NODEGRID User Guide

Release 6.0.19

Table Of Contents

User Interface Information

Access Section

Access Devices via Table

Access Section

Tracking Section

Open Sessions tab

Event List tab

System Usage tab

Discovery Logs tab

Network tab

DHCP sub-tab

Network tab

Devices tab

Scheduler tab

HW Monitor tab

Tracking Section

SD-WAN tab

System Section

License tab

Preferences tab

Slots tab (SR only)

Date and Time tab

Toolkit tab

Logging tab

Custom Fields tab

Dial-Up tab

Schedular tab

SMS tab (installed cellular module)

Remote File System tab

Central Management tab

I/O Ports tab (only with GPIO)

Network Section

Connections tab

Add Network Connections

Connections tab

Network Section

Switch tab (NSR, NSR Lite, GSR, and BSR)

Routing tab

Hosts tab

SNMP tab

Wireless Modem tab

Flow Exporter tab

802.1x tab (Net SR only)

QoS tab

SD-WAN tab

DHCP :: DHCP Server tab

DHCP :: DHCP Relay tab

VPN :: Wireguard tab

VPN :: IPsec tab

VPN :: SSL VPN tab

Managed Devices Section

Devices tab

Manage Devices

Configure Individual Device Settings

Access sub-tab

Management sub-tab

Logging sub-tab

Custom Fields sub-tab

Commands sub-tab

Switch Port tab

Views tab

Types tab

Configuring Auto Discovery

Auto Discovery Processes

Configuring Auto Discovery

Preferences tab

Cluster Section

Clusters tab

Peers tab

Settings tab

Management tab

Security Section

Local Accounts tab

Password Rules tab

Authorization tab

Manage User Group Configuration

Authorization tab

Authentication tab

Firewall tab

NAT tab

Services tab

Certificates Tab

Generating and Managing Certificates Using ACME in Nodegrid

Signing in with ACME

Renewing ACME Certificates

Revoking ACME Certificates

Troubleshooting and Logs

Viewing and Validating device identity with Platform Certificate

Validating the X.509 Certificate

GEO Fence tab

RFID Tag tab

Auditing Section

Settings tab

Events tab

Destinations tab

Dashboard Section

Description Details

Dashboards side-tab

Discover tab

Visualize tab

Dashboard tab

Management tab

Applications Section

Docker tab

Virtual Machines tab

WiFi Controller tab

Network Function Virtualization

About this Document

This user guide provides you with essential features and functions of Nodegrid Manager or Nodegrid Platform and the following supporting units, ensuring you can effectively manage and optimize your IT infrastructure.

- Nodegrid Serial Console
- Nodegrid Serial Console Plus
- Nodegrid Serial Console Plus - Core
- Nodegrid Net Services Router
- Nodegrid Gate SR
- Nodegrid Bold SR
- Nodegrid Link SR
- Nodegrid Hive SR
- Nodegrid Mini SR
- Nodegrid NSR Lite

About Nodegrid Platform

Nodegrid Platform is the network operating system that streamlines the management of data center IT infrastructure, providing network engineers and system administrators with a unified interface for accessing and controlling managed devices. A managed device is any physical or virtual device configured under Nodegrid Manager for access and control. The Nodegrid Manager provides a unified solution to control compute, network, storage, and smart power assets. With Nodegrid Manager, you gain secure, centralized out-of-band management of remote devices, enhancing efficiency and minimizing Mean Time to Repair (MTTR) when integrated with existing serial console servers, service processors, PDUs, UPSs, and KVM/IP devices.

Key Features

- Access and control physical and virtual assets (VMware, KVM) from a single screen.
- Facilitates quick and easy deployment of IT infrastructure.
- Compatible with all IT asset types and console protocols, ensuring flexibility.
- Features policy-based discovery and management to streamline operations.
- Maintains the security of firewalls while providing comprehensive management capabilities.
- Installs directly from a bootable ISO with no additional software required.
- Simplifies initial setup and configuration processes.
- Supports a wide range of vendors and technologies, including Avocent, Raritan, APC, Cisco, NetApp, HP iLO, Dell iDRAC, Redfish, and more.
- Offers access to physical and virtual consoles through various means, including RS-232 Serial, VMware MKS & Serial, KVM-over-IP, SSH, and more.
- Access Nodegrid Manager from mobile, tablet, or desktop devices, with additional options for CLI, API, search bar, bookmarks, and more.

Nodegrid Manager Hardware Requirements

The following table shows the system hardware requirements to set up a Nodegrid Manager:

Item	Description
CPU	Minimum: two cores, x86_64 CPU
Memory & Storage	4 GB RAM, minimum 32 GB HDD
Interfaces	Minimum 1 Gigabit Ethernet interface
Supported Hypervisors	VMWare ESX LinuKVM Oracle Virtualbo-- LinuxOS

Notifications

USA

WARNING

Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the users will be required to correct the interference at their own expense.

Canada

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

European Union

This is a class-A product. In a domestic environment, this product may cause radio interference in which case, the user may be required to take adequate measures.

IMPORTANT

All other marks are the property of their respective owners. This document may contain confidential and/or proprietary information of ZPE Systems, Inc., and its receipt or possession does not convey any right to reproduce, disclose its contents, or to manufacture or sell anything that it may describe. Reproduction, disclosure, or use without specific authorization from ZPE Systems, Inc. is strictly prohibited.

Credits

Contact us
Sales: sales@zpesystems.com
Support: support@zpesystems.com

ZPE Systems, Inc.
3793 Spinnaker Court
Fremont, CA 94538 USA
www.zpesystems.com

User Interface Information

Use the Nodegrid Manager user interface to configure, monitor, and troubleshoot the supported Nodegrid devices. This interface will help you access your devices and leverage powerful search functionality to efficiently manage and optimize your IT infrastructure. Whether you are deploying new managed devices, performing maintenance operations, or troubleshooting issues, this interface equips you with the tools to fully utilize Nodegrid Manager capabilities.

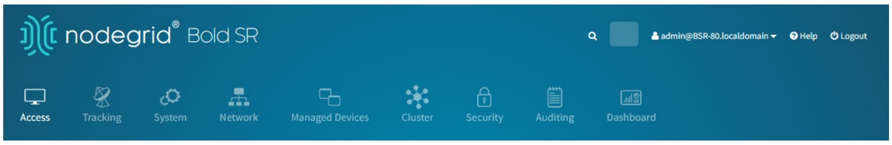
Refer to the following sections for more information about the various user interface options available in the Nodegrid Manager to manage your IT infrastructure:

- User Interfaces
- Access to Devices
- Search Functionality

User Interfaces

Web UI Header

This header provides links to major sections of the Nodegrid OS. Several tools are also available.



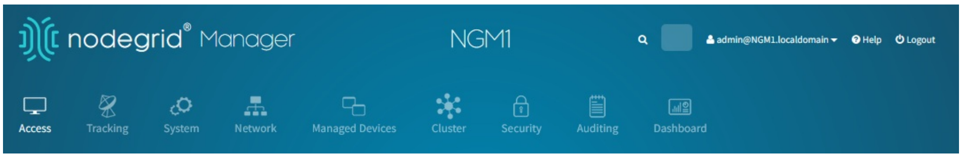
Each icon opens options to view and modify settings. Details on each section are available in the User Guide.

Device Information

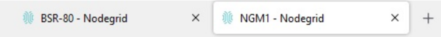
Starting with v5.10.0, the device model is shown right next to the Nodegrid logo. Model names include Manager, Bold SR, Gate SR, Link SR, Hive SR, Net SR, Compute Card, USB-C96, Mini SR, NSC-T48R, NSCP-T48R, among others.

The current user, hostname, and domain name are shown at the right of the search bar (admin@NGM1.localdomain in the example below). Hostname and Domain name can be set in *Network :: Settings*.

If the checkbox *System :: Preferences :: Show Hostname on WebUI Header* is set, the hostname will also show at the center of the header, as in the example below. The color can be configured right below the checkbox.

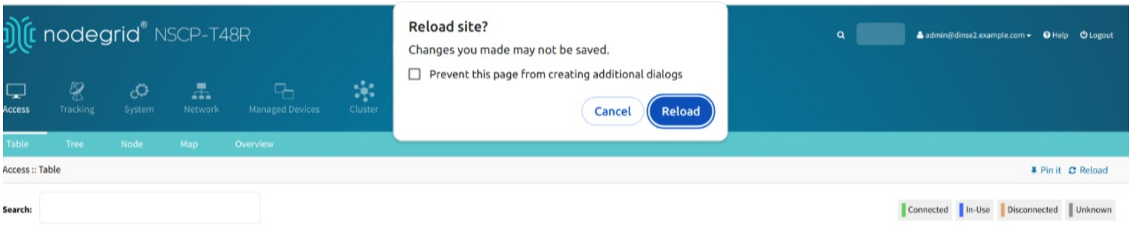


The hostname is also shown in the browser's tab title if the user is logged in:



User Navigation through Browser

When you refresh a page, you get a warning stating you will be logged out of the device.


Reload site?

Changes you made may not be saved.

□ Prevent this page from creating additional dialogs

Note: The warning message may differ from browser to browser.

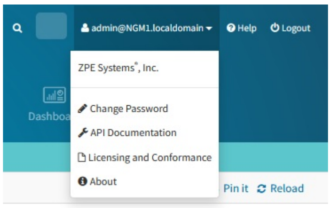
When you click back, you are directed to the previously accessed Nodegrid page; when you click forward, you are taken to the page you accessed before going to the previous page.

Search Bar

The search bar provides advanced search capabilities to locate and view information. Boolean expressions are allowed. See Search Functionality for more details.

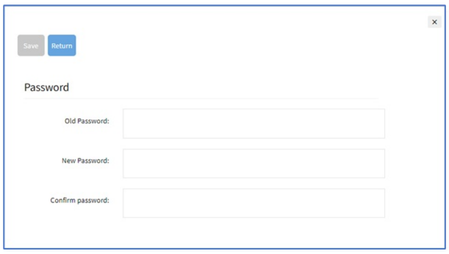
Account drop-down options

The account name drop-down provides several options.



Change Password

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



- Enter **Old Password**.
- Enter **New Password** and **Confirm Password**.

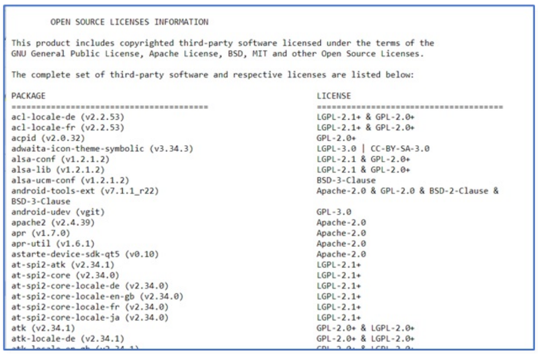
3. Click **Save**.

API Documentation

This links to the Nodegrid API documentation.

Licensing and Conformance

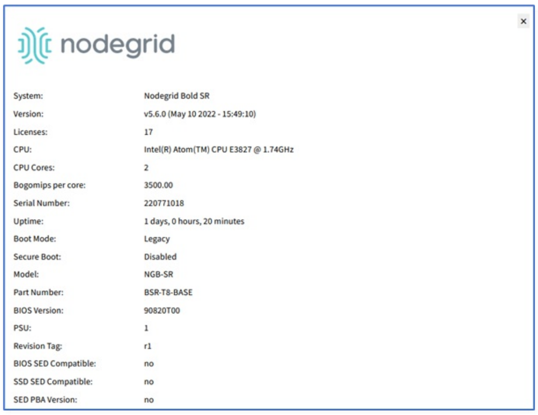
This opens the page with Nodegrid license and conformance details.



```
       OPEN SOURCE LICENSES INFORMATION

This product includes copyrighted third-party software licensed under the terms of the
GNU General Public License, Apache License, BSD, MIT and other Open Source Licenses.

The complete set of third-party software and respective licenses are listed below:

PACKAGE                                            LICENSE
========================================           ======================================
acl-locale-de (v2.2.53)                            LGPL-2.1+ & GPL-2.0+
acl-locale-fr (v2.2.53)                            LGPL-2.1+ & GPL-2.0+
acpid (v2.0.32)                                    GPL-2.0+
adwaita-icon-theme-symbolic (v3.34.3)              LGPL-3.0 | CC-BY-SA-3.0
alsa-conf (v1.2.1.2)                               LGPL-2.1 & GPL-2.0+
alsa-lib (v1.2.1.2)                                LGPL-2.1 & GPL-2.0+
alsa-ucm-conf (v1.2.1.2)                           BSD-3-Clause
android-tools-ext (v7.1.1_r22)                     Apache-2.0 & GPL-2.0 & BSD-2-Clause &
BSD-3-Clause
android-udev (vgit)                                GPL-3.0
apache2 (v2.4.39)                                  Apache-2.0
apr (v1.7.0)                                       Apache-2.0
apr-util (v1.6.1)                                  Apache-2.0
astarte-device-sdk-qt5 (v0.10)                     Apache-2.0
at-spi2-atk (v2.34.1)                              LGPL-2.1+
at-spi2-core (v2.34.0)                             LGPL-2.1+
at-spi2-core-locale-de (v2.34.0)                   LGPL-2.1+
at-spi2-core-locale-en-gb (v2.34.0)                LGPL-2.1+
at-spi2-core-locale-fr (v2.34.0)                   LGPL-2.1+
at-spi2-core-locale-ja (v2.34.0)                   LGPL-2.1+
atk (v2.34.1)                                      GPL-2.0+ & LGPL-2.0+
atk-locale-de (v2.34.1)                            GPL-2.0+ & LGPL-2.0+
```

About

This displays the *About* pop-up dialog with the device version and hardware details.



System: Nodegrid Bold SR
Version: v5.6.0 (May 10 2022 - 15:49:10)
Licenses: 17
CPU: Intel(R) Atom(TM) CPU E3827 @ 1.74GHz
CPU Cores: 2
Bogomips per core: 3500.00
Serial Number: 220771018
Uptime: 1 days, 0 hours, 20 minutes
Boot Mode: Legacy
Secure Boot: Disabled
Model: NGB-SR
Part Number: BSR-T8-BASE
BIOS Version: 90820T00
PSU: 1
Revision Tag: r1
BIOS SED Compatible: no
SSD SED Compatible: no
SED PBA Version: no

Banner Section Icons

Each device’s Nodegrid Platform can be accessed from ZPE Cloud via WebUI. This provides full access to device configuration and management.

All modern browsers with HTML5 are supported, including mobile (phone/tablet) browsers. This includes Internet Explorer 11, Edge, Chrome, and Firefox.

Device WebUI Section Icons

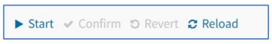
Menu	Description
Access	Easy access for all device users. With appropriate permissions, users can start sessions, control power and review device logging details.
Tracking	Provides an overview of general statistics and system information, including system utilization and serial port statistics.
System	Administrators can perform general admin tasks (firmware updates, backups , restorations, licensing).
Network	Access and management of all network interfaces and features.
Managed Devices	Administrators can add, configure, and remove devices managed through the Nodegrid platform.
Cluster	Administrators can configure Nodegrid Cluster feature.
Security	User access configuration options and general security settings.
Auditing	Administrators can configure auditing levels and locations, and some global logging settings.
Dashboard	Users and administrators can create and view dashboards and reports.
Applications	Only visible with a valid Virtualization license. Administrators can manage and control NFVs and Docker applications.

Configuration Updates

In all sections (excluding Access and Tracking), configuration updates can be implemented with these buttons (located at upper right area on each page). Use of this feature is optional.

> **NOTE**
>
> This feature is not available in all Nodegrid device versions.

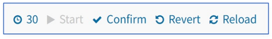
When making changes to Nodegrid configuration (changing firewall, changing network settings, etc.) and Confirm button is not clicked before the 30-second timer expires, modifications are reverted.



In this section, configuration changes can be initiated with these actions.

Start - initiates 30 seconds time window to apply the specific settings.
Confirm – setting changes are confirmed and permanently applied (if clicked before 30 second window). (If not clicked before 30 seconds, settings are reverted back automatically.)
Revert – changes are reverted and are not applied.
Reload – reloads settings to refresh the displayed content.

Configuration Change Procedure

1. Open the configuration dialog.
2. Click **Start** (initiates the 30 second time window).
   

3. Make changes in the parameters.
4. Click **Save** (timer restarts).
5. If changes are acceptable, click Confirm. If not acceptable, two options:
   Click **Revert** (configuration is restored).
   If the timer goes to 0, changes are automatically reverted (configuration is restored).

CLI Interface

The Nodegrid Platform can be accessed through a CLI interface, by connecting to the platform with a SSH client or through its console port. The interface can manage and configure the device, including access to console target sessions. CLI structure generally follows the WebUI.

CLI Folders

Folder	Description
/access	Access for all users to managed devices. Users with appropriate permissions can start sessions, control power, and review device logging details.
/system	Provides access to the combined functions of the Tracking and System menu (accessed with WebUI). Tracking features include an overview of general statistics and system information (system utilization, serial port statistics, etc.). Administrators can perform general admin tasks on the Nodegrid Platform (i.e., firmware updates, backups, restorations, and licensing).
/settings	Provides access to the system, security, auditing, and managed device settings, and configuration options.

The CLI provides many commands and options. General usage includes several basic commands.

CLI Commands

CLI Command	Description
TAB TAB	Lists all available commands, settings, or options currently available.
cd	Returns user to root/home directory.
cd – (cd<space><dash>	Moves to previous location cd /settings/authorization cd /settings/authentication cd - # it goes back to authorization cd - # it goes back to authentication cd - # it goes back to authorization
ls	Lists the current folder structure.
show	Displays current settings in a tabular view.
set	Initiates changes and settings with "set option=value". Multiple settings can be combined in sequence of option=value pairs (i.e., set option1=value1 option2=value2). Regular expressions are supported.
commit	Commits changes to configurations. A "show" command can display whether previous line entries were saved. If not saved, enter commit. A "+" in front of the command prompt, [i.e., +admin@nodegrid /]#" is shown only when editing an entry or configuration. To add new entries, the + indicator is not displayed – and "commit" is required.
cancel or revert	Abort an "add" command".
revert	Restore a setting from the most recent "commit"

Examples

Plaintext Copy

```
[admin@nodegrid /]# ls
access/
system/
settings/
[admin@nodegrid /]# show
[admin@nodegrid /]# show /access/
  name                   status
  =====================  =========
  Device_Console_Serial  Connected
[admin@nodegrid /]# set settings/devices/ttyS2/access/ mode=on-demand
[+admin@nodegrid /]# set settings/devices/ttyS2/access/ rs-232_signal_for_device_state_detection=
CTS   DCD   None
[+admin@nodegrid /]# set settings/devices/ttyS2/access/ rs-232_signal_for_device_state_detection=DCD enable_hostname_detection=yes
[+admin@nodegrid /]# commit
[admin@nodegrid /]#
```

Shell Access

The Nodegrid Platform has direct access to the operating system's shell. By default, this is only available to the root user (directly) and admin user (from CLI). Direct shell access can be granted to users of specific groups (useful for system automation processes which require direct shell access. Authorization for users is provided with SSH key authorization.

Access should be limited based on shell access requirements. This requires careful consideration and caution. Changes made through shell access can have a negative impact.

Access to Devices

This provides an overview of all available devices (Search is available). Users can connect to managed devices and review current device status. User permissions and the current state of Nodegrid Cluster nodes determine which devices are displayed.

Device Sessions

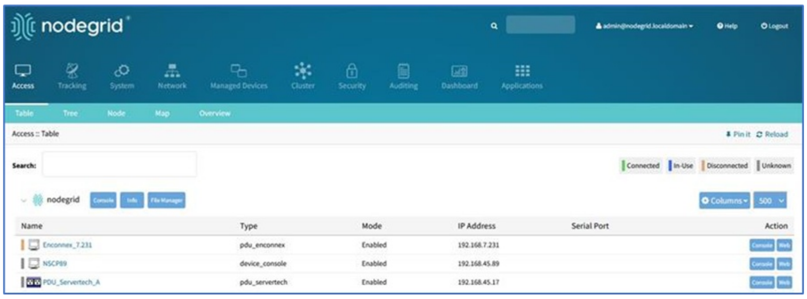
When a user logs into the WebUI, the first page is the Access section. This is an overview of all available user-accessible targets. Each device current connection status and available connection types are shown.

Device Sessions

State	Indicator color	Icon	Description
Connected	Green	🟩 Connected	Nodegrid can successfully connect to the device and it is available for sessions
In-Use	Blue	🟦 In-Use	The Device is currently in use
Disconnected	Orange	🟧 Disconnected	Nodegrid could not successfully connect to the device and it is not available for sessions
Unknown	Grey	▨ Unknown	The connection status is unknown. This is the default state for devices with the connection mode On-Demand or for new devices for which the discovery process is not completed.

Device sessions can be directly started from this location.

WebUI View



Access :: Table

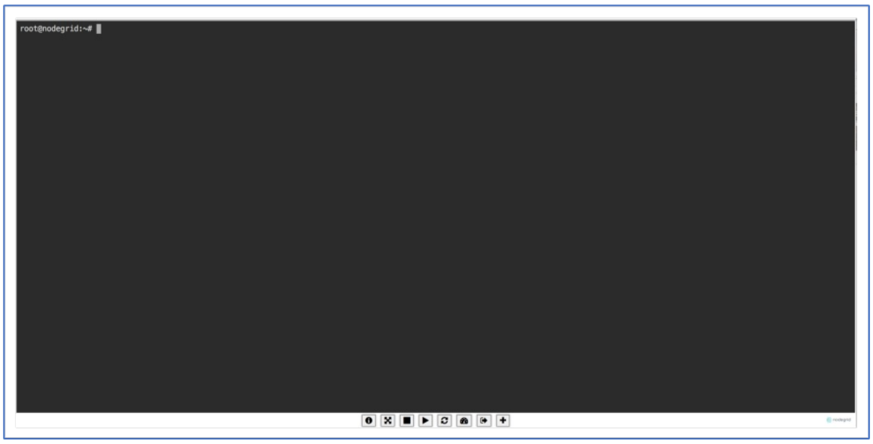
Search:

nodegrid

Name	Type	Mode	IP Address	Serial Port	Action
Enconnex_7.231	pdu_enconnex	Enabled	192.168.7.231		Console Web
NSCP89	device_console	Enabled	192.168.45.89		Console Web
PDU_Servertech_A	pdu_servertech	Enabled	192.168.45.17		Console Web

Console (CLI) View

Click Console to display a new target session window.



```
root@nodegrid:~#
```

Buttons at lower center can further control the session and device. Available options depend on connection type and device configuration.

Session Options

Options	Description
ℹ Info	Displays current device details.
✕ Full Screen	Expand the window to use the full monitor screen. The session window does not expand beyond its maximum size.
■ Power Off	Performs a power off on the device through a connected Rack PDU or IPMI device.
▶ Power On	Performs a power on for the device through a connected Rack PDU or IPMI device.
↻ Reset	Initiates a power cycle on the device through a connected Rack PDU or IPMI device.
Power Status	Display device's current power status (as returned by a connected Rack PDU or IPMI device).
Close Session	Closes the active session.
+	Expands or minimizes the command line options at the window's lower center.

Close the CLI window to end the device session.

Copy & Paste Functionality

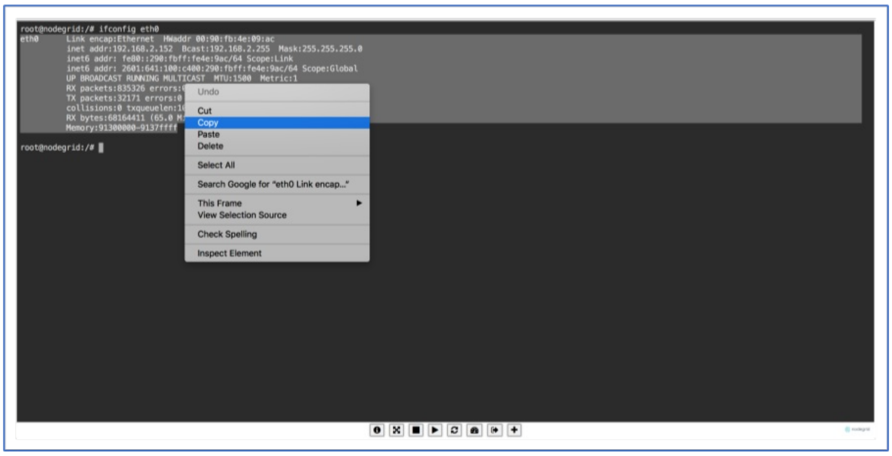
NOTE

TTYD terminal copy and paste is not currently supported within Windows and Linux.

Nodegrid supports Copy & Paste of text between the HTML5 graphical device session window and the desktop environment. Some OS may require a different key combination.

Windows and Linux user – Ctrl+Ins to copy highlighted text and Shift+Ins to paste.
Mac users - Cmd+C to copy, and Cmd+V to paste.

Highlight the text and right-click to open the menu – or use the shortcuts.



```
root@nodegrid:/# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:90:fb:4e:09:ac
          inet addr:192.168.2.152  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::290:fbff:fe4e:9ac/64 Scope:Link
          inet6 addr: 2601:641:100:c400:290:fbff:fe4e:9ac/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:835326 errors:
          TX packets:32171 errors:0
          collisions:0 txqueuelen:1
          RX bytes:68164411 (65.0 M
          Memory:91300000-9137ffff

root@nodegrid:/#
```

CLI Device Sessions

A user can directly go to this directory with cd /access.

View currently available targets

show.

Example:

None   Copy

```
[admin@nodegrid access]# show
  name                   status
  =====================  =========
  Device_Console_SSH     Connected
  Device_Console_Serial  InUse
  IPMI                   Connected
  RPDU                   Connected
  usbS2                  Connected
```

Start a device session

connect <target name>

Example:

None   Copy

```
[admin@nodegrid access]# connect Device_Console_Serial
[Enter '^Ec?' for help]
[Enter '^Ec.' to cli ]

login:
```

NOTE

Only console sessions or sessions which provide a text-based interface can be started from the CLI.

With an established connection, use the escape sequence ^Ec or ^O to further control the session.

NOTE

Escape sequences can be changed in Device Settings.

Session Options

Option	Escape sequence	Description
.	^Ec.	Disconnect the current session.
g	^Ecg	Display current user group information.
l	^Ecl	Send break signal (defined in Device Settings).
w	^Ecw	Display currently connected users.
<cr>	^Ec<cr>	Send ignore/abort command signal.
k	^Eck	Serial port (speed data bits parity stop bits flow).
b	^Ecb	Send a broadcast message. Type message after the escape sequence.
i	^Eci	Display current serial port information.
s	^Ecs	Change current session to read-only mode.
a	^Eca	Change current session to read-write mode.
f	^Ecf	Force current session to read-write mode.
z	^Ecz	Disconnect a specific connected user session.
?	^Ec?	Print this message.

Power Control options are available on targets connected to a managed Rack PDU or provided power control through IMPI. The power menu can be displayed with ^O.

None Copy

```
Power Menu - Device_Console_Serial
Options:
1. Exit
2. Status
3. On
4. Off
5. Cycle

Enter option:
```

Search Functionality

The Nodegrid Manager provides advanced search capabilities to locate and view device information.

Device Search

In the WebUI, this is available on all Device views and can filter device lists based on search criteria. On the CLI, the search command is available in the access folder.

> **NOTE**
>
> The function is available on stand-alone units and units in a Cluster configuration. All changes to device information and newly added device properties are automatically updated in the System as a background function.

Search Field Options

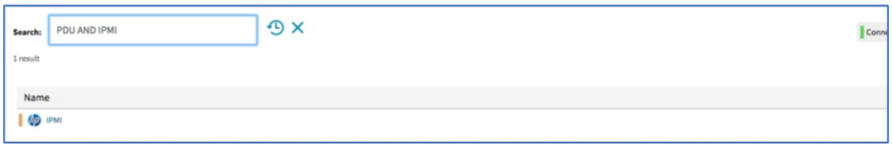
Field	Description
[search string]	Asearch string that represents part of or a complete string.
AND	Combines multiple search strings with an Boolean AND.
OR	Combines multiple search strings with a Boolean OR. Default search behavior for more than one search string.
NOT	Targets matching the search string with Boolean NOT are excluded from the returns.
[field name]	Limits the search results to a specific Field Name.

> **NOTE**
>
> The Boolean keywords AND, OR and NOT are case-sensitive. Lower-case is entered (and, or, not) is included as part of the search string.

Examples of standard and custom field data searches

This includes groups (such as “admin” group), IP addresses or a specific device.

Example with AND “PDU AND IPMI”



Search: PDU AND IPMI

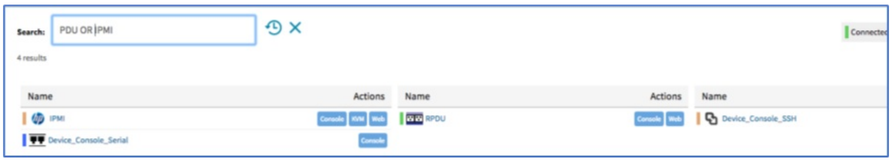
1 result

Name
IPMI

None | Copy

```
[admin@nodegrid search]# search "PDU AND IPMI"

search: PDU AND IPMI
results: 1 result
page: 1 of 1

[admin@nodegrid search]# show
  name  status  action
  ====  ======  ======
  IPMI  -
```

Example with OR "PDU OR IPMI"



Search: PDU OR IPMI

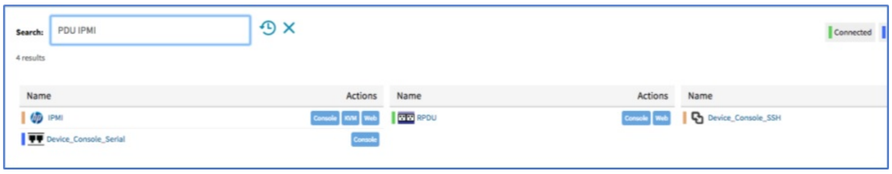
4 results

Name	Actions	Name	Actions	Name
IPMI	Console KVM Web	RPDU	Console Web	Device_Console_SSH
Device_Console_Serial	Console			

None | Copy

```
[admin@nodegrid access]# search "PDU OR IPMI"

search: PDU OR IPMI
results: 4 results
page: 1 of 1

[admin@nodegrid search]# show
  name                   status  action
  =====================  ======  ======
  IPMI                   -
  RPDU                   -
  Device_Console_SSH     -
  Device_Console_Serial  -
```

Example with "PDU IPMI"



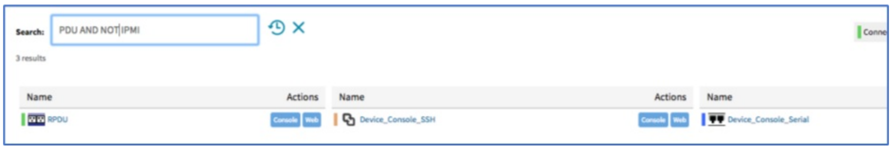
Search: PDU IPMI

4 results

None Copy

```
[admin@nodegrid access]# search "PDU IPMI"

search: PDU IPMI
results: 4 results
page: 1 of 1

[admin@nodegrid search]# show
  name                  status  action
  ====================  ======  ======
  IPMI                  -
  RPDU                  -
  Device_Console_SSH    -
  Device_Console_Serial  -
```

Example with NOT "PDU AND NOT IPMI"



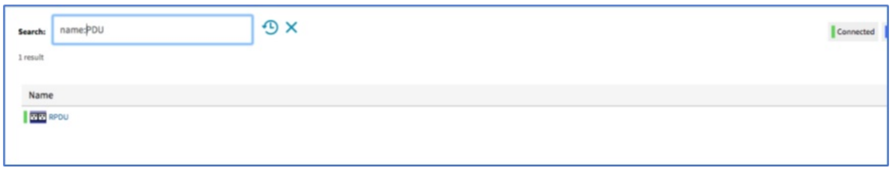
Search: PDU AND NOT IPMI

3 results

None Copy

```
[admin@nodegrid search]# search "PDU AND NOT IPMI"

search: PDU AND NOT IPMI
results: 3 results
page: 1 of 1

[admin@nodegrid search]# show
  name                  status  action
  ====================  ======  ======
  RPDU                  -
  Device_Console_SSH    -
  Device_Console_Serial
```

Example with Field Name "name:PDU"



Search: name:PDU

1 result

None Copy

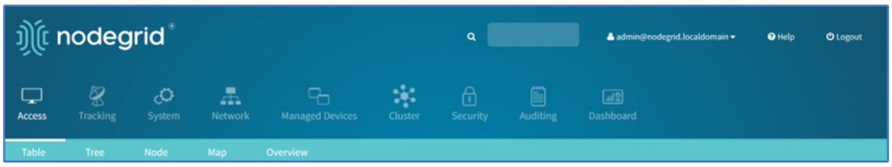
```
[admin@nodegrid search]# search "name:PDU"

search: name:PDU
results: 1 result
page: 1 of 1

[admin@nodegrid search]# show
  name  status  action
  ====  ======  ======
  RPDU  -
```

Global Search

The WebUI has a Global Search field located at the top, next to current user information and log out. Global Search works in the same as Device Search and supports the same keywords. This is available at the top of all pages.

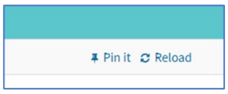
Access Section

Each device on the Nodegrid platform has embedded device information. This information is visible to users and is fully searchable. The stored information includes discovered values and those set during device configuration. An administrator can associate additional device information.



The WebUI offers multiple ways to view and access devices. By default, all users have access to the Table view. Other views are also available and improve the accessibility or visualization of the current device status.

Each user can change the default view after login. To change the default view, display the preferred view and click **Pin It** (upper right).

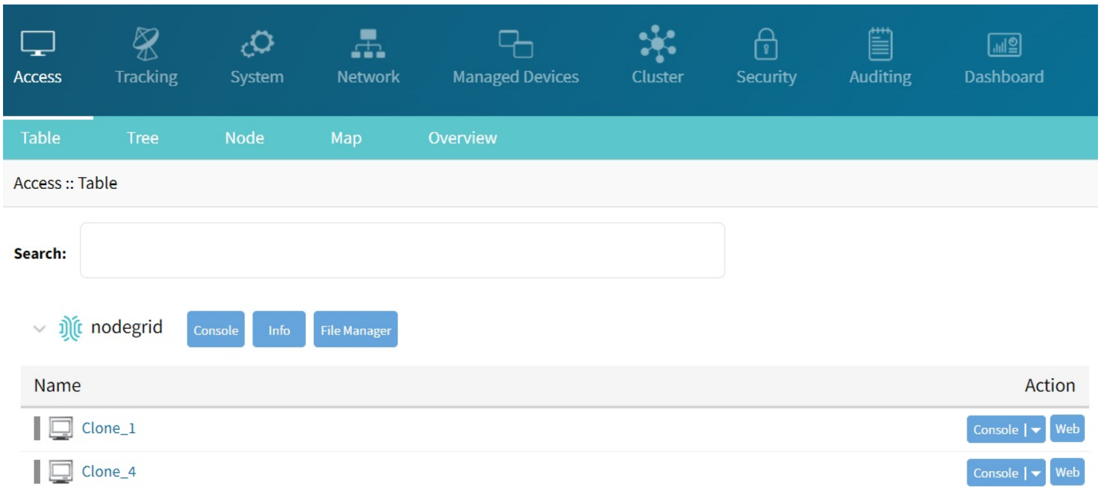


Access Devices via Table

This provides easy access to all devices with current status conditions. Any connected devices to a device are shown on the Cluster page.

> **NOTE**
>
> When attempting to access an unlicensed or expired license device, an error message displays. Contact ZPE to update the license.

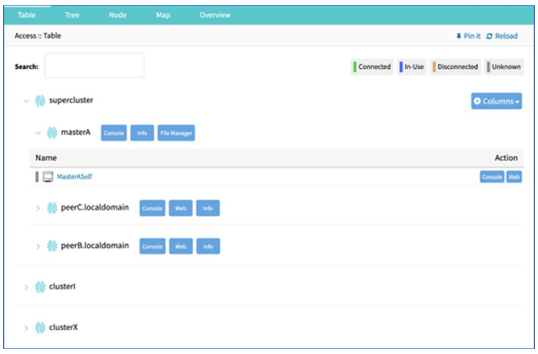
In the Table, the *Action* column shows buttons to access that device. The type of button depends on the device: Console, SSH, Telnet, KVM, MKS.



Name	Action
Clone_1	Console Web
Clone_4	Console Web

Click any device to provide the full range of access.

If the device has joined any remote clusters, the remote cluster details are displayed. This page capture shows three clusters. The top one displays the local cluster details and the others are remote clusters.



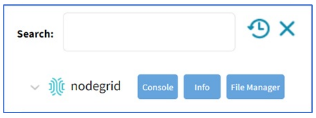
Name	Action
MasterASelf	Console Web

Managing a Device using the Access tab

When managing a large number of devices listed on this page, finding a specific device and configuring it on a separate page can be difficult and time-consuming. To simplify this process, you can click on the device name and then select Manage. This will direct you to the *Managed Access :: Devices* page, where you can easily manage the device settings. For more information, see **Manage Devices**.

Function Descriptions

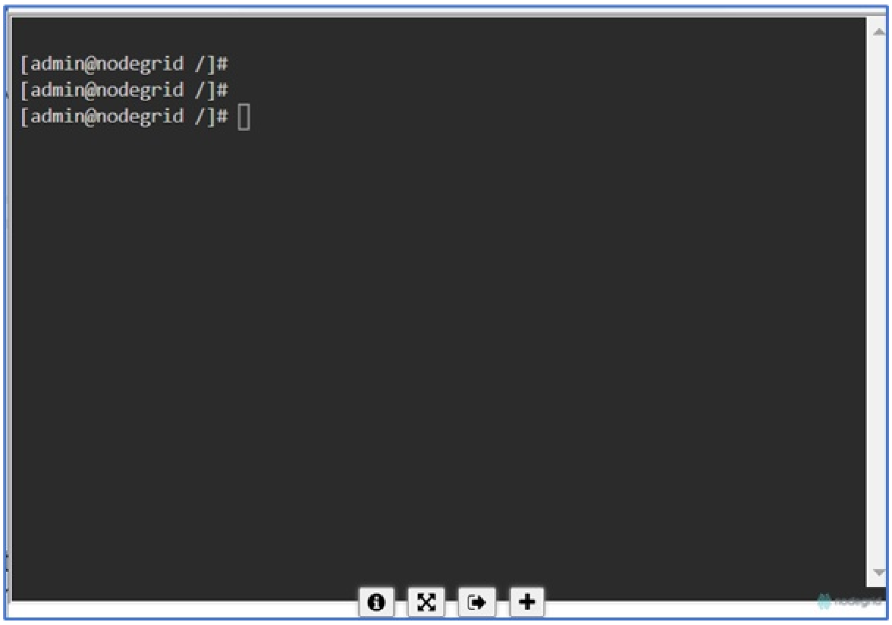
These are additional functions on the page.



- **Search**– entry returns list of matches. These entries are accepted:
  - [search string] (string to represent part of or a complete string)
  - Boolean (AND, OR, NOT – caps only)
  - [field name] (limits results to a specific Field Name).

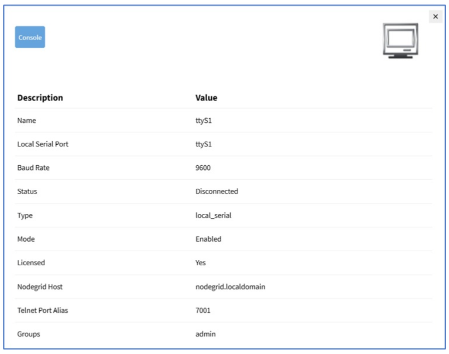
  > **Note**
  >
  > Whether you are working within a single-cluster or multi-cluster setup, you can initiate a search for the coordinator or peer.

- **Clock** icon (shows a history of past searches)
- **"X"** (clears the search field)
- **Arrow** (show/hide table – click **Down-arrow** arrow to hide table, click **Up-arrow** to show table)
- **Console** (display CLI window)



```
[admin@nodegrid /]#
[admin@nodegrid /]#
[admin@nodegrid /]# 
```

- **Info** (pop-up dialog provides device-specific details)

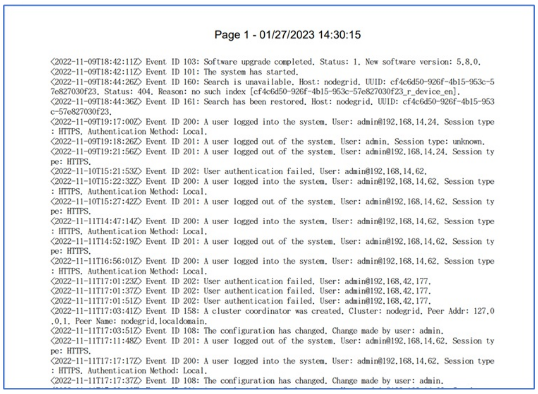


Description	Value
Name	ttyS1
Local Serial Port	ttyS1
Baud Rate	9600
Status	Disconnected
Type	local_serial
Mode	Enabled
Licensed	Yes
Nodegrid Host	nodegrid.localdomain
Telnet Port Alias	7001
Groups	admin

Pop-up dialog buttons:

Console button (opens the Console (CLI) window)

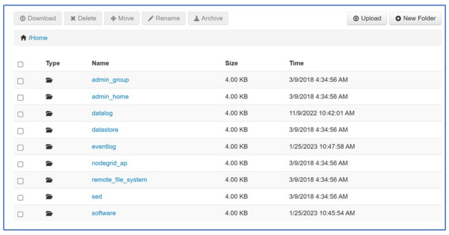
Event Log button (pop-up window displays the raw log details)



Page 1 - 01/27/2023 14:30:15

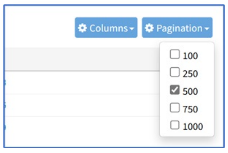
```
<2022-11-09T18:42:11Z> Event ID 103: Software upgrade completed. Status: 1. New software version: 5.8.0.
<2022-11-09T18:42:11Z> Event ID 101: The system has started.
<2022-11-09T18:44:26Z> Event ID 160: Search is unavailable. Host: nodegrid. UUID: cf4c6d50-926f-4b15-953c-5
7e827030f23. Status: 404. Reason: no such index [cf4c6d50-926f-4b15-953c-57e827030f23_r_device_en].
<2022-11-09T18:44:36Z> Event ID 161: Search has been restored. Host: nodegrid. UUID: cf4c6d50-926f-4b15-953
c-57e827030f23.
<2022-11-09T19:17:00Z> Event ID 200: A user logged into the system. User: admin@192.168.14.24. Session type
: HTTPS. Authentication Method: Local.
<2022-11-09T19:18:26Z> Event ID 201: A user logged out of the system. User: admin. Session type: unknown.
<2022-11-09T19:21:56Z> Event ID 201: A user logged out of the system. User: admin@192.168.14.24. Session ty
pe: HTTPS.
<2022-11-10T15:21:53Z> Event ID 202: User authentication failed. User: admin@192.168.14.62.
<2022-11-10T15:22:32Z> Event ID 200: A user logged into the system. User: admin@192.168.14.62. Session type
: HTTPS. Authentication Method: Local.
<2022-11-10T15:27:42Z> Event ID 201: A user logged out of the system. User: admin@192.168.14.62. Session ty
pe: HTTPS.
<2022-11-11T14:47:14Z> Event ID 200: A user logged into the system. User: admin@192.168.14.62. Session type
: HTTPS. Authentication Method: Local.
<2022-11-11T14:52:19Z> Event ID 201: A user logged out of the system. User: admin@192.168.14.62. Session ty
pe: HTTPS.
<2022-11-11T16:56:01Z> Event ID 200: A user logged into the system. User: admin@192.168.14.62. Session type
: HTTPS. Authentication Method: Local.
<2022-11-11T17:01:23Z> Event ID 202: User authentication failed. User: admin@192.168.42.177.
<2022-11-11T17:01:37Z> Event ID 202: User authentication failed. User: admin@192.168.42.177.
<2022-11-11T17:01:51Z> Event ID 202: User authentication failed. User: admin@192.168.42.177.
<2022-11-11T17:03:41Z> Event ID 158: A cluster coordinator was created. Cluster: nodegrid. Peer Addr: 127.0
.0.1. Peer Name: nodegrid.localdomain.
<2022-11-11T17:03:51Z> Event ID 108: The configuration has changed. Change made by user: admin.
<2022-11-11T17:11:48Z> Event ID 201: A user logged out of the system. User: admin@192.168.14.62. Session ty
pe: HTTPS.
<2022-11-11T17:17:17Z> Event ID 200: A user logged into the system. User: admin@192.168.14.62. Session type
: HTTPS. Authentication Method: Local.
<2022-11-11T17:17:37Z> Event ID 108: The configuration has changed. Change made by user: admin.
```

- **File Manager** (display folder/file structure)



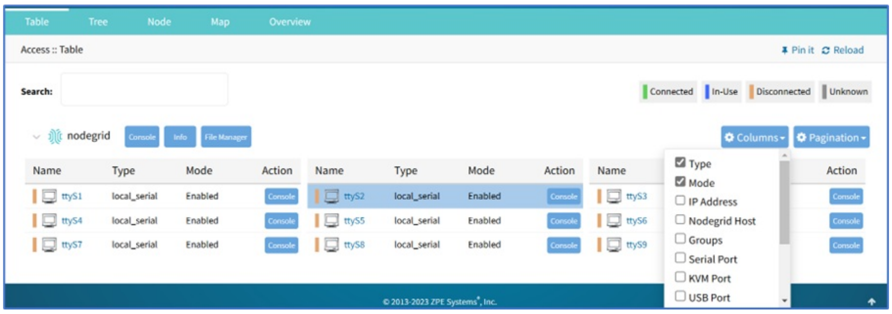
□	Type	Name	Size	Time
□		admin_group	4.00 KB	3/9/2018 4:34:56 AM
□		admin_home	4.00 KB	3/9/2018 4:34:56 AM
□		datalog	4.00 KB	11/9/2022 10:42:01 AM
□		datastore	4.00 KB	3/9/2018 4:34:56 AM
□		eventlog	4.00 KB	1/25/2023 10:47:58 AM
□		nodegrid_ap	4.00 KB	3/9/2018 4:34:56 AM
□		remote_file_system	4.00 KB	3/9/2018 4:34:56 AM
□		sed	4.00 KB	3/9/2018 4:34:56 AM
□		software	4.00 KB	1/25/2023 10:45:54 AM

- **Pagination** button – on the drop-down (100, 250, 500, 750, 1000) to select the number of items to display on the page.



□ 100
□ 250
☑ 500
□ 750
□ 1000

- **Columns** button - Details on each device can be viewed by selecting columns. As columns are selected, they are displayed in the table.

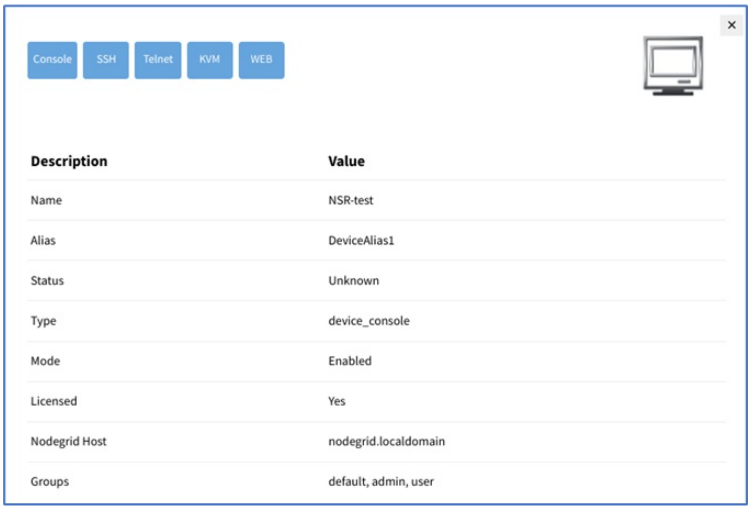


Name	Type	Mode	Action	Name	Type	Mode	Action	Name	Action
ttyS1	local_serial	Enabled	Console	ttyS2	local_serial	Enabled	Console	ttyS3	Console
ttyS4	local_serial	Enabled	Console	ttyS5	local_serial	Enabled	Console	ttyS6	Console
ttyS7	local_serial	Enabled	Console	ttyS8	local_serial	Enabled	Console	ttyS9	Console

☑ Type
☑ Mode
□ IP Address
□ Nodegrid Host
□ Groups
□ Serial Port
□ KVM Port
□ USB Port

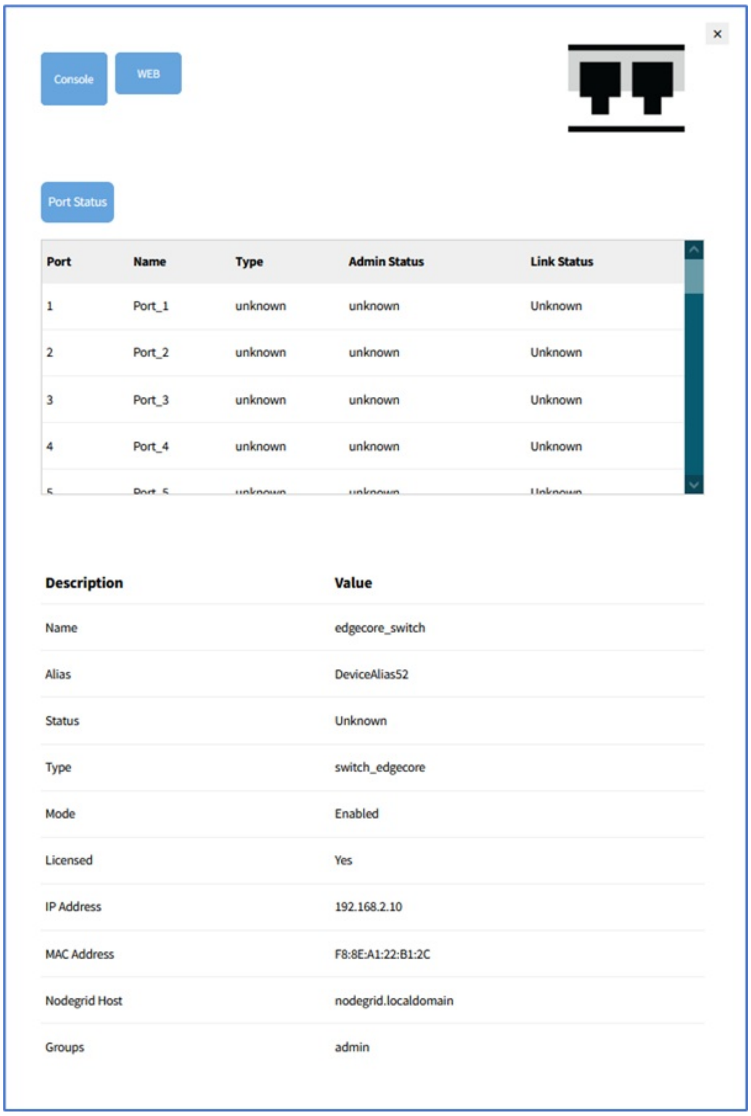
View Device Details

Click on a device to provide the full range of access.



Description	Value
Name	NSR-test
Alias	DeviceAlias1
Status	Unknown
Type	device_console
Mode	Enabled
Licensed	Yes
Nodegrid Host	nodegrid.localdomain
Groups	default, admin, user

This is an example of a Switch device: (available in v5.8+)



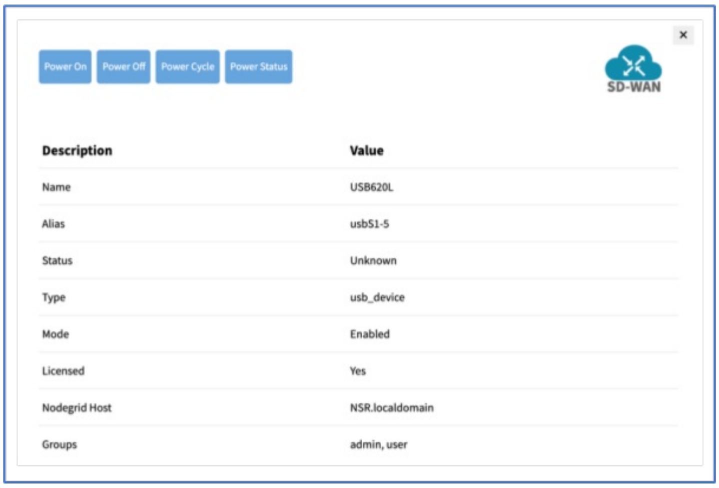
Port	Name	Type	Admin Status	Link Status
1	Port_1	unknown	unknown	Unknown
2	Port_2	unknown	unknown	Unknown
3	Port_3	unknown	unknown	Unknown
4	Port_4	unknown	unknown	Unknown
5	Port_5	unknown	unknown	Unknown

Description	Value
Name	edgecore_switch
Alias	DeviceAlias52
Status	Unknown
Type	switch_edgecore
Mode	Enabled
Licensed	Yes
IP Address	192.168.2.10
MAC Address	F8:8E:A1:22:B1:2C
Nodegrid Host	nodegrid.localdomain
Groups	admin

Manage Power

Set Device USB Power Option

1. To confirm the USB card supports USB Passthrough, go to *System :: Slots. Supported cards* . Check the *Add-ons* column for the entry: **Power Control**.
2. Go to *Access :: Table*.
3. Locate and click the device name.
4. On the pop-up dialog, select a power option.

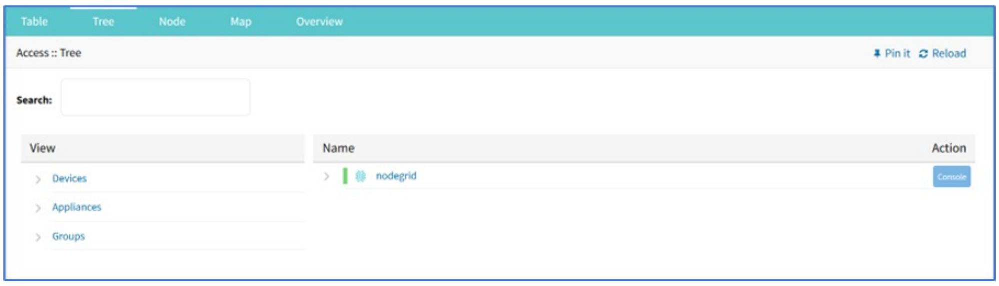


Description	Value
Name	USB620L
Alias	usbS1-5
Status	Unknown
Type	usb_device
Mode	Enabled
Licensed	Yes
Nodegrid Host	NSR.localdomain
Groups	admin, user

- **Power On** < (turns power on)
- **Power Off** (turns power off)
- **Power Cycle** (cycles power on and off)
- **Power Status** (current status)

View Device Hierarchy Using Tree View

View This displays the physical hierarchies of the Nodegrid setup. Start connections can be applied to each device. Devices can be found based on location (i.e., Nodegrid name, city name, data center name, row and rack, and others). Filters can be applied based on location and device types. Select from the expanded *View* column branches: *Devices*, *Appliances*, *Groups*.

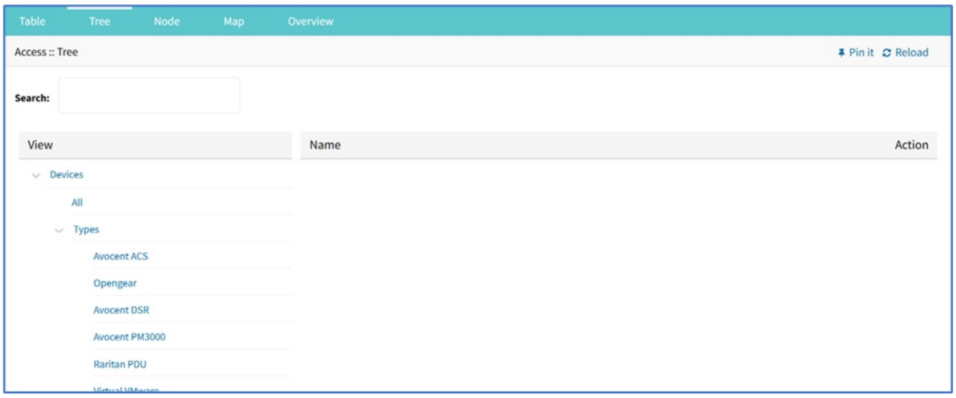


There are three trees in the View columns: **Devices**, **Appliances**, **Groups**. Details can be observed by clicking the **Right-arrow** icon.

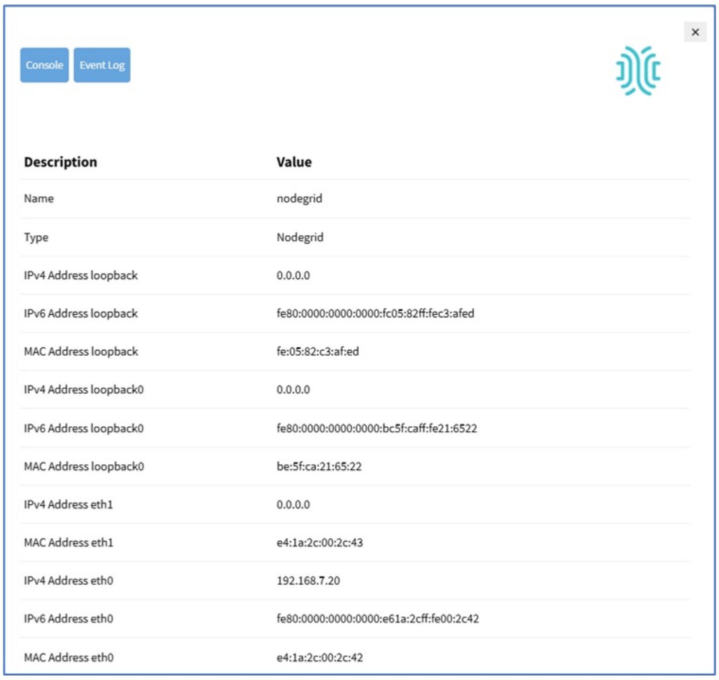
Expand Individual Tree

This example uses *Devices*.

1. Click the **Right-arrow** icon to display the next branch level.



2. If further branch levels are available, expand as needed.
3. To contract the branch, click the **Down-arrow** icon.
4. To see every item in the tree, click on **All**.
5. Click on other items to see associated names (some clicked items may not have names).
6. In the *Name* column, click a name to display a pop-up dialog of details.



Description	Value
Name	nodegrid
Type	Nodegrid
IPv4 Address loopback	0.0.0.0
IPv6 Address loopback	fe80:0000:0000:0000:fc05:82ff:fec3:afed
MAC Address loopback	fe:05:82:c3:af:ed
IPv4 Address loopback0	0.0.0.0
IPv6 Address loopback0	fe80:0000:0000:0000:bc5f:caff:fe21:6522
MAC Address loopback0	be:5f:ca:21:65:22
IPv4 Address eth1	0.0.0.0
MAC Address eth1	e4:1a:2c:00:2c:43
IPv4 Address eth0	192.168.7.20
IPv6 Address eth0	fe80:0000:0000:0000:e61a:2cff:fe00:2c42
MAC Address eth0	e4:1a:2c:00:2c:42

Search Cluster Peers and Devices

In the search bar, enter the name of the coordinator or peer device you want to find within the cluster, then press **Enter**. This action will navigate you to the searched device, enabling quick and easy access to locate the desired device.

Search– entry returns a list of matches. These entries are accepted:

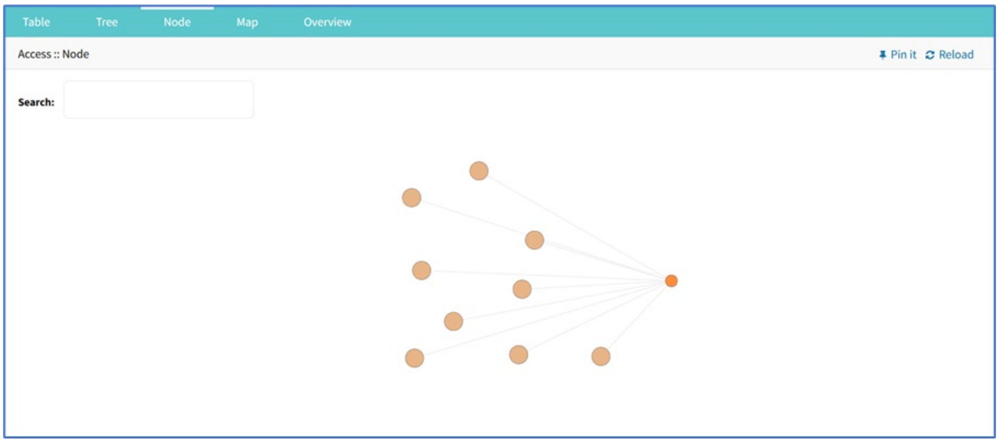
- [search string] (string to represent part of or a complete string)

- Boolean (AND, OR, NOT – caps only)
- [field name] (limits results to a specific Field Name).

