

Alcatraz AI Admin Portal Guide

Contents

Overview	4
1 — QuickStart	5
2 — Dashboard	6
3 — Accounts	8
3.1—Create an Account	9
3.2—Edit an Account	10
3.3—View an Account	11
3.4—Delete an Account	12
3.5—Configure Card Format.	12
3.5.1—Configure a Pre-defined Card Format	13
3.5.2—Configure a Custom Card Type	15
3.5.3—Example of Card Format with No Parity Bits.	17
3.5.4—Example of Card Format Using Parity Bits.	18
4 — Permissions	19
4.1—Create a User	21
4.2—Delete a User	22
5 — Onboard a Rock	23
5.1—Assigning the Rock an Access Group	24
5.5—Find the Rock to Onboard by Search	24
5.6—Authenticate the Device	24
5.4—Name the Device.	25
6 — Device Management	27
6.1—Devices	28
6.1.1—Configure Rock Mode of Operation.	29
6.1.1.1—Mode Setting – Demo	31
6.1.1.2—Mode Setting – 1FA	31
6.1.1.3—Mode Setting – 1FAF	32
6.1.1.4—Mode Setting – 2FA-M	32
6.1.1.6—Mode Setting – 2FA	33
6.1.1.5—Operating in 3FA	33
6.1.1.7—Mode Setting – Enrollment	34
6.1.1.8—Changing Badges	35
6.1.2—LED Control	36
6.1.3—ONVIF	38
6.1.3.1—Adding a Rock to the VMS (ONVIF)	40
6.1.4—HOLD Signal Detection	40
6.1.5—Configure ACS Alerts.	42
6.1.6—Configure OSDP	45
6.1.6.1—Select Rock to Configure OSDP	46
6.1.6.2—Rock Communication with Badge Reader	48
6.1.6.3—Rock Communication with ACS	49
6.1.6.4—Changing from Secure to Unsecure Channel	50
6.1.6.5—Troubleshooting Tips	51
6.1.6.6—Wiring Details.	51
6.2—Access Groups	52
6.2.1—Create an Access Group	52
6.2.2—Delete an Access Group	53
6.2.3—Embedded Access Groups.	54
6.2.4—Change Default Access Group	55
6.2.5—Add Additional Access Groups	56
6.3—Security Events	57
6.3.1—Viewing Security Events	57
6.3.2—Security Events Summary Table.	58
6.4—Generate QR Code	60
6.4.1—Server Location	62
6.4.2—Generate and Download QR Code	63
6.4.3—Present QR Code to the Rock’s Camera	64
6.4.4—When can the Rock read a QR code?	64
6.5—Profiles	65
6.5.1—Viewing Profiles	66
6.5.2—Delete a Profile – Option 1 (delete through Profiles)	68
6.5.3—Delete a Profile – Option 2 (delete through Security Event).	69
6.5.4—Managing Access	70



Contents

6.5.5—Troubleshooting Tips

72

7 — New Rock Firmware

73

7.1—Check Lastest Firmware Version.

74

7.2—Update the Rock Firmware

75

7.3—Verify Update is Successful

77

8 — Advanced Options

79

8.1—Enabling or Disabling QR Code Receptive Icon

80

8.2—Setting the Rock for Corridor Mode

82

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 swipe a badge with facial authentication 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.
Un-Authorized Entry	A user cannot be identified 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.
Tailgating	A user is followed by another person when entering 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.

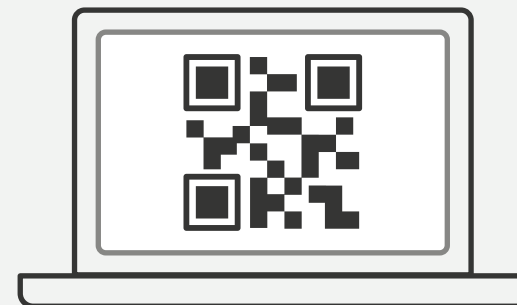
1 — QuickStart



1 Start with

- Requesting an Alcatraz AI Admin Portal login from your Account Administrator
- or
- Submitting a request for a login at support.alcatraz.ai

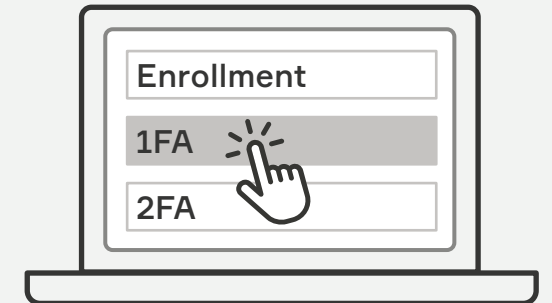
2 Generate QR Code



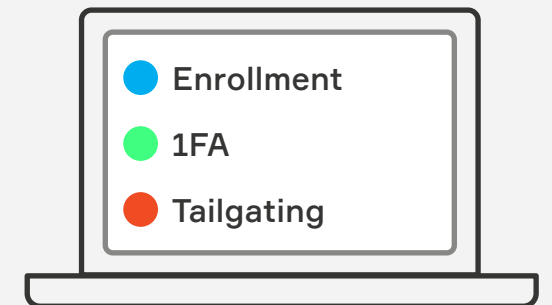
3 Onboard a Rock



4 Configure Rock Mode



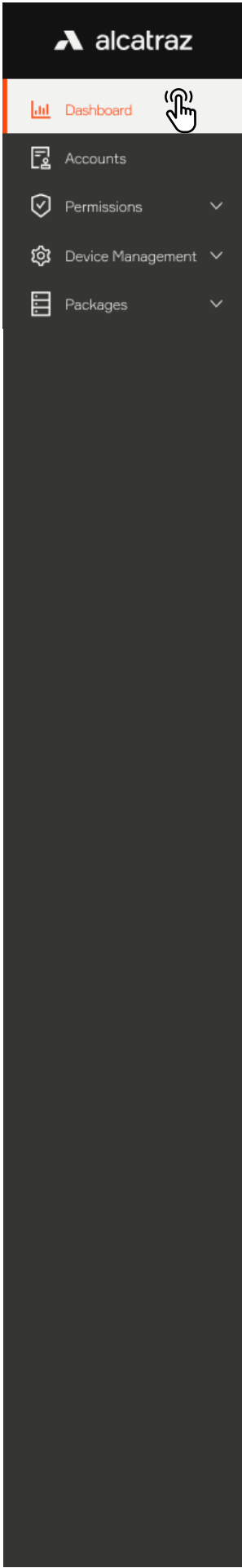
5 View Security Events



6 Check Profiles



2 — Dashboard



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

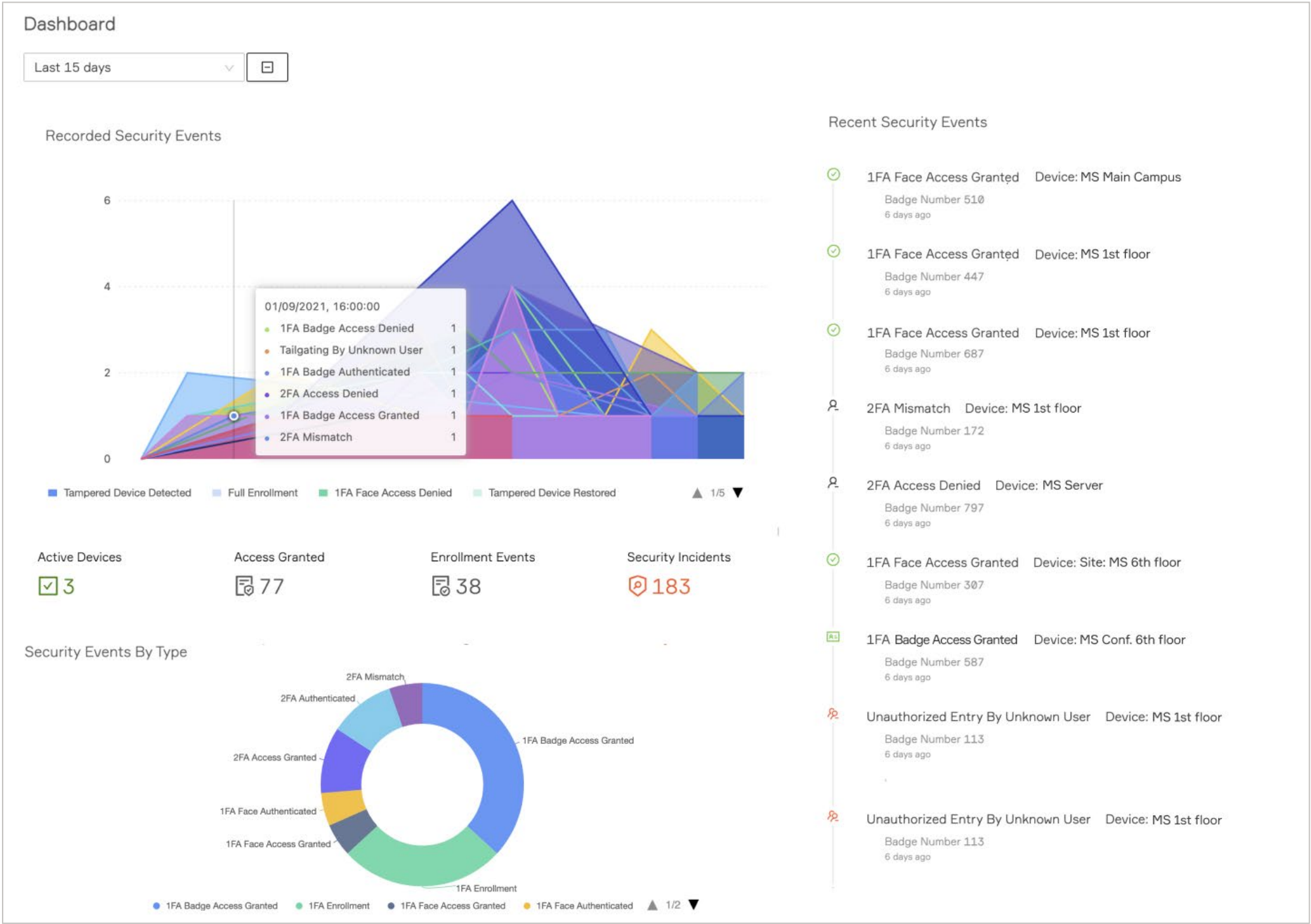
- Hover your cursor over the graph to get metrics for the security events over time or filter on a timeframe by selecting from the drop-down menu
- Click on the security event names to filter out the events you do not wish to view on the graph.

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



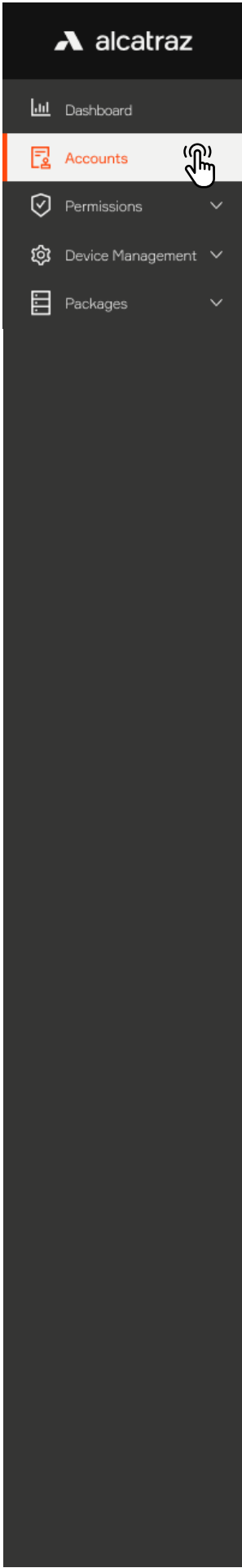
Please note that the information displayed on the dashboard varies with access permissions associated with user roles.



3 — Accounts

Accounts are created for each customer to manage Rocks. Only Dealer Admins can create, delete or edit Accounts. 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—Create an Account	9
3.2—Edit an Account	10
3.3—View an Account	11
3.4—Delete an Account	12
3.5—Configure Card Format	12
3.5.1—Configure a Pre-defined Card Format	13
3.5.2—Configure a Custom Card Type	15
3.5.3—Example of Card Format with No Parity Bits	17
3.5.4—Example of Card Format Using Parity Bits	18



3.1—Create an Account

1. Go to **Accounts** and click on **Create an Account**.
 - **Reference Number** (optional) – gives flexibility to add a number to associate with, for example, a billing account.
2. Complete the information in the **Add Account** pane.
3. Click **Submit**.

Home / Accounts

Accounts

Search accounts...

☐ Name

Reference Number

Devices

+ Create an Account

Home / Accounts

Accounts

Search accounts...

☐ Name

Refer

☐ Alcatraz Organization

2864

☐ ABC Company

2903

☐ ABC Organization

3483

Add Account

Home / Accounts

Create Account

* Account name

Micro Squared

* E-mail

admin@microsquared.com

Reference Number

862548997

Country

City

ZIP Code

United States

San Jose

95129

Billing address

Billing phone number

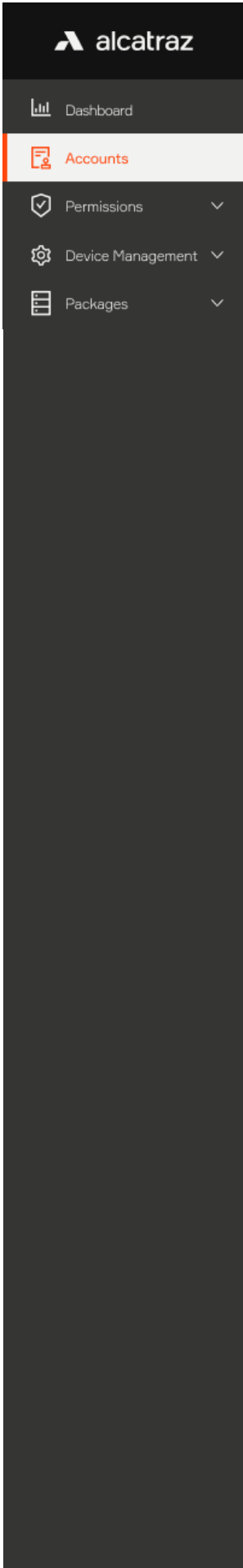
1808 El Camino Real

Billing phone number

Cancel

Submit





3.2—Edit an Account

- 1. Identify the Account from the list or search for the Account in the search bar.
- 2. Navigate to the far right, click on the three dots and select **Edit** to open up the **Edit Account** pane.
- 3. Update Account information and click **Submit**.

Home / Accounts

Accounts

micro

Q

⋮

<input type="checkbox"/>	Name	Reference Number	Devices	
<input type="checkbox"/>	Micro Squared	862548997	3	<div>⋮</div> <div>Edit</div>

Edit Account

Home / Account / Micro Squared

Account admin@microsquared.com

Delete

* Account name

Micro Squared

* E-mail

admin@microsquared.com

Reference Number

862548997

Country

United States

City

San Jose

ZIP Code

95129

Billing address

1808 El Camino Real

Billing phone number

Billing phone number

Active devices

3

Cancel

Submit →

1

2

3



3.3—View an Account

1. Identify the Account from the list or search for the Account in the search bar.
2. Click on the Account name or navigate to the far right, click on the three dots and select **View**.
3. The Account information page will be displayed.

Home / Accounts

Accounts

+ Create an Account

micro

Name

Reference Number

Devices

Micro Squared

862548997

3

...

Edit

View

Delete

Home / Account / Micro Squared

Account - Micro Squared admin@microsquared.com

Delete

Modify Account

Account Information

Account ID: 1997f750-0425-4bfa-a9bd-ea4f7793c985

Account Name: Micro Squared

Reference Number: 86254997

Active Devices

3

View all

Billing Contact Information

E-mail: admin@microsquared.com

Country: United States

City: Redwood City

Zip: 95129

Billing Address: San Jose

Billing Phone Number: N/A

Card Format Information

+ Create a Card Format

Name

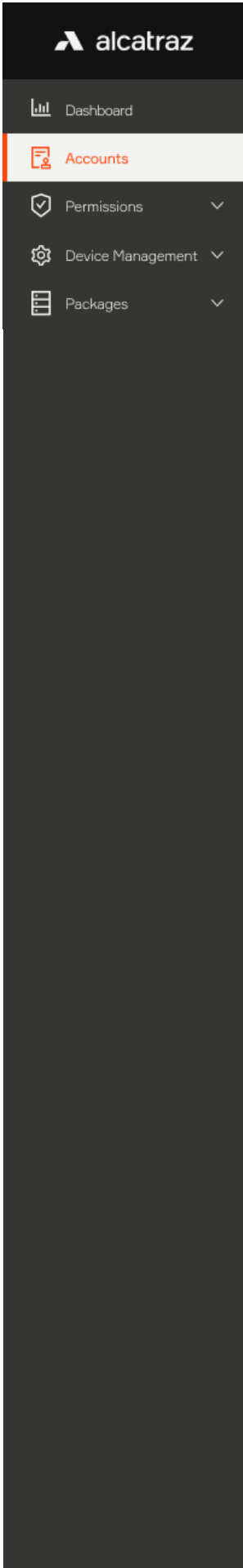
Custom

Number of Bits

No Data

Ver. 1.01

11



3.4—Delete an Account

- 1. Identify the Account from the list or search for the Account in the search bar.
- 2. Navigate to the far right, click on the three dots and select **Delete**.
- 3. Confirm the deletion.

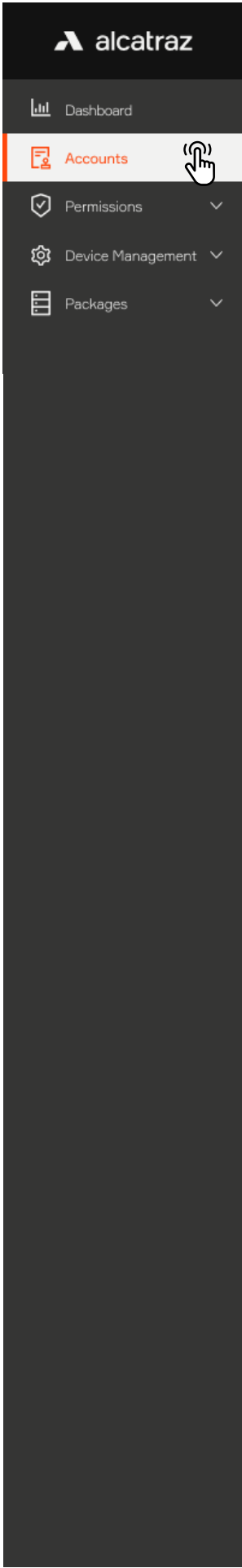
Note that only Dealer Admins can delete an account

The screenshot shows the 'Accounts' page in the Alcatraz Admin Portal. At the top, there's a breadcrumb 'Home / Accounts' and a '+ Create an Account' button. Below is a search bar with 'micro' entered and a search icon. A table lists accounts with columns for Name, Reference Number, and Devices. One account, 'Micro Squared', is listed with Reference Number '862548997' and '3' devices. To the right of the table, there's a three-dot menu. A hand cursor is clicking on the 'Delete' option in this menu. Below the table, a confirmation dialog box is shown. It has a yellow question mark icon and asks 'Are you sure you want to delete organizations with ID: 1f38aa03-0683-43f1-b6d3-ebef9455d7b4?!'. It also states 'Deleting a resource will permanently remove it from the system!'. At the bottom of the dialog are 'Cancel' and 'Confirm' buttons. Numbered callouts 1, 2, and 3 point to the search bar, the three-dot menu, and the 'Confirm' button respectively.

3.5—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.

