

SMART-PSRTNC Series UPS



Remote Monitoring **EAT•N**

Change Log Sheet

Revision	Date	Mobile App Version	Chapter, Description of Change
A	June 2024	1.0	Official release of the Eaton Remote Monitoring Applications Guide.
B	July 2024	1.0	<ul style="list-style-type: none">Added new image toAdded instructions on how to delete user accounts based on the role assignment to the section .
C	September 2024	2.0	Added test

Table of Contents

1 Introduction	1
1.1 Welcome to the Eaton Remote Monitoring Application	1
1.2 User Enrollment and Activation	1
2 Screens and Navigation	11
2.1 User Interface	11
2.2 Login Screen	11
2.3 Organizational Summary Screen	12
2.3.1 Organizational Hierarchy Menu	13
2.3.2 Tabs Menu	14
2.3.3 Help Menu	14
2.3.4 Settings Menu	15
2.3.5 User Menu	16
2.3.6 Timeline Tab	17
2.3.7 Groups Widget	19
2.3.8 Device Widget	19
3 User Management	23
3.1 Managing Users	23
4 Group Management	25
4.1 Creating a Group Within An Organization	25
5 Device Management	29
5.1 Adding a Device	29
5.1.1 Adding a Device with the Mobile Application	31
5.1.2 Device Configuration via NFC	33
6 Alerts and Notifications	37
6.1 Setting Alerts and Notifications	37
6.2 Setting Custom Notifications	38

Chapter 1 Introduction

1.1 Welcome to the Eaton Remote Monitoring Application

The Eaton Tripp Lite Series cloud-connected UPS systems are managed by the Eaton Remote Monitoring Application supported by Eaton's Brightlayer platform so that users can connect to their UPS anywhere. Receive alerts, control outlets, or shutdown devices – all from the touch of a mobile device or desktop computer. Whether a user is setting up one or several units, commissioning has never been more straightforward. The Eaton Remote Monitoring Application can be downloaded from the Apple or Android app stores.

1.2 User Enrollment and Activation

1. Locate and scan the QR code on the left-hand side of the UPS cover or visit the direct link [Eaton Brightlayer Remote Monitoring Application](#) to launch the application in a web browser or to download it to a remote Device.

Figure 1. QR Code Location

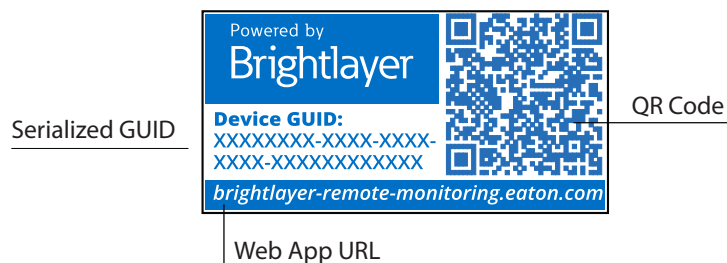
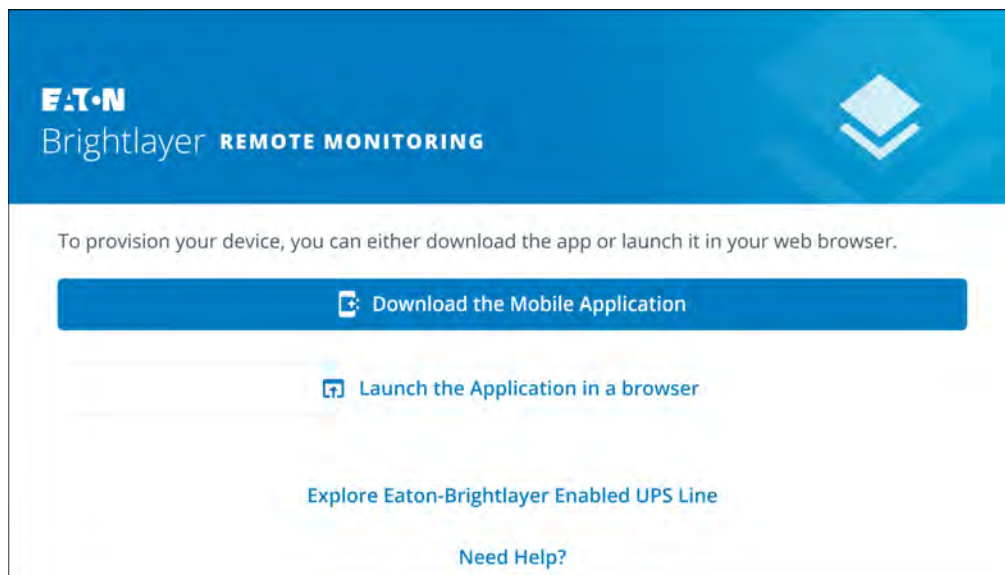


Figure 2. Web Application Page



NOTE

Chrome, Firefox, Edge, and Safari are the supported internet browsers. Do not use Microsoft Internet Explorer.

2. Click the *Sign-Up* link on the login screen.
3. Please read and check the box agreeing to the EATON CORPORATION END USER LICENSE AGREEMENT FOR Brightlayer Software Suites Remote Monitoring. Then click *Next*.

Figure 3. Sign In Screen and End User License Agreement

EATON

Email Address


☐ Keep me signed in

Next

[Don't have an account? Sign up](#)

[Need Help?](#)

[Privacy Policy](#)


EATON
Cybersecurity Certified

License Agreement

EATON CORPORATION END USER LICENSE AGREEMENT FOR Brightlayer Software Suites Remote Monitoring

This End User License Agreement (the "**Agreement**") is a legal agreement between you and the Contracting Entity (as defined below). For the purposes of this Agreement, any reference to "Eaton" shall include the Contracting Entity, its holding company, its affiliates and subsidiaries. This Agreement, and any other terms or conditions notified to you, governs your access to and use of Brightlayer Software Suites Remote Monitoring in all countries/regions (the "**Product Software**").

Your use of the Product Software is subject to the terms of this Agreement as set out below which incorporate by reference our Privacy Statement at <https://www.eaton.com/us/en-us/company/policies-and-statements/privacy>.

☒ I have read and agree to the Terms & Conditions

Cancel • • • • • Next

4. Enter a valid email address to verify your account. A verification code will be sent to your email account. Click *Next*. Click *Next*.
5. Enter the verification code and click *Next*.

Figure 4. Create an Account and Verify Code

The figure consists of two side-by-side screenshots of a web application interface for account creation and verification.

Left Screenshot: Create an Account

- Title:** Create an Account
- Text:** To register for an Eaton account. You will need to verify your email address to continue.
- Form:** A text input field labeled "Email Address" containing the text "newuser1234@gmail.com".
- Buttons:** A "Back" button on the left and a "Next" button on the right, separated by a progress indicator with four dots, the second of which is filled.

Right Screenshot: Verify Email

- Title:** Verify Email
- Text:** A verification code has been sent to the email address you provided. Click the link or enter the code below to continue. This code is valid for 30 minutes.
- Form:** A text input field labeled "Verification Code" containing the text "XXXXXX".
- Buttons:** A "Resend Verification Email" button centered below the input field. At the bottom, there are "Back" and "Next" buttons with a progress indicator showing the second of four dots filled.

6. Enter the account information to complete the account creation. Eaton recommends that the Two-factor Authentication option remain enabled to prevent unauthorized access to the account. When finished, click *Next*.
7. The new user account is now created. Press the *Log-In* button, and an email notification is sent to activate the account.

Figure 5. Account Details

Account Details

Enter your details below to complete account creation.



New


User


Country Code
+1

Phone Number (Optional)

Country
US

Enable Two-factor Authentication  

[Back](#)  [Next](#)



Welcome newuser1234!

Your user account has been successfully created with the email **newuser1234@gmail.com.**

[Log In](#)

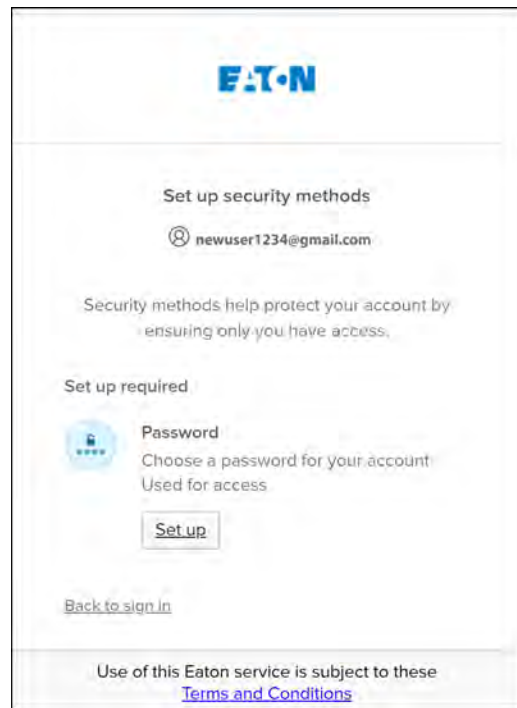
8. Click the *Activate Account* button provided in the email notification.

Figure 6. Email Activation Notification



9. Click *Set up* to create your account password.


Figure 7. Set Up Password Screen




10. Create a password that meets the requirements to log into the application. When finished, click *Next*.

Figure 8. Set Up Password

EAT•N




Set up password

 newuser1234@gmail.com


Password requirements:

- At least 8 characters
- A lowercase letter
- An uppercase letter
- A number
- No parts of your username
- Password can't be the same as your last 4 passwords

Enter password

***** 

Re-enter password

***** 

Next

[Return to authenticator list](#)

[Back to sign in](#)

Use of this Eaton service is subject to these [Terms and Conditions](#)

11. Set up the authentication method that is available to access the account. Click *Set up*.
12. Enter a phone number and click *Receive a code via SMS*.

Figure 9. Security Authentication Setup

The figure consists of two side-by-side screenshots of the Eaton security authentication setup interface.

Left Screenshot: Set up security methods

- Header: Eaton logo.
- Section: Set up security methods.
- User: newuser1234@gmail.com.
- Text: Security methods help protect your account by ensuring only you have access.
- Section: Set up optional.
- Options:
 - Google Authenticator**: Enter a temporary code generated from the Google Authenticator app. Used for access. [Set up]
 - Phone**: Verify with a code sent to your phone. Used for access. [Set up] (This option is highlighted with a red rectangular box).
- Buttons: Continue, Back to sign in.
- Footer: Use of this Eaton service is subject to these [Terms and Conditions](#).

Right Screenshot: Set up phone authentication

- Header: Eaton logo.
- Section: Set up phone authentication.
- User: newuser1234@gmail.com.
- Text: Enter your phone number to receive a verification code via SMS.
- Form:
 - Country**: United States (dropdown menu).
 - Phone number**: +1 (country code) followed by a field with asterisks for the number.
- Buttons: Receive a code via SMS, Return to authenticator list, Back to sign in.
- Footer: Use of this Eaton service is subject to these [Terms and Conditions](#).

13. Enter the code received via SMS. Click *Verify*.
14. Click *Continue* once the code is accepted.

Figure 10. Continue Setup

The figure consists of two side-by-side screenshots of the Eaton user setup interface.

Left Screenshot: Set up phone authentication

- At the top is the Eaton logo.
- Below the logo is a circular icon containing a blue telephone handset.
- The heading "Set up phone authentication" is centered.
- Below the heading is the email address "newuser1234@gmail.com" with a small circular icon to its left.
- The text "A code was sent to your phone . Enter the code below to verify." is centered, followed by "Carrier messaging charges may apply".
- The label "Enter Code" is positioned above a text input field.
- The input field contains six asterisks "*****".
- A large blue button labeled "Verify" is centered below the input field.
- Below the button are two links: "Return to authenticator list" and "Back to sign in".
- At the bottom, a footer states "Use of this Eaton service is subject to these [Terms and Conditions](#)".

