YourSix

Y6OS User Guide for Integrators

May 2025 – Version 3.5

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

Contents

Basic Navigation

→ Email Invitation

→ Login

→ Layout

Email Invitation

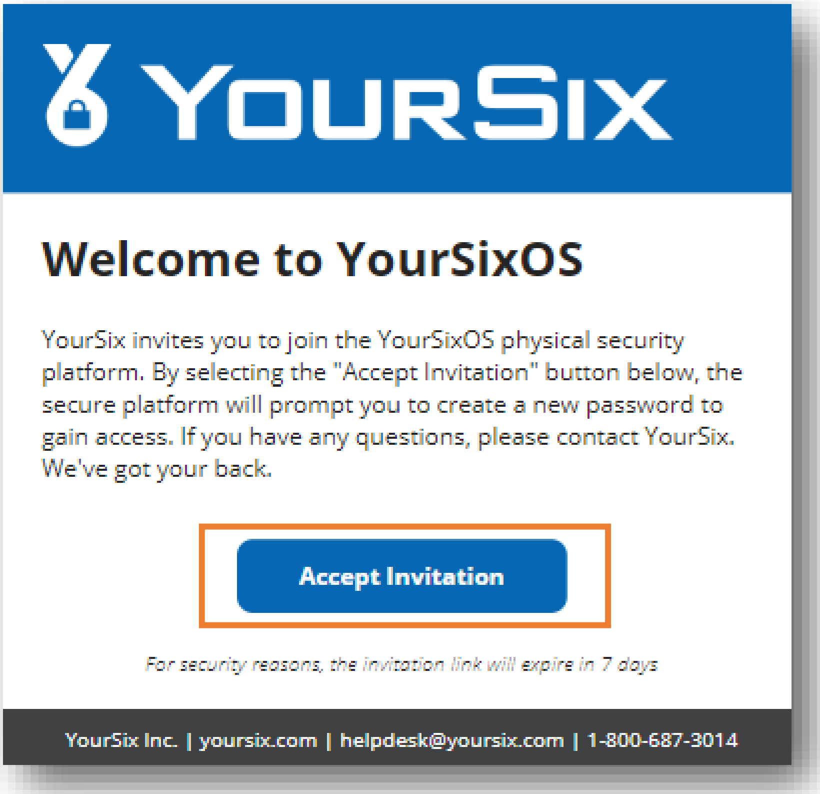
Audience: Integrator Super Admin, Integrator Admin, Integrator Tech

The Y6OS platform will trigger an email invitation:

→ Receive email from: invite@platform.yoursix.com

→ Select Accept Invitation

→ Continue to next page →→→



Welcome to YourSixOS

YourSix invites you to join the YourSixOS physical security platform. By selecting the "Accept Invitation" button below, the secure platform will prompt you to create a new password to gain access. If you have any questions, please contact YourSix. We've got your back.

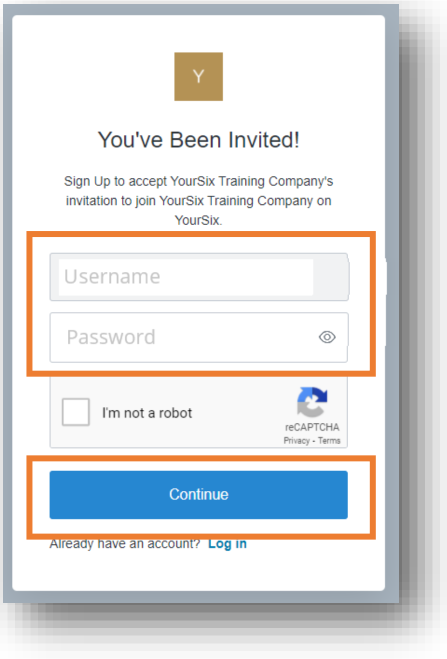
For security reasons, the invitation link will expire in 7 days

YourSix Inc. | yoursix.com | helpdesk@yoursix.com | 1-800-687-3014

Email Invitation

→ Enter Username & Password

→ Select Continue



You've Been Invited!

Sign Up to accept YourSix Training Company's invitation to join YourSix Training Company on YourSix.

Login

Audience: Integrator Super Admin, Integrator Admin, Integrator Tech

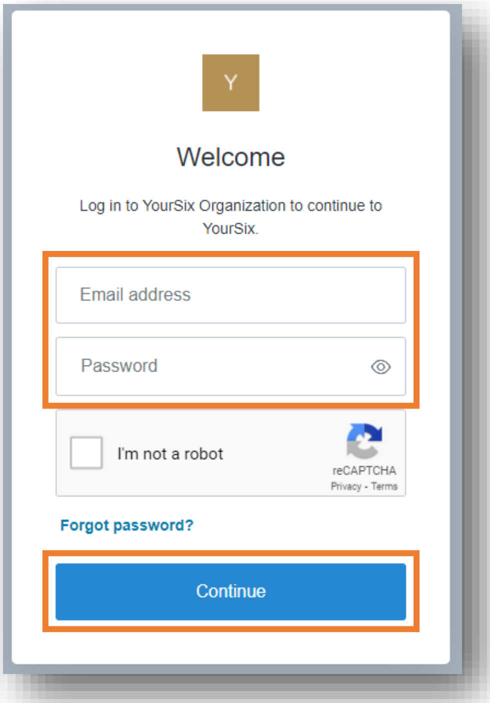
Open a web browser:

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



Y

Welcome

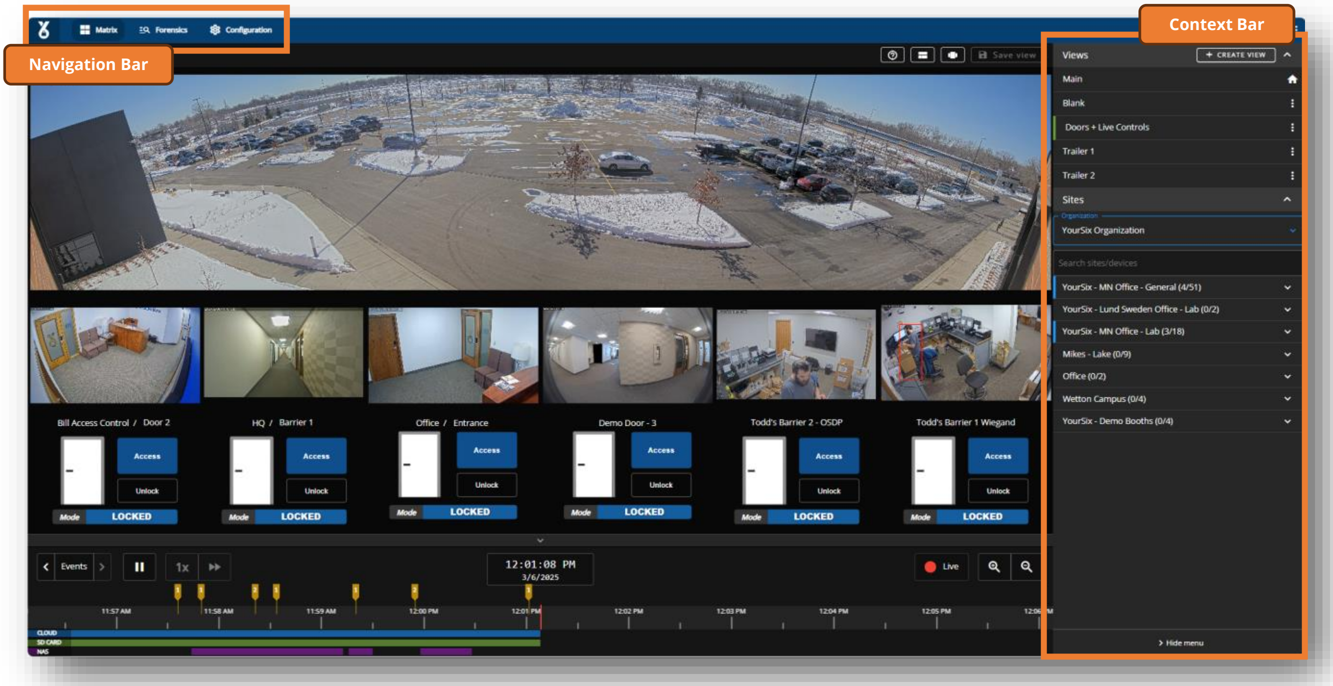
Log in to YourSix Organization to continue to YourSix.

Layout

Audience: Integrator Super Admin, Integrator Admin, Integrator Tech

Additional Resources:

- Basic navigation videos



→ Navigation

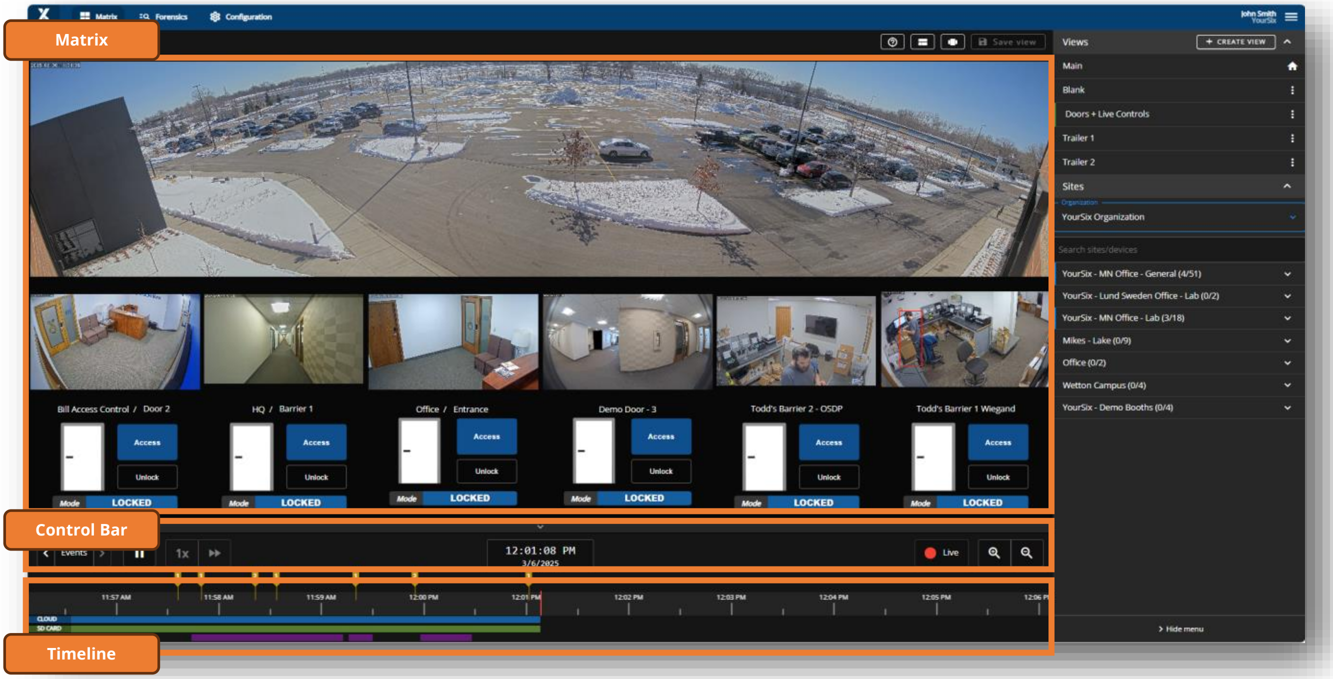
- Matrix
- Forensics
  - Search Events, Access Events, Objects (Object Appearance Search)
  - Exports
  - Validator
- Configuration
  - Organizations
  - Sites
  - Devices
  - Users
  - Notifications
  - Logs
  - Access Control

→ 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

YOURSIX

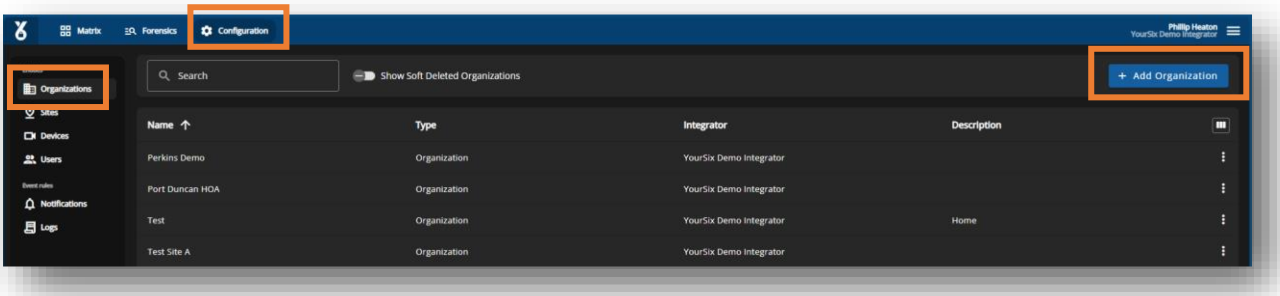
Add an Organization

Audience: Integrator Super Admin, Integrator Admin, Integrator Tech

Objective: Create a new organization.

Additional Resources:

- [Get started videos]



Name ↑	Type	Integrator	Description
Perkins Demo	Organization	YourSix Demo Integrator	
Port Duncan HOA	Organization	YourSix Demo Integrator	
Test	Organization	YourSix Demo Integrator	Home
Test Site A	Organization	YourSix Demo Integrator	

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.

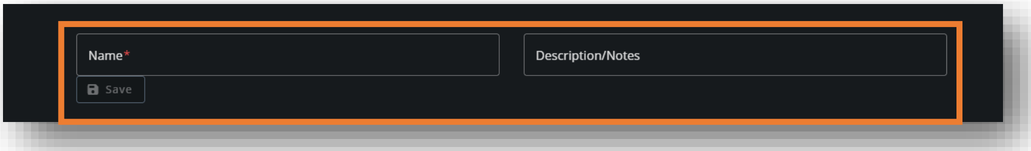
→ Select Configuration located on the navigation bar

→ 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



→ Name the Organization

→ Add Description

→ Select Save

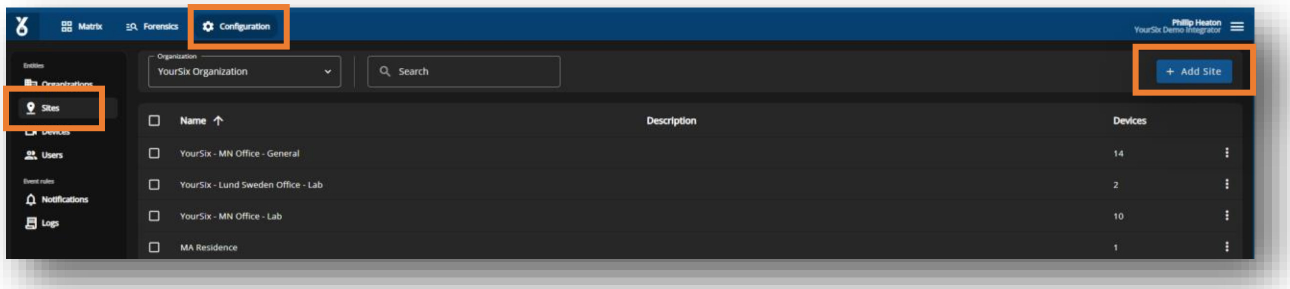
Add Sites

Audience: Integrator Super Admin, Integrator Admin, Integrator Tech

Objective: Create a new site under an organization.

Additional Resources:

- Get started videos



Organization: YourSix Organization

□	Name ↑	Description	Devices
□	YourSix - MN Office - General		14
□	YourSix - Lund Sweden Office - Lab		2
□	YourSix - MN Office - Lab		10
□	MA Residence		1

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.

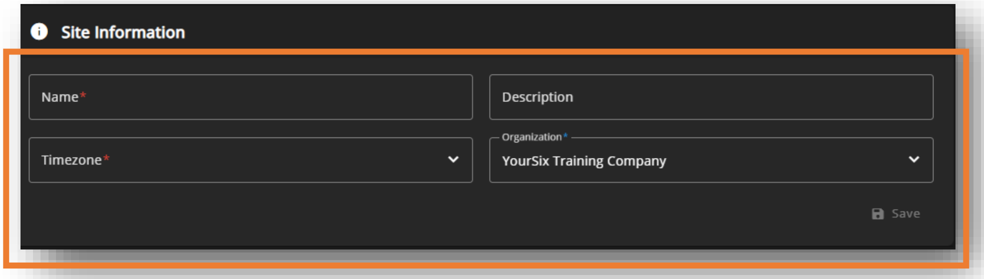
→ Select Configuration located on the navigation bar

→ 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



Organization*: YourSix Training Company

→ Enter the Site Name

→ Enter a Description

→ Select the desired Time Zone

→ Select the Organization that the site should be assigned to

→ Select Save

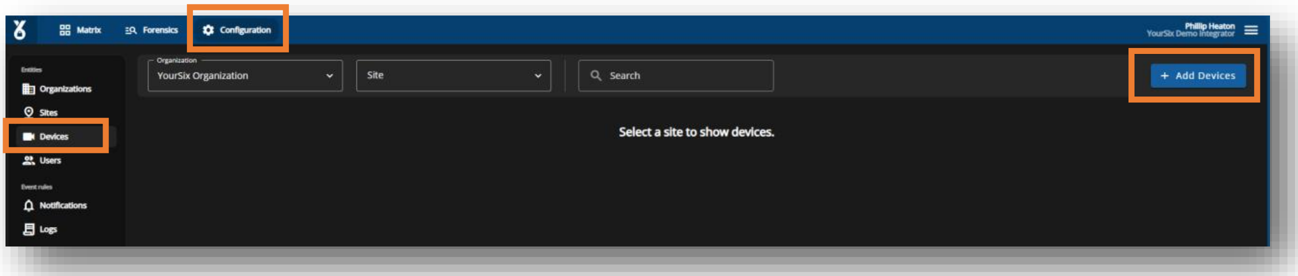
Add Devices

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



Organization: YourSix Organization

Site

Select a site to show devices.

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

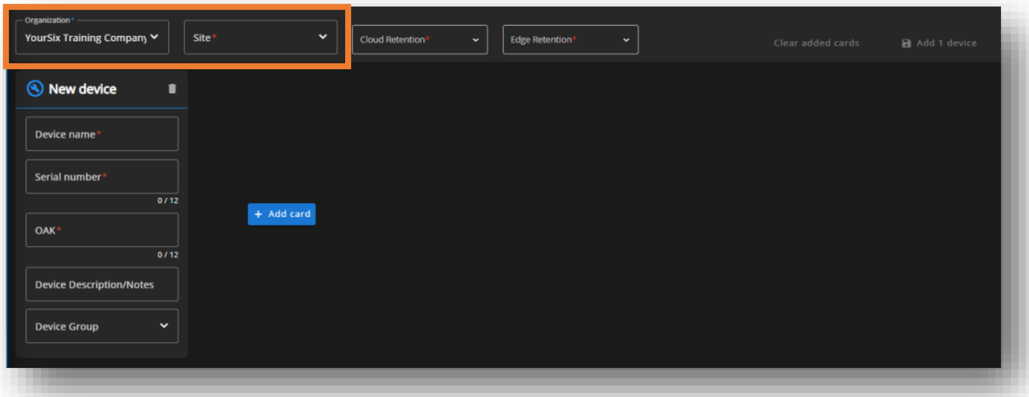
→ Select Configuration located on the navigation bar

→ Select Devices located on the page menu

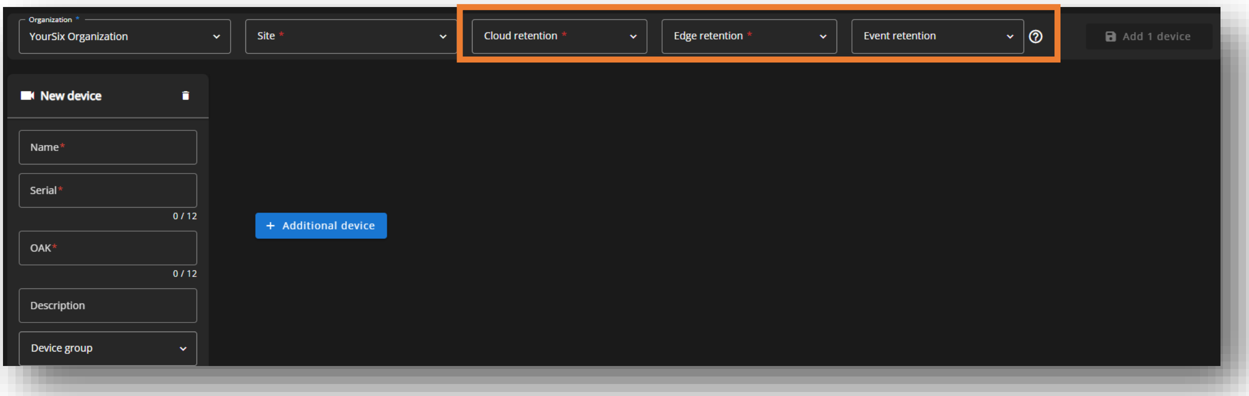
→ Select Add Devices located in the upper right portion of the screen

→ Continue to next page →→→

Add Devices



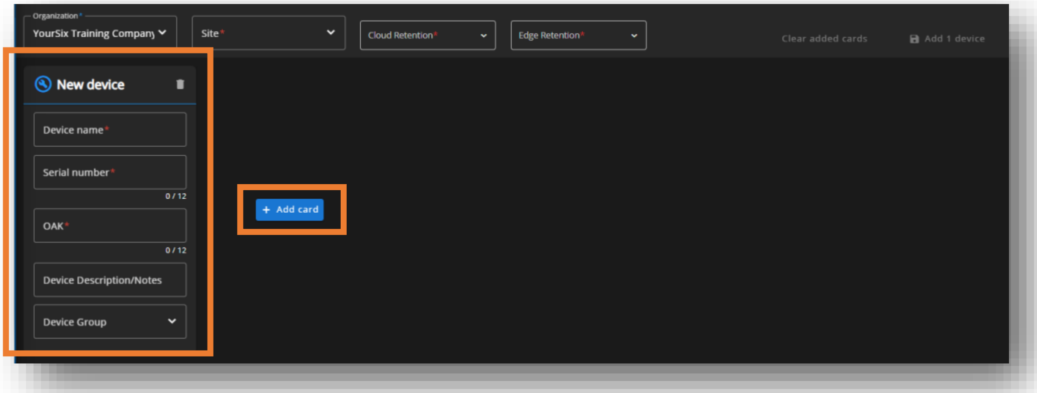
→ Select the Organization and Site that the device(s) will be added to



→ Select the Cloud Retention, Edge Retention, Event Retention for the device(s)
→ Event Retention: Amount of time for which events (triggers) will be logged by the platform. This does not affect anything with footage/recordings.

→ Continue to next page →→→

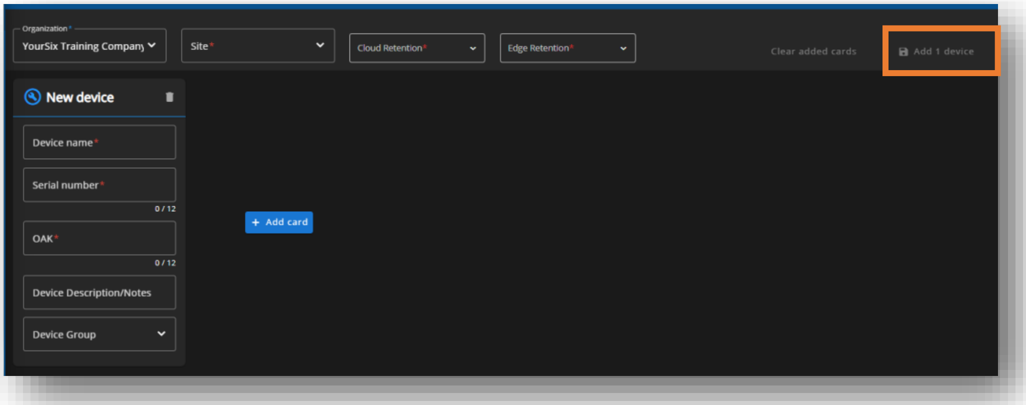
Add Devices



→ 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

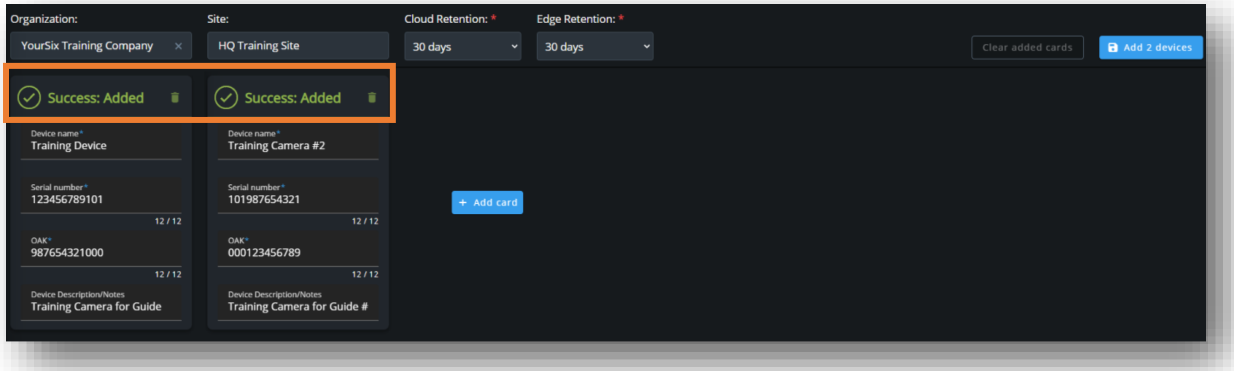
→ If you are adding multiple devices to the same site with the same cloud and edge retention, you can select the +Add card button. This will allow you to mass upload devices.



→ Select Add "#" devices button

→ Continue to next page →→→

Add Devices



Organization: YourSix Training Company

Site: HQ Training Site

Cloud Retention: * 30 days

Edge Retention: * 30 days

✓ Success: Added

Device name* Training Device

Serial number* 123456789101 12 / 12

OAK* 987654321000 12 / 12

Device Description/Notes Training Camera for Guide

✓ Success: Added

Device name* Training Camera #2

Serial number* 101987654321 12 / 12

OAK* 000123456789 12 / 12

Device Description/Notes Training Camera for Guide #

→ 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

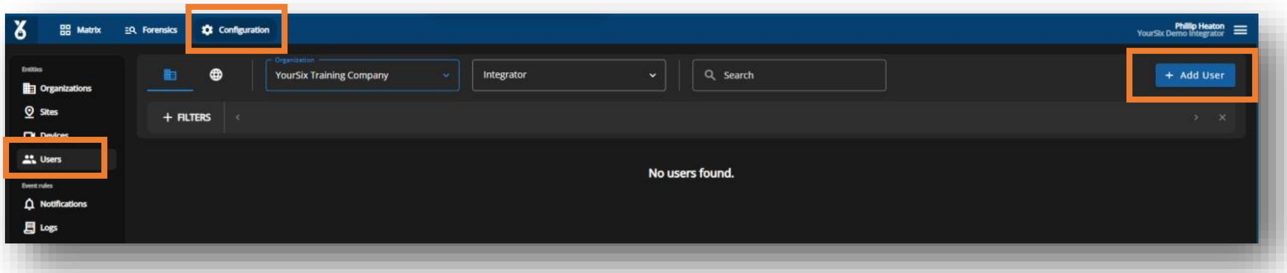
Add Users

Audience: Integrator Super Admin, Integrator Admin

Objective: Add new users to an organization or integrator.

