AVIGILON™ ALTA

Access

Administrator Guide

Avigilon Corporation
avigilon.com

20241209-en

Revisions

Guide	Description
December 2024	Registering devices: Register ACU or SDC in Alta Access web browser on page 90, Register video reader in Alta Access web browser on page 100, Register video intercom reader in Alta Access web browser on page 106
November 2024	Mercury™ MP Series intelligent controller support: Add one ACU or SDC on page 86 Site associations for users: Activity dashboard on page 29, Entry dashboard on page 32, User data model on page 42, Users on page 42, Add users on page 44, Delete users on page 52, Create access groups on page 54, Add roles on page 56, Add sites on page 66, Reports on page 119, Add rules and triggers on page 146, Event triggers and advanced filtering on page 152 Muster report filtering by Safe and Unsafe status: View and mark users as safe in the Muster report (Premium and Enterprise plans) on page 121 Retitled Create access groups on page 54 and Create schedules for users and access groups on page 60; added examples to Apply user schedules on page 61 and Apply access group schedules on page 62
September 2024	Control Center portal renamed to Alta Access License Plate Recognition (LPR) support: Add or edit license plate credentials on page 48, Additional device (control) settings on page 76, Alta Aware app on page 142, System requirements on page 142 Language support in Video Intercom Reader Pro: Configure intercom settings and two-way audio on page 110
August 2024	Device icon enhancements: Device dashboard on page 33, Collapse the Statistics card on page 33 Mercury LP Series intelligent controller and subpanel support: Add multiple ACUs or SDCs using Quick start option on page 85, Add one ACU or SDC on page 86, Edit ACU ports on page 92, Add expansion boards on page 91, Post-installation testing on page 169
July 2024	Avigilon DESFire EV3 Key Fob support: Issue keycard, fob, license plate, mobile, PIN, wiegand, or cloud-based credentials on page 46 Software updates: Apply device updates one at a time on page 117 Wave detection range for Pro Series readers: Openpath reader settings on page 74 Quick actions option: Choose a quick action on page 15, Add users on page 44, Issue keycard, fob, license plate, mobile, PIN, wiegand, or cloud-based credentials on page 46, Edit user access on page 50, Assign permission to remote unlock using Avigilon Alta Open mobile app on page 52 PIN generation and masking (hiding) option: Edit security settings on page 164, Issue

Guide	Description
	keycard, fob, license plate, mobile, PIN, wiegand, or cloud-based credentials on page 46, Add or edit PIN credentials on page 47
May 2024	Alta Video alarm management: Alarm Management workflow on page 18, Event triggers and advanced filtering on page 152 (Aware rule), Schedules on page 154 Common Alerting Protocol (CAP) integration with mass emergency notification and response systems: Add rules and triggers on page 146 (CAP message, Alert code), Action triggers and alarm notifications on page 154; Rave Alert notification system integration: Rave Alert app on page 144 Avigilon Alta Open mobile app (formerly, Openpath Mobile Access app), Avigilon Alta Access mobile app (formerly, Open Admin app) rebrand: User management on page 44 Tip in Device update management on page 116 Reset table option throughout Control Center: Show, hide, or reset information on page 121
April 2024	Occupancy report: Assign permissions to roles on page 57, Reports on page 119, Schedule report generation and forwarding (Premium and Enterprise plans) on page 122; Occupancy limit (previously, Occupancy) widget: Create custom dashboards on page 37 SAML Single Sign-on app: Sign in on page 12, Identity management on page 123, note in Manually sync accounts on page 124, SAML Single Sign-on app on page 137, Device (Read-Only) role in Role management on page 55
February 2024	Device updates: Device update management on page 116, Device update management on page 116 Avigilon Alta Open mobile app help setup: Add help contact for mobile credential users on page 163 Front Desk Connect and Visual Voicemail fields: Configure call routing to users, units, or front desk on page 111

Contents

Revisions **3**

Get started **12**

Sign in 12

Notifications 13

Set your preferred language 14

Set language at sign-in 14

Set language in your profile 14

Set language in organization-wide emails 14

Set language in site-wide emails 14

Choose a quick action 15

Terms 16

For more information 17

Technical support 17

Product documentation 17

Workflows **18**

Alarm Management workflow 18

Muster Reports workflow 19

Alta Video, Alta DMP, and Alta Access workflow 21

User and role management 21

Video playback and access events 22

Aware, DMP, and Alta Access app navigation 22

Triggering lockdown plans 24

Use Alta Access menu bar 24

Use Lockdown widget on custom dashboard 24

Use Lockdown event triggers 25

User profile **26**

Update your account information 26

Change password 26

Add MFA devices 26

Enable intercom notifications 27

Play or mute alarm notification sounds 27
Enable Dark mode, Light mode, or Match system theme 27
Dashboards 29
Activity dashboard 29
Filter by site 29
View camera snapshots 30
Alarms dashboard 30
Filter by alarm severity or status 30
Acknowledge, clear, or reactivate active alarms 30
Export alarm history 31
Entry dashboard 32
View usage statistics of an organization 32
Unlock entries 32
View entries on maps in Aware VMS 32
Device dashboard 33
Collapse the Statistics card 33
Filter controller status and view total number of readers 34
Refresh controller data 34
Restart controller services 35
Verify the physical reader is connected to Alta Access 36
Restart the reader 36
Mute the controller or reader 36
Custom dashboards (Premium and Enterprise plans) 37
Create custom dashboards 37
Edit custom dashboards 38
Cameras 40
View live video feeds 40
Initiate calls to intercom on Video Intercom Reader Pro 41
Play and download video 41
Users 42
Show, hide, or reset information 42
User data model 42
User management 44

Add users ... 44
Upload photo ... 45
Issue keycard, fob, license plate, mobile, PIN, wiegand, or cloud-based credentials ... 46
Generate guest access links and webhook URLs ... 49
Edit user access ... 50
View MFA credentials ... 52
Delete users ... 52
Import users by CSV file ... 53
Issue batch actions to users ... 53
Access groups management ... 54
Create access groups ... 54
Role management ... 55
Export information to CSV ... 56
Show, hide, or reset information ... 56
Add roles ... 56
Assign permissions to roles ... 57
Delete roles ... 59
User schedules ... 59
Create schedules for users and access groups ... 60
Apply user schedules ... 61
Apply access group schedules ... 62
Custom fields ... 63
Create custom fields ... 64
Sites ... 66
Site management ... 66
Add sites ... 66
Add zones ... 66
Building management ... 66
Add buildings ... 67
Add floors to buildings ... 67
Add units to floors and assign access ... 67
Zone management ... 68
Export information to CSV ... 68

Show, hide, or reset information ... 68
Zone sharing between customers ... 68
Add zones ... 68
Anti-passback and occupancy management ... 69
Entry management ... 71
Export information to CSV ... 72
Show, hide, or reset information ... 72
Add entries ... 72
Edit entries ... 73
Entry states ... 77
View trigger methods in entry states ... 78
Add entry states ... 78
Entry schedules ... 79
Add entry schedules ... 79
Add holiday schedules ... 80
Lockdown plans (Premium and Enterprise plans) ... 82
Add lockdown plans ... 82
Assign users and group permissions for lockdown plans ... 83
Devices ... 84
ACU management ... 84
Export information to CSV ... 84
Show, hide, or reset information ... 84
Add ACUs or SDCs ... 85
Register ACU or SDC in Alta Access web browser ... 90
Disable the Static Cloud IP connection ... 91
Add expansion boards ... 91
Edit ACU ports ... 92
Reader management ... 94
Export information to CSV ... 94
Show, hide, or reset information ... 94
Add reader ... 94
Wireless lock management ... 95
Update lock firmware ... 95

Edit locks 95
Wireless lock gateway management 98
Sync gateways with Alta Access 98
Update gateway firmware 98
Video reader management 99
Export information to CSV 99
Show, hide, or reset information 99
Add video reader 99
Register video reader in Alta Access web browser 100
View activated video reader 101
Configure recording, detection, and ONVIF settings 102
Change cloud video storage plan 104
Video intercom reader management 105
Export information to CSV 105
Show, hide, or reset information 105
Add video intercom reader 105
Register video intercom reader in Alta Access web browser 106
View activated video intercom reader 107
Configure recording, detection, and ONVIF settings 108
Change cloud video storage plan 109
Configure intercom settings and two-way audio 110
Configure call routing to users, units, or front desk 111
Use QR codes to look up user directories on phones (optional) 112
View live video feed 115
Answer calls from intercom 115
Device update management 116
Show or hide device updates 116
Apply device updates one at a time 117
Set up a maintenance window for all device updates 118
Reports 119
Show, hide, or reset information 121
Export report to CSV 121
Configure reports (Activity logs, Alarms, and Portal audit report) 121

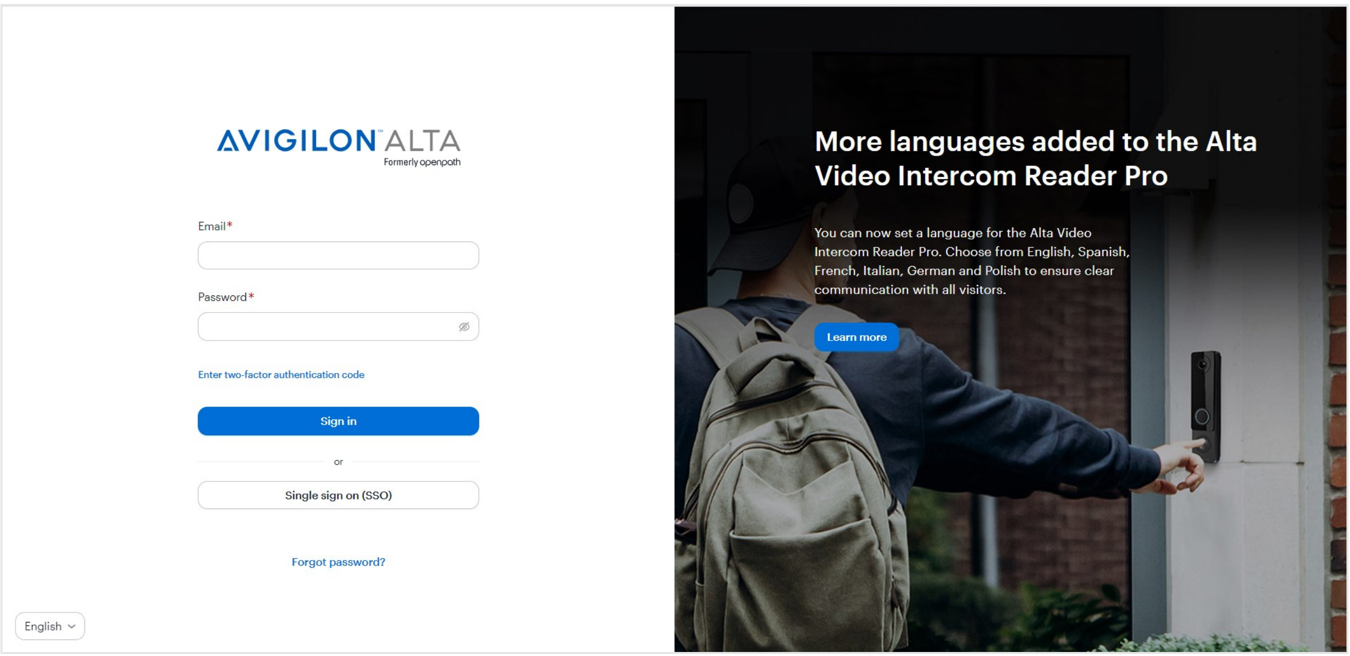
View and mark users as safe in the Muster report (Premium and Enterprise plans) 121
Schedule report generation and forwarding (Premium and Enterprise plans) 122
View scheduled reports (Premium and Enterprise plans) 122
App marketplace 123
Identity management 123
Manually sync accounts 124
Google Workspace 125
Microsoft Azure AD 127
Okta 131
OneLogin 135
SAML Single Sign-on app 137
Workday reports 139
Video management 142
Alta Aware app 142
Camio 144
Cisco Meraki 144
Milestone 144
Rhombus 144
Emergency notification and response 144
Rave Alert app 144
Visitor management 145
Envoy 145
Workplace communication 145
Slack 145
Wireless lock integration 145
Schlage Wireless Locks 145
Middleware integration 145
Zapier 145
Configurations 146
Rules 146
Add rules and triggers 146
Create custom rules 149
Alerts by email or SMS 149

Alarms (Premium and Enterprise plans) 151
Enable, disable, or silence alarms 151
Configure alarms 151
Mobile app 157
Enable badge view 157
Customize badge design 158
Badge templates 159
Add badge template 159
Print badge 161
Printing tips 162
Administration 163
Account 163
Accept terms and conditions 163
Add help contact for mobile credential users 163
Edit organization information 163
Edit security settings 164
Quick start for sites, ACUs, and readers 164
Licenses 164
Troubleshooting 166
Event descriptions 166
Appendix 167
Configure mobile gateway with legacy access control systems 167
System overview 167
Configure Wiegand device settings 168
Post-installation testing 169
Glossary 170

Get started

Avigilon Alta Access is an online portal where administrators can configure the Alta access control system in a web browser. This guide explains how to get started in Alta Access, manage users and hardware, and provide access to your controlled entries.

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



Sign in

1. Go to control.openpath.com/login and sign in. For access in the EU, go to control.eu.openpath.com/login.

    > **Note:** Alta Access is shown automatically in French, Spanish, Italian, German, or English based on the language and locale set in your browser.

2. Sign in using one of these options.

    > **Note:** If Alta Video and Alta Access have been unified in your organization, the Alta Access password must be used to sign in. The Alta Video password is no longer used in both systems. Normal browsing mode must also be used. The ⁝⁝⁝ button and ↗ app switcher links do not work in Chrome™ Incognito mode or private mode.

- If you have not configured Multi-Factor Authentication (MFA) for your account, you are prompted to set it up. For more information, see User profile on page 26.
- If you received admin credentials through Alta Access, enter your email and password, click **Enter two-factor authentication code** to enter the code generated by your app. Click **Sign in**.
- To use the **Single sign-on (SSO)** method, your organization must have enabled authentication with an identity provider and sign-in using an identity credential, such as your Okta on page 131 account. If enabled, enter your email and click **Continue**. Enter the two-factor authentication (2FA) code and click **Sign in**.

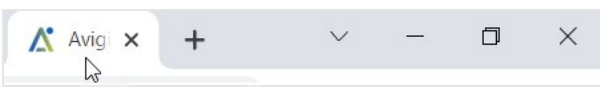
  > **Note:** If an error message asks for your namespace, it means your organization has enabled SSO for two or more identity providers. Ask the admin who set up the identity provider integrations for the correct namespace to use. See also User data model on page 42.

- If you are using the SAML Single Sign-on app method for the first time, enter your email and click **Use Avigilon Alta Id**. Enter the ID provided by your administrator and click **Continue**.

Notifications

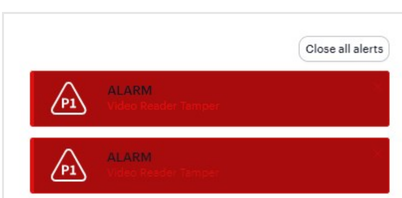
Notifications (also referred to as popup or toast notifications) are system messages that need your attention, such as alarm events, intercom events, and more.

- A visual indicator (blue dot) in the browser tab indicates new notifications.

  > **Tip:** This indicator helps notify you when you have Alta Access notifications even if you are viewing a different browser tab.

- The dot is removed when you click a notification or close all alerts in Alta Access.

  > **Note:** Ensure the audio on your device or machine is enabled when using the alarm notification sound.

Set your preferred language

You can set your preferred language to French, Spanish, Italian, German, or English in Alta Access.

Set language at sign-in

1. Go to control.openpath.com/login and sign in. For access in the EU, go to control.eu.openpath.com/login.

    > **Note:** Alta Access is shown automatically in French, Spanish, Italian, German, or English based on the language and locale set in your browser.

2. Select your preferred language in **Language** in the lower-left corner.
3. Click **Sign in**. The selected language is shown in your current login session.

Set language in your profile

1. Click your name in the upper-right corner and select **Profile**.
2. Select your preferred language in **Language**.
3. Click **Save**. The selected language is shown every time you log in to Alta Access.

Set language in organization-wide emails

1. Go to **Administration** > **Account**.
2. Click **Change settings** in the **Info** section.
3. Select the preferred language in **Organization Language**.
4. Click **Save**. All Alta Access emails for the org will be sent in the selected language.

Set language in site-wide emails

1. Go to **Sites** > **Sites**, and select a site or click the + **Add Site** button.

    For multiple site creation, go to **Administration** > **Quick start** and follow the screen workflow.

2. Select the preferred language in **Site language**.
3. Click **Save**. All Alta Access emails for the site will be sent in the selected language.

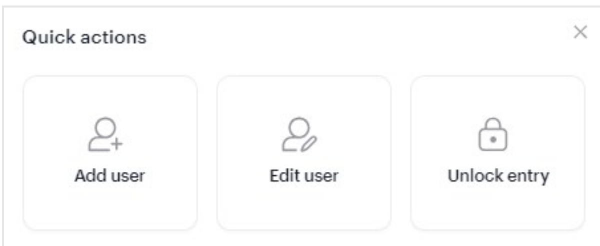
Choose a quick action

If you have the required permissions, you can choose shortcuts to actions that you use frequently.

- To set up permissions for user management in Alta Access, ensure read and write permissions are assigned to users by their role (see Assign permissions to roles on page 57).
- To unlock an entry for an end user, ensure a Cloud Key credential is created on the Credentials tab (see Issue keycard, fob, license plate, mobile, PIN, wiegand, or cloud-based credentials on page 46) and remote unlocking is enabled on the Access tab (see Assign permission to remote unlock using Avigilon Alta Open mobile app on page 52).

To select a quick action:

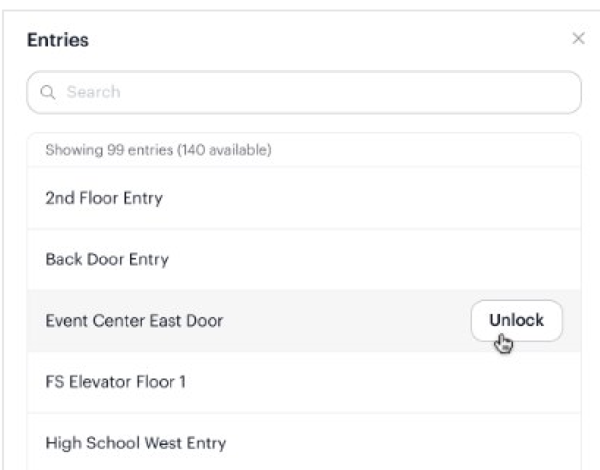
1. Select the icon at the top of the page to see the following menu.



2. To add a new user, click **Add user** and enter user details. For more information, see Add users on page 44.

   To edit an existing user, click **Edit user** and select the user. For more information, see Edit user access on page 50.

   To unlock an entry for a user, hover over the entry. When the **Unlock** button appears, click to unlock.



Terms

- **ACU** — Access Control Unit. A cloud-based control panel that manages access to a secured area.
- **Avigilon Alta Open mobile app** — Used for providing mobile credentials and remote unlock for users. The app is available for iOS and Android devices.
- **Cloud Key credential** — A credential that lets users generate links to provide temporary access through the Alta Open mobile app or Alta Access.
- **Alta Access** — 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 key cards, fobs, and mobile credentials.
- **CSN** — A card serial number on the key card.
- **Entry** — A door, gate, turnstile, elevator floor, or other point of access. Often secured with a reader or wireless lock.
- **Entry state** — Determines whether an entry is locked or unlocked and defines what kinds of credentials and trigger methods are valid.
- **Mobile credential** — An access method tied to a user's smartphone through the use of the Alta Open mobile app.
- **Remote unlock** — A feature that lets users unlock an entry using the Alta Open mobile app without needing to be in range of the Avigilon reader. Supported in gateway-connected devices.
- **Request to Exit (REX)** — 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 keycards, fobs, and Avigilon mobile credentials.
- **Trigger method** — A combination of credential type and 1FA/2FA.
- **User** — A person defined in Alta Access 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.

For more information

Technical support

For additional support documentation, see support.avigilon.com.

Product documentation

For additional product documentation, see the Alta Access (Cloud Solutions) product suite on avigilon.com.

Workflows

Alarm Management workflow

Note: A Premium or Enterprise license is required.

The Alarm Management app supports alarm configuration, monitoring, and reporting for alarm monitoring operators and administrators. Use this app to configure and monitor visual and audible alarms, and take the necessary actions to resolve them.

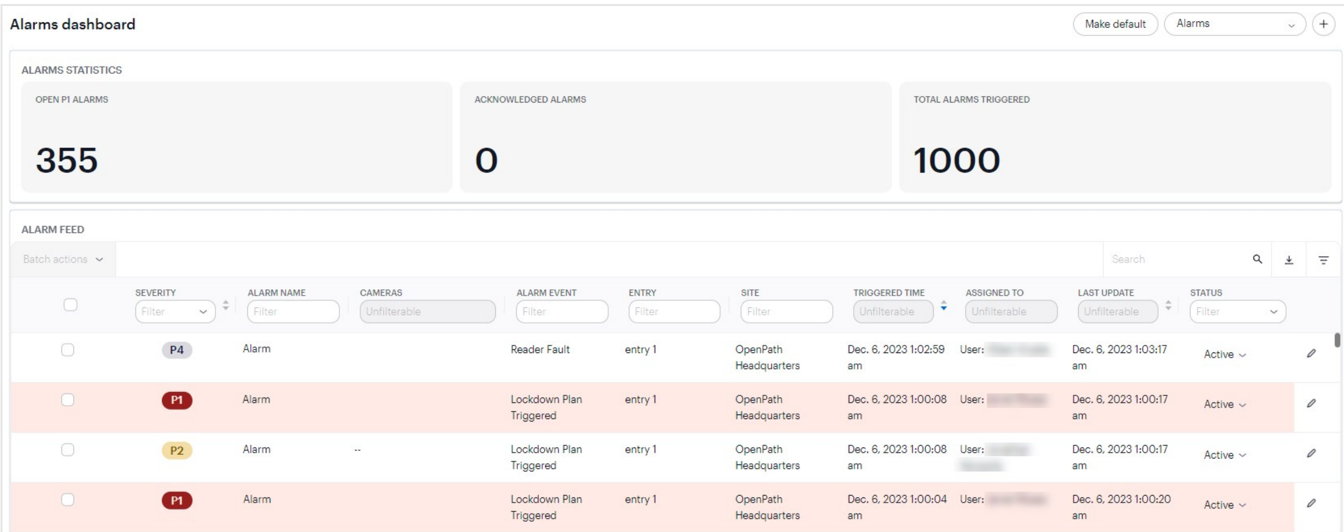


Figure 1 Example of triggered alarms in the Alarms dashboard

Note: If Alta Video and Alta Access have been unified in your organization, you can define rules in Alta Video and use them to trigger alarms in the in **Dashboards** > **Alarms dashboard**. For more information about the Rules tool, see Alta Video documentation.[1]

1. Go to **App marketplace** and install the **Alarm Management** app, if not already done.

   For more information, see App marketplace on page 123.

2. Go to **Configurations** > **Alarms**, configure the alarms, and assign them to roles or users.

   For more information about configuration, see Alarms (Premium and Enterprise plans) on page 151.

[1]https://aware.docs.alta.avigilon.com/en/Products/aware/rules/awarerules.htm

> **Note:** The Premium plan supports 100 alarm configurations. The Enterprise plan supports 500 alarm configurations. These limits include any Alta Video alarms that are configured in Alta Access.

Notifications to the assigned monitoring operator can be specified in an alarm action. For more information, see Action triggers and alarm notifications on page 154.

3. Go to **Dashboards**, and add the **Alarm feed** and **Alarm statistics** widgets to your custom dashboard. Or, change **Activity** to **Alarms** in the upper-right corner. For an example, see Figure 1 on the previous page. For more information, see Alarms dashboard on page 30 and Custom dashboards (Premium and Enterprise plans) on page 37.

> **Note:** The Premium plan supports 100 open alarms. The Enterprise plan supports 1000 open alarms. These limits include any Alta Video alarms that are configured in Alta Access.

Notifications are sent as these limits are approached, and again, when the limit is reached. After that, old open alarms are auto-cleared as new alarms are triggered. For more information, see Alerts by email or SMS on page 149.

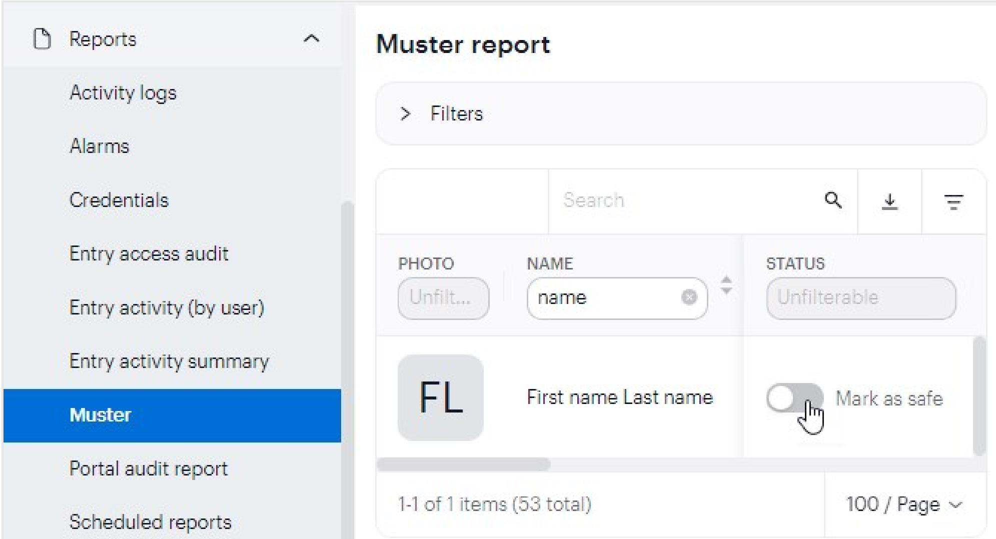
4. Go to **Reports** > **Alarms**, and configure the data to be displayed in the report. For example, configure an Alarm report that includes the users who triggered the alarms (see Triggered column) and the assigned monitoring operators who acknowledged the alarms with notes (see Note Added column).

For more information, see Configure reports (Activity logs, Alarms, and Portal audit report) on page 121.

Muster Reports workflow

> **Note:** A Premium or Enterprise license is required.

The Muster Reports app is an emergency response tool to quickly view the Alta Access users who may be in your building during an emergency evacuation. Use this app to rapidly generate a report, identify who may be on site, and account for their safety.



1. Go to **App marketplace** and install the **Muster Reports** app, if not already done.

   For more information, see App marketplace on page 123.

2. Optional. Go to **Sites** > **Entries**, and add an entry for the muster point.

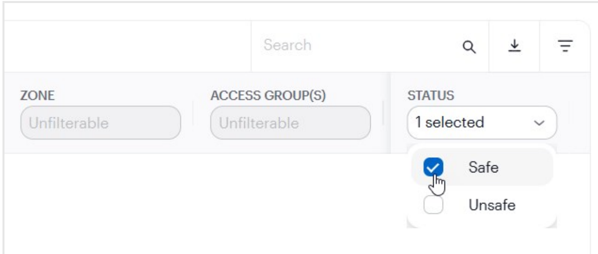
   > **Note:** Optional muster point entries can be installed at your emergency assembly locations. A credential reader is required to be installed at the entry. The reader should only be used in a muster event and not for any other purpose.

   For more information, see Add entries on page 72.

3. Go to **Users** > **Roles** and select the role that will view and edit muster reports.
   a. Scroll down to the REPORTS section and find **Muster report**.
   b. Select the **View and edit a muster report** toggles.
   c. Click **Save**.

4. Go to **Reports** > **Muster** and generate a report.
   a. Select a time period for the report.
   b. Optional. Select sites and zones.
   c. Click **Search**. Do any of the following:
      - Select the **Mark as safe** toggle in the generated report after you have ensured a user is safe.
      - View the users who are automatically marked as safe in the generated report, if their credentials

were scanned at the muster point entry before you generated the report.



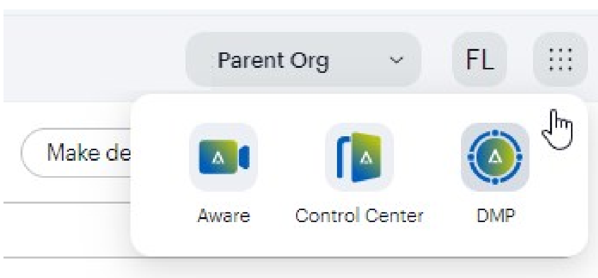
5. Export the report to CSV for record keeping.

   - Click the icon.

Alta Video, Alta DMP, and Alta Access workflow

> **Note:** The preview features in this section are not available to all organizations. Alta DMP (Alta Deployment Management Portal) is only available to Alta Video partners and resellers.

If Alta Video, Alta DMP, and Alta Access have been unified in your organization, you can use three-way app navigation (see example below) and the same password for those systems. If the Alta Video integration is enabled, you will have access to video playback of Alta Video camera feeds, access event sharing, and more. If the Alta Access Alarm Management app is installed, you can can define rules in Alta Video and use them to trigger alarms in the Alarms dashboard (see Alarm Management workflow on page 18) . If Alta DMP is enabled for Alta Video partners, they will have access to an app for managing their customer deployments.



> **Note:** The button and app switcher links cannot be disabled (default setting). Administrators may contact support.avigilon.com for more information.

User and role management

To give an Alta Video user access to Alta Access:

- In the Alta Video dashboard, add the Alta Video user to the **Administrators** user group.

  The Aware Default Role is assigned automatically and generates an email invite to set up a password for the new Alta Alta Access account. For more information about default roles, see Role management on page 55.

> **Note:** If Alta Video and Alta Access have been unified in your organization, the Alta Access password must be used to sign in. The Alta Video password is no longer used in both systems.

- To assign more permissions in Alta Access, see Add users on page 44.

To give an Alta Access user access to Alta Aware:

- Assign the **Aware Default Role** to the Alta Access user account. For more information about default roles, see Role management on page 55.
- Or assign the **Operators** role to the user account in Alta Video. If more permissions are needed, see Aware documentation.

> **Note:** Alta Video SSO users do not have access to the app switcher links in both Alta Video and Alta Access. Alta Access SSO users cannot sign in using the Alta Video sign-in page.

Video playback and access events

To view the Avigilon Ava cameras and access events in Alta Access:

1. Go to **App marketplace** and install the Alta Video video management system, if not already done.

   For more information, see Alta Aware app on page 142.

2. Sign in to Alta Access or Alta Video using the Alta Access password.

   > **Note:** The Alta Aware password is no longer used.

   If signing in through Alta Video, select the button and then **Alta Access**.

3. Go to **Cameras** and select any Avigilon Ava camera connected through your Alta Video account.

   For more information about video playback, see Cameras on page 40.

4. Go to **Dashboards**, and add the **Activity logs** and **Visual activity report** widgets to your custom dashboard. Or, change **Activity** to **Activity logs** or **Visual activity report** in the upper-right corner to view relevant access events.

   For more information about access events, see Dashboards on page 29 and Reports on page 119.

Aware, DMP, and Alta Access app navigation

> **Note:** The button and app switcher links do not work in Chrome™ Incognito mode or private mode. Alta Video SSO users do not have access to these links.

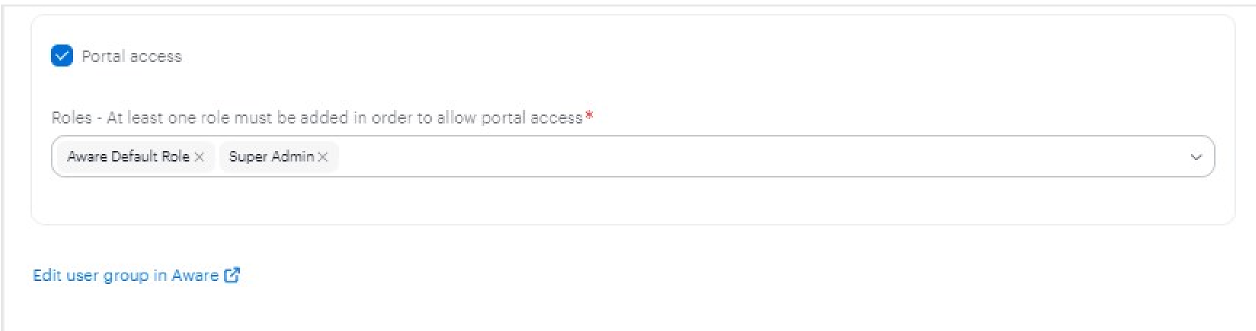
- In Alta Access, select the button and then **Aware** or **DMP** (Deployment Management Portal), if the latter is enabled for your user account in Alta Video.

  The Alta Aware page is displayed on a new browser tab, already signed in. For more information about the Aware dashboard or the DMP portal, see Aware documentation and Aware DMP documentation, respectively.

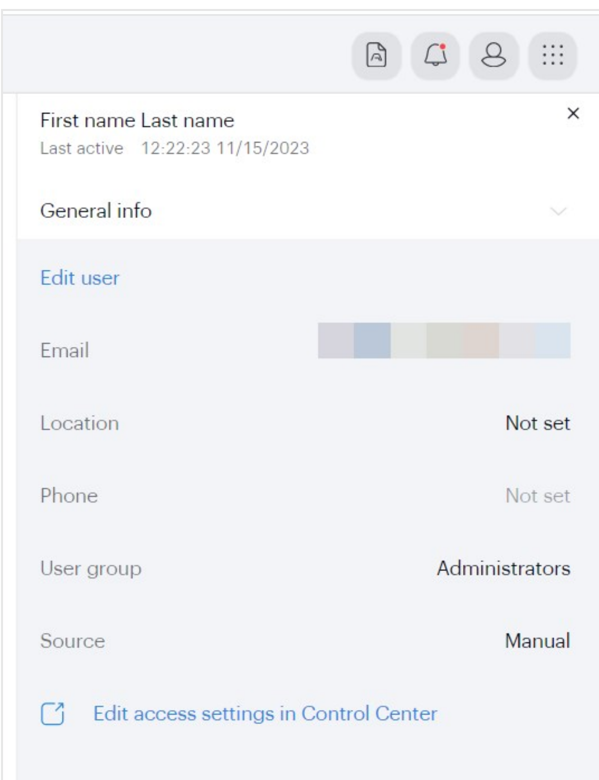
- In Alta Aware, select the app switcher button and then **Alta Access**.

  The Alta Access page is displayed on a new tab, already signed in.

- In Alta Access, click the **Edit user group in Aware** link (example is shown below) on the Edit user page or Entry dashboard page. Alta Aware is displayed on a new tab.



- In Alta Aware, click the **Edit access settings in Control Center** link for the selected user. Alta Access is displayed on a new tab.



Triggering lockdown plans

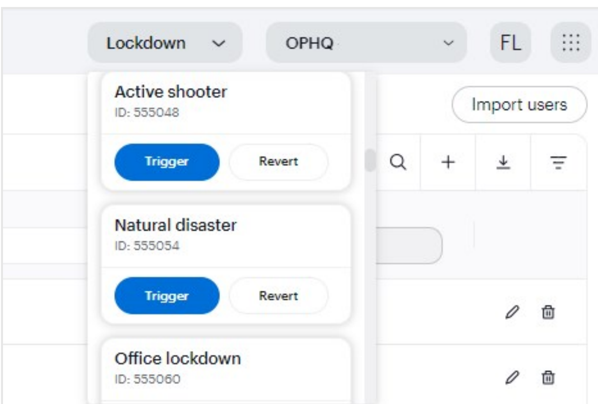
> **Note:** A Premium or Enterprise license is required. You must also have a Cloud Key credential to trigger and revert lockdown plans from Alta Access.

Lockdown plans for an organization can be triggered or reverted in any of the following ways. If you need to create a lockdown plan, see Lockdown plans (Premium and Enterprise plans) on page 82.

Use Alta Access menu bar

> **Note:** To view the Lockdown dropdown menu, users must be assigned the Lockdown - Override Only state. See Assign permission to override lockdowns on page 52.

1. Click **Lockdown** next to your organization and profile in the top-right corner.
2. When a lockdown situation occurs, click **Trigger** on the lockdown plan.

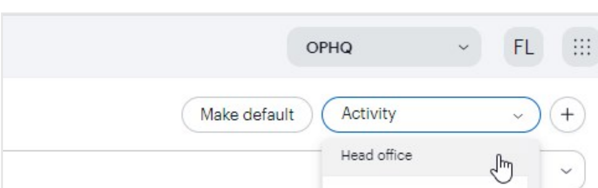


   If a lockdown plan is triggered, the Lockdown menu name changes to red.

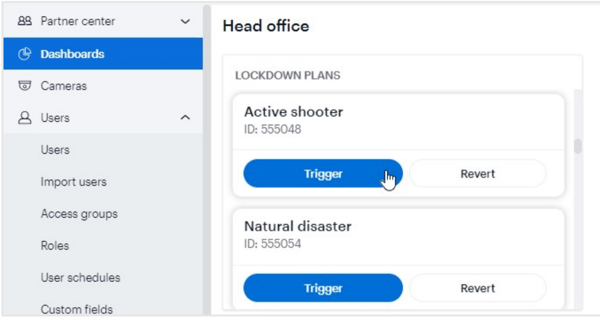
3. When the lockdown situation is resolved, click **Revert** on the lockdown plan. The lockdown plan is reverted and the red flag is removed.

Use Lockdown widget on custom dashboard

1. Go to the **Dashboards** page and select the custom dashboard in the upper-right corner.

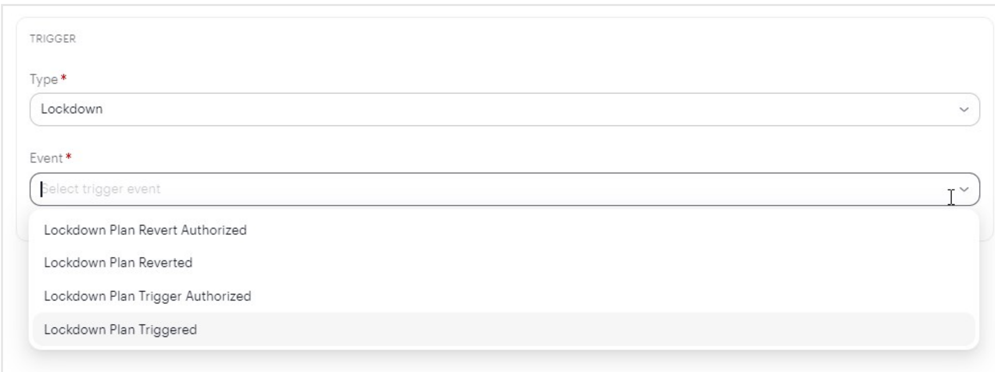


2. When a lockdown situation occurs, click **Trigger**, or when a lockdown situation is resolved, click **Revert**.



Use Lockdown event triggers

1. Go to the **Configurations** > **Alarms** or **Rules**.
2. Set up the lockdown trigger for the alarm or rule.



User profile

View and edit your profile as follows.

1. Go to 👤 in the upper-right corner of Alta Access.
2. Click **Profile**.

Update your account information

1. On the Info tab, edit your email and name.

   > **Note:** An account imported from an identity provider cannot be edited.

2. Select your preferred language in **Language**.
3. Click **Save**.

Change password

1. On the Password tab, enter your old and new passwords.
2. Click **Save**.

Add MFA devices

For extra security, add one or more multi-factor authentication (MFA) devices that can generate a passcode for two-step identity verification at time of login.

> **Note:** Before you start, ensure a Time-based One-Time Password (TOTP) compatible app is installed and configured on your device.

1. On the Security tab, click **Add MFA device**.
2. In **MFA device type**, select **TOTP soft device Google Authenticator, Authy, Duo or compatible)**.
3. Enter a name for the device and click **Next**. A QR code is generated.
4. Set up the app on your mobile or desktop device by scanning the QR code.

   If your device can't scan, click **(show secret)** to display the contents of the QR code. Go to your app and type the code.

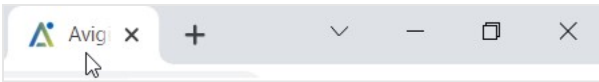
5. Enter the code generated by the app in the **Enter 2FA code** field.
6. Click **Activate MFA device**. The device is added.

Enable intercom notifications

1. On the Settings tab, select the **Enable intercom notifications** toggle to receive notifications from the Video Intercom Reader Pro.
2. Click **Save**.

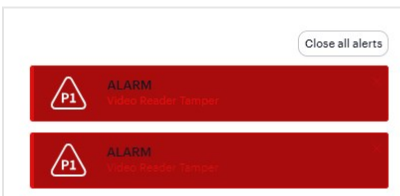
When enabled, the following is shown:

- A visual indicator (blue dot) in the browser tab indicates new notifications.