Whether you are working within a single-cluster or multi-cluster setup, you can initiate a search for the coordinator or peer. In a multi-cluster configuration, there is a super-coordinator alongside peer coordinators and their associated peers/devices. The search option simplifies the device list, making it easier to identify devices based on your specified criteria.

View Device Topology

This arranges all devices around connected Nodegrid units. It provides a complete overview of all targets and Nodegrid units in a Cluster.



Nodes can be dragged and dropped to change the view. Lines show the connections.

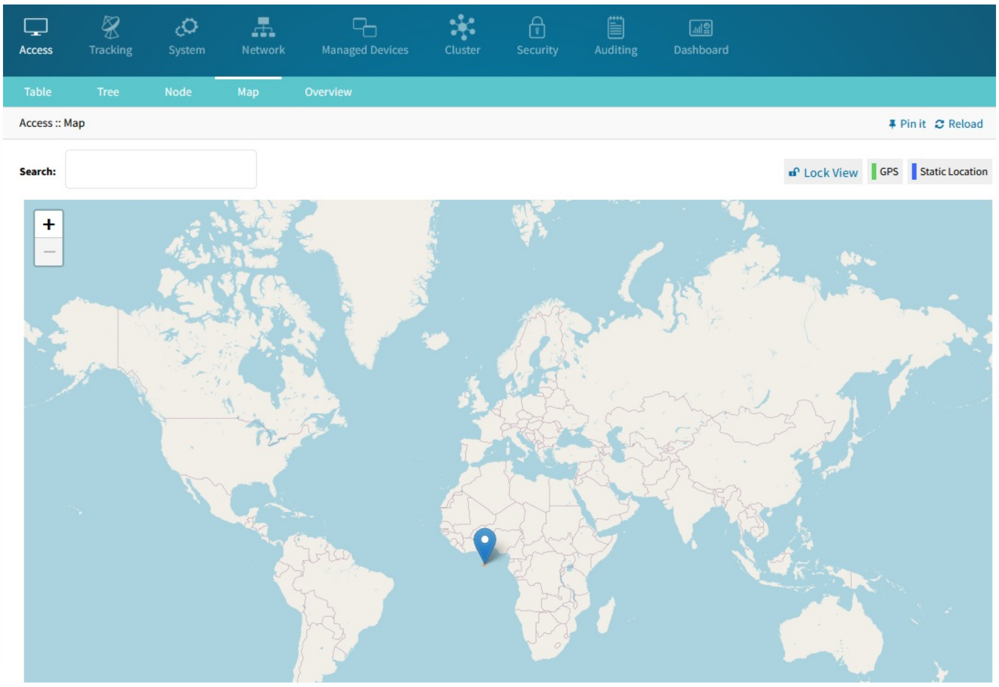
Click on a node to display a pop-up dialog of device details.

View Devices on the Map

This tab shows device status on a global map. It provides an overview of all managed devices and Nodegrid peers in a Cluster. Precise device location details are included down to a building level. Use the mouse to navigate. Hover the mouse over a marker to display further controls. Click on a marker to display device information and connections. Use the *Lock View* button to change the default map window and zoom level.

Map data is fetched from OpenStreetMap directly from/to the user's browser.

Device location can be set on *System :: Preferences :: Nodegrid Location.* When location (static or GPS) is not available, it is considered as (0,0) and a global map is displayed:

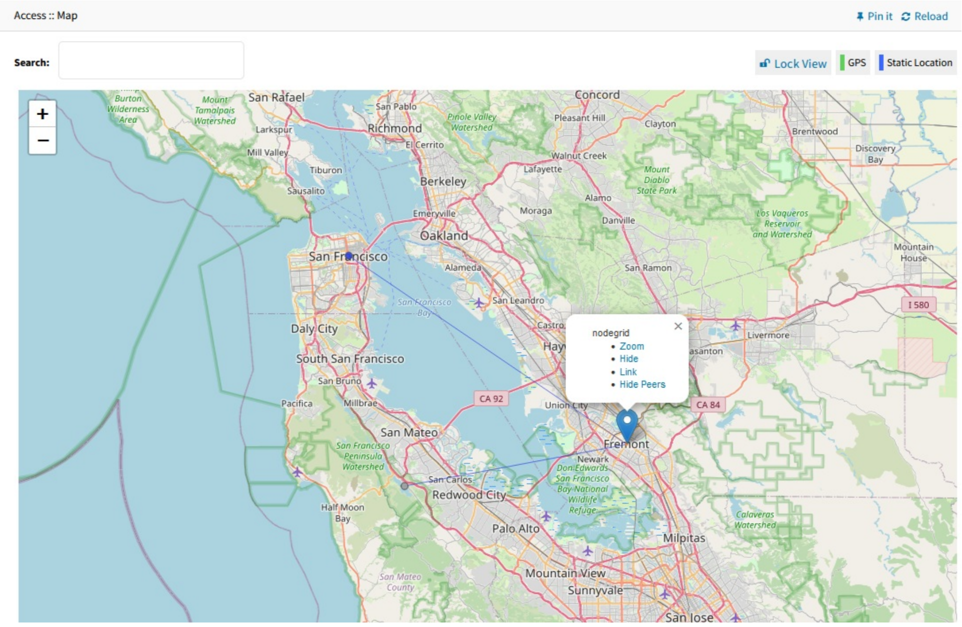


Blue markers are displayed for statically set locations, and green markers are shown when the location is read from GPS.

Managed devices are shown with a circle whose color reflects the device state, similarly to *Access :: Table:*

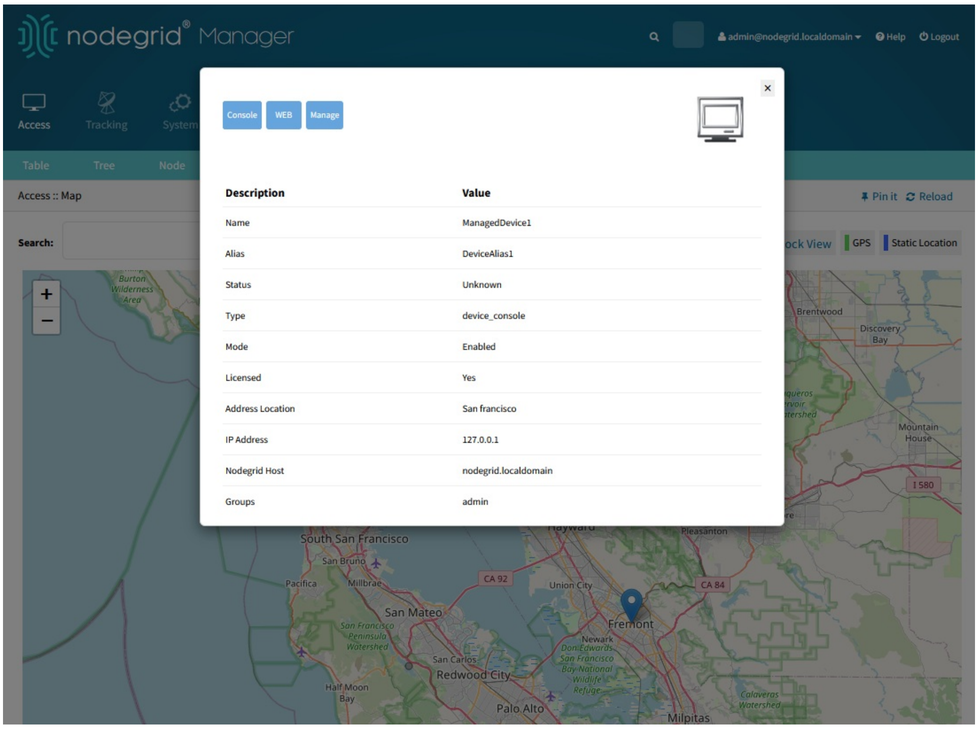
🟩 Connected 🟦 In-Use 🟧 Disconnected ⬜ Unknown

When coordinates are available, the view is zoomed in to fit the devices. Hovering over a device reveals options to *Zoom*, *Hide*, *Link*, and *Hide Peers*. In the following example, a Nodegrid device in Fremont, CA manages two other devices in other locations, and the *Link* option is selected:



When in a cluster, other visible peers are also shown, along with their own visible managed devices.

Clicking on one of the devices shows the summary information and control modal:



Description	Value
Name	ManagedDevice1
Alias	DeviceAlias1
Status	Unknown
Type	device_console
Mode	Enabled
Licensed	Yes
Address Location	San francisco
IP Address	127.0.0.1
Nodegrid Host	nodegrid.localdomain
Groups	admin

Navigation is available with mouse controls (drag, scroll). When the user leaves and returns to the page, the last locked view is loaded.

When the "Lock View" button is clicked, the padlock icon changes:

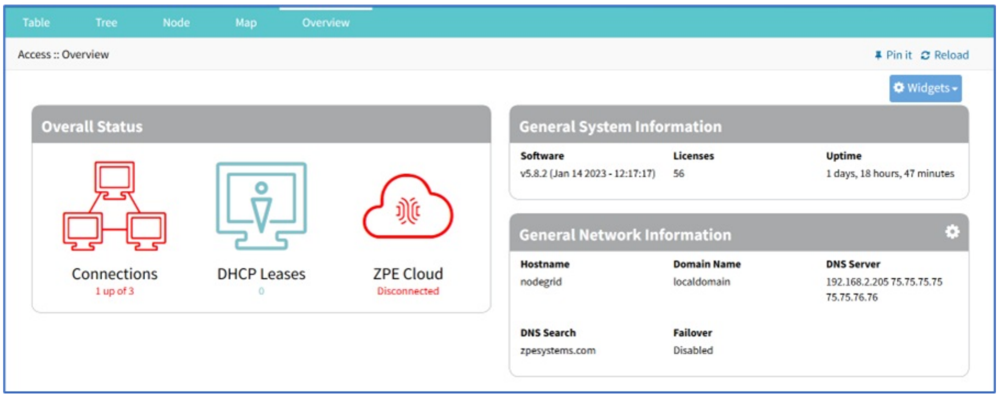
🔒 Lock View

When the button is toggled from unlocked to locked, the current view window is saved in a cookie on the user's browser, and it is displayed when the user returns to the page.

If the user leaves the page with the view unlocked and returns later, the default view is displayed.

View Device Details

This tab provides information on the Nodegrid device.



General System Information

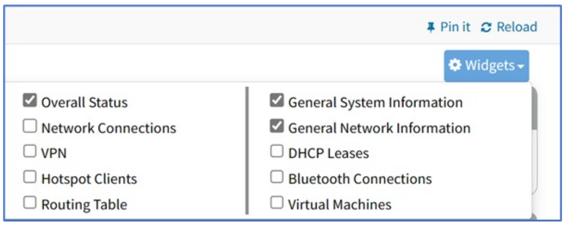
Software	Licenses	Uptime
v5.8.2 (Jan 14 2023 - 12:17:17)	56	1 days, 18 hours, 47 minutes

General Network Information

Hostname	Domain Name	DNS Server
nodegrid	localdomain	192.168.2.205 75.75.75.75 75.75.76.76
DNS Search	**Failover**	
zpesystems.com	Disabled	

If the device's System Profile is configured as Gateway Profile, *Access :: Overview* is the default WebUI page. For devices with Out of Band Profile, the user can use the **Pin It** feature to designate *Access :: Overview* as the default page. (available in v5.6+)

Click the **Widgets** button to configure the display. Select/unselect checkboxes as needed. The order of the checkboxes can be moved (click on a checkbox item, drag and drop inside the widget). This modifies the display of the *Overview* page.



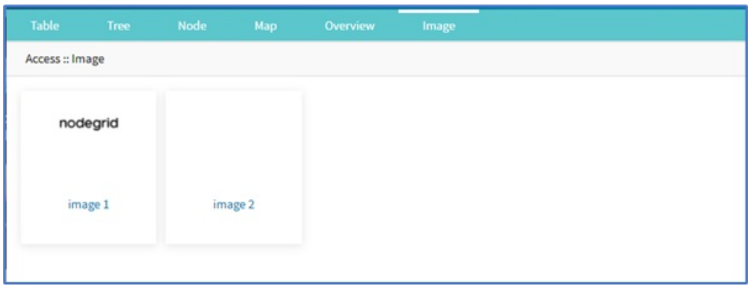
☑ Overall Status
☐ Network Connections
☐ VPN
☐ Hotspot Clients
☐ Routing Table
☑ General System Information
☑ General Network Information
☐ DHCP Leases
☐ Bluetooth Connections
☐ Virtual Machines

Review details, as needed.

Manage Nodegrid Images

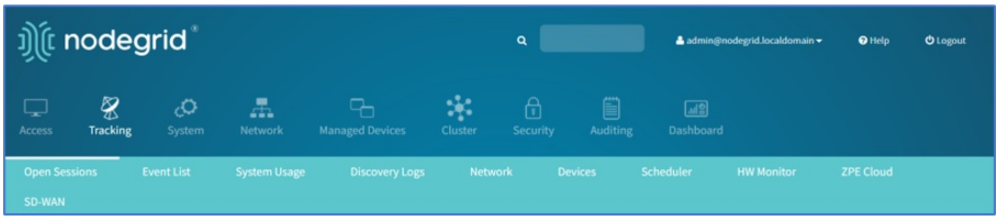
The configuration requires Professional Services implementation. Contact Customer Support at support@zpesystem.com for additional information.

If available, displays a custom view of Nodegrid units and devices with associated information.



Tracking Section

This provides information about the System and connected devices.



You can track the following information:

- Open Sessions: Monitor the ongoing and real-time user sessions.
- Event List: Review a detailed history of system events and alerts.
- Detailed System Usage: Track resource consumption and performance metrics.
- Discovery Logs: Analyze logs related to device and network discovery.
- Network Activities: Observe current network traffic and device interactions.
- Connected Devices: View and manage all linked devices within the system.
- Scheduler: Oversee scheduled tasks and automated operations.
- HW Monitor: Keep tabs on hardware performance and health metrics.
- Integrated ZPE Cloud: Manage and monitor your system through the ZPE Cloud platform.
- SD-WAN: Track and control software-defined networking performance.

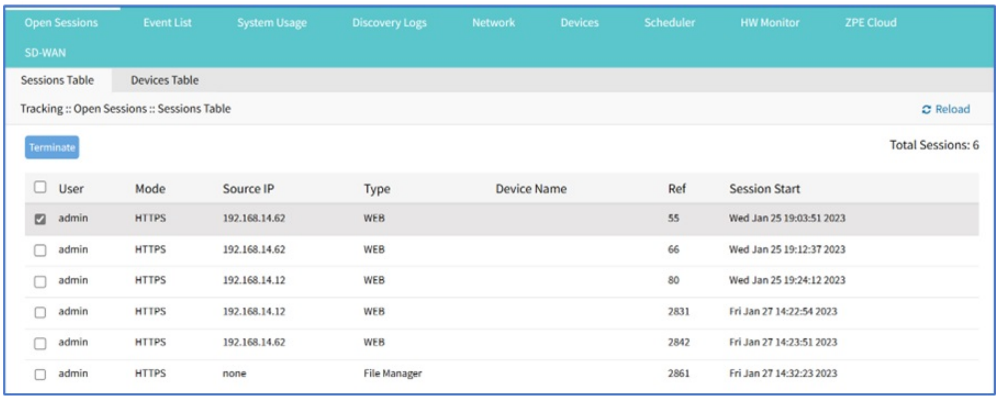
Refer to the sub-sections for more details on each tracking option.

Open Sessions tab

This provides an overview of connected users and devices sessions.

Sessions Table sub-tab

This lists all users actively connected to the system, where they are connected from, and the time period.



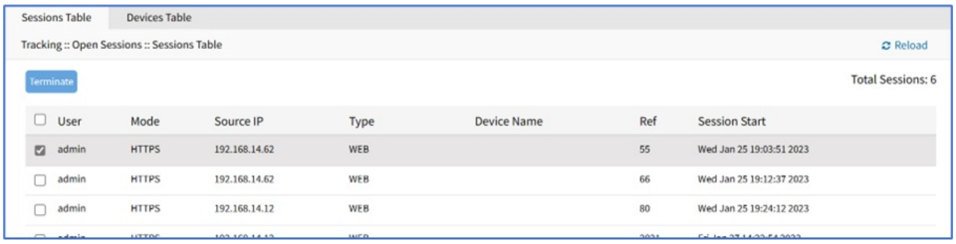
Tracking :: Open Sessions :: Sessions Table

Total Sessions: 6

☐	User	Mode	Source IP	Type	Device Name	Ref	Session Start
☑	admin	HTTPS	192.168.14.62	WEB		55	Wed Jan 25 19:03:51 2023
☐	admin	HTTPS	192.168.14.62	WEB		66	Wed Jan 25 19:12:37 2023
☐	admin	HTTPS	192.168.14.12	WEB		80	Wed Jan 25 19:24:12 2023
☐	admin	HTTPS	192.168.14.12	WEB		2831	Fri Jan 27 14:22:54 2023
☐	admin	HTTPS	192.168.14.62	WEB		2842	Fri Jan 27 14:23:51 2023
☐	admin	HTTPS	none	File Manager		2861	Fri Jan 27 14:32:23 2023

Terminate Session

1. Go to *Tracking :: Open Sessions :: Sessions Table*.
2. In *User* column, locate session and select checkbox.



Tracking :: Open Sessions :: Sessions Table

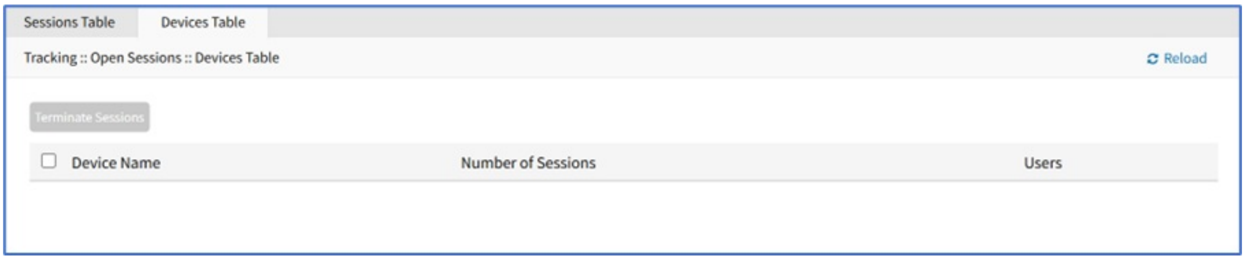
Total Sessions: 6

☐	User	Mode	Source IP	Type	Device Name	Ref	Session Start
☑	admin	HTTPS	192.168.14.62	WEB		55	Wed Jan 25 19:03:51 2023
☐	admin	HTTPS	192.168.14.62	WEB		66	Wed Jan 25 19:12:37 2023
☐	admin	HTTPS	192.168.14.12	WEB		80	Wed Jan 25 19:24:12 2023

3. Click **Terminate**.

Devices Table sub-tab

This shows information about active device sessions, the amount of connected session and the users which are connected.



Tracking :: Open Sessions :: Devices Table

☐	Device Name	Number of Sessions	Users

Terminate Session

1. Go to *Tracking :: Open Sessions :: Devices Table*.
2. In *Device Name* column, locate session and select checkbox.
3. Click **Terminate**.

Event List tab

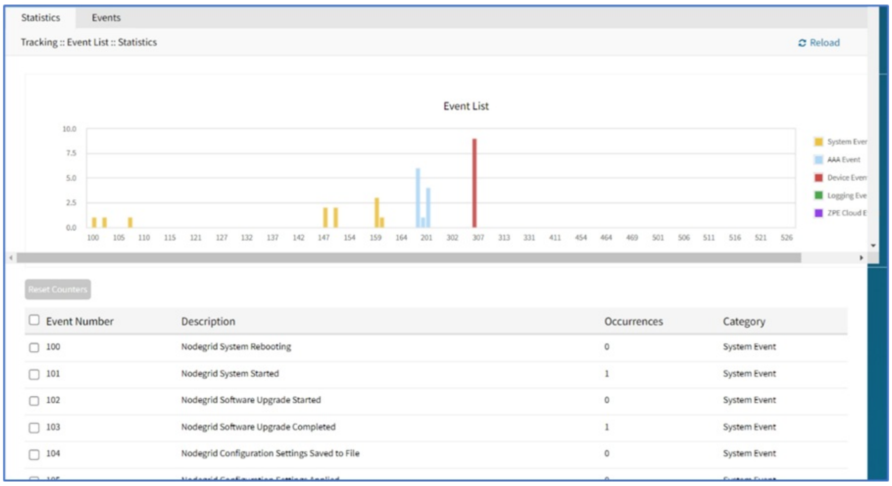
The Event List provides a list of events for a Nodegrid device. It displays the list of events, registered and unregistered, along with statistics.

Refer to the following sections for more information:

- Statistics sub-tab - Viewing Event Statistics
- Events sub-tab - Viewing and Exporting Event Details
- Listing of Registered Events

Statistics sub-tab- Viewing Event Statistics

The Statistics page provides statistical information on the system event occurrences. There are different types of events generated by the system and you can see the list of all the different events triggered by the system on this page:



□ Event Number	Description	Occurrences	Category
□ 100	Nodegrid System Rebooting	0	System Event
□ 101	Nodegrid System Started	1	System Event
□ 102	Nodegrid Software Upgrade Started	0	System Event
□ 103	Nodegrid Software Upgrade Completed	1	System Event
□ 104	Nodegrid Configuration Settings Saved to File	0	System Event
□ 105	Nodegrid Configuration Settings Applied	0	System Event

Reset Event Counter

1. Go to *Tracking :: Event List :: Statistics*.
2. In *Event Number* column, locate the number and select checkbox (can select multiple).
3. Click **Reset Counters**.

Understanding the System Health Check Event

Whenever any alerts are related to the file system, disk space full, or temperature of the device during the periodic scans, the Nodegrid System health check proactively creates an event to notify the user. The timely resolution of such issues is important to keep the system reliable and available.

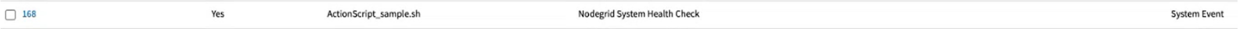
How System Health Check can be useful to the User?

As an administrator, you can view the events and perform the necessary actions to resolve the errors. The following is the list of monitoring checks performed by the System Health, an event is triggered when it occurs for the first time:

- For filesystem errors (bad blocks, critical errors, read-only mode, etc.), filesystem getting full or read-only, SSD life left, and CPU and SSD high-temperature temperature

How does the System Health Check work?

The system health check is executed daily at 2:30 AM; the time of the device. Based on the encountered issues, alerts are displayed under the **Tracking** > **Event** > **Statistics** page. The user can view these alerts and take necessary actions.
Note: You can also upload scripts that take necessary actions based on the alert event that is triggered.



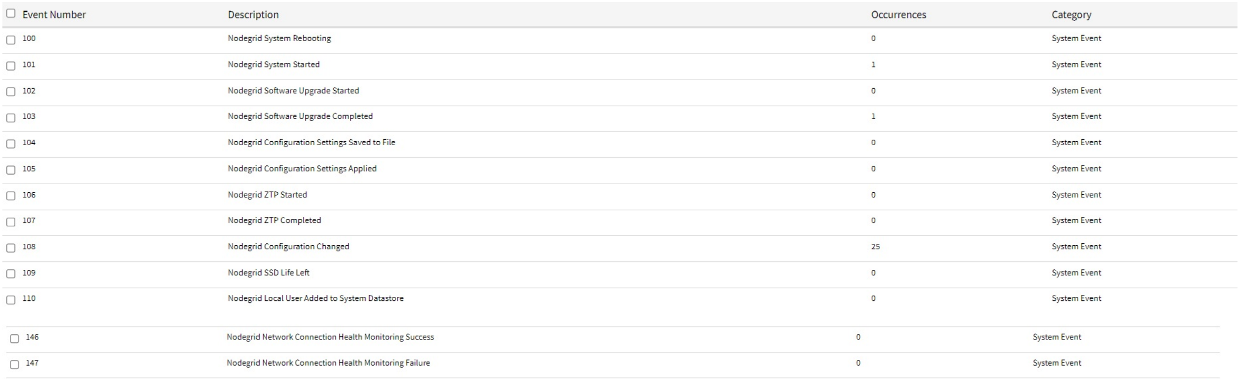
□ 168	Yes	ActionScript_sample.sh	Nodegrid System Health Check	System Event

For more information on uploading scripts, see the Event List sub-tab.

Viewing the System Health Check Alerts

Perform the following actions to view the System Health Check Alerts:

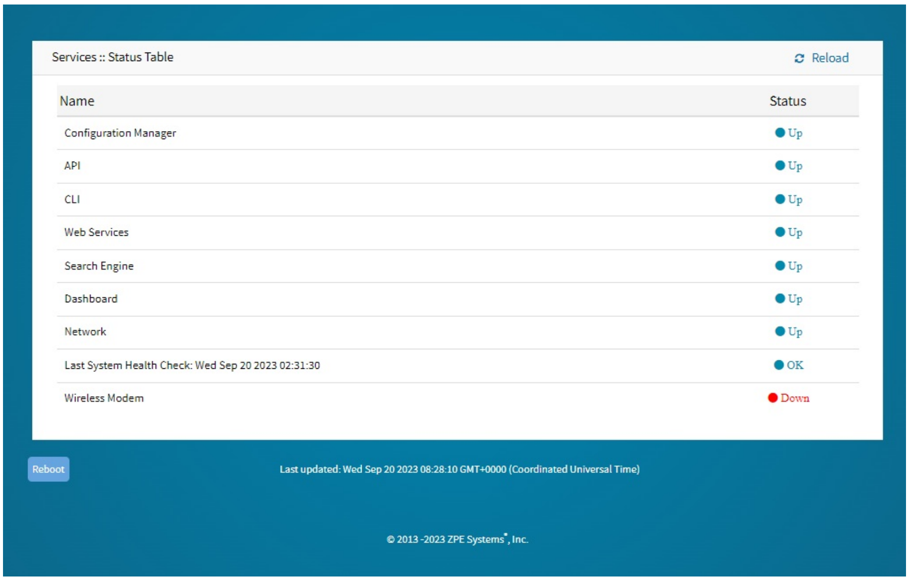
1. Log in to your Nodegrid web UI.
2. Go to Tracking:: Event List
3. Under the **Statistics** tab, the alerts are displayed as shown in the following image:



□ Event Number	Description	Occurrences	Category
□ 100	Nodegrid System Rebooting	0	System Event
□ 101	Nodegrid System Started	1	System Event
□ 102	Nodegrid Software Upgrade Started	0	System Event
□ 103	Nodegrid Software Upgrade Completed	1	System Event
□ 104	Nodegrid Configuration Settings Saved to File	0	System Event
□ 105	Nodegrid Configuration Settings Applied	0	System Event
□ 106	Nodegrid ZTP Started	0	System Event
□ 107	Nodegrid ZTP Completed	0	System Event
□ 108	Nodegrid Configuration Changed	25	System Event
□ 109	Nodegrid SSD Life Left	0	System Event
□ 110	Nodegrid Local User Added to System Datastore	0	System Event
□ 146	Nodegrid Network Connection Health Monitoring Success	0	System Event
□ 147	Nodegrid Network Connection Health Monitoring Failure	0	System Event

You can also view the system alerts using the following URL format: **https://HostIPAddress/services/status**

The Last System Health check column displays when the last system health check was executed as shown in the following image:



Services :: Status Table

Name	Status
Configuration Manager	● Up
API	● Up
CLI	● Up
Web Services	● Up
Search Engine	● Up
Dashboard	● Up
Network	● Up
Last System Health Check: Wed Sep 20 2023 02:31:30	● OK
Wireless Modem	● Down

Last updated: Wed Sep 20 2023 08:28:10 GMT+0000 (Coordinated Universal Time)

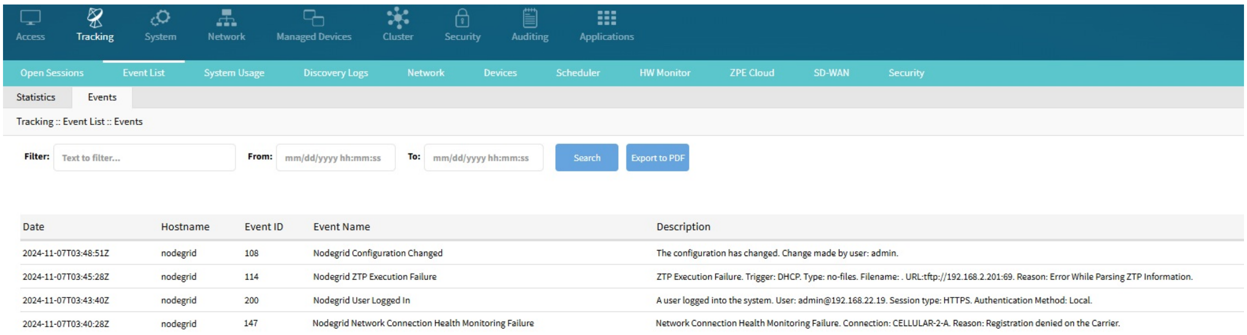
© 2013 -2023 ZPE Systems®, Inc.

The last system check result is saved in the /var/run/system_check.txt file.

Events sub-tab - Viewing and Exporting Event List

The Events page displays event details (read-only).

> **NOTE**
>
> To view the Events tab under the Event List, ensure that the **Enable Search Engine** option is selected. To enable this option:
>
> 1. Go to *Security :: Services*.
> 2. In the Active Services section, select **Enable Search Engine**.
> 3. Click **Save**.



Date	Hostname	Event ID	Event Name	Description
2024-11-07T03:48:51Z	nodegrid	108	Nodegrid Configuration Changed	The configuration has changed. Change made by user: admin.
2024-11-07T03:45:28Z	nodegrid	114	Nodegrid ZTP Execution Failure	ZTP Execution Failure. Trigger: DHCP. Type: no-files. Filename: . URL:tftp://192.168.2.201:69. Reason: Error While Parsing ZTP Information.
2024-11-07T03:43:40Z	nodegrid	200	Nodegrid User Logged In	A user logged into the system. User: admin@192.168.22.19. Session type: HTTPS. Authentication Method: Local.
2024-11-07T03:40:28Z	nodegrid	147	Nodegrid Network Connection Health Monitoring Failure	Network Connection Health Monitoring Failure. Connection: CELLULAR-2-A. Reason: Registration denied on the Carrier.

Export Event Listing to PDF

The PDF file can contain a maximum of 10,000 results. The list is based on the Filter fields and the **From** and **To** dates.

1. Go to *Tracking :: Event List :: Events*.
2. (optional) Enter **Filter** keyword.
3. (optional) Adjust **From** and **To** date/time, then click **Search**.
4. Click **Export to PDF**.
5. On *Save* dialog, navigate to the preferred file location, then click **Save**.

Listing of Registered Events

This listing shows all the registered events and associated categories.

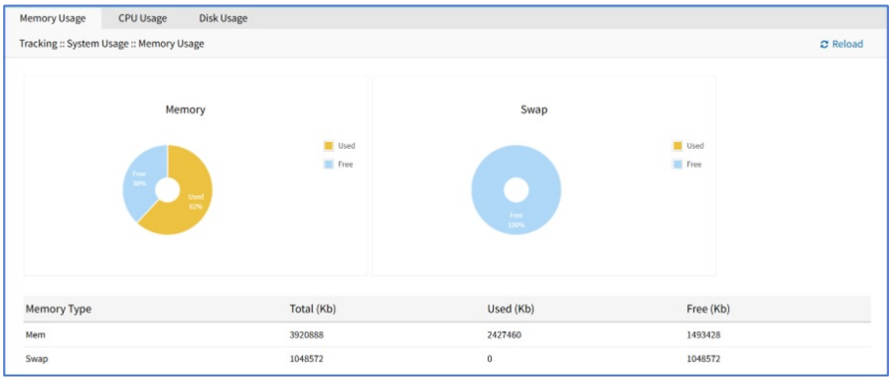
Event #	Description	Category
100	Nodegrid System Rebooting	System Event
101	Nodegrid System Started	System Event
102	Nodegrid Software Upgrade Started	System Event
103	Nodegrid Software Upgrade Completed	System Event
104	Nodegrid Configuration Settings Saved to File	System Event
105	Nodegrid Configuration Settings Applied	System Event
106	Nodegrid ZTP Started	System Event
107	Nodegrid ZTP Completed	System Event
108	Nodegrid Configuration Changed	System Event
109	Nodegrid SSD Life Left	System Event
110	Nodegrid Local User Added to System Datastore	System Event
111	Nodegrid Local User Deleted from System Datastore	System Event
112	Nodegrid Local User Modified in System Datastore	System Event
113	Nodegrid ZTP execution success	System Event
114	Nodegrid ZTP execution failure	System Event
115	Nodegrid Session Terminated	System Event
116	Nodegrid Session Timed Out	System Event
118	Nodegrid Power Supply State Changed	System Event
119	Nodegrid Power Supply Sound Alarm Stopped by User	System Event
120	Nodegrid Utilization Rate Exceeded	System Event
121	Nodegrid Thermal Temperature ThrottleUp	System Event
122	Nodegrid Thermal Temperature Dropping	System Event
123	Nodegrid Thermal Temperature Warning	System Event
124	Nodegrid Thermal Temperature Critical	System Event
126	Nodegrid Fan Status Changed	System Event
127	Nodegrid Fan Sound Alarm Stopped by User	System Event
128	Nodegrid Total number of local serial ports mismatch	System Event
129	Nodegrid dry contact change state	System Event
130	Nodegrid License Added	System Event
131	Nodegrid License Removed	System Event
132	Nodegrid License Conflict	System Event
133	Nodegrid License Scarce	System Event
134	Nodegrid License Expiring	System Event
135	Nodegrid Shell Started	System Event
136	Nodegrid Shell Stopped	System Event
137	Nodegrid Sudo Executed	System Event
138	Nodegrid SMS Executed	System Event
139	Nodegrid SMS Invalid	System Event
140	Nodegrid Connection Up	System Event
141	Nodegrid Connection Down	System Event
142	Nodegrid SIM Card Swap	System Event
144	Network Failover Executed	System Event
145	Network Failback Executed	System Event
150	Nodegrid Cluster Peer Online	System Event
151	Nodegrid Cluster Peer Offline	System Event
152	Nodegrid Cluster Peer Signed On	System Event
153	Nodegrid Cluster Peer Signed Off	System Event
154	Nodegrid Cluster Peer Removed	System Event
155	Nodegrid Cluster Peer Became Coordinator	System Event
156	Nodegrid Cluster Coordinator Became Peer	System Event
157	Nodegrid Cluster Coordinator Deleted	System Event
158	Nodegrid Cluster Coordinator Created	System Event

159	Nodegrid Cluster Peer Configured	System Event
160	Nodegrid Search Unavailable	System Event
161	Nodegrid Search Restored	System Event
166	Nodegrid Wireguard Tunnel Up (Post Up) (v5.8+)	
167	Nodegrid Wireguard Tunnel Down (Post Down) (v5.8+)	
200	Nodegrid User Logged In	AAA Event
201	Nodegrid User Logged Out	AAA Event
202	Nodegrid System Authentication Failure	AAA Event
204	Nodegrid System Authentication Account Blocked	AAA Event
300	Nodegrid Device Session Started	Device Event
301	Nodegrid Device Session Stopped	Device Event
302	Nodegrid Device Created	Device Event
303	Nodegrid Device Deleted	Device Event
304	Nodegrid Device Renamed	Device Event
305	Nodegrid Device Cloned	Device Event
306	Nodegrid Device Up	Device Event
307	Nodegrid Device Down	Device Event
308	Nodegrid Device Session Terminated	Device Event
310	Nodegrid Power On Command Executed on a Device	Device Event
311	Nodegrid Power Off Command Executed on a Device	Device Event
312	Nodegrid Power Cycle Command Executed on a Device	Device Event
313	Nodegrid Suspend Command Executed on a Device	Device Event
314	Nodegrid Reset Command Executed on a Device	Device Event
315	Nodegrid Shutdown Command Executed on a Device	Device Event
400	Nodegrid System Alert Detected	Logging Event
401	Nodegrid Alert String Detected on a Device Session	Logging Event
402	Nodegrid Event Log String Detected on a Device Event Log	Logging Event
410	Nodegrid System NFS Failure	Logging Event
411	Nodegrid System NFS Recovered	Logging Event
450	Nodegrid Datapoint State High Critical	Logging Event
451	Nodegrid Datapoint State High Warning	Logging Event
452	Nodegrid Datapoint State Normal	Logging Event
453	Nodegrid Datapoint State Low Warning	Logging Event
454	Nodegrid Datapoint State Low Critical	Logging Event
460	Nodegrid Door Unlocked	Logging Event
461	Nodegrid Door Locked	Logging Event
462	Nodegrid Door Open	Logging Event
463	Nodegrid Door Close	Logging Event
464	Nodegrid Door Access Denied	Logging Event
465	Nodegrid Door Alarm Active	Logging Event
466	Nodegrid Door Alarm Inactive	Logging Event
467	Nodegrid PoE Power Fault	Logging Event
468	Nodegrid PoE Power Budget Exceeded	Logging Event

System Usage tab

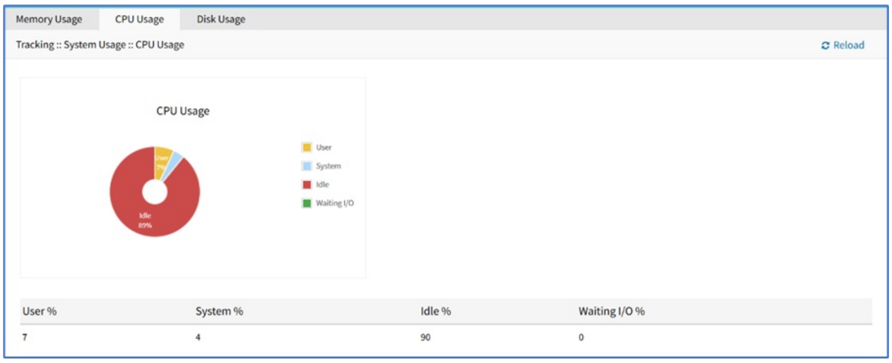
This presents information usage details. The sub-tabs provide read-only information.

Memory Usage sub-tab



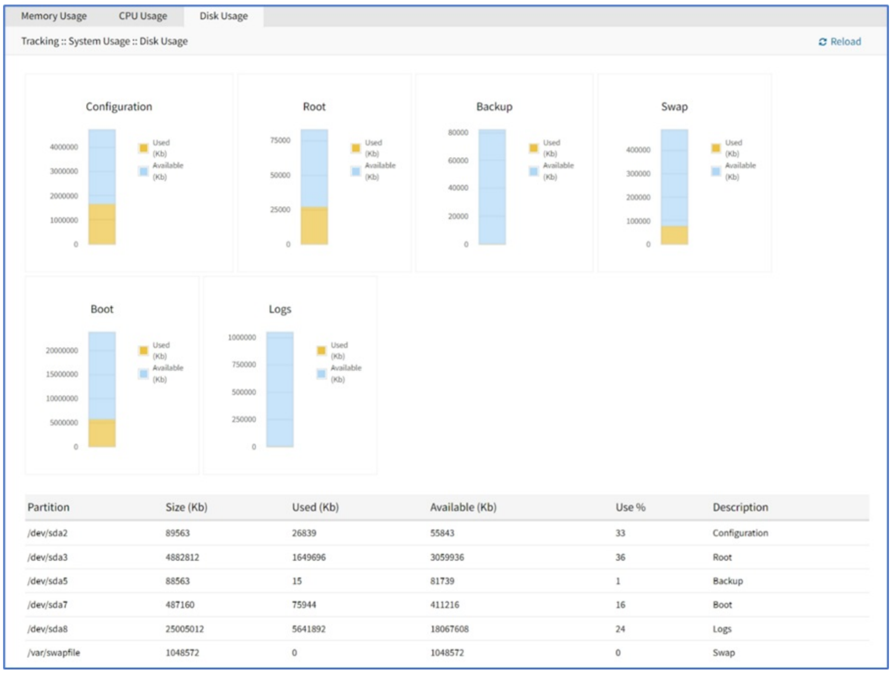
Memory Type	Total (Kb)	Used (Kb)	Free (Kb)
Mem	3920888	2427460	1493428
Swap	1048572	0	1048572

CPU Usage sub-tab



User %	System %	Idle %	Waiting I/O %
7	4	90	0

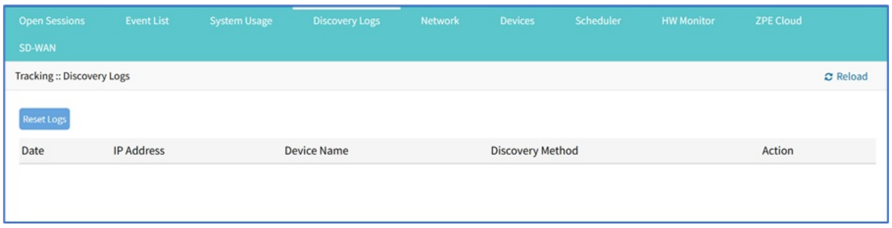
Disk Usage sub-tab



Partition	Size (Kb)	Used (Kb)	Available (Kb)	Use %	Description
/dev/sda2	89563	26839	55843	33	Configuration
/dev/sda3	4882812	1649696	3059936	36	Root
/dev/sda5	88563	15	81739	1	Backup
/dev/sda7	487160	75944	411216	16	Boot
/dev/sda8	25005012	5641892	18067608	24	Logs
/var/swapfile	1048572	0	1048572	0	Swap

Discovery Logs tab

This page shows the logs of the discovery processes set on the Managed Devices setting for auto-discovery. You can also locate the discovery logs at the location/v1/devices/discovery/logs.



Tracking :: Discovery Logs

Date	IP Address	Device Name	Discovery Method	Action

Reset Logs

1. Go to *Tracking :: Discovery Logs*.
2. Click **Reset Logs** to clear the discovery logs table.

Network tab

This displays network Interface information, LLDP, Routing Table, IPsec Table, and Hotspot details.

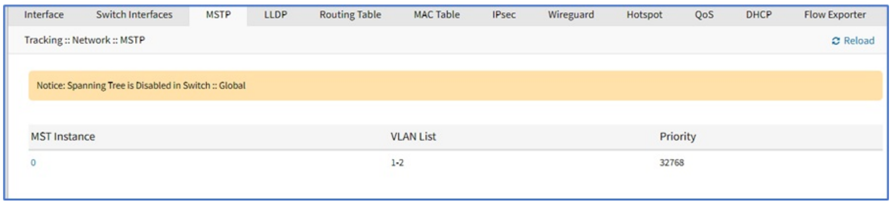
NOTE

The displayed sub-tabs can change depending on the device configuration.

The following topics are covered in this section:

- MSTP sub-tab (Net SR)
- Interface sub-tab
- Tracking Network Failover
- Switch Interfaces Sub-tab
- Viewing the Switch interfaces Status and Statistics
- Routing Table sub-tab
- MAC Table sub-tab (NSR)
- IPsec sub-tab
- Wireguard sub-tab
- Hotspot sub-tab
- QoS sub-tab
- Flow Exporter sub-tab
- DHCP sub-tab
- LLDP sub-tab

MSTP sub-tab (Net SR)



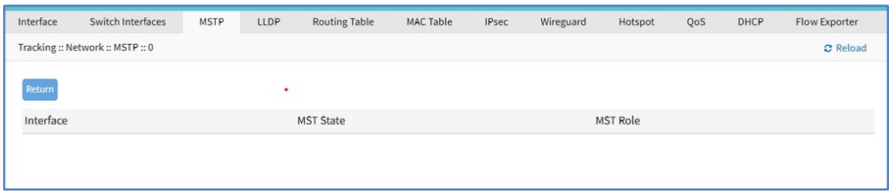
Tracking :: Network :: MSTP

Notice: Spanning Tree is Disabled in Switch :: Global

MST Instance	VLAN List	Priority
0	1-2	32768

View MSTP Instance Details

1. Go to *Tracking :: Network :: MSTP*.
2. In *MST Instance* column, click on name (displays dialog).



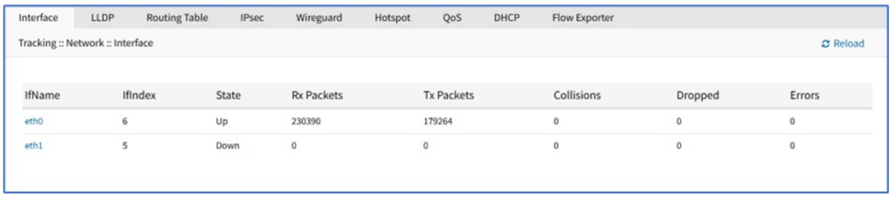
Tracking :: Network :: MSTP :: 0

Interface	MST State	MST Role

3. Click **Return**.

Interface sub-tab

This displays the network interface statistics, like state, package counters, collisions, dropped and errors.

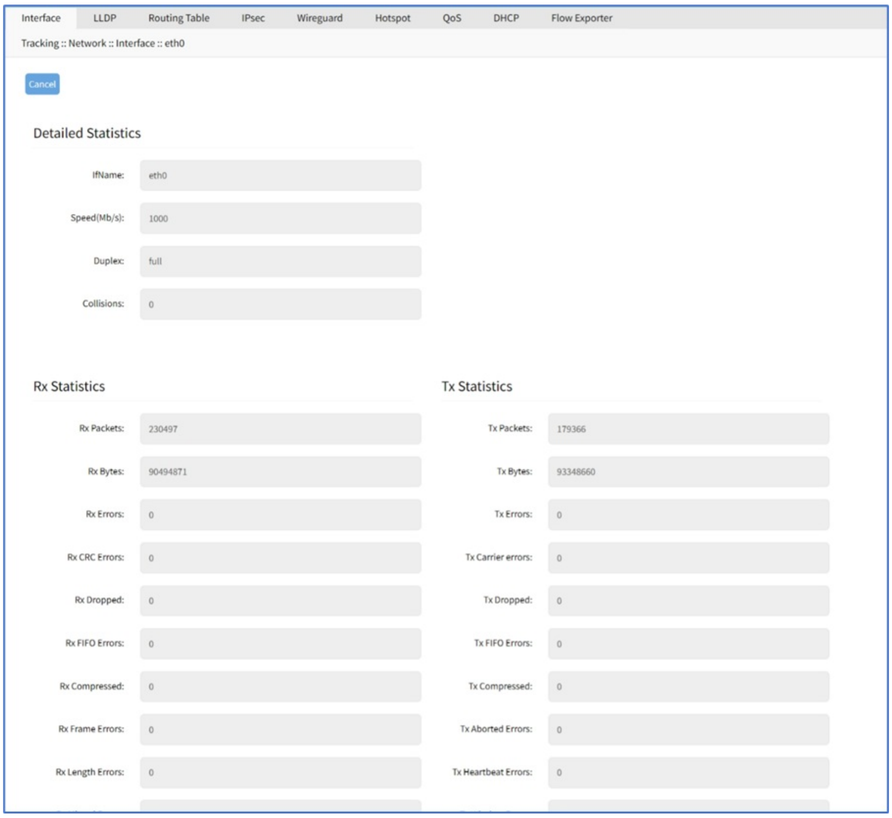


Tracking :: Network :: Interface

IfName	IfIndex	State	Rx Packets	Tx Packets	Collisions	Dropped	Errors
eth0	6	Up	230390	179264	0	0	0
eth1	5	Down	0	0	0	0	0

Review Interface Details

1. Go to *Tracking :: Network :: Interface*.
2. Click on an Interface (displays dialog): Review details:
   - **Detailed Statistics** section
   - **Rx Statistics** section
   - **Tx Statistics** section



Tracking :: Network :: Interface :: eth0

Detailed Statistics

IfName: eth0

Speed(Mb/s): 1000

Duplex: full

Collisions: 0

Rx Statistics

Rx Packets: 230497

Rx Bytes: 90494871

Rx Errors: 0

Rx CRC Errors: 0

Rx Dropped: 0

Rx FIFO Errors: 0

Rx Compressed: 0

Rx Frame Errors: 0

Rx Length Errors: 0

Tx Statistics

Tx Packets: 179366

Tx Bytes: 93348660

Tx Errors: 0

Tx Carrier errors: 0

Tx Dropped: 0

Tx FIFO Errors: 0

Tx Compressed: 0

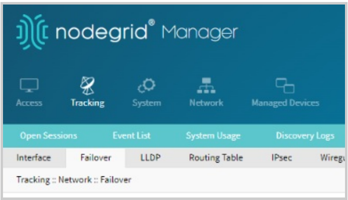
Tx Aborted Errors: 0

Tx Heartbeat Errors: 0

3. **Cancel** button returns to the **Interface** sub-tab.

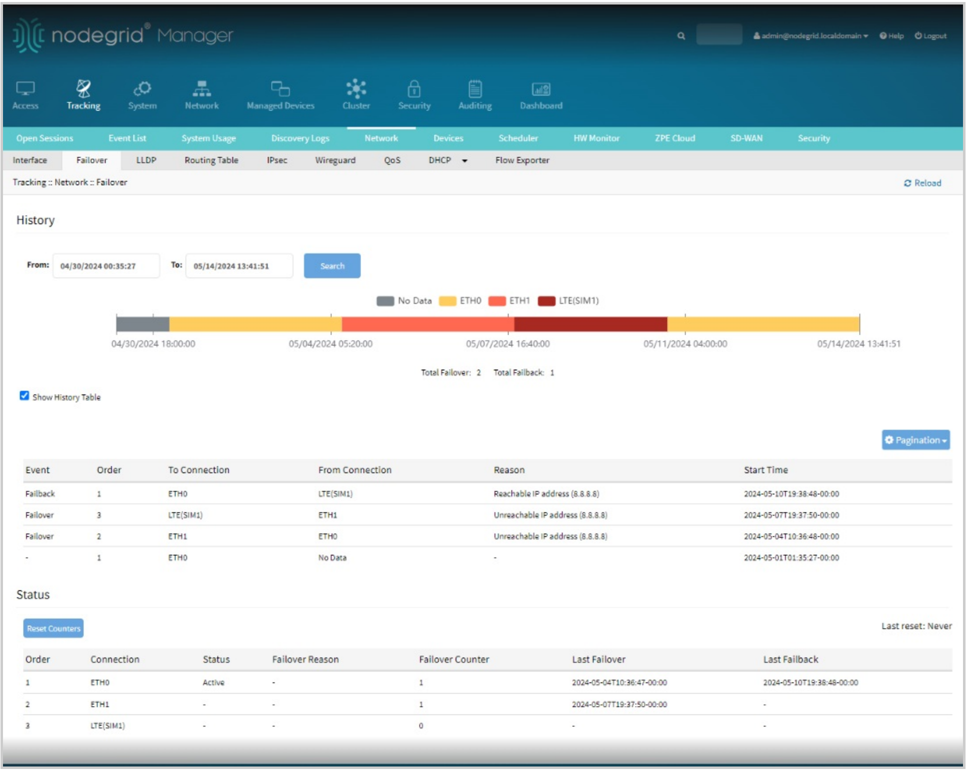
Tracking Network Failover

Before you track the status of the failover of a device you must trigger the failover for that device. To trigger the failover, navigate to the section *Network :: Failover :: Connections*. For more information, see the section Configuring Network Failover. You can track the status of the failover history of devices by navigating to *Tracking:: Network :: Failover.*



This page includes the following options:

- **History**: The history section provides a detailed view of events within a specified time interval, including failover, failback, and failover disabled events. This data is visually presented in a chart, with dates and the connection statuses displayed.
- **Date intervals**: By default, the page opens with a one-month interval, which can be adjusted using the start and end date fields. You can filter historical data by specific date intervals using the search fields, allowing for targeted analysis of past events. This historical data is visually represented in a chart for an intuitive overview.
- **Status table**: The status table displays the current connection status, reasons for failovers, and event counters, providing real-time insights into network performance and issues.
- **Show History Table**: You can choose to view this data in a tabular format by enabling the Show History Table checkbox, offering flexibility in how information is presented and analyzed.
- **Reset Counters**: At the bottom of the chart, counters for failover and failback events within the selected interval are displayed. Clicking on **Reset Counters** resets the Failover counter and displays the last reset timestamp adjacent to it.



History

From: 04/30/2024 00:35:27 To: 05/14/2024 13:41:51

Total Failover: 2 Total Failback: 1

☑ Show History Table

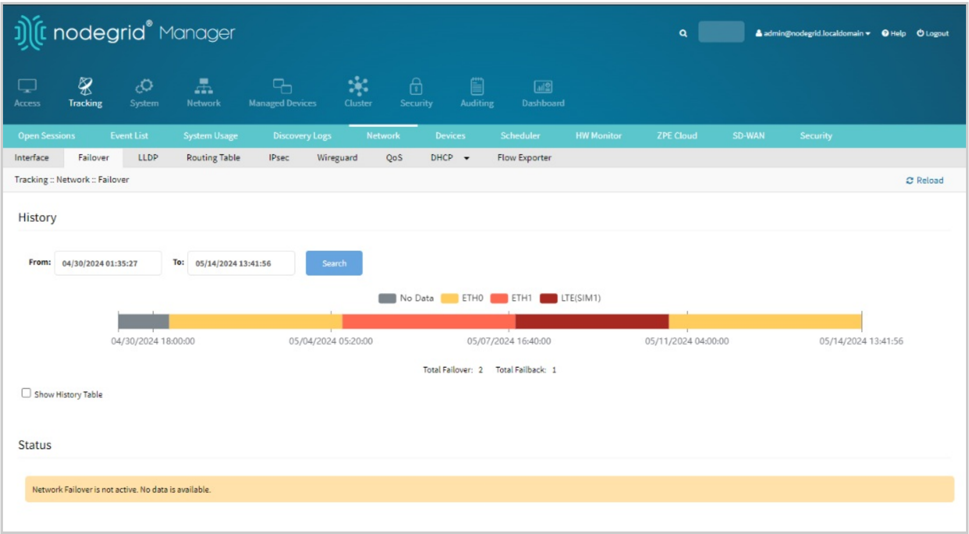
Event	Order	To Connection	From Connection	Reason	Start Time
Failback	1	ETH0	LTE(SIM1)	Reachable IP address (8.8.8.8)	2024-05-10T19:38:48-00:00
Failover	3	LTE(SIM1)	ETH1	Unreachable IP address (8.8.8.8)	2024-05-07T19:37:50-00:00
Failover	2	ETH1	ETH0	Unreachable IP address (8.8.8.8)	2024-05-04T10:36:48-00:00
-	1	ETH0	No Data	-	2024-05-01T01:35:27-00:00

Status

Last reset: Never

Order	Connection	Status	Failover Reason	Failover Counter	Last Failover	Last Failback
1	ETH0	Active	-	1	2024-05-04T10:36:47-00:00	2024-05-10T19:38:48-00:00
2	ETH1	-	-	1	2024-05-07T19:37:50-00:00	-
3	LTE(SIM1)	-	-	0	-	-

When Network Failover is disabled, the status table is absent. Only the historical data is displayed.



Tracking :: Network :: Failover

History

From: 04/30/2024 01:35:27 To: 05/14/2024 13:41:56

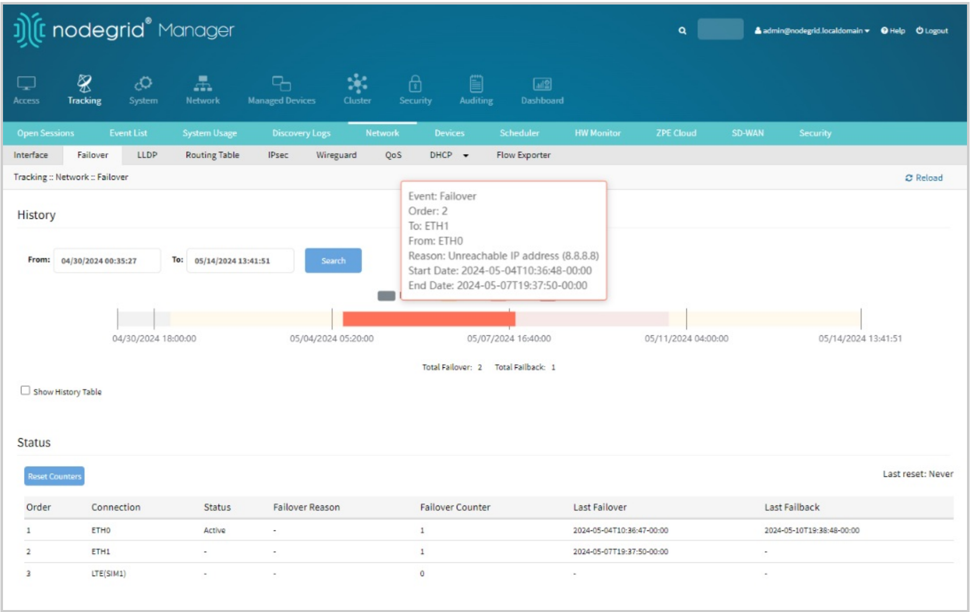
Total Failover: 2 Total Failback: 1

☐ Show History Table

Status

Network Failover is not active. No data is available.

When hovering over a connection interval, additional information is revealed, such as the event type, order number (indicating the sequence of failover active connection), to connection, from connection, reason, start date, and end date.



Tracking :: Network :: Failover

History

From: 04/30/2024 00:35:27 To: 05/14/2024 13:41:51

Event: Failover
Order: 2
To: ETH1
From: ETH0
Reason: Unreachable IP address (8.8.8.8)
Start Date: 2024-05-04T10:36:48-00:00
End Date: 2024-05-07T19:37:50-00:00

Total Failover: 2 Total Failback: 1

☐ Show History Table

Status

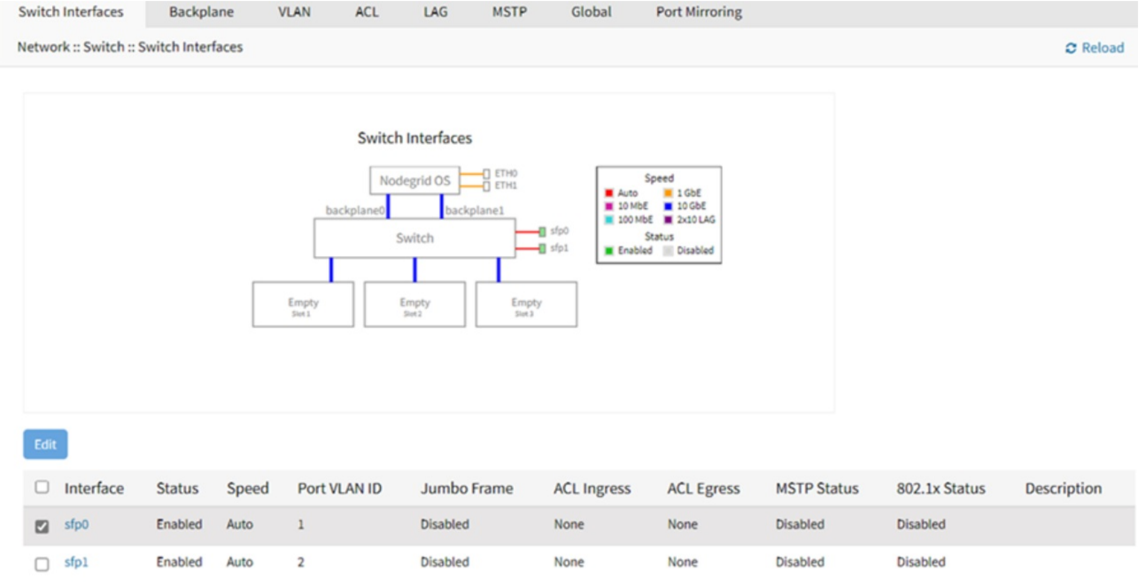
Last reset: Never

Order	Connection	Status	Failover Reason	Failover Counter	Last Failover	Last Failback
1	ETH0	Active	-	1	2024-05-04T10:36:47-00:00	2024-05-10T19:38:48-00:00
2	ETH1	-	-	1	2024-05-07T19:37:50-00:00	-
3	LTE(SIM1)	-	-	0	-	-

Switch Interfaces Sub-tab

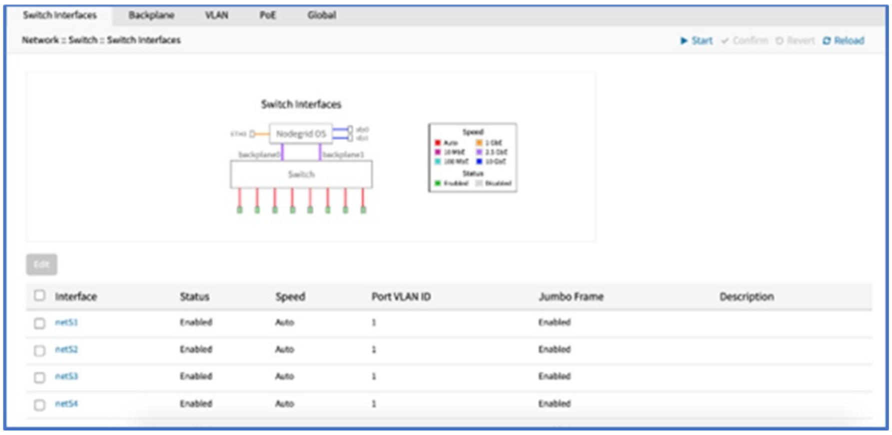
The Switch Interfaces sub-tab provides an overview of all switch ports.

