



Y6OS User Guide for Integrators

March 2025 – Version 3.4

Contents



Audience: Y6OS Authorized Admin Users



Objective: Ensure Y6OS Admin Users understand how to manage & interact with the Y6OS platform admin interface.



Additional Resources:

- [Integrator admin training videos](#)
- [Access control training videos](#)

→ [Basic Navigation](#)

- [Email Invitation](#)
- [Login](#)
- [Layout](#)

→ [Getting Started](#)

- [Add an Organization](#)
- [Add Sites](#)
- [Add Devices](#)
- [Add Users](#)

→ [Organization Functions](#)

- [Manage Organizations](#)
- [Add Organizations](#)
- [Manage My Org \(MFA, SSO, Webhooks & Org Email\)](#)
- [Manage My Account](#)

→ [Site Functions](#)

- [Manage Sites](#)
- [Edit Sites](#)
- [Create Device Group](#)
- [Central Station](#)
- [Create Schedules](#)
- [Add Sites](#)

→ [Devices](#)

- [Manage Devices](#)
- [Create a Rule](#)
- [Edit a Device](#)
- [Add a Device\(s\)](#)



Contents

→ [Access Control](#)

- [Overview](#)
- [Add Controller](#)
- [Barriers](#)
- [Barrier Groups](#)
- [Identities](#)
- [Identity Groups](#)
- [Access Schedules](#)
- [Access Rules](#)

→ [Users](#)

- [Manage Users](#)
- [Edit a User](#)
- [Add a User](#)

→ [Events](#)

- [Overview](#)
- [Create Notifications](#)
- [Create Notification for Video Monitoring](#)
- [Edit Notifications](#)
- [Log Rule](#)

→ [Contact YourSix](#)



Basic Navigation

→ [Email Invitation](#)

→ [Login](#)

→ [Layout](#)

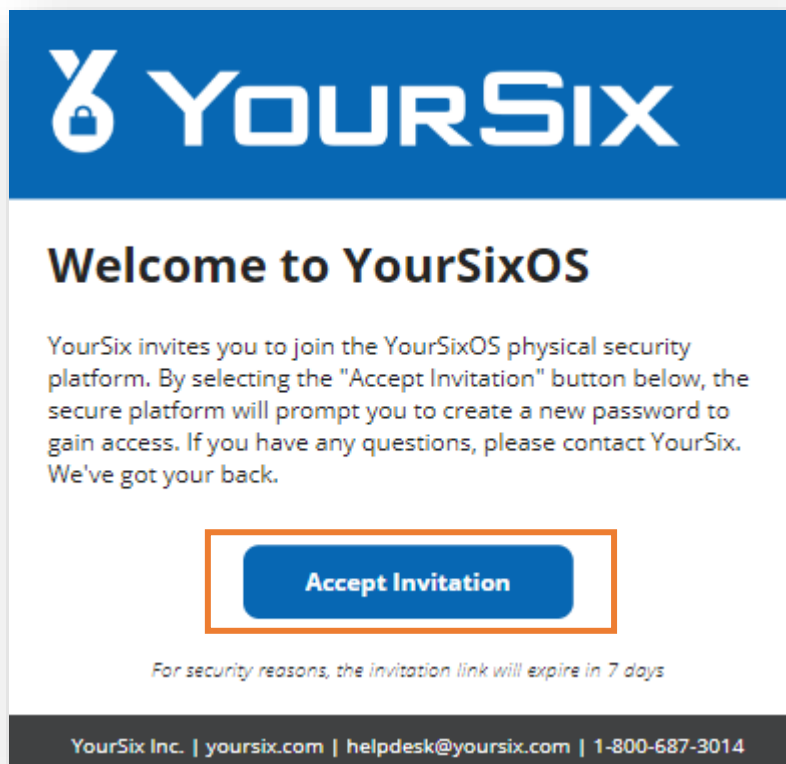
Email Invitation



Audience: Integrator Super Admin, Integrator Admin, Integrator Tech

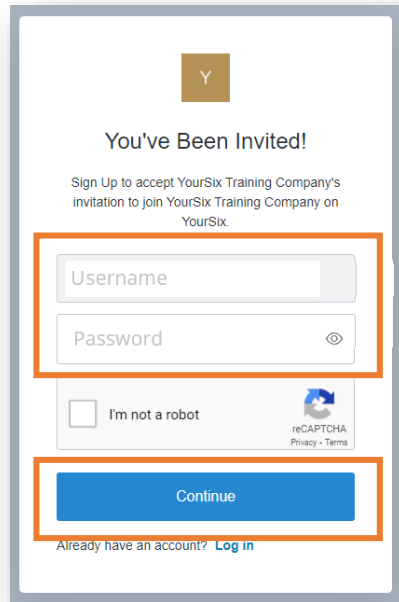
The Y6OS platform will trigger an email invitation:

- Receive email from: invite@platform.yoursix.com
- Select [Accept Invitation](#)
- Continue to next page →→→



Email Invitation

- Enter Username & Password
- Select Continue



The screenshot shows a registration form titled "You've Been Invited!". At the top, there is a brown square icon with a white letter 'Y'. Below the title, the text reads: "Sign Up to accept YourSix Training Company's invitation to join YourSix Training Company on YourSix." The form contains the following elements:

- A "Username" input field.
- A "Password" input field with an eye icon for toggling visibility.
- A checkbox labeled "I'm not a robot" next to a reCAPTCHA logo and the text "reCAPTCHA Privacy - Terms".
- A blue "Continue" button.
- A link at the bottom: "Already have an account? [Log in](#)".

Orange boxes highlight the Username and Password fields, the reCAPTCHA section, and the Continue button.

Login



Audience: Integrator Super Admin, Integrator Admin, Integrator Tech

Open a web browser:

Y6OS is supported on Google Chrome, Microsoft Edge, and Firefox; however, Google Chrome offers the richest support.

- Visit Y6OS: <https://login.platform.yoursix.com>
- Enter **Username & Password**
- Select **Continue**

The screenshot shows a login page with the following elements:

- A gold square logo with the letter 'Y' at the top center.
- The heading "Welcome" below the logo.
- The instruction "Log in to YourSix Organization to continue to YourSix." centered below the heading.
- A login form with three main sections:
 - An "Email address" input field.
 - A "Password" input field with a visibility icon (an eye) to its right.
 - A reCAPTCHA section containing an "I'm not a robot" checkbox and the reCAPTCHA logo with "reCAPTCHA Privacy - Terms" text.
- A blue "Forgot password?" link below the reCAPTCHA section.
- A large blue "Continue" button at the bottom of the form.

Layout

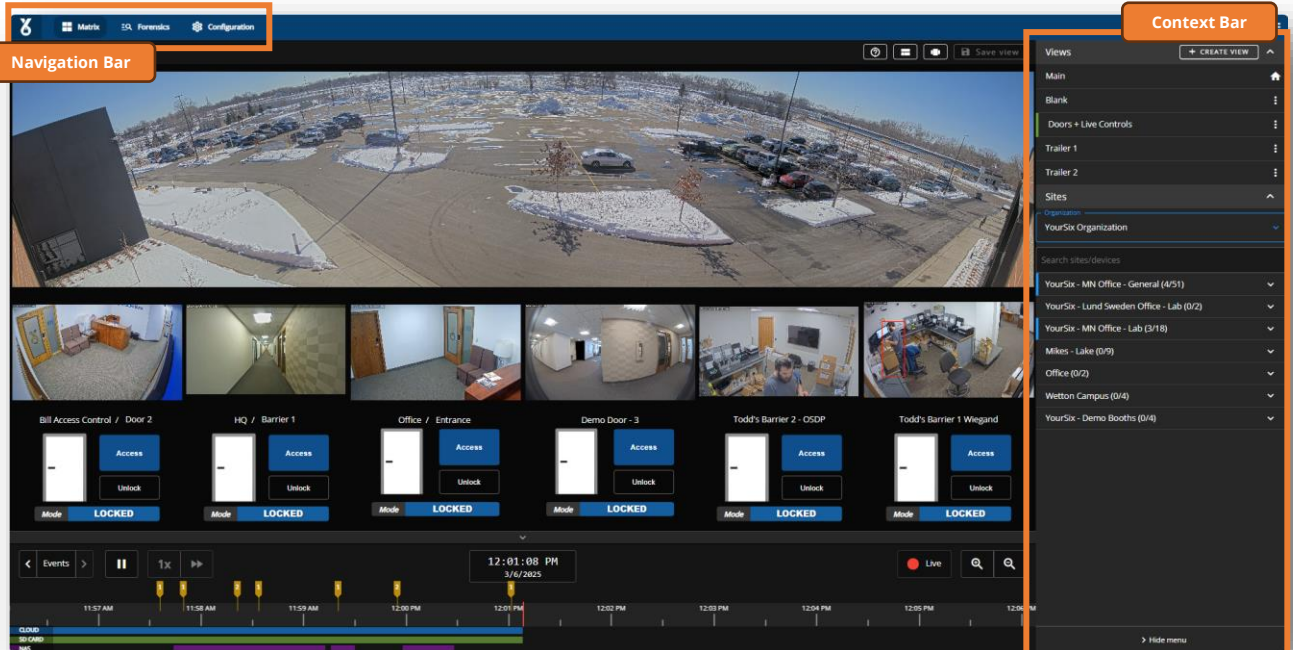


Audience: Integrator Super Admin, Integrator Admin, Integrator Tech



Additional Resources:

- [Basic navigation videos](#)



→ Navigation

- Matrix
- Forensics
 - Search Events, Access Events, Objects (Object Appearance Search)
 - Exports
 - Validator
- Configuration
 - Organizations
 - Sites
 - Devices
 - Users
 - Notifications
 - Logs
 - Access Control

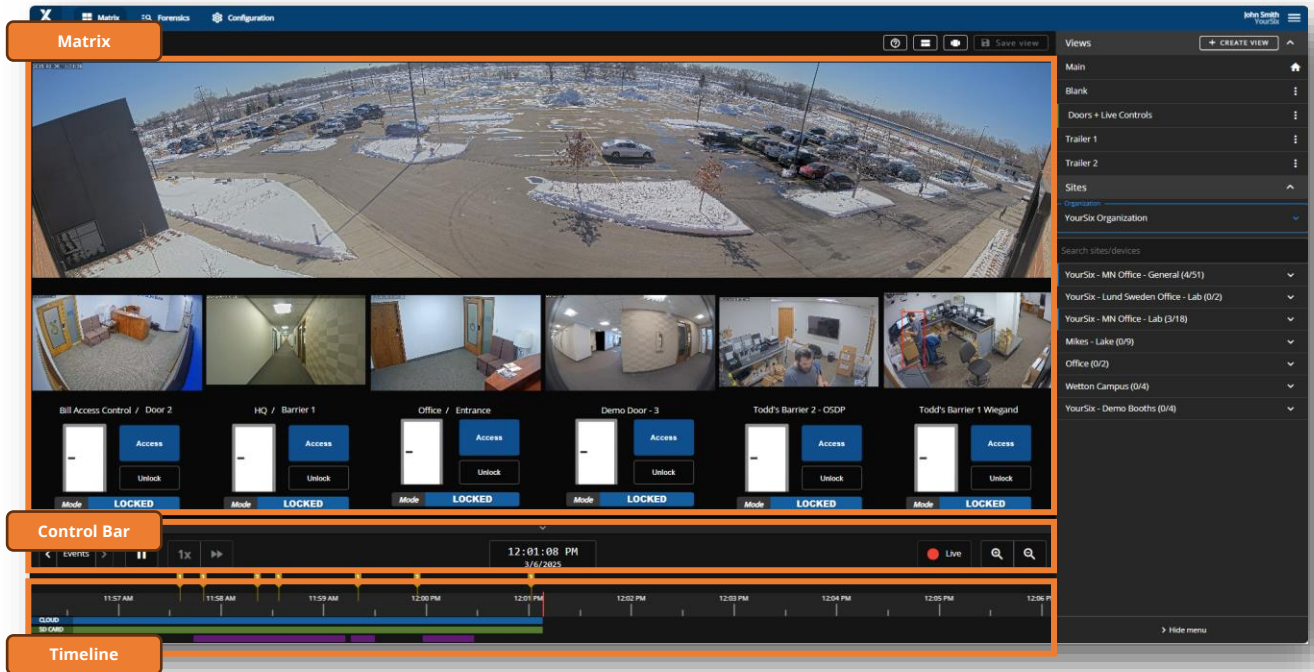
→ Context

- Favorite Views
- Views
- Organization
- Sites
- Devices

Layout



Audience: Integrator Super Admin, Integrator Admin, Integrator Tech



- **Matrix**
 - Video Thumbnails
 - Video Wall
 - Barriers (Live status and controls)
- **Control Bar**
 - Pause/Play
 - Playback Speed
 - Event Flags Settings
 - Time Stamp
 - Live Indicator
 - Zoom In/Out
- **Timeline**
 - Event Flags
 - Video Status (Cloud, SD Card, NAS)

Getting Started

These are the basic steps for getting an end-user setup within the YourSixOS platform

- [Add an Organization](#)
- [Add Sites](#)
- [Add Devices](#)
- [Add Users](#)
- [Create Recording Rule](#)

Add an Organization



Audience: Integrator Super Admin, Integrator Admin, Integrator Tech

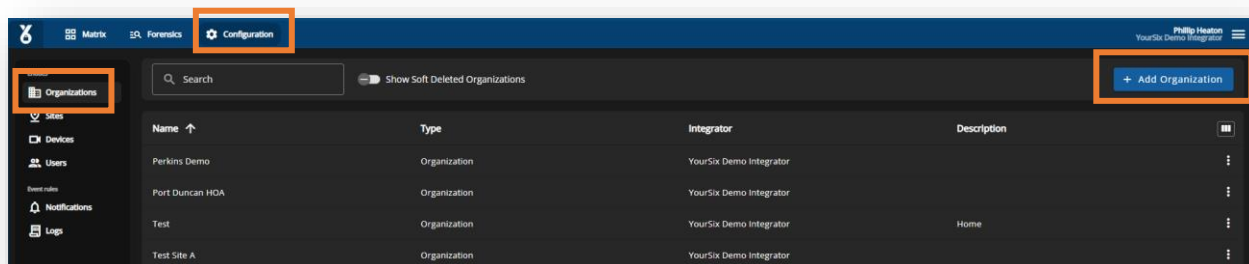


Objective: Create a new organization.



Additional Resources:

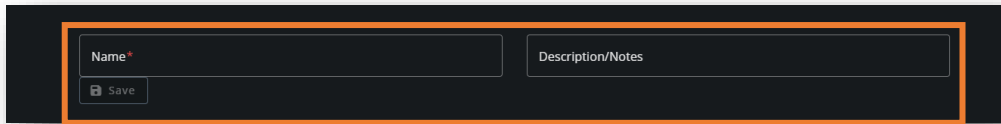
- [Get started videos](#)



Organizations are the top tier used for grouping sites and devices. All devices will be assigned to a site and all sites to an organization.

- Select **Configuration** located on the navigation bar
- Select **Organization** located on the page menu
- Select **Add Organization** located in the upper right portion of the screen
- Continue to next page →→→

Add an Organization

A screenshot of a dark-themed user interface for adding an organization. It features two input fields: 'Name*' on the left and 'Description/Notes' on the right. Below the 'Name*' field is a 'Save' button with a floppy disk icon. The entire form area is highlighted with a thick orange border.

- Name the **Organization**
- Add **Description**
- Select **Save**

Add Sites



Audience: Integrator Super Admin, Integrator Admin, Integrator Tech

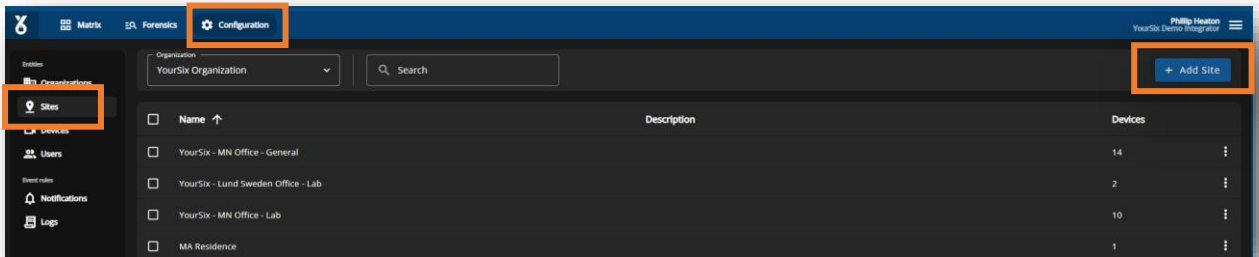


Objective: Create a new site under an organization.



Additional Resources:

- [Get started videos](#)



Sites are the second tier used for grouping devices. All devices will be assigned to a site and all sites to an organization. An organization must be created before a site can be created.

- Select **Configuration** located on the navigation bar
- Select **Sites** located on the page menu
- Select **Add Site** located in the upper right portion of the screen
- Continue to next page →→→

Add Sites

Site Information

Name*

Description

Timezone*

Organization*

- Enter the Site **Name**
- Enter a **Description**
- Select the desired **Time Zone**
- Select the **Organization** that the site should be assigned to
- Select **Save**

Add Devices



Audience: Integrator Super Admin, Integrator Admin, Integrator Tech

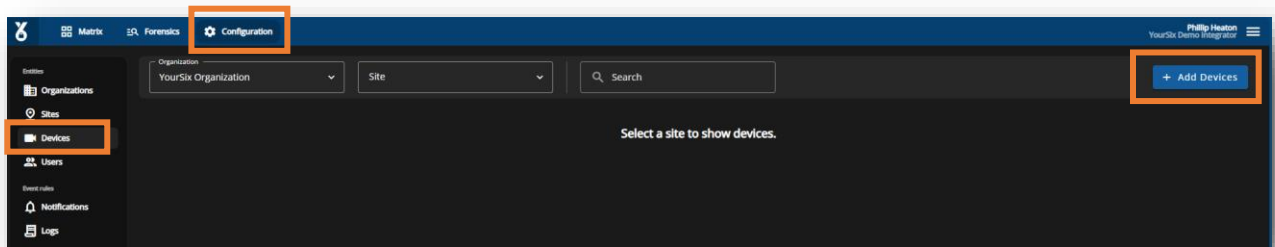


Objective: Add a device to a site.



Additional Resources:

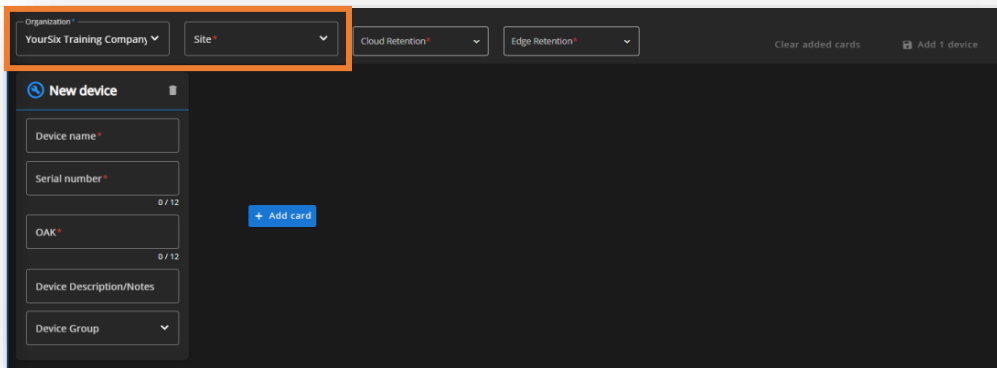
- [Enrolling a device resources](#)
- [Adding a device videos](#)



A site and organization must be created before adding a device.

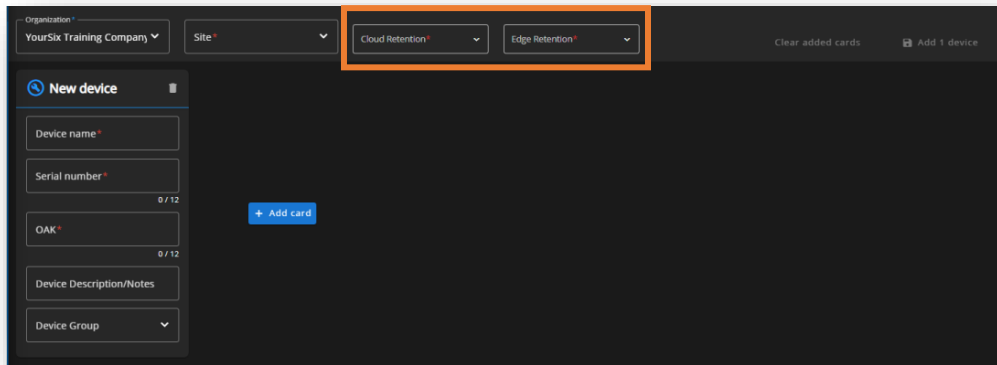
- Select **Configuration** located on the navigation bar
- Select **Devices** located on the page menu
- Select **Add Devices** located in the upper right portion of the screen
- Continue to next page →→→

Add Devices



The screenshot shows the 'New device' form in a dark theme. At the top, there are four dropdown menus: 'Organization' (set to 'YourSix Training Company'), 'Site', 'Cloud Retention', and 'Edge Retention'. The 'Organization' and 'Site' dropdowns are highlighted with an orange border. Below these are input fields for 'Device name', 'Serial number', 'OAK', 'Device Description/Notes', and a 'Device Group' dropdown. A blue '+ Add card' button is positioned to the right of the 'OAK' field. In the top right corner, there are links for 'Clear added cards' and 'Add 1 device'.