Right Screenshot: Set up security methods

- At the top is the Eaton logo.
- Below the logo is the heading "Set up security methods".
- Below the heading is the email address "newuser1234@gmail.com" with a small circular icon to its left.
- The text "Security methods help protect your account by ensuring only you have access." is centered.
- The heading "Set up optional" is centered.
- Below the heading is the Google Authenticator logo (a colorful star icon).
- To the right of the logo, the text "Google Authenticator" is followed by "Enter a temporary code generated from the Google Authenticator app." and "Used for access".
- A button labeled "Set up" is positioned below the text.
- A large blue button labeled "Continue" is centered at the bottom of the main content area.
- Below the button is a link: "Back to sign in".
- At the bottom, a footer states "Use of this Eaton service is subject to these [Terms and Conditions](#)".

15. Click *Create a New Organization*.

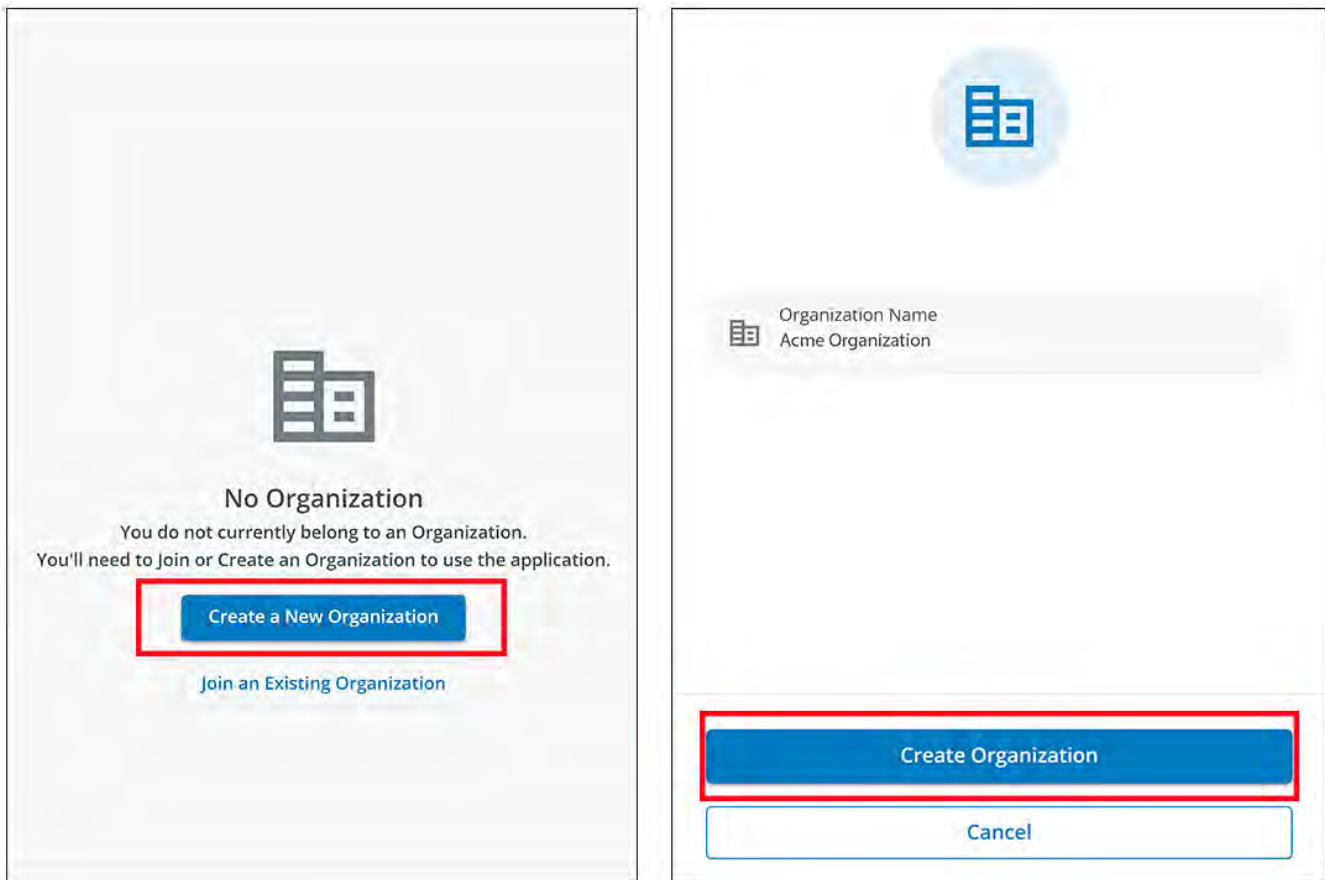


NOTE

If joining an existing organization, contact the administrator to obtain the organizational code and “Click *Join and Existing Organization*”.

16. Enter the name of the new organization. Click *Create Organization*.

Figure 11. Create a New Organization

The figure consists of two side-by-side screenshots of a web application interface. The left screenshot shows a message: 'No Organization' followed by 'You do not currently belong to an Organization. You'll need to Join or Create an Organization to use the application.' Below this text are two buttons: 'Create a New Organization' (highlighted with a red rectangle) and 'Join an Existing Organization'. The right screenshot shows a form for creating a new organization. At the top is a blue icon of a building. Below it is a text input field labeled 'Organization Name' with the text 'Acme Organization' entered. At the bottom of the form are two buttons: 'Create Organization' (highlighted with a red rectangle) and 'Cancel'.

17. The new organization is created, and the initial enrollment is complete. Click *Finish*,

Figure 12. Organization Created Successfully

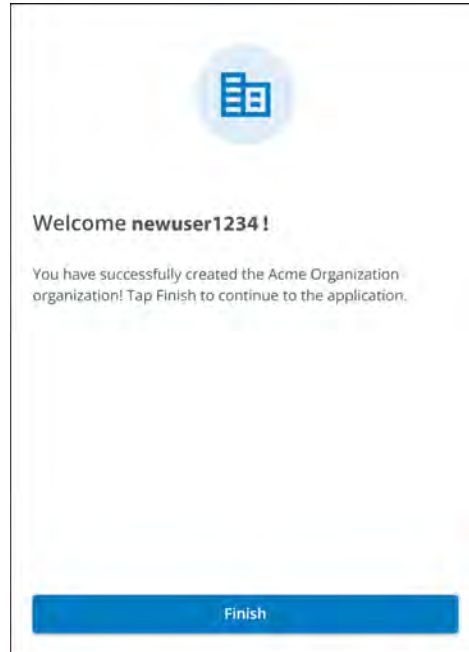


Figure 13. Organization Management Screen

A screenshot of a mobile application screen titled 'Organization'. It displays the following fields and controls:

- Organization Name ***: A text field containing 'Acme Organization'.
- Organization Code ***: A text field containing '7D71B800-BCA9-4FCE-B6C0-BB0BE2366293'. To its right is a copy icon. Below the field, it says 'This code cannot be changed'.
- Require Two-factor Authentication (2FA)**: A toggle switch that is currently turned on.
- Upload Organization Logo**: A button with an upload icon and the text 'Upload Organization Logo'. Above it is a circular logo placeholder with a blue building icon. To the right of the button, it says 'PNG, JPG (300x300px), 2 MB Max.'.
- Switch Organization**: A button.
- Create an Organization**: A button.
- Join an Organization**: A button.
- Leave this Organization**: A button.
- Permanently Delete this Organization**: A button with red text.

Chapter 2 Screens and Navigation

2.1 User Interface

The Eaton Remote Monitoring Application includes a simple summary and detailed views of the connected devices. You can view it with a web browser on a PC, such as Google Chrome, or any mobile device.

**NOTE**

Occasionally clear the browser cache, click the *Reload* button to refresh the Remote Monitoring app, or adjust your browser resolution settings. New features and updates will be released over time, and clearing the browser cache or adjusting the browser resolution settings corrects login or data visibility issues.

2.2 Login Screen

[Figure 14](#) shows the Eaton Remote Monitoring Application login screen viewed in a web browser. From the *Log In* screen, the user can enter a new enrollment, reset their password, or log in to open the Application's Overview (Home) screen.

Figure 14. Log In Screen

The login screen features the Eaton logo at the top. Below it is a text input field labeled "Email Address". Underneath the field is a checkbox labeled "Keep me signed in". A large blue button labeled "Next" is positioned below the checkbox. At the bottom of the form, there are three links: "Don't have an account? Sign up", "Need Help?", and "Privacy Policy". The screen concludes with a lock icon, the Eaton logo, and the text "Cybersecurity Certified".

EAT•N

Email Address

☐ Keep me signed in

Next

Don't have an account? [Sign up](#)

[Need Help?](#)

[Privacy Policy](#)

EAT•N
Cybersecurity Certified

2.3 Organizational Summary Screen

The *Organizational Summary Screen* displays information for all organizational groups and devices, providing easy-to-navigate paths to display information.

Figure 15. Organizational Summary Screen

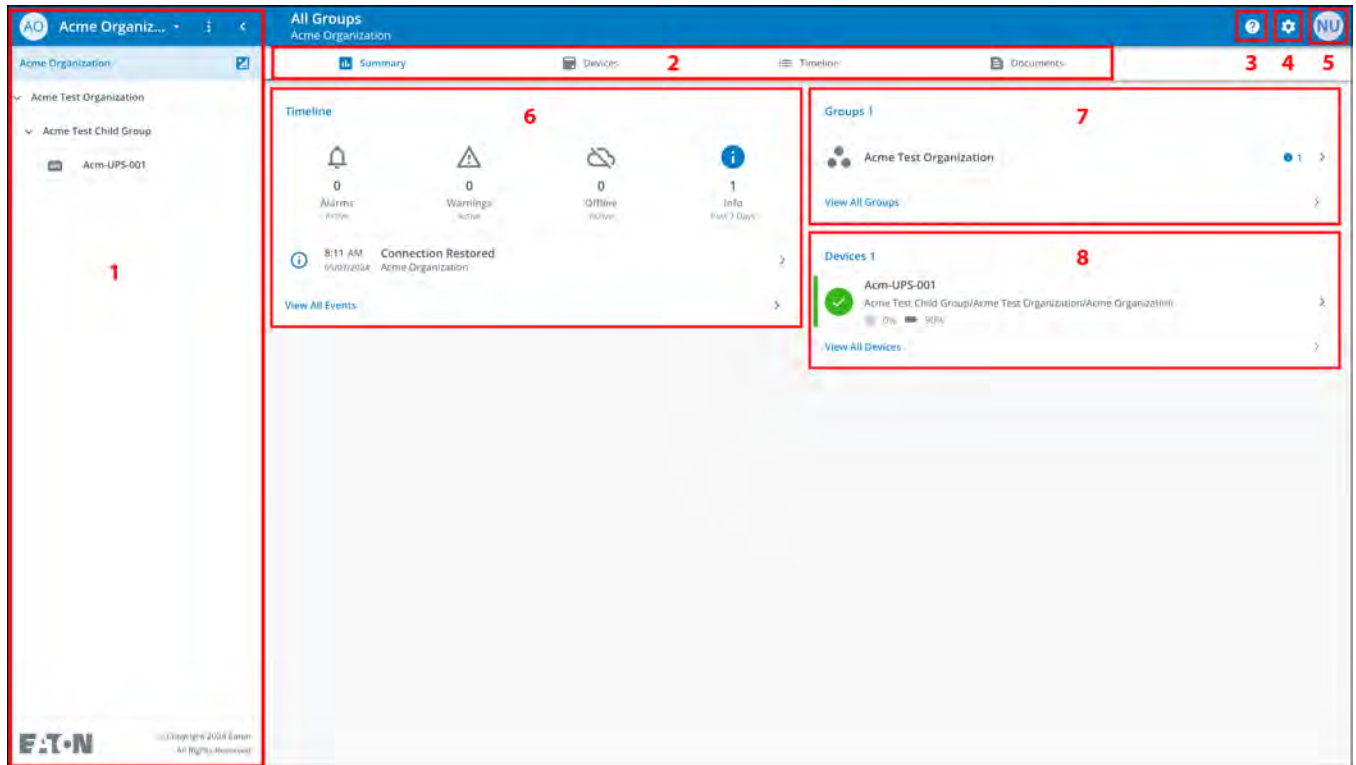


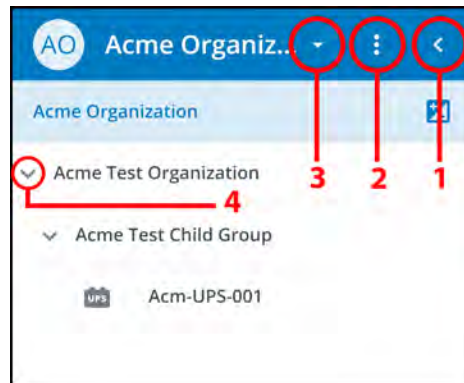
Table 1. Organizational Summary Screen Sections

① Organizational Hierarchy menu	⑤ User menu
② Tabs menu	⑥ Timeline widget
③ Help menu	⑦ Groups widget
④ Settings menu	⑧ Devices widget

2.3.1 Organizational Hierarchy Menu

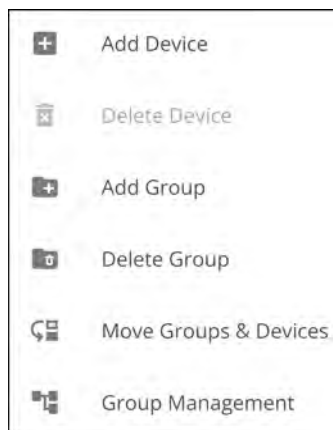
The *Organizational Hierarchy* menu manages organizational hierarchy and devices and allows users to switch between Organizations and Groups.

