

OPENPATH
ACCESS CONTROL SYSTEM
USER GUIDE FOR
ADMINISTRATOR WEB PORTAL
V3.4

Table of Contents

[Openpath Admin Portal User Guide](#)

[NEW FEATURES | SEPTEMBER 2021](#)

[GETTING STARTED](#)

[TERMINOLOGY](#)

[LOGGING IN](#)

[DASHBOARDS](#)

[ACTIVITY DASHBOARD](#)

[CAMERA SNAPSHOTS](#)

[ENTRY DASHBOARD](#)

[HARDWARE DASHBOARD](#)

[CUSTOM DASHBOARDS](#)

[USERS](#)

[USER MANAGEMENT](#)

[CREATE USER](#)

[IMPORT USERS](#)

[ISSUE CREDENTIALS](#)

[ADD A MOBILE CREDENTIAL](#)

[ADD A WIEGAND CREDENTIAL](#)

[USER ACCESS](#)

[USER SECURITY](#)

[MANAGING USERS](#)

[GUEST ACCESS LINKS AND WEBHOOK URLS](#)

[GROUP MANAGEMENT](#)

[CREATE GROUPS](#)

[ROLE MANAGEMENT](#)

[CREATE ROLES](#)

[GRANULAR PERMISSIONS](#)

[USER SCHEDULES](#)

[CREATE USER SCHEDULE](#)

[MULTIPLE SCHEDULES](#)

[CUSTOM FIELDS](#)

[SITES](#)

[SITE MANAGEMENT](#)

[CREATE SITES](#)

[ZONE MANAGEMENT](#)

[ZONE SHARING](#)

[CREATE ZONE](#)

[ANTI-PASSBACK AND OCCUPANCY MANAGEMENT](#)

[RESET ANTI-PASSBACK](#)

[MULTIPLE AREA ANTI-PASSBACK](#)

[ENTRY MANAGEMENT](#)

[CREATE ENTRY](#)

[ENTRY SETTINGS](#)

[ENTRY BEHAVIOR](#)

[ALLEGION WIRELESS LOCK](#)

[CONTACT SENSOR](#)

[ENTRY/EXIT HARDWARE](#)

[OPENPATH READER](#)

[REQUEST TO EXIT](#)

[WIEGAND DEVICE](#)

[ADD CONTROL](#)

[ENTRY STATE MANAGEMENT](#)

[ADD ENTRY STATE](#)

[TRIGGER METHOD DEFINITIONS](#)

[ENTRY SCHEDULES](#)

[LOCKDOWN PLAN MANAGEMENT](#)

[CREATE LOCKDOWN PLAN](#)

[TRIGGER A LOCKDOWN PLAN](#)

[HARDWARE](#)

[ACU MANAGEMENT](#)

[CREATE ACU](#)

[ADD EXPANSION BOARD](#)

[EDIT ACU PORTS](#)

[END OF LINE SUPERVISION](#)

[READER MANAGEMENT](#)

[CREATE READER](#)

[WIRELESS LOCK MANAGEMENT](#)

[EDIT LOCK](#)

[WIRELESS LOCK GATEWAY MANAGEMENT](#)

[REPORTS](#)

[INTEGRATIONS](#)

[GOOGLE G SUITE](#)

[MICROSOFT AZURE ACTIVE DIRECTORY](#)

[OKTA](#)

[ONELOGIN](#)

[SINGLE SIGN-ON](#)

[MANUALLY SYNC](#)

[CAMIO](#)

[RHOMBUS](#)

[MILESTONE](#)

[CISCO MERAKI](#)

[ENVOY](#)

[SLACK](#)

[ALLEGION](#)

[ZAPIER](#)

[BUTTERFLYMX](#)

[WEBHOOKS](#)

[CONFIGURATIONS](#)

[RULES ENGINE](#)

[ALERT SETTINGS](#)

[MOBILE APP](#)

[BADGE VIEW](#)

[BADGE TEMPLATES](#)

[ADMINISTRATION](#)

[ACCOUNT](#)

[SECURITY SETTINGS](#)

[QUICK START](#)

[MY PROFILE](#)

[USER DATA MODEL](#)

[CONFIGURING OPENPATH WITH LEGACY SYSTEMS](#)

[REGULATORY](#)

Openpath Admin Portal User Guide

NEW FEATURES | SEPTEMBER 2021

- Now you can choose to deliver Activity Logs via email. There is no size limit on email reports and you can send the report to multiple recipients. See [REPORTS](#).
- Perform more batch actions on the User Management page, including create and send mobile credentials and enable/disable remote unlock permissions. See [MANAGING USERS](#).

GETTING STARTED

The Openpath Control Center is an online portal where Administrators can configure the Openpath Access Control system through an Internet browser. This user guide will explain how to get started in the Control Center, manage users and hardware, and provide access to your entries.

Note: Some features in the Control Center are only available in certain software packages and as add-on features. Also, depending on your role, not all of these features may be visible to you.

TERMINOLOGY

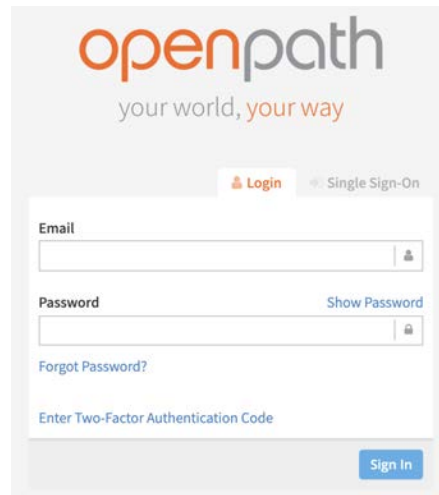
- **ACU:** A cloud-based control panel that manages access to a secured area.
- **Cloud Key Credential:** A credential that lets users generate links to provide temporary access through the Openpath Mobile App or through the Control Center.
- **Control Center:** An online portal that lets administrators manage users, set up entries and permissions, and troubleshoot hardware.
- **Credential:** A key presented to a reader to gain access to an entry. Examples include cards, key fobs, and mobile credentials.
- **Entry:** A door, gate, turnstile, elevator floor, or other point of access. Often secured with a reader or wireless lock.
- **Entry State:** Determines whether an entry is locked or unlocked and defines what kinds of credentials and trigger methods are valid.
- **Mobile Credential:** An access method tied to a user's smartphone through the use of the Openpath Mobile App.
- **Openpath Mobile App:** Used for providing mobile credentials and remote unlock for users. The app is available for iOS and Android devices.

- **Remote Unlock:** A feature that lets users unlock an entry via the Openpath Mobile App without needing to be in range of the Reader.
- **Request to Exit:** A sensor that detects when someone is exiting an entry which lets the Smart Hub ACU know to unlock the door.
- **Schedule:** A set of defined dates and times that can be used to restrict access to entries or users.
- **Site:** A physical location (usually a building) that contains zones and entries.
- **Smart Reader:** A device installed near an entry capable of reading information stored on key cards, fobs, and Openpath mobile credentials.
- **Trigger Method:** A combination of credential type and 1FA/2FA.
- **User:** A person defined in the Control Center with credentials.
- **Wiegand Reader:** A device installed near an entry capable of reading information stored on a Wiegand card and transmitting to an access control unit.
- **Zone:** Contains one or more entries within a site. Zones are the units of physical access permissions that you assign to users and groups.
- **1FA:** Single-Factor Authentication.
- **2FA:** Two-Factor Authentication.

LOGGING IN

1. Go to <https://control.openpath.com/login>
2. There are two ways to log in. If you received admin credentials through Openpath, use the **Login** tab. In order to use the **Single Sign On** (SSO) tab, your organization must have enabled the feature when setting up [GOOGLE G SUITE](#), [MICROSOFT AZURE ACTIVE DIRECTORY](#), [OKTA](#), or [ONELOGIN](#).

Note: If you try logging in via SSO and get an error asking for your namespace, that is because your organization has enabled SSO for two or more identity providers. Ask the admin who set up the identity provider integrations for the correct namespace to use. See also [USER DATA MODEL](#).

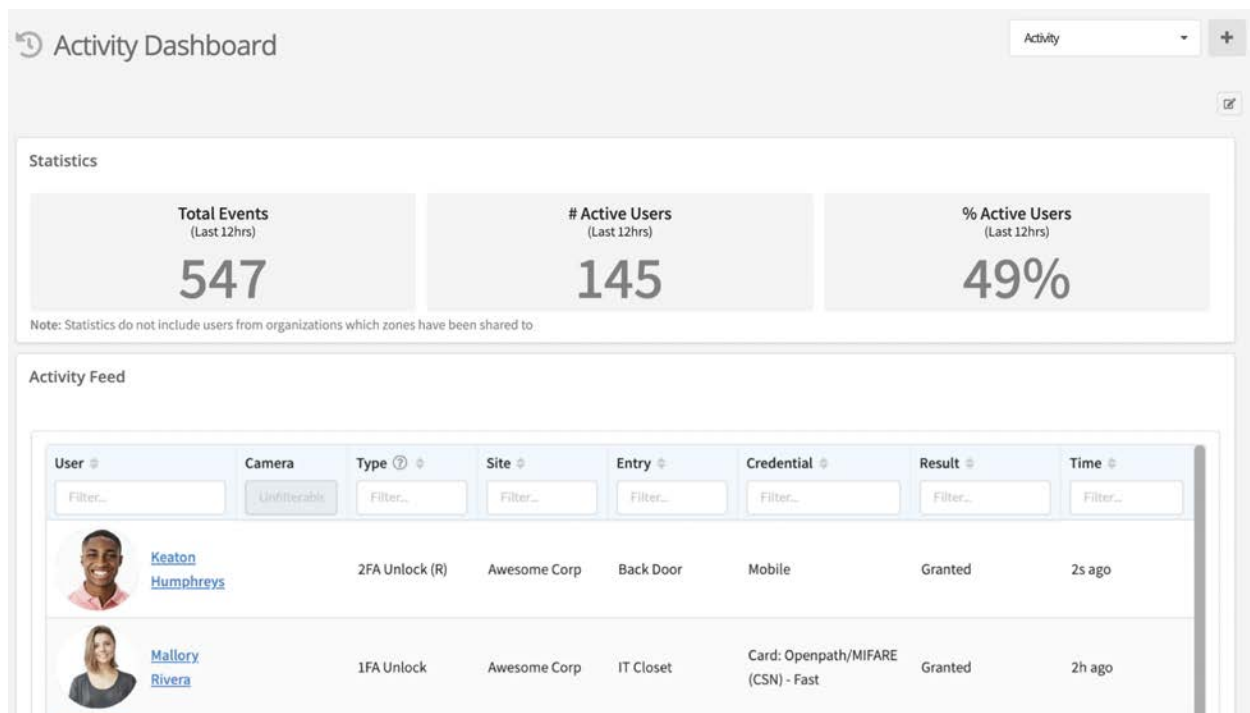


The login screen features the Openpath logo and tagline 'your world, your way'. It includes a 'Login' button with a user icon and a 'Single Sign-On' link. Below these are input fields for 'Email' and 'Password', with a 'Show Password' toggle for the password field. There are also links for 'Forgot Password?' and 'Enter Two-Factor Authentication Code'. A 'Sign In' button is at the bottom right.



DASHBOARDS

ACTIVITY DASHBOARD

Once logged in, you'll see the Activity Dashboard. This page shows a live feed of access events from the past hour, as well as statistics about event activity and active users. Click on the name of a user to go to their User Details.

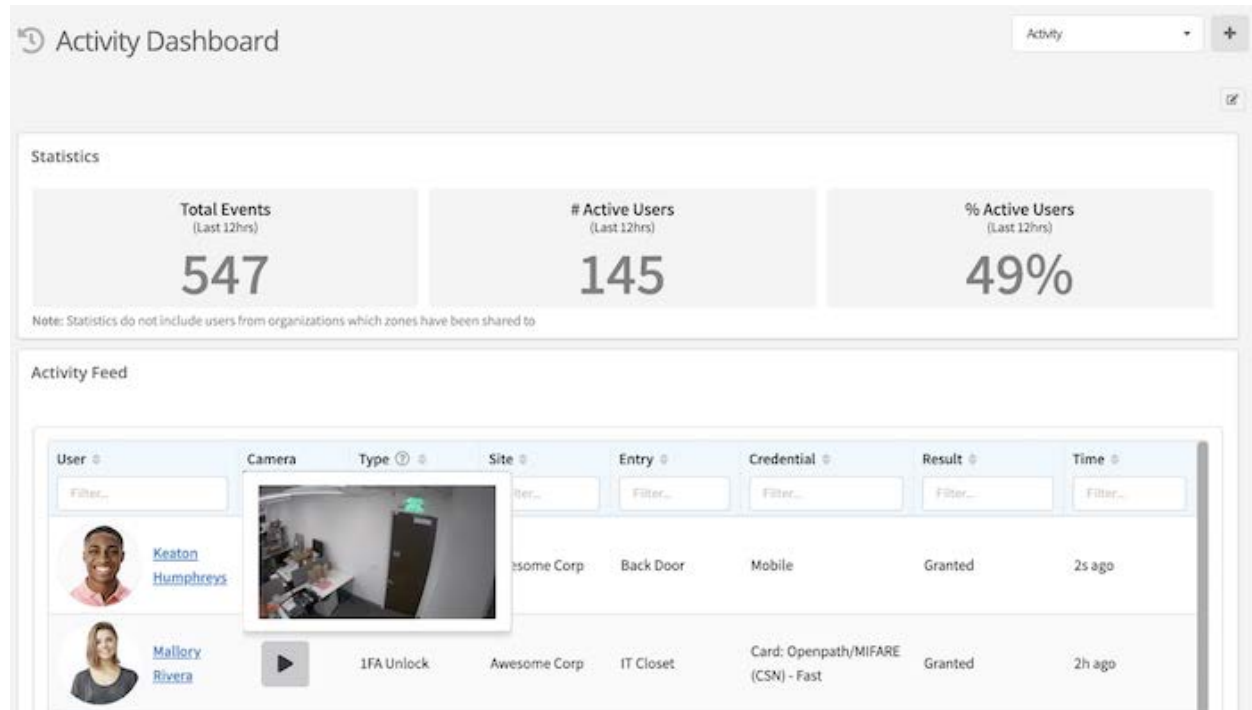


The Activity Dashboard provides a comprehensive overview of system activity. It includes a 'Statistics' section with three key metrics: Total Events (547), # Active Users (145), and % Active Users (49%). Below this is an 'Activity Feed' table showing individual access events.

User	Camera	Type	Site	Entry	Credential	Result	Time
 Keaton Humphreys	Unfilterable	2FA Unlock (R)	Awesome Corp	Back Door	Mobile	Granted	2s ago
 Mallory Rivera		1FA Unlock	Awesome Corp	IT Closet	Card: Openpath/MIFARE (CSN) - Fast	Granted	2h ago

CAMERA SNAPSHOTS

If you have the Cisco Meraki integration enabled, you'll see a Camera column in the Activity Dashboard, where you can view snapshots of entry events by hovering over the Play icon. Click on the Play icon to view the video footage in the Meraki dashboard. Snapshots may take up to a minute to appear in the Openpath Control Center.



ENTRY DASHBOARD

The Entry Dashboard shows a live status of every entry in your site.





