OPENPATH ACCESS CONTROL SYSTEM USER GUIDE FOR ADMINISTRATOR WEB PORTAL V2.1



Table of Contents

Openpath Admin Portal User Guide NEW FEATURES | JULY 2019 **GETTING STARTED TERMINOLOGY** LOGGING IN DASHBOARD MAIN DASHBOARD HARDWARE DASHBOARD 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** SCHEDULE MANAGEMENT **CREATE SCHEDULE** MULTIPLE SCHEDULES CREDENTIALS SITES SITE MANAGEMENT **CREATE SITES** ZONE MANAGEMENT ZONE SHARING **CREATE ZONE** ANTI-PASSBACK **RESET ANTI-PASSBACK** MULTIPLE AREA ANTI-PASSBACK ENTRY MANAGEMENT **CREATE ENTRY ENTRY SETTINGS** ENTRY BEHAVIOR **ENTRY/EXIT HARDWARE OPENPATH READER REQUEST TO EXIT CONTACT SENSOR** WIEGAND DEVICE ADD CONTROL



ENTRY STATE MANAGEMENT CREATE ENTRY STATE **ENTRY SCHEDULES** HARDWARE ACU MANAGEMENT **CREATE ACU** ADD ELEVATOR BOARD READER MANAGEMENT ADD READER REPORTS **ACTIVITY LOGS** USER ACTIVITY AND ENTRY ACTIVITY **ENTRY ACCESS AUDIT INTEGRATIONS IDENTITY PROVIDERS** GOOGLE G SUITE MICROSOFT AZURE ACTIVE DIRECTORY OKTA SINGLE SIGN-ON MANUALLY SYNC **INBOUND WEBHOOKS** OUTBOUND WEBHOOKS **SUBSCRIPTIONS** HOOK ACTIONS **OTHER INTEGRATIONS** ADMINISTRATION **ORGANIZATION DETAILS BILLING** ALERT SETTINGS **QUICK START MY PROFILE USER DATA MODEL** CONFIGURING OPENPATH WITH LEGACY SYSTEMS REGULATORY UL 294 CAN/ULC 60831-11-1-16 GRADE 1 FCC IEC 62368-1 **RF Radiation Hazard Warning** Industry Canada Notice and Marking

Openpath Admin Portal User Guide

NEW FEATURES | JULY 2019

- You can restart services on ACUs from the Hardware Dashboard. See <u>HARDWARE</u> <u>DASHBOARD</u>
- Openpath integrates with Envoy. See <u>OTHER INTEGRATIONS</u>
- You can create and manage all entry schedules from the Entry Schedules page. See <u>ENTRY</u> <u>SCHEDULES</u>

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.

TERMINOLOGY

- **Smart Hub 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, or elevator floor secured with a reader.
- **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 <u>https://control.openpath.com/login</u>
- 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 <u>GOOGLE G SUITE</u> or <u>MICROSOFT AZURE ACTIVE DIRECTORY</u>

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 <u>USER DATA MODEL</u>.

👂 Sign In	
Sign In	🛔 Login 🛛 👘 Single Sign-On
Email	
Password	Show Password
Forgot Password?	
	Sign In

DASHBOARD

MAIN DASHBOARD

Once logged in, you'll see the home screen where the Dashboard shows the latest Entry statistics.

🕋 Dashboard				
Active Users (La	ast 24 Hrs)		Active Entries (Last 24 Hrs)	Total Activity (Last 24 Hrs)
28	3		10	150
Entry Status (i)				
Entry Status (i) Entry Name	Entry State	Lock State	Door State	Last Activity
Entry Status 🚯 Entry Name 2nd Floor Entry	Entry State Convenience	Lock State	Door State ock Ajar Alarm - Open since Feb. 4, 200	Last Activity 9 6.41:43 pm ? Unknown User Jan. 15, 2019 1:38:14 pm
Entry Status ① Entry Name 2nd Floor Entry Autotest Entry 1520537845	Entry State Convenience Convenience	Lock State Locked Unit	Door State ock Ajar Alarm - Open since Feb. 4, 202 ock No Sensor	Last Activity 9 6:41:43 pm ? Unknown User Jan. 15, 2019 1:38:14 pm @ Ross Miller Nov. 28, 2018 4:36:38 pm

On the Main Dashboard, you can quickly 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 remote unlock permissions (and the entry's state also allows remote unlock requests), you can unlock entries from the Main Dashboard by clicking the blue 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 Smart Hubs (ACUs) and readers.

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

• **Identify**: Identify an ACU to verify that the physical wiring matches the Control Center configuration. Clicking this will cause the Status LED on the ACU to flash green.



- **Refresh**: Refresh an ACU to send the latest data from the physical device to the Control Center.
- The **Restart** functions will restart individual software services on the ACU:
 - **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.

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. Select an ACU to see its associated readers. Scroll down to the Reader Status table. 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 center dot will light up green
 - the reader's outer ring LED will light up and spin
 - 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.

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 **Export Data**. Filters can be used on any of the columns to narrow down the users shown in the view.