Figure 16. Organizational Hierarchy Menu



1. Hides or displays the Organizational Hierarchy.
2. Displays the Organizational Hierarchy function to manage groups and devices.

Figure 17. Organizational Hierarchy Menu Options



3. Switches between Organizations if more than one exists.
4. Displays the Organizational Hierarchy.

Selecting a group in the Organizational Hierarchy Menu will display the Organizational Summary Screen see .

Selecting a Device in the Organizational Hierarchy menu will display the *Device Summary* screen, which provides essential information on the status of the UPS. See .

2.3.2 Tabs Menu

The *Tabs* menu summarizes all of the data for the Organization, Group, or Device, selected in the Organizational Hierarchy Menu.

Figure 18. Tabs Menu



- **Summary Tab-** displays information for each Organization, Group, or Device as selected in the Organizational Hierarchy Menu.
- **Devices Tab-** when selected, the *Device Management* screen displays all devices that are set up for an Organization and controls adding or editing those devices.
- **Timeline Tab-** provides an overall summary of events for a specific Organization or Group that can be exported into a .csv file.
- **Documents Tab-** displays Eaton's Cloud-Connected User's Guide and sales brochures.

2.3.3 Help Menu

Clicking on this menu will explain how to contact Eaton for help and the privacy policy.

Figure 19. Help Menu Location

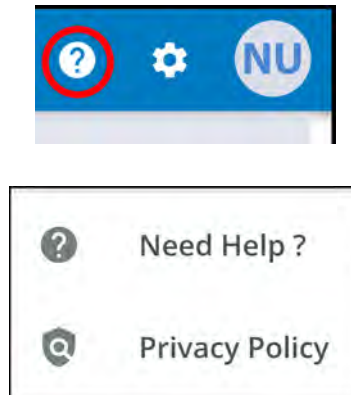
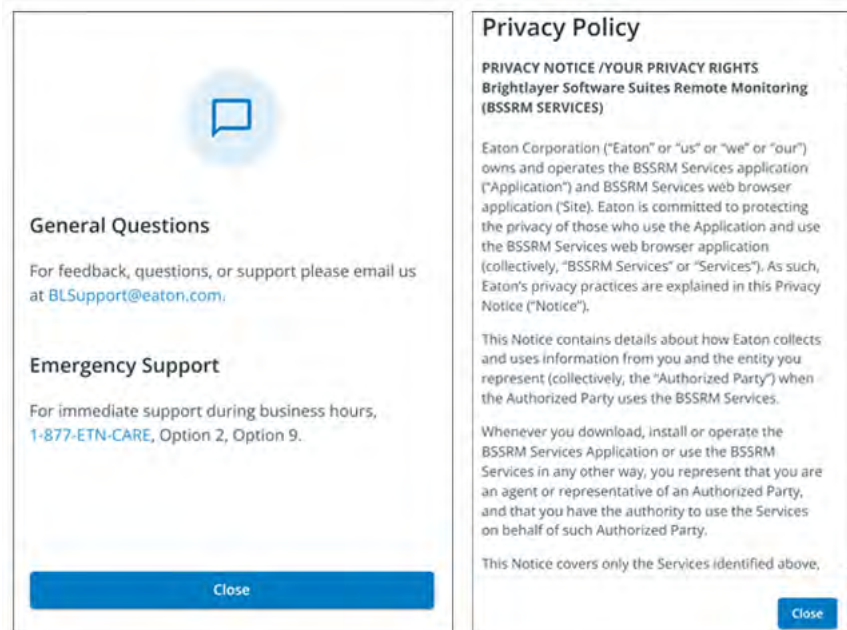


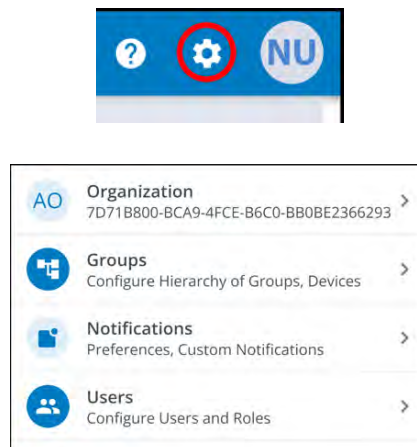
Figure 20. Help Menu Information



2.3.4 Settings Menu

Provides access to all application user settings and configuration settings.

Figure 21. Settings Menu



- **Organizational Management Settings-** displays all of the settings available to manage an Organization (see).
- **Group Management-** add, edit, move, or delete Groups within an Organization (see).
- **Notification Settings-** set and configure alarm, warning, and event notifications via email or text (SMS). Custom Notifications can also be set (see and) here.
- **User Management Settings-** allows administrators to invite other users or coworkers to enroll in the Eaton Remote Management Application either as users or as administrators. It also provides control over deleting, disabling, or enabling user accounts (see).

2.3.5 User Menu

Access the *User* menu by clicking the User avatar in the upper right corner of the *Main Organization* screen, which allows you an option to view or edit profile settings, or log out of the application.

The first section of the user profile page includes general profile information, such as email, phone number, country, an option to enable multi-factor authentication, and to designate a location to upload an image.

The second section is the role that the User holds within the Organization.

The third section displays customizable language, time zone, and date format options.

Figure 22. User Menu

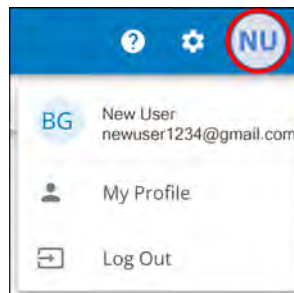


Figure 23. User Profile Screen

New User

Email: newuser1234@gmail.com

Phone Number:

US
Country

Two-factor Authentication
Required by the organization

Roles

Organization Admin
Acme Organization

Preferences

Language: English

Time Zone: (UTC-12:00) International Date Line West

Date Format: MM/DD/YYYY

2.3.6 Timeline Tab

The *Timeline* section is a valuable tool that displays active or inactive alarms and events for the entire Organization. It provides a link to specific event details and a link to the *Event Management* screen. This screen allows you to export events into a .csv file, a feature that significantly aids in data analysis and reporting. This feature helps keep track of all critical events and alarms. It can be accessed via the *Timeline* navigation tab.

Figure 24. Timeline Widget

All Groups
Acme Organization

Timeline

0 Alarms Active

0 Warnings Active

0 Offline Active

1 Info Past 7 Days

8:11 AM 05/07/2024 Connection Restored
Acme Organization

[Click to View Event Details](#)

[View All Events](#)

[Click to View all Events](#)

Figure 25. Event Details

← Acme-UPS-001
Connection Restored

Description
Connectivity to the device has been restored

Event Details		History	
Event Name	Connection Restored	Last Update Received	05/07/2024, 08:11:35
Severity	Informational	Time of Event	05/07/2024, 08:11:35

Device Details	
Name	Acme-UPS-001
Group	Acme Organization
Model	BC350RNC
Serial #	3403AV4BC884900002

Figure 26. Timeline Screen

All Groups
Acme Organization

Summary Devices **Timeline** Documents

Search

Status	Date	Type	Device	Group	
	12:56 PM 05/08/2024	On Utility	Acme-UPS-001 #3403AV4BC884900002	Acme Test Child Group < Acme Test Organization < Acme Organization	>
	12:56 PM 05/08/2024	Input Power Ok	Acme-UPS-001 #3403AV4BC884900002	Acme Test Child Group < Acme Test Organization < Acme Organization	>
	12:56 PM 05/08/2024	On Battery	Acme-UPS-001 #3403AV4BC884900002	Acme Test Child Group < Acme Test Organization < Acme Organization	CLEARED >
	12:56 PM 05/08/2024	Input Power Not Ok	Acme-UPS-001 #3403AV4BC884900002	Acme Test Child Group < Acme Test Organization < Acme Organization	CLEARED >
	8:11 AM 05/07/2024	Connection Restored	Acme-UPS-001 #3403AV4BC884900002	Acme Organization	>

Items per page 10 1-5 of 5

2.3.7 Groups Widget

The Groups widget provides a view of Groups or Child Groups within an Organizational hierarchy. It allows users to view all Groups within an Organization.

Figure 27. Groups Widget

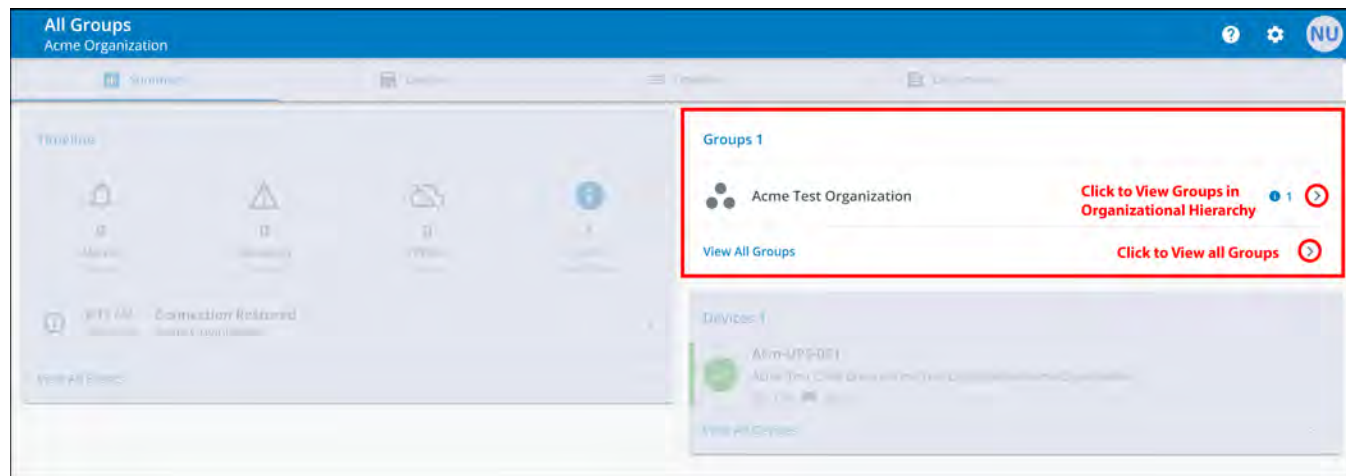


Figure 28. View All Groups



2.3.8 Device Widget

Devices can be viewed and managed by selecting the options on the Main Application page or using the Organizational Hierarchy.

