ACCENTRA
ASSA ABLOY

Experience a safer
and more open world

Multi-Family Management System

Cloud-Based Software User Guide

Table of Contents

1. INTRODUCTION

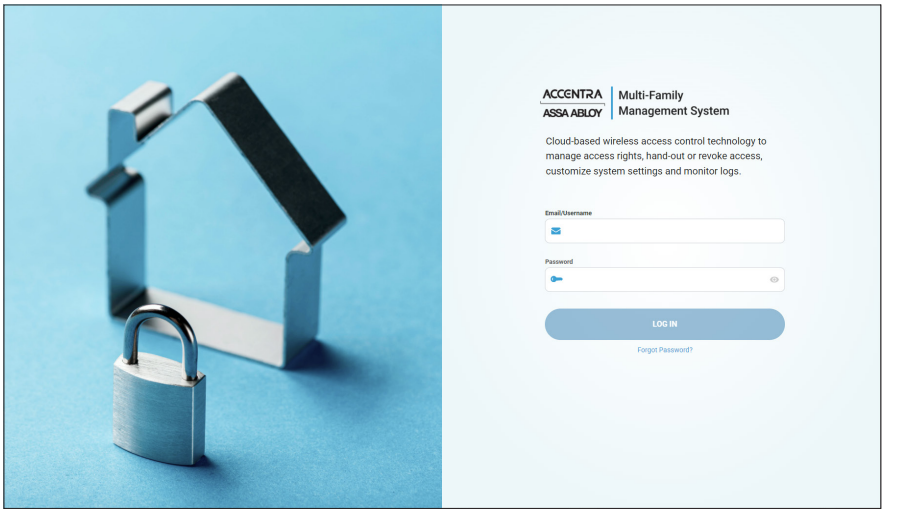
The Multi-Family Solution makes for easy, convenient access management of every opening in your multi-resident property. ASSA ABLOY ACCENTRA™ Multi-Family Management System is the user-friendly, cloud-based software that lies at the heart of the whole access control operation. Featuring an intuitive user interface, access rights for your residents, visitors, and staff can be managed remotely from any internet-enabled PC, tablet, or smart phone, anywhere in the world.

Please note that all of the system setup should be done using the configuration service prior to configuring offline locks and online updaters in the Multi-Family Management System using the Multi-Family mobile configuration app.

To access the Multi-Family Management System Cloud-Based Software, follow the link below:

https://app.accentra-assaabloy.com/

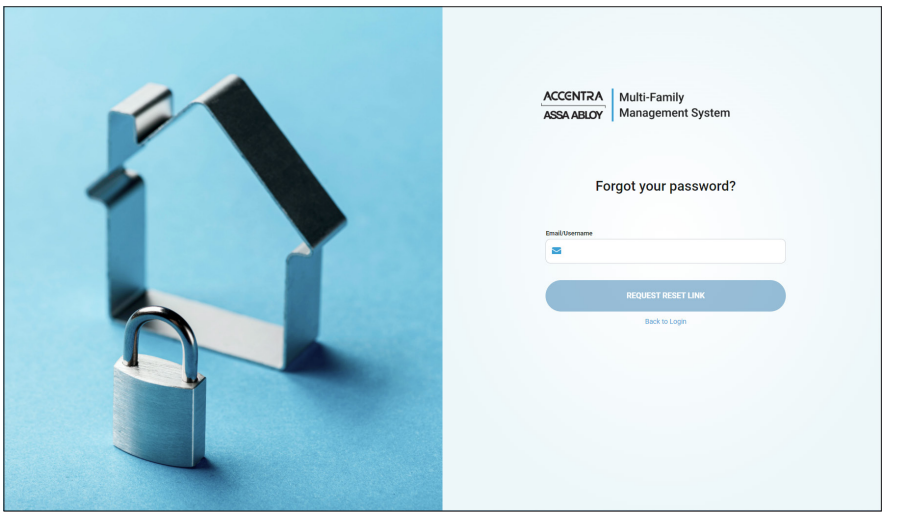
Log in to the software using the user name and password previously provided.



FORGOT PASSWORD

If you forgot your password, click the **Forgot Password?** link below the **Login** button. The Forgot Password screen appears. Enter your email address and then click the **Request Reset Link** button.

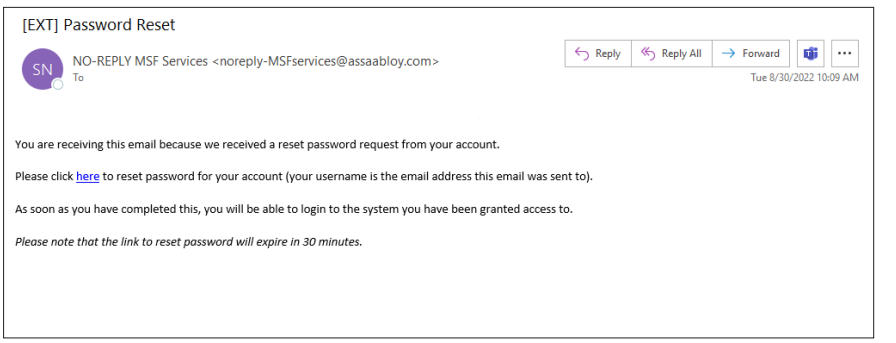
A success message is displayed in the upper right corner of the screen.

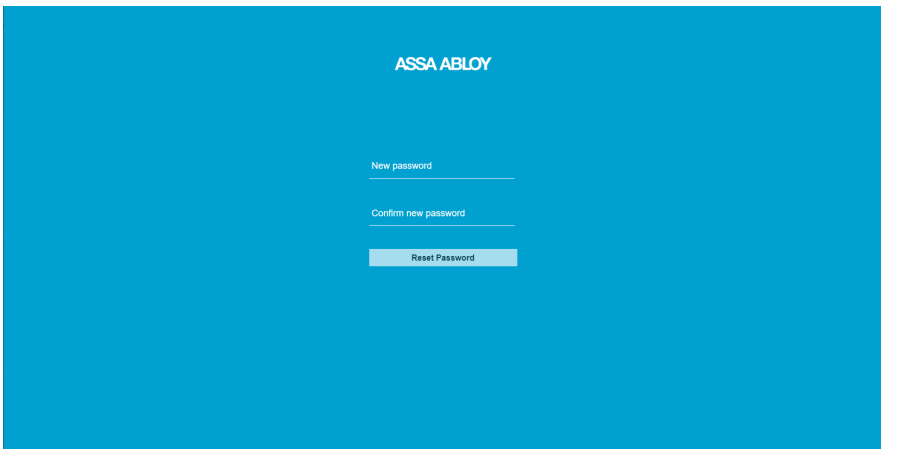


Check the inbox of the email/ username entered in the Forgot Password screen.

Click the link in the email to navigate to the Change Password screen.

In the Change Password screen enter the new password and then enter it a second time to confirm the password. Click the **Reset Password** button.





The Multi-Family Management System Software is managed by three services:

- Administration
- Configuration
- Reporting

These services manage different functions within the software and each is discussed in detail in this User Guide.

To access a service, simply click on the service on the left side of the screen.

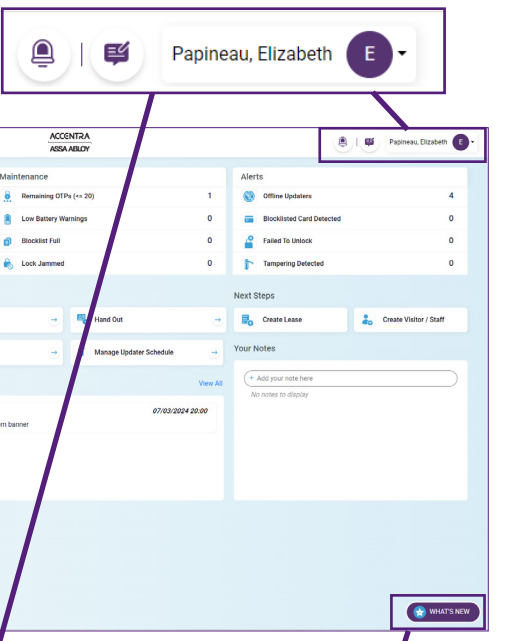
A Super Admin function is available to the System Owner, and to any administrative users the System Owner grants Super Admin privileges. This function only appears on the screen if the user has Super Admin privileges.

If the User manages more than one system, click on the system name at the top of the screen to view a drop-down list of all available systems.

The left side of the screen contains a list of the services and the functions managed by each service.

The User Guides button on the bottom left side of the screen provides access to all of the guides and manuals for the software.

The bottom left side of the screen contains icons for Help, Terms & Conditions, About, and Logout.

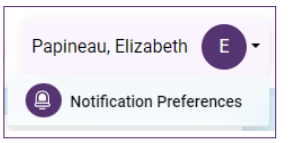


The top right side of the screen shows the logged in User's user name, a **profile** button, **notification** button, and a **feedback** button.

The bottom right side of the screen shows the **What's New** button. Click to see what new features have been added to the system.

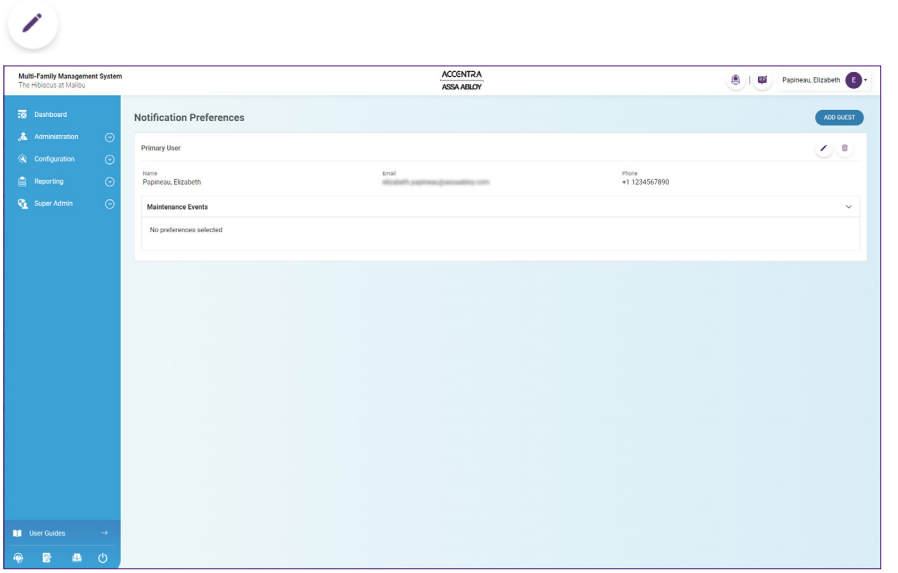
PROFILE, NOTIFICATIONS AND FEEDBACK

Profile:



When clicked, the profile button shows a drop-down menu allowing the user to select their notification preferences. Selecting **Notification Preferences** opens the user notification preferences page of the logged in user. This page displays the User Email address, the user Phone Number and the notification selections.

To edit the Notification selections, click the **edit (pencil)** button.

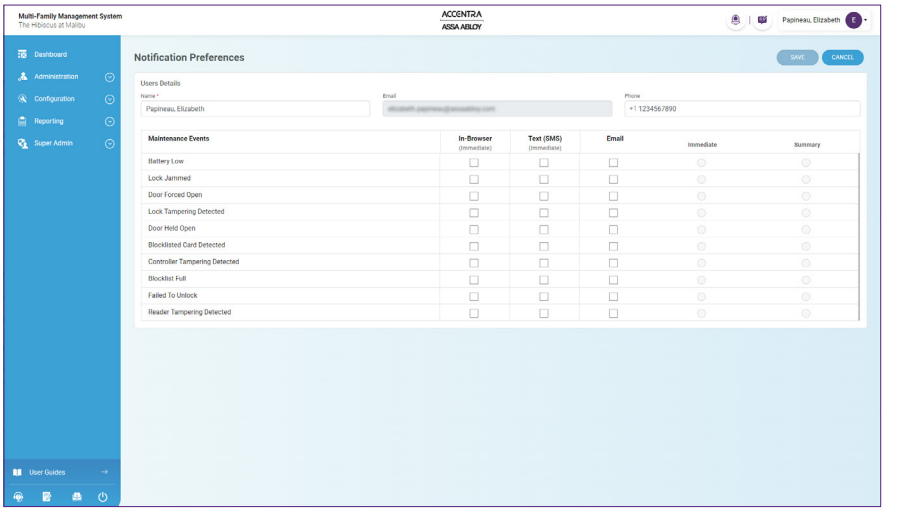


Select the check-boxes for the type of notification desired (**In Browser**, **Text**, or **Email**) for each maintenance event.

If **In Browser** is selected, notification messages appear in the Notification (bell) screen when a notification is triggered.

If **Text (SMS)** is selected, a text message is sent to the phone number entered in the system. **NOTE:** standard message and data rates may apply. A single text message is sent each day for each notification type.

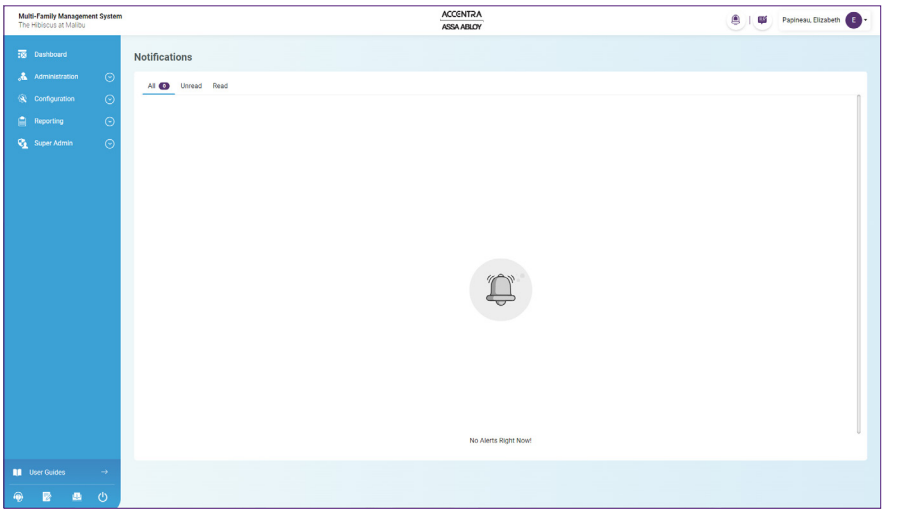
If **Email** is selected choose either **Immediate** or **Summary**. **Immediate** sends an email to the email address entered in the system when the notification is triggered. **Summary** sends a notification list at the end of every day.

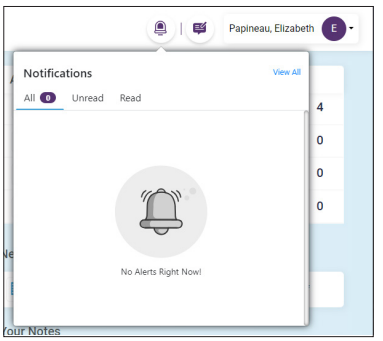


When finished editing, click the **Save** button to save the changes. Click the **Cancel** button to discard the changes.

Notifications:

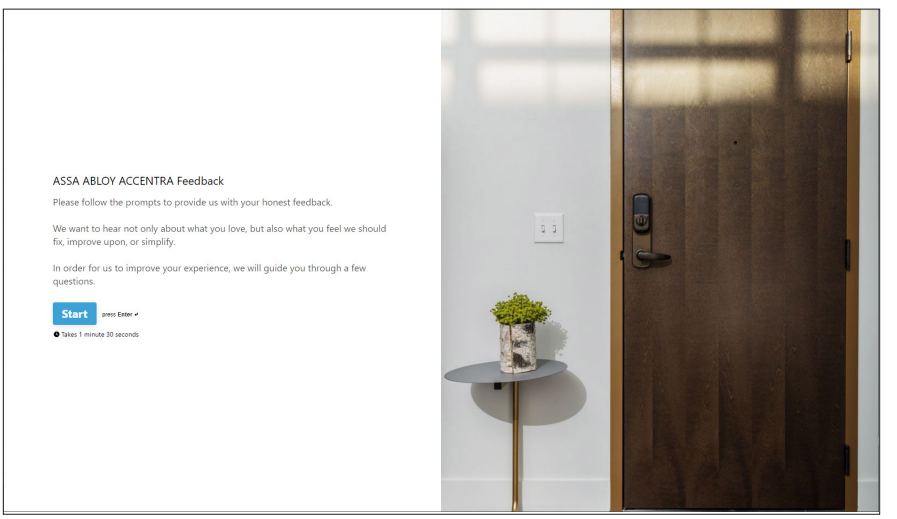
When clicked, the notification button opens a list of notifications. Select **All** to view all the notifications. Select **Unread** to view only the unread notifications. Select **Read** to view only the previously read notifications. Click **View All** to open the list in full-screen mode.





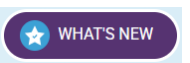
Feedback:

When clicked, the feedback button opens a new browser tab with the ASSA ABLOY ACCENTRA feedback site. Click the **Start** button to begin the feedback survey.



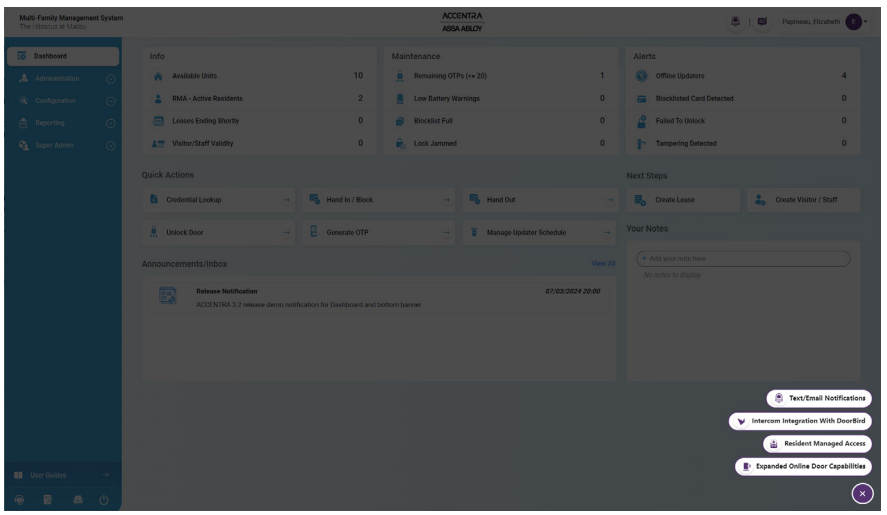
WHAT'S NEW

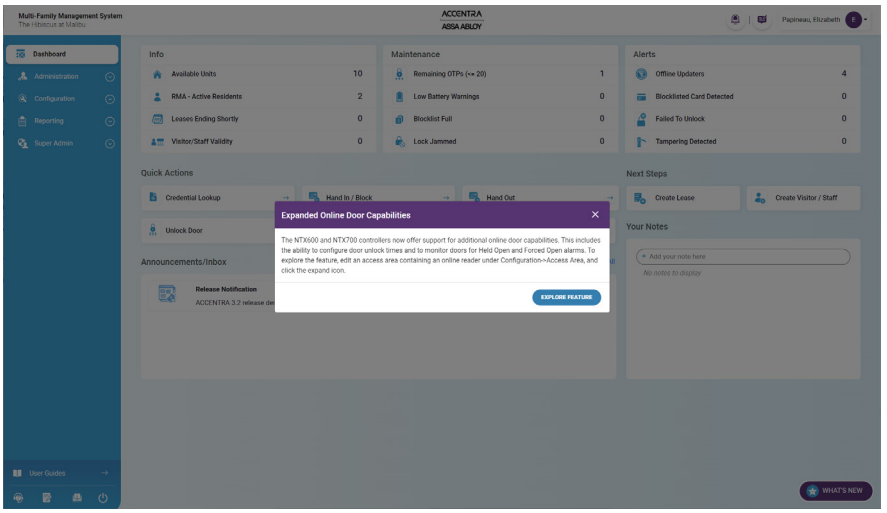
The What's New feature is used to highlight the new features/ functions added for the software release. Click the **What's New** button to view the list of new features/functions.



Click each individual item for more information about that feature/function. Click the **Explore Feature** button, or other buttons in the description as available to see what they do.

To close the information window, click the **X** in the upper right corner of the information window.

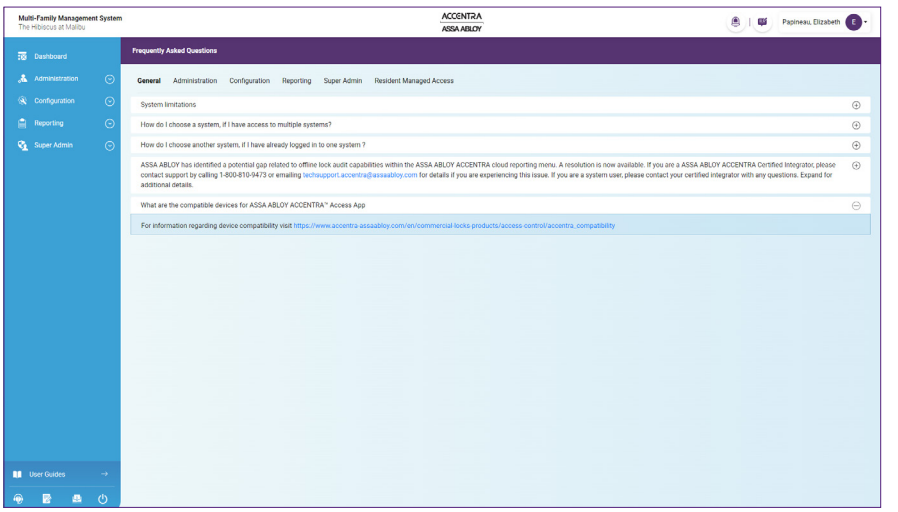


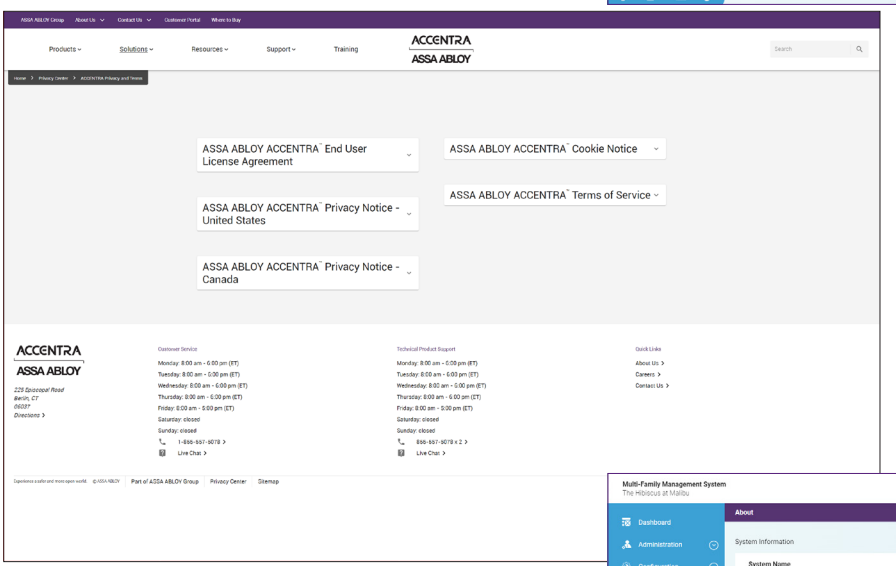


GENERAL TOOLS

General tools appear at the bottom of the navigation pane on the left side of the screen. These tools include Help, Terms & Conditions, About, and Logout.

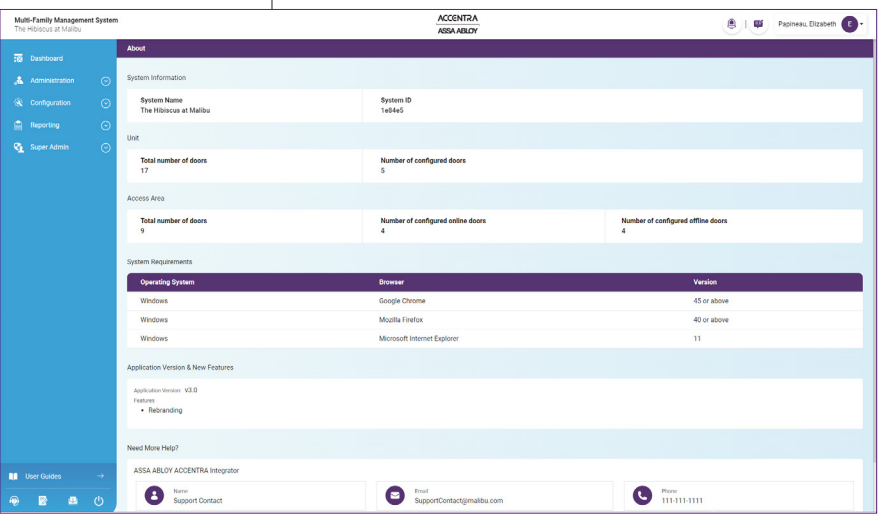
The **Help** screen provides information and Frequently Asked Questions for **General** information, **Administration** service, **Configuration** service **Reporting** service, **Super Admin**, and **Resident Managed Access**.





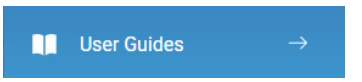
The **Terms & Conditions** button opens a separate browser window and displays the ACCENTRA Policy Center.

The **About** button provides all the system information for the current system.

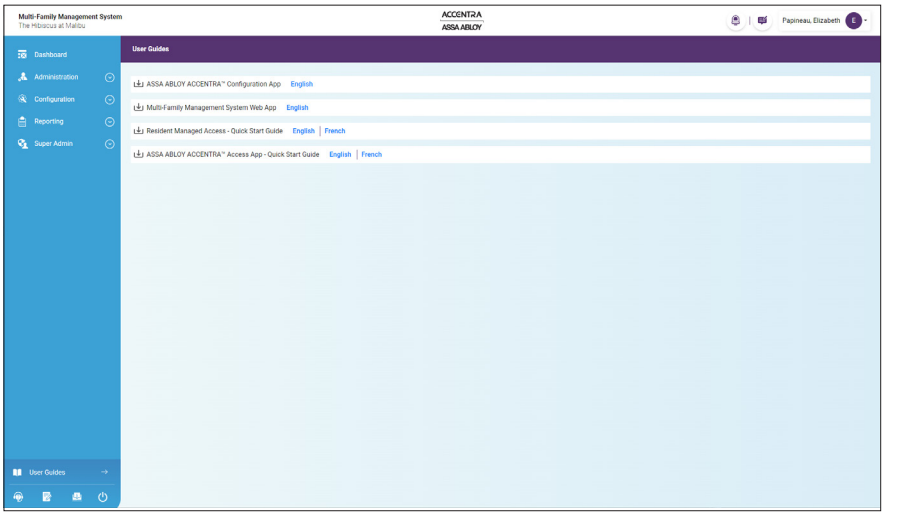


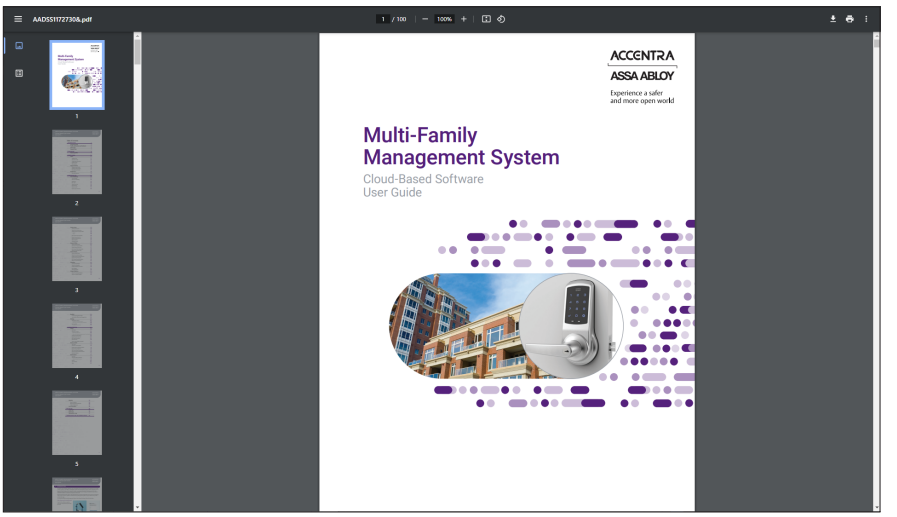
USER GUIDES

The User Guides button appears at the bottom of the navigation pane on the left side of the screen. When clicked, this button opens the User Guides screen.



Click on either **English** or **French** (if available) to open the English or French version of the named document. The document opens in a new browser tab and can be downloaded or printed using the buttons in the upper right corner of the document screen.

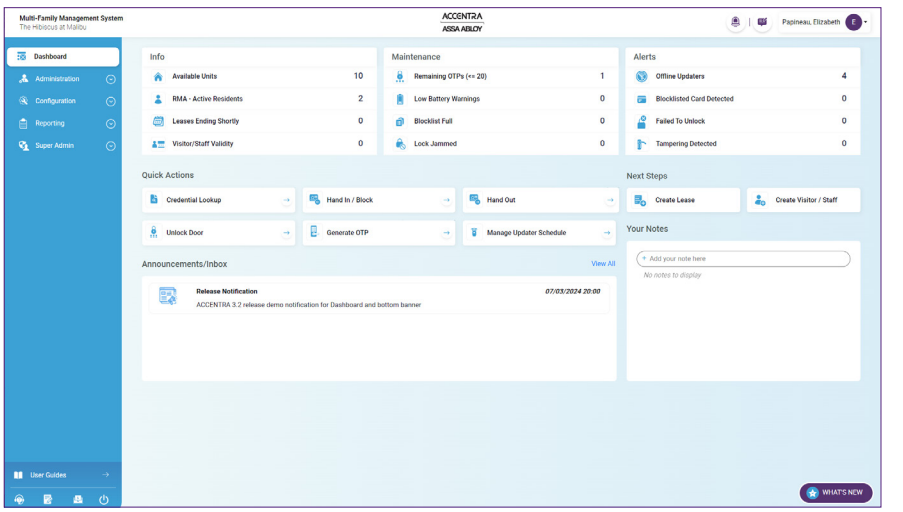




2. DASHBOARD

The Dashboard shows a quick overview of the entire system, system announcements and quick access to functions like creating leases, creating visitors or staff, credential lookup, credential hand out/hand in and lookup, door unlock and One-Time PIN creation.

The top part of the screen shows the following information:



Info:

- Available Units - number of units that are available for lease
- Resident Managed Access™ Active Residents - the number of active residents with access to the Resident Managed Access™ features and functions. (Active residents are those that have set up an individual login.)
- Leases ending shortly - number of leases ending in 30 days or less
- Visitor/Staff Validity - number of visitor/staff credentials expiring in 30 days or less

Maintenance:

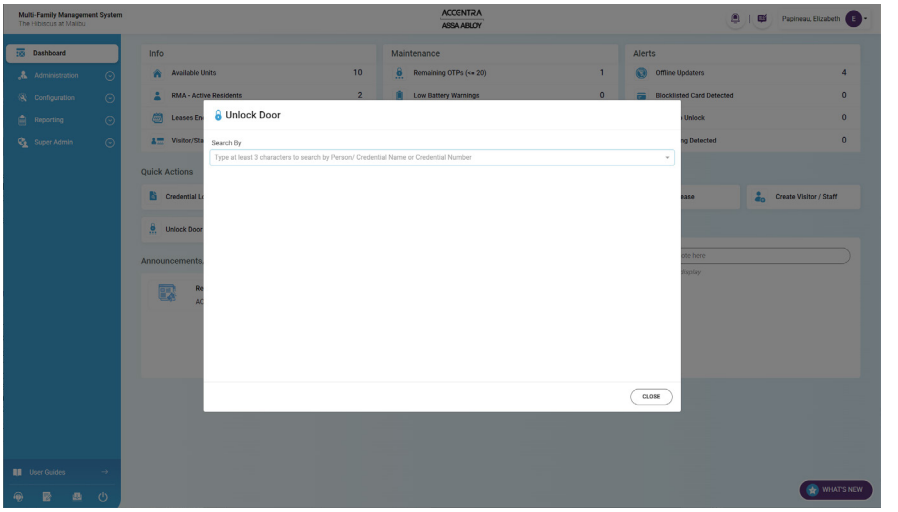
- Remaining OTPs - number of locks that have 20 or fewer One-Time PINs remaining in memory.
- Low Battery Warnings - number low battery warnings from all the locks
- Blocklist Full - number of locks that have a full blocklist
- Lock Jammed - number of doors in a lock jammed state

Alerts:

- Offline updaters - number of updaters that are offline
- Blocklist Card Detected - number of times a card on the blocklist has been attempted to be used
- Failed to Unlock - number of times doors have failed to unlock
- Tampering Detected - number of doors where tampering is detected

The information in each list is ordered based on the number of items, highest number to lowest number. Some of the items have more information. Click on the each display item to see more information.

Buttons on the screen allow the user to quickly access the screens to create a lease, create a visitor/staff, search for a user/credential, hand in/block credential, hand out credential, manage updater schedule, or unlock door. The unlock function can either issue a one-time PIN code for offline locks, or issue an unlock command for online updaters/locks. Create Lease, and Create Visitor/Staff work only if the user has Administrative privileges assigned.



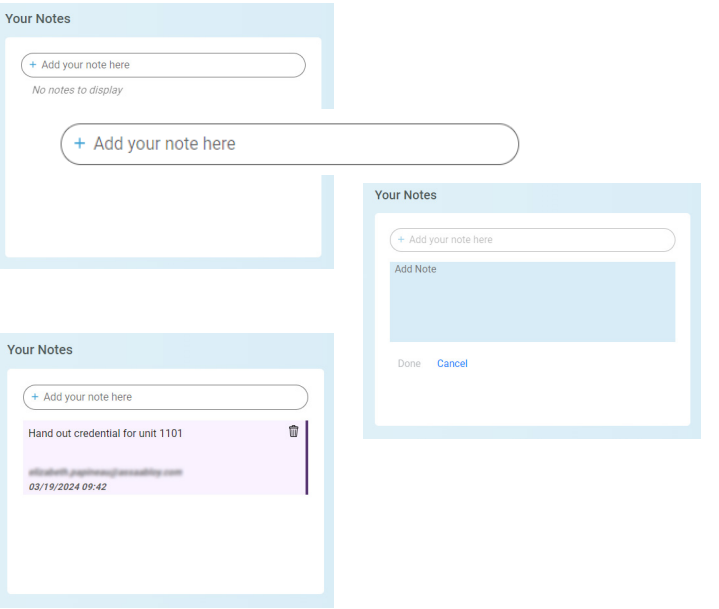
NOTE: The Quick Actions functions are assigned by the SuperAdmin. If these functions do not work, they were not assigned to the user.

System announcements appear in the **Announcements/Inbox** on the left side of the screen. The user can add notes in the **Your Notes** section on the right side of the screen. To add a note click the **Add your note here** button. A note text box appears.

Type the note in the box. When the note is complete, click the **Done** button. Click the **Cancel** button to discard and not save the note. When a note is saved, the author's name and the date the note was entered appears at the bottom of the note box.

To delete a saved note, click the **trash can** button.

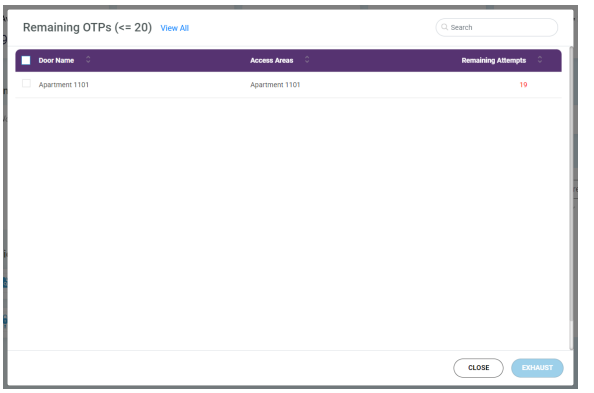
A maximum of ten (10) notes is allowed.

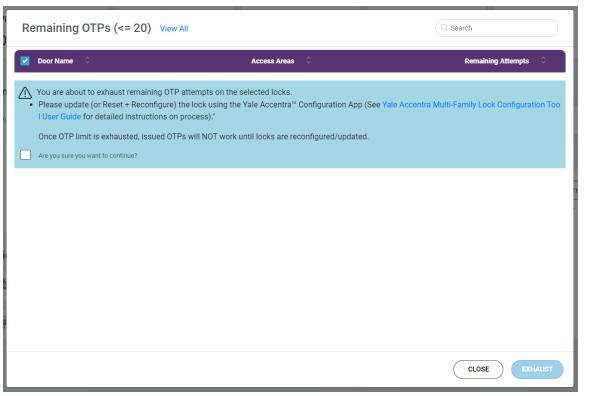


REMAINING OTPS

When there are doors with 20 or fewer remaining One-Time Passcodes, click on the tile for a list of doors. Selecting a door will enable the ability to exhaust the rest of the one-time passwcodes in the door lock. When the warning message appears, select the **Are You Sure You Want To Continue?** checkbox. This enables the **Exhaust** button. Click the **Exhaust** button to exhaust the remaining OTPs. Click the **Close** button to exit without making changes.

NOTE: See the Multi-Family Mobile Configuration Application User Guide for information on how to reset and reconfigure or update individual locks.



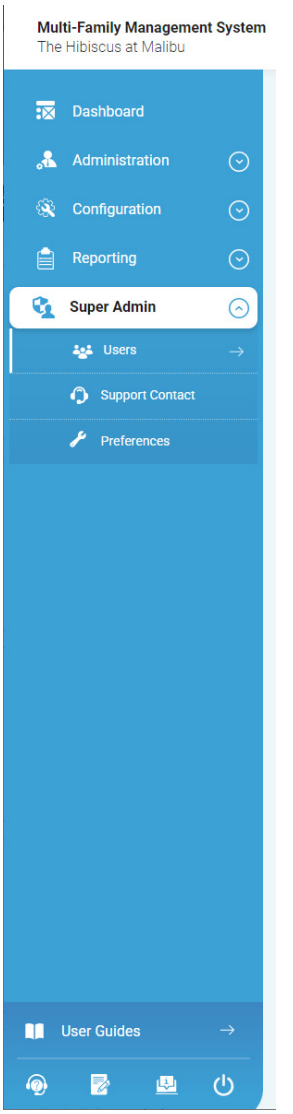


3. SUPER ADMIN

The Super Administration area is only used to create Multi-Family Management System administrative users and assign roles and permissions within the User Interface (UI). It is NOT possible to perform routine tasks, such as assigning area access, creating and maintaining credential holders, and managing leases, in the Super Administration area.