NSR



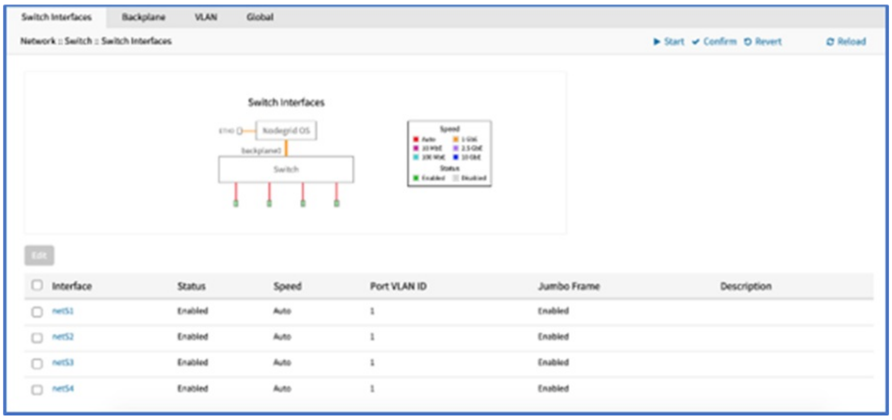
□	Interface	Status	Speed	Port VLAN ID	Jumbo Frame	ACL Ingress	ACL Egress	MSTP Status	802.1x Status	Description
☑	sfp0	Enabled	Auto	1	Disabled	None	None	Disabled	Disabled	
□	sfp1	Enabled	Auto	2	Disabled	None	None	Disabled	Disabled	

GSR



□	Interface	Status	Speed	Port VLAN ID	Jumbo Frame	Description
□	netS1	Enabled	Auto	1	Enabled	
□	netS2	Enabled	Auto	1	Enabled	
□	netS3	Enabled	Auto	1	Enabled	
□	netS4	Enabled	Auto	1	Enabled	

BSR



□	Interface	Status	Speed	Port VLAN ID	Jumbo Frame	Description
□	netS1	Enabled	Auto	1	Enabled	
□	netS2	Enabled	Auto	1	Enabled	
□	netS3	Enabled	Auto	1	Enabled	
□	netS4	Enabled	Auto	1	Enabled	

Edit Switch Port Interface (NSR, NSR Lite)

1. Go to *Network:: Switch:: Switch Interfaces*.
2. In the table, select the checkbox.
3. Click **Edit**(displays dialog). Enter the following details:
    a. **Status**: Enable or disable the switch port. By default, the SFP0 and SFP1 are enabled and the expansion card ports are disabled.
    b. **Description**: Enter port description.
    c. **Speed**:
        i. Auto: For SFP0 and SFP1, the “Auto” means the SFP type will be read from the SFP EEPROM when the configuration is saved or during the boot, and the 10G or 1G speed will be set accordingly; it requires the SFP transceiver to be present when the configuration is saved or during the boot. For non-SFP ports, the “Auto” means auto-negotiation is enabled for 1G, 100M and 10M.
        Note: If auto-negotiation is required for 1G SFP in SFP0, SFP1, and 8-SFP, select 1G speed and select **Auto-negotiation Enabled**

        ii. 10G: 10 Gbps
        iii. 1G: for SFP0, SFP1 and 8-SFP, the “Auto-negotiation” selection is available for speed 1 Gbps.
        iv. 10/100/1000: to be used with 10/100/1000BASE-T SFP transceivers
        v. 100M: 100 Mbps
        vi. 10M: 10 Mbps

    d. **Port VLAN ID**: VLAN to be assigned to the untagged ingress packets.
    e. **Jumbo Frame**: The Jumbo Frame configured under Global will be used if enabled.
    f. **ACL Egress**: Select the Access Control List for the egress packets.
    g. **DHCP Snooping**: Trusted means this is a trusted port so DHCP Server responses will be accepted; Untrusted means the DHCP Server responses will be dropped. This configuration is applicable only if DHCP Snooping is enabled under Global, and DHCP Snooping is enabled in the VLANs.
    h. **MSTP Status**: Enable or disable the spanning tree in the port. For this configuration to be active, the Spanning Tree under Global needs to be enabled.
    i. **BPDU Guard**: If a port with BPDU Guard enabled receives a BPDU, the port is disabled. The MST Role will show **Disabled (BPDU Guard)**. For this configuration to be active, the Spanning Tree under Global needs to be enabled.

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

Edit Switch Port Interface (BSR, GSR)

1. Go to *Network :: Switch :: Switch Interfaces*.
2. In the table, select the checkbox.
3. Click **Edit** (displays dialog).
4. Make changes, as needed.
5. Click **Save**.

Edit Switch Port (BSR, GSR)

1. Go to *Network :: Switch :: Switch Interfaces.*
2. In the table, select the checkbox. Click **Edit** (displays dialog).
    a. ***Status**: Enable or disable the switch port. By default, the switch ports are enabled.
    b. **Description**: Enter port description.
    c. **Speed**:
        i. **Auto**: auto-negotiated speed.

    d. **Port VLAN ID**: VLAN to be assigned to the untagged ingress packets.
    e. **Jumbo Frame**: The default MRU size is 10240 bytes.

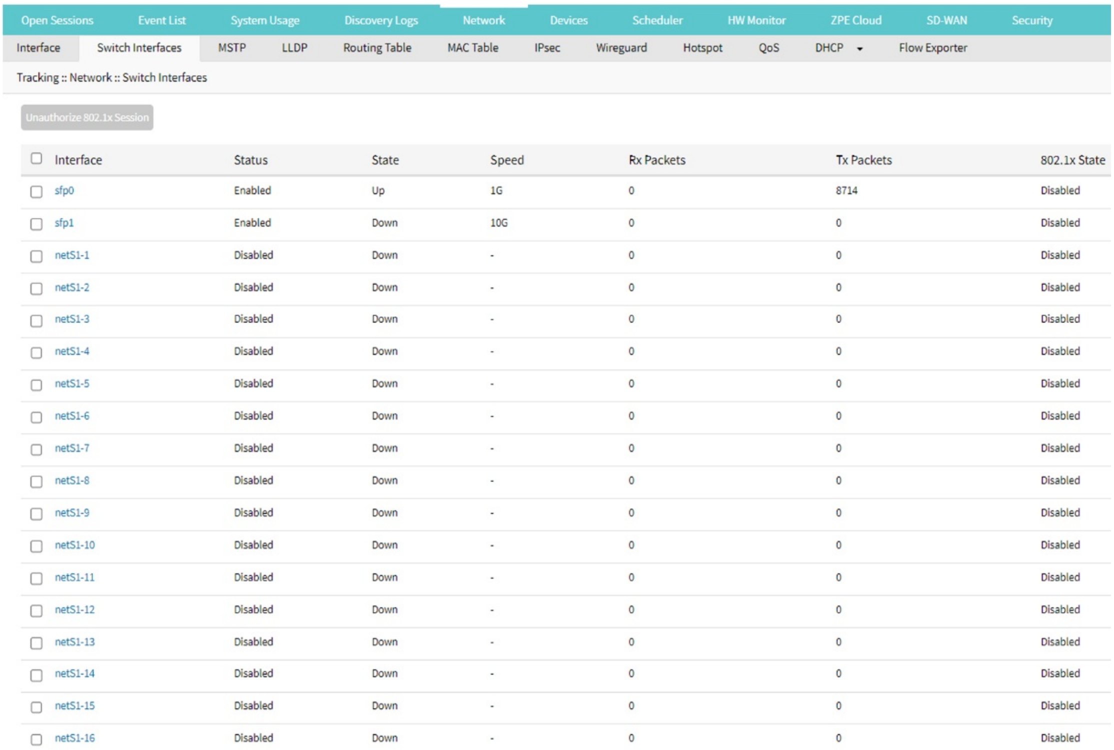
3. Make changes, as needed.
4. Click **Save.**

View the Switch Interfaces Status and Statistics

Go to *Tracking :: Network :: Switch Interfaces* to view the switch interfaces status and statistics.

Viewing the Switch interfaces Status and Statistics

The **Switch interface** tab provides detailed statistics of all the interfaces connected to the Nodegrid device and displays EEPROM information when a transceiver is connected to the SFP interface.



□ Interface	Status	State	Speed	Rx Packets	Tx Packets	802.1x State
□ sfp0	Enabled	Up	1G	0	8714	Disabled
□ sfp1	Enabled	Down	10G	0	0	Disabled
□ netS1-1	Disabled	Down	-	0	0	Disabled
□ netS1-2	Disabled	Down	-	0	0	Disabled
□ netS1-3	Disabled	Down	-	0	0	Disabled
□ netS1-4	Disabled	Down	-	0	0	Disabled
□ netS1-5	Disabled	Down	-	0	0	Disabled
□ netS1-6	Disabled	Down	-	0	0	Disabled
□ netS1-7	Disabled	Down	-	0	0	Disabled
□ netS1-8	Disabled	Down	-	0	0	Disabled
□ netS1-9	Disabled	Down	-	0	0	Disabled
□ netS1-10	Disabled	Down	-	0	0	Disabled
□ netS1-11	Disabled	Down	-	0	0	Disabled
□ netS1-12	Disabled	Down	-	0	0	Disabled
□ netS1-13	Disabled	Down	-	0	0	Disabled
□ netS1-14	Disabled	Down	-	0	0	Disabled
□ netS1-15	Disabled	Down	-	0	0	Disabled
□ netS1-16	Disabled	Down	-	0	0	Disabled

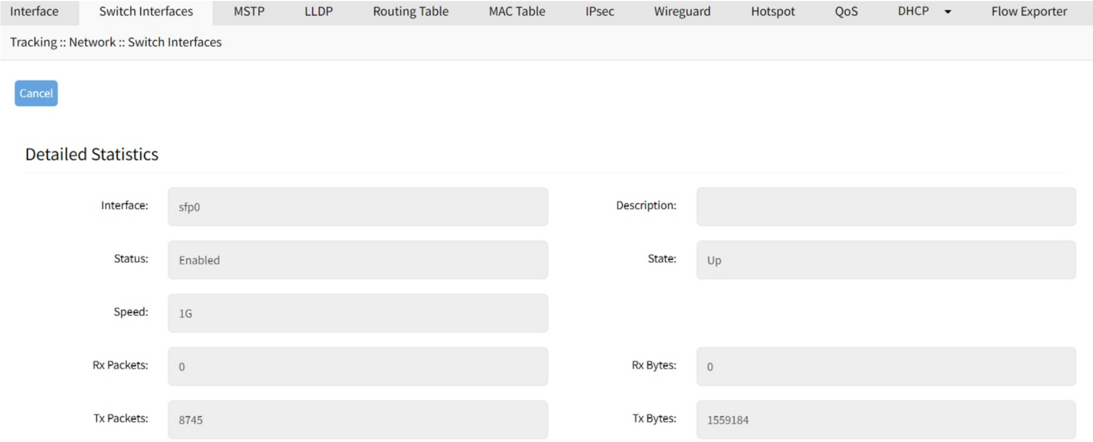
How Users can Benefit from these Detailed Statistics?

Administrators can view the managed switches information to configure and monitor the behavior of switch interfaces and transceiver EEPROM information such as transceiver type, vendor, electrical or optical measurements, part number, and other specifications.

Viewing the Detailed SFP and EEPROM Statistics

To view all the detailed SFP Statistics:

1. Log in to your Nodegrid device.
2. Go to **Tracking** > **Network**> **Switch Interface**. All the available interfaces attached to the device are listed on this page.
3. Click the name of any interface to view the detailed statistics. You can view the following details:
    a. Under **Detailed Statistics** you can view the following information:
        i. **Interface**: The name of the interface.
        ii. **Status**: If the interface is currently enabled or disabled
        iii. **Speed**: The speed at which data is transmitted or received
        iv. **Rx Packets**: Number of packets received.
        v. **Tx Packets**: The number of packets transmitted.
        vi. **State**: The state of the interface, whether it is up and running or not.
        vii. **Rx Bytes**: The number of bytes received.
        viii. **Tx Bytes**: The number of bytes transmitted.
        ix. **Description**: The description provided while adding an interface.



Detailed Statistics

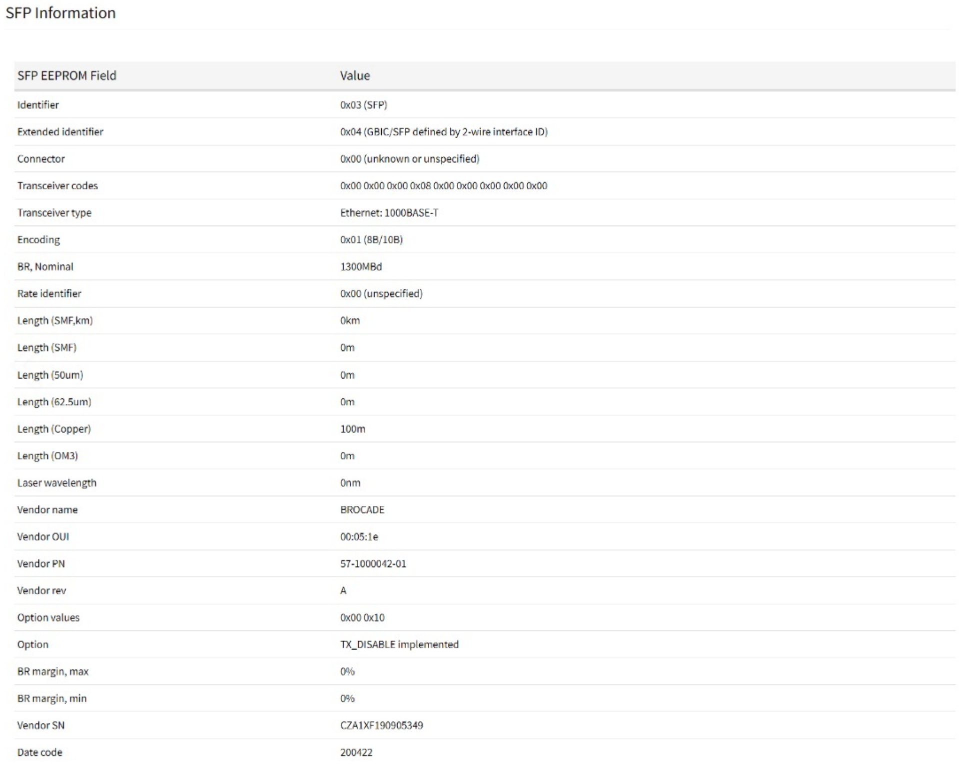
Interface: sfp0
Description:
Status: Enabled
State: Up
Speed: 1G
Rx Packets: 0
Rx Bytes: 0
Tx Packets: 8745
Tx Bytes: 1559184

    b. **SFP Information:** This section is displayed only when there is an EEPROM module connected to the switch.
    For example, if there is a connection issue in a remote site, the Network Administrator can use the transceiver EEPROM data to verify:
        i. If there is a transceiver connected in some interface

ii. The type of transceiver and the vendor

iii. The electrical and optical measurements if supported by the transceiver

The following image displays sample data for an SFP EEPROM module captured in the SFP information section:



SFP Information

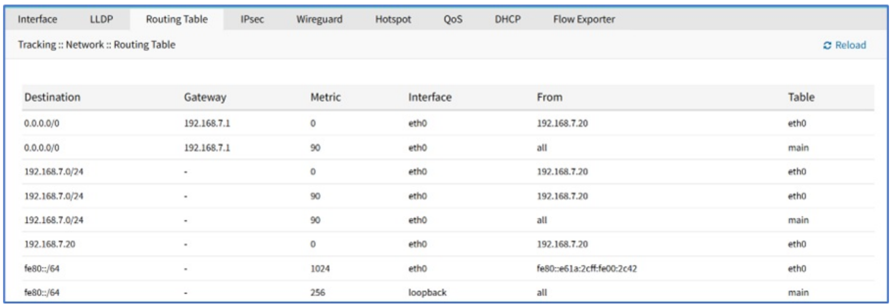
SFP EEPROM Field	Value
Identifier	0x03 (SFP)
Extended identifier	0x04 (GBIC/SFP defined by 2-wire interface ID)
Connector	0x00 (unknown or unspecified)
Transceiver codes	0x00 0x00 0x00 0x08 0x00 0x00 0x00 0x00 0x00
Transceiver type	Ethernet: 1000BASE-T
Encoding	0x01 (8B/10B)
BR, Nominal	1300MBd
Rate identifier	0x00 (unspecified)
Length (SMF,km)	0km
Length (SMF)	0m
Length (50um)	0m
Length (62.5um)	0m
Length (Copper)	100m
Length (OM3)	0m
Laser wavelength	0nm
Vendor name	BROCADE
Vendor OUI	00:05:1e
Vendor PN	57-1000042-01
Vendor rev	A
Option values	0x00 0x10
Option	TX_DISABLE implemented
BR margin, max	0%
BR margin, min	0%
Vendor SN	CZA1XF190905349
Date code	200422

Unauthorize 802.1x Session

1. Go to *Tracking :: Network :: Switch Interfaces*.
2. Select checkbox(es).
3. Click **Unauthorize 802.1x Session**.

Routing Table sub-tab

(read only) This shows the routing rules that Nodegrid follows for network communications. Any added static network routes are included.

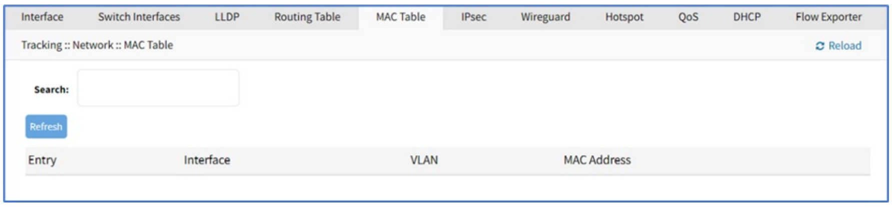


Tracking :: Network :: Routing Table

Destination	Gateway	Metric	Interface	From	Table
0.0.0.0/0	192.168.7.1	0	eth0	192.168.7.20	eth0
0.0.0.0/0	192.168.7.1	90	eth0	all	main
192.168.7.0/24	-	0	eth0	192.168.7.20	eth0
192.168.7.0/24	-	90	eth0	192.168.7.20	eth0
192.168.7.0/24	-	90	eth0	all	main
192.168.7.20	-	0	eth0	192.168.7.20	eth0
fe80::/64	-	1024	eth0	fe80::e61a:2cff:fe00:2c42	eth0
fe80::/64	-	256	loopback	all	main

MAC Table sub-tab (NSR)

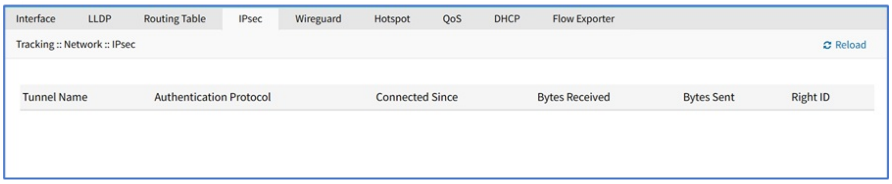
(read only) This displays information in MAC settings.



Entry	Interface	VLAN	MAC Address

IPsec sub-tab

(read only) This displays information for each IPsec tunnel connection.

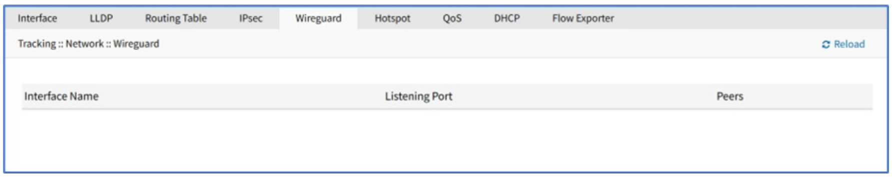


Tunnel Name	Authentication Protocol	Connected Since	Bytes Received	Bytes Sent	Right ID

To appear on the IPsec list, Monitoring must be enabled for each IPsec tunnel.

Wireguard sub-tab

This shows Wireguard connection details.

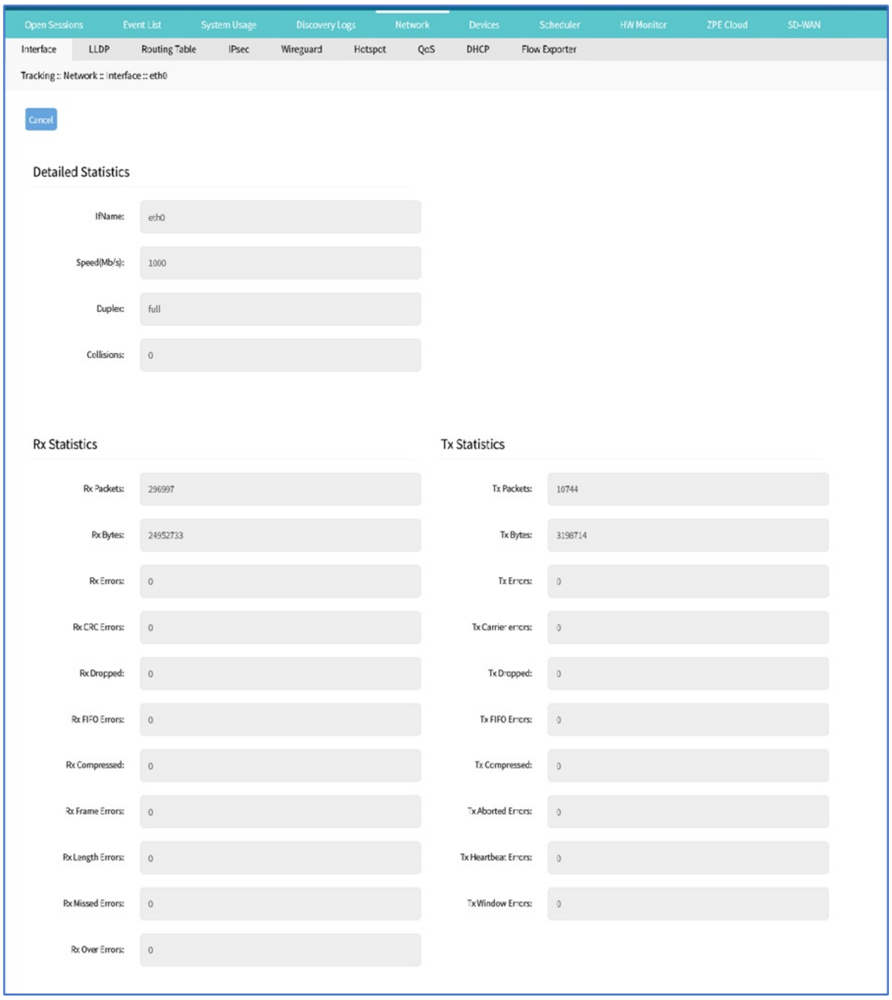


Tracking :: Network :: Wireguard

Interface Name	Listening Port	Peers

View Details on Wireguard Configuration

1. Go to *Tracking :: Network :: Wireguard*.
2. In *Interface Name* column, click on a name (displays dialog of details). Review details.



Tracking :: Network :: Interface :: eth0

Detailed Statistics

IfName: eth0

Speed(Mb/s): 1000

Duplex: full

Collisions: 0

Rx Statistics

Rx Packets: 296997

Rx Bytes: 24952733

Rx Errors: 0

Rx CRC Errors: 0

Rx Dropped: 0

Rx FIFO Errors: 0

Rx Compressed: 0

Rx Frame Errors: 0

Rx Length Errors: 0

Rx Missed Errors: 0

Rx Over Errors: 0

Tx Statistics

Tx Packets: 10744

Tx Bytes: 3198714

Tx Errors: 0

Tx Carrier errors: 0

Tx Dropped: 0

Tx FIFO Errors: 0

Tx Compressed: 0

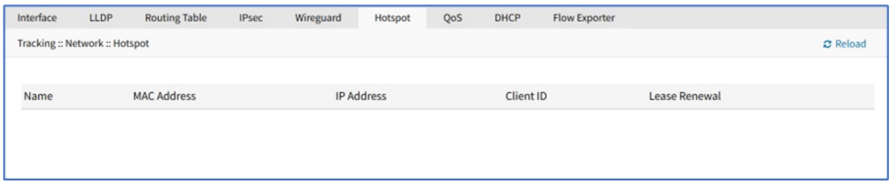
Tx Aborted Errors: 0

Tx Heartbeat Errors: 0

Tx Window Errors: 0

Hotspot sub-tab

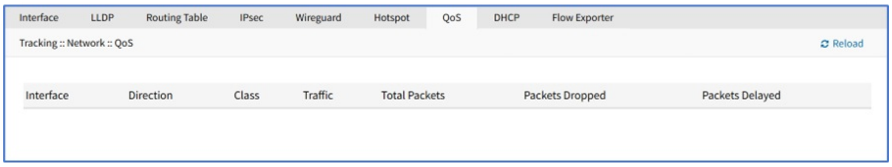
(read-only) This displays all devices currently connected to the hotspot.



Name	MAC Address	IP Address	Client ID	Lease Renewal

QoS sub-tab

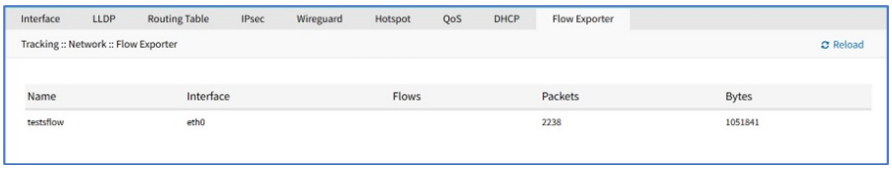
(read only) This displays traffic information from each configured QoS (Quality of Service) class/interface. If the QoS interface is bidirectional, two entries are shown (one for input and one for output).



Interface	Direction	Class	Traffic	Total Packets	Packets Dropped	Packets Delayed

Flow Exporter sub-tab

(read-only) This displays Flow Exporter details.

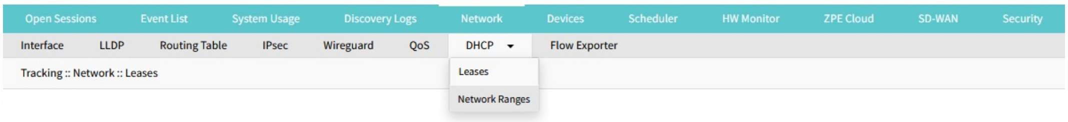


Tracking :: Network :: Flow Exporter

Name	Interface	Flows	Packets	Bytes
testsflow	eth0		2238	1051841

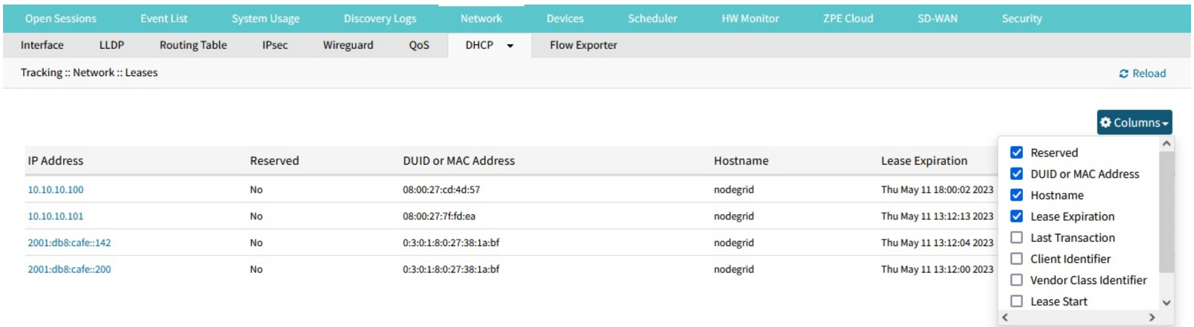
DHCP sub-tab

This tab contains DHCP server tracking information. Since v5.10.0, it is divided into *Leases* and *Network Range* sections.



Leases sub-tab

This sub-tab shows information about all addresses (dynamic and reserved) currently leased by the DHCP server configured on the Nodegrid device. The items displayed in the leases table can be customized by selecting options from the "Columns" button, and the column order can be rearranged by dragging-and-dropping the corresponding items in the "Columns" list. Column preferences are stored in a cookie on the user's browser.



Tracking :: Network :: Leases

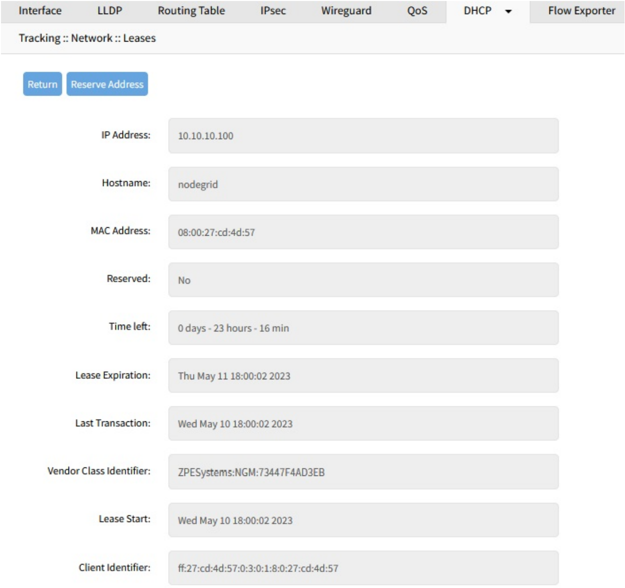
IP Address	Reserved	DUID or MAC Address	Hostname	Lease Expiration
10.10.10.100	No	08:00:27:cd:4d:57	nodegrid	Thu May 11 18:00:02 2023
10.10.10.101	No	08:00:27:7f:fd:ea	nodegrid	Thu May 11 13:12:13 2023
2001:db8:cafe::142	No	0:3:0:1:8:0:27:38:1a:bf	nodegrid	Thu May 11 13:12:04 2023
2001:db8:cafe::200	No	0:3:0:1:8:0:27:38:1a:bf	nodegrid	Thu May 11 13:12:00 2023

☑ Reserved
☑ DUID or MAC Address
☑ Hostname
☑ Lease Expiration
□ Last Transaction
□ Client Identifier
□ Vendor Class Identifier
□ Lease Start

Detailed lease information

Clicking on the IP address of an entry on the table shows for the selected entry all of the values that are potentially shown on the main table, including IP Address, Hostname, MAC Address, Reserved, Time left, Lease Expiration, Last Transaction, Vendor Class Identifier, Lease Start, and Client Identifier. The available details may vary depending on factors such as the lease type (dynamic or reserved) and IP protocol (IPv4 or IPv6).

The *Return* button returns to the main leases table. The *Reserve Address* button is only shown if the lease is dynamic and the current user has *write* permission.



Tracking :: Network :: Leases

IP Address: 10.10.10.100

Hostname: nodegrid

MAC Address: 08:00:27:cd:4d:57

Reserved: No

Time left: 0 days - 23 hours - 16 min

Lease Expiration: Thu May 11 18:00:02 2023

Last Transaction: Wed May 10 18:00:02 2023

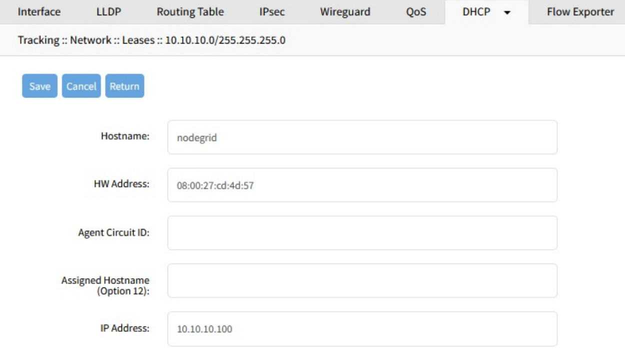
Vendor Class Identifier: ZPESystems:NGM:73447F4AD3EB

Lease Start: Wed May 10 18:00:02 2023

Client Identifier: ff:27:cd:4d:57:0:3:0:1:8:0:27:cd:4d:57

Reserving a dynamic lease

When the *Reserve Address* button is available, clicking it takes the user to a menu similar to *Network :: DHCP Server :: <address> :: Hosts :: Add* (see "Manage DHCP Server" section), with applicable fields pre-populated with the values from the selected dynamic lease. Clicking *Save* turns the dynamic lease into a reserved address for that client.



Tracking :: Network :: Leases :: 10.10.10.0/255.255.255.0

Hostname: nodegrid

HW Address: 08:00:27:cd:4d:57

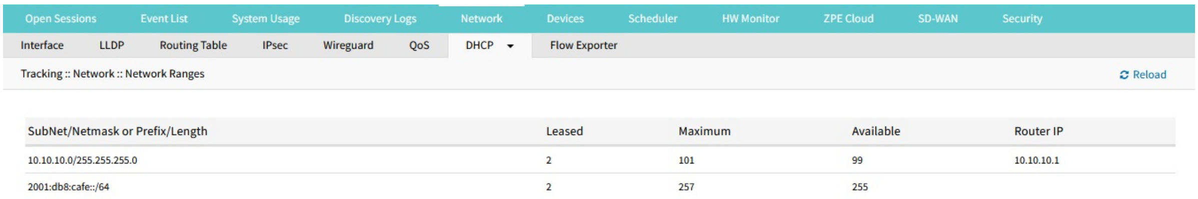
Agent Circuit ID:

Assigned Hostname (Option 12):

IP Address: 10.10.10.100

Network Ranges sub-tab

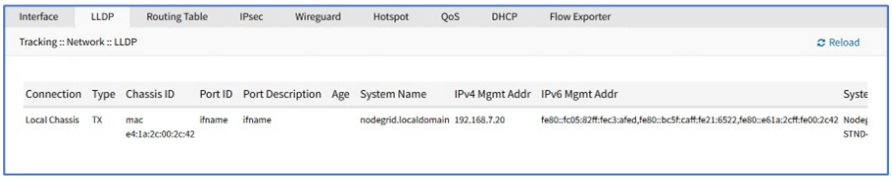
This sub-tab provides an overview of the Network Ranges configured in the Nodegrid DHCP server. For each range, it shows the number of leased IPs, the maximum number of leases possible in that range, the number of leases currently available, and the Router IP. If any number is above 1000, it will show as "1000+".



SubNet/Netmask or Prefix/Length	Leased	Maximum	Available	Router IP
10.10.10.0/255.255.255.0	2	101	99	10.10.10.1
2001:db8:cafe::/64	2	257	255	

LLDP sub-tab

(read only) This shows devices that advertise their identity and capabilities on the LAN. LLDP advertising and reception can be enabled in Nodegrid with network connections.



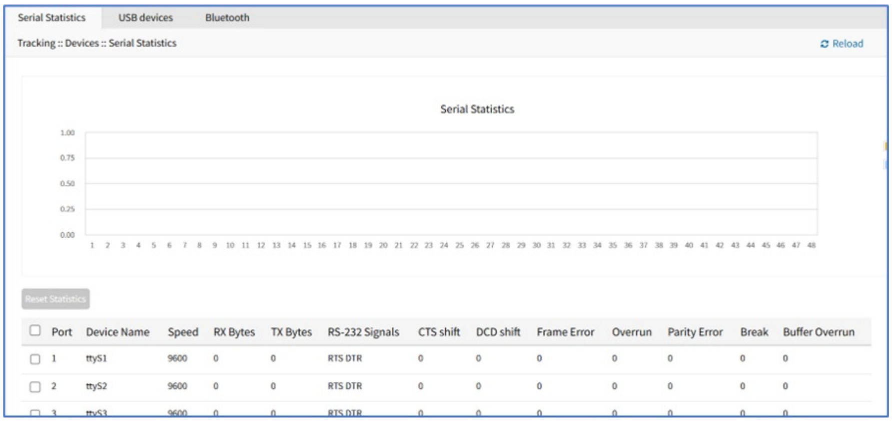
Connection	Type	Chassis ID	Port ID	Port Description	Age	System Name	IPv4 Mgmt Addr	IPv6 Mgmt Addr	Syste
Local Chassis	TX	mac e4:1a:2c:00:2c:42	ifname	ifname		nodegrid.localdomain	192.168.7.20	fe80::fc05:82ff:fec3:afed,fe80::bc5f:caff:fe21:6522,fe80::e61a:2cff:fe00:2c42	Nodeg STND-

Devices tab

This shows connection statistics for physically connected devices, like serial and USB devices, and wireless modems. The available options will depend on the specific Nodegrid unit.

Serial Statistics sub-tab

This provides statistical information on the serial ports connectivity such as transmitted and received data, RS232 signals, errors.



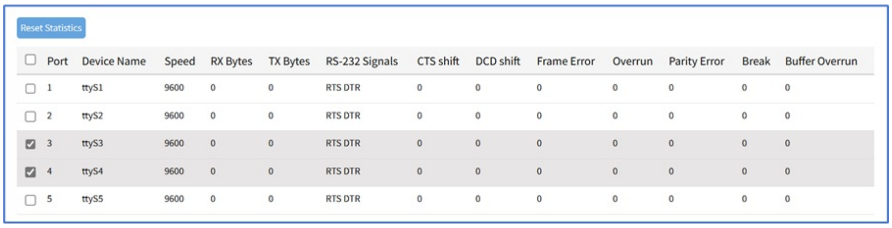
□	Port	Device Name	Speed	RX Bytes	TX Bytes	RS-232 Signals	CTS shift	DCD shift	Frame Error	Overrun	Parity Error	Break	Buffer Overrun
□	1	ttyS1	9600	0	0	RTS DTR	0	0	0	0	0	0	0
□	2	ttyS2	9600	0	0	RTS DTR	0	0	0	0	0	0	0
□	3	ttyS3	9600	0	0	RTS DTR	0	0	0	0	0	0	0

NOTE

This sub-tab is not available on Nodegrid VM.

Reset Statistics

1. Go to *Tracking :: Devices :: Serial Statistics*.
2. Select checkboxes next to Port numbers.

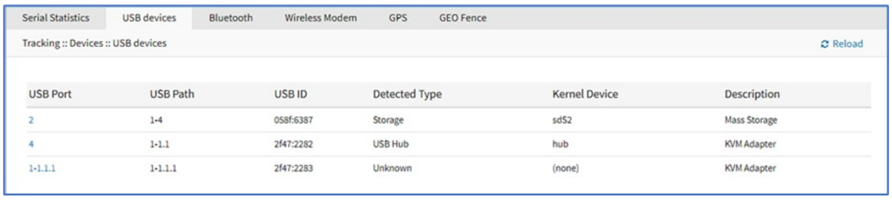


□	Port	Device Name	Speed	RX Bytes	TX Bytes	RS-232 Signals	CTS shift	DCD shift	Frame Error	Overrun	Parity Error	Break	Buffer Overrun
□	1	ttyS1	9600	0	0	RTS DTR	0	0	0	0	0	0	0
□	2	ttyS2	9600	0	0	RTS DTR	0	0	0	0	0	0	0
☑	3	ttyS3	9600	0	0	RTS DTR	0	0	0	0	0	0	0
☑	4	ttyS4	9600	0	0	RTS DTR	0	0	0	0	0	0	0
□	5	ttyS5	9600	0	0	RTS DTR	0	0	0	0	0	0	0

3. Click **Reset Statistics**.

USB devices sub-tab

This provides details about connected USB devices and initialized drivers.



Tracking :: Devices :: USB devices

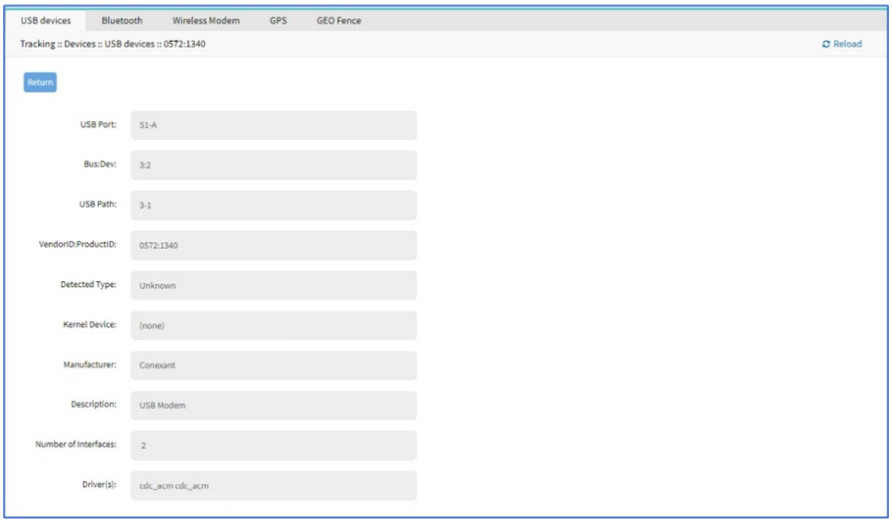
USB Port	USB Path	USB ID	Detected Type	Kernel Device	Description
2	1-4	058f:6387	Storage	sd$2	Mass Storage
4	1-1.1	2f47:2282	USB Hub	hub	KVM Adapter
1-1.1.1	1-1.1.1	2f47:2283	Unknown	(none)	KVM Adapter

NOTE

This sub-tab will only display if a USB adopter is linked to the device.

View USB Device Details

1. Go to *Tracking :: Devices :: USB devices*.
2. In *USB Port* column, click on a USB port (displays dialog).



Tracking :: Devices :: USB devices :: 0572:1340

USB Port: S1-A

Bus:Dev: 3:2

USB Path: 3-1

VendorID:ProductID: 0572:1340

Detected Type: Unknown

Kernel Device: (none)

Manufacturer: Conexant

Description: USB Modem

Number of Interfaces: 2

Driver(s): cdc_acm cdc_acm

3. Review details.
4. Click **Return** to go back.

Convert M2 Analog Modem to USB Serial Device

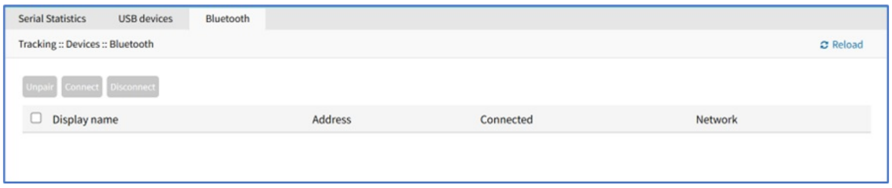
1. Go to *Tracking :: Devices :: USB devices*.
2. In *USB Port* column, click on name of a M.2 Analog Modem.
3. On the dialog, click **Set as Serial Device**.
4. Click **Save**.

Convert USB Analog Modem to USB Serial Device

1. Go to *Tracking :: Devices :: USB devices*.
2. In *USB Port* column, click on name of a USB Analog Modem (displays dialog).
3. On the dialog, click **Set as Serial Device**.
4. Click **Save**.

Bluetooth sub-tab

This displays information about Bluetooth devices.



> **NOTE**
>
> This sub-tab will only display if the device supports Bluetooth, and a Bluetooth device is connected.

Unpair Bluetooth

This removes the pairing relationship between a Bluetooth device and the Nodegrid device, such that they won't automatically connect to each other. This makes the Nodegrid device "forget" a previously paired Bluetooth device.

1. Go to *Tracking :: Devices :: Bluetooth*.
2. Select checkbox.
3. Click **Unpair**.

Connect Bluetooth

This activates the connection between a paired Bluetooth device and Nodegrid device.

1. Go to *Tracking :: Devices :: Bluetooth*.
2. Select checkbox.
3. Click **Connect**.

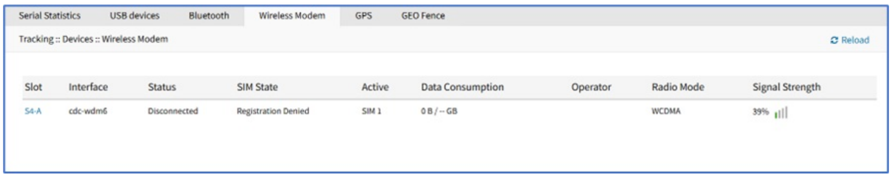
Disconnect Bluetooth

This deactivates the connection between a paired Bluetooth device and Nodegrid device.

1. Go to *Tracking :: Devices :: Bluetooth*.
2. Select checkbox.
3. Click **Disconnect**.

Wireless Modem sub-tab

This displays information about the wireless modem when installed.



Tracking :: Devices :: Wireless Modem

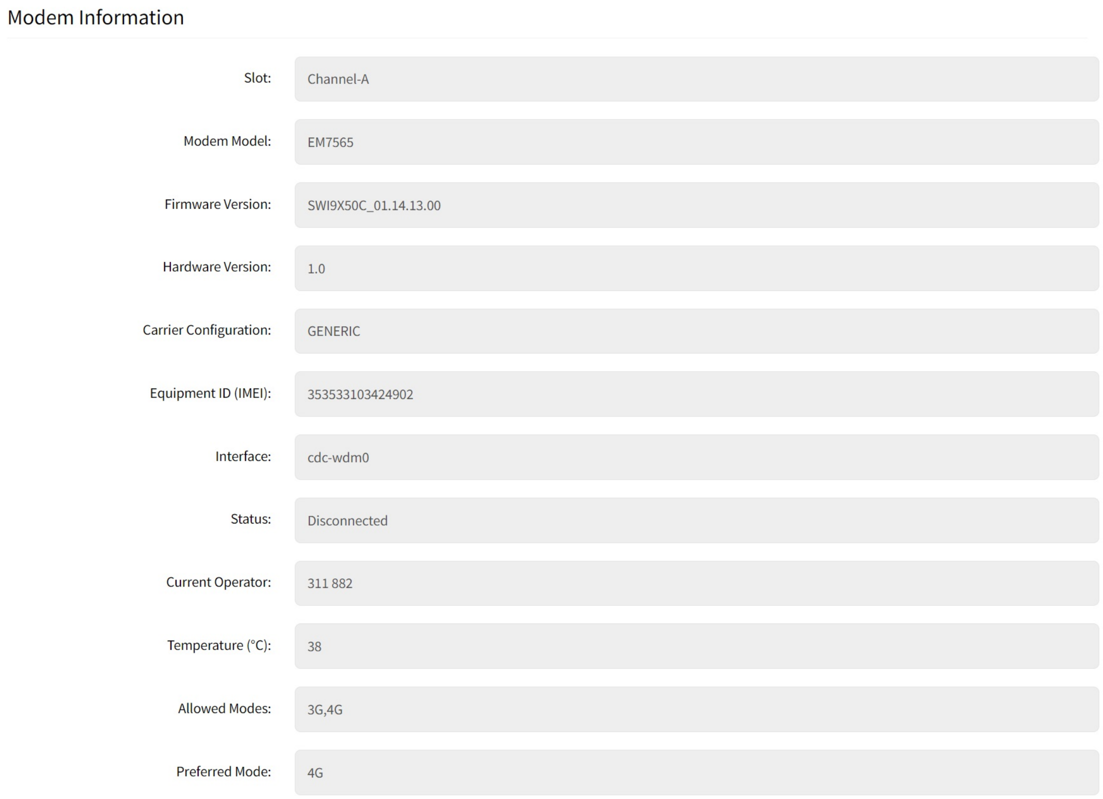
Slot	Interface	Status	SIM State	Active	Data Consumption	Operator	Radio Mode	Signal Strength
S4-A	cdc-wdm6	Disconnected	Registration Denied	SIM 1	0 B / -- GB		WCDMA	39%

NOTE

This sub-tab only displays if the Nodegrid device supports wireless.

View Wireless Modem Details

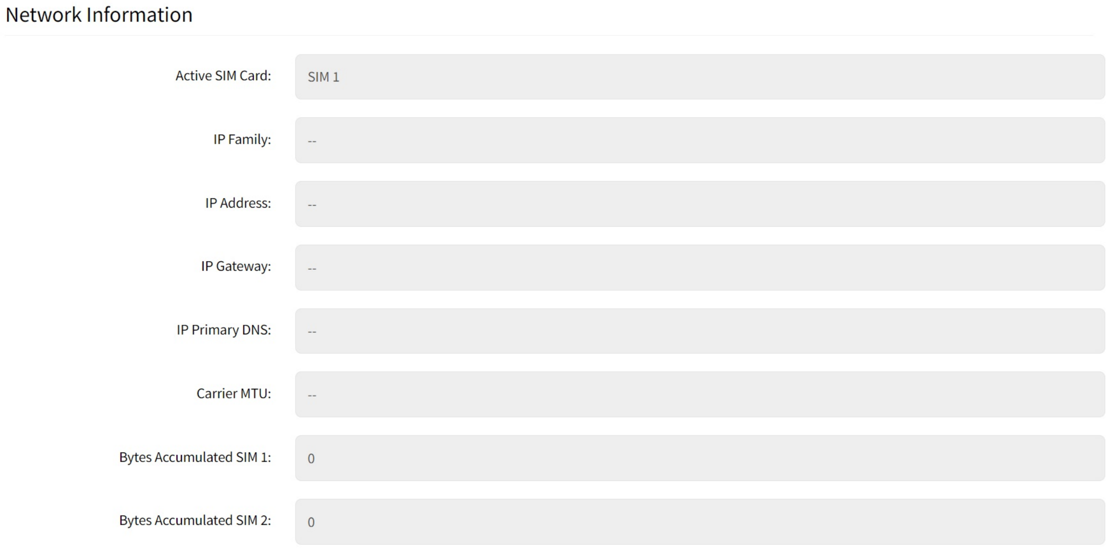
1. Go to *Tracking :: Devices :: Wireless Modem*.
2. In the *Slot* column, click on the name (displays dialog).
3. Review details.
   a. Modem Information:



Modem Information

Slot:	Channel-A
Modem Model:	EM7565
Firmware Version:	SWI9X50C_01.14.13.00
Hardware Version:	1.0
Carrier Configuration:	GENERIC
Equipment ID (IMEI):	353533103424902
Interface:	cdc-wdm0
Status:	Disconnected
Current Operator:	311 882
Temperature (°C):	38
Allowed Modes:	3G,4G
Preferred Mode:	4G

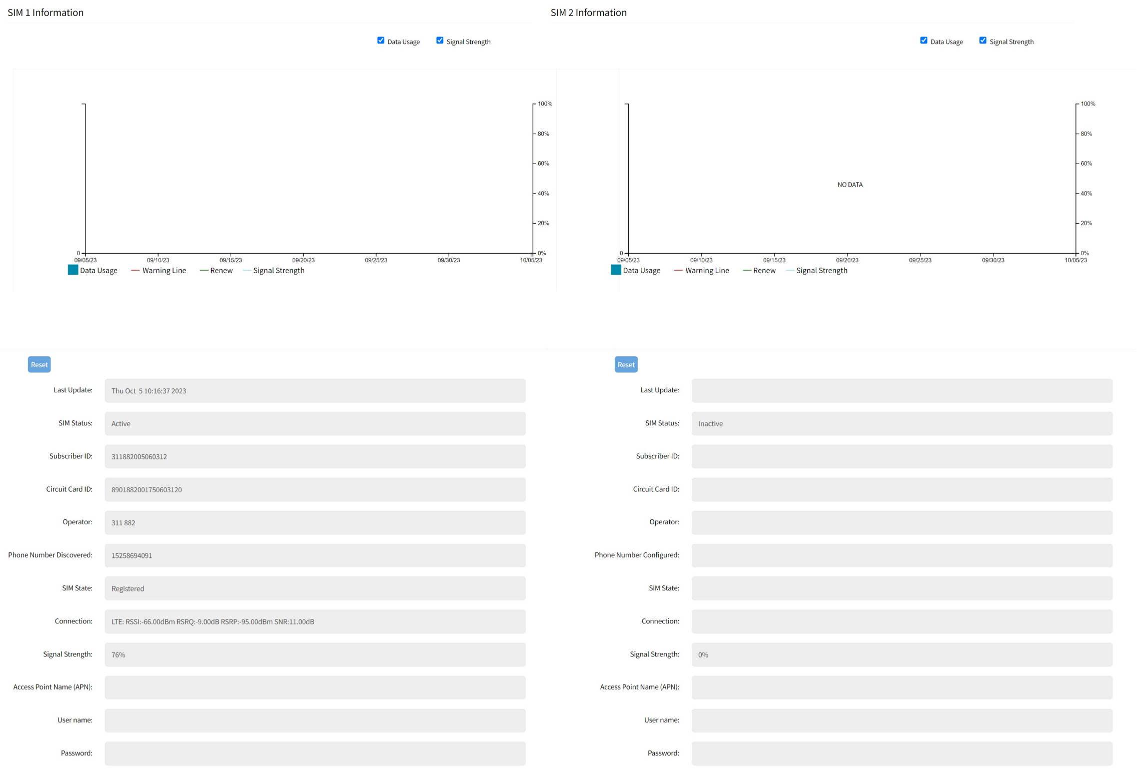
   b. Network Information:



Network Information

Active SIM Card:	SIM 1
IP Family:	--
IP Address:	--
IP Gateway:	--
IP Primary DNS:	--
Carrier MTU:	--
Bytes Accumulated SIM 1:	0
Bytes Accumulated SIM 2:	0

c. Sim Information:



Last Update:	Thu Oct 5 10:16:37 2023
SIM Status:	Active
Subscriber ID:	311882005060312
Circuit Card ID:	8901882001750603120
Operator:	311 882
Phone Number Discovered:	15258694091
SIM State:	Registered
Connection:	LTE: RSSI:-66.00dBm RSRQ:-9.00dB RSRP:-95.00dBm SNR:11.00dB
Signal Strength:	76%
Access Point Name (APN):	
User name:	
Password:	

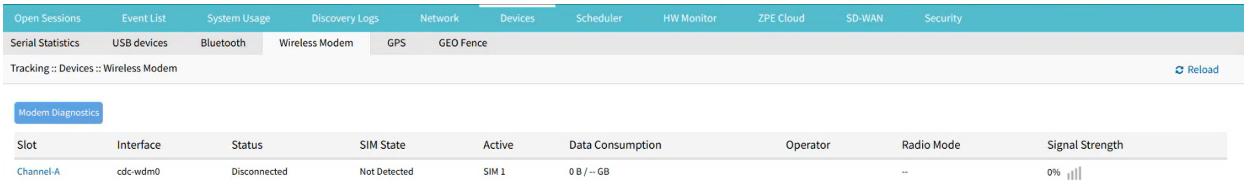
Last Update:	
SIM Status:	Inactive
Subscriber ID:	
Circuit Card ID:	
Operator:	
Phone Number Configured:	
SIM State:	
Connection:	
Signal Strength:	0%
Access Point Name (APN):	
User name:	
Password:	

02

4. Click **Return** to go back.

Diagnosing Modem

When you click the **Modem Diagnosis** option, you can view the **Modem** and **SIM diagnostics** summary.

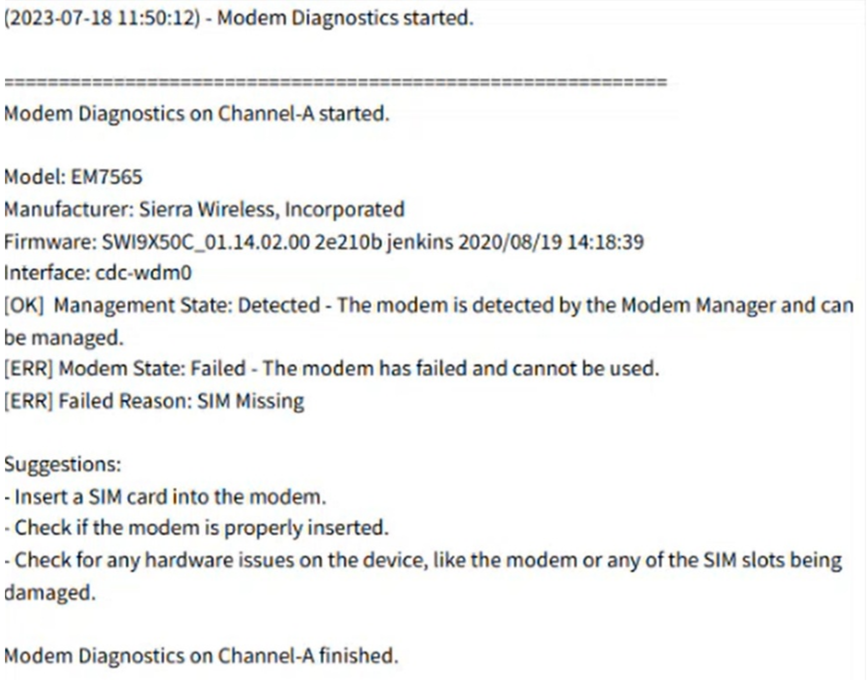


Slot	Interface	Status	SIM State	Active	Data Consumption	Operator	Radio Mode	Signal Strength
Channel-A	cdc-wdm0	Disconnected	Not Detected	SIM 1	0 B / -- GB		--	0%

To view the summary:

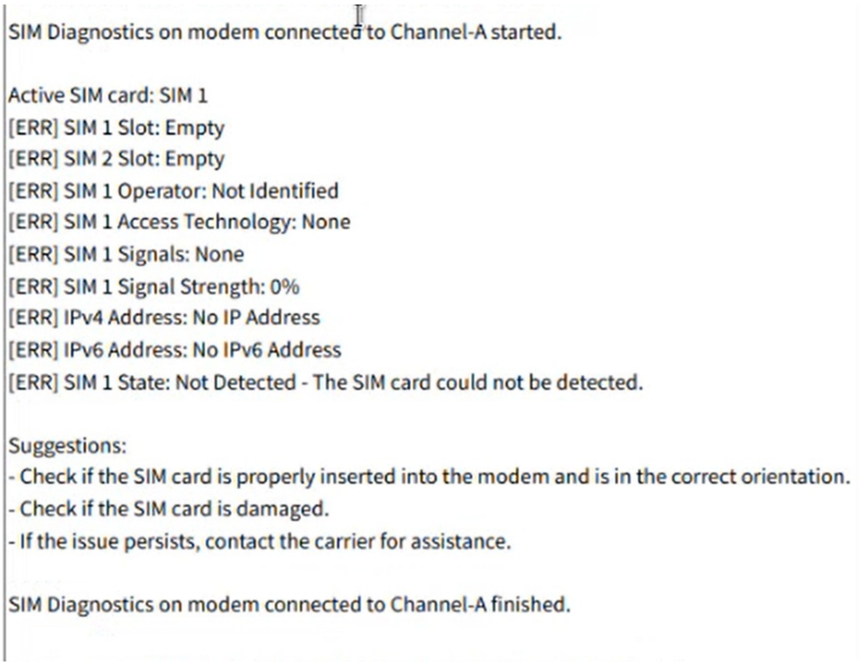
1. Click **Modem Diagnostics**.
2. In the **Run Diagnostics** section, select:
   a. **All Interfaces**: To select all the interfaces
   b. **Specific Interface**: To choose a specific interface from the **Interface** drop-down list.

