BRIVO ONSITE ADMINISTRATOR'S MANUAL

08/02/2018

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

Table of Figures

1. Getting Started

Brivo Onsite Overview

Brivo Onsite is a standalone access control system designed specifically with the smaller organization in mind. Specifically, Brivo Onsite is ideal for managing security at a single facility, even if that facility houses more than one business.

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 is used to manage building-wide security, while individual Tenant Accounts are created for each business, enabling them to manage their own internal security.

NOTE:

The majority of this document assumes you have a single, System Account. For a description of how Brivo Onsite operates differently when Tenant Accounts are defined, see the chapter on Tenant Accounts.

Brivo Onsite is the software application used to interface with the Brivo Onsite hardware. It is accessed via a web browser, and is divided into seven sections. When you click on a section tab, a corresponding menu displays, providing access to data maintained in that section.

- The **Dashboard** section provides a two-fold administrative functionality for monitoring and controlling the output behavior of programmable system devices.
- The **History** section provides access to **Activity** 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, the **Activity Reporting** allows various reports to be generated, and the **Activity Export** allows for the activity log to be downloaded as a tab separated file to an external location. The **Administrative Journal** tracks actions performed by Account Administrators of Brivo Onsite, such as the creation or deletion of an access schedule.
- The **Users** section allows Administrators to manage users, groups and cards. The **Users** section controls if and when users be given access to the facility. The **Groups** section details the various groups in the account, and the **Cards** section lets System Administrators manage their inventory of access cards.
- The **Configuration** section allows System Administrators access to the various sections needed to configure an account. The **Hardware** section lets System Account Administrators manage doors and devices associated with the building, manage control panels, and manage antipassback functionality. The

Cards section allows Administrators to manage card formats. The **Scheduling** section provides Administrators the ability to manage specific periods of time during which a device might be accessed or operated as well as setting up holidays. The **Account** section shows **Account Details** as well as permitting the creation of the System Account as well as any additional Tenant Accounts in the **Account** section. The **Email Notifications** section also allows you to define rules for automatically emailing select individuals when specific security events occur. Finally, the **Custom Fields** section allows Administrators to define custom fields for maintaining additional information on users who have access to a facility.

- The **System** section can be accessed by System Account Administrators only, and is used to configure and monitor system operations.

At the top of each page you will also find:

- A **Log Out** button that allows you to exit Brivo Onsite in a secure manner.
- A **Help** link that transfers you to documentation on Brivo's website.

NOTE:

*Individuals with access to Brivo Onsite are referred to as Administrators. Administrators may have either read/write access to the interface, or read-only. For Administrators with read-only access, data management options, such as **Create**, **Edit**, or **Delete** buttons, are not visible.*

Individuals with access to a facility who cannot log in to Brivo Onsite are referred to as Users.

Browser Requirements

You can use any standard Web browser to access Brivo Onsite.

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

Brivo Onsite 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.

2. Network Environment

This section describes the basic operation of the Brivo Onsite series in an IP network environment. First, the network requirements are identified. Next, the steps for accessing Brivo Onsite are outlined.

Network Requirements

Requirements	Comment
Ethernet 10/100 Base T LAN	CAT5/CAT6 Cabling with RJ45 Connectors
Ethernet Hub/Switch set to Auto-Negotiate	Most hubs and switches default to auto-negotiate, which is the preferred setting.
DHCP	DHCP supported, but not recommended.

Accessing Brivo Onsite

This section describes how to connect to the Brivo Onsite Administrative Interface, Brivo Onsite. You will need to:

- Connect your laptop to the Main Control Board.
- Connect the Main Control Board to your LAN.
- Log on to your laptop and access Brivo Onsite.

NOTE:

In most cases, the Brivo Onsite hardware will self-configure its network settings without any input from the installer. You will only need to access the Administrative Interface if you need to configure your network settings manually or for troubleshooting.

To connect a laptop to the Main Board:

1. Power down your laptop.
2. Connect a CAT5 or CAT6 network cable with RJ45 jacks from the ADMIN port on the Main Board to the Ethernet port on your laptop, as shown in Figure 1 and Figure 2.

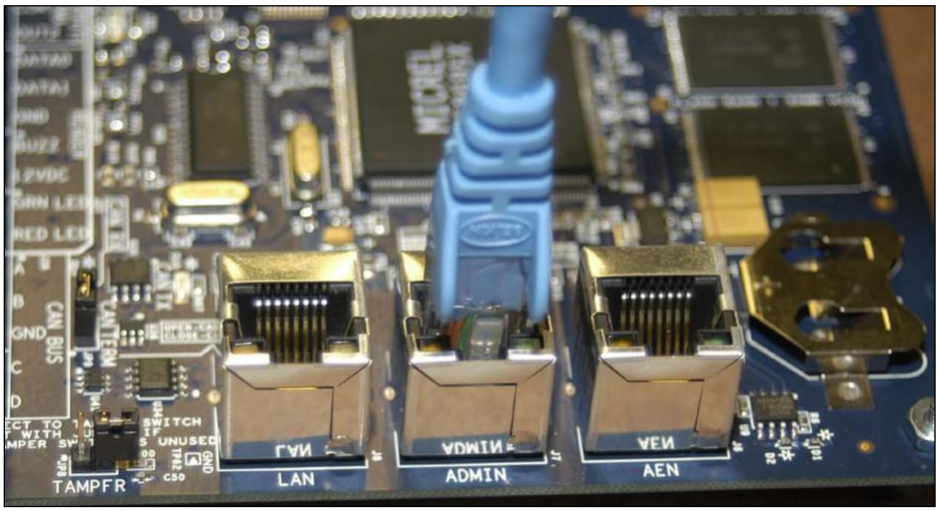

Figure 1. Connect Laptop to Admin Port on MAIN BOARD (ACS5000-S panel)

Figure 2. Connect Laptop to Admin Port on MAIN BOARD (Brivo Onsite panel)

3. When the Ethernet connection is working properly, you will see a green LED illuminated on the right side of the socket. If the green light is not illuminated, check both the connection on the control panel and your laptop.

To connect the Main Board to a LAN:

1. Connect an Ethernet cable from your local network to the LAN port of the Main Board, as shown in Figure 2, below.

NOTE:

Only the Main Board requires an Ethernet connection; any other boards that are slaved off of the Main Board communicate via the CAN bus.

Figure 3. Connect Main Board to LAN (ACS5000-S panel)

Figure 4.

Figure 5. Connect Main Board to LAN (Brivo Onsite Panel)

2. When the Ethernet connection is working properly, you will see a green LED illuminated on the right side of the socket. If the green light is not illuminated, check the connection on the control panel as well as the connection on the Ethernet hub to which the panel is wired.

To access Brivo Onsite:

1. After connecting your laptop to the Main Control Board, power on your laptop.
    - During the power-on sequence, your laptop will obtain local network settings from the Main Board, provided your laptop's network configuration is set to "Automatically Obtain IP Address." This is the most common setting for computers running Microsoft Windows.
    - If your laptop is not configured to obtain network settings automatically, use the Help utilities on your laptop to determine how to change the settings for your operating system.
2. After your computer has finished booting up, open your web browser.
3. In your web browser, enter the address http://Onsite.brivo.com. The Log In page displays, and you can now set up your System Account. See the Accounts section for more information.

Figure 6. Access Log In Screen

4. See the Configuring the Network section for information on how to assign a static IP address for the Brivo Onsite LAN.

3. Dashboard

The Dashboard page is the initial system form displayed after logging into Brivo Onsite. The Dashboard provides a two-fold administrative functionality for monitoring and controlling the output behavior of programmable system devices. The left side of the Dashboard page displays the Activity list. It is a dynamic system activity log that automatically refreshes periodically 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 right side of the Dashboard page displays the Device Status list. It lists system devices in alphabetical order, along with their lock/unlock status. For Administrators configured to use it, the Device Status list also provides corresponding command button mechanisms to control the output behavior of specific devices.

- The System Account Administrator can *always* view *all* events in the Activity listing and use *all* command buttons in the Device Status list on the Dashboard page.
- All Tenant Administrators can *always* view *all* events in the Activity list, but only those with the ability to activate devices can view and use the command button mechanisms in the Device Status list of the Dashboard page (refer to Creating a User).
- On the Edit Device page, system devices *must* be configured for an output behavior of Pulse, Latch or Unlatch *and* have the **Control from website** 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.

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. *All* Administrators can view *all* system activity entries displayed on the Dashboard page.

To view the Dashboard page:

The Dashboard page displays automatically when you first log into Brivo Onsite. From any other page in the system, click the **Dashboard** tab to access the Dashboard page.

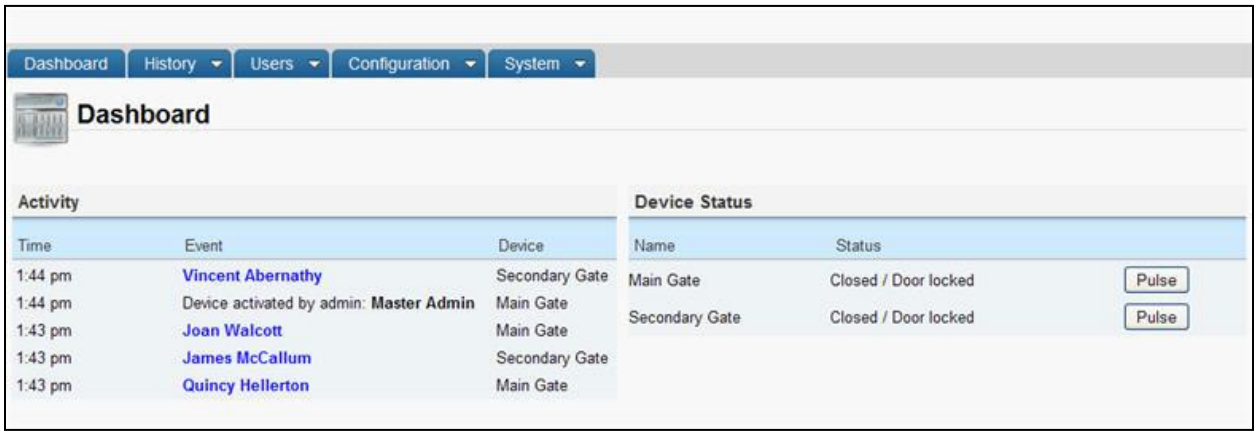

Figure 7. View Dashboard and Live Status

Details displayed include:

- **[Activity] Time**. The time at which the event occurred.
- **[Activity] Event**. The type of system activity event. 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.
- **[Activity] Device**. The device at which the event occurred. Clicking the device name takes you to the corresponding Device Details page.
- **[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.
- **[Device Status] 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.)
- **[Device Status] Pulse**. The pulse button that allows Administrators to pulse a door or device that has been configured to be controlled from the website. If no doors or devices are configured to be controlled from the website, this button does not appear.

All Administrators can:

- View the most recent system 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.

Device Status

When logging into the Brivo interface for Onsite, the **Dashboard** tab displays the live status of a door or device on the right-hand side of the screen. For example, depending on its position, the status of a door will be displayed on the **Dashboard** under "Device Status" as "Open/Door Unlocked" or "Closed/Door Locked." This message cannot be altered.

Under the "Device Status" heading, messages display the status of the device. You may choose to customize the message displayed for programmable devices.

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

Follow these steps to customize the message that displays on the **Dashboard** for a programmable device:

1. Click on the **Configuration** dropdown menu and then click on the **Hardware** tab and then the **Devices** tab.
2. If you want to modify an existing device's message:
    a. Click on the device whose message you wish to modify.
    b. At the bottom of the page, click **Edit**.
    c. At the bottom of the **Edit** page, check the **Report Engage** checkbox. Below that, enter the **Message** you wish to be displayed on the **Dashboard**.
    d. Check the **Control from website** checkbox if you want to control the device from the **Dashboard**.
    e. Click **Save**.

Figure 8. Customize Live Status Message

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.

NOTE:

The Dashboard's Latch function differs from its Lock Early function in that it physically holds the door device locked until the Administrator intentionally releases it with the Unlatch command button. Lock Early also locks the door, but it will still be released in accordance with its associated locking schedule. The Dashboard's Follow Schedule function simply toggles off the Lock Early/Unlock Early feature.

Using the Dashboard's Pulse Feature

The Dashboard's 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. This Pulse feature might also prove useful with a Door Ajar alarm.

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
11:19 am	Device activated by admin: **Lisa Dominci**	Back Door

Figure 9. 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
11:24 am	Output latched by admin: **Lisa Dominci**	Failed Front Door

Figure 10. 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
11:30 am	Output unlatched by admin: **Lisa Dominci**	Failed Front Door

Figure 11. 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.

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
12:49 pm	Door locked ahead of schedule: **Lisa Dominci**	Front Door

Figure 12. 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.

Time	Event	Device
12:13 pm	Door unlocked ahead of schedule: **Lisa Dominci**	Front Door

Figure 13. Dashboard Activity List – Door Unlocked Event Entry

5. 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.

6. 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
12:31 pm	Door returned to following configured unlock schedule: **Lisa Dominci**	Front Door

Figure 14. Dashboard Activity List – Door Unlocked Event Entry

4. History

Brivo Onsite tracks the operation of all system devices, such as when a door is unlocked or when a light is automatically switched on. 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 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. System Account Administrators can view all activity entries.

To view the System Activity page:

Click the **History** dropdown menu then click on the **Activity** tab and then click on the **System Activity** tab to access the System Activity page.

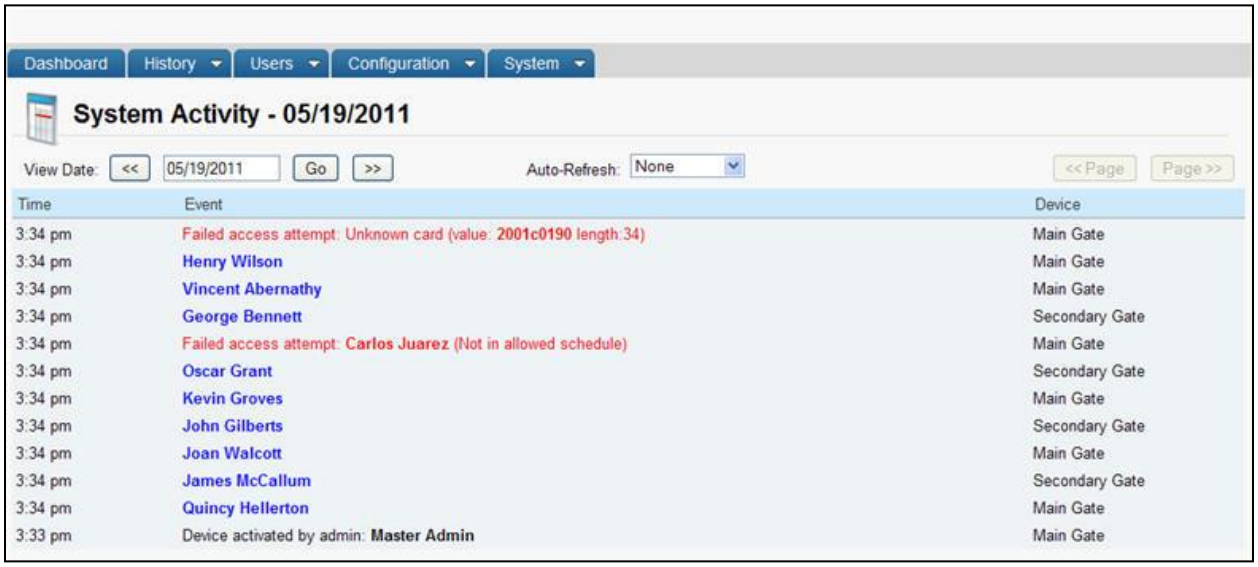

Figure 15. View System Activity Log

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.

All Administrators 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.
- Set the page to refresh automatically by clicking an interval on the **Auto-Refresh** drop-down list.
- 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.

Index of Events

The following events appear in the System Activity log.

Access Events

- Access by User

Exception Events

- Door Ajar
- Door Ajar Cleared
- Too Many Invalid PINs
- Door Forced Open
- Door Locked by Timer
- Door Unlocked by Timer
- Failed access attempt (by Unknown Person): Unknown credential
- Failed access attempt (by Unknown Person): Unassigned or revoked card
- Failed access attempt (by Known User): User is out of effective date range
- Failed access attempt (by Known User): User is at unauthorized door
- Failed access attempt (by Known User): User is out of schedule
- Failed access attempt (by Known User): Antipassback violation
- Invalid Second Factor (by Known User): (Second credential not presented)
- Invalid Second Factor (by Known User): (Invalid Card)
- Invalid Second Factor (by Known User): Same Card Credential Presented Twice
- Invalid Second Factor (by Known User): Same PIN Credential Presented Twice
- Invalid Second Factor (by Known User): (Card Value: (card hex) length: (bit length))

Device Events

- Device Engaged
- Device Disengaged
- 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

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]

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] Antipassback violation
- If the credential belongs to a user who attempts to use it at a door configured for two factor credential use without presenting the second credential: Failed Access by [User Name]: Invalid Second Factor

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

All Administrators can generate an Activity Report.

To generate an activity report:

1. Click the **History** dropdown menu then click on the **Activity** tab then click on the **Activity Reporting** tab. The Activity Report page displays.

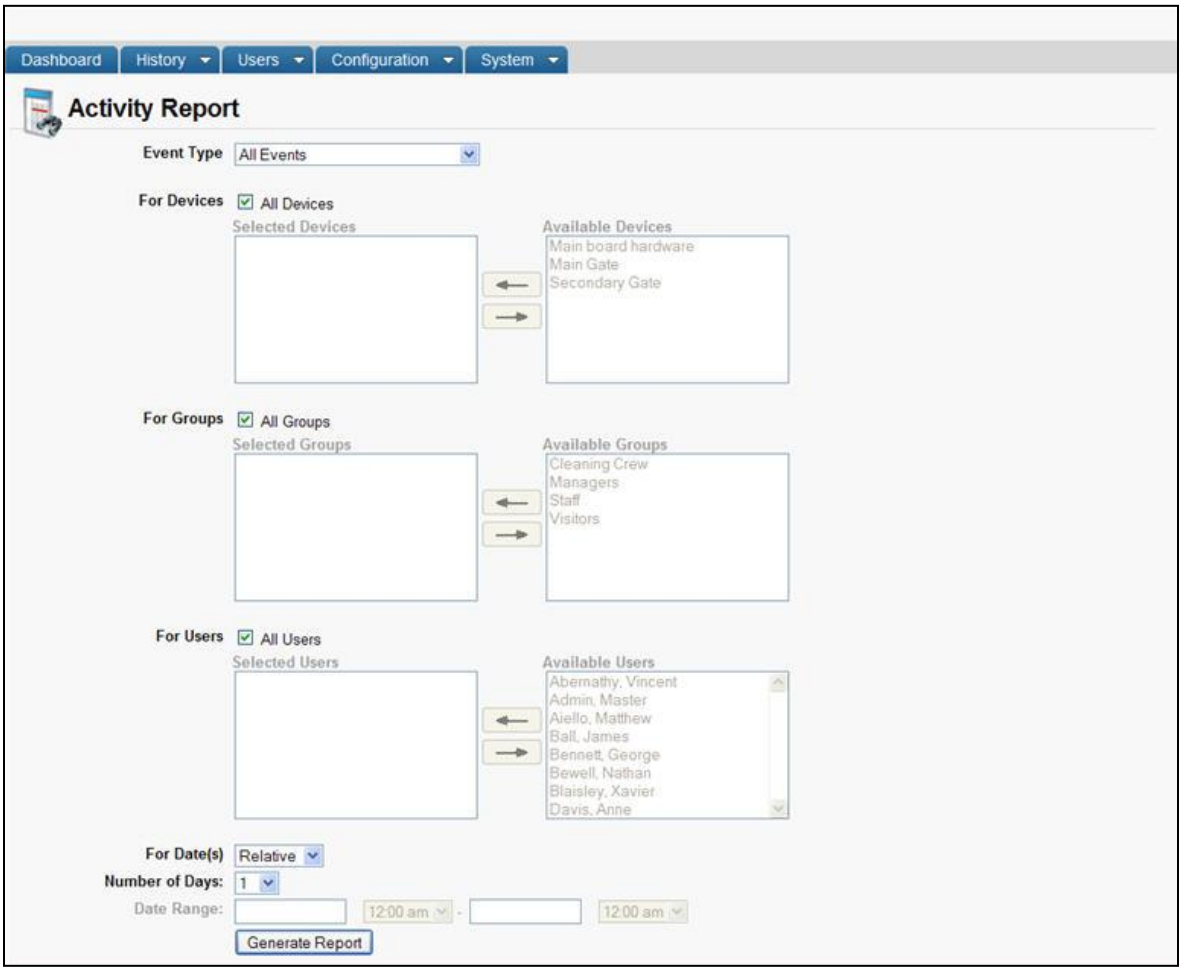

Figure 16. Generate Activity Report

2. From the **Event Type** drop-down list click the type of event(s) you want to include in the report.
3. 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 name of a device in the **Available Devices** list on the left to highlight it.
- Click ← to move the device to the **Selected Devices** list on the right.
- To remove a device from the report, click to highlight it in the **Selected Devices** list, and then click → to move it back to the **Available Devices** list.

4. 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.
5. 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.
6. 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.
7. 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 17. View Activity Report

8. 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.

All Administrators can export the Activity Log.

To export the Activity Log:

1. Click the **History** dropdown menu then click on the **Activity** tab then click on the **Activity Export** tab. The Activity Export page displays.

Figure 18. Export Activity Log

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

Browsing the Administrative Journal

The Administrative Journal tracks all Administrator actions in Brivo Onsite. 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. Click the **History** dropdown menu then click on the **Activity** tab then click on **Administrative Journal**. The Administrative Journal for the current day displays.

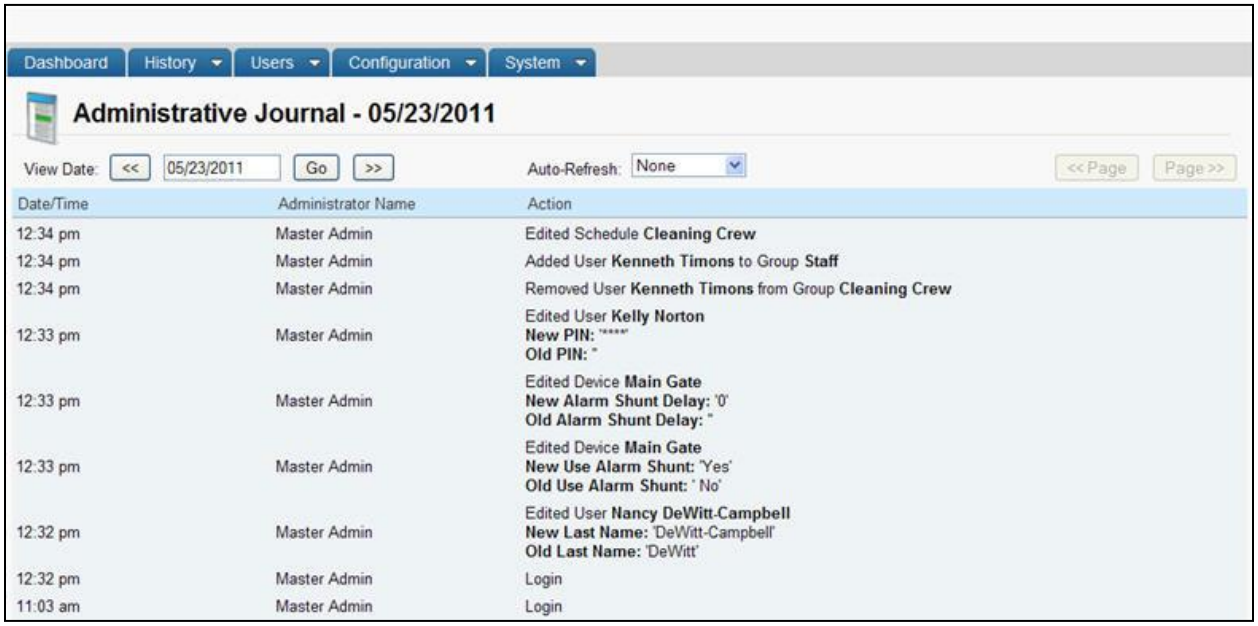

Figure 19. View Administrative Journal

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.