> **Tip:** This indicator helps notify you when you have Alta Access notifications even if you are viewing a different browser tab.

- The dot is removed when you click a notification or close all alerts in Alta Access.



Play or mute alarm notification sounds

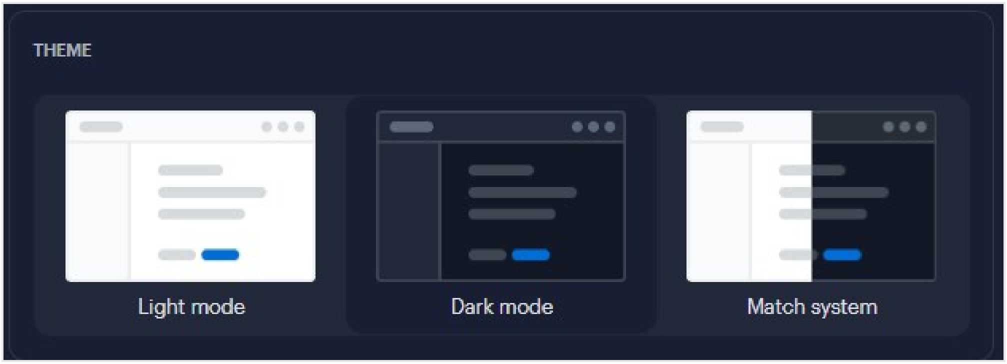
> **Note:** A Premium or Enterprise license is required. Ensure the audio on your device or machine is enabled when using the alarm notification sound.

On the Settings tab:

- To play the default sound when an alarm is generated, select the **Play alarm notification sounds** toggle (default).
- To mute the default sound, deselect the toggle and click **Save**.

Enable Dark mode, Light mode, or Match system theme

- On the Settings tab, select the **Dark mode** (shown below) or **Match system** theme, which uses the current theme of your operating system. **Light mode** is the default theme.



The selected theme is displayed every time you log in to Alta Access.

Dashboards

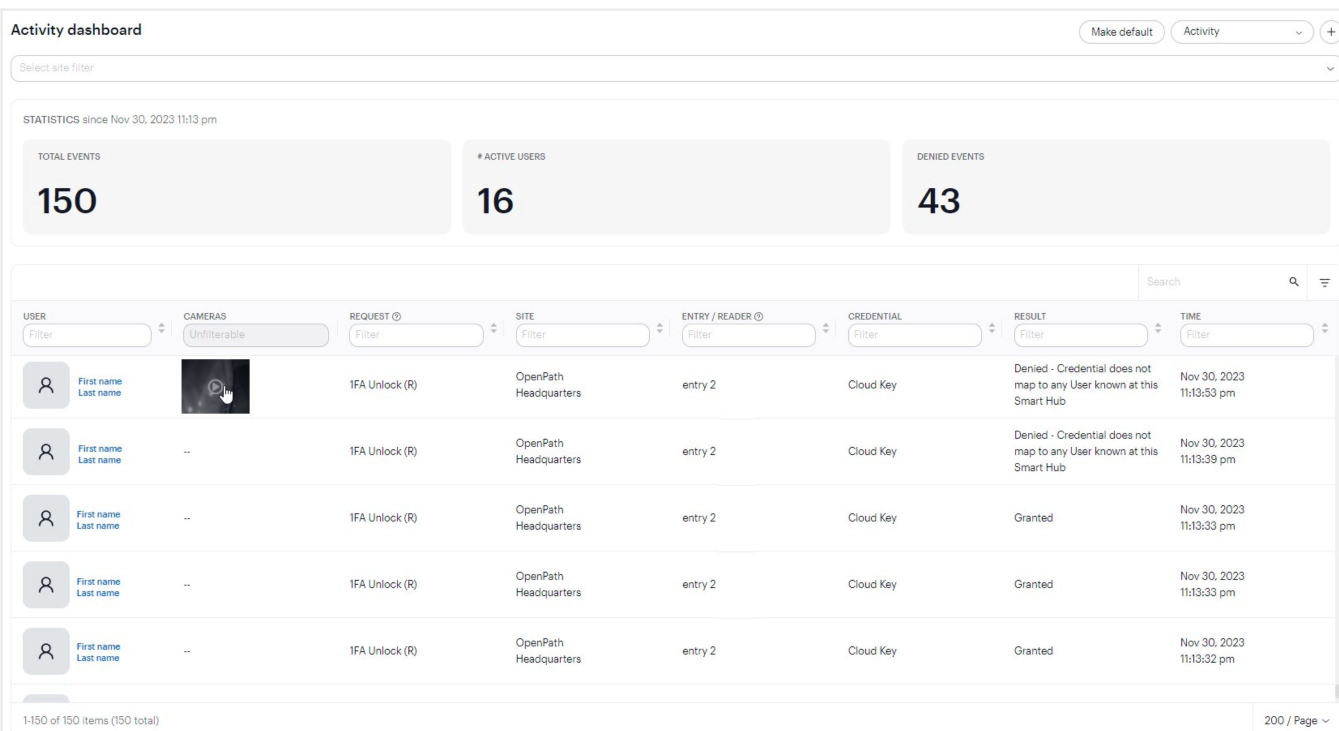
The Dashboards page lets you monitor access control events in the default Activity, Alarms, Device, and Entry dashboards, and to create custom dashboards for your org.

> **Note:** If you are viewing Schlage no-tour wireless locks, information may be out-of-date. Dashboard information is available only after visiting the no-tour wireless lock in person and completing a manual sync using the Alta Access mobile app.

Activity dashboard

After signing in, you'll see the Activity dashboard which shows a live feed of recent access events, as well as statistics about event activity and active users. Click the name of a user to view their details, including a user who is visiting from another site.

> **Note:** When the 1,000 event limit is reached in the dashboard, the events over the limit are cleared on an hourly basis. To view the cleared events, go to **Reports** > **Activity logs**.



Filter by site

- At the top of the Activity dashboard page, select a site to narrow down the list of event activity.

View camera snapshots

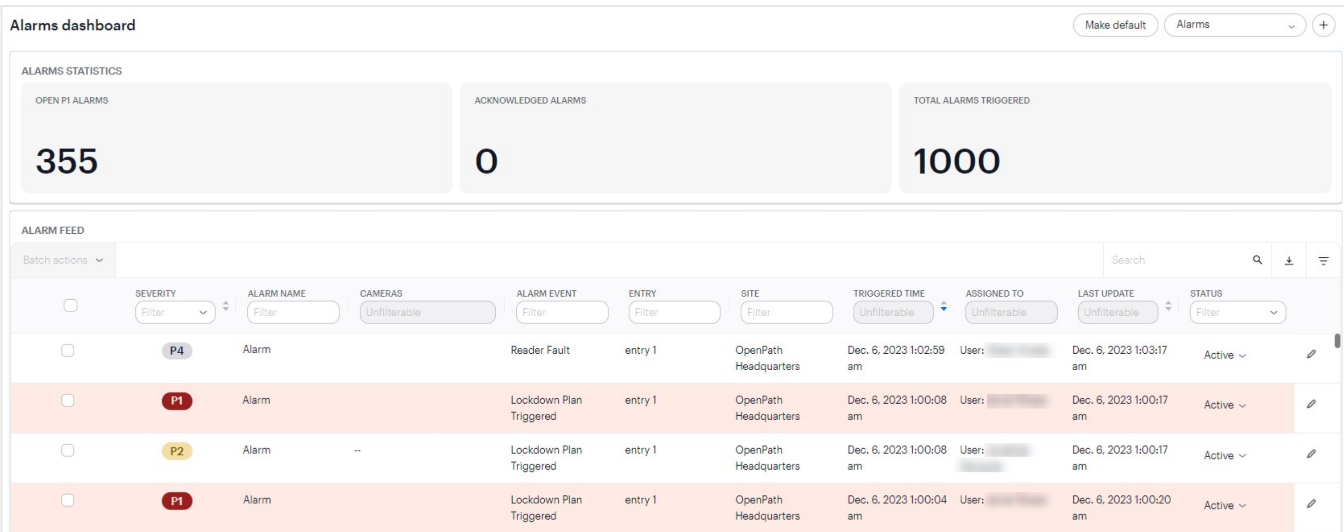
If you have the Avigilon Video Reader Pro or Video Intercom Reader Pro installed, or the Cisco® Meraki® or Alta Video camera integration enabled, you can view snapshots.

1. Go to the CAMERAS column in the Activity dashboard.
2. Click the ▷ play icon to view video footage in Alta Access or in the Meraki dashboard for the Cisco integration.

> **Note:** Video footage may take up to a minute to appear in Alta Access.

Alarms dashboard

The Alarms dashboard shows a live feed of alarm events and statistics for alarm monitoring operators and administrators.



Filter by alarm severity or status

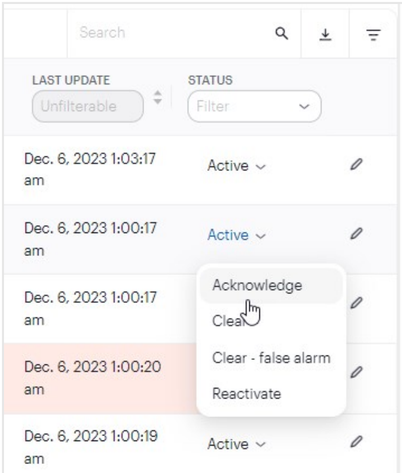
Go to Dashboards and change Activity to **Alarms** in the upper-right corner.

- Click the SEVERITY column in the alarm feed, and select a **P1** to **P5** level.
- Click the STATUS column in the alarm feed, and select the **Active**, **Acknowledged**, **Cleared**, **Cleared - False Alarm**, or **Auto Cleared** status.

Acknowledge, clear, or reactivate active alarms

Monitoring operators can respond to an Active alarm either in the Alarms dashboard or below the ALARM DETAILS section of the alarm page, depending if notes are needed.

- On the Alarms dashboard page, select an **Active** alarm in the STATUS column and an action.



> **Note:** Reactivate takes an alarm out of a cleared state, back to an active state.

- To view the alarm page, click the alarm row or **View alarm** in an open alarm notification in the lower-right corner.

  a. On the alarm page, read the **Instructions** for handling the alarm.

  b. Select the appropriate action in **Action**, and add a note.

  > **Note:** The alarm page includes the additional Add note action and Reassign action for reassigning the alarm to another monitoring user.

  c. Click **Save**.

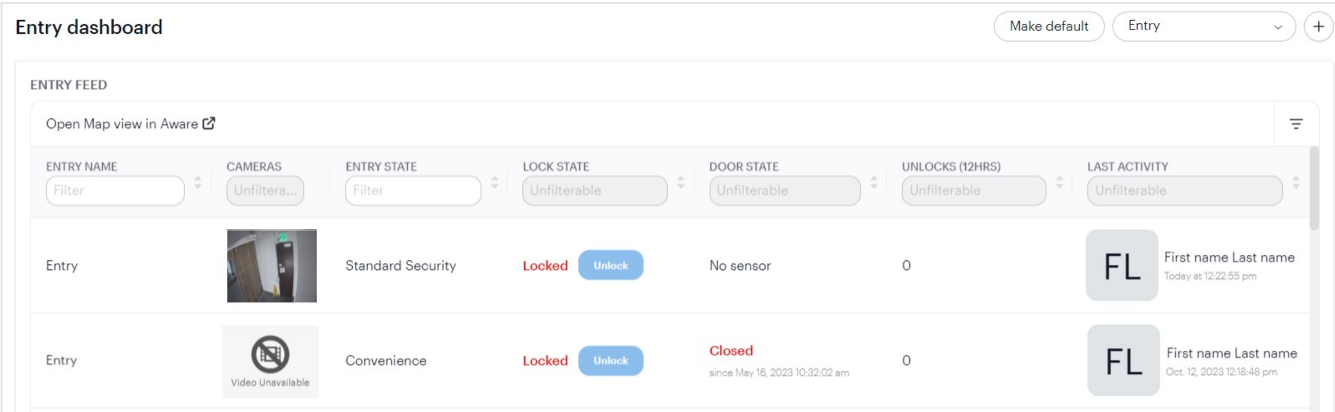
Export alarm history

In the HISTORY section of the alarm page:

- Click the icon.

Entry dashboard

The Entry dashboard shows the live status of every entry in your site, including users who are visiting from other sites.



View usage statistics of an organization

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.

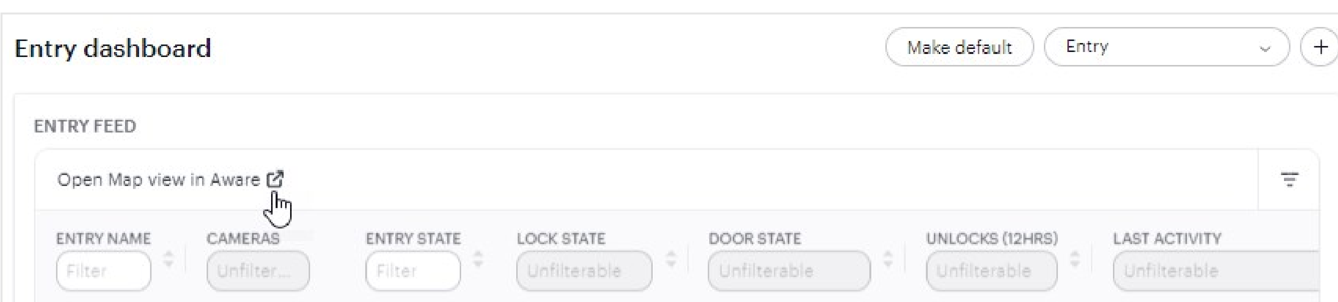
Unlock entries

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

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

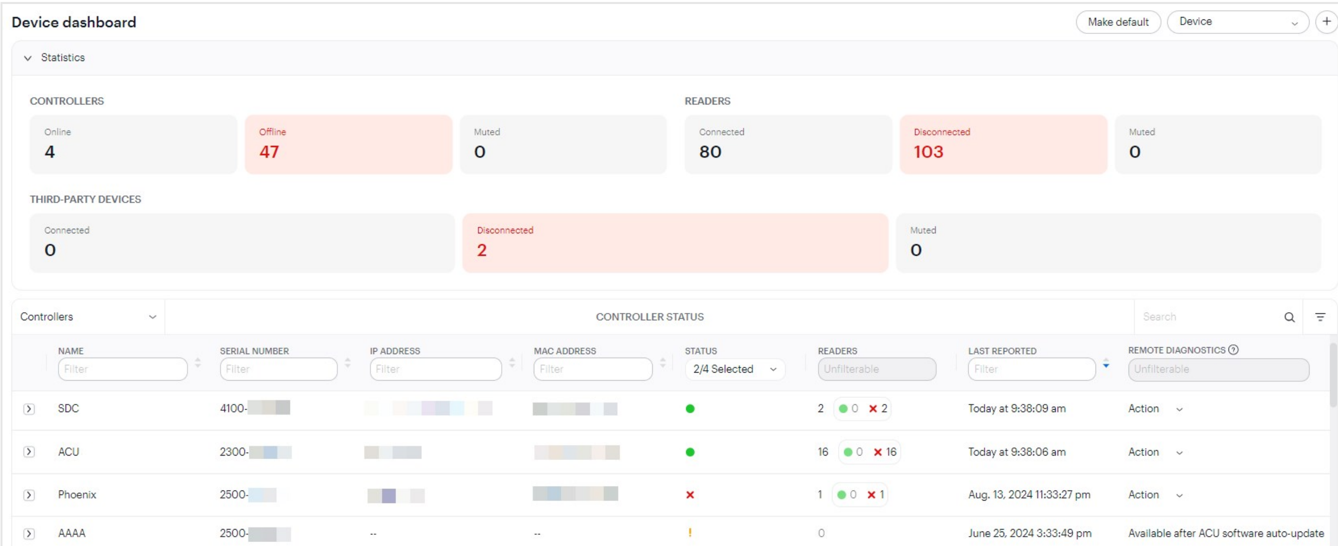
View entries on maps in Aware VMS

If Alta Video and Alta Access have been unified in your organization and you have the permissions in Alta Video to view maps, the **Open Map view in Aware** link will be visible (see below). Click to go directly to the Map view tool in Alta Aware. For more information, see Aware documentation.



Device dashboard

The Device dashboard is where you can get a high-level overview of the online status of your organization's controllers (ACUs and SDCs) and readers.

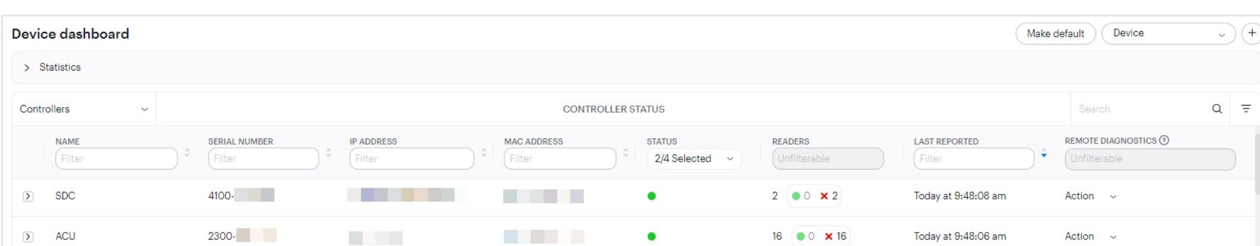


Color	Status	Description
	Connected	The controller or reader is online and communicating as expected.
	Disconnected	The controller or reader is offline. The last message received from the controller is more than 60 minutes old, or more than 20 minutes old, and the VPN is down.
!	Warning	The last message received from the controller is more than 12 minutes old, and the VPN is down.
	Muted	The controller or reader status is undetermined, or is muted in the Device dashboard.

For more information about the color-based state changes, see Device update management on page 116.

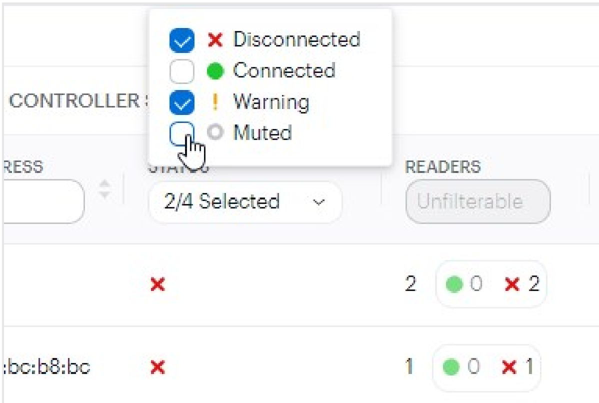
Collapse the Statistics card

- Click the **Statistics** arrow to make more room for your live feed.

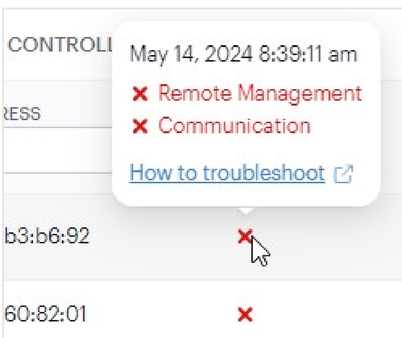


Filter controller status and view total number of readers

- In the STATUS column, select **Filter** and enter checkmarks to filter the controller results.
- In the READERS column, the total number of readers is displayed next to their online or offline status.

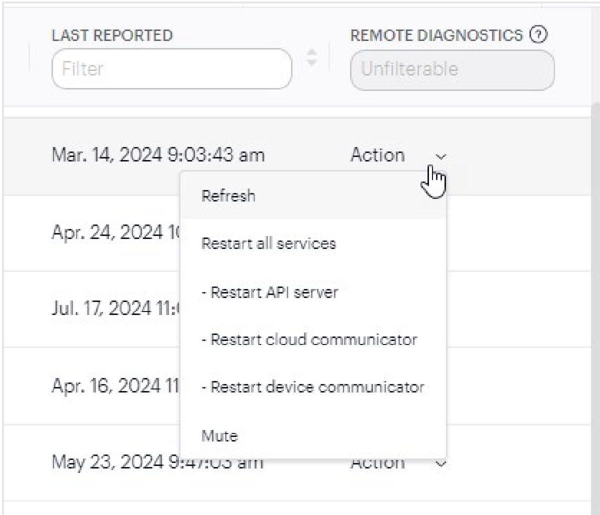


- Hover your mouse over the icon to view online troubleshooting information.



Refresh controller data

1. Select the controller in the dashboard.
2. Select **Action** > **Refresh** in the REMOTE DIAGNOSTICS column.



The latest data is sent from the physical device to Alta Access to ensure that the device is online.

Restart controller services

> **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.

1. Select the controller in the dashboard.
2. Select **Action** and a restart option in the REMOTE DIAGNOSTICS column.
   - **Restart all services** — Restarts all services on the controller.
   - **Restart API server** — Restarts the core application that processes authorization, authentication, and execution of unlock requests.

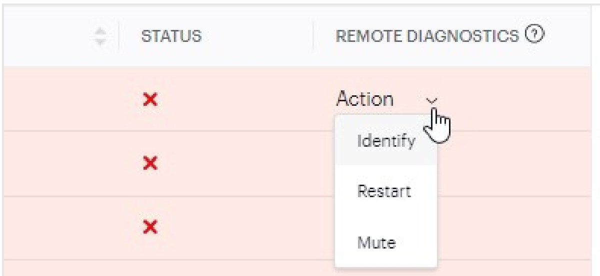
     Restart this service if issues occur with the Alta Open mobile app, such as unlock requests not working.
   - **Restart cloud communicator** — Restarts the service that receives live messages from the cloud, including entry configuration changes, user permissions changes, and cloud-based unlock requests.

     Restart this service if changes, such as new credentials and new schedule, in Alta Access aren't syncing with the controllers, or if issues occur with remote unlock requests.
   - **Restart device communicator** — Restarts the service that sends and receives data between the controller and peripheral hardware.

     Restart this service if issues occur with readers or expansion boards.
3. Click **Yes**.

Verify the physical reader is connected to Alta Access

1. Select the controller in the dashboard.
2. Select the reader from the list.
3. Select **Action** > **Identify** in the REMOTE DIAGNOSTICS column.



- The outer ring LED on the physical reader will light up.
- The center dot on the physical reader will light up green.
- The buzzer on the physical reader will beep several times.

Restart the reader

1. Select the reader in the dashboard.
2. Select **Action** > **Restart** to force a reboot.

   This will interrupt services provided by the reader for up to 60 seconds.

Mute the controller or reader

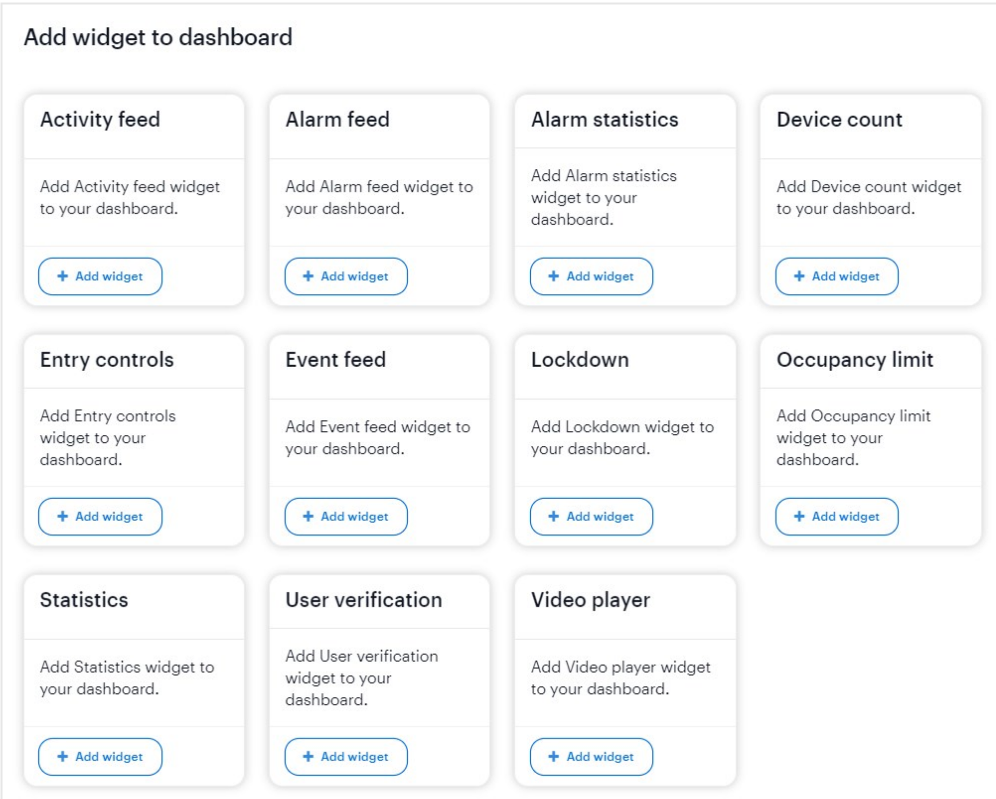
1. Select the controller or reader in the dashboard.
2. Select **Action** > **Mute** in the REMOTE DIAGNOSTICS column.

   The status changes to a gray circle. Any alerts or rules created for the controller or the reader will not be impacted. The device is muted only on your browser.

Custom dashboards (Premium and Enterprise plans)

You can create custom dashboards by adding widgets for use in your organization in addition to the Alta Access default dashboards (Activity, Alarm, Device, and Entry).

Note: Your dashboard can be viewed and edited by all Super Admin users in your organization.



Create custom dashboards

1. Go to the **Dashboards** page.
2. Click the + button in the upper-right corner.
3. Enter a name for the dashboard and click **Save**.
4. Click **Add your first widget** in the tool tip and choose a widget.
    - **Activity feed** — A live feed of the entry activity log.
    - **Alarm feed** — A live feed of all alarm events. A Premium or Enterprise license is required.

- **Alarm statistics** — The open alarms, open P1 alarms, acknowledged alarms, and total alarms triggered. A Premium or Enterprise license is required.
- **Device count** — The number of controllers and readers configured in the system and their online status.
- **Entry controls** — Lets you pin one or more entries to the dashboard and temporarily unlock them instantly, or keep them unlocked for 5, 10, 15, or 60 minutes.

  You need a Cloud Key credential[*] and appropriate access to one or more entries in order to trigger unlocks.
- **Event feed** — A live feed of entry events, door ajar and door propped open alarms, and lockdown activations.
- **Lockdown** — A list of all lockdown plans in the organization with buttons to trigger and revert plans. A Premium or Enterprise license is required.

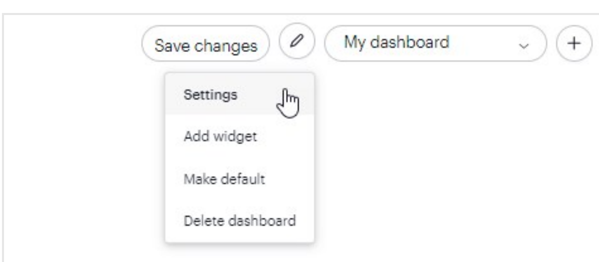
  You need user permission to trigger and revert lockdown plans. For more information, see Assign permission to override lockdowns on page 52 and Assign users and group permissions for lockdown plans on page 83.
- **Occupancy limit** — The occupancy of areas configured using anti-passback.

  You need to configure anti-passback and set occupancy limits to use this widget. For more information, see Anti-passback and occupancy management on page 69.
- **Statistics** — The total events, number of active users, and percentage of active users from the last 12 hours.
- **User verification** — Lets you monitor access events at a particular entry and displays a user's photo when they unlock an entry.
- **Video player** — A live feed of the selected video reader.

5. Click **Save changes**. The widget is added to your new dashboard.

Edit custom dashboards

- Click the edit button in the upper-right corner for the customization options.



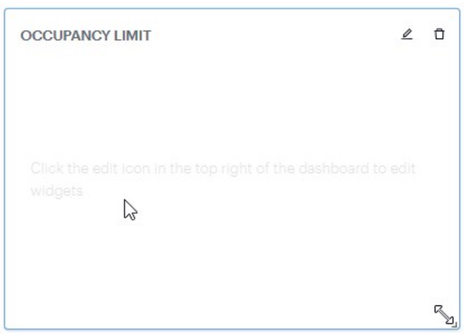
[*] For more information, refer to https://help.openpath.com/what-are-cloud-key-credentials-and-how-do-i-send-guest-access-links-HJ3crp38_.

Update dashboard title

1. Select **Settings** from the menu.
2. Update the **Dashboard title** and click **Save**.

Add more widgets

1. Select **Add widget** from the edit menu.
2. Choose a widget and do any of the following:
   - Click the icon to flip over the widget and see more configuration options.
   - Click in the upper-right corner to delete the widget.
   - Click and drag to place the widget anywhere on the dashboard.
   - Resize the widget by clicking and dragging the lower-right corner.



3. Click **Save changes** when you're done customizing the dashboard.

   The custom dashboard appears in the Dashboards menu in the upper-right corner.

Set dashboard as default

- Select **Make default** from the edit menu.

  The custom dashboard appears at the top of the Dashboards dropdown menu in the upper-right corner.

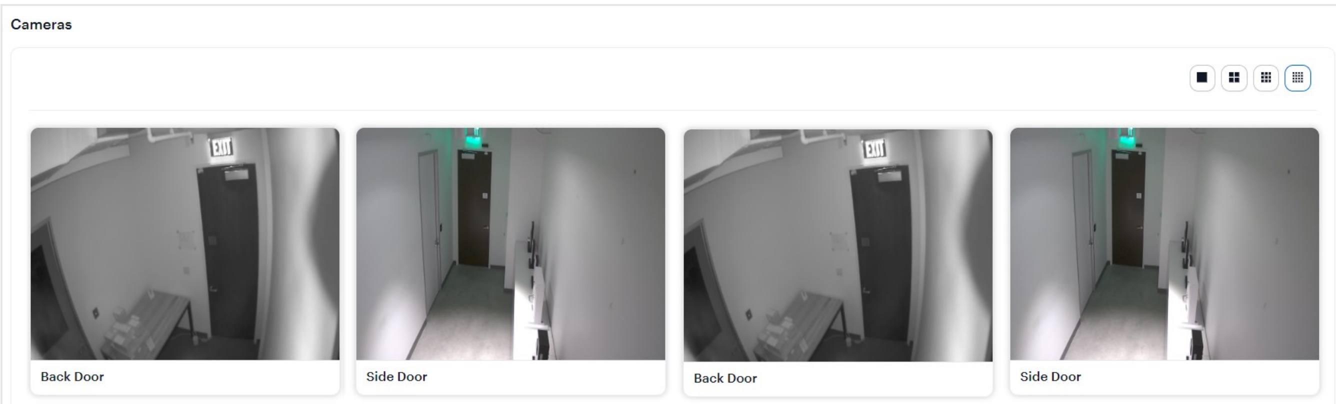
Delete dashboard

- Select **Delete dashboard** from the edit menu.

Cameras

The Cameras page shows all cameras in your org, including the cameras connected through your Alta Video account, Video Reader Pro and Video Intercom Reader Pro devices, and Cisco Meraki cameras.

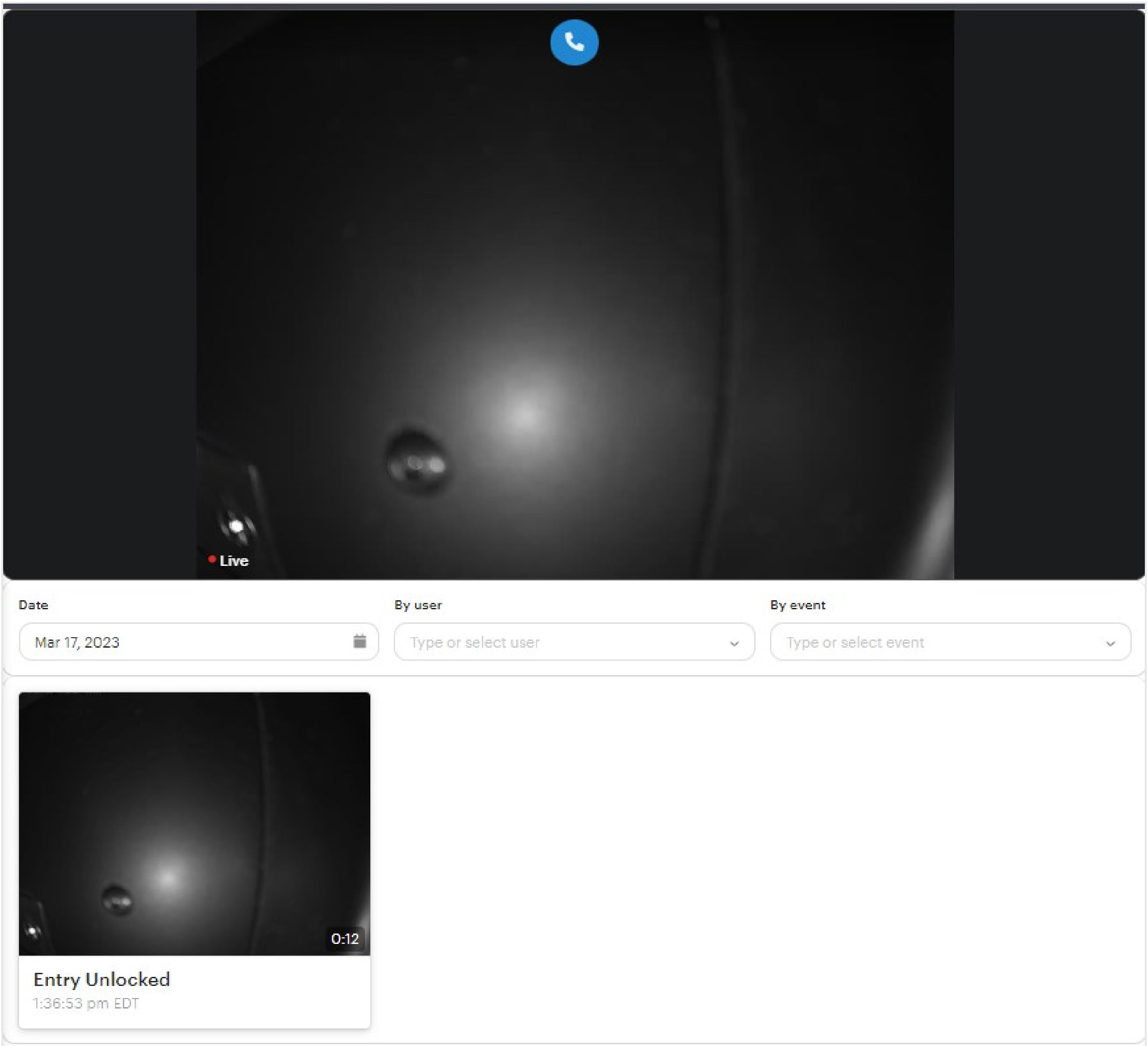
- Click a camera, video reader, or video intercom reader to view a live feed and list of events, such as door unlocks, audio and motion detection, and tamper detection.
- Initiate a call to the video intercom reader using the built-in microphone and speaker on your desktop or the Alta Open mobile app.
- Click a Cisco Meraki camera to go to the Cisco Meraki dashboard.



View live video feeds

- Go to **Cameras** and select a camera.

  A live video feed is shown at the top.



Initiate calls to intercom on Video Intercom Reader Pro

- Click the  phone button on the live video feed.

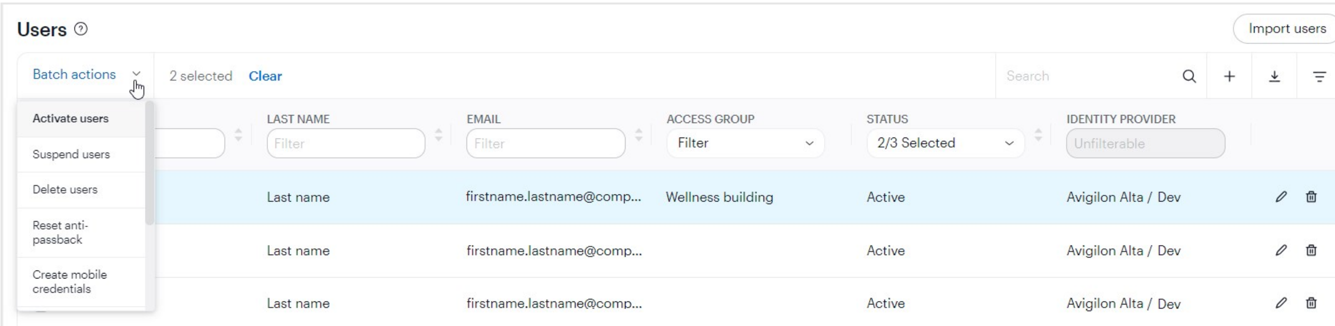
> **Note:** Calls are not supported in Safari and Firefox browsers. Users can also click the phone button on the live feed in the Alta Open mobile app.

Play and download video

1. Play a recording and click the button in the upper-right corner.
2. Find the MP4 file in the Downloads folder on your desktop.

Users

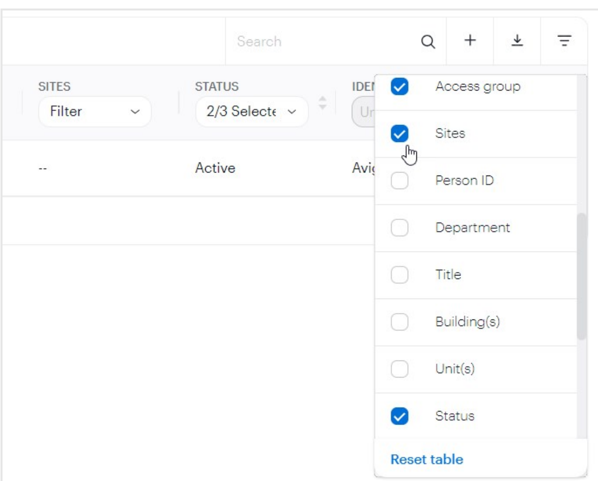
The Users page lets you manage and import users, assign them to sites, create and define groups, credentials, and roles.



Show, hide, or reset information

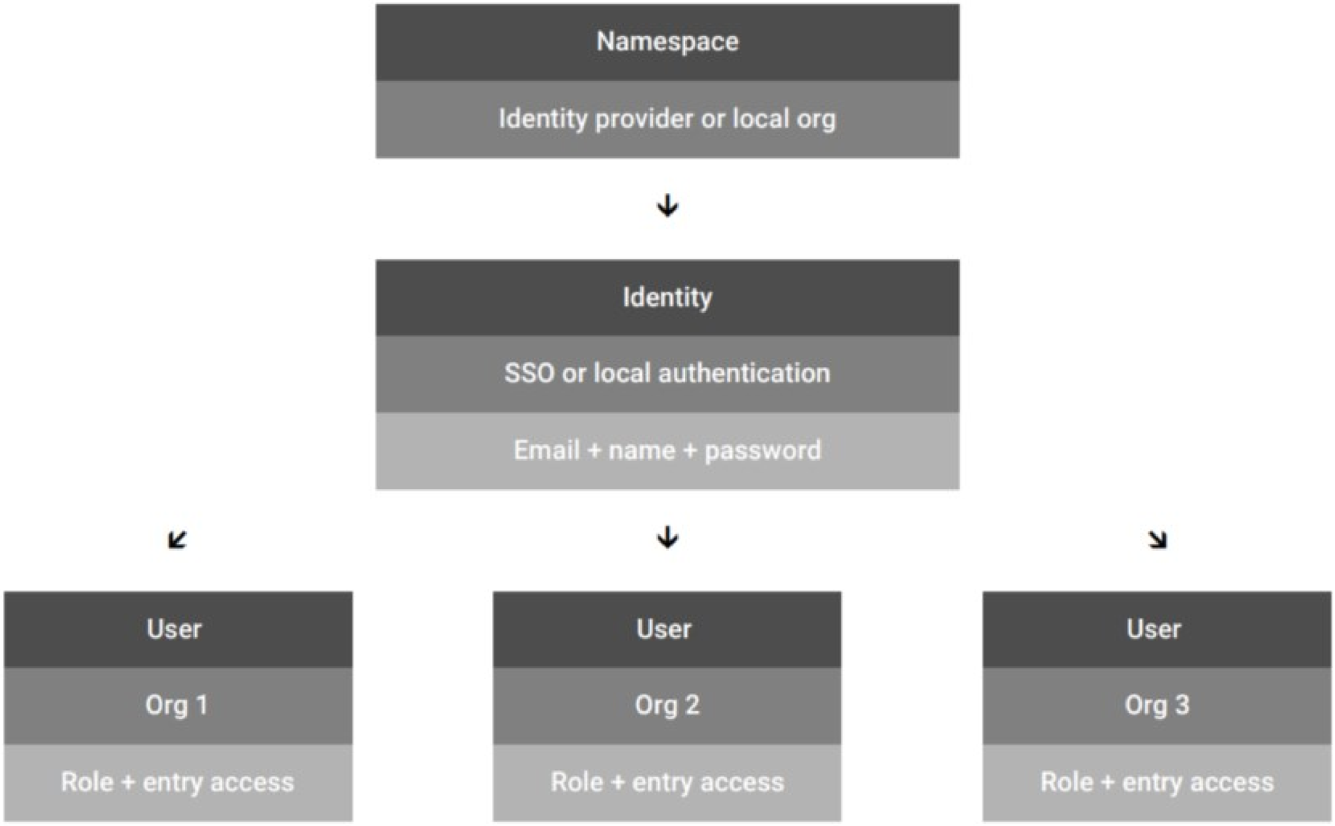
- Click the icon to show or hide information in columns.
- Click **Reset table** to go back to the default view.