3. Click **Run.** The diagnosis summary is populated in the **Modem Diagnostics** section:
   a. Modem Diagnostics: you can view the modem details and the error due to which the wireless modem connection has failed.



```
(2023-07-18 11:50:12) - Modem Diagnostics started.

============================================================
Modem Diagnostics on Channel-A started.

Model: EM7565
Manufacturer: Sierra Wireless, Incorporated
Firmware: SWI9X50C_01.14.02.00 2e210b jenkins 2020/08/19 14:18:39
Interface: cdc-wdm0
[OK]  Management State: Detected - The modem is detected by the Modem Manager and can
be managed.
[ERR] Modem State: Failed - The modem has failed and cannot be used.
[ERR] Failed Reason: SIM Missing

Suggestions:
- Insert a SIM card into the modem.
- Check if the modem is properly inserted.
- Check for any hardware issues on the device, like the modem or any of the SIM slots being
damaged.

Modem Diagnostics on Channel-A finished.
```

   b. SIM Diagnostics: Any errors encountered due to SIM cards are listed in this section as shown in the following section.



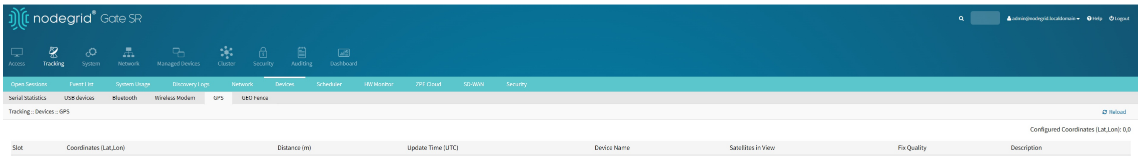
```
SIM Diagnostics on modem connected to Channel-A started.

Active SIM card: SIM 1
[ERR] SIM 1 Slot: Empty
[ERR] SIM 2 Slot: Empty
[ERR] SIM 1 Operator: Not Identified
[ERR] SIM 1 Access Technology: None
[ERR] SIM 1 Signals: None
[ERR] SIM 1 Signal Strength: 0%
[ERR] IPv4 Address: No IP Address
[ERR] IPv6 Address: No IPv6 Address
[ERR] SIM 1 State: Not Detected - The SIM card could not be detected.

Suggestions:
- Check if the SIM card is properly inserted into the modem and is in the correct orientation.
- Check if the SIM card is damaged.
- If the issue persists, contact the carrier for assistance.

SIM Diagnostics on modem connected to Channel-A finished.
```

4. Download: This allows you to download the summary.

GPS sub-tab

This provides information about GPS details. All the GPS devices are listed on this page. You can view the following information related to the GPS devices:

- **Slots**: Lists the channels associated with the GPS
- **Coordinates**: The distance between GPS coordinates and configured one
- **Distance**: Time taken by the signal to arrive at its location from the satellites
- **Update time (UTC)**: The last updated time in UTC
- **Device Name**: Name of the device connected to the GPS
- **Satellites in View**: Indicates the number of satellites the GPS modem is communicating with at that time
- **Fix Quality**: A message that comes from GPGGA, and indicates the type of signal or technique being used by the GPS receiver to determine its location
- **Description**: Informs the user about the current status. Displays **OK** if everything is fine, or displays the reason if something is wrong. You can view one of the following messages:
    - At least 3 satellites need to get the GPS Fix
    - Could not enable GPS protocols
    - Failed to get GPS NMEA information
    - GPS location information is not available
    - Trying to get the GPS Fix



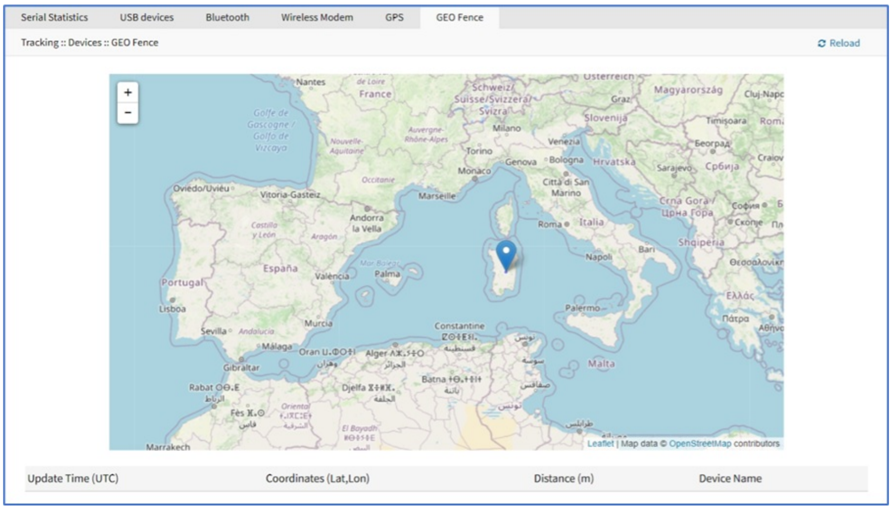
Tracking :: Devices :: GPS

Configured Coordinates (Lat,Lon): 0,0

Slot	Coordinates (Lat,Lon)	Distance (m)	Update Time (UTC)	Device Name	Satellites in View	Fix Quality	Description

GEO Fence sub-tab

(if enabled) This displays a map of GEO Fence locations. View can be zoomed in or out.

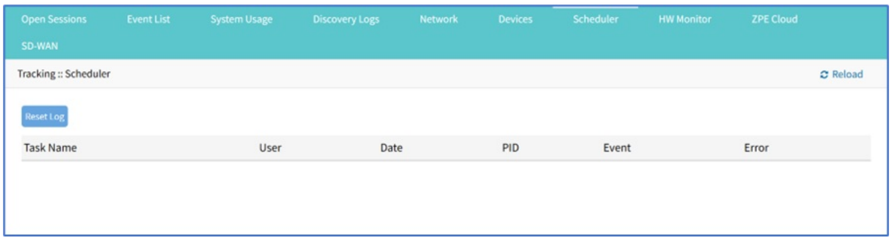


Tracking :: Devices :: GEO Fence

Update Time (UTC)	Coordinates (Lat,Lon)	Distance (m)	Device Name

Scheduler tab

This provides information about scheduled tasks.



Task Name	User	Date	PID	Event	Error

Reset Log

1. Go to *Tracking :: Scheduler*.
2. Select checkbox(es) to reset.
3. Click **Reset**.

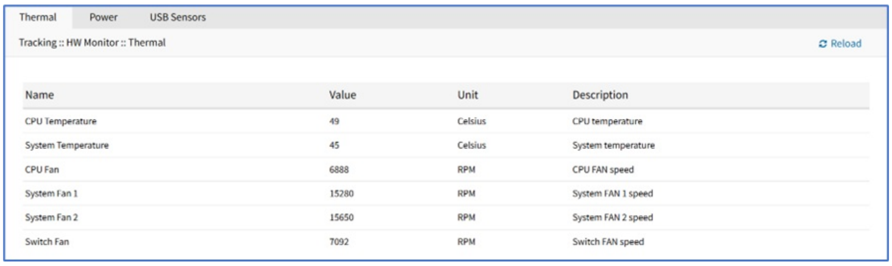
HW Monitor tab

(ready only) This displays Nodegrid system hardware information.

Thermal sub-tab

Go to *Tracking :: HW Monitor :: Thermal*.

This displays the current CPU temperature, System temperature, and FAN speeds (if available).

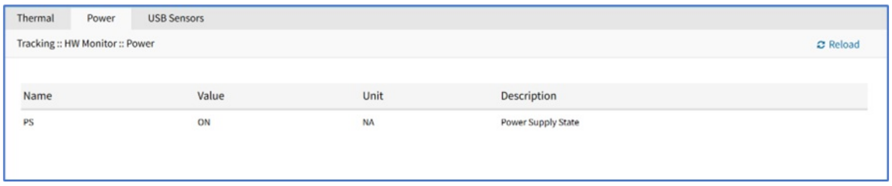


Name	Value	Unit	Description
CPU Temperature	49	Celsius	CPU temperature
System Temperature	45	Celsius	System temperature
CPU Fan	6888	RPM	CPU FAN speed
System Fan 1	15280	RPM	System FAN 1 speed
System Fan 2	15650	RPM	System FAN 2 speed
Switch Fan	7092	RPM	Switch FAN speed

Power sub-tab

Go to *Tracking :: HW Monitor :: Power*.

This displays information about current Power sources (current state and power consumption).



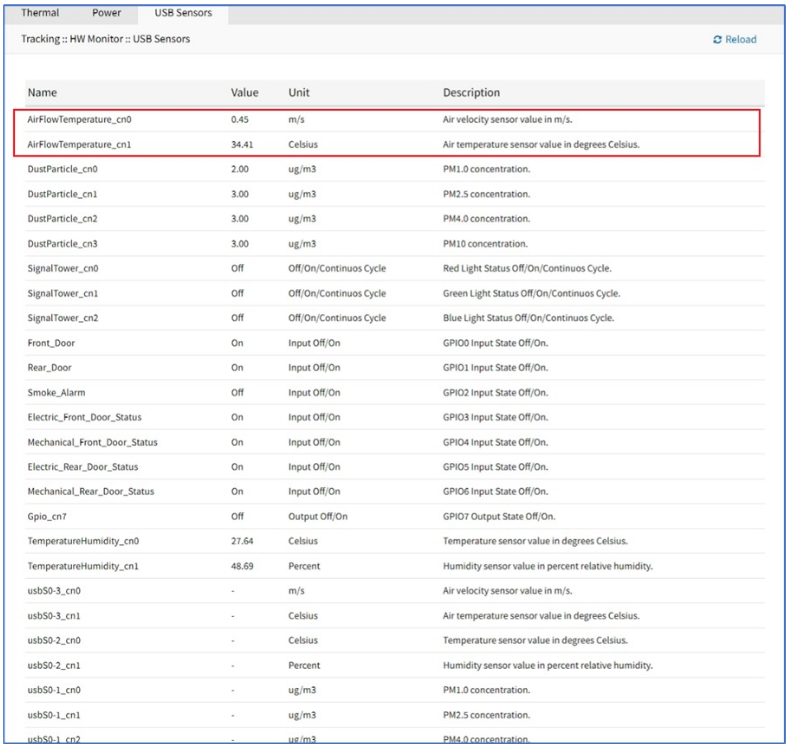
Name	Value	Unit	Description
PS	ON	NA	Power Supply State

USB Sensors sub-tab

Introduction

Go to *Tracking :: HW Monitor :: USB Sensors*.

The details shown depend on the Nodegrid device.



Tracking :: HW Monitor :: USB Sensors

Name	Value	Unit	Description
AirFlowTemperature_cn0	0.45	m/s	Air velocity sensor value in m/s.
AirFlowTemperature_cn1	34.41	Celsius	Air temperature sensor value in degrees Celsius.
DustParticle_cn0	2.00	ug/m3	PM1.0 concentration.
DustParticle_cn1	3.00	ug/m3	PM2.5 concentration.
DustParticle_cn2	3.00	ug/m3	PM4.0 concentration.
DustParticle_cn3	3.00	ug/m3	PM10 concentration.
SignalTower_cn0	Off	Off/On/Continuos Cycle	Red Light Status Off/On/Continuos Cycle.
SignalTower_cn1	Off	Off/On/Continuos Cycle	Green Light Status Off/On/Continuos Cycle.
SignalTower_cn2	Off	Off/On/Continuos Cycle	Blue Light Status Off/On/Continuos Cycle.
Front_Door	On	Input Off/On	GPIO0 Input State Off/On.
Rear_Door	On	Input Off/On	GPIO1 Input State Off/On.
Smoke_Alarm	Off	Input Off/On	GPIO2 Input State Off/On.
Electric_Front_Door_Status	On	Input Off/On	GPIO3 Input State Off/On.
Mechanical_Front_Door_Status	On	Input Off/On	GPIO4 Input State Off/On.
Electric_Rear_Door_Status	On	Input Off/On	GPIO5 Input State Off/On.
Mechanical_Rear_Door_Status	On	Input Off/On	GPIO6 Input State Off/On.
Gpio_cn7	Off	Output Off/On	GPIO7 Output State Off/On.
TemperatureHumidity_cn0	27.64	Celsius	Temperature sensor value in degrees Celsius.
TemperatureHumidity_cn1	48.69	Percent	Humidity sensor value in percent relative humidity.
usbS0-3_cn0	-	m/s	Air velocity sensor value in m/s.
usbS0-3_cn1	-	Celsius	Air temperature sensor value in degrees Celsius.
usbS0-2_cn0	-	Celsius	Temperature sensor value in degrees Celsius.
usbS0-2_cn1	-	Percent	Humidity sensor value in percent relative humidity.
usbS0-1_cn0	-	ug/m3	PM1.0 concentration.
usbS0-1_cn1	-	ug/m3	PM2.5 concentration.
usbS0-1_cn2	-	ug/m3	PM4.0 concentration.

Nodegrid USB Temperature and Humidity Sensors are automatically discovered by the System (usb_sensor). After detection, it must be enabled to use with monitoring and alarm management.

Click a sensor to open a detail page. A click on the **Sensor Status** button displays more details and specifics.

ZPE USB Environmental Sensors and Actuators

ZPE USB Device	Description
THS-U01	Temperature and Humidity USB sensor, cable 2m (6.5ft)
AIR-U01	Air Flow and Temperature USB sensor, 0.15 to 1.0 m/s [30 to 200 fpm], cable 4m (13ft)
AIR-U02	Air Flow and Temperature USB sensor, 0.5 to 10.0 m/s [100 to 2,000 fpm], cable 4m (13ft)
DOOR-01	Proximity sensor, cable 4m (13ft) - Requires IO8-U01
RL4-U01	4-port Relay via USB, cable 3m (10ft)
IO8-U01	8-port GPIO via USB, cable 3m (10ft)
BCON-U01	Beacon with alarm USB, black base, blue light, cable 3m (10ft)
BCON-U05	Beacon, no alarm USB, black base, clear light, cable 5m (16ft)
SMK-U01	Smoke detector, cable 3m (10ft) - Requires IO8-U01 and RL4-U01

Supported USB Sensors

USB Device	Vendor
USB Serial	FTDI, CP2105, CP210X
USB KVM	ZPE KVM-U01 - KVM over USB dongle (VGA, USB kb, USB mouse)
USB Sensor	ZPE Environmental: THS-U01 - temperature & humidity, Degree Controls F200 - Air Velocity Sensor (paired with TLL-232R-3V3 or TTL-232R-5V converter cable)
USB Analog Modem	Zoom, US Robotics
USB Cellular Modem	USB620L, USB730L
USB 1G Ethernet	Any USB 3.0 Gigabit Ethernet adapter
USB SFP Ethernet	Winyao USB1000F USB 3.0 Gigabit Fiber adapter
USB WiFi	Wireless Network adapter for Linux (TP-Link TL-WN722N)
USB Storage	Any USB flash drive

These devices utilize Linux drivers supported by the System. Certain driver versions may not work as expected. If any issues occur, contact support@zpesystems.com.

Supported USB I/O Devices

USB I/O Device	Description	GPIO Input	Analog Input
Numato GP80001E	GPIO Module	8-On/Off	6-Any
Numato USBPOWRL001	Relay Module	No	4-Any
Delcom USB HID 9040XX	Light Tower	No	No
Patlite LR6-USB-W/K	Light Tower	No	No
TRH-320	Humidity and temperature sensors	No	1 Humidity - % 1 Temperature - ºC
Degree Controls F200	Air temperature and velocity sensors	No	1 Air Temperature - ºC 1 Air Velocity - m/s
Homologated Generic USB I/O Device	All in one	100-On/Off	100 generic - any

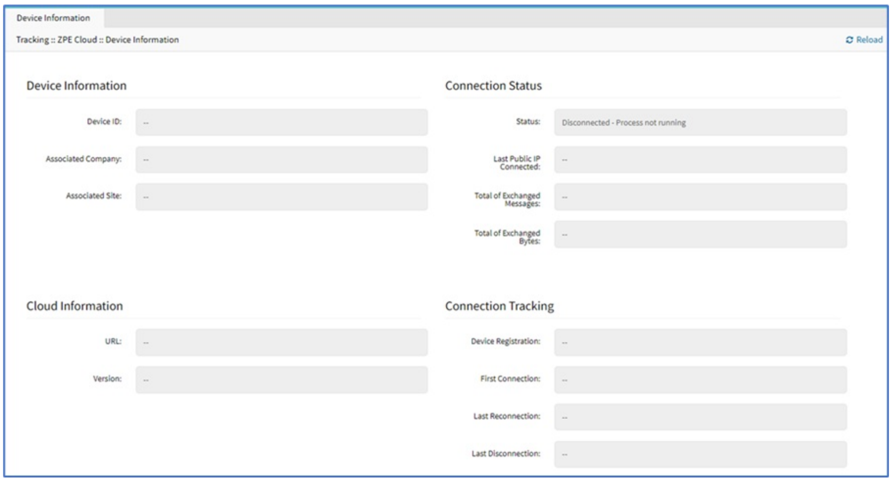
Additional Supported USB Devices

USB i/O Device	GPIO output	Relay	Light	Buzzer
Numato GP80001E	UP TO 8 – On, Off	No	No	No
Numato USBPOWRL001	UP TO 4 – On, Off	2 – On, Off	No	No
Delcom USB HID 9040XX	No	No	3 – On, Off, continuous cycle	1 – On, Off, continuous cycle
Patlite LR6-USB-W/K	No	No	1 – On, Off, continuous cycle	1 – On, Off, continuous cycle
TRH-320	No	No	No	No
Degree Controls F200	No	No	No	No
Homologated Generic USB I/O Device	100 – On, Off	100 – On, Off	100 – On, Off, continuous cycle	100 – On, Off, continuous cycle
Numato GP80001E	UP TO 8 – On, Off	No	No	No
Numato USBPOWRL001	UP TO 4 – On, Off	2 – On, Off	No	No

I/O Ports (GPIO) sub-tab (Gate SR/Link SR only)

This shows the status of GPIO ports (only displayed for models with GPIO ports.

Example – Nodegrid Gate SR WebUI



Device Information

Device ID: --

Associated Company: --

Associated Site: --

Connection Status

Status: Disconnected - Process not running

Last Public IP Connected: --

Total of Exchanged Messages: --

Total of Exchanged Bytes: --

Cloud Information

URL: --

Version: --

Connection Tracking

Device Registration: --

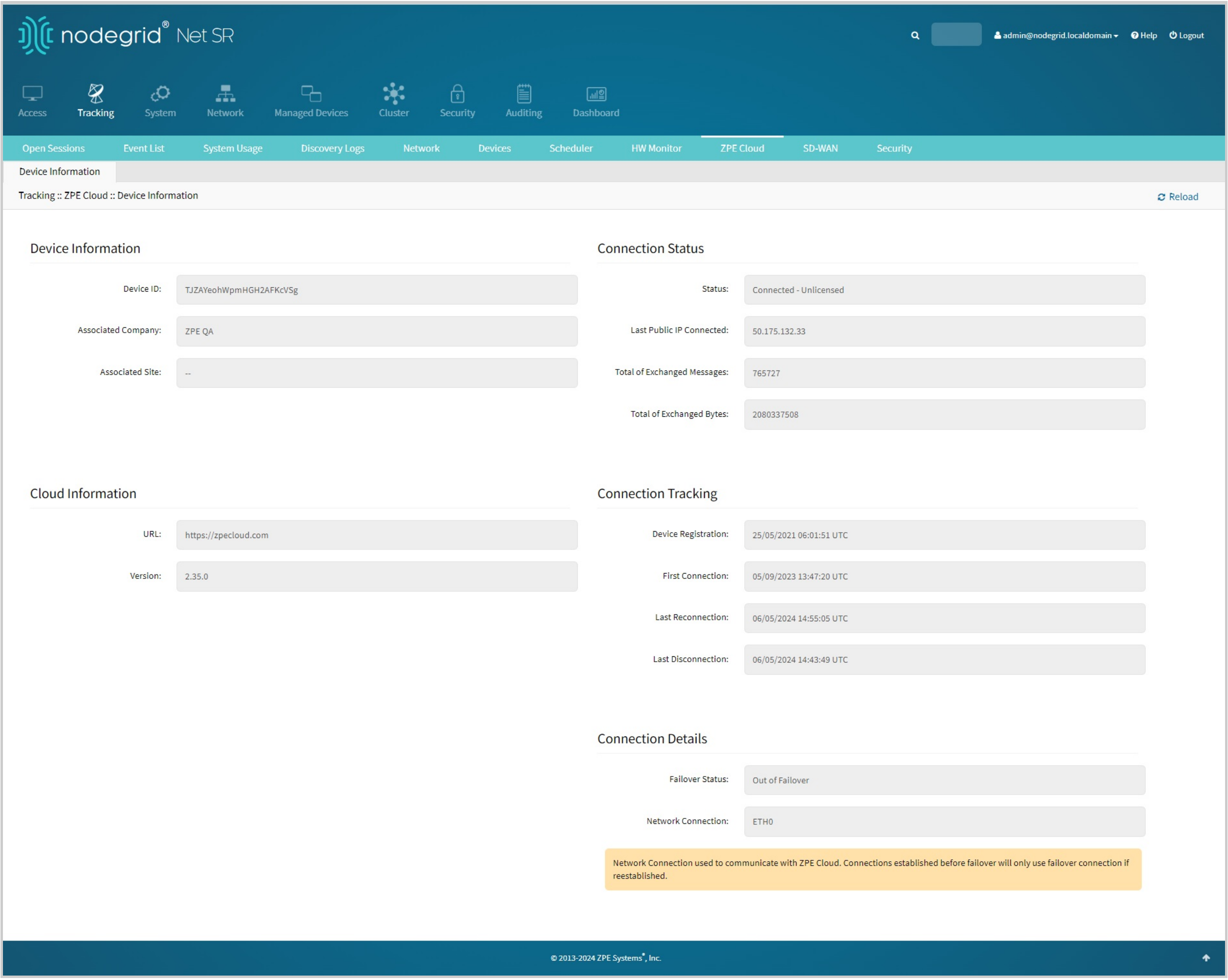
First Connection: --

Last Reconnection: --

Last Disconnection: --

ZPE Cloud Tab

(read-only) This shows configured connections with the ZPE Cloud application.



Tracking :: ZPE Cloud :: Device Information

Device Information

Device ID: TJZAYeohWpmHGH2AFKcVSg

Associated Company: ZPE QA

Associated Site: --

Cloud Information

URL: https://zpecloud.com

Version: 2.35.0

Connection Status

Status: Connected - Unlicensed

Last Public IP Connected: 50.175.132.33

Total of Exchanged Messages: 765727

Total of Exchanged Bytes: 2080337508

Connection Tracking

Device Registration: 25/05/2021 06:01:51 UTC

First Connection: 05/09/2023 13:47:20 UTC

Last Reconnection: 06/05/2024 14:55:05 UTC

Last Disconnection: 06/05/2024 14:43:49 UTC

Connection Details

Failover Status: Out of Failover

Network Connection: ETH0

Network Connection used to communicate with ZPE Cloud. Connections established before failover will only use failover connection if reestablished.

SD-WAN tab

This shows configured underlay and overlay paths of SD-WAN tunnels.

Path status conditions are:

- **Normal** (no issue related to SD-WAN)
- **Warning** (SLA metrics are violated)
- **Error** (path is down)

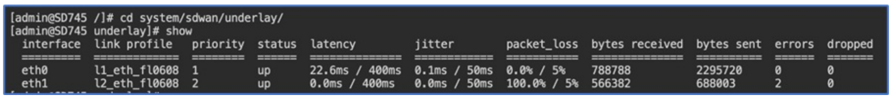
This only displays path information if SD-WAN is enabled. To verify, go to *Network :: SD-WAN :: Settings* and ensure **Enable SD-WAN** checkbox is selected. If disabled, warning message states:
SD-WAN must be enabled.

If topology is not yet configured inside the device, the following message displays:
No information to be displayed.

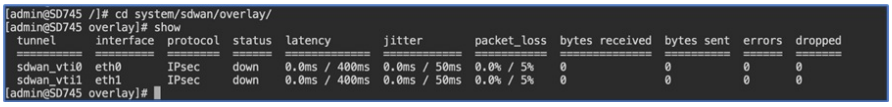
> **NOTE:**
>
> This message is also displayed on overlay tab from Hub device. SD-WAN does not measure overlay paths inside Hub.

If there is an error communicating with the SD-WAN daemon, the following message displays:
Failed to communicate with SD-WAN daemon. Please reload.

On the CLI, go to /system/sdwan/ directory and use show command to display details.



```
[admin@SD745 /]# cd system/sdwan/underlay/
[admin@SD745 underlay]# show
  interface  link profile   priority  status  latency          jitter         packet_loss  bytes received  bytes sent  errors  dropped
  =========  =============  ========  ======  ===============  =============  ===========  ==============  ==========  ======  =======
  eth0       l1_eth_fl0608  1         up      22.6ms / 400ms   0.1ms / 50ms   0.0% / 5%    788788          2295720     0       0
  eth1       l2_eth_fl0608  2         up      0.0ms / 400ms    0.0ms / 50ms   100.0% / 5%  566382          688003      2       0
```

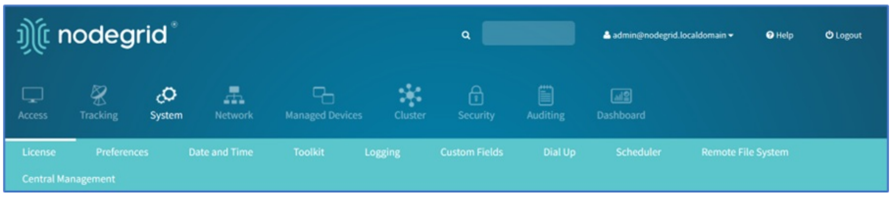


```
[admin@SD745 /]# cd system/sdwan/overlay/
[admin@SD745 overlay]# show
  tunnel      interface  protocol  status  latency         jitter        packet_loss  bytes received  bytes sent  errors  dropped
  ==========  =========  ========  ======  ==============  ============  ===========  ==============  ==========  ======  =======
  sdwan_vti0  eth0       IPsec     down    0.0ms / 400ms   0.0ms / 50ms  0.0% / 5%    0               0           0       0
  sdwan_vti1  eth1       IPsec     down    0.0ms / 400ms   0.0ms / 50ms  0.0% / 5%    0               0           0       0
[admin@SD745 overlay]# 
```

The values displayed under columns of latency, jitter, and packet loss; are the average and the threshold for each metric.

System Section

System settings are configured for each device, including license keys, general system settings, firmware updates, backup and restore, and other device management configurations.

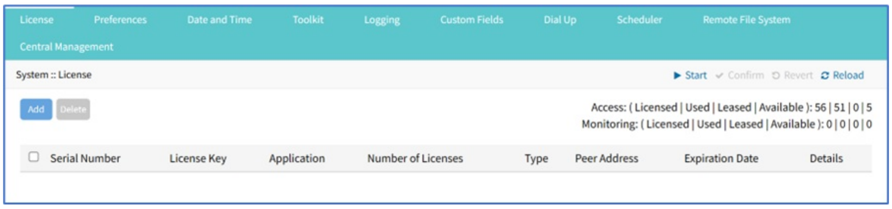


License tab

This displays all licenses enrolled on this Nodegrid device, with license key, expiration date, application, etc. Number of licenses (used and available) are shown in upper right. Licenses can be added or deleted. If licenses expire or are deleted, the devices exceeding the total licenses changes status to "unlicensed" (information is retained in the System). Unlicensed devices are not shown on the Access tab.

For Nodegrid access and control, each managed device must have a license. The required license for each Nodegrid serial port is included with the device.

> NOTE
>
> A managed device is any physical or virtual device defined under Nodegrid for access and control.



System :: License

Access: (Licensed | Used | Leased | Available): 56 | 51 | 0 | 5
Monitoring: (Licensed | Used | Leased | Available): 0 | 0 | 0 | 0

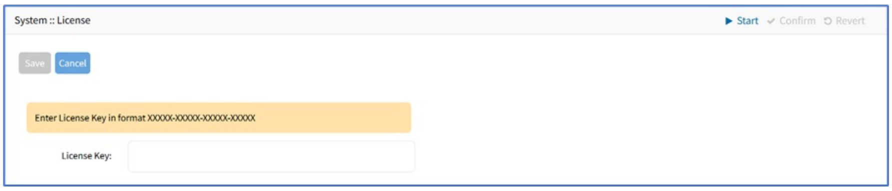
□	Serial Number	License Key	Application	Number of Licenses	Type	Peer Address	Expiration Date	Details

Available license details are listed on the right side.

Manage Licenses

Add a License

1. Go to *System :: License*.
2. Click **Add** (displays dialog).



Enter License Key in format XXXXX-XXXXX-XXXXX-XXXXX

License Key:

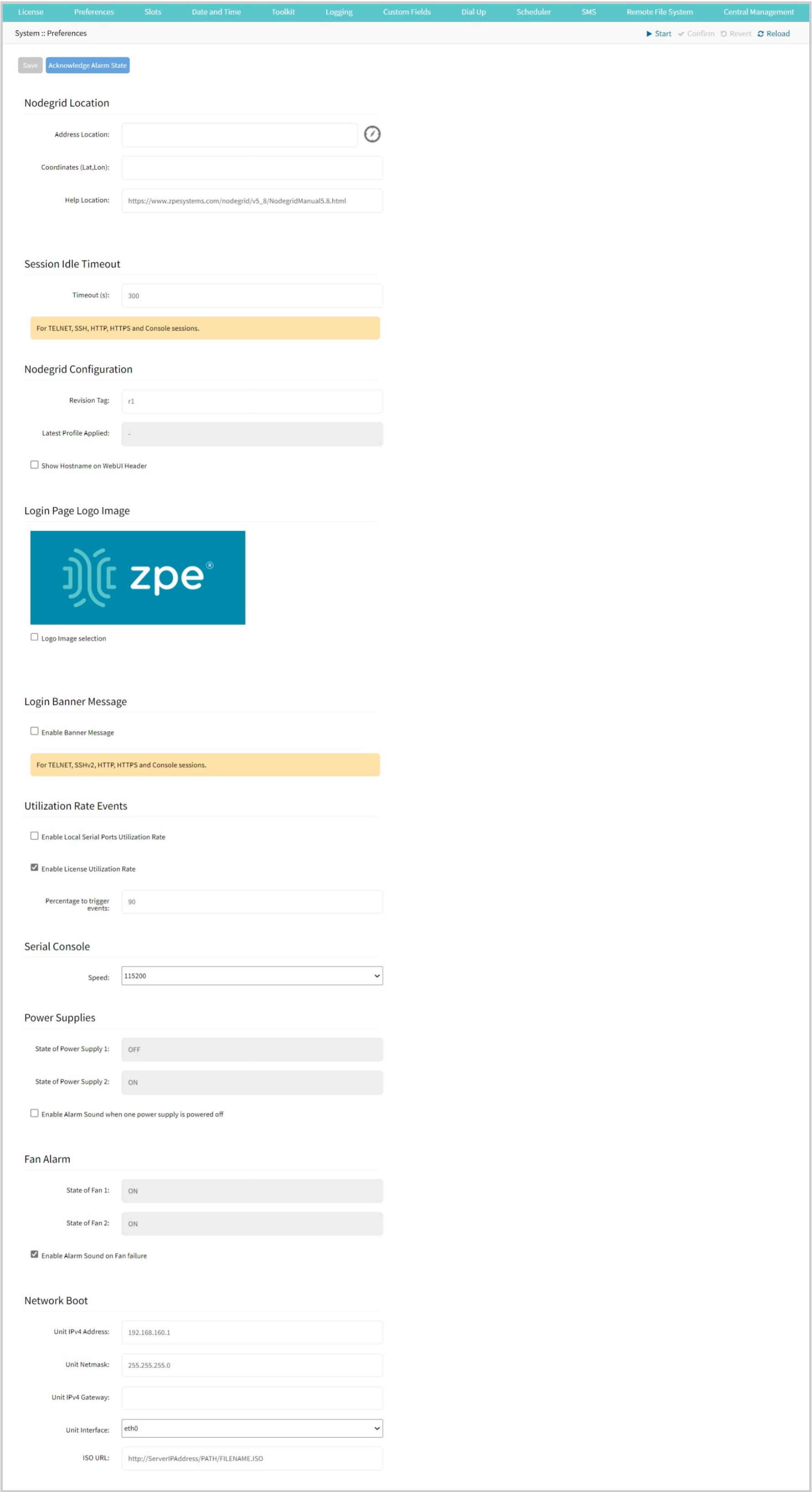
3. Enter **License Key**.
4. Click **Save**.

Delete a License

1. Go to *System :: License*.
2. Select checkbox to remove.
3. Click **Delete**.

Preferences tab

Main system preferences are configured in this tab. Any change in the fields activates the **Save** button.



Nodegrid Location

Address Location:

Coordinates (Lat,Lon):

Help Location: https://www.zpesystems.com/nodegrid/v5_8/NodegridManual5.8.html

Session Idle Timeout

Timeout (s): 300

For TELNET, SSH, HTTP, HTTPS and Console sessions.

Nodegrid Configuration

Revision Tag: r1

Latest Profile Applied: -

□ Show Hostname on WebUI Header

Login Page Logo Image

□ Logo Image selection

Login Banner Message

□ Enable Banner Message

For TELNET, SSHv2, HTTP, HTTPS and Console sessions.

Utilization Rate Events

□ Enable Local Serial Ports Utilization Rate

☑ Enable License Utilization Rate

Percentage to trigger events: 90

Serial Console

Speed: 115200

Power Supplies

State of Power Supply 1: OFF

State of Power Supply 2: ON

□ Enable Alarm Sound when one power supply is powered off

Fan Alarm

State of Fan 1: ON

State of Fan 2: ON

☑ Enable Alarm Sound on Fan failure

Network Boot

Unit IPv4 Address: 192.168.160.1

Unit Netmask: 255.255.255.0

Unit IPv4 Gateway:

Unit Interface: eth0

ISO URL: http://ServerIPAddress/PATH/FILENAME.ISO

Manage Preferences

Settings are provided with individual sections on the page.

Configure Nodegrid Device Preferences

1. Go to *System :: Preferences*.
2. In the *Nodegrid Location*menu, enter details:
   a. Enter **Address Location** (a valid address for the device location).
   b. Enter **Coordinates (Lat, Lon)** (if GPS is available, click **Compass** icon or manually enter GPS coordinates).
   c. For **Help Location**, if applicable, enter alternate URL location for the User Guide. (The administrator can download the documentation from ZPE (HTML5 or PDF, as preferred) to be available for users (when **Help** icon is clicked.)
3. In the *Session Idle Timeout* menu (number of seconds of session inactivity until the session times out and logs the user off.) This setting applies to all telnet, SSH, HTTP, HTTPS, and Console sessions.
   - In **Timeout (seconds)**, enter a value:
     - **zero** (0) – the session will never expire
     - Enter a value greater than or equal to 90. The default unit is seconds. Once the session is inactive for the specified duration, the user is logged out of the session and is informed on the GUI that the session has been timed out.
4. In the *Nodegrid Configuration* menu:
   a. Enter **Revision Tag** (a free format string used as a configuration reference tag - can be manually updated or updated with an automated change management process).
   b. **Latest Profile Applied** (read-only) is the last applied profile (ZTP process or on ZPE Cloud).
   c. (optional) **Show Hostname on WebUI Header** checkbox (displays the device hostname on the WebUI banner. For **Choose Text Color**, click in the color box and select color (click in color grid or enter RGB or CYMK values.

   NOTE

   Any change in value is applied on the next login.

5. In the *Logo Page Logo Image* menu: The administrator can change the logo image (png or jpg) used on the Nodegrid WebUI login. It can be uploaded from the local desktop or a remote server (FTP, TFTP, SFTP, SCP, HTTP, and HTTPS). This is the URL format (username and password may be required): <PROTOCOL>://<Server Address>/<Remote File>.
   a. (optional) **Logo Image selection** checkbox
   b. In *Logo Image* menu, select one:
      Use default logo image radio button.
      Update log image from local computer radio button (expands dialog). Click **Choose File** to locate and select logo (jpg, png)
   c. On **Remote Server** radio button (expands dialog). **URL** (URL can be the IP address or hostname/FQDN. If using IPv6, use brackets [...]. Supported protocols: FTP, TFTP, SFTP, and SCP.)
   d. Enter **Username** and **Password**
      (optional) Select **The path in url to be used as absolute path name** checkbox.
      After upload, refresh the browser cache to display the new image.
6. In the *Logo Banner Message* menu, enter content in **Banner** textbox. Or modify text, as needed (use *Enter* for hard returns).

   NOTE

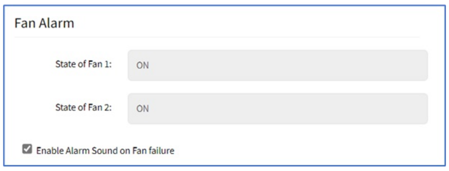
   Nodegrid can be configured to show a login banner on Telnet, SSHv2, HTTP, HTTPS and Console login. This banner is displayed on the device login page. The default content (below) can be edited.
   The message can include device-specific information, such as Device Alias or other device identifier details.

7. In the *Utilization Rate Events* menu:
   a. (optional) **Enable Local Serial Ports Utilization Rate** checkbox
   b. Select **Enable License Utilization Rate** checkbox
   c. Enter **Percentage to trigger events** (event notification is generated when percentage is reached)
8. In the *Serial Console* menu, on **Speed** drop-down, select baud rate (9600, 19200, 38400, 57600, 115200).
9. In the *Power Supplies* menu, select **Enable Alarm Sound when one power supply is powered off**checkbox

   NOTE

   This displays only when device is equipped with two power supplies). Includes option to enable alarm when powered off.

10. In the *Fan Alarm* menu (displays only when device is equipped with fans), select **Enable Alarm Sound on Fan Failure** checkbox



Fan Alarm

State of Fan 1: ON

State of Fan 2: ON

☑ Enable Alarm Sound on Fan failure

11. In the *Network Boot* menu:

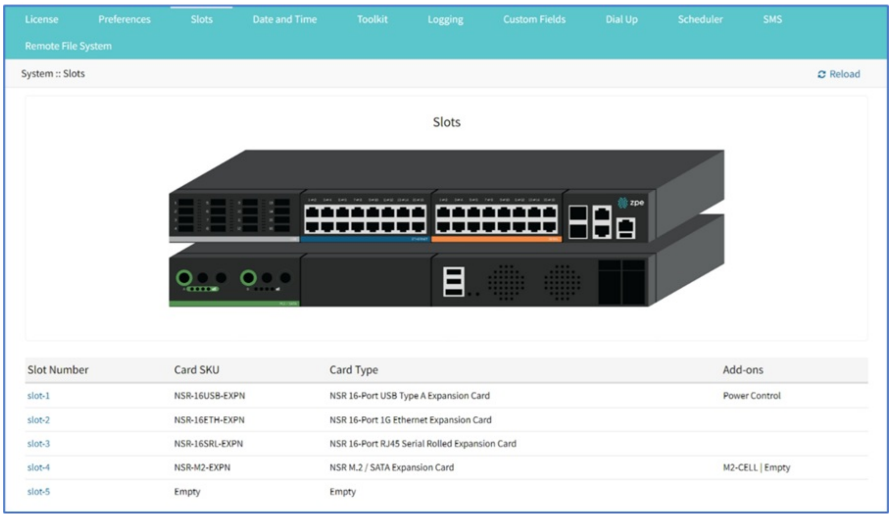
    NOTE

    Nodegrid can boot from a network ISO image.

    a. Enter **Unit IPv4 Address**. (URL format:http://ServerIPAddress/PATH/FILENAME.ISO)
    b. Enter **Unit Netmask**
    c. On **Unit Interface** drop-down, select one (eth0, eth1)
    d. Enter **ISO URL**
12. Review details, then click **Save**.

Slots tab (SR only)

This information identifies slots on SR devices with installed modules.

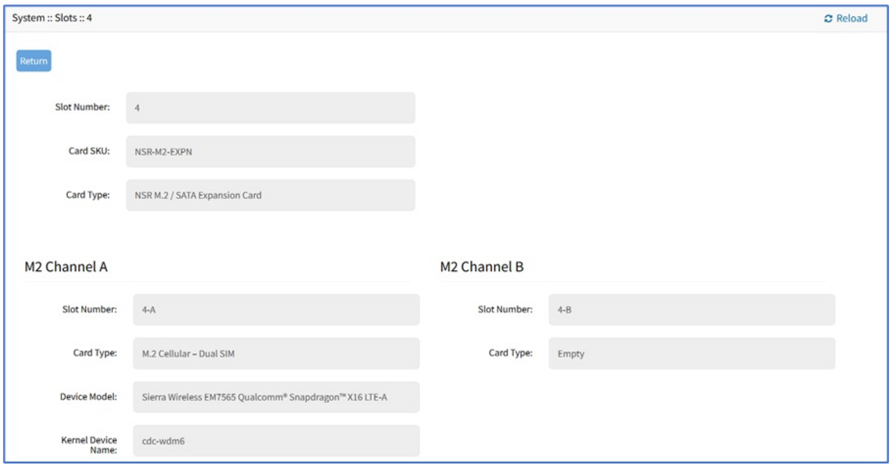


Slot Number	Card SKU	Card Type	Add-ons
slot-1	NSR-16USB-EXPN	NSR 16-Port USB Type A Expansion Card	Power Control
slot-2	NSR-16ETH-EXPN	NSR 16-Port 1G Ethernet Expansion Card	
slot-3	NSR-16SRL-EXPN	NSR 16-Port RJ45 Serial Rolled Expansion Card	
slot-4	NSR-M2-EXPN	NSR M.2 / SATA Expansion Card	M2-CELL | Empty
slot-5	Empty	Empty	

Manage Slots

Review Slot Details

1. Go to *System :: Slots*.
2. In the table, click on a slot name (displays dialog varies according to the module).



Slot Number: 4

Card SKU: NSR-M2-EXPN

Card Type: NSR M.2 / SATA Expansion Card

M2 Channel A

Slot Number: 4-A

Card Type: M.2 Cellular – Dual SIM

Device Model: Sierra Wireless EM7565 Qualcomm® Snapdragon™ X16 LTE-A

Kernel Device Name: cdc-wdm6

M2 Channel B

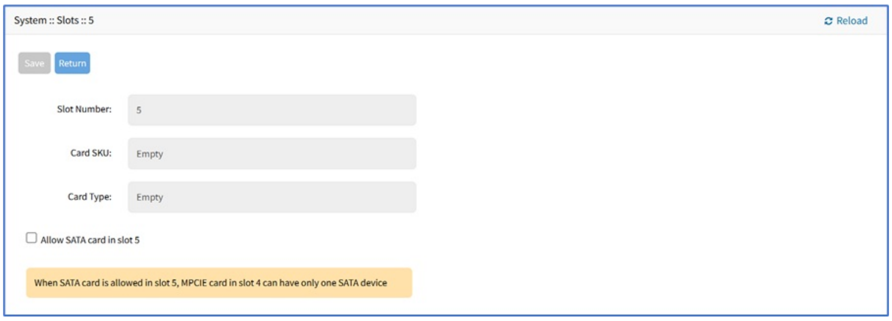
Slot Number: 4-B

Card Type: Empty

3. When done, click **Return**.

Enable SATA Card in Slot 5

1. Go to *System :: Slots*.
2. In the table, click on **Slot 5** (displays dialog).



Slot Number: 5

Card SKU: Empty

Card Type: Empty

☐ Allow SATA card in slot 5

When SATA card is allowed in slot 5, MPCIE card in slot 4 can have only one SATA device

3. Select **Allow SATA card in slot 5** checkbox.
4. Click **Save**.

Date and Time tab

Nodegrid devices supports NTP (Network Time Protocol) Authentication and Cellular Tower Synchronization. This default configuration automatically retrieves accurate date/time from any server in the NTP pool. NTP authentication provides an extra safety measure for Nodegrid to ensure that the timestamp it receives has been generated by a trusted source, protecting it from malicious activity or interception.

Local Settings sub-tab

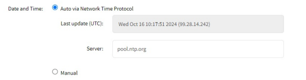
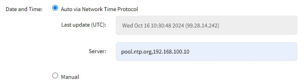
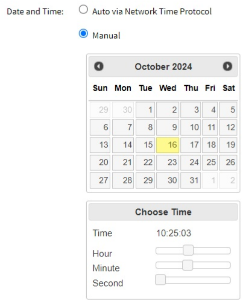
If needed, the date/time can be manually set. NTP is the default configuration. In manual configuration mode, Nodegrid device uses its internal clock to provide date and time information. Refresh the page to see the current system time. Date and time synchronization from cell tower is an additional convenience that obtains exact time directly from the carrier network.

To set the local time zone, select from the drop-down menu (default: UTC).

Configure Local Time

Use this dialog to set up local time and UTC zone for the device location.

1. Go to *System :: Date and Time :: Local Settings*.
2. In *Date and Time* menu, select one:

Field	Description	Reference Image
Auto via Network Time Protocol	You can configure a NTP pool, which will request date and time from NTP servers.	 Date and Time: ● Auto via Network Time Protocol Last update (UTC): Wed Oct 16 10:17:51 2024 (99.28.14.242) Server: pool.ntp.org ○ Manual
	You can also add multiple NTP servers in the Server field. Enter comma-separated values without spaces.	 Date and Time: ● Auto via Network Time Protocol Last update (UTC): Wed Oct 16 10:30:48 2024 (99.28.14.242) Server: pool.ntp.org,192.168.100.10 ○ Manual
Manual	- Scroll through **Calendar** and select date. - **Choose Time** (hour, minute, second)	 Date and Time: ○ Auto via Network Time Protocol ● Manual October 2024 Choose Time Time 10:25:03

3. In *Time Zone* menu, **Options** drop-down, select appropriate time zone.
4. In *Cellular Tower Synchronization* menu:

   > **NOTE**
   >
   > This is supported by units with an installed Wireless Modem card and valid SIM card. The Nodegrid device can get date/time from the cellular tower. The SIM card must be registered to the carrier network).

   - Select **Enable Date and Time Synchronization** checkbox.

     > **NOTE**
     >
     > Both NTP and Cellular Tower Synchronization can be enabled. The last date/time received from either source is applied. This allows updated date/time with any connection failover configuration.

5. Click **Save**.

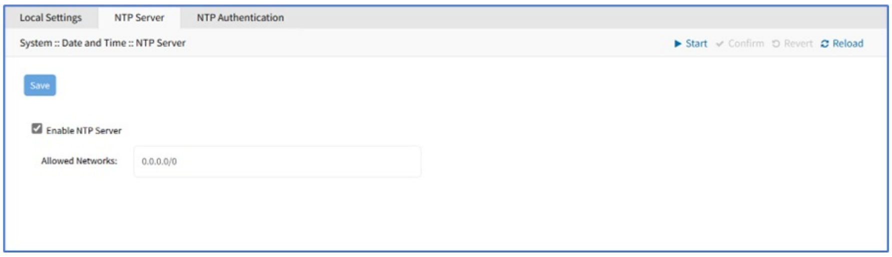
CLI Configuration Example

Plaintext Copy

```
[admin@nodegrid date_and_time]# show /settings/date_and_time/
system time: Wed Oct 16 10:31:33 UTC 2024
date_and_time = network_time_protocol
last_update: Wed Oct 16 10:30:48 2024 (99.28.14.242)
server = pool.ntp.org
zone = us|eastern
```

NTP Server sub-tab

This page enables the NTP Server.



System :: Date and Time :: NTP Server

☑ Enable NTP Server

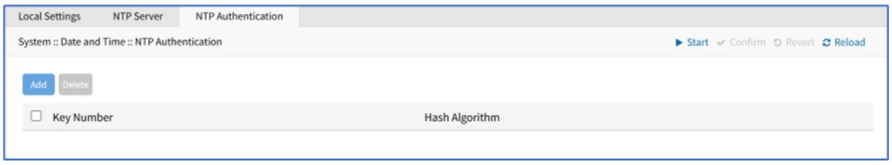
Allowed Networks: 0.0.0.0/0

Configure the local NTP server

1. Go to *System :: Date and Time :: NTP Server*.
2. Select **Enable NTP Server** checkbox.
3. In **Allowed Networks**, enter all allowed networks (comma-separated).
4. Click **Save**.

NTP Authentication sub-tab

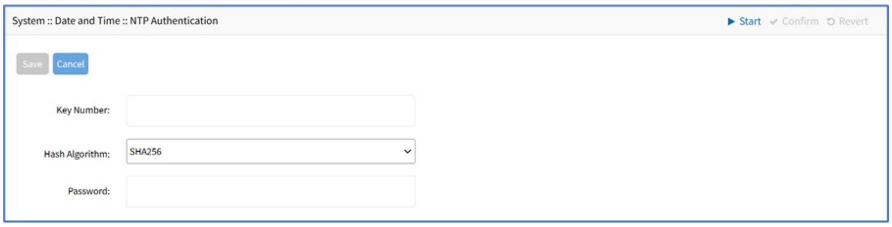
NTP reduces security risks associated with time synchronization. With authentication, there is assurance a generated response is from an expected source (rather than maliciously generated or intercepted). Authentication applies a list of agreed keys (passwords) between a server and a client. Communication between server and client is encrypted with one of the agreed keys appended to the messages. The appended key is un-encrypted to ensure it matches one of the agreed keys. Only then is action taken.



Configure Key Number Set

This requires Admin privileges. Repeat the process for each key number set.

1. Go to *System :: Date and Time :: NTP Authentication*.
2. Click **Add** (displays dialog).



Hash Algorithm: SHA256

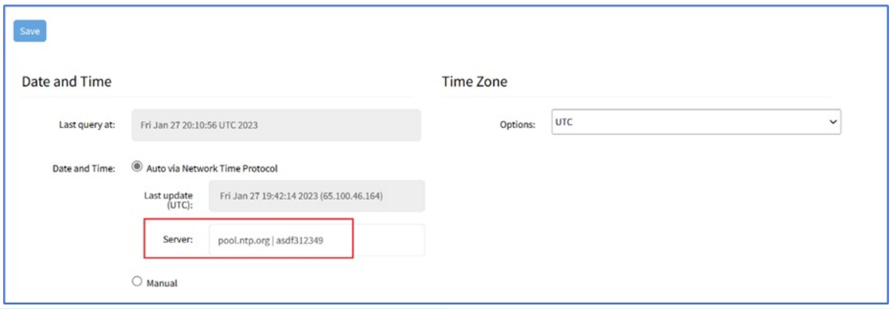
3. Enter **Key Number** (any unsigned integer (range: 1 to 2^{32} – 1).
4. On **Hash Algorithm** drop-down, select one (MD5, RMD160, SHA1, SHA256, SHA384, SHA512, SHA3-224, SHA3-256, SHA3-384, SHA3-512).
5. Enter **Password** character string (space character not allowed). Alternatively, enter a hexadecimal number with prefix **HEX** followed by the number ######.
6. Click **Save**.

Delete Key Number

1. Go to *System :: Date and Time :: NTP Authentication*.
2. Select checkbox next to Key Number to delete.
3. Click **Delete**.

Link the NTP server and Key Number

1. Go to *System :: Date and Time :: Local Settings*.
2. Use separator '|' (pipe) between server address and its key number.



Last query at: Fri Jan 27 20:10:56 UTC 2023

Date and Time: ● Auto via Network Time Protocol

Last update (UTC): Fri Jan 27 19:42:14 2023 (65.100.46.164)

Server: pool.ntp.org | asdf312349

○ Manual

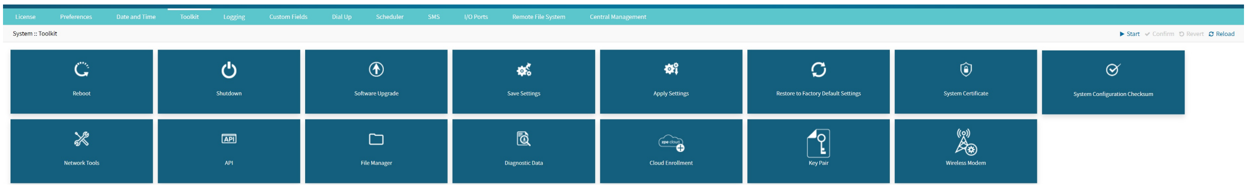
Options: UTC

> **NOTE**
>
> You can also add multiple NTP servers in the Server field. Enter comma-separated values without spaces.

3. Make changes, as needed.
4. Click **Save**.

Toolkit tab

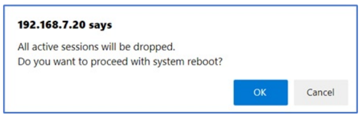
System maintenance features are available in *System :: Toolkit* page.



Reboot tool

Reboot command is a graceful shutdown and reboot of the Nodegrid device. A warning message informs that all active sessions will be dropped. During a reboot, the operating system is automatically restarted.

On click, displays the pop-up dialog. Click **OK** to continue.



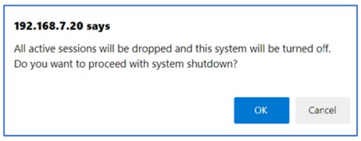
192.168.7.20 says

All active sessions will be dropped.
Do you want to proceed with system reboot?

Shutdown tool

On a shutdown, the operating system will be brought to a halted state. At this point, it is safe to drop the power supply to the unit (turn off power supplies or removing power cords). To turn the unit back on, the power supply must be stopped and then restarted.

On click, displays pop-up dialog. Click **OK** to continue.



192.168.7.20 says

All active sessions will be dropped and this system will be turned off.
Do you want to proceed with system shutdown?

Software Upgrade tool

This section explains the following software upgrade and downgrade procedures of the Nodegrid application:

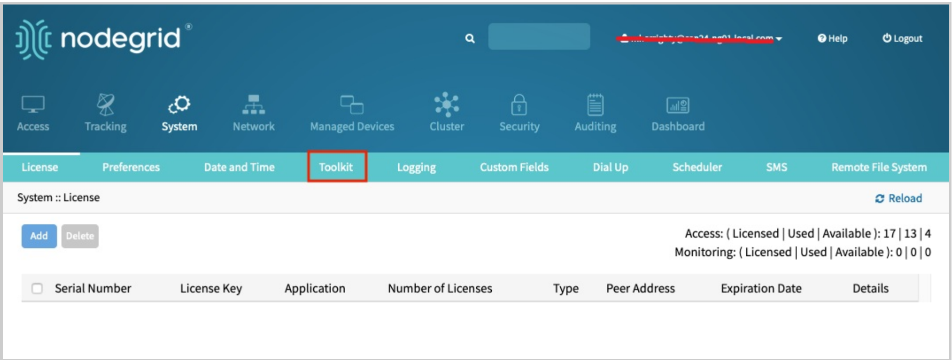
- Upgrading via Web UI
- Upgrading via CLI
- Downgrading

Upgrading via Web UI

NOTE

Software upgrade/downgrade requires several minutes to process. Be patient.

1. Go to *System:: Toolkit*.

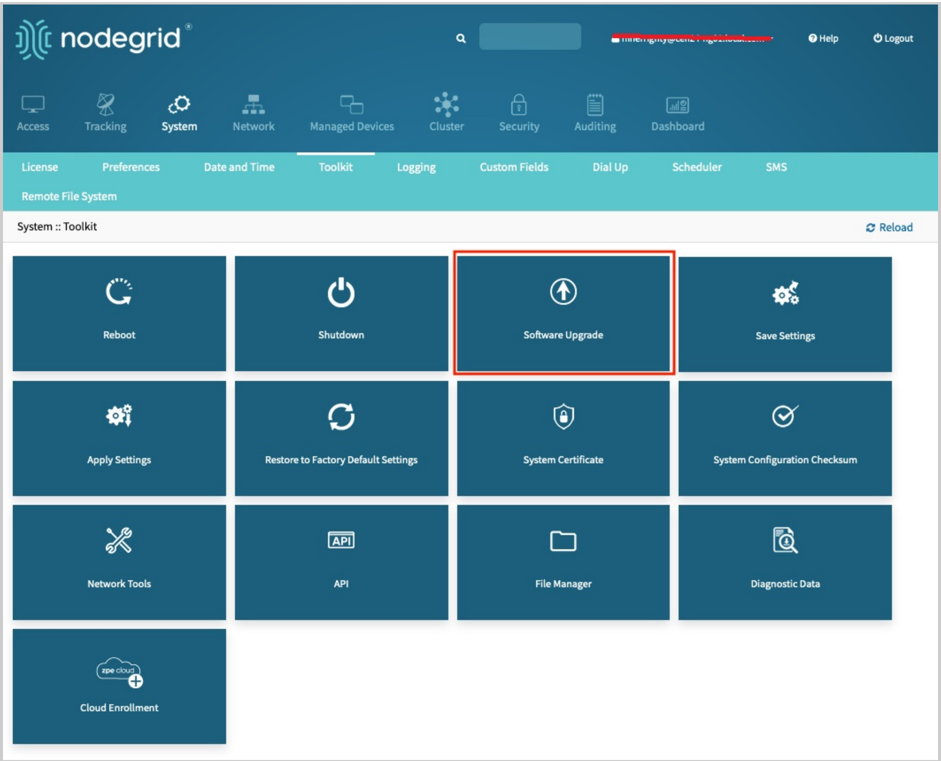


System :: License

Access: (Licensed | Used | Available): 17 | 13 | 4
Monitoring: (Licensed | Used | Available): 0 | 0 | 0

□	Serial Number	License Key	Application	Number of Licenses	Type	Peer Address	Expiration Date	Details

2. Click the **Software Upgrade** icon (displays dialog).



3. In *Image Location* menu, select one:
   - **Local System** radio button (expands dialog). Enter **Filename**.

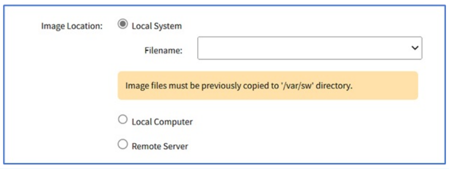


Image Location: ● Local System

Filename:

Image files must be previously copied to '/var/sw' directory.

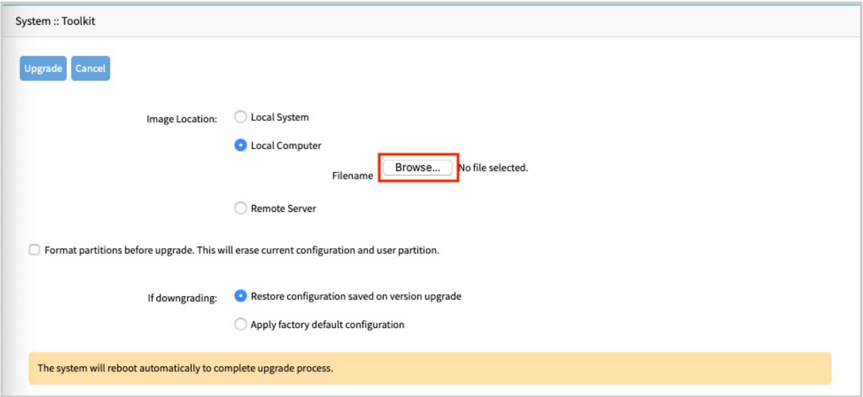
○ Local Computer

○ Remote Server

NOTE

Image files must be previously copied into '/var/sw' directory.

- **Local Computer** radio button (expands dialog). Click **Choose File**. On dialog, locate and select the file. Navigate to the folder where the downloaded firmware file is placed. For instructions on how to download a firmware, see Download Firmware Update. You can also contact support to download the firmware update.



System :: Toolkit

Upgrade Cancel

Image Location: ○ Local System

● Local Computer

Filename Browse... No file selected.

○ Remote Server

□ Format partitions before upgrade. This will erase current configuration and user partition.

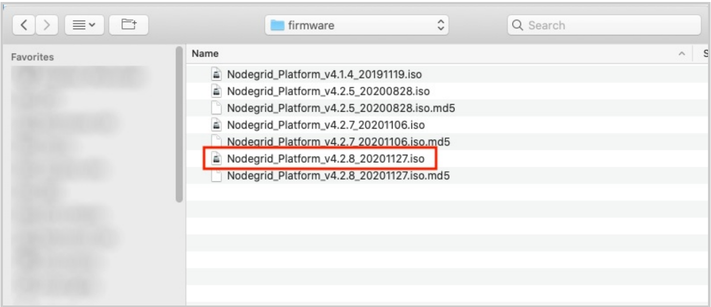
If downgrading: ● Restore configuration saved on version upgrade

○ Apply factory default configuration

The system will reboot automatically to complete upgrade process.

