ELECTRONICS & DEFENSE

PNT 360

Monitoring & Configuration Management for Timing & Synchronization Systems

User Manual

Contents

1. Introduction

PNT 360 is Safran Navigation & Timing's Monitoring and Configuration Management Solution. It provides insight into your timing system and allows you to monitor its functionality and performance by giving you access to metrics related to NTP, PTP, GNSS, System, Network, Oscillator, Timing, White Rabbit, and more. It also provides a centralized configuration management function so you can manage your devices from one location.

2. Installation

2.1. Prerequisites

The PNT 360 application is supported on the Linux operating system **Ubuntu 20.04 (or later)** server or VM.

2.2. Installation

Open a terminal and navigate to the directory with the install file. Then run the following:

```
sudo apt install ./pnt360_bundle_<xxxxxx>.deb
```

Note: When prompted for country name, state, province, etc. pressing the "Enter" key will skip these fields.

To upgrade PNT 360 to a new version, run the same command with a newer bundle. To uninstall the software, run

```
sudo apt remove pnt360
```

Note: to install your own SSL certificate, see the Appendix.

After the installation is complete you will be able to reach the UI at https://<pnt360_Server_IPv4>.

In this document, the text <pnt360_Server_IPv4> should be replaced by the actual IPv4 address (or hostname) of the server running the PNT 360 monitoring application.

3. Getting Started

3.1. SecureSync User Management

IMPORTANT: for both SecureSync 1200 and 2400: You must create a PNT 360-specific User on each SecureSync that will connect to the monitoring application to avoid conflicts with accessing the SecureSync's Web UI.

- On the SecureSync, navigate to **Management > Authentication** and click the +
- Enter the credentials you will use for PNT 360 to monitor your SecureSync
- Select the Group "Admin" and click Submit

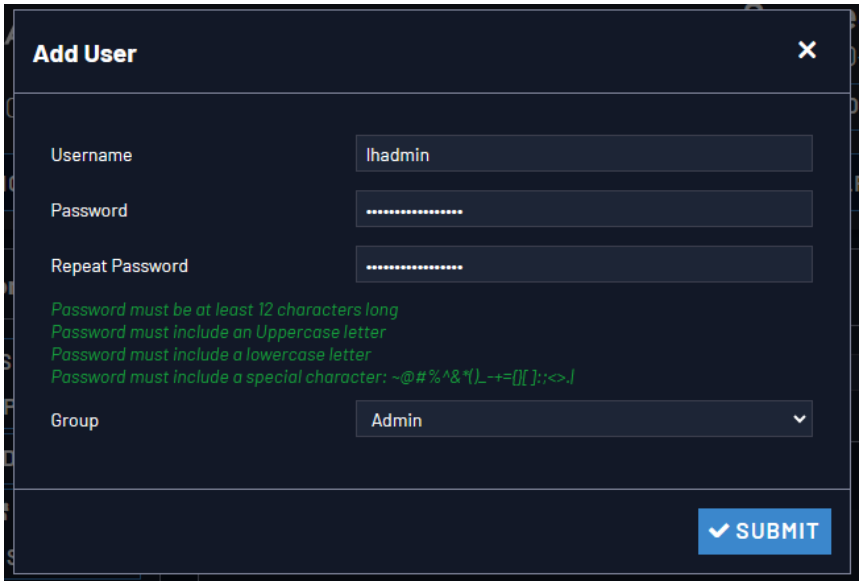


Figure 1: User configuration on SecureSync device

3.2. White Rabbit Zen User Management

It is recommended to use the userSNMP user for PNT 360 SNMP data. You can modify this user's access view and mode, the auth and private key, as well as the password.

- On the WRZ Web UI, Navigate to Administration > SNMPV3
- Enter in the credentials you wish to use and click change password
- You can now use this account in PNT 360

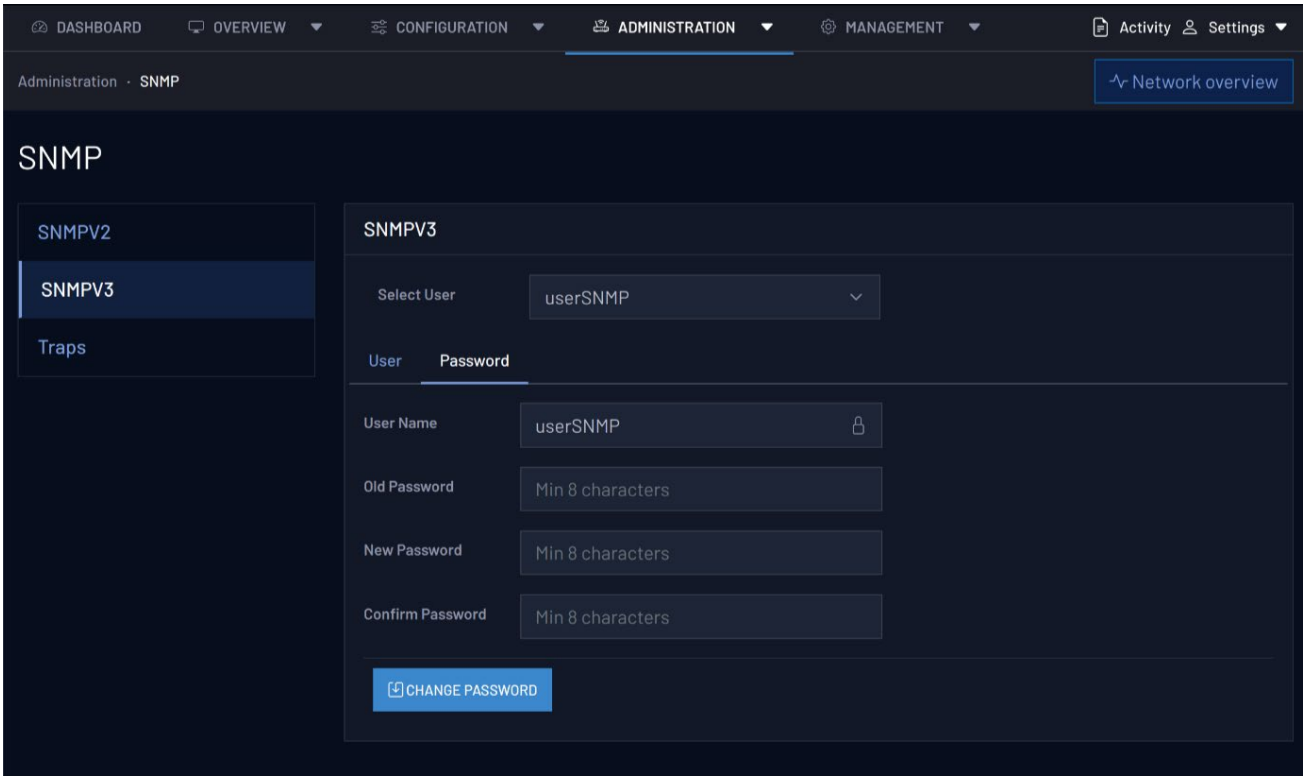
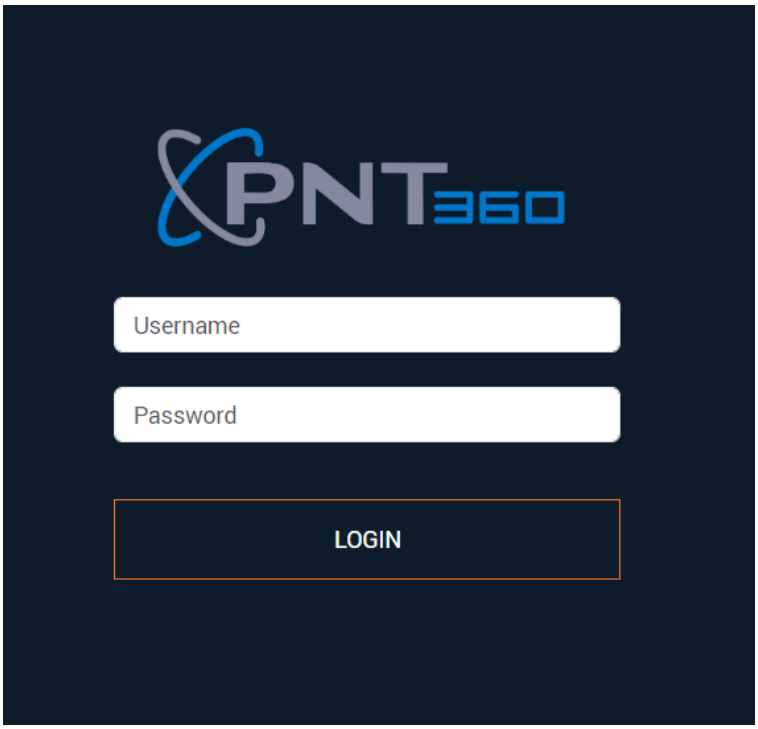


Figure 2: User configuration on WRZ device

3.3. Configuring PNT 360

3.3.1. Logging In

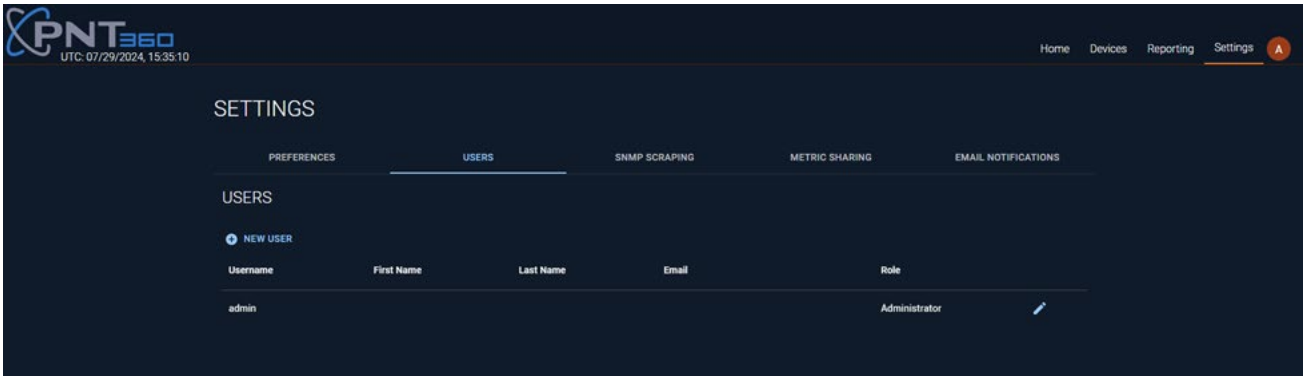
Once PNT 360 is successfully installed, you should be able to reach the login screen in your local browser by navigating to **https://<Server_IPv4>** and login with the default credentials provided to you with your installation package.



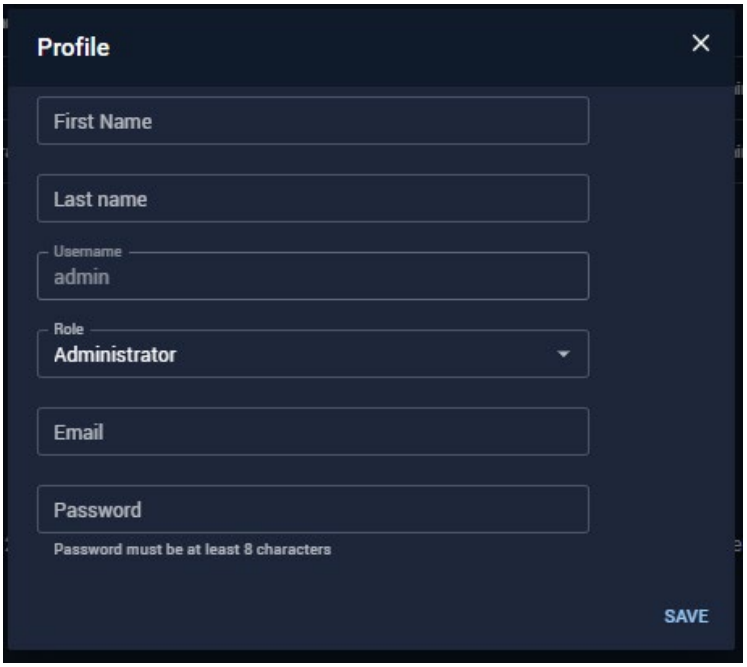
Note: Safran recommends changing your default admin user password at this stage to protect your security (see next section).

3.3.1.1. Update Password

In the **Settings** tab, select Users.



Click the edit icon and enter a new password:

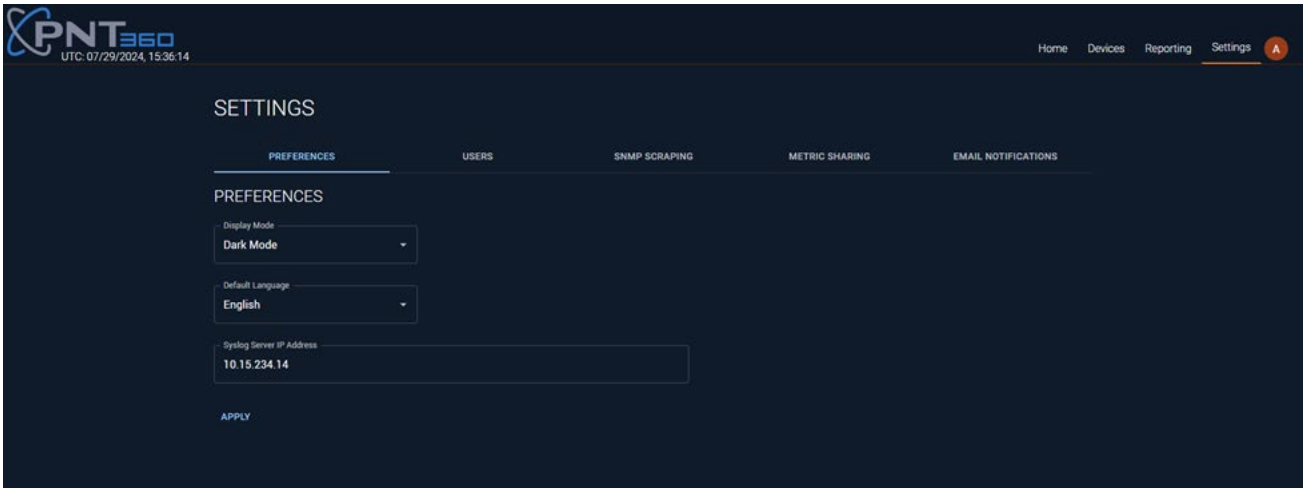


3.3.2. Configuration

Now you must configure for monitoring before you can proceed with creating dashboards.

In the Settings page, select the Preferences tab and enter the Syslog Server IP address.

NOTE: this should be the IPv4 address of the server that you've installed PNT 360 on.



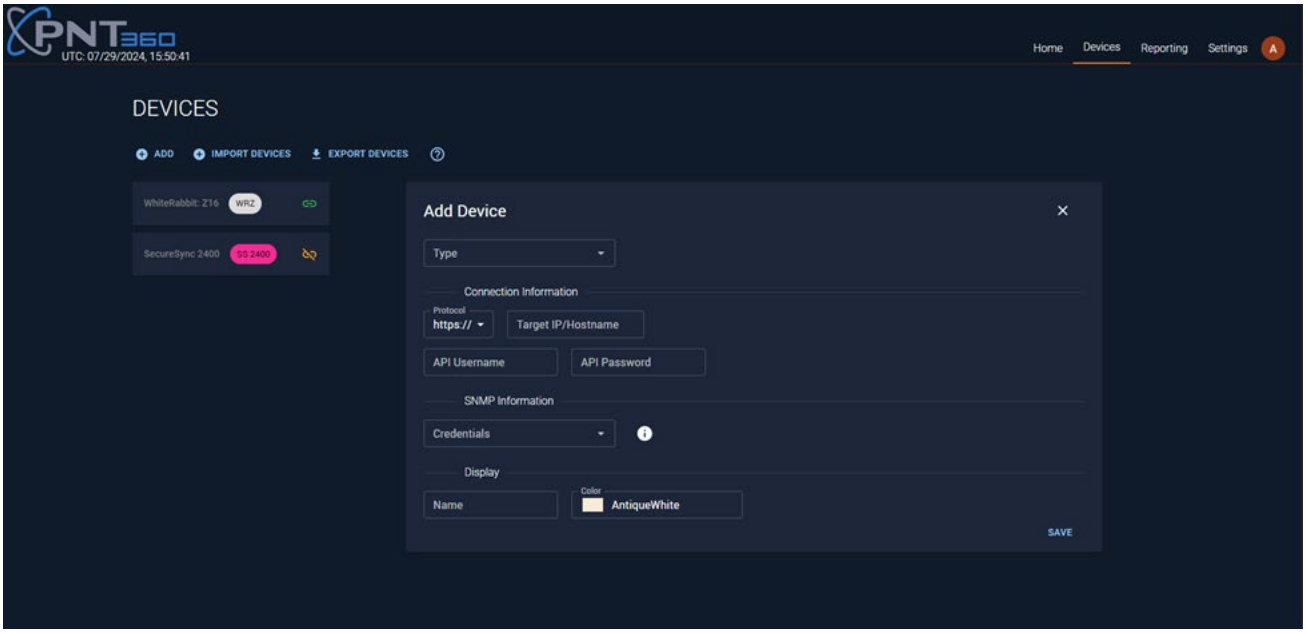
Click **Apply**.

3.4. Adding Devices

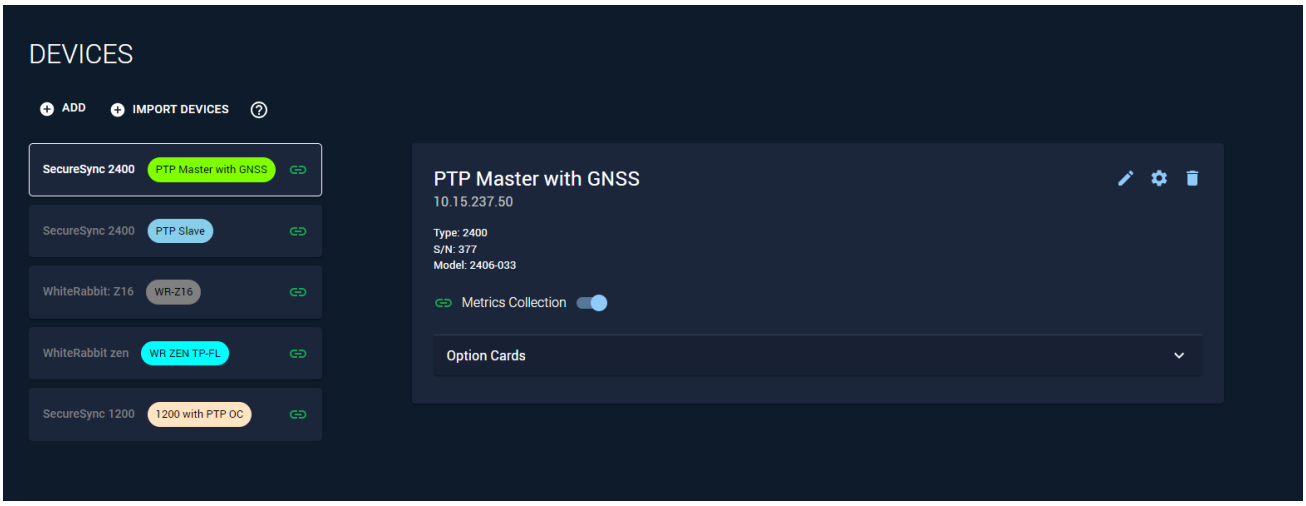
3.4.1. Single Device

Navigate to the Devices tab in the header and click ADD. Enter all the information for that device, then click SAVE.

For SecureSync, the API Username and API Password for each device is the credentials of the user created in SecureSync User Management. For White Rabbit, the API Username is "root", and the API Password is the password for the "root" user.

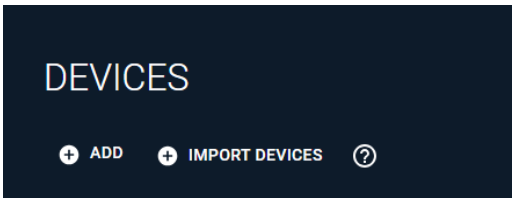


You should now see the device in the Devices list.

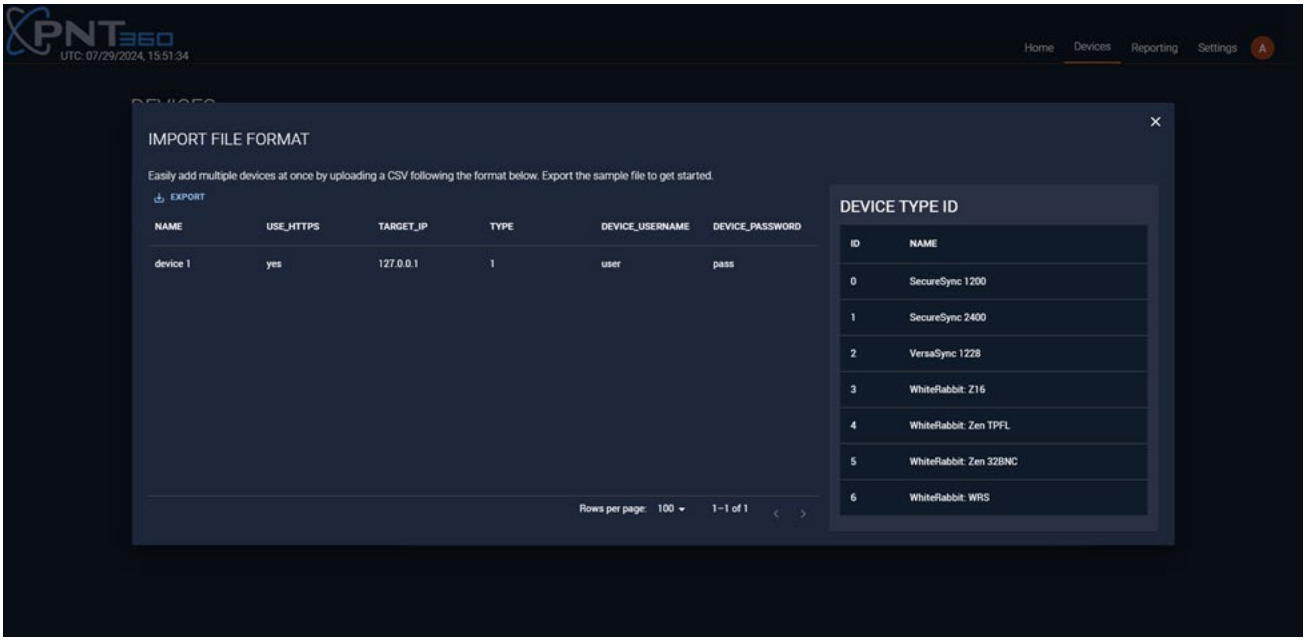


3.4.2. Import devices

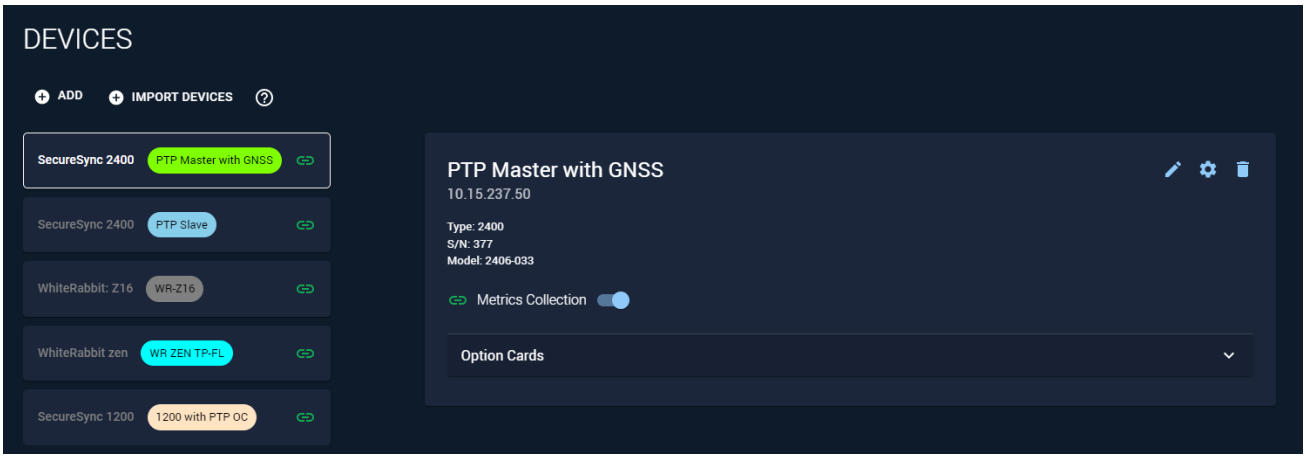
You can import a list of devices from a CSV form. To view the expected file format, Click the **?** icon on the Devices page.



You will see the file format and the option to export a sample file to get started.



Enter the devices you wish to monitor and then upload this file using the Import Devices button. You will see all the devices listed in the Devices page. Duplicate devices will not be added.



3.5. Data Collection

There are two ways that the PNT 360 application gets data for monitoring:

- Accessing the device's REST API
- SNMP

You can see the data collection status through the indicator under Metrics Collection. If either the REST or SNMP metrics collection requires attention, a warning indicator will appear.

Each device must be configured to expose the SNMP data specifically for PNT 360 use. For SecureSync devices, enabling metrics collection will also configure the device to expose SNMP data using the credentials specified in **Settings** > **SNMP Scraping**.

For White Rabbit devices, the credentials in **Settings** > **SNMP Scraping** must match the ones set in White Rabbit Zen User Management.

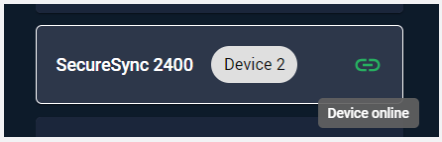
Once these credentials are configured, you can toggle the Metrics Collection switch to ON for each device in the devices list to begin collecting metrics. Please allow a couple minutes for scraping to begin and the Metrics Collection indicator to turn green.

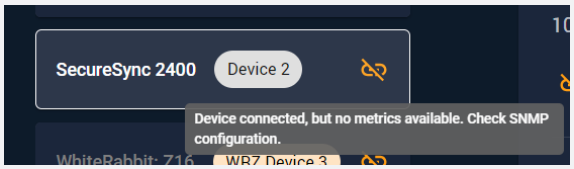
3.5.1. Monitoring Status Indicator

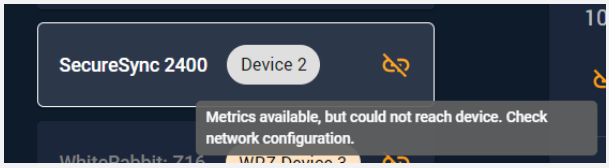
The data collection status can be seen through the Monitoring Status indicator. This indicator displays whether the application is currently able to gather metrics from the device.

This indicator appears next to each device on the Devices page, as well as in the “Monitoring Status” dashboard chart.

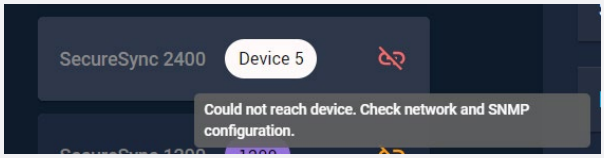
The metrics collection indicator can have the following states:

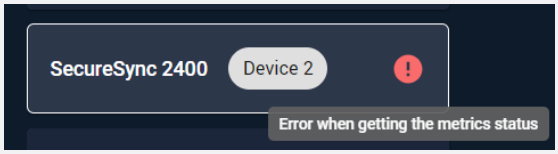
Status	Green (solid link) 
Explanation	Metrics collection for the device is functioning normally. The application has received new SNMP metrics from the device within the last minute, and the device is currently reachable through its REST API.
Resolution	N/A

Status	Yellow (broken link), “device connected, but no metrics available” 
Explanation	The device is currently reachable through its REST API, but the application has not received new SNMP metrics from the device within the last minute. This status may occasionally appear in normal operation: • When metrics collection has recently been turned on and two minutes has not yet elapsed • Due to intermittent network issues If this status persists, and metrics do not appear on dashboard charts, then follow the below resolutions.
Resolution	**Resolution 1** If metrics collection is disabled, press the toggle to enable metrics collection. The indicator will take several minutes to update to Green, after which metrics should be visible for the device on the dashboard. **Resolution 2** SNMP may not be configured correctly on the device or in the application. The credentials configured on the device for SNMP *(in the app, see Devices -> (click your device) -> Configuration Management -> SNMP)* must match the ones that the application is trying to use for that device *(in the app, see Devices -> (click your device) -> Edit -> SNMP Information)*. For SecureSync products, the device will be automatically configured with the given SNMP credentials when metrics collection is enabled, but for other products this must be done manually. **Resolution 3** The network may be configured to block SNMP traffic, ensure port 161 on the device is reachable. Use an external SNMP tool like snmpwalk to verify that metrics are collectable from the device and that the community or v3 credentials are correct.

Status	Yellow (broken link), “metrics available, but could not reach device” 

Explanation	The device is not reachable through its REST API, but the application has received new SNMP metrics from the device within the last minute.
Resolution	**Resolution 1** The username or password on the device may have changed; log in to the device using its Web UI to confirm the credentials. The credentials that the monitoring application is using to log in to the device can be changed by editing the device on the devices page. **Resolution 2** The network may be configured to block traffic from the REST API, or the REST API may be disabled on the device. Ensure the port that the API is hosted on is reachable. Use the product's API documentation to log in (with postman, curl, or other REST API tool) and verify that the API is functioning normally.

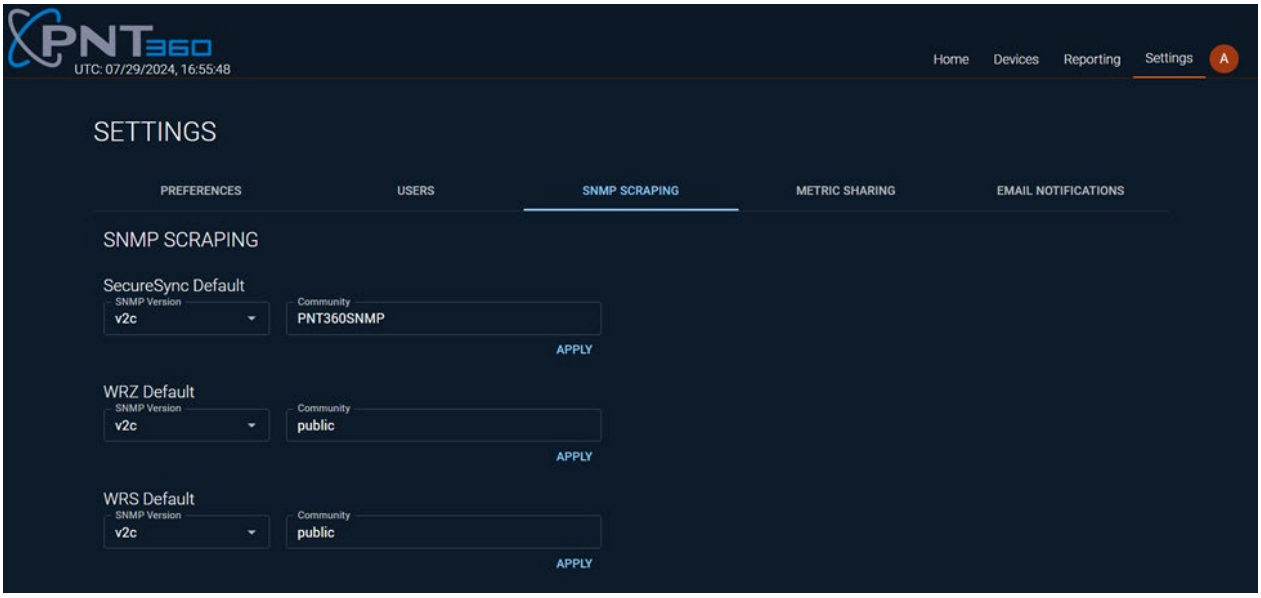
Status	Red (broken link), "could not reach device" 
Explanation	The device is not reachable through its REST API, and the application has not received new SNMP metrics from the device within the last minute.
Resolution	Make sure the device is powered on, connected to the network, and has been added at the correct IP address or hostname. Follow the above resolutions for the Yellow (broken link) statuses to troubleshoot the issue.

Status	Error 
Explanation	The application server could not be reached or encountered an internal error.
Resolution	Close the tab, re-open it, and log back in. If the problem persists, please contact support.

3.5.2. SNMP Global Configuration

You can configure SNMP Scraping for all devices in the PNT 360 settings.

