zpe

zpe® cloud

User Guide v2.14.0

ZPE Systems, Inc.

Contents

Introduction to ZPE Cloud User Guide

Version 2.14. Document published: April 18, 2022.

If any features/functions cannot be viewed, user does not have necessary privileges.

Overview

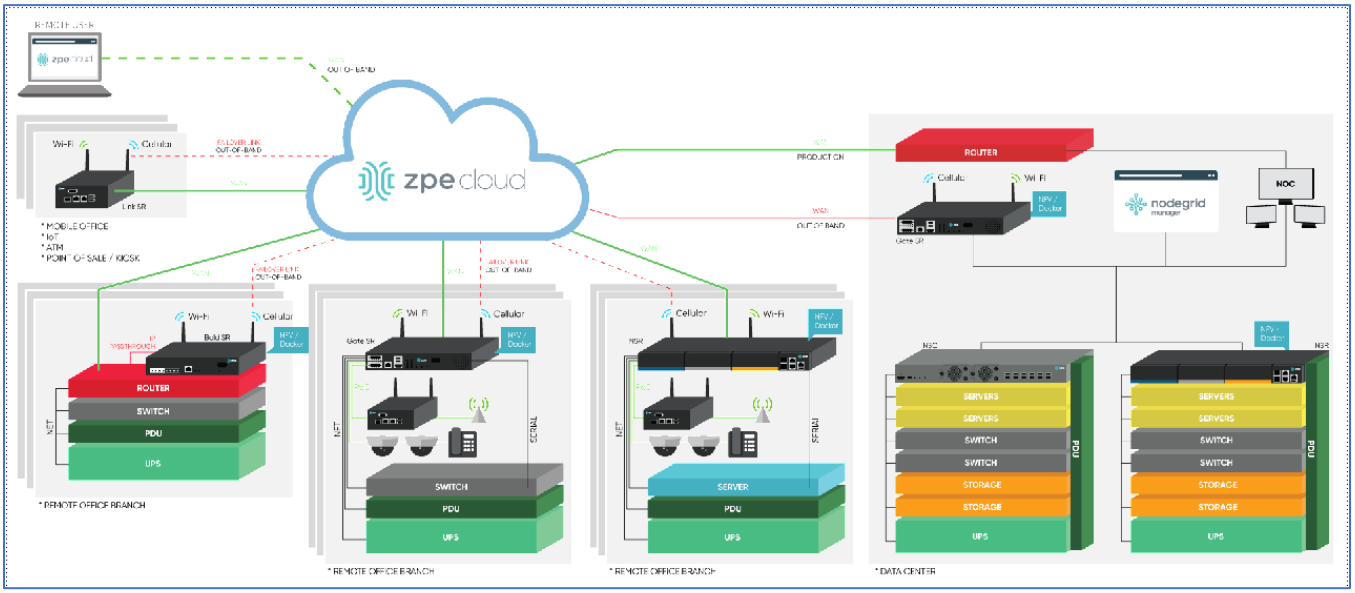
ZPE Cloud is a cloud-based management platform for Nodegrid products. Ongoing management provides a 360° visibility of the entire network deployment, complete with rich analytics. ZPE Cloud integrates all Nodegrid products into a single cloud platform. Branch IT devices are managed with via Serial, USB, IPMI, Power Management, and KVM.

ZPE Cloud ensures IT devices shipped to branch locations do not require staging or pre-configuration. When the device is installed, devices are then configured and integrated into the network. This maintains network security. No risk of shipping a USB thumb drive or third-party hands touching the network. Devices are deployed with consistent, automated provisioning within the ZPE Cloud from the safety of the NOC.

Nodegrid SR devices include failover capabilities via 4G/LTE cellular. Branch reconnection to the NOC is automatic via VPN or IPSec (even when Nodegrid is the first deployed branch device. Networking options can be extended with Guest OS & SDN. Compute power options deploy uCPE on Nodegrid Compute cards. IoT options use deployed Docker and Kubernetes directly on Nodegrid.

All Nodegrid products have a physical "Reset" button that reconnects devices back to the ZPE Cloud - a fast, easy process.

Here is a graphic representation of the ZPE Cloud structure.



Features

Primary ZPE Cloud features include:

- Cloud-based configuration & management of Nodegrid devices.
- Secure, fast, and consistent device deployment across all branch locations.
- Single Sign On (SSO) for fast access to all devices.
- ZTP over WAN – deployed devices are configured at the branch.
- Deploy configurations across the entire network.
- Direct interaction with branch locations to quickly scale and upload configurations from NOC
- All managed devices and ports are remotely accessible.

API Reference

For API developers, ZPE Cloud API details are available here: ZPE Cloud API.

Credits

Contact us

Sales: sales@zpesystems.com

Support: support@zpesystems.com

ZPE Systems, Inc.

3793 Spinnaker Court

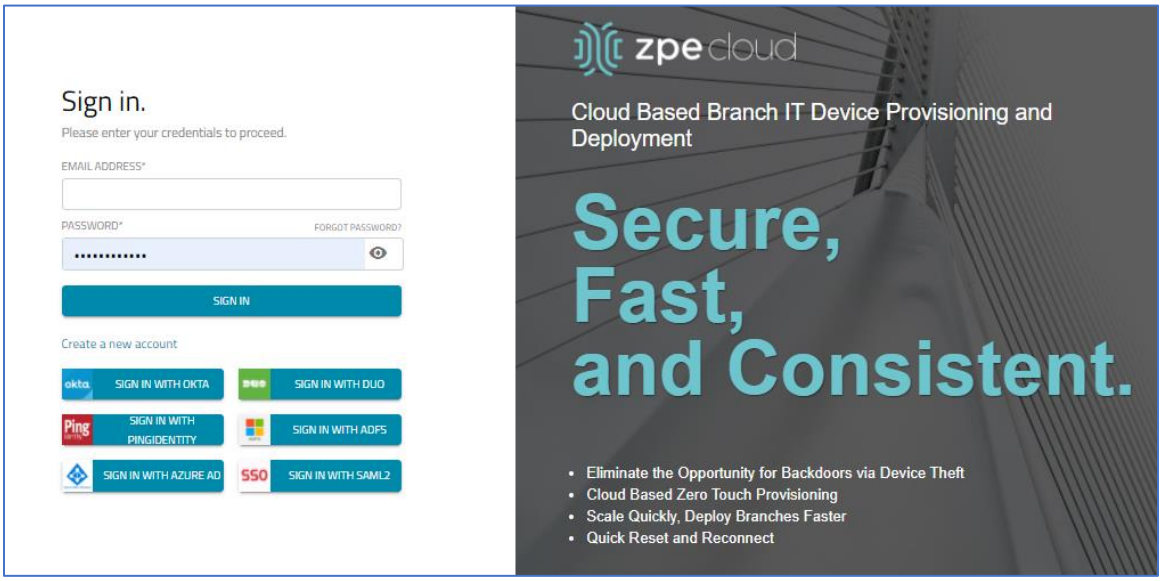
Fremont, CA 94538 USA

www.zpesystems.com

Getting Started

Web Page Sign In

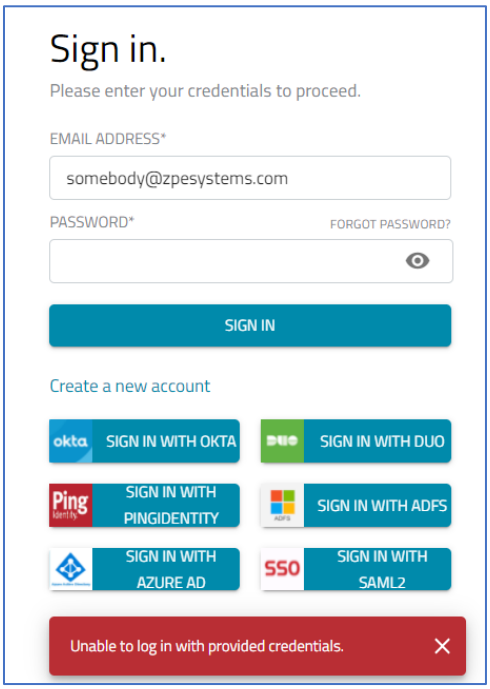
1. In the browser, enter the ZPE Cloud login URL: https://**<your_domain>**.zpecloud.com/login
2. Enter credentials (Email Address and Password), then click **SIGN IN**.



NOTE: The ZPE Cloud default language is based on the browser language setting.

Login Failure

1. If incorrect credentials are entered, this is the response.



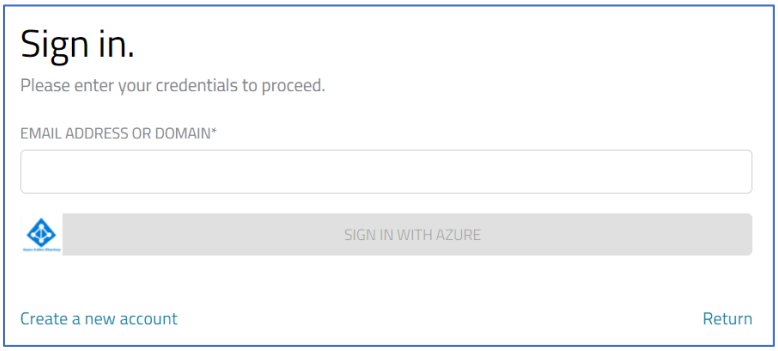
2. On the error message, click the "X" to close.
3. Carefully re-enter the credentials to ensure accurate input.

SSO with Identify Provider

If registered with one of these Identify Providers, use those credential channels to log into ZPE Cloud.

1. Click the appropriate Identify Provider,

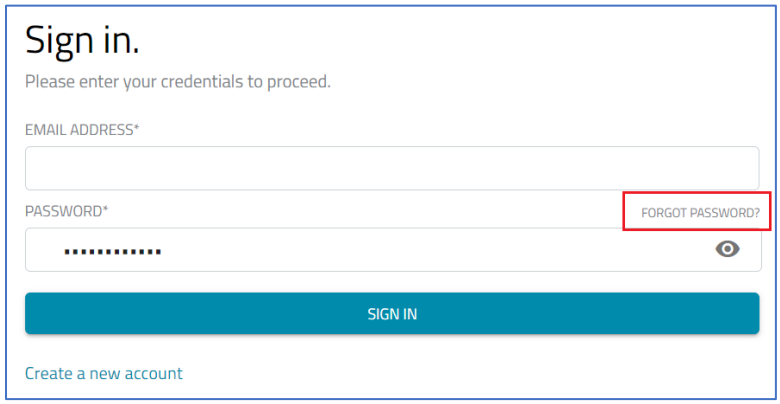
2. On the *Sign-in* dialog, enter personal credentials.



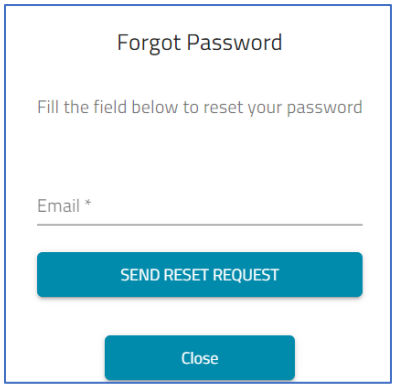
3. On validation, the ZPE Cloud application opens.

Forgot Password?

1. On the *Login* page, click **FORGOT PASSWORD**?.



2. On the *Forgot Password* dialog, enter the email address associated with the ZPE Cloud account.



3. Click **SEND RESET REQUEST**.
4. When the email is received, follow the instructions to reset the password.

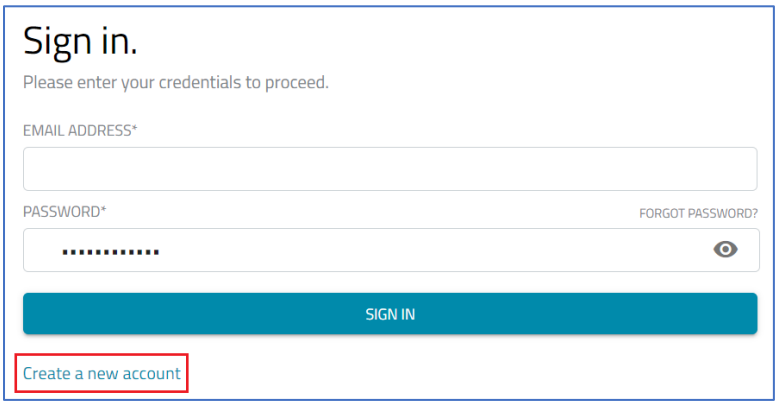
Still need help?

To contact the ZPE Support team, send an email describing the situation to: support@zpesystems.com

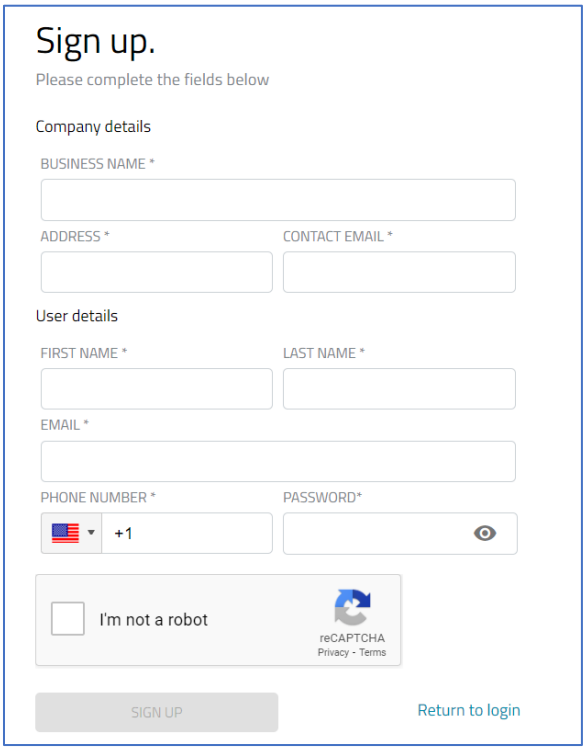
Sign Up for a New Account

For first-time access, a new account is required.

1. In the browser, enter: https://zpecloud.com/signup
2. Click **Create a new account**.



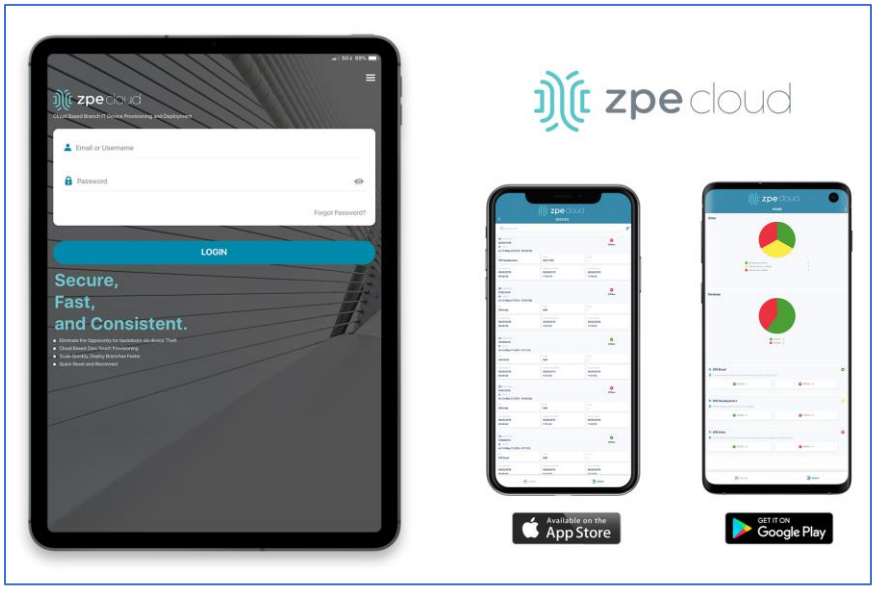
3. On the *Sign up* dialog, enter details in the required fields (marked with red asterisk *****).



4. Click **SIGN UP**.
5. When the verification email is received, follow the instructions.

Mobile Apps

The ZPE Cloud app is available for both iOS and Android.



iOS

On the iOS device, launch the App Store and search for "ZPE Cloud":

https://apps.apple.com/us/app/zpe-cloud/id1467791371

Android

On the Android device, launch the Play Store and search for ZPE Cloud:

https://play.google.com/store/apps/details?id=com.zpe

About ZPE Cloud User Interface Views

The ZPE Cloud UI has three levels of user access permissions. The user interface (UI) changes, based on the assigned permission level. This document contains all procedures, including those only available to administrators. If any functions are unavailable, it is because of limitations of user credentials.

NOTE: To refresh a page, click on the page's tab.

Administrator UI View

This permission allows full functionality and access to all Cloud functions

Operator UI View

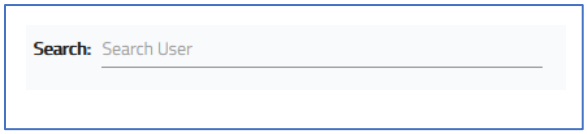
All device operations are allowed within the user's assigned Group(s).

User UI View

Device access is allowed within the assigned group.

Search Function

All section pages include the **Search** field. To use, start to type the search term. The table listing adjusts according to the entered characters.

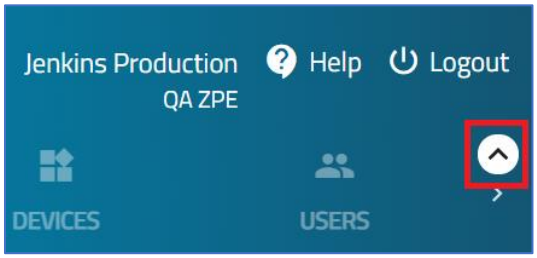


Banner Header

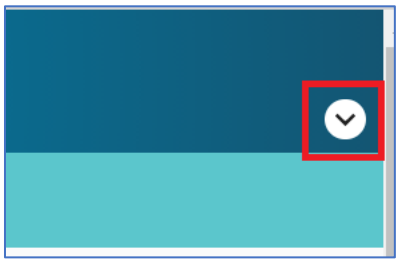
This banner header includes several short-cut links.

Show/Hide Banner Header

1. To hide the Header, click the *Up Arrow* (upper right).



2. To display the Header, click the *Down Arrow*.

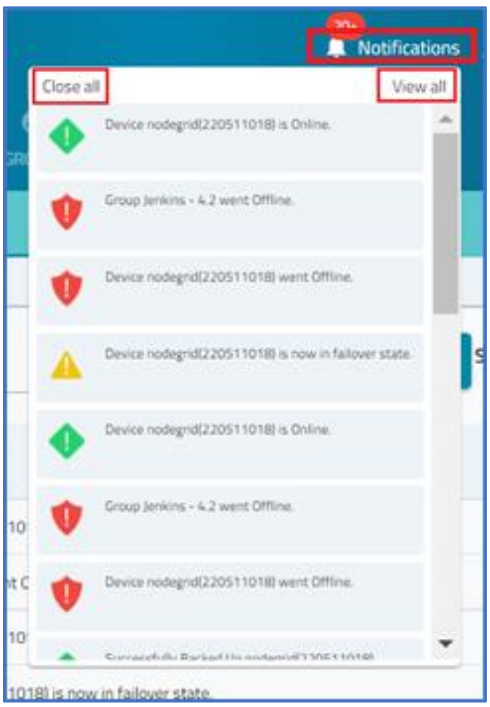


Notifications Shortcut

ZPE Cloud provides notifications of events on enrolled devices. All notifications are available within the application. Warning and Critical Error events can be sent to specific individuals by email and/or SMS. Notifications arrive asynchronously from any enrolled device.

View Events

1. To view recent events, click **Notifications** (upper right).



2. On the *Notifications* dialog, there are two buttons:

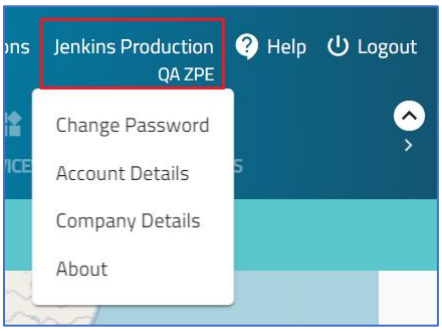
   Close all (upper left) to acknowledge awareness of the listed events.

   View all (upper right) to open the *TRACKING :: NOTIFICATION* page of all current notifications.

Account Settings

To change account and company details, click on the account name (top right corner).

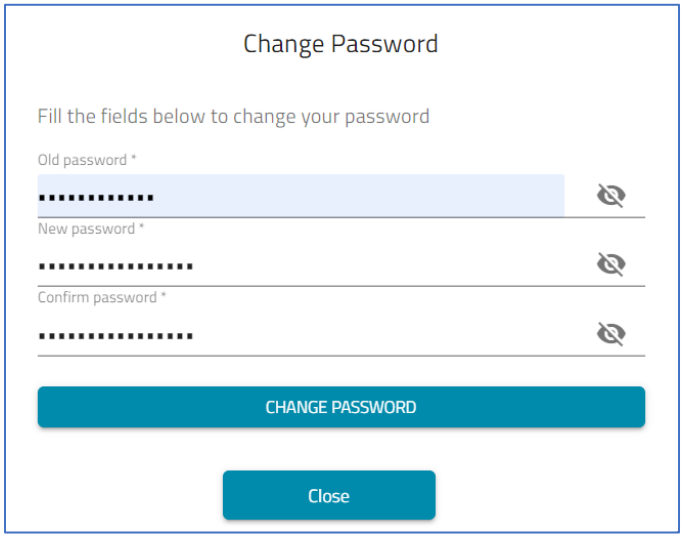
1. Click on the **Account Name** (upper right corner) to display the drop-down menu.



2. Click on the item to be updated.

Change Password

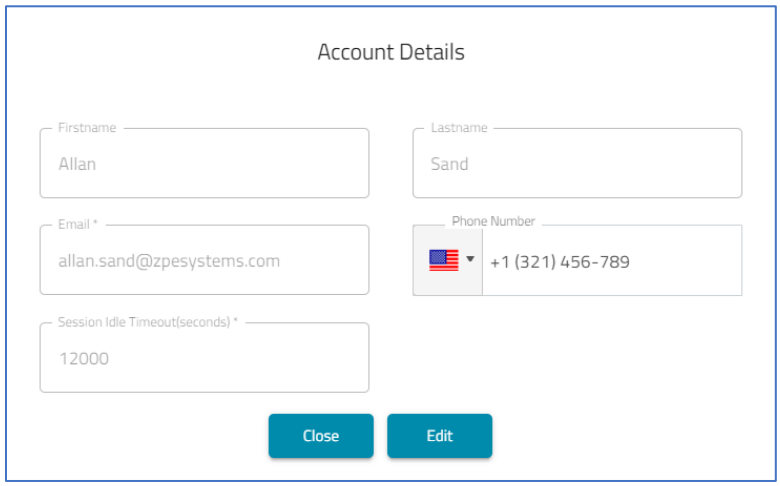
1. On the **Account Name** (upper right) drop-down, click **Change Password**.
2. On the *Change Password* dialog, enter the required fields:



3. Click **CHANGE PASSWORD**.

Account Details

1. On the **Account Name** (upper right) drop-down, click **Account Details**.

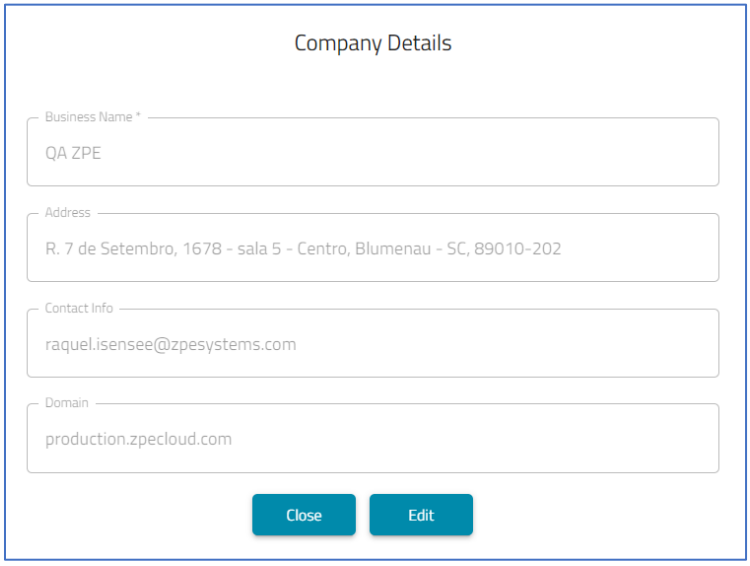


2. On the *Account Details* dialog, click **Edit** to go to *SETTINGS :: ACCOUNT* and update fields, as needed.
3. Click **Close** to close dialog.

Company Details

NOTE: This information can only be edited with Administrator privileges.

1. On the **Account Name** (top right) drop-down, click **Company Details**.
2. On the Company Details dialog, review the fields.

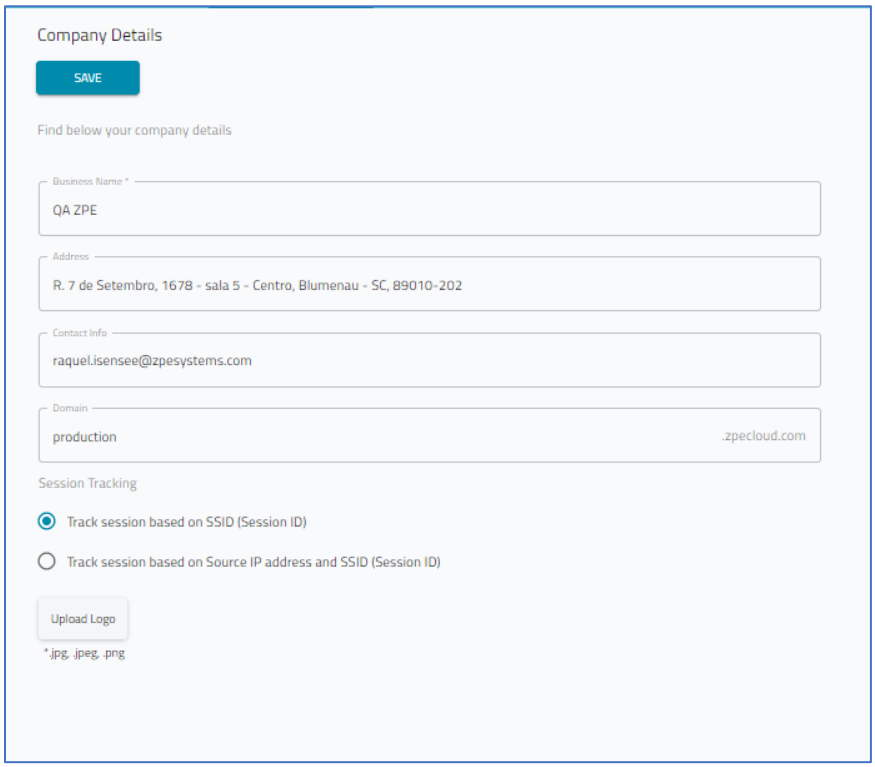


3. When done, click **Close**.

Edit Company Details

NOTE: Access to **Edit** button requires Administrator privileges.

(if available) When Edit is clicked, this opens the SETTINGS :: COMPANY page. Changes can be made here.

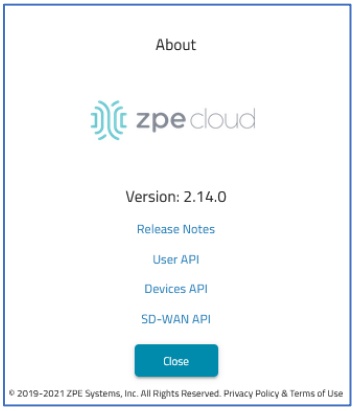


4. To add/change a logo to the user interface, click **Upload Logo** (must be jpg, jpeg, or png format).
5. In the *Open* dialog, locate and select the image.

   The logo is displayed on the Login page and the ZPE Cloud windows (upper left).
6. When done, click **SAVE**.

About

1. On the **Account Name** (top right) drop-down menu, click **About** (displays latest version of ZPE Cloud).

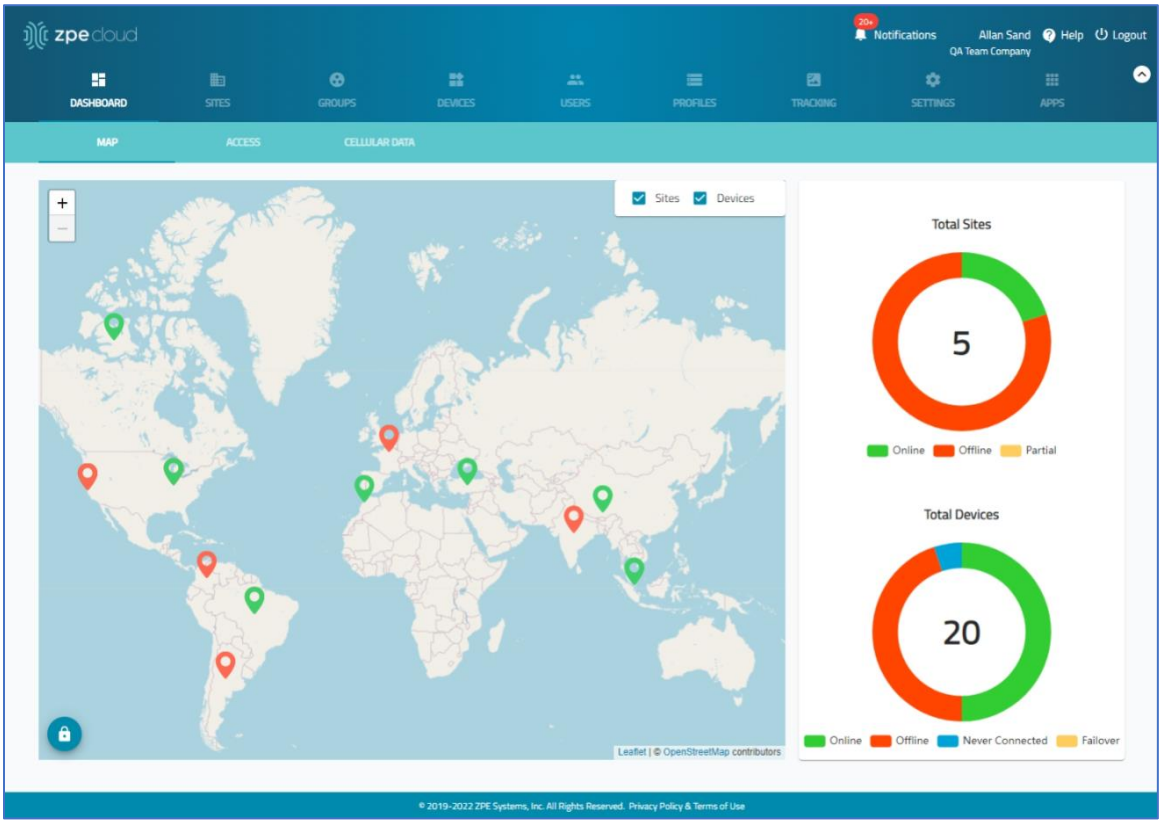


2. Click **Release Notes** link to open another browser window that displays current and previous Release Notes. Review as needed and close the browser window.
3. On the pop-up dialog, click **CLOSE**. or on any area outside the dialog box.

DASHBOARD Section

MAP tab

This page shows device location, relevant statistics, and current status of Sites and Devices.



Map View Controls

Show/Hid Devices/Sites

To toggle Map view of sites and devices, select/unselect the **Sites** checkbox and **Devices** checkbox. (select to display and unselect to hide).

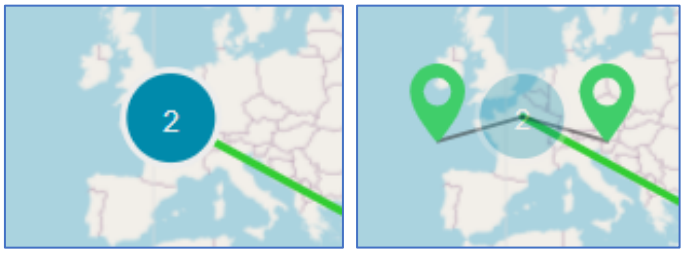
Zoom In/Out

Each user can configure a specific zoomed map view. Once set, the map automatically zooms to that when the Map tab is opened (can be modified any time).

Use the **Zoom plus (+)** and **minus (-)** buttons with drag feature to set the map view. When positioned, click the **Map Lock** button (lower-left). After navigating away from the Map page, on return, the set view will display. Click the **Map Lock** button again to unlock the Zoom function. User can still zoom in and out, as needed.

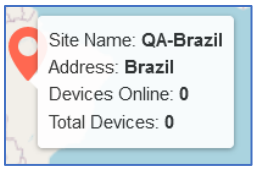
View Double-Device Location Details

When multiple devices are located in the same location, the map shows a circle with a number. Click the circle to expose the device markers. Click the markers to show details.

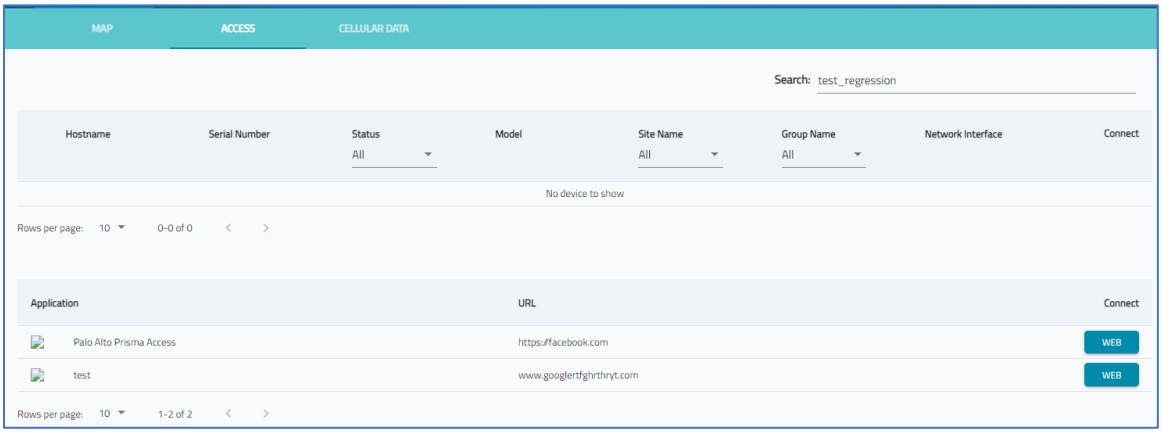


Site Map Details

Hover over a Site to display some details.

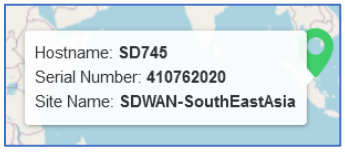


Click on the Site for additional information on the ACCESS tab.

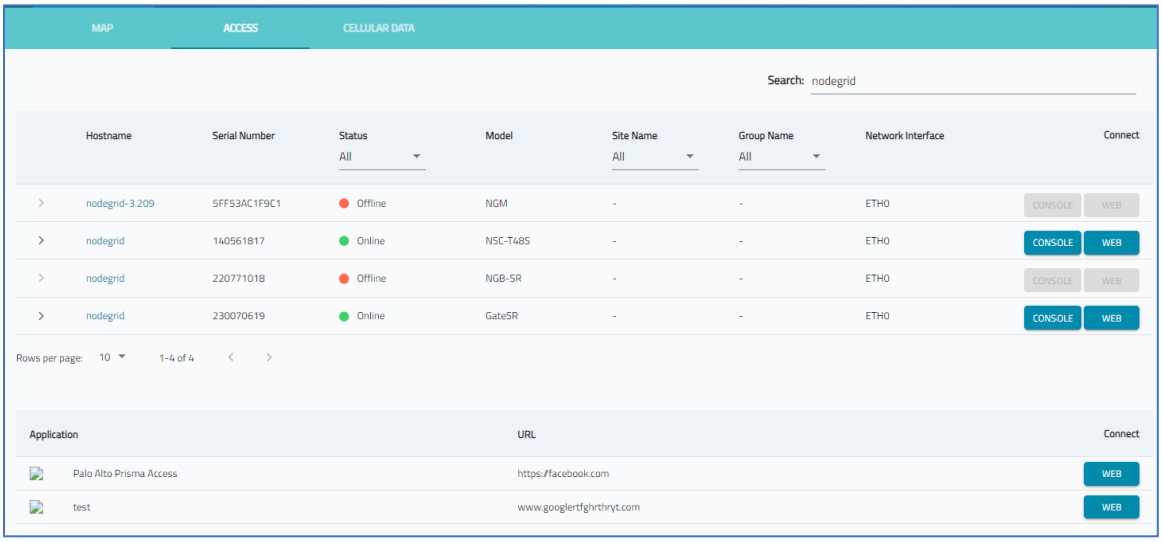


Device Map Details

Hover over a device to display details in a tooltip popup.

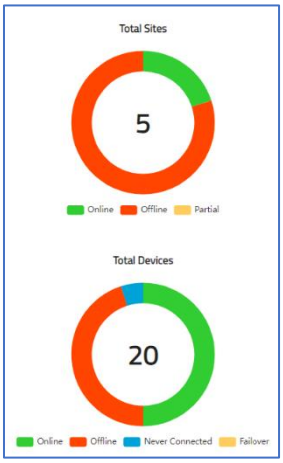


Click on a device for additional information on the ACCESS tab.



Site/Device Status

Status Panel (right side) provides a summary of Sites and Device status conditions. Hover over the individual colors for more information. Legend provides status conditions



Click the Site circle chart to go to the SITES section. Click the Devices circle chart to go to the *DEVICES* section. These Charts show the total registered sites and devices, and the total proportion for each status. Status conditions are shown in the Site Status and Device Status tables.

Site Status

Status	Description
Online	All devices at that site are online
Offline	All devices at that site are offline
Partial	Some devices at that site are online while others are offline

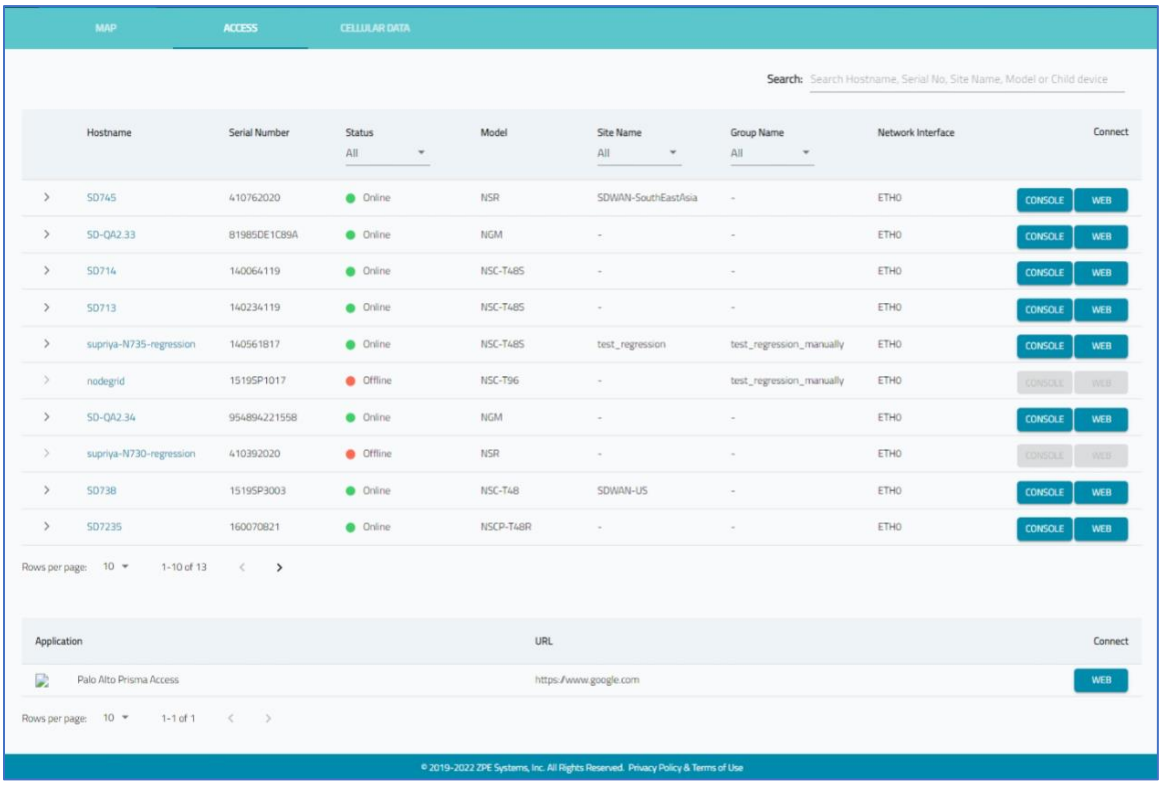
Device Status

Status	Description
Online	Device is online.
Offline	Device is offline.
Never Connected	Device has never connected to ZPE Cloud.
Failover	Device is not using the primary network interface.

NOTE: Device status is updated at regular intervals.

ACCESS tab

On this page, a remote connection can be launched to a Nodegrid device, one of its ports, or a managed device connected to it.



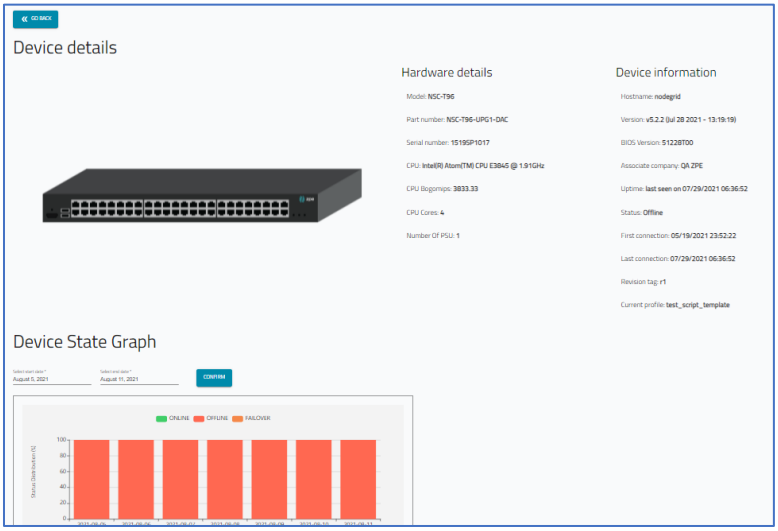
Click the **Right-Arrow** button next to a device to review a drop-down dialog. Click the **Down-Arrow** to close the dialog.

Filters

Listing can be filtered by Status, Site Name, or Group Name.

Device Details

To view details on the device, click on a Hostname:

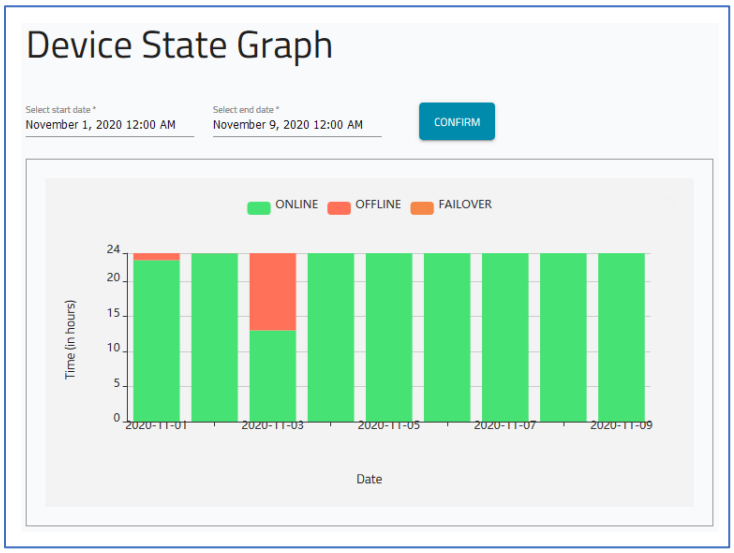


Major menus include:

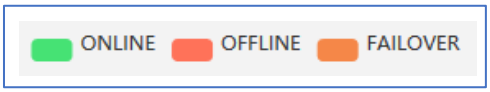
- Device Details
- Device State Graph (state of device by day and hour)
- IMEI Cellular Information
- SIM Card Information
- SIM Status Graphs

Device State Graph

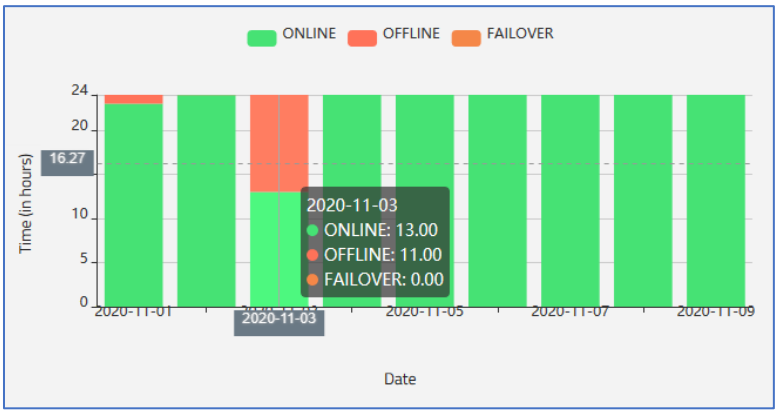
The *Device Status Graph* menu displays the state of the device on a bar chart.



1. To filter data, select a start and end date, then click **Confirm**.
2. Each option can be viewed/hidden by a click on the three categories:



3. For more detailed information, hover the mouse cursor over a point on the graph:



Connections

Supported connections are WEB (WebUI), Console (CLI window), KVM, and MKS. Device connection types are:

Nodegrid (Web and Console)

USB Ports (Console)

Serial Ports (Console)

Managed Device (Web, Console, KVM, MKS)

(Grayed button indicates Connection function is disabled.)

List can be filtered by Site, Group, Device, and Time period.

NOTE: If Remote Access is not enabled on the Nodegrid device, the connection type buttons are disabled (grayed out).

Access a Device

There are two ways to access a listed device.

CONSOLE – on login to the device, opens the CLI command line window.

WEB – on login to the device, open the WebUI of the device.

If these buttons are greyed out, there is no device access.

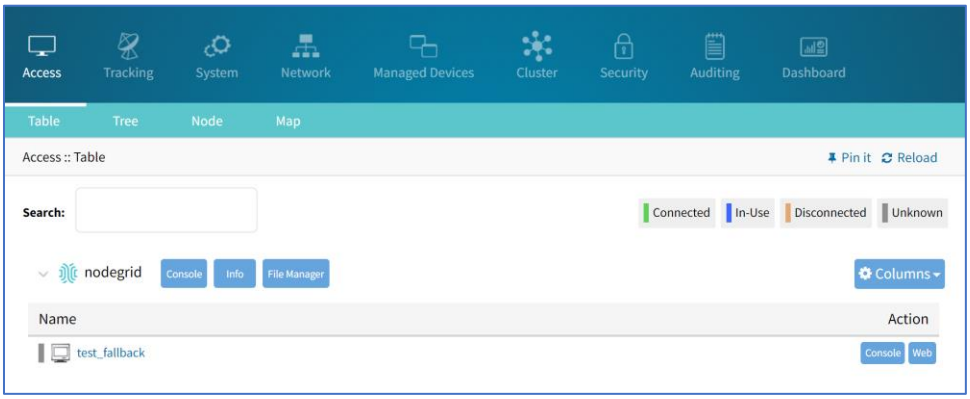
Log into a Device

1. To launch a device's remote connection, in the *Connect* column, click Connect button.
2. On the small pop-up dialog, options are: **CONSOLE** (CLI window) or **WEB** (device UI).

3. (as needed) On the *Login* page, enter device credentials and click **Login**.

4. If **CONSOLE** is selected, the CLI window displays.

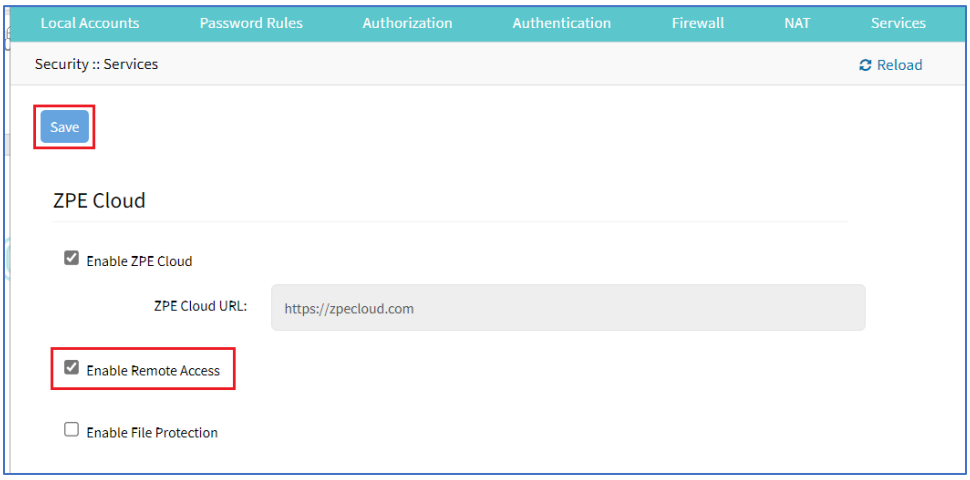
5. If **WEB** is selected, the Nodegrid device user interface displays.



Enable Remote Access on Device

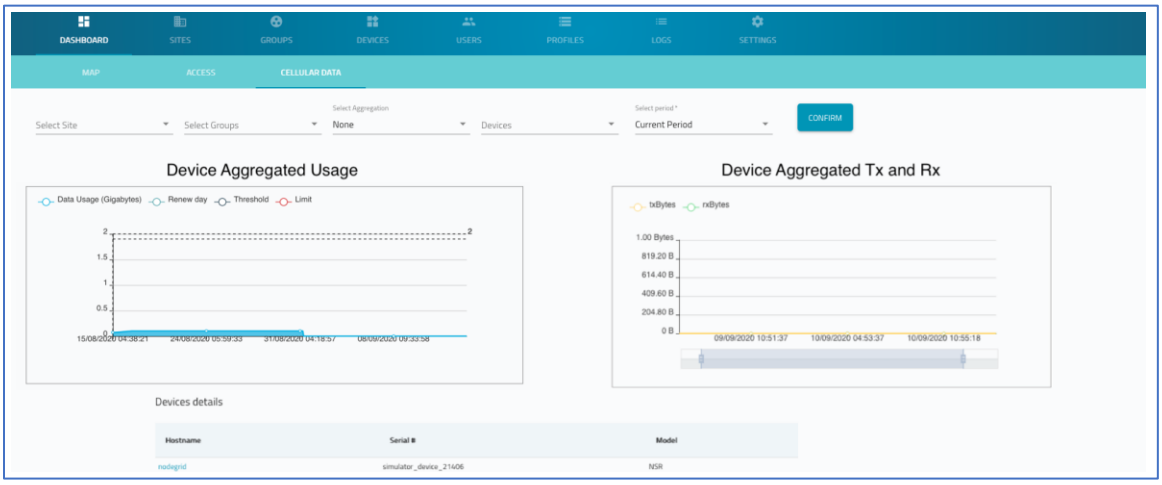
By default, Nodegrid remote access is disabled. To enable:

1. Login to the device's Web connection.
2. Go to *Security :: Services*.
3. In the *ZPE Cloud* menu, select **Enable Remote Access** checkbox, then click **Save**.



CELLULAR DATA tab

This page includes information related to cellular modems and SIM cards. The view can be displayed for a specific time frame.



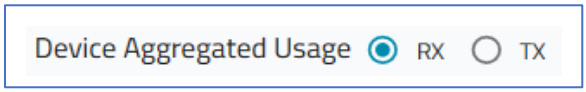
1. To filter results, select one of the following and a designated time range:

   Site

   Group

   Device

2. As appropriate, select RX or TX radio button.



3. Below the graphical data, a table provides additional details:

4. In the table, click the hostname of any device to display its *Device Details* page.

On the *Device Details* page (below the cellular modem information), is the accumulated data consumed per SIM card within the selected time window (in MB). With this graph, a review of data usage limits can be checked against the Data Plan Renewal Date.

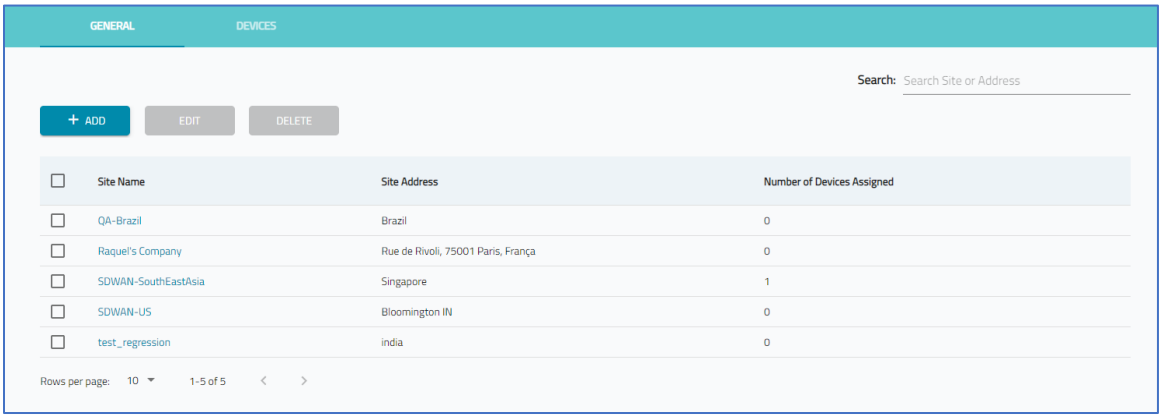
The SIM STATS shows the amount of data transfer with a cellular modem connection for a specified time period. Data is separated by each installed SIM card in that cellular modem. Data is split between data transmitted (TX) and data received (RX).

SITES Section

A Site is a logical association of a name and address (or coordinates) and includes multiple devices. Each device in a Site has a status (online, offline). Sites are viewable on the MAP page, with coordinates.

GENERAL tab

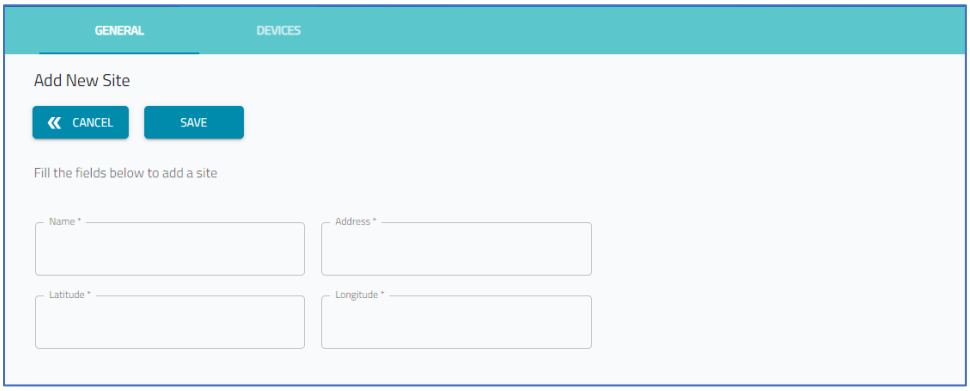
This page lists all of the Company's Sites. Sites can be added, deleted, and updated.



Manage Sites

Add a new Site

1. Go to *SITES :: GENERAL*.
2. Click **+ADD** (displays dialog).



3. Enter **Name** (name of site)
4. Enter **Address** (street, city, state, country)
5. Enter **Latitude** and **Longitude** (use any GPS device)
6. Click **SAVE**.

The Site becomes visible on the *MAP* tab.

Edit Site Details

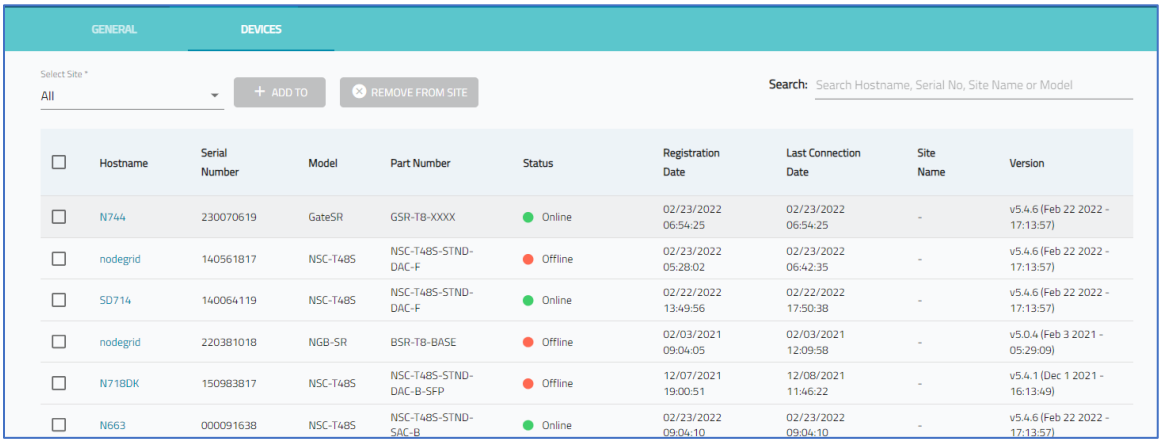
1. Go to *SITES :: GENERAL*.
2. On the list, identify the site and select the checkbox.
3. Click **EDIT**.
4. Make changes, as needed.
5. Click **SAVE**.

Delete a Site

1. Go to *SITES :: GENERAL*.
2. On the list, locate the site and select the checkbox next to the name.
3. Click **DELETE**.
4. On the *Delete Confirmation* dialog, click **DELETE**.

DEVICES tab

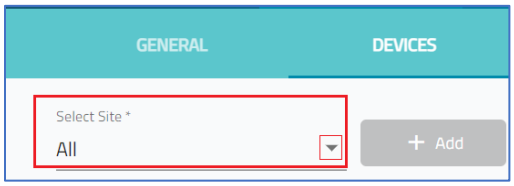
This page lists devices assigned to a site or available to be assigned to a site.

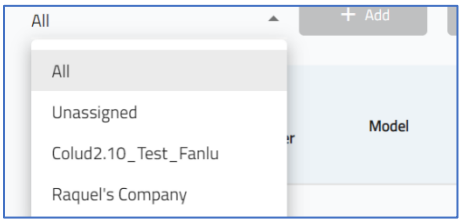


Filter Displayed Devices

View Devices assigned to a Site

1. Go to *SITES :: DEVICES*.
2. ,Click the **Select Site** down arrow.





3. On the drop-down, select one:

   All (all devices, regardless of status)

   Unassigned (only devices not assigned to a Site)

   <name of site> (devices assigned to the Site)

The list updates according to the selection.

Two Ways to View Devices

On the *GENERAL* tab, click the **Site Name**. View changes to the DEVICES tab and lists all devices assigned to that site.

On the *DEVICES* tab, **Select Site** drop-down, click the site name.

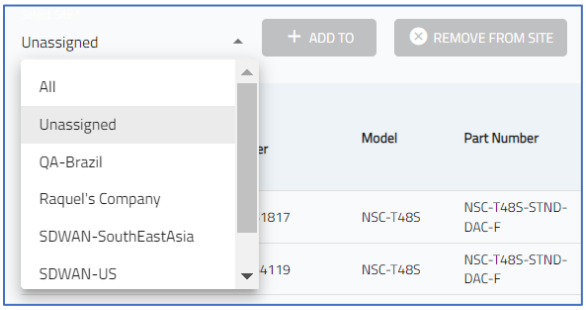
View Devices Not Assigned to a Site

1. Go to *SITES :: DEVICES*.
2. On the **Select Site** drop down, select **Unassigned**.
3. The list displays all unassigned devices.

Manage Devices on Sites

Move an Unassigned Device to 1 or more Site(s)

1. Go to *SITES :: DEVICES*.
2. On the **Select Site** drop down, select **Unassigned**.



3. On the list, identify the device(s) and select each checkbox.
4. Click **+ADD TO** (displays dialog).

5. Select checkbox next to each site the device is to be added.
6. Click **+ADD ON SITE**.

The device is added to the selected Site(s).

Remove a Device from a Site

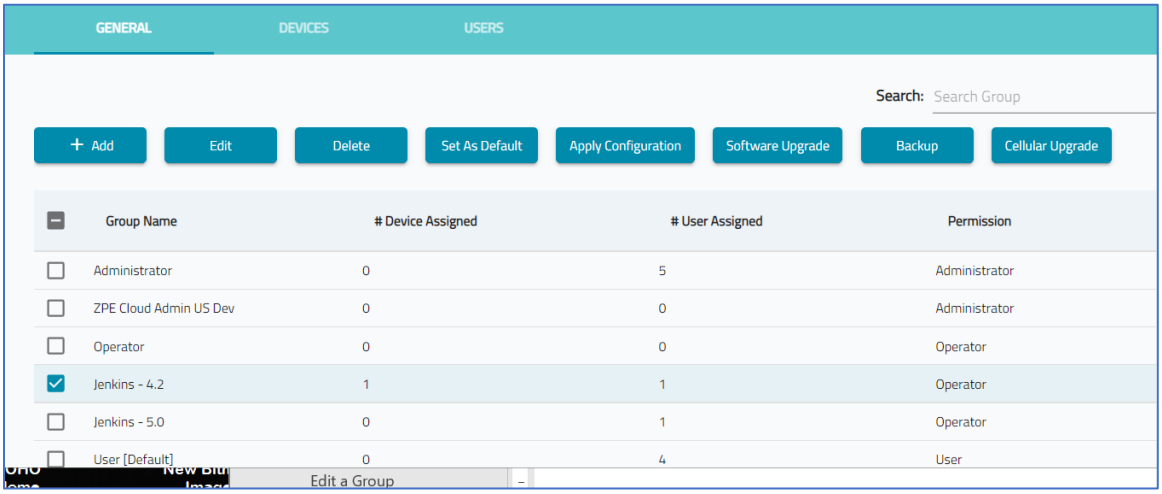
1. Go to *SITES :: DEVICES*.
2. On the **Select Site** drop down, select a site.
3. On the table, identify the device(s) and select each checkbox.
4. Click **REMOVE FROM SITE**.
5. The removed device is displayed in the *Unassigned Device* list.

GROUPS Section

A Group is a logical association of multiple devices and multiple users. The association can use any criteria – location, type, purpose, etc. Each group can have one or more Group Admins who manage one or more groups of devices.

GENERAL tab

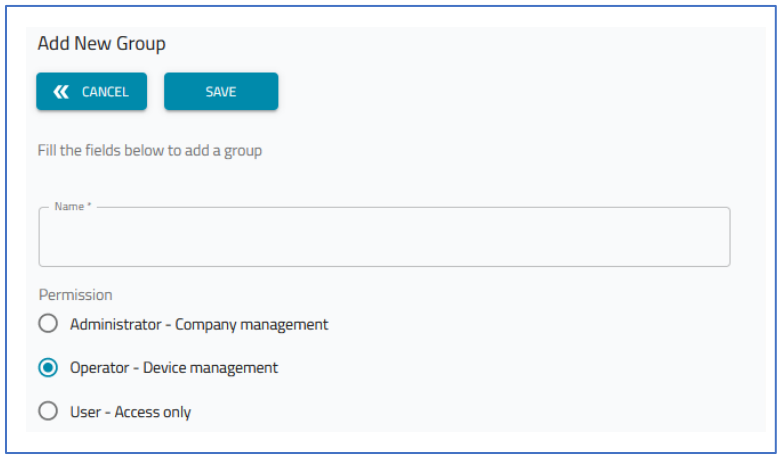
Groups are managed on this page. When a group checkbox is selected, available managements are displayed. Any greyed buttons are unavailable functions.(



Manage Groups

Add a Group

1. Go to *GROUPS :: GENERAL*.
2. Click **+ADD** (displays dialog).



3. Enter a **Name** for the new group.
4. Select the group's permission level.

Administrator radio button (manages all devices, company credentials, and users within their company)

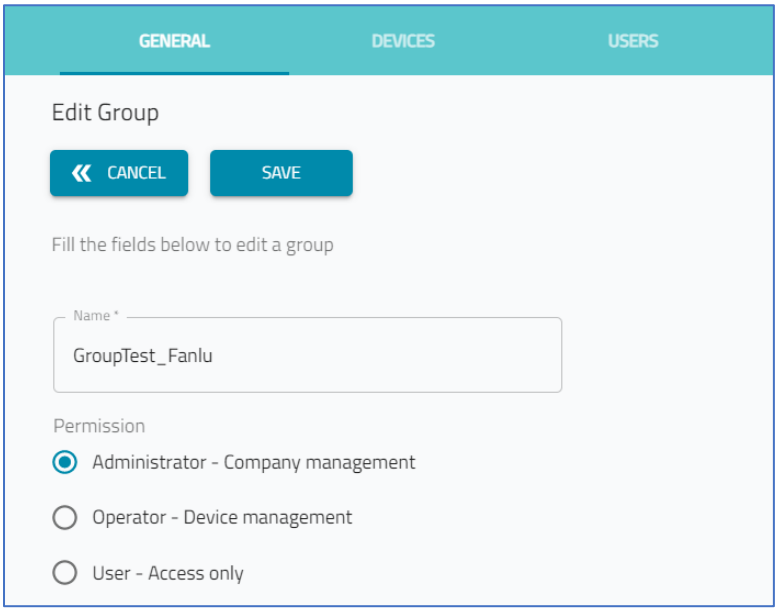
Operator radio button (performs and creates operations within all devices assigned to their group)

User radio button (can only access devices within the group)

5. Click **SAVE**.

Edit a Group

1. Go to *GROUPS :: GENERAL*.
2. Locate the Group and select the checkbox.
3. Click **EDIT** (displays dialog).

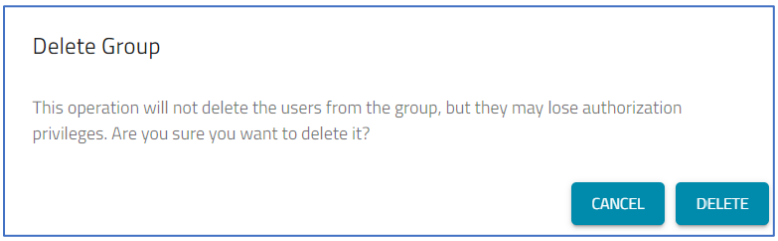


4. Make changes, as needed.
5. Click **SAVE**.

Delete a Group

To delete one (or more) group(s):

1. Go to *GROUPS :: GENERAL*.
2. Locate the Group and select the checkbox.
3. Click **DELETE** (displays dialog).

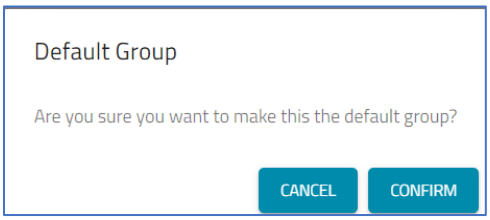


4. On the *Delete Group* pop-up dialog, click **DELETE**.

   NOTE: Default groups cannot be deleted. Deleting a group does not delete users, but privileges on the group are removed.

