Table of Contents

Openpath Admin Portal User Guide
NEW FEATURES | MAY 2020
GETTING STARTED
TERMINOLOGY
LOGGING IN
DASHBOARDS
ACTIVITY DASHBOARD
ENTRY 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
GRANULAR PERMISSIONS

CREDENTIALS
USER SCHEDULES
CREATE USER SCHEDULE
MULTIPLE SCHEDULES

CUSTOM FIELDS

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
CONTACT SENSOR
ENTRY/EXIT HARDWARE
OPENPATH READER
REQUEST TO EXIT
WIEGAND DEVICE
ADD CONTROL
ENTRY STATE MANAGEMENT
ADD ENTRY STATE
ENTRY SCHEDULES
LOCKDOWN PLAN MANAGEMENT
CREATE LOCKDOWN PLAN
TRIGGER A LOCKDOWN PLAN

HARDWARE
ACU MANAGEMENT
CREATE ACU
ADD ELEVATOR BOARD
EDIT ACU PORTS
END OF LINE SUPERVISION

READER MANAGEMENT
ADD READER

REPORTS
ACTIVITY LOGS
USER ACTIVITY AND ENTRY ACTIVITY
ENTRY ACCESS AUDIT
PORTAL AUDIT REPORT

INTEGRATIONS
ALL INTEGRATIONS
GOOGLE G SUITE
MICROSOFT AZURE ACTIVE DIRECTORY
OKTA
ONELOGIN
SINGLE SIGN-ON
MANUALLY SYNC
CAMIO
RHOMBUS
MILESTONE
ENVOY
SLACK
ZAPIER
BUTTERFLYMX

WEBHOOKS

CONFIGURATIONS
RULES ENGINE
CREATE RULE
ALERT SETTINGS

ADMINISTRATION
ACCOUNT
MOBILE APP SETTINGS
QUICK START

MY PROFILE

USER DATA MODEL

CONFIGURING OPENPATH WITH LEGACY SYSTEMS

REGULATORY
UL 294
CAN/ULC 60839-11-1-16 GRADE 1
FCC
IEC 62368-1
RF Radiation Hazard Warning
Industry Canada Notice and Marking
NEW FEATURES | MAY 2020

- You can create custom user fields. See CUSTOM FIELDS.
- You can customize and limit Roles with granular permissions. See GRANULAR PERMISSIONS.
- You can set up and configure the Single Door Controller in the Control Center. See CREATE ACU.
- Openpath’s integration with OneLogin lets you automatically sync users and use Single-Sign On. See ONELOGIN.
- Openpath’s integration with Milestone lets you associate doors and entries with cameras, enabling you to unlock and lock entries directly from the XProtect Smart Client. See MILESTONE.
- The Rules Engine lets you create conditional rules based on Openpath events. See RULES ENGINE.
- Several new alert types are available. See ALERT SETTINGS.

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 the Premium and Premiere User Management packages. Also, depending on your role, not all of these features may be visible to you.

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 [https://control.openpath.com/login](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](https://developers.google.com) or [MICROSOFT AZURE ACTIVE DIRECTORY](https://azure.microsoft.com).

**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](https://developers.google.com).
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.
ENTRY DASHBOARD

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

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 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. 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.
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 Data** 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**

- To create a new User, click the blue **Create 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**
- If desired, upload a User photo, which 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** 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.

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 blue 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 > 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 **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 **SCHEDULE MANAGEMENT**.
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 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 ANTI-PASSBACK.
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.
**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](image)

**CREATE GROUPS**

- To create a new Group, click the blue **Create 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 blue **Save** button to save your new Group.
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.
CREATE ROLES

- To create a new role, click the blue **Create 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 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.

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.
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 the Export Data icon.

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.

CREATE USER SCHEDULE

- To create a User/Group schedule, click the blue Create 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 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).

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.

CUSTOM FIELDS

You can create custom, optional fields for users that appear when you create and edit users, and also appear in the User Management table.

1. To create a custom field, click on the blue Create Custom Field button on the top right corner
2. Enter a name for the field and select a Field Type from the dropdown:
   - Checkbox
   - Date
   - Dropdown
   - Text
3. The field is enabled by default—if you do not want to use the field just yet, click the slider to disable
4. Click **Save**

5. If you selected a Dropdown field, click **Create Dropdown Item** and enter a name, click **Save**, then repeat for the remaining dropdown options

6. 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](image)

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.
CREATE SITES

- To create a new Site, click the blue Create Site button on the top right 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.

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 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 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 blue Save 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 **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 configured with Openpath Readers, but can also be gates, turnstiles, and elevator floors. 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

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

ENTRY BEHAVIOR

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.