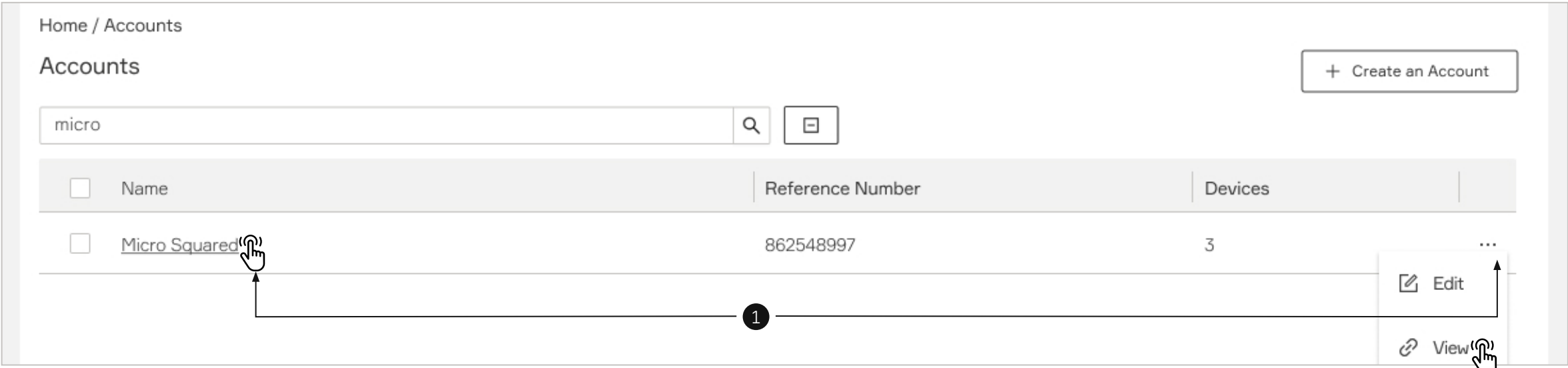




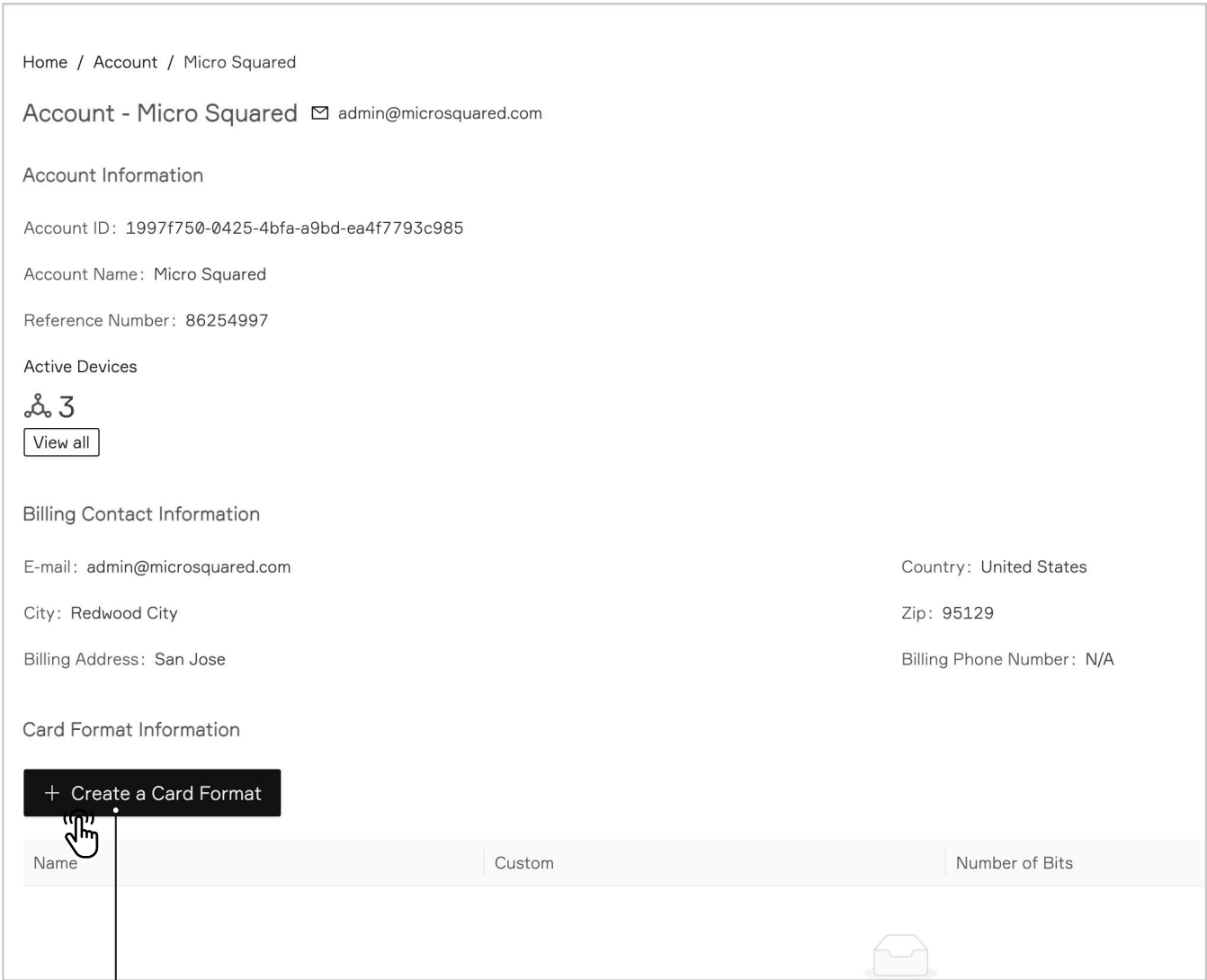
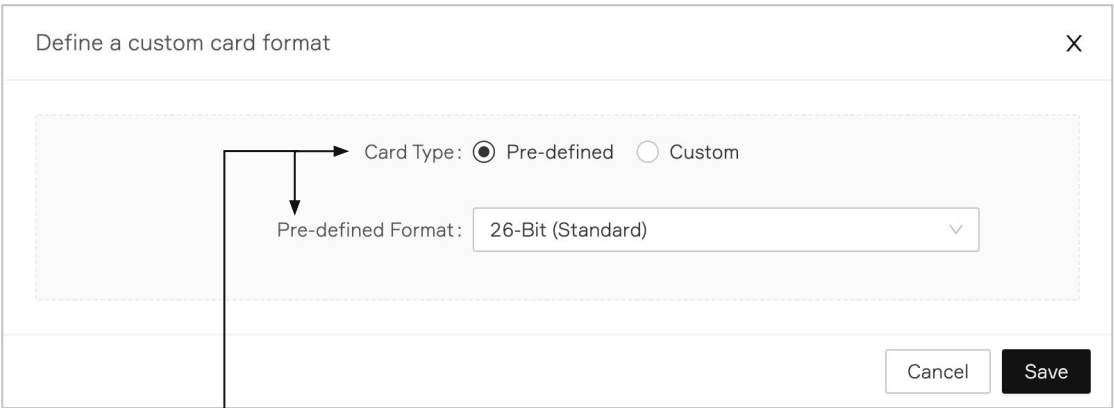
3.5.1—Configure a Pre-defined Card Format

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

1. Click on the Account name or navigate to the far right, click on the three dots and select **View**.



2. Select **Create a Card Format**
3. **Define a custom card format** pop-up window appears



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

Home / Account / Micro Squared

Account - Micro Squared

Account Information

Account ID: 1997f750-0425-4bfa-a5

Account Name: Micro Squared

Reference Number: 86254997

Active Devices

3

View all

Billing Contact Information

E-mail: admin@microsquared.com

City: Redwood City

Billing Address: San Jose

Country: United States

Zip: 95129

Billing Phone Number: N/A

Card Format Information

+ Create a Card Format

Name	Custom	Number of Bits
26-Bit	No	26

Define a custom card format

Card Type: ☒ Pre-defined ☐ Custom

Pre-defined Format: 26-Bit (Standard)

26-Bit (Standard)

34-Bit (Honeywell Quc 26-Bit (Standard)

35-Bit (Corporate 1000)

37-Bit (HID H10302)

37-Bit (HID H10304)

Save

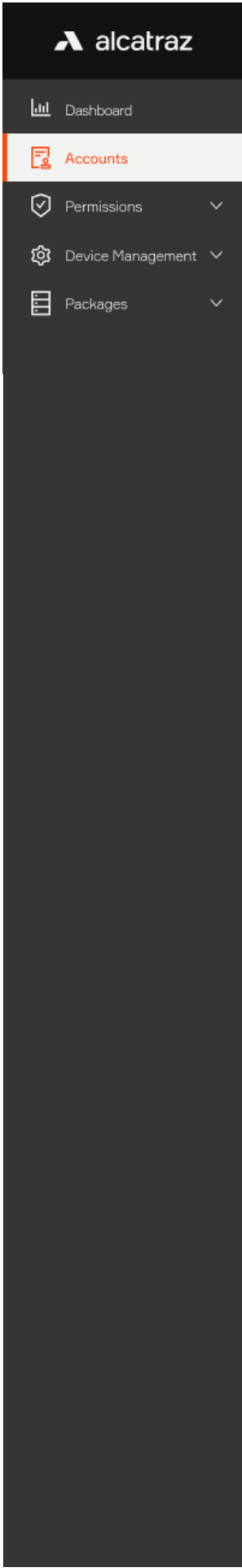
5

Card Information

+ Create a Card Format

Name	Custom	Number of Bits
26-Bit	No	26

Delete



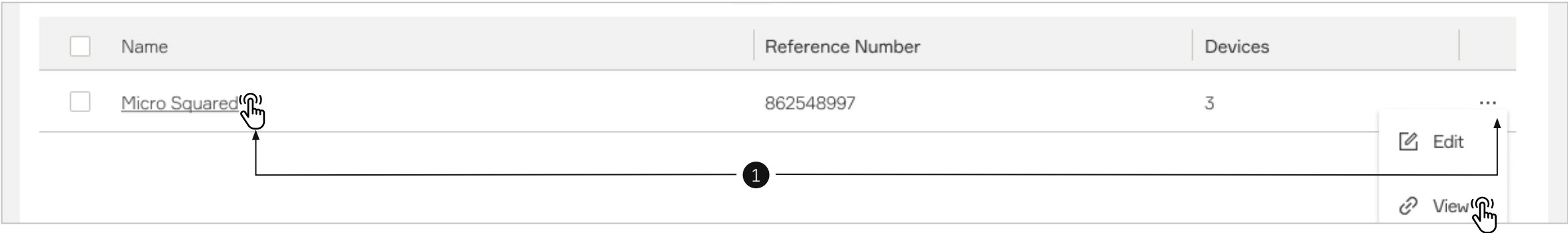
3.5.2—Configure a Custom Card Type

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

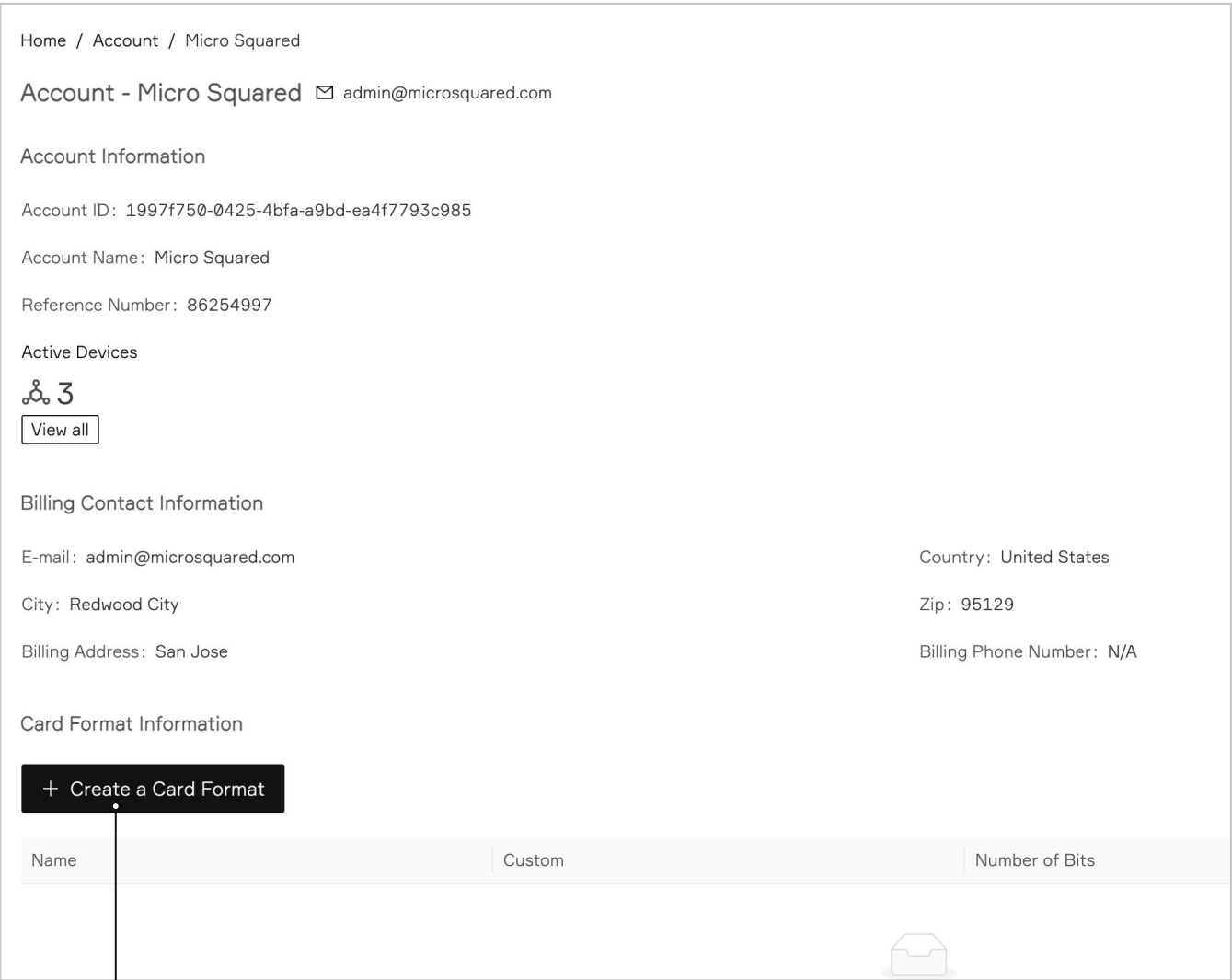
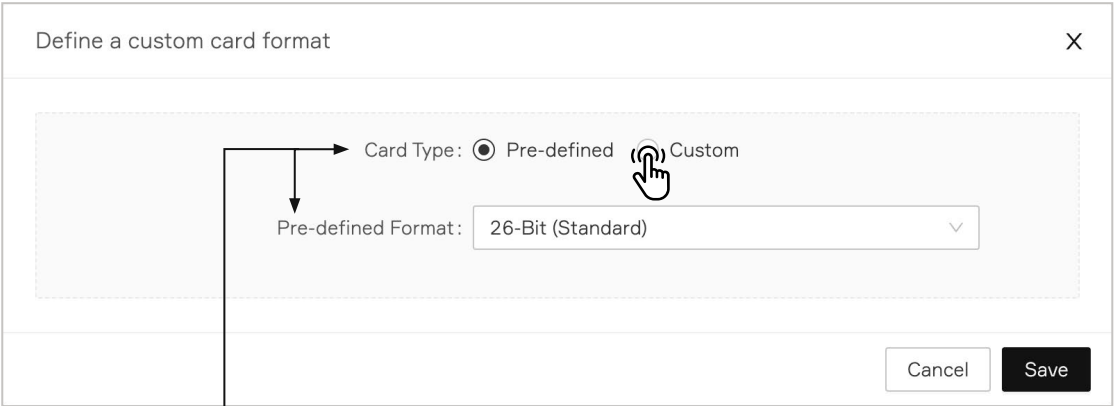
Information that may be part of your card format and needed as part of the configuration include:

- 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 Accounts and click on **View Account**



2. Select **Create a Card Format**
3. **Define a custom card format** pop-up window appears



Name	Custom	Number of Bits
------	--------	----------------



4. Select **Custom** for Card Type. 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.**
5. Follow the information retrieved from the ACS Administrator and toggle bits as required
6. Click **Save** when finished

Define a custom card format

X

Card Type: ☐ Pre-defined ☒ Custom

* Format Name:

* Number of Bits:

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

1

8

16

24

26

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

☐ Parity Enabled ☒ Even ☐ Odd

1

8

16

24

26

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

☐ Parity Enabled ☒ Even ☐ Odd

1

8

16

24

26

Legend

☐ Bit is not defined

☒ Card Number bit or Parity area (or set)

☒ Facility or Parity bit

Cancel

Save

3.5.3—Example of Card Format with No Parity Bits

Name:

Sample Format

(or [add](#) [clone](#) [rename](#))

Enabled: ☒

Description:

Data Format:

Wiegand

Length:

37

Facility Code:

2376

Facility Code Start:

1

Facility Code Length:

17

☐ Reverse bit order

Encoded # Start:

18

Encoded # Length:

19

☐ Reverse bit order

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	37			
N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	?			

Define a custom card format

Card Type: ☐ Pre-defined ☒ Custom

* Format Name:

Corp Format 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

Cancel

Save

Ver. 1.01

17

3.5.4—Example of Card Format Using Parity Bits

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

Define a custom card format

* Format Name:

* Number of Bits:

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

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

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

☐ Parity Enabled ☐ Even ☐ Odd

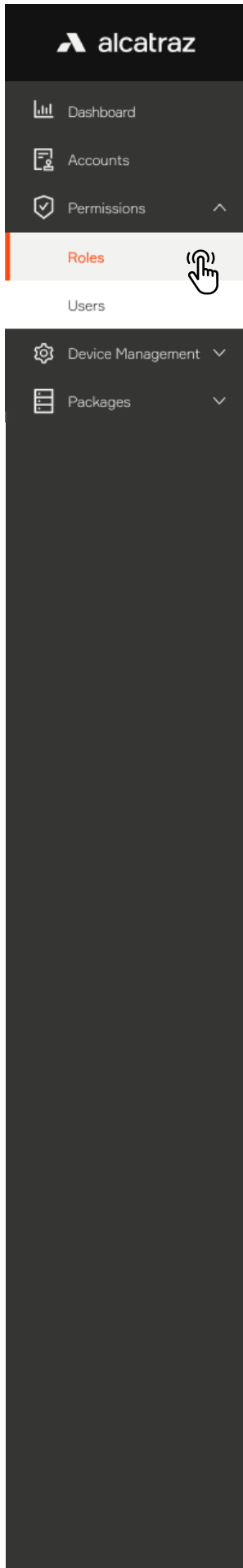
Legend

- ☐ Bit is not defined
- ☒ Card Number bit or Parity area (or set)
- ☒ Facility or Parity bit






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.

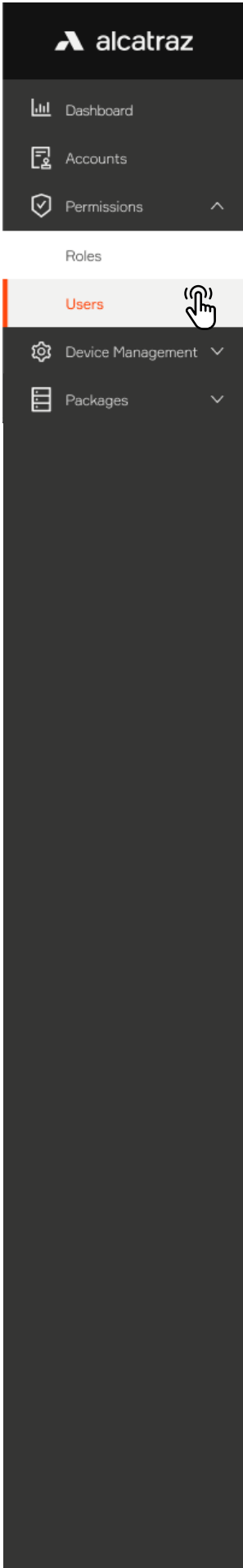
4.1—Create a User	21
4.2—Delete a User	22



Users are associated with an Account so the Account must be previously created in order to assign the user a role for an Account. This is important to note for **Dealer Admins** who must manage multiple Accounts.

Home / Permissions - Roles		
Permissions - Roles		
This page shows all available Roles on the Platform. Users with different access roles have different access to Platform resources.		
	<div>Dealer Admin</div> <p>A Dealer (System Integrator) Administrator has the highest privileges of any user within a Dealer's organization. The Dealer Administrator can Add/Edit/Delete any entities within the system integrator's account. The main role of the Dealer Administrator is to create and manage Accounts and Account Administrators. The Dealer Administrator will also create and manage Installers.</p>	View users assigned to this Role
	<div>Installer</div> <p>An Installer is provisioned privileges by a Dealer Administrator and may have access to one or more accounts. The Installer can Add/Edit/Delete any entities within the Accounts to which the Installer has been given access. The main role of the Installer is to physically install and commission the onsite products at the Account locations.</p>	View users assigned to this Role
	<div>Account Administrator</div> <p>An Account Administrator has the highest privileges of any user within an Accounts 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.</p>	View users assigned to this Role
	<div>Account Manager</div> <p>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.</p>	View users assigned to this Role
	<div>Account User</div> <p>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.</p>	View users assigned to this Role

Note: Only Dealer Admins and Installer roles are able to Delete Rocks from Accounts.



4.1—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 and the Account. If there is more than one Account, select the appropriate one
- 5. Click **Submit**

Home / Permissions - Users

Users

+ Create a User

Name	Email	Account	Access Level
------	-------	---------	--------------

Add User

Home / Permissions - Users

Create User

* User's name

John Smith

* User's E-mail

johnsmith@microsquared.com

* Login Password

.....

* Confirm Password

.....

* Role

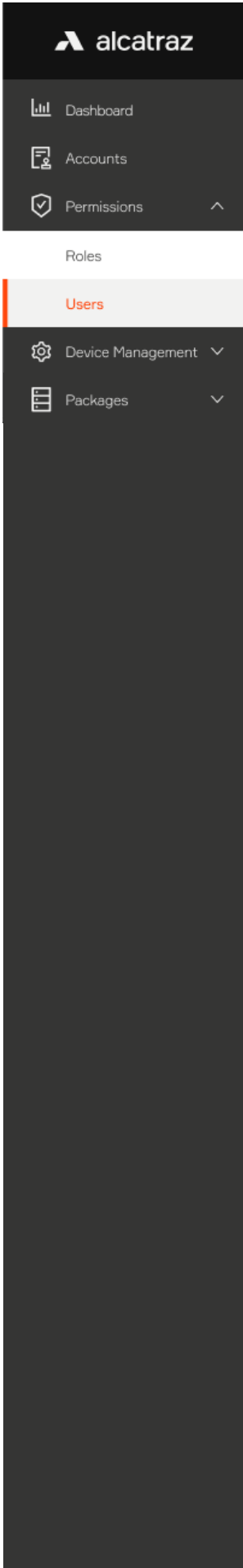
Installer

* Account

Micro Squared

Cancel Submit →





4.2—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

Home / Permissions - Users

Users

+ Create a User

Filter by Role

Name	Email	Account	Access Level	
JS John Smith	johnsmith@microsquared.com	Micro Squared	Installer	<div><div>...</div><div>Edit</div><div>View</div><div>Delete</div></div>

!