Additional Resources:

- Adding user videos
- Scopes and permissions overview



No users found.

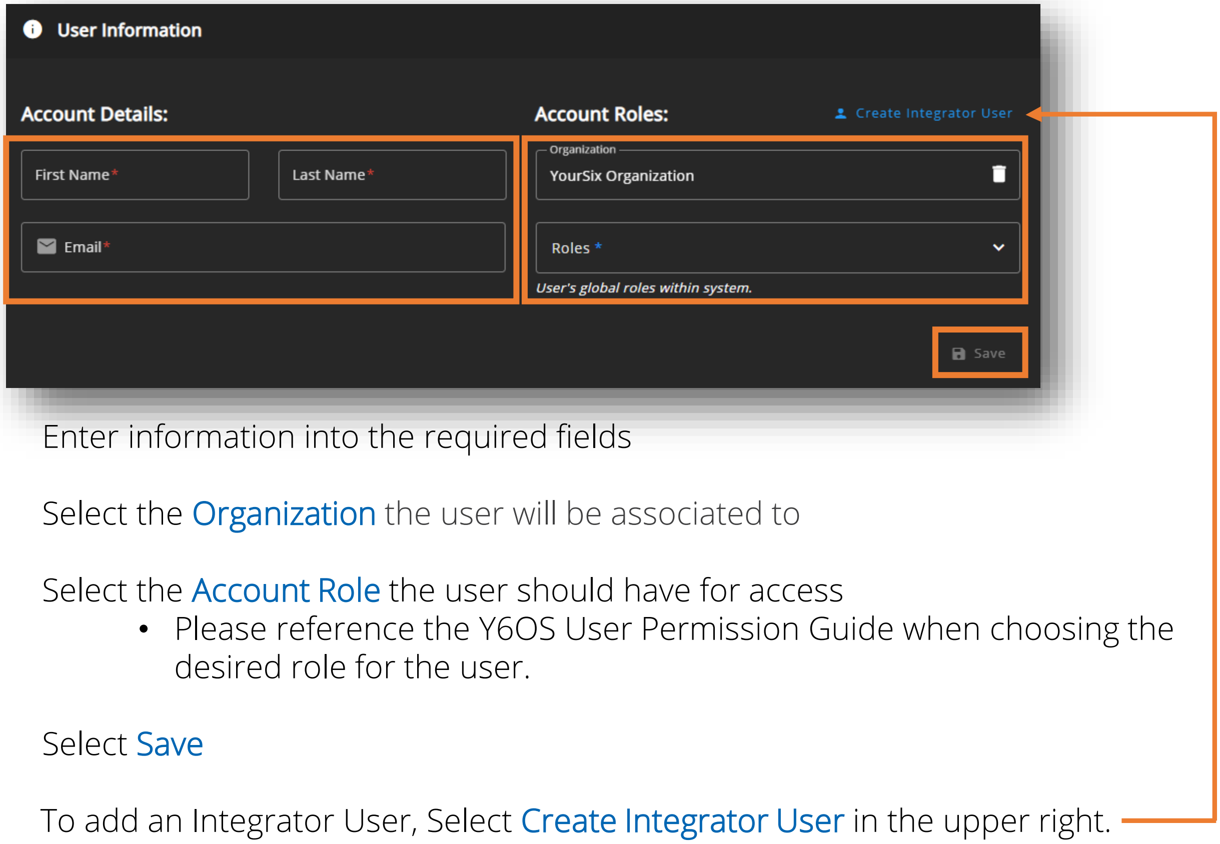
→ Select Configuration located on the navigation bar

→ 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



→ Enter information into the required fields

→ Select the Organization the user will be associated to

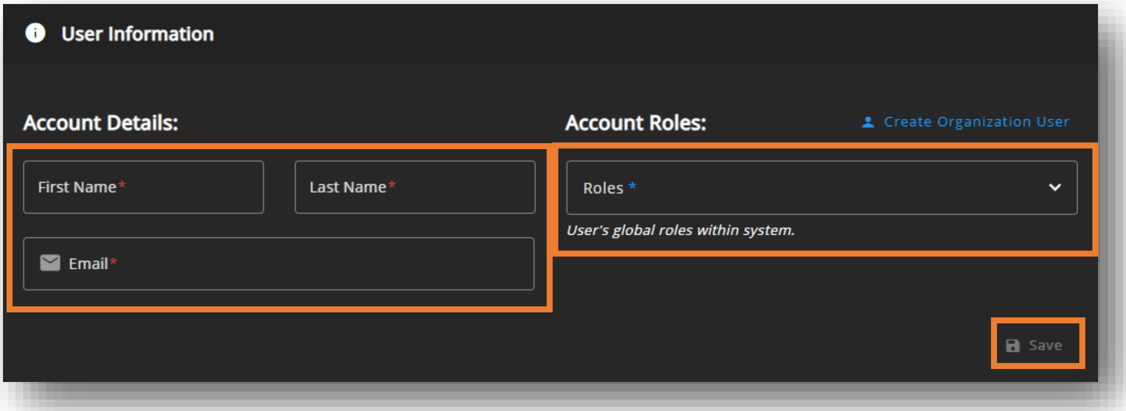
→ Select the Account Role the user should have for access

- 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



→ 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

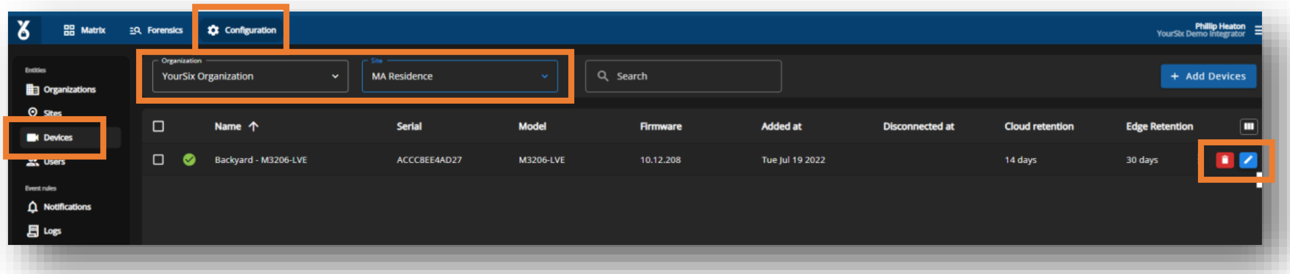
Create a Rule

Audience: Integrator Super Admin, Integrator Admin, Integrator Tech

Objective: Create a recording rule.

Additional Resources:

- Recording rules best practices
- Recording rules and storage videos



□		Name ↑	Serial	Model	Firmware	Added at	Disconnected at	Cloud retention	Edge Retention	
□	✓	Backyard - M3206-LVE	ACCC8EE4AD27	M3206-LVE	10.12.208	Tue Jul 19 2022		14 days	30 days	

→ Select Configuration located on the navigation bar

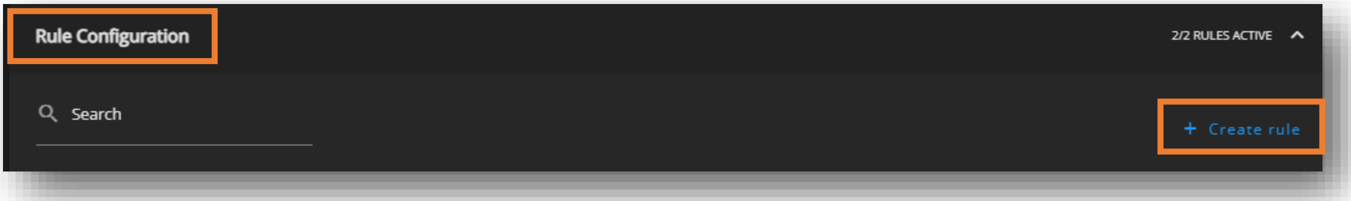
→ Select Devices located on the page menu

→ Use the Organization, Site and Search bar to locate the device you wish to edit

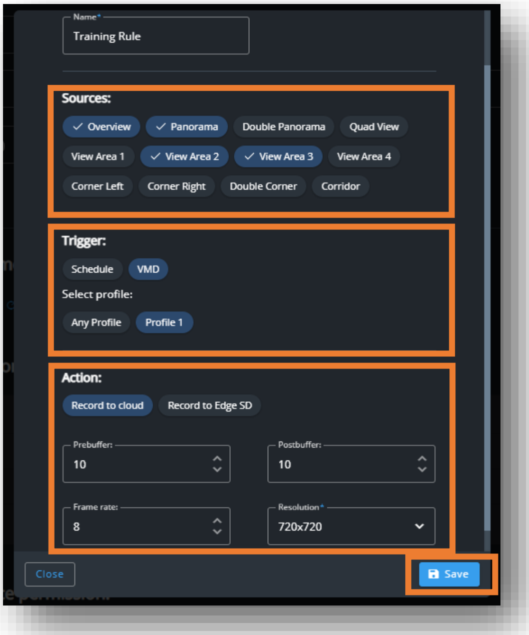
→ Select the Pen icon to edit the device

→ On the Edit Device page locate the Rule Configuration section and select Create Rule

→ Continue to next page →→→



Create a Rule



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 profile:

Any Profile Profile 1

Action:

Record to cloud Record to Edge SD

Prebuffer: 10

Postbuffer: 10

Frame rate: 8

Resolution* 720x720

Motion Based Rule: Record when motion is detected

→ Enter the Rule Name

→ Select the Schedule

→ Select the Source (Limited to multisensor and panoramic devices)

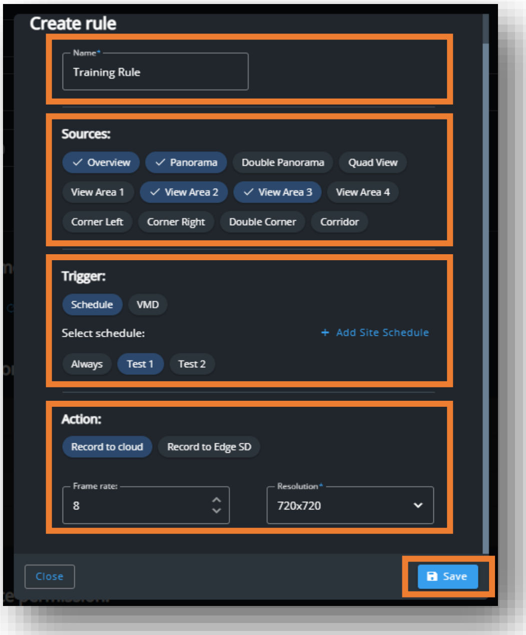
→ Select the Trigger
- VMD: Motion detection recording → Select profile: Profile 1 unless additional profile has been created

→ 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:

Always · Test 1 · Test 2

Action:
Record to cloud · Record to Edge SD

Frame rate: 8

Resolution*: 720x720

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

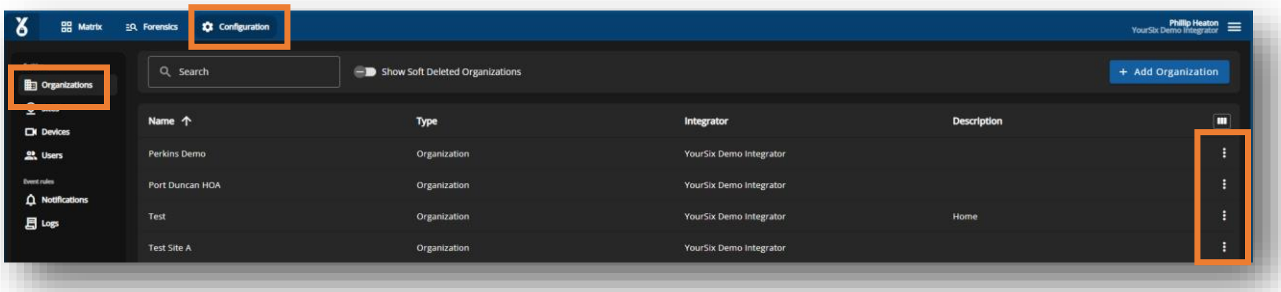
Organization Functions

- → 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.



Name ↑	Type	Integrator	Description
Perkins Demo	Organization	YourSix Demo Integrator	
Port Duncan HOA	Organization	YourSix Demo Integrator	
Test	Organization	YourSix Demo Integrator	Home
Test Site A	Organization	YourSix Demo Integrator	

→ Select Configuration located on the navigation bar

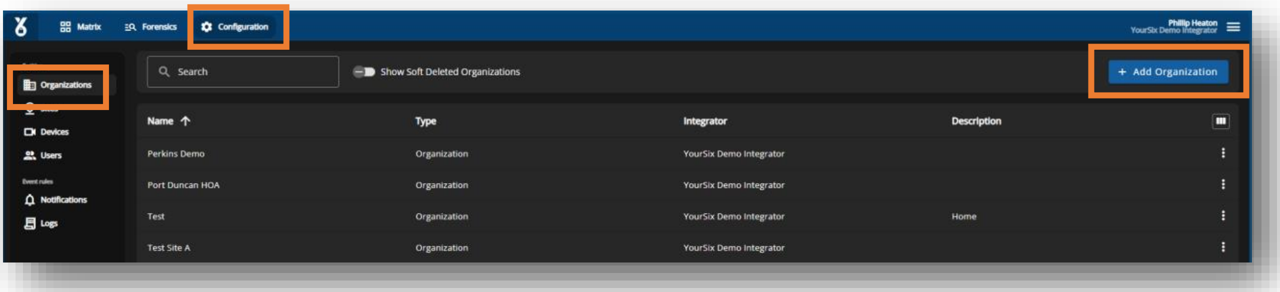
→ Select Organization located on the page menu

→ 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.



Name	Type	Integrator	Description
Perkins Demo	Organization	YourSix Demo Integrator	
Port Duncan HOA	Organization	YourSix Demo Integrator	
Test	Organization	YourSix Demo Integrator	Home
Test Site A	Organization	YourSix Demo Integrator	

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.

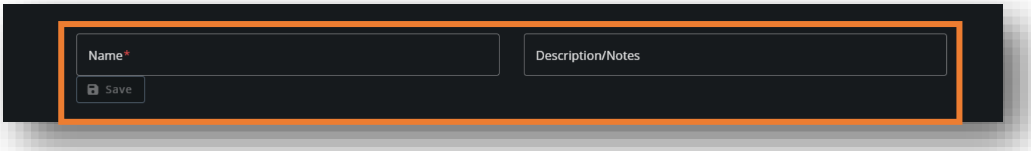
→ Select Configuration located on the navigation bar

→ 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



→ Name the Organization

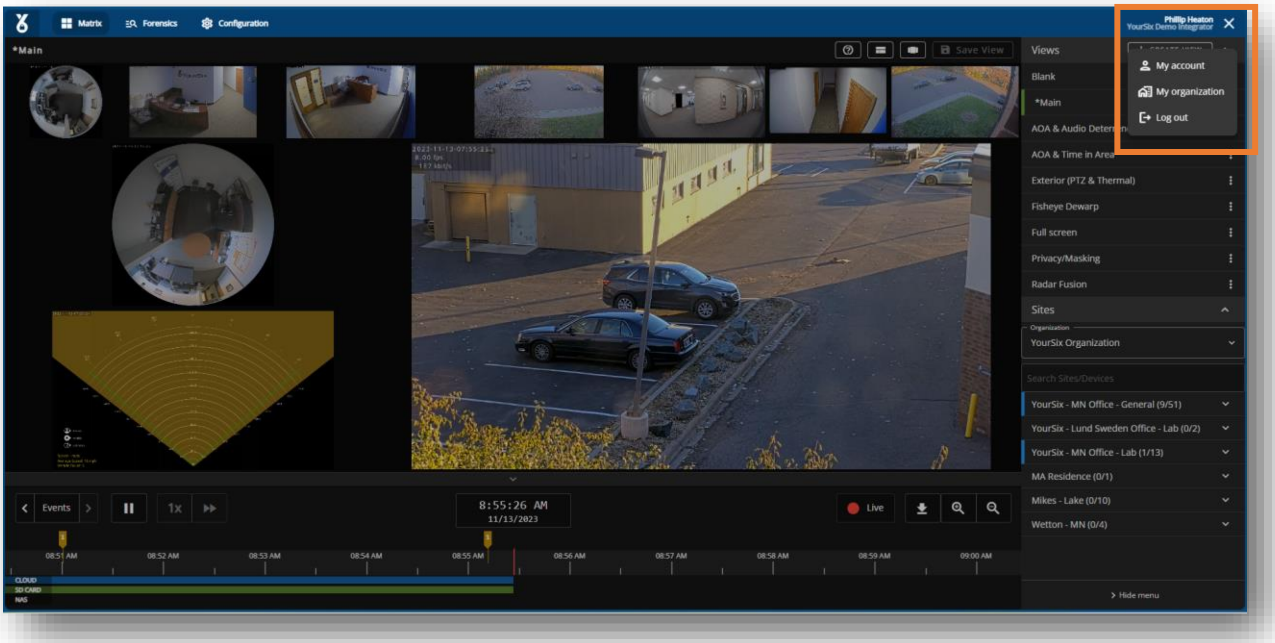
→ Add Description

→ 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.

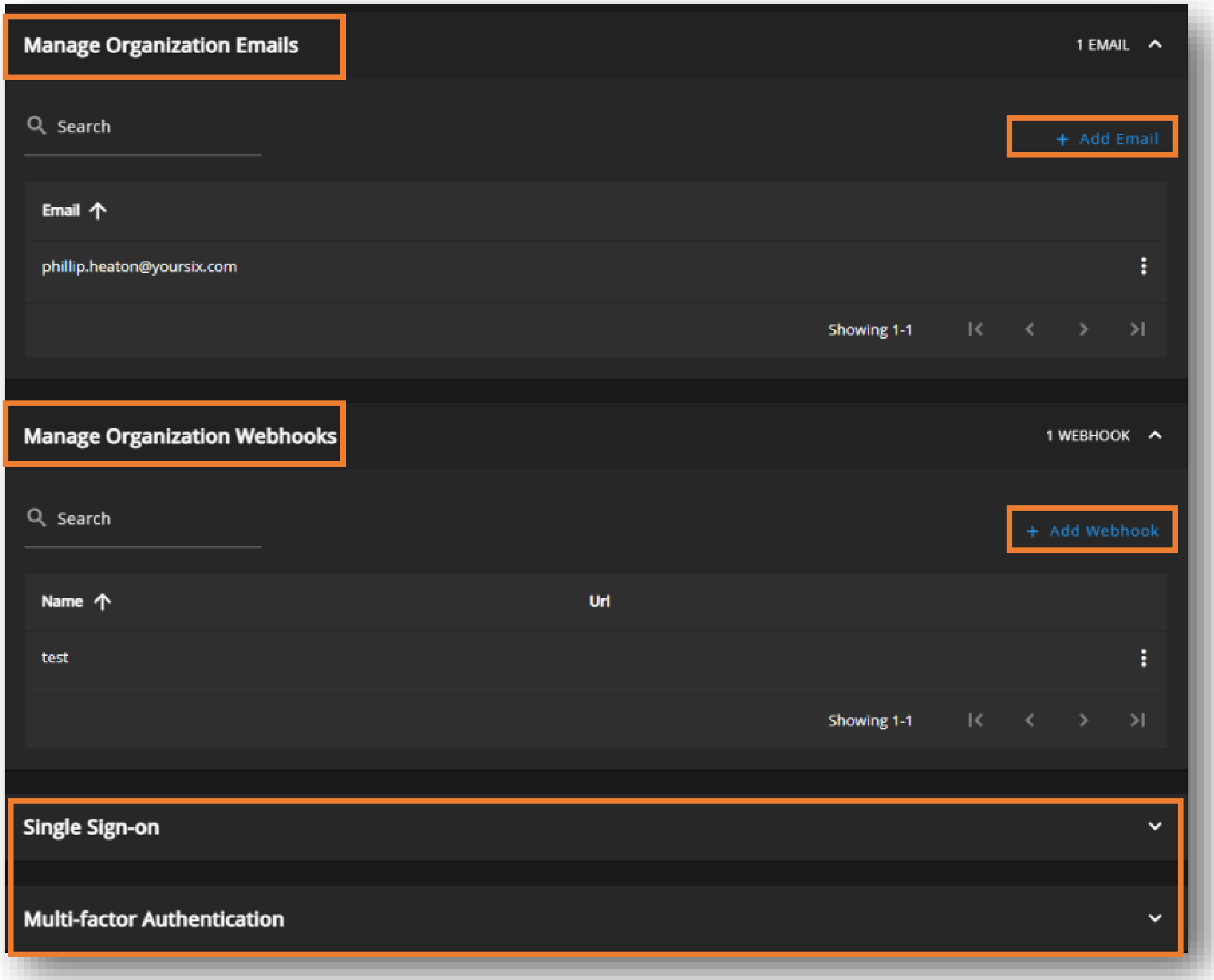


→ Locate the Hamburger Menu in the upper right corner

→ Select My Organization

→ Continue to next page →→→

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



Manage Organization Emails

1 EMAIL

Email ↑
phillip.heaton@yoursix.com

Showing 1-1

Manage Organization Webhooks

1 WEBHOOK

Name ↑	Url
test	

Showing 1-1

Single Sign-on

Multi-factor Authentication

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

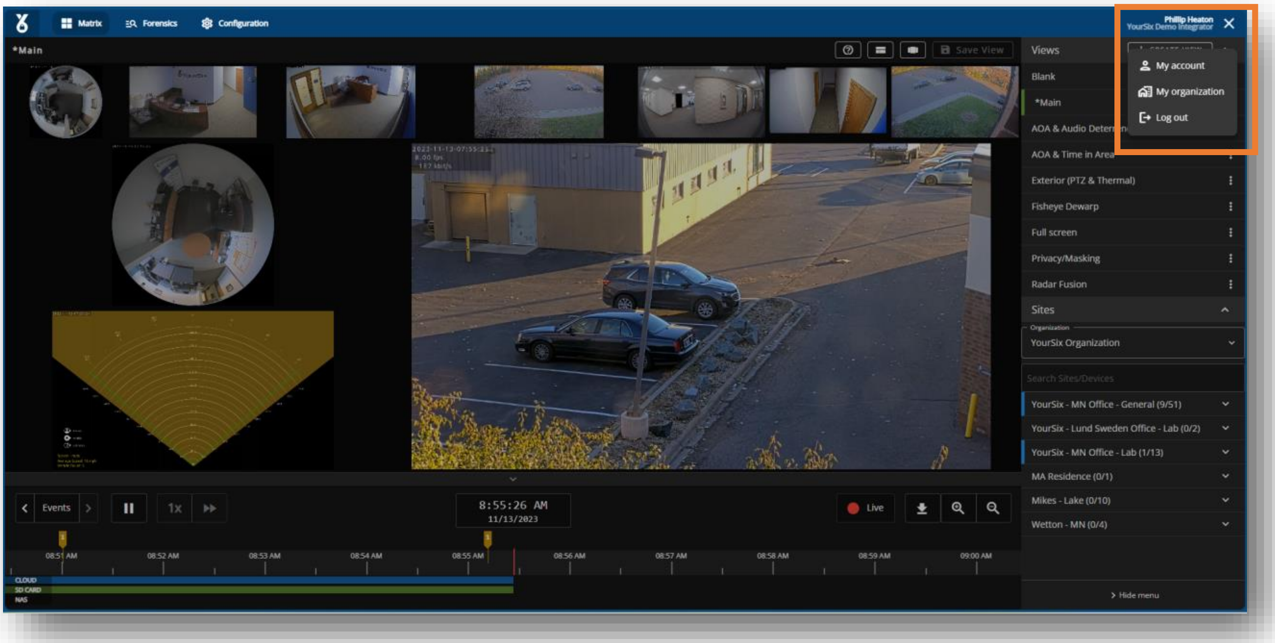
Single Sign On (SSO)

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

Notification Settings

Audience: All users

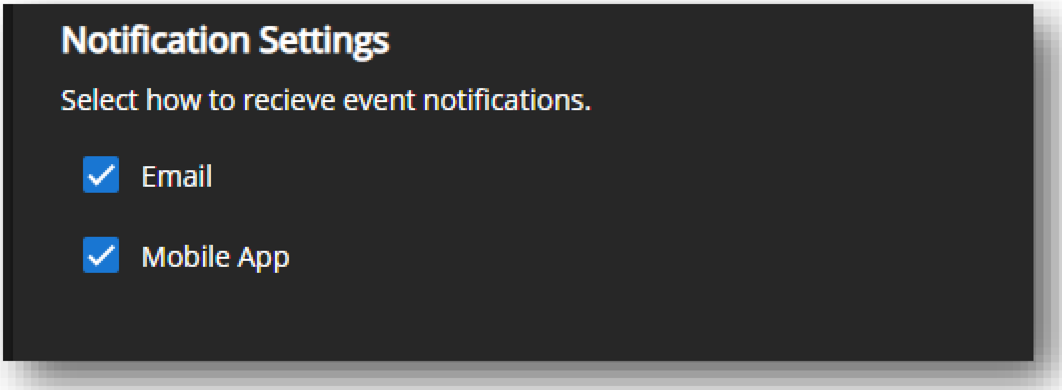
Objective: Manage Notification Settings.



→ Locate the Hamburger Menu in the upper right corner

→ Select My Account

→ Select how you wish to receive notifications



Notification Settings

Select how to recieve event notifications.