CONTACT SENSOR

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](image)

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 (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

![Openpath Reader](image)

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/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 Touch/Wave to Unlock. 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
REX1

Mode
Normally Closed

✓ Trigger Relay to Unlock Entry
```

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 to 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
- **Locked** — 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 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.

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

1. To create a new Entry State, click the blue Create Entry State button in the top right corner.

![Add Entry State](image)

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

1. To add a new ACU or SDC, click the blue Create ACU button on the top right 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 or SDC 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.

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

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

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 to a Request to Exit input and vice versa, or to change either input to a Generic input. This is useful for creating webhook subscriptions. See [SUBSCRIPTIONS](#).
• You can only change the Input Type on a port that has not yet been assigned to an Entry.

**END OF LINE SUPERVISION**

Some Openpath hardware, like the SDC, supports 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

**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.

![Reader Management Screen](image)

**ADD READER**

1. To add a new reader, click the blue **Create 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 Form](image)

**REPORTS**

Reports are where you can view User, entry, and Control Center 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 the **Export Data** icon.
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 the **Export Data** icon.

**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 the **Export Data** icon.

**PORTAL AUDIT REPORT**

The Portal Audit Report shows a log of changes made in the Control Center or through the Openpath API. Each item can be expanded to view the underlying JSON record, which is useful if you’re trying to see why a particular action failed.
INTEGRATIONS

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

ALL INTEGRATIONS

This page lists all 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** — 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. **Enable Single Sign-On (SSO) for users with portal access** — this will let users log into the Control Center with their Google credentials.
   e. **Auto-assign to groups** — this lets you assign G Suite groups to groups you’ve created in Openpath.
      i. **Auto-remove users from groups** — this will remove users from Openpath groups if they no longer exist in G Suite groups.
      ii. **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.
MICROSOFT AZURE ACTIVE DIRECTORY

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

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** — this will sync Openpath with Azure AD once every hour.
   b. **Auto-create mobile credential** — this will create a mobile credential for every User.

<table>
<thead>
<tr>
<th>Provider Group</th>
<th>Openpath Group(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marketing</td>
<td>Marketing</td>
</tr>
<tr>
<td>Sales</td>
<td>Choose Group(s)</td>
</tr>
<tr>
<td>Engineering</td>
<td>Software, Hardware</td>
</tr>
</tbody>
</table>
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. **Auto-assign to groups** — this lets you assign Azure AD groups to groups you've created in Openpath.
   
   i. **Auto-remove users from groups** — this will remove users from Openpath groups if they no longer exist in Azure groups.

   ii. **Only import users from groups that have an Openpath group mapping** — if this is enabled, no users will be imported from Azure AD if they are not assigned to an Openpath group.

   ![Authentication strategy](image)

   Authentication strategy
   
   - **Auto-sync every 1 hour**
   - **Auto-create mobile credential**
   - **Auto-create cloud key credential**

   ![Enable Single Sign-On (SSO) for users with portal access](image)

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

   Namespace: idp:example-namespace
   
The namespace is used to sign in with SSO, so make sure to save it for future use.

   ![Auto-assign to groups](image)

   Auto-assign to groups

   - **Auto-remove users from groups**
   - **Only import users from groups that have an Openpath group mapping**

   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.

   ![Provider Group](image)

   Provider Group | Openpath Group(s)
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Marketing</strong></td>
</tr>
<tr>
<td><strong>Sales</strong></td>
</tr>
<tr>
<td><strong>Engineering</strong></td>
</tr>
</tbody>
</table>
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 > Identity Providers, click **Get Started** on the Okta integration.
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.

   ![API Key Input](image)

   **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. After saving the API key, you can enable the following settings:
   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.
      i. Auto-remove users from groups — this will remove users from Openpath groups if they no longer exist in Okta groups.
      ii. 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.

ONELOGIN

You can integrate OneLogin with Openpath to import and sync users automatically. **Note:** To set 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, and select Read Users, then click Save
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
10. After saving, you now have the option to Manually Sync. You can perform this action at any time by clicking the Sync icon on the lower righthand corner of the OneLogin tile
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](#).
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:
   - 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

![Site Navigation](image)

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

![Create Access Control System Integration](image)

**Note:** Leave User name and Password as the default. Ensure the Port field matches the ACX Plugin.

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:

![Milestone Event Server screenshot](image)

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.

![Milestone XProtect Smart Client screenshot](image)

**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.

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/3857/9330f625fabe427520bf9ba8a21d1ea5

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.

CREATE RULE

1. Click the blue Create Rule button in the top righthand corner
2. Enter a name and description, then select a Trigger Type from the dropdown:
   a. **Entry** triggers include events like entry unlocks, ajar doors, and unlock failures
   b. **Input** triggers include events like input state changes
c. **Event Forwarder** triggers include events from the first two categories, as well as billing activity, user creation and deletion, lockdown activity, identity provider sync issues, and hardware relay changes.

3. If you selected an Event Forwarder trigger, enter the Target URL.

4. If you selected an Entry or Input trigger, use the graphical interface (included in the Premium package) to set Conditions, Schedules, and Actions.

5. If you selected an Entry or Input trigger but do not have the Premium Package, deselect the Graphical Interface and provide additional information via JSON.

6. Click **Save**

### 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.

**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, provide an Accounts Payable Email, and set the 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.

**MOBILE APP SETTINGS**

The Mobile App Settings page is where you can upload the Organization Picture that will appear in the Openpath app.
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 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 [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.
- 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 isotope 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.