



Y6OS User Guide for Organizations

March 2025 – Version 3.4

Contents



Audience: Y6OS Authorized Users



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



Additional Resources:

- [Platform training videos](#)
- [Access control training videos](#)

- [Basic Navigation](#)
 - [Email Invitation](#)
 - [Login](#)
 - [Layout](#)
- [Organization Functions](#)
 - [Manage My Org \(MFA, SSO, Webhooks & Org Email\)](#)
 - [Manage My Account](#)
- [Site Functions](#)
 - [Edit Sites](#) (including device groups and site schedules)
- [Devices](#)
 - [Manage Devices](#)
 - [Create a Rule](#)
 - [Edit a Device](#)
- [Access Control](#)
 - [Barrier Groups](#)
 - [Identities](#)
 - [Identity Groups](#)
 - [Access Schedules](#)
 - [Access Rules](#)



Contents

- [Forensics](#)
 - [Events](#)
 - [Access](#)
 - [Objects](#)
 - [Exports](#)

- [Alert State](#)
 - [Control alert state at a site](#)

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

- [Event Rules](#)
 - [Create Notifications](#)
 - [Edit Notifications](#)
 - [Log Rule](#)
 - [Event Log](#)

- [Contact YourSix](#)



Basic Navigation

→ [Email Invitation](#)

→ [Login](#)

→ [Layout](#)

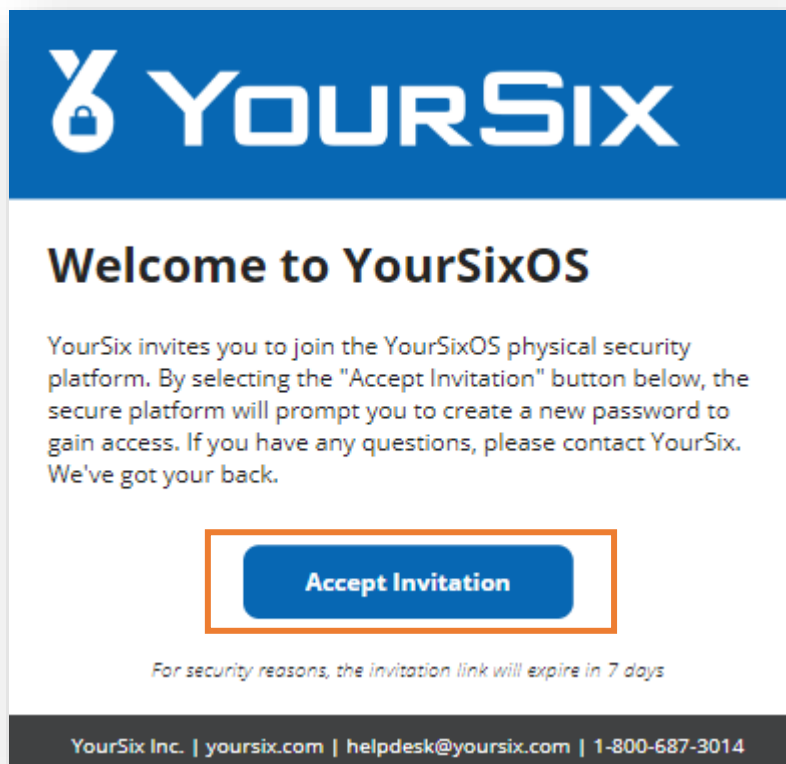
Email Invitation



Audience: Organization Super Admin, Organization Admin, Organization User

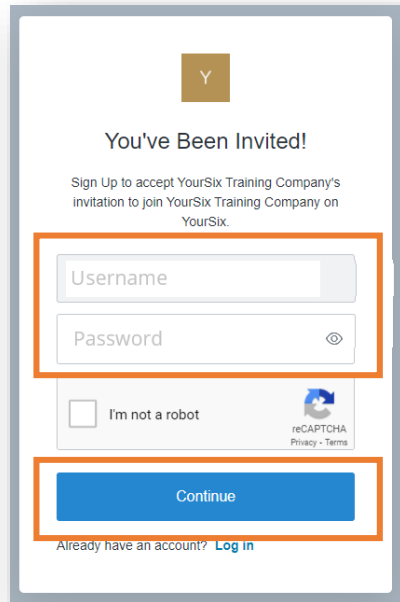
The Y6OS platform will trigger an email invitation:

- 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 sign-up form titled "You've Been Invited!". At the top, there is a brown square icon with a white letter 'Y'. Below the icon, the text reads "You've Been Invited!" followed by "Sign Up to accept YourSix Training Company's invitation to join YourSix Training Company on YourSix." The form contains several fields: a "Username" input field, a "Password" input field with an eye icon for visibility, a checkbox labeled "I'm not a robot" next to a reCAPTCHA logo, and a blue "Continue" button. At the bottom, there is a link that says "Already have an account? [Log in](#)".

Y

You've Been Invited!

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

Username

Password

I'm not a robot

reCAPTCHA
Privacy - Terms

Continue

Already have an account? [Log in](#)

Login



Audience: Organization Super Admin, Organization Admin, Organization User

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.

Email address

Password 

I'm not a robot 
reCAPTCHA
Privacy - Terms

[Forgot password?](#)

Continue

Layout

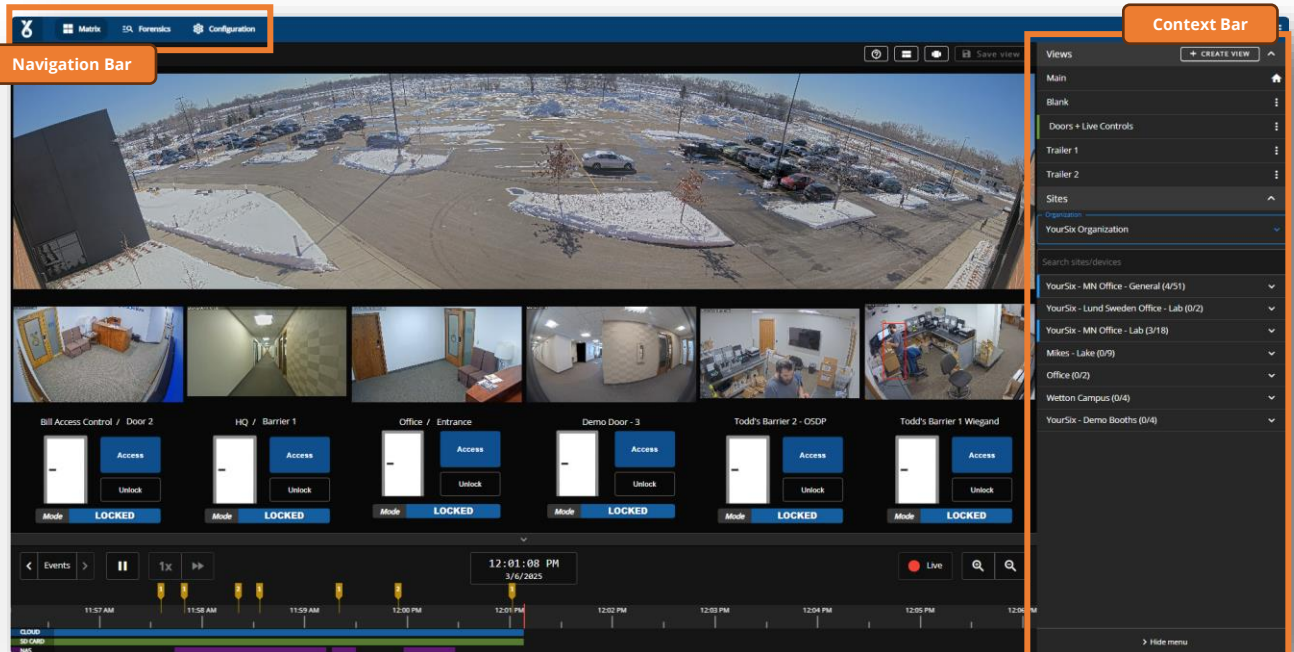


Audience: All Organizational Users



Additional Resources:

- [Basic navigation videos](#)



→ Navigation

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

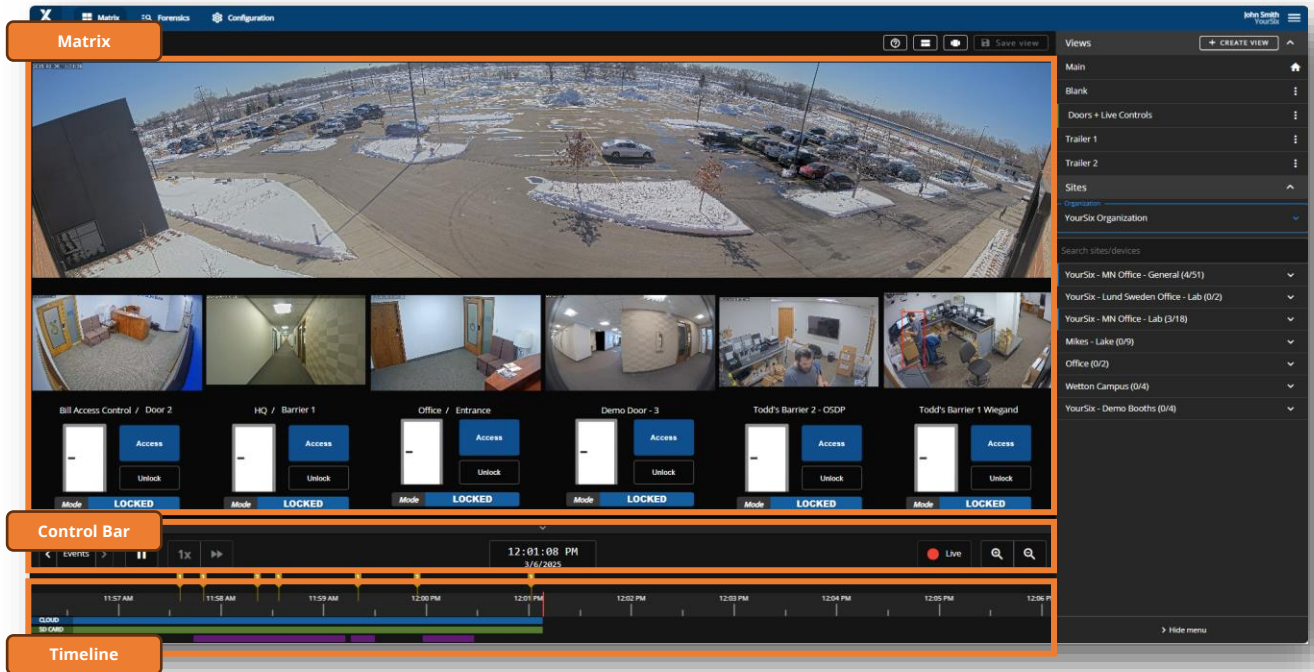
→ Context

- Favorite Views
- Views
- Sites
- Devices

Layout



Audience: Organization Super Admin, Organization Admin, Organization User



- **Matrix**
 - Video Thumbnails
 - Video Wall
 - Barriers
- **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)

Organization Functions

→ [Manage My Org \(MFA, SSO, Webhooks & Org Email\)](#)

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



Audience: Organization Super Admin

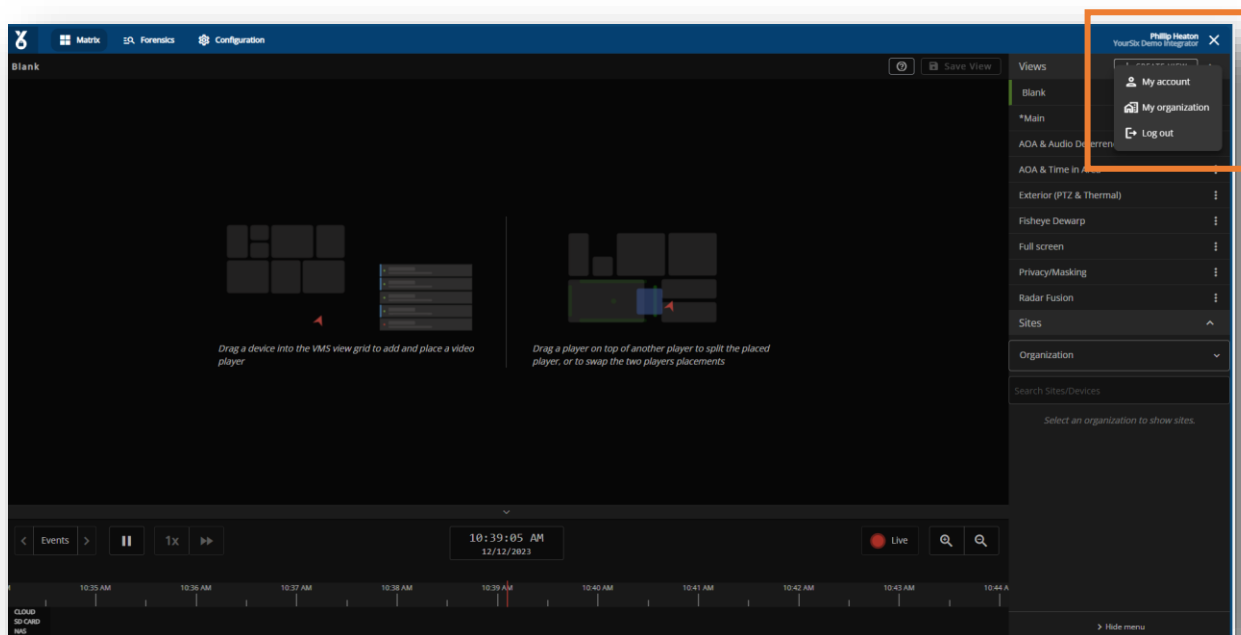


Objective: Manage Multi-Factor Authentication (MFA), Single Sign-On (SSO), webhooks & emails for an organization.



Additional Resources:

- [My Organization \(MFA, SSO, Webhooks, Organization emails\) video](#)



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

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

The screenshot displays three sections of the 'Manage My Org' interface, each with an orange border:

- Manage Organization Emails:** Shows a search bar, a '+ Add Email' button, and a table with one entry: 'Email ↑', 'phillip.heaton@yoursix.com'. It includes pagination controls showing 'Showing 1-1'.
- Manage Organization Webhooks:** Shows a search bar, a '+ Add Webhook' button, and a table with one entry: 'Name ↑', 'test', 'Url'. It includes pagination controls showing 'Showing 1-1'.
- Single Sign-on / Multi-factor Authentication:** A list of two items: 'Single Sign-on' and 'Multi-factor Authentication', each with a dropdown arrow.

