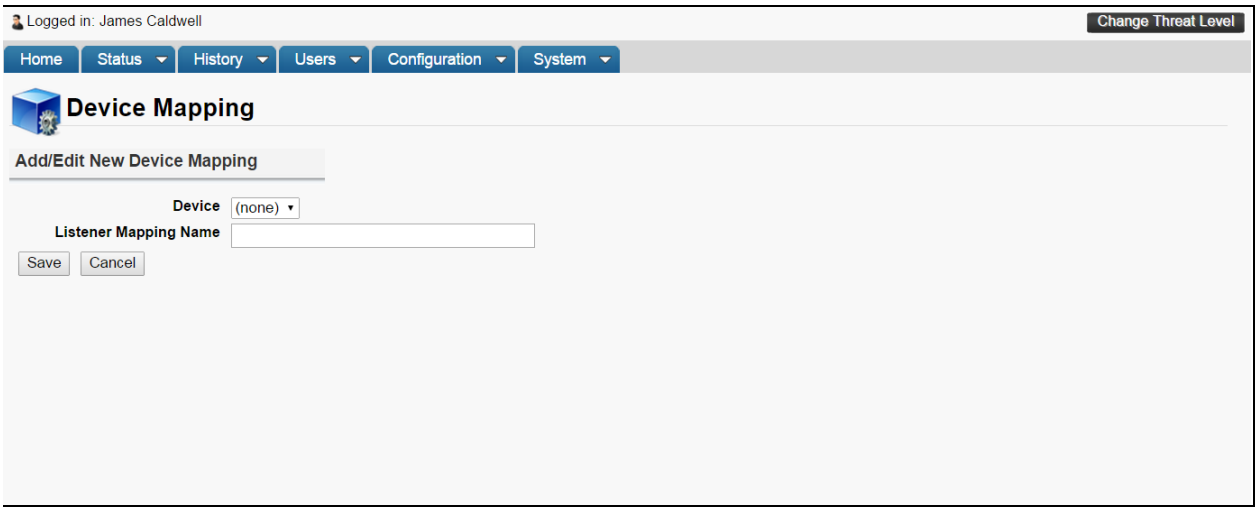
Click Reset to return to the first page of the Control Panel Mappings list.

To create Device Mapping:

1. Scroll over the Configuration section. The sub-navigation menu displays.
2. From the Obix Integration link, click the Device Mapping link. The Device Mapping list page displays.
3. Click on the Add New Device Mapping button in the upper right hand corner.
4. Select the Device from the dropdown menu.
5. Enter the Listener Mapping Name in field provided.

	NOTE: *The Listener Mapping Name selected must match the Obix name exactly or the notification push will not perform correctly.*

6. Click Save.



Details displayed include:

- This page lists all of the devices and their corresponding listener mapping names for the account.

Administrators with appropriate permissions can:

Click on a Device to access the corresponding Device Mapping page.

Click Add New Device Mapping to define new listener mapping names.

Click Reset to return to the first page of the Device Mappings list.

Appendix 5: DVR Installation Notes

	*NOTE:* *Use of DVRs with the Brivo Onsite Server requires a license key. Please consult your dealer about acquiring the necessary license key(s) to match your DVR(s).*

Xtralis DVR Installation Notes

The Xtralis DVR only functions with Internet Explorer.

Xtralis FastTrace2

FastTraceAxV01-00-05 windows client driver is required to be installed on the client's computer. This is an ActiveX implementation, so it will only function with Internet Explorer. The driver is available for download at http://www.brivo.com/support/downloads.php.

Exacq DVR Installation Notes

Brivo Onsite Server supports the following Exacq DVR models:

Exacq EL Series

Exacq Z Series

For instructions on the installation and configuration of Exacq DVRs, please consult the manufacturer's documentation.

For create/edit camera retrieval and for viewing video:

- With IE9, you have to click *Show all content.*
- With IE8, you have to click *No* when asked "Do you want to view only the webpage content that was delivered securely?".
- With IE7, you have to click *Yes* when asked "Do you want to display the nonsecure items?".