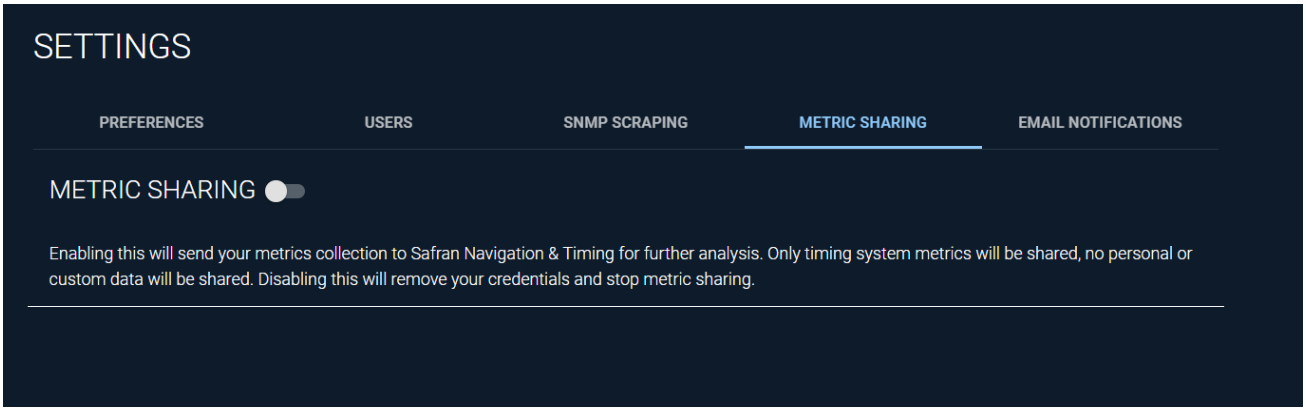
Navigate to **Settings** > **SNMP Scraping**



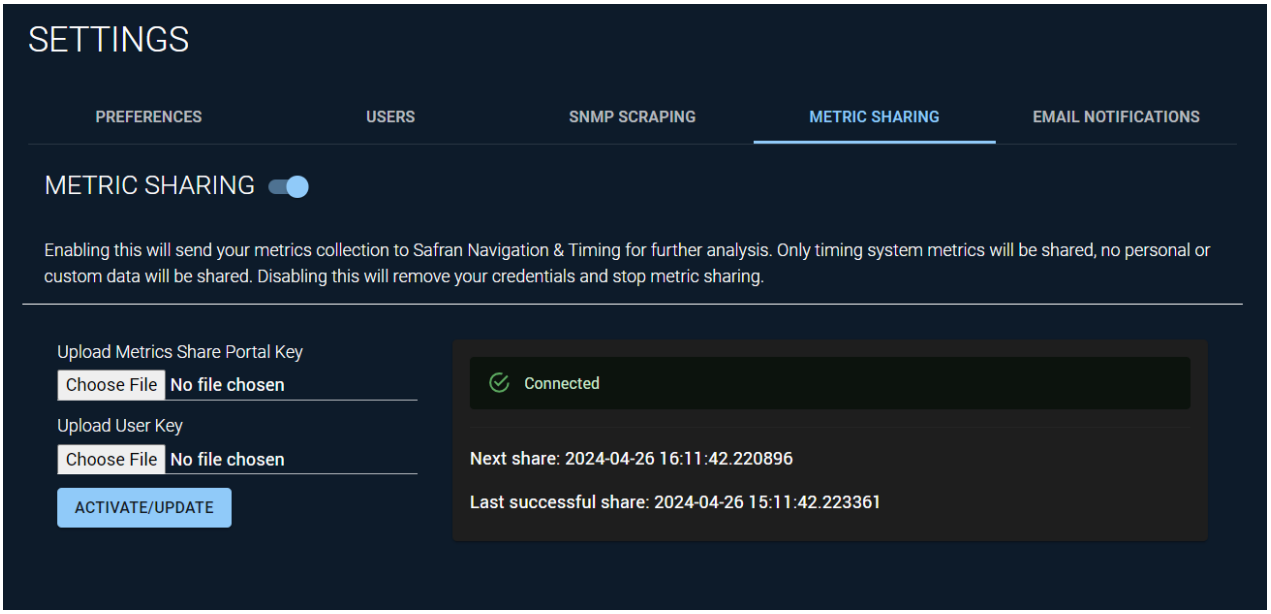
3.5.3. Metric Sharing

We provide the ability to share metrics with Safran Navigation & Timing for analysis purposes. Only device metrics are transmitted; all identifiable information (company name, IP addresses, etc.) are obfuscated prior to data transfer. You will be given a portal key and a user key with your installation package of PNT 360. These keys will be specific to your company and not used by anyone else.

This feature is configurable. Navigate to Settings then the Metric Sharing tab.



Toggle Metric Sharing on.



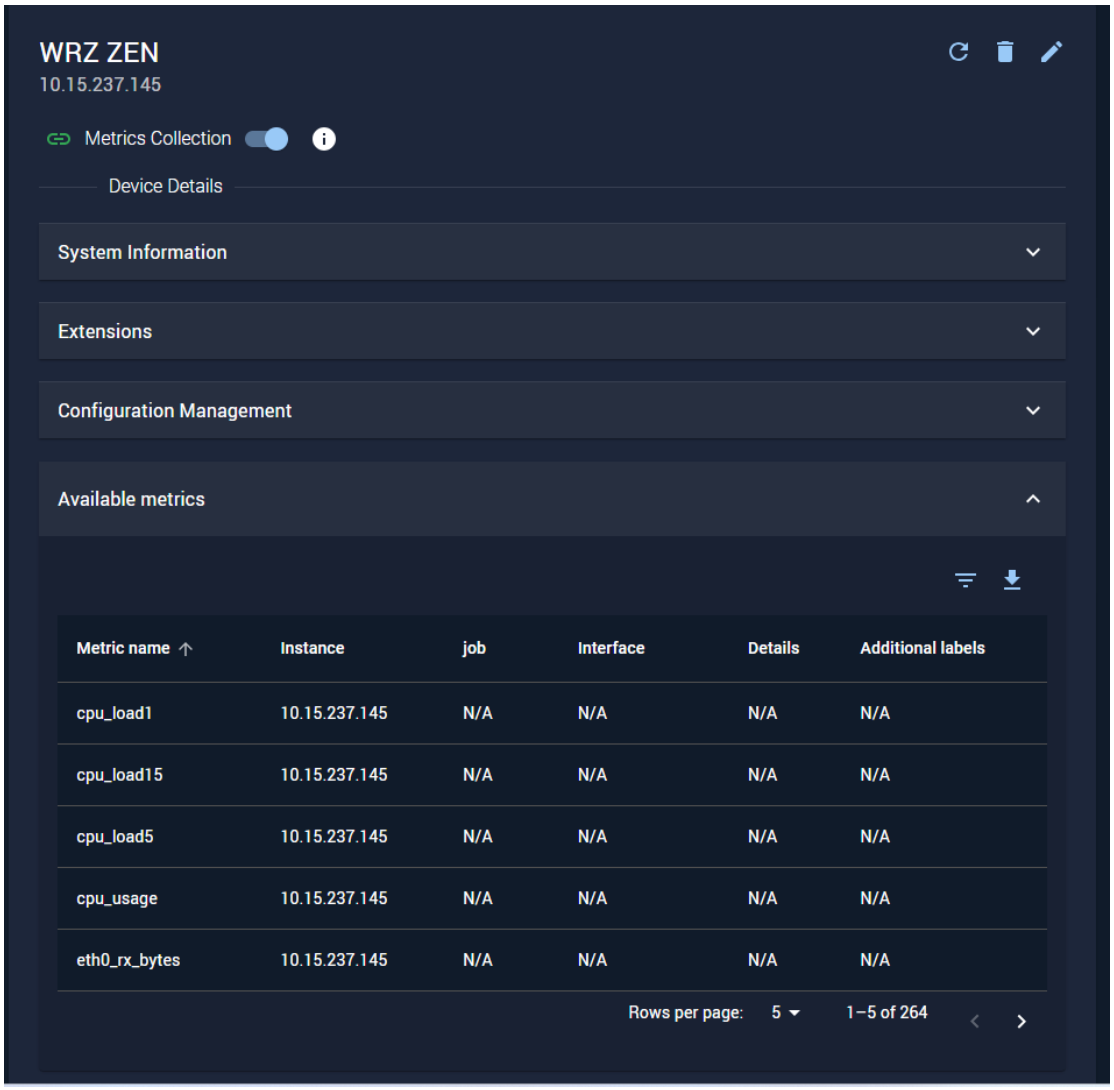
Upload your Portal key and user key and select Activate.

3.5.4. Exporting Metrics

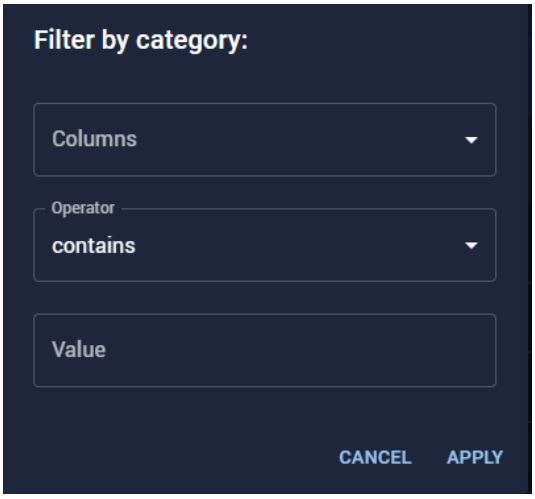
3.5.4.1. Overview

The Exporting Metrics feature allows users to export available metrics lists into downloadable files.

3.5.4.2. Steps to Export Metrics



2. **Filter Metrics (Optional):**
    a. Select the filter icon button located in the top right corner of the metrics table to refine the list of metrics.
    b. In the **Filter by Category** dialog:
        i. Select the **Column** to filter by (e.g., Metric Name, Instance, or Job).
        ii. Choose an **Operator** (e.g., Contains, Equals).
        iii. Enter a **Value** to specify the filter criteria.
        iv. Select **Apply** to display only the relevant metrics.

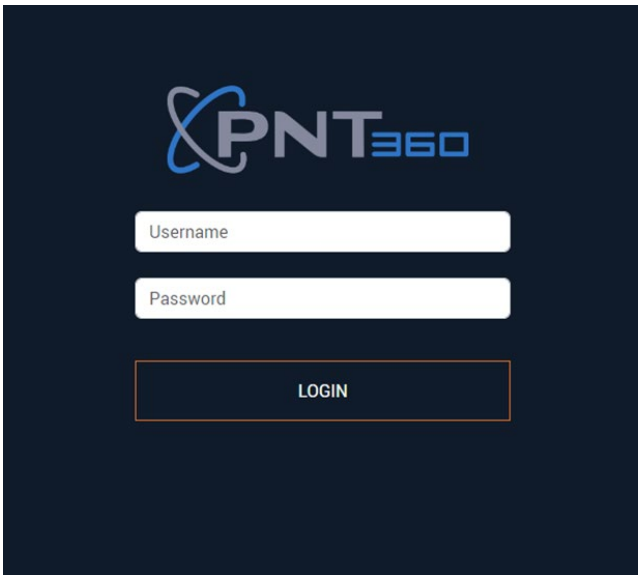


3. **Export the Metrics:**
    a. Select the download icon button located in the top right corner of the metrics table.
    b. The selected metrics will be downloaded and saved to your local system.

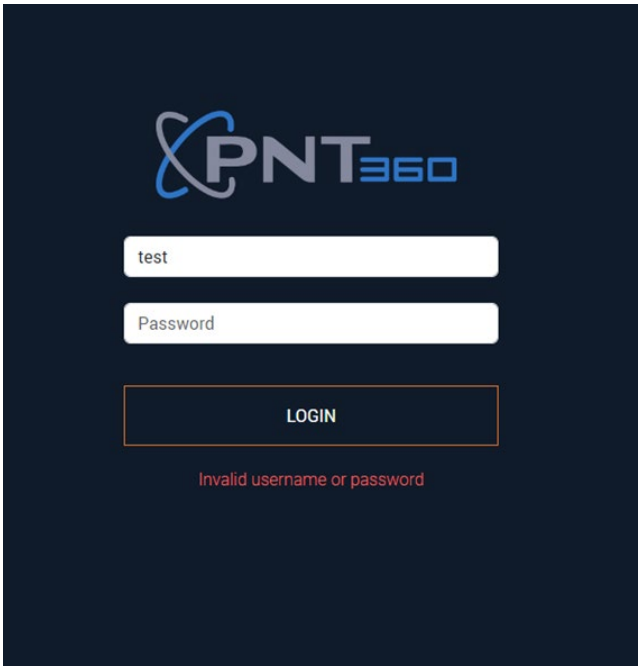
4. Features

4.1. Login/Out

Login with username and password.



An error will display if the account information is incorrect.



4.2. Settings

4.2.1. Preferences

You can update the application theme as well as the default application language in the Preferences section.

Click on **Settings**, then the **Preferences** tab.

Select the display mode and language and click Apply.

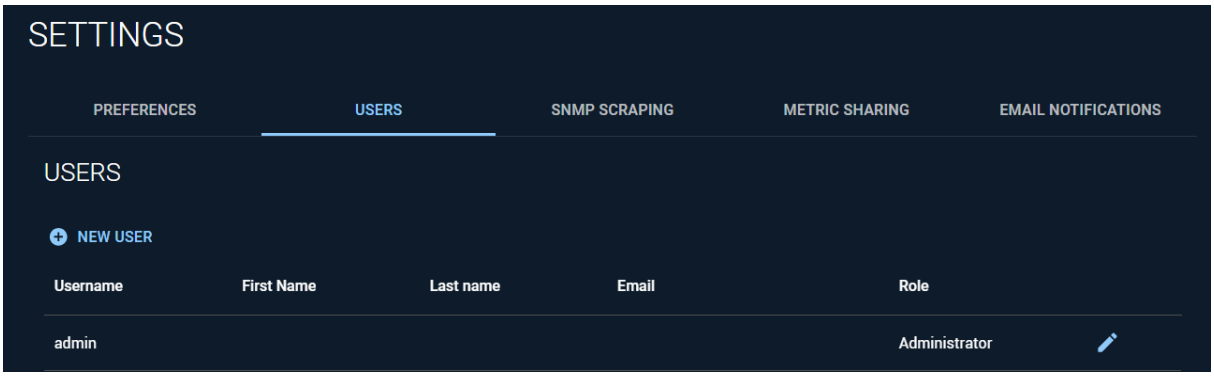
The preference changes will occur immediately.

Figure 3: Light mode, in Spanish

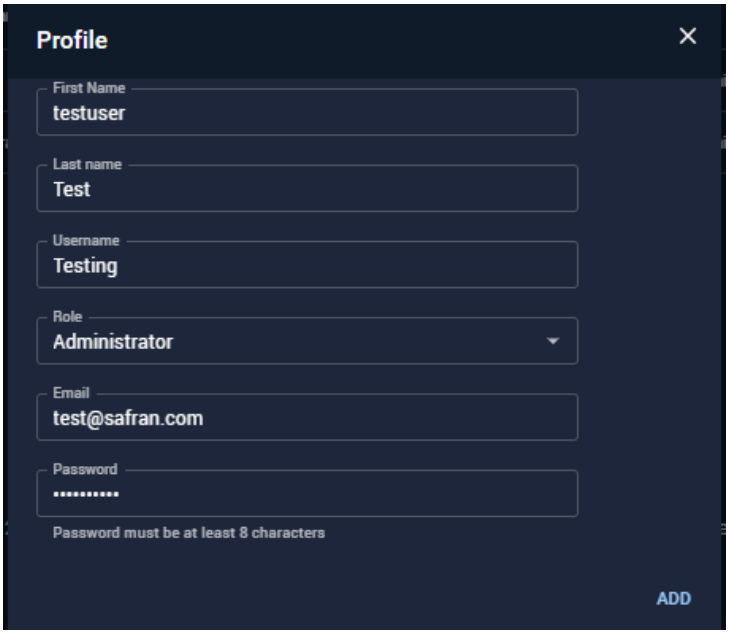
4.2.2. User Management

4.2.2.1. Adding Users

Navigate to Settings, then Users tab and click New User.



The new user modal will display.

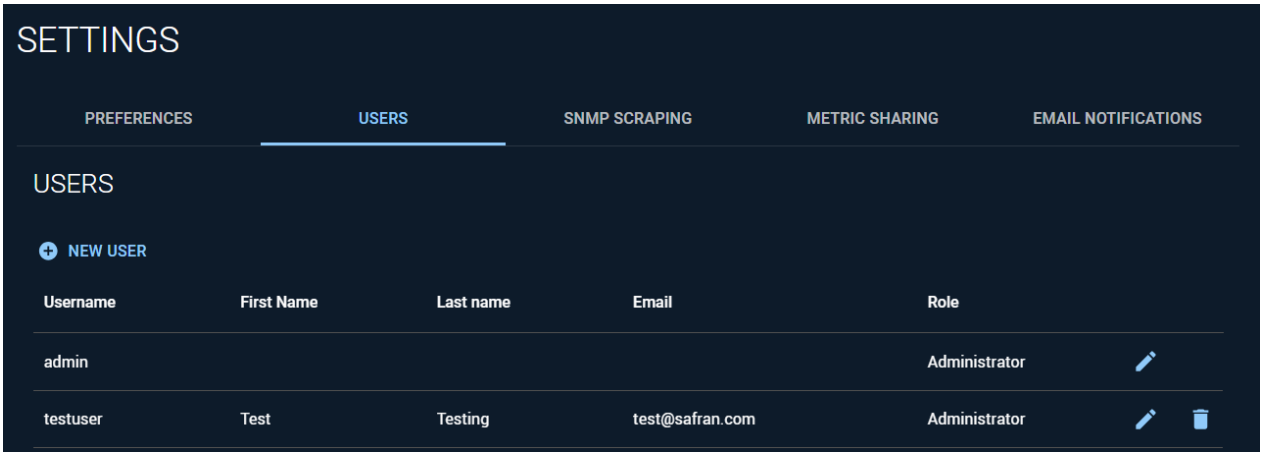


Enter the user information and click Add.

Note: The Administrator role has access to all features of the application, including modifying dashboards, changing device configurations, and updating PNT 360 settings. The General User role has read access to dashboards but cannot change any dashboards, device configurations, or settings.

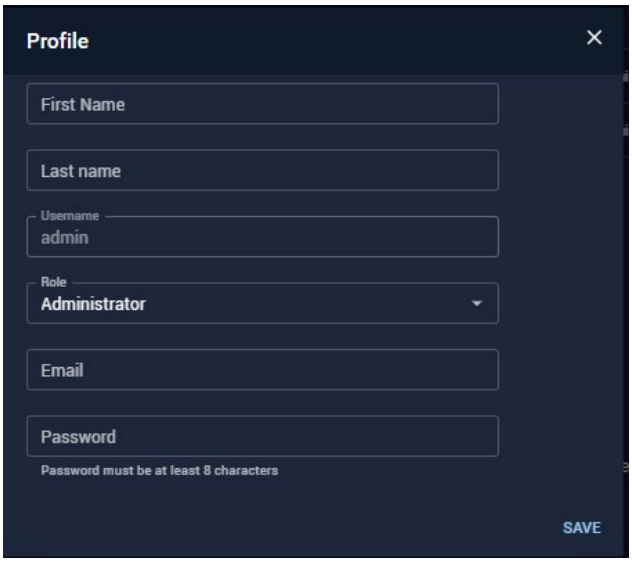
For a complete list of user permissions, see User Permissions.

The new user will appear in the list and can now log in.



4.2.2.2. Editing Users

Navigate to Settings, then Users tab. Click the edit icon next to the user you wish to edit. Note that the username cannot be modified.

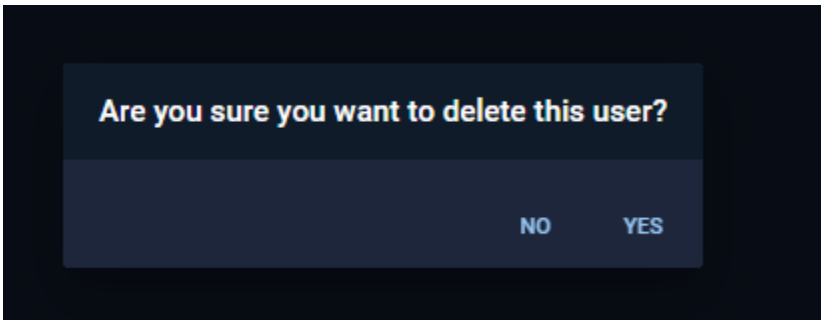


Edit the user information and click SAVE button to save changes.

4.2.2.3. Deleting Users

Navigate to Settings, then Users tab. Click delete icon next to the user you wish to delete. Note: the default admin user cannot be deleted.

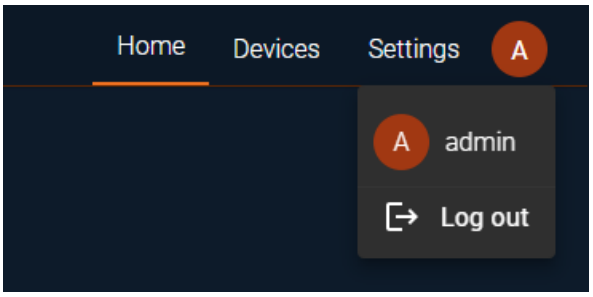
You will see a modal asking you to confirm the deletion.



Click yes to delete user. This action cannot be undone.

4.2.2.4. Current User

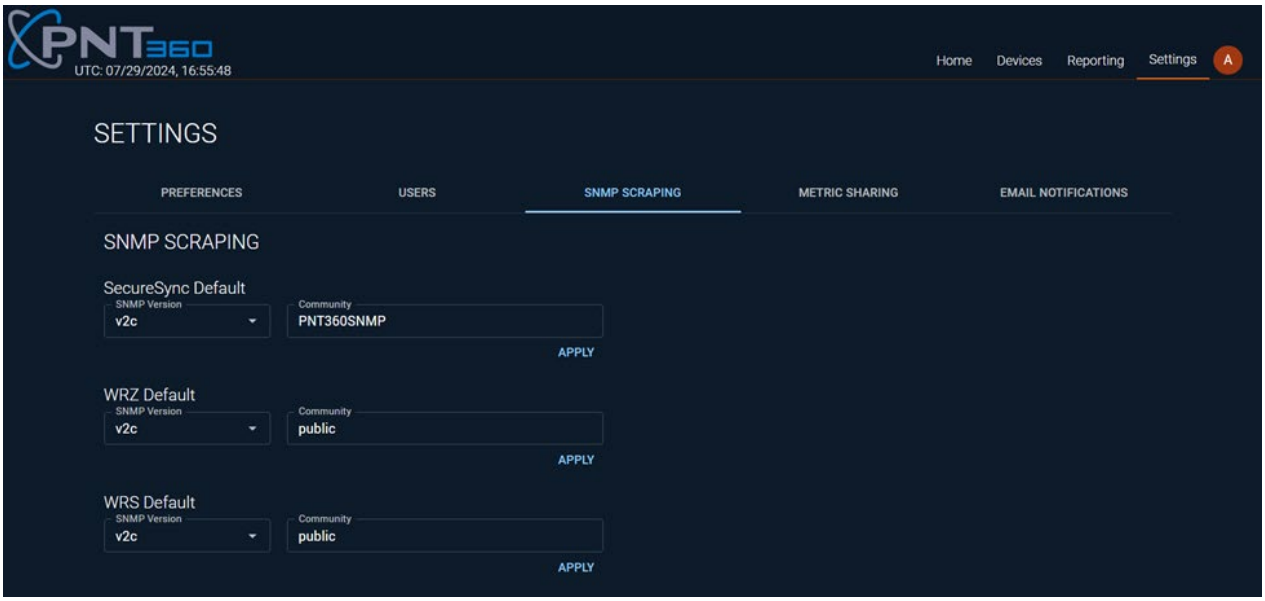
You can see which user is actively logged in by viewing the account at the top right of the application. This is also where you can log out of the application.



4.2.3. SNMP Scraping

You can configure SNMP Scraping for all devices in the PNT 360 settings.

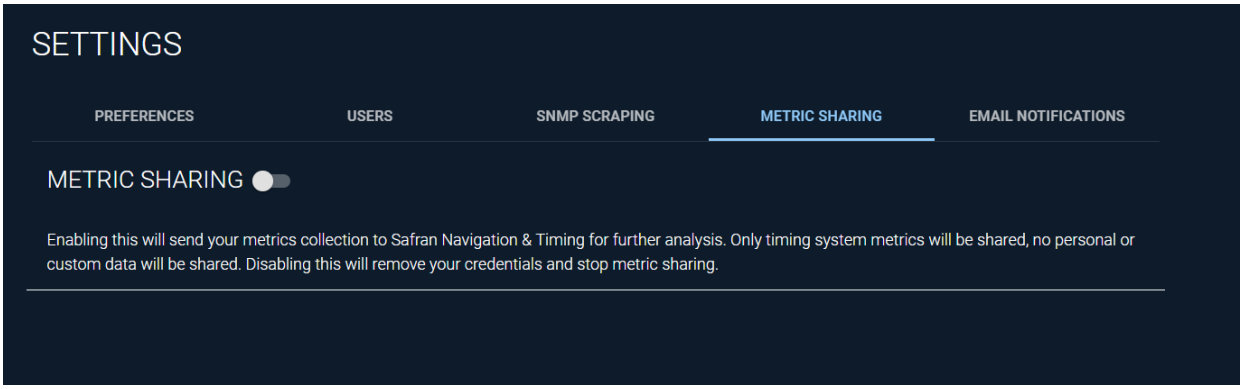
Navigate to **Settings** > **SNMP Scraping**



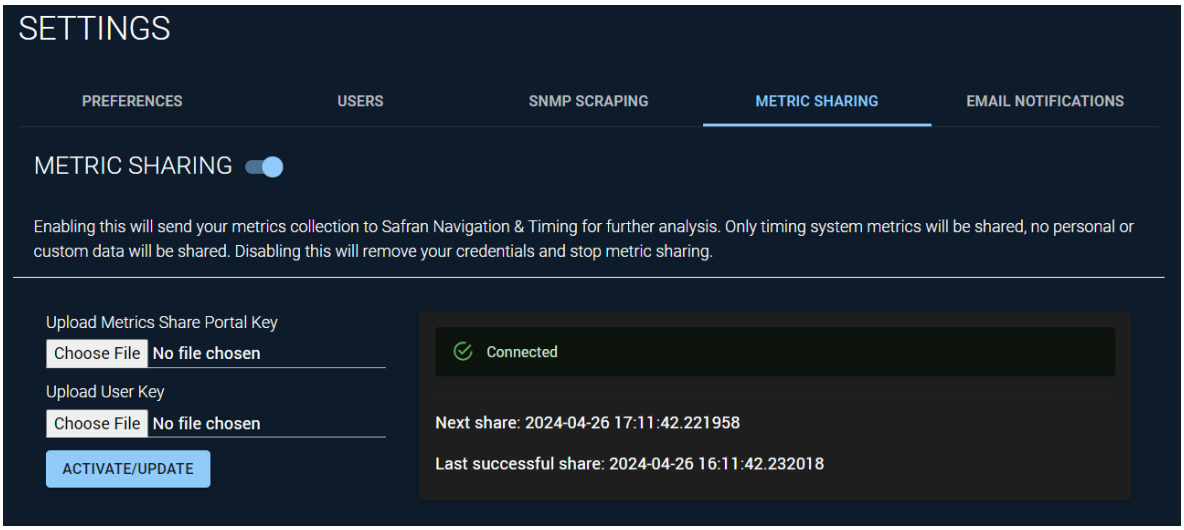
4.2.4. Metric Sharing

4.2.4.1. Turn on metric sharing

Navigate to Settings then the Metric Sharing tab.

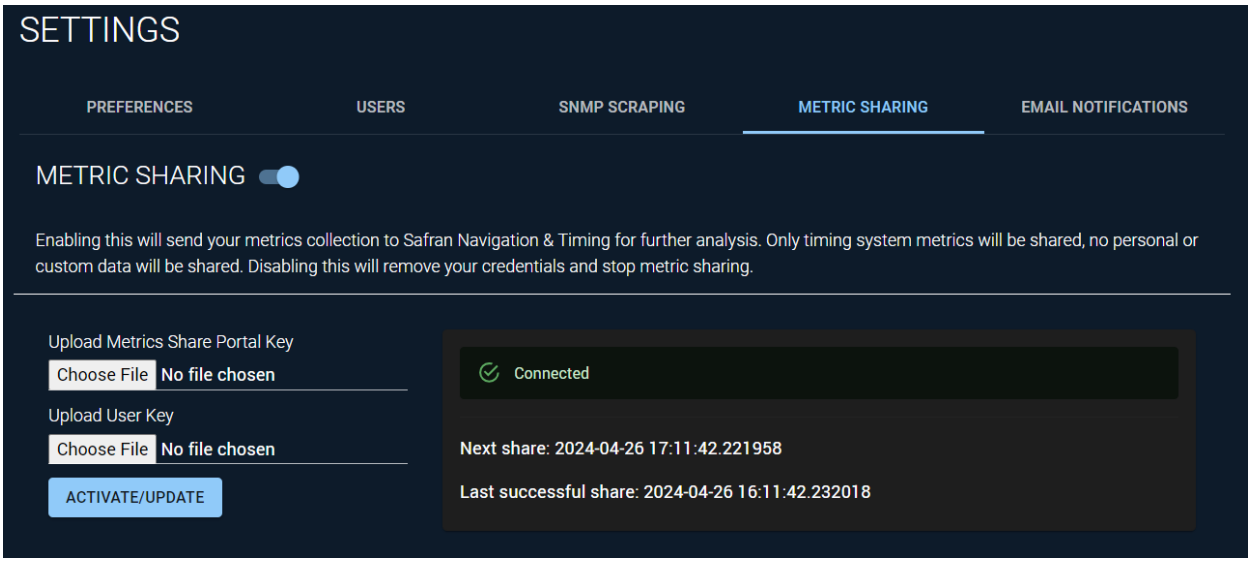


Toggle Metric Sharing on. The toggle will remain in the on position and some status information will be displayed.



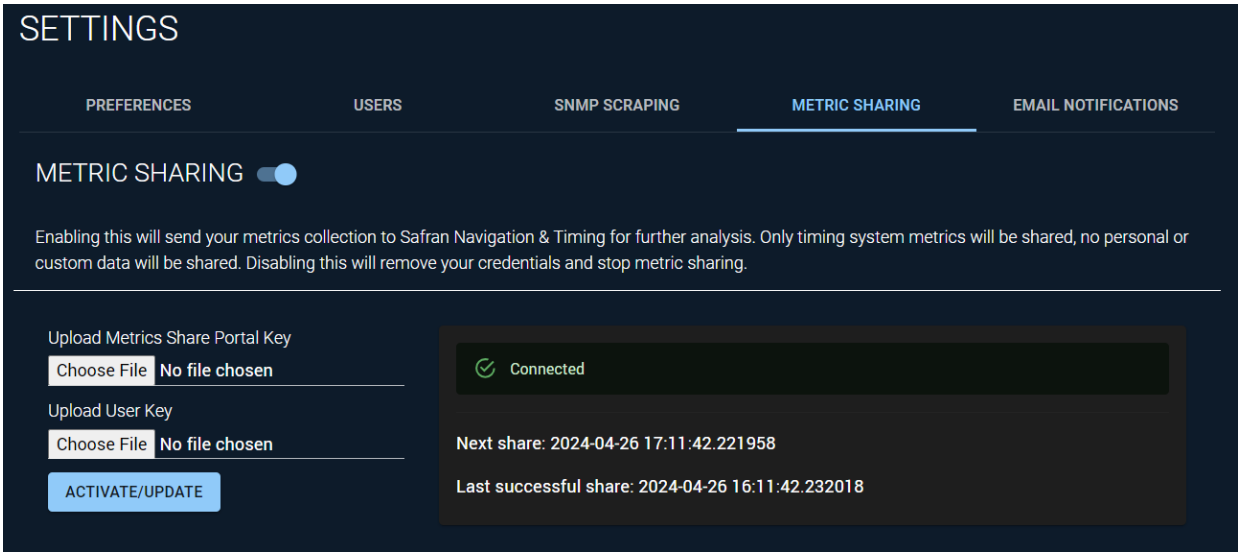
4.2.4.2. View metric sharing status

If metric sharing is actively enabled, there will be a connection status and some information available about the data transfer. Navigate to Settings, then the Metric Sharing tab. The status is indicated in this view.

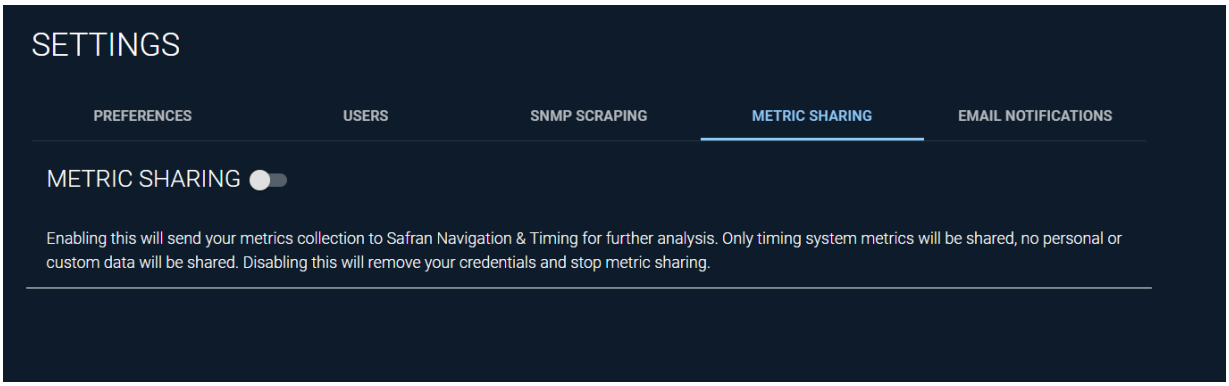


4.2.4.3. Turn off metric sharing

Navigate to Settings then the Metric Sharing tab.