Home > Dashboards > Entry Dashboard

Entry Dashboard

Entry

Entry Status ⓘ

1-10 of 49

Entry Name ⓘ	Camera	Entry State ⓘ	Lock State ⓘ	Door State ⓘ	Unlocks (12hrs) ⓘ	Last Activity ⓘ
Back Door	 	Convenience	Locked Unlock	Closed since Feb. 8, 2021 7:21:57 pm	3	 Keaton Humphreys Today at 12:39:36 pm
Storage Closet		Convenience	Locked Unlock	No Sensor	0	 Mallory Rivera Feb. 19, 2021 5:31:20 pm

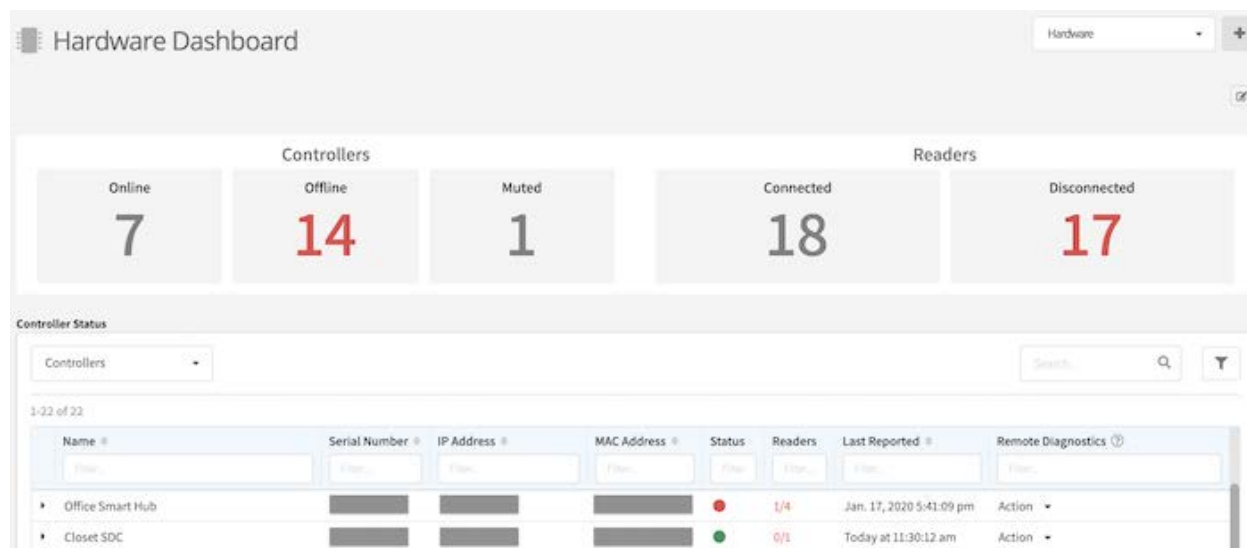
This is where you can see your organization's usage statistics as well as the current lock state for entries. The data on the Dashboard is real time, so as soon as an entry unlock request is made or denied or a lock state changes, the data displayed will update immediately.

If you have a Cloud Key and remote unlock permissions (and the entry's state also allows remote unlock requests), you can unlock entries from the Main Dashboard by clicking the Unlock button next to the entry's name.

Note: If a door is ajar or not properly closed, the Door Ajar alarm will be prominently displayed in the Door State column.

HARDWARE DASHBOARD

The Hardware Dashboard is where you can get a high level overview of your organization's Controllers (ACUs) and readers.



In the Controller Status table under the Remote Diagnostics column, you can perform the following actions:

- **Identify:** Identify a Controller to verify that the physical wiring matches the Control Center configuration. Clicking this will cause the Status LED on the Controller to flash green.
- **Refresh:** Refresh a Controller to send the latest data from the physical device to the Control Center.
- The **Restart** functions will restart individual software services on the Controller:
 - **Restart API Server:** The core application that processes authorization, authentication, and execution of unlock requests. Restart this service if you're having issues with the mobile app, such as unlock requests not working.
 - **Restart Cloud Communicator:** The service that receives live messages from the cloud, including entry-related configuration changes, user permissions changes, and cloud-based unlock requests. Restart this service if changes (new credentials, new schedules) made on the Control Center aren't syncing with the ACUs or if you're experiencing issues with remote unlock requests.
 - **Restart Hardware Communicator:** The service that sends and receives data between the ACU core and peripheral hardware. Restart this service if you're experiencing issues with readers or expansion boards.
- **Mute:** Muting a Controller changes its status icon to gray on the Hardware Dashboard. It will not affect any alerts or rules regarding the Controller, and it will only appear as muted on your browser.

Note: Restarting a service may interrupt the affected service for up to 60 seconds. We recommend restarting services one at a time, waiting a few seconds after restarting one before restarting the next.

You can also perform Remote Diagnostics actions on readers. Expand an ACU to see its associated readers. Under the Remote Diagnostics column, you can perform the following actions:

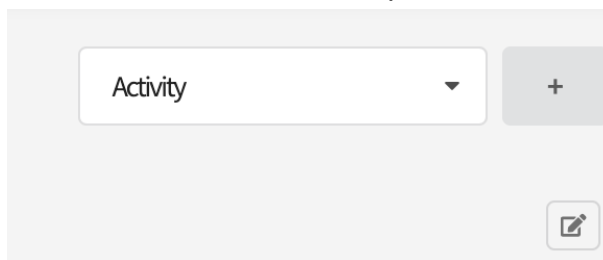
- **Identify:** Identify a reader to verify that the physical wiring matches the Control Center configuration. Clicking this will cause the following:
 - the reader's outer ring LED will light up
 - the reader's center dot will light up green
 - the reader's buzzer will beep several times
- **Restart:** Restart a reader to force a reboot. This will interrupt services provided by the reader for up to 60 seconds.

CUSTOM DASHBOARDS

The Custom Dashboard feature lets you create personalized views comprised of widgets that you can use in your org in addition to Openpath's default dashboards (Activity, Hardware, and Entry).

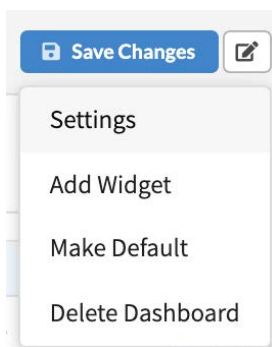
To create a custom dashboard:

1. Next to the dashboard dropdown, click the **Add Dashboard** button (+)



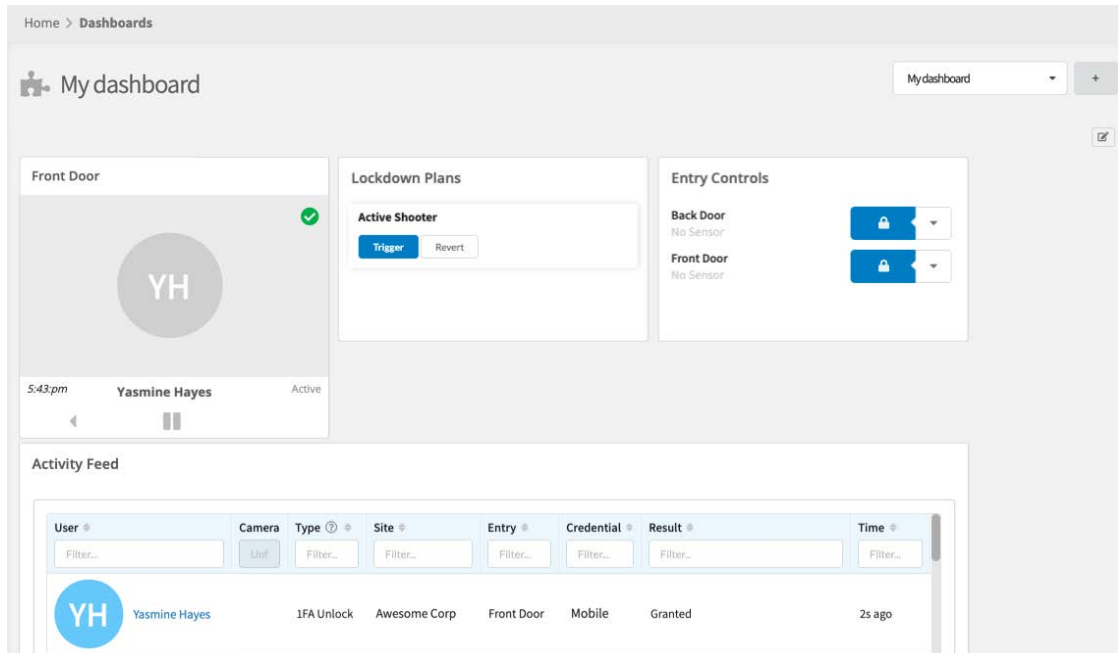
2. Enter a name for the dashboard, then click **Save**

3. Click the edit icon to change settings, add widgets, make a dashboard your default view, or delete a dashboard



1. **Activity Feed Widget** is a live feed of entry activity log
2. **Entry Controls Widget** lets you pin one or more entries to the dashboard and lets you temporarily unlock them instantly, or keep them unlocked for 5, 10, 15, or 60 minutes
 1. **Note:** You will need a [Cloud Key credential](#) and appropriate access to the entry (or entries) in order to trigger unlocks
3. **Lockdown Widget** displays all lockdown plans in the org, with buttons to trigger and revert plans
 1. **Note:** You will need [user permissions](#) on the lockdown plans to trigger and revert
4. **Identity Verification Widget** lets you monitor access events at a particular entry
5. **Event Feed Widget** is a live feed of entry events, door ajar and door propped open alarms, lockdown activation
6. **Occupancy Widget** shows you the occupancy of Areas configured using Anti-Passback

1. **Note:** You will need to configure Anti-Passback and set occupancy limits to use this widget
7. **Hardware Widget** displays the number of controllers and readers configured in the system as well as their online status
8. **Statistics Widget** displays the total events, number of active users, and percentage of active users from the last 12 hours
4. You can click and drag to place the widget anywhere on the dashboard, as well as resize the widget by clicking and dragging the lower righthand corners
5. Click **Save Changes** when you're done customizing the dashboard



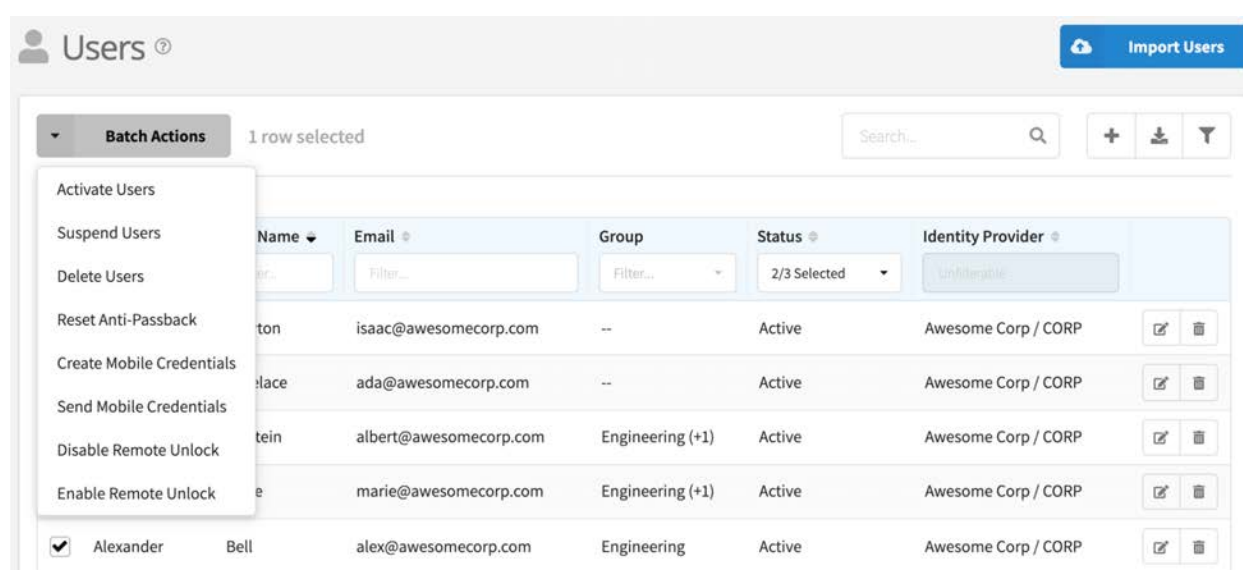
The custom dashboard that you created will appear in the Dashboard dropdown. Your dashboard will be viewable and editable to all other Super Admin users in your org.

USERS

The **Users** tab lets you manage and import users, as well as create and define groups and roles for users.

USER MANAGEMENT

The User Management screen is where you can view and manage users. You can export user data to CSV by clicking the **Export to CSV** icon. Filters can be used on any of the columns to narrow down the users shown in the view. Click the Filter Columns icon to show or hide columns.



The Identity Provider column will list the master user database from where the users were created (within the portal, from Active Directory, G Suite, etc.). You can toggle this column to show the **namespace**. For more information, see [USER DATA MODEL](#).

CREATE USER

Note: For security and auditing purposes, we recommend that you create one user per person, rather than one user per household or unit.

- To create a new user, click the **Add User** button (+) on the top right corner. Enter the user's name, email address, and start/end date.
 - If the user belongs to another Organization, check the box **Add a user from an existing namespace** and enter the **Namespace**
- The **External ID** field can be used for employee IDs or other useful information.

- If desired, click **Change Photo** to upload a User photo, or take a new photo using your device's built-in camera or webcam. This photo will appear on the Control Center and in the user's Openpath mobile app.
- If the user is an admin and requires access to the web portal, click the **Portal Access** slider and then add the **Super Admin** role.

Note: Only give portal access to users who require it, like an office manager or security guard. If you want to give someone limited access to the Control Center, create a role with [GRANULAR PERMISSIONS](#).

Create User

User

Credentials

Access

Email *

alex@example.com

☐ Add a user from an existing namespace ?

First Name

Alexander

Middle Name

Last Name

Bell

Start Date

Nov 01, 2020

Start Time

12:00 am

End Date

Select Date

End Time

Select Time

Time Zone *

(GMT-08:00) Pacific Time

External ID

☒ Portal Access

Roles - At least one role must be added in order to allow portal access *

Super Admin Read-Only ✕

Cancel

Save

IMPORT USERS

In addition to creating individual users, you can also import and update users with a CSV file. You can also import users by using a directory service integration. See [INTEGRATIONS](#).

To add and update users with a CSV file:

- Go to Users > Import Users (or from the User Management page, click the **Import Users** button).
- Click **Download Sample CSV** and fill out all required fields in the format shown.
 - **Note:** If you are updating users, you can click the **Export Data** icon on the User Management page to download a CSV of all users, then modify that file to import.
- On the Import Users page, click **Show Fields** to view examples of acceptable values.
- Save the file as a CSV file (Excel file extensions will not work). Example: openpath-bulk-import-users.csv
- On the Import Users page, click **Select CSV File** and locate the file.
- Select the **Namespace**:
 - Select **Local** if you're adding new users or updating existing ones and you don't use an IDP.
 - **Note:** If using the Local namespace, choose whether you want to skip existing users or update them using the How To Handle Existing Users dropdown.
 - Select **Google G Suite, Microsoft Azure AD, or Okta** if you want to update existing users you previously synced with Openpath (new users will not be added).
- Click **Upload File**.
- The **Upload Status** field will log all users added, updated, and skipped. This step may take a few minutes. When finished, you'll see an "IMPORT COMPLETE" message along with any errors that may have occurred.

ISSUE CREDENTIALS

Once you have created users, you can issue credentials. Credentials are what let users have access to entries.

Note: When adding card credentials, be aware of whether you have high frequency (HF) readers, which require MIFARE/DESFire cards, or low frequency (LF) readers, that use Wiegand cards.

- To issue credentials, click on a user to go to their User Details, then click on the **Credentials** tab in the upper righthand corner.
- Select the type of credential you want to issue. Choose from:
 - Mobile
 - Cloud Key (used for providing Guest Access Links)

- Card: Openpath/MIFARE (CSN) — Fast (select this for Openpath HF key fobs and cards)
- Card: Openpath DESFire (Encrypted) — Secure (select this for Openpath HF cards)
- Card: Wiegand ID (select this for Openpath LF key fobs and cards)
- Enter the required information then click **Create**.

ADD A MOBILE CREDENTIAL

After you add a mobile credential, click **Send** to email the user instructions on how to set up their mobile device as a credential. The **Activation Pending** column indicates that an email has been sent, but the user has not yet activated their mobile credential.

ADD A WIEGAND CREDENTIAL

If you're adding a Wiegand credential, you need to specify the card format. For Openpath LF cards, select **Prox 26-bit (H10301)**.