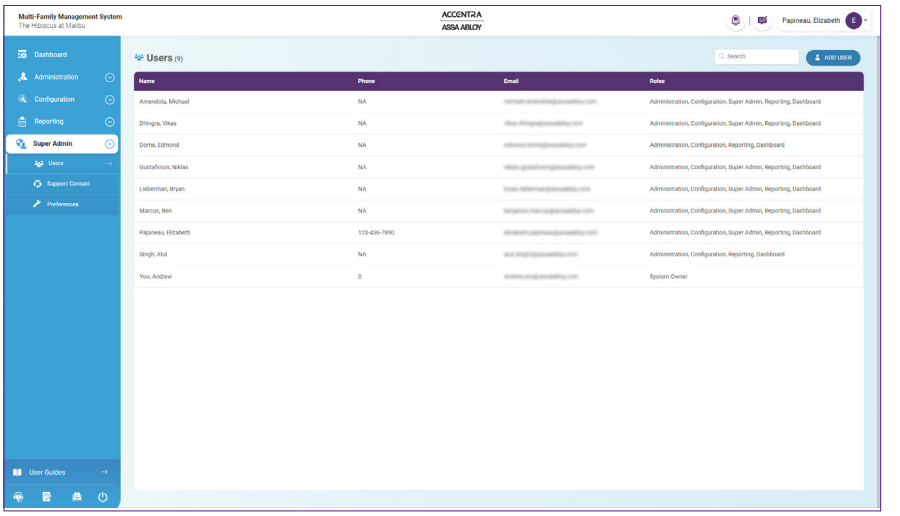
The Super Administration area is used to limit users' ability to access selected functions in the Cloud UI.

After purchase, the system owner receives an email with a link to complete the sign-up procedure. The link directs the system owner to an authentication page where a new password is entered. When the password is successfully changed, a link appears instructing the owner to click the link which directs to the Multi-Family Management System site.



USERS

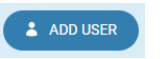
A User is any person who will have access to any of the services in the software. These users have administrative access to the system. Users are assigned roles that specify and restrict their permissions when working in the software.



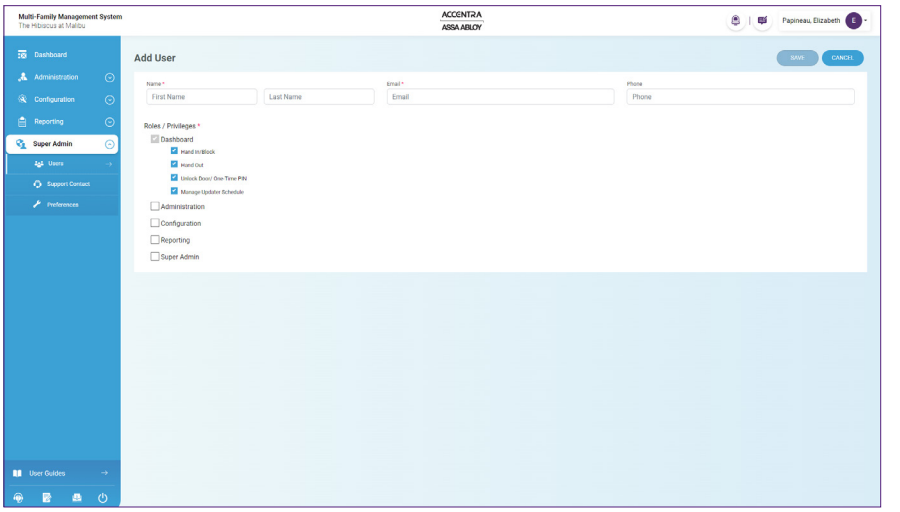
ADDING A USER

To add a user, do the following:

1. Click **Super Admin** and then click **Users** on the left side of the screen. A list of users appears.
2. Click the **Add User** button. The Add User screen appears.
3. Enter a **First Name** (required) for the new user.



4. Enter a **Last Name** (optional) for the new user.
5. Enter an **E-mail address** (required) for the new user. **NOTE:** E-mail address MUST be entered correctly. This is the login User Name that is assigned to a user in the system. It is also the email address to which the invitation email is sent.
6. Enter a **Phone number** (optional) for the new user.



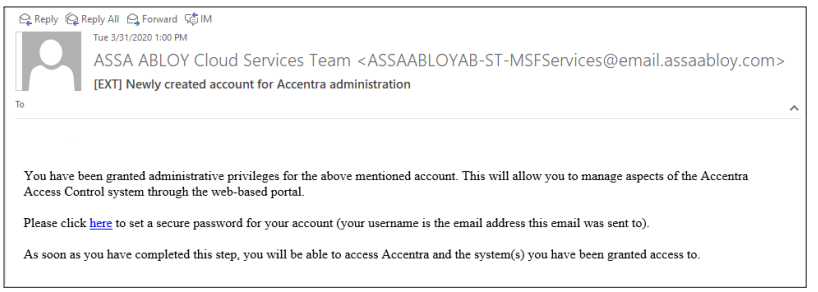
7. Click in one or more role/ privileges check-boxes to select the role/roles for the user and the Dashboard privileges the user will have. At least one role must be selected. The Roles/Privileges default selections are:
   - Dashboard: all available dashboard options selected
   - Administration: Access to the Administration section of the site, Dashboard Quick Actions: Credential lookup, Hand in/Block, Hand out, Unlock Door/One-Time PIN, Create Lease, Create Visitor/Staff

- Configuration: Access to the Configuration section of the site, Dashboard Quick Actions: Credential Lookup, Manage updater Schedule
- Reporting: Access to the Reporting section of the site
- Super Admin: Access to the Super Admin section of the site

8. Review the user information. If the information is correct, click the **SAVE** button to complete the user creation. The **SAVE** button is not enabled until all of the mandatory fields are filled in. Click the **CANCEL** button to discard the changes return to the Users screen.

Once a user is created, the user will receive an email from ASSA ABLOY Cloud Services Team <ASSAABLOYAB-ST-MSFServices@email.assaabloy.com>. Inform the user they will receive an email and they should check their junk and/or spam email folder.

When the user clicks the link in the email, they are brought to the login page to set their password.



SEARCH FOR A USER

To search for a user, do the following:

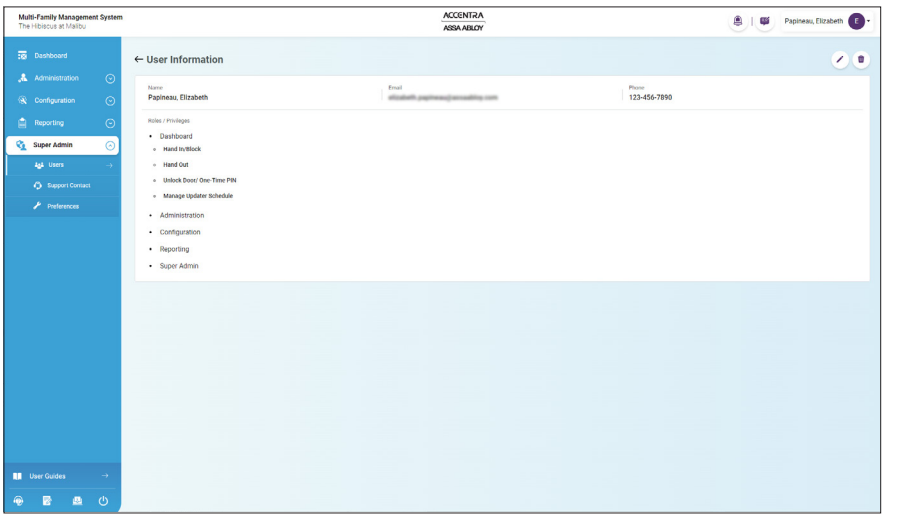
1. Click **Super Admin** and then click **Users** on the left side of the screen. A list of users appears.
2. Enter the search criteria in the **Search** box at the top of the Users list. **NOTE:** Any text or part of text used in the Search field that is part of the user's name will appear in the Search results.

3. The search results are displayed automatically.

DISPLAY USER INFORMATION

To display user information, do the following:

1. Click **Super Admin** and then click **Users** on the left side of the screen. A list of users appears.
2. Click on the desired user name. Use the Search function to find the desired user name. The User Information screen appears.
3. To return to the users list, click **Arrow** next to User Information in the upper left corner of the screen.



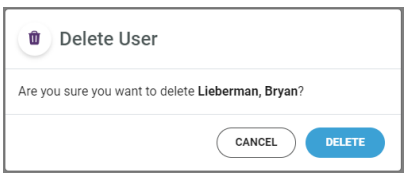
The User Information screen shows the user name, description, email, phone number and the roles/ privileges the user has been assigned.

DELETING A USER

To delete a user, do the following:

1. Click **Super Admin** and then click **Users** on the left side of the screen. A list of users appears.
2. Click on a user name from the list, or use the **Search** tool to find the desired user name. The User Information screen appears.
3. Click the **Trash Can** button in the upper right side of the screen. A Delete Confirmation screen appears.

4. Click the **Delete** button to confirm user delete. Click the **Cancel** button to keep the user.

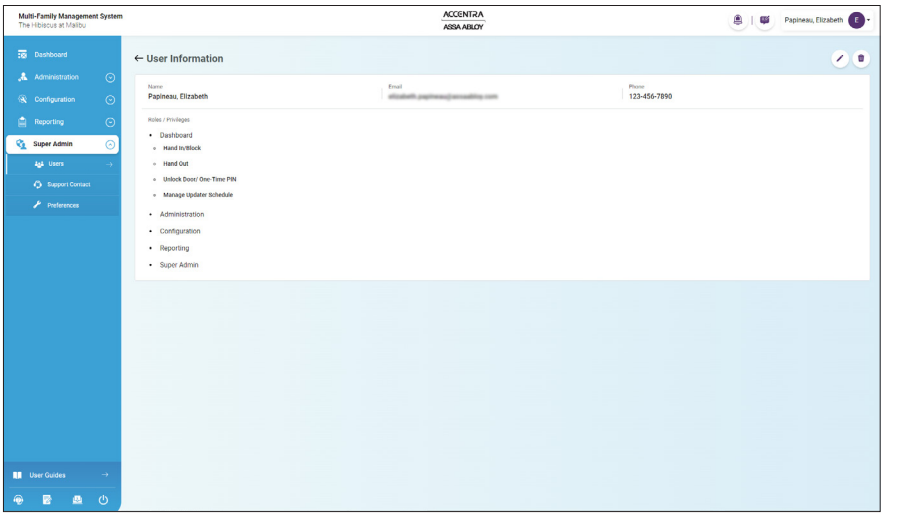


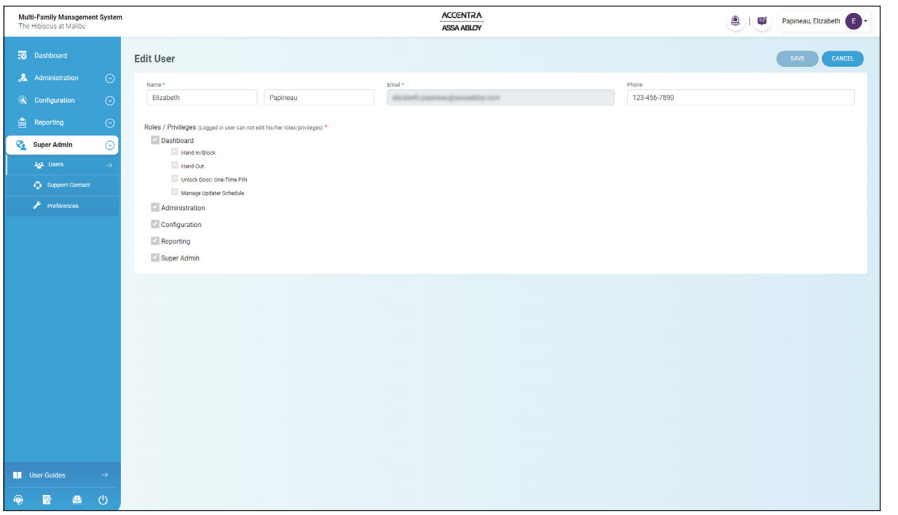
EDITING A USER

To edit a user, do the following:

1. Click **Super Admin** and then click **Users** on the left side of the screen. A list of users appears.
2. Click on a user name from the list, or use the **Search** tool to find the desired user name. The User Information screen appears.
3. Click on the **pencil** button in the upper right side of the screen.

   The Edit User screen appears.
4. Make the desired changes to the user name, phone number, and/or roles and privileges.
   NOTE: the e-mail address cannot be edited.
5. Click the **Save** button to save the changes. The User Information screen is displayed. Click the **Cancel** button to discard changes without saving.



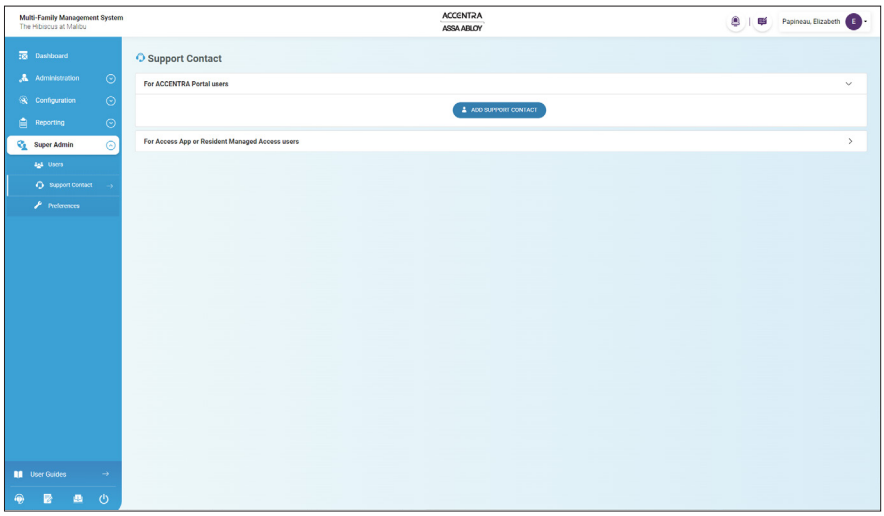


SUPPORT CONTACT

Support Contact contains the information used to contact the designated support representatives for the system. There are two support contacts, one for the system portal users and one for the mobile credential access app or Resident Managed Access™. The support contact information for the system appears in the About screen. The support contact information for residents appears in the Support menu in the ASSA ABLOY ACCENTRA™ mobile credential access application, and in the Help section of the Resident Managed Access™ portal.

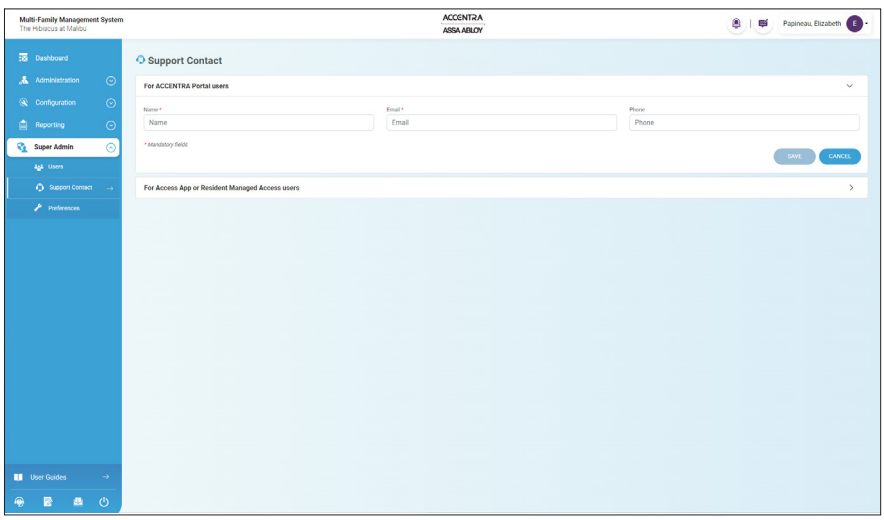
ADDING CONTACT DETAILS

To add a contact, do the following:



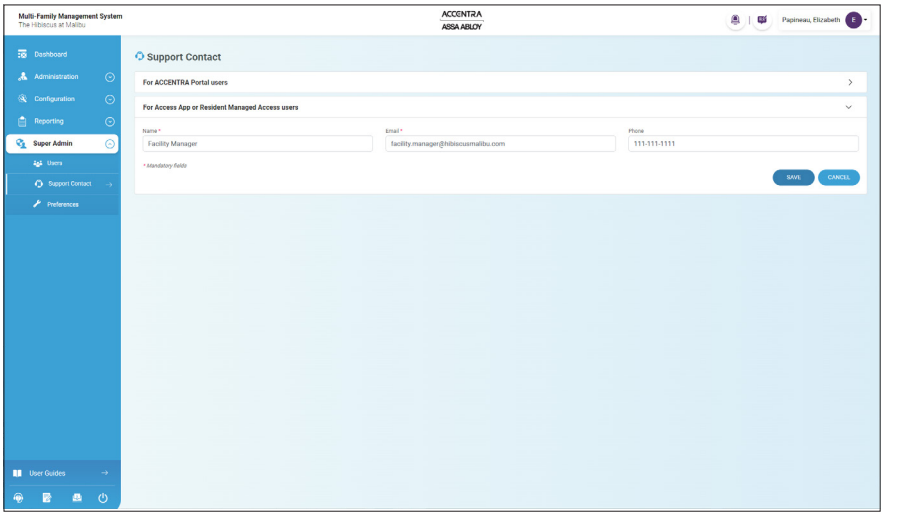
1. Click **Super Admin** and then click **Support Contact** on the left side of the screen. The Support Contact screen appears.
2. Click the **Add Support Contact** button under *For Access App or Resident Managed Access™ Users*. The Add Support Contact screen appears.

3. Enter a **Name** (required) for the new contact.
4. Enter an **E-mail address** (required) for the new contact. **NOTE:** E-mail address MUST be entered correctly.
5. Enter a **Phone number** (optional) for the new contact.
6. Click the **Save** button. The new contact is added to the Support Contact list. Click the **Cancel** button to stop adding the contact information and return to the Support Contact screen.



7. Click on **For Access App or Resident Managed Access users**.

8. Click the **Add Support Contact** button. The Add Support Contact screen appears.

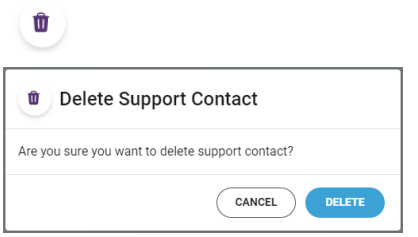


9. Enter a **Name** (required) for the new contact.
10. Enter an **E-mail address** (required) for the new contact. **NOTE:** E-mail address MUST be entered correctly.
11. Enter a **Phone number** (optional) for the new contact.
12. Click the **Save** button. The new contact is added to the Support Contact list. Click the **Cancel** button to stop adding the contact information and return to the Support Contact screen.

DELETING CONTACT DETAILS

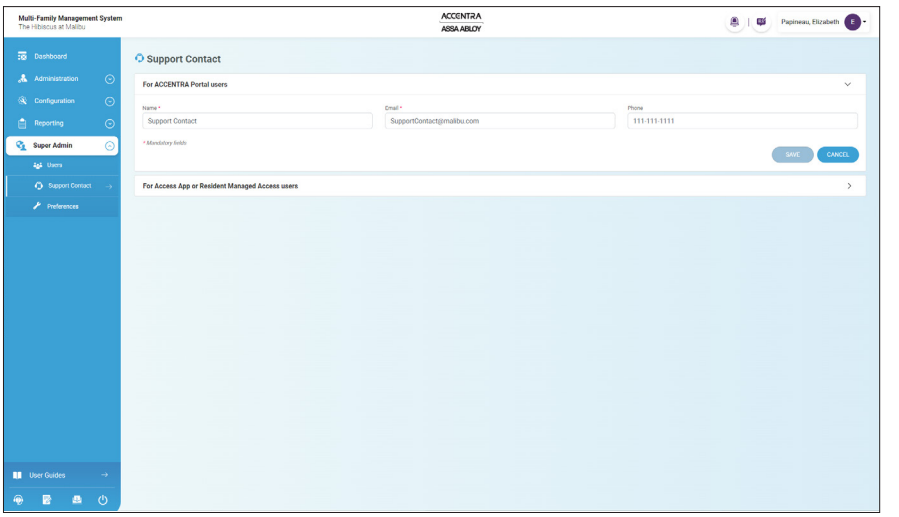
To delete a contact, do the following:

1. Click **Super Admin** and then click **Support Contact** on the left side of the screen. The Support Contact screen appears.
2. Click the **Trash Can** button in the upper right side of the screen. A Delete Confirmation screen appears.
3. Click **Delete** to confirm contact delete the contact details. Click **Cancel** to keep the contact information.



EDITING CONTACT DETAILS

To edit a contact, do the following:



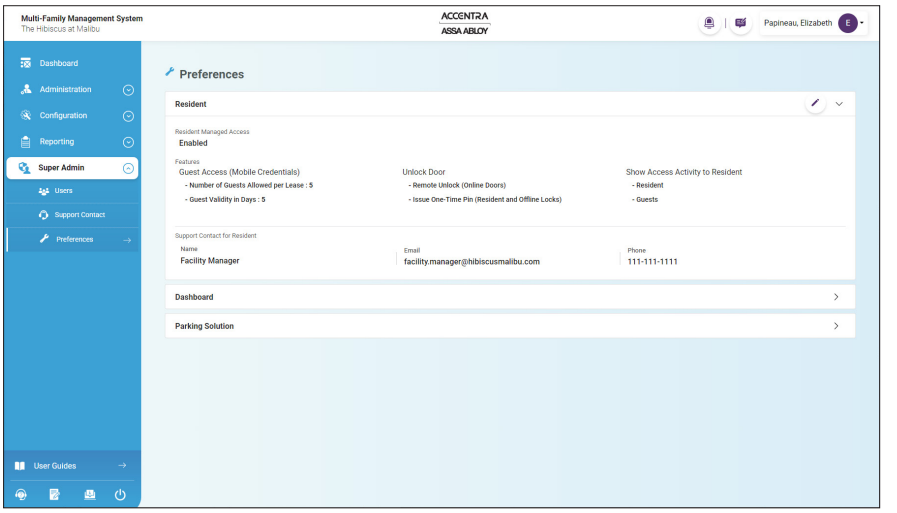
1. Click **Super Admin** and then click **Support Contact** on the left side of the screen. The Support Contact screen appears.
2. Click on **For ACCENTRA Portal users** or **For Access App or Resident Managed Access users**.
3. Click on the **pencil** button on the right side of the screen. The Edit Support Contact screen appears.
4. Edit the **Name** (required) for the contact.
5. Edit the **E-mail address** (required) for the contact.
   NOTE: E-mail address MUST be entered correctly.
6. Edit the **Phone number** (optional) for the contact.
7. Click the **Save** button. The updated contact information is saved. Click the **Cancel** button to stop editing the contact information and return to the Support Contact screen.

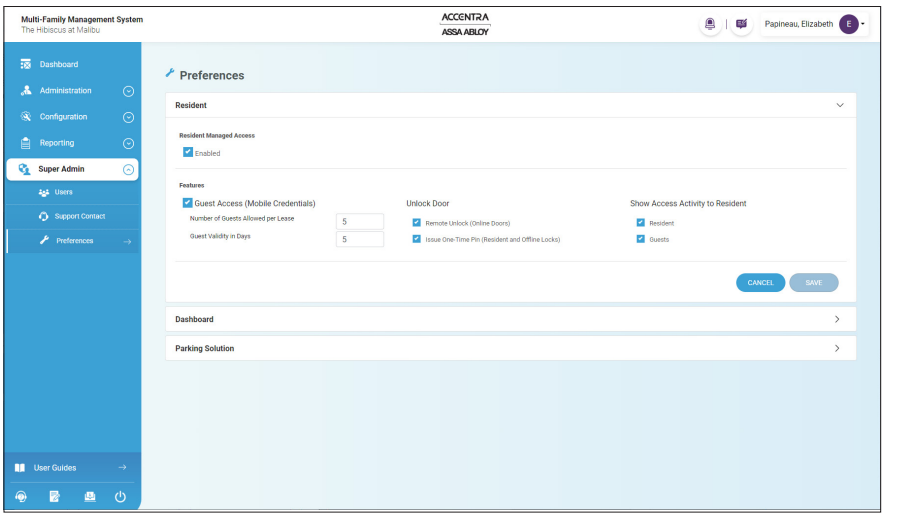
PREFERENCES

Preferences contains the settings for the Resident Managed Access™ functionality, limited Dashboard preferences, and Parking Solution. If Resident Managed Access™ is enabled, selected residents are able to hand out mobile credentials to their guests. Dashboard preferences include the setting of One-Time PIN code lower limit display. If Parking Solution is enabled, administrators are able to hand out parking credentials for resident vehicles.

EDITING PREFERENCES

To edit Resident preferences, do the following:





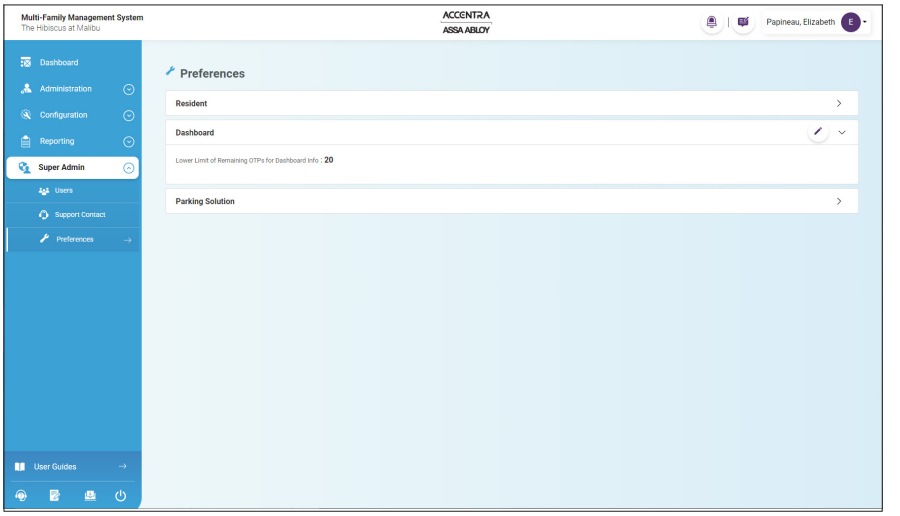
1. Click **Super Admin** and then click **Preferences** on the left side of the screen. The Preferences screen appears with the Resident section displayed as default.
2. Click on the **pencil** button on the right side of the screen. The Edit Resident Preferences screen appears.
3. Select the **Enabled** check box to enable the Resident Managed Access™ functions.
4. Select the desired **Features** check boxes:
   - **Guest Access** - allows the residents to issue mobile credentials to guests. Type in the desired **Number of Guests Allowed per Lease** (maximum number of guest credentials that can be issues per lease) and **Guest Validity in Days** (maximum number of days guest credentials are valid).
   - **Unlock Door** - select the desired check boxes to allow the resident to remotely unlock doors or issue One-Time PINs to offline locks.
   - **Show Access Activity to Resident** - select the desired check boxes to allow the resident to view their and/or their guest's access activity.
5. Click the **Save** button. The updated preferences are saved. Click the **Cancel** button to stop editing the preferences and return to the Preferences screen.

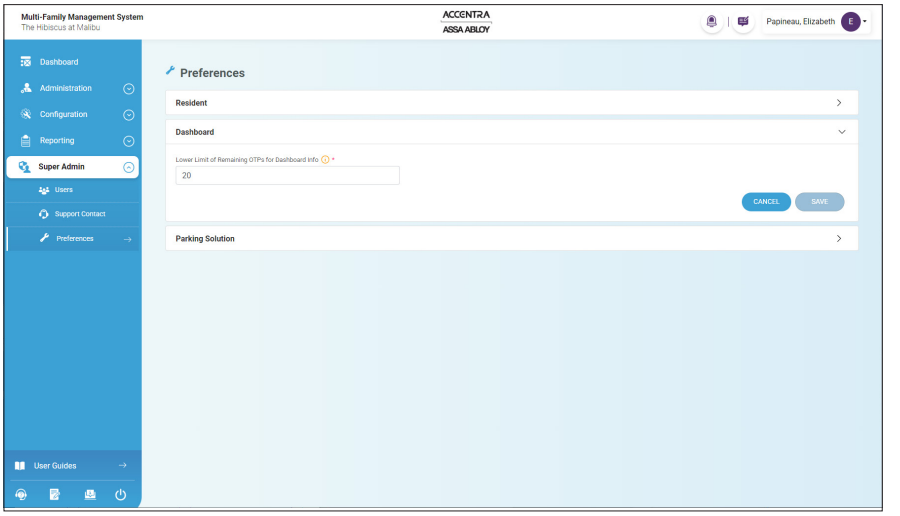
To edit Dashboard preferences, do the following:

1. Click **Super Admin** and then click **Preferences** on the left side of the screen. The Preferences screen appears with the Resident section displayed as default.
2. Click on **Dashboard** to display the Dashboard preferences.
3. Click on the **pencil** button on the right side of the screen.

   The Edit Dashboard Preferences screen appears.
4. Enter the desired value for the lower limit of remaining OTPs in locks. Any locks with the number of remaining OTPs below this number are displayed in the Dashboard.
   See “Remaining OTPs” on page 11.
5. Click the **Save** button. The updated preferences are saved. Click the **Cancel** button to stop editing the preferences and return to the Preferences screen.



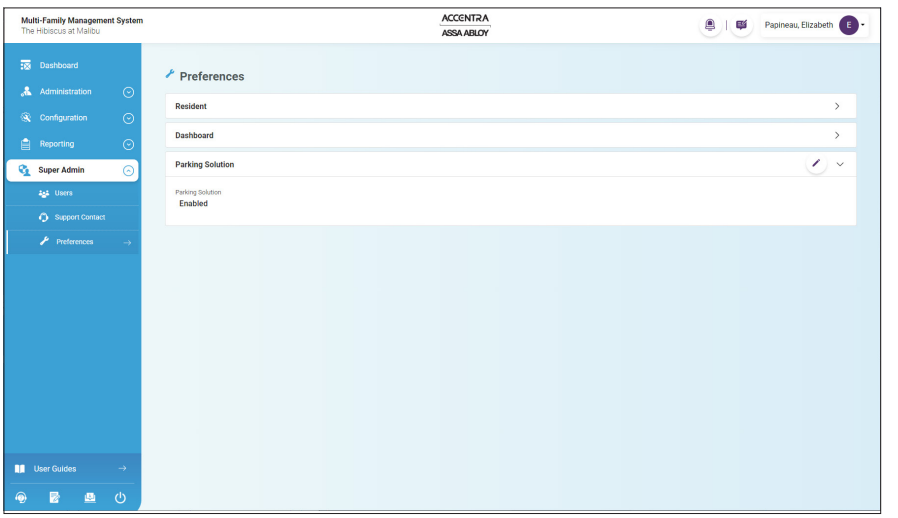


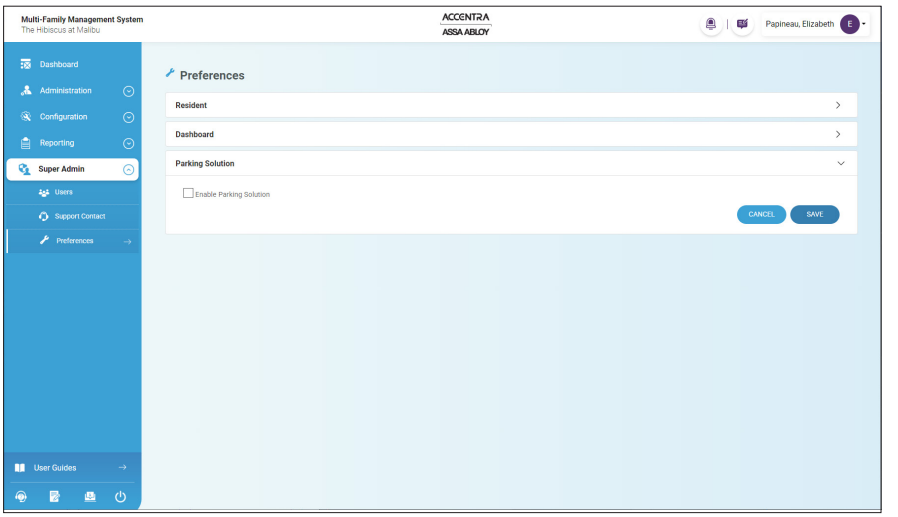
To edit Parking Solution preferences, do the following:

1. Click **Super Admin** and then click **Preferences** on the left side of the screen. The Preferences screen appears with the Resident section displayed as default.
2. Click on **Parking Solution** to display the Parking Solution preferences.
3. Click on the **pencil** button on the right side of the screen.

   The Edit Parking Solution Preferences screen appears.
4. Select the **Enabled** check box to enable the Parking Solution functions.
5. Click the **Save** button. The updated preferences are saved. Click the **Cancel** button to stop editing the preferences and return to the Preferences screen.

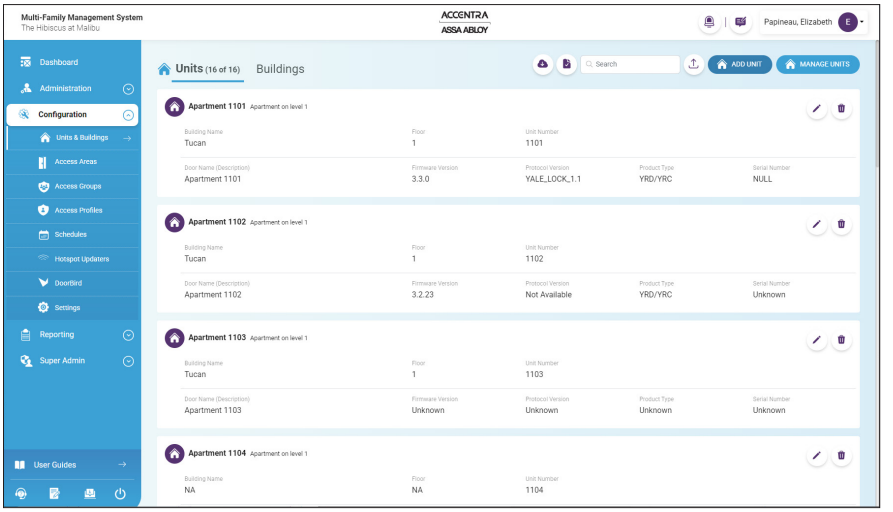




4. CONFIGURATION

The Configuration service manages all elements of the system that control access to the facility, such as residential units and buildings, access areas, access profiles, and access (door) groups. This service also manages door and updater/controller schedules, system settings and preferences such as One Time PIN and revalidation interval.

When Configuration is selected, the Units & Buildings screen appears by default. Any of the other configuration items, such as Schedules and Settings, can be selected from the left side of the screen.



UNITS & BUILDINGS

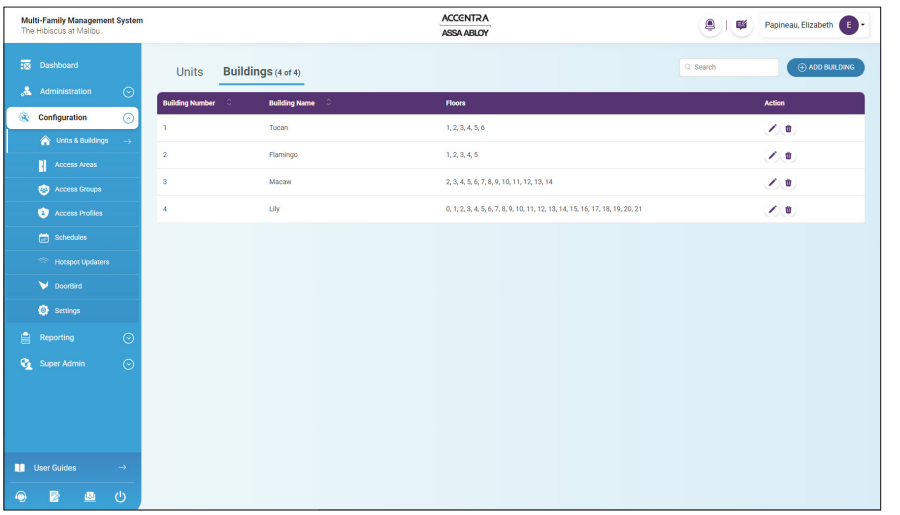
A Building is defined as a structure that contains multiple Units as well as common areas such as exercise rooms, laundry facilities, etc.

A Unit is defined as a room, apartment, condo, or similar location that is managed by a lease. This does not include common areas such as exercise rooms, laundry facilities, etc. A unit has one or more doors with digital door locks.

Access to the Unit and Building is granted through the lease workflow.

The Buildings configuration allows the administrator to add a building, search for a building, and display building information.

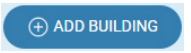
The Building screen displays a list of buildings along with the building information.



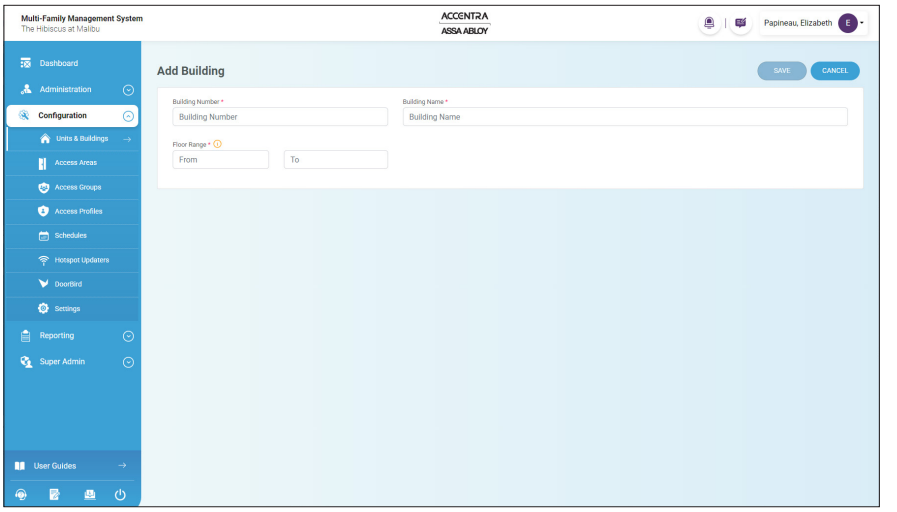
ADD A BUILDING

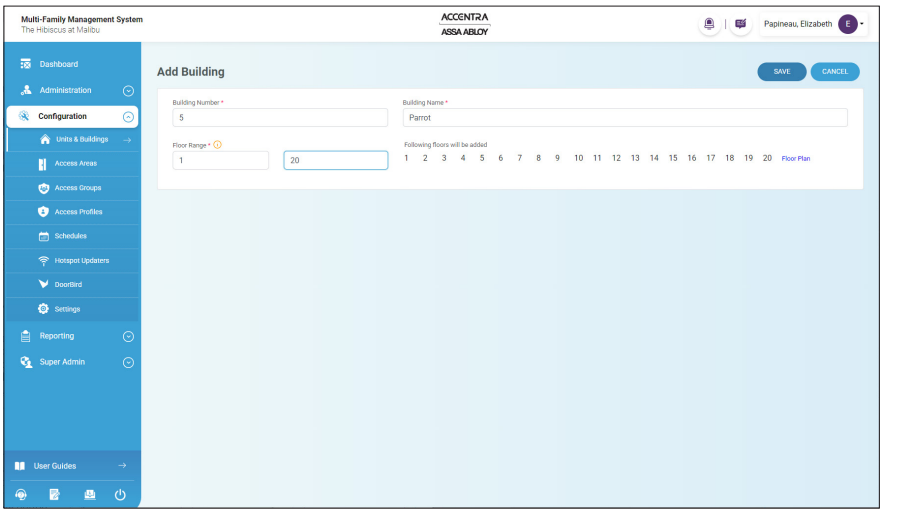
To add a building, do the following:

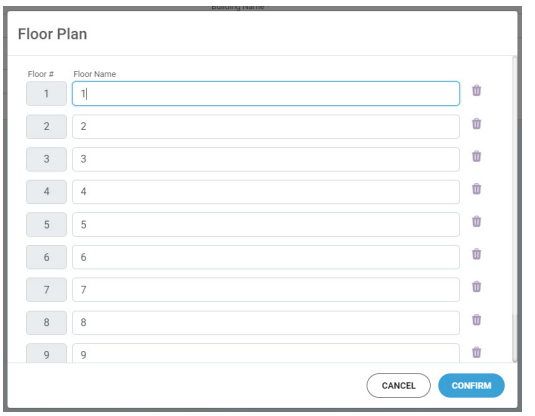
1. Click **Configuration** and then click **Units & Buildings** on the left side of the screen. The Units screen appears.
2. Click the **Buildings** tab at the top of the screen.
3. Click the **Add Building** button above the list of buildings.