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*

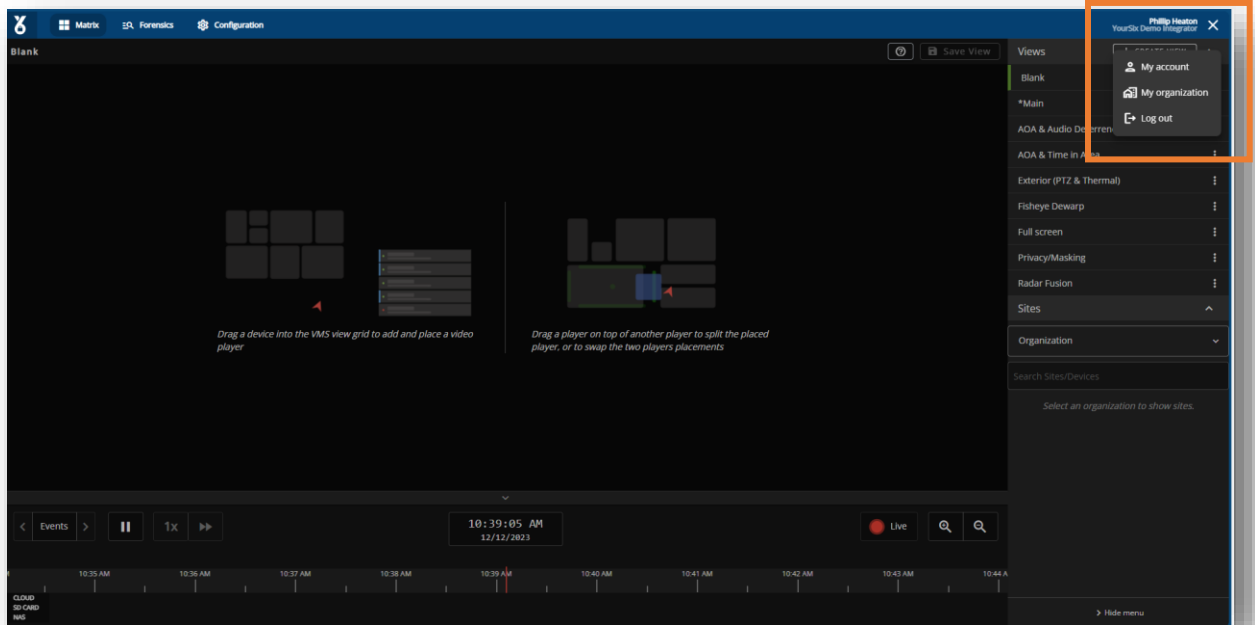
Manage My Account



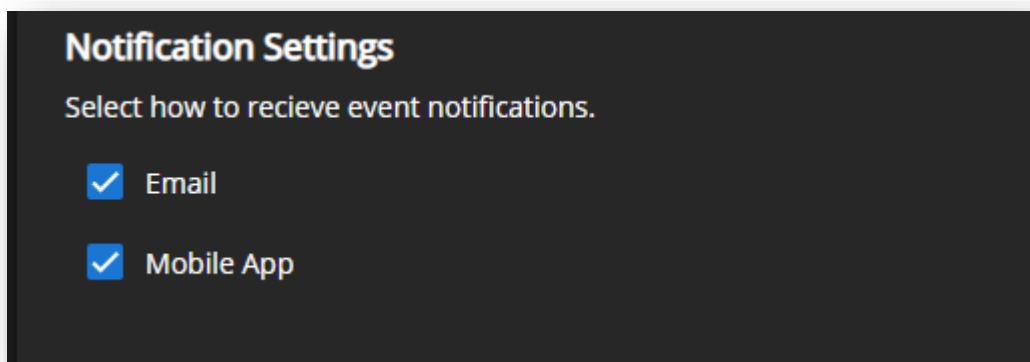
Audience: All users



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

→ [Edit Sites](#)

Edit Sites

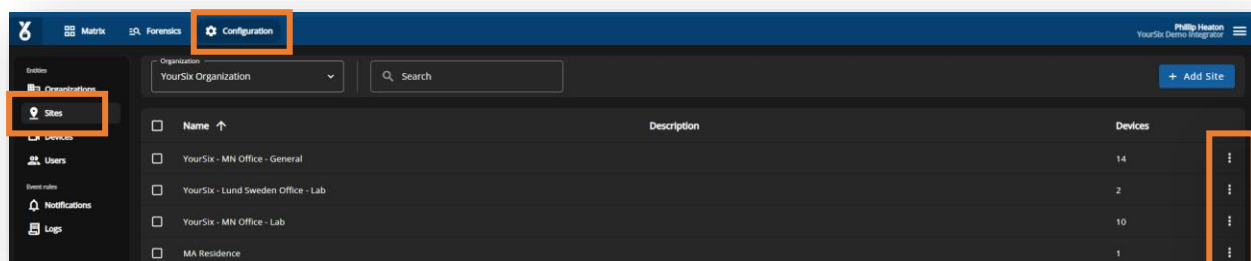


Audience: Organization Super Admin, Organization Admin



Objective: Edit below settings for a site.

- Name
- Time Zone
- Add User
- Device Groups & Central Station access (Refer to full central station guide)
- 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 →→→

Edit 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](#)

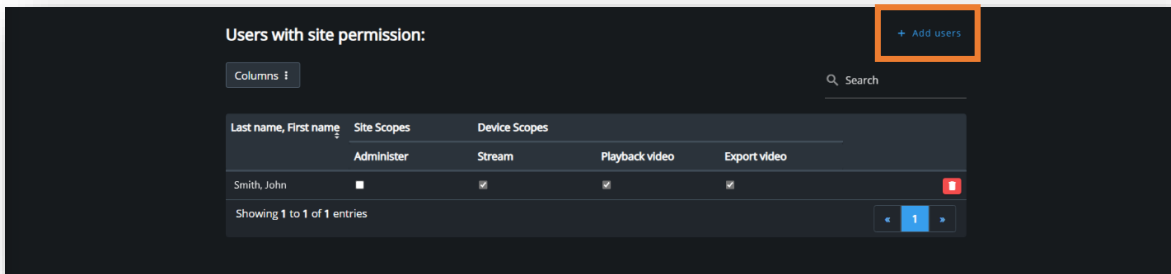
Last name, First name	Site Scopes	Device Scopes	
Smith, John	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

Showing 1 to 1 of 1 entries

Edit Site User Permissions:

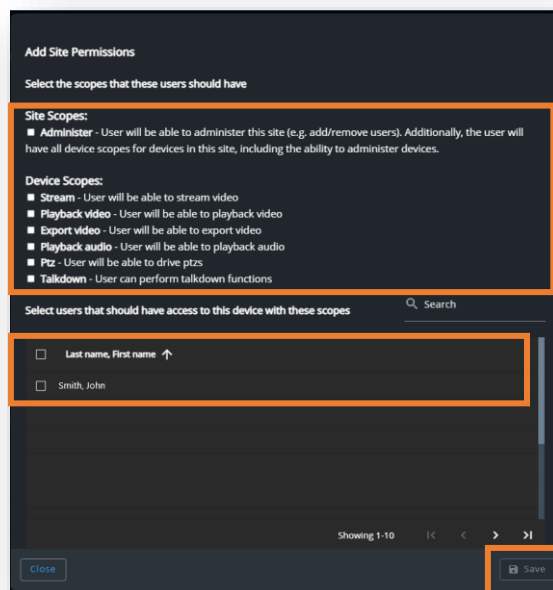
- Locate the [User With Site Permissions](#) and expand
- Select appropriate user [Permissions](#)
- Select [Save](#)
- Users can be deleted by selecting the [Trash Can Icon](#)
- Continue to next page →→→

Edit 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: Organization Super Admin, Organization Admin

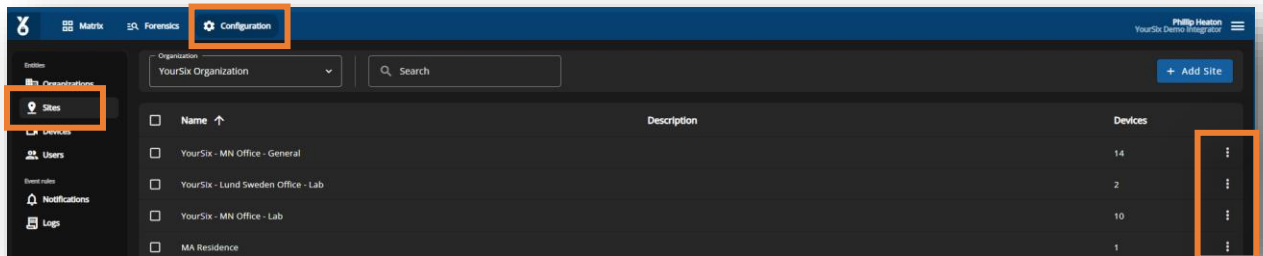


Objective: Create and manage device groups which may be used for notifications.



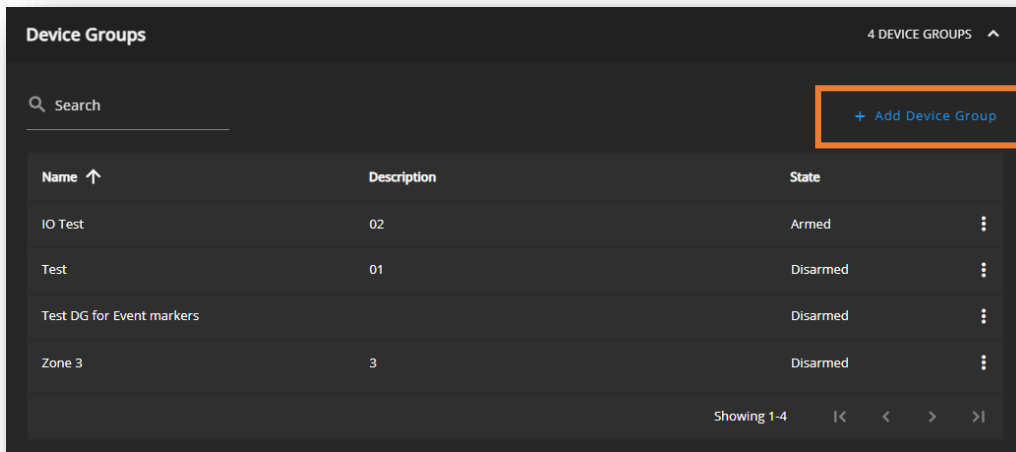
Additional Resources:

- [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:

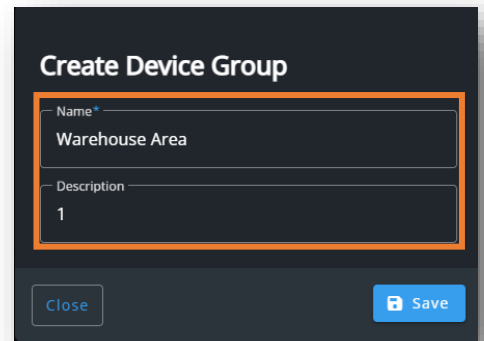
- On the edit site page select locate and expand the Device Group section [Add Device Group](#)

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

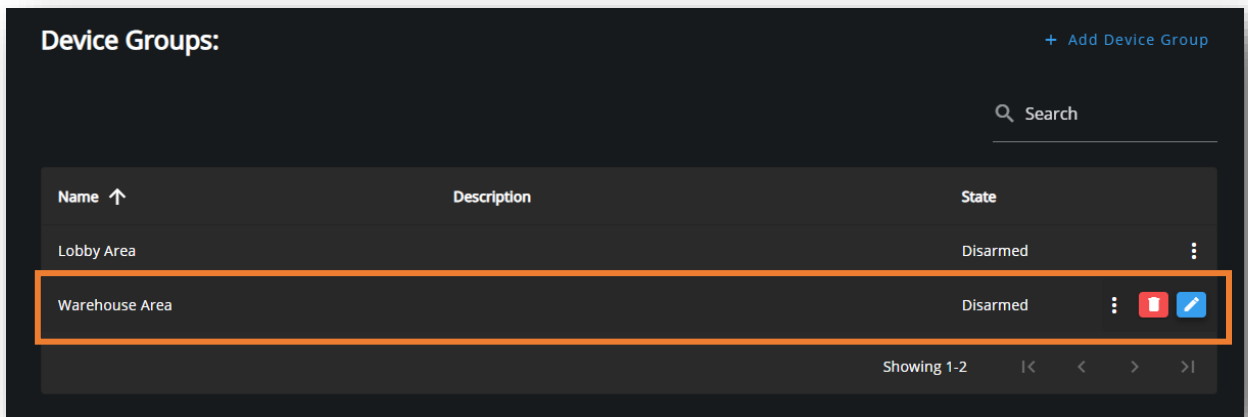
- Within the popup menu, name the device Group and enter the description (zone number)
 - Enter **Name**: Vanity name you wish to call the group
 - Enter **Description**: Zone number (matches the ID of the Zone Number)

- Select [Save](#)

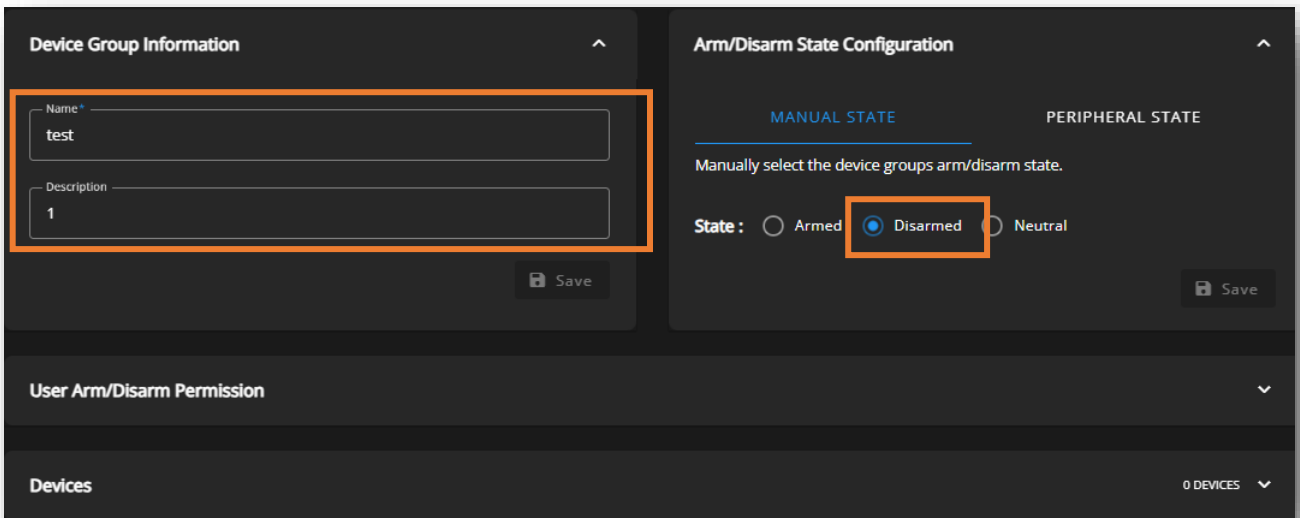
- Continue to the next page → → →



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](#).