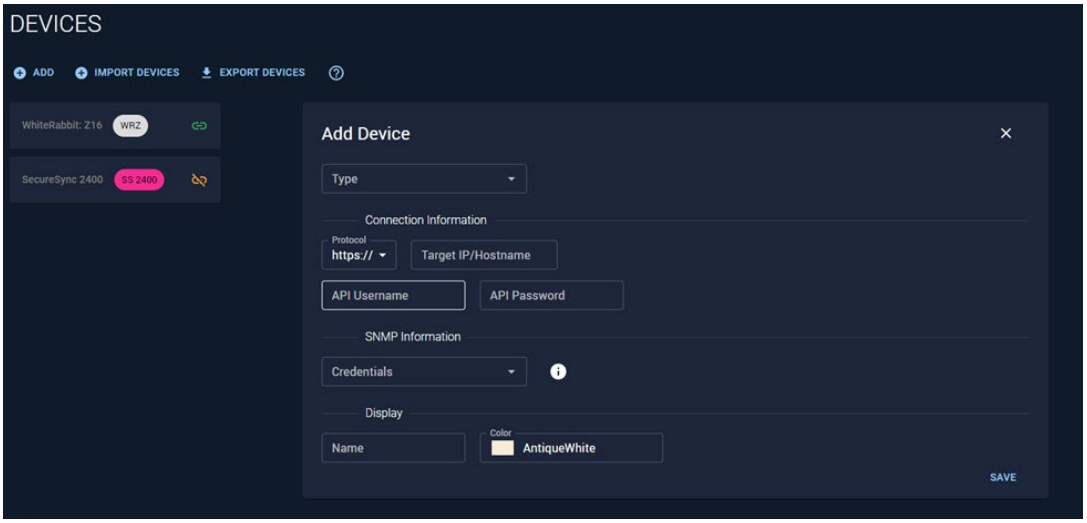
Toggle Metric Sharing off. The toggle will remain in the off position with no status displayed.



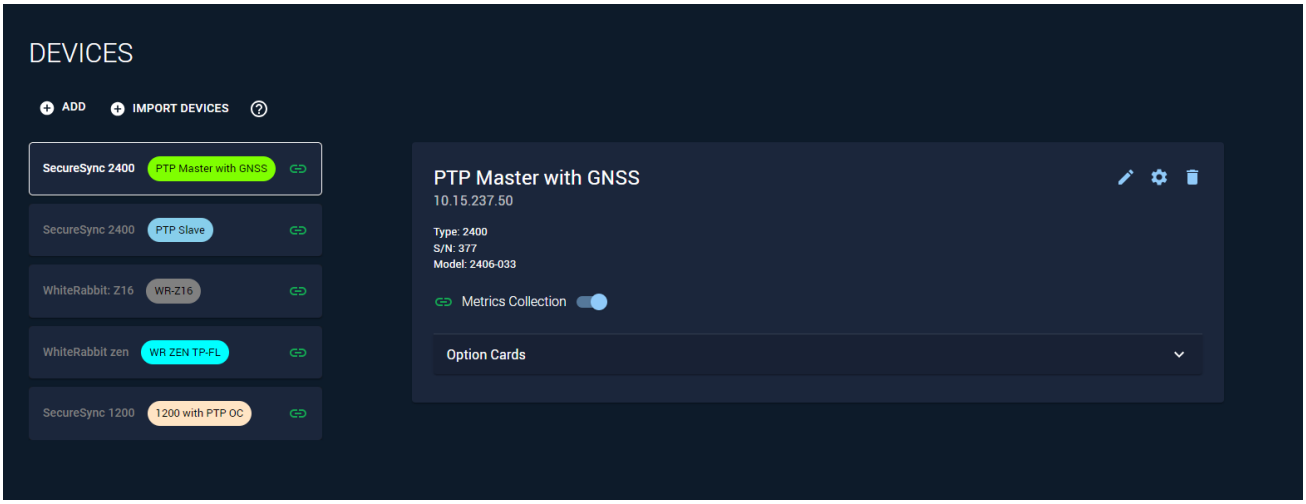
4.3. Device Management

4.3.1. Add Single Device

Navigate to the Devices tab in the header and click ADD. Enter all the information for that device, then select SAVE.

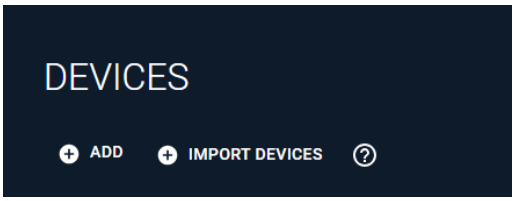


You should now see the device in the Devices list.

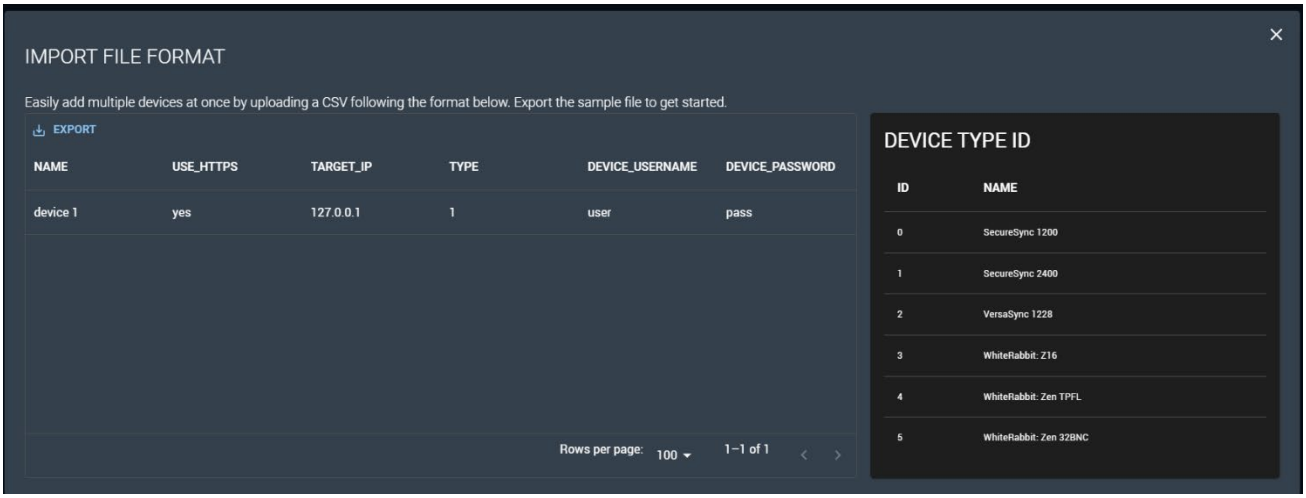


4.3.2. Import Multiple Devices

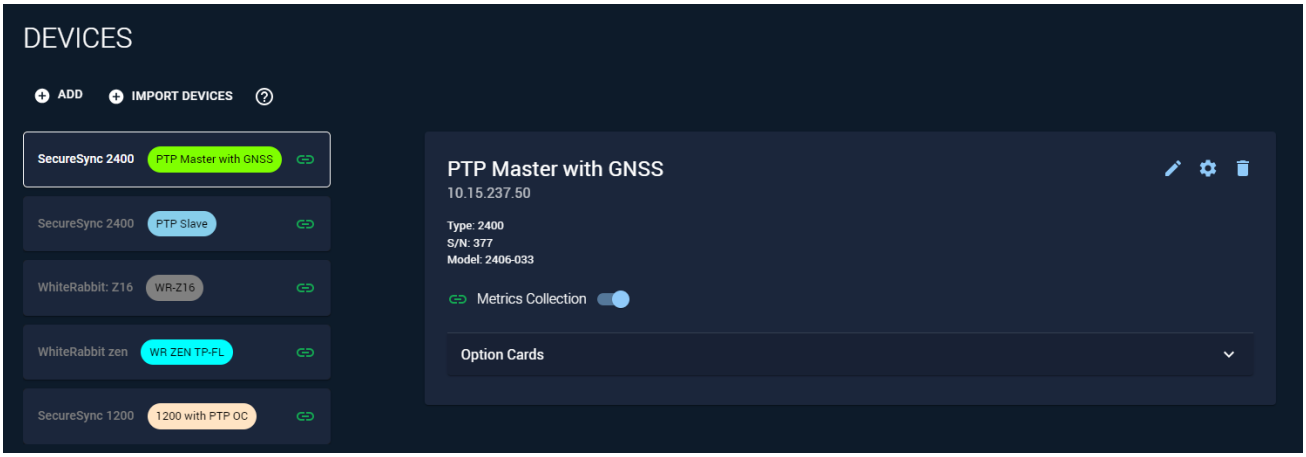
You can import a list of devices from a CSV form. To view the expected file format, Click the **?** icon on the Devices page.



You will see the file format as well as the option to export a sample file to get started.



Enter the devices you wish to monitor and then upload this file using the Import Devices button. You will see all the devices listed in the Devices page. Duplicate devices will not be added.

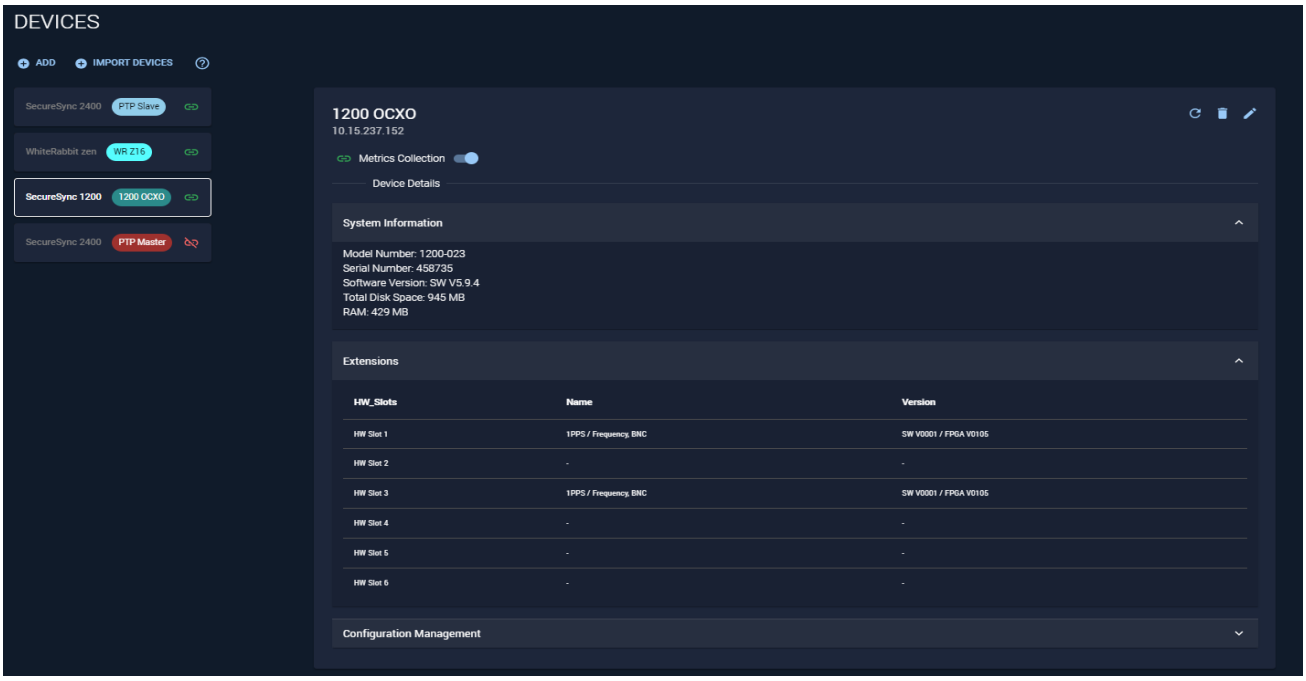


4.3.3. View Device Details

Navigate to Devices and select the device which you would like to view.

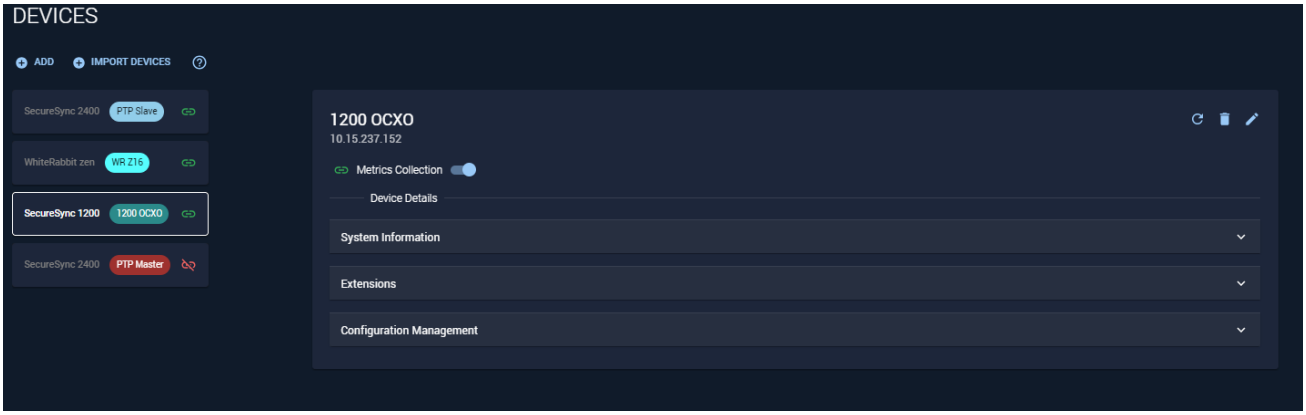
The device details are displayed to the right and include the System Information, Extensions, Configuration Management, and Available Metrics. You can edit, modify configuration, or delete the device using the buttons on this view.

- **System Information:** Relevant system information including Model Number, Serial Number, Software Version, etc.
- **Extensions:** A list of all option cards currently installed.
- **Configuration Management:** Options that allow for control of some of the device's internal configurations from the PNT 360 monitoring application as a central location.
- **Available Metrics:** A list of all available metrics and buttons to filter and export.

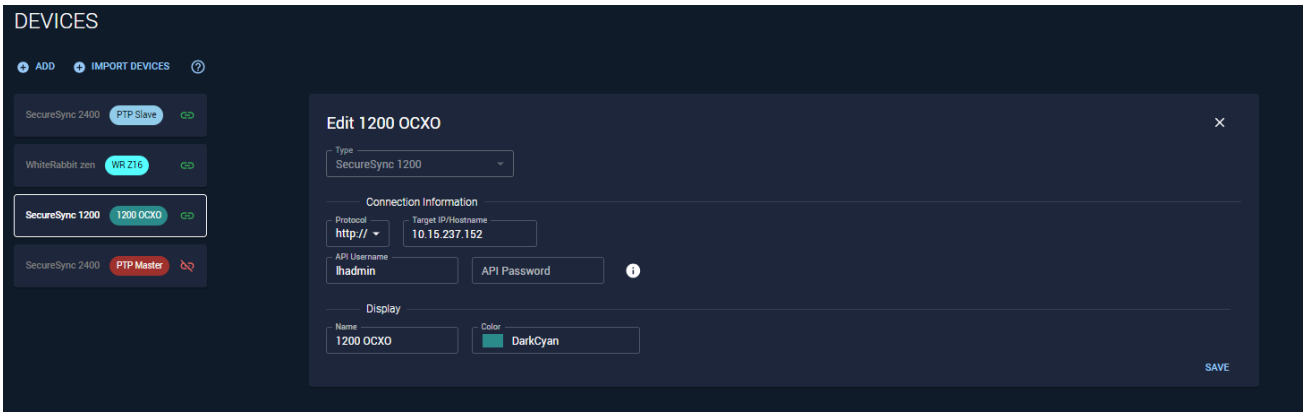


4.3.4. Edit Device

Navigate to Devices. Select the device you wish to edit and click the edit icon.



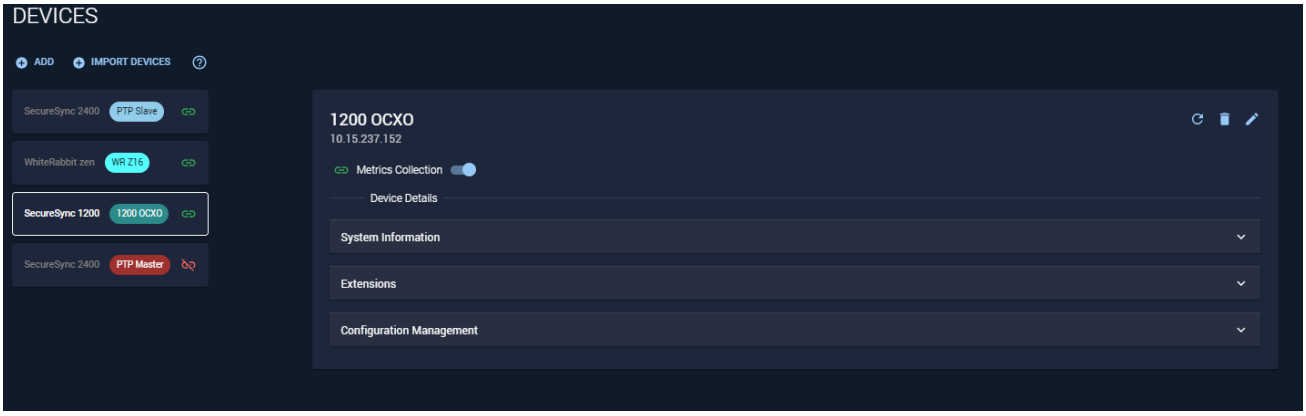
Enter the new information and click SAVE when finished.



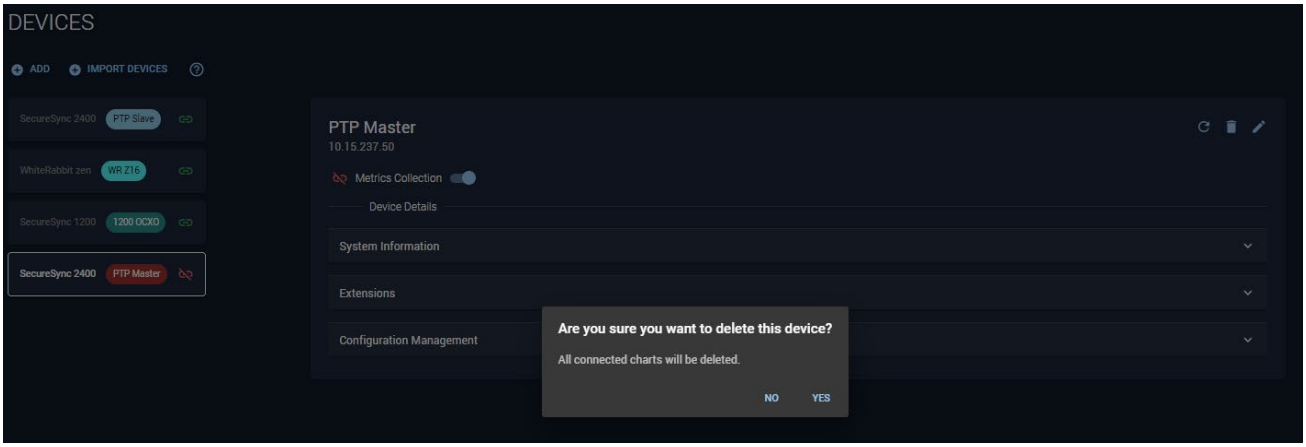
The changes will be visible in the Devices list and Device Details view.

4.3.5. Delete Device

Navigate to Devices. Select the device you wish to delete and click the delete icon.



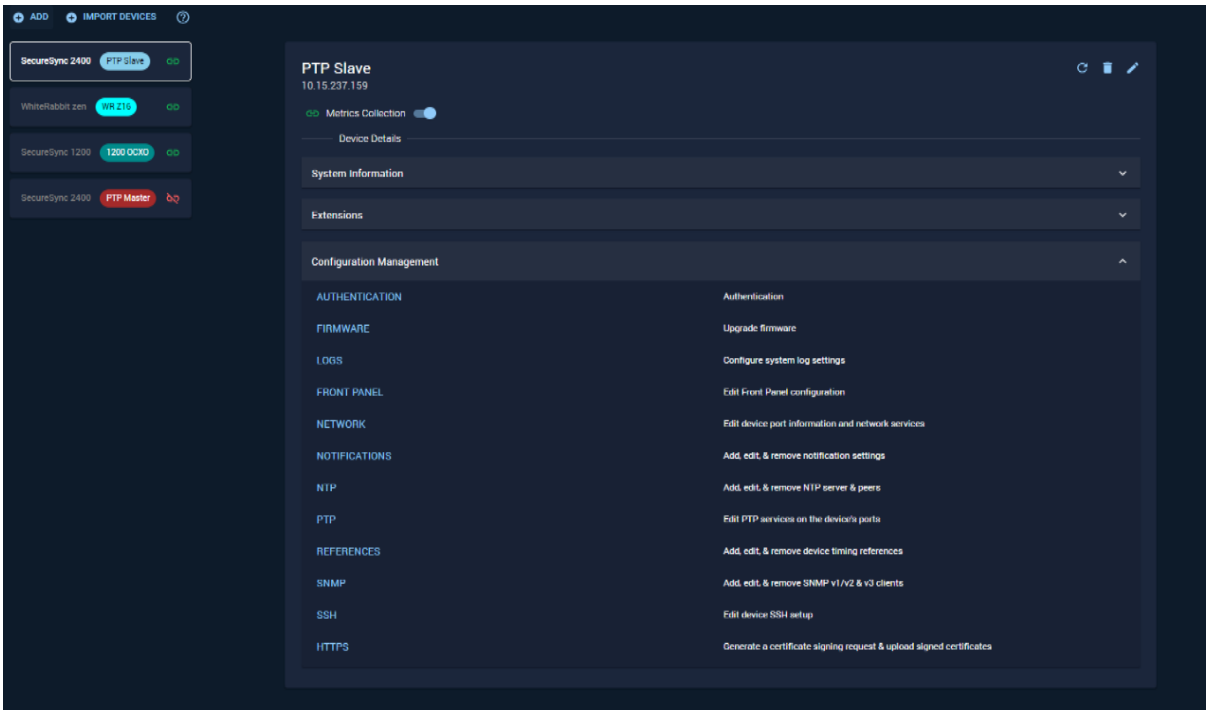
A modal will be displayed asking for confirmation that the device should be deleted.



Click Yes and the device will be removed from the devices list.

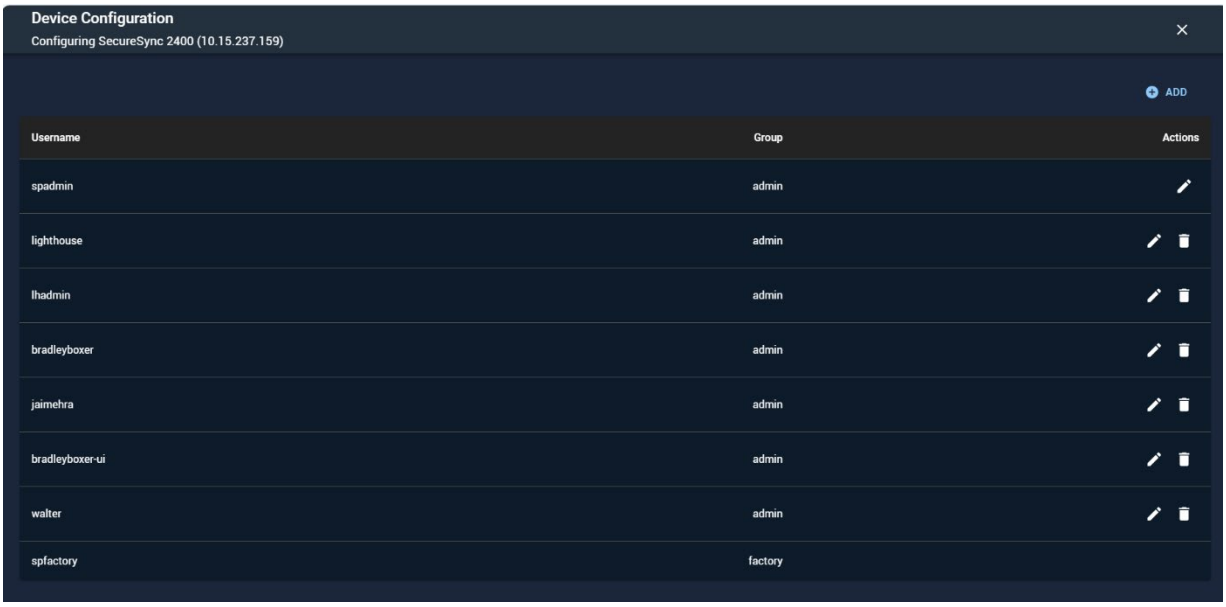
4.3.6. Configuration Management

Remote configuration is a mechanism by which you can control some of the device's internal configurations from the PNT 360 monitoring application as a central location. Navigate to Devices and click on the dropdown for Configuration Management



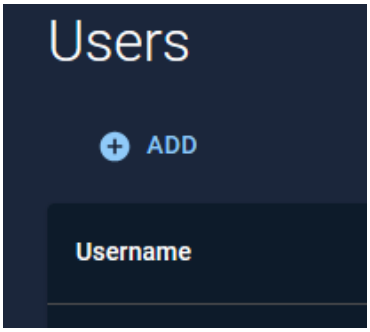
4.3.6.1. Authentication

Select the SecureSync device for which you want to configure authentication, and under the **Configuration Management** dropdown, select **Authentication**.

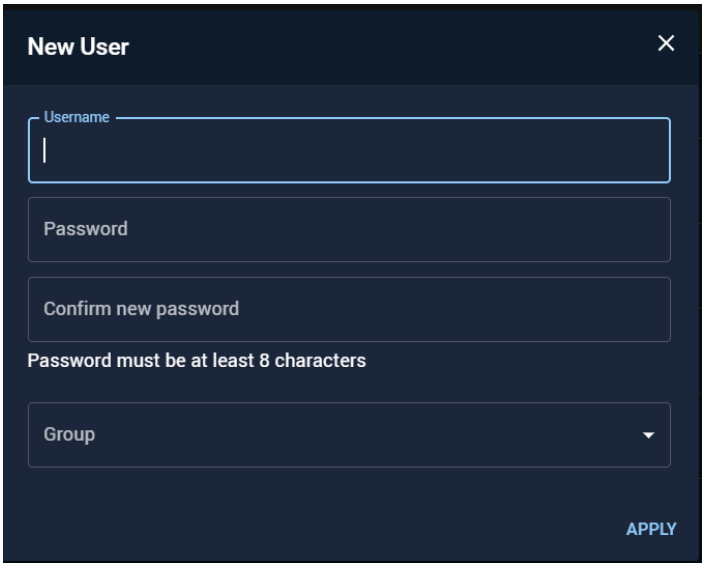


4.3.6.1.1. Add new user

Select the + Add icon to add a new user for SecureSync

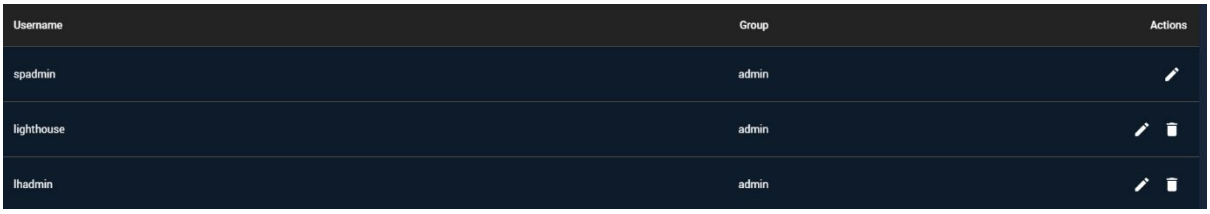


Fill out the form and click APPLY. This will add the user as well as send the configuration to the device via its REST API.

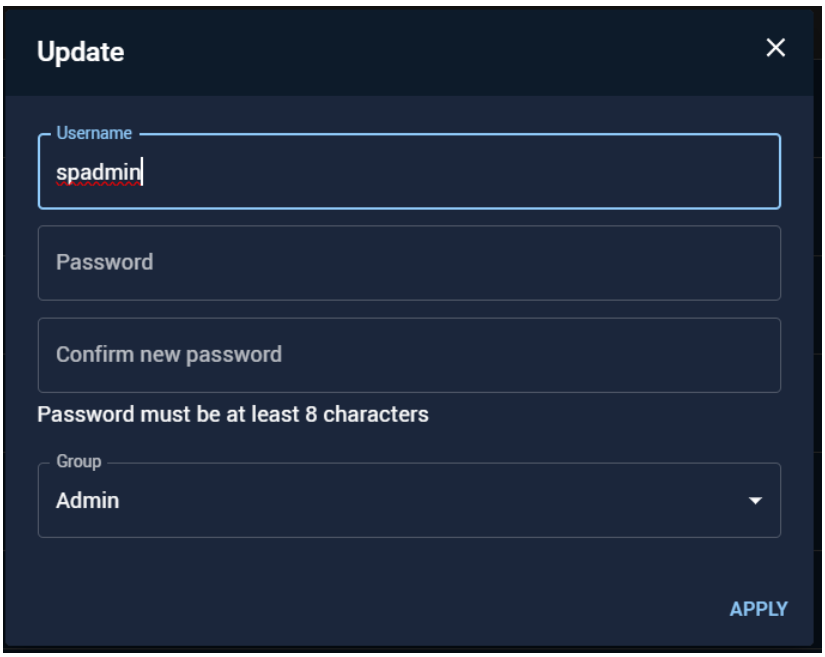


4.3.6.1.2. Edit user

Click the edit icon next to the user that you would like to modify.

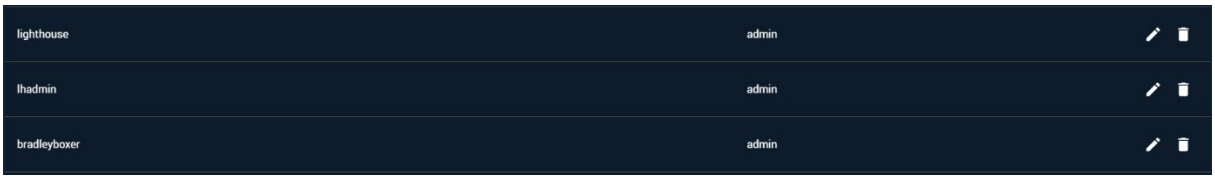


Enter the updated settings and click APPLY. This will update the user details as well as send the updated configuration to the device via its REST API

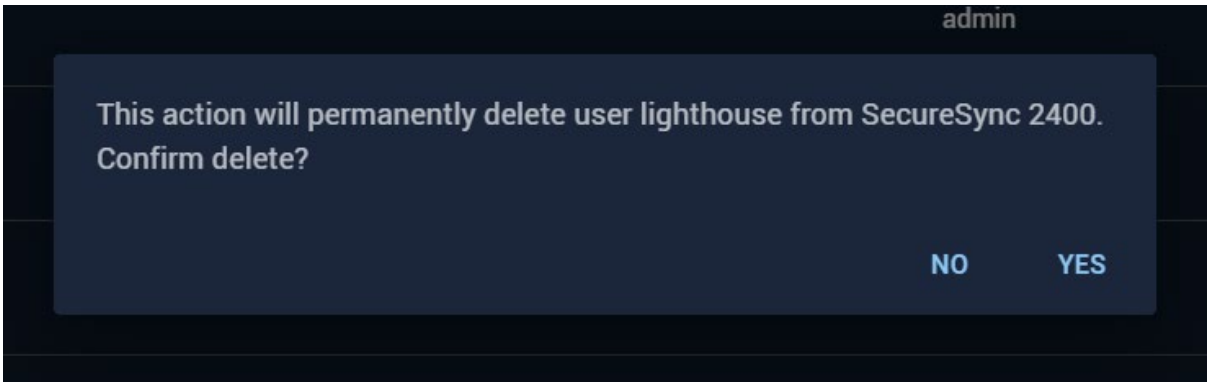


4.3.6.1.3. Delete user

Select the User you wish to delete and click the delete icon.



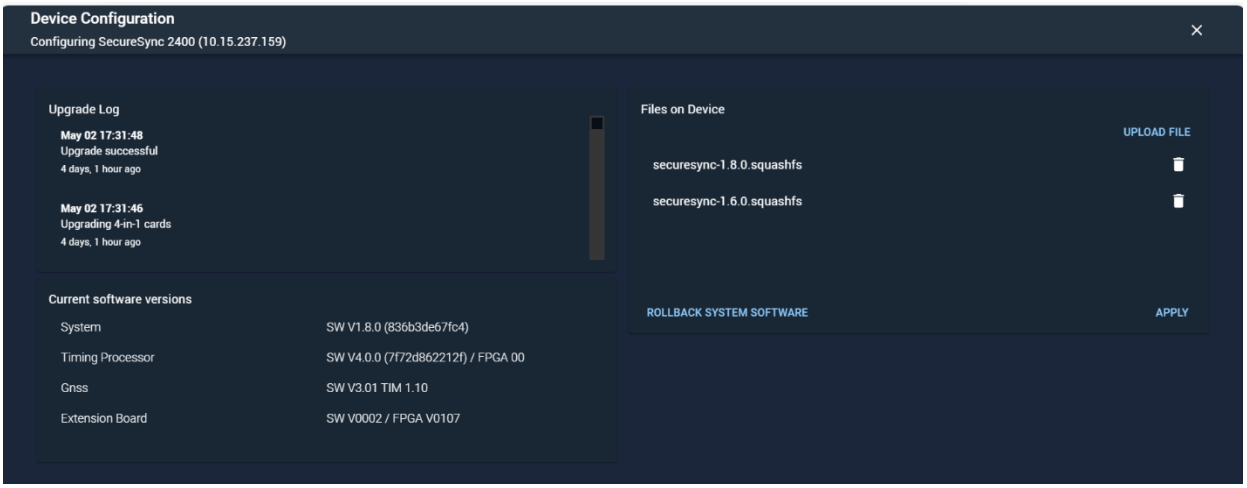
A modal will be displayed asking for confirmation that the User should be deleted.