   The Add Building screen appears.
4. Enter a building **Number** and **Name** and the **Floor Range**. The floor range can be from -10 to 100 floors. When the floors are added a list of the individual floors is displayed.
5. Click **Floor Plan** to edit the building floor plan. Add a Floor Name for each floor, or delete the floor, if desired.
6. Click the **Confirm** button to save the Floor Plan. Click the **Cancel** button to cancel any edits.
7. When all the information is done being added, Click the **Save** button to save the building information. Click the **Cancel** button to discard the building information and return to the Building screen.







SEARCH FOR A BUILDING

To search for a building, do the following:

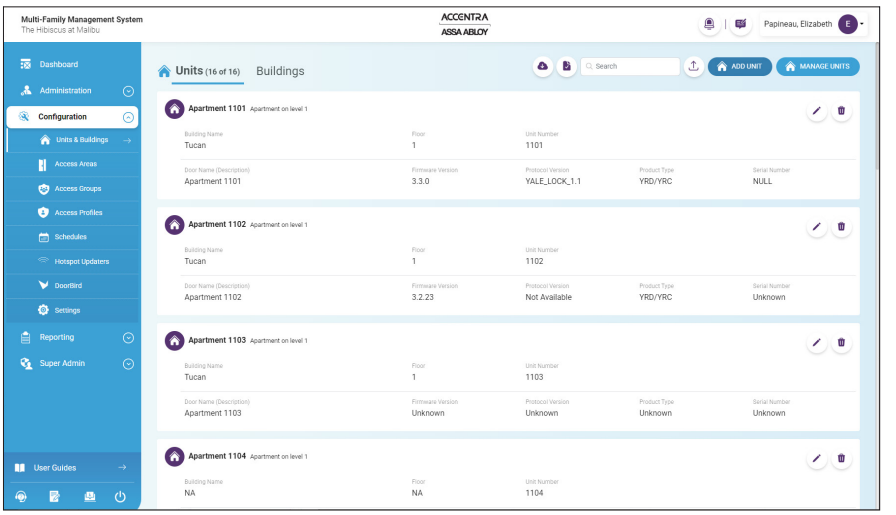
1. Click **Configuration** and then click **Units & Buildings** on the left side of the screen. A list of units appears.
2. Click the **Buildings** tab at the top of the screen.
3. Enter the search criteria in the **Search** box at the top of the Unit list.

NOTE: Any text or part of text used in the Search field that is part of the unit's name or description will appear in the Search results.

4. The search results are displayed automatically.

The Units configuration allows the administrator to add a unit, search for a unit, display unit information, edit unit information, and remove a unit.

The Units screen displays a list of units along with the unit information. This screen displays a maximum of 700 units. If there are more than 700 units in the system, scroll down to display the next 700 units.

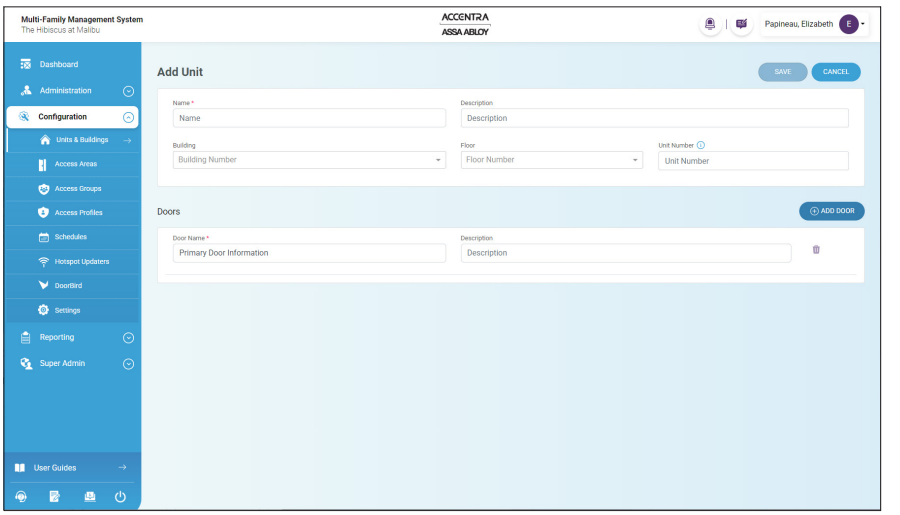


ADD A UNIT

To add a unit, do the following:

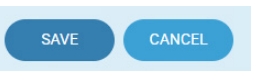
1. Click **Configuration** and then click **Units & Buildings** on the left side of the screen. The Units screen appears.
2. Click the **Add Unit** button above the list of units. The Add Unit screen appears.

3. Enter a unit **Name**. Optionally enter a **Description**, **Building Name**, **Floor Number** and **Unit Number** (6 digits max).



4. Enter a door **Name** and **Description** in the Doors section of the screen. Name is a required field, Description is optional. Each unit must have at least one door associated with it.
5. Click the **Add Door** button to add additional doors and door information to the unit. Select a door and click the **Trash Can** button to delete a door from the unit.

6. Click the **Save** button to save the unit information. Click the **Cancel** button to discard the unit information and return to the Units screen.



NOTE: Unit lock(s) need to be commissioned into the system by the Certified Integrator.

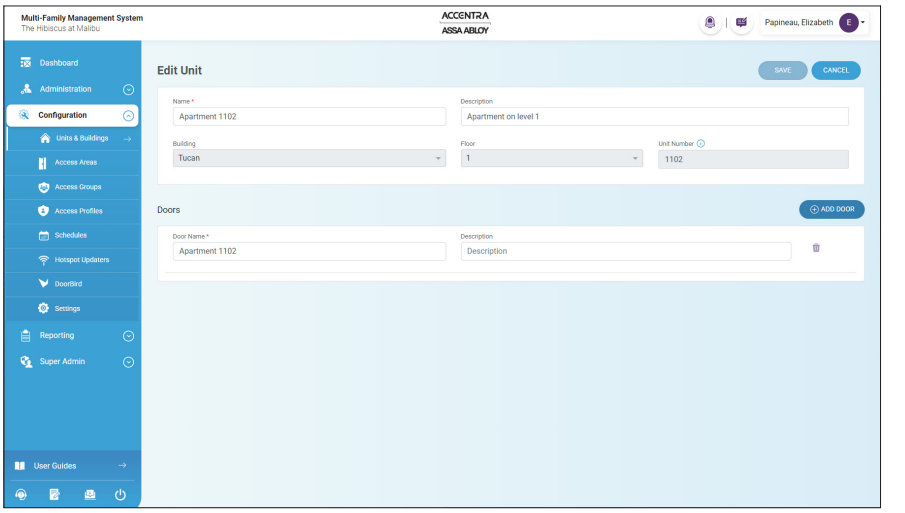
EDIT A UNIT

To edit a unit, do the following:

1. Click **Configuration** and then click **Units & Buildings** on the left side of the screen. A list of units appears.
2. Click the **Edit** (pencil) button next to the unit name to be edited.

   The Edit Unit screen appears with the current unit information filled in.



3. Change or enter information into any of the fields as desired. Add a door by clicking the **Add Door** button. Delete a door by clicking the **Trash Can** button.

4. When finished, click the **Save** button to save the unit information. Click the **Cancel** button to discard the changes and return to the Units screen.

SEARCH FOR A UNIT

To search for a unit, do the following:

1. Click **Configuration** and then click **Units & Buildings** on the left side of the screen. A list of units appears.

2. Enter the search criteria in the **Search** box at the top of the Unit list.

NOTE: Any text or part of text used in the Search field that is part of the unit's name or description will appear in the Search results.

3. The search results are displayed automatically.

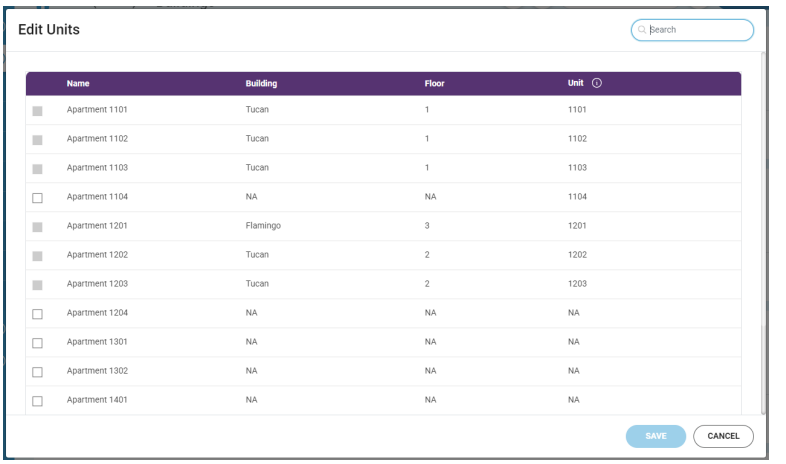
MANAGE UNITS

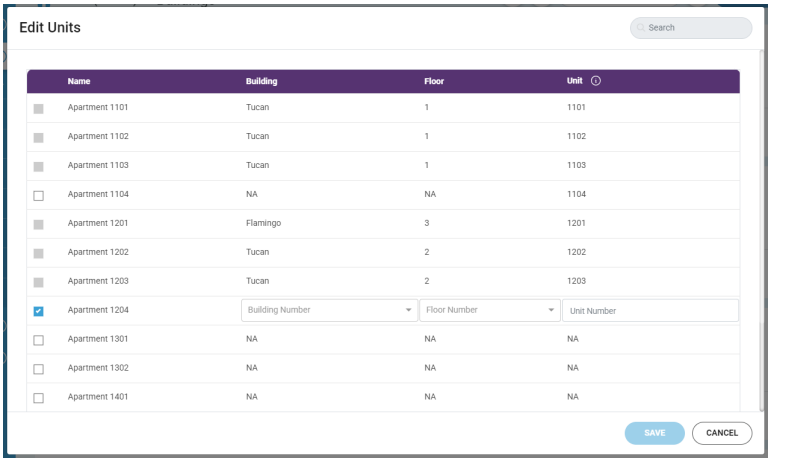
The Manage Units functions allows building, floor, and unit number information to be added to any units that did not have that information when the Unit was added to the system. Multiple units can be edited at the same time.

To manage units, do the following:

1. Click **Configuration** and then click **Units & Buildings** on the left side of the screen. The Units screen appears.
2. Click the **Manage Unit** button above the list of units. 

The Edit Units screen appears.
3. Search for a unit by scrolling through the list or entering the search criteria in the **Search** box at the top of the screen.
4. Select the desired unit by clicking the **checkbox** on the left side of the screen.
5. Select a building name/number from the **Building** dropdown. Select a floor number from the **Floor** dropdown (this is required when a building is selected). Select or enter a unit number from the **Unit** scroll box (6 digits maximum; this is required when a building and floor are selected).
6. When finished editing the desired units, click the **Save** button to save all the unit information. Click the **Cancel** button to discard all the unit information and return to the Units screen.





REMOVE A UNIT

Removing a unit removes a lock, or set of locks, from cloud-based software as well as the mobile configuration app. Unless the lock is reset and/or reconfigured before removal, the lock remains configured with no information for it in the cloud-based software or the mobile configuration app.

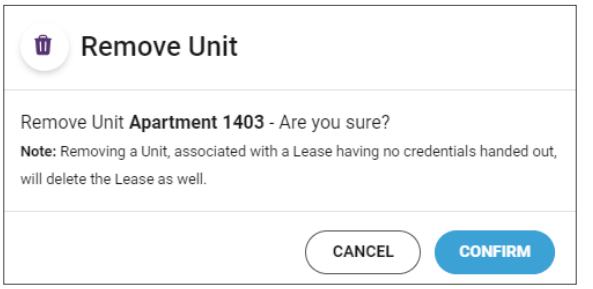
If a unit has an active lease associated with it, the unit cannot be deleted. All credentials for the lease associated with the unit must be handed in or blocked before deleting the unit.

WARNING: Reset or reconfigure the lock BEFORE removing it from the cloud-based software.

NOTE: See the Multi-Family Management System Configuration Application User Guide or the lock user guide for instructions on how to reset or reconfigure the lock.

To remove unit information, do the following:

1. Click **Configuration** and then click **Units & Buildings** on the left side of the screen. A list of units appears.
2. Click the **Trash Can** button next to the unit name to be removed.
   A Confirmation dialog box appears.
3. Click the **Confirm** button to remove the unit. Click the **Cancel** button to keep the unit.



EXPORT/IMPORT UNIT LIST

To export the unit list, do the following:

1. Click **Configuration** and then click **Units & Buildings** on the left side of the screen. A list of units appears.
2. Click the **Export** button to create a .CSV file that contains all of the Units.

It is possible to create a unit list using a .CSV file and then import it into the system.

A .CSV file template is available to use to ensure the .CSV file being used to import the unit information is correctly formatted. This allows for doors with only offline locks, not locks with updaters to be added to the system in a large group.

To download a sample .CSV file template, do the following:

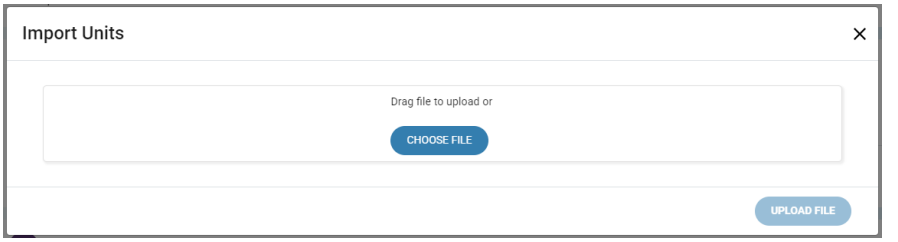
1. Click **Configuration** and then click **Units & Buildings** on the left side of the screen. A list of units appears.
2. Click the **CSV** button to download a .CSV file template.
   The template name is units_template.csv.

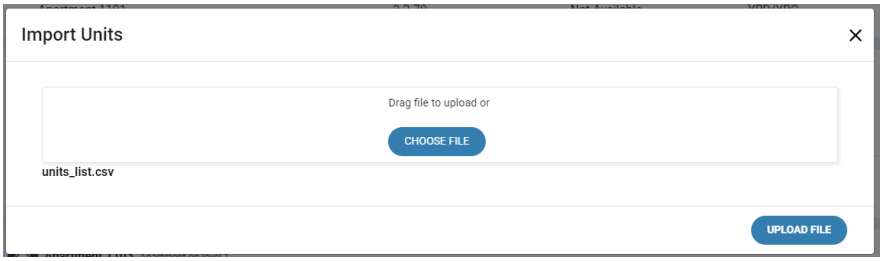
When the .CSV file template is filled in with the desired information, it can be imported to the system. Please note the *maximum file size for the .CSV file is 140KB*.

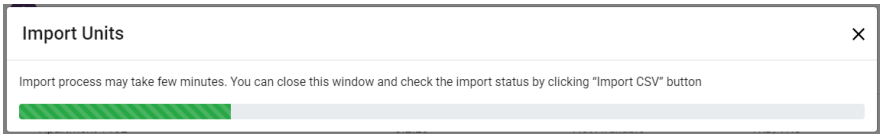
To import a unit list, do the following:

1. Click **Configuration** and then click **Units & Buildings** on the left side of the screen. A list of units appears.
2. Click the **Import** button to load a .CSV file that contains all of the Units.  The Import Units dialog box appears.
3. Select the file to upload using the drag-and-drop method or click the **Choose File** button to select the file.
4. When the file is selected, click the **Upload File** button. A status bar appears.
5. When the upload is complete a completion message appears. If there were no errors a success message is displayed. Click the **Close** button to close the message.

   If data errors, like duplicate data or incorrect data format were found during the upload, an error message is displayed with the incorrect data. It is possible to edit the incorrect data or discard the data through the error message.

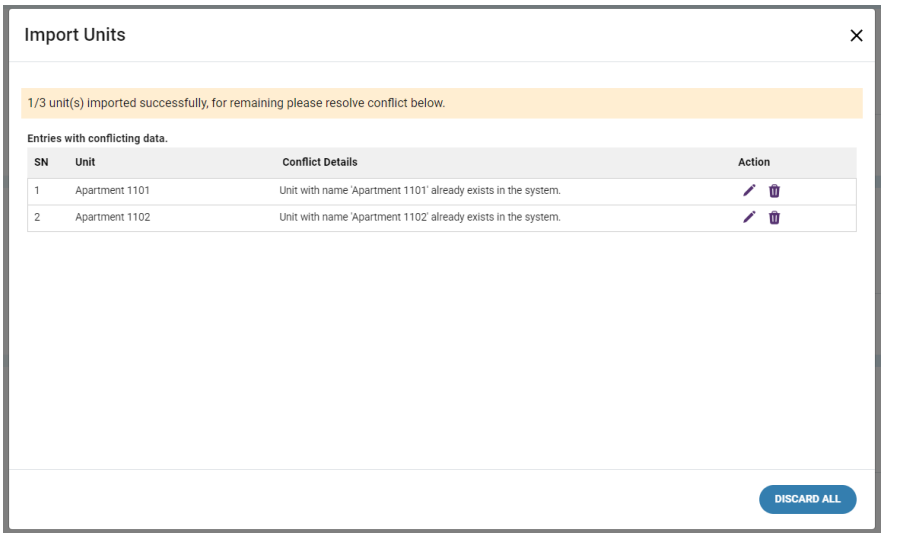


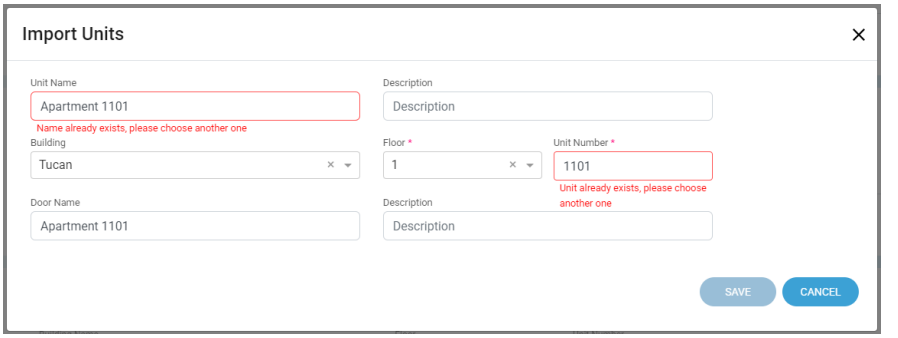




To edit the import errors, do the following:

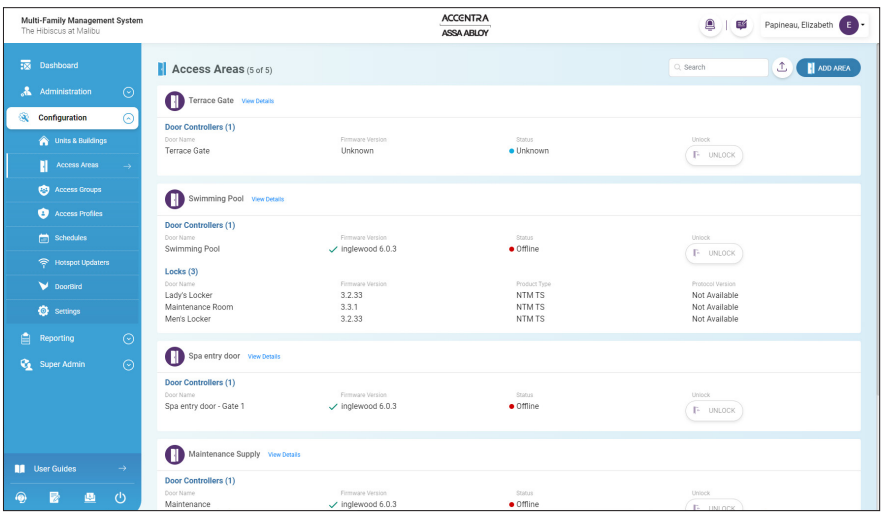
1. Click **Edit** button (pencil)in the Action column next to the desired error. The edit screen appears.
2. Correct the errors as noted in the error screen. When finished, click the **Save** button. To discard the changes, click the **Cancel** button.
3. To discard all errors, click the **Discard All** button.
4. When all errors have been resolved, a notification screens appears. Click **Close** to complete the process.





ACCESS AREAS

An Access Area is defined as an area where credential users will pass through on a routine basis that is not a Unit. It is a grouping of one or multiple doors. An Access Area may have none, one, or more online updaters and can also include offline locks. An online updater can control access to an opening requiring that credential holders present their card, fob, vehicle tage, or mobile credential to the updater in order to gain access. With physical credentials (cards, fobs, vehicle tags) this serves the purpose of both granting/denying access to the opening and updating the credential holder's access privileges. Requiring users to present their physical credential to the updater also retrieves audit trail information from the credential and delivers it to the Multi-Family Management System Cloud service. Mobile credentials are connected to the Multi-Family Management System Cloud service via a cellular or WiFi network and do not need to use an updater to update users' access privileges and deliver audit trail information to the Cloud service. A typical example of an Access Area with an online updater would be the front entrance of an apartment building.



The Access Areas configuration allows the administrator to define different access areas. Administrators can add an access area, display access area information, edit access area information, remove an access area and search for an access area.

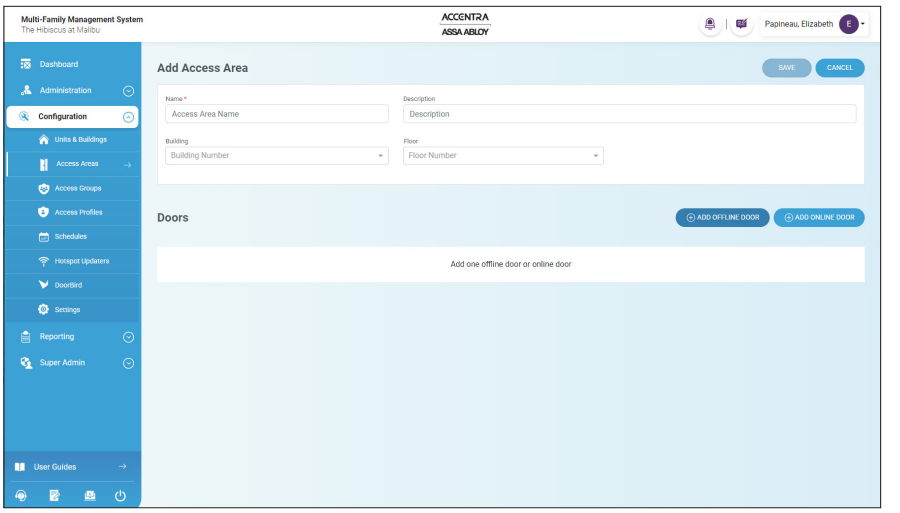
An online updater consists of two components: a wall/door mounted reader and a controller. The online updater is responsible for communicating securely with the Multi-Family Management System Cloud service to update physical credential holders' access privileges while also retrieving audit trail information from the physical credential and delivering it to the Cloud database. An online updater can also control access to an opening requiring that credential holders present their card, fob, vehicle tag, or mobile credential to the updater in order to gain access. The device can be used as a stand-alone enrollment station or as a single door controller.

ADD AN ACCESS AREA

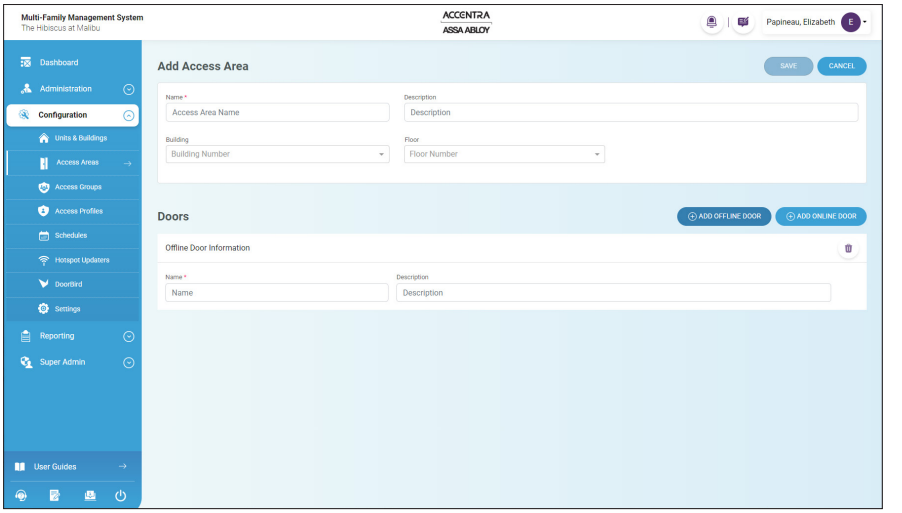
To add an access area, do the following:

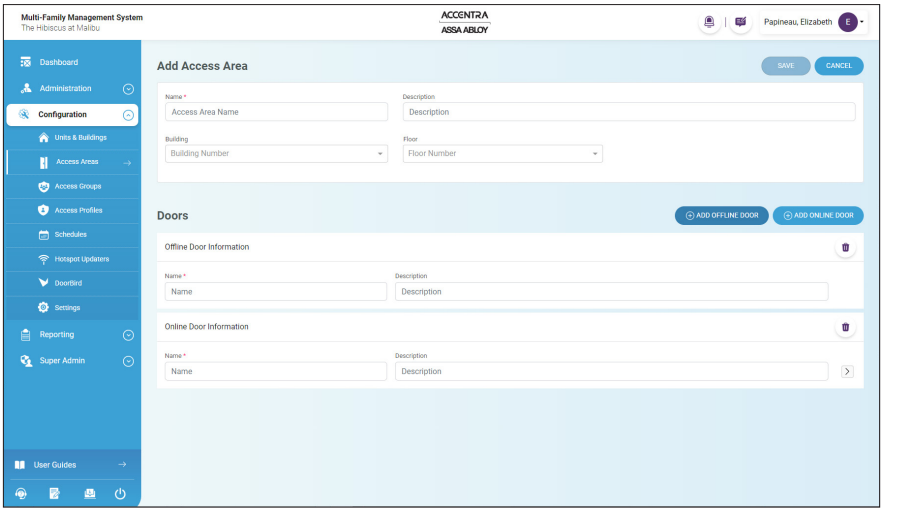
1. Click **Configuration** and then click Access Areas on the left side of the screen. A list of access areas appears.
2. Click the **Add Area** button above the list of access areas.
   

   The Add Access Area screen appears.
3. Enter an access area **Name** and **Description** Name is a required field, Description is optional. Select a **Building Name** and **Floor Number** if desired. If a Building Name is selected, a Floor Number is required.

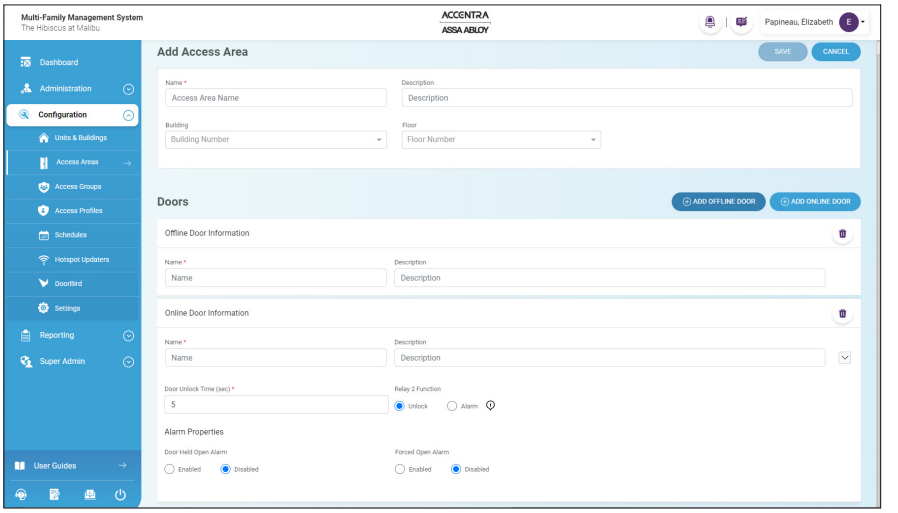


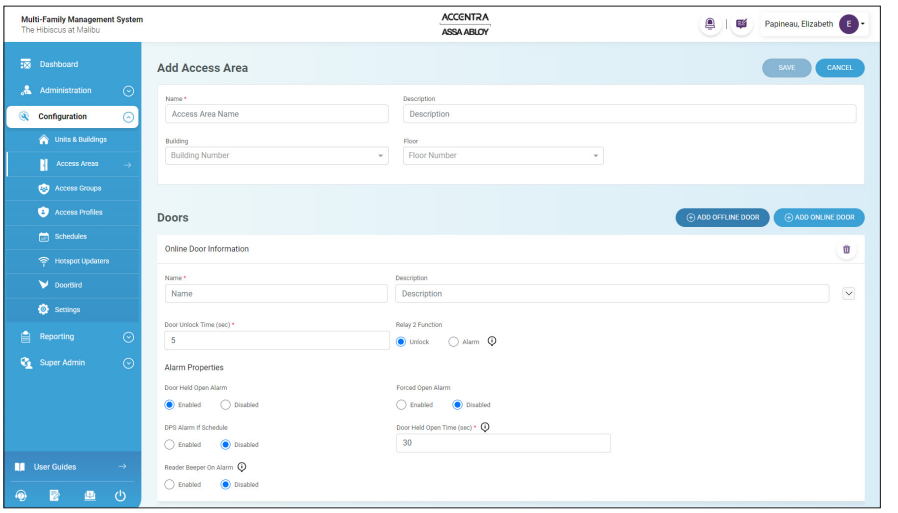
4. Each access area must have at least one door associated with it. To add an Offline Lock, click the **Add Offline Door** button, then enter the door **Name** and **Description**.
5. To add an Online Reader, click the **Add Online Reader** button. The Online Reader Information appears. Enter the **Name** and **Description**.
6. Click the **More Info** arrow on the right of the Description. More configuration fields appear.
   

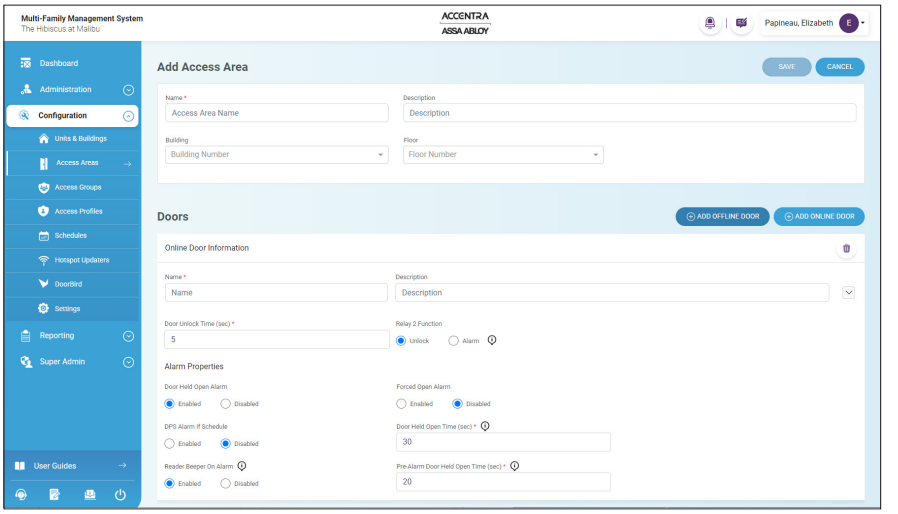


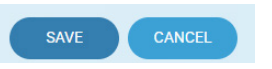


7. Enter the desired **Door Unlock Time** (in seconds) and select the action used with **Relay 2**.
8. Under Alarm Properties, if **Door Held Open Alarm** is enabled, alarm settings are displayed.
9. Enter the **Door Held Open Time** (in seconds). This is the amount of time the door can be held open before the alarm sounds.
10. Enable **Reader Beeper on Alarm** to allow the reader beeper to sound on alarm events. Enter the **Pre-Alarm Door Held Open Time**. This is the amount of time the door can be held open before the pre-alarm warning sounds. It must be less than the Door Held Open time. Select **Enable** or **Disable** for the other alarm settings.
11. To add more doors, click the **Add Offline Door** button or **Add Online Reader** button.
12. To delete doors, click the **Trash Can** button next to the Offline Lock information or Online Reader Information to be deleted.
13. Click the **Save** button to save the access area information. Click the **Cancel** button to discard the access area information and return to the Access Area screen.









NOTE: Online Updaters and offline door locks need to be commissioned into the system by the Certified Integrator.

SEARCH FOR AN ACCESS AREA

To search for an access area, do the following:

1. Click **Configuration** and then click **Access Areas** on the left side of the screen. A list of access areas appears.
2. Enter the search criteria in the **Search** box at the top of the Access Area list.

NOTE: Any text or part of text used in the Search field that is part of the area's name or description will appear in the Search results.

3. The search results are displayed automatically.

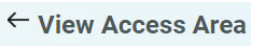
DISPLAY ACCESS AREA INFORMATION

To display access area information, do the following:

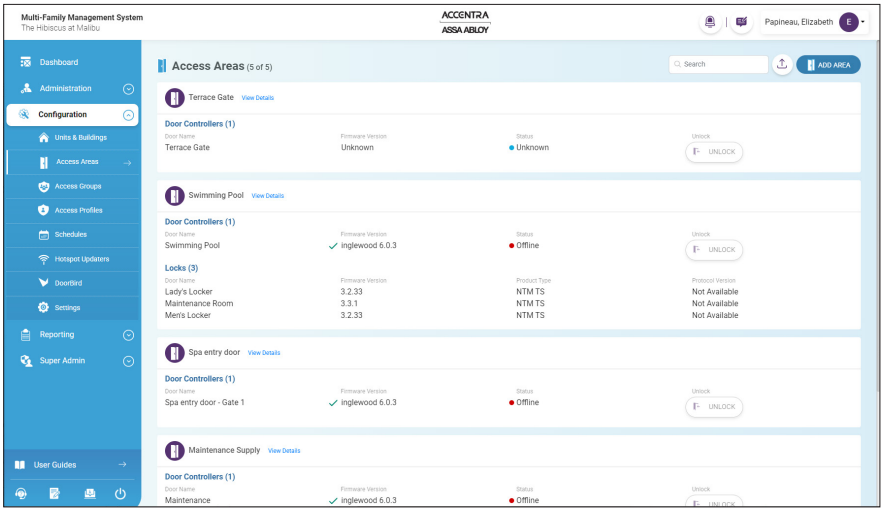
1. Click **Configuration** and then click **Access Areas** on the left side of the screen. A list of access areas appears.
2. Click on the **View Details** button next to the desired access area name.

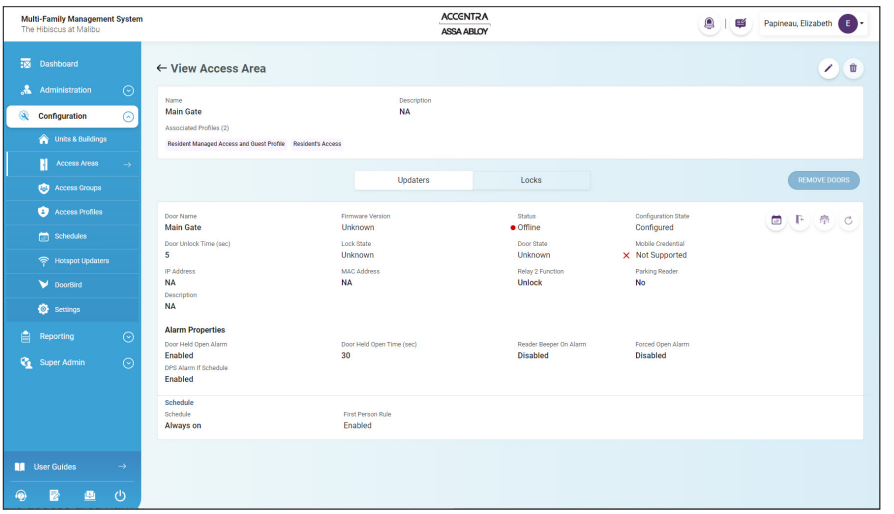
Use the Search function to find the desired access area name. The View Access Area screen appears.

3. To return to the access area list, click **Arrow** next to View Access Area in the upper left corner of the screen.



To remove a door from the access area, click the **Remove Doors** button.

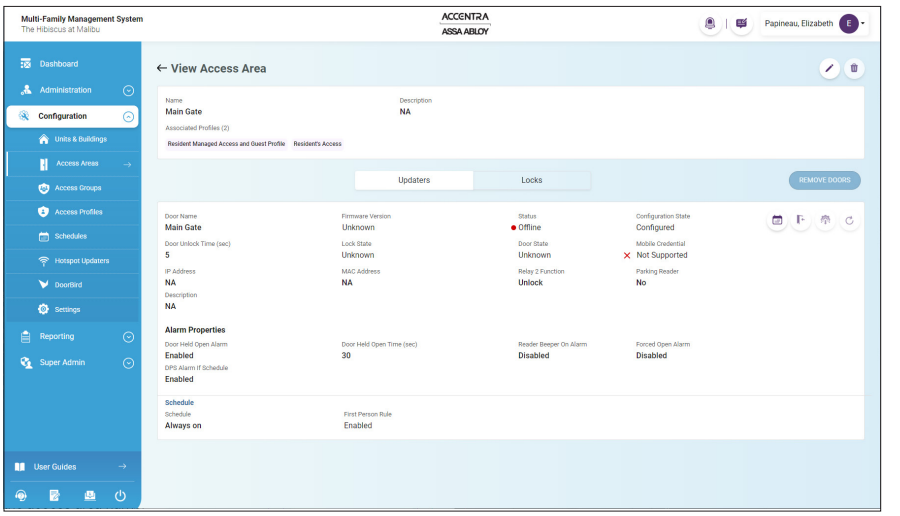




The View Access Area screen shows the access area name, description, and associated profiles. It can display a list of doors with updaters by clicking the **Updaters** button, or a list of doors with offline locks by clicking the **Locks** button.