Dedicated Micros DVR Installation Notes

	*NOTE:* *Due to changes in the Dedicated Micros 4.5 firmware release, client PCs must have version 6 of the Java browser plugin. If the upgrade is necessary, users will be prompted to perform this upgrade when they attempt to view video for the first time through the Brivo Onsite Server. Customers may also be prompted by the Java update mechanism to install further Java6 updates. Brivo recommends that users install all updates suggested by the Java update application. It is important to note that this upgrade process may be required on each client PC used to view video.* *Additionally, customers using both badging and Dedicated Micros video integration on same client PC, will also be asked to re-install the Java Media Framework (JMF) following the upgrade when performing image capture. This behavior is expected, and following the re-installation, image capture and other badging features will operate normally.*

To use a Dedicated Micros DVR with Brivo Onsite Server, you must take steps to ensure that the DVR's system time is synchronized with your Brivo Onsite Server. Failing to do so may result in the incorrect video being displayed for events in the Activity Log.

To install the Dedicated Micros time synchronization utility:

1. Download the Dedicated Micros Time Synchronization Utility from http://www.brivo.com/support/downloads.php.
2. Extract the zip file into a directory on the machine that will host time synchronization tool.
3. Open DVIPSync.exe in the directory used in Step 2. The DVIP Time Sync V0.3 application window displays.
4. Left-click on the toolbar. A popup text edit window opens, displaying the following text:

```
; This is the file defining servers to have the time set by the
; VuSync program. It is in a standard ini file format with each
; server address as a section enclosed in [] brackets. Parameters
; in each section then define the time of day each server should
; be updated and how many days to wait between each update. Lines
; (like these) starting with a ; will be ignored
; Example:
; This is the section header defining the server and can be a URL
; or an IP address
; [server1.net1.pridomain]
; This line defines the time of day to send the update - default
; is 12:00
; SyncTime=13:00
; This line defines the number of days to wait between each update -
; default is 1
; Freq=1
; This is the date and time of the last update and will normally
; be updated by the program
```

; Lasttime=06/09/02 13:18:33

5. In the tenth line, replace the text [server1.net1.pridomain] with the IP address or DNS name of the DVR and remove the leading ; character.
6. In the thirteenth line, replace the text SyncTime=13:00 with the time at which you want to synchronize the DVR and your Brivo control panel(s), and remove the leading ; character.
7. In the sixteenth line, replace the text Freq=1 with the number of days between each update, and remove the leading ; character. It is generally best to leave this value as 1.
8. In the last line, remove the leading ; character.
9. Click Save, then Close the text edit window.
10. Right-click on the grid in the DVIP Time Sync V0.3 window and click Reload List on the popup men. The DVR IP address or DNS name should appear in the grid.
11. Close the DVIP Time Sync V0.3 application window.

To schedule the execution of the time synchronization utility:

1. Open the Windows Start menu.
2. Click All Programs or Programs, depending on your operating system.) The Programs popup menu displays.
3. Click Accessories. The Accessories popup menu displays.
4. Click System Tools. The System Tools popup menu displays.
5. Click Scheduled Tasks. The Scheduled Tasks window opens.

	*NOTE:* *For Microsoft® Windows NT, the location will be slightly different: Click on the My Computer icon, and then click Scheduled Tasks. The Scheduled Tasks window opens.*

6. Double-click Add Scheduled Task. The Scheduled Task Wizard beings running.
7. Click Next.
8. On the next screen, click Browse, and select the DVIPSync.exe from the directory to which it was saved in step 2 of the procedures for installing the Dedicated Micros time synchronization utility above.
9. On the next page, enter a descriptive name for the task, click the Daily radio button, and then click Next.
10. Enter the Start time as one minute before the time entered in step 2 of the procedures for installing the Dedicated Micros time synchronization utility above; click the Every Day radio button; enter today's date as the Start date; and then click Next.
11. Enter the user name and password of the account that will execute the time synchronization task, and then click Next. For most installations, the logged in user name and password is sufficient.
12. Click Open Advanced properties for this task when I click Finish, and then click Finish. A dialog box with the advanced settings displays.

13. Click the Settings tab. Enter 5 minutes for the Stop tasks if it runs for value, and then click OK.

Intellex DVR Installation Notes

Before you can use the Intellex DVR with the Brivo Onsite Server you must first install the Intellex client software, provided by Brivo, and specify the Brivo Onsite Server as a trusted site in Internet Explorer.