Home	/ Users / User M	anagement								
	Users 🛈									
									Direct Council	
	- Create User	a+ Import Use	E* Expo	rt Data	Batch Actions +				Search	Q I
	First Name	Last Name	Email	Grc	Activate Users	Start Date	End Date	Date Added	Identity Provider Show Namespace	
	Filter	Filter	Filter	Filter	Suspend Users Delete Users)				
			justin	HQ Emţ	Reset Anti-Passback			2018-11-15 3	Microsoft Azure AD	2 0
	Graham	Anenberg	graham	HQ Emp	loyees Active	2018-06-08		2018-06-10 1	Openpath / OPHQ	c i
	Ann	Arwin	ann	HQ Emp	loyees Active			2018-11-18 5	Google G Suite	c î

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 <u>USER DATA MODEL</u>.

CREATE USER

- To create a new user, click the blue **Create User** button on the top left corner. Enter the user's name, work email address, and start/end date.
- If desired, upload a user photo, which will appear in the user's Openpath Mobile app.
- If the user is an admin and requires access to the web portal, click the **Portal Access** slide button and then add the **Super Admin** role.

Note: Only give portal access to users who require it, like an office manager or security guard.

openpath

Create User									
								🛔 User 📧 Credentials 🔒 Ac	cess
Note: Addition of	users	may result in an addi	tion	al monthly charge. Plea	ise	check with your adn	ninistra	tor if you have questions.	
Email									
name@company.co	m								
Add a user from an	n existi	ng namespace i							
First Name									
First							å		
Middle Name - Optional									
							\$		
Last Name									
Last							4		
Lust							1-	[Z
Start Date - Optional	1	Start Time - Optional		End Date - Optional		End Time - Optional	1 -		
Jun 01, 2019	曲	9:00 am	0	Select Date		Select Time	C		
Time Zone									
(GMT-08:00) Pacific 1	Гime								
_									
Portal Access	s								
Roles - A role other th	an 'En	try User' must be added	l in o	rder to allow portal acces	S			Total Cou	nt: 2
Entry User × Su	per Ad	lmin ×							~
Cancel								s	ave

IMPORT USERS

In addition to creating individual users, you can also bulk import users via CSV. Go to Users > Import Users (or from the User Management page, click the blue **Import Users** button). There you can upload a CSV file with your users' info. A sample CSV with the required fields is also included on the page. You can also import users by using a directory service integration. See <u>INTEGRATIONS</u>.

ISSUE CREDENTIALS

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

- 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
 - Card: Openpath DESFire (Encrypted) Secure
 - Card: Wiegand ID



• Enter the required information then click **Create**.

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

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. 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 > Access Logs. The card number will be displayed under the Details 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 <u>WIEGAND DEVICE</u>.

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 <u>CREATE GROUPS</u>.
- Alternatively, you can manually assign access to Sites and Zones by using the toggle buttons.
- Enabling **Remote Unlock** for the user will let them 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 <u>SCHEDULE</u> <u>MANAGEMENT</u>.

openpath

ary Anning		🏝 U:	ser Credentials	Access Securi
roups - Optional (i)				Total Cou
2nd Floor Tenants ×				\ \
ccess (i)				
Site	Zone	Access	Group Schedules	User Schedule
 Awesome Corp Office - Los Angeles 		×		
	2nd Floor [4 Entries]			Select Schedule
	3rd Floor [1 Entry]			Select Schedule
	Building Lobby [1 Entry]			Select Schedule
	Gus's Zone [2 Entries]	×		Select Schedule
emote Unlock				

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 <u>MY PROFILE</u>.

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 mobile app 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 <u>ANTI-PASSBACK</u>.

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 open 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 Ent	ry ×		~
Label for Rear Entry			
Rear Entry			•
Label for Side Entry			
Side Entry			•
Description			
Access to rear and side do	ors		din .
Charth Data Optional	Chart Time Optional	Find Date Cotional	
Start Date - Optionat	Start Time - Optional		
Select Date	Select Time	Jun 25, 2019 💼	5:11 pm
Time Zone			
(GMT-08:00) Pacific Time			
https://api.openpath.com	ו/s/2hwckuou6t34f	Guest Ac	cess Link: Copy to clipboard
https://api.openpath.com	ı/tokens/cloudKeyUnlockTol	kens/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 **Export Data**.

Home / Users / Group Management				
Groups 🔅				
+ Create Group	a	Reset Search		۹
Group Name	N 1.2	11 A 1		
oroup Name	Description	User Count		
HQ Employees	All OpenPath employees at the HQ	User Count 82	ľ	Ō
HQ Employees Test group	All OpenPath employees at the HQ Test group for IDP sync	User Count 82 43	ľ	ā ā
HQ Employees Test group Trade Show Group	All OpenPath employees at the HQ Test group for IDP sync People going to trade shows, dem	User Count 82 43 15	ľ	亩

CREATE GROUPS

- To create a new group, click the blue **Create Group** button on the top left 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 blue **Save** button to save your new group.

Marketing		
Description		
Marketing team members		
Jsers - Optional		
Lindsay McLain × Anh Cao × Liz McFarland ×		1.
Access (i)	7	
OpenDath Clabel Headquarters	Zone	Acces
Open autologia neadquarters	Cameron's Test Zone	
	HO Front Door Zone	
	HQ IT Closet Zone	
	Ross Test Zone	
	Test Zone	
OPHQ Autotest Site		() ×
✓ Trade Shows		
	Demo Stand Zone	
	Demo/Convention Zone	

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:

- **Entry User** all users are automatically assigned this role upon creation. This role is required for letting users open Entries via the mobile app.
- **Super Admin** gives full portal access with edit permissions.