UPDATERS

The Updaters tab displays information about the updater associated with a door. This includes:



- Firmware Version - the current firmware version installed in the updater. A green check mark indicates the firmware is up to date. A blue box and arrow indicates a newer version of the firmware is available.
- Status - the updater status, Online, Rebooting, Offline. A green dot indicates online, a blue dot indicates rebooting, a red dot indicates offline.
- Configuration State - the updater configuration state, Configured or Unconfigured.
- Door Unlock Time (sec) - the number of seconds the door will remain unlocked when Remote Unlock is used.
- Lock State - the current state of the lock, Locked or Unlocked.
- Door State - the state of the door, either open or closed, if a door position sensor is installed in the door.
- Mobile Credential - the support of mobile credentials, Supported or Not Supported. A green check mark indicates supported, a red X indicates not supported.
- IP Address - the updater IP address, if applicable
- MAC Address - the updater MAC address, if applicable
- Relay 2 Function - the selected function for Relay 2
- Description - the updater description, if applicable

Alarm Properties:

- Reader Beeper On Alarm - Enabled or Disabled, when enabled allows the reader beeper to sound during an alarm, also required for other alarm properties to be configured.
- Door Held Open Time (sec) - the number of seconds the door is detected open before maintenance alerts are generated to notify the door is open, if a door position sensor is installed in the door.
- DPS Pre Alarm (sec) - the number of seconds the door is detected open before the pre-alarm sounds. This number must be less than the Door Held Open Time. This alarm does not generate maintenance alerts.

- Forced Open Alarm - Enabled or Disabled, when enabled sounds the alarm and generates maintenance alerts to notify a credential was not used to open the door.
- DPS Alarm If Schedule - Enabled or Disabled, when enabled sounds the alarm if the door is held open even if the door is unlocked on a set schedule.

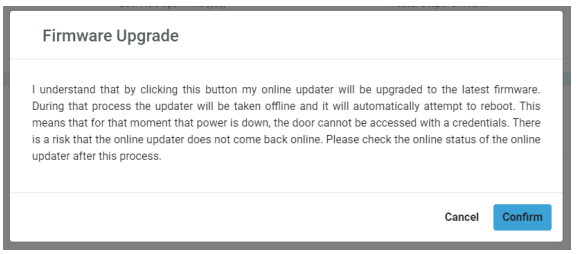
If a schedule has been attached to the door, the schedule information is displayed:

- Schedule - which schedule is selected for the door.
- First Person Rule - if the first person rule is in effect for the door, Enabled or Disabled.
- Remote Duration - the amount of time the door stays unlocked when a remote unlock is executed.

To change the access area schedule, click on the **Schedule** button next to the door information. See “Schedule Unlock” on page 41 for more information.

To remotely unlock a door in the access area, click on the **Unlock** button next to the door information. If the button is grey, this function is not available. The door stays unlocked for the amount of time set in Remote Duration.

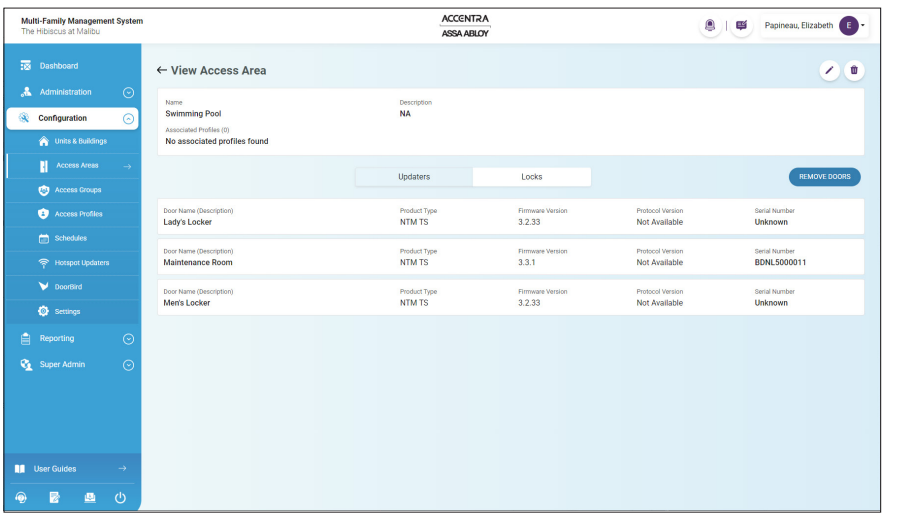
To upgrade the firmware, click on the **Firmware Upgrade** button next to the door information. If the button is grey, this function is not available. When clicked, a confirmation message appears. Click the **Confirm** button to upgrade to the latest firmware version.



To reboot the updater, click on the **Reboot** button next to the door information. A Reboot Updater message box appears. See “Reboot Updater” on page 40 for more information.

LOCKS

The Locks tab displays information about the offline locks associated with the access area. This includes:



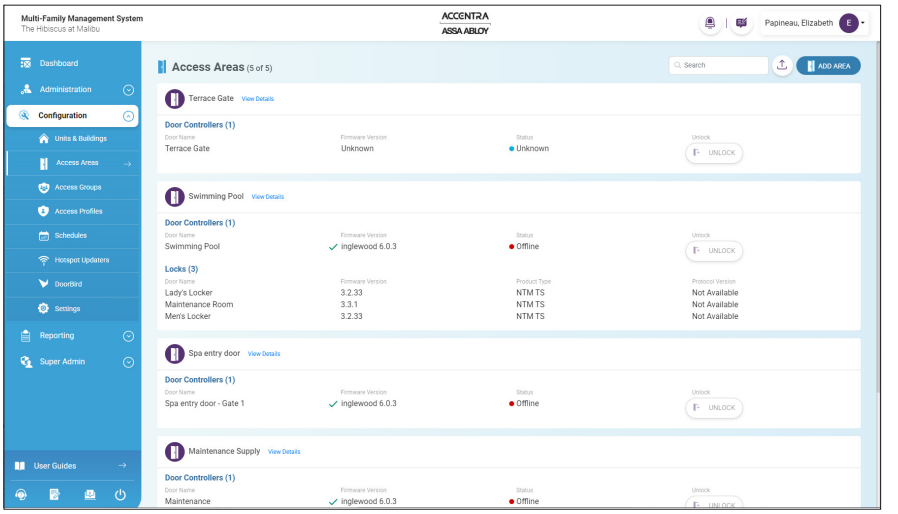
- Door Name/Description - name and description of the door.
- Product Type - the type of lock.
- Firmware Version - the version of firmware installed on the lock.
- Protocol Version - communication protocol between the locks, mobile application and system.
- Serial Number - the serial number of the lock if known.

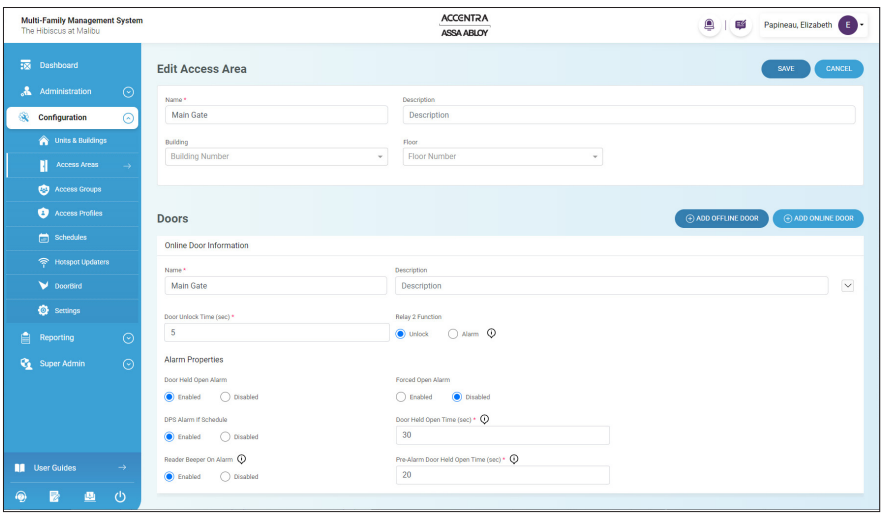
EDIT ACCESS AREA INFORMATION

To edit access area information, do the following:

1. Click **Configuration** and then click **Access Areas** on the left side of the screen. A list of access areas appears.
2. Click on **View Details** next to the desired access area name. Use the Search function to find the desired access area name. The View Access Area screen appears.
3. Click the **Edit Access Area** button (pencil). The Access Area Information screen displays editable text boxes. The Access Area **Name** and **Description** can be changed. A **Building** and **Floor Number** can be added or deleted. Individual door names and descriptions can also be changed or added. If the door is an Online Reader, click the **More Info** button to show the **Alarm Properties** and other settings that can be edited. Click the **Add Offline Door** button to add a new offline door, or click the **Add Online Reader** button to add a new online door.

4. Click the **Save** button to save the changes to the access area. Click the **Cancel** button to cancel any changes made. The screen returns to the View Access Area screen.





EXPORT ACCESS AREA LIST

To export the access area list, do the following:

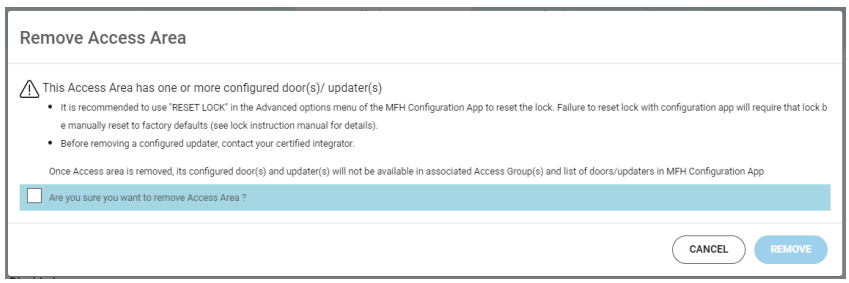
1. Click **Configuration** and then click **Access Areas** on the left side of the screen. A list of access areas appears.
2. Click the **Export** button to create a .CSV file that contains all of the Access Areas.

REMOVE AN ACCESS AREA

NOTE: If the access area includes a controller, the controller MUST be restored to defaults BEFORE deleting the access area. Contact your Certified Integrator for assistance.

To remove access area information, do the following:

1. Click **Configuration** and then click **Access Areas** on the left side of the screen. A list of access areas appears.
2. Click on **View Details** next to the desired access area name. Use the Search function to find the desired access area name. The View Access Area screen appears.
3. Click the **Trash Can** button. A Confirmation dialog box appears.



NOTE: If the access area has one or more configured doors/updater, the Remove Access Area button is disabled. To enable the button click the check box to confirm you want to remove the Access Area.

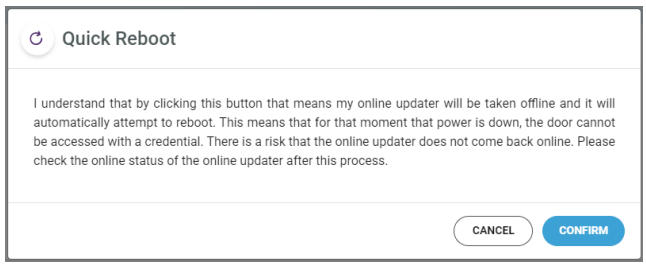
4. Click the **Remove** button to remove the access area. Click the **Cancel** button to keep the access area.

REBOOT UPDATER

Periodically it may be necessary to restart an online updater, such as when a new firmware version is available for download. ACCENTRA developers continuously provide new features and functionality to the Cloud service and it is recommended that all updaters have the latest firmware version to ensure the best user experience.

To reboot an updater, do the following:

1. Click **Configuration** and then click **Access Areas** on the left side of the screen. A list of access areas appears.
2. Click on the **View Details** button next to the desired access area name. Use the Search function to find the desired access area name. The View Access Area screen appears.
3. If the updater is configured, online (a green dot is displayed in the door information), and not already in an unlocked state, the **Unlock** and **Reboot** buttons are enabled (not grey).
4. Click the **Reboot** button. 
   A confirmation dialog box appears.
5. Click **Confirm** in the dialog box. The updater status changes to rebooting.
6. After approximately 20-25 minutes, refresh the web page. When the updater has finished rebooting, the status changes to Online.



NOTE: When the updater is rebooting, access at the opening may be limited and credentials cannot be updated. It is strongly recommended that user discretion be used when choosing the time to reboot and that updaters be restarted one at a time. The controller will search for any new firmware version available and automatically download and install the latest version. During a firmware upgrade, the boot process can take up to 20-25 minutes depending on the connection speed of the Internet Service Provider.

NOTE: If the unit was rebooted in order to download a new firmware update, the new firmware version will appear in the door information area.

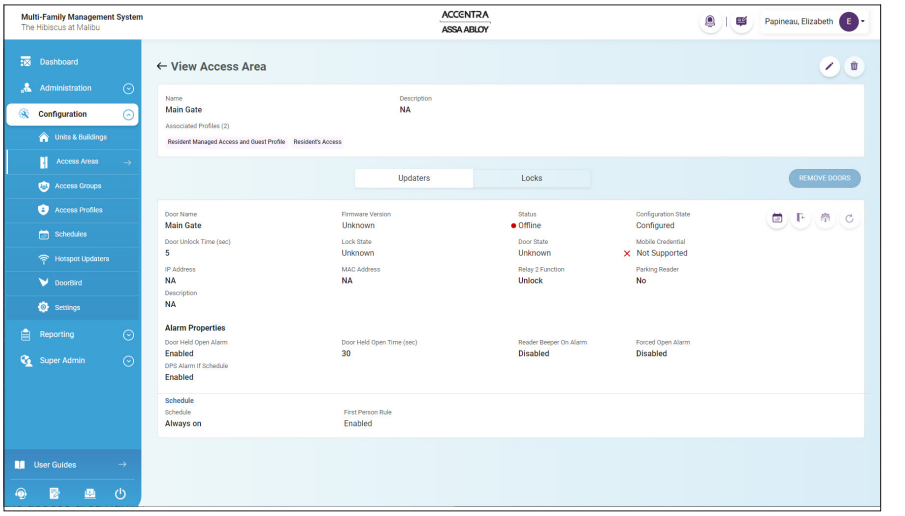
SCHEDULE UNLOCK

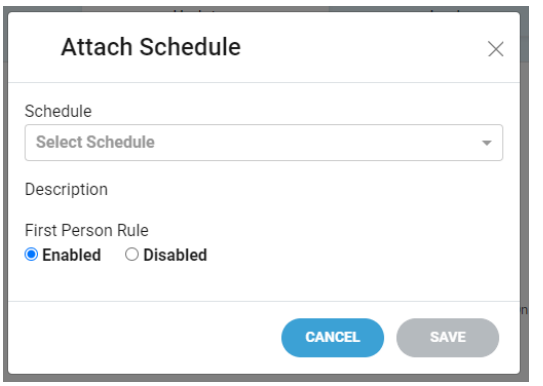
If the updater is controlling access to an opening, it is possible to automatically unlock the door according to a defined schedule. (See “Schedules” on page 51 to learn how to create and manage schedule templates.) In addition to scheduled unlock, there is an optional feature known as the First Person Rule. With this feature enabled, the unlock schedule will not activate until a user with a valid credential first presents their card, fob or mobile credential to the updater.

To **ADD** a schedule to an updater, do the following:

1. Click **Configuration** and then click **Access Areas** on the left side of the screen. A list of access areas appears.
2. Click on the **View Details** button next to the desired access area name. Use the Search function to find the desired access area name. The View Access Area screen appears.
3. Click the **Updaters** tab to view the updater information.
4. Click the **Schedule** button. The Attach Schedule dialog box appears.

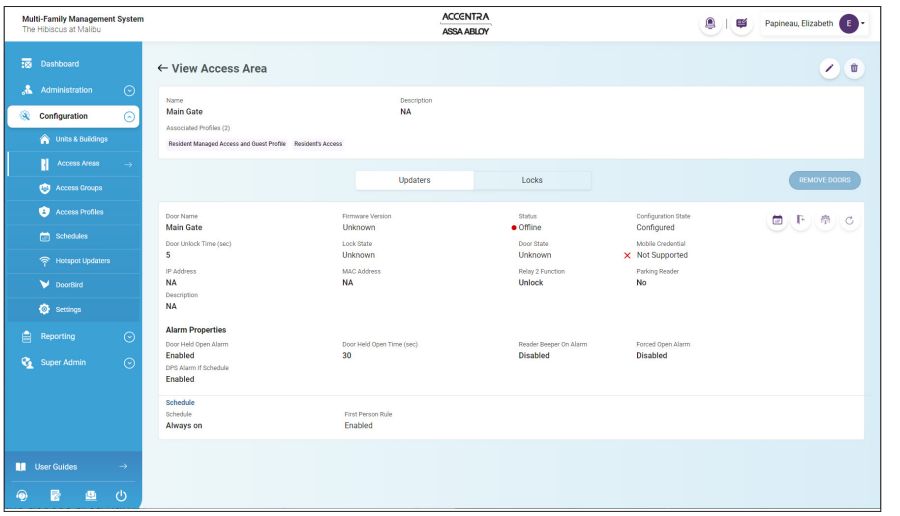
5. Select a saved schedule from the **Schedule** drop-down list.
6. Under **First Person Rule**, select the **Enabled** radio button to turn the feature on, select the **Disabled** radio button to turn the feature off.
7. Click the **Save** button to save the schedule. Click the **Cancel** button to discard the schedule.



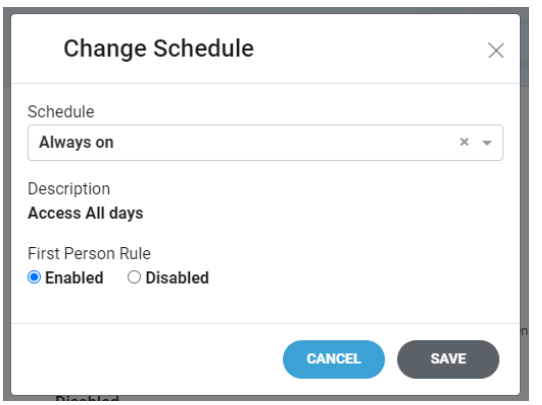


To **CHANGE** or **REMOVE** a schedule from an updater, do the following:

1. Click **Configuration** and then click **Access Areas** on the left side of the screen. A list of access areas appears.
2. Click on the **View Details** button next to the desired access area name. Use the Search function to find the desired access area name. The View Access Area screen appears.
3. Click the **Updaters** tab to view the updater information.
4. Click the **Schedule** button. The Change Schedule dialog box appears.



5. Select a saved schedule from the **Schedule** drop-down list. Or select **No Schedule** from the **Schedule** drop-down list to remove the schedule. If No Schedule is selected, all other information sections disappear.
6. Under **First Person Rule**, select the **Enabled** radio button to turn the feature on, select the **Disabled** radio button to turn the feature off.
7. Click the **Save** button to save the schedule changes. Click the **Cancel** button to discard the schedule changes.



NOTE: If an updater is in an offline state, any changes to the schedule (adding new schedule, modifying existing schedule) will NOT take effect until the updater returns to an online state. However, the updater will continue to unlock in the offline state using the last schedule attached (if there is one).

ACCESS PROFILES

An Access Profile is defined as a set of access permissions and defined schedules assigned to users based on their particular role. Credentials handed out to associated users automatically contain the necessary access permissions as defined in the access profile. Examples of Access Profiles might be “Property Management” or “Custodial Staff”.

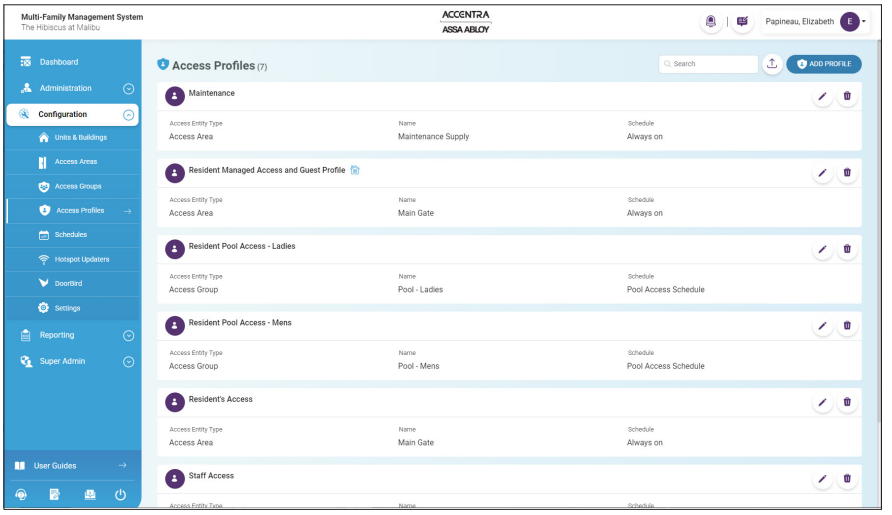
The Access Profiles configuration allows the administrator to define different access profiles. Administrators can add an access profile, display access profile information, edit an access profile, remove an access profile and search for an access profile. Access profiles can also be used by Resident Managed Access™ (RMA) if allowed by the administrator. By default, when access profiles are created they are extended to RMA.

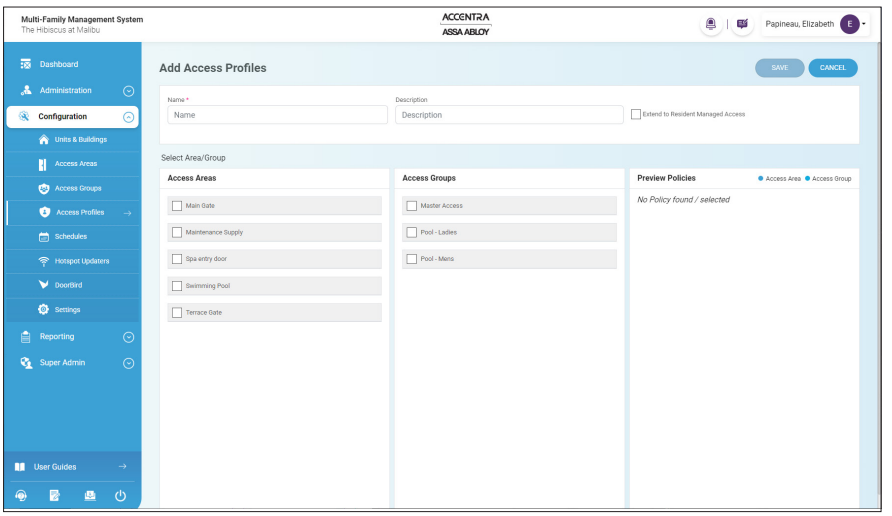
ADD AN ACCESS PROFILE

To add an access profile, do the following:

1. Click **Configuration** and then click **Access Profiles** on the left side of the screen. A list of access profiles appears.
2. Click the **Add Profile** button above the list of access profiles. The Add Access Profile screen appears.

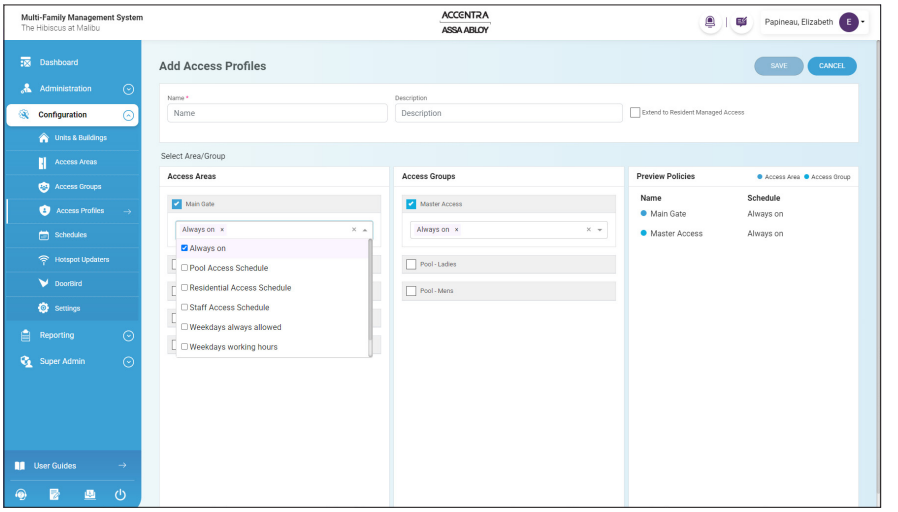
3. Enter an access profile **Name**. The Name is a required field. Enter a Description if desired.
4. To allow this profile to be used in Resident Managed Access™, leave the **Extend to Resident Managed Access** check box selected. Click the check box to remove access from RMA.
5. Select an access area and/or access group by clicking the check box next to the area or group name.
6. If an **Access Area** was selected, select one schedule from the Schedule drop-down below the area name. (See “Create New Schedule” on page 52.)





If an **Access Group** was selected, select the desired schedule from the Schedule drop-down below the group name.

7. To remove an Access Area or Access Group, click the check-box next to the area or group name to deselect.
8. Click the **Save** button to save the changes to the access profile. Click the **Cancel** button to cancel any changes made. The screen returns to the Access Profiles screen.



SEARCH FOR AN ACCESS PROFILE

To search for an access profile, do the following:

1. Click **Configuration** and then click **Access Profiles** on the left side of the screen. A list of access profiles appears.
2. Enter the search criteria in the **Search** box at the top of the Access Profile list.

NOTE: Any text or part of text used in the Search field that is part of the profile's name or description will appear in the Search results.

3. The search results are displayed automatically.

EXPORT ACCESS PROFILE LIST

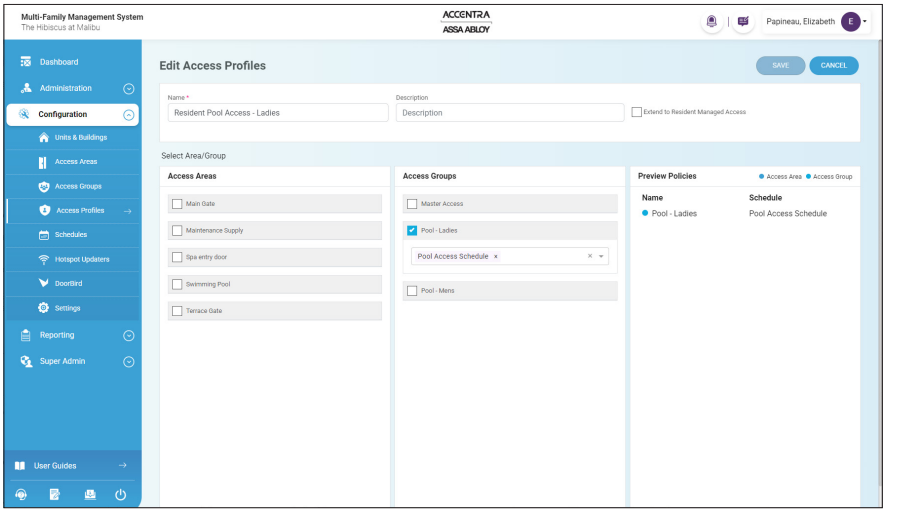
To export the access profile list, do the following:

1. Click **Configuration** and then click **Access Profile** on the left side of the screen. A list of access profiles appears.
2. Click the **Export** button to create a .CSV file that contains all of the Access Profiles.

EDIT ACCESS PROFILE INFORMATION

To edit access profile information, do the following:

1. Click **Configuration** and then click **Access Profiles** on the left side of the screen. A list of access profiles appears.



2. Click the **Edit Access Profile** button (pencil).

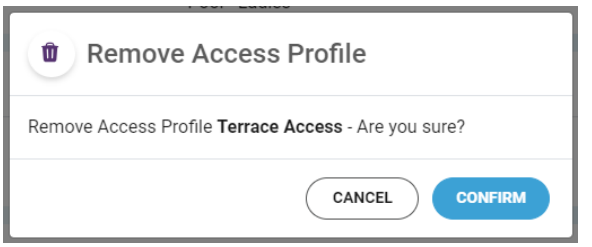
The Access Profile Information screen displays editable text boxes. The Access Profile name and description can be changed. In the Access Policy definition the access area, or access group, and the associated schedule can be changed or added. The Access Profile can be extended to Resident Managed Access™ by clicking the check box.

3. Click the **Save** button to save the changes to the access profile. Click the **Cancel** button to cancel any changes made. The screen returns to the Access Profiles screen.

REMOVE AN ACCESS PROFILE

To remove access profile information, do the following:

1. Click **Configuration** and then click **Access Profiles** on the left side of the screen. A list of access profiles appears.
2. Click the **Trash Can** button next to the access profile name to remove. A Confirmation dialog box appears.



3. Click the **Confirm** button to remove the access profile. Click the **Cancel** button to keep the access profile.

NOTE: The access profile cannot be deleted if it is assigned to a user. A warning will appear in this instance.

ACCESS GROUPS

An Access Group is a user defined group of locks and/or online updaters. An Access Group can contain any number of locks belonging to the same system. One lock can belong to a maximum of 16 different groups, and different groups can be included in an access profile (See “Access Profiles” on page 43). Access Groups are a convenient way to assign user access to a large number of openings without having to select each lock individually. An example of an Access Group would be “First Floor” which could include all or selected openings on the first floor of a building.

The Access Groups configuration allows the administrator to define different access groups. Administrators can add an access group, display access group information, edit an access group, remove an access group, and search for an access group.

IMPORTANT: In order for a lock to be a member of an Access Group, the lock must be assigned to the access group using the cloud-based software prior to being configured with the Multi-Family Management System Configuration app.

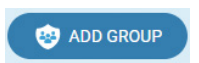
To change the Access Group the lock is a part of, the lock must be updated using the Multi-Family Management System Configuration app after changes are made in the software.

Please see the ACCENTRA Multi-Family Management System Configuration app user guide for steps to update the lock.

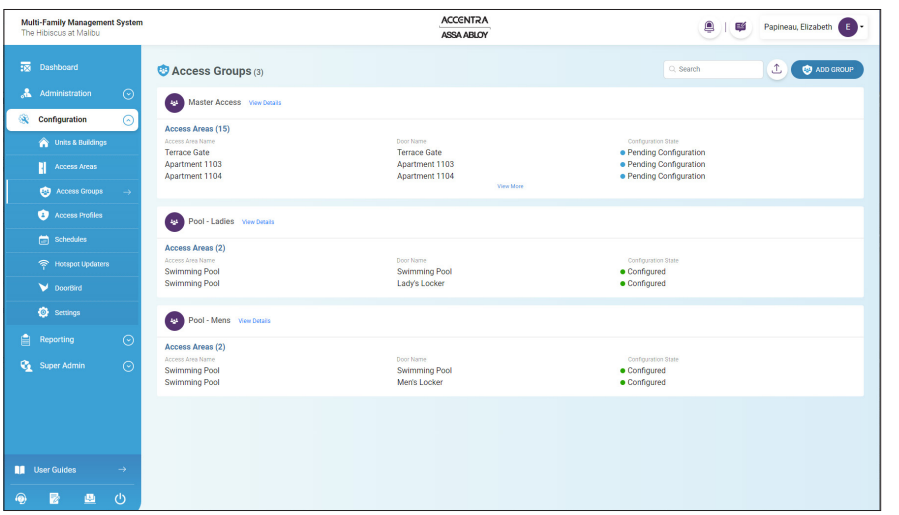
ADD AN ACCESS GROUP

To add an access group, do the following:

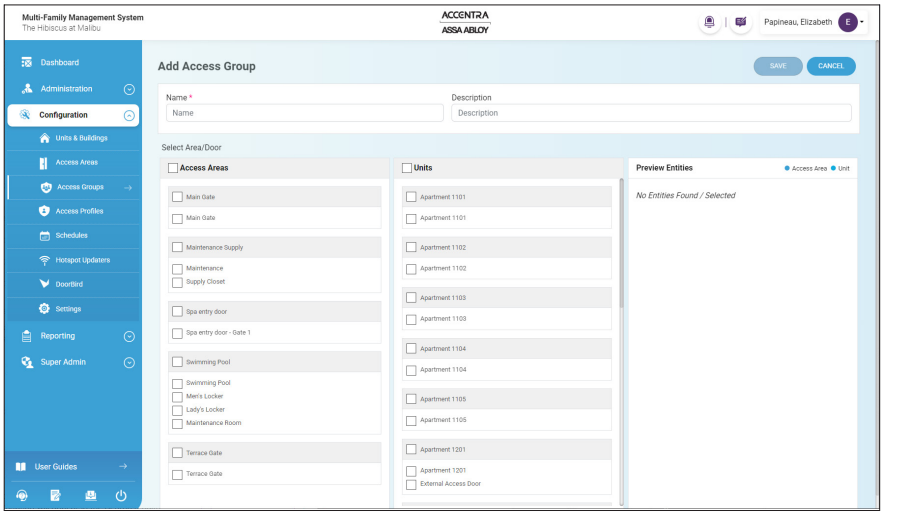
1. Click **Configuration** and then click **Access Groups** on the left side of the screen. A list of access groups appears.
2. Click the **Add Group** button above the list of access groups.



The Add Access Group screen appears.



3. Enter an access group **Name** and **Description**. Name is a required field, Description is optional.
4. Select an access area and/or unit by clicking the check box next to the area or unit name. Or select all access ares and/or units by clicking on the check box at the top of the list.
   If an access area is already part of 16 access groups, that access area will not be able to be selected.



5. To remove an access area or unit, click the check-box next to the area or unit name to deselect.
6. Click the **Save** button to save the changes to the access group. Click the **Cancel** button to cancel any changes made. The screen returns to the Access Groups screen.

SEARCH FOR AN ACCESS GROUP

To search for an access group, do the following:

1. Click **Configuration** and then click **Access Groups** on the left side of the screen. A list of access groups appears.
2. Enter the search criteria in the **Search** box at the top of the Access Groups list.

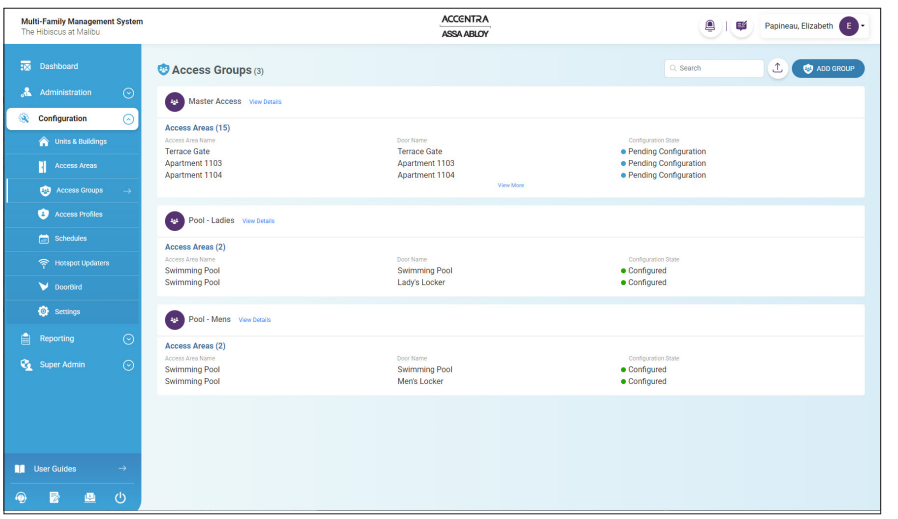
NOTE: Any text or part of text used in the Search field that is part of the profile's name or description will appear in the Search results.

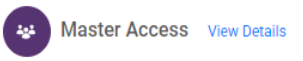
3. The search results are displayed automatically.

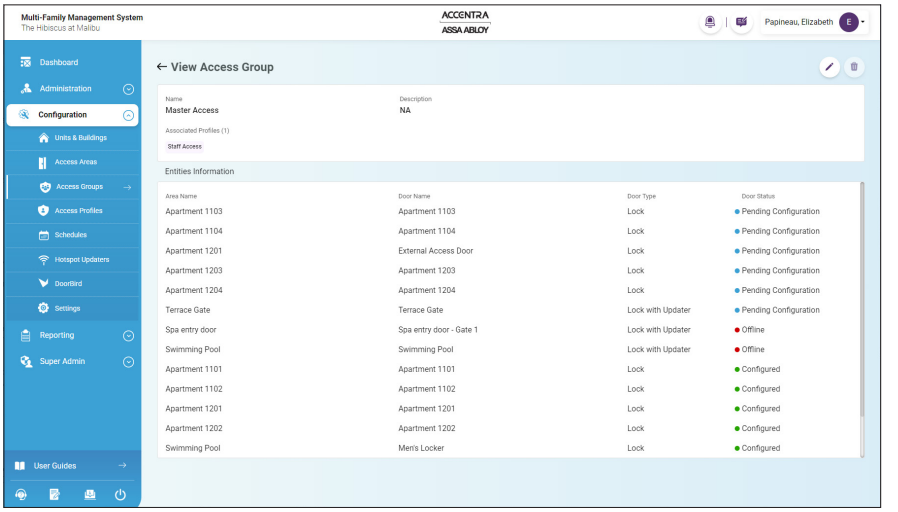
DISPLAY ACCESS GROUP INFORMATION

To display access group information, do the following:

1. Click **Configuration** and then click **Access Groups** on the left side of the screen. A list of access groups appears.
2. Click on the **View Details** button next to the desired access group name. Use the Search function to find the desired access group name. The View Access Group screen appears.
3. To return to the access group list, click **Arrow** next to View Access Group in the upper left corner of the screen.







The View Access Group screen shows the access group name, description, and associated profiles. It displays the area names, door names, door types, and door status associated with the access group.

NOTE: Adding or removing online updaters from an Access Group, after locks and updaters have been configured, DOES NOT require updating the lock with the mobile app. Adding or removing offline locks from an Access Group DOES require updating the affected locks with the mobile configuration app.

EXPORT ACCESS GROUP LIST

To export the access group list, do the following:

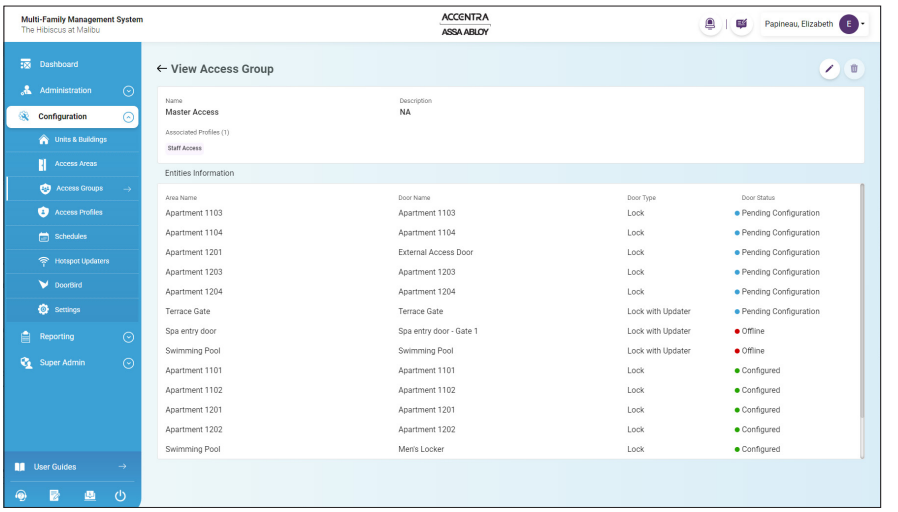
1. Click **Configuration** and then click **Access Groups** on the left side of the screen. A list of access groups appears.
2. Click the **Export** button to create a .CSV file that contains all of the Access Groups.