All Administrators 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 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.
- Set the page to refresh automatically by clicking an interval on the **Auto-Refresh** drop-down list.

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

5. Users and Groups

What are Users 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 *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 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 Groups List

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

Administrators can view the Groups associated with their own accounts.

To view the list of groups for your account:

1. Click the **Users** dropdown menu then click on the **Groups** tab. The Groups list displays.

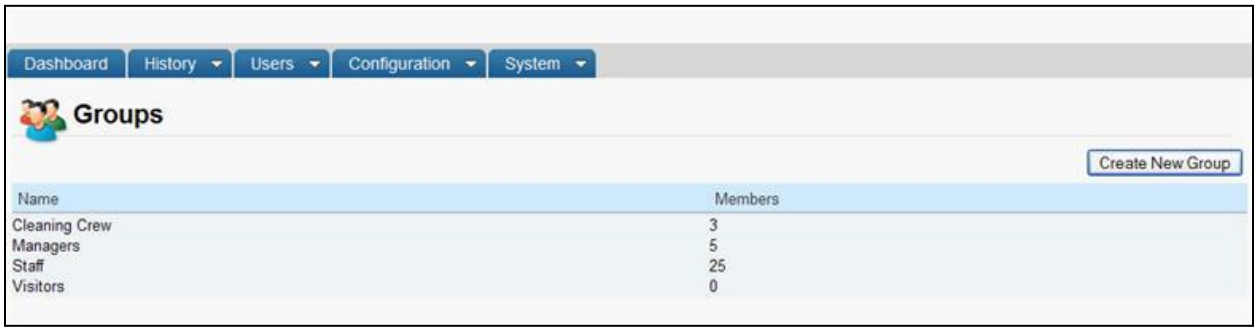

Figure 20. View Groups List

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.

All Administrators can:

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

Administrators with read/write access can:

- 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. Click the **Users** dropdown menu then click on the **Groups** tab. The Groups list displays.
2. Click the name of the group you want to view. The corresponding Group Details page displays.

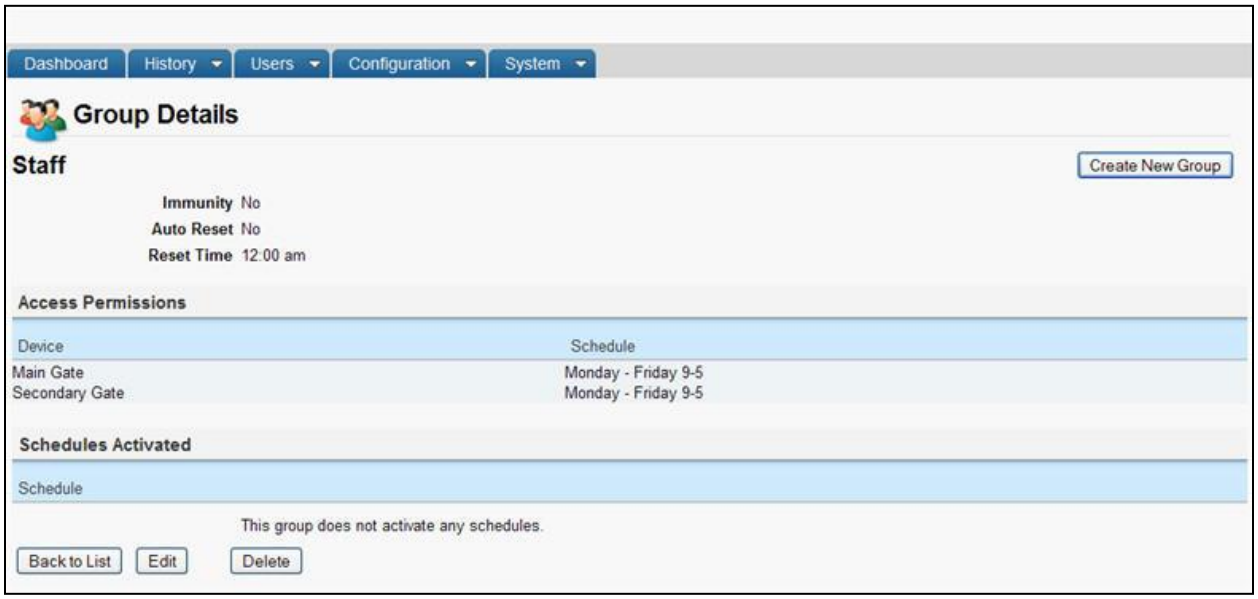

Figure 21. View Group Details

Details displayed include:

- **Antipassback Information.** Shown is whether or not a group has antipassback immunity, if the antipassback zone is reset, and if so, what time that reset occurs.
- **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.

All Administrators 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.

All Administrators with read/write access can:

- 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. Click the **Users** dropdown menu then click on the **Groups** tab. The Groups list displays.
2. Click **Create New Group**. The Edit Group page displays with blank fields.

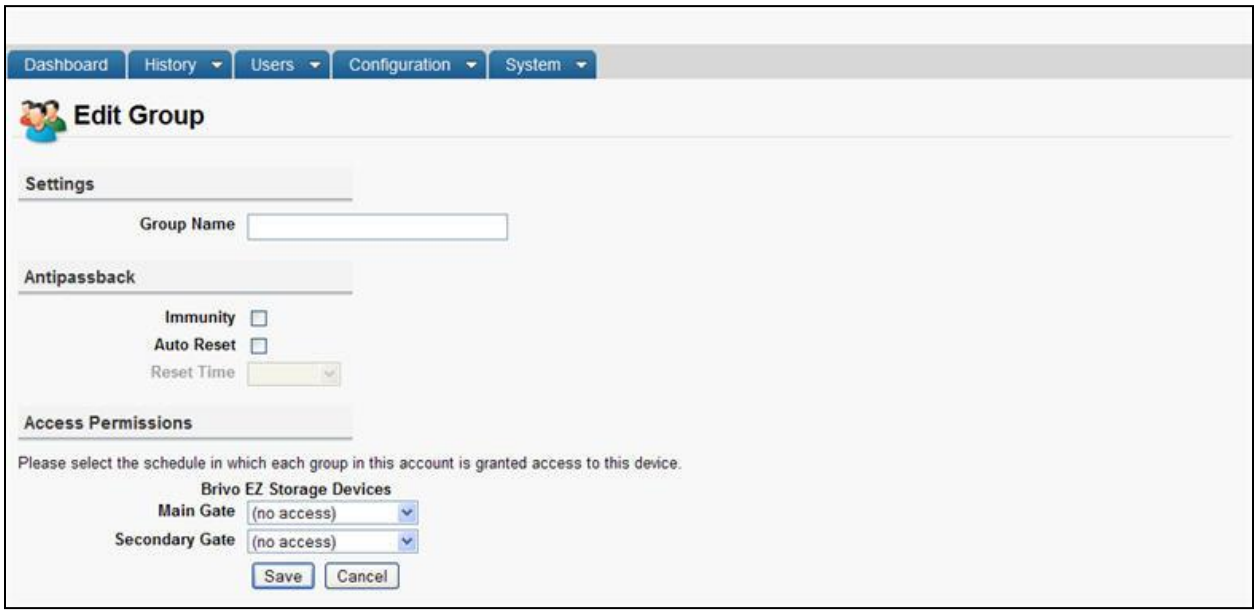

Figure 22. Create New Group

3. Enter a brief, descriptive **Group Name**.
4. For antipassback purposes, check the **Immunity** checkbox if you want the group to be immune to antipassback rules. If you want to enable antipassback, check the **Auto Reset** checkbox. Finally, if you have enabled antipassback, select at what time you want the **Reset Time** to occur each day.
5. 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.
6. Click **Save**. You are returned to the Group Details page associated with the new group.

Creating a Group Enabled Schedule

Brivo Onsite's Group Enabled Schedule feature allows you to implement a First-Person-In or Supervisor-on-Site 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.

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 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 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.

7. *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* 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 read/write access can manage groups.

To edit a group's name or access permissions:

1. Click the **Users** dropdown menu then click on the **Groups** tab. The Groups list displays.
2. Click the group whose permissions you want to change. The corresponding Group Details page displays.
3. Click **Edit**. The Edit Group page displays.

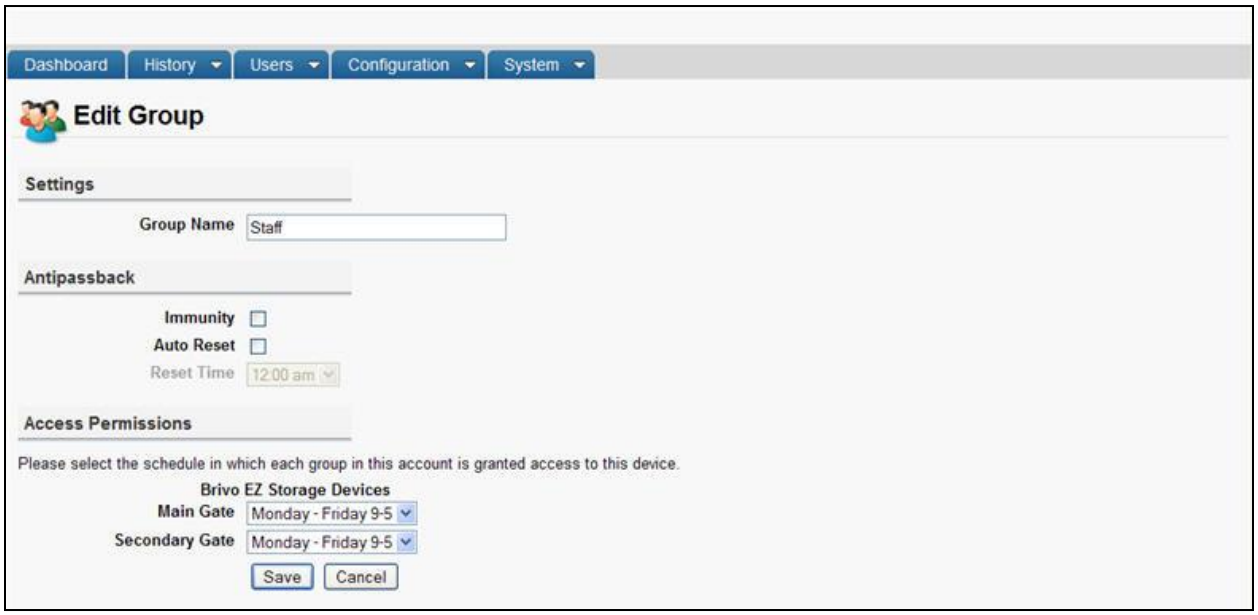

Figure 23. Edit a Group

4. To rename the group, enter a new value in the **Group Name** field.
5. Check the **Immunity** checkbox if you wish the group to be immune to antipassback.
6. Check the **Auto Reset** checkbox if you wish the group to be reset once a day for antipassback settings. Additionally, select a **Reset Time** from the dropdown list.
7. 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)**.
8. Click **Save**. You are returned to the Group Details page with the updates reflected.

To delete a group:

1. Click the **Users** dropdown menu then click on the **Groups** tab. The Groups list displays.
2. Click the name of the group you want to delete. The corresponding Group Details page displays.

3. 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.
4. Click **OK**. You are returned to the Groups list with the deleted group removed.

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 can view the users associated with their account.

To view the list of users for your account:

1. Click the **Users** dropdown menu and click on the **Users** tab. The Users list displays.

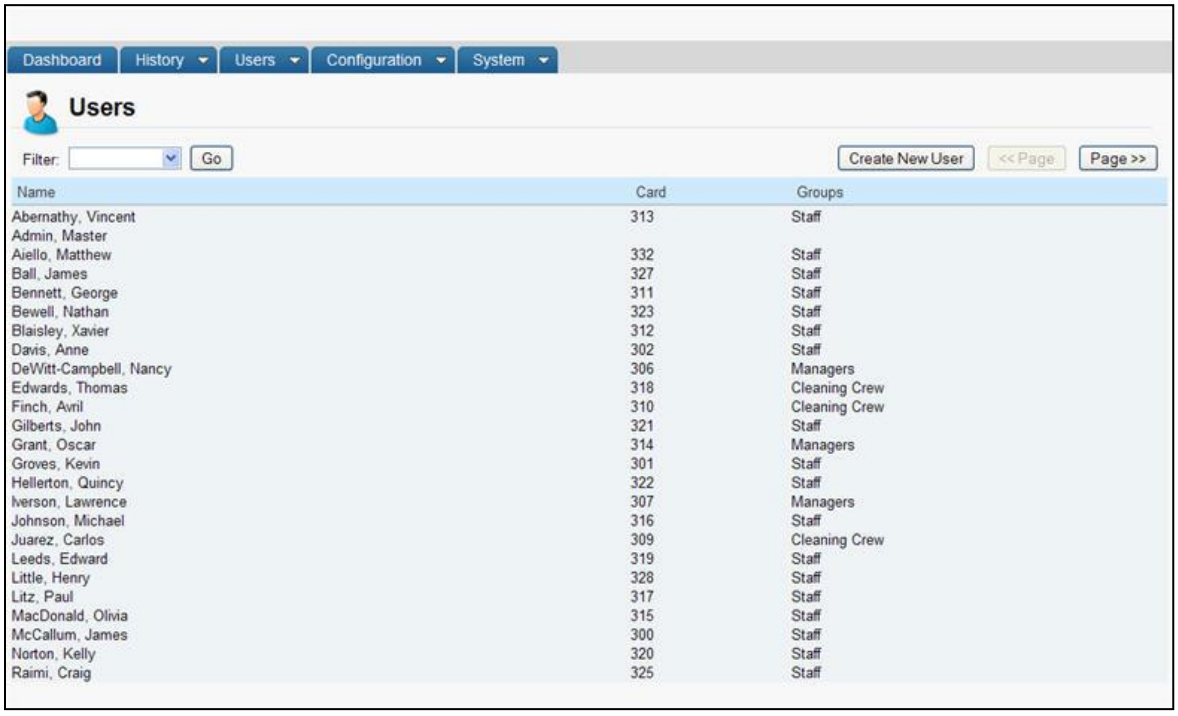

Figure 24. View Users List

Details displayed include:

- **Name**. The user's name.
- **Card**. The user's card number.
- **Groups**. The list of groups with which the user is affiliated.

All Administrators 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 and click **Go** to view a subset of the Users list. You can filter by **Last Name**, **Group**, or any custom field.
- Click **<<Page** or **Page>>** to scroll backward and forward through the list of users.

Administrators with read/write access can:

- 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. Click the **Users** dropdown menu and then click on the **Users** tab. The Users list displays.
2. Click the user you want to view. The corresponding User Details page displays.

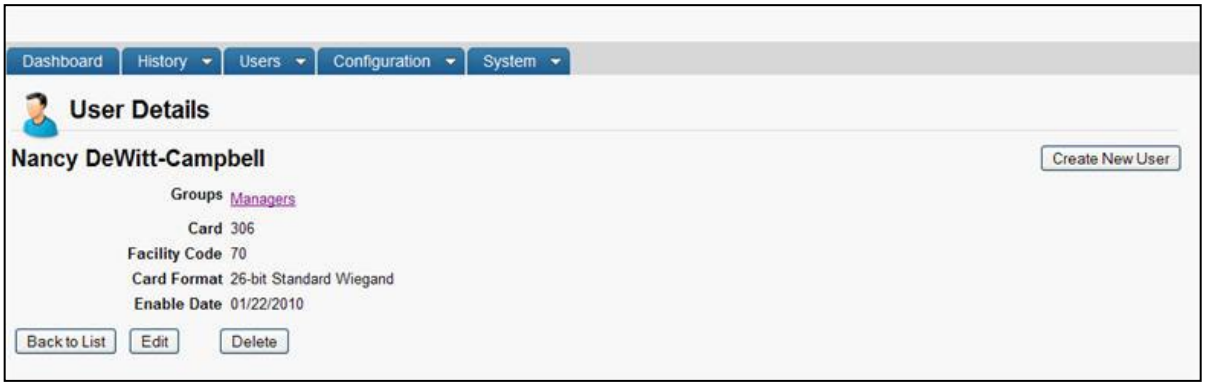

Figure 25. View User Details

Details displayed include:

- **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**, **Facility Code** and **Card Format**. If the user has been assigned a card, that card number displays along with the associated facility code and/or card format.
- **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.
- **Username**, **Preferred Language** and **Permission**. If the user is authorized to log in as an Administrator, his/her username is identified, as are that user's language preference and access permissions: "Read Write" or "Read Only."
- **Activate Devices**. If the user is authorized to log in as an Administrator with Read Only permission, this indicates if that user has access to the control buttons on the Dashboard page. ("No" only permits the user to view the event activity display on the Dashboard page.)

All Administrators can:

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

Administrators with read/write access can:

- 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.

Creating a User

Administrators with read/write access can create users for their account.

To create a user:

1. Click the **Users** dropdown menu and then click on the **Users** tab. The Users list displays.
2. Click **Create New User**. The Edit User page displays with blank fields.

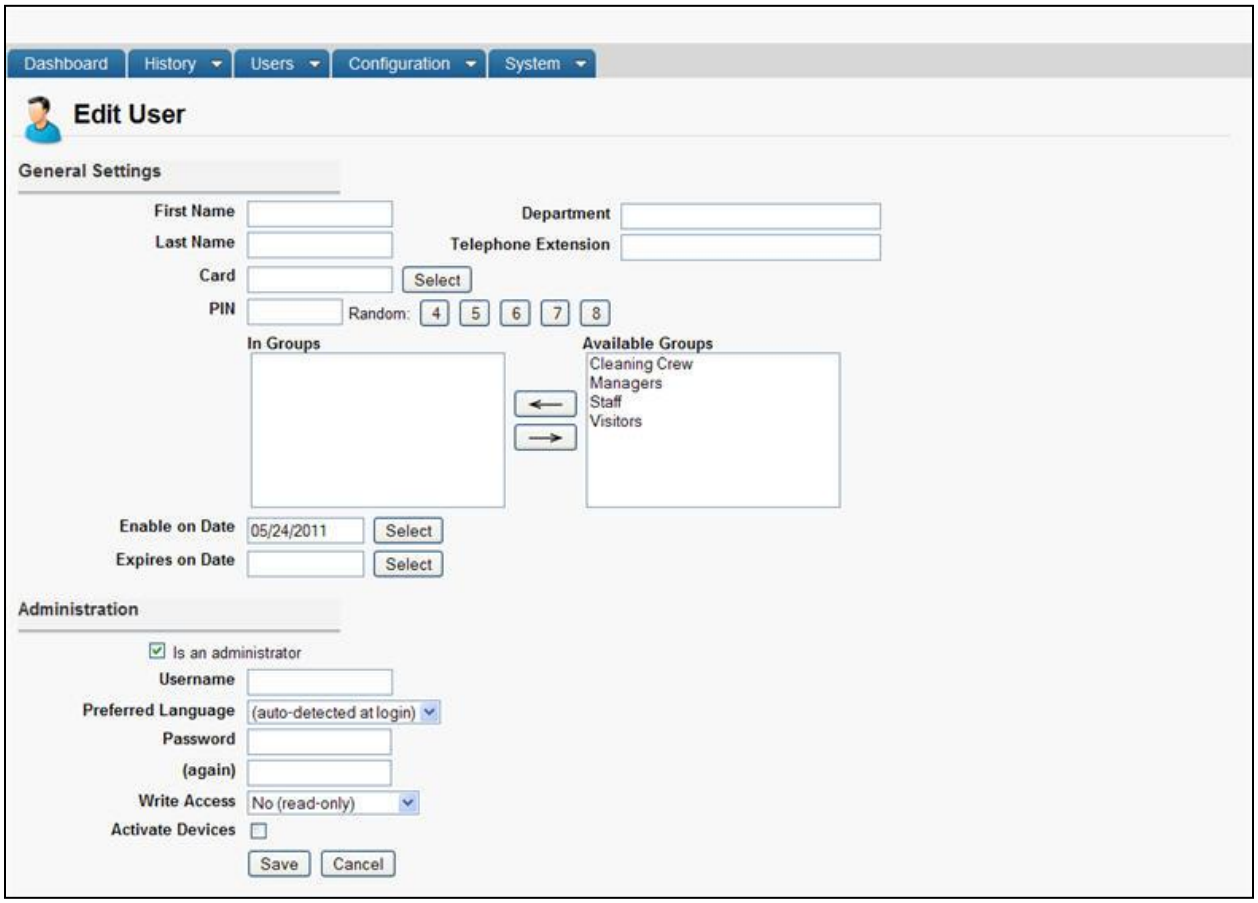

Figure 26. Create a New User

3. Enter the user's **First Name** and **Last Name**. These fields are required.
4. Custom fields display to the right of the name fields. For any custom field, enter valid values for this user. These fields are optional.
5. If your doors have card readers, select a **Card** number by clicking the **Select** button to view a popup list of all currently unassigned cards.