Set the Default Group

1. Go to *GROUPS :: GENERAL*.
2. Locate group and select the checkbox.
3. Click **SET AS DEFAULT** (displays dialog).

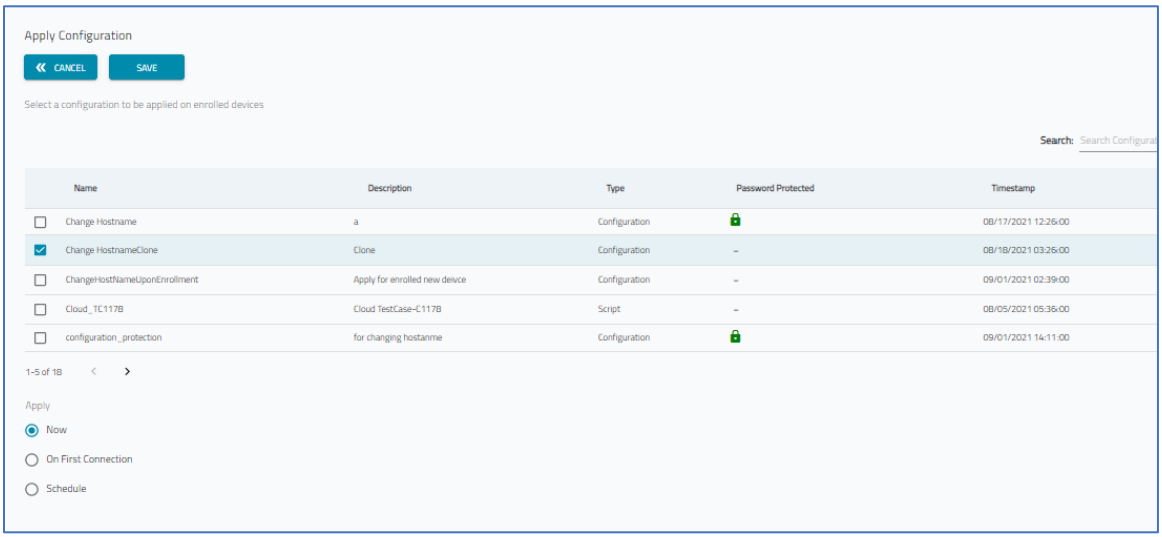


4. On the *Default Group* pop-up dialog, click **CONFIRM**.

   NOTE: The default group is assigned to all new users logging in with SSO by Domain.

Apply Configuration

1. Go to *GROUPS :: GENERAL*.
2. Locate the group and select the checkbox.
3. Click **APPLY CONFIGURATION** (displays dialog).



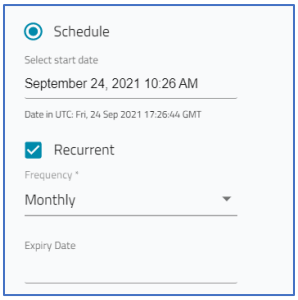
4. On the *Apply Configuration* dialog, select appropriate configuration checkboxes.
5. In *Apply* menu, select when the configuration is applied.

   Now radio button (when saved, operation executes immediately)

   On First Connection radio button (execute operation the first time the device(s) comes online)

   Schedule radio button (if selected, choose a date/time to execute the operation)

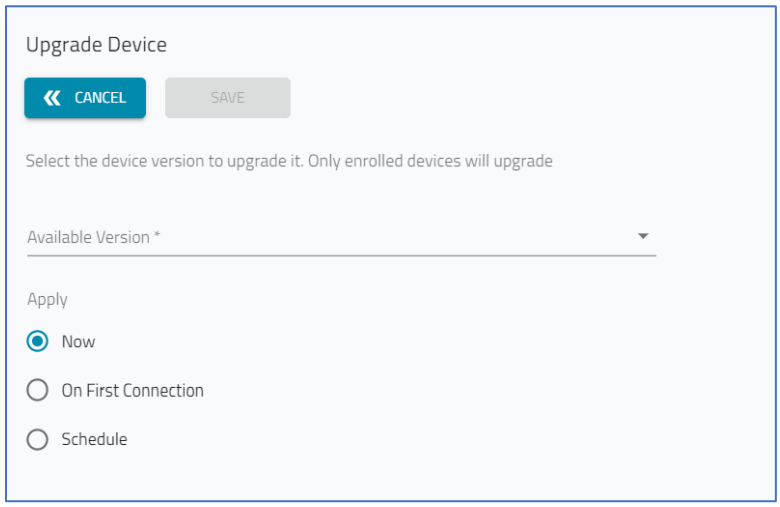
   Recurrent (if selected, how often the operation is executed: hourly, daily, weekly, monthly,



6. Click **SAVE**.

Software Upgrade

1. Go to *GROUPS :: GENERAL*.
2. Locate the group and select the checkbox.
3. Click **SOFTWARE UPGRADE** (displays dialog).

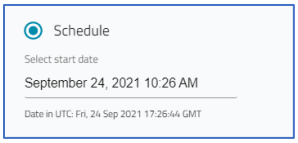


4. On the *Available version* drop-down, select one.
5. In *Apply* menu, select when the action is applied.

   Now (when saved, execute operation immediately)

   On First Connection (execute operation the first time the device(s) comes online)

   Schedule (if selected, choose a date to execute the operation)

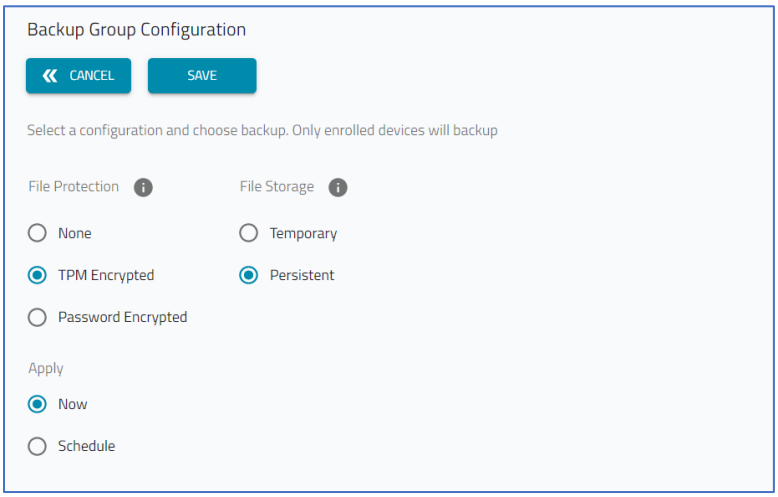


6. Click **SAVE**.

Backup Group

1. Go to *GROUPS :: GENERAL*.
2. Locate the group and select the checkbox.
3. Click **BACKUP** (displays dialog).

   NOTE: The Backup operation requires Nodegrid version 4.1.9 or higher, and the Cellular Upgrade operation requires version 4.2 or higher.



4. In the *File Protection* menu, select one

   None radio button

   TPM Encrypted radio button

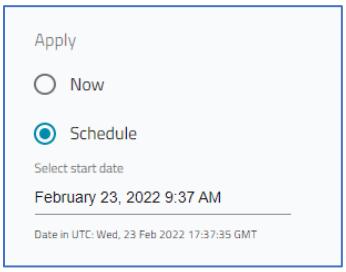
   Password Protected radio button

5. In the *File Storage* menu, select one (**Temporary**, **Persistent**).

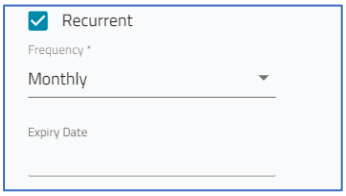
6. In *Apply* menu, select when the action is applied.

   Now (when saved, execute operation immediately)

   Schedule (if selected, choose a date to execute the operation)



   Recurrent (if selected, how often the operation is executed: hourly, daily, weekly, monthly,

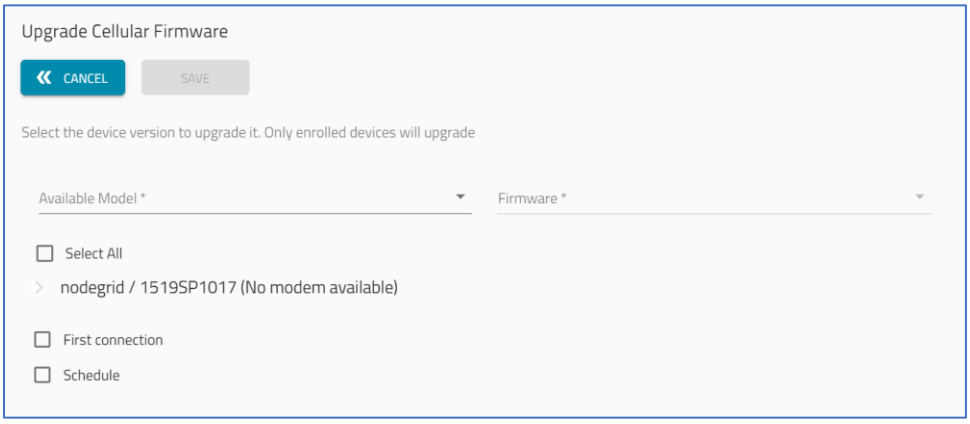


7. Click **SAVE**.

Cellular Upgrade

1. Go to *GROUPS :: GENERAL*.
2. Locate the group and select the checkbox.

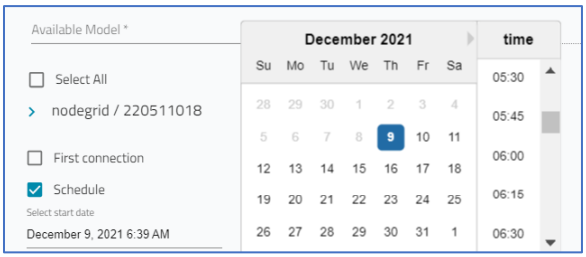
3. Click **CELLULAR UPGRADE** (displays dialog).



4. On the *Available Model* drop-down, select one.
5. On the *Firmware* drop-down, select one.
6. (as needed) Select the **Select All** checkbox to apply all the items in the listing
7. Select a time to apply the upgrade:

   First Connection (execute operation the first time the device(s) comes online)

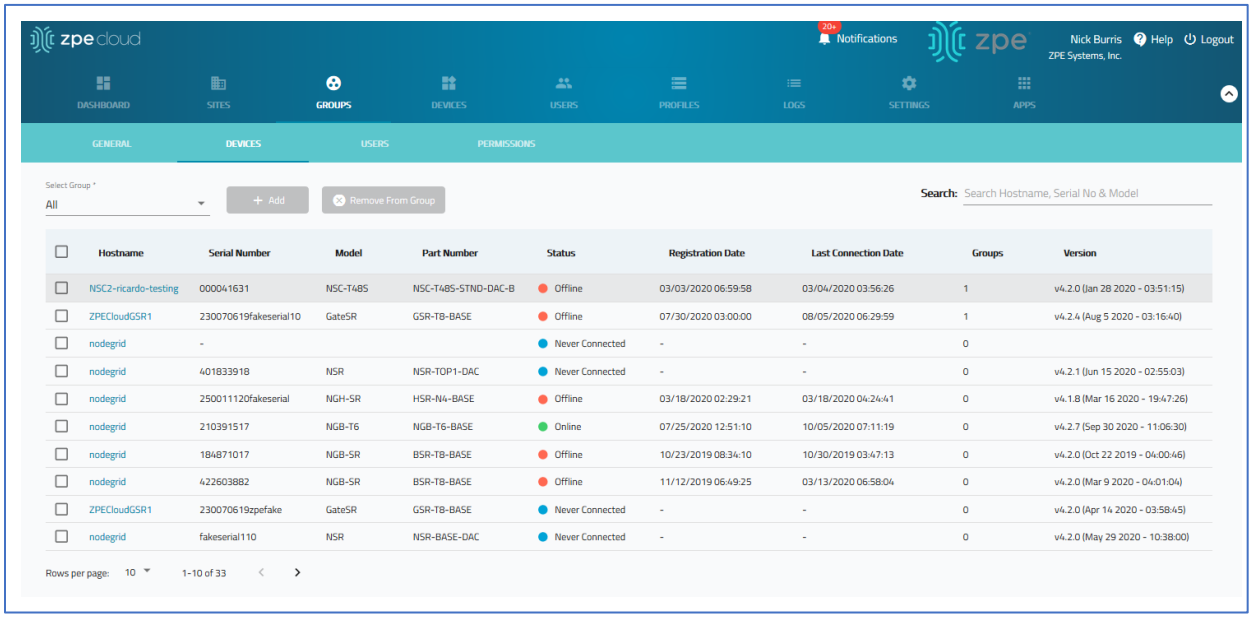
   Schedule (if selected, choose a date/time to execute the operation)



8. Click **SAVE**.

DEVICES tab

This page displays all Nodegrid devices currently registered to ZPE Cloud.



Device Details Table Columns

Column Name	Description
Hostname	The device name.
Serial Number	Serial number of the device.
Model	Device model.
Part Number	Device part number.
Status	Status of the device: Online, Offline, Never Connected.
Registration Date	Date the device was registered.
Last Connection Date	Last date device was connected to ZPE Cloud.
Groups	Number of groups the device is a member.
Version	Version of the device firmware.

Display Device Details page

Click the device Hostname to open the device's details page.

Manage Group's Devices

Add Device(s) to a Group

NOTE: A device can be assigned to one or more groups.

To add a device (or multiple devices) to a group (or groups):

1. Go to *GROUPS :: DEVICES*.
2. On the list, identify devices and select each checkbox.
3. Click **+ADD** (displays dialog).

4. Select the Group(s) checkboxes, then click **ADD ON GROUP**.
5. A small pop-up (lower right) confirms the operation is successful.

Remove Devices from Group

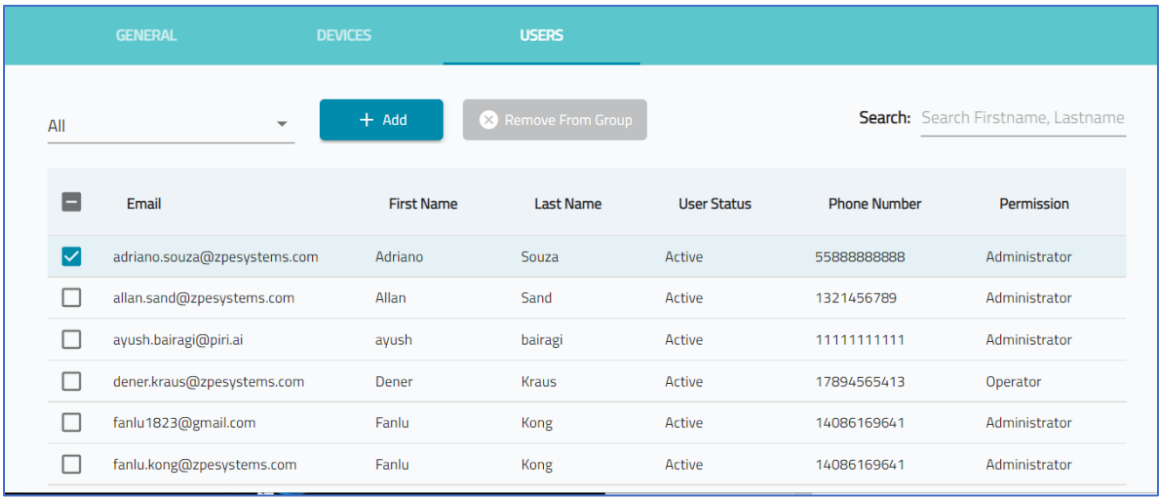
To remove devices (one or more) from a group:

1. Go to *GROUPS :: DEVICES*.
2. On the **Select Group** drop-down, select the Group with devices to be removed.

3. On the listing, locate devices to be removed and select checkboxes.
4. Click **REMOVE FROM GROUP**.
5. A small pop-up (lower right) confirms the operation is successful.

USERS tab

This displays all available users.



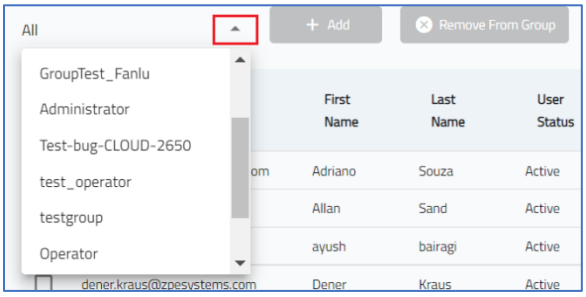
User Details Table Columns

Column Name	Description
Email	User's email address
First Name	User's first name
Last Name	User's last name
User Status	User's status: Active, Inactive
Phone Number	User's phone number
Permission	Administrator, Operator, or User

Manage Users

View Users of a Group

1. On the *Select* drop-down, select one.

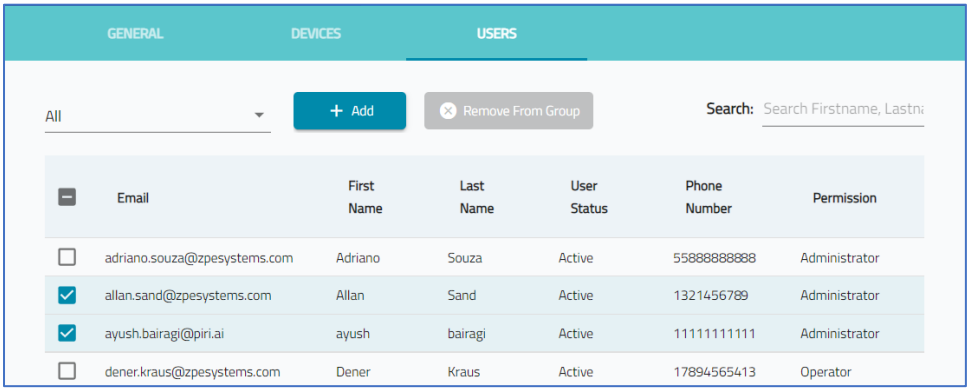


2. The list populates users that belong to the selection.

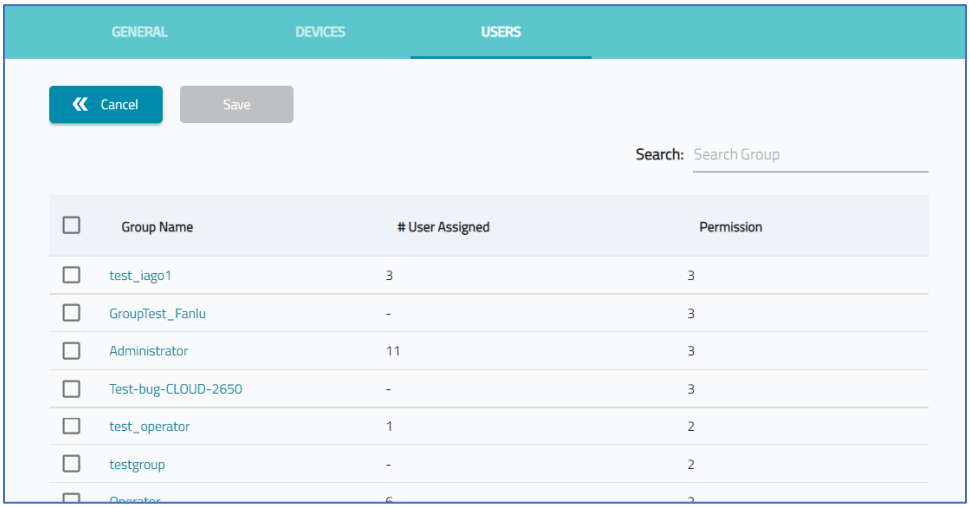
Add Users to Group

To add a user to a one or more groups:

1. Go to *GROUPS :: USERS*.
2. Locate the user(s) and select the checkbox(es).



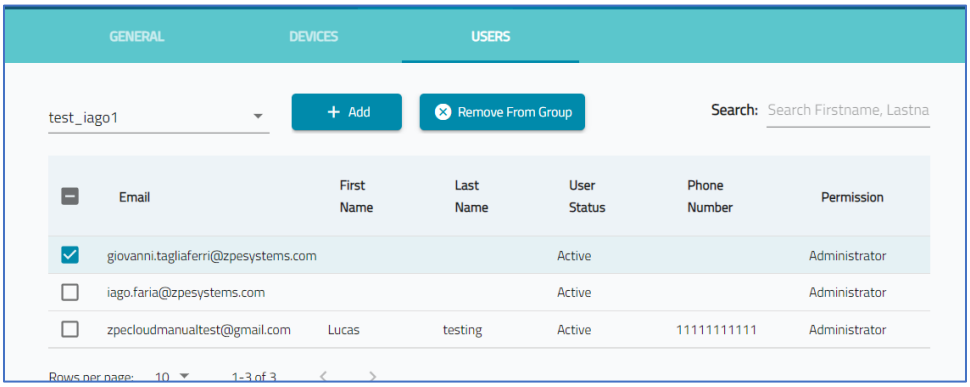
3. Click **+ADD** (displays dialog).



4. Select the Group(s) checkboxes to add user(s).
5. Click **SAVE**.

Remove User(s) from Group

1. Go to *GROUPS :: USERS*.
2. On the *Select* drop-down, select the Group.



3. On the list, select checkboxes of user(s) to remove.
4. Click **REMOVE FROM GROUP**.

DEVICES Section

This section is used for the management, configuration, and enrollment of all Nodegrid devices that are connected to the ZPE Cloud.

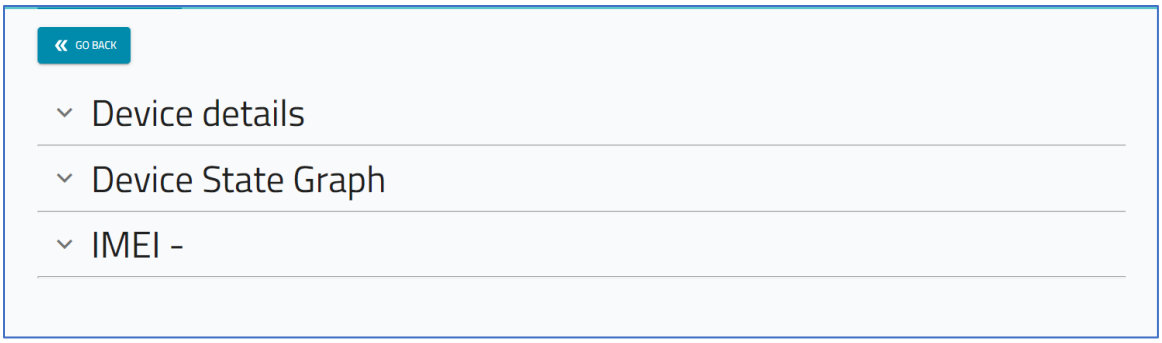
Device details are available on ENROLLED, AVAILABLE, and PENDING APROVAL tabs.

Click Device Hostname

In the Hostname column, click on the device. This displays extensive information On the *Device details* page.

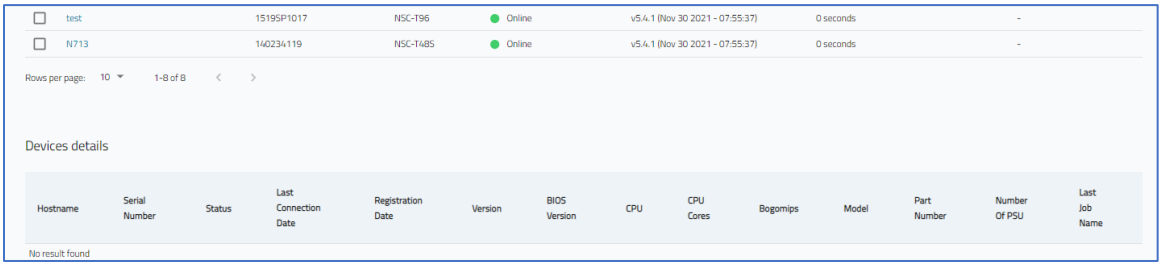
On the **Enrolled** tab, when a device checkbox is selected, the *Devices Details* table provides current information.

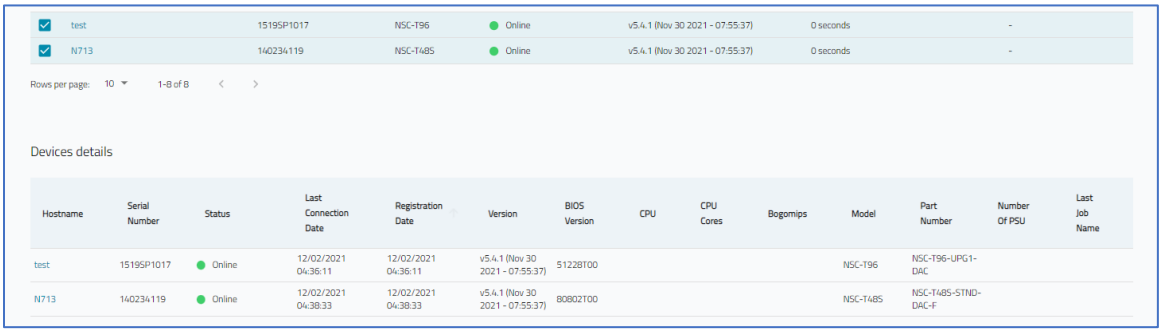
This opens the *Device Details* page with drop-downs that provide more information: *Device details*, *Device Status*, *IMEI*. Click **GO BACK** to return to *AVAILABLE* tab.



Select checkbox(s) on main table

At the bottom of the page, the Device details table is populated with information on selected checkbox(s).





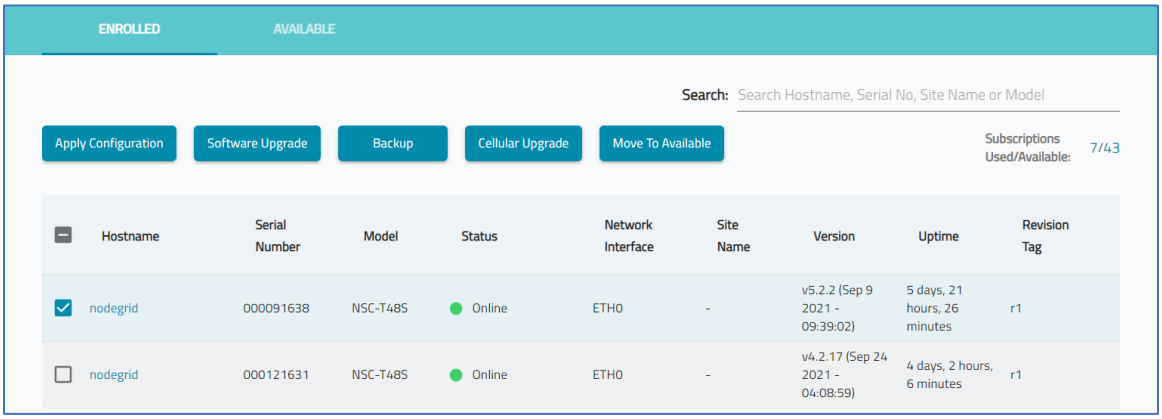
Devices details Table

Column Name	Description
Hostname	Hostname of the device.
Serial Number	Device serial number.
Status	Status of device: Online, Offline, Never Connected.
Last Connected Date	Date/time device last connected.
Registration Date	Date device registered on ZPE Cloud.
Version	Device version level.
BIOS Version	Device's current BIOS version.
CPU	CPU type and model.
CPU Cores	Number of CPU cores.
BogoMips	Measurement of CPU speed (rough estimation).
Model	Device model.
Part Number	Device part number.
Number of PSU	Number of power supply units.

Column Name	Description
Last Job Name	Name of the last Job on the device.
Last Job Status	Status of the last Job run on the device.
Last Backup	Date/time of last device backup.

ENROLLED tab

This lists all connected and approved devices as well as information related to hardware details, such as model, CPU, part number. Current software information such as version, uptime, and revision tag are also available. Other details are: first and last connection times, and the network interface connected to ZPE Cloud.



Device List Table

Column Name	Description
Hostname	Hostname of the device
Serial ID Number	Device serial number.
Model	Device model.
Status	Status: Online, Offline, Never Connected.
Network Interface	Device's network interface.
Site Name	Site device is assigned (Black if no site).
Version	Device version level.
Uptime	Current amount of time device is up.
Revision Tag	Revision number.

Column Name	Description
Backup Time	Date/time of last device backup.
Access	If active, lists two options to access the device: Web (WebUI), Console (CLI). If inactive, is grayed out.

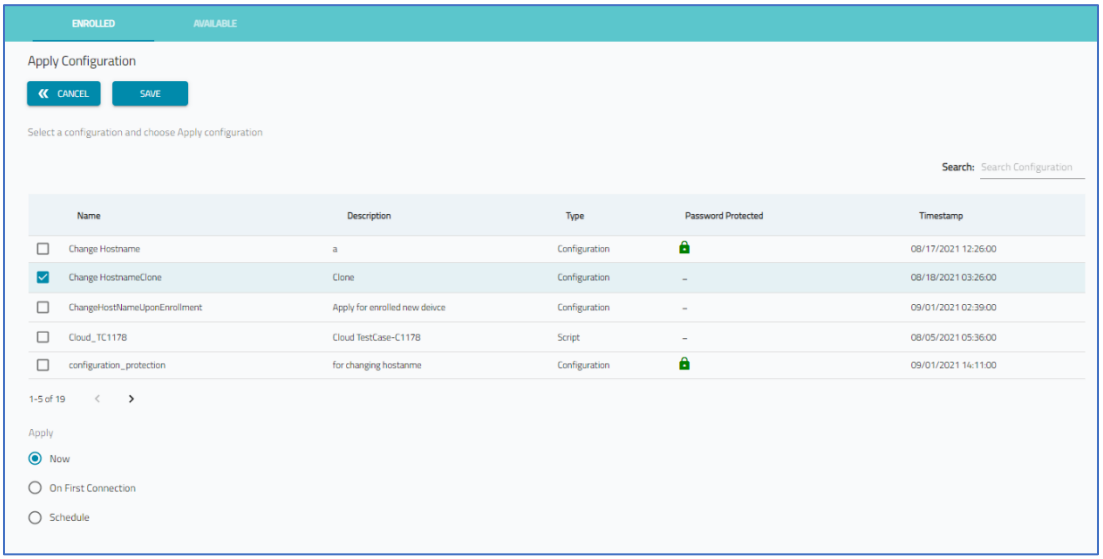
In the *Access* column, if the device is configured for remote access, click the **CONNECT** button and select the desired connection method (Web/Console).

The **Subscriptions Use/Available** (upper right) indicates number of current subscriptions.

Manage Enrollment

Apply Configuration

1. Go to *DEVICES :: ENROLLED*.
2. In the table, locate the device and select checkbox.
3. Click **APPLY CONFIGURATION** (displays dialog).

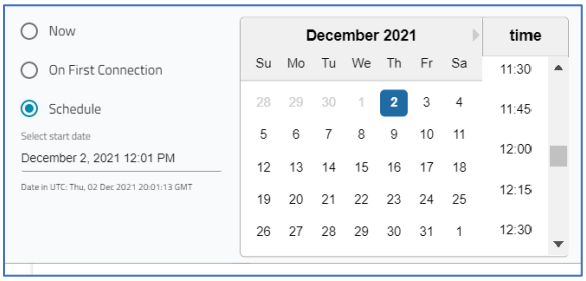


4. Locate the configuration (one or more) and select checkbox(es).
5. In the *Apply* menu, select one:

   Now radio button (when saved, operation executes immediately)

   On First Connection radio button (execute operation the first time the device(s) comes online)

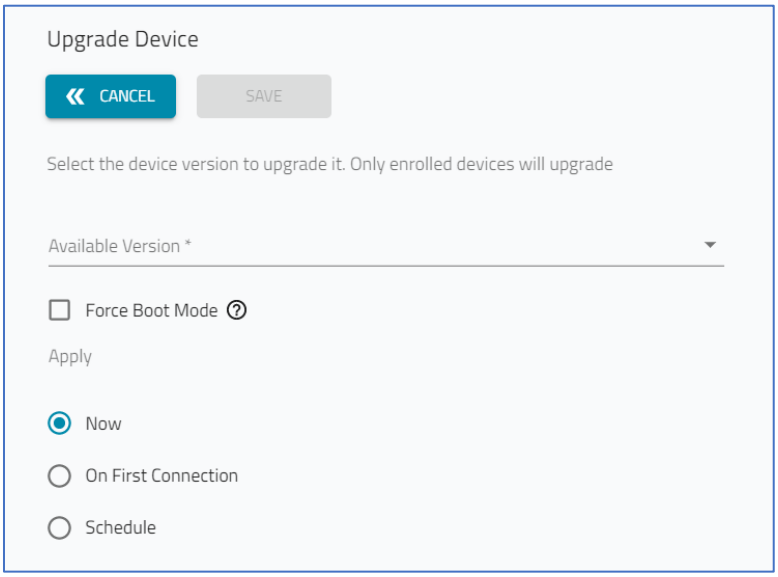
   Schedule radio button (if selected, choose a date/time to execute the operation)



6. Click **SAVE**.

Software Upgrade

1. Go to *DEVICES :: ENROLLED*.
2. In the table, locate the device and select checkbox.
3. Click **SOFTWARE UPGRADE** (displays dialog).



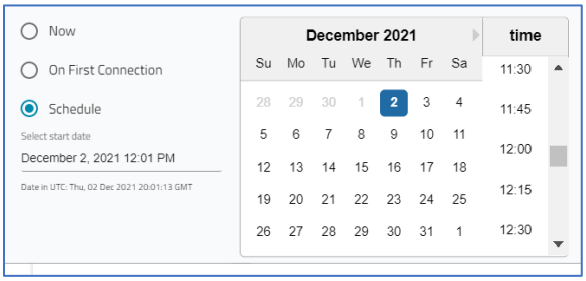
4. On the **Available Versions** drop-down, locate and select the version.

5. (optional) Select the **Force Boot Mode** checkbox (hover mouse pointer on ⓘ for information).
6. In the *Apply* menu, select one:

   Now radio button (when saved, operation executes immediately)

On First Connection radio button (execute operation the first time the device(s) comes online)

Schedule radio button (if selected, choose a date/time to execute the operation)

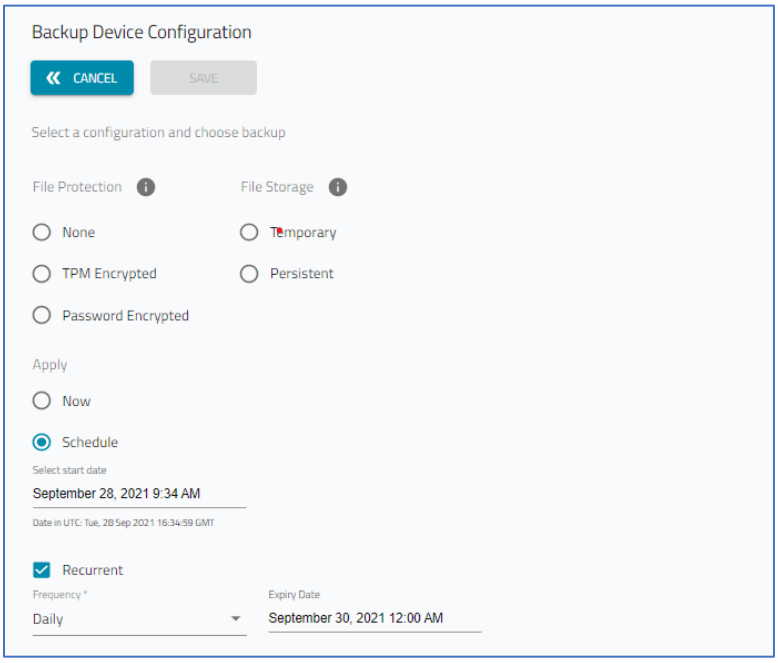


7. Click **SAVE**.

Backup Device

NOTE: The Backup operation requires Nodegrid version 4.1.9 or higher. The Cellular upgrade operation requires version 4.2 or higher.

1. Go to *DEVICES :: ENROLLED*.
2. In the table, locate the device(s) and select checkbox(es).
3. Click **BACKUP** (displays dialog).



4. On *File Protection* menu, select one:

None radio button (Without encryption – backup file sent to ZPE Cloud without encryption. File can be downloaded and applied to a device through Nodegrid Manager.)

TPM Encrypted radio button (TPM encrypted file (backup file is encrypted and sent to ZPE Cloud. File can only be decrypted with the same hardware that encrypted it.)

Password encrypted radio button (backup file is sent to ZPE Cloud encrypted – saved on Nodegrid device under ZPE CLOUD SETTINGS :: ENABLE FILE PROTECTION with openssl. Password must be known to decrypt the backup file when downloaded from ZPE Cloud.)

5. On the *File Storage* menu, select one.

   NOTE: On ZPE Cloud, each device may have a maximum of five backups. At that limit, one or more backups must be deleted. There are two storage options available:

   Temporary radio button (on a new backup request with five backups slots filled, the oldest backup is deleted)

   Persistent radio button (not automatically deleted). When backup slots are full, the user must manually select the backup to be deleted.)

6. On the *Apply* menu:

   Now radio button (backup is made immediately)

   Schedule radio button (expands for additional conditions)

   For **Select start date**, click in date (displays calendar/time) and choose date/time.

   On the **Frequency** drop-down men, select one (**Hourly**, **Daily**, **Weekly**, **Monthly**).

   On **Expiry Date**, click in date and choose date/time from the pop-up calendar.

   On **Recurrent** checkbox, selection:

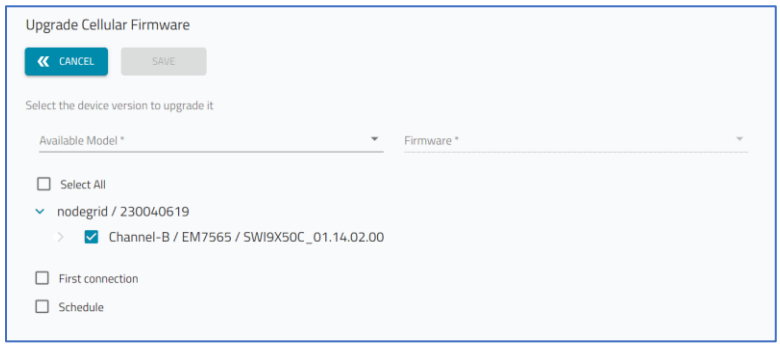
   On **Frequency** drop-down, select one (**Hourly**, **Daily**, **Weekly**, **Monthly**).

   On **Expiry** drop-down, select date.

7. Click **SAVE**.

Cellular Upgrade

1. Go to *DEVICES :: ENROLLED*.
2. In the table, locate the device(s) and select checkbox(es).
3. Click **CELLULAR UPGRADE** (displays dialog).



4. On the **Available Model** drop-down, select one.
5. On the **Firmware** drop-down, select one.
6. (as needed) If **Select All** checkbox is selected, all cellular units are upgraded. Alternatively, select one version on the device drop-down.
7. If **First connection** checkbox is selected, the upgrade occurs when the device next connects to the Cloud (**Schedule** is disabled).
8. If **Schedule** checkbox is selected, select date/time on the pop-up calendar.
9. Click **SAVE**.

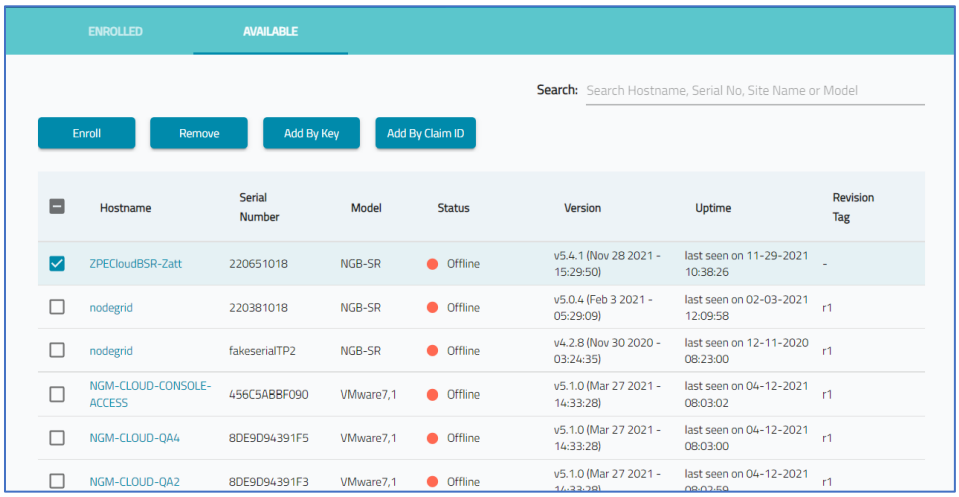
Move to Available

1. Go to *DEVICES :: ENROLLED*.
2. In the table, locate the device(s) and select checkbox(es).
3. Click **MOVE TO AVAILABLE**.

   The selected device is moved to the *AVAILABLE* tab.

AVAILABLE tab

Devices transferred to a company account need to be approved before they become available for operations. The Device listing and Devices Details tables on this tab are the same as on the *ENROLLED* tab.



Manage Available Devices

Enroll Device

When a device is moved from **Available** to **Enrolled**, the default scripts and configurations are applied. If a device is Unenrolled and moves to Available, the next time it is enrolled, a prompt asks whether to re-apply the default configuration.

1. Go to *DEVICES :: AVAILABLE*.
2. In the table, locate the device(s) and select checkbox(es).
3. Click **ENROLL**.

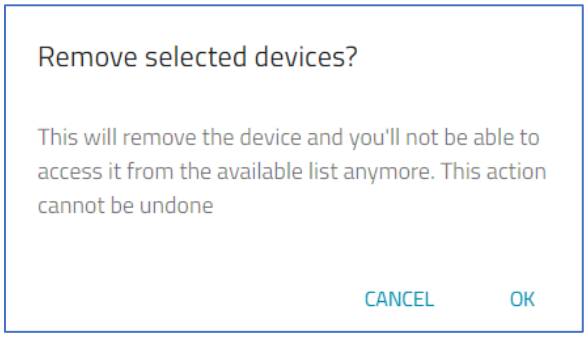
When the enrollment is completed, the device is moved to the *ENROLLED* tab.

> **NOTE**: Devices in *Available* status do not receive data (cellular, application, connection status, etc.).

Remove Device

> **WARNING**: Perform this procedure only for devices that are malfunctioning or to exclude from availability.

1. Go to *DEVICES :: AVAILABLE*.
2. Select checkbox(s) next to devices to be removed.
3. Click **REMOVE** (displays dialog).



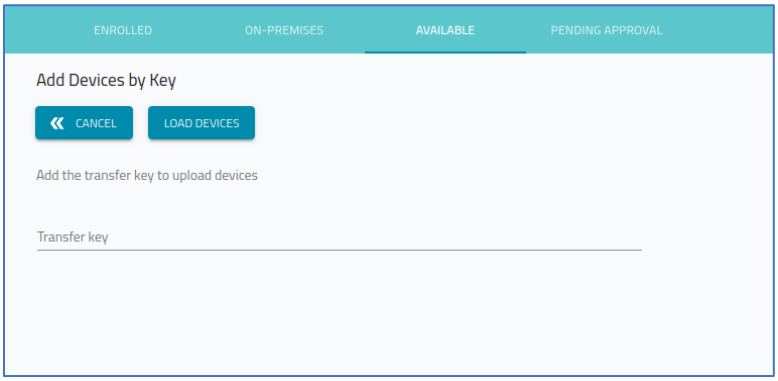
4. Click **OK**.

Add by Key

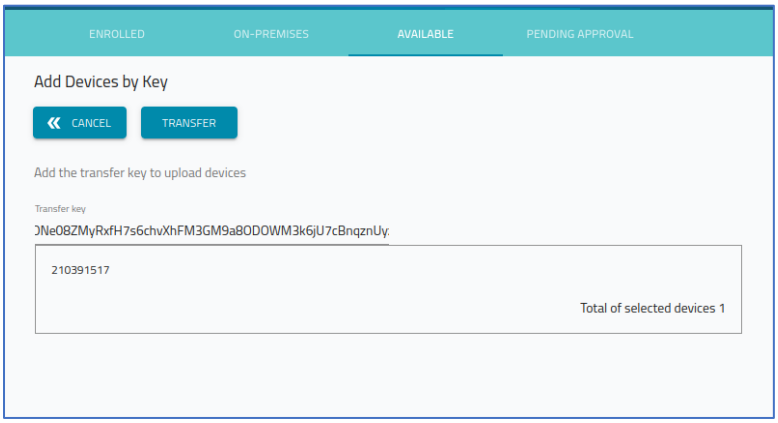
When a new device order is sent, the notification email includes this Transfer Key. This key can be used to import the device to ZPE Cloud.

> **NOTE**: Devices already registered block Transfer of Ownership requests. If attempted, this notification is presented: "Failed to transfer ownership. Device already under Company account."

1. Go to *DEVICES :: AVAILABLE*.
2. Click **ADD BY KEY** (displays dialog).



3. Enter the **Transfer Key**.
4. Click **LOAD DEVICES** (displays dialog). Confirm the list is correct.



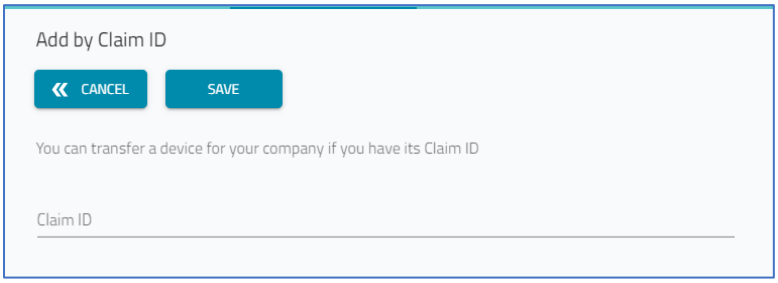
5. Click **TRANSFER**.

The devices on the list are added to the *AVAILABLE* tab.

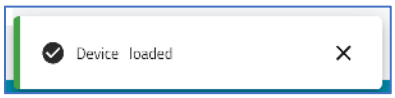
Add by Claim ID

This option imports devices with the Device's Claim ID. A device can only be claimed once. The device must be on the AVAILABLE page. If needed, contact support@zpesystems.com.

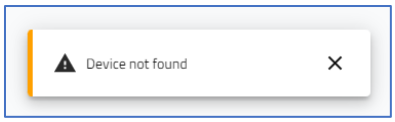
1. Go to *DEVICES :: AVAILABLE*.
2. Click **ADD BY CLAIM ID** (displays dialog).



3. Enter the **Claim ID**.
4. Click **SAVE** (displays success pop-up dialog).



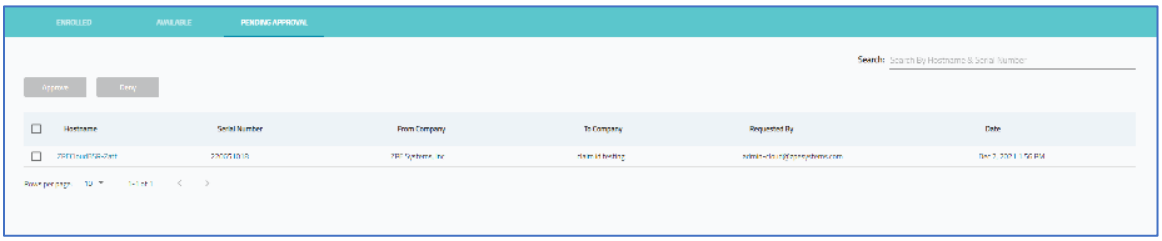
NOTE: If incorrect, this dialog displays.



PENDING APPROVAL tab

NOTE: This only appears if there is a device in "Transfer-pending approval" state.

When ZPE Systems transfers device ownership between companies, the Company Admin associated with the device must approve the transaction.



Manage Device Transfer

Approve a Device Transfer:

1. Go to *DEVICES :: PENDING APROVAL*.
2. In the table, locate the device and select checkbox.

   There are two options on the transfer request:

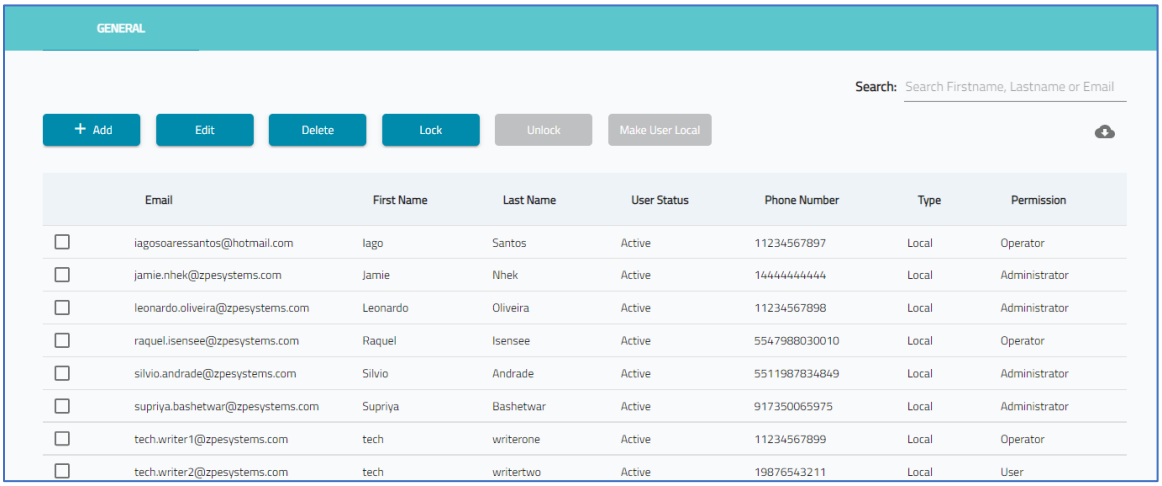
   APPROVE

   DENY
3. To complete the transfer, click **Approve**.

USERS Section

Access and connected accounts are managed under the USERS tab. Users can be added, edited, and removed.

GENERAL tab



Manage Users

User Types

There are two types of users:

Local

Users who are created locally on ZPE Cloud and can access the cloud service via a password.

Remote

Users created automatically with the SSO by Domain option (see "Single Sign On (SSO) by Domain"). These users may only login via domain because no local password is configured.

Permission Levels

There are three permission levels available to users.

Administrator

Manages all devices, company credentials, and users within their company.

Operator

Performs and creates operations within all devices assigned to their group

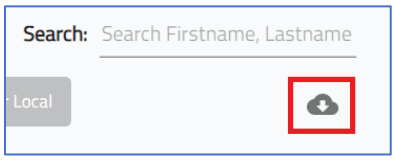
User

Can only access devices within their group.

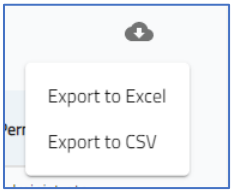
Export User Listing

The user listing can be exported.

1. Go to *USERS :: GENERAL*.
2. On the upper right, click the **Cloud** icon.



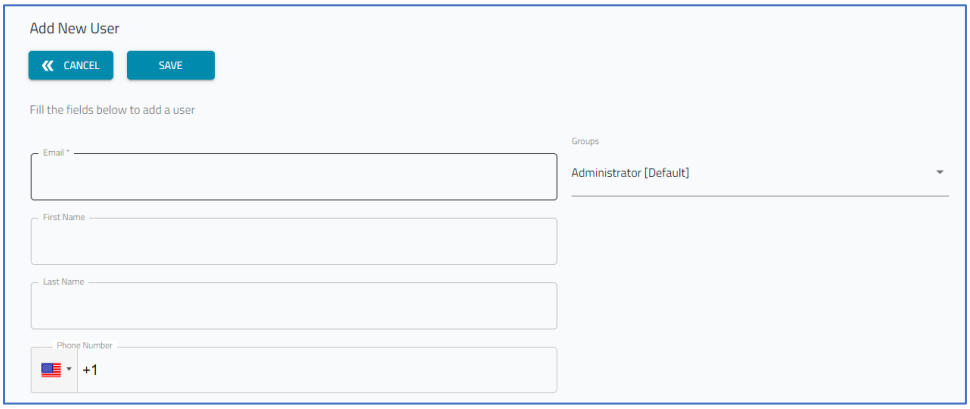
3. On the drop-down listing, select the file format (**Export to Excel**, **Export to CSV**).



4. The file is saved in the local default *Download* folder.

Add a User

1. Go to *USERS :: GENERAL*.
2. Click **+ADD** (displays dialog).

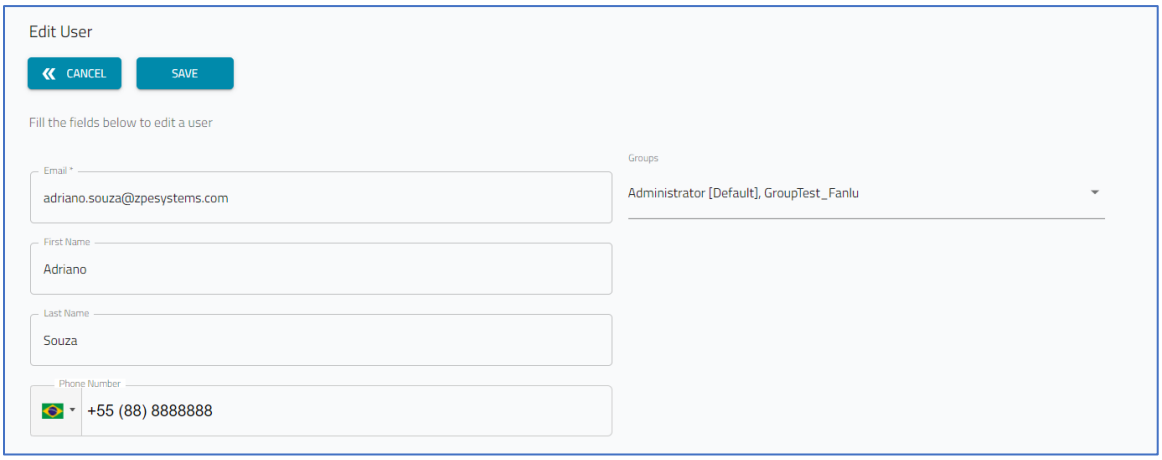


3. Enter **Email**.
4. Enter **First name**.
5. Enter **Last name**.
6. Enter **Phone number**.
7. On **Groups** drop-down, select one.
8. Click **SAVE**.

The new user is sent an email with instructions.

Edit a User

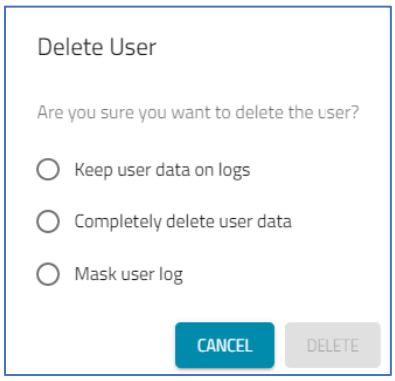
1. Go to *USERS :: GENERAL*.
2. In the table, locate the user and select checkbox.
3. Click **EDIT** (displays dialog).



4. Make changes, as needed.
5. Click **SAVE**.

Delete a User

1. Go to *USERS :: GENERAL*.
2. In the table, locate the user and select checkbox.
3. Click **DELETE** (displays dialog).



4. Select one:

   Keep user data on logs radio button

   Colmpletely delete user data radio button

   Mask user logs radio button

5. Click **DELETE**.

Lock a User

This disables the user account.

1. Go to *USERS :: GENERAL*.
2. In the table, locate the user and select checkbox.
3. Click **LOCK**.

If the account needs to be reactivated, it's only necessary to select it and click the **UNLOCK** button.

Unlock a User

This reactivates the Locked user account.

1. Go to *USERS :: GENERAL*.
2. In the table, locate the locked user and select checkbox.
3. Click **UNLOCK**.

Convert Remote users to Local users

1. Go to *USERS :: GENERAL*.
2. On the listing, select checkbox of Remote user.

3. Click **MAKE USER LOCAL**.

Each user is sent an email that includes a link to create a new ZPE Cloud password.

PROFILES Section

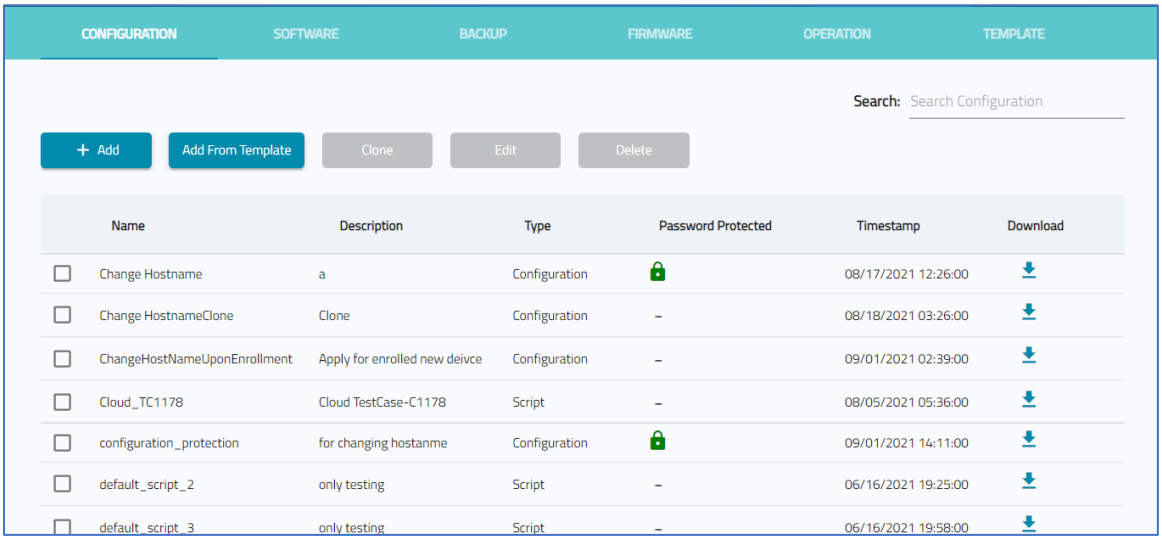
Profiles are managed in this section. This includes configurations, custom scripts, software versions, backup entries, and cellular firmware versions.

CONFIGURATION tab

Device configuration files can be updated in two ways:

Console (CLI) – use save_settings command.

WebUI – go to *System :: Toolkit :: Save Settings*.



Configuration Table Columns

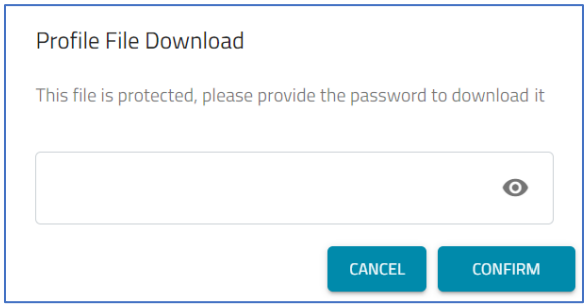
Column Name	Description
Name	Name of the configuration/script.
Description	Description of the configuration/script.
Type	File is a configuration or script.
Password Protected	Icon indicates if file is locked or unlocked.
Timestamp	Date/time the configuration/script was created.
Download	Downloads the file.

Manage Configuration/Script

Download Configuration/Script

1. Go to *PROFILES :: CONFIGURATION*.
2. Locate configuration/script.
3. On *Download* column, click **Download** icon.

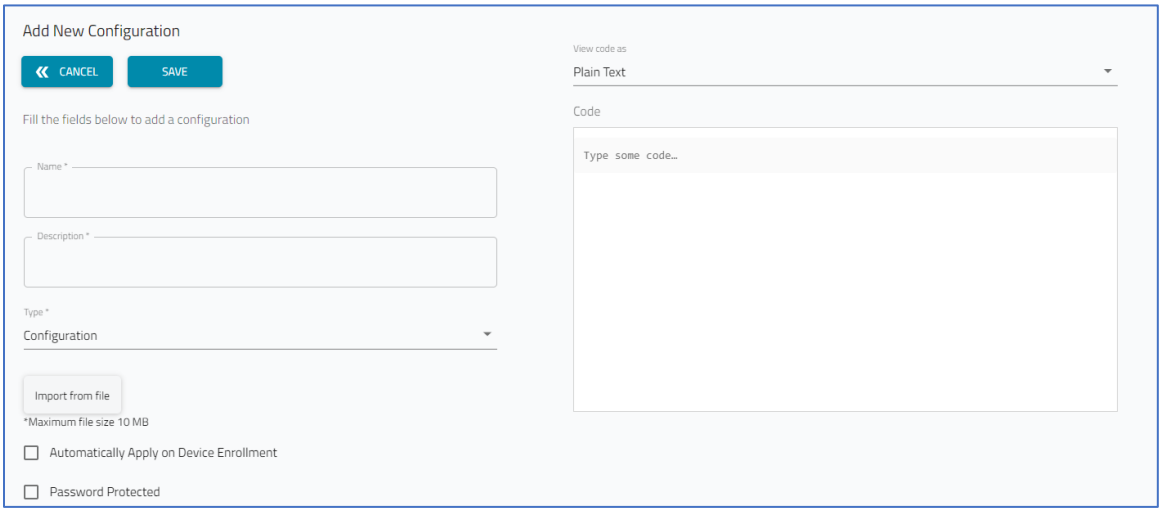
   If password protected, on the *Profile File Download* dialog, enter **Password** and click **CONFIRM**.



4. File is saved on the local computer's Download location.

Add a new Configuration/Script

1. Go to *PROFILES :: CONFIGURATION*.
2. Click **+ADD** (displays dialog).



3. Enter **Name**.
4. Enter **Description**.
5. On the **Configuration** drop-down, select one (**Configuration**, **Script**);
6. (as needed) Click **Import from file**. and select the file.

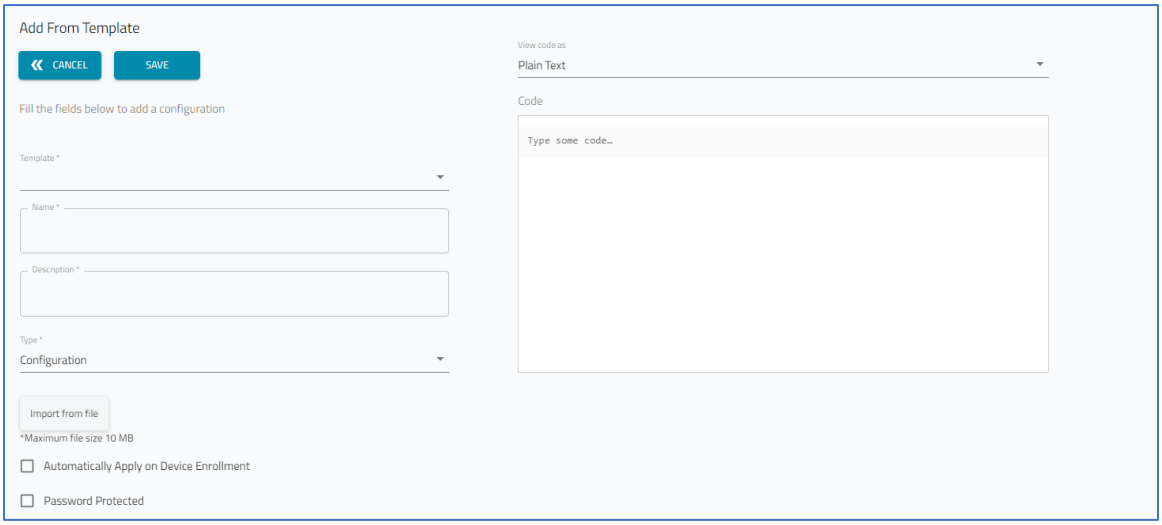
7. (optional) Select **Automatically apply on device enrollment** checkbox (if selected, configuration is applied when the device is enrolled).
8. (optional) Select **Password Protected** checkbox. Enter **Password**.
9. (optional) Select **Default** checkbox (applies this profile to all enrolled devices).