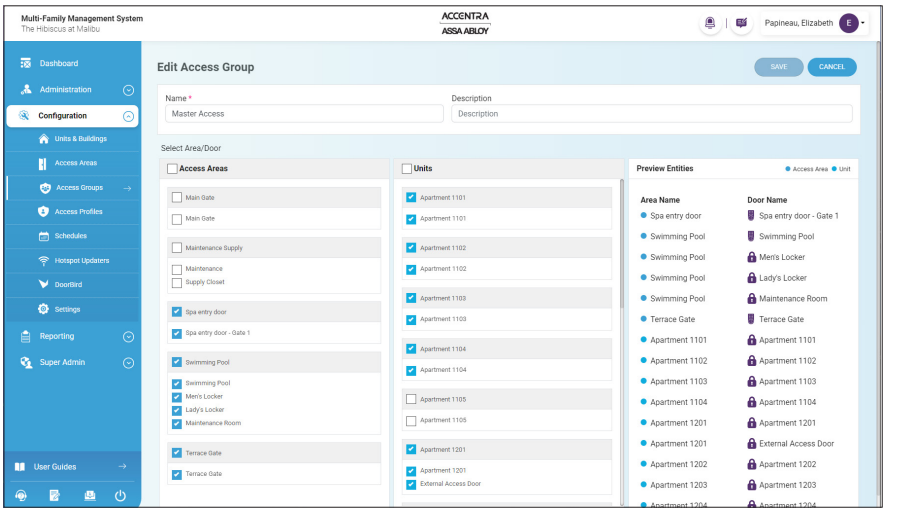
EDIT ACCESS GROUP INFORMATION

To edit access group information, do the following:

1. Click **Configuration** and then click **Access Groups** on the left side of the screen. A list of access groups appears.
2. Click on the **View Details** button next to the desired access group name. Use the Search function to find the desired access group name. The View Access Group screen appears.
3. Click the **Edit Access Group** button (pencil).

   The Edit Access Group screen displays editable text boxes. The Access Group name and description can be changed. Access Areas and Units can be selected or unselected.
4. Click the **Save** button to save the changes to the access area. Click the **Cancel** button to cancel any changes made. The screen returns to the View Access Group screen.

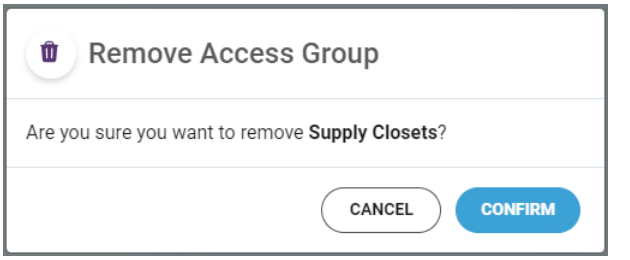




REMOVE AN ACCESS GROUP

To remove access group information, do the following:

1. Click **Configuration** and then click **Access Groups** on the left side of the screen. A list of access groups appears.
2. Click on **View Details** next to the desired access group name. Use the Search function to find the desired access group name. The View Access Group screen appears.
3. Click the **Trash Can** button.
   A Confirmation dialog box appears.



NOTE: If the access group is related to an access profile, the Remove Access Group button is disabled. To enable the button all associated access profiles must be removed first (See “Access Profiles” on page 43).

4. Click the **Confirm** button to remove the access group. Click the **Cancel** button to keep the access group.

SCHEDULES

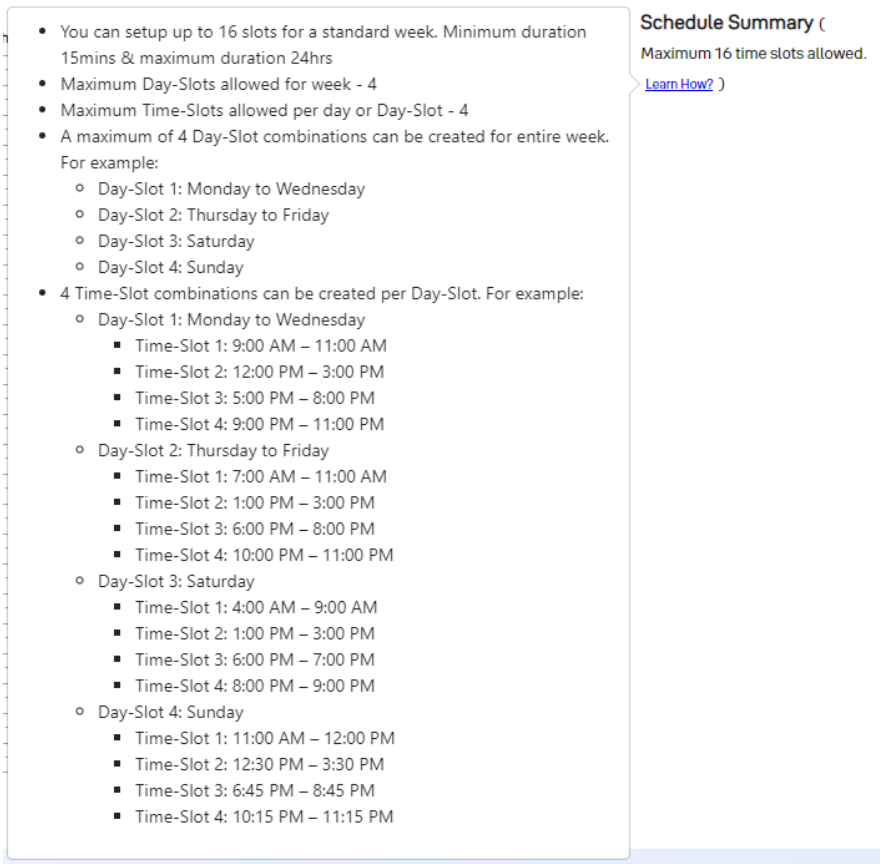
A schedule is a method of setting time or day based access privileges for a credential holder to a unit or area. Schedule configuration is used to create new schedules and manage schedules. Schedules can be set up to manage door access automatically and multiple doors can use the same schedule.

Schedules are defined by Day-Slot and Time-Slot.

A Day-Slot is the selected day or days of the week access is allowed. A total of four (4) Day-Slots are allowed per schedule.

A Time-Slot is the specific time range during a day where access is allowed. The minimum amount of time is 15 minutes, the maximum is 24 hours. A total of four (4) Time-Slots are allowed per Day-Slot. A single day cannot be part of more than four (4) Time-Slots.

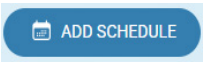
There are several default schedules defined in the system: Always on, Office hours, Weekdays always allowed, Weekdays working hours, Weekends always allowed. These schedules can be edited so that they provide access during the desired times and days.



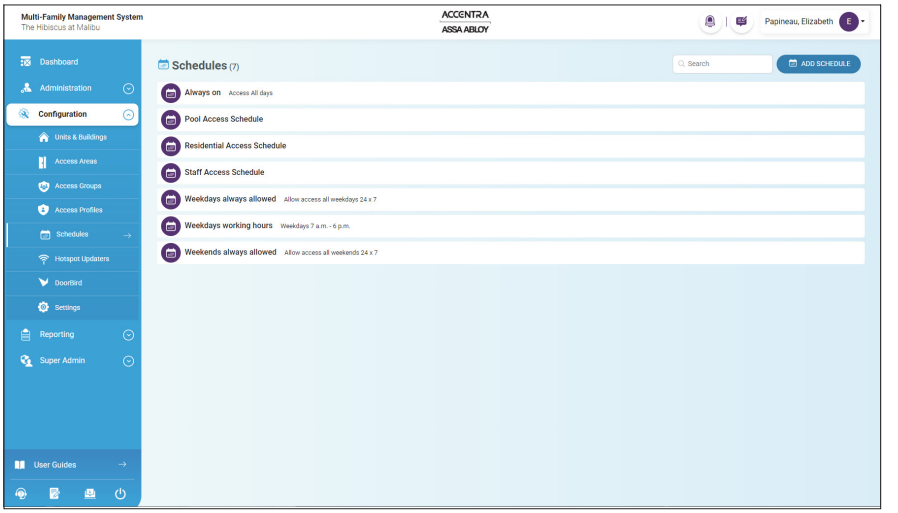
CREATE NEW SCHEDULE

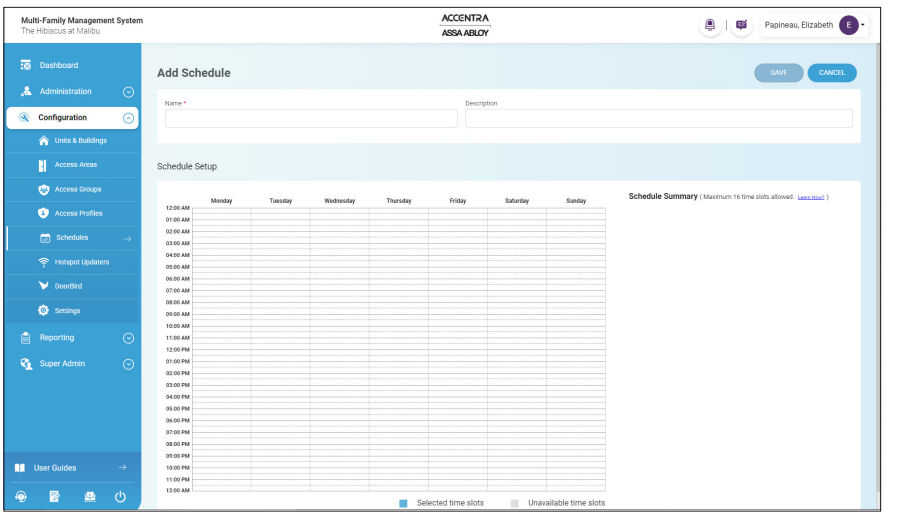
To create a new schedule, do the following:

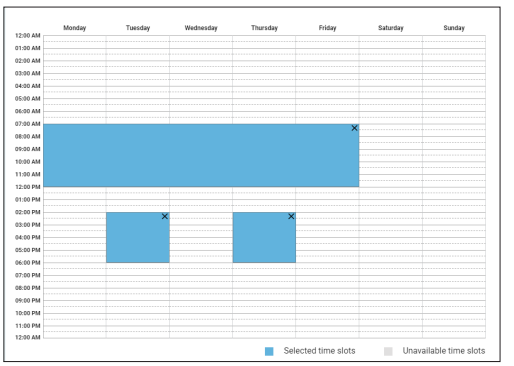
1. Click **Configuration** and then click **Schedules** on the left side of the screen. The Schedules screen appears.
2. Click the **Add Schedule** button.

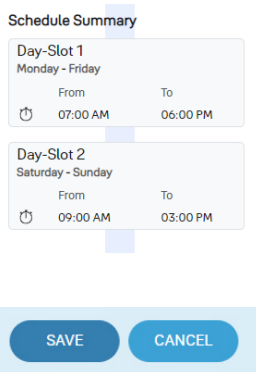


   The Add Schedule screen appears.
3. Enter a **Schedule Name** and a **Description**. Name is a required field, Description is optional.
4. Click in the table cell on the day and time desired to allow access. Drag the cursor across the table for days and times to select a larger access interval. Individual days and times during the days can also be selected.
   To delete a selection, click the black **X** in the upper corner of the selection.
5. Review the details and selected time slots in the Schedule Summary on the right side of the screen.
   If the schedule settings are correct, click the **Save** button. Click the **Cancel** button to cancel any changes made. The screen returns to the Schedules screen.









SEARCH FOR SCHEDULES

To search for a schedule, do the following:

1. Click **Configuration** and then click **Schedules** on the left side of the screen. The Schedules screen appears.
2. Enter the Search criteria in the **Search** box at the top of the schedule list.

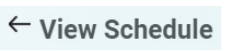
NOTE: Any text or part of text used in the Search field that is part of the profile's name or description will appear in the Search results.

3. The search results are displayed automatically.

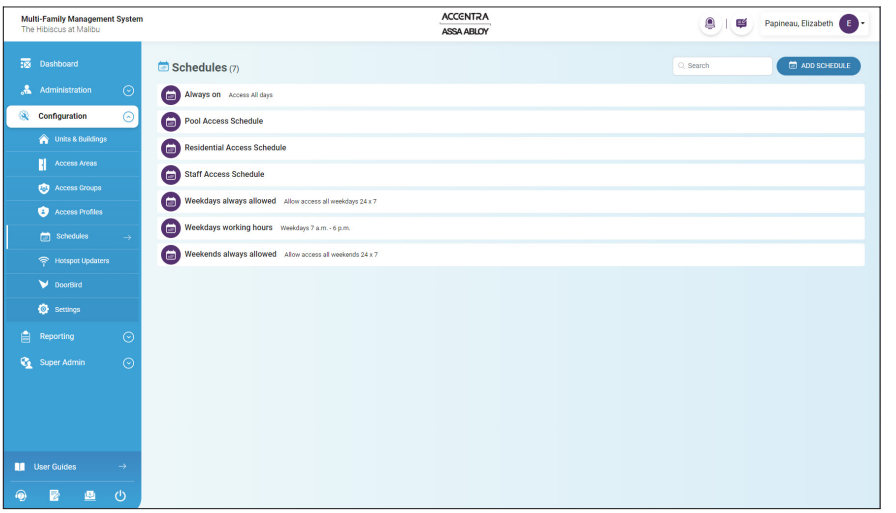
DISPLAY SCHEDULE INFORMATION

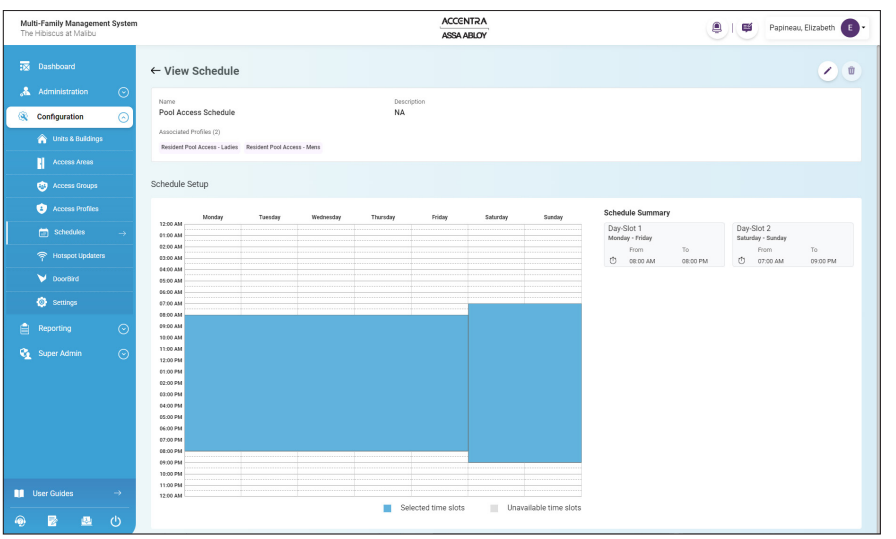
To display schedule information, do the following:

1. Click **Configuration** and then click **Schedules** on the left side of the screen. The Schedules screen appears.
2. Click on the desired schedule name, or use the Search function to find the desired schedule name. The View Schedule screen appears.
3. To return to the schedules list, click **Arrow** next to View Schedule in the upper left corner of the screen.



The View Schedule screen shows the schedule name, description, and associated profiles. It displays the schedule summary and the schedule setup blocks.



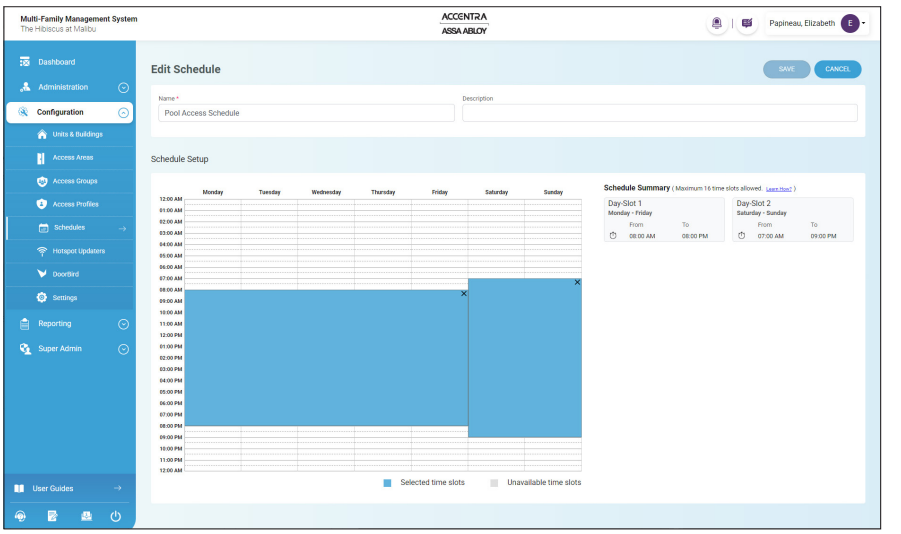


EDIT SCHEDULE

To edit a schedule, do the following:

1. Click **Configuration** and then click **Schedules** on the left side of the screen. The Schedules screen appears.
2. Click on the desired schedule name, or use the Search function to find the desired schedule name. The View Schedule screen appears.
3. Click **Edit Schedule** (pencil) on the right side of the screen.

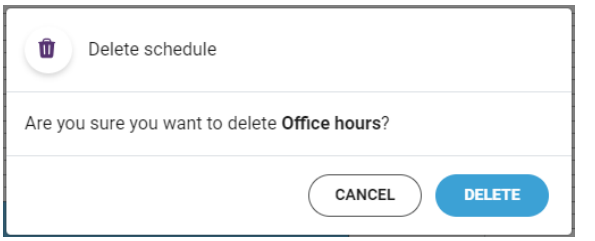
   The screen changes to allow editing of the schedule name, description and details.
   Note that to change the times periods, existing time periods may have to be deleted first and new time periods added.
4. Click the **Save** button to save the changes to the schedule. Click the **Cancel** button to cancel any changes made. The screen returns to the View Schedule screen.



DELETE SCHEDULES

To delete a schedule, do the following:

1. Click **Configuration** and then click **Schedules** on the left side of the screen. A list of schedules appears.
2. Click on the desired schedule name. Use the Search function to find the desired schedule name. The View Schedule screen appears.
3. Click the **Trash Can** button. 
   A Confirmation dialog box appears.



NOTE: If the schedule has an associated access profile, the Delete Schedule button is disabled. To enable the button all associated access profiles must be removed first (See "Access Profiles" on page 43).

4. Click the **Delete** button to remove the schedule.
   Click the **Cancel** button to keep the schedule.

IMPORTANT:
A single physical credential should have no more than six (6) different schedules. For example, if an access profile is created with four (4) access areas and four (4) different schedules, there are only two more schedules that can be assigned to the physical credential. More than six (6) schedules uses a significant amount of the physical credential's memory and can affect read time at the door.

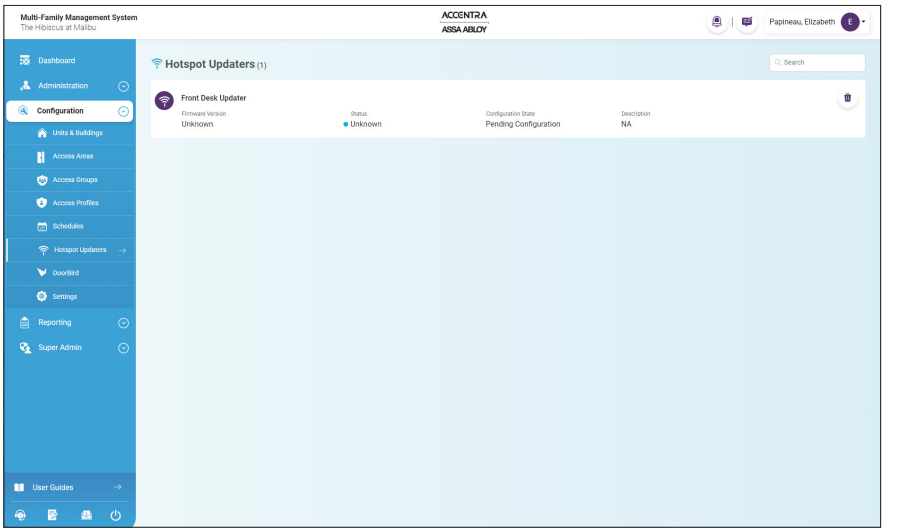
There is no issue creating many more schedules and assigning them to other physical credentials or cardholders.

Each user is allowed to have a maximum of 15 schedules assigned. If the user has multiple schedules that overlap times for a door, the user will have access to the door for the maximum amount of time available. For example: if door Schedule 1 is 8am-3pm and door Schedule 2 is 12pm-7pm, the user can access the door from 8am-7pm.

HOTSPOT UPDATERS

Unlike an updater in an access area, a Hotspot Updater does not control access to an opening. An example of a standalone Hotspot Updater is one on a leasing agent's desk for the purpose of updating or handing out/handing in credentials.

The Hotspot Updaters configuration allows the administrator to define different hotspot updaters. Administrators can display hotspot updater information, remove a hotspot updater and search for a hotspot updater. **Existing hotspot updaters created in previous software versions cannot be edited and new hotspot updaters cannot be added.**



SEARCH FOR A HOTSPOT UPDATER

To search for a hotspot updater, do the following:

1. Click **Configuration** and then click **Hotspot Updaters** on the left side of the screen. A list of hotspot updaters appears.
2. Enter the search criteria in the **Search** box at the top of the Hotspot Updaters list.

NOTE: Any text or part of text used in the Search field that is part of the profile's name or description will appear in the Search results.

3. The search results are displayed automatically.

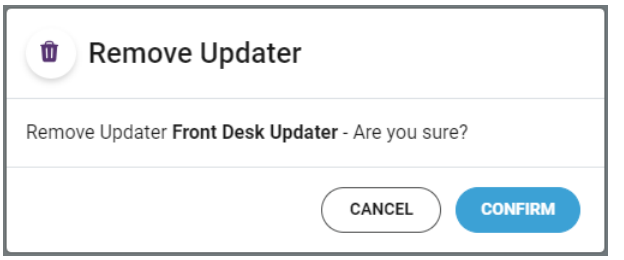
REMOVE A HOTSPOT UPDATER

To remove a hotspot updater, do the following:

1. Click **Configuration** and then click **Hotspot Updaters** on the left side of the screen. A list of hotspot updaters appears.
2. Click the **Trash Can** button next to the name of the desired hotspot updater.

Use the Search function to find the desired schedule name. A Confirmation dialog box appears.

3. Click the **Confirm** button to remove the hotspot updater. Click the **Cancel** button to keep the hotspot updater.



DOORBIRD

DoorBird is a door intercom system that allows residents to see visitors, talk to visitors, and unlock the door using their mobile device from anywhere. Integrating a DoorBird system into the Multi-Family Management System is done using the Multi-Family Management System screens and the DoorBird mobile app.

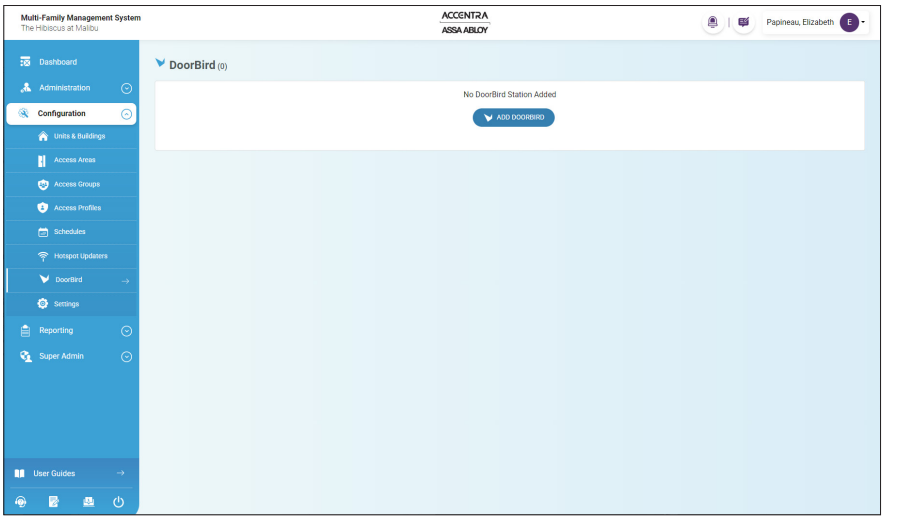
INSTALL AND INTEGRATE DOORBIRD

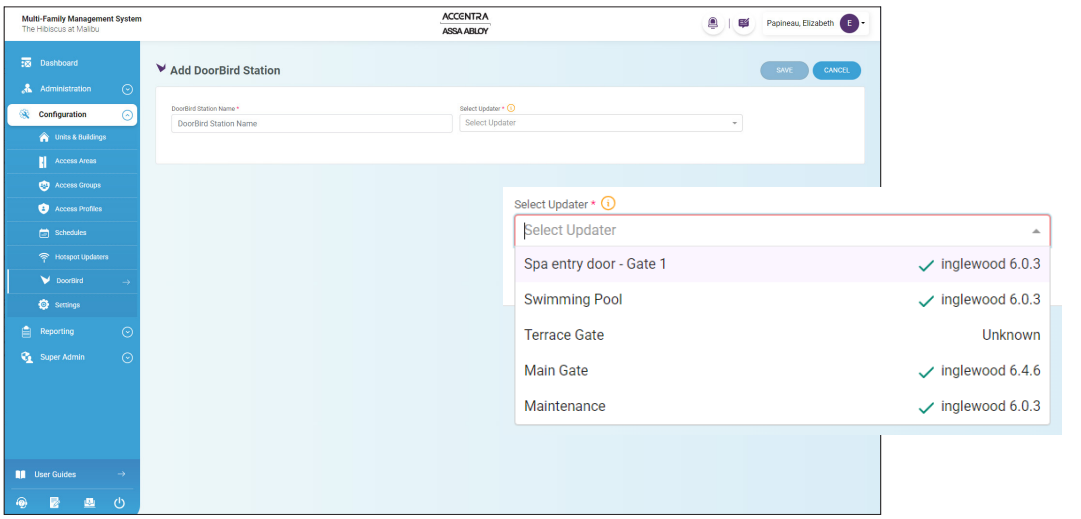
Ensure the DoorBird hardware is installed in the building per the installation instructions provided. Ensure there is a good network connection.

NOTE: It is mandatory that each DoorBird outdoor station is linked to an updater.

To integrate DoorBird, do the following:

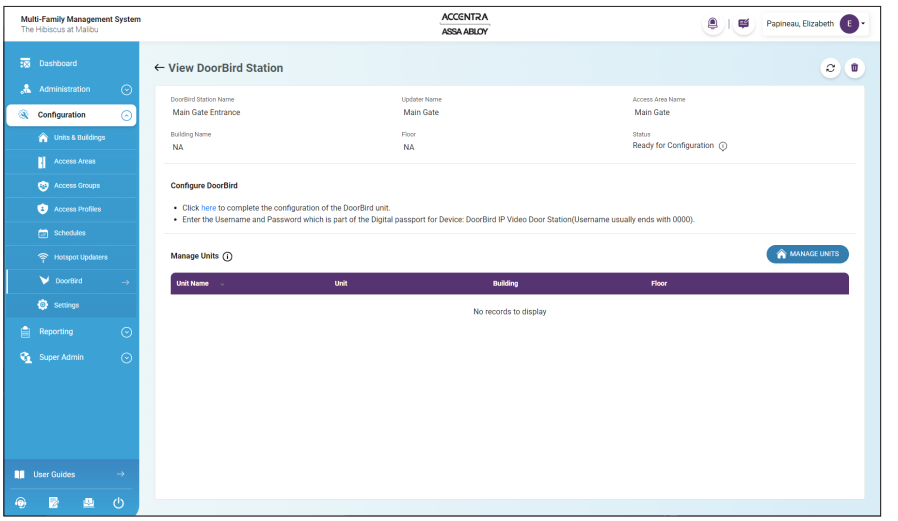
1. Click **Configuration** and then click **DoorBird** on the left side of the screen. A DoorBird screen appears.
2. Click the **Add DoorBird** button.
3. Enter the **DoorBird Station Name** and **Select Updater** from the drop-down list. Note that the updater must have a firmware version of 6.1.0 or above.





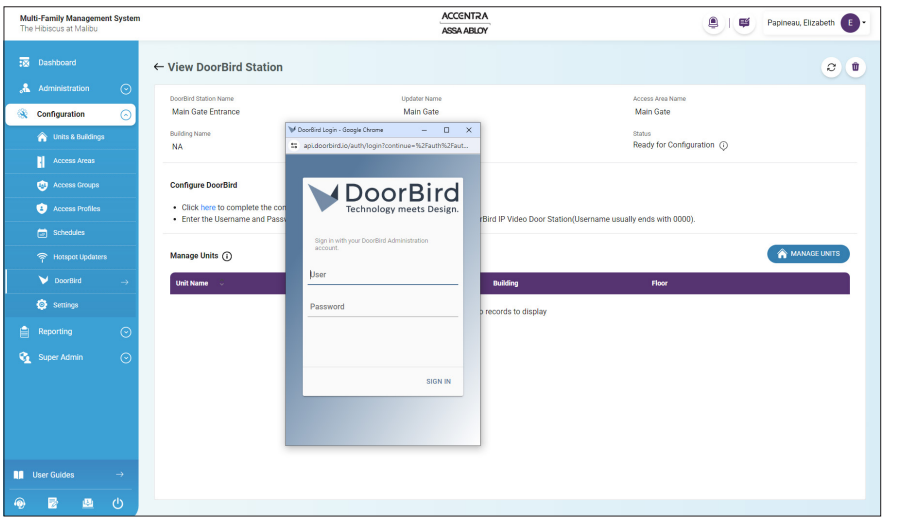
4. When finished, click the **Save** button to save the information. Click the **Cancel** button to discard all changes.

5. Once the DoorBird information is saved, click **View Details**. The screen prompts the user to configure the DoorBird unit.

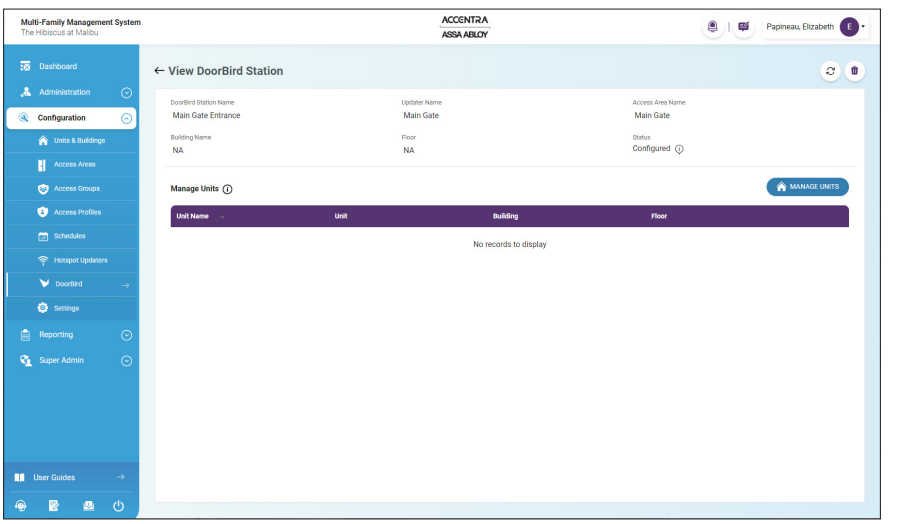


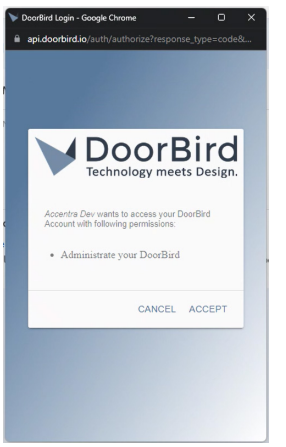
6. Click the blue '**here**' to open the DoorBird app and sign in the with Administration account.
   The Administration account is provided on the Digital Passport document included with the hardware.

7. Once logged in, a message appears stating the Multi-Family Management System wants to access the DoorBird account with administrative permissions. Click **ACCEPT** on the DoorBird app screen.



8. The DoorBird configuration status in the Multi-Family Management System is updated to 'Configured'.





VIEW DOORBIRD DETAILS AND MANAGE UNITS

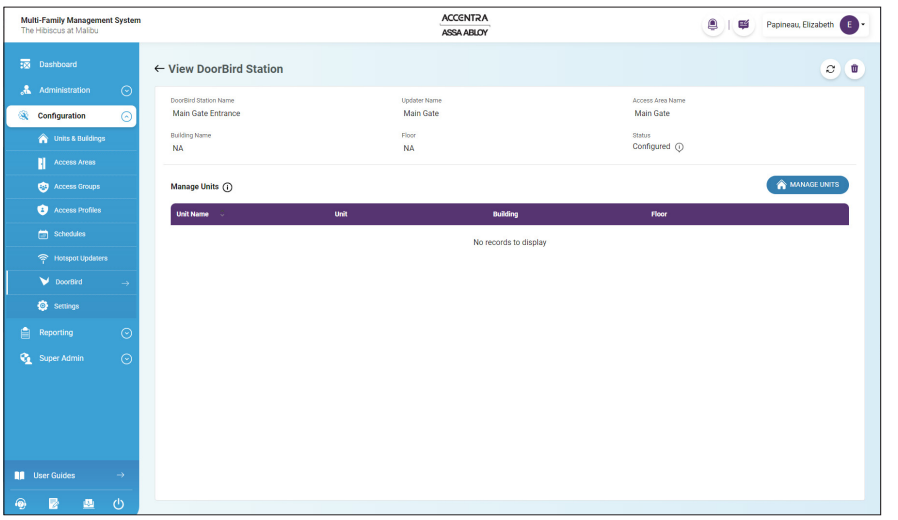
To view DoorBird Details, click **View Details** next to the name of the DoorBird unit.

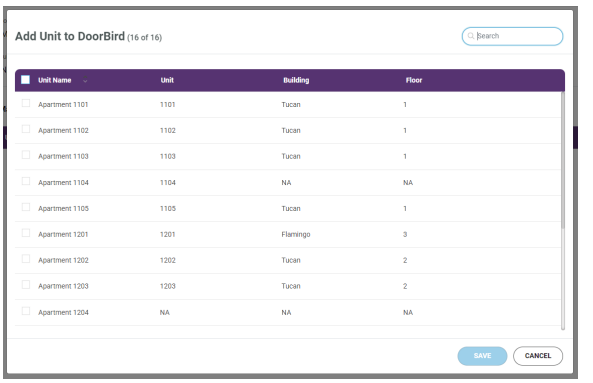
The screen displays all of the details of the DoorBird connected to the system. Adding units can also be done from this screen by doing the following:

Click the **Manage Units** button. The Add Unit to DoorBird box appears.

Click the **checkbox** next to the Unit Name to add to DoorBird.

Click the **Save** button when all the desired Units have been selected.



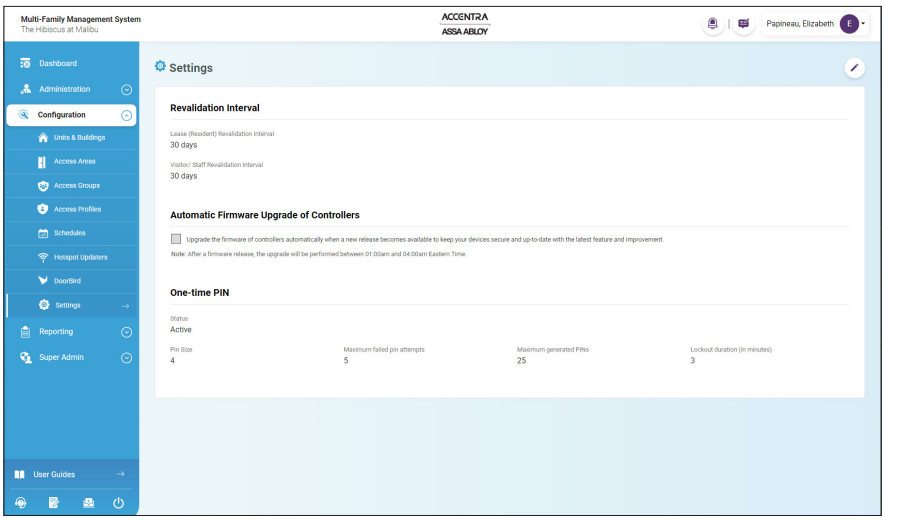


SETTINGS

Settings manages the Revalidation Interval and One-time PIN for all offline locks in the system. It is strongly recommended that desired settings be configured in the Multi-Family Management System prior to lock commissioning with the ACCENTRA Multi-Family Configuration Tool application.

Any changes to One-Time PIN settings after initial commissioning will require that ALL locks in the system either be updated by visiting the opening with the Multi-Family Configuration Tool application OR reset and reconfigured.
Please see the ACCENTRA Multi-Family Configuration app user guide for steps to update the lock.

By default the Revalidation Interval is 30 days and the One-time PIN is set to Inactive.



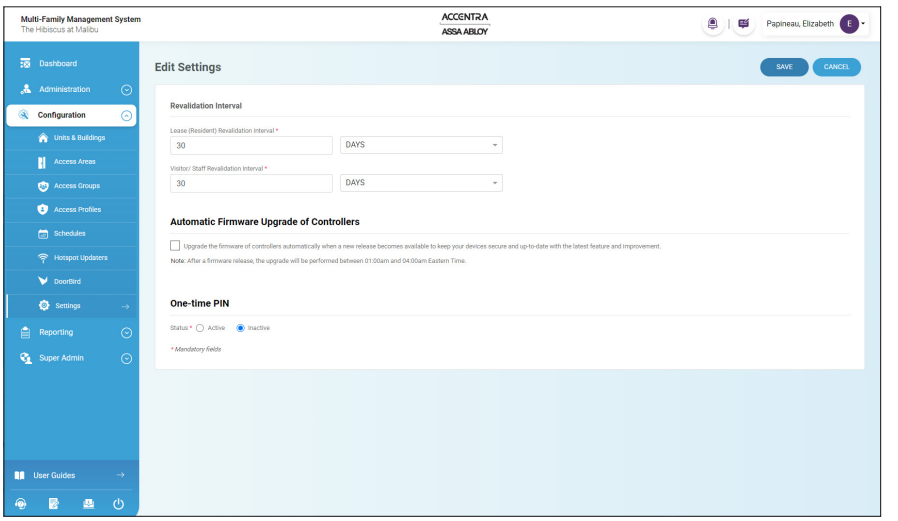
REVALIDATION INTERVAL

All ACCENTRA Multi-Family Management System physical credential holders are required to periodically present their credential to an online updater to receive updated access rights and deliver audit trail information collected from offline openings to the Cloud service. Revalidation interval defines how often physical credentials need to be updated, i.e. present credential to an updater, to be valid in the system. This only applies to mobile credentials if there is no network connection to allow for continuous revalidation. Different revalidation intervals can be set for Leases (Residents) and Visitors/Staff.

If the revalidation interval is set to 1 day, a credential needs to be updated at least one time per day to maintain validity in the system. If the credential is not updated, and a credential holder tries to use it to unlock an offline lock, the credential will not work since the validity has expired. When a credential's revalidation period has passed and its validity has expired, the credential holder must revisit an updater to regain validity in their credential. This adds extra security to the system, since a lost credential will not be usable once the revalidation interval has expired. To reinstate functionality to the credential, simply present it back to any updater in the system.