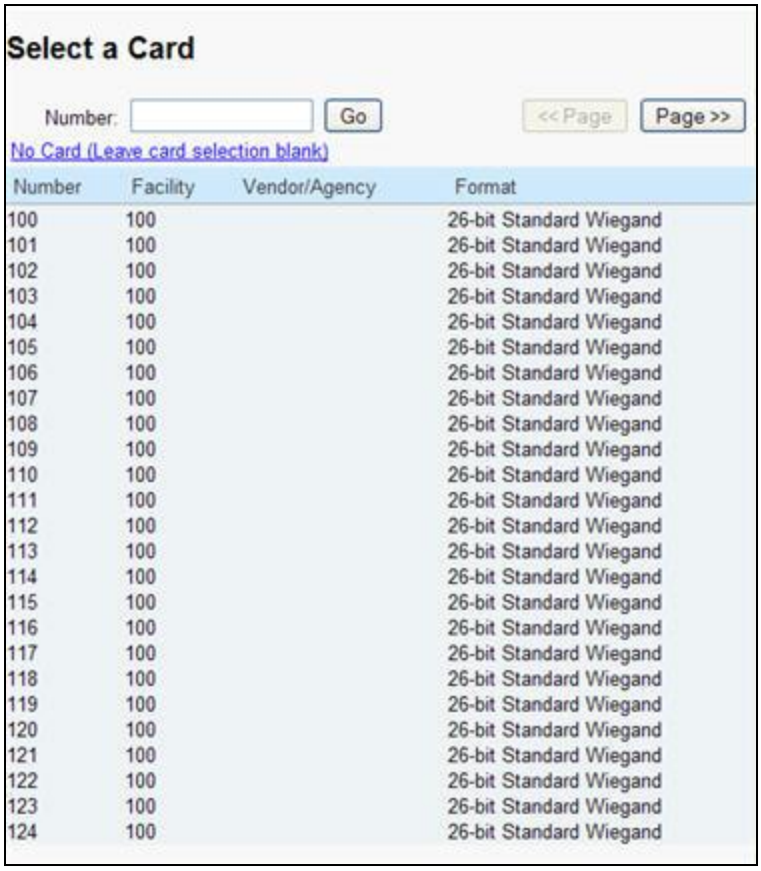

Figure 27. Select a Card Popup List

6. 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.
7. 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.
8. 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.
9. If you want the user to be able to log in to Brivo Onsite, click the box for **Is an administrator**. When you do so, the six associated fields displayed below it become active:
    - **Username**. Enter the name the Administrator will use to log into the system. The username must be 32 or fewer characters long, and can be changed at any time.
    - **Preferred Language**. Select a preferred language from the drop-down list.
    - **Password**. Enter a password for the Administrator. Re-enter the exact same password in the **(again)** field. Both of these fields are required when creating administrative permissions for a user, or when changing the password. Otherwise they are optional fields.

- **Write Access**. This field defaults to **No (read-only)**, allowing the Administrator to view all data associated with his/her account, but not to manipulate that data in any way. You can also choose **Yes**, to give the user read/write access.
- **Activate Devices**. This checkbox option is used to define if an Administrator is authorized to use the command button controls on the Dashboard page. If checked, an Administrator can control devices configured with an output behavior of Pulse, Latch or Unlatch from the Dashboard page. If unchecked, an Administrator is not given the option of controlling devices from the Dashboard page.

10. Click **Save** to create the user. The User Details page for the new user displays.

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. Click the **Users** dropdown menu then click on the **Users** tab. The Users list displays.
2. Click the user you want to edit. The User Details page displays.
3. Click **Edit**. The Edit User page displays.

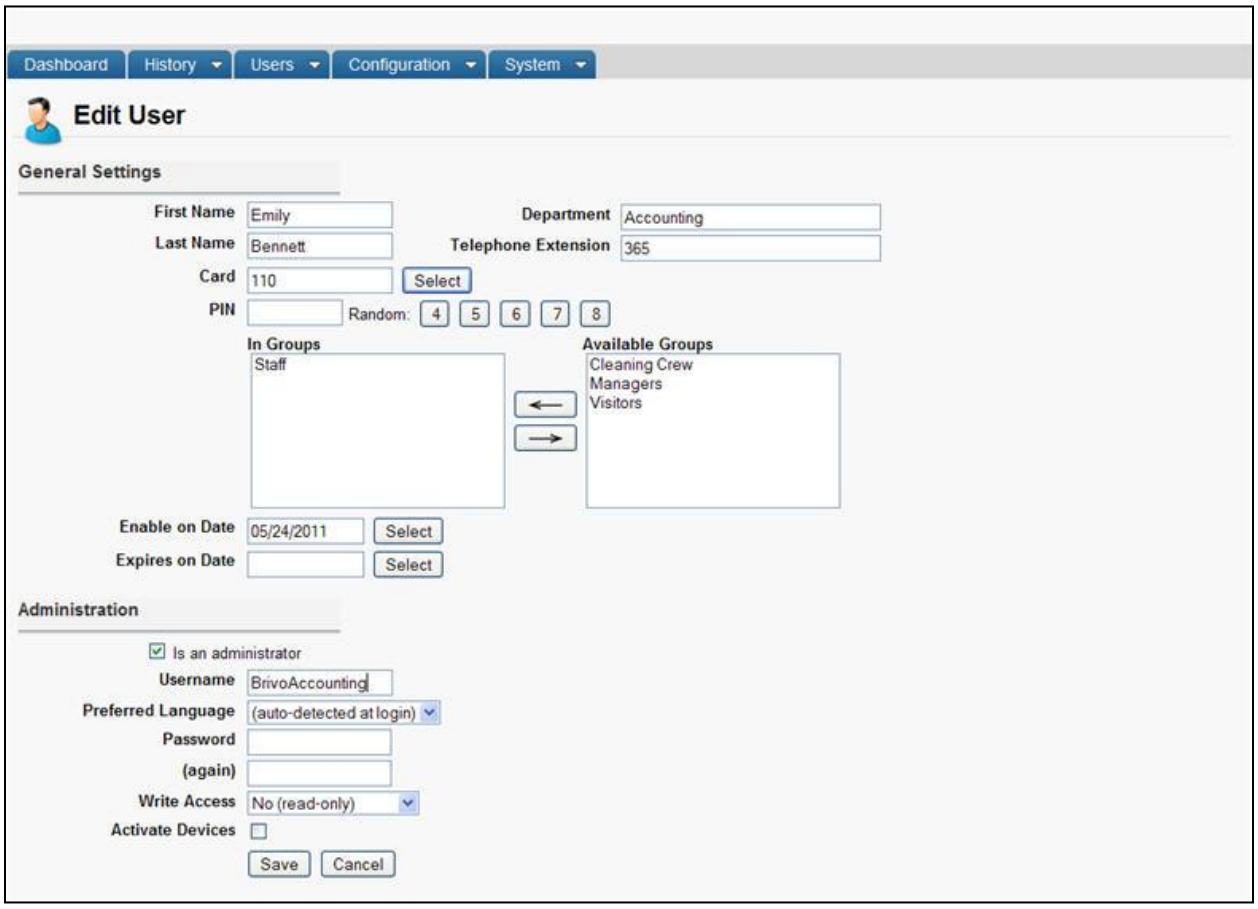

Figure 28. Edit a User

4. All fields on this page can be edited. Enter the desired changes using the guidelines for creating a user, described above.
5. 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.
6. Click **Save**. You are returned to the User Details page with the updates displayed.

To delete a user:

1. Click the **Users** dropdown menu and then click on the **Users** tab. The Users list displays.
2. Click the user you want to delete. The associated User Details page displays.
3. Click **Delete**. A warning message asks you to confirm that you want to delete the user.
4. 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. 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.

Managing Custom Fields

Custom fields store optional information about a user, such as department or parking space assignment. You can define up to ten 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.

All Administrators can view custom fields. Those with read/write access can also create, edit, and delete custom fields.

To view a list of custom fields for an account:

1. From the **Configuration** dropdown menu, click the **Account** tab then click on the **Custom Fields** tab. The Custom Fields list displays.

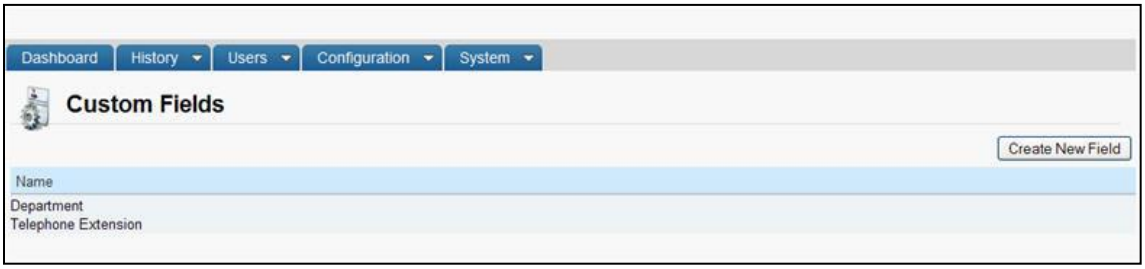

Figure 29. View Custom Fields List

Details displayed include:

This page lists the **Name** of each custom field defined for the account.

Administrators with read/write access can:

- Click 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.

To create a new custom field:

1. From the **Configuration** dropdown menu, click the **Account** tab then click on the **Custom Fields** tab. The Custom Fields list displays
2. Click **Create New Field**. The Edit Custom Field page displays.

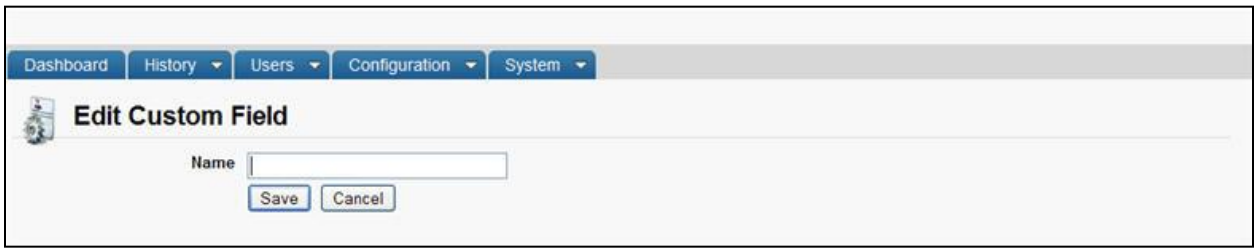

Figure 30. Create a Custom Field

3. Enter a brief, descriptive **Name** for the field, such as "Department" or "Office Number."

4. 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. From the **Configuration** dropdown menu, click the **Account** tab then click on the **Custom Fields** tab. The Custom Fields list displays.
2. Click the field you want to rename. The Edit Custom Field page displays.

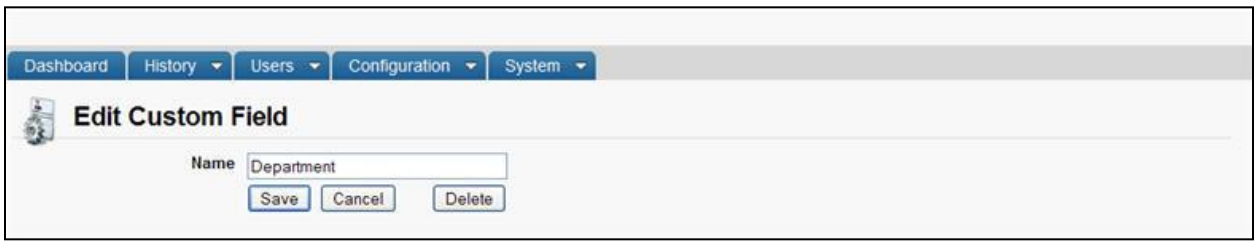

Figure 31. Rename a Custom Field

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

To delete a custom field:

1. From the **Configuration** dropdown menu, click the **Account** tab then click on the **Custom Fields** tab. The Custom Fields list displays.
2. Click the field you want to delete. The Edit Custom Field page display.
3. Click **Delete**. A warning message displays.
4. 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.

6. 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.

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 users to identify themselves 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. Click the **Cards** tab. The Cards list displays.

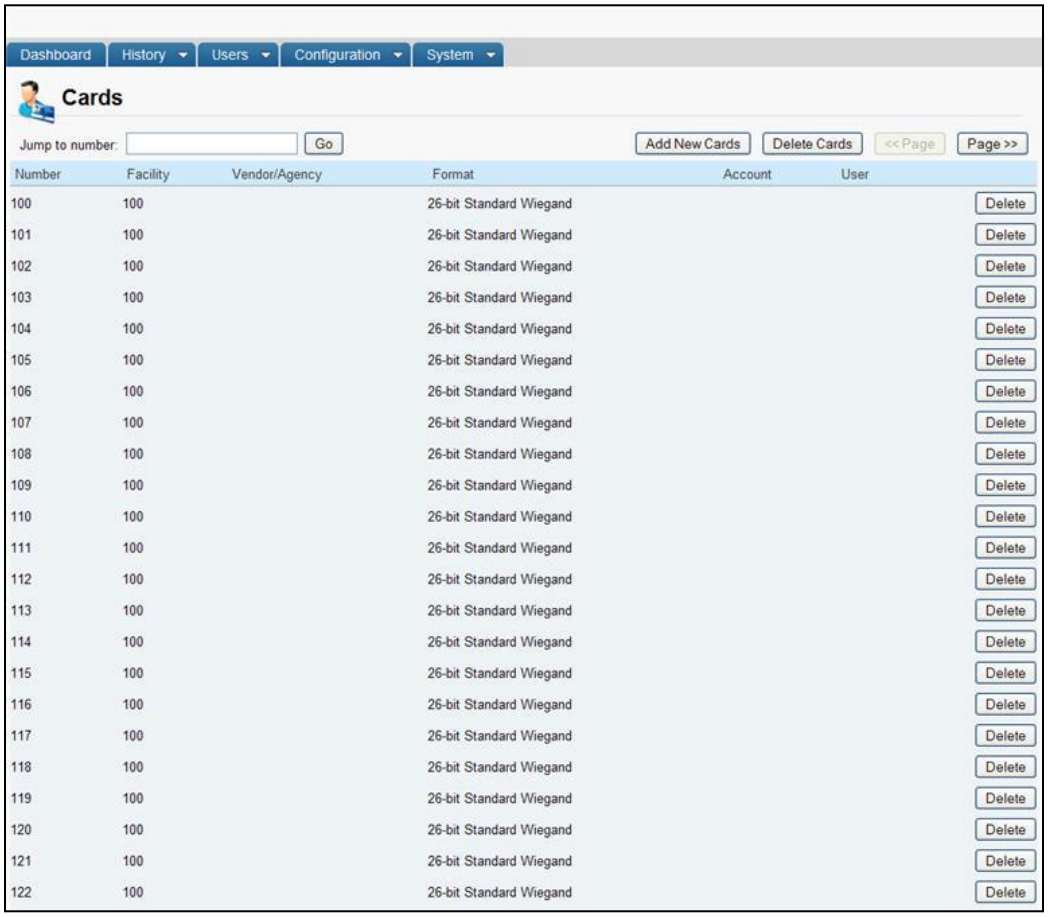

Figure 32. Viewing Cards List

Details displayed include:

- **Number.** The number displaying on the outside of the card
- **Site/Facility.** The site/facility code assigned by the card manufacturer.
- **Vendor/Agency.** The vendor/agency code assigned by the card manufacturer.
- **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.

All Administrators 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.

Administrators with read/write access can:

- 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

System Account Administrators with read/write access 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 up to 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). All System Account Administrators 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. From the **Users** dropdown menu, click on the **Cards** tab. The Cards list displays.
2. Click **Add New Cards**. The Add Cards page displays.

Figure 33. Add New Cards

3. Click the appropriate **Format** on the drop-down list.
4. 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.

5. 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.

6. Enter the **First Internal Number**. The internal number is part of the card's embedded value. **First Internal 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 100. In other words, the range defined by the first and last external numbers can be no greater than 100.*

7. Enter the **Site/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.
8. Enter the **Vendor/Agency Code** if one came from the card manufacturer. Not all card formats have vendor/agency codes. In those cases, the **Vendor/Agency Code** field will remain grayed out.
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. From the **History** dropdown menu, click on the **Activity** tab then click on the **System Activity** tab to view the System Activity log, which displays a list of all activity events, including the unknown credential event just created.
3. Click on the raw card value. The Card Format Recognizer displays, with the **Internal Card Bits**, **Length**, **Format, Card Internal Number, Card External Number,** and **Facility** filled in from the System Activity log entry.

Figure 34. Add Card by Value

4. The **Card External Value** is already populated, the number shown on the outside of the card.
5. Click **Add Card with this format** to add the card to the Card Bank. You are returned to the Card Bank with the new card shown.
6. Alternately, you may choose to add the card as an Opaque Card, assigning it an external number of your own choosing. Enter the card number in the **Card External Number** field under **Add as Opaque Card**.

7. Click **Save**. You are 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 System Account Administrators with read/write access. Only those card formats defined by an Administrator can be edited or deleted.

NOTE:

Only those card formats defined by an Administrator can be edited or deleted.

To view the list of card formats:

1. From the **Configuration** dropdown menu, click the **Cards** tab then click on the **Card Formats** tab. The Card Formats page displays.

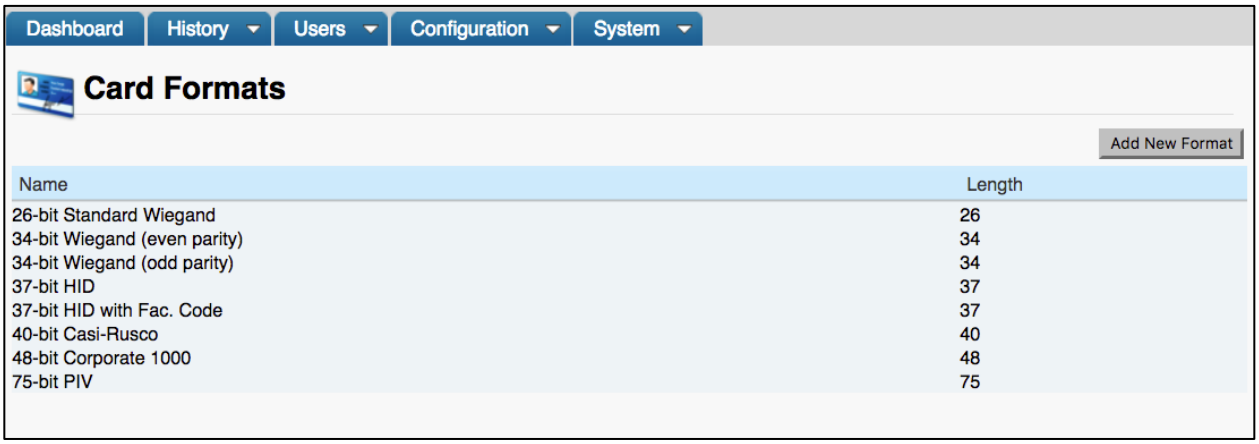

Figure 35. View Card Formats

Details displayed include:

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

All System Administrators can:

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

System Administrators with read/write access can:

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

To view the details for a specific card format:

1. From the **Configuration** dropdown menu, click the **Cards** tab then click the **Card Formats** tab. The Card Formats page displays.
2. Click the card format you want to view. The corresponding Card Format page displays.

Figure 36. View Card Format Details

Details displayed include:

- **Length**. The length, in bit size, of the card format.
- **Number**. The internal value that uniquely identifies the card.
- **Facility**. An internal value set at manufacturing to differentiate cards with the same external value.
- **Vendor bits**. Some card formats have a hardwired set of bits unique to the card vendor.
- **Parity bit 1**, **Parity bit 2**, **Parity bit 3**, **Parity bit 4**. Simple parity bit calculations are a common way to ensure the accuracy of the card read. These fields provide space to inform the card engine how to calculate a single parity 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.

All Administrators can:

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

Administrators with read/write access can:

- 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. From the **Configuration** dropdown menu, click the **Cards** tab then click the **Card Formats** tab. The Card Formats page displays.
2. Click **Add New Format**. The Edit Card Format page displays.

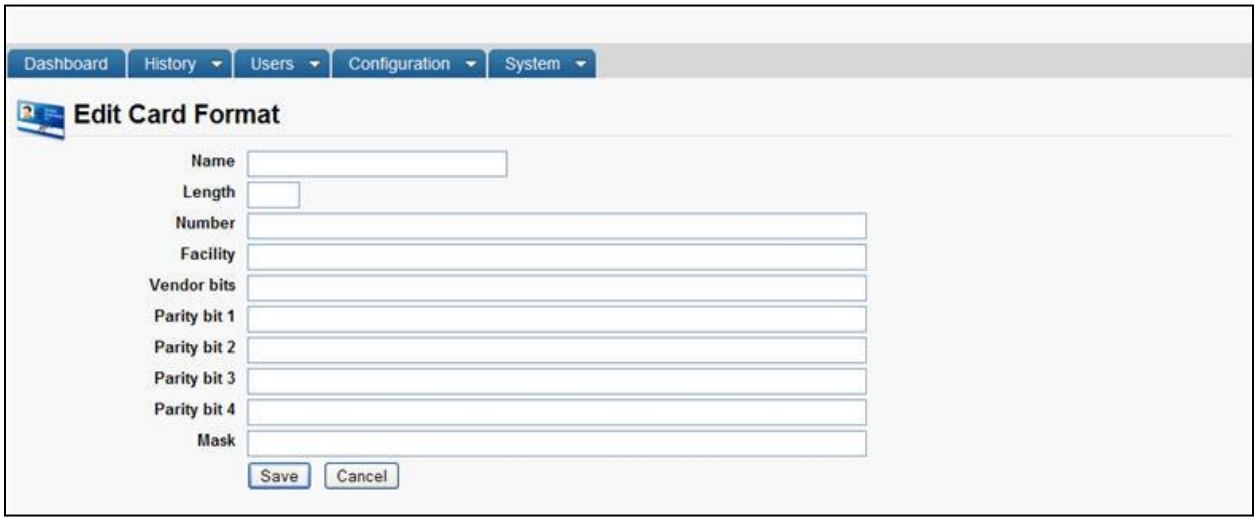

Figure 37. Create New Card Format

3. 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.
4. Enter the **Length**, the number of bits in the card format. This is a required field.
5. Enter the **Number** and **Facility** code for the new card format. The number of characters entered in each field must be the same as the bit length, and valid values include: **.** (period) to indicate an ignored bit position for this value and X to indicate that a bit used for the given value type is at a particular location. These fields are optional.
6. Enter the **Vendor bits**, an optional field that indicates any hardwired bits set in the value by the card vendor. This value would be provided by the card vendor, and is optional. Valid characters are a **.** (period) to indicate ignored bits, or which value (0 or 1) to set at a particular location.
7. **Parity bit 1**, **Parity bit 2**, **Parity bit 3**, and **Parity bit 4**. 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. These fields are optional.
8. Enter the **Mask**. 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.
9. Click **Save**. The Card Format page displays.

To create a new card format from an existing format:

1. From the **Configuration** dropdown menu, click the **Cards** tab then click the **Card Formats** tab. The Card Formats page displays.
2. Click the format you want to use as the basis for the new card format. The associated Card Format page displays.
3. 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.
4. Enter a unique **Name** for this new format. Do not use the same name as the format you copied.
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 edit a card format:

1. From the **Configuration** dropdown menu, click the **Cards** tab then click the **Card Formats** tab. The Card Formats page displays.
2. Click the format you want to edit. The associated Card Format page displays.
3. 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.*

WARNING: Edit Card Format Warning Message

If cards using the format you attempt to edit currently exist in your system, a warning message will be displayed informing you the format for these existing cards will *not* be changed as a result of your modifications. Only newly-created cards will be affected.