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

Home / Users / Role Management					
Roles (i)					
		Poset	Coarch		
+ Create Role		Reset	Search		4
Role Name	Description	User	Count		α
Role Name Entry User	Description Permission to unlock entries	User 107	Count	ľ	α ē
Role Name Entry User Super Admin	Description Permission to unlock entries Full permissions for users	User 1 107 35	Count	ľ	

CREATE ROLES

- To create a new role, click the blue **Create Role** button on the top left corner. Enter a name, description, and assign users.
- Select the permissions you'd like this role to have, then click the blue **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.

openpath

ame Super Admin Read-Only			
Super Adminittead-Only			
escription			
Read-only portal access			đ
sers - Optional			
Click To Add Users			
Dashboard			
Permission	Enabled	Description	
READ		View dashboard	
WRITE	×	View and edit dashboard	
Users			
Permission	Enabled	Description	
READ		View users	
WRITE	×	View and edit users	
READ		View roles	
WDITE		View and edit roles and assign roles to users	

SCHEDULE MANAGEMENT

Schedule Management 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 **Export Data**.

Home / Users / Schedule Management		
Schedules (i)		
+ Create Schedule	Reset Search	Q
Name	Туре	
Filter		
Test	User/Group	2 1
Test - 2	User/Group	2 🖻
Locked	User/Group	2 🖻

CREATE SCHEDULE

- To create a user/group schedule, click the blue **Create Schedule** button on the top left corner. Enter a name, then click **Save**.
- Next, click on the **Scheduled Events** tab to define the schedule. Click the blue **Create 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).

		Search	C
Rank	Event	Scheduled State	
#1	M, Tu, W, Th, F 9:00 am - 5:00 pm PDT Starts Oct. 11, 2018 Ends Never	Standard Security	ư ā =
nowing all 1 iter	ns		Previous 1 Ne

MULTIPLE SCHEDULES

You can assign multiple user/group schedules to users/groups. Access is cumulative of the assigned schedules. For example, if a user has a group schedule that gives access 9:00 am to 5:00 pm and a user schedule that gives access 3:00 pm to 9:00 pm, then that user will have a combined access of 9:00 am to 9:00 pm.

CREDENTIALS

The Credentials page is where you can view all credentials within your organization filtered based on credential type. You can export credential data to CSV by clicking **Export Data**.

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 **Export Data**.

lome / Sites / Site Management		
Sites i		
+ Create Site Export Data	Reset Search	٩
Site Name	Zone Count	
600 Corporate Pointe	4	c ò
OpenPath Global Headquarters	3	2 0
OPHQ Autotest Site	2	2 0
Site Example	0	2 0
Trade Shows	5	2 0
Previous Page 1	of 1 10 rows 🗘 Next	

CREATE SITES

- To create a new Site, click the blue **Create Site** button on the top left corner. Enter a **Site Name** and click **Add Site Details**.
- Enter the address and a phone number for the Site and click the blue **Save** button.

openpath

Ģ
Ş
9
0

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 **Export Data**.

openpath

Home / Sites	/ Zone Management
--------------	-------------------

O allo	70.000	\bigcirc
440	Zones	1

+ Create Zon	e 🕒 Export	Data			Reset S	earch		Q
Zone Name	Description	Entry Count	Group Count	User Count	Anti-Passback	Sharing		
curt test		0	0	2		Shared to: 1	ľ	Ō
Demo Case 4		4	1	4			ľ	Ô
Demo Case 5	Demo Case 5	4	1	4		Shared to: 1	ľ	Ô
Demo Stand		19	2	15			ľ	Ŵ
Demo/Conv	Full ACUS for	8	2	8			ľ	Ô
Elevator Flo	Elevator floor 1	1	3	7		Shared by: 0	ľ	Ō
Elevator Flo		1	2	4		Shared by: 0	ľ	Ô
Elevator Flo		1	2	4		Shared by: 0	ľ	Ō
Elevator Flo		1	2	4		Shared by: 0	ľ	Ô
Elevator Flo		1	2	4		Shared by: 0	ľ	Ŵ
Pr	evious	Page	1 of 5	10 rows	\$	Next		

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 blue **Create Zone** button in the top left 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 blue **Create** button to save your new Zone.



ANTI-PASSBACK

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.

- 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.
 - 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 <u>ALERT SETTINGS</u>. They can also be used to trigger custom integrations. See <u>OUTBOUND WEBHOOKS</u>.

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 <u>MANAGING USERS</u>.

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 configured with Openpath Readers, but can also be gates, turnstiles, and elevator floors. You can export Entry data to CSV by clicking **Export Data**.