☑ Email

☑ Mobile App

Site Functions

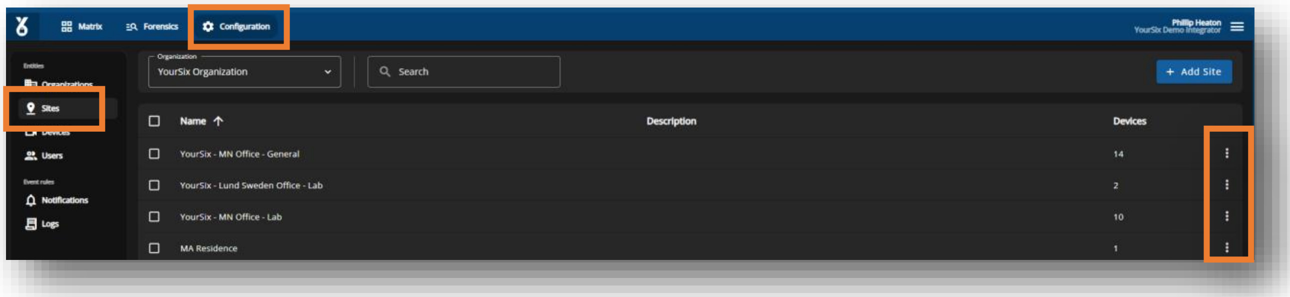
- Manage Sites
- Create Device Group
- Add Devices to Device Group
- Central Station
- Create Schedules
- Add Sites

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



Organization: YourSix Organization

Search

□	Name ↑	Description	Devices
□	YourSix - MN Office - General		14
□	YourSix - Lund Sweden Office - Lab		2
□	YourSix - MN Office - Lab		10
□	MA Residence		1

→ Select Configuration located on the navigation bar

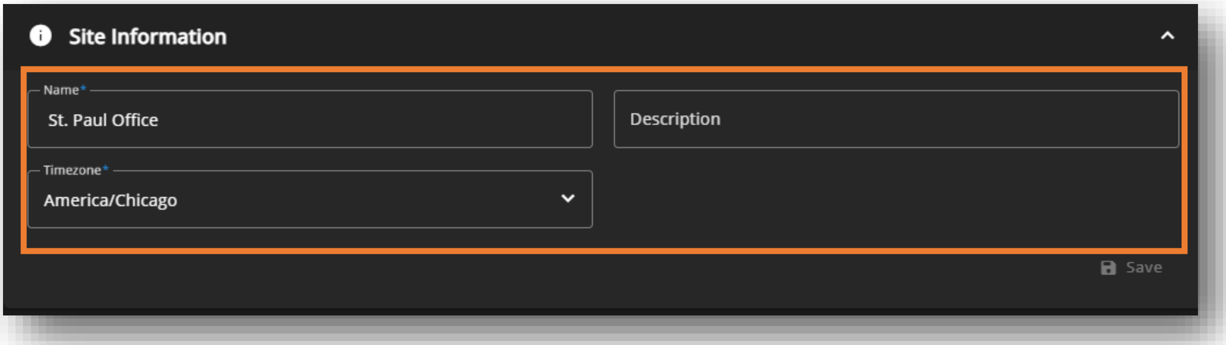
→ Select Sites located on the page menu

→ Use the Organization and Search function to locate the site you with to edit

→ Select the Pen icon to edit the site

→ Continue to next page →→→

Manage Sites



Site Information

Name*: St. Paul Office

Description

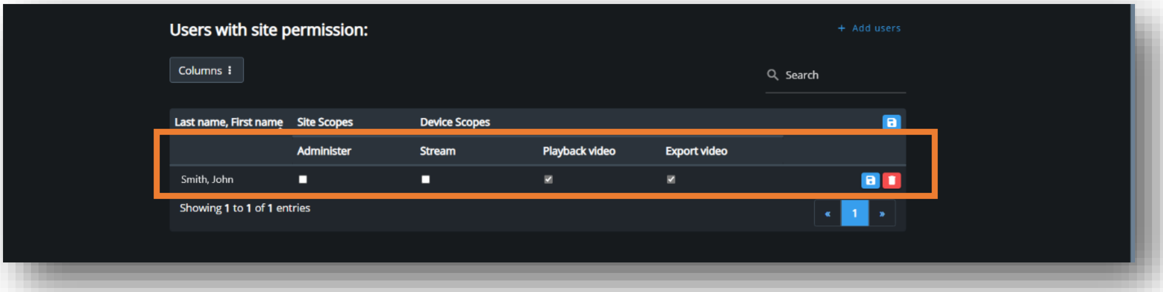
Timezone*: America/Chicago

Update Name, Description or Time Zone:

→ Edit Name or Description

→ Select appropriate Time Zone

→ Continue to next page →→→



Users with site permission:

Last name, First name	Site Scopes	Device Scopes		
	Administer	Stream	Playback video	Export video
Smith, John	□	□	☑	☑

Showing 1 to 1 of 1 entries

Edit Site User Permissions:

→ Locate the User With Site Permissions and expand

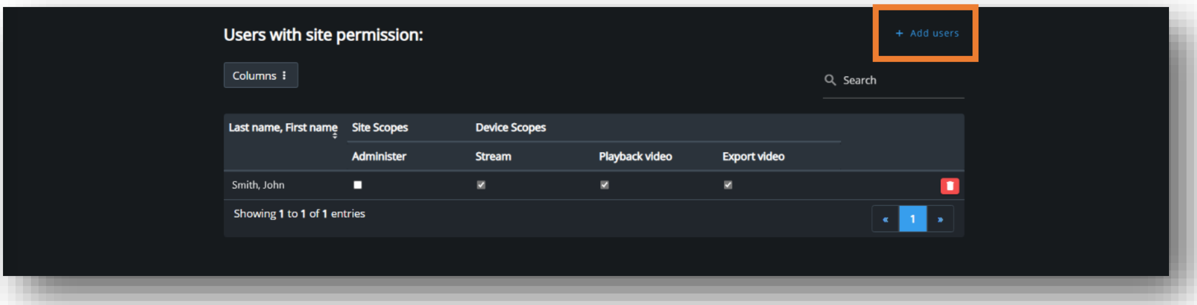
→ Select appropriate user Permissions

→ Select Save

→ Users can be deleted by selecting the Trash Can Icon

→ Continue to next page →→→

Manage Sites



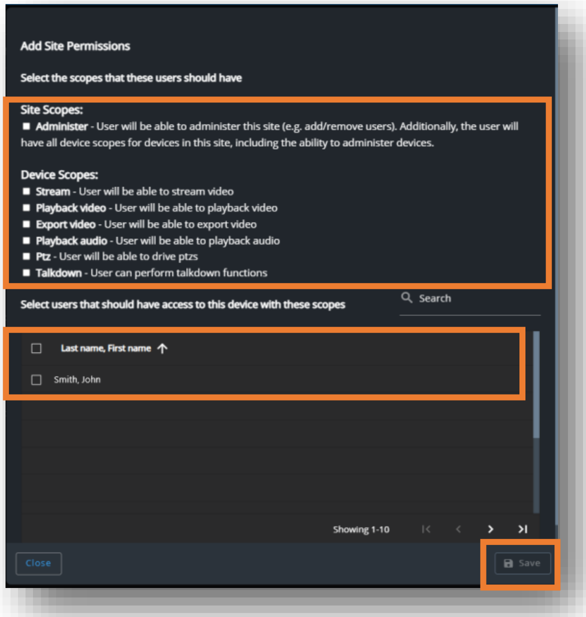
Users with site permission:

Last name, First name	Site Scopes	Device Scopes			
	Administer	Stream	Playback video	Export video	
Smith, John	■	☑	☑	☑	🗑

Showing **1** to **1** of **1** entries

Add a User to a Site:

→ Select Add User Permissions



Add Site Permissions

Select the scopes that these users should have

Site Scopes:
■ **Administer** - User will be able to administer this site (e.g. add/remove users). Additionally, the user will have all device scopes for devices in this site, including the ability to administer devices.

Device Scopes:
■ **Stream** - User will be able to stream video
■ **Playback video** - User will be able to playback video
■ **Export video** - User will be able to export video
■ **Playback audio** - User will be able to playback audio
■ **Ptz** - User will be able to drive ptzs
■ **Talkdown** - User can perform talkdown functions

Select users that should have access to this device with these scopes

□	Last name, First name ↑
□	Smith, John

Showing 1-10

→ 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

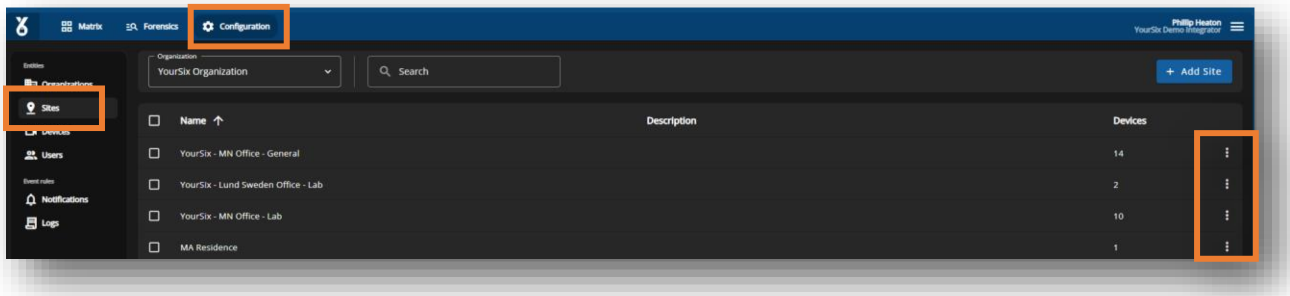
Create/Manage Device Group

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



□	Name ↑	Description	Devices
□	YourSix - MN Office - General		14
□	YourSix - Lund Sweden Office - Lab		2
□	YourSix - MN Office - Lab		10
□	MA Residence		1

→ Select Configuration located on the navigation bar

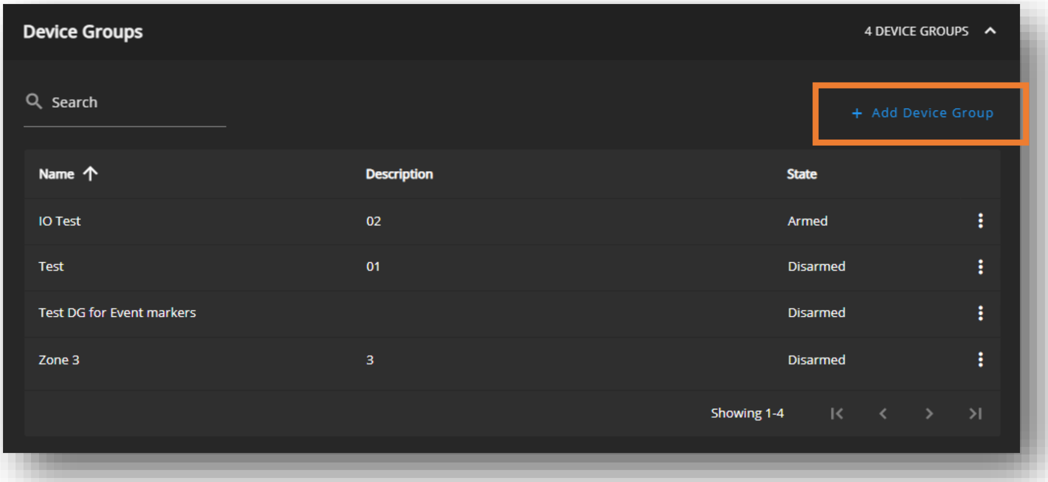
→ Select Sites located on the page menu

→ Use the Organization and Search function to locate the site you with to edit

→ Select the Pen icon to edit the site

→ Continue to next page →→→

Create Device Group



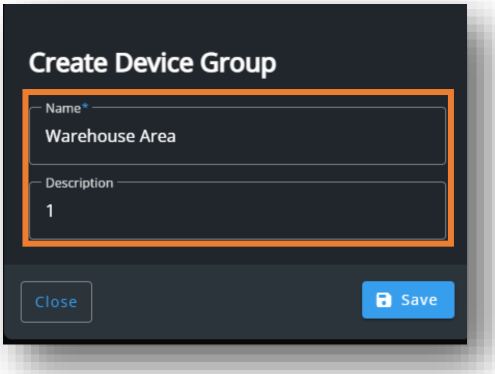
Device Groups

4 DEVICE GROUPS

Name	Description	State
IO Test	02	Armed
Test	01	Disarmed
Test DG for Event markers		Disarmed
Zone 3	3	Disarmed

Showing 1-4

Create Device Groups:



Create Device Group

Name*: Warehouse Area

Description: 1

→ 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

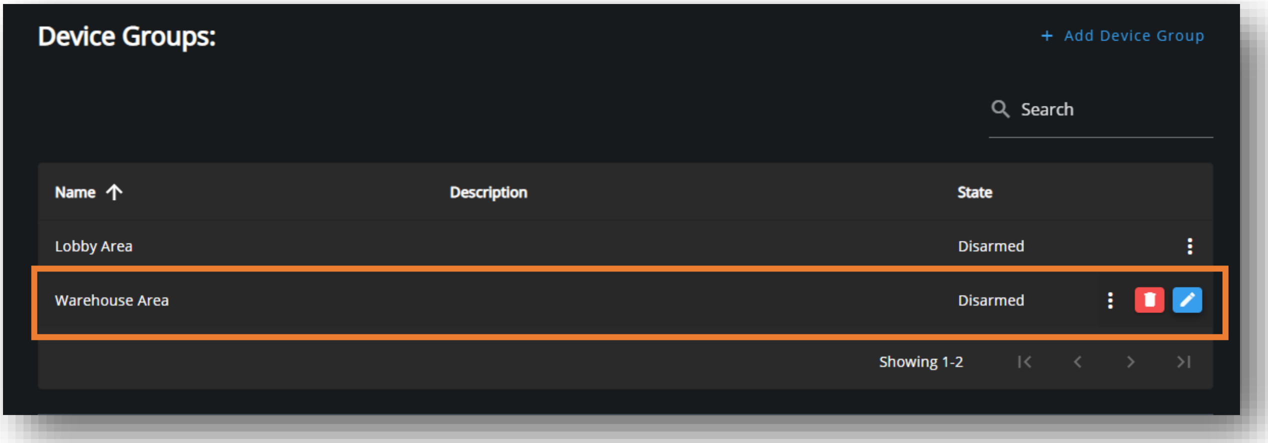
→ Within the popup menu, name the device Group and enter the description (zone number)

- 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



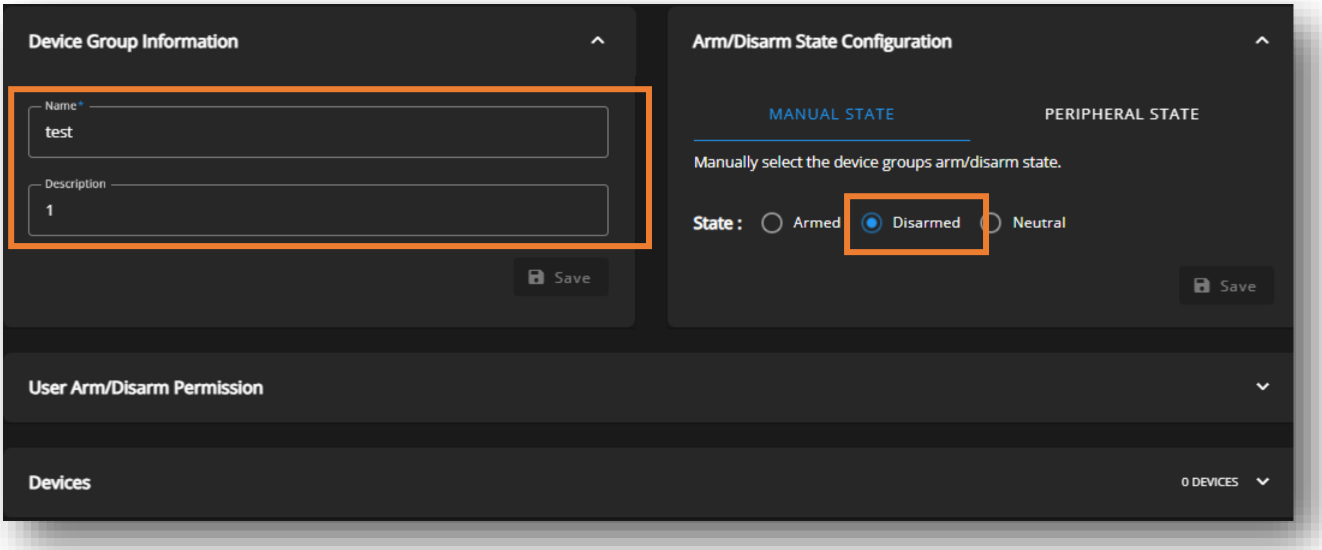
Device Groups:

Name ↑	Description	State
Lobby Area		Disarmed
Warehouse Area		Disarmed

Showing 1-2

→ 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



Device Group Information

Name*: test

Description: 1

Arm/Disarm State Configuration

Manually select the device groups arm/disarm state.

State : ○ Armed ● Disarmed ○ Neutral

User Arm/Disarm Permission

Devices — 0 DEVICES

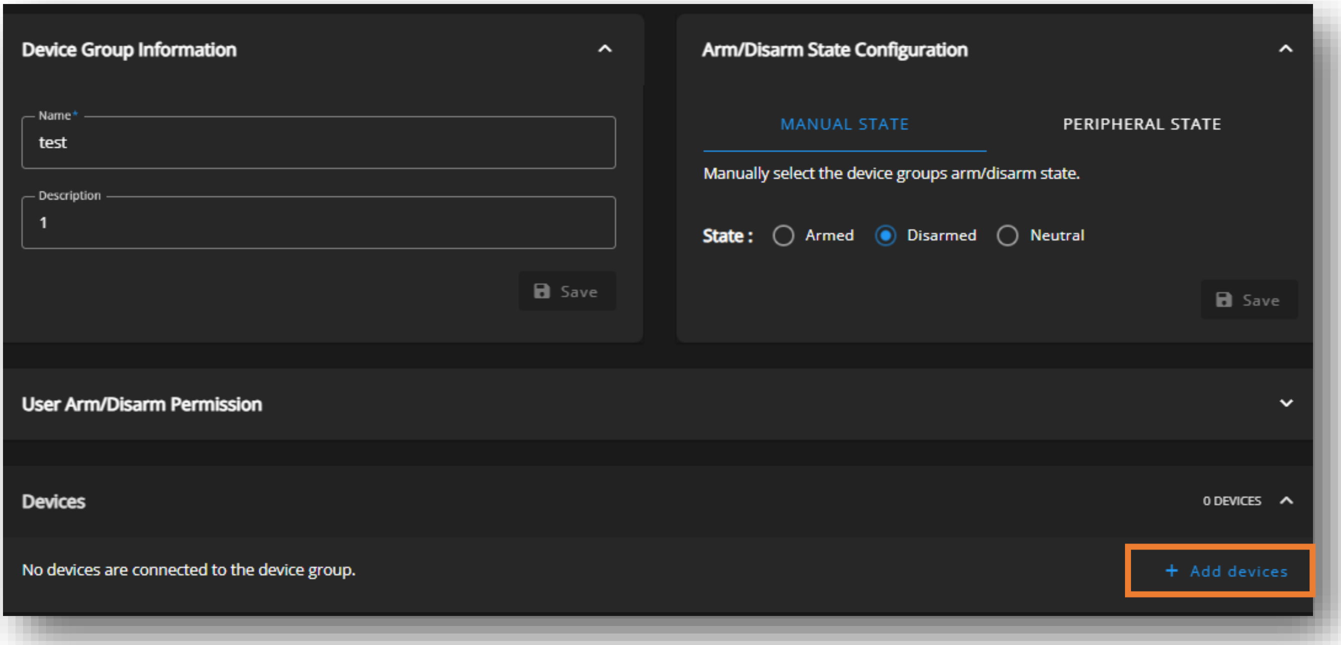
→ Within the edit device group page, confirm Name & Description (Zone Number)

→ 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

Devices — 0 DEVICES

No devices are connected to the device group.

+ Add devices

→ Select Add Devices located on the Device Group page

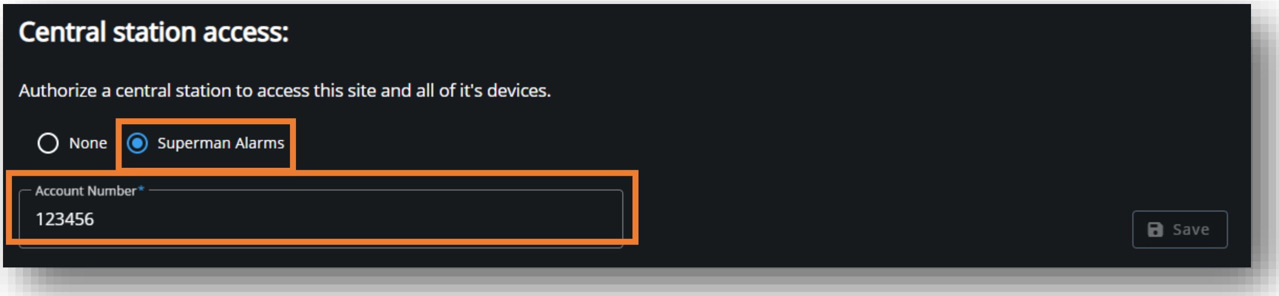
→ Within the popup select the devices to add to the group

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 it's devices.

○ None ● Superman Alarms

Account Number*: 123456

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

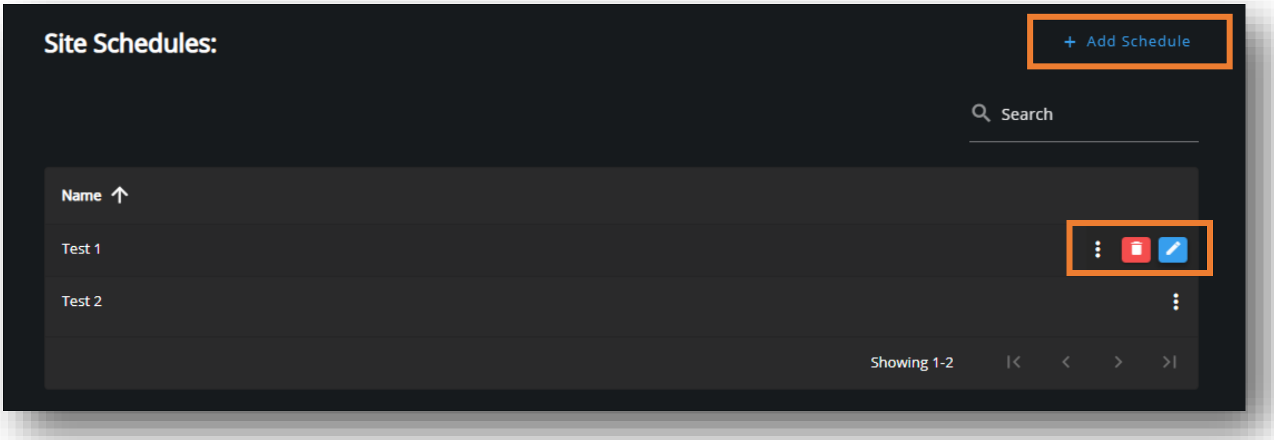
→ Select Save

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.



Site Schedules:

+ Add Schedule

Search

Name ↑
Test 1
Test 2

Showing 1-2

Edit Schedule:

→ Navigate to *Edit Site*

→ Select the Pen Icon to edit the existing schedules

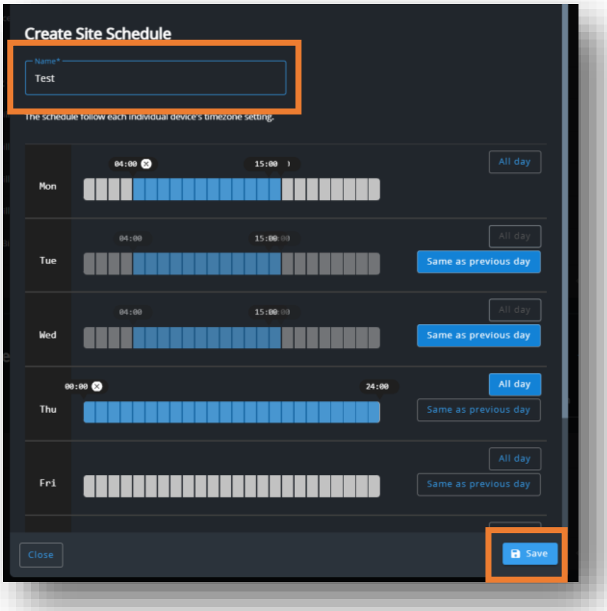
Add Schedule:

→ 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



Create Site Schedule

Name*: Test

The schedule follow each individual device's timezone setting.

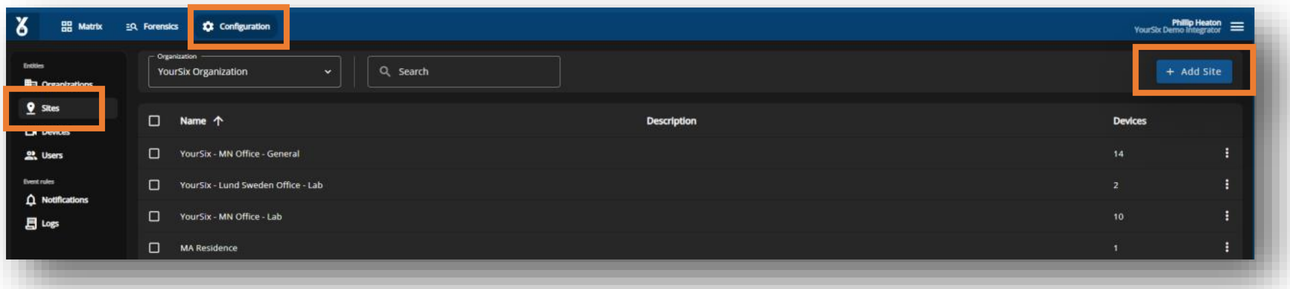
Add Sites

Audience: Integrator Super Admin, Integrator Admin, Integrator Tech

Objective: Create a new site under an organization.

Additional Resources:

- Add site video



□	Name ↑	Description	Devices
□	YourSix - MN Office - General		14
□	YourSix - Lund Sweden Office - Lab		2
□	YourSix - MN Office - Lab		10
□	MA Residence		1

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.