For example, show the Sites column.



User data model

If you have access to more than one organization (org) in Alta Access, or you are using multiple identity provider integrations with SSO enabled, you should be familiar with the Alta Access user data model. This model allows a single identity to access multiple orgs, which is useful for resellers and installers that need to log in once but have access to many orgs.



Data	Description
Namespace	A contained pool of emails, all of which must be unique within the namespace. The two types of namespaces are identity provider and local org. Namespaces allow the flexibility of having multiple instances of the same email that come from different sources or have different authentication mechanisms, such as 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), another identity will be created under the identity provider namespace.
Identity	The data record of a person needing access to Alta Access, including email, first name, last name, and other information. An identity is separate from, but related to a user. Identities are authenticated when signing in to Alta Access. For the supported identity provider integrations, see Identity management on page 123.
User	An instance of an identity that belongs to a specific org. A single identity could have multiple users. User configurations include portal access, roles, and entry access for a particular org. **Note:** You can view the users who are visiting your site from other sites and contact them, but you cannot manage their entry access. For example, a visitor might need to be notified of a muster event occurring at your site.

User management

Tip: You can choose to perform user management using the Alta Access mobile app.

For more information, see this Alta Access article.

App Store® and the Apple logo® are trademarks of Apple Inc. Google Play and the Google Play logo are trademarks of Google LLC.

Add users

1. Go to **Users** > **Users**.

   Tip: Select the Quick actions icon to use the Add user shortcut.

2. Click the + button in the upper-right corner.
3. Enter the user's email, name, and mobile phone number.

   Note: If the email matches a deleted user, that user will be reactivated with all the permissions and credentials they had before deletion.

   Note: If the user belongs to another organization, you can skip the name and enter a checkmark in the **Add a user from an existing namespace** box and the namespace in **Namespace**. For more information about namespaces, see User data model on page 42.

4. Enter other fields, as needed.
   - **Start date/time**, **End date/time**, and **Timezone**.
   - **Person ID**, **External ID** — For employee IDs or other useful info]rmation.
   - **CUSTOM FIELDS** — Additional fields that are configured, such as **License plate number**.
   - **Site associations** — Physical locations, such as office buildings. This setting ensures administrators can only manage users who are assigned to their site. Users not assigned to a site can be managed by all administrators. A Premium or Enterprise license is required.

Note: You can view the users who are visiting your site from other sites and contact them, but you cannot manage their entry access. For example, a visitor might need to be notified of a muster event occurring at your site.

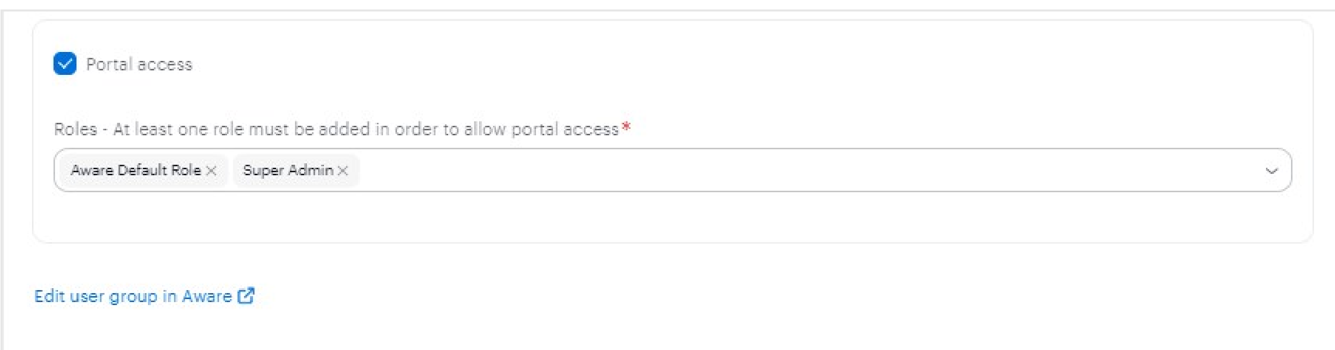
User activity at a site can be viewed in specific dashboards, reports, rule filtering, and alarm event triggers and filtering. For more information, see Dashboards on page 29, Reports on page 119, Add rules and triggers on page 146, and Event triggers and advanced filtering on page 152.

- **Portal access** — For a user who is an administrator and requires access to the Alta Access portal, add the **Super Admin** role. For the default roles that are assigned automatically by the system, see Role management on page 55.

  Note: Only give administrator portal access to users who require it, such as an office manager or security guard. To give someone limited access to Alta Access, create a role with granular permissions, as described in Assign permissions to roles on page 57.

5. Click **Save**. A unique User ID is assigned, which may be used in search filters.
6. Optional. See Upload photo below.

Note: If Alta Video and Alta Access have been unified in your organization and you have the permissions in Alta Video to view users, the **Edit user group in Aware** link will be visible. Click to go directly to the Users list in Alta Aware on a new browser tab.



Upload photo

To upload the user's photo to Alta Access and the user's Alta Open mobile app:

1. Hover your mouse over the photo tile on the user's page and click **EDIT**.
2. Click the **+ Add photo** button.
   - To take a new photo using your device's built-in camera or webcam, click **Use camera** and then **Take photo**. Click **Save photo**.

- To upload a new photo, click **Upload photo** and upload the photo. Click **Save photo**.

Issue keycard, fob, license plate, mobile, PIN, wiegand, or cloud-based credentials

You can issue credentials to a user. A credential is a keycard or fob presented to a reader to gain access to an entry.

> **Note:** The EV3-B MIFARE® DESFire® cards can support a broader set of devices than the EV3-A DESFire cards. If your org is planning to continue using EV3-A DESFire cards or to migrate to EV3-B cards, see this Alta Access article for the steps to maintaining backward and forward compatibility with your devices and readers.
>
> For information about issuing credentials to Schlage no-tour wireless locks, see the Avigilon Access Control System Integration Guide for Schlage Wireless Locks No-Tour (link).

1. Select a user on the page, and click the **Credentials** tab.

   > **Tip:** Select the Quick actions icon to use the Edit user shortcut.

2. Select the type of credential to access an entry, depending on your device.

   > **Note:** If the Embedded USB Smart Reader is installed as an enrollment device, it supports only Avigilon MIFARE and DESFire card credentials.

   - **Card: Openpath DESFire (Encrypted) - Secure** — An Avigilon (formerly Openpath) high-frequency (HF) EV3 card or fob.

     > **Tip:** The user may need to hold the card or fob on the reader a little longer than the CSN option.

   - **Card: Openpath/MIFARE (CSN) - Fast** — The Card Serial Number of an Avigilon HF card or fob.
   - **Card: Schlage** — A Schlage card or fob for Allegion Schlage wireless devices.

- **Card: Wiegand ID** — An Avigilon low-frequency key fob or card for Wiegand-based access control systems. If you choose this option, see Add Wiegand credentials on page 49 after saving.
- **Cloud Key - For Guest Passes, Portal Dashboards, API Integrations** — A web link issued by the Alta Open mobile app or Alta Access to grant temporary or scheduled access to an entry. If you choose this option, see Generate guest access links and webhook URLs on page 49.
- **License Plate** — If you choose this option, see Add or edit license plate credentials on the next page.
- **Mobile** — The Alta Open mobile app used to access an entry. If you choose this option, see Add mobile credentials on the next page after saving.
- **PIN** — A PIN on the keypad of an Avigilon Smart Reader v2. If you choose this option, see Add or edit PIN credentials below.

3. Enter the required information depending on the device.
4. Click **Save**.

Add or edit PIN credentials

The supported PIN length is 4 to 16 digits for custom and auto-generated PINs.

> **Tip:** If PIN masking (hiding) is enabled in your organization (see the Enable PIN masking setting in Edit security settings on page 164), make a note of the PIN before saving the credential.

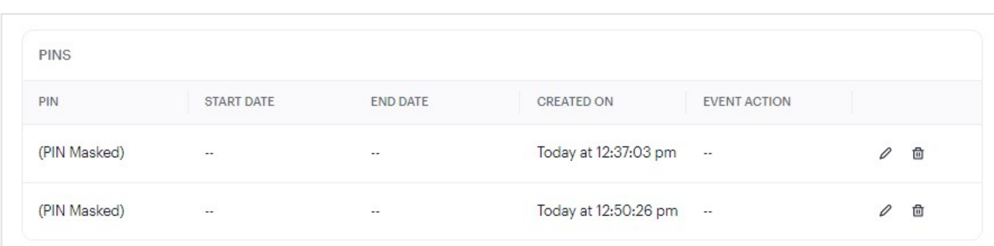
To choose your PIN:

1. Select **Custom PIN**, enter a unique PIN.
2. Optional. Enter details such as start/end dates and a lockdown plan.
3. Click **Save**.

To create an auto-generated PIN:

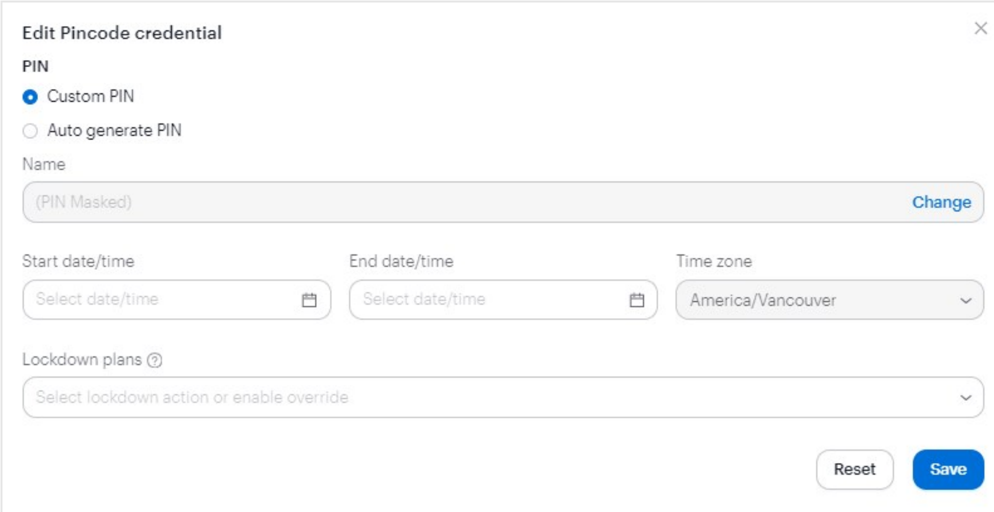
1. Select **Auto generate PIN**, click **Auto generate**.
2. Optional. Enter details such as start/end dates and a lockdown plan.
3. Click **Save**.

A masked PIN is displayed as **(PIN Masked)**.


PINS

PIN	START DATE	END DATE	CREATED ON	EVENT ACTION
(PIN Masked)	--	--	Today at 12:37:03 pm	--
(PIN Masked)	--	--	Today at 12:50:26 pm	--

To edit a PIN credential:



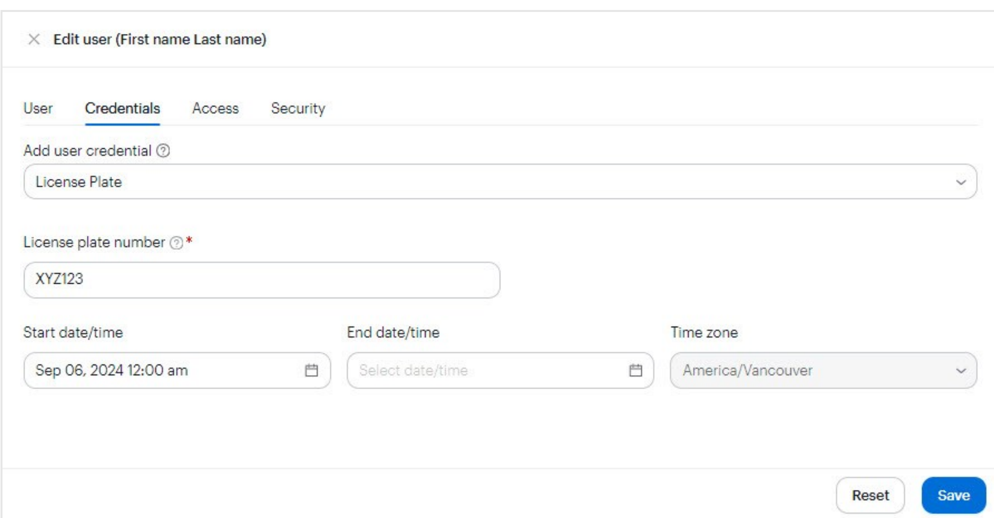
1. Click the icon and then **Change**.
2. For a Custom PIN, enter another unique PIN.

   For an Auto generate PIN, click the **Auto generate** button.
3. Optional. Select start/end dates and a lockdown plan.
4. Click **Save**.

Add or edit license plate credentials

> **Note:** Before you start, ensure the Alta Video setting is configured for the entry, as described in Additional device (control) settings on page 76.

When adding or editing a license plate number, do not use spaces, dashes, or special characters:



Add mobile credentials

After saving a mobile credential:

- Click **Send** to email instructions to the user 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.

  Click **Resend** to issue another mobile credential to a new mobile device.

Add Wiegand credentials

After saving a Wiegand credential:

- For Avigilon LF cards, select **Prox 26-bit (H10301)** in **Card format**.
- If you don't know the card format, select **Raw 64-bit** in **Card format** and enter the **Card number**.

  > **Note:** If you don't know the card number, you can swipe the card at the reader and take note of the rejected access entry in **Reports** > **Activity logs**. The card number will be displayed in the CREDENTIAL DETAIL column.

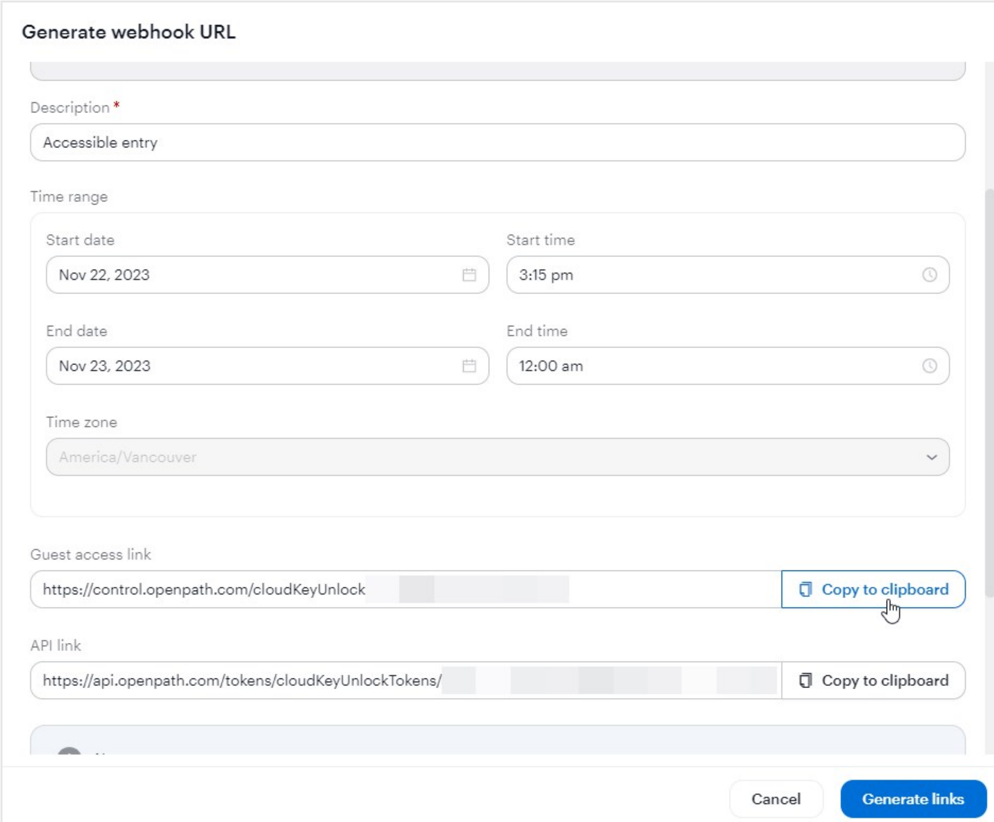
- To send card credential data to a third-party control panel, set **Use for Gateway** to **Enabled**. You must also configure the Wiegand reader to enable this feature. See Edit entries on page 73.

Generate guest access links and webhook URLs

After saving a Cloud Key credential on the Credentials tab:

1. In the CLOUD KEY CREDENTIALS list, click **Get webhook URL** next to the credential.
   - The URL can be used to unlock entries through a web browser and shared with a guest.
   - The URL can be integrated into the software or external services.
2. In the window pop-up, select the entries the URL will unlock:
   - **Entries** (for example, front entry, rear entry)
   - **Description**
   - **Start time** and **End time** (optional)
3. Click **Generate links**.
   - For a **Guest access link** , click **Copy to clipboard** and share the URL with the guest.
   - For an **API link**, click **Copy to clipboard** and use the URL in your own software or external service.

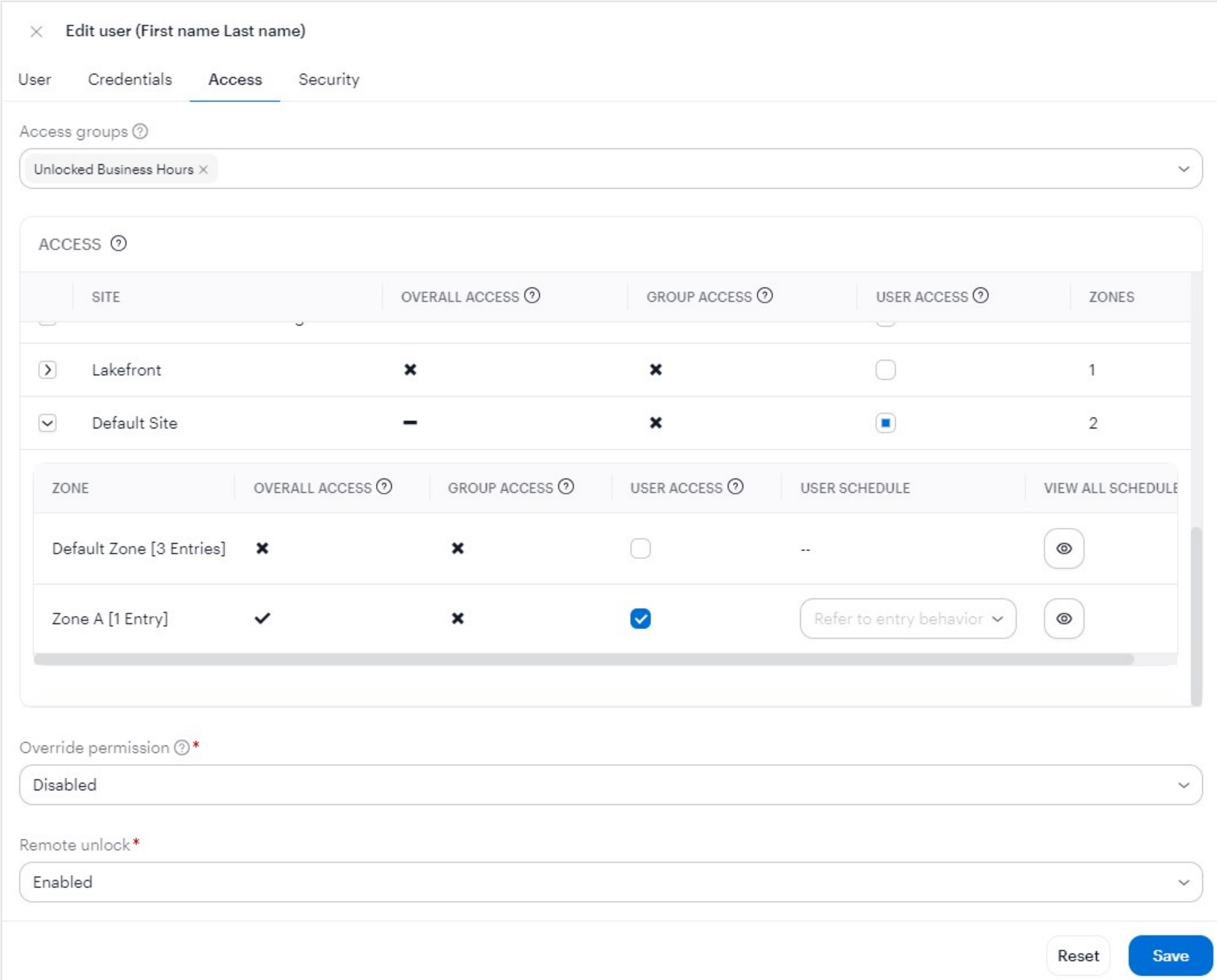
> **Note:** A Cloud Key credential can have multiple webhooks for multiple entries associated with it. Deleting a Cloud Key credential will also remove all the valid webhooks associated with it.



Edit user access

You can assign groups, sites, and zones, and enable permission override and remote unlocking for a user.

Tip: Select the Quick actions icon to use the Edit user shortcut.



Assign access groups, sites, zones, and schedules

1. Select a user on the page, and click the **Access** tab.
2. In **Access groups**, add the user to one or more access groups to give them access to the zones predefined for those groups.

   If you need to add an access group, see Create access groups on page 54.

3. In the grid below, add the user to specific sites and zones by entering checkmarks.
   a. In the SITE column, click a site to view the related zones.
   b. In the USER ACCESS column, click to add a user to a schedule.
   c. In the USER SCHEDULE column, select a predefined user schedule.

If you need to add a user schedule, see User schedules on page 59.

d. In the VIEW ALL SCHEDULES column, click to view all schedules that you've assigned.

4. Click **Save**.

Assign permission to override lockdowns

1. Select a user on the page, and click the **Access** tab.
2. Enable **Override permission** to give the user permission to unlock entries in the Lockdown - Override Only state.
3. Click **Save**.

Assign permission to remote unlock using Avigilon Alta Open mobile app

1. Select a user on the page, and click the **Access** tab.

   > **Tip:** Select the Quick actions icon to use the Unlock entry shortcut.

2. Enable **Remote unlock** to let the user unlock a door remotely using the Avigilon Alta Open mobile app.

   > **Note:** This feature is not applicable to Schlage no-tour wireless locks.

3. Click **Save**.

View MFA credentials

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 User profile on page 26.

Delete users

> **Note:** You can only delete users in your site. Users from other sites cannot be deleted unless you are a Super Admin.

1. Select the user on the Users page.
2. Click the icon.
3. Click **Yes**. The user's access is deleted.

> **Note:** Deleted users are kept in the system for reporting and record-keeping purposes. To find a deleted user, go to the Users page and select Deleted from the STATUS column.

Import users by CSV file

You can import and update users by uploading a CSV file. To import users by using a directory service integration, see App marketplace on page 123.

1. Go to **Users** > **Import users**.

   Or, click the **Import users** button in the upper-right corner of the Users page.

2. Create the CSV file in one of the following ways:

   - Click **Download sample CSV** and fill out all required fields in the supported formats. Save the file as a CSV file (for example, `mycompany-bulk-import-users.csv`). Excel file extensions do not work.

   - Click the **Export to CSV** icon in the upper-right corner of the Users page, and modify the downloaded file.

   > **Tip:** Refer to the **Valid fields** tooltip for the supported values.

3. Click the **Select CSV** button and locate the file.

4. Select your **Namespace**:

   - **Local** — For adding new users or updating existing ones, and if you are not using an identity provider. Choose to **Skip** existing users or **Update** them in the **How to handle existing users** field.

   - **Google Workspace**, **Microsoft Azure AD**, **Okta**, or **OneLogin** — For updating existing users you previously synced with Alta Access. New users will not be added.

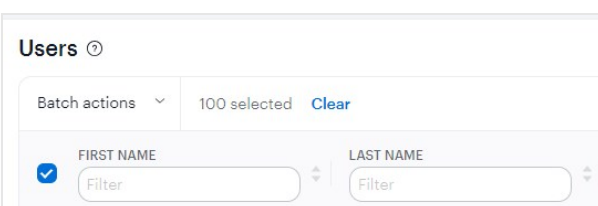
5. Click the **Upload file** button.

   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.

Issue batch actions to users

1. Go to **Users** > **Users**.

2. Enter a checkmark next to one or more users.



3. In **Batch actions** (activated by the previous step), issue any of the following actions to the selected users:

   - **Activate users** — Reactivates a suspended user.

   - **Suspend users** — Disables credential use and admin portal access, if granted to the user.

- **Delete users** — Revokes access from the user and keeps the user in the system for reporting and record-keeping purposes.
- **Reset anti-passback** — Resets the anti-passback state of a user, if using anti-passback. See Anti-passback and occupancy management on page 69.
- **Create mobile credentials** — Automatically creates mobile credentials for the selected users.
- **Send mobile credentials** — Sends mobile setup emails to the selected users. If a user has multiple mobile credentials, they'll receive multiple setup emails.
- **Disable remote unlock** — Disables the remote unlock permissions for the selected users.
- **Enable remote unlock** — Enables the remote unlock permissions for the selected users.

  Note: This feature is not applicable to Schlage no-tour wireless locks.

Access groups management

The Access groups page is where you can create and manage groups of users. Groups let you assign access and entry permissions for one or more users, and are useful for organizing your user base by department or role.

Create access groups

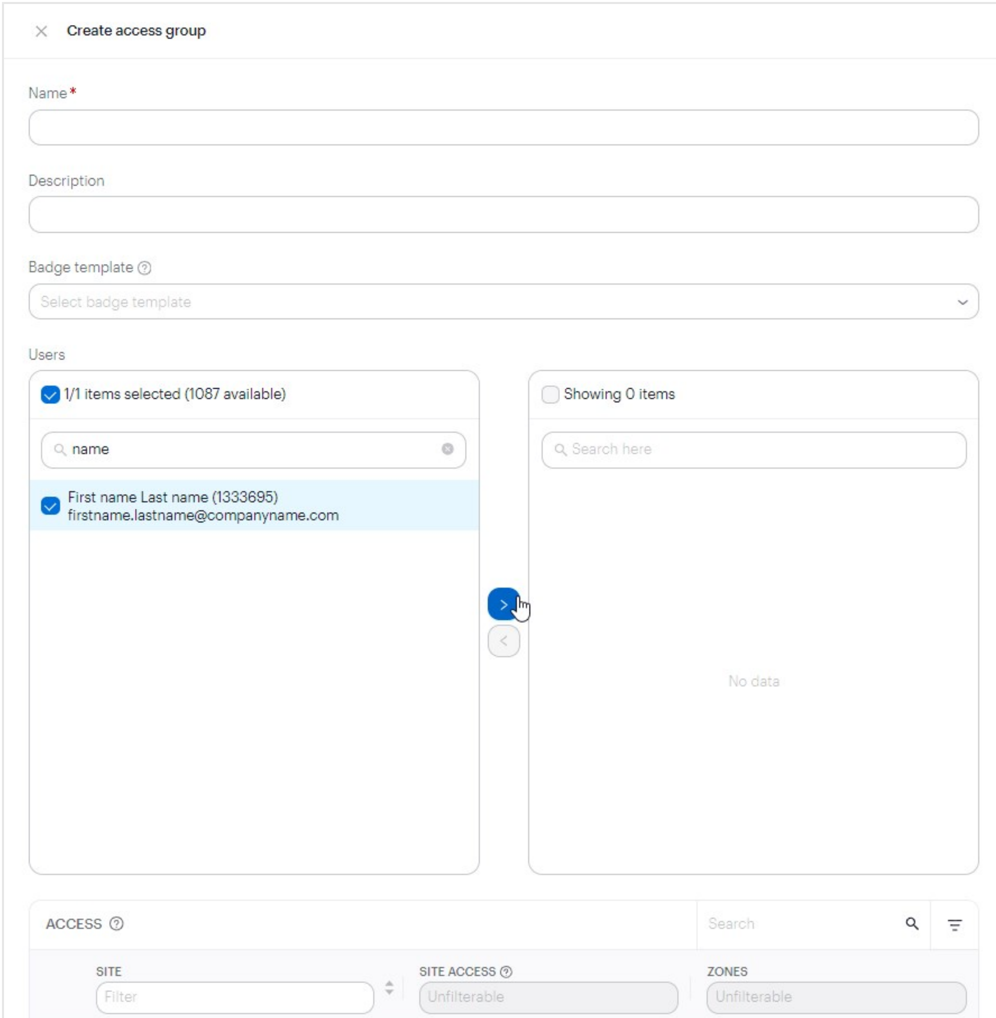
1. Go to **Users** > **Access groups**.
2. Click the + button in the upper-right corner.
3. Enter a name, description, and badge template.

   Note: The Badge template field appears only if the Badge Printing app is installed.

4. Assign users to the access group using the > button.
5. Select the sites and/or zones the access group will have access to.

   Note: You can view the users who are visiting your site from other sites and contact them, but you cannot manage their entry access. For example, a visitor might need to be notified of a muster event occurring at your site.

6. Click **Save**.



Role management

A role is a set of portal access permissions that can be assigned to users in an organization. The following default roles cannot be edited:

- **Dashboard (Read-Only)** — Gives dashboard access with read permissions.
- **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.

- **Super Admin Read-Only** — Gives full portal access with read permissions.
- **MFA enforced Super Admin** — Gives full portal access with edit permissions for users who use MFA.

- **MFA enforced Super Admin Read-Only** — Gives full portal access with read permissions for users who use MFA.
- **Aware Default Role** — Gives Alta Aware Operator users read permissions to the Activity dashboard. Users are created automatically with this role when they are added to the Administrators group in Alta Video. (Aware Operator users will need to check their inbox for an invite from Alta Access to set up a password for their new Alta Access accounts.)

  > **Note:** If Alta Video and Alta Access have been unified in your organization, the Alta Access password must be used to sign in. The Alta Video password is no longer used in both systems.

- **Device (Read-Only)** — Gives device access with read permissions. If new users sign in for the first time using the SAML Single Sign-on (SSO) app integration, they will be assigned this role. The organization's administrator must manually update the assigned roles to expand their permissions.

If more permissions are needed, see Assign permissions to roles on the next page.

Export information to CSV

- Click the icon.

Show, hide, or reset information

- Click the icon to show or hide information in columns.
- Click **Reset table** to go back to the default view.

Add roles

1. Go to **Users** > **Roles**.
2. Click the button in the upper-right corner.
3. Enter a name, description, and assign users.
   - **Enforce MFA** — Require user to set up Multi-Factor Authentication at login.
   - **Limit to specific sites** — Specify the **Sites**. A Premium or Enterprise license is required.

   > **Note:** You can view the users who are visiting your site from other sites and contact them, but you cannot manage their entry access. For example, a visitor might need to be notified of a muster event occurring at your site.

4. Select the permissions the role will have.

Note: You cannot create a role with more permissions than you have, and you cannot assign a role with more permissions to yourself or another administrator.

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

5. Click **Save**.

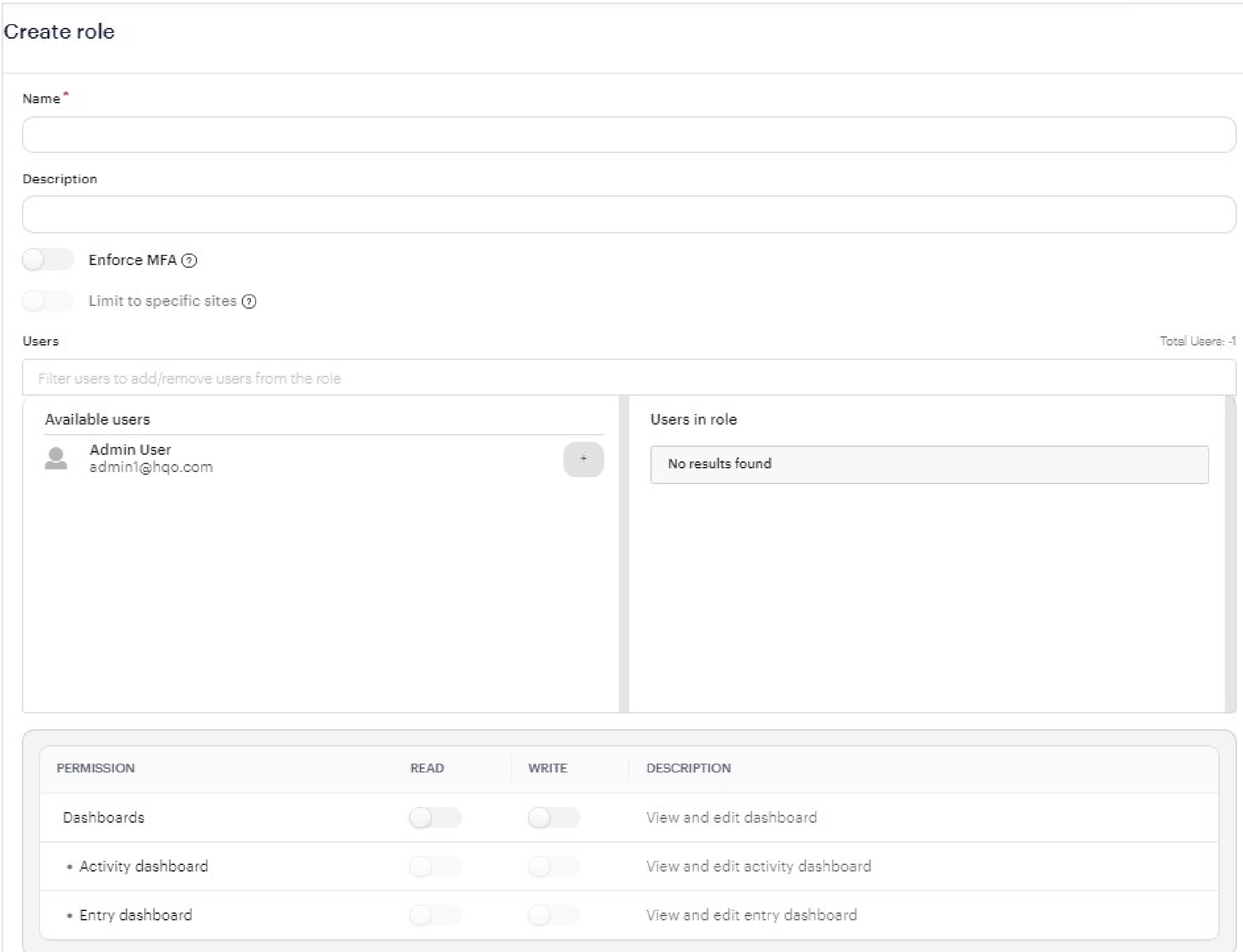
Assign permissions to roles

Permissions gives additional specificity when creating roles. For example, you create a role that limits access to just the Entry dashboard. Or, create a role with full portal access but only for one site.

Note: You cannot limit access to the users of a specific site. If you create a role that has access to users, the role will have access to all users within that organization.

Permissions	Description
Dashboards	View and edit the dashboards, Activity dashboard, Entry dashboard, and Alarms dashboard. **Note:** Access to the Devices dashboard is provided by Devices permission, not Dashboards permissions. A Premium or Enterprise plan is required to use the Alarms dashboard.
Users	View and edit users.
Roles	View and edit roles, and assign roles to users.
Sites	View and edit sites, buildings, entry states, general site settings, and lockdown plans. **Note:** A Premium or Enterprise license is required.
Cameras	View and edit cameras.
View live feed	View live feed from linked cameras. Avigilon Pro series readers only.
Playback video clips	Play back video clips from linked cameras. Avigilon Pro series readers only.
Export video clips	Export video clips for local storage.

Permissions		Description
	Devices	View and edit devices.
	Openpath video device	Adjust video settings for Avigilon (formerly Openpath) Video Reader Pro devices.
	Openpath video intercom	Adjust video settings and routing for Avigilon (formerly Openpath) Video Intercom Reader Pro devices.
	Reports	View and edit reports, entry access audit, portal audit report, credentials, general report settings, alarm report, muster report, and occupancy report. View and download report links. **Note:** A Premium or Enterprise plan is required to use the Alarm report, Muster report, or Occupancy report.
	App marketplace	View and edit app marketplace.
	Configurations	View and edit configurations, rules, alarms, alarm actions on open alarms, alerts, mobile app settings, and badge template printing, which is applicable only if the only if the Badge Printing app is installed.
	Administration	View and edit administration, account, and the Quick start page.



Delete roles

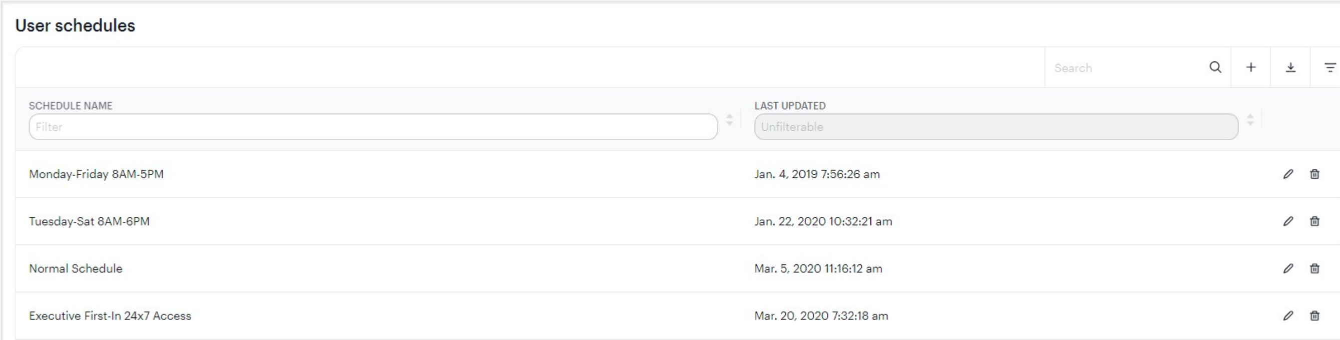
1. Select the role with no active users on the Roles page.
2. Click the icon.

> **Note:** If a user assigned to alarm monitoring is deleted, the alarms continue to be displayed in the Alarms dashboard and report history. You will be prompted to assign another user the next time you edit the alarm configuration.

3. Click **Yes**.

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 and groups. For example, you can define normal business hours for employees or require that certain users only use key cards.



Create schedules for users and access groups

Note: This feature is not applicable to Schlage no-tour wireless locks.

1. Go to **Users** > **User schedules**.
2. Click the button in the upper-right corner.
3. Enter a name for the user schedule and click **Next**.
4. Click the button in the EVENTS section.
    a. Choose **Repeating Event** or **One-time event**.
    b. Optional: Enter a **Name**.
5. For Repeating Event only:
    a. In **Frequency**, select **Daily**, **Weekly**, **Monthly**, or **Annually**.
    b. Select the days or dates the schedule will occur on.
6. Enter a **Start time** and **End time**, and **Time zone**.
7. Enter a **Start date** and **End date**.
8. Select the **Scheduled state**. The default scheduled states are:

    Note: This list depends on the entry states that are created in Sites.