SETTING THE REVALIDATION INTERVAL

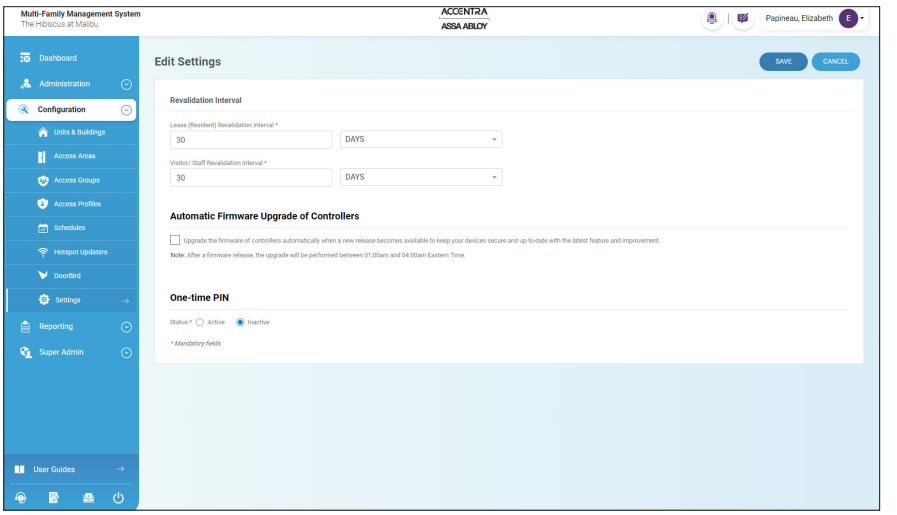
To set the Revalidation Interval, do the following:



1. Click **Configuration** and then click **Settings** on the left side of the screen. The Settings screen appears.
2. Click **Edit Settings** (pencil) on the right side of the screen.

3. Select **DAYS** or **HOURS** from the drop-down list for Lease (Resident) or Visitor/Staff.
4. Enter a number for the number of days or hours the revalidation interval lasts. Minimum of 1 hour, maximum of 999 days.
5. Repeat Steps 3 and 4 for the other revalidation interval (Lease/Resident or Visitor/Staff).
6. Click the **Save** button to save the changes to the revalidation intervals. Click the **Cancel** button to cancel any changes made. The screen returns to the Settings screen.

AUTOMATIC FIRMWARE UPGRADE OF CONTROLLERS



It is important to keep controllers secure and up-to-date with the latest firmware features and improvements. This setting allows all system controller to be updated automatically when new firmware versions are released.

When selected, this checkbox allows the controller firmware, for all controllers in the system, to be automatically upgraded when a new firmware release is available. The firmware updates will be performed between 01:00am and 04:00am Eastern Time.

This function can be disabled at any time by clicking the checkbox to deselect it.

ONE-TIME PIN

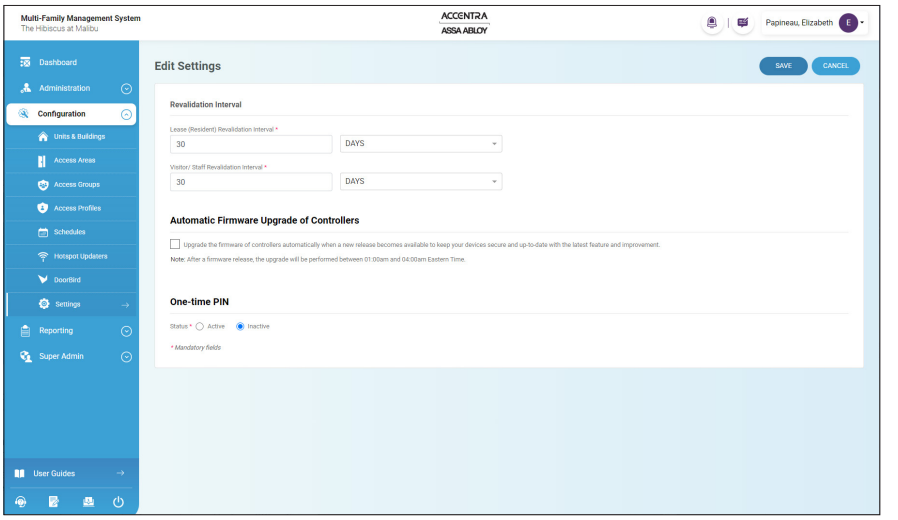
A One-Time PIN code can be issued to a credential holder. This allows access to an offline opening using the keypad instead of a credential, physical (card or fob) or mobile. This is an optional feature that can be turned on or off.

IMPORTANT: One-Time PIN settings configured in the Settings screen apply to ALL offline openings in the Multi-Family Management System. *Editing the settings on this page will require ALL offline locks in the Multi-Family Management System to either be updated with the ACCENTRA Multi-Family Configuration Tool application OR reset and reconfigured*. It is very important that locks are reset and reconfigured, or updated depending on what settings changes are made, after One-Time PIN setting changes. Missing this step will result in the One-Time PIN feature not functioning or giving unexpected results.

SETTING THE ONE-TIME PIN

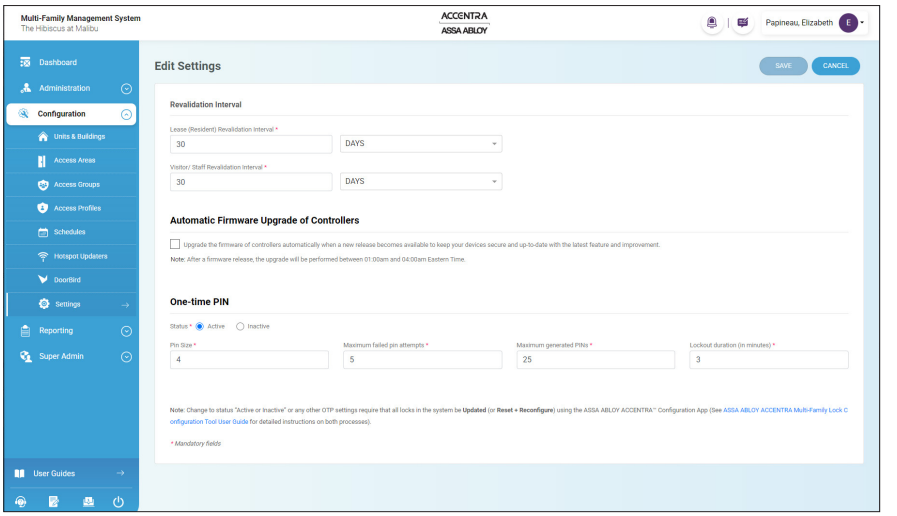
To set the One-Time PIN, do the following:

1. Click **Configuration** and then click **Settings** on the left side of the screen. The Settings screen appears.
2. Click **Edit Settings** (pencil) on the right side of the screen.



3. Select the **Active** radio button to make One-Time PIN active. Select the **Inactive** radio button to disable One-Time PIN.
4. When Active is selected, one-time PIN settings appear.
5. Enter a number to set the desired PIN size. PIN size minimum is 4 digits, maximum is 8 digits.
6. Enter a number to set the maximum number of failed PIN attempts a user can make before they are locked out. Number of attempts minimum is 1 and maximum is 10.

7. Enter the number of One-Time PINs that will be written to all locks' memories. The number of PINs minimum is 1 and maximum is 100.
A bank of One-Time PINs is written into each lock's memory at the time of configuration with the ACCENTRA Multi-Family Configuration Tool application. This sets a specific number of one-time PIN codes that will be available for use in the lock.



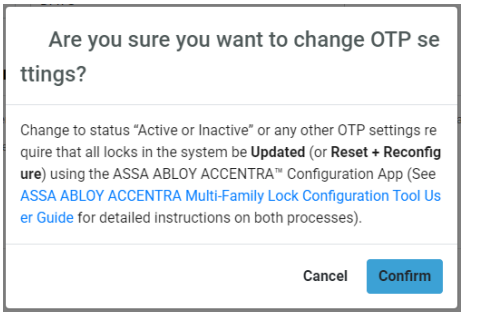
8. Enter the number of minutes for Lockout duration. This is the amount of time a user will be blocked from retrying a PIN code following the maximum failed One-Time PIN attempts. Lockout duration time minimum is 1 minute and maximum is 4 minutes.

9. Click the **Save** button to save the changes to the one-time PIN settings. Click the **Cancel** button to cancel any changes made. A warning message appears when the **Save** button is clicked.

10. Click the **Confirm** button to save the OTP setting changes. Click the **Cancel** button to cancel the changes.

NOTE: All locks need to be either reset and reconfigured OR updated because OTP settings have changed.

NOTE: When a lock reaches zero One-Time PINs left in its memory, it will need to be updated using the Multi-Family Mobile app in order to replenish the bank of PIN codes. See "One-Time PIN" on page 85 to determine how many PINs are left in the lock's memory.



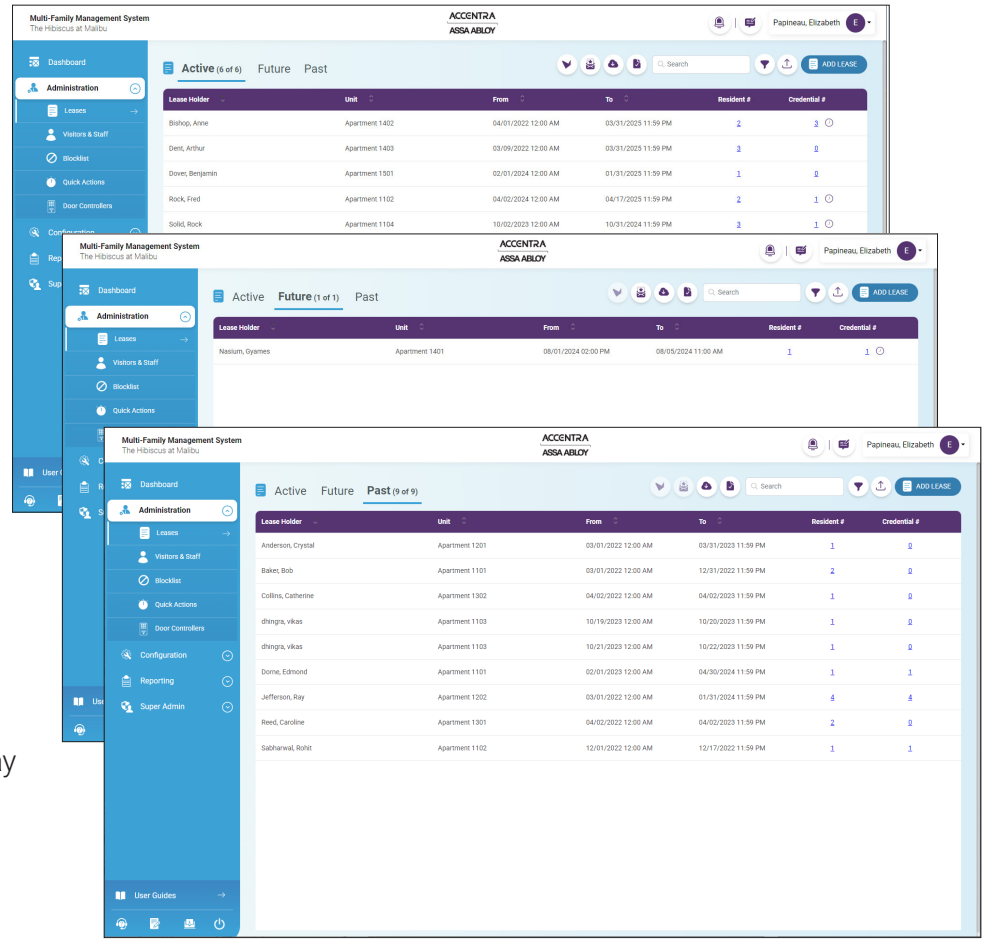
NOTE: See the ACCENTRA Multi-Family Management System Configuration Application User Guide for information on how to reset and reconfigure or update individual locks.

5. ADMINISTRATION

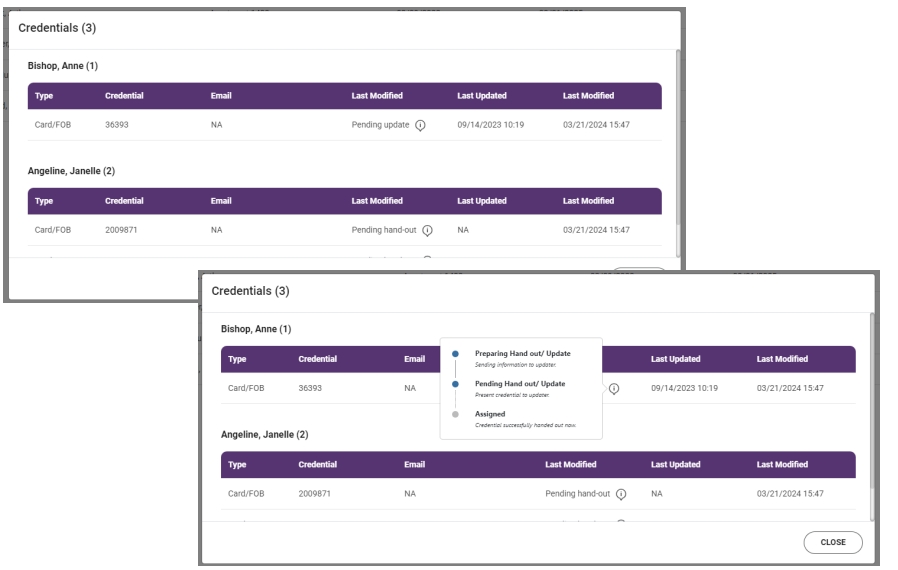
The Administration service manages access privileges for people, such as leases, visitors and staff.

LEASES

Leases allows the administrator to create leases, manage existing leases, past leases, future leases, and manage residents and resident access. The Leases screen displays the Active Leases list by default. Future Leases and Past Leases are displayed in separate tabs on the screen. Past Leases are any leases that have expired, are past the To date defined in the lease. Future Leases are any leases that have a start date after the current date. A maximum of 100 leases is displayed by default. If more than 100 leases are in the system, scroll down to display the next 100 leases.



The Lease lists show the Lease Holder, the Unit number, the From and To dates, the number of residents, and the number of credentials. If the clock icon appears next to a credential number, it means action is required on one or more of the credentials. Click the icon for more information. Positioning the mouse over the info icon in the credentials detail box shows the credential status process steps. Click the **Close** button to close the credential detail box.

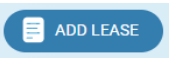


ADD LEASE

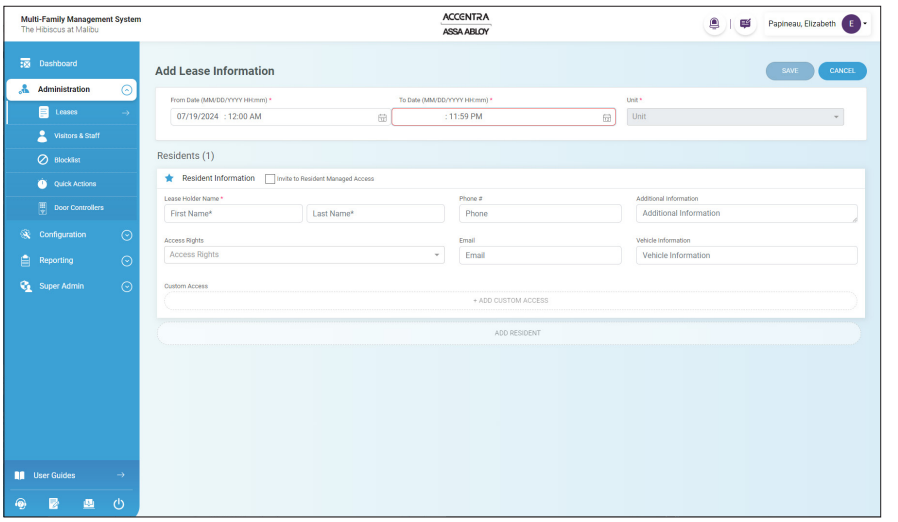
A lease is defined as permission for one or more people to access a unit and its respective doors for a specified time frame.

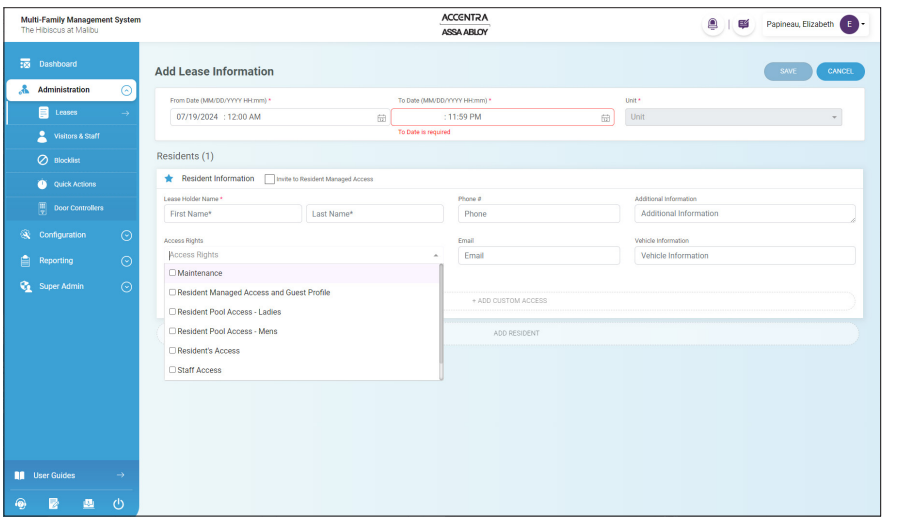
To create a new lease, do the following:

1. Click **Administration** and then click **Leases** on the left side of the screen. The Leases screen appears.
2. Click the **Add Lease** button on the right side of the screen. The Add Lease information screen appears.



3. Use the calendar function to add a **From** date and time and a **To** date and time. The From date automatically populates with the current date and a time of 12:00AM. The To date automatically populates with a time of 11:59PM.
4. Select a **Unit** from the Unit drop-down list. Only available units are displayed.
5. Enter a lease holder **First Name** and a **Last Name**. These are required fields. Phone number, e-mail and Additional Information are optional. Change the size of the Additional Information field by clicking on the lower right corner of the text box.
6. Select the **Invite to Resident Managed Access** check box to allow the resident to use the RMA functions.
7. Click the arrow in the **Access Rights** field to display a list of available access rights. Select the desired access rights from the list.

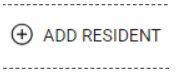




8. If desired, click **Add Custom Access**. Select the **Access Area**, the **From Date**, the **To Date**, **Start Time**, and **End Time**. Use the check boxes to select the desired days of the week to allow access. Up to five custom accesses allowed.

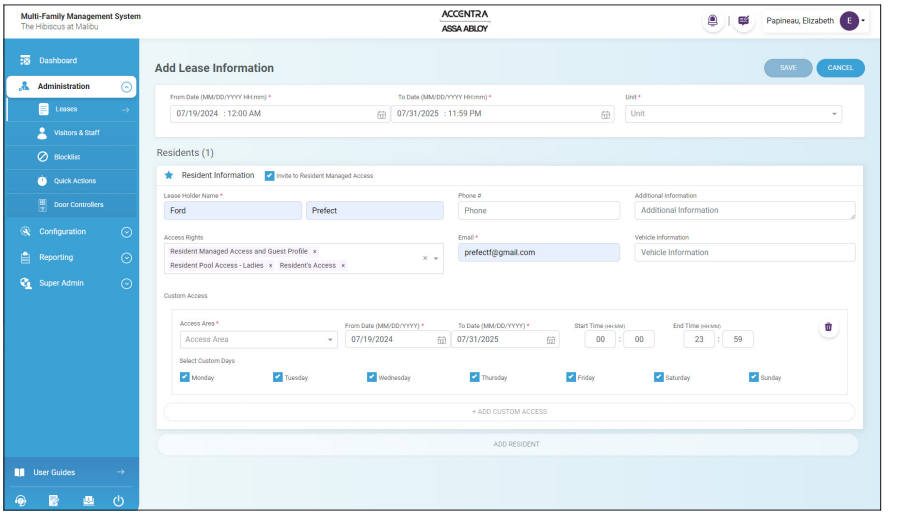
9. To remove the custom access, click the **Trash Can** button in the upper right corner of the Custom Access section of the screen.

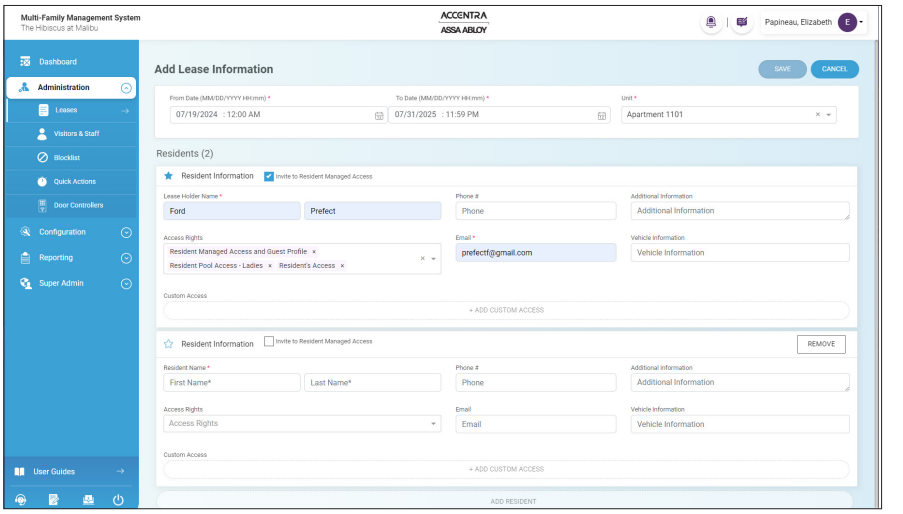
10. Click the **Add Resident** button to add additional residents.



Note that a resident cannot be added until the lease holder information is added.

11. Enter the resident **First Name** and **Last Name**. These are required fields. Phone number, e-mail and Additional Information are optional.





12. Select the **Invite to Resident Managed Access** check box to allow the resident to use the RMA functions. An email address is required for Resident Managed Access™.

13. Click the arrow in the **Access Rights** field to display a list of available access profiles. Select the desired access profiles from the list.

NOTE: Residents can have access rights different from the lease holder.

14. To add more residents, click the **Add Resident** button. To remove residents, click the **Remove** button next to the resident's name.

15. Click the **Save** button to save the the lease. Click the **Cancel** button to cancel any changes made. The screen returns to the Leases screen.

NOTE: If **Invite to Resident Managed Access** is selected, the resident will receive an email with information and instructions to set up their Resident Managed Access™ functions. It is recommended that the Resident Managed Access™ Getting Started Guide (link in the Help section) also be provided to the resident.

SEARCH FOR A LEASE

The search function is the same for Current, Future, and Past Leases. However, the search will only search in the active screen. For example, if search criteria is entered in the Past Leases screen, the system only searches through the past leases.

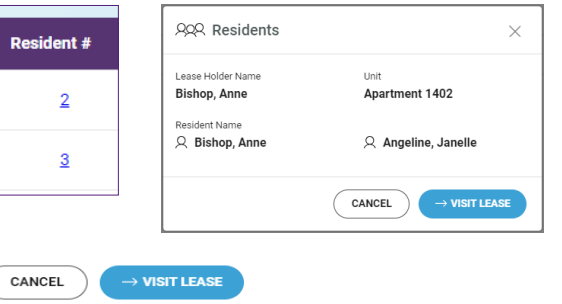
To search for a lease, do the following:

1. Click **Administration** and then click **Leases** on the left side of the screen. A list of leases appears.
2. Enter the search criteria in the **Search** box at the top of the Leases list.
   NOTE: Any text or part of text used in the Search field that is part of the lease holder's name or description will appear in the Search results.
3. The search results are displayed automatically.

QUICK DISPLAY RESIDENTS

To quickly display resident names for each lease, click on the number in the **Resident #** column in the Leases list. A Residents dialog box appears.

This box displays the lease holder name, the unit and the name of each resident. To view the lease, click the **Visit Lease** button. To close the box, click the **Cancel** button.



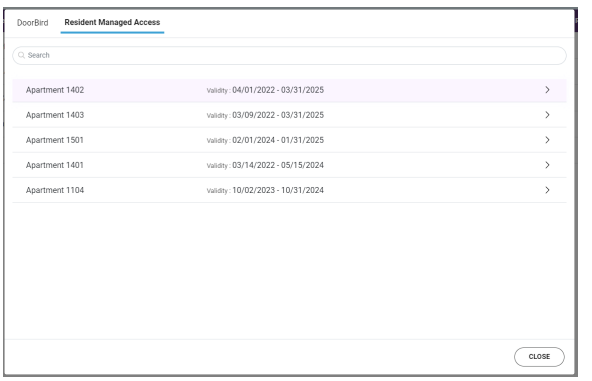
BULK INVITE TO RESIDENT MANAGED ACCESS™ AND DOORBIRD

It is possible to use the bulk invite pop-up box to invite multiple residents to Resident Managed Access™ and Doorbird.

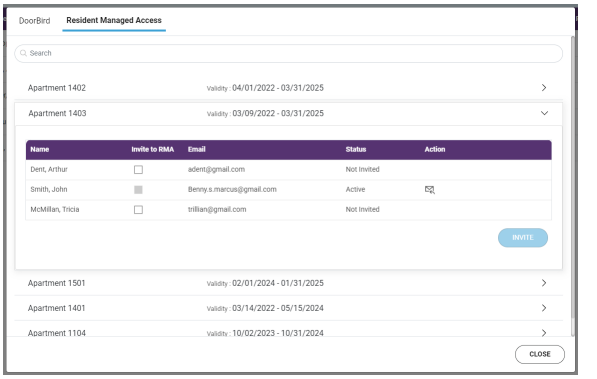
To invite multiple residents to Resident Managed Access™ (RMA), do the following:

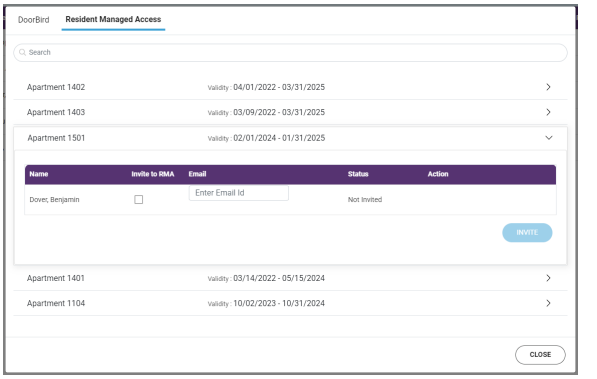
1. Click **Administration** and then click **Leases** on the left side of the screen. A list of leases appears.
2. Click the **Invite to Resident Managed Access** button at the top of the Leases list.

   An Invite to Resident Managed Access™ box appears. The Invite to Resident Managed Access™ box lists the Units that have valid leases with residents that can be invited to use Resident Managed Access™.



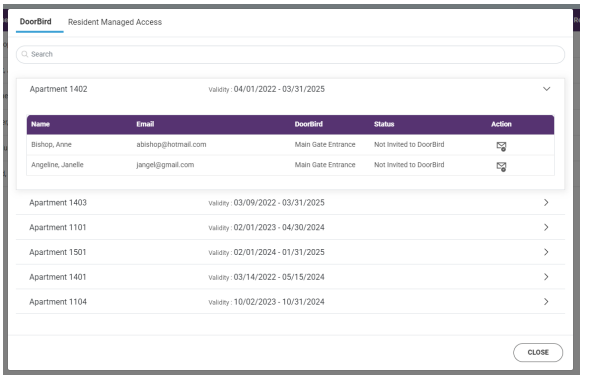
3. Click on a Unit to display a list of residents in that Unit. The list shows the resident's Name, if they have been invited to RMA, Email (if available), and invite status.
4. Click the **Invite to RMA** check box next to the name of each resident to be invited.
5. Enter the resident's **Email address** if it not already in the system. An email address is required to invite a resident to use RMA.
6. When all the desired selections are made for the lease, click the **Invite** button. This will send an email with an invitation to use RMA to each selected resident.
7. Click the envelope icon in the Action column to resend the RMA invitation if the resident was previously invited.
8. Click the **Close** button when finished selecting the residents to be invited to use Resident Managed Access™.





To invite multiple residents to Doorbird, do the following:

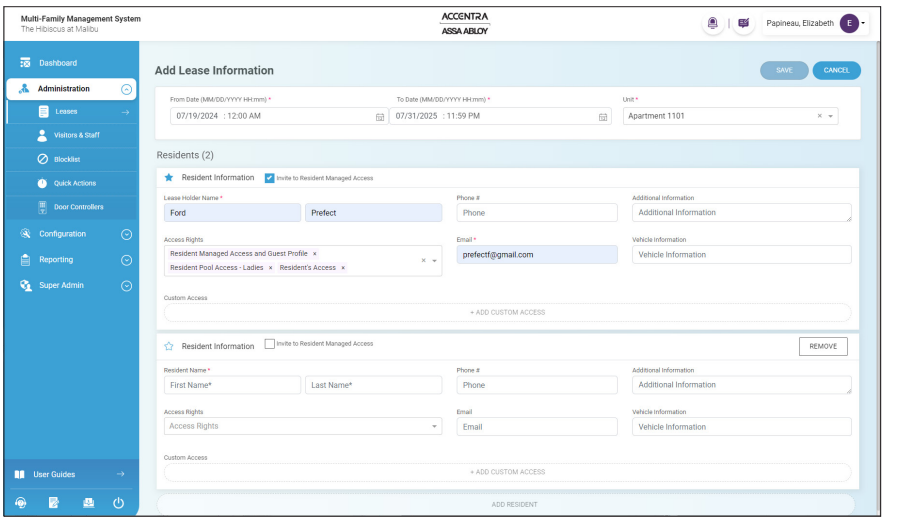
1. Click **Administration** and then click **Leases** on the left side of the screen. A list of leases appears.
2. Click the **Invite to Doorbird** button at the top of the Leases list.
   An Invite to Doorbird box appears. The Invite to Doorbird box lists the Units that have valid leases with residents that can be invited to use Doorbird.
3. Click on a Unit to display a list of residents in that Unit. The list shows the resident's Name, if they have Doorbird access, and Email (if available).
4. Click the **Invite** button next to the name of each resident to be invited.
5. Enter the resident's **Email address** if it not already in the system. An email address is required to invite a resident to use Doorbird.
6. When all the information is entered for the resident, click the **Invite** button. This will send an email with an invitation to use Doorbird to each selected resident.
7. Click the **Close** button when finished selecting the residents to be invited to use Doorbird.



DISPLAY LEASE INFORMATION

To display lease information, do the following:

1. Click **Administration** and then click **Leases** on the left side of the screen. A list of leases appears.
2. Click on any of the columns with the lease information desired. Use the Search function to find the desired lease. The Lease Information screen appears.
3. To return to the lease list, click **Arrow** next to Lease Information in the upper left corner of the screen.



← Lease Information

The Lease Information screen shows the Lease Holder name, the Unit, the lease dates, each resident name, email, phone number, access rights, additional information and credential information.

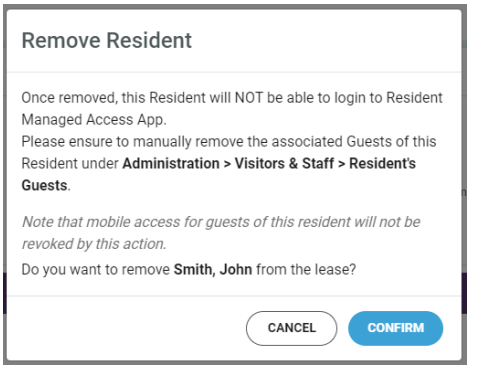
From this screen the lease information can be edited or deleted, the lease can be moved in or moved out, residents can be added or removed, credentials can be handed out/handed in, or blocked for each resident, residents can be invited to DoorBird or Resident Managed Access™. Note that lease holders cannot be deleted.

To view information for a resident, click on the resident's name.

To add a resident to the lease, click the **Add Resident** button and then enter the resident information as desired. Click the **Save** button when done.

To remove a resident from the lease, click the **Delete** button in the Resident Information section. The Remove Resident from Lease confirmation box appears.

Click the **Confirm** button to remove the resident from the lease. *Note that the resident cannot be removed until their assigned credential is handed in/blocked.*



EXPORT/IMPORT LEASE LIST

To export the lease list, do the following:

1. Click **Administration** and then click **Leases** on the left side of the screen. A list of leases appears.
2. Click the **Export** button to create a .CSV file that contains all of the Leases.

It is possible to create a lease list using a .CSV file and then import it into the system.

A .CSV file template is available to use to ensure the .CSV file being used to import the lease information is correctly formatted.

To download a sample .CSV file template, do the following:

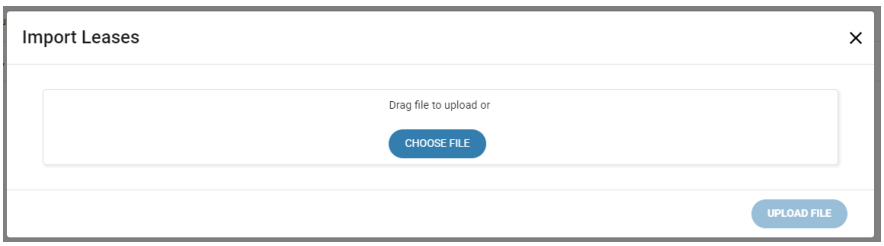
1. Click **Administration** and then click **Leases** on the left side of the screen. A list of leases appears.
2. Click the **CSV** button to download a .CSV file template. The template name is lease_template.csv.

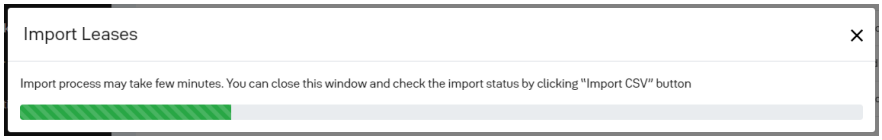
When the .CSV file template is filled in with the desired information, it can be imported to the system. Please note the *maximum file size for the .CSV file is 140KB*.

NOTE: Unit names and Access Rights (Profiles) must exist in the system prior to loading leases using the .CSV file. When entering units into the .CSV file, be sure to use the complete unit name as it exists in the system. For example: if a unit is named "Apartment Room 1101" in the system, "Room 1101" cannot be used in the .CSV file. It must be "Apartment Room 1101".

To import a lease list, do the following:

1. Click **Administration** and then click **Leases** on the left side of the screen. A list of leases appears.
2. Click the **Import** button to load a .CSV file that contains all of the Leases. The Import Leases dialog box appears.
3. Select the file to upload using the drag-and-drop method or click the **Choose File** button to select the file.
4. When the file is selected, click the **Upload File** button. A status bar appears.



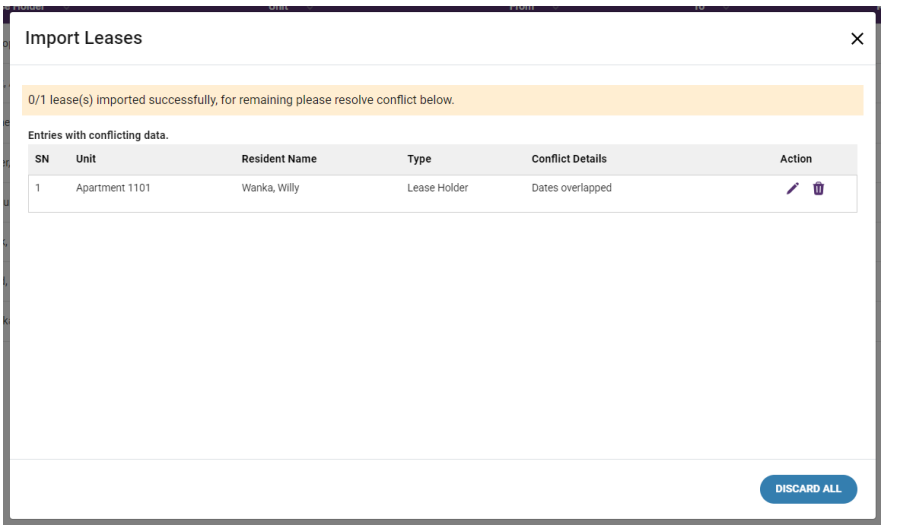


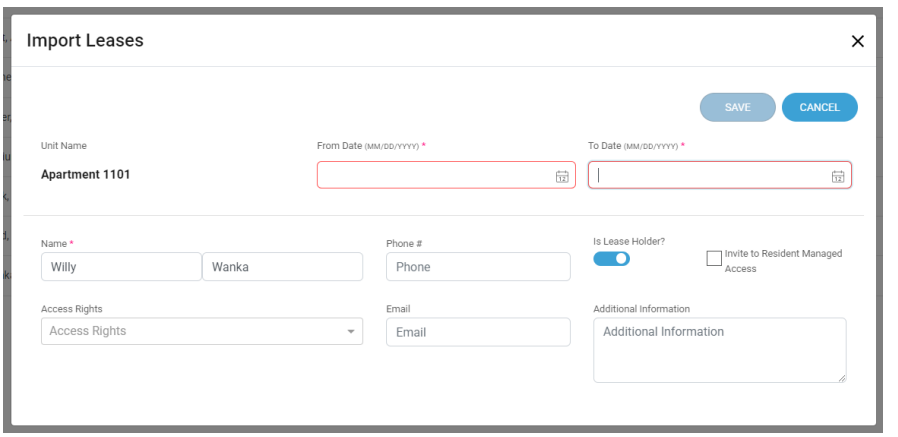
5. When the upload is complete a completion message appears. If there were no errors a success message is displayed. Click the **Close** button to close the message.

If data errors, like duplicate data or incorrect data format were found during the upload, an error message is displayed with the incorrect data. It is possible to edit the incorrect data or discard the data through the error message.

To edit the import errors, do the following:

1. Click **Edit** button (pencil)in the Action column next to the desired error. The edit screen appears.
2. Correct the errors as noted in the error screen. When finished, click the **Save** button. To discard the changes, click the **Cancel** button.
3. To discard all errors, click the **Discard All** button.