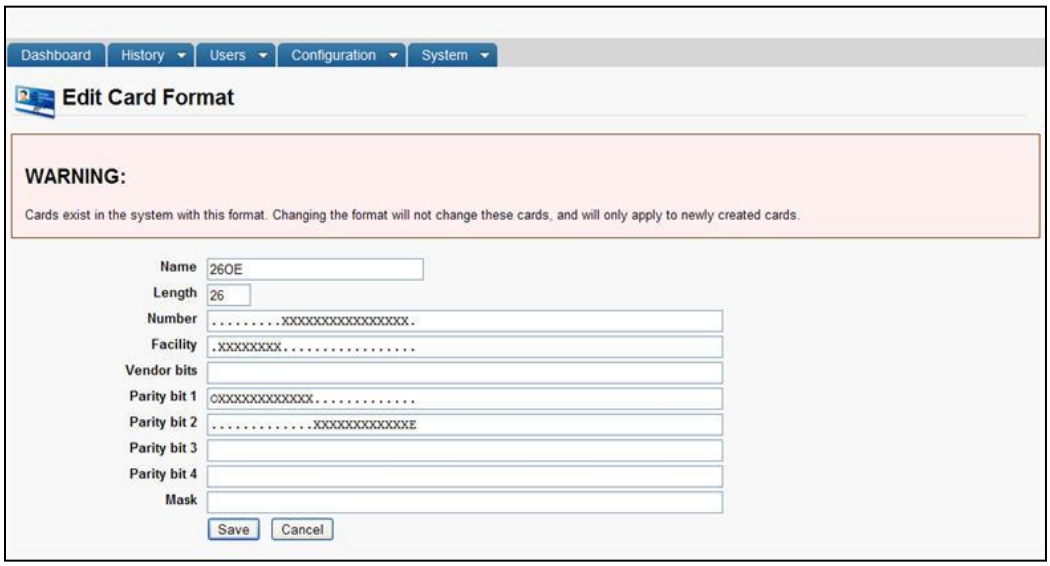

Figure 38. Edit Card Format

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

To delete a card format:

1. From the **Configuration** dropdown menu, click the **Cards** tab then click the **Card Formats** tab. The Card Formats page displays.
2. 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.*

3. 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.
4. 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.

Administrators with read/write access 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. From the **Users** dropdown menu, click the **Cards** tab. The Cards list displays.
2. Click **Delete** on the line of the card you want to delete. A warning message informs you that this operation cannot be undone.

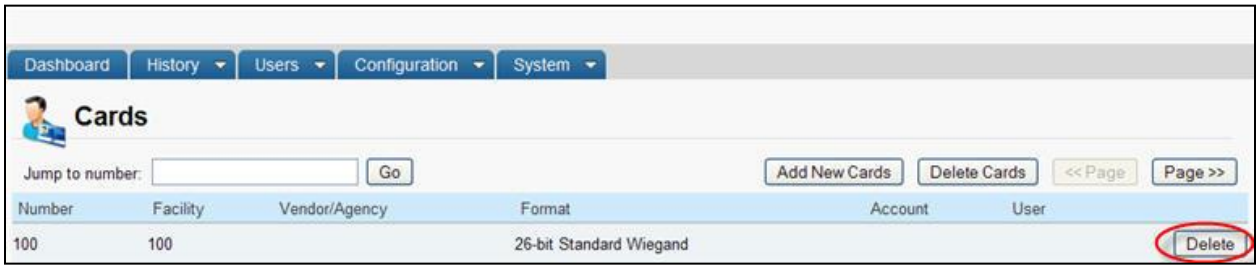

Figure 39. Deleting a Single Card

3. 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. From the **Users** dropdown menu, click the **Cards** tab. The Cards list displays.
2. Click **Delete Cards**. The Delete Cards page displays.

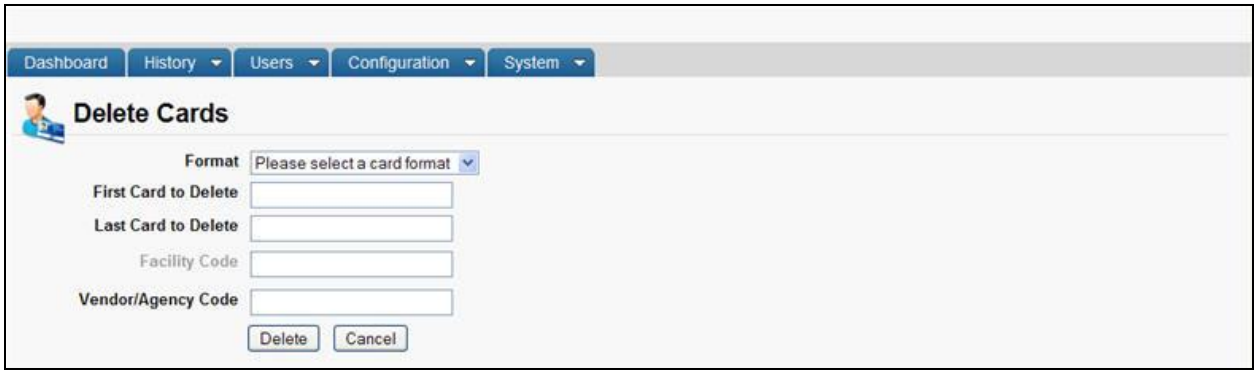

Figure 40. Delete Multiple Cards

3. From the drop-down list, click the **Format** of the cards you want to delete. This is a required field.
4. Enter the numbers of the **First Card to Delete** and the **Last Card to Delete.** These are both required fields.
5. Enter the **Facility Code** for the card range to be deleted.
6. Enter the **Vendor/Agency Code** for the card range if needed.
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.

7. Devices

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. From the **Configuration** dropdown menu, click the **Hardware** tab then click the **Devices** tab.
2. The Devices page displays.

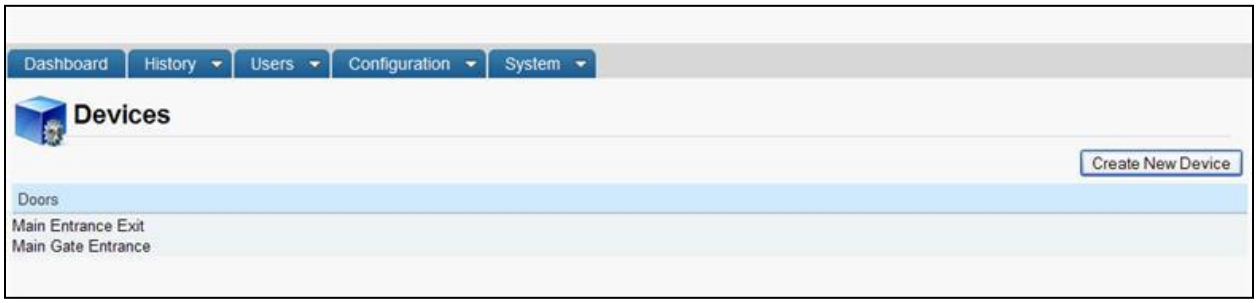

Figure 41. View Devices List

Details displayed include:

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

All Administrators can:

- Click a device to access the associated Device Details page.

Administrators with read/write access can:

- 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. From the **Configuration** dropdown menu, click the **Hardware** tab then click the **Devices** tab.
2. 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.

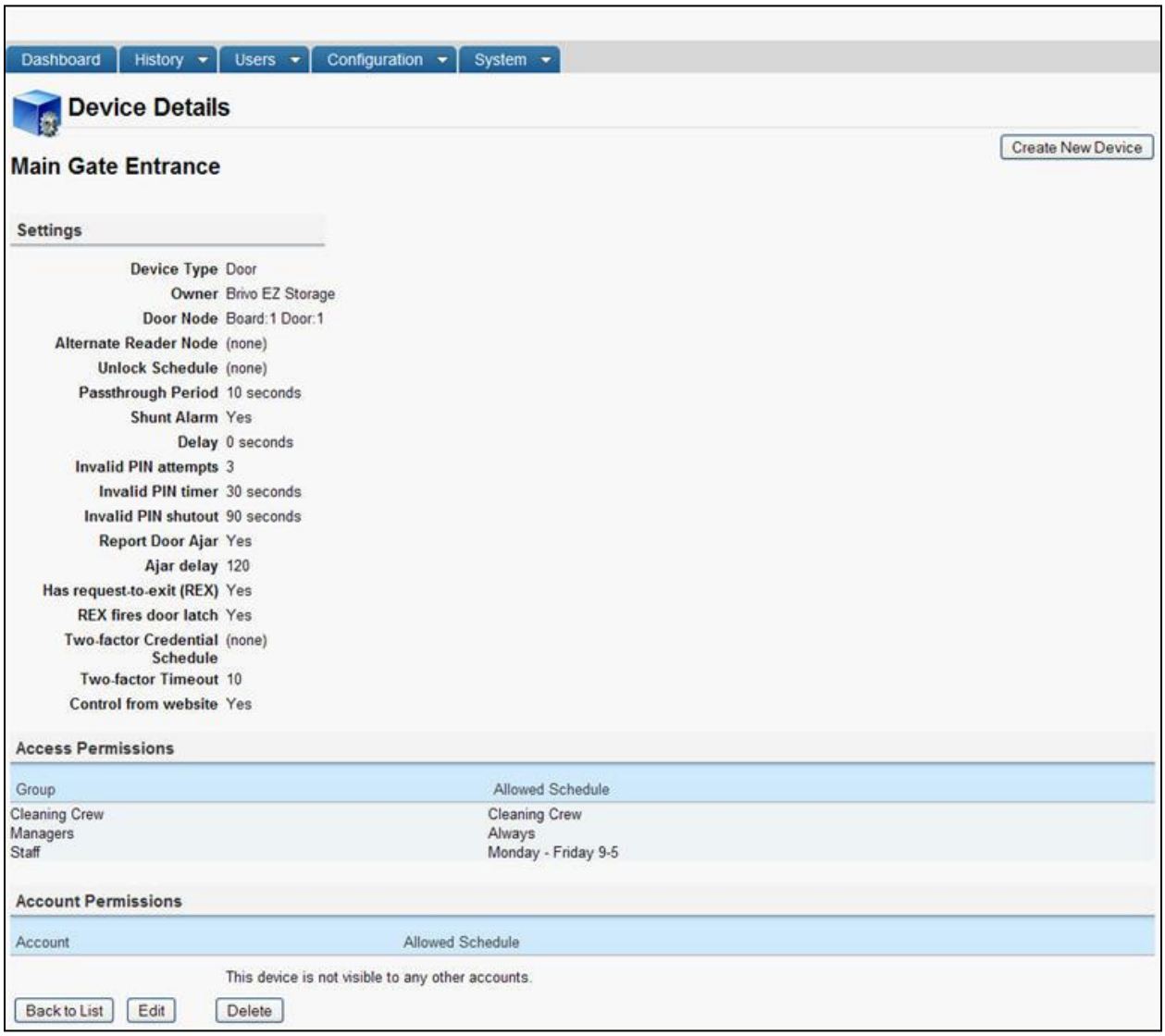

Figure 42. Device Details: Door

Details displayed include:

Details displayed on this page vary depending on the device being viewed.

All Administrators can:

- Click the name of the **Two-factor Credential 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.

Administrators with read/write access can:

- 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

Only System Account Administrators with read/write access can create devices.

To create a device for an account:

1. From the **Configuration** dropdown menu, click the **Hardware** tab then click the **Devices** tab.
2. Click **Create New Device**. The Edit Device page displays.

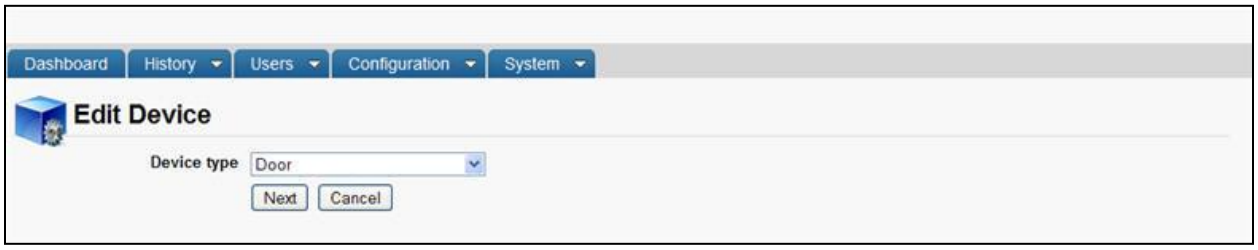

Figure 43. Create a Device

3. Select the **Device type** you want to create. See the *Glossary* at the end of this document for a brief description of each type.
4. Click **Next**. The Edit Device page displays. This page varies noticeably according to the device being created.

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/edit a device:

1. From the **Configuration** dropdown menu, click the **Hardware** tab then click the **Devices** tab.
2. Click the device you want to configure. The corresponding Device Details page displays.
3. Click **Edit**. The Edit Device page displays.

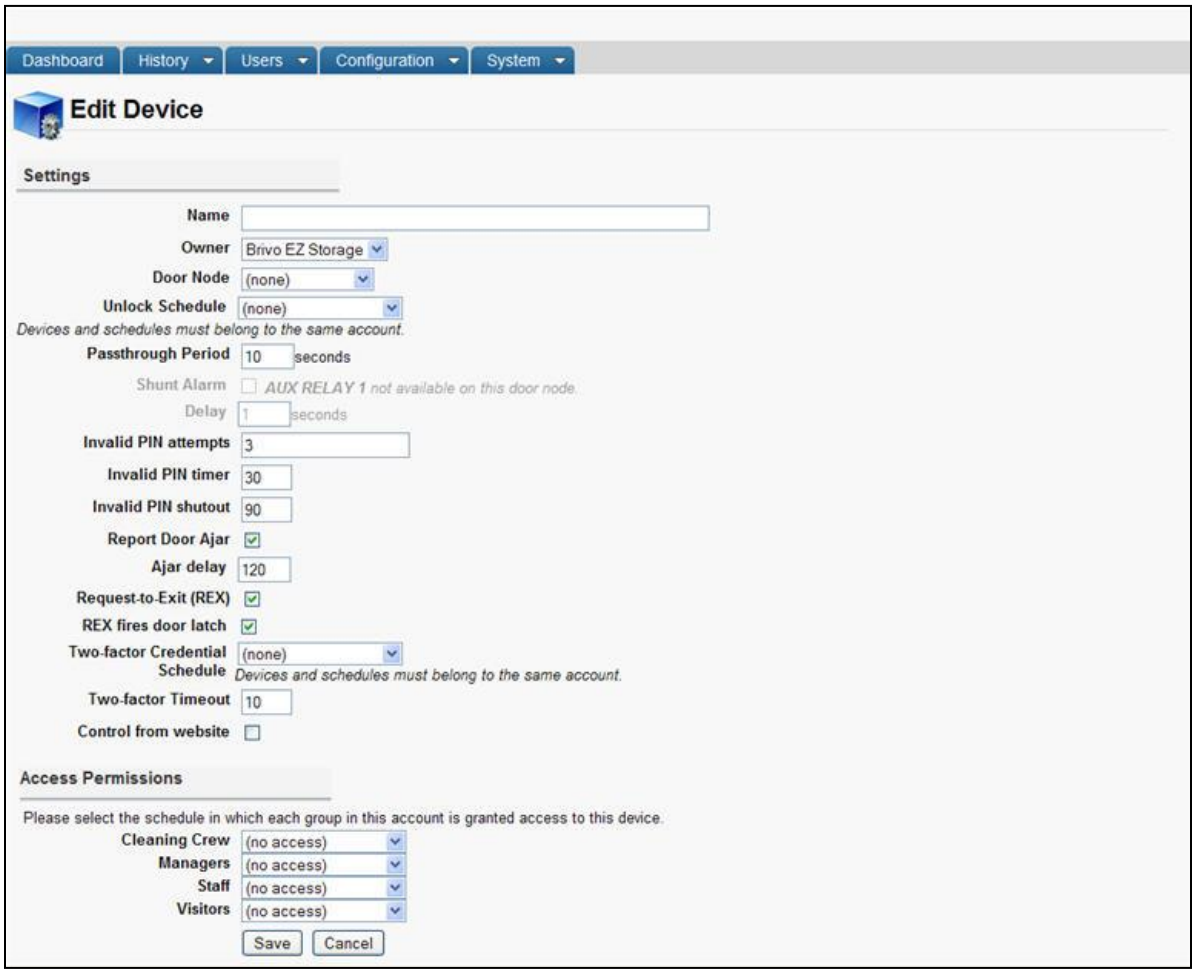

Figure 44. Configure a Door

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

4. **Name** is a required field for any type of device. The name you enter should be brief, but descriptive.
5. **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.

6. 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.
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** drop-down 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 **Output** drop-down lists displays for Input Switch, Valid Credential Input and Event Trigger devices. The list includes all valid, available output points
10. **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.
11. 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.)
12. The **Unlock Schedule** drop-down 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.
13. The **Active Schedule** drop-down 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 first create a door, the currently Active Account is the default owner, and the Unlock Schedule drop-down list automatically includes all schedules defined for that account. If you change the owner, you must first click **Save** and then return to this page to select a valid schedule.*

14. For Doors, set Passthrough, Invalid PIN, Door Ajar, and Request-to-Exit parameters:
    - In the **Passthrough Period** field, enter the maximum length of time (1-999 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 (1-9 seconds) the alarm system should be shunted In the **Delay** field. The default and strongly recommended setting is **1**.

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 (1-10) before it is considered a security risk and the keypad freezes. The default setting is **3**.
- In the **Invalid PIN timer** field, specify the amount of time (1-99 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 shutout** field lets you set the length of time (1-999 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 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 (1-999 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.

15. 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** drop-down 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 (1-99 seconds) the user will have to present both credentials. If the user takes more than the allotted time, access will be denied. The default setting is **10.**

16. 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.
17. When the **Control 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.

18. 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.
19. Click **Save**. The Device Details page displays.

To delete a device:

1. From the **Configuration** dropdown menu, click the **Hardware** tab then click the **Devices** tab.
2. Click the device you want to delete. The corresponding Device Details page displays.
3. Click **Delete**. A message displays warning that this operation cannot be undone.
4. 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. Also, when a door is deleted, this may interfere with antipassback settings.

8. Hardware

The Brivo Onsite hardware consists 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 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.

NOTE:

Although it is labeled DOOR BOARD, the Brivo Onsite 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 matches the actual control panel wiring.

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

A Brivo Onsite installation can comprise up to 15 boards. This includes the main board and up to 14 Door Boards and/or IO Boards.

With Brivo Onsite, 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 door forced open event.

Browsing the Hardware List

Only System Account Administrators can view the list of control boards.

To view the list of control boards:

1. From the **Configuration** dropdown menu, click the **Hardware** tab then click the **Hardware** tab. The Hardware page displays.

Figure 45. View Hardware List

Details displayed include:

- **Board Type**. Indicates if this is a Door Board or an IO Board.
- **Address**. The number assigned to this control board (1-15). Address 1 is automatically assigned to the Main Board
- **Location**. A brief description of where the physical board is located.

All Administrators can:

- Click the name of any board to view the associated Board Details page.

Administrators with read/write access can:

- Click **Add New Board** to access the Add New Board page in order to assign a new control board to the system.

Viewing Board Details

Only System Account Administrators can view the details for a control board.

To view details for a specific control board:

1. From the **Configuration** dropdown menu, click the **Hardware** tab then click the **Hardware** tab. The Hardware page displays.
2. Click the name of the control board you want to view. The corresponding **Board Details** page displays.

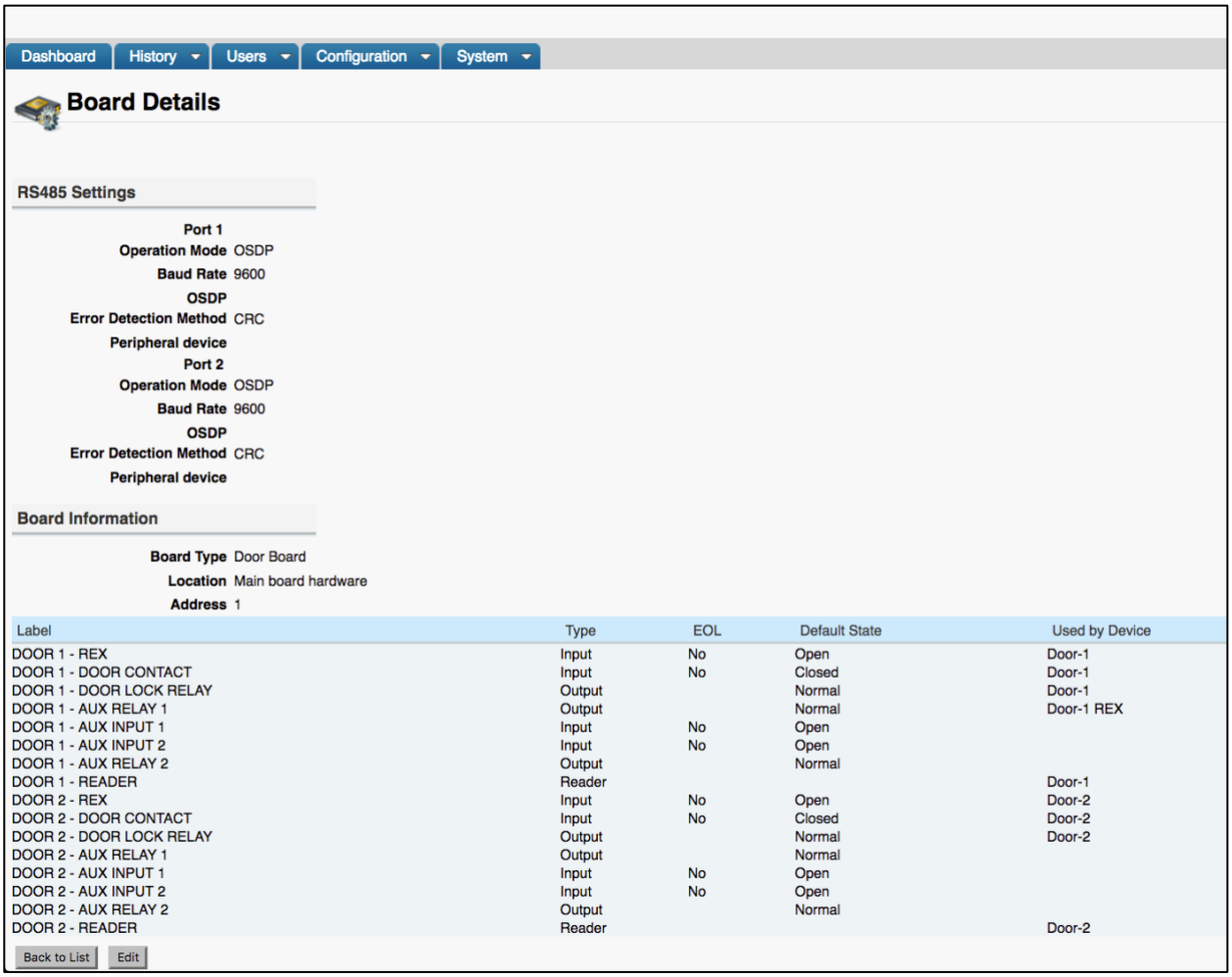

Figure 46. View Board Details: Door Board

Details displayed include:

- **RS485 Settings.** Port 1 and Port 2 list:
  - Operation Mode - Port 1 and Port 2 are set to OSDP Reader.
  - 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.

All Administrators can:

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

Administrators with read/write access can:

- Click **Add New Board** to access a blank Add New Board page in order to create a new control board.
- Click **Edit** to access the Edit Board page to make changes to this control board.
- Click **Delete** to delete any control board other than the Main Board.

NOTE:

*Since the Main Board cannot be deleted, the **Delete** button does not appear on the corresponding Board Details page.*

Adding Control Boards

Only System Account Administrators with read/write access can add a control board.

To add a control board to an account:

1. From the **Configuration** dropdown menu, click the **Hardware** tab then click the **Hardware** tab. The Hardware page displays.
2. Click **Add New Board**. The Add New Board page displays.