Viewing Devices Main Application Page

Click any of the following areas to view a specific screen or a Device:

1. Navigate to the *Device Management* screen, which lists the Devices associated with the Organization account and allows users to move, add, or delete Devices. (See [Figure 30](#)).
2. Navigates to the *Device Summary* screen and allows users to display all of the details for a specific Device. (See [Figure 31](#)).

Figure 29. Device Widget

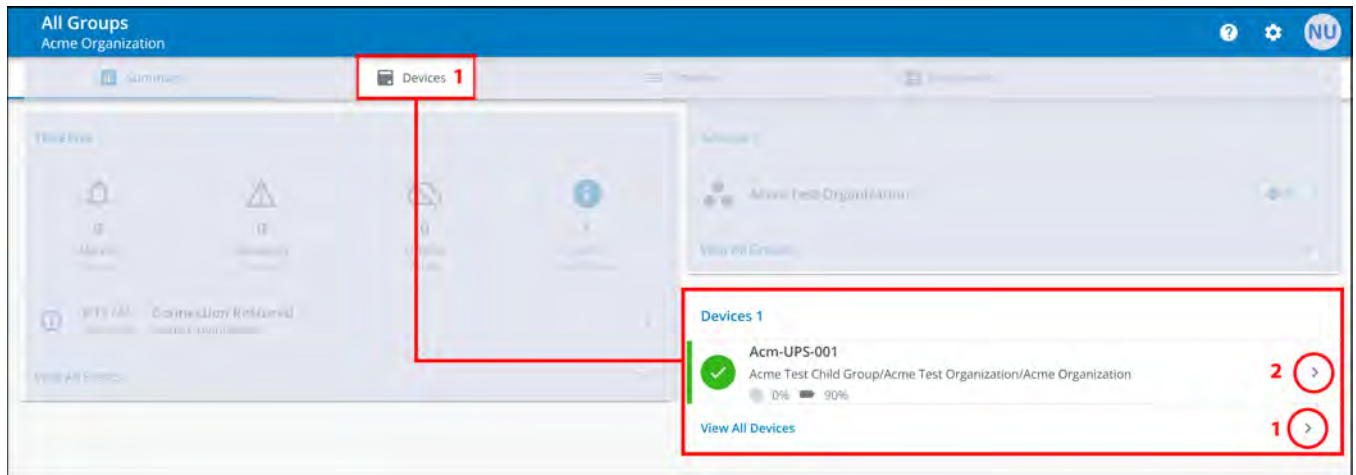
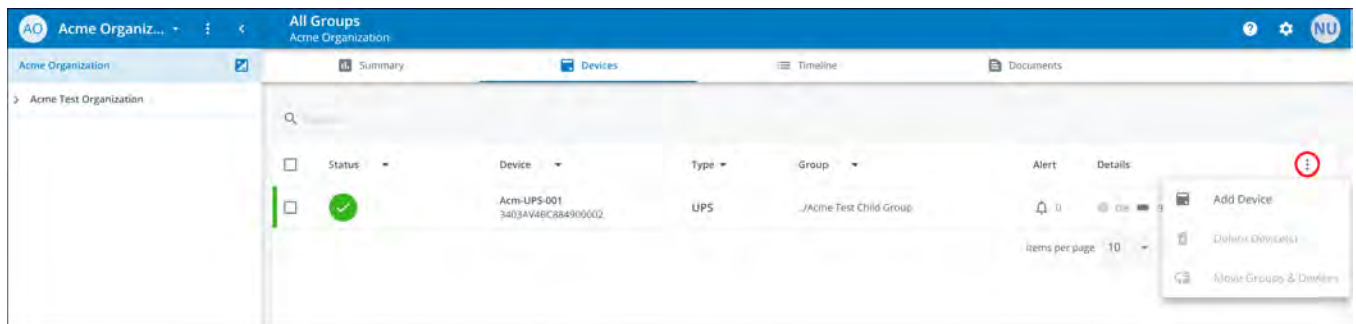


Figure 30. Device Management



The Device Management Screen

The *Device Summary* screen provides a real-time operational snapshot of all Organization-specific Devices: Status, Device Name and Serial Number, Type, Group, Alert, and details.

Figure 31. Device Summary Screen

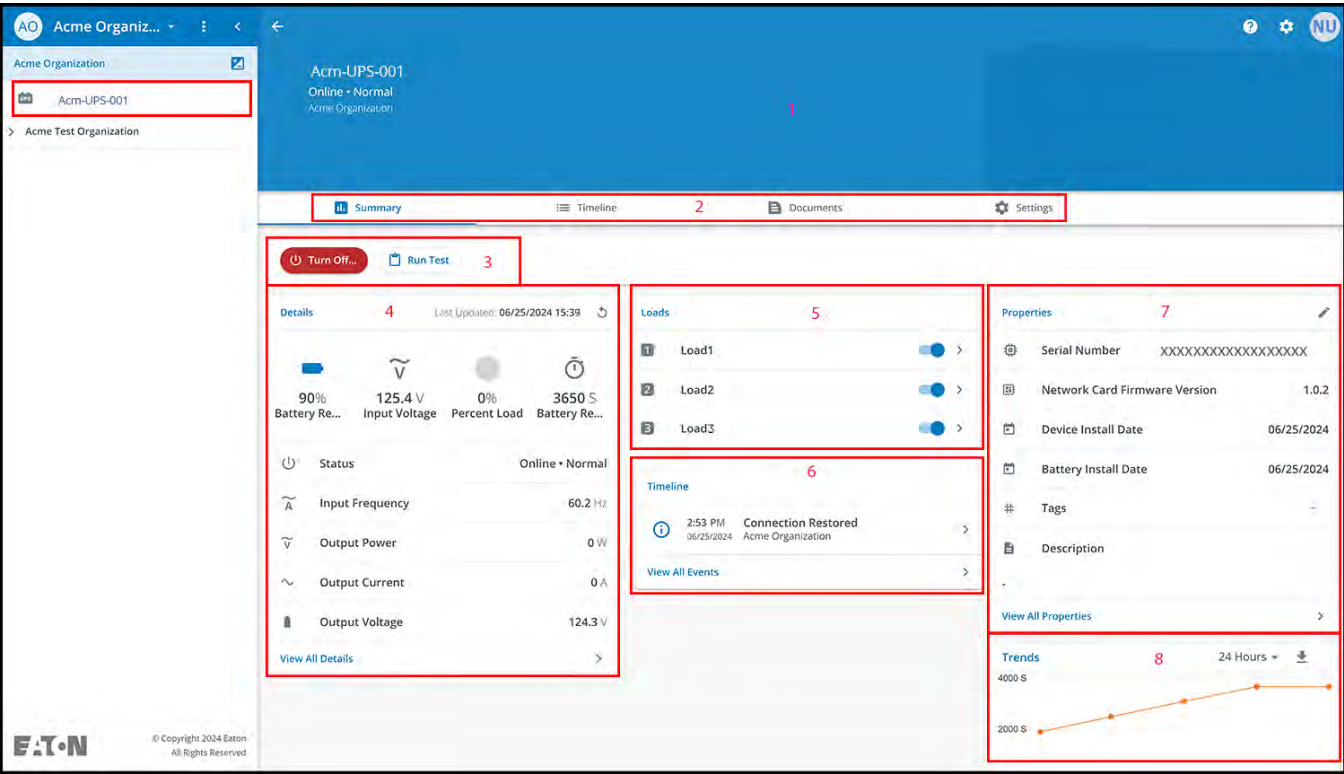
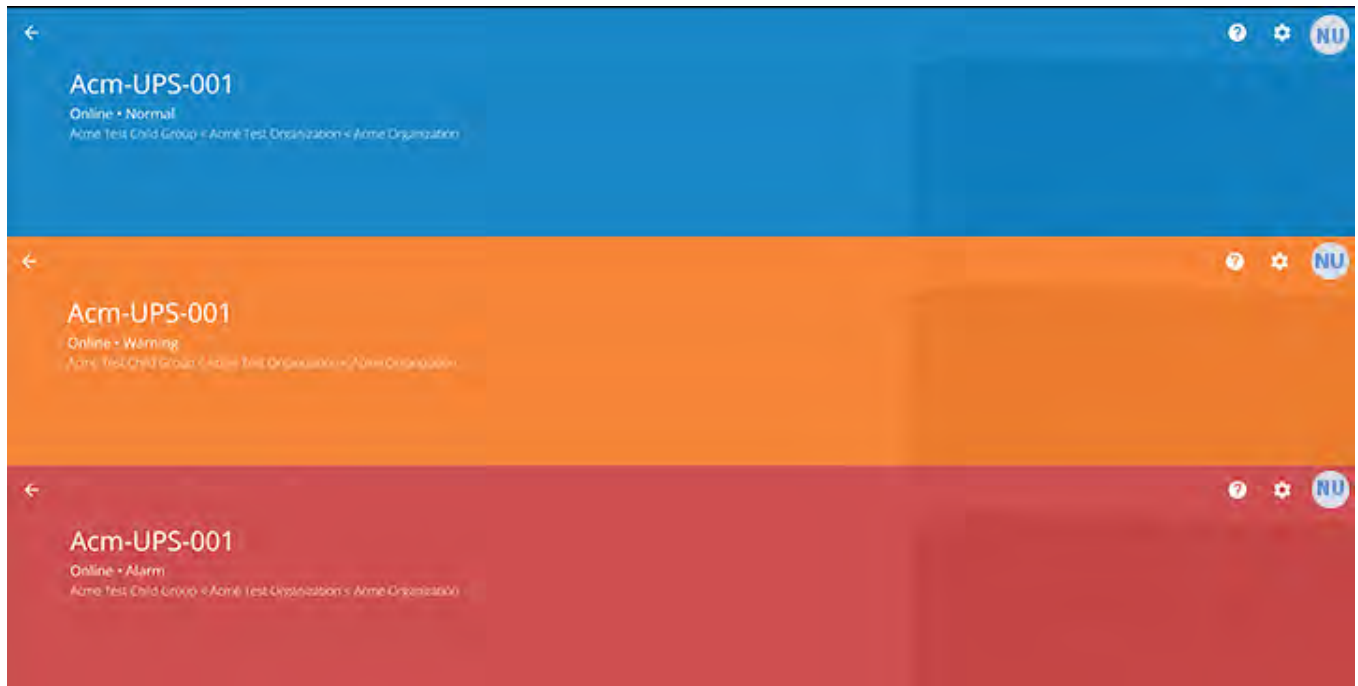


Table 2. Device Summary Screen Areas

① Device Summary Screen banner	⑤ UPS Output control
② Tabs menu	⑥ Timeline
③ Device control	⑦ Device Properties
④ Device details	⑧ Trends

1. **Device Summary Screen Banner**- changes colors, indicating the different UPS operational modes.
- Blue- Online Normal mode.
 - Orange- Online Warning
 - Red- Online Alarm

Figure 32. Device Summary Screen Banner

2. **Tabs Menu:**

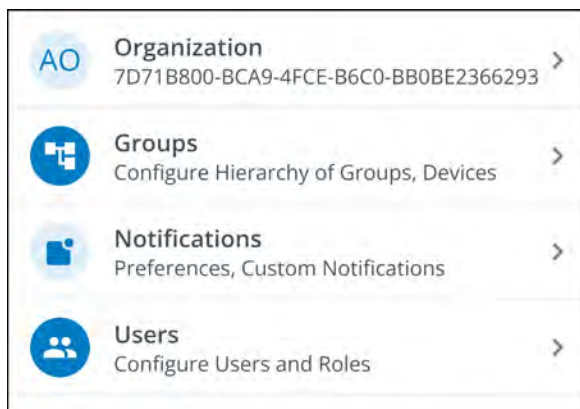
- Summary- displays the *Device Summary Screen*.
 - Timeline- provides an overall summary of events for the Device, which can be exported into a .csv file.
 - Documents- displays the Eaton Cloud-Connected User's Guide and sales brochure files.
 - Settings- general UPS settings.
3. **Device control-** provides limited control over the Device, such as turning the Device ON/OFF/CYCLE, and running a battery test.
 4. **Device details-** displays an overview of the Device's operating status, trends, and properties.
 5. **Device load control-** gives control over the output load segment(s) associated with the selected Device.
 6. **Timeline-** displays active or inactive alarms and events that can be exported into a .csv format(see).
 7. **Device Properties-**allows you to edit or view the Device information.
 8. **Trends-** displays specific UPS performance data that can be customized and downloaded over a 31-day time interval.