→ Select the **Organization** and **Site** that the device(s) will be added to

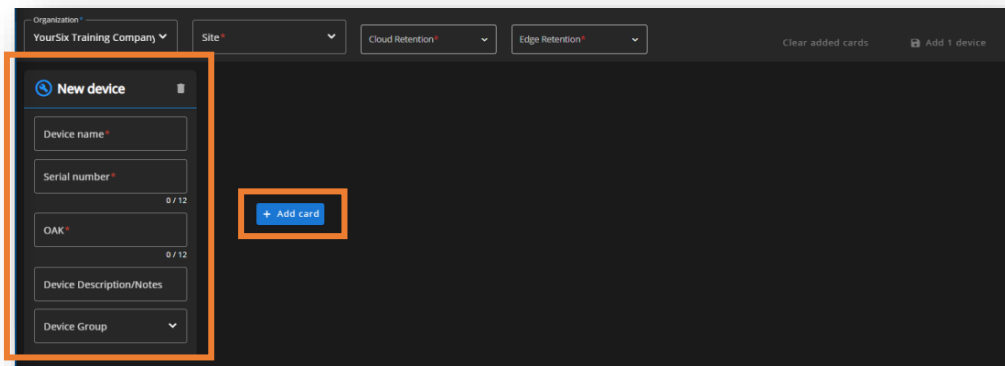


This screenshot is identical to the one above, but the 'Cloud Retention' and 'Edge Retention' dropdown menus are highlighted with an orange border instead of the 'Organization' and 'Site' dropdowns.

→ Select the **Cloud Retention** and **Edge Retention** for the device(s)

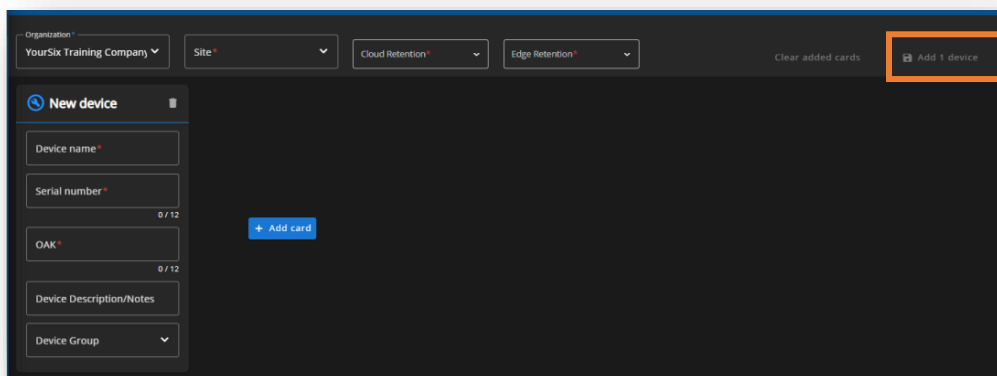
→ Continue to next page →→→

Add Devices



The screenshot shows the 'New device' form in the Y6OS interface. The form is highlighted with an orange border. It includes fields for Device name, Serial number, OAK, Device Description/Notes, and Device Group. A '+ Add card' button is also highlighted with an orange border.

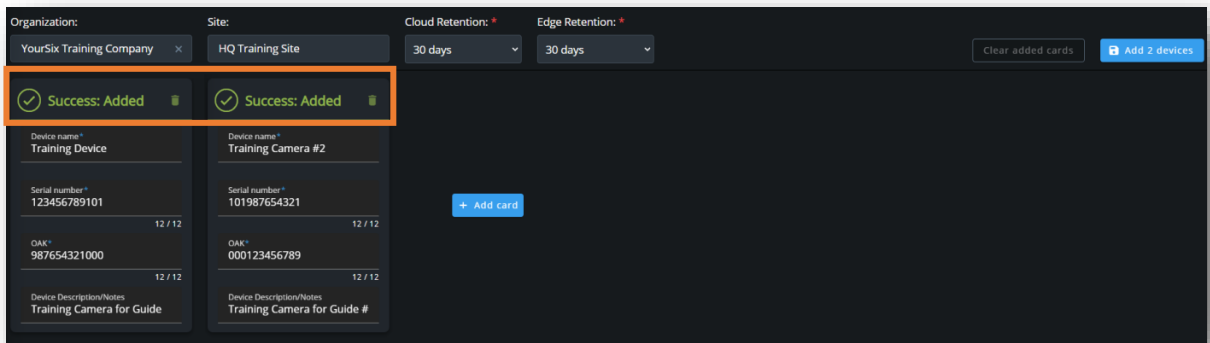
- Fill in the *Required Fields:
- Enter **Device Name**
 - Enter **Serial Number**
 - Enter **OAK**
 - *With each Axis device, you will receive a printed piece of paper with an Owner Authentication Key (OAK). You need the OAK to verify ownership when you register the device with an O3C-based service.*
 - Enter **Device Description/Notes**
 - Select **Device Group**
- If you are adding multiple devices to the same site with the same cloud and edge retention, you can select the **+Add card** button. This will allow you to mass upload devices.



The screenshot shows the 'New device' form in the Y6OS interface. The '+ Add device' button is highlighted with an orange border.

- Select **Add "#" devices** button
- Continue to next page →→→

Add Devices



→ Confirmation of device addition: **Green Check Mark and Success: Added**

→ Physical Connection:

- Plug the device into a secure power & internet source
 - *If the device is not new, please factory reset the device by holding down the control button while plugging the device into its power source. Continue to hold the Control Button for 15 seconds until the status LED flashes amber and then release the button. The process is complete once the status LED turns green for a moment.*
- On the physical device, press and hold the control button for 3 seconds until the light flashes and then release the button. This will connect the device to the platform

Troubleshooting:

- [Adding a device troubleshooting](#)

Add Users



Audience: Integrator Super Admin, Integrator Admin

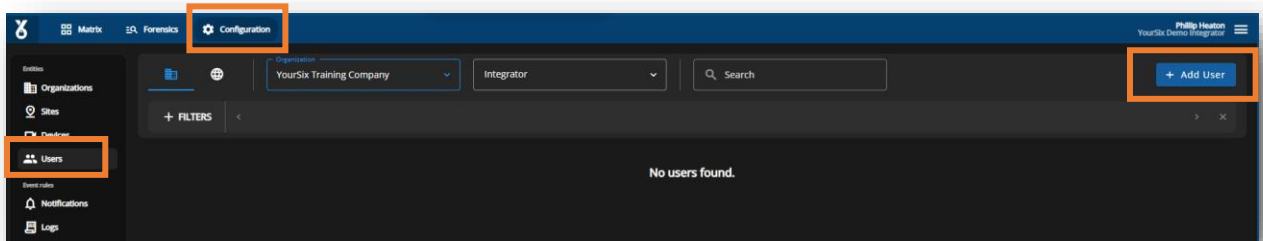


Objective: Add new users to an organization or integrator.



Additional Resources:

- [Adding user videos](#)
- [Scopes and permissions overview](#)



- Select **Configuration** located on the navigation bar
- Select **Users** located on the page menu
- Select **Add User** located in the upper right portion of the screen
- Continue to next page →→→

Add Organization Users

User Information

Account Details:

First Name * Last Name *

Email *

Account Roles: [Create Integrator User](#)

Organization
YourSix Organization

Roles *
User's global roles within system.

Save

- Enter information into the required fields
- Select the [Organization](#) the user will be associated to
- Select the [Account Role](#) the user should have for access
 - Please reference the Y6OS User Permission Guide when choosing the desired role for the user.
- Select [Save](#)
- To add an Integrator User, Select [Create Integrator User](#) in the upper right.

Add Integrator Users

User Information

Account Details:

First Name * Last Name *

Email *

Account Roles: [Create Organization User](#)

Roles *
User's global roles within system.

Save

- From the Create Organization User page, select Create Integrator User.
 - Please see the previous page for details.
- Enter information into the [required fields](#).
- Select the [Account Role](#) the user should have for access
 - Please reference the Y6OS Permission Guide when choosing the desired role for the user.
- Select [Save](#)

Create a Rule



Audience: Integrator Super Admin, Integrator Admin, Integrator Tech

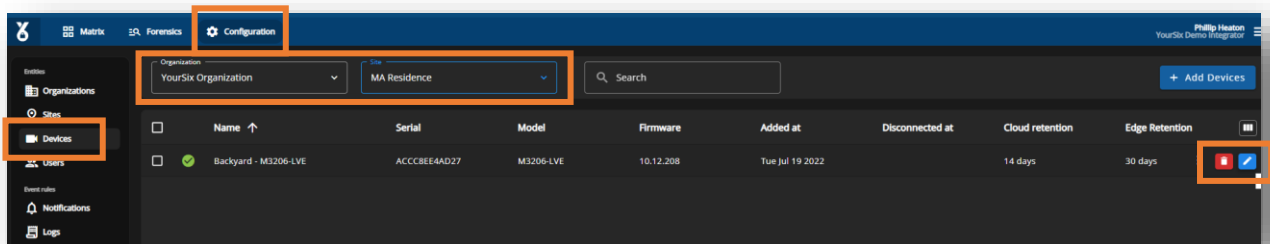


Objective: Create a recording rule.

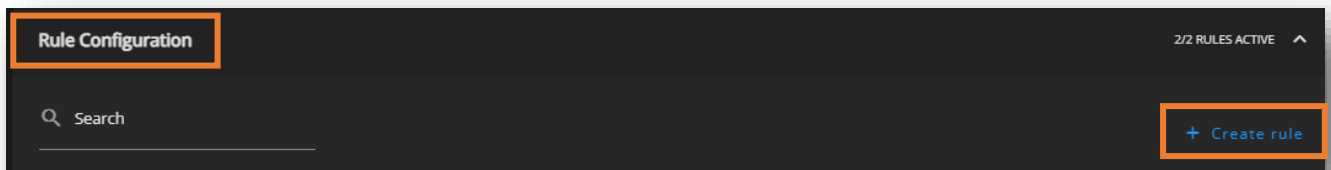


Additional Resources:

- [Recording rules best practices](#)
- [Recording rules and storage videos](#)



- Select **Configuration** located on the navigation bar
- Select **Devices** located on the page menu
- Use the **Organization, Site** and **Search** bar to locate the device you wish to edit
- Select the **Pen** icon to edit the device
- On the Edit Device page locate the **Rule Configuration** section and select **Create Rule**
- Continue to next page →→→



Create a Rule

The screenshot shows a configuration window for a 'Training Rule'. The 'Name' field is 'Training Rule'. The 'Sources' section has 'Overview', 'Panorama', 'View Area 2', and 'View Area 3' selected. The 'Trigger' section has 'Schedule' set to 'VMD' and 'Select profile' set to 'Profile 1'. The 'Action' section has 'Record to cloud' and 'Record to Edge SD' selected. The 'Prebuffer' is 10, 'Postbuffer' is 10, 'Frame rate' is 8, and 'Resolution' is 720x720. 'Close' and 'Save' buttons are at the bottom.

Motion Based Rule: Record when motion is detected

- Enter the Rule **Name**
- Select the **Schedule**
- Select the **Source** (Limited to multisensor and panoramic devices)
- Select the **Trigger**
 - VMD: Motion detection recording → Select profile: Profile 1 unless additional profile has been created
- Select the **Action** (when motion is detected):
 - Record Audio (if applicable)
 - Record to the Cloud
 - Record to the Edge
- Select **Recording settings**:
 - Prebuffer (Recording before the trigger) → Value is seconds
 - Post buffer (Recording after the trigger) → Value is seconds
 - Frame rate → Value is FPS
 - Resolution
- Select **Save**

Create a Rule

Create rule

Name*
Training Rule

Sources:

Overview ✓ Panorama ✓ Double Panorama Quad View
View Area 1 ✓ View Area 2 ✓ View Area 3 ✓ View Area 4
Corner Left Corner Right Double Corner Corridor

Trigger:

Schedule VMD
Select schedule: + Add Site Schedule
Always Test 1 Test 2

Action:

Record to cloud Record to Edge SD
Frame rate: 8 Resolution*: 720x720

Close Save

Continuous and Schedule Based Rule: Record continuously or when schedule is active

- Enter the Rule **Name**
- Select the **Schedule**
- Select the **Source** (Limited to multisensor and panoramic devices)
- Do not select a **Trigger**
- Select the **Action**:
 - Record Audio (if applicable)
 - Record to the Cloud
 - Record to the Edge
- Select **Recording settings**:
 - Frame rate → Value is FPS
 - Resolution
- Select **Save**

Organization Functions

- [Manage Organizations](#)
- [Add Organizations](#)
- [Manage My Org \(MFA, SSO, Webhooks & Org Email\)](#)
- [Manage My Account \(Account Info & Notification Settings\)](#)

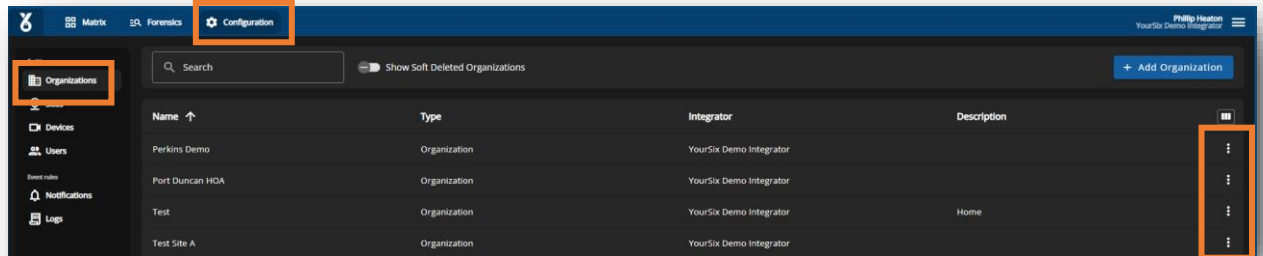
Manage Organizations



Audience: Integrator Super Admin, Integrator Admin, Integrator Tech



Objective: Edit an organization.



- Select **Configuration** located on the navigation bar
- Select **Organization** located on the page menu
- Select the **Pen Icon** to edit the name of the organization, organization webhooks, and organization emails

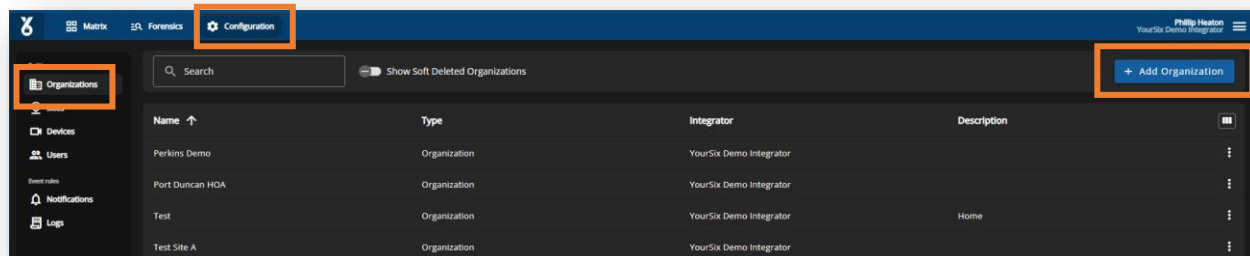
Add an Organization



Audience: Integrator Super Admin, Integrator Admin, Integrator Tech



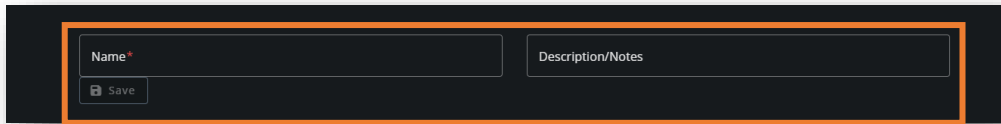
Objective: Create a new organization.



Organizations are the top tier used for grouping sites and devices. All devices will be assigned to a site and all sites to an organization.

- Select [Configuration](#) located on the navigation bar
- Select [Organization](#) located on the page menu
- Select [Add Organization](#) located in the upper right portion of the screen
- Continue to next page →→→

Add an Organization

A screenshot of a dark-themed user interface for adding an organization. It features two input fields: 'Name*' on the left and 'Description/Notes' on the right. Below the 'Name*' field is a 'Save' button with a floppy disk icon. The entire form area is highlighted with a thick orange border.

- Name the **Organization**
- Add **Description**
- Select **Save**

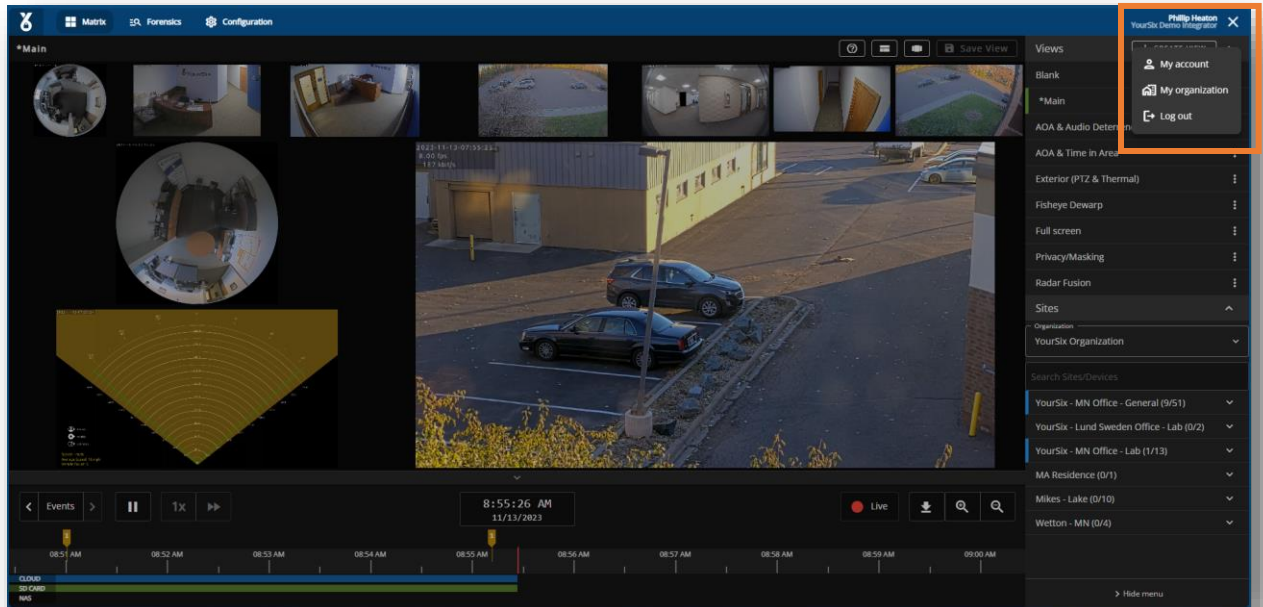
Manage My Org (MFA, SSO, Webhooks & Org Email)



Audience: Integrator Super Admin

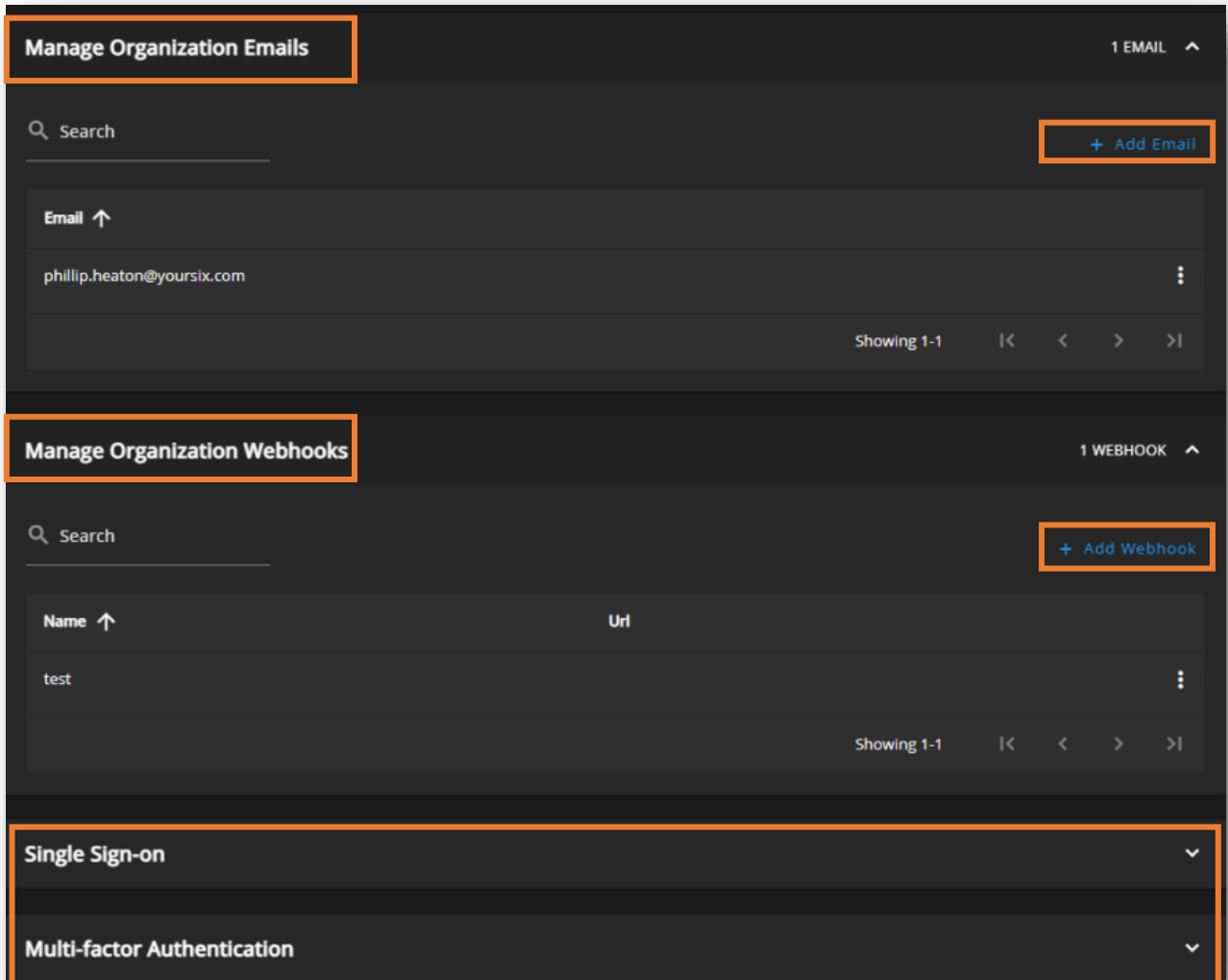


Objective: Manage Multi-Factor Authentication (MFA), Single Sign-On (SSO), webhooks & emails for an organization.