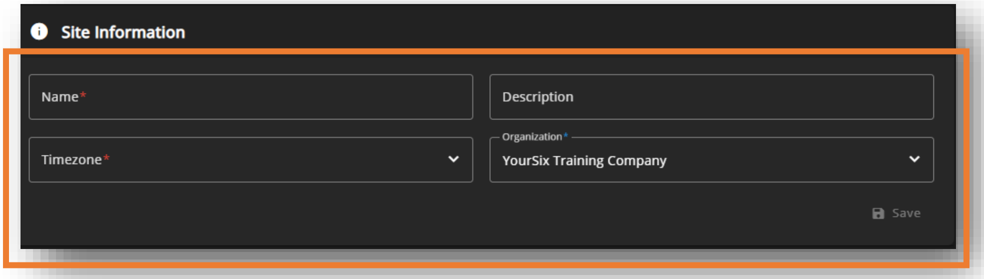
→ Select Configuration located on the navigation bar

→ 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

→ 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

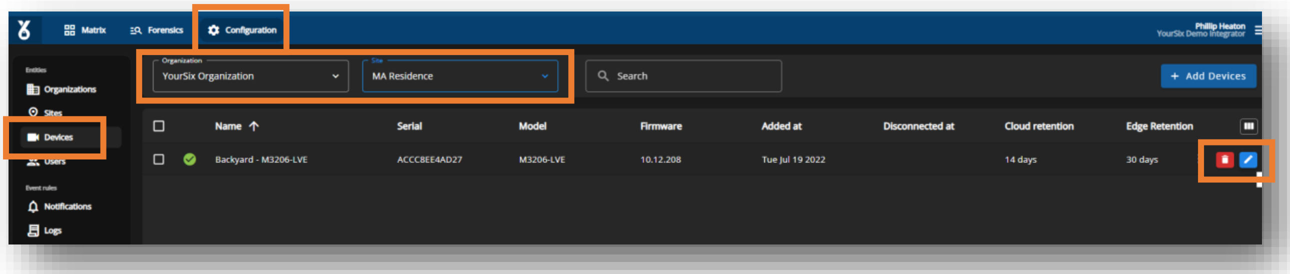
- → Manage Devices
- → Create a Rule
- → Add Devices

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



Organization: YourSix Organization

Site: MA Residence

□		Name ↑	Serial	Model	Firmware	Added at	Disconnected at	Cloud retention	Edge Retention	
□	✓	Backyard - M3206-LVE	ACCC8EE4AD27	M3206-LVE	10.12.208	Tue Jul 19 2022		14 days	30 days	

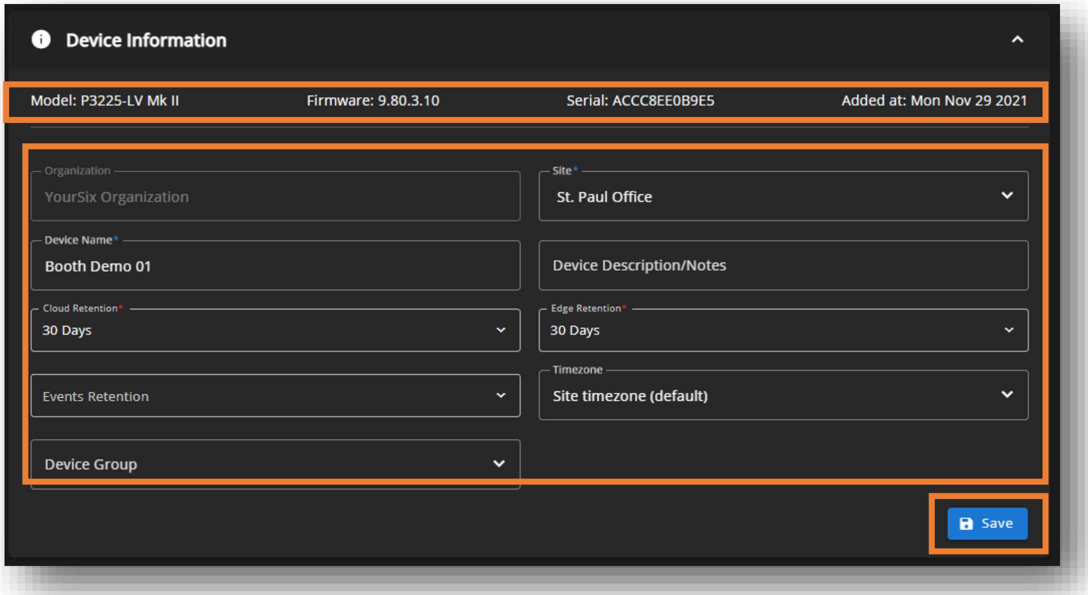
→ Select Configuration located on the navigation bar

→ Select Devices located on the page menu

→ Select Pen icon to edit the device

→ Continue to next page →→→

Manage Devices



Device Information

Model: P3225-LV Mk II Firmware: 9.80.3.10 Serial: ACCC8EE0B9E5 Added at: Mon Nov 29 2021

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)

Device Group

→ View Device Model, Firmware, Serial Number & Date Added at the top of the page

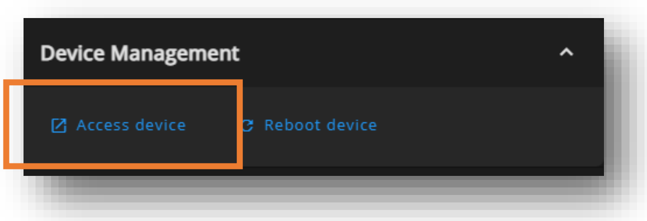
→ Edit the following information about the device:

- 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

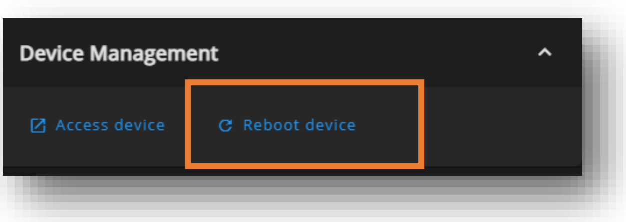


Access the Device Interface:

→ 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

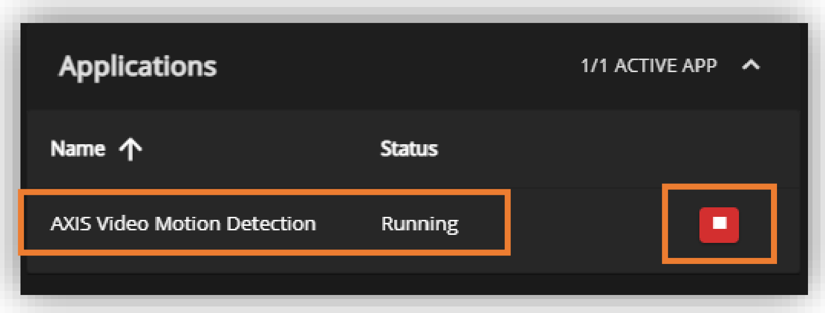


Reboot the Device:

→ Select Reboot Device to restart the device

→ Continue to next page →→→

Manage Devices



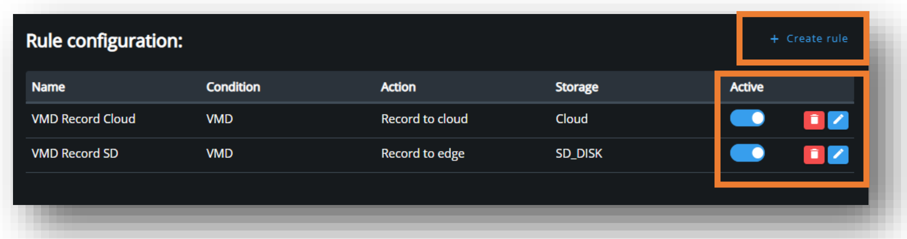
Applications 1/1 ACTIVE APP

Name	Status
AXIS Video Motion Detection	Running

Applications:

→ View current Status of Applications

→ Start or Stop the Application



Rule configuration:

Name	Condition	Action	Storage	Active
VMD Record Cloud	VMD	Record to cloud	Cloud	
VMD Record SD	VMD	Record to edge	SD_DISK	

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

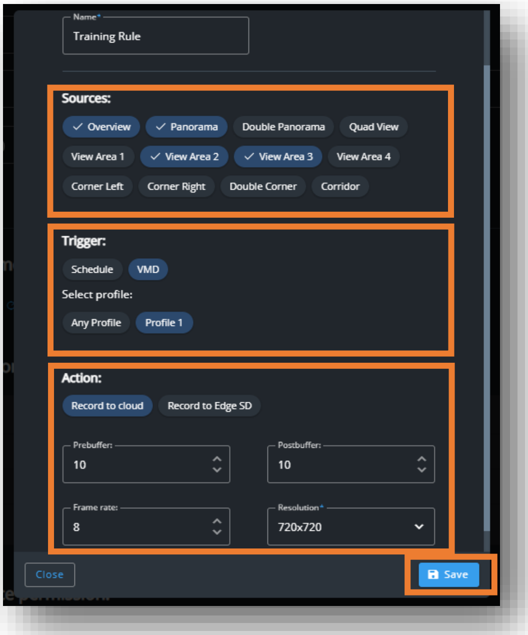
→ Select Create Rule to create a new rule for this device

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



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 profile: Any Profile, [✓ Profile 1]

Action: [✓ Record to cloud], Record to Edge SD

Prebuffer: 10

Postbuffer: 10

Frame rate: 8

Resolution*: 720x720

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

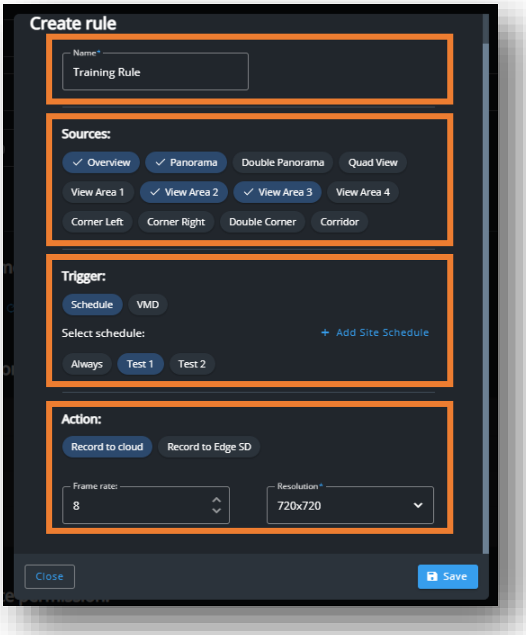
→ Select the Source (Limited to Multi-Sensor and Panoramic Devices)

→ 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



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:

Always, Test 1, Test 2

Action:

Record to cloud, Record to Edge SD

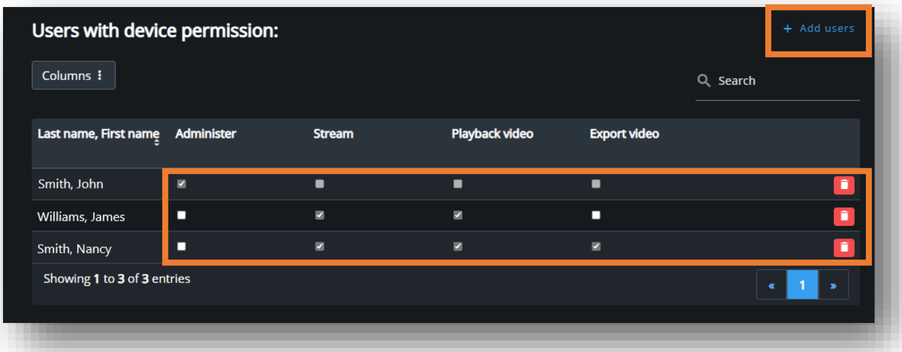
Frame rate: 8

Resolution* 720x720

Additional Device Management

Audience: Integrator Super Admin, Integrator Admin, Integrator Tech

Objective: Edit new & existing devices.



Users with device permission:

Last name, First name	Administer	Stream	Playback video	Export video	
Smith, John	☑	□	□	□	🗑
Williams, James	□	☑	☑	□	🗑
Smith, Nancy	□	☑	☑	☑	🗑

Showing **1** to **3** of **3** entries

Device Permissions:

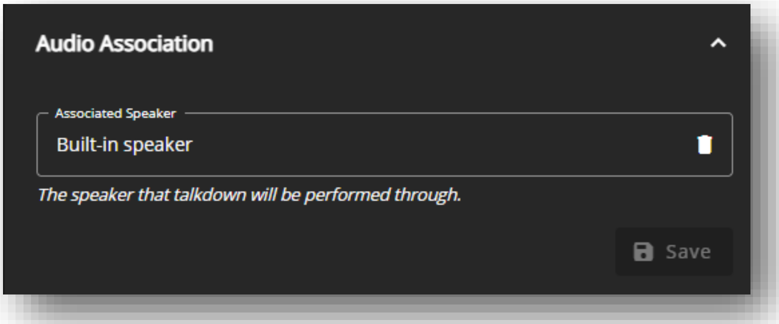
→ View Existing Device Permissions

- 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

Associated Speaker

Built-in speaker

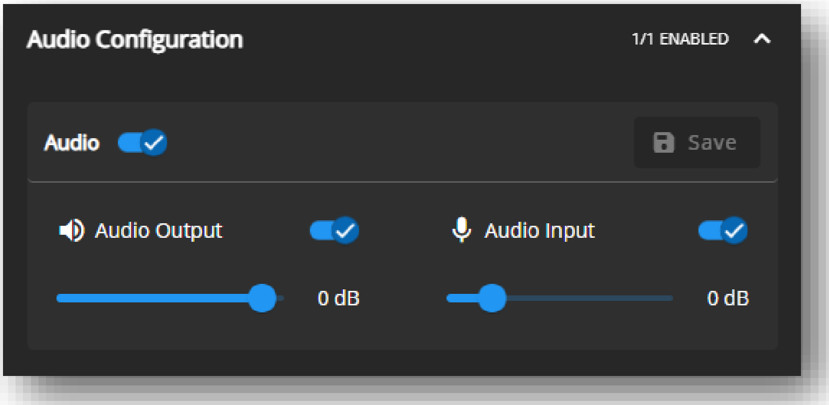
The speaker that talkdown will be performed through.

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



Audio Configuration

1/1 ENABLED

Audio

Audio Output 0 dB

Audio Input 0 dB

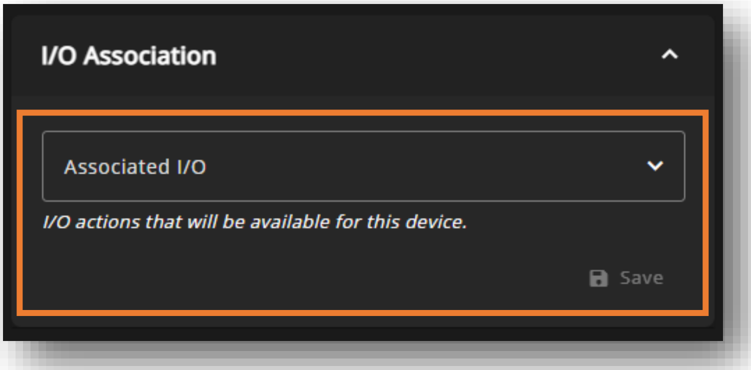
Edit Audio Configuration:

→ 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

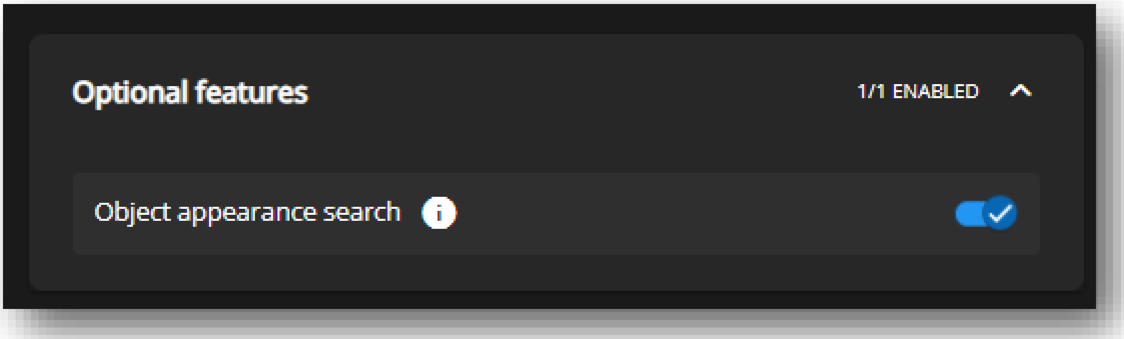


I/O actions that will be available for this device.

I/O Association:

→ Select Associated I/O and select the desired information

→ Select Save



Option Features

→ Select and enable the desired Optional feature

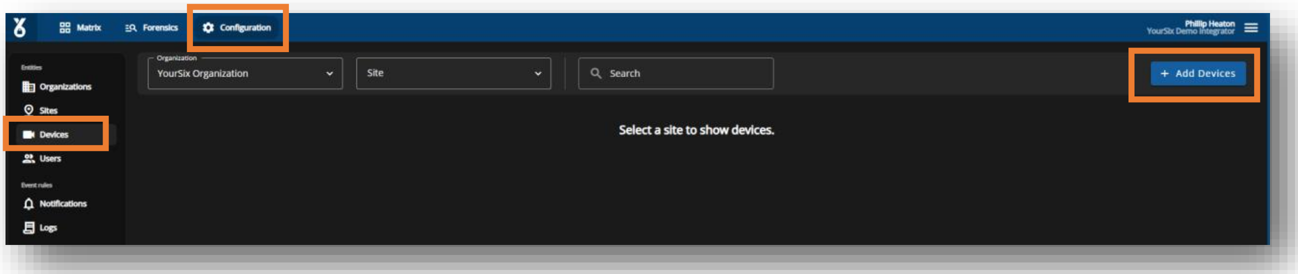
Add Devices

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



Select a site to show devices.

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

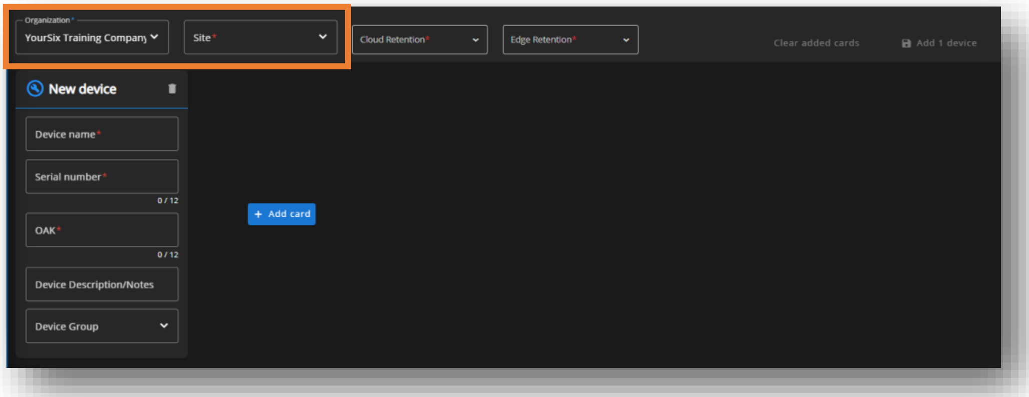
→ Select Configuration located on the navigation bar

→ Select Devices located on the page menu

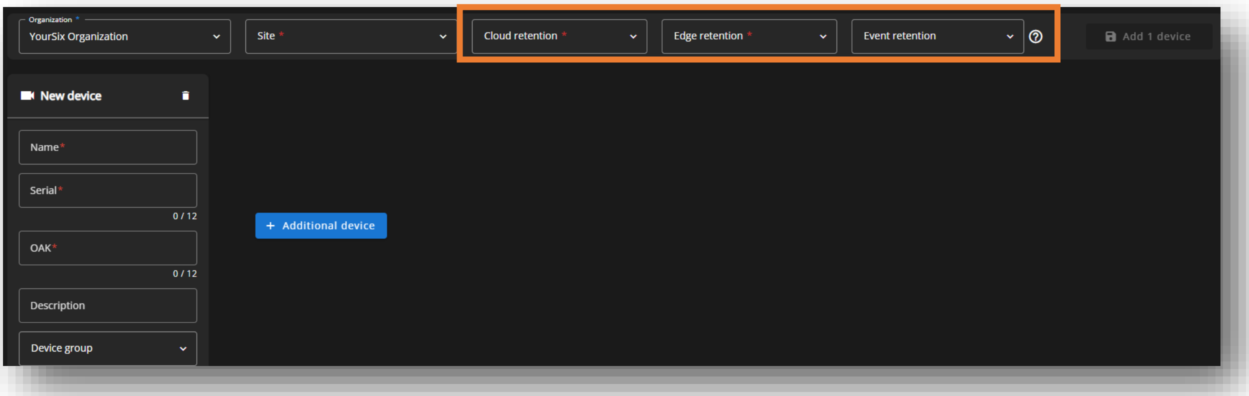
→ Select Add Devices located in the upper right portion of the screen

→ Continue to next page →→→

Add Devices



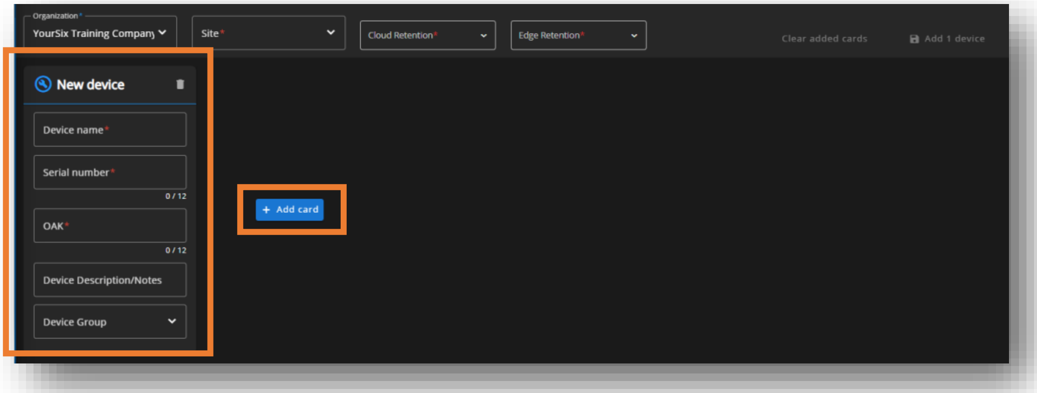
→ Select the Organization and Site that the device(s) will be added to



→ Select the Cloud Retention, Edge Retention, Event Retention for the device(s)
→ Event Retention: Amount of time for which events (triggers) will be logged by the platform. This does not affect anything with footage/recordings.

→ Continue to next page →→→

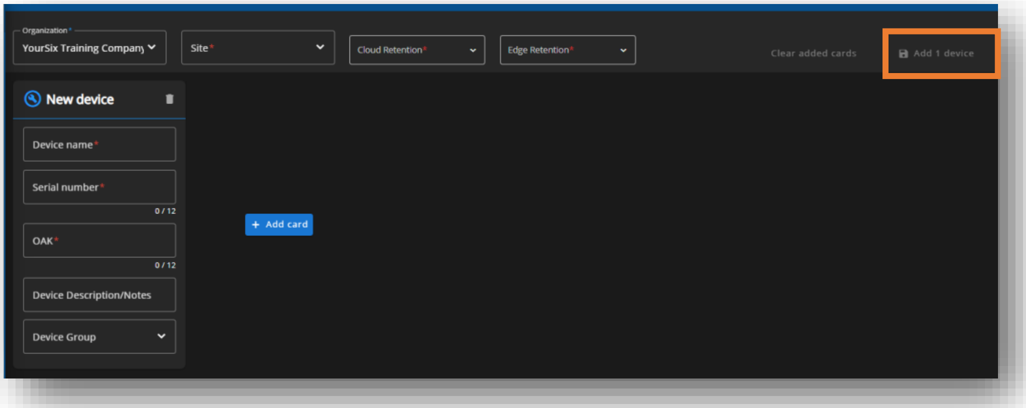
Add Devices



→ 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

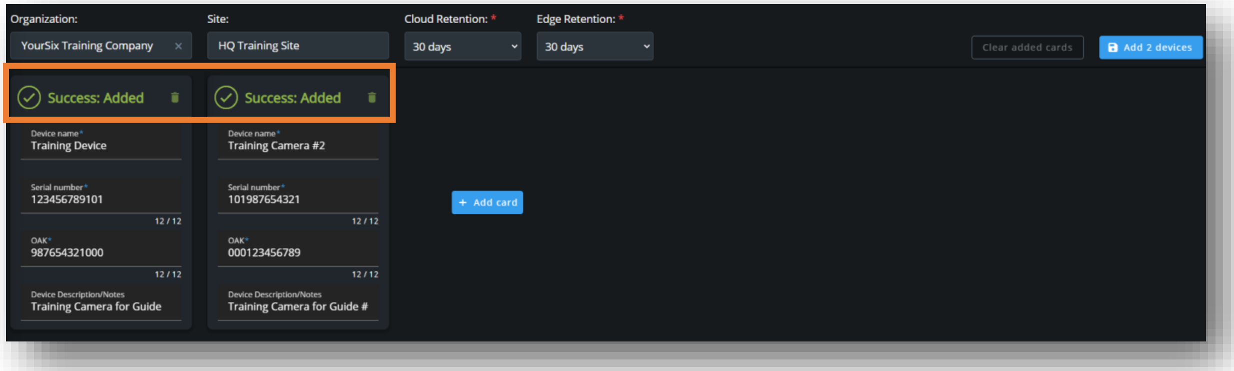
→ If you are adding multiple devices to the same site with the same cloud and edge retention, you can select the +Add card button. This will allow you to mass upload devices.



→ Select Add "#" devices button

→ Continue to next page →→→

Add Devices



Organization: YourSix Training Company

Site: HQ Training Site

Cloud Retention: * 30 days

Edge Retention: * 30 days

✓ Success: Added

Device name* Training Device

Serial number* 123456789101 12 / 12

OAK* 987654321000 12 / 12

Device Description/Notes Training Camera for Guide

✓ Success: Added

Device name* Training Camera #2

Serial number* 101987654321 12 / 12

OAK* 000123456789 12 / 12

Device Description/Notes Training Camera for Guide #

→ 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

Access Control Overview

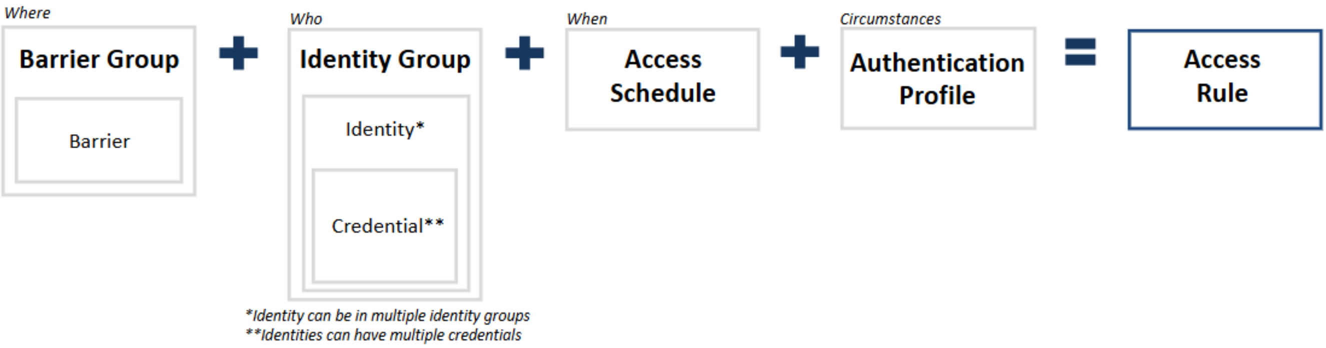
The addition of Access Control to the YourSixOS platform marks a significant advancement in cloud-native physical security solutions. This enhancement integrates Access Control into the YourSixOS cloud-native platform, offering customers a unified solution accessible from any device, anywhere. By bringing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



*Identity can be in multiple identity groups
**Identities can have multiple credentials

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.