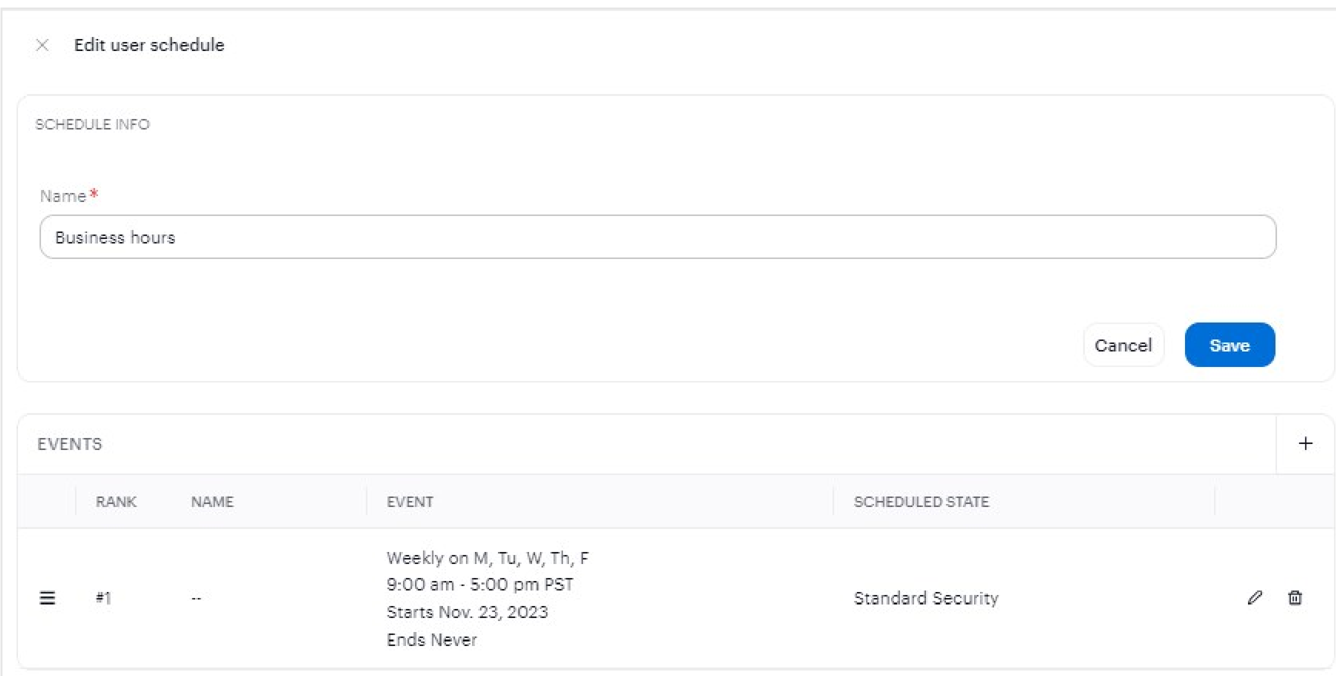
    - **Convenience** — Allows all valid credentials and trigger methods.
    - **Lockdown - Override Only** — No entry allowed, even with an otherwise valid credential (overrides allowed).
    - **No Entry** — No entry allowed, even with an otherwise valid credential.
    - **Onsite Only** — Allows all valid onsite credentials and trigger methods.

- **Standard Security** — Allows most mobile access and cards supported by Avigilon readers, and excludes remote mobile 1FA and third-party Wiegand methods.
- **Strict Security** — Allows only interactive 2FA onsite mobile access and encrypted smart cards, and excludes all remote, 1FA, and non-encrypted methods.
- **Standard Security MFA- PIN** — Standard MFA - Allows most mobile access, cards, and PINs supported by Avigilon readers, and excludes remote mobile 1FA and third-party Wiegand methods for MFA with PIN required as the second factor.
- **Strict Security MFA - PIN** — Strict MFA - Allows only interactive 2FA onsite mobile access, PINs, and encrypted smartcards excluding all remote, 1FA, and non-encrypted methods for MFA with PIN required as the second factor.

9. Click **Save**.

Note: A user schedule cannot be more permissive than what the entry allows. In the following example, the Scheduled state is defined as Standard Security, which only works if the entry state is also set to Standard Security or Convenience (but not say, Strict Security).

Tip: To disable remote unlock access to all users in a group, create a schedule with Onsite Only as the Scheduled state.



Apply user schedules

To apply a schedule to a user:

1. Go to Users > **Users**.

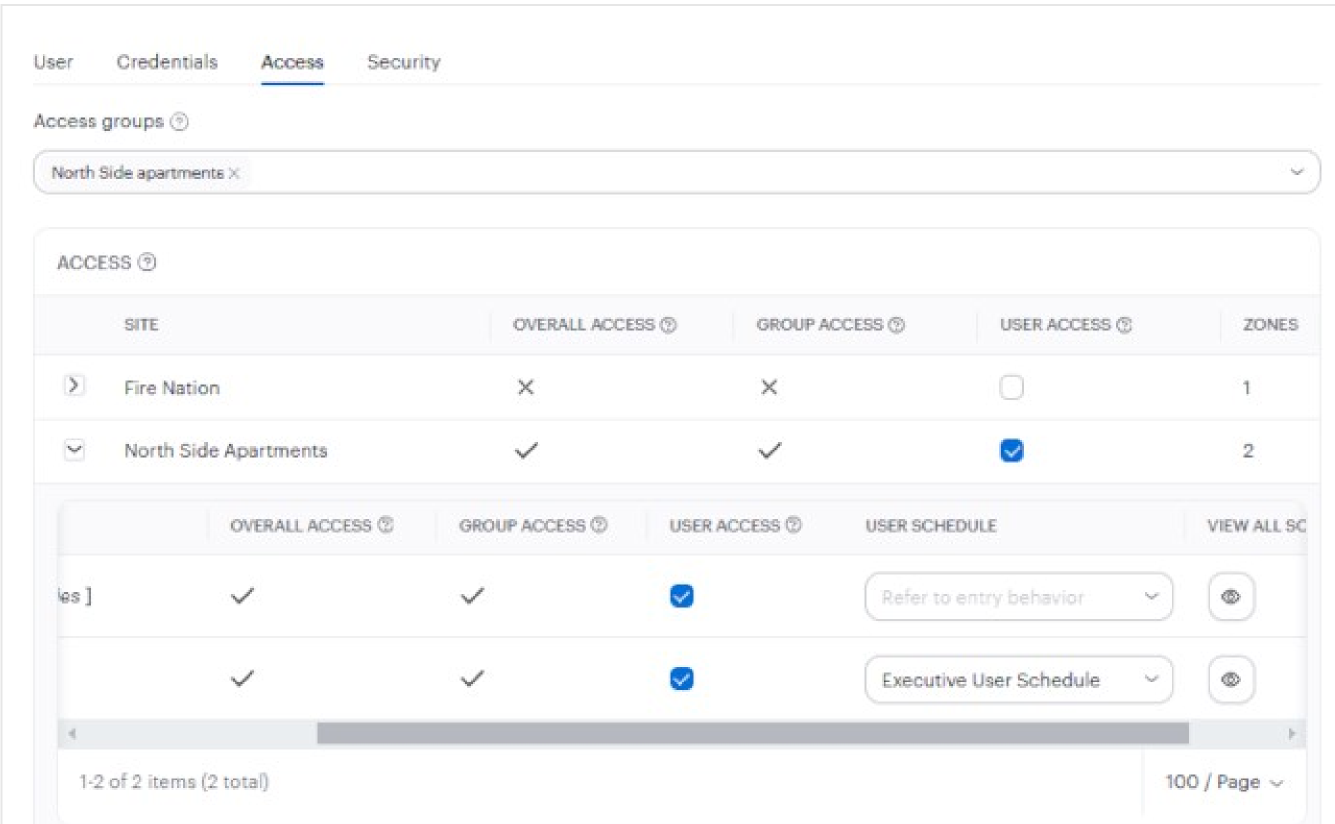
2. Click the edit pencil on the right-hand side of the user.

3. Select the **Access** tab.

4. Select the site under **SITE** (if more than one), and one or more entries under **ZONE**.

5. Add the schedule using the **USER SCHEDULE** drop-down.

6. Click **Save**.



Note: If a user has both user access and group access, you can assign two different schedules. For example, you could set the group's schedule to allow access Monday through Friday, from 9:00 AM to 5:00 PM. If you also want an individual user within that group to also have access on weekends—Saturday and Sunday, from 9:00 AM to 5:00 PM—you would create a second schedule and apply it specifically to that user.

Apply access group schedules

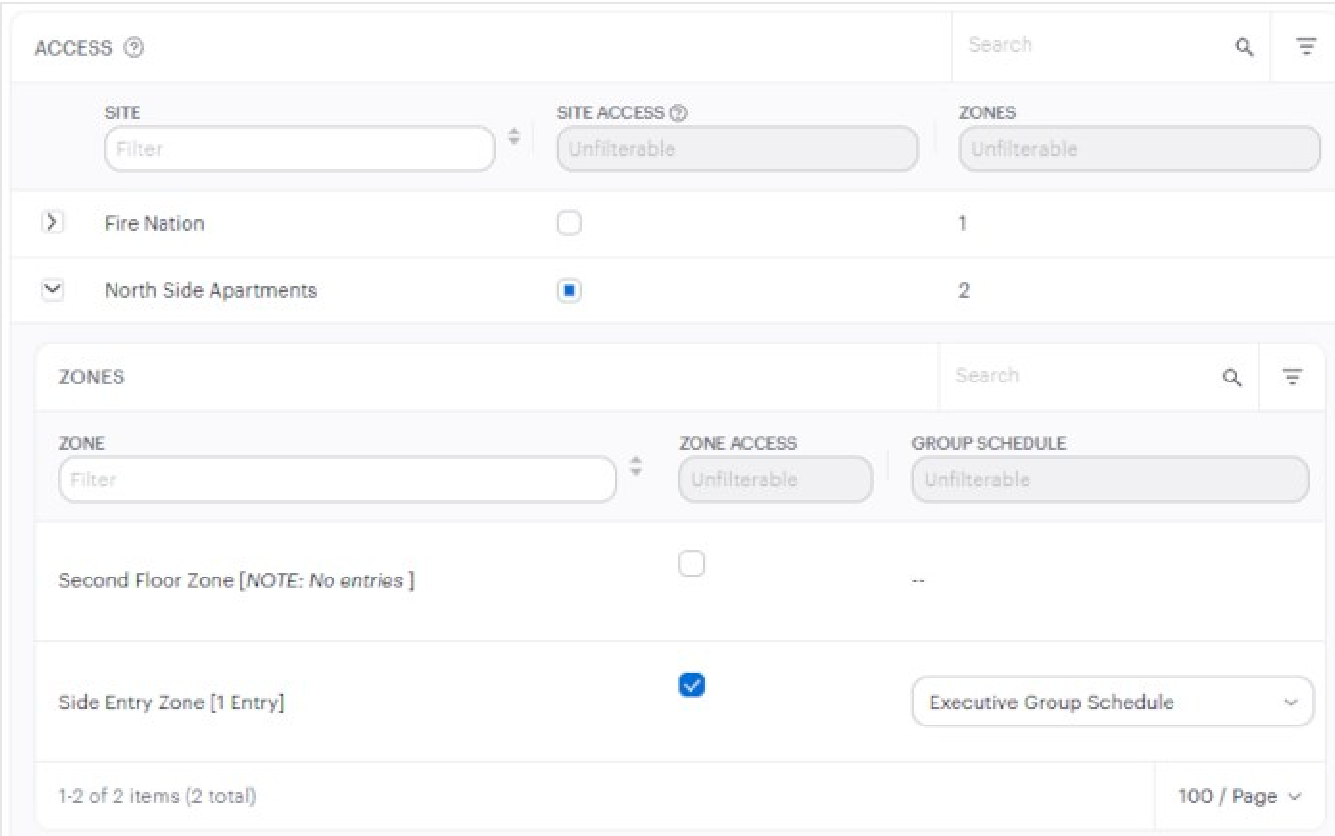
To apply a schedule to an access group:

1. Go to Users > **Access groups**.

2. Click the edit pencil on the right-hand side of the group.

3. Select the site, zone, and entry.

4. Add the schedule using the **GROUP SCHEDULE** drop-down.
5. Click **Save**.



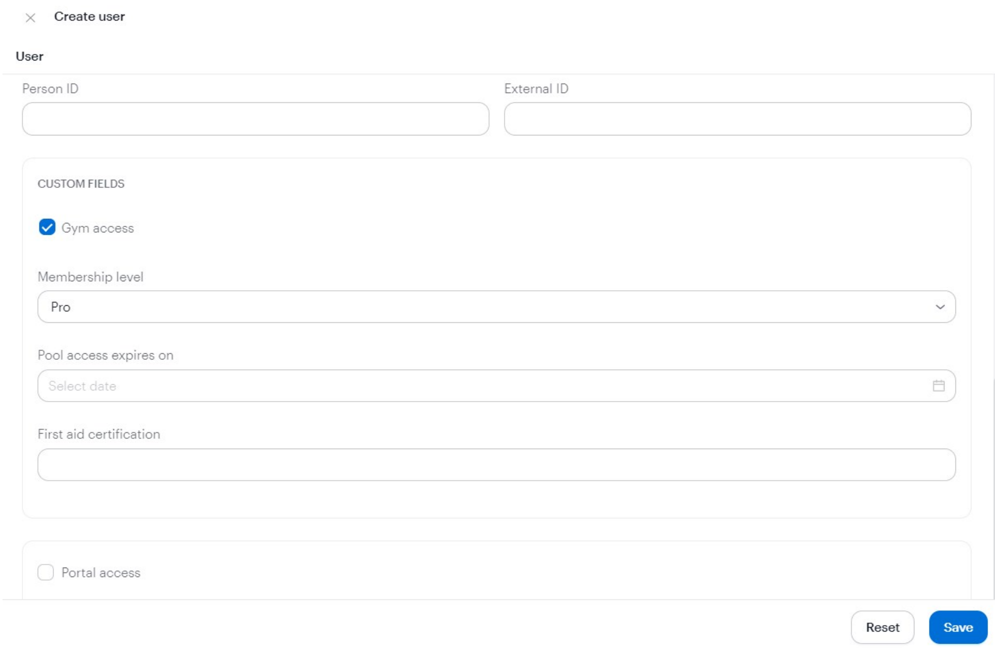
Note: If a user has both user access and group access, you can assign two different schedules. For example, you could set the group's schedule to allow access Monday through Friday, from 9:00 AM to 5:00 PM. If you also want an individual user within that group to also have access on weekends—Saturday and Sunday, from 9:00 AM to 5:00 PM—you would create a second schedule and apply it specifically to that user.

Custom fields

Note: A Premium or Enterprise license is required.

You can create custom, optional fields to capture additional user information (shown below), and filter them on the Users page. See also the **Configurations** > **Mobile app** or **Badge templates** pages.

Example:

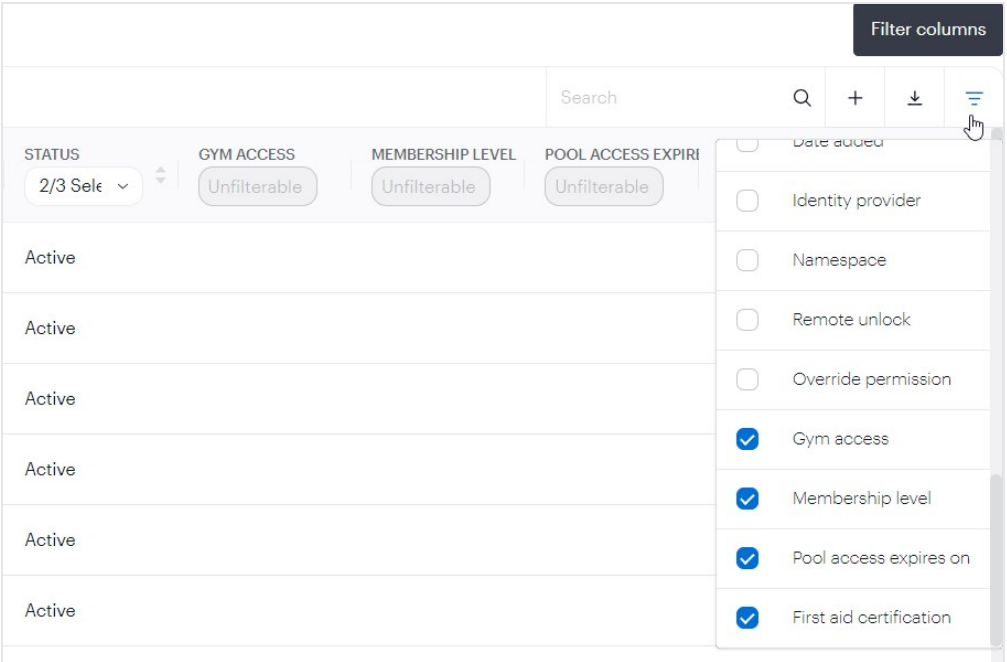


Create custom fields

1. Click the + button in the upper-right corner.
2. If you do not want to use the field yet, click the **Enabled** slider to disable .
3. Enter a **Name** for the field.
4. In **Field type**, select:
   - **Checkbox** for checked and unchecked states
   - **Date** for a calendar date picker
   - **Dropdown** for a list of items
   - **Text** for a box for typing in text
5. Click **Save**.
6. For a Dropdown field:
   a. Click the + button in the DROPDOWN ITEMS section.
   b. Enter a **Name** for the item and click **Save**.
   c. Repeat for the remaining items.
7. Ensure the **Enabled** slider is enabled .

The fields will appear in the CUSTOM FIELDS section on the user page. They can be filtered as shown below.

Example:


Filter columns
Search
STATUS
2/3 Sele
GYM ACCESS
Unfilterable
MEMBERSHIP LEVEL
Unfilterable
POOL ACCESS EXPIRI
Unfilterable
Active
Active
Active
Active
Active
Active
Identity provider
Namespace
Remote unlock
Override permission
Gym access
Membership level
Pool access expires on
First aid certification

Sites

Sites are physical locations, such as office buildings, comprised of zones and entries.

Site management

The Sites page lets you create a site for every location where you have Alta Access installed.

Add sites

1. Click the + button in the upper-right corner.
2. Enter a name for the site, the physical address, and a phone number.
3. Optional. Set the language of Alta Access site-wide emails in **Site language**.
4. Click **Save**.
5. Assign users to the site using the > button.

> **Note:** You can view the users who are visiting your site from other sites and contact them, but you cannot manage their entry access. For example, a visitor might need to be notified of a muster event occurring at your site.

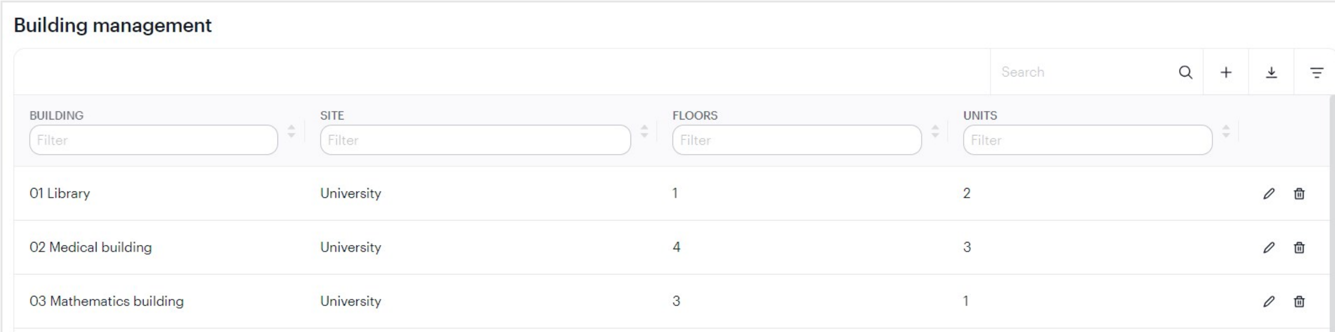
Add zones

1. Click the site on the Sites page.
2. Click the + button in the ZONES section.

   For more information, see Add zones on page 68.

Building management

You can view and manage the floors and units in buildings, and assign access to users and groups, on the Buildings page.



Add buildings

1. Go to Sites > **Buildings**.
2. Click the + button in the upper-right corner.
3. Enter the name of the building and the site.
4. Include the address, phone number, and a description.
5. Click **Save**.

Add floors to buildings

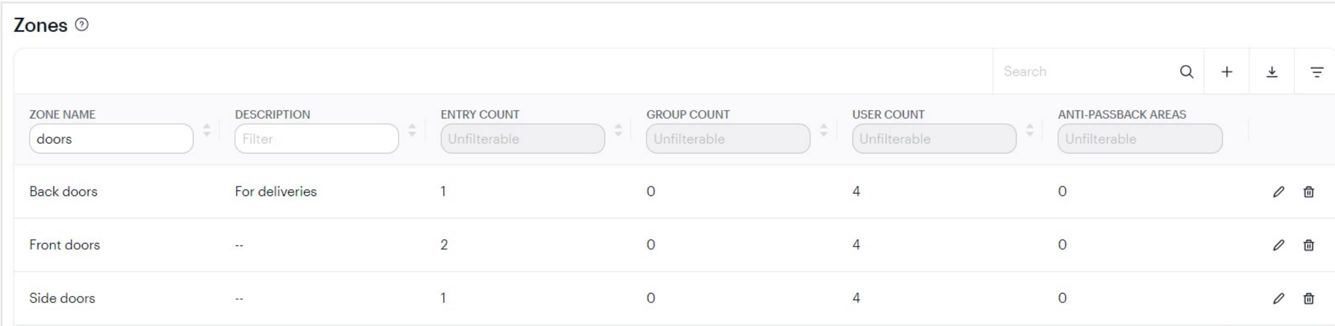
1. Click the building on the Buildings page.
2. Click the **Floors** tab.
3. Click the + button.
4. Enter the name of the floor and a description.
5. Click **Save**.

Add units to floors and assign access

1. Click the building on the Buildings page.
2. Click the **Units** tab.
3. Click the + button.
4. Select the floor.
5. Enter the unit and a description.
6. Select the users and access groups that need access to the unit.
7. Click **Save**.

Zone management

The Zones 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.



Export information to CSV

- Click the icon.

Show, hide, or reset information

- Click the icon to show or hide information in columns.
- Click **Reset table** to go back to the default view.

Zone sharing between customers

Zones can be shared between multiple 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.

> **Note:** This feature is not applicable to Schlage no-tour wireless locks.

Add zones

1. Go to **Sites** > **Zones**.
2. Click the button in the upper-right corner.
3. Enter a **Name** and description (optional).
4. 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. A zone can include a mix of Avigilon locks and Schlage wireless locks.

5. Optional. Add **Access groups** and **Users** to the zone.

6. For Schlage no-tour wireless locks only. In the **Entries** list, click and drag the no-tour locks installed in the zone (left pane) to the zone list (right pane).
7. Optional. If you want to share this zone with a different organization, enter the Org IDs.
8. Click **Save**.

Anti-passback and occupancy management

> **Note:** If you are working with Schlage no-tour wireless locks, information may be out-of-date. Anti-passback and occupancy information is available only after visiting the no-tour wireless lock in person and completing a manual sync using the Alta Access mobile app.

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.

Overview of 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 the following example, all four readers reside on the same ACU and are configured across three areas.

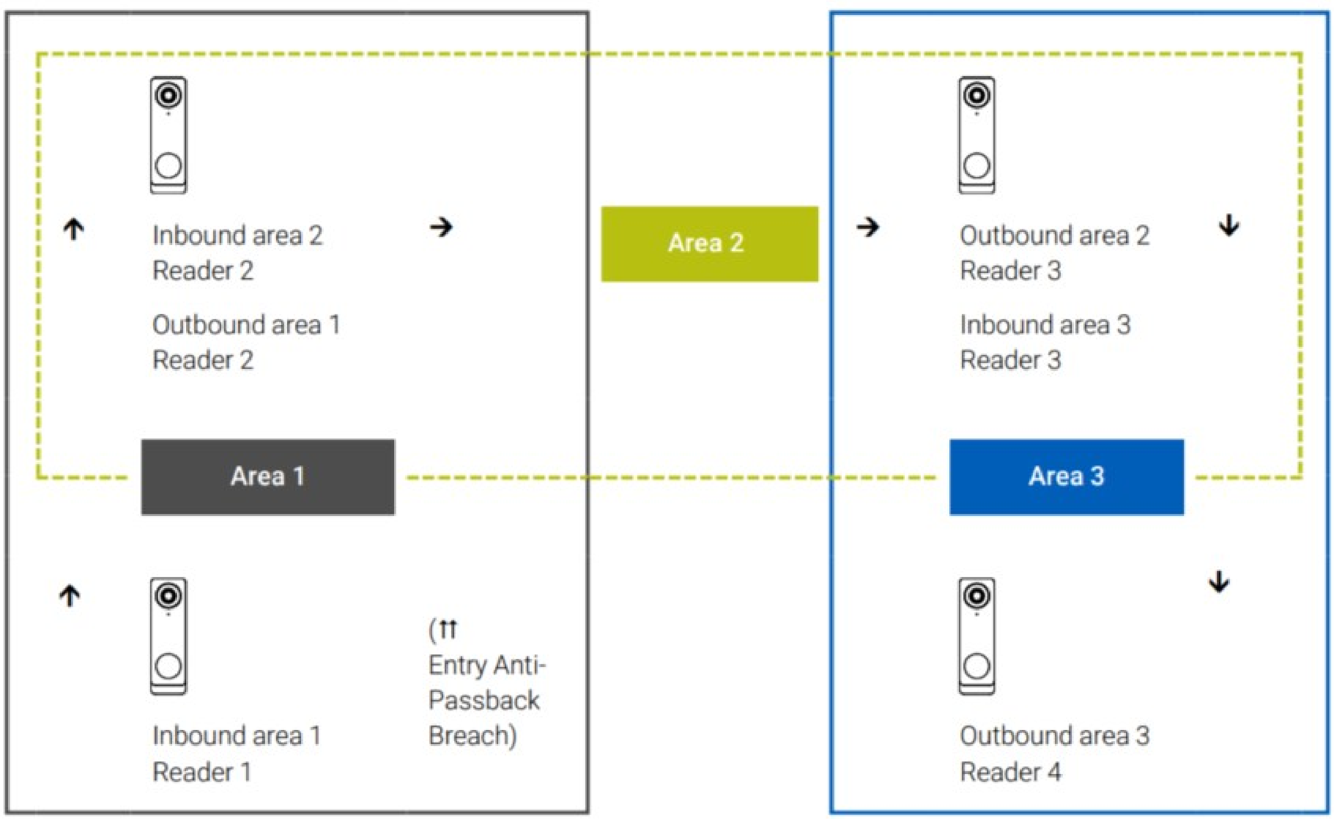


Figure 1 Anti-passback logic

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, any attempt by that user to move in the same direction again will result in an Entry Anti-Passback Breach event (see the example in the above figure).

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, the user's next movement will be allowed in either direction, after which normal rules will apply again.

Configure Entry Anti-Passback Breach event

Entry Anti-Passback Breach events can trigger alerts. See Alerts by email or SMS on page 149. They can also be used to trigger custom integrations. See Rules on page 146.

> **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.

Set up anti-passback and occupancy limit

To set up anti-passback and occupancy limit in a zone:

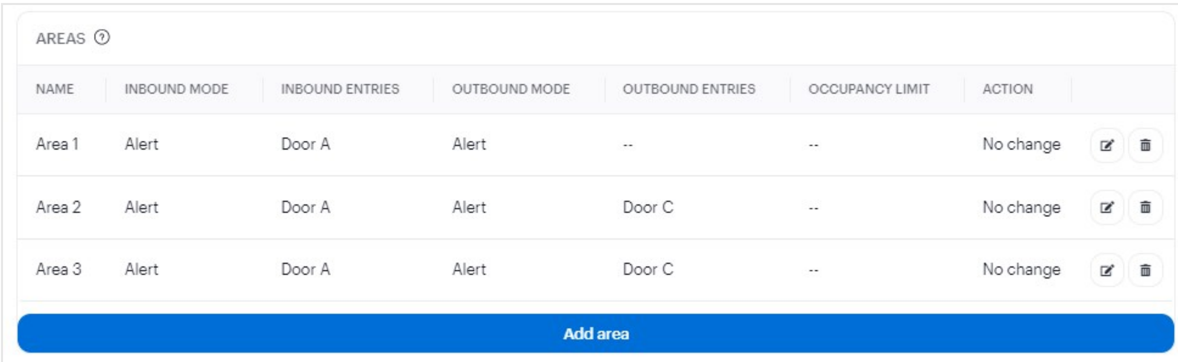
1. Select the zone and click the **Anti-passback** tab.
2. Enable any of the following settings:
    - **Expiration time** — Time in seconds after which the anti-passback state will reset for the user.
    - **Reset Anti-passback Periodically** — A schedule during which a user is not limited to anti-passback logic, until after their second unlock attempt.
        a. Enter a **Reset Time** and **Time zone**.
        b. Select the days or dates the schedule will occur on.
    - **Use contact sensor** — Changes a user's anti-passback state after the contact sensor reports open.
    - **Shared-To Orgs Can Reset Anti-passback** — Gives your organizations that share this zone the permission to reset anti-passback for their users.
3. Define the area within the zone to be enforced by anti-passback and an occupancy limit.
    a. Click **Add area** and enter a **Name**.
    b. Set the **Inbound mode** and **Outbound mode** to configure the system response 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.
    c. Add your entries in **Inbound entries** and **Outbound entries**.

> **Note:** An entry can only be used once within an area, either as inbound or outbound but not both. However an entry can be used in multiple areas. In addition, all entries within an area must reside on the same ACU, and all entries belonging to the parent zone must reside on the same ACU.

d. Optional. In **Occupancy limiting mode**, select **Alert** or **Enforce**. Enter the number in **Occupancy limit**.

e. Click **Add area** to save. The area is added to the zone.

f. Optional. Repeat the above steps to add more areas to the zone.



4. Click **Save**.

Reset anti-passback on zones and users

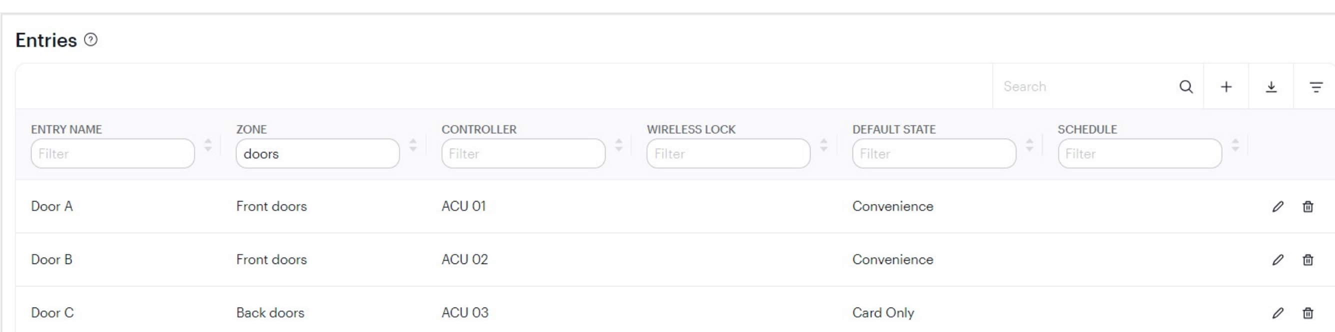
To reset anti-passback at the zone level:

1. Go to **Sites** > **Zones**.
2. Click **Reset anti-passback** in the ANTI-PASSBACK AREAS column.
3. Click **Yes**.

To reset anti-passback on a user or multiple users, see Issue batch actions to users on page 53.

Entry management

The Entries page is where you can add and manage entries. Generally speaking, entries are doors, but can also be gates, turnstiles, and elevator floors. An entry is often secured with a reader or wireless lock.



Note: Your installer may provision some or all of the following features for you during the installation process.

Export information to CSV

- Click the icon.

Show, hide, or reset information

- Click the icon to show or hide information in columns.
- Click **Reset table** to go back to the default view.

Add entries

1. Go to **Sites** > **Entries**.
2. Click the button in the upper-right corner.
3. Enter a name and select the zone.
4. In **Cloud gateway device type**, select the hardware that is configured at the entry.
    - **Openpath** hardware
        - Select the ACU in **Controller**.
        - Select the video reader or video intercom reader in **Controller**.
    - **Schlage** for Allegion Schlage hardware
        - Select the lock in **Schlage wireless lock**.

    Note: The Entry Open Duration and Entry state settings are not applicable to no-tour wireless locks.

5. Optional. Select the **Muster point** toggle to designate the entry as a safe area, where personnel should gather in an emergency situation.

    Note: A credential reader is required to be installed at the entry. The reader should only be used in a muster event and not for any other purpose. For more information, see Muster Reports workflow on page 19.

    If you are working with Schlage no-tour wireless locks, information may be out-of-date. Mustering information is available only after visiting the no-tour wireless lock in person and completing a manual sync using the Alta Access mobile app.

6. Click **Save**.

Edit entries

After saving a new entry, you can configure these settings depending on the installed device.

Set default state and schedule for the entry

1. In ENTRY BEHAVIOR, you can set the default state for the entry.

   > **Note:** Entries installed with gateway-connected Allegion Schlage NDEB and LEB wireless locks only support Unlocked, No Entry, and Convenience entry states. Entry states are not supported by Schlage Control locks and no-tour connected NDEB and LEB series wireless locks.

   - **Unlocked** — No credential is required for access.
   - **Convenience** — Allows all valid credentials and trigger methods.
   - **Lockdown - Override Only** — No entry allowed, even with an otherwise valid credential (overrides allowed).
   - **No Entry** — No entry allowed, even with an otherwise valid credential.
   - **Onsite Only** — Allows all valid onsite credentials and trigger methods.
   - **Standard Security** — Allows most mobile access and cards supported by Avigilon readers, and excludes remote mobile 1FA and third-party Wiegand methods.
   - **Standard Security MFA- PIN** — Standard MFA - Allows most mobile access, cards, and PINs supported by Avigilon readers, and excludes remote mobile 1FA and third-party Wiegand methods for MFA with PIN required as the second factor.
   - **Strict Security** — Allows only interactive 2FA onsite mobile access and encrypted smart cards, and excludes all remote, 1FA, and non-encrypted methods.
   - **Strict Security MFA - PIN** — Strict MFA - Allows only interactive 2FA onsite mobile access, PINs, and encrypted smartcards excluding all remote, 1FA, and non-encrypted methods for MFA with PIN required as the second factor.

2. Optional. Assign a schedule.

   If you need to create a new schedule, click **Manage schedules**. See Entry schedules on page 79.

Schlage wireless lock (gateway connected) settings

- For NDEB and LEB only. In SCHLAGE WIRELESS LOCK, **Ajar Detection** and **Forced-Open detection** are always enabled for wireless locks.

  If needed, edit the duration in **Ajar Duration (255 Sec Max)**, and specify seconds or minutes in **Unit**.

- In **Entry Open Duration**, edit how long the entry will remain unlocked (maximum is 30 seconds).
- For NDEB and LEB only. **Card Reader Sensitivity** is set to **Normal** by default, but you can select **High** or **Max** for more reliable reading of key fobs.

Contact sensor settings

In CONTACT SENSOR, you can specify the port to which the entry is wired and related settings.

- **Port** — The port for the contact sensor. A contact sensor detects if an entry is open.
- **Ajar feature** — If enabled, the maximum time the door can be ajar before an event is generated indicating the door is ajar. Edit the maximum allowed time the door can be ajar before events are generated in **Ajar duration (15 min max)**.

  If disabled, no system action occurs if the door is ajar.
- **Forced-Open detection** — If enabled, an entry opening without first unlocking through the **Openpath** device (specified in **Cloud gateway device type**) or triggering the REX, will generate an event.

To monitor the entry, you can set up contact sensor events that can trigger alerts. See Alerts by email or SMS on page 149 and Rules on page 146 for triggering custom integrations.

Entry and exit hardware settings

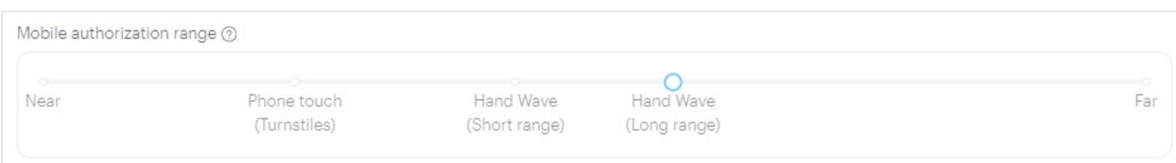
In ENTRY/EXIT DEVICES, you can specify the relay port on the ACU or expansion board to be used for controlling electric strikes or maglocks, and related settings.

- **Port** — The Relay 1, Relay 2, Relay 3, or Relay 4 port to assign the Avigilon reader. When installed, the electric strike is wired to one of the four ACU ports, and the reader is wired to the strike. You will need to select the ACU relay for which this reader/entry is wired to the ACU.
- **Entry open duration (10 min max)** — The maximum time the entry can remain unlocked before reverting back to its default state. Supported range is 1 second and 10 minutes. Specify seconds or minutes in **Unit**.
- **Invert output** — An advanced setting for elevator relays. If enabled, the NC/NO configuration of the physical relay is flipped.

Openpath reader settings

In OPENPATH READER, you can assign the entry to the Avigilon (formerly Openpath) reader and related settings.

- **Port** — The port on the ACU to which the reader is connected.
- **Card reading** — If enabled, allows RFID/NFC cards at this reader.
- **Wave to unlock** — If enabled, allows the Wave to Unlock and Touch Entry functionality.
  - **Mobile authorization range** — The distance between the mobile device and the Avigilon reader in order to register a Wave to Unlock attempt. Set the **Near** to **Far** range using the slider.

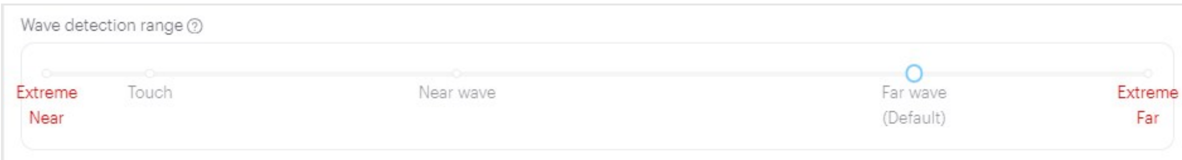


  - **Wave detection range** — The distance between the hand and the Avigilon reader to initiate the unlock attempt. Set the range of detection for the capacitive (cap) touch sensor using the slider.

> **Note:** This setting may require adjustment depending on your environmental conditions and device model.

The range for Video Intercom Reader Pro and Video Reader Pro readers includes:

The range for Smart Readers includes:



- **Auto proximity unlock (Elevators only)** — If enabled, unlocks the entry when a user with a valid mobile credential is within range of the reader.
  - **Mobile authorization/Trigger range** — The distance between the user's mobile device and the reader to initiate an unlock attempt.
- **Advanced options**
  - For the Avigilon reader:

    Mobile communication 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 Alta Open mobile app installed on the phone.
  - For the Avigilon keypad reader:

    Key press audible feedback — If enabled, audible feedback upon key press.

    Key press LED feedback — If enabled, LED feedback upon key press.

    Allowed time interval for completion of 1FA PIN entry (Max 20 seconds) — Adjust the time interval, as needed.

Request to exit (REX) settings

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

- **Port** — The port for the REX device to which the entry is wired.
- **Mode** — The **Normally closed** or **Normally open** mode of the REX device that sends commands to the ACU.

  > **Note:** Contact your electrical installer for the required mode for your entry configuration.

- **Trigger relay to unlock entry** — If enabled, a triggered REX will open the associated relays and prevent forced-open alarms.

Wiegand device settings

Alta Access is compatible with legacy Wiegand devices.

- **Port** — The port for the Wiegand device to which this entry is wired.
- **Mode** — The direction the card credential data is sent.
  - **Input** — Receives data from the Wiegand reader.
  - **Output (gateway)** — Sends credential data to a third-party control panel.

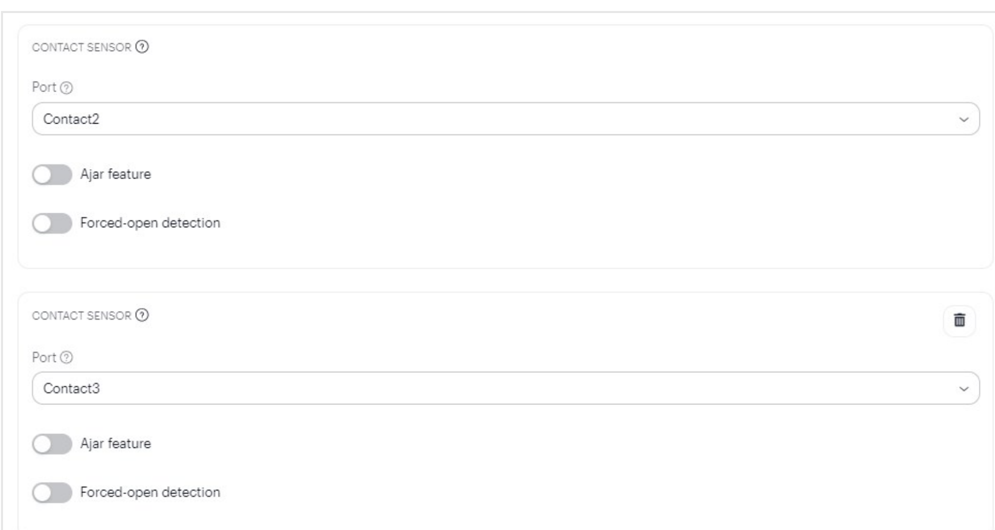
    Enable **Gateway credential pass-through** if you do not want Alta Access to authenticate credentials, but rather send all data to the legacy panel for authentication.

    Enter a **Default gateway card number** so that all credentials (including mobile credentials) are sent to the legacy panel as a Wiegand ID.