If you're unsure of the card format, you can use the Raw 64-bit option and enter the card number. If you're unsure of the card number, you can swipe the card at the reader and take note of the rejected access entry under Reports > Activity Logs. The card number will be displayed under the Credential Detail column.

If you'd like to send card credential data to a third-party control panel, set **Use for Gateway** to **Enabled**. You must also configure the Wiegand reader to enable this feature. See [WIEGAND DEVICE](#).

USER ACCESS

The **Access** tab on the User Details page is where you can assign groups, sites, and zones, as well as enable Remote Unlock for a user.

- Use the **Groups** field to add a user to a group and give them access to zones available for that group. See [CREATE GROUPS](#).
- Alternatively, you can manually assign access to sites and zones by using the toggle buttons.
- Enable **Override Permission** to give the user permission to unlock entries in the Lockdown (Override Only) state.
- Enable **Remote Unlock** to let the user unlock a door remotely (i.e. physically outside of Bluetooth range of the door reader) using the mobile app.
- The **Group Schedules** column will display any applicable Group Schedules if you assigned a group with a schedule.

- The **User Schedule** column lets you assign user-specific schedules. See [USER SCHEDULES](#).

User Access

Alexander Bell

User

Credentials

Access

Security

Groups

HQ Employees

Access

Site	Overall Access	Group Access	User Access	Zones
Awesome Corp - Los Angeles	✗	✗	<input type="checkbox"/>	7
Awesome Corp - New York	—	✗	<input type="checkbox"/>	2

Zone	Overall Access	Group Access	User Access	User Schedule	View All Schedules
Back Door [1 Entry]	✓	✗	<input checked="" type="checkbox"/>	Refer to Entry Behavior	
Lobby Door [1 Entry]	✗	✗	<input type="checkbox"/>	--	

Override Permission

Disabled

Remote Unlock

Enabled

Cancel

Save

USER SECURITY

The Security tab is where you can manage Multi-Factor Authentication (MFA) credentials. You cannot add MFA credentials for other users — only view and delete. You can add a MFA credential for yourself under [MY PROFILE](#).

MANAGING USERS

From the User Management screen, use the checkboxes and **Batch Actions** to change the status of individual or multiple users:

- **Activate Users:** reactivates a suspended user
- **Suspend Users:** disables credential usage and admin portal access (if granted to the user)

- **Delete Users:** revokes access from the user but still keeps the user in the system for reporting and record keeping purposes
- **Reset Anti-Passback:** if using Anti-Passback, resets a user's Anti-Passback state. See [ANTI-PASSBACK](#).
- **Create Mobile Credentials:** automatically creates mobile credentials for the selected users
- **Send Mobile Credentials:** send mobile setup emails to the selected users. If a user has multiple mobile credentials, they'll receive multiple setup emails.
- **Disable Remote Unlock:** disables remote unlock permissions for the selected users
- **Enable Remote Unlock:** enables remote unlock permissions for the selected users

GUEST ACCESS LINKS AND WEBHOOK URLS

Users with Cloud Keys can share temporary Guest Access Links and generate webhook URLs. Webhook URLs can be used to unlock entries via a web browser or integrated into software or external services.

- To generate links, click on a user to go to their User Details, then click on the Credentials tab in the upper righthand corner. Next to the Cloud Key credential, click **Get Webhook URL**.
- A window will pop up where you can select which entries the URL will unlock:
 - Choose the entries
 - Edit the labels (optional)
 - Provide a description
 - Enter a Start and End Time (optional)
 - Click **Generate Links**
- Use the Guest Access Link for sharing access with a person; use the API Link for your own software or other external service.

Entries

Total Count: 2

Rear Entry × Side Entry ×

Label for Rear Entry

Rear Entry

Label for Side Entry

Side Entry

Description

Access to rear and side doors

Start Date - Optional

Start Time - Optional

End Date - Optional

End Time - Optional

Select Date

Select Time

Jun 25, 2019

5:11 pm

Time Zone

(GMT-08:00) Pacific Time

https://api.openpath.com/s/2hwckuou6t34f

Guest Access Link: Copy to clipboard


https://api.openpath.com/tokens/cloudKeyUnlockTokens/eyJhbGciOiJIUzI1NiIsI





API Link: Copy to clipboard

Note: A Cloud Key can have multiple webhooks for multiple entries associated with it. Deleting a Cloud Key credential will also remove all the valid webhooks associated with it.








GROUP MANAGEMENT





The Group Management page is where you can create and manage groups for users. Groups let you assign access and entry permissions for one or more users, and they're useful for organizing your user base by department or role. You can export group data to CSV by clicking the **Export Data** icon.

 Groups

Search...    

1-2 of 2


Group Name 	Description 	User Count 	
Filter...	Filter...	Unfilterable	
Engineering	--	2	 
HQ Employees	--	1	 



1



Show 100 rows

CREATE GROUPS

- To create a new group, click the **Add Group** button (+) on the top right corner. Enter a name, description, and assign users.
- Next, select which sites and/or zones this group will have access to.
- When you have finished, click the **Save** button to save your new group.

 Create Group



Name *

Engineering

Description


Engineering team members

Users

Albert Einstein  Alexander G. Bell 

Access ?

Site	Site Access ?	Zones
▶ Old Headquarters	<input checked="" type="checkbox"/>	4
▼ Test Lab	<input type="checkbox"/>	2

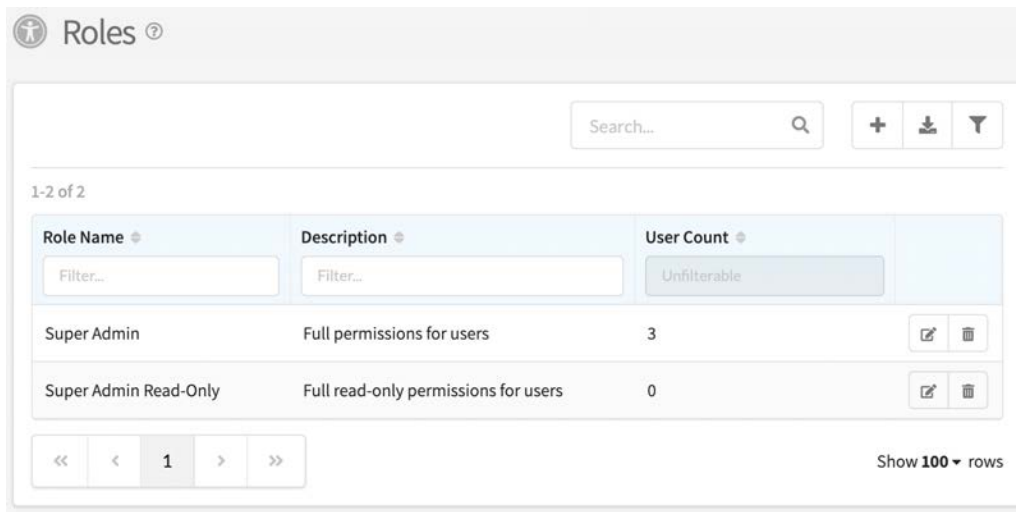
Zone	Zone Access	Group Schedule
Lab Door	<input checked="" type="checkbox"/>	Refer to Entry Behavior 
Storage Closet	<input type="checkbox"/>	--

ROLE MANAGEMENT

A role is a set of portal access permissions that can be assigned to users. There are two default roles that cannot be edited:

- **Super Admin** — gives full portal access with edit permissions
- **Super Admin Read-Only** — gives full portal access with read permissions

Note: Users with the Super Admin role can assign and revoke portal access for other users.



The screenshot shows a web interface titled "Roles" with a search bar and action buttons (+, download, filter). Below the search bar, it indicates "1-2 of 2" roles. The table has three columns: Role Name, Description, and User Count. The first row is "Super Admin" with the description "Full permissions for users" and a user count of 3. The second row is "Super Admin Read-Only" with the description "Full read-only permissions for users" and a user count of 0. At the bottom, there are pagination controls showing page 1 of 2 and a "Show 100 rows" option.

Role Name	Description	User Count
Super Admin	Full permissions for users	3
Super Admin Read-Only	Full read-only permissions for users	0

CREATE ROLES

- To create a new role, click the **Add Role** button (+) on the top right corner. Enter a name, description, and assign users.
- Select the permissions you'd like this role to have, then click the **Save** button in the lower right corner.

Note: You can assign multiple roles to the same user. The user's permissions will be cumulative across all assigned roles.

GRANULAR PERMISSIONS

Granular Permissions gives additional specificity when creating Roles. For example, you create a role that limits access to just the Entry Dashboard (see example below). Or, create a role with full portal access but only for one site.

Note: Hardware Dashboard is tied to the “Hardware” permission, not the Dashboard permissions.

Note: You cannot limit access to a specific site’s users—if you create a role that has access to users, that role will have access to all users within that org.

Create Role

Name *

Dashboard Read-Only

Description

Read-only access to the Activity and Entry Dashboard

☒
Limit to specific sites ?

Sites *

Awesome Corp - Los Angeles ✕

Users

Liz McFarland ✕
Keaton Humphreys ✕


Dashboard ?





Permission	Read	Write	Description
Dashboards	<input checked="" type="checkbox"/>	<input type="checkbox"/>	View and edit dashboard
• Activity Dashboard	<input checked="" type="checkbox"/>	<input type="checkbox"/>	View and edit activity dashboard
• Entry Dashboard	<input checked="" type="checkbox"/>	<input type="checkbox"/>	View and edit entry dashboard

USER SCHEDULES







The User Schedules page is where you can define schedules for users and groups. User and Group Schedules are useful if you want to restrict access or trigger methods for certain users/groups. For example, you can define normal business hours for employees or require that certain users only use key cards.





You can export schedule data to CSV by clicking the **Export Data** icon.

 User Schedules

Search...    

1-2 of 2 (6 total)

Schedule Name 	Last Updated 	
Filter...	Unfilterable	
Normal Business Hours	Oct. 21, 2019 4:43:47 pm	 
Executive First-In 24x7 Access	Apr. 9, 2020 1:55:35 pm	 



1



Show 100 rows

CREATE USER SCHEDULE

- To create a User/Group schedule, click the **Add User Schedule** button (+) on the top right corner. Enter a name, then click **Save**.
- Next, click on the **Scheduled Events** tab to define the schedule. Click the **Add Event** button.
- Choose between a **Repeating Event** and a **One-Time Event**. In this example, we're creating a normal business hours schedule, so we'll define a Repeating Event.
- Enter a Start and End Time, choose a Time Zone, and select which days this event will occur.
- Enter a Start Date and End Date (optional), and set the Scheduled State.

Note: A User/Group schedule cannot be more permissive than what the entry allows. In this example, we've defined the Scheduled State as "Standard Security" which only works if the entry state is also set to Standard Security or Convenience (but not say, Strict Security).

- The fields you create will appear at the bottom of User Details and can be viewed in the User Management table by clicking **Filter Columns** and clicking the checkbox next to the field

Custom Fields

Employee ID

12345

Forklift Exp Date

Sep 01, 2021

☒ Gym Access

Membership Level

Pro

SITES

Sites are physical locations (like office buildings) comprised of zones and entries. You should create a site for every location where you have Openpath installed.

SITE MANAGEMENT

The Site Management page is where you can view and manage sites. You can export site data to CSV by clicking the **Export Data** icon.

Sites ?

Search...

+

↓

⌵

1-2 of 2

Site Name	Zone Count	
Awesome Corp - Los Angeles	7	
Awesome Corp - New York	2	

<<

<

1

>

>>

Show 100 rows

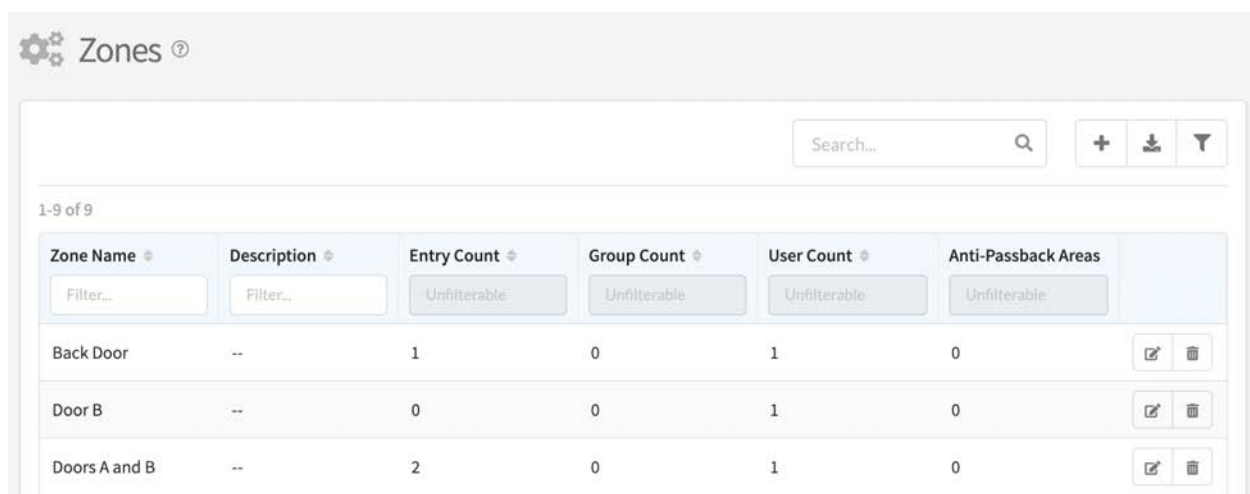
CREATE SITES







- To create a new site, click the **Add Site** button.
- Enter a **Site Name**, address, and phone number, then click the **Save** button.

ZONE MANAGEMENT

The Zone Management page is where you can view and manage zones. Zones are groups of one or more entries that you can assign to sites. Zones are useful for breaking up large sites into smaller areas like floors or common areas (in multi-tenant scenarios). Most significantly, zones are the units of physical access permissions that you assign to users.

You can export zone data to CSV by clicking the **Export Data** icon. Click the **Filter Columns** icon to show or hide columns.



Zone Name	Description	Entry Count	Group Count	User Count	Anti-Passback Areas	
Filter...	Filter...	Unfilterable	Unfilterable	Unfilterable	Unfilterable	
Back Door	--	1	0	1	0	 
Door B	--	0	0	1	0	 
Doors A and B	--	2	0	1	0	 

ZONE SHARING

Zones can be shared between multiple Openpath customers. This is useful if you're a landlord who wants to share a zone of common entries with multiple tenants. Recipients cannot edit shared zones.

CREATE ZONE

- To create a zone, click the **Add Zone** button (+) in the top right corner.
- Enter a name and description (optional) and select the site to which the zone will be assigned.
 - **Note:** A zone can only be assigned to one site, but a site can have multiple zones assigned to it.

- Next, add User Groups and Users to the zone (optional).
- If you want to share this zone to a different Organization, enter the Org ID(s) (optional).
- Click the **Save** button to save your new zone.

ANTI-PASSBACK AND OCCUPANCY MANAGEMENT

Anti-Passback lets you define a sequence in which entries must be accessed in order to gain entry. Sequences are defined using **Areas** — each Area contains a set of inbound and outbound entries. For each Area, after every successful inbound entry the user must exit through an outbound entry before entering an inbound entry again. This feature is commonly used with parking gates and helps prevent users from sharing credentials with other users. You can also use Anti-Passback to limit occupancy and prevent users from accessing inbound entries until enough users exit through outbound entries.

