alcatraz ai

Alcatraz AI Admin Portal Guide v 2.5

Ver. 1.0

Contents

Contents

Glossary

1FA	Single Factor Authentication allows a user to access an area with either a badge credential or facial authentication.
1FAF	Single Factor Authentication Face-Only allows a user to access an area with facial authentication only.
2FA	Two Factor Authentication requires a user to authenticate with face and swipe a badge to access an area.
3FA	Three Factor Authentication requires a user to authenticate with face, swipe a badge and enter a PIN to access an area.
ACS (Access Control System)	A system that controls who has access to a space, determines who can enter or exit.
Card Format	Digital representation of the badge ID programmed onto a physical badge.
Crossing	A person enters a space when the user exits.
Enrollment	The process to bind a badge with a user to create a profile that is unique to the user for authentication purposes. The Rock can perform auto-enrollment where it will learn over time and associate a badge with a user. The Rock can perform manual enrollment where the user profile is created in one shot.
Mask Enforcement	Mask enforcement can be set in the Rock to ensure that a user must always wear a mask when entering a space.
Onboarding	Steps to associated the Rock with the Alcatraz AI Admin Portal once physical installation is complete and confirmed to be wired correctly.
ONVIF (Open Network Video Interface Forum)	Forum to standardize IP-based video security products.
ONVIF Profile S	Supports basic streaming and configurations.
ONVIF Profile T	Expands on Profile S to widen features covered such as imaging configurations, compression formats, HTTPS for secure video streaming.
OSDP	An access control communications standard developed by the Security Industry Association (SIA) to improve interoperability among access control and security products.
Tailgating	A user is followed by another person when entering a space.
Un-Authorized Entry	A user cannot be identified when entering a space.
Crossing	A user that gains entry while another user is leaving a space.

Overview

The Alcatraz AI Admin Portal provides administrative functions for Alcatraz Rocks. Once the Rock has been installed on the wall, the portal is required to commission the Rocks. After the Rocks are commissioned, the portal is used to configure, monitor and administer Rocks.

Log in to the Alcatraz AI Admin Portal to:

- Monitor the status of Rocks
- Configure Rock mode of operation
- Change configuration parameters
- Update firmware
- View security events
- Manage user profiles

To request access to the Alcatraz AI Admin Portal, contact your Company Account Administrator. Permissions to make changes or delete in the portal will be limited to user roles assigned by your Account Admin.

1 —
Quick Start

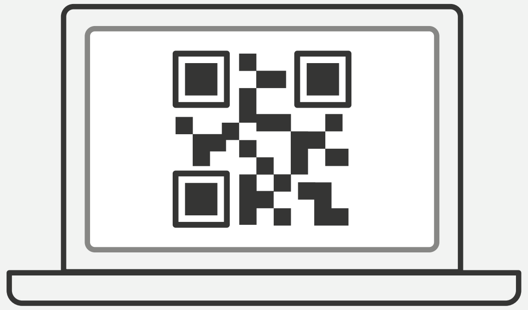
1 Start with

— Requesting an Alcatraz AI Admin Portal login from your Account Administrator

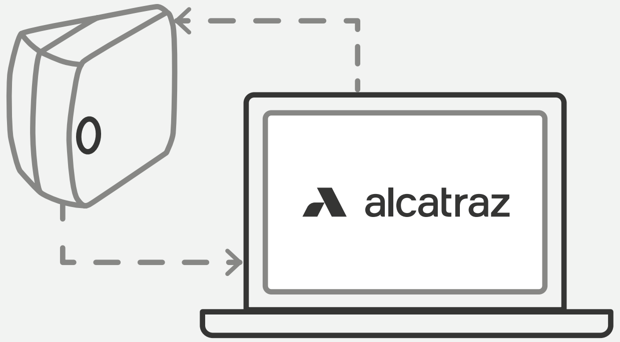
or

— Submiting a request for a login at support.alcatraz.ai

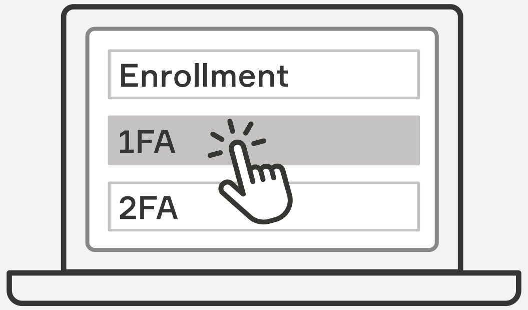
2 Generate QR Code



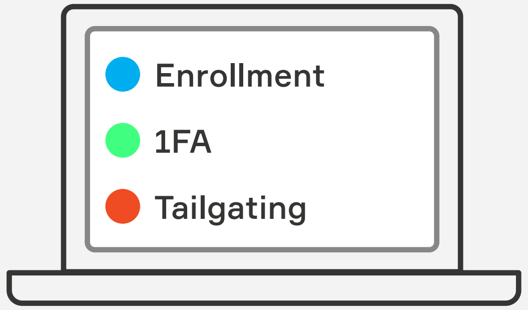
3 Onboard a Rock



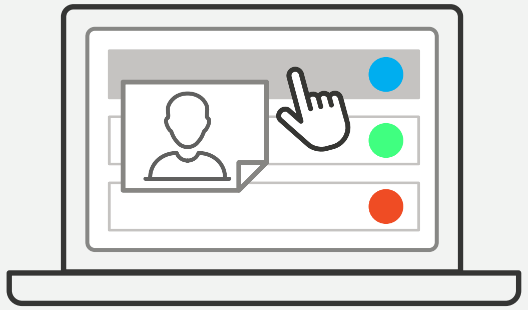
4 Configure Rock Mode



5 View Security Events



6 Check Profiles



2 —
Dashboard

alcatraz ai
Dashboard
Account
Permissions
Device Management
Security Events
Profiles

The dashboard is the landing page after logging in to the Alcatraz AI Admin Portal. This page provides a summary of metrics and security events information.

Recorded Security Events

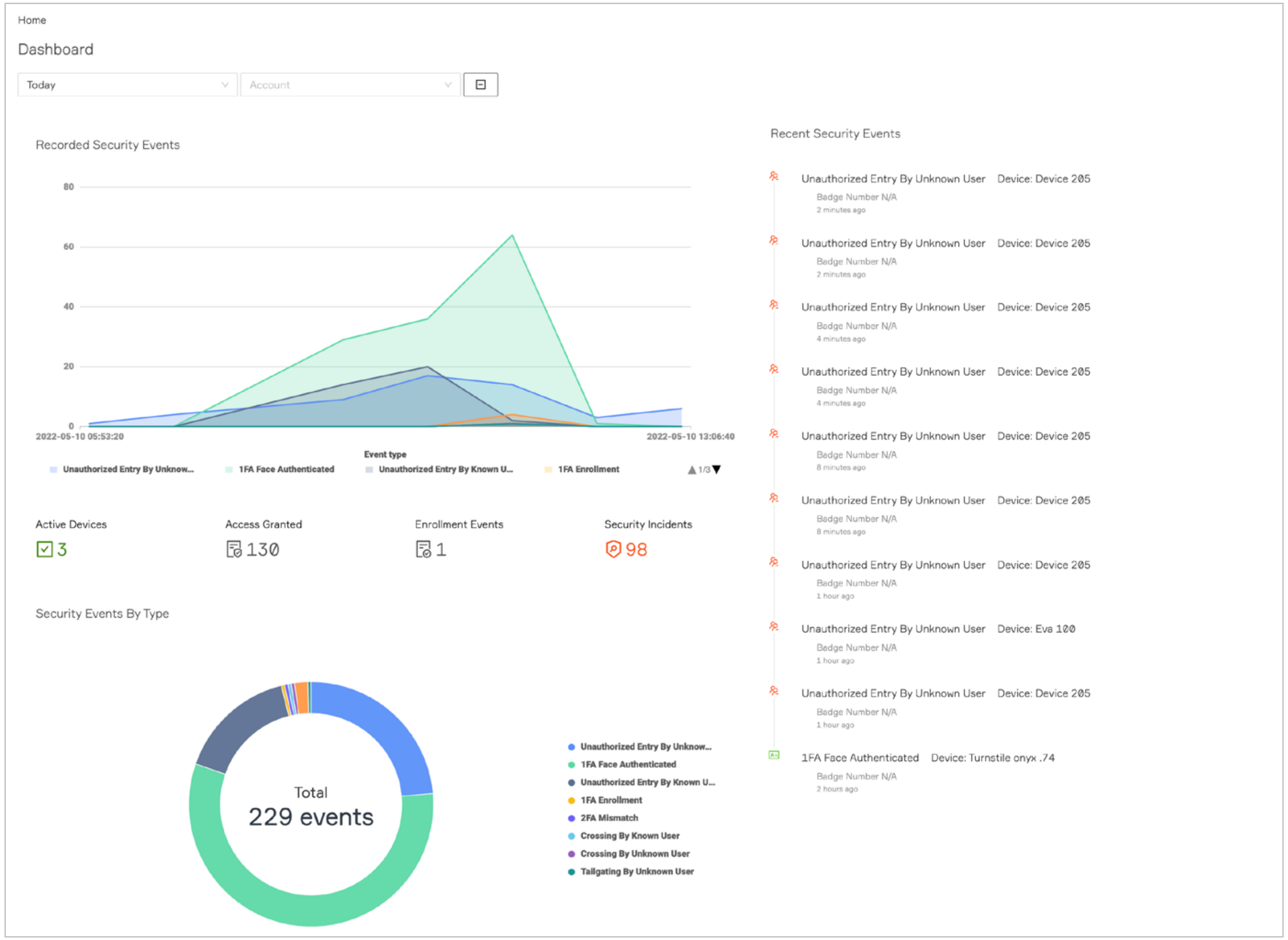
- Hover your cursor over the graph to get metrics for the security events over time or filter on a timeframe by selecting from the drop-down menu
- Click on the security event names to filter out the events you do not wish to view on the graph.

Recent Security Events

- View Recent Security Events as they occur on the right-hand side
- Click on the event to view additional info including the image

Security Events by Type

- Hover your cursor over the donut to get metrics for the security events by the different types
- Click on the color-coded circles or security event name to gray and filter out the security events from the donut



Active Devices 3

Access Granted 130

Enrollment Events 1

Security Incidents 98

Recent Security Events

Unauthorized Entry By Unknown User Device: Device 205
Badge Number N/A
2 minutes ago

Unauthorized Entry By Unknown User Device: Device 205
Badge Number N/A
2 minutes ago

Unauthorized Entry By Unknown User Device: Device 205
Badge Number N/A
4 minutes ago

Unauthorized Entry By Unknown User Device: Device 205
Badge Number N/A
4 minutes ago

Unauthorized Entry By Unknown User Device: Device 205
Badge Number N/A
8 minutes ago

Unauthorized Entry By Unknown User Device: Device 205
Badge Number N/A
8 minutes ago

Unauthorized Entry By Unknown User Device: Device 205
Badge Number N/A
1 hour ago

Unauthorized Entry By Unknown User Device: Eva 100
Badge Number N/A
1 hour ago

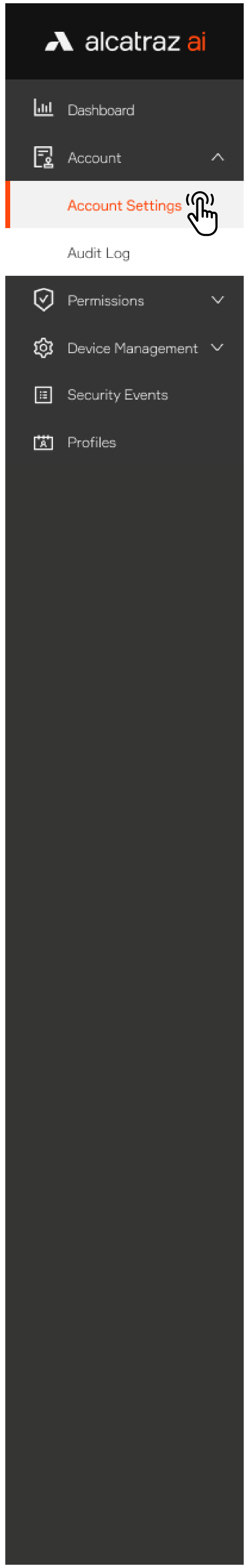
Unauthorized Entry By Unknown User Device: Device 205
Badge Number N/A
1 hour ago

1FA Face Authenticated Device: Turnstile onyx .74
Badge Number N/A
2 hours ago

Please note that the information displayed on the dashboard varies with access permissions associated with user roles.

3 —
Account

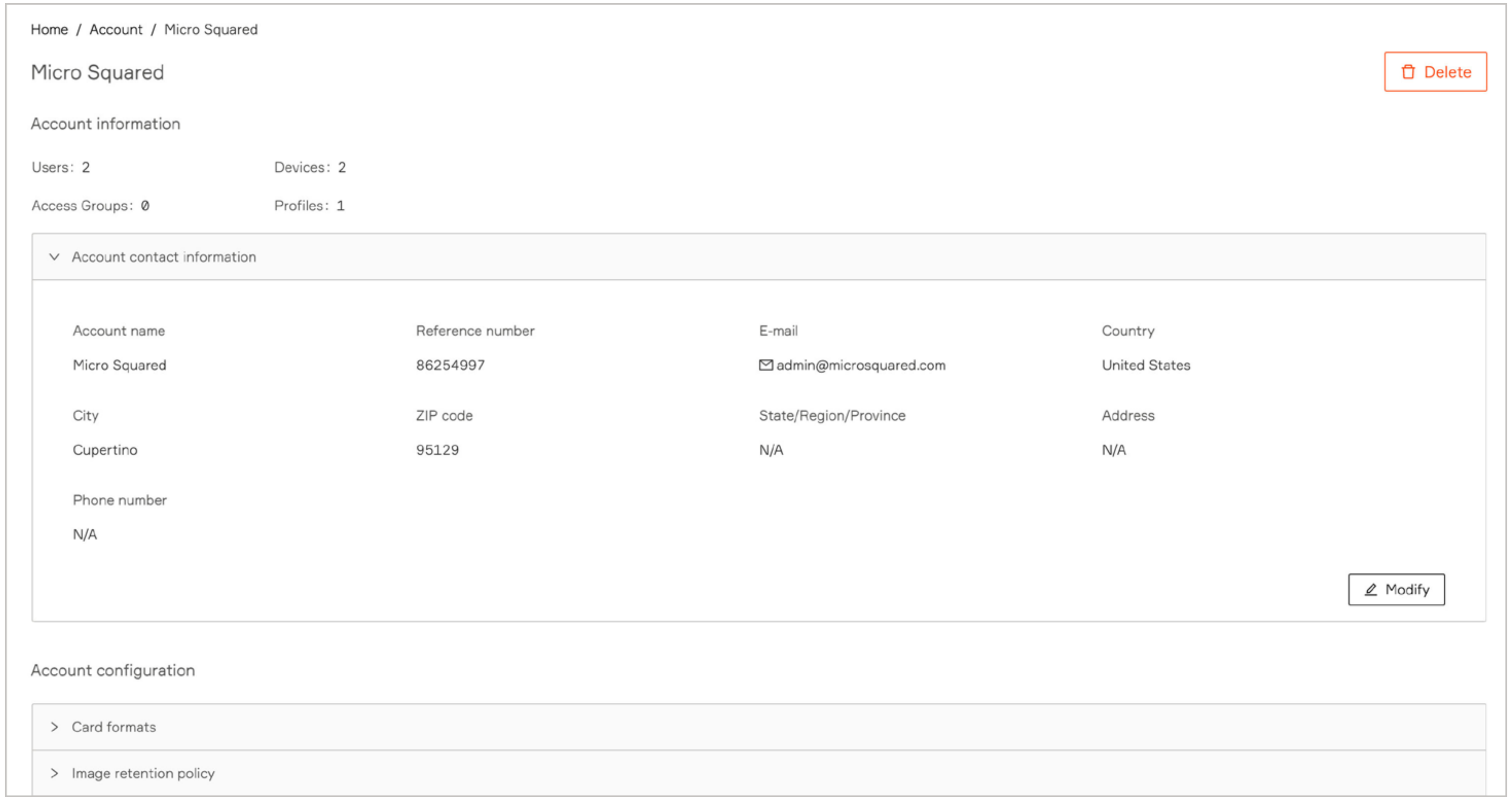
Accounts are created for each customer to manage Rocks. Each account should be assigned an Account Administrator to be responsible for managing the Account. This would include creating other admins or portal users as well as configuring card formats.



3.1—Account Settings

3.1.1—View Account Information

1. To view the account information go to **Account —> Account Settings**.
2. The Account information page will be displayed.



Micro Squared

Account information

Users: 2 Devices: 2

Access Groups: 0 Profiles: 1

Account contact information

Account name	Reference number	E-mail	Country
Micro Squared	86254997	admin@microsquared.com	United States
City	**ZIP code**	**State/Region/Province**	**Address**
Cupertino	95129	N/A	N/A
Phone number			
N/A			

Account configuration

> Card formats

> Image retention policy

alcatraz ai
Dashboard
Account
Account Settings
Audit Log
Permissions
Device Management
Security Events
Profiles

3.1.2—Configure Card Format

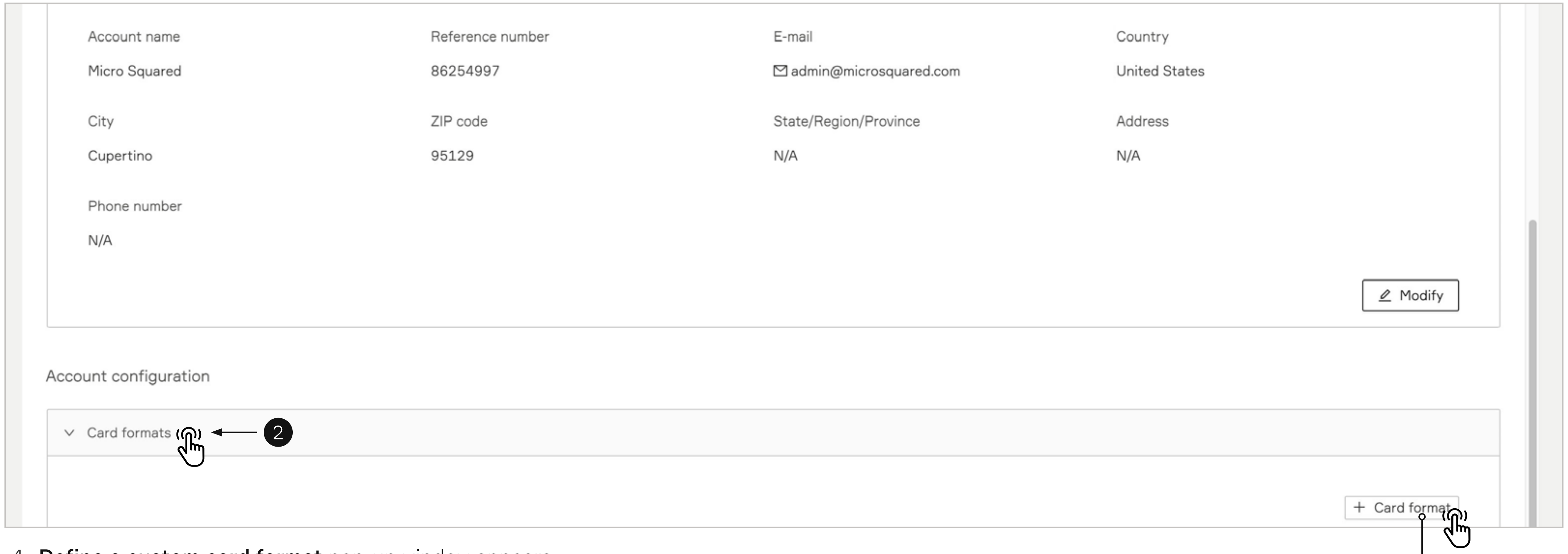
The Rock operates with any type of badge reader and badge.
When a company distributes badges to its employees, these badges will have a specific card “format”. Card formats define how data is encoded in the card. Many cards have a facility code and a card number but it is possible that the format only contains a card number. Cards will vary in sizes such as 26, 33, 37, 48 bits although the bits do not indicate the format. The facility code and card number can be displayed if the size and location of the bits within the bit length are known.
Companies may also have more than one card format. The Alcatraz AI Admin Portal is able to display the correct badge number and facility code as long the card formats are configured for the account. The portal supports configuring multiple card formats.

Card formats are configured once for the Account. The information used for configuring can be obtained from your Access Control System (ACS) administrator.

3.1.2.1—Configure a Pre-defined Card Format

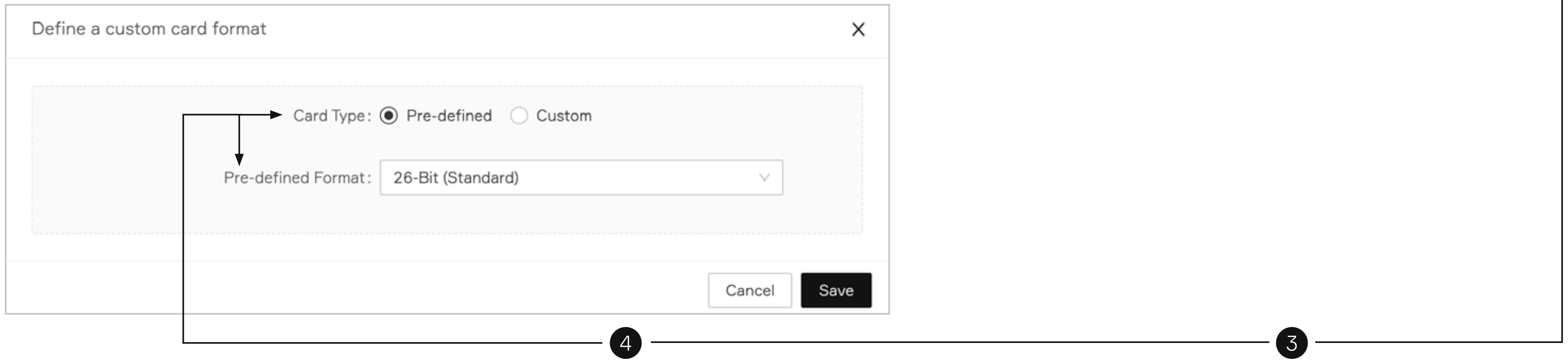
For convenience, some of the popular card formats have been pre-defined and can be selected for use.

1. Go to **Account —> Account Settings** .
2. Scroll down to **Account Configuration** and open the **Card formats** section.
3. Click **Create a Card Format**.



Account name	Reference number	E-mail	Country
Micro Squared	86254997	admin@microsquared.com	United States
City	**ZIP code**	**State/Region/Province**	**Address**
Cupertino	95129	N/A	N/A
Phone number			
N/A			

4. **Define a custom card format** pop-up window appears.



Define a custom card format

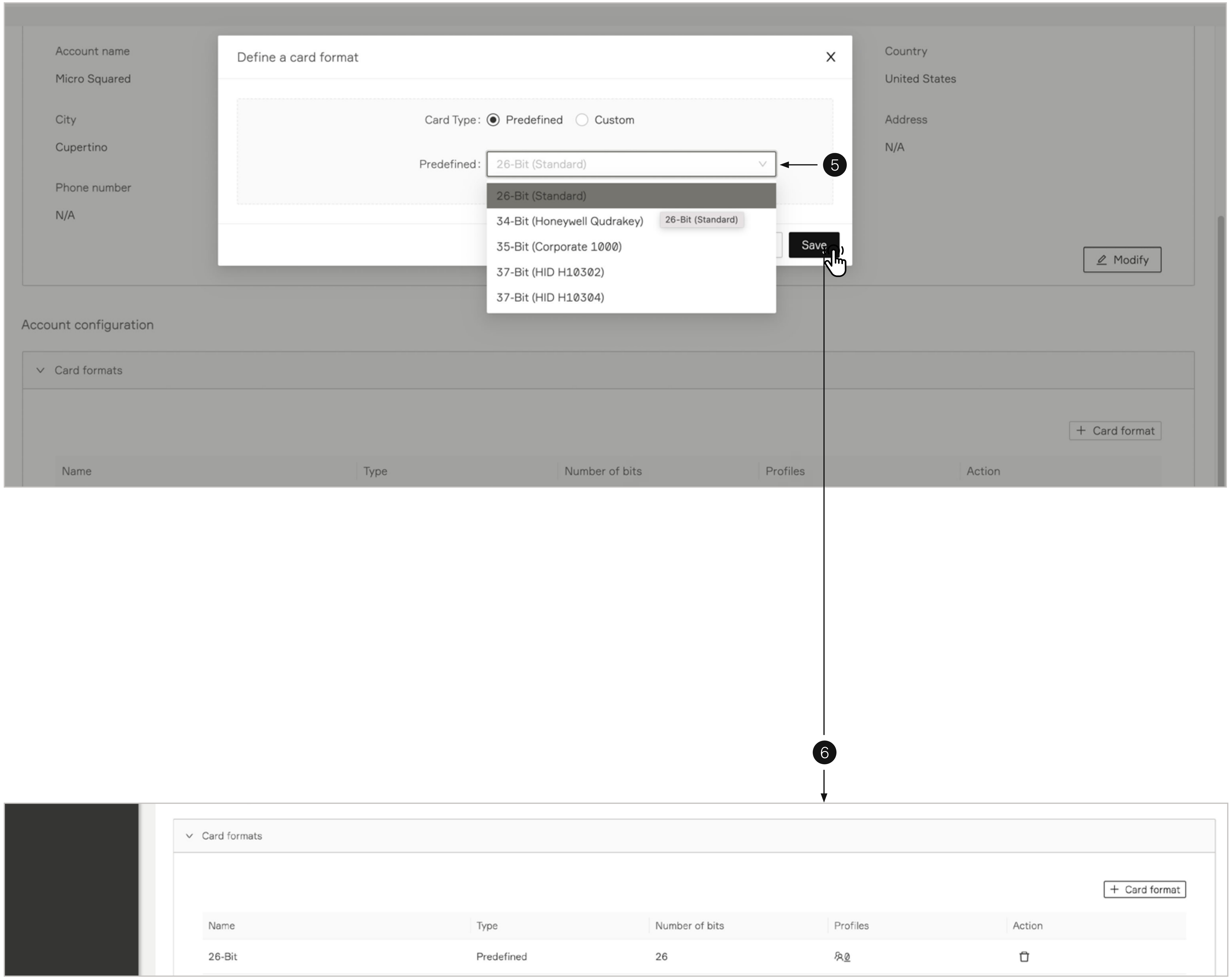
Card Type: ● Pre-defined ○ Custom

Pre-defined Format: 26-Bit (Standard)

alcatraz ai

- Dashboard
- Account
  - Account Settings
  - Audit Log
- Permissions
- Device Management
- Security Events
- Profiles

5. Select **Pre-defined** for Card Type and select a format from the Pre-defined Format list.
6. Click **Save** and the selected card format will be displayed in the list.



Account name: Micro Squared
City: Cupertino
Phone number: N/A
Country: United States
Address: N/A

Define a card format

Card Type: ● Predefined ○ Custom

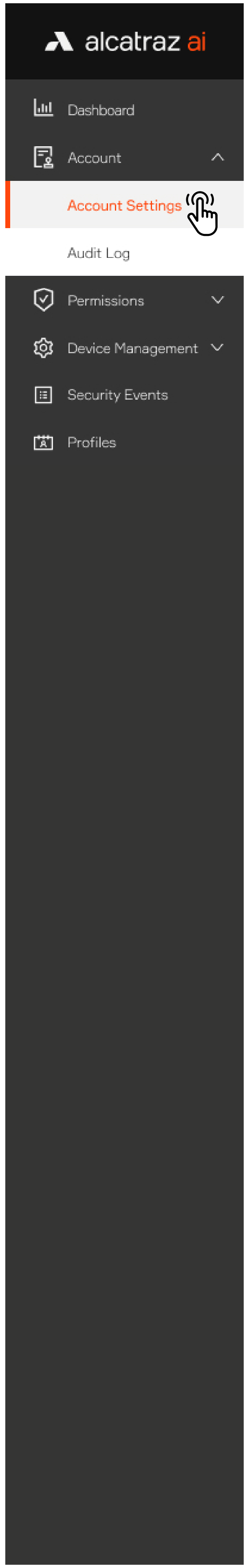
Predefined: 26-Bit (Standard)

- 26-Bit (Standard)
- 34-Bit (Honeywell Qudrakey)
- 35-Bit (Corporate 1000)
- 37-Bit (HID H10302)
- 37-Bit (HID H10304)

Account configuration

Card formats

Name	Type	Number of bits	Profiles	Action
26-Bit	Predefined	26		



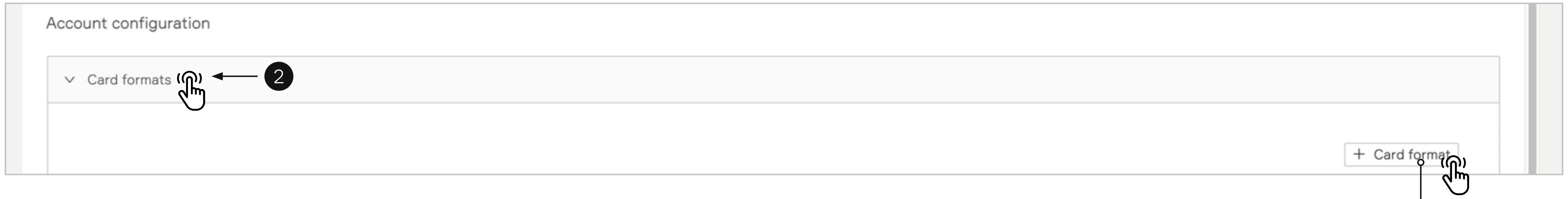
3.1.2.2—Configure a Custom Card Type

To configure a custom card format, before proceeding, retrieve the information from your Access Control System (ACS) Administrator.

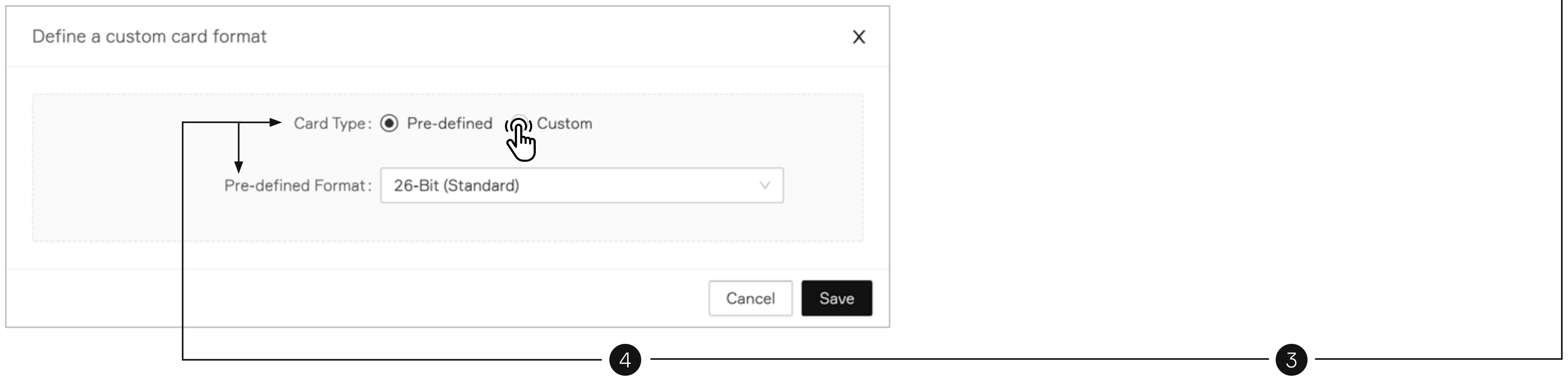
Information that may be part of your card format and needed as part of the configuration include:

- The start position and the number of bits for card number
- The start position and number of bits for the facility code
- Parity bits info

1. Go to **Account** —> **Account Settings** .
2. Scroll down to **Account Configuration** and open the **Card formats** section.
3. Click **Create a Card Format**.



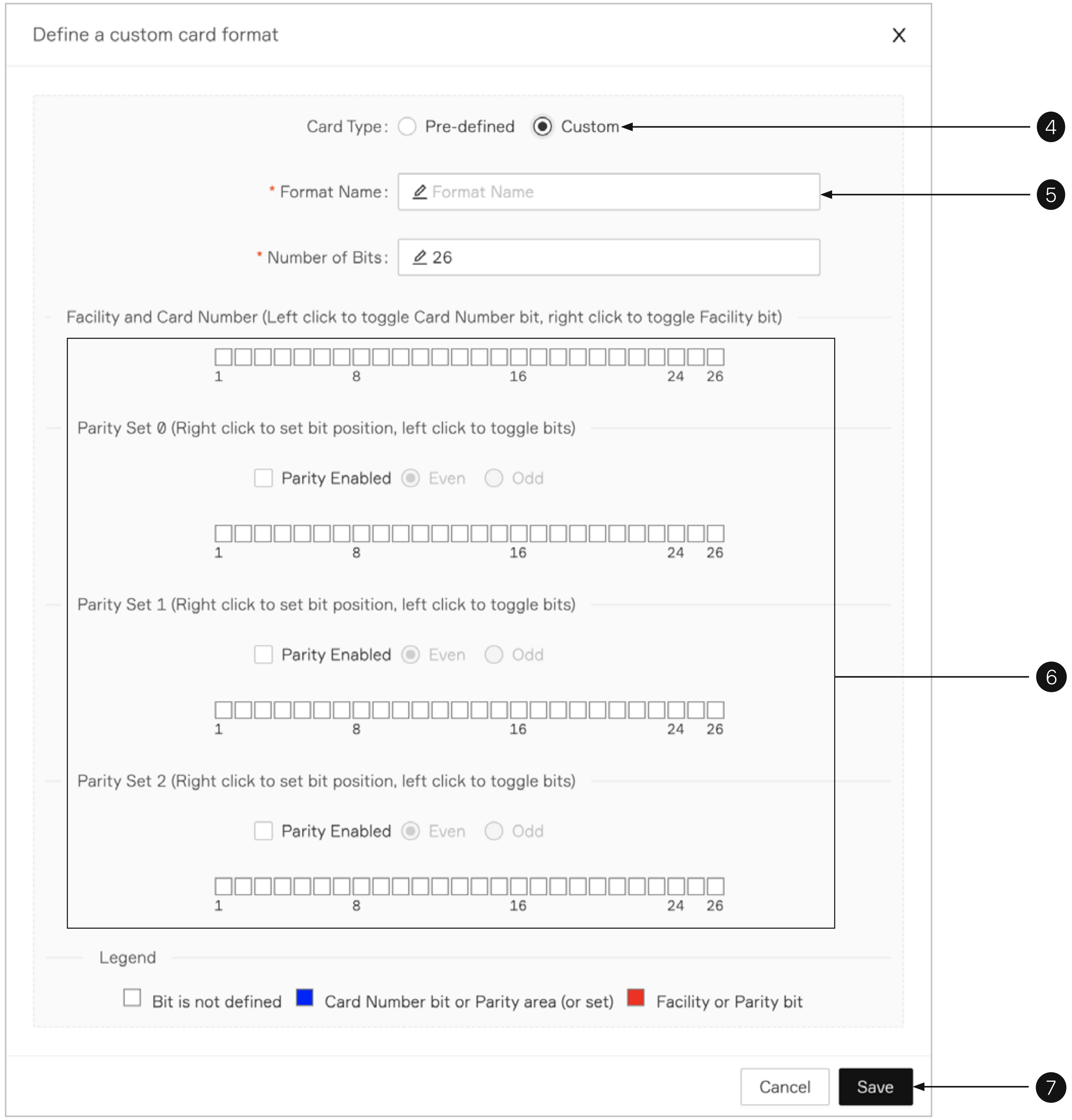
4. Select **Custom** for Card Type.
5. Give the card format a name and indicate number of bits.
   Please note that only one card format is allowed for a given bit length.


Define a custom card format

Card Type: ● Pre-defined ○ Custom

Pre-defined Format: 26-Bit (Standard)

6. Follow the information retrieved from the ACS Administrator and toggle bits as required.
7. Click **Save** when finished.



Define a custom card format

Card Type: ○ Pre-defined ● Custom

* Format Name: Format Name

* Number of Bits: 26

Facility and Card Number (Left click to toggle Card Number bit, right click to toggle Facility bit)

Parity Set 0 (Right click to set bit position, left click to toggle bits)

□ Parity Enabled ● Even ○ Odd

Parity Set 1 (Right click to set bit position, left click to toggle bits)

□ Parity Enabled ● Even ○ Odd

Parity Set 2 (Right click to set bit position, left click to toggle bits)

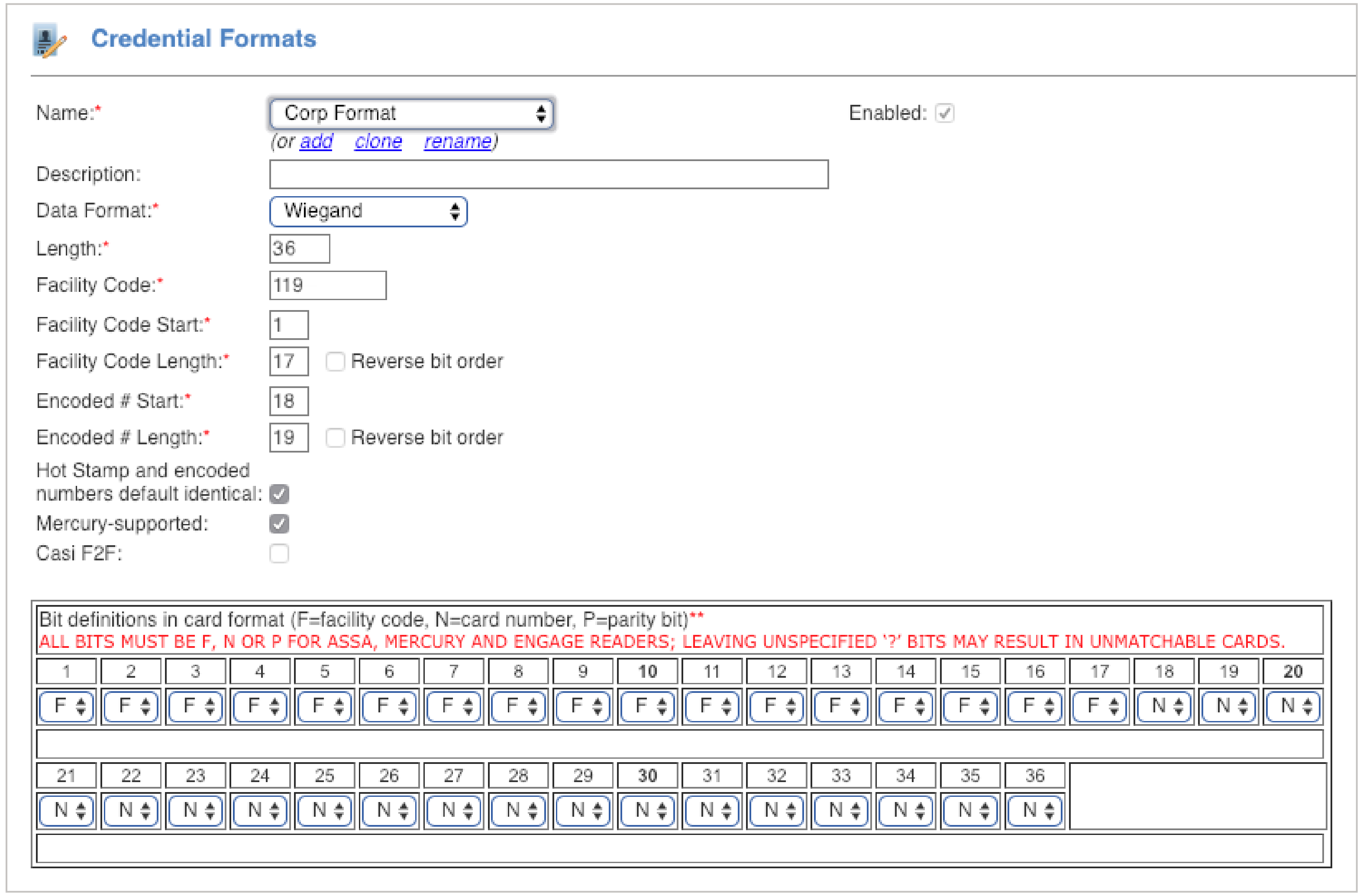
□ Parity Enabled ● Even ○ Odd

Legend

□ Bit is not defined 🟦 Card Number bit or Parity area (or set) 🟥 Facility or Parity bit

3.1.2.3—Example of Card Format with No Parity Bits

Card format info from ACS



Credential Formats

Name:* Corp Format (or add clone rename) Enabled: ☑

Description:

Data Format:* Wiegand

Length:* 36

Facility Code:* 119

Facility Code Start:* 1

Facility Code Length:* 17 □ Reverse bit order

Encoded # Start:* 18

Encoded # Length:* 19 □ Reverse bit order

Hot Stamp and encoded numbers default identical: ☑

Mercury-supported: ☑

Casi F2F: □

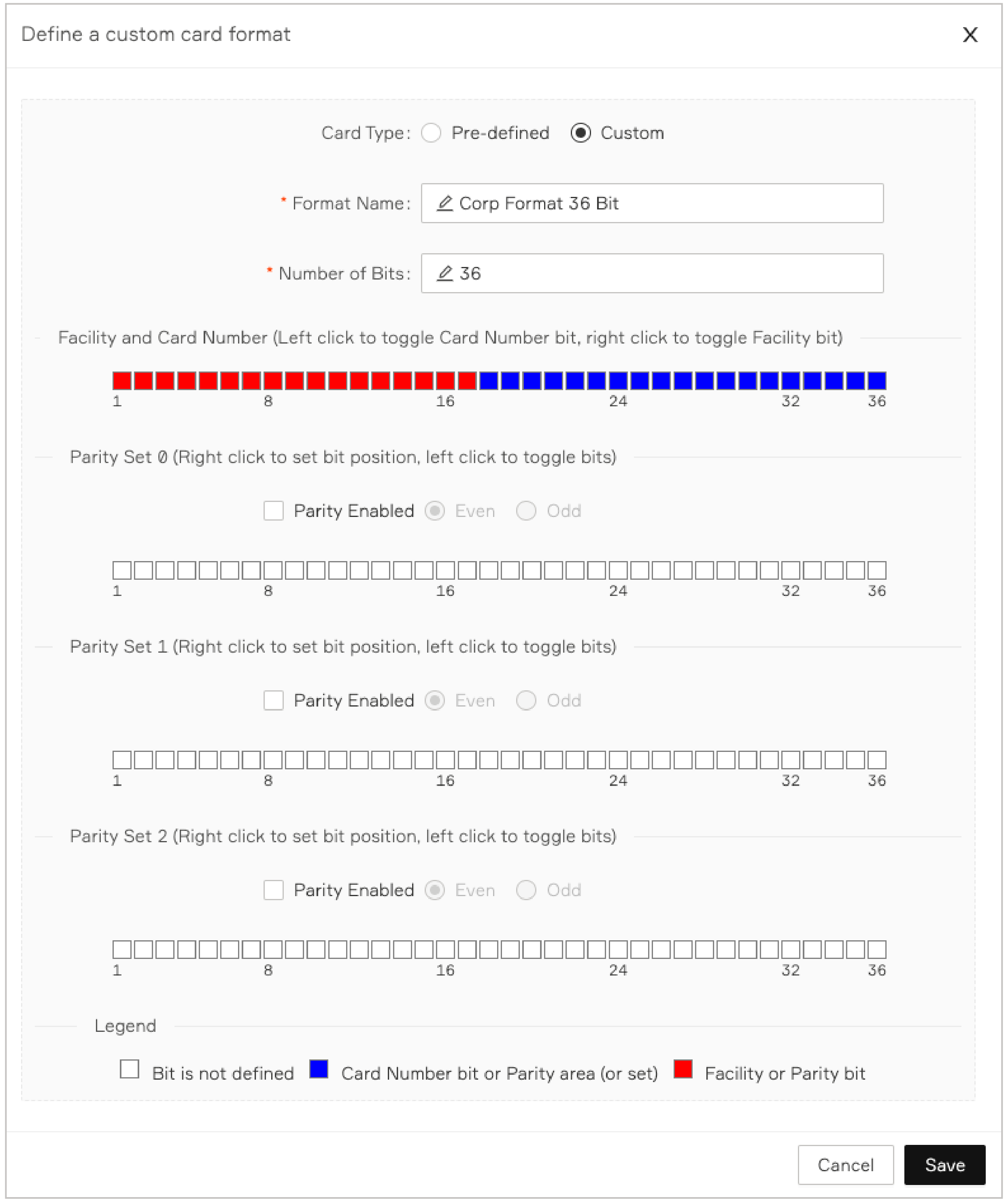
Bit definitions in card format (F=facility code, N=card number, P=parity bit)**

ALL BITS MUST BE F, N OR P FOR ASSA, MERCURY AND ENGAGE READERS; LEAVING UNSPECIFIED '?' BITS MAY RESULT IN UNMATCHABLE CARDS.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	N	N	N

21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N

Custom card format configured in Alcatraz AI Admin Portal



Define a custom card format ✕

Card Type: ○ Pre-defined ● Custom

* Format Name: Corp Format 36 Bit

* Number of Bits: 36

Facility and Card Number (Left click to toggle Card Number bit, right click to toggle Facility bit)

🟥🟥🟥🟥🟥🟥🟥🟥🟥🟥🟥🟥🟥🟥🟥🟥🟥🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦

1 8 16 24 32 36

Parity Set 0 (Right click to set bit position, left click to toggle bits)

□ Parity Enabled ● Even ○ Odd

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

1 8 16 24 32 36

Parity Set 1 (Right click to set bit position, left click to toggle bits)

□ Parity Enabled ● Even ○ Odd

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

1 8 16 24 32 36

Parity Set 2 (Right click to set bit position, left click to toggle bits)

□ Parity Enabled ● Even ○ Odd

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

1 8 16 24 32 36

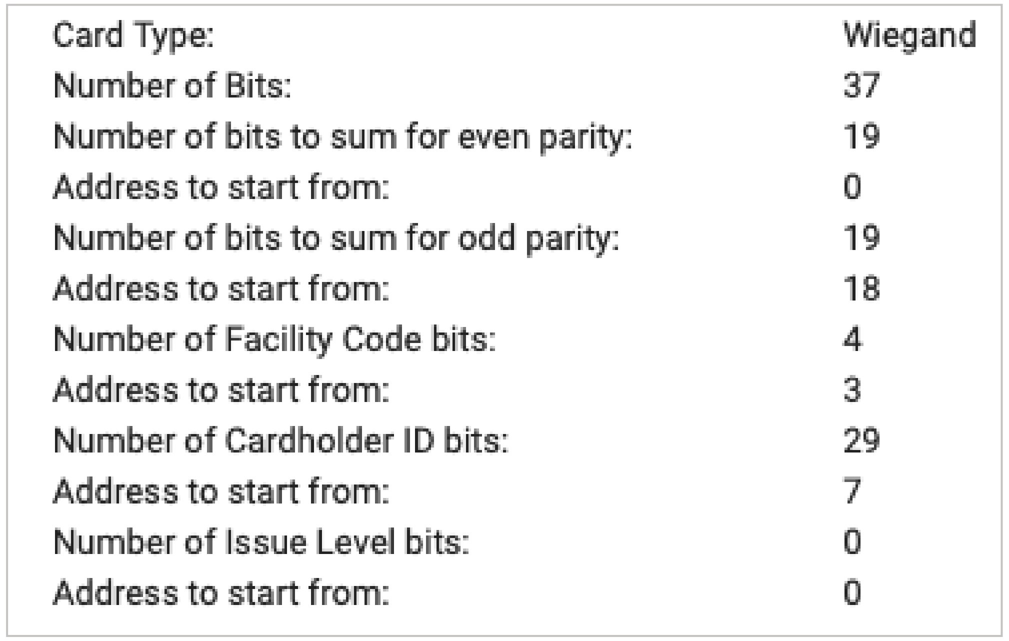
Legend

□ Bit is not defined 🟦 Card Number bit or Parity area (or set) 🟥 Facility or Parity bit

Cancel Save

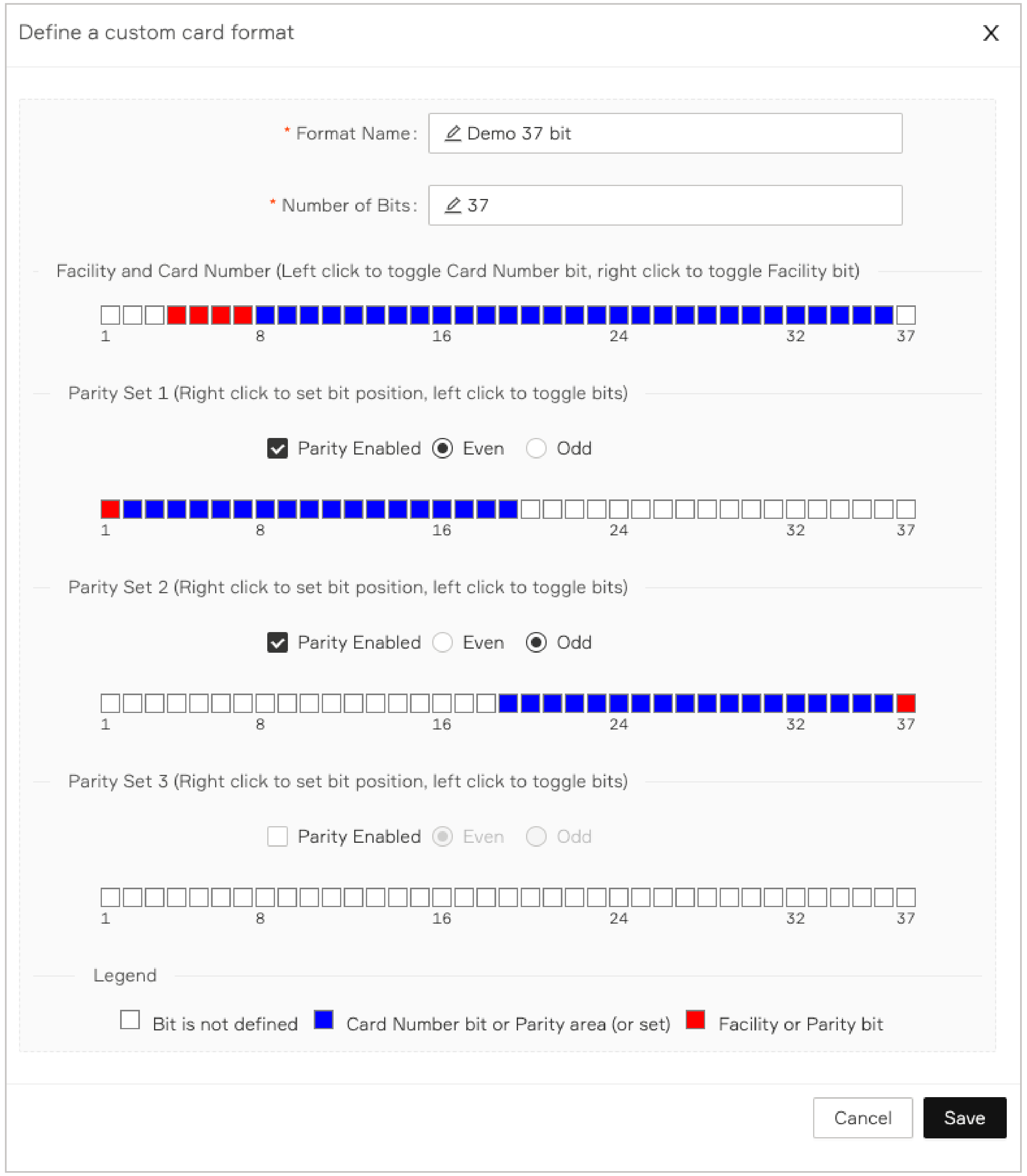
3.1.2.4—Example of Card Format Using Parity Bits

Card format info from ACS



Card Type:	Wiegand
Number of Bits:	37
Number of bits to sum for even parity:	19
Address to start from:	0
Number of bits to sum for odd parity:	19
Address to start from:	18
Number of Facility Code bits:	4
Address to start from:	3
Number of Cardholder ID bits:	29
Address to start from:	7
Number of Issue Level bits:	0
Address to start from:	0

Custom card format configured in Alcatraz AI Admin Portal



Define a custom card format

* Format Name: Demo 37 bit

* Number of Bits: 37

Facility and Card Number (Left click to toggle Card Number bit, right click to toggle Facility bit)

□□□🟥🟥🟥🟥🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦□
1 8 16 24 32 37

Parity Set 1 (Right click to set bit position, left click to toggle bits)

☑ Parity Enabled ● Even ○ Odd

🟥🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦□□□□□□□□□□□□□□□□□□
1 8 16 24 32 37

Parity Set 2 (Right click to set bit position, left click to toggle bits)

☑ Parity Enabled ○ Even ● Odd

□□□□□□□□□□□□□□□□□□🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟦🟥
1 8 16 24 32 37

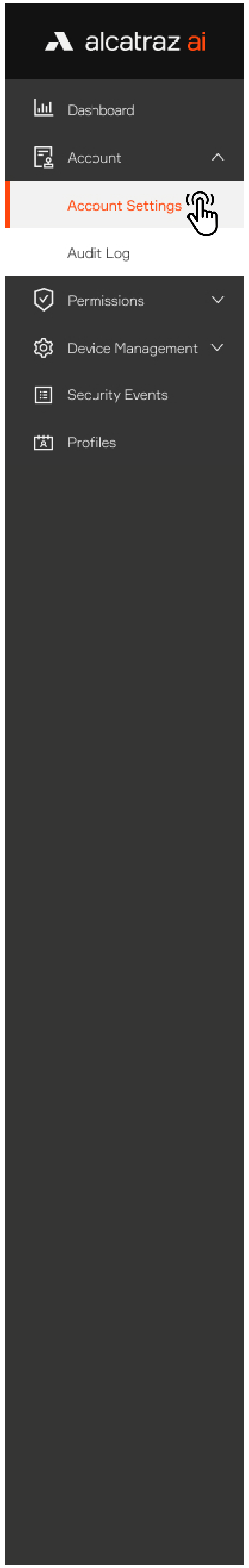
Parity Set 3 (Right click to set bit position, left click to toggle bits)

□ Parity Enabled ● Even ○ Odd

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
1 8 16 24 32 37

Legend

□ Bit is not defined 🟦 Card Number bit or Parity area (or set) 🟥 Facility or Parity bit



3.1.3—Image Retention Policy

Alcatraz AI allows different retention options for images, related to events.