Home / Sites / Entry Managem	ent			
Entries 🔅				
+ Create Entry	port Data		Reset Search	Q
Entry Name	Zone	ACU (Smart Hub)	Default State	
Filter	Filter	Filter	Filter	
2nd Floor Entry	Test Zone	Office Smart Hub	Convenience	2 0
Autotest Entry 1520537845	OPHQ Autotest Zone 1	Office Smart Hub	Convenience	2
Autotest Entry 1520537848	OPHQ Autotest Zone 2		Convenience	2 0

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

- To create a new Entry, click the blue **Create Entry** button in the top left corner.
- Enter a name and select the Zone (optional) and ACU to which this Entry belongs. Once you select an ACU, then more Entry settings will display.





ENTRY SETTINGS

ENTRY BEHAVIOR

Default State	
Convenience	~
Allows all valid credentials and trigger methods	
chedule - Optional (1)	

Entry Behavior is where you set the Default State for the Entry. See <u>ENTRY STATE MANAGEMENT</u>. You can also assign an Entry Schedule, which is optional. See <u>ENTRY SCHEDULES</u>.

ENTRY/EXIT HARDWARE

Entry/Exit H	ardware i	
Port (i)		
Relay3		× ~
Entry Open Duration	on (10 Min Max) 👔 Unit	

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.
- **Open Entry Time** enter a time for how long the Entry remains unlocked before reverting back to its default state.
- **Unit** select whether to use seconds or minutes.