- To set up Anti-Passback on a zone, click on the zone to edit it, then click on the Anti-Passback tab in the upper righthand corner
- Enter an **Expiration** time in seconds after which the Anti-Passback state will reset for the user.
- Enable **Reset Anti-Passback Periodically** to configure a schedule during which a user is not limited to Anti-Passback logic until after their second unlock attempt
- Enable **Use Contact Sensor** to only change a user's Anti-Passback state until after the Contact Sensor reports open
- Enable **Shared-To Orgs Can Reset Anti-Passback** if you want orgs sharing this zone to have permission to reset Anti-Passback for their users.
- Lastly, define the Area(s) within the zone to be enforced by Anti-Passback
 - Enter a name
 - Set the **Inbound Mode** and **Outbound Mode**, which determines how the system reacts to Anti-Passback breaches:
 - **None** — access is granted; no additional response
 - **Alert** — access is granted and an event is generated
 - **Enforce** — access is denied and an event is generated
 - Add Inbound and Outbound Entries
 - **Note:** An entry can only be used once within an Area, either as Inbound or Outbound but not both; however an entry *can* be used in multiple Areas. In addition, all entries within an Area must reside on the same ACU, and all entries belonging to the parent zone must reside on the same ACU.
 - If limiting occupancy, select either **Alert** or **Enforce** (definitions above) from the Occupancy Limiting Mode dropdown, then enter the Occupancy Limit

- Click **Add Area**
- Click **Save**

Internally, the ACU tracks each user's most recent direction of movement (inbound or outbound) within each Area. When the user's most recent direction is known, then an attempt by that user to move in the same direction again will result in an Anti-Passback Breach event. When the user's most recent direction is unknown, as in the case of a newly created Area, or following a scheduled or manual Reset action, then the user's next movement will be allowed in either direction, after which normal rules will apply again.

Anti-Passback Breach events can trigger alerts. See [ALERT SETTINGS](#). They can also be used to trigger custom integrations. See [RULES ENGINE](#).

Note: Anti-Passback logic also applies to Cloud Key credentials and other remote unlock methods. In general, you might not want to allow remote unlock methods on zones with Anti-Passback enabled.

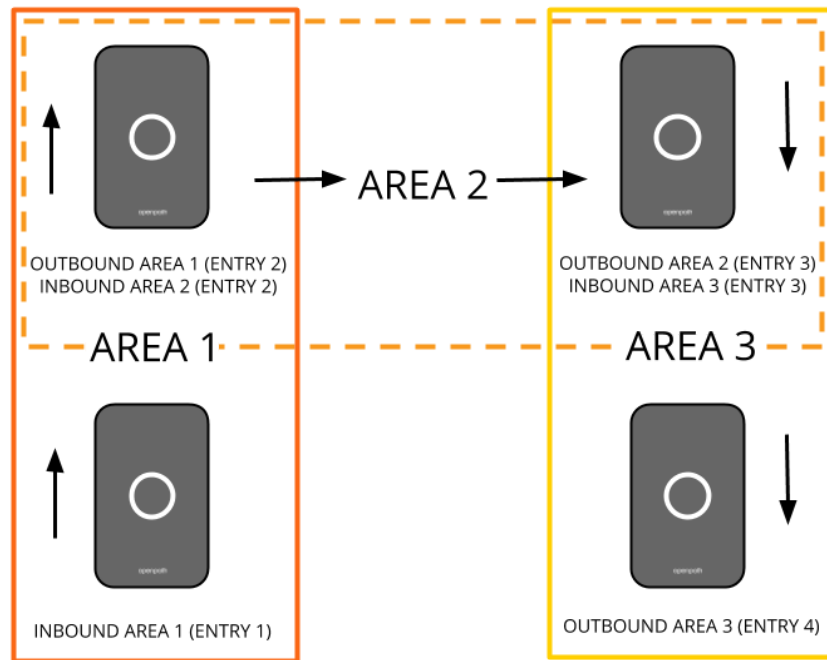
RESET ANTI-PASSBACK

You can reset Anti-Passback in two ways: on the Zone level and on the User level.

- To reset Anti-Passback on the Zone level, go to Zone Management and click **Reset Anti-Passback** under the Anti-Passback column.
- To reset Anti-Passback on a User (or multiple Users), see [MANAGING USERS](#).

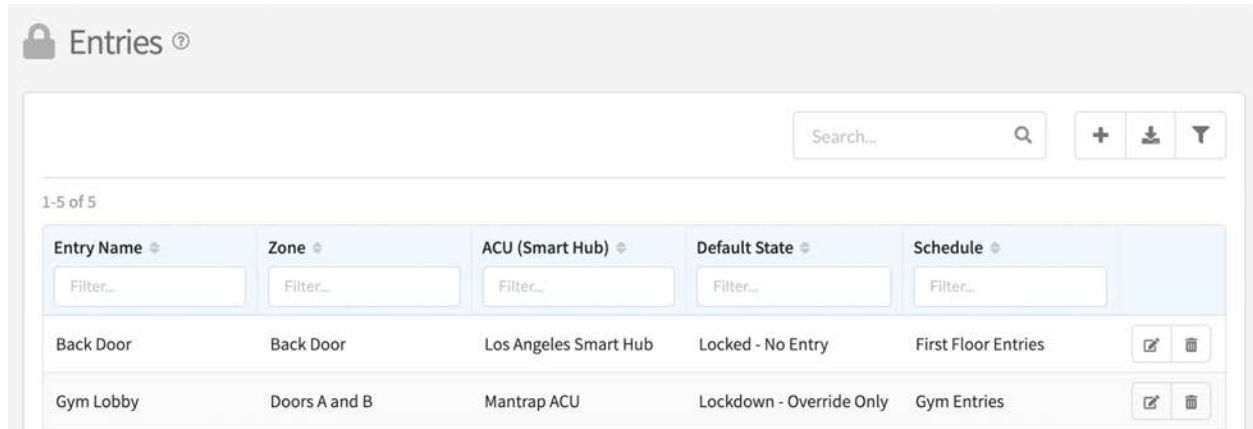
MULTIPLE AREA ANTI-PASSBACK

Most Anti-Passback scenarios will only require a single Area, but multiple Areas can be used to create multi-step sequences of entry access. In this example, all four Readers reside on the same ACU and are configured across three Areas, resulting in a complex flow of movement.



ENTRY MANAGEMENT

Entry Management is where you can add and manage entries. Generally speaking, entries are doors, but can also be gates, turnstiles, and elevator floors. An entry is often secured with an Openpath reader or wireless lock. You can export entry data to CSV by clicking the **Export Data** icon. Click the **Filter Columns** icon to show or hide columns.



Note: It is likely that your Openpath installer may provision some or all of the following features for you during the installation process.

CREATE ENTRY

- Enter a name and select the zone
- From the Cloud Gateway Device Type dropdown, select whether this entry is configured with Openpath hardware (Reader and ACU) or with Allegion hardware (Gateway and Lock)
- If using Openpath hardware, select the Controller (ACU). If using Allegion hardware, select the Allegion Wireless Lock

Basic Info

Name *

Front Door

Zone *

Exterior Doors

Cloud Gateway Device Type *

Openpath

Controller *

Office Smart Hub

ENTRY SETTINGS

ENTRY BEHAVIOR

Entry Behavior

Default State *

Convenience

Allows all valid credentials and trigger methods

Schedule ?

First Floor Entries

Manage Schedules

Entry Behavior is where you set the Default State for the entry. See [ENTRY STATE MANAGEMENT](#). You can also assign an Entry Schedule, which is optional. See [ENTRY SCHEDULES](#).

Note: Entries configured with Allegion Wireless Locks only support Unlocked, No Entry, and Convenience states.

ALLEGION WIRELESS LOCK

Allegion Wireless Lock

☒ Ajar Detection ?

Ajar Duration (15 Min Max) * Unit *

☒ Forced Open Detection ?

Entry Open Duration * Unit *

Card Reader Sensitivity *

Entries configured with Allegion Wireless Locks have this additional section.

- **Ajar Detection** and **Forced Open Detection** are always enabled for wireless locks
- **Card Reader Sensitivity** is set to Normal by default, but you can select High or Max for more reliable reading of key fobs

CONTACT SENSOR

Contact Sensor ?

Port ? *

☒ Ajar Feature ?

Ajar Duration (15 Min Max) * Unit *

☒ Forced-Open Detection ?

A contact sensor detects if an entry is open.

- **Port** — select the port for the contact sensor to which the entry is wired

- **Ajar Feature** — if enabled, you can specify the maximum allowed time the door can be ajar before an event is generated indicating the door is ajar. If disabled, there will be no system action if the door is ajar.
- **Duration** — the maximum allowed time the door can be ajar before events are generated
- **Unit** — select whether to use seconds or minutes
- **Forced-Open Detection** — if enabled, an entry opening without first unlocking through Openpath or triggering the REX will generate an event

Contact sensor events can trigger alerts. See [ALERT SETTINGS](#). They can also be used to trigger custom integrations. See [RULES ENGINE](#).

ENTRY/EXIT HARDWARE

Entry/Exit Hardware is where you can select a relay to use on the ACU (or expansion board), like for controlling electric strikes or maglocks.

- **Port** — select which port to assign the reader, from Relay 1-4. Technically, the electric strike is wired to one of the 4 ACU ports, and the reader is wired to the strike. You will need to select the ACU relay for which this reader/entry is wired to the ACU.
- **Entry Open Duration** — enter a time (between 1 second and 10 minutes) for how long the entry remains unlocked before reverting back to its default state.
- **Unit** — select whether to use seconds or minutes
- **Invert Output** — this advanced setting is typically only needed for elevator relays; if enabled, it flips the NC/NO configuration of the physical relay

OPENPATH READER

Associate the entry with the Openpath Reader.

- **Port** — select the port on the ACU to which the Openpath Reader is connected.
- **Card Reading** — enable this to allow RFID/NFC cards at this reader.
- **Wave to Unlock** — enable this to allow Wave to Unlock and Touch Entry.
 - **Mobile Authorization Range** — This range specifies how close the mobile device must be to the reader in order to register a Wave to Unlock. Set the range using the slider.
 - **Wave Detection Range** — This range specifies how close the hand must be to the Openpath reader to initiate the unlock attempt—this behavior may vary depending on your environment and this setting might require adjustment
- **Auto Proximity Unlock (Elevators Only)** — enable this to unlock the entry when a user with a valid mobile credential is in range of the reader. Set the range using the slider.
- **Advanced Options** — toggle this to configure advanced range options for the Openpath Reader:
 - **Mobile Reader Range** — the distance that the reader can detect a mobile phone that is in BLE range
 - **Mobile Beacon Range** — the distance that the beacon can detect a mobile phone and “wakes up” the Openpath app

REQUEST TO EXIT



Often, doors will have a Request to Exit button or sensor that will unlock the door from the inside.

- **Port** — select the port for the Request to Exit device to which the entry is wired
- **Mode** — this is an electrical term regarding how the Request to Exit device sends the command to the ACU. Your installer will be able to give you guidance on whether the Mode should be set to Normally Closed or Normally Open for a particular entry configuration.
- **Trigger Relay to Unlock Entry** — if enabled, a triggered REX will open the associated Relay(s) and prevent forced-open alarms

WIEGAND DEVICE



Openpath is compatible with legacy Wiegand Devices.

- **Port** — select the port for the Wiegand Device to which this entry is wired
- **Mode** — select the Mode to set which direction the card credential data is sent:
 - Use **Input** to receive data from devices such as a Wiegand reader

- Use **Output (Gateway)** to send credential data to a third-party control panel. See [CONFIGURING OPENPATH WITH LEGACY SYSTEMS](#) for more information.

ADD CONTROL

- If an entry has more than one of any controls (Openpath Readers, Entry/Exit Hardware, Contact Sensor, Request to Exit, or Wiegand Device) installed, you can select which additional control(s) you would like to associate with the entry
- Once you add an additional control, it will appear in the relevant section on this page

ENTRY STATE MANAGEMENT

An Entry State defines whether an entry is unlocked and what access methods may be used to unlock it. Openpath provides the following default Entry States:

- **Unlocked** — no credential is required for access
- **No Entry** — no entry allowed, even with an otherwise valid credential
- **Lockdown - Override Only** — no entry allowed, even with an otherwise valid credential, except for override unlock requests
- **Convenience** — allows all valid credentials and trigger methods
- **Onsite Only** — allows all valid onsite credentials and trigger methods
- **Standard** — allows most mobile access and cards, and excludes remote mobile IFA and third-party Wiegand methods
- **Strict** — allows only interactive 2FA onsite mobile access and encrypted smart cards. Excludes all remote, IFA, and non-encrypted methods.

The **Trigger Methods** column refers to the number of ways that an entry can be unlocked in that particular state.

Entry States ?

Search...

+

↓

⌵

1-7 of 7

Entry State Name ⌵	Description ⌵	Relay State ⌵	# Trigger Methods ⌵	
Filter...	Filter...	Filter...	Unfilterable	
Unlocked	No credential required for access	Unlocked	N/A	
No Entry	No entry allowed, even with an otherwise valid credential	Locked	0	
Lockdown - Override Only	No entry allowed, even with an otherwise valid credential (overrides allowed)	Locked	11	
Convenience	Allows all valid credentials and trigger methods	Locked	32	
Onsite Only	Allows all valid onsite (non-remote) credentials and trigger methods	Locked	27	
Standard Security	Allows most mobile access and cards supported by Openpath readers, and excludes remote mobile 1FA and third-party Wiegand methods	Locked	12	
Strict Security	Allows only interactive 2FA onsite mobile access and encrypted smartcards, and excludes all remote, 1FA, and non-encrypted methods	Locked	4	

<<

<

1

>

>>

Show 100 rows

Click on an Entry State in order to view the trigger methods included in that that State.

ADD ENTRY STATE

1. To create a new Entry State, click the **Add Entry State** button (+) in the top right corner

Add Entry State

Basic Info

Name *

Description *

Trigger Methods

☐ Mobile 1FA over BLE

☐ Mobile 2FA over BLE

☐ Mobile 1FA remote over WiFi

2. Use the sliders to enable the trigger methods you want to be valid with this Entry State. Definitions for the various methods are provided below.
3. Click the **Save** button when finished

TRIGGER METHOD DEFINITIONS

- **Mobile 1FA:** An unlock request that is triggered either from a mobile device that has no homescreen PIN-code, biometric, or other similar protection, or from a device whose homescreen is currently not unlocked.
- **Mobile 2FA:** An unlock request that is triggered from a device with PIN-code, biometric, or other similar protection on the homescreen, and whose homescreen is currently unlocked. Therefore in order to trigger a Mobile 2FA unlock, a person must both be in possession of the mobile device, as well as know or possess the PIN-code or biometric needed to unlock the device.
- **Wave:** An unlock request that is triggered by passing a hand in close proximity to, a Wave-enabled Openpath Smart Reader, and which is authenticated by the mobile credential provisioned into Wave-enabled Openpath Mobile Access app.
- **Auto:** An unlock request that is triggered by being in close proximity to an Auto-enabled Openpath Smart Reader, and which is authenticated by the mobile credential provisioned into Auto-enabled Openpath Mobile Access app. This mode is often used for elevator scenarios.
- **Remote:** An unlock request that is triggered while the user is not near the entry.

- **Onsite:** Opposite of Remote; an unlock request that is triggered while the user is near the entry.
- **Near Reader:** An unlock request that is considered Onsite because the mobile device is within Bluetooth range of the entry's Openpath Reader.
- **Over BLE:** A mobile unlock request that is sent over BLE (Bluetooth Low Energy) through the Openpath Reader. Such a request is always Onsite.
- **Over WiFi:** A mobile unlock request that is sent over the mobile device's WiFi connection over the local network directly to the Openpath Access Control Unit. Such a request may be considered Onsite or Remote depending on whether the mobile device is in range of the entry's Reader.
- **Over Cloud:** A mobile unlock request that is sent over the mobile device's WiFi or cell/LTE connection, and routed via the Openpath cloud back to the Access Control Unit. Such a request, if permitted, enables Remote unlock from anywhere in the world where the mobile device has an internet connection, but also may be considered Onsite if the mobile device is in range of the entry's Reader.
- **Geofence:** A mobile unlock request that uses a device's location services to support an onsite unlock.
- **Over NFC:** A mobile unlock request triggered by holding a mobile device close to the Openpath Reader. This entry state only works with Android devices that support NFC.
- **Override:** An unlock request that is typically used with Lockdown plans.