1. Go to **Account** –> **Account Settings**.
2. Scroll down to the **Account Configuration** and open the **Image Retention** section to select the preferred retention period.
   Select one of the following:
   Keep all – all enrollment and event images are stored until storage is full (default option).
   Retention period – select options from the pre-defined list.
   Do not retain – no images will be saved. Be aware that also **all existing images will be deleted** if selected.
   a. **The ⓘ icon** next to each option displays **on hover** descriptive information about the retention period and its specifics.
   b. Each time when a new option is selected, a pop-up with detailed content is displayed, to make the user aware of the picked retention choice.

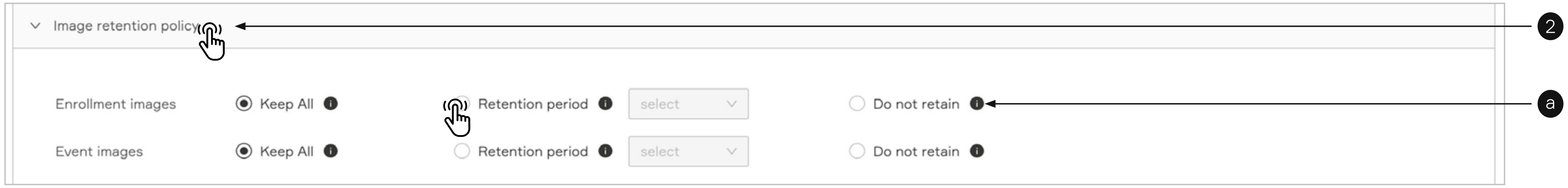
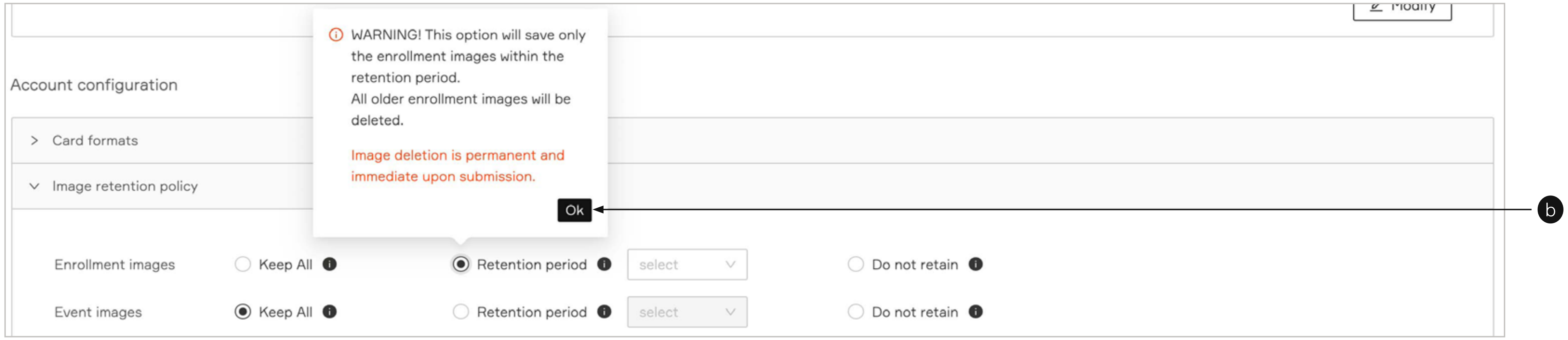


Image retention policy

Enrollment images ● Keep All ⓘ ○ Retention period ⓘ select ○ Do not retain ⓘ

Event images ● Keep All ⓘ ○ Retention period ⓘ select ○ Do not retain ⓘ



Account configuration

> Card formats

Image retention policy

ⓘ WARNING! This option will save only the enrollment images within the retention period.
All older enrollment images will be deleted.

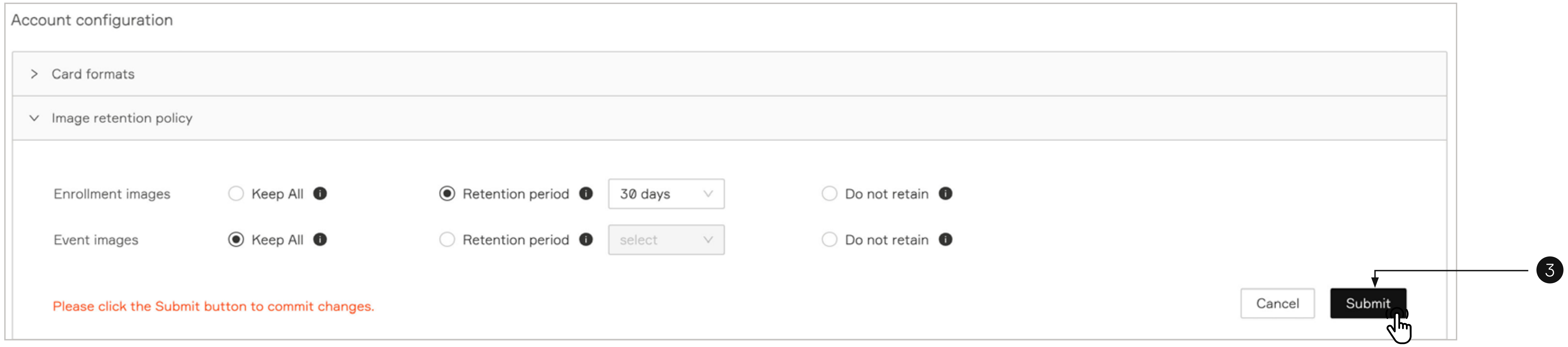
Image deletion is permanent and immediate upon submission.

Ok

Enrollment images ○ Keep All ⓘ ● Retention period ⓘ select ○ Do not retain ⓘ

Event images ● Keep All ⓘ ○ Retention period ⓘ select ○ Do not retain ⓘ

3. To save the retention settings click the **Submit**.
   A notification text below the options informs that the changes will be applied after submission.



Account configuration

> Card formats

Image retention policy

Enrollment images ○ Keep All ⓘ ● Retention period ⓘ 30 days ○ Do not retain ⓘ

Event images ● Keep All ⓘ ○ Retention period ⓘ select ○ Do not retain ⓘ

Please click the Submit button to commit changes.

alcatraz ai
Dashboard
Account
Account Settings
Audit Log
Permissions
Device Management
Security Events
Profiles

3.1.5—SSO configuration

Alcatraz AI Admin Portal supports SSO (Single Sign On) integration which makes user authentication a seamless experience and consistent with your chosen identity provider. The current supported identity providers are **Azure AD (Office Login), Okta** and **Ping Identity**.

For more information how to configure your identity provider system and the Alcatraz AI Admin Portal SSO option, read our SSO guide.

3.1.6—ACS Integration

Alcatraz AI Access Control System (ACS) Integration is a Windows application provided by Alcatraz AI that uses APIs licensed by ACS companies to synchronize user access management between the ACS and the Alcatraz AI Platform. Once installed, the application runs as a Windows Service.

Integration with the ACS is enabled for the account in the Alcatraz AI Admin Portal.
Alcatraz AI Admin Portal supports C•Cure and Genetec access control systems.

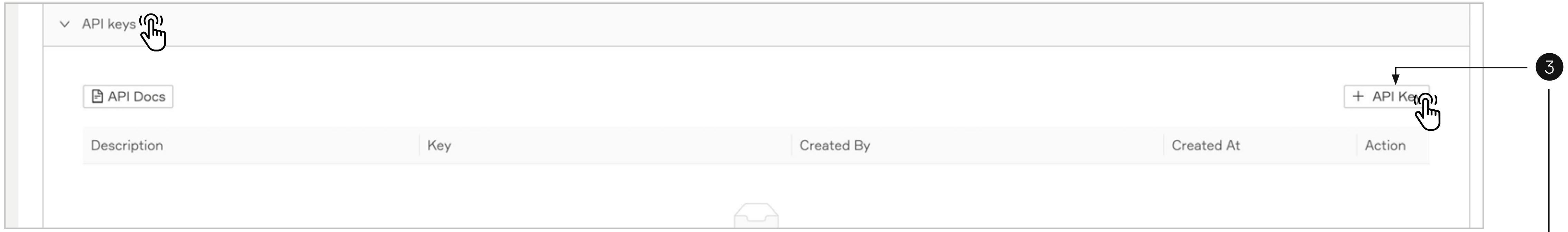
For more information about the installation and configuration of the ACS options read our C•Cure or Genetec guides.

3.1.7—API Keys

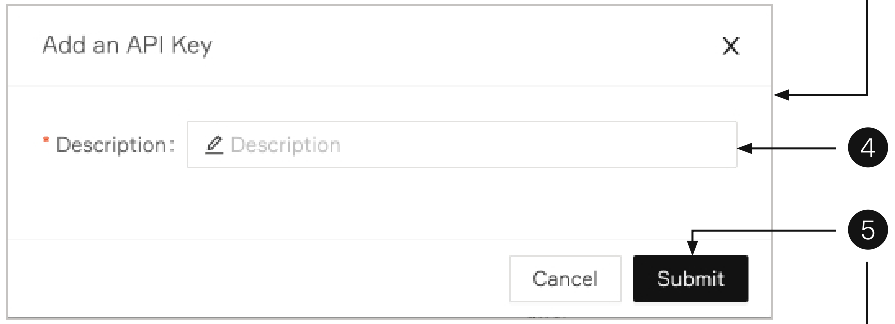
API Keys are generated in order to identify and authorize a third-party project/application to access the Alcatraz Admin Portal API.

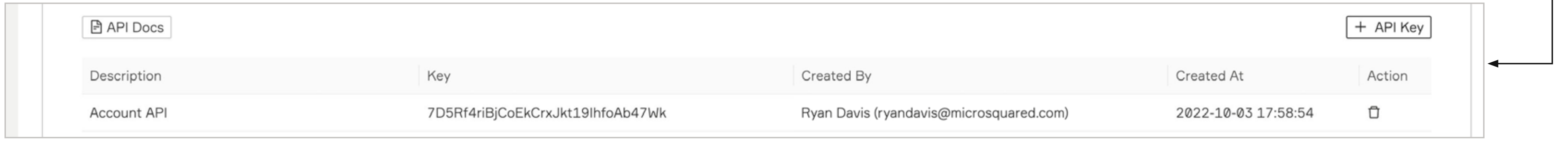
3.1.7.1—Creating an API Key

1. Go to **Account —> Account Settings**.
2. Scroll down to the **Account Configuration** and open the **API Keys** section.
3. Click the **+ API Key** button.



4. In the **Add an API Key** dialog - give a description/name of the project/application which will access the Alcatraz Admin Portal API.
5. Click **Submit**.
6. After the API key is generated it will be active immediately and can be provided to the project/application to start accessing the necessary data.



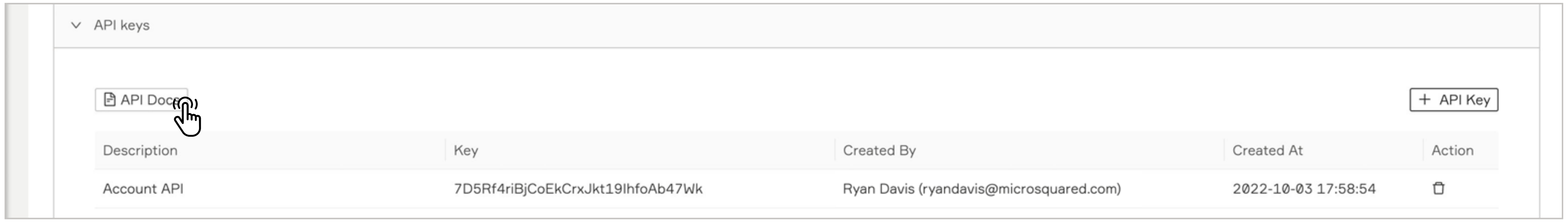


Description	Key	Created By	Created At	Action
Account API	7D5Rf4riBjCoEkCrxJkt19IhfoAb47Wk	Ryan Davis (ryandavis@microsquared.com)	2022-10-03 17:58:54	🗑

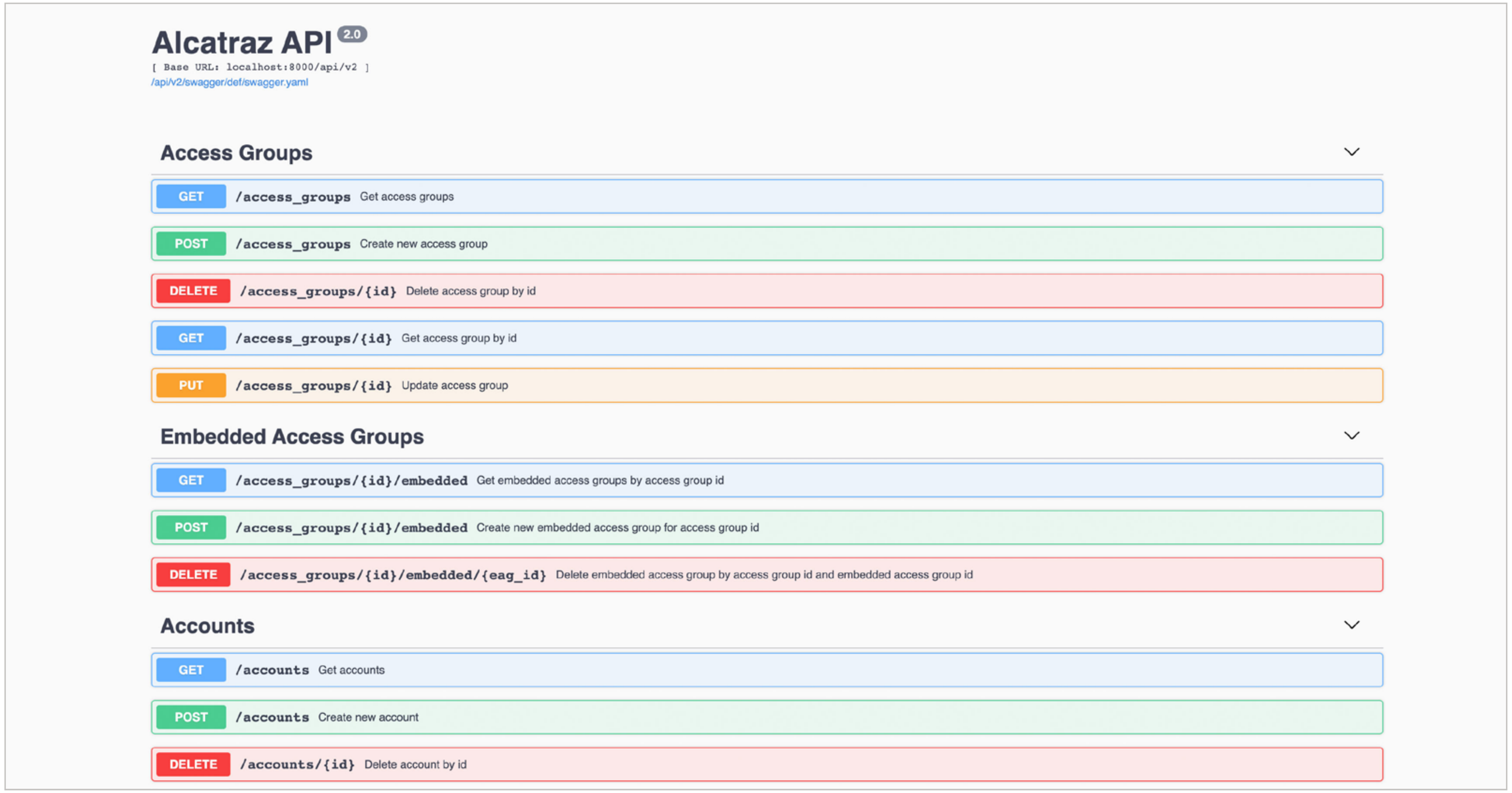
alcatraz ai
Dashboard
Accounts
Accounts List
Audit Log
Permissions
Device Management
Security Events
Profiles

3.1.7.2—API Key Documentation

Request URL for Alcatraz AI API is https://platform.alcatraz.ai/api/v2/
To authenticate the API, use the authentication header: x-alcatraz-api-key and the API Key value (displayed in the Key column of the API Keys table).
Click the API Docs button for more information about all of the Alcatraz AI API endpoints and each endpoint parameters.



Description	Key	Created By	Created At	Action
Account API	7D5Rf4riBjCoEkCrxJkt19IhfoAb47Wk	Ryan Davis (ryandavis@microsquared.com)	2022-10-03 17:58:54	🗑



Alcatraz API 2.0
[Base URL: localhost:8000/api/v2]
/api/v2/swagger/def/swagger.yaml

Access Groups

GET /access_groups Get access groups
POST /access_groups Create new access group
DELETE /access_groups/{id} Delete access group by id
GET /access_groups/{id} Get access group by id
PUT /access_groups/{id} Update access group

Embedded Access Groups

GET /access_groups/{id}/embedded Get embedded access groups by access group id
POST /access_groups/{id}/embedded Create new embedded access group for access group id
DELETE /access_groups/{id}/embedded/{eag_id} Delete embedded access group by access group id and embedded access group id

Accounts

GET /accounts Get accounts
POST /accounts Create new account
DELETE /accounts/{id} Delete account by id

alcatraz ai
Dashboard
Account
Account Settings
Audit Log
Permissions
Device Management
Security Events
Profiles

3.2—Audit Log

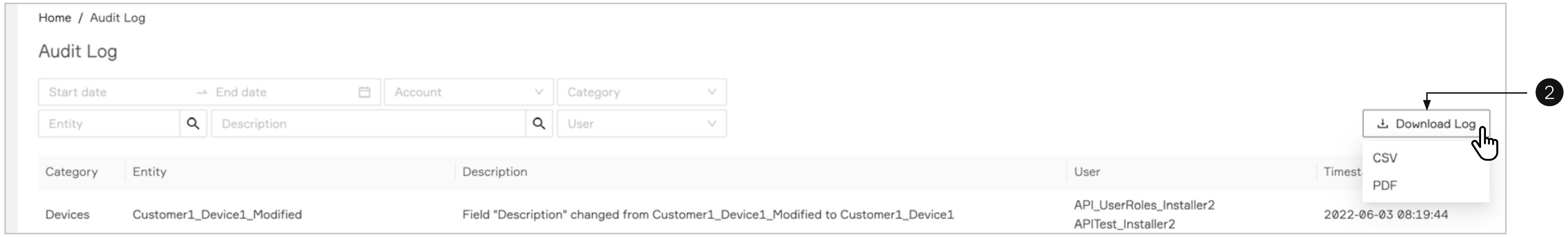
Audit logs in the Alcatraz AI Admin Portal provides means of displaying records of all events that have taken place in the system. The events recorded relate to one of the following categories – **Account**, **User**, **Device**, **Access Group**, **Security Event**, **Profile**, **Firmware Update**, **System Manager**.
The event description is typically in the format "[entity] – [field] changed from [old value] to [new value]" or other as appropriate.

When viewing Audit logs, filters can be applied to show more specific results in a date range, category, entity etc.

3.2.1—Export Audit Log

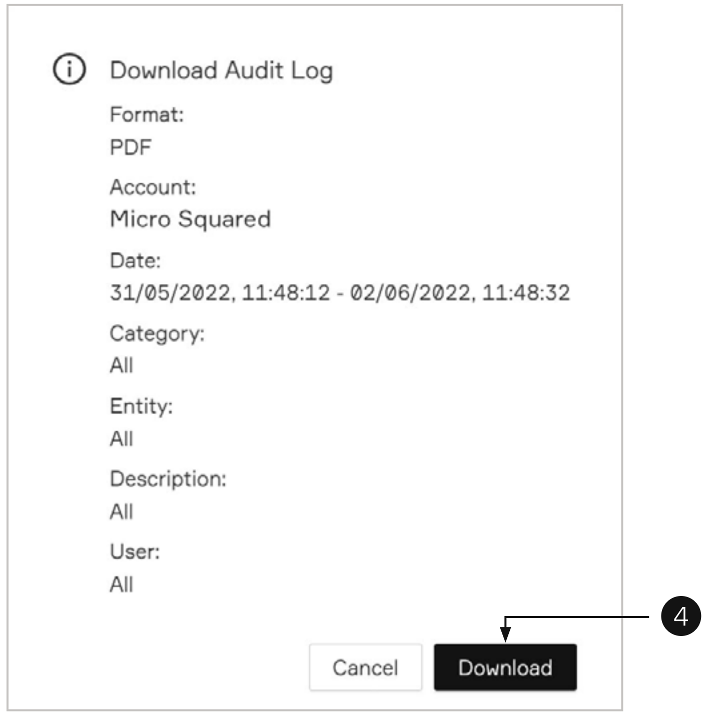
Users can export and download these records via the **Download Log** button in CSV or PDF format. Use the filters to export required data.

1. Go to **Account** –> **Audit Log**.
■ Apply filters as needed.
2. Hover on **Download Log** button and select the preferred file format.
3. A pop-up with the filtered information will appear.



Category	Entity	Description	User	Timest
Devices	Customer1_Device1_Modified	Field "Description" changed from Customer1_Device1_Modified to Customer1_Device1	API_UserRoles_Installer2 APITest_Installer2	2022-06-03 08:19:44

4. Click **Download** button to continue.



Download Audit Log

Format:
PDF

Account:
Micro Squared

Date:
31/05/2022, 11:48:12 - 02/06/2022, 11:48:32

Category:
All

Entity:
All

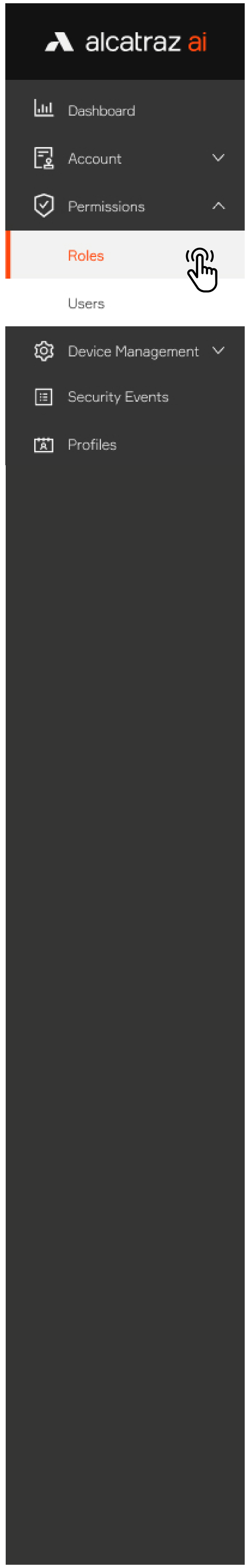
Description:
All

User:
All

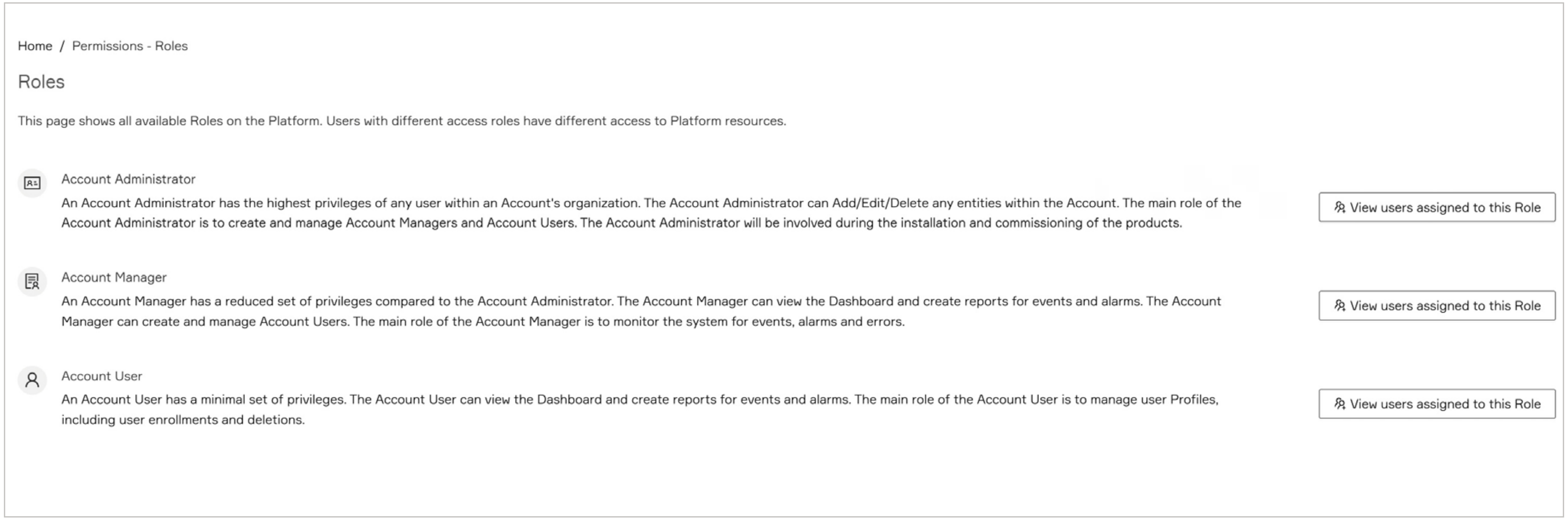
5. A zip file of the selected logs will be downloaded. (The file will contain up to 500 records.)

4 —
Permissions

The Permissions section of the Alcatraz AI Admin Portal provides capability to create new system users to log into the Alcatraz AI Admin Portal.
When a new system user is created, they must be assigned a role. This role will be associated with permissions to create, edit, view, or delete in the portal.



4.1—Overview of User Roles



Home / Permissions - Roles

Roles

This page shows all available Roles on the Platform. Users with different access roles have different access to Platform resources.

Account Administrator

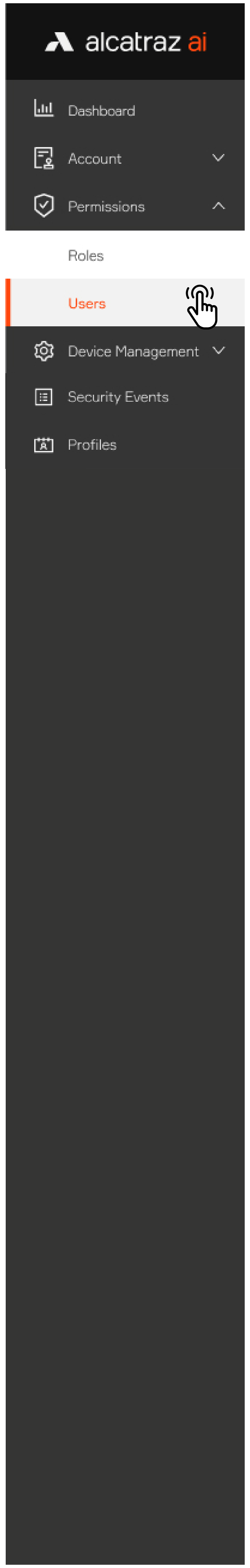
An Account Administrator has the highest privileges of any user within an Account's organization. The Account Administrator can Add/Edit/Delete any entities within the Account. The main role of the Account Administrator is to create and manage Account Managers and Account Users. The Account Administrator will be involved during the installation and commissioning of the products.

Account Manager

An Account Manager has a reduced set of privileges compared to the Account Administrator. The Account Manager can view the Dashboard and create reports for events and alarms. The Account Manager can create and manage Account Users. The main role of the Account Manager is to monitor the system for events, alarms and errors.

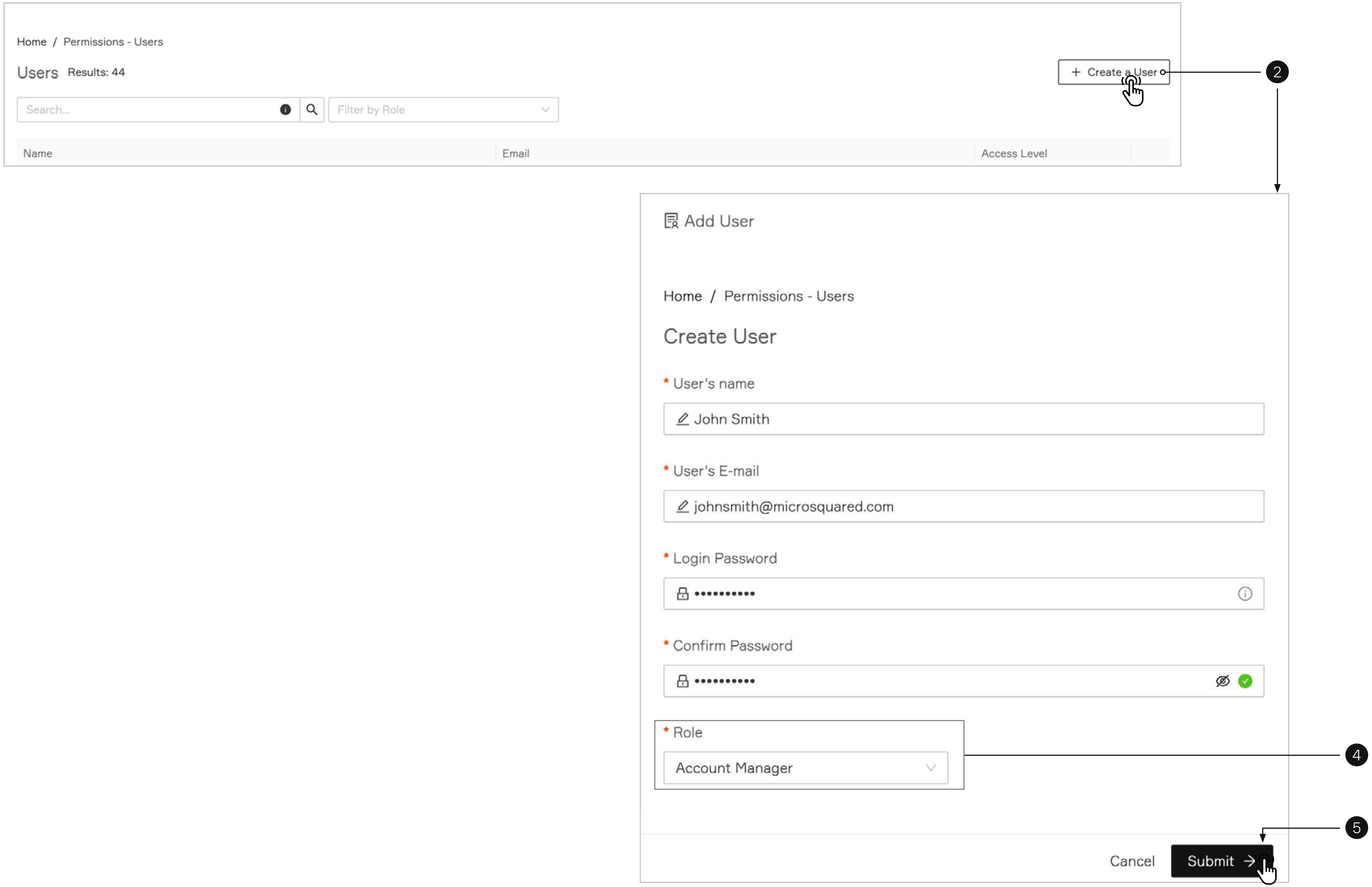
Account User

An Account User has a minimal set of privileges. The Account User can view the Dashboard and create reports for events and alarms. The main role of the Account User is to manage user Profiles, including user enrollments and deletions.



4.2—Create a User

1. Go to **Permissions** –> **Users** and filter on the User to ensure that an account has not already been set up.
2. To add a new user, select **Create a User**.
3. Fill in the required information.
4. Select the appropriate **Role**.
5. Click **Submit**.



Home / Permissions - Users

Create User

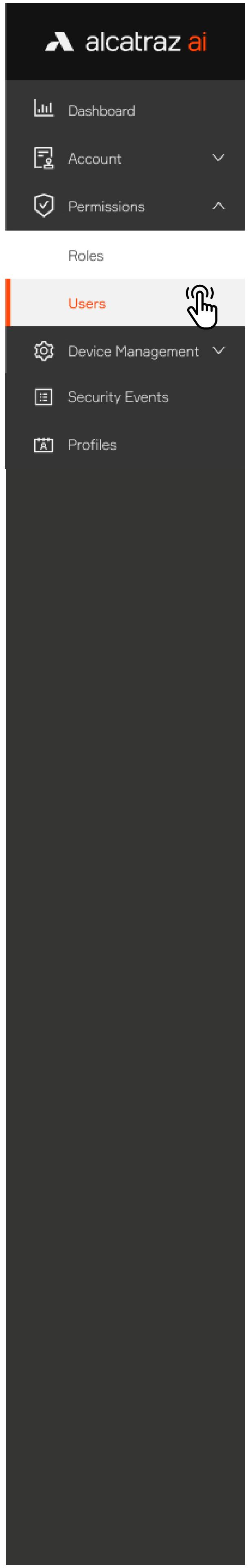
* User's name: John Smith

* User's E-mail: johnsmith@microsquared.com

* Login Password: ••••••••••

* Confirm Password: ••••••••••

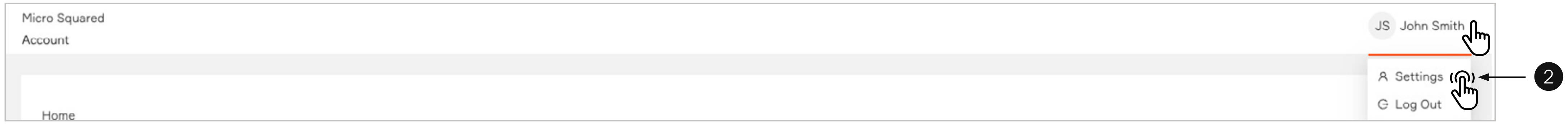
* Role: Account Manager

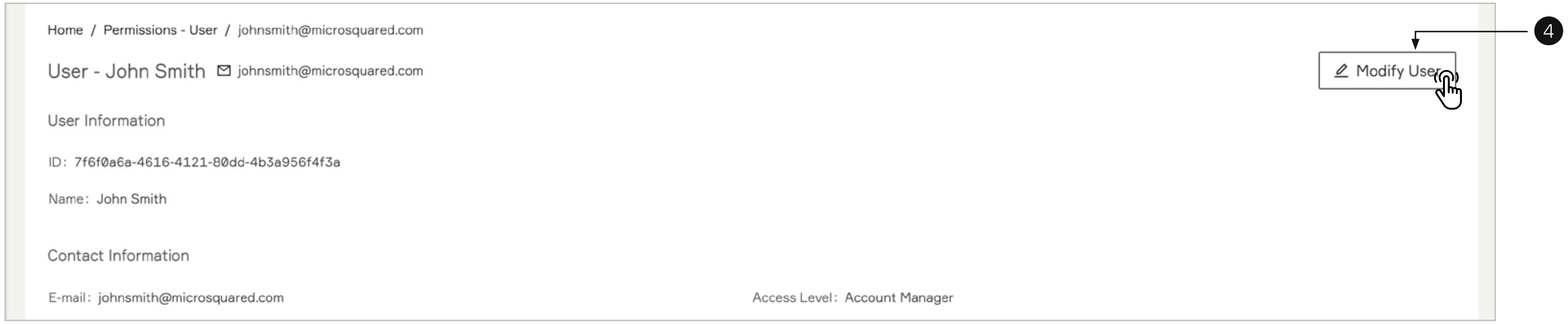


4.3—Edit User

4.3.1— Edit current logged user

1. Navigate to right side of the header & hover on user's name.
2. Click **Settings**.
3. User's details will be displayed.
4. Click **Modify User**.





Home / Permissions - User / johnsmith@microsquared.com

User - John Smith johnsmith@microsquared.com

User Information

ID: 7f6f0a6a-4616-4121-80dd-4b3a956f4f3a

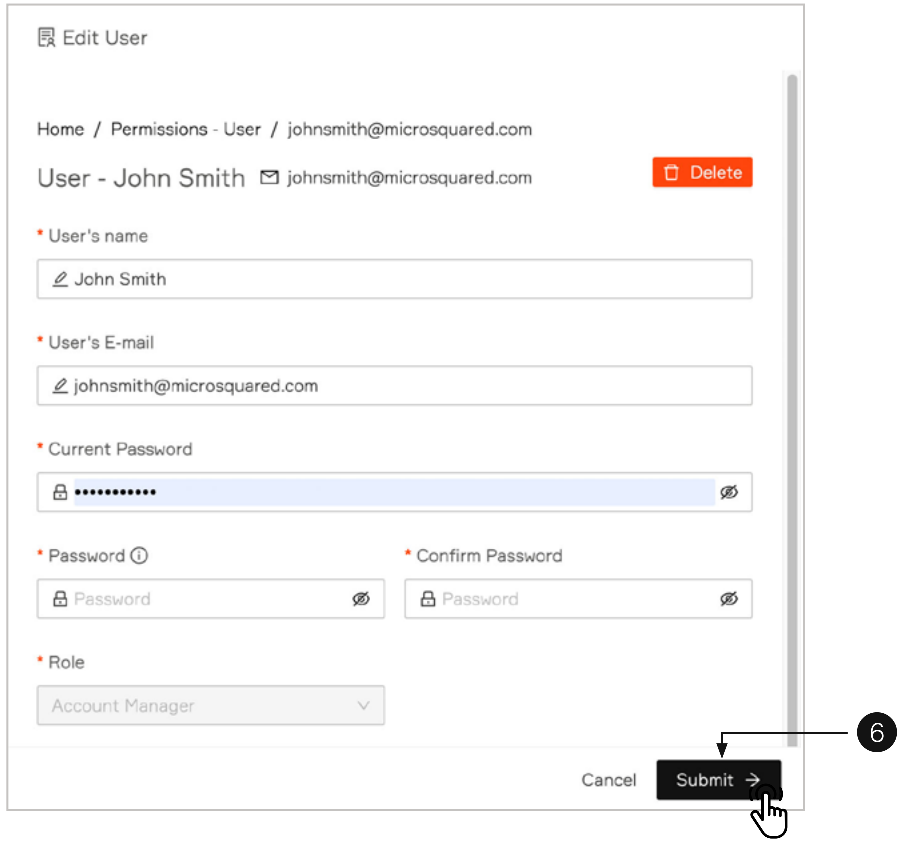
Name: John Smith

Contact Information

E-mail: johnsmith@microsquared.com

Access Level: Account Manager

5. Modify user details.
6. Click **Submit**.



Home / Permissions - User / johnsmith@microsquared.com

User - John Smith johnsmith@microsquared.com

* User's name: John Smith

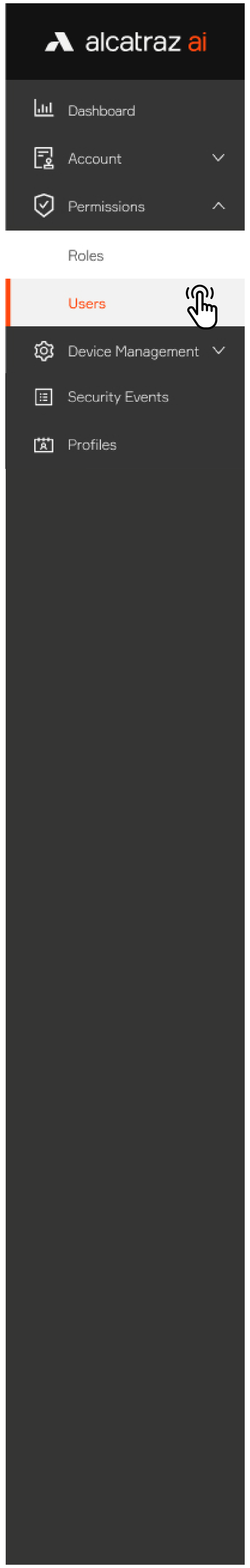
* User's E-mail: johnsmith@microsquared.com

* Current Password: •••••••••••

* Password: Password

* Confirm Password: Password

* Role: Account Manager

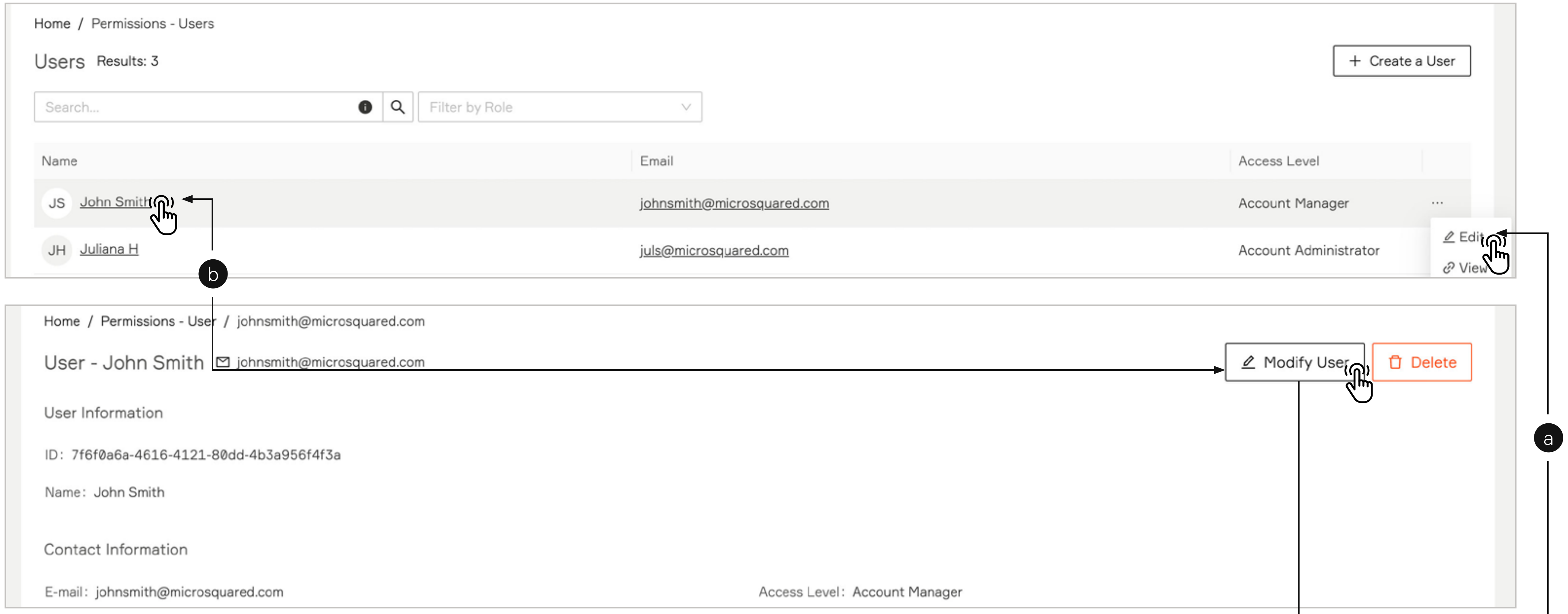


4.3.2— Edit user

1. Go to **Permissions** —> **Users**.
2. The system provides two ways to edit the credentials of preferred user:

a. Navigate to the far right on the row which contains the user that need to be edited. Click on the three dots (context menu) and select **Edit**. **Edit User** panel will be displayed.

b. Clicking on user's name in the table will open a user's details page. Click **Modify User** to open **Edit User** panel.



Name	Email	Access Level
JS John Smith	johnsmith@microsquared.com	Account Manager
JH Juliana H	juls@microsquared.com	Account Administrator

User - John Smith johnsmith@microsquared.com

User Information

ID: 7f6f0a6a-4616-4121-80dd-4b3a956f4f3a

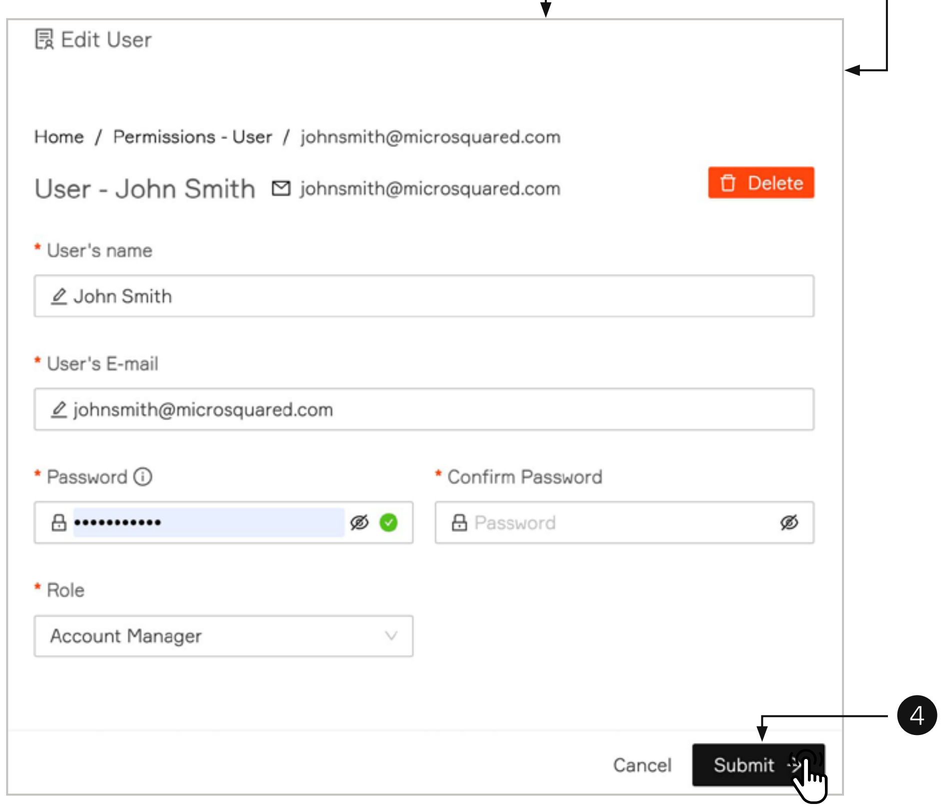
Name: John Smith

Contact Information

E-mail: johnsmith@microsquared.com

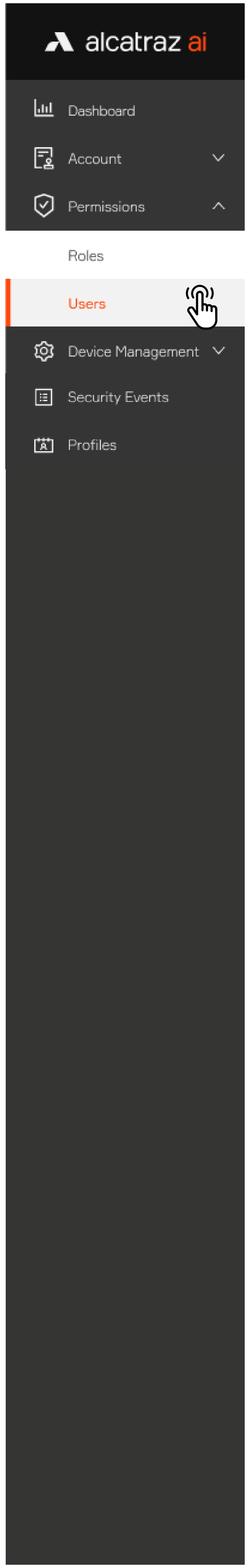
Access Level: Account Manager

3. Modify user details.
4. Click **Submit**.



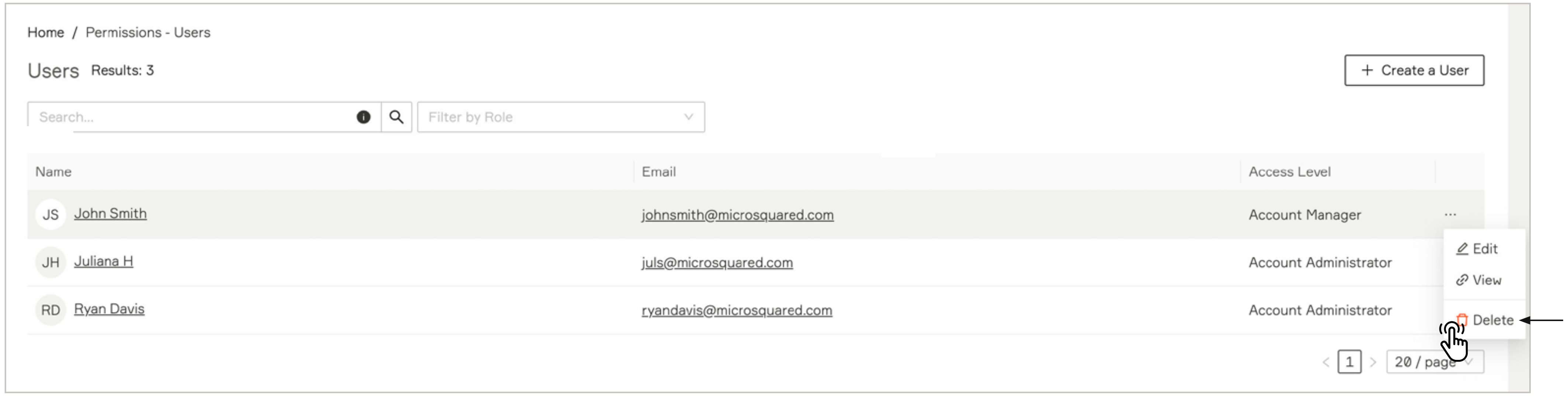
User - John Smith johnsmith@microsquared.com

* User's name: John Smith
* User's E-mail: johnsmith@microsquared.com
* Password: •••••••••••
* Confirm Password: Password
* Role: Account Manager

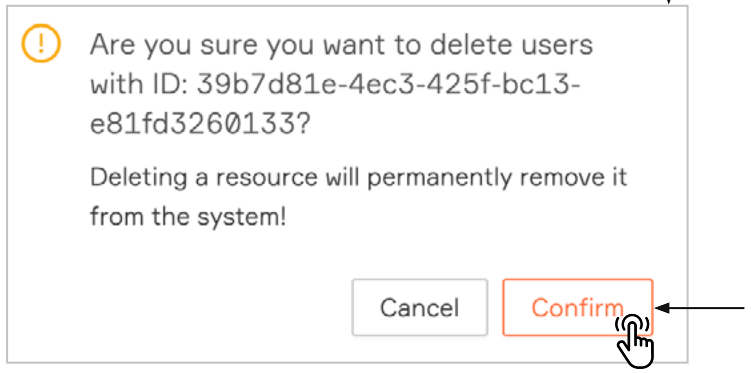


4.4—Delete a User

1. Go to **Permissions** —> **Users** and identify the user you wish to delete.
2. Navigate to the far right, click on the three dots and select **Delete**.
3. You will be asked to confirm before deleting.



Name	Email	Access Level
JS John Smith	johnsmith@microsquared.com	Account Manager
JH Juliana H	juls@microsquared.com	Account Administrator
RD Ryan Davis	ryandavis@microsquared.com	Account Administrator



Are you sure you want to delete users with ID: 39b7d81e-4ec3-425f-bc13-e81fd3260133?

Deleting a resource will permanently remove it from the system!

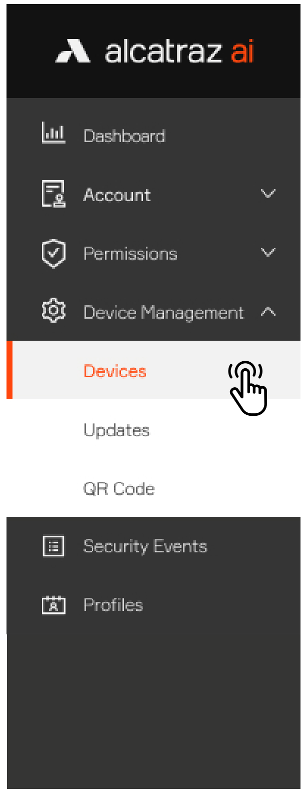
5 —
Onboard a Rock

Newly installed Rocks will need to be onboarded and assigned to the Default Access Group. Onboarding a Rock associates the Rock with the server where the Alcatraz AI Admin Portal is hosted.

For Cloud-Hosted Rocks, the server is maintained by Alcatraz AI.
For On-prem Rocks, the server is maintained on customer site.