   (optional) In **View Code as** textbox, select type of code (**Plain Text**, **Shell**, **Python**, **Javascript/Node JS**).

   In the textbox, paste the lines of code.
10. Click **SAVE**.

Add Configuration from Template

1. Go to *PROFILES :: CONFIGURATION*.
2. Click **ADD FROM TEMPLATE** (displays dialog).

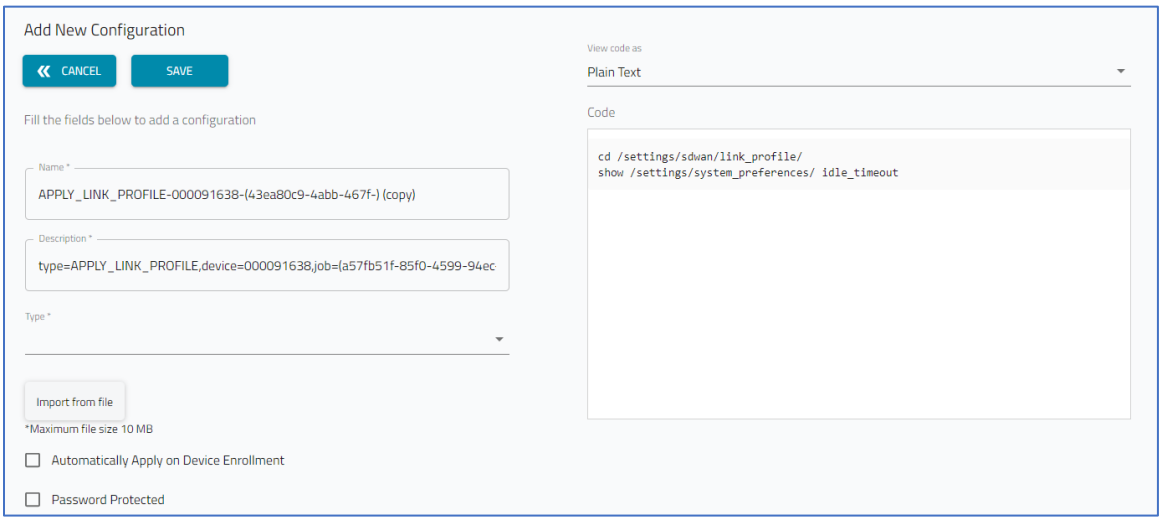


3. In **Template** drop-down, select one.
4. Enter **Name**.
5. Enter **Description**.
6. On **Type** drop-down, select one (**Configuration**, **Script**).
7. (as needed) Click **Import from file** (on dialog, locate and select the file).
8. (optional) Select **Automatically Apply on Device Enrollment** checkbox.

   (optional) Select **Password Protected** checkbox. Enter **Password**.
9. On **View Code As** drop-down, select one (**Plain Text**, **Shell**, **Python**, **Javascript/Node.js**).
10. In **Code** textbox, review code (modify as needed).
11. Click **SAVE**.

Clone a Configuration

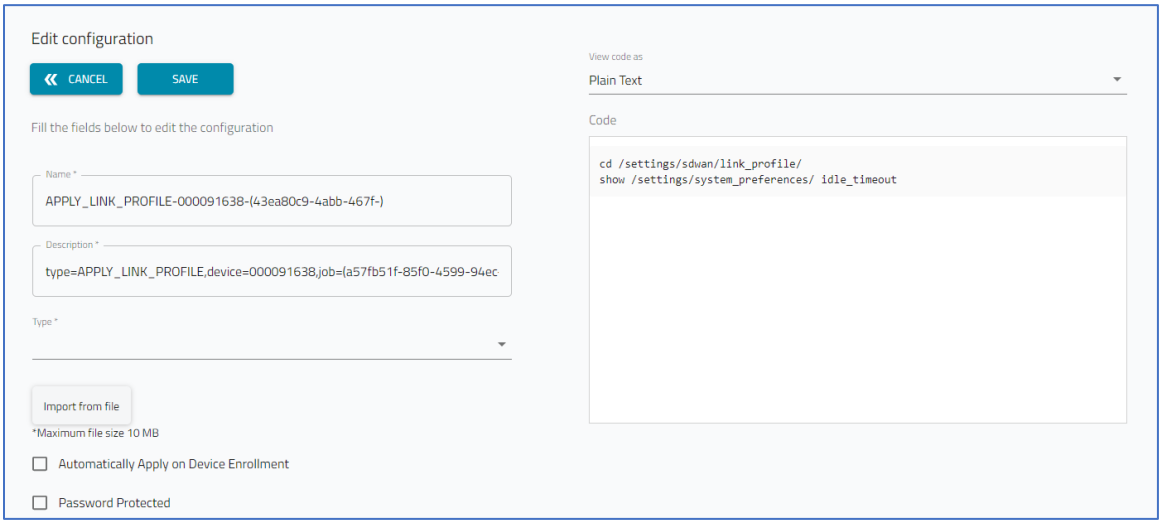
1. Go to *PROFILES :: CONFIGURATION*.
2. In the table, locate profile and select checkbox.
3. Click **CLONE** (displays dialog).



4. Change **Name**.
5. Make other modifications, as needed.
6. Click **SAVE**.

Edit a Configuration

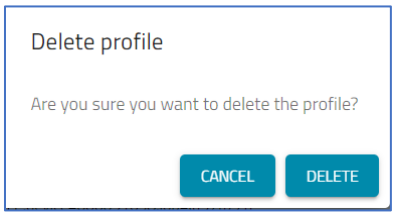
1. Go to *PROFILES :: CONFIGURATION*.
2. In the table, locate profile and select checkbox.
3. Click **EDIT** (displays dialog).



4. Make changes, as needed.
5. Click **SAVE**.

Delete a Configuration

1. Go to *PROFILES :: CONFIGURATION*.
2. In the table, locate profile and select checkbox.
3. Click **DELETE** (displays dialog).

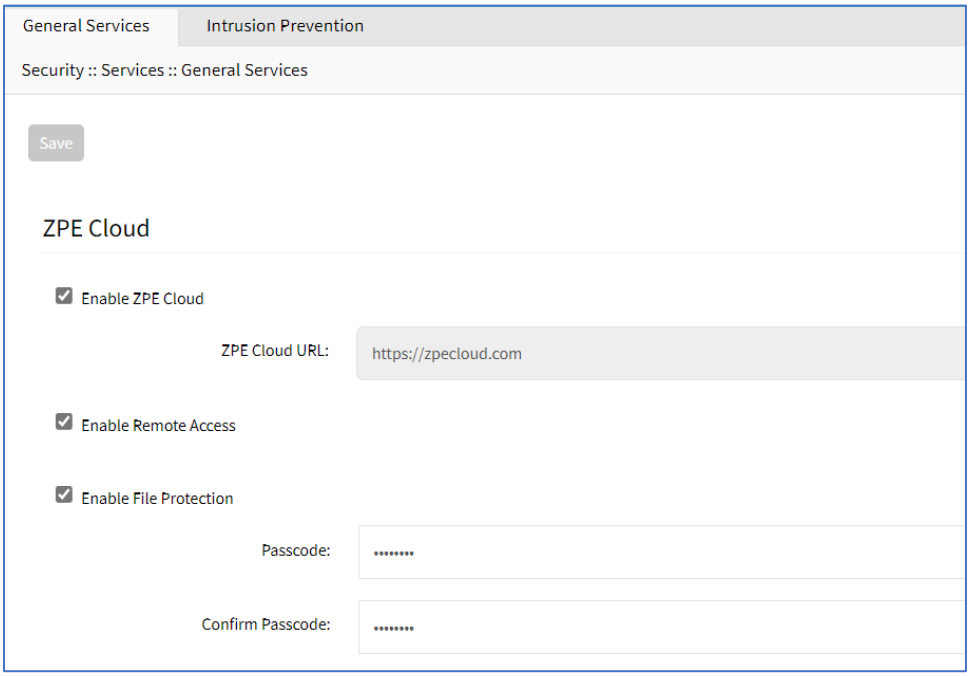


4. On the confirmation dialog, click **DELETE**.

Enable Password Protection on the Configuration/Script File

If password-protected, the file is only installed on the device(s) configured with the matching password.

1. Log into the device and go to *Security :: Services :: General Services*.
2. In the *ZPE Cloud* menu, review the **Enable File Protection** checkbox.
3. If selected, must include the **Passcode** and **Confirm Passcode** (must match the password in the *Add New Configuration* dialog).



Encrypt Configuration Files

Before upload to ZPE Cloud, configuration/script files can be encrypted. The file can only be installed if the Nodegrid device settings are correctly enabled.

1. Log into the Nodegrid device.
2. Go to *Security :: Services :: ZPE Cloud*.
3. Select **Enable File Protection** checkbox and enter **Passcode**.
4. Select **Enable File Encryption** checkbox.
5. Click **Save**.

Encryption Requirements

To add extra security to the file encryption process, the following openssl features must be enabled:

Cipher: aes-256-cbc

Encoding: base64

Salted: yes

Key Digest Algorithm: sha256

Requirements

Openssl version :: 1.1.0

Before upload to ZPE Cloud; Files (CLI commands, custom scripts and save_config tarball) can be encrypted externally or on the Nodegrid device.

OS Encryption

Nodegrid OS Encryption

Requirements

Nodegrid version >= 4.1

Openssl 1.1.1

To encrypt a file using Nodegrid, enter:

```
openssl aes-256-cbc -base64 -salt -md sha256 -in <input_file> -out <encrypted_file>
```

To encrypt the file, openssl asks for the password. Alternatively, instead of entering at the prompts, use **– k**, followed by the password flag.

Linux OS Encryption

Requirements

Openssl 1.1.0

To install on Ubuntu machines, enter:

```
sudo apt-get install libssl-dev
```

To encrypt the file using Linux, enter:

```
openssl aes-256-cbc -base64 -salt -md sha256 -in <input_file> -out <encrypted_file>
```

To encrypt the file, openssl asks for the password. Alternatively, instead of entering at the prompts, use **– k**, followed by the password flag.

Mac OS Encryption

Requirements

Openssl >= 1.1.0

On Mac OS, install Brew. Follow the steps at https://brew.sh/

After Brew is installed, to install openssl, enter:

```
brew install openssl
brew link --force openssl
```

To encrypt the file on Mac OS, enter:

```
openssl aes-256-cbc -base64 -salt -md sha256 -in <input_file> -out <encrypted_file>
```

To encrypt the file, openssl asks for the password. Alternatively, instead of entering at the prompts, use **– k**, followed by the password flag.

Windows OS Encryption

Requirements

Openssl >= 1.1.0

Openssl can be installed on Windows via the binary installer. For more information, please see the Openssl Wiki.

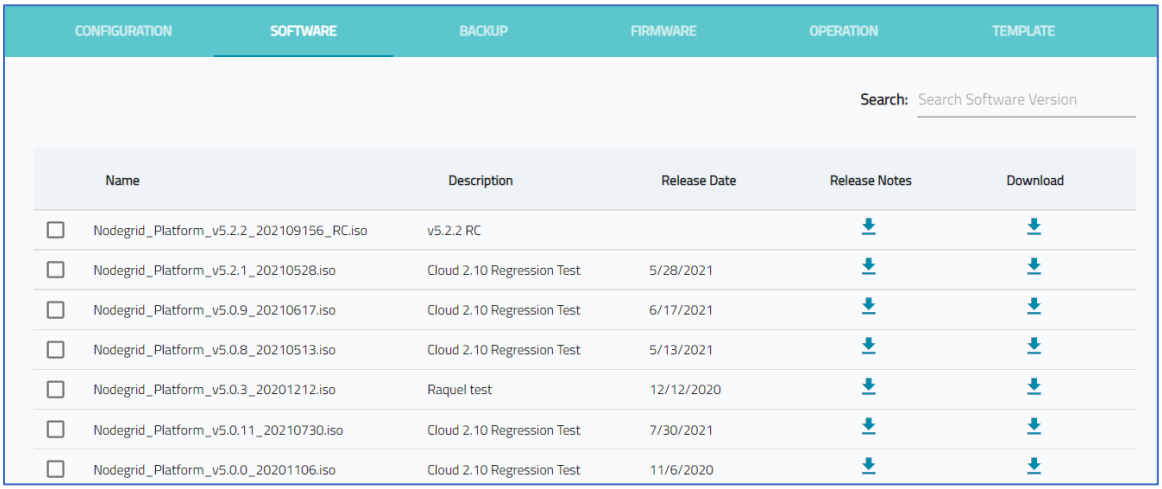
To encrypt the file using Windows, use the following command:

```
openssl aes-256-cbc -base64 -salt -md sha256 -in <input_file> -out <encrypted_file>
```

To encrypt the file, openssl asks for the password. Alternatively, instead of entering at the prompts, use **– k**, followed by the password flag.

SOFTWARE tab

This lists all available software images. The images can be downloaded, as needed. The image's release notes can also be downloaded.



Software Table Columns

Column Name	Description
Name	Name of the software image.
Description	Description of image.
Release Date	Date of release for this image.
Release Notes	Link to release notes of the image.
Download	Link to download of the image.

Software Options

Download Release Notes

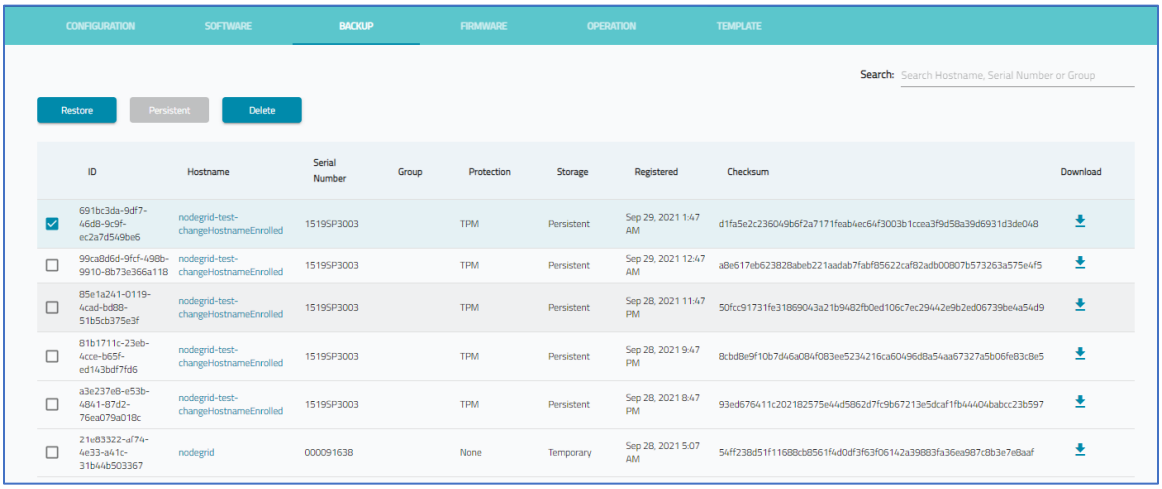
1. Go to *PROFILES :: SOFTWARE*.
2. In the table, locate software.
3. In the *Release Notes* column, click the **Download** icon.
4. The file is downloaded to the local computer's download location.

Download Software

1. Go to *PROFILES :: SOFTWARE*.
2. In the table, locate software.
3. In the *Download* column, click the **Download** icon.
4. The file is downloaded to the local computer's download location.

BACKUP tab

This page displays backup images of devices. Images can be managed, and devices restored. Backups are done on the DEVICES section.



NOTE: The BACKUP button is disabled for devices that do not support this feature. If multiple devices are selected and one or more of them does not support this feature, a log message about the failure is displayed.

Backup Table Columns

Column Name	Description
ID	Name of the software image.
Hostname	Hostname of the device which was backed up.
Serial Number	Device serial number
Group	Assigned to which Group.
Protection	Type of protection (password, TPE)
Storage	Type of storage for the backup (Persistent, Temporary) .
Registered	Date/time of backup.
Checksum	The checksum calculation.
Download	Click icon to download the backup file.

Manage Backups

Restore a Backup

1. Go to *PROFILES :: BACKUP*.

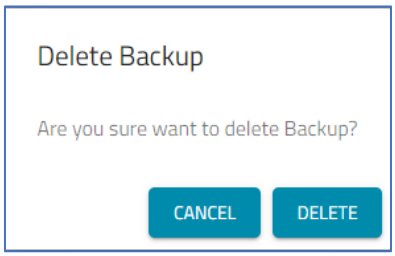
2. Locate and select the checkbox of the backup.
3. Click **RESTORE**.
4. Wait for the process to complete.

Change Backup from Temporary to Persistent

1. Go to *PROFILES :: BACKUP*.
2. Locate and select the checkbox of the backup in *Temporary* status.
3. Click **PERSISTENT**.

Delete a Backup

1. Go to *PROFILES :: BACKUP*.
2. Locate and select the checkbox of the backup.
3. Click **DELETE** (displays dialog).



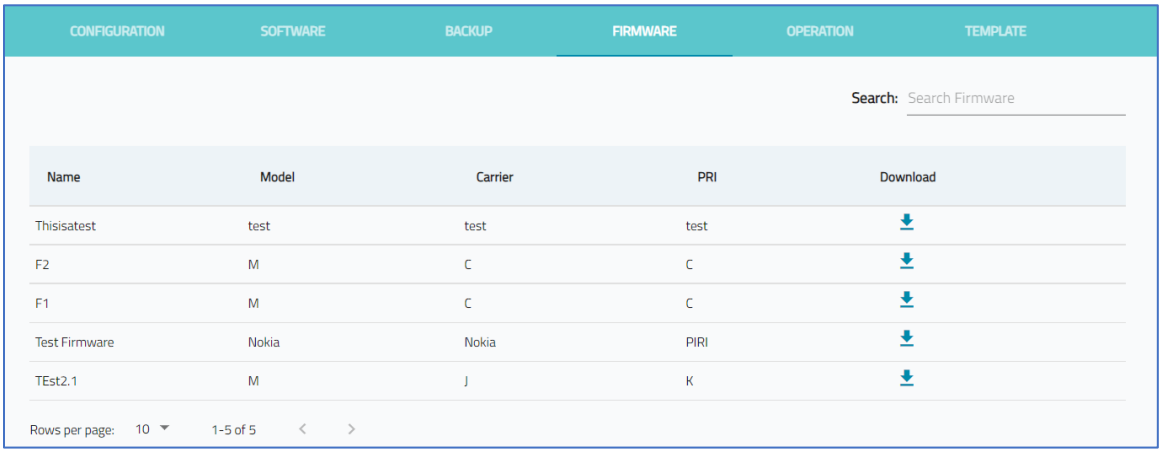
4. On the *Delete Backup* pop-up dialog, click **DELETE**.

Download Backup

1. Go to *PROFILES :: BACKUP*.
2. In the table, locate the backup.
3. In the *Download* column, click the **Download** icon.
4. The file is downloaded to the local file location.

FIRMWARE tab

The FIRMWARE page displays all available cellular modem firmware. The file can be downloaded.



NOTE: For unsupported devices, Cellular Upgrade is disabled. If multiple devices are selected, unsupported devices display a (Not supported) label next to the name.

Firmware Table Columns

Column Name	Description
Name	Name of the firmware
Model	Model for the firmware
Carrier	Carrier of the firmware.
PRI	.Primary Rate Interface
Download	Click icon to download the firmware package.

Manage Firmware

Download Firmware

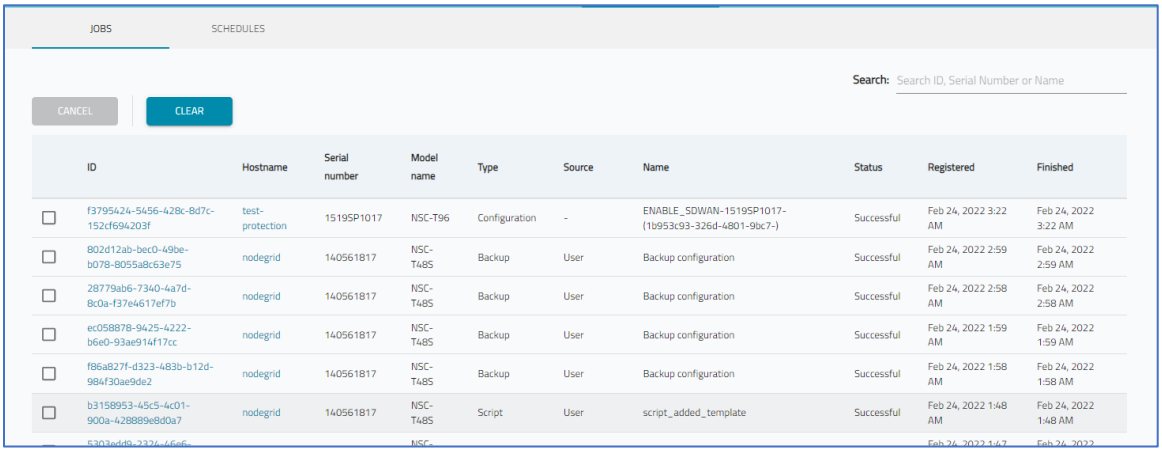
1. Go to *PROFILES :: FIRMWARE*.
2. In the table, locate firmware.
3. In the *Download* column, click the **Download** icon.
4. The file is downloaded to the local file location.

OPERATION tab

Every operation including CONFIGURATION, SCRIPT, UPGRADE, and BACKUP is registered under ZPE Cloud with a unique ID for all cases where they're scheduled or applied right away. On the OPERATION tab, job details are available.

JOBS sub-tab

This page shows current job operations.

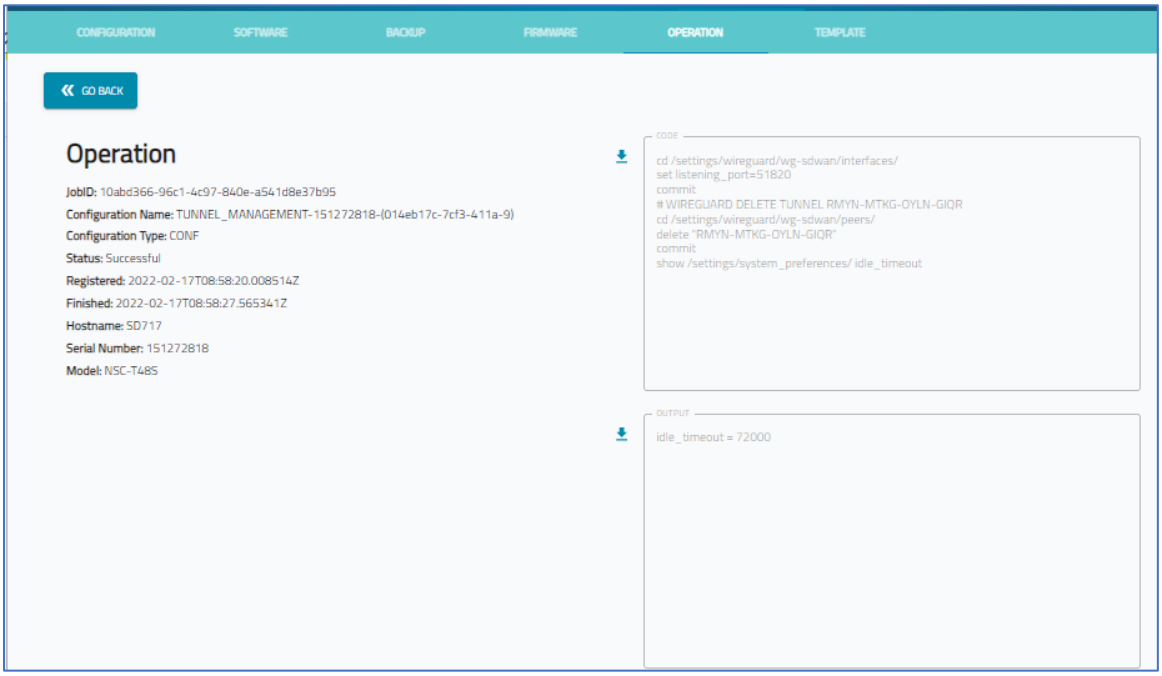


Jobs Table Columns

Column Name	Description
ID	Job ID.
Hostname	Hostname of device.
Serial Number	Serial number of device.
Model Name	Model name of device.
Type	Type of job: Script, Configuration.
Source	Source that initiated the job.
Name	Name of script/configuration.
Status	Status of the job: Scheduled, Started, Successful, Failed.
Registered	Date/time job was registered.
Finished	Date/time job was finished.

Download Results from a Job

1. Go to *PROFILES :: OPERATION :: JOBS.*
2. Click on a Job ID (opens *OPERATION* dialog).



3. .To download the *CODE*, click the **Download** icon.
4. To download the *OUTPUT*, click the **Download** icon.

Cancel Job

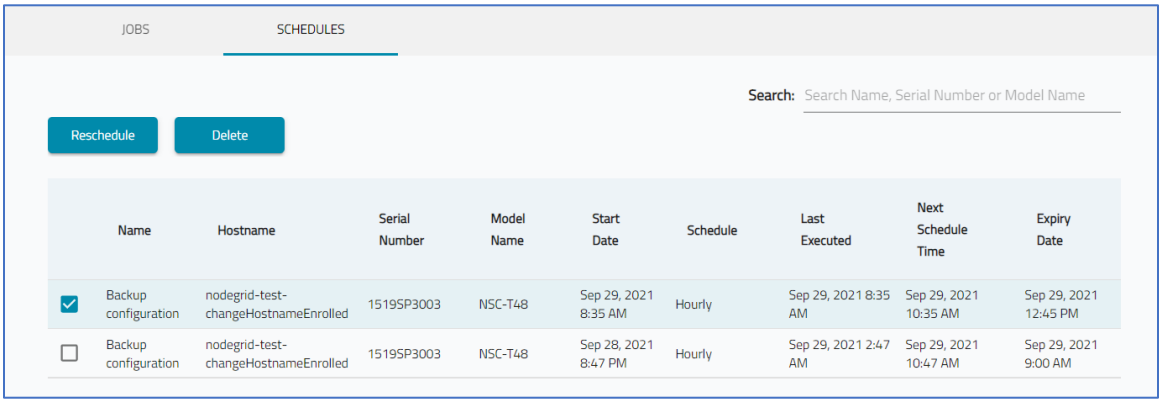
1. Go to *PROFILES :: OPERATION :: JOBS.*
2. Locate and select the checkbox of the job.
3. Click **CANCEL**.

Clear Job

1. Go to *PROFILES :: OPERATION :: JOBS.*
2. Locate and select the checkbox of the job.
3. Click **CLEAR**.

SCHEDULES sub-tab

This page shows scheduled jobs.

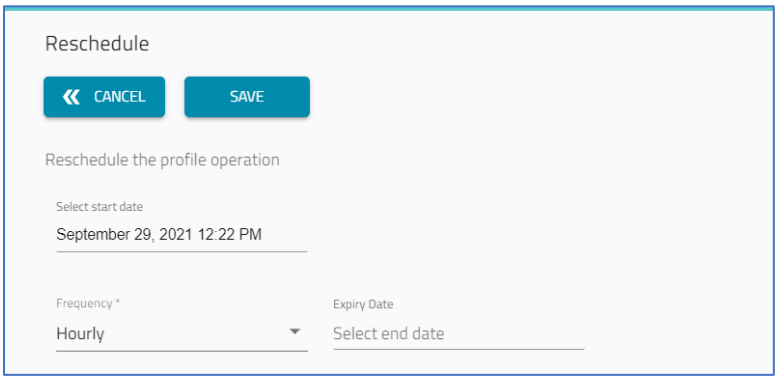


Schedules Table Columns

Column Name	Description
Name	Name of the job.
Hostname	Hostname of the device.
Serial Number	Serial number of the device.
Model Name	Model name of the device.
Start Date	Start date/time of job.
Scheduled	How often job is run:
Last Executed	Date/time job was last run.
Next Schedule Time	Date/time of the next start.
Expiry Date	Date the job stops running.

Reschedule Job

1. Go to *PROFILES :: OPERATION :: SCHEDULES.*
2. Locate and select the checkbox of the job.
3. Click **RESCHEDULE** (displays dialog).



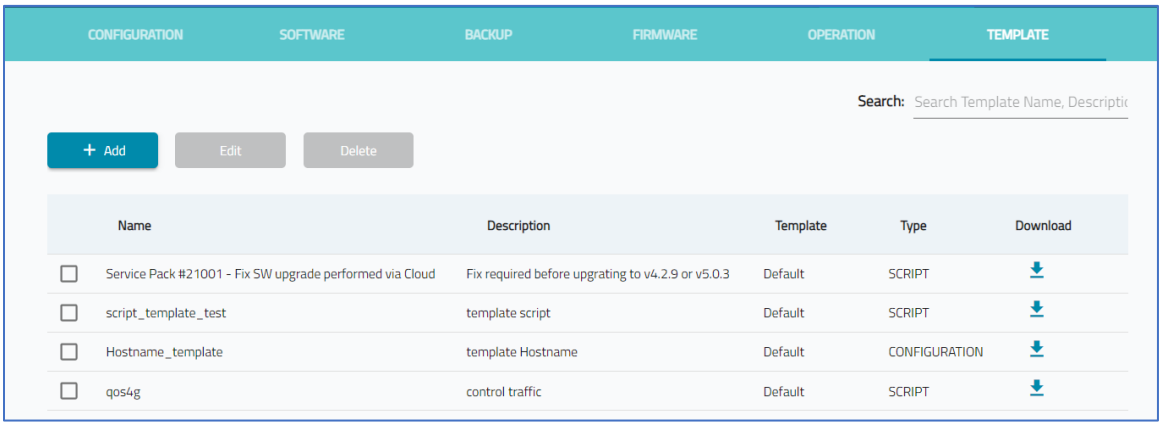
4. On **Select Start Date**, chose the date/time.
5. On **Frequency** drop-down, select one (**Hourly**, **Daily**, **Weekly**, **Monthly**).
6. On **Expiry Date**, chose the date/time.
7. Click **SAVE**.

Cancel Job

1. Go to *PROFILES :: OPERATION :: SCHEDULES.*
2. Locate and select the checkbox of the job.
3. Click **CANCEL**.

TEMPLATE tab

This page lists current templates and can create custom scripts and configurations. Click the **Download** icon to copy the file.



Template Table Columns

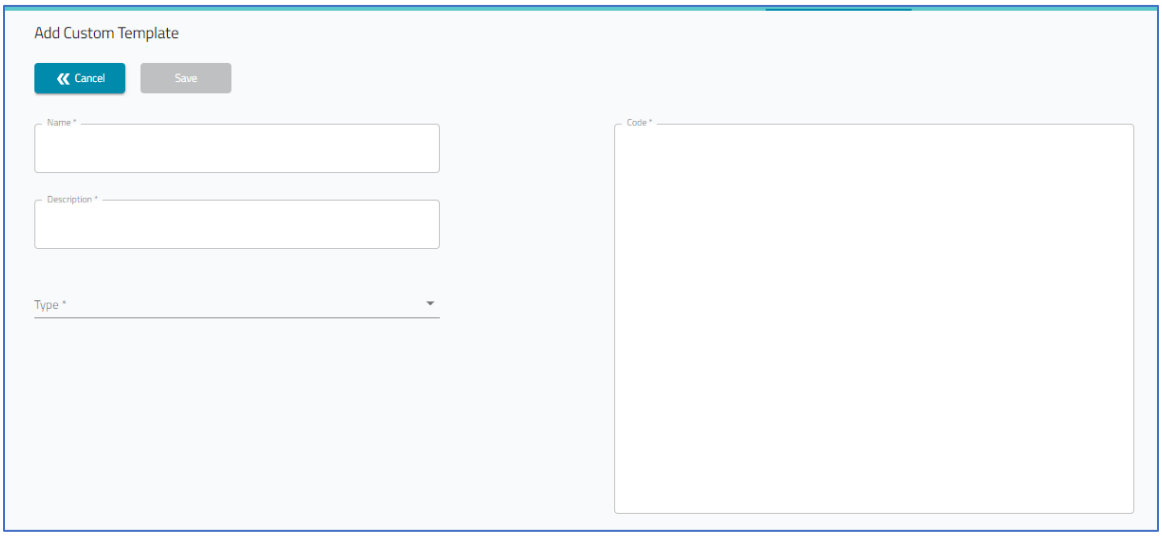
Column Name	Description
Name	Name of the template.
Description	Description of the template.

Column Name	Description
Template	Purpose of template (Custom, Default).
Type	Type of template (Configuration, Script).
Download	Download the template.

Manage Templates

Add a New Template

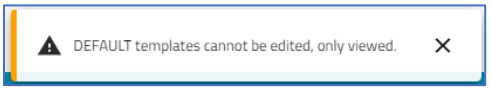
1. Go to *PROFILES :: TEMPLATE.*
2. Click **+ADD** (displays dialog).



3. Enter **Name**.
4. Enter **Description**.
5. On **Type** drop-down, select one (**Configuration**, **Script**).
6. In **Code** text box, enter the needed code.
7. Click **SAVE**.

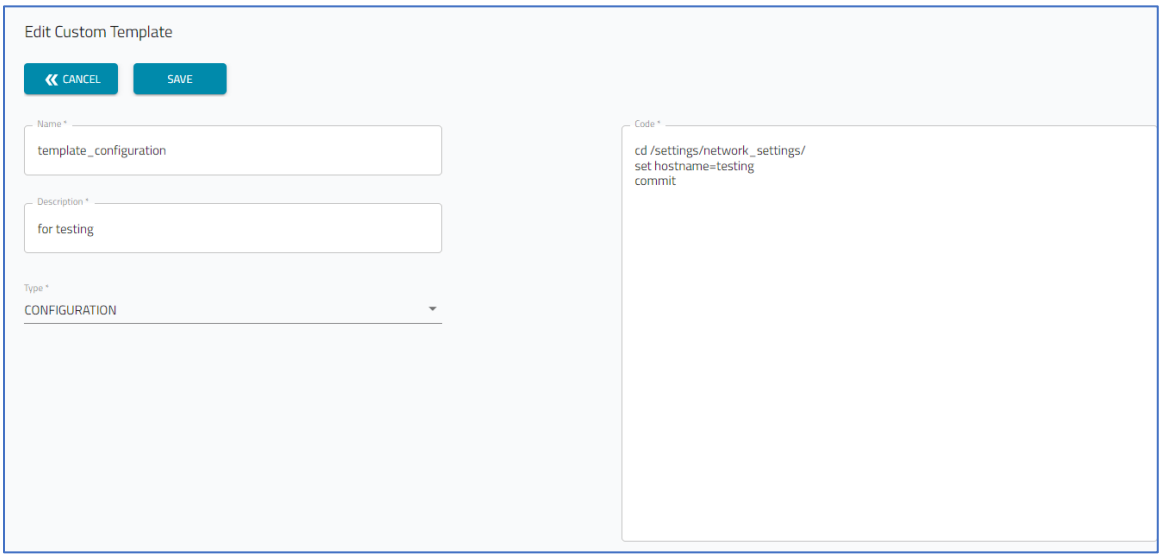
Edit a Template

NOTE: Default templates cannot be edited. An attempt to edit displays pop-up dialog (lower right).



1. Go to *PROFILES :: TEMPLATE.*
2. Locate the template and select the checkbox.

3. Click **EDIT** (displays dialog).

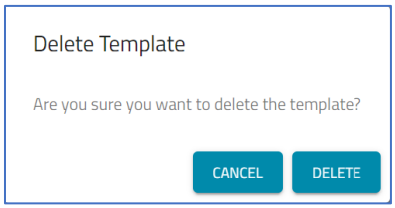


4. Make changes, as needed.
5. Click **SAVE**.

   NOTE: Templates created by a Super Admin may only be viewed, not edited.

Delete a Template

1. Go to *PROFILES :: TEMPLATE.*
2. Locate the template and select the checkbox.
3. Click **DELETE** (displays dialog).



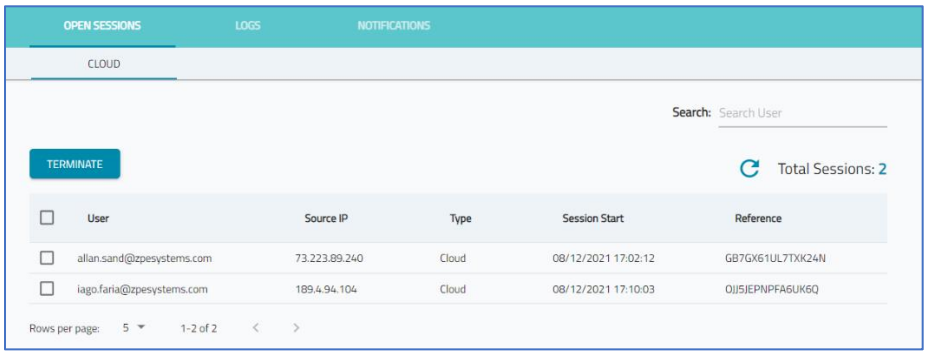
4. Click **DELETE**.

TRACKING Section

OPEN SESSIONS tab

CLOUD sub-tab

This displays currently active user sessions. From here, information can be viewed related to each active session.



Cloud Table Columns

Column Name	Description
User	Name of User.
Source IP	User's IP address.
Type	Type of access
Session Start	Date/time session began.
Reference	Session Reference ID.

Terminate Session(s)

1. Go to *TRACKING :: OPEN SESSIONS :: CLOUD*.
2. Select the checkbox next to the session(s) to be terminated.
3. Click **TERMINATE**.

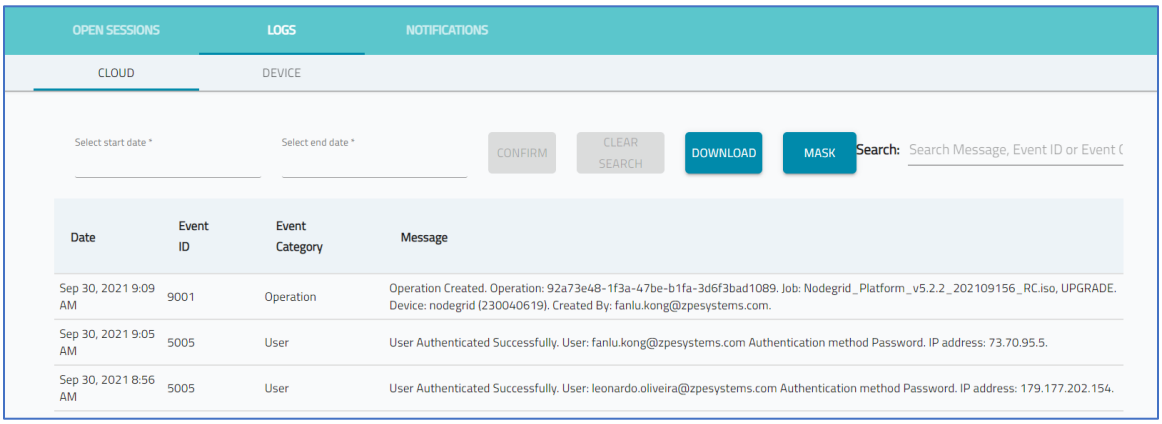
   NOTE: User's own session cannot be terminated.

LOGS tab

All actions within ZPE Cloud are registered and displayed under the LOGS tab. Operations conducted on attached devices are also listed here.

CLOUD sub-tab

This displays logs of connections between Nodegrid devices and ZPE Cloud. User login and logout information is also available on this page.



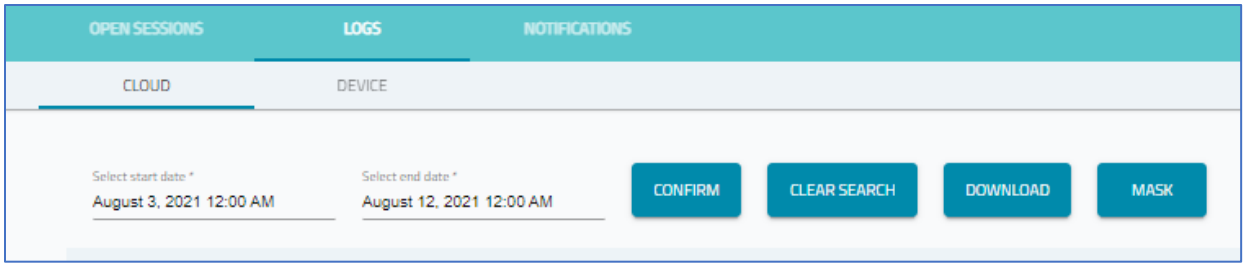
NOTE: Events can also be viewed on the Nodegrid device. Login to device and go to *Tracking :: Event List*.

Cloud Table Columns

Column Name	Description
Date	Date/time of the event.
Event ID	ID number related to the event.
Event Category	Category of the event.
Message	Message of event details.

Filter Events by Date/Time

1. Go to *TRACKING :: LOGS :: CLOUD*.



2. Click **Select Start Date** to choose a date/time.
3. Click **Select End Date** to choose a date/time.
4. Click **CONFIRM**.

The list repopulates with the time/date filters.

Restore full listing

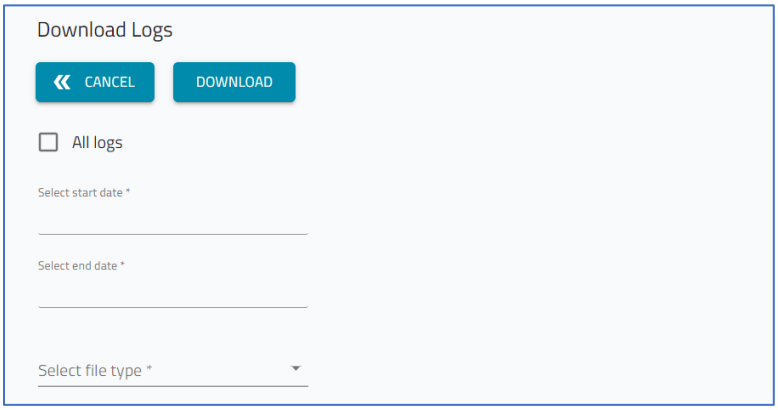
1. Go to *TRACKING :: LOGS :: CLOUD*.
2. Click **CLEAR SEARCH**.

3. List is populated with all logs.

   NOTE: If Search date/times are not applied, the listing does not change.

Download Logs

1. Go to *TRACKING :: LOGS :: CLOUD*.
2. Click **DOWNLOAD** (displays dialog).



3. Select *one* of these options:

   For every log, select **All logs** checkbox.

   For a time range, enter date/times for **Select Start Date** and **Select End Date**.
4. In the **Select file type** drop-down, select one (**CSV**, **Excel**).
5. Click **DOWNLOAD**.

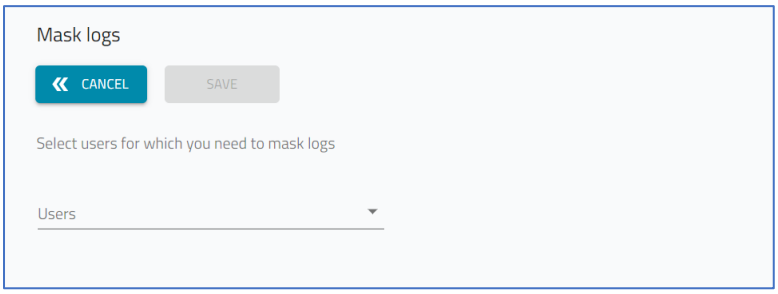
The file is saved to the local download location.

If no logs, a pop-up dialog (lower right), indicates no logs available.

Mask User Logs

Use this to exclude logs of certain users.

1. Go to *TRACKING :: LOGS :: CLOUD*.
2. Click **MASK** (displays Mask logs dialog).



3. On the **Users** drop-down, select checkboxes of users to be excluded from logs.

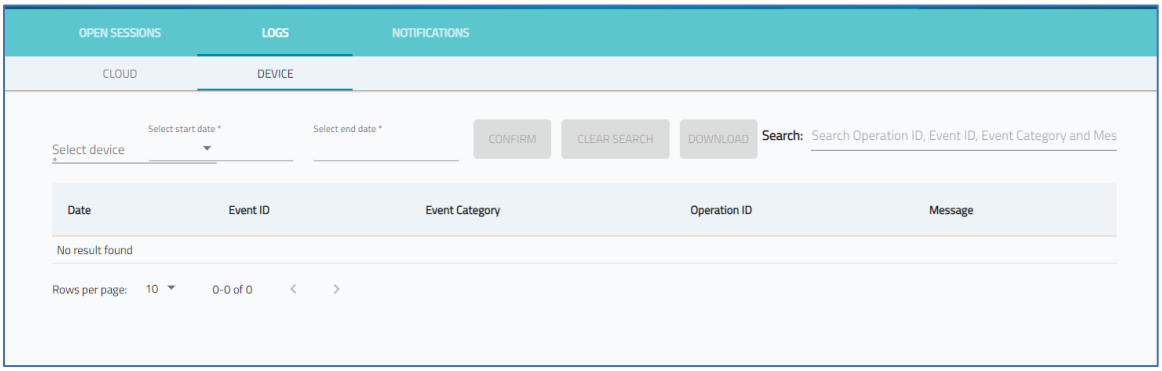
4. Click **SAVE**.

Masking continues until a new Mask filter is created.

NOTE: When a user is deleted, there is the option to mask that user's logs.

DEVICE sub-tab

This listing provides event details on devices.

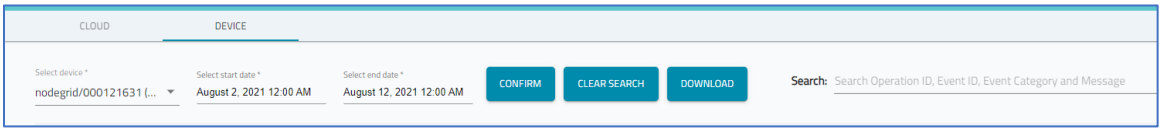


Device Table Columns

Column Name	Description
Date	Date of event.
Event ID	Identification of Event.
Event Category	Category of event.
Operation ID	Identification of device optional.
Message	Message about device event.

Filter the List

1. Go to *TRACKING :: LOGS :: DEVICE*.
2. To filter on a specific device, click **Select device** to choose an individual device. (Leave blank for all devices.)



3. Click **Select Start Date** to choose a date/time.
4. Click **Select End Date** to choose a date/time.
5. Click **CONFIRM**.

The list populates based on the date/time filters.

Restore full listing

1. Go to *TRACKING :: LOGS :: DEVICE*.
2. Click **CLEAR SEARCH**.
3. List is populated with all logs.

   NOTE: If Search date/times are not applied, the listing does not change.

Download Device Events

1. Go to *TRACKING :: LOGS :: DEVICE*.
2. (as needed) Apply device/date/time filters to the listing.
3. Click **DOWNLOAD**.

The file is saved to the local download location.

NOTIFICATIONS tab

This page lists events within two conditions: OPEN and CLOSED.

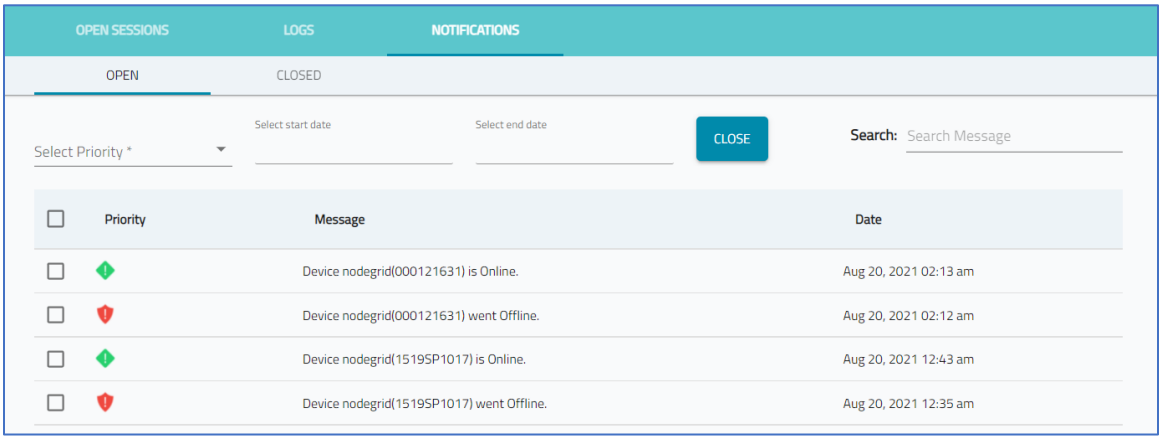
ZPE Cloud sends emails to selected users when certain events occur on enrolled devices. Specified managers receive email updates on critical conditions. Go to *SETTINGS :: NOTIFICATIONS* to configure email and SMS notifications for designated event types.

There are three notification priority levels.

Notification	Warning	Critical Error
 New device enrolled New device available Configuration applied successfully Script applied successfully Successful software upgrade Successful backup Backup restored successfully	 Device in failover state License expires in 60, 30, 20, or 10 days	 Device in failover state Site went offline Group went offline Failed to apply configuration Software upgrade failed Failed to backup Failed to restore backup License expires in 5, 4, 3, 2, or 1 day(s)

OPEN sub-tab

This page lists open event messages. These messages are not yet acknowledged.



Open Message Table Columns

Column Name	Description
Priority	This symbol indicates type of event: Notification, Warning, and Critical
Message	Description and details of the event.
Date	Date and time

Filter the List

1. Go to *TRACKING :: NOTIFICATIONS :: OPEN*.
2. To filter on a specific notification type, on **Select notification** dropdown, select one (**All**, **Critical**, **Warning**, **Notification**)

   The list repopulates, based on the selection.
3. To filter based on date/time:

   Click **Select Start Date** to choose a date/time.

   Click **Select End Date** to choose a date/time.

   The list repopulates, based on the time range.

NOTE: to restore the list, click on the *CLOSED* sub-tab, then click on the *OPEN* sub-tab.

Move Open Notifications to Closed Listing

1. Go to *TRACKING :: NOTIFICATIONS :: OPEN*.
2. To filter the table listing:

   In the **Select Priority** drop-down, select one (**All**, **Critical**, **Warning**, **Notification**).

   Click **Select Start Date** to choose a date/time.

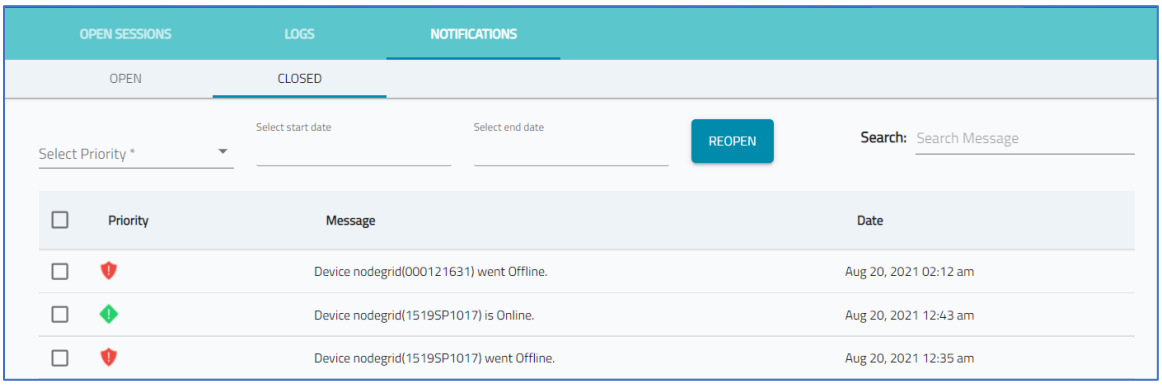
   Click **Select End Date** to choose a date/time.
3. Select **Event** checkboxes to be closed.

4. Click **CLOSE**.

Notifications are moved to CLOSED sub-tab.

CLOSED sub-tab

This table lists messages marked as closed messages. These event messages are acknowledge as read and resolved.



Closed Message Table Columns

Column Name	Description
Priority	This symbol indicates type of event: Notification, Warning, and Critical
Message	Description and details of the event.
Date	Date and time

Filter the List

1. Go to *TRACKING :: NOTIFICATIONS :: CLOSED*.
2. To filter on a specific notification type, on **Select notification** dropdown, select one (**All**, **Critical**, **Warning**, **Notification**)

   The list repopulates, based on the selection.
3. To filter based on date/time:

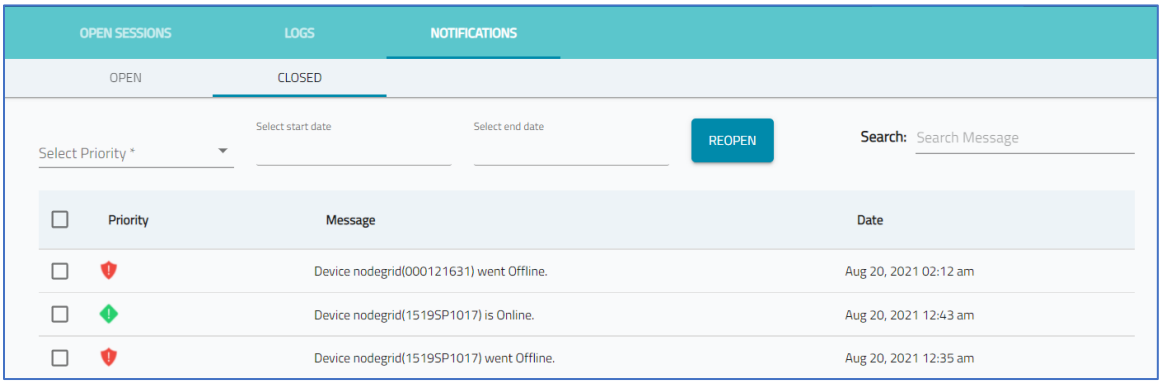
   Click **Select Start Date** to choose a date/time.

   Click **Select End Date** to choose a date/time.

   The list repopulates, based on the time range.

NOTE: to restore the list, click on the *OPEN* sub-tab, then click on the *CLOSED* sub-tab.

Move Closed Notifications back to Open Listing



1. Go to *TRACKING :: NOTIFICATIONS :: CLOSED*.
2. To filter the table listing:

   In the **Select Priority** drop-down, select one (**All**, **Critical**, **Warning**, **Notification**).

   Click **Select Start Date** to choose a date/time.

   Click **Select End Date** to choose a date/time.
3. Select **Event** checkboxes to be re-opened.
4. Click **REOPEN**.

Notifications are moved to *OPEN* sub-tab.

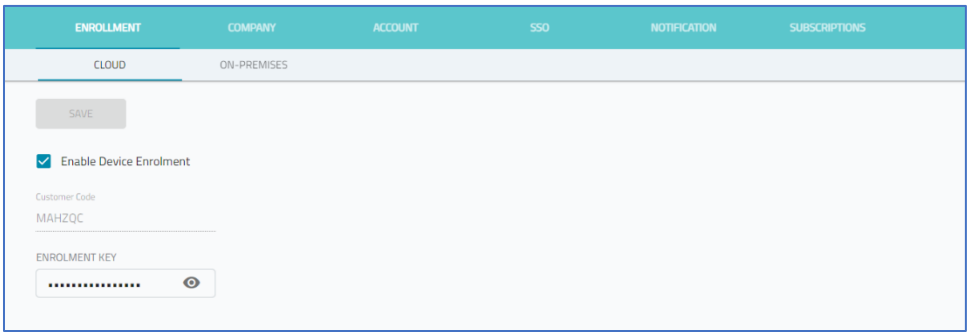
SETTINGS Section

Configurations and actions specific to company specifications and requirements are managed within this section.

ENROLLMENT tab

CLOUD sub-tab

Enrollment of devices can be enabled or disabled (default: disabled).



Enable Enrollment

1. Select **Enable Device Enrollment** checkbox.
2. Enter the **Enrollment Key**.

   The Enrollment Key should be a combination of numbers, letters, and special characters.
3. Click **SAVE**.
4. A pop-up dialog (lower right) confirms the Enrollment Key is saved.

   NOTE: Customer Code is an identifier unique to the company associated with the device. It is used to enroll devices and transfer device ownership.

Enrollment from Device

NOTE: This is only available for Nodegrid devices, version 4.2 or later.

WebUI Procedure

1. Login on the device with admin permissions.
2. Go to *System :: Toolkit :: Cloud Enrollment*.
3. Enter **ZPE Cloud URL**.
4. Enter **Customer Code.**
5. Enter **Enrollment Key**.
6. Click **ENROLL**.

If the process is successful, a pop-up dialog confirms success.

Device CLI Enrollment (Nodegrid v4.1)

CLI is required to enroll devices with Nodegrid version 4.1.

CLI Procedure

1. On CLI window, login with root permissions.
2. Execute:

   ```
   zpe_cloud_enroll
   ```
3. Enter the **Customer Code**.
4. Enter the registered **Enrollment Key**.
5. Use commit command.
6. If successful, this message displays:

   ```
   Enrollment process successful!
   ```

Device CLI Enrollment (Nodegrid v4.2)

CLI is required to enroll devices with Nodegrid version 4.2.

CLI Procedure

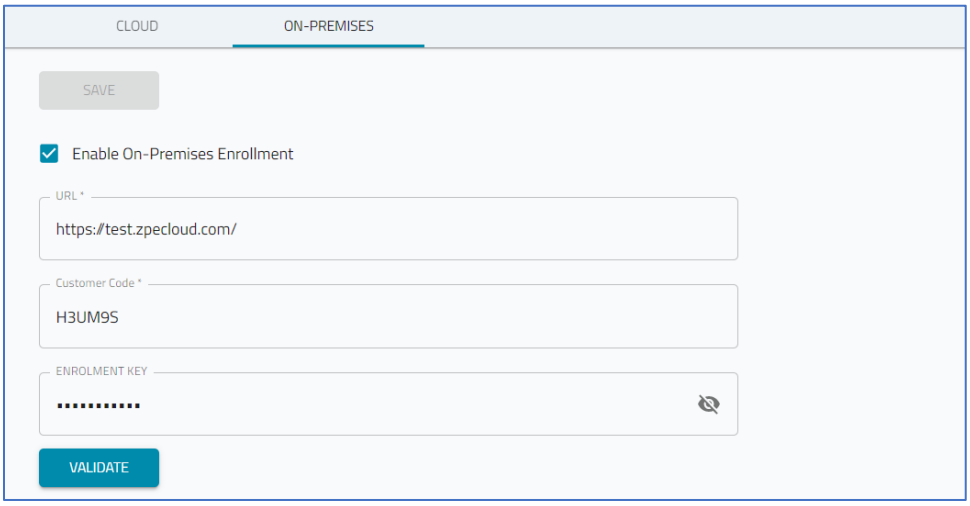
1. On CLI window, login with root permissions.
2. Execute:

   ```
   zpe_cloud_enroll
   ```

3. Enter the **Customer Code** value.
4. Enter the registered **Enrollment Key**.
5. For enrollment into ZPE Cloud or ZPE Cloud On-Premise, enter **yes** or **no**.
6. If successful, this message displays:

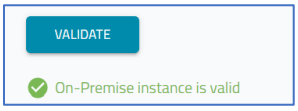
   ```
   Enrollment process successful!
   ```

ON-PREMISE sub-tab



Enable On-Premise Enrollment

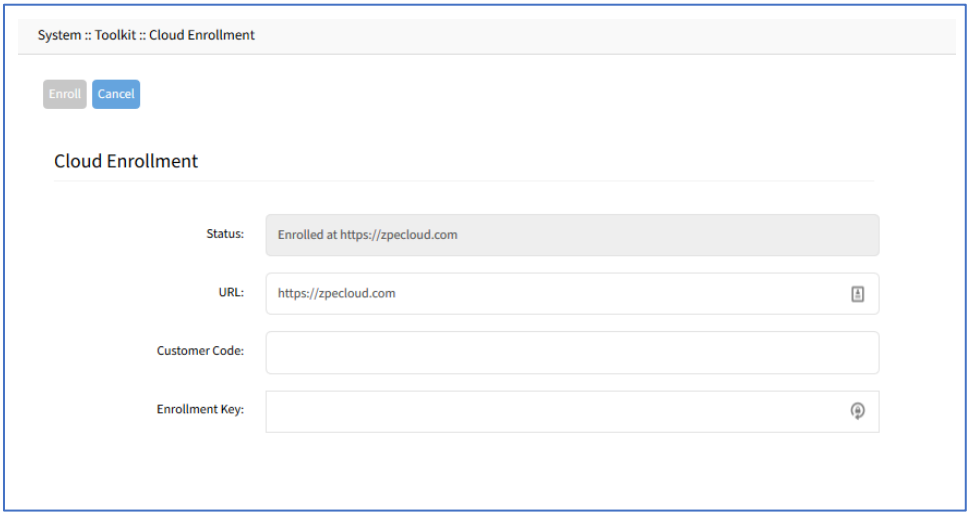
1. Go to *SETTINGS :: ENROLLMENT :: ON-PREMISE*.
2. Select **Enable On-Premise Enrollment** checkbox.
3. Enter **URL**.
4. Enter **Customer Code**.
5. Enter **Enrollment Key**.
6. Click **VALIDATE**.



7. On confirmation (below the VALIDATE button), click **SAVE**.

Enroll a New On-Premise Device (including Nodegrid Manager)

1. Go to *SETTINGS :: ENROLLMENT :: CLOUD*.
2. Copy the **Customer Code** and **Enrollment Key**.
3. Login to the new Nodegrid device.
4. Go to *System :: Toolkit :: Cloud Enrollment*.

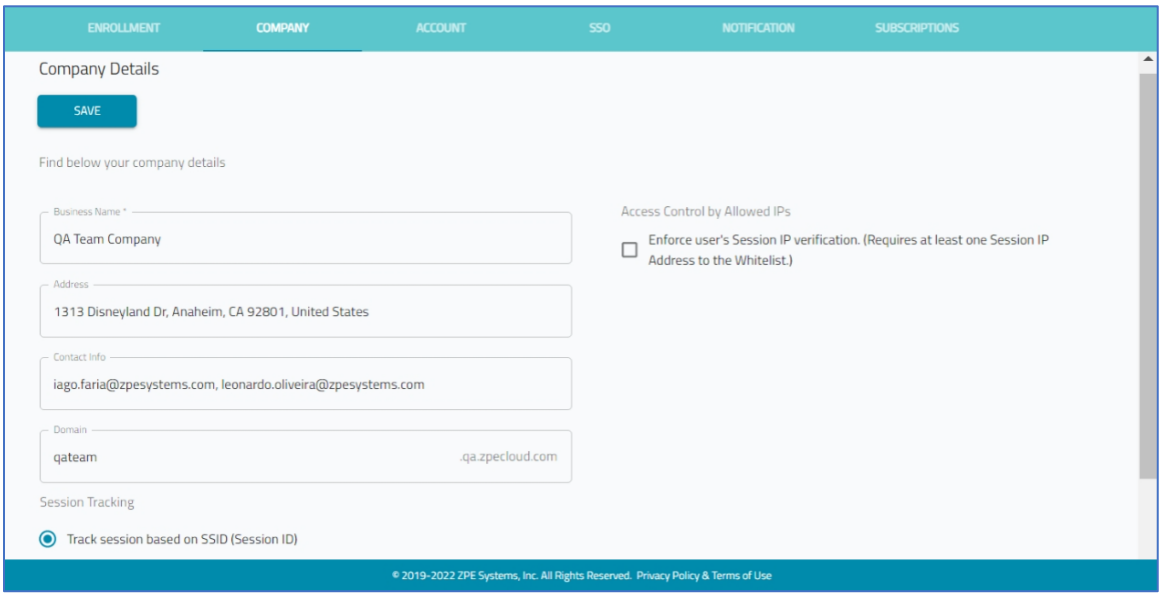


5. Enter **Customer Code** and **Enrollment Key**.
6. Click **Enroll**.

   NOTE: If "Failed to enroll device. TPM is disabled." error displays, log into the device's BIOS and go to *Configuration :: TPM Configuration* and select **Enable TPM** checkbox.

COMPANY tab

This includes company details used with ZPE Cloud.



Manage Company Details

To update details, administrator privileges are required.

Enter Company Details

1. Go to *SETTINGS :: COMPANY*.
2. Enter **Business Name**.
3. Enter **Address**.
4. Enter **Contact Info** (email).
5. Enter **Domain**.
6. On *Session Tracking* menu, select one:

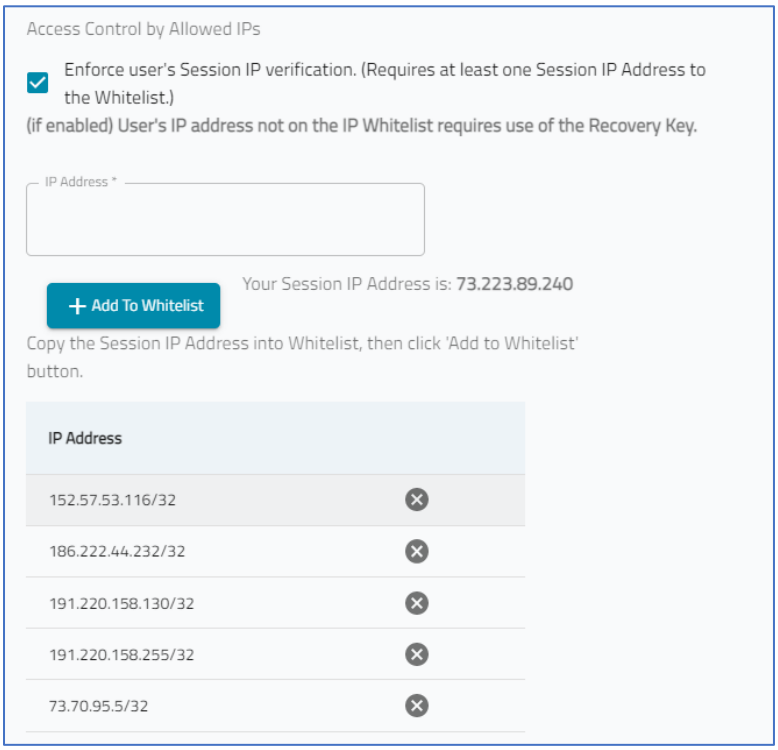
   Track session based on SSID (Session ID) radio button.