Click Yes and the user will be removed from the Users list.

4.3.6.2. Firmware

Select the Secure Sync device for which you want to configure Firmware.



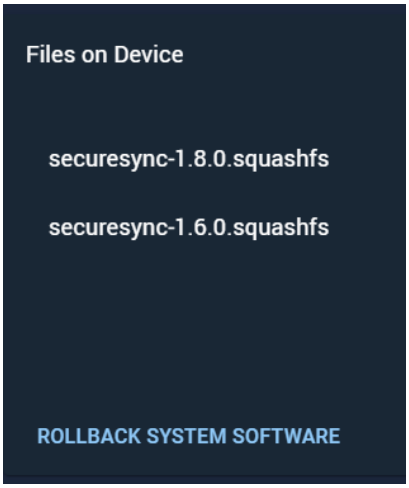
4.3.6.2.1. Upload files to SecureSync device

Click on upload file to upload any file to the SecureSync device and click APPLY.

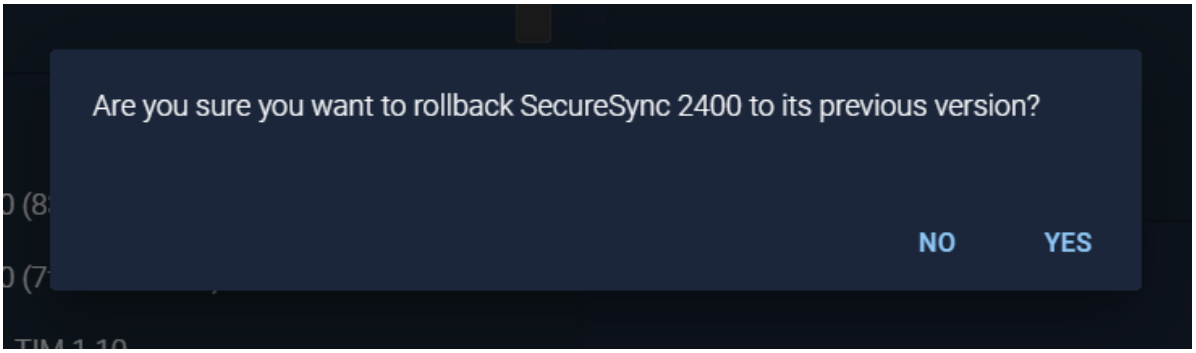
Click the delete icon to delete any file uploaded to the device.

4.3.6.2.2. Rollback System Software

Click on the ROLLBACK SYSTEM SOFTWARE button to roll back the software.



A modal will be displayed asking for confirmation to roll back the device to its previous version.



Click Yes and the device will be rolled back to its previous version.

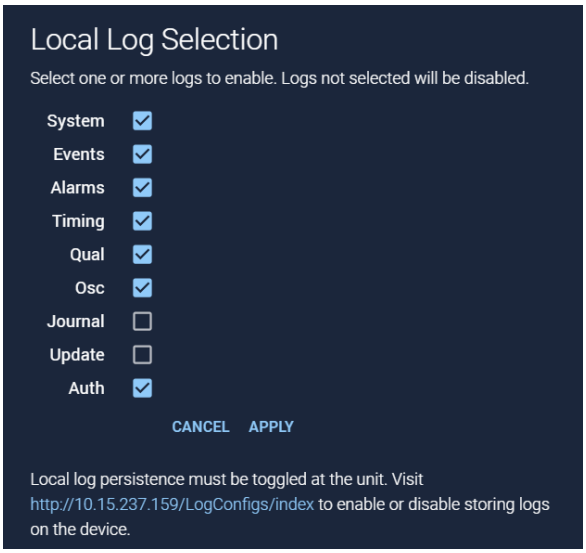
4.3.6.3. Logs

4.3.6.3.1. Configuring Logs for SecureSync

Select the device for which you want to configure Logs and add Remote Log Servers

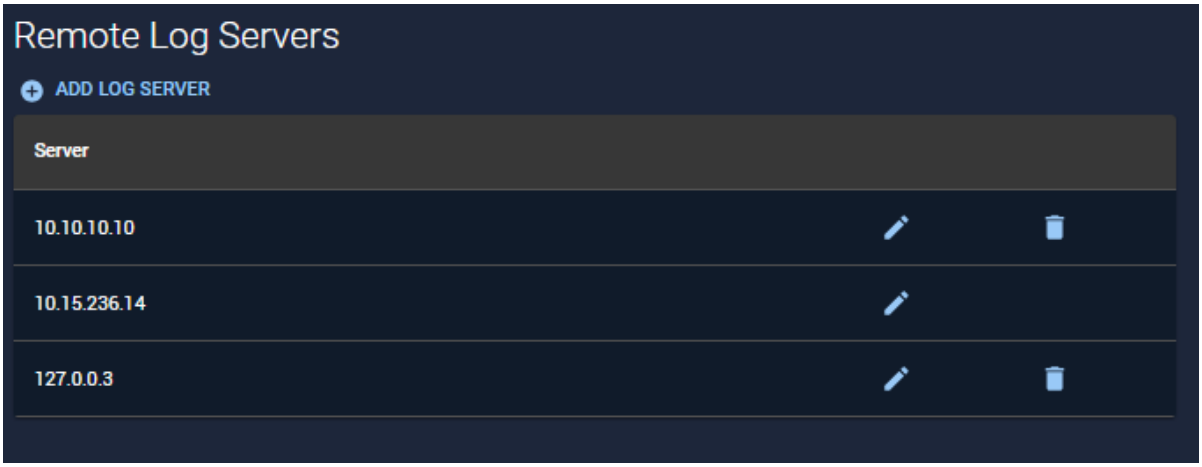
4.3.6.3.1.1. Local Log Selection

Select one or more logs to enable and the ones not selected will be disabled. Click APPLY to apply the changes.

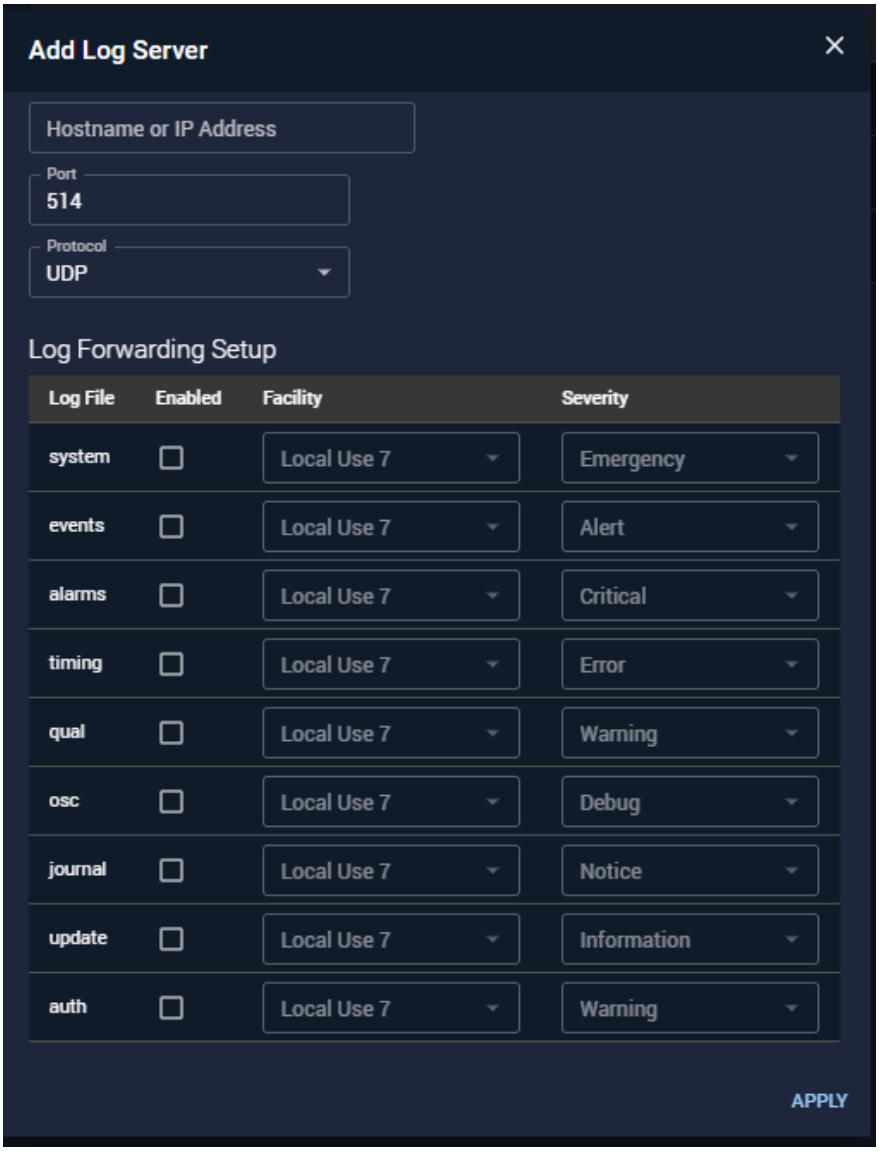


4.3.6.3.1.2. Add Remote Log Server

Click on the +ADD LOG SERVER button to add a log server.

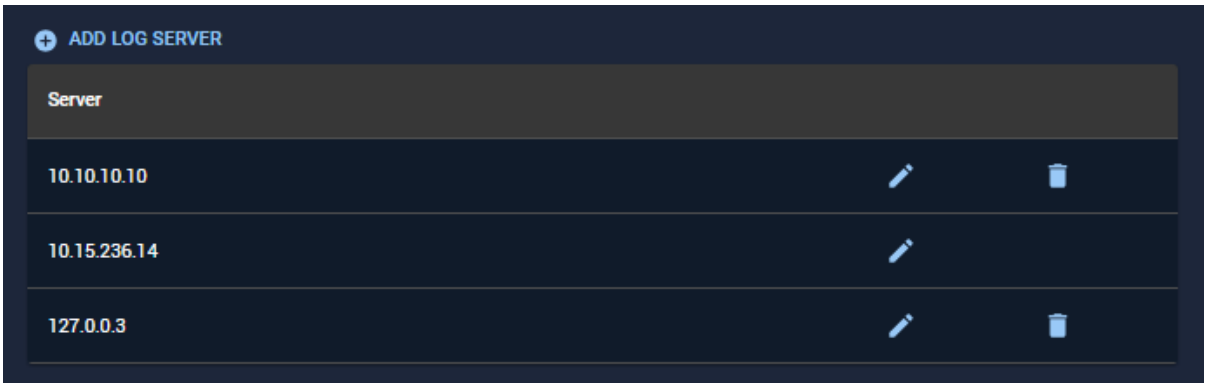


Fill out the form and click APPLY. This will add the configuration as well as send the configuration to the device via its REST API.

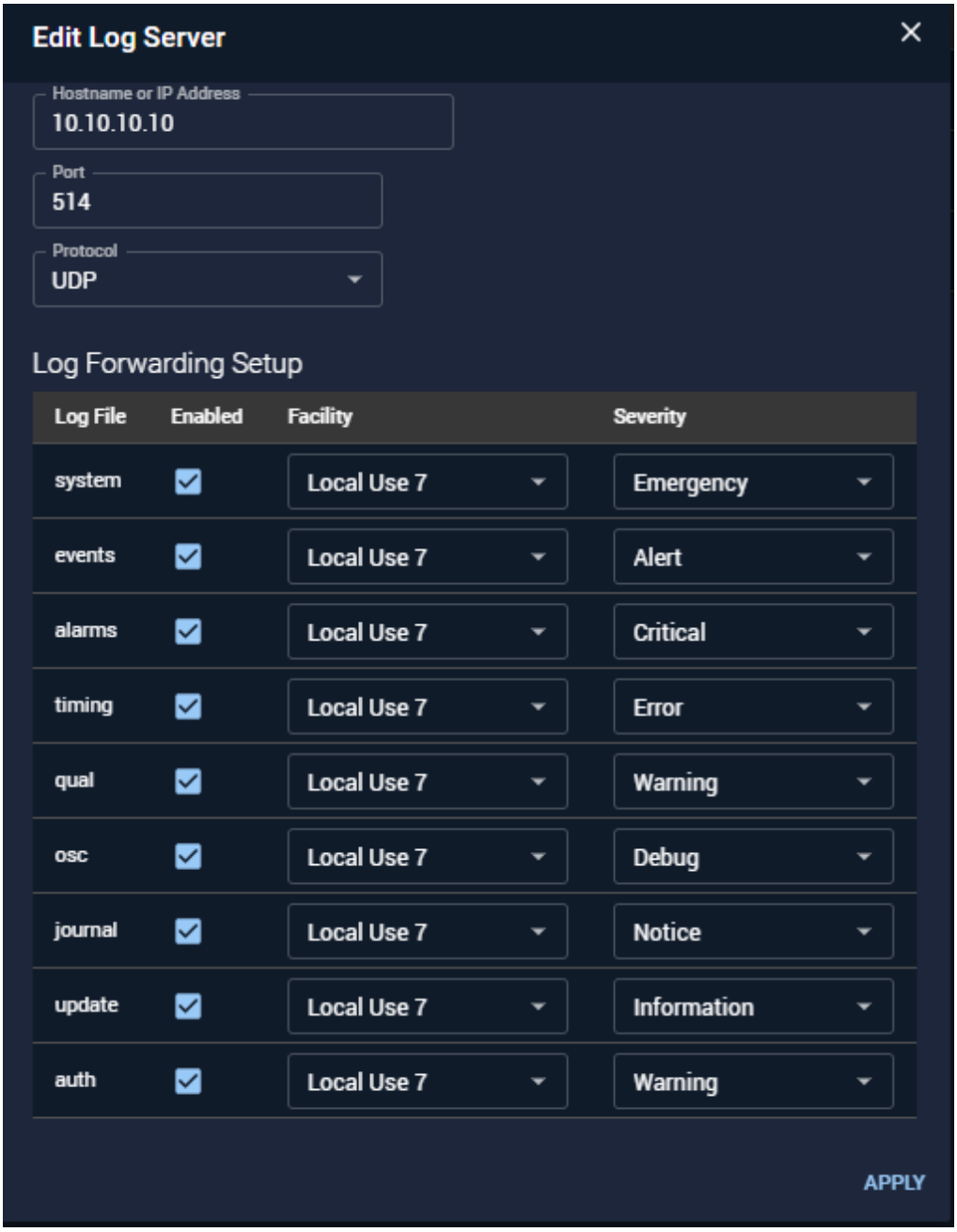


4.3.6.3.1.3. Edit Log Server

Click the edit icon next to the configuration that you would like to modify.



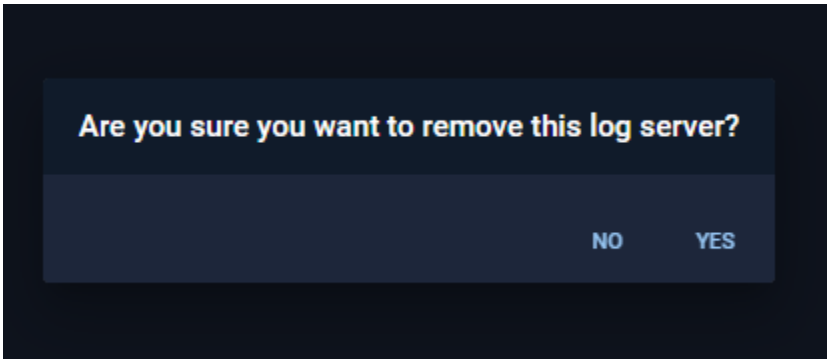
Enter the updated settings and click APPLY. This will update the configuration as well as send the updated configuration to the device via its REST API



4.3.6.3.1.4. Delete Log Server

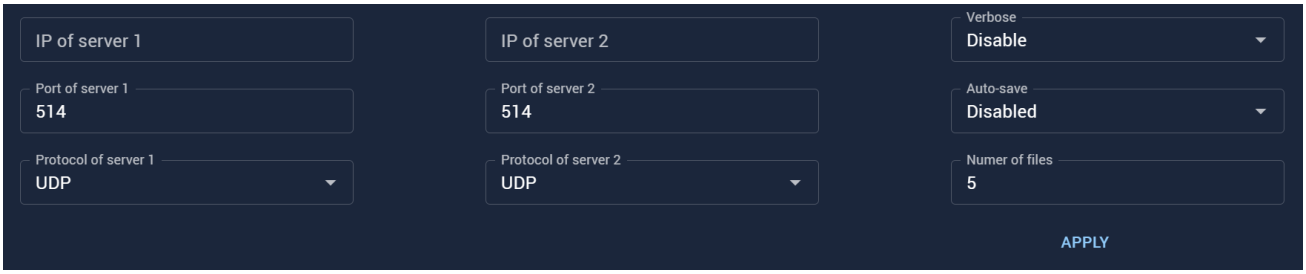
Select the Log Server you wish to delete and click the delete icon.

A modal will be displayed asking for confirmation that the Log Server should be deleted.



Click Yes and the configuration will be removed from the Log Servers list.

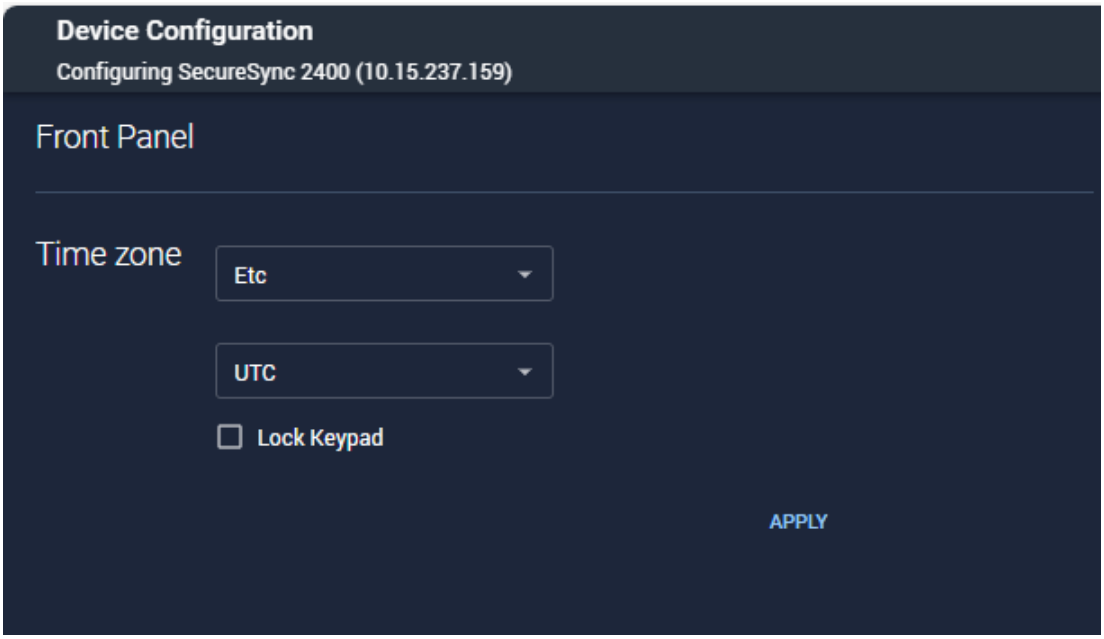
4.3.6.3.2. Configuring Logs for White Rabbit device



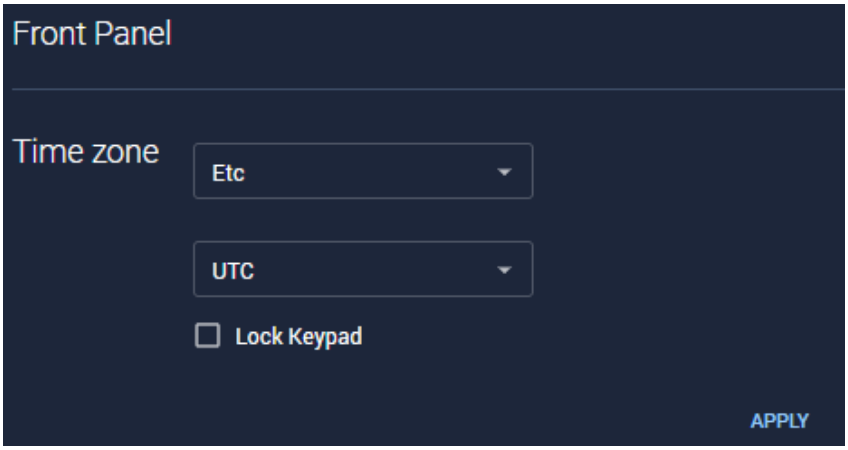
Fill out the form and click APPLY. This will add the configuration as well as send the configuration to the device via its REST API.

4.3.6.4. Front Panel

Select the device for which you want to configure and view the configured Front Panel settings.



4.3.6.4.1. Edit Front Panel Configuration

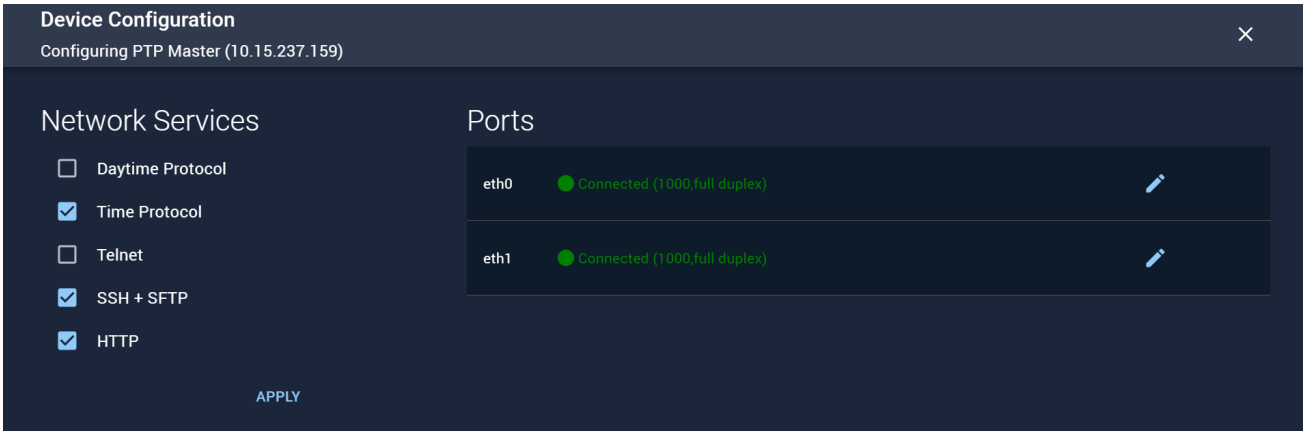


Update the fields from the dropdown and click Apply. This will update the configuration as well as send the configuration to the device via its REST API.

4.3.6.5. Network

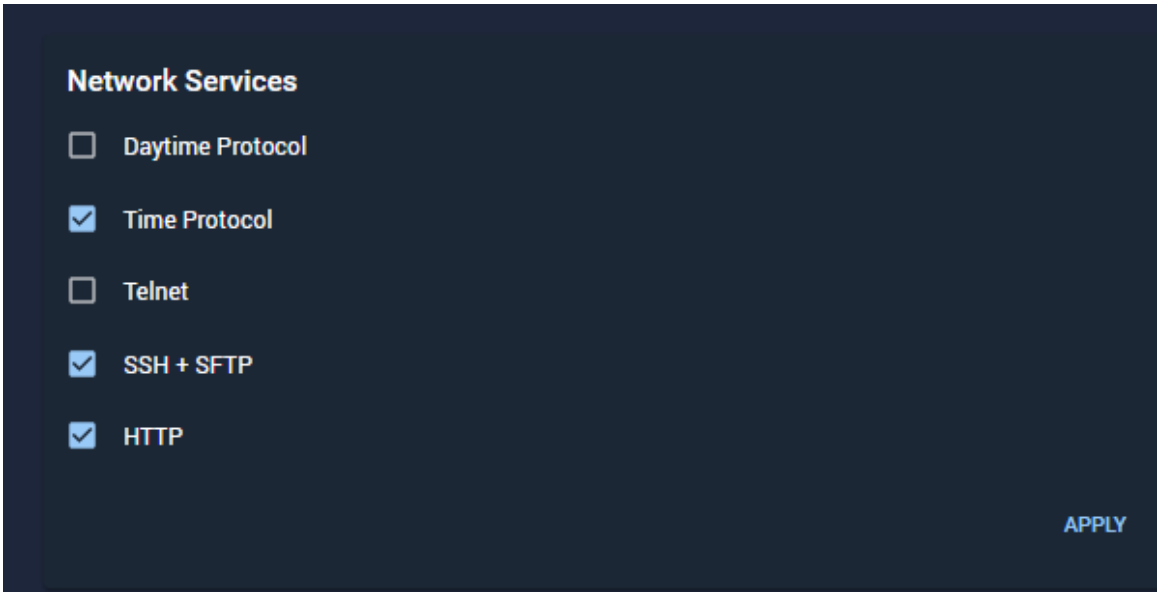
4.3.6.5.1. Configuring Network for SecureSync devices

Select the Device for which you want to configure Network services and ports



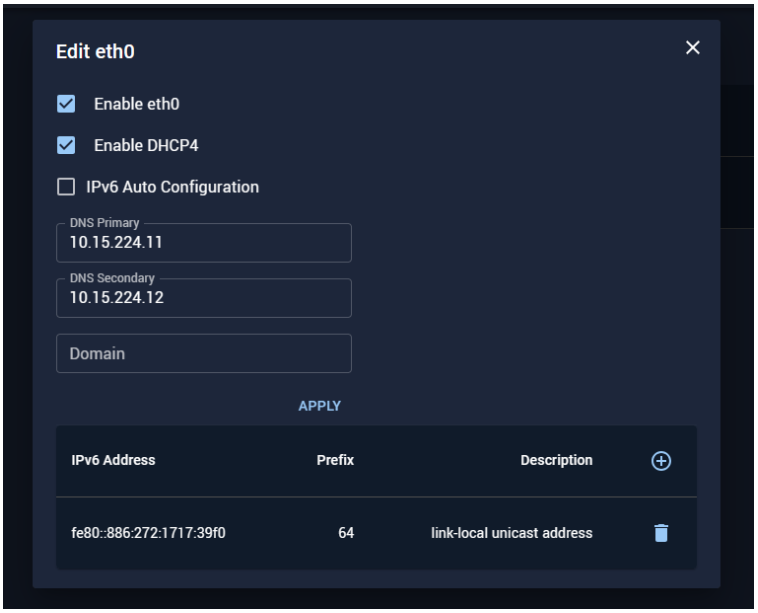
4.3.6.5.1.1. Enable Network Services

Select one or more services to enable and the ones not selected will be disabled. Click APPLY to apply the changes.



4.3.6.5.1.2. Edit Ethernet Port Setting

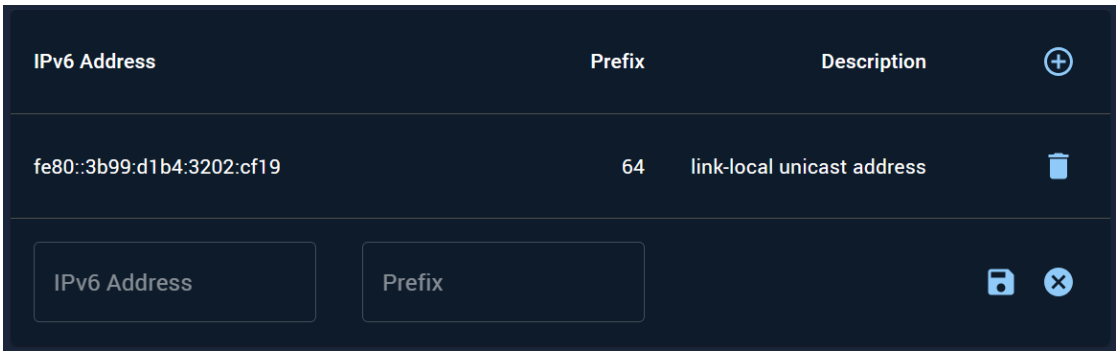
Select the edit icon for the ethernet port that you wish to modify and a modal with settings should appear.



Enter the updated settings and select APPLY.

Add new IPv6 address

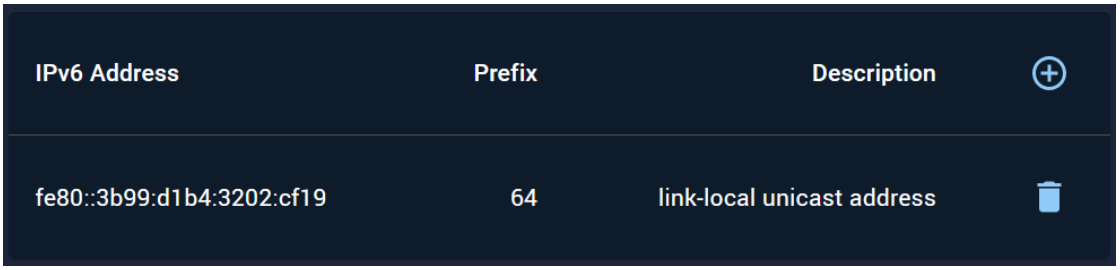
Select the + icon to add a new IPv6 address



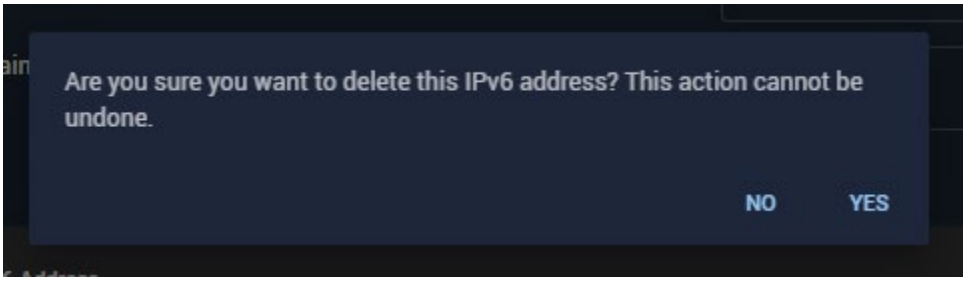
Fill out the IPv6 address and Prefix and click on the Save icon to save the changes

Delete IPv6 address

Select the IPv6 address you wish to delete and select the delete icon.



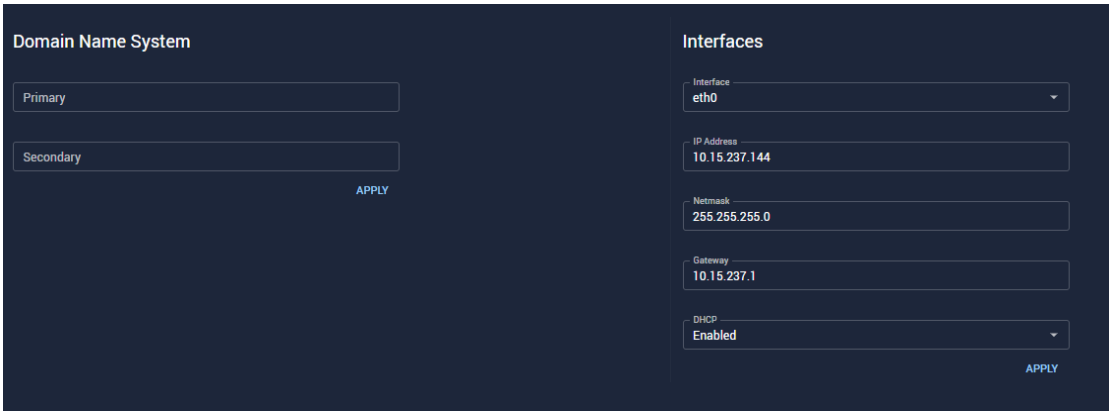
A modal will be displayed asking for confirmation that the IPv6 address should be deleted.



Select Yes and the IPv6 address will be removed from the IPv6address list.

4.3.6.5.2. Configuring Network for White Rabbit devices

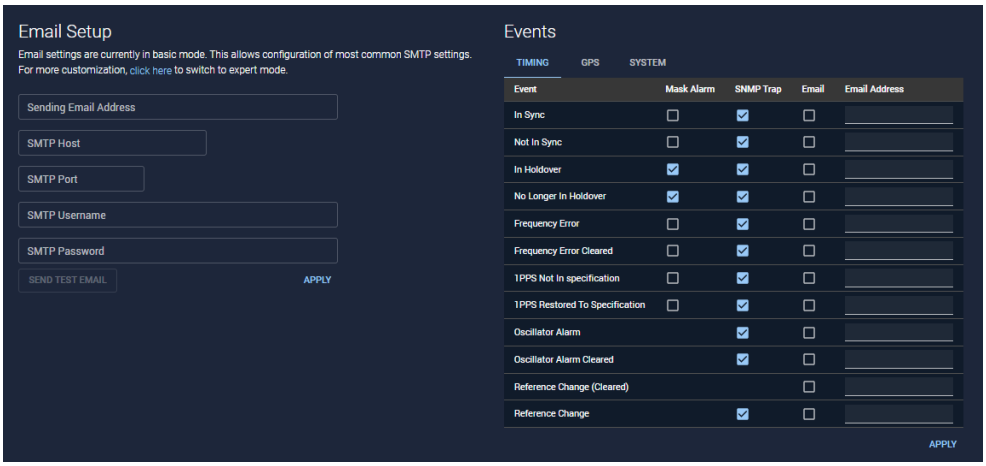
Select the Device for which you want to configure Network interfaces and domains



Fill out the form and click APPLY. This will add the configuration as well as send the configuration to the device via its REST API.