NOTE

A dynamic status bar provides a real-time status of the file upload progress. Once the upload is finished, the upgrade process will automatically commence. You can use the **Cancel** button to abort the operation.



firmware

Search

Favorites

Name

Nodegrid_Platform_v4.1.4_20191119.iso
Nodegrid_Platform_v4.2.5_20200828.iso
Nodegrid_Platform_v4.2.5_20200828.iso.md5
Nodegrid_Platform_v4.2.7_20201106.iso
Nodegrid_Platform_v4.2.7_20201106.iso.md5
Nodegrid_Platform_v4.2.8_20201127.iso
Nodegrid_Platform_v4.2.8_20201127.iso.md5

- **Remote Server** radio button (expands dialog). Enter details.

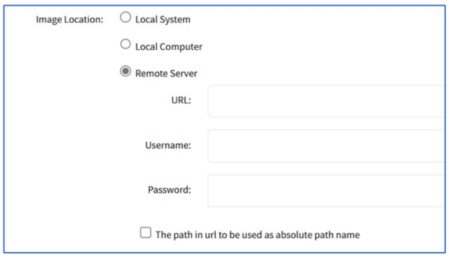


Image Location: ○ Local System

○ Local Computer

● Remote Server

URL:

Username:

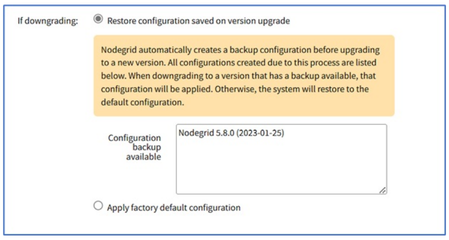
Password:

□ The path in url to be used as absolute path name

Enter **URL**. (URL can be the IP address or hostname/FQDN. If using IPv6, use brackets [...]. Supported protocols: FTP, TFTP, SFTP, and SCP.) Enter **Username** and **Password**.

(optional) Select **The path in url to be used as absolute path name** checkbox.

4. (optional) Select **Format partitions before upgrade. This will erase current configuration and user partition** checkbox.
5. In *If downgrading* section, select one:
   - **Restore configuration saved on version upgrade** radio button (*Read the instructions.*)



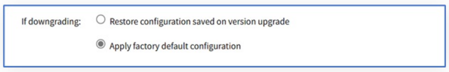
If downgrading: ● Restore configuration saved on version upgrade

Nodegrid automatically creates a backup configuration before upgrading to a new version. All configurations created due to this process are listed below. When downgrading to a version that has a backup available, that configuration will be applied. Otherwise, the system will restore to the default configuration.

Configuration backup available: Nodegrid 5.8.0 (2023-01-25)

○ Apply factory default configuration

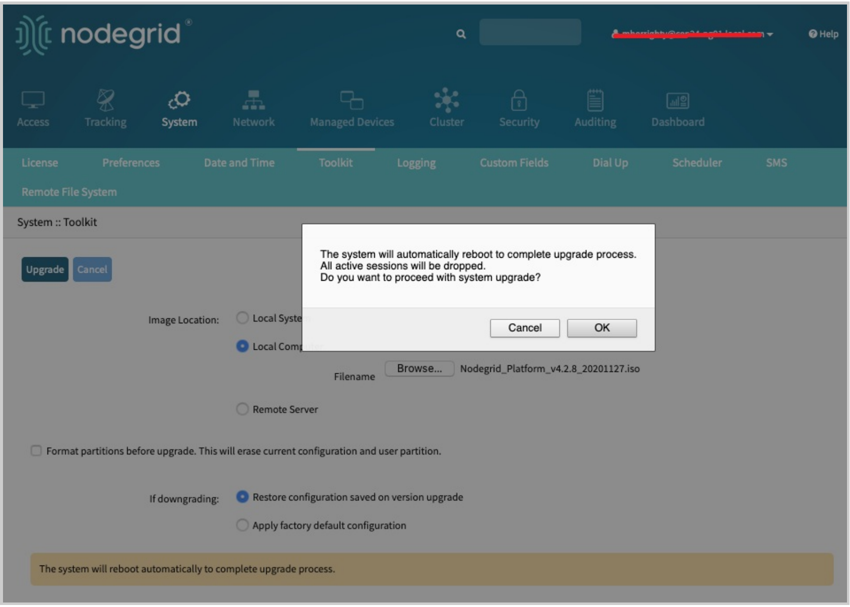
   - **Apply factory default configuration** radio button (out-of-the-box configuration)



If downgrading: ○ Restore configuration saved on version upgrade

● Apply factory default configuration

6. Click **Upgrade** (requires several minutes) and click **OK** to continue.



System :: Toolkit

The system will automatically reboot to complete upgrade process.
All active sessions will be dropped.
Do you want to proceed with system upgrade?

Image Location: ○ Local Syste… ● Local Comp…

Filename: Nodegrid_Platform_v4.2.8_20201127.iso

○ Remote Server

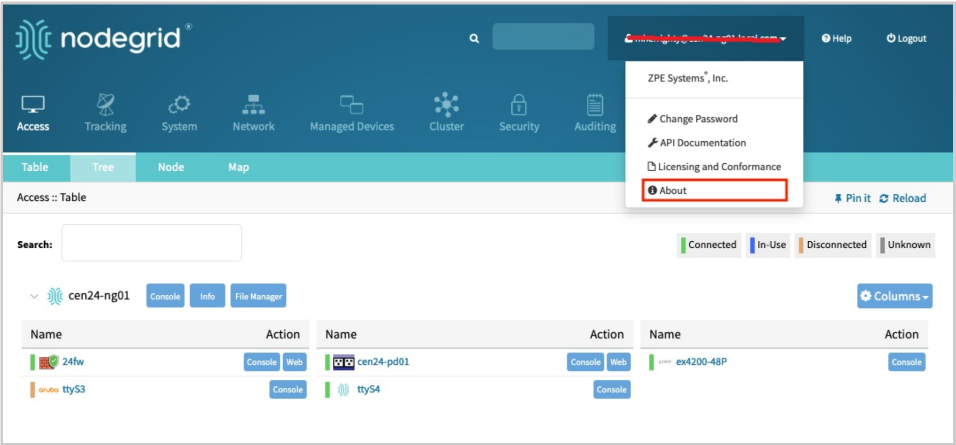
□ Format partitions before upgrade. This will erase current configuration and user partition.

If downgrading: ● Restore configuration saved on version upgrade ○ Apply factory default configuration

The system will reboot automatically to complete upgrade process.

The firmware gets updated and the unit is rebooted (this will take a couple of minutes).

7. Log in to the Nodegrid Web UI.
8. Click **About** to verify the upgraded version.

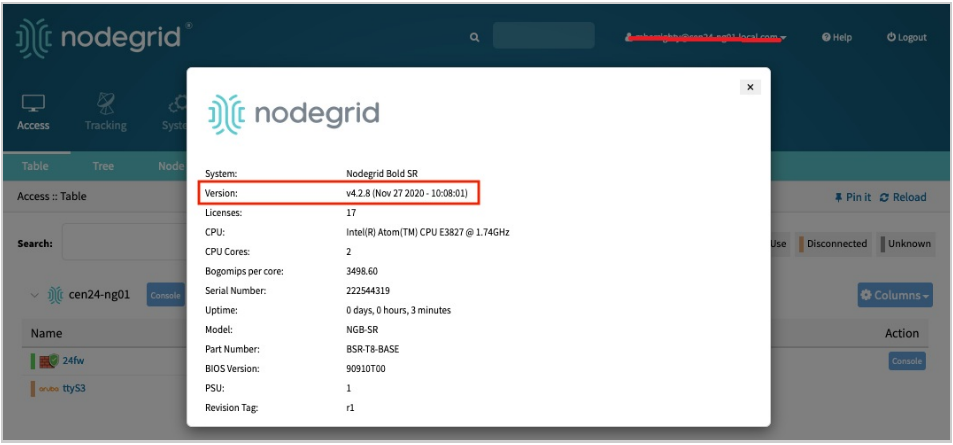


Access :: Table

Search:

cen24-ng01

Name	Action	Name	Action	Name	Action
24fw	Console Web	cen24-pd01	Console Web	ex4200-48P	Console
ttyS3	Console	ttyS4	Console		



Access :: Table

Search:

cen24-ng01

System:	Nodegrid Bold SR
Version:	v4.2.8 (Nov 27 2020 - 10:08:01)
Licenses:	17
CPU:	Intel(R) Atom(TM) CPU E3827 @ 1.74GHz
CPU Cores:	2
Bogomips per core:	3498.60
Serial Number:	222544319
Uptime:	0 days, 0 hours, 3 minutes
Model:	NGB-SR
Part Number:	BSR-T8-BASE
BIOS Version:	90910T00
PSU:	1
Revision Tag:	r1

The software version can be upgraded from the previous release v4.2.4 or newer. If necessary, to upgrade from v3.2, v4.0, v4.1, or older v4.2 must first upgrade to v4.2.4, and then upgrade to the latest version.

Upgrading via CLI

The following is the prerequisite before you upgrade the Nodegrid software via the CLI application:

1. Download Firmware Update and save the ISO file to one of these locations.
   a. Remote Server such as FTP, SSH, or HTTP.
   b. Nodegrid, to the /var/sw directory:
      i. Transfer the iso file using SCP. For example: scp nodegrid.iso admin@nodegrid:/var/sw/
      ii. Copy the iso file to a USB flash drive and plug it into a Nodegrid USB port.
      iii. Log in as admin to Nodegrid and launch the root shell (shell sudo su -).
      iv. Change the location (cd) to /run/media/sdb or /run/media/sdb1 directory.
      v. Copy the iso file to the/var/sw directory.

Follow these steps to upgrade the software via CLI:

1. Access the Nodegrid via SSH, local port (Console or HDMI port), or telnet (if enabled).
2. Log in as admin.
3. Execute the following commands:

None

Copy

```
 cd /system/toolkit/
     software_upgrade
     set image_location=local_system
     set filename=<image_file>
     upgrade
- OR -
     cd /system/toolkit/
     software_upgrade
     set image_location=remote_server
     set url=<protocol://ServerAddress/image_file>
     set username=<user>
     set password=<password>
     upgrade
```

NOTE

For the URL, the supported protocols are FTP, SFTP, TFTP, HTTP, HTTPS, and SCP.

CLI Configuration Examples

Local System

None

Copy

```
[admin@nodegrid /]# cd /system/toolkit/
[admin@nodegrid toolkit]# software_upgrade
[admin@nodegrid {toolkit}]# set image_location=local_system
[admin@nodegrid {toolkit}]# set filename=NodeGrid_Platform_v3.2.38_20170520.iso
[admin@nodegrid {toolkit}]# upgrade
```

FTP Server

None

Copy

```
[admin@nodegrid /]# cd /system/toolkit
[admin@nodegrid toolkit]# software_upgrade
[admin@nodegrid {toolkit}]# set image_location=remote_server url=ftp://10.0.0.1/NodeGrid_Platform_v3.2.38_20170520.iso
[admin@nodegrid {toolkit}]# set username=john
[admin@nodegrid {toolkit}]# set password=john1234
[admin@nodegrid {toolkit}]# upgrade
```

SCP Server

None

Copy

```
[admin@nodegrid /]# cd /system/toolkit
[admin@nodegrid toolkit]# software_upgrade
[admin@nodegrid {toolkit}]# set image_location=remote_server
[admin@nodegrid {toolkit}]# set url=scp://SCP.server.com/NodeGrid_Platform_v3.2.38_20170520.iso
[admin@nodegrid {toolkit}]# set username=jane.jane
[admin@nodegrid {toolkit}]# set password=janepasswd
[admin@nodegrid {toolkit}]# upgrade
```

HTTPS Server

None

Copy

```
[admin@nodegrid /]# cd /system/toolkit
[admin@nodegrid toolkit]# software_upgrade
[admin@nodegrid {toolkit}]# set image_location=remote_server url= https://<nodegrid_IP>/NodeGrid_Platform_v3.2.38_20170520.iso
[admin@nodegrid {toolkit}]# set username=user password=userpassword
[admin@nodegrid {toolkit}]# upgrade
```

View the Software Upgrade via CLI

None Copy

```
[admin@nodegrid /]# software_upgrade
[admin@nodegrid {toolkit}]# show

The system will reboot automatically to complete upgrade process.
image_location = local_system
filename =
Image files must be previously copied to '/var/sw' directory.
format_partitions_before_upgrade = no
if_downgrading = restore_configuration_saved_on_version_upgrade

If no configuration matches the version, factory default will be applied.
saved_configurations:
Nodegrid 5.4.1 (2022-08-16)
Nodegrid 5.4.1 (2022-05-02)
Nodegrid 5.2.1 (2021-11-01)
```

Downgrading

If you need to downgrade to a previous version of the Nodegrid software, two options are available:

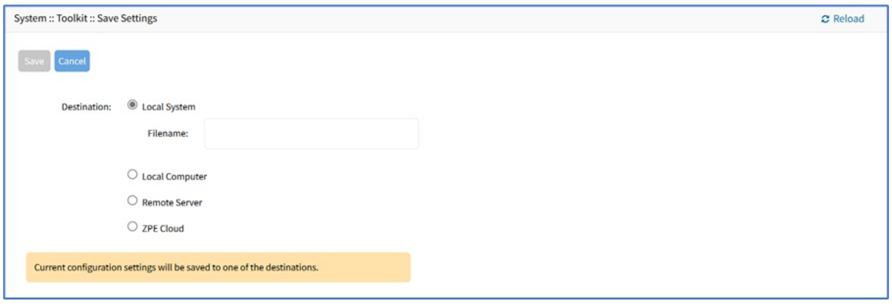
- Restore to factory default
- Restore configuration

> **NOTE**
>
> To use the restore configuration option, the Nodegrid software version must match the version used to create the restoration file. For example, if the configuration file was created in version 4.2 and Nodegrid is currently on version 5.0, Nodegrid must be downgraded to version 4.2 before the restoration file can be used.

Save Settings tool

The Save Settings tool helps the users to save the current configuration.

1. Go to *System :: Toolkit*.
2. Click the **Save Settings** icon (displays dialog).



Destination: ● Local System

Filename:

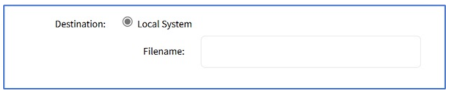
○ Local Computer

○ Remote Server

○ ZPE Cloud

Current configuration settings will be saved to one of the destinations.

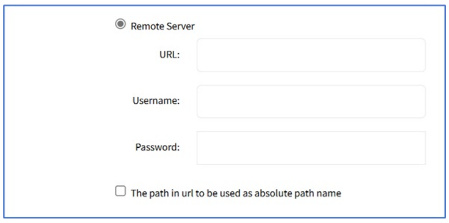
3. In the *Destination* menu, select one.
   - **Local System** radio button (expands dialog). When you select this option, the backup is stored in the local file system that is accessible to the administrator through the **File Manager**. Enter **Filename**.



Destination: ● Local System

Filename:

   You can go to the File Manager and access the admin_group/config_backup file.
   - **Local Computer** radio button (file is saved on the local computer Download folder)
   - **Remote Server** radio button (expands dialog)



● Remote Server

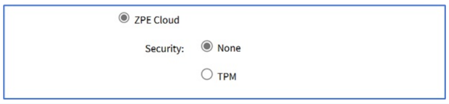
URL:

Username:

Password:

□ The path in url to be used as absolute path name

     - Enter **URL.** (URL can be the IP address or hostname/FQDN. If using IPv6, use brackets [...]. Supported protocols: FTP, TFTP, SFTP, and SCP.)
     - Enter **Username** and **Password**
     - (optional) Select **The path in the URL to be used as the absolute path name** checkbox.
     - **ZPE Cloud** radio button (expands dialog) (displays only if ZPE Cloud is enabled).



● ZPE Cloud

Security: ● None

○ TPM

NOTE

ZPE Cloud must be enabled on Security :: Services before this is available.

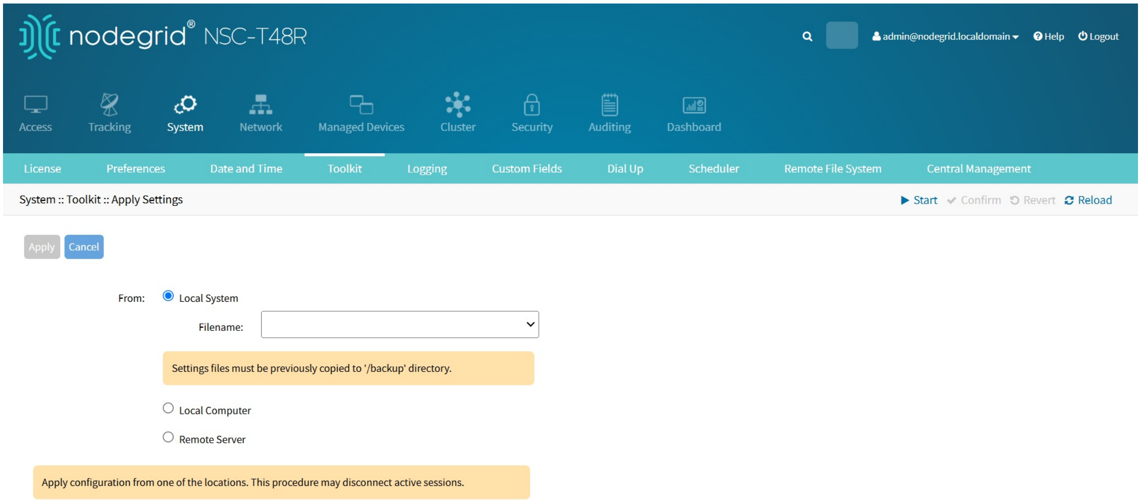
     - On *Security*, select one:
       - **None** radio button
       - **TMP** radio button

4. Click **Save**.

Apply Settings tool

Saved configurations can be loaded from the Nodegrid device, a local connected computer, or from a remote server. When applied on the Nodegrid device, that becomes the new configuration. The server address can be the IP address or hostname/FQDN. If using IPv6, use brackets [...]. Supported protocols: FTP, TFTP, SFTP, SCP, HTTP, and HTTPS.

1. Go to *System :: Toolkit*.
2. Click **Apply Settings** icon (displays dialog).
3. From the *From* menu, select one:
    - **Local System** radio button (expands dialog). Enter **Filename**. You can select the saved config from the Filename drop-down list as shown in the following image. The backup files are available in the */backup* folder.



System :: Toolkit :: Apply Settings

From: ● Local System

Filename:

Settings files must be previously copied to '/backup' directory.

○ Local Computer

○ Remote Server

Apply configuration from one of the locations. This procedure may disconnect active sessions.

    - **Local Computer** radio button (expands dialog). Click **Choose File** (locate and select the file).
    - **Remote Server** radio button (expands dialog):
        - Enter **URL.** (URL can be the IP address or hostname/FQDN. If using IPv6, use brackets [...]. Supported protocols: FTP, TFTP, SFTP, and SCP.)
        - Enter **Username** and **Password**
        - (optional) Select **The path in URL to be used as the absolute path name** checkbox.
4. Click **Apply**.

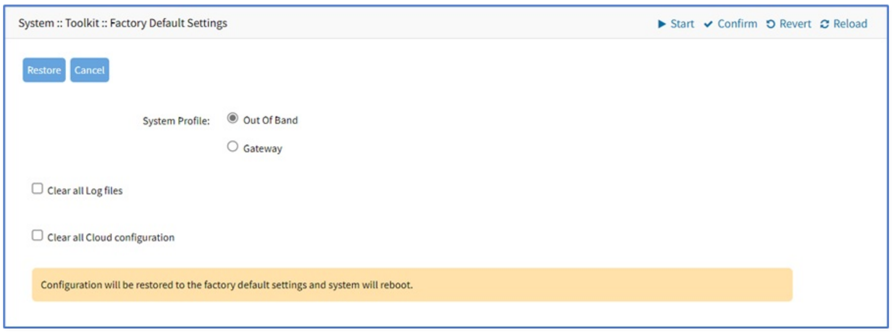
Restore to Factory Default Settings tool

The Nodegrid solution offers the following options to reset the unit to factory default settings. During this action, all configuration files are set to factory default.

- Via Web UI
- Via Console
- Hard Restore
- System Partition

Web UI Procedure

1. Go to *System :: Toolkit*.
2. Click the **Restore to Factory Default Settings** icon (displays dialog, depending on the device)
   Gate SR, Bold SR, Net SR, Hive SR, Link SR, NSCP, Mini SR devices, NSC, NGM (VM) devices



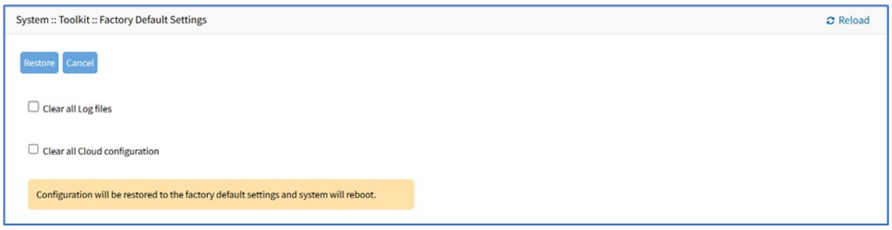
System :: Toolkit :: Factory Default Settings

System Profile: ● Out Of Band ○ Gateway

□ Clear all Log files

□ Clear all Cloud configuration

Configuration will be restored to the factory default settings and system will reboot.



System :: Toolkit :: Factory Default Settings

□ Clear all Log files

□ Clear all Cloud configuration

Configuration will be restored to the factory default settings and system will reboot.

3. In the *System Profile* menu, select one:
   - **Out of Band** radio button
   - **Gateway** radio button
4. (optional) Select the **Clear all Log files** checkbox.
5. (optional) Select the **Clear all Cloud Configuration** checkbox.
6. Click **Restore**.

CLI Procedure

To perform the factory reset via the device console connection:

1. Access the Nodegrid device via telnet, ssh, or console.
2. Log in as an administrator user.
3. Type the following commands:

Plaintext

```
[admin@nodegrid /]# cd /system/toolkit/
[admin@nodegrid toolkit]# factory_settings
[admin@nodegrid {toolkit}]# restore
You are about to restore the configuration to factory default settings. The system will reboot after that.
Do you want to proceed? (yes, no)  : yes
```

Hard Restore

Hard restore is available on the Nodegrid device. To use, locate the RST button on the chassis. Press the RST button down for at least 10 seconds. All configuration files are reset to defaults and log files are cleared. The RST button (reset to factory default) requires a minimum ET version of 80814T00. To determine the current version, see the *About* page details.

System Partition

The system can also be reset by reformatting the whole system partition. This wipes all existing files and resets the system back to the shipped state.

Regaining Web UI Access to the Devices

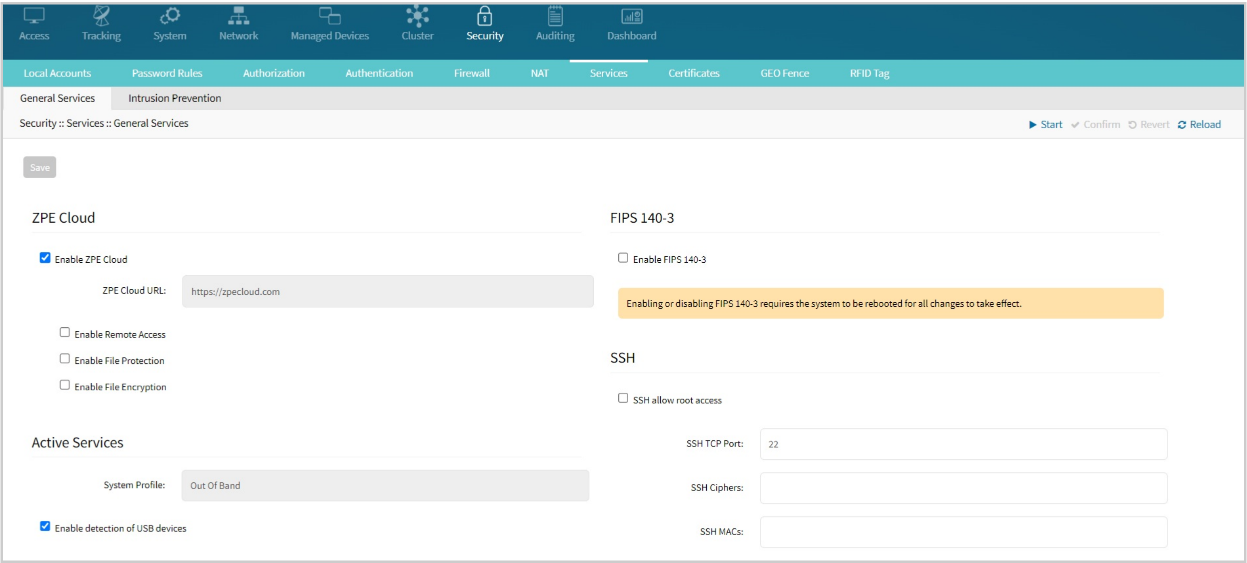
When you factory reset a device using the Gateway system profile, you lose access to the device through the Web UI. To access the device through Web UI, you need to perform the following actions:

1. Access the device through the console.
2. Reset the password.
3. Set the value of the following field to no: **set block_unsolicited_incoming_package= no**
4. Save the changes.

You can now access the device through Web UI. Once you get access, ensure to set the security settings.

Setting up Security Settings

1. Go to **Security** :: **Services.**
2. Set the **Cipher Suite Level Field** value to **High.**
3. Select the **Block host with the Multiple Authentication Failure** field.
4. Verify if the following fields are disabled:
    - Enable VMware Manager
    - Enable Automatic Cluster Enrollment
    - Enable VM Serial Access
    - Enable Zero Touch Provisioning
    - Enable Telegraf
    - Enable SNMP Service
    - Enable Detection of USB devices
    - Enable PXE (Preboot Execution Environment)



Security :: Services :: General Services

ZPE Cloud

☑ Enable ZPE Cloud

ZPE Cloud URL: https://zpecloud.com

☐ Enable Remote Access

☐ Enable File Protection

☐ Enable File Encryption

Active Services

System Profile: Out Of Band

☑ Enable detection of USB devices

FIPS 140-3

☐ Enable FIPS 140-3

Enabling or disabling FIPS 140-3 requires the system to be rebooted for all changes to take effect.

SSH

☐ SSH allow root access

SSH TCP Port: 22

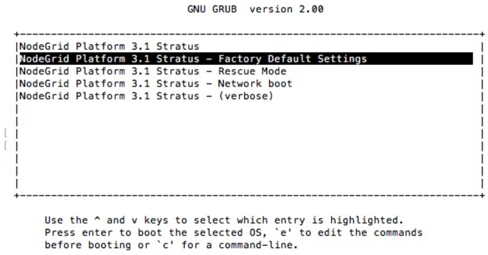
SSH Ciphers:

SSH MACs:

Troubleshooting

If you need to reset your Nodegrid to Factory Default and if for some reason the Nodegrid is unresponsive or does not work properly, then follow the steps below:

1. If you have the Nodegrid Serial Console access, have a terminal (Putty, SecureCRT) with a 115200bps baud rate connected to the Nodegrid console port, or a monitor to the HDMI and a keyboard to the USB port. If you have the Nodegrid Manager, launch the Remote Console on the VM.
2. Reboot the Nodegrid device.
3. Select **Factory Default Settings** in the bootloader menu. The bootloader loads the factory default configuration and presents the login prompt.



```
                     GNU GRUB  version 2.00

 +--------------------------------------------------------------------------+
 |NodeGrid Platform 3.1 Stratus                                             |
 |NodeGrid Platform 3.1 Stratus - Factory Default Settings                  |
 |NodeGrid Platform 3.1 Stratus - Rescue Mode                               |
 |NodeGrid Platform 3.1 Stratus - Network boot                              |
 |NodeGrid Platform 3.1 Stratus - (verbose)                                 |
 |                                                                          |
 |                                                                          |
[|                                                                          |
[|                                                                          |
 |                                                                          |
 |                                                                          |
 |                                                                          |
 +--------------------------------------------------------------------------+

      Use the ^ and v keys to select which entry is highlighted.
      Press enter to boot the selected OS, `e' to edit the commands
      before booting or `c' for a command-line.
```

4. Log in as admin to the Web UI or CLI, and reconfigure the Nodegrid device.

System Certificate tool

A certificate can be loaded to the Nodegrid device from a connected local computer or a remote server. On the dialog, there are two sub-tabs: **Upload Certificate** and **Create CSR**.

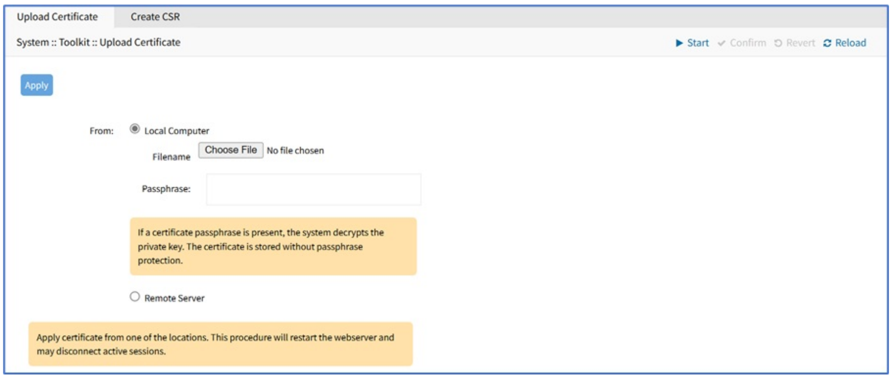
WARNING!

When the certificate is applied, the web server is restarted and active sessions are disconnected.

The protocols FTP, TFTP, SFTP, SCP, HTTP, and HTTPS are supported.

Upload Certificate

1. Go to *System :: Toolkit*.
2. Click **System Certificate** icon (displays *Upload Certificate* sub-tab dialog).



From: ● Local Computer

Filename Choose File No file chosen

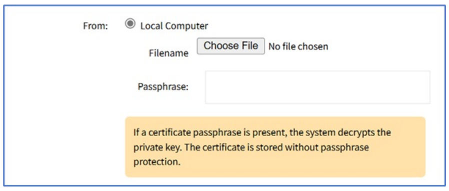
Passphrase:

If a certificate passphrase is present, the system decrypts the private key. The certificate is stored without passphrase protection.

○ Remote Server

Apply certificate from one of the locations. This procedure will restart the webserver and may disconnect active sessions.

3. On *From* menu, select one.
   - **Local Computer** radio button (expands dialog). Click **Choose File** (locate and select the file). Enter **Passphrase**.



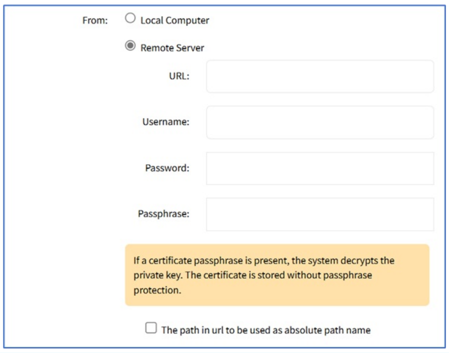
From: ● Local Computer

Filename Choose File No file chosen

Passphrase:

If a certificate passphrase is present, the system decrypts the private key. The certificate is stored without passphrase protection.

   - If **Remote Server** radio button selected (expands dialog).



From: ○ Local Computer

● Remote Server

URL:

Username:

Password:

Passphrase:

If a certificate passphrase is present, the system decrypts the private key. The certificate is stored without passphrase protection.

□ The path in url to be used as absolute path name

NOTE

Importing an encrypted certificate (with the Passphrase) is supported.

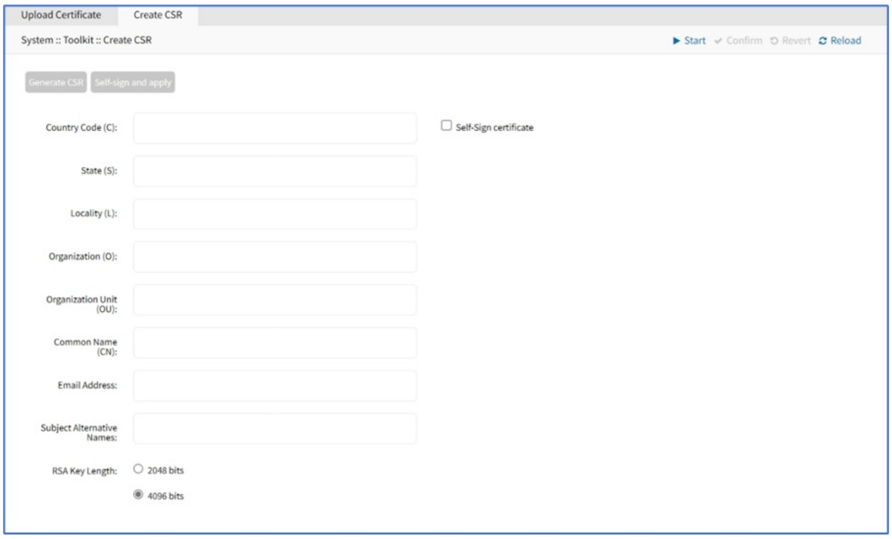
- Enter **URL**. (URL can be the IP address or hostname/FQDN. If using IPv6, use brackets [...]. Supported protocols: FTP, TFTP, SFTP, and SCP.)
- Enter **Username**, **Password**, and **Passphrase**.
- (optional) Select **The path in url to be used as absolute path name** checkbox.

4. Click **Apply**.

Create a Self-Sign Certificate

A self-sign certificate can be created and applied directly in the Nodegrid.

1. Go to *System :: Toolkit*.
2. Click **System Certificate** icon.
3. On the **Create CSR** sub-tab, enter details:



Country Code (C):

□ Self-Sign certificate

State (S):

Locality (L):

Organization (O):

Organization Unit (OU):

Common Name (CN):

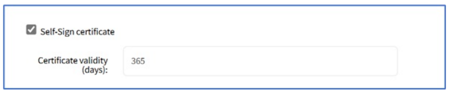
Email Address:

Subject Alternative Names:

RSA Key Length: ○ 2048 bits ● 4096 bits

a. **Country Code (C)**
b. **State (S)**
c. **Locality (L)**
d. **Organization (O)**
e. **Organization Unit (OU)**
f. **Common Name (CN)**
g. **Email Address**
h. (optional) Enter **Subject Alternative Names.**

4. Select **Self-Sign certificate checkbox** (expands dialog). Enter **Certificate validity (days)** value.



☑ Self-Sign certificate

Certificate validity (days): 365

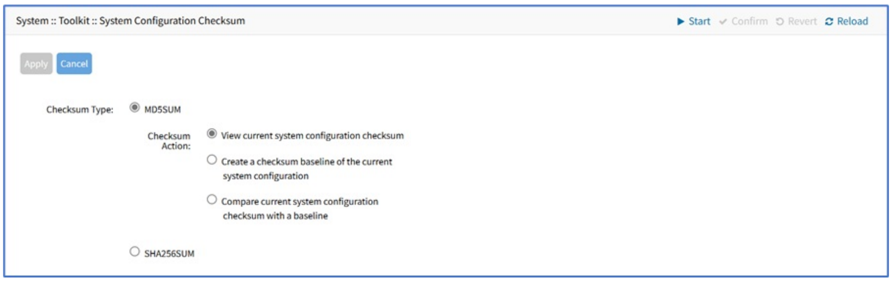
5. Click **Self-sign and apply.**

The page reloads after 10 seconds, and the certificate is applied.

System Configuration Checksum tool

This creates a checksum baseline of a specific current configuration. Administrators can use this quick tool to periodically verify if the configuration has changed.

1. Go to *System :: Toolkit*.
2. Click **System Configuration Checksum** icon (displays dialog).



System :: Toolkit :: System Configuration Checksum

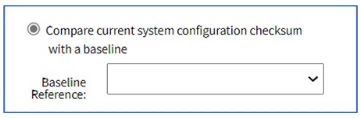
Checksum Type: ● MD5SUM

Checksum Action:
● View current system configuration checksum
○ Create a checksum baseline of the current system configuration
○ Compare current system configuration checksum with a baseline

○ SHA256SUM

3. On *Select Checksum Type*menu, select one:
   - **MD5SUM** radio button.
   - **SHA256SUM** radio button

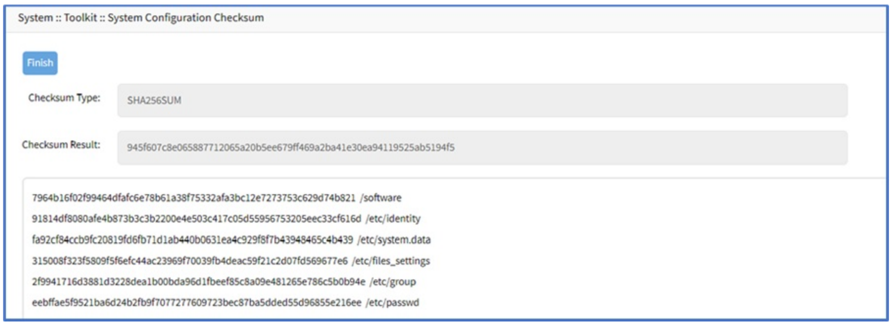
4. On *Checksum Action* menu, select one:
   - **View current system configuration checksum** radio button
   - **Create a checksum baseline of the current system configuration** radio button
   - **Compare current system configuration checksum with a baseline** radio button
   - On **Baseline Reference** drop-down, select one.



● Compare current system configuration checksum with a baseline

Baseline Reference:

5. Click **Apply** (displays results).



System :: Toolkit :: System Configuration Checksum

Checksum Type: SHA256SUM

Checksum Result: 945f607c8e065887712065a20b5ee679ff469a2ba41e30ea94119525ab5194f5

```
7964b16f02f99464dfafc6e78b61a38f75332afa3bc12e7273753c629d74b821  /software
91814df8080afe4b873b3c3b2200e4e503c417c05d55956753205eec33cf616d  /etc/identity
fa92cf84ccb9fc20819fd6fb71d1ab440b0631ea4c929f8f7b43948465c4b439  /etc/system.data
315008f323f5809f5f6efc44ac23969f70039fb4deac59f21c2d07fd569677e6  /etc/files_settings
2f9941716d3881d3228dea1b00bda96d1fbeef85c8a09e481265e786c5b0b94e  /etc/group
eebffae5f9521ba6d24b2fb9f7077277609723bec87ba5dded55d96855e216ee  /etc/passwd
```

6. Review the results. If the configurations match, the main result is "Passed". If any change, all altered locations are identified.
7. When done, click **Finish**.

Network Tools tool

This provides essential network communication tools ("ping", "traceroute" and "DNS lookup"). Output is displayed in the *Command Output* panel. Displays this dialog.

Send a Ping

This command-line utility checks if a network device is reachable. The command sends a request over the network to a specific device. If successful, a response from the device is displayed.

1. Go to *System :: Toolkit*.
2. Click **Network Tools** icon (displays dialog).
3. In the *Ping or Traceroute and IP Address* menu, enter **IP Address**.
4. On **Interface** drop-down, select one (selection depends on available interfaces: eth0, eth1, backplane0, backplane1, docker0, sit0, tap0, tap1, Source IP Address).
5. Click **Ping**.
6. Review results in *Command Output* panel.

Send a Traceroute

A traceroute sends ICMP (Internet Control Message Protocol) packets. Every router during the packet transfer is identified. This determines if the routers effectively transferred the data.

1. Go to *System :: Toolkit*.
2. Click **Network Tools** icon (displays dialog).
3. In the *Ping or Traceroute and IP Address* menu, enter **IP Address**
4. On **Interface** drop-down, select one (selection depends on available interfaces: eth0, eth1, backplane0, backplane1, docker0, sit0, tap0, tap1, Source IP Address).
5. Click **Traceroute**
6. Review results in *Command Output* panel.

Run a DNS Lookup

This process looks for the DNS record returned from a DNS server. Devices need to translate email addresses and domain names into meaningful numerical addresses.

1. Go to *System :: Toolkit*.
2. Click **Network Tools** icon.
3. In the *Perform a DNS Lookup* menu, enter **Host name**.
4. Click **Lookup**.
5. Review results in *Command Output* panel.

Detect MTU

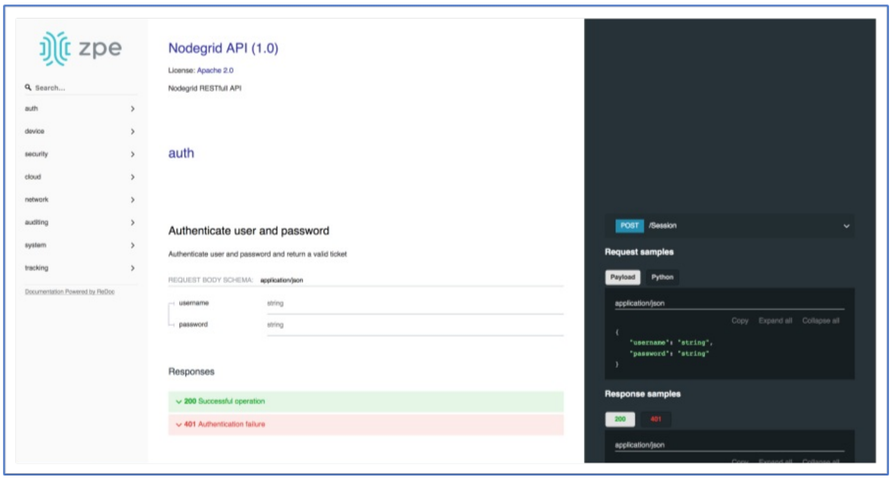
1. Go to *System :: Toolkit*.
2. Click **Network Tools** icon.
3. In the *Ping or Traceroute and IP Address* menu, enter **IP Address**.
4. On **Interface** drop-down, select one (selection depends on available interfaces: eth0, eth1, backplane0, backplane1, docker0, sit0, tap0, tap1, Source IP Address – enter Source IP Address).
5. Click **Detect MTU.**
6. Review results in *Command Output* panel.

API tool

RESTful API

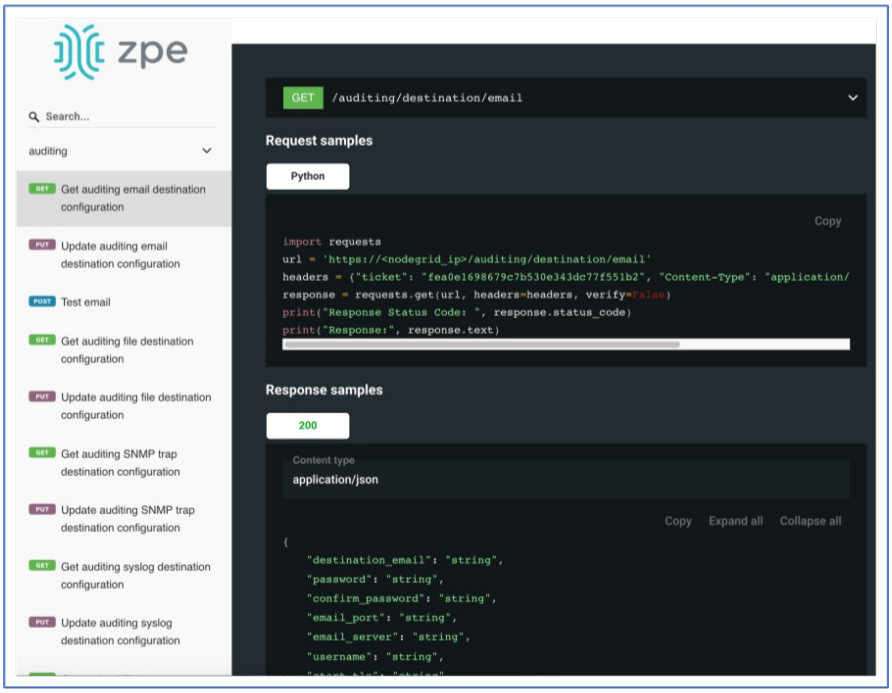
The Nodegrid Platform provides an embedded RESTful API. This provides API calls to access and modify the Nodegrid device configuration. Displays this dialog.

1. Go to *System :: Toolkit*.
2. Click on the **API** icon.
   Alternatively, on Banner, **User Name** drop-down (top right), click **API Documentation**.
3. On the left panel, click the **Right-arrow** to display API calls for that function. Request and Response examples are included.



```
{
    "username": "string",
    "password": "string"
}
```

Example: "get auditing email destination configuration"


zpe
Search...
auditing
GET Get auditing email destination configuration
PUT Update auditing email destination configuration
POST Test email
GET Get auditing file destination configuration
PUT Update auditing file destination configuration
GET Get auditing SNMP trap destination configuration
PUT Update auditing SNMP trap destination configuration
GET Get auditing syslog destination configuration
PUT Update auditing syslog destination configuration
GET /auditing/destination/email
Request samples
Python
Copy
Response samples
200
Content type
application/json
Copy Expand all Collapse all

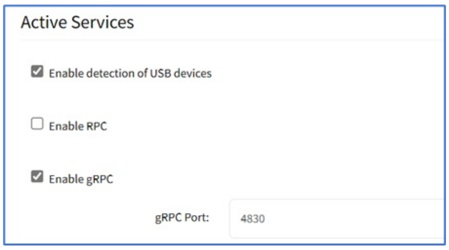
```
import requests
url = 'https://<nodegrid_ip>/auditing/destination/email'
headers = {"ticket": "fea0e1698679c7b530e343dc77f551b2", "Content-Type": "application/
response = requests.get(url, headers=headers, verify=False)
print("Response Status Code: ", response.status_code)
print("Response:", response.text)
```

```
{
    "destination_email": "string",
    "password": "string",
    "confirm_password": "string",
    "email_port": "string",
    "email_server": "string",
    "username": "string",
```

gRPC

The gRPC framework is supported (default: disabled). To enable gRPC:

1. Go to *Security :: .Services*.



☑ Enable detection of USB devices

☐ Enable RPC

☑ Enable gRPC

gRPC Port: 4830

2. In *Active Services*menu, enter details:
   a. Select **Enable gRPC** checkbox.
   b. Enter **gRPC Port**
3. Click **Save**.

gRPC is very scalable, performance-based RPC framework that uses simple service definitions and structured data.

There are four service definitions:

- get_request (APIRequest) - reads data. Returns (APIReply).
- post_request (APIRequest) - executes commands or add an entry. Returns (APIReply).
- put_request (APIRequest) - executes commands that need a selected entry or update an entry. Returns (APIReply).
- delete_request (APIRequest) - deletes existing data sets (or destroys a session). Returns (APIReply).

APIRequest expects three arguments:

- path - gRPC path to be used.
- ticket - authentication ticket for the request.
- data - structured data, in json format.

All three arguments follow the same structure as the existing REST API's. See https://<Nodegrid IP>/api_doc.html for more details.

APIReply returns two arguments:

- message - structured data in json format
- status_code - status_code as int32 number

Examples

post_request (Authentication - returns a session ticket)

None Copy

```
post_request({path: '/v1/Session', data: '{"username": "admin", "password": "admin"}'}, [...]
```

get_request (get network connection details)

None Copy

```
get_request({path: '/v1/network/connections', ticket: 'xxxxxxxxxxxxx'}, [...]
```

post_request (add a phone number to the sms whitelist)

None Copy

```
post_request({path: '/v1/system/sms/whitelist', ticket: 'xxxxxxxxxxxxx', data '{"name": "phone1", "phone_number": "+111111111111"}' }, [...]
```

put_request (update an existing value on the sms whitelist)

None Copy

```
put_request({path: '/v1/system/sms/whitelist/phone1', ticket: 'xxxxxxxxxxxxx', data '{"phone_number": "+122222222222"}' }, [...]
```

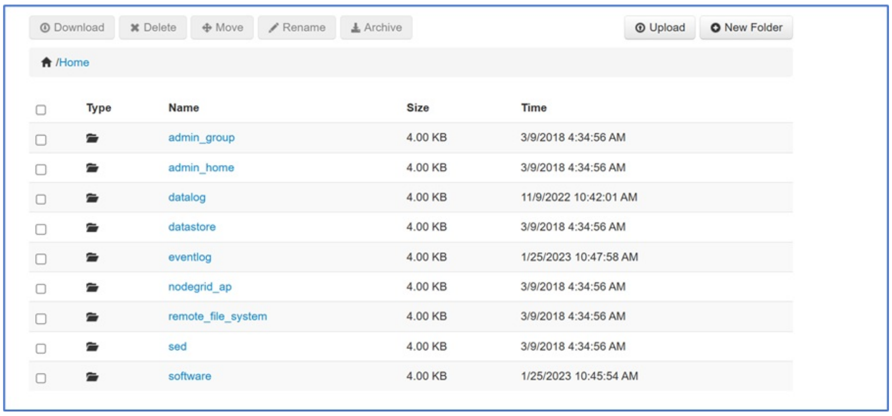
delete_request (delete an existing value on the sms whitelist)

None Copy

```
delete_request({path: '/v1/system/sms/whitelist', ticket: 'xxxxxxxxxxxxx', data '{"whitelists": [ "phone1", "phone2" ]}' }, [...]
```

File Manager tool

This displays the folder and file structure. To review folder contents, click on the folder name. Root (Home) folders cannot be renamed, deleted, or moved. The basic folder structure cannot be modified. This is only available to users with administrator privileges.



☐	Type	Name	Size	Time
☐	📂	admin_group	4.00 KB	3/9/2018 4:34:56 AM
☐	📂	admin_home	4.00 KB	3/9/2018 4:34:56 AM
☐	📂	datalog	4.00 KB	11/9/2022 10:42:01 AM
☐	📂	datastore	4.00 KB	3/9/2018 4:34:56 AM
☐	📂	eventlog	4.00 KB	1/25/2023 10:47:58 AM
☐	📂	nodegrid_ap	4.00 KB	3/9/2018 4:34:56 AM
☐	📂	remote_file_system	4.00 KB	3/9/2018 4:34:56 AM
☐	📂	sed	4.00 KB	3/9/2018 4:34:56 AM
☐	📂	software	4.00 KB	1/25/2023 10:45:54 AM

Download File

This downloads the selected file(s) in a folder. Only files can be downloaded.

1. Go to *System :: Toolkit*.
2. Click **File Manager** icon (opens a new browser tab with the folder system).
3. Navigate to the folder that contains the file.
4. Select the checkbox for each file to download.
5. Click **Download**.

Alternately, click on the *File Name* to download. Repeat as needed.

Delete File or Folder

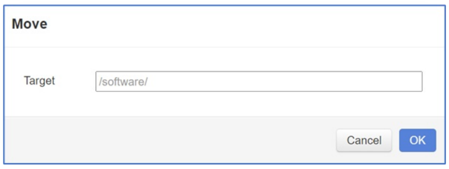
This deletes the selected files/folders.

1. Go to *System :: Toolkit*.
2. Click **File Manager** icon (opens a new browser tab).
3. At the file location, select checkbox(es).
4. Click **Delete**.

Move File or Folder

This moves the selected folders/files to a different folder location.

1. Go to *System :: Toolkit*.
2. Click **File Manager** icon (opens a new browser tab).
3. At the file location, select checkbox(es).
4. Click **Move**.
5. On the *Move* pop-up dialog, enter **Target** path.

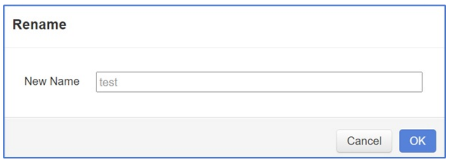


Target: /software/

6. Click **OK**.

Rename File or Folder

1. Go to *System :: Toolkit*.
2. Click **File Manager** icon (opens a new browser tab).
3. At the file location, select checkbox.
4. Click **Rename**.
5. On the *Rename* pop-up dialog, enter **New Name**.



New Name: test

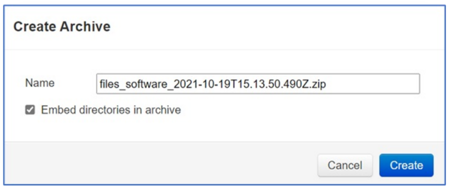
6. Click **OK**.

Archive File or Folder

When a root folder is archived, it is saved in the Home directory. It cannot be deleted or moved.

1. Go to *System :: Toolkit*.
2. Click **File Manager** icon (opens a new browser tab).
3. At the file location, select checkbox(es).
4. Click **Archive**.

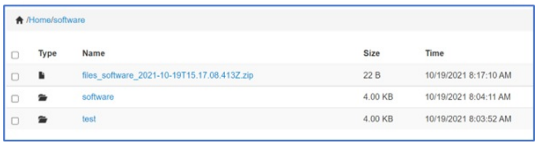
5. On the *Create Archive* pop-up dialog, confirm the **Name** (modify as needed). Select **Embed directories in archive** checkbox. Click **Create**.



Name files_software_2021-10-19T15.13.50.490Z.zip

☑ Embed directories in archive

The archive is saved in the same folder location. It can be renamed, moved, or downloaded, as needed.

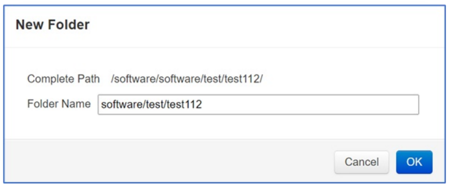


□	Type	Name	Size	Time
□		files_software_2021-10-19T15.17.08.413Z.zip	22 B	10/19/2021 8:17:10 AM
□		software	4.00 KB	10/19/2021 8:04:11 AM
□		test	4.00 KB	10/19/2021 8:03:52 AM

Create New Folder

Cannot be done in Home location.

1. Go to *System :: Toolkit*.
2. Click **File Manager** icon (opens a new browser tab).
3. Navigate to the folder location for the new folder.
4. Click **New Folder**.
5. On the *New Folder* pop-up dialog, enter **Folder Name**. Click **OK.**



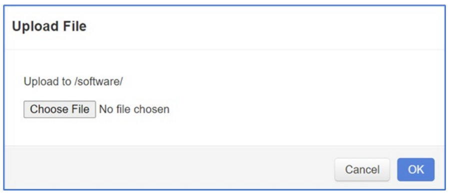
Complete Path /software/software/test/test112/

Folder Name software/test/test112

The new folder is added in that location.

Upload File

1. Go to *System :: Toolkit*.
2. Click **File Manager** icon (opens a new browser tab).
3. Navigate to the folder to contain the uploaded file.
4. Click **Upload**.
5. On the *Upload File* pop-up dialog, click **Choose File**. Locate and select the file, then click **OK**.



Upload to /software/

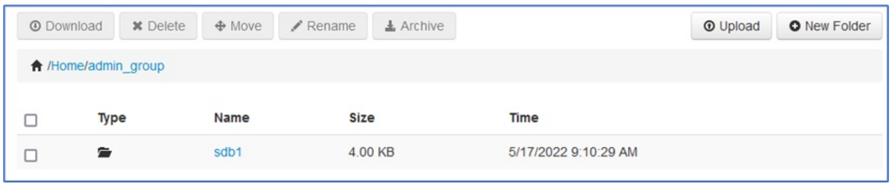
No file chosen

The file uploads and becomes available.

Access Additional Drive(s)/Drive Partitions

(available in v5.6+)

If additional drives/drive partitions are mounted on the Nodegrid device, these are shown on the *File Manager* page. These locations can be used to store VMs and Docker images. This is enabled only if the additional drive is mapped as "sdb" and formatted as ext2, ext3 or ext4. See the *Create sdb Storage* procedure (*Applications :: Virtual Machines*) and review the *Storage pools* section.

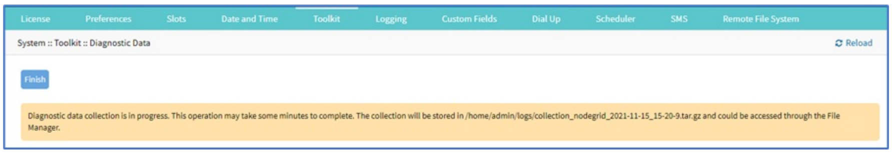


□	Type	Name	Size	Time
□		sdb1	4.00 KB	5/17/2022 9:10:29 AM

Diagnostic Data tool

This tool creates a report on the system status of the Nodegrid device. The contents help investigate the device's functionality. A series of commands output the state of the system, collect various log files, and copy the important configuration files. The output compacted file helps debug the system in case of any error or unexpected behavior.

The generated file is saved at:
/home/admin/logs/collection_nodegrid_XXXX-XX-XX_XX-XX-X.tar.gz

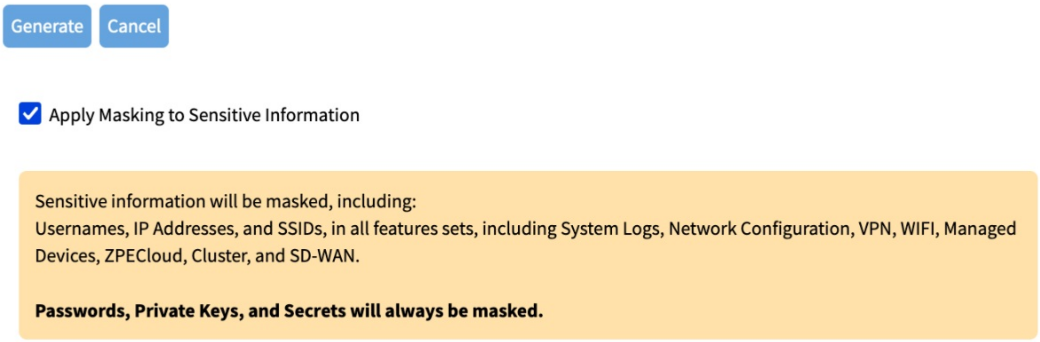


Diagnostic data collection is in progress. This operation may take some minutes to complete. The collection will be stored in /home/admin/logs/collection_nodegrid_2021-11-15_15-20-9.tar.gz and could be accessed through the File Manager.

Step 1 – Initiate Diagnostic Data

This runs the Diagnostic Data tool. The results are accessible in the File System or in the File Manager tool.

1. Go to *Systems :: Toolkit*.
2. Click the **Diagnostic Data** icon.
3. (Optionally) Uncheck the **Apply Masking to Sensitive Information** box to not mask the sensitive information in case support needs raw data for troubleshooting.

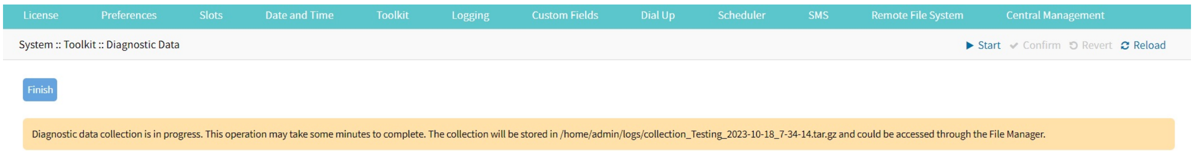


☑ Apply Masking to Sensitive Information

Sensitive information will be masked, including:
Usernames, IP Addresses, and SSIDs, in all features sets, including System Logs, Network Configuration, VPN, WIFI, Managed Devices, ZPECloud, Cluster, and SD-WAN.

Passwords, Private Keys, and Secrets will always be masked.

4. Click **Generate**.
5. The tool will run the diagnostics.



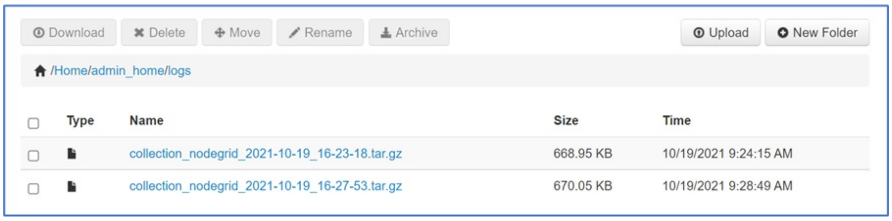
Diagnostic data collection is in progress. This operation may take some minutes to complete. The collection will be stored in /home/admin/logs/collection_Testing_2023-10-18_7-34-14.tar.gz and could be accessed through the File Manager.