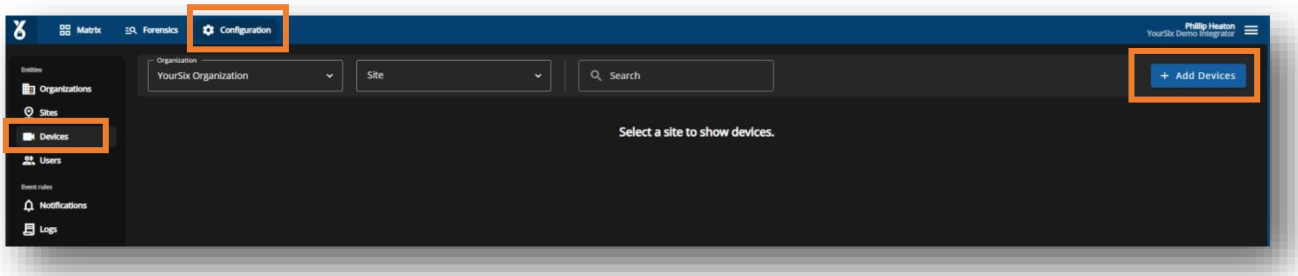
Add Controller

Audience: Integrator Super Admin, Integrator Admin, Integrator Tech

Objective: Add a controller to a site.

Additional Resources:

- Adding a device videos



Select a site to show devices.

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

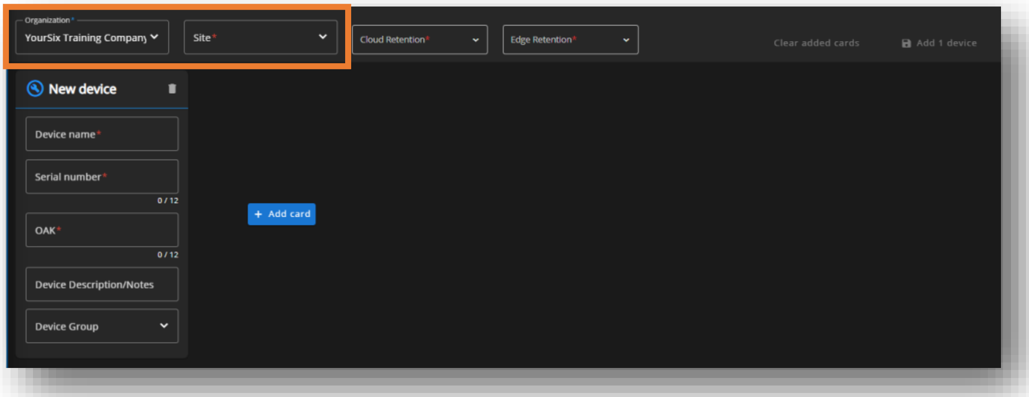
→ Select Configuration located on the navigation bar

→ Select Devices located on the page menu

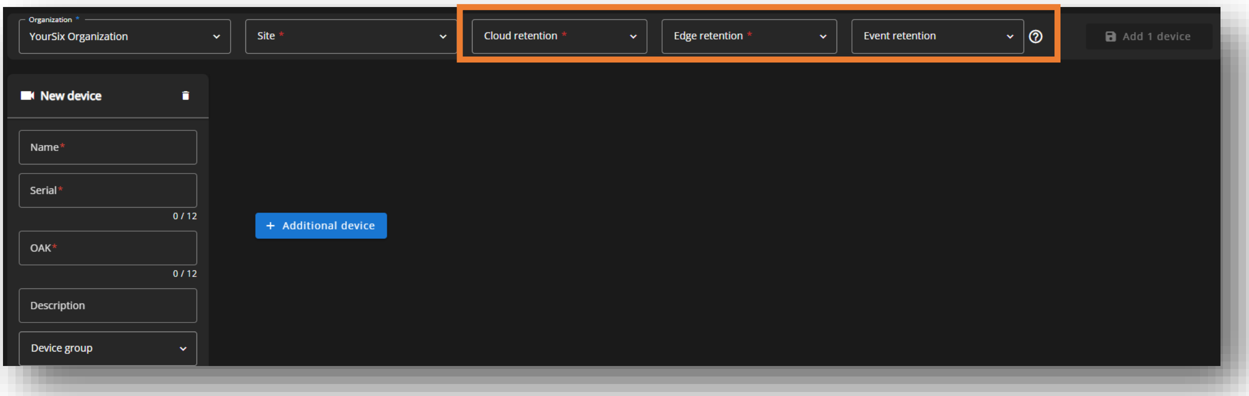
→ Select Add devices located in the upper right portion of the screen

→ Continue to next page →→→

Add Controller


Organization *
YourSix Training Company
Site *
Cloud Retention *
Edge Retention *
Clear added cards
Add 1 device
New device
Device name *
Serial number *
0 / 12
OAK *
0 / 12
Device Description/Notes
Device Group
+ Add card

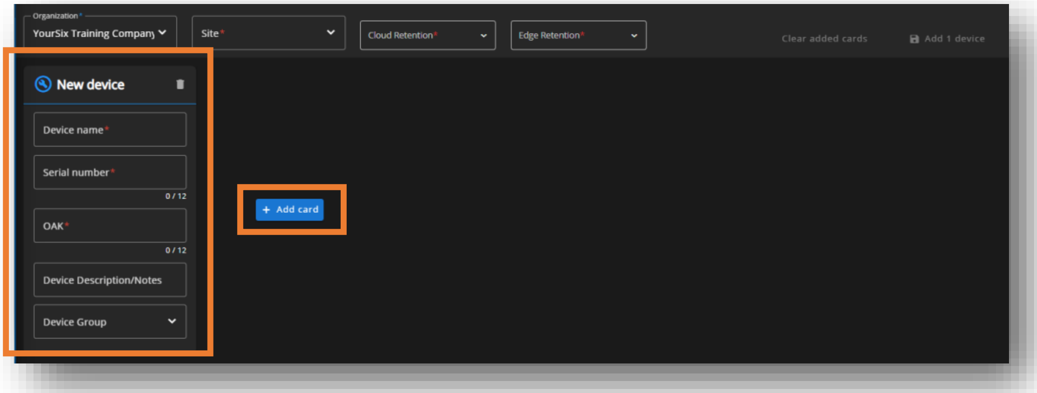
→ Select the Organization and Site that the device(s) will be added to


Organization *
YourSix Organization
Site *
Cloud retention *
Edge retention *
Event retention
Add 1 device
New device
Name *
Serial *
0 / 12
OAK *
0 / 12
Description
Device group
+ Additional device

→ Set the Cloud Retention, Edge Retention, Event Retention for the device(s)
→ Event Retention: Amount of time for which events will be logged by the platform. This includes events such as “access granted” and “access denied” as well as alarms such as “barrier forced” and “open too long”
→ Cloud and Edge retention should be set to the lowest option since no video is being stored.

→ Continue to next page →→→

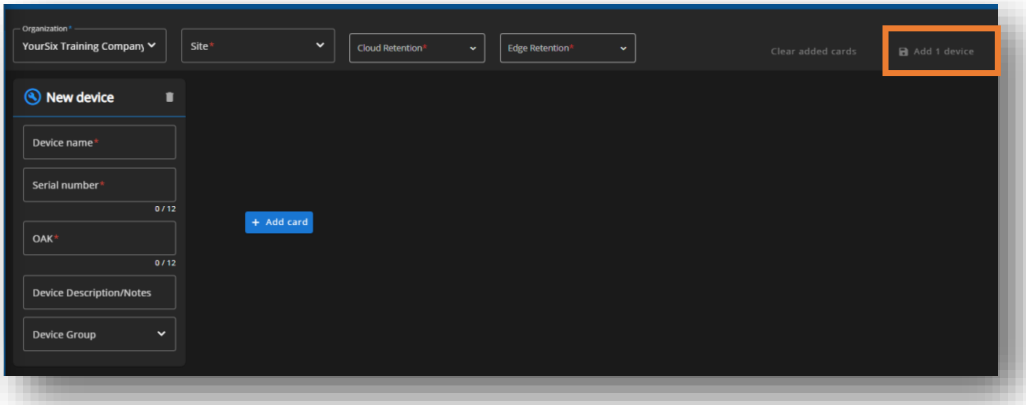
Add Controller



→ 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

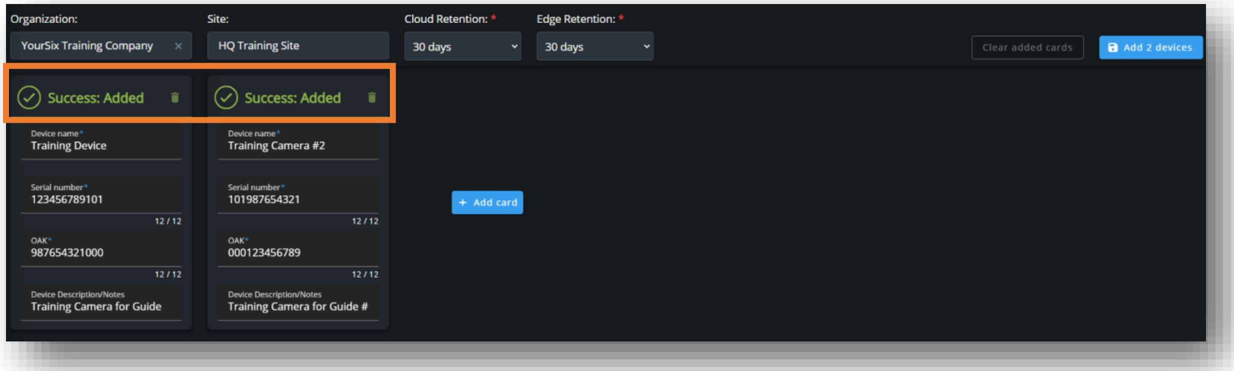
→ If you are adding multiple devices to the same site with the same cloud and edge retention, you can select the +Add card button. This will allow you to mass upload devices.



→ Select Add "#" devices button

→ Continue to next page →→→

Add Controller



Organization: YourSix Training Company

Site: HQ Training Site

Cloud Retention: * 30 days

Edge Retention: * 30 days

Success: Added

Device name* Training Device

Serial number* 123456789101 12 / 12

OAK* 987654321000 12 / 12

Device Description/Notes Training Camera for Guide

Success: Added

Device name* Training Camera #2

Serial number* 101987654321 12 / 12

OAK* 000123456789 12 / 12

Device Description/Notes Training Camera for Guide #

→ 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

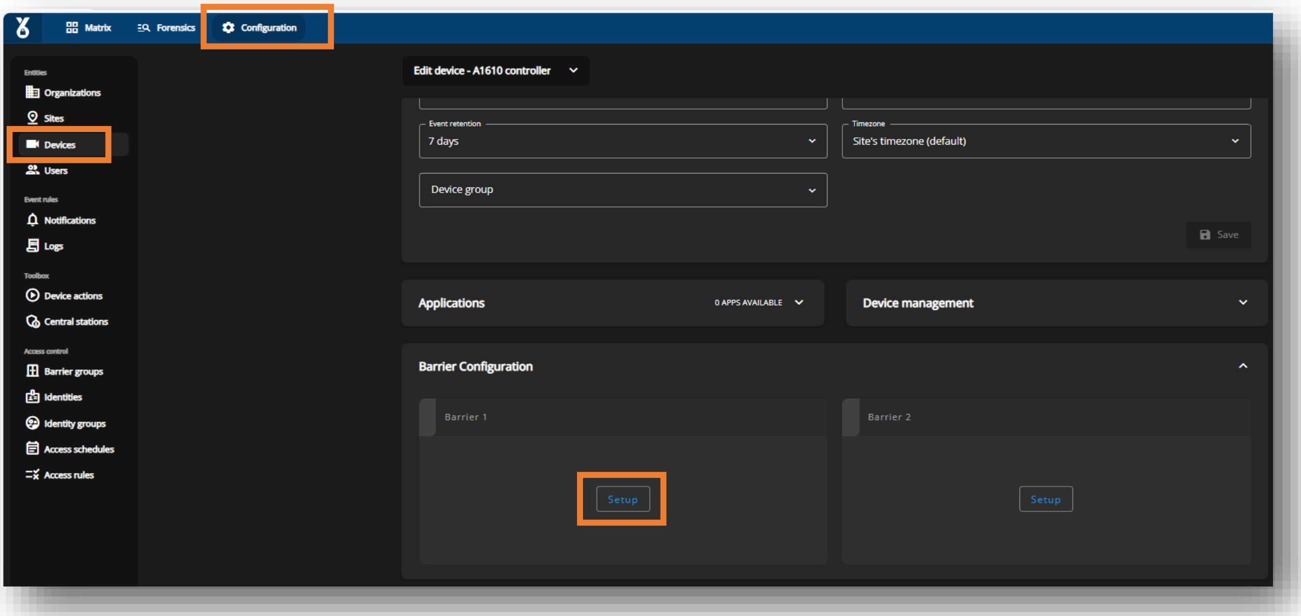
Add Barrier

Audience: Integrator Super Admin, Integrator Admin

Objective: Add a barrier to a controller.

Additional Resources:

- Access control configuration videos



Event retention: 7 days

Timezone: Site's timezone (default)

Device group

→ Select Configuration located on the navigation bar

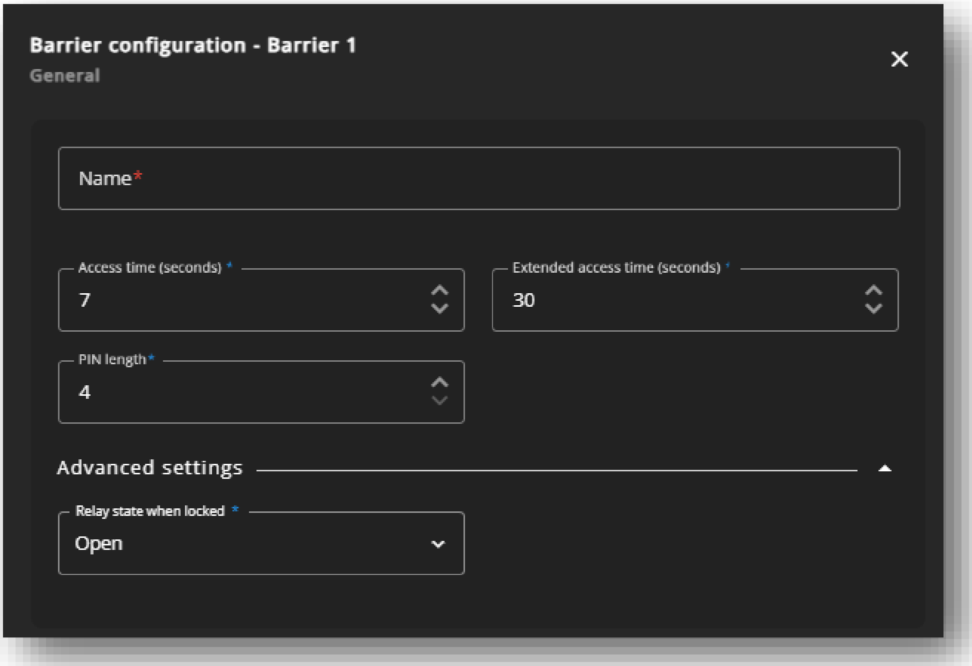
→ Select Devices located on the page menu

→ 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

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

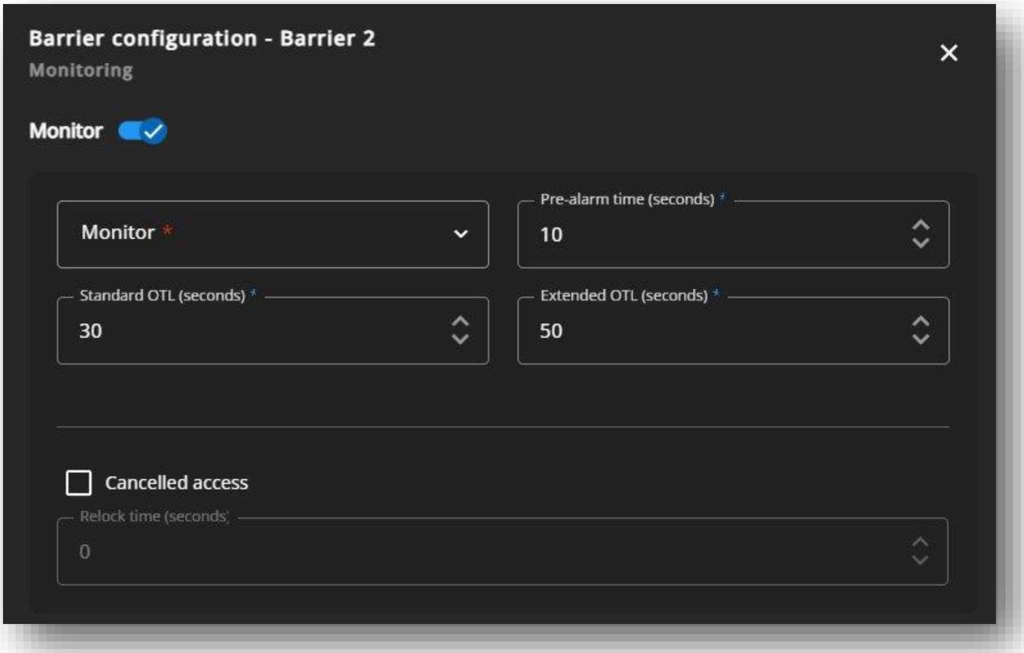
→ Pin Length: Required length of the pin

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

□ Cancelled 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

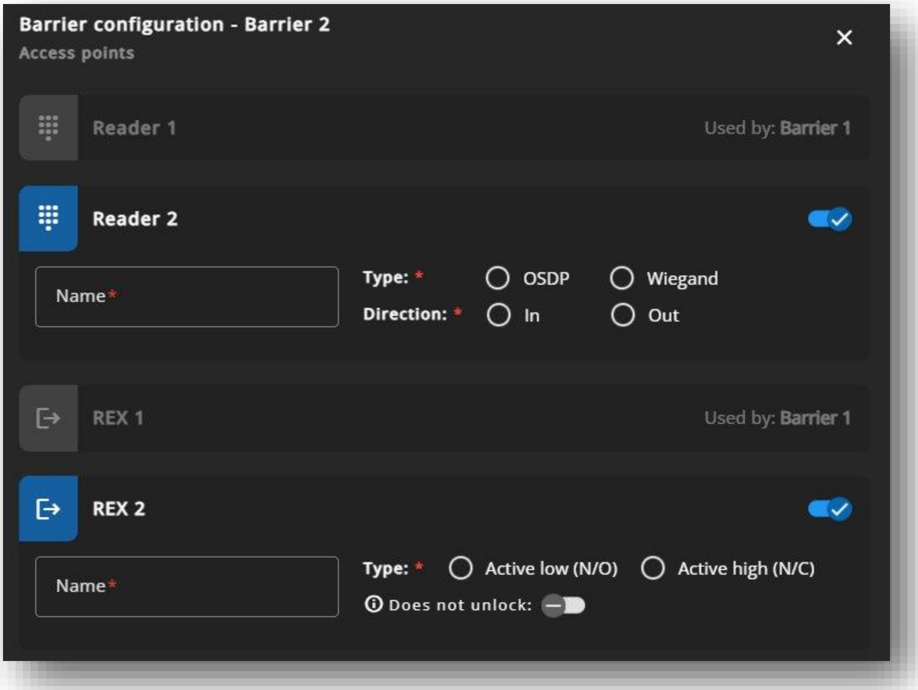
→ Extended OTL: the number of seconds between barrier opening and the barrier open too long event when using extended access

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



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

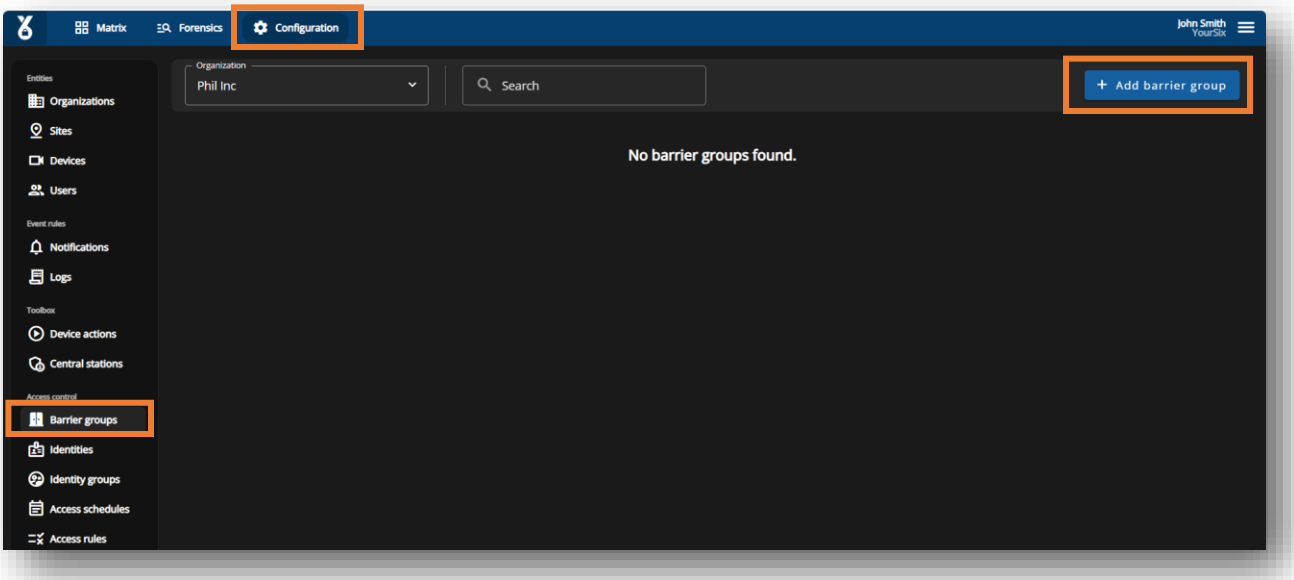
Add Barrier Groups

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



No barrier groups found.

→ 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

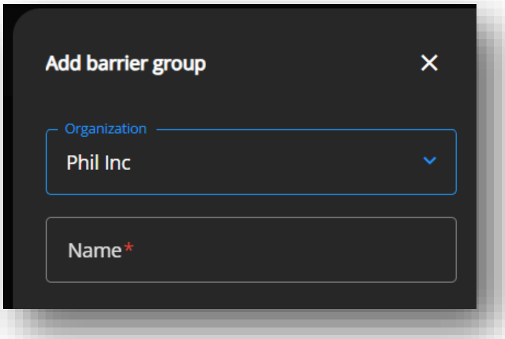
Add Barrier Groups

Add barrier group

→ Confirm the Organization

→ Name the Barrier group

→ Select Save at the bottom of the window



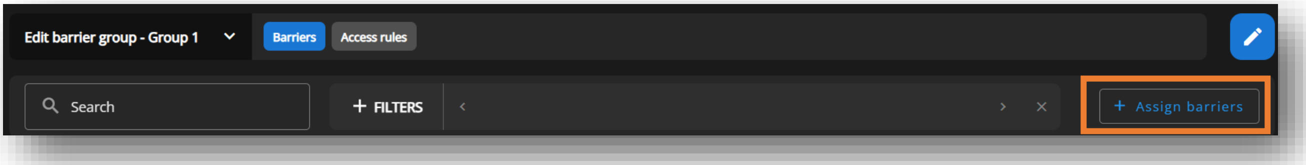
Add barrier group

Organization: Phil Inc

Name*

Assign barriers to the group

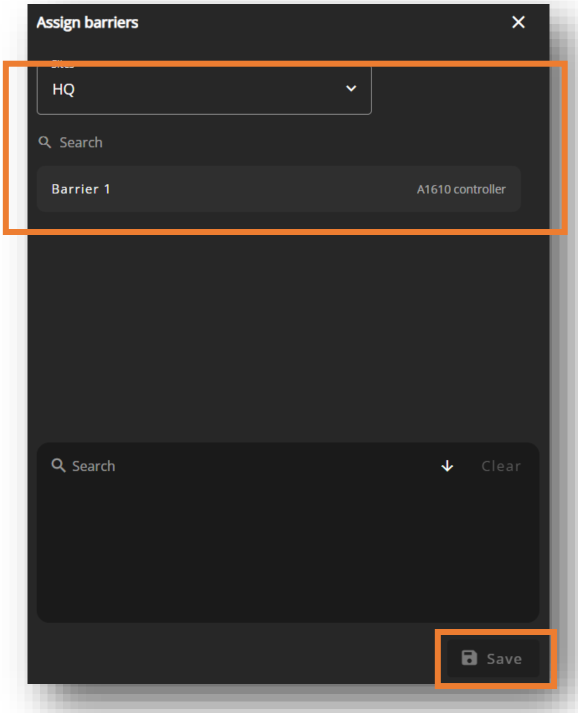
→ After selecting save on the add barrier group window (Previous section above), select Assign barriers in the upper right corner



Edit barrier group - Group 1

→ On the popout menu, select the Site and Barrier

→ Confirm selection and select Save



Assign barriers

HQ

Barrier 1 A1610 controller

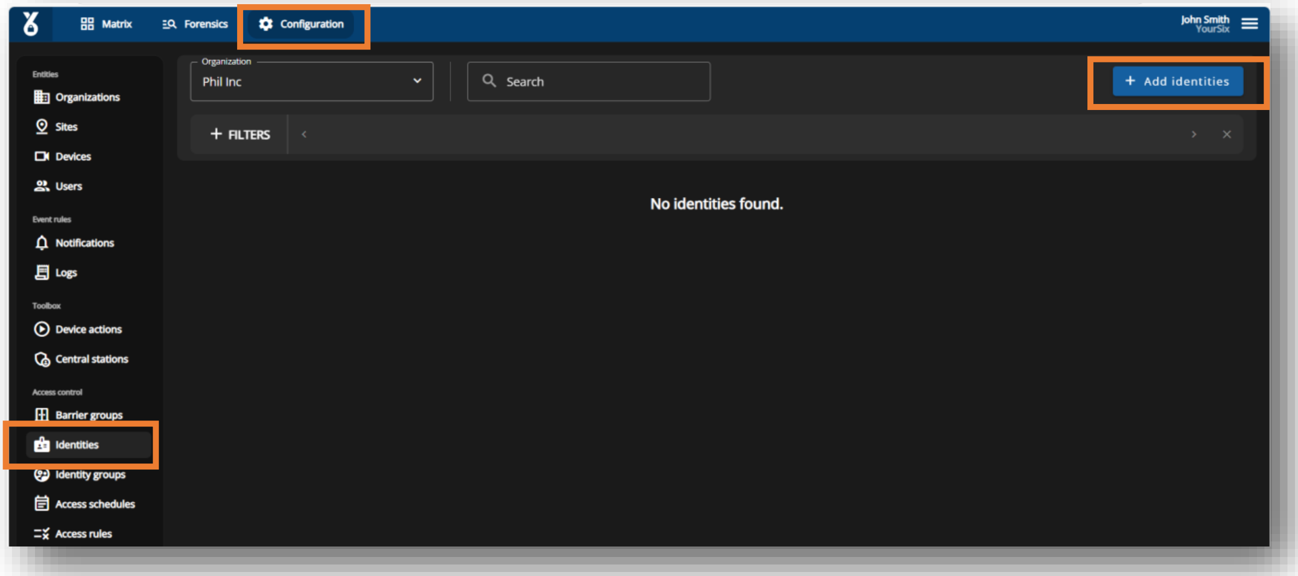
Add Identities and Credentials

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



No identities found.