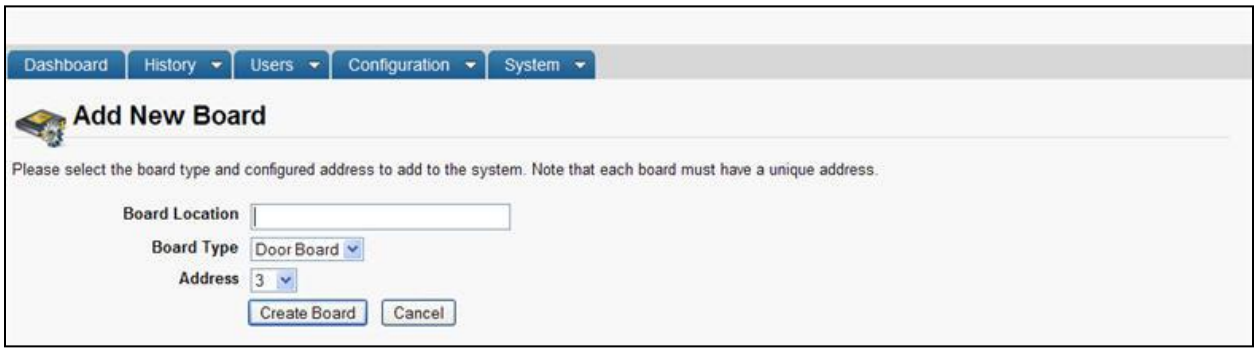

Figure 47. Add New Board

3. Select the correct **Board Type** from the dropdown list.
4. In the **Board Location** field, enter a brief description of the board's location, such as "Server Room."
5. 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 Onsite 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.*

6. Click **Create Board**. The Edit Board Details page displays.

Managing Control Boards

Once the control board is created, you must configure it on the Edit Board Details page. You are taken to this page automatically when you first add the board to an account. After that, you can return to this page at any time to update the board's settings.

Only System Account Administrators with read/write access can configure or delete control boards.

To edit a Door Board:

1. From the **Configuration** dropdown menu, click the **Hardware** tab then click the **Hardware** tab. The Hardware page displays.
2. Click the Door Board you want to edit. The corresponding Board Details page displays.
3. Click **Edit**. The Edit Board Details page displays.

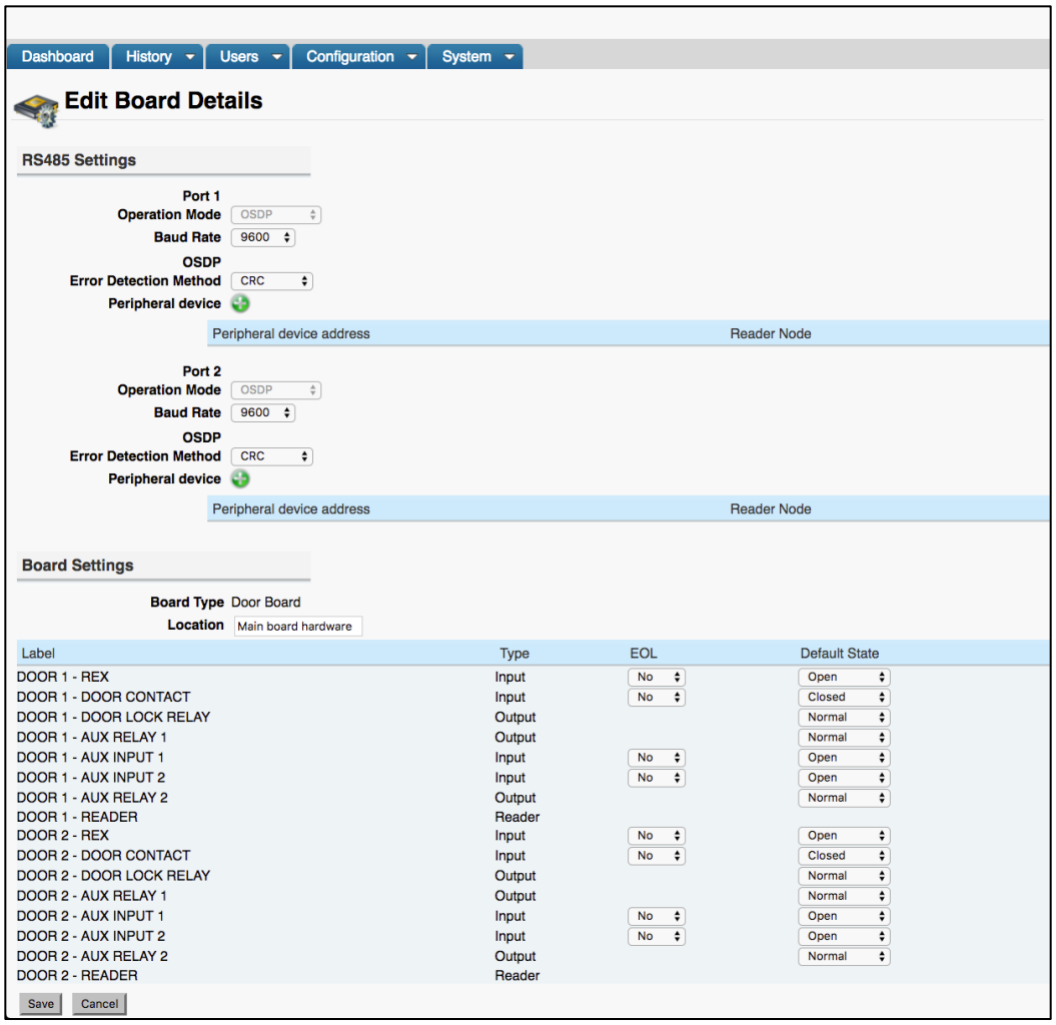

Figure 48. Define Door Board Settings

4. **For Brivo Onsite main panels only**, the RS485 settings are set to OSDP for Port 1 and Port 2. To change any RS485 settings, click Edit at the bottom of the Board Details page. Details of RS485 functionality can be found in the Viewing Board Details section above.
5. The **Location** field 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. Click **Save**. The Board Details page displays.

To edit an IO Board:

1. From the **Configuration** dropdown menu, click the **Hardware** tab then click the **Hardware** tab. The Hardware page displays.
2. Click the IO Board you want to edit. The corresponding Board Details page displays.
3. Click **Edit**. The Edit Board Details displays.

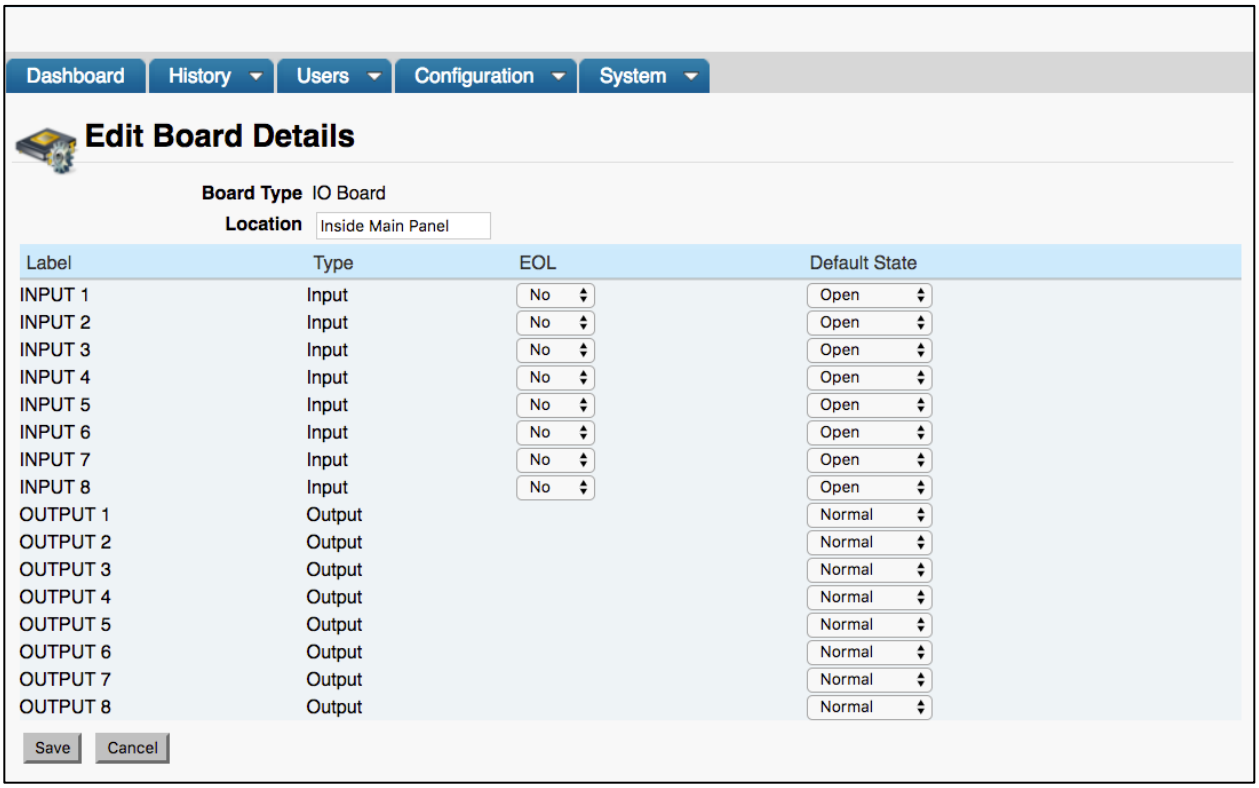

Figure 49. Define IO Board Settings

4. 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.
5. For each input device (**INPUT 1** - **INPUT 8**), 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.

6. For each output point **(OUTPUT 1 – OUTPUT 8)**, there is a set of fields used to define the operation of the associated terminals.
    - In the **Default State** field, click **Norma**l to indicate 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 with Brivo Onsite:

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.

7. Click **Save**. The Board Details page displays.

To delete a control board:

1. From the **Configuration** dropdown menu, click the **Hardware** tab then click the **Hardware** tab. The Hardware page displays.
2. Click the control board you wish to delete. The corresponding Board Details page displays.
3. Click **Delete**. A message displays warning that this operation cannot be undone.
4. Click **OK** to complete the deletion and return to the **Hardware** 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.

9. Antipassback

What is 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.

Configuring Antipassback

Antipassback controls whether or not groups are permitted to enter or exit a particular door at any given time. With these controls come the following options: Hard Antipassback, Soft Antipassback, Antipassback Reset Interval and Antipassback Reset Time.

Hard Antipassback

Hard Antipassback controls keep users in groups from using their card to enter the premises if they are already inside, or exiting if they are already outside. With Hard Antipassback implemented, once a user presents his credential, Onsite recognizes his entry and will not allow the user to re-enter unless he first exits.

Soft Antipassback

The **Antipassback Reset Interval** offers the ability to determine a time interval prevents a user who enters or exits from doing so again before a period of time elapses. After elapsed interval, the user is free to enter or exit.

The **Antipassback Reset Time** refers to the option where a group's status as inside or outside the Antipassback Zone is automatically reset to being outside at a specific time of day, with the ability to enter the time on a 24-hour clock with fifteen minute detail.

Important Antipassback Considerations:

The panel's firmware must be at least version 1.2.0 in order to configure Antipassback settings.

The maximum number of doors that can be configured for Antipassback is 30, either with one ingress and one egress or with one ingress configured along with an antipassback reset interval.

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

If you wish for only one individual to have immunity to Antipassback controls, create a group with only one user—the user you wish to have immunity. Then check the box **Immunity**.

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.

All Administrators can:

- View groups to determine antipassback immunity or antipassback auto reset time.

Administrators with read/write access can:

- Set doors to ingress or egress readers as well as setting up alternate readers.
- Set the Antipassback Reset Interval.
- Set Group immunity to antipassback and set Auto Reset Time for antipassback.

Managing Antipassback Controls

To configure controls for Antipassback Reset Interval:

1. From the **Configuration** dropdown menu, click on the **Hardware** tab then click on the **Antipassback** tab. The Antipassback page displays.

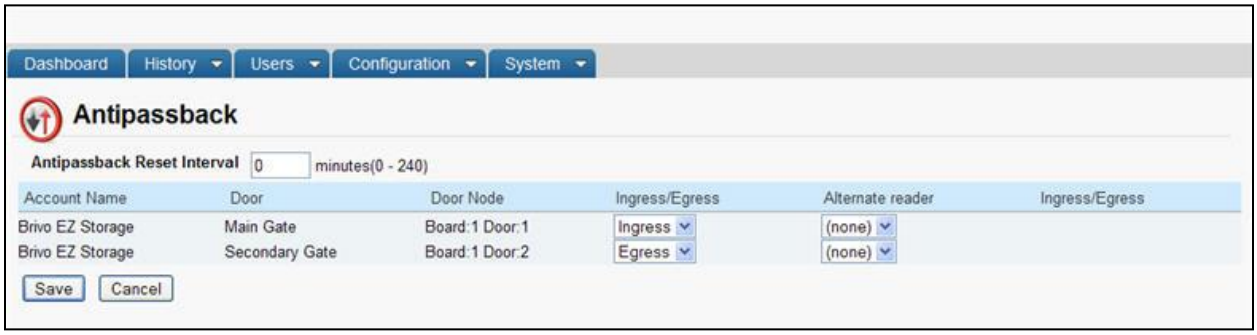

Figure 50. Antipassback Reset Interval

2. The Antipassback page displays information regarding the panel's doors, nodes, and alternate readers, and allows you to choose whether you would like to configure the door as an ingress or egress.
3. Enter the number of minutes from 0 to 240 for the Antipassback Reset Interval.
4. Select whether from the drop down list whether you wish to configure Antipassback controls for the door as an ingress, egress, or neither.
5. If you would like the door to be controlled by two readers, you may configure Antipassback controls for an alternate reader by selecting a board from the Alternate Reader dropdown list.
6. Click **Save**. You are returned to the panel details page.

To configure Antipassback Reset Time:

1. From the **Users** dropdown menu, click the **Groups** tab. The group directory displays.
2. Click the group for which you wish to configure the Antipassback Reset Time. The page displays the group details.
3. Click **Edit** at the bottom of the group details list. The Edit Privileges page displays.
4. If you would like the group to remain immune from the Antipassback controls, check the **Immunity** box underneath the Antipassback title. If you would like for only a particular user to remain immune from Antipassback controls, you may create a group containing just that particular user.

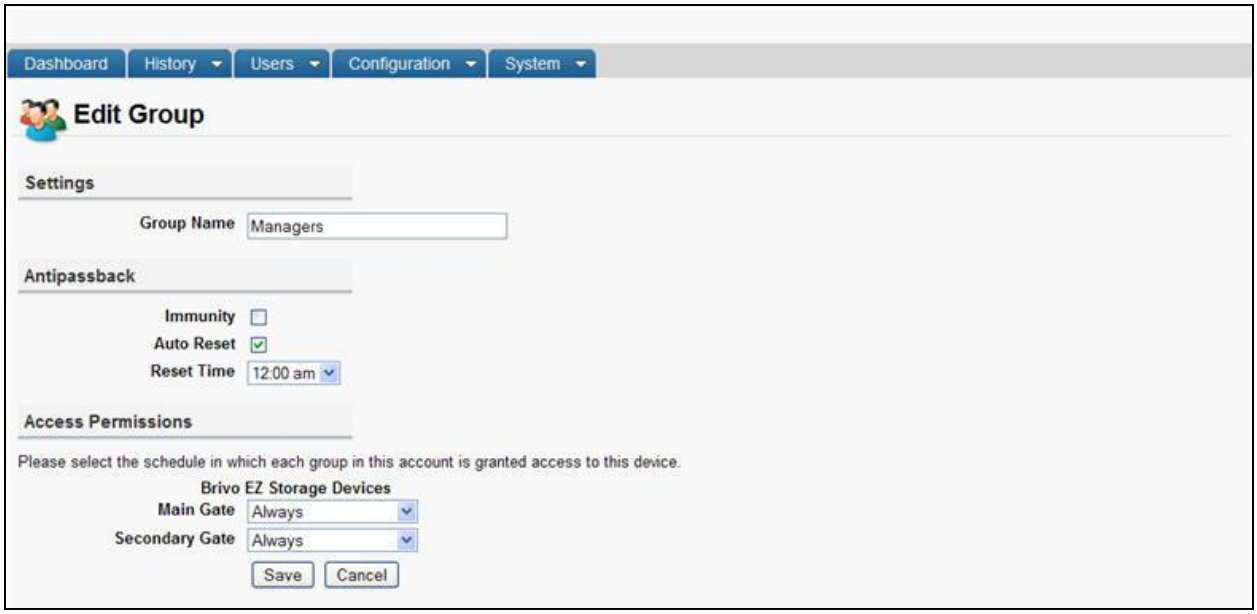

Figure 51. Antipassback Reset Time

5. To select an Antipassback Reset Time, check the **Auto Reset** checkbox. Below that, select a **Reset Time** from the dropdown list for the time that you would like the Antipassback controls to be reset.
6. Click **Save**. You are returned to the group details page.

10. 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 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.

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 Managing Devices.)

What are Holidays?

An observed holiday is a specific day 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 on that day.

Browsing the Schedules List

The Schedules list displays a list of all schedules currently defined for the account.

Account Administrators can view the schedules associated with their own accounts.

To view the list of schedules:

1. From the **Configuration** dropdown menu, click on the **Scheduling** tab then click on the **Schedules** tab. The Schedules list displays.

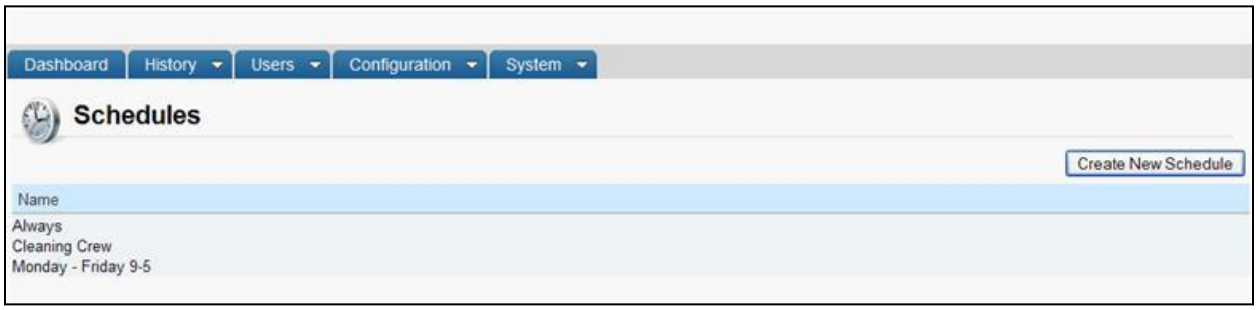

Figure 52. View Schedules List

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".

All Administrators can:

- Click a schedule to access the corresponding Schedule Details page.

Administrators with read/write access can:

- Click **Create New Schedule** to access a blank Edit Schedule page in order to define a new schedule.

Viewing Schedule Details

All Administrators 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. From the **Configuration** dropdown menu, click on the **Scheduling** tab then click on the **Schedules** tab. The Schedules list displays.
2. Click the schedule you want to view. The corresponding Schedule Details page displays.

Figure 53. 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.

All Administrators 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.

Administrators with read/write access can:

- 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 read/write access can create new schedules.

To create a schedule:

1. From the **Configuration** dropdown menu, click on the **Scheduling** tab then click on the **Schedules** tab. The Schedules list displays.
2. Click **Create New Schedule**. The Edit Schedule page displays with blank fields.

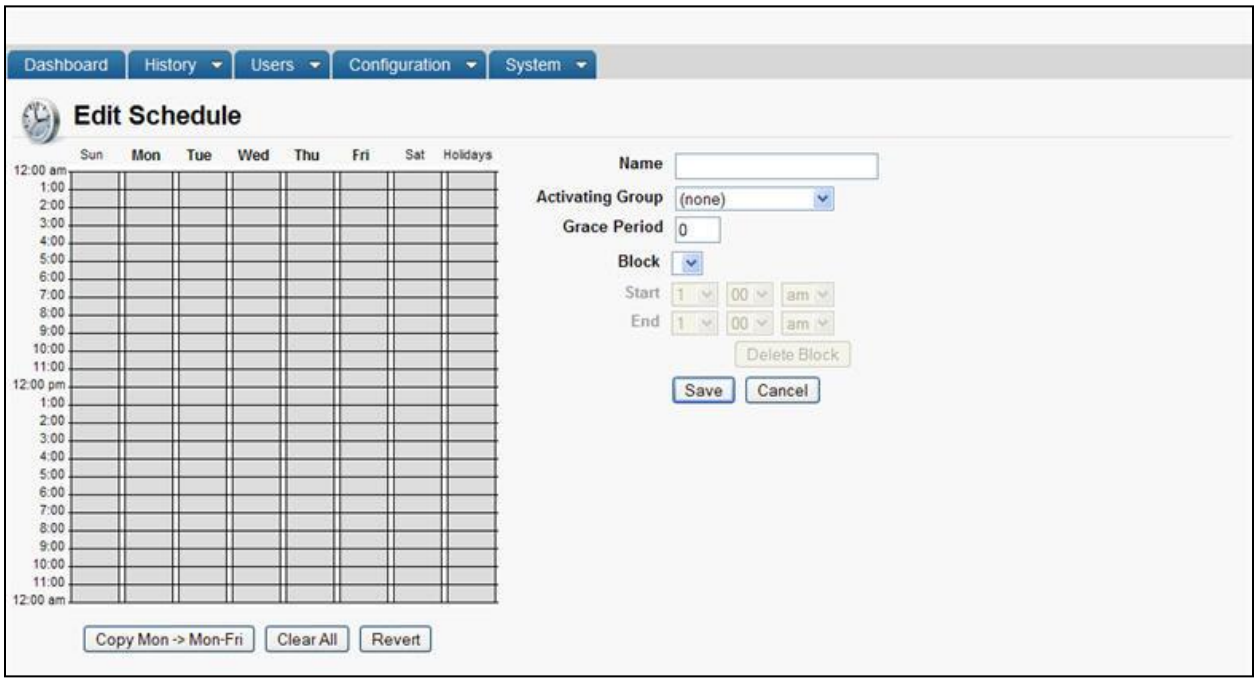

Figure 54. Create New Schedule

3. Enter a brief, descriptive **Name** for the schedule, such as "Night Shift" or "Cleaning Crew."
4. If this is a Group Enabled Schedule, select the **Activating Group** from the drop-down list and enter an associated **Grace Period**. Please refer to the section *Creating a Group* before assigning an activating group to any schedule,

	**WARNING: Group Enabled Schedules** Group Enabled Schedules support the Brivo Onsite 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 *Creating a Group Enabled Schedule* before assigning an activating group to any schedule.

5. 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.

a. 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.

b. 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.

c. 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.

d. To repeat an access period for the work week, fill in the Monday column, and then click **Copy Mon -> Mon-Fri**.

e. To clear all active blocks, click **Clear All**.

f. To revert to the most recently saved settings, click **Revert**.

6. 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.*

7. Click **Save**. The Schedule Details page displays. This schedule can now be used to define access permissions and to control devices.