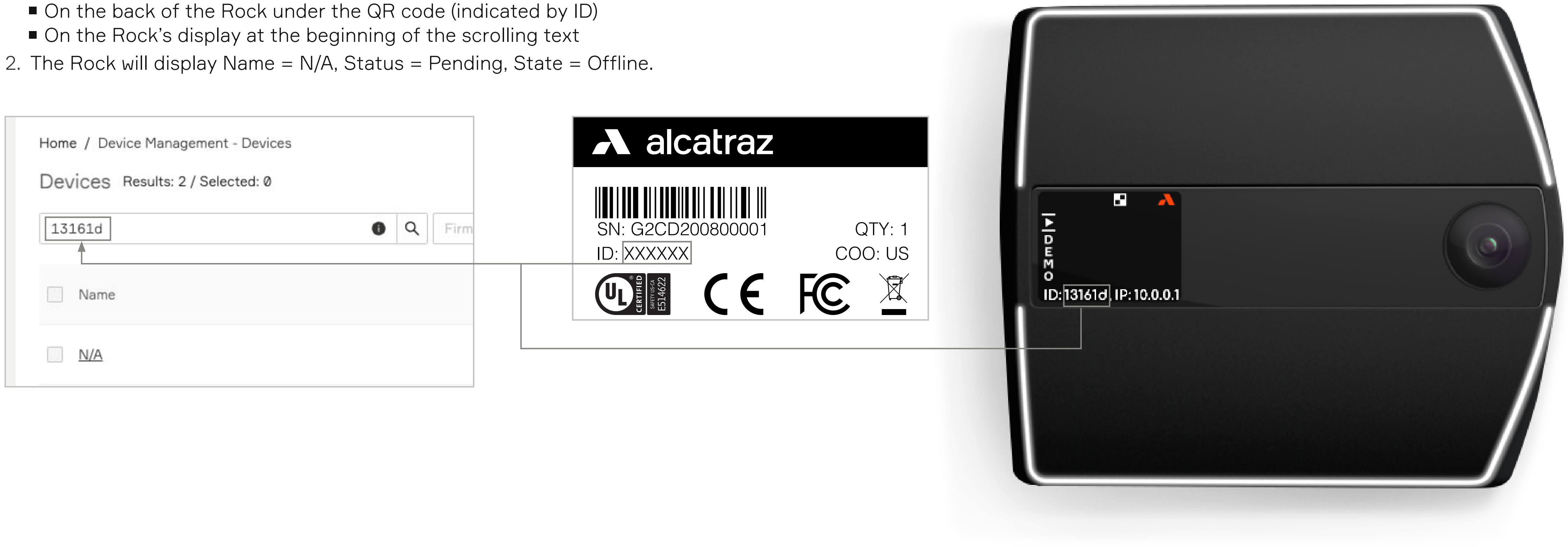
Before onboarding a Rock:
— Obtain login credentials to the Alcatraz AI Admin Portal. Make a request to your administrator.
— Make a list of the Device ID for each Rock to be onboarded. DeviceID can be found on the back of the Rock under the QR code, on the outside of the box the Rock was shipped in or scrolling at the bottom of the Rock's display. (when powered on)

If the newly installed Rock does not show up in the Alcatraz AI Admin Portal for onboarding, it is possible that it cannot connect to the Server. Check the network information scrolling on the Rock's display to help troubleshoot.



5.1—Find the Rock to Onboard by Search

1. Enter the 6 digit Device ID in the search bar to filter the Rock. The 6 digit Device ID can be found:
   - On the outside of the package the Rock was shipped in (indicated by ID, as seen on label here)
   - On the back of the Rock under the QR code (indicated by ID)
   - On the Rock's display at the beginning of the scrolling text
2. The Rock will display Name = N/A, Status = Pending, State = Offline.



Home / Device Management - Devices

Devices Results: 2 / Selected: 0

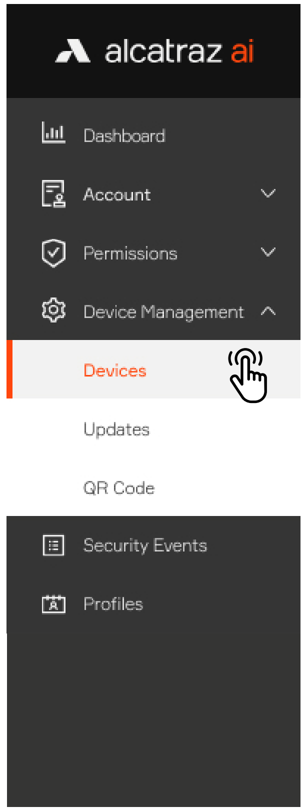
13161d

□	Name
□	N/A

alcatraz

SN: G2CD200800001 QTY: 1

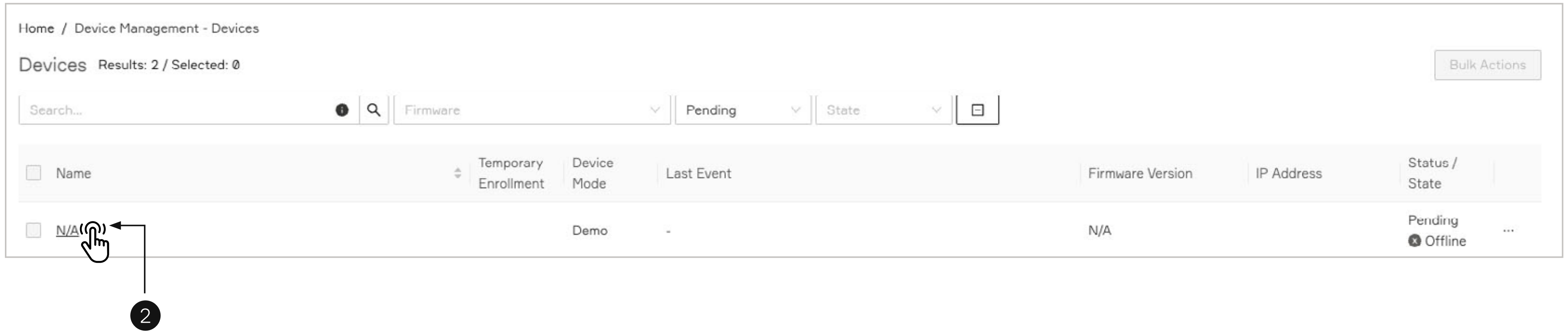
ID: XXXXXX COO: US



5.2—Authenticate the Device

Authenticating the device will establish the connection with the Rock.

1. Go to **Device Management** and select **Devices**.
2. Click on Name **N/A** to open the Rock's info page.

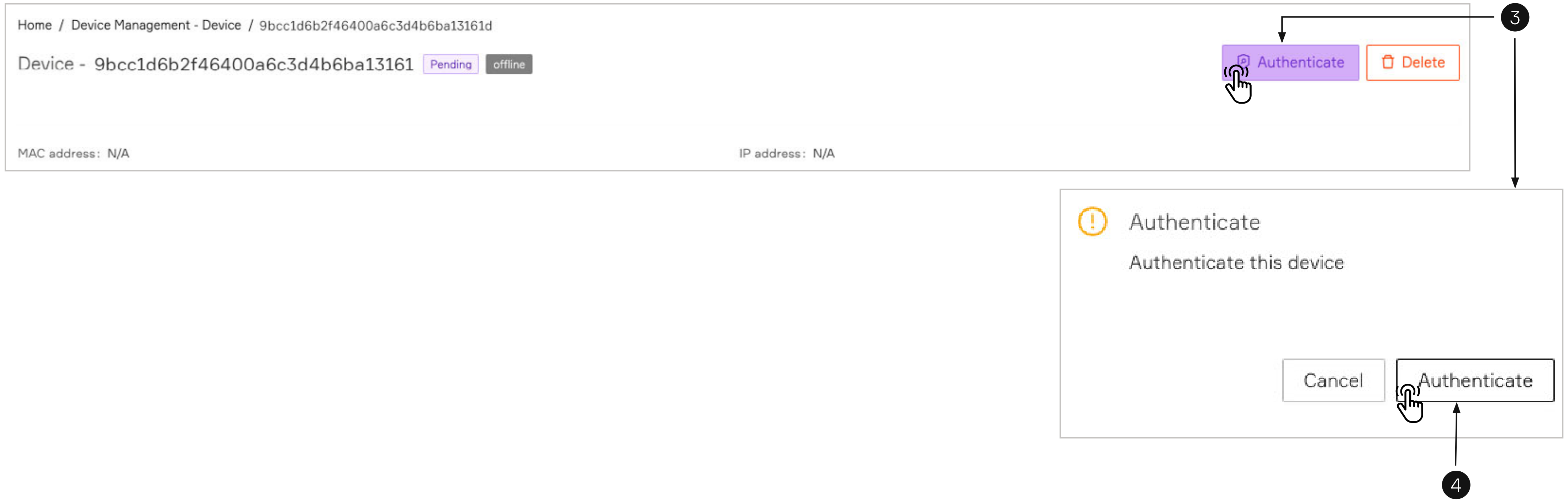


Home / Device Management - Devices

Devices Results: 2 / Selected: 0

□	Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State	
□	N/A		Demo	-	N/A		Pending Offline	...

3. Click on **Authenticate**.
4. A window pops open, click the **Authenticate** button.



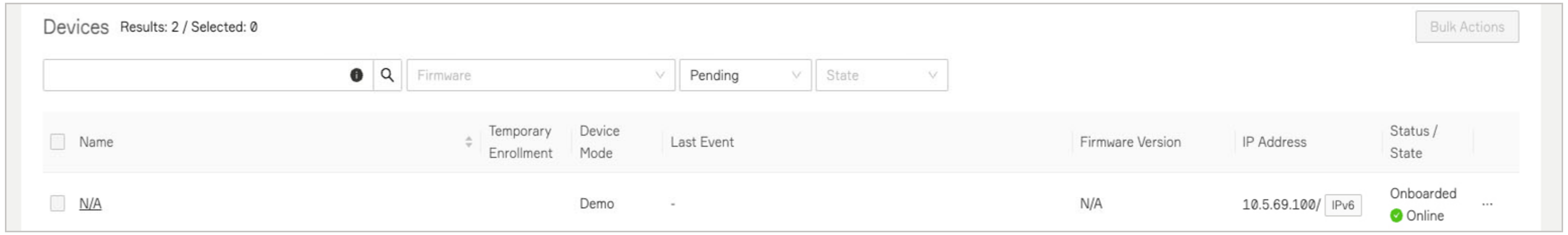
Home / Device Management - Device / 9bcc1d6b2f46400a6c3d4b6ba13161d

Device - 9bcc1d6b2f46400a6c3d4b6ba13161 Pending offline

MAC address: N/A

IP address: N/A

The Rock has been successfully onboarded when the Status = Onboarded and State = Online. Refresh the browser to see the update.

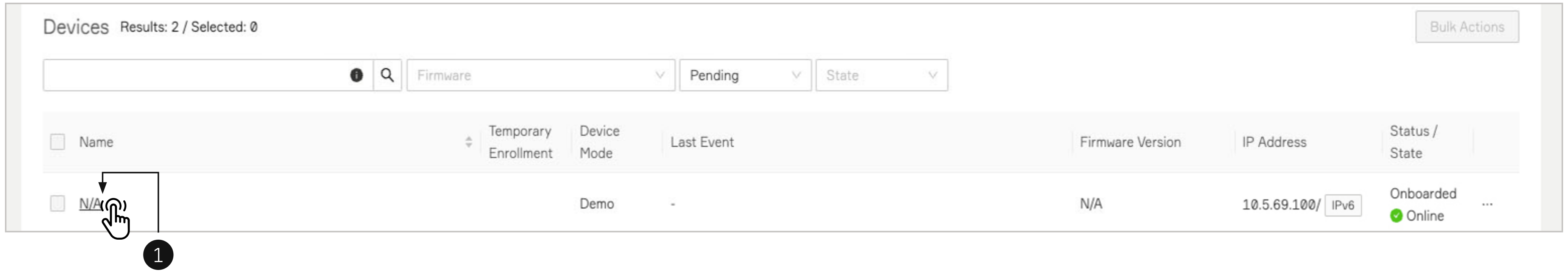


Devices Results: 2 / Selected: 0

	Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State
□	N/A		Demo	-	N/A	10.5.69.100/ IPv6	Onboarded ● Online

5.3—Name the Device

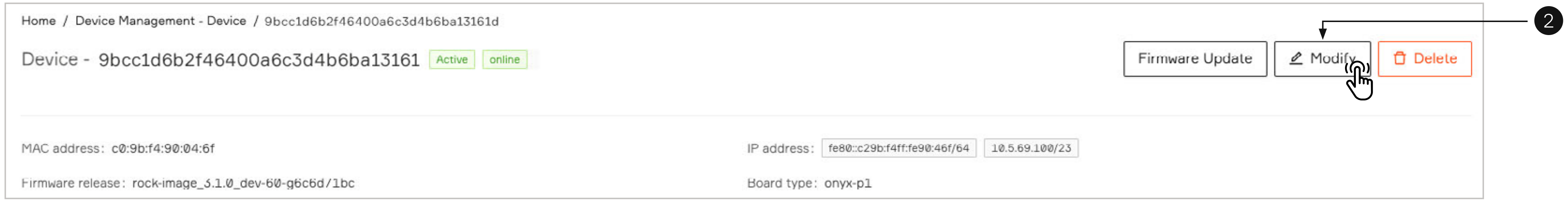
1. Click on the Name (**N/A** in this instance).



Devices Results: 2 / Selected: 0

	Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State
□	N/A		Demo	-	N/A	10.5.69.100/ IPv6	Onboarded ● Online

2. The Rock's information will be displayed. Click on **Modify**.
3. Modify the **Name** field.
4. Click **Submit** at the bottom of the page.



Home / Device Management - Device / 9bcc1d6b2f46400a6c3d4b6ba13161d

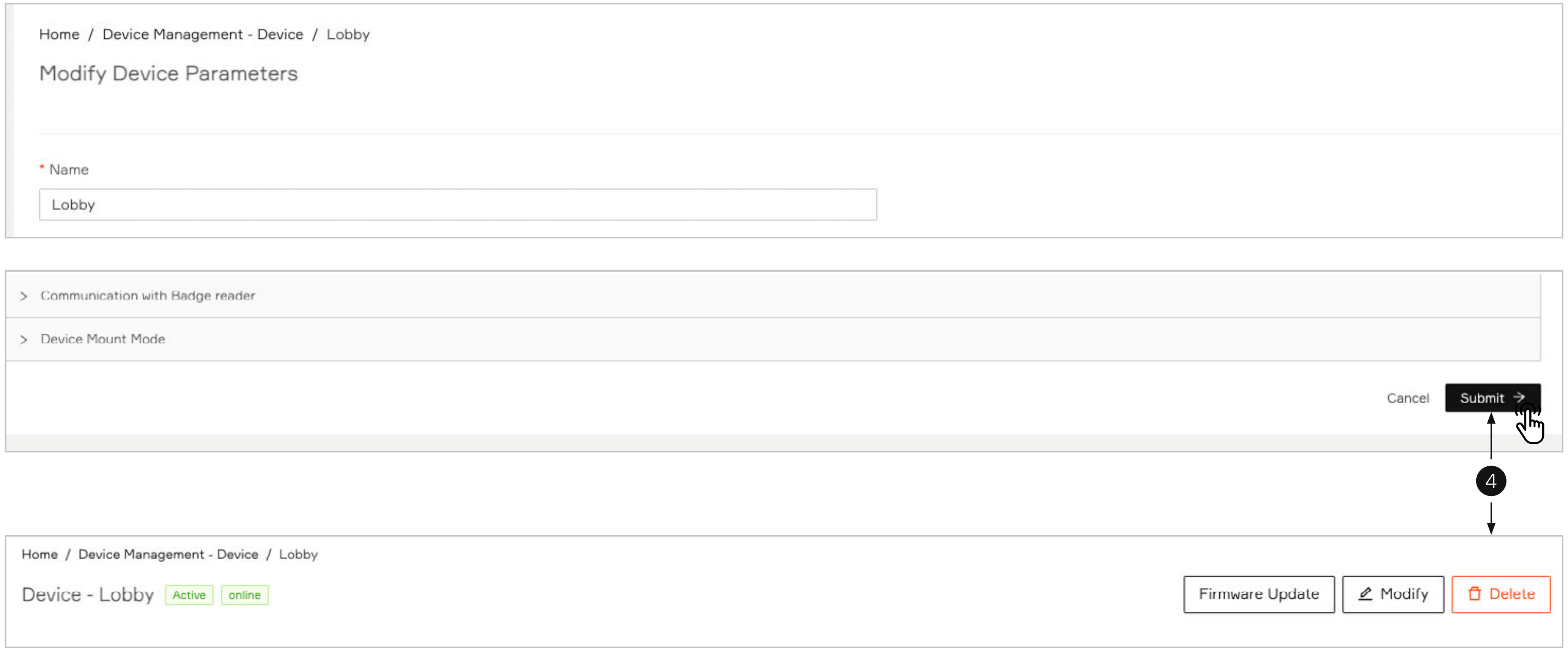
Device - 9bcc1d6b2f46400a6c3d4b6ba13161

MAC address: c0:9b:f4:90:04:6f

IP address: fe80::c29b:f4ff:fe90:46f/64 10.5.69.100/23

Firmware release: rock-image_3.1.0_dev-60-g6c6d/1bc

Board type: onyx-p1



Home / Device Management - Device / Lobby

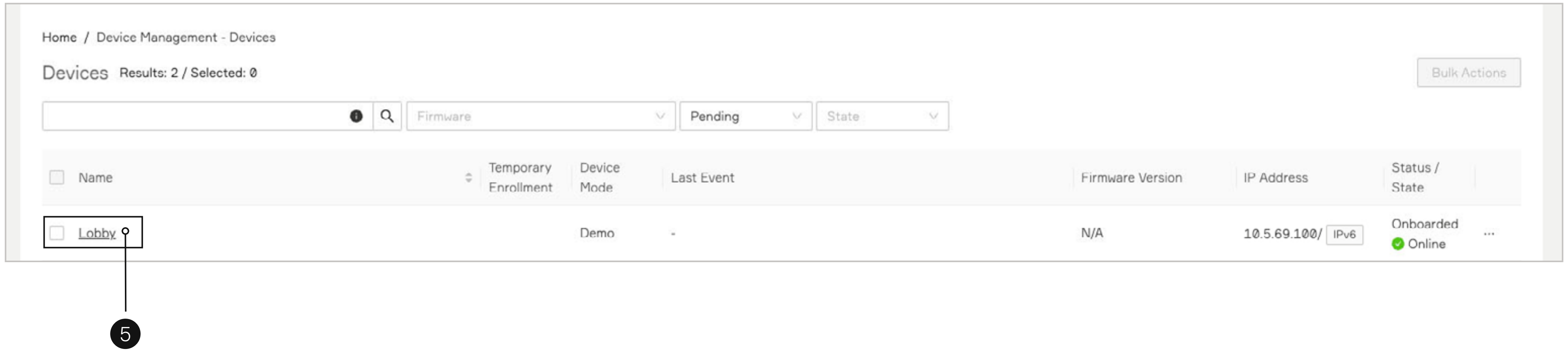
Modify Device Parameters

* Name: Lobby

Home / Device Management - Device / Lobby

Device - Lobby

5. View the new **Name** in the list.



Home / Device Management - Devices

Devices Results: 2 / Selected: 0

Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State
Lobby		Demo	-	N/A	10.5.69.100/ IPv6	Onboarded Online

6 —
Device Management

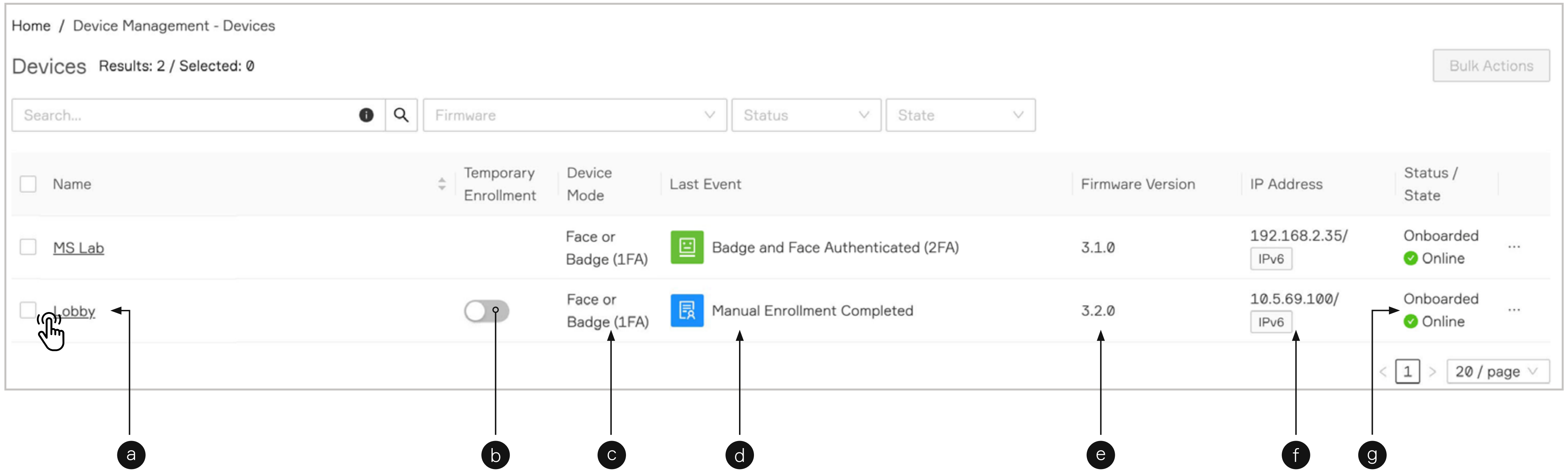
6.1—Devices

6.1.1—Devices page overview

Go to **Device Management** and select **Devices**. A table containing all devices in your account will be displayed.
The table provides more detailed information for each Rock device about:

a. Device Name
b. Temporary Enrollment Availability (and status – on/off)
c. Device Operation Mode
d. Last Recorded Event
e. Rock Firmware Version
f. IP Address
g. Authentication System Status / Network State

The filters above the table allow filtering of the devices by **Firmware**, **Status**, and **State**.
The pagination below the table allows selecting the number of visible devices per page.



Home / Device Management - Devices

Devices Results: 2 / Selected: 0

□	Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State	
□	MS Lab		Face or Badge (1FA)	Badge and Face Authenticated (2FA)	3.1.0	192.168.2.35/ IPv6	Onboarded ✓ Online	···
□	Lobby	○	Face or Badge (1FA)	Manual Enrollment Completed	3.2.0	10.5.69.100/ IPv6	Onboarded ✓ Online	···

Clicking on the name of a selected device opens a device's details page.
Selecting the name of a device will open up the device's information page.

alcatraz ai
Dashboard
Account
Permissions
Device Management
Devices
Updates
QR Code
Security Events
Profiles

6.1.2—Device details page

The device's information page displays comprehensive and accurate information about the device:

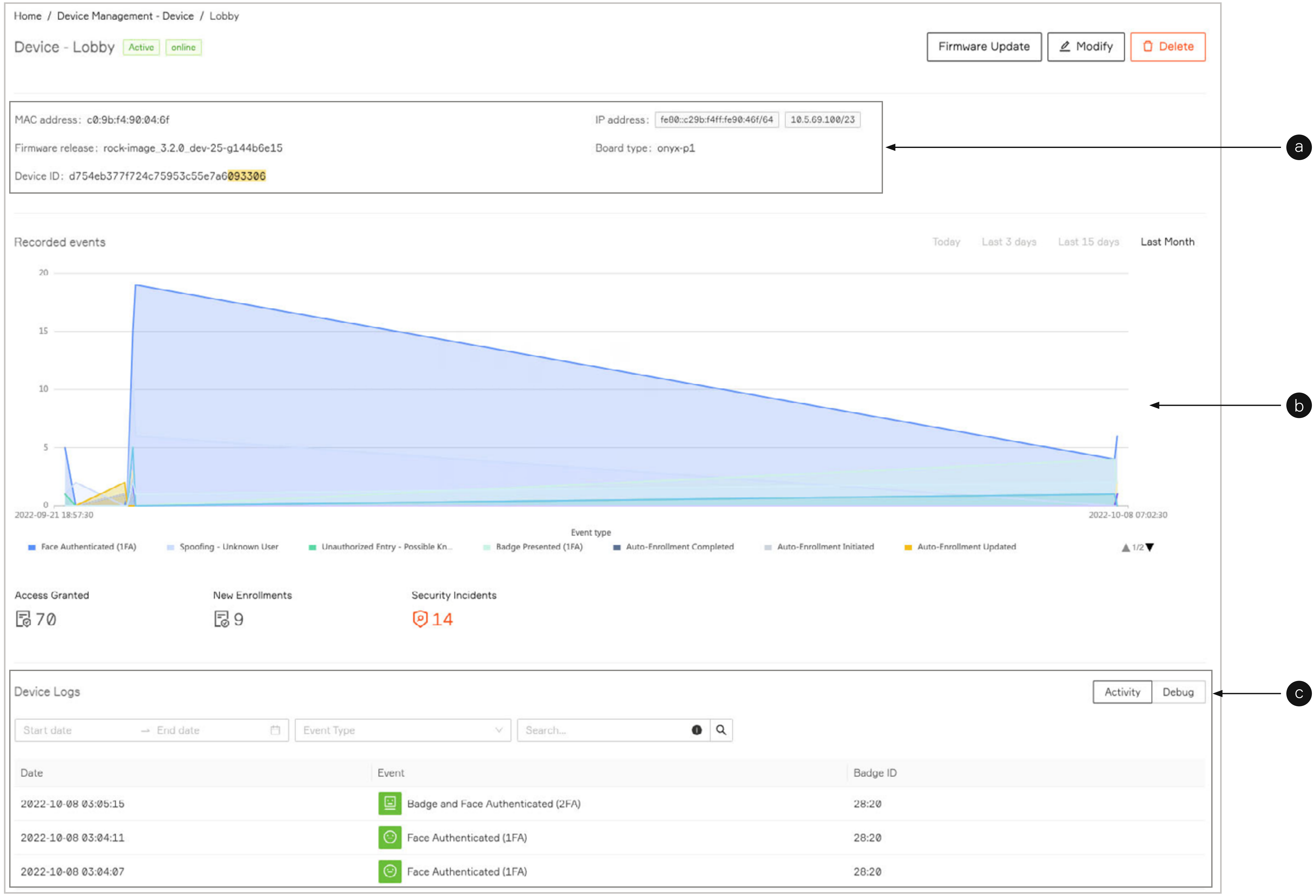
a. Device details about:

- **MAC** and **IP address**
- **Firmware Release** and **Board Type**
- **Device ID number**
- **Default Access Group** and **Access Group** information (optional or specific to integration)

b. Chart presenting the recorded events (with 4 different filter – Today / Last 3 days / Last 15 days / Last Month).

c. **Device Logs** section with:

- **Activity Log** (presenting a table with the device recorded events)
- **Debug Log** (used only for support purposes)



MAC address: c0:9b:f4:90:04:6f

IP address: fe80::c29b:f4ff:fe90:46f/64 10.5.69.100/23

Firmware release: rock-image_3.2.0_dev-25-g144b6e15

Board type: onyx-p1

Device ID: d754eb377f724c75953c55e7a6093306

Access Granted 70

New Enrollments 9

Security Incidents 14

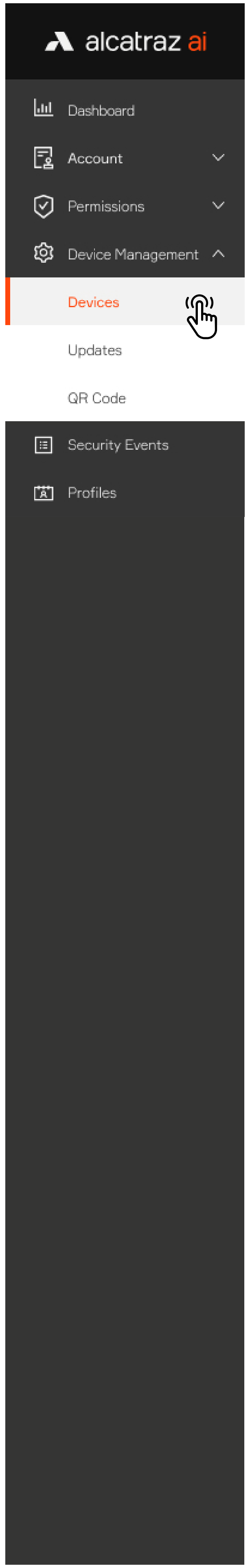
Date	Event	Badge ID
2022-10-08 03:05:15	Badge and Face Authenticated (2FA)	28:20
2022-10-08 03:04:11	Face Authenticated (1FA)	28:20
2022-10-08 03:04:07	Face Authenticated (1FA)	28:20

6.2—Device Configuration

6.2.1—Operating Modes

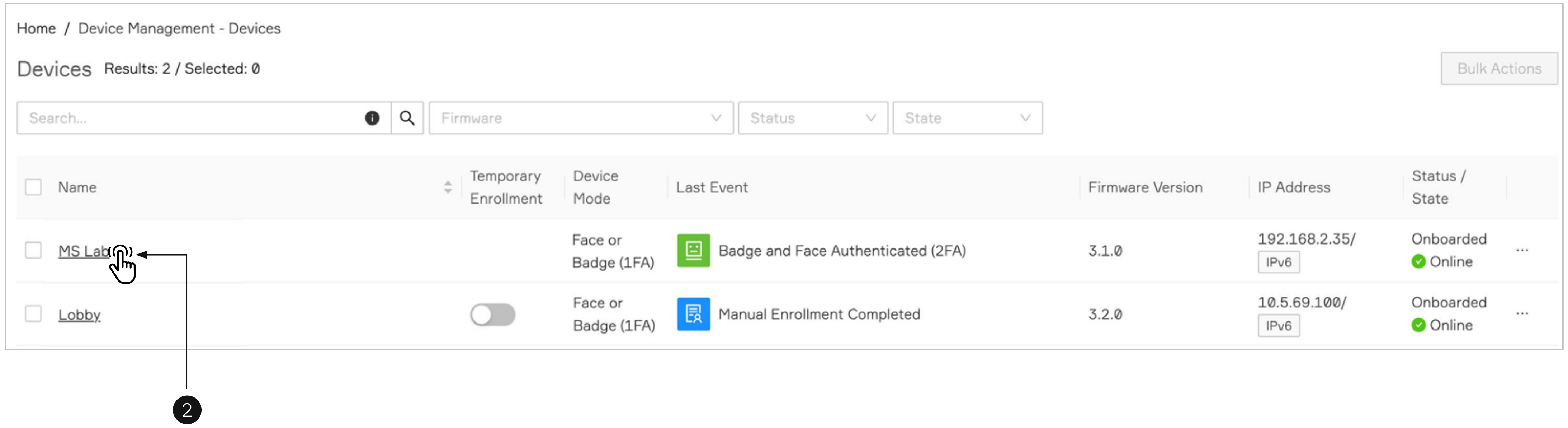
The Rock can operate in a number of modes.

Device Mode	Description
Demo Mode	■ Demo is used for demonstrations. ■ Similar to 1FA - requires face or badge as credential. ■ Auto-enrollment is enabled and requires only 2 consecutive badge swipes (instead of 4-6 badge-ins) with no wait in between to be enrolled. ■ Enrollment profiles are not retained and will be deleted when the Rock reboots.
Face or Badge (1FA)	■ Single Factor Authentication requires either face or badge as the credential. ■ The Rock will authenticate users that are enrolled. Users not yet enrolled will require their badge. ■ 1FA allows to turn on the Auto-enrollment. (The feature is disabled by default.) The option allows people to enroll by swiping their badge 4-6 times over the course of a few days. Once enrolled, the user will find that they will be authenticated when they walk up to the Rock and hear the door click open.
Face-Only (1FAF)	■ Single Factor Face Only requires face as the credential. ■ This mode is used at doors that do not have a badge reader. ■ Enrollment is completed at an enrollment station, often located at the Security Operations Office.
Face and Badge 2FA /	■ Two Factor Authentication requires face and badge as the credentials. ■ Enrollment is completed at an enrollment station, often located at the Security Operations Office.
(3FA)	■ The mode supports 3FA when **Support 3FA** is toggled on. The functionality for third authentication factor should be enabled when requiring users to enter a PIN or other additional authentication factor. The Rock will authenticate the face but the user must swipe a badge and then enter a PIN. The ACS must be configured to accept Badge + PIN. Reach out to Alcatraz AI for questions on authentication factors.
Mask Enforcement (2FA-M)	■ Mask Enforcement requires a mask and badge. ■ The Rock will enforce the user to wear a mask before allowing a user to badge in.
Enrollment	■ Referred to as manual enrollment. ■ Allows companies to dedicate a Rock as an enrollment station to enroll users quickly,. ■ Ideal to have a dedicated Rock for enrollment in companies that have Rocks operating in 2FA, 1FAF, or regularly enrolling employees.

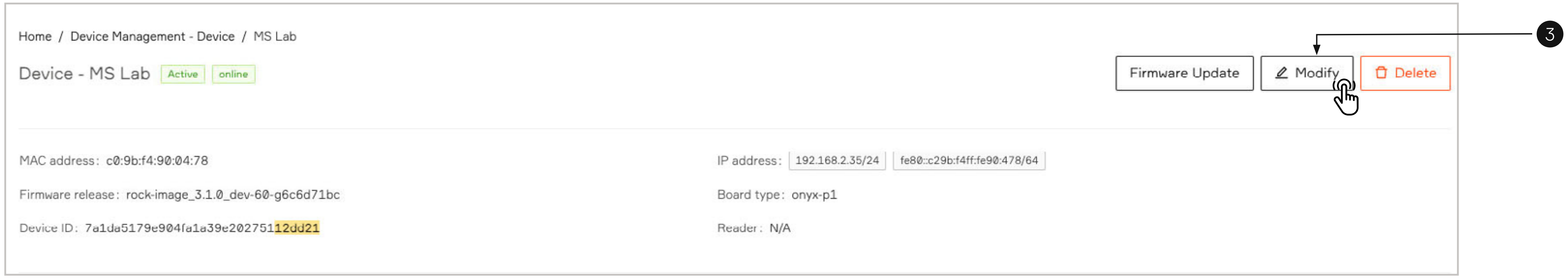


6.2.2—Configure Rock Mode of Operation

1. Go to **Device Management** and select **Devices**.
2. Click on the Name of the Rock to open the Rock's info page.
3. Click on **Modify** to open up the configurations page.


Home / Device Management - Devices
Devices Results: 2 / Selected: 0
Bulk Actions
Search...
Firmware
Status
State
2

Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State
MS Lab		Face or Badge (1FA)	Badge and Face Authenticated (2FA)	3.1.0	192.168.2.35/ IPv6	Onboarded Online
Lobby		Face or Badge (1FA)	Manual Enrollment Completed	3.2.0	10.5.69.100/ IPv6	Onboarded Online



MAC address: c0:9b:f4:90:04:78

Firmware release: rock-image_3.1.0_dev-60-g6c6d71bc

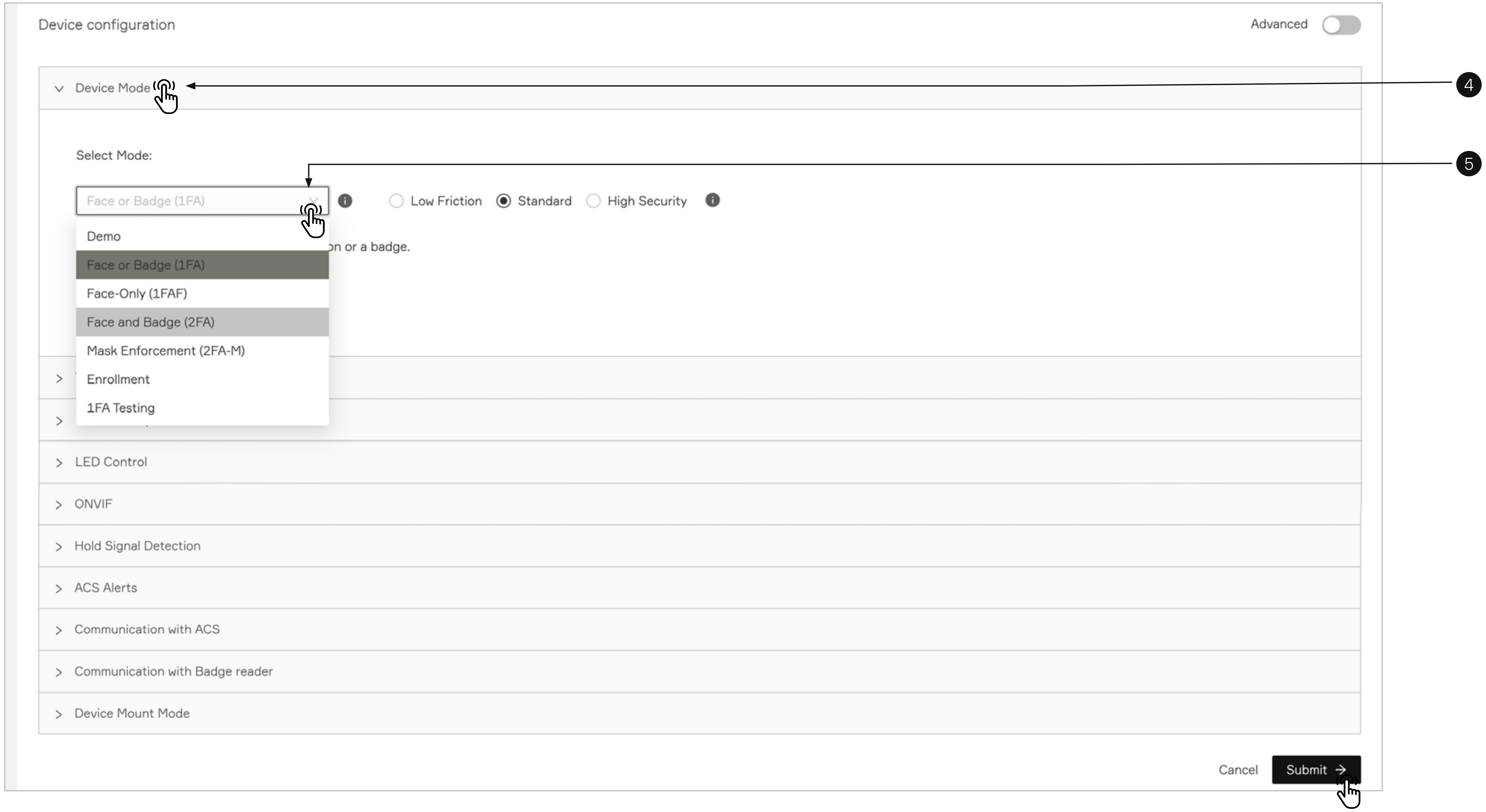
Device ID: 7a1da5179e904fa1a39e20275112dd21

IP address: 192.168.2.35/24 fe80::c29b:f4ff:fe90:478/64

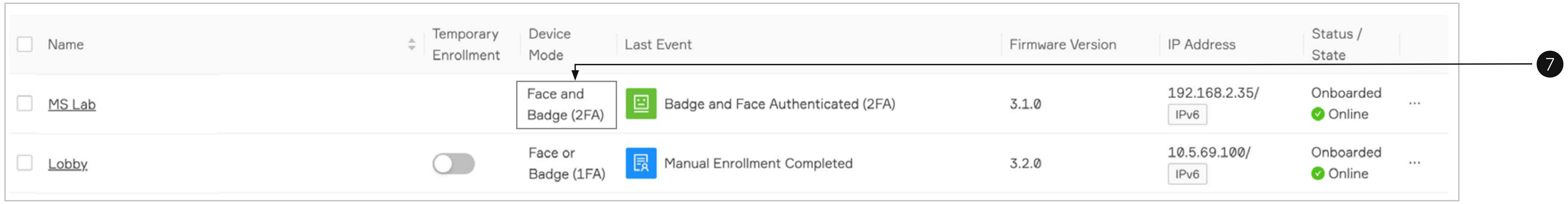
Board type: onyx-p1

Reader: N/A

4. Scroll down the page to **Device Configuration** and expand the **Device Mode** section.
5. Select the operational mode for the Rock.
   Low Friction, Standard, and High Security will be defaulted according to the mode but can be change.
   The various levels will determine if the Rock will make more/fewer checks, more/less friction and tolerance of light levels.
   The Rock will require more time to authenticate moving from low-friction to high security.
6. Click **Submit** when done.



7. Go to **Device Management** —> **Devices page**. The new selected mode will be displayed in the table next to the device name.



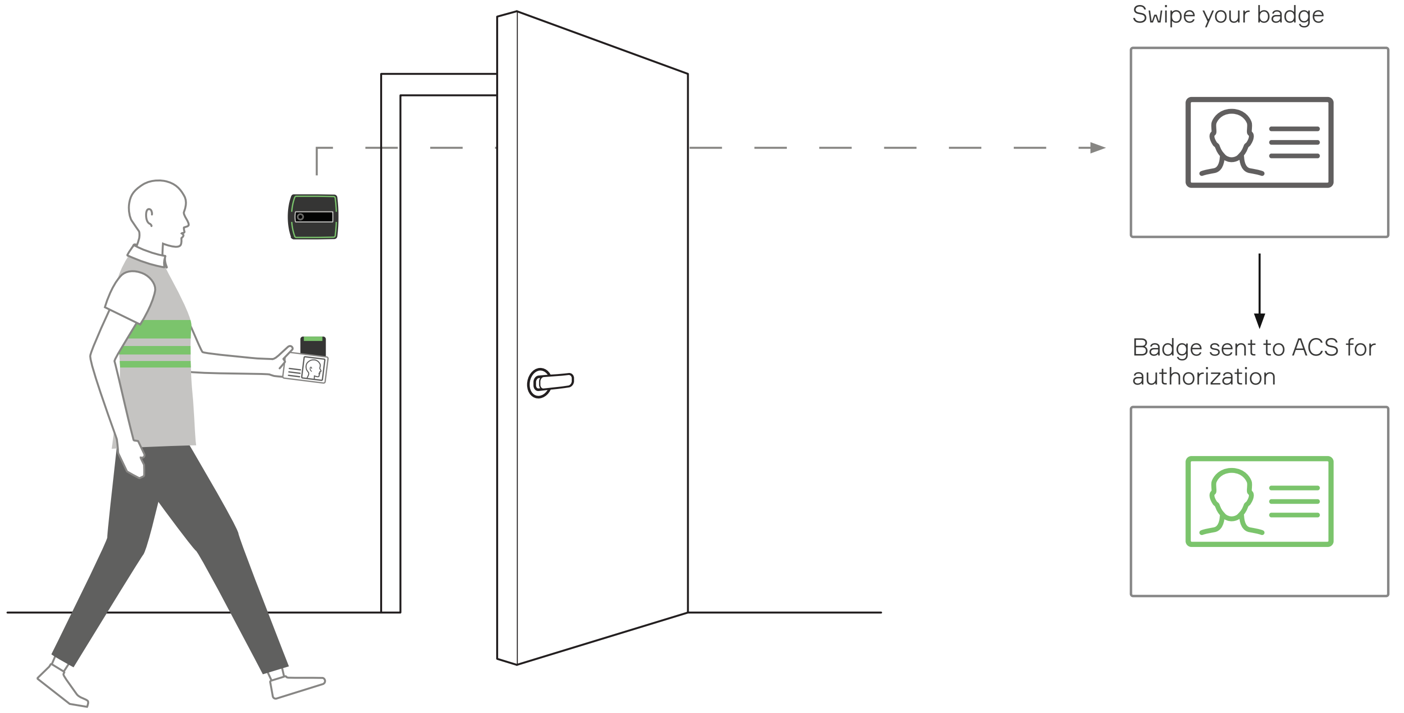
□	Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State	
□	MS Lab		Face and Badge (2FA)	Badge and Face Authenticated (2FA)	3.1.0	192.168.2.35/ IPv6	Onboarded Online	···
□	Lobby		Face or Badge (1FA)	Manual Enrollment Completed	3.2.0	10.5.69.100/ IPv6	Onboarded Online	···

6.2.2.1—Mode Setting – Demo

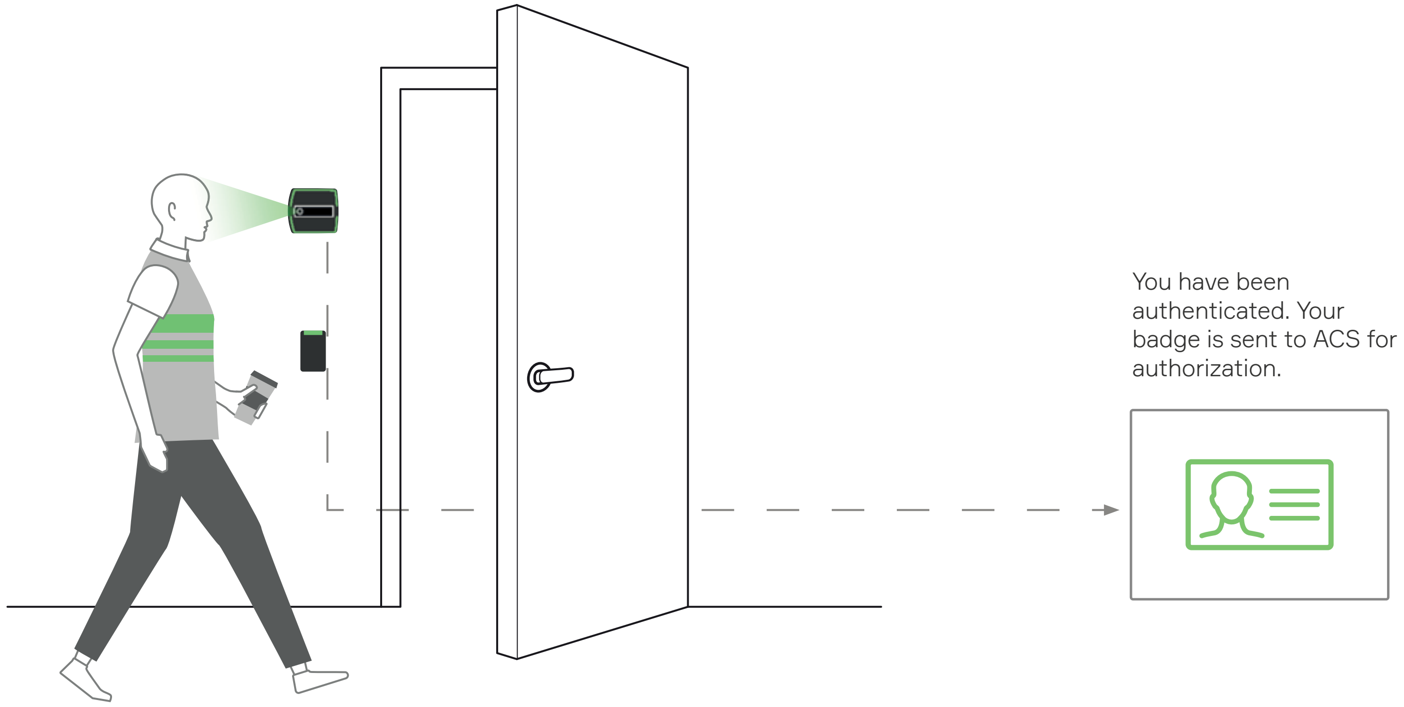
The Rock is shipped in Demo mode. In Demo mode, auto-enrollment is completed by swiping a badge twice with a few seconds in between. On the third entry, you will not be required to present your badge as the Rock will authenticate by facial credential.

Auto-Enrollment

Badge-in at least 2 times. It can be consecutive badge-ins.



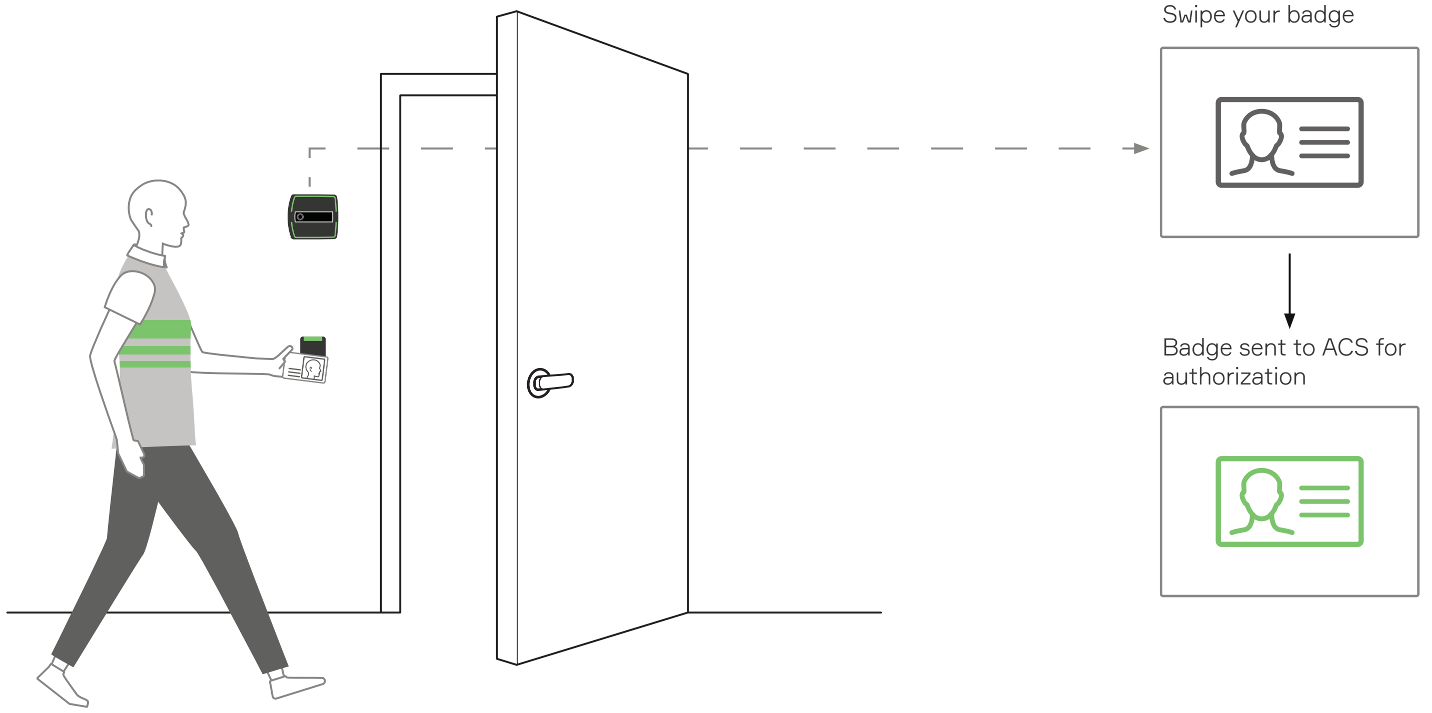
You have completed auto-enrollment. No badge is required, simply look at the Rock as you approach the door.


You have been authenticated. Your badge is sent to ACS for authorization.

6.2.2.2—Mode Setting – Face or Badge (1FA)

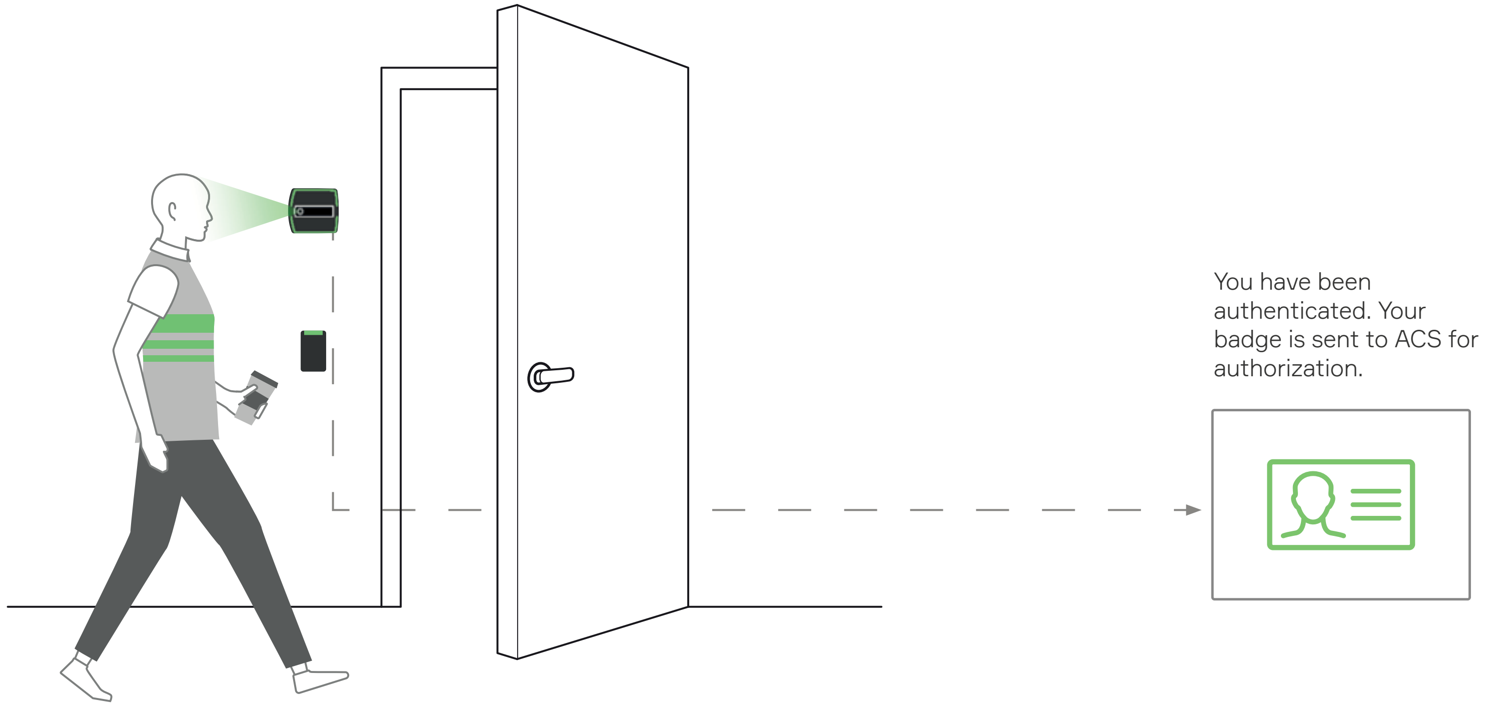
Auto-Enrollment

In 1FA, auto-enrollment is completed by swiping a badge at least 4-6 times over the period of a day or two. After that, your face is enrolled.