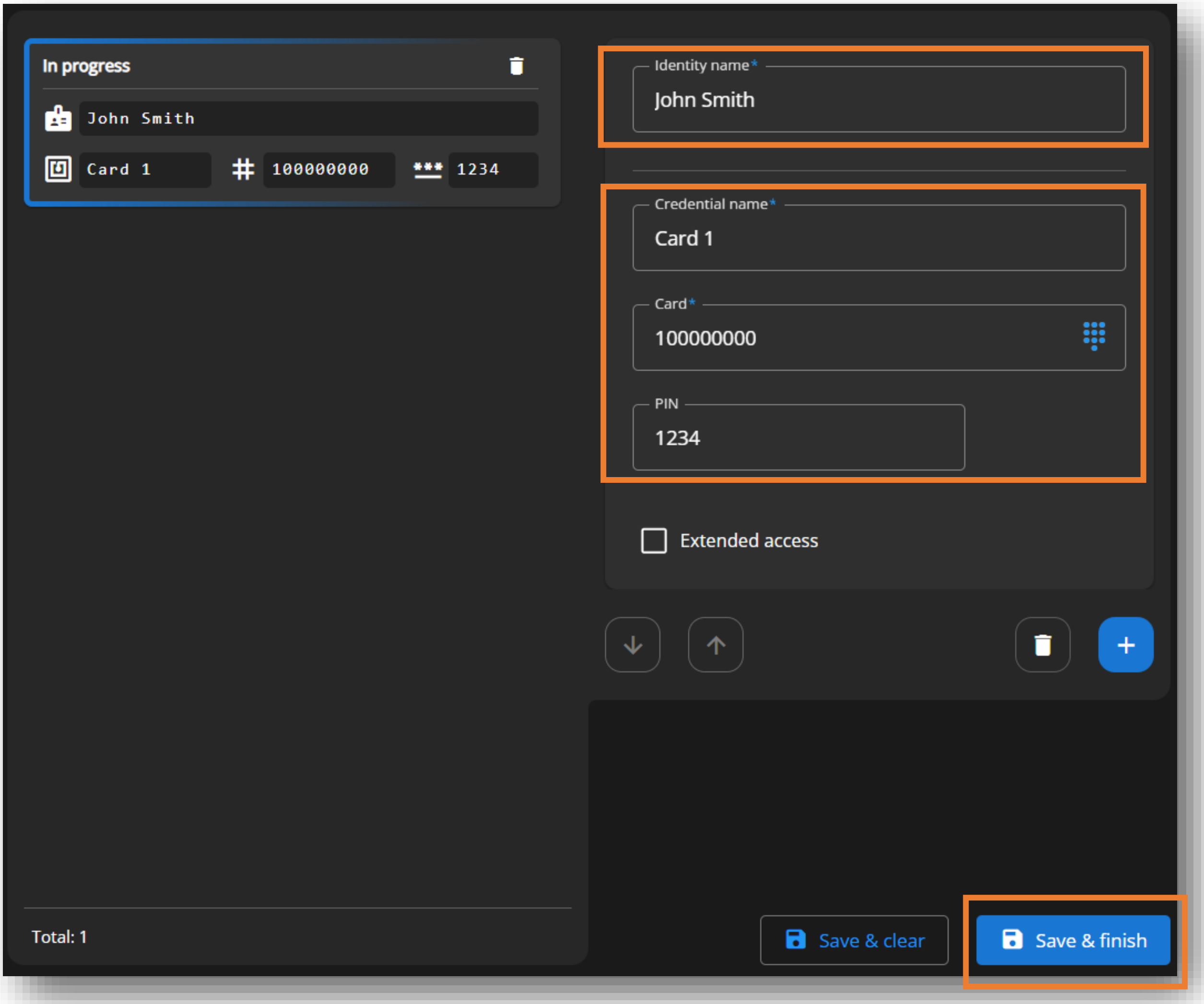
→ Select Configuration located on the navigation bar

→ 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

Total: 1

→ Add the Name of the identity

→ Add the Name of the credential

→ 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

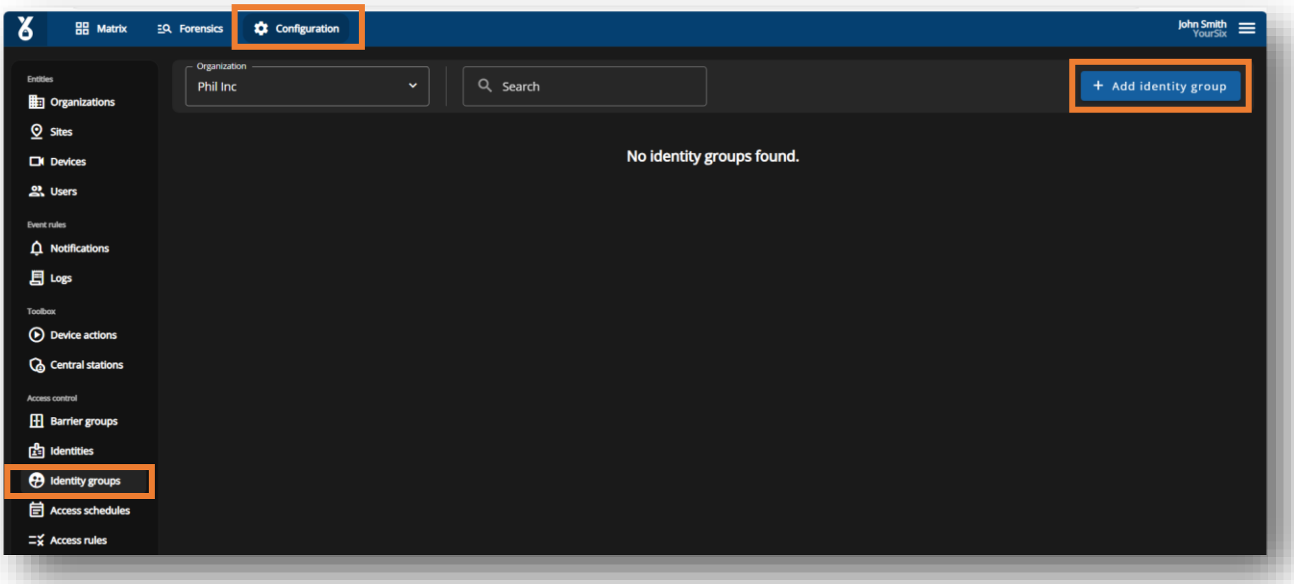
Add Identity Groups

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



No identity groups found.

→ 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

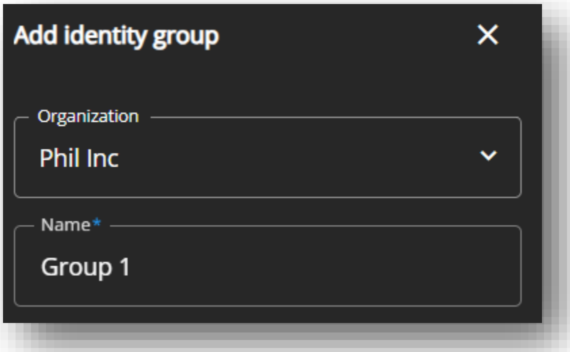
Add Identity Groups

Add identity group

→ Confirm the Organization

→ Name the Identity group

→ Select Save at the bottom of the window

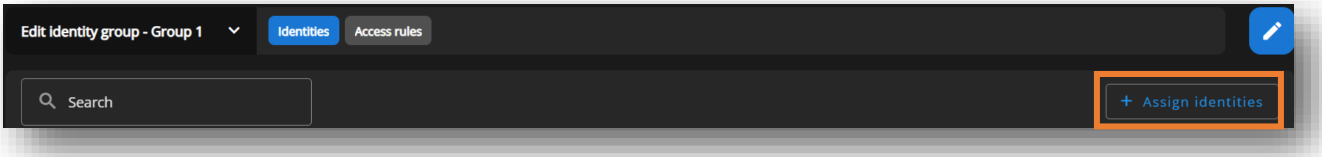

Add identity group

Organization: Phil Inc

Name*: Group 1

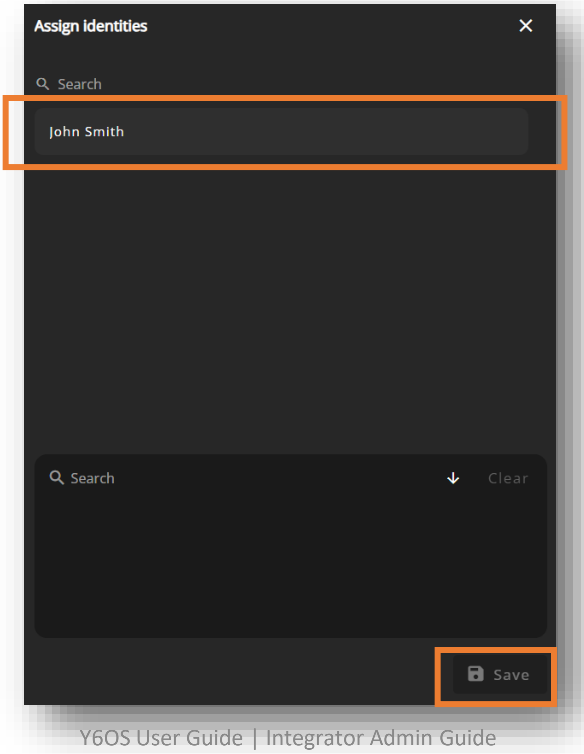
Assign identities to the group

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



→ On the popout menu, select the identities

→ Confirm selection and select Save



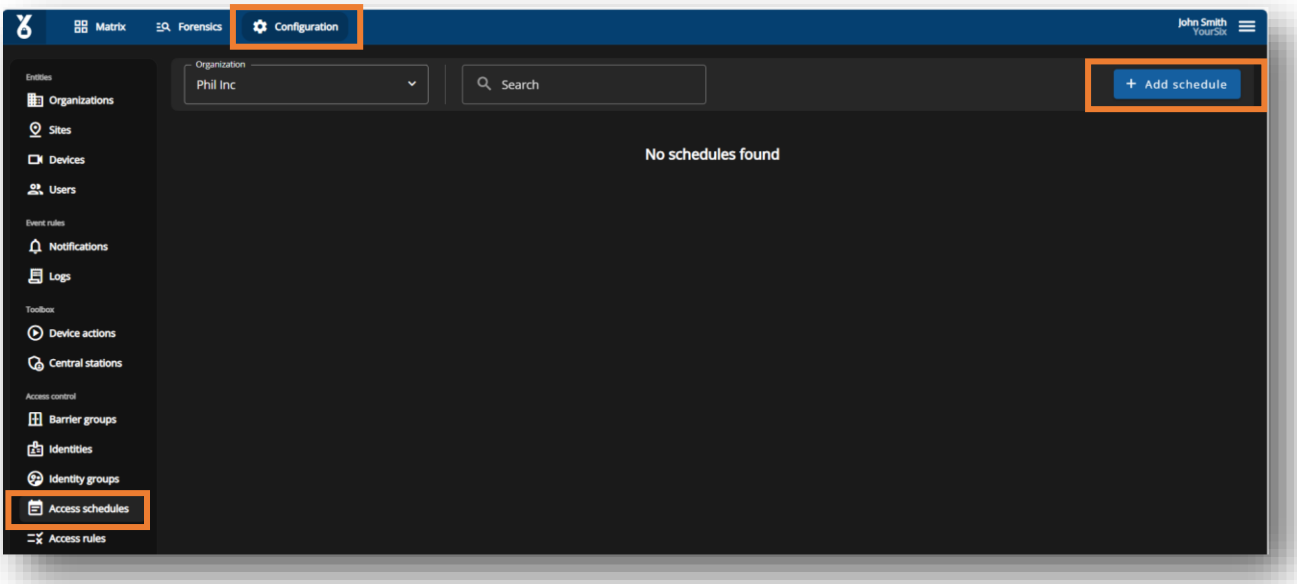
Add Access Schedules

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

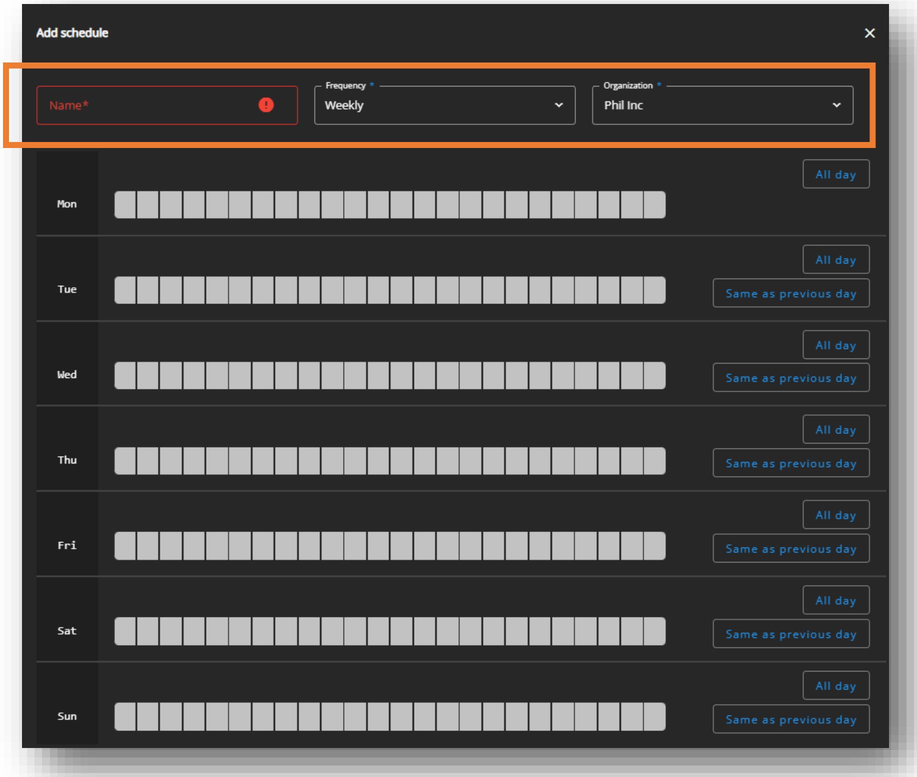
→ Select Access schedules located on the page menu

→ 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


Add schedule

Name*

Frequency *: Weekly

Organization *: Phil Inc

→ 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

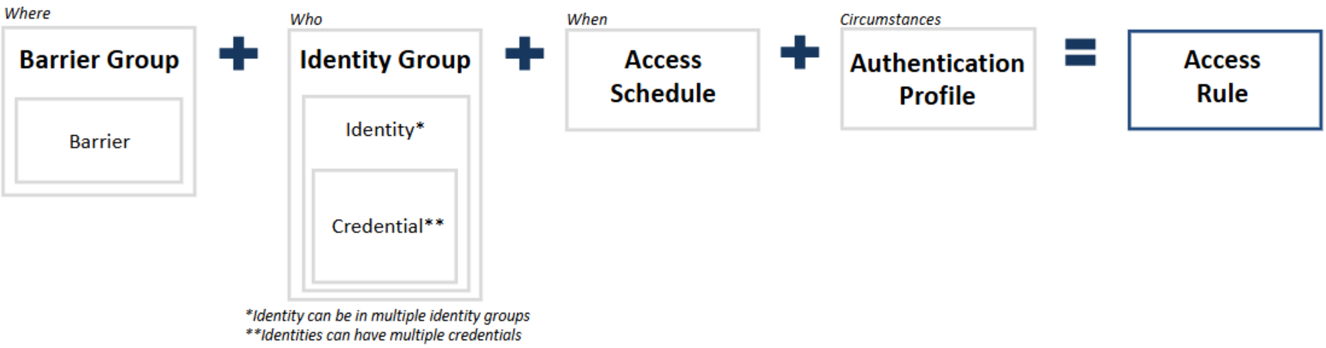
- *Important note: If a REX is used, a 24/7 schedule is recommended*

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

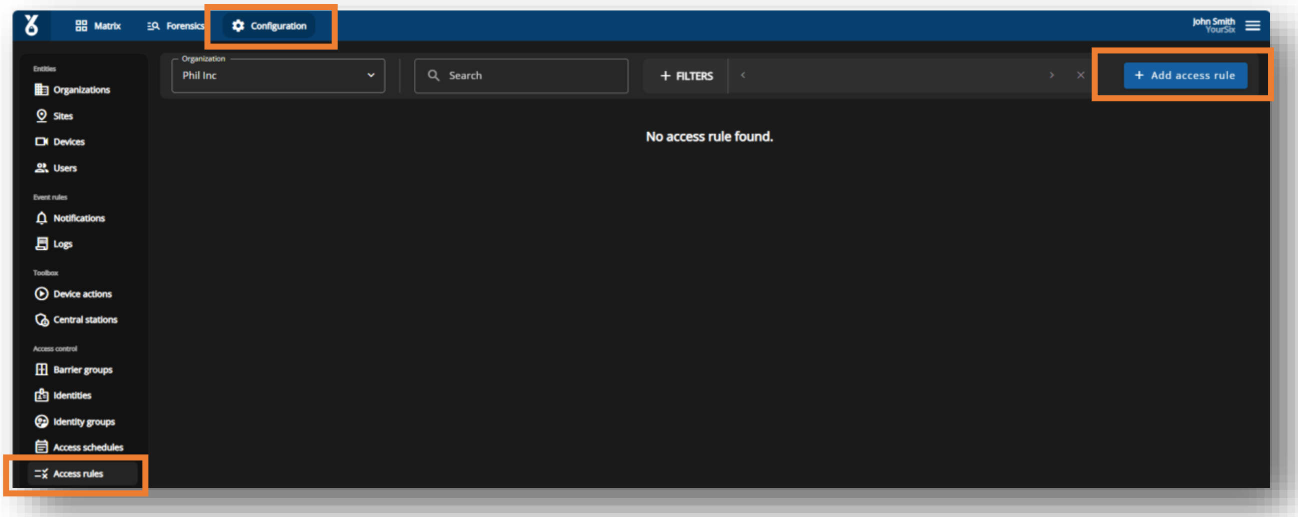
Add Access Rules

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



No access rule found.

→ 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

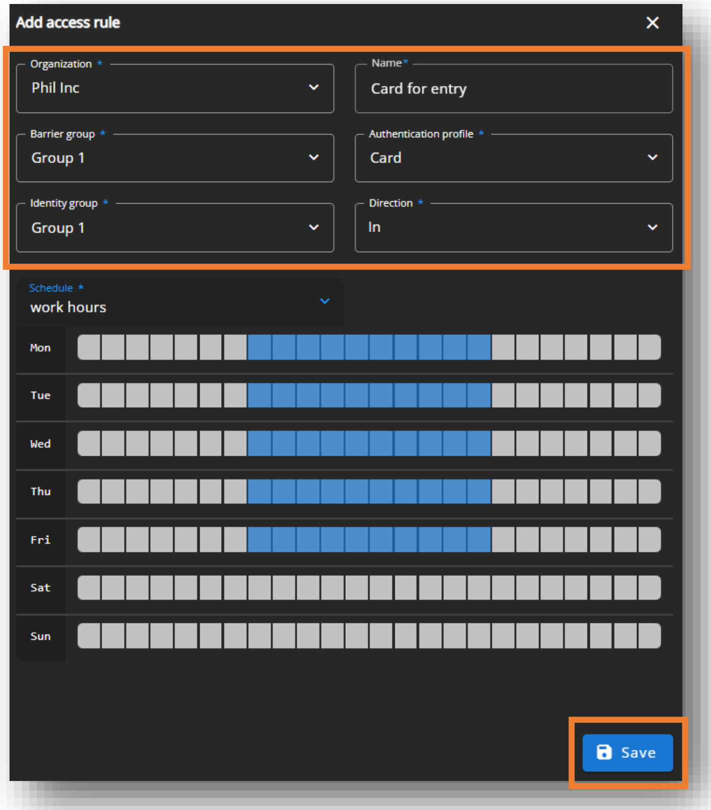
→ Select the Authentication profile
- Card
- Pin
- Card+Pin *(Requires both card & pin)*

→ Select the Identity group

→ Select Direction

→ Select the Schedule

→ Select Save



Add access rule

Organization * Phil Inc

Name* Card for entry

Barrier group * Group 1

Authentication profile * Card

Identity group * Group 1

Direction * In

Schedule * work hours

REX Rule

→ Confirm Organization

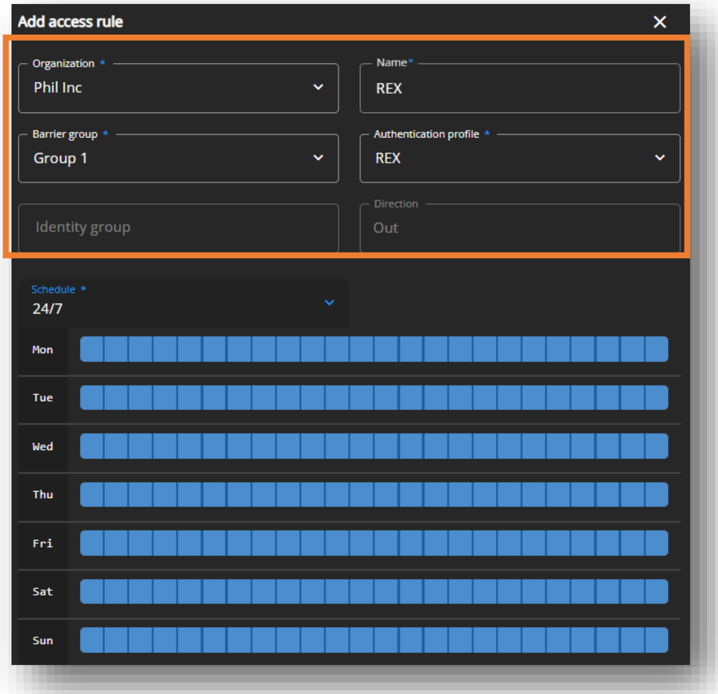
→ Enter Name

→ Select the Barrier group

→ Select REX as the Authentication profile

→ Select the Schedule

→ Select Save



Add access rule

Organization * Phil Inc

Name* REX

Barrier group * Group 1

Authentication profile * REX

Identity group

Direction Out

Schedule * 24/7

Add Access Rules

Unlocked Rule
When will Barriers be unlocked

→ Confirm Organization

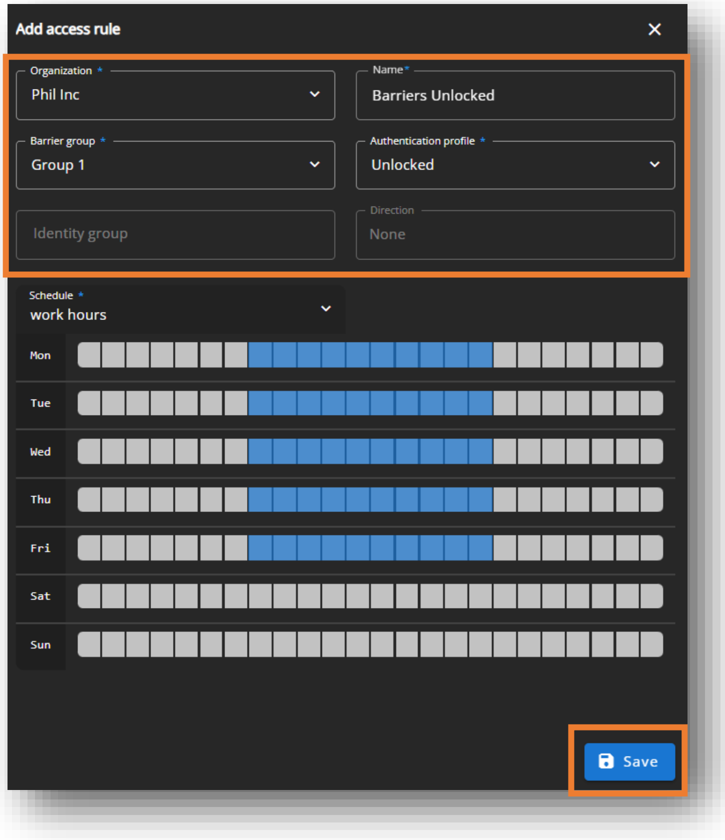
→ Enter Name

→ Select the Barrier group

→ Select Unlocked as the Authentication profile

→ Select the Schedule

→ Select Save



Add access rule

Organization *: Phil Inc

Name*: Barriers Unlocked

Barrier group *: Group 1

Authentication profile *: Unlocked

Identity group

Direction: None

Schedule *: work hours

Review Rules and Testing

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

Users

Manage Users

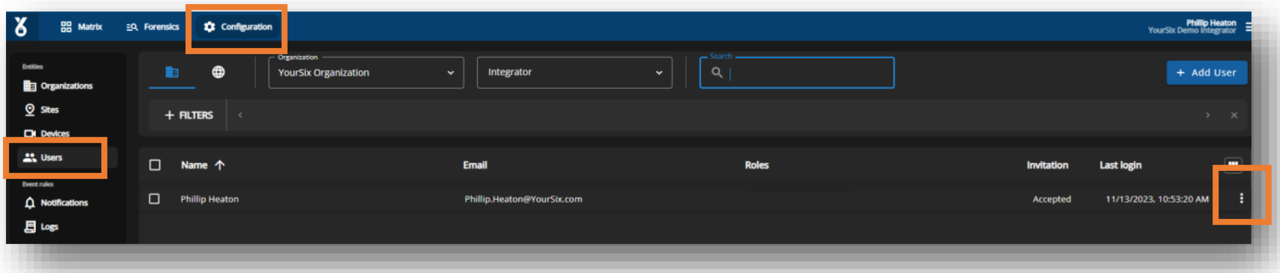
Audience: Integrator Super Admin, Integrator Admin

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



☐	Name ↑	Email	Roles	Invitation	Last login
☐	Phillip Heaton	Phillip.Heaton@YourSix.com		Accepted	11/13/2023, 10:53:20 AM

→ Select Configuration located on the navigation bar

→ Select Users located on the page menu

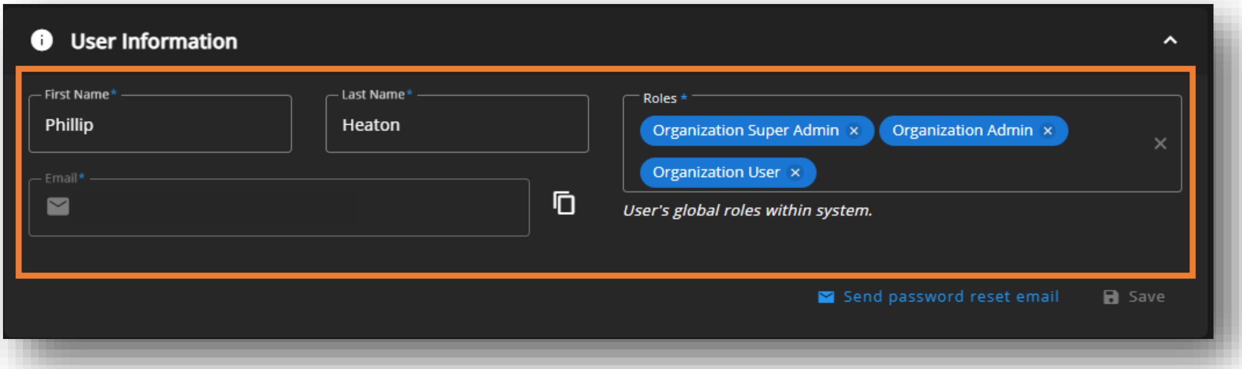
→ Select Pen icon to edit the user

→ 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 × Organization Admin × Organization User ×

User's global roles within system.