- Locate the [Hamburger Menu](#) in the upper right corner
- Select [My Organization](#)
- Continue to next page →→→

Manage My Org (MFA, SSO, Webhooks & Org Email)



Manage Organization Emails

→ Select [Add Email](#) to add a user email to the organization email list

Manage Organization Webhooks

→ Select [Add Webhook](#) to add a webhook to the organization

Multi-Factor Authentication (MFA)

→ Select the desired [Multi-Factor Authentication](#) setting

Single Sign On (SSO)

→ *Please contact YourSix to enable SSO for your organization*

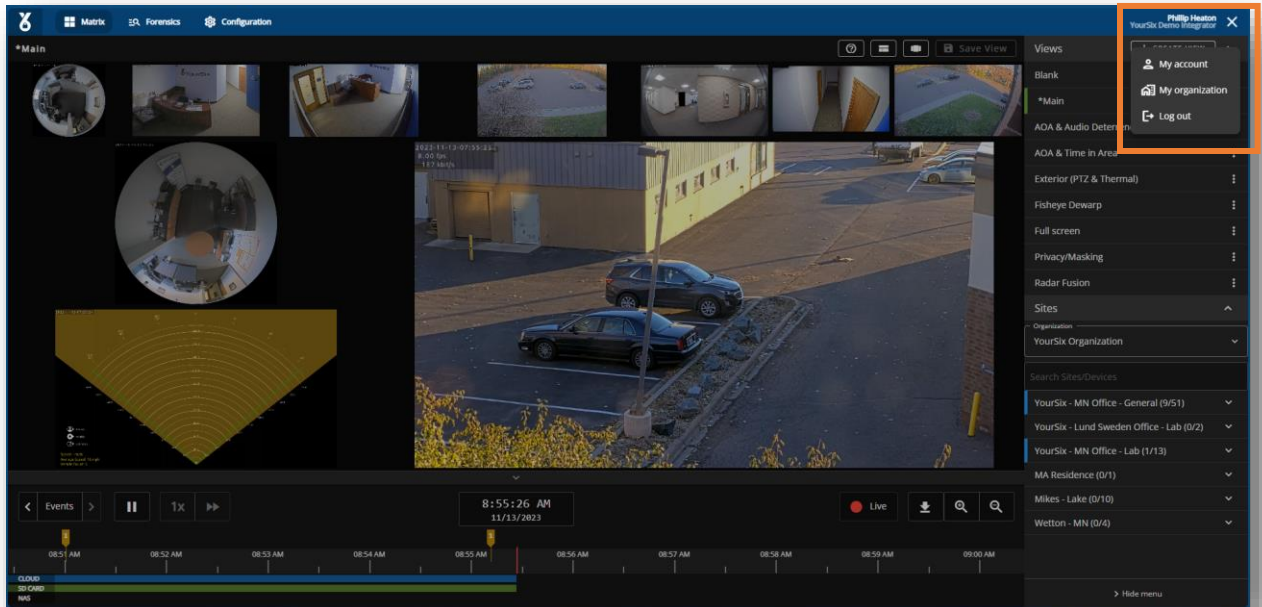
Notification Settings



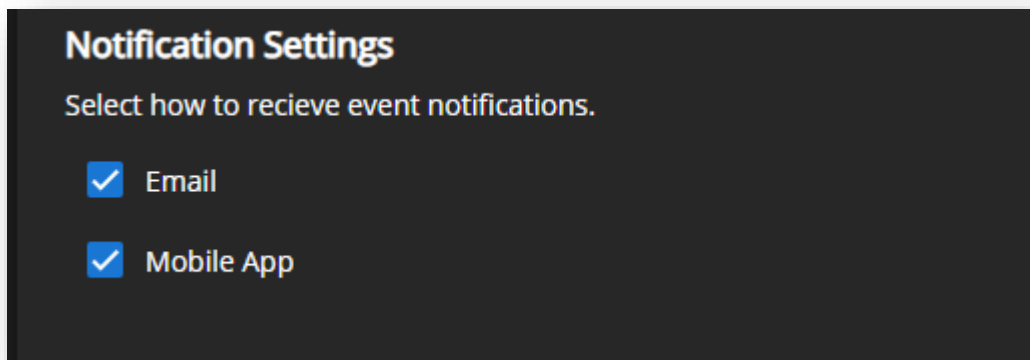
Audience: All users



Objective: Manage Notification Settings.



- Locate the [Hamburger Menu](#) in the upper right corner
- Select [My Account](#)
- Select how you wish to receive notifications



Site Functions

- [Manage Sites](#)
- [Create Device Group](#)
- [Add Devices to Device Group](#)
- [Central Station](#)
- [Create Schedules](#)
- [Add Sites](#)

Manage Sites

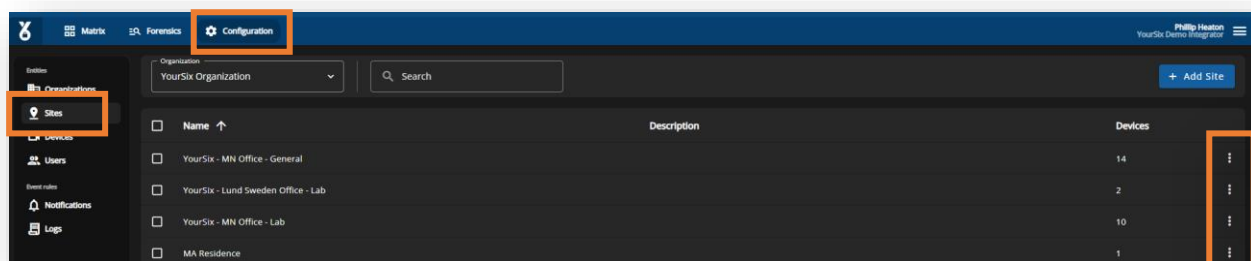


Audience: Integrator Super Admin, Integrator Admin, Integrator Tech



Objective: Edit below settings for a site.

- Name
- Time Zone
- Add User
- Device Groups & Central Station access
- User Permissions for site
- Create Schedules



- Select **Configuration** located on the navigation bar
- Select **Sites** located on the page menu
- Use the **Organization** and **Search** function to locate the site you wish to edit
- Select the **Pen** icon to edit the site
- Continue to next page →→→

Manage Sites

Site Information

Name*
St. Paul Office

Description

Timezone*
America/Chicago

Save

Update Name, Description or Time Zone:

- Edit [Name](#) or [Description](#)
- Select appropriate [Time Zone](#)
- Continue to next page →→→

Users with site permission: [+ Add users](#)

Columns: [Search](#)

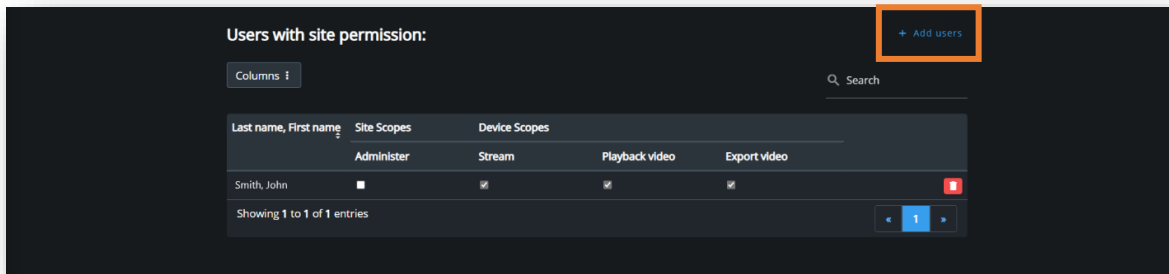
Last name, First name	Site Scopes	Device Scopes	
Smith, John	<input type="checkbox"/>	<input checked="" type="checkbox"/> Stream <input checked="" type="checkbox"/> Playback video <input checked="" type="checkbox"/> Export video	<input type="checkbox"/> <input type="checkbox"/>

Showing 1 to 1 of 1 entries

Edit Site User Permissions:

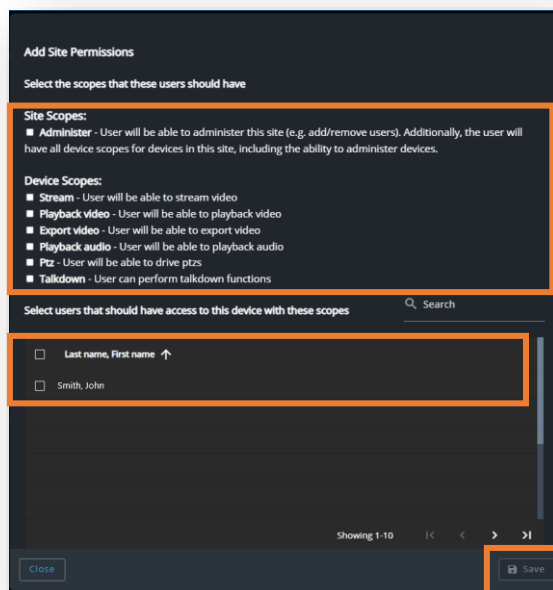
- Locate the [User With Site Permissions](#) and expand
- Select appropriate user [Permissions](#)
- Select [Save](#)
- Users can be deleted by selecting the [Trash Can Icon](#)
- Continue to next page →→→

Manage Sites



Add a User to a Site:

→ Select [Add User Permissions](#)



→ Select the [Scope](#) of the user's permissions

→ Select which [User](#) to assign permission

- Only users that have been created within the organization will show as an option to add. Refer to the ["Add User"](#) section of this guide to add a new user to the organization.

→ Select [Save](#)

Create/Manage Device Group



Audience: Integrator Super Admin, Integrator Admin, Integrator Tech

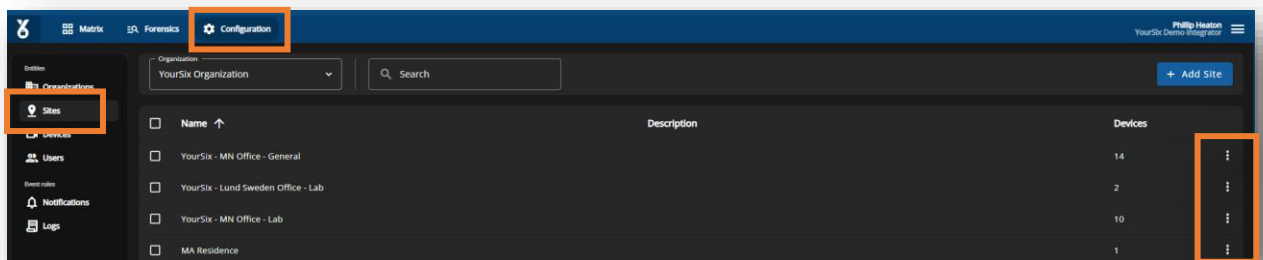


Objective: Create and manage device groups which may be used for notifications.



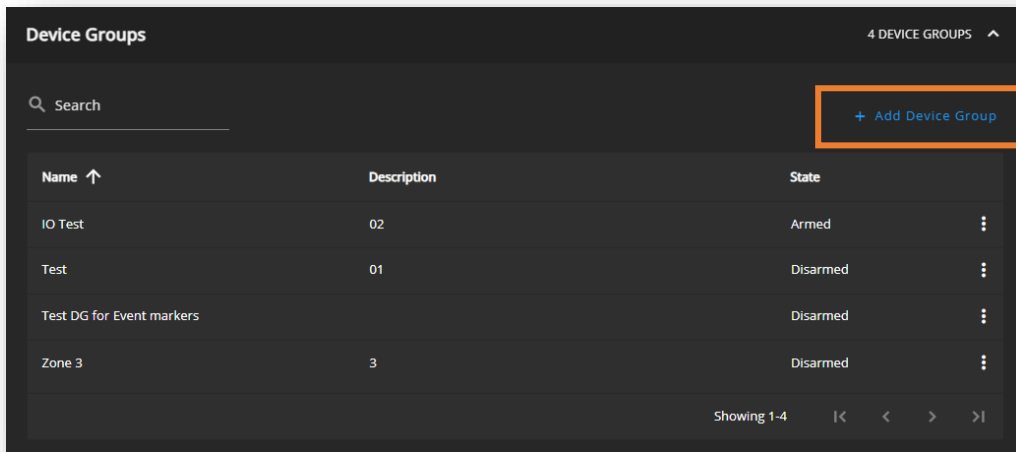
Additional Resources:

- [Device group videos](#)



- Select **Configuration** located on the navigation bar
- Select **Sites** located on the page menu
- Use the **Organization** and **Search** function to locate the site you wish to edit
- Select the **Pen** icon to edit the site
- Continue to next page →→→

Create Device Group



Create Device Groups:

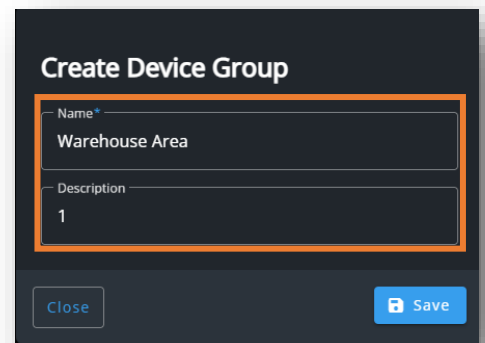
- On the edit site page select locate and expand the Device Group section [Add Device Group](#)

Note: Device Groups are the same as Alarm Zones in the Guardian Platform

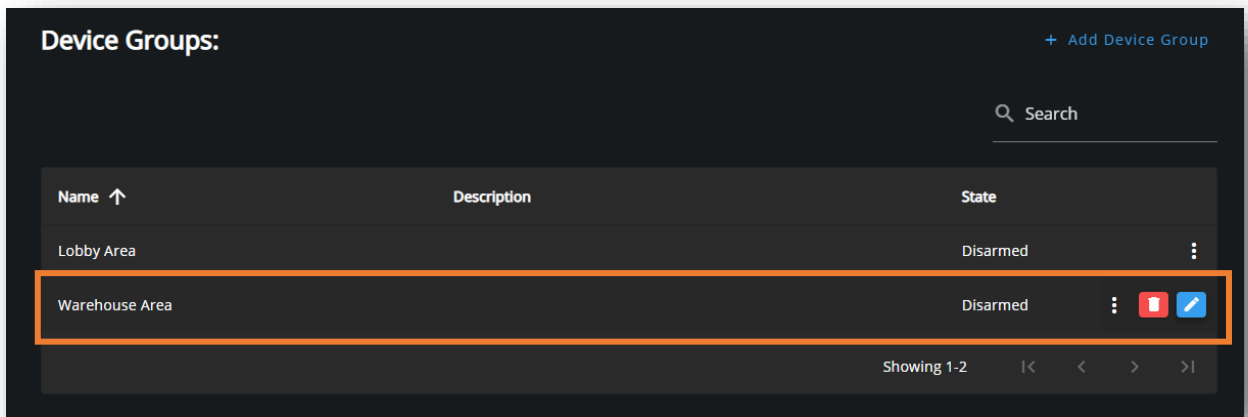
- Within the popup menu, name the device Group and enter the description (zone number)
- Enter **Name**: Vanity name you wish to call the group
 - Enter **Description**: Zone number (matches the ID of the Zone Number)

- Select [Save](#)

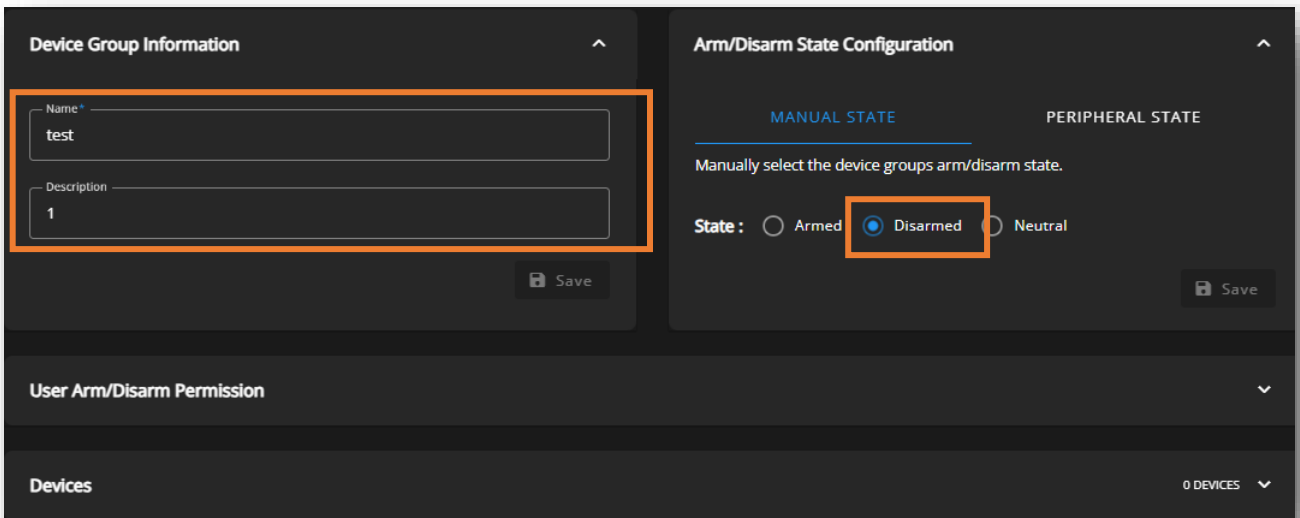
- Continue to the next page → → →



Manage Device Group



- Once you select save in the popup menu, the new device group will appear in the list of device groups.
- Select the recently created [Device Group](#)



- Within the edit device group page, confirm [Name](#) & [Description](#) (Zone Number)
- Set the state to [Disarmed](#)

Note: Device groups are always built in a DISARMED state. This is very important in order to avoid a flood of alarms during the configuration process.

- Select [Save](#).

Add Devices to Device Group

Device Group Information ^

Name*
test

Description
1

Save

Arm/Disarm State Configuration ^

MANUAL STATE PERIPHERAL STATE

Manually select the device groups arm/disarm state.

State: Armed Disarmed Neutral

Save

User Arm/Disarm Permission v

Devices 0 DEVICES ^

No devices are connected to the device group.

+ Add devices

- Select [Add Devices](#) located on the [Device Group](#) page
- Within the popup select the devices to add to the group

Central Station



Audience: Integrator Super Admin, Integrator Admin, Integrator Tech



Objective: Create device groups which may be used for notifications.



Please reference our Central Station guide for complete guidance on setting up a central station.

Central station access:

Authorize a central station to access this site and all of its devices.

None Superman Alarms

Account Number*

123456

Save

Central Station Access:

- Navigate to [Edit Site](#)
- Locate [Central Station Access](#) (directly below the [Device Groups](#) section)
- Select the [Central Station](#) to authorize access to this site and device(s)

Note: Only central stations that have been enabled for your account will appear. If the required central station is not an option, please contact YourSix.

- Enter the [Account Number](#) that the central station has assigned to this site. This number is provided to you by the central station; this number is **NOT** assigned by YourSix
- Select [Save](#)

Create Schedules

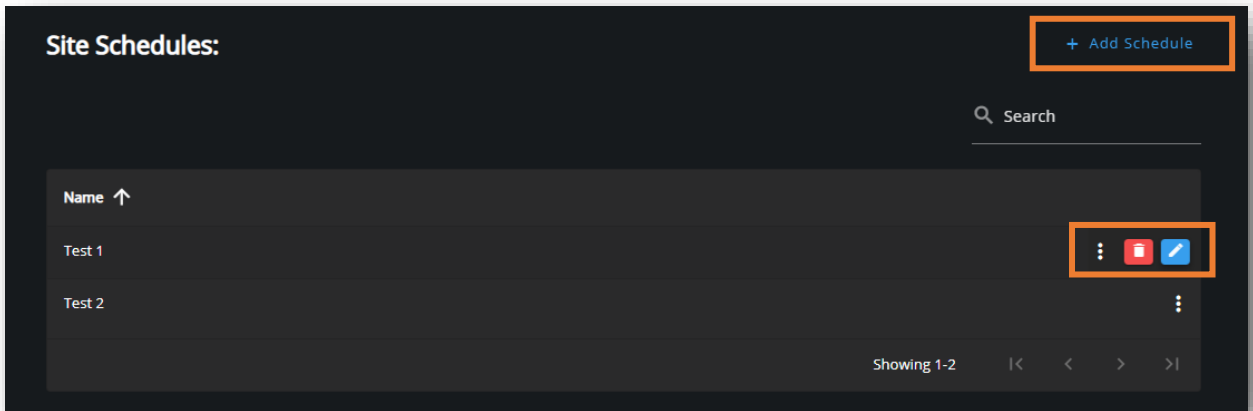


Audience: Integrator Super Admin, Integrator Admin, Integrator Tech



Objective: Edit & create schedules.

Note: Created schedules will be selectable when creating rules for devices.