OPENPATH READER

Reader1 (IT Closet Reader Prod) Card Reading () Touch To Unlock () Range Near Phone Touch (Turnstiles) (Short range) Auto Proximity Unlock (Elevators & Turnstiles Only) () de Advanced Options Mobile Reader Range ()	Reader1 (IT Closet Reader Prod) Card Reading ① Touch To Unlock ① Range Near Phone Touch (Short range) (Long range) Auto Proximity Unlock (Elevators & Turnstiles Only) ① ide Advanced Options Mobile Reader Range ① Near Normal	Range Near Mobile Reader Range Mobile Beacon Range Near Near Near Normal Near Normal Normal	rt 🗉				
Card Reading (1) Touch To Unlock (1) Range Near Phone Touch Hand Touch (Short range) (Long range) Auto Proximity Unlock (Elevators & Turnstiles Only) (1) de Advanced Options Mobile Reader Range (1) Near Normal	 Card Reading (1) Touch To Unlock (1) Range Near Phone Touch Hand Touch (Long range) Auto Proximity Unlock (Elevators & Turnstiles Only) (1) Auto Proximity Unlock (Elevators & Turnstiles Only) (1) ide Advanced Options Mobile Reader Range (1) Near Normal 	 Card Reading (1) Touch To Unlock (1) Range Near Phone Touch Hand Touch (Short range) (Long range) Auto Proximity Unlock (Elevators & Turnstiles Only) (1) Auto Proximity Unlock (Elevators & Turnstiles Only) (1) Advanced Options Mobile Reader Range (1) Near Normal (1) 	Reader1 (IT Closet Read	der Prod)		×	\sim
Card Reading (1) Touch To Unlock (1) Range Near Phone Touch Hand Touch (Short range) (Long range) Auto Proximity Unlock (Elevators & Turnstiles Only) (1) de Advanced Options Mobile Reader Range (1) Near Normal	Card Reading () Touch To Unlock () Range Near Phone Touch Hand Touch (Iurnstiles) (Short range) (Long range) Auto Proximity Unlock (Elevators & Turnstiles Only) () Auto Proximity Unlock (Elevators & Turnstiles Only) () ide Advanced Options Mobile Reader Range () Near Normal	Card Reading () Touch To Unlock () Range Near Phone Touch Hand Touch Hand Touch (Inrustiles) (Short range) (Long range) Auto Proximity Unlock (Elevators & Turnstiles Only) () He Advanced Options Mobile Reader Range () Near Normal F					
Touch To Unlock (a) Range Near Phone Touch (Turnstiles) Hand Touch (Short range) (Long range) Auto Proximity Unlock (Elevators & Turnstiles Only) (a) de Advanced Options Mobile Reader Range (a) Near Near Normal	Touch To Unlock (Range Near Hand Touch (Short range) (Long range) Auto Proximity Unlock (Elevators & Turnstiles Only) () ide Advanced Options Mobile Reader Range () Near Normal	Touch To Unlock (1) Range Near Mobile Reader Range (1) Near Normal Mobile Beacon Range (1) Near Near Normal	Card Reading	i			
Range Near Phone Touch Hand Touch (Turnstiles) (Short range) Auto Proximity Unlock (Elevators & Turnstiles Only) (i) de Advanced Options Mobile Reader Range (i) Near Normal	Range Near Phone Touch Hand Touch (Short range) (Long range) Auto Proximity Unlock (Elevators & Turnstiles Only) (1) ide Advanced Options Mobile Reader Range (1) Near Normal	Near Phone Touch (Short range) Auto Proximity Unlock (Elevators & Turnstiles Only) (i) Che Advanced Options Mobile Reader Range (i) Near Normal F Mobile Beacon Range (i)					
Range Near Phone Touch Hand Touch (Turnstiles) Short range) Long range) Auto Proximity Unlock (Elevators & Turnstiles Only) (i) de Advanced Options Mobile Reader Range (i) Near	Range Near Near Hand Touch (Turnstiles) Hand Touch (Long range) Kanto Proximity Unlock (Elevators & Turnstiles Only) (1) ide Advanced Options Mobile Reader Range (1) Near	Range Near Hand Touch Hand Touch (Iong range) Auto Proximity Unlock (Elevators & Turnstiles Only) (i) Control Mobile Reader Range (i) Near Normal Normal	Touch To Unloc	K (i)			
Near Phone Touch (Turnstiles) Hand Touch (Short range) Hand Touch (Long range) X Auto Proximity Unlock (Elevators & Turnstiles Only) (i) de Advanced Options Mobile Reader Range (i) Normal	Near Phone Touch (Turnstiles) (Short range) (Long range) Auto Proximity Unlock (Elevators & Turnstiles Only) (1) ide Advanced Options Mobile Reader Range (1) Near Normal	Near Phone Touch (Turnstiles) Hand Touch (Short range) Hand Touch (Long range) Auto Proximity Unlock (Elevators & Turnstiles Only) () de Advanced Options Mobile Reader Range () Near Normal	Range				
Near Phone Touch (Turnstiles) Hand Touch (Short range) Hand Touch (Long range) X Auto Proximity Unlock (Elevators & Turnstiles Only) i de Advanced Options Mobile Reader Range i Near Normal	Near Phone Touch Hand Touch (Turnstiles) (Short range) (Long range) Auto Proximity Unlock (Elevators & Turnstiles Only) (1) ide Advanced Options Mobile Reader Range (1) Near Normal	Near Phone Touch Hand Touch Hand Touch Hand Touch (Turnstiles) (Short range) (Long range) Auto Proximity Unlock (Elevators & Turnstiles Only)	0		0		
(Turnstiles) (Short range) (Long range) Auto Proximity Unlock (Elevators & Turnstiles Only) i de Advanced Options Mobile Reader Range (i) Near	(Turnstiles) (Short range) (Long range) Auto Proximity Unlock (Elevators & Turnstiles Only) (i) ide Advanced Options Mobile Reader Range (i) Near	(Turnstiles) (Short range) (Long range) Auto Proximity Unlock (Elevators & Turnstiles Only) (1) de Advanced Options Mobile Reader Range (1) Near Normal F Mobile Beacon Range (1)	Near Phone Touch	Hand Touch	Hand Touch		F
Auto Proximity Unlock (Elevators & Turnstiles Only) (i) de Advanced Options Mobile Reader Range (i) Near Normal	Auto Proximity Unlock (Elevators & Turnstiles Only) (i) ide Advanced Options Mobile Reader Range (i) Near Normal	Auto Proximity Unlock (Elevators & Turnstiles Only) (1) de Advanced Options Mobile Reader Range (1) Near Normal F Mobile Beacon Range (1)					
de Advanced Options Mobile Reader Range (i) Near Normal	ide Advanced Options Mobile Reader Range () Near Normal	Advanced Options Mobile Reader Range () Near Normal F Mobile Beacon Range () Near Normal F	(Turnstiles)	(Short range)	(Long range)		
de Advanced Options Mobile Reader Range (i) Near Normal	ide Advanced Options Mobile Reader Range (1) Near Normal	de Advanced Options Mobile Reader Range (1) Near Normal F Mobile Beacon Range (1)	(Turnstiles)	(Short range)	(Long range)		
Mobile Reader Range (1) Near Normal	Mobile Reader Range (1) Near Normal	Mobile Reader Range (1) Near Normal F Mobile Beacon Range (1)	(Turnstiles)	(Short range) Unlock (Elevator	(Long range) rs & Turnstiles Only) (j		
Mobile Reader Range (i) Near Normal	Mobile Reader Range (i) Near Normal	Mobile Reader Range (i) Near Normal F Mobile Beacon Range (i)	(Turnstiles) Auto Proximity de Advanced Options	(Short range) Unlock (Elevator	(Long range) rs & Turnstiles Only) (j		
Near Normal	Near Normal	Near Normal F	(Turnstiles) Auto Proximity de Advanced Options	(Short range) Unlock (Elevator	(Long range) rs & Turnstiles Only) (į́)		
Near Normal	Near Normal	Near Normal F Mobile Beacon Range (i)	(Turnstiles) Auto Proximity de Advanced Options Mobile Reader Range	(Short range) Unlock (Elevator	(Long range) rs & Turnstiles Only) (j		
		Mobile Beacon Range (i)	(Turnstiles) Auto Proximity de Advanced Options Mobile Reader Range	(Short range) Unlock (Elevator	(Long range) rs & Turnstiles Only) (i)	·	
		Mobile Beacon Range (i)	(Turnstiles) Auto Proximity de Advanced Options Mobile Reader Range Near	(Short range) Unlock (Elevator	(Long range)	o O Normal	F
Nahila Daaran Damaa	Mahila Dagaran Dagaran ()	Near Normal E	(Turnstiles) Auto Proximity de Advanced Options Mobile Reader Range Near	(Short range) Unlock (Elevator	(Long range)	o O Normal	F
Monile Beacon Range	Mobile Beacon Range	Near Normal E	(Turnstiles) Auto Proximity de Advanced Options Mobile Reader Range Near	(Short range) Unlock (Elevator	(Long range) rs & Turnstiles Only) (j	o O Normal	F
Mobile Deacon Range		Near Normal F	(Turnstiles) Auto Proximity de Advanced Options Mobile Reader Range Near Mobile Beacon Range	(Short range) Unlock (Elevator	(Long range) rs & Turnstiles Only) (i)	Normal	F

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.
- **Touch to Unlock** enable this to allow Touch Entry. Set the range using the slider.
- **Auto Proximity Unlock** 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.
- Show 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

Request to Exit 🗈	
Port (i)	
REX1	× ~
REX1	×
lode 1	

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.