Chapter 3 User Management

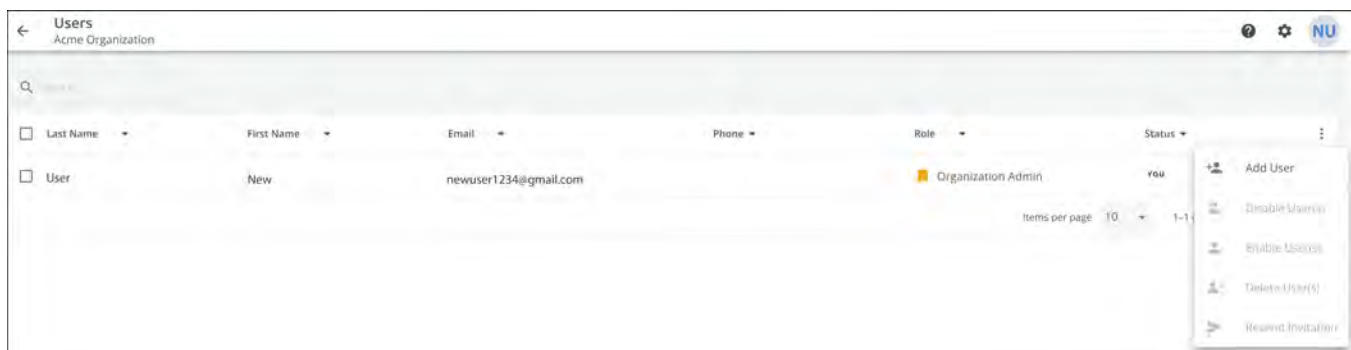
3.1 Managing Users

The *User Management* screen allows the administrator or other users to add, invite, or remove inactive members from an Organization.

To access the *User Management* screen, click on the Settings menu and select Users (Configure Users and Roles).



To add a User, click the three dots to the right of the page, then select Add User.



Enter the User information and click the Invite User button. An email will be sent to invite the new User to the Organization.



NOTE

The new Users will have to set up an account if they do not have one. See [User Enrollment and Activation](#).

Figure 33. Invite New User

Invite User to Acme Organization

Fields marked with an asterisk(*) are required.

First Name New	Last Name User2
-------------------	--------------------

Email Address*
newuser2@gmail.com

Country Code ▾

Phone Number

A mobile number is required in order to receive SMS notifications.

Select a Role*
Viewer ▾

Assign to Group(s)*
Acme Test Child Group ⓧ

Cancel

Invite And Add Another User

Invite User

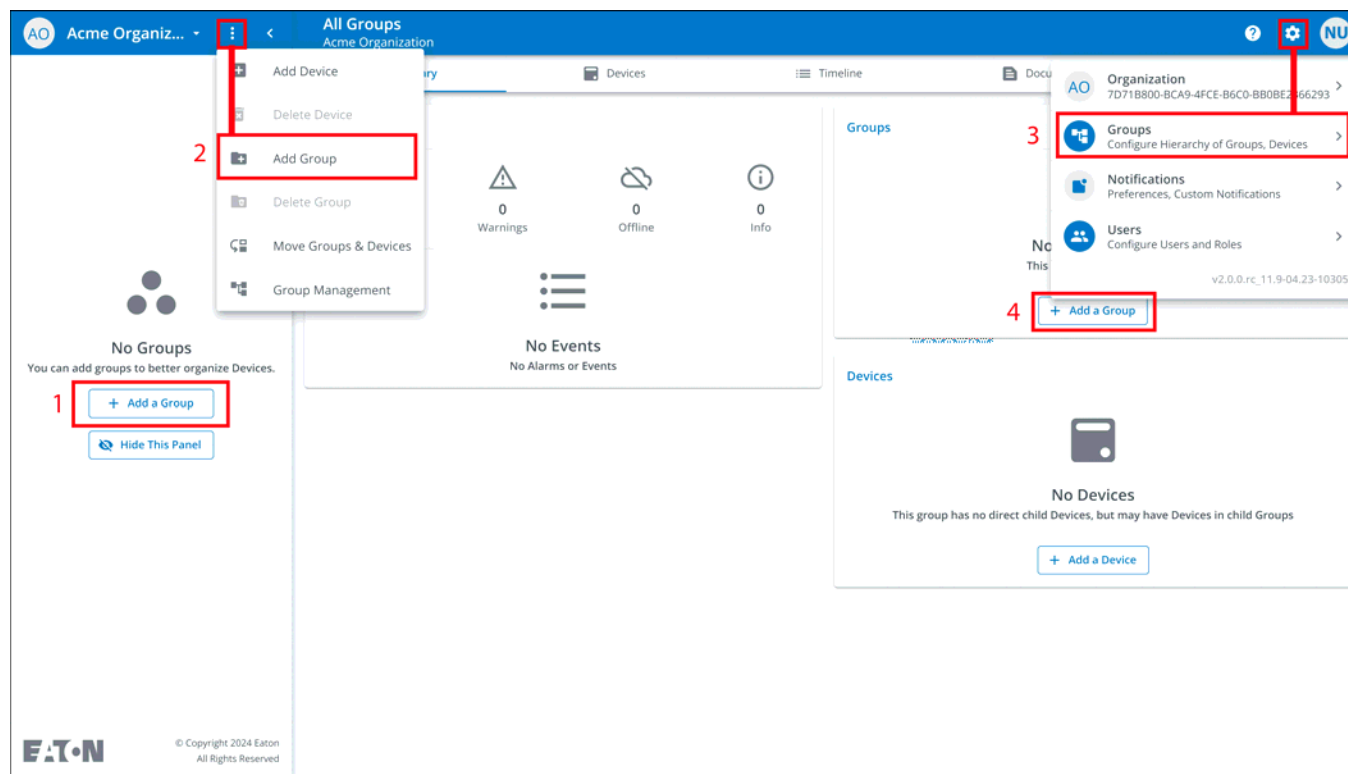
To Enable/Disable/ Delete a User select the User, and click the three dots to open the *Management* menu.

Chapter 4 Group Management

4.1 Creating a Group Within An Organization

1. Click on the *Add a Group* option on any one of the four areas on the summary screen.

Figure 34. Adding a Group



2. Enter in a name and then select the parent organization where the new Group will reside. Click *Next*.

Figure 35. Group Details

New Group

Group Details

Group Name *
Acme Test Organization
e.g., Location, Region, Division, etc. 22/24

Group Short Name
ATC
A short name can be used when displaying a breadcrumb or auto-naming a device. 3/6

Parent Group *
Acme Organization (Organization Root) ▼
This structure can also be edited from the main hierarchy page with a drag-and-drop function.

Cancel Add Group & Finish Next

3. Move any existing Groups to the newly created Group (if applicable).

Figure 36. Move Groups

New Group

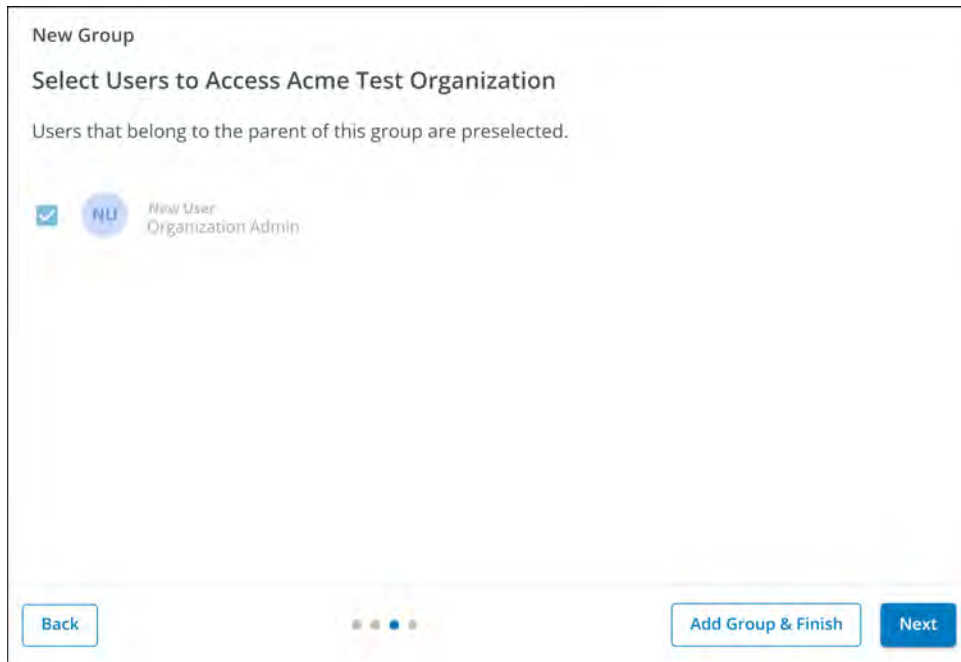
Move Existing Groups & Devices to Acme Test Organization

Existing groups can be moved to this group. Moving groups will also move their children.

Back Add Group & Finish Next

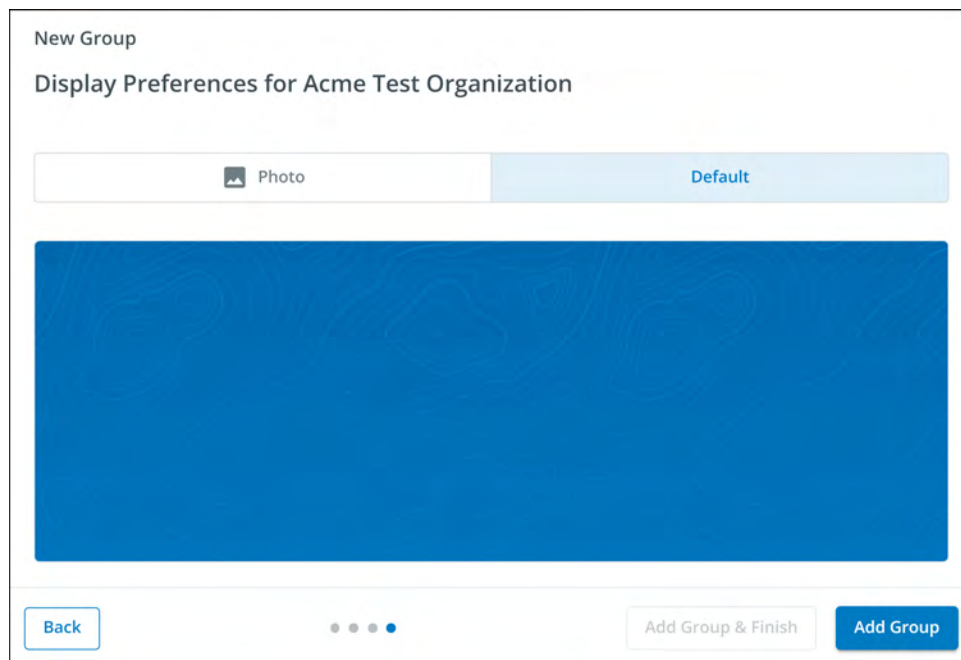
4. Assign users to the newly created Group.