   Track session based on Source IP address and SSID (Session ID) radio button.
7. Click **Upload Logo**.

   Locate and select the image (must be jpg, jpeg, or png).

   NOTE: The logo is displayed on the login page and top-left on the interface.
8. In *Access Control by Allowed IPs* section:

   Select **Enforce user's Session IP verification. (Requires at least one Session IP Address to the Whitelist.)** checkbox (expands dialog).



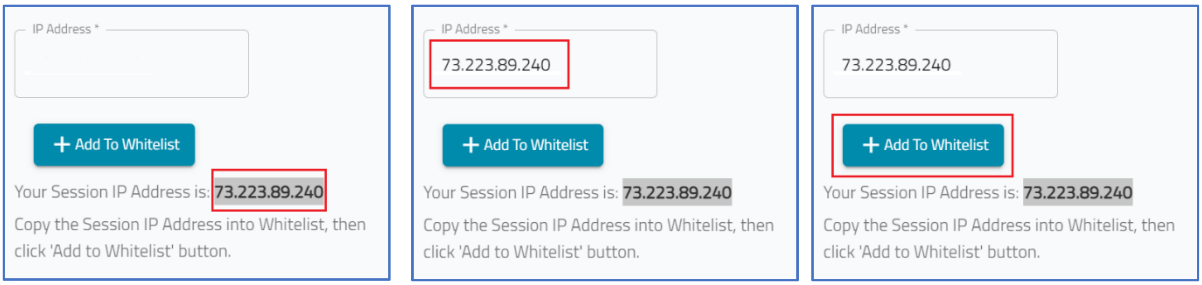
NOTE: The IP Address section lists already whitelisted IP addresses. IP Addresses can be whitelisted only one at a time.

To add to the whitelisted IP Addresses: (this example uses *Your Session IP Address*)

Identify the **Session IP Address**

Type or copy/paste into **IP Address** textbox

Click **+Add to Whitelist**.



To remove a white-listed IP Address:

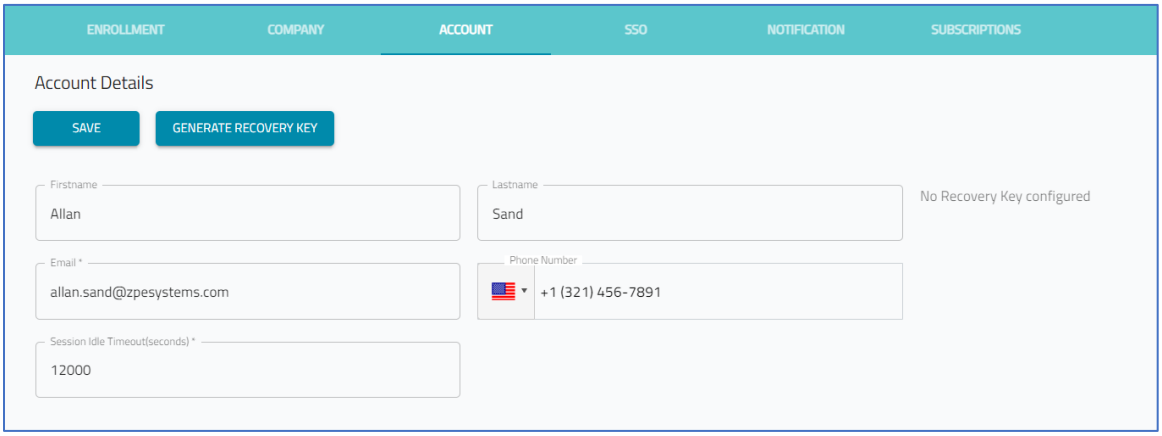
In the *IP Address* list, click ⊗.

NOTE: If the Recovery Key is necessary, go to *SETTINGS :: ACCOUNT* and click **GENERATE RECOVERY KEY**. Save it in a location to be used when needed.

9. Click **SAVE**.

ACCOUNT tab

The user can modify account details, and (as needed), generate the Recovery Key.



Manage Account

Edit Account Details

1. Go to *SETTINGS :: ACCOUNT*.
2. Edit details, as needed:

   First Name

   Last Name

   Email

   Phone Number (select country from flag drop-down list)

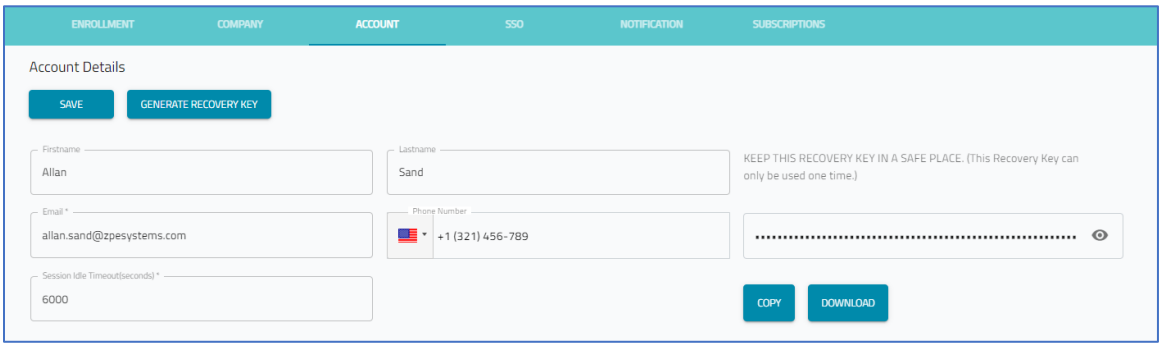
   Session Idle Timeout (seconds) (zero "0" indicates no timeout)
3. Click **SAVE**.

Generate the Recovery Key

The Recovery Key is only required when the user logs in from an IP Address that is NOT on the whitelisted IP Addresses. The Recovery Key is linked to the username.

NOTE: The generated Recovery Key can only be used once. Once logged in, another Recovery Key can be generated.

1. Go to *SETTINGS :: ACCOUNT*.
2. Click **GENERATE RECOVERY KEY**.



To download as a text file, click **DOWNLOAD**.

To copy and paste into another location, click **COPY**.

3. Use the key on the *Login* page as the *Password*.

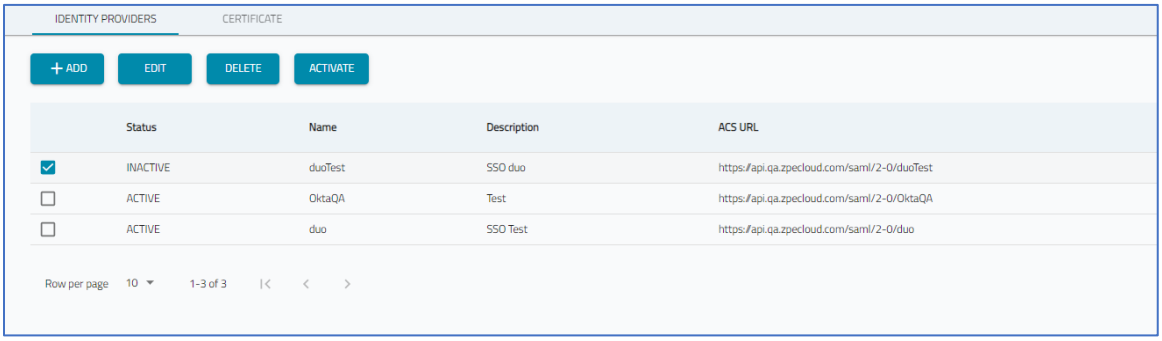
   CAUTION: If this process is not correctly used, the user must contact the Company Administrator to resolve the whitelist permissions.

SSO tab

On this tab, identity providers and certificates are managed.

IDENTITY PROVIDERS sub-tab

Identity provider information is managed on this page.

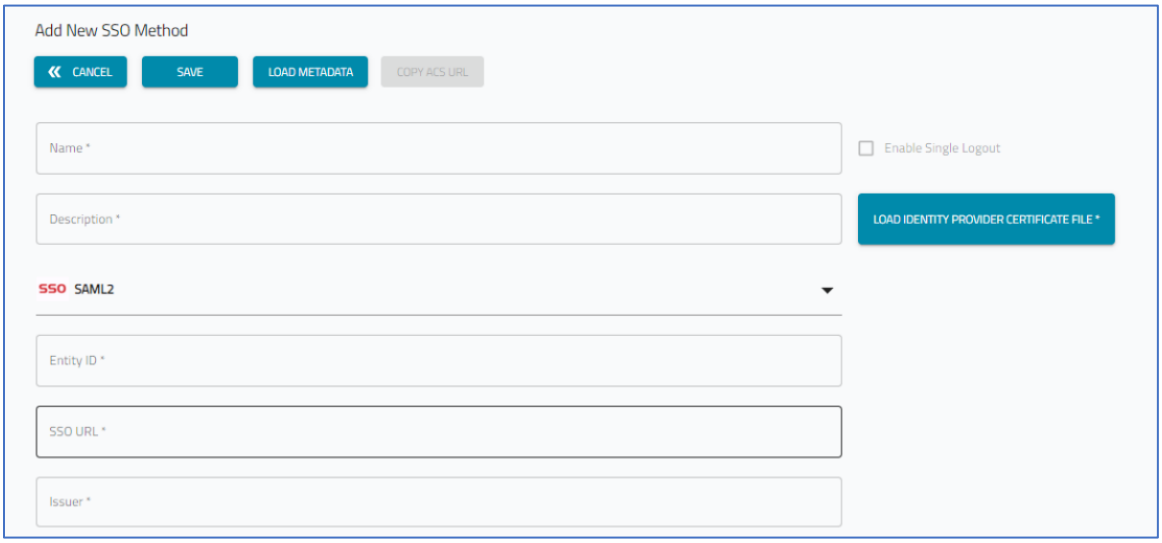


Identity Provider Table Columns

Column Name	Description
Status	Status of identity provider: Active, Inactive.
Name	Name of the identity provider.
Description	Information on the identity provider.
ACS URL	Web address of ACS.

Add a new Identity Provider

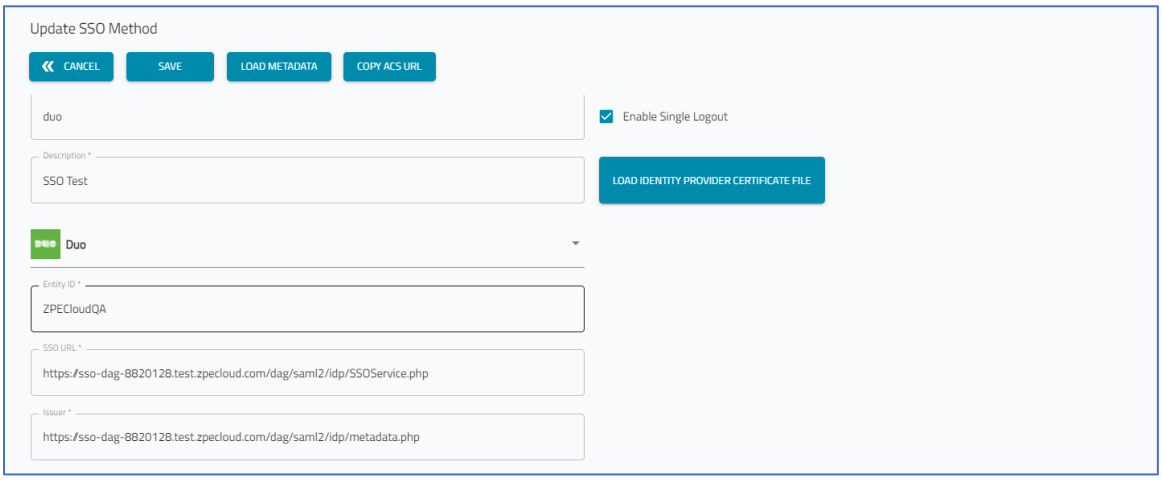
1. Go to *SETTINGS :: SSO :: IDENTITY PROVIDERS*.
2. Click **+ADD** (displays dialog).



3. Enter **Name** (name of the SSO method).
4. Enter **Description** (information about the provider).
5. On **SSO Method** drop-down, select one.
6. Enter **Entity ID**.
7. Enter **SSO URL**.
8. Enter **Issuer**.
9. Click **LOAD IDENTITY PROVIDER CERTIFICATE FILE** (locate and select a valid certificate).
10. Select **Enable Single Logout** checkbox (if there is a valid certificate). If not, leave unselected.
11. Click **SAVE**.

Edit an Identity Provider

1. Go to *SETTINGS :: SSO :: IDENTITY PROVIDERS*.
2. In the table, locate identity provider and select checkbox.
3. Click **EDIT** (displays dialog).

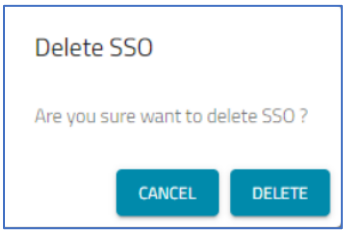


4. Make changes, as needed.
5. Click **SAVE**.

Delete an Identity Provider

One or more identity providers can be deleted in a single operation

1. Go to *SETTINGS :: SSO :: IDENTITY PROVIDERS*.
2. In the table, locate identity provider(s) and select checkbox(es).
3. Click **DELETE** (displays dialog).



4. Click **DELETE** to complete the action.

Deactivate an Identity Provider

One or more identity providers can be deactivated.

1. Go to *SETTINGS :: SSO :: IDENTITY PROVIDERS*.
2. In the table, locate identity provider(s) in *Active* state, and select checkbox(es).
3. Click **DEACTIVATE**.

The *Status* changes to **INACTIVE**.

Activate an Inactive Identity Provider

One or more inactive identity providers can be activated.

1. Go to *SETTINGS :: SSO :: IDENTITY PROVIDERS*.

2. In the table, locate identity provider(s) with *Inactive* state, and select checkbox(es).
3. Click **ACTIVATE**.
4. The *Status* of the identity provider changes to **ACTIVE**.

Configure SSO Identify Providers

Okta Setup

Access to a developer account is required (free trial options are available).

1. Access the Okta developer console.
2. Change the UI view from *Developer* to *Classical*.

   (SAML applications are not shown in *Developer* view).
3. Go to *Application :: Add Applications :: Create New App*.
4. Select **Web** and **SAML 2.0** , then click **Create**.
5. The following fields are required:

   Single sign on URL (https://api.zpecloud.com/saml/2-0/**<sso_name>**)

   SP entity ID (ID name for the service)

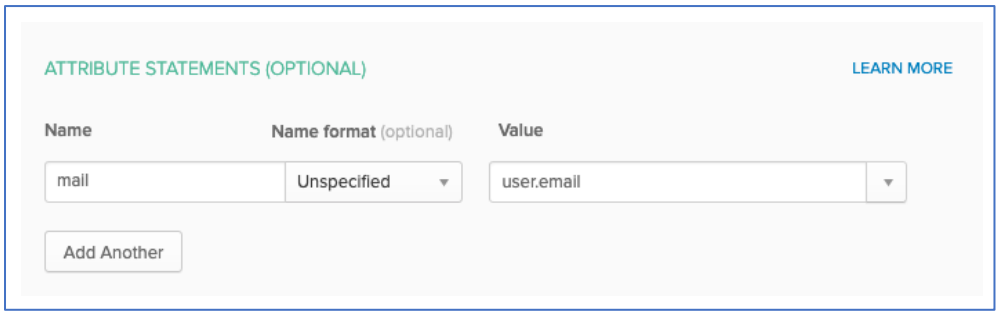
   Name ID format (unspecified)

   Application username (email address)
6. (optional) To enable SLO, click **Show Advances Settings** and select **Single Logout** checkbox.
7. Enter details in the required fields:

   Single Logout URL (https://api.zpecloud.com/saml/2-0/**<sso_name>**/logout)

   SP Issuer (same as SP entity ID)

   Signature Certificate (use the certificate downloaded from ZPE Cloud under *Settings :: SSO :: Certificate*)
8. On the *Attribute Statements* dialog, add mail to the attribute mapping.



9. Click **Save**.
10. On the **Assignment** tab, select users to have access to SSO.

Okta Cloud Setup

1. Login to Okta cloud and go to the *Application Configuration* page.
2. On the **Sign On** tab, click **View Setup Instructions**:

   Entity ID (SP Entity)

   SSO URL (Identity Provider Single Sign-On URL)

   Issuer (Identity Provider Issuer)
3. Download the X.509 certificate and upload it to the Cloud.

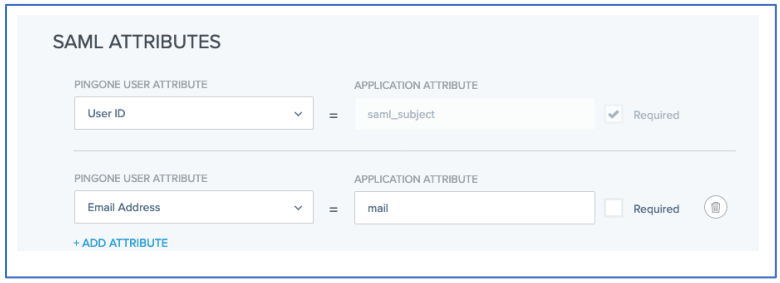
   NOTE: To use the logout function, select the **Single Logout** checkbox, and add the single logout URL from the identity provider. If the XML file is loaded, this is automatic.

Ping Setup

1. On the *PingOne* administrator console, go to *Connection :: Applications* and click **Add Application**.
2. Under *Advanced Configuration*, select the option for **SAML**
3. Enter these details:

   ACS URL (https://api.zpecloud.com/saml/2-0/**<sso_name>**)

   Entity ID (any meaningful ID for the service)
4. Download the signing certificate.
5. On the **Mapping Attributes** tab, add the mail attribute.



6. (optional) To enable SLO, enter:

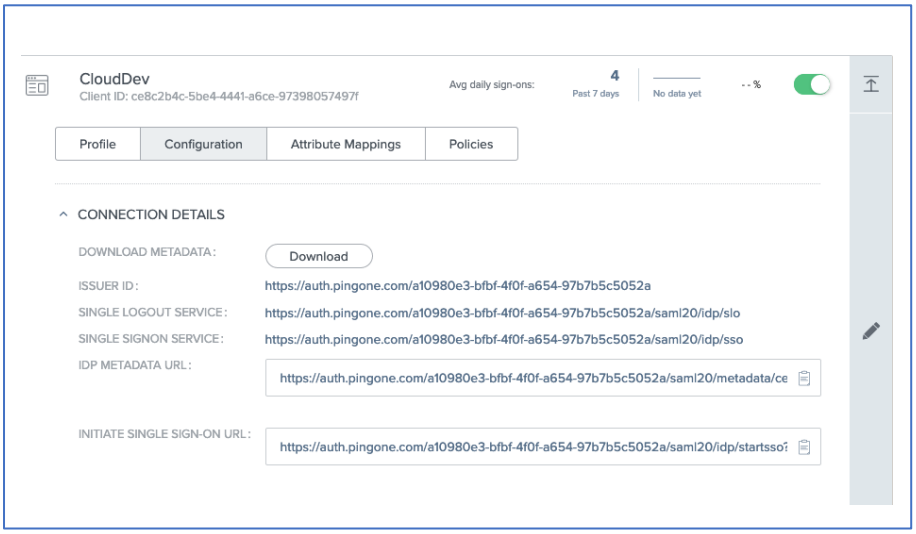
   SLO Endpoint (https://api.zpecloud.com/saml/2-0/**<sso_name>**/logout)

   SLO Binding (HTTP Post)

   Verification Certificate (click **Import** and choose the certificate previously downloaded from ZPE Cloud at Settings :: SSO :: Certificate)
7. Click **Save**.

PingID Cloud Setup

1. On the *PingOne Administrator Console*, access the application.



2. Enter these configuration details:

   Entity ID (Entity ID configured earlier)

   SSO URL (Single Sign-On Service web address)

   Issuer (Issuer ID)

3. (optional) Download metadata and upload the SSO form.

   NOTE: To use the logout function, select the **Single Logout** checkbox, and add the single logout URL from the identity provider. If the XML file is loaded, this is automatic.

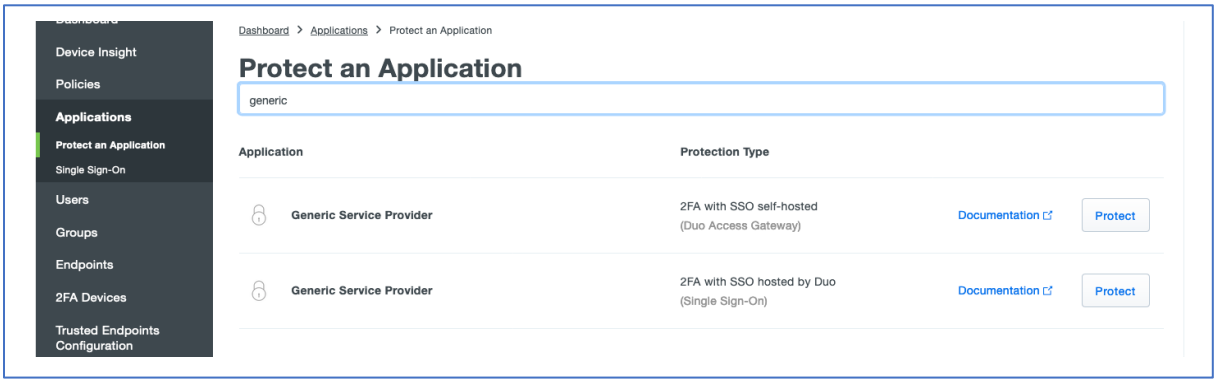
Duo

To authenticate, Duo requires the *Duo Access Gateway* (DAG). DAG requires a configuration specific to the selected authentication method. See the DUO website for further information.

To set up the authentication source, refer to Duo Guide (available here). Options include an external IdP, Active Directory and LDAP. After the authentication source is configured, setup the Duo Cloud application. On the *Application* menu, load the JSON to DAG application.

Create Application on Duo Cloud

1. Login to the Duo administrator account.
2. On the *Application* menu, click **Protect an Application**.
3. Use **Search** to locate the Generic Service Provider for DAG.



4. Click **Protect**.
5. Enter these details:

   Service Provider Name (Name to identify the service)

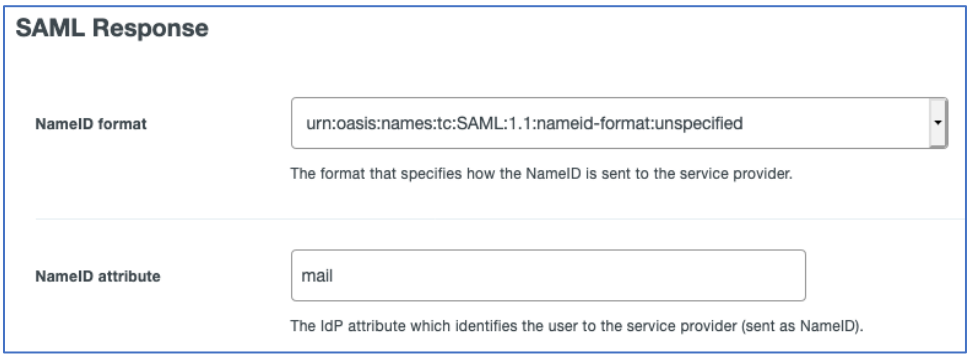
   Entity ID (meaningful ID to identify the service)

   Assertion Consumer Service (https://api.zpecloud.com/saml/2-0/**<sso_name>**)

   (optional) **Single Logout URL** (https://api.zpecloud.com/saml/2-0/**<sso_name>**/logout)
6. On the *SAML Response* menu:

   On **NameID format** drop-down, select **unspecified**

   On **NameID attribute**, enter **mail**

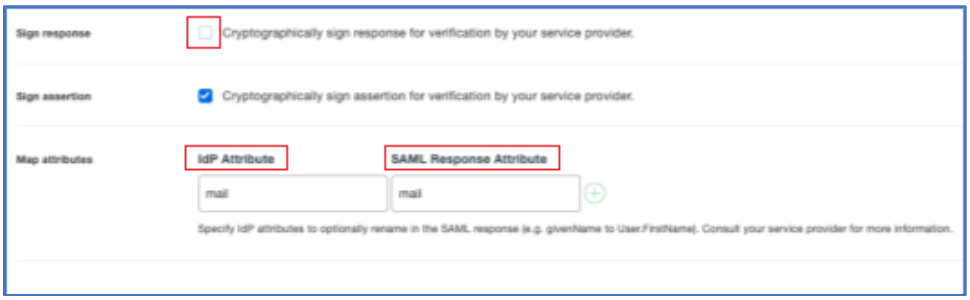


7. Complete these:

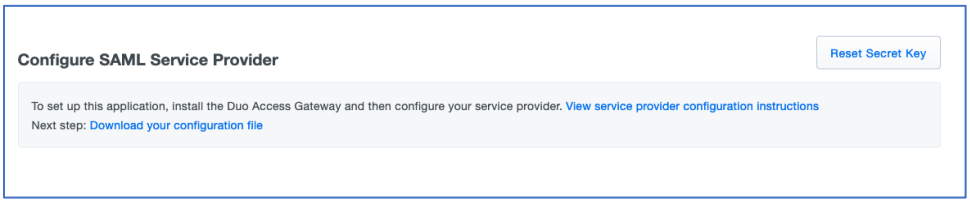
   Unselect **Sign response** checkbox.

   On **IdP Attribute**, enter **mail**.

   On **SAML Response Attribute**, enter **mail**.



8. Click **Save**.
9. Download the application: **JSON**.
10. In the *Application* menu, upload it to **Duo DAG**.



Duo Cloud Setup

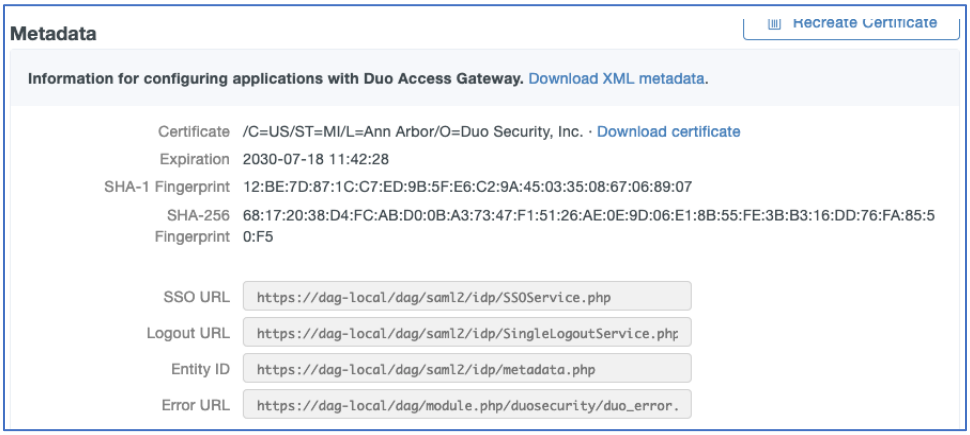
This requires Administrator credentials.

1. Login to *ZPE Cloud* and go to *SETTINGS :: SSO*.
2. Follow the *Add a new Identity Provider* procedure with the required fields (located within Duo DAG at *Application :: Metadata*):

   Entity ID (configured earlier)

   SSO URL (same as metadata)

   Issuer (Entity ID shown on metadata)
3. Download the certificate and upload it to ZPE Cloud.
4. (optional) To download the XML metadata and click **LOAD METADATA**.



AD FS

To add ZPE Cloud as a relaying party trust:

1. On the *Server Manager*, click **Tools**.
2. Select **AD FS Management**.
3. On the new window:

   Click **Relaying Party Trusts**.

   Click **Add Relaying Party Trust**
4. On the *Relaying Party Trust Wizard*, click **Start**.

   Select **Enter data about the relaying party manually** checkbox.

   Enter **Display Name**.

   Do not configure the certificate.
5. Click **Next**.

   In the *Configure URL for SAML 2.0* menu, enter: https://api.zpecloud.com/saml/2-0/**<sso name>**

   Add a relaying party trust identifier (same as Entity ID).

   On **Access Control Policy** drop-down, select **Permit Everyone**.
6. Confirm settings are correct, then click **Finish**.
7. To add a claim issuance policy:

   For the **Claim Rule Template**, select **Send LDAP Attributes as Claims**.

   On **Claim Rule Name**, enter **zpe_cloud**.

   On **Attribute Store**, select **Active Directory**.

   On **LDAP Attributes Mapping** drop-down, select **REQUIRED: E-Mail Addresses - Name ID**.

   In sequence, click **Finish**, **Apply**, **OK**.
8. To get AD FS Metadata (optional but recommended):

   Go to *AD FS :: Service :: Endpoints*

   In the *Metadata* menu, locate the **Federation Metadata**.

   Find the URL and copy into the browser address line.

   > **NOTE**: Should be: https://**<yourdomain.com>**/FederationMetadata/2007-06/FederationMetadata.xml.

   This automatically downloads the XML file.
9. To download the AD FS Certificate (X.509): (if Metadata was downloaded, skip this step)

   Go to *AD FS :: Service :: Certificates*.

   Click **Token-decrypting certificate**.

On the **Details** tab, click **Copy to file**.

Select **Base-64 encoded X.509 (.CER)** checkbox.

Save the file and click **Finish**.

10. To configure AD FS in ZPE Cloud: (if metadata was imported, only enter **Name** and **Description**). Follow the *Add a new Identity Provider* procedure:

    Name (name of the SSO)

    Description (generic description field)

    SSO Method (**ADFS**)

    Entity ID (relaying party trust identifier)

    SSO URL (copied from XML file https://**<yourdomain.com>**/adfs/ls/)

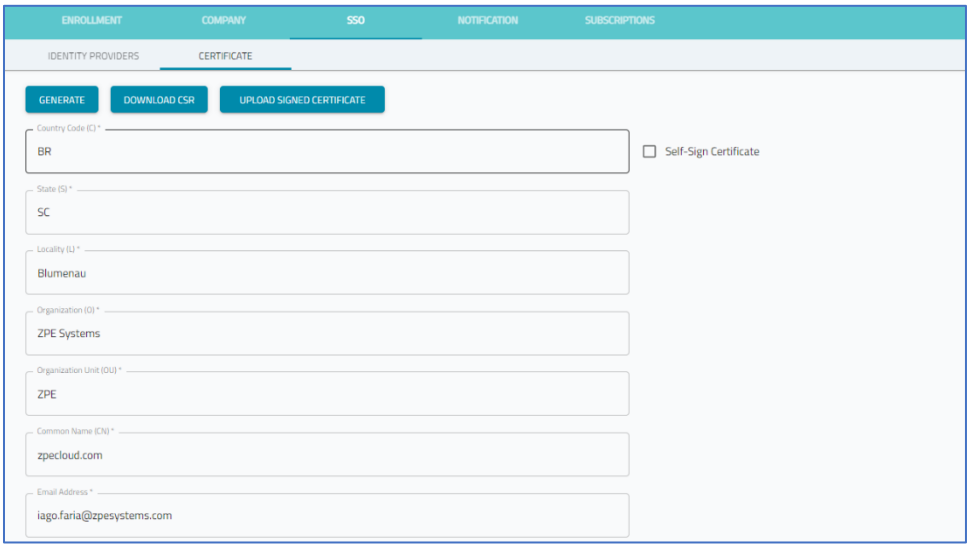
    Issuer (copy Entity ID from XML file https://**<yourdomain.com>**/adfs/services/trust)

    Load Identity Provider Certificate (upload the *AD FS Certificate*)

11. Click **Finish**.

CERTIFICATE sub-tab

A certificate can be generated on this page.



Generate a Certificate

1. Go to *SETTINGS :: SSO :: CERTIFICATE*.
2. Enter these details:

   Country Code

   State

   Locality

Organization

Organization Unit

Common Name

Email address

3. Click **GENERATE**.

Generate a Self-Sign Certificate

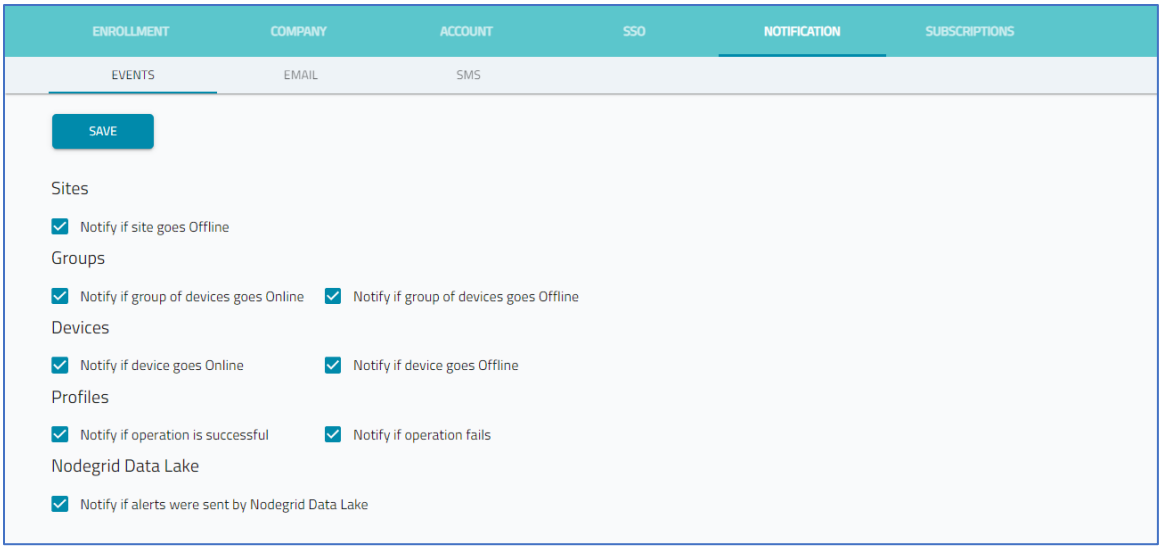
1. Go to *SETTINGS :: SSO :: CERTIFICATE*.
2. Select **Self-Sign Certificate** checkbox.
3. In **Certificate Validity (days)**, enter the valid period in days.
4. Click **GENERATE**.
5. (optional) Click **Download Certificate**.

NOTIFICATIONS tab

The notification system is managed on this page. nd SMS notifications for events.

EVENTS sub-tab

This page configures what events triggers an Email or SMS notification.



Configure Notification Events

1. Go to *SETTINGS :: NOTIFICATIONS :: EVENTS*.

   Select/unselect checkbox, as needed.

2. On *Sites* menu:

   Select **Notify if site goes Offline** checkbox.

3. In *Groups* menu:

   Select **Notify if group of devices goes Online** checkbox.

   Select **Notify if group of devices goes Offline** checkbox.

4. In *Devices* menu:

   Select **Notify if device goes Online** checkbox

   Select **Notify if device goes Offline** checkbox

5. In *Profiles* menu:

   Select **Notify if operation is successful** checkbox

   Select **Notify if operation fails** checkbox

6. (if installed) In *Nodegrid Data Lake* menu:

   Select **Notify if alerts were sent by Nodegrid Data Lake** checkbox

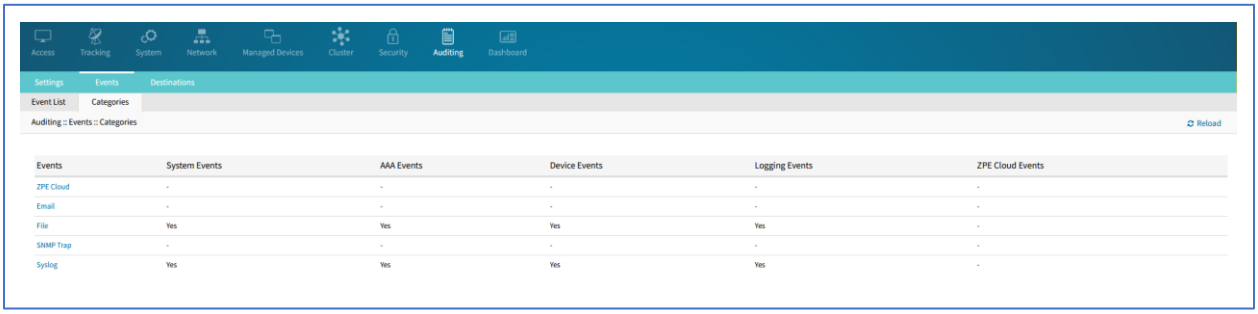
7. Click **SAVE**.

Configure Device to share Events with ZPE Cloud

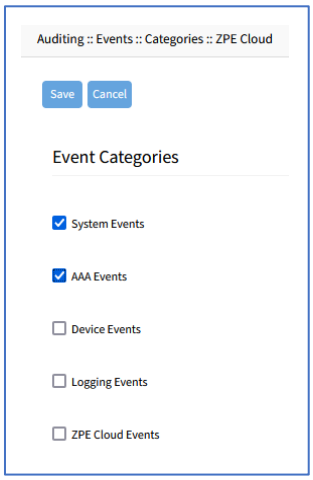
Nodegrid devices connected to ZPE Cloud do not automatically forward all event categories. Administrator privileges are required to configure.

WebUI Procedure

1. Login to the Nodegrid device.
2. Go to *Auditing :: Events :: Categories*.



3. In the *Events* column, click **ZPE Cloud**. (opens dialog).



4. In *Event Categories* menu, select/unselect, as needed.

   System Events checkbox

   AAA Events checkbox

   Device Events checkbox

   Logging Events checkbox

   ZPE Cloud Events checkbox

5. Click **Save**.

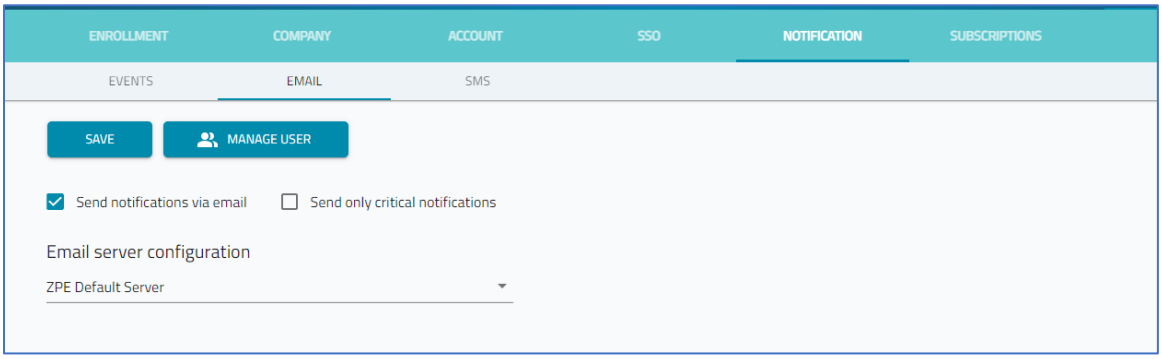
CLI Procedure

This CLI example selects event categories.

```
[admin@nodegrid /]# cd /settings/auditing/events/
[admin@nodegrid events]# cd <TAB><TAB>
email/      file/       snmp_trap/  syslog/     zpe_cloud/
[admin@nodegrid events]# cd zpe_cloud/
[admin@nodegrid zpe_cloud]# show
system_events = no
aaa_events = no
device_events = no
logging_events = no
zpe_cloud_events = no
[admin@nodegrid zpe_cloud]#
```

Email sub-tab

On this page, emails are configured when triggered by notifications.



Configure Email Notification for User

Make checkbox selections, as needed.

1. Go to *SETTINGS :: NOTIFICATIONS :: EMAIL*.
2. Select **Send notifications via email** checkbox.
3. Select **Send only critical notifications** checkbox.
4. On **Email server configuration** drop-down, select one:

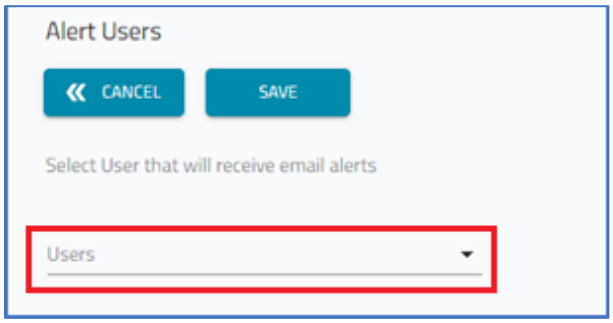
   If **ZPE Default server**, continue to next step.

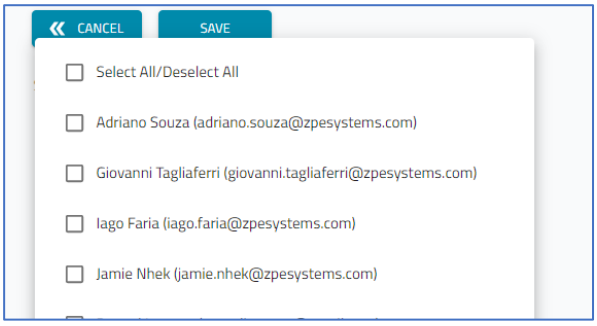
   If **SMTP**:

   Enter **Host**, **Port**, **User**, **Password**, **Sender Email**, **Timeout**.

   (optional) Select **TDS** checkbox.

   To validate, click **TEST CONFIGURATION**. If email is received, the settings are correct.
5. Click **MANAGE USERS** (displays dialog).
6. On **Users** drop-down, select individuals to receive notifications.



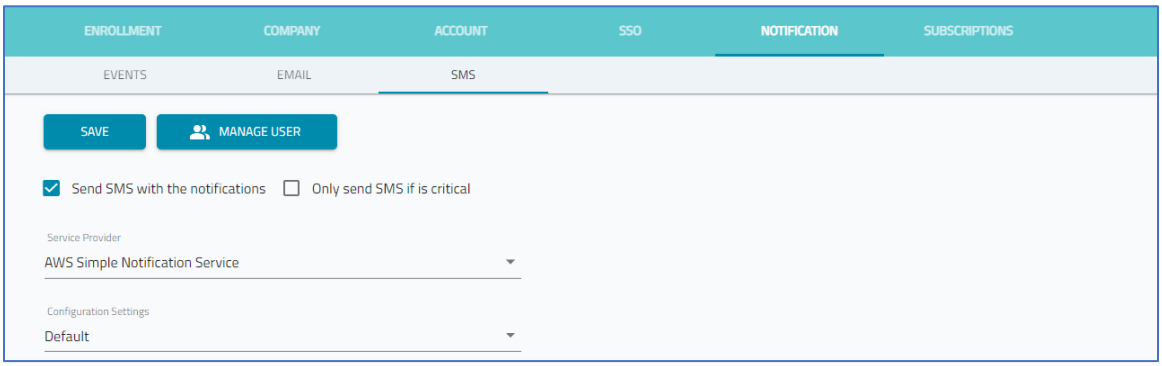


7. Click **SAVE**.

SMS sub-tab

Configure SMS Notifications

1. Go to *SETTINGS :: NOTIFICATIONS :: SMS*.



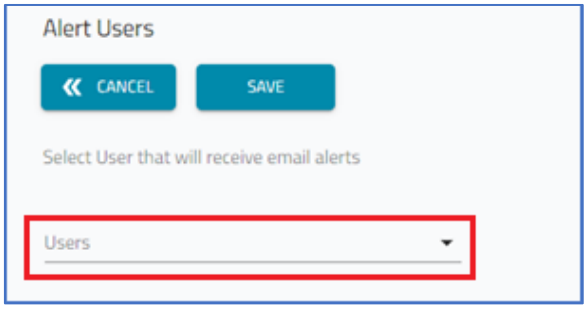
2. Select one:

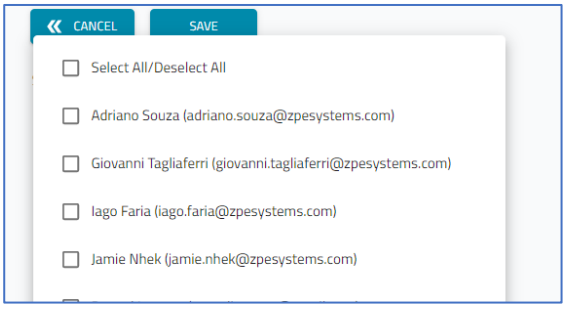
   Send SMS with the notifications checkbox

   Only send SMS if is critical checkbox

3. Click **MANAGE USERS** (displays *Alert Users* dialog).

   On **Users** drop-down, select checkboxes for individuals to receive notifications.

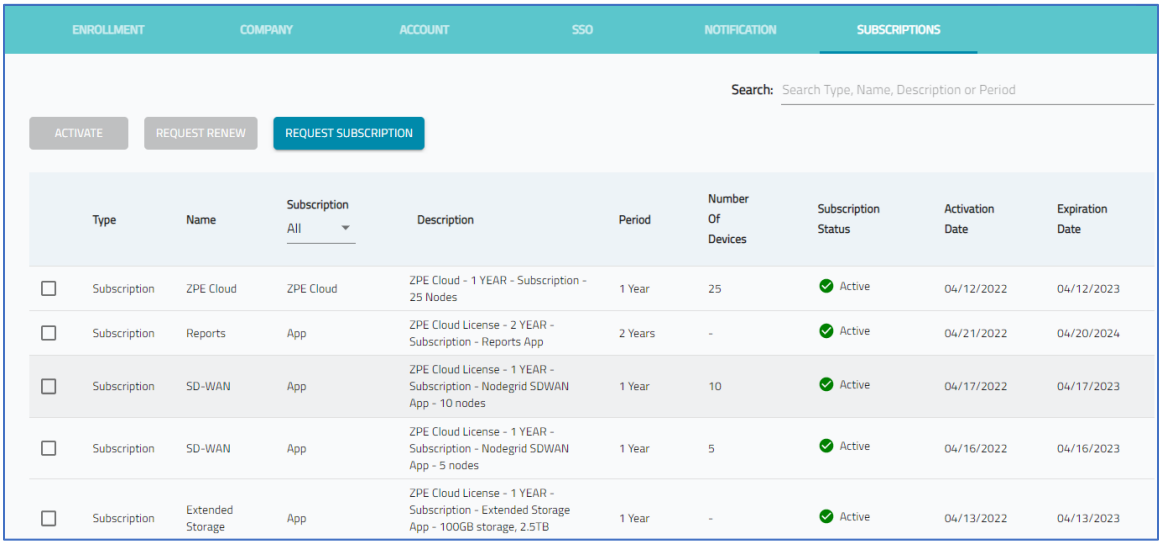




4. Click **SAVE**.

SUBSCRIPTIONS tab

Subscriptions are managed on this page.



Subscriptions Table Columns

Column Name	Description
Type	Type of subscription.
Name	Name of subscription,
Subscription drop-down	List is sorted, based on drop-down selection: All, Cloud, App.
Description	Information about the subscription.
Period	Length of time of the subscription.
Number of Devices	Number of devices for the subscription.
Subscription Status	Status of subscription: Active, Inactive.
Activation Date	Date subscription started.
Expiration Date	Date subscription expires.

Manage Subscriptions

Activate Subscription

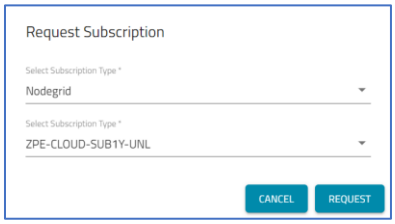
1. Go to *SETTINGS :: SUBSCRIPTIONS*.
2. In the table, locate and select checkbox of an inactive subscription.
3. Click **ACTIVATE**.

Request Subscription

1. Go to *SETTINGS :: SUBSCRIPTIONS*.
2. Click **REQUEST SUBSCRIPTION** (displays *Request Subscription* dialog).
3. On the **Select Subscription Type** drop-down, select one.

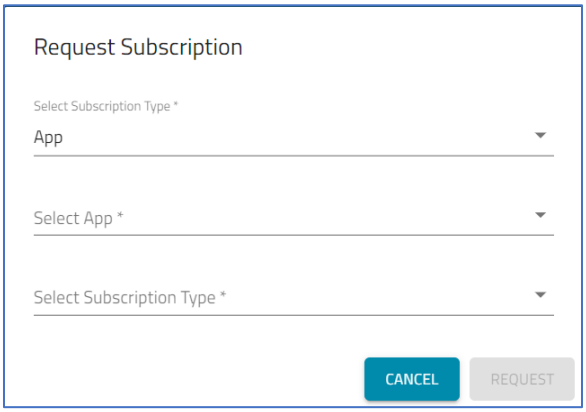
   Nodegrid

   On **Select Subscription Type** drop-down, select one. Then, click **REQUEST**.



   A dialog confirms the Request was submitted.

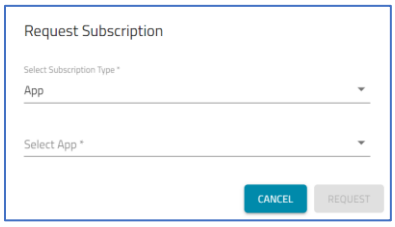
   App



On **Select App** drop-down, select one. (selection can display the following drop-down option).

On **Select Subscription Type** drop-down, select one.

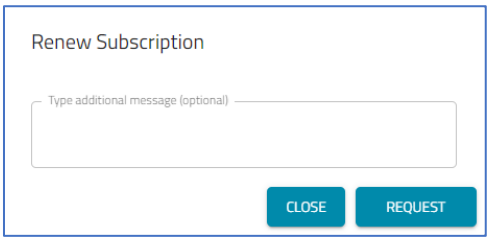
4. Click **REQUEST**.



A dialog confirms the Request was submitted.

Request a Subscription Renewal

1. Go to *SETTINGS :: SUBSCRIPTIONS*.
2. Select checkbox next to the subscription (Active or Inactive) to renew.
3. Click **REQUEST RENEW** (displays *Renew Subscription* dialog).



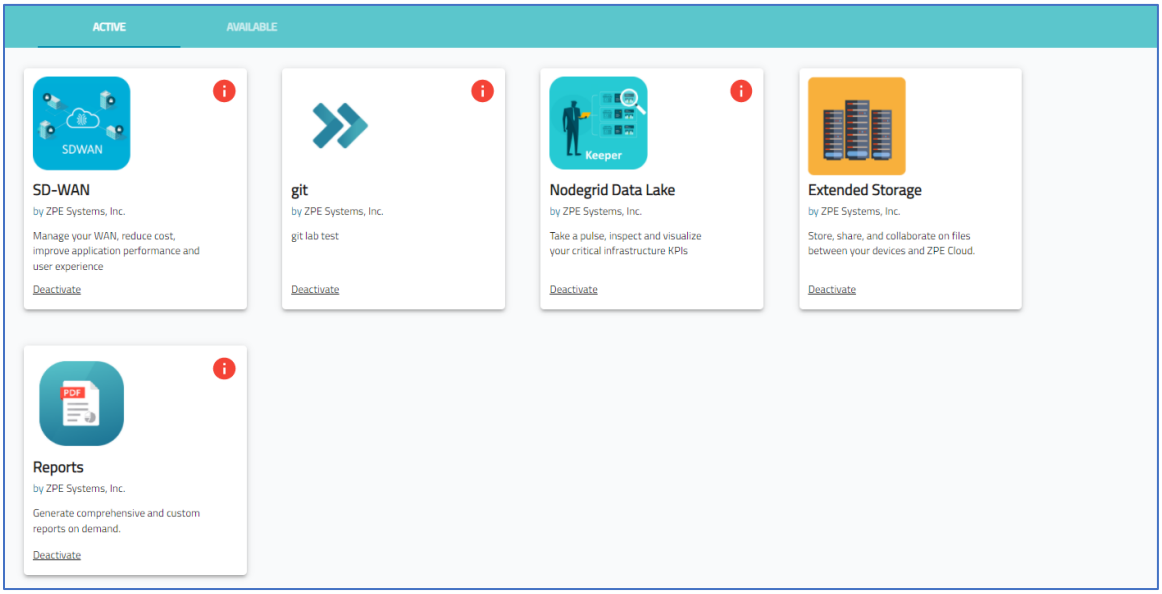
4. (optional) In **Type additional message** field, enter needed details.
5. Click **REQUEST**.

APPS Section

The apps page displays all active and available apps.

ACTIVE tab

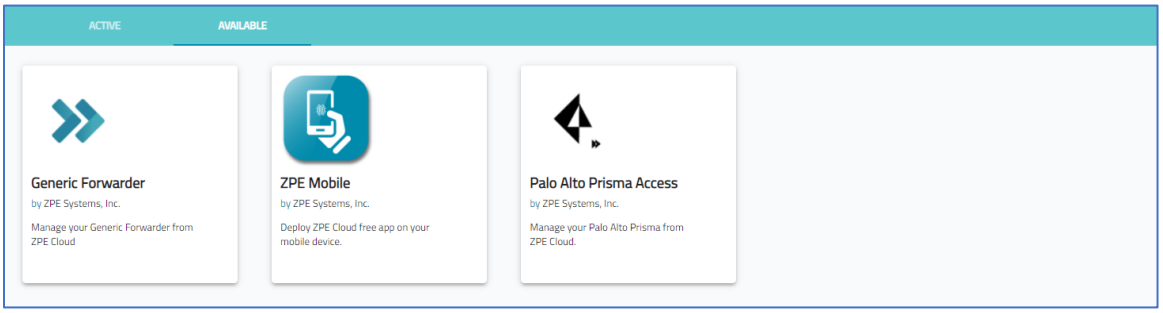
This displays all active apps currently available. Selection depends on customer's configuration.



NOTE: Apps only work for enrolled devices.

AVAILABLE tab

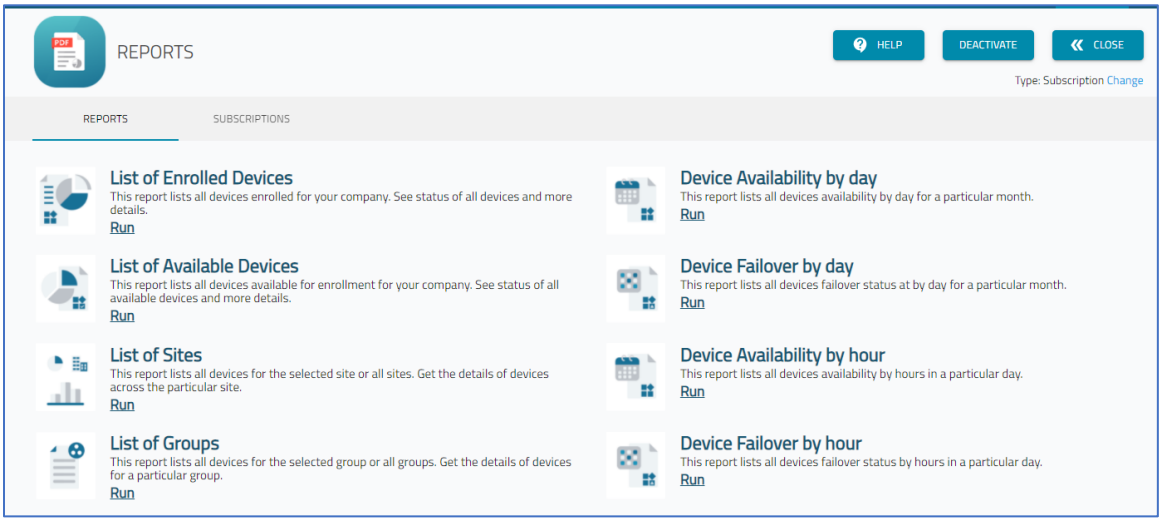
This page displays any available app not yet installed. Check back often to see newly added apps.



App Descriptions

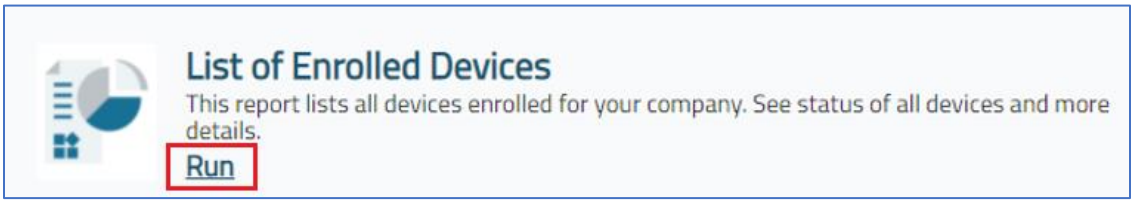
Reports App

This app generates reports (pre-configured and custom).

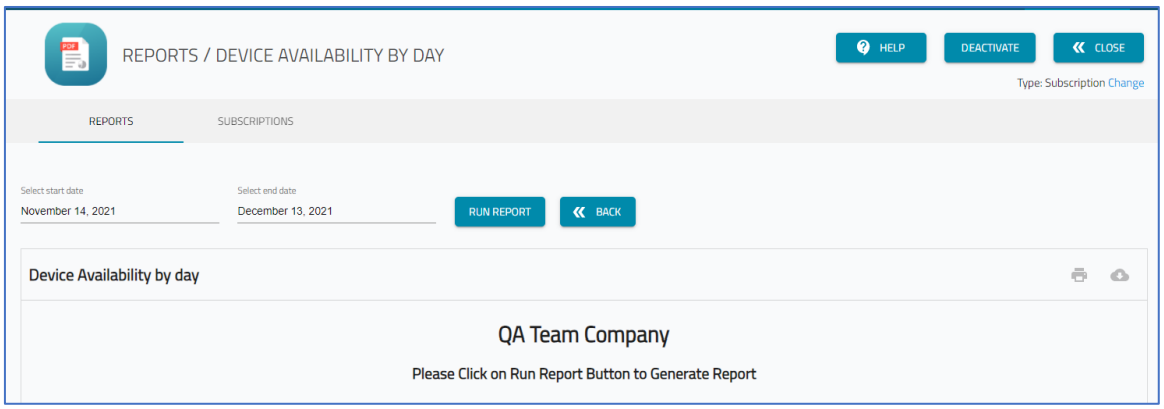


Run Individual Report

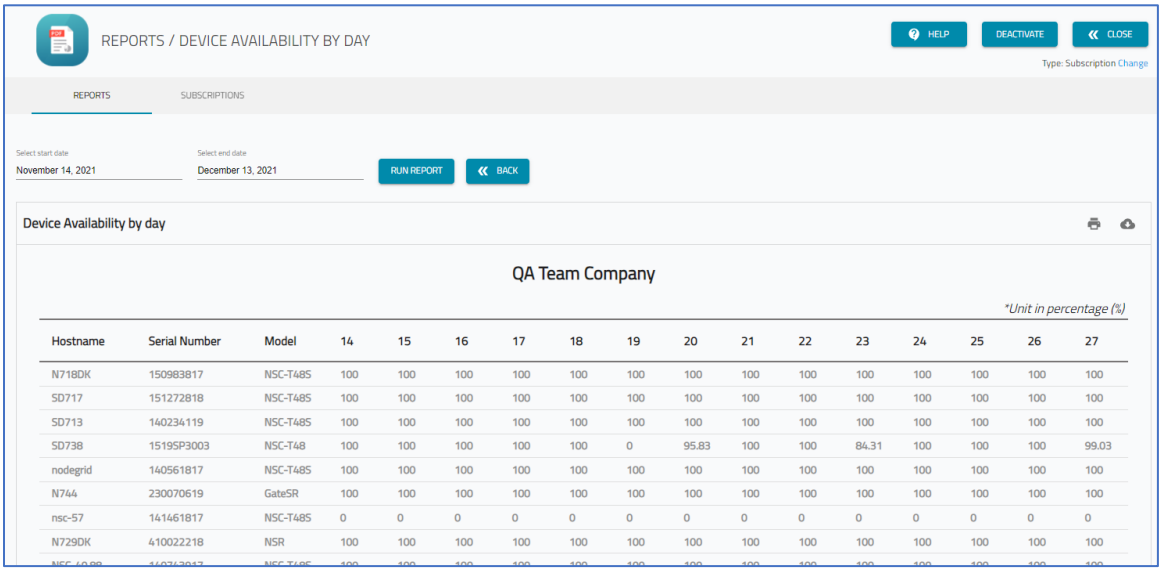
1. Go to *APPS :: ACTIVE :: REPORTS :: REPORTS*.
2. In the list, identify the needed report and click **Run**.



3. The dialog to set parameters displays.



4. Click in **Select start date** (displays calendar) and select a beginning date.
5. Click in **Select end date** (displays calendar) and select an end date.
6. Click **Run Report** (displays report on page).



Hostname	Serial Number	Model	14	15	16	17	18	19	20	21	22	23	24	25	26	27
N718DK	150983817	NSC-T48S	100	100	100	100	100	100	100	100	100	100	100	100	100	100
SD717	151272818	NSC-T48S	100	100	100	100	100	100	100	100	100	100	100	100	100	100
SD713	140234119	NSC-T48S	100	100	100	100	100	100	100	100	100	100	100	100	100	100
SD738	1519SP3003	NSC-T48	100	100	100	100	100	0	95.83	100	100	84.31	100	100	100	99.03
nodegrid	140561817	NSC-T48S	100	100	100	100	100	100	100	100	100	100	100	100	100	100
N744	230070619	GateSR	100	100	100	100	100	100	100	100	100	100	100	100	100	100
nsc-57	141461817	NSC-T48S	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N729DK	410022218	NSR	100	100	100	100	100	100	100	100	100	100	100	100	100	100

7. In upper right corner, select an export option: 

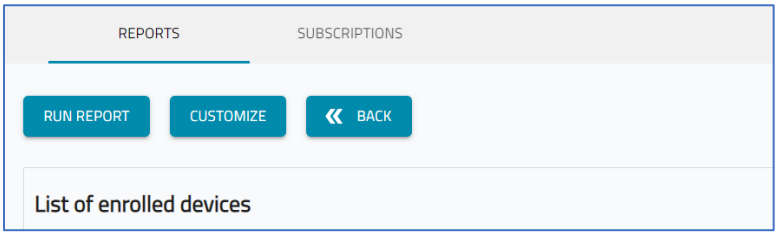
   To print report, click **Printer** icon 

   To save as a file, click **Download** icon 

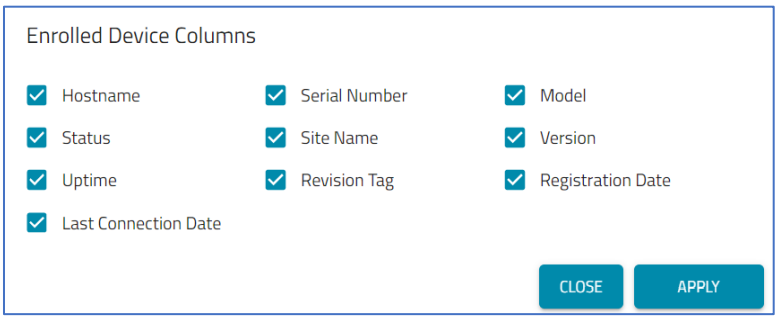
8. When done, click **BACK**.

Customize Reports

1. Go to *APPS :: ACTIVE :: REPORTS :: REPORTS*
2. Click on **Run** (displays dialog).



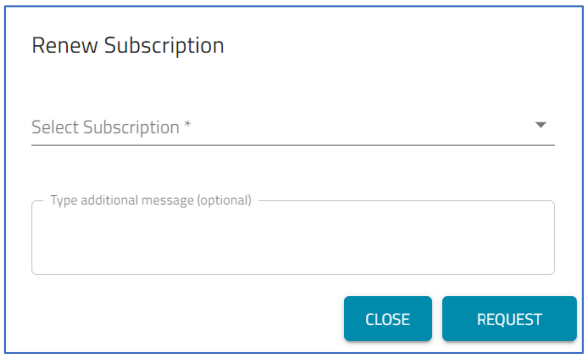
3. Click **CUSTOMIZE** (displays dialog). (If button is not shown, customization is unavailable.)



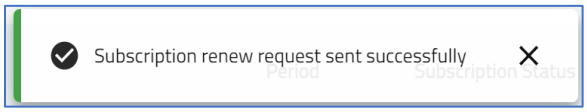
4. In the dialog, select appropriate items, then click **APPLY**.

Renew Subscription

1. Go to *APPS :: ACTIVE :: REPORTS :: SUBSCRIPTIONS*.
2. Click **Request Renew** (opens dialog).



3. On **Select Subscription** drop-down, select one.
4. (as needed) In **Type additional message (optional)**, add details.
5. Click **REQUEST** (displays success dialog).