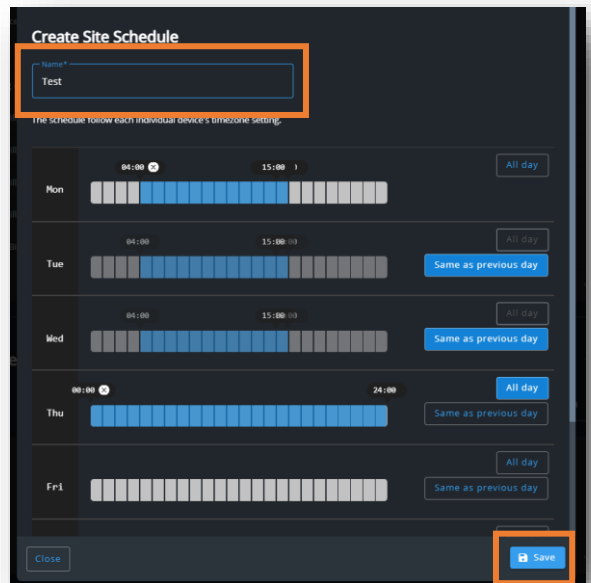


Edit Schedule:

- Navigate to [Edit Site](#)
- Select the **Pen Icon** to edit the existing schedules

Add Schedule:

- Select **Add schedule**
- Enter a **Name** for the schedule
- Using the slide bars or options on the right to create the schedules for each day
- Select **Save**



Add Sites



Audience: Integrator Super Admin, Integrator Admin, Integrator Tech

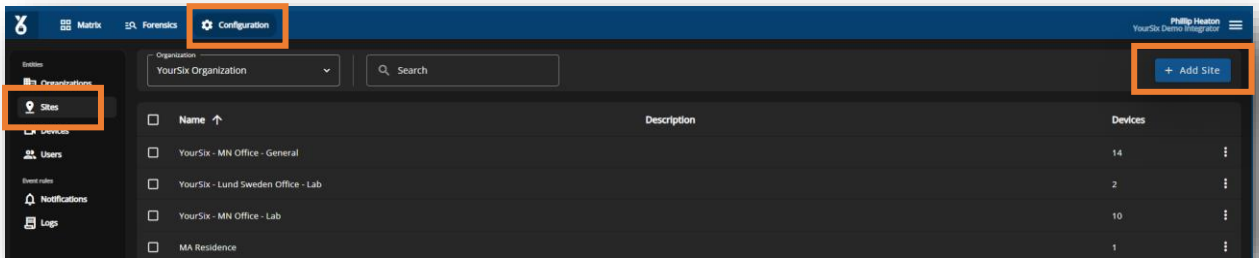


Objective: Create a new site under an organization.



Additional Resources:

- [Add site video](#)



Sites are the second tier used for grouping devices. All devices will be assigned to a site and all sites to an organization. An organization must be created before a site can be created.

- Select **Configuration** located on the navigation bar
- Select **Sites** located on the page menu
- Select **Add Site** located in the upper right portion of the screen
- Continue to next page →→→

Add Sites

Site Information

Name *

Description

Timezone *

Organization *

YourSix Training Company

Save

- Enter the Site **Name**
- Enter a **Description**
- Select the desired **Time Zone**
- Select the **Organization** that the site should be assigned to
- Select **Save**

Devices

- [Manage Devices](#)
- [Create a Rule](#)
- [Add Devices](#)

Manage Devices

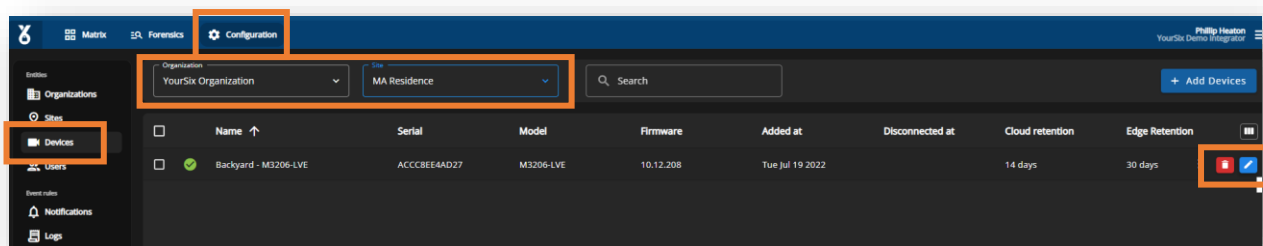


Audience: Integrator Super Admin, Integrator Admin, Integrator Tech



Objective: Manage & delete devices from an organization or site.

- Check model, firmware, serial number
- Edit the organization, site, time zone, cloud & edge retention settings
- Access or reboot the device
- Create & configure device rules
- Create & configure barriers
- Create & configure user device permissions
- Manage applications on device
- Manage audio configuration
- Assign device to a device group
- Edit Event Retention
- Manage Applications



- Select [Configuration](#) located on the navigation bar
- Select [Devices](#) located on the page menu
- Select [Pen](#) icon to edit the device
- Continue to next page →→→

Manage Devices

The screenshot shows a 'Device Information' form with a dark theme. At the top, there is a header bar with an information icon and the title 'Device Information'. Below the header, a summary bar displays key device details: Model: P3225-LV Mk II, Firmware: 9.80.3.10, Serial: ACCC8EE0B9E5, and Added at: Mon Nov 29 2021. The main form area contains several input fields and dropdown menus, all highlighted with an orange border. These include: Organization (YourSix Organization), Site (St. Paul Office), Device Name (Booth Demo 01), Device Description/Notes, Cloud Retention (30 Days), Edge Retention (30 Days), Events Retention, Timezone (Site timezone (default)), and Device Group. A blue 'Save' button is located at the bottom right of the form.

→ View [Device Model, Firmware, Serial Number & Date Added](#) at the top of the page

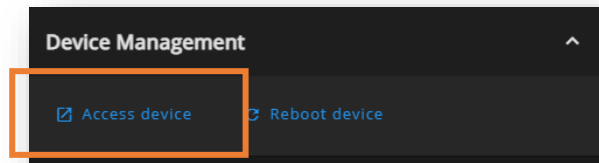
→ Edit the following information about the device:

- Organization
- Site
- Device Name
- Device Description
- Cloud Retention
- Edge Retention
- Time Zone
- Device Group
- Events Retention ([guide](#))

→ Select [Save](#)

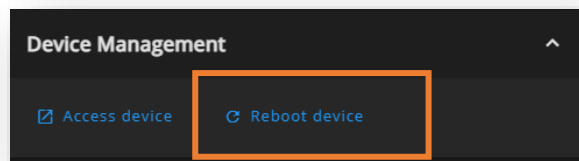
→ Continue to next page →→→

Manage Devices



Access the Device Interface:

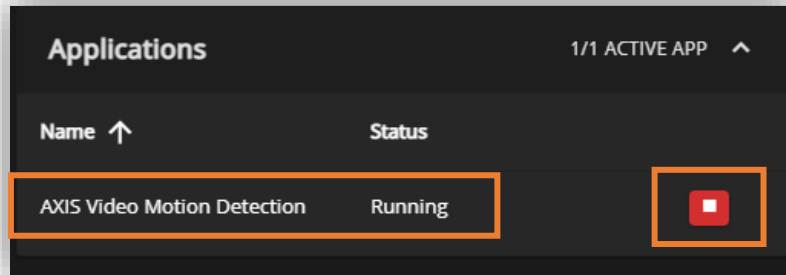
- Locate the Device Management section on the Manage Device page
- Select [Access Device](#) to view the device live feed and access the direct device interface:
 - Image settings
 - Stream settings
 - Overlay settings
 - Audio settings
 - PTZ settings
 - Privacy Mask settings
 - Application settings
 - System settings



Reboot the Device:

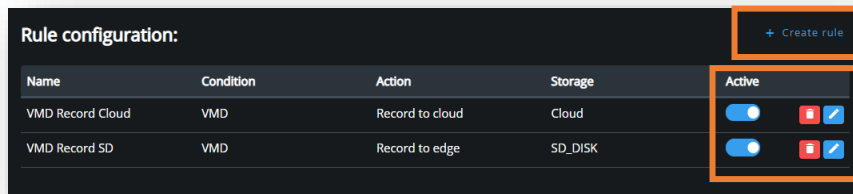
- Select [Reboot Device](#) to restart the device
- Continue to next page →→→

Manage Devices



Applications:

- View current **Status** of Applications
- **Start** or **Stop** the Application



Edit & Create Action Rules:

- View existing rules:
 - Toggle **Active/Inactive**
 - Select the **Trash Can Icon** to delete the rule
 - Select the **Pen Icon** to edit the rule
- Select **Create Rule** to create a new rule for this device

Create a Rule



Audience: Integrator Super Admin, Integrator Admin, Integrator Tech



Objective: Create a new action rule for a device.



Additional Resources:

- [Recording rules and storage videos](#)

Motion Based Rule

Record when motion is detected

- Enter the Rule **Name**
- Select the **Schedule**
- Select the **Source** (Limited to Multi-Sensor and Panoramic Devices)
- Select the **Trigger**
 - VMD: Motion detection recording → Select profile: Profile 1
- Select the **Action** (when motion is detected):
 - Record Audio (if applicable)
 - Record to the Cloud
 - Record to the Edge
- Select **Recording Settings**:
 - Prebuffer (Recording before the trigger) → Value is seconds
 - Post buffer (Recording after the trigger) → Value is seconds
 - Frame Rate → Value is FPS
 - Resolution
- Select **Save**

Create a Rule

Continuous and Schedule Based Rule

Record continuously or when schedule is active

- Enter the Rule **Name**
- Select the **Schedule**
- Select the **Source** (Limited to Multi-Sensor and Panoramic Devices)
- Do not select a **Trigger**
- Select the **Action**:
 - Record Audio (if applicable)
 - Record to the Cloud
 - Record to the Edge
- Select **Recording Settings**:
 - Frame Rate → Value is FPS
 - Resolution
- Select **Save**

The screenshot shows the 'Create rule' configuration window with the following settings:

- Name:** Training Rule
- Sources:** Overview, Panorama, Double Panorama, Quad View, View Area 1, View Area 2, View Area 3, View Area 4, Corner Left, Corner Right, Double Corner, Corridor
- Trigger:** Schedule, VMD. Select schedule: Always, Test 1, Test 2. + Add Site Schedule
- Action:** Record to cloud, Record to Edge SD. Frame rate: 8. Resolution: 720x720

Buttons: Close, Save

Additional Device Management



Audience: Integrator Super Admin, Integrator Admin, Integrator Tech



Objective: Edit new & existing devices.

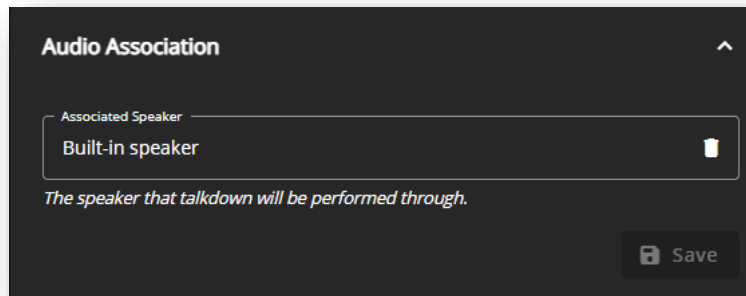
Last name, First name	Administer	Stream	Playback video	Export video
Smith, John	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Williams, James	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Smith, Nancy	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Showing 1 to 3 of 3 entries

Device Permissions:

- View Existing Device Permissions
 - Edit the [Check Boxes](#) to edit [User Permissions](#)
 - Select the [Trash Can Icon](#) to delete [User Permissions](#) from the device
- Select [Add User](#) to create a new user for this device
 - Follow the screen prompts

Additional Device Management

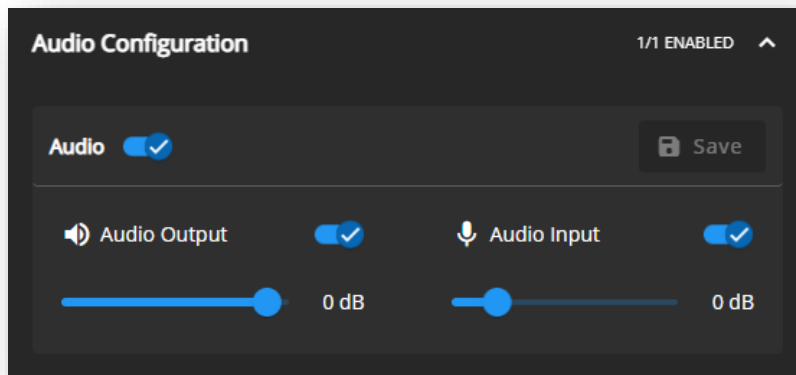


Audio Association:

- Select [Associated Speaker](#)

Note: Only speakers that have been added to the same site as the device being edited will appear in the drop down.

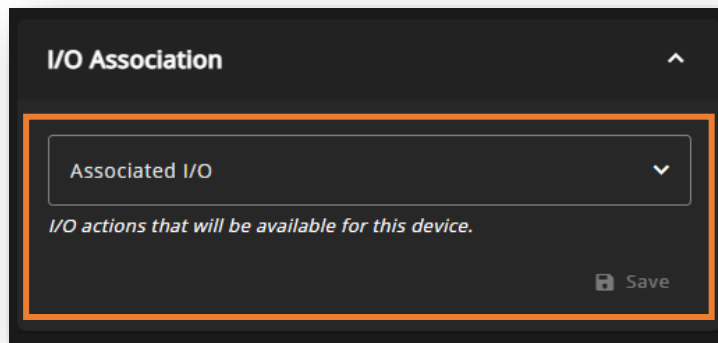
- Select [Save](#)



Edit Audio Configuration:

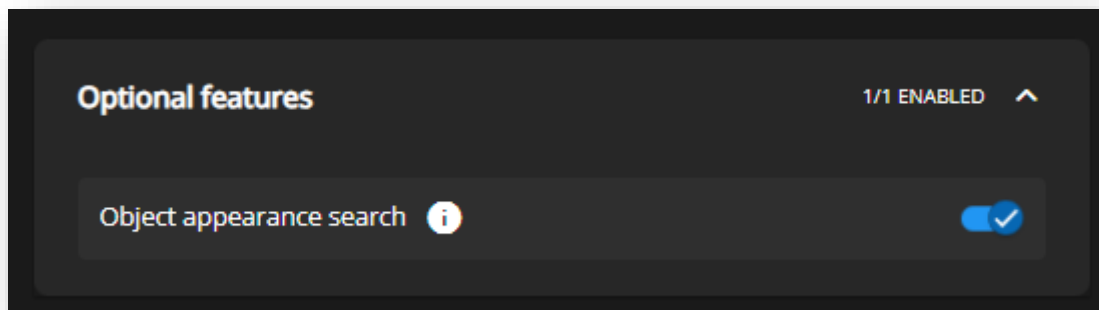
- Toggle [Audio](#) to turn audio on or off
 - Toggle [Audio Output](#) to turn the speaker on or off
 - Toggle [Audio Input](#) to turn the microphone on or off
- Select [Save](#)

Additional Device Management



I/O Association:

- Select [Associated I/O](#) and select the desired information
- Select [Save](#)



Option Features

- Select and enable the desired [Optional feature](#)

Add Devices



Audience: Integrator Super Admin, Integrator Admin, Integrator Tech

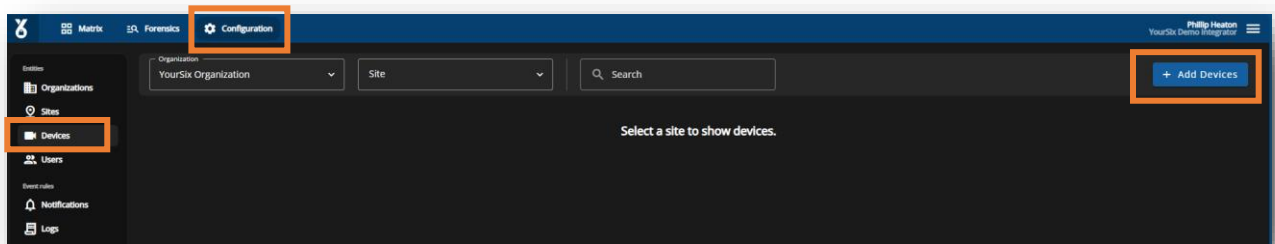


Objective: Add a device to a site.



Additional Resources:

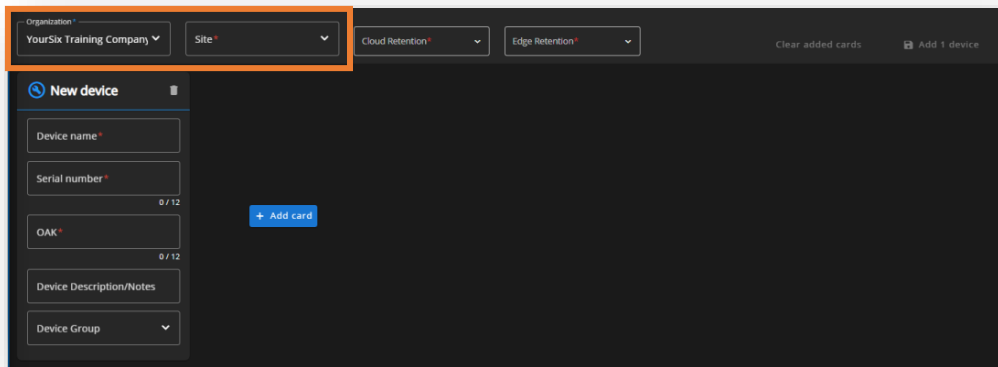
- [Enrolling a device resources](#)
- [Adding a device videos](#)



A site and organization must be created before adding a device.

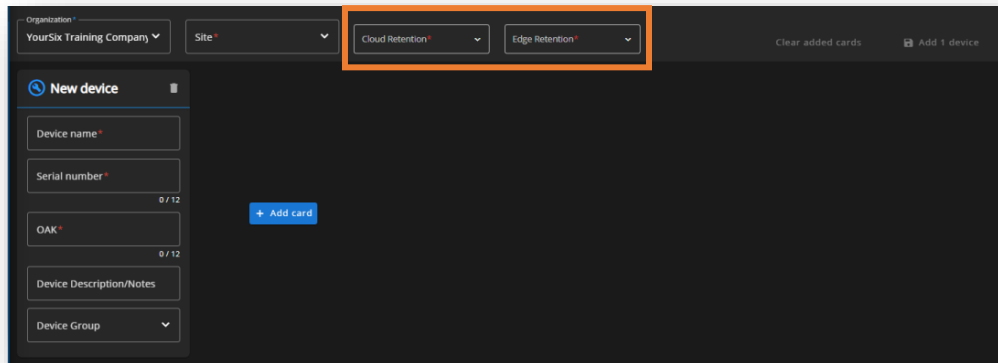
- Select [Configuration](#) located on the navigation bar
- Select [Devices](#) located on the page menu
- Select [Add Devices](#) located in the upper right portion of the screen
- Continue to next page →→→

Add Devices



The screenshot shows the 'New device' form in a dark theme. At the top, there are four dropdown menus: 'Organization' (set to 'YourSix Training Company'), 'Site', 'Cloud Retention', and 'Edge Retention'. The 'Organization' and 'Site' dropdowns are highlighted with an orange border. Below these are input fields for 'Device name', 'Serial number', 'OAK', 'Device Description/Notes', and a 'Device Group' dropdown. A blue '+ Add card' button is positioned to the right of the 'OAK' field. In the top right corner, there are links for 'Clear added cards' and 'Add 1 device'.

→ Select the **Organization** and **Site** that the device(s) will be added to



The screenshot shows the same 'New device' form. In this view, the 'Cloud Retention' and 'Edge Retention' dropdowns are highlighted with an orange border. The 'Organization' and 'Site' dropdowns are no longer highlighted. All other elements, including the input fields and the '+ Add card' button, remain the same as in the previous screenshot.

→ Select the **Cloud Retention** and **Edge Retention** for the device(s)

→ Continue to next page →→→

Add Devices

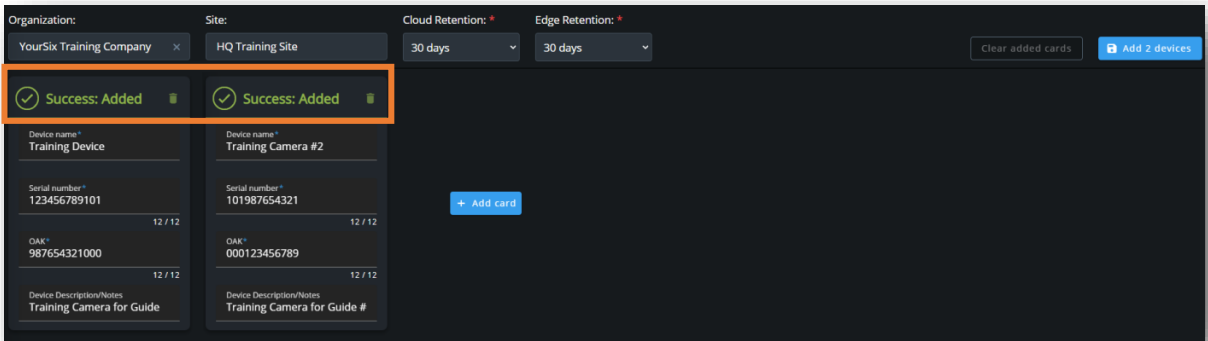
The screenshot shows the 'New device' form in the Y6OS interface. The form is highlighted with an orange border. It includes fields for Device name, Serial number, OAK, Device Description/Notes, and Device Group. A '+ Add card' button is also highlighted with an orange border.

- Fill in the *Required Fields:
- Enter **Device Name**
 - Enter **Serial Number**
 - Enter **OAK**
 - *With each Axis device, you will receive a printed piece of paper with an Owner Authentication Key (OAK). You need the OAK to verify ownership when you register the device with an O3C-based service.*
 - Enter **Device Description/Notes**
 - Select **Device Group**
- If you are adding multiple devices to the same site with the same cloud and edge retention, you can select the **+Add card** button. This will allow you to mass upload devices.

The screenshot shows the 'New device' form in the Y6OS interface. The '+ Add device' button is highlighted with an orange border.