Single Factor Authentication

You have completed auto-enrollment. No badge is required, simply look at the Rock as you approach the door.

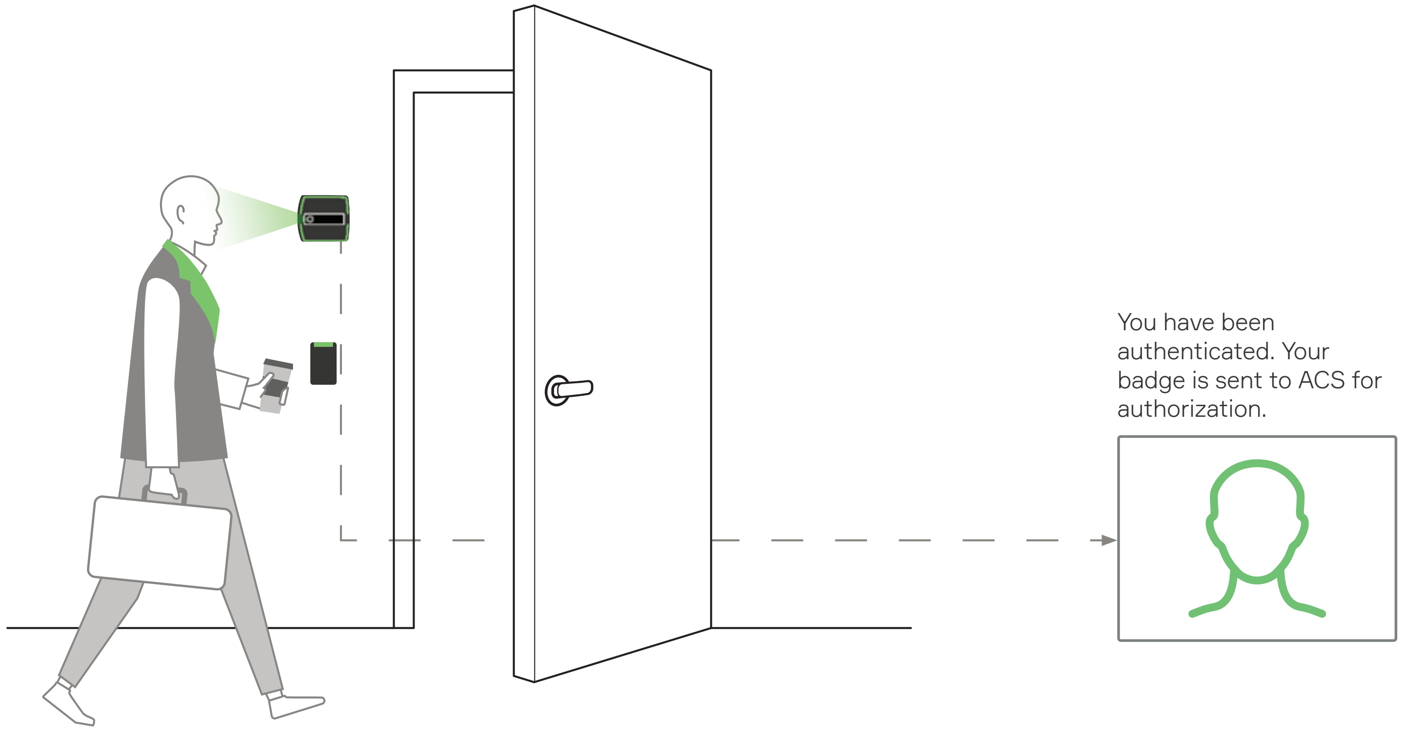

You have been authenticated. Your badge is sent to ACS for authorization.

6.2.2.3—Mode Setting – Face-Only (1FAF)

This Rock is in 1FAF or Single Factor Authentication Face-only.
This mode requires that you present your face. No badge is required.

Single Factor Authentication

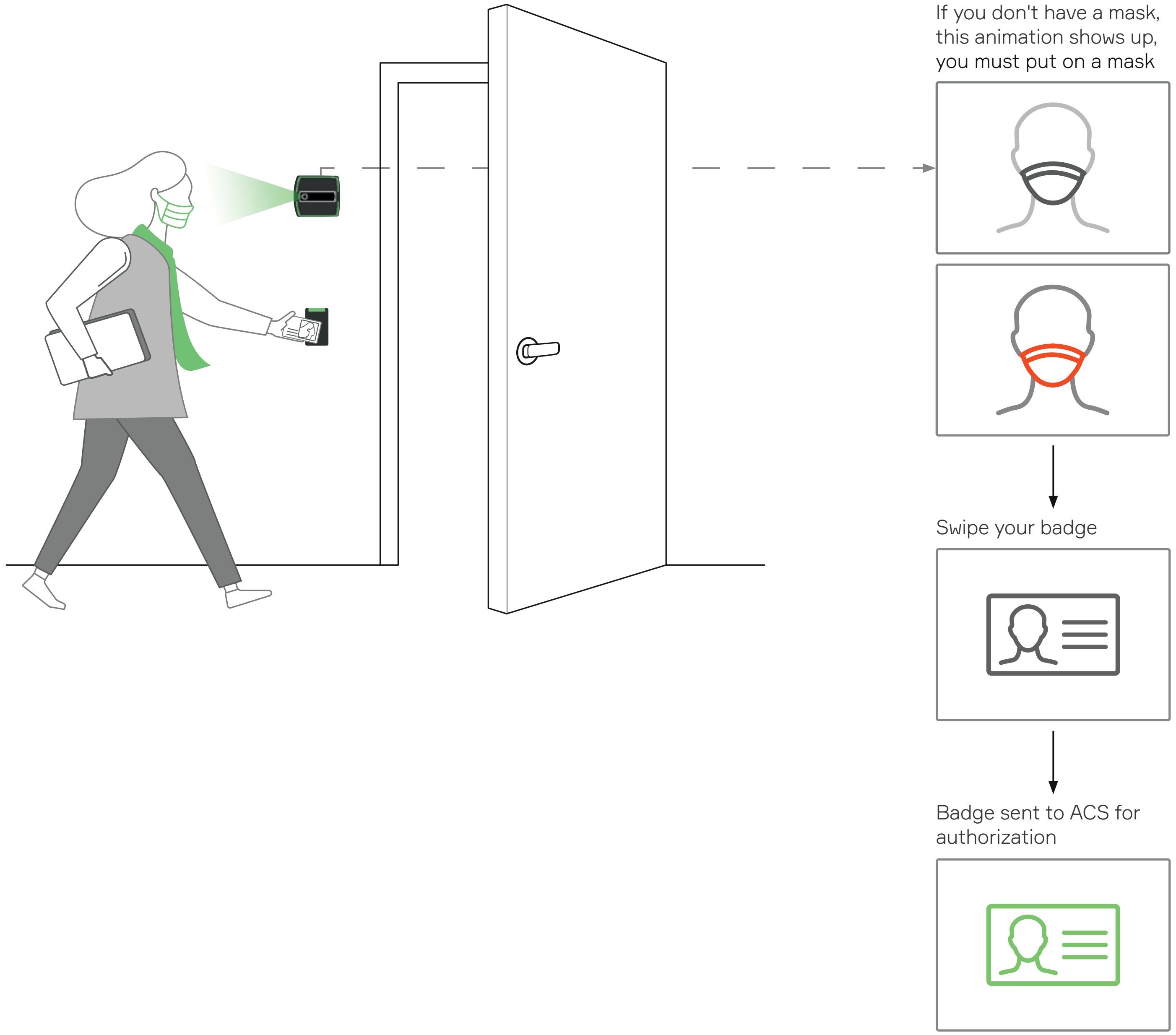
You have completed enrollment at an enrollment station. No badge is required, simply look at the Rock as you approach the door.



You have been authenticated. Your badge is sent to ACS for authorization.

6.2.2.4—Mode Setting – Mask Enforcement (2FA-M)

This Rock is in Mask Enforcement mode.
This mode requires you to wear a mask and present your badge.
No enrollment is required.
*If you are not wearing a mask when approaching the door, you must put one on before swiping your badge.



If you don't have a mask, this animation shows up, you must put on a mask

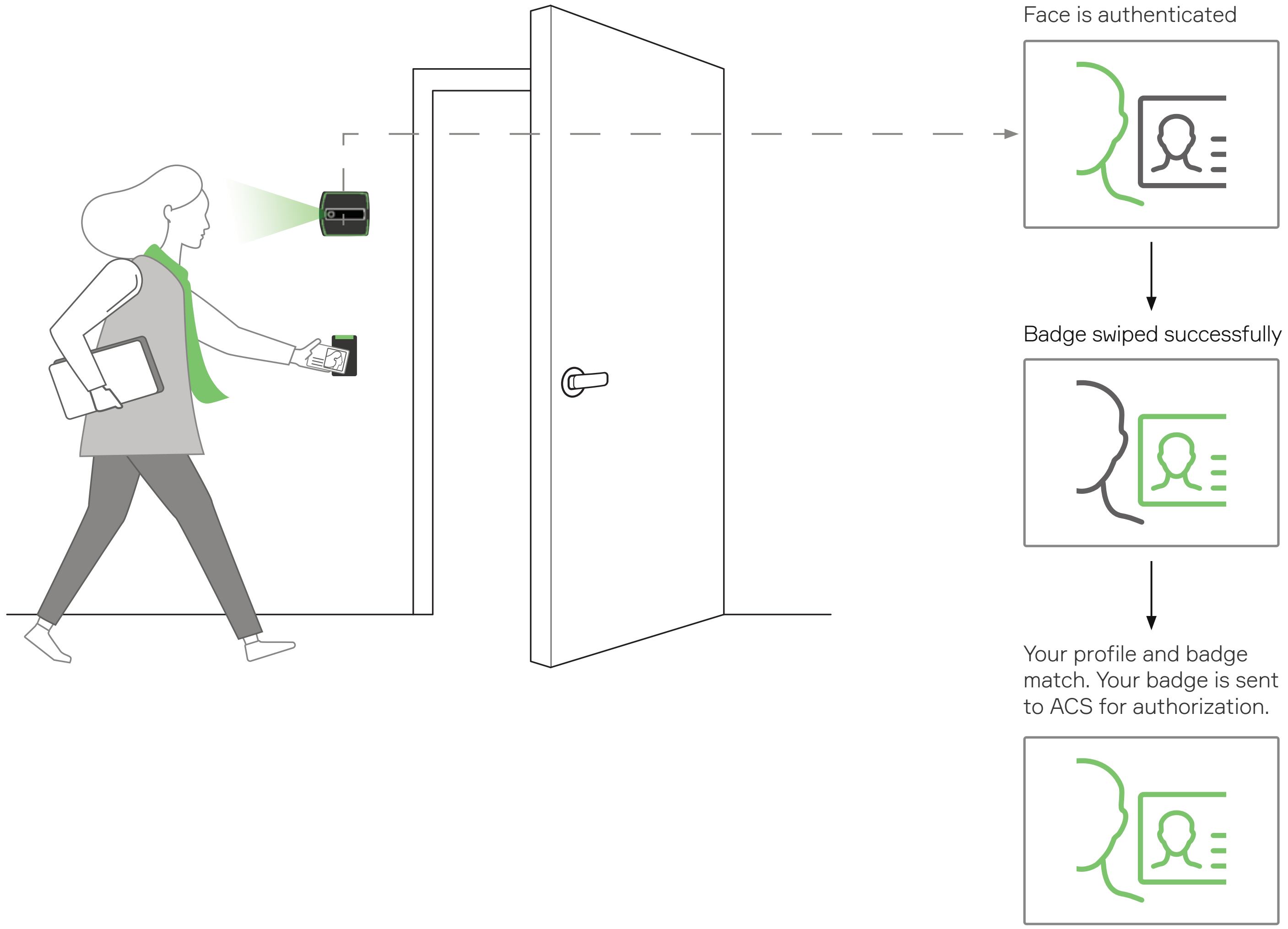
Swipe your badge

Badge sent to ACS for authorization

6.2.2.5—Mode Setting – Face and Badge (2FA)

This Rock is in 2FA mode or Two Factor Authentication.
This mode requires that you present you face and badge.

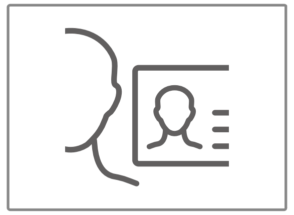
You have completed enrollment at an enrollment station. As you approach the door and badge in, the Rock captures your face and will verify if your face and your badge match.



Face is authenticated

Badge swiped successfully

Your profile and badge match. Your badge is sent to ACS for authorization.



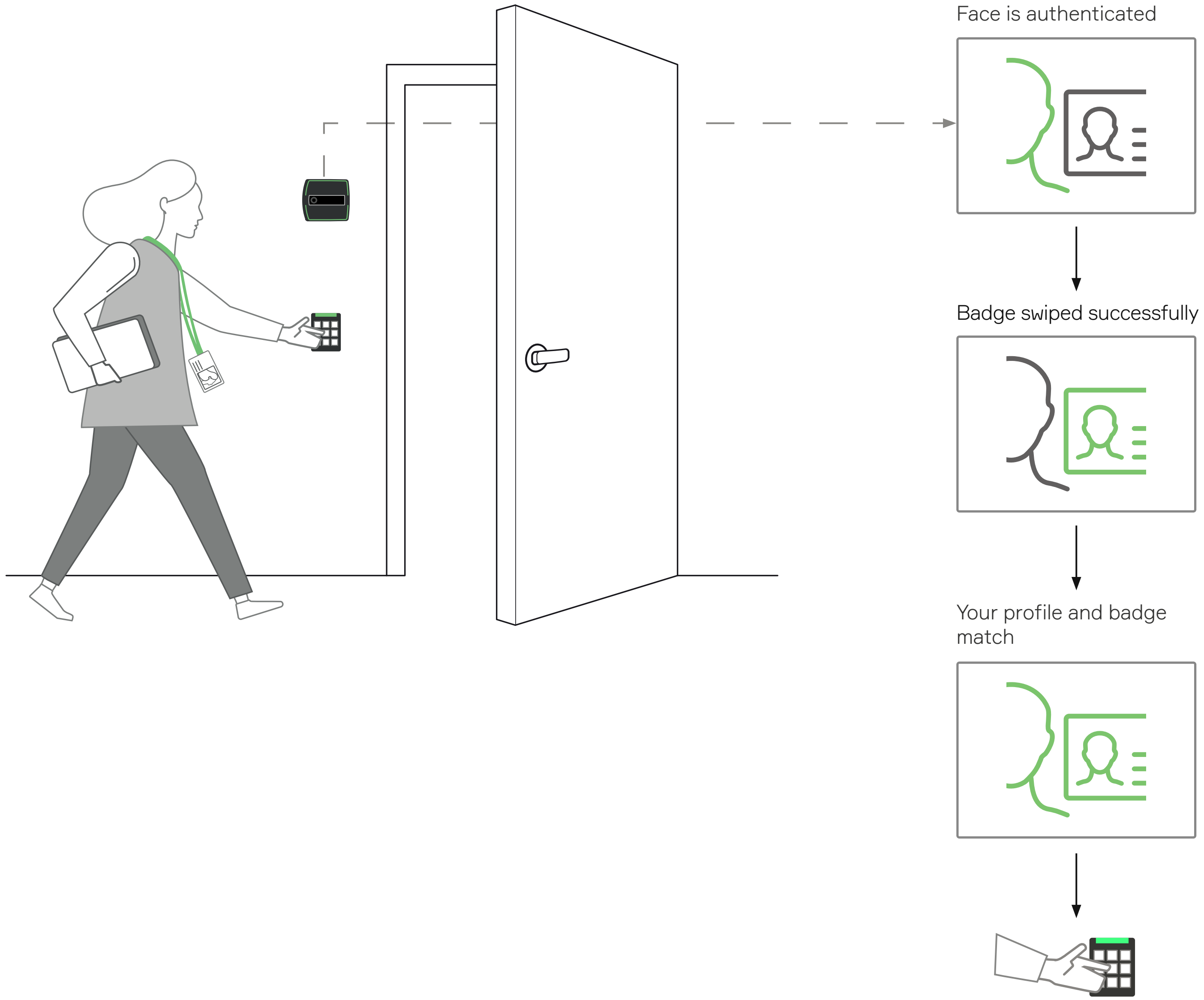
Seeing this on the Rock’s display?

You will need to enroll at the enrollment station. Please visit it and complete your enrollment.

6.2.2.6—Operating in 3FA

Follow 2FA requirements for presenting face and badge credentials but you will also enter a PIN.
ACS must be configured to accept Badge + PIN.

Toggle on **Support 3FA** option when selecting **2FA mode**.



Face is authenticated

Badge swiped successfully

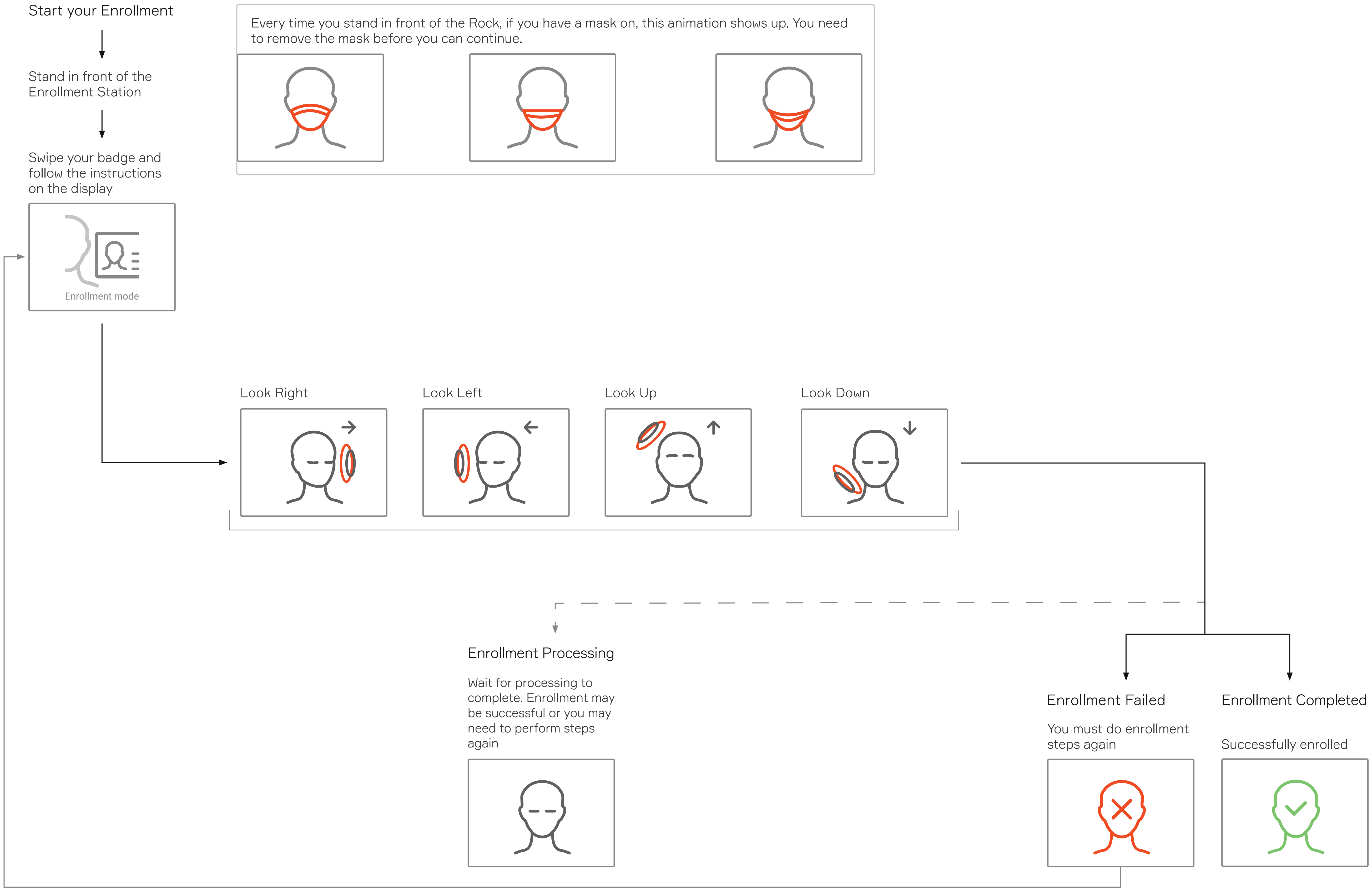
Your profile and badge match

Enter PIN. Your badge and PIN are sent to ACS for authorization.

Your ACS must be configured to accept badge and PIN.

6.2.2.7—Mode Setting – Enrollment

When the Rock mode is enrollment, the Rock will only enroll users. This is referred to as manual enrollment.
A Rock is designated as an enrollment station when set in enrollment mode.



Start your Enrollment

Stand in front of the Enrollment Station

Swipe your badge and follow the instructions on the display

Every time you stand in front of the Rock, if you have a mask on, this animation shows up. You need to remove the mask before you can continue.

Look Right

Look Left

Look Up

Look Down

Enrollment Processing

Wait for processing to complete. Enrollment may be successful or you may need to perform steps again

Enrollment Failed

You must do enrollment steps again

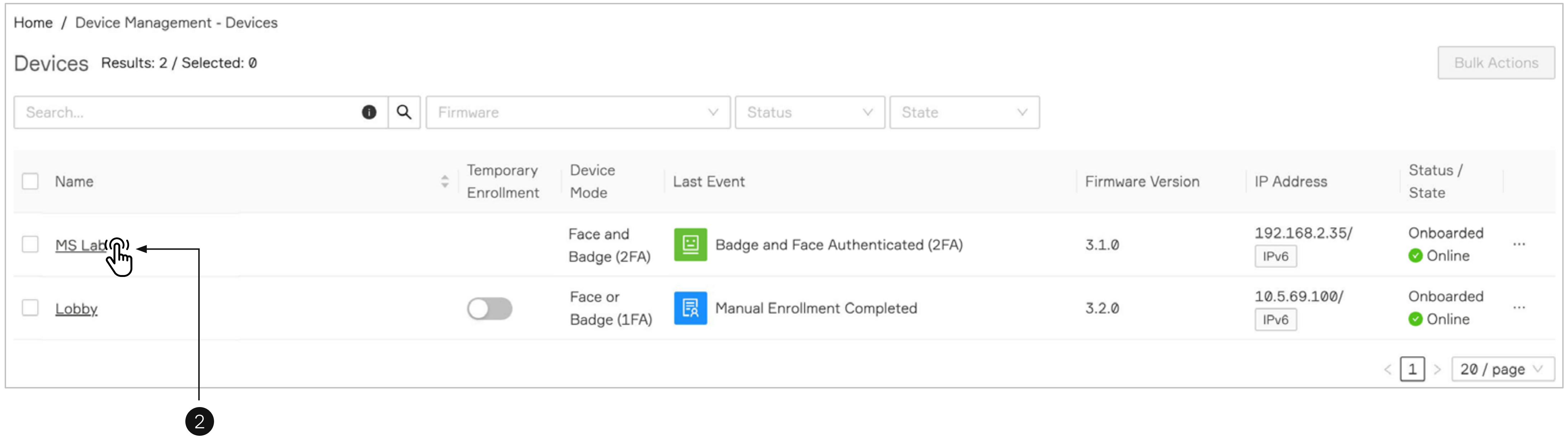
Enrollment Completed

Successfully enrolled

6.2.2.8—Temporary Enrollment

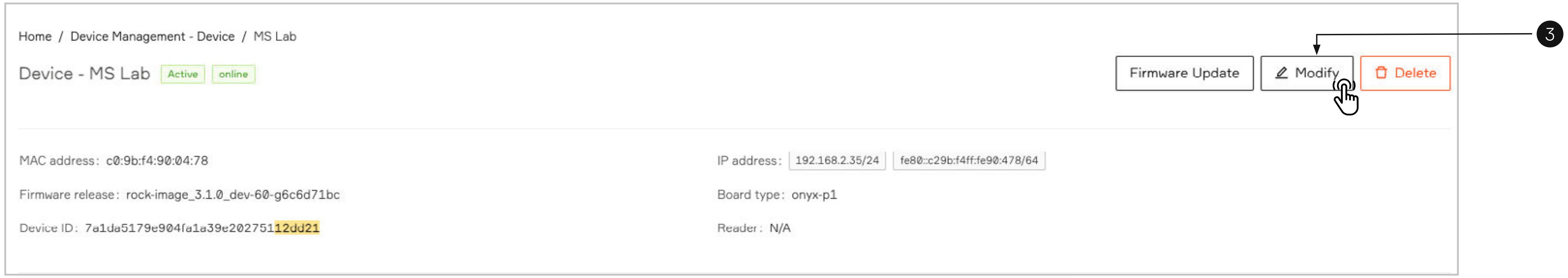
Temporary enrollment mode is an feature allowing to enroll additional people without requiring a change to Device Mode configuration. Enable it once and use it from the **Devices** page.

1. Go to **Device Management** and select **Devices**.
2. Click on the Name of the Rock to open the Rock’s info page.
3. Click on **Modify** to open up the configurations page.



Results: 2 / Selected: 0

	Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State	
□	MS Lab		Face and Badge (2FA)	Badge and Face Authenticated (2FA)	3.1.0	192.168.2.35/ IPv6	Onboarded ● Online	···
□	Lobby	○	Face or Badge (1FA)	Manual Enrollment Completed	3.2.0	10.5.69.100/ IPv6	Onboarded ● Online	···



MAC address: c0:9b:f4:90:04:78

Firmware release: rock-image_3.1.0_dev-60-g6c6d71bc

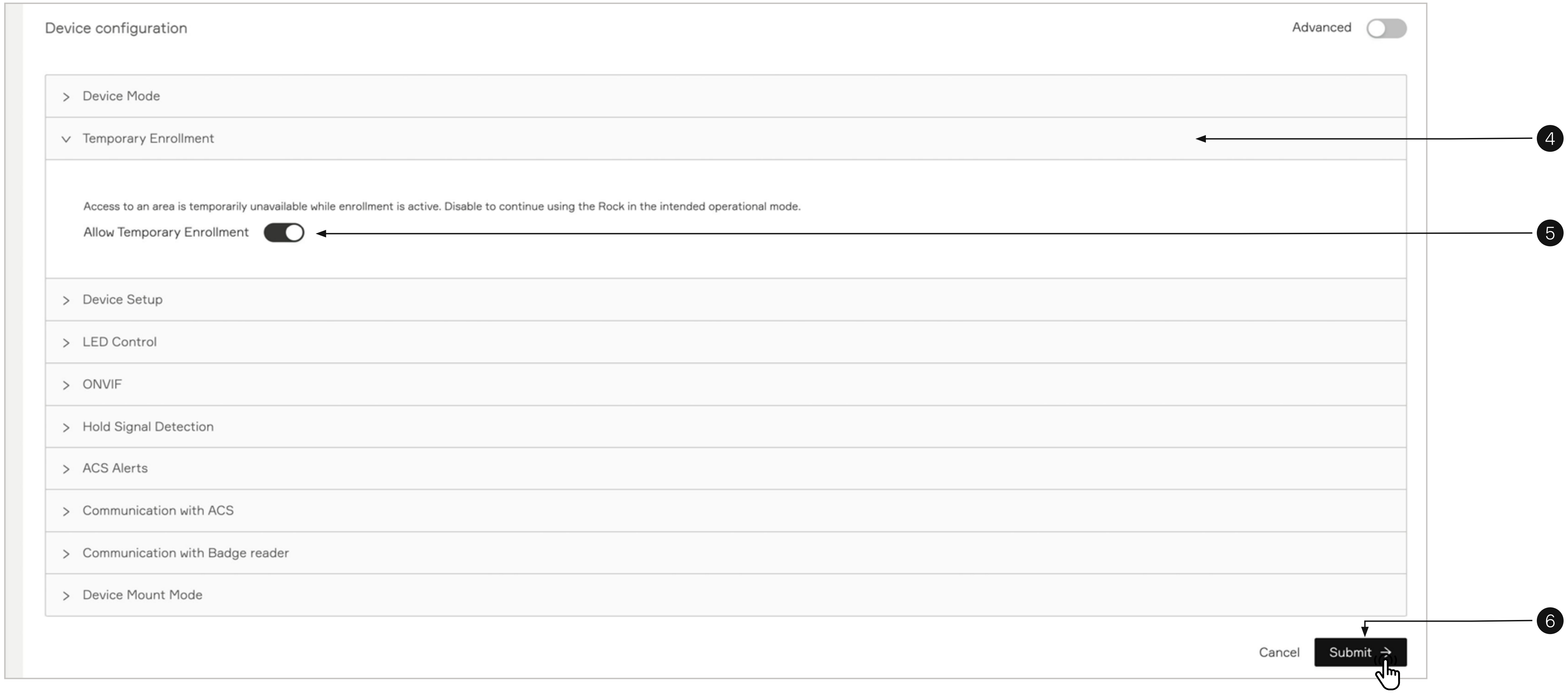
Device ID: 7a1da5179e904fa1a39e20275112dd21

IP address: 192.168.2.35/24 fe80::c29b:f4ff:fe90:478/64

Board type: onyx-p1

Reader: N/A

4. Scroll down the page to **Device Configuration** and expand the **Temporary Enrollment** section.
5. Enable the toggle for **Temporary Enrollment** feature.
6. Click **Submit** when done.



Device configuration

Advanced

- Device Mode
- Temporary Enrollment

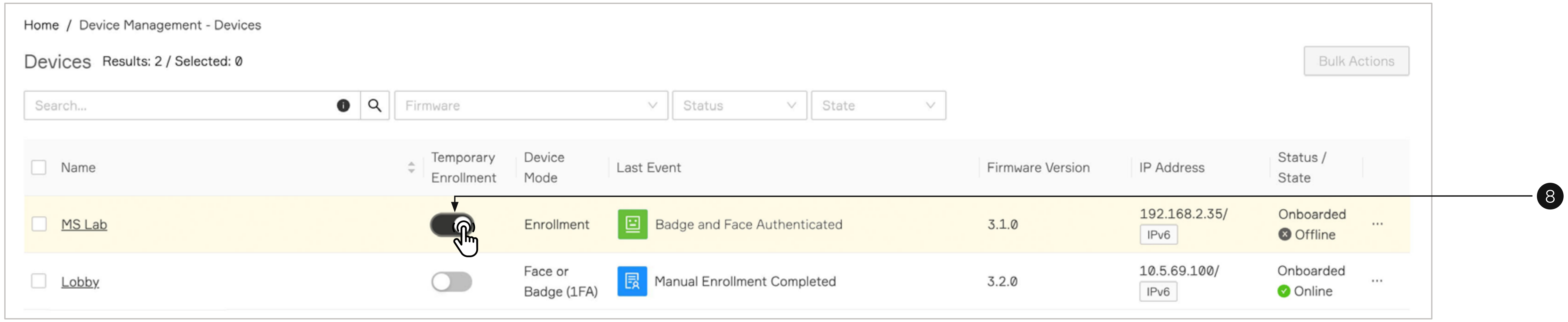
Access to an area is temporarily unavailable while enrollment is active. Disable to continue using the Rock in the intended operational mode.

Allow Temporary Enrollment

- Device Setup
- LED Control
- ONVIF
- Hold Signal Detection
- ACS Alerts
- Communication with ACS
- Communication with Badge reader
- Device Mount Mode

Cancel | Submit →

7. Go back to **Devices** page.
8. Toggle on **Temporary Enrollment** to switch the Rock to **Enrollment** mode.

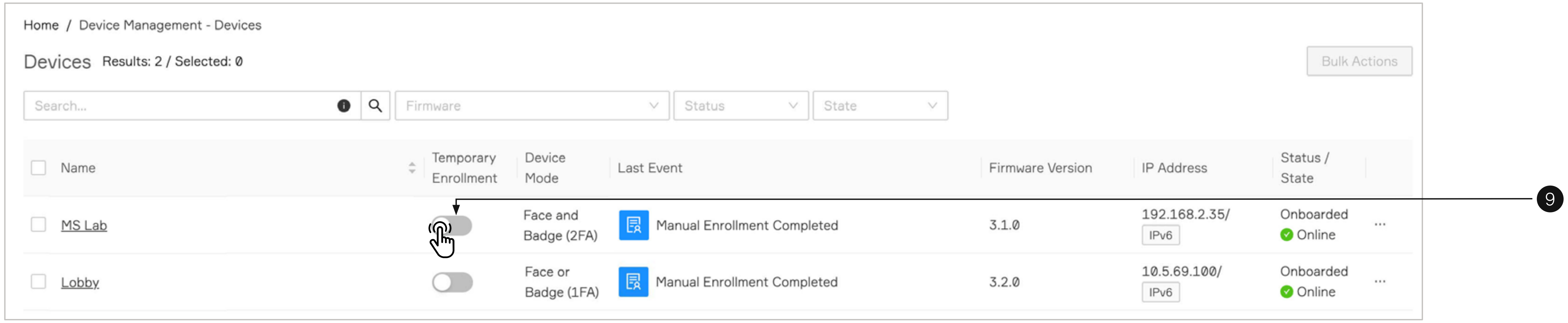


Home / Device Management - Devices

Devices Results: 2 / Selected: 0

□	Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State	
□	MS Lab	●	Enrollment	Badge and Face Authenticated	3.1.0	192.168.2.35/ IPv6	Onboarded Offline	···
□	Lobby	○	Face or Badge (1FA)	Manual Enrollment Completed	3.2.0	10.5.69.100/ IPv6	Onboarded Online	···

9. Toggle off to switch back to the previous device mode.

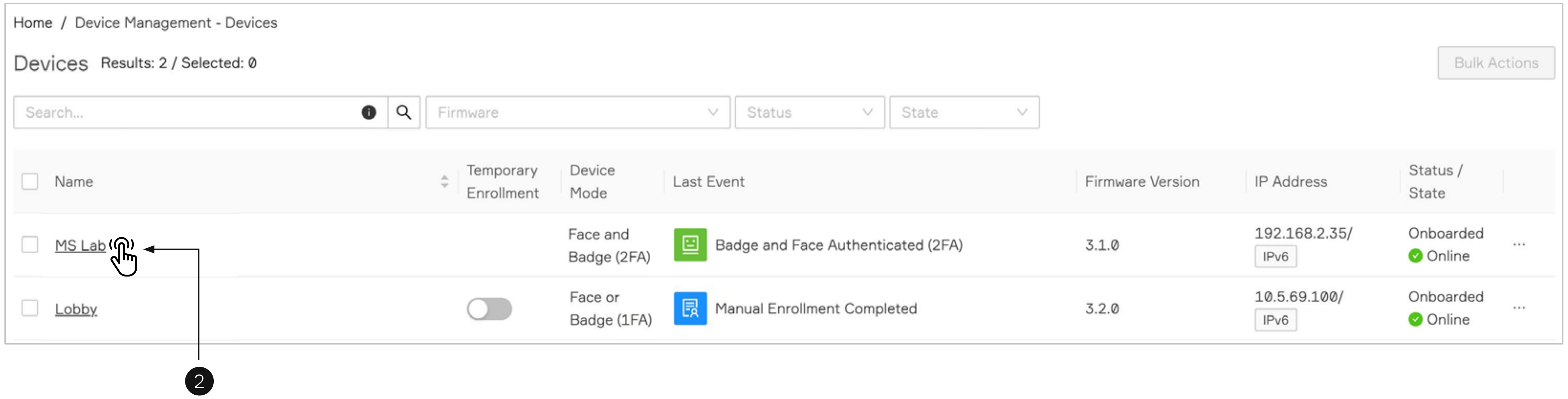

Home / Device Management - Devices
Devices Results: 2 / Selected: 0
Bulk Actions
Search...
Firmware
Status
State
9

□	Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State	
□	MS Lab		Face and Badge (2FA)	Manual Enrollment Completed	3.1.0	192.168.2.35/ IPv6	Onboarded Online	···
□	Lobby		Face or Badge (1FA)	Manual Enrollment Completed	3.2.0	10.5.69.100/ IPv6	Onboarded Online	···

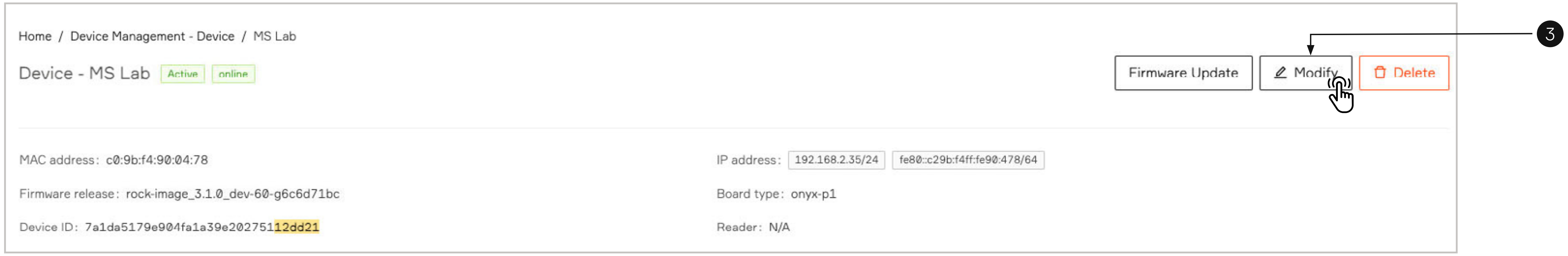
6.2.3—Device Setup (QR code configuration)

The Device options allow the rock to be easily reconfigured with QR code.

1. Go to **Device Management** and select **Devices**.
2. Click on the Name of the Rock to open the Rock's info page.
3. Click on **Modify** to open up the configurations page.


Home / Device Management - Devices
Devices Results: 2 / Selected: 0
Bulk Actions
Search...
Firmware
Status
State
2

□	Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State	
□	MS Lab		Face and Badge (2FA)	Badge and Face Authenticated (2FA)	3.1.0	192.168.2.35/ IPv6	Onboarded Online	···
□	Lobby		Face or Badge (1FA)	Manual Enrollment Completed	3.2.0	10.5.69.100/ IPv6	Onboarded Online	···



MAC address: c0:9b:f4:90:04:78

Firmware release: rock-image_3.1.0_dev-60-g6c6d71bc

Device ID: 7a1da5179e904fa1a39e20275112dd21

IP address: 192.168.2.35/24 fe80::c29b:f4ff:fe90:478/64

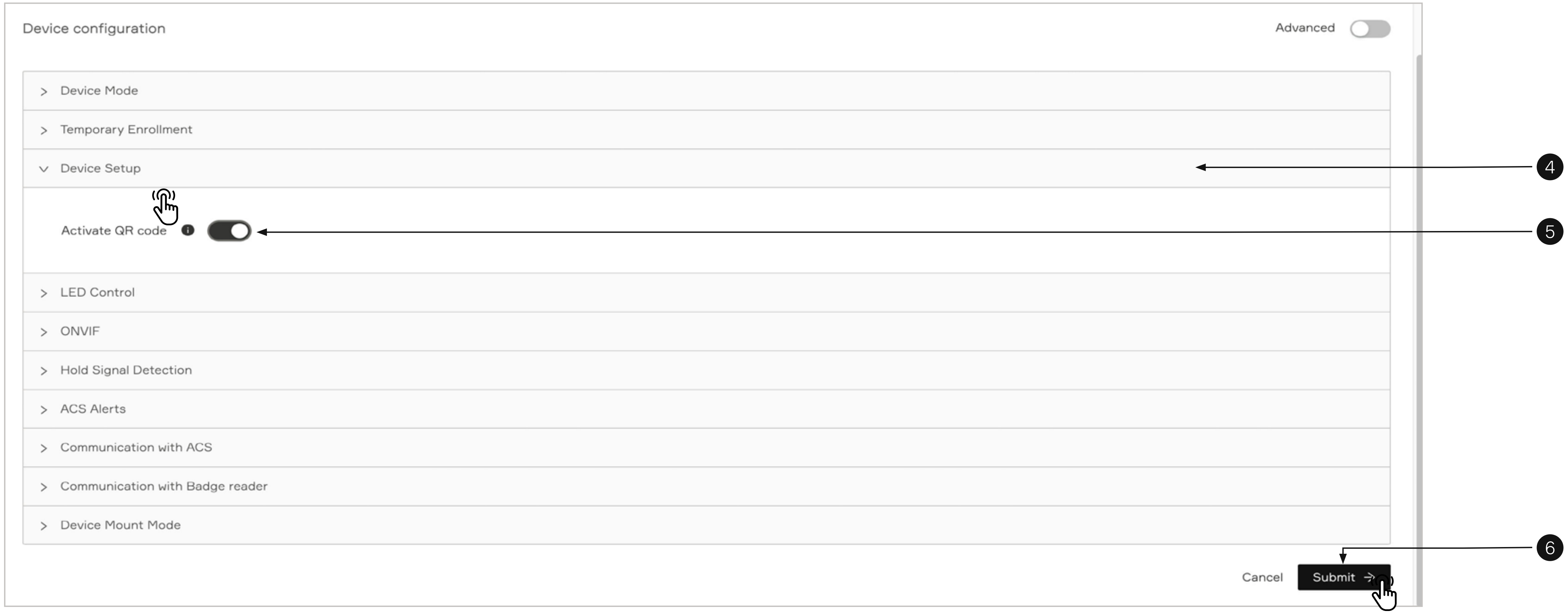
Board type: onyx-p1

Reader: N/A

alcatraz ai

- Dashboard
- Account
- Permissions
- Device Management
  - Devices
  - Updates
  - QR Code
- Security Events
- Profiles

1. Scroll down the page to **Device Configuration** and expand the **Device Setup** section.
2. Enable the toggle for **Activate QR code** feature (The option is disabled by default).
6. Click **Submit** when done.



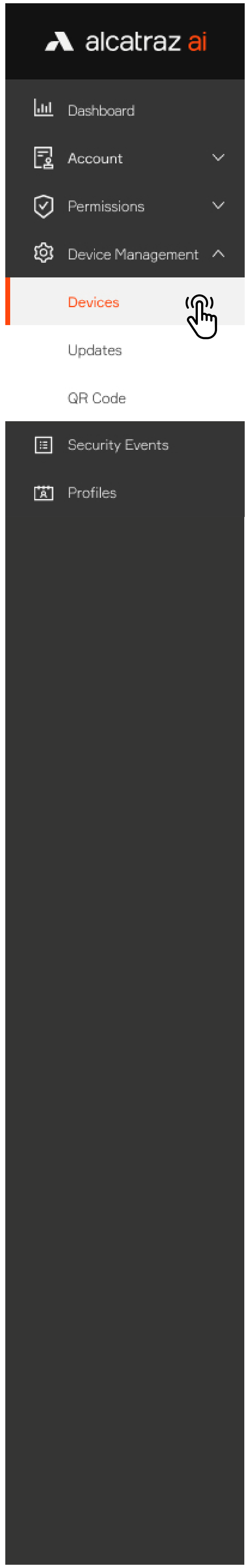
Device configuration

Advanced

- Device Mode
- Temporary Enrollment
- Device Setup
  - Activate QR code
- LED Control
- ONVIF
- Hold Signal Detection
- ACS Alerts
- Communication with ACS
- Communication with Badge reader
- Device Mount Mode

Cancel Submit

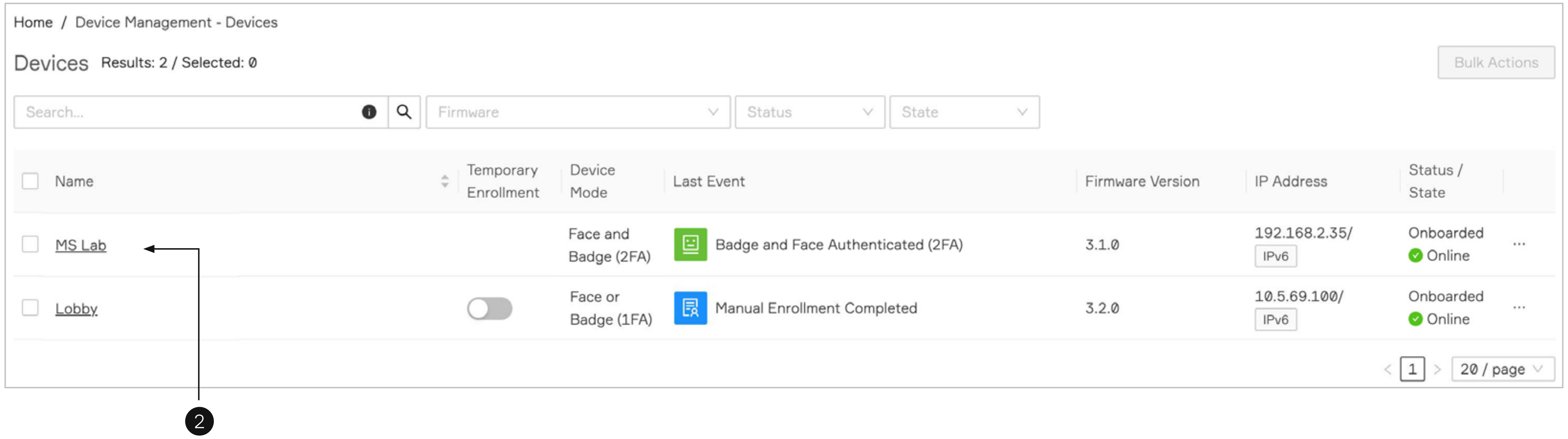
After Enabling the QR code receptive icon will be displayed on the device screen.



6.2.4—LED Control

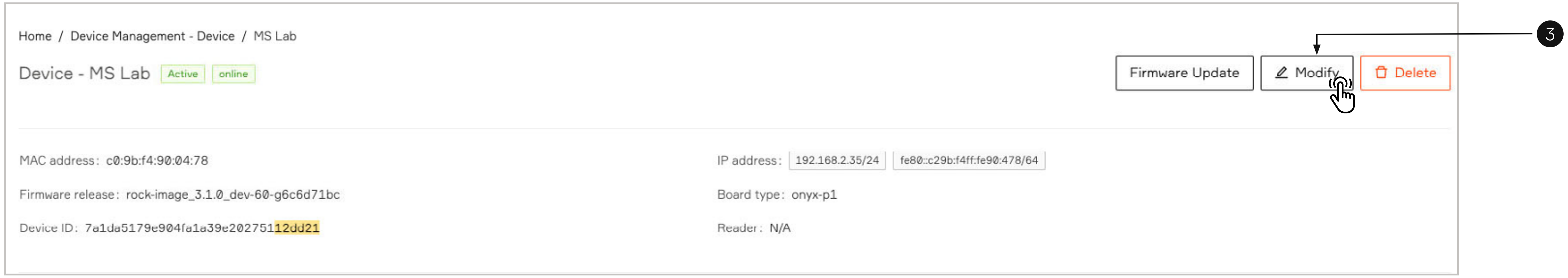
The Rock has a Ring of LEDs that will change color depending on what controls the color change. That is, the Rock could be configured to control the color change and ignore any color signals from the ACS, or it can be configured to change colors based on feedback from the ACS, or it could be configured so that the LED color changes are controlled by the ACS.

1. Go to **Device Management** and select **Devices**.
2. Click on the Name of the Rock to open the Rock's info page.
3. Click on **Modify** to open up the configurations page.



Results: 2 / Selected: 0

Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State
MS Lab		Face and Badge (2FA)	Badge and Face Authenticated (2FA)	3.1.0	192.168.2.35/ IPv6	Onboarded Online
Lobby		Face or Badge (1FA)	Manual Enrollment Completed	3.2.0	10.5.69.100/ IPv6	Onboarded Online



MAC address: c0:9b:f4:90:04:78

Firmware release: rock-image_3.1.0_dev-60-g6c6d71bc

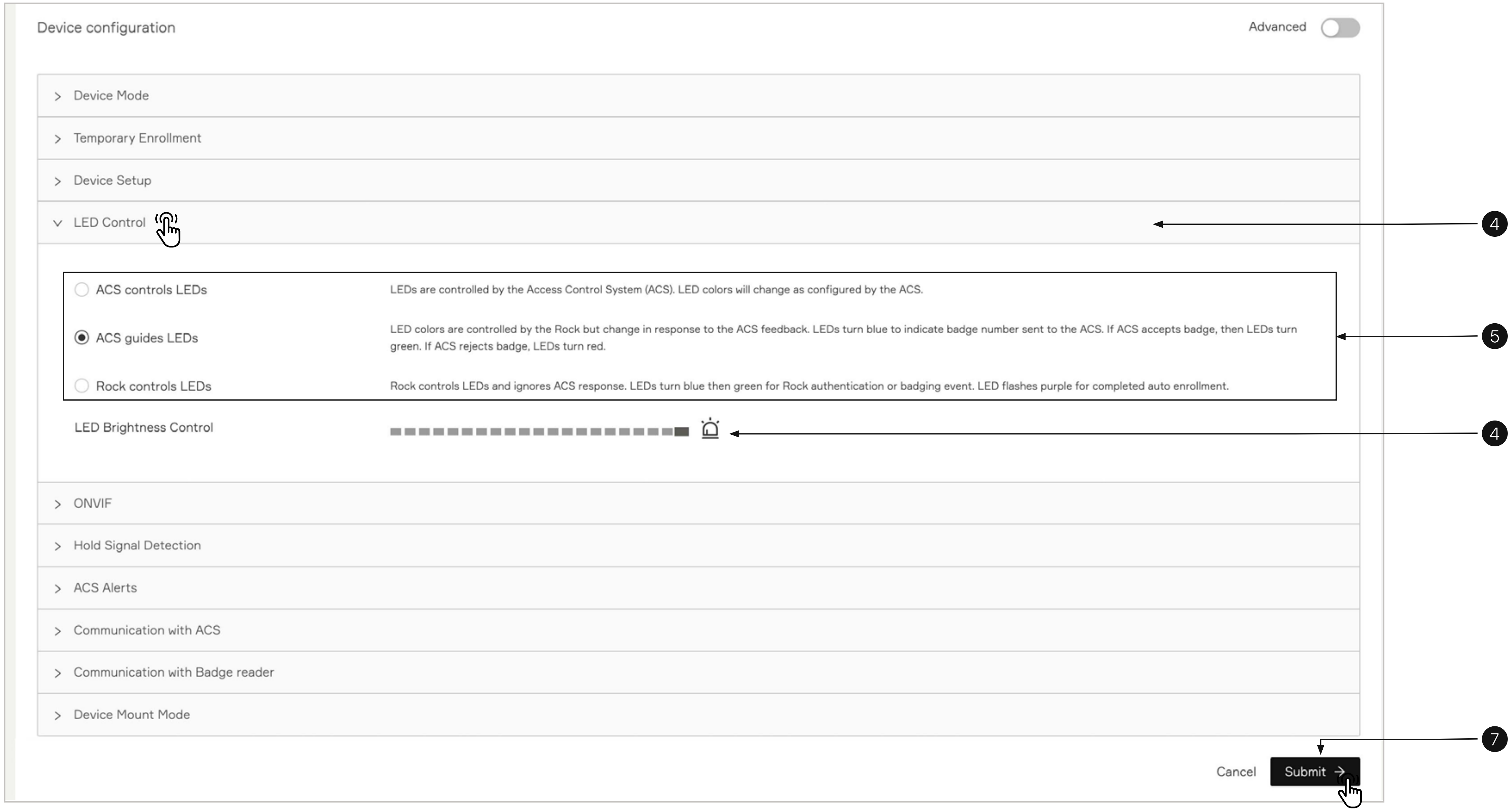
Device ID: 7a1da5179e904fa1a39e20275112dd21

IP address: 192.168.2.35/24 fe80::c29b:f4ff:fe90:478/64

Board type: onyx-p1

Reader: N/A

4. Scroll down the page to **Device Configuration** and expand the **LED control** section
5. Select one of the LED Control setting
   a. **ACS controls LEDs** – this is the default mode of the Rock, the LEDs are controlled by the ACS so changes in the LED color seen should be checked with ACS configurations
   b. **ACS guides LEDs** – LED color change is in response to ACS feedback. The Rock will display green in response to a badge accepted by the ACS and red if rejected.
   If face is authenticated and accepted by ACS, then the Rock will display blue then green.
   c. **Rock controls LEDs** – LED color is controlled by the Rock. LEDs will turn blue then green for authentication event and and just green for badging event. It will also display purple for a person who has completed auto-enrollment.
6. **LED Brightness Control** (optional). The LED brightness control section allows to the user to configure the intensity/brightness of the LED lights on the peripheral of the Rock. A user can choose an option between 0 and 20, where zero means that the LED lights will be turned off and 20 means the LED lights brightness will be set to maximum intensity. Adjust the LED brightness if needed.
7. Click **Submit** when done.