ENTRY SCHEDULES

Entry Schedules allow for entries to be in a specific state (e.g. locked, unlocked, etc) based on date and time. For example, an entry can be set to an unlocked state during normal business hours, Monday – Friday but remain locked (its Default Entry State) when the Schedule is inactive.

1. Click **Add Entry Schedule**, enter a name, then click **Next**

Edit Entry Schedule

Schedule Info

Name *

First Floor Entries

Entries *

Lobby Door ✕

Back Door ✕

✕

Cancel

Save

Events

+

	Rank	Event	Scheduled State	State To Trigger	
≡	#1	One-Time Starts Jan. 1, 2021 at 12:00 am PST Ends Jan. 1, 2021 at 11:59 pm PST	Onsite Only	--	
≡	#2	M, Tu, W, Th, F 9:00 am - 5:00 pm PST Starts Dec. 24, 2020 Ends Never	Convenience	--	

2. Assign this Entry Schedule to entries by either typing in the names of the entries or using the dropdown
3. Click **Add Event** to create a new schedule
 - a. Choose between a **Repeating Event** and a **One-Time Event**
 - b. Enter a Start and End Time, choose a Time Zone, and select which days this event will occur (if a Repeating Event)
 - c. Enter a Start Date and End Date (optional)
 - d. Set the Scheduled State and if desired, enable and set **Trigger after an unlock method**
 - e. Click **Save**

The screenshot shows a 'Scheduler' window with a close button (X) in the top right corner. Below the title bar, there are two tabs: 'Repeating Event' (active, highlighted in red) and 'One-Time Event'. The form contains the following fields:

- Start Time:** A text input field with '9:00 am' and a clock icon.
- End Time:** A text input field with '5:00 pm' and a clock icon.
- Time Zone:** A text input field with '(GMT-08:00) Pacific Time' and a globe icon.
- Repeating:** A row of checkboxes for days of the week: Sun, Mon, Tue, Wed, Thu, Fri, Sat. Tue, Wed, Thu, and Fri are checked.
- Start Date:** A text input field with 'Oct 26, 2018' and a calendar icon.
- Repeats Until:** A text input field with 'Repeats Forever' and a calendar icon.
- Default State:** A text input field with 'Convenience'.
- Scheduled State:** A dropdown menu with 'Unlocked' selected.
- Trigger after an unlock method included in:** A checkbox (unchecked) followed by a dropdown menu with 'Convenience' selected.

At the bottom of the window, there are two buttons: 'Cancel' and 'Save'.

LOCKDOWN PLAN MANAGEMENT

This is where you can view and manage Lockdown Plans. You can export Lockdown Plan data to CSV by clicking the **Export Data** icon.

CREATE LOCKDOWN PLAN

1. Click **Add Lockdown Plan**
2. Give the plan a useful name and assign a **rank**. The rank is important because it determines which plans take priority in the case of triggering multiple plans that share entries. The lower the number, the higher the rank.
3. Optionally, you can enter a time after which the plan will auto-revert using Auto-Revert Plan. If you do not want the Lockdown Plan to revert automatically, leave this value blank.
4. Optionally, you can enable the **Use standard (free-eligible) zone configuration** slider to create a Lockdown Plan that includes all zones with triggered states of Lockdown – Override Only.
5. Click **Add Zone** to select which entries this Lockdown Plan will affect
 - a. **Note:** You cannot add zones that have been shared with you to a Lockdown Plan
6. Select the desired Entry State for the zone. For lockdown scenarios, we recommend using **Lockdown – Override Only**. This means only users with Override permissions are able to unlock entries in this state.

Lockdown Plans

Lockdown Lockdown User Config

Name *

Rank ? * **Duration** **Unit**

☐ Use standard zone configuration ?

+ Add Zone

Zone	Triggered State	
<input type="text" value="Back Door"/>	<input type="text" value="Lockdown - Override Only"/>	

7. Click **Save**
8. Go to the User Config tab to select Users and Groups that can trigger and revert the Lockdown Plan

Lockdown Plans

Lockdown Lockdown User Config

Note: To trigger a lockdown via the Openpath Control Center, User must also have a valid Cloud Key credential.

Users that can Trigger Lockdown Plan *

Groups that can Trigger Lockdown Plan *

Users that can Revert Lockdown Plan *

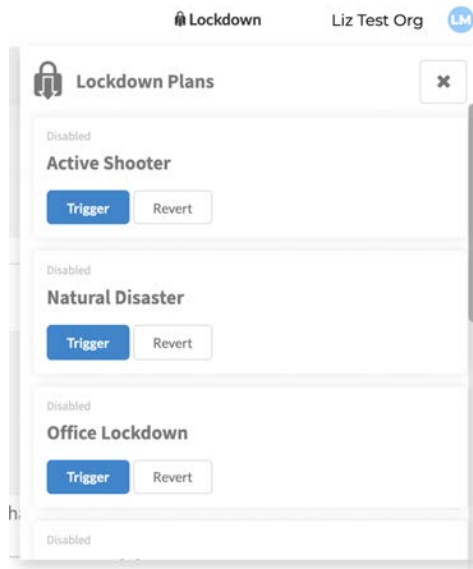
Groups that can Revert Lockdown Plan *

9. Click **Save**

TRIGGER A LOCKDOWN PLAN

Note: You must have a Cloud Key Credential to trigger and revert Lockdown Plans from the Control Center

1. Click on **Lockdown** from the top right corner
2. Click **Trigger** or **Revert** on the desired Lockdown Plan



HARDWARE

Hardware is divided in two categories: ACUs and Readers.

ACU MANAGEMENT

The ACU Management screen is where you can view and manage ACUs and SDCs. You can export ACU data to CSV by clicking the **Export Data** icon. Click the **Filter Columns** icon to show or hide columns.

ACUs ⓘ

Search... 🔍 + ⬇️ ⚙️

1-7 of 7

ACU Name ⓘ	ACU Serial ⓘ	Entry Count ⓘ	Status ⓘ	Status Detail ⓘ	Status Changed ⓘ	
Filter...	Unfilterable	Unfilterable	Filter... ▾	Filter...	Unfilterable	
ACU 01 (Test Site)	--	1	Unregistered ⚡	--	--	✎️ 🗑️
Garage ACU	--	0	Unregistered ⚡	--	--	✎️ 🗑️
Los Angeles Smart Hub	--	2	Unregistered ⚡	--	--	✎️ 🗑️

CREATE ACU

1. To add a new ACU or SDC, click the **Add ACU** button (+)
2. Enter a name for the ACU
3. From the Controller Type dropdown, select the appropriate type:
 - a. **4 Door Controller (OP-AS-01)** — for first gen Smart Hubs
 - b. **Single Door Controller (SDC)**
 - c. **Core Series ACU** — for Core Series Smart Hubs
4. If your ACU also connects to an expansion board (this is most common with Core Series Smart Hubs), then from the **Add Expansion Board** dropdown, select and add the appropriate type(s):
 - a. **Openpath 4-Port Expansion**
 - b. **Openpath 8-Port Expansion**
 - c. **Openpath 16-Port Elevator**
5. A description will appear in green. Click **Save**.

Create ACU

Controller Name *
2nd Floor Smart Hub

Controller Type *
Core Series ACU

Expansion Boards

Add Expansion Board *
Openpath 4-Port Expansion + Add Board

Expansion Board Number	Expansion Board Name	Action
1	Openpath 4-Port Expansion	To Be Added

Cancel Save

Once you add an ACU to the system, you need to register it (also known as provisioning). For Smart Hubs, please refer to the [Openpath Installation Guide](#). For Single Door Controllers, refer to the [Openpath SDC Installation Guide](#).

ADD EXPANSION BOARD

You need to edit ACUs when you install additional expansion boards in existing Smart Hubs.

1. To edit an ACU, click on the ACU from the ACU Management page
2. From the **Add Expansion Board** dropdown, select and add the expansion board
3. Click **Save**

EDIT ACU PORTS

From the Edit ACU page, click on the **Ports** tab to view and manage ACU ports:

- In the Options column, click on the Ports icon open Port Options
- Click on the **Input Type** dropdown to change a Contact Sensor, Request to Exit input or AUX I/O to a different input type, Wiegand Device, or to a Generic input. This is useful for creating rules. See [RULES ENGINE](#).
- You can only change the Input Type on a port that has not yet been assigned to an entry

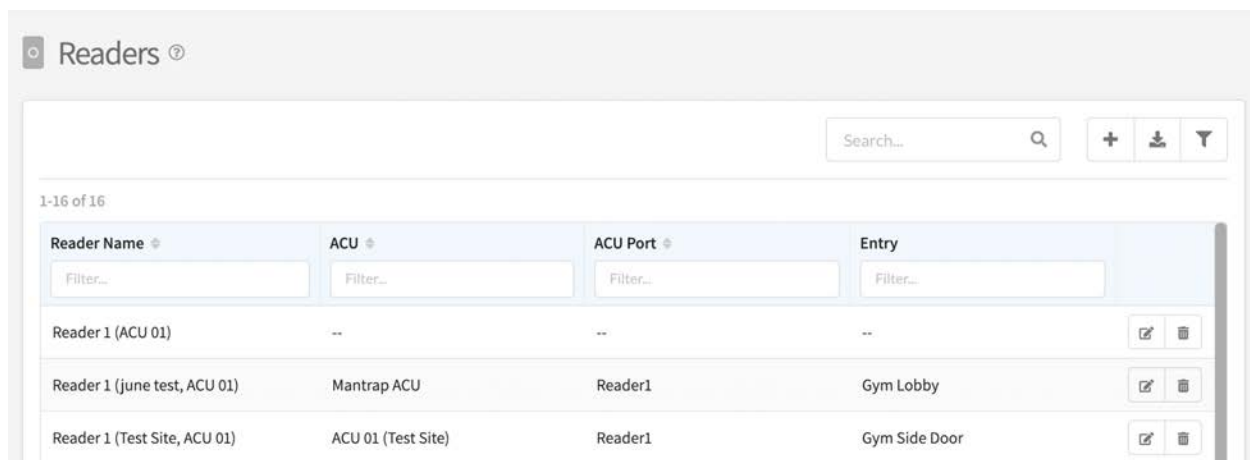
END OF LINE SUPERVISION

The SDC and Core Series Smart Hubs support end-of-line (EOL) supervision:

- Click on the **Cable** icon to open Cable Options
- Click on the **End of Line Supervision** dropdown to select **Line Shorted Detect**, **Line Cut Detect**, or **Both**
- The setting selected must match your physical wiring configuration, see the [Openpath Installation Guide](#) for more information

READER MANAGEMENT

The Reader Management screen is where you can view and manage readers. You can export Reader data to CSV by clicking the **Export Data** icon. Click the **Filter Columns** icon to show or hide columns.



The screenshot shows the 'Readers' management screen. At the top, there is a search bar and icons for adding, exporting, and filtering. Below the search bar, a table displays reader information. The table has four columns: Reader Name, ACU, ACU Port, and Entry. Each column has a filter input field. The table shows three rows of data, each with edit and delete icons on the right.

Reader Name	ACU	ACU Port	Entry
Reader 1 (ACU 01)	--	--	--
Reader 1 (june test, ACU 01)	Mantrap ACU	Reader1	Gym Lobby
Reader 1 (Test Site, ACU 01)	ACU 01 (Test Site)	Reader1	Gym Side Door

CREATE READER

1. To add a new reader, click the **Add Reader** button (+) on the top right corner
2. Enter a name for the reader — names are usually relevant to the location where the reader is installed
3. Select the ACU to which this reader belongs
4. Select the port to which this reader is wired
5. Click **Save**

Create Reader

Name *

Front Door

ACU *

Office Smart Hub

Port *

Openpath 4-Port Expansion (Expansion: 1): Reader1

Cancel

Save

WIRELESS LOCK MANAGEMENT

If you have the Allegion integration enabled, you can view and manage wireless locks and [gateways](#).

From this page, you can select locks and click **Batch Actions** to update firmware.

Wireless Locks

Batch Actions

1 row selected

Search

Download

Filter

Update Firmware

	Wireless Lock Name	Gateway	Lock Serial	Model Name	Firmware Version	State	Battery	Connection Status	
<input type="checkbox"/>	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	
<input checked="" type="checkbox"/>	Storage Closet LE Lock	Main Office	f2000000f151eaf	LEB	03.06.10	Unlocked	6.13 V	Connected	
<input type="checkbox"/>	Conference Room NDE Lock	Main Office	a2000000f14b233	NDEB	03.06.10	-	-	Unknown	
<input type="checkbox"/>	Hardware Cabinet LE Lock	Hardware Section	f2000000f14b3d4	LEB	03.07.01	Secured	4.76 V	Connected	

EDIT LOCK

- Click on the name of the lock to edit it
- From the **Power Failure** dropdown, select how the lock will behave in the event of the battery failing
 - As Is** – lock will remain in the same state



- b. **Safe** – unlocked
 - c. **Secure** – locked
3. Under **Reader Settings**, choose which type of card and fob credentials may be used at this lock
 - a. For Openpath DESFire EV1, EV2, and EV3 select 14443 UID (CSN)
 - b. For Openpath DESFire EV3-A, select 14443 Secure Mifare
 - i. **Note:** You cannot enable 14443 UID (CSN) and 14443 Secure Mifare/Mifare Plus/EV1 (NOC) at the same time
4. Under **Mobile Credential**, choose whether to enable mobile credentials on this lock
 - a. Adjust **Communication Range** to determine how close the mobile credential needs to be to the lock before appearing as a nearby entry in the app
 - b. Adjust **Performance** to determine how often the mobile app scans for locks
5. Click **Save**

The screenshot displays the configuration interface for an Openpath lock, organized into three main sections:




- Basic Settings:**
 - Power Failure Mode: Secure (dropdown)
 - Beeper Enabled: ☒
 - Blink interior LED when locked: ☐
 - Blink interior LED rapidly: ☐
 - Invalid Card Audit: ☐
- Reader Settings:**
 - Credential Reader: Prox in use:**
 - HiID: ☒
 - AWID: ☒
 - GE/CASI: ☒
 - GE4001: ☐
 - GE4002: ☒
 - Credential Reader: Smart in use:**
 - 14443 UID (CSN): ☐
 - 14443 Secure Mifare: ☒
 - 14443 Secure Mifare Plus: ☒
 - 14443 EV1 (NOC): ☒
 - 15593 UID (CSN): ☒
- Mobile Credential:**
 - Mobile Credential: ☒
 - Communication Range: Short (dropdown)
 - Performance: Normal (dropdown)

WIRELESS LOCK GATEWAY MANAGEMENT

This page shows you the list of gateways synced using the the Allegion ENGAGE™ app. From here, you can **Sync Gateways** and **Update Firmware**.

 **Wireless Lock Gateway Management** 

Note: To add new gateways or locks, use the Allegion ENGAGE™ App and then tap the Sync Gateways button.

1-7 of 7

Name	Lock Count	Status	Firmware Version	Actions
<input type="text" value="Filter..."/>	<input type="text" value="Unfilterable"/>	<input type="text" value="Unfilterable"/>	<input type="text" value="Unfilterable"/>	<input type="text" value="Unfilterable"/>
Engineering Gateway (000000689D)	1	● Disconnected	1.58.04	Update Firmware
Marketing Gateway (00000011FA)	1	● Disconnected	--	Update Firmware
Hallway Gateway (000000645D)	0	● Disconnected	1.60.08	Update Firmware
Lobby Gateway (0000006EBF)	1	● Connected	1.58.04	Update Firmware

REPORTS

Reports are where you can view user, entry, and Control Center activity.