- Select **Add "#" devices** button
- Continue to next page →→→

Add Devices



→ Confirmation of device addition: **Green Check Mark and Success: Added**

→ Physical Connection:

- Plug the device into a secure power & internet source
 - *If the device is not new, please factory reset the device by holding down the control button while plugging the device into its power source. Continue to hold the Control Button for 15 seconds until the status LED flashes amber and then release the button. The process is complete once the status LED turns green for a moment.*
- On the physical device, press and hold the control button for 3 seconds until the light flashes and then release the button. This will connect the device to the platform.

Troubleshooting:

- [Adding a device troubleshooting](#)

Access Control

- [Overview](#)
- [Add Controller](#)
- [Barriers](#)
- [Barrier Groups](#)
- [Identities](#)
- [Identity Groups](#)
- [Access Schedules](#)
- [Access Rules](#)

Access Control Overview

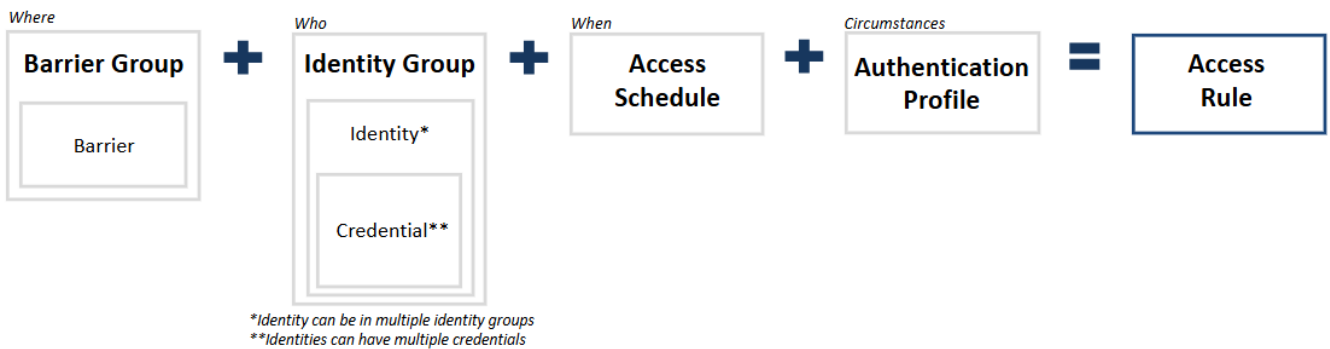
The addition of Access Control to the YourSixOS platform marks a significant advancement in cloud-native physical security solutions. This enhancement integrates Access Control into the YourSixOS cloud-native platform, offering customers a unified solution accessible from any device, anywhere. By bringing Access Control into the cloud,

Additional Resources:

- [All Access Control Resources](#)
- [Training Videos](#)
- [User Permissions and Guides](#)

The Goal of YourSix Access Control

Who is permitted to enter, where, when, and under what circumstances. In order to do this, you create **Access Rules**.



Basic Steps for Access Control Setup

1. Add Device
2. Add Barriers + Configure Barriers
3. Add Barrier Groups
4. Add Identities + Add credentials
5. Add Identity Groups
6. Add Access Schedules
7. Add Access Rules

For hardware instructions, please consult the vendor's hardware manuals and guides. Additionally, it is the installation partner's responsibility to comply with all life safety codes.

Add Controller



Audience: Integrator Super Admin, Integrator Admin, Integrator Tech

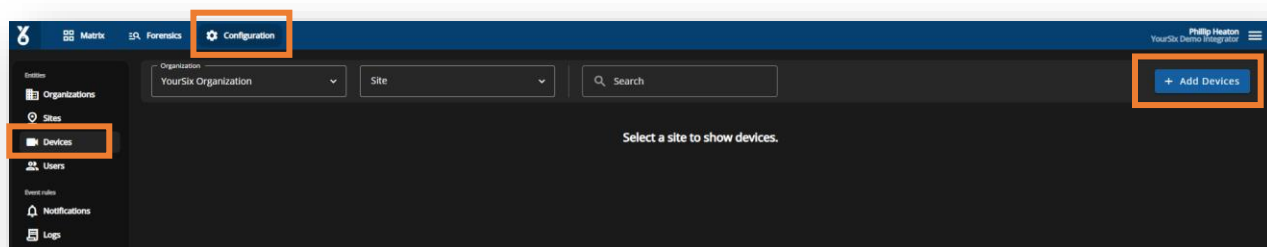


Objective: Add a controller to a site.



Additional Resources:

- [Adding a device videos](#)



A site and organization must be created before adding a device.

- Select **Configuration** located on the navigation bar
- Select **Devices** located on the page menu
- Select **Add devices** located in the upper right portion of the screen
- Continue to next page →→→

Add Controller

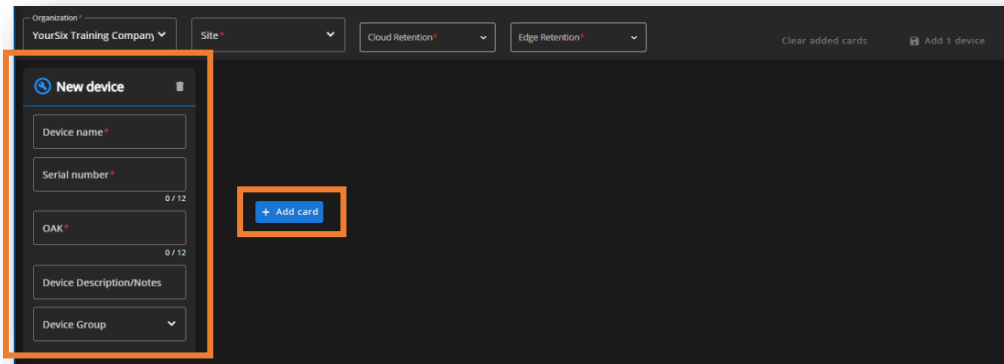
The screenshot shows a 'New device' form with the following fields and options:

- Organization: YourSix Training Company (highlighted)
- Site: (empty, highlighted)
- Cloud Retention: (dropdown)
- Edge Retention: (dropdown)
- Clear added cards
- Add 1 device
- Device name: (text input)
- Serial number: (text input, 0 / 12)
- OAK: (text input, 0 / 12)
- Device Description/Notes: (text input)
- Device Group: (dropdown)
- + Add card (button)

→ Select the **Organization** and **Site** that the device(s) will be added to

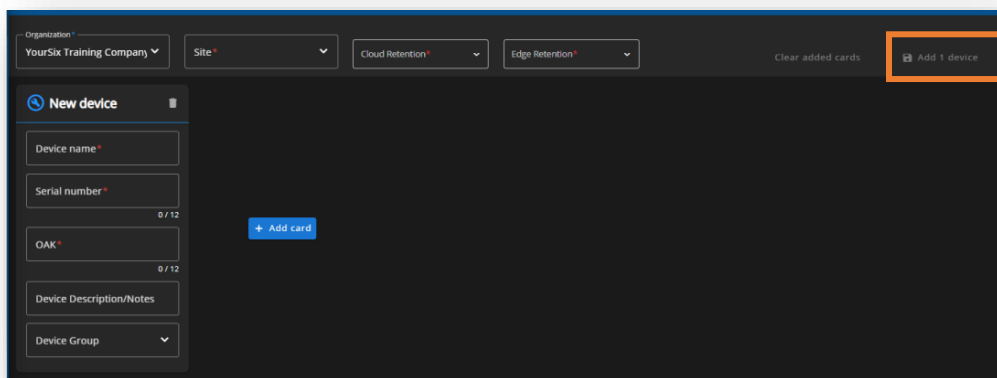
→ Continue to next page →→→

Add Controller



The screenshot shows the 'New device' form in the Y6OS interface. The form is highlighted with an orange border. It includes fields for Device name, Serial number, OAK, Device Description/Notes, and Device Group. A '+ Add card' button is also highlighted with an orange border.

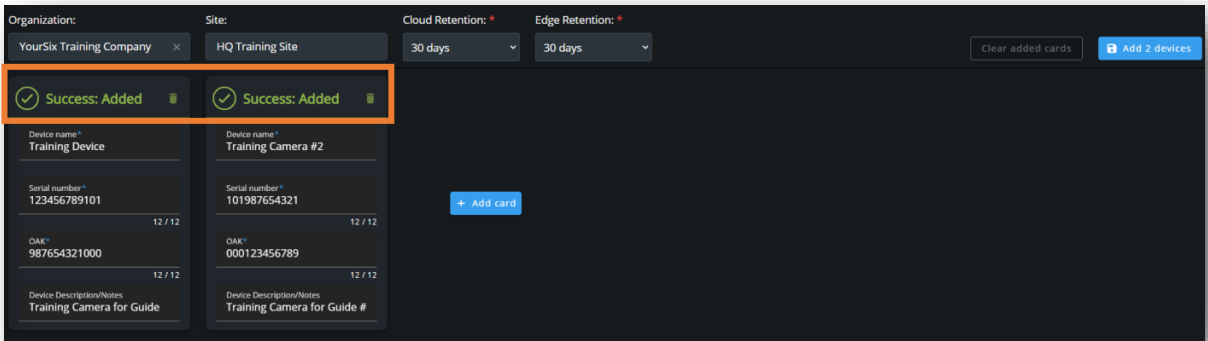
- Fill in the *Required Fields:
- Enter **Device Name**
 - Enter **Serial Number**
 - Enter **OAK**
 - *With each Axis device, you will receive a printed piece of paper with an Owner Authentication Key (OAK). You need the OAK to verify ownership when you register the device with an O3C-based service.*
 - Enter **Device Description/Notes**
 - Select **Device Group**
- If you are adding multiple devices to the same site with the same cloud and edge retention, you can select the **+Add card** button. This will allow you to mass upload devices.



The screenshot shows the 'New device' form in the Y6OS interface. The '+ Add device' button is highlighted with an orange border.

- Select **Add "#" devices** button
- Continue to next page →→→

Add Controller



→ Confirmation of device addition: **Green check mark and “Success: Added”**

→ Physical Connection:

- Plug the device into a secure power & internet source
 - *If the device is not new, please factory reset the device by holding down the control button while plugging the device into its power source. Continue to hold the Control Button for 15 seconds until the status LED flashes amber and then release the button. The process is complete once the status LED turns green for a moment.*
- On the physical device, press and hold the control button for 3 seconds until the light flashes and then release the button. This will connect the device to the platform.

Troubleshooting:

- [Adding a device troubleshooting](#)

Add Barrier



Audience: Integrator Super Admin, Integrator Admin

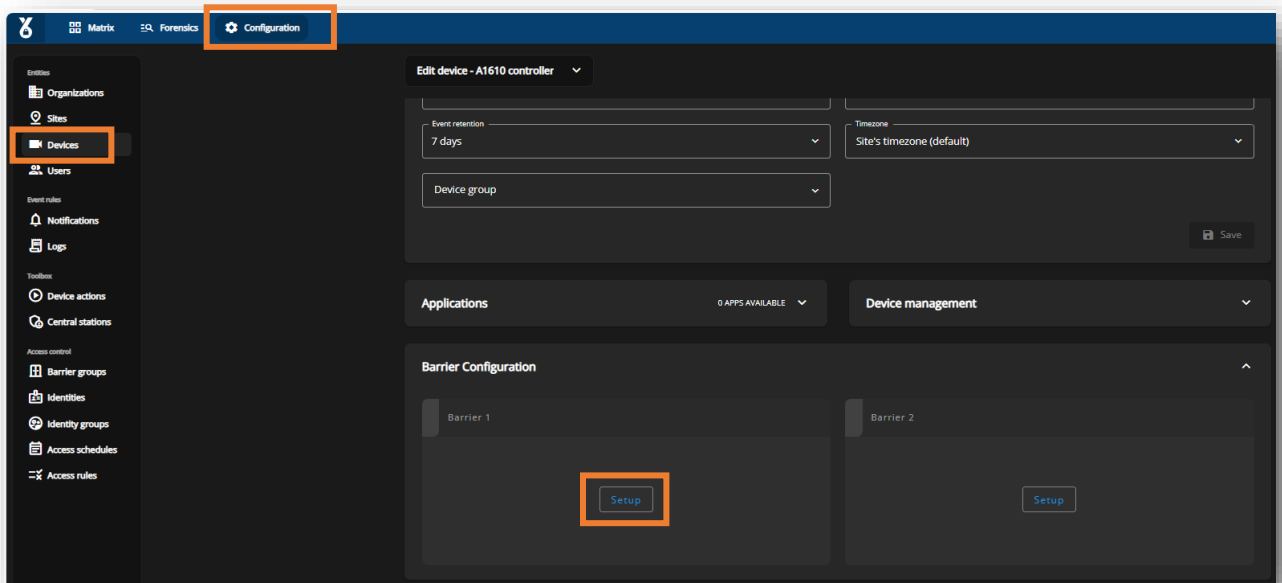


Objective: Add a barrier to a controller.



Additional Resources:

- [Access control configuration videos](#)



- Select [Configuration](#) located on the navigation bar
- Select [Devices](#) located on the page menu
- Using the Organization and Site filters along the top, locate and select the controller which the barrier will be added to
- Once on the edit device page, locate the barrier configuration section and select [Setup](#)
- Continue to next page →→→

Add Barrier

Barrier configuration - Barrier 1 X

General

Name*

Access time (seconds) * 7

Extended access time (seconds) * 30

PIN length * 4

Advanced settings

Relay state when locked * Open

Complete the General (step 1) portion of the barrier configuration

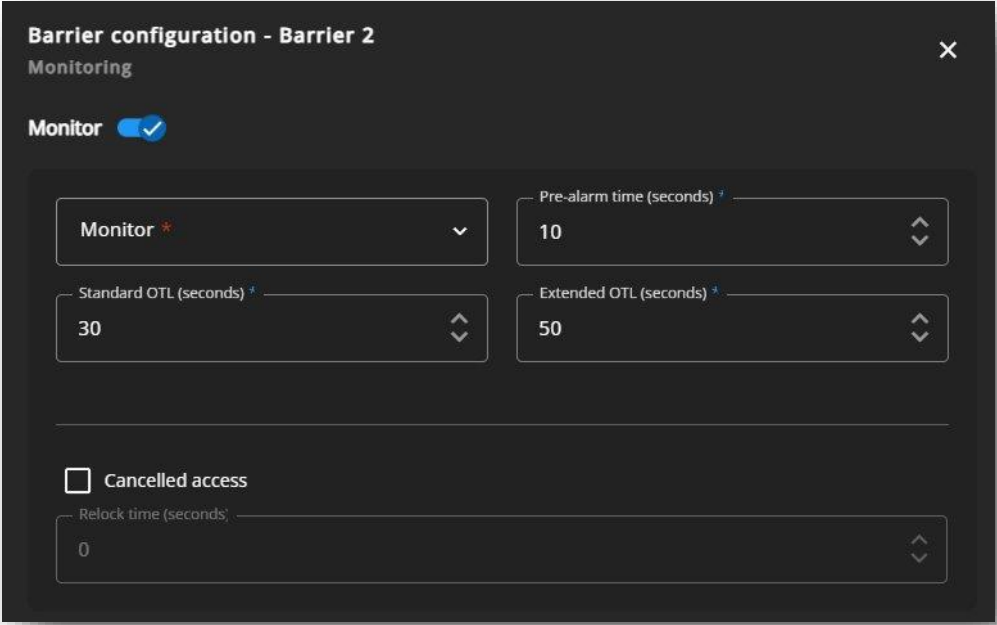
- **Access Time:** the number of seconds that a barrier shall be unlocked upon access
- **Extended Access Time:** the number of seconds that a barrier shall be unlocked upon access for those with extended access enabled
- **Pin Length:** Required length of the pin

Advanced Settings

- **Relay State when locked:** Open (prepopulated value) or Closed

- Select **Next** at the bottom of the window

Add Barrier



Barrier configuration - Barrier 2 ✕

Monitoring

Monitor

Monitor * ▼

Pre-alarm time (seconds) * 10 ⬆️⬇️⬆️

Standard OTL (seconds) * 30 ⬆️⬇️⬆️

Extended OTL (seconds) * 50 ⬆️⬇️⬆️

Canceled access

Relock time (seconds) 0 ⬆️⬇️⬆️

Complete the Monitoring (step 2) portion of the barrier configuration

Monitoring a barrier requires a door contact to be present in the deployment

- **Monitor:** Trigger event based on barrier state
 - Closing Circuit (N/O): "Normally Open" and thus would "alarm" when the circuit is closed
 - Opening Circuit (N/C): "Normally Closed" and thus would "alarm" when the circuit is opened
- **Pre-alarm Time:** the number of seconds between barrier opening and the pre-alarm event
- **Standard OTL:** the number of seconds between barrier opening and the barrier open too long event
- **Extended OTL:** the number of seconds between barrier opening and the barrier open too long event when using extended access

Cancelled Access

- Purpose is to allow for barrier constructions that rely on the lock for closing (e.g. magnetic locks)
 - Relock Time: the number of seconds that the barrier shall be unlocked after it has been opened
- Select **Next** at the bottom of the window

Add Barrier

The screenshot shows the 'Barrier configuration - Barrier 2' window with the 'Access points' section expanded. It lists four access points: Reader 1, Reader 2, REX 1, and REX 2. Reader 1 and REX 1 are currently disabled (greyed out), while Reader 2 and REX 2 are enabled (blue with a checkmark). Reader 2 has a 'Name' field and radio buttons for 'Type' (OSDP, Wiegand) and 'Direction' (In, Out). REX 2 has a 'Name' field, radio buttons for 'Type' (Active low (N/O), Active high (N/C)), and a 'Does not unlock' toggle switch.

Complete the Access Points (step 3) portion of the barrier configuration

Reader

→ **Type:** Weigand or OSDP

→ **Direction:**

- In (Read In): reader used to enter
- Out (Read Out): reader used to exit

REX

→ **Type:** Active high or active low

→ **Does not unlock:** When enabled, the barrier can be accessed as usual, but the person exiting must manually disengage the lock

→ Select **Next** at the bottom of the window and review the overview page. If accurate select **save**. This completes the barrier configuration portion of the setup

Add Barrier Groups



Audience: Integrator Super Admin, Integrator Admin

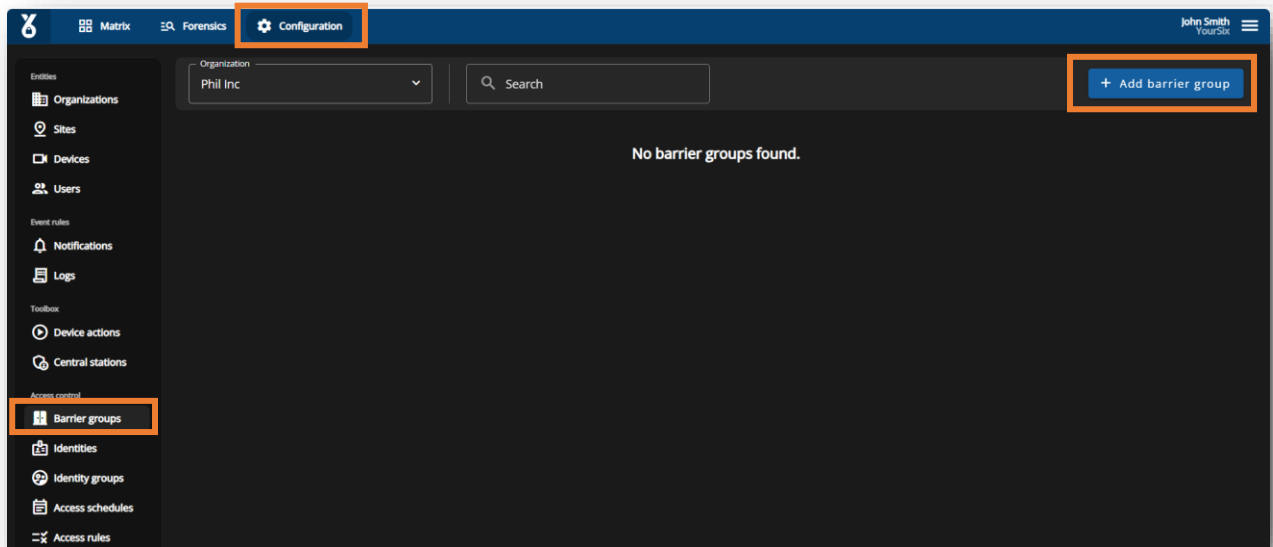


Objective: Add barriers to barrier groups. Barrier groups allow for the simultaneous configuration of the barriers when using access rules.