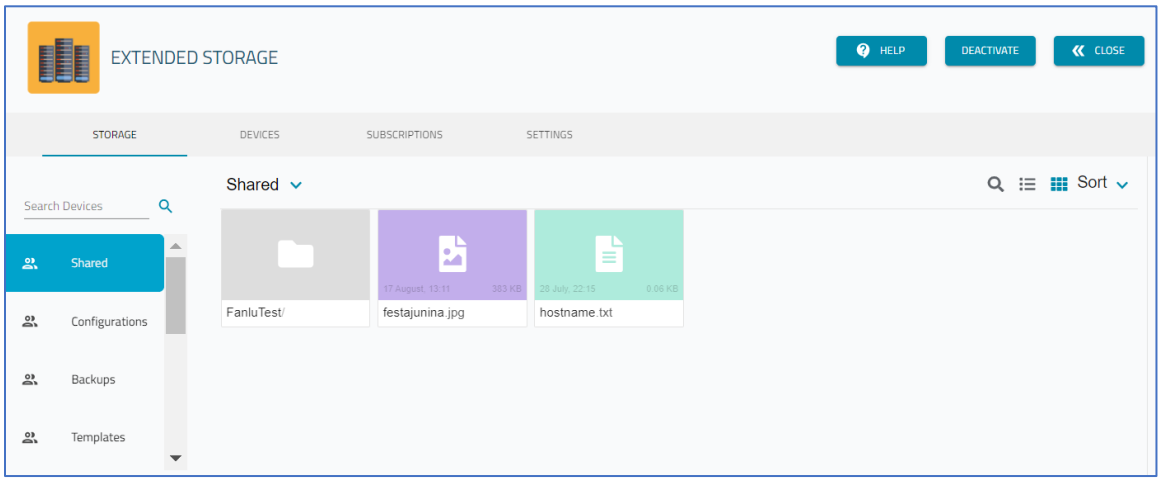
SD-WAN app

SD-WAN is a ZPE Cloud plugin application that manages Nodegrid SD-WAN configurations and topology. See Appendix B – SD-WAN User Guide.

Extended Storage app

STORAGE tab

This app allows storage on devices to be increased and managed. Files and folders for each available device can be viewed and organized.

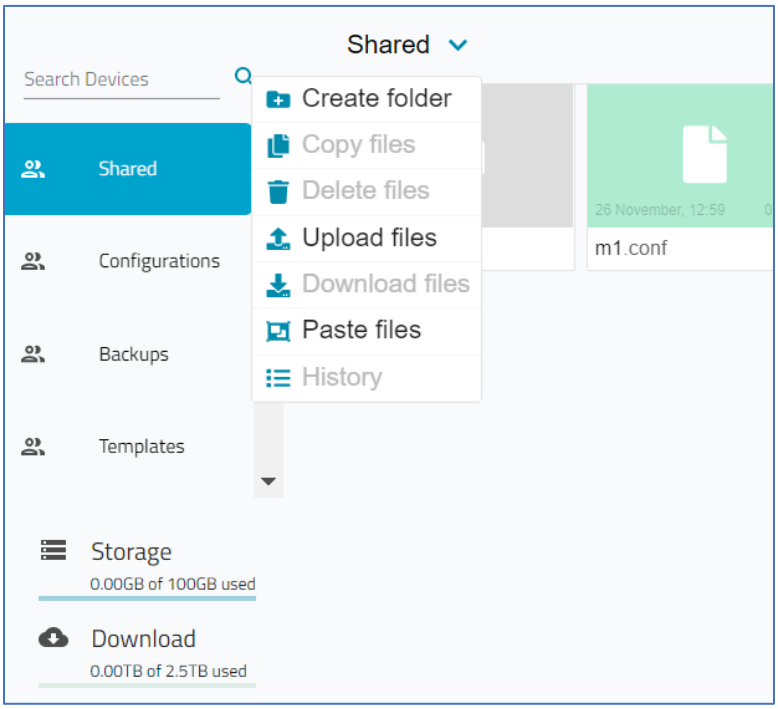


Extended Storage Functions

1. Go to *APPS :: ACTIVE :: EXTENDED STORAGE*.
2. The left panel provides management options:

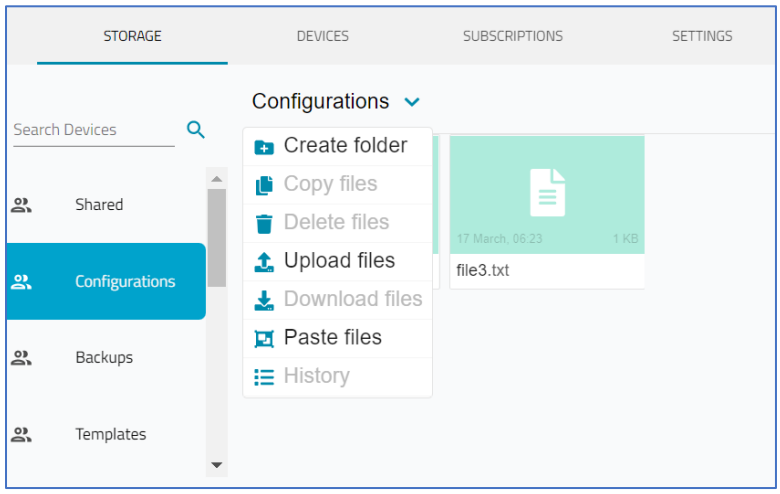
   Shared side-tab:

   Click **Shared** drop-down and select as needed.



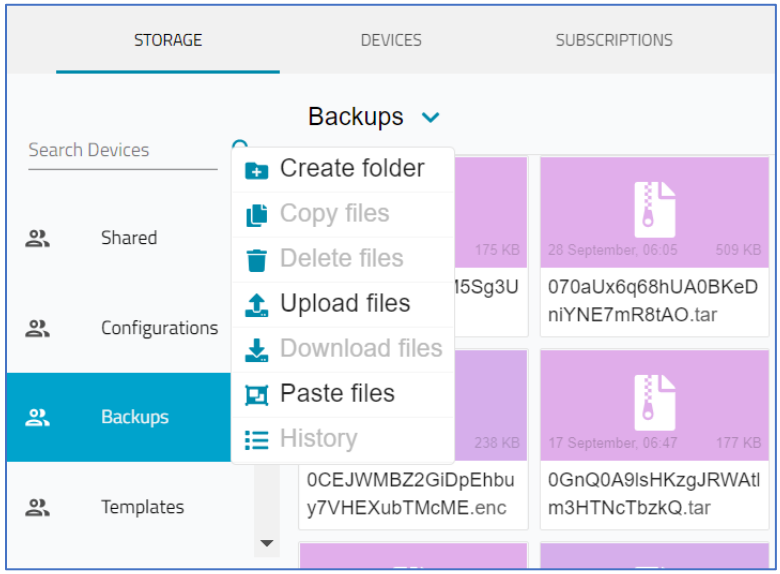
   Configuration side-tab

   Click **Configuration** drop-down and select as needed.



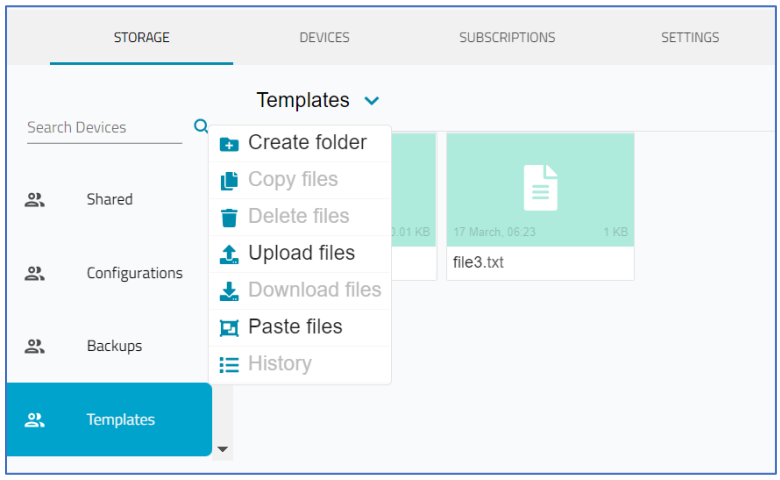
Backups side-tab

On the **Backups** drop-down, select as needed.



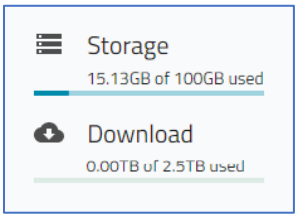
Templates side-tab

On **Templates** drop-down, select as needed.



Scrolling further down on the side panel shows the available enrolled devices.

Side Panel Status:



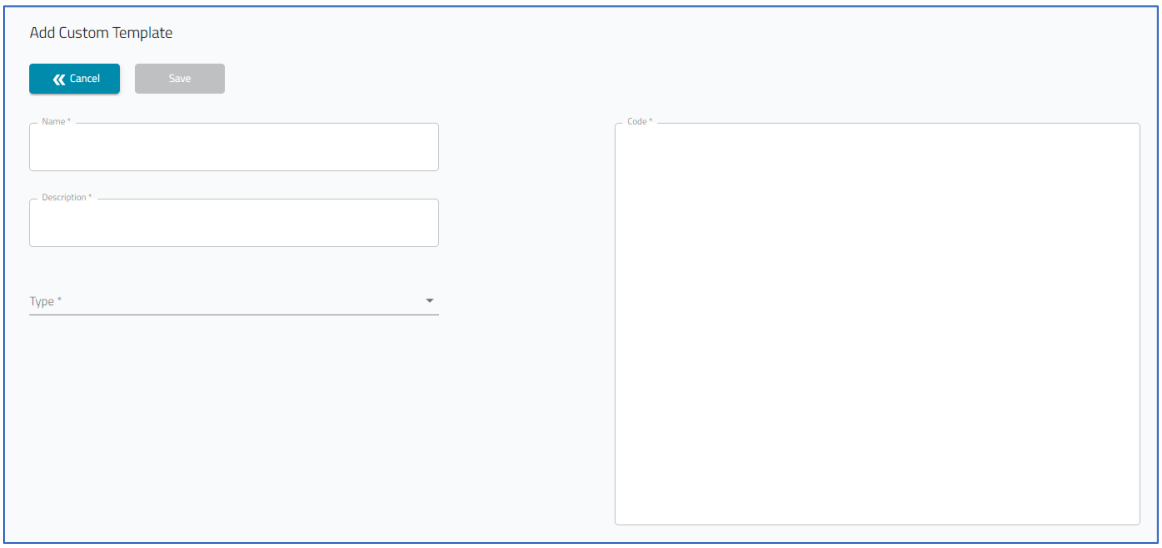
Storage shows used and available space.

Download shows amount of downloads and the maximum allowed.

Upgrade a Device with Extended Storage

Devices may be upgraded using a shared image placed within the Extended Storage application as follows: Following are options to manage extended storage.

1. Go to *APPS :: ACTIVE :: EXTENDED STORAGE*.
2. In left panel, click **Shared** side-tab (displays available folders.
3. On **Shared** drop-down, click **Upload Files** and select image and checksum files.
4. Go to *PROFILES :: TEMPLATE,* click **+Add** (opens dialog).



Enter **Name**.

Enter **Description**.

On **Type** drop-down, select **Script**.

In the **Code** textbox, paste the following block:

```
#!/bin/bash

# Check if image and checksum exists on Extended storage
if [ -f
/var/local/file_manager/remote_file_system/extended_storage/Shared/nodegrid.iso ] &&
   [ -f
/var/local/file_manager/remote_file_system/extended_storage/Shared/nodegrid.md5 ];
then

    # Files are located on Cloud storage, and it is better to download the files first
instead of use direct
    # inside the mounted folder
    cp /var/local/file_manager/remote_file_system/extended_storage/Shared/nodegrid.iso
/var/sw 2>/dev/null
    RET_ISO=$?
    cp /var/local/file_manager/remote_file_system/extended_storage/Shared/nodegrid.md5
/var/sw 2>/dev/null
    RET_MD5=$?
    if [ $RET_ISO != "0" ] || [ $RET_MD5 != "0" ]; then
        echo "Failed to copy files"
        exit 1
    fi

    ISO_MD5=$(md5sum /var/sw/nodegrid.iso | cut -d " " -f 1)
    ISO_CHECKSUM=$(cat /var/sw/nodegrid.md5 | cut -d " " -f 1)
```

```
    if [ $ISO_MD5 != $ISO_CHECKSUM ]; then
        echo "Failed to verify checksum"
        exit 1
    fi

    echo "Upgrading device..."
    upgrade_software --local /var/sw/nodegrid.iso

else
    echo "Not able to find image or checksum file"
    exit 1
fi
```

5. Click **Save**.
6. The script checks for the image and checksum within the shared folder, downloads both files to the target device, confirms the md5 checksum, and starts the upgrade process.

Access Extended Storage Folders (WebUI)

To access the extended storage folders directly on a Nodegrid device via the WebUI:

1. Log into the device.
2. Go to *System :: Toolkit* and click **File Manager**.
3. Open **remote_file_system** folder.
4. Open **extended_storage** sub-folder.
5. Two folders are available in this directory:

   Shared – this folder is shared between all company devices.

   Nameofdevice – this folder is only accessible by the device itself and the Extended Storage application on ZPE Cloud.
6. Review contents, as needed.

Access Extended Storage Folders (CLI)

The extended storage folder can be access with a terminal session.

1. Log into the device with the Console.
2. To connect to the target device via ssh with root permission, execute:

```
cd /var/local/file_manager/remote_file_system/extended_storage
```

3. The following options are available:

   List contents

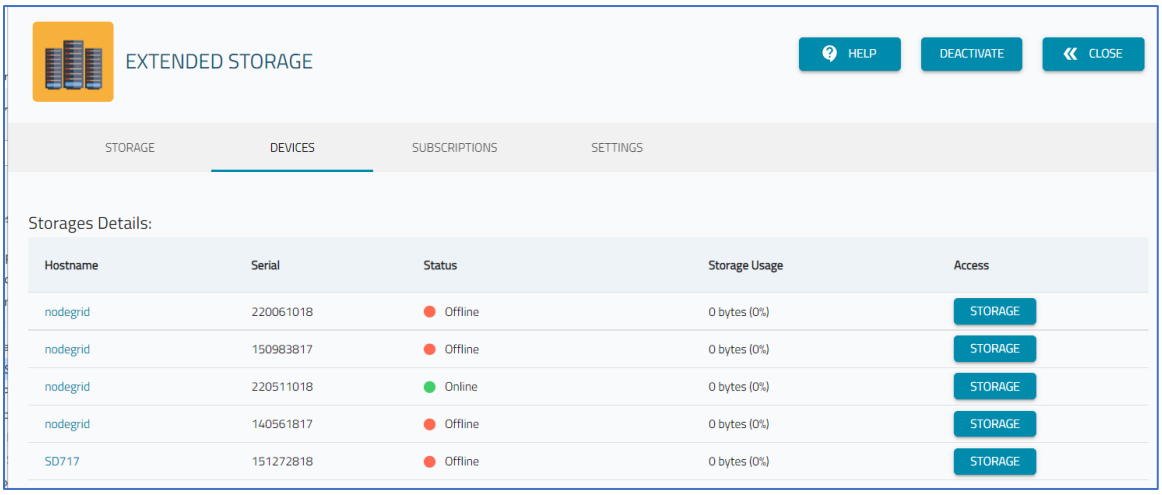
   Read or copy content from extended storage (triggers a download from cloud storage to the device)

Write or copy content from Nodegrid to extended storage (triggers an upload from the device to cloud storage)

4. The mv operation deletes the selected content from extended storage.

DEVICES tab

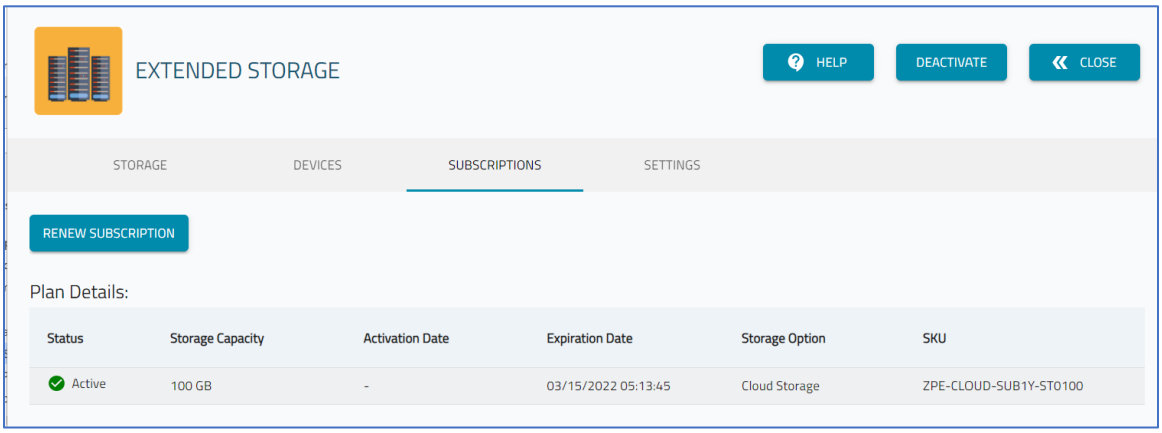
This tab presents storage details for individual devices.



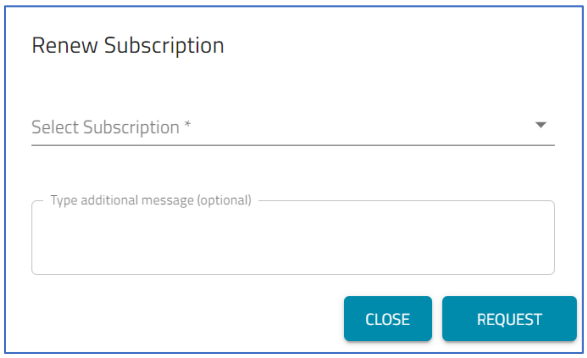
Click **STORAGE** to display device's folders/files (displayed on **STORAGE** tab).

SUBSCRIPTIONS tab

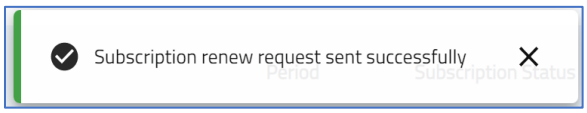
This displays current subscriptions and status details.



1. As needed, click **RENEW SUBSCRIPTION** (displays dialog).

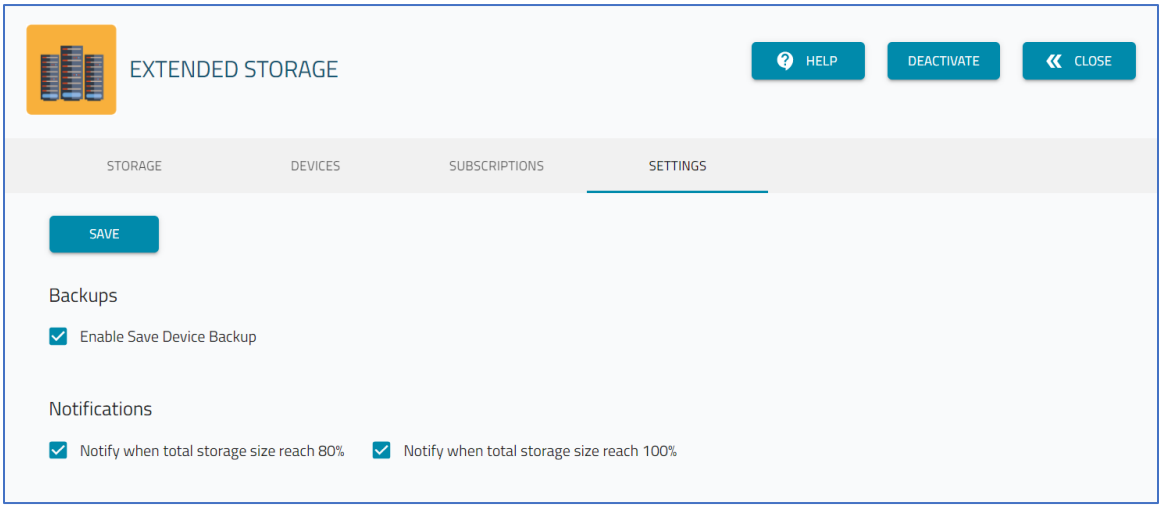


2. On **Select Subscription** drop-down, select one.
3. In **Type additional message (optional)** textbox, add details.
4. Click **REQUEST** (displays success dialog).



SETTINGS tab

This provides configuration options for extended storage.



To modify settings, make changes, as needed.

1. On *Backups* menu:

   Select **Enable Save Device Backup** checkbox.

2. On *Notifications* menu:

   Select **Notify when total storage size reach 80%** checkbox.

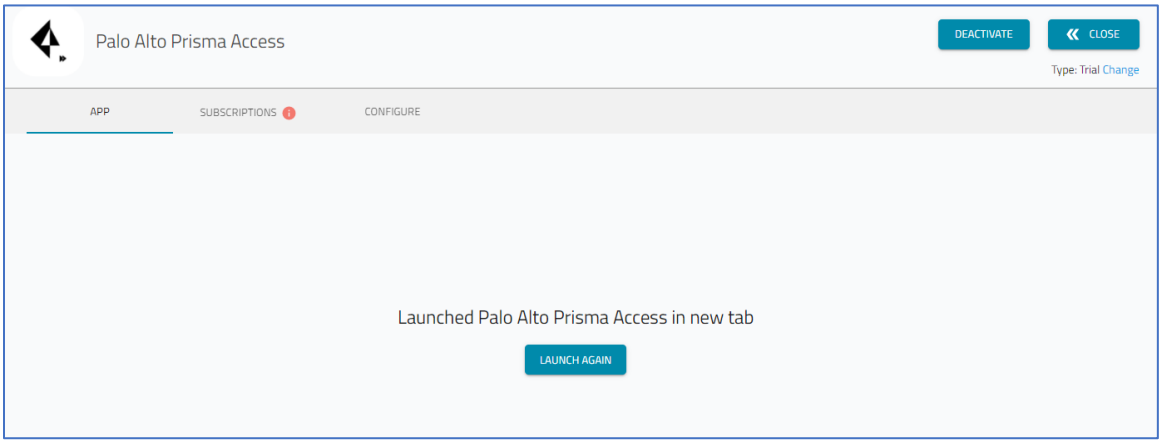
   Select **Notify when total storage size reach 100%** checkbox.

3. Click **SAVE**.

Palo Alto Prisma Access app

This app allows managing Palo Alto Prisma Access directly from ZPE Cloud.

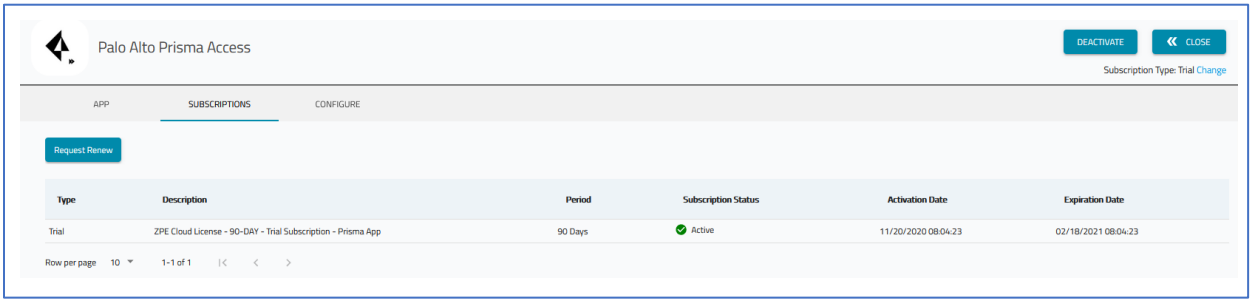
APP tab



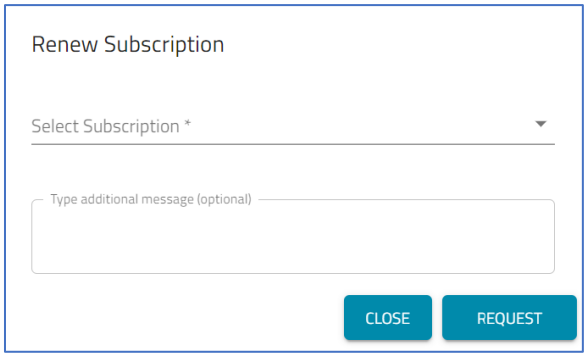
Palo Alto Prisma Access can now be directly launched from ZPE Cloud.

SUBSCRIPTIONS tab

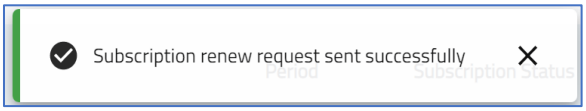
Prisma Access subscriptions are listed.



1. As needed, click **RENEW SUBSCRIPTION** (displays dialog).

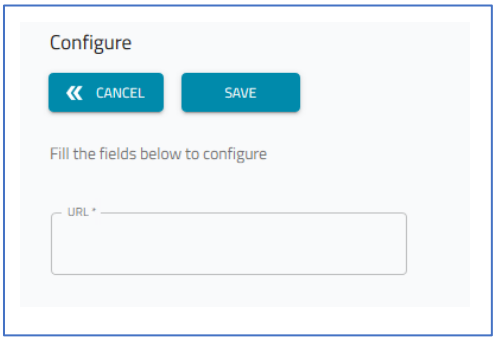


2. On **Select Subscription** drop-down, select one.
3. (as needed) In **Type additional message (optional)**, add details.
4. Click **REQUEST** (displays success dialog).



CONFIGURE tab

Displays configuration settings.



To modify settings:

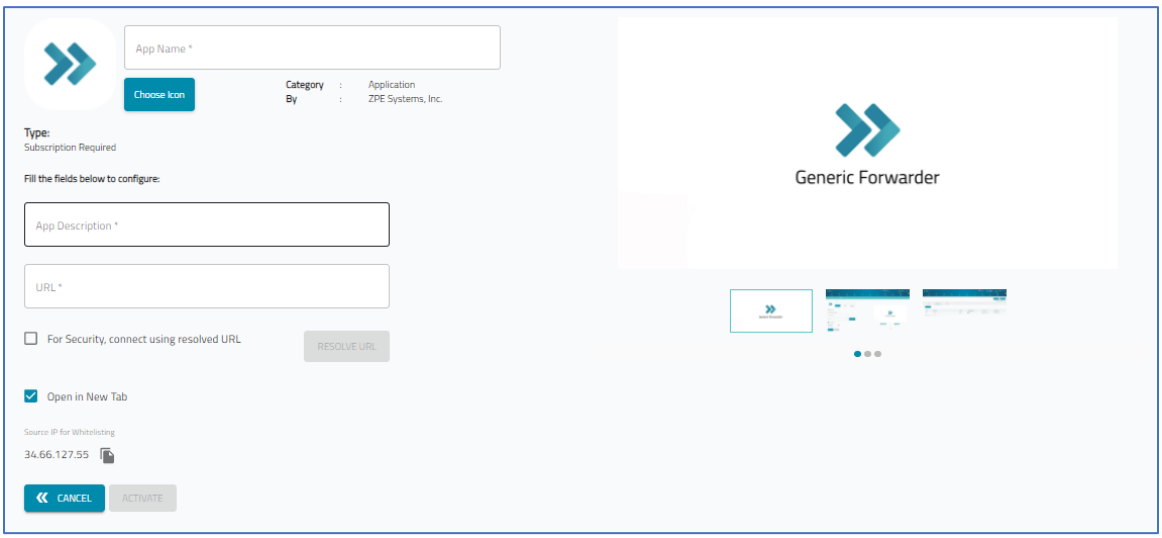
1. In **URL**, enter the *Prisma access* web address.
2. Click **SAVE**.

After configuration, when the app is accessed, the Prisma access page is opened.

NOTE: The app does not function until the Prisma access URL has been configured.

Generic Forwarder app

The generic forwarder app manages generic forwarders from the ZPE Cloud.



Create New Generic Forwarder

1. Go to *APPS :: ACTIVE :: GENERIC FORWARDER*.
2. Enter **App Name**.

3. To select a custom icon, click **Choose Icon**. (opens selection menu).
4. Enter a **Description**.
5. Select **For Security, connect using resolved URL** checkbox.

   Enter **URL** and click **Resolve URL**.
6. (optional) **Select Open in New Tab** checkbox.
7. Click **Activate**

   NOTE: The source IP is displayed for white-listing purposes. Click the icon next to the IP to copy it.

All created forwarders are available under *APPS ::ACTIVE* tab.

Nodegrid Data Lake app

The Nodegrid Data Lake application gathers device information from sensors, application stats, network traffic, data logs, system logs, events, bridges to third-party IoT devices. The dashboard presents visual representations of the metrics for quick evaluation of the represented infrastructure.

See Appendix C – Nodegrid Data Lake User Guide.

Appendix A - Nodegrid Manager

Nodegrid Manager simplifies networking jobs. Instead of juggling unique tools and UIs from an array of vendors, Nodegrid Manager puts all solutions under one umbrella. A single intuitive interface controls console servers, routers, PDUs, VMs, and everything on the network.

Install Nodegrid Manager

VMware vSphere

Virtual machine requirements:

EFI firmware

Host requirements:

vCenter Server 6.7 or later

Key Management Server (KMS)

External component requirements:

Computer running Windows with access to PowerCLI to execute commands on vCenter.

Key Management Server

Nodegrid Manager depends on vTPM features from VMware, and requires a Key Management Server installed on VMware's infrastructure. HyTrust is used in this tutorial, but other options can be chosen. The following link lists all the KMS options available for VMware.

https://www.vmware.com/resources/compatibility/search.php?deviceCategory=kms
Installing HyTrust KeyControl

NOTE: If a key management server is installed on the VMware infrastructure, skip to *Deploying Nodegrid Manager*.

1. Download the OVA package to the local computer and extract its contents.
2. Access the vSphere Client.
3. On the "Menu" drop-down. select Hosts and Clusters.
4. On the *Select an OVF template*" page:

   Select **Local file** checkbox.

   Click **Upload Files**.

   In the *Open* dialog, locate and select the HyTrust KeyControl OVF file

   Click **Next**.
5. On the *Select a name and folder* page:

   For **KMS**, enter a name.

   Enter the **VM location**.

   Click **Next**.
6. On the *Select a compute resource* page:

   Select the resource.

   Click **Next**.
7. On the *Review details* page:

   Review the entries.

   Click **Next**.
8. On the *License agreements* page:

   Read HyTrust's license agreement.

   Select **I accept all license agreements**.

   Click **Next**.
9. On the *Configuration* page:

Select the best suited configuration.

Click **Next**.

10. On the *Select storage* page:

    Choose the best suited storage.

    Click **Next**.

11. On the "*Select networks*" page:

    Enter a destination network.

    Click **Next**.

12. On the *Customize template* page:

    For **Host IP address**, enter a static IPv4 address (cannot be changed after node is deployed).

    Enter **Hostname** (alphanumeric & hyphens only) (cannot be changed after node is deployed).

    Enter **Domain Name** (alphanumeric & hyphens only).

    Enter **Netmask** (can change later).

    Enter **Gateway** (can change later).

    Enter **DNS servers** (i.e., 8.8.8.8)

    Click **Next**.

13. On the "*Ready to complete*" page:

    Review the displayed information.

    Click **Finish**.

VMware starts the deployment process. This takes time, due to the size of the HyTrust image.

Configure the KeyControl Node

1. Access the vSphere Client.
2. Power on the HyTrust VM.
3. For the KeyControl system's admin account, enter the password ("htadmin").
4. Review the confirmation dialog (URL of KeyControl web GUI)

   Press Enter to finish the installation.
5. On the browser, enter **https://<node-ip-address>**
6. On the *HyTrust KeyControl Login* page, for username and password, enter **secroot**.
7. Review the EULA, then click **I Agree** (accepting the license terms).
8. On the *Welcome to KeyControl* page, click **Continue as Standalone Node**.
9. On the *Change Password* page:

Enter a new **Password**.

Click **Update Password**.

10. On the "*Configure E-Mail and Mail Server Settings*" page:

    Specify email settings.

    Click **Continue**.

11. On the *Download Admin Key* page:

    Click **Download** (saves the admin key locally).

    Click **Continue**.

12. On the "*Automatic Vitals Reporting*" page:

    As needed, enable/disable **Automatic Vitals Reporting**.

    Click **Continue**.

13. On the top bar, click **KMIP**.

14. On the **Basic**" tab, select:

    For **State**, set to **ENABLED**.

    For **Protocol**, set to **Version 1.1**.

    Click **Apply**.

This completes the KeyControl Node configuration.

Configure KMS

1. Access the vSphere Client with an account with administrator permissions.
2. On the **Menu** drop-down. select **Hosts and Clusters**.

   In the **Host and Clusters** list, click the vCenter's machine.
3. On the **Configure** tab, in *Security* menu, click **Key Providers**.
4. Click **Add Standard Key Provider**.

   In **Name**, enter name of the key providers.

   In **KMS**, enter the name of the key management server.

   Enter the **IP address** (defined earlier for HyTrust KeyControl).

   In **Communication Port**, enter a value (default: 5696).

   Click **ADD KEY PROVIDER**.
5. Verify displayed details, then click **TRUST**.

   Select the **Key Provider** (created on the first list).

   Select the **KMS** (created on the second list).

On the **Establish Trust** drop-down., select **Make KMS trust vCenter**.

6. In the *Choose a method* page:

   Select **New Certificate Signing Request (CSR)**.

   Click **Next**.

7. Click **Submit CSR to KMS**.

   Click **Download**.

   Click **Done**.

8. To access the HyTrust web GUI, enter the URL: **https://<node-ip-address>**
9. On the top bar, click **KMIP**.

   On **Client Certificates** tab, **Actions** drop-down, click **Create Certificate**.

10. On the *Create a New Client Certificate*" page:

    Type a **Name** for the certificate

    Click **Load File**.

    Locate and select the certificate (downloaded earlier on vSphere).

    Click **Create**.

11. Select the new certificate.
12. On the **Actions** drop-down, click **Download Certificate**.

    Download and unpack the zip file.

13. On the **ESTABLISH TRUST** drop-down, click **Upload Signed CSR Certificate**.
14. Click **UPLOAD FILE**.

    Search for the pem file (extracted with the name given previously).

    Click **UPLOAD**.

After completion, **Connection Status** of the key provider should show as **Connected**.

Deploy Nodegrid Manager

Create a New VM

1. Access the vSphere Client.
2. Upload NGM's iso image to vCenter storage.
3. On **Menu** drop-down., select **Hosts and Clusters**.

   On the **Actions** drop-down., select **New Virtual Machine**.

   Click **Next**.

4. On the *Select a creation type* page:

Select **Create a new virtual machine**.

Click **Next**.

5. On the *Select a name and folder* page:

   Enter a **Name** for the VM.

   Select the **Location** for the new VM.

   Click **Next**.

6. Inside the *Select a compute resource* page:

   Select the **Destination Compute Resource**.

   Click **Next**.

7. On the *Select storage* page:

   Select the Storage Configuration.

   Click **Next**.

8. Inside the "*Select compatibility*" page:

   On the "Compatible with" drop-down., select "ESXi 6.7 and later"

   Click **Next**.

9. Inside the "*Select a guest OS*" page:

   On the Guest OS Family drop-down, select Linux.

   On the Guest OS Version drop-down, select "Other 4.x or later Linux (64-bit)"

   Click **Next**.

10. On the *Customize hardware* page, **Virtual Hardware** tab, select:

    CPU = 2

    Memory = 4GB

    New Hard disk:

    Size = 32GB

    Virtual device node = IDE 0

    On *New CD/DVD Drive - Datastore ISO File*:

    Select the uploaded iso image.

    Select **Connected at power on** checkbox.

    To create a second network adapter, on *Add new device*, select **Network Adapter**.

    Under *New network*, for both network adapters, enter **Adapter type = E1000E**.

11. On the *Customize hardware* page, **VM Options** tab:

Under *Boot options* select:

Firmware = EFI

Secure boot = disabled

Click **Next**.

12. On *Ready to complete* page:

    Review the VM configuration details.

    Click **Finish**.

This configures the VM.

Configure vTPM

1. On a Windows machine, open **PowerCLI**.
2. Install the **VMware A**PI.
3. Download **VMware cmdlet**.
4. Execute:

   ```
   save-module -Name VMware.PowerCLI -Path C:\folder\path\
   ```

5. To install VMware, execute:

   ```
   install-module VMware.PowerCLI -Scope CurrentUser
   ```

6. If the server does not have a certificate, it is possible to disable the certificate validation

   ```
   set-PowerCLIConfiguration -InvalidCertificateAction Ignore -Confirm:$false
   ```

7. To connect to vCenter, execute

   ```
   connect-VIServer <vCenter-ip-address>
   ```

8. Enter the administrator credentials for the VMware API.
9. To list all VMs on vCenter, execute:

   ```
   get-VM
   ```

10. To add a TPM device to the VM, execute the following commands:

```
$VMname = "<VM-name>"
$spec = New-Object VMware.Vim.VirtualMachineConfigSpec
$spec.DeviceChange = New-Object VMware.Vim.VirtualDeviceConfigSpec[] (1)
$spec.DeviceChange[0] = New-Object VMware.Vim.VirtualDeviceConfigSpec
$spec.DeviceChange[0].Device = New-Object VMware.Vim.VirtualTPM
$spec.DeviceChange[0].Device.DeviceInfo = New-Object VMware.Vim.Description
$spec.DeviceChange[0].Device.DeviceInfo.Summary = 'Trusted Platform Module'
$spec.DeviceChange[0].Device.DeviceInfo.Label = 'Trusted Platform Module'
$spec.DeviceChange[0].Device.Key = -1
$spec.DeviceChange[0].Operation = 'add'
$_this = Get-VM $VMname | Get-View
$_this.ReconfigVM_Task($spec)
```

11. Access the vSphere Client. If the task was completed properly, on "Recent Task" list, this action is listed.

Install Nodegrid Manager

1. Access the **vSphere Client**.
2. On the **Menu** drop-down, select **Hosts and Clusters**.
3. On the **Hosts and Clusters** list, select the **Nodegrid Manager VM**.
4. On the **Actions** drop-down, click **Power**.
5. Click **Power On**.
6. Click **Launch Web Console**.
7. On **Type your choice**: enter **Accept-efi**.
8. On **Please select an install target or press n to exit**, type sda.

   Wait for the installation to complete
9. When complete, **Power off** the VM
10. On the VM, go to **Edit Settings**.
11. Under *CD/DVD Media*, unselect **Connect At Power On** checkbox.
12. **Power On** the VM.

    Wait the boot process to finish.
13. Login with username **admin** and password **admin**.
14. To retrieve the IP address, execute:

    ```
    show /system/routing_table/
    ```
15. To change "admin" password, execute:

    ```
    cd settings/local_accounts/admin/
    change_password
    ```

VMware Workstation

This information creates a Nodegrid Manager VM on VMware Workstation. To secure communication, NGM requires a virtual Trusted Module Platform (vTPM).

NOTE: Nodegrid Manager does not require a physical TPM chip installed on the host computer.

Virtual Machine Requirements:

EFI Firmware

Host Requirements:

VMware Workstation Pro 14.0 or later

Deploy Nodegrid Manager on VMware Workstation

1. Open VMware Workstation.
2. In the **File** drop-down menu, click **New virtual machine...**

   This starts the VM wizard.
3. On the dialog:

   Select Custom (advanced)

   Click **Next**.
4. On *Hardware compatibility* page:

   Select **Workstation 14.x** (or later releases).

   Click **Next**.
5. On the dialog:

   Select **Installer disc image file (iso)**.

   Locate and select the Nodegrid image iso file

   Click **Next**.
6. On the dialog:

   On "**Guest operating systems**, select **Linux**.

   On **Version**, select **Other linux 4.x kernel 64-bit**.

   Click **Next**.
7. On the dialog:

   Enter **Virtual machine name**.

   Select the **Location**.

   Click **Next**.
8. On the dialog:

For **Number of Processes**, enter **2**.

Click **Next**.

9. On the dialog:

   For **Memory for this virtual machine**, select **4096Mb**.

   Click **Next**.

10. On the dialog:

    Select **Use network address translation (NAT)** checkbox.

    Click **Next**.

11. On the dialog:

    For I/**O Controller Types**, select **LSI Logic**.

    Click **Next**.

12. On the dialog:

    For **Virtual Disk Type**, select **SCSI**.

    Click **Next**.

13. On the dialog:

    Select **Create a new virtual disk** checkbox

    Click **Next**.

14. On the dialog:

    For **Maximum Disk size**, select **32Gb**

    Click **Next**.

15. On the dialog (no changes, click **Next**.

16. On the dialog, click **Finish**.

17. On *Library* view, locate the created VM.

    Select the VM.

    Right click and select **Settings**.

18. On **Options** tab:

    On the *Advanced* menu, for **Firmware Type**, select **UEFI**.

    On *Access control*, menu, click **Encrypt**.

    Enter a **Password**.

    Click **Encrypt**.

19. On **Hardware** tab:

Click **Add**.

Select **Trusted Platform Module** checkbox.

Click **Finish**.

Click **Ok**.

20. Right-click the VM:

    Select **Start**.

    Go to **Power**.

    Go to **Start Up Guest**.

21. Follow the Nodegrid installation wizard.
22. On command window, execute:

    ```
    accept-efi
    ```

23. Execute:

    ```
    sda
    ```

    Wait the installation to finish

24. Power off the VM.
25. On the VM settings:

    Go to *CD/DVD* menu.

    Disable **Connected on power on** checkbox.

    Click **OK**.

26. Power up the VM.

Enroll Nodegrid Manager to ZPE Cloud

WebUI/CLI Procedure

1. Access ZPE Cloud.
2. Enter credentials on the login page.
3. To get enrollment information, go to the SETTINGS :: ENROLLMENT:: CLOUD.
4. To access the vSphere Client, on the "Menu" drop-down. select "Hosts and Clusters"
5. On the list of "Hosts and Clusters", select the Nodegrid Manager VM
6. Click on "Launch Web Console"
7. Enter admin credentials
8. To enable ZPE Cloud

   ```
   cd settings/zpe_cloud
   ```

```
set enable_zpe_cloud=yes
```

9. To enable the remote access feature:

```
set enable_remote_access=yes
commit
```

10. To enroll device

```
cloud_enrollment
set customer_code=xxxx
set enrollment_key=xxxxxx
```

11. if enrolling the device in one on-premise instance of ZPE Cloud:

```
set url=https://xxxx
commit
```

Enroll Device on ZPE Cloud

WebUI Procedure

1. Log into ZPE Cloud.
2. To get enrollment information, go to *SETTINGS :: ENROLLMENT :: CLOUD*.
3. On the device's IP address, open the Nodegrid Manager to access the device WebUI.

Enable ZPE Cloud on Device

WebUI Procedure

1. Go to *Security :: Services*.
2. Select **Enable ZPE Cloud** checkbox.
3. To enroll device in a single on=premise instance of ZPE Cloud, select **Enable Remote Access** checkbox.
4. Click **Save**.

Enroll Device in ZPE Cloud

WebUI Procedure

1. Go to *System :: Toolkit*.
2. Click **Cloud Enrollment**.
3. Enter **Customer Code**.
4. Enter "**Enrollment Key**".
5. If device is enrolled in one on-premise instance of ZPE Cloud, add the **On-premise URL**.
6. Click **Enroll**.

Appendix B – SD-WAN User Guide

SD-WAN is a ZPE Cloud plugin application. Use this to configure device network topologies (mesh or hub-spoke configurations).

Activate SD-WAN App

The SD-WAN application is located in the APPS Section. If not available, contact ZPE Systems Support (support@zpesystems.com) to enable it.

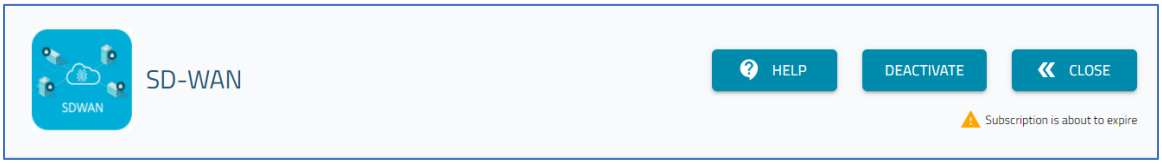
1. To activate SD-WAN, go to *APPS* section.
2. Click the **SD-WAN** icon.

3. This initiates the activation process.

4. When finished, click the **SD-WAN** icon to access the application.

5. This displays the *SD-WAN* home page (*DASHBOARD :: MAP*).

SD-WAN Banner



HELP (opens the SD-WAN User Guide section of the ZPE Cloud user document.

DEACTIVATE (shuts down the SD-WAN app and removes all configurations).

Click **DEACTIVATE**.

On the pop-up confirmation dialog, click **DEACTIVATE**.

CLOSE (closes the SD-WAN app and returns to the APP section root).

SD-WAN Setup Process

This is a general process to configure SD-WAN.

NOTE: Ensure GPS is enabled on devices. This ensures the location is displayed on the geographical map.

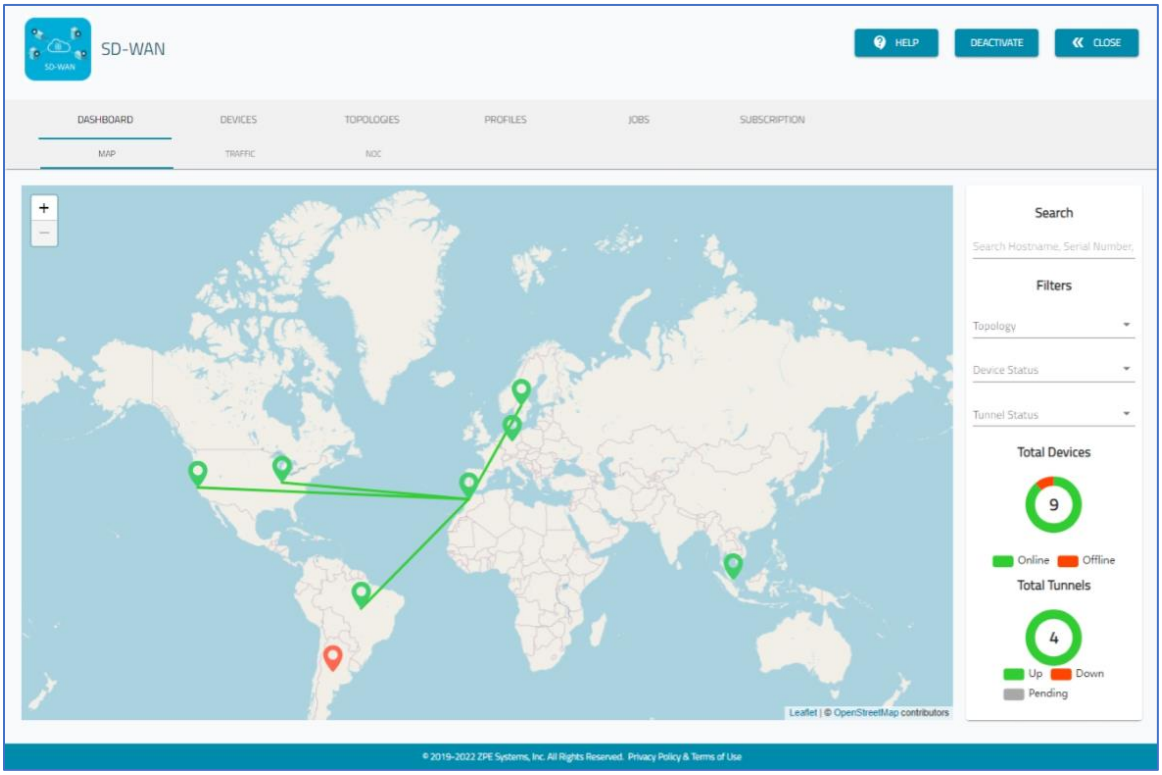
1. Enable devices for SD-WAN (*APPS :: ACTIVE :: SD-WAN :: DEVICES*).
2. Create a Topology (*APPS :: ACTIVE :: SD-WAN :: TOPOLOGIES*).
3. Add enabled devices to a Topology (*APPS :: ACTIVE :: SD-WAN :: DEVICES*)..
4. (optional) Create a Link Profile (*APPS :: ACTIVE :: SD-WAN :: PROFILE :: LINKS*).
5. (optional) Create a Network Profile (*APPS :: ACTIVE :: SD-WAN :: PROFILE :: NETWORKS*).

DASHBOARD :: MAP tab

The Map page presents a geographic representation of the SD-WAN topologies.

A colored pin shows the geographical position of each device based on coordinates. These coordinates are defined by the device's coordinates (set on the device – see *System :: Preferences :: Coordinates*). Pin color: green (online), red (offline), yellow (failover).

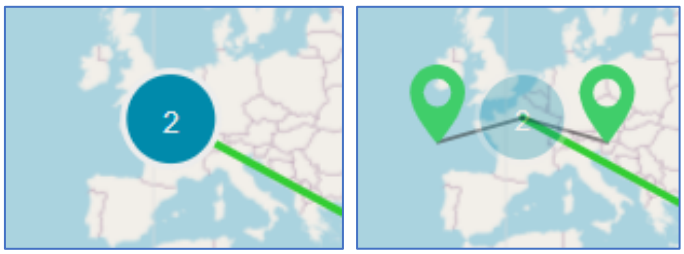
The lines connecting each pin represents tunnels, created when a device is added to a topology. Line color: green (tunnel is up), red (tunnel is down), grey (tunnels in pending state – indicates device has a configuration situation that prevents use).



Manage Map Details

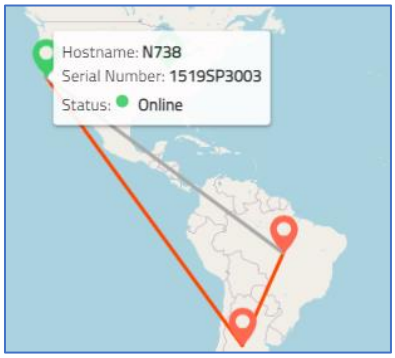
View Double-Device Location Details

When multiple devices are located in the same location, the map shows a circle with a number. Click the circle to expose the device markers. Click the markers to show details.



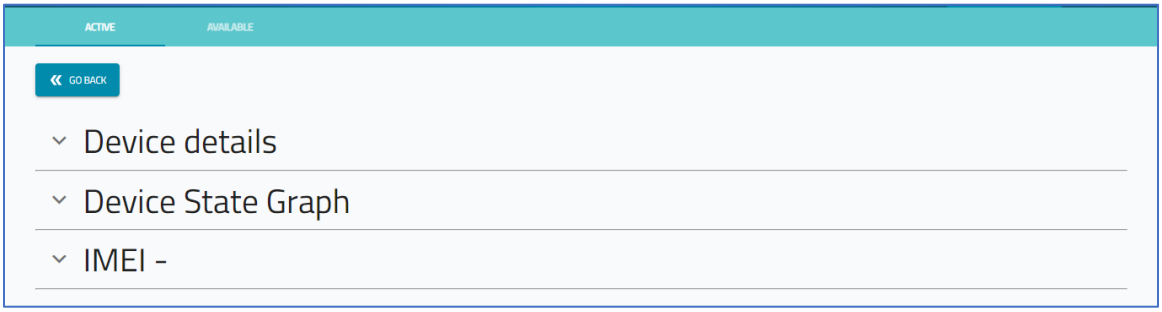
View Location Details

To view details on a location, hover over the marker.



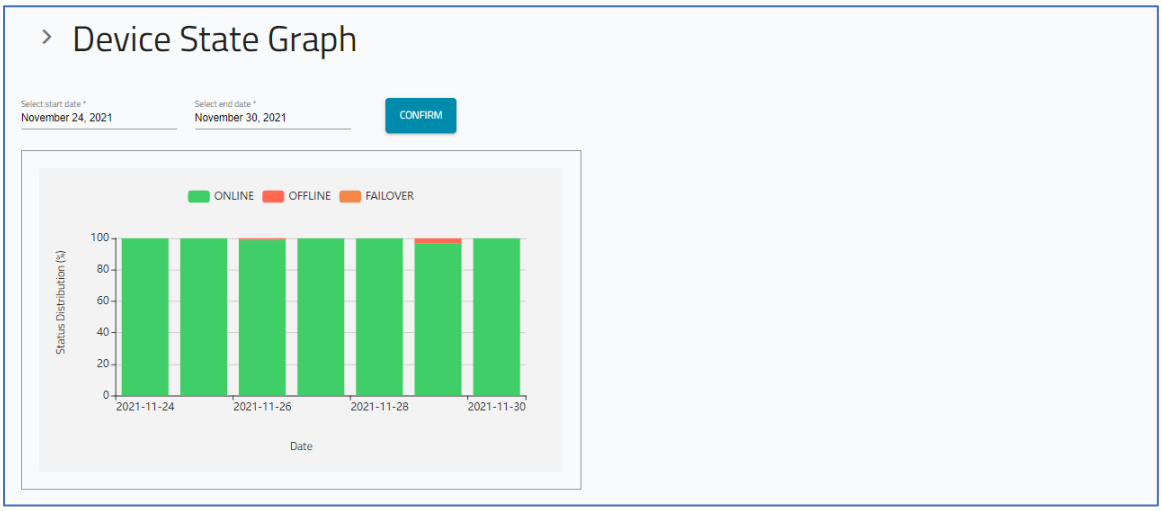
View Device Details on Map

To view device details, click on the marker. To return, click **GO BACK**.



To display **Device details**, click the down arrow (left side).

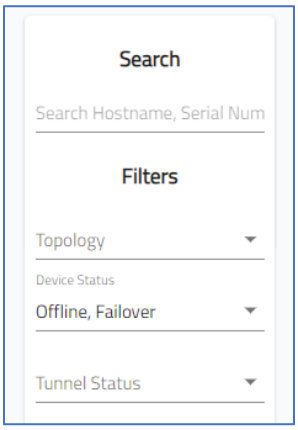
To view **Device State Graph** information, click the down arrow (left side).



To view **IMEI** details, click the down arrow (left side).

Search function

On the right side of the page is the *Search* function. This identifies devices that match the search conditions.



1. Go to *APPS :: ACTIVE :: SD-WAN :: DASHBOARD :: MAP*.
2. In the **Search** field, enter text.
3. In *Filters*: (conditions to apply to the search).

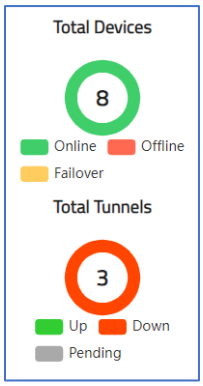
   On **Topology** drop-down, select a specific topology.

   On **Device Status** drop-down, select one or more items. Options are: **Online**, **Offline**, Failover (click to select, click again to unselect).

   On **Tunnel Status** drop-down, select one or more items. Options are: **UP**, **DOWN** (click to select, click again to unselect).
4. The table list adjusts according to the selections.

Status

At lower right of page, is the status indicators: *Total Devices* and *Total Tunnels*. The color legend indicates status.

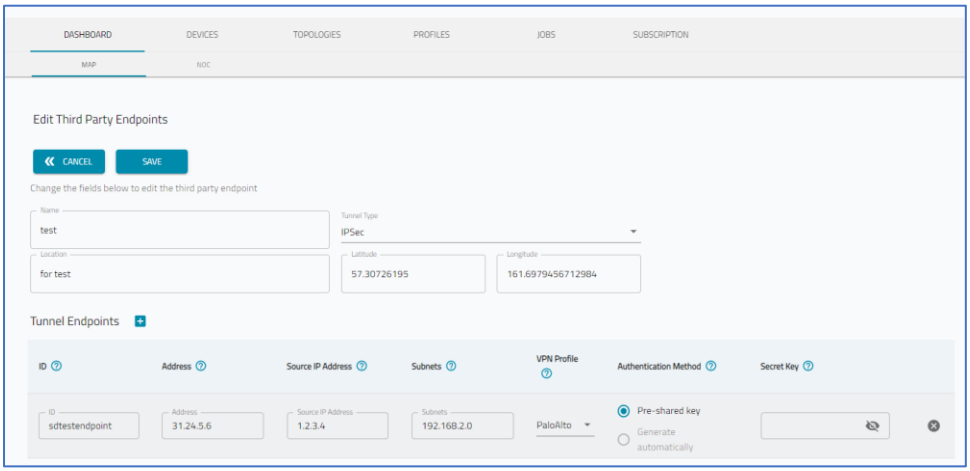


Total Devices reports the number of enrolled devices with SD-WAN support. Pie chart displays proportion of devices for each status: Online, Offline, Failover.

Total Tunnels identifies number of tunnels for all topologies. Pie chart displays the proportion of tunnels for each status: Up, Down, Pending.

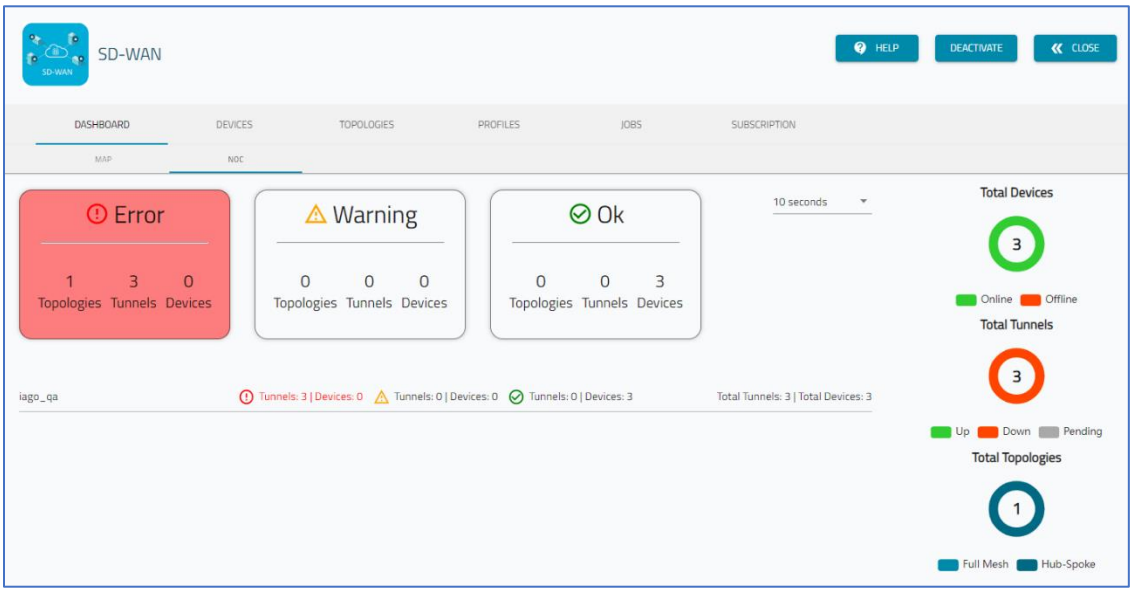
Click on a 3rd Party Device

3rd party devices are shown on the map. When the device marker is clicked, the Edit Third Party Endpoints dialog displays.



DASHBOARD :: NOC tab

This tab shows NOC status messages: Error, Warning, OK.



Types of Incidents

Errors:

Topologies: number of topologies with an error

Tunnels: number of tunnels with an error

Devices: number of devices with an error

Warning:

Topologies: number of topologies with a warning condition

Tunnels: number of tunnels with a warning condition

Devices: number of devices with a warning condition

OK:

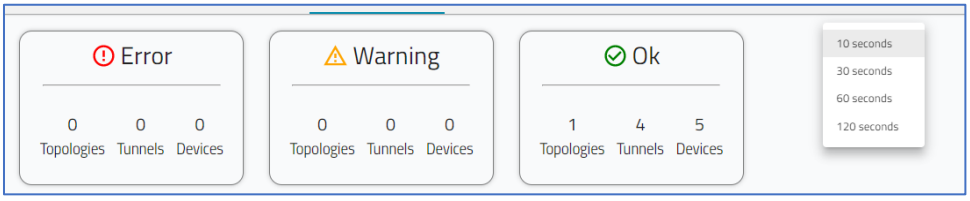
Topologies: number of operational topologies

Tunnels: number of operational tunnels

Devices: number of operational devices

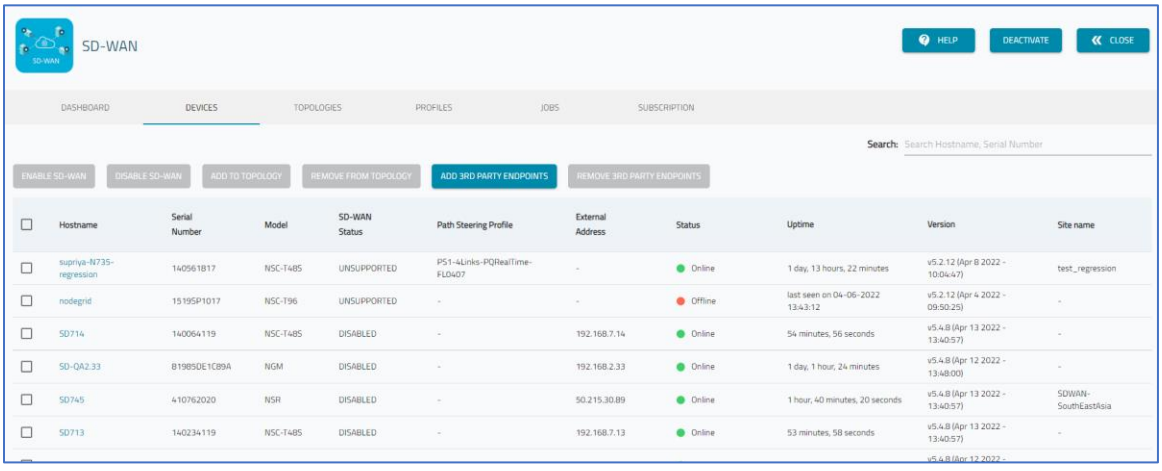
Change Timing of Reporting Intervals

Click the **Timing** drop-down to select reporting intervals in seconds: 10, 30 60 120



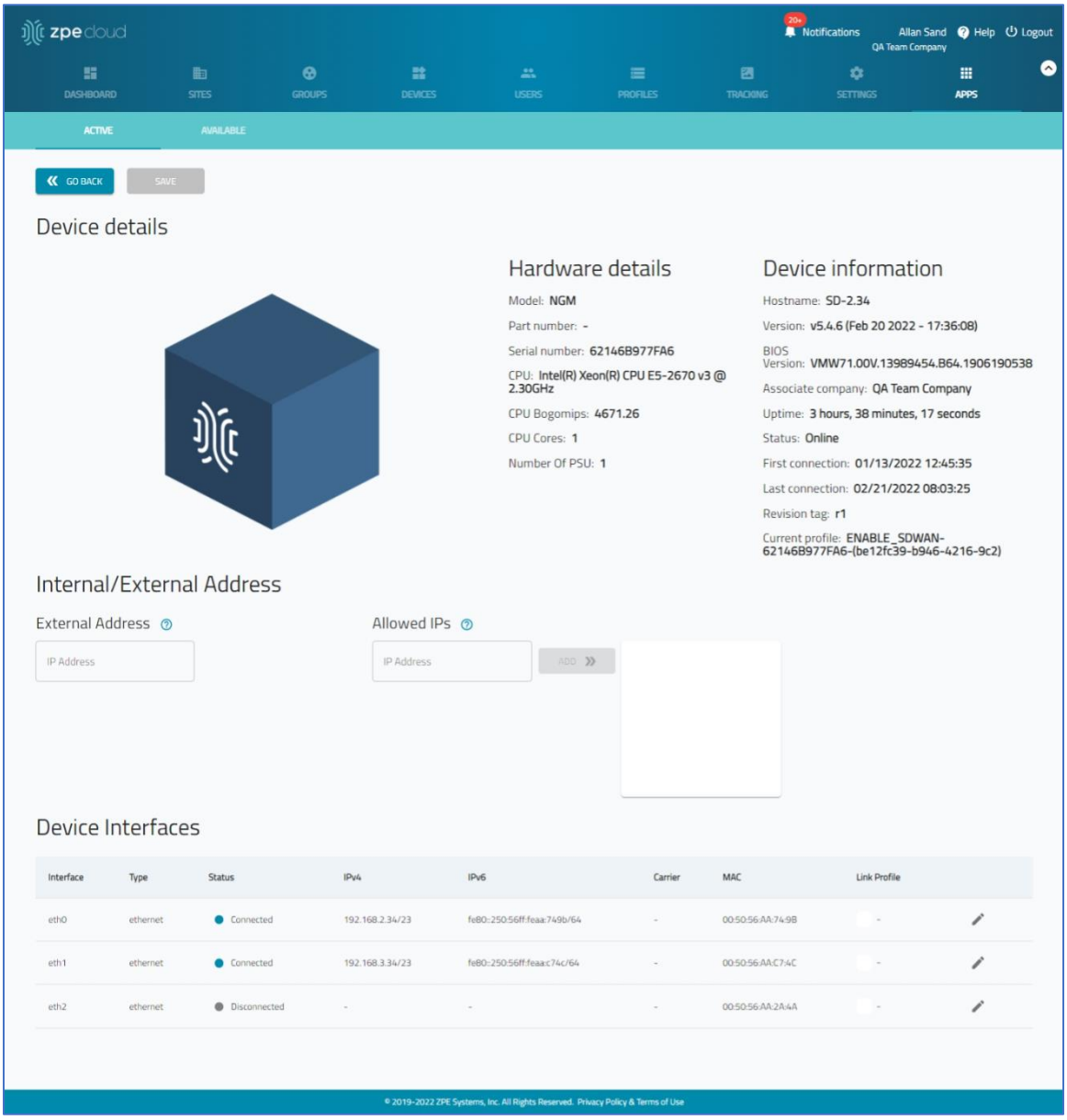
DEVICES section

Page lists devices that support SD-WAN with basic details.



Review Device Details

1. To access device details, click the Hostname (displays dialog).



2. In the *Internal/External Address* menu:

   As needed, change **External Address**.

   As needed, enter **Allowed IPs** (comma separated list).

3. In the *Device Interfaces* menu:

   In the table, at the far right, click the **Pencil** icon.

   On the *Link Profile* column, in the drop-down, select one.