Openpath offers a wide variety of report types:

- **Activity Logs** — display a list of all unlock requests across your Openpath access control system
- **User and Entry Activity Reports** — view user activity and entry activity via helpful charts and diagrams
- **Visual Activity Report** — view video snapshots related to entry events, and filter by user, site, entry, and time
 - In order to use this report, you must first set up the [Cisco Meraki integration](#)
- **Entry Access Report** — view which users have access to any given entry
- **User Access Report** — select or type in the name of a user to view all entries they have access to
- **Portal Audit Report** — shows a log of changes made in the Control Center or through the Openpath API
- **Credential Management** — view all credentials within your organization filtered based on credential type

To generate a report:

1. Go to <https://control.openpath.com/login> and log in
2. Under Reports, click on the report type you'd like to generate

3. Select a time period for the report
4. (Activity Logs only) Select Report Delivery:
 - a. **Deliver to Browser** — When using this method, do not refresh or close the browser tab. Reports may take a few minutes to generate. Not recommended for large datasets.
 - b. **Deliver via Email** — Useful for large datasets, select this method to run the report in the background and receive an email when the report is done. You can deliver the report to multiple email addresses.
5. Click **Search**
6. To download a report, click **Export to CSV**

INTEGRATIONS

Integrations are programmatic links to third party software and services, that let you sync users and add functionality to apps you already use.

This page lists available integrations. Click on the integration to learn more about setup and configuration.

Identity provider integrations let you add and sync users from providers you already use. Currently, Openpath integrates with **Google G Suite**, **Microsoft Azure Active Directory**, and **Okta**.

GOOGLE G SUITE

Note: To enable this feature, you must have administrative privileges in your Google G Suite account.

1. Under Integrations > All Integrations, click on the **G Suite** tile
2. Google will prompt you to sign in. Sign in with your G Suite account and allow Openpath to access your users and groups. This is also where you can enable the **Single Sign On** feature. Be sure to take note of the **namespace**.
3. After signing in, you'll be directed back to Openpath where you can enable the following settings:
 - a. **Auto-sync every 1 hour/15 minutes** — this will sync Openpath with G Suite once every hour or once every 15 minutes depending on which user management package you're using (see Administration > Account for package details)
 - b. **Auto-create mobile credential** — this will create a mobile credential for every user
 - c. **Auto-create cloud key credential** — this will create a Cloud Key credential for every user

- d. **Enable Single Sign-On (SSO) for users with portal access** — this will let users log into the Control Center with their Google credentials
- e. **Only import users from groups that have an Openpath group mapping** — if this is enabled, no users will be imported from G Suite if they are not assigned to an Openpath group
- f. **Auto-remove users from groups** — this will remove users from Openpath groups if they no longer exist in G Suite groups

Authentication strategy	OAuth2
Auto-sync every 1 hour	<input checked="" type="checkbox"/>
Auto-create mobile credential	<input checked="" type="checkbox"/>
Auto-create cloud key credential	<input type="checkbox"/>
Enable Single Sign-On (SSO) for users with portal access	<input type="checkbox"/>
Only import users from groups that have an Openpath group mapping ?	<input type="checkbox"/>
Auto-remove users from groups ?	<input type="checkbox"/>

Groups will continue to be assigned to users that have already been imported.
If you have not created any Openpath groups yet, please first create them in [Group Management](#).

[+ Create Group Mapping](#)

Provider Group	Openpath Group(s)
All Users	<input type="text"/>
Founders	Executive <input type="text"/>
Developers	Engineering <input type="text"/>

4. To map a specific group from G Suite to Openpath (required if you enabled **Only import users from groups that have an Openpath group mapping**), click **+Create Group Mapping**
 - a. Select the group from G Suite
 - b. Select the group from Openpath
 - c. Click **+Create Group Mapping**
5. Repeat step 4 until all groups that need to be mapped have been created

Add Provider Group Mapping

Identity Provider Group
Tech

Openpath Group
Engineering

+ Create Group Mapping

MICROSOFT AZURE ACTIVE DIRECTORY

Note: To enable this feature, you must have the Global Administrator role.

1. Under Integrations > All Integrations, click on the Microsoft Azure AD tile
2. Microsoft will prompt you to sign in. Sign in with your Azure AD account and allow Openpath to access your users and groups. This is also where you can enable the **Single Sign On** feature. Be sure to take note of the **namespace**.
3. After signing in, you'll be directed back to Openpath where you can enable the following settings:
 - a. **Auto-sync every 1 hour/15 minutes** — this will sync Openpath with Azure AD once every hour or once every 15 minutes depending on which user management package you're using (see Administration > Account for package details)
 - b. **Auto-create mobile credential** — this will create a mobile credential for every user
 - c. **Auto-create cloud key credential** — this will create a Cloud Key credential for every user
 - d. **Enable Single Sign-On (SSO) for users with portal access** — this will let users log into the Control Center with their Azure credentials
 - e. **Only import users from groups that have an Openpath group mapping** — if this is enabled, no users will be imported from Azure if they are not assigned to an Openpath group
 - f. **Auto-remove users from groups** — this will remove users from Openpath groups if they no longer exist in Azure groups

Authentication strategy	OAuth2
Auto-sync every 1 hour	<input checked="" type="checkbox"/>
Auto-create mobile credential	<input checked="" type="checkbox"/>
Auto-create cloud key credential	<input type="checkbox"/>
Enable Single Sign-On (SSO) for users with portal access	<input type="checkbox"/>
Only import users from groups that have an Openpath group mapping [?]	<input type="checkbox"/>
Auto-remove users from groups [?]	<input type="checkbox"/>

Groups will continue to be assigned to users that have already been imported.
If you have not created any Openpath groups yet, please first create them in Group Management.

[+ Create Group Mapping](#)

Provider Group	Openpath Group(s)
All Users	<input type="text"/>
Founders	Executive <input type="text"/>
Developers	Engineering <input type="text"/>

- To map a specific group from Azure to Openpath (required if you enabled **Only import users from groups that have an Openpath group mapping**), click **+Create Group Mapping**
 - Select the group from Azure
 - Select the group from Openpath
 - Click **+Create Group Mapping**
- Repeat step 4 until all groups that need to be mapped have been created

Add Provider Group Mapping

Identity Provider Group

Tech

Openpath Group

[Engineering](#)

[+ Create Group Mapping](#)

OKTA

Note: To enable this feature, you must have administrative privileges in your Okta account. We recommend using a [dedicated service account](#) that uses only the “Group” role as that role contains only the permissions that Openpath requires to synchronize your users and groups.

1. Under Integrations > All Integrations, click on the Okta tile
2. Enter your **API URL**. This should be the [Okta domain](#) for your organization, prefixed with `https://`, for example, `https://yourcompanyname.okta.com`.
3. Enter an **API Key**. First you’ll need to generate an [Okta API Key \(Token\)](#) associated with the Okta service account you have created for this integration. Ideally you should create a dedicated API Key to be used only with the Openpath integration, so that you have control over the lifecycle of this integration.
 - a. **Note:** Once you save the API Key, Openpath does not use or otherwise expose the API Key anywhere except when using it to call Okta to synchronize users and groups.

Authentication strategy

API URL:

API Key:

API Key ?

Auto-sync every 15 minutes: ☒

Auto-create mobile credential: ☒

Auto-create cloud key credential: ☐

4. After saving the API key, you can enable the following settings:
 - a. **Auto-sync every 15 minutes** — this will sync Openpath with Okta once every 15 minutes
 - b. **Auto-create mobile credential** — this will create a mobile credential for every user
 - c. **Auto-create cloud key credential** — this will create a Cloud Key credential for every user
 - d. **Only import users from groups that have an Openpath group mapping** — if this is enabled, no users will be imported from Okta if they are not assigned to an Openpath group

- e. **Auto-remove users from groups** — this will remove users from Openpath groups if they no longer exist in Okta groups
5. To let Super Admin users log into the Control Center with their Okta credentials, click the toggle next to **Enable Single Sign-On SSO with portal access**
6. To let users log into the Openpath app using Okta credentials, click the toggle next to **Enable Single Sign-On (SSO) for mobile app**

Auto-create mobile credential	<input type="checkbox"/>
Auto-create cloud key credential	<input type="checkbox"/>
Enable Single Sign-On (SSO) for users with portal access	<input checked="" type="checkbox"/>
Enable Single Sign-On (SSO) for mobile app	<input checked="" type="checkbox"/>

7. To let users log into the Control Center from the Okta portal, click the toggle next to **Allow IDP-Initiated SSO**
8. Fill out the required fields: **SAML SSO URL**, **SAML Issuer**, and **SAML Certificate**. You'll find this information in Okta.
 - a. Log into Okta and click on **Admin**
 - b. Go to Applications and click on your Openpath application
 - c. If you haven't already added Openpath, first click **Add Application**, then search for and add the Openpath Security application
 - d. Click **Sign On**
 - e. In the Settings box, click **View Setup Instructions**
 - f. Copy **SAML SSO URL**, **SAML Issuer**, and **SAML Certificate** from the Okta portal into their corresponding locations in the Openpath portal

Allow IDP-Initiated SSO ?	<input checked="" type="checkbox"/>
SAML SSO URL ?	<input type="text" value="https://yourcompanyname.oktapreview.com/app/openpathsecurit"/>
SAML Issuer ?	<input type="text" value="http://www.okta.com/abcde12345"/>
SAML Certificate ?	<pre>-----BEGIN CERTIFICATE----- TABoNGHSTXnXXAaFQ53WvOa9mG3T0lfhBdfjTpRFNaMz21eLUPToAM eoOPi8NOI3zcFye5XtZz1YQPe4clVilv1QSVQDD5r67i07NCwuaP8rXXQ Di2RRr5raPuVcglTbDFljXFLom1WdcFnm5HwEVbulJSBbmUY9Rw3B9 1Ycdbapkl1kncdfxgWaWCkc60eVQuMzEQUNKfVufvcputKIDJi1VsYD5u KcuGVYZq5S8ihB9rB3gmPcDxDjcaCiiJ3eEiQCBXvxv7EMp6rY6dXsCx WdQDx1lkjsg4FitJuMTABoNGHSTXnXXAaFQ53WvOa9mG3T0lfhBdfjTp RFNaMz21eLUPToAMeoOPi8NOI3zcFye5XtZz1YQPe4clVilv1QSVQDD5r 67i07NCwuaP8rXXQDi2RRr5raPuVcglTbDFljXFLom1WdcFnm5HwEVb uLJSBbmUY9Rw3B91Ycdbapkl1kncdfxgWaWCkc60eVQuMzEQUNKfVuf vcputKIDJi1VsYD5uKcuGVYZq5S8ihB9rB3gmPcDxDjcaCiiJ3eEiQCBXv -----</pre>
Only import users from groups that have an Openpath group mapping ?	<input checked="" type="checkbox"/>
Auto-remove users from groups ?	<input type="checkbox"/>

9. (After saving API credentials) To map a specific group from Okta to Openpath (required if you enabled **Only import users from groups that have an Openpath group mapping**), click **+Create Group Mapping**
 - a. Select the group from Okta
 - b. Select the group from Openpath
 - c. Click **+Create Group Mapping**
10. Repeat step 7 until all groups that need to be mapped have been created

The screenshot shows a web form titled "Add Provider Group Mapping". It contains two dropdown menus. The first, labeled "Identity Provider Group", has "Tech" selected. The second, labeled "Openpath Group", has "Engineering" selected. Below these is a blue button with a white plus icon and the text "Create Group Mapping".

ONELOGIN

You can integrate OneLogin with Openpath to import and sync users automatically.

Note: To enable this feature, you must have administrative privileges in your OneLogin account.

1. Go to <https://control.openpath.com/login> and log in
2. Under Integrations > All Integrations, click on the OneLogin tile
3. Enter the **Subdomain** for your OneLogin account—it should look something like ***yourcompanyname.onelogin.com*** with ***yourcompanyname*** being the subdomain
4. Click **Get API credentials** to go to OneLogin, then click **New Credential**
5. Enter a name for the credential, select **Read Users**, then click **Save**
 - a. Refer to [Working with API Credentials in OneLogin](#)
6. Copy and paste the **Client ID** and **Client Secret** to Openpath, then click **Save**
7. To make changes to the OneLogin integration settings, click on the OneLogin tile
8. Adjust sync options accordingly
9. Click the toggle next to **Enable Single Sign-On (SSO) with portal access** to let users log into the Control Center with their OneLogin credentials
 - a. Copy and paste your **SSO Client ID** here, which you can find by [connecting an OIDC enabled app in OneLogin](#)

10. **Only import users from groups that have an Openpath group mapping** – if this is enabled, no users will be imported from OneLogin if they are not assigned to an Openpath group
 - a. **Note:** After saving the integration and enabling it via your OneLogin API credentials, you can select OneLogin groups to map to Openpath groups. Or, you can map **All Users** to Openpath groups.
11. **Auto-remove users from groups** – this will remove users from Openpath groups if they no longer exist in OneLogin groups.

onelogin

Authentication strategy

Subdomain

companyname

.onelogin.com

OAuth Client ID

abcdefghijklmnopqrstuvwxyz1234567890

OAuth Client Secret

abcdefghijklmnopqrstuvwxyz1234567890

Auto-sync every 15 minutes

☒

Auto-create mobile credential

☒

Auto-create cloud key credential

☐

Enable Single Sign-On (SSO) for users with portal access

☒

Only import users from groups that have an Openpath group mapping ?

☒

Auto-remove users from groups ?

☐

Groups will continue to be assigned to users that have already been imported.

If you have not created any Openpath groups yet, please first create them in [Group Management](#).

+

Create Group Mapping

12. (After saving API credentials) To map a specific group from OneLogin to Openpath (required if you enabled **Only import users from groups that have an Openpath group mapping**), click **+Create Group Mapping**
 - a. Select the group from OneLogin

- b. Select the group from Openpath
 - c. Click **+Create Group Mapping**
13. Repeat step 12 until all groups that need to be mapped have been created

Add Provider Group Mapping

Identity Provider Group
Tech

Openpath Group
Engineering

+ Create Group Mapping

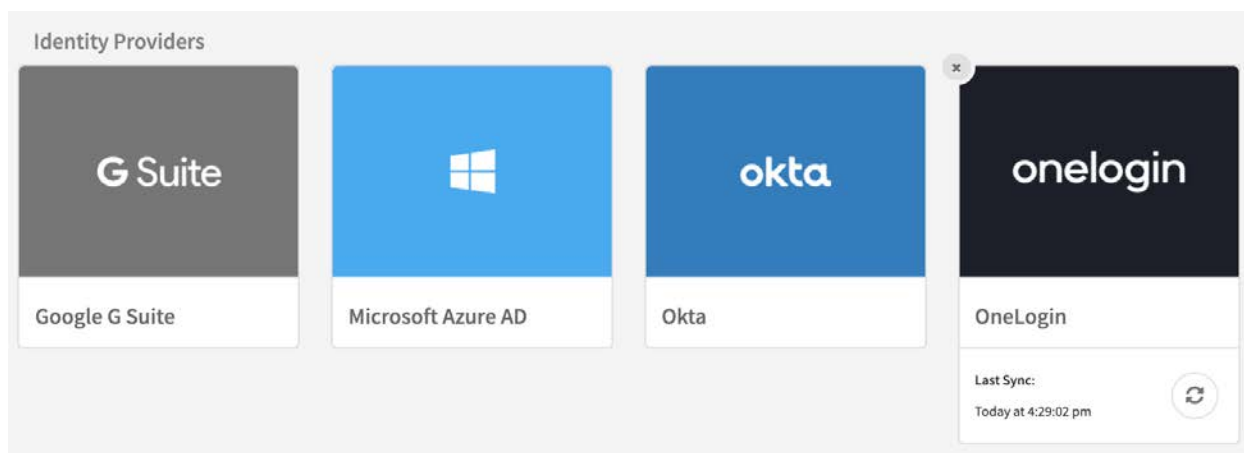
SINGLE SIGN-ON

Google G Suite, Microsoft Azure Active Directory, Okta, and OneLogin integrations support Single Sign-On (SSO). If enabled, users with portal access can log into the Control Center with their identity provider credentials.

Note: Openpath requires that you keep at least one Openpath-native administrative account in case there are ever any issues connecting to your identity provider.

MANUALLY SYNC

After setting up an identity provider integration, you now have an option to **Manually Sync**. You can perform this action at any time by clicking the sync icon in the lower righthand corner.