Additional Resources:

- [Access control configuration videos](#)



- Select [Configuration](#) located on the navigation bar
- Select [Barrier groups](#) located on the page menu
- Select [Add barrier group](#) located in the upper right portion of the screen
- Continue to next page →→→

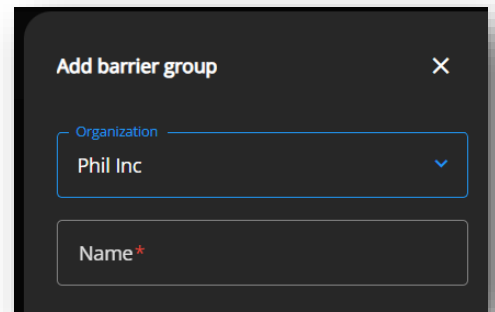
Important Note

- A barrier can only be assigned to a single barrier group

Add Barrier Groups

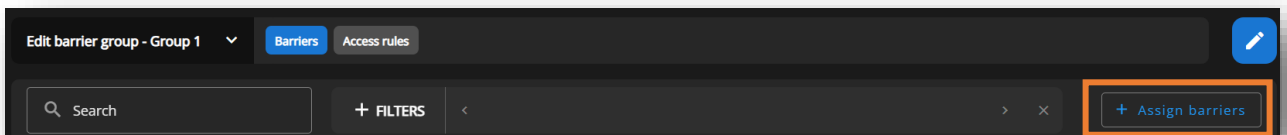
Add barrier group

- Confirm the [Organization](#)
- Name the [Barrier group](#)
- Select [Save](#) at the bottom of the window

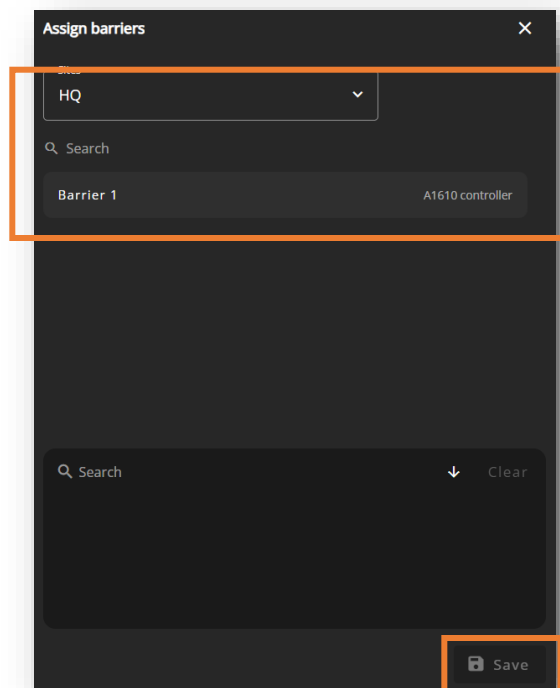


Assign barriers to the group

- After selecting save on the add barrier group window (Previous section above), select [Assign barriers](#) in the upper right corner



- On the popout menu, select the [Site](#) and [Barrier](#)
- Confirm selection and select [Save](#)



Add Identities and Credentials



Audience: Integrator Super Admin, Integrator Admin

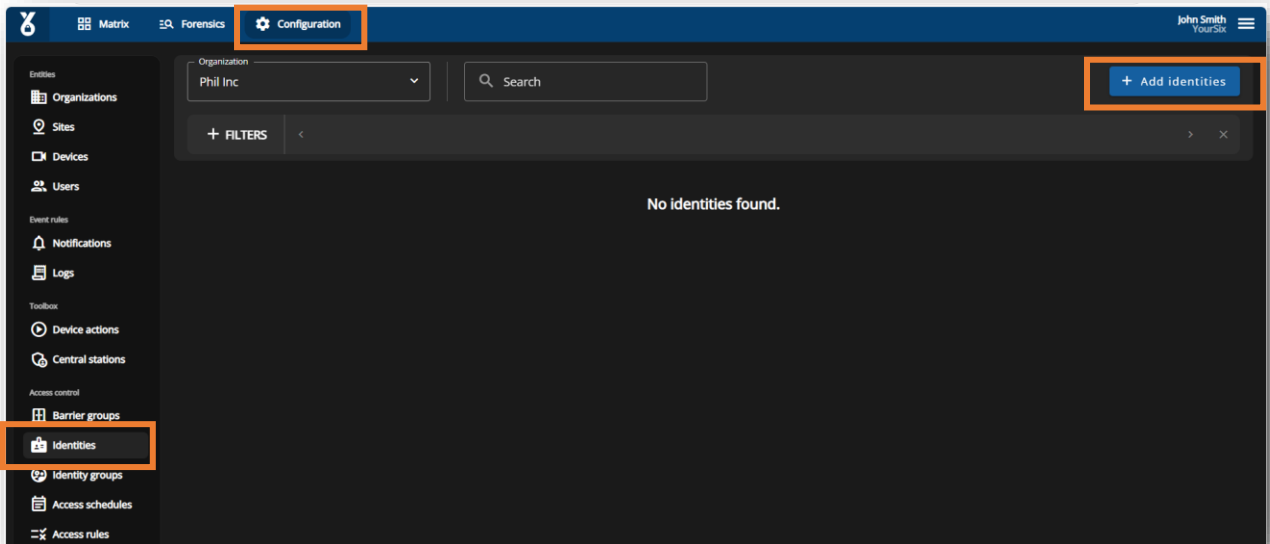


Objective: Add identities and credentials. An identity is an individual in the access control domain, whom is in possession of a credential.



Additional Resources:

- [Identities and credentials videos](#)



- Select [Configuration](#) located on the navigation bar
- Select [Identities](#) located on the page menu
- Select [Add Identities](#) located in the upper right portion of the screen
- Continue to next page →→→

Add Identities

In progress

John Smith

Card 1 # 100000000 *** 1234

Identity name*
John Smith

Credential name*
Card 1

Card*
100000000


PIN
1234

Extended access

↓ ↑

Save & clear Save & finish

Total: 1

- Add the **Name** of the identity
- Add the **Name** of the credential
- Type in the **Card detail information** or select the  icon in order to get the card information from a reader
 - *Card detail must be in same order as how reader reads the data*
- Select **Save**. In order to add multiple indemnities at once, select the + icon

Add Identity Groups



Audience: Integrator Super Admin, Integrator Admin

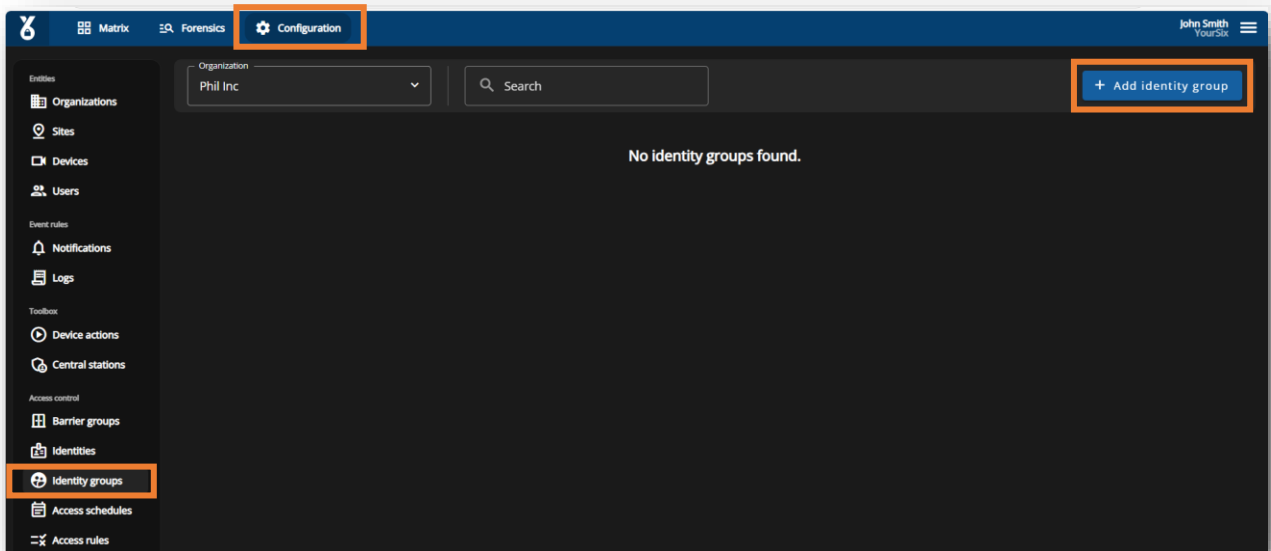


Objective: Add identity groups. Identity groups are a group of identities that allows for simultaneous configuration of access using access rules.



Additional Resources:

- [Identities and credentials videos](#)



- Select [Configuration](#) located on the navigation bar
- Select [Identity groups](#) located on the page menu
- Select [Add identity group](#) located in the upper right portion of the screen
- Continue to next page →→→

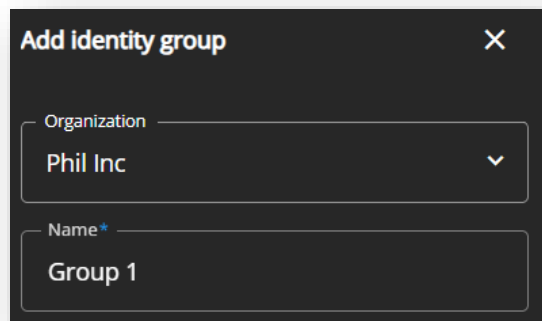
Important Note

- An identity can be assigned to multiple identity groups

Add Identity Groups

Add identity group

- Confirm the [Organization](#)
- Name the [Identity group](#)
- Select [Save](#) at the bottom of the window



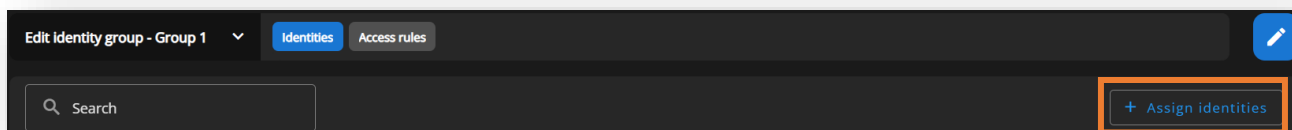
Add identity group [X]

Organization [Phil Inc]

Name* [Group 1]

Assign identities to the group

- After selecting save on the add identity groups window (Previous section above), select [Assign identities](#) in the upper right corner

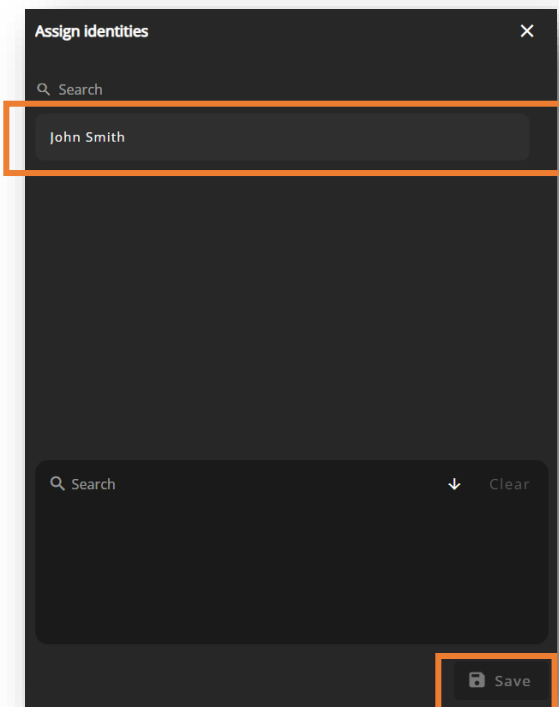


Edit identity group - Group 1 [v] [Identities] [Access rules] [Edit]

Search

+ Assign identities

- On the popout menu, select the [identities](#)
- Confirm selection and select [Save](#)



Assign identities [X]

Search

John Smith

Search [Clear]

Save

Add Access Schedules



Audience: Integrator Super Admin, Integrator Admin

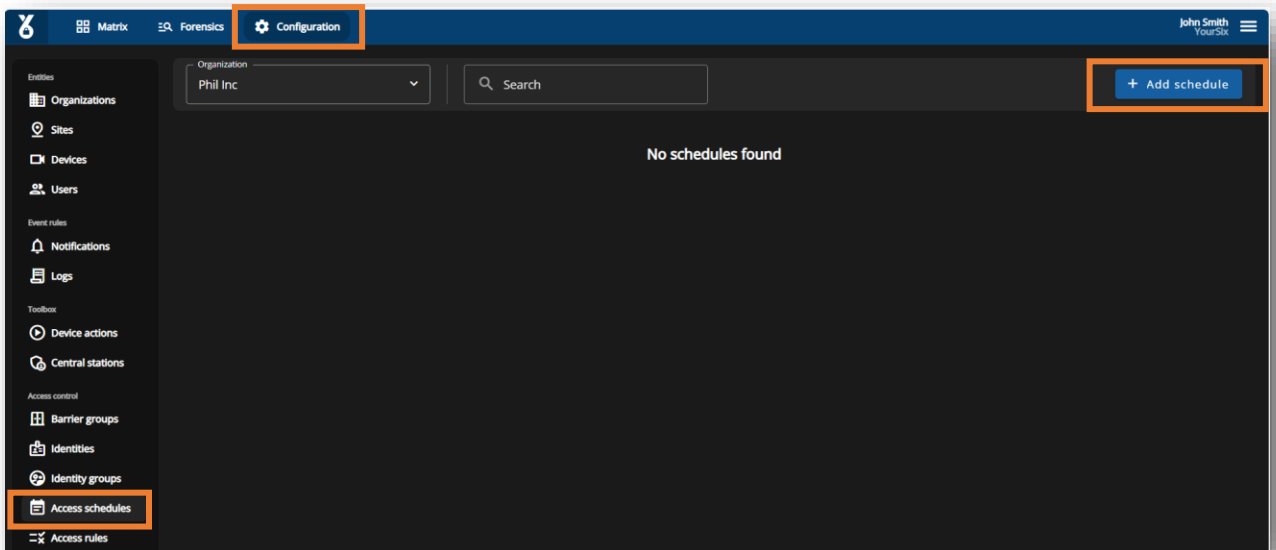


Objective: Add access schedules. An access schedule will be used as the “when” in granting access.



Additional Resources:

- [Access control configuration videos](#)



- Select [Configuration](#) located on the navigation bar
- Select [Access schedules](#) located on the page menu
- Select [Add schedules](#) located in the upper right portion of the screen
- Continue to next page →→→

Add Access Schedules

Schedules can be setup based on a weekly frequency or a one-time occurrence

The screenshot shows the 'Add schedule' dialog box. At the top, there is a title bar with 'Add schedule' and a close button 'X'. Below the title bar, there are three input fields: 'Name*' (with a red error icon), 'Frequency' (set to 'Weekly'), and 'Organization' (set to 'Phil Inc'). Below these fields are seven rows for days of the week (Mon through Sun). Each row has a grid of 24 checkboxes for time slots and a button on the right. The 'All day' button is present for all days. The 'Same as previous day' button is present for Tue through Sun. The 'Name*' field is highlighted with an orange border.

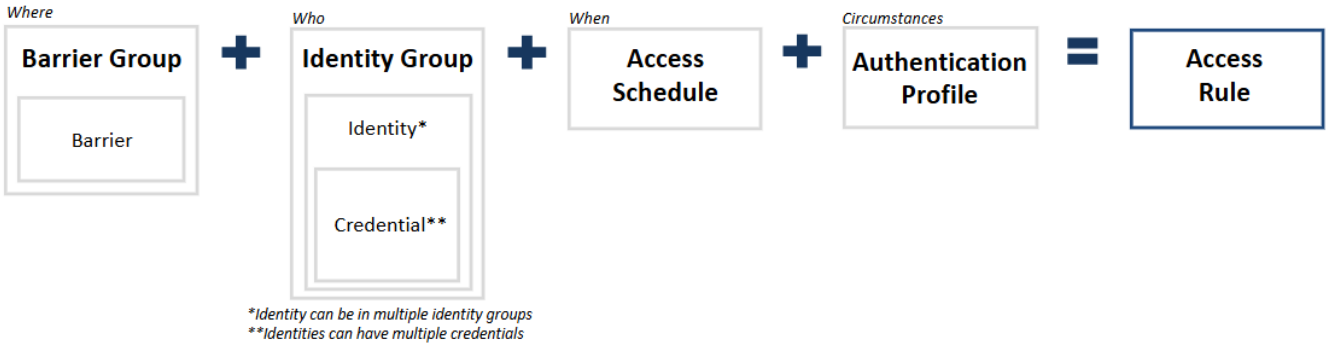
- Name the schedule
- Select the **Frequency** (Weekly or one-time)
 - Weekly: Reoccurring schedule that is standard each week
 - One-time: One-time schedules based on certain dates
- Confirm **Organization**
- Select the desired time windows that make up the schedule
 - *Important note: If a REX is used, a 24/7 schedule is recommended*

Exceptions: Exceptions can be used to exclude a specific time window from the schedule. Note that exceptions will only one-time time windows that are otherwise in schedule, they can not be used to include additional time windows. If you want to add extra time to your schedule, consider using one-time schedules.

- Select **Save** at the bottom of the window

Access Rules Overview

Once the previous components are in place, access rules must be created. Access rules utilize the previous created components to specify who is permitted to enter, where, when, and under what circumstances.



Important Notes

- Each rule must be created separately. So, if someone has a barrier that requires a card to access and a REX to exit then 2 rules must be created.

Access Rule General Options

Entry Rules

Rule	Authentication Profile	Direction
Pin required to access	Pin	In
Card required to access	Card	In
Card + Pin required to access	Card + PIN	In

Exit Rules

Rule	Authentication Profile	Direction
Request to exit	REX	Out
Pin required to exit	Pin	Out
Card required to exit	Card	Out
Card + Pin required to exit	Card + PIN	Out

Unlock Rules

Rule	Authentication Profile	Direction
Barrier unlocked	Unlocked	None

Add Access Rules



Audience: Integrator Super Admin, Integrator Admin

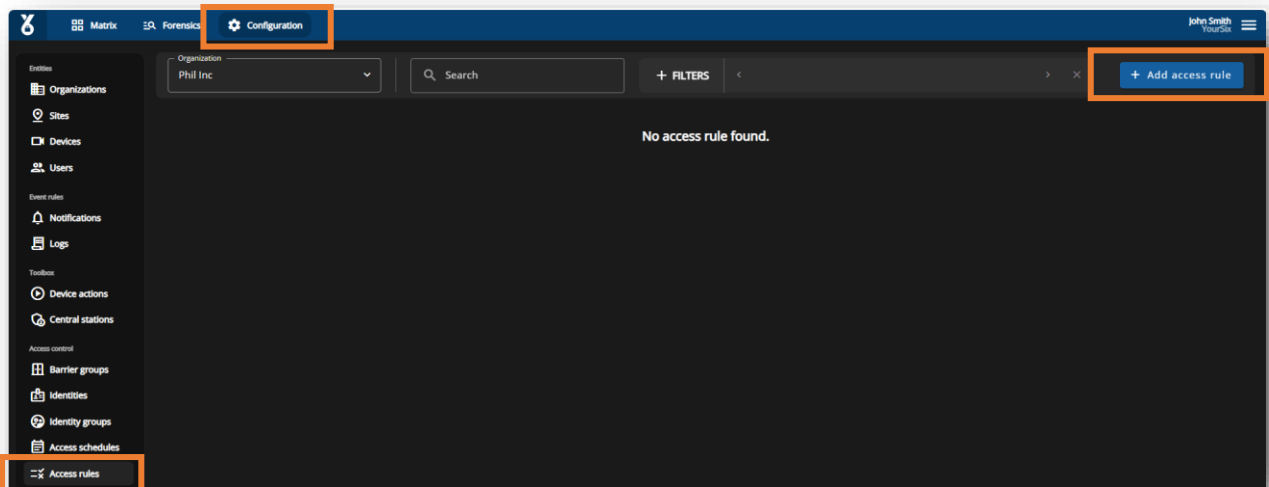


Objective: Create access rules. Access rules utilize the previous created components to specify who is permitted to enter, where, when, and under what circumstances.



Additional Resources:

- [Access control configuration videos](#)



- Select [Configuration](#) located on the navigation bar
- Select [Access rules](#) located on the page menu
- Select [Add access rules](#) located in the upper right portion of the screen
- Continue to next page →→→

Add Access Rules

Entry/Exit Rule

- Confirm **Organization**
- Enter **Name**
- Select the **Barrier group**
- Select the **Authentication profile**
 - Card
 - Pin
 - Card+Pin (*Requires both card & pin*)
- Select the **Identity group**
- Select **Direction**
- Select the **Schedule**
- Select **Save**

The screenshot shows the 'Add access rule' form with the following fields and values:

- Organization: Phil Inc
- Name: Card for entry
- Barrier group: Group 1
- Authentication profile: Card
- Identity group: Group 1
- Direction: In
- Schedule: work hours

The schedule is visualized as a grid for the days of the week (Mon-Sun). The 'work hours' schedule is active, showing blue bars for the working hours of each day. A 'Save' button is highlighted in the bottom right corner.

REX Rule

- Confirm **Organization**
- Enter **Name**
- Select the **Barrier group**
- Select **REX** as the Authentication profile
- Select the **Schedule**
- Select **Save**

The screenshot shows the 'Add access rule' form with the following fields and values:

- Organization: Phil Inc
- Name: REX
- Barrier group: Group 1
- Authentication profile: REX
- Identity group: (empty)
- Direction: Out
- Schedule: 24/7

The schedule is visualized as a grid for the days of the week (Mon-Sun). The '24/7' schedule is active, showing blue bars for all 24 hours of every day. A 'Save' button is highlighted in the bottom right corner.

Add Access Rules

Unlocked Rule

When will Barriers be unlocked

- Confirm **Organization**
- Enter **Name**
- Select the **Barrier group**
- Select **Unlocked** as the Authentication profile
- Select the **Schedule**
- Select **Save**

The screenshot shows the 'Add access rule' configuration window. The fields are as follows:

Organization *	Phil Inc	Name *	Barriers Unlocked
Barrier group *	Group 1	Authentication profile *	Unlocked
Identity group		Direction	None

The Schedule section is set to 'work hours' and shows a grid of 24 columns for each day of the week (Mon-Sun). The 'work hours' schedule shows blue bars for the first 8 hours of each weekday.

A 'Save' button is located in the bottom right corner.

Review Rules and Testing

- Confirm all Access Rules are configured properly
- Test all barriers to ensure desired response

Users

- [Manage Users](#)
- [Edit a User](#)
- [Add a User](#)

Manage Users



Audience: Integrator Super Admin, Integrator Admin



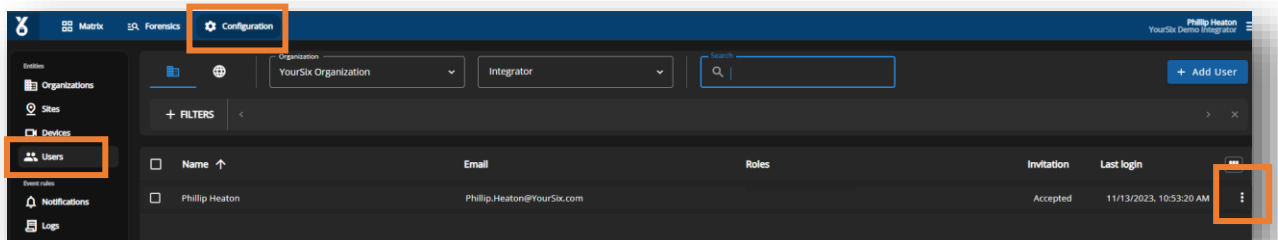
Objective: Manage users.