Figure 37. Select Users



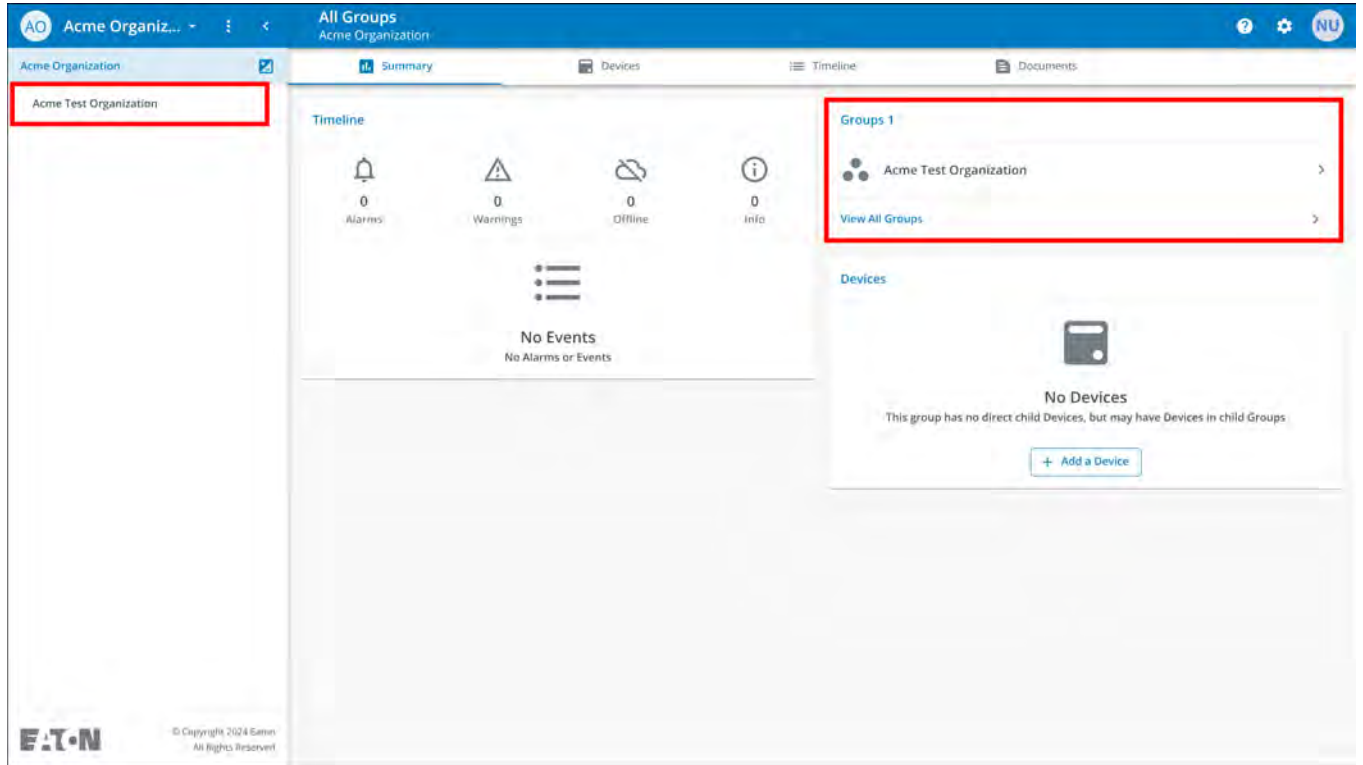
5. Choose between the default image or upload a new photo to help identify the Group. Click *Add Group* when finished.

Figure 38. Display Preferences



- The newly created Group has now been created under the Acme Organization and can now be viewed on the application Organizational Hierarchy Screen.

Figure 39. New Group



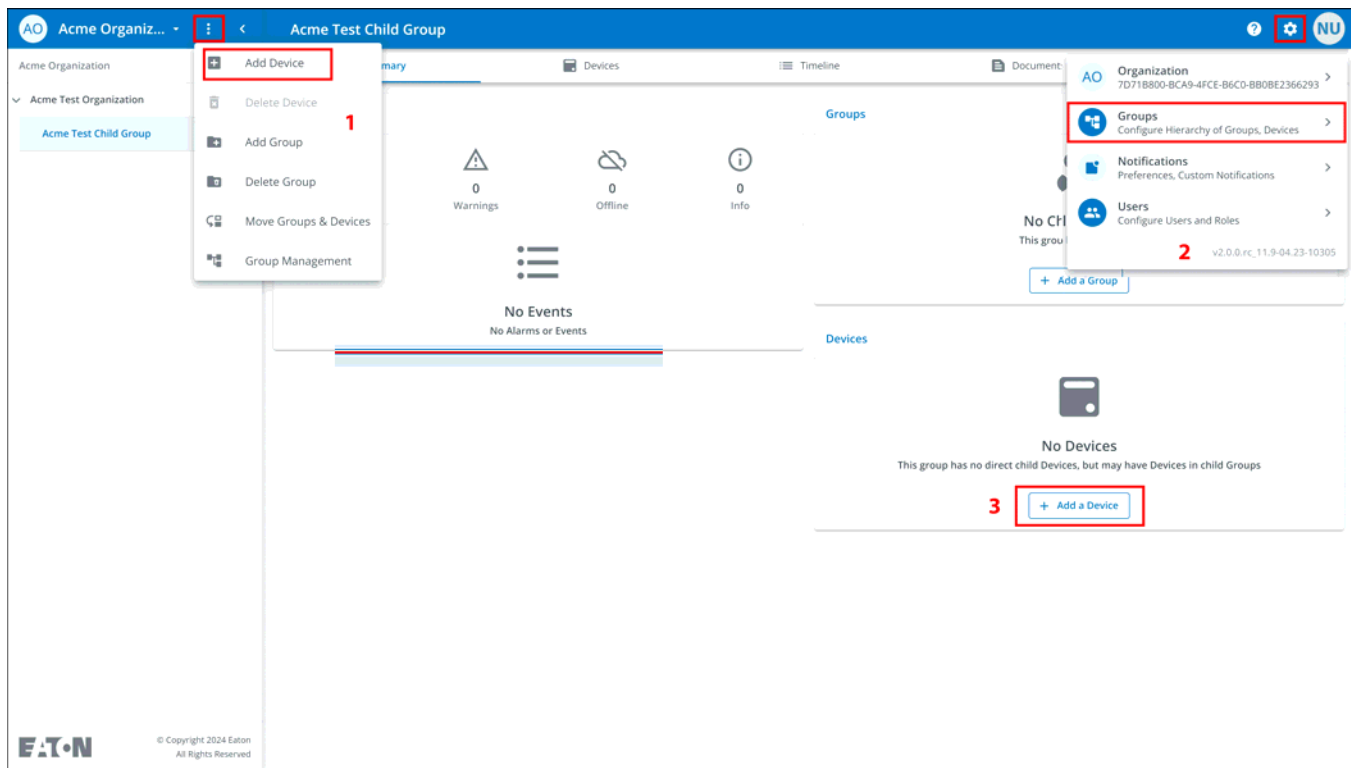
Chapter 5 Device Management

5.1 Adding a Device

Adding a Device Manually

1. Power the UPS ON and verify that it is in Online mode.
2. Connect an Ethernet cable (not supplied) from an active network connection to the port on the UPS.
3. Click the organization or group to which the device will be added in the sidebar menu.
4. Click one of the three areas of the *Group* screen or in the *Device Management* screen (see).

Figure 40. Add Device Options



- Enter all of the required information about the device. Click **Save Device**.

Figure 41. Add Device

Add Device to Acme Organization

Fields marked with an asterisk(*) are required when adding a Device.

Assign to Group(s)
Acme Test Child Group

Device Type*
UPS

Device Name*
Acme-UPS-001

GUID* **GUID is located on the UPS QR code label**

Tags
6 tags maximum

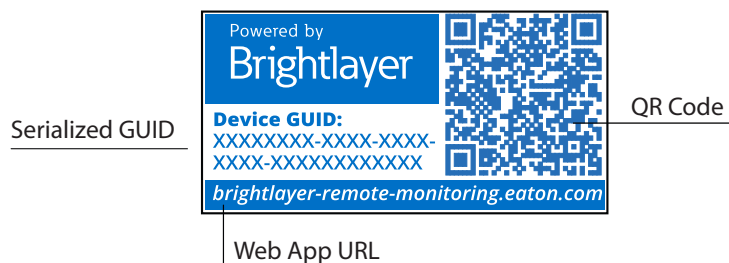
Description
Server Rack 1 Room 1

Buttons: Cancel, Save & Add New Device, Save Device



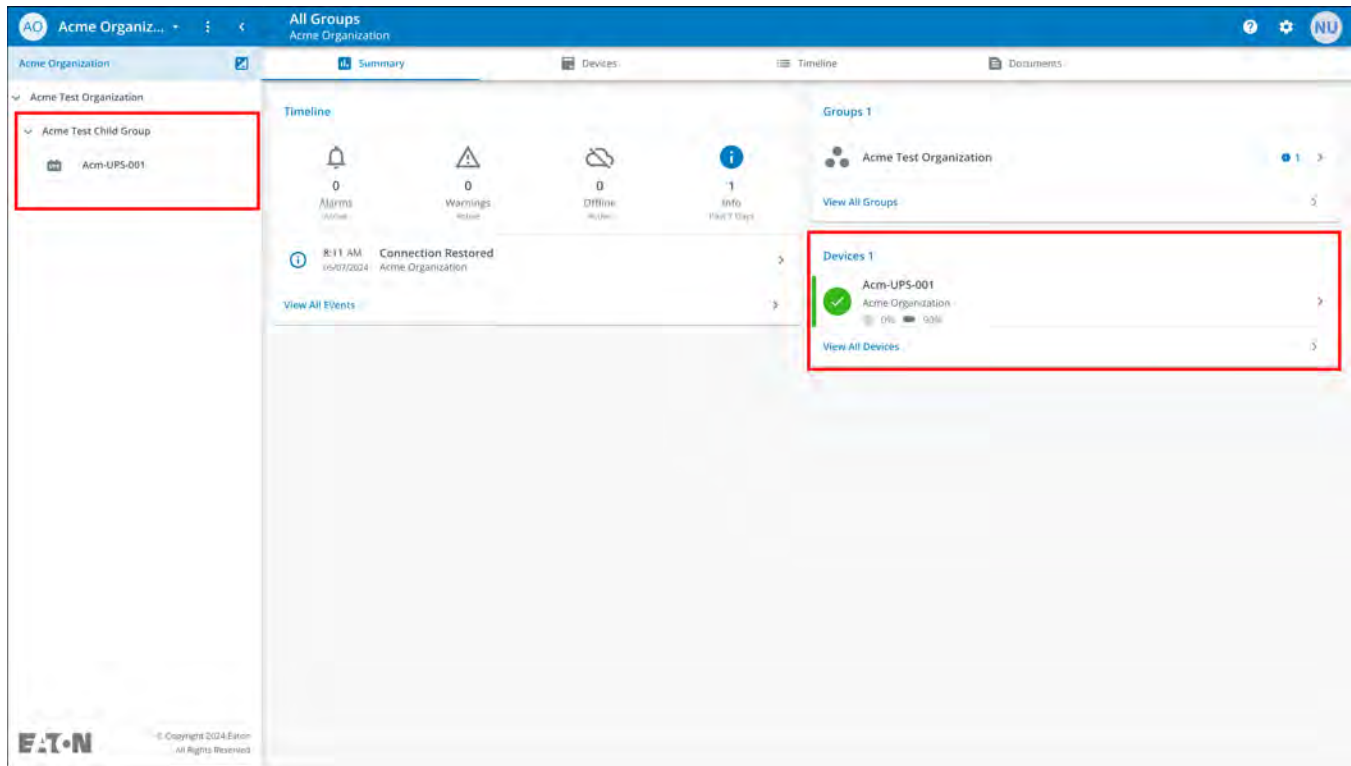
NOTE

The GUID can be found on the QR code sticker on the UPS cover.



- The device will show that it is attached to the group or organization.