Managing Schedules

System Account Administrators with read/write access can edit and delete all schedules associated with an account.

To edit an existing schedule:

1. From the **Configuration** dropdown menu, click on the **Scheduling** tab then click on the **Schedules** tab. The Schedules list displays.
2. Click the schedule you want to edit. The corresponding Schedule Detail page displays.
3. Click **Edit**. The Edit Schedule page displays.

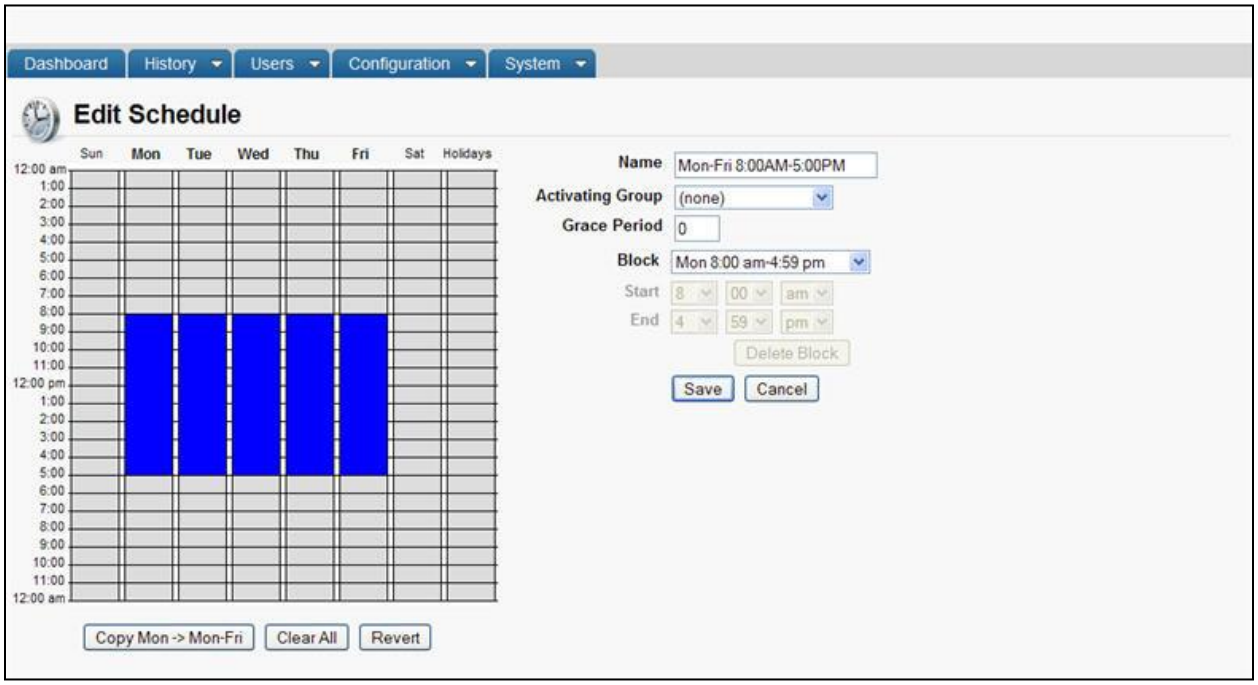

Figure 55. Edit Schedule

4. Edit the schedule according to the preceding guidelines for *Creating a Schedule*.
5. Click **Save**. You are returned to the Schedule detail page.

To delete a schedule:

1. From the **Configuration** dropdown menu, click on the **Scheduling** tab then click on the **Schedules** tab. The Schedules list displays.
2. Click the name of the schedule you wish to delete. The corresponding Schedule Detail page displays
3. Click **Delete**. A confirmation prompt displays.
4. 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.

Account Administrators can view the holidays associated with their own accounts.

To view the list of holidays:

1. From the **Configuration** dropdown menu, click on the **Scheduling** tab then click on the **Holidays** tab. The Holidays list displays.

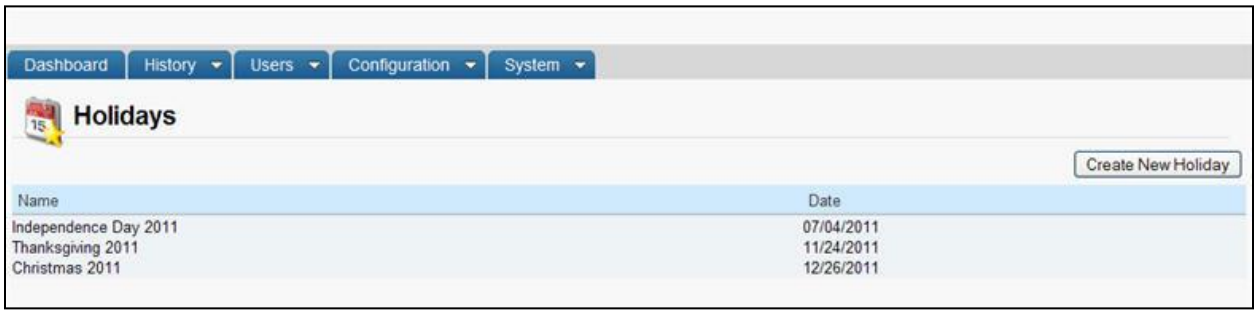

Figure 56. View Holidays List

Details displayed include:

- **Name**. The name of the holiday. Holidays are listed in chronological rather than alphabetical order.
- **Date**. The calendar date on which this holiday is to be observed. On this date, all schedules will operate according to their **Holidays** hours, as indicated on the Schedule Details page.

Administrators with read/write access 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 read/write access can create new holidays.

To create a holiday:

1. From the **Configuration** dropdown menu, click on the **Scheduling** tab then click on the **Holidays** tab. The Holidays list displays.
2. Click **Create New Holiday**. The Edit Holiday page displays.

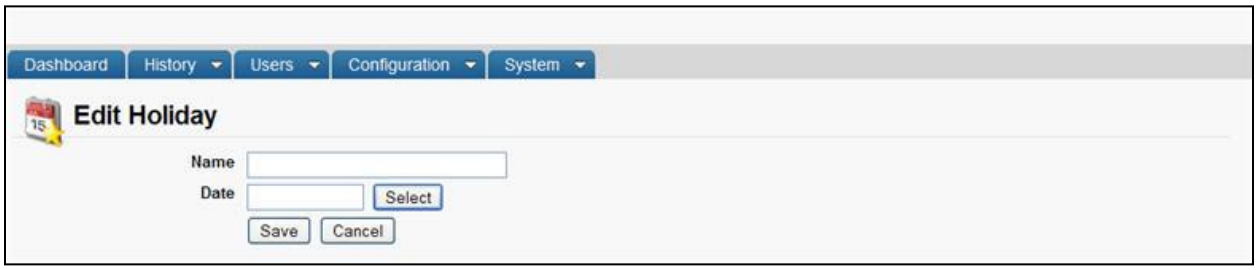

Figure 57. Create a Holiday

3. Enter a brief, meaningful **Name** for the holiday, such as "Memorial Day."
4. Click anywhere in the **Date** field or click **Select** to open a pop-up calendar and select the date on which this holiday should be observed.

NOTE:

You can select only one date per holiday. So, for example, to give employees two days off for Thanksgiving you would have to create one holiday each for "Thanksgiving Day" and "Thanksgiving Friday."

Also, a holiday is active for one day only. You must redefine holidays at the beginning of each calendar year.

5. Click **Save**. The Holidays page displays with the new holiday listed.

Managing Holidays

Administrators with read/write access can edit or delete a holiday.

To edit a holiday:

1. From the **Configuration** dropdown menu, click on the **Scheduling** tab then click on the **Holidays** tab. The Holidays list displays.
2. Click the name of the holiday you want to edit. The corresponding Edit Holiday page displays.

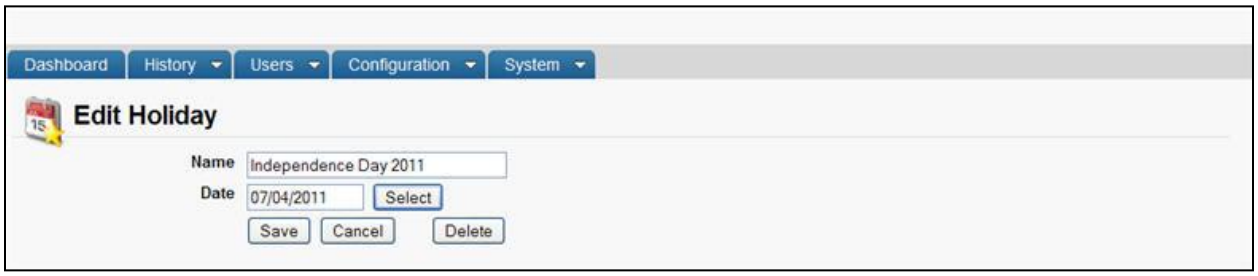

Figure 58. Edit a Holiday

3. Update the **Name** and **Date** fields according to the preceding guidelines for *Creating a Holiday*.
4. Click **Save**. You are returned to the Holidays list with the changes reflected.

To delete a holiday:

1. From the **Configuration** dropdown menu, click on the **Scheduling** tab then click on the **Holidays** tab. The Holidays list displays.
2. Click the holiday you want to delete. The corresponding Edit Holiday page displays.
3. Click **Delete**. A message displays warning that this operation cannot be undone.
4. 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.

11. Accounts

What is an Account?

An *account* is essentially a "span of control." With Brivo Onsite, there is usually only one account, the System Account. This is the account that manages the overall facility at which the Brivo Onsite control panel 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:

Administrators of the System Account have access to all Tenant Account data. All System Account Administrators can view all Tenant Account information; those with read/write access can create, edit, and delete data.

Defining a System Account Administrator

An Administrator with read/write privileges 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 Brivo Onsite. If you are plugged into the ADMIN port this address will be http://Onsite.brivo.com.
2. The Log In page displays.

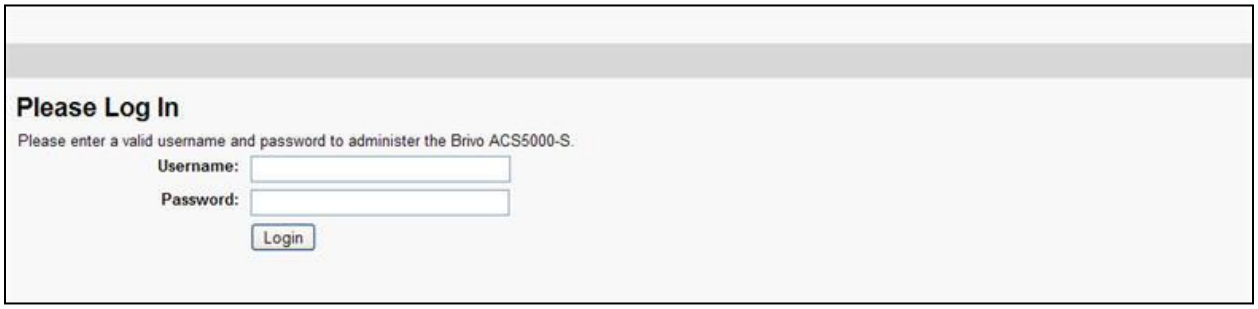

Figure 59. Log In

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

To define a System Account Administrator:

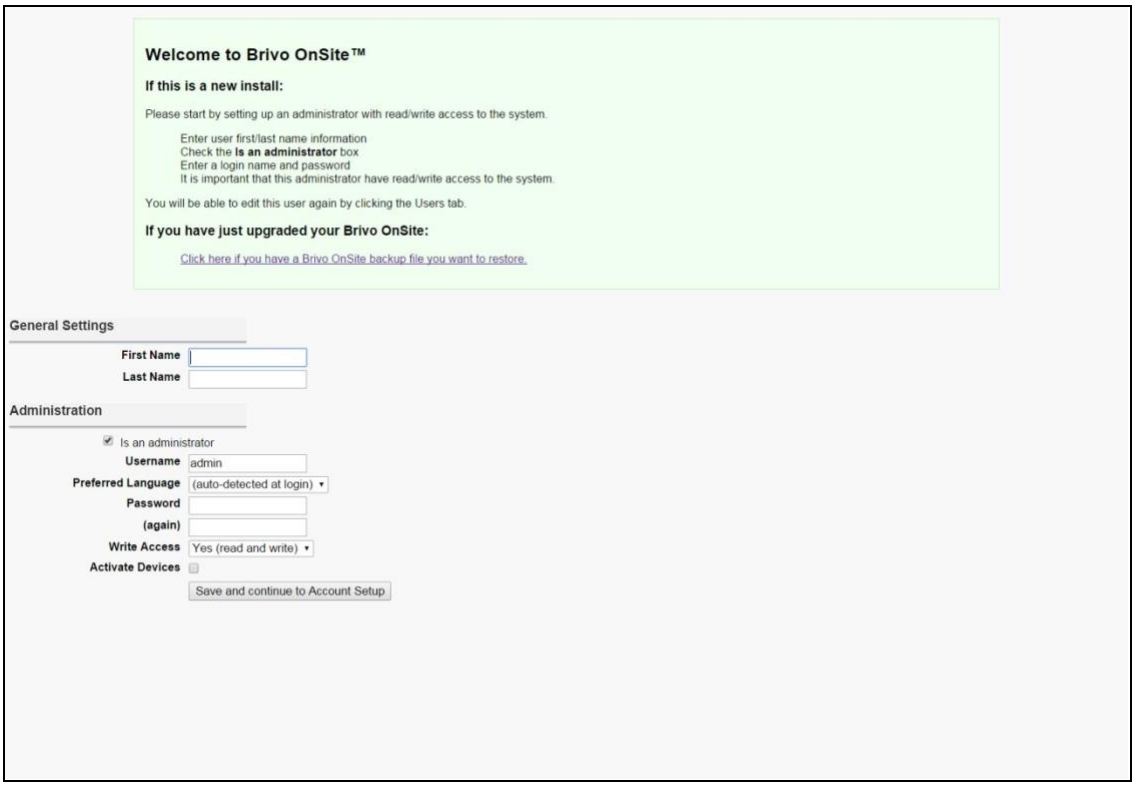

Figure 60. Define System Account Administrator

1. In the **First Name** and **Last Name** fields enter the first and last names of the Administrator for the System Account.
2. The first time you log in to Brivo Onsite, the box for **Is an Administrator** is checked. Do not uncheck it.
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. In the **Password** field, enter a password for the Administrator. Re-enter the exact same password in the **(again)** field. Both of these fields are required.

NOTE:

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

5. The **Write Access** field defaults to **Yes (read and write)**. This allows the Administrator to enter and edit as well as view data. Do not change the value in this field.
6. Click **Save and continue to Account Setup**. The Edit Account Details page displays.

To set up the System Account:

Figure 61. 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 Brivo Onsite 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. Click **Save and Finish Setup**. The System Activity page displays. You are now ready to begin configuring the system. See System Management for further details.

Viewing Account Details

All Administrators 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. From the **Configuration** dropdown menu, click the **Accounts** tab then click the **Account Details** tab.
2. The Account Details page displays.

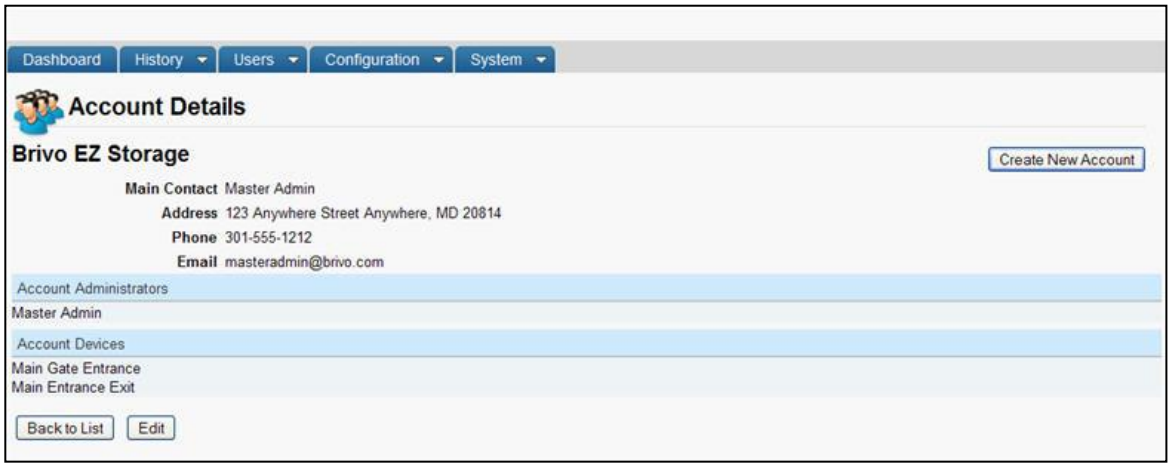

Figure 62. View Account Details

Details displayed include:

- **Main Contact.** The name of the person primarily responsible for the operation of Brivo Onsite 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.
- **Account Administrators.** A list of Administrators for the account--those persons who can view and possibly manage the account data maintained in Brivo Onsite. Click an Administrator's name to access the associated User Details page.
- **Account Devices.** A list of doors and devices associated with the account, as defined on the Edit Devices page. Click a device name to access the associated Device Details page.

All Administrators can:

- Click **Back to List** to return to the Accounts list.

Administrators with read/write access can:

- 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 System Administrators with read/write access can create new Tenant Accounts.

To create a Tenant Account:

1. From the **Configuration** dropdown menu, click the **Accounts** tab then click the **Account Details** tab.
2. Click **Create New Account**. The Edit Account Details page displays with blank fields.

Figure 63. Create Tenant Account

3. 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.
4. In the **Main Contact** field enter the name of the person primarily responsible for managing Brivo Onsite for this account.
5. 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.
6. 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.
7. In the **Email** field enter the email address for the main contact.
8. Click **Save**. The Account Details page displays, and the drop-down list **Active Account** is now visible at the top of the screen and a new menu item **Accounts** is now visible just below the **Account Details** tab.

Figure 64. View Tenant Account Details: No Administrator

NOTE:

You now have a multi-account setup. See the chapter on Tenant Accounts for further details.

9. At the bottom of the page is the message, "There are no administrators created for this account," and you are encouraged to give Administrator permissions to a new or existing user.
10. 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 assigned 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 System Account Administrator with read/write access.

To edit account contact information:

1. From the **Configuration** dropdown menu, click the **Accounts** tab then click the **Account Details** tab.
2. Click **Edit**. The Edit Account Details page displays.

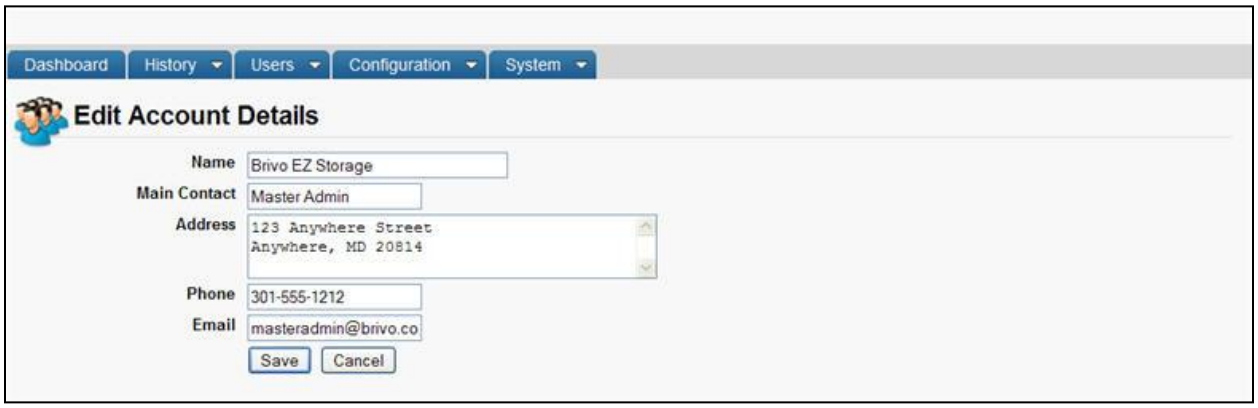

Figure 65. Edit Account Details

3. You can change the account **Name**, but you cannot delete it. This is the only required field on this page.
4. Update the remaining fields according to the procedures for creating tenant accounts.
5. Click **Save**. You are returned to the Account Details page with the updated information displayed.

12. 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 *whom* should be notified about *what* events. Notifications are formatted in plain text.

In order to use the Email Notification function in Brivo Onsite, you must first configure your SMTP Server.

Browsing the Notifications List

Administrators with read/write access can create, edit and delete notification rules, while those with read only access can view notification rules.

To view the Notifications list for a specific account:

1. From the **Configuration** dropdown menu, click the **Accounts** tab then click the **Email Notifications** tab. The Email Notifications page displays.

Figure 66. 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 *Schedules and Holidays* for more information.
- **Details**. The specific door or device at which the event occurred.

Administrators with read/write access 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 read/write access can create notification rules.

To create a notification rule:

1. From the **Configuration** dropdown menu, click the **Accounts** tab then click the **Email Notifications** tab. The Email Notifications page displays.
2. Click **Create New Rule**. The Edit Notification page displays with all the fields blank.

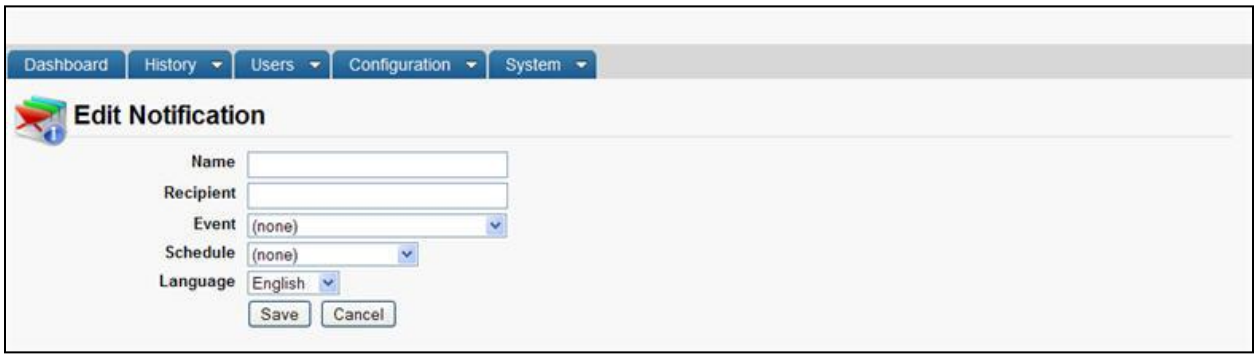

Figure 67. Create Notification Rule

3. Enter a brief, descriptive **Name** for the rule, such as "Lobby Door Ajar."
4. In the **Recipient** field, enter the email address of the individual to receive the email notification. Enter only one email address in this field.
5. From the drop-down list, select the **Event** for which you want a notification sent.
6. 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.
7. For some event types, you will need to specify a **Device**, a **User**, or a **Group**.
8. From the **Language** drop-down list select a language for the email message.
9. 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 read/write access.