CAMIO

The Camio integration links Openpath Entry events and users with videos in Camio. To enable this integration, you create Outbound Webhooks that send data to Camio, designate a user with read-only portal access that translates UserIds to names, then input Org and Entry information into the Camio portal. Refer to the [Openpath and Camio support article](#).

RHOMBUS

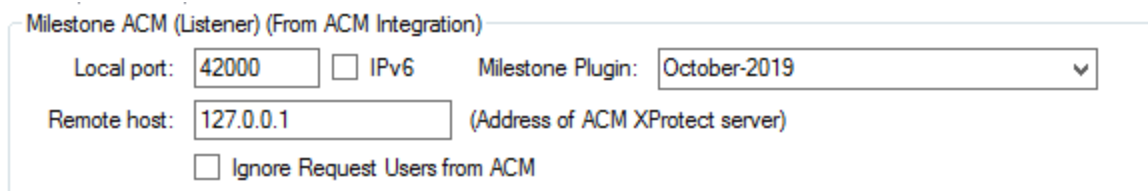
The Rhombus integrations links Openpath entry events and users with videos in Rhombus. To enable this integration, designate a user with read-only portal access and use those credentials to enable the integration in the Rhombus console. Refer to the [Openpath and Rhombus support article](#).

MILESTONE

To set up the Milestone VMS integration, you'll need to log into the Control Center, go to Integrations > All Integrations and click on the Milestone tile. Download and install Microsoft .NET 4.8, ACX, and Milestone Plugin.

To set up the Openpath integration on the Milestone server:

1. Run the Openpath_ACX_Plugin exe
2. Find the Openpath_ACX exe and run as administrator
3. Change the following settings under Milestone Configuration:



- Local port is required, and it must match the port defined in the Milestone Access Control settings
 - Remote host is required, and it must be the IP address of the machine that is running the event server
 - Milestone plugin has two settings, October-2019 or Before October-2019—select the appropriate version for your setup
4. Change the following settings under Openpath Configuration:

OPACX (To openpath Cloud)

User: ☐ Pass: Id:

Status polling frequency: seconds. (0 = no polling)

☐ Check door status after 'Admit' ☒ via Acu ☒ Check door status on 'Other Events' (Should be off when using PA)

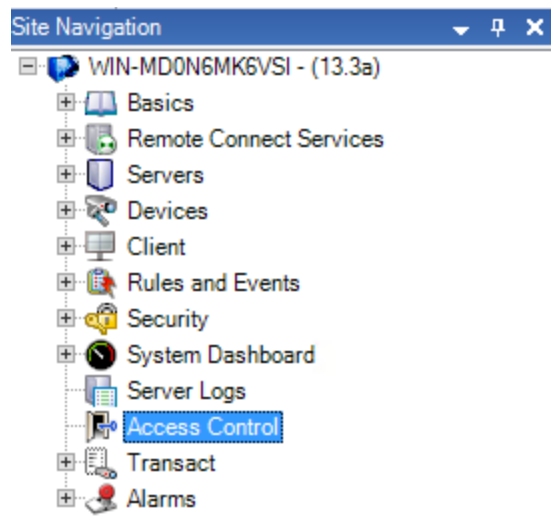
Image path: Deep link:

- User and Pass is required. Enter the login credentials of an Openpath Super Admin user. Openpath recommends creating a dedicated user for this purpose.

5. Click **Save** then **Close**

Milestone Management Client Configuration:

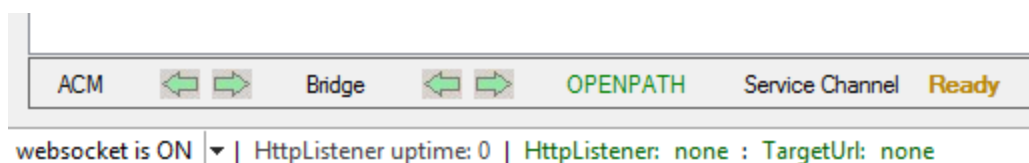
1. Go to Site Navigation



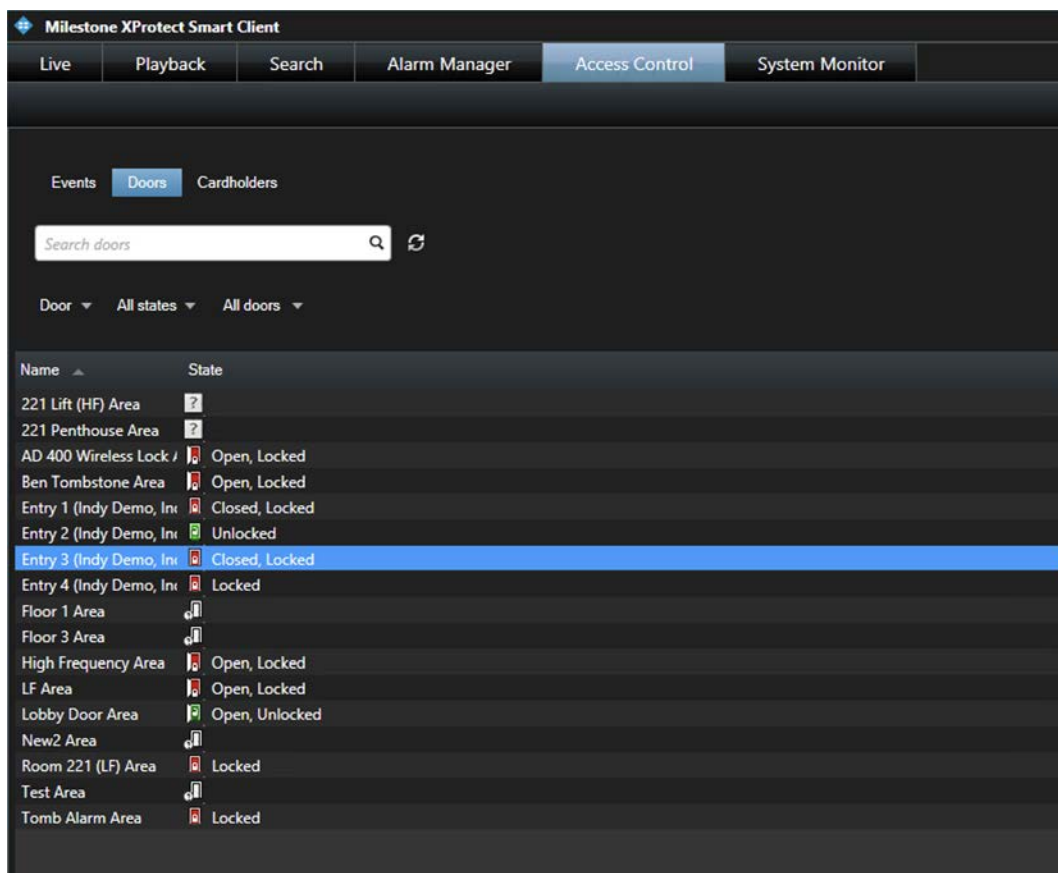
2. Right-click on **Access Control** and click **Create New**

Note: Leave User name and Password as the default. Ensure the Port field matches the ACX Plug-in.

3. Click **Next** and follow the prompts to tie cameras to doors
4. Restart Milestone Event Server, then open Openpath_ACX exe and confirm everything is connected:



5. Open XProtect Client. There should be an Access Control tab in the client now, and you can add information to live views as well.



CISCO MERAKI

You can integrate Cisco Meraki to view video snapshots within the Control Center and enable the [Visual Activity Report](#). To set up this integration, refer to the [Openpath and Cisco Meraki support article](#).

ENVOY

If you use Envoy for your visitor management system, Openpath can automatically assign access to Envoy visitors. You do this by creating an "Envoy Bot" in the Openpath Control Center that will generate guest access links for visitors in the Envoy system that can be shared by email or SMS. Refer to the [Openpath and Envoy support article](#).

SLACK

The Openpath and Slack integration works by defining commands that you type into Slack that unlock individual entries. Refer to the [Openpath and Slack support article](#).

ALLEGION

The Openpath and Allegion integrates works by connecting Allegion's Schlage® NDE and LE wireless locks via the ENGAGE™ technology.

ZAPIER

You can integrate Openpath with Zapier to trigger Zaps when new users are created, as well as automatically generate Guest Access Links, Credentials, and Users when Zaps are triggered.

To enable the integration, log into Zapier, then click this link:

https://zapier.com/developer/public-invite/3857/9330f625fabe427520bf9ba8a21dle_a5/

BUTTERFLYMX

Openpath hardware integrates with ButterflyMX's video intercom system by using the existing relay output from the intercom. Refer to the [Openpath and ButterflyMX support article](#).

WEBHOOKS

The Webhooks page provides information on setting up webhooks for users and unlock events.

CONFIGURATIONS

RULES ENGINE

The Rules Engine lets you create conditional rules that trigger actions based on Openpath events.

To create a new rule:

1. Go to <https://control.openpath.com/login> and log in
2. Go to Integrations > Rules Engine and click the **Add Rule** button (+)
3. Enter a name and description, then select a Trigger Type from the dropdown:
 - **Input** triggers include events like input state changes
 - **Entry** triggers include events like entry unlocks, ajar doors, and unlock failures

- The **Reader** trigger includes the Reader Fault State Changed event, which lets you monitor and take action when a reader loses or regains power
 - The **Relay** trigger includes the Relay Fault State Changed event, which lets you monitor and take action when a relay is short or over current
 - **Lockdown** triggers include lockdown plan triggers and reverts, as well as trigger and revert authorizations
 - A. For an example of a Lockdown type rule created using the Rules Engine, refer to [How do I set up a mantrap using the Rules Engine?](#)
 - **Event Forwarder** triggers include events from the previous categories, as well as billing activity, user creation and deletion, and identity provider sync issues
 - A. To learn more, refer to [How to create Event Forwarder rules in Openpath](#)
4. If you selected an Event Forwarder trigger, enter the Target URL, otherwise, use the graphical interface to set Conditions, Schedules, and Actions
 5. (Optional) To limit when this rule will occur, use Conditions. The types of Conditions available depend on the Trigger Type you selected:
 - If Trigger Type is **Input**, choose from Input State, ACU Port Filter, or ACU Filter
 - If Trigger Type is **Entry**, choose from Entry Filter, Zone Filter, or Site Filter
 - If Trigger Type is **Reader** or **Relay**, choose from ACU Port Filter or ACU Filter
 - If Trigger Type is **Lockdown**, choose from Lockdown Plan Filter or User Filter
 6. (Optional) To apply a time constraint on this rule, choose from a One-Time Schedule Event or a Repeating Schedule Event, then enter date and time information
 7. To specify what the rule will do once triggered, select an Action Type:
 - For **Relay** actions, you'll need to provide the **ACU Relay Port Number To Trigger**:
 - A. Single Door Controller: 1 or 2
 - B. 4 Door Controller: 1, 2, 3, or 4
 - C. Core Series expansion boards: (Expansion number x 10000) + Relay Number
 - Auxiliary relays are (Expansion number x 10000) + (Max Port Number + AUX number), so AUX Relay 2 on expansion board 3 which is an 8-Port Board would be 30010
 - D. You can also find these port IDs [using the API](#)
 - For **Notification** actions, enter the Subject and Body of the notification and the recipients' email or phone number

- A. **Note:** Enter phone numbers using the following format:
+15556667777 (no hyphens and a +1 before the number)
 - For **Webhook** actions, enter the URL and specify the HTTP method (GET or POST)
 - For **Lockdown** actions, specify the Lockdown Plan and select whether to Trigger or Revert the plan
8. To create custom or more complex rules, select the **Use JSON Editor** checkbox
 - For an example of a rule created using the JSON editor, refer to [How do I push Openpath events to Slack?](#)
9. Click **Save**

Note: The Basic package only includes the graphical interface for Input trigger types, but you can still use the JSON editor to create other rules

ALERT SETTINGS

Configure Alert Settings to receive email or SMS (US mobile numbers only) warnings regarding:

- **Billing** — invalid payments, expired terms, and/or your account being frozen
- **Entry Ajar** — an entry entering or leaving the ajar alarm state (i.e. when the contact sensor reports the door being open longer than the set duration.)
 - **Note:** In order to receive this alert, you must also enable the Ajar Feature under [CONTACT SENSOR](#) settings on the entry
- **Entry Authentication Failure** — an entry unlock request failing due to an invalid credential being used (e.g. a card with a number/CSN unknown to the ACU)
- **Entry Authorization Failure** — an entry unlock request failing due to a user not having access to that entry, using the wrong trigger method, or making an unlock request outside of associated schedules
- **Entry Unlock Failure** — an entry unlock request failing during the physical unlock phase, either due to a hardware issue or a failed webhook API call
- **Entry Forced Open** — an entry opening without first unlocking through Openpath or triggering the REX
 - **Note:** In order to receive this alert, you must also enable the Forced-Open Detection feature under [CONTACT SENSOR](#) settings on the entry
- **Entry Anti-Passback Breach** — a user attempting to re-enter a defined Anti-Passback Area without first exiting and vice versa
- **Lockdown Plan Triggered/Reverted** — receive notifications for every Lockdown Plan trigger/revert. If a Lockdown Plan contains entries from two Smart Hubs, you'll receive two notifications for every trigger/revert of that plan. See [LOCKDOWN PLAN MANAGEMENT](#).

- **Generic Input State Changed** — receive notifications when a Generic Input changes state
- **REX State Changed** — receive notifications when a REX (Request to Exit) input changes state
- **Contact Sensor State Changed** — receive notifications when a Contact Sensor input changes state
- **Identity Provider** — receive notifications when an identity provider synchronization fails
- **ACU Online Status Changed** — receive notifications when an ACU goes offline or comes back online
- **Tamper Detector State Changed** — receive notifications when an ACU's tamper detector reports a change.
- **Relay Fault State Changed** — receive notifications when a Relay port reports a change in fault state.
- **Reader Fault State Changed** — receive notifications when a Reader port reports a change in fault state.
- **Input EOL State Changed** — receive notifications when any input (Generic Input, REX, or Contact Sensor) changes End-Of-Line Supervision (EOL) state.
- **Occupancy Management** — receive notifications when the configured occupancy limit is exceeded within an Anti-Passback Area.

MOBILE APP

The Mobile App page is where you can enable Badge View and customize your organization's badge design.

BADGE VIEW

Badge View is a simplified UI for the Openpath mobile app. With Badge View enabled, users will see a digital ID badge with their name, photo, and other organizational information on their home screen of the Openpath app. If they are in proximity of a reader, the entry will appear below their Badge. Users can also view a list of all entries they have access to by tapping **View All**.

To enable Badge View:

1. Go to <https://control.openpath.com/login> and log in
2. Go to Administration > Mobile App and toggle **Enable Badge View**

Note: Users may need to update their Openpath app to the latest version in order to see the badge in their app.

To customize the badge design:

1. Click on the **Badge UI** tab to customize the look and feel of the digital badge
2. On the **Name** tab, adjust the size, position, and text formatting
3. On the **Photo** tab, adjust the position of the user's photo, and select a color for the photo's border
 - a. **Note:** A user without a photo will instead display their initials
4. On the Logo tab, click **Select Logo** to upload an image, **Replace Logo** to replace an existing one, or remove the image/leave the image blank to use text instead
 - a. **Note:** You cannot edit the Text settings if an image is selected
5. On the **Background** tab, use the default background or click **Replace Background** to use your own. You can also remove the background image and use a solid color background instead – click the color tile to select a color using the color picker, or click the arrows to enter your color in HEX, RGBA, or HSLA
6. On the **External ID** tab, click the slider to enable the optional External ID field, and adjust the size, position, and text formatting
7. On the **Custom Fields** tabs, select which Custom Field you'd like to use, then adjust the size, position, and text formatting
 - a. Custom Fields are only available on the Premium plan and can be edited under Users > Custom Fields
8. Click **Save** to publish your changes

Tips for badge design:

- You can enable or disable any of the fields using the **Enabled** sliders
- You can customize the placement of any field by adjusting the **Position** settings, increasing or decreasing the Center X and Center Y coordinates as desired
 - Dimensional coordinates are based on the default badge size of 300 x 188px. If you're trying to center a field, try inputting Center X (px): 150 and Center Y (px): 94.
- For text fields, you can customize the font family, size, weight, line height, alignment, color, case (lower, UPPER, or Capitalize Each Word). You can also choose whether first and last name appear on two lines or one.
- At any point you can click **Restore defaults** within a tab to revert changes made to that particular field – clicking **Restore defaults** will only affect the current field you are customizing.