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!

Cancel

Confirm



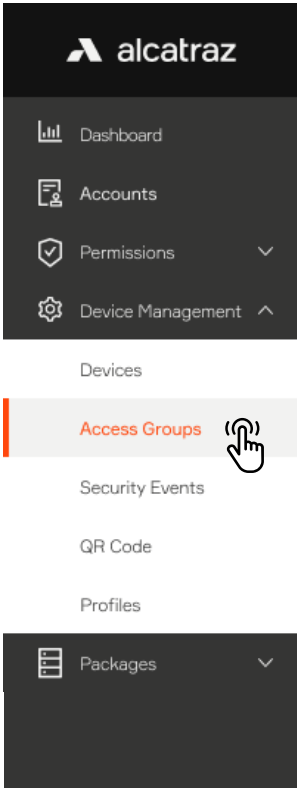
5 — Onboard a Rock

Newly installed Rocks will need to be onboarded and assigned an Access Group. Onboarding a Rock associates the Rock with the server where the Alcatraz AI Admin Portal is hosted and also requires that the Rock be assigned an Access Group during this process.

For Cloud-Hosted Rocks, the server is maintained by Alcatraz.
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.
 - Find out the Access Groups to assign to the Rock(s).
 - Make a list of the Device ID for each Rock to be onboarded and associate the Rock with the Access group. 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.
- 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—Verify Existing Site or Create a New Site	24
5.2—Find the Rock to Onboard by Search	24
5.3—Authenticate the Device	24
5.4—Name the Device	25



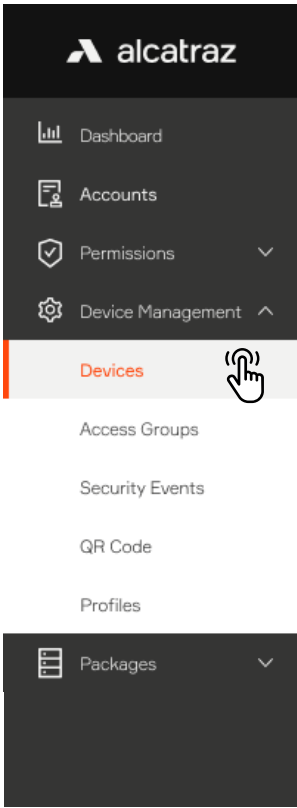
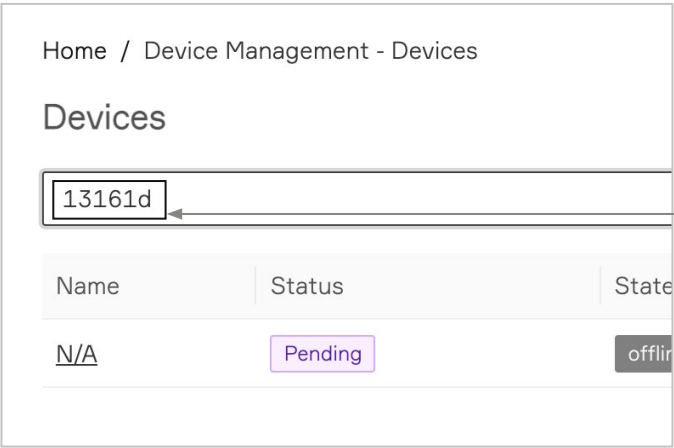
5.1—Assigning the Rock an Access Group

It is not necessary to create a new access group for onboarding. If none is specified during onboarding, the Rock will be assigned the default access group that can be changed after it has been onboarded.

To check for an existing or default Access Group, or create a new Access Group, go to [Access Groups](#).

5.5—Find the Rock to Onboard by Search

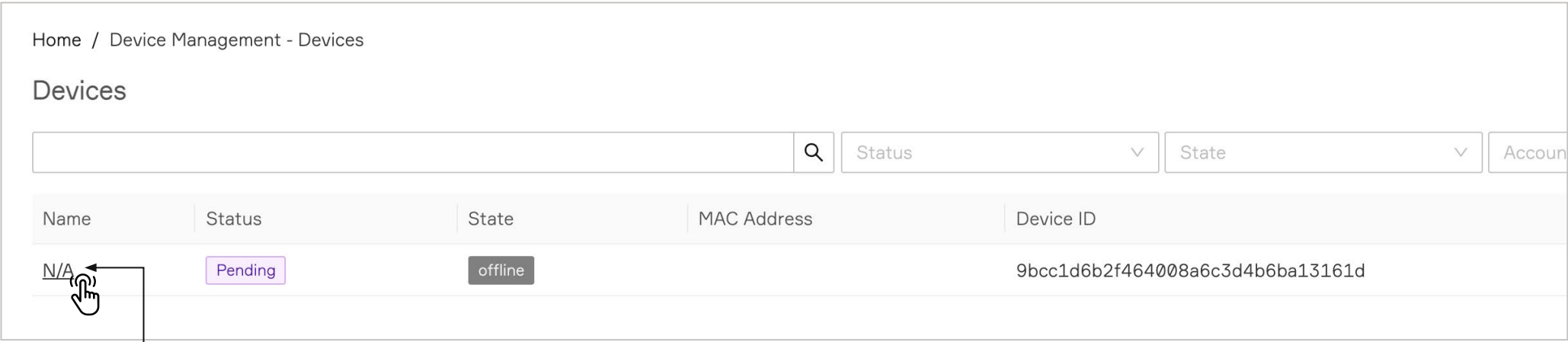
1. Enter the 6 digit Device ID in the search bar to filter the Rock. The 6 digit Device ID can be found:
 - On the outside of the package the Rock was shipped in (indicated by ID, as seen on label here)
 - On the back of the Rock under the QR code (indicated by ID)
 - On the Rock's display at the beginning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

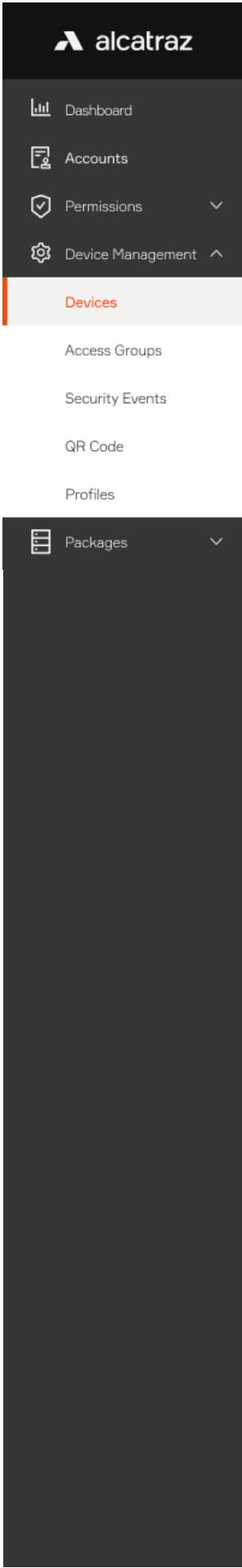


5.6—Authenticate the Device

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.





- 3. Click on **Authenticate**
- 4. A window pops open, choose the Access Group and click **Authenticate**.

This screenshot shows the 'Device - 9bcc1d6b2f464008a6c3d4b6ba13161d' page in the Alcatraz application. The device status is 'Pending'. A purple 'Authenticate' button and a red 'Delete' button are visible. An arrow points from the 'Authenticate' button to a modal dialog box titled 'Authenticate'. The dialog box contains the text 'Authenticate this device', a dropdown for 'Access Group' set to 'Employees', and another dropdown for 'Reader' set to 'Reader'. At the bottom of the dialog are 'Cancel' and 'Authenticate' buttons. A red circle with the number '3' is placed over the 'Authenticate' button in the dialog. Another red circle with the number '3' is placed over the 'Authenticate' button in the main interface.

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

Home / Device Management - Devices					
Devices					
Search devices... <input type="text"/>					
Status <input type="text"/> State <input type="text"/> Account <input type="text"/>					
Name	Status	State	MAC Address	Device ID	
N/A	Active	online	c0:9b:f4:90:05:74	9bcc1d6b2f464008a6c3d4b6ba13161d	...

5.4—Name the Device

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

This screenshot shows the 'Devices' table from the previous screenshot. A hand cursor is clicking on the 'N/A' value in the 'Name' column. A red circle with the number '1' is placed over the hand cursor.



alcatraz

Dashboard

Accounts

Permissions

Device Management

Devices

Access Groups

Security Events

QR Code

Profiles

Packages

2. The Rock's information will be displayed. Click on **Modify Device**.

3. Modify the Name field

Home / Device Management - Devices / 9bcc1d6b2f464008a6c3d4b6ba13161d

Device - 9bcc1d6b2f464008a6c3d4b6ba13161d Active

Device Information

Device ID: 9bcc1d6b2f464008a6c3d4b6ba13161d

Modify Device

Delete

Home / Device Management - Devices / 9bcc1d6b2f464008a6c3d4b6ba13161d

Modify Device Parameters Delete

Device Information

Device ID

9bcc1d6b2f464008a6c3d4b6ba13161d

Default access group

North Campus Labs

Name

Lab M12 - IDF Rm 201

Reader

Reader

4. Click **Submit** at the bottom of the page.

5. View the new Name in the list

Home / Device Management - Devices

Devices

Search devices...

Q

Status

State

Account

Name	Status	State	MAC Address	Device ID
Lab M12 - IDF Rm 201	Active	online	c0:9b:f4:90:05:74	9bcc1d6b2f464008a6c3d4b6ba13161d

Ver. 1.01

26

6 —

Device Management

6.1—Devices	28	6.2—Access Groups	52
6.1.1—Configure Rock Mode of Operation	29	6.2.1—Create an Access Group	52
6.1.1.1—Mode Setting – Demo	31	6.2.2—Delete an Access Group	53
6.1.1.2—Mode Setting – 1FA	31	6.2.3—Embedded Access Groups	54
6.1.1.3—Mode Setting – 1FAF	32	6.2.4—Change Default Access Group	55
6.1.1.4—Mode Setting – 2FA-M	32	6.2.5—Add Additional Access Groups	56
6.1.1.6—Mode Setting – 2FA	33	6.3—Security Events	57
6.1.1.5—Operating in 3FA	33	6.3.1—Viewing Security Events	57
6.1.1.7—Mode Setting – Enrollment	34	6.3.2—Security Events Summary Table	58
6.1.1.8—Changing Badges	35	6.4—Generate QR Code	60
6.1.2—LED Control	36	6.4.1—Server Location	62
6.1.3—ONVIF	38	6.4.2—Generate and Download QR Code	63
6.1.3.1—Adding a Rock to the VMS	40	6.4.3—Present QR Code to the Rock’s Camera	64
6.1.4—HOLD Signal Detection	40	6.4.4—When can the Rock read a QR code?	64
6.1.5—Configure ACS Alerts	42	6.5—Profiles	65
6.1.6—Configure OSDP	45	6.5.1—Viewing Profiles	66
6.1.6.1—Select Rock to Configure OSDP	46	6.5.2—Delete a Profile – Option 1 (delete through Profiles)	68
6.1.6.2—Rock Communication with Badge Reader	48	6.5.3—Delete a Profile – Option 2 (delete through Security Event)	69
6.1.6.3—Rock Communication with ACS	49	6.5.4—Managing Access	70
6.1.6.4—Changing from Secure to Unsecure Channel	50	6.5.5—Troubleshooting Tips	72
6.1.6.5—Troubleshooting Tips	51		
6.1.6.6—Wiring Details	51		

6.1—Devices

The Rock can operate in a number of modes.

Device Mode	Description
Demo mode	<ul style="list-style-type: none">■ 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.
1FA	<ul style="list-style-type: none">■ 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.■ Auto-enrollment is enabled by default in 1FA. This 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.
1FAF	<ul style="list-style-type: none">■ 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.
2FA	<ul style="list-style-type: none">■ Two Factor Authentication requires face and badge as the credentials.■ Enrollment is completed at an enrollment station, often located at the Security Operations Office.■ Also the mode to select when requiring users to enter a PIN. Rock will require face + badge and send user entered PIN to Access Control System (ACS). ACS must be configured to accept Badge + PIN.
2FA-M	<ul style="list-style-type: none">■ 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	<ul style="list-style-type: none">■ 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.



alcatraz

Dashboard

Accounts

Permissions

Device Management

Devices

Access Groups

Security Events

QR Code

Profiles

Packages

6.1.1—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 Device** to open up the configurations page.

Home / Device management - Devices

Device Management - Devices

Search devices...

Status

State

Account

Name	Status	State	MAC Address	Device ID	
Lab M12 - IDF Rm 201	Active	online	c0:9b:f4:90:05:74	9bcc1d6b2f464008a6c3d4b6ba13161d	...
MS Lab	Active	online	c0:9b:f4:90:04:51	c582962c39ac46e7b7d26815d3468244	...

Home / Device Management - Devices / MS Lab

Device - MS Lab Active

Modify Device

Delete

Device Information

ID: 60ed22c756ca57e169bb1ace

Device ID: 003bef414c9d43e9a55203514ec5574d

Device status: online

Name: MS Lab

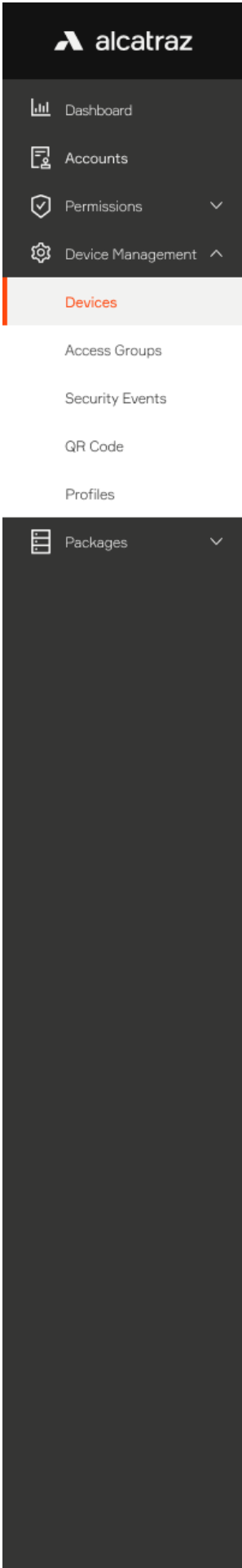
MAC address: c0:9b:f4:90:05:74

IP address: 10.5.69.83/23

Default access group: Default Access Group

Access groups: [TopLevel](#)





- 4. Scroll down the page to **Device Configuration** and expand the **Device Mode** section.
- 5. Select the operational mode for the Rock.
- 6. Click **Submit** when done.

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.

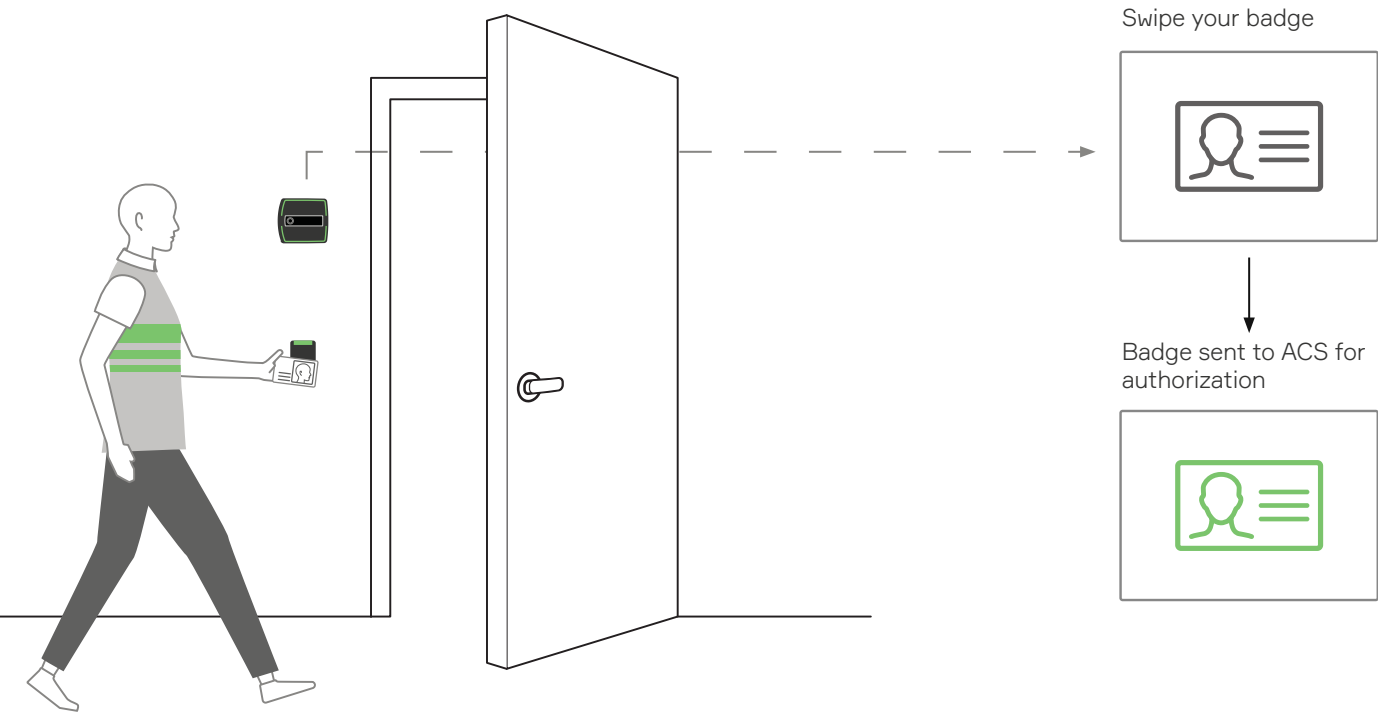
The 'Device Configuration' form is shown with the 'Device Mode' section expanded. A dropdown menu for 'Select Mode:' is open, showing options: '1FA', 'Demo mode', '1FAF', '2FA', '2FA - M', and 'Enrollment'. A hand icon points to the '1FA' option in the dropdown. To the right of the dropdown, there are radio buttons for 'Low Friction', 'Standard' (which is selected), and 'High Security'. A circled '5' with an arrow points to the 'Standard' radio button. Below the radio buttons, there is a text label: 'for facial authentication or a badge. Auto enrollment is enabled by default.' At the bottom of the form, there are 'Cancel' and 'Submit ->' buttons. A circled '6' with an arrow points to the 'Submit ->' button. The 'Advanced' toggle switch is turned off in the top right corner of the form.

6.1.1.1—Mode Setting – Demo

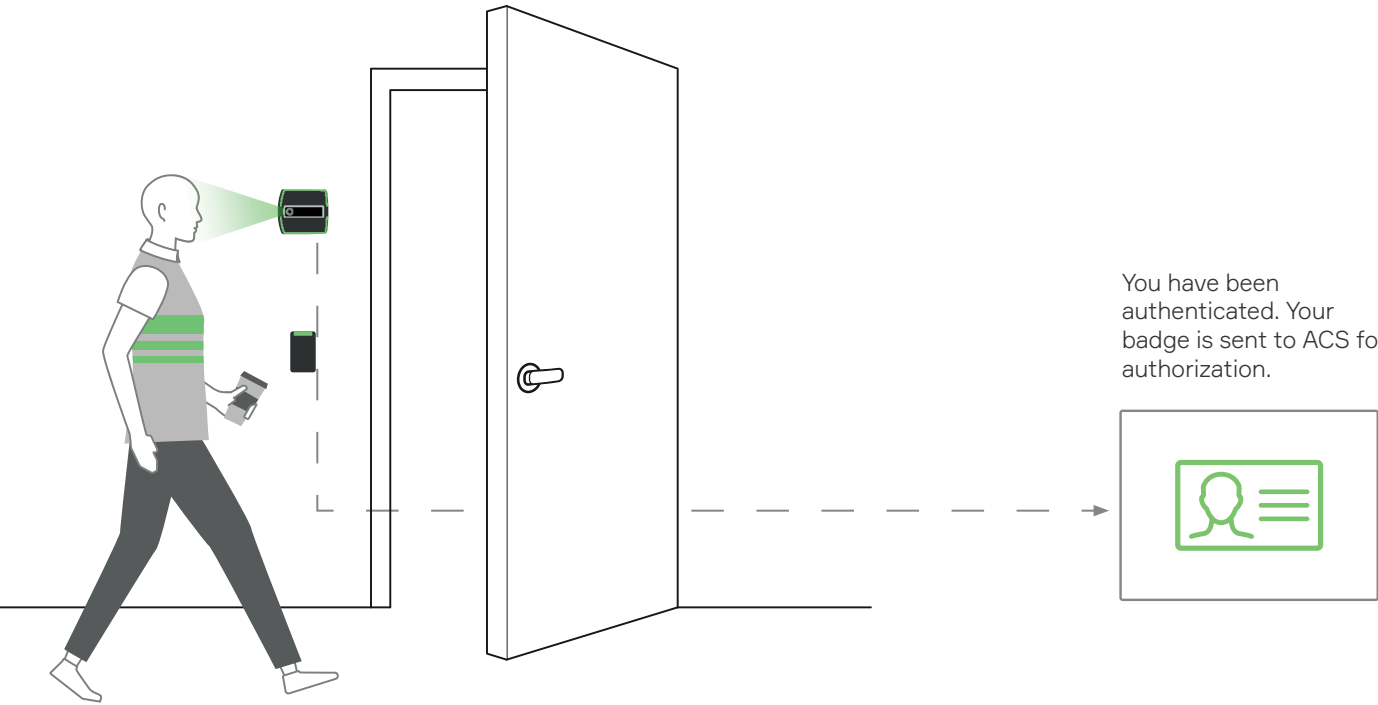
The Rock is shipped in Demo mode. In Demo mode, auto-enrollment is completed by swiping a badge twice with a few seconds in between. On the third entry, you will not be required to present your badge as the Rock will authenticate by facial credential.