6. When done, click **Finish** (returns to the *Toolkit* page).

Step 2 – Access the Diagnostic Data Results

(Admin privileges required.)

1. Go to *System :: Toolkit*.
2. Click the **File Manager** icon.
3. Go to folder: **/Home/admin_home/logs**.



□	Type	Name	Size	Time
□	🗎	collection_nodegrid_2021-10-19_16-23-18.tar.gz	668.95 KB	10/19/2021 9:24:15 AM
□	🗎	collection_nodegrid_2021-10-19_16-27-53.tar.gz	670.05 KB	10/19/2021 9:28:49 AM

4. Locate the tarball and select the checkbox.
5. Click **Download**.

Review the file, as needed.

Cloud Enrollment tool

This allows enrollment of the device in ZPE Cloud. Displays this dialog.

Enable Cloud Enrollment

1. Go to *System :: Toolkit*.
2. Click **Cloud Enrollment** icon (displays dialog)
3. In the *Cloud Enrollment* menu:
   a. Enter **URL** (of the Cloud application).
   b. Enter **Customer Code.**
   c. Enter **Enrollment Key.**
4. Click **Save**.

CLI Procedure

1. On the Access table, click **Console**.
2. On the CLI window, enter these parameters, then use “show” to confirm the configuration.

Plaintext Copy

```
[admin@nodegrid /]# cloud_enrollment
[admin@nodegrid {toolkit}]# <TAB><TAB>
cancel    commit    enroll    ls      set     show
[admin@nodegrid {toolkit}]# set <TAB><TAB>
customer_code=      enrollment_key=      url=
[admin@nodegrid {toolkit}]# set customer_code=12341234
[admin@nodegrid {toolkit}]# set enrollment_key=12341234
[admin@nodegrid {toolkit}]# set url=https://zpecloud.com
[admin@nodegrid {toolkit}]# show
status: Enrolled at https://zpecloud.com
url = https://zpecloud.com
customer_code = 12341234
enrollment_key = ********
[admin@nodegrid {toolkit}]# commit
```

For EU region:

Plaintext Copy

```
[admin@nodegrid /]# cloud_enrollment
[admin@nodegrid {toolkit}]# <TAB><TAB>
cancel    commit    enroll    ls      set     show
[admin@nodegrid {toolkit}]# set <TAB><TAB>
customer_code=      enrollment_key=      url=
[admin@nodegrid {toolkit}]# set customer_code=12341234
[admin@nodegrid {toolkit}]# set enrollment_key=12341234
[admin@nodegrid {toolkit}]# set url=https://zpecloud.eu
[admin@nodegrid {toolkit}]# show
status: Enrolled at https://zpecloud.eu
url = https://zpecloud.com
customer_code = 12341234
enrollment_key = ********
[admin@nodegrid {toolkit}]# commit
```

NOTE

To locate the Customer Code and Enrollment Key, log into your ZPE Cloud account and go to *Settings :: Enrollment*. (The **Enable Device Enrollment** checkbox must be enabled.)

To show ZPE Cloud enrollment settings:

Plaintext Copy

```
[admin@nodegrid /]# cd /settings/zpe_cloud/
[admin@nodegrid zpe_cloud]# show
enable_zpe_cloud = yes
zpe cloud url: https://zpecloud.com
enable_remote_access = yes
enable_file_protection = yes
passcode = ********
enable_file_encryption = no
[admin@nodegrid zpe_cloud]#
```

For EU region:

Plaintext Copy

```
[admin@nodegrid /]# cd /settings/zpe_cloud/
[admin@nodegrid zpe_cloud]# show
enable_zpe_cloud = yes
zpe cloud url: https://zpecloud.eu
enable_remote_access = yes
enable_file_protection = yes
passcode = ********
enable_file_encryption = no
[admin@nodegrid zpe_cloud]#
```

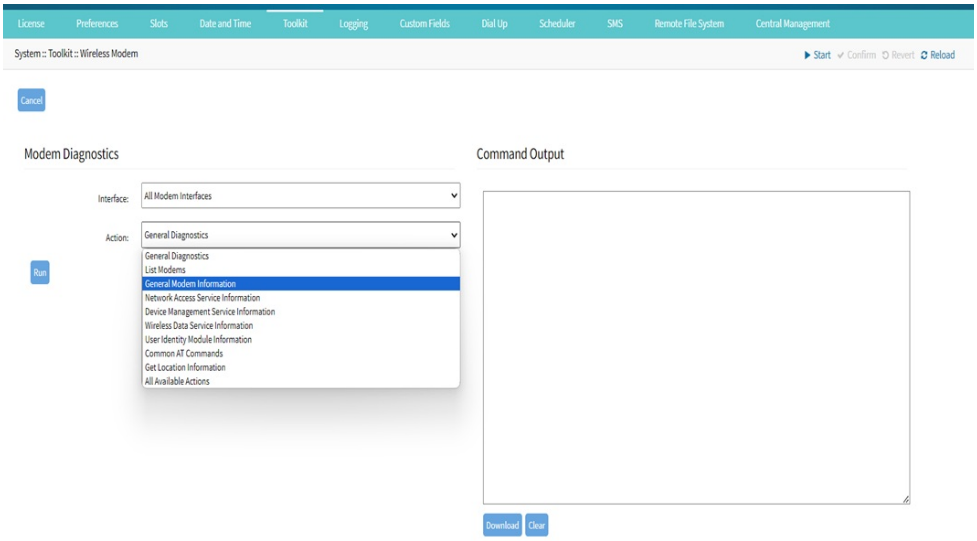
A confirmation is sent when the enrollment succeeds.

Once the ZPE Cloud is enabled on the device, access ZPE Cloud application to manage all enrolled devices. Access requires a company registration and an admin user account.

Wireless Modem

On this page, you can run diagnosis commands on the available Wireless Modems to resolve issues related to the modem. You can also view modem information, a list of modems, device management service information, and so on. You can execute individual actions on the modems or perform all these actions at once.

1. You can select the desired modem or select **All modem Interface** to select all the listed modems from the interface drop-down list.
2. Select the desired action from the Action drop-down list.
3. Click **Run**. The Command Output section displays the results of the command.



Interface: All Modem Interfaces

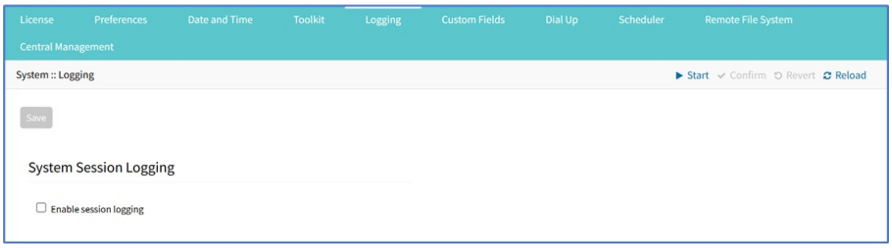
Action: General Diagnostics

Note: The Command Output section retains the previous output results. Click **Clear** to remove the previous results and populate only the newly executed command output results.

Logging tab

Data Logging is used to collect information and can also create event notifications. This is archived by defined alert strings (a simple text match or regular expression pattern string) that are evaluated against the data source stream. Events are automatically generated for each match.

Data logging can be enabled for all CLI sessions to be used for inspection and auditing. Data logs are stored locally or remotely (depending on Auditing settings).



System Session Logging

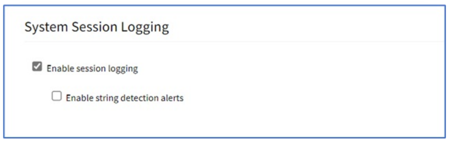
□ Enable session logging

Manage Logging

Enable Session Logging

Details can be modified, as needed.

1. Go to *System :: Logging*.
2. In *System Session Logging* menu:
   a. Select **Enable session logging** checkbox (expands dialog).

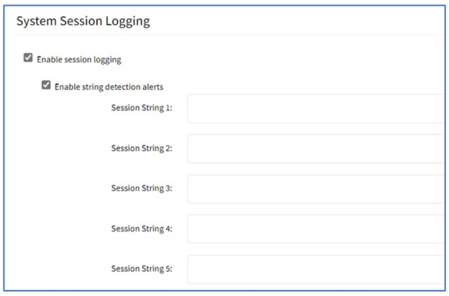


System Session Logging

☑ Enable session logging

□ Enable string detection alerts

   b. (optional) **Enable string detection alerts** checkbox (expands dialog). Enter **Session String** sets, as needed) that sends a notification alert upon occurrence.



System Session Logging

☑ Enable session logging

☑ Enable string detection alerts

Session String 1:

Session String 2:

Session String 3:

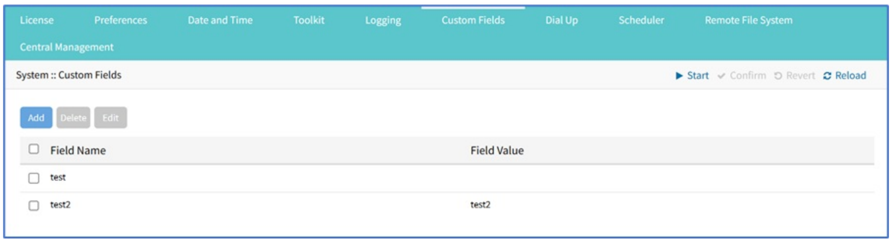
Session String 4:

Session String 5:

3. Click **Save**.

Custom Fields tab

Searchable custom fields can be created here. For example, add details not available by default. These custom fields become part of the device details.

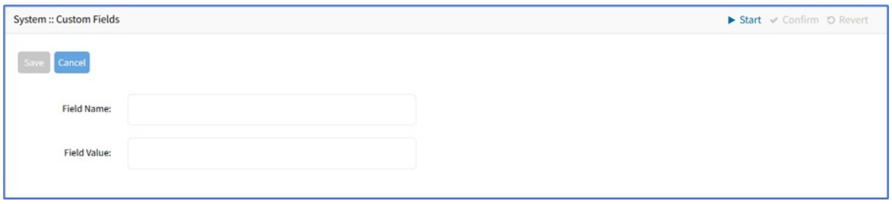


□	Field Name	Field Value
□	test	
□	test2	test2

Manage Custom Fields

Add Custom Field

1. Go to *System :: Custom Fields*.
2. Click **Add** (displays dialog).



   a. Enter **Field Name**.
   b. Enter **Field Value**.

3. Click **Save**.

Edit Custom Field

1. Go to *System :: Custom Fields*.
2. Select checkbox next to *Field Name*.
3. Click **Edit** (displays dialog).
4. Make changes, as needed.
5. Click **Save**.

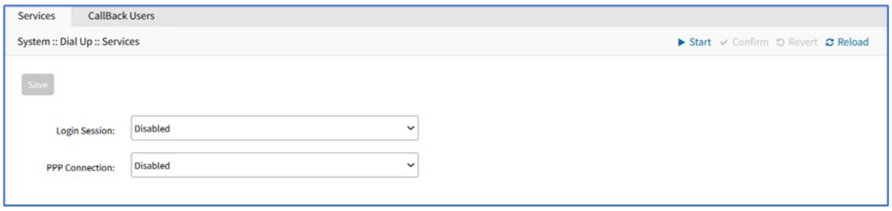
Delete Custom Field

1. Go to *System :: Custom Fields*.
2. Select checkbox next to *Field Name*.
3. Click **Delete**.

Dial-Up tab

Parameters for dialing to the device and callback users are configured here. Login and PPP connection features are also defined using the drop-down menu.

Services sub-tab



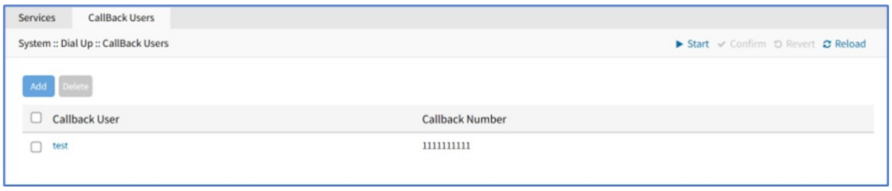
Login Session: Disabled

PPP Connection: Disabled

Manage Dial Up Services

1. Go to *System :: Dial Up :: Services*.
2. On **Login Session** drop-down, select one (Enabled, Disabled, Callback).
3. On **PPP Connection** drop-down, select one (Enabled, Disabled, Callback).
4. Click **Save**.

Callback Users sub-tab

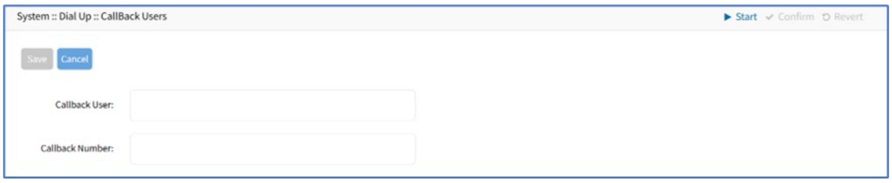


System :: Dial Up :: CallBack Users

□	Callback User	Callback Number
□	test	1111111111

Add Callback User

1. Go to *System :: Dial Up :: Callback Users*.
2. Click **Add** (displays dialog).



System :: Dial Up :: CallBack Users

Callback User:

Callback Number:

   a. Enter **Callback User.**
   b. Enter **Callback Number.**

3. Click **Save**.

Edit Callback User

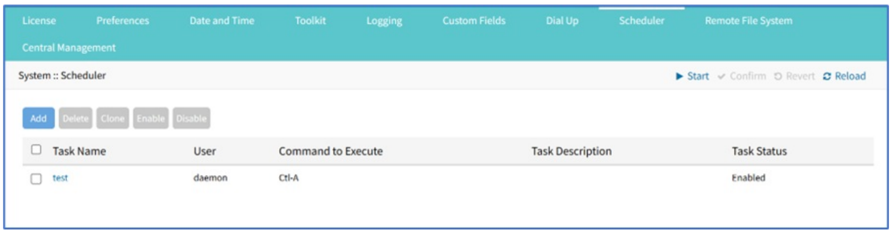
1. Go to *System :: Dial Up :: Callback Users*.
2. In *Callback User* column, click name.
3. Make changes as needed.
4. Click **Save**.

Delete Callback User

1. Go to *System :: Dial Up :: Callback Users*.
2. Select checkbox next to Callback User.
3. Click **Delete**.

Schedular tab

On this tab, administrators can execute tasks and scripts on a schedule. These can be maintenance tasks or automation tasks that include end devices.



□	Task Name	User	Command to Execute	Task Description	Task Status
□	test	daemon	Ctl-A		Enabled

The tasks must be a text file with Nodegrid CLI commands or script file located on the device. The file needs to be accessible and executable by the user.

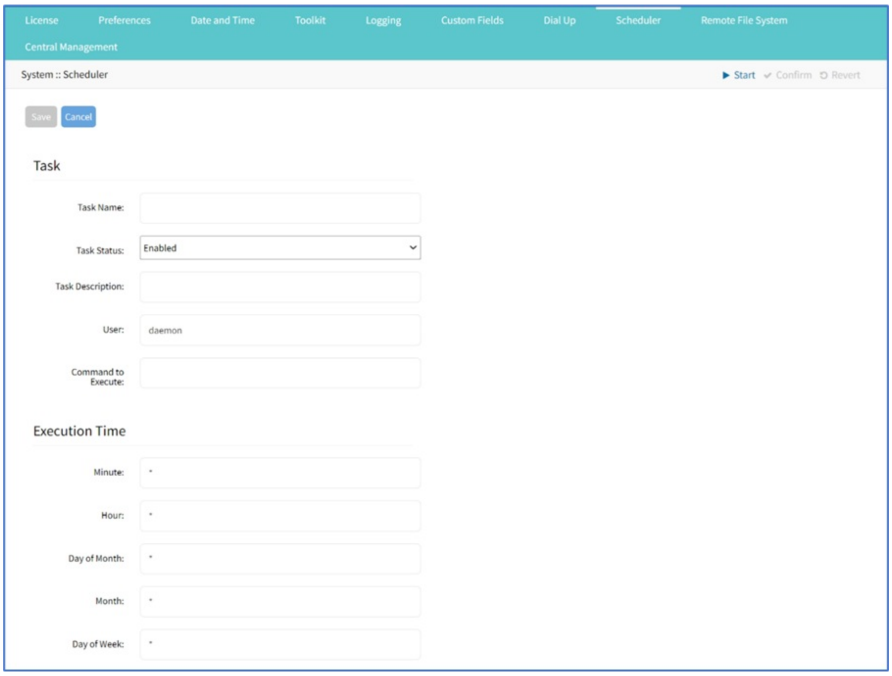
Manage Scheduled Tasks

Scheduler Date/Time examples

Factor	**Daily Task** **00:01 hours**	**Every Saturday:** **23:45 hours**	**Every Hour** **on the Hour**
Minute	1	45	0
Hour	0	23	*
Day of Month	*	*	*
Month	*	*	*
Day of Week	*	6	*

Add a Task

1. Go to *System :: Scheduler*.
2. Click **Add** (displays dialog).



Task

Task Name:

Task Status: Enabled

Task Description:

User: daemon

Command to Execute:

Execution Time

Minute: *

Hour: *

Day of Month: *

Month: *

Day of Week: *

3. In the *Task* menu,
   a. Enter **Task Name**.
   b. On **Task Status** drop-down, select one (Enabled, Disabled).
   c. (optional) Enter **Task Description**
   d. **User** (accept default)
   e. Enter **Command to Execute** (Shell command to execute)

4. In the *Execution Time* menu, modify fields as needed.
   a. **Minute** ('*', numbers [0 to 59], '2,3,4', '2-5', '3/12')
   b. **Hour** ('*', numbers [0 to 23], '0,4,8', '10-12', '4/7')
   c. **Day of month** ('*', numbers [1 to 31], '8,12,20', '10-20', '3/12')
   d. **Month** ('*', numbers [Jan=1, Feb=2, ..., Dec=12], '3,6,9,12', '1-5', '2/10')
   e. **Day of Week** ('*', numbers (Sun=0, Mon=1, ..., Sat=6), '0,4,6', '1-5', '1/4')

5. Click **Save**.

Edit a Task

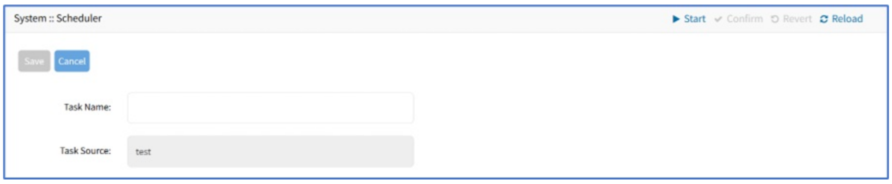
1. Go to *System :: Scheduler*.
2. In the *Task Name* column, click on the name (displays dialog).
3. Make changes as needed.
4. Click **Save**.

Delete a Task

1. Go to *System :: Scheduler*.
2. Select checkbox next to a task.
3. Click **Delete**
4. On confirmation dialog, click **OK**.

Clone a Task

1. Go to *System :: Scheduler*.
2. In the *Task Name* column, click checkbox next to the task to be cloned.
3. Click **Clone** (displays dialog).



Task Name:

Task Source: test

4. Enter **Task Name**.
5. As needed, edit the cloned task.
6. Click **Save**.

Enable a Task

1. Go to *System :: Scheduler*.
2. In the *Task Name* column, select checkbox of a disabled task.
3. Click **Enable**.

Disable a Task

1. Go to *System :: Scheduler*.
2. In the *Task Name* column, select checkbox of an enabled task.
3. Click **Disable** (to disable task).

SMS tab (installed cellular module)

This feature is only available on devices with the cellular module installed: Nodegrid Services Router, Bold SR, Gate SR, Link SR, and Hive SR (loaded with M2/wireless modem).

Actions can be run remotely with an SMS incoming message. The SMS message authentication must be valid. Only allowed actions are executed.

By default, Enable Actions via incoming SMS is disabled. When enabled in the default state (no password), the device accepts SMS-triggered actions from all phone numbers. The MAC address of ETH0 is the default password.

The SMS option requires that the SIM card and plan be SMS-enabled. This can be checked with the service provider. It is recommended to check the costs for this service, as some actions can respond with multiple SMS.

Settings sub-tab

Enable Incoming SMS Actions

1. Go to *System :: SMS :: Settings*.
2. In *SMS Actions Settings* menu, select **Enable Actions via Incoming SMS** checkbox (displays dialog). Enter **Password**.
3. In *Allowed SMS Actions*menu, select/unselect checkboxes (as needed):
   - **apn - configure temporary APN** checkbox (configure a temporary APN).
   - **simswap - temporary swap SIM card** checkbox (triggers a SIM card failover).
   - **connect and disconnect - on/off data connection** checkbox (triggers a modem to connect or disconnect).
   - **mstatus - request wireless modem status** checkbox (returns current modem status)
   - **reset - reset wireless modem** checkbox (triggers a modem reset).
   - **info - request information about Nodegrid** checkbox (returns *About* information).
   - **factorydefault - factory default Nodegrid** checkbox (factory default of the Nodegrid device is triggered).
   - **reboot - reboot Nodegrid** checkbox (triggers device reboot).
4. Click **Save**.

CLI Examples: SMS Actions and Messages

The format of SMS actions and subsequent response is given in the list below. Some actions may not require a response.

Format

```
Message format: < password >;< action >;< argument >;
   Response: <response>;
```

apn (configure temporary APN)

```
< password >;apn;<new apn>;
```

simswap (swap sim card temporary)

```
< password >;simswap;<timeout for sim to register in secs. max 180>;
Modem will reset to swap sim;
```

connect (try to power on data connection)

```
< password >;connect;
Connect action started;
```

disconnect (drop current data connection)

```
< password >;disconnect;
Disconnect action started;
```

mstatus (request modem status)

```
< password >;mstatus;
Service:< LTE|WCDMA >;RSSI:< value dbm >;SIM:< sim number in use >;State:< status >;APN:< apn in use >;IP addr:< ip address when connected >
```

reset (reset wireless modem)

```
< password >;reset;
Modem Reset will start soon;
```

info (request device information)

```
< password >;info;
Model: < Nodegrid model >; Serial Number: < Nodegrid serial number >; Version: < firmware version >;
```

factorydefault (restore Nodegrid configuration to factory default)

```
< password >;factorydefault;
Nodegrid will restore configuration to factory default and reboot;
```

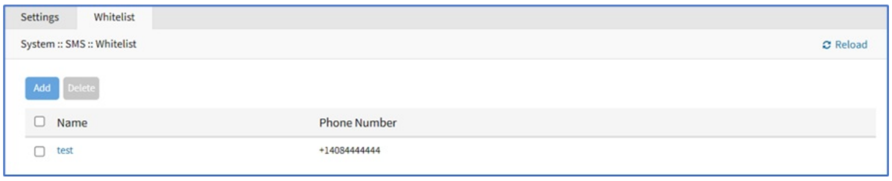
reboot (reboot Nodegrid device)

None Copy

```
< password >;reboot;
Nodegrid will reboot soon;
```

Whitelist sub-tab

On the table, administrators can add, delete, or change phone numbers which can send SMS action triggers. Requests from all other phone numbers are ignored.

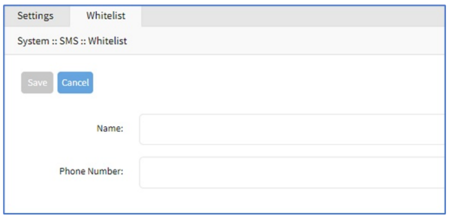


□ Name	Phone Number
□ test	+14084444444

If the whitelist table is empty, requests from all phone numbers are accepted.

Add Entry to Whitelist

1. Go to *System :: SMS :: Whitelist*.
2. Click **Add** (displays dialog).

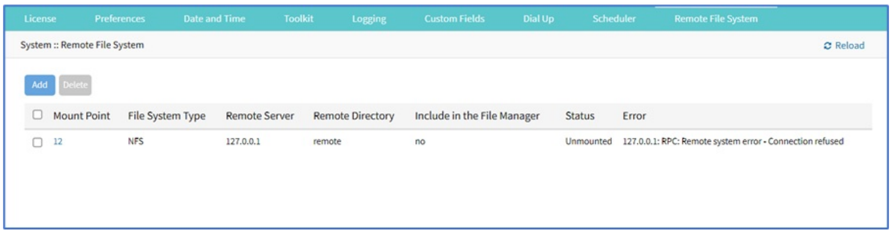


   a. Enter **Name**
   b. Enter **Phone Number**

3. Click **Save**.

Remote File System tab

This designates remote file system folders.

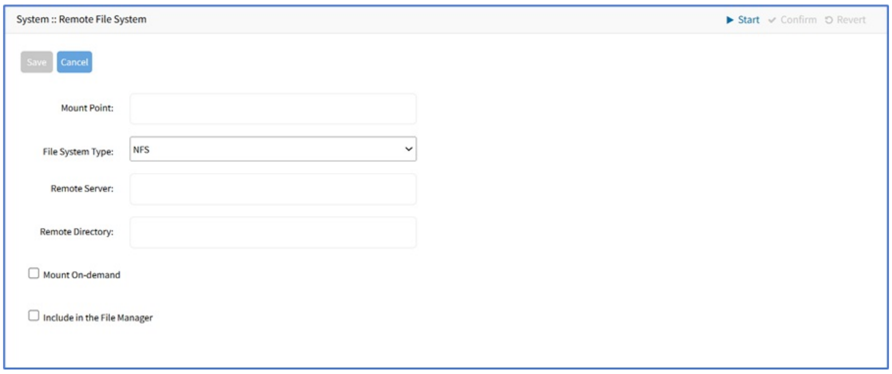


□	Mount Point	File System Type	Remote Server	Remote Directory	Include in the File Manager	Status	Error
□	12	NFS	127.0.0.1	remote	no	Unmounted	127.0.0.1: RPC: Remote system error - Connection refused

Manage Remote File System

Add Remote File System: NFS

1. Go to *System :: Remote File System*.
2. Click **Add** (displays dialog).



System :: Remote File System

▶ Start ✓ Confirm ⟲ Revert

Save Cancel

Mount Point:

File System Type: NFS

Remote Server:

Remote Directory:

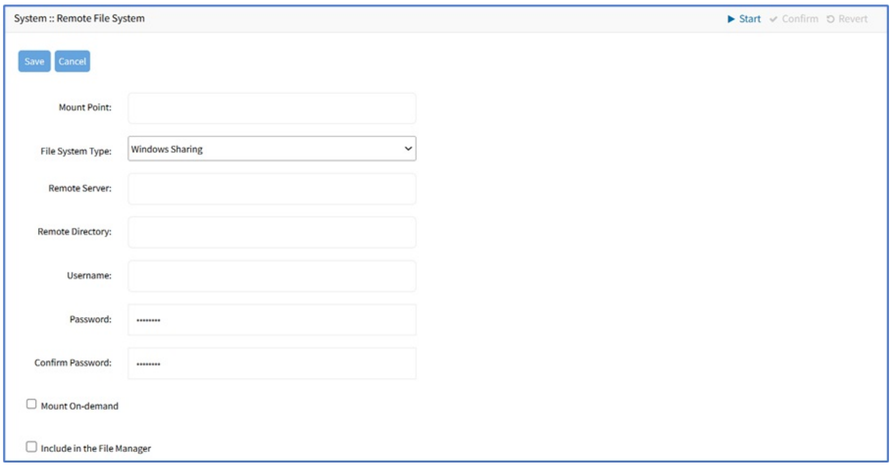
□ Mount On-demand

□ Include in the File Manager

3. Enter details:
   a. **Mount Point**
   b. **File System Type** drop-down, select **NFS**
   c. **Remote Server**
   d. **Remote Directory**
   e. (optional) **Mount On-demand** checkbox
   f. (optional) **Include in the File Manager** checkbox
4. Click **Save**.

Add Remote File System: Windows Sharing

1. Go to *System :: Remote File System*.
2. Click **Add** (displays dialog).



System :: Remote File System

▶ Start ✓ Confirm ⟲ Revert

Save Cancel

Mount Point:

File System Type: Windows Sharing

Remote Server:

Remote Directory:

Username:

Password: ••••••••

Confirm Password: ••••••••

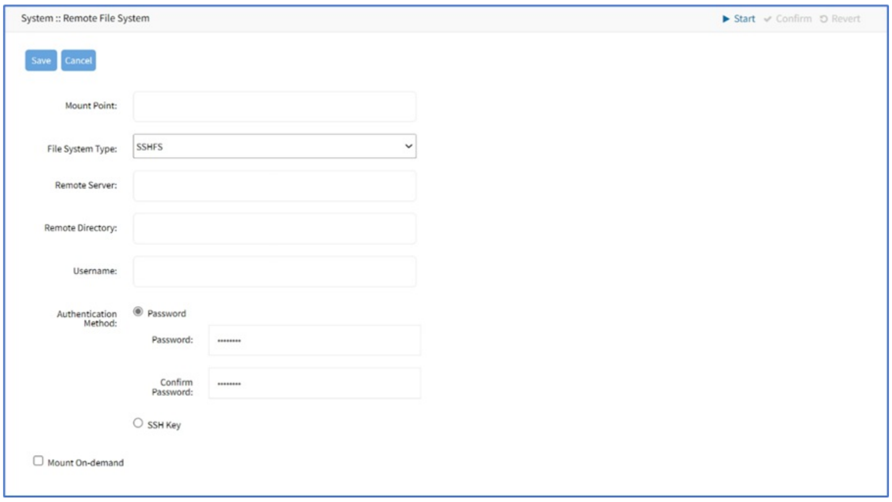
□ Mount On-demand

□ Include in the File Manager

3. Enter details:
   a. **Mount Point**
   b. **File System Type** drop-down, select **Windows Sharing**
   c. **Remote Server**
   d. **Remote Directory**
   e. **Username**
   f. **Password**
   g. **Confirm Password**
   h. (optional) **Mount On-demand** checkbox
   i. (optional) **Include in the File Manager** checkbox
4. Click **Save**.

Add Remote File System: SSHFS

1. Go to *System :: Remote File System*.
2. Click **Add** (displays dialog).



Mount Point:

File System Type: SSHFS

Remote Server:

Remote Directory:

Username:

Authentication Method: ● Password

Password: ••••••••

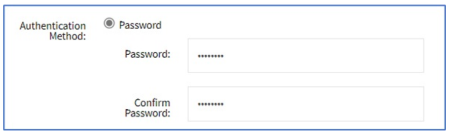
Confirm Password: ••••••••

○ SSH Key

☐ Mount On-demand

3. Enter details:
    a. **Mount Point**
    b. **File System Type** drop-down, select **SSHFS**.
    c. **Remote Server**
    d. **Remote Directory**
    e. **Username**

4. On *Authentication Method* menu, select one:
    a. **Password** radio button (expands dialog). Enter **Password** and **Confirm Password**.

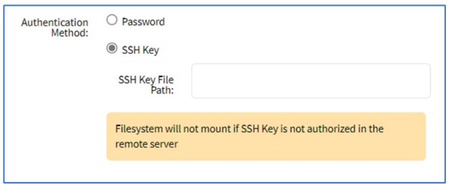


Authentication Method: ● Password

Password: ••••••••

Confirm Password: ••••••••

    b. **SSH Key** radio button (expands dialog). Enter **SSH Key File Path**.



Authentication Method: ○ Password

● SSH Key

SSH Key File Path:

Filesystem will not mount if SSH Key is not authorized in the remote server

    c. (optional) **Mount On-demand** checkbox
    d. (optional) **Include in the File Manager** checkbox

5. Click **Save**.

Edit Remote File System

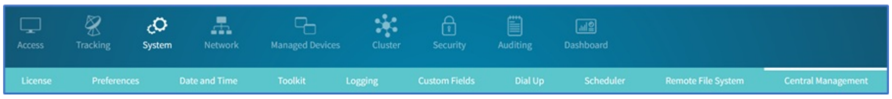
1. Go to *System :: Remote File System*.
2. Click on the name in the *Mount Point* column.
3. On the dialog, make changes, as needed.
4. Click **Save**.

Delete Remote File System

1. Go to *System :: Remote File System*.
2. Select checkbox next to name.
3. Click **Delete**.
4. On the confirmation dialog, click **OK**.

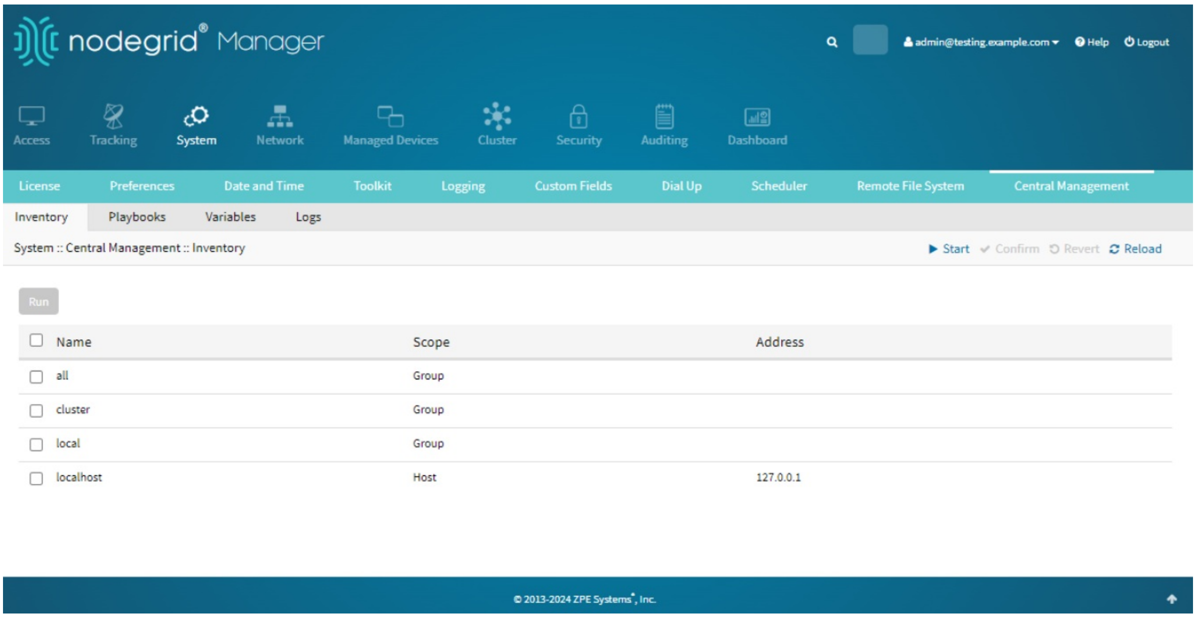
Central Management tab

The Central management allows an admin user to run Ansible Playbooks on a set of peers in the cluster. This can only be done from the Coordinator device.



Inventory sub-tab

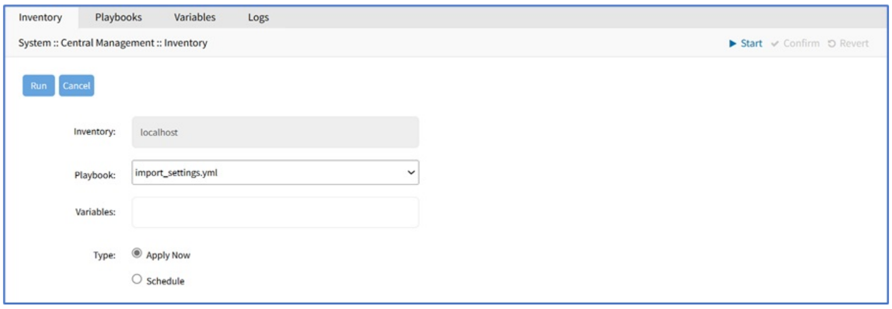
In this tab, you can view the peers that have Peer Management enabled in a cluster. These are devices that can be selected to run a Playbook. This page also lists the ansible inventories associated with your Nodegrid device. When you run an `ansible-inventory --list` command in Ansible, all the inventories are listed on the **Inventory** tab. For a coordinator, the peers of Cluster are automatically added to the ansible inventory.



□ Name	Scope	Address
□ all	Group	
□ cluster	Group	
□ local	Group	
□ localhost	Host	127.0.0.1

Run Inventory Item

1. Go to *System :: Central Management :: Inventory*.
2. In the table, select the checkbox of name to run.
3. Click **Run** (displays dialog).



Inventory: localhost

Playbook: import_settings.yml

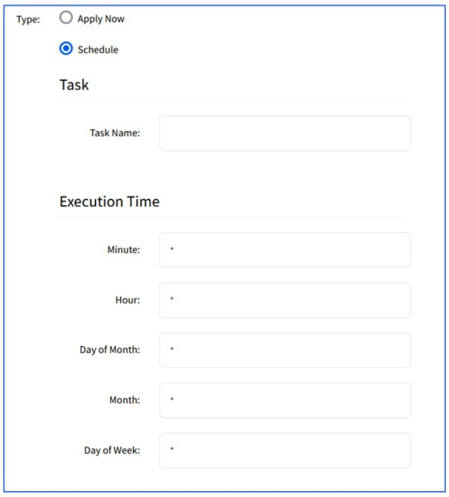
Variables:

Type: ● Apply Now ○ Schedule

4. From the **Playbook** drop-down, select one.
5. Enter **Variables**. (Variables entered here have priority over variables created in the *Variables* tab.)

> **Examples**
>
> name=value
> name="value with space"
> name1=value1 name2=value2
> {"name":"value"}
> @/tmp/custom_vars_file.yml

6. On *Type* menu, select one:
   a. **Apply Now** radio button
   b. **Schedule** radio button (expands dialog)



Type: ○ Apply Now

● Schedule

Task

Task Name:

Execution Time

Minute: *

Hour: *

Day of Month: *

Month: *

Day of Week: *

In the *Task* menu, enter **Task Name**.

In the *Execution Time* menu, enter details (see table below).

7. Click **Run**.

> **NOTE**
>
> Scheduled tasks can be managed on *System* :: *Scheduler* tab.

Execution Time Date/Time examples

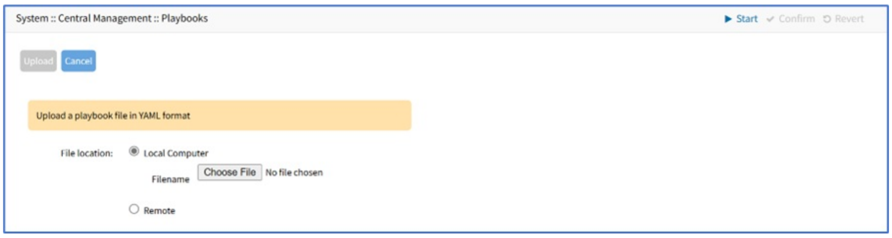
Factor	Daily Task: 00:01 hours	Every Saturday: 23:45 hours	Every Hour on the Hour
Minute	1	45	0
Hour	0	23	*
Day of Month	* (every day)	*	*
Month	* (every month)	*	*
Day of Week	* (every day of week)	6	*

Playbooks sub-tab

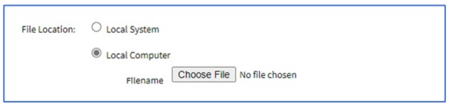
The table lists the Ansible Playbooks files available for selection on the Inventory tab. Files can be uploaded and deleted.

Upload Playbook

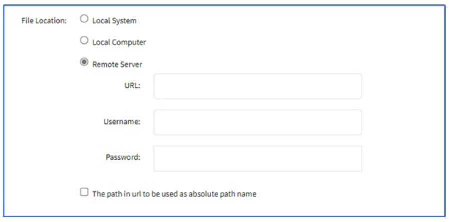
1. Go to *System :: Central Management :: Playbooks*.
2. Click **Upload** (displays dialog).



3. On *File Location* menu, select one:
   - **Local Computer** radio button (expands dialog). Click **Browse**. Locate and select the file.



   - **Remote Server** radio button (expands dialog).

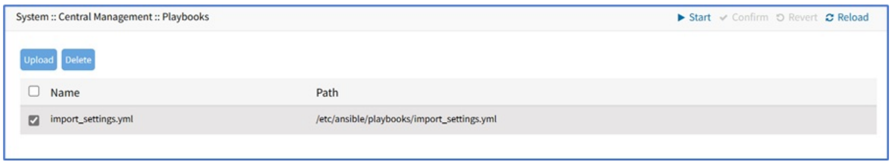


     - Enter **URL**. (URL can be the IP address or hostname/FQDN. If using IPv6, use brackets [...]. Supported protocols: FTP, TFTP, SFTP, and SCP.)
     - Enter **Username** and **Password**.
     - (optional) Select **The path in url to be used as absolute path name** checkbox.

4. Click **Upload**.

Delete Playbook

1. Go to *System :: Central Management :: Playbooks*.
2. Select checkbox of name to be deleted.

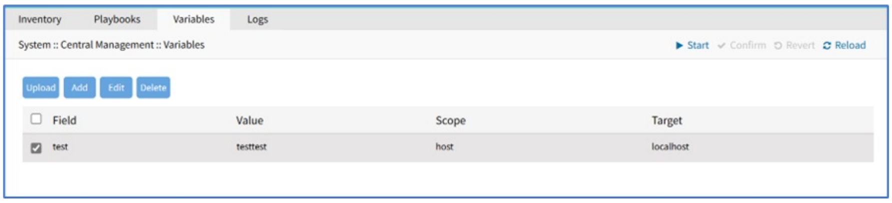


□	Name	Path
☑	import_settings.yml	/etc/ansible/playbooks/import_settings.yml

3. Click **Delete**.

Variables sub-tab

This tab lists the specific host variables used in Playbooks. The user can upload a CSV variables file or manually create variables.

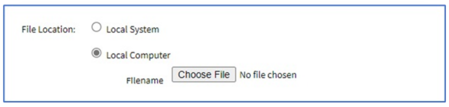


System :: Central Management :: Variables

□ Field	Value	Scope	Target
☑ test	testtest	host	localhost

Upload Variable

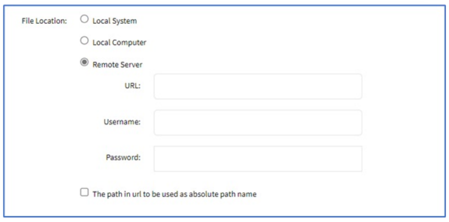
1. Go to *System :: Central Management :: Variables*.
2. Click **Upload** (displays dialog).
3. On *File Location* menu, select one:
   - **Local Computer** radio button (expands dialog). Click **Browse**. Locate and select the file.

     File Location: ○ Local System ● Local Computer

     Filename No file chosen

   - **Remote Server** radio button (expands dialog):

     File Location: ○ Local System ○ Local Computer ● Remote Server

     URL:

     Username:

     Password:

     □ The path in url to be used as absolute path name

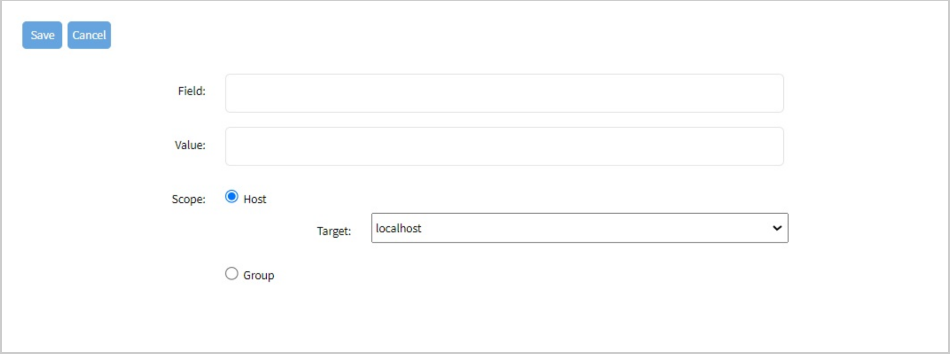
     - Enter **URL**. (URL can be the IP address or hostname/FQDN. If using IPv6, use brackets [...]. Supported protocols: FTP, TFTP, SFTP, and SCP.)
     - Enter **Username** and **Password**.
     - (optional) Select **The path in url to be used as the absolute path name** checkbox.
4. Click **Upload**.

> **CVS file content example:**
>
> field,value,scope,target
>
> session_timeout,1200,host,peer1.localdomain

Add Variable

You can add variables for a host and a group of hosts.

1. Go to *System :: Central Management :: Variables*.
2. Click **Add** (displays dialog).

   Field:

   Value:

   Scope: ● Host

   Target: localhost

   ○ Group

   a. Enter **Field**.
   b. Enter **Value**.
   c. Under the **Scope** section, select the variables for **Host** from the **Target** drop-down list.
   d. Similarly, select the Group field and the variables from the **Target** drop-down list.
3. Click **Save**.

Edit Variable

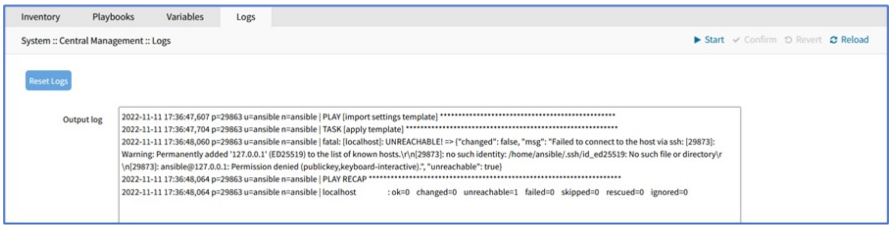
1. Go to *System :: Central Management :: Variables*.
2. Select the checkbox of the item to be edited.
3. Click **Edit**.
4. On the dialog, make changes as needed.
5. Click **Save**.

Delete Variable

1. Go to *System :: Central Management :: Variables*.
2. Select checkbox of name to be deleted.
3. Click **Delete**.

Logs sub-tab

The Logs tab show activity of the Ansible Playbook execution.



```
2022-11-11 17:36:47,607 p=29863 u=ansible n=ansible | PLAY [import settings template] ************************************************
2022-11-11 17:36:47,704 p=29863 u=ansible n=ansible | TASK [apply template] **********************************************************
2022-11-11 17:36:48,060 p=29863 u=ansible n=ansible | fatal: [localhost]: UNREACHABLE! => {"changed": false, "msg": "Failed to connect to the host via ssh: [29873]:
Warning: Permanently added '127.0.0.1' (ED25519) to the list of known hosts.\r\n[29873]: no such identity: /home/ansible/.ssh/id_ed25519: No such file or directory\r
\n[29873]: ansible@127.0.0.1: Permission denied (publickey,keyboard-interactive).", "unreachable": true}
2022-11-11 17:36:48,064 p=29863 u=ansible n=ansible | PLAY RECAP *********************************************************************
2022-11-11 17:36:48,064 p=29863 u=ansible n=ansible | localhost          : ok=0   changed=0   unreachable=1   failed=0   skipped=0   rescued=0   ignored=0
```

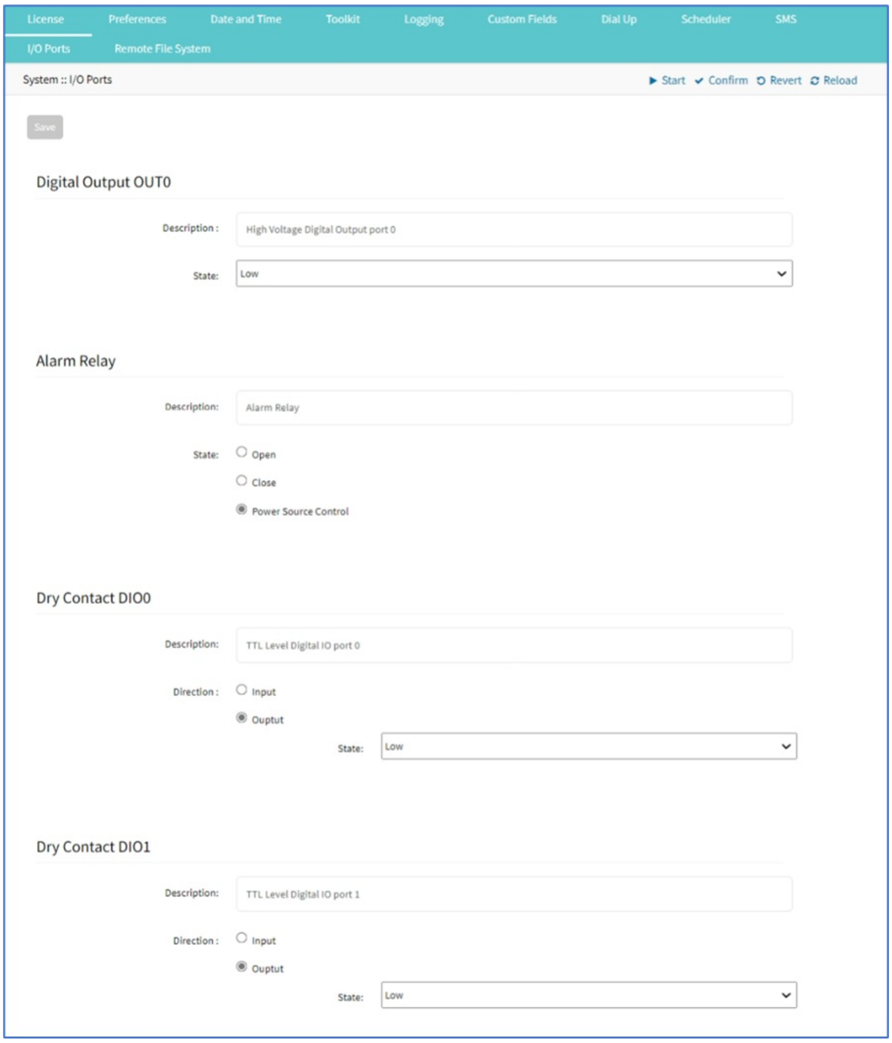
Reset Log

1. Go to *System :: Central Management :: Logs*.
2. Click **Reset Logs** (clears the *Output Log* panel.

I/O Ports tab (only with GPIO)

> **NOTE**
>
> This tab is displayed only if the Nodegrid device is equipped with GPIO (Digital I/O ports).

This sets the configuration of the state of digital outputs and DIO0/DIO1 as input or output. When DIO0/DIO1 is configured as output, the state can be set to Low or High.



Digital Output OUT0

Description : High Voltage Digital Output port 0

State: Low

Alarm Relay

Description: Alarm Relay

State: ○ Open ○ Close ● Power Source Control

Dry Contact DIO0

Description: TTL Level Digital IO port 0

Direction : ○ Input ● Ouptut

State: Low

Dry Contact DIO1

Description: TTL Level Digital IO port 1

Direction : ○ Input ● Ouptut

State: Low

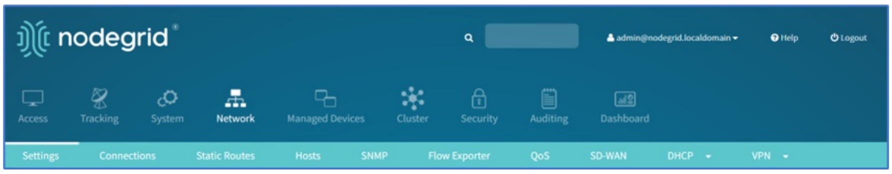
Configure I/O Port Settings

Use the procedure to set up the I/O Port configuration.

1. In *Digital Output OUT0* menu, enter **Description**.
   On **State** drop-down, select one (Low, High).
2. In *Alarm Relay* menu, enter **Description**.
3. On *State*menu, select one:
   - **Open** radio button
   - **Close** radio button
   - **Power Source Control** radio button
4. In *Dry Contact DIO0* menu, enter **Description**.
   a. On *Direction*, select one:
      - **Input** radio button
      - **Output** radio button – on **State** drop-down, select one (Low, High)
5. In *Dry Contact DIO1* menu, enter **Description**.
   a. On *Direction*, select one:
      - **Input** radio button
      - **Output** radio button – on **State** drop-down, select one (Low, High).
6. Click **Save**.

Network Section

Administrators can configure and adjust all network-related settings, including network configuration, LTE, WIFI interfaces, bounding, and VLAN details.



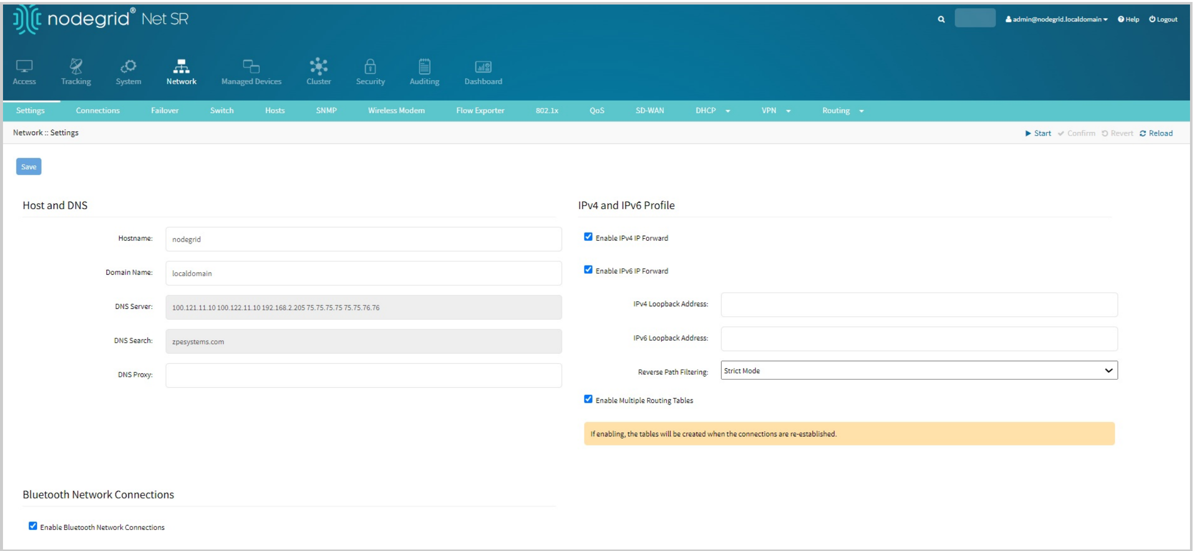
NOTE

Nodegrid currently supports the FRRouting suite. For more information, see http://docs.frrouting.org/en/latest/

Settings tab

Administrators can define network details in the network settings page. To configure network settings:

1. Go to *Network :: Settings*.



Network :: Settings

Host and DNS

Hostname: nodegrid

Domain Name: localdomain

DNS Server: 100.121.11.10 100.122.11.10 192.168.2.205 75.75.75.75 75.75.76.76

DNS Search: zpesystems.com

DNS Proxy:

IPv4 and IPv6 Profile

☑ Enable IPv4 IP Forward

☑ Enable IPv6 IP Forward

IPv4 Loopback Address:

IPv6 Loopback Address:

Reverse Path Filtering: Strict Mode

☑ Enable Multiple Routing Tables

If enabling, the tables will be created when the connections are re-established.

Bluetooth Network Connections

☑ Enable Bluetooth Network Connections

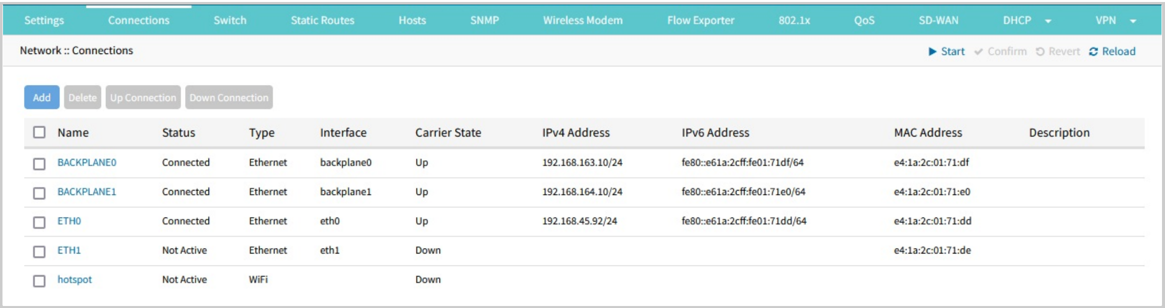
2. In the *Host & DNS* menu, enter:
   a. **Hostname**
   b. **Domain Name**
   c. (**DNS Server** and **DNS Search** are read-only.)
   d. **DNS Proxy**
3. In *IPv4 and IPv6 Profile* menu (select one or both IP Forwards to route network traffic between network interfaces):

   > **NOTE**
   >
   > IPv4 and IPv6 IP Forward is automatically selected if SD-WAN is enabled on the device.

   a. **Enable IPv4 IP Forward** checkbox (enables routing stack for IPv4 traffic)
   b. **Enable IPv6 IP Forward** checkbox (enables routing stack for IPv6 traffic)
   c. **IPv4 Loopback Address** (address is assigned a bitmask of /32)
   d. **IPv6 Loopback Address** (address is assigned a bitmask of /128)
4. On **Reverse Path Filtering** drop-down, select one:
   - **Disabled** (no source address validation is performed).
   - **Strict** (Each incoming packet is tested against the routing table and if the interface represents the best return path. If the packet cannot be routed or is not the best return path. it is dropped.)
   - **Loose** (Each incoming packet is tested only against the routing table. If the packet cannot be routed, it gets dropped. This allows for asymmetric routing scenarios.)
5. If **Enable Multiple Routing Tables** checkbox is selected, tables are created when connections re-established.
6. In *Blue Tooth Network Connections* menu (applies only if Bluetooth is enabled), select **Enable Bluetooth Network Connections** checkbox.
7. Click **Save**.

Connections tab

Administrators can edit, add, delete, and turn up or down existing network connections.



Network :: Connections

□	Name	Status	Type	Interface	Carrier State	IPv4 Address	IPv6 Address	MAC Address	Description
□	BACKPLANE0	Connected	Ethernet	backplane0	Up	192.168.163.10/24	fe80::e61a:2cff:fe01:71df/64	e4:1a:2c:01:71:df	
□	BACKPLANE1	Connected	Ethernet	backplane1	Up	192.168.164.10/24	fe80::e61a:2cff:fe01:71e0/64	e4:1a:2c:01:71:e0	
□	ETH0	Connected	Ethernet	eth0	Up	192.168.45.92/24	fe80::e61a:2cff:fe01:71dd/64	e4:1a:2c:01:71:dd	
□	ETH1	Not Active	Ethernet	eth1	Down			e4:1a:2c:01:71:de	
□	hotspot	Not Active	WiFi		Down				

Some connections are automatically available, depending on the device model, hardware setup, and system profile. Some connections will attempt to get an IP with DHCPv4 requests, and have fixed fallback IP addresses in case a DHCP server is not available:

- ETH0: 192.168.160.10/24
- ETH1: 192.168.161.10/24
- hotspot: 192.168.162.1/24
- SFP0 (BACKPLANE0 instead in NSR devices): 192.168.163.10/24
- SFP1 (BACKPLANE1 instead in NSR devices): 192.168.164.10/24

These addresses can be used to reach the Nodegrid device by connecting it directly to a client device and adjusting the client's network configuration manually.

On NSR devices in Out-Of-Band profile, the BACKPLANE0 connection is reachable from any of the embedded switch interfaces, except for sfp1. The BACKPLANE1 connection is reachable only from the sfp1 interface.

The "hotspot" connection is a WiFi hotspot that will serve the network "NodeGrid", its password being the Serial Number of the Nodegrid device. It will be available by default if the device supports it.

Any of these default configurations can be changed or removed if desired, and new connections can be added.

When a network connection is added, the page fields change depending on the **Type** drop-down selection.