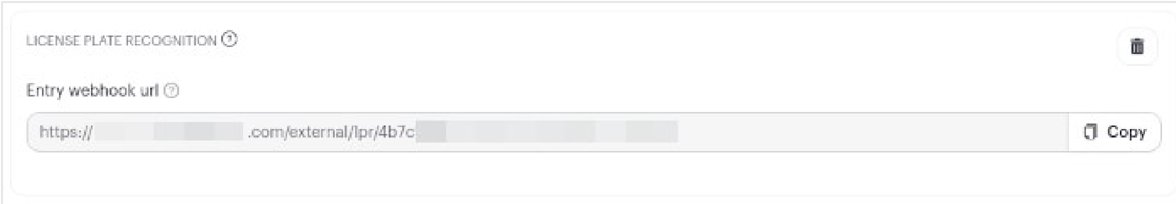
Additional device (control) settings

1. If your entry is configured with more than one of the above devices, select it from **Control** and click **Add control**.
   - **Contact sensor**
   - **Entry/Exit devices**
   - **License plate recognition**
   - **Openpath reader**
   - **Request to exit**
   - **Wiegand device**

   The additional device appears below the first device.

2. If you added **License plate recognition** to the entry, save the entry webhook URL.
    a. Make a note of the URL which will be used later during Alta Video configuration.



> **Note:** If you have multiple entries that need to be connected to different Alta Video cameras, repeat the above steps for each entry and note their unique webhook URLs.

    b. Configure the user credential on the **Users** page.
    c. Select the user and click the **Credentials** tab.
    d. Enter **License Plate** — The alphanumeric value of the license plate.
    e. Click **Save**.

> **Note:** After saving, perform LPR setup in Alta Video. For more information, see this Alta Access article.

3. To remove the additional device, click .

Entry states

An entry state defines whether an entry is unlocked and what access methods may be used to unlock it. Alta Access provides the following default entry states:

- **Unlocked** — No credential is required for access.
- **No Entry** — No entry allowed, even with an otherwise valid credential.
- **Lockdown - Override Only** — No entry allowed, even with an otherwise valid credential (overrides allowed).
- **Convenience** — Allows all valid credentials and trigger methods.
- **Onsite Only** — Allows all valid onsite credentials and trigger methods.
- **Standard Security** — Allows most mobile access and cards supported by Avigilon readers, and excludes remote mobile 1FA and third-party Wiegand methods.
- **Strict Security** — Allows only interactive 2FA onsite mobile access and encrypted smart cards, and excludes all remote, 1FA, and non-encrypted methods.
- **Standard Security MFA- PIN** — Standard MFA - Allows most mobile access, cards, and PINs supported by Avigilon readers, and excludes remote mobile 1FA and third-party Wiegand methods for MFA with PIN required as the second factor.

- **Strict Security MFA - PIN** — Strict MFA - Allows only interactive 2FA onsite mobile access, PINs, and encrypted smartcards excluding all remote, 1FA, and non-encrypted methods for MFA with PIN required as the second factor.

View trigger methods in entry states

The TRIGGER METHODS column refers to the number of ways that an entry can be unlocked in that particular state.

- Click an entry state in order to view the trigger methods included in that state.

Add entry states

1. Go to **Sites** > **Entry states**.
2. Click the + button in the upper-right corner.
3. Enter the name for the entry state and a description.
4. Optional. If the entry requires two credentials from each user:
   a. Click the **Enable multi-factor** slider.
   b. Enter the trigger methods in **Factor 1** and **Factor 2**.
   c. In **Multi-factor interval (5-30 seconds)**, specify the interval between the trigger methods.
5. In TRIGGER METHODS, use the **Mobile**, **Card**, **PIN**, **Cloud key**, **Mobile override**, **Card override**, and **Cloud key override** checkboxes to enable the trigger methods for the entry state.

   > **Tip:** Refer to the **Definitions** tooltip for the various methods.

6. Click **Save**.

Trigger method definitions

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

- **Onsite** — Opposite of Remote; an unlock request that is triggered while the user is near the entry.
- **Near reader** — An unlock request that is considered Onsite because the mobile device is within close range of the entry's Avigilon reader.
- **Over BLE** — A mobile unlock request that is sent over BLE through the Avigilon Reader. Such a request is always Onsite.
- **Over WiFi** — A mobile unlock request that is sent over the mobile device's WiFi connection over the local network directly to the Avigilon Access Control Unit. Such a request may be considered Onsite or Remote depending on whether the mobile device is in range of the entry's Avigilon reader.
- **Over cloud** — A mobile unlock request that is sent over the mobile device's WiFi or cell/LTE connection, and routed via the Alta Access cloud back to the Access Control Unit. Such a request, if permitted, enables Remote unlock from anywhere in the world where the mobile device has an internet connection, but also may be considered Onsite if the mobile device is in range of the entry's Avigilon reader.
- **Geofence** — A mobile unlock or override request that is sent within the virtual geographic boundary of the Avigilon reader and uses the location-based service on the Avigilon Alta Open mobile app over a Cloud, WiFi, or BLE connection.
- **Multi-Factor** — An unlock request that requires two different credential types from a single user (such as card and PIN). When enabled, users with permissions at the entry must present both credentials using the approved trigger methods for each type to gain access.

Entry schedules

Entry schedules allow for entries to be in a specific state, such as locked and unlocked, based on date and time. For example, an entry can be set to an unlocked state during normal business hours, Monday to Friday, but remain locked (its default entry state) when the schedule is inactive.

> **Important:** If no entry schedules are assigned to an entry, the entry is unlocked at all times.

> **Note:** Devices that do not support real-time communication with a gateway will not support this feature. Offline devices include Schlage no-tour connected wireless locks.

Add entry schedules

1. Go to **Sites** > **Entry schedules**.
2. Click the + button in the upper-right corner.
3. Enter a name for the schedule and click **Next**.
4. In **Entries**, assign the entry schedule to entries by typing in the entry names or selecting from the list.
5. Click the + button in the EVENTS section.

a. Choose **Repeating Event** or **One-time event**.

b. Optional: Enter a **Name**.

6. For Repeating Event only:

    a. In **Frequency**, select **Daily**, **Weekly**, **Monthly**, or **Annually**.

    b. Select the days or dates the schedule will occur on.

7. Enter a **Start time** and **End time**, and **Time zone**.
8. Enter a **Start date** and **End date**.
9. Select the **Scheduled state**. The default scheduled states are:

> **Note:** This list depends on the entry states that are created in Sites.

- **Convenience** — Allows all valid credentials and trigger methods.
- **Lockdown - Override Only** — No entry allowed, even with an otherwise valid credential (overrides allowed).
- **No Entry** — No entry allowed, even with an otherwise valid credential.
- **Onsite Only** — Allows all valid onsite credentials and trigger methods.
- **Standard Security** — Allows most mobile access and cards supported by Avigilon readers, and excludes remote mobile 1FA and third-party Wiegand methods.
- **Strict Security** — Allows only interactive 2FA onsite mobile access and encrypted smart cards, and excludes all remote, 1FA, and non-encrypted methods.
- **Standard Security MFA- PIN** — Standard MFA - Allows most mobile access, cards, and PINs supported by Avigilon readers, and excludes remote mobile 1FA and third-party Wiegand methods for MFA with PIN required as the second factor.
- **Strict Security MFA - PIN** — Strict MFA - Allows only interactive 2FA onsite mobile access, PINs, and encrypted smartcards excluding all remote, 1FA, and non-encrypted methods for MFA with PIN required as the second factor.

10. Optional: Enable **Trigger after an unlock method included in** and set the scheduled state.

    If enabled, the entry will not change to the scheduled state until the first person with access triggers a door to unlock.

11. Click **Save**.

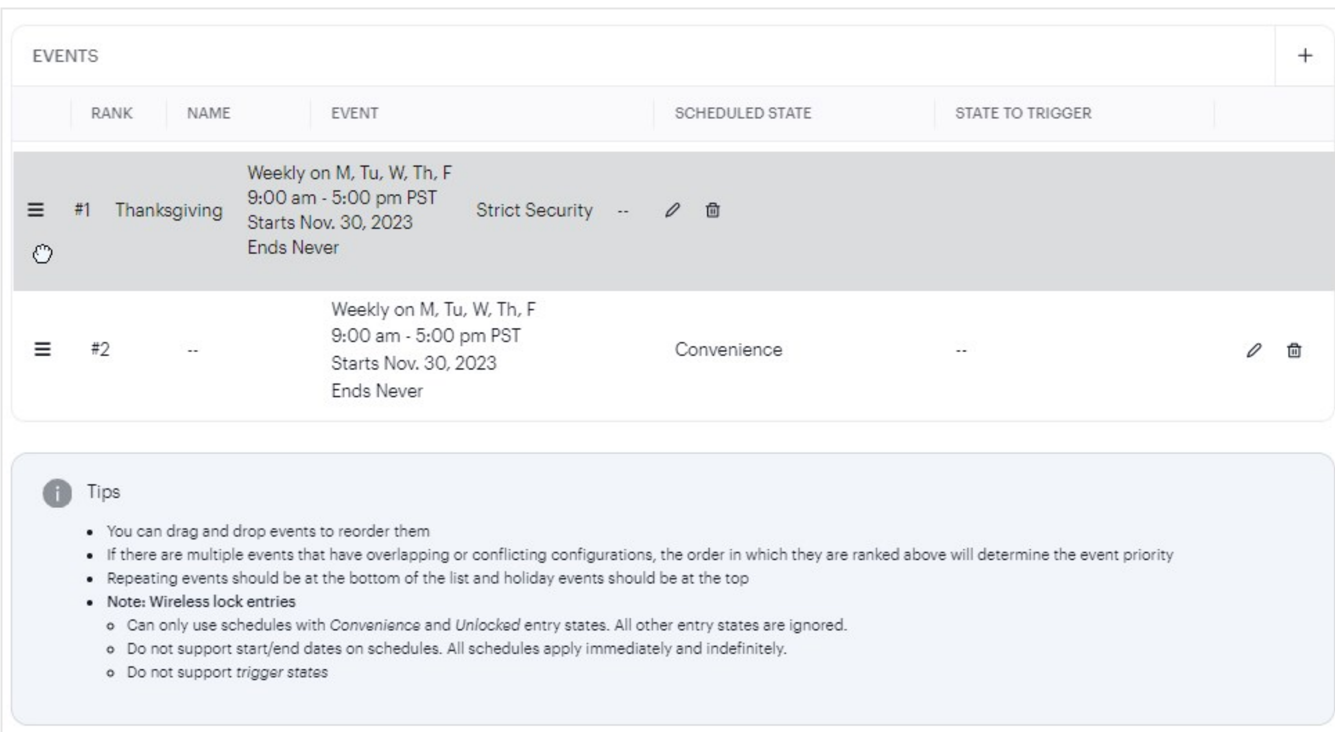
Add holiday schedules

1. Go to **Sites** > **Entry schedules**.
2. Create an entry schedule or edit an existing one.

3. Click the + button in the EVENTS section.
    a. Choose **Repeating Event**.
    b. Optional. Enter a **Name**. Example: Thanksgiving.
    c. In **Frequency**, select **Annually**.
    d. Select the day the schedule will occur on. Example: On the Fourth Thursday.
    e. Enter a **Start time** and **End time**, and **Time zone**.

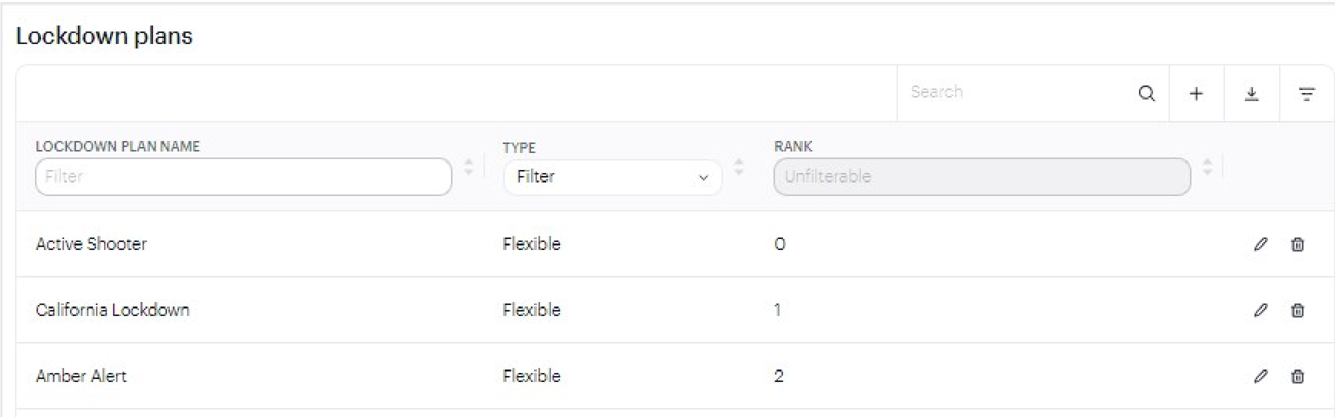
        Example: For a 24-hour schedule, enter 12:00 am for the start time and 11:59 pm for the end time.
    f. Enter a **Start date** and optional **End date**. The default is Never ends.
    g. In **Scheduled state**, select an option.
    h. Optional: Enable and set the state **Trigger after an unlock method included in**.

        If enabled, the entry will not change to the scheduled state until the first person with access triggers a door to unlock.
    i. Click **Save**.
4. Hover your mouse over the ☰ icon in the EVENTS list and drag ( ) to reorder your holiday entry event. The holiday should rank higher than your usual schedule.



Lockdown plans (Premium and Enterprise plans)

The Lockdown plans page is where you can view and manage lockdown plans that are applied at the zone level in an emergency situation, including specifying a ranking of the possible scenarios, the triggered entry state, and all the users and groups that may trigger a lockdown when the situation arises and revert the lockdown when the emergency situation is resolved.



Note: Lockdown is supported only for locks that are connected to an ACU or gateway.

After adding a lockdown plan, see Triggering lockdown plans on page 24.

Add lockdown plans

1. Go to **Sites** > **Lockdown plans**.
2. Click in the upper-right corner.
3. Enter the name of the lockdown plan and a **Rank**, the lower the number, the higher the rank.

   Important: The rank determines the lockdown plan that takes priority when multiple lockdown plans share entries. When assigning a rank, ensure the number is not already used.

4. Optional. In **Duration**, enter a time in minutes or hours after which the plan will auto-revert.

   If you do not want the lockdown plan to revert automatically, leave this value blank.

5. Optional. The **Use standard zone configuration** setting is enabled by default to create a lockdown plan that automatically includes all zones with the Lockdown - Override Only trigger state.
6. Select the zones that the lockdown plan will impact.

   Note: You cannot add the zones that have been shared with you to a lockdown plan.

a. Click **Add zone** and the zone name.

b. In TRIGGERED STATE , select the entry state that will be triggered.

> **Note:** We recommend using the **Lockdown - Override Only** entry state. This means only users with override permissions can unlock entries in this state.

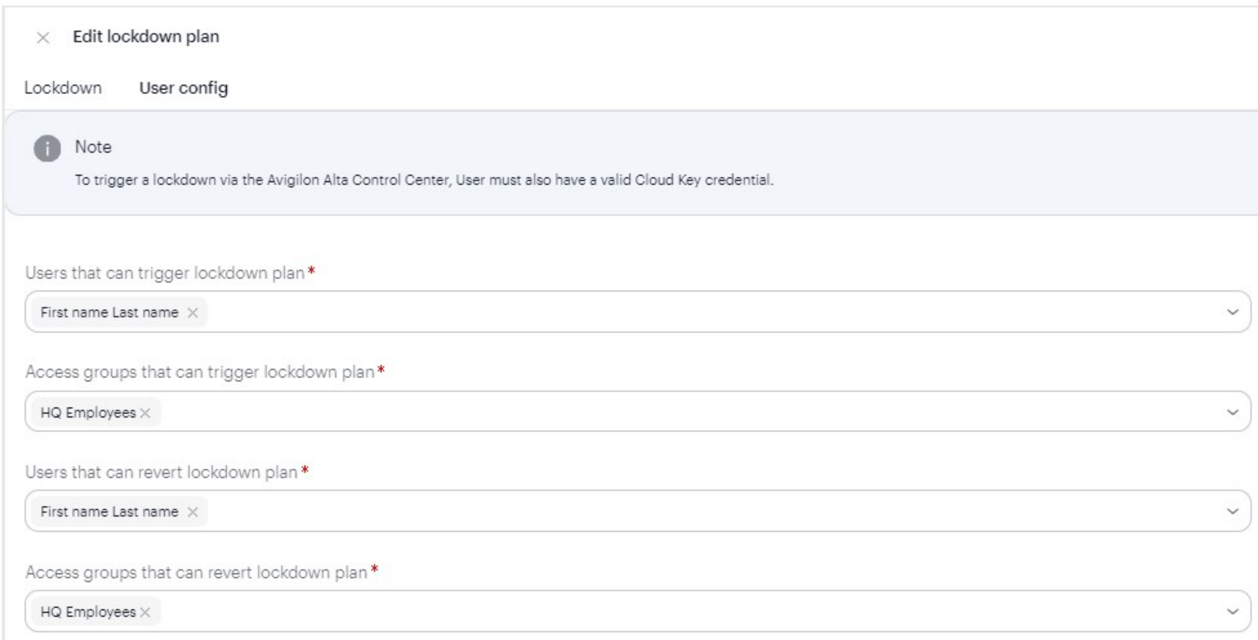
c. Repeat the above steps, as needed.

7. Click **Save**.

   The User config tab is displayed. See Assign users and group permissions for lockdown plans below.

Assign users and group permissions for lockdown plans

1. On the **User config** tab, select the users and groups that can trigger and revert the lockdown plan.



> **Note:** Enable **Override permission** to give the user permission to unlock entries in the Lockdown - Override Only state. See Assign permission to override lockdowns on page 52.

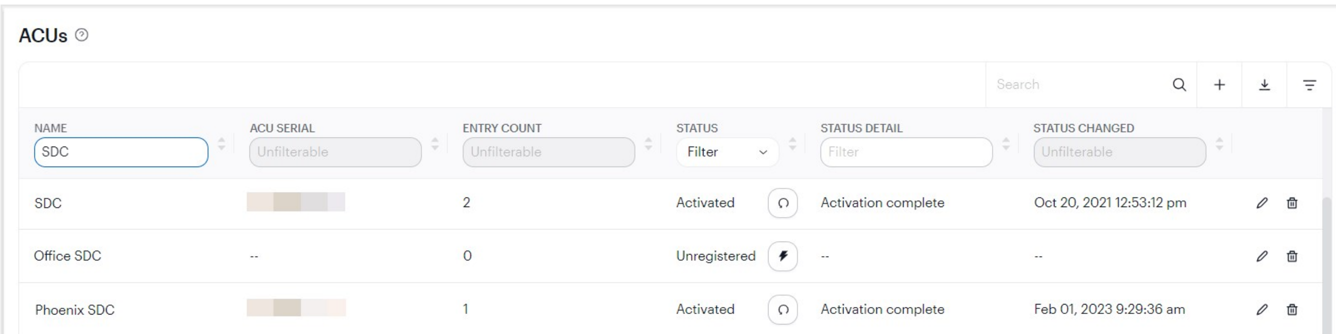
2. Click **Save**.

Devices

You can use the **Devices** page to create and manage Avigilon and third-party hardware, including access control units (ACUs), Single Door Controllers (SDCs), readers, video readers, video intercom readers, wireless locks, wireless lock gateways, and more.

ACU management

The ACUs page is where you can view and manage controllers including ACUs and Single Door Controllers (SDC example is shown below).



Export information to CSV

- Click the icon.

Show, hide, or reset information

- Click the icon to show or hide information in columns.
- Click **Reset table** to go back to the default view.

Add ACUs or SDCs

Tip:
Using the Alta Access mobile app is recommended, which automatically creates and provisions the ACU in Alta Access and adds any connected devices.

For more information, see this Alta Access article.

Add multiple ACUs or SDCs using Quick start option

Note: Bulk ACU creation is not supported for the Access Control Core that connects to third-party Mercury™ intelligent controllers and subpanels. These ACUs must created one at a time.

1. Go to control.openpath.com/login and sign in. For access in the EU, go to control.eu.openpath.com/login.
2. Go to **Administration** > **Quick start**.
3. Enter a **Site name** and any other relevant site information.
    a. In **Site language**, select the preferred language for the site-wide emails sent by the system.
    b. Click **Next**.
4. Enter the number of controllers located at your site and:
    a. Enter names for the controllers.
    b. In **Controller type**, select the type used:
        - **First generation - Red Board (OP-AS-01)** — For first generation Smart Hubs.
        - **Single Door Controller (SDC)**

          Note: Expansion board connections are not applicable to SDCs.
        - **Core series ACU** — For Core Series Smart Hubs.

    c. If your ACU also connects to an expansion board, add the appropriate types in EXPANSION BOARDS:
        - **Openpath 4-Port Expansion**
        - **Openpath 8-Port Expansion**
        - **Openpath 16-Port Elevator**

      Tip: The Avigilon (formerly, Openpath) boards are most common with the Core Series Smart Hub.
5. Enter the number of readers connected to the controllers. Enter their names and click **Next**.
6. Review your site details and click **Confirm & submit**. It may take a few minutes for setup to complete.

Add one ACU or SDC

1. Go to Devices > ACUs.
2. To add a new ACU or SDC, click the + button in the upper-right corner.
3. Enter a unique name for the ACU or SDC.
4. In **Controller type**, select the type used:
    - **First generation - Red Board (OP-AS-01)** — For first generation Smart Hubs.
    - **Single Door Controller (SDC)**

      > **Note:** Expansion board connections are not applicable to SDCs.

    - **Core series ACU** — For Core Series Smart Hubs.
5. If your ACU also connects to an expansion board, add the appropriate types in EXPANSION BOARDS:

    > **Tip:** The Avigilon (formerly, Openpath) boards are most common with the Core Series Smart Hub. The Mercury boards are applicable only to ACUs.

    - **Mercury LP1501**
    - **Mercury LP1501 (With Downstream)**
    - **Mercury LP1502**
    - **Mercury LP2500**
    - **Mercury MP1501**
    - **Mercury MP1501 (With Downstream)**
    - **Mercury MP1502**
    - **Mercury MP2500**

    > **Note:** For the Mercury controller board, enter also their unique **IP address** and **Network port** (default is `3001`). **TLS Enabled (Recommended)** is enabled by default.
    >
    > If you select **Mercury MP1501 (With Downstream)** or **Mercury LP1501 (With Downstream)**, ensure the baud rate matches the baud rate on the physical board (default is `38400`).

6. Click **Add board**. The newly added Mercury board is disabled by default.
    a. When you are ready to open communication to the Mercury board, ensure it is disconnected from any previous access control system.
    b. In the ENABLE column, select **Enabled** for the selected board.

⚠ **Caution:** The previous configuration on the legacy access control system will be overwritten.

7. If you have additional subpanels, click **Add board** again and add the appropriate types in EXPANSION BOARDS.

    - **Mercury MR16IN-S3**
    - **Mercury MR16OUT-S3**
    - **Mercury MR50-S3**
    - **Mercury MR52-S3**

Note: For the Mercury readers and panels, enter also the **Port** and **RS-485 address** (supported range is `0 – 31`).

8. Optional. To connect your network to the Cloud using a static IP address and port on an allowlist, select the **Enable Static Cloud IP** toggle. Default port is 443.

Note: An Enterprise plan is required to use Static Cloud IP.

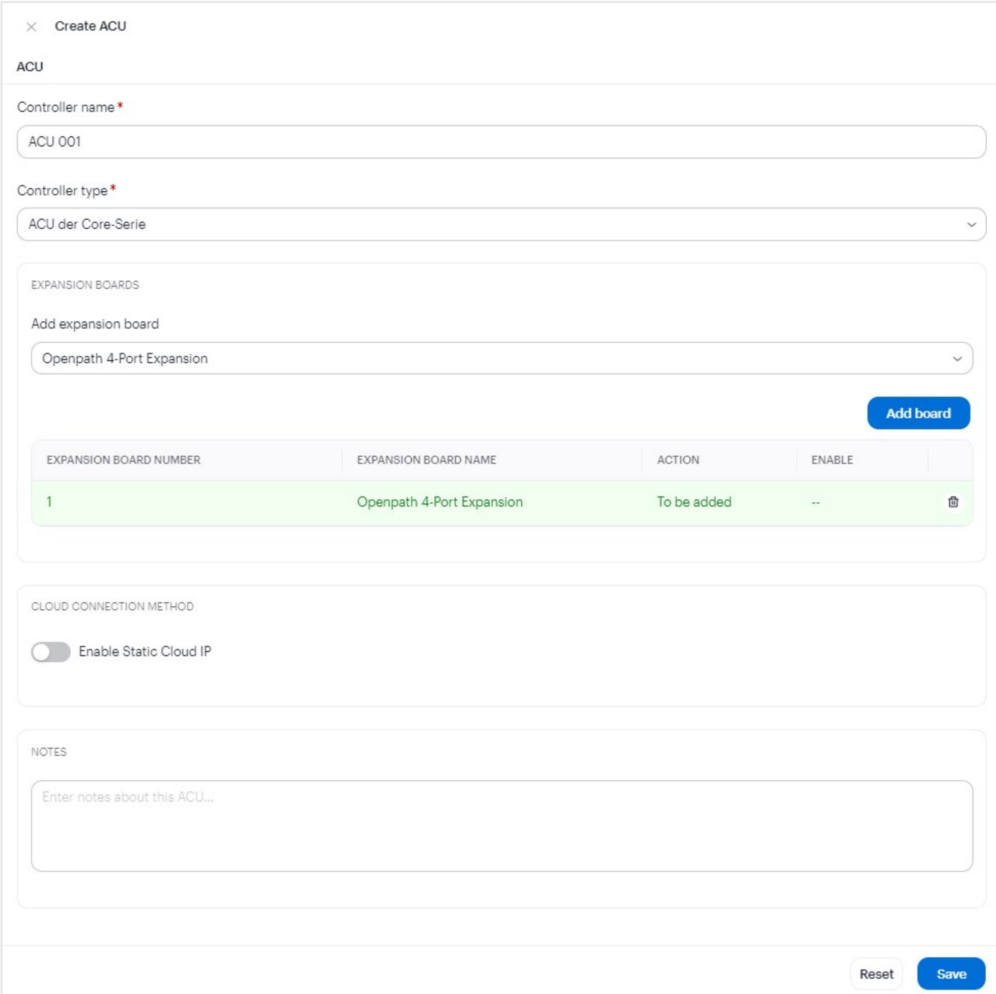
    a. Go to **App marketplace** and ensure the **Static Cloud IP** app is installed.

    b. After the toggle is enabled in Alta Access, open the Alta Access mobile app and select **Provision with Static Cloud IP** to provision the devices.

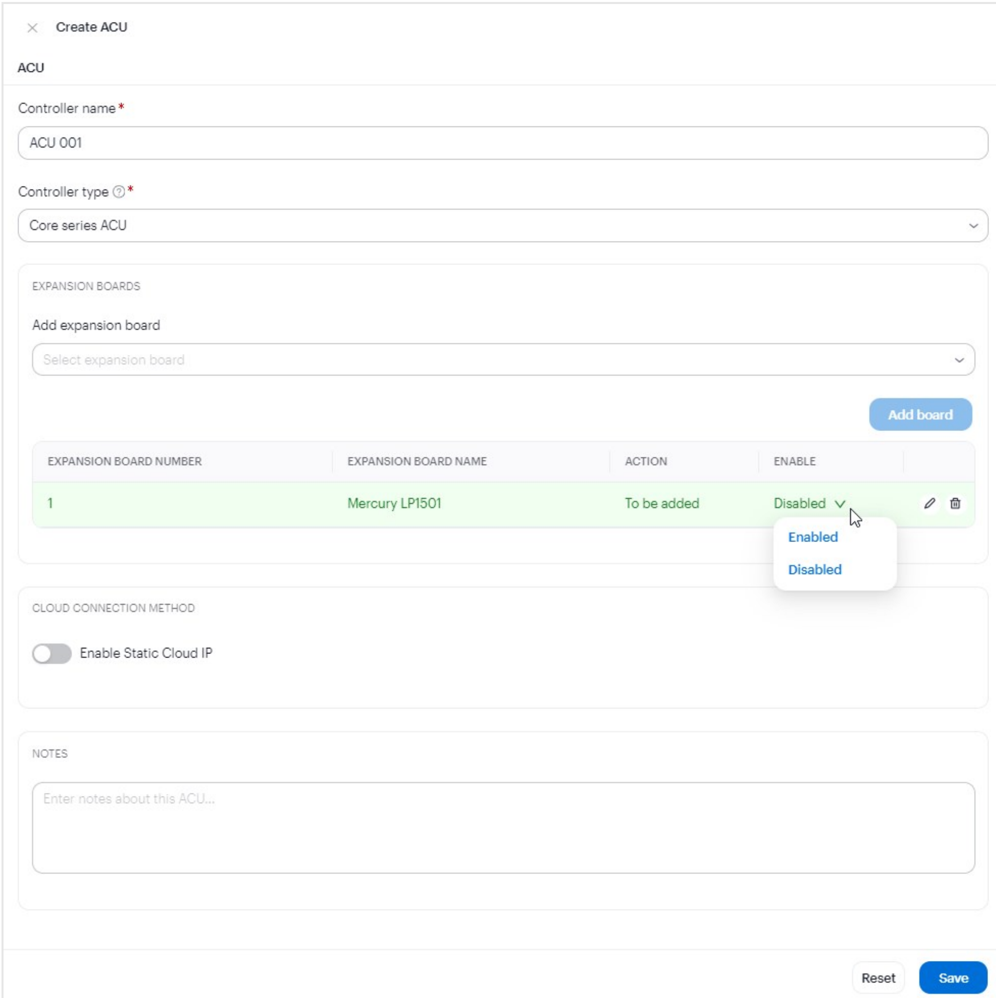
9. Click **Save**.

Note: If you are saving a new Mercury expansion board, Access Control Core firmware will automatically download and install for up to 30 minutes, depending on network speed.

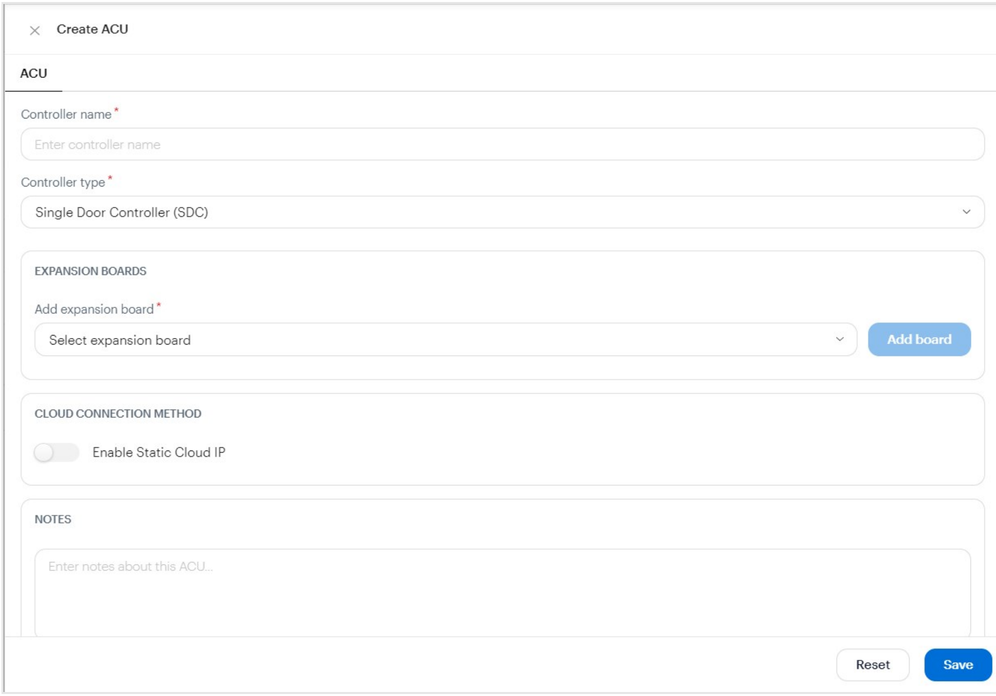
Example: Avigilon expansion board connected to an ACU



Example: Mercury expansion board connected to an ACU



Example: Single Door Controller

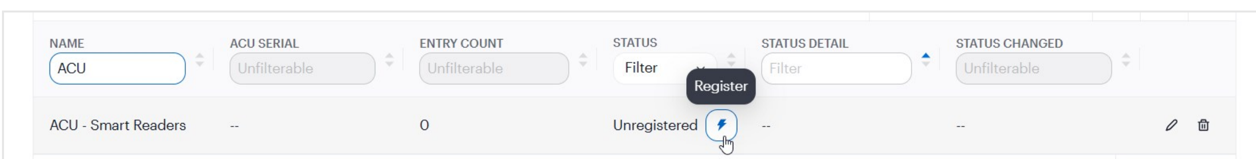


Register ACU or SDC in Alta Access web browser

The ACU or SDC is registered in Alta Access during provisioning.

> **Tip:**
> Using the Alta Access mobile app is recommended, which automatically creates and provisions the ACU in Alta Access and adds any connected devices. For more information, see this Alta Access article.

1. On the ACUs page, click **Register**.



2. In the Register ACU popup, click **Yes**.
3. Click **Provision** in the window popup.

> **Note:**
> The laptop must be on the same network as the ACU. If you have a VLAN, make sure the laptop is on the same VLAN as the ACU.
>
> If you are using a laptop running Microsoft™ Windows or Linux®, you must download the iTunes app. The provisioning process uses Bonjour software that comes with iTunes. Optionally, you can download iTunes and use an archive utility to extract and install only the Bonjour MSI.

4. If the `This site can't be reached` error is displayed, you need to ping the ACU using the command line:

   a. Open a command prompt and run:

      - On Windows: `ping oppi.local`
      - On Mac or Linux: `ping -c4 oppi.local`

        If nothing returns, check your network requirements.

   b. You should see the ACU's IP address, either in IPv4 or IPv6 format. Copy the address and return to the error page.

   c. In the URL, delete everything before `:8080`.

      - If using an IPv4 address, paste before `:8080`. For example: `192.0.2.0:8080`
      - If using an IPv6 address, delete the last two digits and the percentage sign, put square brackets outside the address, and paste before `:8080`.

        Correct: `a123::b456:5a18:eb8f:7fd6:8080`

        Incorrect: `a123::b456:5a18:eb8f:7fd6%29:8080`

   d. Press **Enter** and then click the **Provision** button.

      - If the Provision button doesn't appear, contact Avigilon Alta Support at (844) 673-6728 Ext 2 or support@openpath.com.

Disable the Static Cloud IP connection

If it is necessary to disable the Static Cloud IP connection:

- Go to the Edit ACU page, and deselect the **Enable Static Cloud IP** toggle.

  Normal cloud operation resumes after the Static Cloud IP connection is disabled.

Add expansion boards

You need to edit ACUs when you install additional expansion boards in existing Smart Hubs or third-party Mercury controllers.

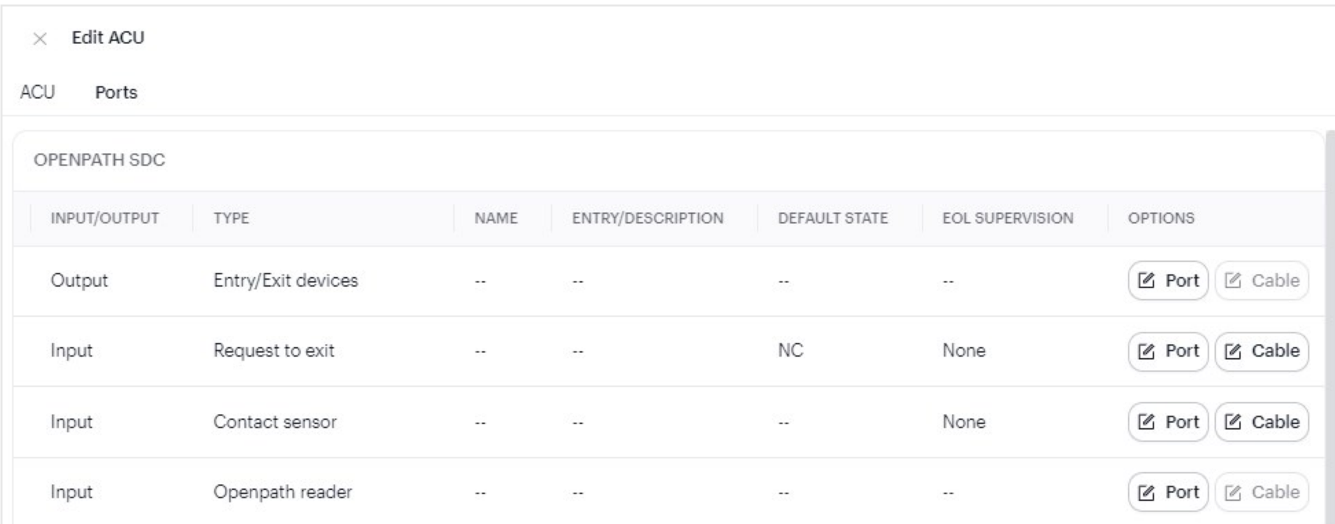
1. To edit an ACU, click on the ACU from the **ACUs** page.
2. From **Add expansion board**, select and add the expansion board.

   For a Mercury controller: If you have additional subpanels, click **Add board** again and add the appropriate types.
3. Click **Save**.

Edit ACU ports

- On the Edit ACU page, click the **Ports** tab to view and manage ACU ports.

> **Tip:** Scroll down and then scroll right to view the OPTIONS column.



Input type

1. Click the **Port** icon.
2. For an Avigilon board, click **Input type** to change a **Contact sensor**, **Openpath reader**, **Request to exit** device, **Wiegand device**, or **Generic input** to a different input type.

   For a Mercury board, click **Input type** to select **Contact sensor**, **Generic input**, or **Request to exit** device.

   This can be used for creating rules. See Rules on page 146.

   > **Note:** Inputs cannot be changed if they are already assigned to an entry.
3. Click **Save**.

End-of-line supervision

The Single Door Controller and Core Series Smart Hub support end-of-line (EOL) supervision.

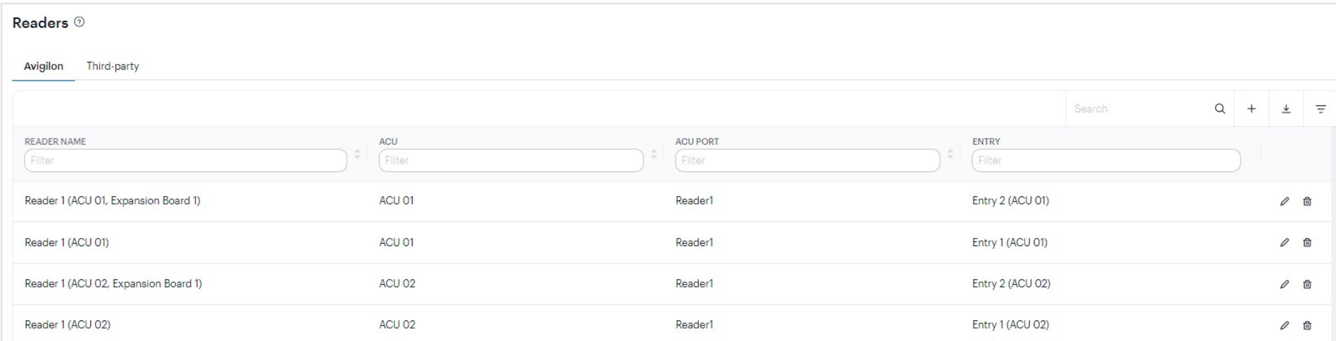
1. Click the Cable icon.
2. Select the appropriate **End of line supervision** setting — **None**, **Cut Line Detect**, **Line Shorted Detect**, or **Both**.

   Note: The setting selected must match your physical wiring configuration. See the Alta Access installation guide for more information.

3. Click **Save**.

Reader management

The Readers page is where you can view and manage readers.



Export information to CSV

- Click the icon.

Show, hide, or reset information

- Click the icon to show or hide information in columns.
- Click **Reset table** to go back to the default view.