Auto-Enrollment

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



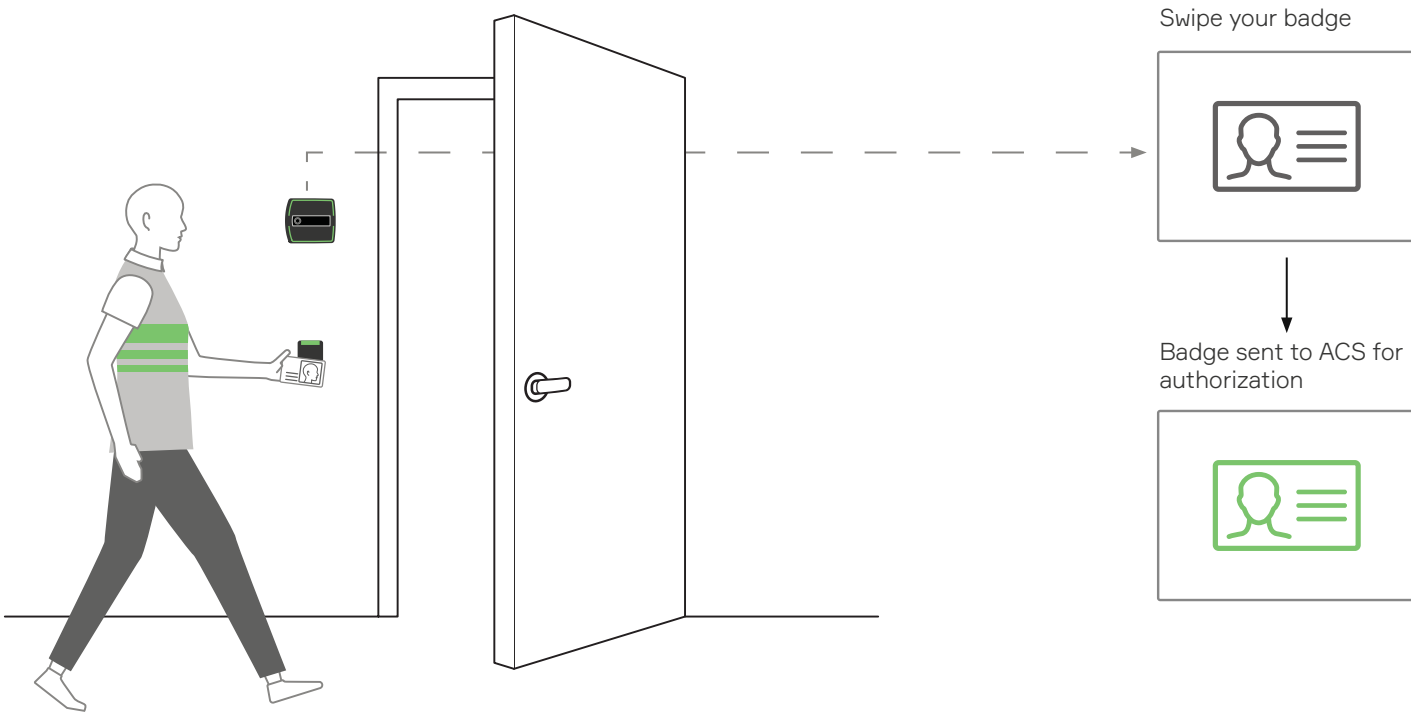
You have completed auto-enrollment. No badge is required, simply look at the Rock as you approach the door.



6.1.1.2—Mode Setting – 1FA

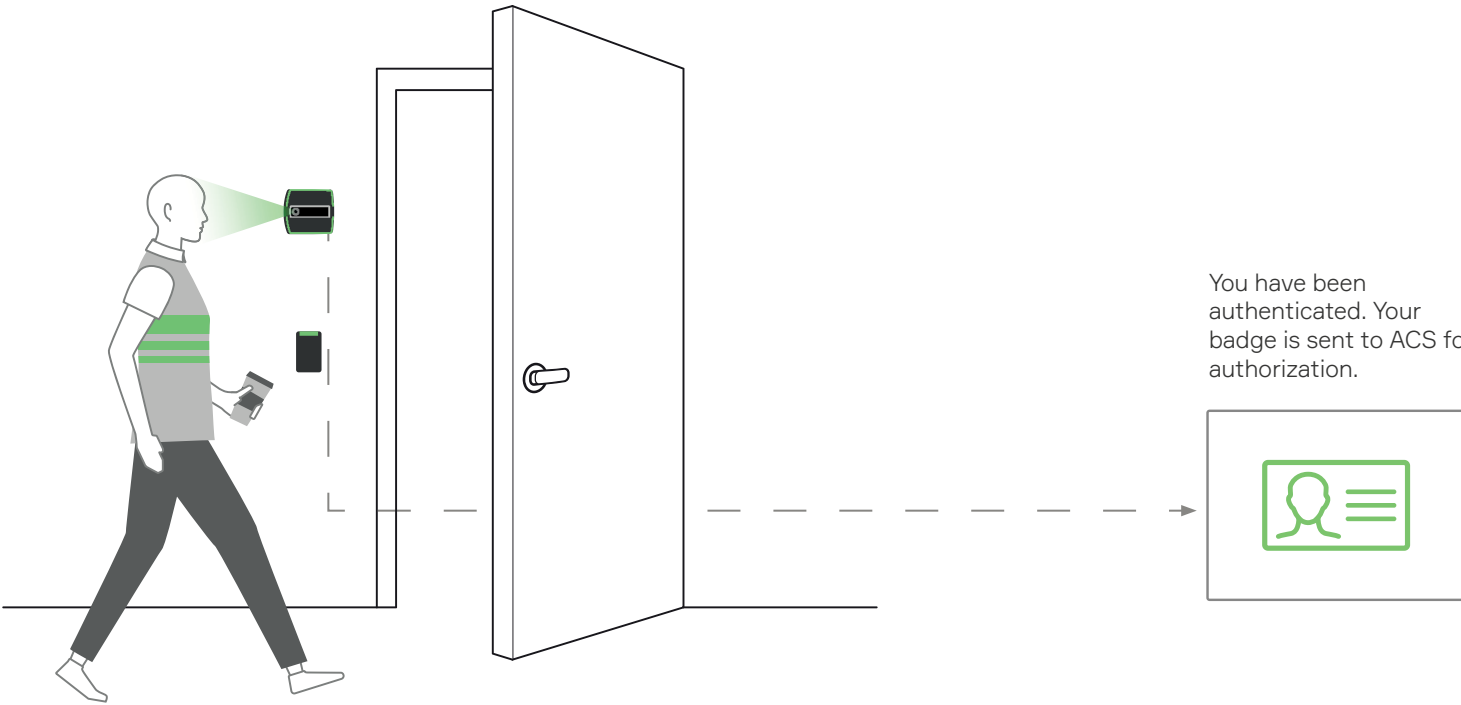
Auto-Enrollment

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.

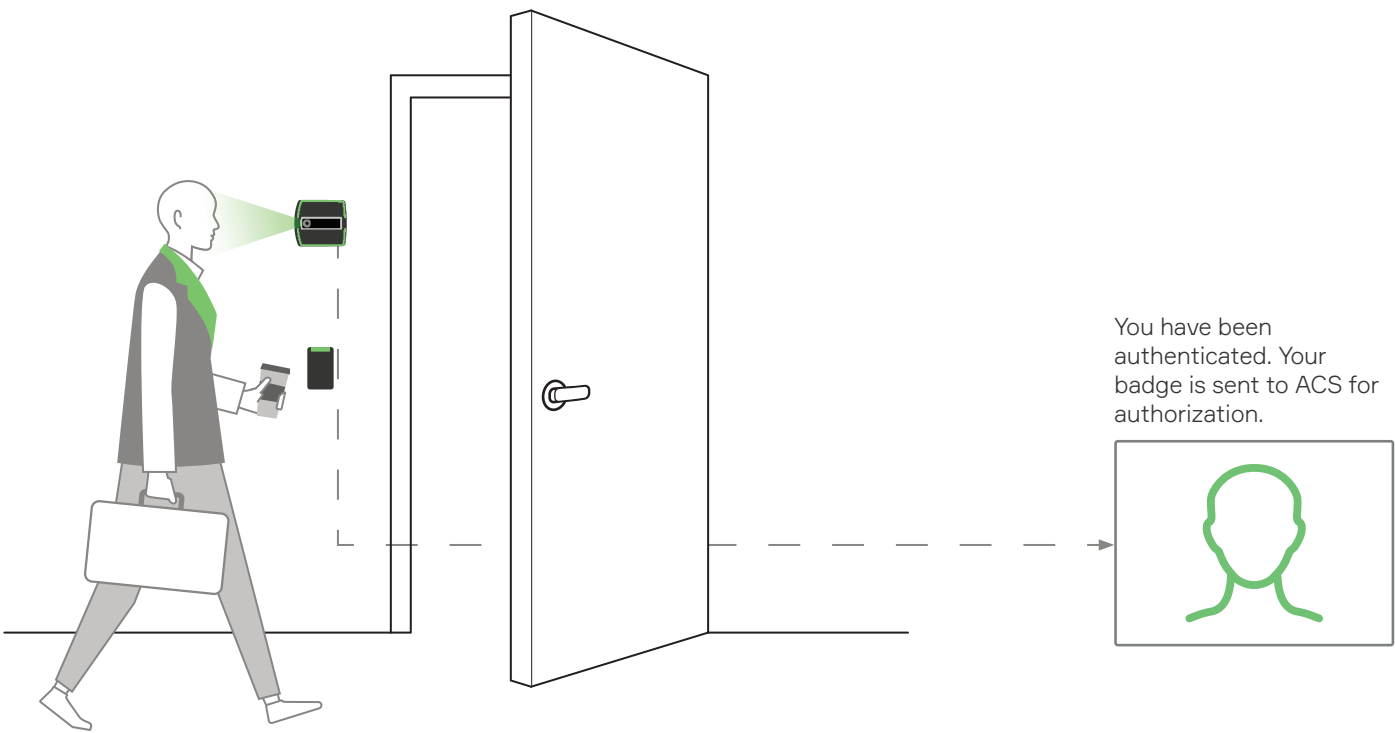


6.1.1.3—Mode Setting – 1FAF

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

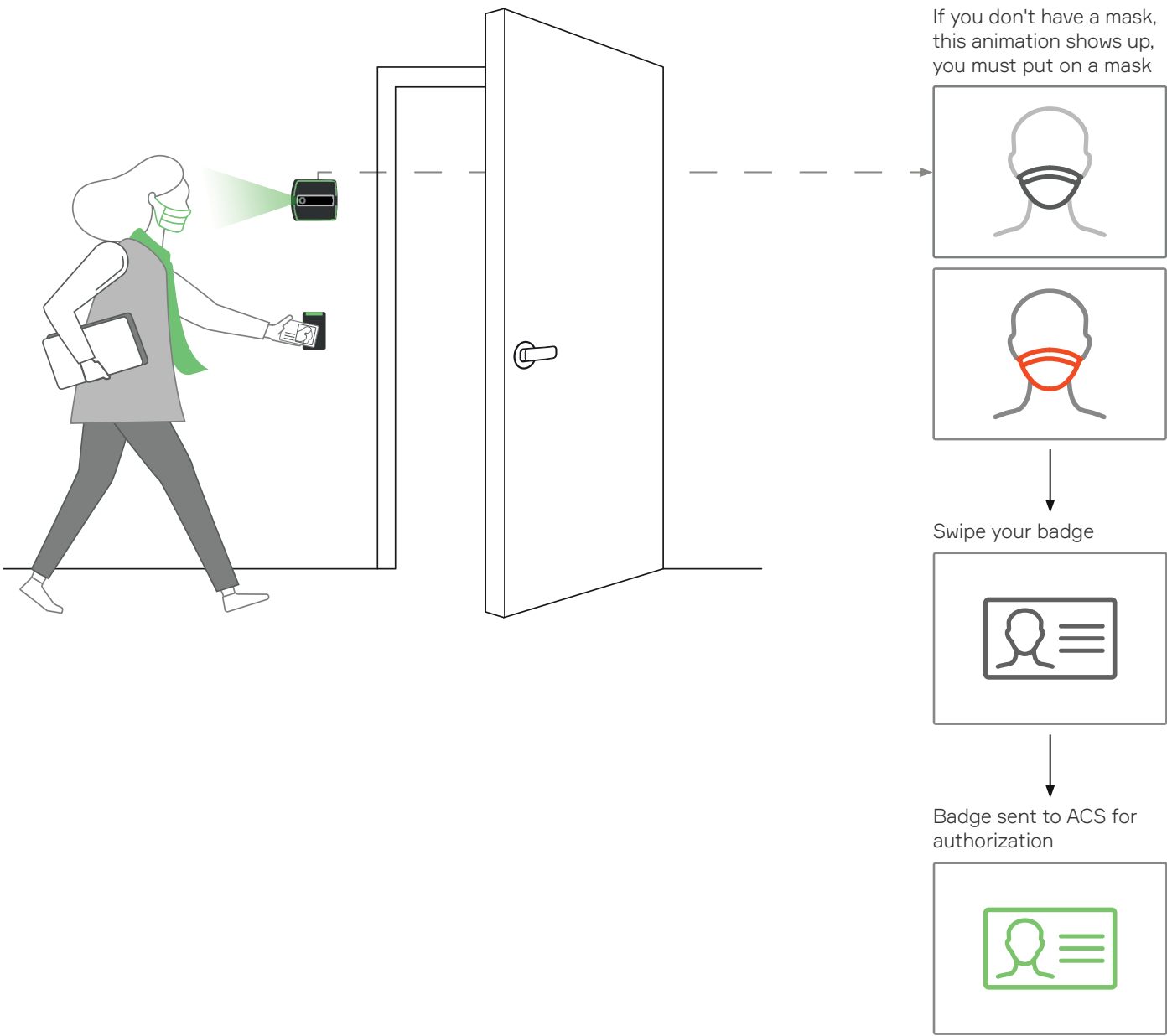
Single Factor Authentication

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



6.1.1.4—Mode Setting – 2FA-M

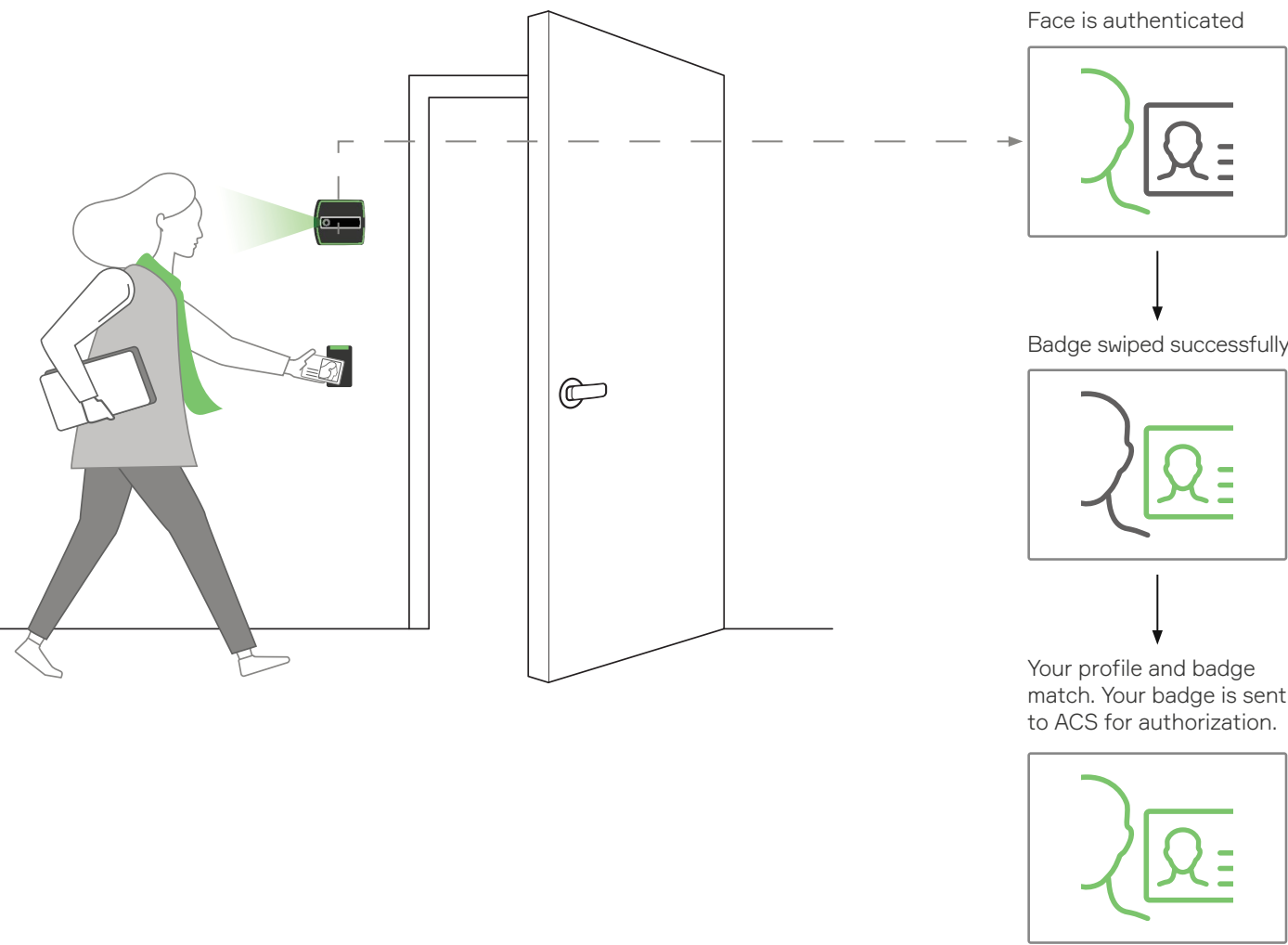
This Rock is in Mask Enforcement mode.
This mode requires you to wear a mask and present your badge.
No enrollment is required.
*If you are not wearing a mask when approaching the door, you must put one on before swiping your badge.



6.1.1.6—Mode Setting – 2FA

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

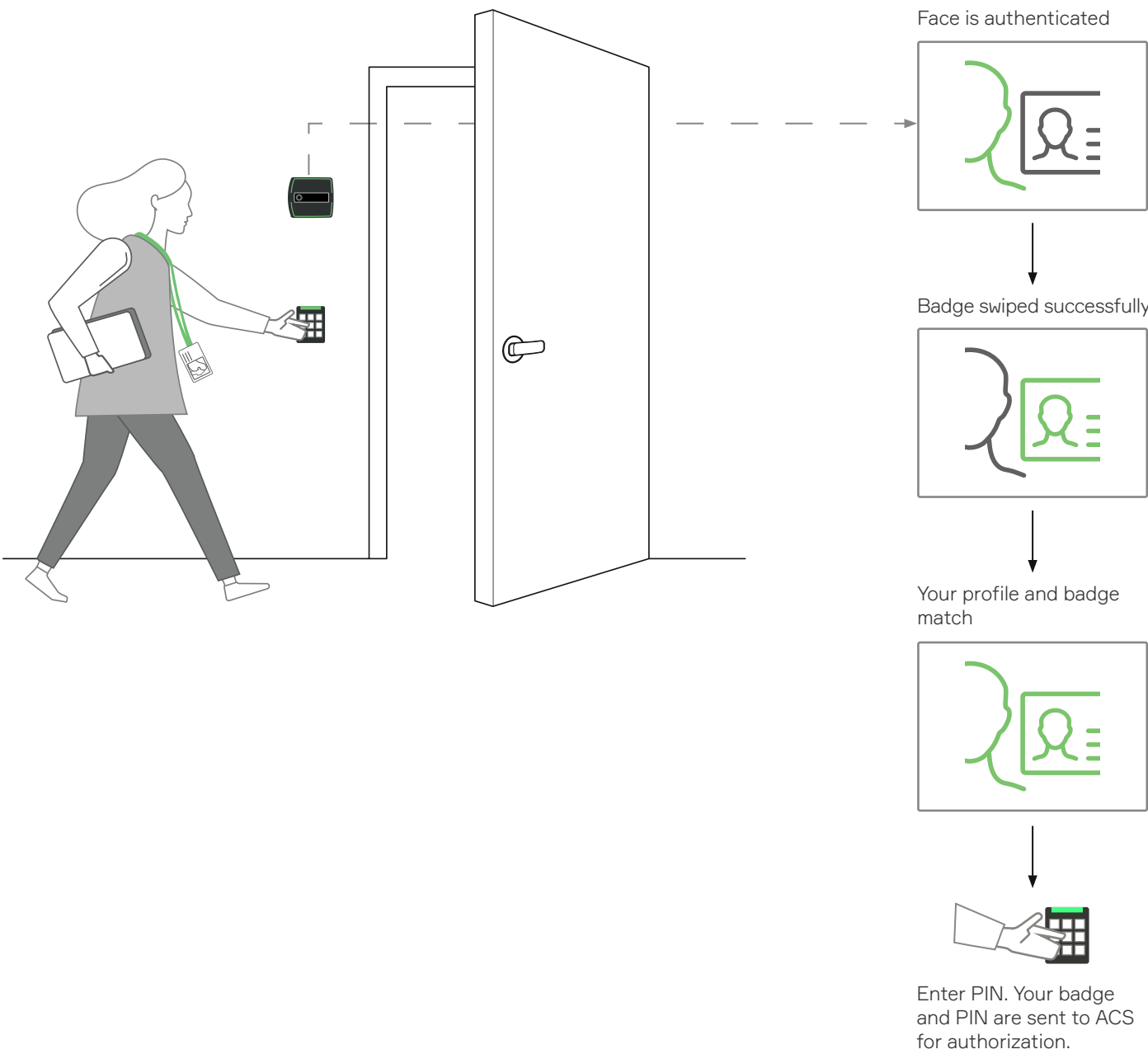
You have completed enrollment at an enrollment station. As you approach the door and badge in, the Rock captures your face and will verify if your face and your badge match.