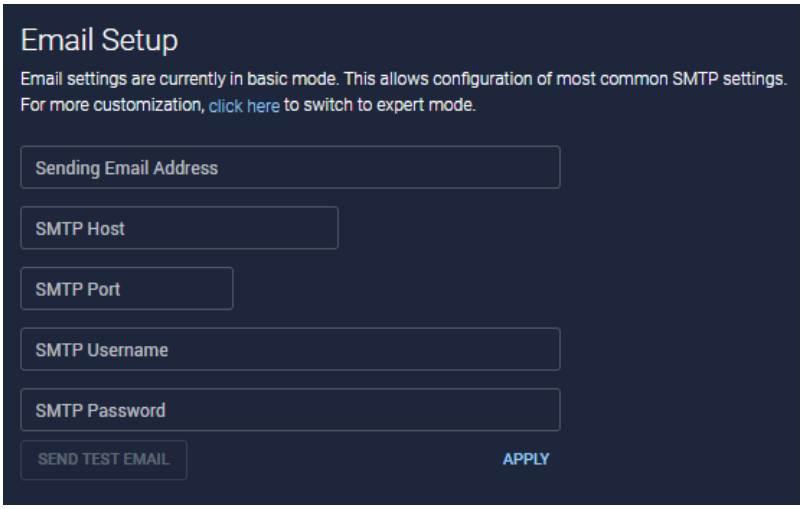
4.3.6.6. Notifications

Select the device for which you want to configure Notifications.



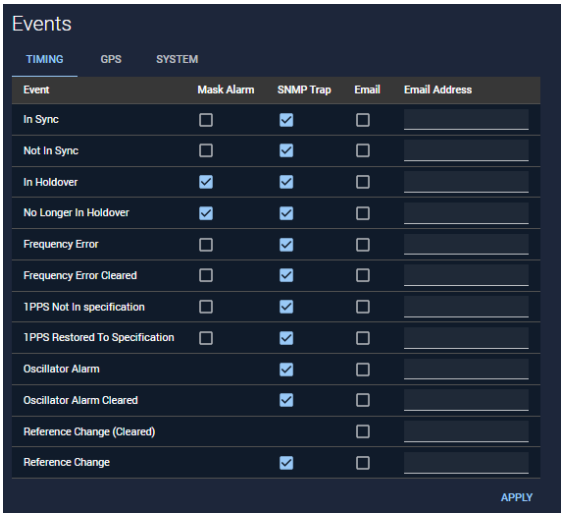
4.3.6.6.1. Configure Email Setup

Fill out the form to configure SMTP setting and click APPLY. This will add the configuration as well as send the configuration to the device via its REST API.



4.3.6.6.2. Configure Events

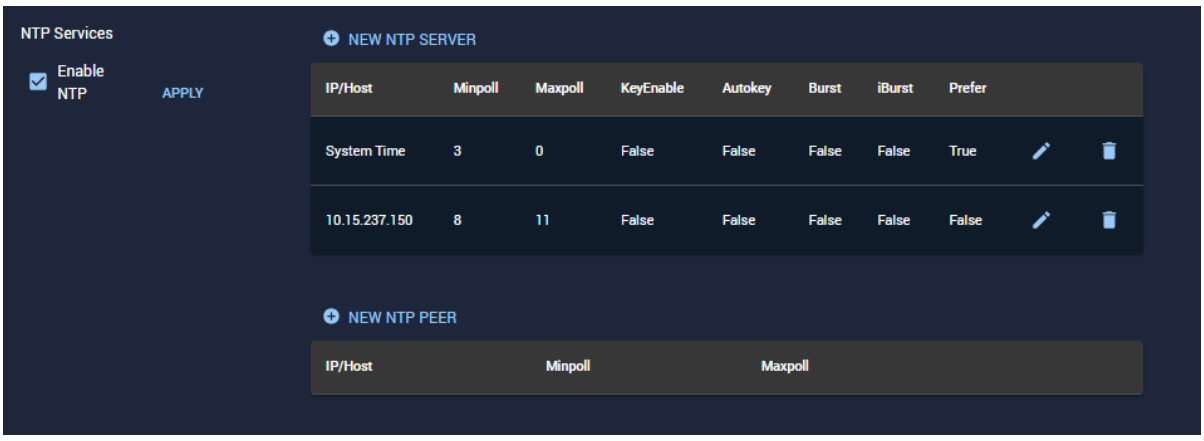
Select one or more events and enter the email address to be used to notify the events. Click APPLY to apply the changes.



4.3.6.7. NTP

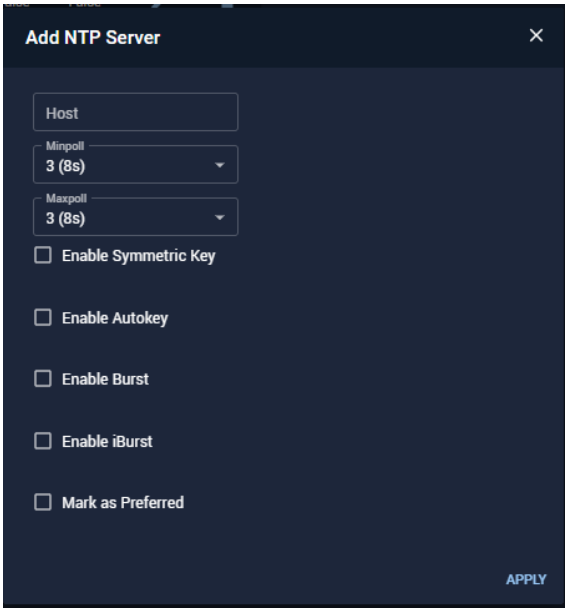
4.3.6.7.1. Configuring NTP for SecureSync devices

Select the device for which you want to configure NTP to view, edit and add a new NTP server.



4.3.6.7.1.1. Add NTP Server

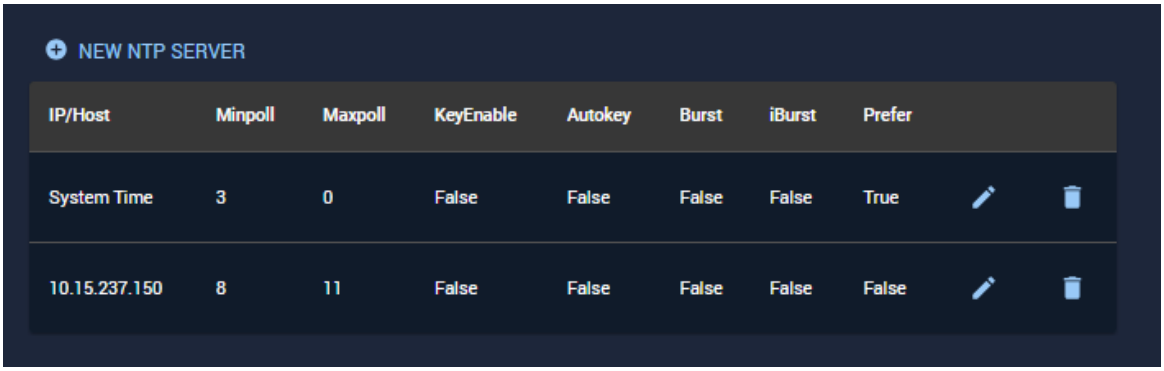
Click the + NEW NTP SERVER button to add a new reference priority.



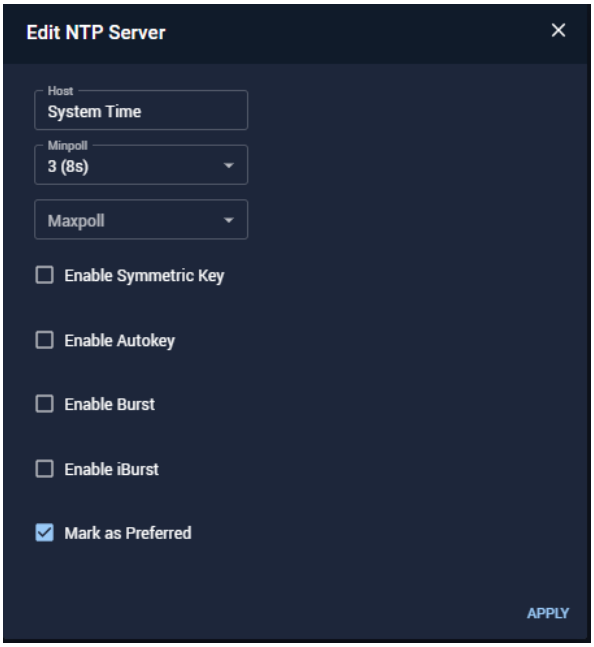
Fill out the form and click Add. This will add the configuration as well as send the configuration to the device via its REST API.

4.3.6.7.1.2. Edit NTP Server

Click the edit icon next to the configuration that you would like to modify.



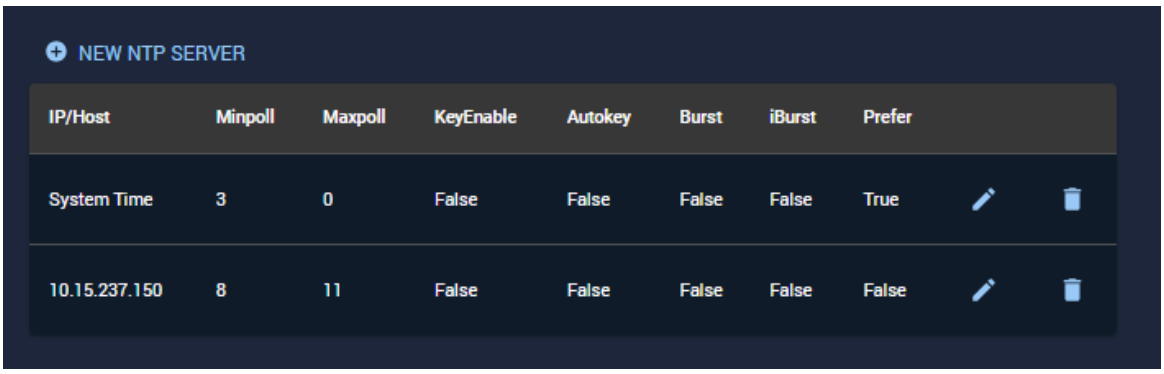
The current settings will be displayed in a modal.



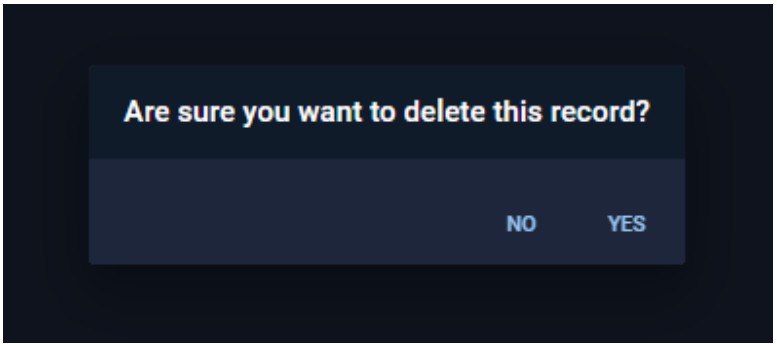
Enter the updated settings and click APPLY. This will update the configuration as well as send the updated configuration to the device via its REST API.

4.3.6.7.1.3. Delete NTP Server

Select the NTP Server you wish to delete and click the delete icon.



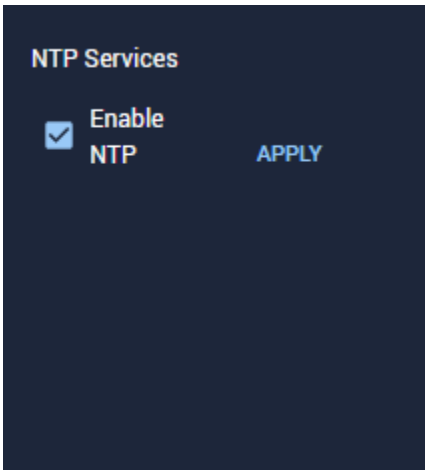
A modal will be displayed asking for confirmation that the NTP Server should be deleted.



Click Yes and the configuration will be removed from the NTP Servers list.

4.3.6.7.1.4. Enable/Disable NTP Services

Select the checkbox to enable the NTP services or unselect the checkbox to disable the NTP services for the selected device



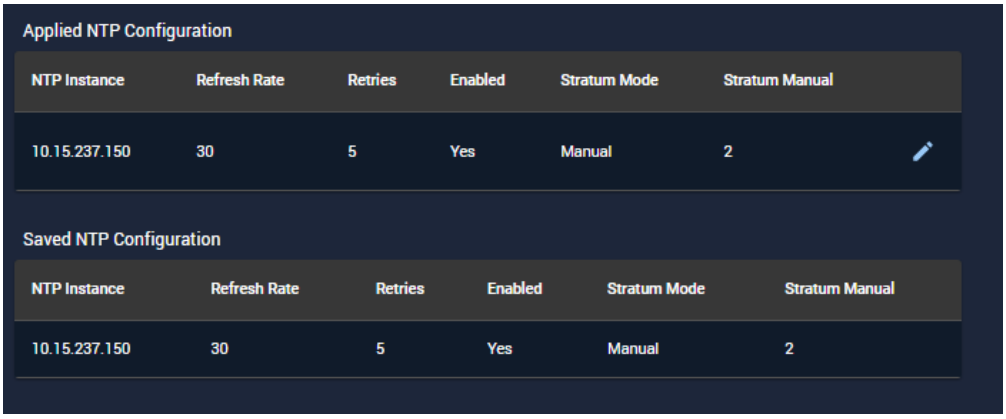
Click APPLY to apply the changes.

4.3.6.7.2. Configuring NTP for White Rabbit devices

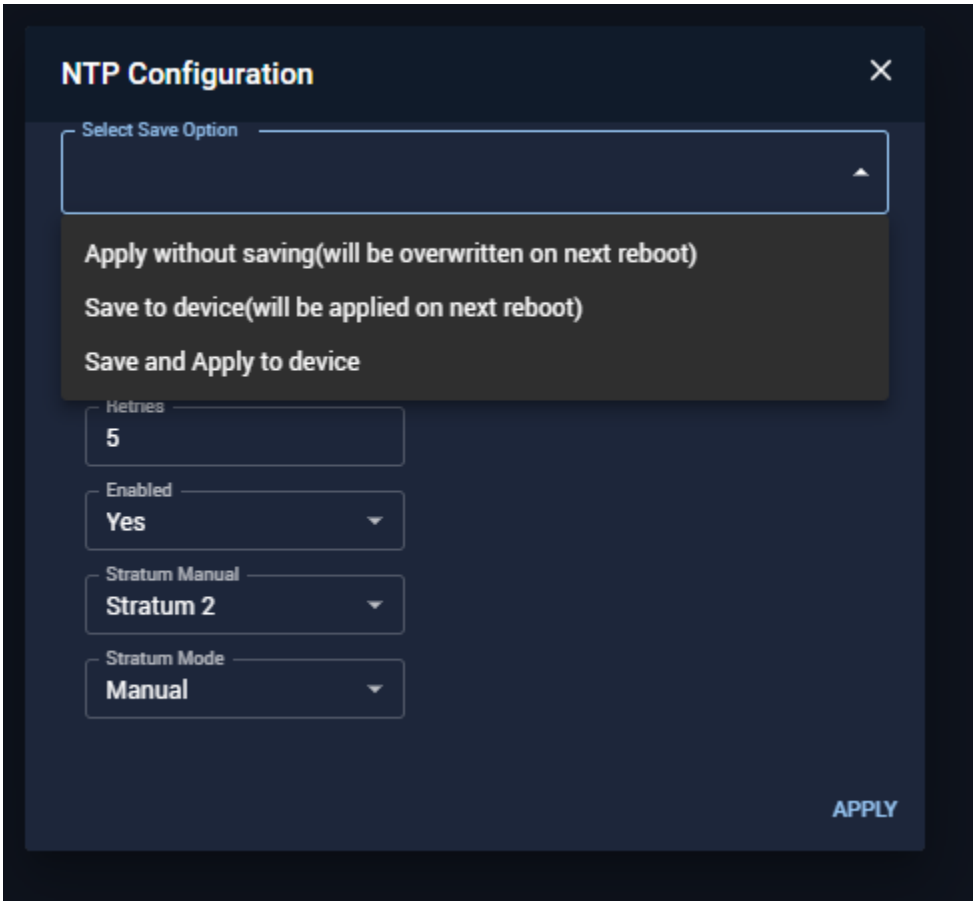
Select the device for which you want to configure NTP to view and edit the NTP Configuration.

4.3.6.7.2.1. Edit NTP Configuration

Click the edit icon for the NTP instance added.



Update the fields and select an option from the dropdown to apply changes accordingly.



This will update the configuration as well as send the configuration to the device via its REST API. You can view the saved configuring under Saved NTP Configuration which will be applied to the device on the next reboot.

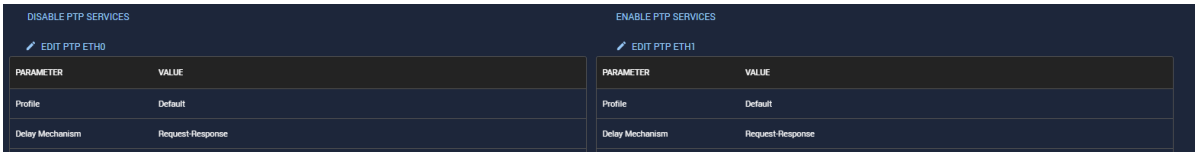
4.3.6.8. PTP

4.3.6.8.1. Configuring PTP for SecureSync devices

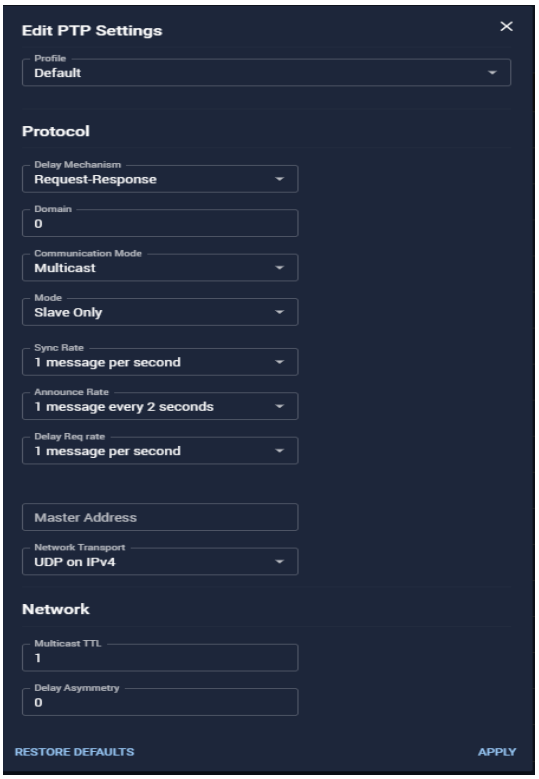
Select the device for which you want to configure PTP to view and edit PTP Servers.

4.3.6.8.1.1. Edit PTP Server

Click the edit icon for the PTP interface that you would like to modify.

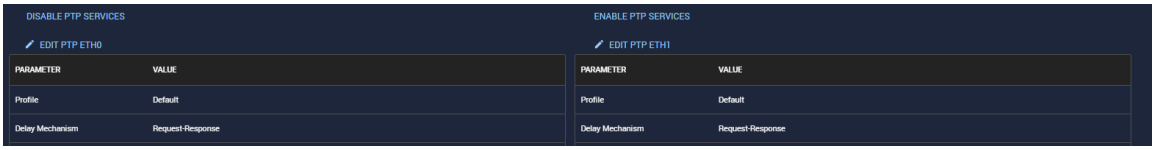


Enter the updated settings and click APPLY. This will update the configuration as well as send the updated configuration to the device via its REST API.

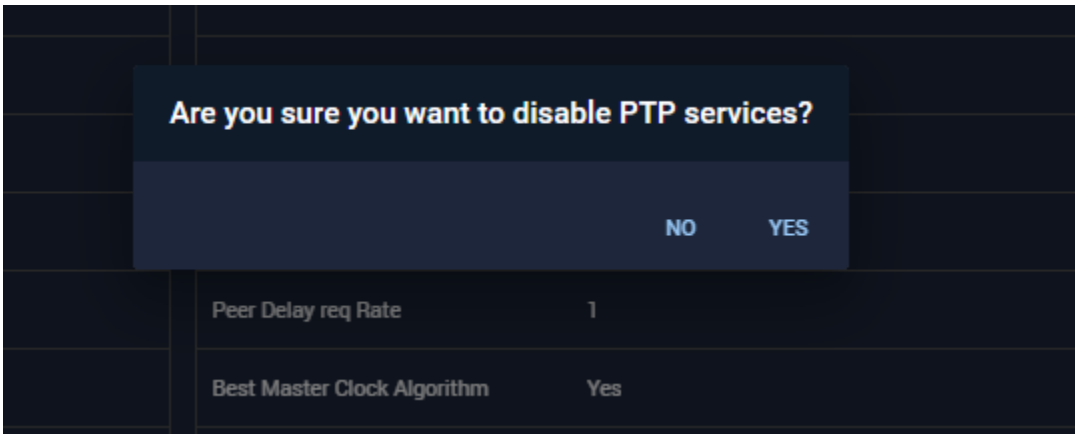


4.3.6.8.1.2. Disable/ Enable PTP Services

Click on Disable PTP Services to disable it for the PTP interface that you would want to.

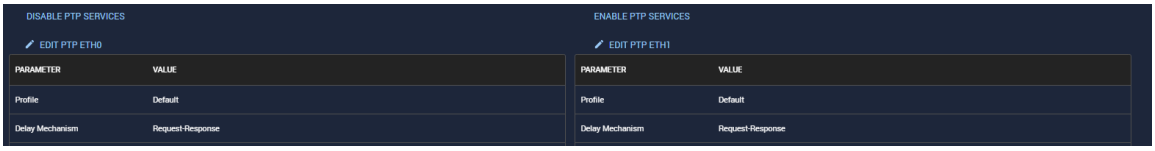


A modal will be displayed asking for confirmation that the PTP services will be disabled.



Click yes and the services will be disabled.

You can Enable the PTP services by following the same steps.

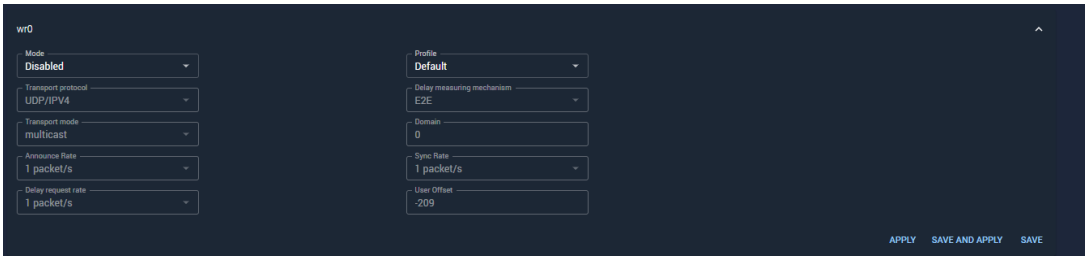


4.3.6.8.2. Configuring PTP for White Rabbit devices

Select the device for which you want to configure PTP.

4.3.6.8.2.1. Edit PTP interface

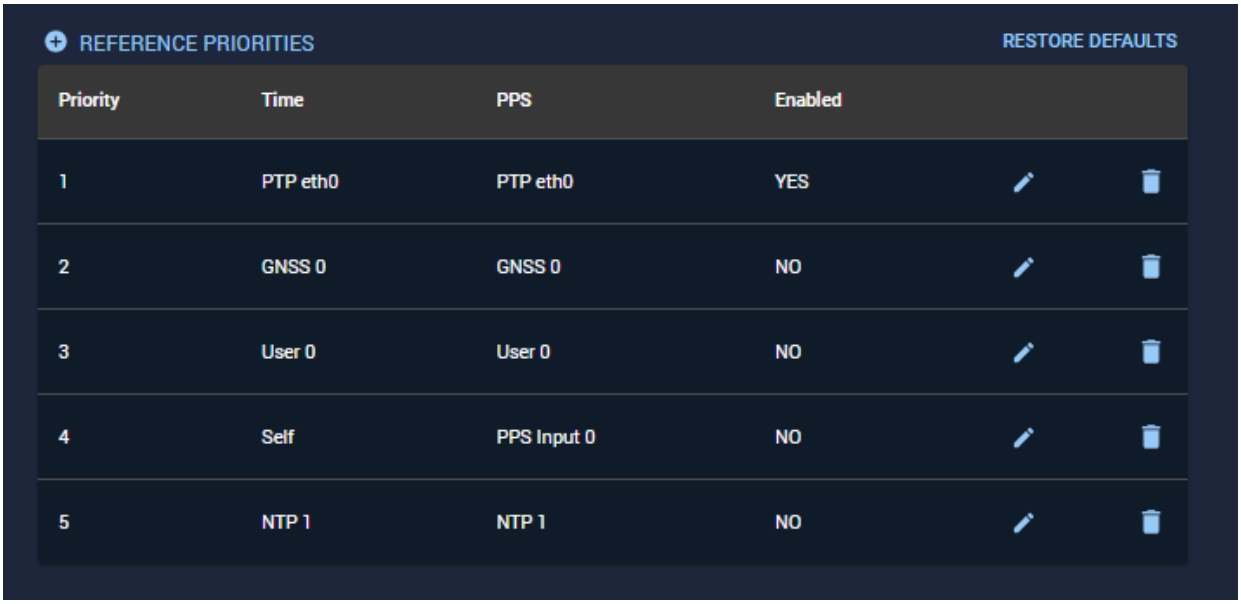
Select the interface that you wish to modify by clicking on the dropdown



Enter the updated settings and select the save or apply option to make changes. This will update the configuration as well as send the updated configuration to the device via its REST API.

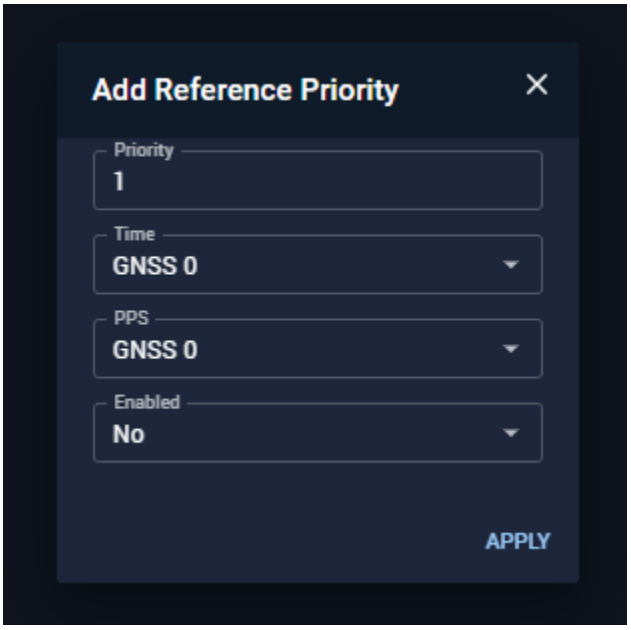
4.3.6.9. References

Select the device for which you want to configure References to view, edit and add new References config.



4.3.6.9.1. New Reference Priority

Click the + REFERENCE PRIORITIES button to add a new reference priority.

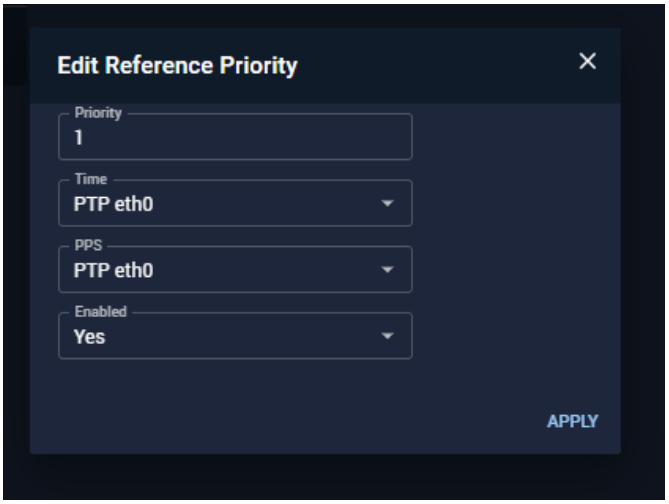


Fill out the form and click Add. This will add the configuration as well as send the configuration to the device via its REST API.

4.3.6.9.2. Edit Reference Priority

Click the edit icon next to the configuration that you would like to modify.

The current settings will be displayed in a modal.

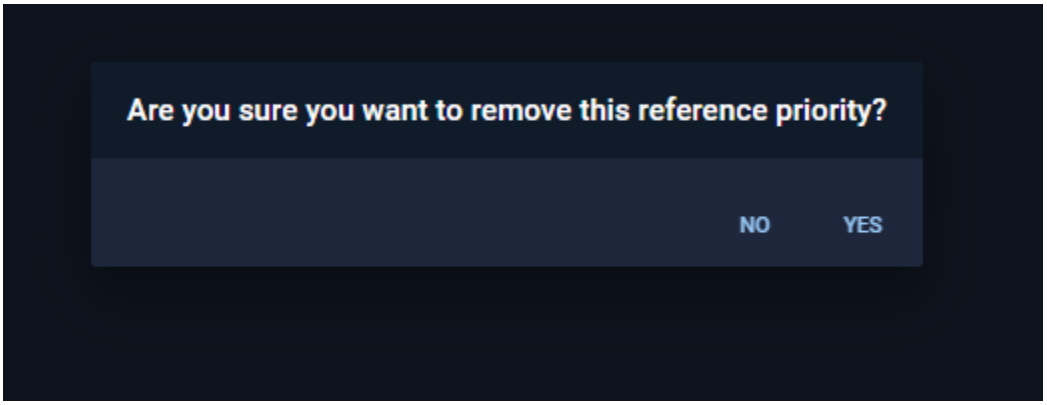


Enter the updated settings and click APPLY. This will update the configuration as well as send the updated configuration to the device via its REST API.

4.3.6.9.3. Delete Reference Priority

Select the Reference Priority you wish to delete and click the delete icon.

A modal will be displayed asking for confirmation that the Reference Priority should be deleted.

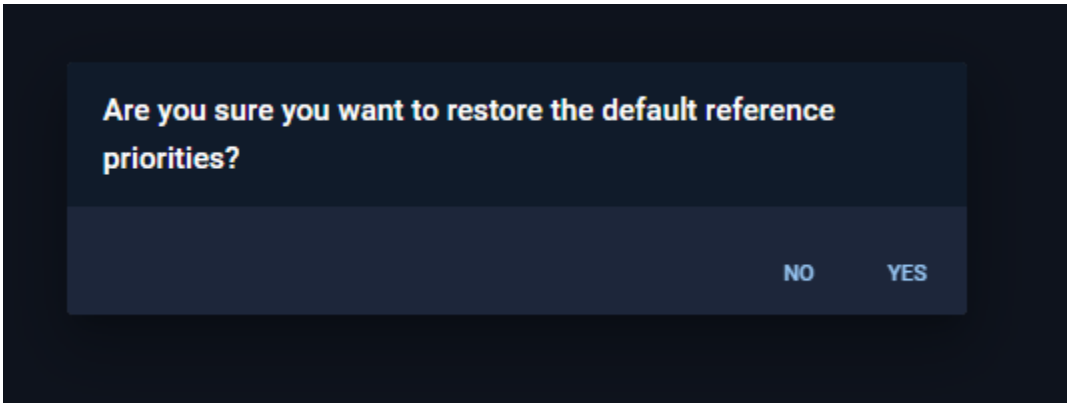


Click Yes and the configuration will be removed from the Reference Priorities list.

4.3.6.9.4. Restore default configuration

Click on Restore Defaults to restore the default configuration

A modal will be displayed asking for confirmation that the configuration will be restored to defaults.

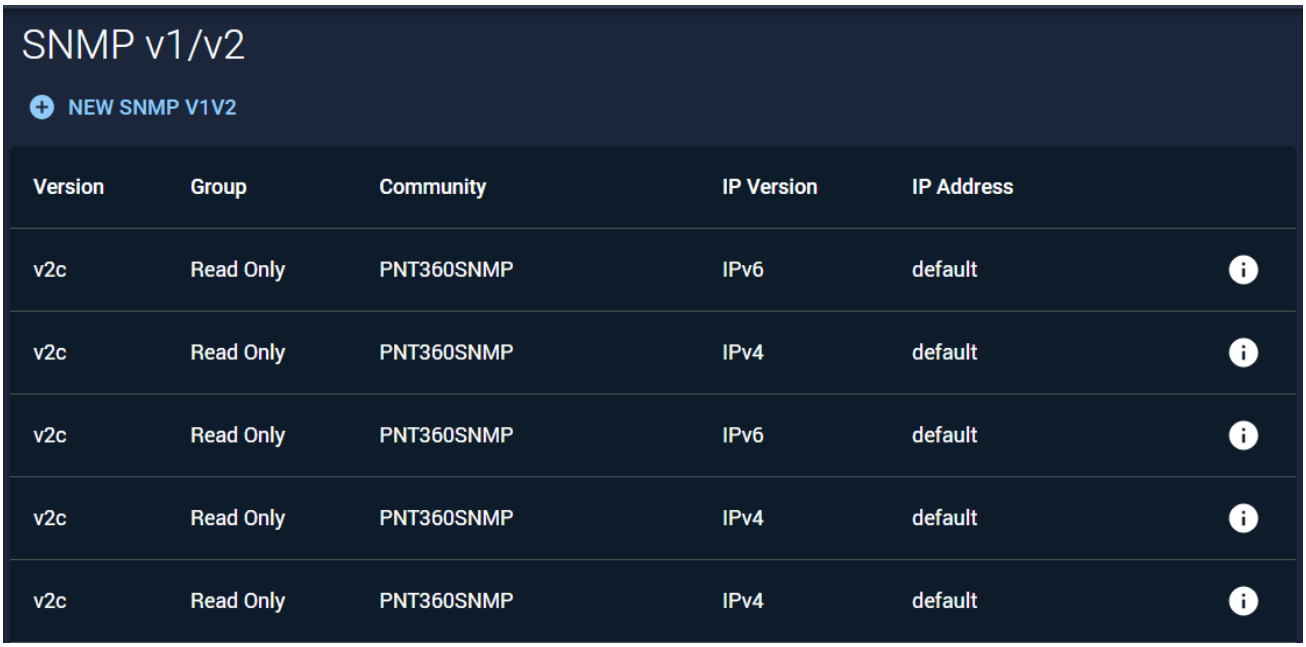


Click yes and the configurations will be restored to defaults.