CONTACT SENSOR

	× ~
iture (i)	
i Min Max) Unit	
	iture (j) Min Max) Unit

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 <u>ALERT SETTINGS</u>. They can also be used to trigger custom integrations. See <u>OUTBOUND WEBHOOKS</u>.

WIEGAND DEVICE

Port 🛈	Mode (j)	
Wiegand2	\$ Input	\$

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 <u>CONFIGURING OPENPATH WITH LEGACY SYSTEMS</u> 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.

Add Control (1)	
Control	
Select Control	~
Add	

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
- Locked no entry allowed, even with an otherwise valid credential
- **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 1FA and third-party Wiegand methods
- **Strict** allows only interactive 2FA onsite mobile access and encrypted smart cards. Excludes all remote, 1FA, and non-encrypted methods.

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

+ Add Ei	ntry State		Search		
Туре 🗘	Entry State Name	Description	Relay State	# Trigger Methods	
Default	Unlocked	No credential required for access	Unlocked	N/A	
Default	Locked - No Entry	No entry allowed, even with an otherwise valid credential	Locked	0	
Default	Convenience	Allows all valid credentials and trigger methods	Locked	27	
Default	Onsite Only	Allows all valid onsite (non-remote) credentials and trigger methods	Locked	22	•
Default	Standard Security	Allows most mobile access and cards supported by Openpath readers, and excludes remote mobile 1FA and third-party Wiegand methods	Locked	11	
Default	Strict Security	Allows only interactive 2FA onsite mobile access and encrypted smartcards, and excludes all remote, 1FA, and non-encrypted methods	Locked	4	

Click the **View** button next to each default State in order to display the trigger methods for that State.

CREATE ENTRY STATE

1. To create a new Entry State, click the blue **Add Entry State** button in the top left corner.

openpath

Add E	ntry State
Name	
Description	
Trigger Met	nods
Enabled	Description
×	Mobile 1FA over BLE
×	Mobile 2FA over BLE
×	Mobile 1FA remote over WiFi
×	Mobile 2FA remote over WiFi

- 2. Use the sliders shown above to enable the trigger methods you want to be valid with this Entry State. Definitions for the various methods are provided at the bottom of the page.
- 3. Click the blue **Create** button when finished.

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 Create Entry Schedule, enter a name, then click Next

ront Door			着 Entry 🛛 🛗 Schedule
+ Create Event		Search	Q
Rank	Event	Entry State	
		No data available	
Showing all 0 entries			Previous 1 Next
Tips			

- 2. Assign this Entry Schedule to Entries by either typing in the names of the Entries or using the dropdown.
- 3. Click **Create 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.

			C ^e Repeating Event	🛗 One-Time Ever
Start Time		End Time		
9:00 am	0	5:00 pm		0
Time Zone				
(GMT-08:00) Pacific Time				0
Sun Mon Tue Wed Thu Fri Sat				
Start Date	1.44	Repeats Ur	ntil	1.44
Start Date Oct 26, 2018	i	Repeats Un Repeats I	-orever	t
Oct 26, 2018 Default State		Repeats Un	ntil	
Start Date Oct 26, 2018 Default State Convenience	t	Repeats Ur Repeats I	itil	#
Start Date Oct 26, 2018 Default State Convenience Scheduled State	##	Repeats Un	ntil Forever	######################################
Start Date Oct 26, 2018 Default State Convenience Scheduled State Unlocked	±	Repeats U	ıtil Forever	
Start Date Oct 26, 2018 Default State Convenience Scheduled State Unlocked Trigger after an unlock method inc	tuded in	Repeats Un	ttil	i #

HARDWARE

Hardware is divided in two categories: ACUs and Readers.

ACU MANAGEMENT

The ACU Management screen is where you can view and manage ACUs. You can export ACU data to CSV by clicking **Export Data**.



Home / Hardware / ACU Management								
ACUs (1)								
+ Add ACU						Reset Search		۹
ACU Name	ACU Serial	Entry Count	Status		Status Detail	Status Changed		
Filter			Filter	-	Filter			
ACU 01 (test site)		1	Unregistered	Register			ľ	Ē
ACU 1 (600 Corporate Point-General	2300-001	3	Activated	Re-register	Activation complete	2019-01-23 12:59:23 pm	ľ	Ō
ACU 2 (600 Corporate Point-Internal	2300-001	3	Activated	Re-register	Activation complete	2019-01-24 9:39:36 am	ľ	Ô
Chicago Field Sales Demo Case	2300-001	4	Activated	Re-register	Activation complete	2018-12-19 1:01:00 pm	ľ	Ô
Demo Case 2	2300-001	4	Activated	Re-register	Activation complete	2019-01-14 5:35:42 pm	ľ	Ē

CREATE ACU

- 1. To add a new ACU, click the blue **Add ACU** button on the top left corner.
- 2. Enter a name for the ACU. Names are usually relevant to the location where the ACU is installed.
- 3. From the **Add ACU Expansion Board** dropdown, select Openpath ACU and click **Add**. If your Smart Hub also contains an Elevator Expansion Board, select Openpath 16-port Elevator and click **Add**.
- 4. A description of the ACU (and/or Elevator Board) will appear in green. Click **Save**.

vame				
Office Smart Hub				
Select Expansion Board	Expansion Board Name	Expansion Board Ports	Action	

Once you add an ACU to the system, you need to register it (also known as provisioning). Please refer to the <u>Openpath Access Control System Installation Guide</u>.