6.1.1.5—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.

Select Mode = 2FA



Your ACS must be configured to accept badge and PIN.

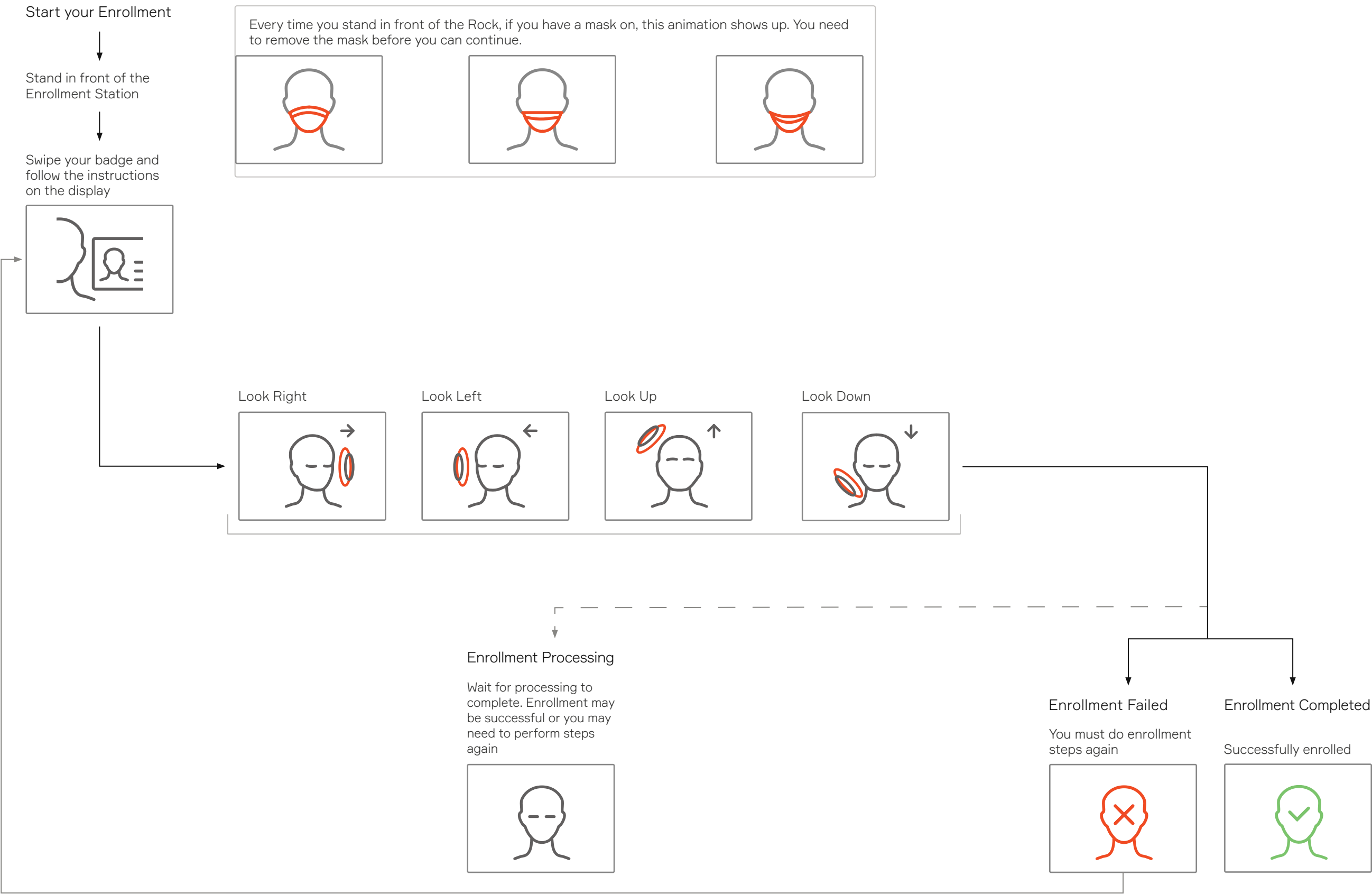
Seeing this on the Rock's display?

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



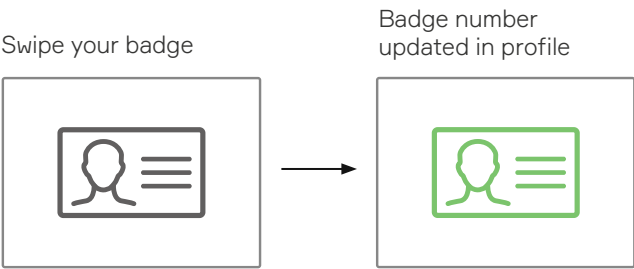
6.1.1.7—Mode Setting – Enrollment

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.



6.1.1.8—Changing Badges

Once a user is enrolled, if at any time, the user needs to switch to a new badge, they can walk up to an enrollment Rock and swipe their new badge to update their profile.



alcatraz

Dashboard

Accounts

Permissions

Device Management

Devices

Access Groups

Security Events

QR Code

Profiles

Packages

Old Badge number in profile

Access Details				+ Add Access
Badge Number	Facility Code	Access Group	Action	
232217	37	Lab Technicians	...	

New Badge number in profile

Access Details				+ Add Access
Badge Number	Facility Code	Access Group	Action	
44324	37	Lab Technicians	...	



alcatraz

Dashboard

Accounts

Permissions

Device Management

Devices

Access Groups

Security Events

QR Code

Profiles

Packages

6.1.2—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 Device** to open the configurations page.

Home / Device management - Devices

Device Management - Devices

Search devices...

Status

State

Account

Name	Status	State	MAC Address	Device ID	
Lab M12 - IDF Rm 201	Active	online	c0:9b:f4:90:05:74	9bcc1d6b2f464008a6c3d4b6ba13161d	...
MS Lab	Active	online	c0:9b:f4:90:04:51	c582962c39ac46e7b7d26815d3468244	...

Home / Device Management - Device / MS Lab

Device - MS Lab Active

Modify Device

Delete

Device Information

Device ID: c582962c39ac46e7b7d26815d3468244

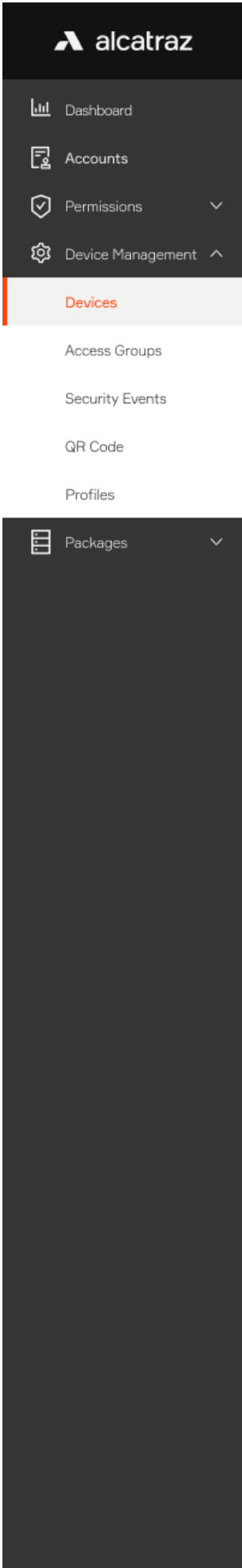
Device status: online

Name: MS Lab

MAC Address: c0:9b:f4:90:04:51

IP Address: 10.5.69.111/23





- 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.
 - c. Rock controls LEDs – LED color is controlled by the Rock. LEDs will turn blue then green for badging and authentication event. It will also display purple for a person who has completed auto-enrollment.
- 6. Click **Submit** when done

The image shows the 'Device configuration' page in the Alcatraz interface. At the top right is an 'Advanced' toggle switch. The main content area has several expandable sections: 'Device Mode', 'LED Control', 'ONVIF', 'Hold Signal Detection', 'ACS Alerts', 'Communication with ACS', and 'Communication with Badge reader'. The 'LED Control' section is expanded, showing three radio button options: 'ACS controls LEDs' (selected), 'ACS guides LEDs', and 'Rock controls LEDs'. Each option has a descriptive text block. At the bottom left are 'Cancel' and 'Submit' buttons. Numbered callouts 4, 5, and 6 point to the 'LED Control' section, the selected 'ACS controls LEDs' option, and the 'Submit' button respectively.

Device configuration Advanced ☐

> Device Mode

▼ 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.

> ONVIF

> Hold Signal Detection

> ACS Alerts

> Communication with ACS

> Communication with Badge reader

Cancel **Submit** →



alcatraz

Dashboard

Accounts

Permissions

Device Management

Devices

Access Groups

Security Events

QR Code

Profiles

Packages

6.1.3—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 Device** to open up the configurations page.

Home / Device management - Devices

Device Management - Devices

Search devices...

Status

State

Account

Name	Status	State	MAC Address	Device ID	
Lab M12 - IDF Rm 201	Active	online	c0:9b:f4:90:05:74	9bcc1d6b2f464008a6c3d4b6ba13161d	...
MS Lab	Active	online	c0:9b:f4:90:04:51	c582962c39ac46e7b7d26815d3468244	...

Home / Device Management - Device / MS Lab

Device - MS Lab

Active

Device Information

Device ID: c582962c39ac46e7b7d26815d3468244

Device status: online

Name: MS Lab

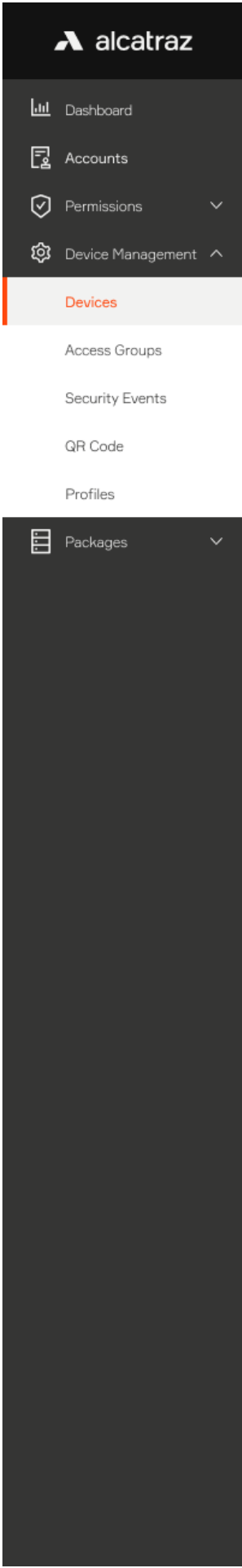
MAC Address: c0:9b:f4:90:04:51

IP Address: 10.5.69.111/23

Modify Device

Delete





4. Scroll down the page to **Device Configuration** and expand the **ONVIF** section.
ONVIF is enabled by default. To disable, click on the slider.

Device Configuration

Advanced ☐

> Device Mode

> LED Control

> ONVIF

> Hold Signal Detection

> ACS Alerts

> Communication with ACS

> Communication with Badge reader

Cancel

Submit →

4

Default setting

▼ ONVIF

Enable ONVIF ⓘ ☒

> Hold Signal Detection

> ACS Alerts

> Communication with ACS

> Communication with Badge reader

Cancel

Submit →

To disable

▼ ONVIF

Enable ONVIF ⓘ ☐

> Hold Signal Detection

> ACS Alerts

> Communication with ACS

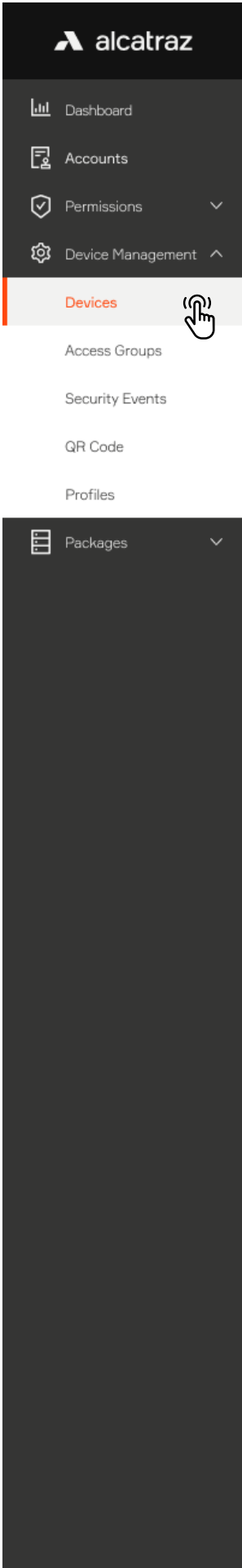
> Communication with Badge reader

Cancel

Submit →

5. Click **Submit** when done





6.1.3.1—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 and take the last 6 digits of the Device ID as the password.

Home / Device management - Devices

Device Management - Devices

Name	Status	State	MAC Address	Device ID	
Lab M12 - IDF Rm 201	Active	online	c0:9b:f4:90:05:74	9bcc1d6b2f464008a6c3d4b6ba13161d	...
MS Lab	Active	online	c0:9b:f4:90:04:51	c582962c39ac46e7b7d26815d3468244	...

2

6.1.4—HOLD Signal Detection

The HOLD signal works for both Wiegand and 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 Device** to open up the configurations page.

Name	Status	State	MAC Address	Device ID	
Lab M12 - IDF Rm 201	Active	online	c0:9b:f4:90:05:74	9bcc1d6b2f464008a6c3d4b6ba13161d	...
MS Lab	Active	online	c0:9b:f4:90:04:51	c582962c39ac46e7b7d26815d3468244	...

2

Home / Device Management - Device / MS Lab

Device - MS Lab Active

3



alcatraz

Dashboard

Accounts

Permissions

Device Management

Devices

Access Groups

Security Events

QR Code

Profiles

Packages

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. The Rock will suspend all operations when a Hold signal is asserted from the ACS.

6. Click **Submit** when done

Device Configuration

Advanced

> Device Mode

> LED Control

> ONVIF

> Hold Signal Detection

> ACS Alerts

> Communication with ACS

> Communication with Badge reader

Cancel

Submit

Default setting

Hold Signal Detection

Allow Hold Signal Detection

> ACS Alerts

> Communication with ACS

> Communication with Badge reader

Cancel

Submit

To enable

Hold Signal Detection

Allow Hold Signal Detection

> ACS Alerts

> Communication with ACS

> Communication with Badge reader

Cancel

Submit



6.1.5—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

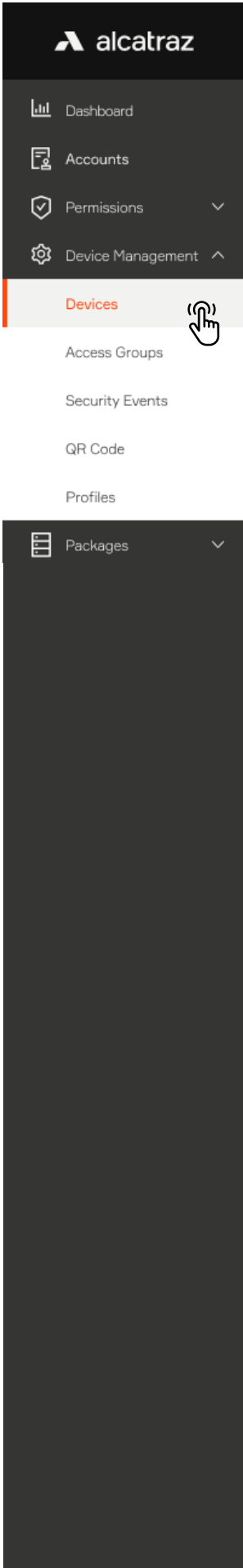
Use the following table to gather info for the alert(s) to configure:

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

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.





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 Device** to open up the configurations page.
- 4. Scroll down the page to **Device Configuration** and expand the **ACS Alerts** section.

Name	Status	State	MAC Address	Device ID	
Lab M12 - IDF Rm 201	Active	online	c0:9b:f4:90:05:74	9bcc1d6b2f464008a6c3d4b6ba13161d	...
MS Lab	Active	online	c0:9b:f4:90:04:51	c582962c39ac46e7b7d26815d3468244	...

Home / Device Management - Device / MS Lab

Device - MS Lab Active

Device Information

Device ID: c582962c39ac46e7b7d26815d3468244

Device status: online

Modify Device Delete

Device Configuration Advanced ☐

> Device Mode

> LED Control

> ONVIF

> Hold Signal Detection

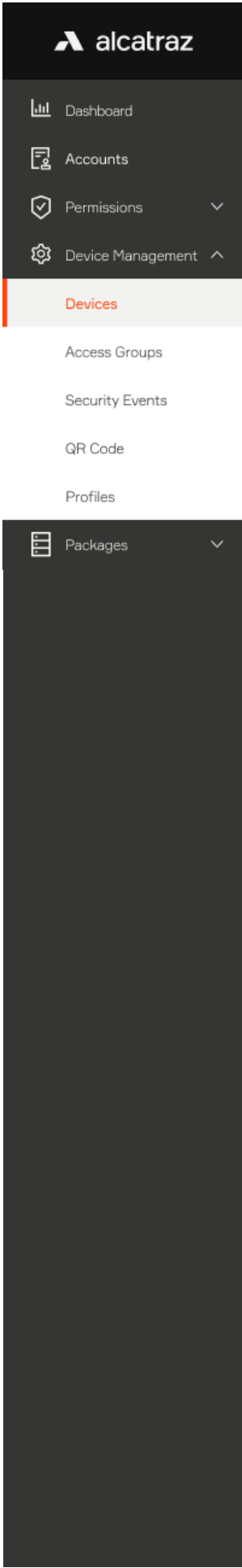
> ACS Alerts

> Communication with Badge reader

> Communication with ACS

Cancel Submit →





- 5. Toggle to turn on **Enable ACS Alerts**.
- 6. Enter the information for the alerts (use table from Step 1).
- 7. Scroll down and Click **Submit** when done.

This screenshot shows the 'ACS Alerts' configuration panel. At the top, there is a toggle switch for 'Enable ACS Alerts' which is currently turned off. A hand icon is shown clicking the toggle. Below the toggle are two expandable sections: 'Communication with Badge reader' and 'Communication with ACS'. At the bottom of the panel are 'Cancel' and 'Submit' buttons. A circled number '5' is placed over the 'Communication with ACS' section.This screenshot shows the 'ACS Alerts' configuration panel with the 'Enable ACS Alerts' toggle turned on. Below the toggle, there are three rows of alert types: 'Tailgating', 'Crossing', and 'Unauthorized Entry'. Each row has an information icon and an 'Add' button.This screenshot shows the 'ACS Alerts' configuration panel with the 'Enable ACS Alerts' toggle turned on. The 'Tailgating' alert type is selected, and its configuration details are shown in a table. The table has columns for 'Badge Number', 'Facility code', 'Card format', and a 'Delete' button. The 'Badge Number' and 'Facility code' fields contain the value '0'. The 'Card format' field has a dropdown menu with the text 'Please select ca...'. Below the table are the 'Communication with Badge reader' and 'Communication with ACS' sections. At the bottom of the panel are 'Cancel' and 'Submit' buttons. A circled number '6' is placed over the 'Delete' button, and a circled number '7' is placed over the 'Submit' button.

*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

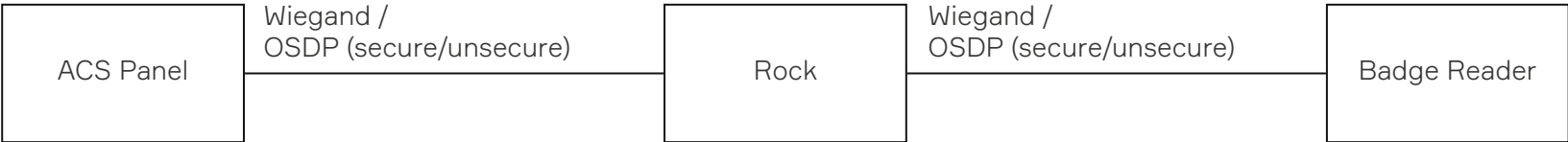
Important: if the tailgating event is not seen in the Alcatraz AI Admin Portal, the ACS will not receive an alert.