4.3.6.10. SNMP

Note: This section is currently only applicable to SecureSync devices.

Select the device for which you want to configure SNMP to view, edit and add new SNMP config.



4.3.6.10.1. New SNMP Configuration

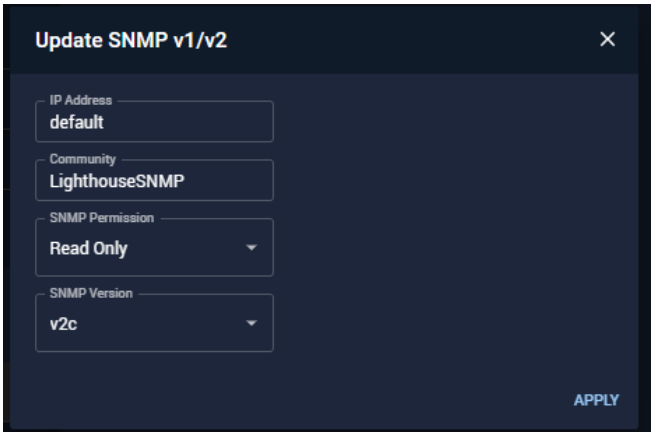
Click the + button to add a new configuration.

Fill out the form and select APPLY. This will add the configuration as well as send the configuration to the device via its REST API.

4.3.6.10.2. Edit SNMP Configuration

Click the edit icon next to the configuration that you would like to modify.

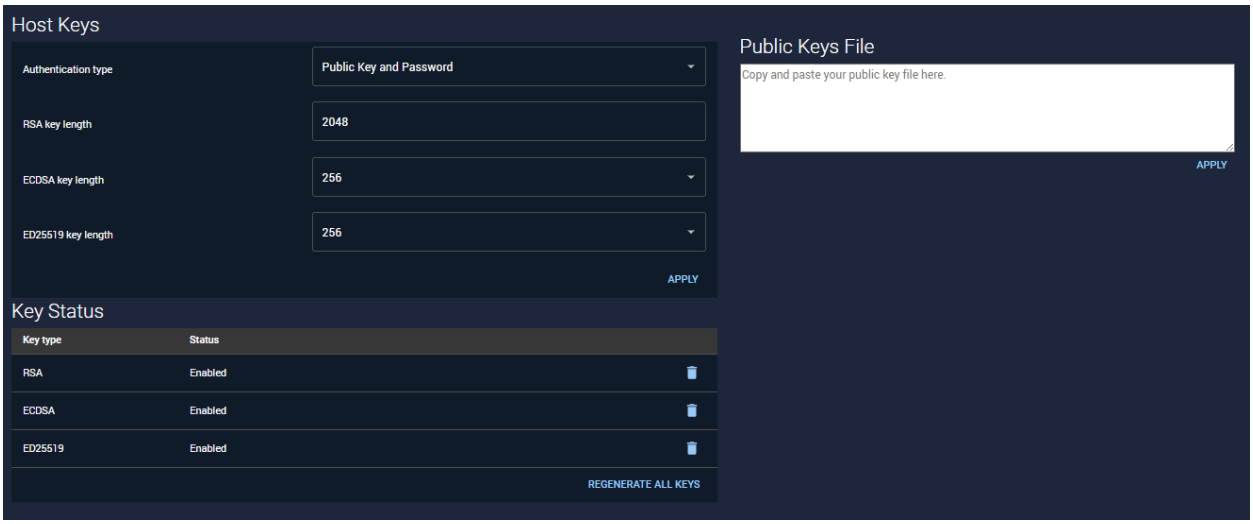
The current settings will be displayed in a modal.



Enter the updated settings and click APPLY. This will update the configuration as well as send the updated configuration to the device via its REST API.

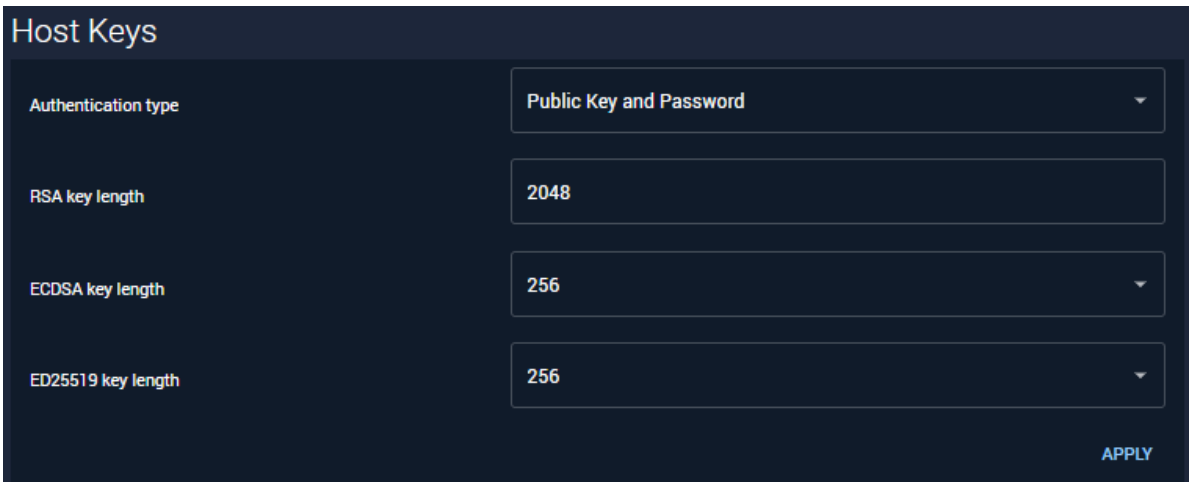
4.3.6.11. SSH

Select the device for which you want to configure SSH



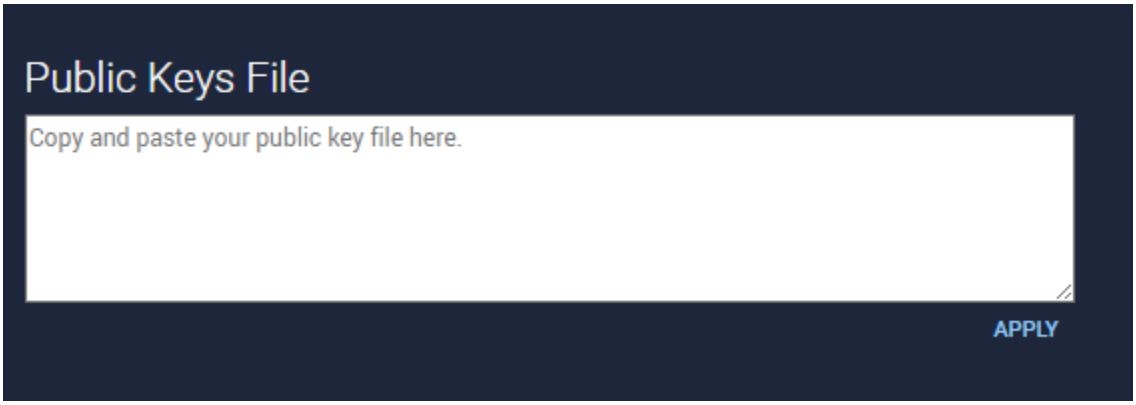
4.3.6.11.1. Configure Host Keys

Fill out the form and click APPLY. This will add the configuration as well as send the configuration to the device via its REST API.

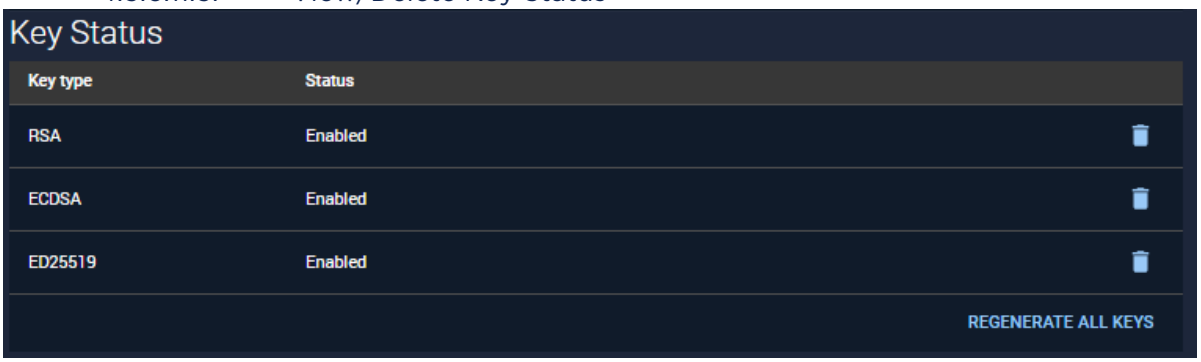


4.3.6.11.2. Configure Public Key

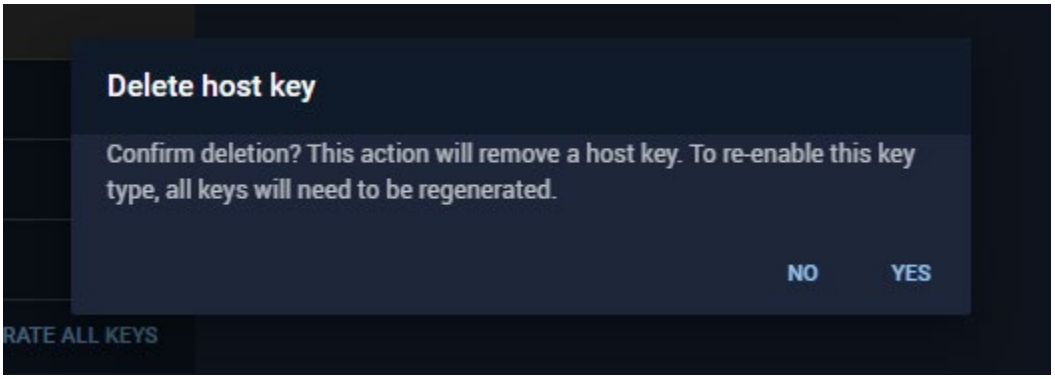
Copy and paste your public key file and click APPLY



4.3.6.11.3. View/Delete Key Status



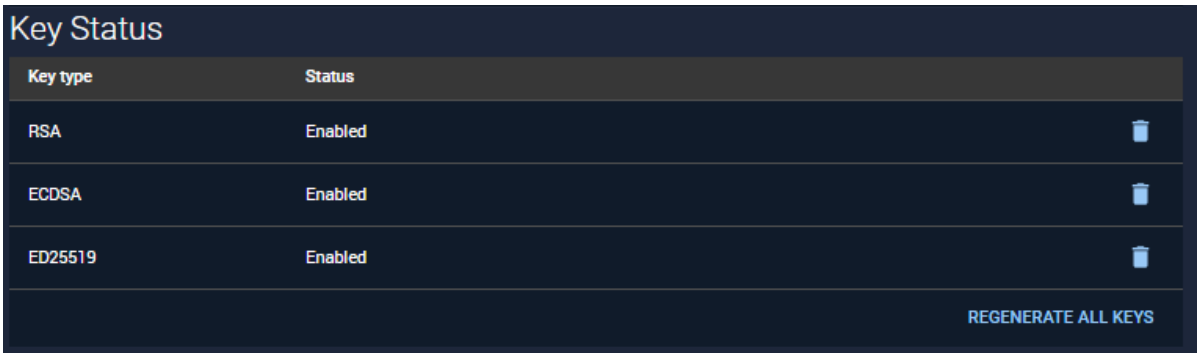
Click the delete icon to delete the Key that you want to delete. A modal will be displayed asking for confirmation that the host key should be deleted.



Click Yes and the host key will be removed from the Key Status list.

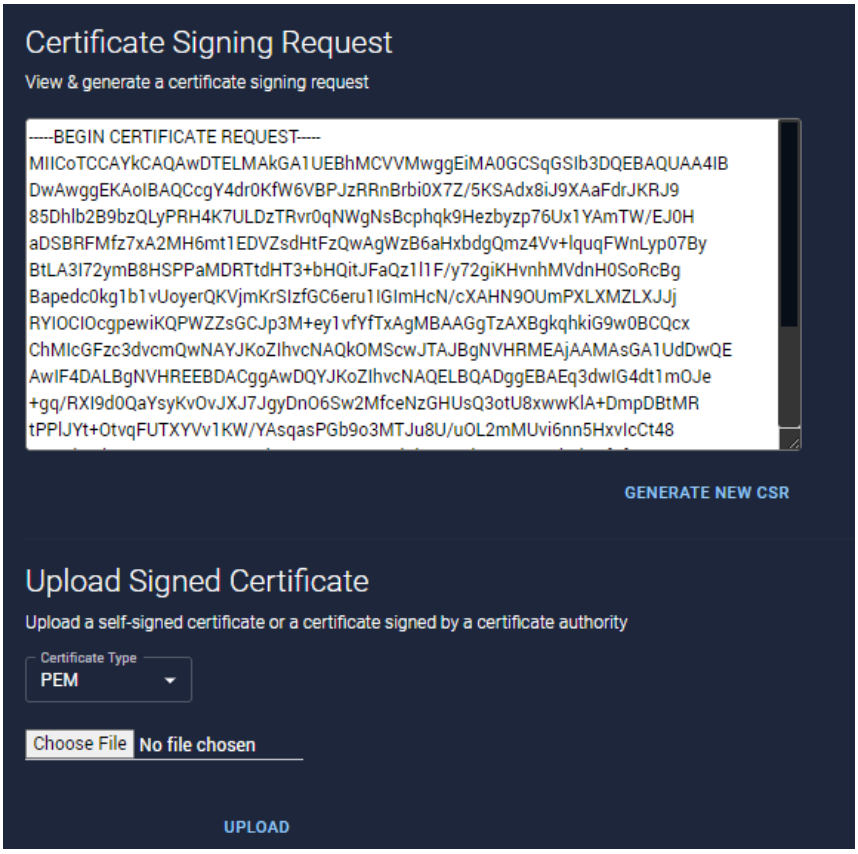
4.3.6.11.1. Regenerate Keys

Click Regenerate All Keys to enable the deleted host keys.



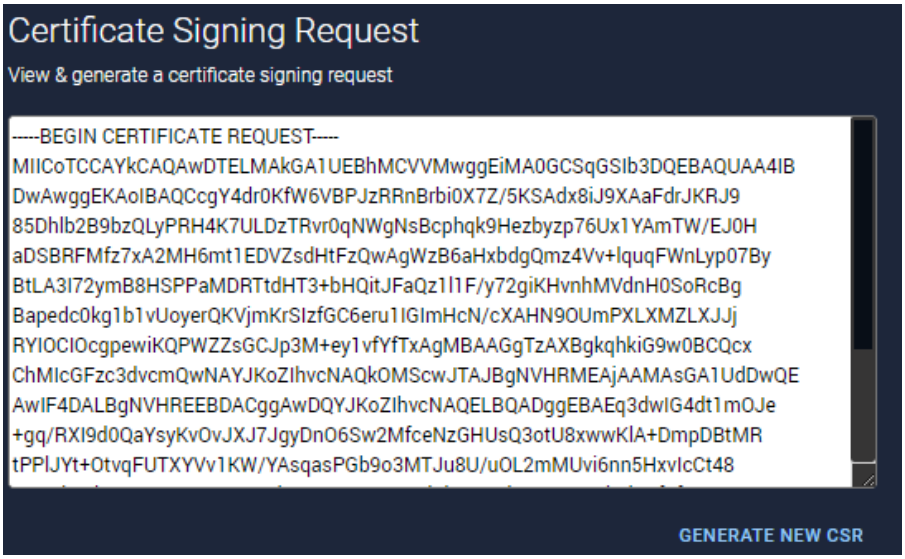
4.3.6.12. HTTPS

Select the device for which you want to configure HTTPS

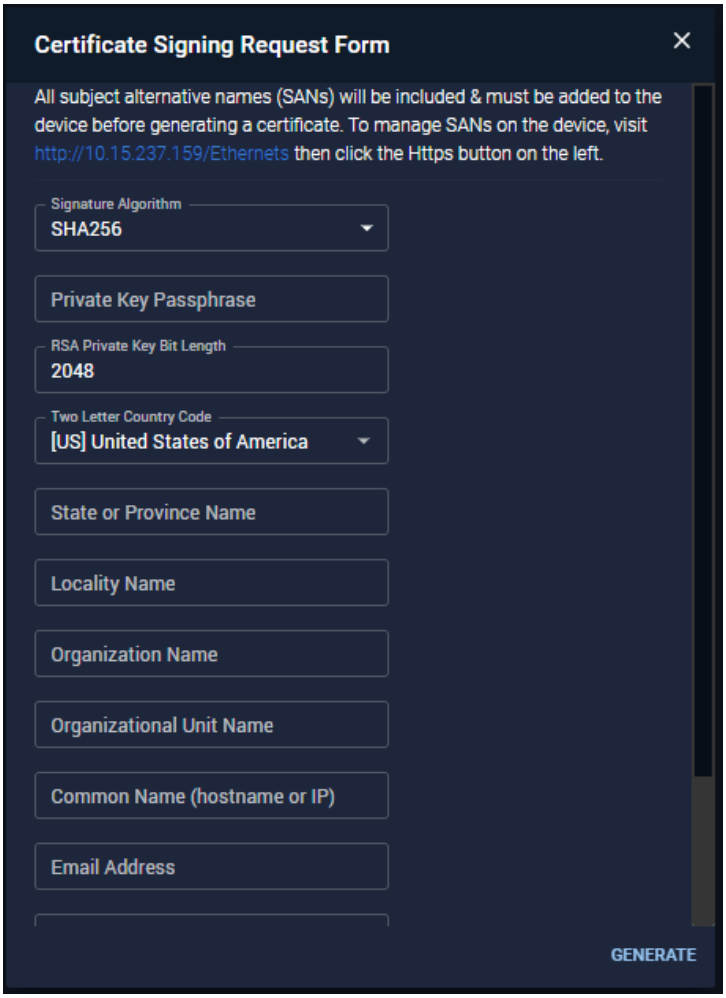


4.3.6.12.1. Generate new CSR

Click on Generate New CSR to generate one.



Fill out the form and click Generate.



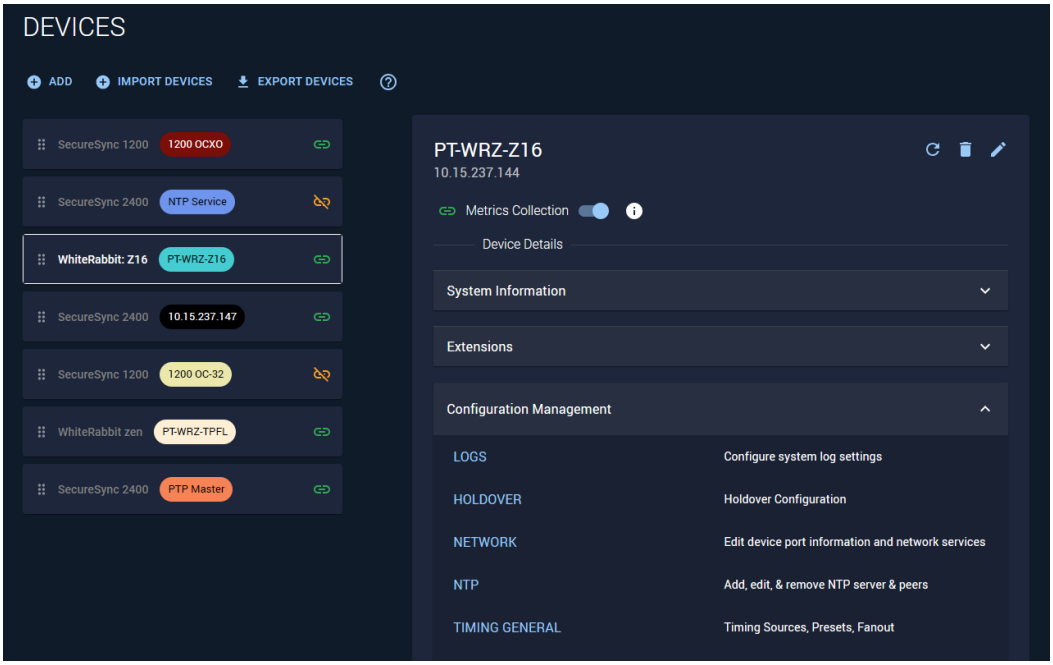
4.3.6.13. Timing General Configuration for White Rabbit Devices

4.3.6.13.1. Overview

The Timing General Configuration section allows users to configure time sources, fanout configurations, and timing presets for White Rabbit devices. This ensures accurate time synchronization across the network.

4.3.6.13.2. Accessing Timing General Configuration

To access Timing General configuration, navigate to the **Devices** tab, select a White Rabbit device and expand the **Configuration Management** dropdown menu. Select **Timing General** to access the available settings.



4.3.6.13.3. Configuring Timing General Settings

4.3.6.13.3.1. Preset Configuration

Select a preset from the dropdown menu (e.g., BC: WR0 | PTP). The selected preset defines default configurations for the device's timing and protocols and interfaces. Select "APPLY" to activate the preset or "SAVE" to store the changes.

4.3.6.13.3.2. Time Sources

Multiple time sources can be configured to provide time data to the device. Each time source is listed (e.g., Time Source #1, Time Source #2). Configure the following fields for each source:

- **Type:** Select the type of time source (e.g., WR for White Rabbit).
- **Interface (Iface):** Specify the interface (e.g., WR0, ETH0) for the selected time source.

Expand additional time sources as needed to configure multiple inputs.

4.3.6.13.3.3. Fanout Configuration

Fanout sources are used to distribute the synchronized time to other devices. Each fanout source is listed (e.g., Fanout Source #WR0, Fanout Source #ETH1). Configure the following fields for each fanout source:

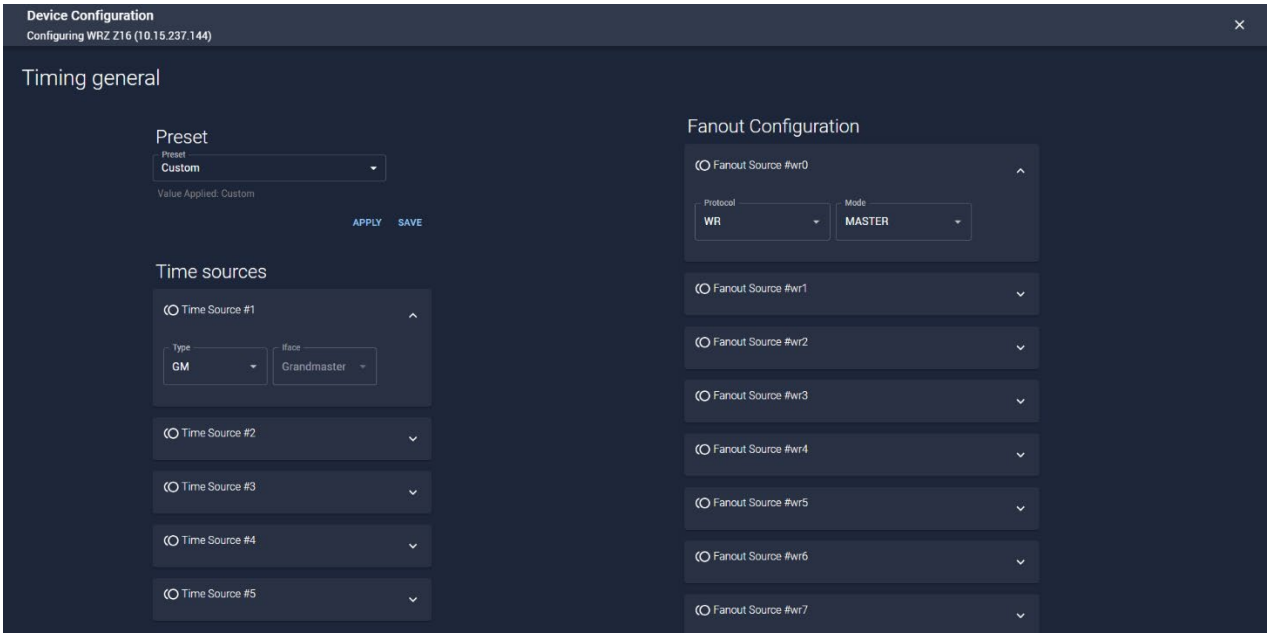
- **Protocol:** Select the protocol used (e.g., WR for White Rabbit, PTP for Precision Time Protocol).
- **Mode:** Set the mode (e.g., Slave, Master).

Select "APPLY" to activate the fanout configuration or "SAVE" to store the settings.

4.3.6.13.4. Saving and Applying Changes

APPLY: Immediately implements the changes on the device.

SAVE: Stores the changes without immediately applying them, allowing further edits as needed.



4.3.6.14. Misc Configuration for White Rabbit Devices

4.3.6.14.1. Overview

The Misc Configuration section provides additional configuration options for managing timezone, PPS (Pulse Per Second) mode, leap second file alerts, and updating leap seconds. These settings enhance the device's regional and synchronization accuracy.

4.3.6.14.2. Timezone Configuration

Allows you to set the device's timezone.

Steps:

- Select the desired timezone from the dropdown menu (e.g., Europe/Madrid).
- Select "APPLY" to implement the changes immediately.
- Alternatively, select "SAVE" to store the changes for later

4.3.6.14.3. PPS Mode Configuration

Configures the Pulse Per Second (PPS) mode.

Options:

- Always ON: PPS is always output even if CRITICAL.
- Only Locked: PPS is only output if the active reference is locked.
- Legacy: PPS follows the same behavior as in the legacy release (wr-zynq-os-v2.x).

Steps:

- Choose the desired PPS mode from the dropdown menu.
- Select "APPLY" to activate the mode immediately or "SAVE" to save the configuration.

4.3.6.14.4. Ignore Leap Seconds File Alerts

Enables or disables alerts related to issues with the leap seconds file.

Options:

- Yes: Disables alerts.
- No: Keeps alerts enabled.

Steps:

- Select your preference from the dropdown menu.

- Select “SAVE” to confirm the change.

4.3.6.14.5. Updating Leap Seconds

Ensures timekeeping accuracy by updating the leap seconds file.

Steps:

- Download the latest leap second file from https://hpiers.obspm.fr/iers/bul/bulc/ntp/leap-seconds.list.
- Upload the file using the **Update Leap Seconds** section.
- Verify the upload to ensure the changes are applied.

4.3.6.15. Holdover Configuration (White Rabbit Devices)

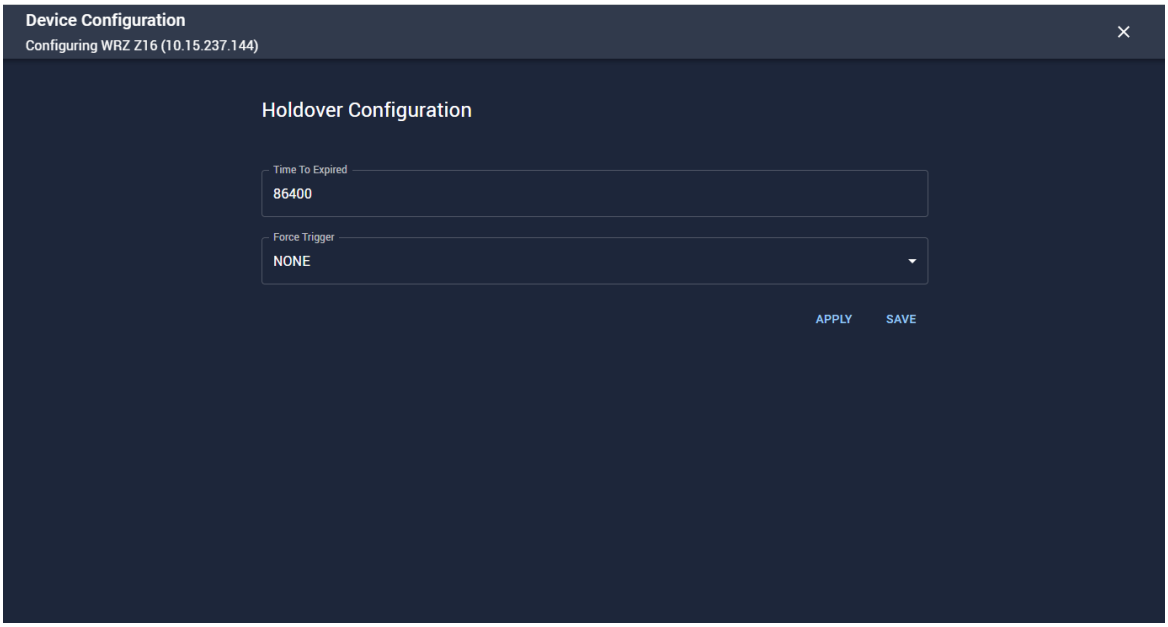
4.3.6.15.1. Overview

The Holdover Configuration feature allows users to set the parameters for how long the device can maintain timing accuracy in the absence of an external time reference. This ensures that the system continues to operate within acceptable accuracy limits during interruptions.

4.3.6.15.2. Configurable Options

1. **Time to Expire:**
    a. Time until the holdover is considered out of specification and expired (default ~24h).
    b. **Steps:**
        i. Enter the desired duration in seconds in the input field.
        ii. Select “APPLY” to implement the change immediately or “SAVE” to store the setting for future application.
2. **Force Trigger:**
    a. The Force Trigger can manually trigger the holdover (START) or expire it (STOP) without waiting for the expiration timer. NONE does nothing.
    b. **Options:**
        i. NONE
        ii. START
        iii. STOP
    c. **Steps:**
        i. Select the desired trigger option from the dropdown menu.

ii. Select “APPLY” to activate the selection immediately or “SAVE” to store the setting.



4.3.7. Reordering Devices

4.3.7.1. Overview

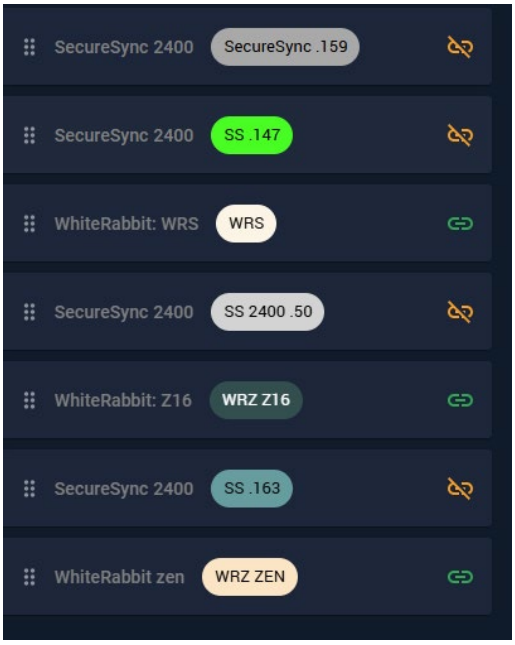
The Reordering Devices feature allows users to organize their device list manually by dragging and dropping devices into the desired order. This ensures a more intuitive and user-friendly experience when managing multiple devices.

4.3.7.2. Drag-and-Drop Reordering

Reorder devices in the list of devices by dragging and dropping them into the preferred sequence.

Steps:

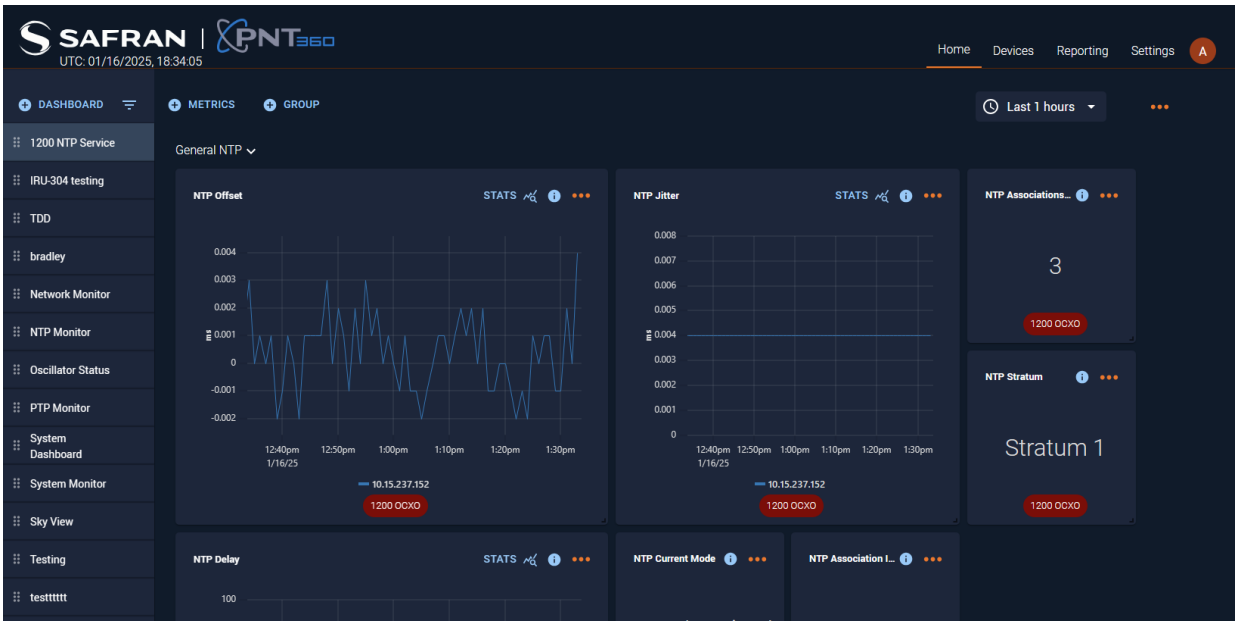
- Locate the **drag handle** (represented by the dotted grid icon) next to each device name.
- Click and hold the drag handle of the device you want to move.
- Drag the device to the desired position in the list.
- Release the mouse button to finalize the new order.