Add Bonding Interface

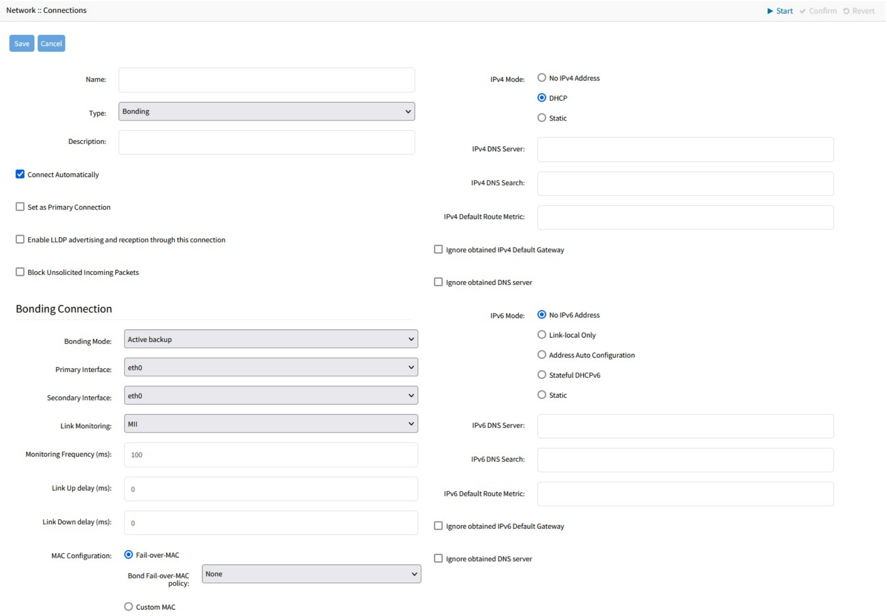
With bonding interfaces, the system can bond two or more physical network interfaces to one interface. All physical interfaces in the bond act as one interface. This allows for an active failover between the interfaces if an interface's physical connection is interrupted.

The built-in Network Failover can do the same. The main difference is that the built-in feature Network Failover works on the IP layer for more functionality. A bonding interface works on the link layer.

> NOTE
>
> - The Network Failover and Bonding functions can be combined.
> - When using a Bonding interface, ensure that the DNS configuration is valid (reachable DNS). This allows the Nodegrid device to reconnect to the ZPE Cloud.

The administrator can define normal network settings (IP address, bitmask, and other settings) for the bonding interface.

1. Go to *Network :: Connections*.
2. Click **Add** (displays dialog).
3. Enter **Name**.
4. On **Type** drop-down, select **Bonding** (dialog changes).



Network :: Connections

▶ Start ✔ Confirm ↺ Revert

Save Cancel

Name:

Type: Bonding

Description:

☑ Connect Automatically

□ Set as Primary Connection

□ Enable LLDP advertising and reception through this connection

□ Block Unsolicited Incoming Packets

Bonding Connection

Bonding Mode: Active backup

Primary Interface: eth0

Secondary Interface: eth0

Link Monitoring: MII

Monitoring Frequency (ms): 100

Link Up delay (ms): 0

Link Down delay (ms): 0

MAC Configuration: ● Fail-over-MAC

Bond Fail-over-MAC policy: None

○ Custom MAC

IPv4 Mode: ○ No IPv4 Address ● DHCP ○ Static

IPv4 DNS Server:

IPv4 DNS Search:

IPv4 Default Route Metric:

□ Ignore obtained IPv4 Default Gateway

□ Ignore obtained DNS server

IPv6 Mode: ● No IPv6 Address ○ Link-local Only ○ Address Auto Configuration ○ Stateful DHCPv6 ○ Static

IPv6 DNS Server:

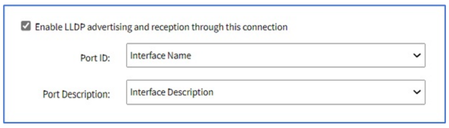
IPv6 DNS Search:

IPv6 Default Route Metric:

□ Ignore obtained IPv6 Default Gateway

□ Ignore obtained DNS server

5. Enter **Description**.
6. Select checkboxes as needed:
   a. If **Connect Automatically** checkbox is selected, connection is automatically established at startup.
   b. **Set as Primary Connection** checkbox (defines interface as the primary connection. Only one interface can be the primary.)
   c. **Enable LLDP advertising and reception through this connection** checkbox. On **Port ID** drop-down, select one. On **Port Description** drop-down, select one.



☑ Enable LLDP advertising and reception through this connection

Port ID: Interface Name

Port Description: Interface Description

   d. **Block Unsolicited Incoming Packets** checkbox (automatically blocks all inbound connections on the interface).

7. In *Bonding Connection* menu, **Bonding Mode** drop-down, select one (dialog changes):
   - **Round-robin** (packets transmitted in sequential order from first available slave through the last)
   - **Active backup** (only one slave in the bond is active. A different slave becomes active if, and only if, the active slave fails)
   - **XOR load balancing** (transmit based on the selected transmit hash policy)
   - **Broadcast** (transmits everything on all slave interfaces)
   - **802.3ad(LACP)** (IEEE 802.3ad Dynamic link aggregation. Creates aggregation groups that share the same speed and duplex settings. Utilizes all slaves in the active aggregator according to the 802.3ad specification. Slave selection for outgoing traffic is done according to the transmit hash policy)
   - **Adaptive Transmit load balancing** (channel bonding that does not require any special switch support. Outgoing traffic is distributed according to the current load (computed relative to the speed) on each slave. Incoming traffic is received by the current slave)
   - **Adaptive load balancing** (includes balance-TLB plus receive load balancing - RLB for IPV4 traffic. Does not require any special switch support. Receive load balancing is achieved by ARP negotiation)

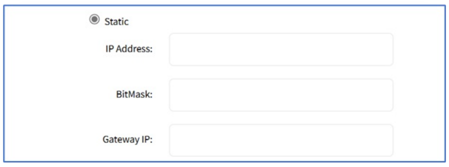
8. Enter the list of interfaces that participate on the bond:
   - **Primary Interface** and **Secondary Interface** drop-down menus (when Active backup mode is selected)
   - **Slave(s)** interface(s) (comma separated) (when any other mode is selected)

9. Configure the Link Monitoring method according to the chosen bonding mode:
   - **Link Monitoring** drop-down, select one (MII, ARP):
     - **MII** (monitors the carrier state as sensed by the interface). The following configuration options apply to this mode:
       - **Monitoring Frequency (ms)** (how often the link state of each slave is inspected for link failure)
       - **Link Up delay (ms)** (time to wait before enabling a slave after a link recovery has been detected. Should be a multiple of **Monitoring Frequency**)
       - **Link Down delay (ms)** (time to wait before disabling a slave after a link failure has been detected. Should be a multiple of **Monitoring Frequency**)
     - **ARP** (monitors connectivity to another host on the local network by regularly generating ARP probes). The following configuration options apply to this

mode:

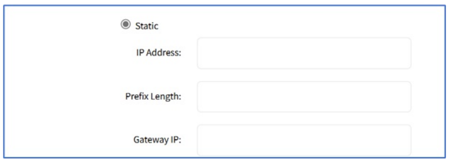
- **Monitoring Frequency (ms)** (how often to check if slaves have recently sent or received traffic, and generate ARP probes)
- **ARP target** (an IP address to use as target for the ARP requests)
- **ARP validate** (whether or not ARP probes and replies should be validated):
    - **None** (No validation is performed)
    - **Active** (Validation is performed only for the active slave)
    - **Backup** (Validation is performed only for the backup slave(s))
    - **All** (Validation is performed for all slaves)

10. Configure the MAC address policy (applicable only to **Active backup** bonding mode):
    - **MAC Configuration** checkbox, select one (Fail-over-MAC, Custom MAC). This will dictate how the MAC address for the interface will be determined:
        - **Fail-over-MAC,** select a **Bond Fail-over-MAC policy:**
            - **None** (sets the primary, secondary, and bond interfaces to the same MAC address at the point of assignment. This address may change on system reboot)
            - **Current Active Interface** (the MAC address of the bond shall always be the MAC address of the currently active port. The MAC addresses of the primary/secondary interfaces are not changed; instead, the MAC address of the bond interface changes during a failover)
            - **Follow Active Interface** (similar to **None**, but the backup interface's MAC is not changed at assignment. When failover happens, the new active interface is assigned the bond interface MAC)
        - **Custom MAC:**
            - Enter a custom, persistent **MAC Address** to be used by the bonding interface
11. For bonding modes XOR load balancing, 802.3ad(LACP), Adaptive Transmit load balancing, select one **Transmit Hash Policy** drop-down value (Layer 2, Layer 2 and 3, Layer 3 and 4, Layer 2 and 3 and Encap, Layer 3 and 4 and Encap)
12. For bonding mode 802.3ad(LACP), configure the remaining settings:
    - **System Priority** value
    - **Actor MAC address**
    - **User Port Key**
    - **LACP rate** drop-down, select one (Slow, Fast)
    - **Aggregation Selection Logic** drop-down, select one (Stable, Bandwidth, Count)
13. In *IPv4 Mode* menu, enter details:
    a. **No IPv4 Address** radio button
    b. **DHCP** radio button
    c. **Static** radio button (if selected, expands dialog). Enter **IP Address**, **BitMask**, and (optional) **Gateway IP**.



    d. (optional) **IPv4 DNS Server**
    e. **IPv4 DNS Search** (defines a domain name for DNS lookups)
    f. **IPv4 Default Route Metric**
    g. **Ignore obtained IPv4 Default Gateway** checkbox
    h. **Ignore obtained DNS server** checkbox

14. In *IPv6 Mode* menu, enter details:
    a. **No IPv6 Address** radio button
    b. **Link local Only** radio button.
    c. **Address Auto Configuration** radio button
    d. **Stateful DHCPv6** radio button
    e. (If **Static** radio button is selected, displays menu) Enter **IP Address**, **Prefix Length**, and (optional) **Gateway IP**.

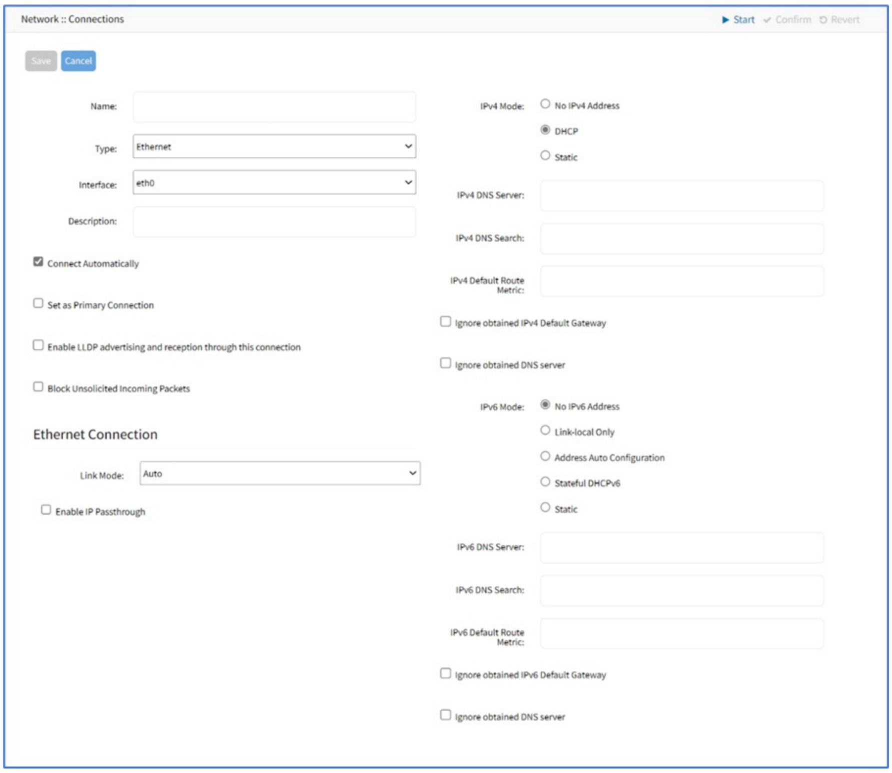


15. (optional) **IPv6 DNS Server**
    a. **IPv6 DNS Search** (defines domain name for DNS lookups)
    b. **IPv6 Default Route Metric**
    c. **Ignore obtained IPv6 Default Gateway** checkbox
    d. **Ignore obtained DNS server** checkbox
16. Click **Save**.

Add Ethernet Interface

Additional Ethernet interfaces can be added and configured when an additional physical interface is added. This can occur during a Nodegrid Manager installation, where the System might have more than two interfaces to better support network separation.

1. Go to *Network :: Connections*.
2. Click **Add** (displays dialog).
3. Enter **Name**.
4. On **Type** drop-down, select **Ethernet** (dialog changes).



Network :: Connections ▶ Start ✓ Confirm ↻ Revert

Save Cancel

Name:

Type: Ethernet

Interface: eth0

Description:

☑ Connect Automatically

□ Set as Primary Connection

□ Enable LLDP advertising and reception through this connection

□ Block Unsolicited Incoming Packets

Ethernet Connection

Link Mode: Auto

□ Enable IP Passthrough

IPv4 Mode: ○ No IPv4 Address ● DHCP ○ Static

IPv4 DNS Server:

IPv4 DNS Search:

IPv4 Default Route Metric:

□ Ignore obtained IPv4 Default Gateway

□ Ignore obtained DNS server

IPv6 Mode: ● No IPv6 Address ○ Link-local Only ○ Address Auto Configuration ○ Stateful DHCPv6 ○ Static

IPv6 DNS Server:

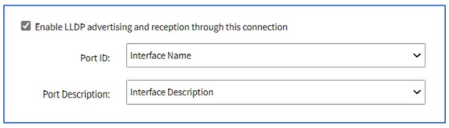
IPv6 DNS Search:

IPv6 Default Route Metric:

□ Ignore obtained IPv6 Default Gateway

□ Ignore obtained DNS server

5. Enter **Description**.
6. If the **Connect Automatically** checkbox is selected, the connection is automatically established at startup.
7. **Set as Primary Connection** checkbox (defines interface as the primary connection. Only one interface can be the primary.)
8. If **Enable LLDP advertising and reception through this connection** checkbox is selected. On the **Port ID** drop-down, select one. On **Port Description** drop-down, select one.



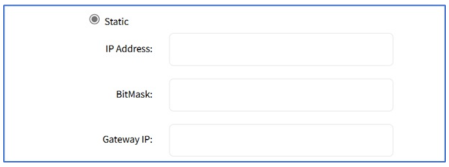
☑ Enable LLDP advertising and reception through this connection

Port ID: Interface Name

Port Description: Interface Description

9. Select the **Block Unsolicited Incoming Packets** checkbox (automatically blocks all inbound connections on the interface).
10. In the *Ethernet Connection* menu, on the **Link Mode** drop-down (availability depends on the interface and the device model), enable the **Auto** selection or select the forced or advertised speed/duplex (options vary depending upon the hardware and SFP transceiver used). You can navigate to the path *Tracking:: Network:: Interface* or execute the command "ethtool <*interface*>" from the shell access to view the configured speed/duplex.
11. On the **Enable IP Passthrough** checkbox (expands dialog) enter the details:
    a. **Ethernet Connection** drop-down, select one (selection varies depending on device)
    b. **MAC Address** (if blank, the system uses DHCP to get the device)
    c. **Port Intercepts** (any ports that should NOT pass through the Nodegrid device).

12. In *IPv4 Mode* menu, enter details:
    a. **No IPv4 Address** radio button
    b. **DHCP** radio button
    c. **Static** radio button (if selected, expands dialog). Enter **IP Address**, **BitMask**. and (optional) **Gateway IP**.



● Static

IP Address:

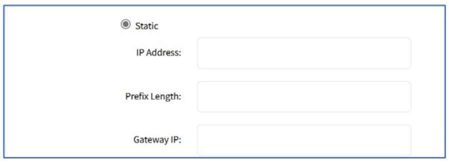
BitMask:

Gateway IP:

    d. (optional) **IPv4 DNS Server**
    e. **IPv4 DNS Search** (defines a domain name for DNS lookups)
    f. **IPv4 Default Route Metric**
    g. **Ignore obtained IPv4 Default Gateway** checkbox
    h. **Ignore obtained DNS server** checkbox

13. In *IPv6 Mode* menu, enter details:
    a. **No IPv6 Address** radio button
    b. **Link local Only** radio button.
    c. **Address Auto Configuration** radio button
    d. **Stateful DHCPv6** radio button

e. If **Static** radio button is selected (displays menu). Enter **IP Address**, **Prefix Length**, and (optional) **Gateway IP.**



◉ Static

IP Address:

Prefix Length:

Gateway IP:

14. (optional) Enter **IPv6 DNS Server.**
    a. **IPv6 DNS Search** (defines domain name for DNS lookups)
    b. **IPv6 Default Route Metric**
    c. **Ignore obtained IPv6 Default Gateway** checkbox
    d. **Ignore obtained DNS server** checkbox

15. Click **Save**.

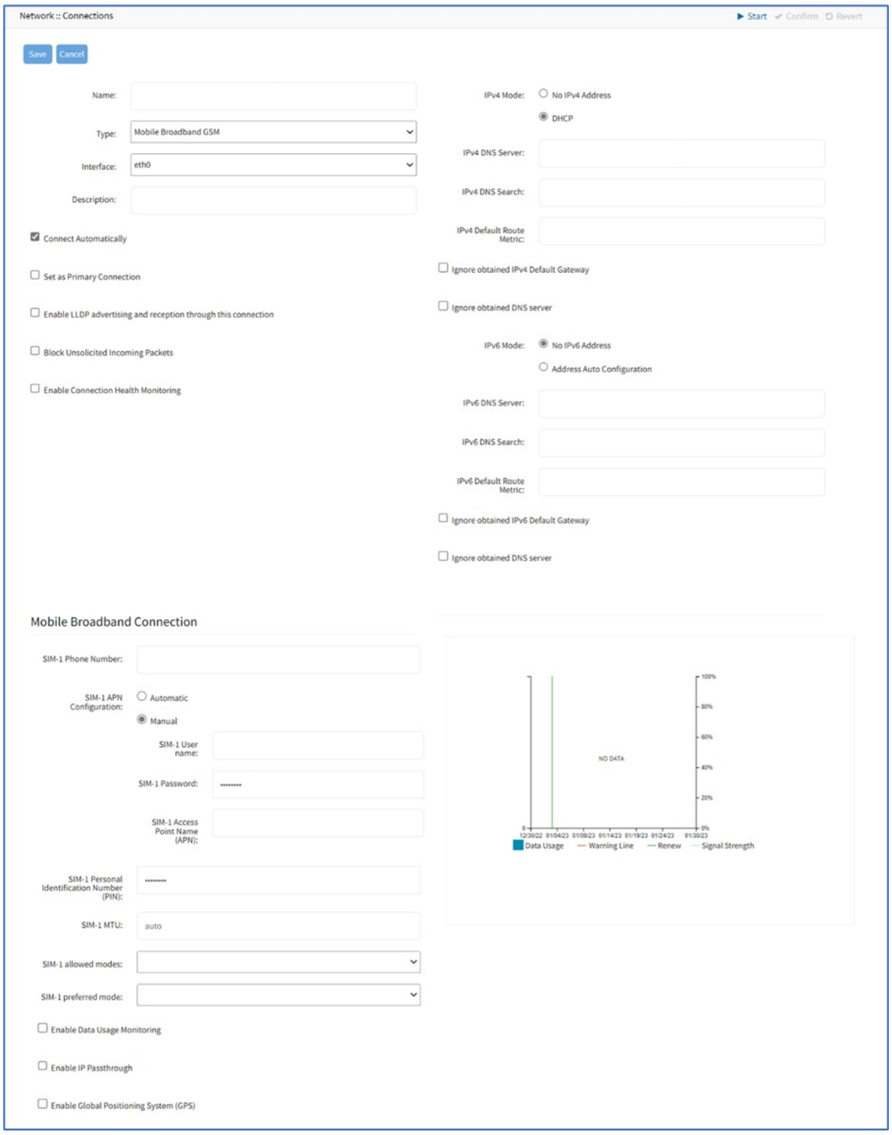
Add Mobile Broadband GSM Interface

Mobile Broadband interfaces can be configured when a mobile broadband modem is available to the device. The Nodegrid SR family (NSR, GSR, BSR, LSR, HSR) support built-in modems available as optional add-ons. For all other units, external modems can be used.

The created interfaces allow the system to establish an Internet connection most used for failover options. Users and remote systems can directly access the device through a mobile connection (if supported by the ISP).

An APN (provided by the carrier) is required for all cellular connections. For more information on APNs, see https://support.zpesystems.com/portal/kb/articles/what-is-the-apn-for-my-nsr-or-bsr-to-connect-to-4g-lte

1. Go to *Network :: Connections*.
2. Click **Add** (displays dialog).
3. Enter **Name**.
4. On **Type** drop-down, select **Mobile Broadband GSM** (dialog changes).



Network :: Connections

▶ Start ✓ Confirm ↻ Revert

Save Cancel

Name:

Type: Mobile Broadband GSM

Interface: eth0

Description:

☑ Connect Automatically

□ Set as Primary Connection

□ Enable LLDP advertising and reception through this connection

□ Block Unsolicited Incoming Packets

□ Enable Connection Health Monitoring

IPv4 Mode: ○ No IPv4 Address ● DHCP

IPv4 DNS Server:

IPv4 DNS Search:

IPv4 Default Route Metric:

□ Ignore obtained IPv4 Default Gateway

□ Ignore obtained DNS server

IPv6 Mode: ● No IPv6 Address ○ Address Auto Configuration

IPv6 DNS Server:

IPv6 DNS Search:

IPv6 Default Route Metric:

□ Ignore obtained IPv6 Default Gateway

□ Ignore obtained DNS server

Mobile Broadband Connection

SIM-1 Phone Number:

SIM-1 APN Configuration: ○ Automatic ● Manual

SIM-1 User name:

SIM-1 Password: ••••••••

SIM-1 Access Point Name (APN):

SIM-1 Personal Identification Number (PIN): ••••••••

SIM-1 MTU: auto

SIM-1 allowed modes:

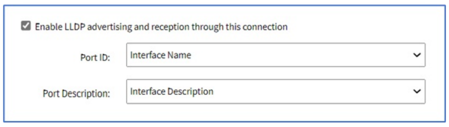
SIM-1 preferred mode:

□ Enable Data Usage Monitoring

□ Enable IP Passthrough

□ Enable Global Positioning System (GPS)

5. On **Interface drop-down**, select one.
6. Enter **Description.**
7. If **Connect Automatically** checkbox is selected, connection is automatically established at startup.
8. **Set as Primary Connection** checkbox (defines interface as the primary connection. Only one interface can be the primary.)
9. If **Enable LLDP advertising and reception through this connection** checkbox is selected: On **Port ID** drop-down, select one. On **Port Description** drop-down, select one.

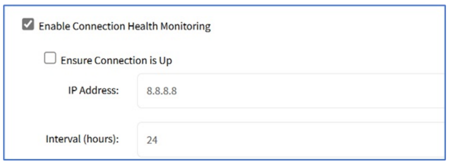


☑ Enable LLDP advertising and reception through this connection

Port ID: Interface Name

Port Description: Interface Description

10. Select **Block Unsolicited Incoming Packets** checkbox (automatically blocks all inbound connections on the interface).
11. If the **Enable Connection Health Monitoring** checkbox is selected (expands dialog). When a modem fails to connect the system automatically resets the modem if it has already been reset the system performs a power cycle.



☑ Enable Connection Health Monitoring

□ Ensure Connection is Up

IP Address: 8.8.8.8

Interval (hours): 24

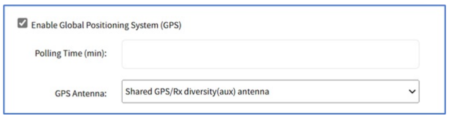
a. Select **Ensure Connection is Up** checkbox
b. Enter **IP Address**
c. Enter **Interval (hours)** (default: 24)
Note: If Connection Health Monitoring is enabled for the interface and a modem is detected but not usable, the system automatically resets the modem. If a reset fails to fix the issue, the system performs a power cycle on the modem in the next run of the health monitoring. The next power cycle is performed only after 24 hours.

12. In *IPv4 Mode* menu, select one:
    - **No IPv4 Address** radio button
    - **DHCP** radio button
    - Enter IPv4 details:
        - (optional) **IPv4 DNS Server**
        - **IPv4 DNS Search** (defines a domain name for DNS lookups)
        - **IPv4 Default Route Metric**
        - **Ignore the obtained IPv4 Default Gateway** checkbox
        - **Ignore the obtained DNS server** checkbox
13. In *IPv6 Mode* menu, select one:
    - **No IPv6 Address** radio button
    - **Address Auto Configuration** radio button
    - Enter IPv6 details:
        - (optional) **IPv6 DNS Server**
        - **IPv6 DNS Search** (defines a domain name for DNS lookups)
        - **IPv6 Default Route Metric**
        - **Ignore the obtained IPv6 Default Gateway** checkbox
        - **Ignore the obtained DNS server** checkbox
14. In *Mobile Broadband Connection* menu:

    a. Enter **SIM-1 Phone Number**.
    b. On SIM-*1 APN Configuration* menu, select one:
    - **Automatic** radio button
    - If the **Manual** radio button is selected (expands dialog), enter details:

    c. Enter SIM-1 details:
    - **SIM-1 User name** (user name to unlock the SIM)
    - **SIM-1 Password**
    - **SIM-1 Access Point Name (APN)**
    - Enter **SIM-1 Personal Identification Number (PIN)**
    - **SIM-1 MTU (**bytes – can be set to 'auto' = 1500 bytes)
    - **Enable the Data Usage Monitoring** checkbox (monitors the data usage and signal strength at regular intervals and provides historical data). If selected (expands dialog):
        - **SIM-1 Data Limit Value (GB)** (monthly data limit)
        - **SIM-1 Data Warning (%)** (percentage that triggers an event notification when reached)
        - **SIM-1 Renew Day** (day to reset accumulated data)

    d. If **Enable IP Passthrough** checkbox is selected (expands dialog):
    - **Ethernet Connection** drop-down, select one (selection varies depending on the device)
    - **MAC Address** (if blank, the system uses DHCP to get the device)
    - **Port Intercepts** (any ports that should NOT pass through the Nodegrid device)
    - If **Enable Global Positioning System (GPS)** checkbox is selected (expands dialog):



☑ Enable Global Positioning System (GPS)

Polling Time (min):

GPS Antenna: Shared GPS/Rx diversity(aux) antenna

- Enter **Polling Time (min).**
- On the **GPS Antenna** drop-down, select one (Shared GPS/Rx diversity(aux) antenna, Dedicated Active GPS antenna, Dedicated Passive GPS antenna).

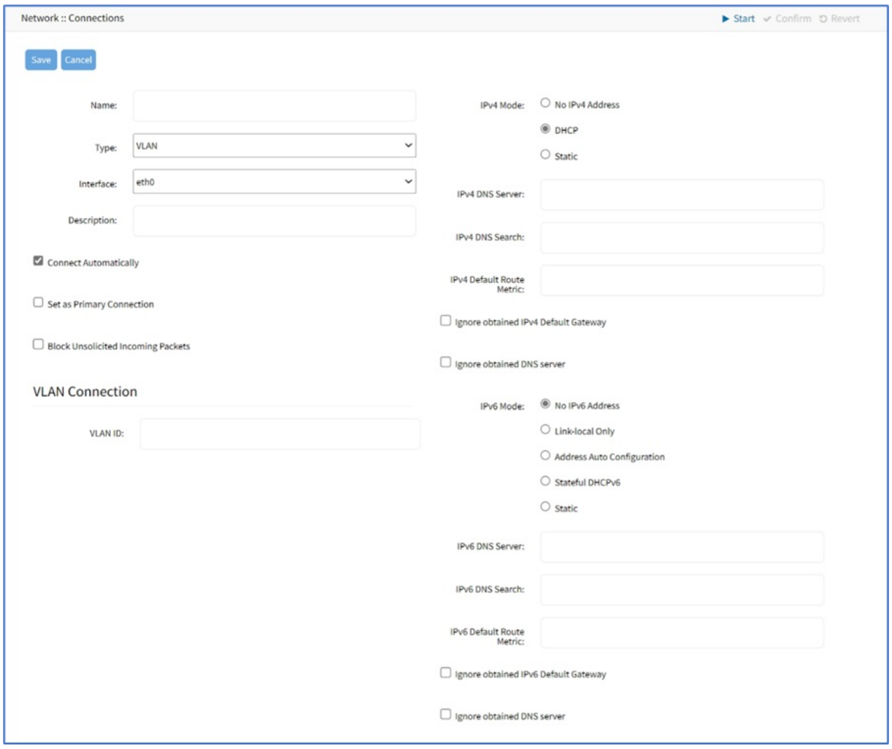
15. (if available) Select the **Enable Second SIM card** checkbox. Repeat entries for SIM-2 settings. There is a setting **Active SIM card** that can designate SIM-2 as the primary SIM card.
16. Click **Save**.

Add VLAN Interface

VLAN Interfaces allow the Nodegrid system to natively tag network traffic with a specific VLAN ID. For this, a VLAN Interface needs to be created. The VLAN interface will behave and allows the same settings as any other network interface on in Nodegrid solution. The new interface will be bound to a specific physical interface and the administrator as the ability to define the VLAN ID.

Ports can be assigned, as needed. By default, VLAN 1 and VLAN 2 exist. All ports belong to VLAN 1 except BACKPLANE1 and SFP1 (belongs to VLAN 2).

1. Go to *Network :: Connections*.
2. Click **Add** (displays dialog).
3. Enter **Name**.
4. On **Type** drop-down, select **VLAN** (dialog changes).



Network :: Connections

▶ Start ✓ Confirm ⟲ Revert

Save Cancel

Name:

Type: VLAN

Interface: eth0

Description:

☑ Connect Automatically

□ Set as Primary Connection

□ Block Unsolicited Incoming Packets

VLAN Connection

VLAN ID:

IPv4 Mode: ○ No IPv4 Address ● DHCP ○ Static

IPv4 DNS Server:

IPv4 DNS Search:

IPv4 Default Route Metric:

□ Ignore obtained IPv4 Default Gateway

□ Ignore obtained DNS server

IPv6 Mode: ● No IPv6 Address ○ Link-local Only ○ Address Auto Configuration ○ Stateful DHCPv6 ○ Static

IPv6 DNS Server:

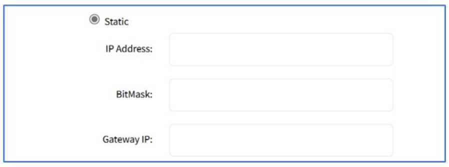
IPv6 DNS Search:

IPv6 Default Route Metric:

□ Ignore obtained IPv6 Default Gateway

□ Ignore obtained DNS server

5. On **Interface drop-down**, select one.
6. Enter **Description.**
7. If **Connect Automatically** checkbox is selected, connection is automatically established at startup.
8. **Set as Primary Connection** checkbox (defines interface as the primary connection. Only one interface can be the primary.).
9. Select **Block Unsolicited Incoming Packets** checkbox (automatically blocks all inbound connections on the interface).
10. In *VLAN Connection* menu, enter **VLAN ID**.
11. In *IPv4 Mode* menu, select one:
    - **No IPv4 Address** radio button
    - **DHCP** radio button
    - **Static** radio button (if selected, expands dialog). Enter **IP Address**, **BitMask**, and (optional) **Gateway IP**.



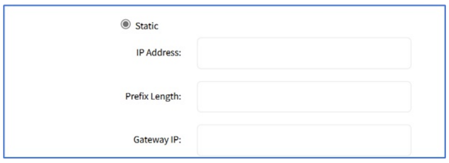
● Static

IP Address:

BitMask:

Gateway IP:

    - Enter IPv4 details:
        - (optional) **IPv4 DNS Server**
        - **IPv4 DNS Search** (defines a domain name for DNS lookups)
        - **IPv4 Default Route Metric**
        - **Ignore obtained IPv4 Default Gateway** checkbox
        - **Ignore obtained DNS server** checkbox
12. In *IPv6 Mode* menu, select one:
    - **No IPv6 Address** radio button
    - **Link local Only** radio button.
    - **Address Auto Configuration** radio button
    - **Stateful DHCPv6** radio button
    - If **Static** radio button is selected (displays menu). Enter **IP Address**, **Prefix Length**, and (optional) **Gateway IP**



● Static

IP Address:

Prefix Length:

Gateway IP:

    - Enter IPv6 details:
        - (optional) **IPv6 DNS Server**
        - **IPv6 DNS Search** (defines domain name for DNS lookups)

- **IPv6 Default Route Metric**
- **Ignore obtained IPv6 Default Gateway** checkbox
- **Ignore obtained DNS server** checkbox

13. Click **Save**.

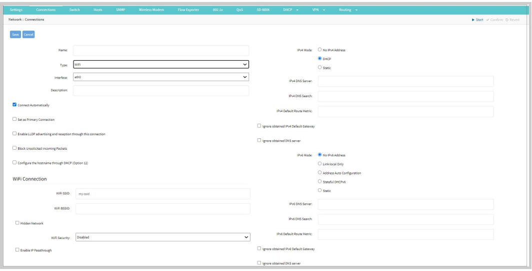
Add WiFi Interface

You can set up a WiFi interface to connect the Nodegrid to a WiFi network.

Note: To use the device as a WiFi client, any existing hotspot connection must be disabled (make sure Carrier State is Down).

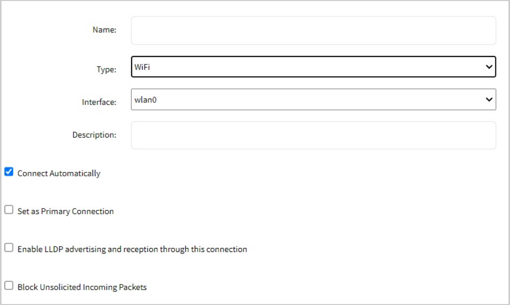
To configure the interface:

1. Go to *Network :: Connections*.
2. Click **Add**. All default interfaces are listed on this page.



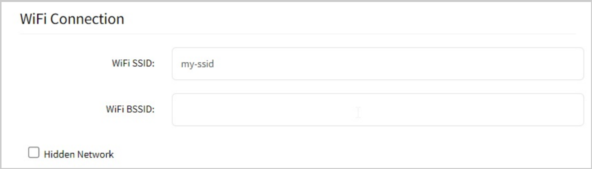
Name:
Type: WiFi
Interface: eth0
Description:
☑ Connect Automatically
□ Set as Primary Connection
□ Enable LLDP advertising and reception through this connection
□ Block Unsolicited Incoming Packets
□ Configure the hostname through DHCP (Option 12)
WiFi Connection
WiFi SSID: my-ssid
WiFi BSSID:
□ Hidden Network
WiFi Security: Disabled
□ Enable IP Passthrough
IPv4 Mode: ○ No IPv4 Address ● DHCP ○ Static
IPv4 DNS Server:
IPv4 DNS Search:
IPv4 Default Route Metric:
□ Ignore obtained IPv4 Default Gateway
□ Ignore obtained DNS server
IPv6 Mode: ● No IPv6 Address ○ Link-local Only ○ Address Auto Configuration ○ Stateful DHCPv6 ○ Static
IPv6 DNS Server:
IPv6 DNS Search:
IPv6 Default Route Metric:
□ Ignore obtained IPv6 Default Gateway
□ Ignore obtained DNS server

3. Enter **Name**.
4. From the **Type** drop-down list, select **WiFi.**
5. Select the required Interface from the **Interface** drop-down list. For a WiFi connection the interface must be any wlanX interface, in case of any other selection, the system throws an error.
6. Enter **Description.**
7. **Connect Automatically**: Select if you want to automatically establish a connection when the system starts.
8. **Set as Primary Connection**: Select only if you want the interface as the primary connection. Only one interface can be the primary interface.
9. **Enable LLDP advertising and reception through this connection:** If you want to allow the network to advertise information about themselves to other devices, specify:
   a. **Port ID**: Select the required Port ID from the drop-down list.
   b. **Port Description**: Select the required port description from the drop-down list.



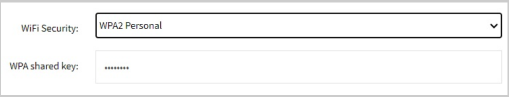
Name:
Type: WiFi
Interface: wlan0
Description:
☑ Connect Automatically
□ Set as Primary Connection
□ Enable LLDP advertising and reception through this connection
□ Block Unsolicited Incoming Packets

10. Select the **Block Unsolicited Incoming Packets** field to block all inbound connections on the interface automatically.
11. In the *WiFi Connection* section, specify:
   a. **WiFi SSID:** Unique identifier for your WiFi network.
   b. **WiFi BSSID**: The MAC address of the access point or the router used to connect to the network.
   c. **Hidden Network:** Allows the user to connect to a hidden network.



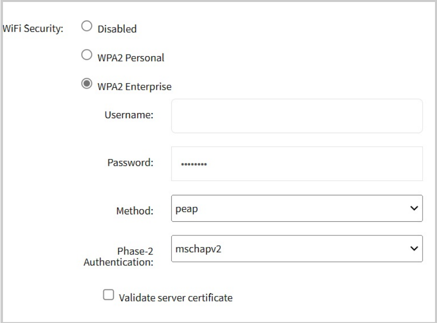
WiFi Connection
WiFi SSID: my-ssid
WiFi BSSID:
□ Hidden Network

   d. From the *WiFi Security* drop-down list, select:
      i. **Disabled**: to disable the security of your WiFi hotspot network.
      ii. **WPA2 Personal**: uses pre-shared keys (PSK) for authentication and a single password to connect to the network.
         i. Enter the **WPA shared key** to authenticate the user to connect to the network.



WiFi Security: WPA2 Personal
WPA shared key: ••••••••

      iii. **WPA2 Enterprise:** Offers enterprise-level security, uses IEEE 802.1X, and requires a password and phase-2 authentication. To enable, enter the following:
         i. **Username**: The username of the account.
         ii. **Password:** The password to log in to the account.
         iii. **Method:** Select the required Method from the drop-down list.
         iv. **Phase 2 Authentication:** select the required authentication.
         v. **Validate server certificate checkbox:** Select the field to ensure that the server’s certificate is not expired



WiFi Security: ○ Disabled

○ WPA2 Personal

● WPA2 Enterprise

Username:

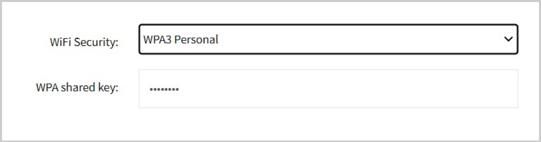
Password: ••••••••

Method: peap

Phase-2 Authentication: mschapv2

□ Validate server certificate

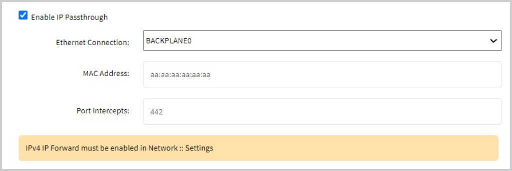
12. **WPA3 Personal:** WPA3 is the latest security standard for WiFi networks. WPA3 offers stronger encryption and authentication, which makes it more secure for users to connect to WiFi hotspots. WPA3 Personal is preferred for personal use. To enable, specify, **WPA shared key:** Pass to authenticate the user to connect to the network.



WiFi Security: WPA3 Personal

WPA shared key: ••••••••

13. **Enable IP Passthrough:**



☑ Enable IP Passthrough

Ethernet Connection: BACKPLANE0

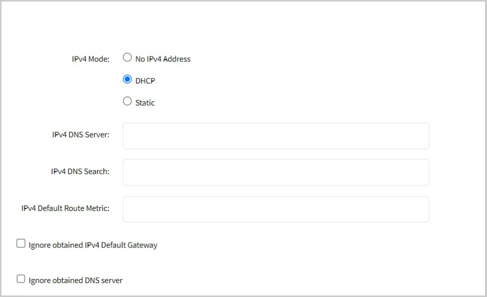
MAC Address: aa:aa:aa:aa:aa:aa

Port Intercepts: 442

IPv4 IP Forward must be enabled in Network :: Settings

   a. Select the check box **Enable IP Passthrough**. This option enables the Nodegrid device to provide its IP address to another network device linked to the Ethernet Connection interface.
   b. Choose the specific type of **Ethernet Connection** of the Nodegrid device from the dropdown list. The available options are dynamically generated based on the type of Nodegrid device being used.
   c. Enter the **MAC Address** of the device that will receive the IP address when there is more than one network device linked to the Ethernet Connection interface sending DHCP requests.
   d. Specify the port numbers (HTTP, TCP port numbers etc) in the **Port Intercepts** field. Nodegrid will only respond to requests directed at the ports specified in this field. Any request to other ports will be routed to the network device that receives the IP address.

14. In the *IPv4 Mode* section, select one of the following options:
   a. **No IPv4 Address**
   b. **DHCP**: enables network administrators to automatically assign and distribute IP addresses and other network configuration parameters to devices within a network.
   c. **Static**: If you want a specific IP to communicate with other devices, enter the following details:
      i. **IP Address** and **BitMask, and,** (optional) **Gateway IP**



IPv4 Mode: ○ No IPv4 Address

● DHCP

○ Static

IPv4 DNS Server:

IPv4 DNS Search:

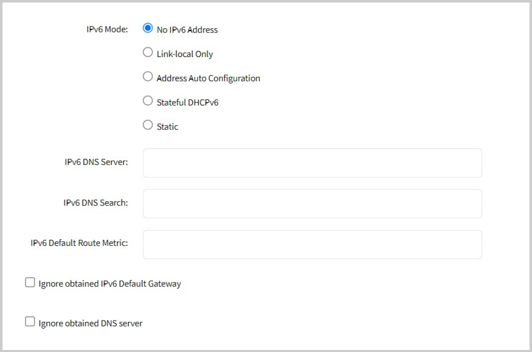
IPv4 Default Route Metric:

□ Ignore obtained IPv4 Default Gateway

□ Ignore obtained DNS server

   d. (optional) **IPv4 DNS Server**
   e. **IPv4 DNS Search** (defines a domain name for DNS lookups)
   f. **IPv4 Default Route Metric**
   g. **Ignore obtained IPv4 Default Gateway** checkbox
   h. **Ignore obtained DNS server** checkbox

15. In the *IPv6 Mode* section, select one of the following:
   a. **No IPv6 Address**
   b. **Link-local Only**
   c. **Address Auto Configuration**
   d. **Stateful DHCPv6**
   e. if you select **Static,** enter **IP Address**, **Prefix Length**, and (optional) **Gateway IP.**



IPv6 Mode: ● No IPv6 Address

○ Link-local Only

○ Address Auto Configuration

○ Stateful DHCPv6

○ Static

IPv6 DNS Server:

IPv6 DNS Search:

IPv6 Default Route Metric:

□ Ignore obtained IPv6 Default Gateway

□ Ignore obtained DNS server

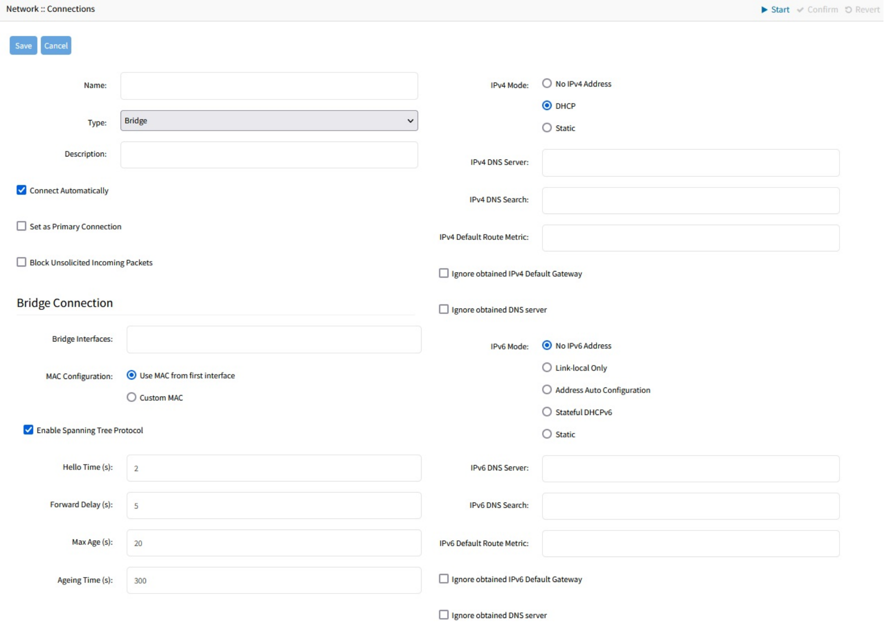
16. Enter IPv6 details:
    a. (optional) **IPv6 DNS Server**
    b. **IPv6 DNS Search** (defines domain name for DNS lookups)
    c. **IPv6 Default Route Metric**
    d. **Ignore the obtained IPv6 Default Gateway** checkbox
    e. **Ignore** the **obtained DNS server** checkbox

17. Click **Save**.

Add Bridge Interface

With Bridge interfaces, the System can create a virtual switch that crosses one or more interfaces. The switch is completely transparent to the network interfaces and does not require additional setup. The most common use for a bridge network is easy network access for any running NFV (outside as well as the Nodegrid System). Bridge network interfaces use the same network configuration options as all Ethernet interfaces.

1. Go to *Network :: Connections*.
2. Click **Add** (displays dialog).
3. Enter **Name**.
4. On **Type** drop-down, select **Bridge** (dialog changes).



Network :: Connections
▶ Start ✓ Confirm ↻ Revert

Save Cancel

Name:

Type: Bridge

Description:

☑ Connect Automatically

□ Set as Primary Connection

□ Block Unsolicited Incoming Packets

Bridge Connection

Bridge Interfaces:

MAC Configuration: ● Use MAC from first interface ○ Custom MAC

☑ Enable Spanning Tree Protocol

Hello Time (s): 2

Forward Delay (s): 5

Max Age (s): 20

Ageing Time (s): 300

IPv4 Mode: ○ No IPv4 Address ● DHCP ○ Static

IPv4 DNS Server:

IPv4 DNS Search:

IPv4 Default Route Metric:

□ Ignore obtained IPv4 Default Gateway

□ Ignore obtained DNS server

IPv6 Mode: ● No IPv6 Address ○ Link-local Only ○ Address Auto Configuration ○ Stateful DHCPv6 ○ Static

IPv6 DNS Server:

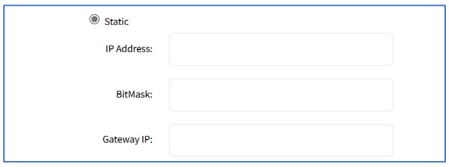
IPv6 DNS Search:

IPv6 Default Route Metric:

□ Ignore obtained IPv6 Default Gateway

□ Ignore obtained DNS server

5. Enter **Description**.
6. If **Connect Automatically** checkbox is selected, connection is automatically established at startup.
7. Select **Set as Primary Connection** checkbox (defines interface as the primary connection. Only one interface can be the primary.)
8. Select **Block Unsolicited Incoming Packets** checkbox (automatically blocks all inbound connections on the interface).
9. In *Bridge Connection* menu, enter details:
   a. **Bridge Interfaces** (list of physical interfaces, separated by commas and/or spaces)
   b. **MAC Configuration** (default: **Use MAC from first interface**) (if selected, a text field shows where the user can enter a custom, persistent MAC address for this connection)
   c. **Enable Spanning Tree Protocol** checkbox
   d. **Hello Time (s)** (default: 2) (number of seconds a HELLO packet is sent when Spanning Tree is enabled)
   e. **Forward Delay (s)** (default: 5) (packet forward delay. Can be set to 0 when **Enable Spanning Tree Protocol** is not checked)
   f. **Max Age (s)** (default: 20) (maximum age for packages when Spanning Tree is enabled)
   g. **Ageing Time (s)** (default: 300) (how long the bridge will keep information about a specific address in its forwarding database)
10. In *IPv4 Mode* menu, select one:
    - **No IPv4 Address** radio button
    - **DHCP** radio button
    - **Static** radio button (if selected, expands dialog). Enter **IP Address**, **BitMask**, and (optional) **Gateway IP**.



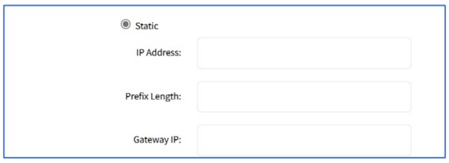
● Static

IP Address:

BitMask:

Gateway IP:

    - Enter IPv4 details:
      - (optional) **IPv4 DNS Server**
      - **IPv4 DNS Search** (defines a domain name for DNS lookups)
      - **IPv4 Default Route Metric**
      - **Ignore obtained IPv4 Default Gateway** checkbox
      - **Ignore obtained DNS server** checkbox
11. In *IPv6 Mode* menu, select one:
    - **No IPv6 Address** radio button
    - **Link local Only** radio button.
    - **Address Auto Configuration** radio button
    - **Stateful DHCPv6** radio button
    - If **Static** radio button is selected, displays menu). Enter **IP Address**, **Prefix Length**, and (optional) **Gateway IP**.



● Static

IP Address:

Prefix Length:

Gateway IP:

    - Enter IPv6 details:

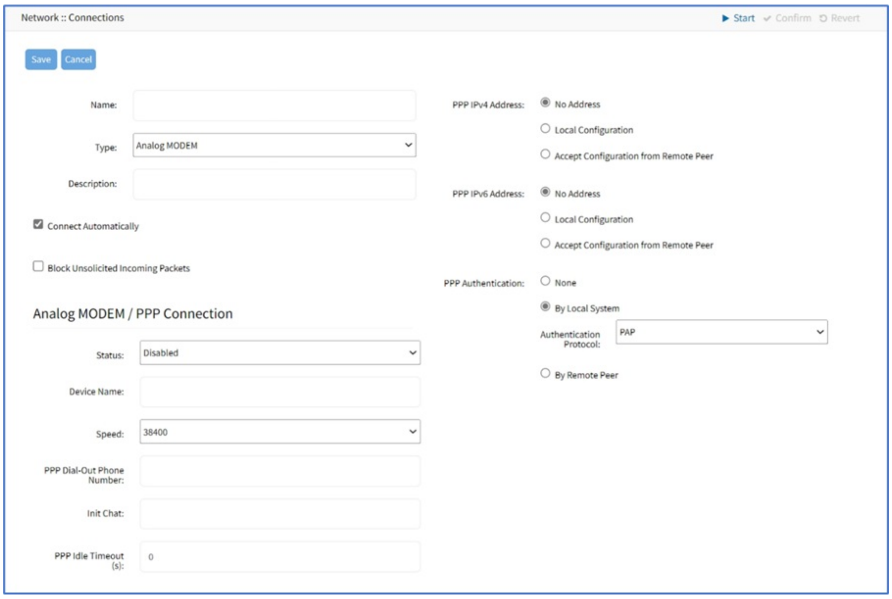
- (optional) **IPv6 DNS Server**
- **IPv6 DNS Search** (defines domain name for DNS lookups)
- **IPv6 Default Route Metric**
- **Ignore obtained IPv6 Default Gateway** checkbox
- **Ignore obtained DNS server** checkbox

12. Click **Save**.

Add Analog Modem Interface

With the analog modem interface, administrators can configure an existing analog modem and required PPP connection details. A supported analog modem must be connected to the Nodegrid System.

1. Go to *Network :: Connections*.
2. Click **Add** (displays dialog).
3. Enter **Name**.
4. On **Type** drop-down, select **Analog MODEM** (dialog changes).



Name:
Type: Analog MODEM
Description:
☑ Connect Automatically
□ Block Unsolicited Incoming Packets

Analog MODEM / PPP Connection

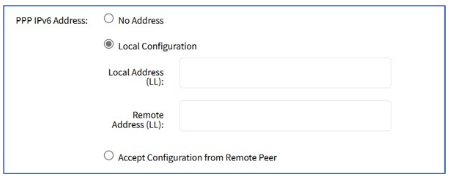
Status: Disabled
Device Name:
Speed: 38400
PPP Dial-Out Phone Number:
Init Chat:
PPP Idle Timeout (s): 0

PPP IPv4 Address: ● No Address ○ Local Configuration ○ Accept Configuration from Remote Peer
PPP IPv6 Address: ● No Address ○ Local Configuration ○ Accept Configuration from Remote Peer
PPP Authentication: ○ None ● By Local System
Authentication Protocol: PAP
○ By Remote Peer

5. Enter **Description**.
6. If **Connect Automatically** checkbox is selected, connection is automatically established at startup.
7. Select **Block Unsolicited Incoming Packets** checkbox (automatically blocks all inbound connections on the interface).
8. In *Analog MODEM / PPP Connection* menu, enter details:
   a. **Status** drop-down, select one (Enabled, Disabled)
   b. **Device Name**
   c. **Speed** drop-down, select one (9600, 19200, 38400, 57600, 115200)
   d. **PPP Dial-Out Phone Number**
   e. **Init Chat** (a specific AT init string, if required)
   f. **PPP Idle Timeout (sec)** (connection idle timeout after which the connection is automatically disconnected. 0 sec = connection is not automatically disconnected.)

9. In *PPP IPv4 Address* menu (select one), enter details:
   a. **No Address** radio button
   b. **Local Configuration** radio button (expands dialog). Enter **Local Address** and **Remote Address. Accept Configuration from**
   c. **Remote Peer** radio button

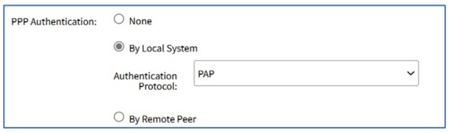
10. In *PPP IPv6 Address* menu (select one) enter details:
    - **No Address** radio button
    - **Local Configuration** radio button (expands dialog). Enter **Local Address (LL)** and **Remote Address (LL)**.



PPP IPv6 Address: ○ No Address ● Local Configuration
Local Address (LL):
Remote Address (LL):
○ Accept Configuration from Remote Peer

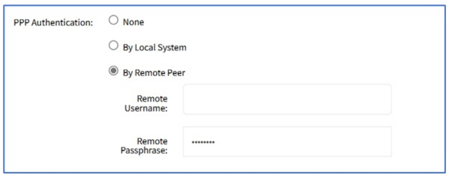
    - **Accept Configuration from Remote Peer** radio button

11. In *PPP Authentication* menu, select one:
    - **None** radio button
    - **Local System** radio button (displays menu). **Authentication Protocol** drop-down, select one (PAP, CHAP, EAP).



PPP Authentication: ○ None ● By Local System
Authentication Protocol: PAP
○ By Remote Peer

    - **Remote Peer** radio button (expands dialog). Enter **Remote Username** and **Remote Passphrase**.

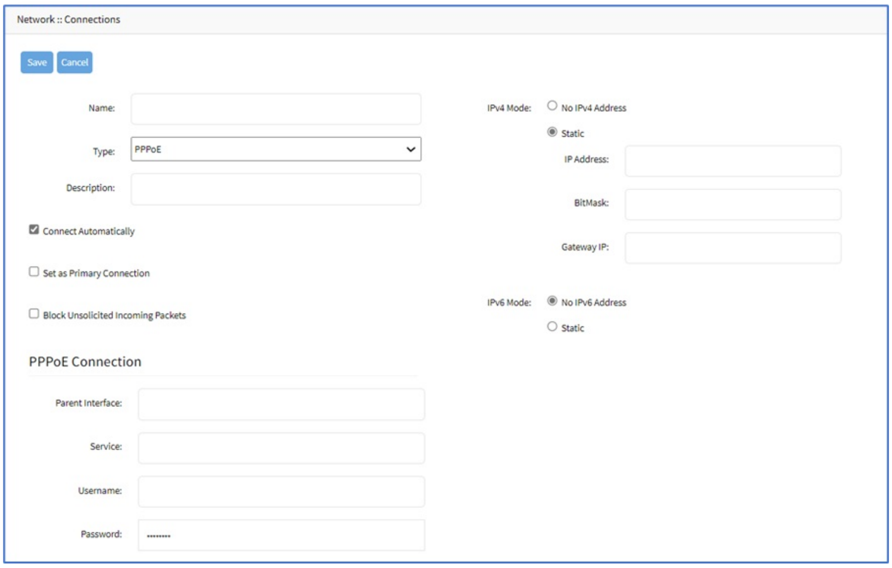


PPP Authentication: ○ None ○ By Local System ● By Remote Peer
Remote Username:
Remote Passphrase: ••••••••

12. Click **Save**.

Add PPPoE Interface

1. Go to *Network :: Connections*.
2. Click **Add** (displays dialog).
3. Enter **Name**.
4. On **Type** drop-down, select **PPPoE** (dialog changes).



Name:

Type: PPPoE

Description:

☑ Connect Automatically

☐ Set as Primary Connection

☐ Block Unsolicited Incoming Packets

Parent Interface:

Service:

Username:

Password: ••••••••

IPv4 Mode: ○ No IPv4 Address ● Static

IP Address:

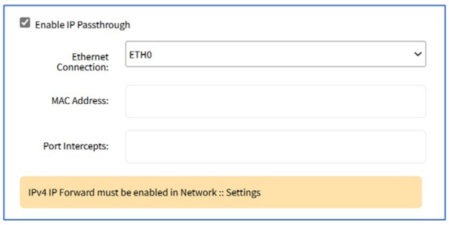
BitMask:

Gateway IP:

IPv6 Mode: ● No IPv6 Address ○ Static

5. Enter **Description**.
6. If **Connect Automatically** checkbox is selected, connection is automatically established at startup.
7. **Set as Primary Connection** checkbox (defines interface as the primary connection. Only one interface can be the primary.)
8. Select **Block Unsolicited Incoming Packets** checkbox (automatically blocks all inbound connections on the interface).
9. In *PPPoE Connection* menu, enter details:
   a. **Parent Interface** (default: blank) Specifies the parent interface name on which this PPPoE connection should be created. If blank, connection is activated on the ethernet interface.
   b. **Service** (default: blank) Specifies PPPoE only initiates sessions with access concentrators that provide the specified service. For most providers, leave blank. Required only if there are multiple access concentrators or a required specific service. Access concentrators grants access to multiple users with needing a dedicated connection for each user.
   c. Enter **Username** and **Password**

10. If **Enable IP Passthrough** checkbox selected (expands dialog) enter details:



☑ Enable IP Passthrough

Ethernet Connection: ETH0

MAC Address:

Port Intercepts:

IPv4 IP Forward must be enabled in Network :: Settings

   a. **Ethernet Connection** drop-down, select one (ETH0, ETH1, hotspot)
   b. **MAC Address**
   c. **Port Intercepts**

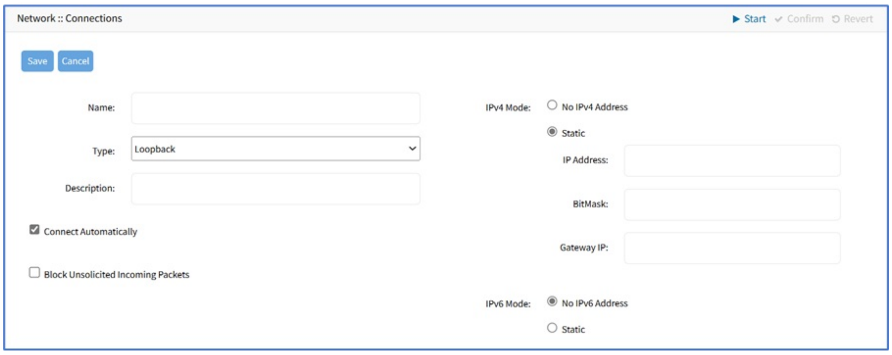
11. In *IPv4 Mode* menu, select one:
    - **No IPv4 Address** radio button
    - **DHCP** radio button

12. In *IPv6 Mode* menu, select one:
    - **No IPv6 Address** radio button
    - **Address Auto Configuration** radio button

13. Click **Save**.

Add Loopback Interface

1. Go to *Network :: Connections*.
2. Click **Add** (displays dialog).
3. Enter **Name**.
4. On **Type** drop-down, select **Loopback** (dialog changes).



Name:

Type: Loopback

Description:

☑ Connect Automatically

□ Block Unsolicited Incoming Packets

IPv4 Mode: ○ No IPv4 Address ● Static

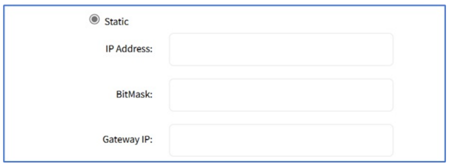
IP Address:

BitMask:

Gateway IP:

IPv6 Mode: ● No IPv6 Address ○ Static

5. Enter **Description**
6. If **Connect Automatically** checkbox is selected, connection is automatically established at startup.
7. Select **Block Unsolicited Incoming Packets** checkbox (automatically blocks all inbound connections on the interface).
8. In *IPv4 Mode* menu, select one:
   - **No IPv4 Address** radio button
   - **Static** radio button (if selected, expands dialog). Enter **IP Address**, **BitMask**, and (optional) **Gateway IP**.