BADGE TEMPLATES

The Badge Templates feature lets you design and format badges to print on your Openpath key cards. You can design multiple templates, including landscape and portrait styles, or select from several default templates for contractors, employees, and visitors.

To create a badge template:

1. Go to <https://control.openpath.com/login> and log in
2. Go to Configurations > Badge Templates
3. Click Add Badge Template (+)
4. On the **Settings** tab, select the Base Template and enter a name for the Template
 - a. If you'd like to use the default template without customizing further, click **Save** and proceed to printing your badges.
5. (Optional) Click the slider to make this template the **Org Default**
6. On the **Name** tab, adjust the size, position, and text formatting
7. On the **Photo** tab, adjust the position of the user's photo, and select a color for the photo's border
 - a. **Note:** A user without a photo will instead display their initials
8. On the **Logo** tab, click **Select Logo** to upload an image, **Replace Logo** to replace an existing one, or remove the image/leave the image blank to use text instead
 - a. **Note:** You cannot edit the Text settings if an image is selected
9. On the **Background** tab, click **Select Image** to use your own background image. You can also use a solid color background instead – click the color tile to select a color using the color picker, or click the arrows to enter your color in HEX, RGBA, or HSLA
10. On the **External ID** tab, click the slider to enable the optional External ID field, and adjust the size, position, and text formatting
11. On the **Custom Fields** tabs, select which Custom Field you'd like to use, then adjust the size, position, and text formatting
 - a. Custom Fields are only available on the Premium plan and can be edited under Users > Custom Fields
12. Click **Save** to publish your changes

To print a badge:

1. From Configurations > Badge Template:
 - a. Click on the template you'd like to print
 - b. Under the Preview section, select the name of the user whose badge you want to print

- c. Click **Print Badge**
 - d. Select the badge printer from the browser's print utility, or close and save the high res image to print via a different method
- 2. From Users > User Management:
 - a. Click on the name of the user whose card credential you want to print
 - b. On the Credentials tab, click the **Print** icon next to the card credential
 - i. If you don't see the Print icon, click the Edit icon next to the card, assign a Badge Template, then click Save
 - c. Select the badge printer from the browser's print utility, or close and save the high res image to print via a different method

Printing tips:

- Badge Templates should work with any printer, but you may need to adjust print settings for your printer
 - For the Evolis Primacy printer, we recommend printing at 96 DPI at 100% scale
 - If using a high definition printer, you may need to adjust the scale of the image in the printer settings
- Openpath Badge Templates are designed for use with Openpath key cards which are 3.37 x 2.125 in. Printing on different size cards may result in the image looking distorted.
- If using Safari, you may need to enable popups in order for the print utility to open

ADMINISTRATION

The Administration tab is where you can define organization details and set up billing information.

ACCOUNT

The Account page is where you can define organization details and set up billing information. This is where you can review and accept the Terms of Service.

In the Info section, you can change your Organization Name and provide an Accounts Payable Email.

SECURITY SETTINGS

Under Security Settings, click **Change Settings** to adjust timeout settings and view/edit access to your account.

- **Offline Timeout Setting.** This setting is the time (in days) that an ACU can be offline before the token will expire. After this time, credentials may not authenticate properly. The maximum value for this setting is 30 days.
- **Suspend Idle Users Timeout Setting.** This setting will suspend users who have not unlocked an entry within the set time duration. The minimum duration is the Offline Timeout Setting plus 7 days. Leave the setting blank to never suspend users.
 - Users with portal access will never be suspended.
- **Allow [your parent org] to have VIEW access to this organization.** You will see this option if your integrator is configured as a parent org. This setting is enabled by default. You may disable it at anytime to prevent your parent org from viewing your organization.
- **Allow Openpath Support to have VIEW access to this organization.** This setting is enabled by default. You may disable it at anytime to prevent Openpath Support from viewing your organization.
- **Allow Openpath Support to have EDIT access to this organization.** This setting cannot be enabled; you must escalate changes to Openpath Support or Engineering.
- **Allow Openpath Support to have UNLOCK access to this organization.** This setting cannot be enabled; you must escalate changes to Openpath Support or Engineering.

Security Settings

Offline Timeout Setting (30 Days Max) ? *

7

Suspend Idle Users Timeout Setting ? *

☒ Allow Openpath Support to have VIEW access to this organization

☐ Allow Openpath Support to have EDIT access to this organization ?

☐ Allow Openpath Support to have UNLOCK access to this organization ?

Cancel
Save

QUICK START

Use Quick Start to set up a site with ACUs and readers all on one page. This is useful if you're already familiar with setting up Openpath sites and hardware.

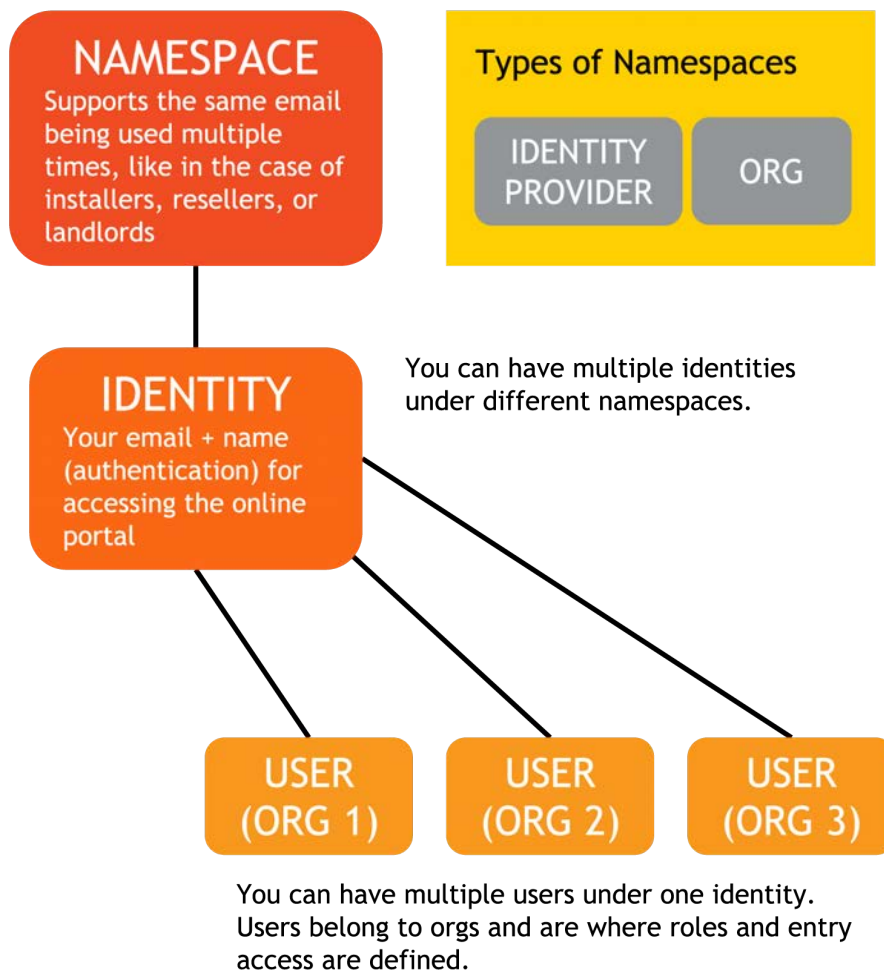
MY PROFILE

You can view and edit your profile by clicking the My Profile icon on the top right corner of the Control Center.

From there, you can edit your email and name (but not if you were imported from an identity provider), change your password, and configure Multi-Factor Authentication (MFA) by adding an MFA Device such as Google Authenticator. This gives you an extra layer of security when logging into the Control Center.

USER DATA MODEL

If you have portal access to more than one org, or you're using multiple identity provider integrations with SSO enabled, you should be familiar with how the Openpath User data model works.



A **namespace** is a contained pool of emails, all of which must be unique within the namespace. These emails (along with first name and last name and other info) are called **identities**. Identities are used for authentication and are what allow you to log into the Control Center. There are two types of namespaces: "identity provider" (e.g. G Suite, Active Directory), and "local org."

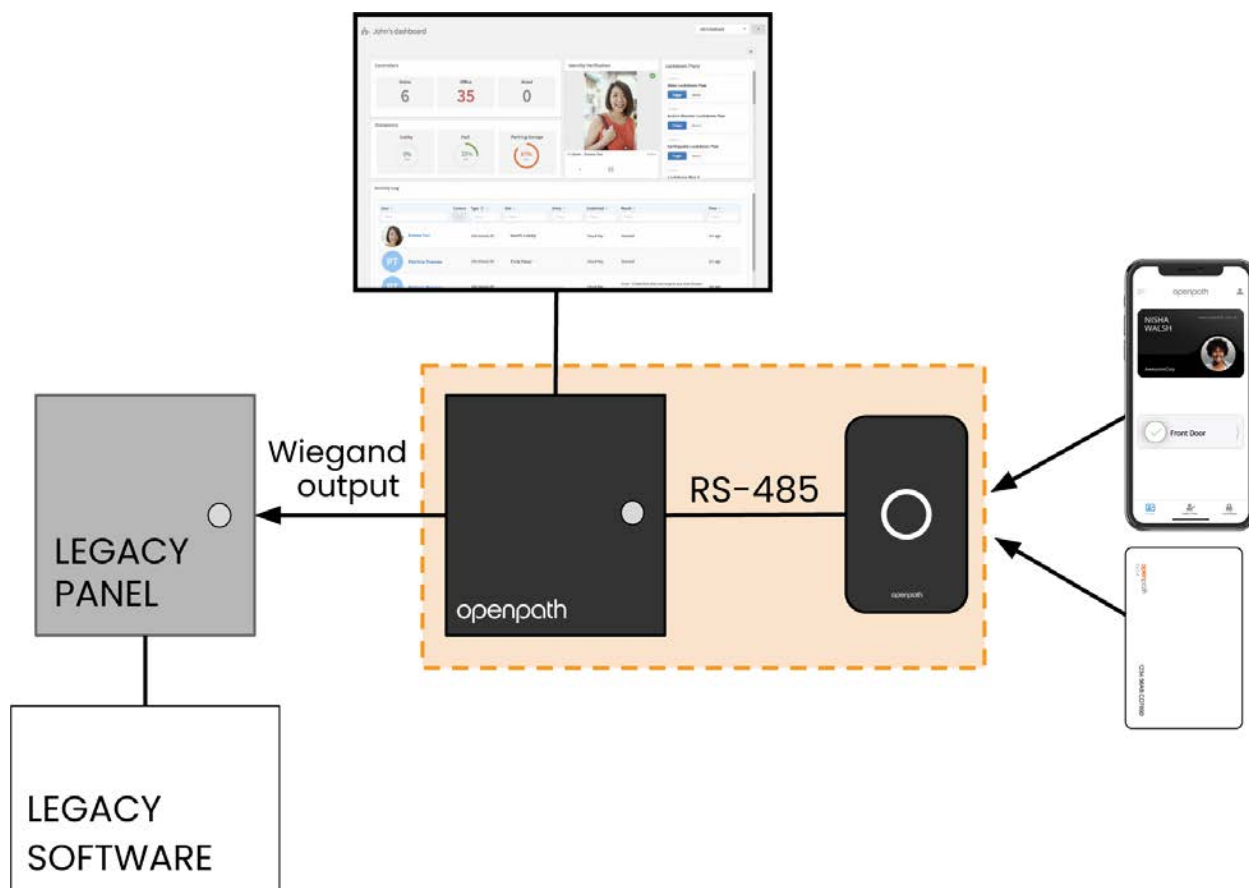
Namespaces allow the flexibility of having multiple instances of the same email that might come from different sources or have different authentication mechanisms (i.e. local password authentication or SSO). For example, you might have one identity (me@company.com) from when the org was created (under the local org namespace) that is authenticated through email and password. If you sync with an identity provider that has the same email (me@company.com) in it, another identity will be created under the identity provider namespace.

Identities are separate from, but related to **Users**. A **User** is an instance of an identity that belongs to a specific org, so a single identity could have multiple Users. This

model allows a single identity (email and password) to be able to access multiple orgs, which is useful for resellers and installers that need to be able to log in once but have access to many orgs. Identities are what let you log into the Control Center; Users are where you configure portal access, roles, and entry access for a particular org.

CONFIGURING OPENPATH WITH LEGACY SYSTEMS

You can configure Openpath to support existing legacy access control systems. In this setup, Openpath Smart Readers replace the legacy Wiegand readers and Openpath Smart Hub ACUs are installed between the Smart Readers and the legacy panel, with the Wiegand ports configured as outputs to the legacy panel. In this setup, the legacy panel makes the access control decisions while the Openpath hardware allows the use of Openpath credentials (including mobile and Cloud Key credentials).



If you're supporting a legacy system, there are a few items you need to configure in the Control Center:

- Under Entry settings, configure the Wiegand Device to **Output (Gateway)** mode. See [WIEGAND DEVICE](#).
 - If you want credential data to pass directly through to the legacy panel (without being authenticated by the Smart Hub ACU), enable **Gateway Credential Pass-Through**.
 - If you want users who make authenticated unlock requests with valid Openpath credentials but do not have dedicated Use for Gateway Wiegand IDs to be sent to the legacy panel, define a **Default Gateway Card Number** that will be sent instead.
- If you want to send individual user credentials to the legacy panel (instead of setting up a Default Gateway Card Number for the entry) you can create a Wiegand card credential (physical card not required) for the user and enable **Use for Gateway**. This way, that card number will be sent to the legacy panel whenever the user makes an authorized unlock request using any of the user's valid Openpath credentials. This is useful if you want to use one-to-one credential mapping for accurate user-level reporting within the legacy system. See [ADD A WIEGAND CREDENTIAL](#).

REGULATORY

All national and local electrical codes apply.

UL 294

When the Openpath Smart Hub 4 Door Controller is enclosed in the EI enclosure and powered by FPO75, the following performance levels are defined for the access control unit as per UL 294:

Attack:	Level I
Endurance:	Level I
Line Security:	Level I
Standby:	Level I

CAN/ULC 60839-11-1-16 GRADE 1

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

FCC

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2)

this device must accept any interference received, including interference that may cause undesired operation. To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm should be maintained between the antenna of Openpath Smart Reader(s) and persons during operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the User will be required to correct the interference at his own expense.

OP-RLF-STD/MULB: FCC ID: 2APJVOPRLF

OP-RHF-STD/MULB: FCC ID: 2APJVOPRHF

IEC 62368-1

- This equipment is intended only for use in a restricted access area.
- Securely fasten the equipment according to LifeSafety Power mounting instructions. See [FlexPower Vantage Standard Power System - Installation Manual](#).
- PROTECTIVE EARTHING: For safety, the Smart Hub must only be plugged into a grounded 3-prong outlet, wired with a minimum of 16 gauge wire to ground.

RF Radiation Hazard Warning

To ensure compliance with FCC and Industry Canada RF exposure requirements, this device must be installed in a location where the antennas of the device will have a minimum distance of at least 20 cm from all persons. Using higher gain antennas and types of antennas not certified for use with this product is not allowed. The device shall not be co-located with another transmitter.

Installez l'appareil en veillant à conserver une distance d'au moins 20 cm entre les éléments rayonnants et les personnes. Cet avertissement de sécurité est conforme aux limites d'exposition définies par la norme CNR-102 relative aux fréquences radio.

Industry Canada Notice and Marking

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by

Industry Canada. To reduce potential radio interference to other Users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.