To edit a notification rule:

1. From the **Configuration** dropdown menu, click the **Accounts** tab then click the **Email Notifications** tab. The Email Notifications page displays.
2. Click anywhere on the line of information for the rule you want to edit. The corresponding Edit Notification page displays.

Figure 68. Edit Email Notification Rule

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

To delete a rule:

1. From the **Configuration** dropdown menu, click the **Accounts** tab then click the **Email Notifications** tab. The Email Notifications page displays.
2. Click the name of the notification rule you wish to delete. The corresponding Edit Notification page displays.
3. 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 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

Door Locked or Unlocked on Schedule

Subject: Door unlocked on schedule
To: jack@acme.com

Door unlocked on schedule
When: Mon Mar 20 09:00:00 2006
Device: Acme Megaplex Side 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

13. System Management

The **System** tab only displays when you log in as an Administrator of the System Account. Tenant Account Administrators have no access to this section of Brivo Onsite. This is because, to a large extent, the System section deals with the configuration and networking aspects of the Brivo Onsite hardware.

Browsing the System Status

The System Status page displays automatically when you first click the **System** tab in Brivo Onsite. Since no actions can be performed on this display-only page, all System Account Administrators can access it.

To view the current system status for your Brivo Onsite control panel:

1. From the **System** dropdown menu, click on the **System Status** tab. The System Status page displays.

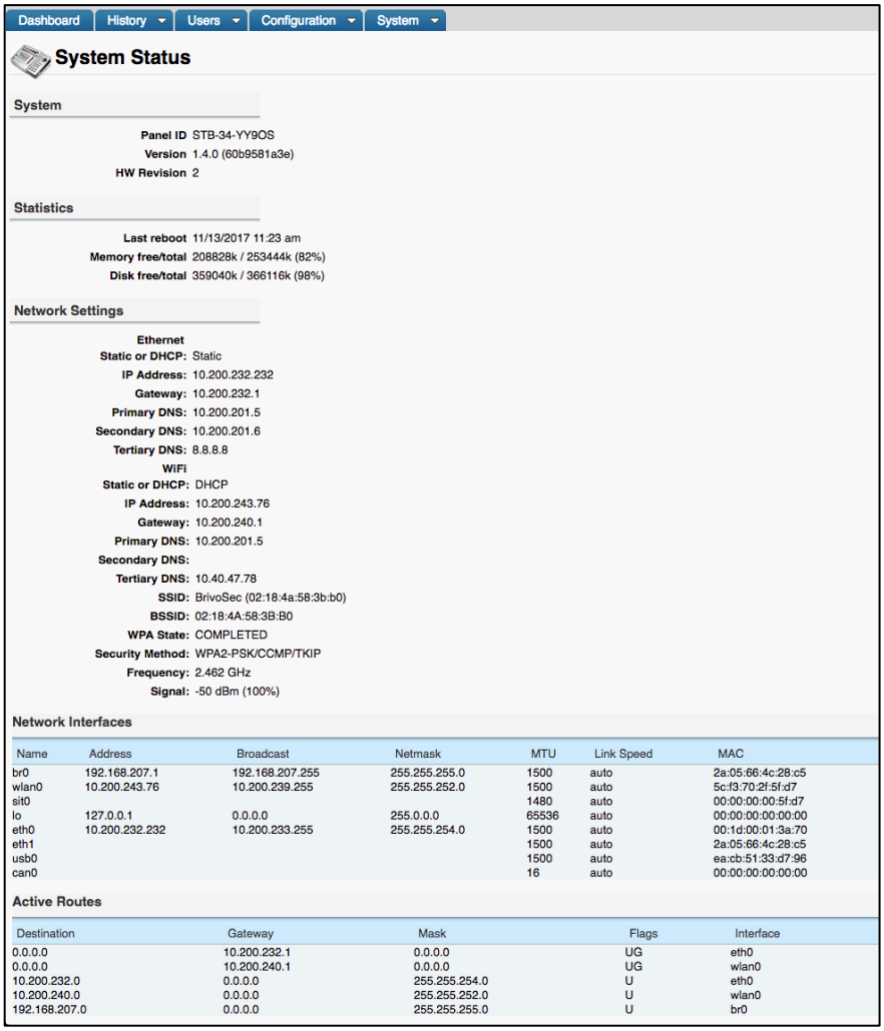

Figure 69. View System Status

Details displayed include:

System

- **Panel ID.** The CP number of the panel.
- **Version**. The version of Brivo Onsite currently being run.
- **HW Revision**. The current revision of hardware of the control panel.

Statistics

- **Last reboot**. The date and time at which the Brivo Onsite control panel was last rebooted.
- **Memory free/total**. The amount of free memory compared to total memory on the machine running Brivo Onsite.
- **Disk free/total**. The amount of free disk space compared to the total disk space.

Network Settings (Ethernet)

- **Static or DHCP**. Indicates whether the network settings on this Brivo Onsite control panel were set by an automatic network service (**DHCP**) or set manually (**Static**).
- **IP Address**. The IP address of the Brivo Onsite control panel, 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 Brivo Onsite control panel 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 Settings (WiFi)

- **Static or DHCP**. Indicates whether the wireless network settings on this Brivo Onsite control panel were set by an automatic network service (**DHCP**) or set manually (**Static**).
- **IP Address**. The IP address of the Brivo Onsite control panel, 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**. This tells the Brivo Onsite control panel 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.
- **SSID**. Service Set Identifier is the primary name associated with a wireless local area network (WLAN)
- **BSSID**. Basic Service Set Identifier is the MAC address of the control panel on the wireless local area network.
- **WPA State, Security Method, Frequency,** and **Signal**. These fields will automatically populate from information provided by your wireless network.

Network Interfaces

- **Name**. A list of interfaces currently in use.
  - **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.

  - **eth1**. The interface available via the ADMIN interface on the panel. This maintains a hardwired address as well as a small set of system services to make plugging directly into the Brivo Onsite control panel for administration. This is generally only necessary at system installation, to provide initial network settings.

- **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.
- **Link Speed**. Speed at which a network interface is operating.
- **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**. A mask of the address range covered by the routing rule.
- **Interface**. Routing specific flag values.

Browsing the System Logs

The System Logs page provides access to three different views of the system log:

- **Application**. Lists only application output.
- **System**. Lists all system operations
- **Kernel**. Lists only operations related to the system kernel.

All System Account Administrators can access this page.

To view a system log:

1. From the **System** dropdown menu, click on the **System Logs** tab. The System Logs page displays.

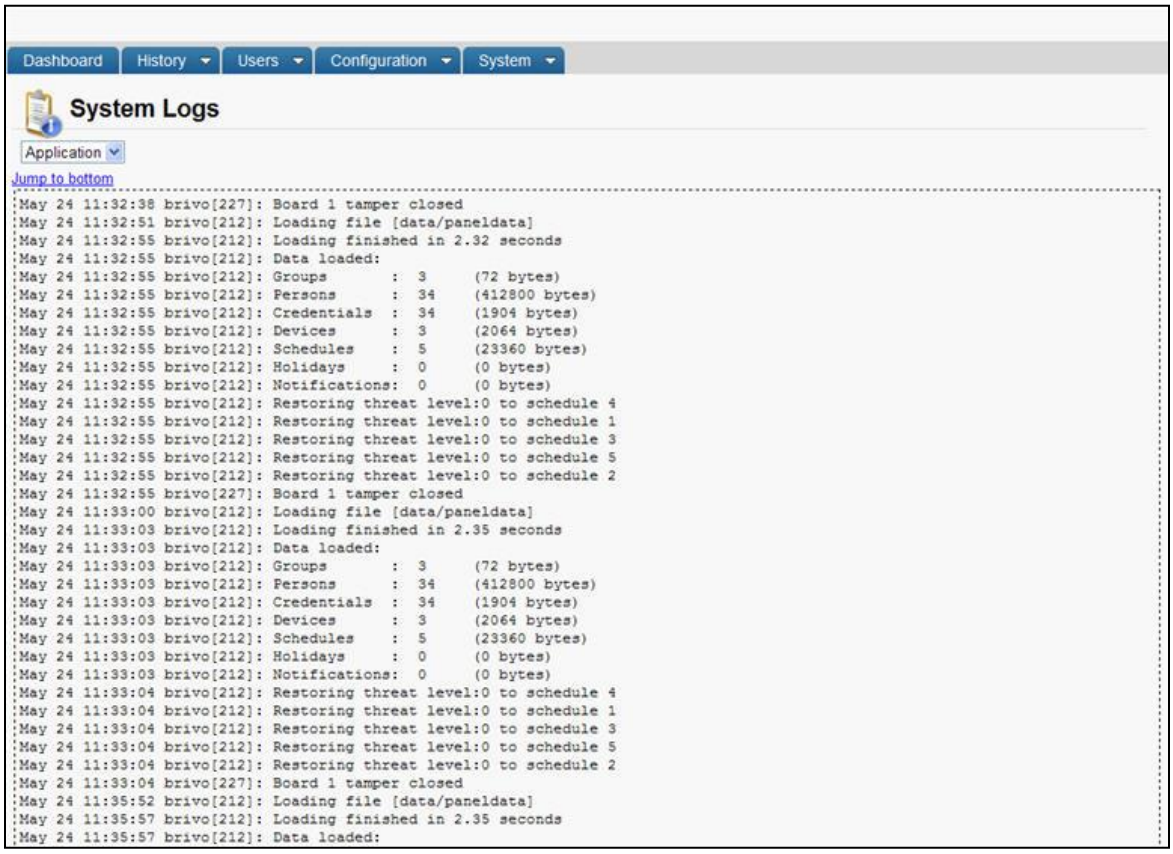

Figure 70. View System Log: Application

All Administrators 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 Tools

Brivo Onsite provides access to basic system commands via the Tools page in the System section.

All System Account Administrators can access on enter commands on the Tools page.

To use the tools:

1. From the **System** dropdown menu, click on the **Tools** tab. The Tools page displays.

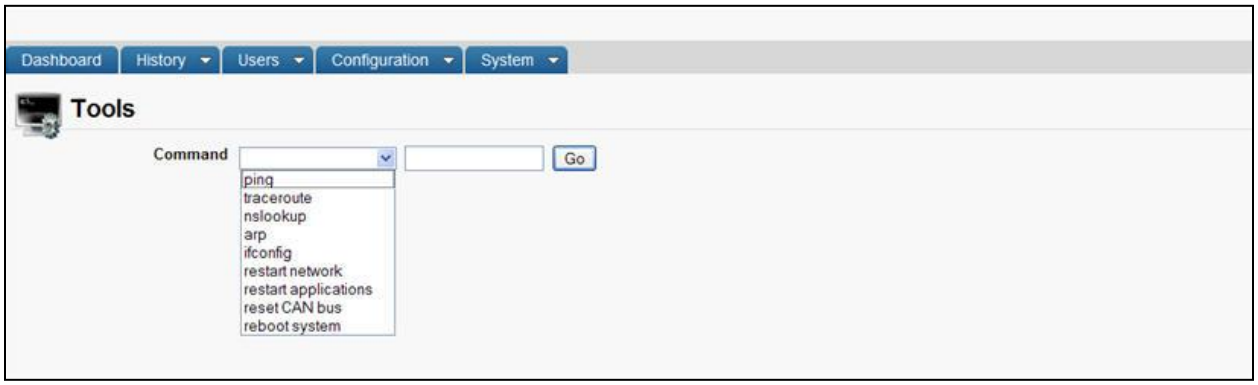

Figure 71. Enter System Command (Drop-Down List Displayed)

All Administrators can:

- Select a **Command** from the drop-down list.
- Enter a parameter for that command in the adjoining data entry field, excluding restart network, restart applications, reset CAN bus, and reboot system.
- Click **Go** to activate the command.

All Administrators with read/write permissions can:

- Enter a parameter for any command in the adjoining data entry field.

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 network**. Reinitializes the network layer, potentially releasing DHCP leases and activating any outstanding changes to network configurations.

WARNING: restart applications

*Generally, you should only use the **restart applications** command when instructed to do so by Brivo Technical Support.*

- **restart applications**. Shuts down the access control software on the control panel, and then restarts it.
- **reset CAN bus.** Locally resets the CAN bus on the control panel.
- **reboot system**. Performs a graceful restart of the Brivo Onsite control panel.

Setting System Date and Time

Brivo Onsite normally synchronizes its system clock via NTP (Network Time Protocol) with servers over the Internet, to ensure accuracy. In case Brivo Onsite cannot reach an external server for time synchronization, such as when a firewall blocks access or the Brivo Onsite control panel is simply not on a network with Internet access, the system time must be set manually by administrators with read/write permissions.

To set the date and time for your system:

1. From the **System** dropdown menu, click on the **System Date/Time** tab. The System Date/Time page displays.

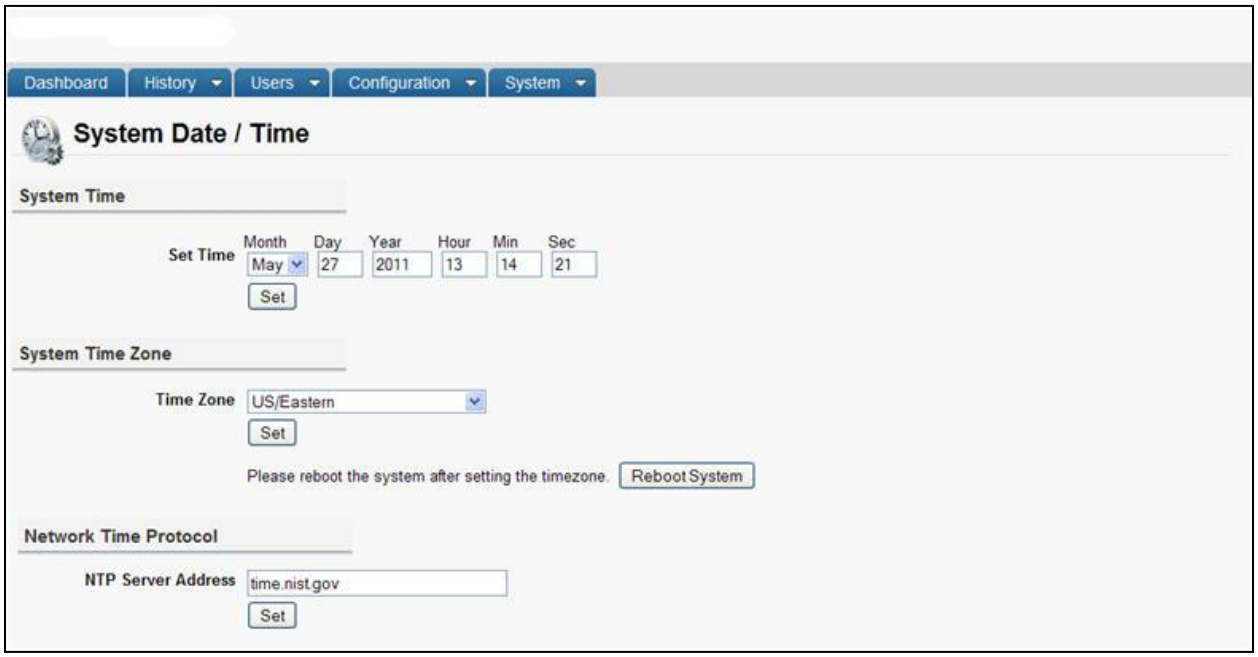

Figure 72. Set System Date and Time

2. 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. Remember to **Reboot System** after changing the timezone.
3. To manually set the **System Time**, enter the current time using the **Set Time** fields, and then click the corresponding **Set** button.
4. The **Network Time Protocol** defaults to time.nist.gov. To set the system to automatically synchronize with a different Internet time server enter the associated **NTP Server Address**, and then click the corresponding **Set** button.

Configuring the Network

You can configure Brivo Onsite to use manually defined (static) network settings, or to use an automatic network service (DHCP).

Only System Account Administrators with read/write access can configure network settings.

To configure your network settings:

1. From the **System** dropdown menu, click on the **Network Configuration** tab. The Network Configuration page displays.

Figure 73. Configure the Network

2. To configure a static network:
    - Enter the **IP Address** of the Brivo Onsite control panel, 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 Brivo Onsite 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.
3. 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 Brivo Onsite may change, forcing you to manually change the URL of the browser through which you are accessing the device.

It is recommended that network configuration changes only be made while connected directly to the ADMIN port of the Brivo Onsite control panel from a laptop.

Configuring WiFi (not available for ACS5000-S panels)

You can configure Brivo Onsite to utilize WiFi functionality.

To configure your WiFi

1. From the **System** dropdown menu, click on the **WiFi Configuration** tab. The WiFi Configuration page displays.

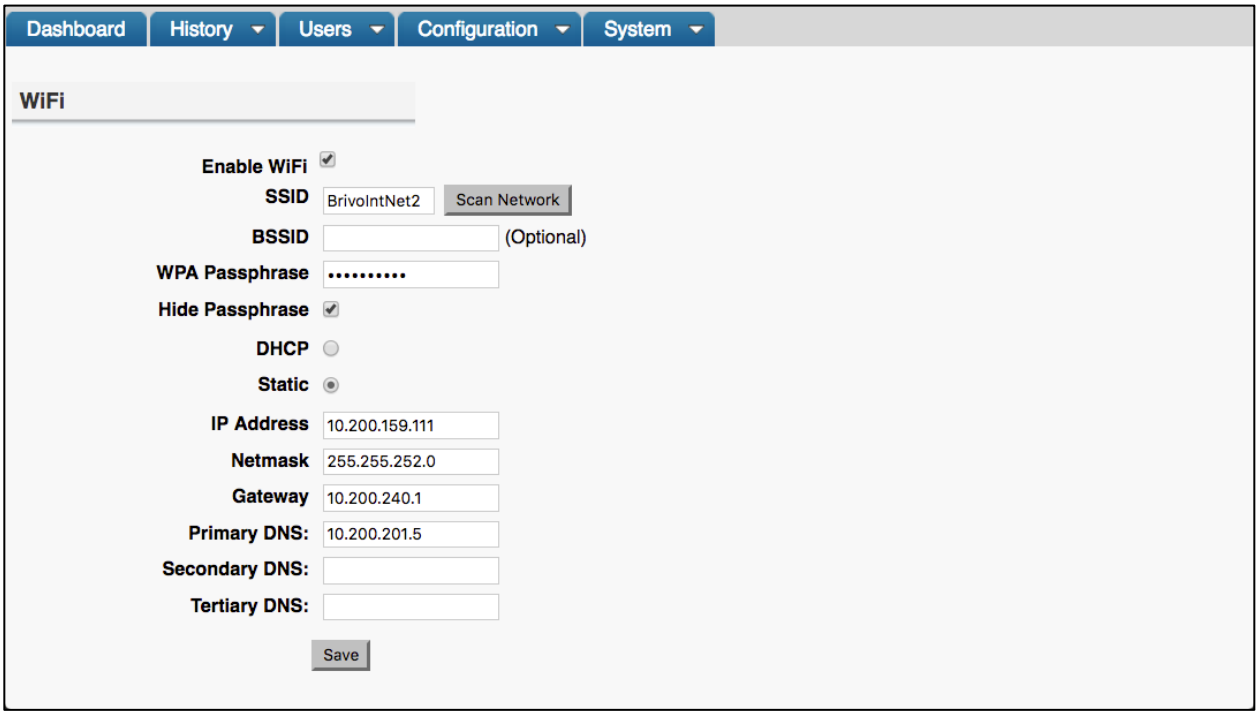

Figure 74. Configure WiFi

2. To configure WiFi:
    - Check the **Enable WiFi** checkbox.
    - Enter the **SSID** of the wireless network to which the Brivo Onsite control panel will be connected.
    - Optionally, click the **Scan Network** button to scan for all available SSIDs which will provide a pop-up window with the available wireless networks. Click the **SSID** to which the Brivo Onsite control panel will be connected. You are returned to the **WiFi** page.
    - Optionally, enter the **BSSID** for the wireless network.
    - Enter the **WPA Passphrase** for the wireless network.
    - If you wish the passphrase to be hidden, make sure the **Hide Passphrase** checkbox is checked.
    - Choose **DHCP** or **Static** for determining the IP address. If you selected **Static**, enter the **IP Address, Netmask, Gateway** and **DNS** information for the wireless network.
3. Click **Save**. The WiFi settings are set.

Configuring Advanced Network Setup

Brivo Onsite defaults to Auto when establishing a link speed between the panel and the network.

1. From the **System** dropdown menu, click on the **Advanced Network Setup** tab. The Advanced Network Setup page displays.

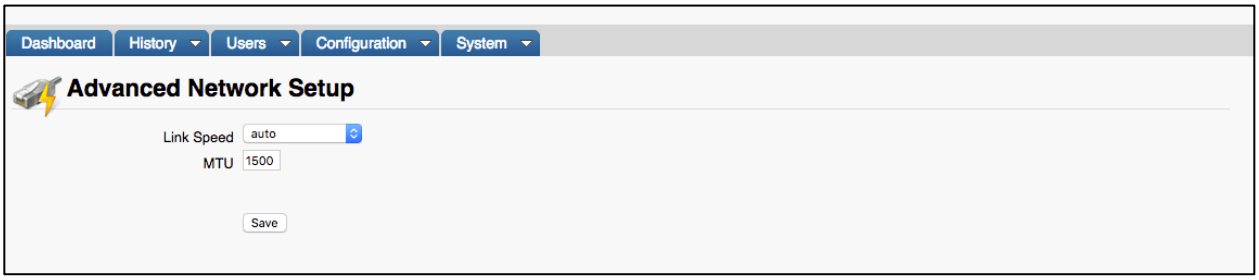

Figure 75. Configure Advanced Network Setup

2. If desired, select a **Link Speed** from the Link Speed dropdown menu. 10Mbs or 100Mbs at either half-duplex (HD) or full-duplex (FD) are available, but the panel will default to Auto.
3. Enter the maximum transmission unit (**MTU**) in the field provided. The MTU is set to 1500 by default.
4. When finished, click **Save**.

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 control panel is installed.