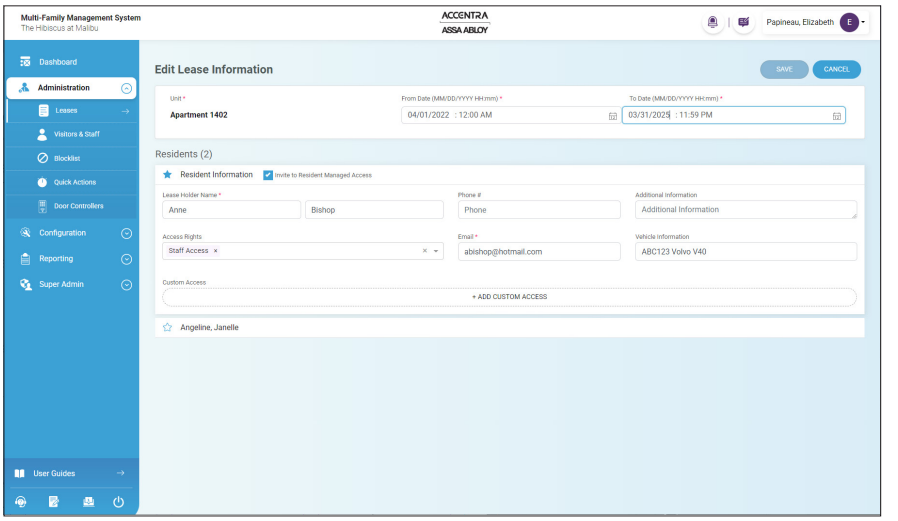


EDIT LEASE INFORMATION

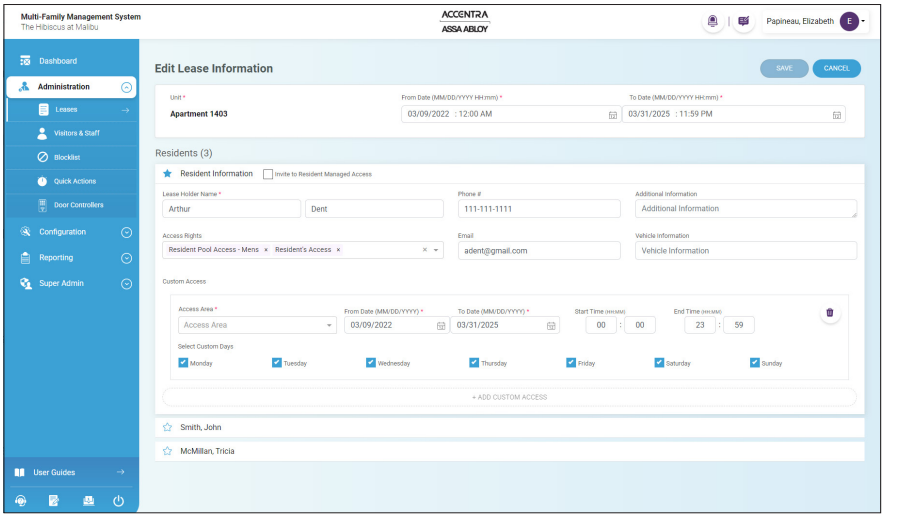
To edit lease information, do the following:

1. Click **Administration** and then click **Leases** on the left side of the screen. A list of leases appears.
2. Click on any of the columns with the lease information desired. Use the Search function to find the desired lease. The Lease Information screen appears.
3. Click the **Edit Lease** button (pencil).

The Edit Lease Information screen displays editable text boxes. The lease dates, lease holder or other resident name, email, phone number, access rights and additional information can be changed. Also any resident can be invited as a Resident User by clicking in the check box above the resident's name. The leaseholder can be changed by clicking on the star next to the resident name. The resident becomes the leaseholder. The Unit name cannot be changed.



4. Click **Add Custom Access** to add custom access to a resident. Select the **Access Area**, the **From Date**, the **To Date**, **Start Time**, and **End Time**. Use the check boxes to select the desired days of the week to allow access. Up to five (5) custom accesses can be assigned for the resident.



5. To remove the custom access, click the **Trash Can** button in the upper right corner of the Custom Access section of the screen.

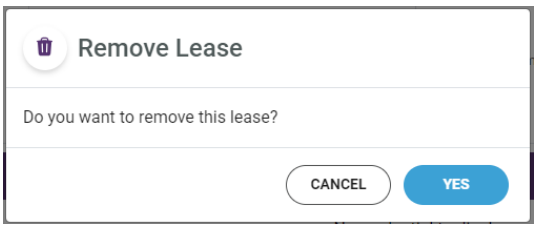

6. Click the **Save** button to save the changes to the access area. Click the **Cancel** button to cancel any changes made. The screen returns to the Leases screen.

REMOVE LEASE

A lease can be removed without having to remove the residents and lease holder. Note that all the credentials must be handed in or blocked before the lease can be removed.

To remove a lease, do the following:

1. Select the lease to remove from the lease list.
2. Check to be sure all the resident credentials are handed in or blocked.
3. Click the **Delete** button (trash can) in the upper right of the screen. The Remove Lease confirmation box appears.

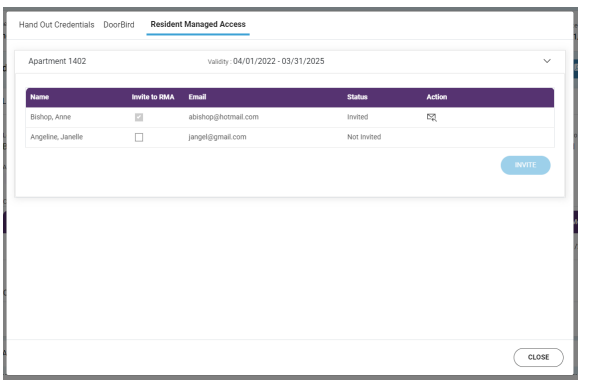


4. Click the **Yes** button in the Remove Lease confirmation box to remove the lease. Click the **Cancel** button to keep the lease.

LEASE INVITE TO RMA OR DOORBIRD

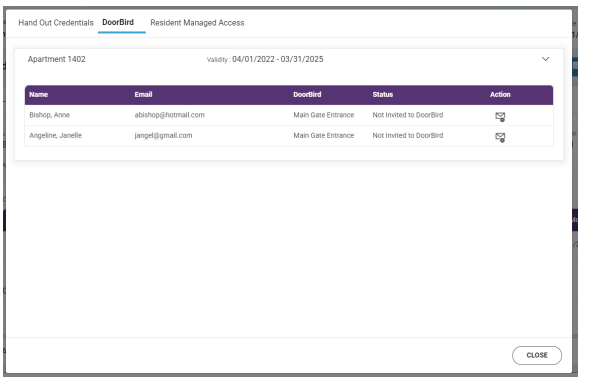
Individual residents on a lease can be invited to Resident Managed Access™ or DoorBird using the RMA or DoorBird icons in the Lease Information screen. Note that there must be a valid email address for the resident entered into the system. If a resident does not get an invitation email, instruct them to check their spam or junk folder.

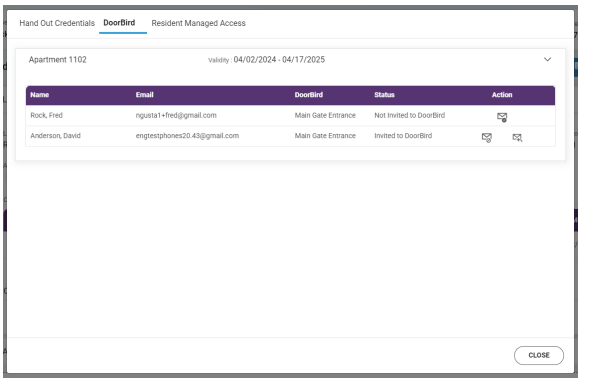
To invite residents to Resident Managed Access™, do the following:



1. Click **Administration** and then click **Leases** on the left side of the screen. A list of leases appears.
2. Click on any of the columns with the lease information desired. Use the Search function to find the desired lease. The Lease Information screen appears.
3. Click on the **Resident Managed Access** icon  next to the **Hand Out** button. A pop-up box appears.
4. Select the **Invite to RMA** check-box next to the name of the resident to invite. If the check-box is grayed out, the resident has already been invited to RMA.
5. Click the **Invite** button to send the invitation.
6. To resend the invitation, click the **Resend Invitation** icon in the Action column. 

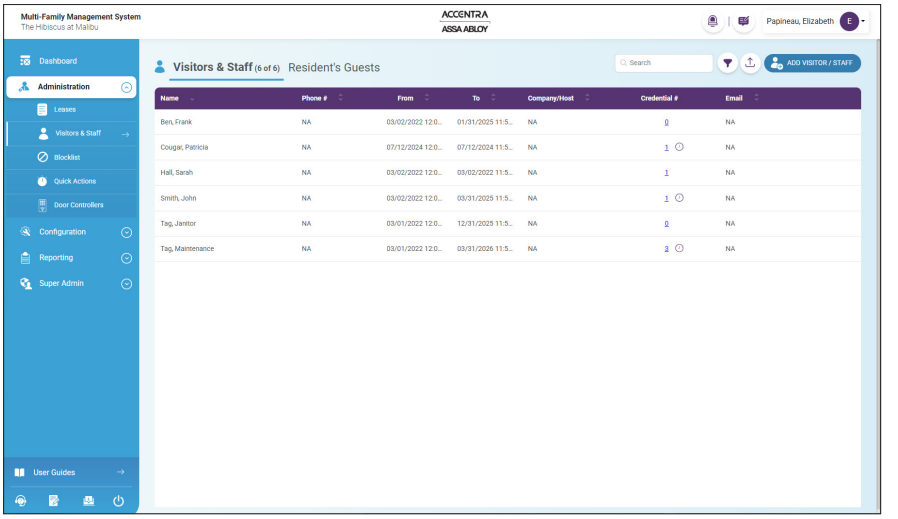
To invite residents to DoorBird, do the following:





1. Click **Administration** and then click **Leases** on the left side of the screen. A list of leases appears.
2. Click on any of the columns with the lease information desired. Use the Search function to find the desired lease. The Lease Information screen appears.
3. Click on the **DoorBird** icon next to the **Hand Out** button. A pop-up box appears.
4. Click the **Invite** button next to the name of the resident to invite. 
5. To remove a resident's DoorBird permissions, click the **Un-Invite** button. 
6. To re-send the invitation, click the **Resend Invite** button. 

VISITORS & STAFF



Visitors and Staff allows the user to create new visitors and new staff members in the system, manage the visitors and staff member access and view guests added by residents through the Resident Managed Access™ function.

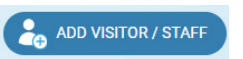
The visitor & staff list shows the visitor/staff name, phone number, the From and To dates, the company or host, the number of credentials and email. If the clock icon appears next to a credential number, it means action is required on the credential. Click the icon for more information. Positioning the mouse over the info icon in the credentials detail box shows the credential status process steps. Click the **Close** button to close the credential detail box.

ADD VISITOR

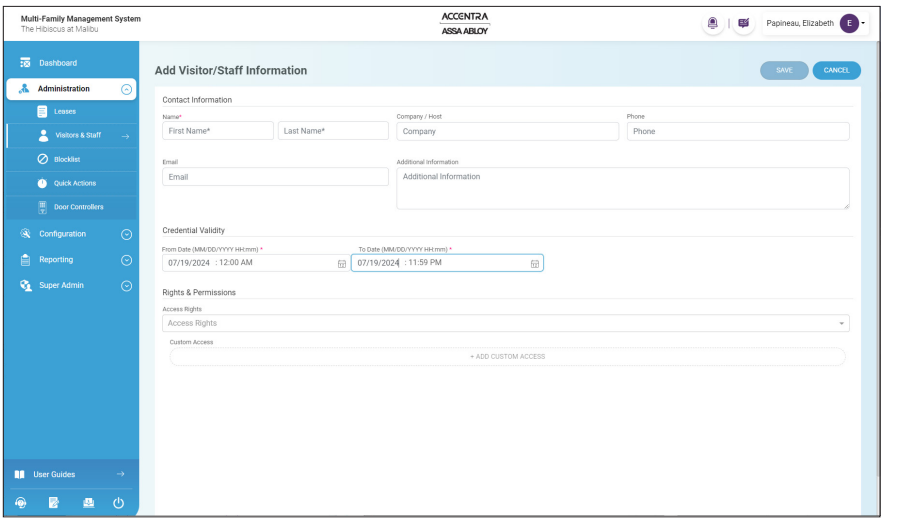
The Add Visitor features allow the administrator to create a credential for an individual visiting the site or a staff member working on the site.

To create a new visitor or staff member, do the following:

1. Click **Administration** and then click **Visitors & Staff** on the left side of the screen. The Visitors & Staff screen appears.
2. Click the **Add Visitor/Staff** button on the right side of the screen. The Add Visitor Information screen appears.

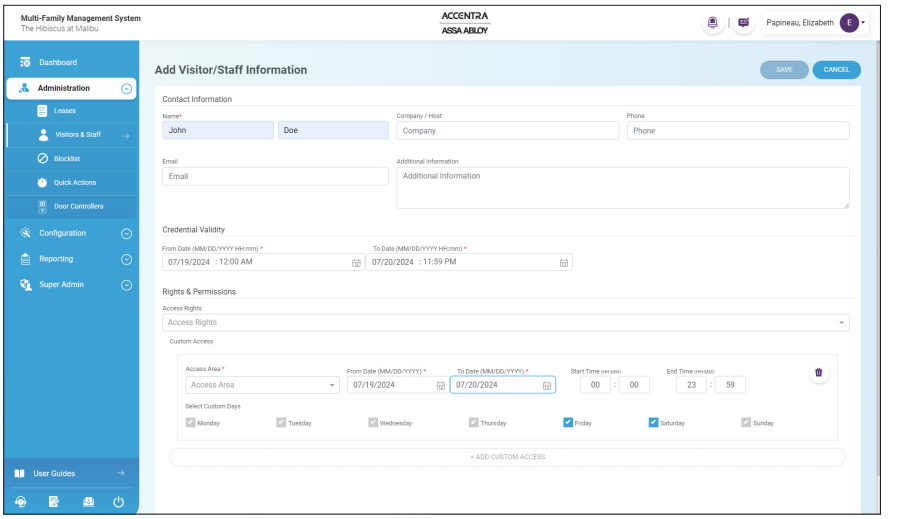


3. Enter the Visitor or Staff person contact information. **First name** and **Last name** are mandatory fields. Company/Host, Phone, Email and Additional Information are optional.
4. Add the Credential Validity information. Select the appropriate dates for how long the person's credential is valid. The default **From** date is the current date, but can be changed.



NOTE: The **To** date cannot be a date before the **From** date. The To date will automatically be changed so that it is not before the From date.

5. Select the desired **Access Rights** from the Access Rights drop-down list.
6. Click the **Add Custom Access** button to add custom access rights. The Custom Access information section appears.
7. Select an **Access Area** from the drop-down list, set the allowed access time using the **Start Time** and **End Time** clocks, and set the **From** and **To** date range using the calendar buttons, select **Custom Days** to set the specific days the person is allowed access within the time and date range selected. Up to five (5) custom accesses can be assigned for the visitor/staff member.



8. To remove the custom access, click the **Trash Can** button in the upper right corner of the Custom Access section of the screen.

9. Click the **Save** button to save the changes to the visitor/staff information. Click the **Cancel** button to cancel any changes made. The screen returns to the Visitor & Staff screen.

SEARCH FOR A VISITOR/STAFF

To search for a visitor or staff member, do the following:

1. Click **Administration** and then click **Visitors & Staff** on the left side of the screen. A list of visitors and staff appears.
2. Enter the search criteria in the **Search** box at the top of the Visitors & Staff list.

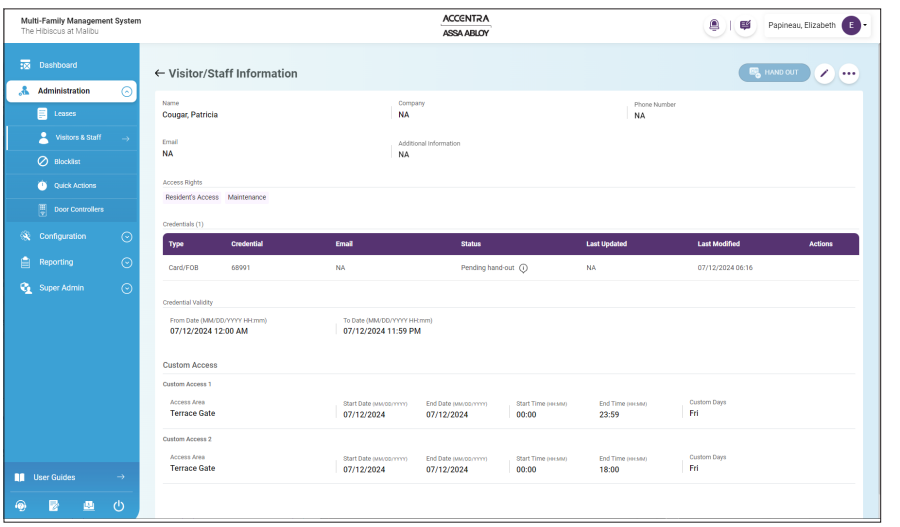
NOTE: Any text or part of text used in the Search field that is part of the visitor's name or description will appear in the Search results.

3. The search results are displayed automatically.

DISPLAY VISITOR & STAFF INFORMATION

To display visitor and staff information, do the following:

1. Click **Administration** and then click **Visitors & Staff** on the left side of the screen. A list of visitors and staff appears.
2. Click on any of the columns with the visitor information desired. Use the Search function to find the desired lease. The Visitor Information screen appears.
3. To return to the lease list, click **Arrow** next to Lease Information in the upper left corner of the screen.



← Visitor/Staff Information

The Visitor Information screen shows the Visitor name, company, email, phone number, access rights including custom access, additional information and credential information. It is also possible to hand out a credential using the **Hand Out** button.

EXPORT VISITOR & STAFF LIST

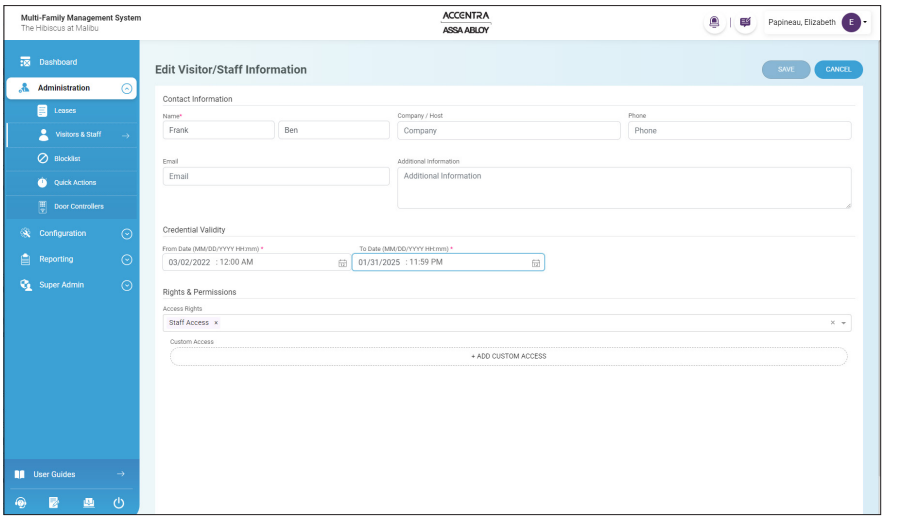
To export the visitor and staff list, do the following:

1. Click **Administration** and then click **Visitors & Staff** on the left side of the screen. A list of visitors appears.
2. Click the **Export** button to create a .CSV file that contains all of the Visitors and Staff.

EDIT VISITOR & STAFF INFORMATION

To edit visitor and staff information, do the following:

1. Click **Administration** and then click **Visitors & Staff** on the left side of the screen. A list of visitors and staff appears.
2. Click on any of the columns with the visitor information desired. Use the Search function to find the desired lease. The Visitor Information screen appears.
3. Click the **Edit Visitor** button (pencil).



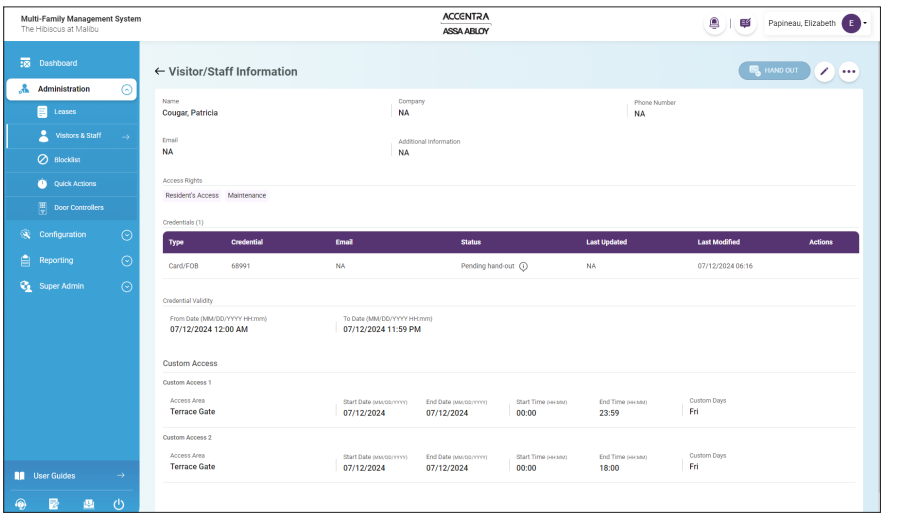
The Edit Visitor Information screen displays editable text boxes. The visitor name, email, company/host, phone number, access rights, additional information, and credential validity can be changed.

4. Click the **Save** button to save the changes to the access area. Click the **Cancel** button to cancel any changes made. The screen returns to the Visitor Information screen.

REMOVE VISITOR & STAFF INFORMATION

To remove visitor and staff information, do the following:

1. Click **Administration** and then click **Visitors & Staff** on the left side of the screen. A list of visitors and staff appears.
2. Click on any of the columns with the visitor information desired. Use the Search function to find the desired lease. The Visitor Information screen appears.
3. Click the **More Menu** button (ellipsis).
The More menu is displayed.



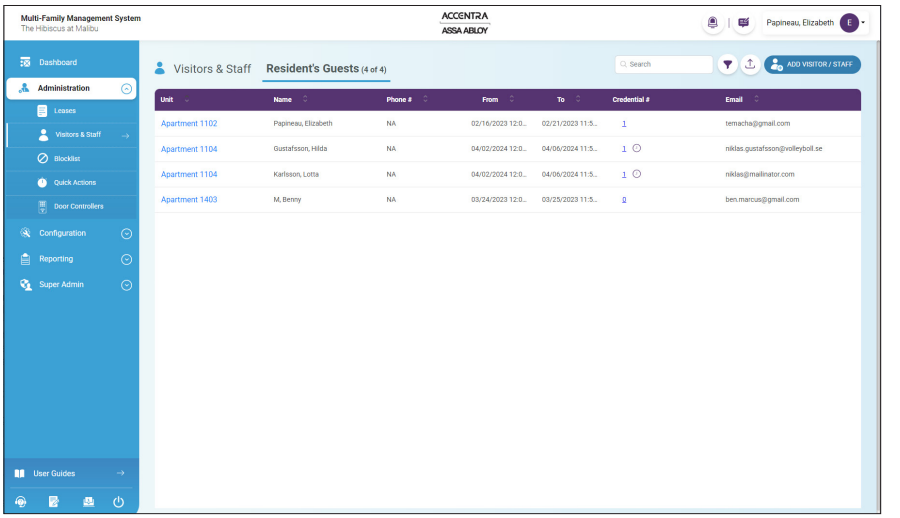
4. Select **Remove** from the menu.

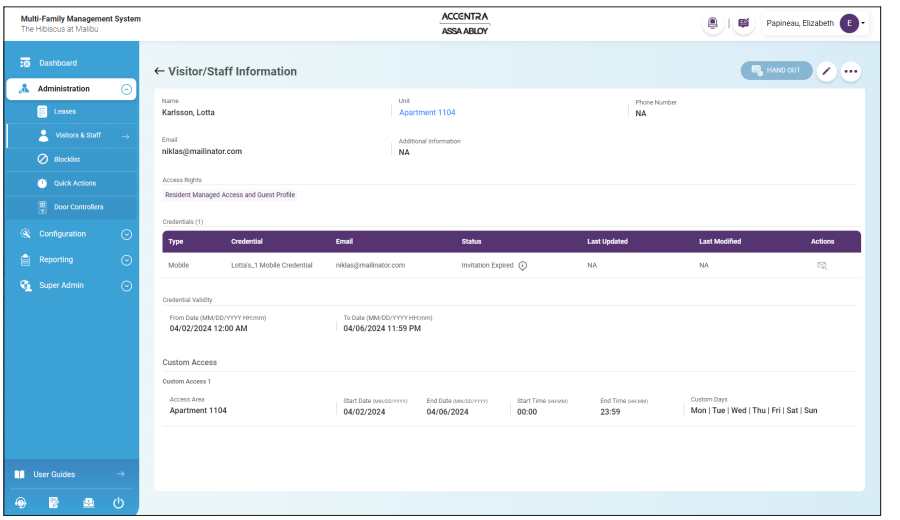
RESIDENT'S GUESTS

To view a list of resident's guests, click on the **Resident's Guests** tab at the top of the screen. The list shows the Unit who issued the credential, guest's name, phone number if entered, From and To dates, the number of credentials issued and guest's email address.

Clicking on the **Unit** name opens the lease information for the resident who issued the guest credential. Clicking on the **Credential #** opens a pop-up box displaying the credential information and status.

Clicking on the guest name opens the Visitor/Staff Information screen to display the access information assigned to that guest. This information can be edited in the same way that Administrator assigned visitor information is edited.





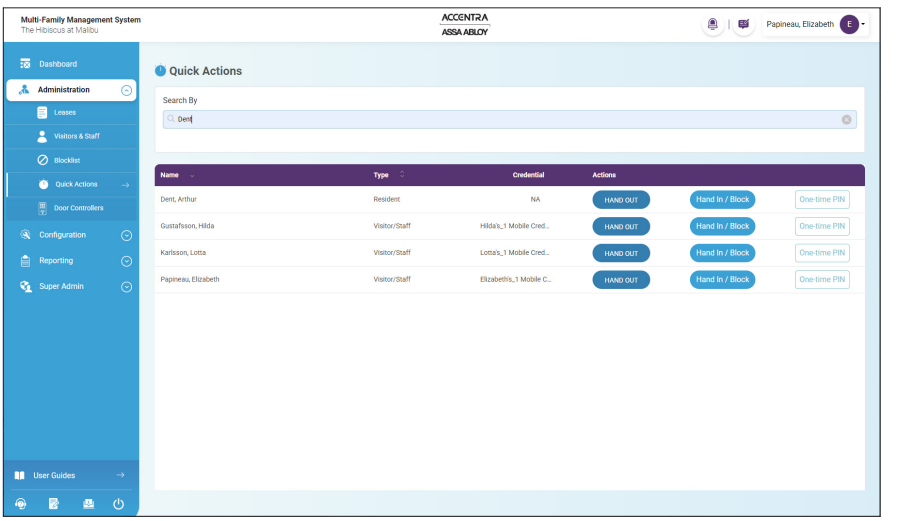
QUICK ACTIONS

Quick Actions allows the administrator to hand out credentials, hand in credentials, issue a one-time PIN, and block credentials.

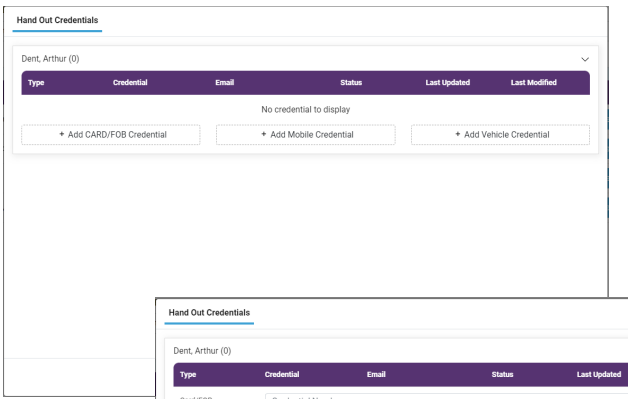
HAND OUT

The Hand Out feature allows the administrator to hand out credentials to lease holders, residents, visitors and staff members so that the system knows which credentials are assigned to each person. Each person (lease holder, resident, visitor, staff member) is allowed to have a maximum of nine (9) credentials assigned, three (3) physical credentials, three (3) mobile credentials and three (3) vehicle credentials.

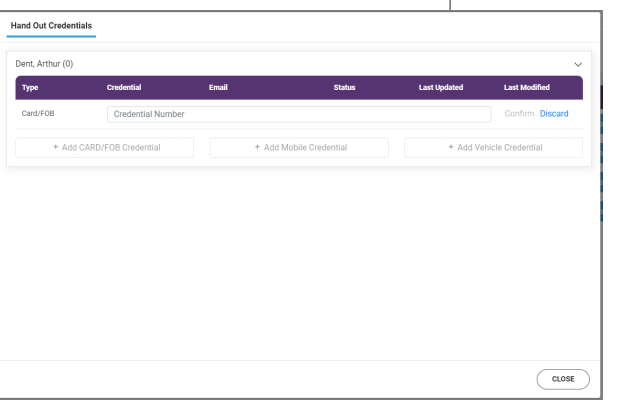
To hand out credentials, do the following:



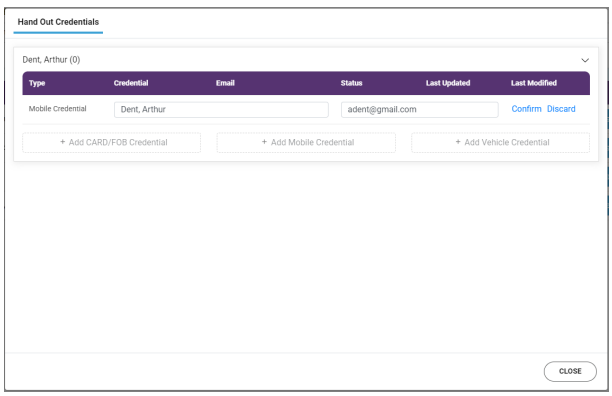
1. Click **Administration** and then click **Quick Actions** on the left side of the screen. The Quick Actions screen appears.
2. Enter a name or partial name (3 characters minimum) in the Search By field. A list of names automatically appears containing the search criteria.
3. Click the **Hand Out** button next to the desired name. The Hand Out Credential dialog box appears.

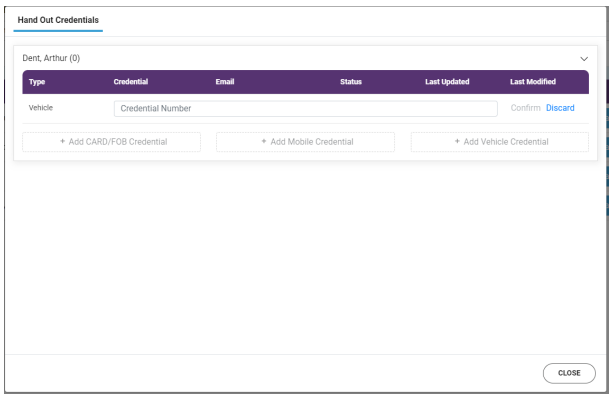


4. If a physical credential (card/FOB) is being handed out, click the **Add CARD/FOB Credential** button.
5. Enter the credential number from the card or fob being given to the person. See “Reading Credential Numbers” on page 83.
6. Click **Confirm**. To cancel the action, click **Discard**.
7. Present the physical credential to an online updater. This step is REQUIRED to complete the Hand Out process for physical credentials.



8. If a mobile credential is being handed out, click the **Add Mobile Credential** button.
9. Enter a credential name and email address.
   NOTE: The credential name can be anything to associate the credential with an individual, such as “Joe’s iPhone”.
   NOTE: The email address used for a mobile credential can only be used once. Each additional mobile credential for a resident must use a different email address.
10. Click **Confirm**. To cancel the action, click **Discard**.
11. If a vehicle credential is being handed out, click the **Add Vehicle Credential** button.
12. Enter the credential number from the vehicle tag being given to the person. See “Reading Credential Numbers” on page 83.
13. Click **Confirm**. To cancel the action, click **Discard**.
14. When finished handing out all the required credentials, click the **Close** button.

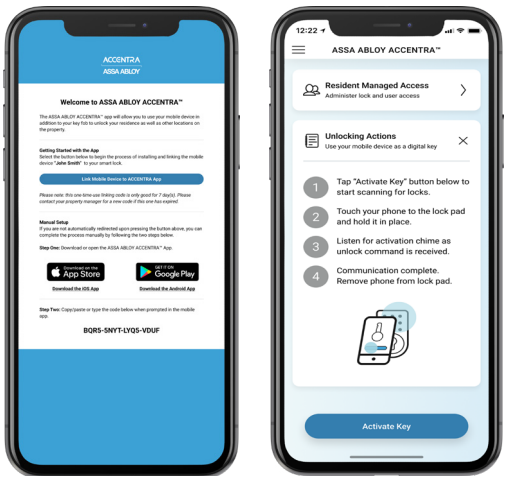




HAND OUT MOBILE CREDENTIAL

When a mobile credential is handed out, the user receiving the credential is sent an email to the entered email address.

That email contains a link to download the Multi-Family Management System access app and a code used to connect the app/mobile device to the Multi-Family Management System.



The user needs to follow the directions in the email and app to connect their device.

Once the mobile device is connected, the user can use the app to access locks and online updaters as assigned.

Once the mobile credential is handed out, the user has seven (7) days to link their device to the Multi-Family Management System before the credential expires. If the credential expires, the system administrator can resend the credential using the **Resend** button next to the credential from the Lease Information screen or Visitor Information screen.

READING CREDENTIAL NUMBERS

For cards and FOBs there are two types of multi-technology credentials available:

- SEOS offline + SEOS PACS online credentials:
  (Card Part Number: NTX600-ACCCRD-8K, FOB Part Number: NTX600-ACCFOB-8K)

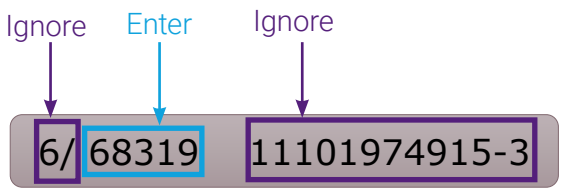
  These physical credentials (cards and FOBs) can be used in the ACCENTRA Multi-Family Management System and also in a third party Physical Access Control System (PACS) that reads HID High Frequency SEOS technology credentials.

- SEOS offline + SEOS PACS online + 125kHz proximity credentials:
  (Card Part Number: NTX600-ACCPRX-8K)

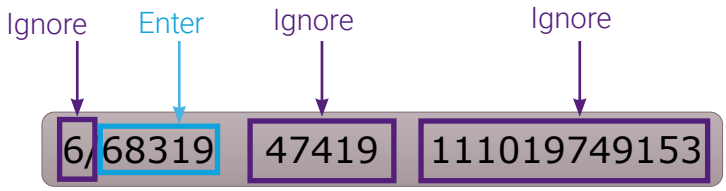
  These physical credentials (cards) can be used in the ACCENTRA Multi-Family Management System and also in a third party Physical Access Control System (PACS) that reads HID High Frequency SEOS technology credentials and in systems that read low frequency proximity credentials.

When entering a credential number on a card or FOB, enter the digits directly after the forward slash (/) and ignore all other number groups.

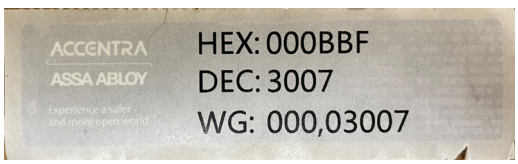
SEOS only format



SEOS and Prox Format



For vehicle credentials, enter the digits labeled “DEC:”. Ignore all other number groups.

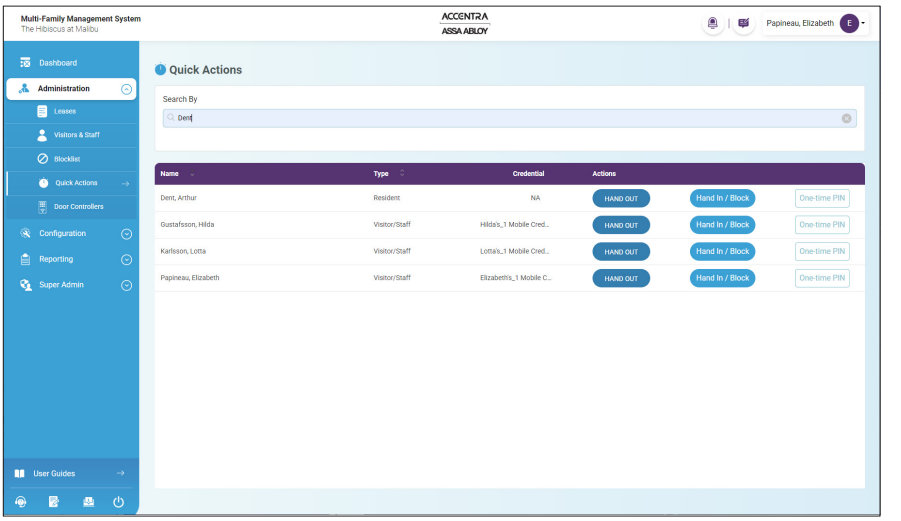


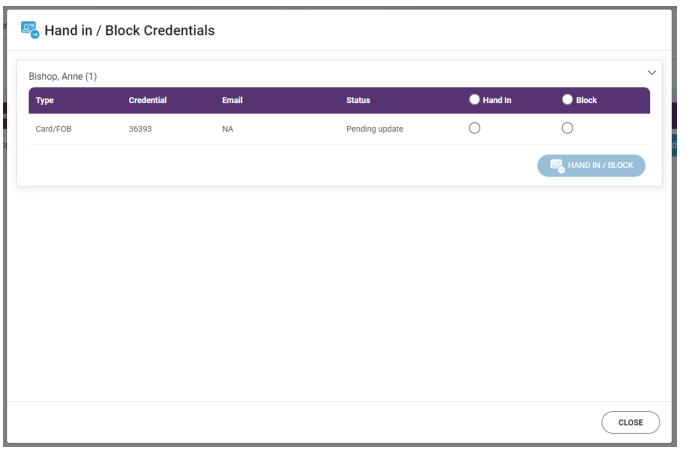
HAND IN

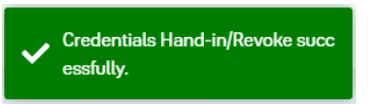
The Hand In feature allows the administrator to receive, or hand in, credentials from lease holders, residents, visitors and staff members so that the system knows which credentials are no longer assigned to a person.

To hand in a credential, do the following:

1. Click **Administration** and then click **Quick Actions** on the left side of the screen. The Quick Actions screen appears.
2. Enter a name or partial name in the Search By field. A list of names automatically appears containing the search criteria.
3. Click the **Hand In/Block** button next to the desired name. The Hand In/Block Credentials dialog box appears.
4. Select the Hand In radio button for credential(s) to hand in.
5. Click the **Hand In/Block** button. A success message appears.
6. Present the physical credential to an online updater. This step is REQUIRED so that the credential may be reassigned to a different system user.







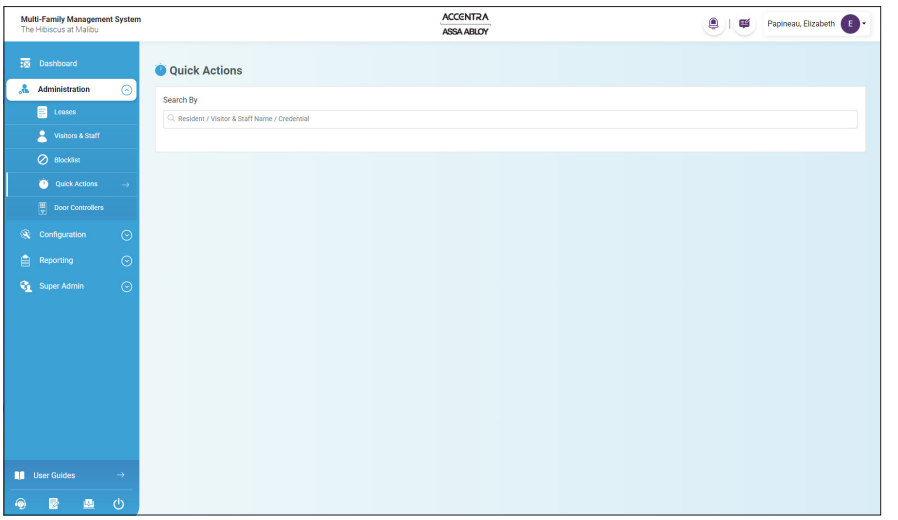
ONE-TIME PIN

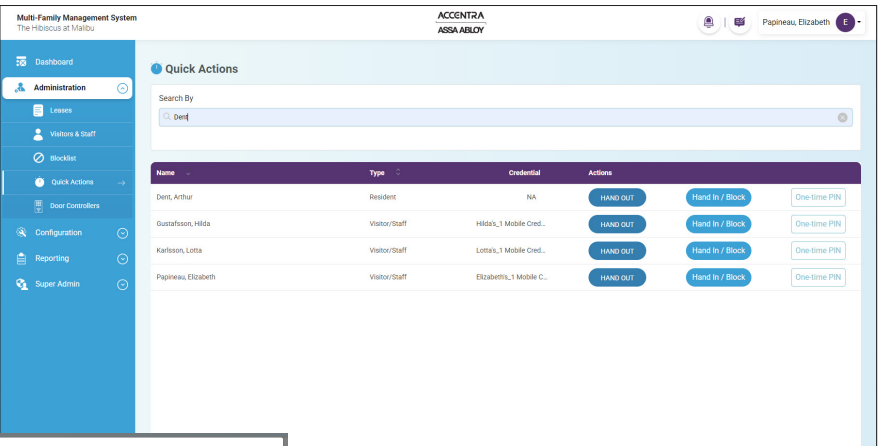
The One-Time PIN feature allows the administrator to issue a one-time numeric code to a person for an individual door so that the person can gain entry to that door one time.