6.1.6—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:

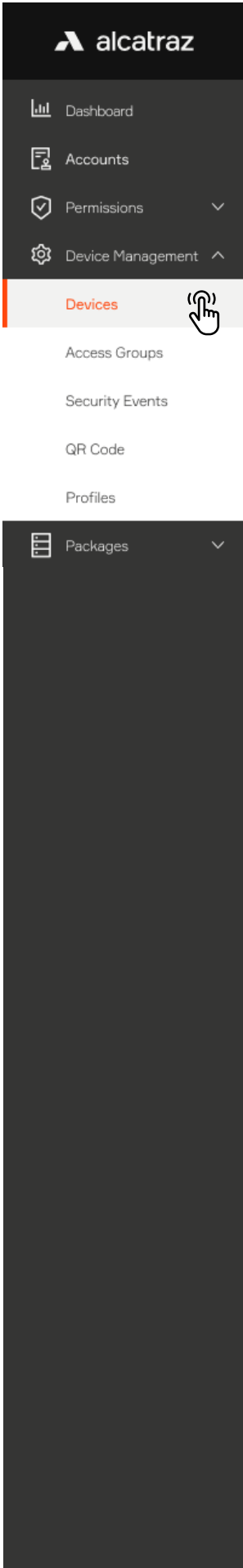
- 1. Rock is installed and powered up (refer to Install Guide)
- 2. Access to the ACS Panel (for OSDP setup between ACS Panel and Rock)
- 3. Access to the Badge Reader (for OSDP setup between Rock and Badge Reader)
- 4. Access to the Alcatraz AI Admin Portal (request login credentials)



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

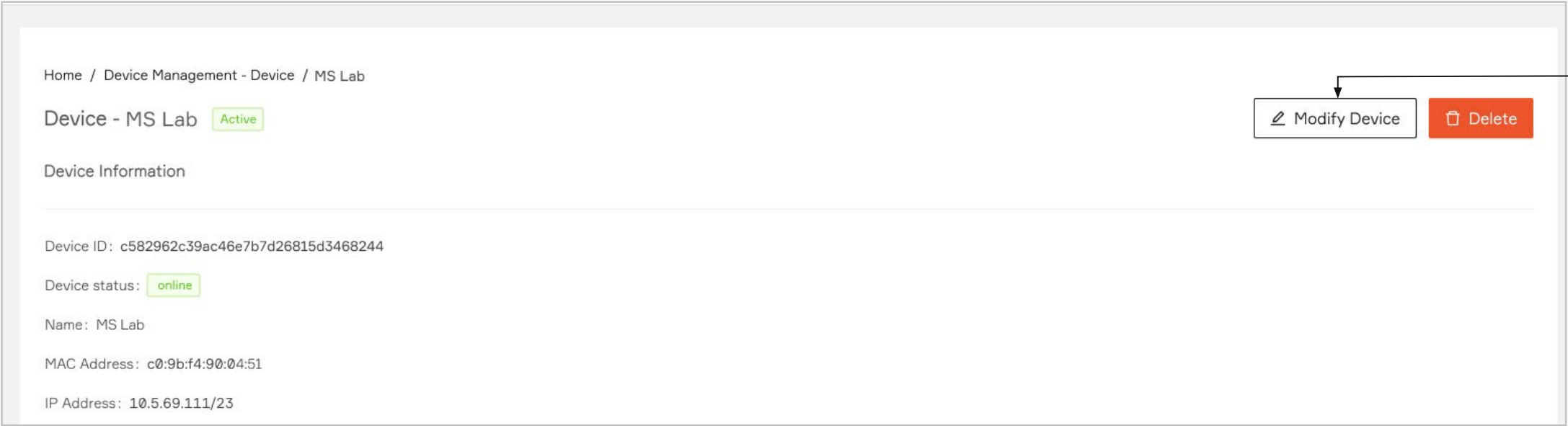
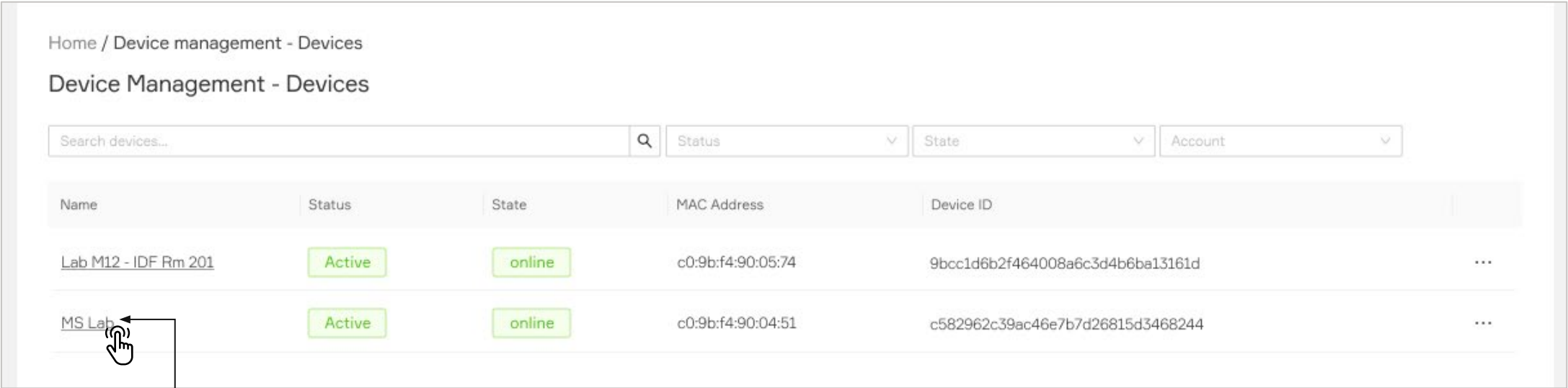
Required from Badge Reader to configure OSDP:
Device address = [range 0 - 126]
Baud rate = 57600 (example)
Enable secure/install mode - for OSDP secure channel ONLY
*enabling OSDP will vary with Badge Readers





6.1.6.1—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 Device** to open up the configurations page.



alcatraz

Dashboard

Accounts

Permissions

Device Management

Devices

Access Groups

Security Events

QR Code

Profiles

Packages

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

> Device Mode

> LED Control

> ONVIF

> Hold Signal Detection

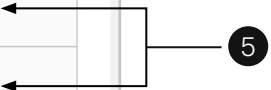
> ACS Alerts

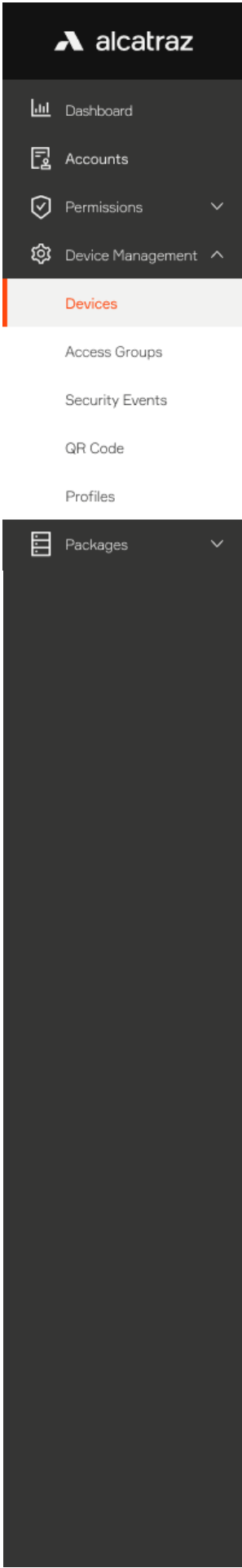
> Communication with Badge reader

> Communication with ACS

Cancel

Submit





6.1.6.2—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

Communication with Badge reader

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

☐ Disabled

☐ Wiegand

☒ OSDP

Baud Rate: 9600

Device Address: 0

Unsecure mode | Secure channel

1

Unsecure mode

Communication with Badge reader

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

☐ Disabled

☐ Wiegand

☒ OSDP

Baud Rate: 9600

Device Address: 0

Unsecure mode | Secure channel

Secure mode

Communication with Badge reader

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

☐ Disabled

☐ Wiegand

☒ OSDP

Baud Rate: 9600

Device Address: 0

Unsecure mode | Secure channel

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

Revert | Confirm

- 3. Click **Submit**



alcatraz

Dashboard

Accounts

Permissions

Device Management

Devices

Access Groups

Security Events

QR Code

Profiles

Packages

6.1.6.3—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

Secure channel

1

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

Unsecure mode

Secure channel

Secure mode

Communication with ACS

Indicate which protocol the ACS will use t

☐ Disabled

☐ Wiegand

☒ OSDP

Baud Rate

9600

Device

0

Unsecure mode

Secure channel

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

Revert

Confirm

3. Click **Submit**



alcatraz

Dashboard

Accounts

Permissions

Device Management

Devices

Access Groups

Security Events

QR Code

Profiles

Packages

6.1.6.4—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

Baud Rate

9600

Device

0

Revert

Confirm

Unsecure mode

Secure channel

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

Revert

Confirm

Communication with ACS

Indicate which protocol the ACS will use t

☐ Disabled

☐ Wiegand

☒ OSDP

Baud Rate

9600

Device

0

Revert

Confirm

Unsecure mode

Secure channel







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

Revert

Confirm



6.1.6.5—Troubleshooting Tips

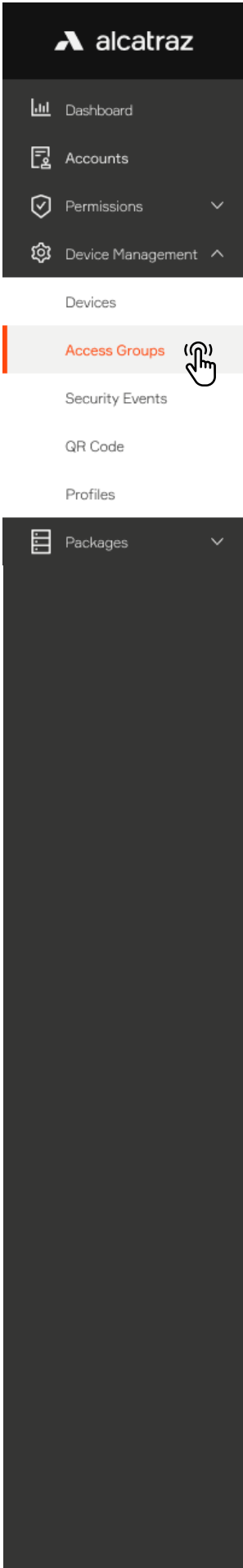
Troubleshooting			
OLED		Issue	Action
Rock ↔ ACS Panel	Rock ↔ Badge Reader		
		No communications between Rock device and ACS Panel or Badge Reader	Check: <ul style="list-style-type: none">■ Address/baud rate for mismatch■ Address/baud rate is valid■ Bad connections■ Devices are powered on
		Rock device is in Install mode, but secure link has not been established with the ACS Panel or Badge Reader *Applicable to OSDPv2 only.	Check: <ul style="list-style-type: none">■ 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: <ul style="list-style-type: none">■ 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

6.1.6.6—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—Access Groups

User access to doors and spaces can be managed in Access Groups. Users can belong to more than one Access Group. Access groups in turn are assigned to Rocks. When an Access Group is assigned to Rock(s), users belonging to that Access group will be able to access the door(s). Adding a user to an access group is done in Profiles. Note that before an Access Group can be assigned to a Rock or a user can be added, it must be created first. As part of the the onboarding process, an Access Group can be assigned to the Rock. If left empty, the default access group will be assigned. Only one default can exist for an Account. Any Rocks with no access group is assigned the default one.

6.2.1—Create an Access Group

1. Go to **Device Management** → **Access Groups**
 - Use the filter to search if the access group already exists.

Access Groups

Search access groups...

Q

Account

▼

+ Create an Access Group

2. Create a new access group by clicking **Create an Access Group**
 3. Fill out the Description and toggle **Default** if this Access Group will be the default for the Account.
 4. Click **Submit**
- Note that an Account can have only one default Access Group

Add Access Group

Home / Device Management - Access Groups

Create access group

Description

Security Team

Account

Micro Squared

▼

Default

Cancel

Submit →

Access Groups

Search access groups...

Q

Account

▼

+ Create an Access Group

Name		Account	Id	
R&D Lab Building 7		Micro Squared	cf994ea3-0b0e-4484-8fbe-ca3aeabd609e	...
Employees	<div>default</div>	Micro Squared	0f68c964-649b-4f23-b6a0-d0c2dbb81c79	...
Security Team		Micro Squared	82b1e6f5-cc61-437b-b38d-773dd1e25a15	...



alcatraz

Dashboard

Accounts

Permissions

Device Management

Devices

Access Groups

Security Events

QR Code

Profiles

Packages

6.2.2—Delete an Access Group

1. Go to **Device Management** —> **Access Groups**
2. Select the Access Group to open the Access Group Information page
3. Click on **Modify Access Group**
4. Click on **Delete** and **Confirm**

Access Group - Security Team

Modify Access Group

Delete

Access Group Information

Id: 82b1e6f5-cc61-437b-b38d-773dd1e25a15

Description: Security Team

Account: 1997f750-0425-4bfa-a9bd-ea4f7793c985

Embedded access groups

+ Add embedded access group

Description	Action
No results	

Edit Access Group

Home / Device Management - Access Group / Security Team

Delete

Access Group

* Description

Security Team

Account

Micro Squared

Default

Cancel

Submit →

!

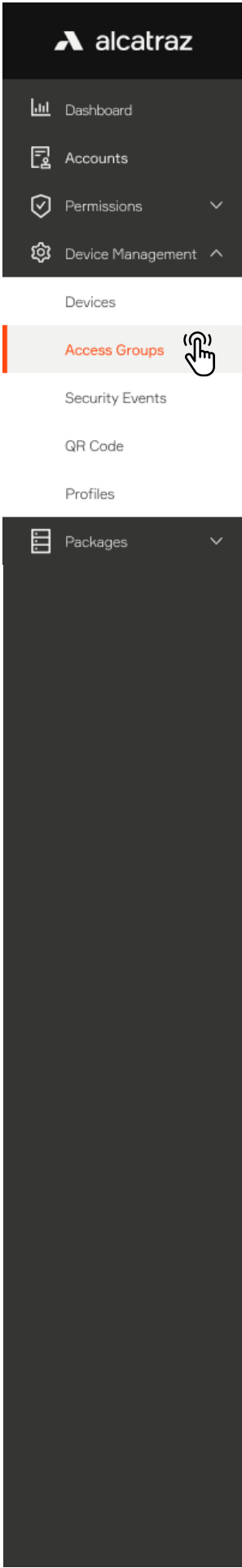
Delete access group?

This will permanently delete this access group from the system

Cancel

Delete





6.2.3—Embedded Access Groups

1. Go to **Device Management** → **Access Groups**
2. Select **Access Group** to open the Access Group Information page
3. Click on **Add embedded access group**

Home / Device Management - Access Group / Employees

Access Group - Employees

Access Group Information

Id: f9ac25f5-a3b6-47ce-bdf4-f91a6a82a9a0

Description: Employees

Account: cfc588f0-c73f-4264-b276-360d59fc0a5f

Embedded access groups

[+ Add embedded access group](#)

Description	Action
No results	

4. Select from the drop-down. The Access Group must be created first in order to appear in the list.
5. Click **Save**

Embedded access groups

Access group:

- Lab Technicians
- Default Access Group
- Part-Time Employees**

[Cancel](#) [Save](#)

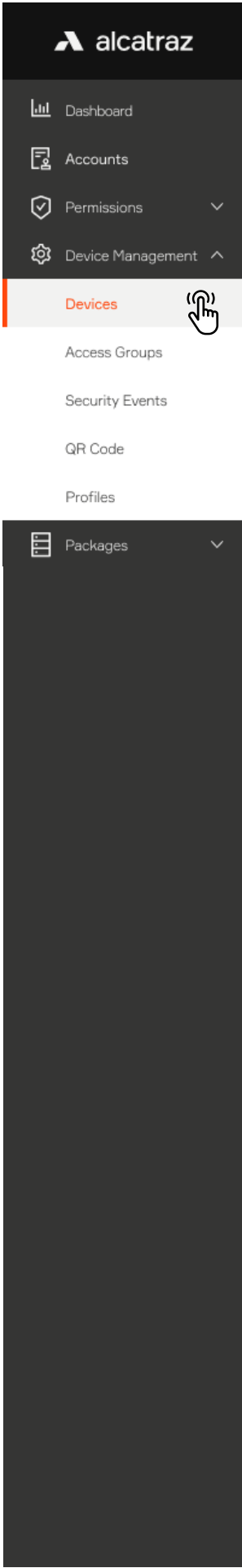
6. View in the embeddded access group.

Embedded access groups

[+ Add embedded access group](#)

Description	Action
Part-Time Employees	Delete





6.2.4—Change Default Access Group

- 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 Device** to open up the configurations page
 - 4. In **Default access group**, change the Access Group to another from the drop down
- Note that any embedded Access Groups will also have the same access as the parent Access Group.

Device Management - Devices

Search devices...

Name	Status	State	MAC Address	Device ID	
Lab M12 - IDF Rm 201	Active	online	c0:9b:f4:90:05:74	9bcc1d6b2f464008a6c3d4b6ba13161d	...
MS Lab	Active	online	c0:9b:f4:90:04:51	c582962c39ac46e7b7d26815d3468244	...

2

Home / Device Management - Device / MS Lab

Device - MS Lab Active

3

Home / Device Management - Device / MS Lab

Modify Device Parameters

Device Information

Device ID
003bef414c9d43e9a55203514ec5574d

* Name

Default access group

Lab Technicians
Employees
Default Access Group

IP address
10.5.69.83/23

4



alcatraz

Dashboard

Accounts

Permissions

Device Management

Devices

Access Groups

Security Events

QR Code

Profiles

Packages

6.2.5—Add Additional Access Groups

- 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 Device** to open up the configurations page
- 4. In **Access groups**, add any additional Access Groups to the Rock

Search devices...

Status

State

Account

Name	Status	State	MAC Address	Device ID	
Lab M12 - IDF Rm 201	Active	online	c0:9b:f4:90:05:74	9bcc1d6b2f464008a6c3d4b6ba13161d	...
MS Lab	Active	online	c0:9b:f4:90:04:51	c582962c39ac46e7b7d26815d3468244	...

Home / Device Management - Device / MS Lab

Device - MS Lab Active

Modify Device

Delete

Modify Device Parameters

Delete

Device Information

Device ID

003bef414c9d43e9a55203514ec5574d

* Name

MS Lab

Default access group

Employees

MAC address

c0:9b:f4:90:05:74

IP address

10.5.69.83/23

Access groups

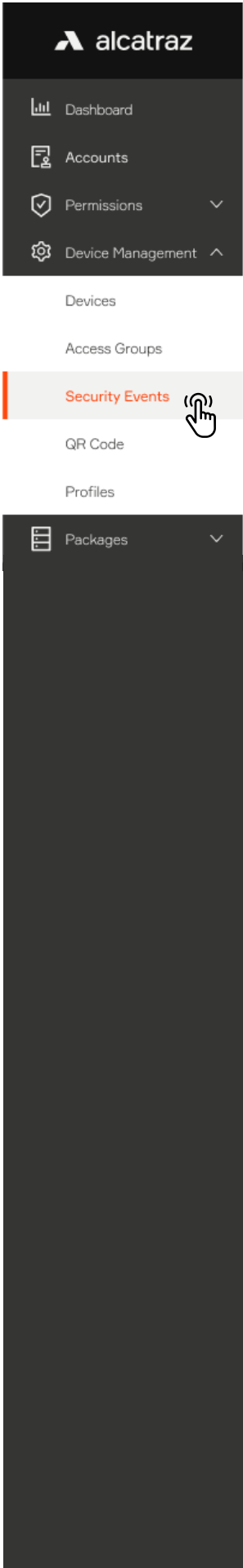
Lab Technicians

Remove

Lab Technicians

Default Access Group





6.3—Security Events

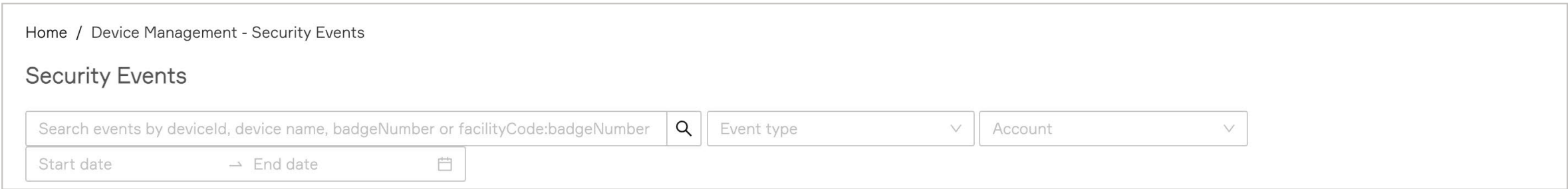
Security Events are displayed in the Alcatraz AI Admin Portal for

- Enrollment - auto-enrollment or manual enrollment
- Authentication - Single, Face-Only, Two Factor or Three Factor Authentication
- Tailgating Intelligence – tailgating, crossing or unauthorized entry

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.