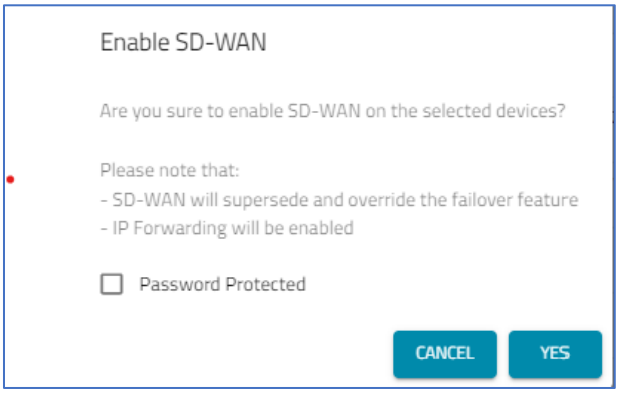
   Click the green checkmark icon.

4. If changes are made, click **SAVE**.

Manage Devices

Enable SD-WAN Device

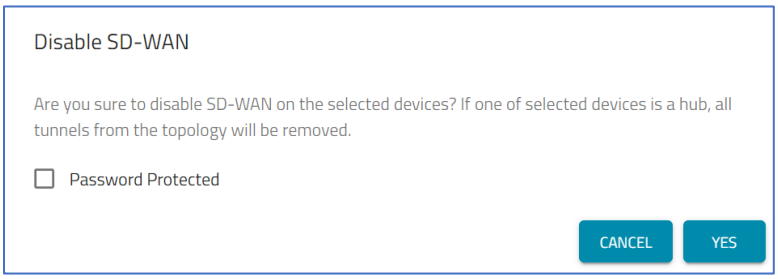
1. Go to *APPS :: ACTIVE :: SD-WAN :: DEVICES*.
2. On the list, identify a device (on column *SD-WAN Status*, device listed as *DISABLED*), and select checkbox.
3. Click **ENABLE SD-WAN** (displays dialog).



4. (optional) Select **Password Protected** checkbox. Then enter **Password**.
5. Click **OK**

Disable SD-WAN Device

1. Go to *APPS :: ACTIVE :: SD-WAN :: DEVICES*.
2. On the list, identify a device (on column *SD-WAN Status*, device listed as *ENABLED*), and select checkbox.
3. Click **DISABLE SD-WAN** (displays dialog).

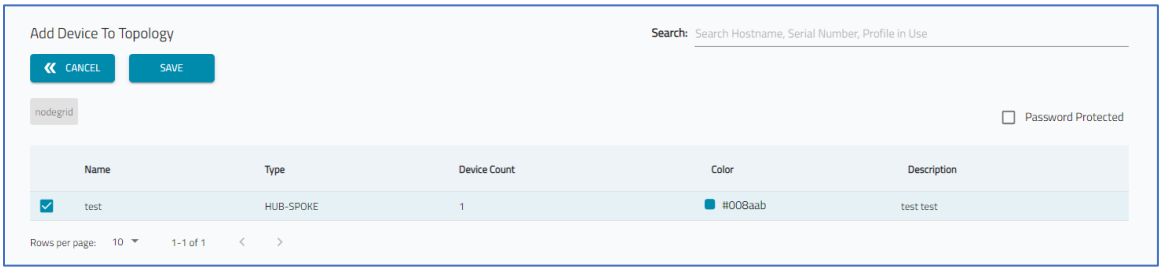


4. (optional) Select **Password Protected** checkbox.
5. Click **YES**.

Add to Topology

1. Go to *APPS :: ACTIVE :: SD-WAN :: DEVICES*.
2. On the list, identify a device to be associated with a Topology.

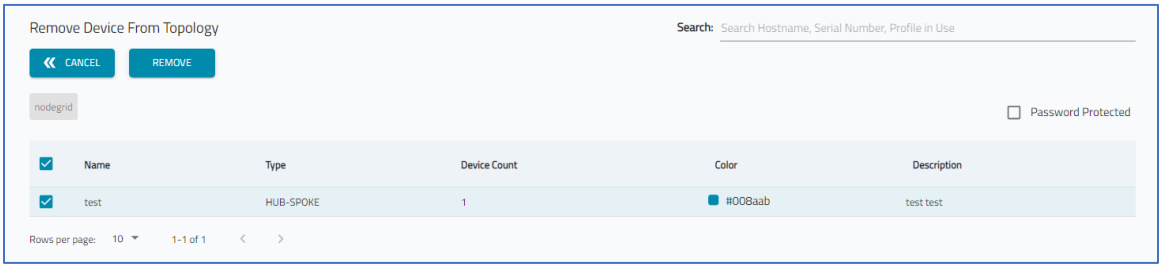
3. Click **ADD TO TOPOLOGY** (displays dialog).



4. On the table, select checkbox next to Topology Name.
5. (optional) Select **Password Protected** checkbox. Enter **Password**.
6. Click **SAVE**.

Remove from Topology

1. Go to *APPS :: SD-WAN :: DEVICES*.
2. On the list, identify a device to be removed from a Topology.
3. Click **REMOVE FROM TOPOLOGY** (displays dialog).



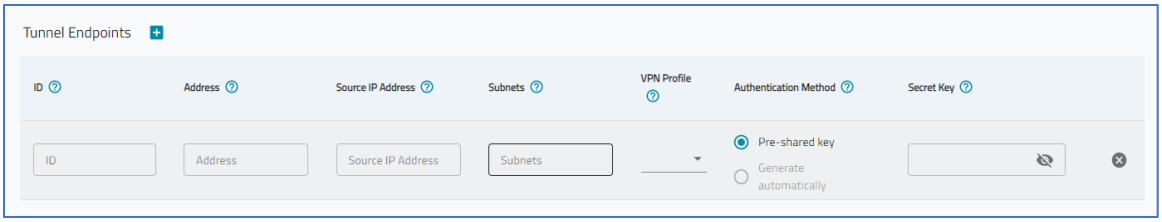
4. On table, select checkbox next to Topology Name.
5. Click **REMOVE**.

Add 3rd Party Endpoints

1. Go to *APPS :: SD-WAN :: DEVICES*.
2. On the list, select a device.
3. Click **ADD 3RD PARTY ENDPOINTS** (displays dialog).

4. Enter **Name**.
5. On **Tunnel Type** drop-down, select one (**IPsec**).
6. In **Location**, enter full street address details. (Latitude and Longitude fields automatically populate.)

   Alternately, directly enter **Latitude** and **Longitude**.
7. On Tunnel Endpoints, click + button (displays dialog)



   Enter details:

   ID

   Address

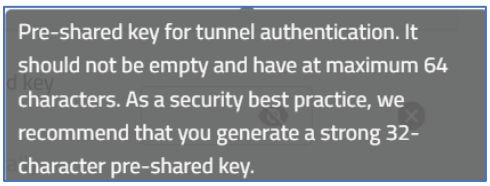
   Source IP Address

   Subnets (comma separated)

   On **VPN** drop-down, select one (**Cisco_ASA**, **Palo AltoIKEv2**, **PaloAlto**, **etc**.)

   On **Authentication Method**, select one (**Pre-shared Key**, **Generate automatically**)

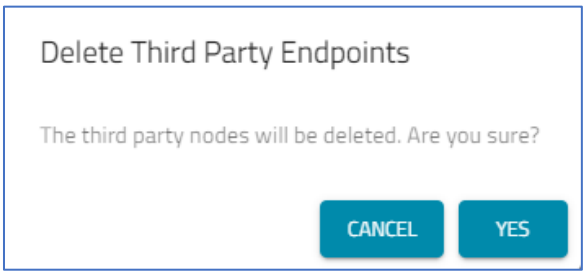
   On **Secret Kay**, enter characters. Follow this requirement (click **?** to view).:



8. Click **SAVE**.

Remove 3rd Party Endpoints

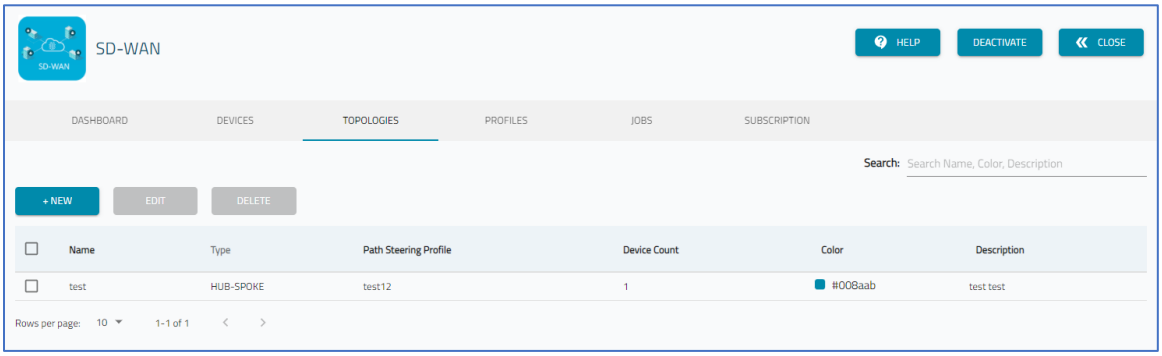
1. Go to *APPS :: SD-WAN :: DEVICES*.
2. On the list, select a device.
3. Click **REMOVE 3RD PARTY ENDPOINTS** (displays dialog).



4. On confirmation dialog, click **YES**.

TOPOLOGIES section

This page is used to manage topologies.

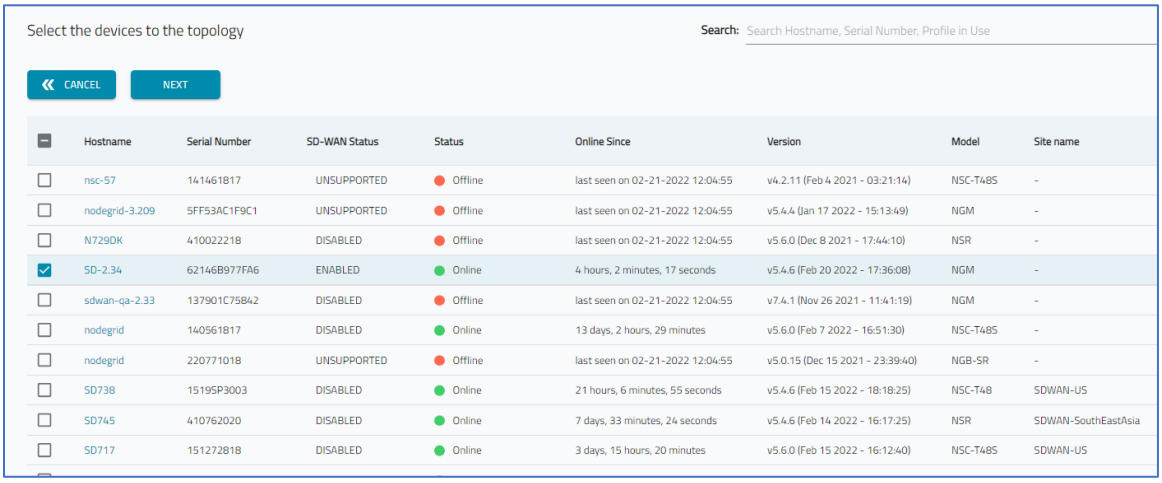


Manage Topologies

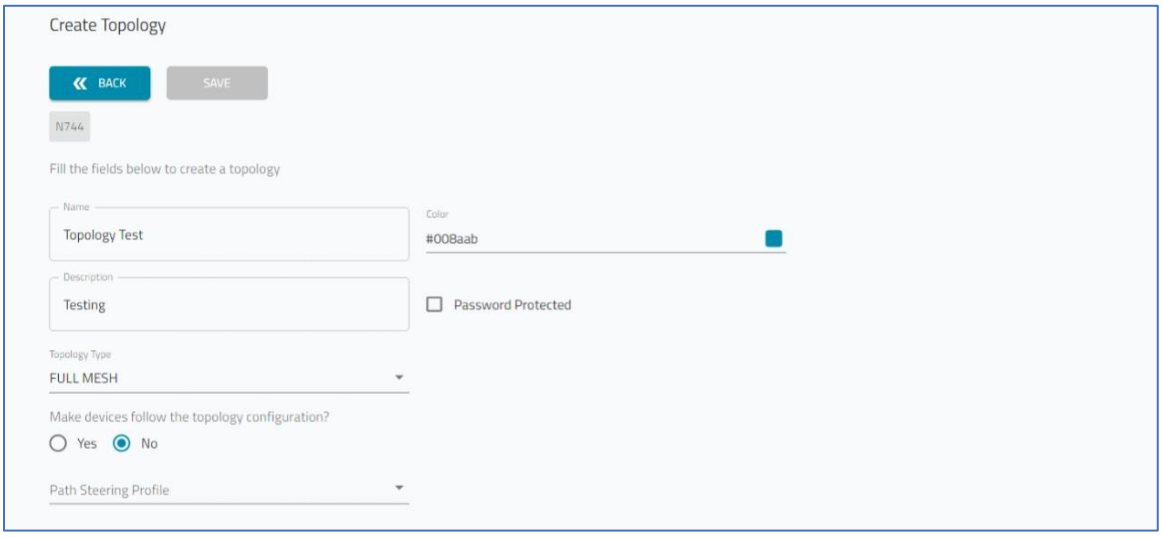
NOTE: When 3rd party devices are included in a topology, a warning notice displays.

Create Topology

1. Go to *APPS :: ACTIVE :: SD-WAN :: TOPOLOGIES*.
2. Click **+NEW** (displays dialog).



3. Select devices to be added to the new Topology.
4. Click **NEXT** (displays dialog).



5. Enter **Name**.
6. Enter **Description**.
7. (optional) Select **Password Protected** checkbox. Enter **Password**.

8. In **Color**, click in the field to display the color menu.

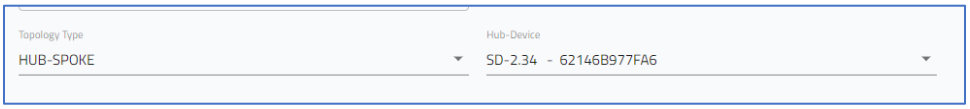
Click in the color bar to select a range, then inside the color zone.

Alternatively, to manually enter color values, use Up/down (right side) arrows to select HEX, RGBA, HSLA).

Click outside the dialog to close.

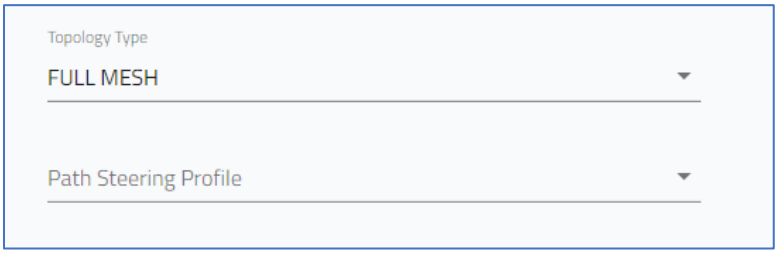
9. On **Topology Type** drop-down, select one.

   HUB SPOKE selection:



   On **Network Profile** drop-down, select one.

   FULL MESH selection:



10. On **Make device follow the topology configuration?**, select radio button (**Yes**, **No**).
11. On **Path Steering Profile** drop-down, select one.
12. Click **SAVE**.

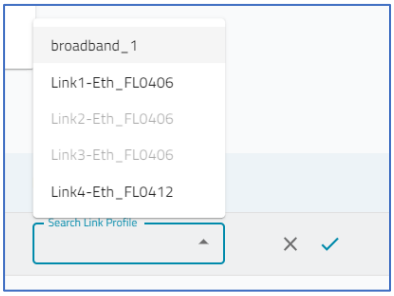
(optional) Confirm Topology is Applied to Device

After the Path Steering Profile has been applied (see above), this can be confirmed:

1. Go to *APPS :: ACTIVE :: SD-WAN :: DEVICES*.
2. Click the device name associated with the Topology (displays Device Details).

3. Scroll to Device Interfaces.

4. In the **Link Profile** column, confirm the Path Steering Profile has been applied.
5. If not, click **Pencil** icon.
6. Click in the **Link Profile** search field. Select from the drop-down list.



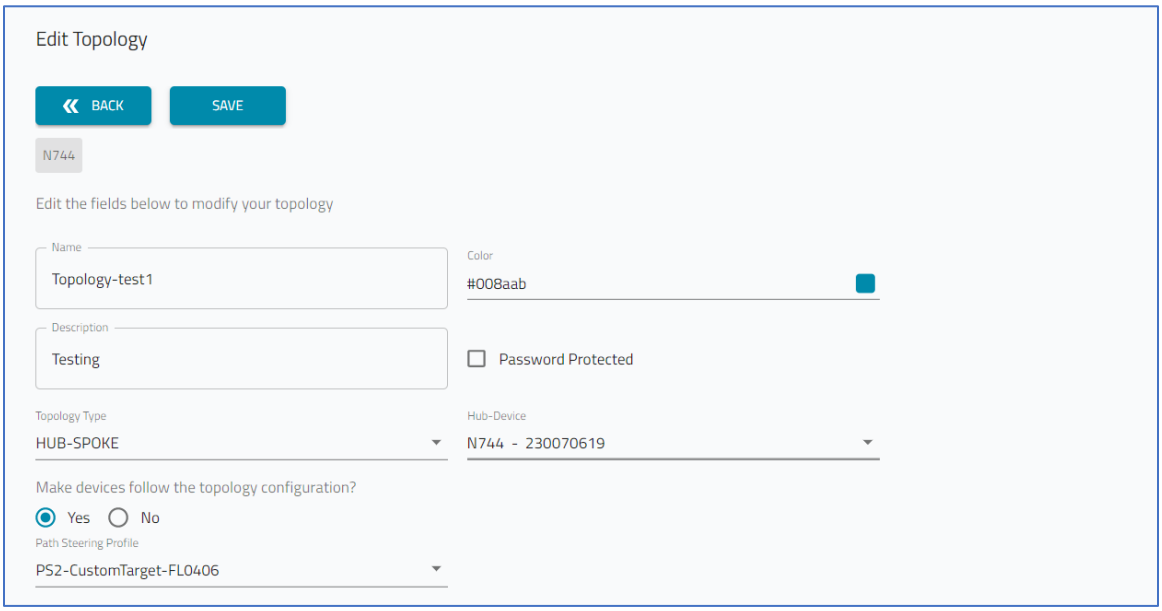
7. At the top of the page, click **SAVE**.

(optional) On Device's Nodegrid Manager, confirm Link Priority

1. Open the device's Nodegrid Manager application.
2. Go to *Network :: SD-WAN :: Network Profile*.
3. Confirm **Link Priority** order. As needed, use **Up/Down** arrows.
4. If changes, click **SAVE**.

Edit a Topology

1. Go to *APPS :: ACTIVE :: SD-WAN :: TOPOLOGIES*.
2. In table, select checkbox on Topology to edit.
3. Click **EDIT** (displays dialog).

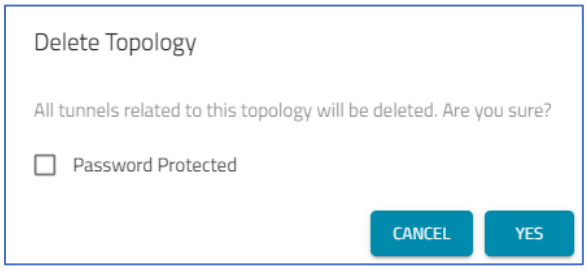


4. Make changes, as needed.
5. Click **SAVE**.

   ***II*??NOTE**: (as needed) To confirm, use the optional *Confirm Topology is Applied to Device* procedure.

Delete a Topology

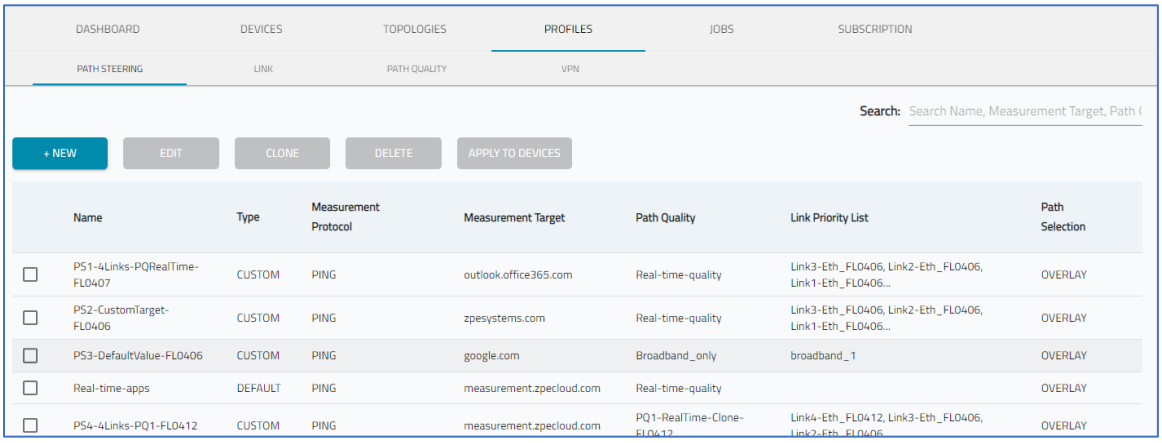
1. Go to *APPS :: ACTIVE :: SD-WAN :: TOPOLOGIES*.
2. In table, select checkbox on item to delete.
3. Click **DELETE** (displays pop-up dialog).



4. (optional) Select **Password Protected** checkbox. Enter **Password**.
5. Click **YES**.

PROFILES :: PATH STEERING tab

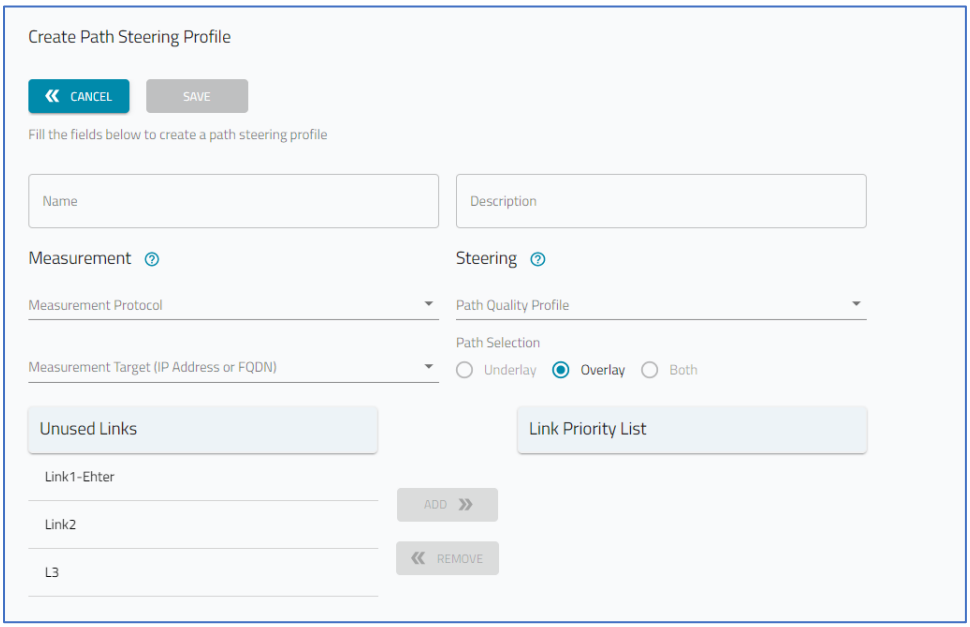
This page manages path steering profiles.



Manage Path Steering Profiles

Create Path Steering Profile

1. Go to *APPS :: ACTIVE :: SD-WAN :: PROFILE :: PATH STEERING*.
2. Click **+NEW** (displays dialog).

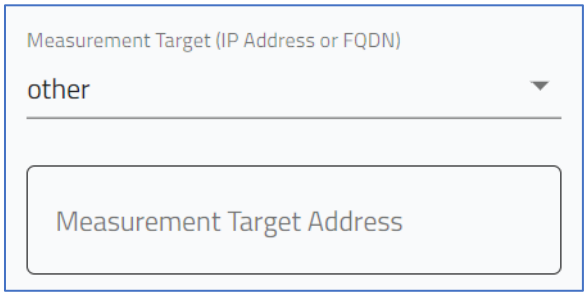


3. Enter **Name**.
4. Enter **Description**.
5. In *Measurement* menu:

   On **Measurement Protocol** drop-down, select one (**PING**).

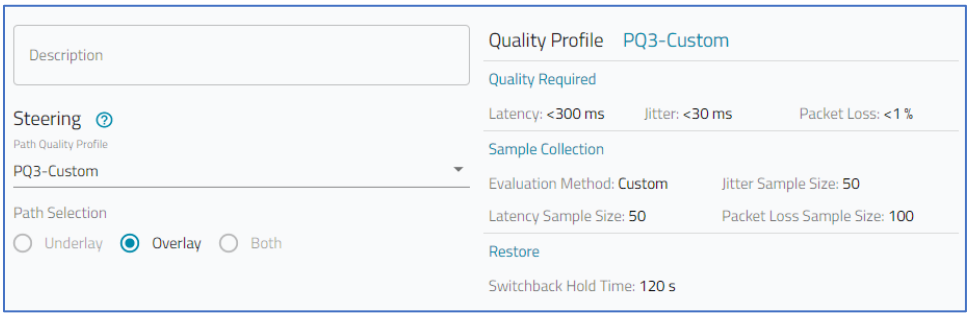
   On **Measurement Target (IP Address or FQDN)** drop-down, select one (**measurement.zpecloud.com, measurement. zpecloud.eu, google.com, Microsoft-my.sharepoint.com, outlook.office365.com, other**)

   If **other** is selected, enter the **Measurement Target Address**.



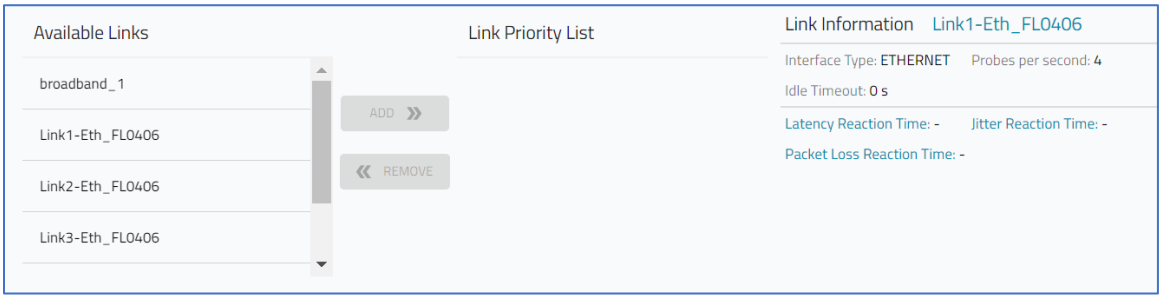
6. In *Steering* menu:

   On **Path Quality Profile** drop-down, select one (selection displays *Quality Profile* details).



   On *Path Selection*, select appropriate radio button (**Underlay**, **Overlay**, **Both**).

7. In the *Link Selection* menu:

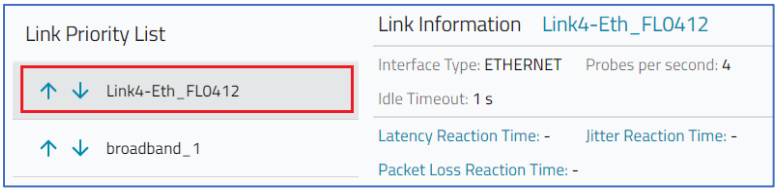


   Select link in *Available Links*, click **Add >>** button (moves to *Link Priority List*).

   To remove a link from *Link Priority List*, select and click **<< Remove** button.

   To set priorities, click on **Up** or **Down** arrow.

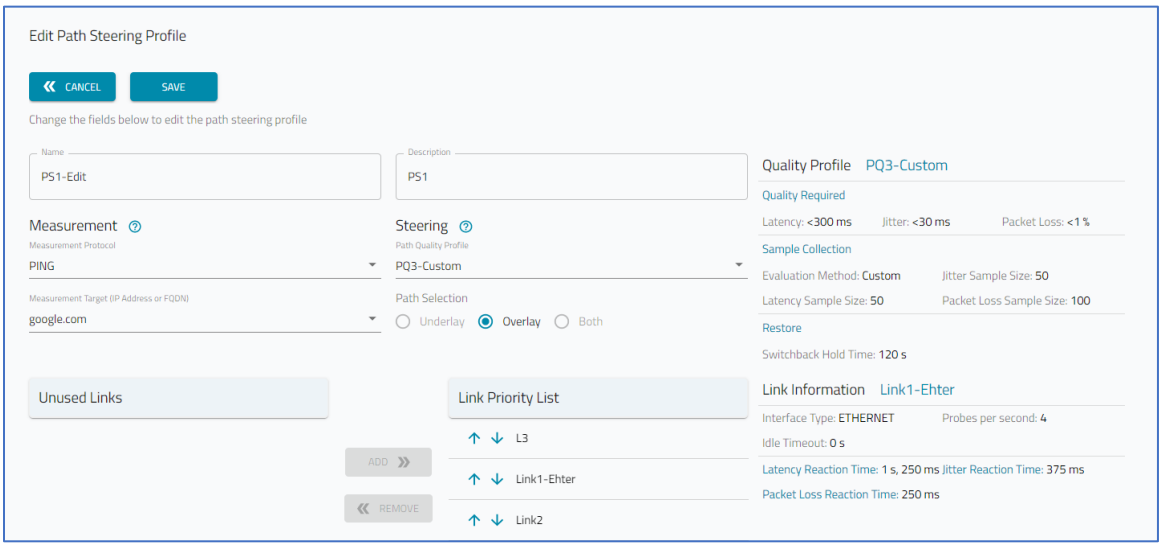
   Additional **Link Information** is displayed when the mouse hovers over a link.



8. Click **SAVE**.

Edit Path Steering Profile

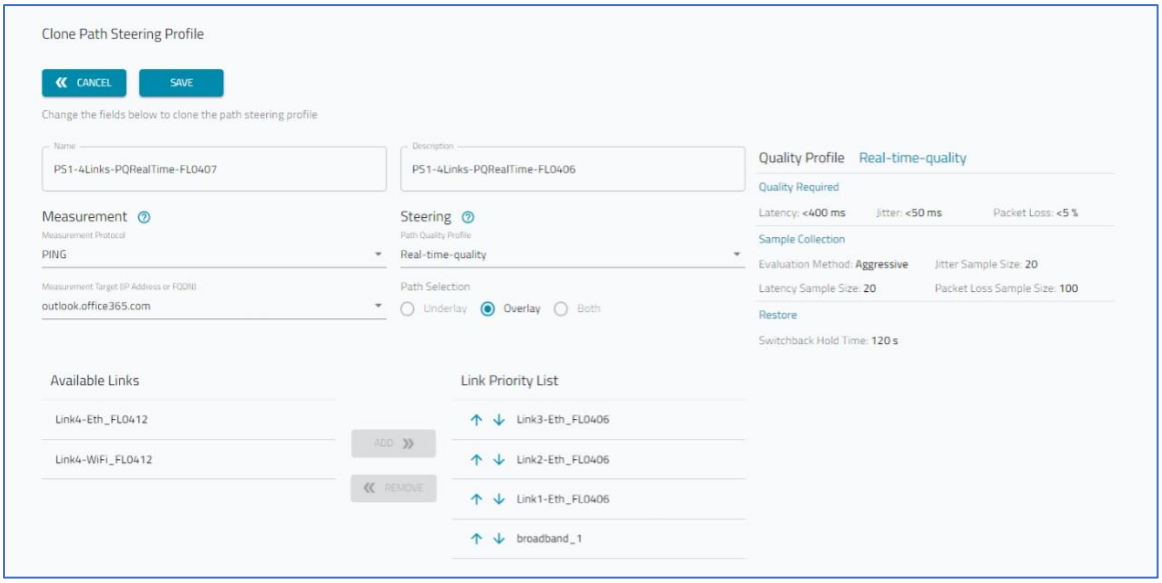
1. Go to *APPS :: ACTIVE :: SD-WAN :: PROFILE :: PATH STEERING*.
2. In table, select checkbox of profile to edit.
3. Click **EDIT** (displays dialog).



4. Make changes, as needed.
5. Click **SAVE**.

Clone Path Steering Profile

1. Go to *APPS :: ACTIVE :: SD-WAN :: PROFILE :: PATH STEERING*.
2. In table, select checkbox on which item to clone.
3. Click **CLONE** (displays dialog).



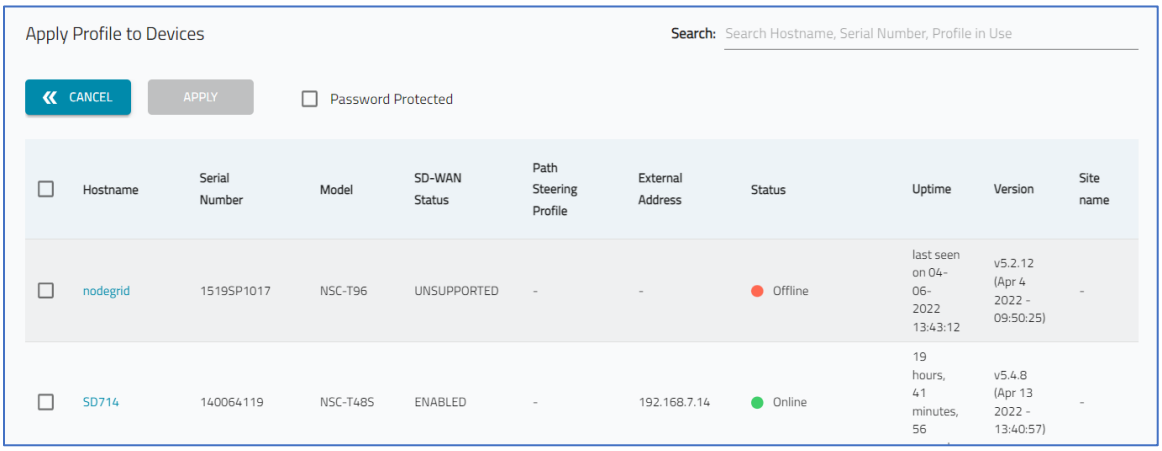
4. Update details, as needed.
5. Click **SAVE**.

Delete Path Steering Profile

1. Go to *APPS :: ACTIVE :: SD-WAN :: PROFILE :: PATH STEERING*.
2. In table, select checkbox on item to delete.
3. Click **DELETE**.
4. On *Confirmation* dialog, click **YES**.

Apply Path Setting Profile to Devices

1. Go to *APPS :: ACTIVE :: SD-WAN :: PROFILE :: PATH SETTING*.
2. In table, select checkbox on profile.
3. Click **APPLY TO DEVICES** (displays dialog).



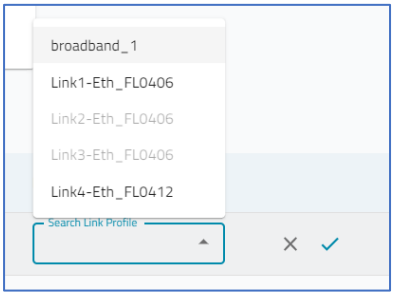
4. On table, select checkboxes to apply the profile.
5. Click **APPLY**.

(optional) Verify Path Steering Profile is Applied to Device

After the Path Steering Profile has been applied (see above), this can be confirmed:

1. Go to *APPS :: ACTIVE :: SD-WAN :: DEVICES*.
2. Click the device name associated with the Topology (displays Device Details).
3. Scroll to Device Interfaces.

4. In the **Link Profile** column, confirm the Path Steering Profile has been applied.
5. If not, click **Pencil** icon.
6. Click in the **Link Profile** search field. Select from the drop-down list.



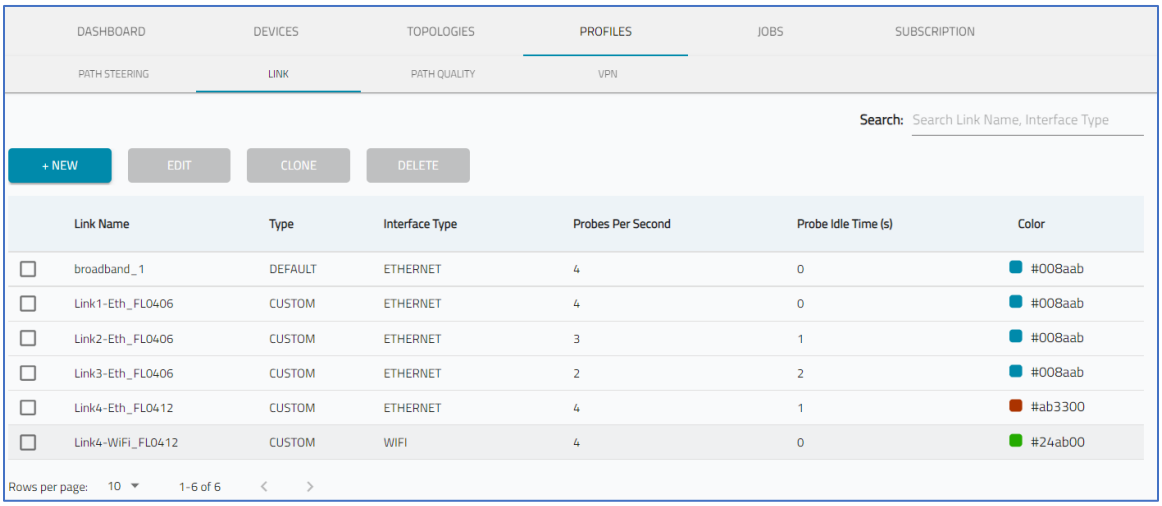
7. At the top of the page, click **SAVE**.

(optional) On Device's Nodegrid Manager, confirm Link Priority Order

1. Open the device's Nodegrid Manager application.
2. Go to *Network :: SD-WAN :: Network Profile*.
3. Confirm **Link Priority** order. As needed, use **Up/Down** arrows.
4. If changes, click **SAVE**.

PROFILES :: LINK tab

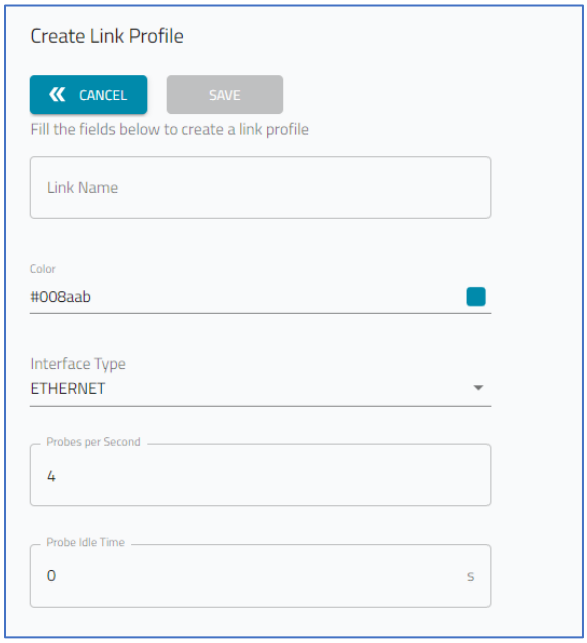
This page manages profile links.



Manage Link Profiles

Create Link Profile

1. Go to *APPS :: ACTIVE :: SD-WAN :: PROFILE :: LINK*.
2. Click **+NEW** (displays dialog).



3. Enter **Link Name**.

   NOTE: Naming convention restrictions follows this regex:
   – / ^ [A-Z a-z _] [A-Z a-z 0-9 _ -] * $ / .
   ● First character of Name must be a letter (A-Z, a-z) or _ (underscore)
   ● Following characters can be letters (A-Z, a-z), numbers (0-9), _ (underscore), or - (dash).

4. Enter **Description**.
5. (optional) Select **Color**, click in the field to display the color menu.

Click in the color bar to select a range, then inside the color zone.

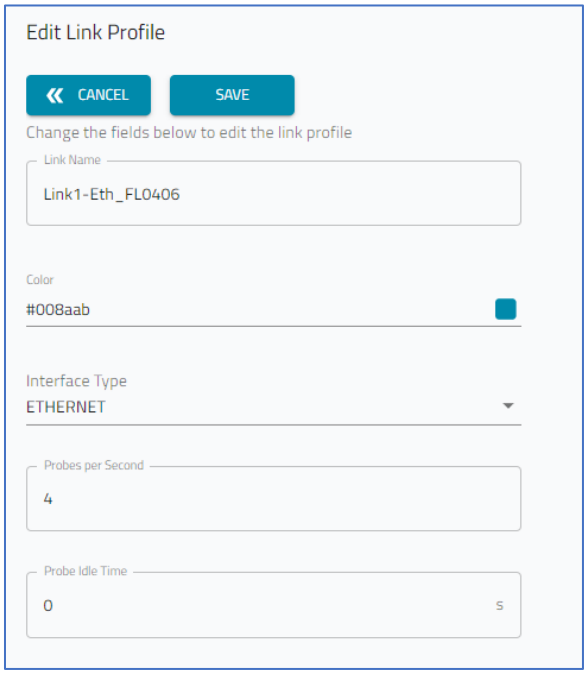
Alternatively, to manually enter color values, use Up/down (right side) arrows to select HEX, RGBA, HSLA).

Click outside the dialog to close.

6. On **Interface Type** drop-down, select one (**ETHERNET**, **ADSL**, **GSM**, **WIFI**, **PPPOE**).
7. In **Probes per Second**, enter a number.
8. In **Probe Idle Time**, enter a value (seconds).
9. Click **SAVE**.

Edit Link Profile

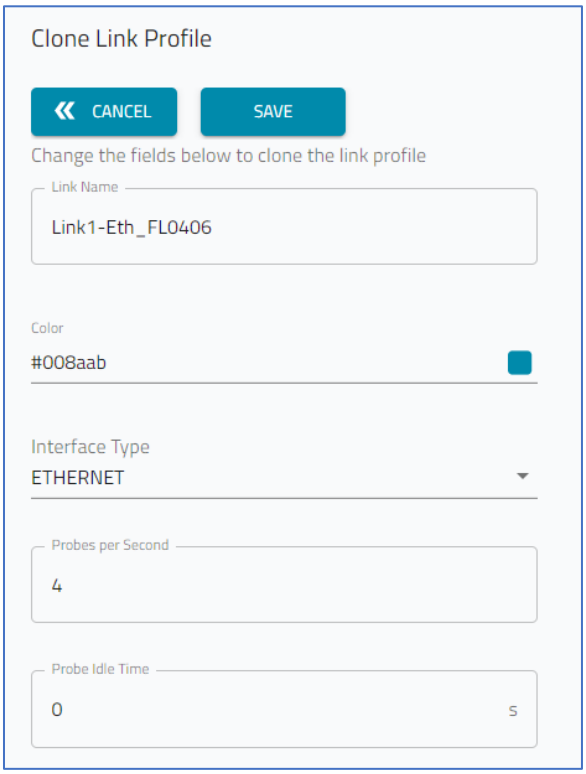
1. Go to *APPS :: ACTIVE :: SD-WAN :: PROFILE :: LINK*.
2. In table, select checkbox to edit.
3. Click **EDIT** (displays dialog).



4. Make changes, as needed.
5. Click **SAVE**.

Clone Link Profile

1. Go to *APPS :: ACTIVE :: SD-WAN :: PROFILE :: VPN*.
2. In table, select checkbox on which item to clone.
3. Click **CLONE** (displays dialog).



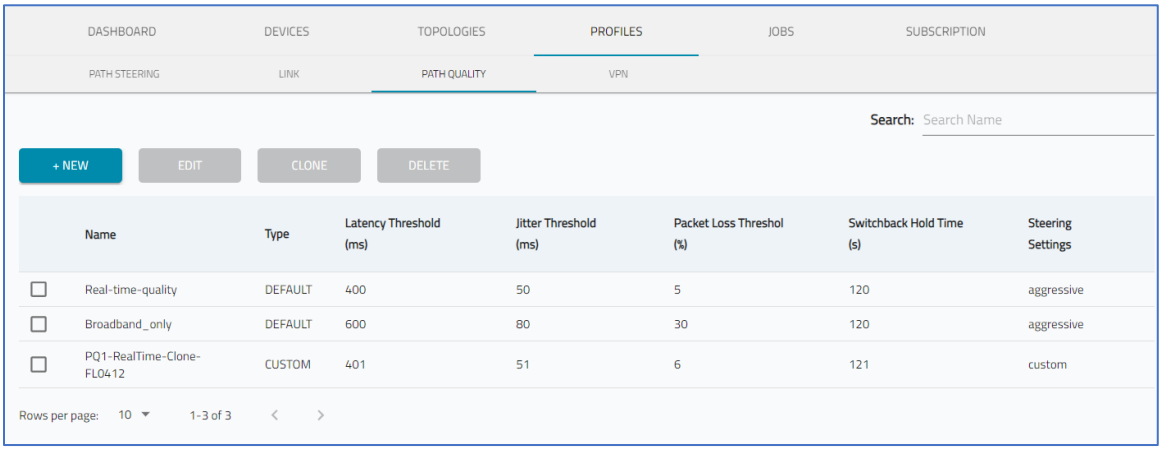
4. Update details, as needed.
5. Click **SAVE**.

Delete Link Profile

1. Go to *APPS :: ACTIVE :: SD-WAN :: PROFILE :: LINK*.
2. In table, select checkbox on which item to delete.
3. Click **DELETE**.
4. On *Confirmation* dialog, click **YES**.

PROFILES :: PATH QUALITY tab

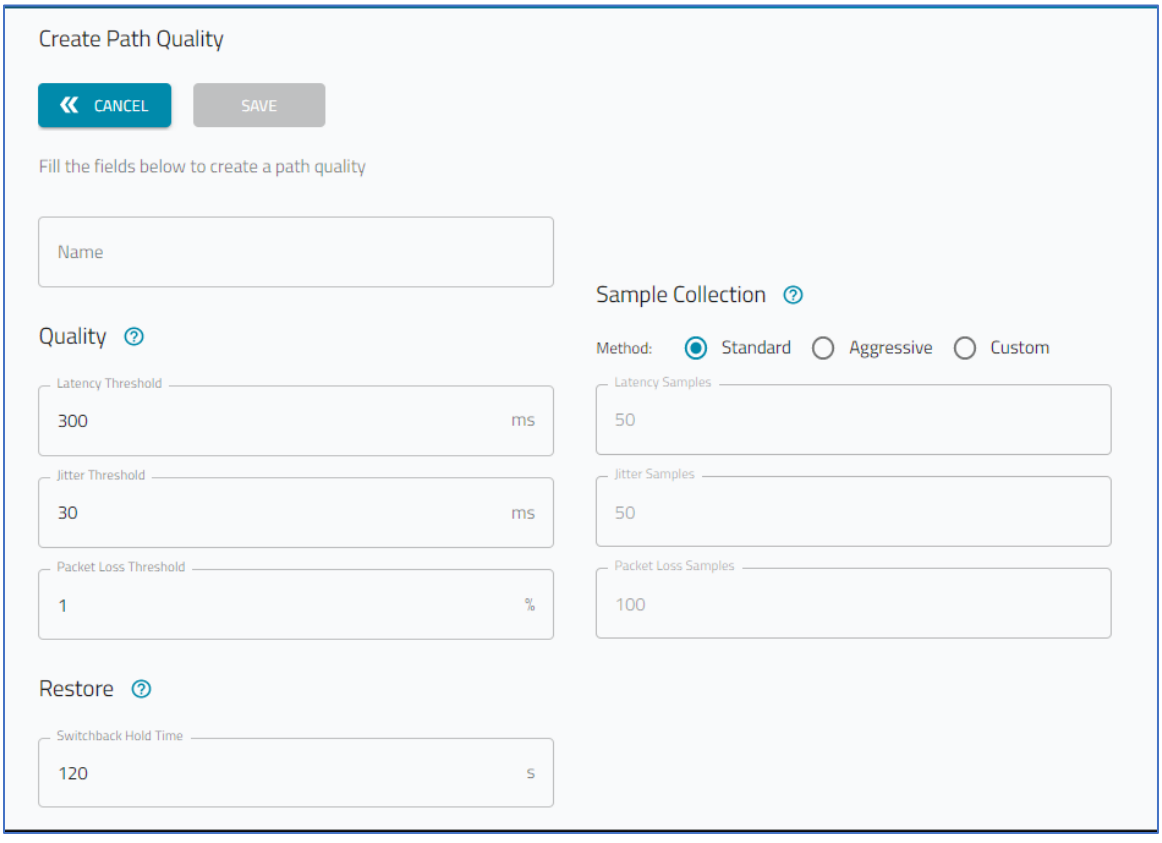
This page manages quality level of path.



Manage Path Quality Profiles

Create Path Quality Profile

1. Go to *APPS :: ACTIVE :: SD-WAN :: PROFILE :: PATH QUALITY*.
2. Click **+NEW** (displays dialog).



3. Enter **Name**.
4. In *Quality* menu:

   In **Latency Threshold**, enter value (default: 300)

In **Jitter Threshold**, enter value (default: 30)

In **Packet Loss Threshold**, enter value (default: 1)

5. In *Restore* menu:

   Enter **Switchback Hold Time** value (default: 120)

6. In *Sample Collection* menu:

   For **Method**, select one:

   Standard radio button

   Aggressive radio button

   Custom radio button (activates additional fields)

   Enter **Latency Samples** value (default: 50)

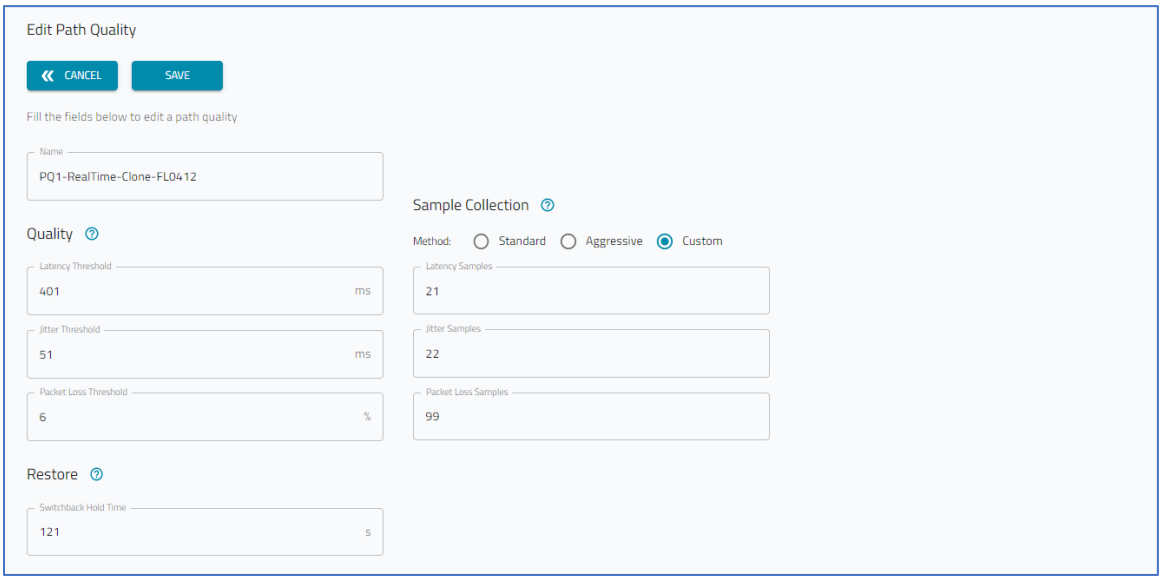
   Enter **Jitter Samples** value (default: 50)

   Enter **Packet Loss Samples** value (default: 100)

7. Click **SAVE**.

Edit Path Quality Profile

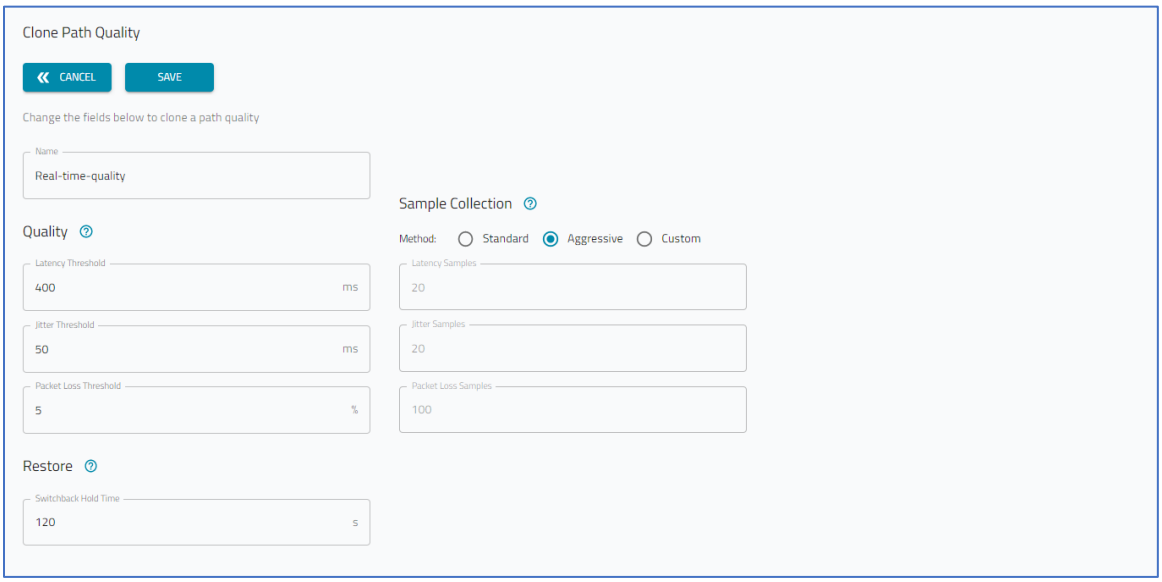
1. Go to *APPS :: ACTIVE :: SD-WAN :: PROFILES :: PATH QUALITY*.
2. In table, select checkbox to edit.
3. Click **EDIT** (displays dialog).



4. Make changes, as needed.
5. Click **SAVE**.

Clone Path Quality Profile

6. Go to *APPS :: ACTIVE :: SD-WAN :: PROFILE :: PATH QUALITY*.
7. In table, select checkbox on which item to clone.
8. Click **CLONE** (displays dialog).



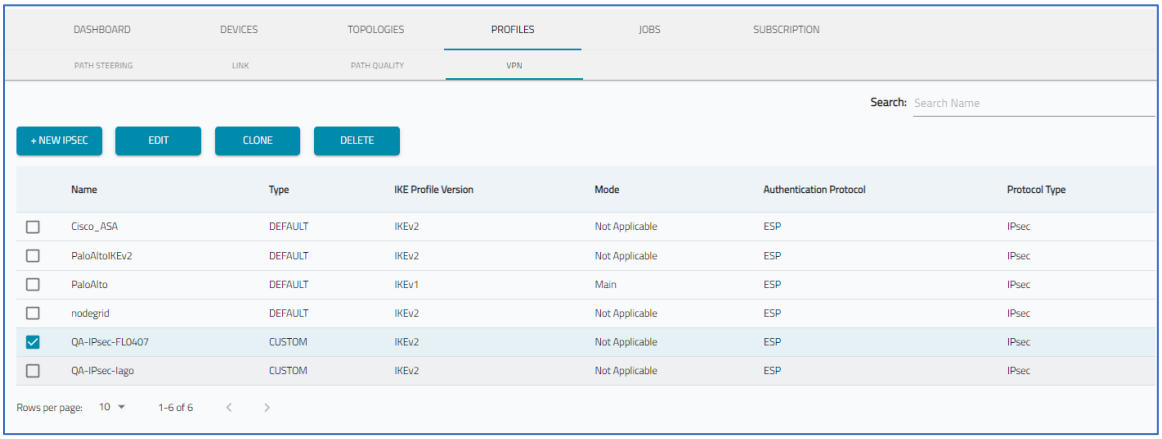
9. Update details, as needed.
10. Click **SAVE**.

Delete Path Quality Profile

1. Go to *APPS :: ACTIVE :: SD-WAN :: PROFILE :: PATH QUALITY*.
2. In table, select checkbox on item to delete.
3. Click **DELETE**.
4. On *Confirmation* dialog, click **YES**.

PROFILES :: VPN tab

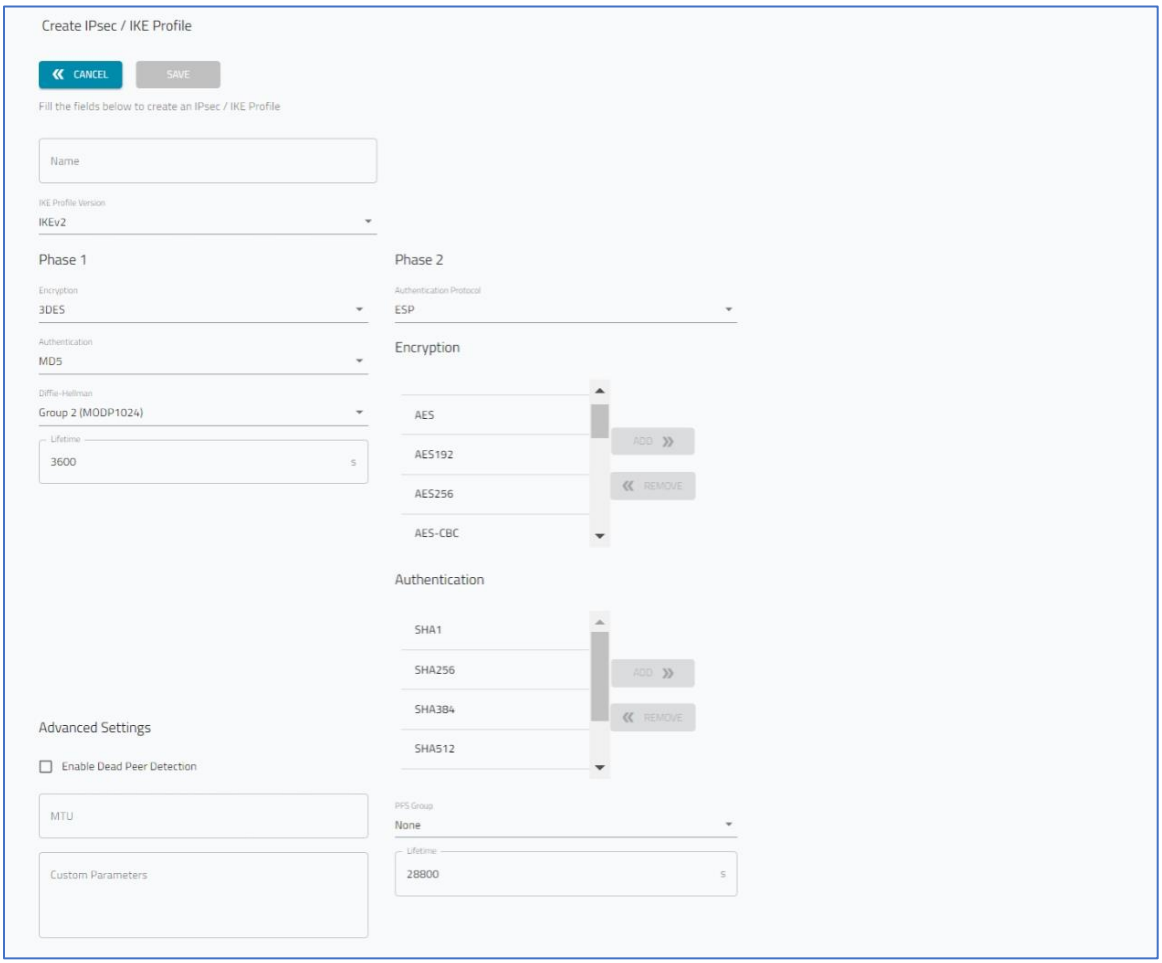
This page manages quality level of path.



Manage VPN Profiles

Create VPN Profile

1. Go to *APPS :: ACTIVE :: SD-WAN :: PROFILE :: VPN*.
2. Click **+NEW IPSEC** (displays dialog).



3. Enter **Name**.

4. On **IKE Profile Version** drop-down, select one (**IKEv1**, **IKEv2**).
5. In *Phase 1* menu:

   In **Encryption** drop-down, select one (**3DES**, **AES**, **AES192**, **AES256**, **AES-CBC**, **AES-CBC192**, **AES-CBC256**, **AES-CTR**, **AES-CTR192**, **AES-CTR256**, **AES-GCM**, **AES-GCM192**, **AES-GCM256**)

   In **Authentication** drop-down, select one (**SHA1**, **SHA256**, **SHA386**, **SHA512**, **MD5**)

   In **Diffie-Hellman** drop-down, select one (**Group 2 (MODP1026)**, etc.)

   Enter **Lifetime** value (default 3600)
6. In *Phase 2* menu:

   On **Authentication Protocol** drop-down, select one (**ESP**, **AH**)

   ESP selection

   On *Encryption* section: select item, click **Add >>** button (moves to list on right). To remove item on right, select and click **<< Remove** button.

   On *Authentication* section: select item, click **Add >>** button (moves to list on right). To remove item on right, select and click **<< Remove** button.

   AH selection

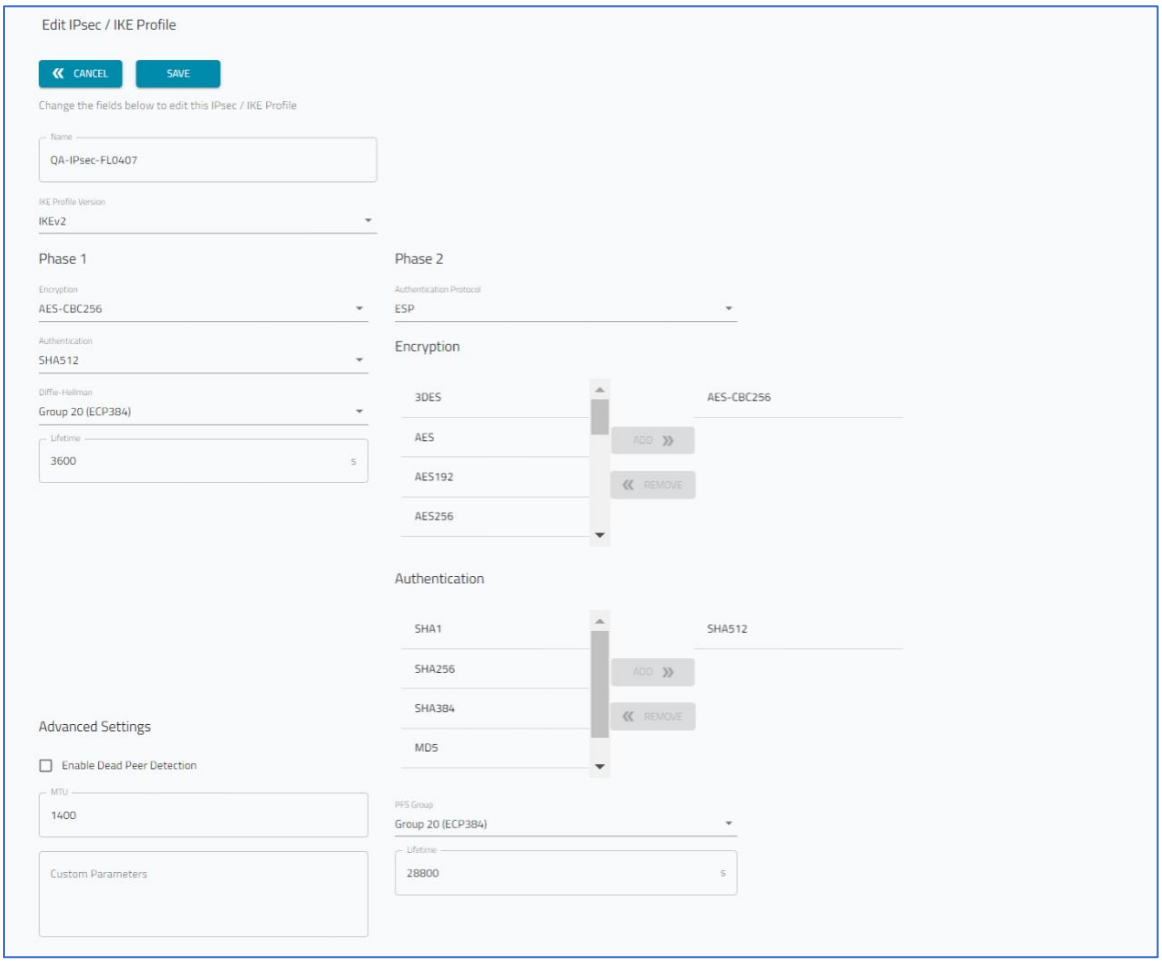
   On *Encryption* section: select item, click **Add >>** button (moves to list on right). To remove item on right, select and click **<< Remove** button.

   On **PES Group** drop-down, select one (**Group 16 (MODP4096)**, etc.)

   Enter Lifetime value (default: 28800).
7. Click **SAVE**.