Figure 42. Organization Summary Screen



5.1.1 Adding a Device with the Mobile Application

- Download the Remote Monitoring Application and create an account or log into your existing account.

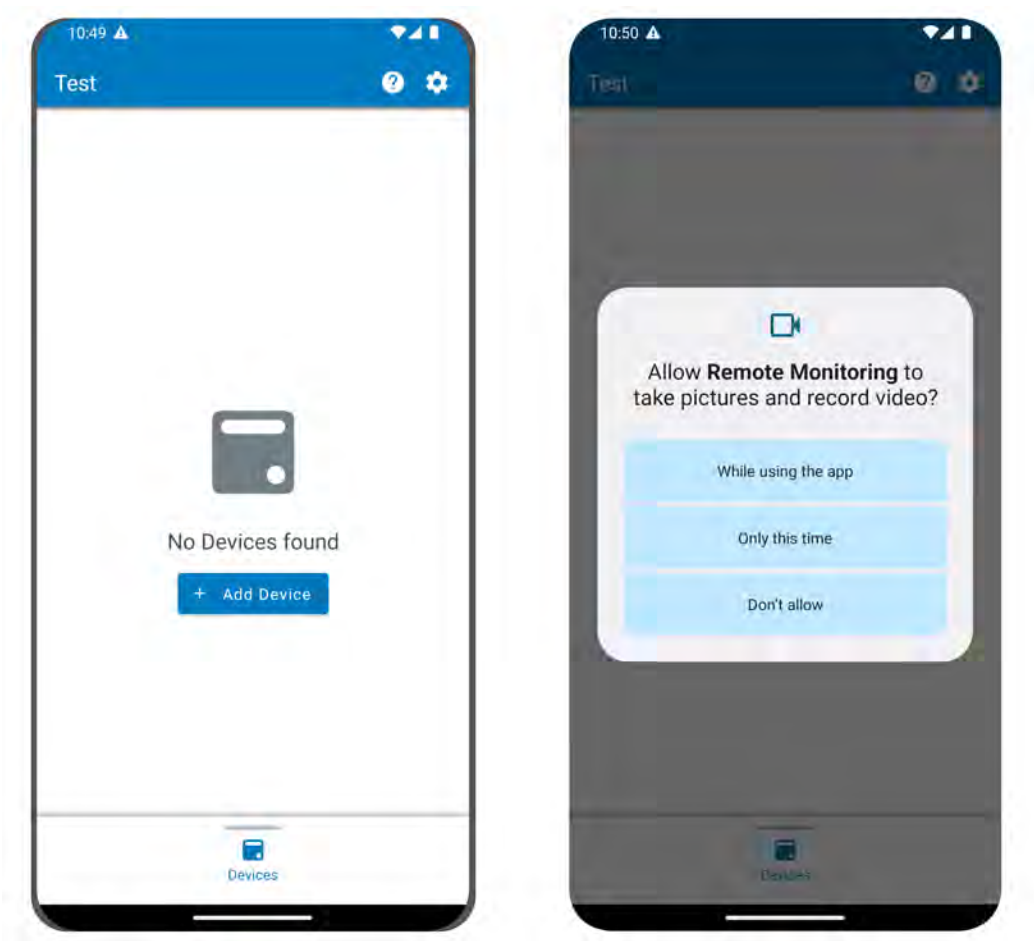


NOTE

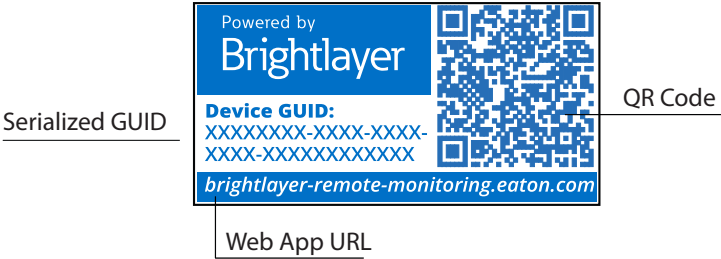
If the Remote Monitoring Application has already been downloaded to the device, the QR code will automatically take you to the *Add Device* screen in the application. If it was not previously downloaded, scanning the QR code will redirect the user to the App Store to download it and set up a user account.

- Power the UPS ON and verify that it is in Online mode.
- Connect an Ethernet cable (not supplied) from an active network connection to the port on the UPS.
- Navigate to the Organizational Summary screen and click on **Devices**.
- Click **Add Device** icon button.
- Click **OK** to allow camera access.

Figure 43. Adding a Device



7. Scan the QR code on the UPS cover.



8. Edit the Device Name, Tags, and Description. The Product ID, Serial Number, and GUID information will automatically populate. Click **Save Device**.

Figure 44. Device Information

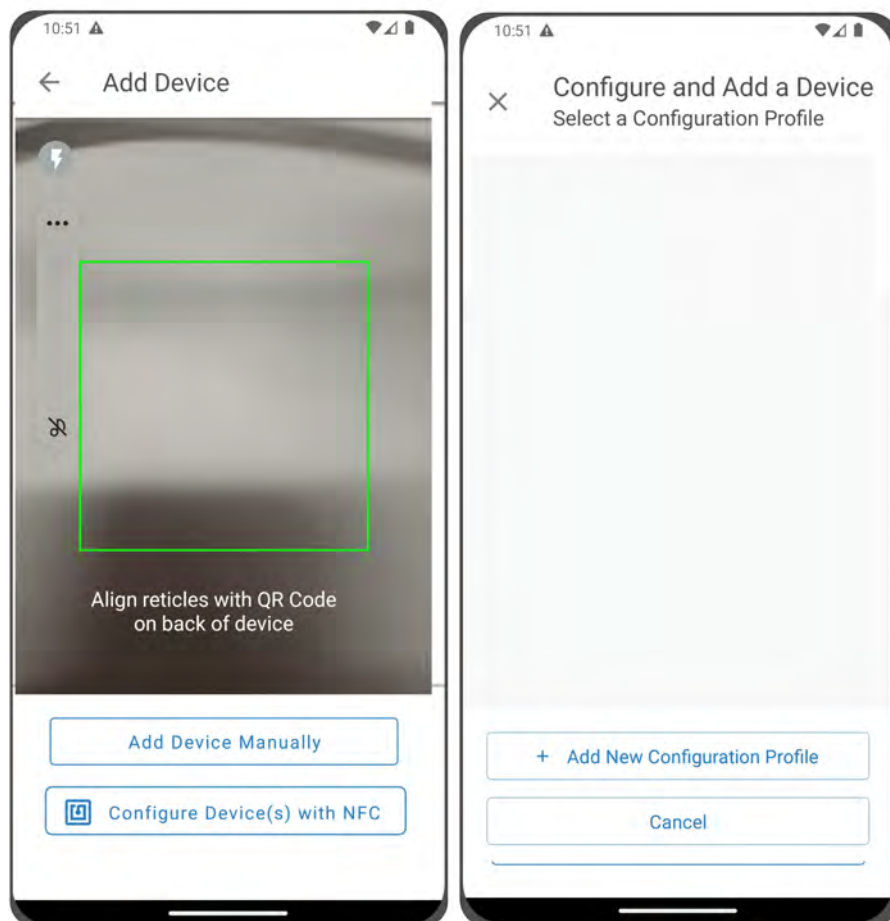
The figure displays two side-by-side screenshots of the 'Add Device' screen in the Eaton Brightlayer Remote Monitoring Application. Both screens show the same form with the following fields and options:

- Assign to Group:** A dropdown menu with 'Acme Test Child Group' selected.
- UPS:** A dropdown menu with 'ACM-UPS-001' selected.
- Product ID:** A text field containing 'ACM-UPS-001'.
- Serial Number:** A text field containing 'XXXXXXXXXXXXXXXXXXXX'.
- GUID:** A text field containing 'XXXXXXXXXXXXXXXXXXXX'.
- Network Settings:** A dropdown menu with 'Current Device Configuration' selected.
- Tags:** A text field with a placeholder '6 tags maximum' and a character count '0 / 16'.
- Description:** A text field with a placeholder '0 / 256'.
- Buttons:** 'Save Device' (blue), 'Cancel' (blue), and 'Go Back & Add New Device' (orange).

9. Check the *Organizational Summary* screen in the Application to ensure that the Device was added successfully.

5.1.2 Device Configuration via NFC

1. Power the UPS ON and verify it is in Online Mode.
2. Connect an Ethernet cable (not supplied) from an active network connection to the port on the UPS.
3. Scan the QR code label on the UPS with an NFC enabled smartphone or tablet device and create an account if needed.
4. Navigate to the Eaton Remote Monitoring Organizational Summary Screen.
5. Select the *Add Device* icon button

Figure 45. Add and Configure Device

6. Click on Configure Device(s) with NFC.
7. Click on + Add New Configuration Profile.
8. Enter in a Configuration Profile Name.
9. Select the IPv4 Method, DHCP (Automatic) or Static.

**NOTE**

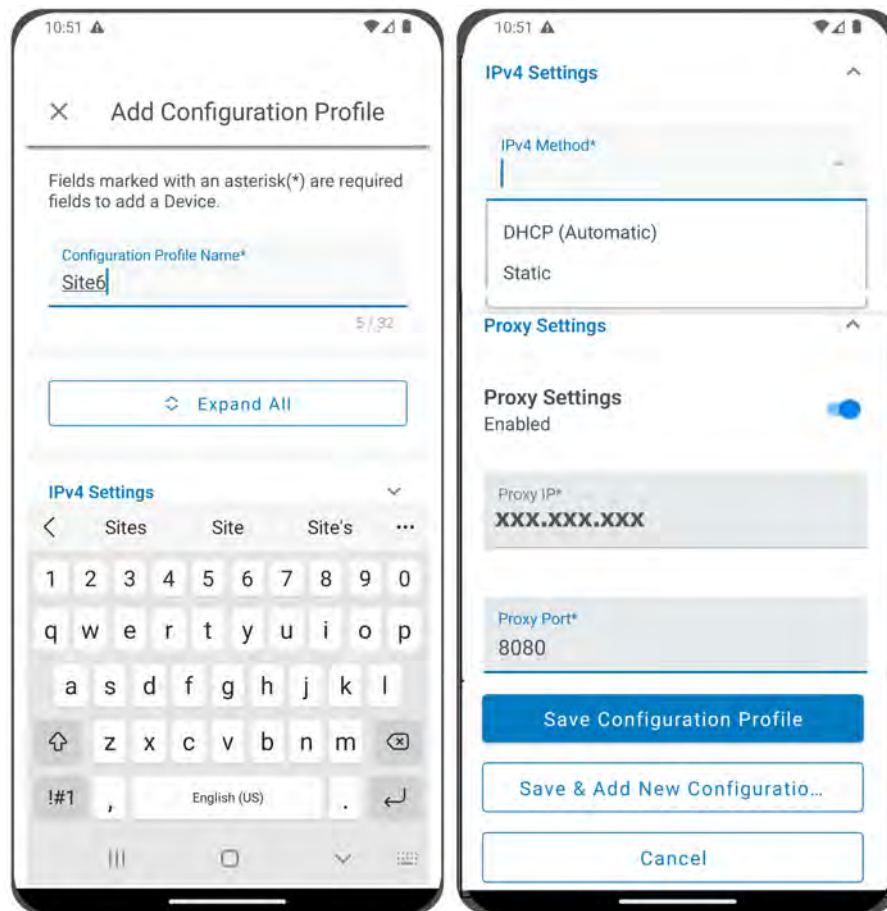
If the IPv4 method selected is Static then the subnet mask and default gateway address must be entered.

10. Set the Proxy IP address and the Proxy Port number.

**NOTE**

An additional proxy user name and password may be required.