6.3.1—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.



This is a sample list of the events.

Search events by deviceId, device name, badgeNumber or facilityCode:badgeNumber

Start date → End date

Q

Event type

Account

Event

Badge Number

Facility Code

2FA Badge Access Granted

3790829169

240

1FA Face Access Granted

4291593991

388

Unauthorized Entry By Known User

4230016983

388

1FA Badge Access Granted

4230016983

388

Tailgating By Unknown User

3061101082

240

1FA Enrollment

3061101082

240

Crossing By Known User

2915574810

240

1FA Badge Access Granted

1FA Badge Authenticated

1FA Enrollment

1FA Face Access Denied

1FA Face Access Granted

1FA Face Authenticated

Conf. Room Door

Lab-floor8

Conf. Room Door

Conf. Room Door


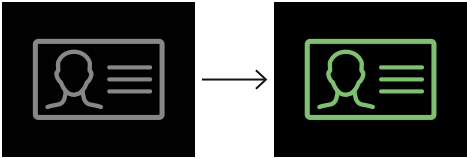

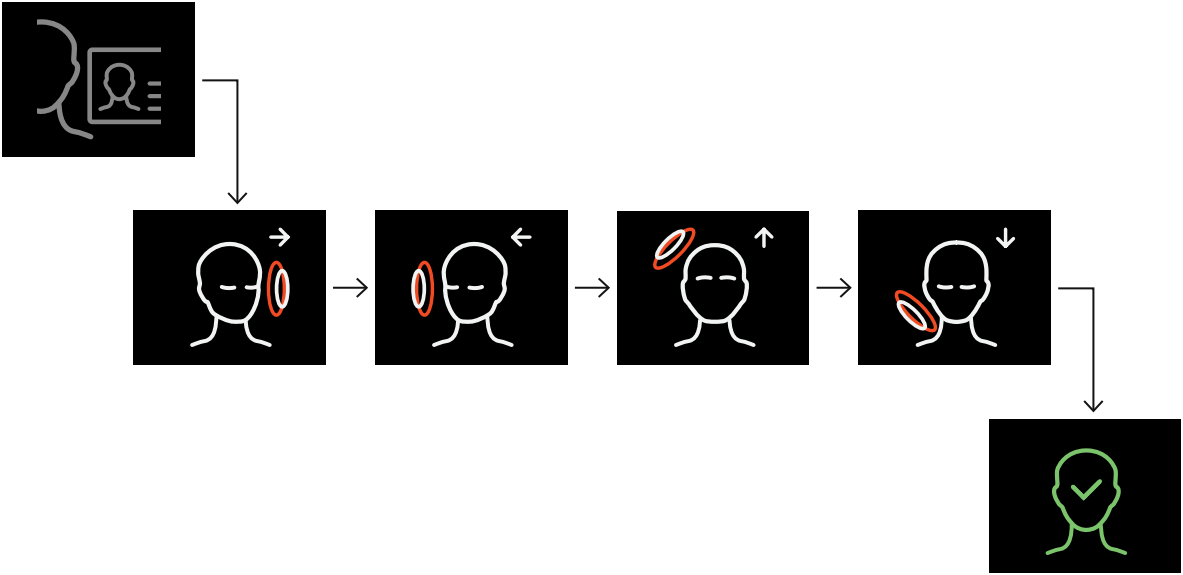

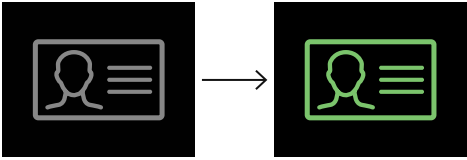
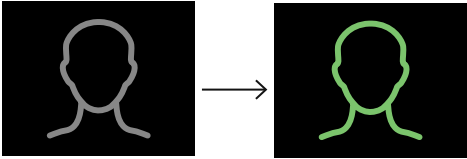

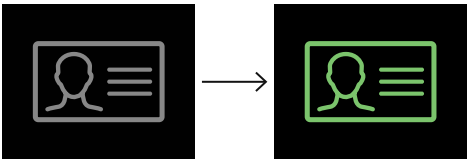

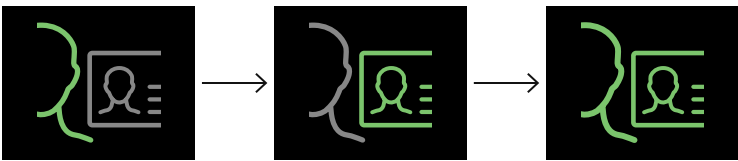
Entrance Door

Events can be filtered using the Event type drop down menu


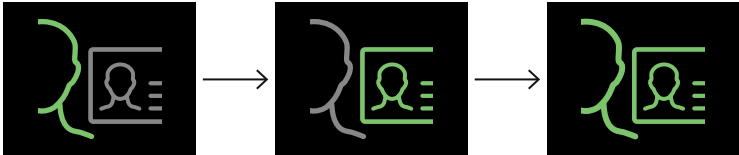

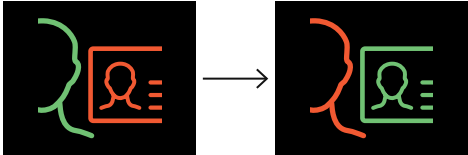

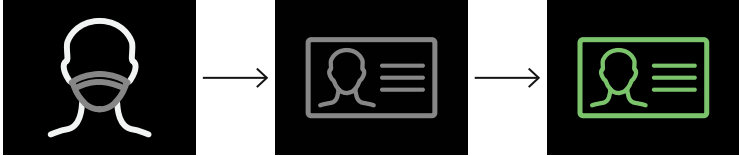
















6.3.2—Security Events Summary Table

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.

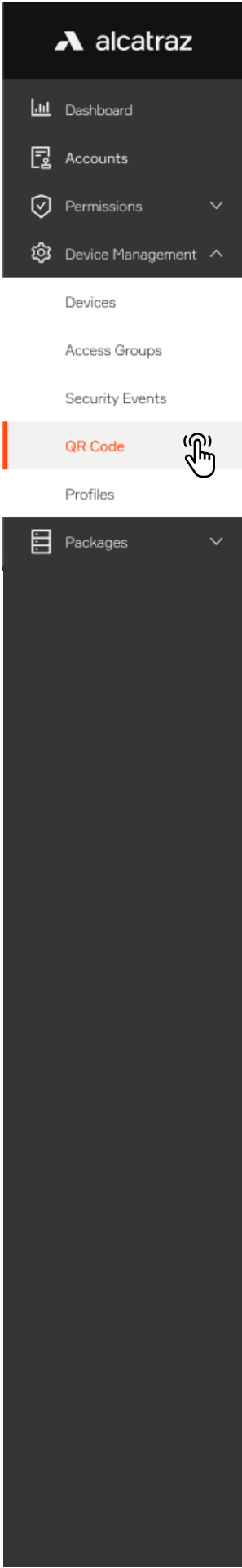
Event	Event Trigger	Rock mode	Display Icons
 1FA Enrollment	A user swiped a badge for auto-enrollment. 4-6 events will be displayed before the user is fully enrolled.	1FA with auto-enrollment	
 Full Enrollment	A user manually enrolled at an enrollment station.	Enrollment	
 1FA Face Access Granted	A user has been granted access in 1FA.	1FA 1FA face-only	  *grey icons will display very briefly
 1FA Badge Access Granted	A user swiped their badge for entry.	1FA	
 2FA Access Granted	A has been granted access with – face and badge match.	2FA	



Event	Event Trigger	Rock mode	Display Icons
 2FA Access Granted	Also seen for 3FA using face, badge and pin A user authenticated in 2FA - face and badge match. User then enters PIN. Badge and PIN are sent to the ACS. ACS must be configured to accept a badge and PIN.	2FA	
 2FA Mismatch	The authenticated face and the swiped badge did not match.	2FA	 *animation of green and red
 2FAM Access Granted	A user entered with a mask and swiped their badge.	2FA - M	
 Unauthorized Entry by Unknown User	A person gained entry that could not be authenticated.	All	
 Crossing by Unknown User	An unknown person gained entry when a user exited the door.	All	
 Crossing by Known User	A known user gained entry when a user exited the door.	All	
 Tailgating by Unknown User	An unknown person gained entry by tailgating a user.	All	
 Tailgating by Known User	A known user gained entry when tailgating a user.	All	
 1FA Badge Access Denied	The ACS rejected the badge.	1FA	
 1FA Face Access Denied	The ACS rejected the badge.	1FA	
 2FA Access Denied	The ACS rejected the badge.	2FA	
 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	

Reference Configure Rock Mode
guide to change the mode for
the Rock.





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;

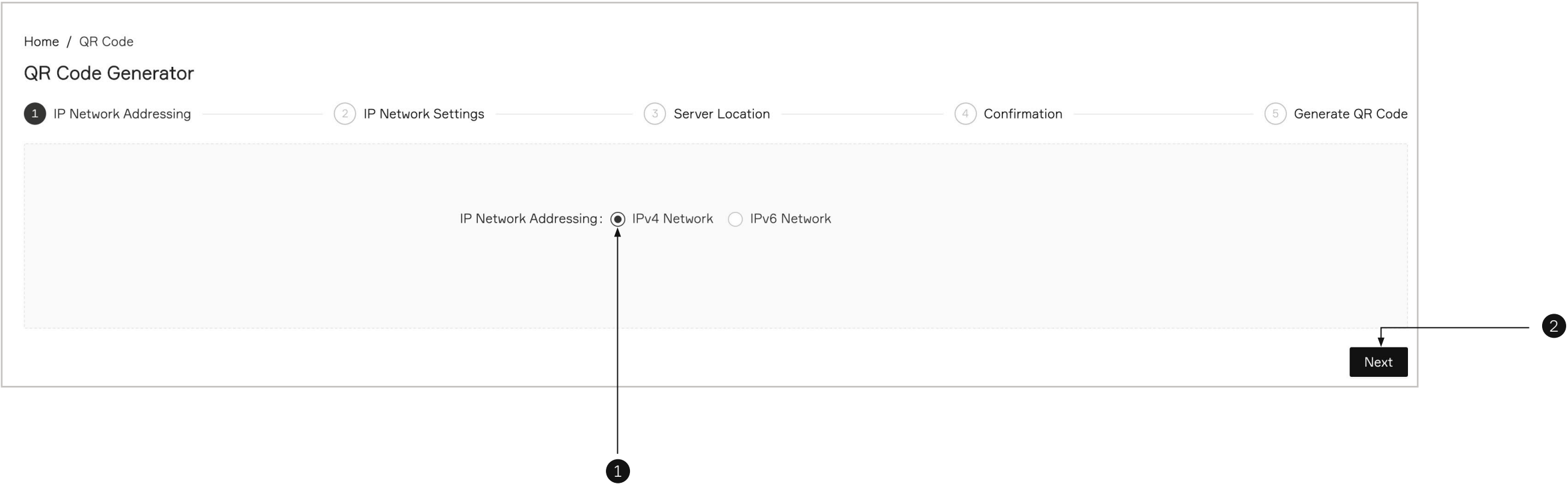
- First enter the network settings
- Next generate the QR code which encodes those settings
- Third print the QR code on a piece of paper (or use your laptop screen)
- Finally present that printed code to the Rock's image sensor

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)



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

QR Code Generator

✓ IP Network Addressing

2 IP Network Settings

3 Server Location

4 Confirmation

5 Generate QR Code

IP Network Settings: ☒ Automatically ☐ Manually

Previous

Next

A

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

IP Network Settings: ☐ Automatically ☒ Manually

+ Add/Remove DNS

* Device IP:

Device IP format X.X.X.X

* Subnet Mask:

Network mask format X.X.X.X

Gateway:

Gateway must be a valid IPv4 or IPv6 address

DNS:

DNS must be a valid IPv4 or IPv6 address

NTP:

NTP must be a valid IPv4 or IPv6 address

Previous

Next

B

Ver. 1.01

61

6.4.1—Server Location

- Select a **Server Location** and click **Next**.
1. For Cloud Hosted – select **Hosted by Alcatraz**
 2. For On-Premise – select **Local Server** and enter the Server IP

Home / QR Code

QR Code Generator

✓ IP Network Addressing

✓ IP Network Settings

3 Server Location

4 Confirmation

5 Generate QR Code

Server Location: ☒ Hosted by Alcatraz ☐ Local Server

PreviousNext

1 For Cloud Hosted

2 For On-Premise Rocks, a Server Hostname / IP Address will be required

Home / QR Code

QR Code Generator

✓ IP Network Addressing

✓ IP Network Settings

3 Server Location

4 Confirmation

5 Generate QR Code

Server Location: ☐ Hosted by Alcatraz ☒ Local Server

Server Hostname / IP Address:

PreviousNext

6.4.2—Generate and Download QR Code

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

QR Code Generator

✓ IP Network Addressing

✓ IP Network Settings

✓ Server Location

4 Confirmation

5 Generate QR Code

Configuration

IP Network Addressing: IPv4

IP Network Settings: Automatically

Server Location: Hosted by Alcatraz

Previous

Generate

2. Click **Download QR Code** to save to your computer, email or text.

QR Code Generator

✓ IP Network Addressing


✓ IP Network Settings

✓ Server Location

✓ Confirmation

5 Generate QR Code

Present QR Code to device



Configure another device

Download QR Code

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.



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, go to Advance Options – Enabling and Disabling QR Code Receptive Icon.code.



6.5—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

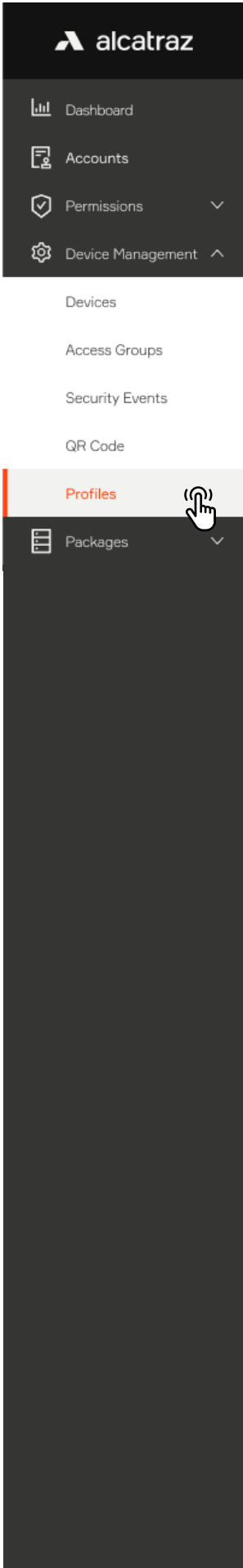
Auto-enrollment is available in Single Factor Authentication (1FA) mode. Users will badge in as normal to enter the door. The Rock builds the user profile with each badge in by capturing quality facial biometrics. After about 4-6 badge ins over the course of a few days, the user will realize as they 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

Manual enrollment is 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.



In summary,

- 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.



6.5.1—Viewing Profiles

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

Search profile by Badge Number or Facility Code:Badge Number: <input type="text"/>				Site: <input type="text"/>	Account: <input type="text"/>
Badge Number	Last Event	Device Name	Timestamp		
10514	 1FA Face Access Granted	MS Lab 4th floor	22/04/2021, 14:31:18		
10277	 1FA Face Access Granted	MS 1st floor	22/04/2021, 13:31:24		







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

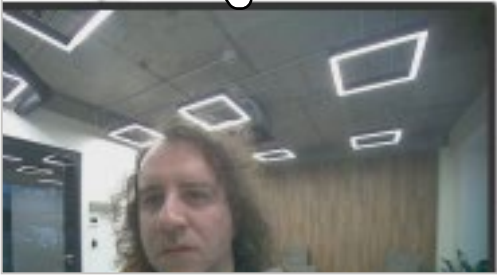
Profiles

Search profile by Badge Number or Facility Code:Badge Number:

Site:

Account:

Badge Number	Last Event	Device Name	Timestamp
10514	 1FA Face Access Granted	MS Lab 4th floor	22/04/2021, 14:31:18
10277	 1FA Face Access Granted	MS 1st floor	22/04/2021, 13:31:24
	 1FA Enrollment	MS Conf. 6th floor	29/04/2021, 12:48:04
	 Full Enrollment	MS Lobby	23/06/2021, 17:27:26
	 1FA Face Access Granted	MS Lab 8th floor	08/04/2021, 13:14:48
	 1FA Badge Access Granted	MS Main Depot	09/04/2021, 13:02:07



2



alcatraz

Dashboard

Accounts

Permissions

Device Management

Devices

Access Groups

Security Events

QR Code

Profiles

Packages

3. To view additional Profile information, click on the Badge Number

Search profile by Badge Number or Facility Code:Badge Number

Site

Account

Badge Number	Last Event	Device Name	Timestamp
10514	1FA Face Access Granted	MS Lab 4th floor	22/04/2021, 14:31:18
10277	1FA Face Access Granted	MS 1st floor	22/04/2021, 13:31:24

Home / Profile / beb64731-e2d6-4308-b755-2d5a07dd571e

Profile - beb64731-e2d6-4308-b755-2d5a07dd571e

Profile information

Last Event: Details

Access Details

Badge Number	Facility Code	Access Group	Action
10277	31	Default Access Group	



alcatraz

Dashboard

Accounts

Permissions

Device Management

Devices

Access Groups

Security Events

QR Code

Profiles

Packages

6.5.2—Delete a Profile – Option 1 (delete through Profiles)

- 1. Click on **Device Management**→**Profile**
- 2. Click on a Badge Number to open the Profile
- 3. Click on **Delete** at top right to delete this Profile.

Search profile by Badge Number or Facility Code:Badge Number.

Site

Account

Badge Number	Last Event	Device Name	Timestamp
10514	1FA Face Access Granted	MS Lab 4th floor	22/04/2021, 14:31:18
10277	1FA Face Access Granted	MS 1st floor	22/04/2021, 13:31:24

Home / Profile / beb64731-e2d6-4308-b755-2d5a07dd571e

Profile - beb64731-e2d6-4308-b755-2d5a07dd571e

Profile information

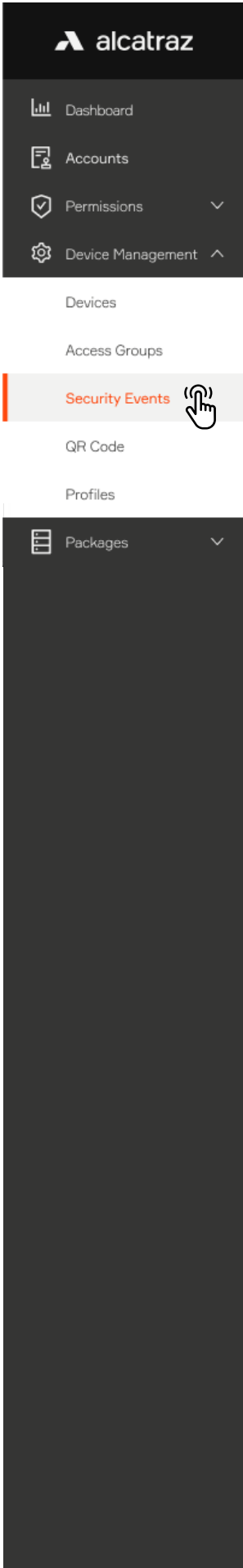
Last Event: Details →

Access Details

+ Add Access

Badge Number	Facility Code	Access Group	Action
10277	31	Default Access Group	...





6.5.3—Delete a Profile – Option 2 (delete through Security Event)

- 1. Click on **Device Management** → **Security Events**
- 2. Click on an Event and an **Edit Security Events** pane will open.
- 3. Click on the **Un-enroll** button at top right of any security event panel.
- 4. A pop up window will appear to confirm by selecting **Un-enroll** again.

Home / Device Management - Security Events

Security Events

Search events by deviceId, device name, badgeNumber or facilityCode:badgeNumber

Event type

Account

Start date

End date

Event	Badge Number	Facility Code	Name
1FA Badge Access Granted	10514	31	MS Lobby
1FA Face Access Granted	10277	31	MS 1st floor

Edit securityevents

Home / Security Event

Security Event 1FAUser

Un-enroll

Event details

Event type: 1FA Face Access Granted

Badge number: 10277

Facility code: 31

Name MS 1st floor

Device mode: 1FAUser

Date: 22/04/2021, 14:31:10

Un-enroll Profile?

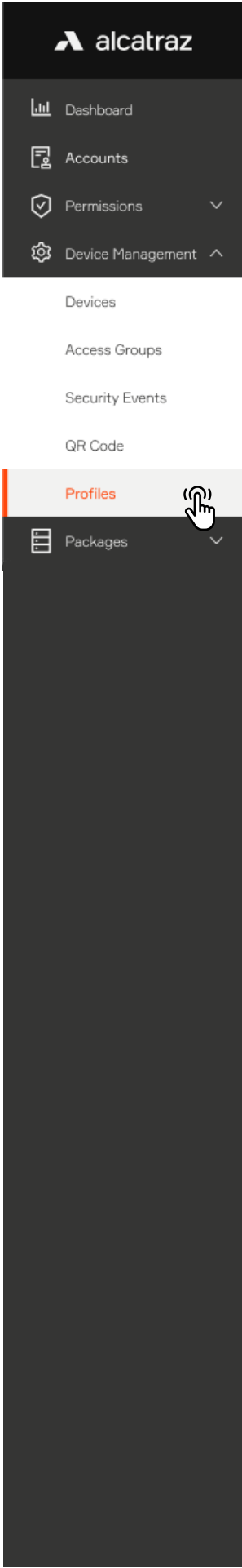
This will permanently delete this profile from the system

Cancel

Un-enroll

Note: The un-enroll option will only be displayed in events where the user profile can be deleted.