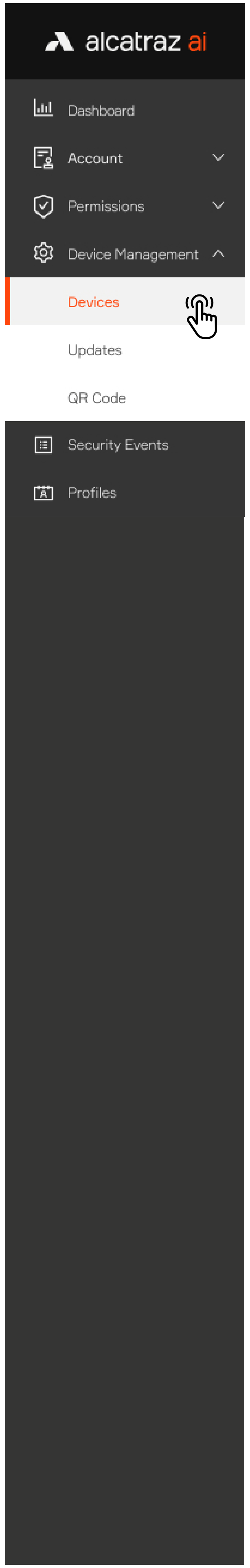


○ ACS controls LEDs — LEDs are controlled by the Access Control System (ACS). LED colors will change as configured by the ACS.

● ACS guides LEDs — LED colors are controlled by the Rock but change in response to the ACS feedback. LEDs turn blue to indicate badge number sent to the ACS. If ACS accepts badge, then LEDs turn green. If ACS rejects badge, LEDs turn red.

○ Rock controls LEDs — Rock controls LEDs and ignores ACS response. LEDs turn blue then green for Rock authentication or badging event. LED flashes purple for completed auto enrollment.

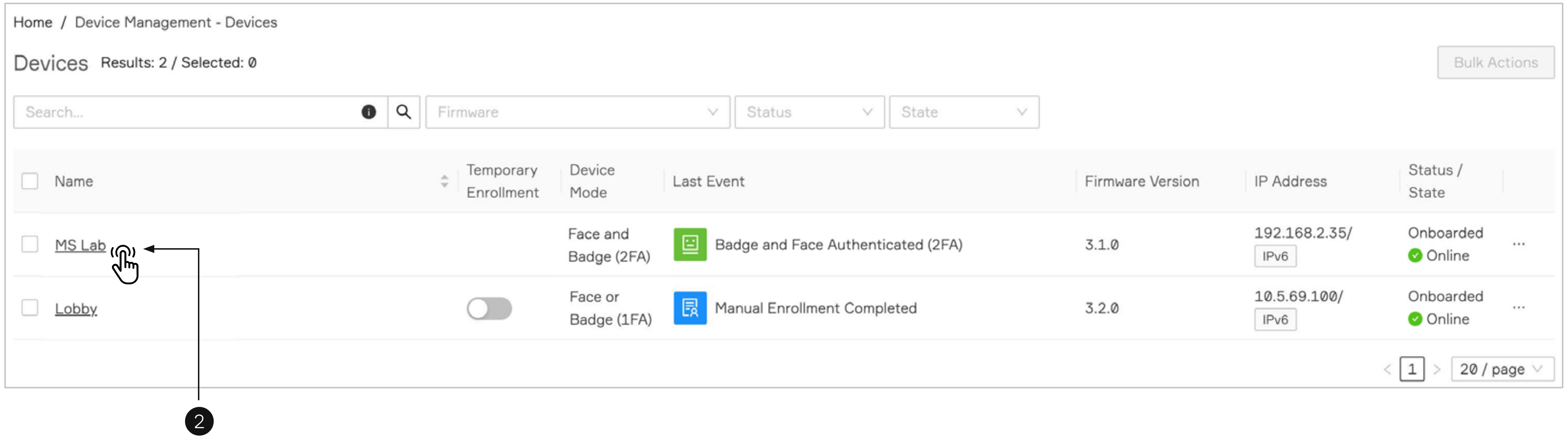
LED Brightness Control



6.2.5—ONVIF

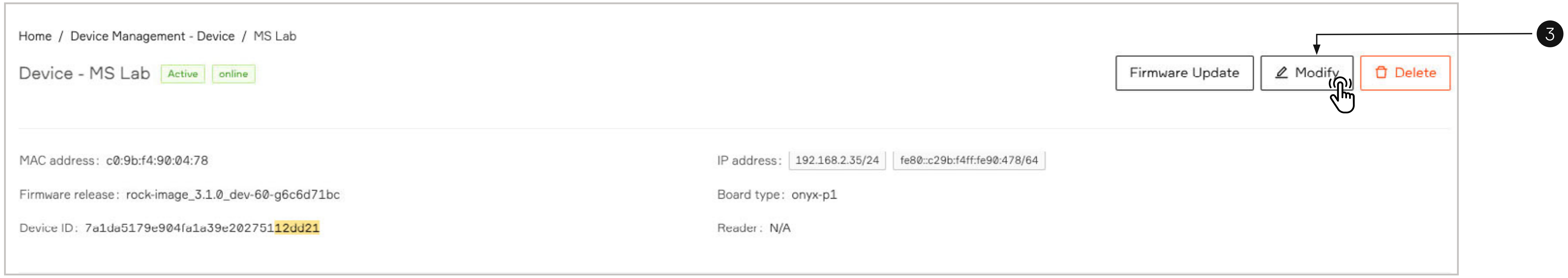
The Rock can communicate with any device that is ONVIF (Open Network Video Interface Forum) compatible. The Rock is compatible for Profile S and Profile T for devices that follow the ONVIF standards.

1. Go to **Device Management** and select **Devices**.
2. Click on the Name of the Rock to open the Rock's info page.
3. Click on **Modify** to open up the configurations page.



Results: 2 / Selected: 0

	Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State
□	MS Lab		Face and Badge (2FA)	Badge and Face Authenticated (2FA)	3.1.0	192.168.2.35/ IPv6	Onboarded ● Online
□	Lobby	○	Face or Badge (1FA)	Manual Enrollment Completed	3.2.0	10.5.69.100/ IPv6	Onboarded ● Online



MAC address: c0:9b:f4:90:04:78

Firmware release: rock-image_3.1.0_dev-60-g6c6d71bc

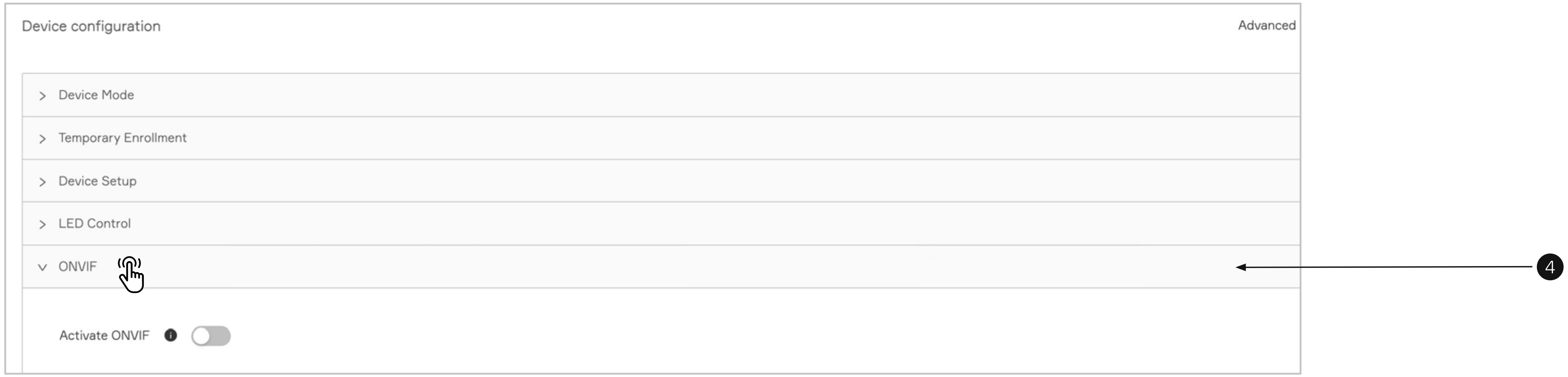
Device ID: 7a1da5179e904fa1a39e20275112dd21

IP address: 192.168.2.35/24 fe80::c29b:f4ff:fe90:478/64

Board type: onyx-p1

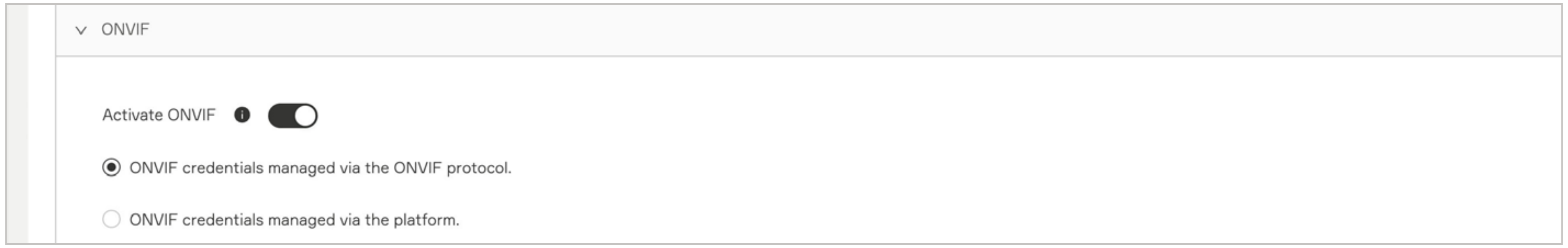
Reader: N/A

4. Scroll down the page to **Device Configuration** and expand the **ONVIF** section.
   ONVIF is disabled by default. To enable it turn on the toggle. There are two options for managing ONVIF credentials for accessing the video stream



Activate ONVIF ○

a. First option is those credentials to be managed via the ONVIF protocol. Where those credentials are default. Username is admin and password is the last 6 digits of the device id.

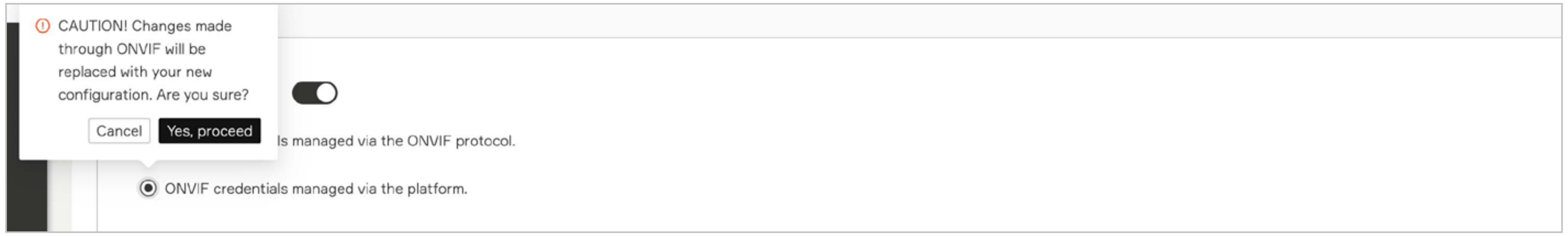


Activate ONVIF ●

● ONVIF credentials managed via the ONVIF protocol.

○ ONVIF credentials managed via the platform.

b. Second option is the credentials to be managed by the platform. Selecting it will replace the default ONVIF configuration.

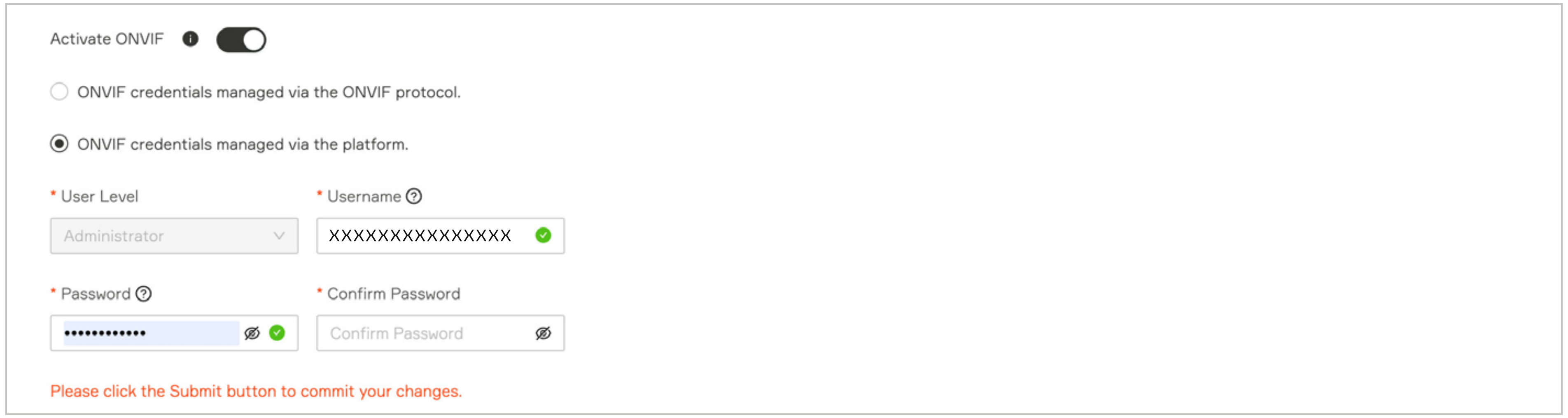


CAUTION! Changes made through ONVIF will be replaced with your new configuration. Are you sure?

ls managed via the ONVIF protocol.

● ONVIF credentials managed via the platform.

After choosing this option input fields will be displayed allowing to change the default credentials.
Select the appropriate option by your preferences.


Activate ONVIF

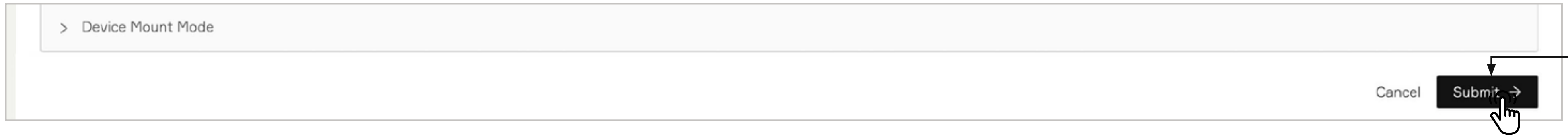
○ ONVIF credentials managed via the ONVIF protocol.

● ONVIF credentials managed via the platform.

* User Level	* Username
Administrator	XXXXXXXXXXXXXXX
* Password	* Confirm Password
••••••••••••	Confirm Password

Please click the Submit button to commit your changes.

5. Click **Submit** to confirm

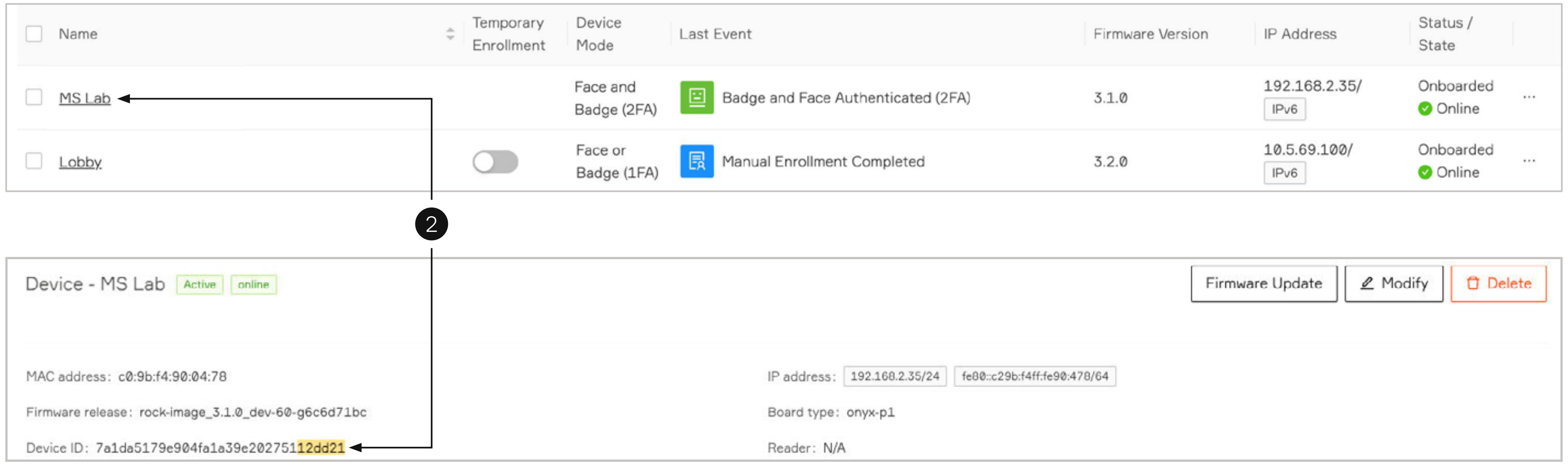


6.2.5.1—Adding a Rock to the VMS (ONVIF)

The Rock supports any Video Management System (VMS) that adheres to the ONVIF standard.
Please use the following info to connect with the VMS:
Username: admin
Password: (the last 6 digits of the device ID)

To locate the last 6 digits:

1. Go to **Device Management** and select **Devices**.
2. Locate the Rock to be connected to the VMS from the list.
   Open the device details page by clicking on the name of the rock from the table. Use the last 6 digits of the Device ID (marked in yellow) as the password.



Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State
MS Lab		Face and Badge (2FA)	Badge and Face Authenticated (2FA)	3.1.0	192.168.2.35/ IPv6	Onboarded ✓ Online
Lobby	○	Face or Badge (1FA)	Manual Enrollment Completed	3.2.0	10.5.69.100/ IPv6	Onboarded ✓ Online

Device - MS Lab Active online

MAC address: c0:9b:f4:90:04:78
Firmware release: rock-image_3.1.0_dev-60-g6c6d71bc
Device ID: 7a1da5179e904fa1a39e20275112dd21

IP address: 192.168.2.35/24 fe80::c29b:f4ff:fe90:478/64
Board type: onyx-p1
Reader: N/A

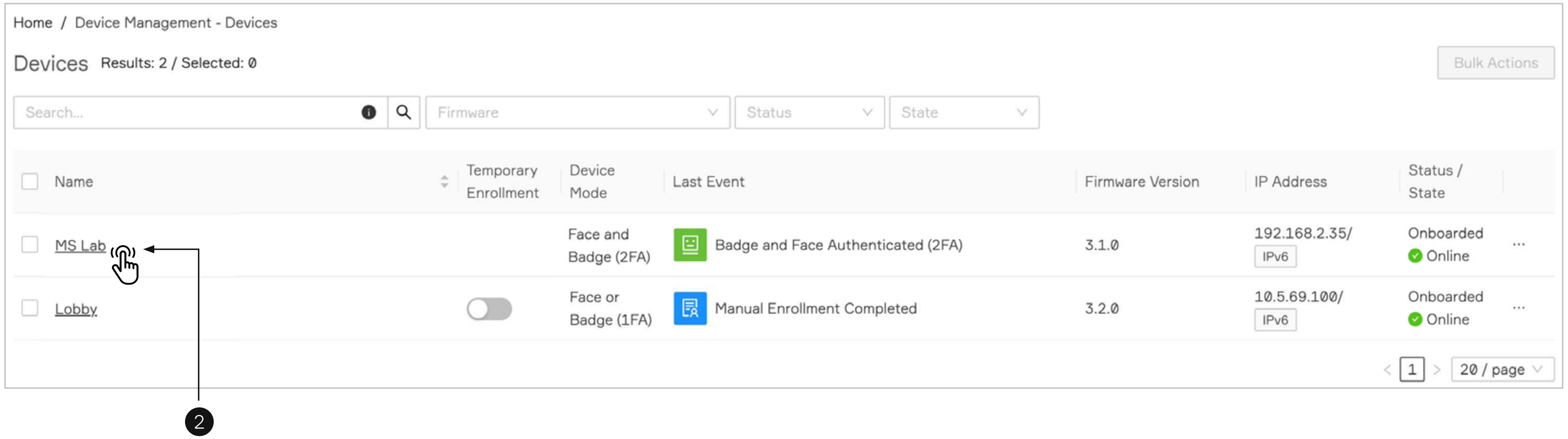
alcatraz ai
Dashboard
Account
Permissions
Device Management
Devices
Updates
QR Code
Security Events
Profiles

6.2.6—HOLD Signal Detection

The HOLD signal works for only Wiegand. (The HOLD signal does not work when Rock to ACS Panel interface is OSDP.)
Asserting the HOLD signal will suspend operations

- no authentications
- no badge numbers sent to the ACS
- no new events displayed in the portal

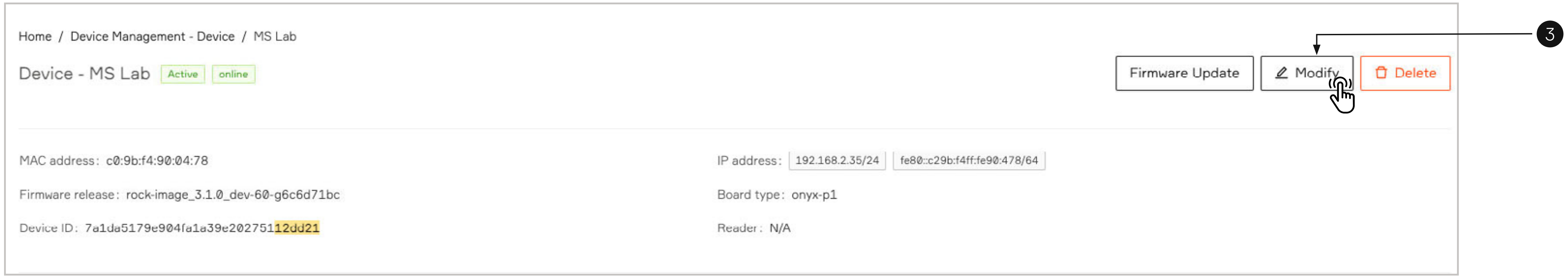
1. Go to **Device Management** and select **Devices**.
2. Click on the Name of the Rock to open the Rock's info page.
3. Click on **Modify** to open up the configurations page.



Results: 2 / Selected: 0

	Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State	
□	MS Lab		Face and Badge (2FA)	Badge and Face Authenticated (2FA)	3.1.0	192.168.2.35/ IPv6	Onboarded Online	...
□	Lobby		Face or Badge (1FA)	Manual Enrollment Completed	3.2.0	10.5.69.100/ IPv6	Onboarded Online	...

< 1 > 20 / page



MAC address: c0:9b:f4:90:04:78

Firmware release: rock-image_3.1.0_dev-60-g6c6d71bc

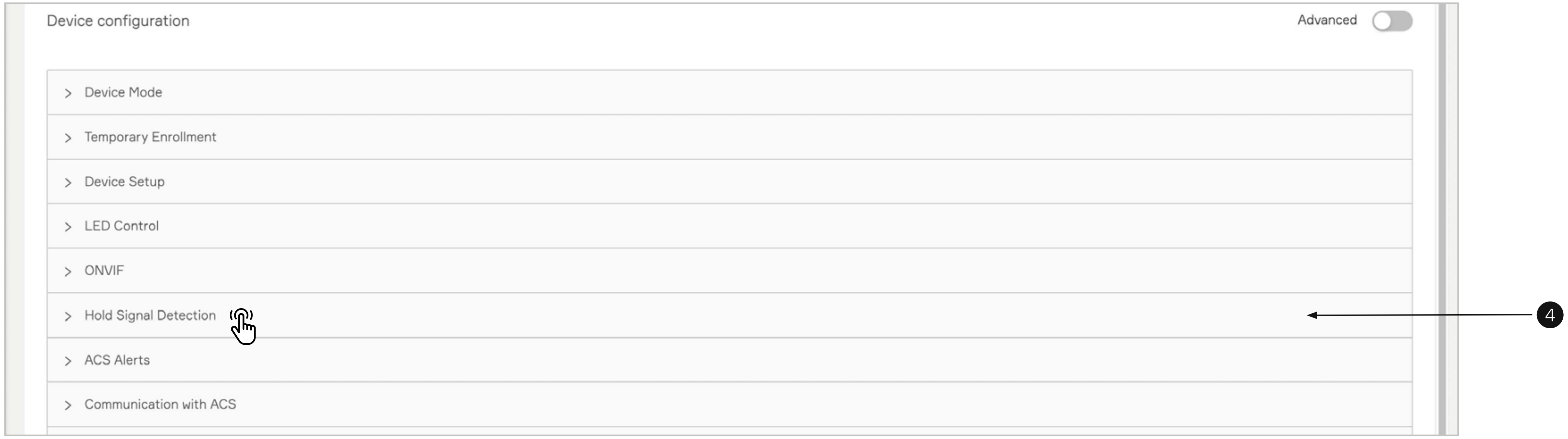
Device ID: 7a1da5179e904fa1a39e20275112dd21

IP address: 192.168.2.35/24 fe80::c29b:f4ff:fe90:478/64

Board type: onyx-p1

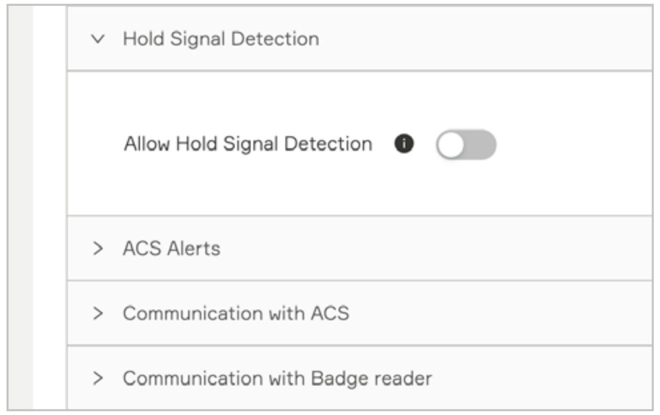
Reader: N/A

4. Scroll down the page to **Device Configuration** and expand the **Hold Signal Detection**

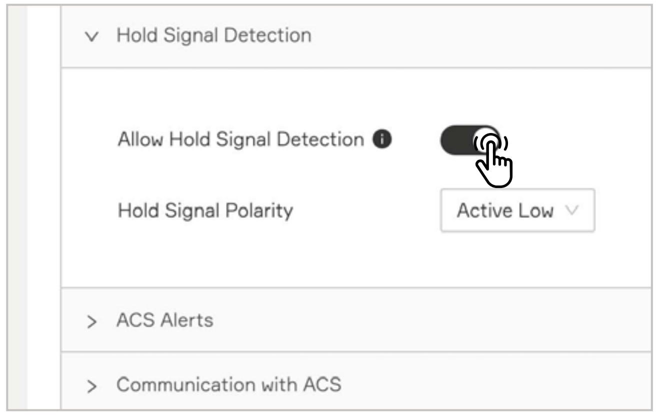


5. The **Hold Signal Detection** is disabled by default, click to enable.
6. To enable turn on the toggle. When enabled, a selection for the polarity of the Hold signal will appear. For Hold Signal Polarity select Active Low (Hold is effective when the Hold signal from the ACS is Low) or Active High (Hold is effective when the Hold signal from the ACS is High). The Rock will suspend all operations when the Hold signal is asserted from the ACS

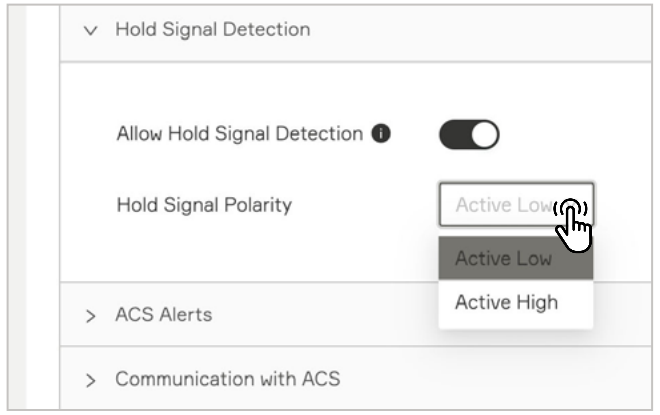
Default setting



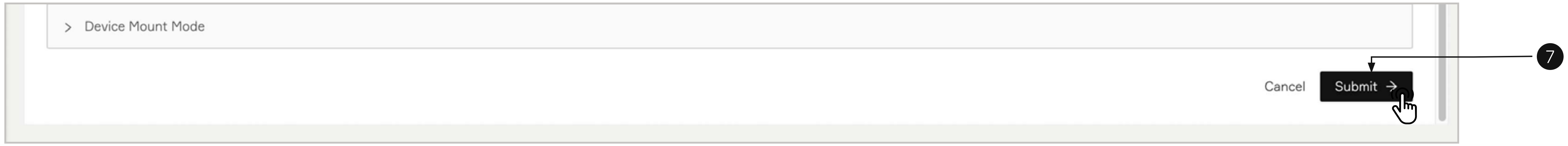
To enable



Hold Signal Polarity options



7. Click **Submit** when done



6.2.7—Configure ACS Alerts

An "un-allocated" badge number can be assigned to send the ACS alerts about a tailgating, crossing, or unauthorized entry security event that occurred at the door. This badge number will be sent via Wiegand or OSDP just like the badge number of authenticated users. The events will show up in the ACS just like an 'Access Granted' or 'Door Forced' along with the associated door. Once in the ACS, they can be used to trigger video call-ups, sound alarms, or simply for reporting purposes.

TIP: Before proceeding to configure, ensure that the badge number and facility code info is displayed correctly in the Alcatraz AI Admin Portal. Swipe the badge with the card reader. A 1FA Badge Access Granted event will appear under Device Management -> Security Events. Read the badge number and facility code for the event and verify the info matches when configuring in the ACS.

Step 1 – Configure Cardholder in Access Control System (ACS)

Create one or more cardholders by assigning the "un-allocated" badge numbers to the alert(s) you wish to be notified.
For example the cardholder could have a first name = 'Tailgating' and last name = 'Alert'.
Potential alerts are:

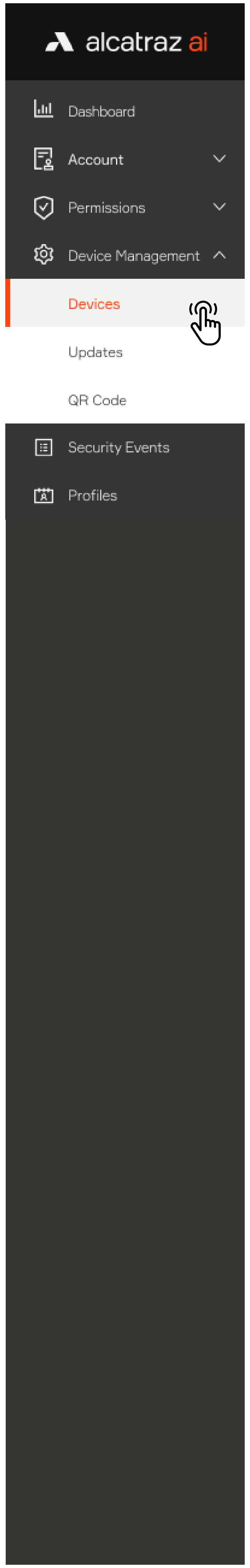
- Tailgating
- Unauthorized Entry
- Crossing

Use the following table to gather info for the alert(s) to configure:

Alert	Badge Number	Facility Code	Card Format
Tailgating			like 26-bit, 35-bit corp1000, etc
Crossing			
Unauthorized Entry			
2FA Mismatch			

Step 2 – Card Format is Configured in Alcatraz AI Admin Portal

If the Card Format has not already been assigned and/or configured for the site, details for doing so can be found here: Configure Card Format.
If you are unsure whether or not a card format has been configured, go to Accounts and scroll down to the Card Information section.



alcatraz ai

Dashboard

Account

Permissions

Device Management

Devices

Updates

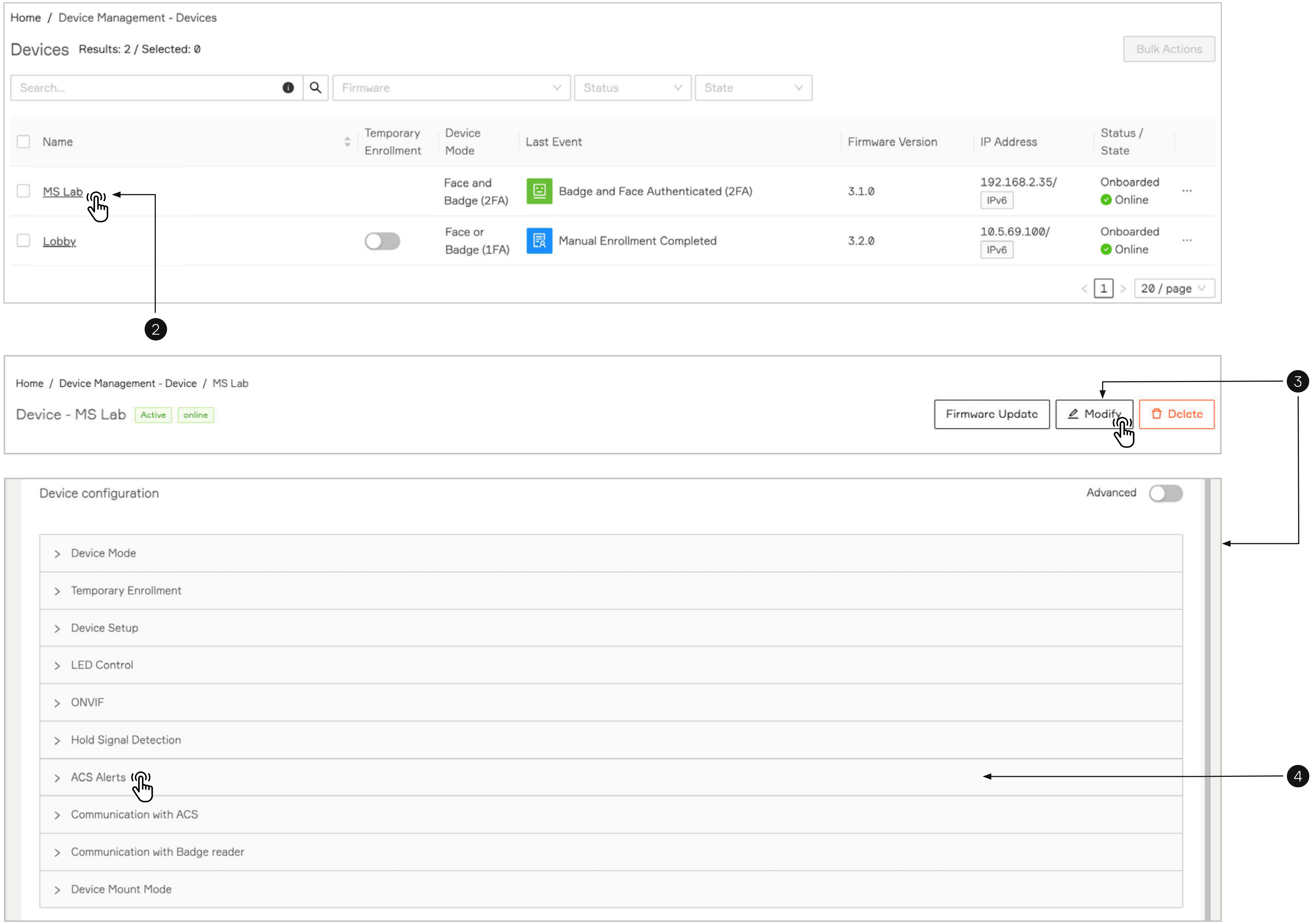
QR Code

Security Events

Profiles

Step 3 – Configure Alerts in the Alcatraz AI Admin Portal

1. Go to **Device Management** and select **Devices**.
2. Click on the Name of the Rock to open the Rock's info page.
3. Click on **Modify** to open up the configurations page.
4. Scroll down the page to **Device Configuration** and expand the **ACS Alerts section**.



Home / Device Management - Devices

Devices Results: 2 / Selected: 0

Bulk Actions

Search... | Firmware | Status | State

	Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State	
□	MS Lab		Face and Badge (2FA)	Badge and Face Authenticated (2FA)	3.1.0	192.168.2.35/ IPv6	Onboarded ● Online	···
□	Lobby	○	Face or Badge (1FA)	Manual Enrollment Completed	3.2.0	10.5.69.100/ IPv6	Onboarded ● Online	···

< 1 > 20 / page

Home / Device Management - Device / MS Lab

Device - MS Lab Active online

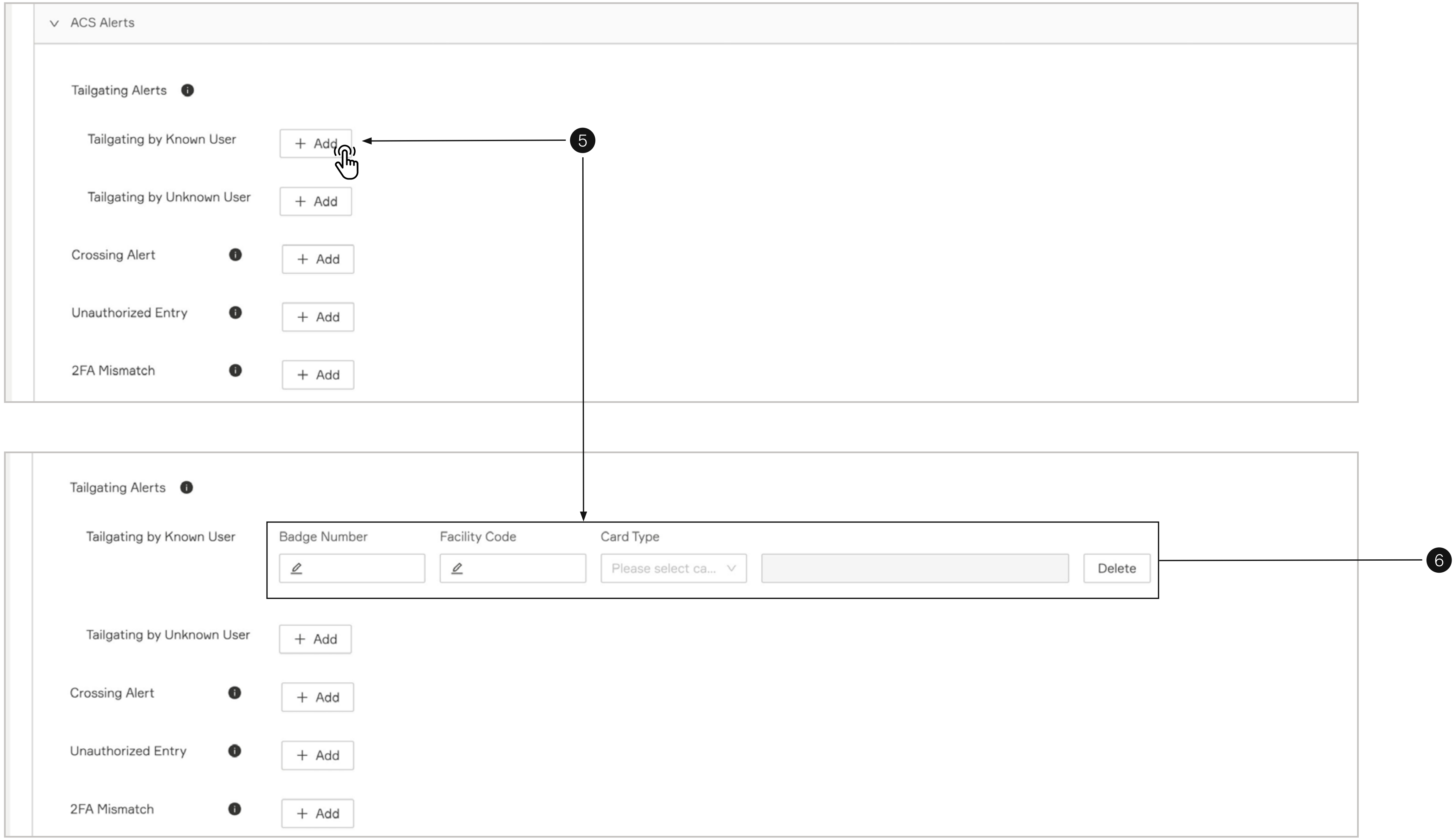
Firmware Update | Modify | Delete

Device configuration

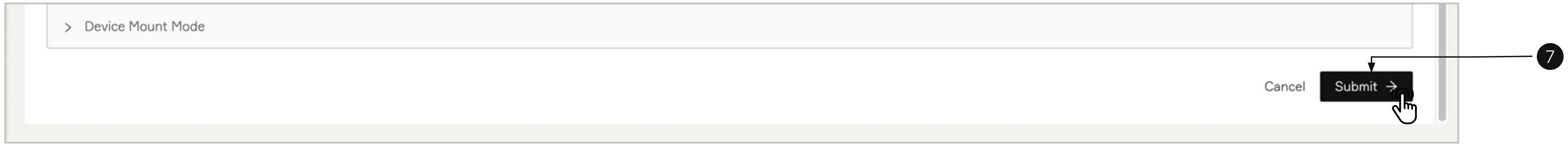
Advanced ○

- Device Mode
- Temporary Enrollment
- Device Setup
- LED Control
- ONVIF
- Hold Signal Detection
- ACS Alerts
- Communication with ACS
- Communication with Badge reader
- Device Mount Mode

5. Click on **+Add** button to set a preferred alert.
6. Enter the information for the alerts (use table from Step 1).



7. Scroll down and Click **Submit** when done.



*The badge numbers should be not associated with any cardholders and are used only for the purpose of receiving alerts from the Rock

Important: If the Card Format assigned to an event is modified, you must delete and re-enter.

Step 4 – Test Alert Appears in ACS

Trigger any configured alert event and verify that the event shows up in the ACS.

For example, to test a tailgating alert, try the following with 2 people.

1. Enrolled user authenticates at the door
2. Second person follows them through the door within 5 seconds
3. Check for the tailgating event in the Alcatraz AI Admin Portal under Device Management –> **Security Events**
4. Verify the event appears in the ACS event log

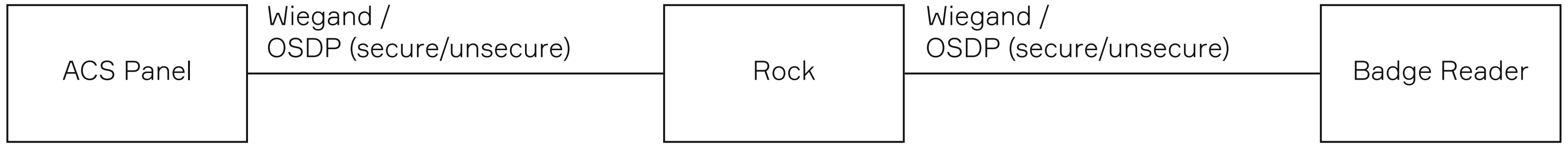
Important: if the tailgating event is not seen in the Alcatraz AI Admin Portal, the ACS will not receive an alert.

6.2.8—Configure OSDP

The Rock supports independent communication interfaces for the Badge Reader and the ACS Panel.
It is possible to set one to Wiegand and the other to OSDP, or one to OSDP secure channel and the other to OSDP unsecure channel.

Pre-requirements:

1. Rock is installed and powered up (refer to Install Guide)
2. Access to the ACS Panel (for OSDP setup between ACS Panel and Rock)
3. Access to the Badge Reader (for OSDP setup between Rock and Badge Reader)
4. Access to the Alcatraz AI Admin Portal (request login credentials)



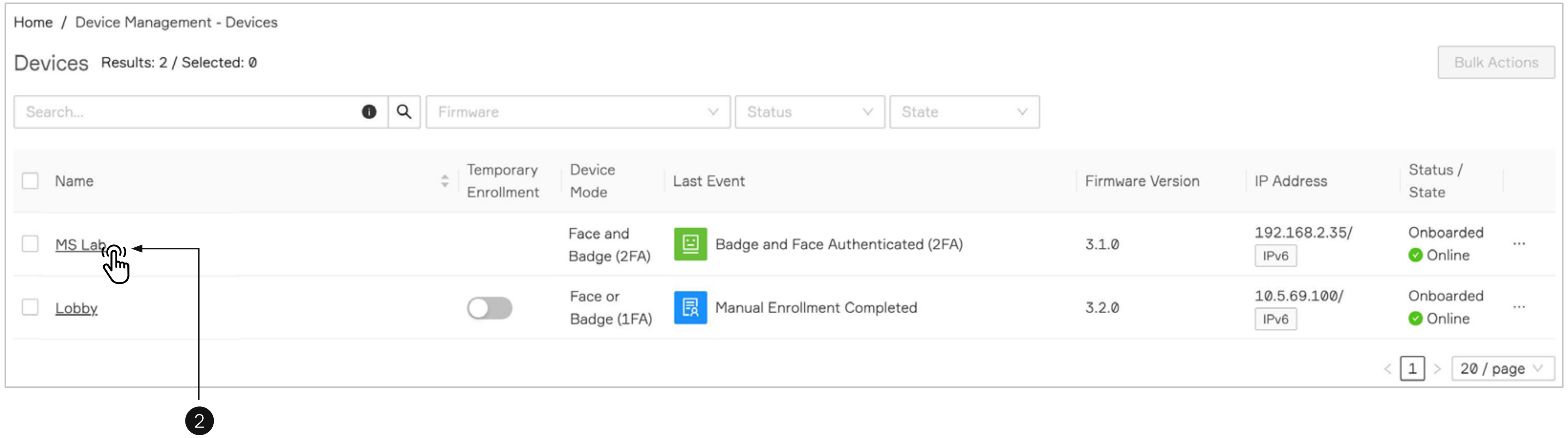
Required from ACS Panel to configure OSDP:
Device address = [range 0 - 126]
Baud rate = 57600 (example)
Enable secure/install mode - for OSDP secure channel ONLY
*enabling OSDP will vary with ACS panels

Required from Badge Reader to configure OSDP:
Device address = [range 0 - 126]
Baud rate = 57600 (example)
Enable secure/install mode - for OSDP secure channel ONLY
*enabling OSDP will vary with Badge Readers

alcatraz ai
Dashboard
Account
Permissions
Device Management
Devices
Updates
QR Code
Security Events
Profiles

6.2.8.1—Select Rock to Configure OSDP

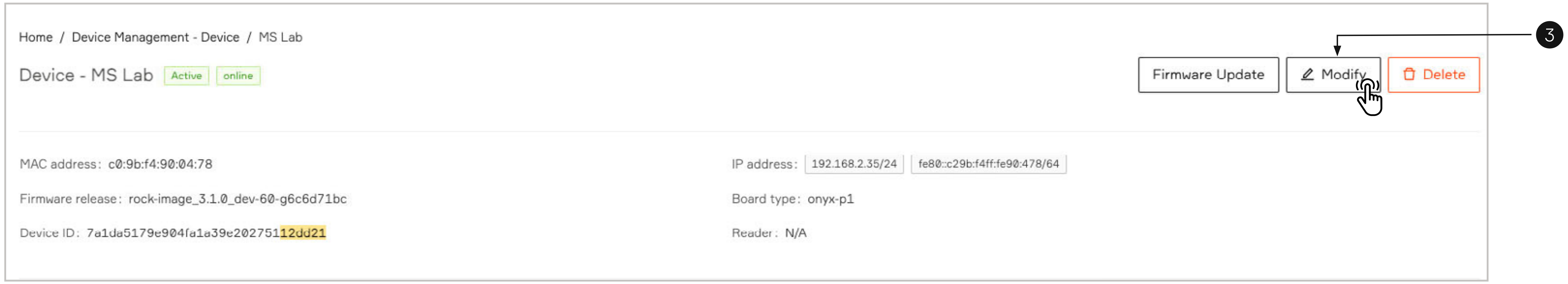
1. Go to **Device Management** and select **Devices**.
2. Click on the Name of the Rock to open the Rock's info page.
3. Click on **Modify** to open up the configurations page.



Home / Device Management - Devices

Devices Results: 2 / Selected: 0

	Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State	
□	MS Lab		Face and Badge (2FA)	Badge and Face Authenticated (2FA)	3.1.0	192.168.2.35/ IPv6	Onboarded ● Online	...
□	Lobby	○	Face or Badge (1FA)	Manual Enrollment Completed	3.2.0	10.5.69.100/ IPv6	Onboarded ● Online	...



Home / Device Management - Device / MS Lab

Device - MS Lab Active online

MAC address: c0:9b:f4:90:04:78

IP address: 192.168.2.35/24 fe80::c29b:f4ff:fe90:478/64

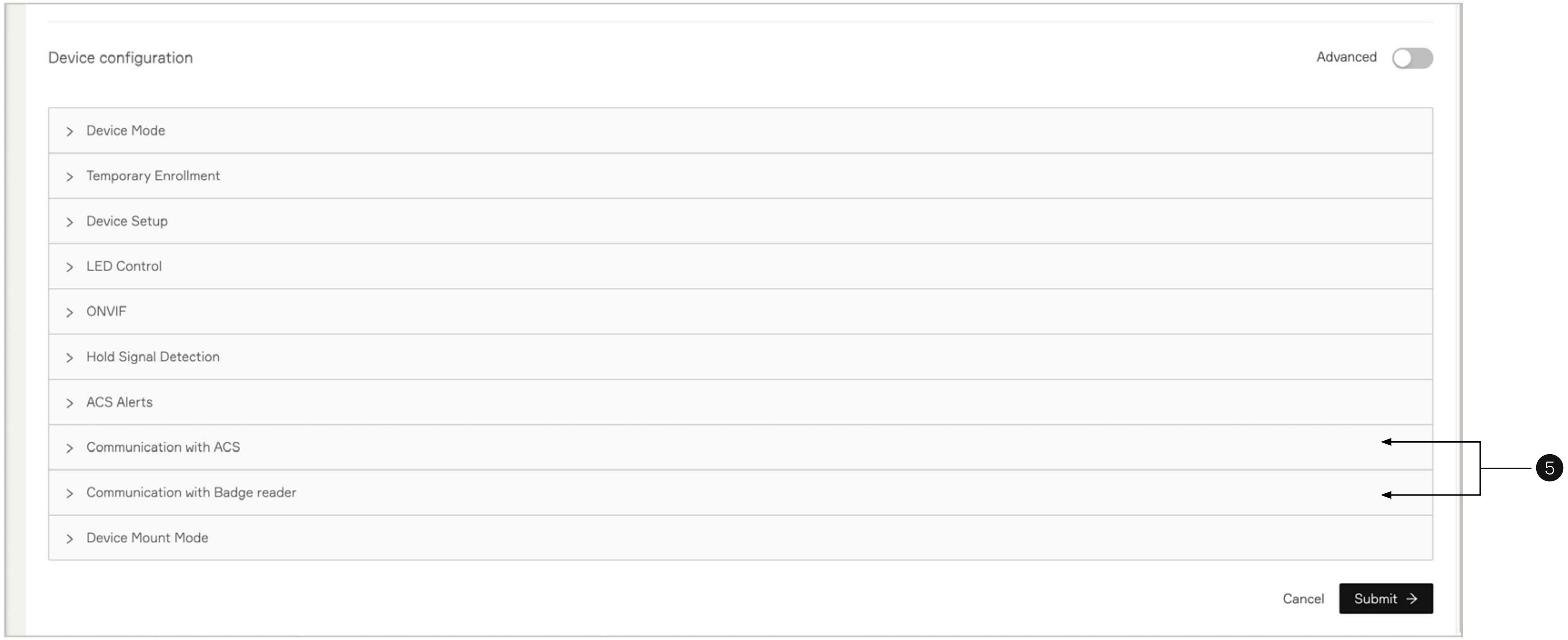
Firmware release: rock-image_3.1.0_dev-60-g6c6d71bc

Board type: onyx-p1

Device ID: 7a1da5179e904fa1a39e20275112dd21

Reader: N/A

4. Scroll down the page to **Device Configuration**.
5. Expand either of the following to configure.
   A. Communication with Badge reader
   B. Communication with ACS

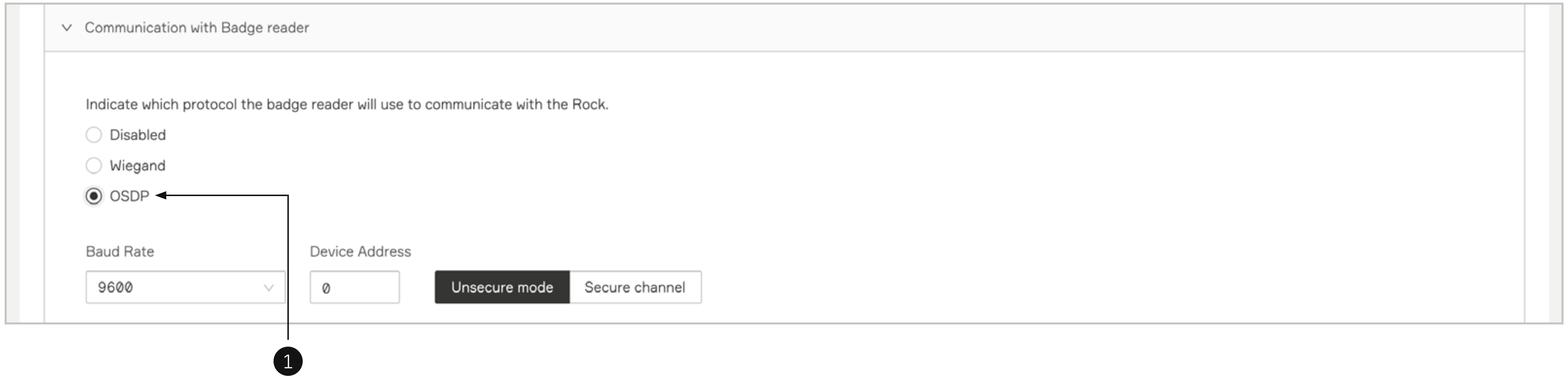


Device configuration

Advanced

6.2.8.2—Rock Communication with Badge Reader

1. Select **OSDP**
2. Enter the Badge Reader's
   a. Baud Rate
   b. Device Address
   c. Select **Unsecure** or **Secure** OSDP channel mode
   d. If selecting Secure channel, confirm to proceed with setup

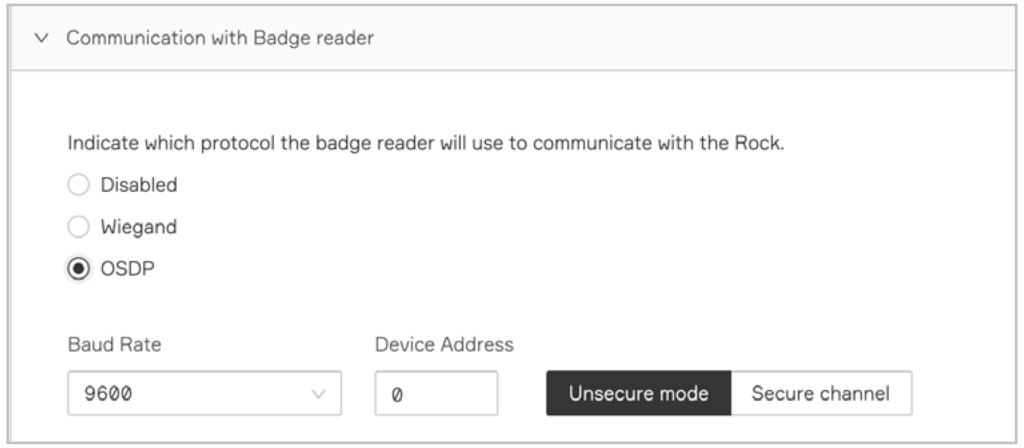


Indicate which protocol the badge reader will use to communicate with the Rock.