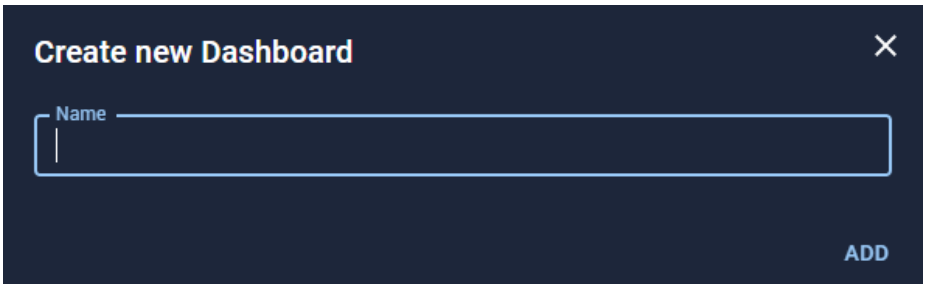
4.4. Dashboard Management

4.4.1. Add New Dashboard

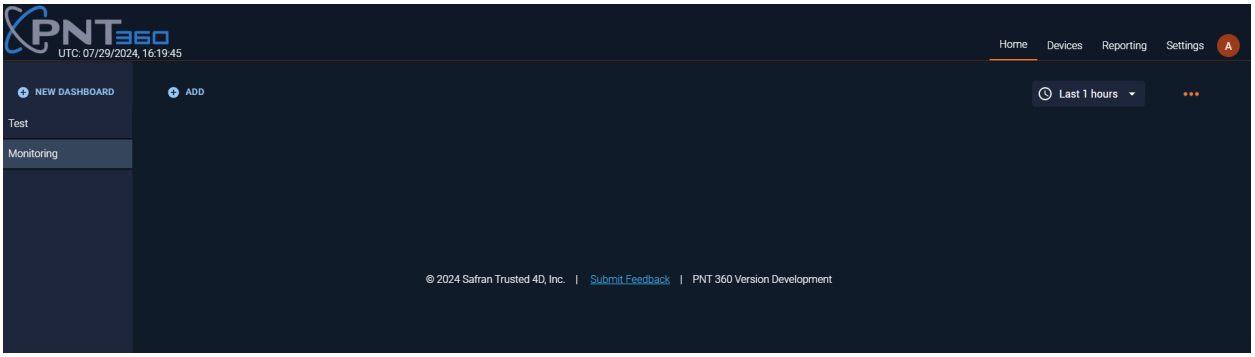
Login to the application and click “+ DASHBOARD.”



A modal will be displayed and ask for the dashboard name. Enter a name and click ADD.

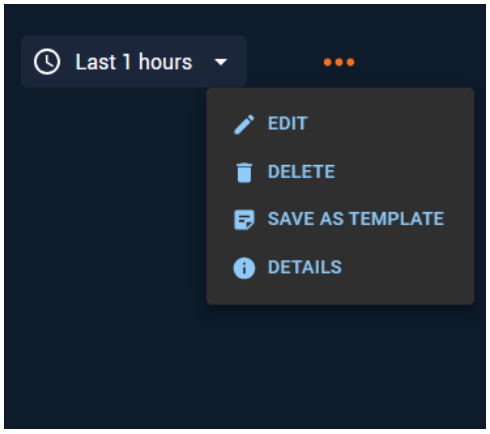


An empty dashboard will be created with no visible charts.

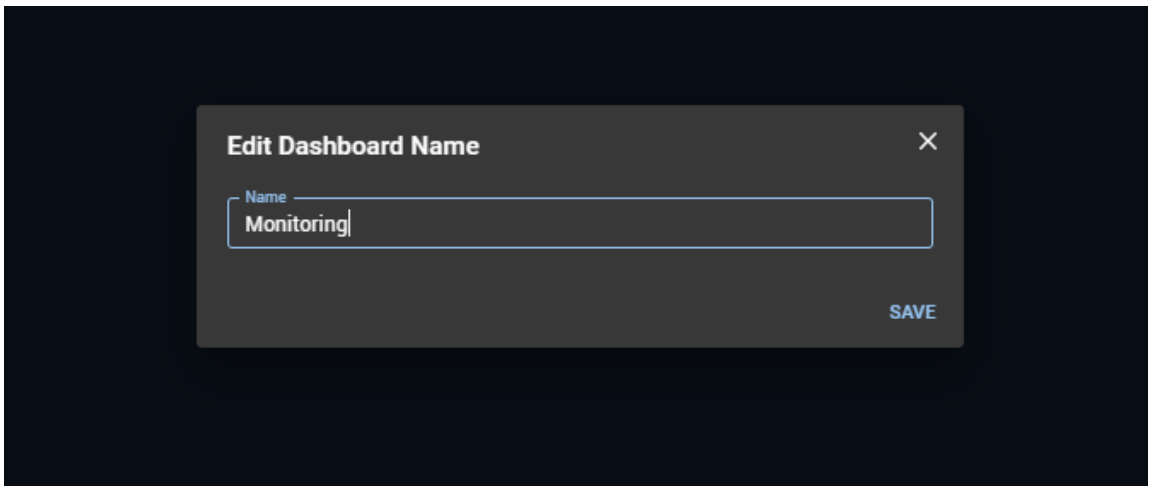


4.4.2. Edit Dashboard Name

- Select the “more” ellipses and click Edit

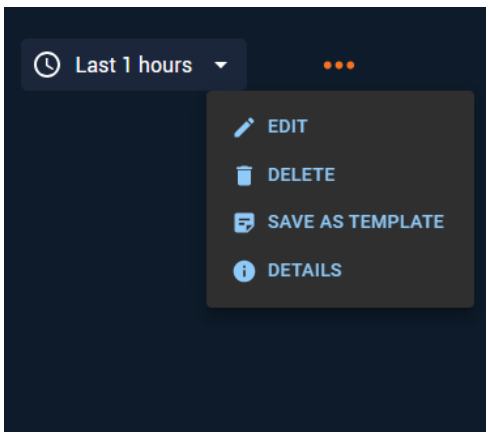


- Enter a new dashboard name and click SAVE.

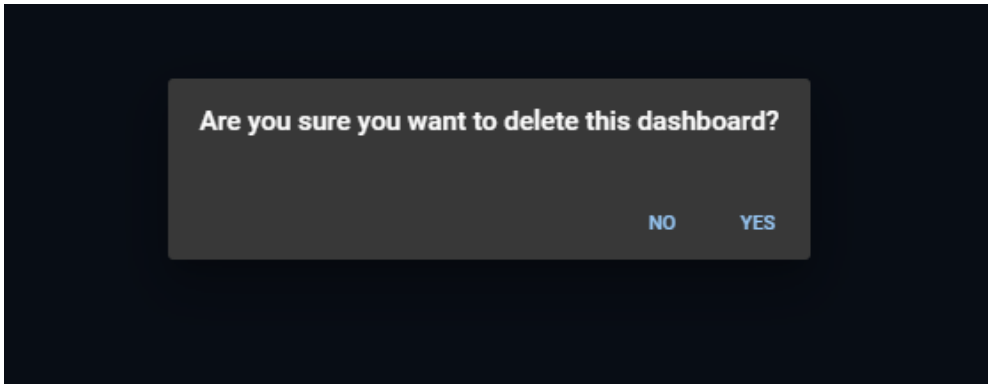


4.4.3. Delete Dashboard

- Select the “more” ellipses and select Delete.



- A modal will be displayed asking for confirmation.

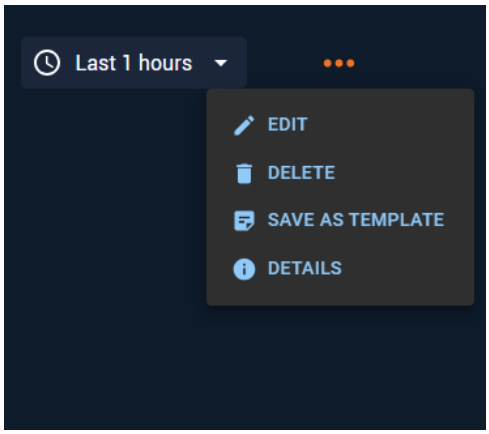


- Select Yes to delete.
- The dashboard and all of its components are deleted and you will be moved to the next available dashboard.

4.4.4. Creating Templates

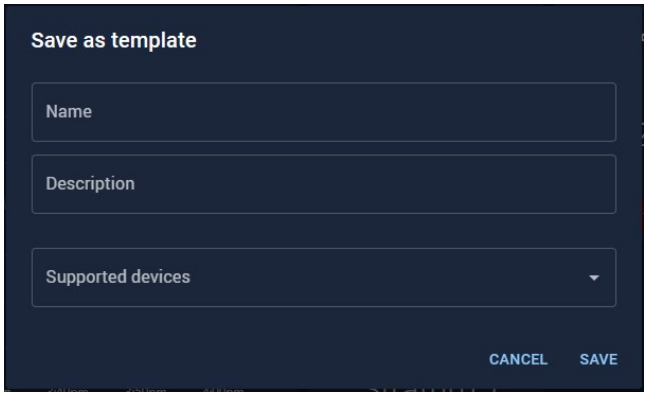
You can create templates of dashboard configurations to save and add pre-configured charts to any dashboard.

- Navigate to the dashboard you would like to create a template of.
- Select the “more” ellipses and select “SAVE AS TEMPLATE.”



- A modal will be displayed with the following template settings.
  - Name (Required)
  - Description
  - Supported Devices (Required)

Note: You may select more than one supported device.

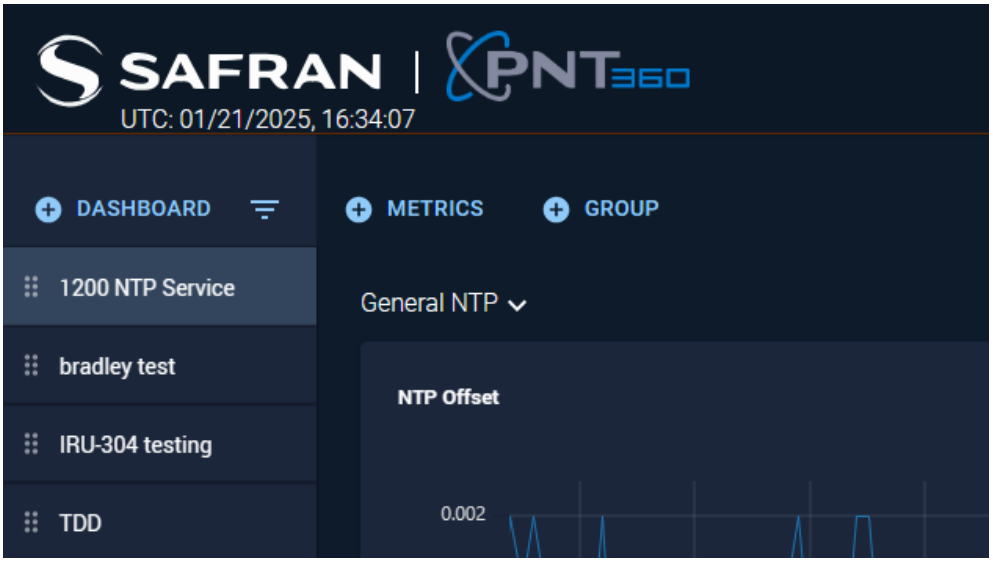


- Select “SAVE” to save the template.

4.4.5. Add Components to Dashboard

You can choose which components you want to visualize on your dashboard easily.

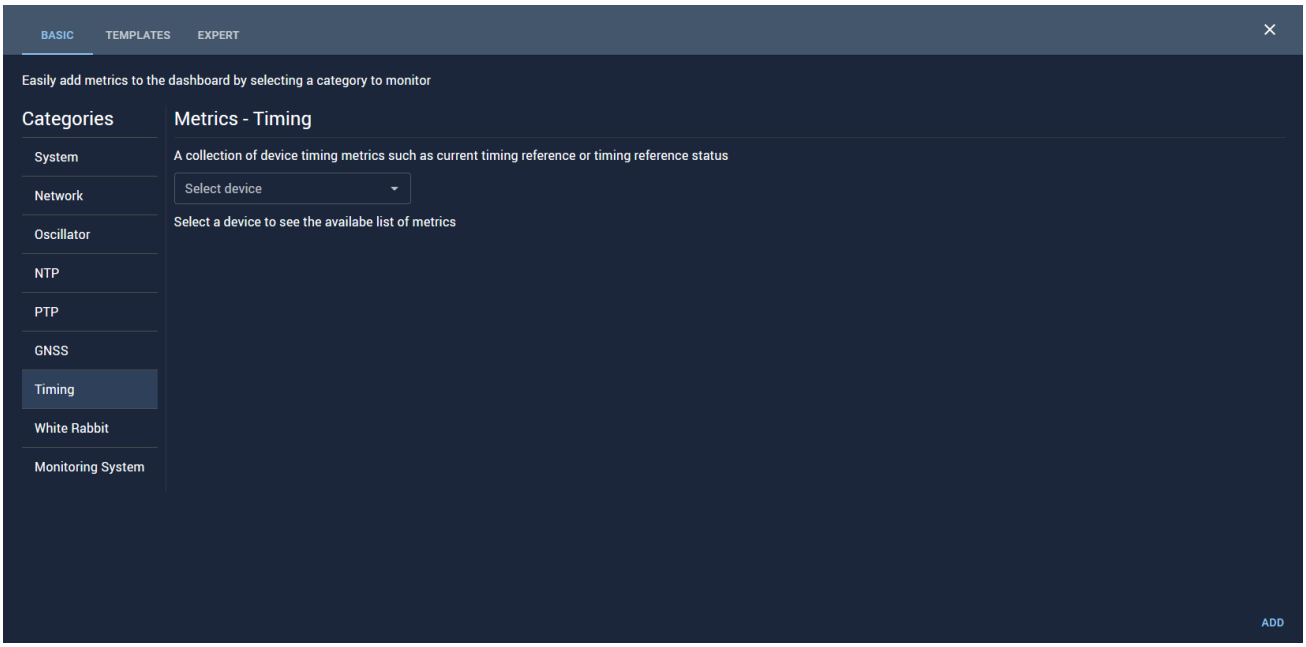
- Navigate to the dashboard you want to modify.
- Selecting the + METRICS button will allow you to add a collection of general metrics for a device.
- Selecting the + GROUP button will allow you to create a group to sort and organize metrics in the selected dashboard.



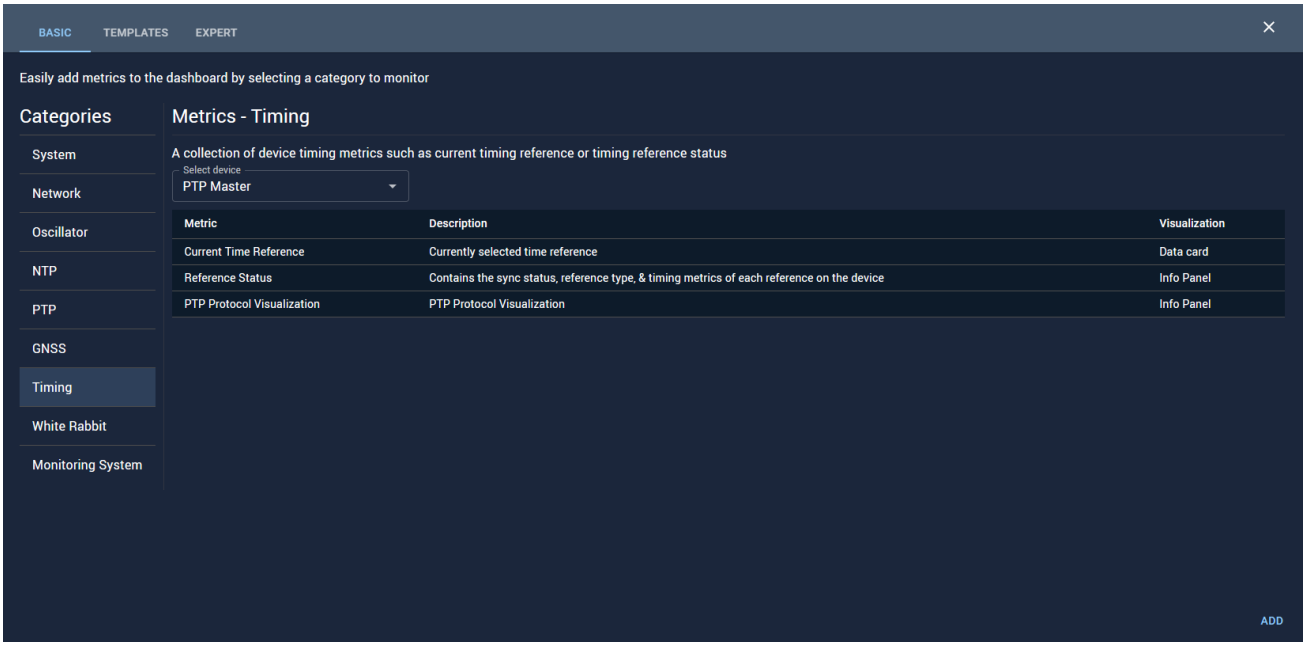
4.4.5.1. Metrics

4.4.5.1.1. Basic Mode

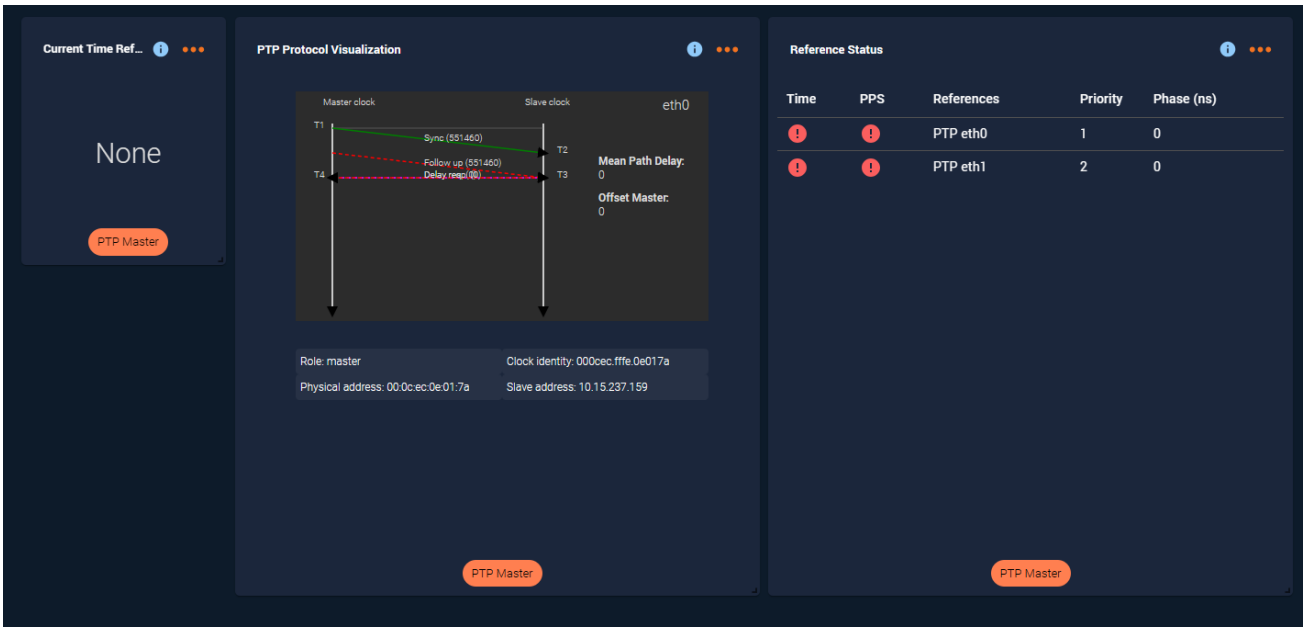
To create a basic mode metrics display, select the + METRICS button and navigate to the BASIC tab. Select a Category to easily add a collection of general metrics for a device.



Select the device to see the list of metrics available for the selected category.

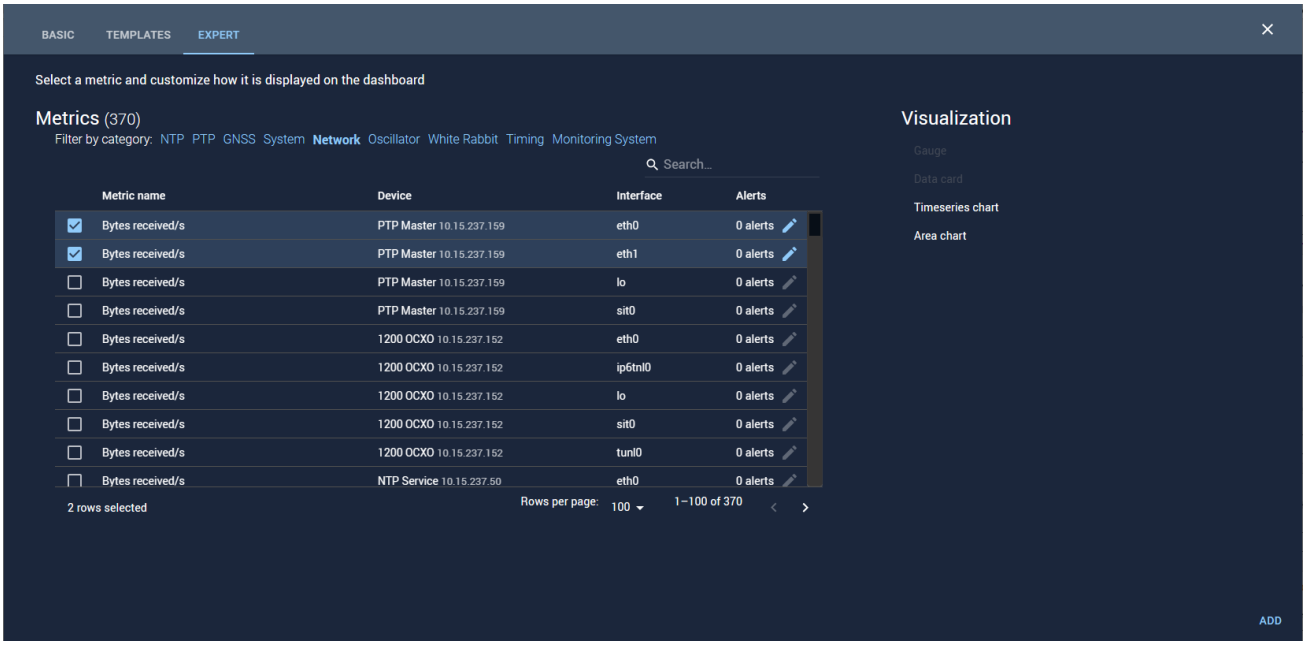


Select ADD to add the selected collection of metrics for the selected device to the dashboard.

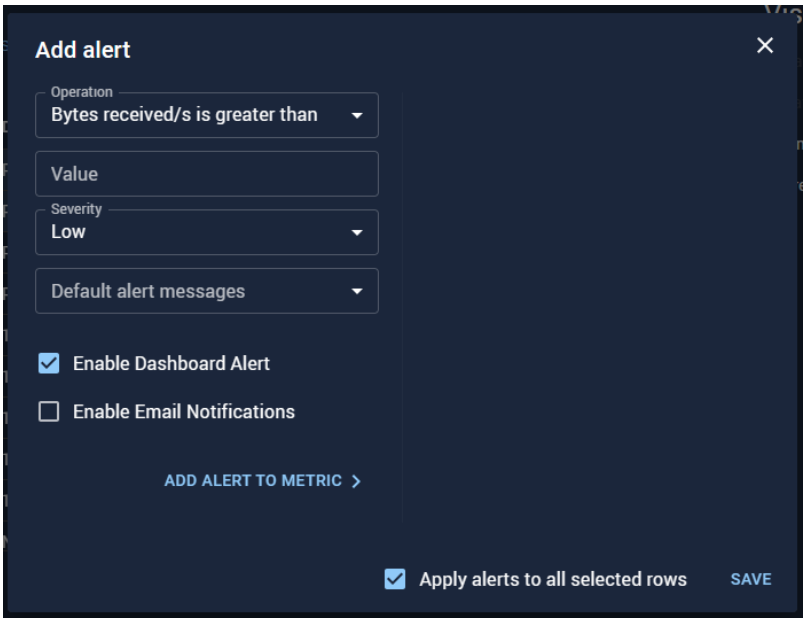


4.4.5.1.2. Expert Mode

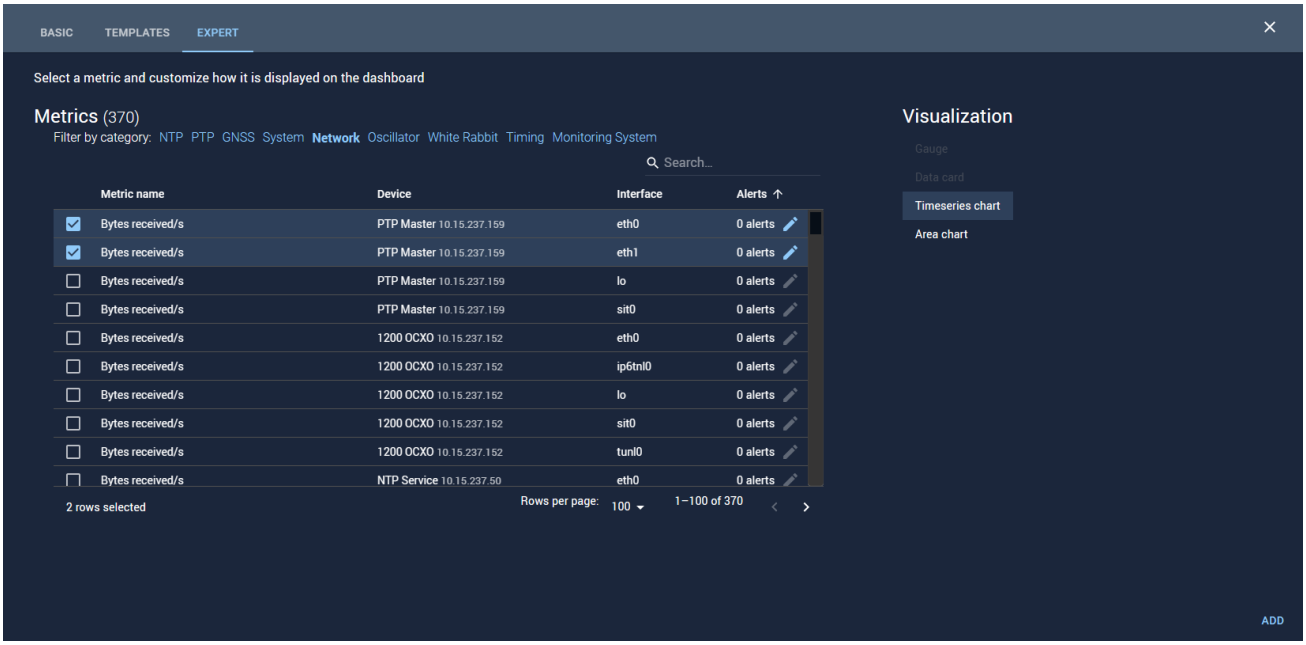
To create an expert mode metrics display, select the + METRICS button and navigate to the EXPERT tab. Filter the metrics by category and select a metric by customizing how it is displayed.



Select the edit icon to add alerts to the selected metric. A form will be displayed in which you can add the alerts and apply the alerts to all selected rows. Select SAVE to apply the alerts to the dashboard.



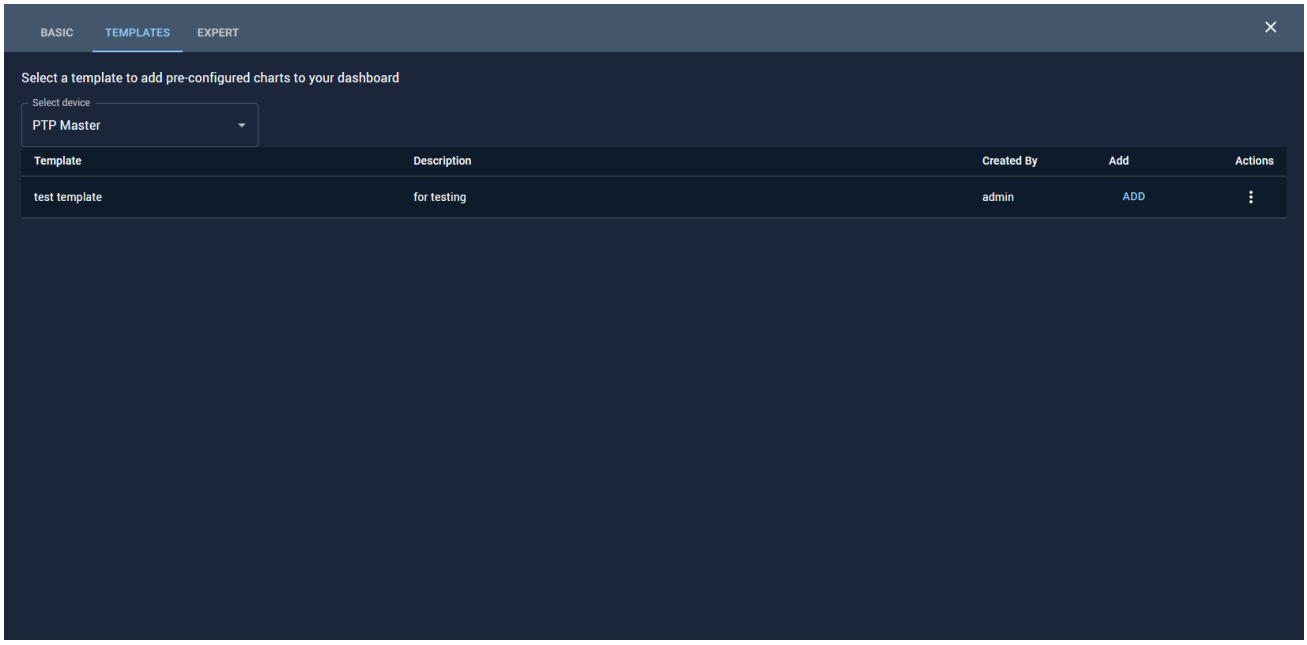
Select the visualization and select ADD.



4.4.5.1.3. Using Templates

Templates can be used to add saved, pre-configured charts to your dashboard.

- To use a template, select the + METRICS button and navigate to the TEMPLATES tab.

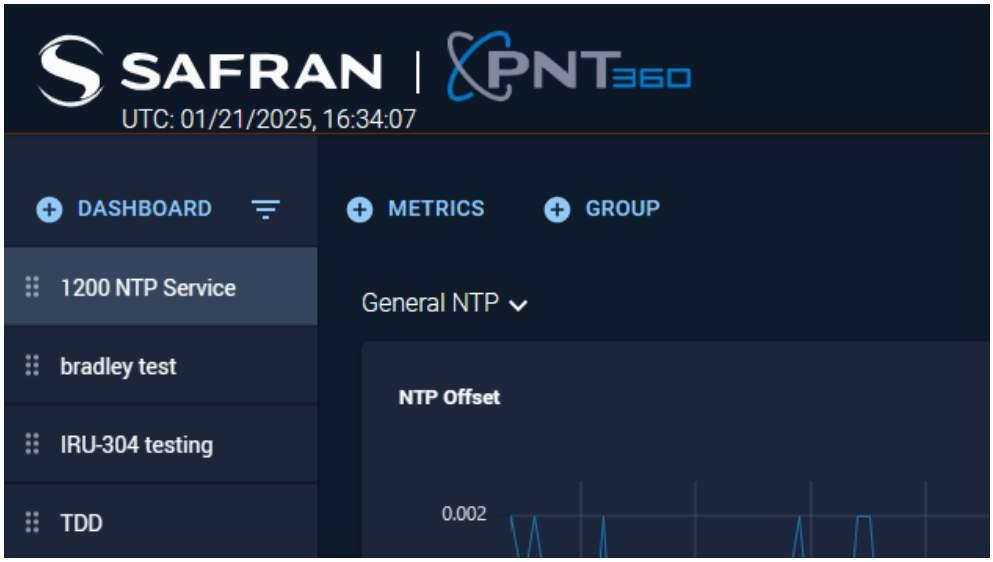


- Select a device from the dropdown menu and a list of available templates for the selected device will display.
- Select the ADD button to add the template to your dashboard.