Edit VPN Profile

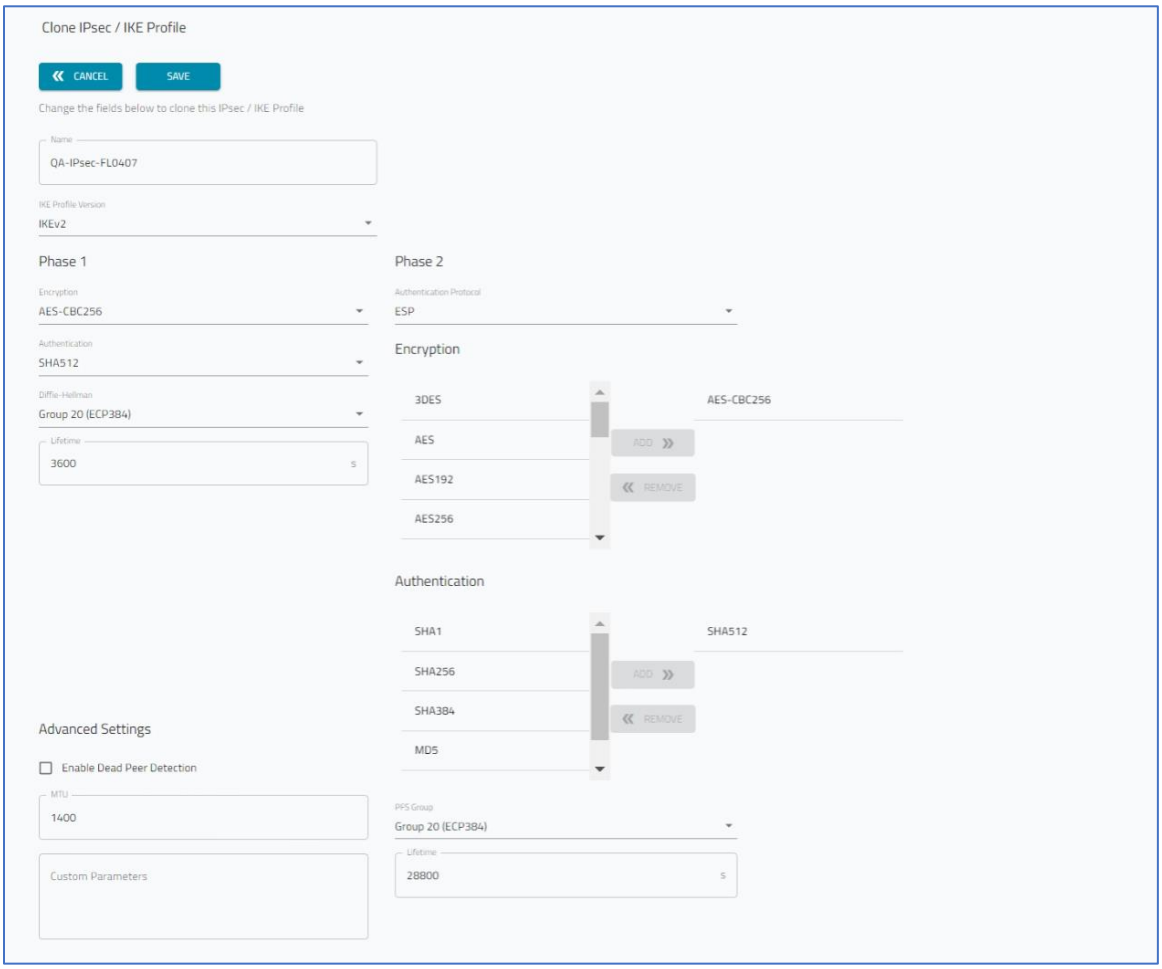
1. Go to *APPS :: ACTIVE :: SD-WAN :: PROFILES :: VPN*.
2. In table, select checkbox to edit.
3. Click **EDIT** (displays dialog).



4. Make changes, as needed.
5. Click **SAVE**.

Clone VPN Profile

1. Go to *APPS :: ACTIVE :: SD-WAN :: PROFILE :: VPN*.
2. In table, select checkbox on which item to clone.
3. Click **CLONE** (displays dialog).



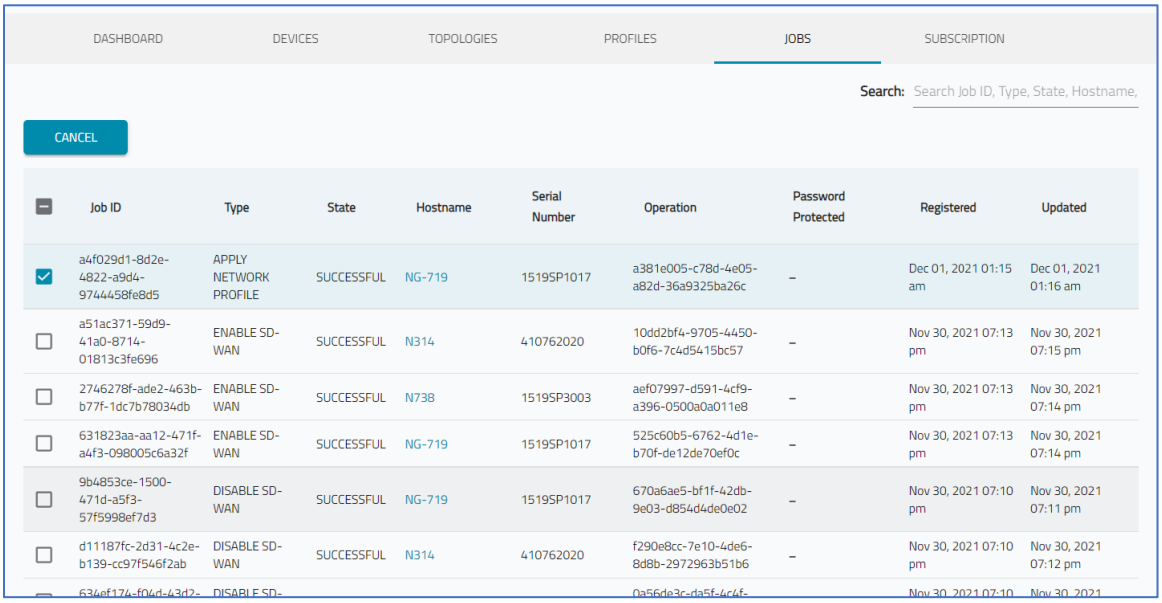
4. Update details, as needed.
5. Click **SAVE**.

Delete VPN Profile

1. Go to *APPS :: ACTIVE :: SD-WAN :: PROFILE :: VPN*.
2. In table, select checkbox on item to delete.
3. Click **DELETE**.
4. On *Confirmation* dialog, click **YES**.

JOBS section

An overview of the configuration updates, generated by SD-WAN. Each table entry represents a configuration update.



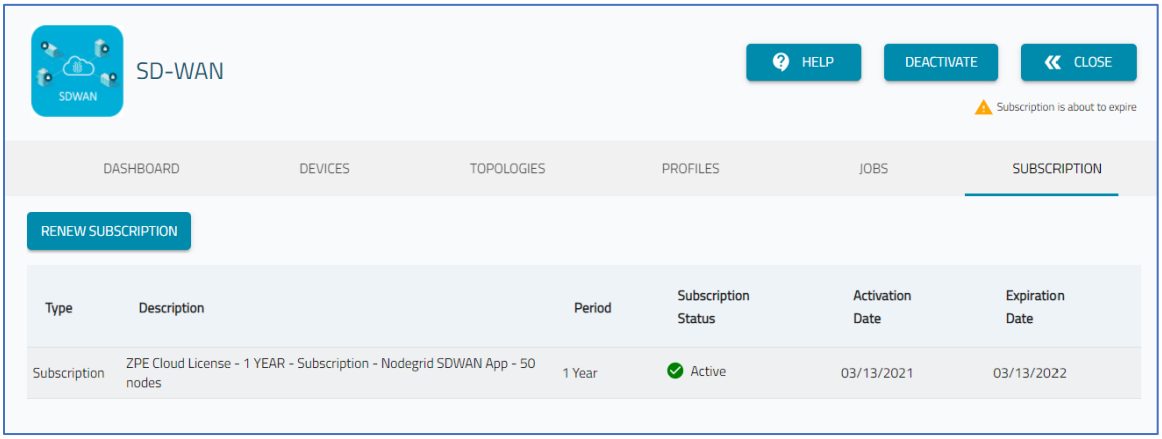
Manage Jobs

Cancel a Job

1. Go to *APPS :: ACTIVE :: SD-WAN :: JOBS*.
2. On the table, select the job(s) to be canceled.
3. Click **CANCEL**.

SUBSCRIPTION section

This page presents information about current SD-WAN subscriptions.

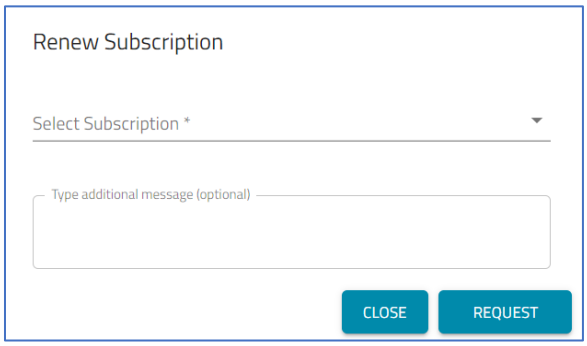


Manage Subscriptions

Renew Subscription

1. Go to *APPS :: ACTIVE :: SD-WAN :: SUBSCRIPTIONS*.

2. Click **RENEW SUBSCRIPTION** (displays dialog).



3. On the **Select Subscription** drop-down, select one.

4. In the *Type additional message (optional)* textbox, enter details as needed.
5. Click **REQUEST**.

Appendix C – Nodegrid Data Lake User Guide

When available, the Nodegrid Data Lake app is located in the *APPS* Section.

The Nodegrid Data Lake application gathers device information from sensors, application stats, network traffic, data logs, system logs, events, bridges to third-party IoT devices. The dashboard presents visual representations of the metrics for quick evaluation of the represented infrastructure.

The application uses the Kibana® interface, which is easily configurable and secure. Details are stored on ZPE Cloud.

The application uses the Kibana® interface, which is easily configurable and secure. Details are stored on ZPE Cloud.

Use Case Example

This example creates an interface plugin using the clone process. The new plugin is included in a new Profile to collect metrics from the new interface, memory, and cpu usage plugins.

1. Go to *APPS ;; ACTIVE ;; NODEGRID DATA LAKE :: PLUGINS*.
2. Select **Interface eth0** checkbox.
3. Click **CLONE** (displays dialog).

   Change **Name** to **Interface eth1**.

   (optional) Edit **Description** (as needed).

   In **Code** textbox, change "**eth0**" to "**eth1**".

   ```
   <Plugin interface>
     Interface "eth1"     <<CHANGE "eth0" to "eth1">>
   </Plugin>
   ```

   Click **SAVE**.
4. Go to *APPS ;; ACTIVE ;; NODEGRID DATA LAKE :: PROFILES*.
5. Click **+NEW** (displays dialog).

   Enter **Name** and **Description**.

   On the *Available Plugins* panel, select: **interface eth1**, **memory** and **cpu usage**.

   In **Default interval**, enter **5**. On **Interval** drop-down, select **minute**.

   Click **SAVE**.
6. On the PROFILES page, select the new profile. Click **APPLY TO DEVICES** (displays dialog).

   Select device checkboxes, then click **APPLY**.

7. On the Banner, go to *PROFILES :: OPERATION*. Look for an operation that indicates the Profile was successfully applied to the selected devices. (To refresh the page, click *OPERATION* tab.)
8. To review results, go to: *APPS :: ACTIVE :: NODEGRID DATA LAKE :: EXPORER*.

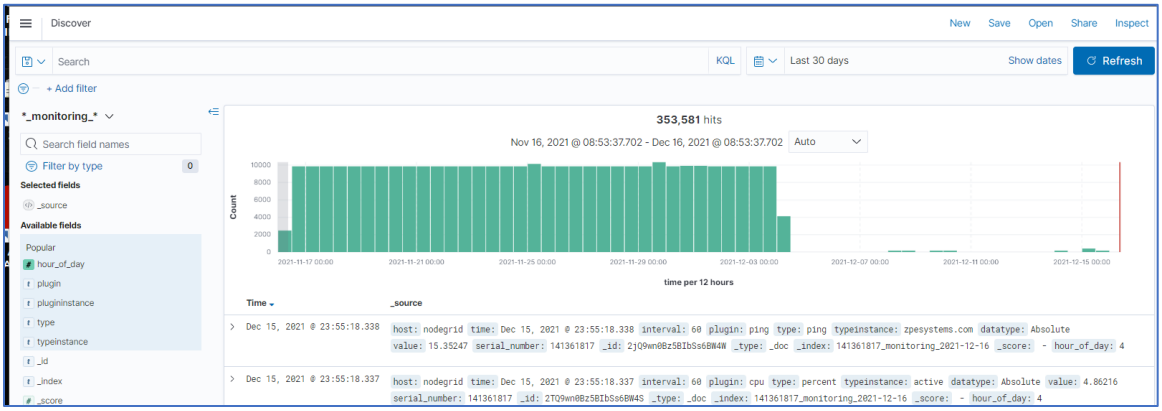
   Click the **Hamburger** icon.

   On the drop-down dialog, click **Discover** (displays dialog).

   The *Discover* panel provides these options: New, Save, Open, Share, Inspect.

   The table lists events on the Profile.

   To view more details, click to display Expanded document details.

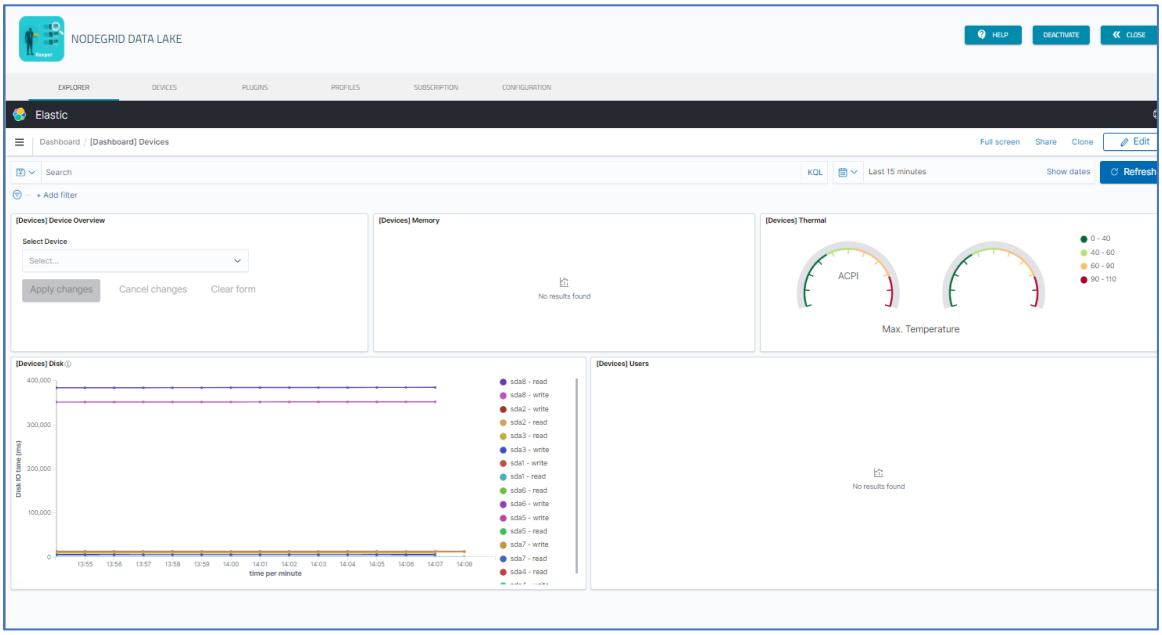


   Hover over the symbol to display operation options.

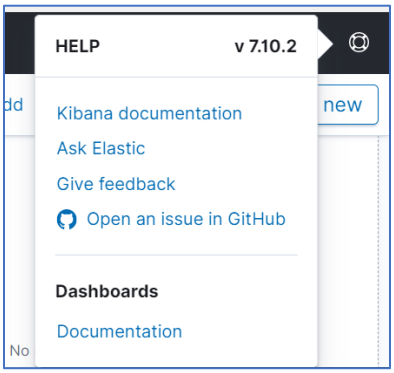
   Hover over these pop-out options for tooltips on functionality (**Filter for value**, **Filter out value**, Toggle column in table, Filter for field present).

EXPLORER tab

The customizable Kibana® dashboard can be configured to show logs, metrics, events, and more. For more information on how to customize the dashboard, see http://www.elastic.co/guide/index.html.

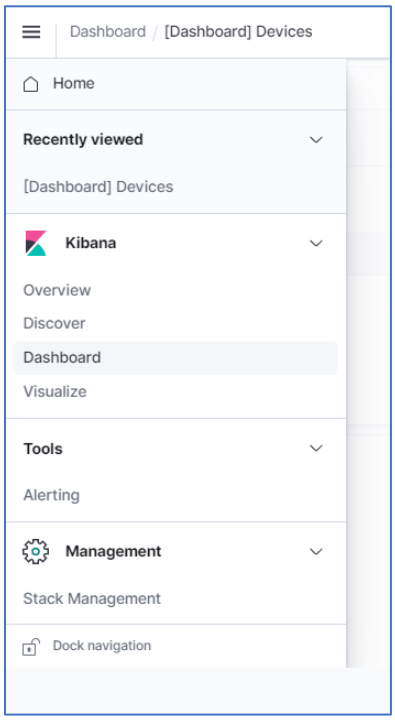


On the right side of the **Elastic** bar, click the icon to display available Help resources.

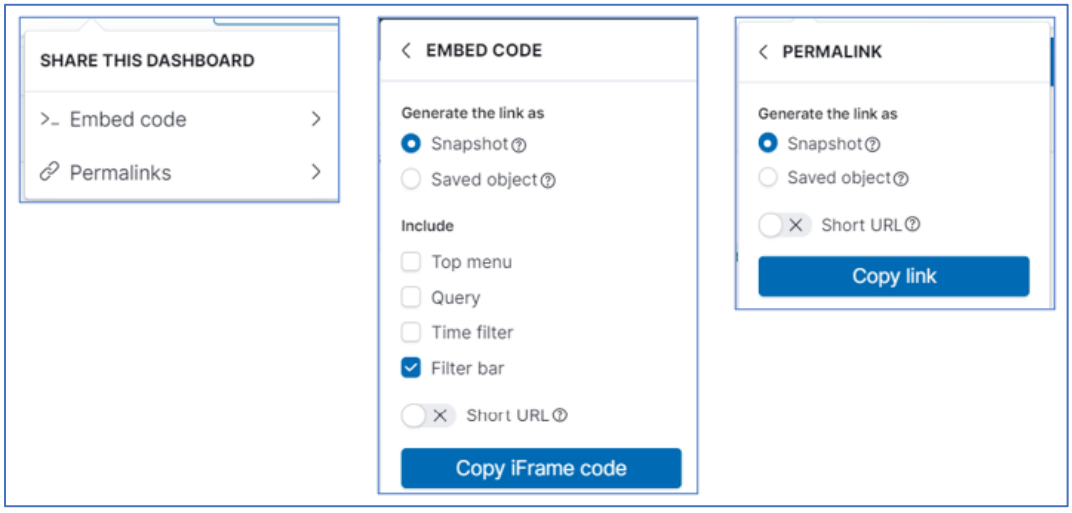


On *Dashboard* bar, are these features:

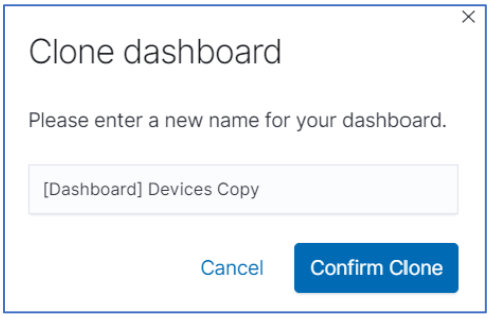
- Click **Hamburger** icon (left side) to display Kibana dashboard.



- Click **Full Screen** to hide the Dashboard bar.
- Click **Share** (displays dialog).



- Click **Clone** (displays dialog).



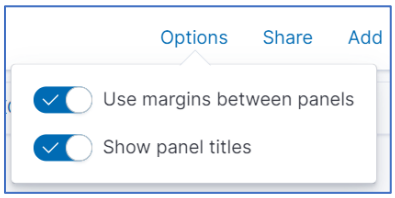
Enter **Name** for the cloned dashboard.

Click **Confirm Clone**.

Open and edit cloned dashboard, as needed.

- Click **Edit** (right side) to display choices.

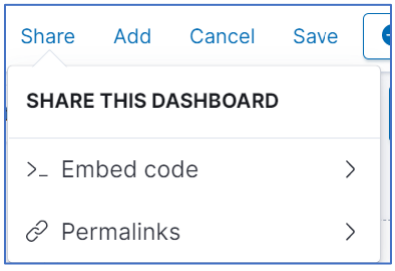
Options (displays drop-down).



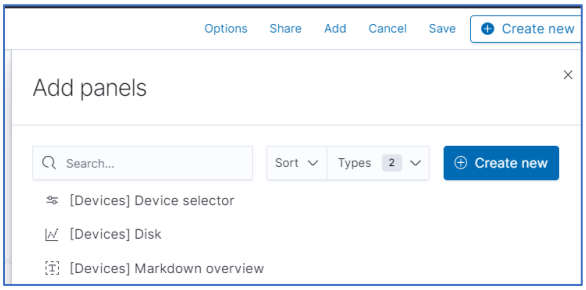
Select/unselect **Use margins between panels** toggle.

Select/unselect **Show panel titles** toggle.

Share (displays *Share this Dashboard* dialog).



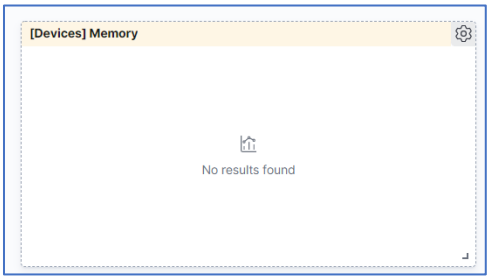
Add (displays *Add Panels* dialog).



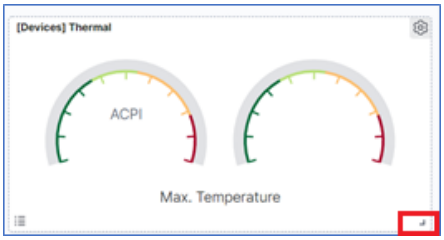
Cancel (closes **Edit** dialogs).

To manage Panels in *Dashboard*:

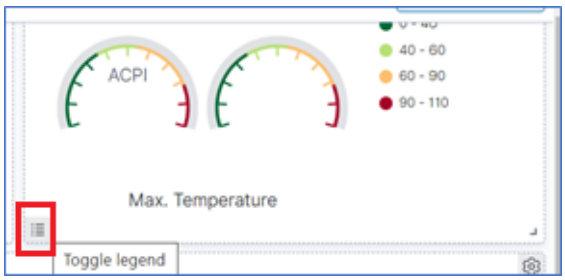
Move panel – click on panel title. Drag and drop panel in new location.

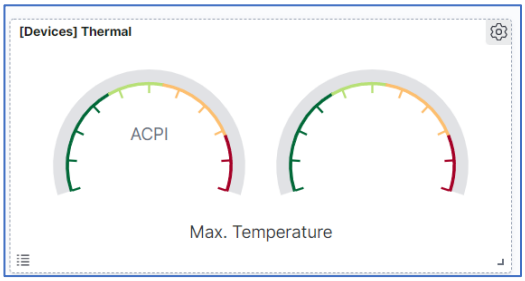


Resize panel – at lower right corner, click on corner symbol. Drag and drop to resize.

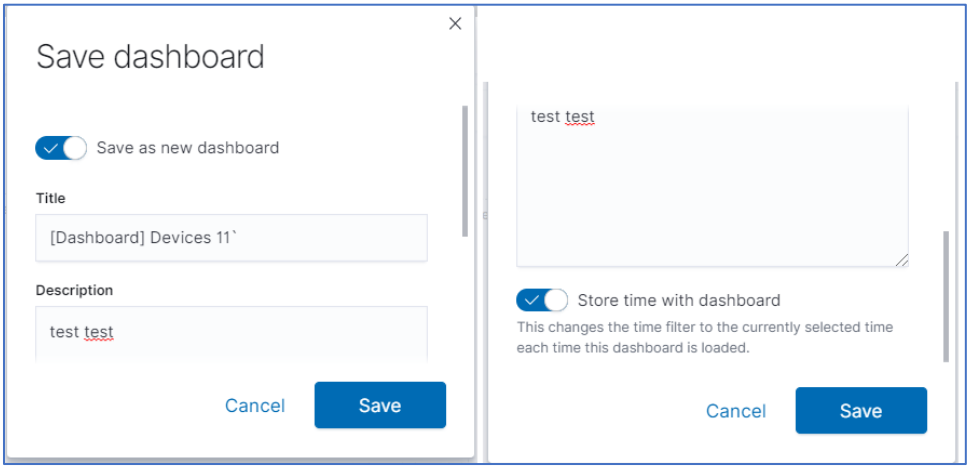


Toggle panel legend – at lower left corner, click to enable/disable.





Save (saves the changes).



(optional) Select **Save as a new dashboard** checkbox.

Enter **Title**.

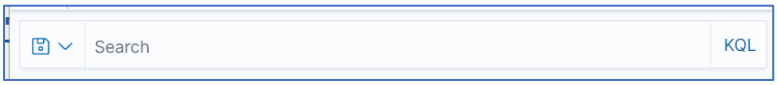
Enter **Description**.

(scroll down)

(optional) Select **Store time with dashboard** checkbox.

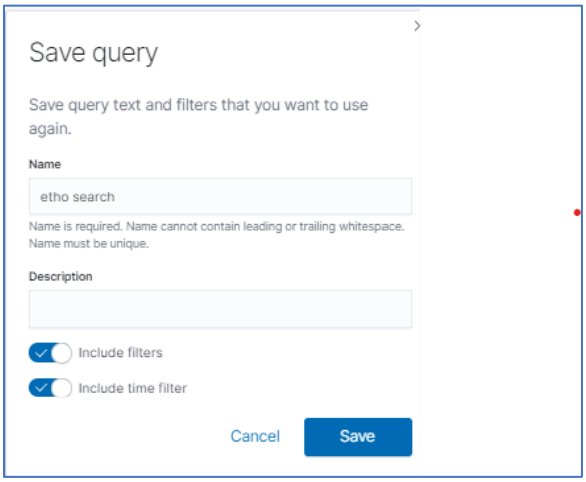
Click **Save**.

On **Search** panel:



Enter a **Search** condition.

(optional) Click **Save Query**  icon (displays dialog).



Enter **Name**.

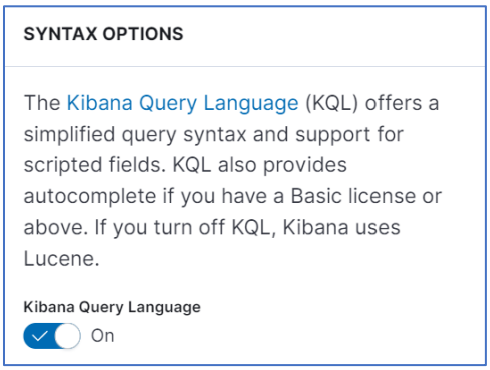
Enter **Description**.

(optional) Enable/disable **Include Filters** toggle.

(optional) Enable/disable **Include time filter** toggle.

Click **Save**.

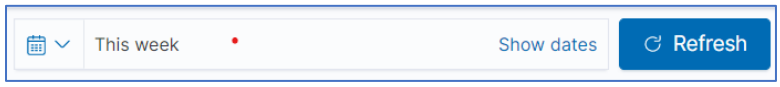
To use **KQL** (Kibana Query Language), click link (displays dialog).



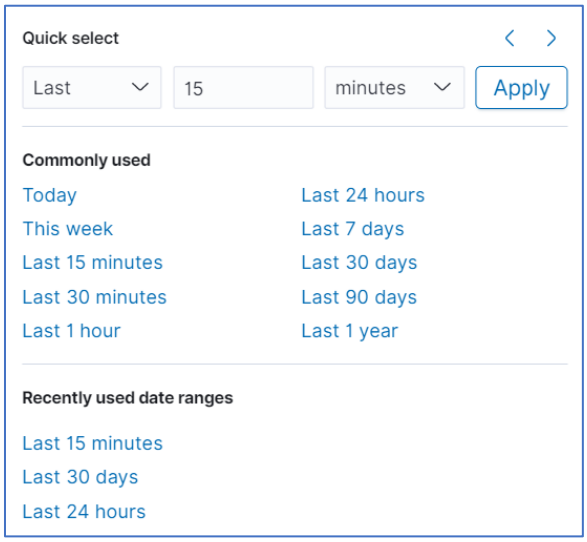
Enable/disable **Kilbana Query Language** toggle.

To close dialog, click outside dialog box.

On **Time range** panel (click **Refresh**, as needed).



To select time range, click **Calendar**  icon (displays dialog)



Click any of the options listed in **Commonly used** or **Recently used data ranges** menus.

Alternatively, in **Quick Select**:

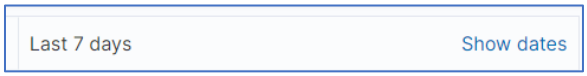
On **Time direction** drop-down, select one (**Last**, **Future**).

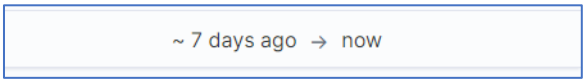
Enter a number.

On **Time download**, select one (**seconds**, **minutes**, **hours**, **days**, **weeks**, **months**).

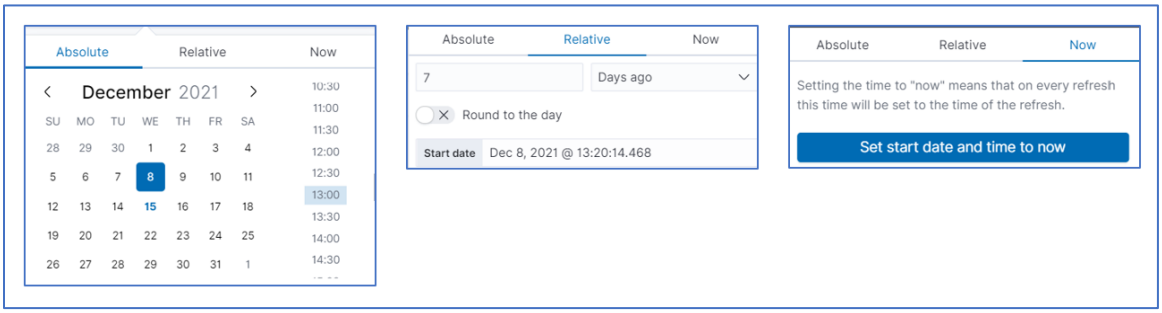
Click **Apply**.

Click **Show dates** (modifies details according to the time range selected)

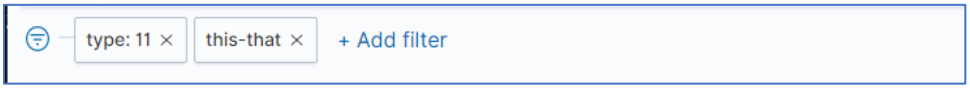




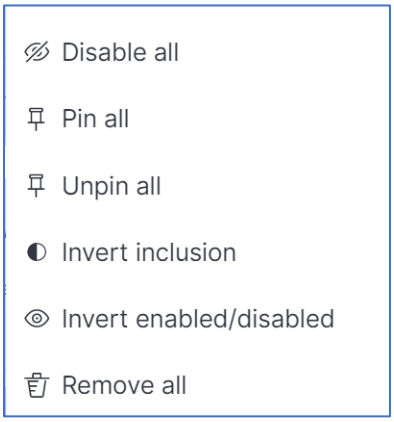
Click within the date/time (displays dialog of three tabs). Make modifications, as needed. If changes to **Absolute** tab or **Now** tab, click **Update**. If changes to **Relative** tab, click **Refresh**.



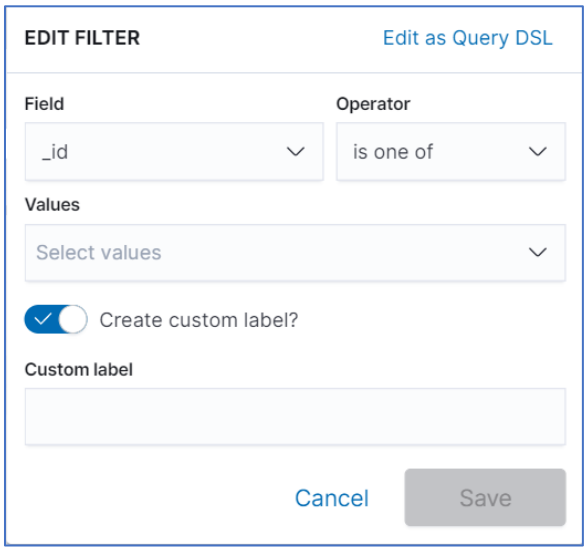
On **Filters** panel:



To manage filters, click **Manage Filter**  icon (displays dialog). Select items for control filters, as needed.



To include a new filter, click **Add Filters** (displays dialog)



To create a new Filter:

On **Field** drop-down, select one.

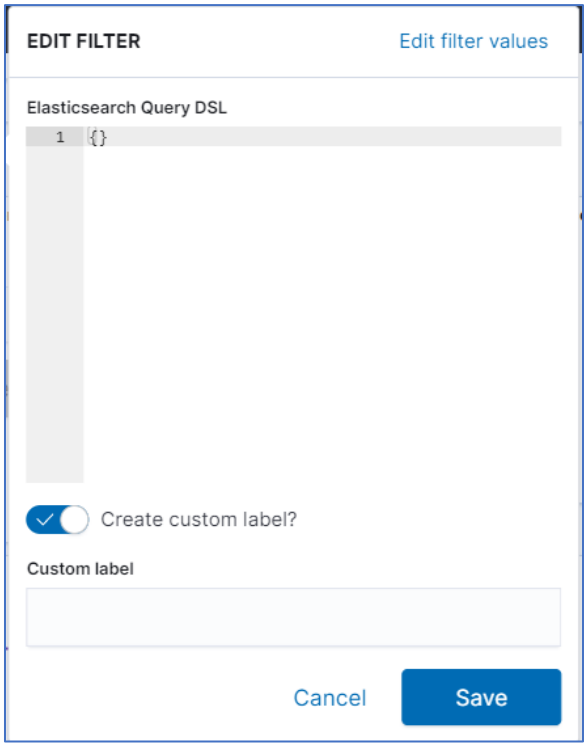
On **Operator** drop-down, select a Boolean expression.

Based on **Field** selection, **Values** drop-down changes. Select one.

(optional) Enable/disable **Create custom label** toggle. If enabled, enter **Customer label**.

Click **Save**. (Filter names are displayed on the *Filter* panel.)

(optional) Click **Edit as Query DSL** (displays dialog).

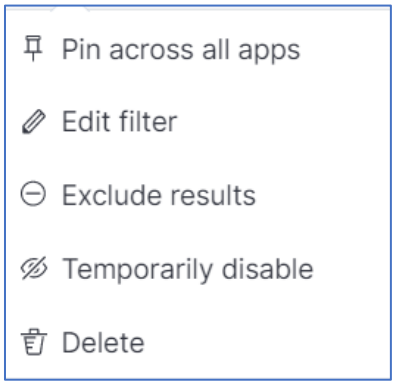


Enter code block.

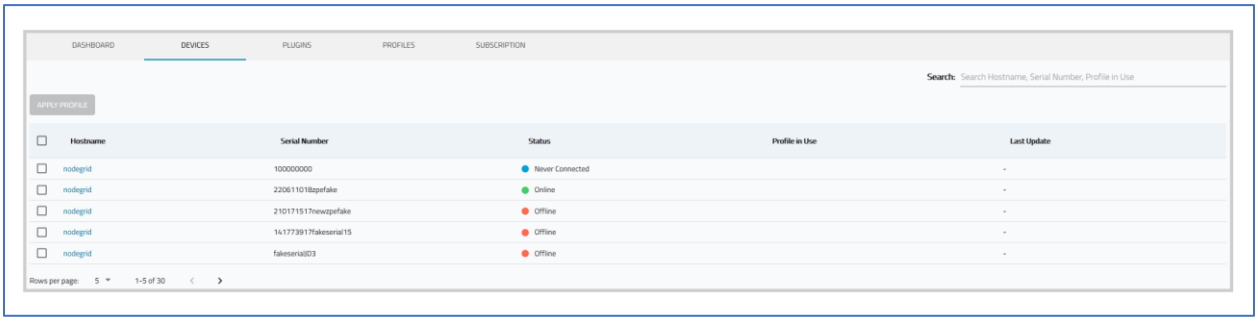
(optional) Enable/disable **Create custom label** toggle. If enabled, enter **Customer label**.

Click **Save**.

To edit an existing Filter, click on the filter name (displays dialog). Select an item as needed.



DEVICES tab



This lists all devices linked to the ZPE Cloud account. For each device, the following information is displayed: Any profile can be applied to one or more devices.

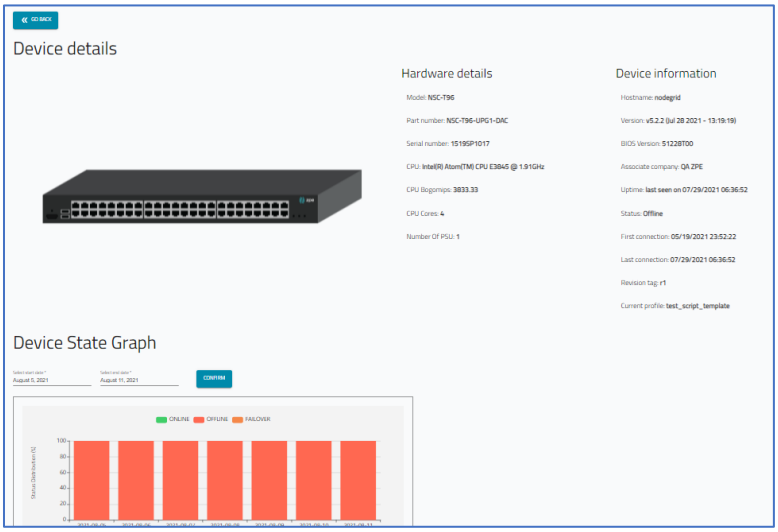
Device Table Columns

Column Name	Description
Hostname	Hostname of the device.
Serial Number	Serial number of the device.
Status	Current status of the device.
Profile in Use	Device's current profile.
Last Update	Last date/time device was updated.

Manage Devices

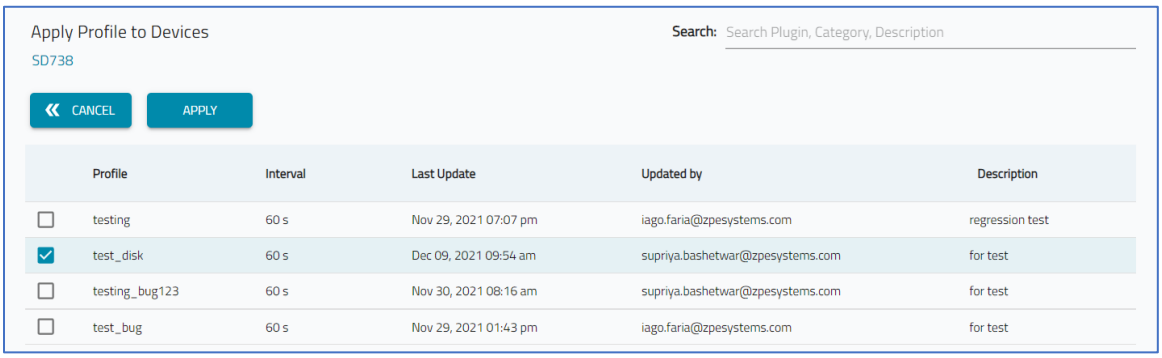
View Device Details

Click on the device hostname to view the *Device Details* page.

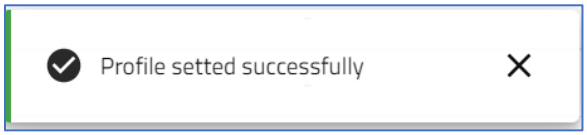


Apply Profile

1. Go to *APPS :: ACTIVE :: NODEGRID DATA LAKE :: DEVICES*.
2. On table, locate device(s), and select checkbox(es).
3. Click **Apply Profile** (displays dialog).

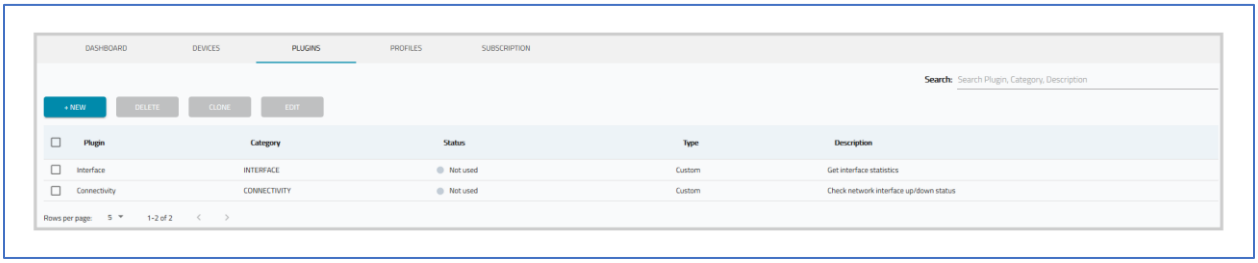


4. Select profile checkboxes to apply.
5. Click **APPLY**.
6. *Success* dialog displays (lower right corner).



PLUGINS tab

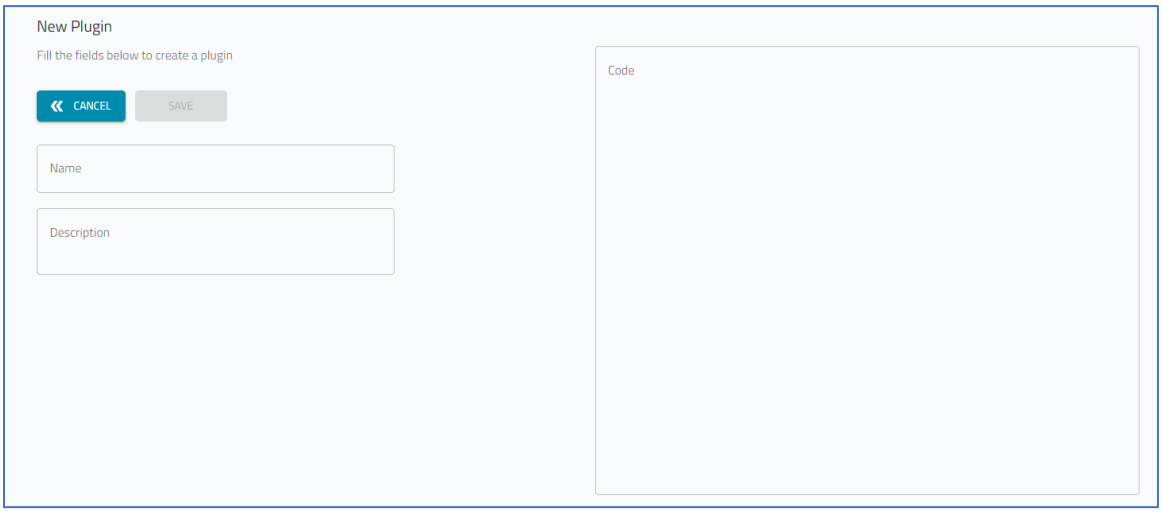
The plugins page manages all plugins.



Manage Plugins

Create new Plugin

1. Go to *APPS :: ACTIVE :: NODEGRID DATA LAKE :: PLUGINS*.
2. Click **NEW** (displays dialog).



3. Enter **Name**.
4. Enter **Description**.
5. In **Code**, paste code for the plugin.
6. Click **SAVE**.

Delete Plugin

1. Go to *APPS :: ACTIVE :: NODEGRID DATA LAKE :: PLUGINS*.
2. On the table, locate and select checkbox.
3. Click **DELETE**.

Clone Plugin

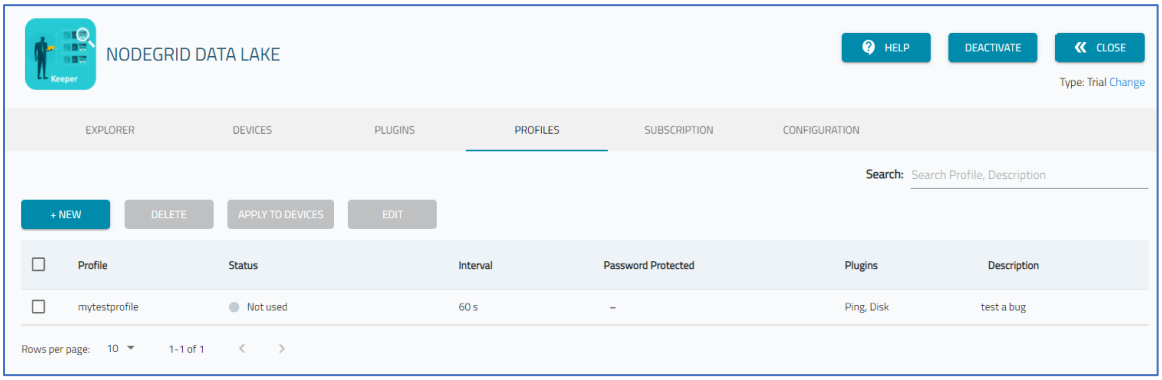
1. Go to *APPS :: ACTIVE :: NODEGRID DATA LAKE :: PLUGINS*.
2. On the table, locate and select checkbox.
3. Click **CLONE** (displays dialog).
4. Make modifications, as needed.
5. Click **SAVE**.

Edit Plugin

1. Go to *APPS :: ACTIVE :: NODEGRID DATA LAKE :: PLUGINS*.
2. On the table, locate and select checkbox.
3. Click **EDIT** (displays dialog).
4. Make modifications, as needed.
5. Click **SAVE**.

PROFILES tab

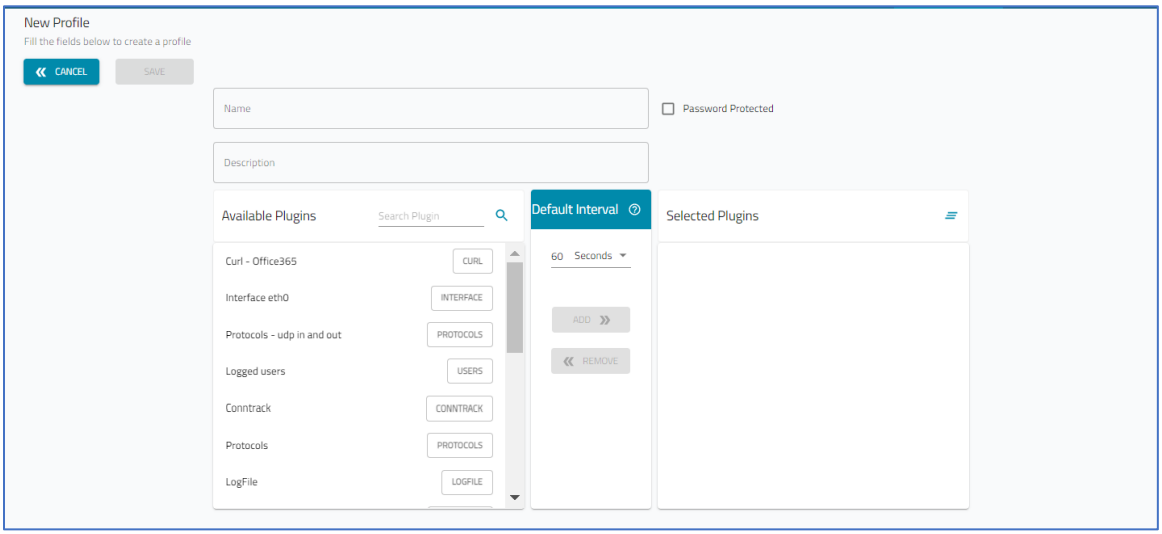
This displays available profiles.



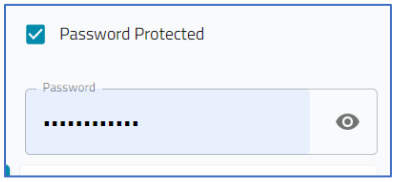
Manage Profiles

Create new Profile

1. Go to *APPS :: ACTIVE :: NODEGRID DATA LAKE :: PROFILES*.
2. Click **NEW** (displays dialog).



3. Enter **Name**.
4. Enter **Description**.
5. (optional) Select **Password Protected** checkbox. Enter **Password**.



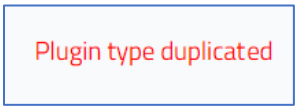
6. In *Available Plugins* panel:

   Select plugin.

   Click **Add** (moves to *Selected Plugins* panel.

   As needed, select one in *Selected Plugins* and click **Remove**.

   If an item is duplicated, a message displays (lower right). To resolve, remove duplicate.



7. In **Default Interval** settings:

   Enter a number.

   On drop-down, select one (**Seconds**, **Minutes**, **Hours**, **Days**, **Weeks**, **Months**)
8. Click **SAVE**.

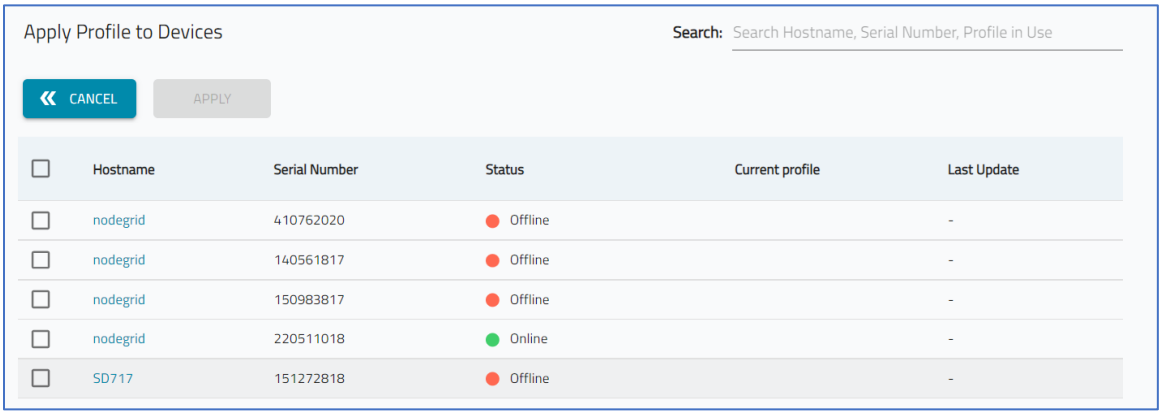
Delete Profile

1. Go to *APPS :: ACTIVE :: NODEGRID DATA LAKE :: PROFILES*.
2. On the table, locate and select checkbox.

3. Click **DELETE**.

Apply Profile to Devices

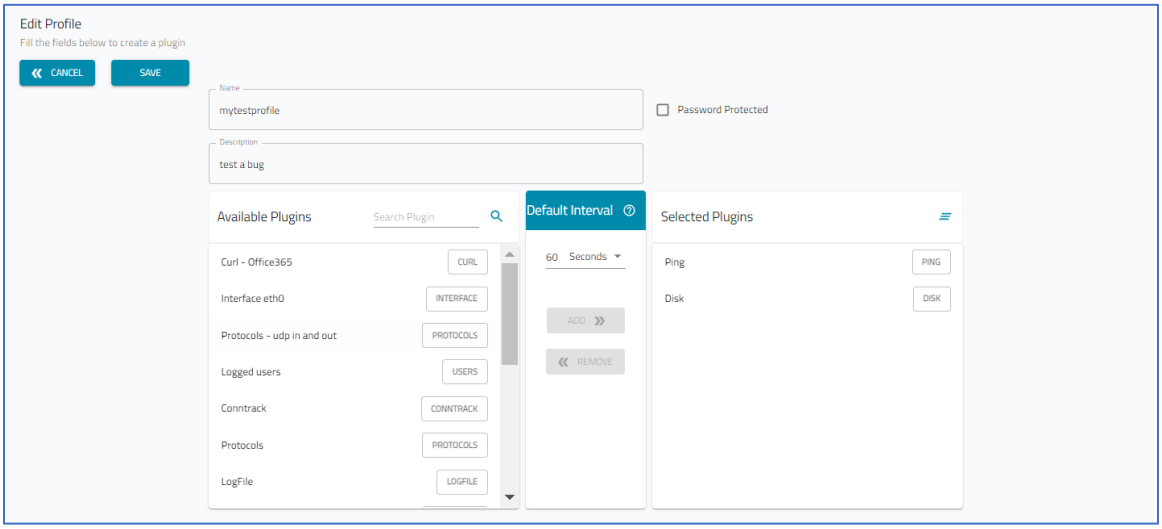
1. Go to *APPS :: ACTIVE :: NODEGRID DATA LAKE :: PROFILES*.
2. On the table, locate and select checkbox.
3. Click **APPLY TO DEVICES** (displays dialog).



4. Select checkboxes.
5. Click **APPLY**.

Edit Profile

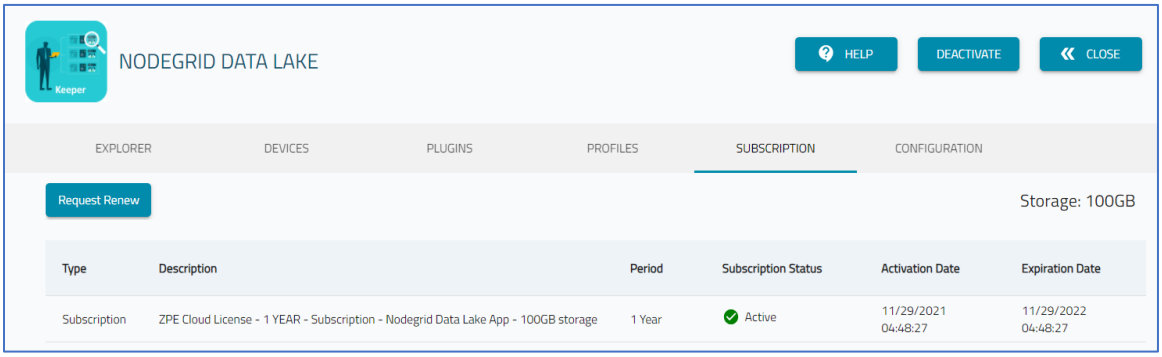
1. Go to *APPS :: ACTIVE :: NODEGRID DATA LAKE :: PROFILES*.
2. On the table, locate and select checkbox.
3. Click **EDIT** (displays dialog).



4. Make modifications, as needed.
5. Click **SAVE**.

SUBSCRIPTION tab

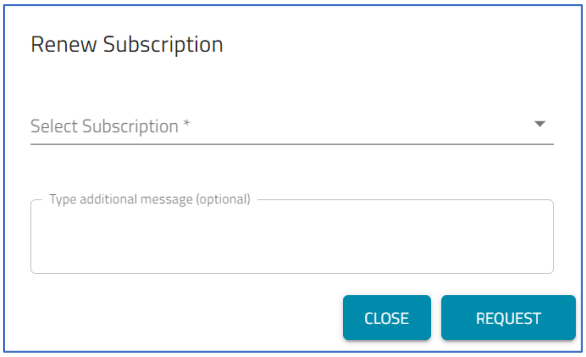
This displays available subscriptions.



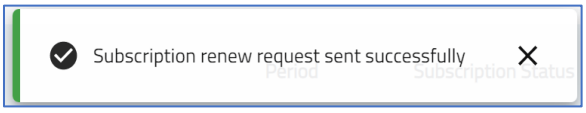
Manage Subscriptions

Renew Subscription

1. Go to *APPS :: ACTIVE :: NODEGRID DATA LAKE :: SUBSCRIPTIONS*.
2. Click **RENEW SUBSCRIPTION** (displays dialog).



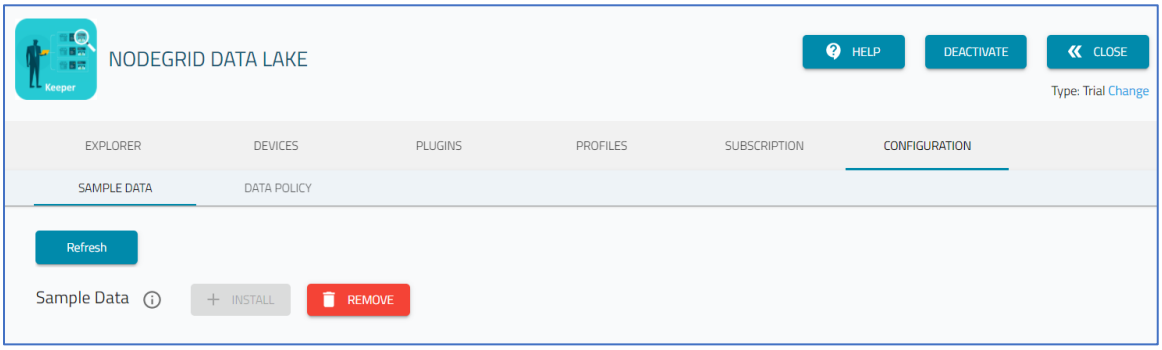
3. On **Select Subscription** drop-down, select one.
4. (as needed) In **Type additional message (optional)**, add details.
5. Click **REQUEST** (displays success dialog).



CONFIGURATION tab

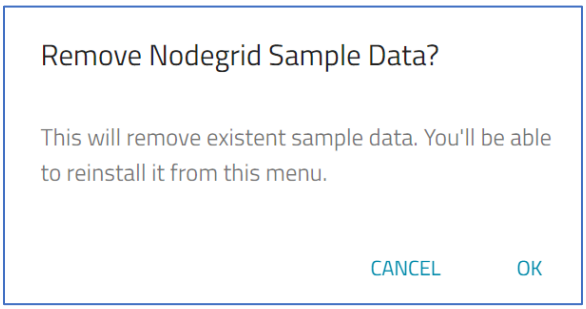
SAMPLE DATA sub-tab

Sample data is provided to demonstrate visualizations on the dashboard works. It is installed on zpe_monitoring_sample index (to avoid conflicts with your device data).



Remove Sample Data

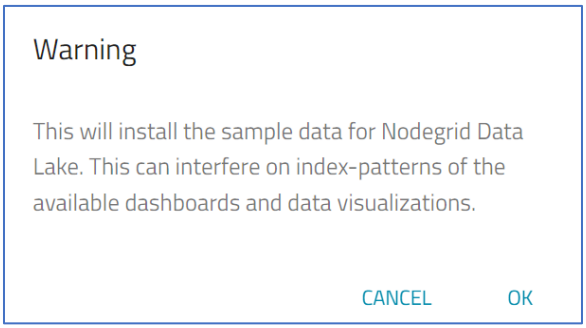
1. Go to *APPS :: ACTIVE :: NODEGRID DATA LAKE :: CONFIGURATION :: SAMPLE DATA*.
2. Click **REMOVE** (displays dialog).



3. Click **OK** to remove (may take about a minute to be removed).

Install Sample Data

1. Go to *APPS :: ACTIVE :: NODEGRID DATA LAKE :: CONFIGURATION :: SAMPLE DATA*.
2. Click **+INSTALL** (displays dialog).



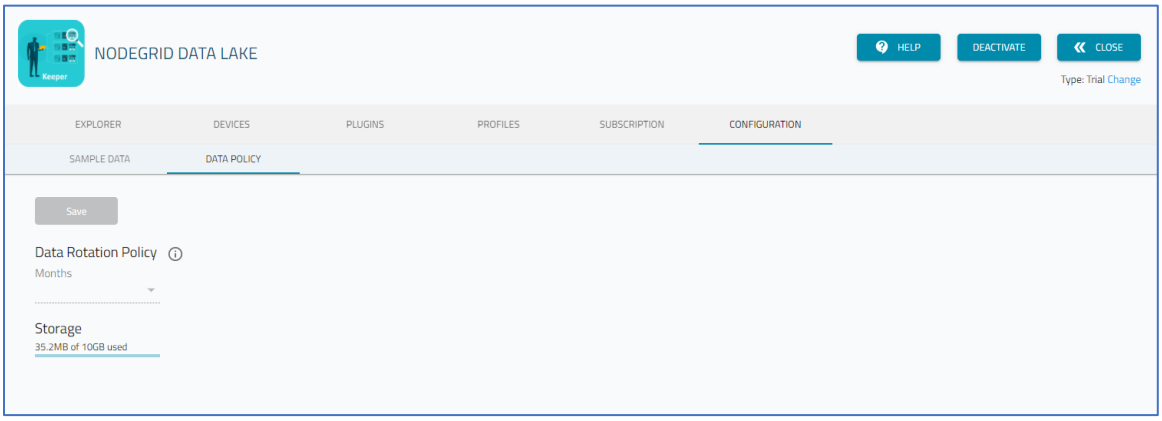
3. Click **OK**.

Refresh Sample Data

1. Go to *APPS :: ACTIVE :: NODEGRID DATA LAKE :: CONFIGURATION :: SAMPLE DATA*.
2. Click **Refresh**
3. Updates and REMOVE becomes available..

DATA POLICY sub-tab

This configuration deletes data older than the selected amount of months.



Change Data Rotation Policy

1. Go to *APPS :: ACTIVE :: NODEGRID DATA LAKE :: CONFIGURATION :: DATA POLICY*.
2. On **Months** drop-down, select one.
3. Click **SAVE**.

Nodegrid Data Lake Plugins

For Nodegrid Data Lake, plugins are available that provide live status details, viewed on the Dashboard. Supported plugins are listed on *APPS :: ACTIVE :: NODEGRID DATA LAKE :: PLUGINS*.

> **NOTE**: Additional plugins are available on the collectd website. If not on the PLUGINS table, check with ZPE Support before using other plugins.

A plugin must be included in a defined Profile. When the Profile is applied to the Dashboard, the plugin is displayed.

See Use Case Example for an overview of the process.

The following plugins are currently provide details (graphics, reports) on the Nodegrid Data Lake application.

ConnTrack

This tracks the number of entries in the Linux connection tracking table.

Arguments

None

Example

Collect usage of the entire CPU.

```
<Plugin conntrack>
```

```
  </Plugin>
```

CPU (Usage, State)

The CPU plugin collects CPU usage metrics. By default, CPU usage is reported as Jiffies, depending on the cpu type. Two aggregations are available:

Sum, per-state (CPUs installed in the system)

Sum, per-CPU (non-idle states of a CPU)

The two aggregations can be combined, leading to collectd only emitting a single "active" metric for the entire system. When an aggregation (or both) is enabled, the cpu plugin reports a percentage, rather than Jiffies. In addition, metric percentages are reported for: individual, per-state, per-CPU.

Arguments

ReportByState <Boolean>

When true (default), reports per-state metrics, i.e., "system", "user" and "idle". When false, aggregates (sums) all non-idle states into one "active" metric.

ReportByCpu <Boolean>

When true (default), reports per-CPU (per-core) metrics. When false, reports only global sum of CPU states.

ValuesPercentage <Boolean>

To be available, ReportByCpu and ReportByState must be true – reports metrics as Jiffies. In the un-aggregated (per-CPU, per-state) mode, percentage values are reported.

ReportNumCpu <Boolean>

When true, reports the number of available CPUs (default: false).

ReportGuestState <Boolean>

When true, reports "guest" and "guest_nice" CPU states (default: false).

SubtractGuestState <Boolean>

Only used if ReportGuestState is true. "guest" and "guest_nice" are included in respectively "user" and "nice". If true, "guest" is subtracted from "user". "guest_nice" is subtracted from "nice" (default: true).