○ Disabled
○ Wiegand
● OSDP

Baud Rate: 9600
Device Address: 0

Unsecure mode

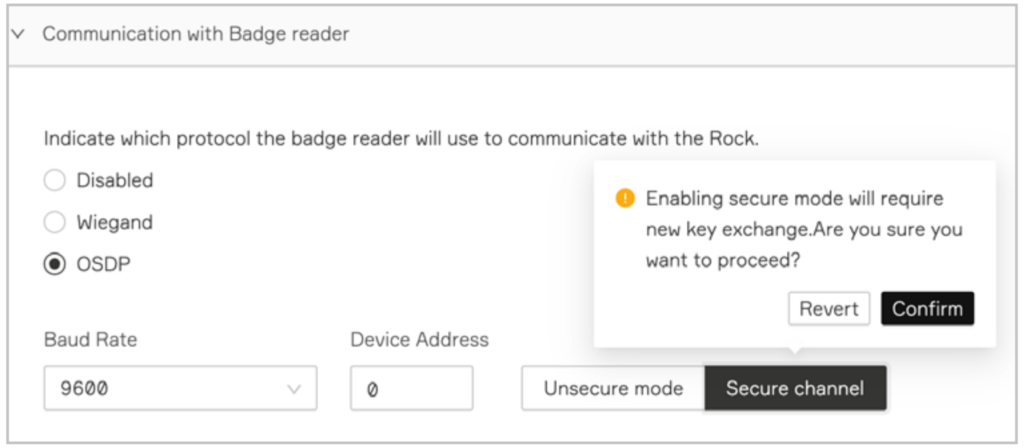


Indicate which protocol the badge reader will use to communicate with the Rock.

○ Disabled
○ Wiegand
● OSDP

Baud Rate: 9600
Device Address: 0

Secure mode



Indicate which protocol the badge reader will use to communicate with the Rock.

○ Disabled
○ Wiegand
● OSDP

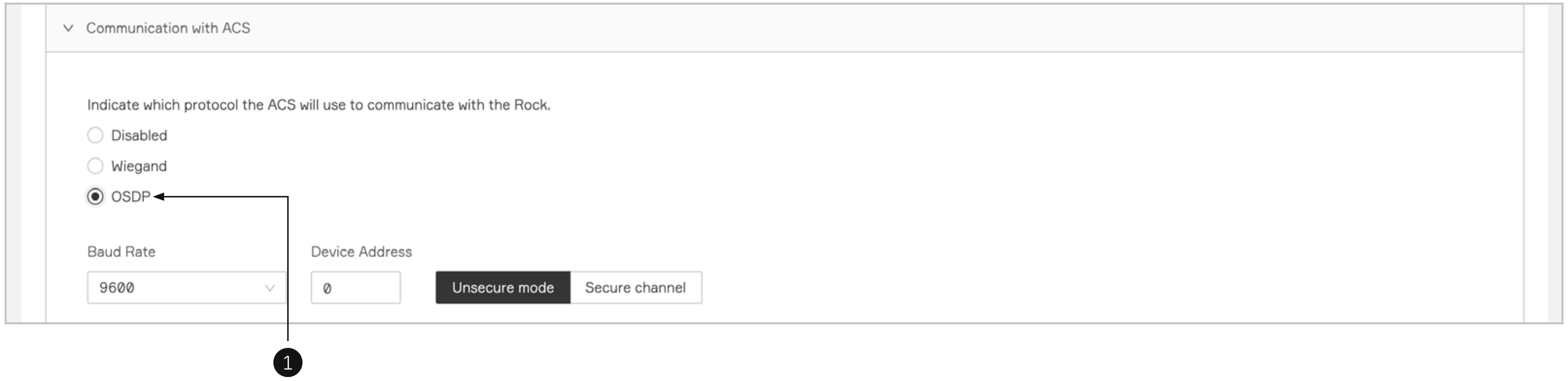
Enabling secure mode will require new key exchange.Are you sure you want to proceed?

Baud Rate: 9600
Device Address: 0

3. Click **Submit**

6.2.8.3—Rock Communication with ACS

1. Select **OSDP**
2. Enter the ACS'
   a. Baud Rate
   b. Device Address
   c. Select **Unsecure** or **Secure** OSDP channel mode
   d. If selecting Secure channel, confirm to proceed with setup



Communication with ACS

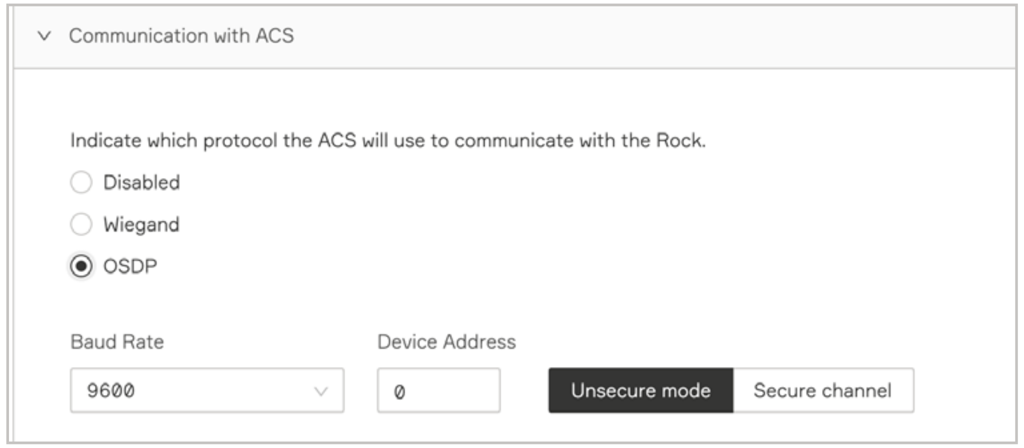
Indicate which protocol the ACS will use to communicate with the Rock.

○ Disabled
○ Wiegand
● OSDP

Baud Rate: 9600

Device Address: 0

Unsecure mode



Communication with ACS

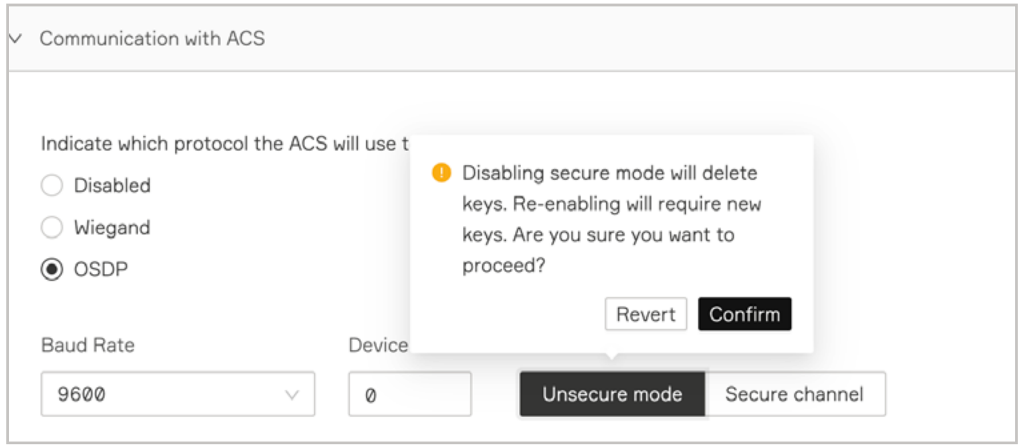
Indicate which protocol the ACS will use to communicate with the Rock.

○ Disabled
○ Wiegand
● OSDP

Baud Rate: 9600

Device Address: 0

Secure mode



Communication with ACS

Indicate which protocol the ACS will use t

○ Disabled
○ Wiegand
● OSDP

Disabling secure mode will delete keys. Re-enabling will require new keys. Are you sure you want to proceed?

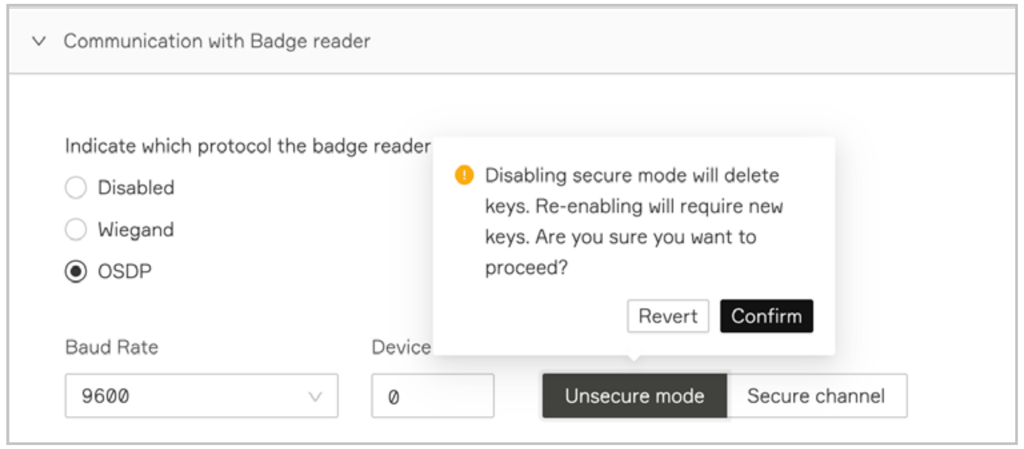
Baud Rate: 9600

Device: 0

3. Click **Submit**

6.2.8.4—Changing from Secure to Unsecure Channel

OSDP requires the exchange of encryption keys. To change from secure channel to unsecure channel, the keys will be deleted. Confirm to continue when changing to Unsecure mode.



Communication with Badge reader

Indicate which protocol the badge reader

○ Disabled

○ Wiegand

● OSDP

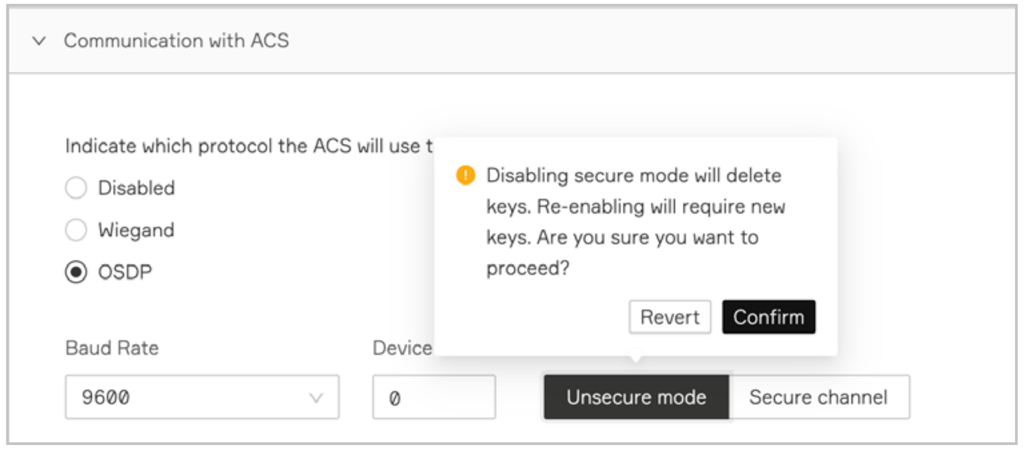
Disabling secure mode will delete keys. Re-enabling will require new keys. Are you sure you want to proceed?

Revert Confirm

Baud Rate: 9600

Device: 0

Unsecure mode | Secure channel



Communication with ACS

Indicate which protocol the ACS will use t

○ Disabled

○ Wiegand

● OSDP

Disabling secure mode will delete keys. Re-enabling will require new keys. Are you sure you want to proceed?

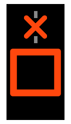
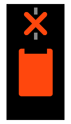
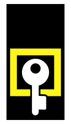
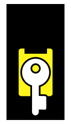
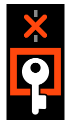
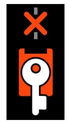
Revert Confirm

Baud Rate: 9600

Device: 0

Unsecure mode | Secure channel

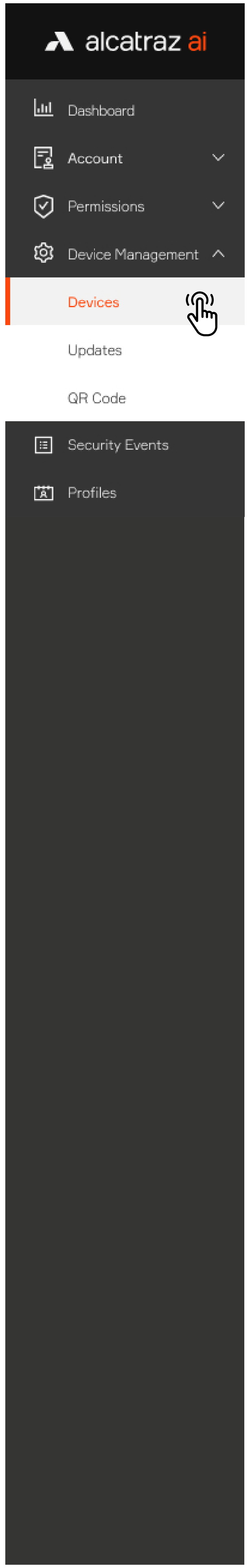
6.2.8.5—Troubleshooting Tips

Troubleshooting			
OLED		Issue	Action
Rock <–> ACS Panel	Rock <–> Badge Reader		
		No communications between Rock device and ACS Panel or Badge Reader	Check: ■ Address/baud rate for mismatch ■ Address/baud rate is valid ■ Bad connections ■ Devices are powered on
		Rock device is in Install mode, but secure link has not been established with the ACS Panel or Badge Reader *Applicable to OSDPv2 only.	Check: ■ OSDP install mode is enabled on ACS/Badge Reader ■ OSDP secure channel is supported by ACS/Badge Reader
		Rock device is in Install mode, but no communications with the ACS Panel or Badge Reader. *Applicable to OSDPv2 only.	Check: ■ Address/baud rate for mismatch ■ Address/baud rate is valid ■ Bad connections ■ Devices are powered on ■ OSDP install mode is enabled on ACS/Badge Reader ■ OSDP secure channel is supported by ACS/Badge Reader

6.2.8.6—Wiring Details

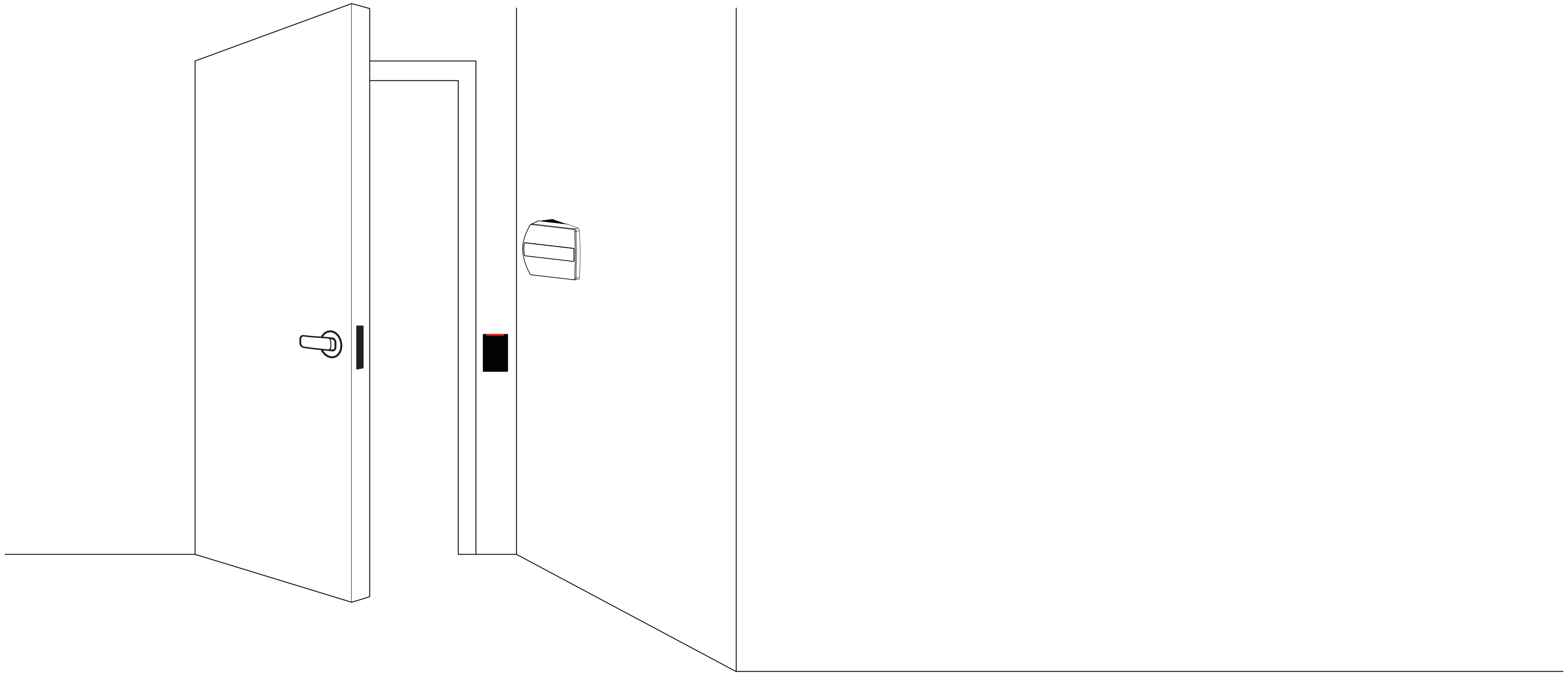
Rock <–> Reader (OSDP)		
Reader Type	Rock Green Wire	Rock White Wire
HID (Legacy)	GPIO1 (Red/Green)	GPIO2 (Tan)
HID Signo	485-A (White)	485-B (Green)
Farpoint OSDP	Green	White
WaveLynx OSDP	RS 485A (Green)	RS 485B (White)

Rock <–> Panel (OSDP)		
Panel Type	Rock Green Wire	Rock White Wire
Mercury	CLK/D1	DAT/D0
iStar IUltra	D+	D-
AMAG SR	Rx+	Rx-

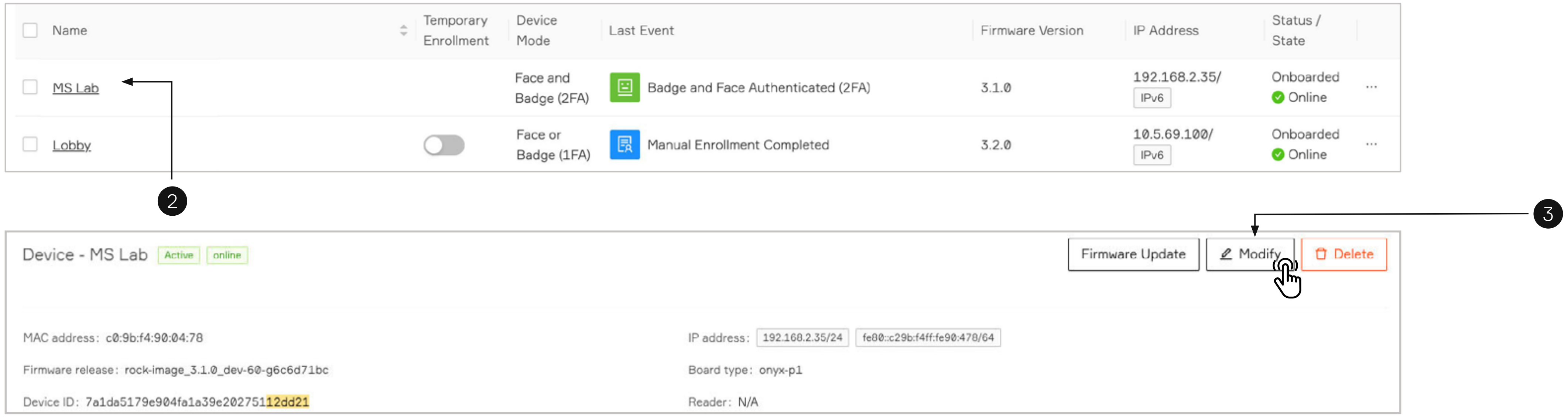


6.2.9—Device Mount Mode

Corridor Mode is required for installations on where the Rock is mounted on walls that are right angle to the door.



1. Go to **Device Management —> Devices**
2. Click on the Name of the Rock to open the Rock's info page.
3. Click on **Modify** to open up the configurations page.



☐	Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State	
☐	MS Lab		Face and Badge (2FA)	Badge and Face Authenticated (2FA)	3.1.0	192.168.2.35/ IPv6	Onboarded ✓ Online	...
☐	Lobby	○	Face or Badge (1FA)	Manual Enrollment Completed	3.2.0	10.5.69.100/ IPv6	Onboarded ✓ Online	...

Device - MS Lab Active online

MAC address: c0:9b:f4:90:04:78

Firmware release: rock-image_3.1.0_dev-60-g6c6d71bc

Device ID: 7a1da5179e904fa1a39e20275112dd21

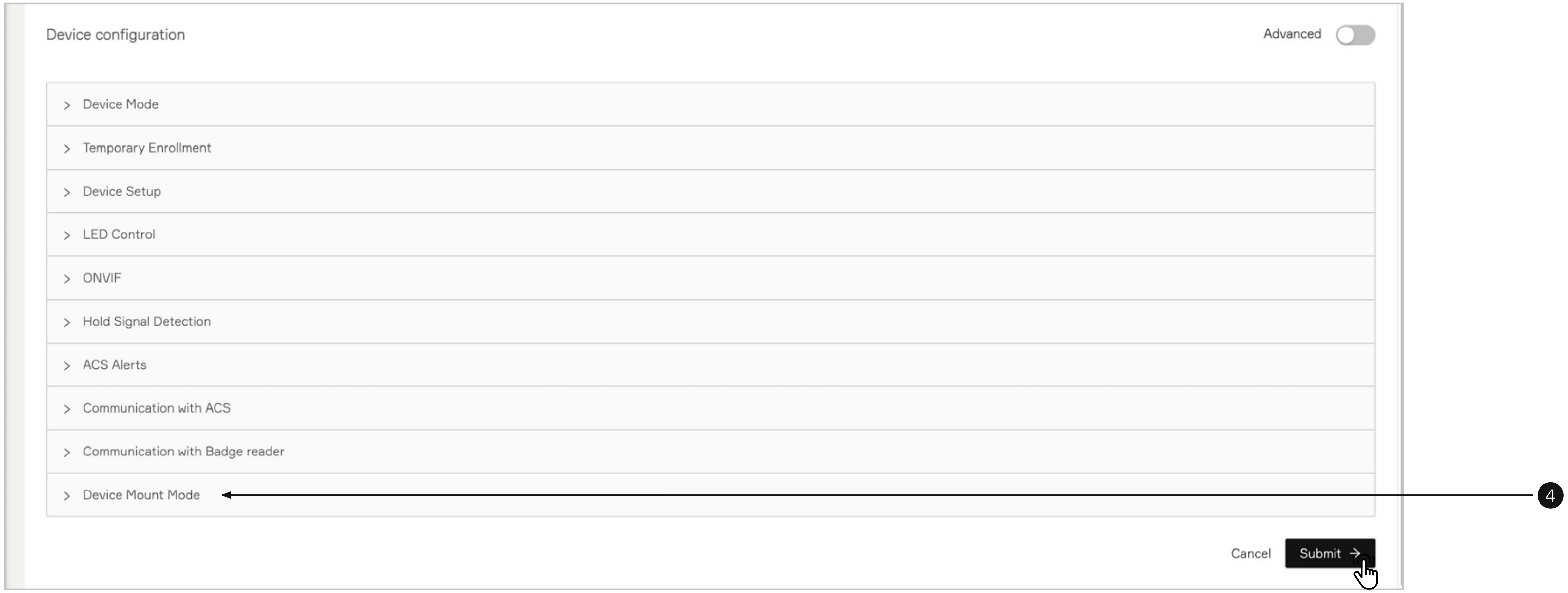
IP address: 192.168.2.35/24 fe80::c29b:f4ff:fe90:470/64

Board type: onyx-p1

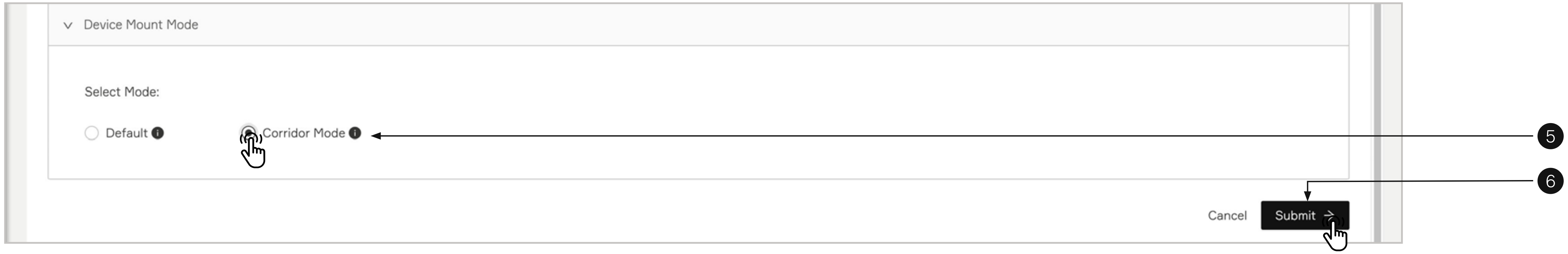
Reader: N/A

alcatraz ai
Dashboard
Account
Permissions
Device Management
Devices
Updates
QR Code
Security Events
Profiles

1. Go to **Device Management —> Devices**



2. Click on the Name of the Rock to open the Rock's info page.
3. Click on **Modify** to open up the configurations page.
4. Scroll down the page to **Device Mount Mode**.
5. Click on the **Corridor Mode** option.
6. Click **Submit** when done.


Device Mount Mode

Select Mode:

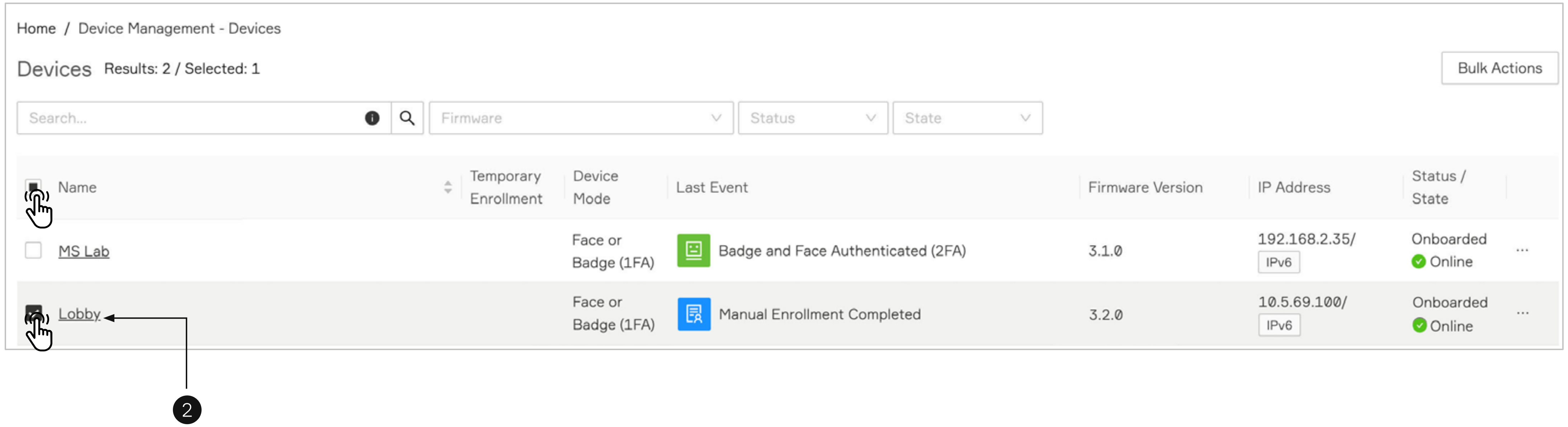
○ Default ● Corridor Mode

alcatraz ai
Dashboard
Account
Permissions
Device Management
Devices
Updates
QR Code
Security Events
Profiles

6.3—Devices Bulk Operation

The device bulk operation allows managing and configuring of multiple devices.

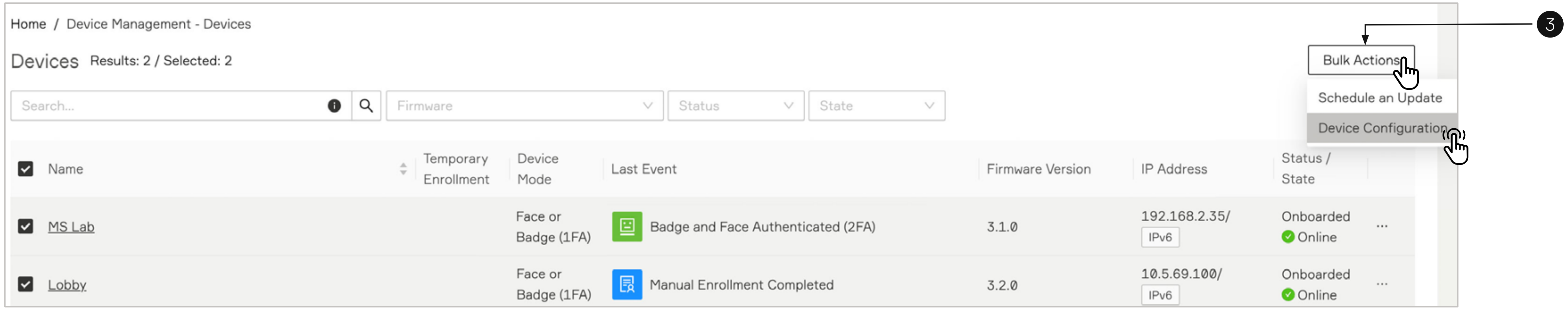
1. Go to **Device Management** and select **Devices**.
2. Click the checkbox of the rock's name to select it. Continue to select devices. Each time when selecting a device the number of **Selected** value increases which confirms that rock was added to the selection.
   To select all of the devices on the page click the checkbox bext to Name title of the table (optional).
3. Hover over **Bulk Actions** and select **Device Configuration** to open up the configurations page.



Home / Device Management - Devices

Devices Results: 2 / Selected: 1

☐ Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State	
☐ MS Lab		Face or Badge (1FA)	Badge and Face Authenticated (2FA)	3.1.0	192.168.2.35/ IPv6	Onboarded ✓ Online	...
☑ Lobby		Face or Badge (1FA)	Manual Enrollment Completed	3.2.0	10.5.69.100/ IPv6	Onboarded ✓ Online	...

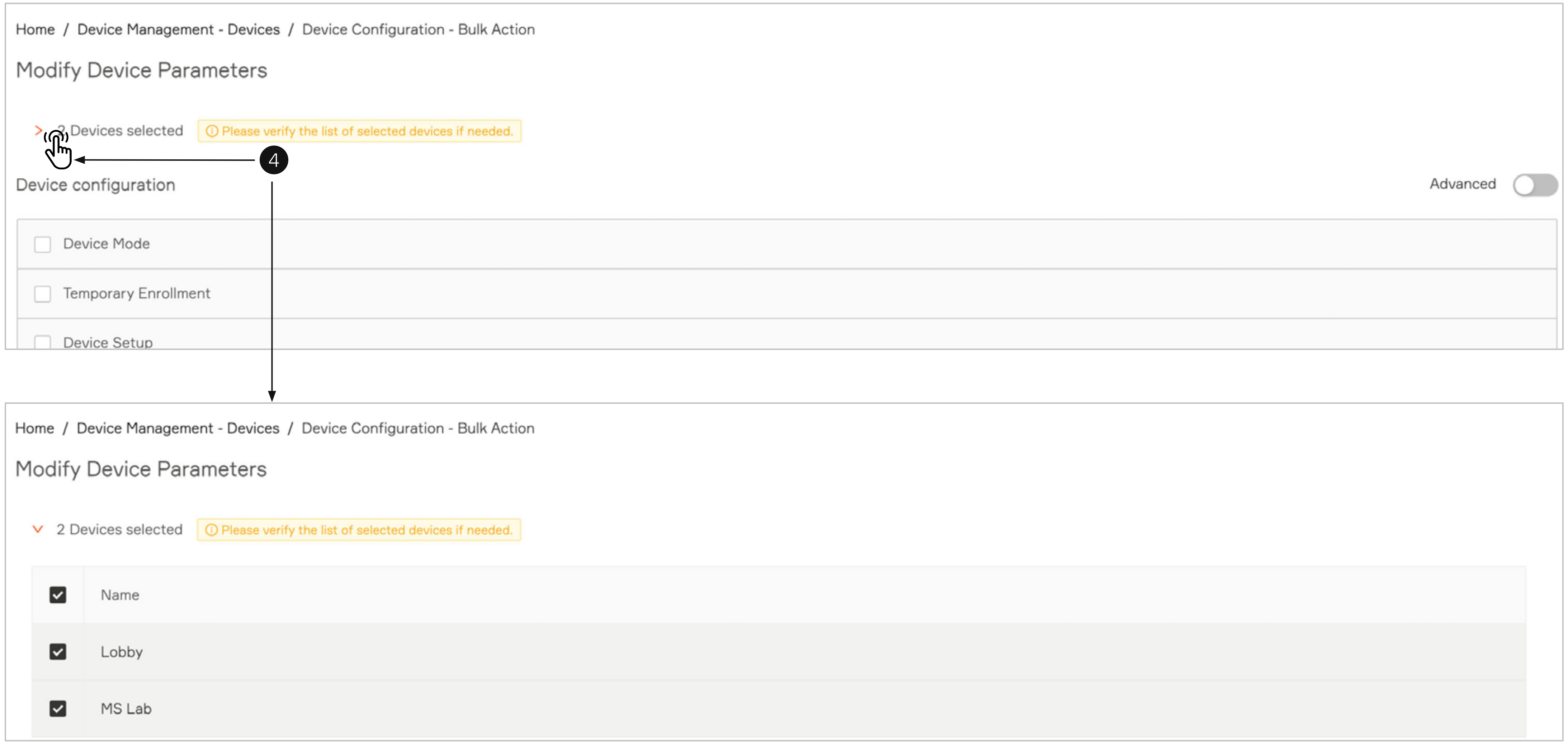


Home / Device Management - Devices

Devices Results: 2 / Selected: 2

☑ Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State	
☑ MS Lab		Face or Badge (1FA)	Badge and Face Authenticated (2FA)	3.1.0	192.168.2.35/ IPv6	Onboarded ✓ Online	...
☑ Lobby		Face or Badge (1FA)	Manual Enrollment Completed	3.2.0	10.5.69.100/ IPv6	Onboarded ✓ Online	...

4. **Modify Device Parameters** page will display, containing number of the selected devices. Clicking on the arrow will open the list of the selected devices.
The device list allows also deselecting some of the devices. The device configuration changes will not apply the unselected ones.



Home / Device Management - Devices / Device Configuration - Bulk Action

Modify Device Parameters

2 Devices selected ⓘ Please verify the list of selected devices if needed.

Device configuration

Advanced ○

□ Device Mode

□ Temporary Enrollment

□ Device Setup

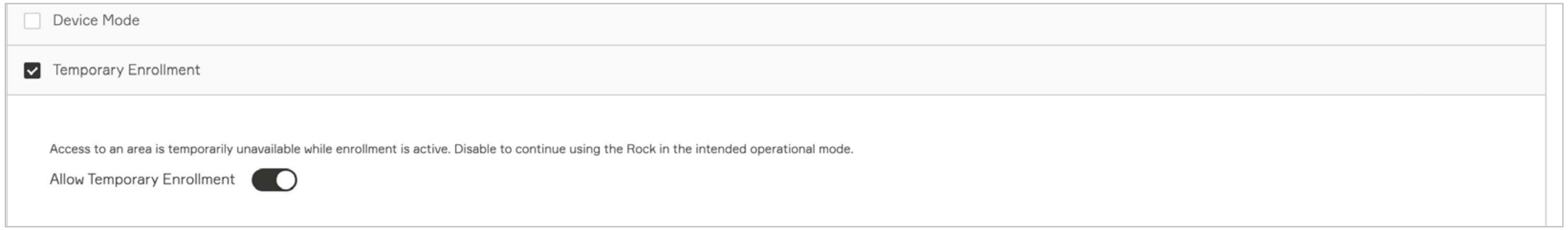
Home / Device Management - Devices / Device Configuration - Bulk Action

Modify Device Parameters

2 Devices selected ⓘ Please verify the list of selected devices if needed.

☑	Name
☑	Lobby
☑	MS Lab

5. Start configuring parameters by opening sections and selecting preferred options.
Each section with changes need to be checkmarked. **The system applies only the changes of the checkmarked modules.**



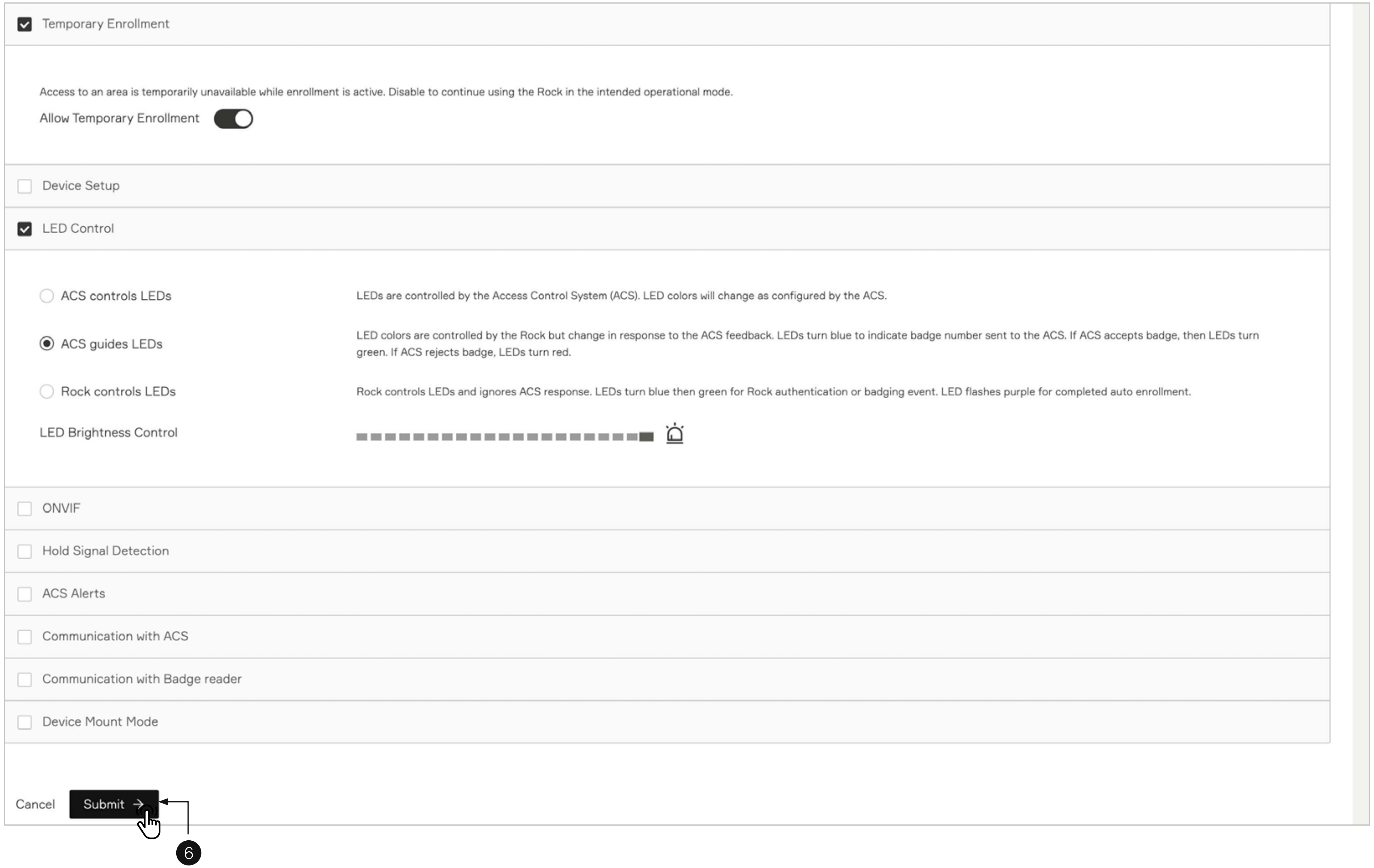
□ Device Mode

☑ Temporary Enrollment

Access to an area is temporarily unavailable while enrollment is active. Disable to continue using the Rock in the intended operational mode.

Allow Temporary Enrollment ●

6. Click **Submit** after configuring all of the changes to apply them.
7. A summary of the configuration will be displayed. Check if the changes match with the selected changes and click **Confirm** to apply the changes.



☑ Temporary Enrollment

Access to an area is temporarily unavailable while enrollment is active. Disable to continue using the Rock in the intended operational mode.

Allow Temporary Enrollment: On

□ Device Setup

☑ LED Control

○ ACS controls LEDs — LEDs are controlled by the Access Control System (ACS). LED colors will change as configured by the ACS.

● ACS guides LEDs — LED colors are controlled by the Rock but change in response to the ACS feedback. LEDs turn blue to indicate badge number sent to the ACS. If ACS accepts badge, then LEDs turn green. If ACS rejects badge, LEDs turn red.

○ Rock controls LEDs — Rock controls LEDs and ignores ACS response. LEDs turn blue then green for Rock authentication or badging event. LED flashes purple for completed auto enrollment.

LED Brightness Control

□ ONVIF

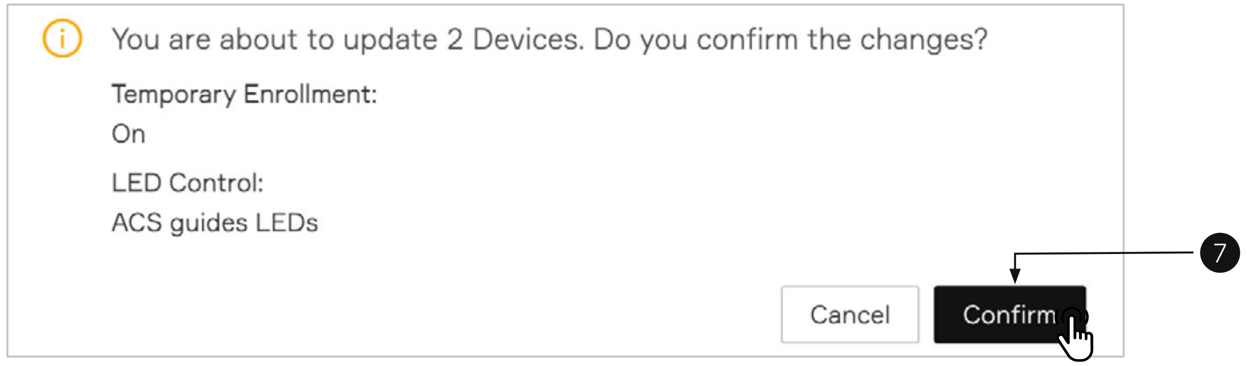
□ Hold Signal Detection

□ ACS Alerts

□ Communication with ACS

□ Communication with Badge reader

□ Device Mount Mode



You are about to update 2 Devices. Do you confirm the changes?

Temporary Enrollment:
On

LED Control:
ACS guides LEDs

alcatraz ai
Dashboard
Account
Permissions
Device Management
Devices
Updates
QR Code
Security Events
Profiles

6.4—Generate QR Code

The Rock can accept an IP address dynamically via DHCP, or be assigned a static IP address.

To configure the network settings of a Rock, we use the Rock like a QR code scanner.

The Admin Portal has a QR Code Generator feature that encodes network settings;

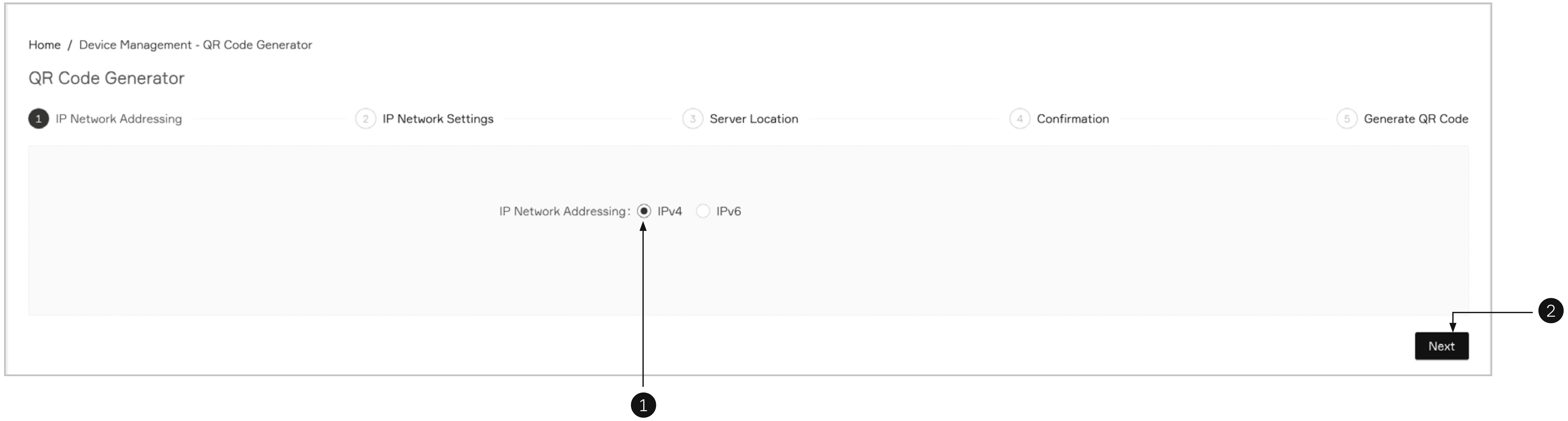
- First enter the network settings
- Next generate the QR code which encodes those settings
- Third print the QR code on a piece of paper (or use your laptop screen)
- Finally present that printed code to the Rock's image sensor

After the Rock detects and reads that QR code, the encoded network settings will take affect.

To edit or update those settings, generate a new QR code.

The Rock can only read in the QR code when it displays the QR Code Receptive icon. ▣
Before taking a Rock offline for network changes, make sure that the icon is turned on.

1. Go to Device Management —> **QR Code**
2. Select **IPv4 Network** and click **Next**. (IPv6 Network is a future release)



Home / Device Management - QR Code Generator

QR Code Generator

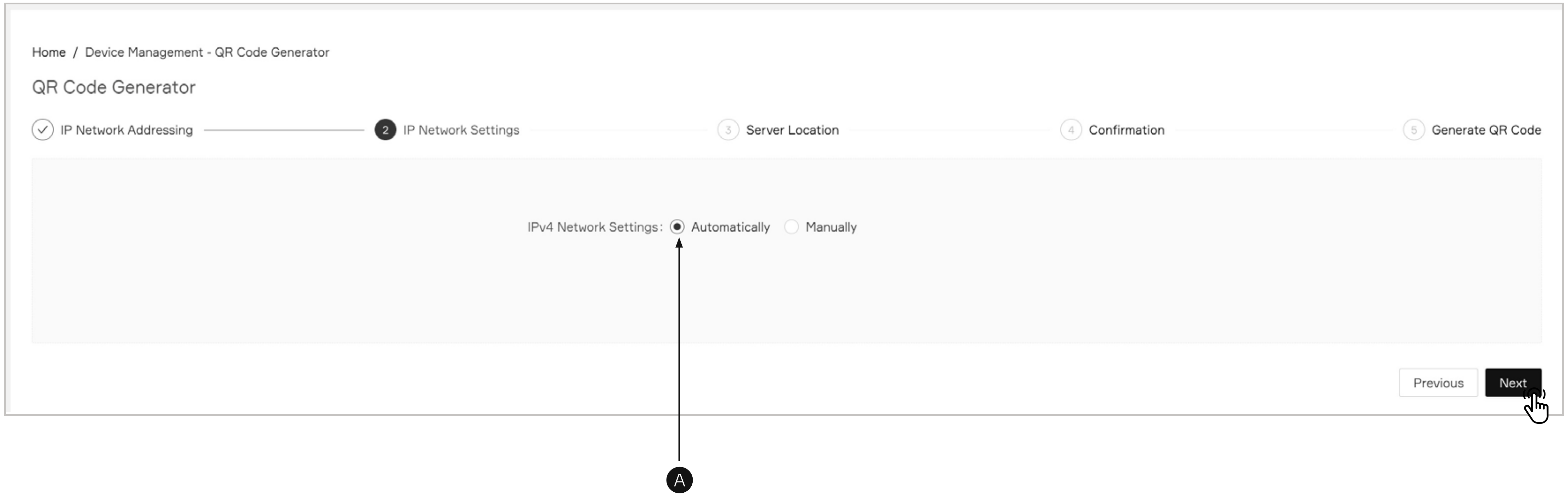
1 IP Network Addressing — 2 IP Network Settings — 3 Server Location — 4 Confirmation — 5 Generate QR Code

IP Network Addressing: ● IPv4 ○ IPv6

alcatraz ai

- Dashboard
- Account
- Permissions
- Device Management
  - Devices
  - Updates
  - QR Code
- Security Events
- Profiles

A. For DHCP - Select **Automatically** if the Rock will acquire an IP address by DHCP, than click **Next**



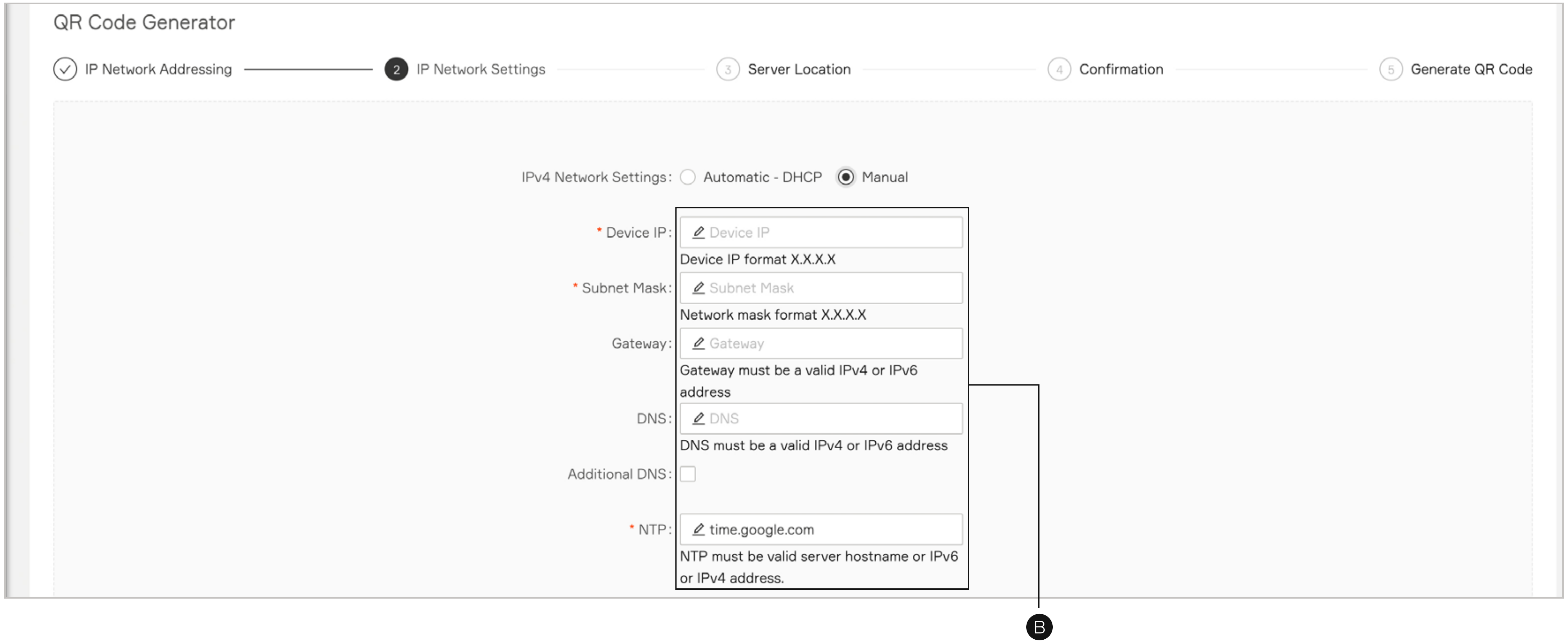
Home / Device Management - QR Code Generator

QR Code Generator

✓ IP Network Addressing — 2 IP Network Settings — 3 Server Location — 4 Confirmation — 5 Generate QR Code

IPv4 Network Settings: ● Automatically ○ Manually

B. For Static IP - select **Manually** and enter the required information, than click **Next** to continue



QR Code Generator

✓ IP Network Addressing — 2 IP Network Settings — 3 Server Location — 4 Confirmation — 5 Generate QR Code

IPv4 Network Settings: ○ Automatic - DHCP ● Manual

* Device IP: Device IP
Device IP format X.X.X.X

* Subnet Mask: Subnet Mask
Network mask format X.X.X.X

Gateway: Gateway
Gateway must be a valid IPv4 or IPv6 address

DNS: DNS
DNS must be a valid IPv4 or IPv6 address

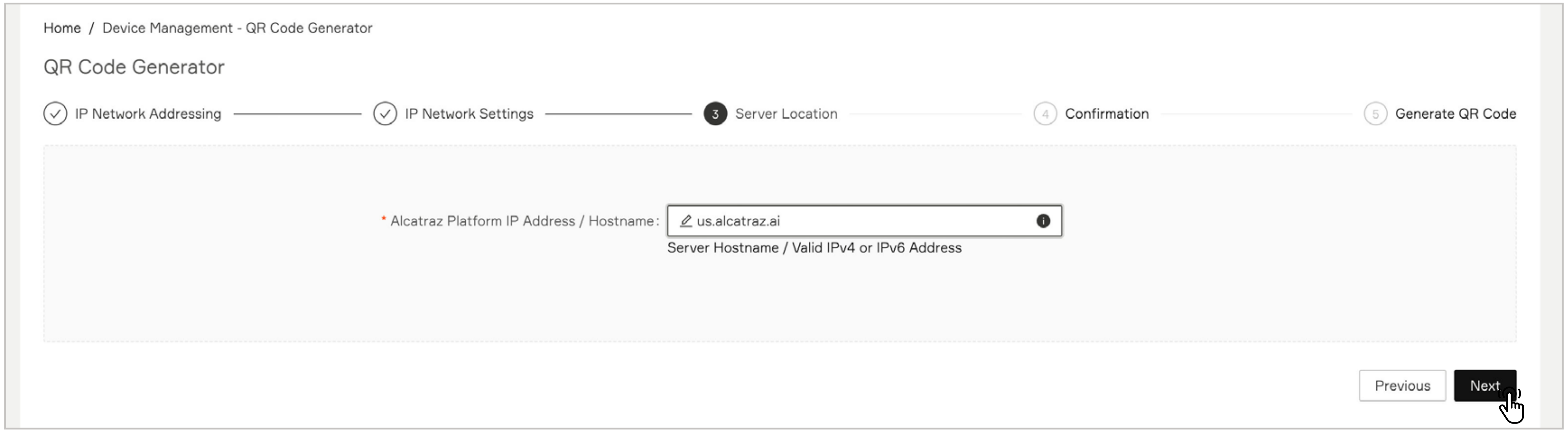
Additional DNS: □

* NTP: time.google.com
NTP must be valid server hostname or IPv6 or IPv4 address.