ADD ELEVATOR BOARD

You need to edit ACUs when you install Openpath Elevator Boards in existing Smart Hubs.



- 1. To edit an ACU, click on the ACU from the ACU Management page
- 2. From the **Add ACU Expansion Board** dropdown, select Openpath 16-port Elevator and click **Add**.
- 3. Click Save.

READER MANAGEMENT

The Reader Management screen is where you can view and manage readers.

Home / Hardware / Reader Management						
Readers 3						
+ Add Reader			Reset	Search		٩
Reader Name	ACU	ACU Port	En	try		
Filter	Filter	Filter	Filter			
Chicago Demo Case No reader	Chicago Field Sales Demo Case	4	Demo Case 1 - 4		ľ	Ô
Chicago Demo Case Reader 1	Chicago Field Sales Demo Case	1	Demo Case 1 - 1		ľ	Ô
Chicago Demo Case Reader 2	Chicago Field Sales Demo Case	2	Demo Case 1 - 2		ľ	Ô
Chicago Demo Case Reader 3	Chicago Field Sales Demo Case	3	Demo Case 1 - 3		ľ	亩

ADD READER

- 1. To add a new reader, click the blue **Add Reader** button on the top left 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	
Reader port 4	
Cancel	Save

REPORTS

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

ACTIVITY LOGS

Activity Logs display a list of all unlock requests across your Openpath access control system. You can export Activity Log data to CSV by clicking **Export Data**.



Home / Reports / Activity Logs

Activity Logs

					St	tart Date	Start Time		End Date	End Time	
						Mar 31, 2019	1:42 pm	G	Apr 01, 2019	1:42 pm	0
Export D	ata										
Time	User	User Org	Credential T	Detail	ACU	Entry	Request	Location	n Result	Denied Reas	on
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	
2019-04-01	Ross Miller	OPHQ	Mobile	Titanium/1	ACU 1 (600 .	Rear Entry	2FA Unlock	Onsite	Denied	The user is not found	for the
2019-03-31	Cameron Ni	OPHQ	Card: Wiega	3628504095	ACU 1 (600 .	Rear Entry	1FA Unlock	Onsite	Granted		
019-03-31	Graham An	OPHQ	Card: Wiega	1088619480	Turnstile	Turnstile En	1FA Unlock	Onsite	Granted		
2019-03-31	Cameron Ni	OPHQ	Mobile	Titanium/1	Turnstile	Turnstile En	2FA Touch	Onsite	Granted		
2019-04-01	Cameron Ni	OPHQ	Mobile	Titanium/1	ACU 1 (600 .	Side Entry	1FA Touch	Onsite	Granted		
019-04-01	Kyle Reynish	OPHQ	Mobile	Titanium/1	ACU 1 (600 .	Lobby Entry	1FA Touch	Onsite	Granted		
019-04-01	Ashley Funes	OPHQ	Mobile	Titanium/1	ACU 1 (600 .	Lobby Entry	1FA Touch	Onsite	Granted		
019-04-01	Kyle Reynish	OPHQ	Mobile	Titanium/1	ACU 1 (600 .	Lobby Entry	1FA Touch	Onsite	Granted		
2019-04-01	Brian Jausu	OPHQ	Mobile	Titanium/1	ACU 1 (600 .	Lobby Entry	1FA Touch	Onsite	Granted		
019-04-01	Marissa Sch	OPHQ	Mobile	Titanium/1	ACU 1 (600 .	Lobby Entry	1FA Touch	Onsite	Granted		
	Previou	5		Page 1	of 10		10 rows 🗘			Next	

The default view lists requests chronologically with most recent first. Filters can be used on the columns to narrow down the requests shown in the view. The Denied Reason column provides information on why access is denied.

USER ACTIVITY AND ENTRY ACTIVITY

View user activity and entry activity via helpful charts and diagrams. Export to CSV by clicking **Export Data**.

ENTRY ACCESS AUDIT

View which users have access to any given entry by using the Entry Access Audit report. Select the entry from the dropdown. Export to CSV by clicking **Export Data**.

INTEGRATIONS

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

IDENTITY PROVIDERS



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**.

Home / Integrations / Identity Providers	
Google G Suite	
G Suite Connect Google G Suite to your Openpath account, allowing you to automatically synchronize users and provision access credentials for them.	Connect
Microsoft Azure AD	
Connect Microsoft Azure AD to your Openpath account, allowing you to automatically synchronize users and provision access credentials for them.	Connect
Okta	
okto Connect Okta to your Openpath account, allowing you to automatically synchronize users and provision access credentials for them.	Connect

GOOGLE G SUITE

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

- 1. Under Integrations > Identity Providers, click **Get Started** on the G Suite integration.
- 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 this will sync Openpath with G Suite once every hour.
 - 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. **Auto-assign to group** this lets you assign G Suite groups to groups you've created in Openpath.