Create Schedules

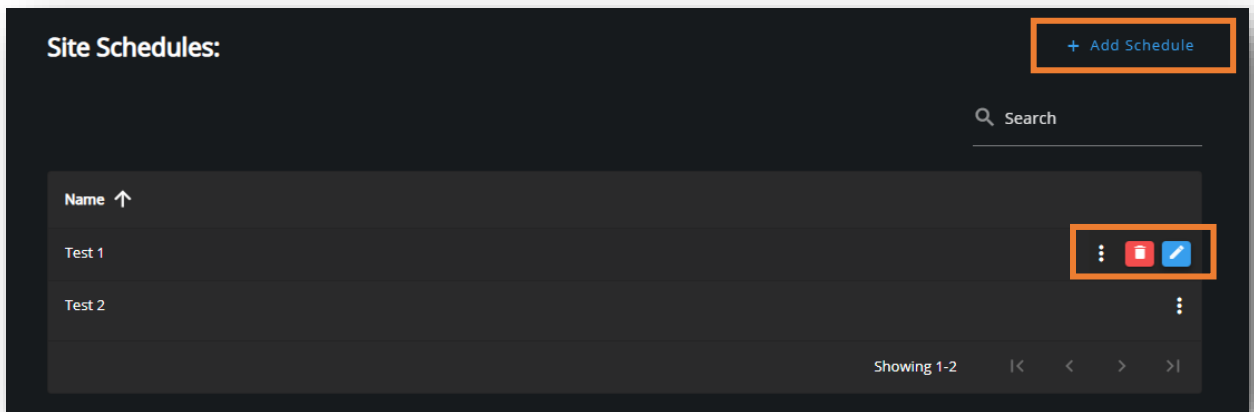


Audience: Organization Super Admin, Organization Admin



Objective: Edit & create schedules.

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

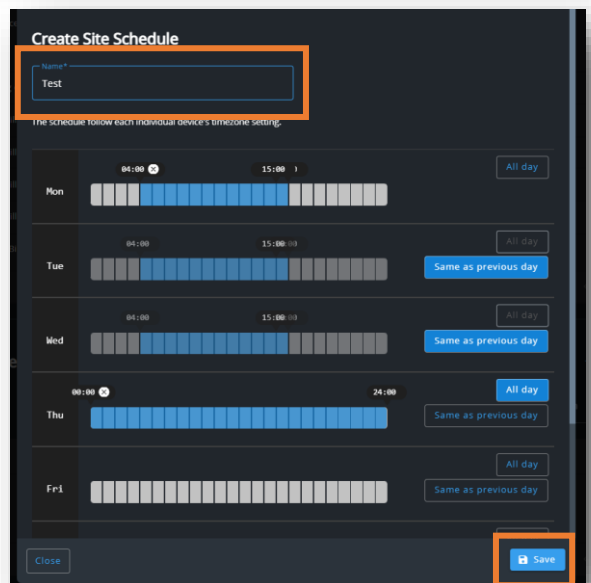


Edit Schedule:

- 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**



Devices

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

Manage Devices

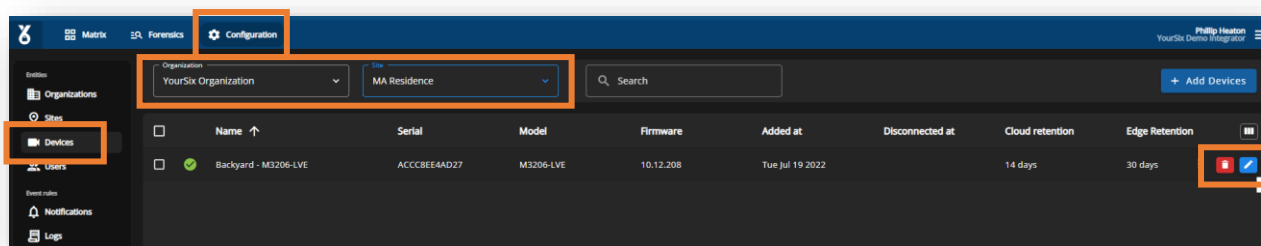


Audience: Organization Super Admin, Organization Admin



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

- Check model, firmware, serial number
- Access or reboot the device
- Create & configure device rules
- Create & configure user device permissions
- Manage applications on device
- Manage audio configuration
- Assign device to a device group
- Edit Event Retention



- 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: P3245-LVE Firmware: 11.0.93 Serial: Added at: Tue Sep 20 2022

Site: Branch Device Name: Phil

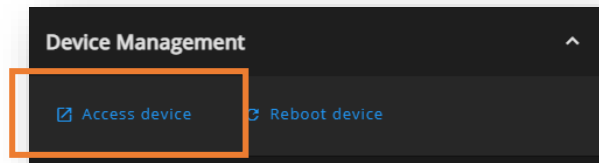
Device Description/Notes Event Retention: 30 Days

Timezone: Site's timezone (default) Device Group

Save

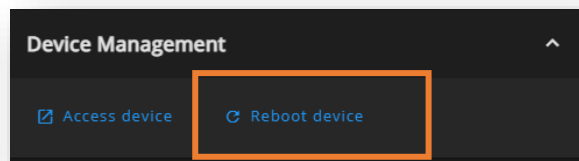
- View [Device Model, Firmware, Serial Number & Date Added](#) at the top of the page
- Edit the following information about the device:
 - [Organization](#)
 - [Site](#)
 - [Device Name](#)
 - [Device Description](#)
 - [Time Zone](#)
 - [Device Group](#)
 - [Events Retention \(guide\)](#)
- Select [Save](#)
- Continue to next page →→→

Manage Devices



Access the Device Interface:

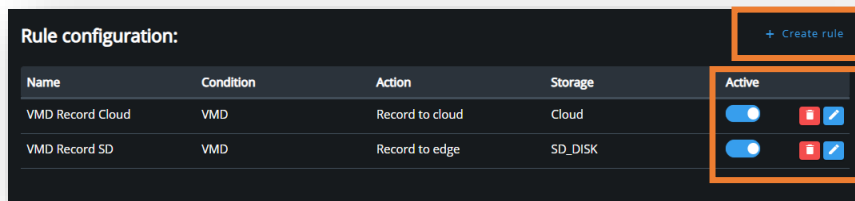
- Locate the Device Management section on the Manage Device page
- Select [Access Device](#) to view the device live feed and access the direct device interface:
 - Image settings
 - Stream settings
 - Overlay settings
 - Audio settings
 - PTZ settings
 - Privacy Mask settings
 - Application settings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







Reboot the Device:

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

Manage Devices



Name	Condition	Action	Storage	Active
VMD Record Cloud	VMD	Record to cloud	Cloud	<input checked="" type="checkbox"/>  
VMD Record SD	VMD	Record to edge	SD_DISK	<input checked="" type="checkbox"/>  

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: Organization Super Admin, Organization Admin



Objective: Create a new action rule for a device.



Additional Resources:

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

The screenshot shows the 'Training Rule' configuration interface. It is divided into three main sections: Sources, Trigger, and Action. The Sources section includes options for Overview, Panorama, Double Panorama, Quad View, View Area 1-4, and Corner Left/Right/Double Corner/Corridor. The Trigger section includes Schedule (VMD) and Select profile (Any Profile, Profile 1). The Action section includes Record to cloud and Record to Edge SD, with fields for Prebuffer (10), Postbuffer (10), Frame rate (8), and Resolution (720x720). A Save button is visible at the bottom right.

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: + Add Site Schedule

Always Test 1 Test 2

Action:

Record to cloud Record to Edge SD

Frame rate: 8 Resolution* 720x720

Close Save

Additional Device Management



Audience: Organization Super Admin, Organization Admin



Objective: Edit new & existing devices.

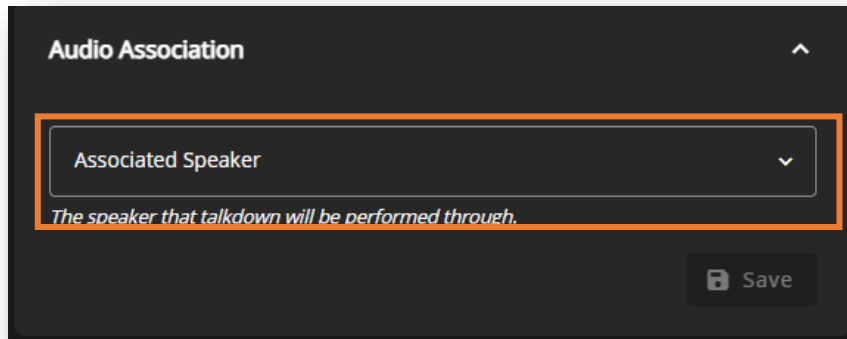
Last name, First name	Administer	Stream	Playback video	Export video	
Smith, John	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Williams, James	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<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
- Continue to next page →→→

Edit Devices

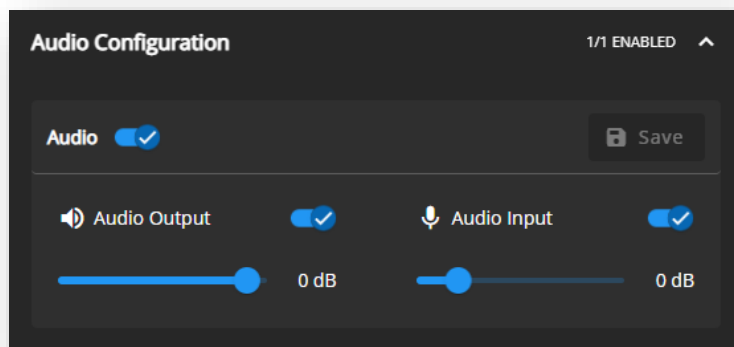


Audio Association:

→ Select the [Associated Speaker](#)

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

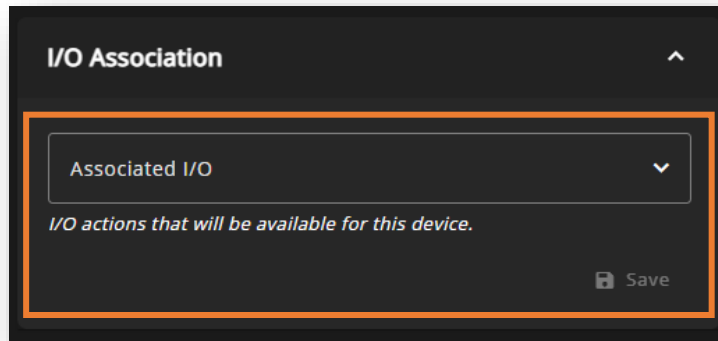
→ Select [Save](#)



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](#)

Edit Devices



I/O Association:

- Select the [Associated I/O](#)
- Select [Save](#)

Access Control

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

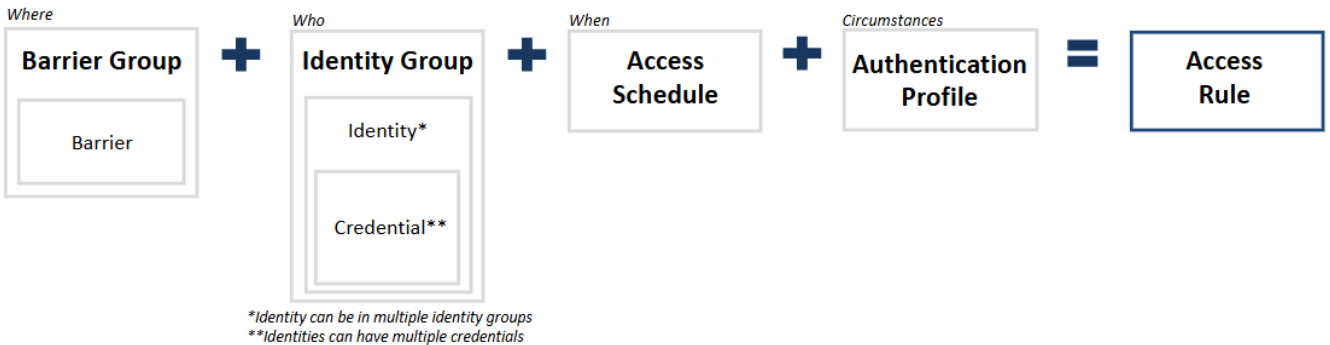
Access Control Overview

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 *(Must be completed by the integrator)*
2. Add Barriers + Configure Barriers *(Must be completed by the integrator)*
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 Barrier Groups



Audience: Administrators of the Organization

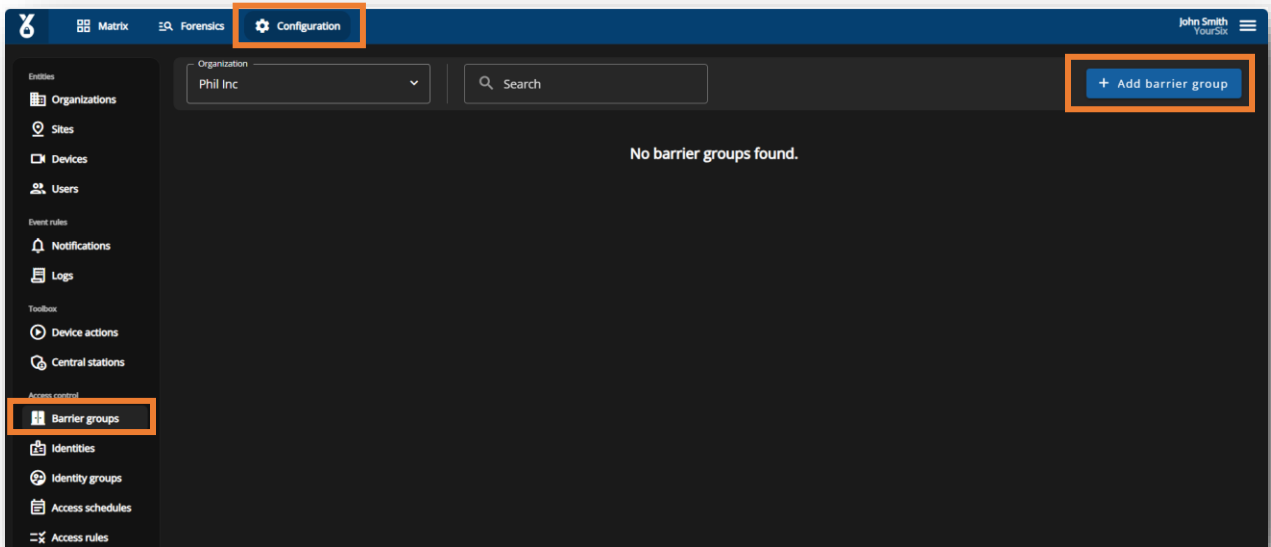


Objective: Add barriers to barrier groups. Barrier groups allow for the simultaneous configuration of the barriers when using access rules.