6.4.1—Server Location

Select a **Server Location** and click **Next**.

1. Demo / Pilot Rocks hosted on Alcatrtaz Cloud should use “us.alcatraz.ai”
2. For Cloud Hosted – use a URL provided by Alcatraz (“<CloudInstance>.alcatraz.ai”).
3. For On-Premise – enter the Server IPv4 or IPv6 Address


Home / Device Management - QR Code Generator

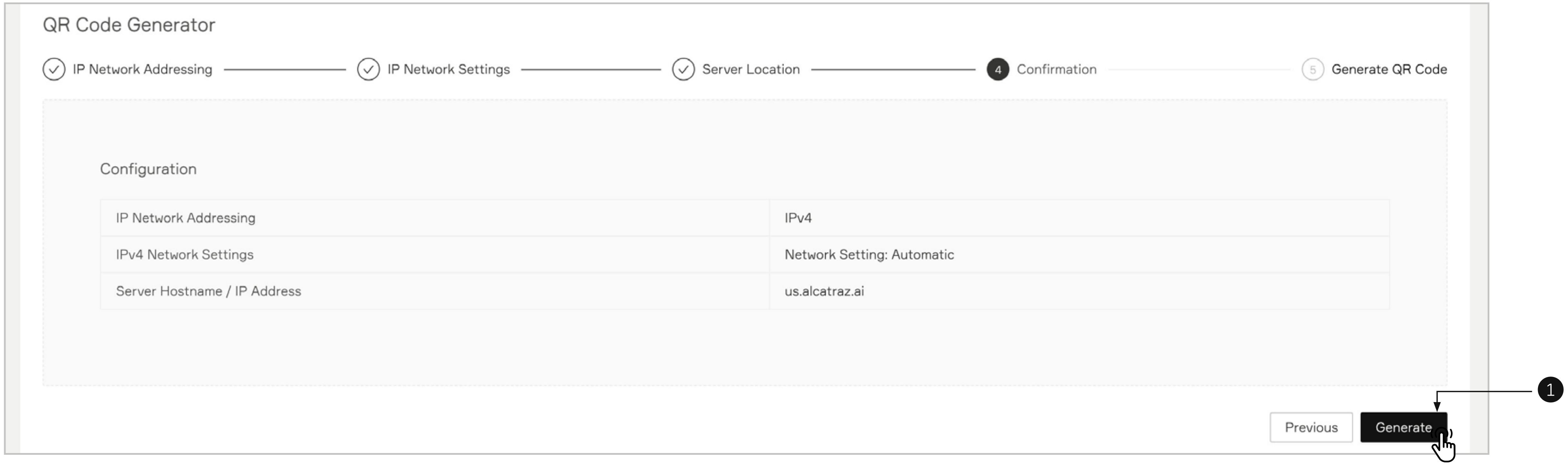
QR Code Generator

* Alcatraz Platform IP Address / Hostname: us.alcatraz.ai

Server Hostname / Valid IPv4 or IPv6 Address

6.4.2—Generate and Download QR Code

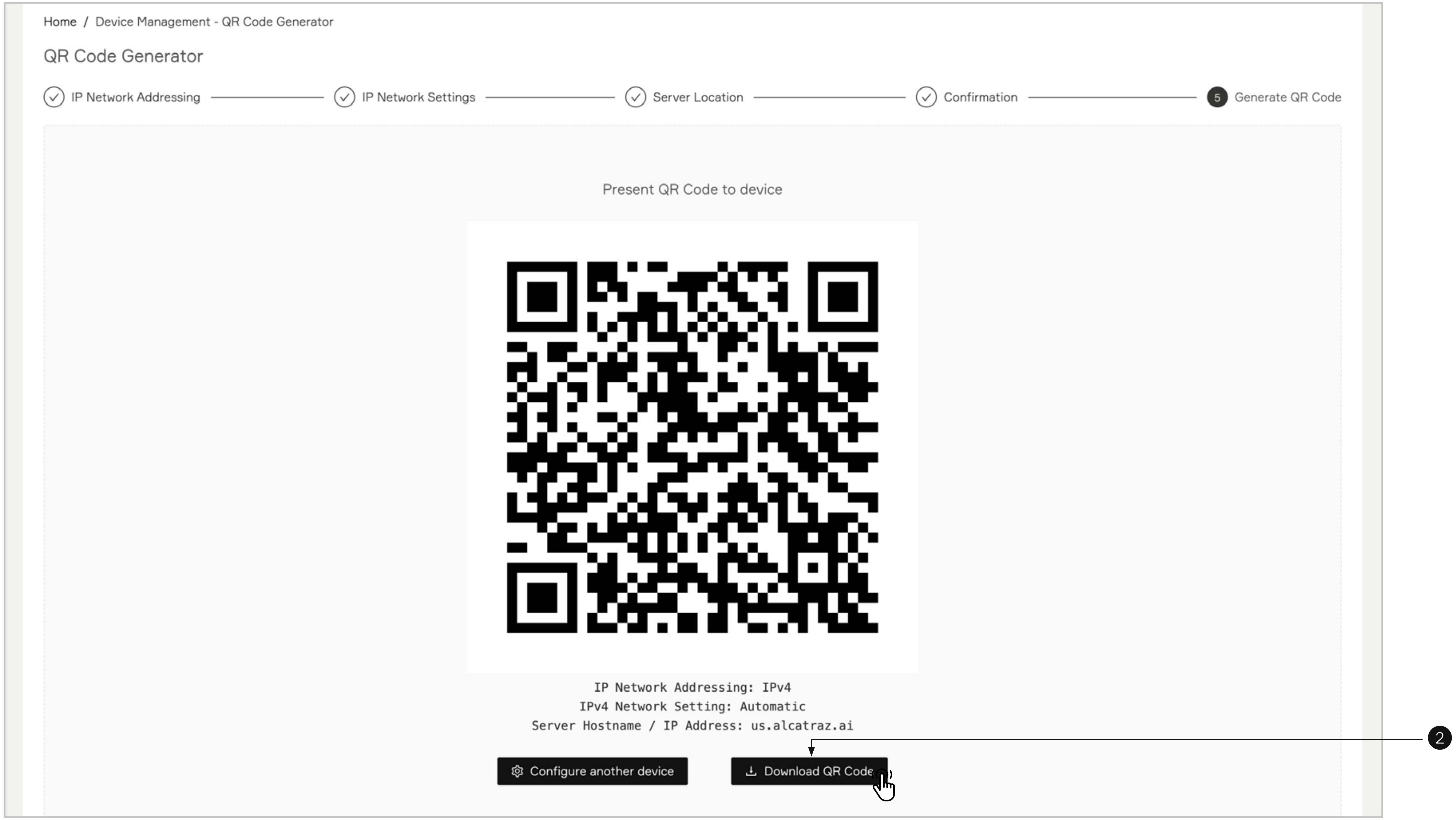
1. Review your settings and then hit **Generate**


QR Code Generator

Configuration

IP Network Addressing	IPv4
IPv4 Network Settings	Network Setting: Automatic
Server Hostname / IP Address	us.alcatraz.ai

1. Review your settings and then hit **Generate**
2. Click **Download QR Code** to save to your computer, email or text.



Home / Device Management - QR Code Generator

QR Code Generator

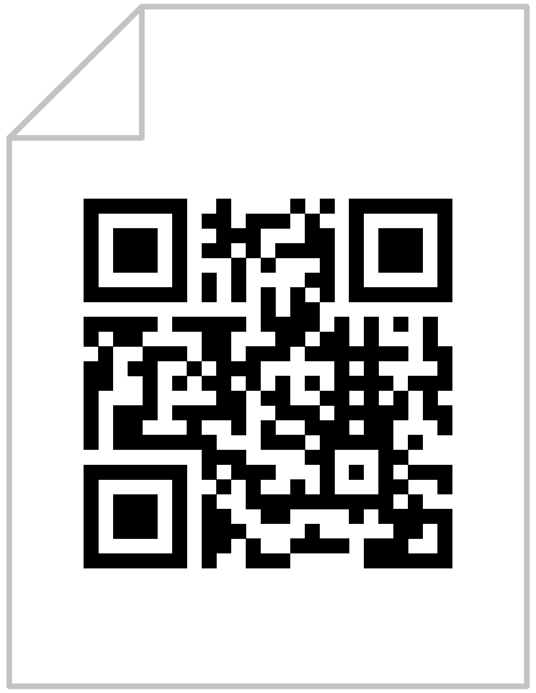
```
IP Network Addressing: IPv4
IPv4 Network Setting: Automatic
Server Hostname / IP Address: us.alcatraz.ai
```

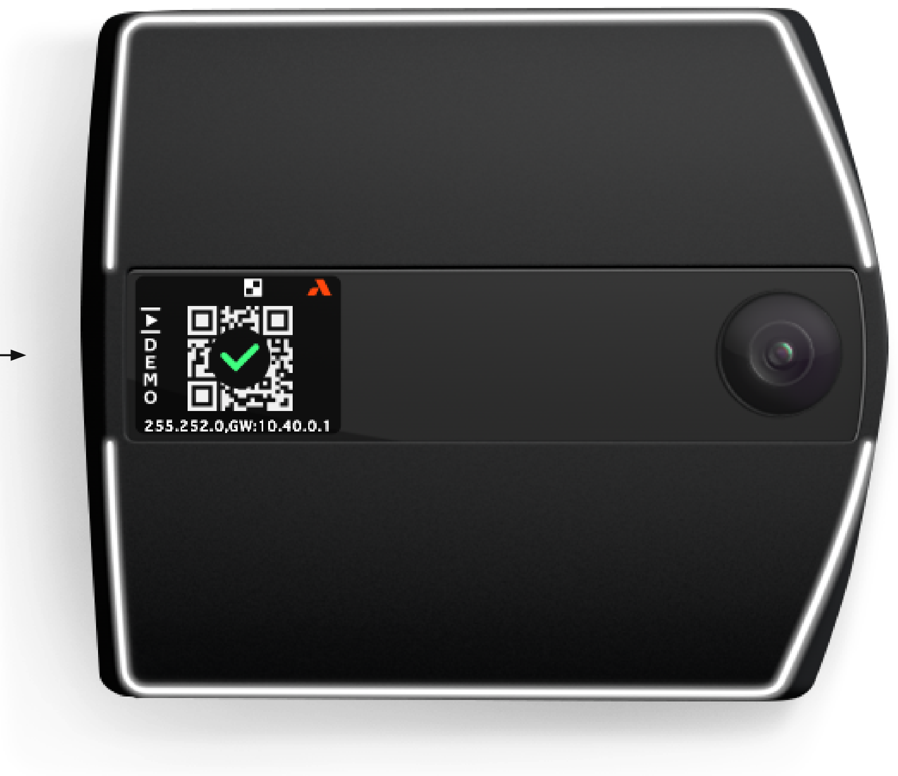
6.4.3—Present QR Code to the Rock's Camera

Present to the Rock by:

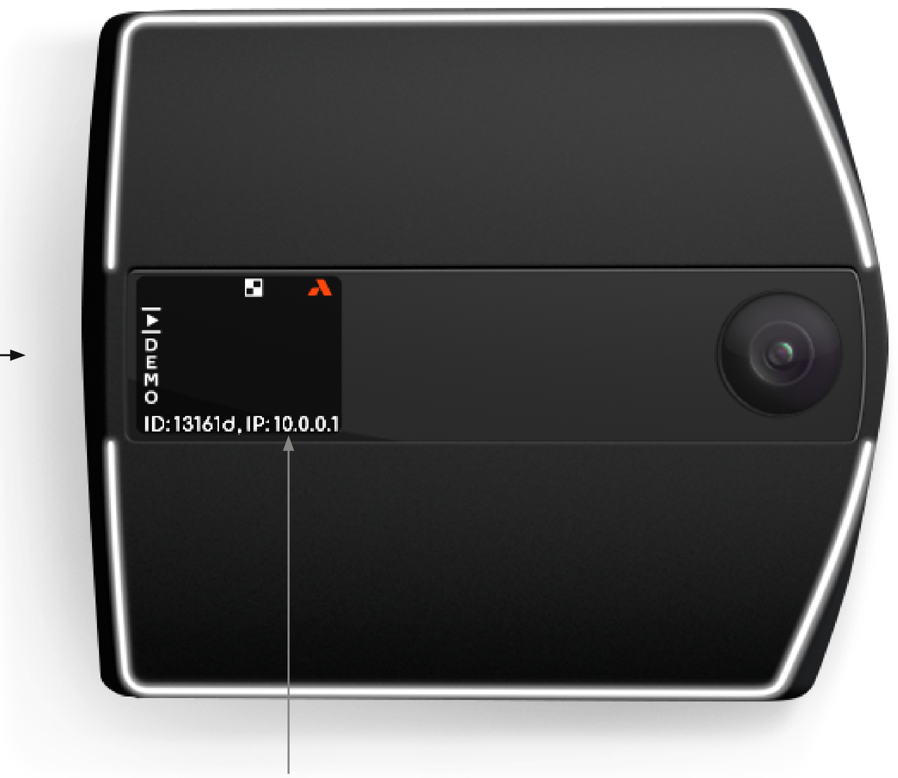
- Printing it out on a piece of paper
- Laptop
- Mobile device

Note: The recommended method is to print out on a piece of paper.
The glare off screens of laptops and mobile devices may prevent the Rock from scanning the code reliably.





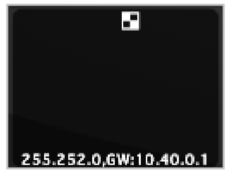
When the Rock has read the QR code successfully, the display will show the QR Config Accepted icon.



Check the IP information scrolling near the bottom of the display and verify that the information is correct for the Rock to connect to the server where the Alcatraz AI Admin Portal resides.

6.4.4—When can the Rock read a QR code?

- A Rock must display the QR Code Receptive icon to be able to scan a QR code. If the icon is not shown on the display, the Rock cannot scan in the QR code.
- To activate QR Code Receptive icon, use the device configuration settings – Device Setup (QR code configuration).



7 —
Security Events

Security Events are displayed in the Alcatraz AI Admin Portal for:

- Enrollment – Manual Enrollment or Auto-enrollment
- Authentication – Single, Two Factor or Three Factor Authentication
- Tailgating Intelligence – Tailgating, Crossing or Unauthorized Entry (by Unknown or Possible Known User)
- Badge–Face Mismatch – Face Unknown or Badge Unknown
- Removing profile/s – Deleted Profiles reporting
- Tamper Detection – Rock Device or Badge Reader Tamper Detecting

When an event occurs at the Rock, the corresponding security event will be displayed in the Alcatraz AI Admin Portal in real time if network connections are healthy.

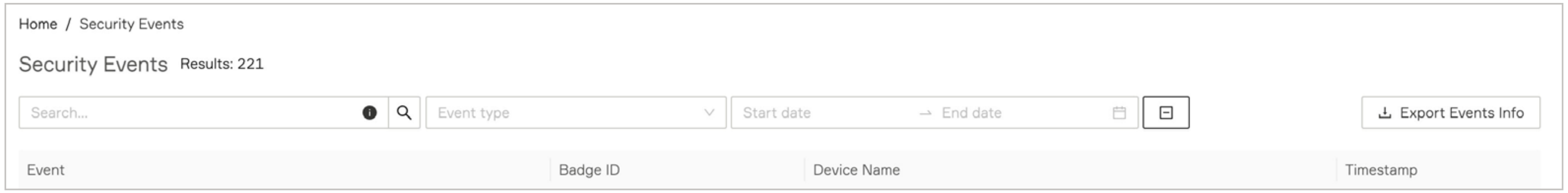
In the case of any network disruptions, events will be queued in the Rock and will sync with the Alcatraz AI Admin Portal when connections are re-established.

The Rock is capable of queuing thousands of events but there will be potential loss of events if the connection is down for a long period of time.

7.1—Managing Security Events

7.1.1—Viewing Security Events

Security events can be viewed by navigating to Device Management –> Security Events.
In addition to the search bar, a number of filters are available by Event type, Account, or Start date and End date.



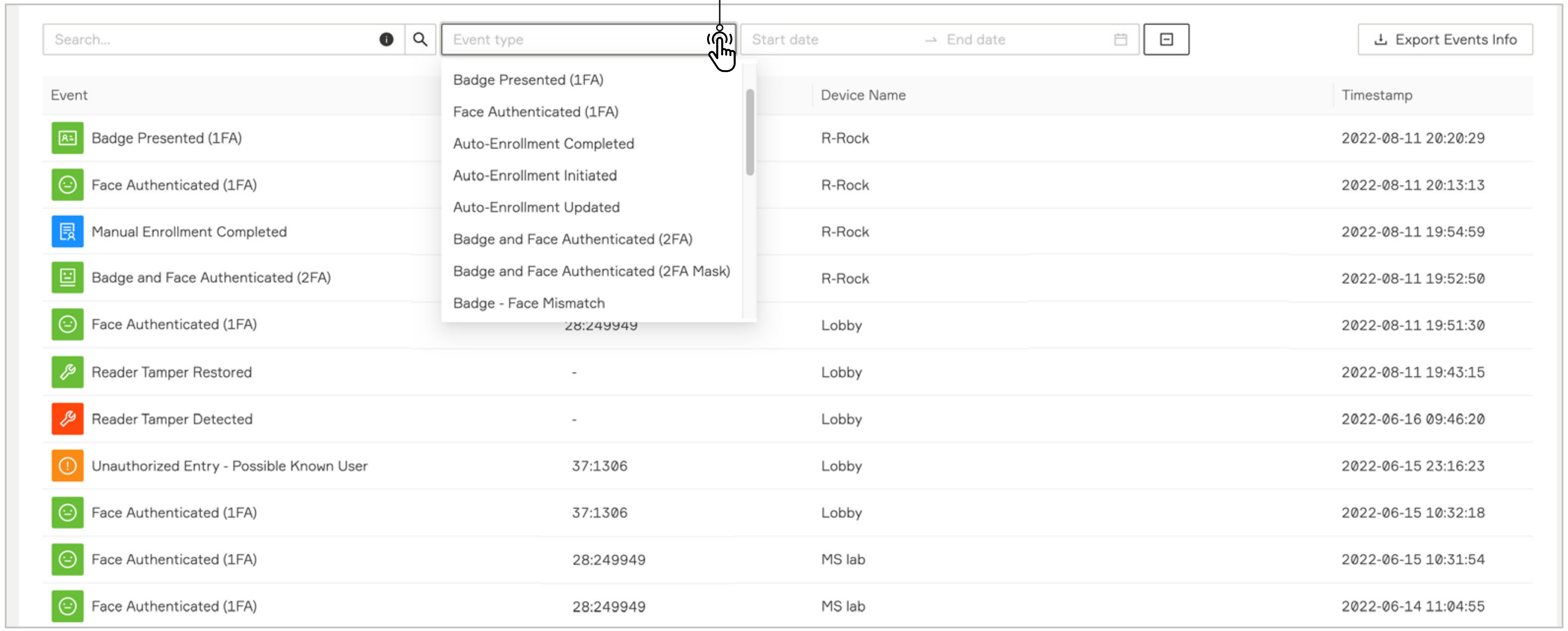
Home / Security Events

Security Events Results: 221

Event	Badge ID	Device Name	Timestamp

This is a sample list of the events.

Events can be filtered using the Event type drop down menu

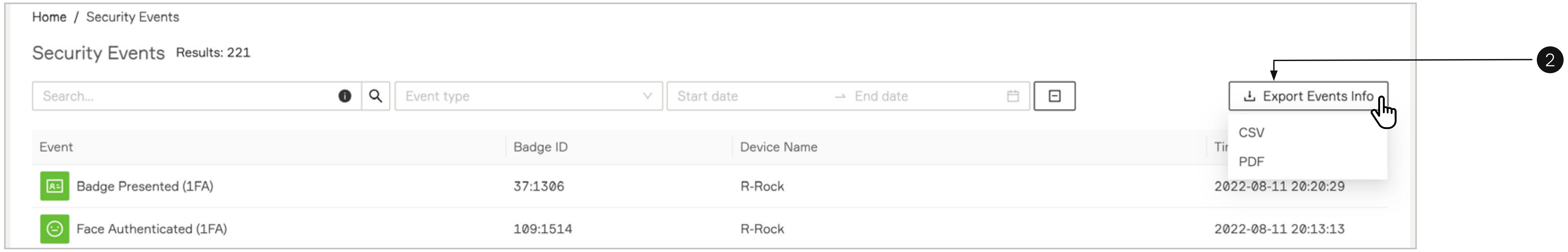


Event		Device Name	Timestamp
Badge Presented (1FA)		R-Rock	2022-08-11 20:20:29
Face Authenticated (1FA)		R-Rock	2022-08-11 20:13:13
Manual Enrollment Completed		R-Rock	2022-08-11 19:54:59
Badge and Face Authenticated (2FA)		R-Rock	2022-08-11 19:52:50
Face Authenticated (1FA)	28:249949	Lobby	2022-08-11 19:51:30
Reader Tamper Restored	-	Lobby	2022-08-11 19:43:15
Reader Tamper Detected	-	Lobby	2022-06-16 09:46:20
Unauthorized Entry - Possible Known User	37:1306	Lobby	2022-06-15 23:16:23
Face Authenticated (1FA)	37:1306	Lobby	2022-06-15 10:32:18
Face Authenticated (1FA)	28:249949	MS lab	2022-06-15 10:31:54
Face Authenticated (1FA)	28:249949	MS lab	2022-06-14 11:04:55

7.1.2—Export Security Events

Users can export and download Security Event records CSV and PDF formats are supported and the exported file will contain all events corresponding to the currently applied filters (if any).

1. Go to **Device Management** —> **Security Events**
■ Apply any preferred filters if needed.
2. Hover on **Export Events Info** button and select the preferred file format.
3. A pop-up with the filtered information will appear. (In case that additional filters need to be applied click **Cancel** and continue filtering the log information.)

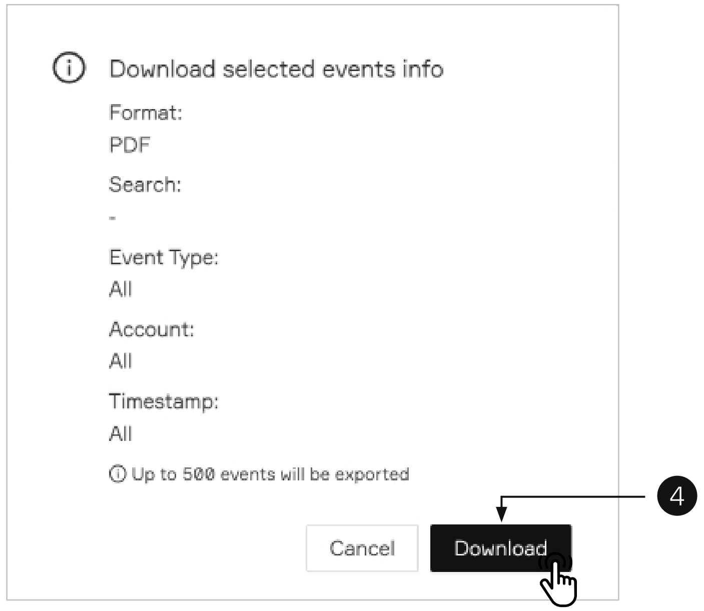


Home / Security Events

Security Events Results: 221

Event	Badge ID	Device Name	Ti
Badge Presented (1FA)	37:1306	R-Rock	2022-08-11 20:20:29
Face Authenticated (1FA)	109:1514	R-Rock	2022-08-11 20:13:13

4. Click **Download** button to continue.



Download selected events info

Format:
PDF

Search:
-

Event Type:
All

Account:
All

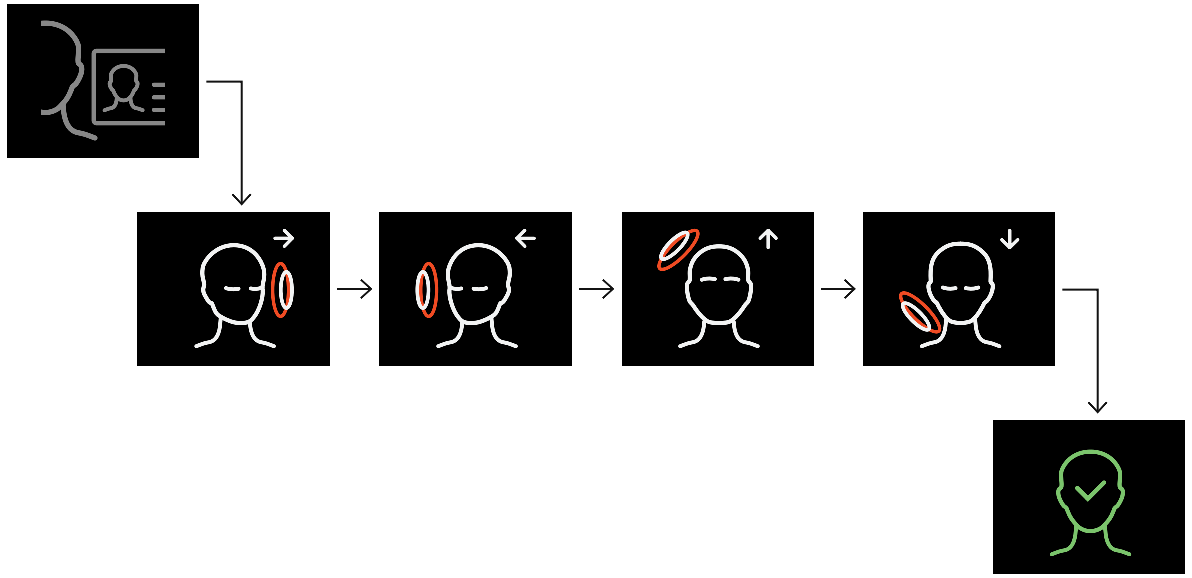
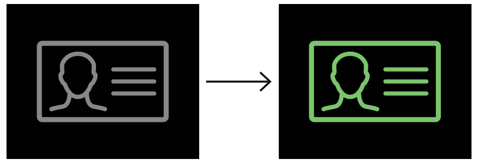
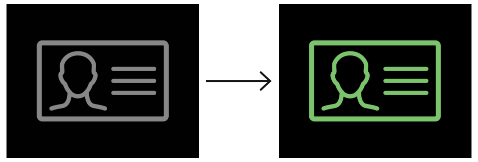
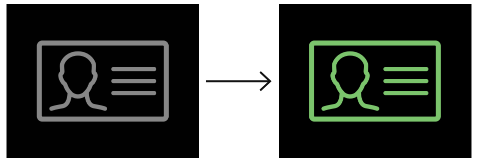
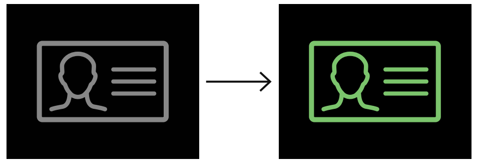
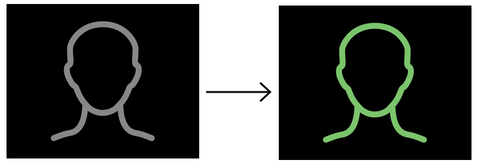
Timestamp:
All

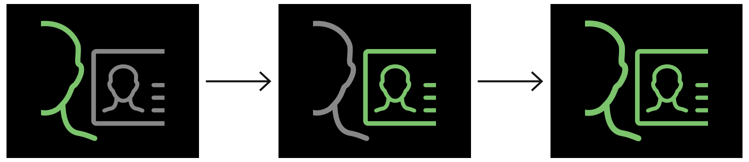
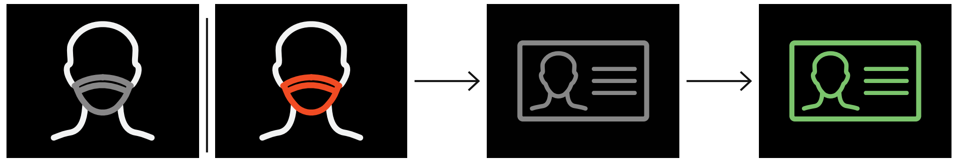
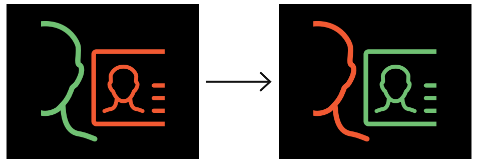
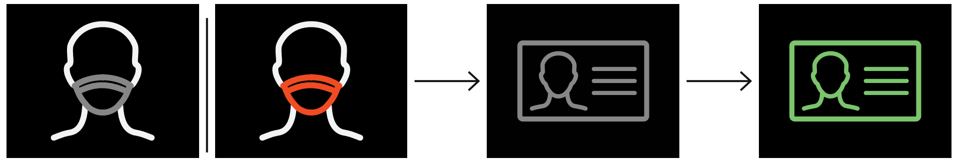
ⓘ Up to 500 events will be exported

5. A zip file of the selected logs will be downloaded (The file will contain up to 500 events.)

7.2—Security Events Summary Table

The table summarizes the most common security events displayed in the Alcatraz AI Admin Portal and the sequence of icons that can be observed on the Rock's display.

	Event Name	Event Trigger	Rock mode	Display Icons
Enrollment	Manual Enrollment Completed	A user manually enrolled at an enrollment station.	Enrollment	
	Auto-Enrollment Initiated	A user swiped a badge for auto-enrollment. Displayed at the first time a person begins the "Auto Enrollment" process.	Face or Badge (1FA) with auto-enrollment	
	Auto-Enrollment Updated	Displayed when a profile is updated during the "Auto Enrollment" process.	Face or Badge (1FA) with auto-enrollment	
	Auto-Enrollment Completed	Displayed when the Auto Enrollment process is completed for a person.	Face or Badge (1FA) with auto-enrollment	
Access Granted	Badge Presented (1FA) Face Authenticated (1FA)	A user authenticated with face or badge.	Face or Badge (1FA)	
	Face Authenticated (1FA)	A user authenticated with face.	Face-Only (1FAF)	 *grey icon will display very briefly

Access Granted	Badge and Face Authenticated (2FA)	Also seen for 3FA using face, badge and PIN. A user authenticated in 2FA – face and badge match. User then enters PIN (or other 3rd authentication factor). Badge and PIN are sent to the ACS. ACS must be configured to accept a badge and PIN.	Face and Badge (2FA)	
		A user entered with a mask and swiped their badge.	Mask Enforcement (2FA–M)	 *flashing animation
	Badge–Face Mismatch	In case of face unknown or badge unknown or face matches another badge, Alcatraz AI Admin Portal will report this event as 2FA Mismatch.	Face and Badge (2FA)	 *animation of green and red
	Entry Without Mask	A user enters without having a Mask. With or without swiping the enrolled badge.	Mask Enforcement (2FA–M)	 *flashing animation
	Profile Deleted	In order to track all security activities Alcatraz AI Admin Portal will report if the user profile is deleted. The event is logged only from the platform not the device.	All	–
Tailgating	Unauthorized Entry–Possible Known User	A person gained entry that could not be authenticated.	All	
	Unauthorized Entry–Unknown User	An unknown person gained entry when a user exited the door.	All	
	Crossing–Possible Known User	A known user gained entry when a user exited the door.	All	
	Crossing–Unknown User	An unknown person gained entry when a user exited the door.	All	
	Tailgating–Possible Known User	A known user gained entry when tailgating a user.	All	
	Tailgating–Unknown User	An unknown person gained entry by tailgating a user.	All	
Tamper	Tamper Reader Detected	The Reader has been removed from the wall.	All	
	Tamper Reader Restored	The Reader has been restored on the wall.	All	
	Tamper Device Detected	The Rock has been removed from the wall.	All	
	Tamper Device Restored	The Rock has been restored on the wall.	All	

8 —
Profiles

Users must enroll with the Rock to be authenticated. Enrolling with the Rock creates a user profile that binds a user’s badge number(s) with their facial biometrics.
Enrollment can be done in two ways:

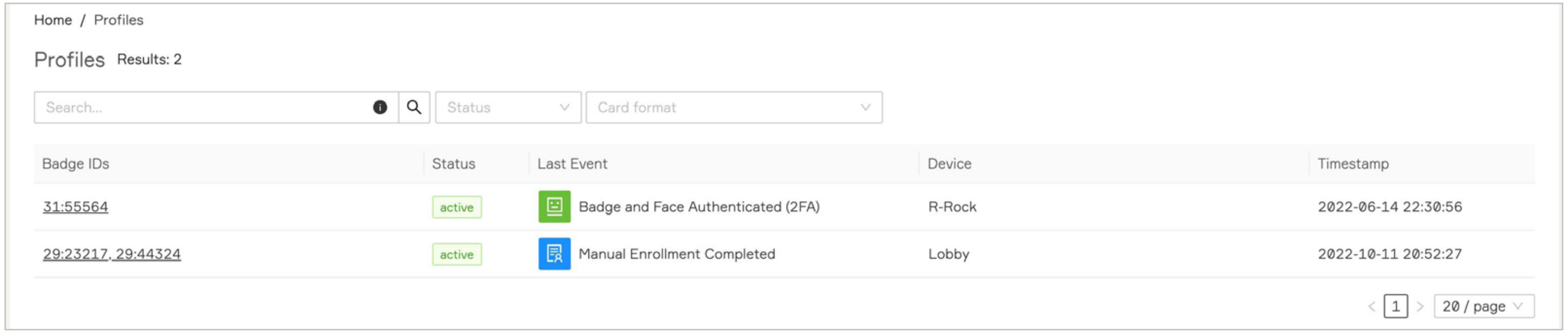
- Auto-enrollment – in Single Factor Authentication (1FA) mode. Users will badge in as normal to enter the door. The Rock builds the user profile with each badge in by capturing quality facial biometrics. After about 4-6 badge ins over the course of a few days, the user will realize as they approach to badge in, the Rock will authenticate, and the door will unlock. When this occurs, the Rock has fused the user’s facial biometrics with the badge number and created a user profile.
- Manual enrollment – available at an enrollment station, usually at a location monitored by a security guard. The Rock is set to enrollment mode for the purpose of only enrolling users and no authentication. The user will be guided by the display icons that will allow the Rock to capture quality facial biometrics to fuse the user with their badge number to create the user profile. The process is one time. Manual enrollment is ideal for organizations that require 2FA (face and badge), installing Rocks where no badge reader is required or want a dedicated enrollment station.

8.1—Managing Profiles

- Profiles will be displayed in the Profiles section in the Alcatraz AI Admin Portal only when enrollment is successful. The Rock must be able to capture good quality images of the user. The user's face must be visible and not obstructed by coverings.
- Profiles associate a user's badge number with their facial biometrics for the purposes of authentication. No personal identifiable information is stored.
- Profiles are synced across all Rocks in the organization for authentication purposes. If a user does not have access to a space, the Access Control System (ACS) will not unlock the door.
- Badge info and the site accessible for the user's badge(s) are managed in the user's Profile with flexibility for users to have multiple badges that can be assigned to one or multiple sites.

8.1.1—Viewing Profiles

1. To view the list of Profiles for the Account, go to **Device Management** and select **Profiles**.

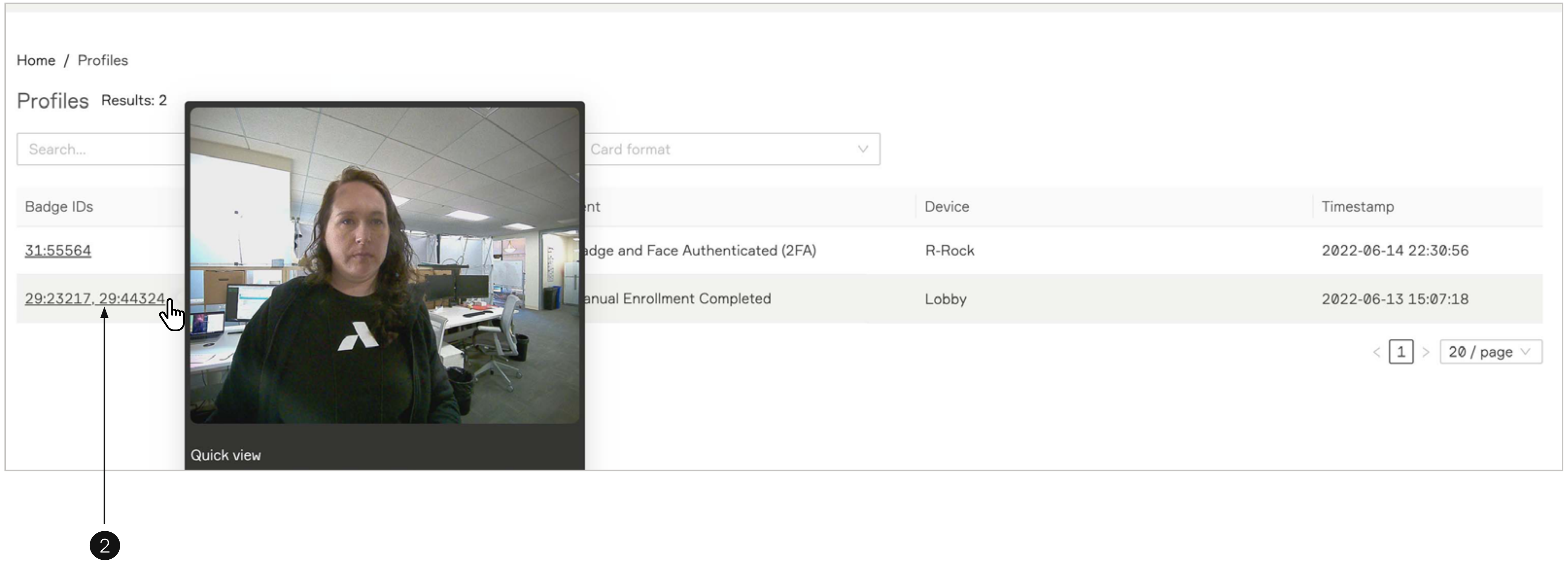


Home / Profiles

Profiles Results: 2

Badge IDs	Status	Last Event	Device	Timestamp
31:55564	active	Badge and Face Authenticated (2FA)	R-Rock	2022-06-14 22:30:56
29:23217, 29:44324	active	Manual Enrollment Completed	Lobby	2022-10-11 20:52:27

2. Hover your cursor over the Badge number to see an image of the Last Event

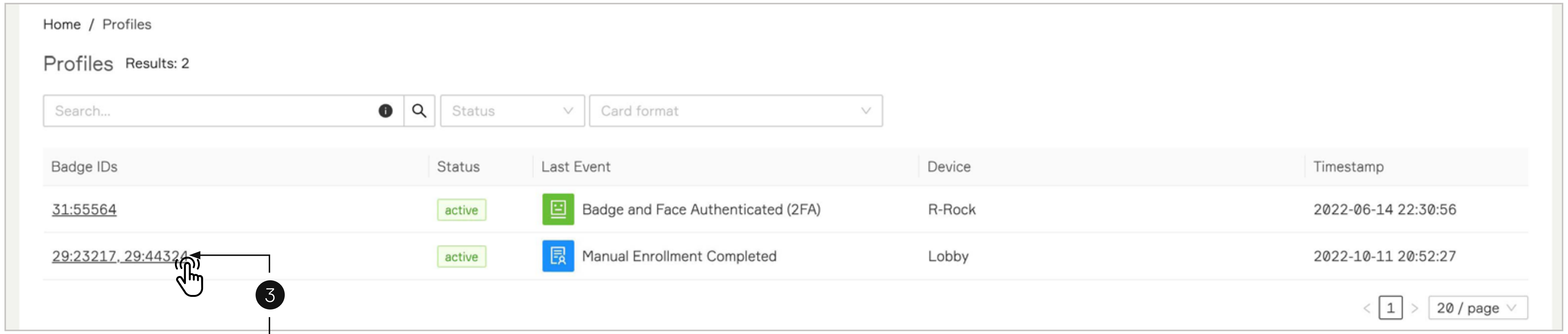


Home / Profiles

Profiles Results: 2

Badge IDs	nt	Device	Timestamp
31:55564	adge and Face Authenticated (2FA)	R-Rock	2022-06-14 22:30:56
29:23217, 29:44324	anual Enrollment Completed	Lobby	2022-06-13 15:07:18

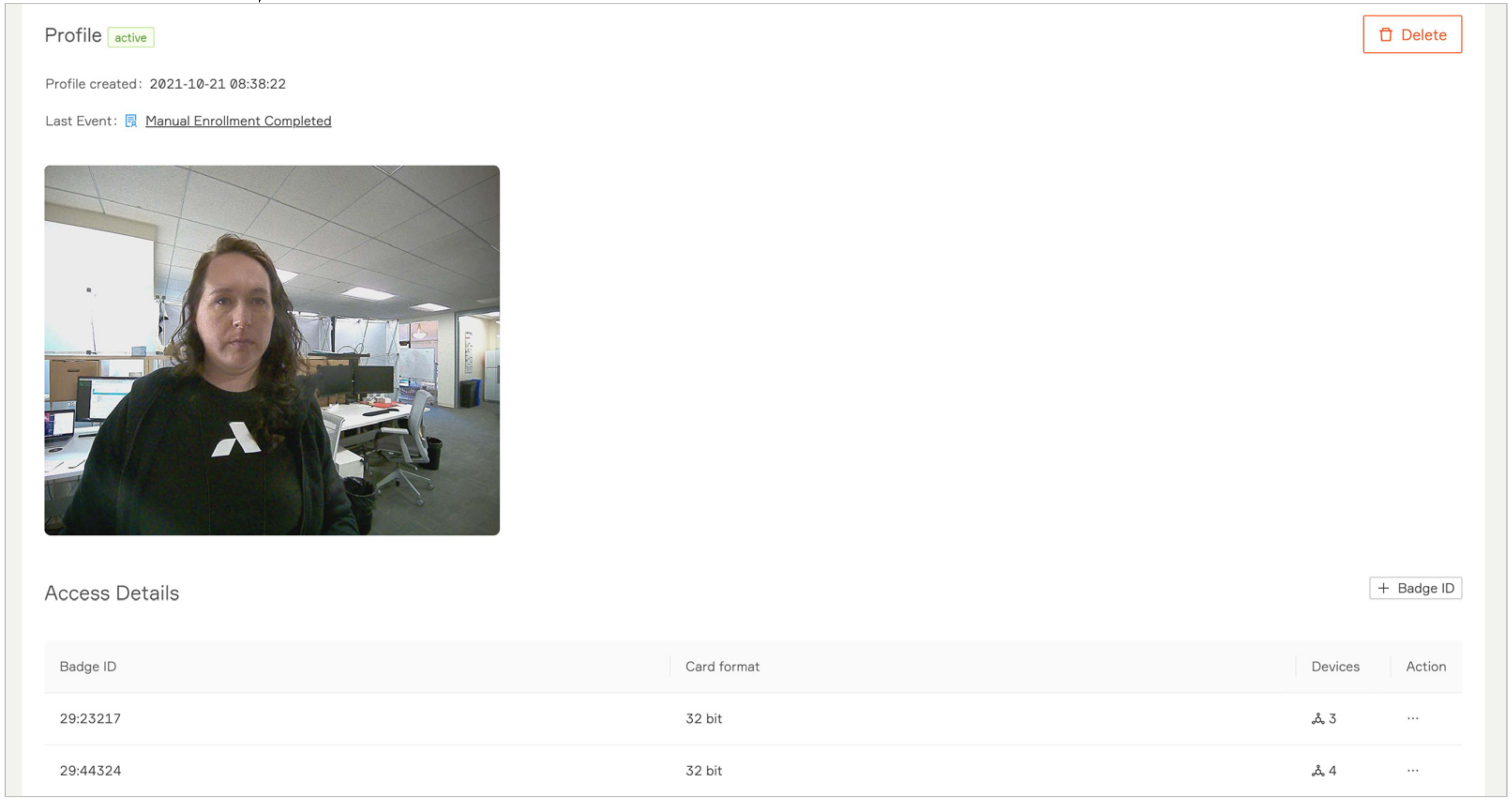
3. To view additional Profile information, click on the Badge ID.
Some of the profiles may have more than one Badge IDs, which are displayed on profiles table separated by commas.
If all profile's cards are deactivated a label no active cards will be added next to the profile badge IDs.



Home / Profiles

Profiles Results: 2

Badge IDs	Status	Last Event	Device	Timestamp
31:55564	active	Badge and Face Authenticated (2FA)	R-Rock	2022-06-14 22:30:56
29:23217, 29:44324	active	Manual Enrollment Completed	Lobby	2022-10-11 20:52:27



Profile active

Profile created: 2021-10-21 08:38:22

Last Event: Manual Enrollment Completed

Access Details

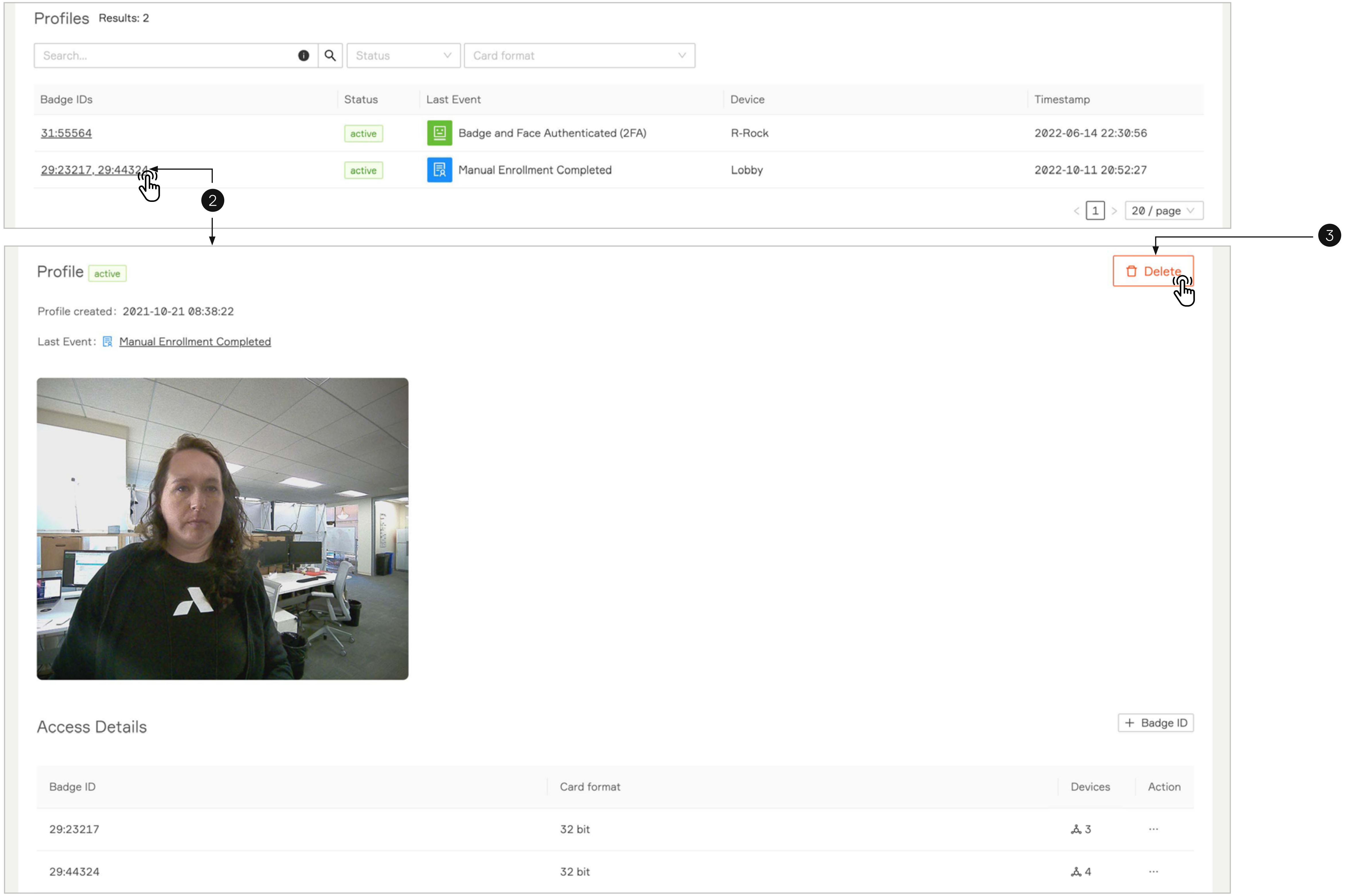
Badge ID	Card format	Devices	Action
29:23217	32 bit	3	···
29:44324	32 bit	4	···

On profile's details page the Badge IDs are organized in a table with additional information about card formats.
The deactivate badge IDs are displayed with lighter color. If all of them are inactive – each row is with lighter colors and a label with text **no active cards** no active cards is visible next to the **Profile** headline at the top of the page.

alcatraz ai
Dashboard
Account
Permissions
Device Management
Security Events
Profiles

8.1.2—Delete a Profile

1. Click on **Profile**
2. Click on selected Badge ID to open the profile's details page.
3. Click on **Delete** at top right to delete this Profile.
4. A pop-up will be displayed requesting to confirm the delete operation.