Integration Provider		
G Suite		
Auto-sync every 1 hour Auto-create mobile credential Auto-create cloud key credential Auto-assign to group:		
Provider Group	Openpath Group(s)	
All Users	HQ Employees ×	× ~
All (all@openpath.com)	Choose Group(s)	•]
Accounts Payable (ap@openpath.com)	Test group ×	x ~
Billing (billing@openpath.com)	Choose Group(s)	•]
Bugs (bugs@openpath.com)	Choose Group(s)	v

MICROSOFT AZURE ACTIVE DIRECTORY

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

- Under Integrations > Identity Providers, click Get Started on the Microsoft Azure AD integration.
- 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 this will sync Openpath with Azure AD once every hour.
 - 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. **Auto-assign to group** this lets you assign Azure AD groups to groups you've created in Openpath.

- Integration Provider	
Microsoft Azure Active Directory	
Auto-sync every 1 hour Auto-create mobile credential Auto-create cloud key credential Auto-assign to group:	 C C C C C C
Provider Group	Openpath Group(s)
All Users	Openpath Demo Group 1 × X
Sales	Openpath Demo Group 2 × X
Engineering	Openpath Demo Group 3 × X

OKTA

Note: To enable this feature, you must have administrative privileges in your Okta account. We recommend using a <u>dedicated service account</u> 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 > Identity Providers, click **Get Started** on the Okta integration.



- 2. Enter your **API URL**. This should be the <u>Okta domain</u> for your organization, prefixed with *https://*, for example, *https://yourcompanyname.okta.com*.
- 3. Enter an **API Key**. First you'll need to generate an <u>Okta API Key (Token)</u> 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.

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.

4. Configure the following settings:

Integration Provider

- a. Auto-sync every 1 hour this will sync Openpath with Okta once every hour.
- 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. **Auto-assign to group** this option will be grayed out until you save the API credentials. After saving, return to the settings page to use this feature. This option lets you assign Okta groups to groups you've created in Openpath.

okta		
Authentication strategy	АРІ Кеу 😧	
API URL		0
АРІ Кеу		Q.
Auto-sync every 1 hour	×	
Auto-create mobile credential	\checkmark	
Auto-create cloud key credential	×	
Auto-assign to group	×	
Cancel		Save

SINGLE SIGN-ON

Google G Suite and Microsoft Azure Active Directory 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 setup, you now have an option to **Manually Sync**. You can perform this action at any time.

identity Providers	
Google G Suite	
G Suite Manually Sync	Update Settings
Last Sync: Today at 3:15:39 pm	
Microsoft Azure AD	
Microsoft Azure Active Directory Last Sync: Sep. 17, 2018 at 1:00:38 pm	Update Settings

INBOUND WEBHOOKS

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

OUTBOUND WEBHOOKS

SUBSCRIPTIONS

An outbound webhook subscription allows you to set up a listener for a "hook event," which will then trigger your choice of either a POST to your own specified target URL, or a "hook action" which is essentially a customized JSON configuration.

If you specify a target URL, your URL needs to be set up with "intent to subscribe," which is essentially like a handshake. This indicates that it intends to receive hooks from Openpath. When



you add a subscription with a target URL, we will be sending a request to the target URL with an "x-hook-secret" header that has a unique value. This same header must be echoed in the response.

Hook actions are currently set up by the Openpath support team to handle a defined set of hooks that Openpath can process on your ACU. We expose the JSON configuration in the "Hook Actions" section, but highly recommend that you do not edit the configuration.

HOOK ACTIONS

Hook actions are customized JSON configurations that are used as triggers for subscriptions. They handle specialized integration setups, such as triggering the disable of your ADT alarm.

Hook actions are currently set up by the Openpath support team to handle a defined set of hooks that Openpath can process on your ACU. We expose the JSON configuration here, but highly recommend that you do not edit the configuration.

OTHER INTEGRATIONS

The Other Integrations screen is where you can learn more about setting up integrations with Slack, Zapier, and Envoy.

ADMINISTRATION

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

ORGANIZATION DETAILS

The Organization Details screen is where you can define the name of the organization and add a logo.

I Organiz	zation Details	
Organization OPHQ	Name	
	openpath	
Cancel		Save



BILLING

The Billing page is where you set up payment details for your Openpath subscription and accept the Terms and Conditions.

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 <u>CONTACT SENSOR</u> 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 <u>CONTACT SENSOR</u> 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.

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.



Users belong to orgs and are where roles and entry access are defined.

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 <u>WIEGAND</u> <u>DEVICE</u>.
 - If you want card 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 <u>ADD A WIEGAND CREDENTIAL</u>.

REGULATORY

All national and local electrical codes apply.

UL 294

When the Openpath Smart Hub 4 Door Controller is enclosed in the E1 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 60831-11-1-16 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 <u>FlexPower Vantage Standard Power System Installation Manual</u>.
- 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 at 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.