6.5.4—Managing Access

In some organizations, users can have multiple badges belonging to different Access Groups. Within the user profile, there is flexibility to manage badge number(s) associated with different Access Groups.

- Badge 12345 => Security Team
- Badge 67890 => Employees

Add an Access Group

1. Select the Badge Number to open the profile record.
2. Scroll down to the **Access Details** section to see the access groups the user belongs to.
3. Select **Add Access**

Badge Number	Last Event	Device Name	Timestamp
10514	1FA Face Access Granted	MS Lab 4th floor	22/04/2021, 14:31:18
10277	1FA Face Access Granted	MS 1st floor	22/04/2021, 13:31:24

Home / Profile / beb64731-e2d6-4308-b755-2d5a07dd571e

Profile - beb64731-e2d6-4308-b755-2d5a07dd571e

Delete

Profile information

Last Event:

Details

Access Details

Badge Number

Facility Code

Access Group

Action

10277

31

Default Access Group

...

+ Add Access



4. Click **Save**.

Profile - beb64731-e2d6-4308-b755-2d5a07dd571e

Delete

Profile information

Last Event:

Details →

Add new access

Badge number:

10277

Access groups:

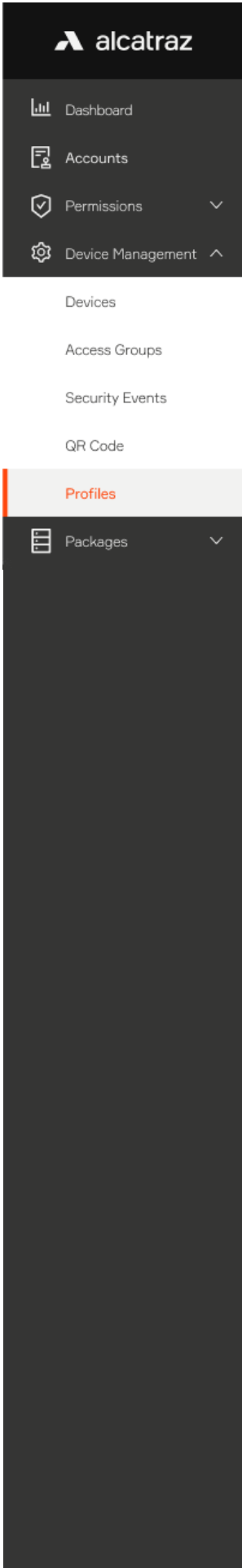
Select an Access group

Security Team

Cancel

Save

Badge Number	Facility Code	Access Group	Action
10277	31	2	...
		Security Team	
		Default Access Group	



Delete Access Group

1. Select the Badge Number to open the profile record.

Badge Number	Last Event	Device Name	Timestamp
10514	1FA Face Access Granted	MS Lab 4th floor	22/04/2021, 14:31:18
10277	1FA Face Access Granted	MS 1st floor	22/04/2021, 13:31:24

1

2. Scroll down to the **Access Details** section to see the access groups the user belongs to.
3. Select **Delete Access** to delete all or the **trash can** to delete the selected Access Group.

Access Details				+ Add Access
Badge Number	Facility Code	Access Group	Action	
10277	31	Default Access Group	...	
			Delete Access	

Access Details				+ Add Access
Badge Number	Facility Code	Access Group	Action	
10277	31	2	...	
		Security Team		
		Default Access Group		

3

6.5.5—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.

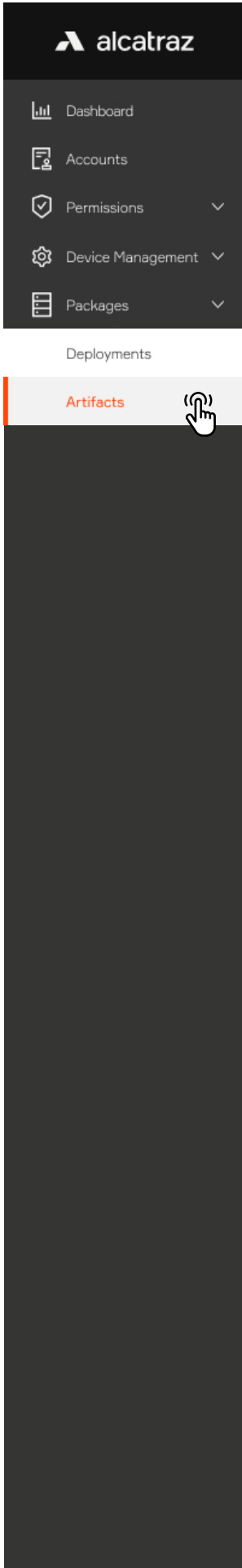


New Rock Firmware

Rock firmware can only be updated by Dealer Administrators or Installers.
Login credentials to the Alcatraz AI Admin Portal must be either Dealer Administrator role 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.

7.1—Check Lastest Firmware Version	74
7.2—Update the Rock Firmware	75
7.3—Verify Update is Successful	77













7.1—Check Latest Firmware Version

- 1. Log into the Admin Portal
- 2. Go to **Packages** → **Artifacts** and check if the latest version is in the list
- 3. On-prem Only - Click **Upload an artifact** and select the file that was downloaded to your computer from an Alcatraz AI link. Uploading can take several minutes

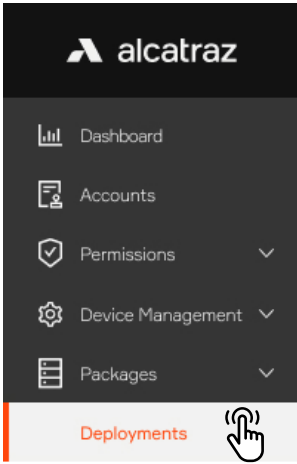
Home / Artifacts

Artifacts

+ Upload an artifact

Name	Size	Last modified
 rock-prod-image_2.12.0	1.23 GB	2021-04-15T20:14:11.924Z
 rock-prod-image_2.9.2	1.20 GB	2021-04-19T09:10:36.813Z
 rock-prod-image_2.10.4	1.21 GB	2021-04-19T09:37:16.312Z
 rock-prod-image_2.11.2	1.20 GB	2021-04-19T10:03:30.501Z
 rock-prod-image_2.12.0	1.23 GB	2021-04-19T10:19:30.41Z
 rock-image_2.11.3	1.24 GB	2021-04-21T11:18:34.013Z
 rock-prod-image_2.12.1	1.23 GB	2021-04-28T18:24:18.04Z
 rock-prod-image_2.13.0	1.23 GB	2021-05-10T22:02:25.936Z
 rock-prod-image_2.13.1	1.23 GB	2021-06-07T05:31:36.613Z
 rock-prod-image_2.14.0	1.40 GB	2021-07-05T11:39:21.353Z





7.2—Update the Rock Firmware

1. Go to **Packages** → **Deployments** – The list displays deployments that have been scheduled in the past.
2. Click **Create a Deployment** and the **Add deployments** side pane will open up.

Home / Packages - Deployments

Deployments

+ Create a Deployment

Add deployments

Home / Packages - Deployments

Create deployment

* Deployment name

Deployment name

* Artifact name

Artifact name

* Devices

Search by Device ID Device ID

Devices selected: 0

Phases

+ Add

Artifact name

rock-image_2.8.3

rock-image_2.13.1

rock-prod-image_2.11.0

rock-prod-image_2.12.0

rock-image_2.14.0

rock-image_2.10.0

* Devices

Search by Site Site

Search by Account

Search by Site

Search by Device ID

3. Enter a Deployment name – this can be anything but best practice is to use Rock name and firmware version number.
4. Select the **Artifact Name** – this is the firmware for updating the Rock.
5. In Devices drop down menu, select **Search by Site** and then start typing to see the site name. Optionally search **by Account** or **Device ID**.
6. A list of Rocks in the Site will be displayed. Make sure ALL Rocks that need to be updated are selected before clicking **Submit**.



Dashboard

Accounts

Permissions

Device Management

Packages

Deployments

Artifacts

7. 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 **Deployment Status = finished**. A restart will occur during this process. The Rock will be offline for approximately 60 seconds.
8. If the Deployment Status shows Failed, check that the Rock is online and network connection is stable. Restart the update.

Home / Packages - Deployments

Deployments

+ Create a Deployment

Search deployments...

Name	Artifact	Deployment Status	Nr of Artifacts	Devices	Created
Juls_2.14	rock-prod-image_2.14.0	inProgress	1	1	2021-07-06T21:50:46.937Z

Name	Artifact	Deployment Status	Nr of Artifacts	Devices	Created
Juls_2.14	rock-prod-image_2.14.0	finished	1	1	2021-07-06T21:50:46.937Z

7



alcatraz

Dashboard

Accounts

Permissions

Device Management

Devices

Access Groups

Security Events

QR Code

Profiles

Packages

7.3—Verify Update is Successful

1. Click on the name to open up the Deployment job. A successful update will show success and the number in the blue circle will indicate how many Rocks got updated successfully if multiple Rocks were being updated.

Home / Packages - Deployment / Juls_2.14

Deployment - Juls_2.14 finished

Info

Artifact name:

rock-prod-image_2.14.0

Created at:

2021-07-06T21:50:46.937Z

Artifacts ids:

2b6b9ce5-b7b8-4ed1-947e-b1f053f619dc

Finished:

2021-07-06T22:06:46.209Z

Device count:

1

Stats

1

success

Devices

Id	Device type	Status	State	Substate	Created at	Finished
5fa1c9e0bd0553475b62cd98		success		Executing script: ArtifactInstall_Leave_80_bl-update	2021-07-06T21:50:46.937Z	2021-07-06T22:06:46.207Z

< 1 >

2. To verify the new version for the Rock, go to **Device Management** → **Devices** and click on the Name

Name	Status	State	MAC Address	Device ID
Lab M12 - IDF Rm 201	Active	online	c0:9b:f4:90:05:74	9bcc1d6b2f464008a6c3d4b6ba13161d
MS Lab	Active	online	c0:9b:f4:90:04:51	c582962c39ac46e7b7d26815d3468244



alcatraz

Dashboard

Accounts

Permissions

Device Management

Devices

Access Groups

Security Events

QR Code

Profiles

Packages

3.The information page for the Rock will open. Scroll down midway and check the Firmware Release

Home / Device Management - Devices / MS Lab

Device - MS Lab Active

Modify Device

Delete

Device Information

ID: 60ed22c756ca57e169bb1ace

Device ID: 003bef414c9d43e9a55203514ec5574d

Device status: online

Name: MS Lab

MAC address: c0:9b:f4:90:05:74

IP address: 10.5.69.83/23

Default access group: Default Access Group

Access groups: TopLevel

Security events recorded for the past month

Tampered Reader Detected1FA Face Access Denied1FA Badge Access Granted2FA Access Granted

Spoofing Attempmts

31

Tailgating Attempts

349

Access Granted

920

New User Enrollments

282

Device Configuration

Board Type: N/A

Firmware Release: rock-prod-image_2.14.0

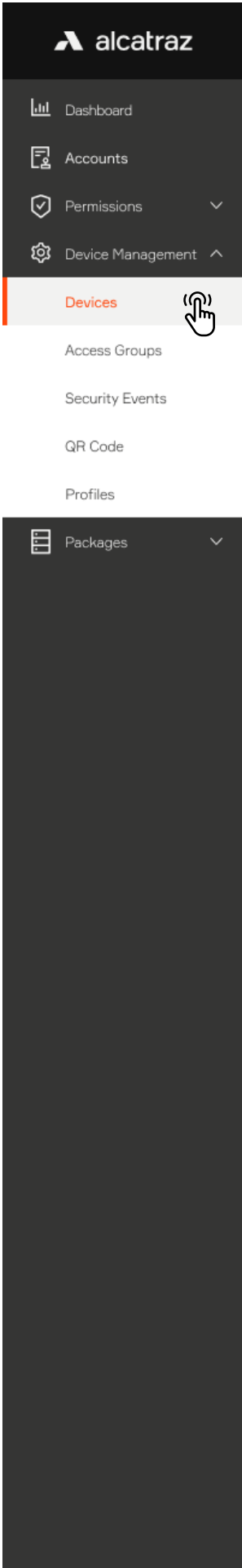
3



8 — 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.

8.1—Enabling or Disabling QR Code Receptive Icon	80
8.2—Setting the Rock for Corridor Mode	82



8.1—Enabling or Disabling QR Code Receptive Icon

The Rock can read a QR code when the QR Code Receptive icon is shown in the display. To enable the icon, do the following.

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 Device** 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**.

Search devices...	Q	Status	State	Account
Name	Status	State	MAC Address	Device ID
Lab M12 - IDF Rm 201	Active	online	c0:9b:f4:90:05:74	9bcc1d6b2f464008a6c3d4b6ba13161d
MS Lab	Active	online	c0:9b:f4:90:04:51	c582962c39ac46e7b7d26815d3468244

Home / Device Management - Device / MS Lab

Device - MS Lab Active

Device Information

Modify Device Delete

Device Configuration

Advanced ☒

> Device Mode

> LED Control

> ONVIF

> Hold Signal Detection

> ACS Alerts

> Communication with Badge reader

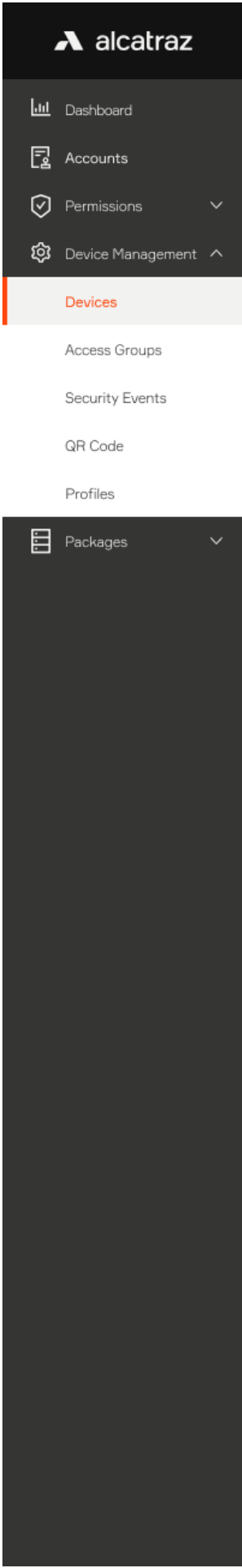
> Communication with ACS

> Add a Parameter

> Add a Custom Configuration

Cancel Submit →





6. Under **Manual Configuration**, select **device.setup_mode** and set the value to **qrcode**.

A screenshot of the 'Manual Configuration' dialog box. The 'Parameter Name' dropdown is set to 'device.setup_mode'. The 'Value' dropdown is open, showing options: 'disabled', 'qrcode' (highlighted with a hand cursor), 'bluetooth', and 'any'. A dashed box with a '+ Add parameter' button is visible below the dropdowns. A line with a circled '6' points to the 'qrcode' option in the dropdown.

*To disable QR Code

- 7. The qrcode can be turned off from the display at anytime by changing the value to disabled. Note that this also removes the IP info scrolling.
- 8. Click **Submit** when done.

A screenshot of the 'Manual Configuration' dialog box. The 'Parameter Name' dropdown is set to 'device.setup_mode'. The 'Value' dropdown is now set to 'disabled'. A dashed box with a '+ Add parameter' button is visible below the dropdowns. A line with a circled '7' points to the 'disabled' option in the dropdown. At the bottom, there are 'Cancel' and 'Submit ->' buttons. A line with a circled '8' points to the 'Submit' button.

alcatraz

Dashboard

Accounts

Permissions

Device Management

Devices

Access Groups

Security Events

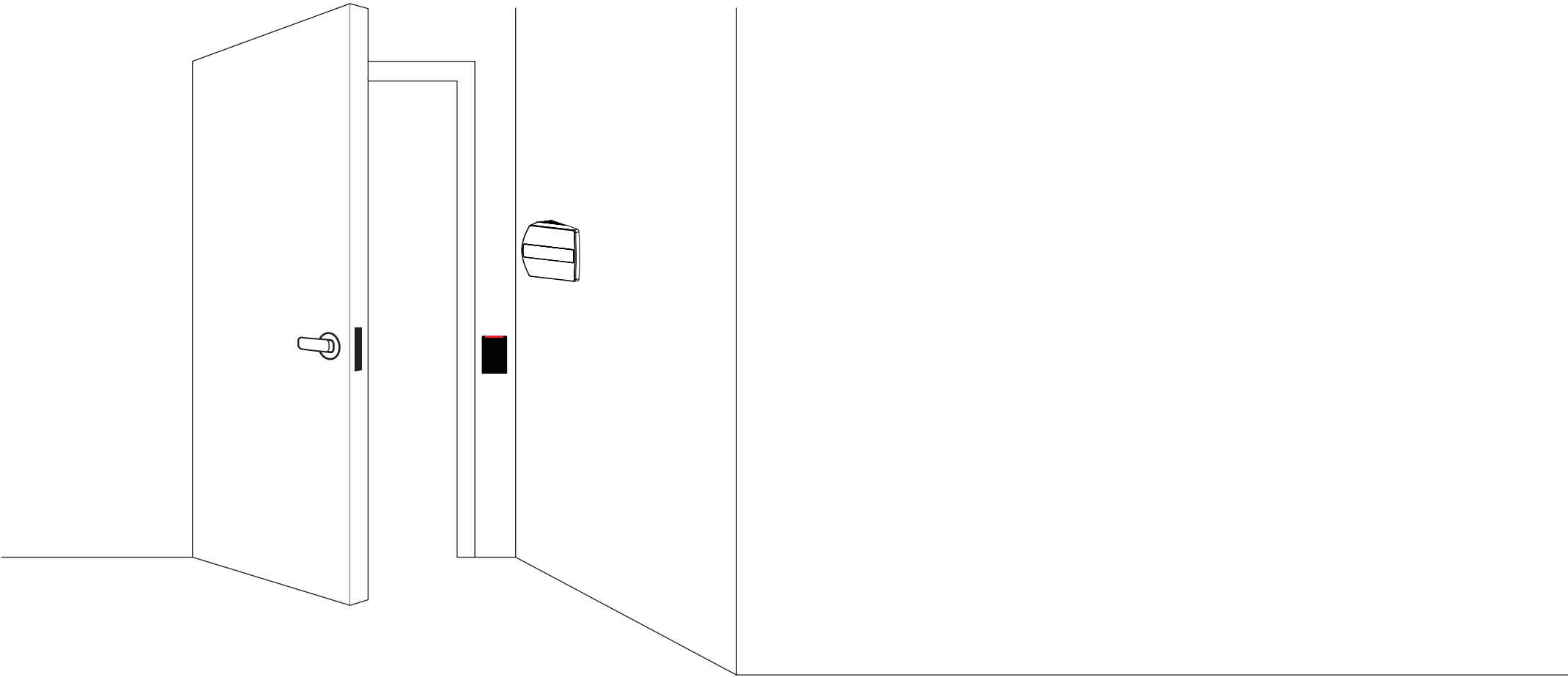
QR Code

Profiles

Packages

8.2—Setting the Rock for Corridor 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 Device** to open up the configurations page.

Search devices...

Status

State

Account

Name	Status	State	MAC Address	Device ID	
Lab M12 - IDF Rm 201	Active	online	c0:9b:f4:90:05:74	9bcc1d6b2f464008a6c3d4b6ba13161d	...
MS Lab	Active	online	c0:9b:f4:90:04:51	c582962c39ac46e7b7d26815d3468244	...

Home / Device Management - Device / MS Lab

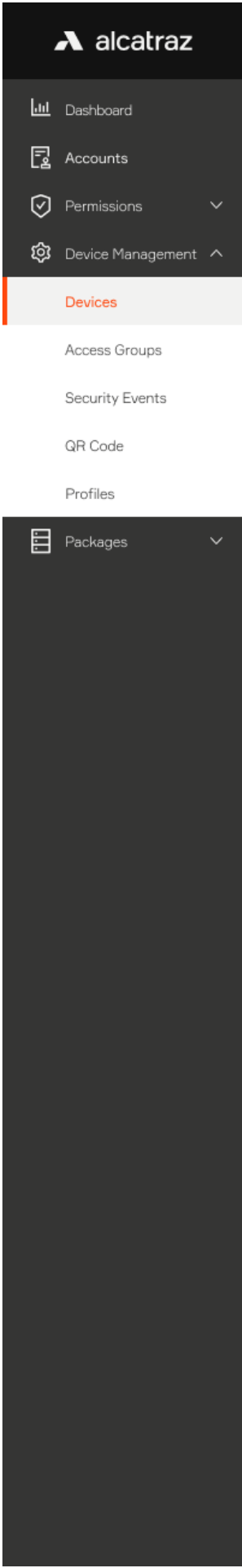
Device - MS Lab Active

Device Information

Modify Device

Delete





- 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**.



- 6. Under **Manual Configuration**, select **corridor_setup.is_corridor_setup_enabled**. Slide to turn on.
- 7. Click **Submit** when done.