To configure a network route:

1. From the **System** dropdown menu, click on the **Networking Routing** tab. The Network Routing page displays.

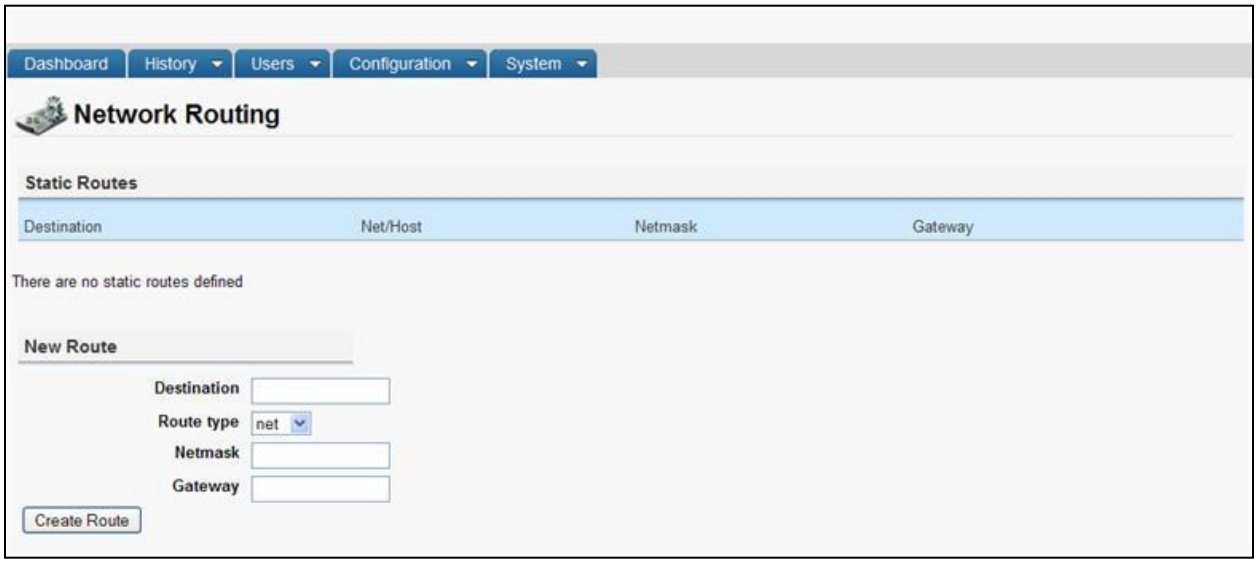

Figure 76. Configure Network Routing

2. On the bottom half of the page, enter a **Destination** IP Address or network.
3. Select a **Route type** from the drop-down list, either **net** or **host**.
4. Enter the **Netmask** address for the static route, a mask used to separate a sub-network of machines; for example, 255.255.255.0
5. 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.
6. 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 function in Brivo Onsite, you must first configure your SMTP Server. SMTP (Simple Mail Transfer Protocol) is how email is sent between machines on the Internet.

Only System Account Administrators with read/write access can configure the SMTP server.

To configure your SMTP server:

1. From the **System** dropdown menu, click on the **SMTP Server Settings** tab. The SMTP Server Settings page displays.

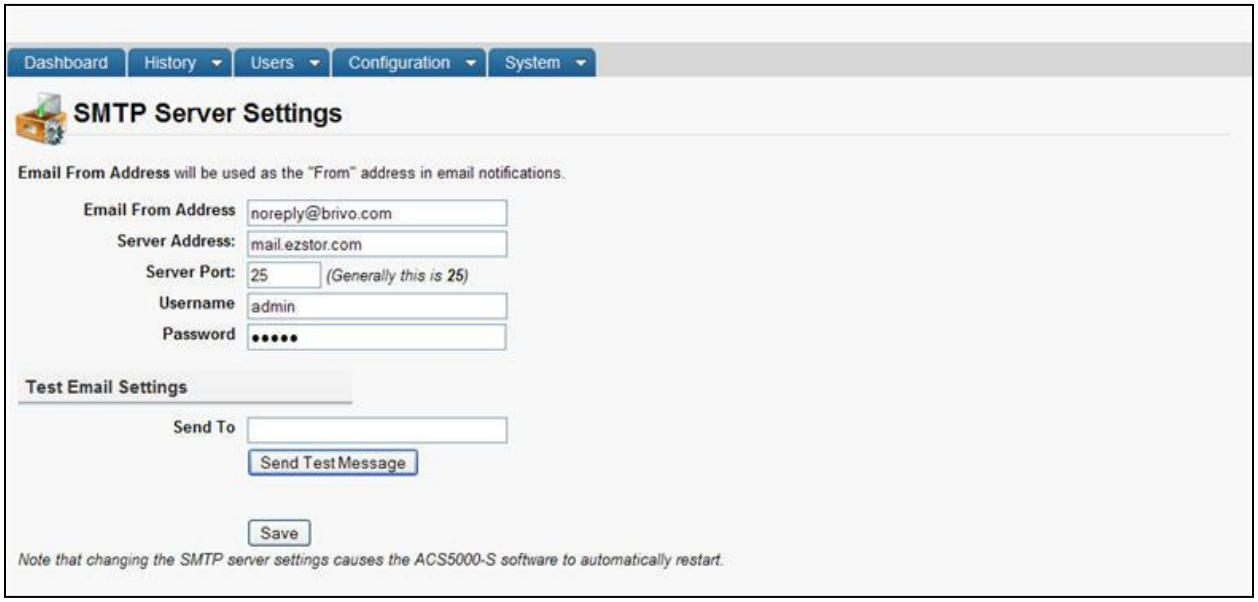

Figure 77. Configure SMTP Server

2. In the **Email From Address** field, enter the email address you would like to appear in the **From** field of email notifications.
3. Enter the address of your SMTP server in the **Server Address** field.
4. Enter the port of your SMTP server in the **Server Port** field. This value is usually 25.
5. 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.
6. Click **Save**. Brivo Onsite internal applications take a moment to restart automatically at this point.

Viewing Hardware Status

The Hardware status page provides a complete view of the state of all major components of the control panel hardware. The page shows the status of each terminal node on each control board.

All System Account Administrators can view this display-only page.

To view the status of your hardware:

1. From the **System** dropdown menu, click on the **Hardware Status** tab. The Hardware Status page displays.

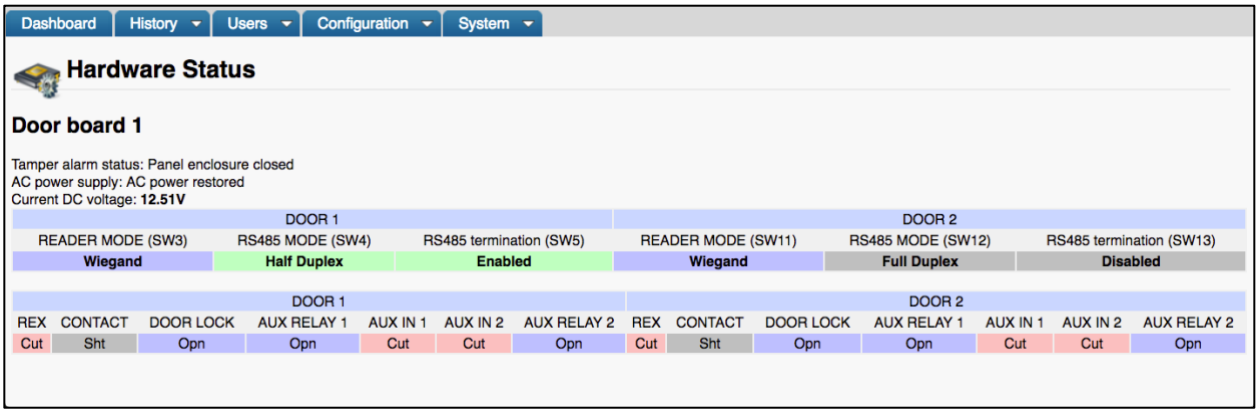

Figure 78. View Hardware Status

Details displayed include:

- **Tamper alarm status**. Indicates the current status of the tamper alarm.
- **AC power supply**. Indicates if the AC power supply for the control board is on or off.
- **Current DC voltage**. Indicates the current voltage of the control panel.
- For Brivo Onsite panels, the first row of **DOOR 1/DOOR 2** indicates the reader mode (Wiegand or OSDP), whether the RS485 is set to half duplex or full duplex, and whether or not the RS485 Termination switch is enabled or disabled.
- The second row (only row if using an ACS5000-S control panel) of **DOOR 1/DOOR 2**. Indicates the raw state of each terminal node on the control board. The names on this page (e.g., **REX**, **CONTACT**, etc.) match the actual node labels. Each node displays a status of **Opn** (Open), **Cut**, **Cls** (Closed) or **Sht** (Short).

NOTE:

*For circuits wired without EOL detection, **Opn** and **Cut** are the same, as are **Cls** and **Sht**.*

Importing User Data

Brivo Onsite provides a mechanism for importing user data from a flat file.

Brivo Onsite supports 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:

- 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

Only System Account Administrators with read/write access can import user data.

To import user data from a flat file:

1. From the **System** dropdown menu, click on the **Import User Data** tab. The Import User Data page displays.

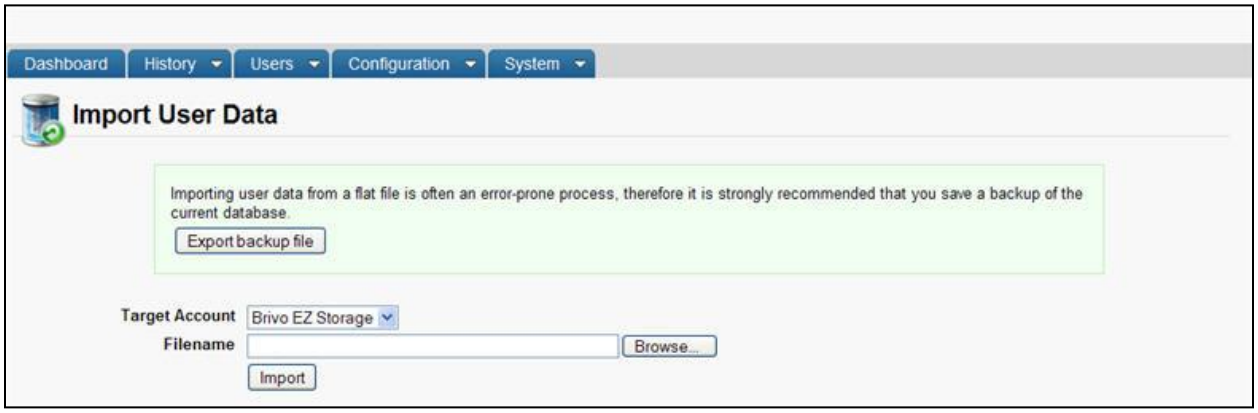

Figure 79. Import User Data, Step One

2. 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.

3. After the database is successfully backed up, select the **Target Account** to which you want to import user data.
4. 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.
5. Click **Import**. If you have entered a valid filename, the second portion of the Import User Data page displays.

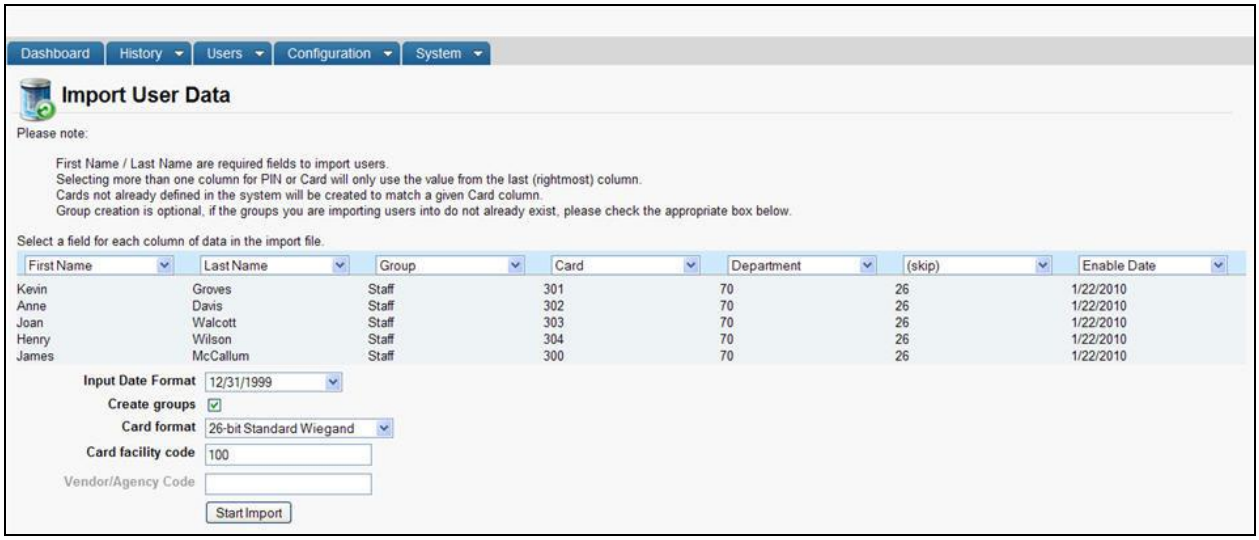

Figure 80. Import User Data, Step Two

6. 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**.
7. From the **Input Date Format** drop-down list, click the date format used in the input file.
8. 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.
9. If you are importing **Card** numbers, click a valid **Card format** from the drop-down list and enter the corresponding **Card facility code**.
10. 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 your Brivo Onsite firmware. Brivo Onsite 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 Brivo Onsite. As a rule, it is strongly recommended that backups be taken, either manually or automatically, to preserve data against unintentional or catastrophic loss.

Note that the backup and restore mechanisms do not restore activity data. Archival of activity is done via the export activity functionality on this page.

Please consult the Brivo Technical Support site (http://www.brivo.com) for more information about automating backups of the account and configuration data, and automating exports of system activity data.

All System Account Administrators can make backups of the system.

To create a backup of your database:

1. From the **System** dropdown menu, click on the **Backup & Restore** tab. The Backup & Restore page displays.

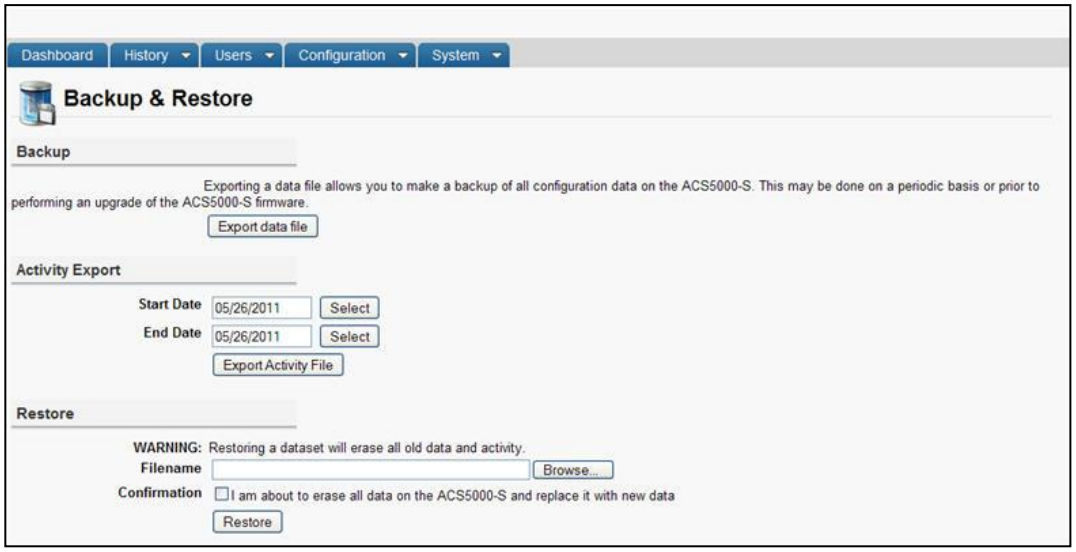

Figure 81. Backup and Restore the Database

2. Click **Export data file** in the **Backup** section of the page. Your operating system guides you through the procedures for saving the backup file.

To export data from the System Activity Log:

1. From the **System** dropdown menu, click on the **Backup & Restore** tab. The Backup & Restore page displays.
2. In the **Activity Export** section, click the **Start Date** field to select from a pop-up calendar the first day of activity you want to include in the log.
3. Click the **End Date** field to select the last day of activity to include.
4. Click **Export activity file**. Your operating system guides you through the procedures for saving the backup log.

To restore a backed up database:

1. From the **System** dropdown menu, click on the **Backup & Restore** tab. The Backup & Restore page displays.
2. 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

When you restore your database file, you completely overwrite *all existing data with the data from the restoration file. Therefore, it is highly recommended that all restore operations be performed via the ADMIN port of the Brivo Onsite control panel as it is possible to import new LAN network settings.*

3. 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 Brivo Onsite panel and replace it with new data.
4. Click **Restore**. The system restore can take a while to complete. Progress is reported along every step of the way.

Upgrading Your Firmware

On occasion, Brivo will issue an upgrade of the Brivo Onsite firmware. All upgrades will be listed on the Brivo website.

This operation is restricted to System Account Administrators with read/write access.

WARNING: Firmware Upgrades

When new firmware is installed, all existing data will be erased. Therefore, it is highly recommended that all upgrade operations be performed via the ADMIN port of the Brivo Onsite control panel as it is possible to lose LAN network settings.

To upgrade your Brivo Onsite firmware:

1. From the **System** dropdown menu, click on the **Upgrade Firmware** tab. The Upgrade Firmware page displays.

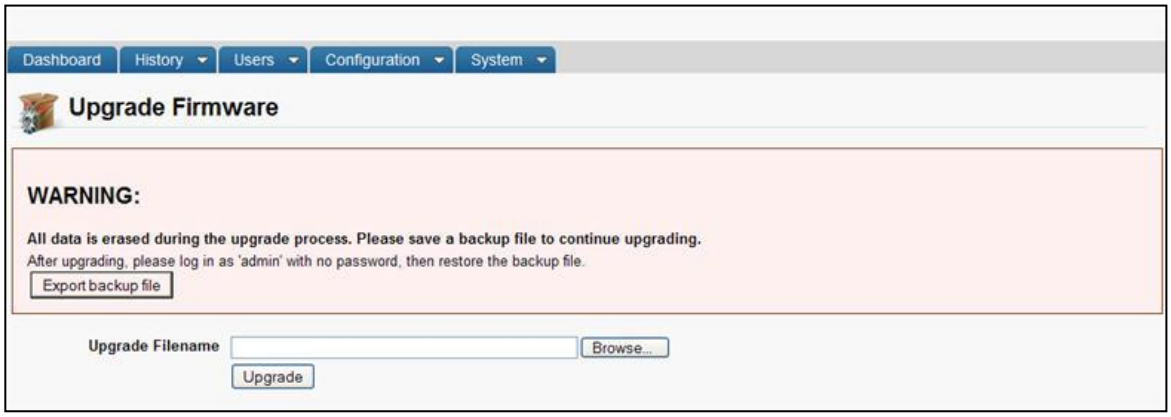

Figure 82. Upgrade System Firmware

2. Create a backup of your current database by clicking **Export backup file**. Your operating system guides you through the procedures for saving the backup.
3. Enter the name of the upgrade file in the **Upgrade Filename** field, or click **Browse** to search your system for the appropriate file
4. To complete the restoration, check the **Confirmation** box that reads I am about to erase all data on the Brivo Onsite control panel and have just made a backup.
5. 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.

6. At the conclusion of the upgrade, necessary system services will restart.

7. Log back into Brivo Onsite and follow instructions above to restore the database.

14. Tenant Accounts

Typically, there will be a single Account defined in Brivo Onsite, the System Account. However, if sections of a facility are leased out, then there may also be one or more Tenant Accounts. 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 System Account Administrators can view Tenant Account information; while those with read/write access can also create, edit, and delete data.

This chapter explains how Brivo Onsite 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 functions for Tenant Account Administrators.

Changes in System Account Administrator Access

For the most part, a System Account Administrator's access to Brivo Onsite 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 dropdown list of each section. This is the **Active Account** drop-down list, 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 83. Active Account Drop-Down List

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** tab 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 drop-down list 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.

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 tab. This is the **Accounts** option, which provides access to the Accounts list, a list of all currently defined Accounts.

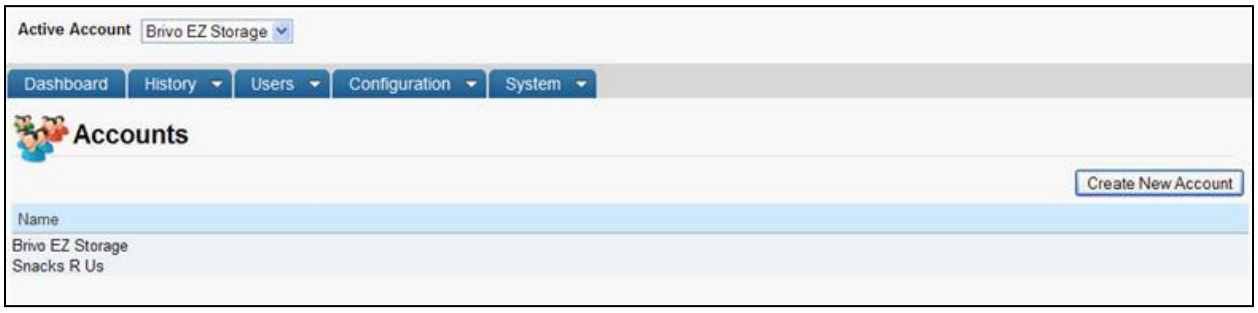

Figure 84. View Accounts List

Operations that can be performed on this page include:

- **Create New Account.** This button appears for System Account Administrators with read/write access. 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. From the **Configuration** dropdown menu, click the **Account** tab then click the **Accounts** tab. The Accounts list displays.
3. Click the Tenant Account you want to delete. The corresponding Account Details page displays.
4. 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.
5. 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. 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. From the **Configuration** dropdown menu, click the **Hardware** tab then click the **Devices** tab. The Devices page displays.
2. 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 85. Share a Door or Valid Credential Device

3. For new devices, follow the procedures in the Managing Devices section for data entry guidelines *not* related to the **Account Visibility** section.
4. 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.
5. 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 read/write access while others have read-only access. This distinction is the same for both types of Account Administrators. In other words, Administrators with read/write privileges can manage (create, edit and delete) the data to which they have access, while Administrators with read-only access can only view the data.

Following is a list of all the ways in which Brivo Onsite 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 read/write access.

Schedules and Holidays

Tenant Account Administrators 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* for more information.
- Cannot create or delete 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.

Antipassback

Tenant Account Administrators:

- Cannot view the Antipassback settings.

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.

Users and Groups

- User and group management is the same for Tenant Administrators and System Administrators.

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.

Email Notifications

- Administration of email notifications is the same for Tenant Administrators and System Administrators.

System Management

- No access to the System tab or any system management pages.

15. 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. Administrators may have 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, System Account
System Account Administrators have access to all data maintained via Brivo Onsite.

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.

Antipassback
Antipassback is a control that 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.

Brivo Onsite
The software interface for the Brivo Onsite control panel.

Card
A proximity card, magnetic stripe card, smart card or similar token issued to a user.

Control Panel
A system consisting of 1-15 control boards: one Main Board and up to 14 Door Boards and/or Input Output Boards. For Brivo Onsite, the ACS5000-S and the newer Brivo Onsite control panels are the two control panel options.

Dashboard
The Dashboard page is the initial system form displayed after logging into Brivo Onsite. The Dashboard provides a two-fold functionality for monitoring and controlling the operation of system devices for authorized Administrators.

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 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.

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.

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, 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.

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."

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

System Activity Log
A record of Access Events, Exception Events, Device Events and Control Panel Events.

Two Factor Credential
A security feature that requires users to provide both forms of credentials, a card and a PIN, at a door 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 groups.

Revision Table	Date	Author	Change
1.3.1	9/13/2017	LMW	Added Brivo Onsite control panel and WiFi configuration instructions
1.4.0	11/9/2017	LMW	Added WiFi scanning, lock-on-open functionality, debounce, fail-open and fail-secure functionality
1.4.0.1	1/18/2018	LMW	Maintenance release addressing minor bug fixes
1.4.0.2	5/15/2018	LMW	**Brivo Onsite Panel Only**, added CAN bus lockup detection logic
1.4.0.3	6/14/2018	LMW	Maintenance release addressing minor bug fixes
1.4.0.4	8/2/2018	LMW	Maintenace release addressing minor bug fixes