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 →→→

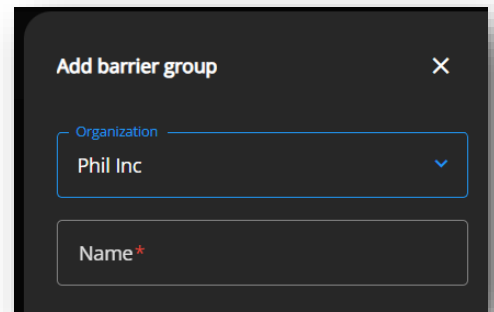
Important Note

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

Add Barrier Groups

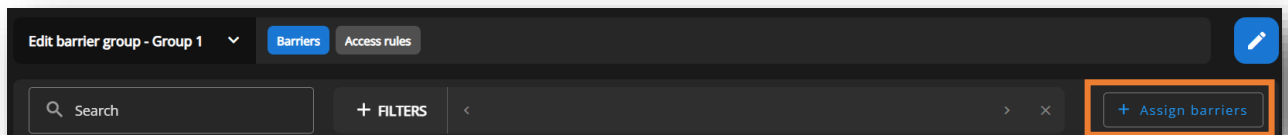
Add barrier group

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

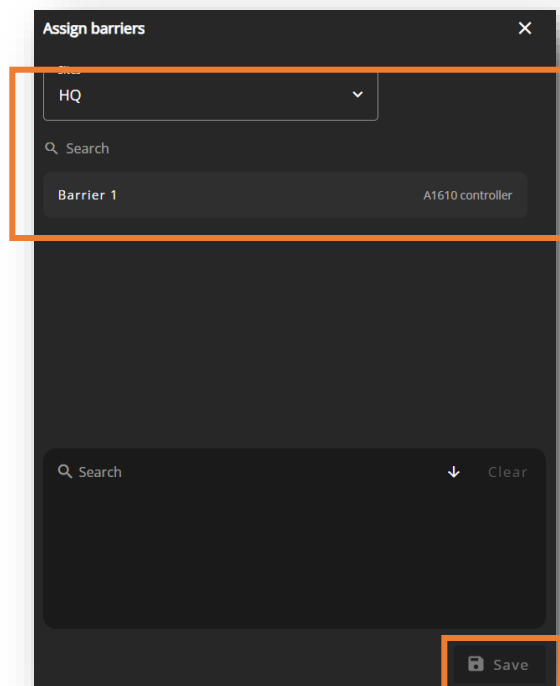


Assign barriers to the group

- 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: Administrators of the Organization

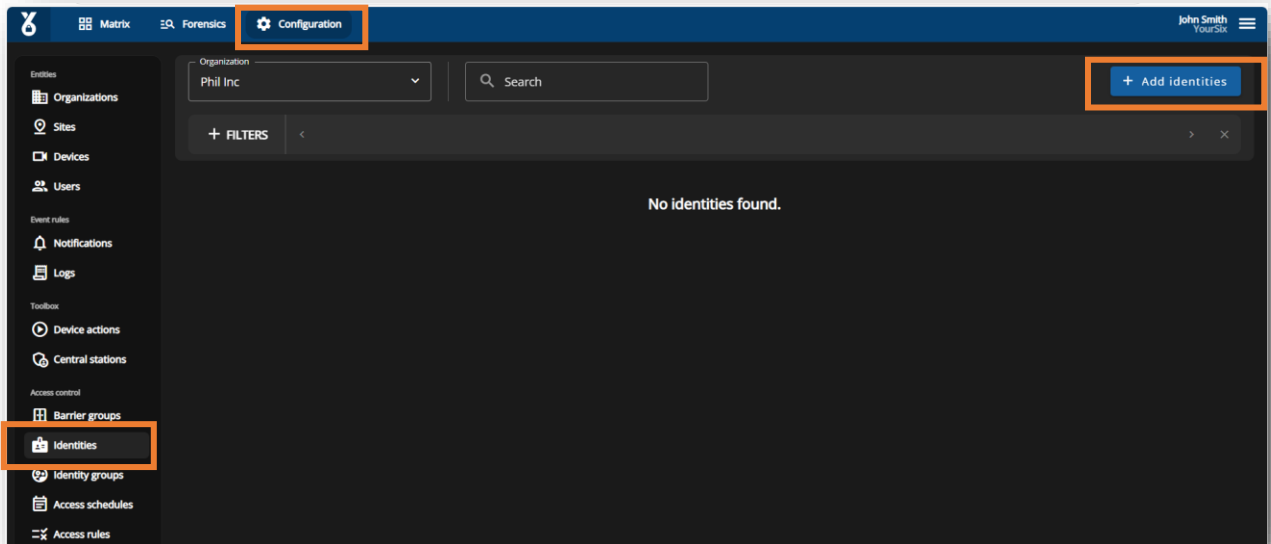


Objective: Add identities and credentials. An identity is an individual in the access control domain, whom is in possession of a credential.



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: Administrators of the Organization

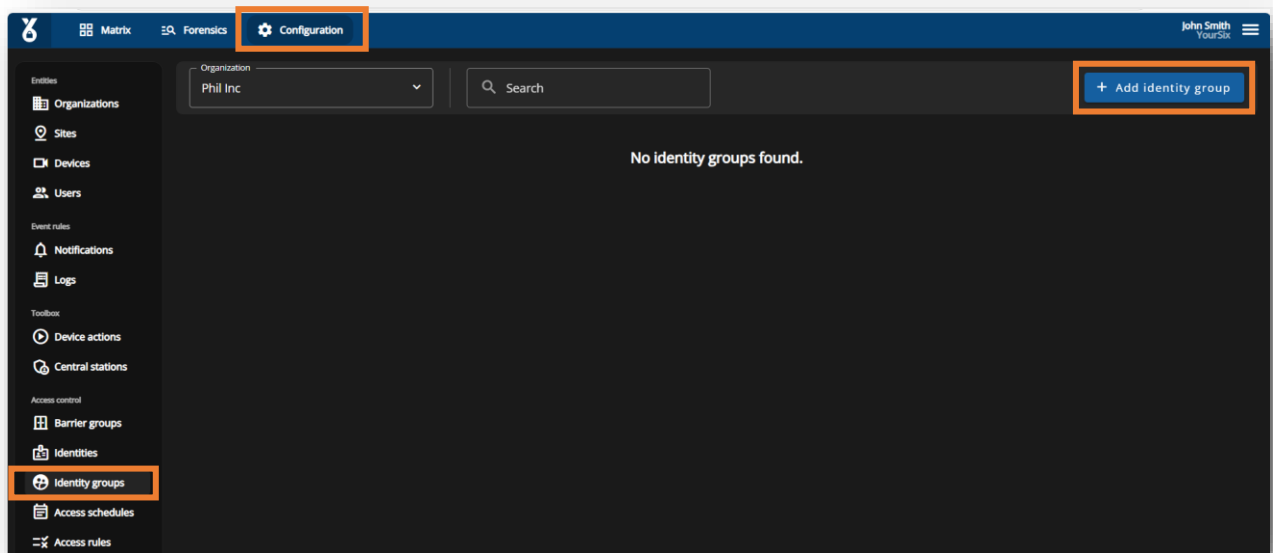


Objective: Add identity groups. Identity groups are a group of identities that allows for simultaneous configuration of access using access rules.



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 →→→

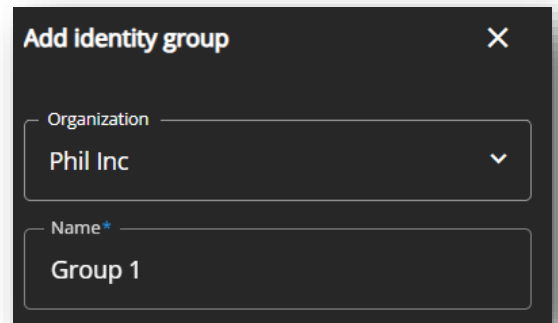
Important Note

- 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



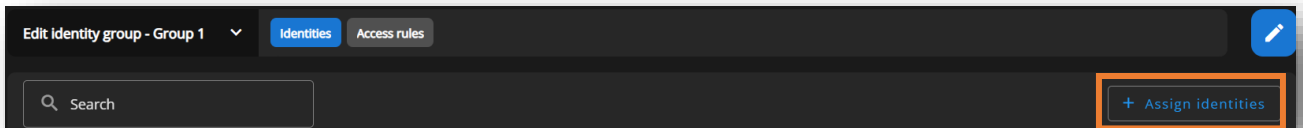
Add identity group [X]

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

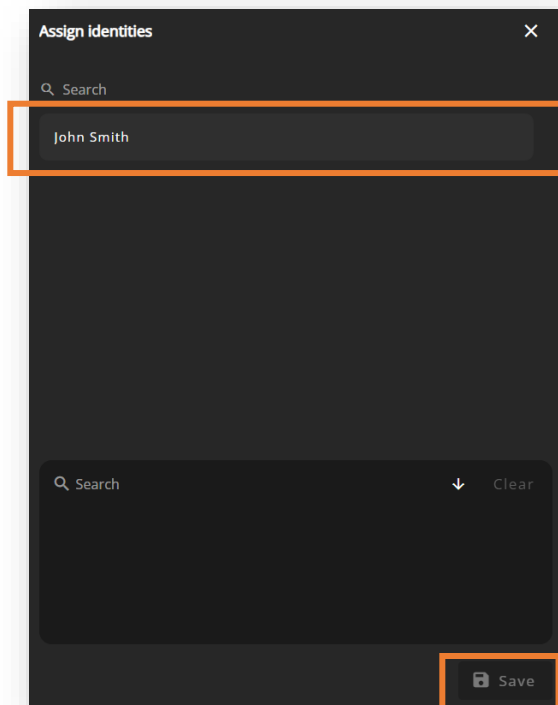


Edit identity group - Group 1 [v] [Identities] [Access rules] [Edit]

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: Administrators of the Organization

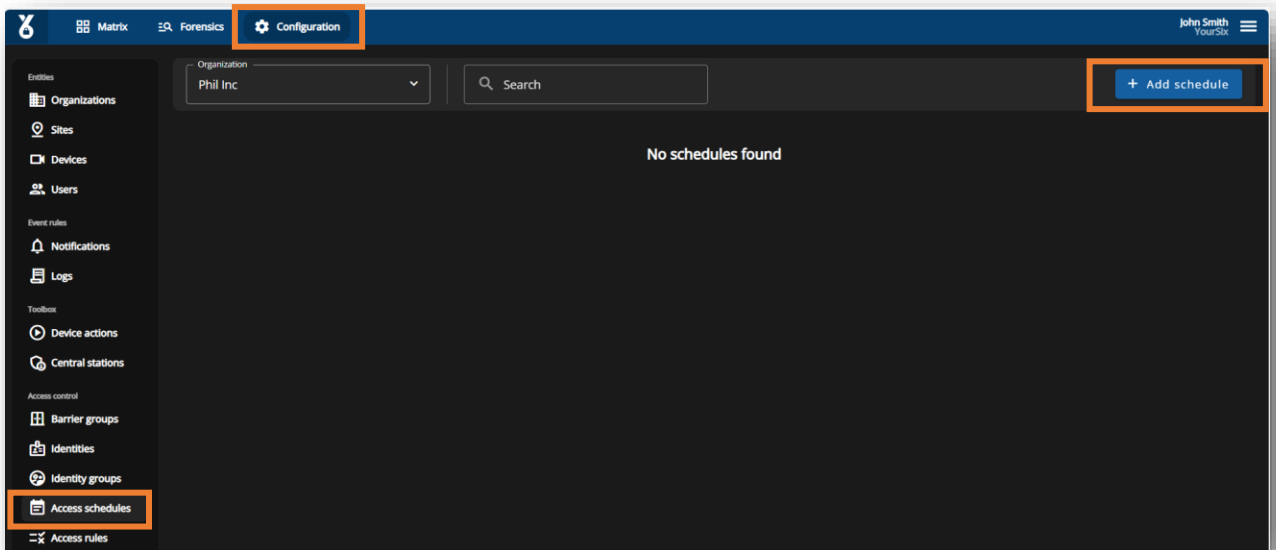


Objective: Add access schedules. An access schedule will be used as the “when” in granting access.



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 a dark-themed dialog box titled "Add schedule". At the top, 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, one for each day of the week (Mon to Sun). Each row contains a horizontal grid of 24 small squares representing time slots. To the right of each grid is a button labeled "All day". For Tuesday through Sunday, there is also a button labeled "Same as previous day".

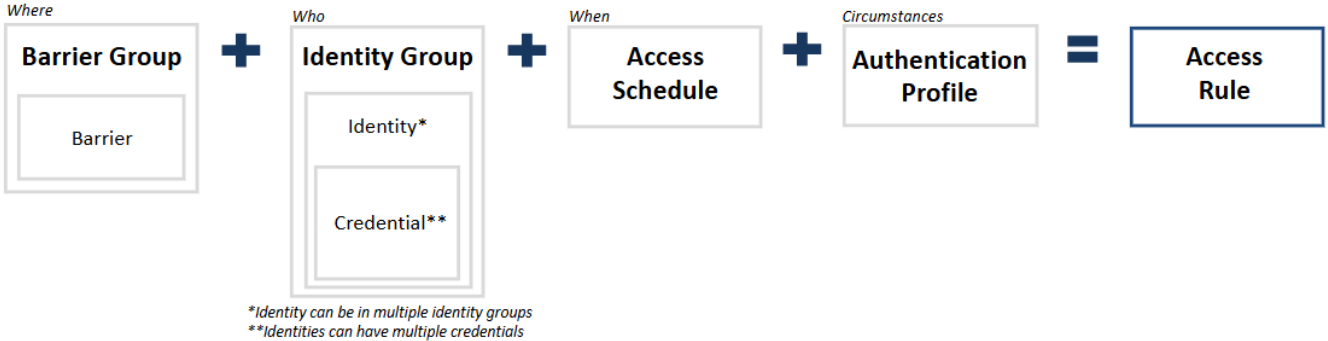
- Name the schedule
- Select the **Frequency** (Weekly or one-time)
 - Weekly: Reoccurring schedule that is standard each week
 - One-time: One-time schedules based on certain dates
- Confirm **Organization**
- Select the desired time windows that make up the schedule
 - *Important note: If a REX is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

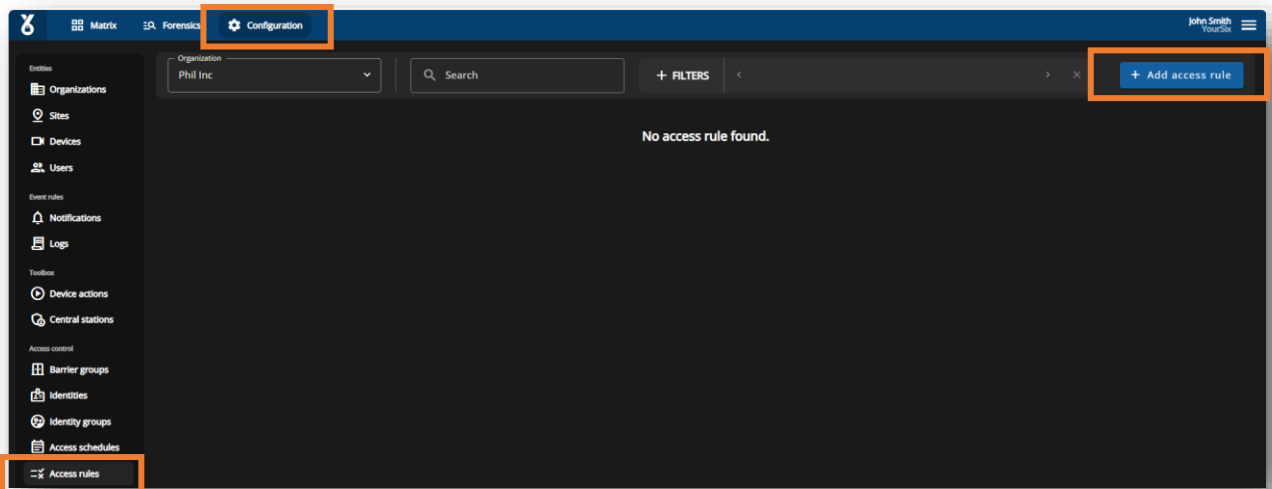


Objective: Create access rules. Access rules utilize the previous created components to specify who is permitted to enter, where, when, and under what circumstances.