Example 1 – CPU Usage

Collect usage of the entire CPU

```
  <Plugin cpu>
    ReportByCpu false
    ReportByState false
    ValuesPercentage false
    ReportNumCpu false
    ReportGuestState false
```

```
    SubtractGuestState false
  </Plugin>
```

Create Visualization, Example 1

Graph

Chart Type: Area

Mode: Normal

Filters

Plugin - is - cpu

serial_number - is - <serial-number

Y-Axis

Aggregation: average

Field: value

Label: Jiffies

X-Axis

Sub aggregation: Data histogram

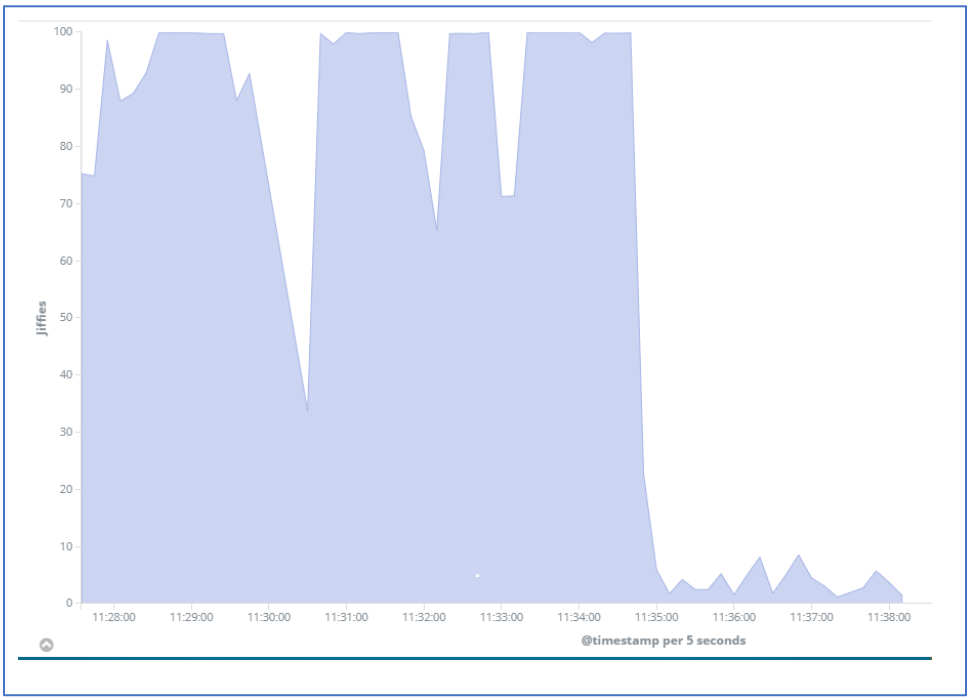
Field: time

Minimum interval: Auto

Example 2 CPU usage by state

Visualize CPU usage by state, stacking system, user and idle states.

```
  <Plugin cpu>
    ReportByCpu true
    ReportByState true
    ValuesPercentage true
    ReportNumCpu false
    ReportGuestState false
    SubtractGuestState false
  </Plugin>
```



Create Visualization, Example 2

Graph

Chart type: Area

Mode: Stacked

Filters

plugin - is - cpu

serial_number - is - <serial-number>

Y-Axis

Aggregation: average

Field: value

Split series

Aggregation: Filters

Filter 1: typeinstance:idle

Filter 2: typeinstance:user

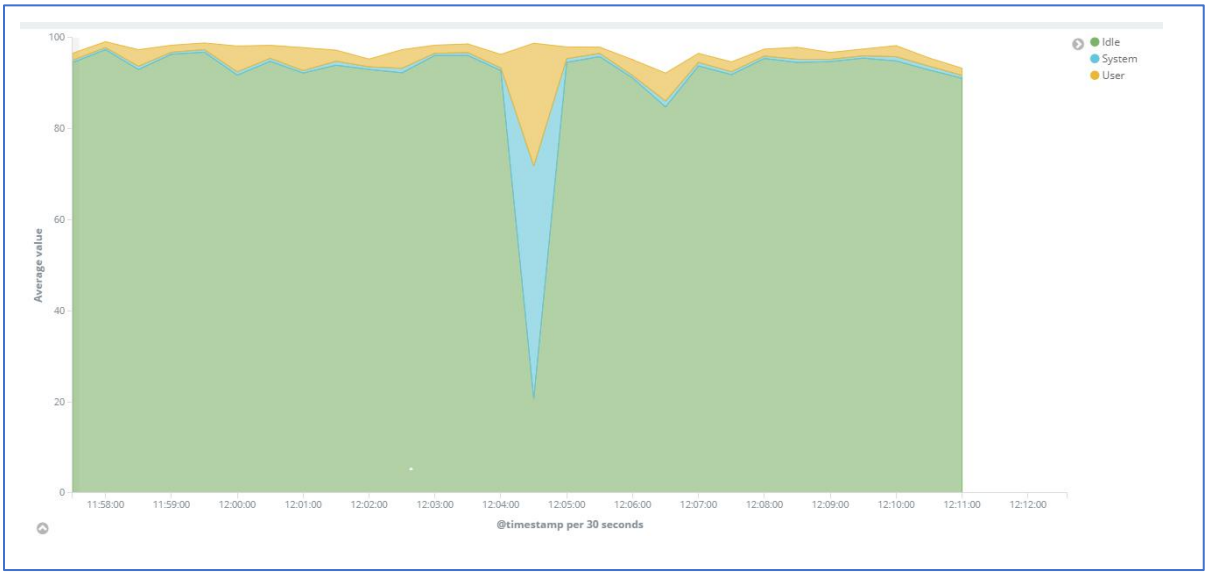
Filter 3: typeinstance:system

X-Axis

Sub aggregation: Data histogram

Field: time

Minimum interval: Auto



Curl

This plugin uses libcurl to read files and then parses them according to the configuration. The cURL library reads web pages via HTTP. Many protocol handlers are available – reading via SSH or from FTP as well as local access via file://.

Arguments

URL <String>

URL of the web site to retrieve. Since a regular expression is used to extract information from this data, non-binary data is a big plus.

User Name <String>

Username to use if authorization is required to read the page.

Password <String>

Password to use if authorization is required to read the page.

Digest <Boolean>

Enable HTTP digest authentication.

VerifyPeer <Boolean>

Enable or disable peer SSL certificate verification. See http://curl.haxx.se/docs/sslcerts.html for details (default: enabled).

VerifyHost <Boolean>

Enable or disable peer host name verification. If enabled, the plugin checks if the Common Name or a Subject Alternate Name field of the SSL certificate matches the host name provided by the URL option. If this identity check fails, the connection is aborted. Obviously, only works when connecting to an SSL-enabled server. Default: enabled.

CACert file <String>

File of one or more SSL certificates. To use HTTPS, this is needed. The CA certificates bundled with libcurl and are applied depend on the distribution.

Header <String>

A HTTP header to add to the request. Multiple headers are added if this option is specified more than once.

Post Body <String>

Specifies the HTTP operation should be POST instead of GET. The complete data to be posted is given as the argument. This option needs to be accompanied by a Header option to set an appropriate Content-Type for the post body (i.e., to application/x-www-form-urlencoded).

MeasureResponseTime <Boolean>

Measure response time for the request. If this setting is enabled, Match blocks (see below) are optional (default: disabled).

IMPORTANT: requests are aborted if take too long to complete. Adjust Timeout accordingly expected MeasureResponseTime to report slow requests. This option is similar to enabling the TotalTime statistic but is measured by collectd instead of cURL.

MeasureResponseCode <Boolean>

Measure response code for the request. If is enabled, Match blocks (see below) are optional. Default: disabled.

<Statistics>

One Statistics block can be used to specify cURL statistics to be collected for each request to the remote web site. See "cURL Statistics" above for details. If enabled, Match blocks (see below) are optional.

<Match>

One or more Match blocks that define how information is matched in the data returned by libcurl. The cURL plugin uses the same infrastructure as the tail plugin. See the documentation of the tail plugin below on how matches are defined. If the MeasureResponseTime or MeasureResponseCode options are set to true, Match blocks are optional.

Timeout Milliseconds <Integer>

The Timeout option sets the overall timeout for HTTP requests to URL, in milliseconds. By default, the configured Interval is used to set the timeout. Prior to version 5.5.0, there was no timeout and requests could hang indefinitely. To use this legacy behavior, set Timeout = 0.

If Timeout is 0 or bigger than the Interval, each slow network connection stalls one read thread. Adjust the ReadThreads global setting to prevent blocking other plugins.

Example: Curl – Office 365

Check if Office 365 is up and display response code

```
   <Plugin curl>
```

```
    <Page "office365">
      URL "http://office365.com/"
      MeasureResponseTime true
      MeasureResponseCode true
      Timeout 10000 # 10 seconds
    </Page>
  </Plugin>
```

Disk

The Disk plugin collects performance statistics of hard-disks and partitions.

Arguments

Disk Name <String|Regex>

Select the disk Name. Whether it is collected or ignored depends on the IgnoreSelected setting, see below. As with other plugins that use the daemon's ignorelist functionality, a string that starts and ends with a slash is interpreted as a regular expression.

IgnoreSelected <Boolean>

Sets whether selected disks, i. e. the matches by any of the Disk statements, are ignored or if all other disks are ignored. The behavior (hopefully) is intuitive: If no Disk option is configured, all disks are collected. If at least one Disk option is given and no IgnoreSelected or set to false, only matching disks are collected. If IgnoreSelected = true, all disks are collected except those that match.

UseBSDName <Boolean>

Whether to use the device's "BSD Name", on Mac OS X, instead of the default major/minor numbers. Requires collectd to be built with Apple's IOKitLib support.

UdevNameAttr <String>

Attempt to override disk instance name with the value of a specified udev attribute when built with libudev. If the attribute is not defined for the given device, the default name is used.

Example

Collect statistics for all partitions

```
  <Plugin disk>
    Disk "/sda[0-9]/"
    IgnoreSelected false
  </Plugin>
```

Create Visualization

Graph

Chart type: Line

Mode: Normal

Filters

plugin - is - disk

type.keyword - is - disk_time

Y-Axis

Aggregation: average

Field: value

Custom label: Avg.Time/Operation (ms)

Split series

Aggregation: Terms

Field: plugininstance.keyword

X-Axis

Sub aggregation: Data histogram

Field: time

Minimum interval: Auto

Exec

The Exec plugin executes bash scripts and reads values back that are printed to STDOUT by that program. This allows the daemon to be extended in an easy, flexible way.

Arguments

```
Exec "system-user" "/path/to/script" "arg0" "arg1"
```

Example 1

Collect statistics for all partitions

```
<Plugin exec>
  Exec "collectd-user" "/home/admin/custom_df.sh"
</Plugin>
```

NOTE: The DF plugin from collectd is not currently installed on NG v5.0, but it is possible to obtain the statistics with the following exec scripts.

Create a file named **custom_df.sh** under the /home/admin/ directory of the device and add the following script:

```
HOSTNAME="${COLLECTD_HOSTNAME:-nodegrid}"
INTERVAL="${COLLECTD_INTERVAL:-10}"

# Collectd metric output pattern
# PUTVAL "<hostname>/<plugin-name>-<plugin-instance>/<type>-<type-instance>"
interval=<interval> N:<value>
# Type = [gauge, absolute, derive, counter]

df | awk -v hostname="$HOSTNAME" -v interval="$INTERVAL" '
$0 !~ /\/dev\/sda[0-9]/ { next }
    {split($1, filesystem, "/")}
    {sub(/%/, "", $5)}
    {print "PUTVAL \""hostname"/custom_df-"filesystem[3]"/gauge-total\"
interval="interval" N:"$2}
    {print "PUTVAL \""hostname"/custom_df-"filesystem[3]"/gauge-used\"
interval="interval" N:"$3}
    {print "PUTVAL \""hostname"/custom_df-"filesystem[3]"/gauge-available\"
interval="interval" N:"$4}
    {print "PUTVAL \""hostname"/custom_df-"filesystem[3]"/gauge-percent-used\"
interval="interval" N:"$5}
'
sleep "$INTERVAL"
```

Create Visualization, Example 1

Graph

Chart type: Line

Mode: Normal

Filters

plugin - is - custom_df

typeinstance.keyword - is - percentage-used

Y-Axis

Aggregation: average

Field: value

Custom label: % Usage

Split series

Aggregation: Terms

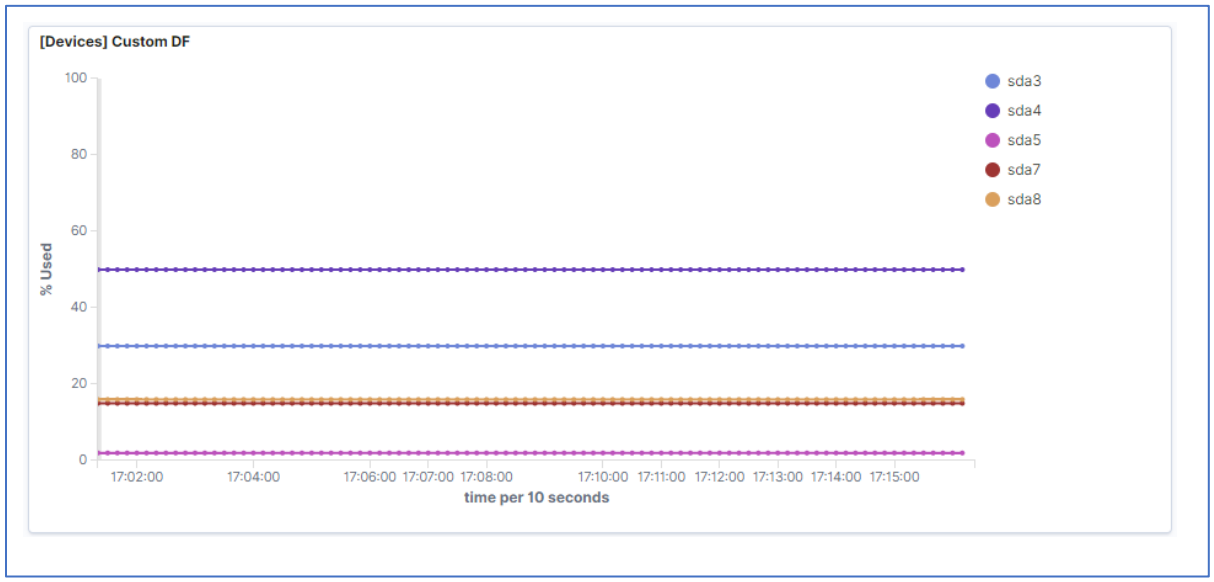
Field: plugininstance.keyword

X-Axis

Sub aggregation: Data histogram

Field: time

Minimum interval: Auto



Example 2

This collect statistics from smartctl

```
<Plugin exec>
  Exec "collectd-user" "/home/admin/custom_smartctl.sh"
</Plugin>
```

NOTE: The smartctl plugin from collectd is not installed on NG5.0, but metrics can be collected from smartctl with the following script.

Create a file named custom_smartctl.sh under /home/admin/ directory of the device and add the following script:

```
HOSTNAME="${COLLECTD_HOSTNAME:-nodegrid}"
INTERVAL="${COLLECTD_INTERVAL:-10}"

# Collectd metric output pattern
```

```
# PUTVAL "<hostname>/<plugin-name>-<plugin-instance>/<type>-<type-instance>"
interval=<interval> N:<value>
# Type = [gauge, absolute, derive, counter]


sudo /usr/sbin/smartctl -f old -H -A /dev/sda -C | awk -v hostname="$HOSTNAME" -v
interval="$INTERVAL" '
{
        if ($0 ~ /^SMART overall-health self-assessment test result/){
                if ($0 ~ /PASSED/){
                        print "PUTVAL \""hostname"/custom_smartctl-sda/gauge-health-
result\" interval="interval" N:1"
                        next
                }
                else{
                        print "PUTVAL \""hostname"/custom_smartctl-sda/gauge-health-
result\" interval="interval" N:0"
                        next
                }
        }
        else{
                if ($3 ~ /^0x/){
                        if ($2 == "Later_Bad_Block" ||
                            $2 == "Power_On_Hours" ||
                            $2 == "Power_Cycle_Count" ||
                            $2 == "Remaining_Lifetime_Perc" ||
                            $2 == "Temperature_Celsius" ||
                            $2 == "Current_Pending_Sector"){
                            print "PUTVAL \""hostname"/custom_smartctl-"$2"/gauge-
value\" interval="interval" N:"$4
                            print "PUTVAL \""hostname"/custom_smartctl-"$2"/gauge-
worst\" interval="interval" N:"$5
                            print "PUTVAL \""hostname"/custom_smartctl-"$2"/gauge-
thresh\" interval="interval" N:"$6
                        }
                }
        }
}
'
sleep "$INTERVAL"
```

smartctl requires root permission to execute. For security reasons, the Exec plugin (collectd) cannot execute scripts as root. To resolve this, create a user with permissions to use collectd for script executions.

On the device, create a new collectd user.

```
adduser -s /bin/false collectd-user
```

```
usermod -aG sudo collectd-user
```

On the device, go to /etc/sudoers folder and open the sudoers file. Add the following lines to the end of the file (allows collectd-user to execute only the smartclt command as sudo).

```
collectd-user ALL=(ALL) !ALL
collectd-user ALL=(ALL) NOPASSWD: /usr/sbin/smartctl -f old -H -A /dev/sda -C
```

Create Visualization, Example 2

Graph

Chart type: Line

Mode: Normal

Filters

plugin - is - custom_smartctl

typeinstance.keyword - is - Remaining_Lifetime_Perc

Y-Axis

Aggregation: average

Field: value

Custom label: % Remaining Lifetime

Split series

Aggregation: Filters

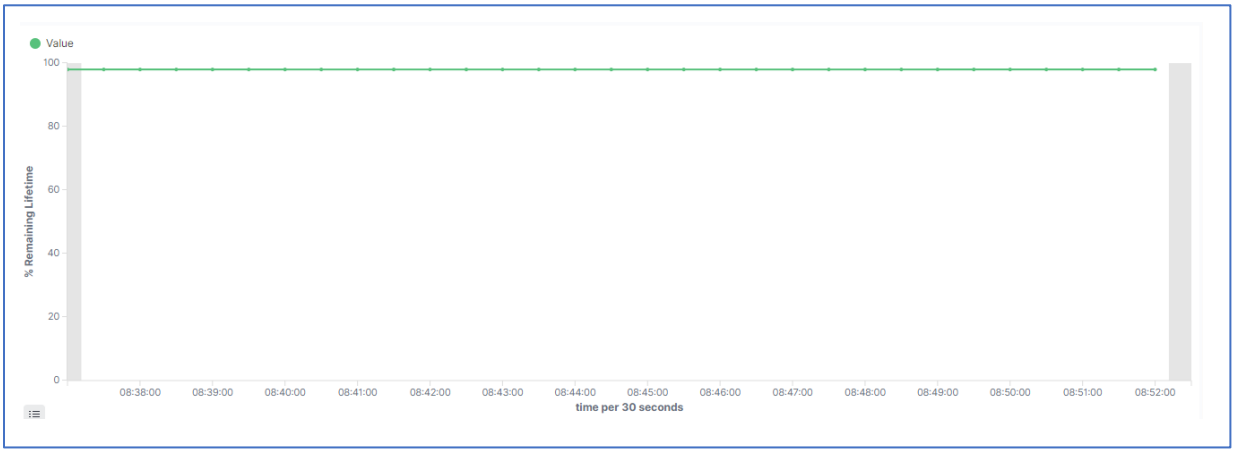
Filter 1: typeinstance:value

X-Axis

Sub aggregation: Data histogram

Field: time

Minimum interval: Auto



Example 3

Reading air velocity and temperature from USB sensor.

```
<Plugin exec>
  Exec "collectd-user" "Exec "admin" "/home/admin/usb_sensor.sh"
</Plugin>
```

This example collects air velocity and air temperature from a sensor connected to an USB port from Nodegrid. Once the USB ports are owned by root, it is necessary to modify permissions to allow the user described on the exec plugin to access the sensor.

The following script must be stored inside the device and the user defined on the configuration must have execution permission:

```
HOSTNAME="${COLLECTD_HOSTNAME:-nodegrid}"
INTERVAL="${COLLECTD_INTERVAL:-10}"

# Collectd metric output pattern
# PUTVAL "<hostname>/<plugin-name>-<plugin-instance>/<type>-<type-instance>"
interval=<interval> N:<value>
# Type = [gauge, absolute, derive, counter]

/usr/bin/python3 - <<EOF
import serial
import os

hostname = os.getenv('HOSTNAME') or 'nodegrid'
interval = os.getenv('INTERVAL') or 10
sensor = "usb_sensor"
sensor_port = "usbS3"

try:
        ser = serial.Serial(port='/dev/usbS3', baudrate=19200,
bytesize=serial.EIGHTBITS, parity=serial.PARITY_NONE, stopbits=serial.STOPBITS_ONE)
```

```
        if not ser.is_open:
                print('PUTVAL "{0}/{1}-{2}/gauge-air_temperature_success" interval={3}
N:{4}'.format(hostname, sensor, sensor_port, interval, 0))
                print('PUTVAL "{0}/{1}-{2}/gauge-air_velocity_success" interval={3}
N:{4}'.format(hostname, sensor, sensor_port, interval, 0))
                exit(1)
except:
        print('PUTVAL "{0}/{1}-{2}/gauge-air_temperature_success" interval={3}
N:{4}'.format(hostname, sensor, sensor_port, interval, 0))
        print('PUTVAL "{0}/{1}-{2}/gauge-air_velocity_success" interval={3}
N:{4}'.format(hostname, sensor, sensor_port, interval, 0))
        exit(1)


# Creating read air temperature request
request_msg = bytearray(4)
request_msg[0] = 0X02                               # read air temperature operation
request_msg[1] = 0X00                               # reserved
request_msg[2] = 0X00                               # reserved
request_msg[3] = request_msg[0] ^ request_msg[1] ^ request_msg[2]      # XOR checksum

ser.write(request_msg)

# read reply
reply_msg_size = 4                                  # protocol definition
reply = ser.read(reply_msg_size)

# reply verification
reply_checksum = reply[0] ^ reply[1] ^ reply[2]    # XOR checksum

if reply_checksum == reply[3]:
        # Value convertion to Celsius grades
        temperature = float(0)
        temperature = reply[0] << 8                 # reply[0] is Most Significant byte
        temperature |= reply[1]                     # reply[1] is Least Significant
byte
        temperature /= 100                          # to Celsius grades conversion

        print('PUTVAL "{0}/{1}-{2}/gauge-air_temperature" interval={3}
N:{4}'.format(hostname, sensor, sensor_port, interval, temperature))
        print('PUTVAL "{0}/{1}-{2}/gauge-air_temperature_success" interval={3}
N:{4}'.format(hostname, sensor, sensor_port, interval, 1))

else:
        print('PUTVAL "{0}/{1}-{2}/gauge-air_temperature_success" interval={3}
N:{4}'.format(hostname, sensor, sensor_port, interval, 0))
```

```
# Creating read air velocity request
request_msg = bytearray(4)
request_msg[0] = 0X01                                  # read air velocity operation
request_msg[1] = 0X00                                  # reserved
request_msg[2] = 0X00                                  # reserved
request_msg[3] = request_msg[0] ^ request_msg[1] ^ request_msg[2]      # XOR checksum

ser.write(request_msg)

# read reply
reply_msg_size = 4                                     # protocol definition
reply = ser.read(reply_msg_size)

# reply verification
reply_checksum = reply[0] ^ reply[1] ^ reply[2]     # XOR checksum

if reply_checksum == reply[3]:
        # Value convertion to m/s
        velocity = float(0)
        velocity = reply[0] << 8                # reply[0] is Most Significant byte
        velocity |= reply[1]                    # reply[1] is Least Significant byte
        velocity /= 1000                        # to m/s conversion

        print('PUTVAL "{0}/{1}-{2}/gauge-air_velocity" interval={3}
N:{4}'.format(hostname, sensor, sensor_port, interval, velocity))
        print('PUTVAL "{0}/{1}-{2}/gauge-air_velocity_success" interval={3}
N:{4}'.format(hostname, sensor, sensor_port, interval, 1))

else:
        print('PUTVAL "{0}/{1}-{2}/gauge-air_velocity_success" interval={3}
N:{4}'.format(hostname, sensor, sensor_port, interval, 0))

EOF

sleep "$INTERVAL"
```

Interface

The Interface plugin collects information about the traffic (octets per second), packets per second and errors of interfaces (of course number of errors during one second).

Arguments

Interface <String>

Select this interface. By default, these interfaces are collected. For a more detailed description see IgnoreSelected below.

IgnoreSelected <Boolean>

If no configuration is given, the interface-plugin collects data from all interfaces. This may not be practical, especially for loopback- and similar interfaces. Use the Interface-option to pick appropriate interfaces. Sometimes it is easier/preferred to collect all interfaces except a couple excluded interfaces. If IgnoreSelected = true, the effect of Interface is inverted: All selected interfaces are ignored and all other interfaces are collected.

It is possible to use regular expressions to match interface names. If the name is surrounded by /.../ and collectd was compiled with support for regexps. This is useful if there's a need to collect (or ignore) data for a group of interfaces that are similarly named, without the need to explicitly list all of them (especially useful if the list is dynamic).

ReportInactive <Boolean>

When set to false, only interfaces with non-zero traffic is reported. Note that the check is done by looking into whether a package was sent at any time from boot, and the corresponding counter is non-zero. So, if the interface has been sending data in the past since boot, but not during the reported time-interval, it is still reported.

Default = true collects data from all interfaces selected by Interface and IgnoreSelected options.

Example: Interface eth0/eth1

Collect statistics of eth0 and eth1

```
<Plugin interface>
  Interface "eth0"
  Interface "eth1"
</Plugin>
```

Load

This plugin collects the system load. The numbers give a rough overview over the utilization of a machine. The system load is defined as the number of runnable tasks in the run-queue and is provided by many operating systems at a one, five, or fifteen minute average.

Arguments

ReportRelative <Boolean>

When enabled, system load, divided by number of available CPU cores, is reported for intervals 1 min, 5 min and 15 min. Default: false.

Example: CPU Load

Collect statistics of eth0 and eth1

```
<Plugin load>
</Plugin>
```

LogFile

The LogFile plugin receives log messages from the daemon and writes them to a text file. This plugin can be used to debug the configuration of plugins to make sure collectd is running properly. In order for

other plugins to be able to report errors and warnings during initialization, the LogFile plugin should be loaded as the first plugin (or one of the first) in the configuration file.

Arguments

LogLevel <String> [debug | info | notice | warning | err]

Sets log-level. If, for example, set to notice, then all events with severity notice, warning, or err will be written to the logfile.

Debug is only available if collectd has been compiled with debugging support.

File <String>

Sets the file to write log messages. The special strings "stdout" and "stderr" can be used to write to the standard output and standard error channels, respectively. This makes sense when collectd is running in foreground- or non-daemon-mode.

Timestamp <Boolean>

Prefix all lines with timestamp. Default: true.

PrintSeverity <Boolean>

When enabled, all lines are prefixed by the severity of the log message, for example "warning". Default: false.

Example

Log collectd info messages to a file.

```
  <Plugin logfile>
    LogLevel info
    File "/home/admin/collectd.log"
    Timestamp true
    PrintSeverity false
  </Plugin>
```

Use this example to ensure the created profile is working properly on the device. Collectd creates file in the home directory of admin user and logs information about the loaded plugins. This file can be retrieved with the device's File Manager.

Memory

Collects physical memory utilization follow the categories below:

Usage

Buffered

Cached

Free

slab_recl

slab_unrecl

Arguments

ValuesAbsolute <Boolean>

Enables or disables reporting of physical memory usage in absolute numbers (i.e., bytes). Default: true.

ValuesPercentage <Boolean>

Enables or disables reporting of physical memory usage in percentages (i.e., percent of physical memory used). Default: false.

This is useful for deploying collectd in a heterogeneous environment in which the sizes of physical memory vary.

Example

Display memory usage with stacked categories:

```
<Plugin memory>
        ValuesAbsolute false
        ValuesPercentage true
</Plugin>
```

Create visualization

Graph

Chart type: Area

Mode: Stacked

Filters

plugin - is - memory

serial_number - is - <serial-number>

Y-Axis

Aggregation: average

Field: value

Custom label: % of memory usage

Split series

Aggregation: Filters

Filter 1: typeinstance:free

Filter 2: typeinstance:used

Filter 3: typeinstance:buffered

Filter 4: typeinstance:cached

Filter 5: typeinstance:slab_unrecl

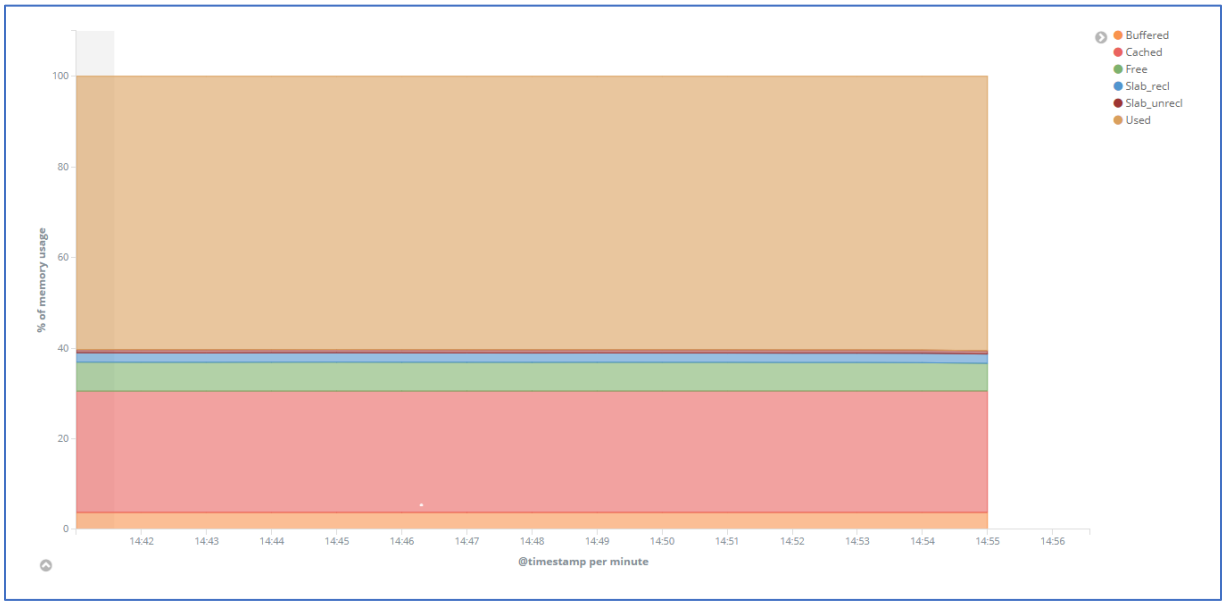
Filter 6: typeinstance:slab_recl

X-Axis

Sub aggregation: Data histogram

Field: time

Minimum interval: Auto



Ping

Measures network latency using ICMP echo requests.

Arguments

Host <String>

Host to ping periodically. This option may be repeated several times to ping multiple hosts.

Interval <Float>

Sets the interval in which to send ICMP echo packets to the configured hosts. This is not the interval in which metrics are read from the plugin but the interval in which the hosts are "pinged". Therefore, the setting here should be smaller than or equal to the global Interval setting. Fractional times, such as "1.24" are allowed.

Default: 1.0

Timeout <Float>

Time to wait for a response from the host to which an ICMP packet had been sent. If a reply was not received after Seconds value, the host is assumed to be down or the packet to be dropped. This setting must be smaller than the Interval setting above for the plugin to work correctly. Fractional arguments are accepted.

Default: 0.9

TTL <Integer> [0-255]

Sets the Time-To-Live of generated ICMP packets.

Size <Integer>

Sets the size of the data payload in ICMP packet to specified size (it will be filled with regular ASCII pattern). If not set, default 56 byte long string is used so that the packet size of an ICMPv4 packet is exactly 64 bytes, similar to the behavior of normal ping(1) command.

SourceAddress <String>

Sets the source address to use. host may either be a numerical network address or a network hostname

Device <String>

Sets the outgoing network device to be used. name has to specify an interface name (e. g. eth0). This might not be supported by all operating systems.

MaxMissed <Integer>

Trigger a DNS resolve after the host has not replied to Packets. This enables the use of dynamic DNS services (like dyndns.org) with the ping plugin.

Default: -1 (disabled)

Example

Display latency for 2 websites

```
<Plugin ping>
        Host "zpecloud.com"
        Host "zpesystems.com"
        Interval 1.0
        Timeout 0.9
</Plugin>
```

Create visualization

Filters

plugin - is - ping

type - is - ping

Y-Axis

Aggregation: average

Field: value

Custom label: ms

Split series

Aggregation: Terms

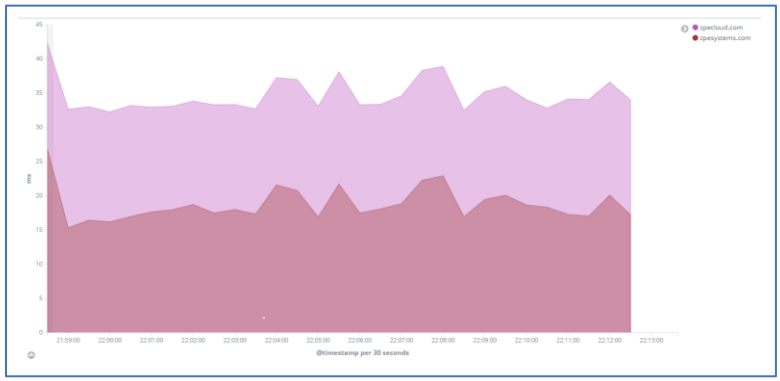
Field: typeinstance.keyword

X-Axis

Sub aggregation: Data histogram

Field: time

Minimum interval: Auto



Process

Collects information about processes of local system. By default, with no process matches configured, only general statistics are collected, such as the number of processes in each state and fork rate.

Process matches can be configured by Process and ProcessMatch options. These may also be a block in which further options may be specified.

The statistics collected for matched processes are: - size of the resident segment size (RSS) - user- and system-time used - number of processes - number of threads - number of open files (under Linux) - number of memory mapped files (under Linux) - io data (where available) - context switches (under Linux) - minor and major page faults.

Arguments

Process <String>

Select more detailed statistics of processes matching this name.

Some platforms have a limit on the length of process names. Name must stay below this limit.

ProcessMatch <String>

Select more detailed statistics of processes matching the specified regex (see regex(7) for details). The statistics of all matching processes are summed up and dispatched to the daemon using the specified name as an identifier. This allows one to "group" several processes together. name must not contain slashes.

CollectContextSwitch <Boolean>

Collect the number of context switches for matched processes. Disabled by default.

CollectFileDescriptor <Boolean>

Collect number of file descriptors of matched processes. Disabled by default.

CollectMemoryMaps <Boolean>

Collect the number of memory mapped files of the process. The limit for this number is configured via /proc/sys/vm/max_map_count in the Linux kernel.

(options) CollectContextSwitch and CollectFileDescriptor can be used inside Process and ProcessMatch blocks (affects corresponding match only). Otherwise, this sets the default value for subsequent matches.

Example

Display processes

```
<Plugin processes>
       CollectFileDescriptor false
       CollectContextSwitch false
       CollectMemoryMaps false
       CollectDelayAccounting false
</Plugin>
```

Protocols

Collects information about various network protocols, such as IP, TCP, UDP.

Arguments

Value <Protocol:ValueName|Regex>

Selects whether or not to select a specific value. The string being matched is of the form "Protocol:ValueName", where Protocol will be used as the plugin instance and ValueName will be used as type instance. An example of the string being used would be Tcp:RetransSegs.

Use regular expressions to match a large number of values with just one configuration option. To select all "extended" TCP values, use the following parameters:

Value "/^TcpExt:/"

Whether only matched values are selected or all matched values are ignored depends on the IgnoreSelected. By default, only matched values are selected. If no value is configured at all, all values will be selected.

See /"IGNORELISTS" for details.

IgnoreSelected <Boolean>

If set to true, inverts the selection made by Value, I. e. all matching values will be ignored.

Example 1: ICMP Reachable

Collect statistics about the number of ICMP Destination Unreachable messages received

```
<Plugin protocols>
  Value "Icmp:InDestUnreachs"
  IgnoreSelected false
</Plugin>
```

Example 2: UDP in and out

Collect statistics about UDP in and out activity.

```
  <Plugin protocols>
    Value "Udp:InDatagrams"
    Value "Udp:OutDatagrams"
    IgnoreSelected false
  </Plugin>
```

Tail

Tail plugin follows files, similar to tail command, being able to parse each line and check matches using regular expressions. The matches can be used to increment counters.

Arguments

Regex <Regex>

Sets the regular expression to use for matching against a line.

ExcludeRegex <Regex>

Sets an optional regular expression to use for excluding lines from the match.

Type <Type>

Sets the type used to dispatch this value.

Instance <String>

This optional setting sets the type instance to use.

Example: Tail – Failed login

Count failed attempts to login via ssh or console

```
  <Plugin tail>
    <File "/var/log/auth-fail">
      Instance "auth"
      <Match>
        Regex ".*.Event.ID.*[0-9]\..Failed:.*@[0-9\.]{7,15}\."
        DSType "DeriveInc"
        Type "derive"
        Instance "failed_login_ssh"
      </Match>
      <Match>
        Regex ".*.Event.ID.*[0-9]\..Failed:.*.on.'ttyS[0-9]'\."
        DSType "DeriveInc"
        Type "derive"
        Instance "failed_login_console"
      </Match>
    </File>
```

```
  </Plugin>
```

Tcpconns

The tcpconns plugin counts the number of currently established TCP connections based on the local port and/or the remote port. It collects information from the files:

```
/proc/net/snmp
/proc/net/netstat
```

Arguments

ListeningPorts <Boolean>

If this option is set to true, statistics for all local ports for which a listening socket exists are collected. The default depends on LocalPort and RemotePort (see below): If no port at all is specifically selected, the default is to collect listening ports. If specific ports (no matter if local or remote ports) are selected, this option defaults to false, i. e. only the selected ports will be collected unless this option is set to true specifically.

LocalPort <Integer>

Count the connections to a specific local port to see how many connections are handled by a specific daemon (i.e., mailserver). Port must be numeric characters. For the mailserver example, use 25.

RemotePort <Boolean>

Count the connections to a specific remote port to determine how much a remote service is used (i.e., how many connections a mail server or news server has to other mail or news servers, or how many connections a web proxy holds to web servers). Port must be numeric characters only.

AllPortsSummary <Boolean>

(optional) If true, a summary of statistics from all connections are collected (default: false).

Example

Collect information from all ports that are listening

```
  <Plugin tcpconns>
    ListeningPorts true
  </Plugin>
```

Thermal

The thermal plugin reads the ACPI thermal zone.

Arguments

ForceUseProcfs <Boolean>

The Thermal plugin tries to read statistics from the Linux sysfs interface. If not available, the plugin falls back to the procfs interface. If true, the plugin is forced to use the procfs (default: false).

Device <String>

Selects name of the thermal device to collect or ignore (value of the IgnoreSelected option). Can be used multiple times to specify a list of devices.

IgnoreSelected <Boolean>

Invert the selection: If true, all devices except those that match the specified device names (Device option) are collected. By default, only selected devices are collected if a selection is made. If no selection is configured, all devices are selected.

Example: CPU Temperature

Display temperature from ACPI and CPU package

```
  <Plugin thermal>
  </Plugin>
```

Create visualization

Graph

Chart type: Gauge

Filters

plugin - is - thermal

Y-Axis

Aggregation: average

Field: value

Custom label: Degrees Celsius

Split group

Aggregation: Filters

Filter 1: plugininstance:thermal_zone0

Filter 2: plugininstance:thermal_zone1

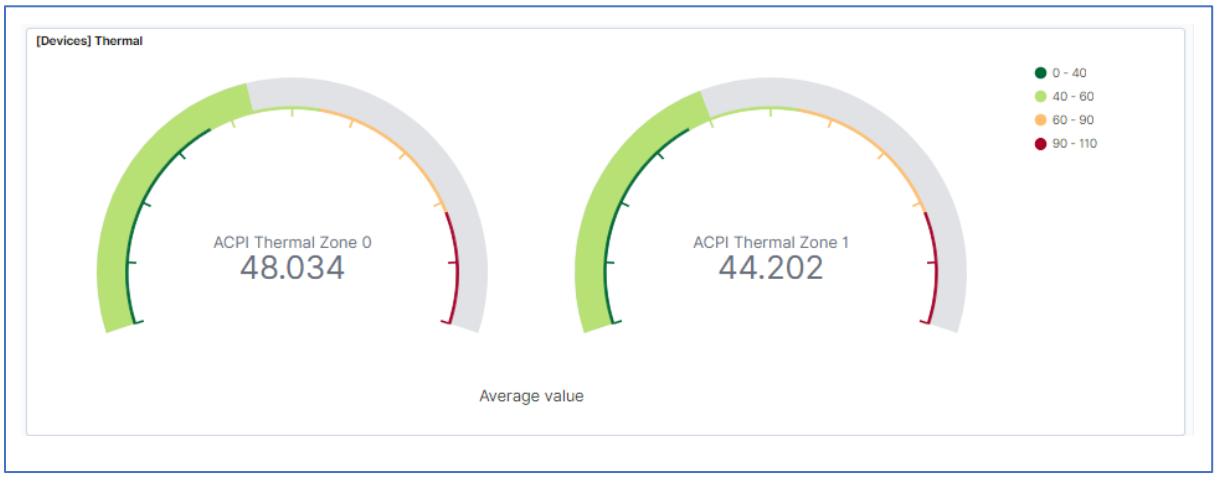
Ranges:

0 → 40

40 → 60

60 → 90

90 → 110



Uptime

The Uptime plugin keeps track of the system uptime.

Arguments

None

Example

Display uptime in seconds

```
<Plugin uptime>
</Plugin>
```

Create visualization

Graph

Chart type: Metric

Filters

plugin - is - uptime

Metric

Aggregation: Top hit

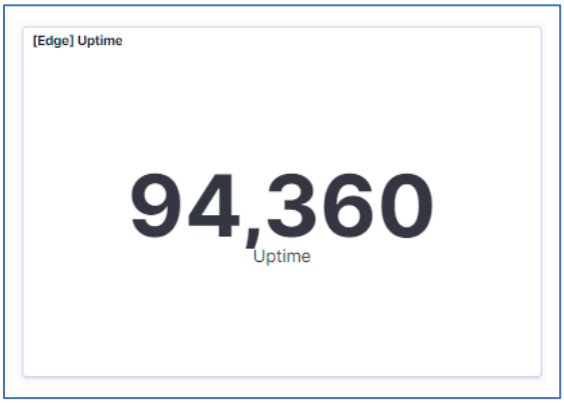
Field: value

Aggregate with: Concatenate

Size: 1

Sort on: time

Custom label: Uptime (seconds)



Users

The Users plugin counts the number of users currently logged into the system.

Arguments

None

Example: Logged users

Display logged users

```
    <Plugin users>
    </Plugin>
```

Create visualization

Graph

- Chart type: Line
- Mode Normal

Filters

- plugin - is - users

Y-Axis

- Aggregation: Top Hit
- Field: value
- Aggregate with: Max
- Sort on: Time
- Custom label: Logged users

Split series

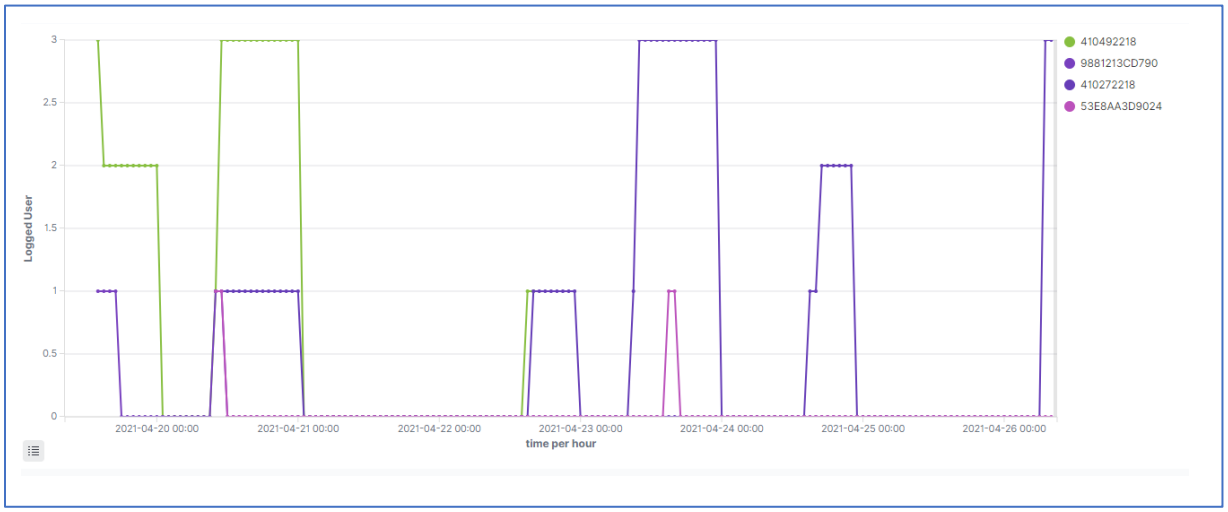
- Aggregation: Terms
- Field: serial_number.keyword

X-Axis

Sub aggregation: Data histogram

Field: time

Minimum interval: Auto

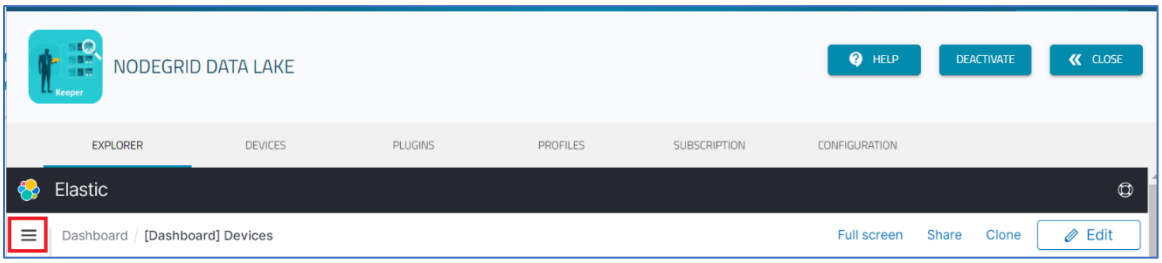


Create Visualization

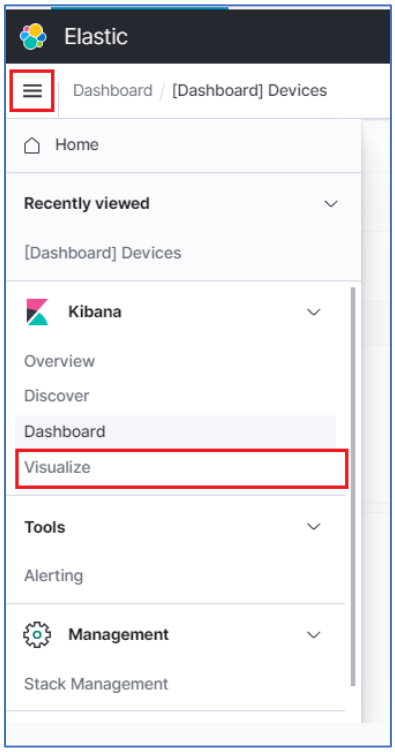
Visualizations display aggregate data in a variety of options. Following includes examples on setting up some data presentations.

To access visualization functions:

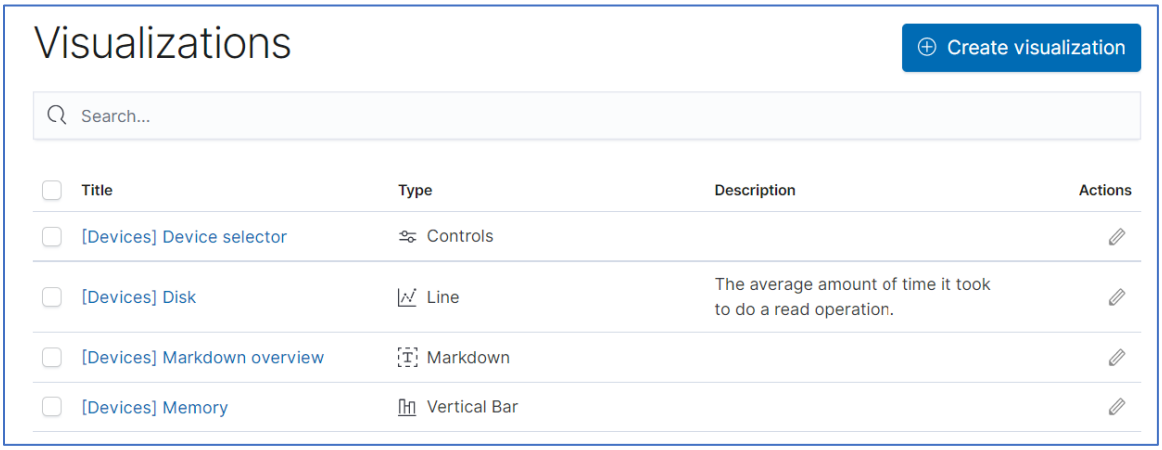
1. Go to *APPS :: NODEGRID DATA LAKE :: EXPLORER*.
2. Click the **Hamburger** icon (left side) to display the drop-down menu.



On the drop-down, click **Visualize**.

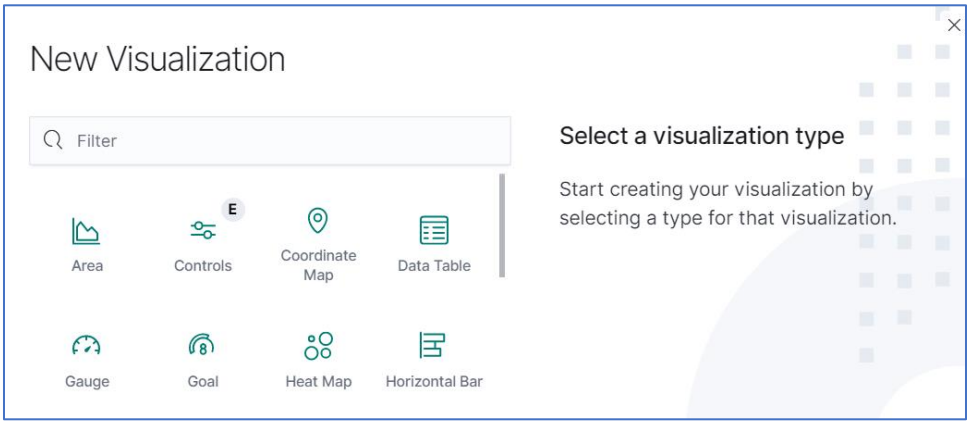


3. This displays the *Visualizations* panel (lists table of current visualizations). The **Pencil** icon (right side) opens the *Edit* panel.



To edit an existing visualization, click the **Pencil** icon (*Actions* column), edit details, and update.

4. To create a new visualization, click **Create Visualization** (displays dialog).



5. Click the visualization to be created. On the dialog, enter specifications and details.
6. When done, click **Update**. If there is an error, a red border displays around the error item. Fix the error and click **Update**.
7. If needed, click **Discard** to abandon the process.

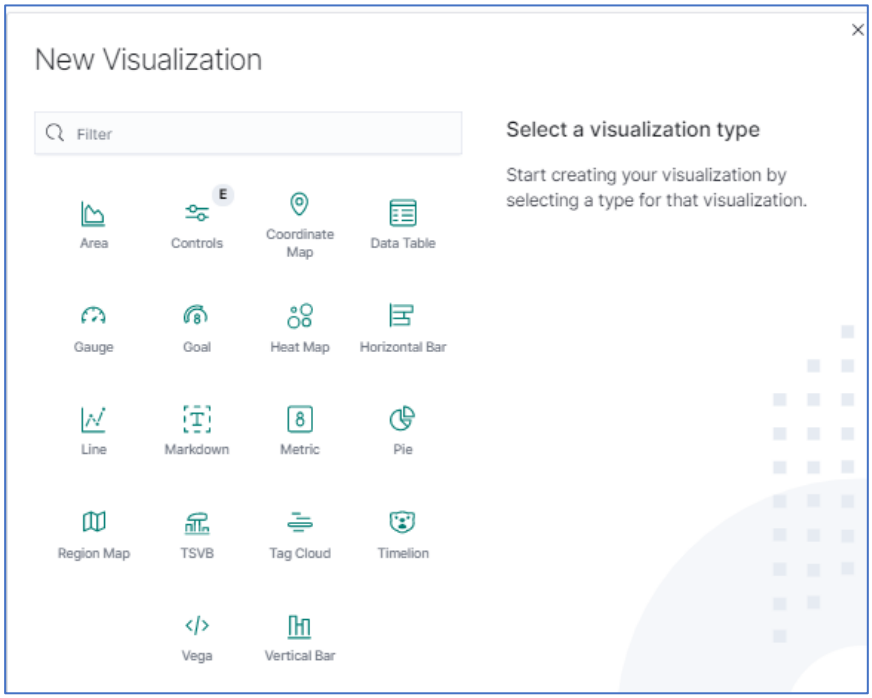
Line Charts

Line Charts visualize data points along a line graph.

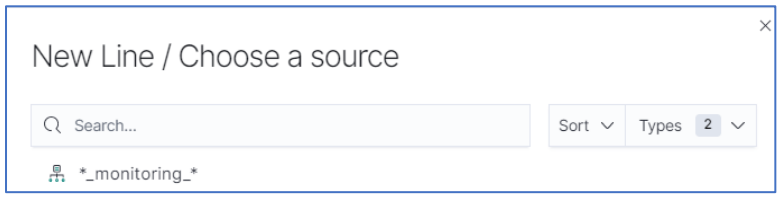
Create a Single or Multi-Line Chart (Configuration Example)

WebUI Procedure

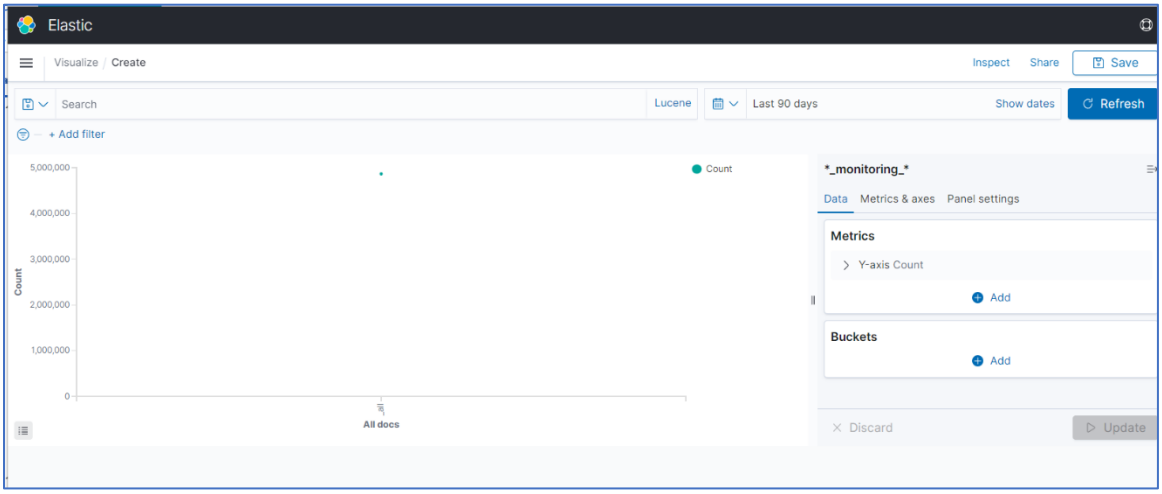
1. On the *Visualization* panel, click **Create visualization** (displays dialog).



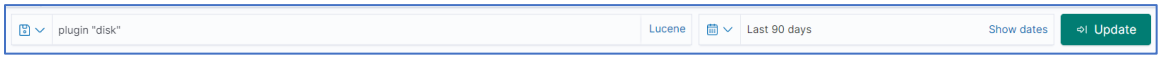
2. Click the **Line** icon (displays dialog).



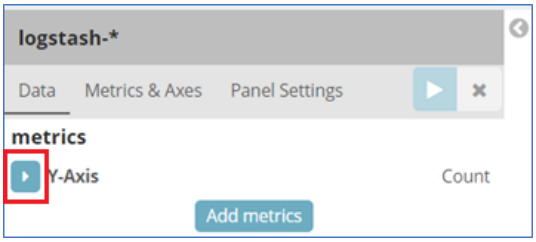
3. On the dialog, click ***_monitoring_*** (displays dialog).



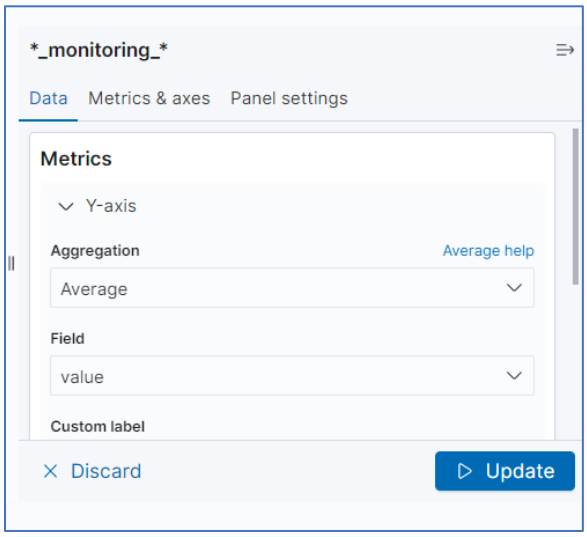
4. To select the data points to visualize, enter a search expression, and click **Update**.



5. In the *Metrics* section, click **Y-Axis** arrow.

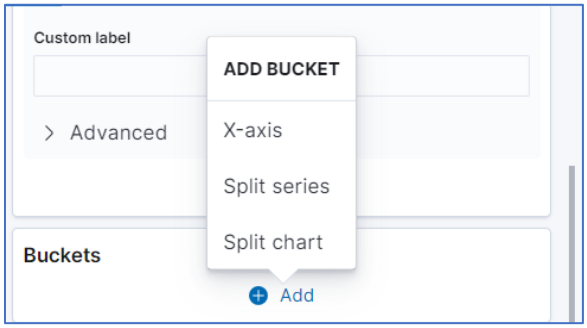


6. On the **Aggregation** drop-down, under *Metric Aggregations* section, select **Average** . In **Field** drop-down, select **value**. Click **Update**.

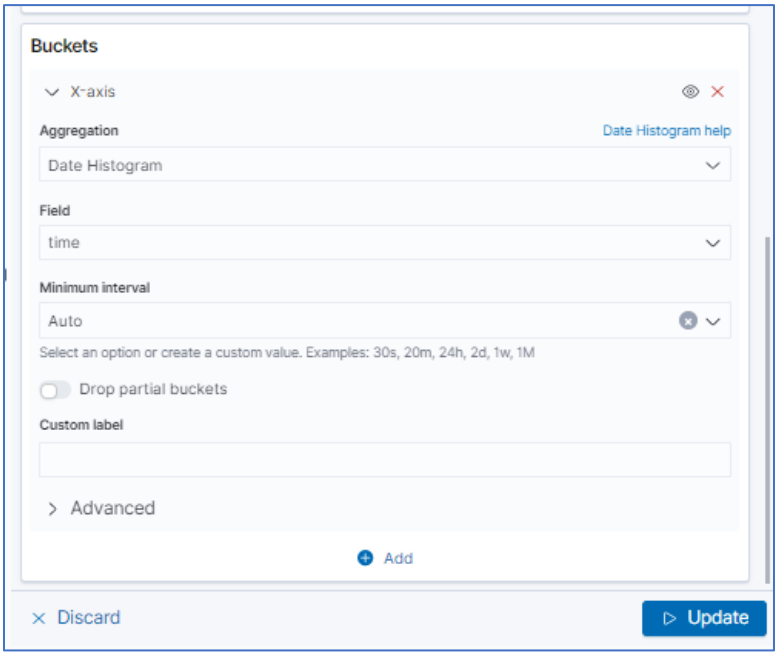


7. In *buckets* section, in *Select buckets type* menu, the plug-in selection is entered here.

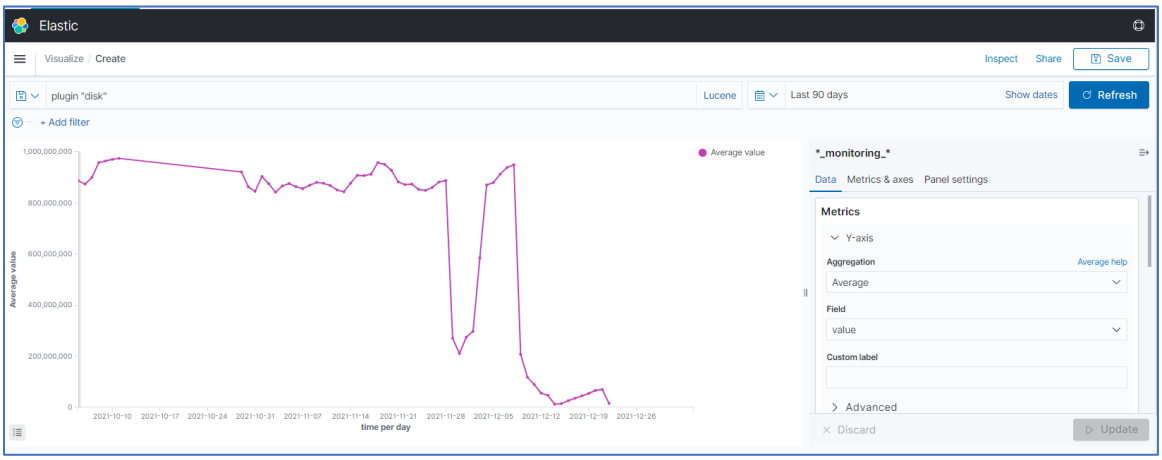
   For this example, click **Add**. And select **X-Axis**



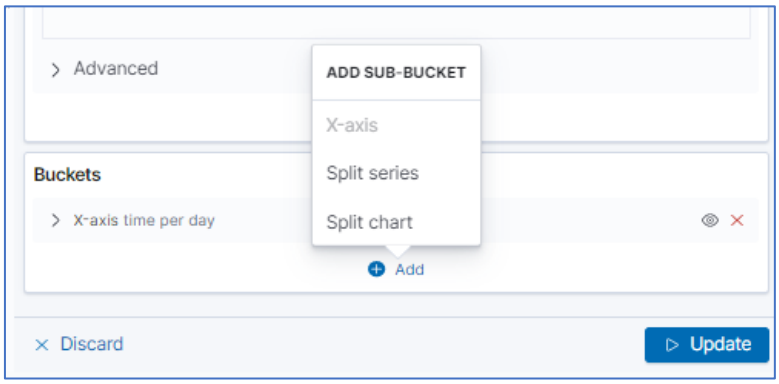
8. On **Aggregation** drop-down, select **Date Histogram**. Accept **Field** and **Interval** defaults. Click **Update**.



9. Example graph is displayed.



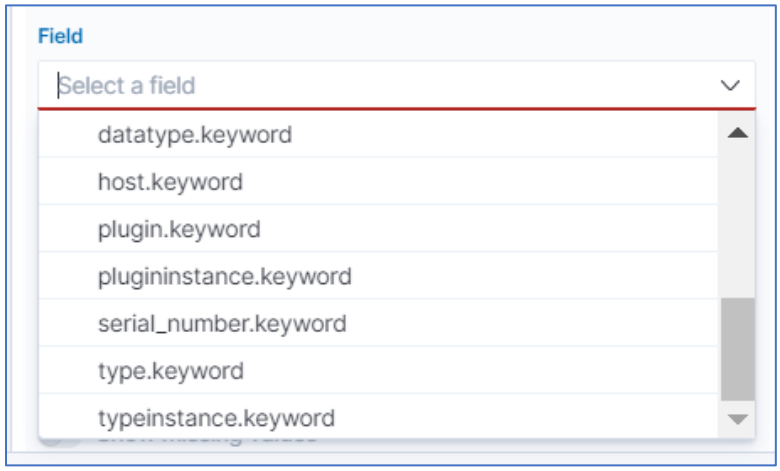
10. To split the values on individual lines, on **Buckets**, click **Add**. On dialog, click **Split series**.



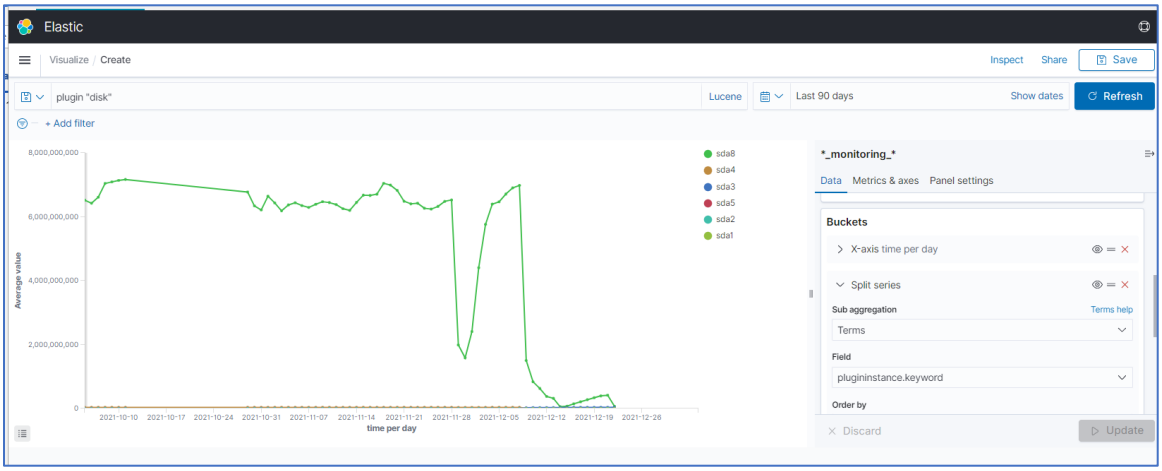
:

11. On the **sub-aggregation** drop-down, select **Terms**.

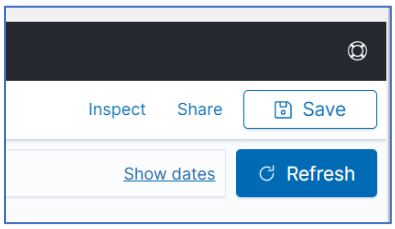
12. On **Field** drop-down, select the item **selectplugininstance.keyword**.



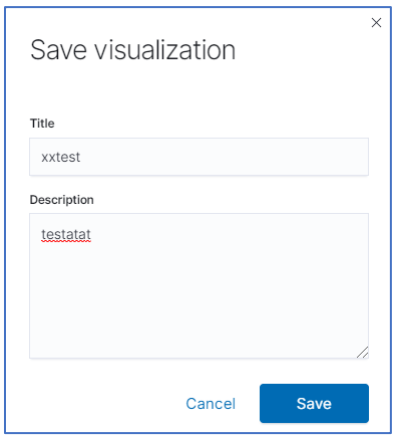
Click **Update** (graph shows the split aggregation).



13. On the Toolbar, click **Save** (upper right corner).



14. On the dialog, enter a **Title** and **Description** for the visualization. Click **Save**.



Other Plugin Graph Representations

See the Nodegrid Data Lake Plugins (above) for configuration and setup details.