- Account Details
- Account Role
- View User Site Permissions
- Add Site Permissions
- View User Device Permissions
- Add Device Permissions



Additional Resources:

- [Adding user videos](#)



- Select **Configuration** located on the navigation bar
- Select **Users** located on the page menu
- Select **Pen** icon to edit the user
- Continue to next page →→→

Edit a User



Audience: Integrator Super Admin, Integrator Admin



Objective: Edit a user and permissions.

User Information

First Name* Phillip

Last Name* Heaton

Email*

Roles*

Organization Super Admin x Organization Admin x

Organization User x

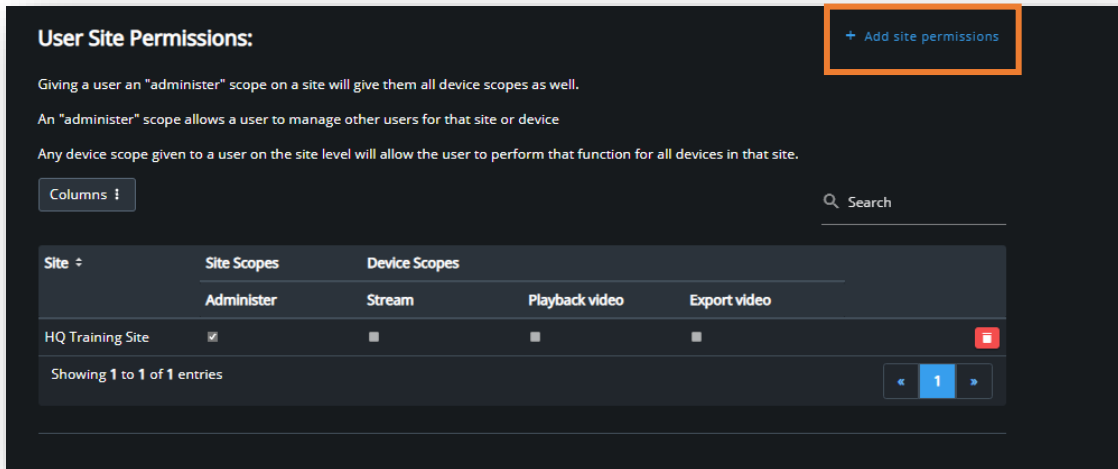
User's global roles within system.

Send password reset email Save

Basic User Information:

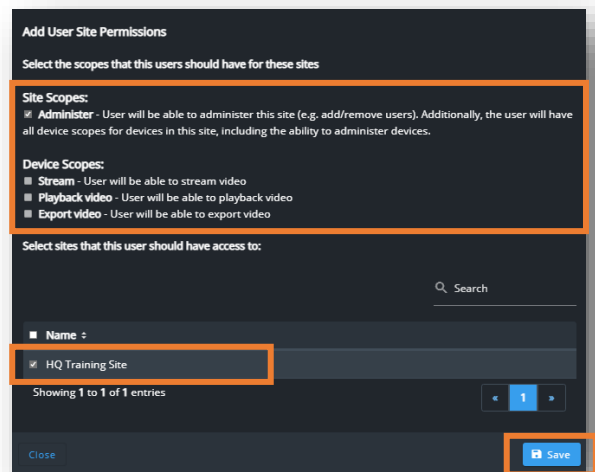
- Enter user [First Name](#) and [Last Name](#)
- Select or remove [Permissions](#)
- Select [Save](#)
- Continue to next page →→→

Edit a User

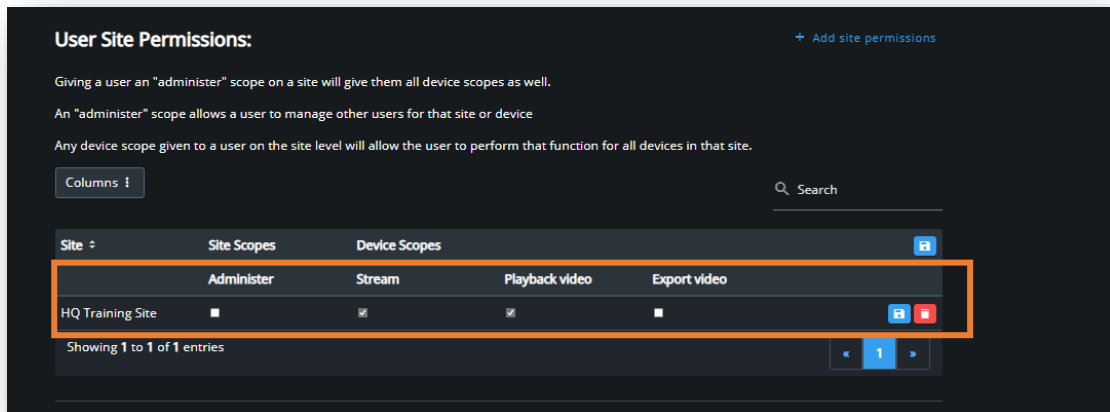


Add Site Permissions:

- Select [Add Site Permissions](#)
- In the popup menu select the [Site Scopes](#) or [Device Scopes](#) for the user
- Select the [Site](#) from the list
- Select [Save](#)
- Continue to next page →→→



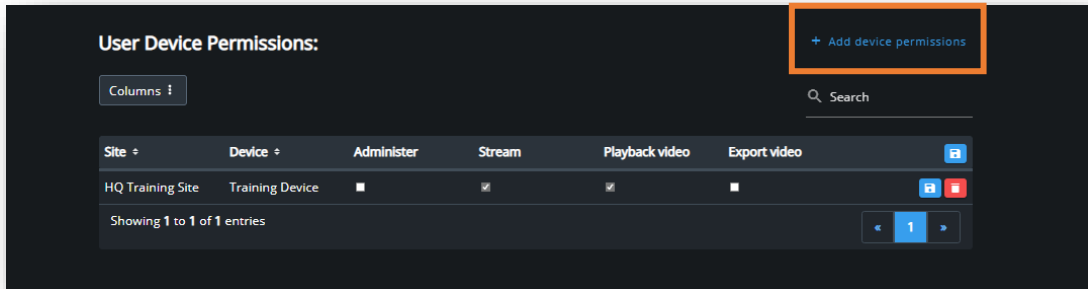
Edit a User



Edit Site Permissions:

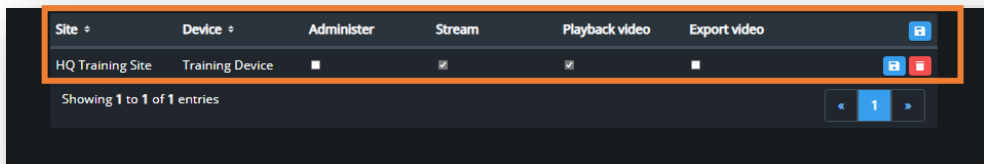
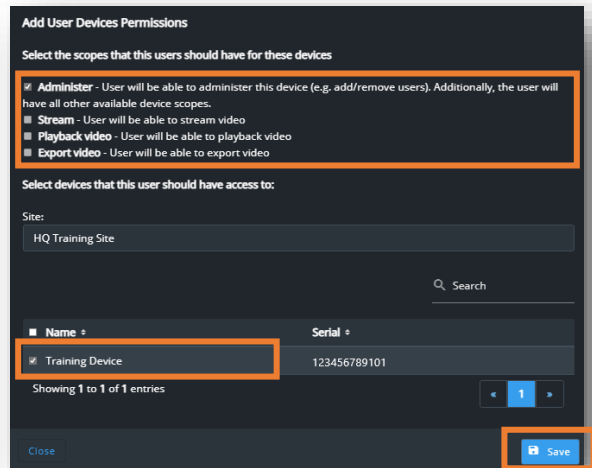
- Select the desired [Site Scopes](#) or [Device Scopes](#)
- Select the [Save Icon](#)
- *To delete a site permission, select the [Trash Can Icon](#)*
- Continue to next page →→→

Edit a User



Add Device Permissions:

- Select [Add Device Permissions](#)
- In the popup menu select the [Site Scopes](#) or [Device Scopes](#) for the user
- Select the [Device](#) from the list
- Select [Save](#)
- Continue to next page →→→



Edit Device Permissions:

- Select the desired [Site Scopes](#) or [Device Scopes](#)
- Select the [Save Icon](#)
- *To delete a site permission, select the [Trash Can Icon](#)*

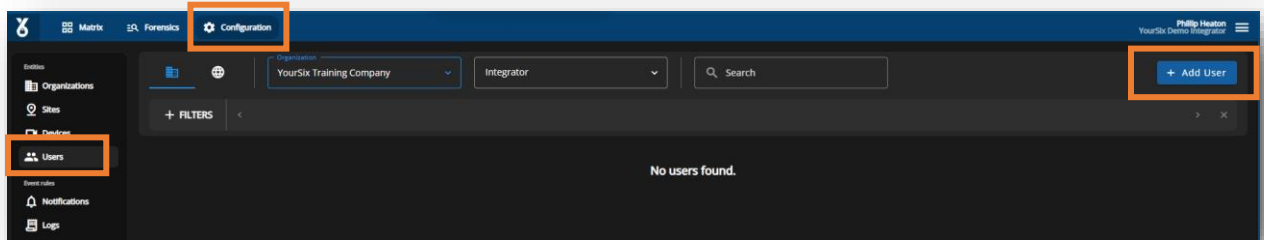
Add Users



Audience: Integrator Super Admin, Integrator Admin



Objective: Add new users to an organization or integrator.



- Select [Configuration](#) located on the navigation bar
- Select [Users](#) located on the page menu
- Select [Add User](#) located in the upper right portion of the screen
- Continue to next page →→→

Add Organization Users

User Information

Account Details:

First Name * Last Name *

Email *

Account Roles: [Create Integrator User](#)

Organization
YourSix Organization

Roles *
User's global roles within system.

Save

- Enter information into the required fields
- Select the [Organization](#) the user will be associated to
- Select the [Account Role](#) the user should have for access
 - Please reference the Y6OS User Permission Guide when choosing the desired role for the user.
- Select [Save](#)
- To add an Integrator User, Select [Create Integrator User](#) in the upper right.

Add Integrator Users

User Information

Account Details:

First Name * Last Name *

Email *

Account Roles: [Create Organization User](#)

Roles *
User's global roles within system.

Save

- From the Create Organization User page, select Create Integrator User.
 - Please see the previous page for details.
- Enter information into the [required fields](#).
- Select the [Account Role](#) the user should have for access
 - Please reference the Y6OS Permission Guide when choosing the desired role for the user.
- Select [Save](#)

Events

- [Notification Overview](#)
- [Create Notifications](#)
- [Create Notification for Video Monitoring](#)
- [Edit Notifications](#)
- [Logs](#)

Notification Overview

Source:

- Notifications can be sent based on events that come from different sources. Those sources are:
 - Devices: Select individual devices that are the source of the event
 - Device Groups: Select a group of devices that are the source of the event (Device Groups should always be utilized as the source when creating a notification that will go to a central monitoring station)
 - Sites: Select an entire site which allows all devices at that site to be the source of the event

Events:

- There are two main kinds of events that can trigger a notification
 1. **Event Based** (motion detection, audio detection, etc)
 - The most used event/trigger is AXIS VMD (Video Motion Detection). When enabled, this notification will be sent out anytime there is movement within the field of view
 - When setting up a notification for central stations, AOA (AXIS object Analytics) should be utilized as the event to reduce false alarms
 - Tuning the Analytic: It is important to utilize include/exclude areas in order to cut out objectives that continuously cause motion in the field of view (like trees, water, etc). Include/exclude areas do not hinder the ability to see the entire field of view nor the camera's ability to record footage for the entire field of view.
 2. **Health Based** (device disconnect/connect, storage disruption, etc)
 - Device connect and disconnect are the most utilized health event. These events will trigger once when a device disconnects and once when the device reconnects
- Event and Health based notifications should be setup as separate notifications in the platform

Notification Overview

Recipients:

- The platform supports notifications being sent to the following recipients:
 - Users of the platform
 - Organization Emails
 - Organization Webhooks
 - Central Stations

Receiving Notifications

- Notifications can be received by text or email. Each user can control their own preference. This is located under “My Account” located within the upper right hamburger menu

Create Notifications



Audience: Integrator Super Admin, Integrator Admin

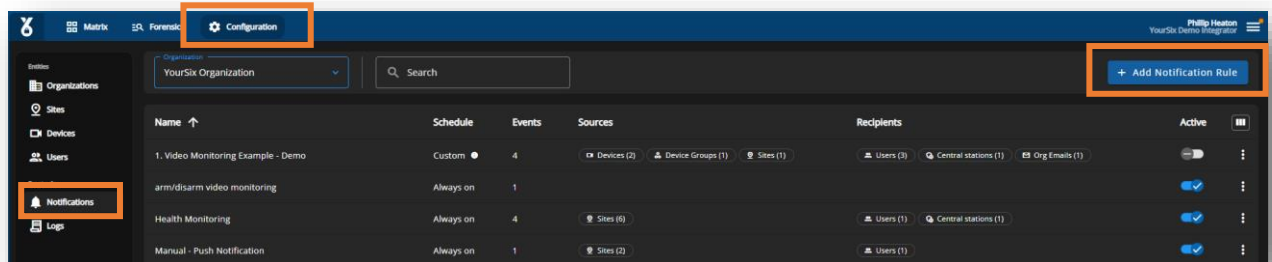


Objective: Create a notification rule.



Additional Resources:

- [Notification videos](#)



- Select [Configuration](#) located on the navigation bar
- Select [Notifications](#) located on the page menu
- Select [Add Notification](#) located in the upper right portion of the screen
- Continue to next page →→→

Create Notifications

Create Notification Rule

Notification Information

Name* Description

Organization*

Custom Schedule

A custom schedule allows to only trigger notifications within a specified timeframe. If no scheduling is used, the notification rule will always be active.

Timezone

Select what timezone the schedule should follow.

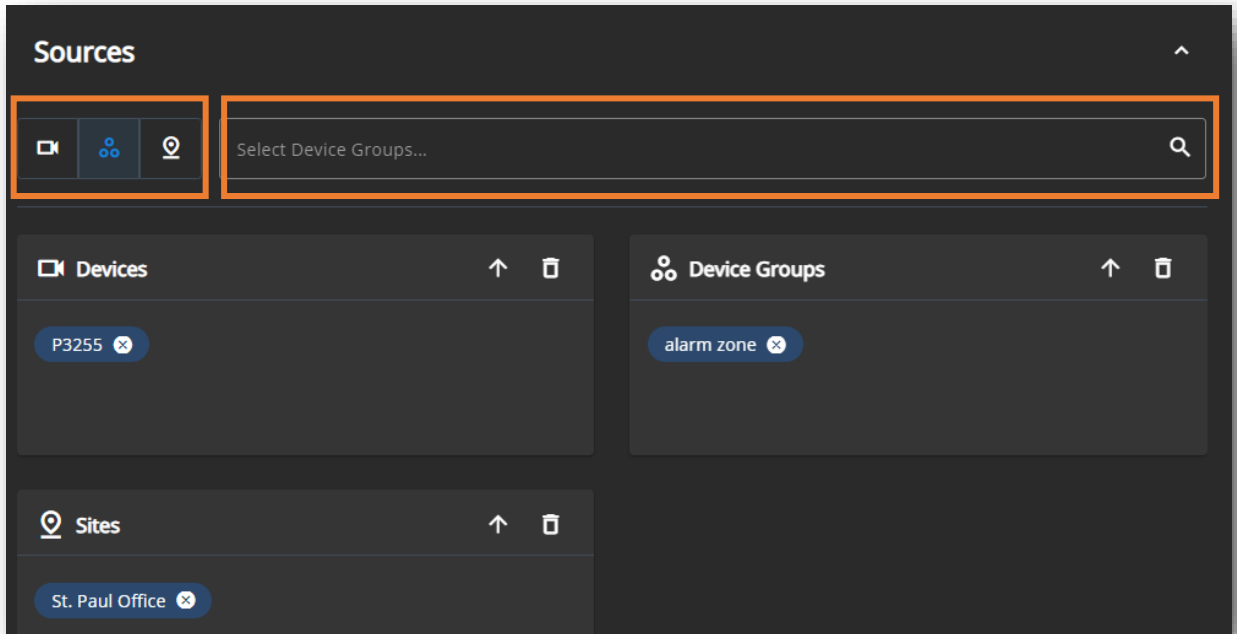
In this example the rule is set to be active from 6 PM to 8 AM Monday – Friday and all-day Saturday and Sunday.

Day	00:00	06:00	18:00	24:00	Action
Mon	Active	Active	Active	Active	All day
Tue	Active	Active	Active	Active	Same as previous day
Wed	Active	Active	Active	Active	Same as previous day
Thu	Active	Active	Active	Active	Same as previous day
Fri	Active	Active	Active	Active	Same as previous day
Sat	Active	Active	Active	Active	Same as previous day
Sun	Active	Active	Active	Active	Same as previous day

Rule Name & Schedule:

- Add the **Name & Description** and select the **Organization** for the rule
- Select the desired **Time Zone** for the rule
- Create the **Schedule** for the rule (i.e., when the rule will be active)
 - Health notifications should use a schedule that is always active
- Continue to next page →→→

Create Notifications






Rule Sources:

- On the [Edit Notification Rule](#) page navigate to the [Sources](#) section

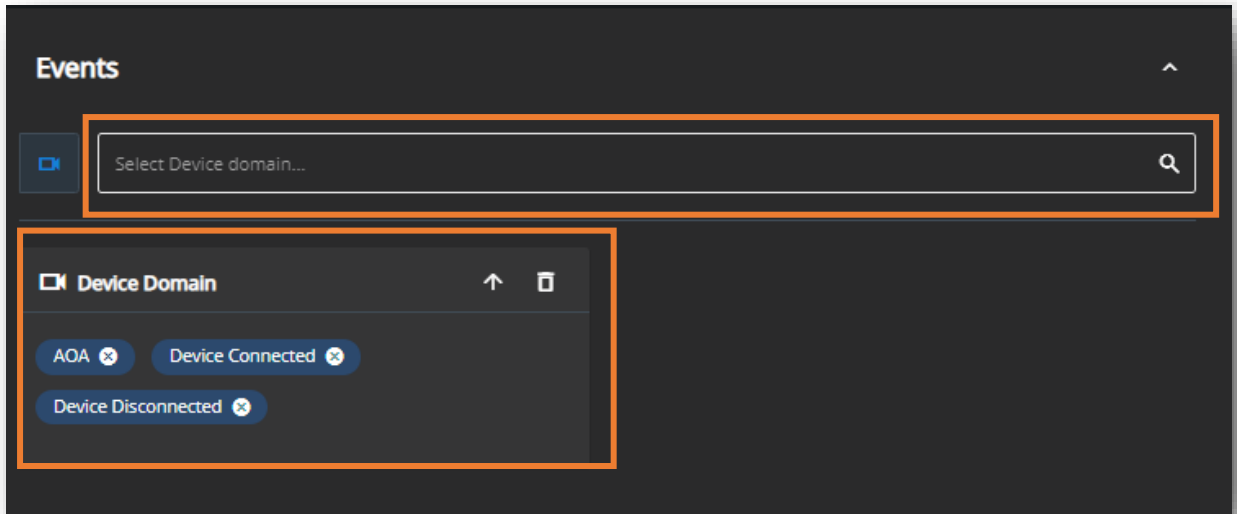
Note: The rule/notification being created can apply to a device, device groups, and/or sites.

- Select the [Icon](#) for which you want to assign as the source; these icons are located below the upper left corner of the sources box

-  Devices
-  Device Groups (To create see [Create Device Group](#))
-  Sites

- After selecting from the options above, select the [Search Bar](#) located to the right of the icons
- Select the source from the drop-down menu; the selected source will appear in the appropriate box
- Continue to next page →→→

Create Notifications



If the notification is for a central station, then please refer to the next section which covers [Notifications for Video Monitoring](#)

Rule Events:

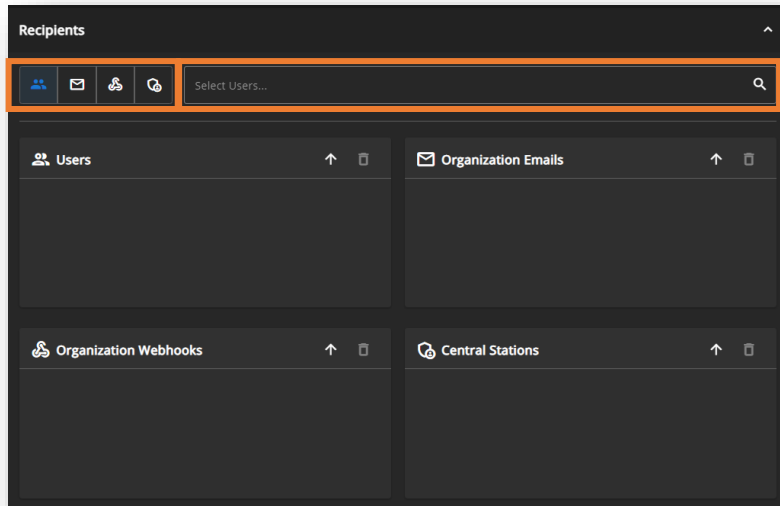
- On the [Edit Notification Rule](#) page navigate to the [Events](#) section
- From the drop-down, select the Event/Domain for which the rule will trigger

Note: Selected domains will only work on devices that have been enabled. For example, if a device group has some devices with AOA and some without then only the devices with AOA will trigger the notification.