Basic User Information:

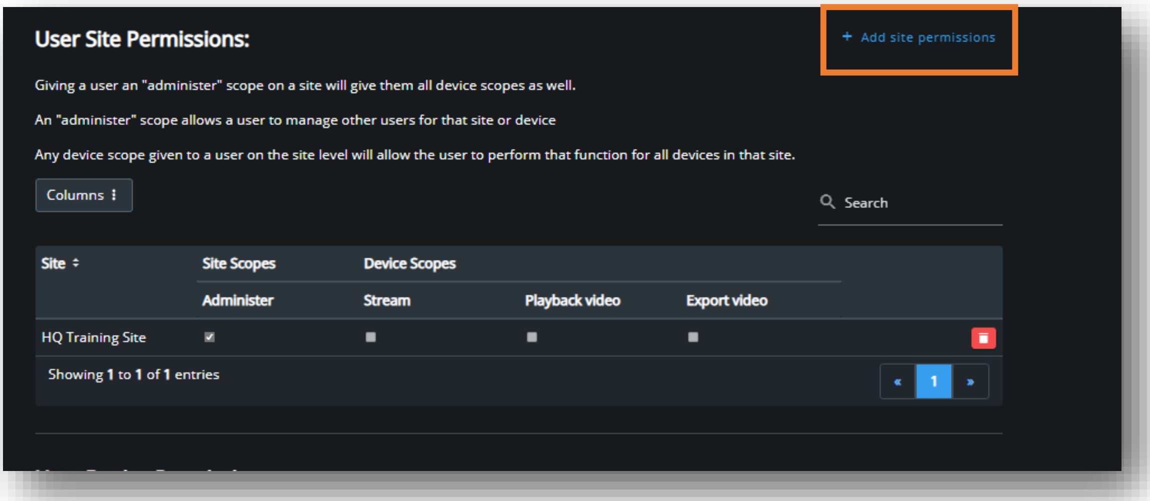
→ Enter user First Name and Last Name

→ Select or remove Permissions

→ Select Save

→ Continue to next page →→→

Edit a User



User Site Permissions:

Giving a user an "administer" scope on a site will give them all device scopes as well.

An "administer" scope allows a user to manage other users for that site or device

Any device scope given to a user on the site level will allow the user to perform that function for all devices in that site.

Site	Site Scopes	Device Scopes		
	Administer	Stream	Playback video	Export video
HQ Training Site	☑	□	□	□

Showing **1** to **1** of **1** entries

Add Site Permissions:

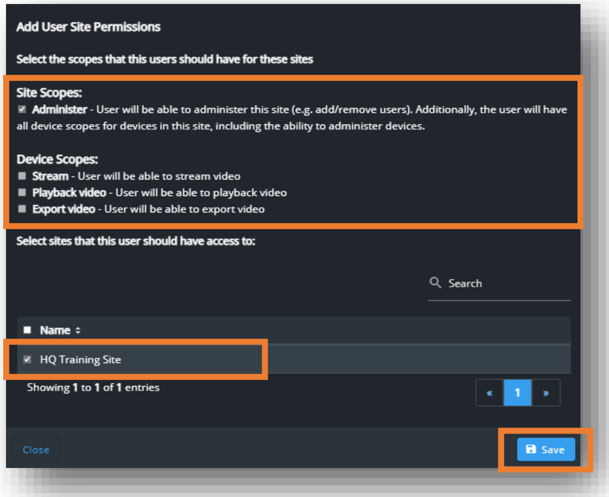
→ Select Add Site Permissions

→ 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 →→→



Add User Site Permissions

Select the scopes that this users should have for these sites

Site Scopes:

☑ **Administer** - User will be able to administer this site (e.g. add/remove users). Additionally, the user will have all device scopes for devices in this site, including the ability to administer devices.

Device Scopes:

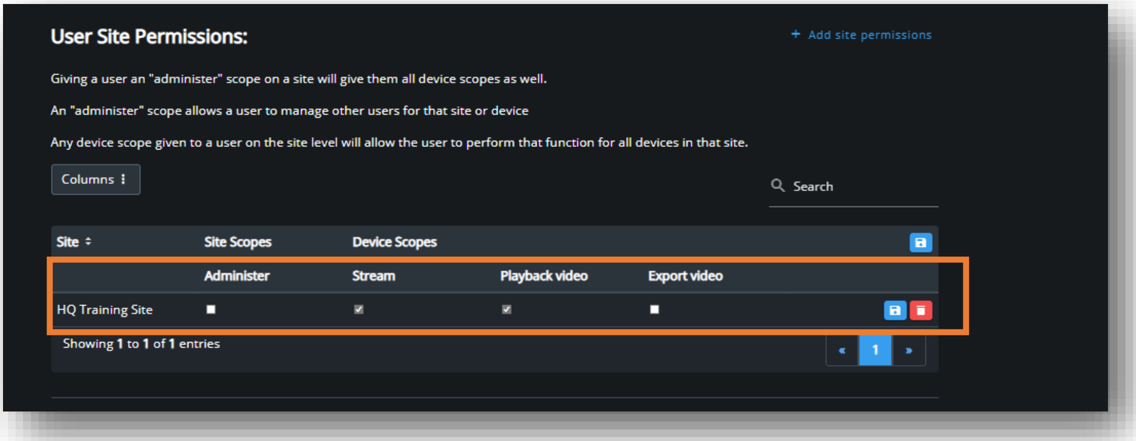
□ **Stream** - User will be able to stream video
□ **Playback video** - User will be able to playback video
□ **Export video** - User will be able to export video

Select sites that this user should have access to:

□ Name
☑ HQ Training Site

Showing **1** to **1** of **1** entries

Edit a User



User Site Permissions:

+ Add site permissions

Giving a user an "administer" scope on a site will give them all device scopes as well.

An "administer" scope allows a user to manage other users for that site or device

Any device scope given to a user on the site level will allow the user to perform that function for all devices in that site.

Site	Site Scopes	Device Scopes			
	Administer	Stream	Playback video	Export video	
HQ Training Site	□	☑	☑	□	

Showing 1 to 1 of 1 entries

Edit Site Permissions:

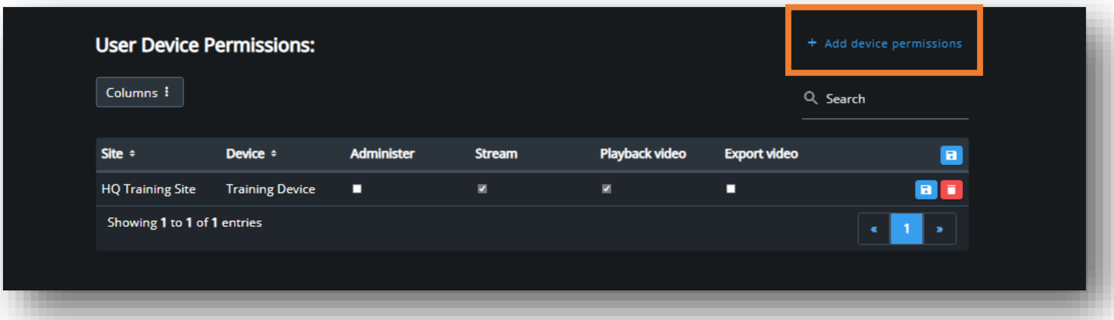
→ Select the desired Site Scopes or Device Scopes

→ Select the Save Icon

→ *To delete a site permission, select the Trash Can Icon*

→ Continue to next page →→→

Edit a User



User Device Permissions:

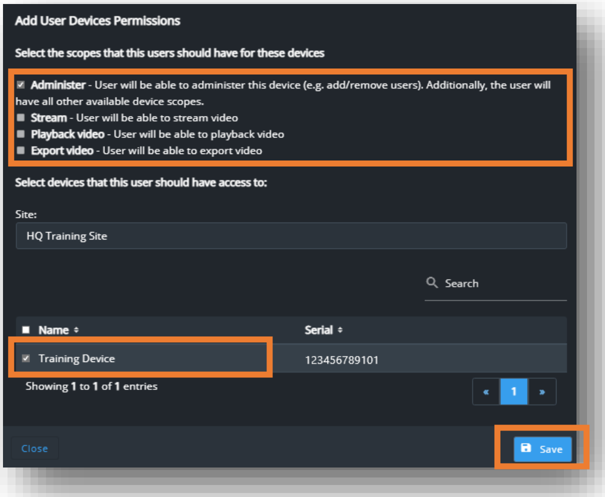
+ Add device permissions

Site	Device	Administer	Stream	Playback video	Export video
HQ Training Site	Training Device	☐	☑	☑	☐

Showing 1 to 1 of 1 entries

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 →→→



Add User Devices Permissions

Select the scopes that this users should have for these devices

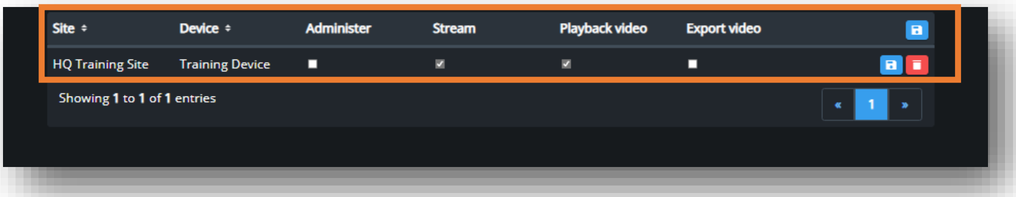
☑ **Administer** - User will be able to administer this device (e.g. add/remove users). Additionally, the user will have all other available device scopes.
☐ **Stream** - User will be able to stream video
☐ **Playback video** - User will be able to playback video
☐ **Export video** - User will be able to export video

Select devices that this user should have access to:

Site: HQ Training Site

☐ Name	Serial
☑ Training Device	123456789101

Showing 1 to 1 of 1 entries



Site	Device	Administer	Stream	Playback video	Export video
HQ Training Site	Training Device	☐	☑	☑	☐

Showing 1 to 1 of 1 entries

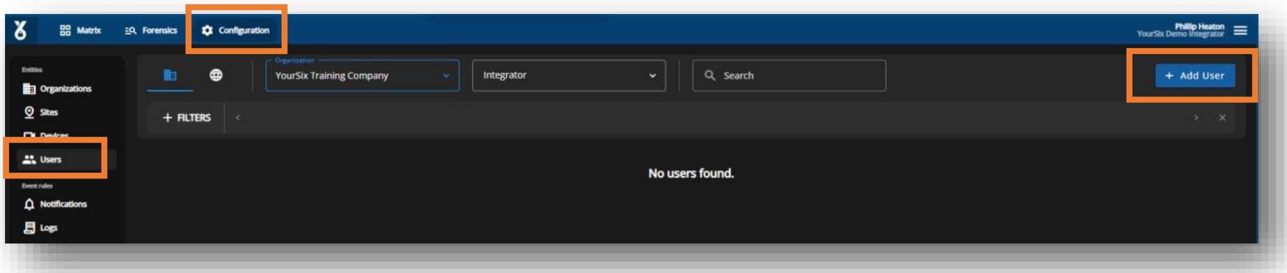
Edit Device Permissions:

- → 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.



No users found.

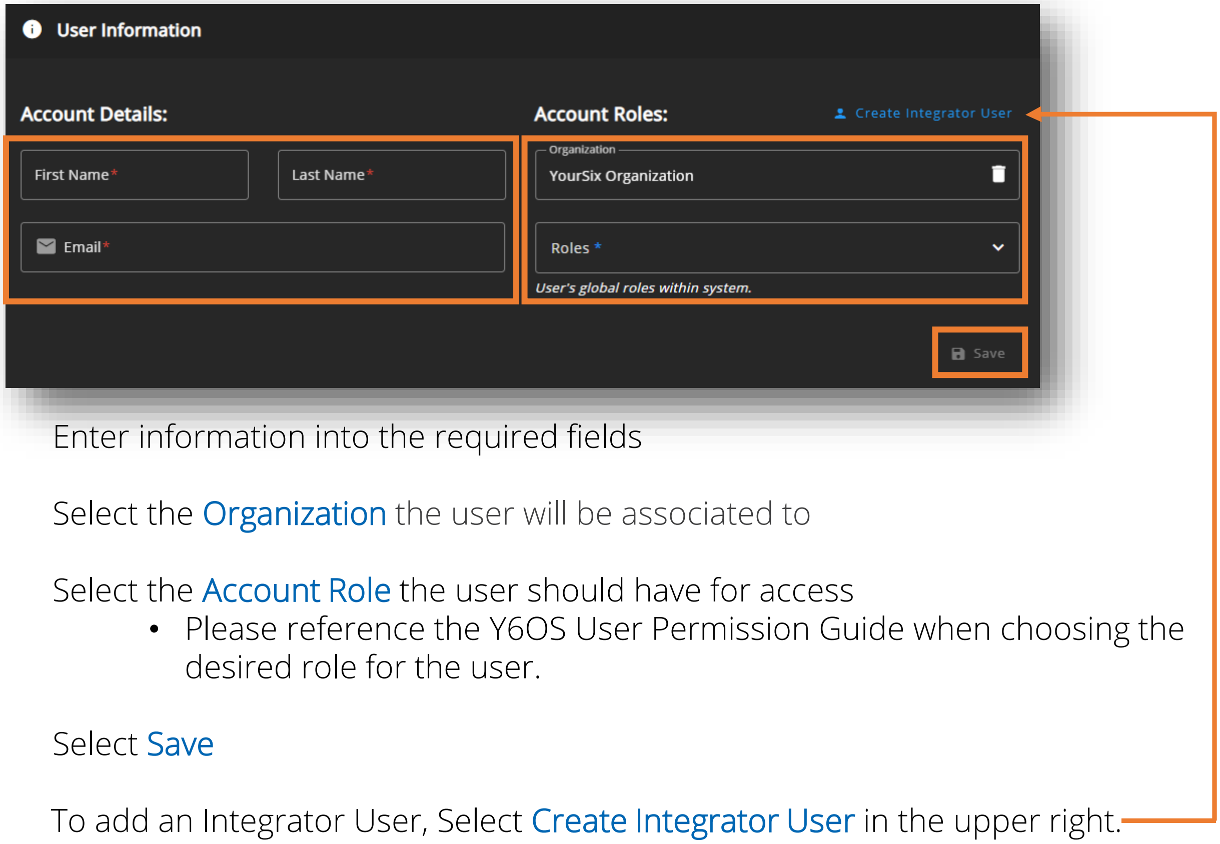
→ Select Configuration located on the navigation bar

→ 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:

Organization: YourSix Organization

Roles *

User's global roles within system.

→ Enter information into the required fields

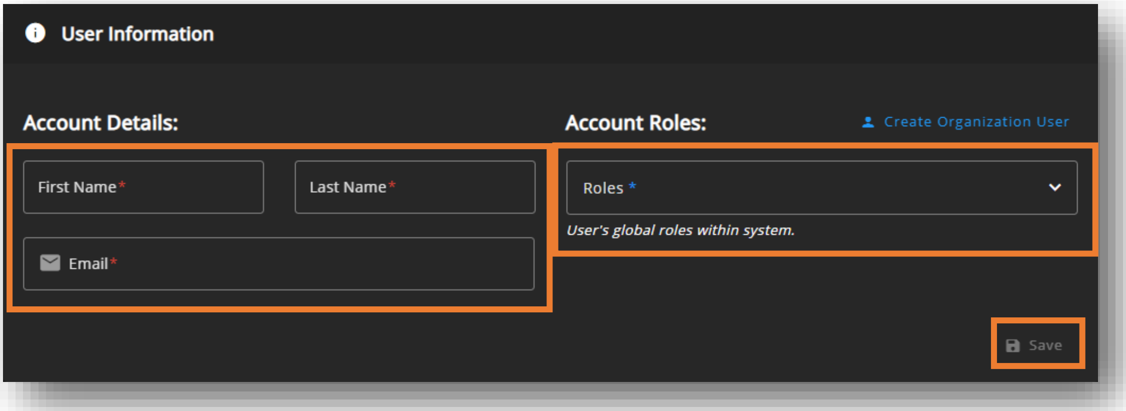
→ Select the Organization the user will be associated to

→ 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

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
        - Tunning 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

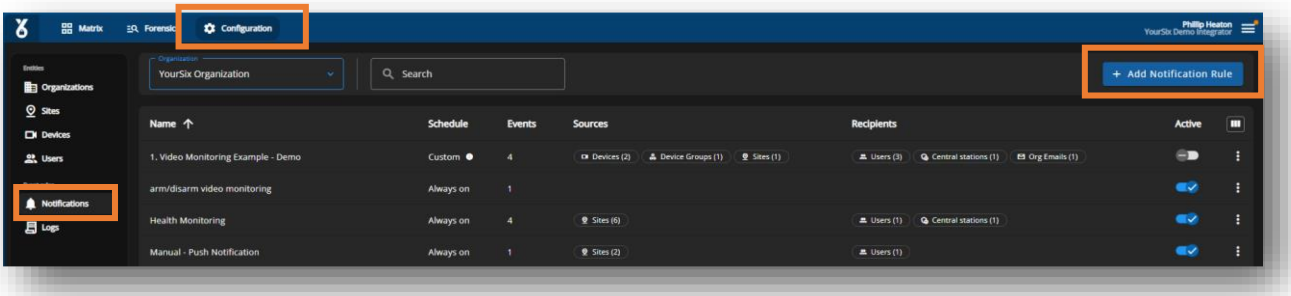
Create Notifications

Audience: Integrator Super Admin, Integrator Admin

Objective: Create a notification rule.

Additional Resources:

- Notification videos



Name ↑	Schedule	Events	Sources	Recipients	Active
1. Video Monitoring Example - Demo	Custom ●	4	Devices (2) Device Groups (1) Sites (1)	Users (3) Central stations (1) Org Emails (1)	○
arm/disarm video monitoring	Always on	1			✓
Health Monitoring	Always on	4	Sites (6)	Users (1) Central stations (1)	✓
Manual - Push Notification	Always on	1	Sites (2)	Users (1)	✓

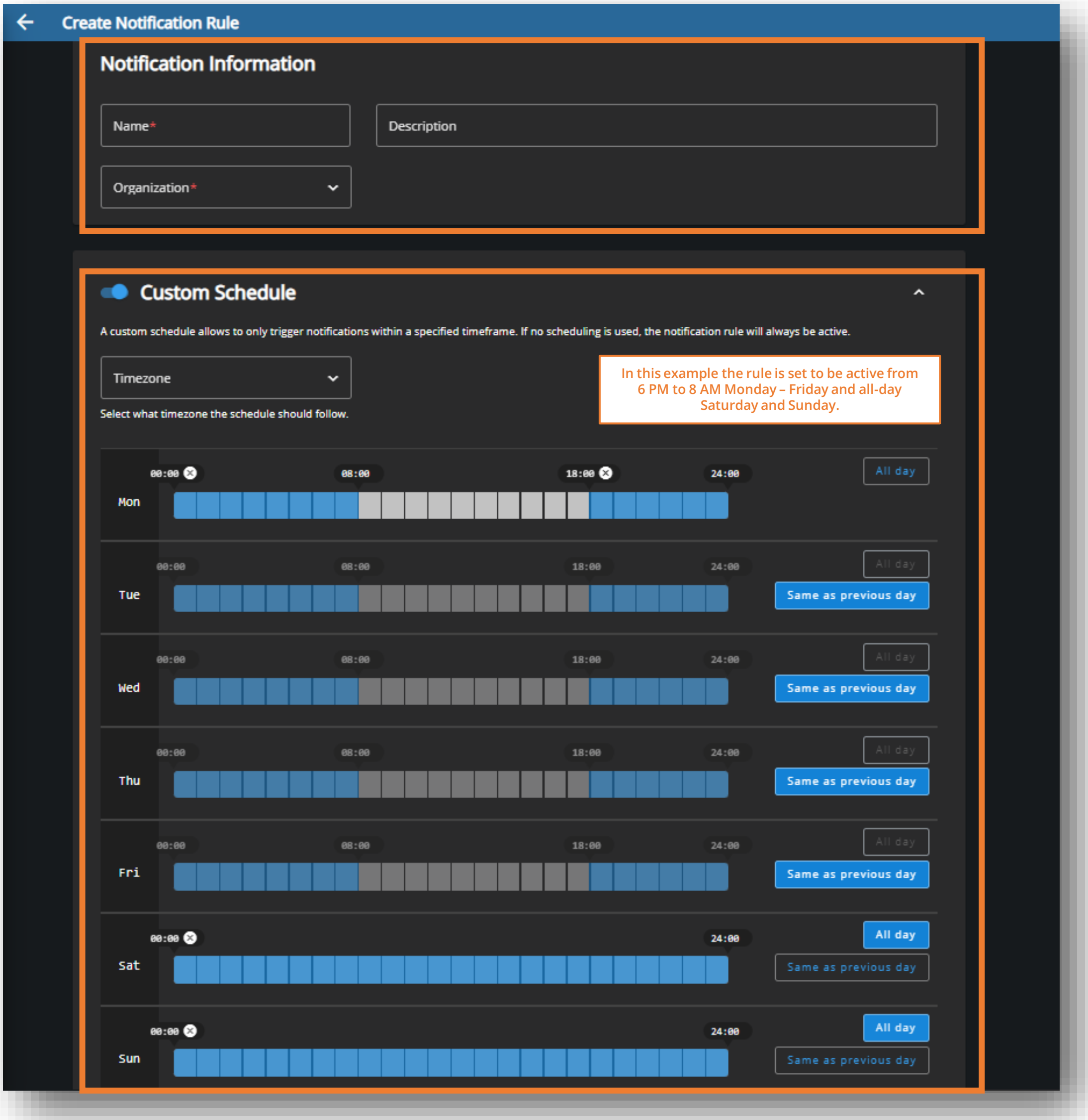
→ Select Configuration located on the navigation bar

→ 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.

Rule Name & Schedule:

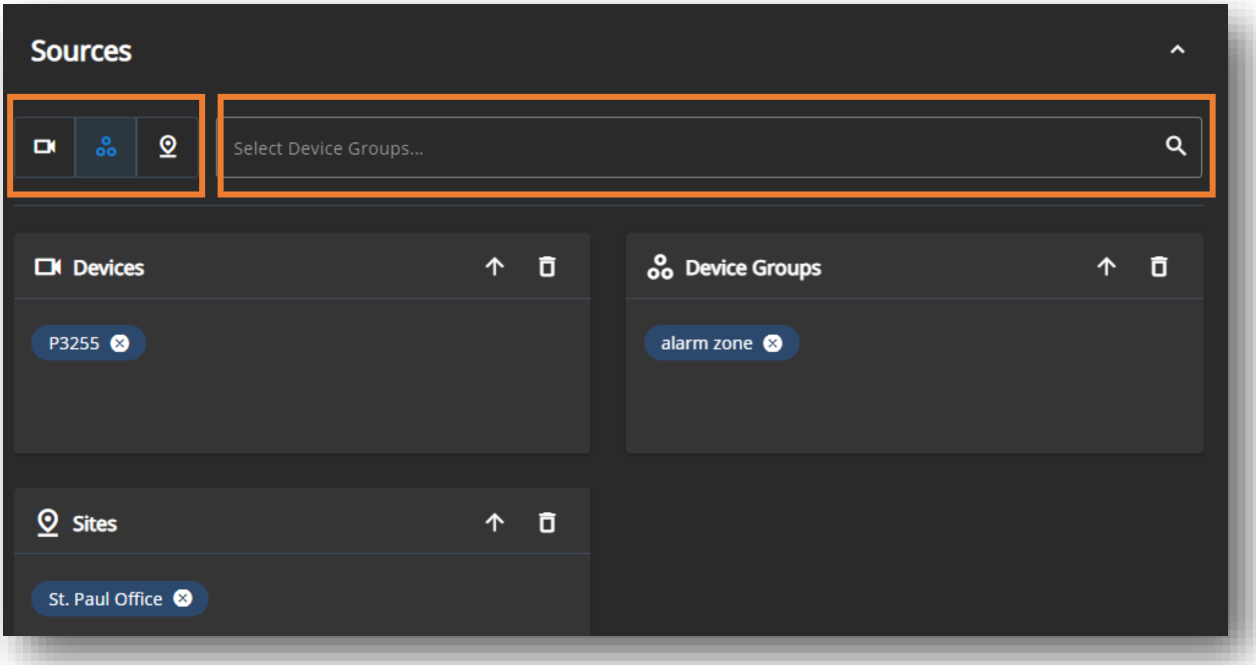
→ Add the Name & Description and select the Organization for the rule

→ 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

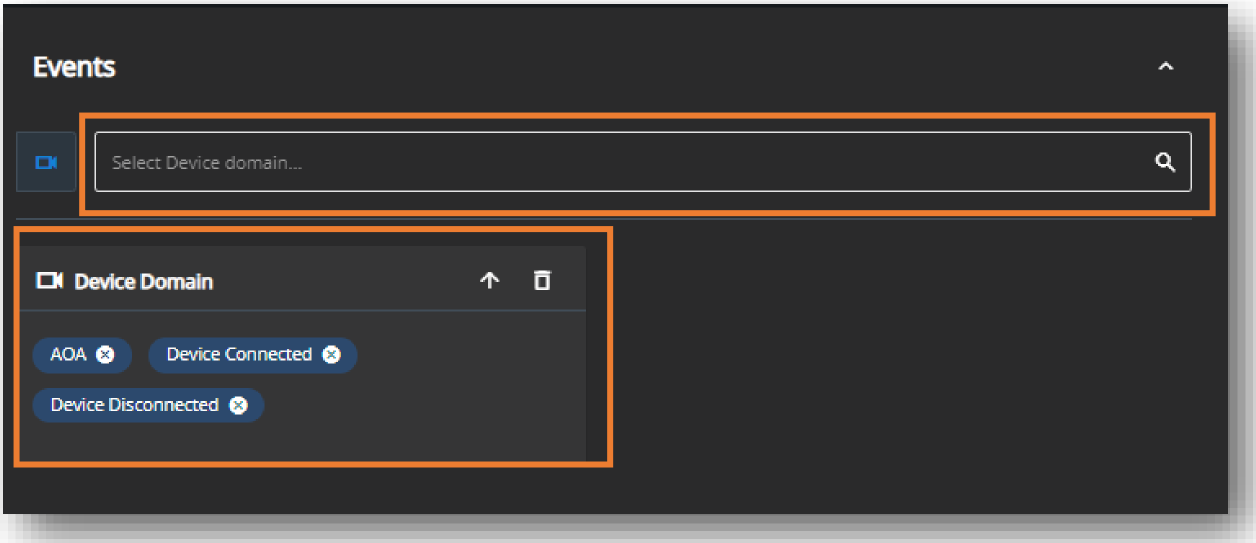
🎥	Devices
⚇	Device Groups *(To create see [Create Device Group](#))*
⌾	Sites

→ 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

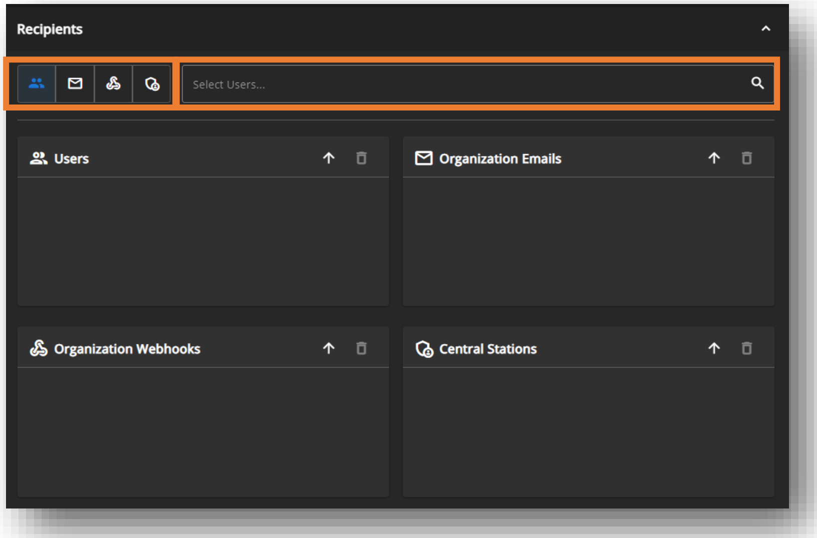
Note: Selected domains will only work on devices that have been enabled. For example, if a device group has some devices with AOA and some without then only the devices with AOA will trigger the notification.