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' dialog with the following configuration:

- Organization: Phil Inc
- Name: Card for entry
- Barrier group: Group 1
- Authentication profile: Card
- Identity group: Group 1
- Direction: In
- Schedule: work hours (Monday-Friday, 9:00-17:00)

A blue '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' dialog with the following configuration:

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

A blue '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' dialog box. 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' are highlighted in blue.

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

Forensics

- Events
- Access
- Objects
- Exports

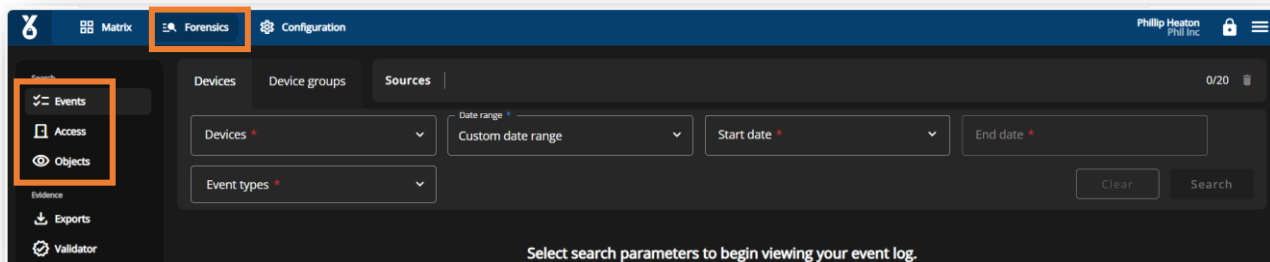
Events



Audience: Organization Super Admin, Organization Admin

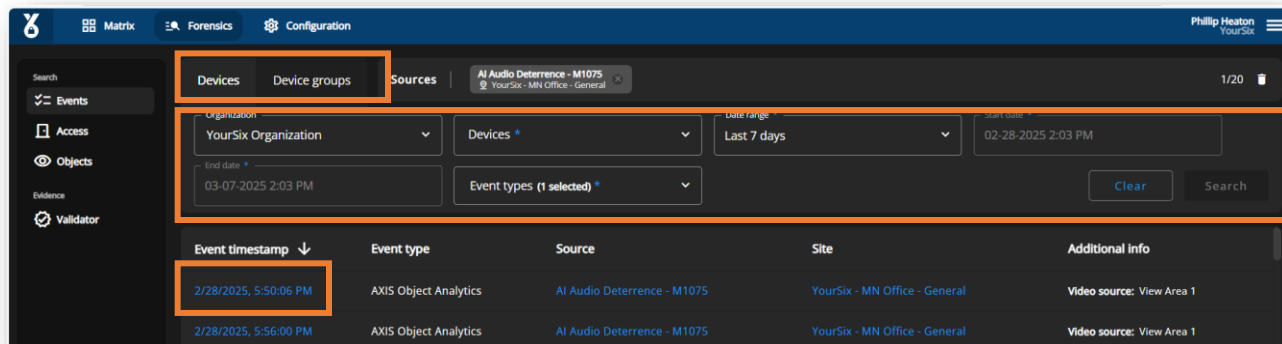


Objective: Search for events, access events, and objects



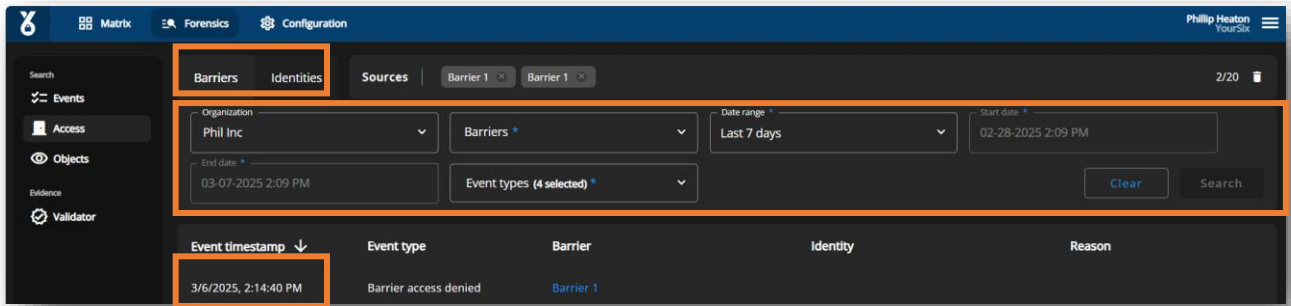
- Select **Forensics** located on the navigation bar
- Along the left menu, select the desired search tool from the following options
 - **Events**: Search for events by type (e.g. AOA or VMD)
 - **Access**: Search for access events by barrier or identity
 - **Objects**: Search for humans or vehicles with the option to search by color
- Continue to next page →→→

Event Search



- Select the desired search criteria:
 - [Device](#) or [Device groups](#)
- Complete the search details:
 - [Organization](#)
 - [Devices/Device Groups](#)
 - [Date Range](#)
 - [Event Types](#)
- Select [Search](#)
- Once results are presented, users can select the text in blue font in order to view the [recorded footage](#) on the matrix (if footage is available based on recording rules)

Access Search



- Select the desired search criteria:
 - **Barriers** or **Identities**
- Complete the search details:
 - **Organization**
 - **Barriers/Identities**
 - **Date Range**
 - **Event Types**
- Select **Search**

Object Search



Additional Resources:

- [Object Appearance Search](#)

→ Select the desired search criteria:

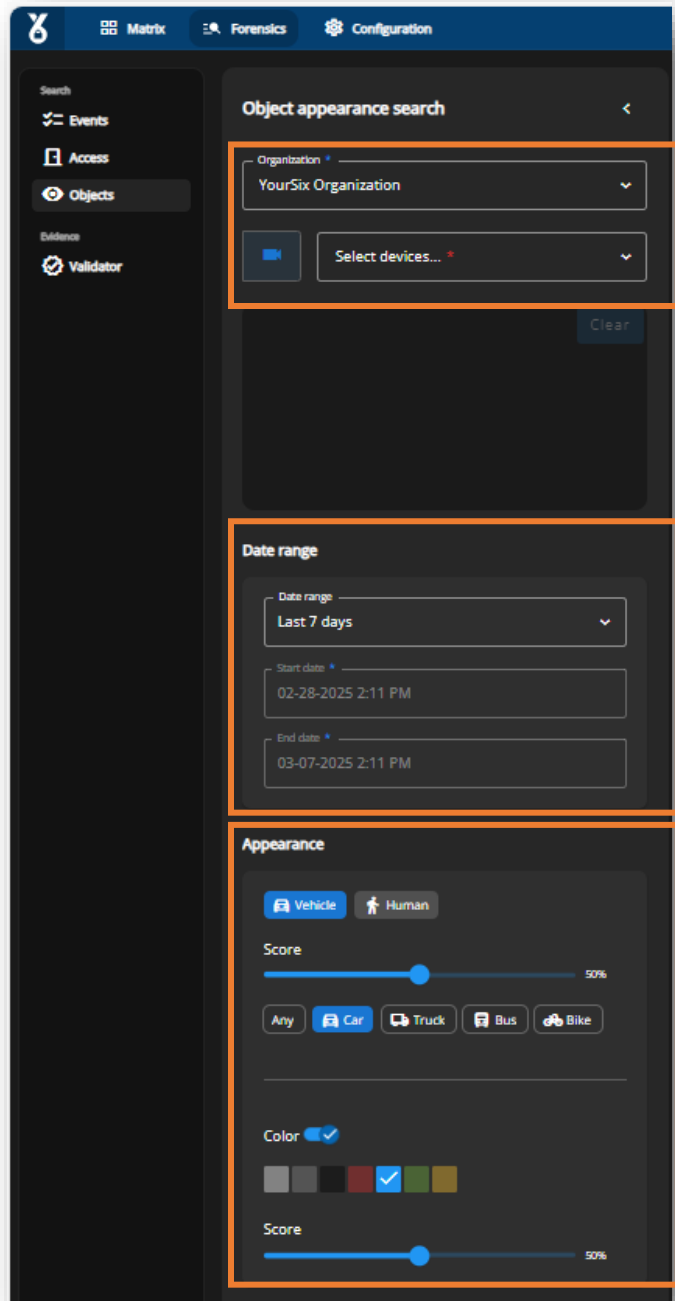
- **Organization**
- **Devices** (Sites can be searched by typing in the name of the site in the device field and then selecting the devices at the site)

→ Complete **date range** information

→ Select the **Appearance** information

- Class: Human or vehicle
- Vehicle Class: Car, truck, bus, bike
- Color: Vehicle color and human upper and lower body clothing color
- Score: the confidence level of the results. The higher the score setting, the stricter the system will be on Class and Color accuracy.

→ Select **Search**



Export Video



Audience: Organization Users

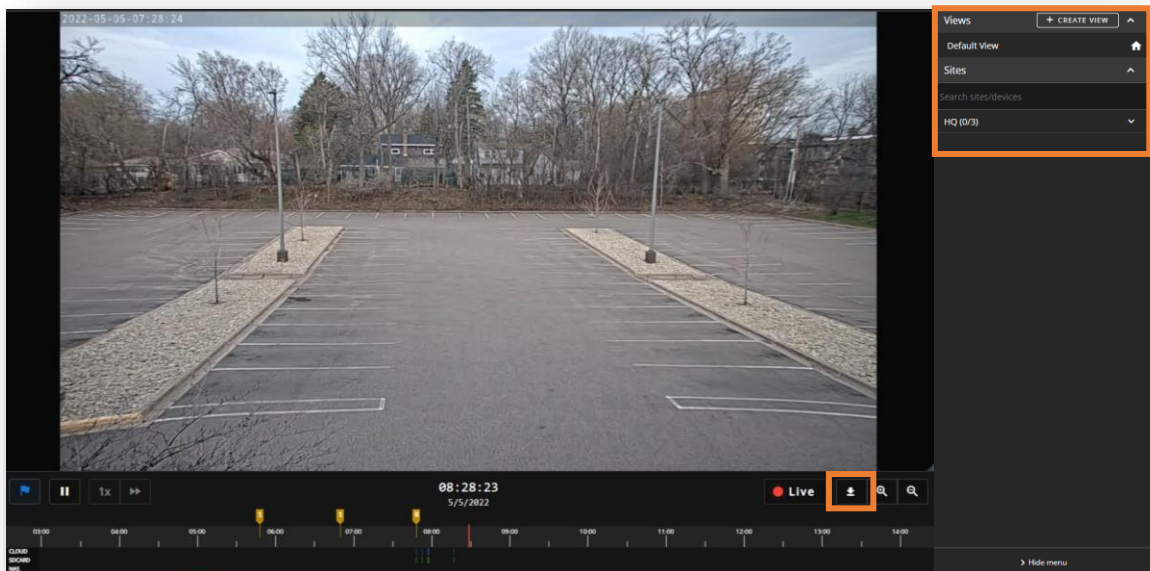


Objective: Creating an export from the Matrix



Additional Resources:

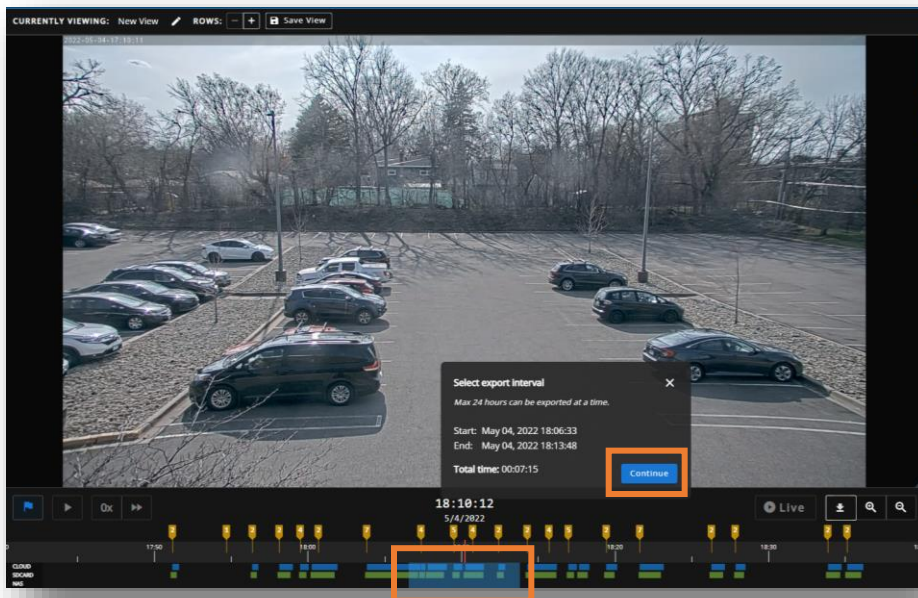
- [Exports training](#)



The YourSixOS platform can export 24 hours of footage at a time, from up to 8 devices.