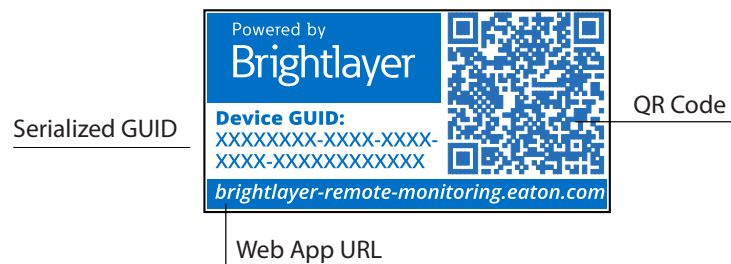
11. Click Save Configuration Profile. The Profile is now saved and ready to apply to the UPS.



12. Select a NFC profile.



13. Scan the QR code on label of the UPS to obtain the GUID.



14. Align the phone with the NFC label location on the UPS. A popup will appear if the configuration is updated. If there is a problem, an error popup will appear with the option to scan again.

**NOTE**

The NFC label location may vary depending on the UPS model.

Figure 46. UPS NFC Label Location Example



15. The device is now updated with the configuration.

Figure 47. Application Update Success



Chapter 6 Alerts and Notifications

6.1 Setting Alerts and Notifications

The *Notifications* page allows you to configure individual preferences for receiving notifications of device events via email and SMS text messages.

Three categories of notifications may be enabled or disabled.

1. **Alarms**- Alarms, incidents, device faults
2. **Warning Events**- Threshold warnings, device warnings
3. **Device Events**- Status changes, informational events

Figure 48. Preferences Notifications Screen

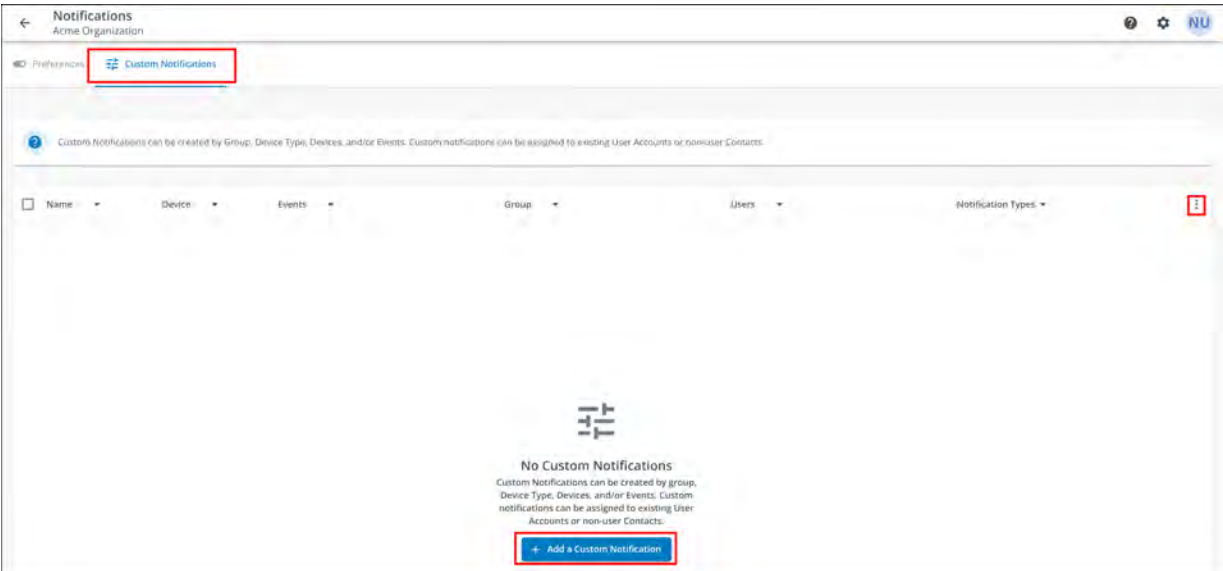
The screenshot displays the 'Preferences Notifications' screen for the 'Acme Organization'. At the top, a message states: 'You're currently setting your notification preferences for Acme Organization and the groups you have access to. Your Preferences do not affect other users.' A 'Switch Organization' link is located in the top right corner. The screen is organized into three main sections, each with a category icon and title, followed by sub-items and toggle switches.

Category	Sub-item	Status
Alarms Alarms, Incidents, Device Faults	Email Notifications	Enabled
	Text Notifications (SMS)	Enabled
Warning Events Threshold Warnings, Device Warnings	Email Notifications	Enabled
	Text Notifications (SMS)	Enabled
Device Events Status Changes, Informational Events	Email Notifications	Enabled
	Text Notifications (SMS)	Enabled
Account and Organization Your Account, Organization Changes, Role Changes		

6.2 Setting Custom Notifications

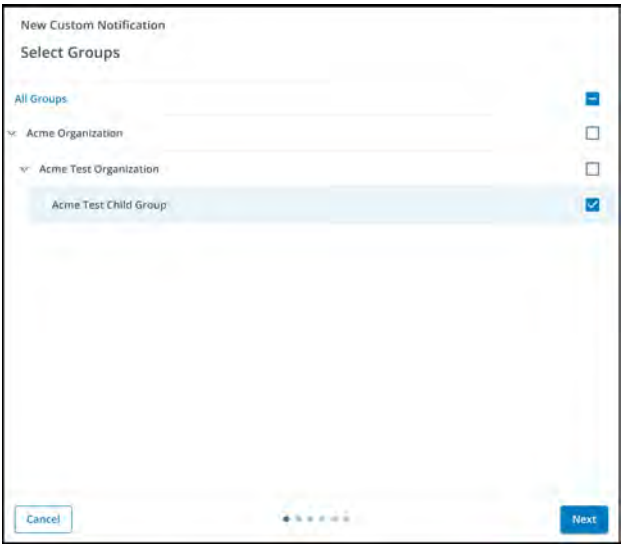
1. Click **Custom Notifications** in the top left corner of the page.
2. Click **Add Custom Notification** at the bottom of the page or the three dots on the right side of the page to add a custom notification.

Figure 49. Add Custom Notification



3. Select the Group or Organization.

Figure 50. Select Groups



4. Select the Device Type.

Figure 51. Device Type

The screenshot shows the 'New Custom Notification' interface at the 'Select Device Types' step. It features a list of device types with checkboxes for selection. The 'All Device Types' option is selected, and the 'UPS' option is also selected. At the bottom, there are 'Back' and 'Next' buttons, and a progress indicator showing the current step.

Device Type	Selected
All Device Types	<input checked="" type="checkbox"/>
UPS	<input checked="" type="checkbox"/>


5. Choose the Device.

Figure 52. Select the Device

The screenshot shows the 'New Custom Notification' interface at the 'Select Devices' step. It features a list of devices with checkboxes for selection. The 'All Devices' option is selected, and the 'Acm-UPS-001' device is also selected. At the bottom, there are 'Back' and 'Next' buttons, and a progress indicator showing the current step.

Device	Selected
All Devices	<input checked="" type="checkbox"/>
Acm-UPS-001 Acme Test Child Group < Acme Test Organization < Acme Organization	<input checked="" type="checkbox"/>

6. Select the specific event types for the notification.



NOTE Enable the Advanced feature in the top left corner to set a custom notification delay.

Figure 53. Select Event Types

New Custom Notification

Select Events

Advanced

Delay 30s

All Events

Input Wiring Fault
UPS

☒ Input Wiring Fault

☐ Input Wiring Ok

Over Temperature
UPS

☒ Over Temperature

☐ Device Temperature Ok

Input Power Not Ok
UPS

☐ Input Power Not Ok

☐ Input Power Ok

Poor Battery Health
UPS

☐ Poor Battery Health

☐ Battery Health Ok

Overload
UPS

☐ Overload

☐ Load Ok

Internal Fault
UPS

☐ Internal Fault

☐ Internal Fault Cleared

Offline

☐ Offline

☐ Connection Restored

Back

Next

7. Select the User who will receive the notifications.

Figure 54. Add Users

New Custom Notification

Select Users

All Users With Access

NU

New User
Organization Admin

You

☒

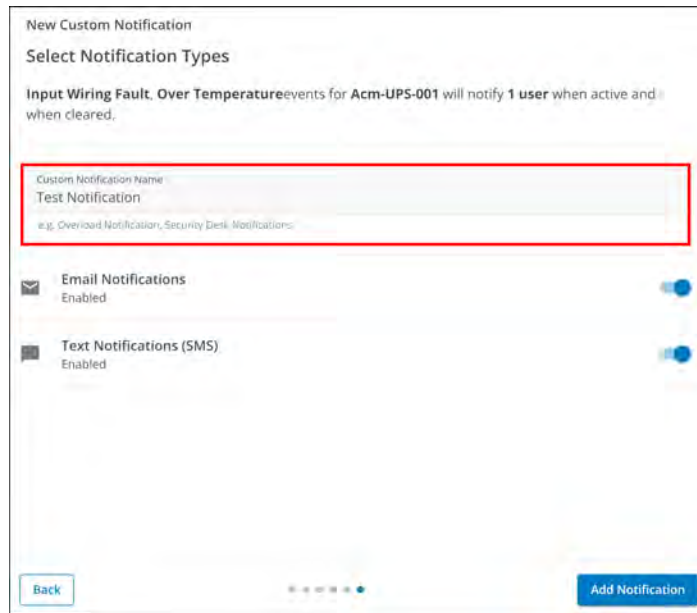
Back

Next

Setting Custom Notifications

8. Give the notification a name and enable email or text notifications. Click **Add Notification**.

Figure 55. Set Name of Notification



New Custom Notification

Select Notification Types

Input Wiring Fault, Over Temperature events for Acme-UPS-001 will notify 1 user when active and when cleared.

Custom Notification Name
Test Notification
e.g. Overload Notifications, Security Desk Notifications

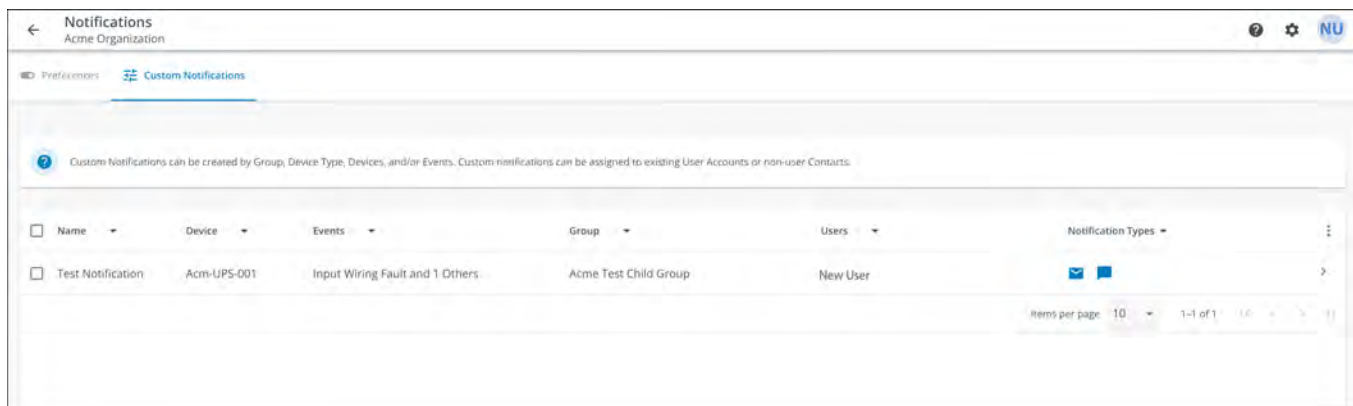
Email Notifications
Enabled

Text Notifications (SMS)
Enabled

Back Add Notification

9. The notification is created and active.

Figure 56. Custom Notification Success



Notifications
Acme Organization

Custom Notifications

Custom Notifications can be created by Group, Device Type, Devices, and/or Events. Custom notifications can be assigned to existing User Accounts or non-user Contacts.

Name	Device	Events	Group	Users	Notification Types
Test Notification	Acme-UPS-001	Input Wiring Fault and 1 Others	Acme Test Child Group	New User	Email, Text

Items per page: 10 1-1 of 1



934CF9 A