Profiles Results: 2

Badge IDs	Status	Last Event	Device	Timestamp
31:55564	active	Badge and Face Authenticated (2FA)	R-Rock	2022-06-14 22:30:56
29:23217, 29:44324	active	Manual Enrollment Completed	Lobby	2022-10-11 20:52:27

Profile active

Profile created: 2021-10-21 08:38:22

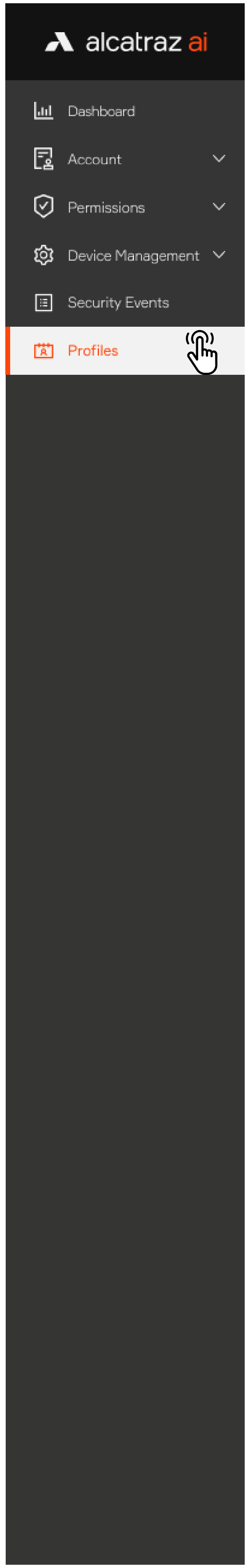
Last Event: Manual Enrollment Completed

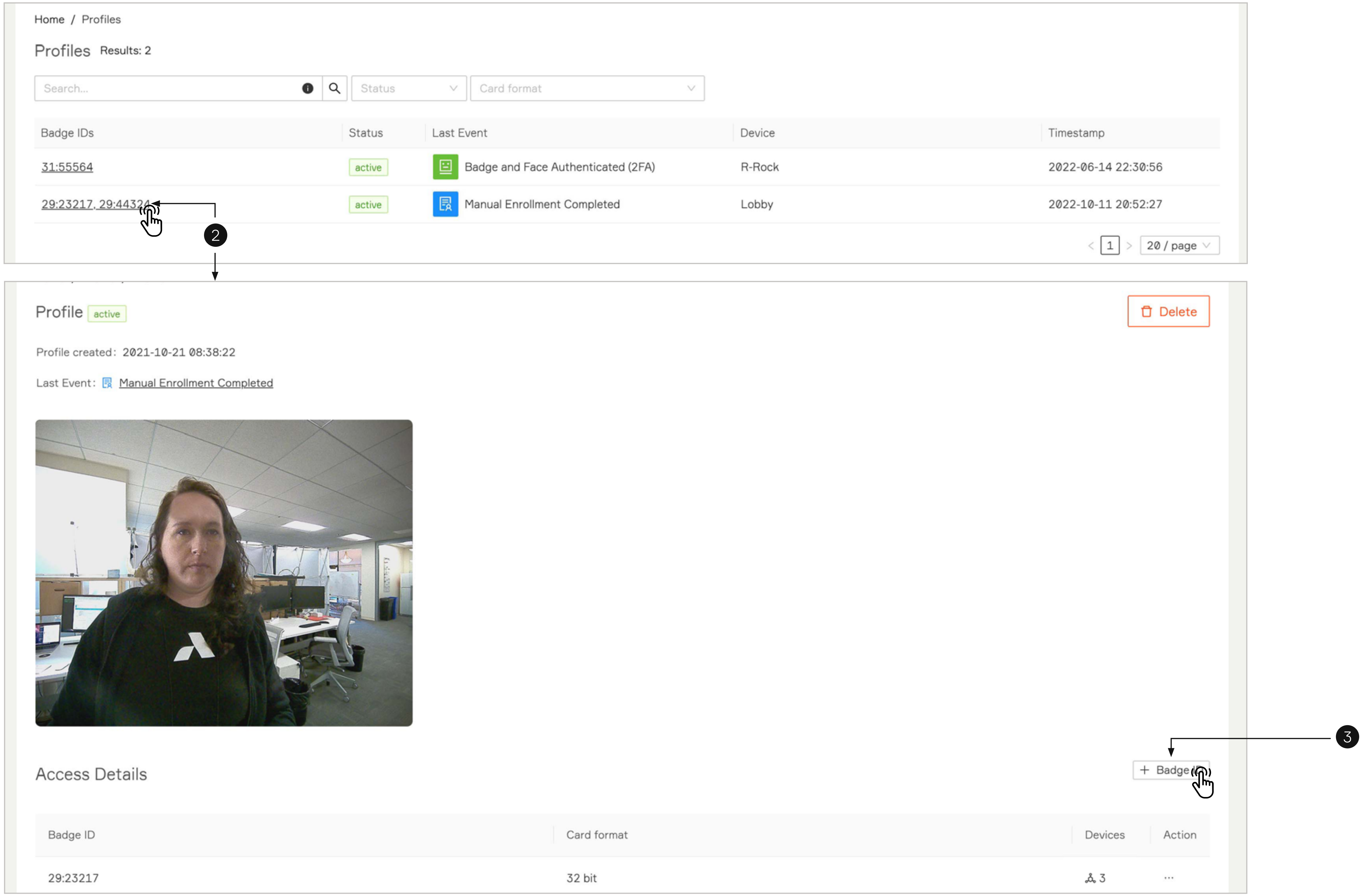
Access Details

Badge ID	Card format	Devices	Action
29:23217	32 bit	3	···
29:44324	32 bit	4	···

8.1.3—Add Badge ID to Profile

1. Click on **Profile**
2. Click on selected Badge ID to open the profile's details page.





Badge IDs	Status	Last Event	Device	Timestamp
31:55564	active	Badge and Face Authenticated (2FA)	R-Rock	2022-06-14 22:30:56
29:23217, 29:44324	active	Manual Enrollment Completed	Lobby	2022-10-11 20:52:27

Profile active

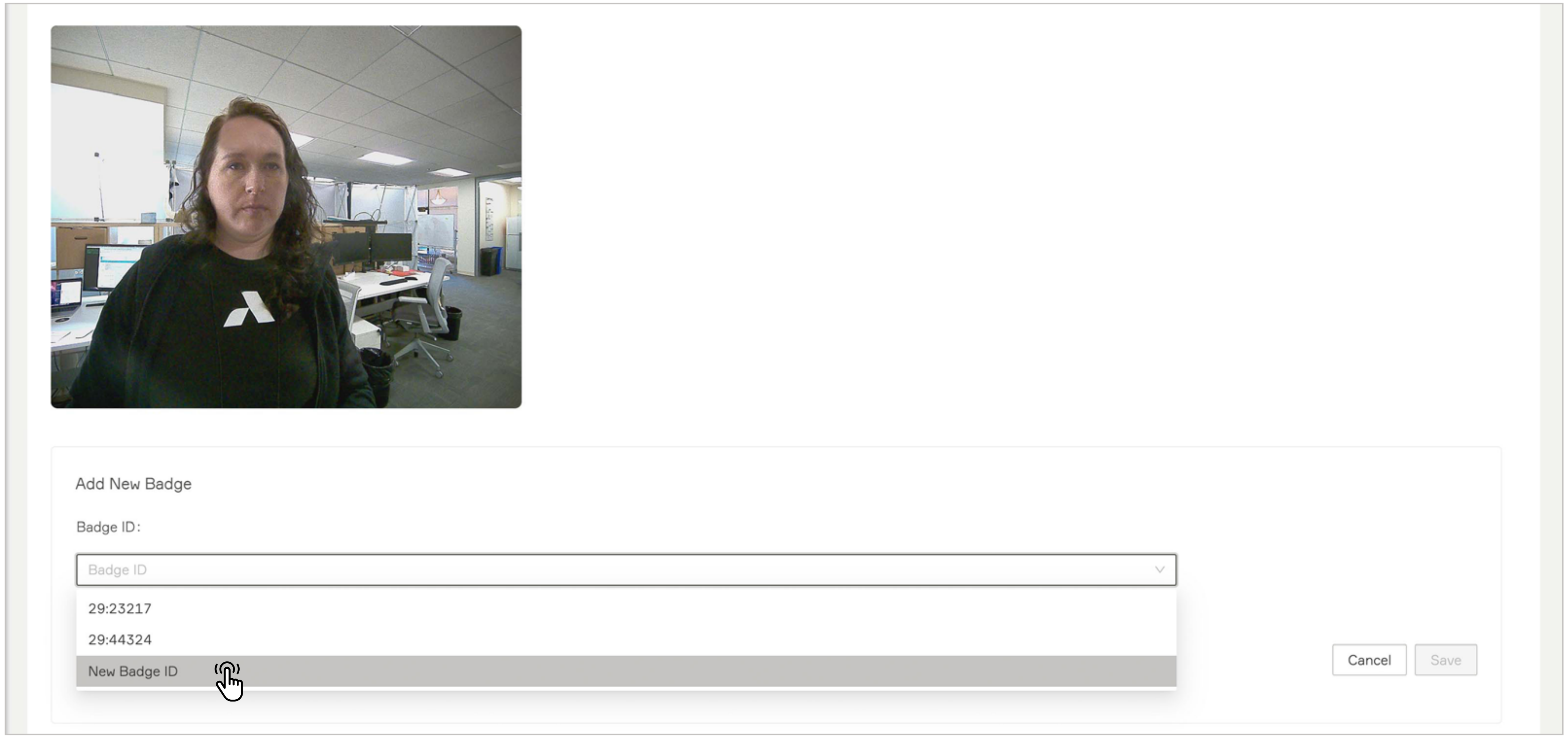
Profile created: 2021-10-21 08:38:22

Last Event: Manual Enrollment Completed

Access Details

Badge ID	Card format	Devices	Action
29:23217	32 bit	3	···

3. Click on **+Badge ID** button.



Add New Badge

Badge ID:

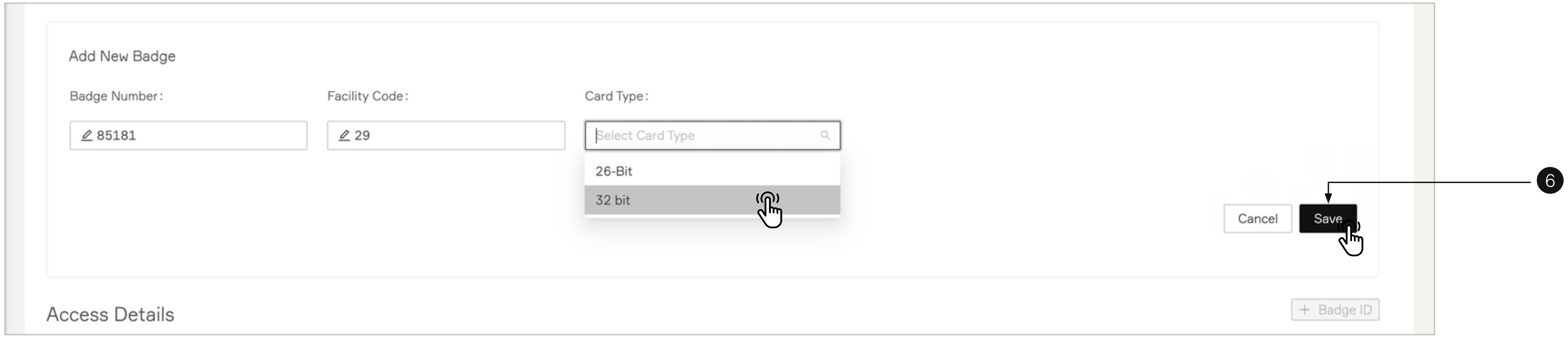
Badge ID

29:23217

29:44324

New Badge ID

4. Select **New Badge ID** from the drop down list.
5. Insert the required fields: **Badge Number**, **Facility Code** and **Card Type**.
6. Click **Save**.



Add New Badge

Badge Number: 85181

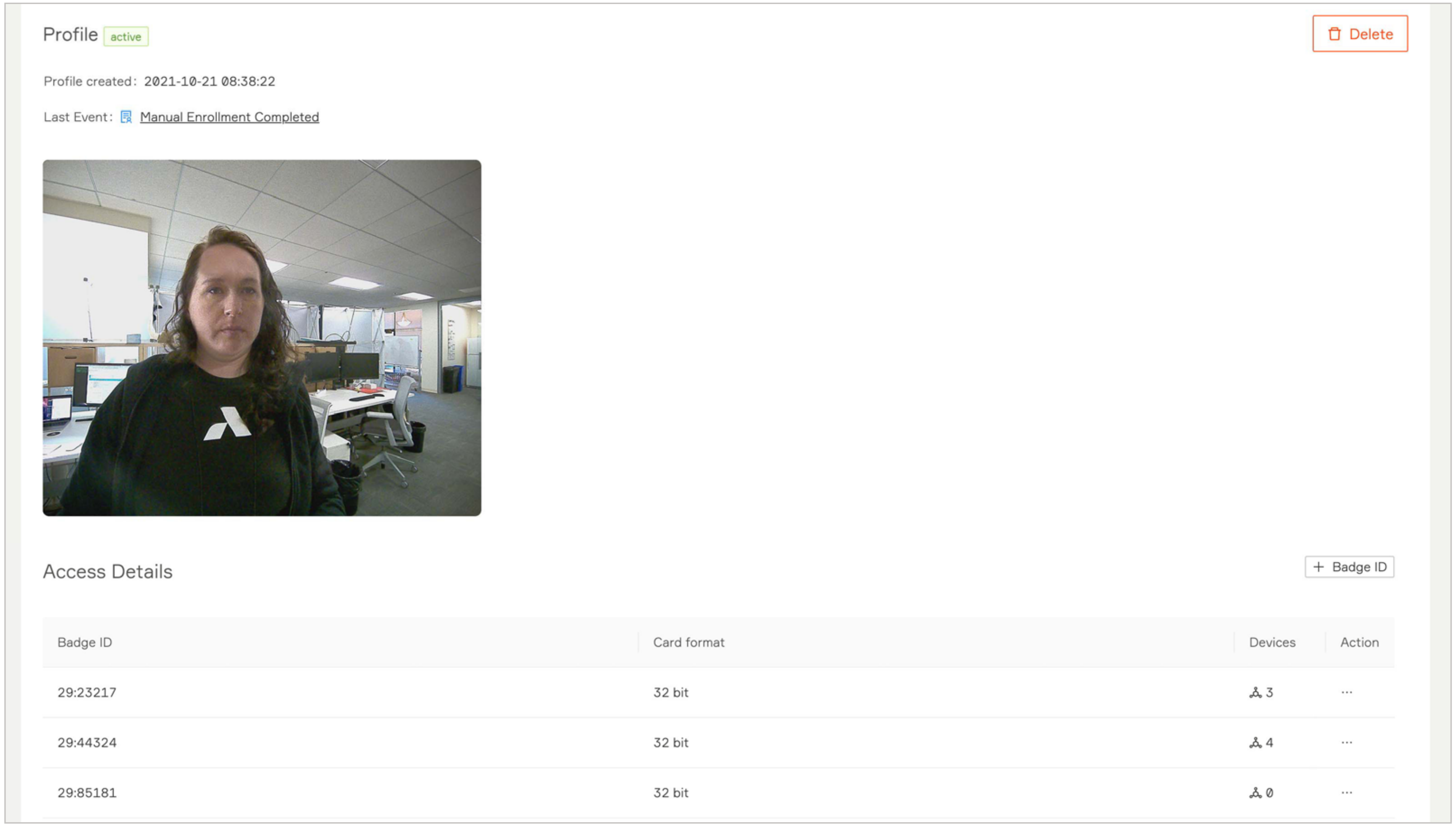
Facility Code: 29

Card Type: Select Card Type

26-Bit

32 bit

alcatraz ai
Dashboard
Account
Permissions
Device Management
Security Events
Profiles



Profile active

Delete

Profile created: 2021-10-21 08:38:22

Last Event: Manual Enrollment Completed

Access Details

+ Badge ID

Badge ID	Card format	Devices	Action
29:23217	32 bit	3	···
29:44324	32 bit	4	···
29:85181	32 bit	0	···

The new badge ID will be added as a last row of the **Access Details** table (also it will be displayed to the profiles page).

8.2.4—Troubleshooting Tips

For generating profiles through enrollment, follow Mode Setting - 1FA (for auto-enrollment) or Mode Setting - Enrollment.
If the badge number is not displayed correctly, review Configure Card Format.
If a profile is not created, check if there are the Security events for enrollment.

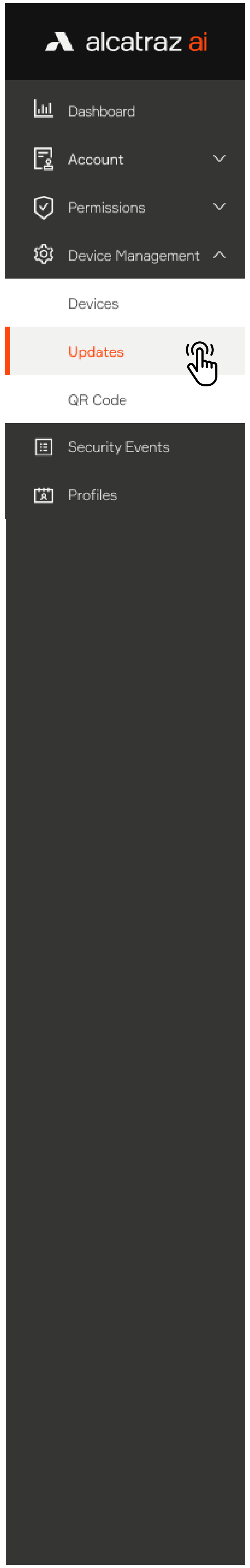
- Profiles are not created in Demo mode.
- Auto-enrollment requires a minimum of 4 New Enrollment events.
- Manual enrollment requires 1 New Enrollment (2FA) event.

9 —

New Rock Firmware

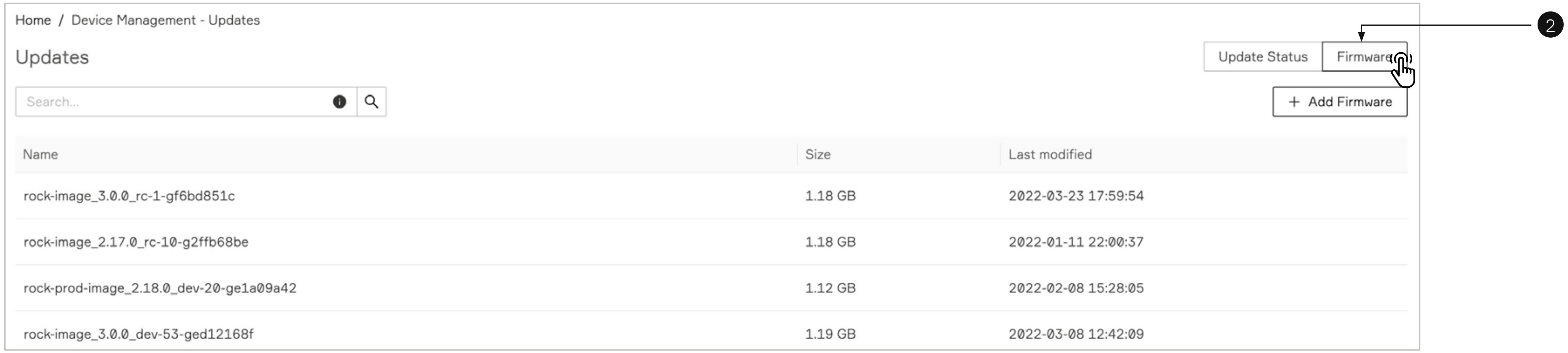
Login credentials to the Alcatraz AI Admin Portal must be Account Administrator or Installer role.
For On-Prem Rocks, before starting

— Visit support.alcatraz.ai to see current releases and download. Submit a request for any questions.
— Download the firmware package to a computer which is connected to the appliance.



9.1—Check Latest Firmware Version in your System

1. Go to **Device Management** and select **Updates**.
2. Click on **Firmware** tab.
3. A table with all firmware versions in your system will be displayed.

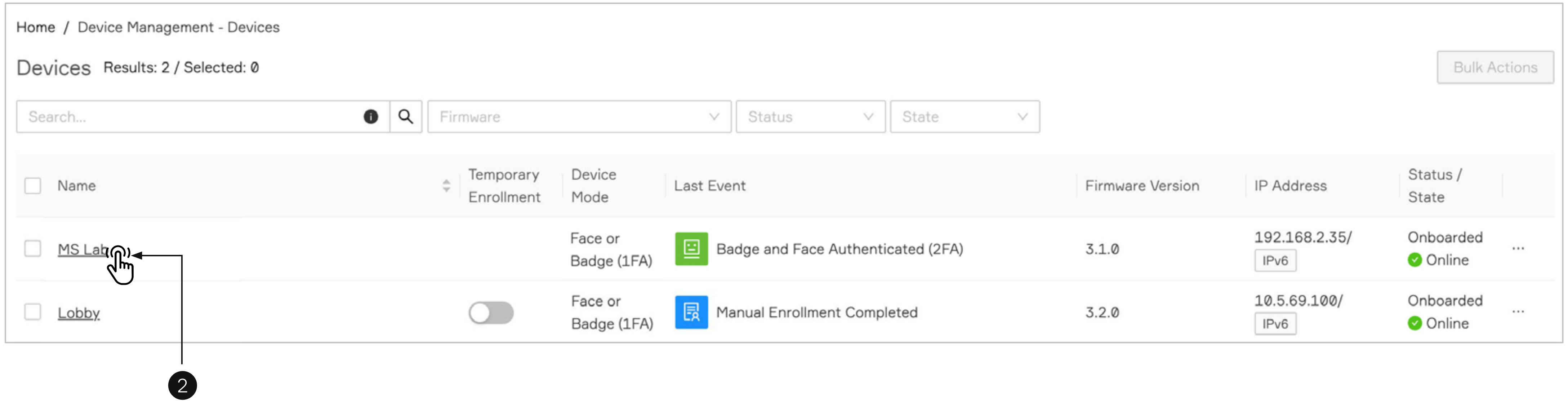


Name	Size	Last modified
rock-image_3.0.0_rc-1-gf6bd851c	1.18 GB	2022-03-23 17:59:54
rock-image_2.17.0_rc-10-g2ffb68be	1.18 GB	2022-01-11 22:00:37
rock-prod-image_2.18.0_dev-20-ge1a09a42	1.12 GB	2022-02-08 15:28:05
rock-image_3.0.0_dev-53-ged12168f	1.19 GB	2022-03-08 12:42:09

alcatraz ai
Dashboard
Account
Permissions
Device Management
Devices
Updates
QR Code
Security Events
Profiles

9.2—Update the Rock Firmware

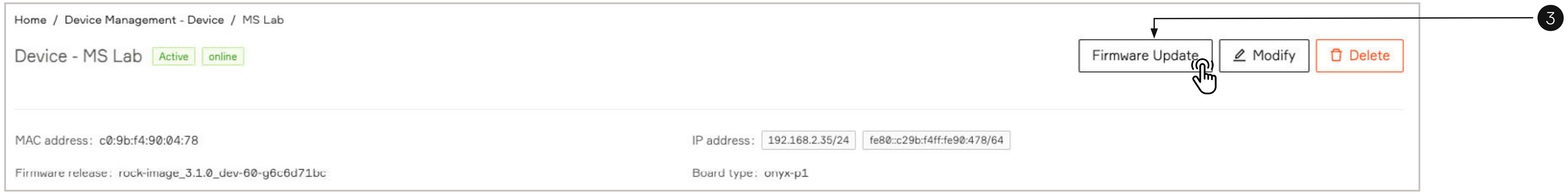
1. Go to **Device Management** and select **Devices**.
2. Click on the Name of the Rock to open the Rock's info page.
3. Click on **Firmware Update**.



Home / Device Management - Devices

Devices Results: 2 / Selected: 0

□	Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State	
□	MS Lab		Face or Badge (1FA)	Badge and Face Authenticated (2FA)	3.1.0	192.168.2.35/ IPv6	Onboarded ● Online	···
□	Lobby	○	Face or Badge (1FA)	Manual Enrollment Completed	3.2.0	10.5.69.100/ IPv6	Onboarded ● Online	···



Home / Device Management - Device / MS Lab

Device - MS Lab Active online

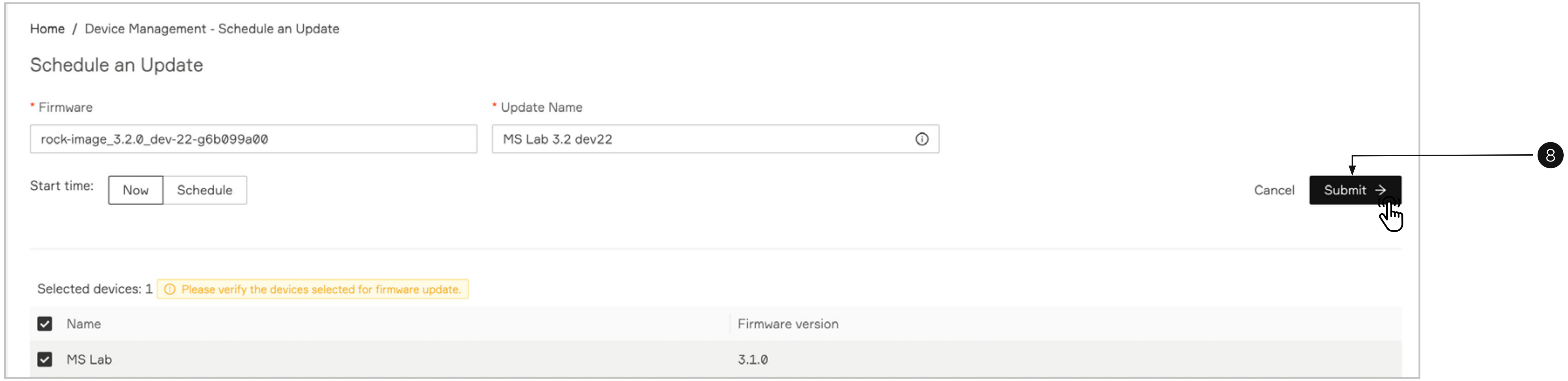
MAC address: c0:9b:f4:90:04:78

IP address: 192.168.2.35/24 fe80::c29b:f4ff:fe90:478/64

Firmware release: rock-image_3.1.0_dev-60-g6c6d71bc

Board type: onyx-p1

4. **Schedule and update** page will be displayed.
5. Select **Firmware** version.
6. Add **Update Name** to the required field
7. Select **Start time**. The Firmware update may be scheduled for a specific date and time.
8. Click the **Submit** button.



Home / Device Management - Schedule an Update

Schedule an Update

* Firmware: rock-image_3.2.0_dev-22-g6b099a00

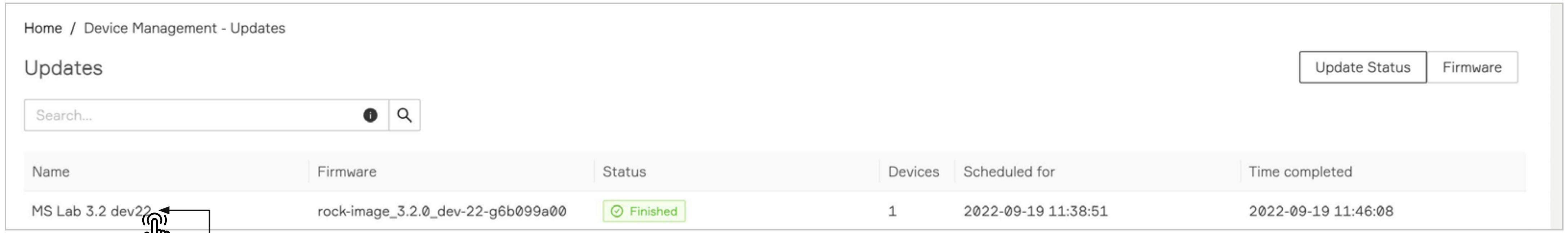
* Update Name: MS Lab 3.2 dev22

Start time: Now Schedule

Selected devices: 1 ⓘ Please verify the devices selected for firmware update.

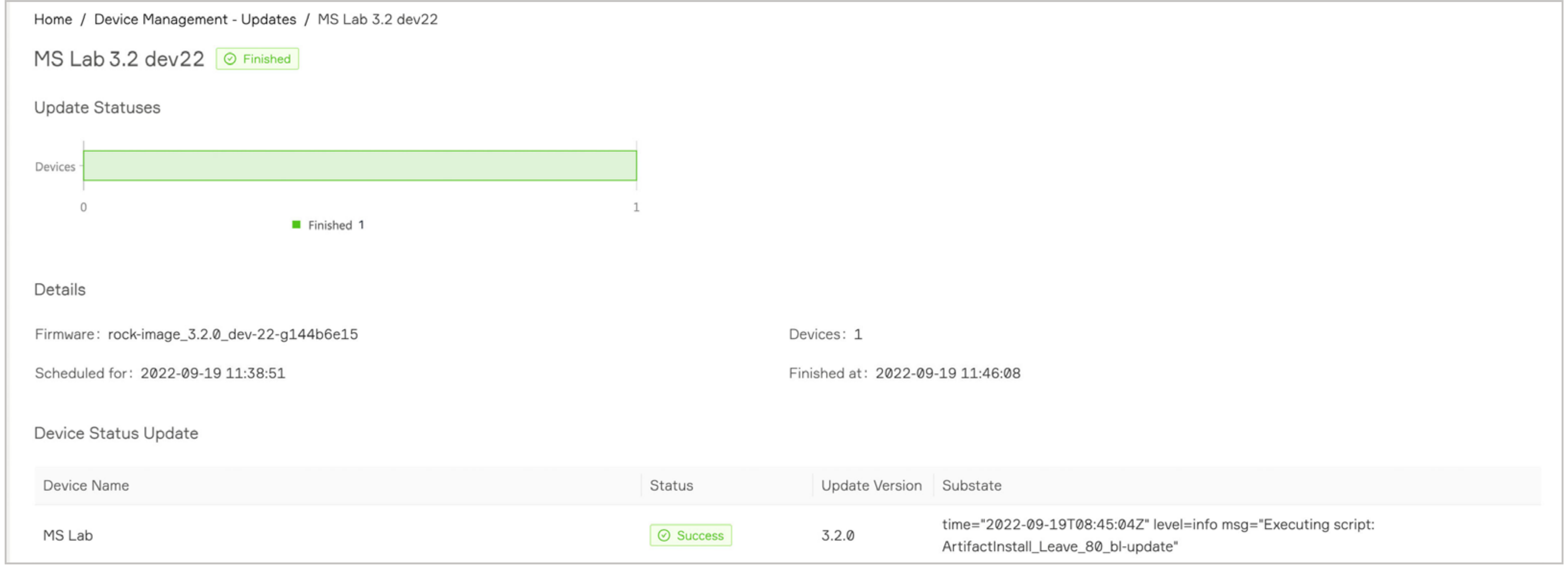
☑ Name	Firmware version
☑ MS Lab	3.1.0

9. The **Update Name** of the selected device will be listed on **Updates** page —> **Update Status** tab.
10. Every 5-10 minutes the update jobs will be checked and processed. View the status change of the update by refreshing the page. The Status will change as the update progresses until **Update Status** = **Finished**. A restart will occur during this process. The Rock will be offline for approximately 60 seconds.
11. If the Deployment Status shows Failed, check that the Rock is online and network connection is stable than create a new update.
12. Click on the Update name to open the details page. A successful update will show a green status (Finished) bar and a **Success** status.
13. To verify the new version for the Rock, go to **Device Management** —>**Devices** and in the table will be displayed the updated firmware version of the device.



Name	Firmware	Status	Devices	Scheduled for	Time completed
MS Lab 3.2 dev22	rock-image_3.2.0_dev-22-g6b099a00	Finished	1	2022-09-19 11:38:51	2022-09-19 11:46:08

12



Details

Firmware: rock-image_3.2.0_dev-22-g144b6e15

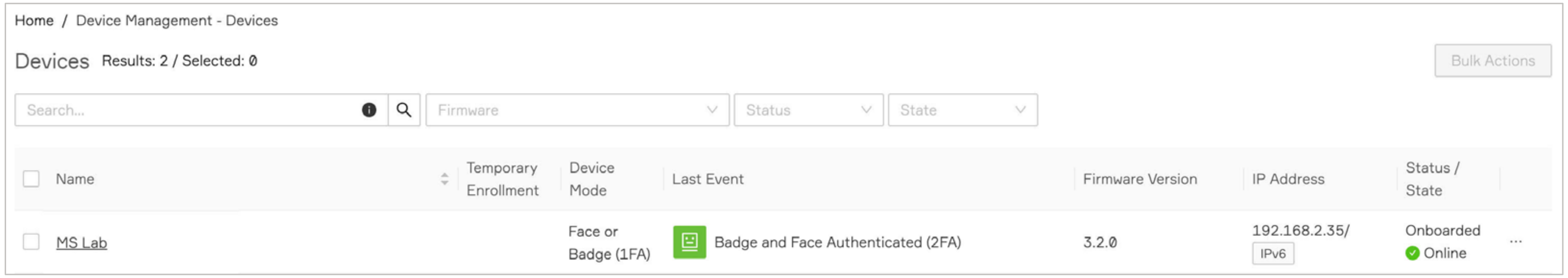
Devices: 1

Scheduled for: 2022-09-19 11:38:51

Finished at: 2022-09-19 11:46:08

Device Status Update

Device Name	Status	Update Version	Substate
MS Lab	Success	3.2.0	time="2022-09-19T08:45:04Z" level=info msg="Executing script: ArtifactInstall_Leave_80_bl-update"



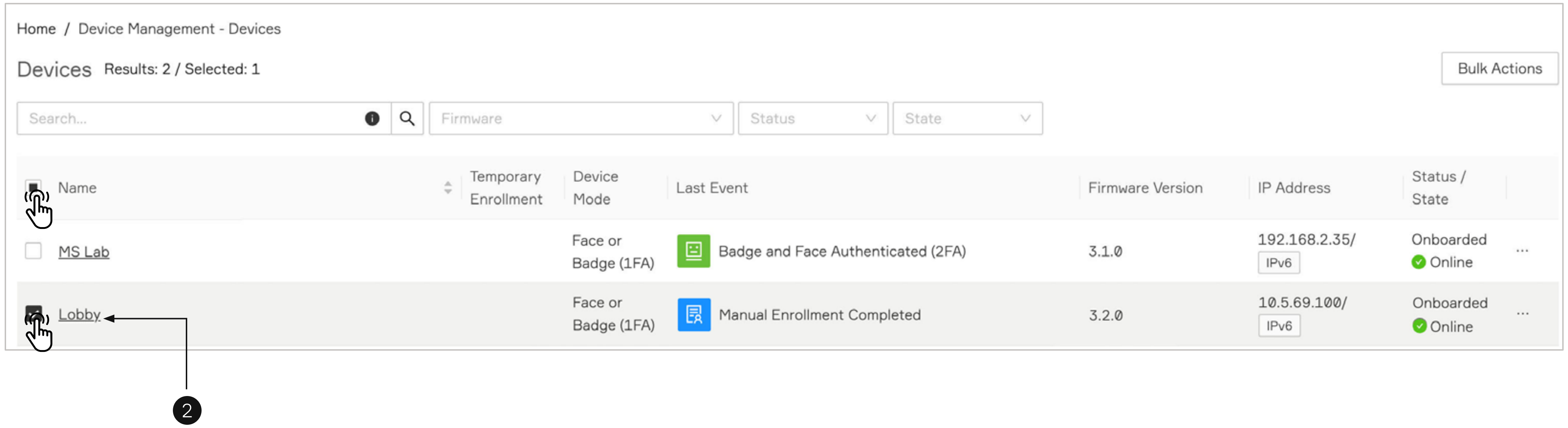
□	Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State
□	MS Lab		Face or Badge (1FA)	Badge and Face Authenticated (2FA)	3.2.0	192.168.2.35/ IPv6	Onboarded Online

alcatraz ai
Dashboard
Account
Permissions
Device Management
Devices
Updates
QR Code
Security Events
Profiles

9.3—Rock firmware update bulk operation

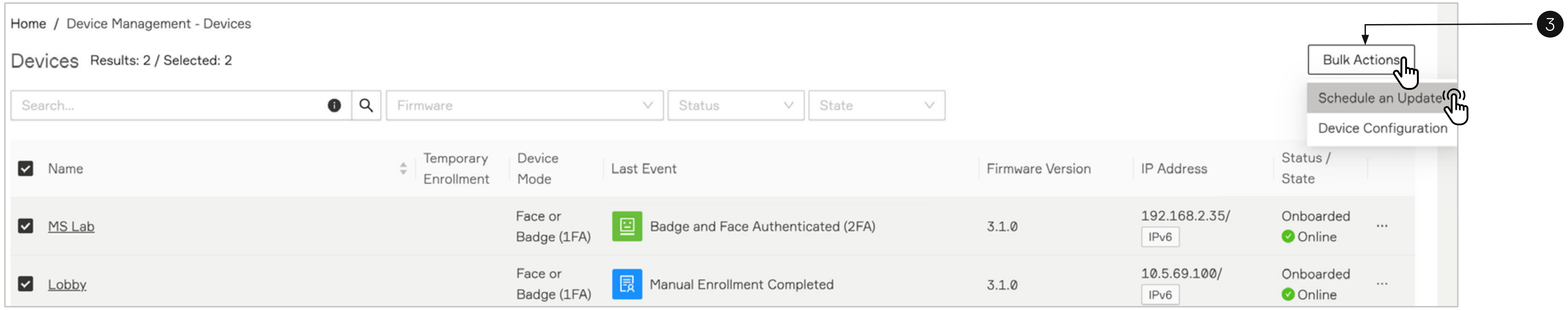
The device bulk operation allows updating the firmware of multiple devices.

1. Go to **Device Management** and select **Devices**.
2. Click the checkbox of the rock's name to select it. Continue to select devices that need to be updated to newer version. To select all of the devices on the page click the checkbox next to Name title of the table (optional).
3. Hover over **Bulk Actions** and select **Schedule an Update**.



Devices Results: 2 / Selected: 1

	Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State
□	MS Lab		Face or Badge (1FA)	Badge and Face Authenticated (2FA)	3.1.0	192.168.2.35/ IPv6	Onboarded ● Online
☑	Lobby		Face or Badge (1FA)	Manual Enrollment Completed	3.2.0	10.5.69.100/ IPv6	Onboarded ● Online

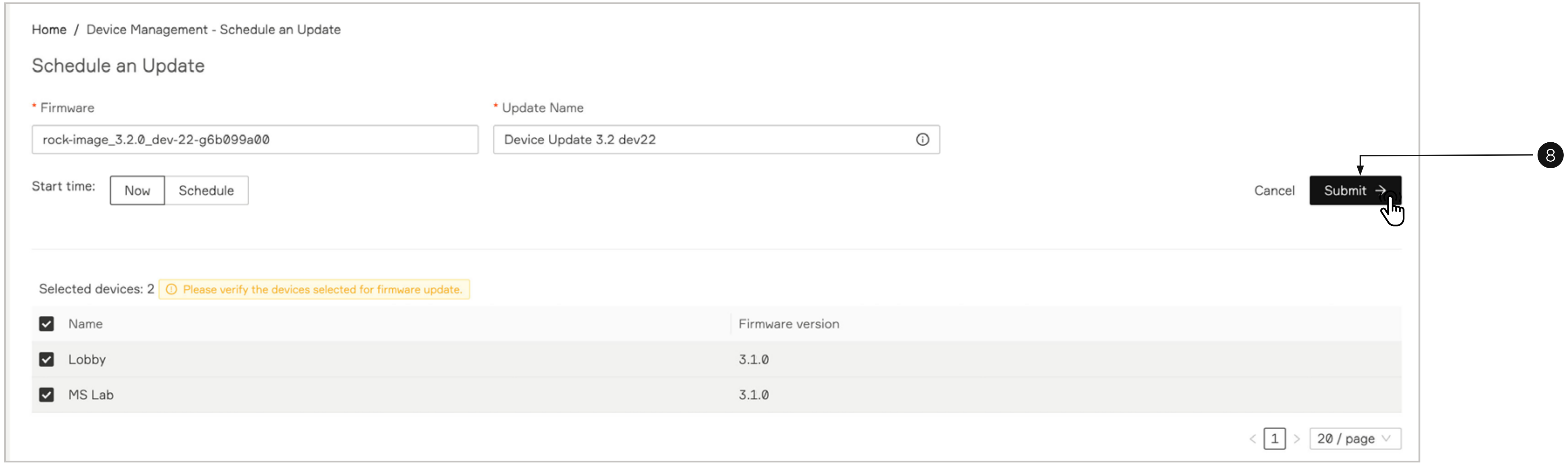


Devices Results: 2 / Selected: 2

☑	Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State
☑	MS Lab		Face or Badge (1FA)	Badge and Face Authenticated (2FA)	3.1.0	192.168.2.35/ IPv6	Onboarded ● Online
☑	Lobby		Face or Badge (1FA)	Manual Enrollment Completed	3.1.0	10.5.69.100/ IPv6	Onboarded ● Online

alcatraz ai
Dashboard
Account
Permissions
Device Management
Devices
Updates
QR Code
Security Events
Profiles

4. **Schedule and update** page will be displayed. Selected devices are organized in table bellow.
   The system allows to uncheck devices from the list and they will be excluded of the firmware update operation.
5. Select **Firmware** version.
6. Add **Update Name** to the required field.
7. Select **Start time**.
8. Click the **Submit** button.



Home / Device Management - Schedule an Update

Schedule an Update

* Firmware: rock-image_3.2.0_dev-22-g6b099a00

* Update Name: Device Update 3.2 dev22

Start time: Now | Schedule

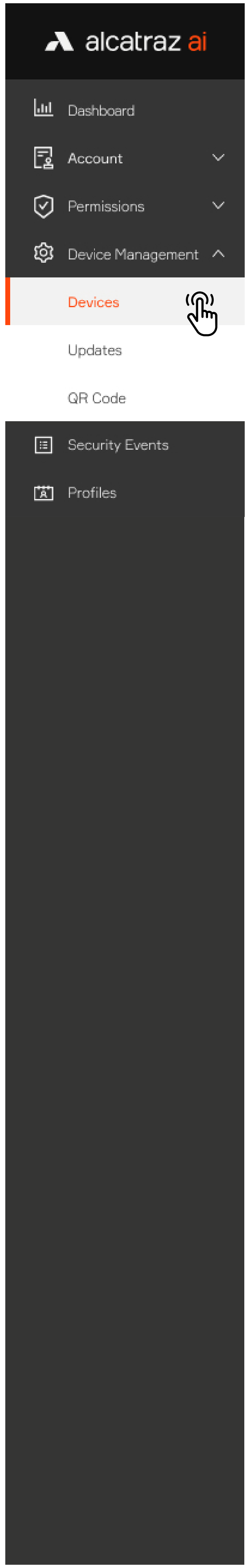
Selected devices: 2 ⓘ Please verify the devices selected for firmware update.

☑ Name	Firmware version
☑ Lobby	3.1.0
☑ MS Lab	3.1.0

9. After Submitting the **Update Name** of the selected device will be listed on **Updates** page (**Update Status** tab).
10. Every 5-10 minutes the update jobs will be checked and processed. View the status change of the update by refreshing the page. On the updates details page, the status progress bar will change as the update processes of the different devices. **Device Status Update** table will show the status of each device. If any of the devices failed during the update you can schedule a new update process for them.

10 —
Advanced Options

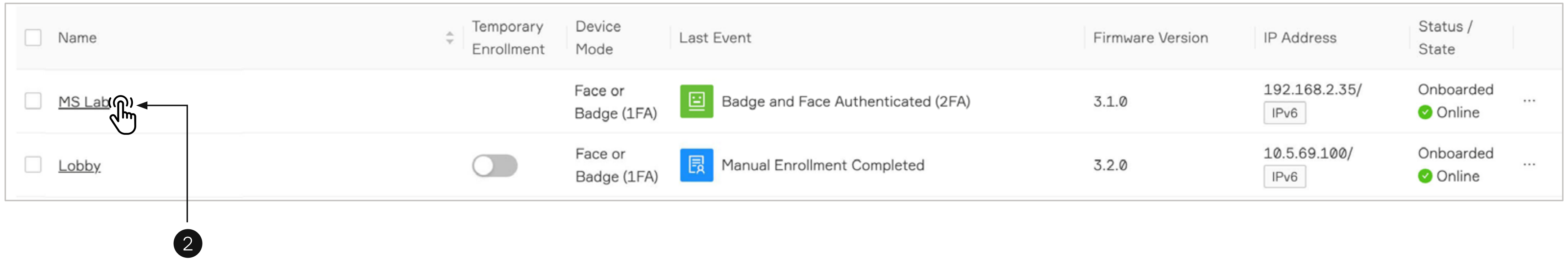
Some of the most frequently used parameters are discussed here but it is recommended to check with Alcatraz AI when changing configurations in the Advanced section.



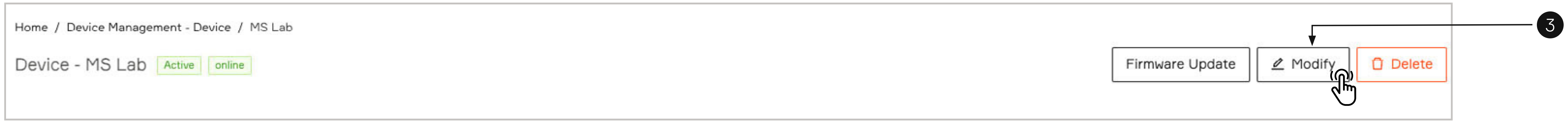
10.1—Applying Advanced Options

To enable the advanced options, follow the described steps below.

1. Go to **Device Management** —> **Devices**
2. Click on the Name of the Rock to open the Rock's info page.
3. Click on **Modify** to open up the configurations page.
4. Scroll down the page to **Device Configuration** and on the right side of the page, slide the **Advanced** slider to on.
5. Scroll down to **Add a Parameter**. Click to open the section

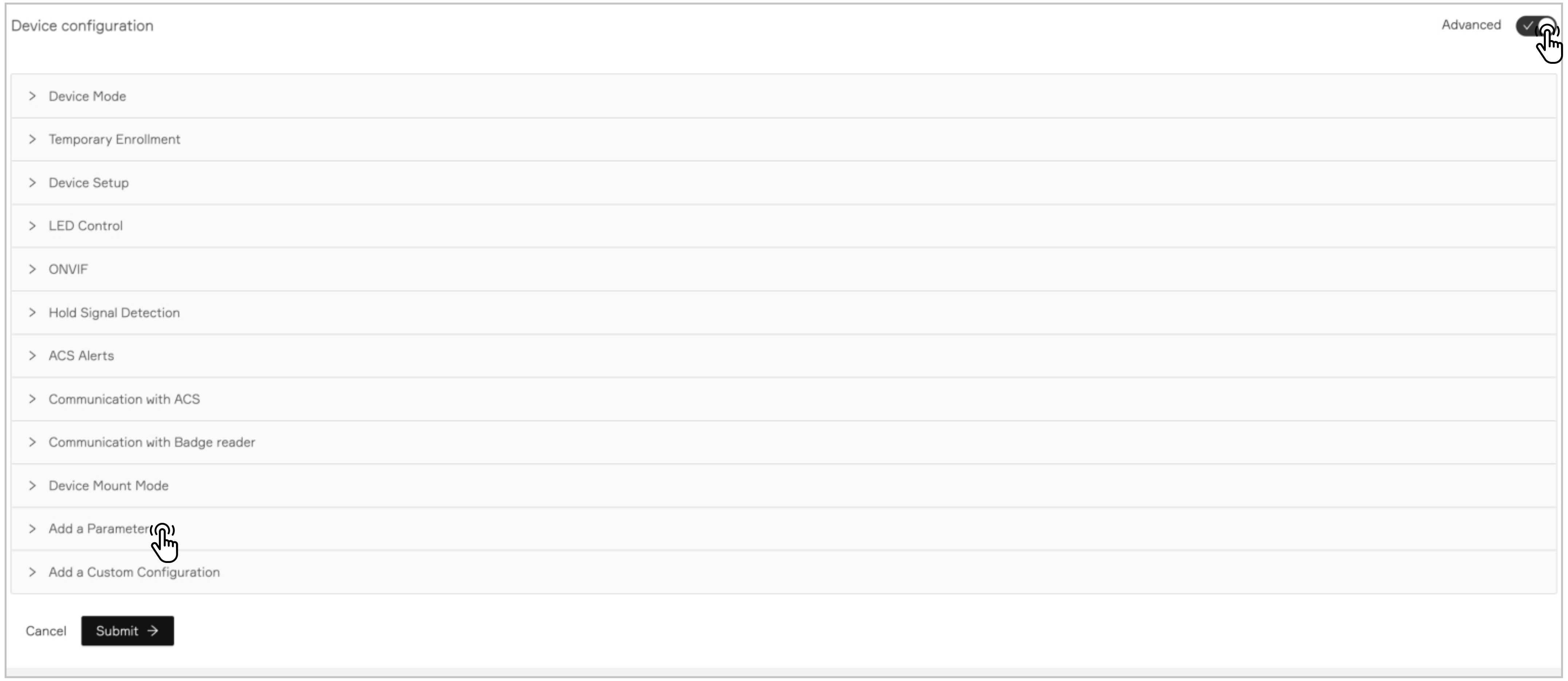


□ Name	Temporary Enrollment	Device Mode	Last Event	Firmware Version	IP Address	Status / State
□ MS Lab		Face or Badge (1FA)	Badge and Face Authenticated (2FA)	3.1.0	192.168.2.35/ IPv6	Onboarded Online
□ Lobby	○	Face or Badge (1FA)	Manual Enrollment Completed	3.2.0	10.5.69.100/ IPv6	Onboarded Online



Home / Device Management - Device / MS Lab

Device - MS Lab Active online

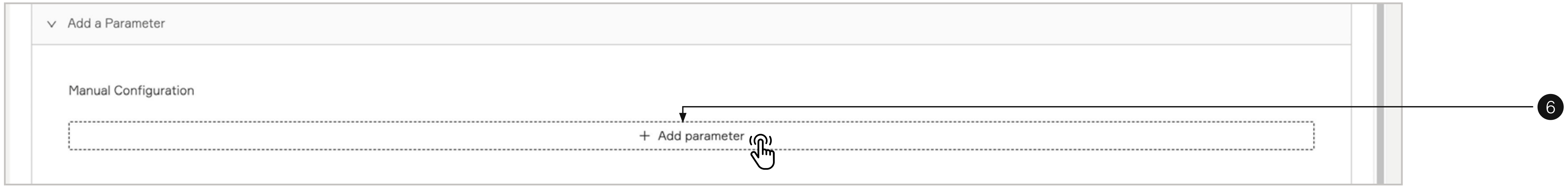


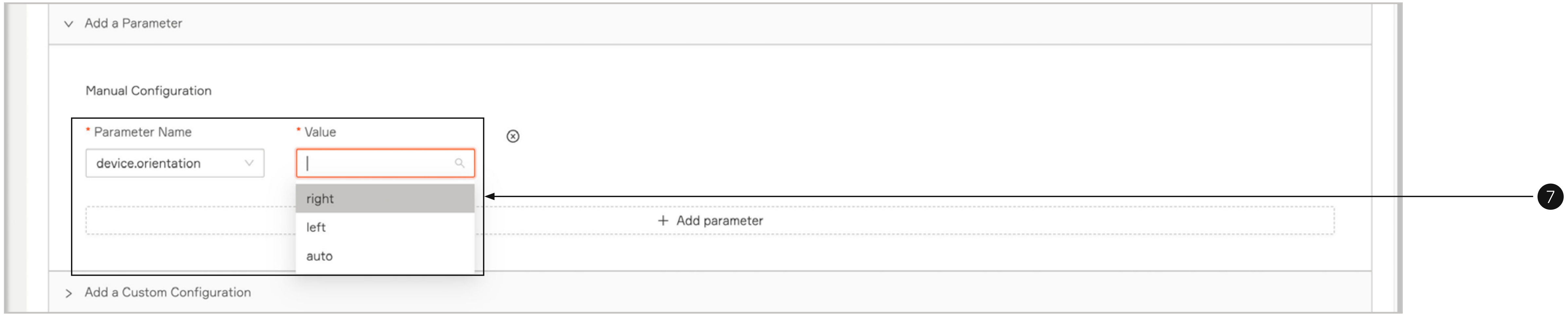
Device configuration

Advanced ✓

- Device Mode
- Temporary Enrollment
- Device Setup
- LED Control
- ONVIF
- Hold Signal Detection
- ACS Alerts
- Communication with ACS
- Communication with Badge reader
- Device Mount Mode
- Add a Parameter
- Add a Custom Configuration

6. Under **Manual Configuration** click on **+Add parameter** button.
7. Select a preferred parameter and value.

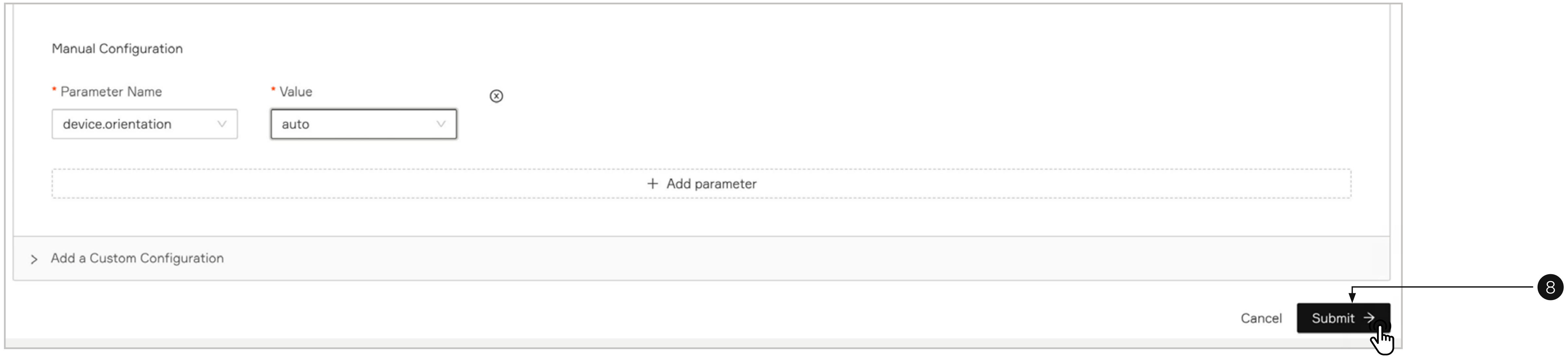




* Parameter Name: device.orientation

* Value: right / left / auto

8. Click **Submit** when done.



* Parameter Name: device.orientation

* Value: auto

alcatraz ai