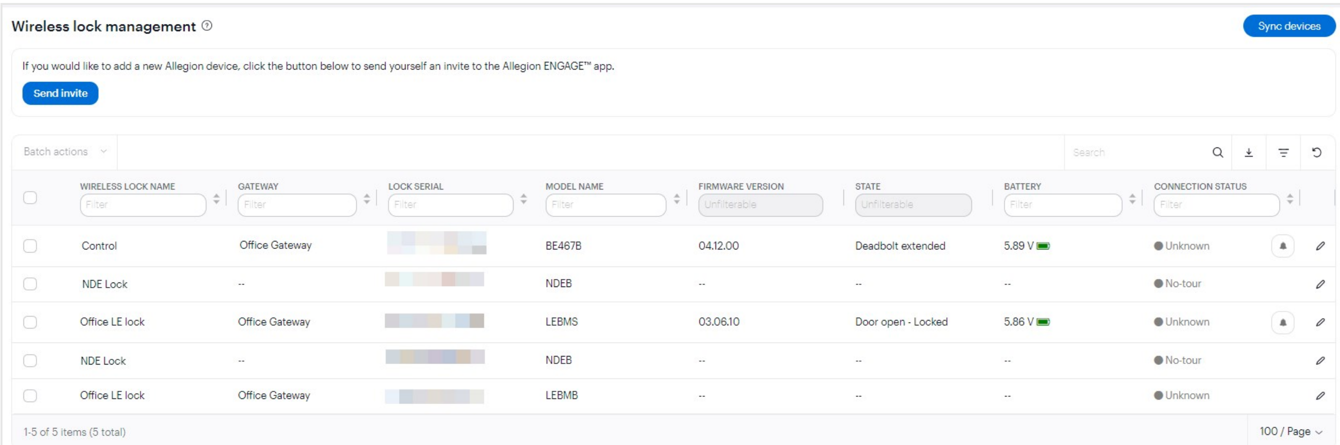
Add reader

1. Go to **Devices** > **Readers**.
2. Click the button in the upper-right corner.
3. Enter a name for the reader.

   Names are usually relevant to the location where the reader is installed.
4. Select the ACU that will control the reader.
5. Select the port to which this reader is wired.
6. Click **Save**.

Wireless lock management

The Wireless lock management page is where you can view and manage wireless locks that are connected to gateways or without gateways.



For more information about the Schlage® no-tour wireless locks, see the Avigilon Access Control System Integration Guide for Schlage Wireless Locks No-Tour (link).

Update lock firmware

1. Enter a checkmark next to one or more locks.
2. Click **Batch actions** to select **Update firmware**.

> **Note:** To update the firmware of Schlage no-tour wireless locks, use the Alta Access mobile app to update and sync the locks with Alta Access.

Edit locks

> **Note:** Settings are dependent on the lock model and configuration. To configure the following wireless lock function, set it during the commissioning process or post-installation using the Schlage ENGAGE mobile app (and not the Alta Access mobile app):
>
> - Apartment mode — Supported in LEB and NDEB series locks only. Ensures the gateway-connected or no-tour connected lock remains open or closed, when the credential is scanned. The door doesn't automatically relock when unlocked, and thus, lock out the user.
>
>   Accept the 'Openpath does not support Toggle Credential' message during initial configuration. For more information, see the Schlage ENGAGE documentation.

Configure NDEB or LEB locks

1. Go to **Wireless locks** and select the lock.
2. In BASIC SETTINGS, set any of the following:
   - **Power Failure Mode** — Determines how the lock behaves when the battery fails.
     - **As Is** — Lock remains in the same state.
     - **Safe** — Lock is unlocked.
     - **Secure** — Lock is locked.
   - **Beeper Enabled** — Beeping is emitted from the lock when a credential is scanned.
   - **Invalid Card Audit** — Generates an event when an unknown (invalid) card is presented to the NDEB wireless lock. To view these events, go to **Reports** > **Activity logs** or **Dashboards** > **Activity dashboard**.
3. In READER SETTINGS, set the type of card and fob credentials supported by the lock.
   - For Openpath DESFire EV1, EV2, and EV3, select **14443 UID (CSN)**.
   - For Openpath DESFire EV3-A and Avigilon DESFire EV3-B, select **14443 Secure Mifare**.

   > **Note:** You cannot enable 14443 UID (CSN) and 14443 Secure Mifare, 14443 Secure Mifare Plus, and 14443 EV1 (NOC) at the same time.

4. In MOBILE CREDENTIAL, choose whether to enable mobile credentials on this lock.
   - **Communication Range** — Adjust to determine how close the mobile credential needs to be near the lock before appearing as a nearby entry in the Alta Open mobile app.
   - **Performance** — Adjust to determine how often the mobile app scans for locks.
5. Click **Save**.

Configure Control locks

1. From **Wireless locks**, select the lock.
2. Under BASIC SETTINGS, you can do the following:
   - **Beeper Enabled** — Beeping is emitted from the lock when a credential is scanned.
   - **Invalid Card Audit** — Generates an event when an unknown (invalid) card is presented to the NDEB wireless lock. To view these events, go to **Reports** > **Activity logs** or **Dashboards** > **Activity dashboard**.

> **Note:** Reader settings cannot be edited on Control locks; high frequency cards and fobs are enabled by default.

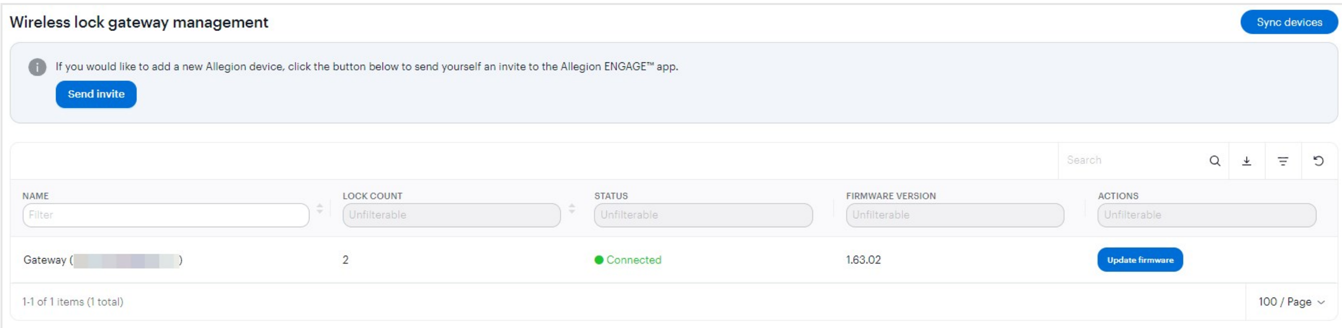
3. In MOBILE CREDENTIAL, choose whether to enable mobile credentials on this lock.
    - **Communication Range** — Adjust to determine how close the mobile credential needs to be near the lock before appearing as a nearby entry in the Alta Open mobile app.
    - **Performance** — Adjust to determine how often the mobile app scans for locks.

Configure Schlage no-tour wireless locks

1. Select a lock and edit the name or serial number.
2. Click **Save**.

Wireless lock gateway management

The Wireless lock gateways page provides the list of gateways synced using the Allegion ENGAGE app. From here, you can sync gateways and update firmware.



Sync gateways with Alta Access

- After completing the ENGAGE commissioning procedures, click **Sync devices**.

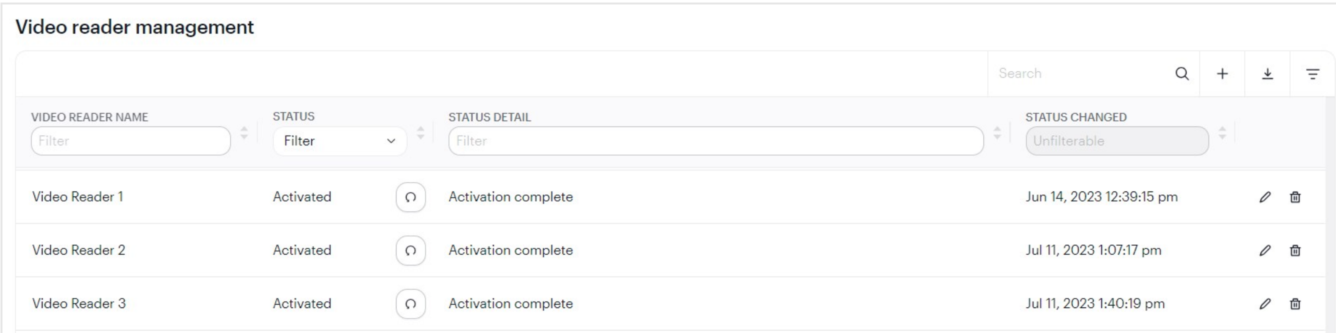
  The gateways are displayed with their connection status and details.

Update gateway firmware

- Click **Update firmware**.

Video reader management

You can view and manage Video Reader Pro devices on the Video readers page.



Export information to CSV

- Click the icon.

Show, hide, or reset information

- Click the icon to show or hide information in columns.
- Click **Reset table** to go back to the default view.

Add video reader

1. Go to **Devices** > **Video readers**.
2. Click the button in the upper-right corner.
3. Enter a name for the reader.
4. If Wiegand wiring is used to connect to existing legacy systems, select the **Standalone Mode** toggle.

   > **Note:** Alta Access licenses and internet access are not required. For more information, see this Alta Access article.*

5. In the CLOUD VIDEO STORAGE section, select a plan length.

   > **Note:** A cloud video storage license is required to view the video recordings.

---

*For more information, see:
https://openpath.atlassian.net/servicedesk/customer/portal/16/article/1668284452?src=1724573529

The DETAILS section (read-only) displays information only after the reader is provisioned.

6. In the SETTINGS section:

    - **Tamper sensor** — Enable (default) or disable the recording of Tamper Detected events when the reader is touched or moved.
    - **Tamper sensor sensitivity** — Adjust lower or higher, depending on your needs.

    > **Note:** A higher sensitivity level may produce false tamper events, for example, when someone triggers a Touch to Unlock.

7. Click **Save**.
8. On the **Ports** tab, click the **Port** button to view and manage reader, relay, and Wiegand port settings.

For next steps:

- Add zones on page 68 if not created yet.
- Add entries on page 72 and enter the device in the Controller field.

  > **Note:** During this step, you can configure the Wiegand port on the video intercom reader, as an input or output, for Mobile Gateway mode.

- Installing the Video Reader Pro / Video Reader Intercom Pro or the Avigilon Access Control Core Installation Guide (link)

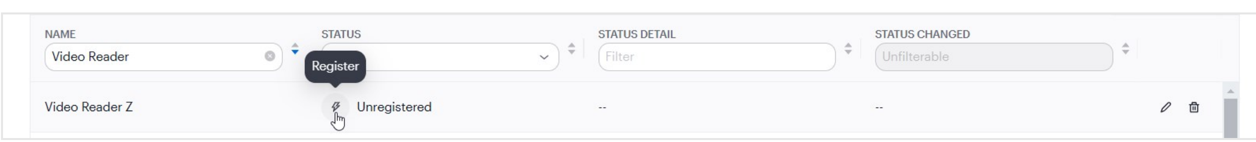
After provisioning, return to Alta Access to finish configuring video settings or to enable ONVIF[1].

Register video reader in Alta Access web browser

The Video Reader Pro is registered as an ACU during provisioning.

> **Tip:**
> Using the Alta Access mobile app is recommended, which automatically creates and provisions the ACU in Alta Access and adds any connected devices. For more information, see this Alta Access article.

1. On the Video readers page, click **Register**.



2. In the Register ACU popup, click **Yes**.
3. Click **Provision** in the window popup.

[1]ONVIF is a trademark of Onvif, Inc.

> **Note:**
> The laptop must be on the same network as the ACU. If you have a VLAN, make sure the laptop is on the same VLAN as the ACU.
>
> If you are using a laptop running Microsoft™ Windows or Linux®, you must download the iTunes app. The provisioning process uses Bonjour software that comes with iTunes. Optionally, you can download iTunes and use an archive utility to extract and install only the Bonjour MSI.

4. If the `This site can't be reached` error is displayed, you need to ping the ACU using the command line:

    a. Open a command prompt and run:

    - On Windows: `ping oppi.local`
    - On Mac or Linux: `ping -c4 oppi.local`

      If nothing returns, check your network requirements.

    b. You should see the ACU's IP address, either in IPv4 or IPv6 format. Copy the address and return to the error page.

    c. In the URL, delete everything before `:8080`.

    - If using an IPv4 address, paste before `:8080`. For example: `192.0.2.0:8080`
    - If using an IPv6 address, delete the last two digits and the percentage sign, put square brackets outside the address, and paste before `:8080`.

      Correct: `a123::b456:5a18:eb8f:7fd6:8080`

      Incorrect: `a123::b456:5a18:eb8f:7fd6%29:8080`

    d. Press **Enter** and then click the **Provision** button.

    - If the Provision button doesn't appear, contact Avigilon Alta Support at (844) 673-6728 Ext 2 or support@openpath.com.

View activated video reader

1. After provisioning the physical reader, return to Alta Access to view the activated device in the DETAILS section.

2. Finish configuring video settings or to enable ONVIF.

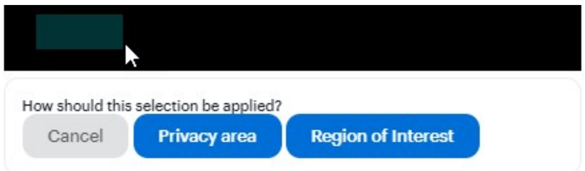
Configure recording, detection, and ONVIF settings

1. Go to **Devices** > **Video readers**, and select a reader.
2. Select the **Video** tab.
   - In the VIDEO PROPERTIES section:
     - **Quality** — **High**, **Medium**, or **Low** quality.
     - **Brightness**, **Contrast**, **Saturation**, and **Sharpness** — Adjust as necessary.
     - **Wide Dynamic Range (WDR)** — Disable (default) or enable to adjust for backlighting and other extreme lighting conditions.
     - **Night mode** — **Auto (default)**, **Always on**, or **Always off**.
     - **Anti-overexposure** — Enable (default) to reduce IR glare on persons and objects approaching the video reader.
   - In the DETECTION SETTINGS section:
     - **Enable motion detection** — Enable (default) or disable to adjust the sensitivity settings of motion detection by the camera.

- **Enable QR code recognition** — Enable or disable (default) QR code detection by the camera when a user presents a third-party QR code before entry. To set up the action taken when a QR code is detected by the camera, see Add rules and triggers on page 146.

  > **Note:** A Premium or Enterprise license is required.

- In the live video feed, draw a box on the feed to add privacy areas or regions of interest.

  Privacy area — Hides sensitive areas of the feed from users.

  Region of interest — Applies motion detection to only the marked areas.

- In the RECORDING SETTINGS section:
  - **Burn current time into recordings** and **Burn camera name into recordings** — Enable (default) or disable the settings.

3. Click **Save**.

Enable ONVIF

Enable ONVIF[1] if you are exporting video to a third-party VMS.

1. On the Video tab, select the **Enable ONVIF** toggle (off by default).
2. Click **Open camera UI**.

   > **Note:** For best results, use Chrome, Firefox, or Microsoft Edge.

3. Log in using the default username and password.

   > **Important:** You must be logged in on the same LAN as the camera.

4. Go to **Configurations** > **Security** > **User accounts** to change the password.

   > **Note:** Alta Access always displays the default password, even if you change the password in the Open camera UI page. To reset the password back to the default, disable ONVIF, wait 10 seconds, then enable again.

[1] ONVIF is a trademark of Onvif, Inc.

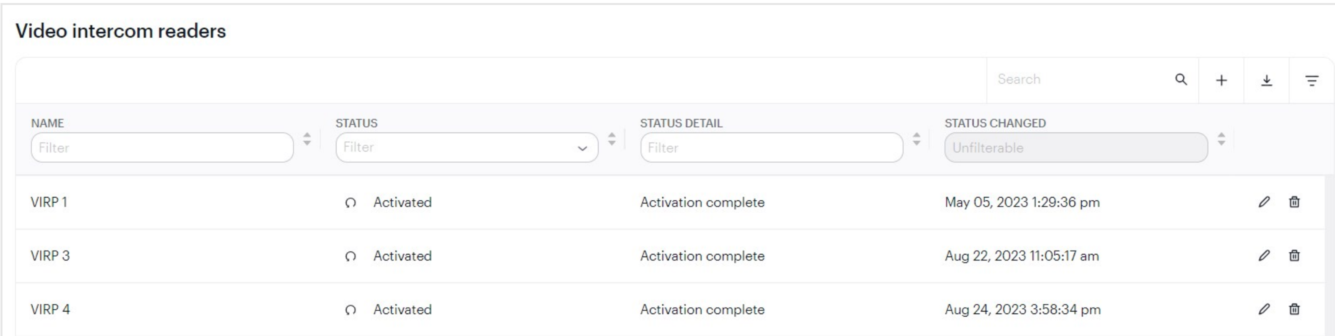
Change cloud video storage plan

You can change your cloud video storage plan length, however, plans are not retroactive. For example, if you are currently on a 30-day plan and you switch to an 180-day plan, you'll still only have access to the past 30 days of clips with 180 days of storage moving forward.

1. Go to **Devices** > **Video readers**, and select the video reader.
2. In CLOUD VIDEO STORAGE, select a different plan length.
3. Click **Save**.

Video intercom reader management

You can view and manage Video Intercom Reader Pro devices on the Video intercom reader management page, including configuring two-way audio and call routing to building occupants, and more.



Export information to CSV

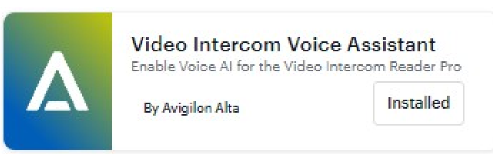
- Click the icon.

Show, hide, or reset information

- Click the icon to show or hide information in columns.
- Click **Reset table** to go back to the default view.

Add video intercom reader

Note: Before you start, go to the App marketplace and install the Video Intercom Voice Assistant app.



1. Go to **Devices** > **Video intercom readers**.
2. Click the button in the upper-right corner.
3. Enter a name for the device.
4. In the CLOUD VIDEO STORAGE section, select a plan length.

   Note: A cloud video storage license is required to view the video recordings.

The DETAILS section (read-only) displays information only after the reader is provisioned.

5. In the SETTINGS section:

   - **Tamper sensor** — Enable (default) or disable the recording of Tamper Detected events when the reader is touched or moved.
   - **Tamper sensor sensitivity** — Adjust lower or higher, depending on your needs.

   > **Note:** A higher sensitivity level may produce false tamper events, for example, when someone triggers a Touch to Unlock.

6. Click **Save**.

7. On the **Ports** tab, click the **Port** button to view and manage reader, relay, and Wiegand port settings.

For next steps:

- Add zones on page 68 if not created yet.
- Add entries on page 72 and enter the device in the Controller field.

  > **Note:** During this step, you can configure the Wiegand port on the video intercom reader, as an input or output, for Mobile Gateway mode.

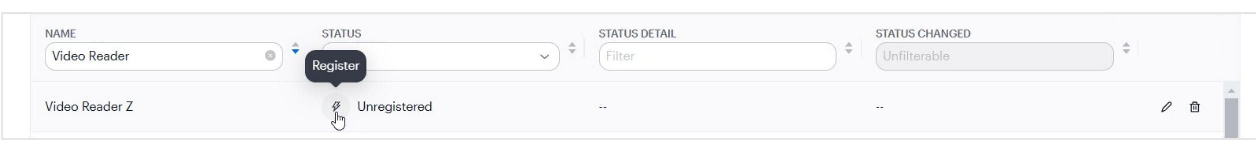
- Installing the Video Reader Pro / Video Reader Intercom Pro or the Avigilon Access Control Core Installation Guide (link)

Register video intercom reader in Alta Access web browser

The Video Intercom Reader Pro is registered as an ACU during provisioning.

> **Tip:**
> Using the Alta Access mobile app is recommended, which automatically creates and provisions the ACU in Alta Access and adds any connected devices. For more information, see this Alta Access article.

1. On the Video intercom readers page, click **Register**.



2. In the Register ACU popup, click **Yes**.

3. Click **Provision** in the window popup.

> **Note:**
> The laptop must be on the same network as the ACU. If you have a VLAN, make sure the laptop is on the same VLAN as the ACU.
>
> If you are using a laptop running Microsoft™ Windows or Linux®, you must download the iTunes app. The provisioning process uses Bonjour software that comes with iTunes. Optionally, you can download iTunes and use an archive utility to extract and install only the Bonjour MSI.

4. If the `This site can't be reached` error is displayed, you need to ping the ACU using the command line:

   a. Open a command prompt and run:

      - On Windows: `ping oppi.local`
      - On Mac or Linux: `ping -c4 oppi.local`

      If nothing returns, check your network requirements.

   b. You should see the ACU's IP address, either in IPv4 or IPv6 format. Copy the address and return to the error page.

   c. In the URL, delete everything before `:8080`.

      - If using an IPv4 address, paste before `:8080`. For example: `192.0.2.0:8080`
      - If using an IPv6 address, delete the last two digits and the percentage sign, put square brackets outside the address, and paste before `:8080`.

        Correct: `a123::b456:5a18:eb8f:7fd6:8080`

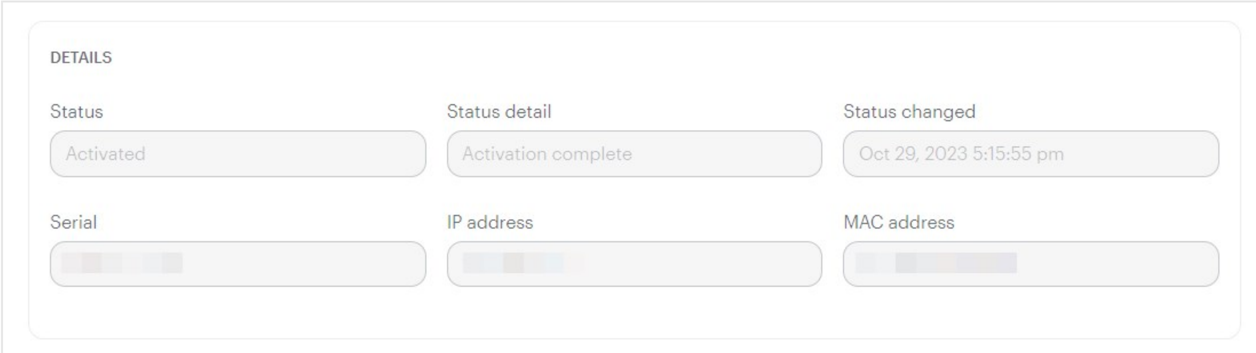
        Incorrect: `a123::b456:5a18:eb8f:7fd6%29:8080`

   d. Press **Enter** and then click the **Provision** button.

      - If the Provision button doesn't appear, contact Avigilon Alta Support at (844) 673-6728 Ext 2 or support@openpath.com.

View activated video intercom reader

1. After provisioning the physical reader, return to Alta Access to view the activated device in the DETAILS section.



2. Finish configuring video settings, intercom and routing profile settings, or to enable ONVIF.

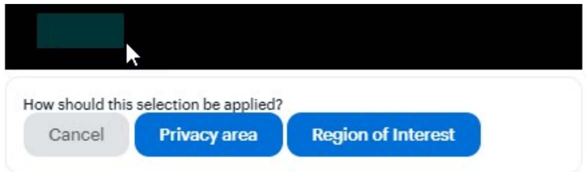
Configure recording, detection, and ONVIF settings

1. Go to **Devices** > **Video intercom readers**, and select a reader.
2. Select the **Video** tab.
   - In the VIDEO PROPERTIES section:
     - **Quality** — **High**, **Medium**, or **Low** quality.
     - **Brightness**, **Contrast**, **Saturation**, and **Sharpness** — Adjust as necessary.
     - **Wide Dynamic Range (WDR)** — Disable (default) or enable to adjust for backlighting and other extreme lighting conditions.
     - **Night mode** — **Auto (default)**, **Always on**, or **Always off**.
     - **Anti-overexposure** — Enable (default) to reduce IR glare on persons and objects approaching the video reader.

   In the DETECTION SETTINGS section:
     - **Enable motion detection** — Enable (default) or disable to adjust the sensitivity settings of motion detection by the camera.
     - **Enable QR code recognition** — Enable or disable (default) QR code detection by the camera when a user presents a third-party QR code before entry. To set up the action taken when a QR code is detected by the camera, see Add rules and triggers on page 146.

       > **Note:** A Premium or Enterprise license is required.

     - In the live video feed, draw a box on the feed to add privacy areas or regions of interest.



Privacy area — Hides sensitive areas of the feed from users.

Region of interest — Applies motion detection to only the marked areas.

- In the RECORDING SETTINGS section:
    - **Burn current time into recordings** and **Burn camera name into recordings** — Enable (default) or disable the settings.

3. Click **Save**.

Enable ONVIF

Enable ONVIF[1] if you are exporting video to a third-party VMS.

1. On the Video tab, select the **Enable ONVIF** toggle (off by default).
2. Click **Open camera UI**.

> **Note:** For best results, use Chrome, Firefox, or Microsoft Edge.

3. Log in using the default username and password.

> **Important:** You must be logged in on the same LAN as the camera.

4. Go to **Configurations** > **Security** > **User accounts** to change the password.

> **Note:** Alta Access always displays the default password, even if you change the password in the Open camera UI page. To reset the password back to the default, disable ONVIF, wait 10 seconds, then enable again.

Change cloud video storage plan

You can change your cloud video storage plan length, however, plans are not retroactive. For example, if you are currently on a 30-day plan and you switch to an 180-day plan, you'll still only have access to the past 30 days of clips with 180 days of storage moving forward.

1. Go to **Devices** > **Video intercom readers**, and select the video reader.
2. In CLOUD VIDEO STORAGE, select a different plan length.
3. Click **Save**.

---

[1]ONVIF is a trademark of Onvif, Inc.

Configure intercom settings and two-way audio

On the Intercom tab of a Video Intercom Reader Pro, you can configure two-way audio communication.

Welcome greeting and message

- In the CONFIGURATION section, enter:
    - **Language** — The language spoken to and replied from the video intercom:
        - **English (North America)**
        - **French (France)**
        - **German (Germany)**
        - **Italian (Italy)**
        - **Polish (Poland)**
        - **Spanish (Mexico)**
        - **Spanish (Spain)**
    - **Default message** — Plays if no user routing profiles have been added.
    - **Initial greeting** — Plays when a guest presses the intercom call button.
    - **Skip greeting for front desk** — Skips the initial greeting and forwarding message if the only routing profile active is **Front Desk Connect**. When visitors press the call button, front desk users will be notified immediately.

> **Note:** The default message and initial greeting have a maximum 130-character limit each.

Microphone and speaker settings

- In the AUDIO section, MICROPHONE section, enter:
    - **Enabled - always on** — Audio is 'on' during intercom calls and in the live video feed.
    - **Enabled - On during intercom events** — Audio is 'on' during intercom calls only.
    - **Disabled** — Audio is disabled.
    - **Microphone level** — Adjust lower or higher, as needed.
    - **Audio recording** toggle — Enable to record audio during intercom events.
- SPEAKER section, enter:
    - **Speaker enabled** — Adjust the speaker volume, lower or higher, as needed.
    - **Privacy** — Deselect the toggle, as needed.
    - **Audio detection** toggle — Enable to detect audio when the microphone is always on. Adjust the detection sensitivity, lower or higher, as needed.

SIP mode

For SIP enabled and Voice over IP (VoIP) devices.

For information about the installation and configuration of your PBX software and VoIP phone systems, see third-party vendor documentation.

- In the SIP section, enter:
  - **SIP mode** — Change **SIP disabled** (default) to **SIP only** to use SIP or **SIP failover** to use SIP only during internet outages.

    > **Note:** When SIP is enabled on the video intercom reader, the voice assistant will be disabled.

  - **SIP address** — The IP address of the PBX software.
  - **Authentication user** — The extension number for the video intercom reader (for example, 5555).
  - **Authentication password** — The password for the extension number for the video intercom reader.
  - **Display name** (optional) — The caller ID to be displayed on the video intercom reader (for example, OP intercom).
  - **ID/Call destination** — The extension number for the VoIP phone system.
  - **Device SIP number** — The extension number for the video intercom reader. Use the same value in **Authentication user**.

Configure call routing to users, units, or front desk

On the Routing profile tab of a Video Intercom Reader Pro, you can configure the call routing profiles used by the voice assistant to find users, units, or the front desk.

> **Note:** Ensure you are added to an active routing profile to receive notifications in Alta Access.

Before you start

- Create access groups and access schedules for the Direct Connect profile.

  > **Note:** This step is required for all routing profiles.

- Add building details and zones for multi-tenants for the Unit Connect profile.

Add existing routing profile

1. Click the + button in the upper-right corner.
2. Select the **Use existing profile** toggle.
3. In **Intercom profile**, select an existing profile.
4. Click **Save**.

Add new routing profile

1. Click the + button in the upper-right corner.
2. Leave the **Use existing profile** toggle deselected.
3. In the PROFILE CONFIGURATION section, enter the name of the profile. In **Profile type**, select:
   - **Direct Connect** — Visitors call users by stating their name.
   - **Front Desk Connect** — Visitors call a group of users designated as the Front Desk.
   - **Unit Connect** — Visitors call one or more users by stating the unit or apartment number. For more information, see Building management on page 66.
   - **Visual Voicemail** — Visitors may leave a voicemail to be seen by a site administrator.
4. In the RECIPIENT CONFIGURATION section, enter the access groups that can be searched by name at the intercom.
5. In the BACKUP CONFIGURATION section, enter the timeout in seconds before using the fallback profile when the recipient can't be reached.

   For example, if a visitor can't reach a user (Direct Connect) after 15 seconds, the visitor will hear the **Farewell message**.
6. Click **Save**.

Use QR codes to look up user directories on phones (optional)

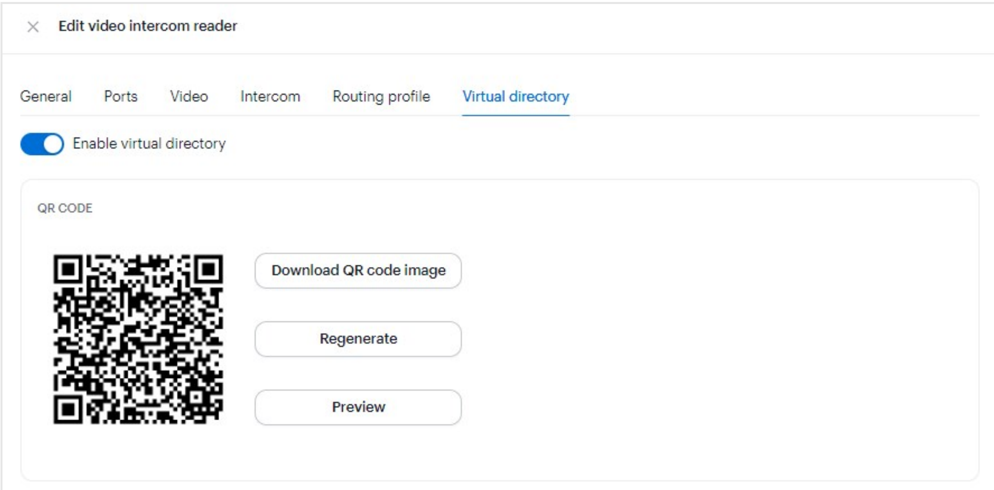
On the Virtual directory tab of a Video Intercom Reader Pro, you can generate and print a QR code that visitors can scan to look up a user directory on their phone and then tap the icon to speak to the user or unit through the intercom. If nobody answers, they can leave a voicemail message (if enabled) or tap **Front desk** to let them in.

Figure 1 Overview of QR code placement (a), QR code scanning and user directory retrieval (b), and intercom communication (c)

Create user directory and/or unit directory

Before you start, ensure the Direct Connect and/or Unit Connect settings are defined on the **Routing profile** tab, as described in the previous section.

Generate QR code



1. Select the **Enable virtual directory** toggle (deselected by default).

   A QR code is generated and additional fields are shown.

2. In **Directory title**, enter the title of the user directory.

   Example: "Welcome to our building"

3. In **Notes for visitors**, enter instructions.

   Example: "Select the person from the directory to initiate a call with them through the intercom"

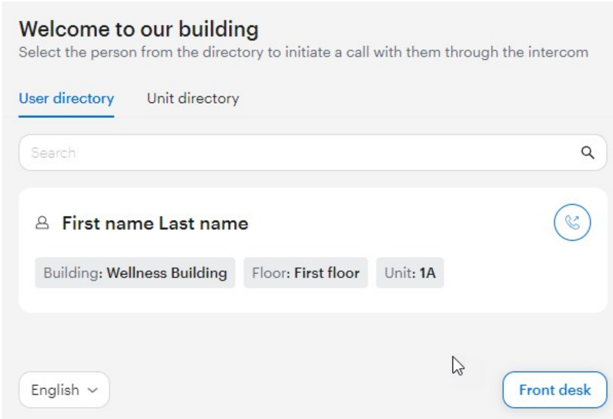
4. In **User directory values to display**, enter the user directory values.

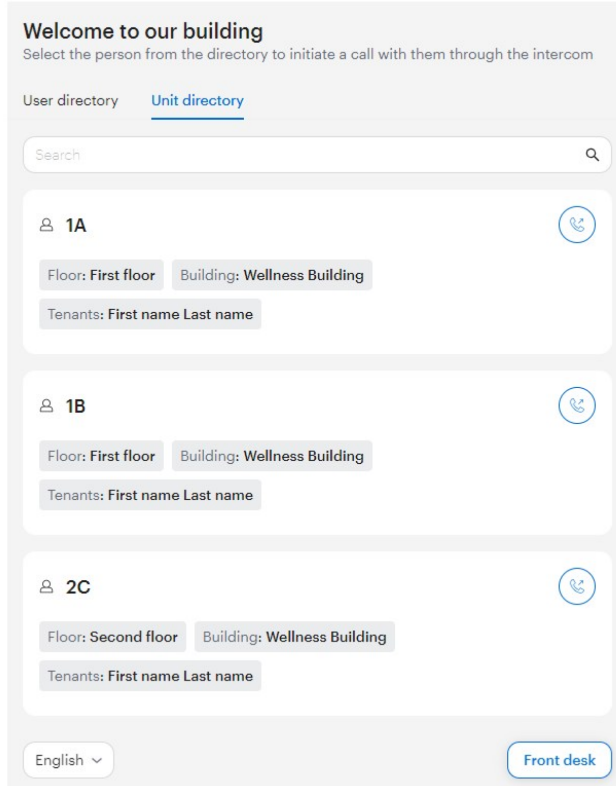
   Examples: "Building, Floor, Unit"

5. In **Unit directory values to display**, enter the unit directory values.

   Examples: "Floor, Tenant"

6. Click **Save** and then **Preview** to preview the user and unit directories (example below).





Tip: If the preview window expires, click **Preview** again to redisplay the directories.

Download and print QR code

1. When you are satisfied with the preview, click **Download QR code image**.
2. Find the JPG file in the Downloads folder on your desktop.
3. Incorporate the QR code into signage to be placed near the Video Intercom Reader Pro.

Tip: Printing the QR code onto a waterproof sticker is recommended. You may find ready-to-use labels and templates at your local supplier.

Regenerate QR code

1. Click **Regenerate** and confirm the operation.

Note: Regenerating the QR code will delete the former QR code.

2. Download and reprint the new QR code.

Disable directory

1. Deselect the **Enable virtual directory** toggle.
2. Click **Delete** to confirm the operation.

   > **Note:** Disabling the directory will delete it.

View live video feed

After provisioning the Video Intercom Reader Pro, you can view live video feed from the device in several places.

> **Note:** A cloud video storage license is required to view the video recordings.

- Go to **Devices**, select the video intercom reader, and then the **Video** tab.
- Go to **Dashboards** and select the **Activity dashboard**.
- Go to **Cameras** page and select the video intercom reader. See Initiate calls to intercom on Video Intercom Reader Pro on page 41 and Play and download video on page 41.

Answer calls from intercom

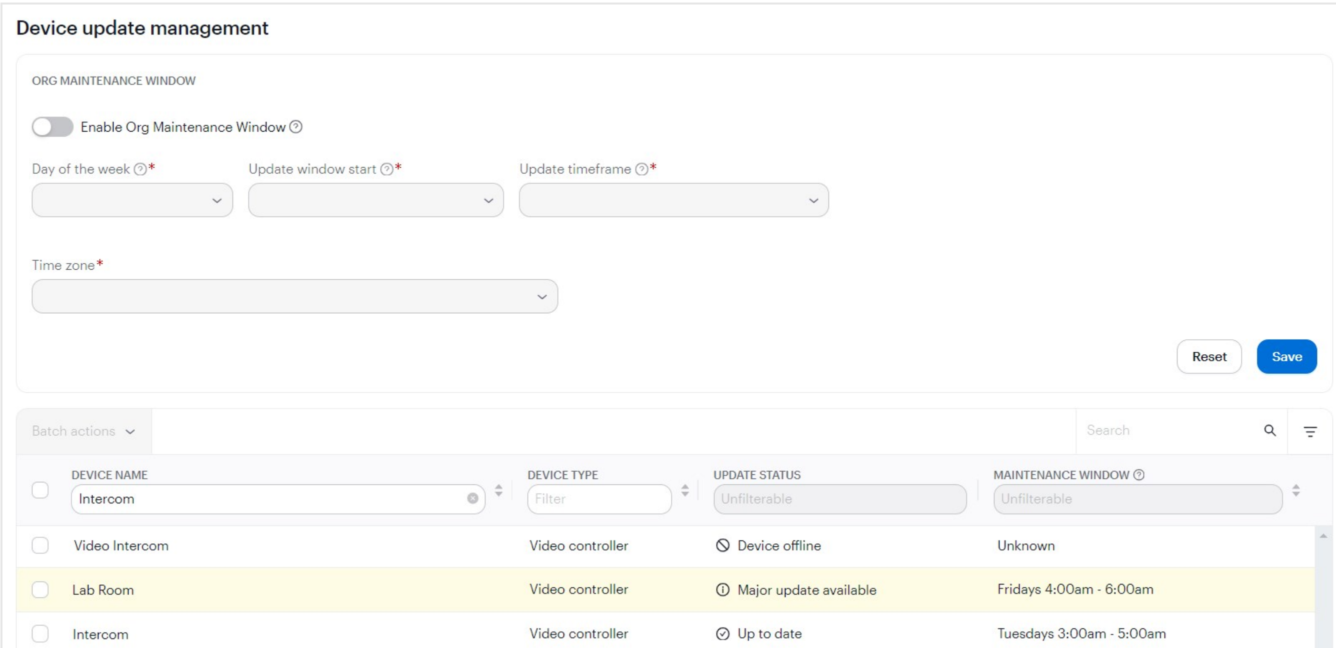
If configured, you can receive notifications in Alta Access when a visitor calls a user, group, or unit from the intercom.

1. Click the notification in the lower-right corner to view the intercom device.
2. Do any of the following:
   - Answer the call
   - Unlock the entry

For the required configuration, see the Enable intercom notifications toggle in User profile on page 26 and Configure call routing to users, units, or front desk on page 111.

Device update management

The Device updates page provides a list of the software updates for the devices managed in Alta Access, including when their default maintenance windows are scheduled to run. Updates are typically small and do not introduce noticeable downtime. Kernel and firmware updates may take longer and require downtime.



Show or hide device updates

- Click the icon to show or hide information in columns.
- Click **Reset table** to go back to the default view.

Information is read-only and cannot be edited.

Field	Description
Device ID	The ACU or Video device ID.
Device name	The configured name of the device.
Device type	Controller or Video controller.
Update status	**Device offline** — The device is offline. **Unavailable** — A connection issue has occurred between the device and the cloud. For more information on the device status, go to **Dashboards** > **Device dashboard**. **Up to date** — The device has the newest software version. **Minor update queued** — The device has a minor software version available.

Field	Description
	Major update available — The device has a major software version available. **Important update - Action required** — The device has an important software update that requires your immediate action.
Maintenance window	The weekly maintenance window for applying software updates at the beginning of the hour shown.

Apply device updates one at a time

Note: Some device updates require downtime and are recommended to be performed on site. For example, it can take up to four hours to update one controller and its connected devices. For more information and troubleshooting tips, see this Alta Access article.*

1. Go to **Devices** > **Device updates**.
2. Click a device that displays the **Important update - Action required**, **Major update available**, or **Minor update queued** status. For example:

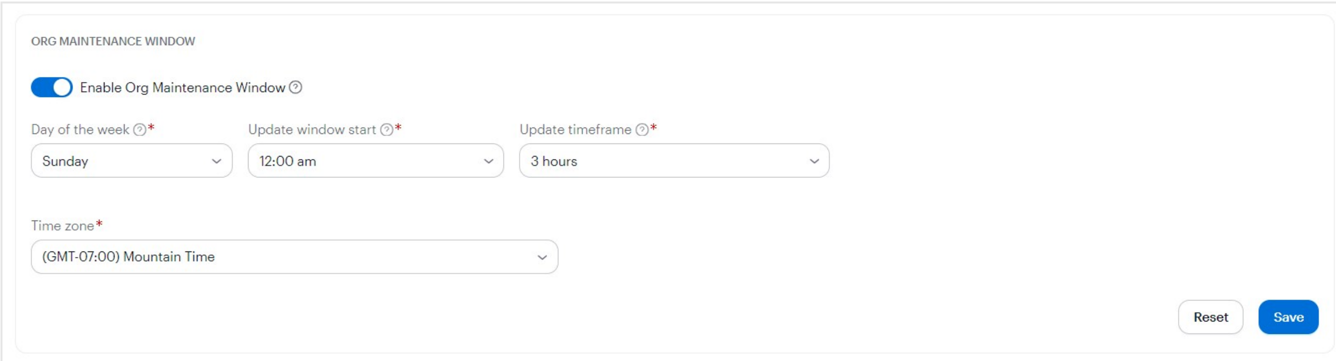
   

   A message indicates the expected downtime for an important update.
3. Click **Update Now**.
   - The Status LED indicator on the controller device will change from blinking yellow to solid yellow during software updates.
   - The Status LED indicator on the expansion board and reader devices will blink red during software updates. For firmware updates, the LED indicator will be off for readers.