Note: If the event is a health notification such as device connect or disconnect it is recommended that users create two separate notifications. One for events/triggers (motion for example) that is based on a certain schedule. The second rule would be on 24/7 and would send notifications based on device health (device connect/disconnect)

- Once the device domain is selected the device domain will appear in the [Device Doman Box](#)
- Continue to next page →→→

Create Notifications



Rule Recipients:

- On the [Edit Notification Rule](#) page navigate to the [Recipients](#) section

Note: The rule/notification being created can notify a user, org email, webhooks and/or a central station.

- Select the [Icon](#) for which you want to select a recipient; these icons are located below the upper left corner of the recipient box



Users



Organization Emails (*To create see [Manage My Org](#)*)



Organization Webhooks



Central Stations (*Full guide available*)

- After selecting from the options above, select the [Search Bar](#) located to the right of the icons
- Select the recipient from the drop-down menu; the selected recipient will appear in the appropriate box
- Select [Save](#) rule at the bottom of the page

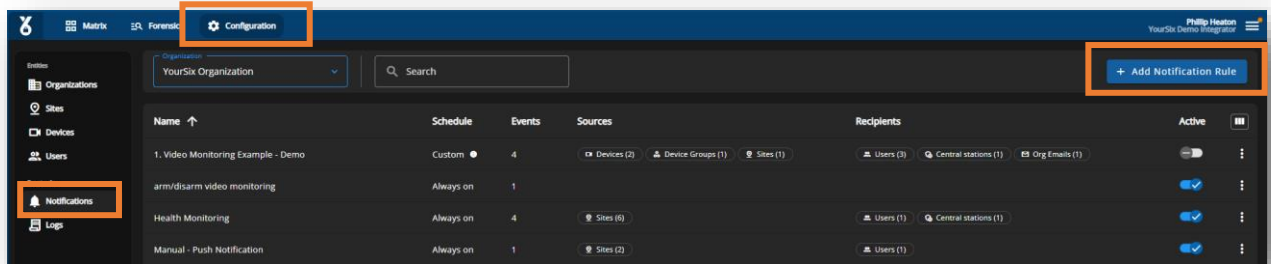
Create Notifications for Video Monitoring



Audience: Integrator Super Admin, Integrator Admin



Objective: Create a notification rule for notifications that will be sent to a central Station



- Select [Configuration](#) located on the navigation bar
- Select [Notifications](#) located on the page menu
- Select [Add Notification](#) located in the upper right portion of the screen
- Continue to next page →→→

Create Notifications for Video Monitoring

Create Notification Rule

Notification Information

Name* Description

Organization*

Custom Schedule

A custom schedule allows to only trigger notifications within a specified timeframe. If no scheduling is used, the notification rule will always be active.

Timezone

Select what timezone the schedule should follow.

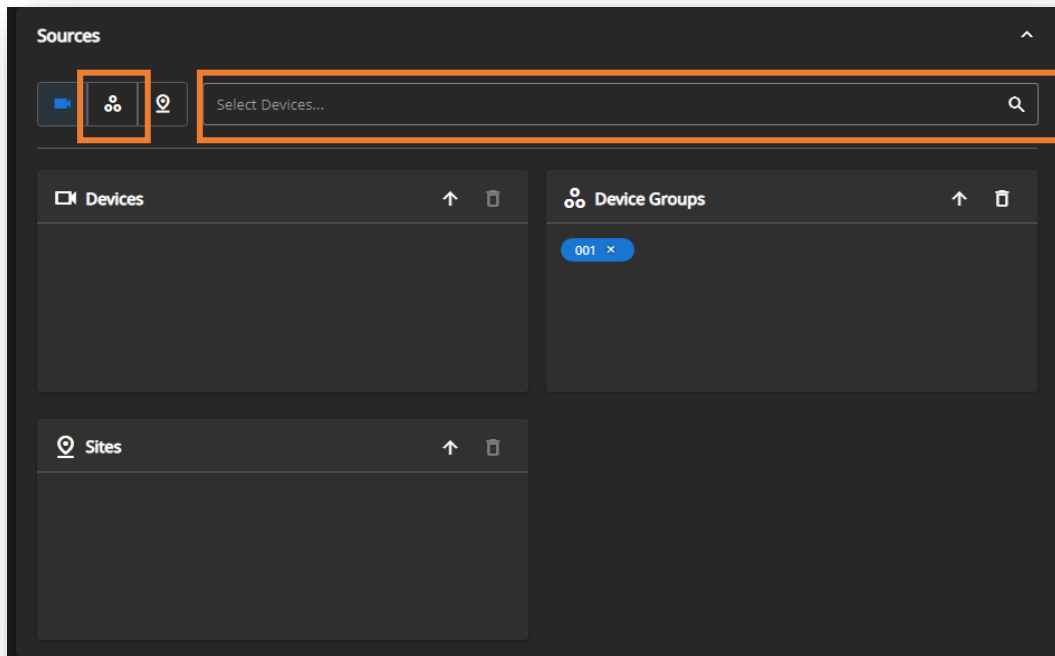
In this example the rule is set to be active from 6 PM to 8 AM Monday - Friday and all-day Saturday and Sunday.

Day	00:00	06:00	18:00	24:00	Action
Mon	Active	Active	Active	Active	All day
Tue	Active	Active	Active	Active	Same as previous day
Wed	Active	Active	Active	Active	Same as previous day
Thu	Active	Active	Active	Active	Same as previous day
Fri	Active	Active	Active	Active	Same as previous day
Sat	Active	Active	Active	Active	Same as previous day
Sun	Active	Active	Active	Active	Same as previous day

Rule Name & Schedule:

- Navigate to the [Notifications Icon](#) and Select [Create Notification Rule](#)
- Add the [Name & Description](#) and select the [Organization](#) for the rule
- Select the desired [Time Zone](#) for the rule
- Create the [Schedule](#) for the rule (i.e., when the rule will be active). For Video Monitoring this is when the central station will receive notifications.
- Continue to next page →→→

Create Notifications for Video Monitoring



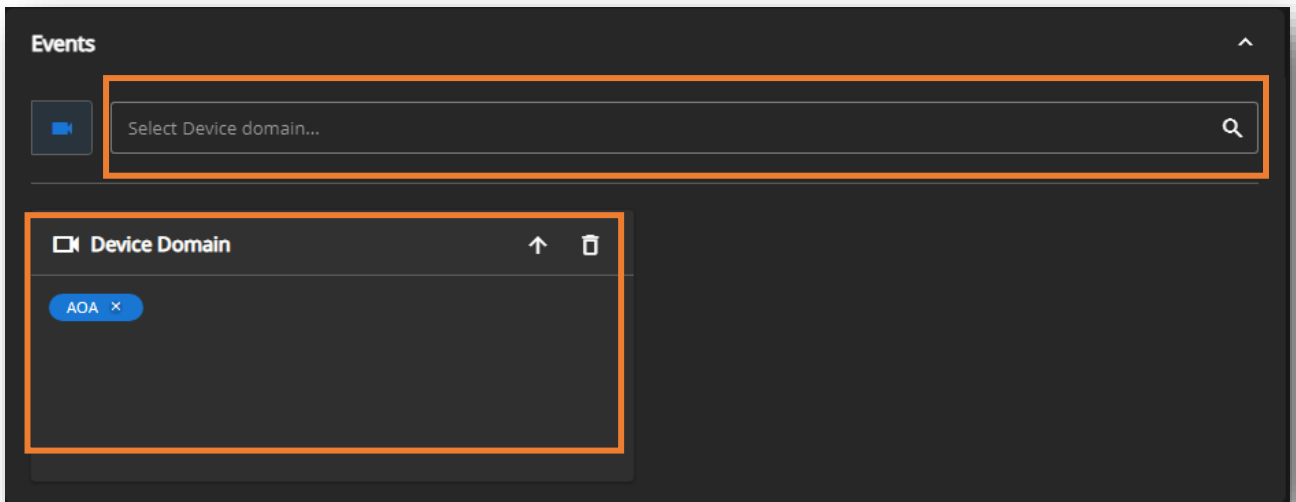
Rule Sources:

- On the [Edit Notification Rule](#) page navigate to the [Sources](#) section
- Select the [Device Group Icon](#). Notifications for video monitoring must be set up at a device group level. Do not setup video monitoring notifications for site.

Device Groups (To create see [Create Device Group](#))

- Select the [Search Bar](#) located to the right of the icons and select the proper device group
- Continue to next page →→→

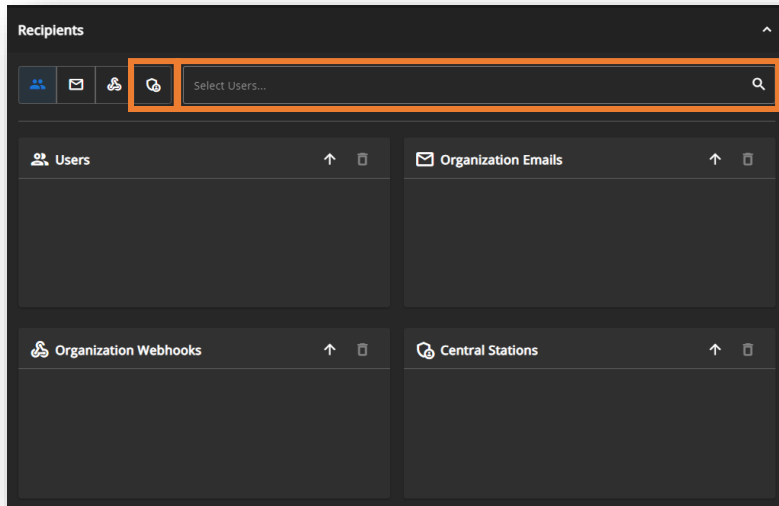
Create Notifications for Video Monitoring



Rule Events:

- On the [Edit Notification Rule](#) page navigate to the [Events](#) section
- From the drop-down, select AOA (Axis Object Analytics) which is the trigger used to send the notification
- Once the device domain is selected the device domain will appear in the [Device Doman Box](#)
- Continue to next page →→→

Create Notifications for Video Monitoring



Rule Recipients:

- On the [Edit Notification Rule](#) page navigate to the [Recipients](#) section
- Select the [Central Station Icon](#)
- Select the [Search Bar](#) located to the right of the icons and select the central station you wish the notifications to go to. If you do not see the proper central station, then please reach out to YourSix
- Select [Save](#) rule at the bottom of the page

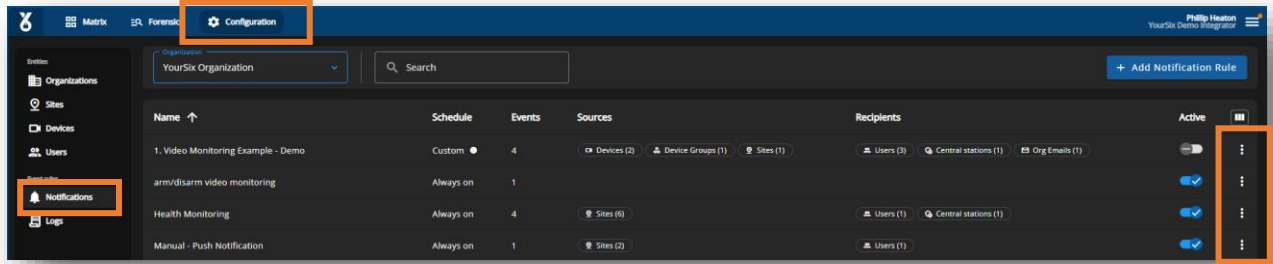
Edit Notifications



Audience: Integrator Super Admin, Integrator Admin



Objective: Manage notification rules.



- Select [Configuration](#) located on the navigation bar
- Select [Notifications](#) located on the page menu
- Select the [Pen](#) icon located to the right of the notification you wish to edit
- Editing a notification is the same user experience as creating one
 - [\(Create Notification\)](#)

Logs



Audience: Integrator Super Admin, Integrator Admin

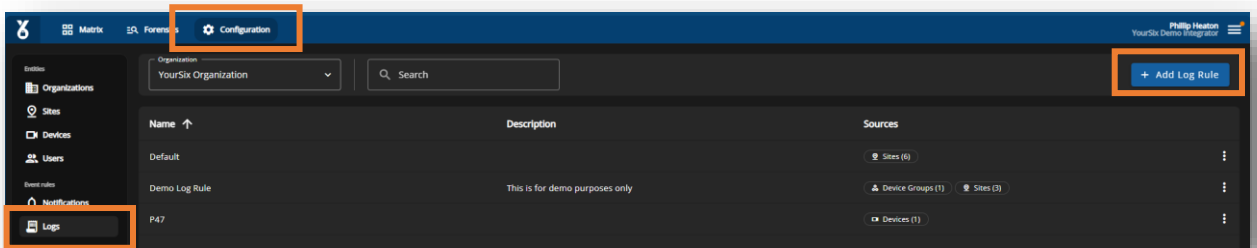


Objective: Setup log rules to create event flags on the timeline



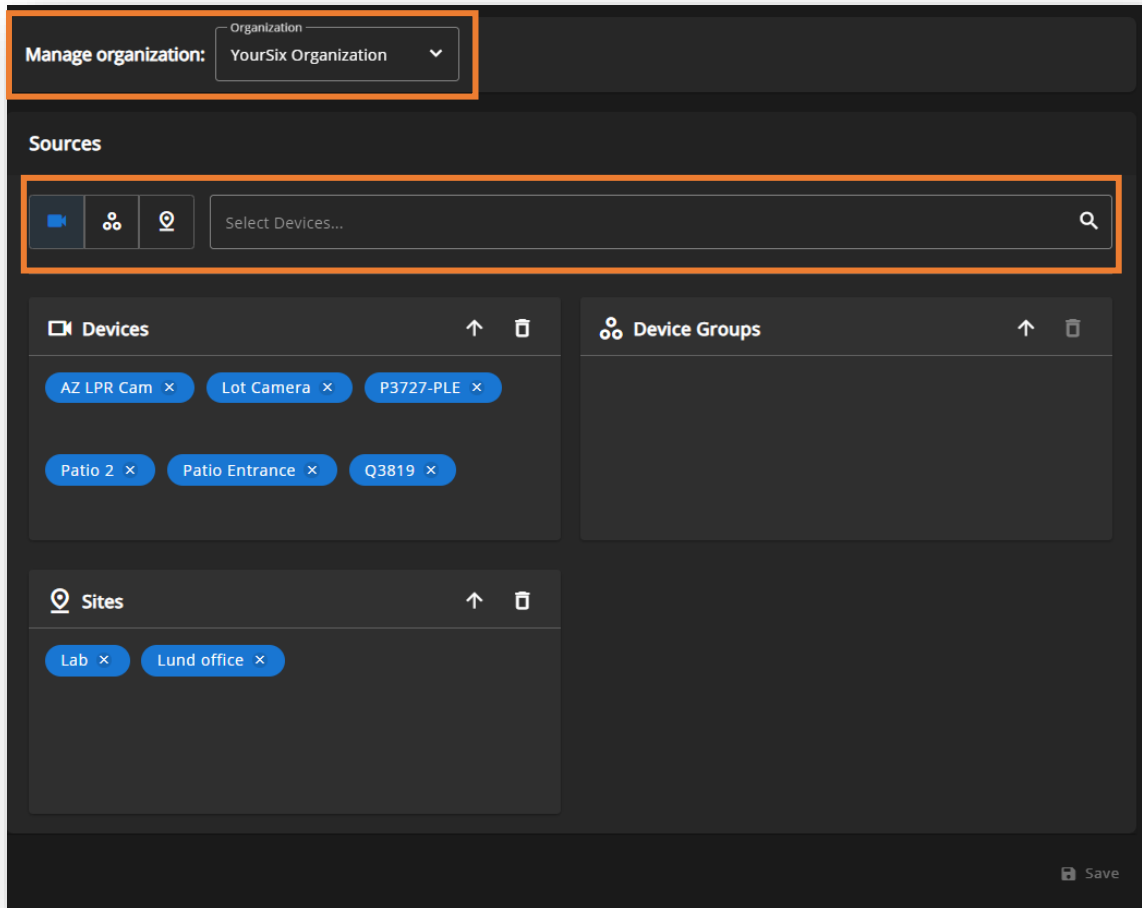
Additional Resources:

- [Notification videos](#)



- Select [Configuration](#) located on the navigation bar
- Select [Logs](#) located on the page menu
- Select [Add Log Rules](#) located in the upper right portion of the screen
- Continue to next page →→→

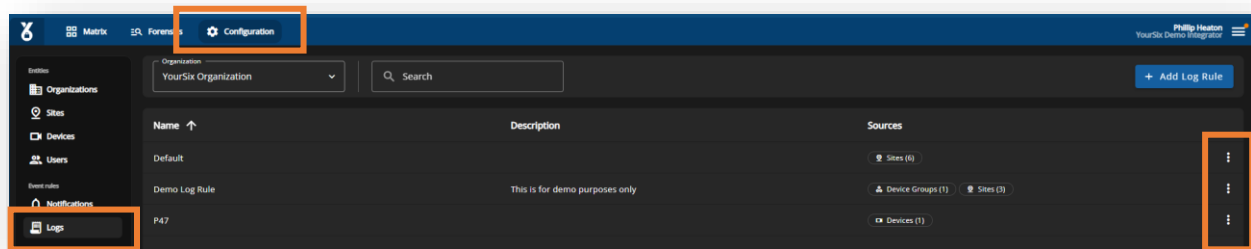
Manage Log Rule



Log Rule:

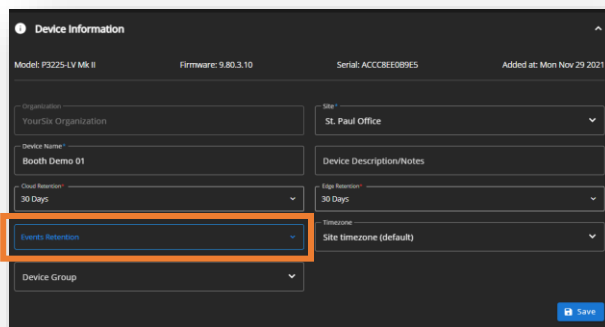
- Select the organization from the [Manage Organization](#) dropdown
- Select the [Device, Device Group or Sites](#) the log rule should apply
- Continue to next page →→→

Manage Log Rule



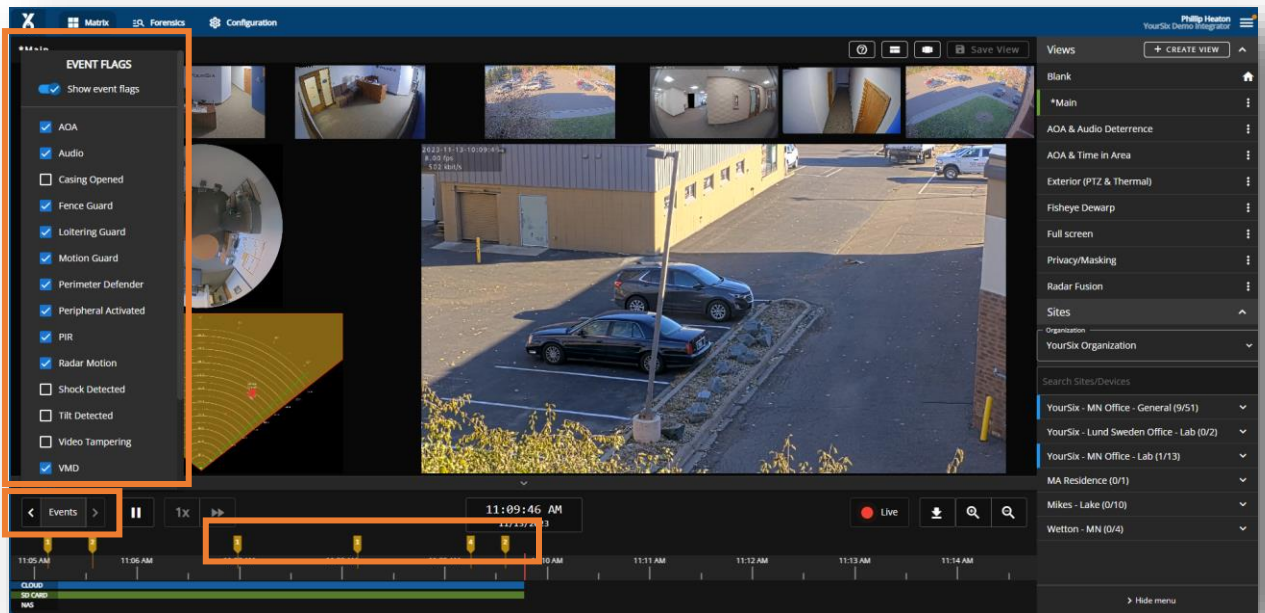
Event Retention for Log Rules:

- Select **Devices** on the Navigation menu
- Use the **Organization, Site** and **Search** bar to locate the device you wish to edit
- Select the **Pen** icon to edit the device



- On the edit/manage device page select the desired **Events Retention** for that device. This is how long the event flags will be saved for this device. Users should select the longest retention time they have selected in the cloud/edge retention sections.
- Select **Save**
- Continue to next page →→→

Manage Log Rule



Event Flags Setup:

- Navigate to the Matrix
- Select **Events** above the timeline
- From the menu, select the **Event Flags** you wish to see on the timeline



Contact Y6

1.800.687.3014

helpdesk@yoursix.com

yoursix.com

About YourSix Inc.

YourSix is an award-winning Physical Security as a Service (PSaaS) provider. The Y6OS cloud platform leverages a unique convergence of surveillance, access control, audio, sensors, artificial intelligence, and monitoring to deliver a singular operational intelligence and physical security solution. YourSix's commitment to innovation continues to transform the industry through its open standards-based framework, robust cybersecurity protocols, and ongoing advancements powered by machine learning/artificial intelligence. YourSix was founded in 2015 and headquartered in St. Paul, Minnesota. In 2021, Inc. 5000, the most prestigious ranking of the nation's fastest-growing private companies, ranked YourSix Inc., No. 208 in America.