- From the matrix, locate the device you wish to export footage from along the right [Context Bar](#)
- [Add](#) the device to the matrix
- Use the timeline controls to locate the footage you wish to export
- Select the [Export Icon](#) located above the timeline to the right
- Continue to next page →→→

Export Video



- Once you click the export icon, a popup box will appear above the timeline. This box will indicate the details of your export
- In the middle of the timeline a **Blue Shaded Box** will appear on the time frame that will be exported
- Users can drag and drop this box along the timeline or drag the margins to increase/decrease the length of the export
- Once the desired timeframe has been selected and appears in the popup box, select **Continue**
- Continue to next page →→→

Export Video

Export Video

Creating an export will start a job that bundles your footage into a zipped folder for download. Exports and their statuses can be found on the "Exports" page.

Description *

New incident in Parking lot

Start Date: * 2022-05-04 18:04:49 End Date: * 2022-05-04 18:12:03

Length of exported footage: 00:07:14

Storages *

Cloud x

St. Paul Office

1 of maximum 8 devices selected. Search

	Name ↑	Serial
<input type="checkbox"/>	Booth Demo 01	ACCC8EE0B9E5
<input type="checkbox"/>	P3727-PLE	B8A44F283774
<input type="checkbox"/>	Front Hall	ACCC8ED2B0CB
<input type="checkbox"/>	Office Ceiling Speaker	ACCC8E876DFD

Close Export Footage

- After selecting continue, a new popup menu will appear. This contains full details of the export
- In the **Description** field add information for you to identify the export
- Confirm the start and end time/date
- Select the **Storage Location** to export from (Cloud, SD card, NAS)
- Confirm or **Select Additional Device** to export footage from
- Select **Export Footage** at the bottom of the popup

A new case (export file) has now been created and can be locate in the Forensics section along the top navigation menu. Cases/Exports are kept for 90 days

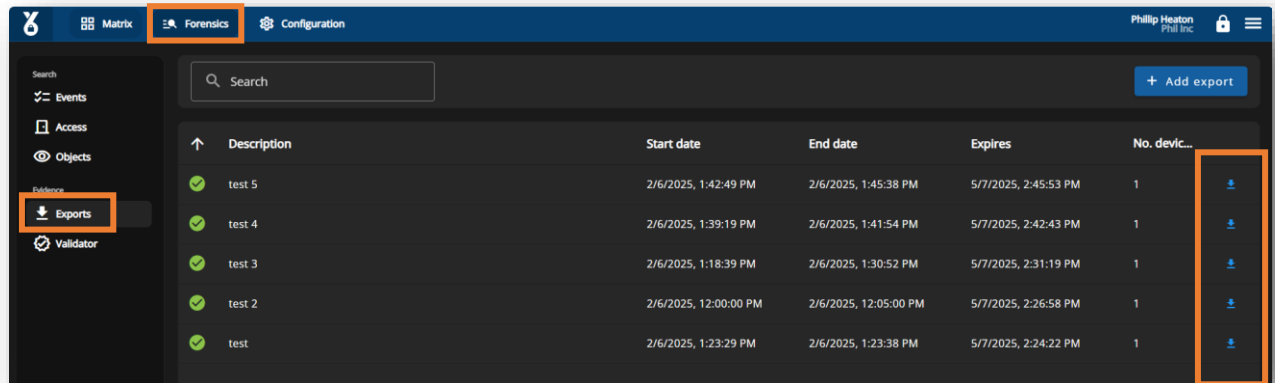
Export List



Audience: Organization Users



Objective: Viewing and downloading exports



- Select the **Exports** icon on the navigation menu
- From the list of created exports, select the **Download** icon to the right. This will download the export to your device

Users can also create an export from the export tab by selecting Add Export in the upper right corner

Alert Status

Alert State



Audience: Organization Users



Objective: View status and set the alert state for device groups



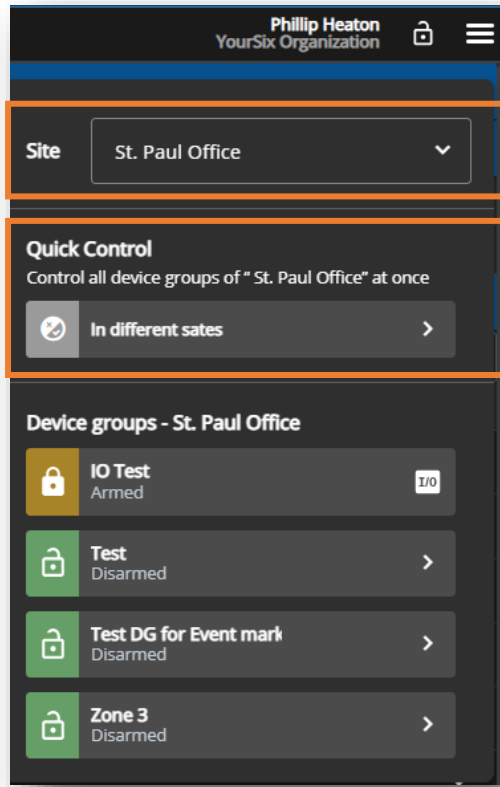
Additional Resources:

- [Alert State and Device Groups training](#)



- From the VMS screen select the [Lock Icon](#) in the upper right corner of the screen
- Continue to next page →→→

Alert State



- Within the popup window you can see the state of device groups
- Use the [Site](#) dropdown to select the desired site
- The Quick [Control section](#) will allow you to set the status for all device groups at the site
- The lower portion will allow you to set the status of individual device groups
- Use the controls to set the device groups to [Neutral](#), [Armed](#), or [Disarmed](#).
 - Neutral means the notification schedule will be followed
 - Armed means the device group is armed (ignores the schedule)
 - Disarmed means the device group is disarmed (ignores the schedule)



Users

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

Manage Users

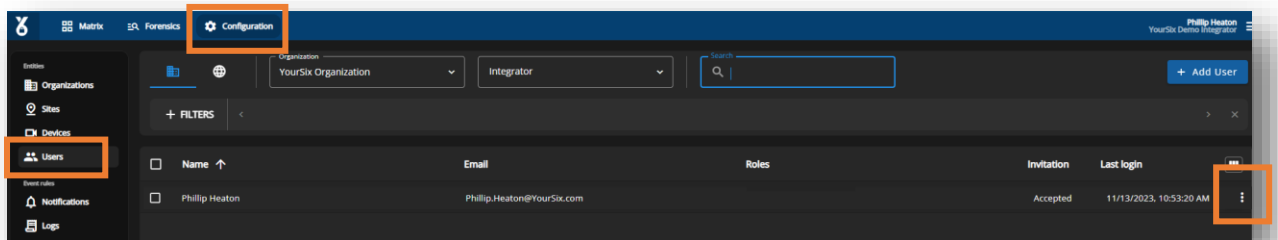


Audience: Organization Super Admin, Organization Admin



Objective: Manage users.

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



- 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: Organization Super Admin, Organization 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

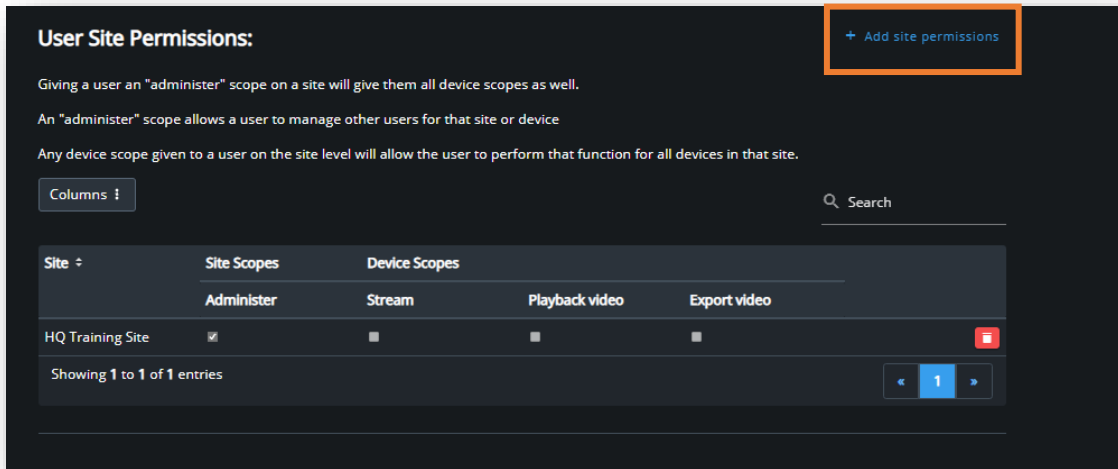
User's global roles within system.

Send password reset email Save

Basic User Information:

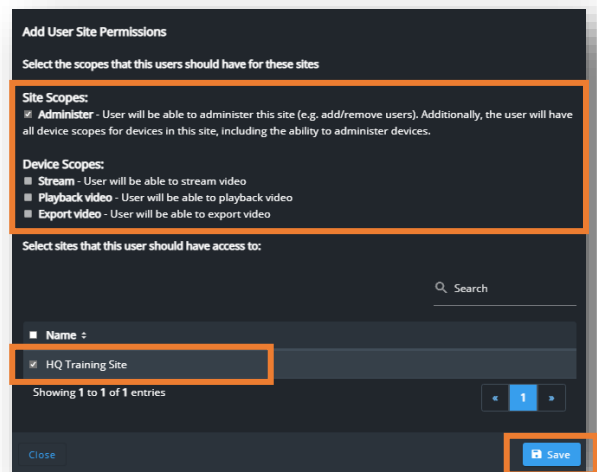
- Enter user [First Name](#) and [Last Name](#)
- Select or remove [Permissions](#)
- Select [Save](#)
- Continue to next page →→→

Edit a User

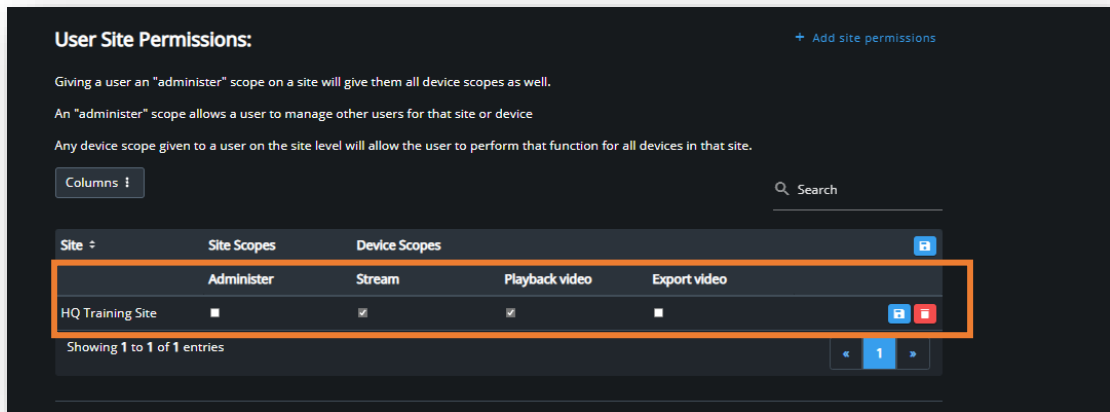


Add Site Permissions:

- 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 →→→



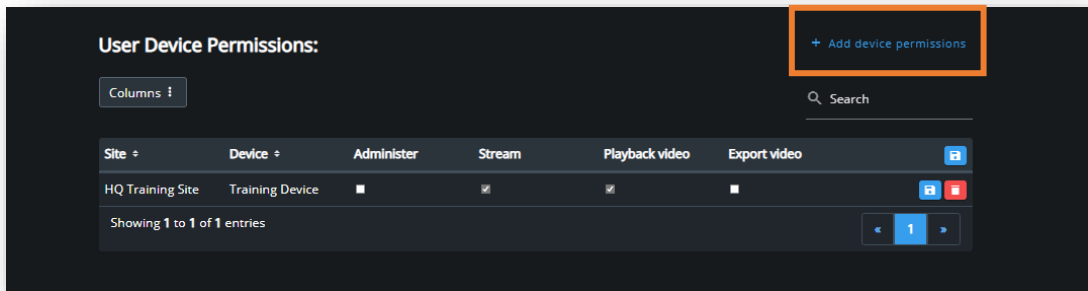
Edit a User



Edit Site Permissions:

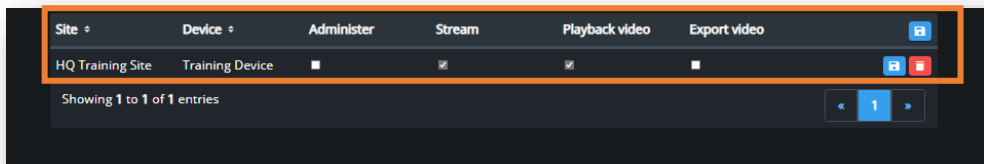
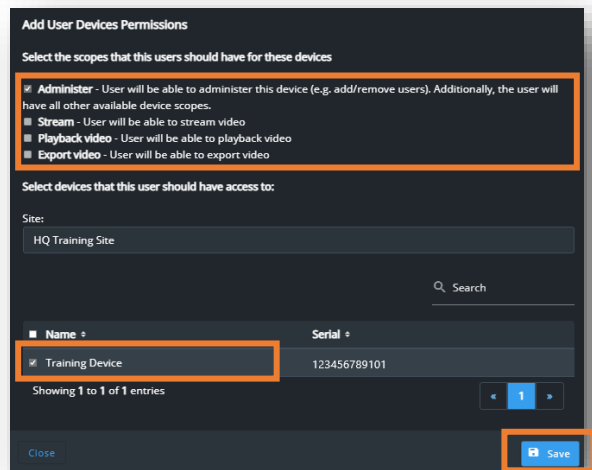
- Select the desired [Site Scopes](#) or [Device Scopes](#)
- Select the [Save Icon](#)
- *To delete a site permission, select the [Trash Can Icon](#)*
- Continue to next page →→→

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](#)*

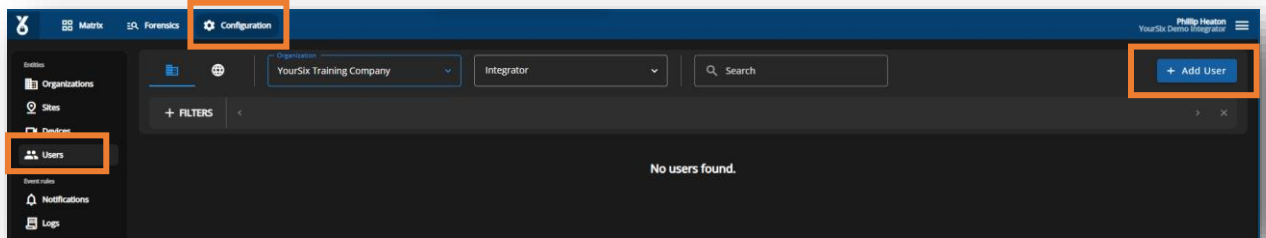
Add Users



Audience: Organization Super Admin, Organization Admin



Objective: Add new users to an organization



- 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

The screenshot shows a dark-themed 'User Information' form. At the top left is an information icon and the title 'User Information'. Below the title are two main sections: 'Account Details' and 'Account Roles'. The 'Account Details' section contains three input fields: 'First Name *', 'Last Name *', and 'Email *'. The 'Account Roles' section contains a dropdown menu labeled 'Roles *' with a downward arrow, and a sub-label 'User's global roles within system.' below it. A 'Save' button with a floppy disk icon is located in the bottom right corner. Orange rectangular boxes highlight the 'Account Details' and 'Account Roles' sections, and the 'Save' button.