   When the update is complete:
   - The solid green LED indicator is displayed on all devices, except for the Single Door Controller which displays the solid white indicator.
   - The **Up to date** status is displayed for each device on the **Device update management** page.

*For more information, see: https://help.openpath.com/space/EHC/2495971332/Detailed+Overview+and+Troubleshooting+of+the+Controller+OS+and+Device+Firmware+Update

Set up a maintenance window for all device updates



1. Select the **Enable Org Maintenance Window** toggle.
2. Specify the day of the week, the beginning of the hour, the total hours allotted for completing all device updates, and the timezone of the organization.

   Tip: A longer timeframe is recommended when applying software updates to many devices.

3. Click **Save**.

   The updates are applied in random order and complete within the allotted timeframe. The **Up to date** status is displayed.

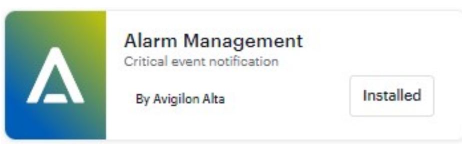
Reports

The Reports page is where you can view user, entry, and system activity.

Alta Access offers a wide variety of report types:

> **Note:** If you are viewing reports about Schlage no-tour wireless locks, only the following reports are applicable: **Activity logs**, **Alarms**, **Entry activity (by user), Entry activity summary**, **User activity (by entry)**, and **User activity summary**. Information may be out-of-date. Report information is available only after visiting the no-tour wireless lock in person and completing a manual sync using the Avigilon Alta Access mobile app.

- **Activity logs** — Displays a list of all unlock requests and hardware-related events across Alta Access and any cameras connected through Alta Video.
- **Alarms** — Displays the severity levels of alarms, the actions of the user or role that resolved them, video camera recordings, and more.

  > **Note:** A Premium or Enterprise license is required. The Alarm Management app must be installed.
  >
  > 
  >

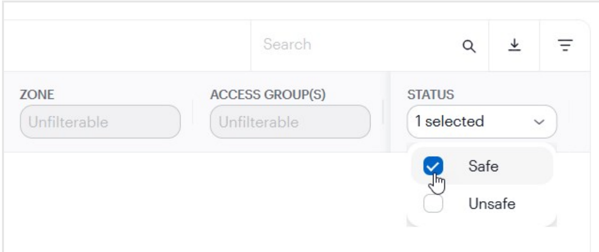
- **Credentials** — Displays all credentials within your organization, filtered by credential type.
- **Entry access audit**— Displays the users that have access to any given entry.
- **Entry activity (by user)**, **Entry activity summary**, **User activity (by entry)**, **User activity summary** — Displays user activity, entry activity, and external ID of the entry or user, in helpful charts and diagrams.

  > **Note:** Administrators can only view activities in their respective sites. Super Admin users can view activities in all sites.

- **Muster** — Used during an emergency evacuation or drill to view the users who may be on site, including users who are visiting from other sites, and account for their safety. The user must be assigned the Muster report role.

  > **Note:** A Premium or Enterprise license is required. The Muster Reports app must be installed.
  >
  > 
  >

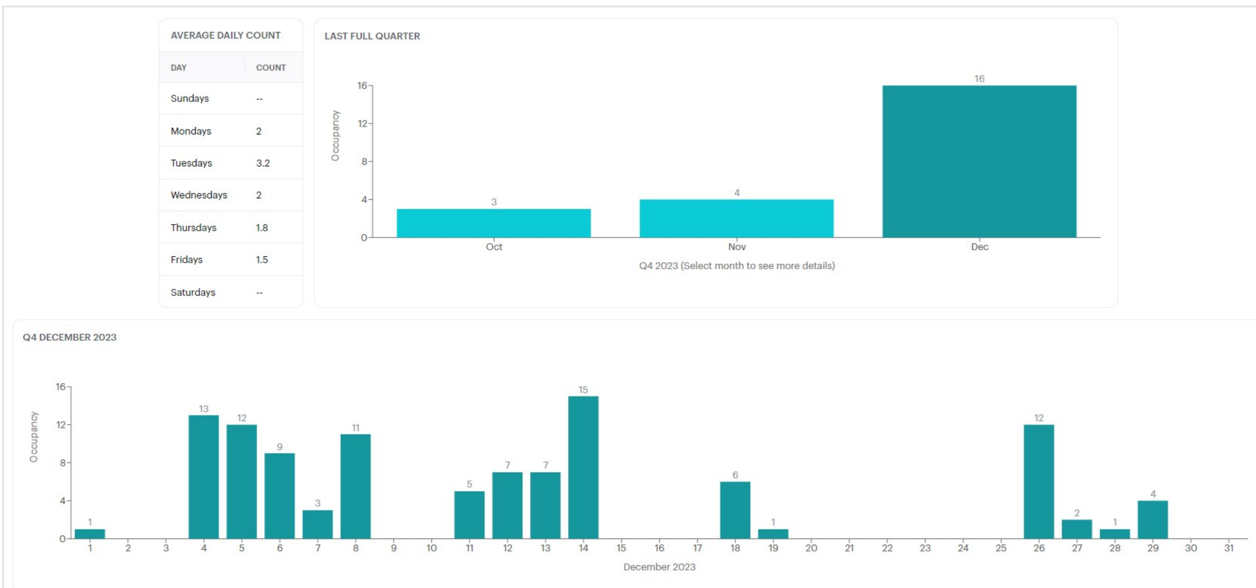
  Example filtering:



- **Occupancy** — Displays the number of unique users who have accessed one or more sites, including users who are visiting from other sites, over a period of time and the average number of occupants each day.

> **Note:** A Premium or Enterprise license is required.

Example:



- **Portal audit report**— Displays a log of the changes in Alta Access or through the Alta Access API.
- **Scheduled reports** — Displays the reports scheduled for specified time periods and data categories and includes the history of report requests.
- **User access audit** — Displays all entries that a selected user has accessed, including visits to other sites.

  A Premium or Enterprise license is required.
- **Visual activity report** — Displays video snapshots of entry events, which are filtered by user, site, entry, and time.

> **Note:** Before using this report, you must set up the Cisco Meraki integration or have Video reader management on page 99 installed.

Show, hide, or reset information

- Click the icon to show or hide information in columns.
- Click **Reset table** to go back to the default view.

Export report to CSV

- Click the icon.

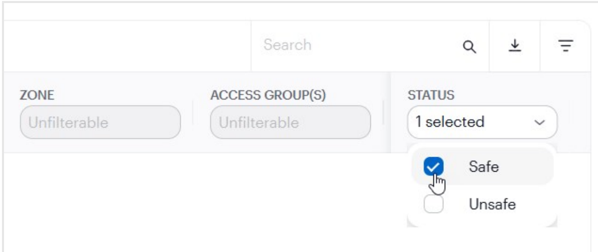
Configure reports (Activity logs, Alarms, and Portal audit report)

1. Go to **Reports** and select the report type.
2. Select a time period for the report.
3. Select a **Report delivery** option:
    - **Deliver to current browser tab** — When using this method, do not refresh or close the browser tab. Reports may take a few minutes to generate. Not recommended for large datasets.
    - **Deliver via email** — Use for large datasets. Select this method to run the report in the background and receive an email when the report is done. You can deliver the report to multiple email addresses.
4. In **Filter reports by**, enter the report data to be retrieved, such as Alarm event. In **Filter items**, enter additional report criteria.
5. Optional. Click **Add filter** to repeat the previous step.
6. Click **Search**. The report is displayed in the current browser tab or emailed, depending on the delivery option.

View and mark users as safe in the Muster report (Premium and Enterprise plans)

1. Go to **Reports** > **Muster**.
2. Select a time period for the report.
3. Optional. Select sites and zones.
4. Click **Search**. Do any of the following:
    - Select the **Mark as safe** toggle in the generated report after you have ensured a user is safe.
    - View the users who are automatically marked as safe in the generated report, if their credentials were

scanned at the muster point entry before you generated the report.



> **Note:** A credential reader is required to be installed at the entry. This reader should only be used in a muster event and not for any other purpose.

Schedule report generation and forwarding (Premium and Enterprise plans)

1. Go to **Reports** > **Scheduled reports**.
2. Click in the upper-right corner.
3. Enter a name for the scheduled report.
4. Select the type of report.

   > **Note:** Only Activity logs, Occupancy report, and Portal audit report logs are supported.

5. Select a time period for the report and configure report settings.
6. Enter email addresses to send the reports to and select a **Frequency**.
7. Click **Save**.

View scheduled reports (Premium and Enterprise plans)

1. Go to **Reports** > **Scheduled reports**.
2. Select the **Request history** tab.

   Previously generated scheduled reports will appear here. A scheduled report will expire after 30 days.

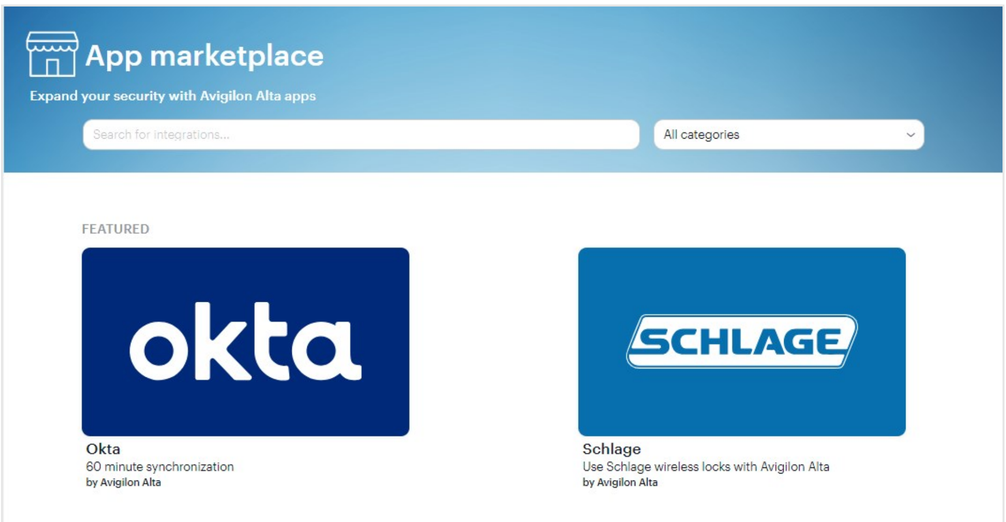
3. Click to download a CSV file of the report.

App marketplace

> **Note:** Depending on how your account is configured, you may need your integrator to enable **App marketplace** apps.

Alta Access apps connect to third-party software and services that let you sync users and add functionality to Alta Access and other systems that you use.

- **Get apps** is where you can add and configure apps for your system. Click an app to learn more about setup and configuration.
- Select **All categories** to view all the apps that can be installed from Alarm Integrations to Workplace Communication.



- **My apps** is where you can view your installed apps. Click an app to edit or configure settings.

Identity management

Identity Management / HR Software apps let you add and sync users from identity providers you already use. Currently, Alta Access integrates with Google Workspace™ productivity and collaboration tools, Microsoft Azure Active Directory, OneLogin Trusted Experience Platform™, Okta, and Workday® Human Capital Management applications. The SAML Single Sign-on app works with your SAML-enabled identity provider system for single sign-on only, without user syncing.

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

Manually sync accounts

After setting up an IDP integration, you have the option to manually synchronize users at any time to display them in Alta Access.

- Click the **Synchronize** button on the app's settings page.

Note: Manual synchronization is not applicable to the SAML Single Sign-on app integration.

Google Workspace

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

- Directory User Read-Only: `https://www.googleapis.com/auth/admin.directory.user.readonly`
- Directory Group Read-Only: `https://www.googleapis.com/auth/admin.directory.group.readonly`

1. Go to **App marketplace** > **Get apps**. Click the **Google Workspace** or **Google Workspace Advanced** tile, depending on your subscription, and then **+ Get app**.

2. Google will prompt you to sign in. Sign in with your Google account and allow Alta Access to access your users and groups.
3. After signing in, you'll be directed back to Alta Access where you can enable the following settings:
   - **Auto-sync every 1 hour** or **Auto-sync every 15 minutes** — Syncs Alta Access with the identity provider system, once every hour or once every 15 minutes, depending on your subscription. See **Administration** > **Account** for subscription details.
   - **Auto-create mobile credential** — Creates a mobile credential for every user.
   - **Auto-create cloud key credential** — Creates a cloud key credential for every user.
   - **Sync mobile phone numbers** — Syncs the mobile phone number for every user. Phone numbers must use E.164 format with a maximum of 15 digits: `+[country code][subscriber number including area code]`

     Note: The default mobile phone number (`mobile` field) will be synced. If users have a work mobile phone number (`work_mobile` field) that is the primary number, the work mobile phone number will be synced instead.

   - **Enable single sign-on (SSO) for users with portal access** — Lets users log in to Alta Access with their Google credentials.

     Tip: Consider using the control.openpath.com/loginSSO or control.eu.openpath.com/loginSSO setup page to prevent users from trying a standard login.

- **Only import users from groups that have an Avigilon Alta group mapping** — If enabled, no users are imported from the identity provider if they are not assigned to a group.
- **Auto-remove users from groups** — Removes users from groups if they no longer exist in the identity provider's groups.

4. To map a specific group or all groups from the identity provider to Alta Access:

> **Note:** Complete this step if you have enabled the **Only import users from groups that have an Avigilon Alta group mapping** setting.

   a. Select the group from the identity provider.

   b. Select the access group from Alta Access.

   c. Click **Create access group mapping**.

   d. Repeat for all the groups that need to be mapped.

Microsoft Azure AD

You can integrate Microsoft Azure Active Directory (Azure AD)[1] with Alta Access to import and sync users and access groups automatically. OAuth2 and OAuth Client authentication are supported.

- Set up OAuth2 authentication below
- Set up OAuth Client authentication on the next page

> **Note:** To enable this integration, you must be assigned the Application Administrator role in Azure AD.

Set up OAuth2 authentication

1. Go to control.openpath.com/login and sign in. For access in the EU, go to control.eu.openpath.com/login.
2. Go to **App marketplace** > **Get apps**. Click the **Microsoft Azure AD** or **Microsoft Azure AD Advanced** tile, depending on your subscription.

3. Go to **App marketplace** > **My apps**. Select the Microsoft app.
4. Microsoft will prompt you to sign in. Sign in with your Azure AD account and click **Accept** to allow Alta Access to access your users and groups.

   > **Note:** Alta Access can only read data from your Azure account; it cannot write data or make any changes within the Azure system. The token Alta Access uses only has read permissions for Azure users, groups, and directory data.

5. After signing in, you'll be directed back to Alta Access where you can enable the following settings:
   - In **Authentication strategy**, select **OAuth2**.
   - **Auto-sync every 1 hour** or **Auto-sync every 15 minutes** — Syncs Alta Access with the identity provider system, once every hour or once every 15 minutes, depending on your subscription. See **Administration** > **Account** for subscription details.
   - **Auto-create mobile credential** — Creates a mobile credential for every user.
   - **Auto-create cloud key credential** — Creates a cloud key credential for every user.

[1] Microsoft and Azure are trademarks of the Microsoft group of companies.

- **Sync mobile phone numbers** — Syncs the mobile phone number for every user. Phone numbers must use E.164 format with a maximum of 15 digits: `+[country code][subscriber number including area code]`
- **Enable single sign-on (SSO) for users with portal access** — Lets users log in to Alta Access with their Azure credentials.

  > **Tip:** Consider using the control.openpath.com/loginSSO or control.eu.openpath.com/loginSSO setup page to prevent users from trying a standard login.

- **Only import users from groups that have an Avigilon Alta group mapping** — If enabled, no users are imported from the identity provider if they are not assigned to a group.
- **Auto-remove users from groups** — Removes users from groups if they no longer exist in the identity provider's groups.

6. To map a specific group or all groups from the identity provider to Alta Access:

   > **Note:** Complete this step if you have enabled the **Only import users from groups that have an Avigilon Alta group mapping** setting.

   a. Select the group from the identity provider.

   b. Select the access group from Alta Access.

   c. Click **Create access group mapping**.

   d. Repeat for all the groups that need to be mapped.

Set up OAuth Client authentication

1. Sign in to your Microsoft Azure account and register your application in the Azure portal.[1]
2. Set up OAuth client (service principal) authentication:[2]

   a. Select your application in the Azure portal.

   b. Go to the **Certificates & secrets** page and select **Client secrets (0)**. Set up your client secret (also known as application password). Record the **Secret ID** (which appears only this one time) in a secure place.

   c. Set an expiration period for the client secret (for example, 180 days or 6 months).

---

[1] For more information, see Microsoft documentation: https://learn.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principalportal

[2] For more information, see Avigilon Alta article: https://openpath.atlassian.net/wiki/spaces/EHC/pages/2023391259/How+do+I+sync+users+using+OAuth+Client+Service+Principal+with+Microsoft+Azur e+Active+Directory#service

> **Note:** Syncing will *stop* at the end of the expiration period. Remember to update the client secret before this occurs.

   d. Configure your application permissions in **Configured permissions**. At a minimum, **Group.Read.All** and **User.Read.All** must be granted admin consent in the API / Permissions name column.

   e. Go to the **Overview** page. Record the **Application (client) ID** and **Directory (tenant) ID** to be entered in Alta Access.

3. Go to control.openpath.com/login and sign in. For access in the EU, go to control.eu.openpath.com/login.

4. Go to **App marketplace** > **My apps**. Click the Microsoft app.

5. Microsoft will prompt you to sign in. Sign in with your Azure AD account and click **Accept** to allow Alta Access to access your users and groups.

> **Note:** Alta Access can only read data from your Azure account; it cannot write data or make any changes within the Azure system. The token Alta Access uses only has read permissions for Azure users, groups, and directory data.

6. Now you can enable the following settings:

   - In **Authentication strategy**, select **OAuth Client**.
   - In **Client Id**, enter the Application (client) ID from the Azure portal.
   - In **Client secret**, enter the Secret ID for the client secret from the Azure portal.
   - **Auto-sync every 1 hour** or **Auto-sync every 15 minutes** — Syncs Alta Access with the identity provider system, once every hour or once every 15 minutes, depending on your subscription. See **Administration** > **Account** for subscription details.
   - **Auto-create mobile credential** — Creates a mobile credential for every user.
   - **Auto-create cloud key credential** — Creates a cloud key credential for every user.
   - **Sync mobile phone numbers** — Syncs the mobile phone number for every user. Phone numbers must use E.164 format with a maximum of 15 digits: `+[country code][subscriber number including area code]`
   - **Enable single sign-on (SSO) for users with portal access** — Lets users log into Alta Access with their Azure credentials.

   > **Tip:** Consider using the control.openpath.com/loginSSO or control.eu.openpath.com/loginSSO setup page to prevent users from trying a standard login.

   - **Only import users from groups that have an Avigilon Alta group mapping** — If enabled, no users are imported from the identity provider if they are not assigned to a group.

- **Auto-remove users from groups** — Removes users from groups if they no longer exist in the identity provider's groups.

7. To map a specific group or all groups from the identity provider to Alta Access:

> **Note:** Complete this step if you have enabled the **Only import users from groups that have an Avigilon Alta group mapping** setting.

   a. Select the group from the identity provider.

   b. Select the access group from Alta Access.

   c. Click **Create access group mapping**.

   d. Repeat for all the groups that need to be mapped.

Okta

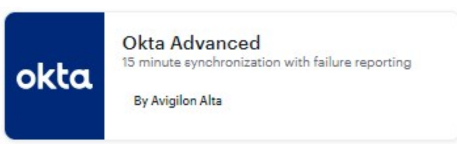
You can integrate Okta with Alta Access to import and sync users and access groups in the US or EU region. Choose the directory sync method to sync external identity provider (IDP) information every 15 or 60 minutes.

Directory sync every 15 or 60 minutes

The API token and OAuth 2.0 authentication methods are supported.

> **Note:** Before you]start, contact your integrator to install and configure the Okta and Alta Access SAML integration for the required region. Go to **Sign on** > **Edit** > **Advanced Sign-on Settings**, and enter in **Region Base URL**:
>
> - `https://api.openpath.com` for US users
> - `https://api.eu.openpath.com` for EU users
>
> For more information, see this Alta Access article[1] about using the Okta Administrator Dashboard.
>
> To use the API token (API Key) authentication method, you need admin privileges in your Okta account. We recommend using a dedicated service account[2] that uses only the Okta group membership admin role to synchronize your users and access groups. You also need to generate an Okta API Key (token[3]) for the Okta service account.
>
> To use the OAuth 2.0 authentication method, you need the Okta super administrator (admin) role to add the API Service Integration.[4]

1. Go to control.openpath.com/login and sign in. For access in the EU, go to control.eu.openpath.com/login.
2. Go to **App marketplace** > **Get apps**.
   a. Click the **Okta** (auto-sync every hour) tile or **Okta Advanced** (auto-sync every 15 minutes) tile, depending on your subscription. Click the **+ Get app** button.

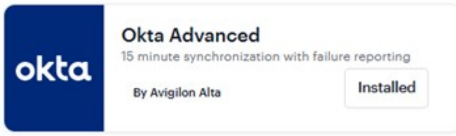


   b. In the window popup, select **License** in **Item Class**, your **Organization**, and a **License Term**. Click **Submit**.

---

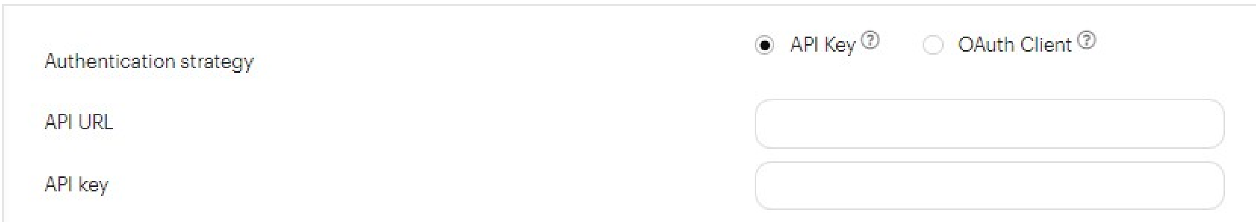
[1] For more information, see Alta Access article: https://help.openpath.com/space/EHC/2006908929/How+to+Configure+SAML+2.0+for+Okta+and+Avigilon+Alta+Security.htm
[2] For more information, see Okta documentation: https://developer.okta.com/docs/guides/create-an-api-token/overview/#token-best-practice-service-account
[3] For more information, see Okta documentation:https: //developer.okta.com/docs/guides/create-an-api-token/main
[4] For more information, see Okta documentation: https://help.okta.com/en-us/Content/Topics/apiservice/add-api-service-integration.htm

c. Ensure the Okta Advanced app is installed.



3. In **Sync type**, select **Directory**.

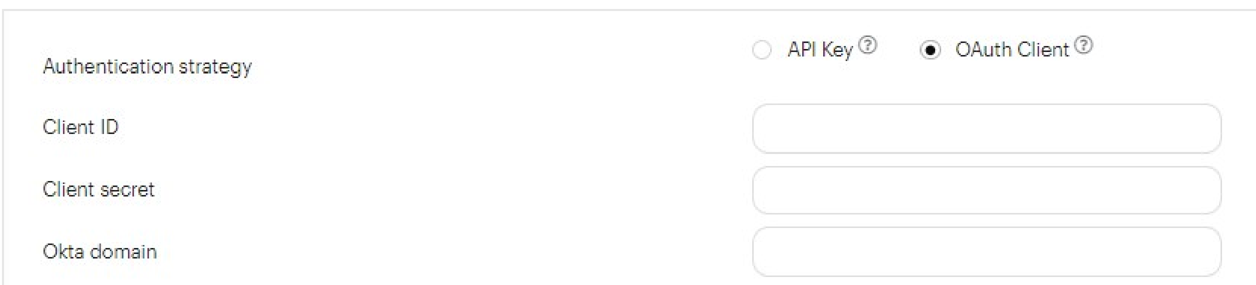
4. To use API key authentication, select **API Key** and enter the following settings:



   - **API URL** — The Okta domain[1] for your organization (for example, `https://yourcompanyname.okta.com`).
   - **API key** — The API key for the service account that is dedicated to the integration.

   > **Note:** After you save the API Key, Alta Access does not use, or otherwise expose, the API Key anywhere except when using it to call Okta to synchronize users and groups.

5. To use OAuth 2.0 authentication, select **OAuth Client** and enter the following settings:



   - **Client ID** — The Client ID from the API Service Integration step.
   - **Client secret** — The Client secret value from the API Service Integration step.
   - **Okta domain** — The Okta domain[2] for your organization (for example, `https://yourcompanyname.okta.com`).

6. After saving one of the authentication strategies, you can enable the following settings:

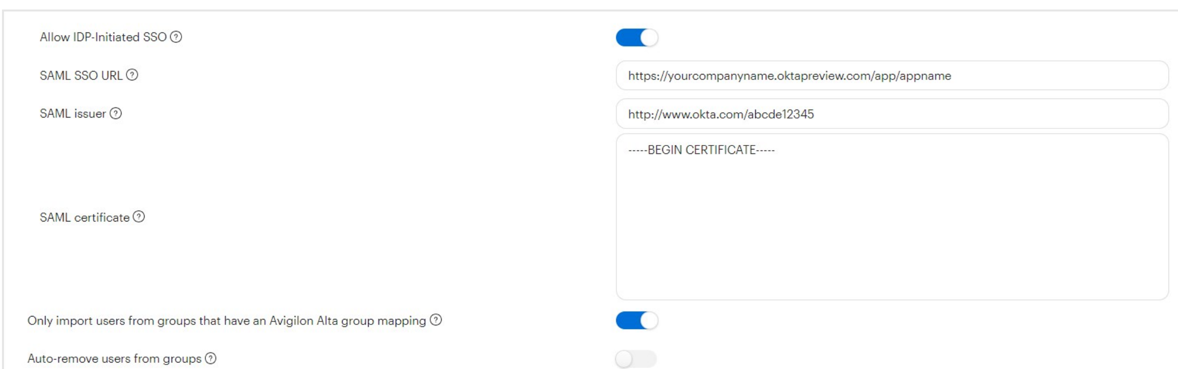
---

[1] For more information, see Okta documentation:https://developer.okta.com/docs/guides/find-your-domain/main
[2] For more information, see Okta documentation:https://developer.okta.com/docs/guides/find-your-domain/main

- **Auto-sync every 1 hour** or **Auto-sync every 15 minutes** — Syncs Alta Access with the identity provider system, once every hour or once every 15 minutes, depending on your subscription. See **Administration** > **Account** for subscription details.
- **Auto-create mobile credential** — Creates a mobile credential for every user.
- **Auto-create cloud key credential** — Creates a cloud key credential for every user.
- **Sync mobile phone numbers** — Syncs the mobile phone number for every user. Phone numbers must use E.164 format with a maximum of 15 digits: `+[country code][subscriber number including area code]`
- **Enable single sign-on (SSO) for users with portal access** — Lets Okta super admin users log in to Alta Access with their Okta credentials.

> **Tip:** Consider using the control.openpath.com/loginSSO or control.eu.openpath.com/loginSSO setup page to prevent users from trying a standard login.

- **Enable single sign-on (SSO) for mobile app** — Lets users log in to the Alta Open mobile app using Okta credentials.
- **Only import users from groups that have an Avigilon Alta group mapping** — If enabled, no users are imported from the identity provider if they are not assigned to a group.
- **Auto-remove users from groups** — Removes users from groups if they no longer exist in the identity provider's groups.
- **Allow IDP-Initiated SSO** — Lets users log in to Alta Access from the Okta portal. If enabled, fill out the required fields: **SAML SSO URL**, **SAML issuer**, and **SAML certificate**.



> **Note:** You'll find this information in the Okta portal.
>
> a. Log in to the Okta portal and click **Admin**.
>
> b. Go to **Applications** and click your Alta Access application.
>
>   If you haven't already added Alta Access, click **Add Application** and then search for and add the **Avigilon Alta** application.
>
> c. Click **Sign on**.
>
> d. In the Settings box, click **View Setup Instructions**.
>
> e. Copy **Sign on URL**, **Issuer**, and **Signing Certificate** from the Okta portal into their corresponding locations in Alta Access.
>
>   **Tip:** Go to **Sign on** > **More details** in the Okta portal.

7. To map a specific group or all groups from the identity provider to Alta Access:

   > **Note:** Complete this step if you have enabled the **Only import users from groups that have an Avigilon Alta group mapping** setting.

   a. Select the group from the identity provider.

   b. Select the access group from Alta Access.

   c. Click **Create access group mapping**.

   d. Repeat for all the groups that need to be mapped.

Inactivate identity provider

If it is necessary to remove an identity provider integration and credentials:

- Click **Inactivate identity provider** on the identity provider page and contact billing@openpath.com to remove the license.

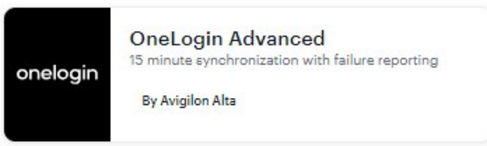
  > **Note:** Inactivated users are kept in the system for reporting and record-keeping purposes. To find an inactivated user, go to the **Users** page and select **Deleted** from the STATUS column.

OneLogin

You can integrate the OneLogin Trusted Experience Platform™ with Alta Access to import and sync users automatically.

> **Note:** To enable the OneLogin identity provider integration, you must have admin privileges in your OneLogin account.

1. Go to control.openpath.com/login and sign in. For access in the EU, go to control.eu.openpath.com/login.
2. Go to **App marketplace** > **Get apps**. Click the **OneLogin** or **OneLogin Advanced** tile, depending on your subscription.

3. Enter the **Subdomain** for your OneLogin account (for example, `yourcompanyname.onelogin.com`).
4. Click **Get API credentials** to go to the OneLogin page.
   a. Click **New Credential** on the API Access page.
   b. Enter a name for the credential, select **Read Users**, and click **Save**.

   For more information, refer to OneLogin documentation.[*]
5. Copy and paste the **Client ID** and **Client secret** to Alta Access, and click **Save**.
6. Enable the following settings:
   - **Auto-sync every 1 hour** or **Auto-sync every 15 minutes** — Syncs Alta Access with the identity provider system, once every hour or once every 15 minutes, depending on your subscription. See **Administration** > **Account** for subscription details.
   - **Auto-create mobile credential** — Creates a mobile credential for every user.
   - **Auto-create cloud key credential** — Creates a cloud key credential for every user.
   - **Sync mobile phone numbers** — Syncs the mobile phone number for every user. Phone numbers must use E.164 format with a maximum of 15 digits: `+[country code][subscriber number including area code]`

[*]Refer to OneLogin documentation: https://developers.onelogin.com/api-docs/1/getting-started/working-with-api-credentials

> **Note:** The default phone number (`phone` field) will be synced, including non-mobile phone numbers. Users that don't have mobile numbers may not have access to some features in Alta Access.

- **Enable single sign-on (SSO) for users with portal access** — Lets users log in to Alta Access with their OneLogin credentials.

> **Note:** Copy and paste your **SSO Client ID**, which you can find by connecting to an OIDC-enabled app. For more information, see OneLogin documentation.*

> **Tip:** Consider using the control.openpath.com/loginSSO or control.eu.openpath.com/loginSSO setup page to prevent users from trying a standard login.

- **Only import users from groups that have an Avigilon Alta group mapping** — If enabled, no users are imported from the identity provider if they are not assigned to a group.
- **Auto-remove users from groups** — Removes users from groups if they no longer exist in the identity provider's groups.

7. To map a specific group or all groups from the identity provider to Alta Access:

> **Note:** Complete this step if you have enabled the **Only import users from groups that have an Avigilon Alta group mapping** setting.

   a. Select the group from the identity provider.
   b. Select the access group from Alta Access.
   c. Click **Create access group mapping**.
   d. Repeat for all the groups that need to be mapped.

*Refer to OneLogin documentation:https://developers.onelogin.com/openid-connect/connect-to-onelogin

SAML Single Sign-on app

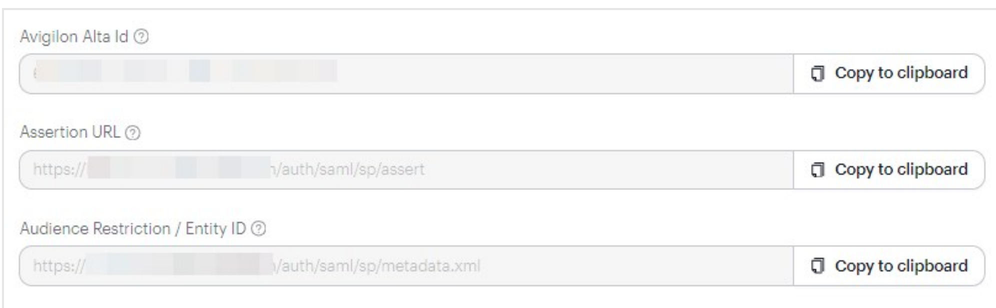
You can integrate the SAML Single Sign-on app with your SAML-enabled identity provider system to import users to Alta Access. User single sign-on will occur after authentication by your identity provider.

1. Go to control.openpath.com/login and sign in. For access in the EU, go to control.eu.openpath.com/login.
2. Go to **App marketplace** > **+ Get app**.
3. Click the **SAML Single Sign-on** tile.

   This app is available for Basic, Premium, and Enterprise plans.
4. After the app is installed, click **Configure**.

   If you are on the My apps page, click the icon.
5. Set up the app integration in your SAML-enabled identity provider system.

   a. Click **Copy to clipboard** next to the following field in Alta Access, and provide the ID to new users.

      Avigilon Alta Id — The ID for initial Alta Access sign-in. Users will enter this ID with their email when signing in for the first time.

      Tip: Consider using the control.openpath.com/loginSSO or control.eu.openpath.com/loginSSO setup page to prevent users from trying a standard login.

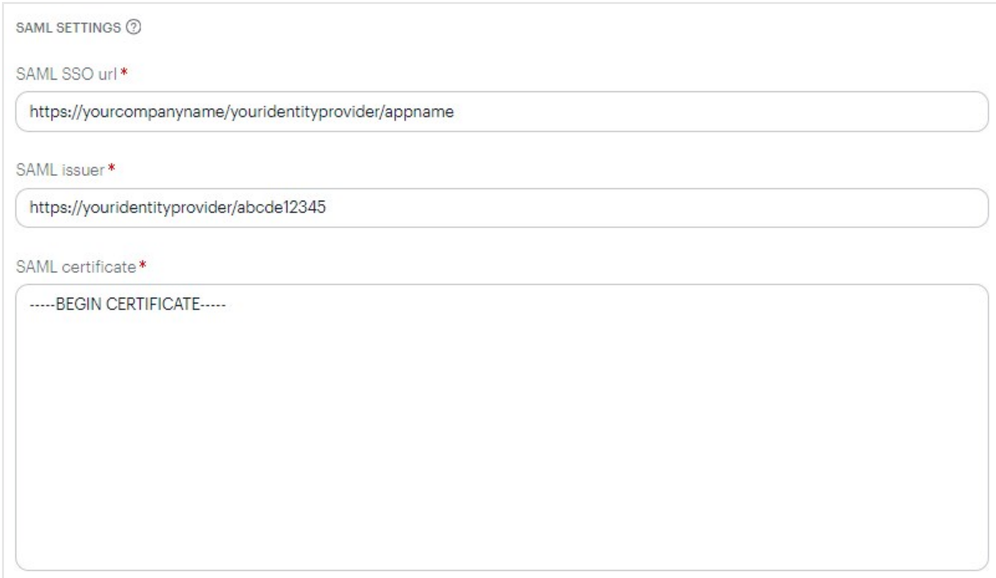
   b. Click **Copy to clipboard** next to the following fields in Alta Access, and paste them in the identity provider configuration.

      Assertion URL — The SAML Assertion Consumer Service (ACS) URL where the SAML assertion is sent in an HTTP POST.

      Audience Restriction / Entity ID — The auto-generated ID for your SAML audience.

c. Create the email, firstName, lastName, and **uniqueId** attribute statements in the identity provider system.

6. Enter the **SAML SSO url**, **SAML issuer**, and **SAML certificate** from the identity provider system in Alta Access.



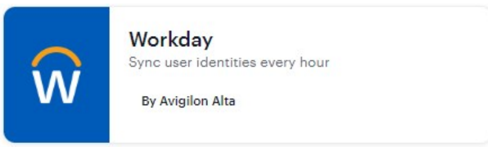
7. Click **Save**.

Workday reports

You can integrate Workday® Human Capital Management reports with Alta Access to import and sync users and access groups automatically.

> **Note:** Workday Web Service API v39.1 or newer is required. In addition, you must have admin privileges in your Workday account to configure custom reports. Custom reports must be configured before you start this procedure. For more information, see this Alta Access article[1].

1. Go to control.openpath.com/login and sign in. For access in the EU, go to control.eu.openpath.com/login.
2. Go to **App marketplace** > **Get apps**.
3. Click the **Workday** or **Workday Advanced** tile, depending on your subscription.

4. Enter the Workday account details.
   - **Report URL** — The URL of your Workday custom report for users.
   - Select **+ Get app**.
   - Choose the appropriate license for your organization.
   - Click **Submit**.

     > **Note:** In the Workday application, go to **CR - OpenPath Data Interface** and click the **... Actions** menu. Select **Web Service** > **View URLs** and right-click on **JSON** to select **Copy URL**.

   - **Report username** — The username.
   - **Report password** — The password.
   - (Optional) **Groups URL** — The URL of your Workday custom report for access groups.

     > **Note:** In the Workday application, go to **View Custom Report Openpath - Group Names** and click the **... Actions** menu. Select **Web Service** > **View URLs** and right-click on **JSON** to select **Copy URL**.

[1]For more information, see: https://openpath.atlassian.net/servicedesk/customer/portal/15/article/1836056610.

5. Manually trigger the first sync.
   - Click the **Synchronize** button to display the active users and access groups on the Users page.

   > **Note:** With the Workday Advanced package subscription, you can enable alerts for sync failures. For more information, see the Identity Provider toggle in Alerts by email or SMS on page 149.

6. Enable the following settings, as needed.
   - **Auto-sync every 1 hour** or **Auto-sync every 15 minutes** — Syncs Alta Access with the identity provider system, once every hour or once every 15 minutes, depending on your subscription. See **Administration** > **Account** for subscription details.
   - **Auto-create mobile credential** — Creates a mobile credential for every user.
   - **Auto-create cloud key credential** — Creates a cloud key credential for every user.
   - **Sync mobile phone numbers** — Syncs the mobile phone number for every user. Phone numbers must use E.164 format with a maximum of 15 digits: `+[country code][subscriber number including area code]`

     > **Note:** In the Workday application, the name of the report column must be defined as `mobilePhone`.

   - **Sync person Id** — Syncs the employee ID from the identity provider system.
   - **Sync department** — Syncs the department from the identity provider system.
   - **Sync job title** — Syncs the job title from the identity provider system.
   - **Only import users from groups that have an Avigilon Alta group mapping** — If enabled, no users are imported from the identity provider if they are not assigned to a group.

     > **Tip:** Consider using the control.openpath.com/loginSSO or control.eu.openpath.com/loginSSO setup page to prevent users from trying a standard login.

   - **Auto-remove users from groups** — Removes users from groups if they no longer exist in the identity provider's groups.

7. To map a specific group or all groups from the identity provider to Alta Access:

   > **Note:** Complete this step if you have enabled the **Only import users from groups that have an Avigilon Alta group mapping** setting.

   a. Select the group from the identity provider.

   b. Select the access group from Alta Access.

c. Click **Create access group mapping**.
d. Repeat for all the groups that need to be mapped.

Video management

Video management apps let you view and play back video clips from cameras and video management systems that are integrated with Alta Access. Currently, Alta Access integrates with the following video management systems, and more.

Alta Aware app

The Alta Aware app integration links the access control events in Alta Access with video feeds from cameras in Alta Video. The integration also supports the issuing of license plate credentials for user access at parking entries, if License Plate Recognition (LPR) is configured in Alta Video.

System requirements

- Alta Access event integration
  - Alta Access added as a device in Alta Aware

    For more information, see Alta Aware integration documentation.
  - Alta Access user account with Super Admin rights

    For more information, see Alta Access event integration below.
- Alta Video camera integration
  - Alta Video version 4.4 or newer

    For more information on upgrading your Alta Aware version, see support.avasecurity.com.
  - Alta Aware app from App marketplace

    For more information, see Alta Video camera integration on the next page.
  - License Plate Recognition configuration

    For more information, see this Alta Access article.
- Normal browsing mode when navigating between systems

  The button and app switcher links do not work in Chrome™ Incognito mode or private mode. For more information, see Alta Video, Alta DMP, and Alta Access workflow on page 21.