	*NOTE:* *American Dynamics has limited who is authorized to utilize the Intellex DVR interface with the Brivo Onsite Server. Please check with your Brivo representative if you have any questions about your access to this integration.*

To install the Intellex client software:

1. Create a temporary directory on the C: drive named c:\temp.
2. Go to http://www.brivo.com/support/downloads.php.
3. Download the file intellex_client.zip to the directory just created.
4. After the zip file is downloaded, open it. Inside you will find the file intellex_client.msi. Extract this file.
5. When the intellex_client.msi file is extracted, double click on it. The Intellex installation program begins running. Follow the default prompts to install the program.

	*NOTE:* *To uninstall the Intellex software, you must rerun the installation program and select Remove when prompted.*

To add your Brivo Onsite Server as a trusted site on Internet Explorer when using the Intellex DVR:

1. In Internet Explorer, click Internet Options on the Tools menu.
2. Click the Security tab.
3. Click Trusted sites. The Sites button becomes active.
4. Click Sites. The Trusted sites window opens.
5. In the Add this Web site to the zone field, enter your direct IP address https://NNN.NNN.NNN.NNNN or http://brivoOnsiteserver-name.subdomain.top-level-domain (if a DNS name has been established for your Brivo Onsite Server).
6. Click Add. The url now displays in the Web sites field.
7. Click OK to return to the Sites window.
8. Click OK to close the Internet Options window.

To configure the Windows NTP synchronization program for Intellex.

1. Right click on the time displayed in the lower right-hand corner of the Start bar. The Date/Time popup menu displays.
2. Click Adjust Date/Time. The Date and Time Properties dialog box opens.
3. Click the Internet Time.
4. Click the Automatically synchronize with an Internet time server checkbox. The Server field becomes active.
5. In the Server field, enter www.time.gov
6. Click OK. The Date and Time Properties dialog box closes.

	*NOTE:* *The Brivo Onsite Server supports Intellex DVR version 4.0 and greater.* *At this time, support for the Intellex DVR does not include password-authenticated video playback. Nor does it include custom network ports; the Intellex DVR must be configured to use the default network ports.*

Revision Table	Date	Author	Change
3.4.0	8/22/2017	LMW	Added ACS6000 and ACS300 configuration instructions
3.4.1	9/6/2017	LMW	
3.4.2	11/27/2017	LMW	Added Allegion LE Privacy Mode functionality
3.4.3	2/2/2018	LMW	Added Reset Panel Communications functionality as well as Unauthorized IP Access monitoring
3.4.4	7/9/2018	LMW	Added CAN bus recovery logic and LE locks privacy mode enhancements
3.4.4.1	9/17/2018	LMW	Updated message queueing for command channel
3.4.4.2	9/17/2018	LMW	Added enable/disable functionality to network monitoring
3.4.4.3	10/16/2018	LMW	Improved panel restart performance for input/output relays
3.4.4.4	10/31/2018	LMW	Improved panel response time during threat level changes
3.4.5	12/21/2018	LMW	Added support for AD400 wireless locks.
3.4.5.1	1/24/2019	LMW	Improved panel reboot process to suppress false door forced events at start up
3.4.5.2	2/17/2019	LMW	Improved ACS5000 panel firmware upgrade process
3.4.5.3	4/4/2019	LMW	Updated Ethernet driver for -A panels and improved panel communication if command channel drops
3.4.5.4	4/26/2019	LMW	Minor system improvements and bug fixes

3.4.5.5	6/6/2019	LMW	Minor system improvements and bug fixes
3.4.6	8/6/2019	LMW	Panel firmware upgrade improvements
3.4.6.1	10/5/2019	LMW	Updated activity log displays for Salto locks during cache mode
3.4.6.2	11/8/2019	LMW	Minor system improvements and bug fixes
3.4.6.3	2/20/2020	LMW	Added Allegion NDE door position delay configuration
3.4.7	06/25/2020	LMW	Enabled OSDP firmware upgrades via WebCLI and added critical battery events to Activity Log

P-MAN-PUB-Brivo Onsite Server Administrator's Manual Rev 3.4.7