- 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](#)
- Continue to next page →→→

Add User Device and Site Permissions

The screenshot displays a dark-themed interface for configuring user permissions. It is divided into three main sections, each with a title, a count of items, and a description. Each section also includes a button to add permissions.

- Device Group Permissions:** Shows 0 GROUPS. Description: "Device groups that the user will be able to arm/disarm." Status: "The user doesn't have access to any device groups." Button: "+ Add device group permissions".
- Site Permissions:** Shows 0 SITES. Description: "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 on that site." Status: "No site permissions set." Button: "+ Add site permissions".
- Device Permissions:** Shows 0 DEVICES. Status: "No device permissions set." Button: "+ Add device permissions".

→ After a user is added to the platform then Admin's can assign [Site](#), [Device](#), and [Device Group](#) permissions. ([User Permissions](#)).

Events

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

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

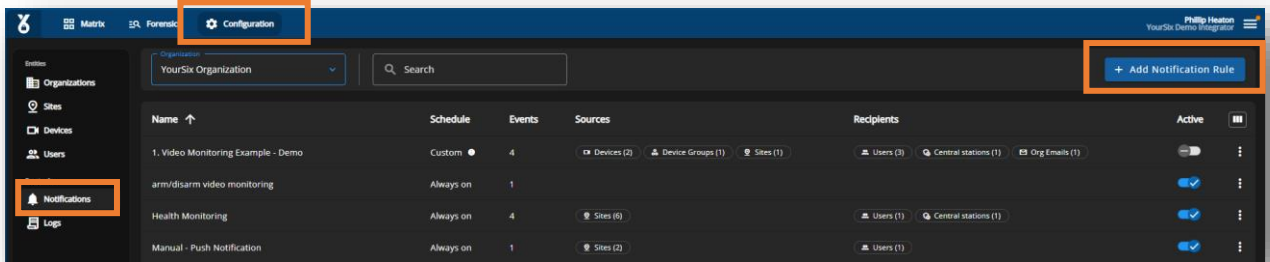
Create Notifications



Audience: Organization Super Admin



Objective: Create a notification rule.



- 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

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.

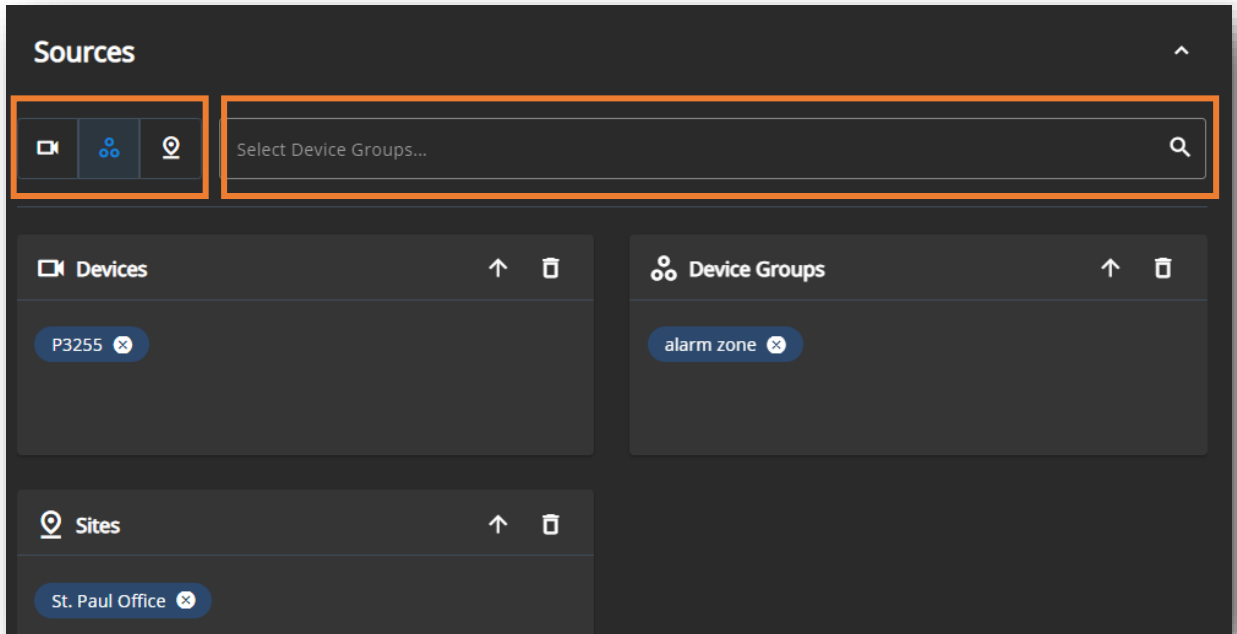
In this example the rule is set to be active from 6 PM to 8 AM Monday – Friday and all-day Saturday and Sunday.

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)
- Continue to next page →→→

Create Notifications






Rule Sources:

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

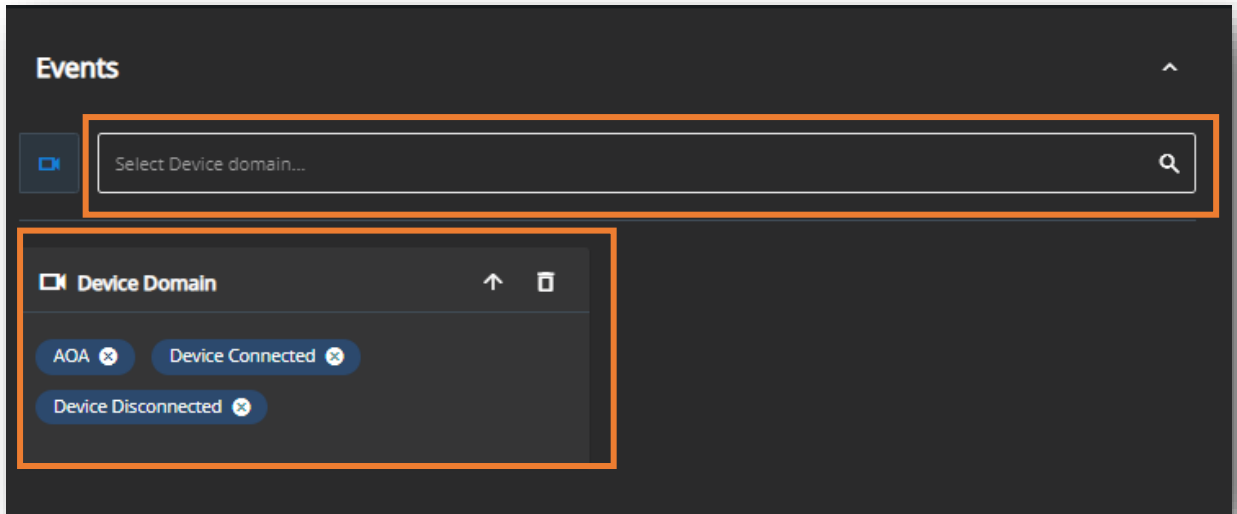
Note: The rule/notification being created can apply to a device, device groups, and/or sites.

- 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:

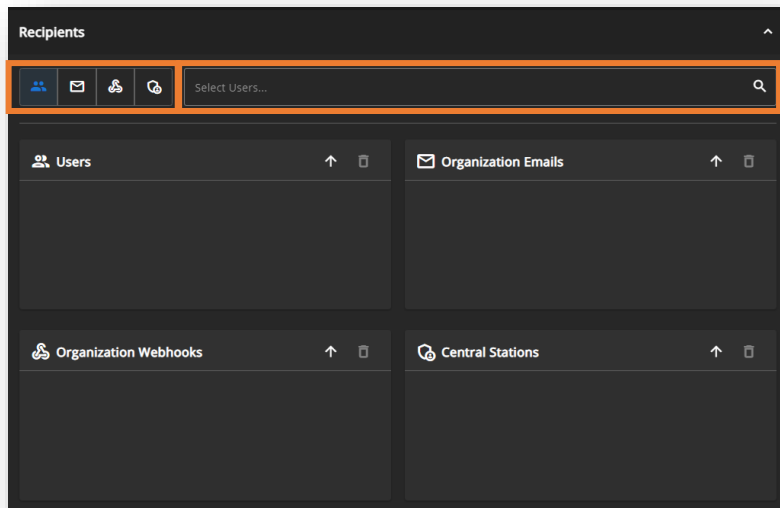
- On the [Edit Notification Rule](#) page navigate to the [Events](#) section
- From the drop-down, select the Event/Domain for which the rule will trigger

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

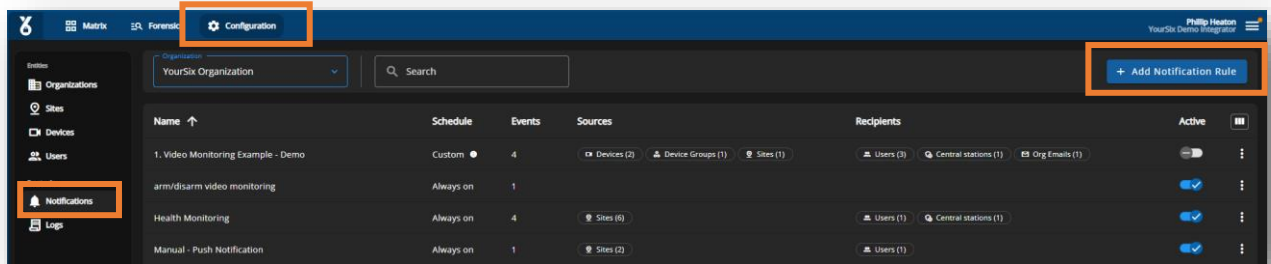
Create Notifications for Video Monitoring



Audience: Organization Super 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.

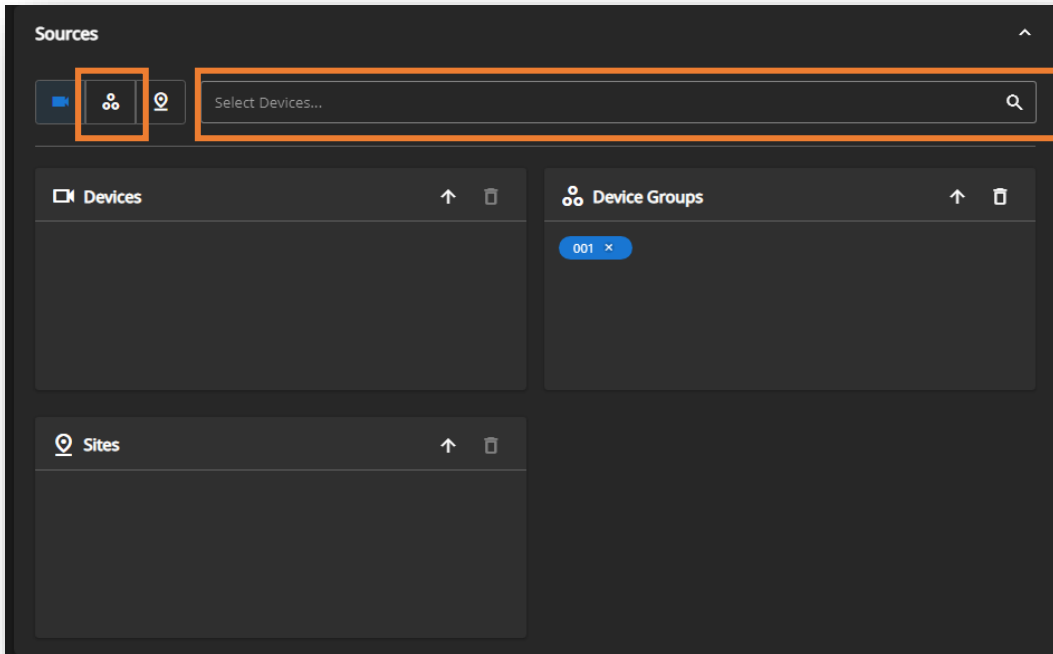
In this example the rule is set to be active from 6 PM to 8 AM Monday – Friday and all-day Saturday and Sunday.

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



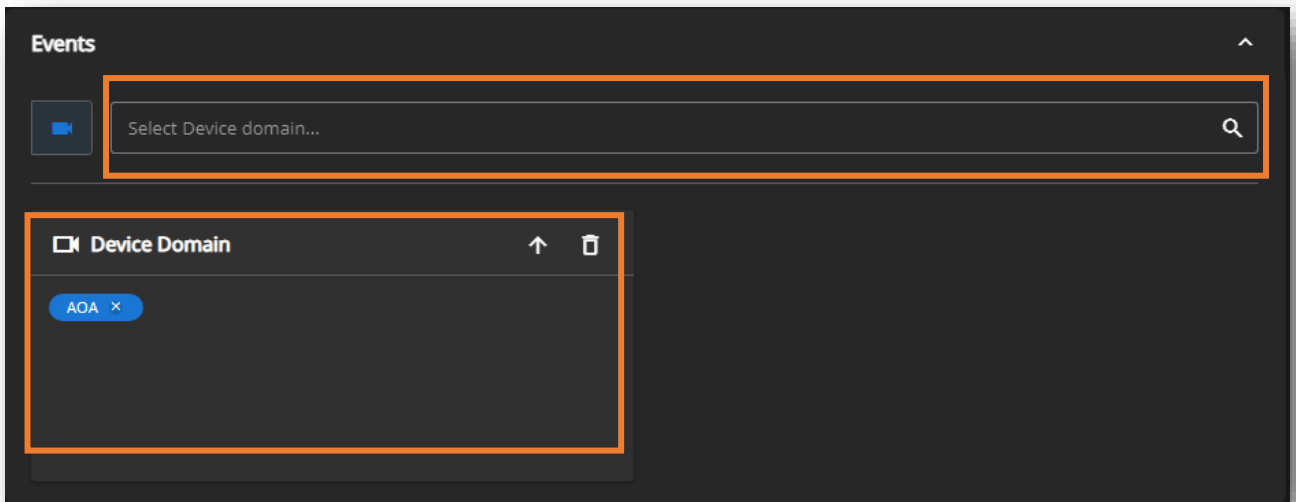
Rule Sources:

- 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 →→→

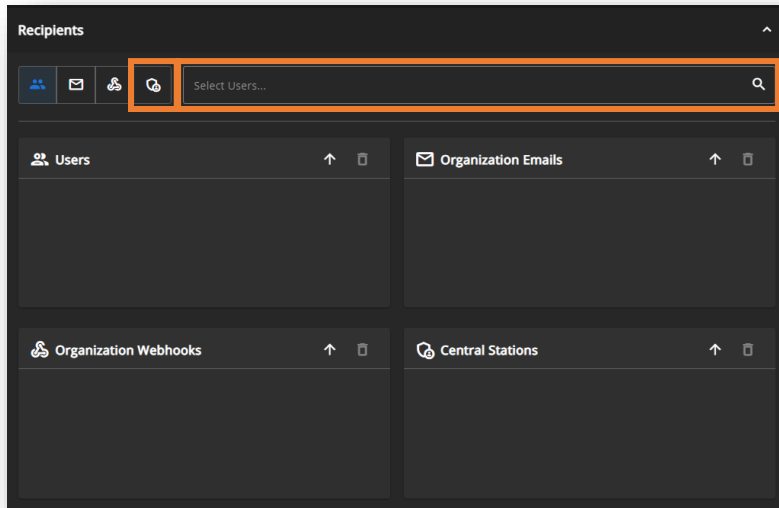
Create Notifications for Video Monitoring



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

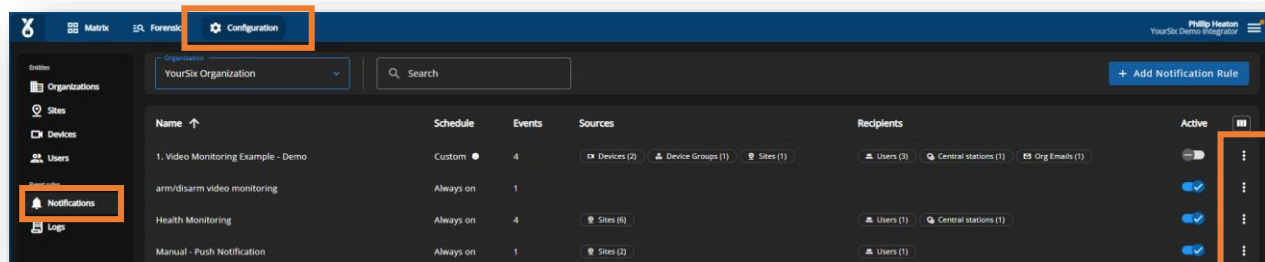
Edit Notifications



Audience: Organization Super 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
 - [\(Create Notification\)](#)

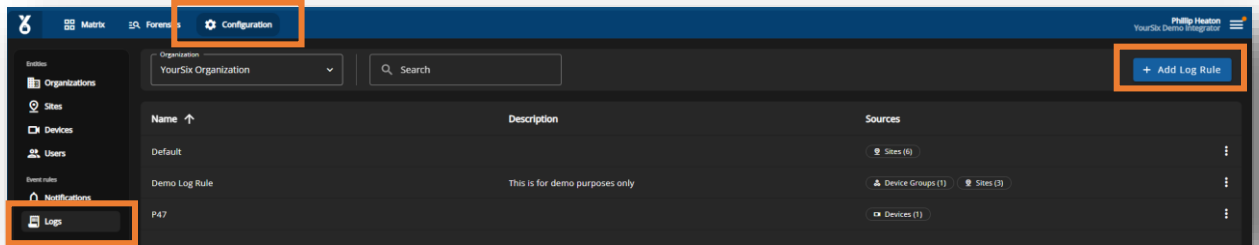
Log Rule



Audience: Organization Super Admin

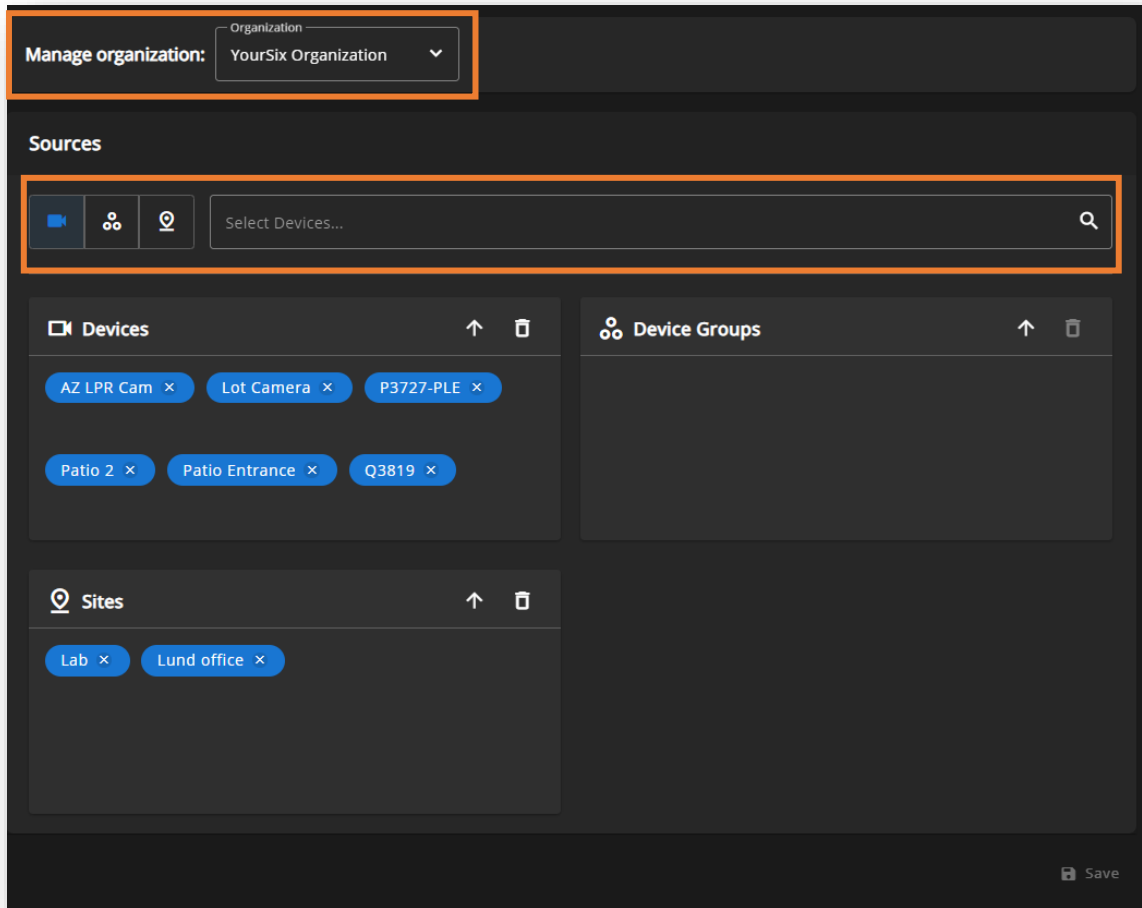


Objective: Setup log rules to create event flags on the timeline



- 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 →→→

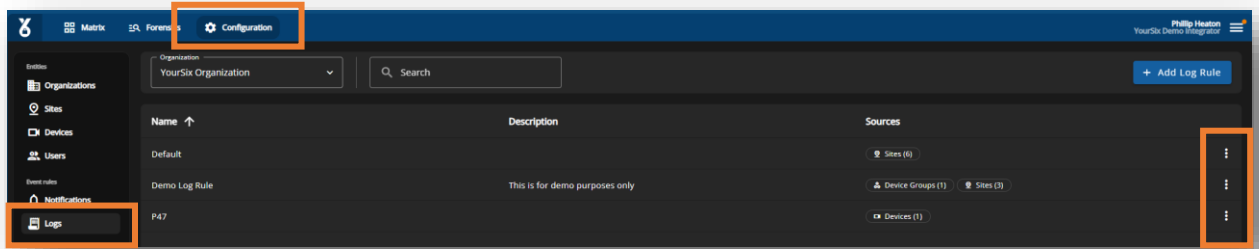
Manage Log Rule



Log Rule:

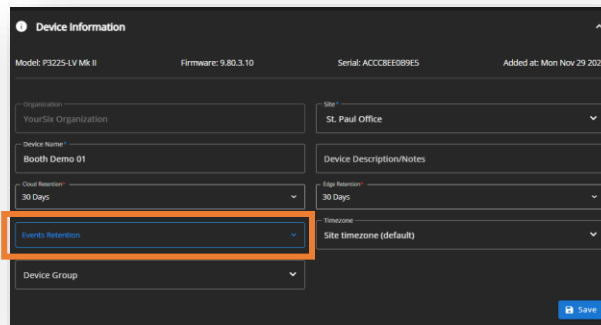
- Select the organization from the [Manage Organization](#) dropdown
- Select the [Device, Device Group or Sites](#) the log rule should apply
- Continue to next page →→→

Manage Log Rule



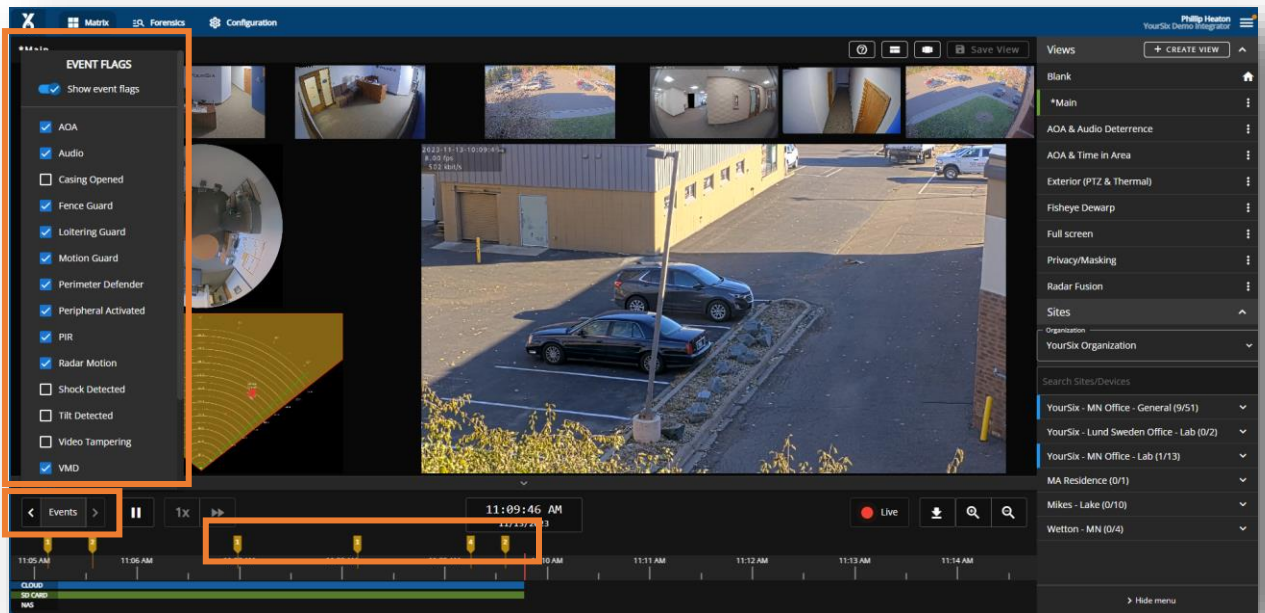
Event Retention for Log Rules:

- 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

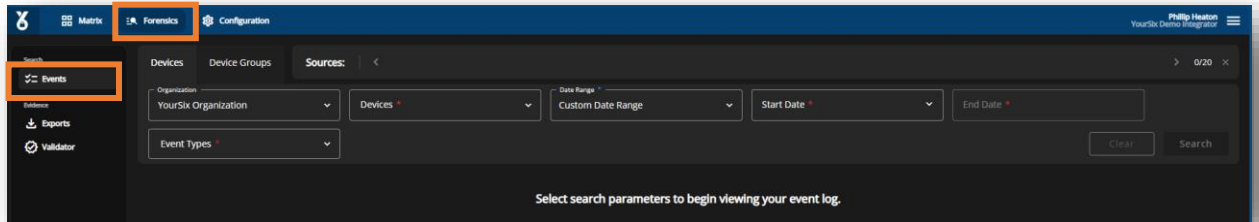
Event Log



Audience: Organization Super Admin, Admin, User



Objective: View list of events



- Select **Forensics** located on the navigation bar
- Select **Events** located on the page menu
- Continue to next page →→→

Event Log

The screenshot displays the 'Event Log - YourSix Organization' interface. At the top, there are search filters: Organization (YourSix Organization), Devices (*), Date Range (Last 7 Days), Start Date (10-25-2022 3:54 PM), and End Date (11-01-2022 3:54 PM). A 'Search' button is located to the right of the End Date field. Below the filters, there is a section for 'Event Types (2 selected)'. Underneath, a 'Sources' section shows a list of selected devices: Call Center - M0115-VE-IC-EYE-U, Employee Intercom - A8105-E, Front Hall - M0115-VE-IC-EYE-U, Main Entrance Intercom - A8207-VE, Office Floorplate - M0057, and Office Lobby - M1065-L-EDFLIND. The main area contains a table with the following columns: Event Timestamp, Event Type, Device, and Site. The table lists 13 events, all of type 'VMD', occurring at the 'Main Entrance Intercom - A8207-VE' device at the 'YourSix - MN Office - General' site. The events are timestamped from 10/25/2022 3:58:50 PM to 10/25/2022 4:16:52 PM. At the bottom of the table, there is a pagination control showing 'Showing 1-100' and an 'Export Events' button.

Event Timestamp	Event Type	Device	Site
10/25/2022, 3:58:50 PM	VMD	Main Entrance Intercom - A8207-VE	YourSix - MN Office - General
10/25/2022, 3:59:19 PM	VMD	Main Entrance Intercom - A8207-VE	YourSix - MN Office - General
10/25/2022, 3:59:35 PM	VMD	Main Entrance Intercom - A8207-VE	YourSix - MN Office - General
10/25/2022, 4:00:03 PM	VMD	Main Entrance Intercom - A8207-VE	YourSix - MN Office - General
10/25/2022, 4:01:55 PM	VMD	Main Entrance Intercom - A8207-VE	YourSix - MN Office - General
10/25/2022, 4:03:22 PM	VMD	Main Entrance Intercom - A8207-VE	YourSix - MN Office - General
10/25/2022, 4:08:29 PM	VMD	Main Entrance Intercom - A8207-VE	YourSix - MN Office - General
10/25/2022, 4:13:51 PM	VMD	Main Entrance Intercom - A8207-VE	YourSix - MN Office - General
10/25/2022, 4:15:11 PM	VMD	Main Entrance Intercom - A8207-VE	YourSix - MN Office - General
10/25/2022, 4:15:35 PM	VMD	Main Entrance Intercom - A8207-VE	YourSix - MN Office - General
10/25/2022, 4:16:52 PM	VMD	Main Entrance Intercom - A8207-VE	YourSix - MN Office - General

- Select the desired parameters
- Select **Search**
- A list of results will appear



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.