Alta Access event integration

To add a Super Admin user account that is used specifically for Alta Access event integration:

1. Go to **Users** > **Users**.

   > **Tip:** Select the Quick actions icon to use the Add user shortcut.

2. Click the button in the upper-right corner.

3. Enter the email and name.
4. Select the **Portal access** checkbox and add **Super Admin**. Click **Save**.
5. Log in to Alta Aware.
6. Enter the username and password for the 'access control point' integration. For more information, see Aware documentation.
7. Go to **Dashboards**, and add the **Activity logs** and **Visual activity report** widgets to your custom dashboard. Or, change **Activity** to **Activity logs** or **Visual activity report** in the upper-right corner to view relevant access events.

Alta Video camera integration

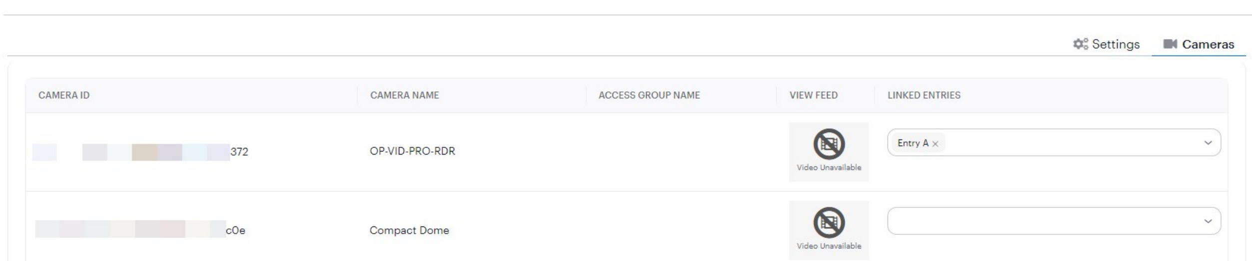
1. Go to **App marketplace** > **Get apps**.
2. Select the **Alta Aware** tile.

3. Select **+ Get app**. The app is installed.
4. Select **Configure** and fill out the **Settings** page.

   Server address — The URL to access the Alta Aware VMS. For example: `https://yourcompanyname.us1.aware.ava.uk`

   Username and **Password** — The administrator's credentials which creates a user account in Alta Video.

5. Click **Create**. All cameras connected to Alta Aware are displayed on the Cameras page.



   In the VIEW FEED column, you can click a video feed to access the camera in Alta Aware displayed on a new browser tab.

   In the LINKED ENTRIES lists, you can link multiple entries to a camera or multiple cameras to an entry.

6. Click **Save**.

Next, go to the Cameras page to view live video feeds from Alta Aware. For more information, see Cameras on page 40.

Camio

The Camio app integration links Alta Access entry events and users with videos in the Camio video management system. To set up this integration, you create outbound webhooks that send data to Camio, designate a user with read-only portal access that translates UserIds to names, and then input Org and Entry information into the Camio portal. For more information, see this Alta Access article.

Cisco Meraki

The Cisco® Meraki® app integration lets you to view video snapshots in Alta Access and events in the Visual activity report under Reports. To set up this integration, see this Alta Access article.

Milestone

The Milestone app integration links Alta Access entry events and users with videos in the Milestone XProtect® video management system. To set up this integration, see this Alta Access article.

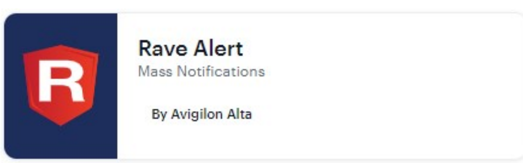
Rhombus

The Rhombus app integration links Alta Access entry events and users with videos in the Rhombus video management system. To set up this integration, designate a user with read-only portal access and use those credentials to enable the integration in the Rhombus console. For more information, see this Alta Access article.

Emergency notification and response

Rave Alert app

In Alta Access, you can configure a rule or alarm that sends an Alert code to the Rave Alert app to notify employees, visitors, or students of a lockdown or emergency situation.



- To configure your Common Alerting Protocol (CAP) listener and mass notification template, see Rave Alert system documentation.
- To configure rules and alarms in Alta Access, see Add rules and triggers on page 146 and Action triggers and alarm notifications on page 154.

Note: App installation and configuration are not applicable in the App marketplace.

Visitor management

Visitor management apps let you assign credentials to visitors in your visitor management systems and track their entry activity in Activity logs in Alta Access. Currently, Alta Access integrates with the following visitor management systems, and more.

Envoy

The Envoy app integration lets you assign cloud credentials to visitors in the Envoy visitor management system. To set up this integration, you generate guest access links for visitors in the Envoy system that can be shared by email or SMS. For more information, see this Alta Access article.

Workplace communication

Workplace communication apps let you use your business communication platform to manage access control events through the integration with Alta Access.

Slack

The Slack* app integration works by defining commands that you type into Slack that will unlock individual entries. To set up this integration, see this Alta Access article.

Wireless lock integration

Schlage Wireless Locks

The Schlage wireless lock app integration connects the Allegion Schlage® NDE and LE series locks, and Control™ smart locks, in online or offline mode.

- To set up online mode using the ENGAGE™ gateway, see this Alta Access article.
- To set up offline mode using the no-tour system integration which does not require the ENGAGE gateway, see the Avigilon Access Control System Integration Guide for Schlage Wireless Locks No-Tour.[2]

Middleware integration

Zapier

The Zapier® app integration triggers automated workflows that connect apps and services (called zaps) when new users are created, as well as automatically generate guest access links and credentials.

To set up this integration, see this Alta Access article.

---

*Slack is a trademark and service mark of Slack Technologies, Inc., registered in the U.S. and in other countries.

[2] https://assets.avigilon.com/documents/avigilon-access-control-system-integration-guide-schlage-wireless-locks-notour-en.pdf

Configurations

Rules

The rules engine lets you create conditional rules that trigger actions based on access events and custom rules.

Tip: For advanced alarm management, refer to Alarms (Premium and Enterprise plans) on page 151.

Add rules and triggers

1. Go to control.openpath.com/login and sign in. For access in the EU, go to control.eu.openpath.com/login.
2. Go to **Configurations** > **Rules**.
3. Click + in the upper-right corner. Enter a name and description.
4. In the TRIGGER section, select the type of trigger and event.

   Note: The Basic package only includes the **Input** trigger type, but you can still use the JSON editor to create other rules.

Trigger type	Name or related events	Filter event by CONDITIONS[1]
Entry	Entry Ajar Ended, Entry Ajar Started, Entry Forced Open, Entry Unlock Authentication Failed, Entry Unlock Authorization Failed	Entry filter, Site filter, Zone filter
	Entry Anti-Passback Breach, Entry Unlock Authenticated*, Entry Unlock Authorized*, Entry Unlock Failed, Entry Unlocked*	Entry filter, Site filter, User filter, Zone filter
	Occupancy Limit Exceeded Within Anti-Passback Area	(not applicable)
Event forwarder	Includes events in this trigger list, as well as billing activity, user creation and deletion, and identity provider sync issues. To learn more, see this Alta Access article.	
Input*	Contact Sensor End-Of-Line Supervision State Changed, Contact Sensor State Changed, Generic Input End-Of-Line	ACU filter, ACU port filter, State filter

[1] Choosing to filter by site, zone, or entry includes the users who are visiting from other sites.
*Certain events may need a response before triggering an action (for example, failed authorization to unlock an entry). To block a failed REX, authentication, or authorization request, select the **Use blocking mode** toggle.

Trigger type	Name or related events	Filter event by CONDITIONS[1]
	Supervision State Changed, Generic Input State Changed, REX End-Of-Line Supervision State Changed, REX State Changed	
	Tamper Detector State Changed	ACU filter
Lockdown	Lockdown Plan Revert Authorized*, Lockdown Plan Reverted*, Lockdown Plan Trigger Authorized, Lockdown Plan Triggered For an example of a lockdown trigger, refer to this Alta Access article.	Lockdown plan filter, User filter
Reader	Reader Fault State Changed*	ACU filter, ACU port filter
Relay	Relay Fault State Changed*	ACU filter, ACU port filter
Video intercom reader	Intercom Button Pressed, Intercom Direct Connect session requested, Intercom Front Desk Connect session requested, Motion Detected, SIP DTMP digit heard, Sound Detected, Tamper Detected, Video Voicemail Notification, Video device - QR code detected	State filter, Video intercom reader filter, Video reader filter
Video reader	Motion Detected, Tamper Detected, Video device - QR code detected	State filter, Video reader filter

5. Optional. To apply a time constraint on this rule, click **Add schedule** and select a **One-time schedule event** or **Repeating schedule event**. Enter date and time information.
6. In the ACTIONS section, specify what the rule will do once triggered.

> **Note:** Only the **Webhook** action is applicable to the **Video device - QR code detected** event.

Type	Related settings
CAP message	**Alert code** — The alert code that will be sent to the mass emergency notification and response system in Common Alerting Protocol (CAP) version 1.2 or newer. **Note:** The alert code must match the alert code defined in the third-party system.

[1] Choosing to filter by site, zone, or entry includes the users who are visiting from other sites.

Type	Related settings
	Authentication method — Choose from: **Note:** Supported authentication methods are dependent on the emergency notification and response system. **Basic** — Enter the **URL** of the emergency notification and response system (example: `https://www.yourdomain.com/authentication_pathname`), **Username**, and **Password**. **Header** — Enter the **URL** of the emergency notification and response system (see example above), and credentials in the **Authorization header value** (example: `Basic ABCdef123`). **URL** — Embed the credentials in the **URL** of the emergency notification and response system (example: `https://www.yourdomain.com/authentication_pathname?auth=BasicABCdef123`). For more examples, see this Alta Access article.
Email / SMS	**Subject** — The subject of the notification. **Body** — The body of the notification. **Recipients** — The phone numbers or emails.
Lockdown	**Lockdown plan** — The lockdown plan. **Lockdown action** — **Trigger lockdown** or **Revert lockdown**.
Relay	**ACU relay port number to trigger** — The port number. The triggered relay will be on the same ACU that the trigger event occurred on. • Single Door Controller: 1 or 2 • Access Control Core: 1, 2, 3, or 4 • Core Series expansion boards: `(expansion number x 10000) + relay port number` Example: Expansion board 2 on relay port 12 is 20012. • Auxiliary relays: `(expansion number x 10000) + (max. port number + AUX number)` Example using 8-Port Board: Expansion board 3 on AUX Relay 2 is 30010. You can also find these port IDs using the Alta Access API. **State** — **Engage** or **Disengage**. **Duration (seconds)** — The duration in seconds.
Webhook	**URL** — The URL for the webhook API call. **HTTP method** — The GET or POST method.

Type	Related settings
For all types	Select when the action is triggered by the user: • **Delay before action (seconds)** — The delay in seconds. • **Block next action until finished and quit on error** — The action needs a response before triggering another action (for example, acknowledging before clearing an alarm).

7. Click **Save**.

Create custom rules

1. To create custom or more complex rules, select the **Use JSON editor** checkbox.

   For an example of a rule created using the JSON editor, this Alta Access article.

2. Click **Save**.

Alerts by email or SMS

Receive alerts by email or SMS to monitor your Alta access control system.

1. Go to control.openpath.com/login and sign in. For access in the EU, go to control.eu.openpath.com/login.
2. Go to **Configurations** > **Alerts**.
3. Configure alerts that generate email or SMS warnings to US mobile numbers.

   > **Note:** The alerts depend on the locks or devices. For the alerts supported in offline locks, see the Avigilon Access Control System Integration Guide for Schlage Wireless Locks No-Tour (link).

   - **Include camera link** checkbox — Includes a link to the camera in the alert that supports the option.
   - **Billing** — Invalid payments, expired terms, and/or your account being frozen.
   - **Entry Ajar** — An entry entering or leaving the ajar alarm state, such as when the contact sensor reports the door being open longer than the set duration.

     > **Note:** To receive this alert, you must enable the **Ajar feature**. See Contact sensor settings on page 73.

   - **Entry Authentication Failure** — An entry unlock request failing due to an invalid credential being used (e.g. a card with a number or 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 Alta Access or triggering the REX.

  > **Note:** To receive this alert, you must also enable the Forced-Open Detection feature in Edit entries on page 73 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.
- Other supported alerts: **Lockdown Plan Triggered**, **Generic Input State Changed**, **REX State Changed**, **Contact Sensor State Changed**, **Identity Provider**, **ACU Online Status Changed**, **Tamper Detector State Changed**, **Relay Fault State Changed**, **Reader Fault State Changed**, **Input EOL State Changed**, **Occupancy Management**, **Intercom Button Pressed**, **Motion Detected**, **Audio Detected**, **Video Reader Tamper Detected**, **3rd Party Device Communication Lost**, **3rd Party Device Battery Low/Critical**, **3rd Party Device Error Detected**, **3rd Party Device Tamper Detected**, **New Alarm Rate Limit Reached**, **Approaching Open Alarm Limit**, **Open Alarm Limit Reached**

4. Enter the email addresses and/or US-based phone numbers that will receive alerts.

   > **Note:** Enter phone numbers using the following format: `+15556667777` (no hyphens and `+1` before the number).

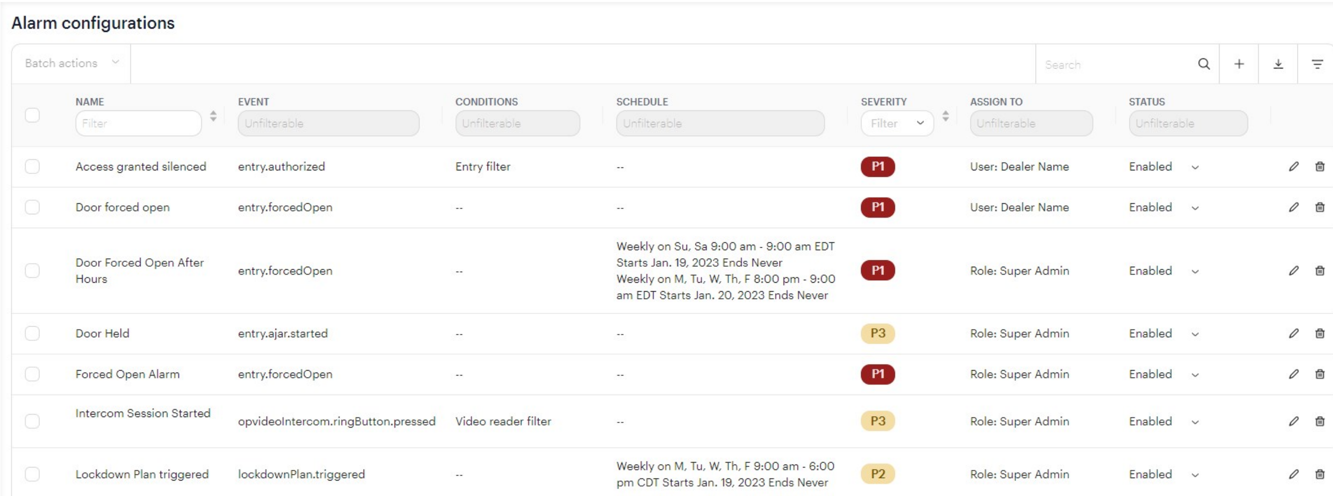
   > **Note:** If the alert is enabled, but no email addresses or phone numbers are specified, the alert will be sent to all Super Admin emails within the organization.

5. Click **Save**.

Alarms (Premium and Enterprise plans)

> **Note:** A Premium or Enterprise license is required.

The Alarm configurations page is used by administrators to configure alarms that notify monitoring operators about a security situation (for example, a door forced open). After configuration is completed, monitoring operators can receive popup notifications in Alta Access, or emails and SMS notifications, and acknowledge and resolve them.



Enable, disable, or silence alarms

1. Enter a checkmark next to one or more alarm configurations.
2. Click **Batch actions** to select:
   - **Enable** — Shows alarms in Alta Access.
   - **Disable** — Disables alarms and notifications. No alarms are logged in Alta Access.
   - **Silence** — Disables alarm notifications only. Alarms are still visible in the Alarms dashboard, and report history if enabled, in Alta Access.

Configure alarms

1. Go to control.openpath.com/login and sign in. For access in the EU, go to control.eu.openpath.com/login.
2. Go to **Configurations** > **Alarms**.
3. Click in the upper-right corner to create an alarm. Or, double-click an existing alarm to select it.
4. In the **INFO** section, enter a name and description for the alarm.

Severity and instructions for resolution

- In **Severity**, enter the priority of the alarm to be shown in the Alarms dashboard and popup notifications.
  - **P1** displays as P1 (highest priority).
  - **P2** displays as P2.
  - **P3** displays as P3.
  - **P4** displays as P4.
  - **P5** displays as P5 (lowest priority).
- In **Instructions**, enter the instructions for resolving the alarm. For example, you might dispatch security staff to the physical location of the door forced open.

Alarm enabling and silencing

- To show the alarm in Alta Access, ensure the **Enabled** toggle is selected (default).
- To silence popup notifications in Alta Access (if configured in Profile settings) and show the alarm in emails or SMS notifications, ensure the **Silenced** toggle is deselected (default).

Event triggers and advanced filtering

1. In the TRIGGER section, select the type of trigger and event, and then click **Add filter**.
2. If needed, enable the **Use blocking mode** toggle for the events marked by * in the table below.

Trigger type	Name or related events	Filter event by CONDITIONS[1]
Aware rule	**Event**: The name of the rule defined in Alta Video. **Note:** If Alta Video and Alta Access have been unified in your organization and you have the permissions in Alta Video to edit rules, the **Edit rules in Aware** link will be visible. Click to go directly to the Rules list in Alta Aware on a new browser tab.	(not applicable)

[1]Choosing to filter by site, zone, or entry includes the users who are visiting from other sites.

Trigger type	Name or related events	Filter event by CONDITIONS[1]
		
Entry	Entry Ajar Ended, Entry Ajar Started, Entry Forced Open, Entry Unlock Authentication Failed, Entry Unlock Authorization Failed	Entry filter, Site filter, Zone filter
	Entry Anti-Passback Breach, Entry Unlock Authenticated*, Entry Unlock Authorized*, Entry Unlock Failed, Entry Unlocked*	Entry filter, Site filter, User filter, Zone filter
	Occupancy Limit Exceeded Within Anti-Passback Area	(not applicable)
Input*	Contact Sensor End-Of-Line Supervision State Changed, Contact Sensor State Changed, Generic Input End-Of-Line Supervision State Changed, Generic Input State Changed, REX End-Of-Line Supervision State Changed, REX State Changed	ACU filter, ACU port filter, State filter
	Tamper Detector State Changed	ACU filter
Lockdown	Lockdown Plan Revert Authorized*, Lockdown Plan Reverted*, Lockdown Plan Trigger Authorized, Lockdown Plan Triggered For an example of a lockdown trigger, refer to this Alta Access article.	Lockdown plan filter, User filter
Reader	Reader Fault State Changed*	ACU filter, ACU port filter
Relay	Relay Fault State Changed*	ACU filter, ACU port filter
Video intercom reader	Intercom Button Pressed, Intercom Direct Connect session requested, Intercom Front Desk Connect session requested, Motion Detected, SIP DTMP digit heard, Sound Detected, Tamper Detected, Video Voicemail Notification, Video device - QR code detected	State filter, Video intercom reader filter, Video reader filter

[1] Choosing to filter by site, zone, or entry includes the users who are visiting from other sites.
*Certain events may need a response before triggering an action (for example, failed authorization to unlock an entry). To block a failed REX, authentication, or authorization request, select the **Use blocking mode** toggle.

Trigger type	Name or related events	Filter event by CONDITIONS[1]
Video reader	Motion Detected, Tamper Detected, Video device - QR code detected	State filter, Video reader filter

User or role assignment

- To assign one user, select **Assign to** > **User** and the user.
- To assign a group of users, select **Assign to** > **Role** and the role.
- To require the user to acknowledge the alarm in a note in Alta Access, enter a checkmark in **Require notes for acknowledgement**.

> **Note:** Only one user or one role can be assigned, however, you can enter multiple users to receive notifications about the alarm, as described in Action triggers and alarm notifications below.

Cameras for video monitoring

In **Camera(s)**, select any installed video intercom cameras that is relevant to the alarm.

Schedules

1. Click **Add schedule** to put the event triggers on a schedule.

   > **Tip:** If the event triggers need to be active at all times, do not add a schedule.
   >
   > If you have configured a schedule in Alta Video , you do not need to repeat the schedule in Alta Access alarm configuration.

2. In **Type**, select **One-time schedule event** or **Repeating schedule event**.
3. Fill out the dates and times.
4. Click **Add schedule** to add another schedule.

Action triggers and alarm notifications

In the ACTIONS section, select the type of action and related settings, and click **Add action**.

> **Note:** Only the **Webhook** action is applicable to the **Video device - QR code detected** event.

Type	Related settings
CAP message	**Alert code** — The alert code that will be sent to the mass emergency notification and response system in Common Alerting Protocol (CAP) version 1.2 or newer.

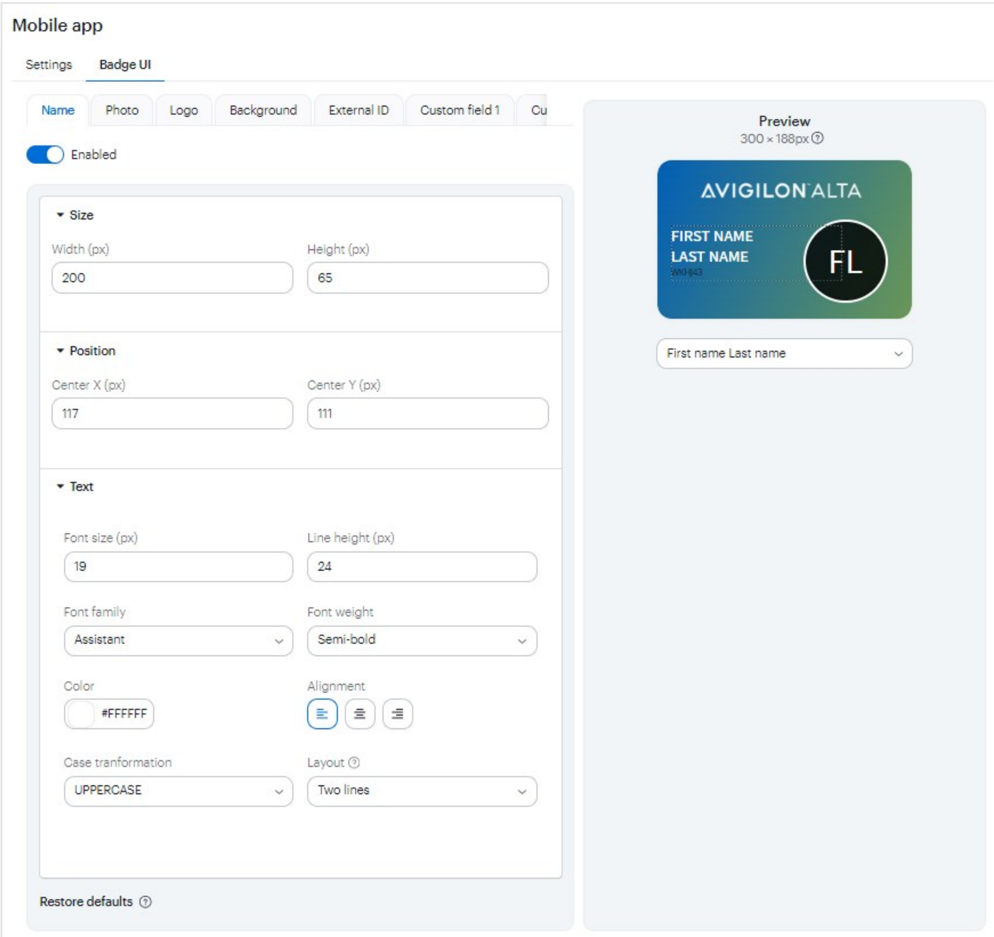
[1] Choosing to filter by site, zone, or entry includes the users who are visiting from other sites.

Type	Related settings
	Note: The alert code must match the alert code defined in the third-party system. **Authentication method** — Choose from: **Note:** Supported authentication methods are dependent on the emergency notification and response system. **Basic** — Enter the **URL** of the emergency notification and response system (example: `https://www.yourdomain.com/authentication_pathname`), **Username**, and **Password**. **Header** — Enter the **URL** of the emergency notification and response system (see example above), and credentials in the **Authorization header value** (example: `Basic ABCdef123`). **URL** — Embed the credentials in the **URL** of the emergency notification and response system (example: `https://www.yourdomain.com/authentication_pathname?auth=BasicABCdef123`). For more examples, see this Alta Access article.
Email / SMS	**Subject** — The subject of the notification. **Body** — The body of the notification. **Recipients** — The phone numbers or emails.
Lockdown	**Lockdown plan** — The lockdown plan. **Lockdown action** — **Trigger lockdown** or **Revert lockdown**.
On-screen notification	**Send to** — One or more users who will receive email notifications.
Relay	**ACU relay port number to trigger** — The port number. The triggered relay will be on the same ACU that the trigger event occurred on. • Single Door Controller: 1 or 2 • Access Control Core: 1, 2, 3, or 4 • Core Series expansion boards: `(expansion number x 10000) + relay port number` Example: Expansion board 2 on relay port 12 is 20012. • Auxiliary relays: `(expansion number x 10000) + (max. port number + AUX number)` Example using 8-Port Board: Expansion board 3 on AUX Relay 2 is 30010. You can also find these port IDs using the Alta Access API. **State** — **Engage** or **Disengage**.

Type	Related settings
	Duration (seconds) — The duration in seconds.
Webhook	**URL** — The URL for the webhook API call. **HTTP method** — The GET or POST method.
For all types	Select when the action is triggered by the user: • **Delay before action (seconds)** — The delay in seconds. • **Block next action until finished and quit on error** — The action needs a response before triggering another action (for example, acknowledging before clearing an alarm). Select when one or more actions are performed by the monitoring operator: • **Created** — When alarm is created. • **Acknowledged** — When alarm is acknowledged. • **Cleared** — When alarm is cleared manually. • **Auto cleared** — When alarm is cleared automatically. • **Cleared - false alarm** — When a false alarm is cleared manually. • **Reassigned** — When alarm is reassigned.

Mobile app

The Mobile app page is where you can enable badges on the Alta Open mobile app and design your organization's badge.



Enable badge view

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

1. Go to **Configurations** > **Mobile app**.
2. Select the **Enable badge view** toggle.

> **Note:** Users may need to update their Alta Open mobile app to the latest version to see the badge in their app.

Customize badge design

1. Click the **Badge UI** tab to design the digital badge.
2. On the **Name** tab, adjust the size, position, and text formatting.
3. On the **Photo** tab, adjust the position of the user's photo and select a color for the photo's border.

> **Note:** A user without a photo will instead display their initials.

4. On the **Logo** tab:
   - Click **Select Logo** to upload an image in PNG, JPG, or JPEG format.
   - Click **Replace Logo** to replace an existing one, or remove the image to use text instead.

> **Note:** You cannot edit the **Text** settings if an image is selected.

5. On the **Background** tab:
   - Click **Select Image** to use your own background image.
   - To use a solid color background instead, click the color tile in **Background color** to select a color using the color picker (see example below), or drag the slider to enter your color in the **HEX**, **RGB**, or **HSB** color model.

6. On the **External ID** tab, select the **External ID** toggle, and adjust the size, position, and text formatting.
7. On the **Custom field 1** and **Custom field 2** tabs, choose additional user information.

> **Note:** To create a custom field, go to **Users** > **Custom fields**.

8. Click **Save** to publish your changes.

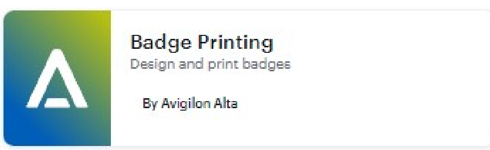
Tips for badge design

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

Badge templates

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

Note: Before you start, go to the App marketplace and install the Badge Printing app.



Add badge template

1. Go to **Configurations** > **Badge templates**.
2. Click in the upper-right corner.
3. On the **Settings** tab, select a **Base template** (see the Preview on the right) and enter a name in **Template name**.

Tip: To use the default template without customizing further, click **Save** and proceed to printing your badges.

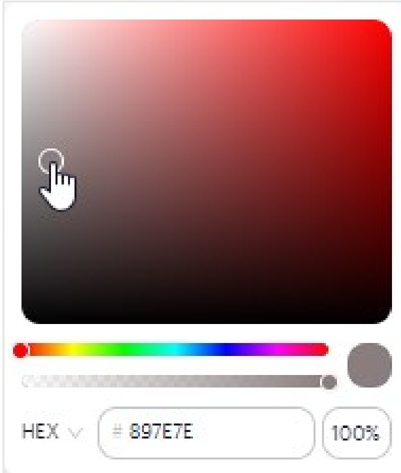
4. To set the template as the default for the organization, click the **Org default** slider.
   - On the **Name** tab, adjust the size, position, and text formatting.
   - On the **Photo** tab, adjust the position of the user's photo and select a color for the photo's border.

     Note: A user without a photo will instead display their initials.

   - On the **Logo** tab:
     - Click **Select Logo** to upload an image in PNG, JPG, or JPEG format.
     - Click **Replace Logo** to replace an existing one, or remove the image to use text instead.

     Note: You cannot edit the **Text** settings if an image is selected.

   - On the **Background** tab:
     - Click **Select Image** to use your own background image.
     - To use a solid color background instead, click the color tile in **Background color** to select a color using the color picker (see example below), or drag the slider to enter your color in the **HEX**, **RGB**, or **HSB** color model.



- On the **External ID** tab, select the **External ID** toggle, and adjust the size, position, and text formatting.
- On the **Custom field 1** and **Custom field 2** tabs, choose additional user information.

> **Note:** To create a custom field, go to **Users** > **Custom fields**.

- Click **Save** to publish your changes.

Print badge

- From **Configurations** > **Badge templates**:
  1. Click the template you'd like to print.
  2. In the **Preview** section, select the name of the user whose badge you want to print.
  3. Click **Print Badge**.
  4. Select the badge printer from the browser's print utility, or close and save the high res image to print via a different method.
- From **Users** > **Users**:
  1. Click on the name of the user whose card credential you want to print.
  2. On the Credentials tab, click the print icon next to the card credential.

  > **Note:** If you don't see the print icon , click the Edit icon next to the card, assign a badge template, and click **Save**.

  3. Select the badge printer from the browser's print utility, or close and save the high-res image to print via a different method.

Printing tips

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

Administration

The Administration page is where you set up an account for the organization; choose a subscription plan depending on the number of users, devices and entries in your organization; and set up billing information.

Account

Use the Account page to define organization details, set up purchasing and billing information, and review and accept the Terms of service.

Accept terms and conditions

1. Go to **Administration** > **Account**.
2. Review the terms and conditions and click **Agree and submit**.

Add help contact for mobile credential users

When a user is unable to access an entry using the Alta Open mobile app, an email can be sent to the site's administrator for help.

> **Note:** Alta Open mobile app version 2.10.0 or newer is required. If an email is not provided, the request will go to Avigilon Alta Support by default.

1. In the USER HELP CONTACT section, click **Change settings**.
   - Enter one or more emails in **Email**.

     The email will provide an error code with the reason and troubleshooting steps. For a list of the possible codes, see this Alta Access article.
   - Optional. Enter one or more phone numbers in **Phone**.
2. Click **Save**.

Edit organization information

1. In the INFO section, click **Change settings**.
   - Enter your **Organization Name** and **Accounts payable email**.
   - Set the language of Alta Access emails in **Organization Language**.
2. Click **Save**.

Edit security settings

1. In the **Security settings** section, click **Change settings**.
   - **Offline timeout setting (days)**: The number of days that an ACU can be offline before the token expires. After this time, credentials will not authenticate. The maximum duration is 60 days.
   - **Suspend idle users timeout setting (days)**: Suspends users who have not unlocked an entry within the set duration. The minimum duration is the offline timeout duration plus 7 days. Leave the setting blank to never suspend users.

     > **Note:** Users with portal access will never be suspended.

   - **Allow your parent org to have VIEW access to this org**: Enabled by default. Disable at anytime to prevent your parent organization from viewing your organization.

     > **Note:** Setting is shown only your integrator is configured as a parent org.

   - **Allow Avigilon Alta Support to have VIEW access to this organization**: Enabled by default. Disable at anytime to prevent Avigilon Alta Support from viewing your organization.
   - **Allow Avigilon Alta Support to have EDIT access to this organization** and **Allow Avigilon Alta Support to have UNLOCK access to this organization**: These settings cannot be enabled; you must escalate changes to Avigilon Alta Support or Engineering.
   - **Enable remote unlock by default for new users**

     > **Note:** Existing users are not impacted by changes to this setting. This feature is not applicable to Schlage no-tour wireless locks.

   - **Enable PIN masking**: Disabled by default throughout an organization. Enable at anytime to mask (hide) PIN credentials from viewing by all Alta Access users.
2. Click **Save**.

Quick start for sites, ACUs, and readers

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

Licenses

To upgrade a Basic package to Premium or Enterprise:

1. Go to **Administration** > **Licenses**.
2. View the licensed-based features that can be purchased and details, including SKUs and quantities.

For example, the **Basic: Entries** license provides 2 entries and the **Enterprise: Entries** license provides 1000 entries.

3. Click **Request package** and then **Yes**.

To view the requested licenses, select the **Request history** tab.

Troubleshooting

Event descriptions

For the event descriptions for Alta Access, see
help.openpath.com/space/EHC/1504247809/Avigilon+Alta+event+definitions.

Appendix

Configure mobile gateway with legacy access control systems

You can configure Alta Access to support legacy access control systems. In this configuration, the legacy panel controls all locking hardware and entry mechanisms while the Alta access control system lets you use the Alta Open mobile app, Smart Reader, and Wave to Unlock functionality.

System overview

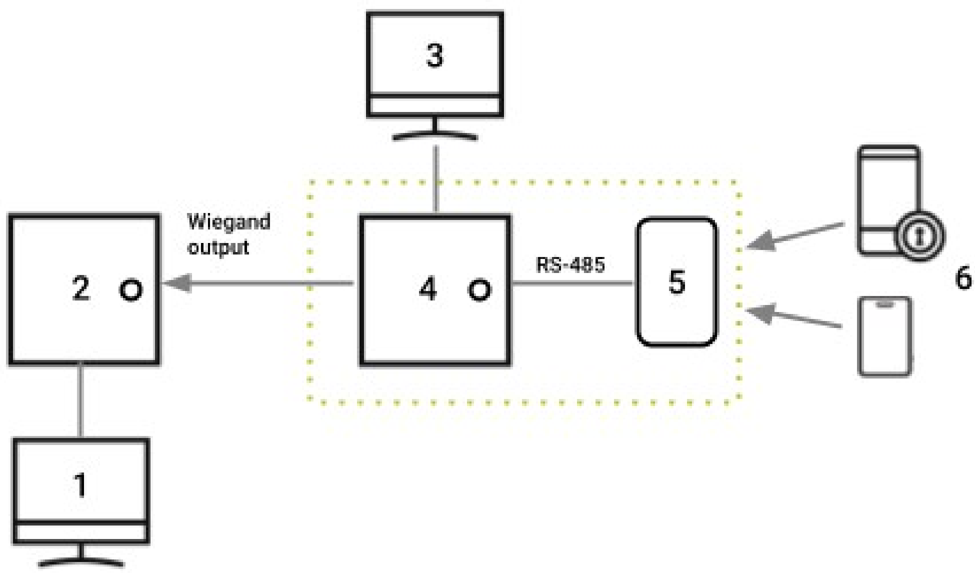


Figure 1 Mobile Gateway diagram

1	Legacy access control system software
2	Legacy access control system panel
3	Alta Access
4a	Smart Hub ACU installed between the Smart Reader and the legacy panel **Note:** The Pro series reader does not require a controller, however, a Smart Hub is required to support locking hardware.
4b	Wiegand port configured as output to the legacy panel For more information, see advanced wiring configuration.
5	Smart Readers If existing Wiegand readers use a proprietary card format, they can be wired to new Smart Readers. Otherwise, replace existing readers with Smart Readers.

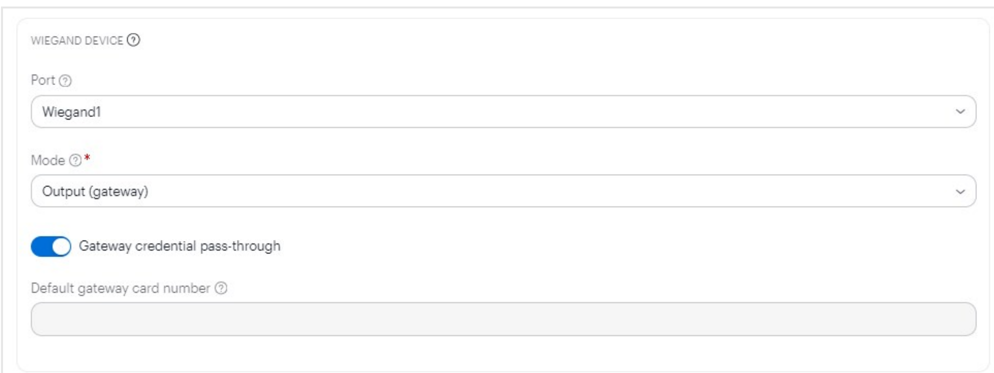
6	Avigilon Alta Open mobile app, Cloud Key credentials and Wave to unlock functionality Avigilon credential with default gateway number or Wiegand ID

Configure Wiegand device settings

- On the **Sites** > **Entries** page, configure the Wiegand port for Output (gateway) mode.
  - **Port** — The port for the Wiegand device to which this entry is wired.
  - **Mode** — The direction the card credential data is sent.
    - **Input** — Receives data from the Wiegand reader.
    - **Output (gateway)** — Sends credential data to a third-party control panel.

      Enable **Gateway credential pass-through** if you do not want Alta Access to authenticate credentials, but rather send all data to the legacy panel for authentication.

      Enter a **Default gateway card number** so that all credentials (including mobile credentials) are sent to the legacy panel as a Wiegand ID.



- On the **Users** page, configure the credential.
  - For users who initiate authenticated unlock requests with a valid Avigilon credential but do not have a dedicated **Card: Wiegand ID** credential set to **Use for Gateway** to be sent to the legacy panel, define a **Default gateway card number** on the Entries page that will be sent instead.
  - Instead of setting up a **Default gateway card number** for the entry, you can send individual user credentials to the legacy panel. Create a **Card: Wiegand ID** 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 Avigilon credentials.

> **Note:** This configuration supports one-to-one credential mapping for accurate user-level reporting within the legacy system. See Issue keycard, fob, license plate, mobile, PIN, wiegand, or cloud-based credentials on page 46.

Post-installation testing

To test newly installed devices, complete any of the following in Alta Access:

- On the Users page, issue the following credentials to a user account:
  - **Card: Wiegand ID** — An Avigilon low-frequency key fob or card for Wiegand-based access control systems.
  - **Card: Openpath/MIFARE (CSN) - Fast** — The Card Serial Number of an Avigilon HF card or fob.
- Scan the user's keycards on a connected reader. Also scan keycards not added to the user account.
  - On the Dashboards page, confirm the access grant and access denial events on the **Activity dashboard** and **Activity logs**.
- If using a contact sensor, enable the **Ajar feature** and **Forced-Open detection** settings on the entry page.
  - Trigger the door ajar event by keeping the door open past the maximum duration.
  - Trigger the forced-open event by opening the door without using the keycard.
  - On the **Entry dashboard**, confirm the state changes.
  - On the **Configurations** > **Alerts** page, set up email or SMS alerts for the above events and confirm they are received.
- If using a REX device, enable the **Trigger relay to unlock entry** setting on the entry page.
  - If controlling the relay, ensure the relay is firing correctly.
  - If not controlling the relay, confirm the REX events on **Activity logs**.
- If using an entry schedule, go to **Sites** > **Entry schedules** and create a schedule to change from **Convenience** to **Unlocked**.
  - On the **Entry dashboard**, confirm the entries are all open when this schedule takes effect.
  - Confirm the revert to a locked state when the schedule ends.
- If using a mobile credential over a cellular network, confirm the unlocking event on the **Entry dashboard**.
- If using a lockdown plan, go to **Sites** > **Lockdown plans** and configure the lockdown trigger and revert settings.
  - Trigger a lockdown plan and revert it.
  - Dashboards page, confirm the state changes.
- If using a rule to perform an action based on an **Input** trigger and events, go to **Configurations** > **Rules**.

Glossary

C

CAP

Common Alerting Protocol. An open, industry-standard message format for exchanging emergency notifications and alerts over a network. The transmission of alert codes to external systems is supported, if associated actions are triggered in Alta Access rule or alarm configuration.