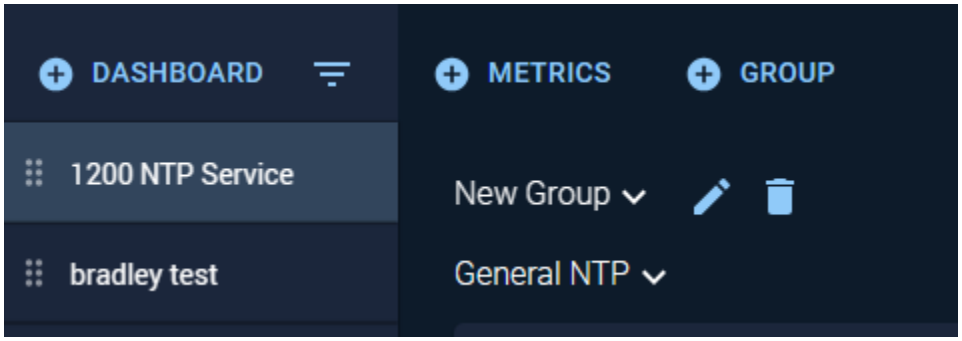
4.4.5.2. Groups

Groups can be used to sort and organize metrics panels in your dashboard.

- With the desired dashboard selected, select the + GROUP button.



- A new group will be created, hovering over the group name will display the “edit” and “delete” icons.

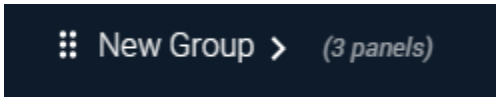


- Selecting the “edit” icon will display a modal that allows you to rename the selected group.
- Selecting the “delete” icon will display a modal confirming if you would like to delete the selected group.

Note: Deleting a group will not delete the panels residing within that group.

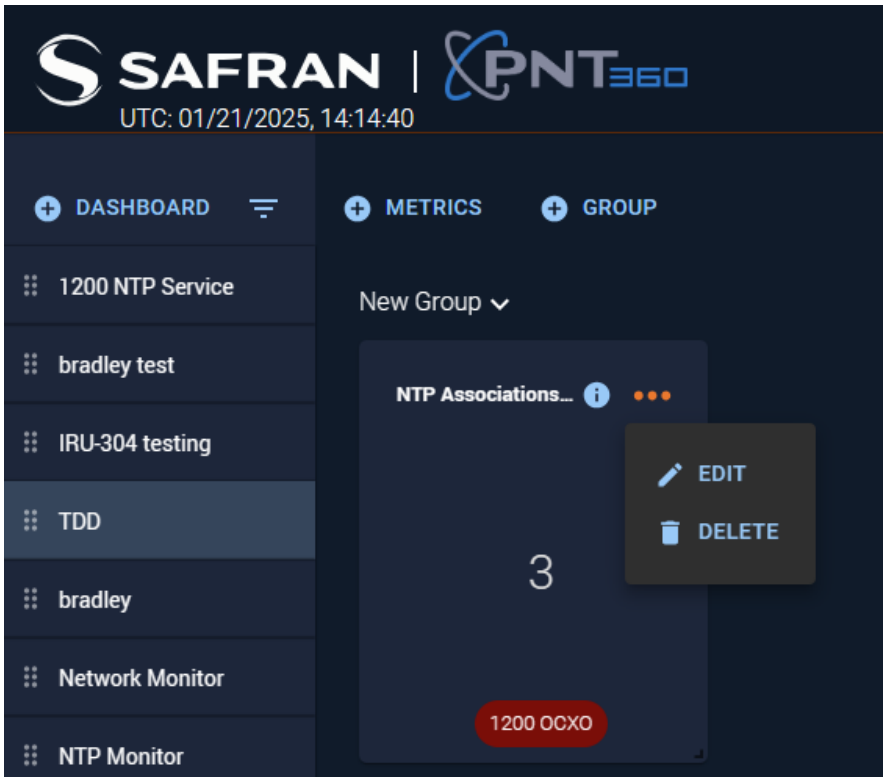
- You may drag and drop a metrics panel into a group by dropping the panel below the group name.

- Selecting the group will collapse the group, displaying a **drag handle** (represented by the dotted grid icon) that will allow you to drag and drop the group within the dashboard.

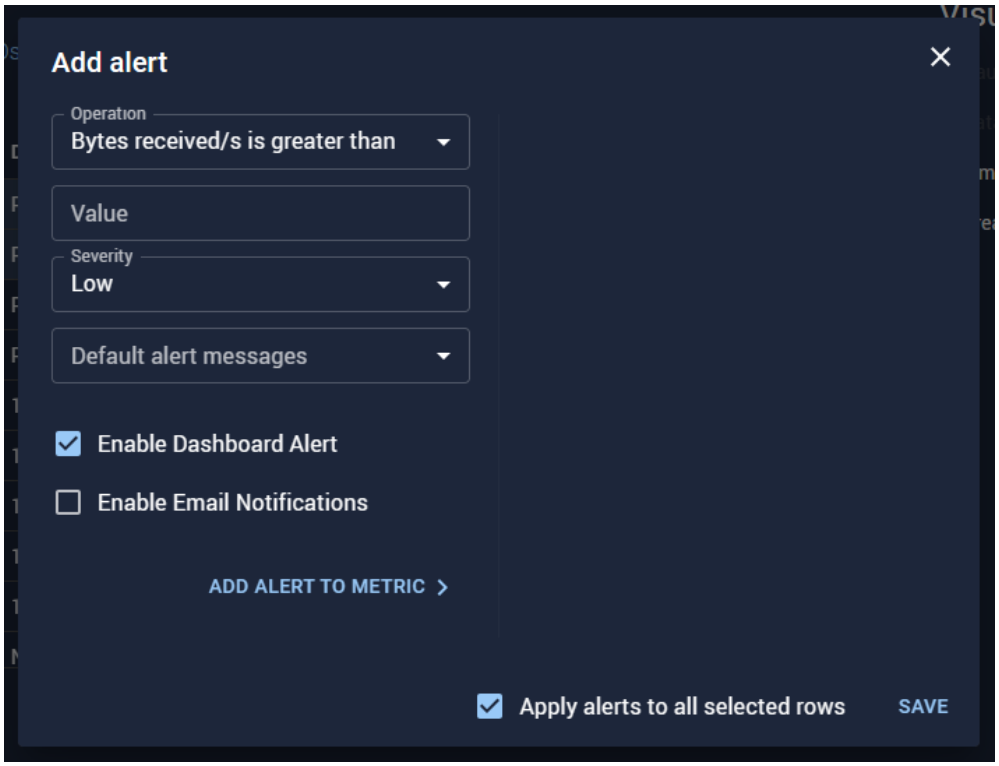


4.4.6. Edit Dashboard Component

- In dashboard view, select the ellipses menu on the component you wish to edit.



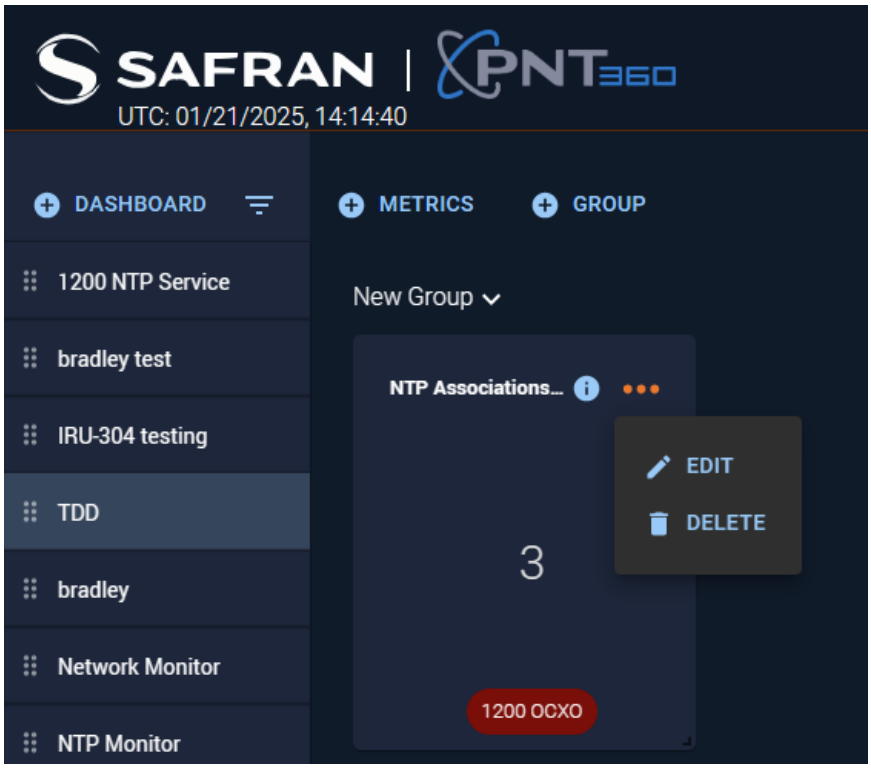
- Select Edit.
- A form will be displayed in which you can edit the details.



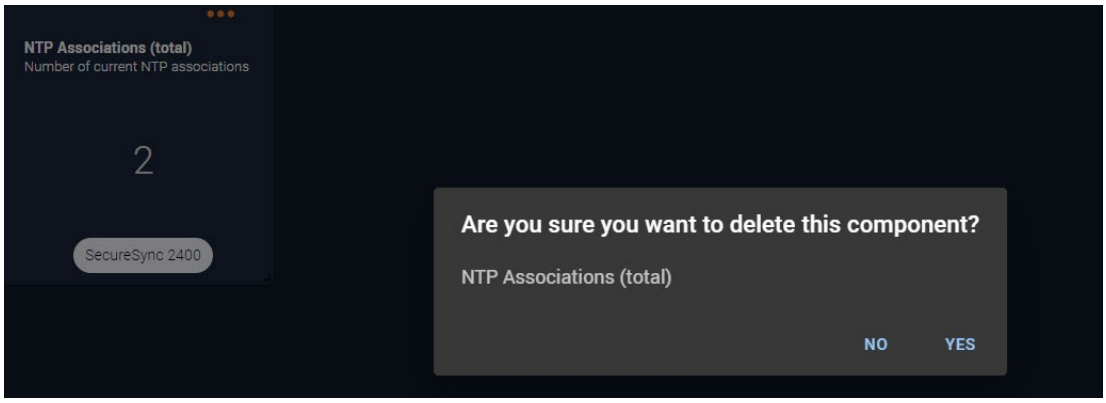
- Click SAVE when finished with changes.

4.4.7. Delete Dashboard Component

- In dashboard view, select the ellipses menu on the component you wish to Delete.



- Click Delete.
- A modal will be displayed asking for verification of the delete action.



- Click yes if you are sure you wish to delete this component.

4.4.8. Dashboard Visualizations

4.4.8.1. Data Card

The data card is available to display singular values that are either the most recent current value or a static value that does not change.

4.4.8.2. Gauge

The gauge is available to display singular current values of data that you wish to view within a standard range such as a temperature or a percentage value. Useful for quick assessments of whether a value is within a safe, expected, or critical range.

4.4.8.3. Timeseries

The timeseries chart is available to display data over a range of time with an x and y axis. This timeseries chart has a zoom function, as well as a pause and filter function.

4.4.8.4. Area Chart

The area chart is available and works like the timeseries chart. The area chart fills specific areas under the plotted lines, which provides a visual representation of volume or magnitude.

4.4.8.5. Sky View Visualization

The sky view visualization provides a graphical representation of the elevation and azimuth of in-view satellites. It displays the position and movement of satellites in real-time, help users monitor their visibility and trajectory relative to the device's location.

4.4.8.6. Info Icons in Visualizations

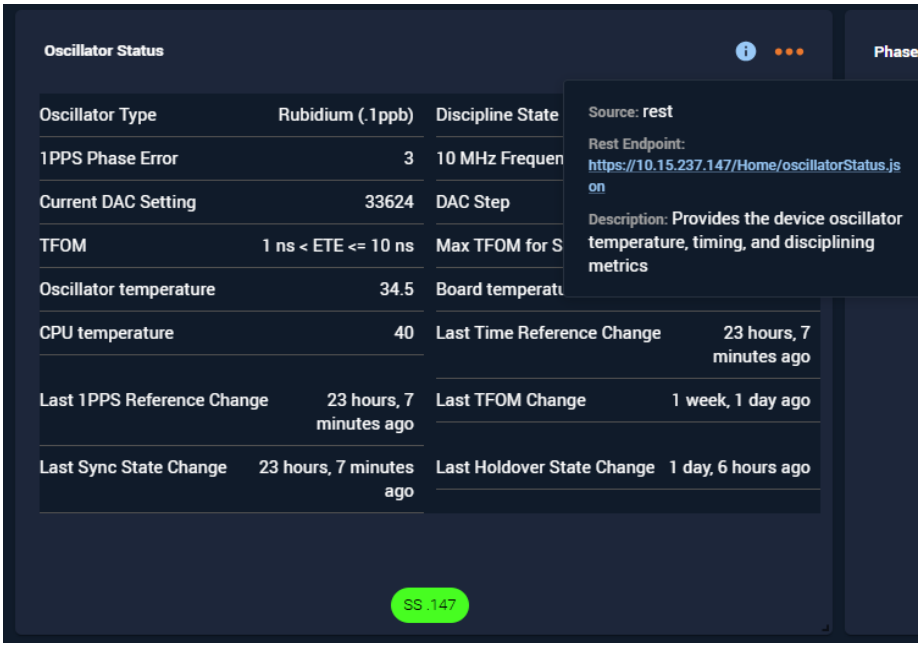
4.4.8.6.1. Info Tooltip

Provides detailed information about the data source, collection method, and additional context for the visualization. To access, hover over the info icon (i) in any visualization chart to see details.

Endpoint or OID

- For REST: Displays the API endpoint used for data collection.
- For SNMP: Displays the SNMP Object Identifier (OID).

The **Description** explain purpose or relevance of the data.



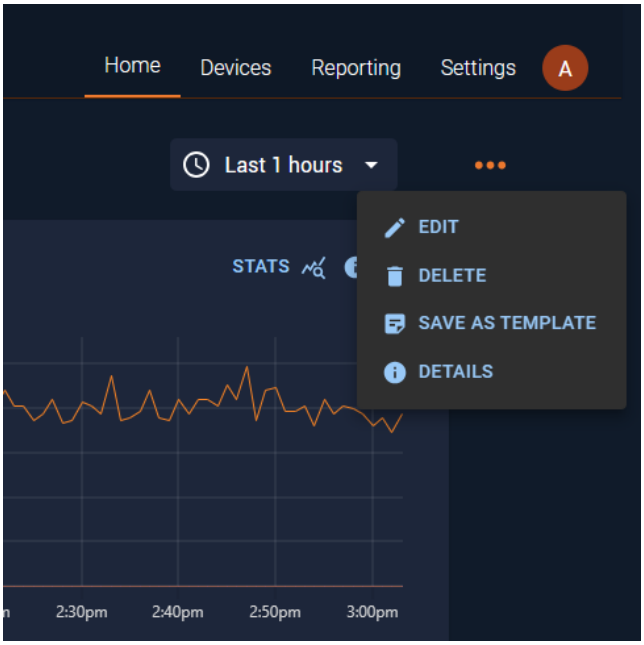
4.4.8.7. Dashboard Details

4.4.8.7.1. Overview

The Dashboard Details feature provides metadata about a dashboard, including its creation and modification history. This is particularly useful for tracking ownership, changes, and versioning in collaborative environment.

4.4.8.7.2. Accessing Dashboard Details

Navigate to the dashboard of interest, select the three-dot menu (ellipsis) in the top-right corner of the dashboard widget, and select **DETAILS** from the dropdown menu.



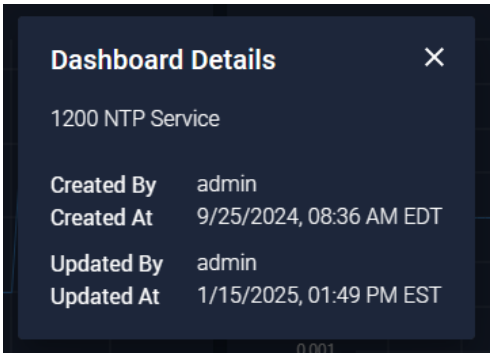
4.4.8.7.3. Metadata Displayed

Created By: Displays the username of the user who created the dashboard.

Created At: Indicates the date and time when the dashboard was initially created.

Updated By: Displays the username of the user who last updated the dashboard (if available).

Updated At: Displays the date and time of the last modification of the dashboard (if available).



4.4.9. Sorting Dashboards

4.4.9.1. Overview

The **Sorting Dashboards** feature allows users to organize their dashboards either manually using drag-and-drop or automatically by sorting them alphabetically. This provides an efficient way to keep the dashboard list tidy and accessible

4.4.9.2. Drag-and-Drop Sorting

Enables users to reorder dashboards manually by dragging and dropping them into the desired position in the list. This is useful for prioritizing dashboards based on importance or frequency of use.

Steps:

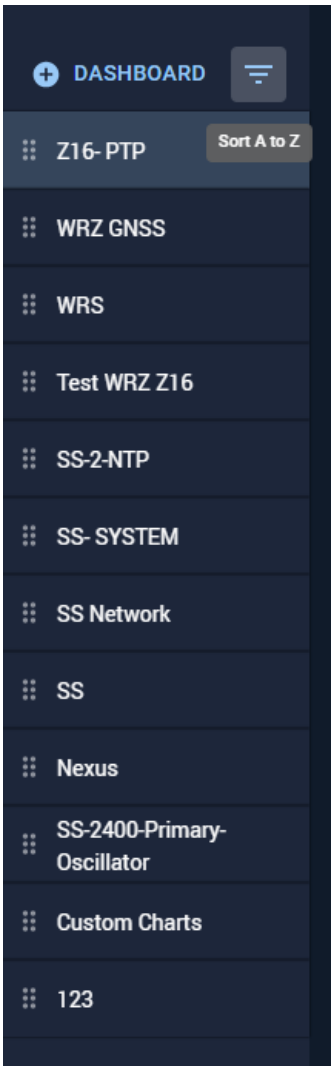
- Locate the **drag handle** (represented by the dotted grid icon) next to each dashboard name.
- Click and hold the drag handle.
- Drag the dashboard to the preferred position in the list.
- Release the mouse button to drop it into place.

4.4.9.3. Alphabetical Sorting

Automatically sorts all dashboards in alphabetical order (A to Z). This is ideal for quickly organizing dashboards in a consistent manner, especially in collaborative environments.

Steps:

- Select the **Sort A to Z** button located at the top of the dashboard list.
- The system will rearrange the dashboards in alphabetical order.



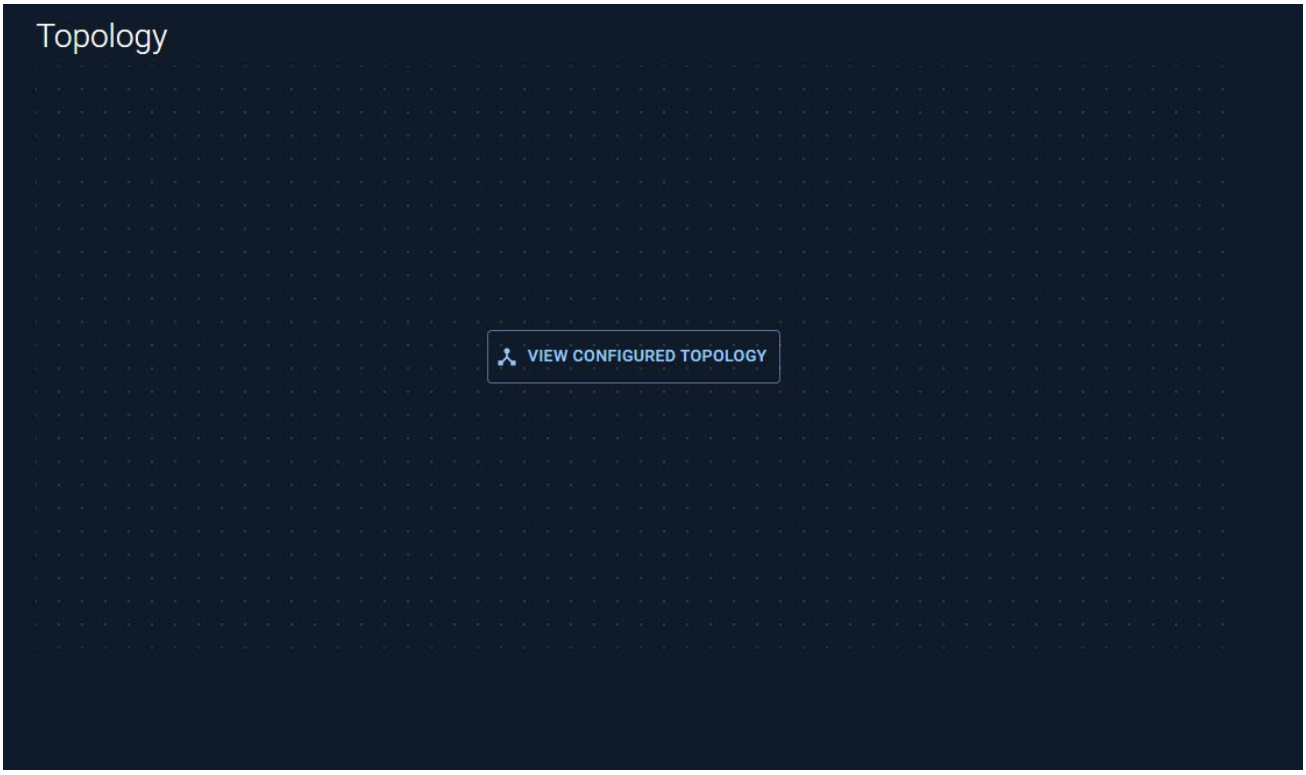
4.5. System Topology Visualization

4.5.1. Overview

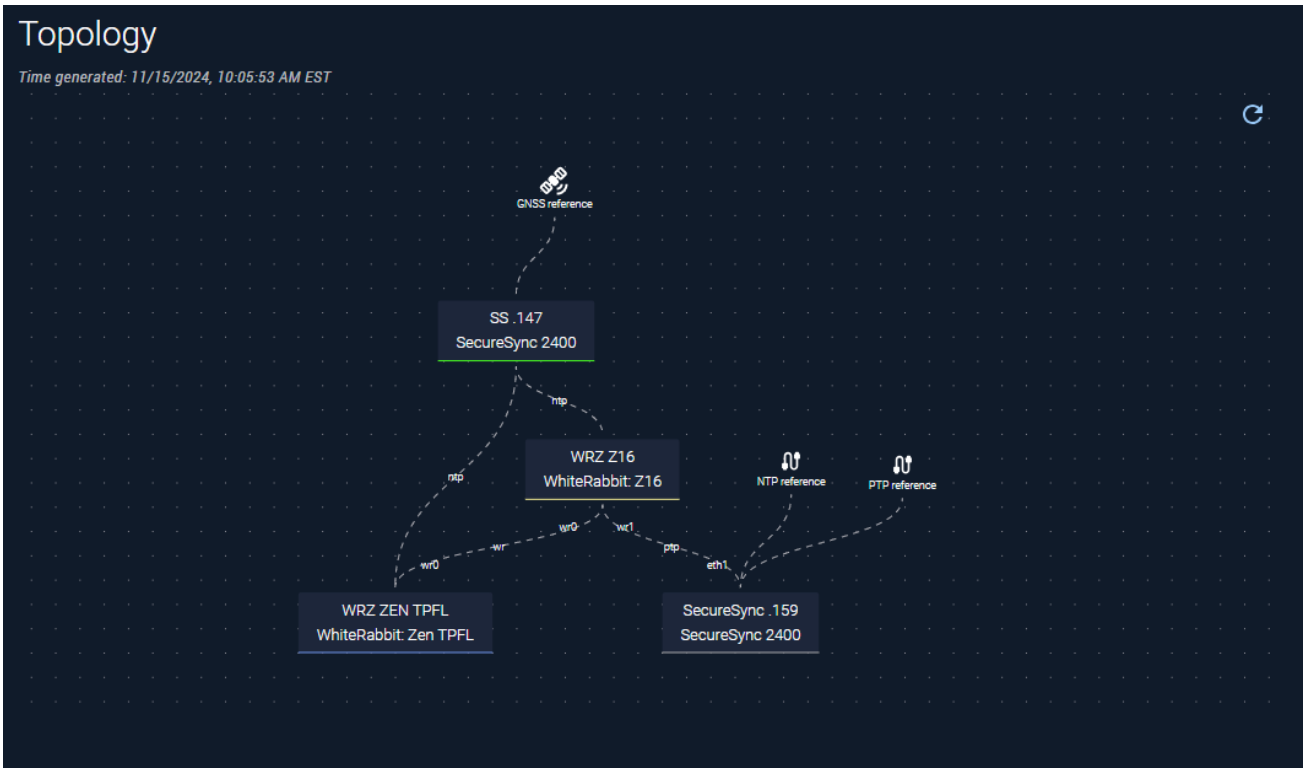
The **System Topology Visualization** feature allows users to view a graphical representation of their system's topology. This visualization is generated by retrieving the configuration of each connected device and mapping their roles based on a normalized configuration.

4.5.2. Accessing the Topology View

1. Navigate to the **Devices** tab in the main navigation menu.
2. Select the **View Configured Topology** option.



3. The topology will display an interactive diagram of the system, similar to the example below:



4.5.3. Key Features

Device Mapping: Displays the connected devices along with their references.

Visual Connections: Shows the relationships between devices with labeled connections like NTP, PTP, and WR. Shows the time when the topology is generated.

Interactive Features:

- **Click for Details:** Click on the device node to go to the **Device** detail page.

- **Refresh Button:** Click the refresh icon in the top-right corner to update the topology.

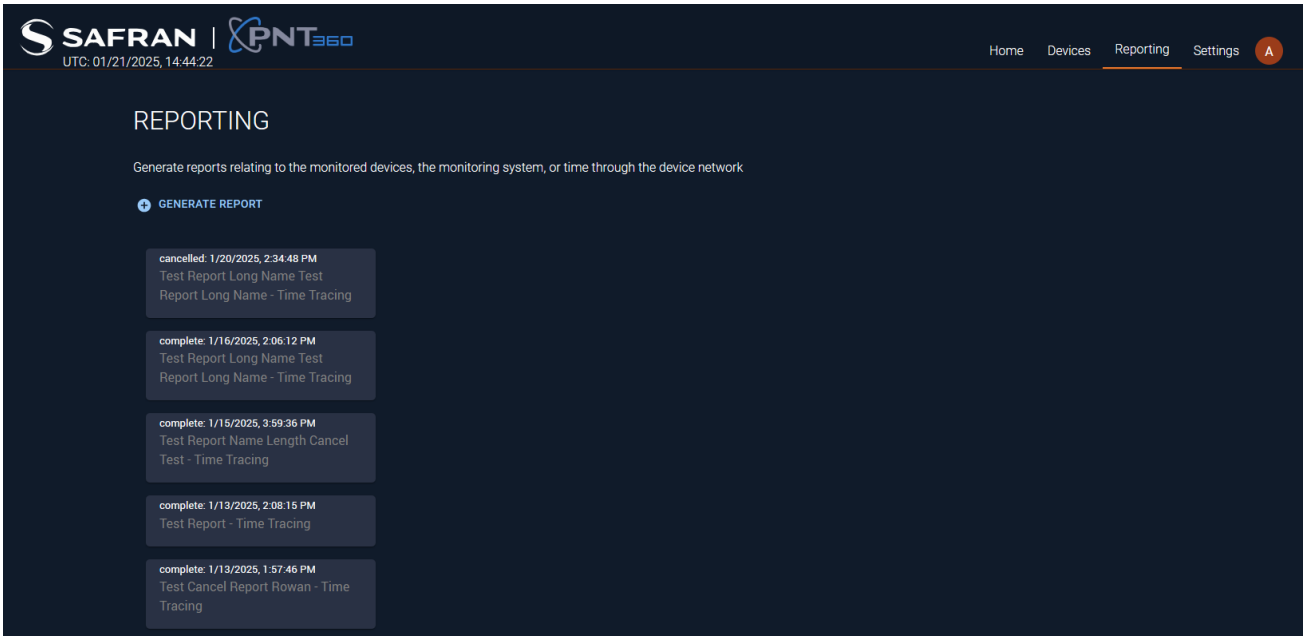
4.6. Time Tracing Report

4.6.1. Overview

The **Time Tracing Report** feature allows users to generate detailed reports related to monitored devices, the monitoring system, and time propagation across the device network. These reports provide insights into device information, source transitions, and time propagation.

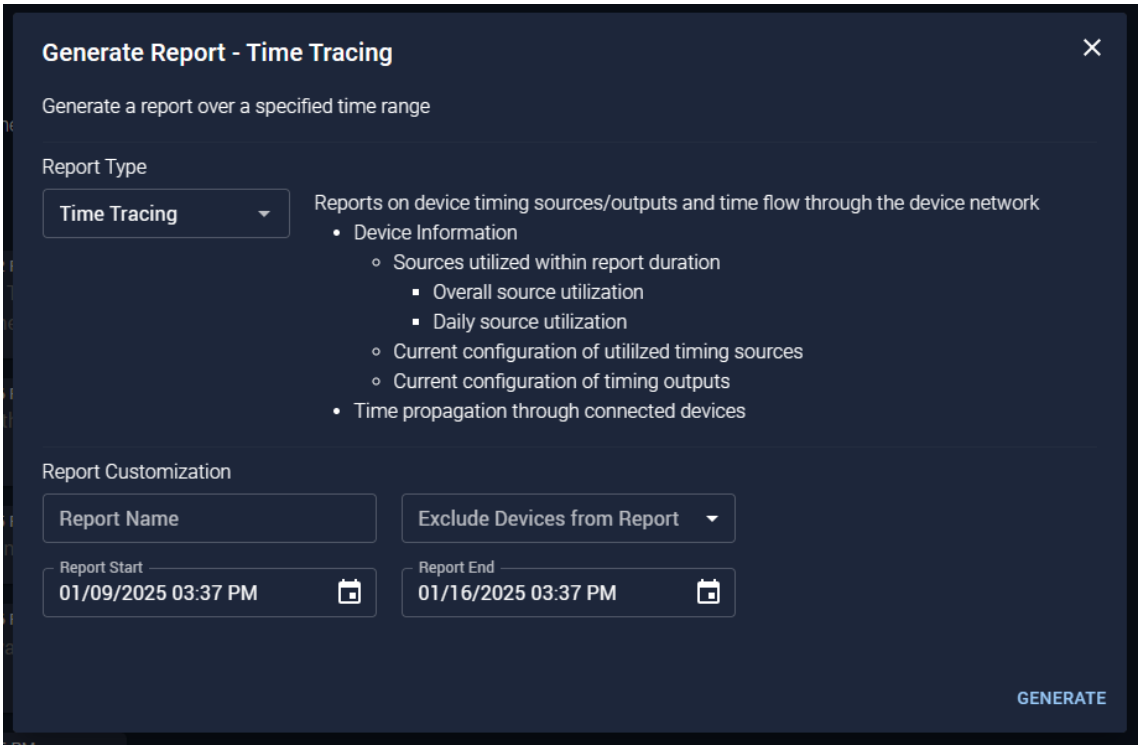
4.6.2. Accessing the Reporting Section

To access the reporting section, navigate to the **Reporting** tab in the main navigation menu. The **Reporting** page will display a list of previously generated reports and an option to create new ones.



4.6.3. Generating a Time Tracing Report

Select the **GENERATE REPORT** button, this will open a modal with available settings.



The following report customization options will be available:

- Report name.
- A dropdown list of devices that will exclude the selected devices from the report.
- Report start and end times.

4.6.4. Viewing a Report

Once a report is complete, it will appear in the list of generated reports with its status and timestamp. Select the report name to open it in the embedded viewer. The report contains:

- Device Information
- Source Transitions
- Source & Output Configuration
- Time Propagation

Use the embedded toolbar to download, print, or zoom into the report as needed.

4.6.5. Managing Reports

Delete a Report: Select the trash icon next to a report to remove it from the system.

5. Appendix

5.1. Installing a Custom SSL Certificate

To use your own SSL certificate instead of the self-signed certificate:

- Prepare your SSL certificate and key files ready. Rename your certificate file to **eclipse.pem** and rename your key file to **eclipse.key** and upload your files to the server.
- Replace the current certificate with your custom certificate:
  `sudo cp /path/to/your/eclipse.pem /etc/pnt360/ssl/eclipse.pem`
- Replace the current key with your custom key:
  `sudo cp /path/to/your/eclipse.key /etc/pnt360/ssl/eclipse.key`
- Restart the Nginx service using the following command:
  `sudo systemctl restart nginx`
- Verify the installation of your custom SSL certificate by accessing your application via a web browser and inspecting the certificate details.

5.2. User Permissions

Users in the General User and Administrator roles have the following permissions:

	General User	Administrator
Add, update, and remove devices	No	Yes
Add, update, and remove dashboards	No	Yes
Change device configurations	No	Yes
Change PNT 360 configuration	No	Yes
See, add, update, and remove users	No	Yes
See devices, dashboards, device configurations, and PNT 360 configuration	Yes	Yes

6. Safran Technical Support

For technical support, product specifications, and additional documentation, you can visit https://safran-navigation-timing.com/support-hub/ to submit a support request.

More information on standard unit behavior or any other features or functions of the SecureSync series or White Rabbit products can be found in the user manuals on our website at https://safran-navigation-timing.com/manuals/