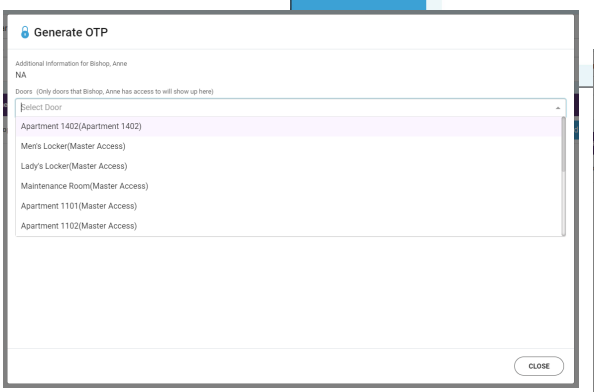
NOTE: the One-Time PIN can be used at any time twice, once to open/unlock a door and once to lock the door if one-touch locking is disabled. The One-Time PIN does not expire if another PIN is generated and used before a previously generated PIN.

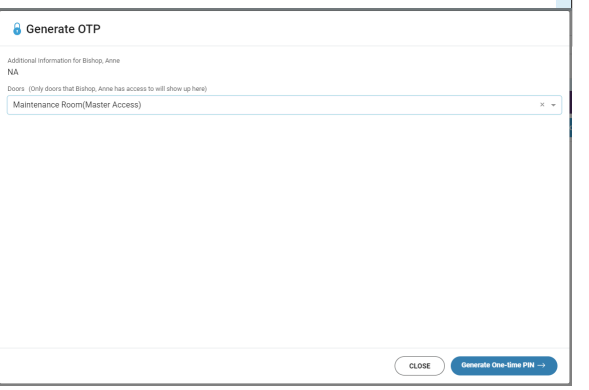
To issue a One-Time PIN, do the following:

1. Click **Administration** and then click **Quick Actions** on the left side of the screen. The Quick Actions screen appears.
2. Enter the name or partial name of the person to get a One-Time PIN in the Search By box.
3. Click the **One-Time PIN** button next to the person's name in the search results list. A Generate OTP dialog box appears.
4. Use the drop-down list to select the specific door to issue the One-Time PIN for.
5. Click the **Generate One-Time PIN** button.









A Generated One-Time PIN dialog box appears with the PIN code displayed. Make note of the PIN and provide it to the designated person. The person must enter the PIN and press the check mark button on the lock. *Note how many One-Time PIN numbers are left for the lock, as displayed in the dialog box*.

6. Click the **Close** button in the Generated One-Time PIN dialog box.

NOTE: When a lock reaches zero One-Time PINs left in its memory, it will need to be updated using the Multi-Family Configuration app in order to replenish the bank of PIN codes.

NOTE: See the Multi-Family Configuration Application User Guide for information on how to reset and reconfigure or update individual locks.

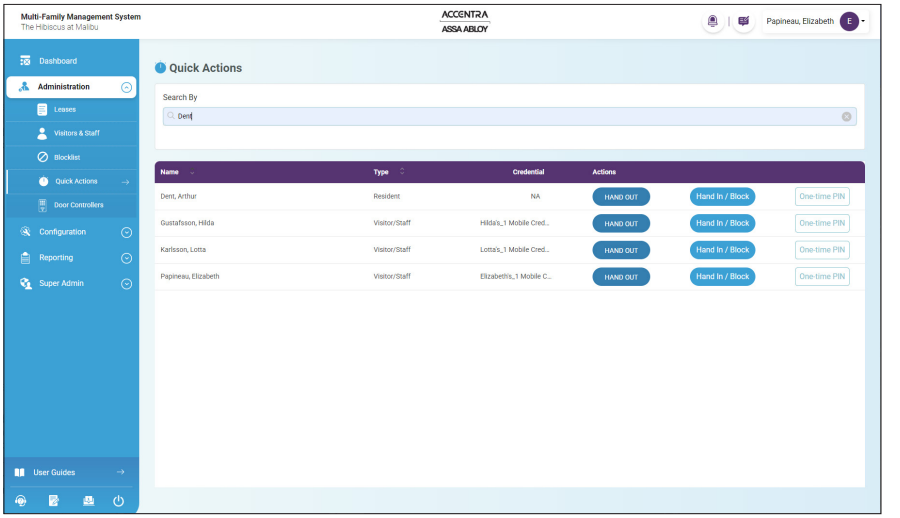
BLOCK

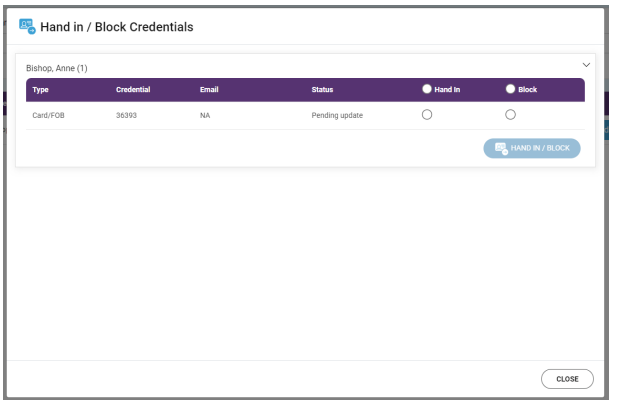
The Block feature is used to block credentials in the system. This allows the administrator to control a person's access without having to end a lease. If a person's credential is blocked, the next time they present their credential to an online updater, the credential will be removed from the system and the credential is wiped of all information.

NOTE: There is no way to remove a blocked credential from the blocklist. If the blocked credential holder is granted access, a new credential must be issued.

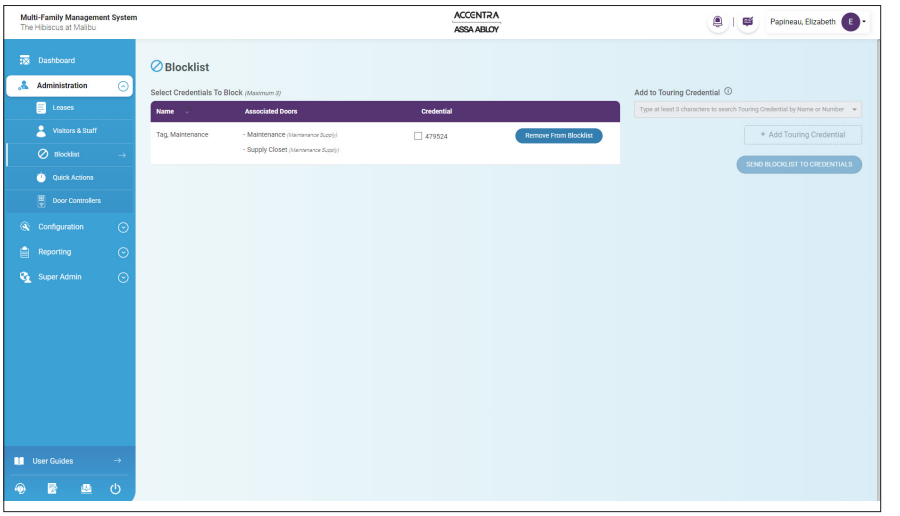
To block a credential, do the following:

1. Click **Administration** and then click **Quick Actions** on the left side of the screen. The Quick Actions screen appears.
2. Enter the name or partial name of the person to have their credential blocked in the Search By box.
3. Click the **Hand In/Block** button next to the name of the desired person. The Hand In/Block Credentials dialog box appears.
4. Click the **Block** radio button next to the credential to block.
5. Click the **Hand In/Block** button. A Block Credentials success dialog box appears.





BLOCKLIST



The Blocklist feature is used to block a credential from opening doors and allowing a person access to the facility. It can also be used to send the Blocklist to another physical credential so that offline locks can be updated quickly with the current Blocklist. The physical credential being used to update the offline locks must have access permissions to the locks.

It is also possible to unblock credentials and assign them back to their original user or allow them to be assigned to a different user.

BLOCK CREDENTIALS

To block a credential, do the following:

1. From the main screen, click **Administration** on the left side of the screen.
2. Select the resident or visitor/staff credential to block and click the Hand In/Block button on the Quick Actions screen. (See “Block” on page 87)

   OR

3. Navigate to the Visitor Information or Lease Information screen and select Hand In/Block from the **More Menu** button (ellipsis).
   (See “Leases” on page 64, “Visitors & Staff” on page 75)
   The credential is added to the Blocklist.

BLOCK USING OTHER CREDENTIALS

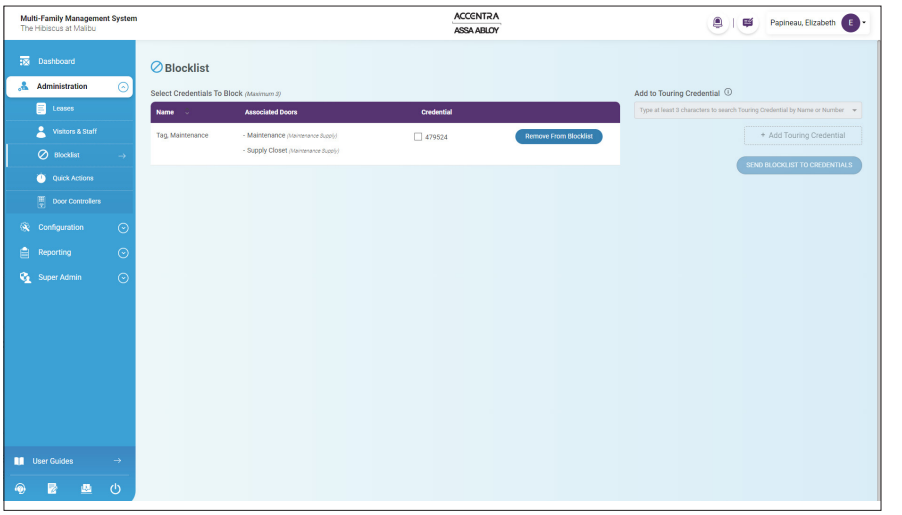
There is another method available to block physical credentials using the online updater and another person’s physical credentials. The administrator can use a second person’s physical credential to do the blocking. The second person’s physical credential must have access permissions with an “always on” schedule, to all doors for which the first person’s physical credential is to be blocked at the time the blocking is executed.

For example, the administrator chooses to block User 1 and selects User 2’s physical credential to do the blocking. User 2 presents their physical credential to an online updater and then to a lock. User 1 is now blocked from that lock. If there are multiple locks, User 2 must visit all of the locks User 1 has access to block User 1’s access.

To block a user using other physical credentials, follow the **Block** procedure above. When that is complete, click **Blocklist** on the left side of the screen.

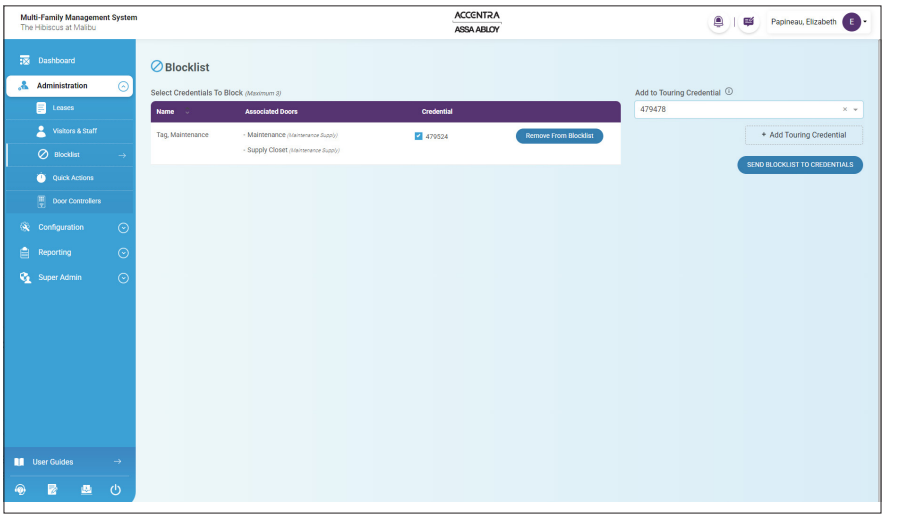
To send the Blocklist to a credential, do the following:

1. Click **Administration** and then click **Blocklist** on the left side of the screen. The Blocklist screen appears.



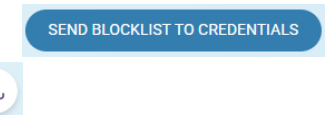
2. Select the blocked credential(s) from the list to be assigned to a touring credential by clicking the Credential check-box. A maximum of three (3) credentials (physical and/or mobile) can be selected.

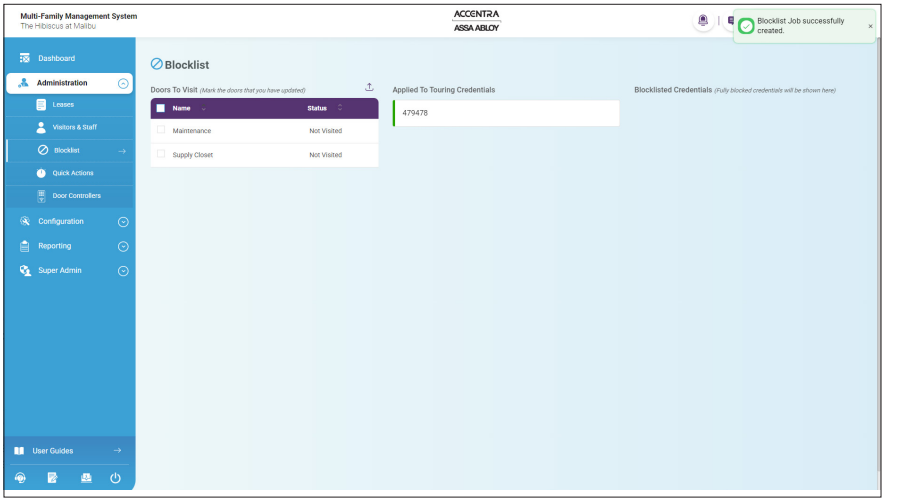
3. When the desired blocked credentials are selected, type the touring credential name or number in the text box on the right side of the screen.



4. To add another touring credential, click the **+Add Touring Credential** button. A maximum of three touring (3) credentials (physical and/or mobile) can be selected.

5. When finished adding touring credentials, click the **Send Blocklist to Credentials** button. A Blocklist job is created. Export the list of doors (as a PDF file) by clicking the **Export** button at the top of the list.

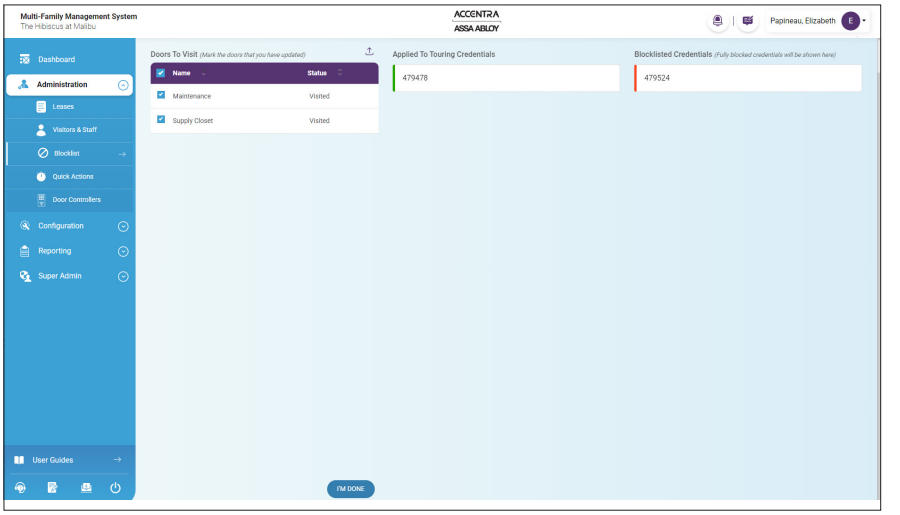


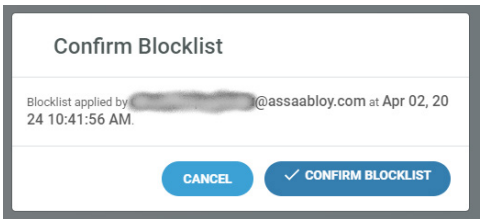


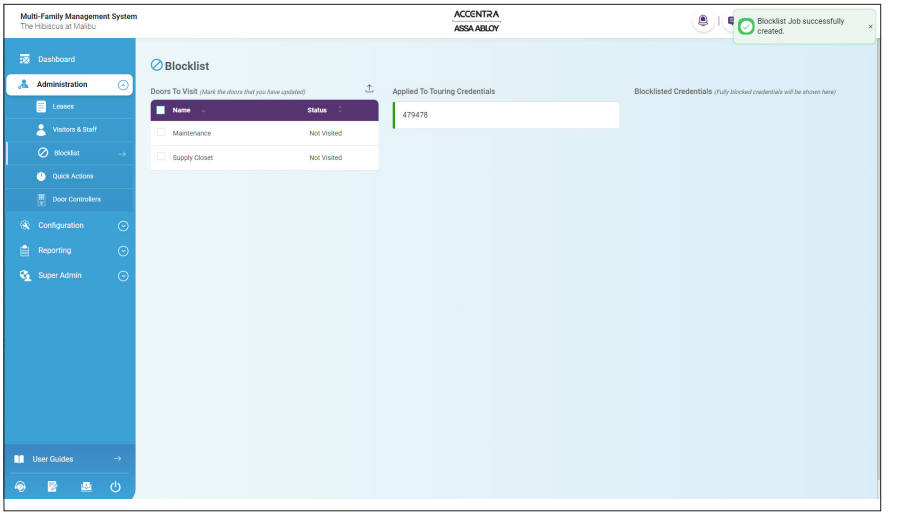
6. Present the credential to an updater so that the blocklist is loaded to the credential.

7. Present the updated credential to all of the offline locks that require updating with the blocklist.

8. When all of the required locks have been visited by the touring credential, check each lock on the Blocklist - Doors To Visit column by clicking the check-box next to each lock/door, or by clicking the check box next to the Name heading.
9. Once all of the locks have been visited, click the **I'm Done** button at the bottom of the screen. The Confirm Blocklist dialog box appears.
10. Click the **Confirm Blocklist** button. A Blocklist updated successfully message appears in the upper right corner of the screen.





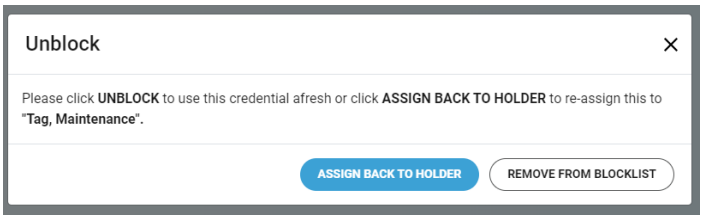


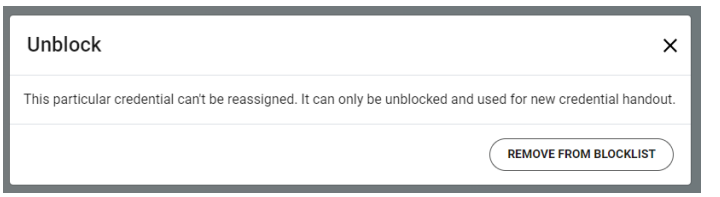
UNBLOCK CREDENTIALS

Unblocking a credential allows the credential to be assigned back to the original credential holder, or re-assigned to a different resident.

To unblock a credential, do the following:

1. From the main screen, click **Administration** on the left side of the screen.
2. Click **Blocklist**. The blocklist is displayed.
3. Select a credential from the blocklist.
4. Click the **Remove from Blocklist** button. The Unblock dialog box appears. The Unblock dialog box can show both the **Assign Back to Holder** button and the **Remove from Blocklist** button, or only the **Remove from Blocklist** button.
5. Click the **Assign Back to Holder** button to assign the credential back to the original credential holder as listed in the dialog box.
   OR
   Click the **Remove from Blocklist** button to put the credential in an unused state so it can be handed out to a different resident.
6. The credential is removed from the blocklist.

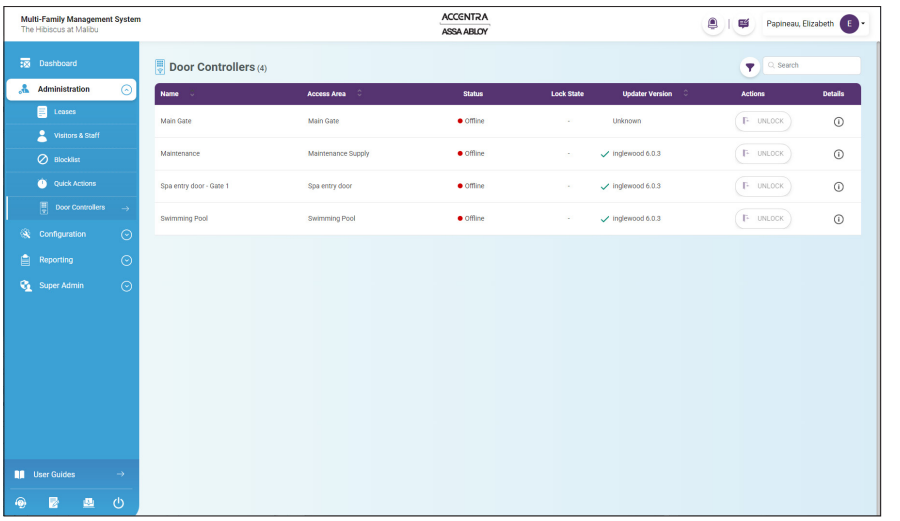




DOOR CONTROLLERS

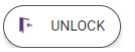
Door Controllers feature allows the administrator to remotely unlock a door with an online controller and have visibility to the online status of the doors controlled by an online updater. If a door controller is offline, remote actions cannot be performed. The administrator can search for a door controller by name using the search function.
This feature requires the latest door controller firmware update to be installed.

To allow remote access to a door, do the following:

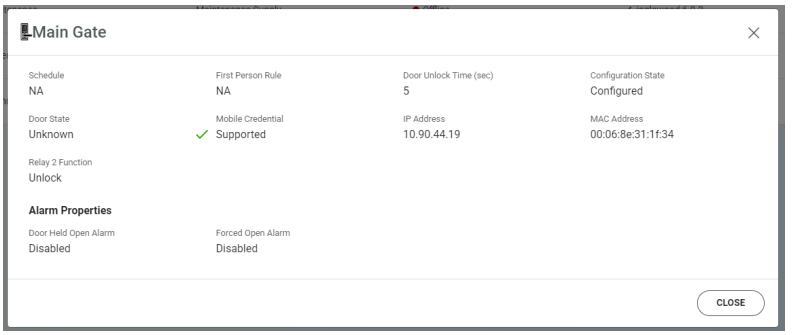


1. Click **Administration** and then click **Door Controller** on the left side of the screen. The Door Controller screen appears.
2. Use the **Search** box to find the desired door controller. Enter a name or partial name, a list of door names automatically appears containing the search criteria.

3. Click the **Unlock** button next to the door information to automatically unlock the door. This function is only available if the door controller is online.



4. A success message appears in the upper right corner of the screen. The door remains unlocked for five seconds before re-locking.
5. Use the **Info** button in the Details column to see more information about the door controller.

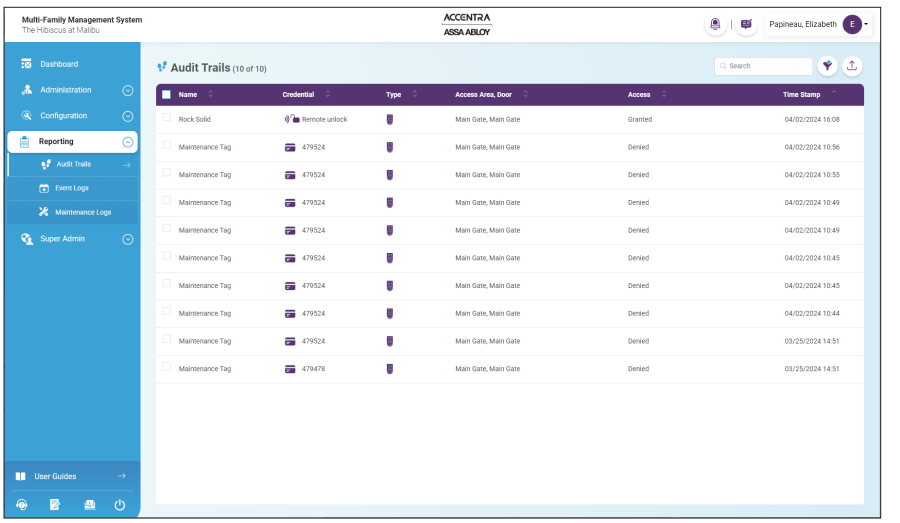


6. REPORTING

The Reporting service manages the different types of reports and logs available in the Multi-Family Management System. These include Audit Trail, Event Log, and Maintenance Log.

AUDIT TRAIL

The Audit Trail feature allows the administrator to view access logs collected from a credential thus providing a historical record of the locks and online updaters, to which a credential has been presented. It includes time, date, and transaction status, such as granted or denied, etc.



The columns include:

- Name - name of credential holder
- Credential - credential number, credential type icon (card/fob/mobile), or remote unlock
- Type - type of lock (online/offline)
- Access Area, Door - name of the access area and door that was accessed
- Access - access event (denied, granted, denied validity)
- Time Stamp - date and time the access event occurred

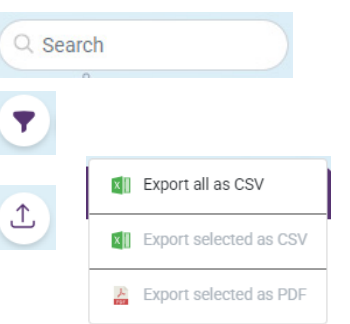
Some of the reportable events that appear on the Audit Trail report are:

- Granted - Access policies and time are valid for this location and time
- Denied - Access policies are not valid for this location
- Denied Validity - Credential validity/time has expired, or the credential has not been presented to an online updater during the revalidation time period.

Use the **Search** box to search for a specific user, credential, access area/door, or access event.

Use the **Filter** button to search for specific dates/times.

Use the **Export** button to create a .CSV file that includes all the audit events, or a .CSV or .PDF that includes just selected audit events.

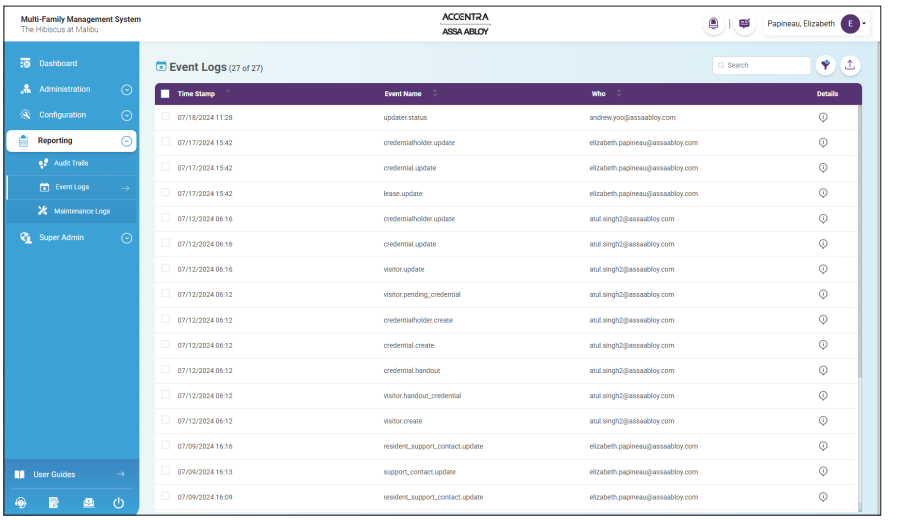


EVENT LOGS

The Event Logs feature allows the administrator to view all actions performed by the user/administrator in the Multi-Family Management System software application. Events like Visitor Created, Credential Handout, or Lease Created, along with the time and date and the administrator identity are included in the log.

The reportable events are in the format of the events is “what” was touched/changed/modified and “how” the what was touched/changed modified. For example: credential.create indicates a credential was created. schedule.update indicates a schedule was changed/updated.

Some of the reportable events that appear on the Event Logs report are:



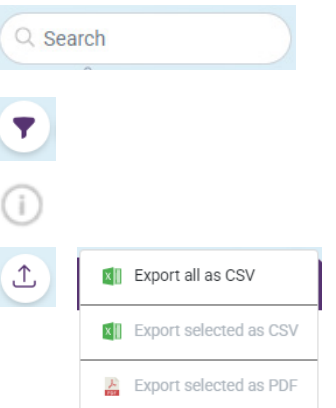
- Lock Status/Updater Status - These events show the state of the updater or lock being configured or not.
- OTP_params.update - This event occurs when the administrator/user changes OTP settings in the Configuration tools.
- Seos.issue/revoke-setup card - This event occurs when an administrator configures or re-configures a lock or updater using the configuration app.
- Seos.revoke-setup card - Access-right/profile.update - This event occurs when an administrator changes the access rights or access profiles in the Configuration tools.
- lease.assign/handout_credential - This event occurs when the administrator assigns a tenant to a lease and hands out credentials to tenants.

Use the **Search** box to search for a specific event (Event Name column) or user (Who column).

Use the **Filter** button to search for specific dates/times.

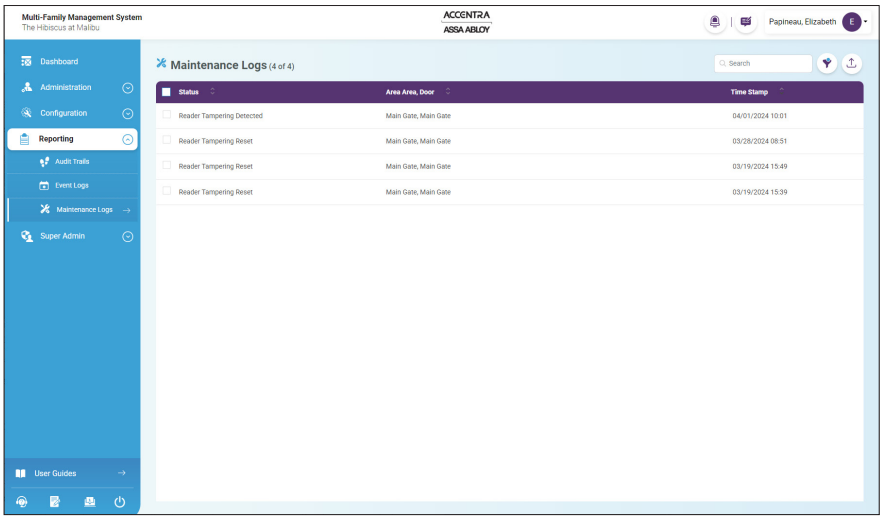
Use the **Info** button in the Details column to see more information about the event.

Use the **Download** button to create a .CSV file that includes all the audit events, or a .CSV or .PDF that includes just selected audit events.



MAINTENANCE LOGS

The Maintenance Logs feature allows the administrator to view lock status events such as lock jammed and low battery. These are carried on credentials through an online updater back to the Multi-Family Management System.



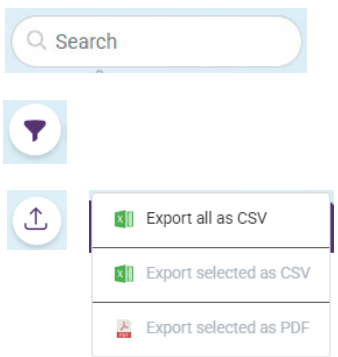
Some of the reportable events that appear on the Maintenance Logs report are:

- Battery Low - This events occurs when the battery life of a lock is low.
- Lock Jammed - This event occurs when the deadbolt is unable to be properly moved by the motor on locking or unlocking.
- System Event - This event occurs when operating system level events occur (update, reconfigure, change of lock settings).
- Tampering Detected
- Failed to Unlock
- Door Held Open - This event occurs when the door position sensor does not sense the door in a closed position for a period of time.
- Door Forced Open - This event occurs when the door position sensor senses the door is open but no open request was given (presenting credential/turning inside handle/pressing inside bar).

Use the **Search** box to search for a specific event (Event Name column) or user (Who column).

Use the **Filter** button to search for specific dates/times.

Use the **Download** button to create a .CSV file that includes all the audit events, or a .CSV or .PDF that includes just selected audit events.



7. TROUBLESHOOTING AND COMMON ISSUES

Problem	Common Causes	Solution
Lock is configured successfully but status is not changed in the Multi-Family Management System	Mobile device does not have any internet connection when configuration is performed.	Check WiFi/Cellular network is turned on in the mobile device.
		Check WiFi/Cellular network has coverage at the location of the door.
	If account has access to different multiple systems, and wrong system was selected when configuration was performed	Go back and verify the correct system was selected. Possibility that the door lock may have the same name on multiple different systems.
Mobile credential not opening offline lock or online updater	Credential revalidation period has lapsed.	Revalidate mobile credential by turning on and connecting with WiFi or cellular network.
	Credential does not have access within the lock schedule.	Check lock access areas, profiles and schedules to determine if credential should have access during the time it was presented.
	Online updater or lock is not configured.	Configure updater/lock using the Multi-Family Management System Configuration application.
	Time on offline lock is not updated.	Update time on offline lock with update time function in Multi-Family Management System Configuration application.
	Mobile Access device presentation.	Mobile device must be presented to the lock or online updater within read range to initiate the mobile credential read. A static hold is recommended on the face of the target lock/updater to retry.
	Mobile Access app is not open or “Activate Key” button has not been tapped.	Unlock mobile device, open Multi-Family Management System access app, tap “Activate Key” button, place mobile device within the read range of the target lock/online updater.
	Mobile device is presented to the lock/online updater prior to tapping “Activate Key” button.	Move the mobile device 1 to 2 feet away from the lock/online updater, wait approximately 5 seconds for the lock light to go dark, tap “Activate Key” and then present mobile device to lock.

Problem	Common Causes	Solution
User is not able to connect their mobile device to the Multi-Family Management System	Invitation code has expired.	Issue a new mobile credential with a new invitation code. Invitation code must be used within seven (7) days of issuance.
	Invitation code entered incorrectly.	Ask user to copy/paste invitation code into the Mobile Access app
	Credential name does not match the one in the Multi-Family Management System.	Verify correct credential name.
	Same email address used for multiple mobile credentials	Re-issue credential using a different email address.
Credentials denied at the updater when updater is configured and online	Credential does not have access.	Check to ensure credential has access to the lock controlled by the updater (areas, profiles, schedules).
	Controller is configured but reader was changed.	Updater needs to be reconfigured to save the correct configuration in both the controller and reader. Use the Multi-Family Management System Configuration app.
Cards and/or FOBs being denied access at offline door	Credential has not been handed out with access permissions.	Hand out credential and present to online updater.
	Credential does not have access to opening.	Check to see if credential was given access to opening.
	Credential was handed out but was not presented to online updater.	Present credential to online updater.
	Credential was blocked at the opening.	Check to see if credential was added to block list for opening. If on block list, new credential will need to be issued.
	If batteries within the lock have died and not been replaced, the lock loses the ability to maintain its internal clock.	Update time on offline lock with update time function in Multi-Family Management System Configuration app.
Offline door not unlocking when One Time PIN is entered	OTP being used on incorrect door.	Ensure user is entering OTP on the correct door. Issue new OTP if needed.
	More than one OTP issued for the same door. Later issued code was used before the previous code.	Issue new OTP to user.
	OTP codes in lock have run out, lock requires updating to seed new set of OTP codes.	Use Multi-Family Management System Configuration app to update lock.

Problem	Common Causes	Solution
Unable to issue One Time PIN (OTP) code to user	OTP codes in lock have run out.	Use Multi-Family Management System Configuration app to update lock.
Door added to Access Group but credential being denied access	Offline lock was not updated with new Access Group.	Use Multi-Family Management System Configuration app to update offline lock.
	Access Profile only has access area attached.	Verify that the Access Profile has the Access Group attached.
Credentials have access to doors they are not supposed to access	Access Profiles have multiple different access areas/groups associated.	Check the access profile and verify the areas/groups selected are correct. To further verify, check/save the .csv file for access groups and verify which door(s) the group is associated with.
	Credential has multiple different profiles attached to it.	
Not able to give residents permission to Resident Managed Access™ functions	Resident Managed Access™ features not enabled for the site.	Contact the site Certified Integrator for assistance enabling Resident Managed Access™ functionality.
Resident mobile credential only has guest permissions associated	Guest credential installed on same mobile device as resident mobile credential, in the same Multi-Family Management System.	Issue new mobile credential for the resident with appropriate resident permissions. This automatically removes the guest credential.
		This does not affect physical credentials. A physical credential can be used to access the resident's regular access areas and the mobile credential can be used for guest access permissions.
		Have the resident use two different mobile devices, one for resident access and one for guest access.

The ASSA ABLOY Group is the global leader in access solutions. Every day, we help billions of people experience a more open world.

ASSA ABLOY Opening Solutions leads the development within door openings and products for access solutions in homes, businesses and institutions. Our offering includes doors, frames, door and window hardware, mechanical and smart locks, access control and service.

ACCENTRA

ASSA ABLOY

Contact Us

U.S.A.
ASSA ABLOY ACCENTRA
Address: 225 Episcopal Road
Berlin, CT 06037-4004
Tel: 1-800-438-1951
Fax: 1-800-338-0965
accentra.assaabloy.com

Canada:
ASSA ABLOY Door Security Solutions Canada
Address: 160 Four Valley Drive
Vaughan, Ontario L4K 4T9
Tel: 1-800-461-3007
Fax: 1-800-461-8989
assaabloydss.ca

International:
ASSA ABLOY Americas International
Tel: 1-905-821-7775
Fax: 1-905-821-1429
assaabloyai.com

Phone
1-800-810-9473
Customer Service Email
customerservice.accentra@assaabloy.com
Technical Product Support Email
techsupport.accentra@assaabloy.com
Order Entry Email
orders.accentra@assaabloy.com
Fax
1-800-338-0965
Website
www.accentra-assaabloy.com

80-8150-0060-999
07/24