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

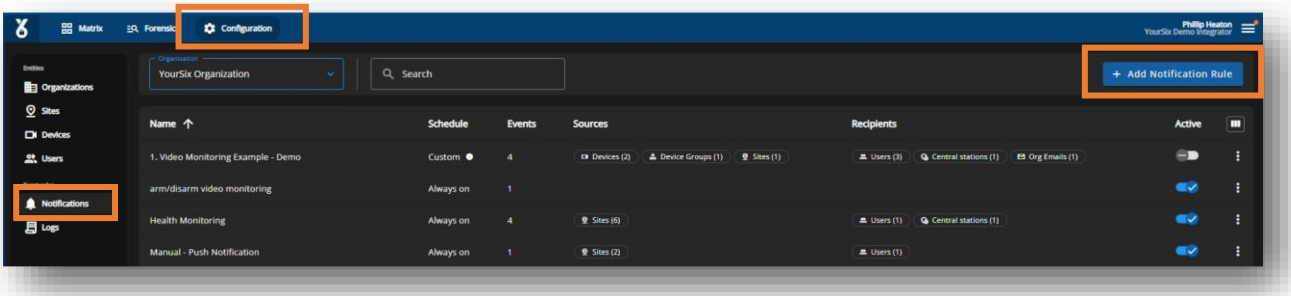
→ Select the recipient from the drop-down menu; the selected recipient will appear in the appropriate box

→ 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



Name	Schedule	Events	Sources	Recipients	Active
1. Video Monitoring Example - Demo	Custom	4	Devices (2) Device Groups (1) Sites (1)	Users (3) Central stations (1) Org Emails (1)	○
arm/disarm video monitoring	Always on	1			✓
Health Monitoring	Always on	4	Sites (6)	Users (1) Central stations (1)	✓
Manual - Push Notification	Always on	1	Sites (2)	Users (1)	✓

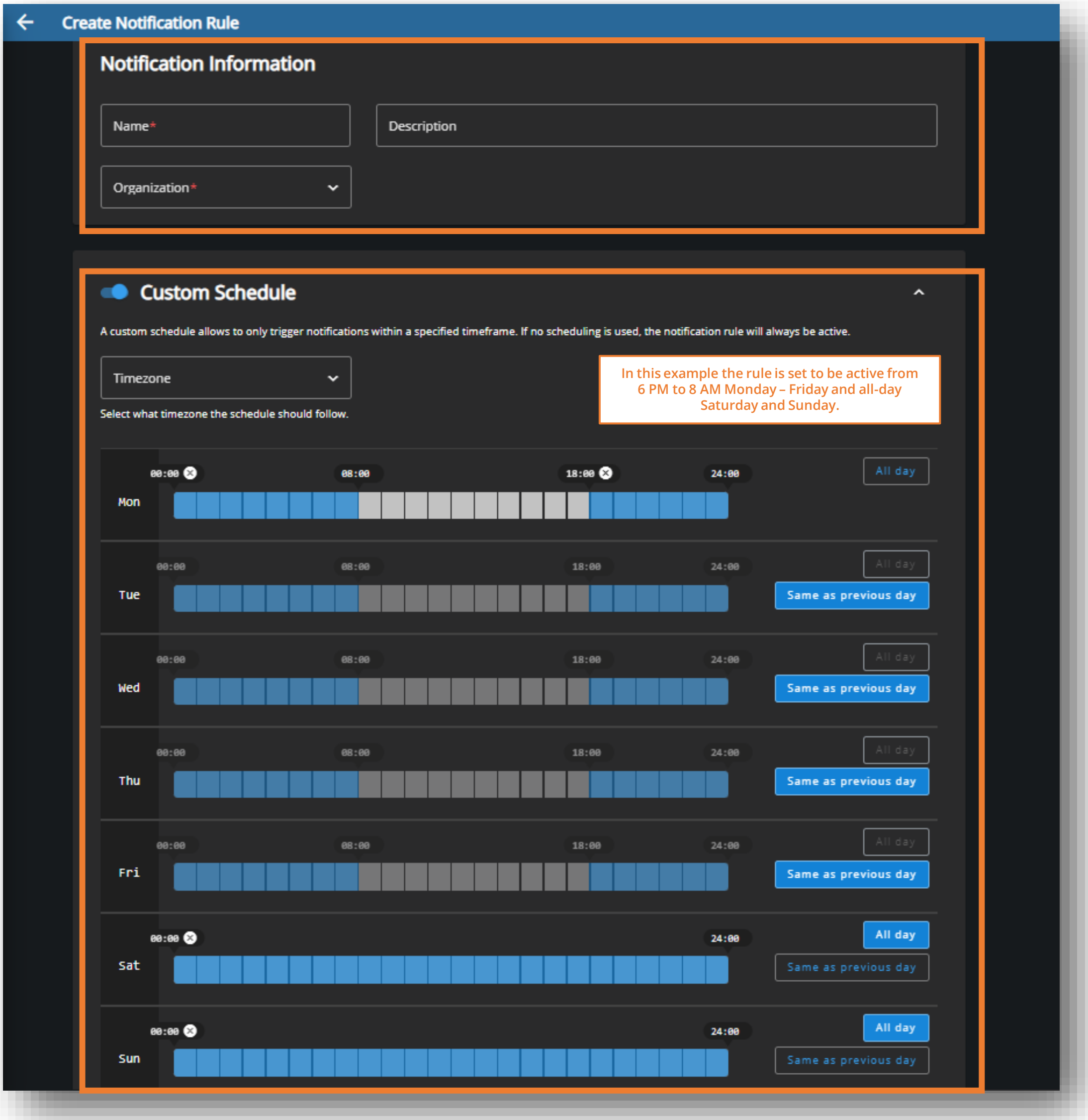
→ Select Configuration located on the navigation bar

→ 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.

Rule Name & Schedule:

→ Navigate to the Notifications Icon and Select Create Notification Rule

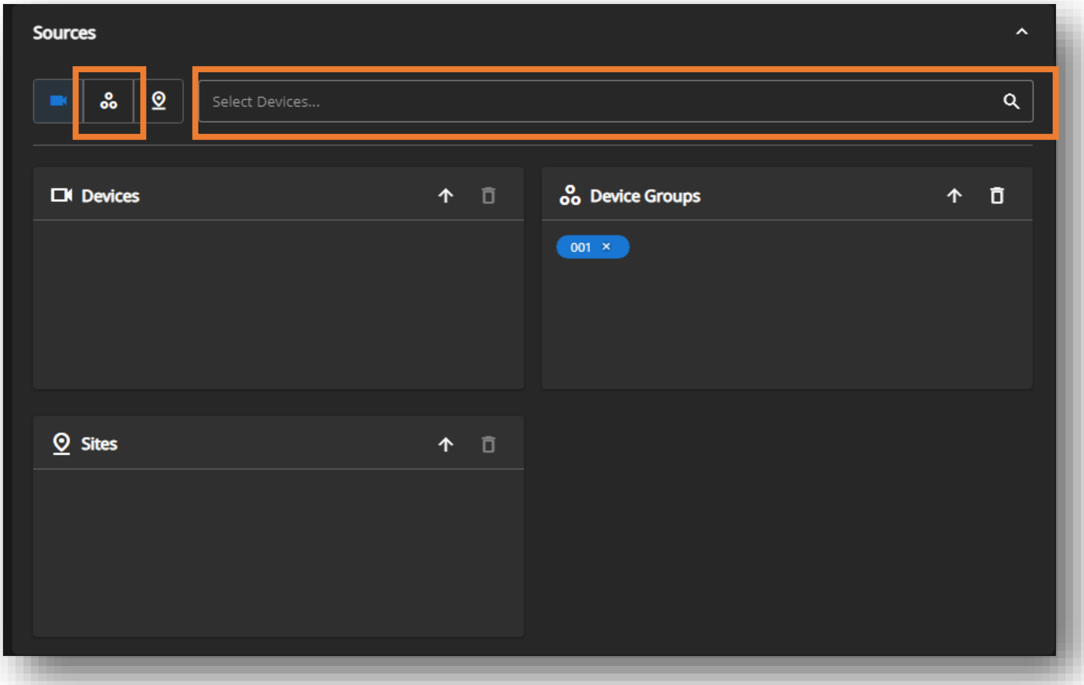
→ Add the Name & Description and select the Organization for the rule

→ 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

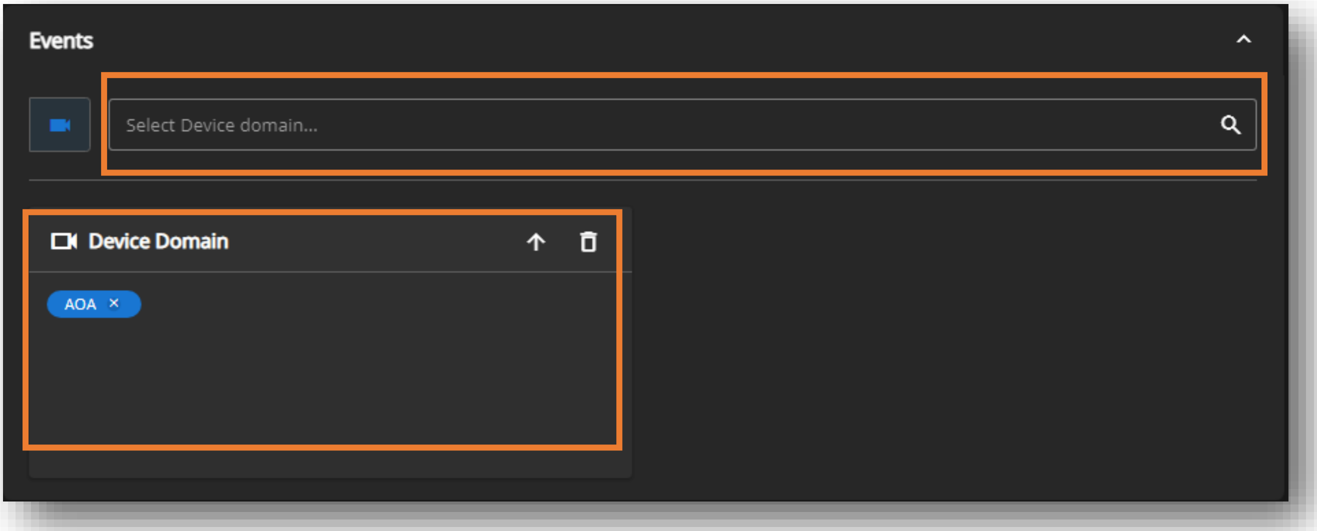
→ Select the Device Group Icon. Notifications for video monitoring must be set up at a device group level. Do not setup video monitoring notifications for site.

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:

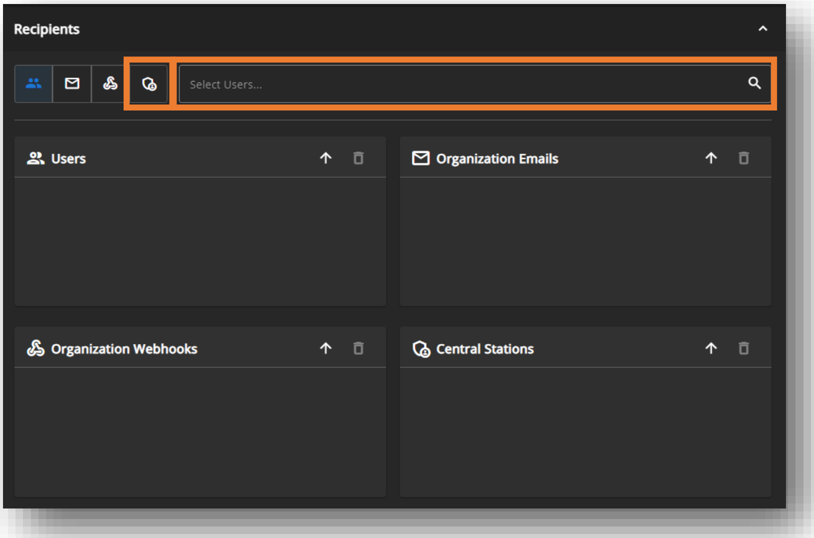
→ On the Edit Notification Rule page navigate to the Events section

→ 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

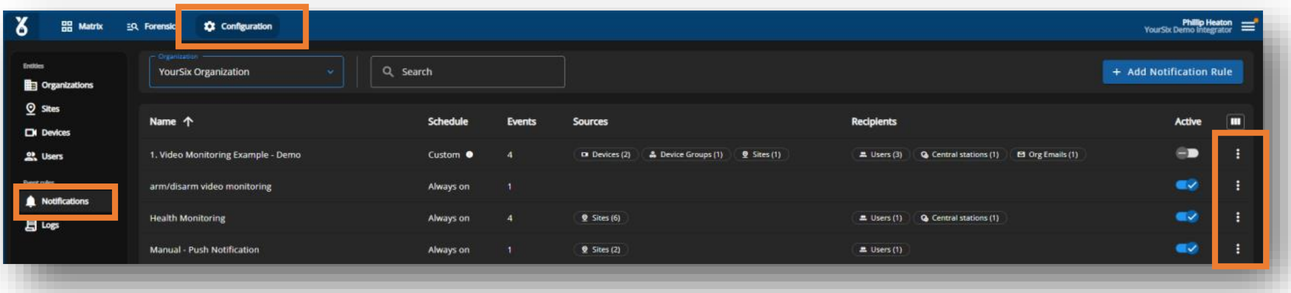
→ Select the Search Bar located to the right of the icons and select the central station you wish the notifications to go to. If you do not see the proper central station, then please reach out to YourSix

→ Select Save rule at the bottom of the page

Edit Notifications

Audience: Integrator Super Admin, Integrator Admin

Objective: Manage notification rules.



Name ↑	Schedule	Events	Sources	Recipients	Active
1. Video Monitoring Example - Demo	Custom ●	4	Devices (2) Device Groups (1) Sites (1)	Users (3) Central stations (1) Org Emails (1)	○
arm/disarm video monitoring	Always on	1			✓
Health Monitoring	Always on	4	Sites (6)	Users (1) Central stations (1)	✓
Manual - Push Notification	Always on	1	Sites (2)	Users (1)	✓

→ 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)

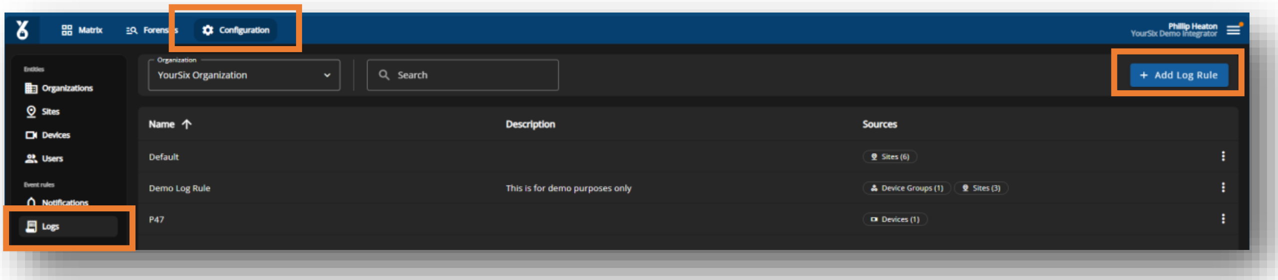
Logs

Audience: Integrator Super Admin, Integrator Admin

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

Additional Resources:

- Notification videos



Name ↑	Description	Sources
Default		Sites (6)
Demo Log Rule	This is for demo purposes only	Device Groups (1) Sites (3)
P47		Devices (1)

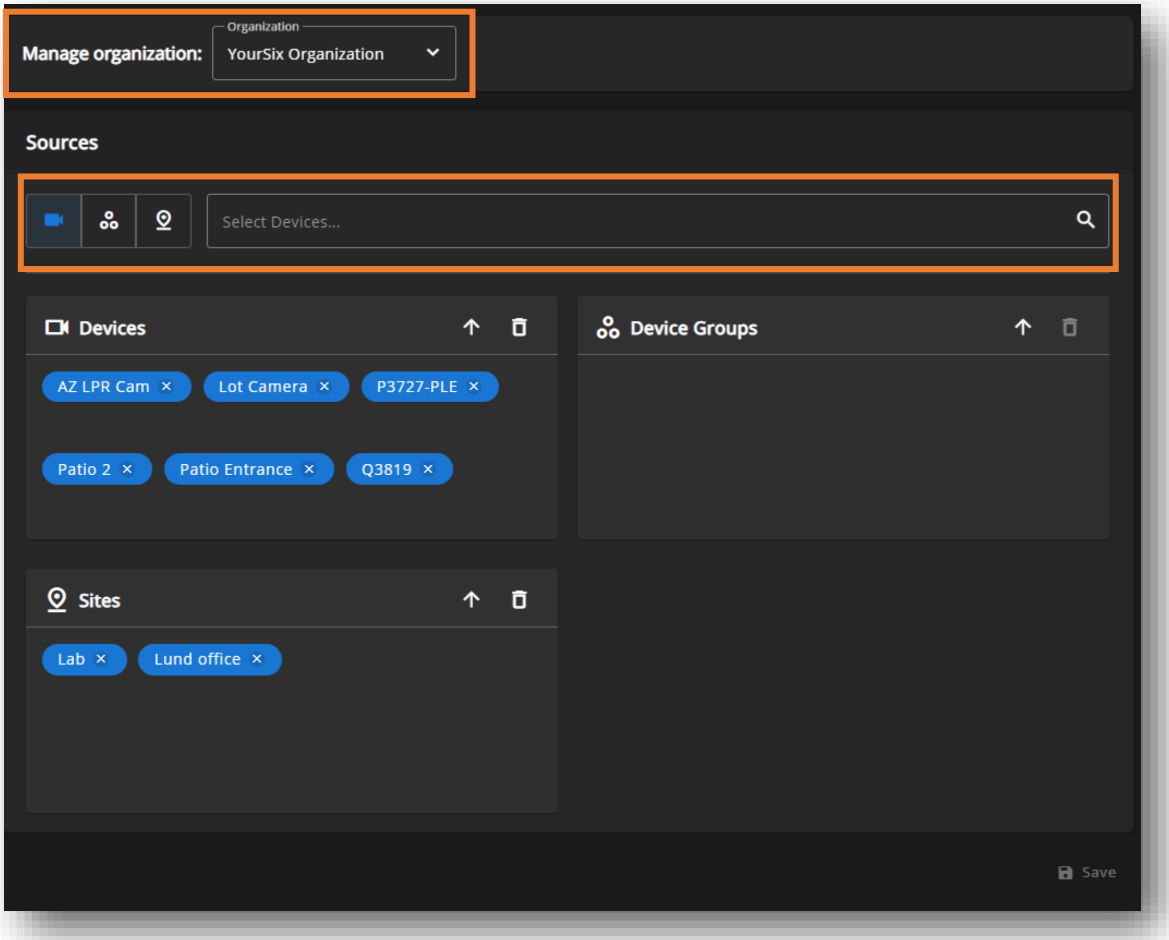
→ Select Configuration located on the navigation bar

→ 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



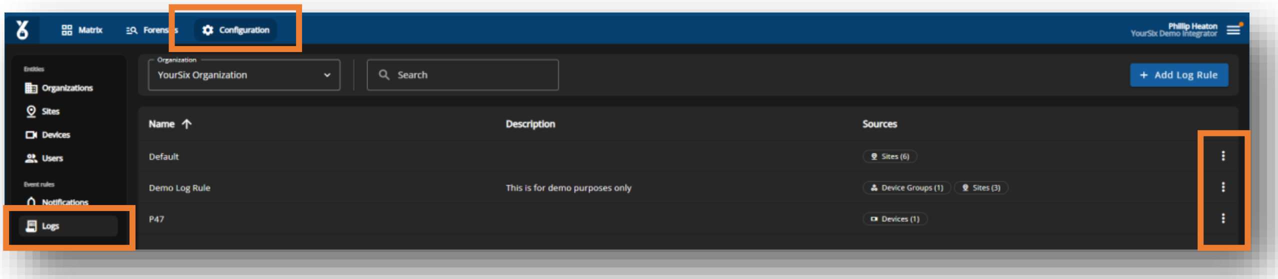
Log Rule:

→ 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



Organization: YourSix Organization

Search

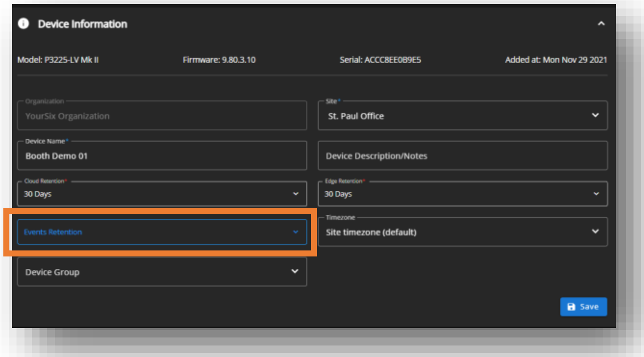
Name ↑	Description	Sources
Default		Sites (6)
Demo Log Rule	This is for demo purposes only	Device Groups (1) Sites (3)
P47		Devices (1)

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



Model: P3225-LV Mk II   Firmware: 9.80.3.10   Serial: ACCC8EE0B9E5   Added at: Mon Nov 29 2021

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)

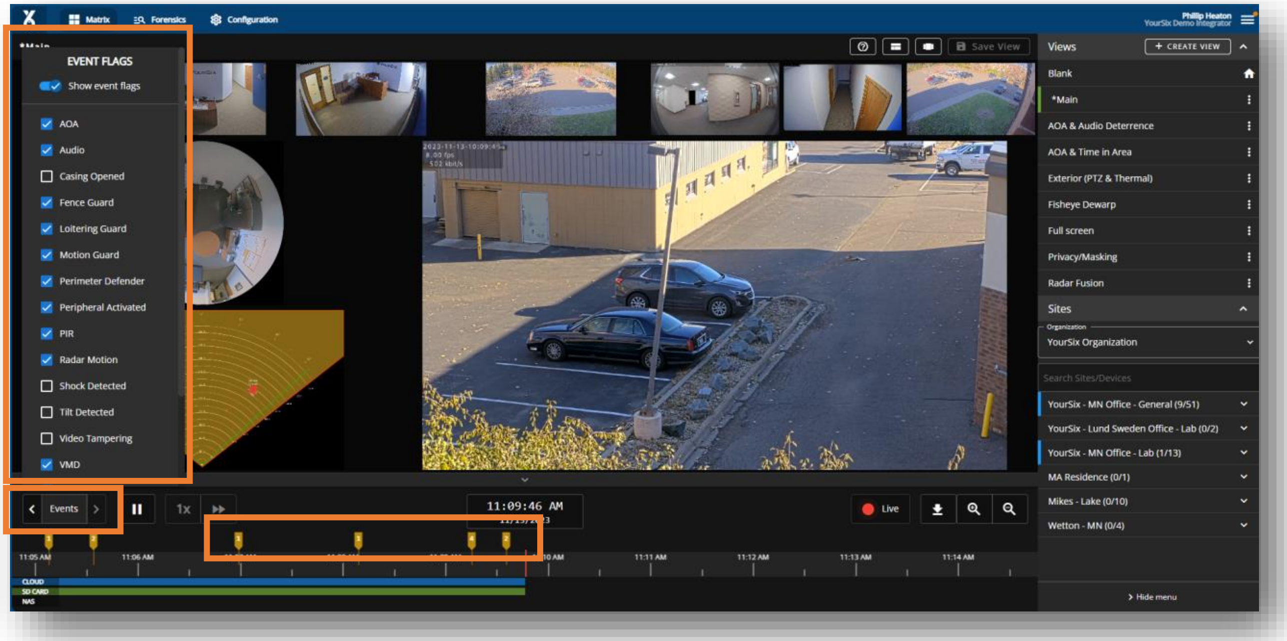
Device Group

→ 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

Show event flags ✓

- ☑ AOA
- ☑ Audio
- ☐ Casing Opened
- ☑ Fence Guard
- ☑ Loitering Guard
- ☑ Motion Guard
- ☑ Perimeter Defender
- ☑ Peripheral Activated
- ☑ PIR
- ☑ Radar Motion
- ☐ Shock Detected
- ☐ Tilt Detected
- ☐ Video Tampering
- ☑ VMD

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

YourSix

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.