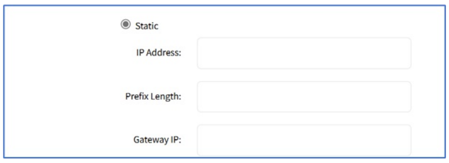
● Static

IP Address:

BitMask:

Gateway IP:

9. In *IPv6 Mode* menu, select one:
   - **No IPv6 Address** radio button
   - If **Static** radio button is selected, displays menu). Enter **IP Address**, **Prefix Length**, and (optional) **Gateway IP.**



● Static

IP Address:

Prefix Length:

Gateway IP:

10. Click **Save**.

Manage Network Connections

Edit Network Connection

This applies to all connections, except the hotspot connection.

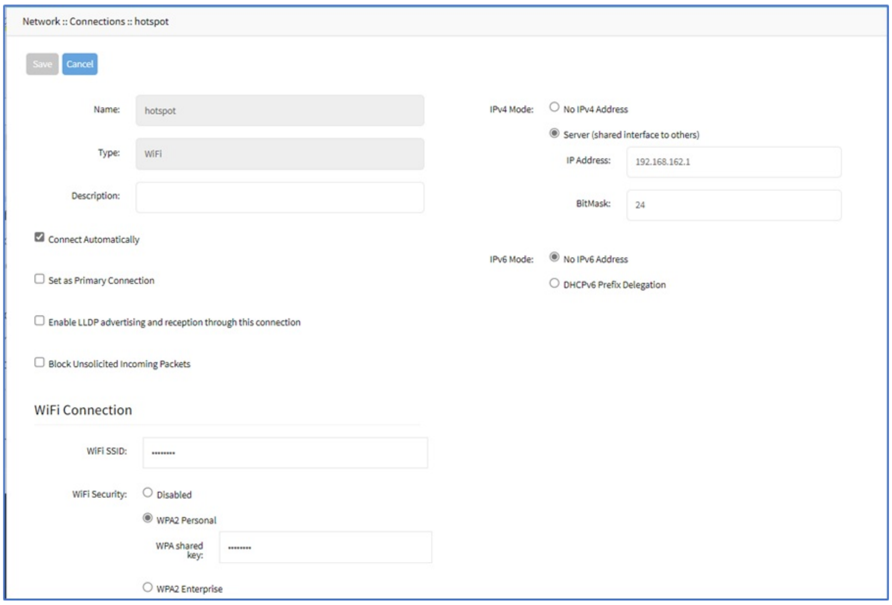
1. Go to *Network :: Connections*.
2. In the *Name* column, click the connection you want to edit.
3. Make the required changes.
4. Click **Save**.

Configure Hotspot Network Connection

(available in v5.6+)
The system supports a Nodegrid device as a Hotspot access point. Define a compatible WiFi module to use the default hotspot interface. This interface configures the device as an access point and allows other devices to connect. You cannot delete the default Hotspot interface and the system throws an error when you try to delete it.

To use the Nodegrid as a Hotspot Access Point, perform the following actions:

1. Go to *Network :: Connections*.
2. In the *Name* column, click **hotspot** (displays dialog).



Network :: Connections :: hotspot

Save Cancel

Name: hotspot

Type: WiFi

Description:

☑ Connect Automatically

□ Set as Primary Connection

□ Enable LLDP advertising and reception through this connection

□ Block Unsolicited Incoming Packets

WiFi Connection

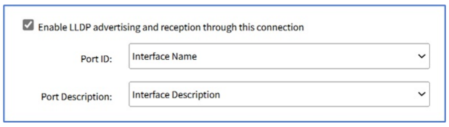
WiFi SSID: ••••••••

WiFi Security: ○ Disabled
● WPA2 Personal
WPA shared key: ••••••••
○ WPA2 Enterprise

IPv4 Mode: ○ No IPv4 Address
● Server (shared interface to others)
IP Address: 192.168.162.1
BitMask: 24

IPv6 Mode: ● No IPv6 Address
○ DHCPv6 Prefix Delegation

3. Enter the required details:
   a. **Description:** Provide a suitable description.
   b. **Connect Automatically**: Select if you want to establish a connection when the system starts automatically.
   c. **Set as Primary Connection**: Select only if you want the interface as the primary connection. Only one interface can be the primary interface.
   d. **Enable LLDP advertising and reception through this connection:** If you want to allow the network to advertise information about themselves to other devices, specify:
      i. From the **Port ID** drop-down list, select one.
      ii. From the **Port Description** drop-down, choose one.



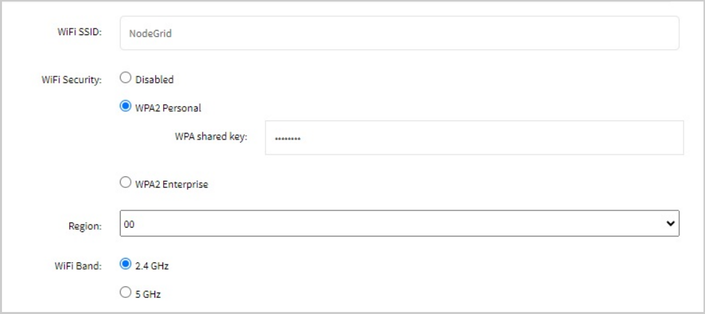
☑ Enable LLDP advertising and reception through this connection

Port ID: Interface Name

Port Description: Interface Description

   e. Select the **Block Unsolicited Incoming Packets** field to automatically block all inbound connections on the interface.

4. In the *WiFi Connection* menu, enter the details:
   a. **WiFi SSID:** Unique identifier for your WI-FI network.
   b. From the *WiFi Security* menu, select one:
      - **Disabled:** Disable the WiFi hotspot network.
      - If **WPA2 Personal:** uses pre-shared keys (PSK) for authentication and a single password to connect to the network.
        It is recommended to use for personal use.
        - Enter the **WPA shared key** to authenticate the user to connect to the network. The shared key is the serial number of the Nodegrid device.
        - Region: Select the required region from the drop-down list.
        - WiFi Band: select the required WiFi band. You can select 2.4 GHz or 5 GHz.



WiFi SSID: NodeGrid

WiFi Security: ○ Disabled

● WPA2 Personal

WPA shared key: ••••••••

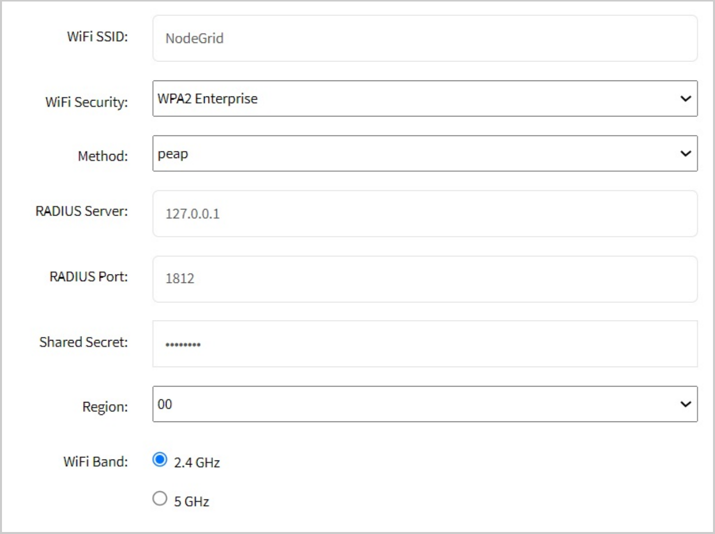
○ WPA2 Enterprise

Region: 00

WiFi Band: ● 2.4 GHz

○ 5 GHz

- **WPA2 Enterprise:** Offers enterprise-level security, uses IEEE 802.1X, and requires a password and phase-2 authentication. To enable, enter the following:
  - **Method:** Select the required method from the drop-down list.
  - **RADIUS Server:** To enable remote desktop access.
  - **RADIUS** Port: Enter the RADIUS port number.
  - **Shared Secret**:: The shared secret key to connect to the hotspot.
  - **Region**: Select the required region from the drop-down list.
  - **WiFI Band**: Select the frequency of the WiFi band.



WiFi SSID: NodeGrid

WiFi Security: WPA2 Enterprise

Method: peap

RADIUS Server: 127.0.0.1

RADIUS Port: 1812

Shared Secret: ••••••••

Region: 00

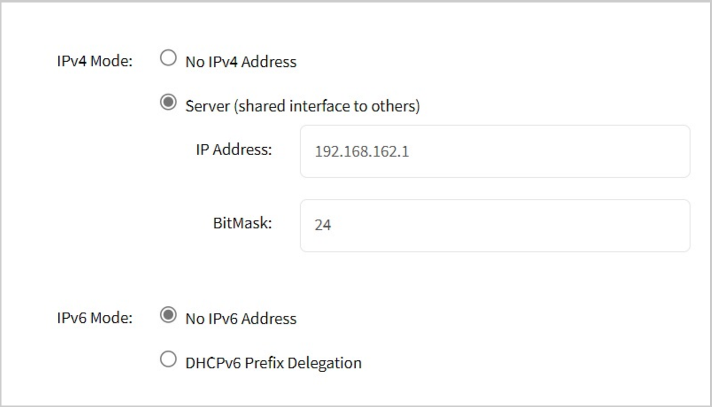
WiFi Band: ● 2.4 GHz

○ 5 GHz

- **WPA3 Personal:** WPA3 is the latest security standard for Wi-Fi networks. WPA3 offers stronger encryption and authentication, which makes it more secure for users to connect to Wi-Fi hotspots.
  To enable, specify:
  - **WPA shared key:** to authenticate the user to connect to the network.
  - **Region**: Select the required region from the drop-down list. The region should match the physical location or Country the device is in. If unsure, ZPE Systems recommends using 00 as it is restrictive and works for all locations.
  - **WiFi Band**: The frequency of the WiFi band. If the user selects the 00 region, the 5 GHz band cannot be used in that region.

c. IPV4

- **No IPV4 address;** If you do not want to specify any IPV4 address.
- **Enter** the **IP Address** and **BitMask**



IPv4 Mode: ○ No IPv4 Address

● Server (shared interface to others)

IP Address: 192.168.162.1

BitMask: 24

IPv6 Mode: ● No IPv6 Address

○ DHCPv6 Prefix Delegation

d. IPV6 Mode:

i. **No IPv6**: select if you do not want to mention an IPV6 address

ii. **DHCPv6 Prefix Delegation**: allows automatic prefix delegation

Delete Network Connection

1. Go to ***Network :: Connections***.
2. Select a connection checkbox.
3. Click **Delete**.

Move Connection Carrier State Up (active)

1. Go to ***Network :: Connections***.
2. Select a connection checkbox.
3. To make it active, click **Up Connection**.

Move Connection Carrier State Down (inactive)

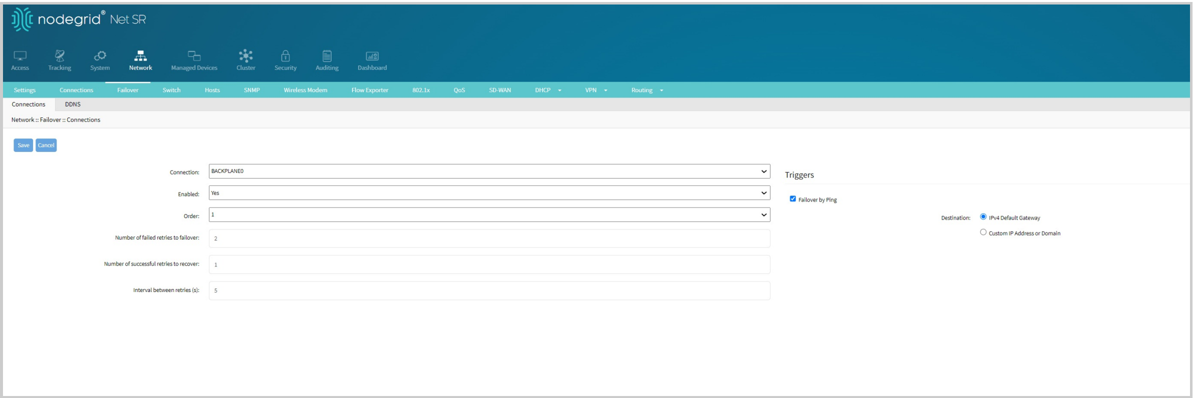
1. Go to *Network :: Connections*.
2. Select a connection checkbox.
3. To make it inactive, click **Down Connection**.

Configuring Network Failover on Nodegrid Device

Configuring Nodegrid Network Failover

When a network failover is active, the connection in the network failover tree switches to the next active connection when the previous one fails providing network availability and stability to the system. Network failover facilitates actively changing the network connections' route metrics. Note that you must configure at least two network connections for the failover to be active. To configure connections for a network failover on the Nodegrid device:

1. Log in to the Nodegrid UI.
2. Navigate to the path *Network:: Failover*.
3. Click **Connections** and then click **Add**.



Network :: Failover :: Connections

Connection: BACKPLANE0

Enabled: Yes

Order: 1

Number of failed retries to failover: 2

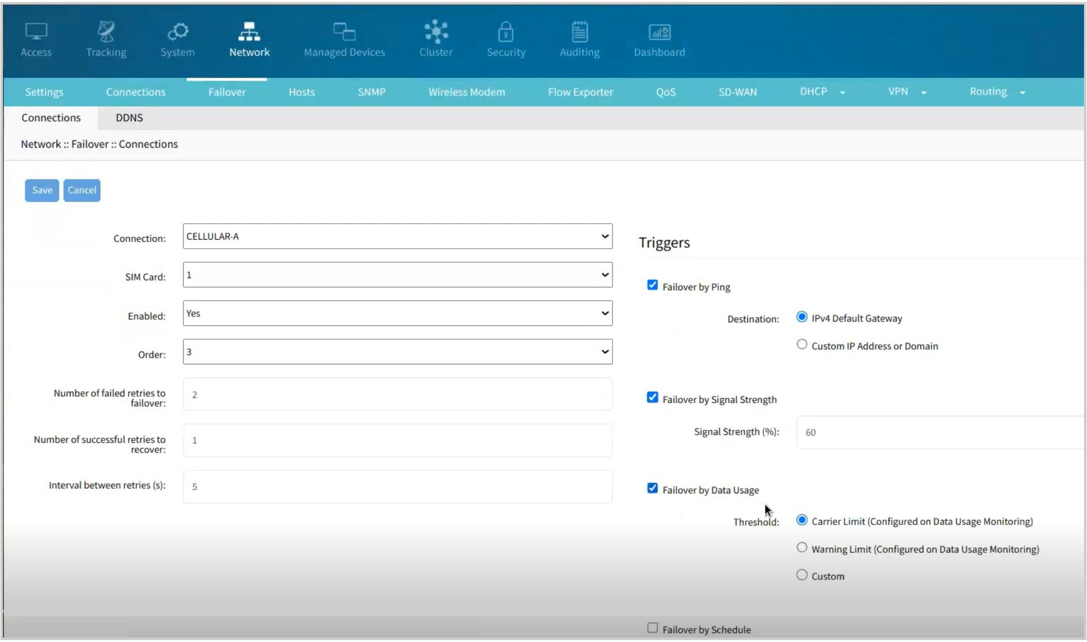
Number of successful retries to recover: 1

Interval between retries (s): 5

☑ Failover by Ping

Destination: ● IPv4 Default Gateway ○ Custom IP Address or Domain

4. Select the connection for the failover.
5. Select **Yes** to enable the connection. Selecting **No** disables the connection and triggers on the selected interface will not be active as well.
6. Select the **Order** in which you want the failover to occur. In a Nodegrid device, you can configure multiple failover connections. This facilitates multiple backup devices during a failover. However, if the failover connection is the last one, their trigger is not used for failover.
7. Enter the number of failed trigger retires that a connection should attempt before failover to the next connection on failure. This applies to the connections with ping and strength triggers.
8. Enter the number of successful trigger retires that a connection should attempt to failback to the previous connection. This applies to the connections with ping and strength triggers.
9. Enter the time interval the network failover should wait before testing the triggers again. This applies to the connections with ping and strength triggers.
10. Select the checkbox **Failover by Ping** to send ICMP requests (ping) to the configured destination to test the connection. Upon failover, the connection initiates a failover process with the next connection to ensure service continuity. You could ping:
    a. the IPv4 default gateway **or**
    b. a custom IP address or Domain.
11. For the cellular connection, you could trigger the failover to the next connection depending on:
    a. signal strength: Failover is triggered when the signal strength drops below a user-defined percentage.
    b. data usage: Failover is triggered when the SIM card data usage consumption limit is exceeded: Carrier limit, Warning Limit, or a Custom data value.
    c. schedule:
        i. scheduled trigger: If a connection is configured with this trigger, the connection triggers a failover when the input *cron expression* schedule is triggered. After the configured amount of hours elapses, the connection triggers a failback.
        ii. scheduled failback: trigger occurs when two SIM cards of the same GSM (cellular) are configured (under *Failover::Connections*). The trigger is associated with the first SIM card, with a lower order. When the input *cron expression* schedule is triggered, a failback is triggered if the second SIM card with a higher order is active.



Network :: Failover :: Connections

Connection: CELLULAR-A

SIM Card: 1

Enabled: Yes

Order: 3

Number of failed retries to failover: 2

Number of successful retries to recover: 1

Interval between retries (s): 5

☑ Failover by Ping

Destination: ● IPv4 Default Gateway ○ Custom IP Address or Domain

☑ Failover by Signal Strength

Signal Strength (%): 60

☑ Failover by Data Usage

Threshold: ● Carrier Limit (Configured on Data Usage Monitoring) ○ Warning Limit (Configured on Data Usage Monitoring) ○ Custom

□ Failover by Schedule

12. Click **Save**.

Failover retries conditions:

- Failed retries to failover: Applies to Ping Trigger and Signal Strength triggers.
- Successful retries to recover: Applies to Ping Trigger and Signal Strength triggers.
- All the other triggers do not have retries: Only one failure or success will trigger the Failover or Failback.

Cellular modem behavior with two SIM cards configured for Failover:

- When two SIM cards of the same connection are configured, only one can be active at a time. *Ping and Signal Strength* triggers are applicable on the active SIM card only.
- In a Circular SIM swap, if the two SIM cards are below (lower order) the currently active failover connection, the modem continuously swaps to the other SIM when the selected SIM fails.
- When one of the SIM cards is the last connection on the failover, the *Ping and Signal Strength* triggers from the first SIM to the last SIM until the first SIM is active again. This is also a Circular SIM swap, however, the difference is that it can also change the active failover connection (failback).

CLI Configuration Example

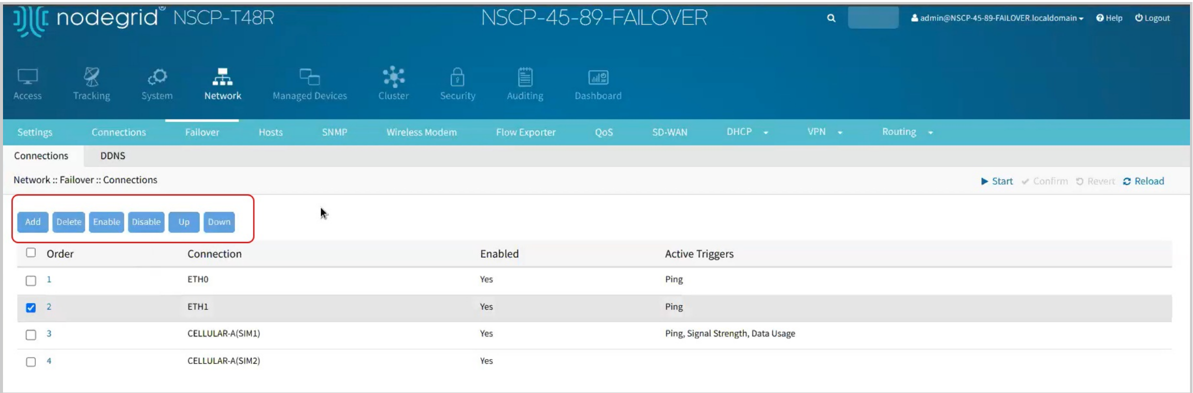
ActionScript

ActionScript Copy

```
[admin@nodegrid /]# cd /settings/network_failover/connections/
[admin@nodegrid connections]# show
  order  connection        enabled  active triggers
  =====  ================  =======  =============================
  1      CELLULAR-A(SIM1)  yes      data usage, failback schedule
  2      SFP0              yes      ping
  3      ETH0              yes      ping
  4      SFP1              yes      ping
  5      ETH1              yes      ping
  6      CELLULAR-A(SIM2)  yes
[admin@nodegrid connections]# add
[admin@nodegrid {connections}]# show
connection = CELLULAR-A
sim_card = 1
enabled = yes
order = 7
failed_retries_to_failover = 2
successful_retries_to_recover = 1
interval_between_retries = 5
enable_failover_by_ping = yes
ping_destination = ipv4_default_gateway
enable_failover_by_signal_strength = no
enable_failover_by_data_usage = no
enable_failover_by_schedule = no
enable_failback_by_schedule = no
[admin@nodegrid {connections}]# set connection=ETH2
[admin@nodegrid {connections}]# set ping_destination=custom_ip_address_or_domain
[admin@nodegrid {connections}]# set ping_custom_address=api.zpesystems.com
[admin@nodegrid {connections}]# set failed_retries_to_failover=3
[admin@nodegrid {connections}]# set successful_retries_to_recover=2
[admin@nodegrid {connections}]# set interval_between_retries=4
[admin@nodegrid {connections}]# set order=5
[admin@nodegrid {connections}]# commit
```

Managing Failover Connections

After you have configured a failover connection you can perform the following operations:



□ Order	Connection	Enabled	Active Triggers
□ 1	ETH0	Yes	Ping
☑ 2	ETH1	Yes	Ping
□ 3	CELLULAR-A(SIM1)	Yes	Ping, Signal Strength, Data Usage
□ 4	CELLULAR-A(SIM2)	Yes	

- **Delete**: Select the failover connection and click **Delete**.
- **Enable**: If not already enabled, select the failover connection and click **Enable**. Enabling the connection makes the failover connection active.
- **Disable**: If you want to disable a failover connection, select the failover connection and click **Disable**. If disabled, although the failover connection is configured, it will not be active. Therefore, this connection automatically gets eliminated from the failover connection list.
- **Up** and **Down**: You can increase or decrease the order of the failover connection by clicking on the **Up** and **Down** buttons respectively.
- CLI Configuration Example

-
-
-

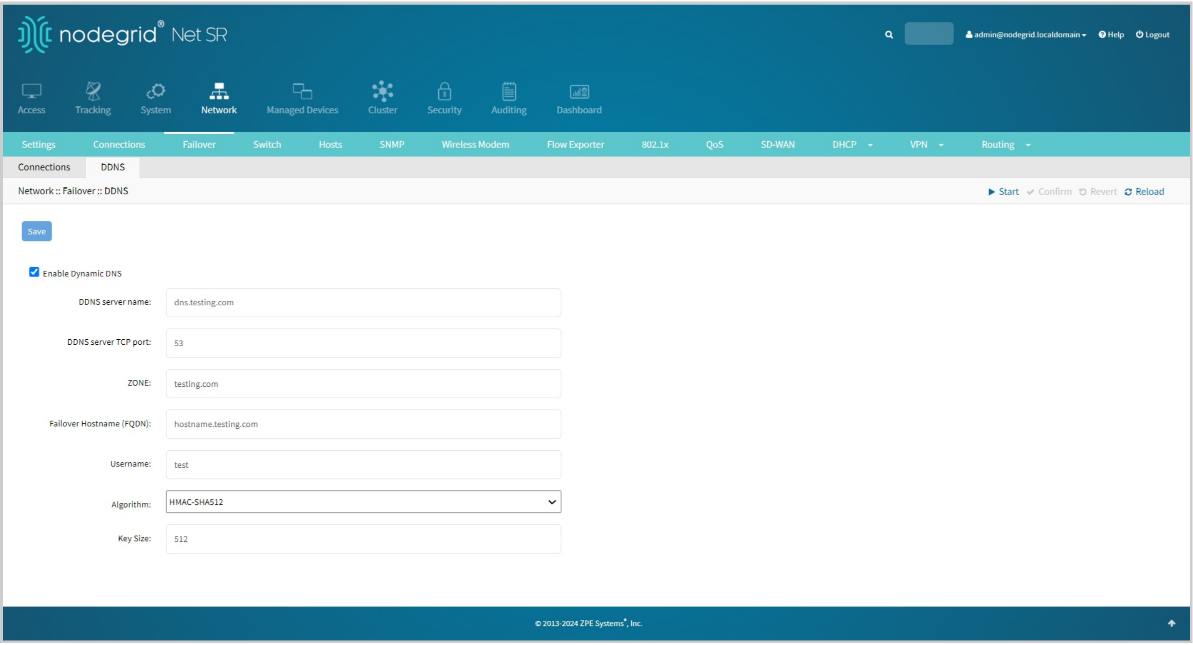
ActionScript Copy

```
[admin@nodegrid /]# cd /settings/network_failover/connections/
[admin@nodegrid connections]# show
  order  connection        enabled  active triggers
  =====  ================  =======  =============================
  1      CELLULAR-A(SIM1)  yes      data usage, failback schedule
  2      SFP0              yes      ping
  3      ETH0              yes      ping
  4      SFP1              yes      ping
  5      ETH1              yes      ping
  6      CELLULAR-A(SIM2)  yes
[admin@nodegrid connections]# delete 4
[+admin@nodegrid connections]# show
  order  connection        enabled  active triggers
  =====  ================  =======  =============================
  1      CELLULAR-A(SIM1)  yes      data usage, failback schedule
  2      SFP0              yes      ping
  3      ETH0              yes      ping
  4      ETH1              yes      ping
  5      CELLULAR-A(SIM2)  yes
[+admin@nodegrid connections]# up 3
[+admin@nodegrid connections]# show
  order  connection        enabled  active triggers
  =====  ================  =======  =============================
  1      CELLULAR-A(SIM1)  yes      data usage, failback schedule
  2      ETH0              yes      ping
  3      SFP0              yes      ping
  4      ETH1              yes      ping
  5      CELLULAR-A(SIM2)  yes
[+admin@nodegrid connections]# down 1
[+admin@nodegrid connections]# show
  order  connection        enabled  active triggers
  =====  ================  =======  =============================
  1      ETH0              yes      ping
  2      CELLULAR-A(SIM1)  yes      data usage, failback schedule
  3      SFP0              yes      ping
  4      ETH1              yes      ping
  5      CELLULAR-A(SIM2)  yes
[+admin@nodegrid connections]# disable 1,3
[+admin@nodegrid connections]# show
  order  connection        enabled  active triggers
  =====  ================  =======  =============================
  1      ETH0              no
  2      CELLULAR-A(SIM1)  yes      data usage, failback schedule
  3      SFP0              no
  4      ETH1              yes      ping
  5      CELLULAR-A(SIM2)  yes
[+admin@nodegrid connections]# enable 3
[+admin@nodegrid connections]# show
  order  connection        enabled  active triggers
  =====  ================  =======  =============================
  1      ETH0              no
  2      CELLULAR-A(SIM1)  yes      data usage, failback schedule
  3      SFP0              yes      ping
  4      ETH1              yes      ping
  5      CELLULAR-A(SIM2)  yes
```

Configuring DDNS

Configuring Dynamic DNS (DDNS) in a failover scenario ensures that there is continuity in services by automatically updating the DNS records to redirect the traffic to the next connection when the current connection has failed. Before you configure the DDNS ensure that there are at least two failover connections configured. The Nodegrid device interfaces should be able to reach the DDNS server and need to have two network connections with public IPs, for example, ETH0 and ETH1. To configure DDNS:

1. Log in to the Nodegrid UI.
2. Navigate to the path *Network:: Failover*.
3. Click **DDNS**.
4. Select the checkbox **Enable Dynamic DNS**.



☑ Enable Dynamic DNS

DDNS server name: dns.testing.com

DDNS server TCP port: 53

ZONE: testing.com

Failover Hostname (FQDN): hostname.testing.com

Username: test

Algorithm: HMAC-SHA512

Key Size: 512

5. Enter the DDNS server name. The server name allows the Nodegrid device to update the IP addresses associated with this name.
6. Enter the DDNS server TCP port number.
7. Enter the zone name.
8. Enter the Failover Hostname (FQDN) of the Nodegrid device.
9. Enter the username of the DDNS server.
10. To secure the connection between the DDNS server and the Nodegrid device, select the required algorithm and enter the key size.
11. Click **Save**.

CLI Configuration Example

ActionScript Copy

```
[admin@nodegrid /]# cd /settings/network_failover/ddns/
[admin@nodegrid ddns]# set enable_dynamic_dns=yes
[+admin@nodegrid ddns]# set ddns_server_name=dns.testing.com
[+admin@nodegrid ddns]# set ddns_server_tcp_port=53
[+admin@nodegrid ddns]# set zone=testing.com
[+admin@nodegrid ddns]# set failover_hostname=hostname.testing.com
[+admin@nodegrid ddns]# set username=test
[+admin@nodegrid ddns]# set algorithm=HMAC-SHA512
[+admin@nodegrid ddns]# set key_size=512
[admin@nodegrid ddns]# commit
```

Tracking Failover

When a failover occurs you can track the status of the failover history of devices by navigating to *Tracking :: Network :: Failover.* For more information, see Tracking Network Failover.

Switch tab (NSR, NSR Lite, GSR, and BSR)

These functions are only available on Nodegrid NSR, NSR Lite, GSR, and BSR devices.

NSR

The NSR built-in switch ports are SFP0, SFP1, BACKPLANE0 and BACKPLANE1. The NSR also supports network expansion cards. By factory default, the SFP0, BACKPLANE0, and the network expansion card ports are in VLAN 1; the SFP1 and BACKPLANE1 are in VLAN2.

The network expansion cards need to be placed in the front three slots to reach the Nodegrid OS.

NSR Lite

The NSR Lite doesn't have a built-in switch, but it supports network expansion cards. The switch ports are connected to the OS via a tunnel interface BACKPLANE0. The network cards need to be placed in the front 3 slots, and If more than one network expansion card is present, they need to be in consecutive slots.

GSR

The GSR has a built-in 8-port switch, BACKPLANE0 and BACKPLANE1. The first four ports also support PoE.

BSR

The BSR has a built-in 4-port switch and BACKPLANE0.

Backplane sub-tab

Backplane settings configure the switch interfaces directly exposed to the Nodegrid OS. For the Nodegrid OS to communicate with any existing switch ports, at least one of the backplane interfaces must be part of the specific VLAN. The backplane settings display the current VLAN associations. If the switch backplane port is added as a tagged member of a VLAN, a corresponding VLAN interface needs to be created in Nodegrid OS to receive the packets from the switch.

The Backplane settings also configure the switch ports connected to the compute expansion card. The compute card has two 10G network interfaces that are connected to the built-in switch in NSR, and to the neighbor slot network expansion card in NSR Lite. The switch ports connected to the compute card appear as slot<X>-0 and slot<X>-1, where X is the slot number where the compute card is inserted.

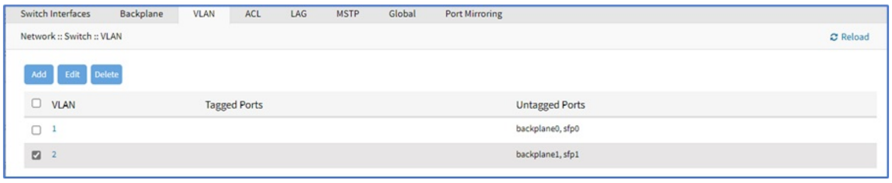
> NOTE
>
> Display varies depending on device – GSR, BSR, or NSR).

Edit Backplane Settings

1. Go to *Network :: Switch :: Backplane*.
2. Make changes, as needed:
   a. **Port VLAN ID:** VLAN to be assigned to the untagged ingress packets coming from Nodegrid OS
   b. **Jumbo Frame:** If enabled, the Jumbo Frame configured under Global will be
   c. **DHCP Snooping:** Trusted means this is a trusted port so DHCP Server Responses will be accepted; Untrusted means the DHCP Server responses will be dropped. This configuration is applicable only if DHCP Snooping is enabled under Global, and DHCP Snooping is enabled in the VLANs in the DHCP Snooping sub-tab.
3. Click **Save**.

VLAN sub-tab

It shows the VLAN configuration of the switch ports.



	VLAN	Tagged Ports	Untagged Ports
☐	1		backplane0, sfp0
☑	2		backplane1, sfp1

VLAN-tagged packets are accepted if the port is a member of that VLAN; VLAN untagged packets are accepted and forwarded to the port that matches the Port VLAN Id.

Untagged/Access Ports

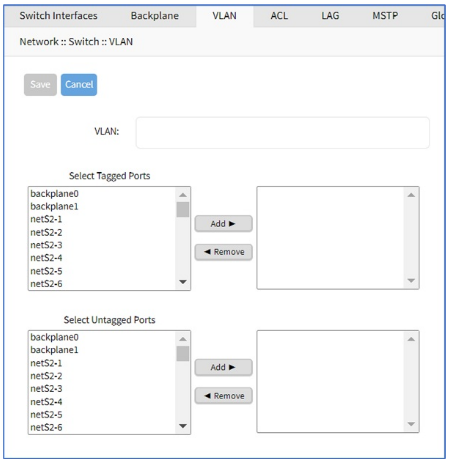
Packets egressing from Untagged (or Access) ports are untagged, i.e., they don't have the VLAN tag.

Tagged/Trunk Ports

Tagged ports accept any packet that belongs to an assigned VLAN. The VLAN must exist before the port can be assigned. The Egress packet includes the VLAN tag.

Add VLAN

1. Go to *Network :: Switch :: VLAN*.
2. Click **Add** (displays dialog).



3. Enter **VLAN**
4. On *Select Tagged Ports*, select from the left-side panel, and click **Add►** to move to the right-side panel. To remove from the right-side panel, select and click **◄Remove**.
5. On *Select Untagged Ports*, select from the left-side panel, and click **Add►** to move to the right-side panel. To remove from the right-side panel, select and click **◄Remove**.
6. Click **Save**.

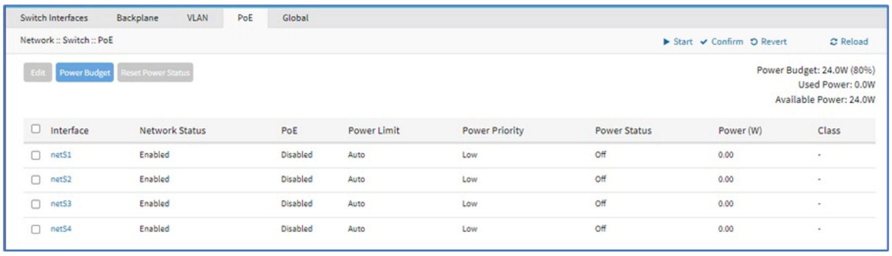
Edit VLAN

1. Go to *Network :: Switch :: VLAN*.
2. Select the checkbox next to the item to edit.
3. Click **Edit** (displays dialog).
4. Make changes, as needed.
5. Click **Save**.

Delete VLAN

1. Go to *Network :: Switch :: VLAN*.
2. Select checkbox next to item to delete.
3. Click **Delete**.
4. On the confirmation dialog, click **OK**.

PoE sub-tab (NSR with PoE card, GSR)

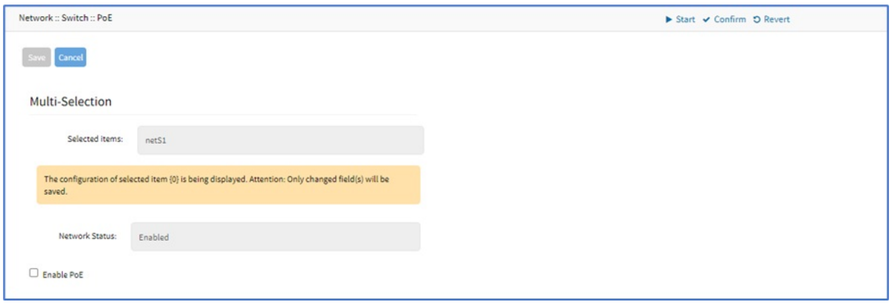


Power Budget: 24.0W (80%)
Used Power: 0.0W
Available Power: 24.0W

□ Interface	Network Status	PoE	Power Limit	Power Priority	Power Status	Power (W)	Class
□ netS1	Enabled	Disabled	Auto	Low	Off	0.00	-
□ netS2	Enabled	Disabled	Auto	Low	Off	0.00	-
□ netS3	Enabled	Disabled	Auto	Low	Off	0.00	-
□ netS4	Enabled	Disabled	Auto	Low	Off	0.00	-

Edit PoE Configuration

1. Go to *Network :: Switch :: PoE*.
2. Select checkbox of interface to edit.
3. Click **Edit** (displays dialog).



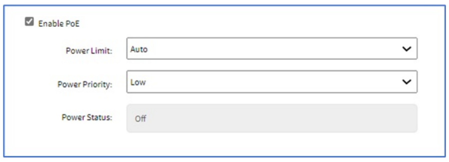
Selected items: netS1

The configuration of selected item {0} is being displayed. Attention: Only changed field(s) will be saved.

Network Status: Enabled

□ Enable PoE

4. **If Enable PoE** checkbox selected (expands dialog):



☑ Enable PoE

Power Limit: Auto

Power Priority: Low

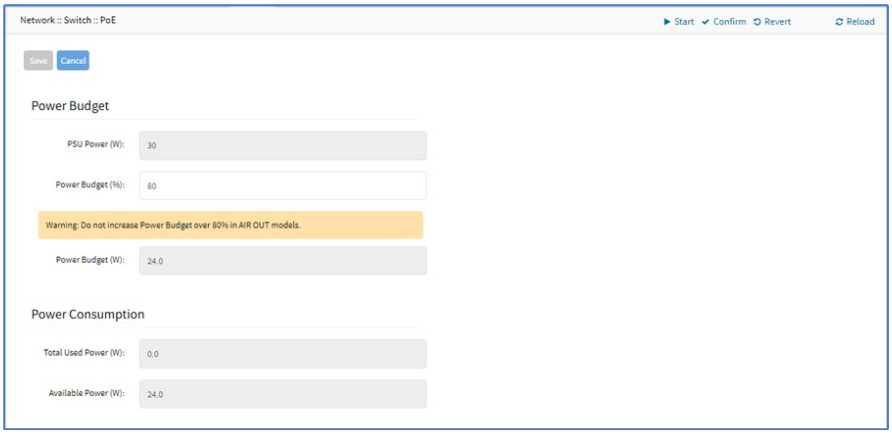
Power Status: Off

   a. **Power Limit** drop-down, select one (Auto, 6W, 12W, 18W, 24W, 30W). For Auto, the power limit depends on the PoE device class.
   b. **Power Priority** drop-down, select one (Low, High, Critical). The order ports are powered off in case of power consumption is over the power budget, where the port with Low priority is powered off first and the Critical is powered off last.

5. Click **Save**.

Configure Power Budget

1. Go to *Network :: Switch :: PoE*.
2. Select the checkbox of the interface.
3. Click **Power Budget** (displays dialog):



PSU Power (W): 30

Power Budget (%): 80

Warning: Do not increase Power Budget over 80% in AIR OUT models.

Power Budget (W): 24.0

Total Used Power (W): 0.0

Available Power (W): 24.0

4. In *Power Budget* menu, modify **Power Budget (%).**
5. In *Power Consumption* menu, review values.
6. Click **Save**.

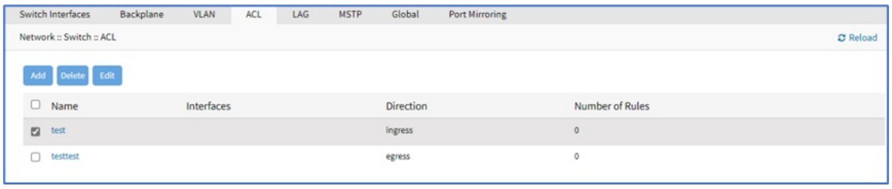
Reset Power Status

1. Go to *Network :: Switch :: PoE*.
2. Select checkbox of interface.
3. Click **Reset Power Status** to reset error Power Status, e.g. Over Budget, Overcurrent, PSU Fault, etc.

The power error/alarm status of the selected interface is reset.

ACL sub-tab (NSR only)

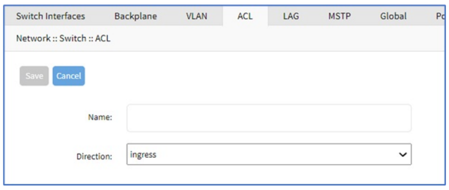
With the ACL (access control list) option, custom ACL rules can be managed (add, delete, edit) for each interface.



□	Name	Interfaces	Direction	Number of Rules
☑	test		ingress	0
□	testtest		egress	0

Add ACL

1. Go to *Network :: Switch :: ACL*.
2. Click **Add** (displays dialog).



Name:

Direction: ingress

   a. Enter **Name**.
   b. From the **Direction** drop-down, select one (ingress, egress)

3. Click **Save**.

Add ACL Rules

To add ACL Rules:

1. Go to Network :: Switch :: ACL.
2. Click one of the added ACL names.
3. Click Add (displays dialog).
4. Select if the action should be **Deny** or **Permit** and enter the source or destination MAC or IP, and/or VLAN ID.

-- add screenshot of Add Rule --

Edit ACL

1. Go to *Network :: Switch :: ACL*.
2. Select the checkbox next to the item to edit.
3. Click **Edit** (displays dialog).
4. Make changes, as needed.
5. Click **Save**.

Delete ACL

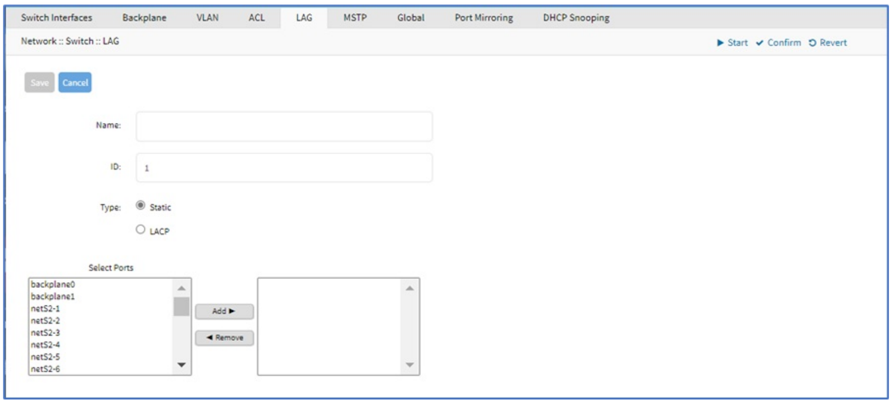
1. Go to *Network :: Switch :: ACL*.
2. Select the checkbox next to the item to delete.
3. Click **Delete**.
4. On the confirmation dialog, click **OK**.

LAG sub-tab (NSR only)

Link aggregation allows the combination of multiple network connections in parallel. This increases throughput beyond what a single connection sustains. Redundancy occurs in the event one of the links fails.

Add LAG

1. Go to *Network :: Switch :: LAG*.
2. Click **Add** (displays dialog).



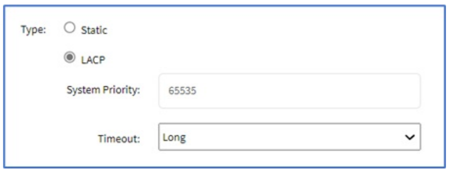
Name:

ID: 1

Type: ● Static ○ LACP

   a. Enter **Name**.
   b. Enter **ID**.

3. On *Type* menu, select one:
   a. **Static** radio button
   b. **LACP** radio button (expands dialog). Enter System Priority. On the Timeout drop-down, select one (Long, Short).

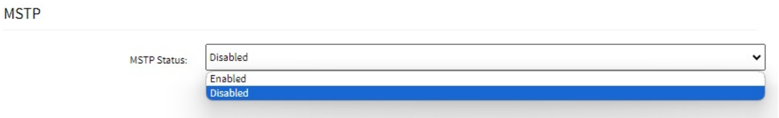


Type: ○ Static ● LACP

System Priority: 65535

Timeout: Long

4. In *Select Ports*, select from the left-side panel, and click **Add►** to move to the right-side panel. To remove from the right-side panel, select and click **◄Remove**.
5. Change MSTP Status to Enable to enable Spanning Tree on the LAG interface. The Spanning Tree Status under Global also needs to be enabled.



MSTP

MSTP Status: Disabled

6. Click **Save**.

Edit LAG

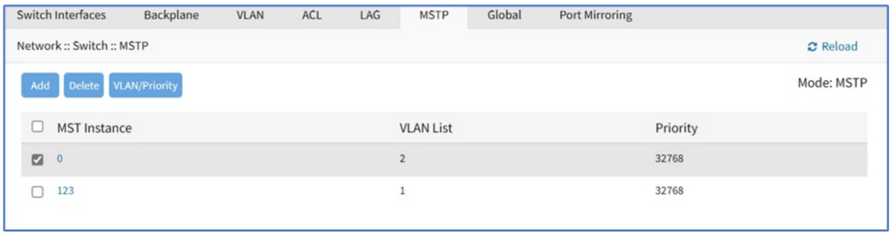
1. Go to *Network :: Switch :: LAG*.
2. In the *Name* column, click on a name (displays dialog).
3. Make changes, as needed.
4. Click **Save**.

Delete LAG

1. Go to *Network :: Switch :: LAG*.
2. Select checkbox next to item to delete.
3. Click **Delete**.
4. On the confirmation dialog, click **OK**.

MSTP sub-tab (NSR and NSR LITE only)

MSTP (Multiple Spanning Tree Protocol) exchanges BPDU (Bridge Protocol Data Units) to prevent loops in MSTI (Multiple Spanning Tree Instances) and CIST (Common and Internal Spanning Tree).

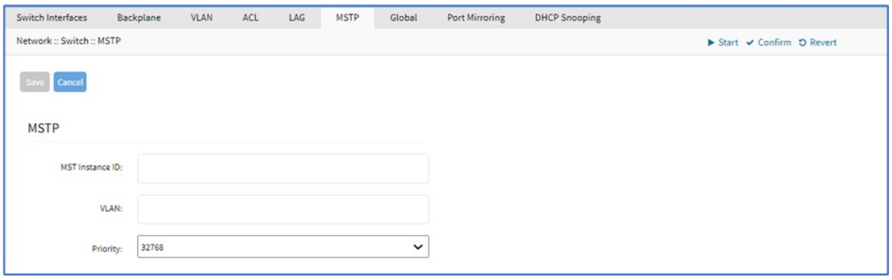


□ MST Instance	VLAN List	Priority
☑ 0	2	32768
□ 123	1	32768

Besides the changes in the MSTP sub-tab, the Spanning Tree Status needs to be enabled under the Global sub-tab, and the STP Status needs to be enabled in the interfaces under the Switch Interfaces sub-tab.

Add MSTP

1. Go to *Network :: Switch :: MSTP*.
2. Click **Add** (displays dialog).



MST Instance ID:

VLAN:

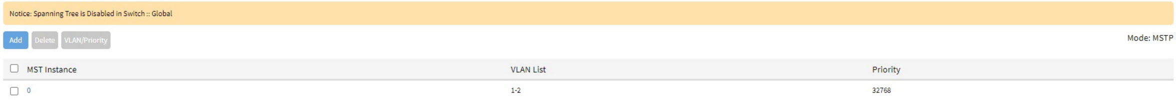
Priority: 32768

   a. Enter **MST Instance ID,**
   b. Enter **VLAN,**
   c. On **Priority** drop-down, select one (0, 4096, 8192, 12288, 16384, 20480, 24594, 28672, 32768, 40960, 45056, 49152, 53248, 57344, 61440)

3. Click **Save**.

Change MST instance port priority and cost

1. Go to Network :: Switch :: MSTP.
2. In the MST Instance column, click an instance number.
3. In the Interface column, click the interface name, or select multiple interfaces


Notice: Spanning Tree is Disabled in Switch :: Global

□ MST Instance	VLAN List	Priority
□ 0	1-2	32768

4. Click **Edit**.
5. As needed, make changes to port priority and cost. The lower the priority
6. number, the higher the priority.
7. Click **Save**.

Edit MSTP

1. Go to *Network :: Switch :: MSTP*.
2. In *Interface* column, click a name (displays dialog).
3. As needed, make changes.
4. Click **Save**.

Delete MSTP

1. Go to *Network :: Switch :: MSTP*.
2. In the *MST Interface* column, select the checkbox.
3. Click **Delete**.
4. On the confirmation dialog, click **OK**.

View MSTP State and MST Role

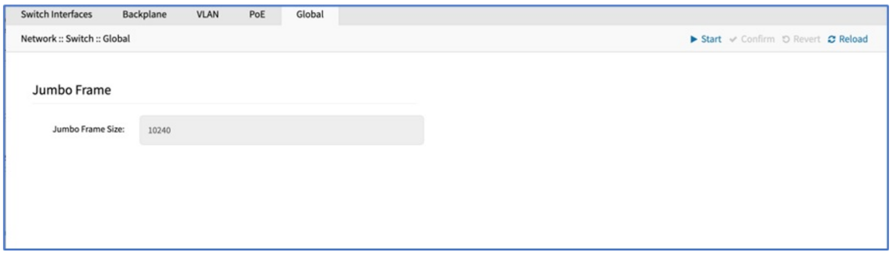
Go to Tracking :: Network :: MSTP to view the MSTP State and Role.

Set VLAN/Priority

1. Go to *Network :: Switch :: MSTP*.
2. In the *MST Interface* column, select the checkbox.
3. Click **VLAN/Priority** (displays dialog).
4. Make changes,
5. Make changes to the MST instance priority, or to the VLANs associated with the MST instance.
6. Click **Save**.

Global sub-tab (BSR, GSR)

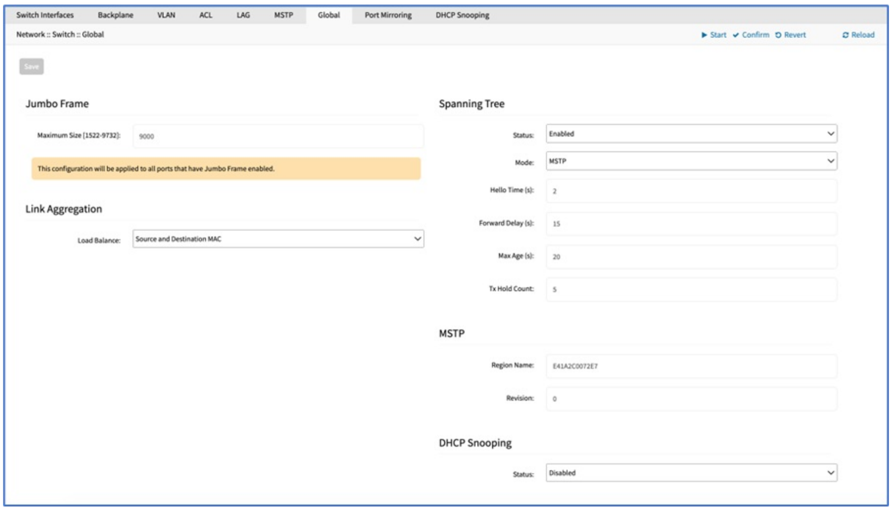
Details are read only.



Jumbo Frame

Jumbo Frame Size: 10240

Global sub-tab (NSR, NSR LITE only)



Network :: Switch :: Global

Jumbo Frame

Maximum Size [1522-9732]: 9000

This configuration will be applied to all ports that have Jumbo Frame enabled.

Link Aggregation

Load Balance: Source and Destination MAC

Spanning Tree

Status: Enabled

Mode: MSTP

Hello Time (s): 2

Forward Delay (s): 15

Max Age (s): 20

Tx Hold Count: 5

MSTP

Region Name: E41A2C0072E7

Revision: 0

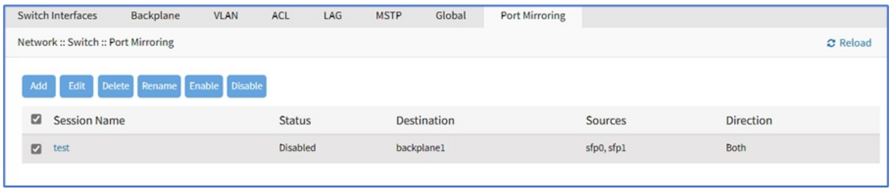
DHCP Snooping

Status: Disabled

Edit Global Settings

1. Go to *Network :: Switch :: Global*.
2. In the *Jumbo Frame* menu, update **Maximum Size (1522 to 9732).**
   When the Jumbo Frame is enabled in the switch interfaces, packets with MRU up to the Jumbo Frame size will be accepted.
3. In the *Link Aggregation* menu, **Load Balance**drop-down, select the load balance to use with the LAG members:
   a. Source and Destination IP
   b. Source and Destination MAC
   c. Source and Destination MAC and IP
   d. Source and Destination MAC and IP and TCP/UDP Ports
4. On the *Spanning Tree* menu, enable/disable Spanning Tree and make changes, as needed:
   a. **Status** drop-down, select one (Enabled, Disabled) drop-down, select one (Enabled, Disabled). To enable Spanning Tree, enable Status and enable STP Status in the switch ports.
   b. **Hello Time (sec):** transmission interval between BPDUs. The default value is 2.
   c. **Forward Delay (sec):** time spent in the listening and learning states. The default value is 15.
   d. **Max Age (sec):** maximum time that the switch can wait without receiving a BPDU before attempting to regenerate a new spanning tree. The default value is 20.
   e. **Tx Hold Count:** maximum number of BPDUs transmitted per port in a given second. The default value is 5.
5. In the *MTSP* menu, enter **Region Name** and **Revision**. enter Region Name and Revision. The Region Name must match the Region Name of the connected switches with identical configuration.
6. On the *DHCP Snooping* menu, **Status** drop-down, select one (Enabled, Disabled). Status drop-down, select one (Enabled, Disabled). If enabled, only trusted interfaces in a VLAN that has DHCP enabled will accept DHCP Server responses. When disabled, the DHCP Snooping functionally is disabled globally.
7. Click **Save**.

Port Mirroring sub-tab (NSR only)



Network :: Switch :: Port Mirroring

☑	Session Name	Status	Destination	Sources	Direction
☑	test	Disabled	backplane1	sfp0, sfp1	Both

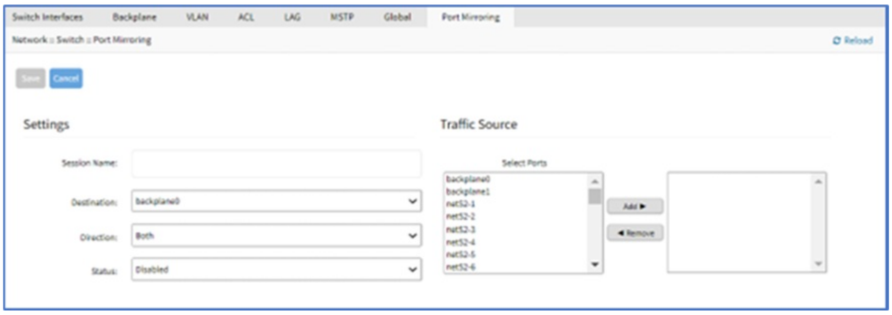
Port mirroring allows copying the traffic passing through a port to another port, to allow a remote system to analyze the packets, for instance with tcpdump or Wireshark.

The Source port is the port where the packets will be copied from and the Destination port is the destination for the mirrored traffic. The system running tcpdump or Wireshark should be connected to the Destination port.

There is a restriction where the source and destination ports need to be in the same network card, or if the source is a built-in port (instead of a network card port), the destination also needs to be a built-in port.

Add Port Mirroring

1. Go to *Network :: Switch :: Port Mirroring*.
2. Click **Add** (displays dialog).



Network :: Switch :: Port Mirroring

Session Name:

Destination: backplane0

Direction: Both

Status: Disabled

3. On *Settings* menu:
   a. Enter **Session Name**.
   b. On **Destination** drop-down, select one (backplane0, backplane1, netS2-(1-16), netS3-(1-8), netS4-(1-16), sfp0, sfp1, slot1-0, slot1-1).
   c. On **Direction** drop-down, select one (Both, Egress, Ingress).
   d. On **Status** drop-down, select one (Enabled, Disabled).
4. On *Traffic Source* menu: To add, select from left-side panel, click **Add►** to move to right-side panel. To remove from right-side panel, select, and click **◄Remove**.
5. Click **Save**.

Edit Port Mirroring

1. Go to *Network :: Switch :: Port Mirroring*.
2. In *Session Name* column, select checkbox.
3. Click **Edit**.
4. Make changes, as needed.
5. Click **Save**.

Delete Port Mirroring

1. Go to *Network :: Switch :: Port Mirroring*.
2. In *Session Name* column, select checkbox.
3. Click **Delete**.
4. On the confirmation dialog, click **OK**.

Rename Port Mirroring

1. Go to *Network :: Switch :: Port Mirroring*.
2. In the *Session Name* column, select checkbox.
3. Click **Rename**.
4. On the dialog, enter **New Name**.
5. Click **Save**.

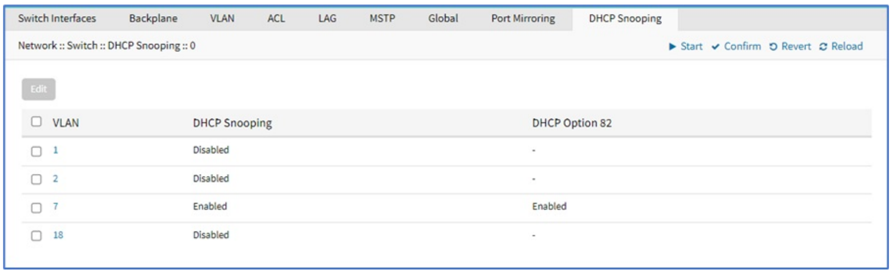
Enable Port Mirroring

1. Go to *Network :: Switch :: Port Mirroring*.
2. In *Session Name* column, select checkbox.
3. Click **Enable** (enables port mirroring).

Disable Port Mirroring

1. Go to *Network :: Switch :: Port Mirroring*.
2. In *Session Name* column, select checkbox.
3. Click **Disable** (disables port mirroring).

DHCP Snooping sub-tab (NSR only)



Network :: Switch :: DHCP Snooping :: 0

☐ VLAN	DHCP Snooping	DHCP Option 82
☐ 1	Disabled	-
☐ 2	Disabled	-
☐ 7	Enabled	Enabled
☐ 18	Disabled	-

The DHCP Snooping provides a defense against untrusted DHCP Servers providing IPs. This feature can be enabled per VLAN, and it requires that the DHCP. Snooping is also enabled under Global. The ports that have trusted DHCP Servers should be configured as Trusted. When DHCP Snooping is enabled, the DHCP requests will be broadcasted to trusted ports, and DHCP responses from trusted ports will be forwarded. The DHCP responses from untrusted ports will be dropped.

DHCP Option 82 can also be enabled when DHCP Snooping is enabled. The DHCP Option 82 adds the Circuit ID to the DHCP request so that the DHCP Server can assign IPs based on Circuit ID. If the Nodegrid DHCP Server is used, the Agent Circuit ID needs to be configured under the DHCP Server Hosts sub-tab.

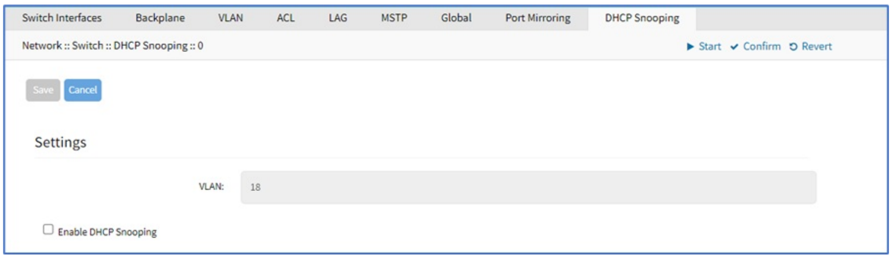
There are 3 options for the Circuit ID format:

- vlan:interface
- hostname:vlan:interface and
- hostname:interface
- vlan:interface: “VLAN0005:netS1-1”
- hostname:vlan:interface: “mynodegrid:VLAN0005:netS1-1”
- hostname:interface: “mynodegrid:netS1-1”

Enable DHCP Snooping

(available in v5.6+)

1. Go to *Network :: Switch :: DHCP Snooping*.
2. Select a checkbox with a disabled VLAN.
3. Click **Edit** (displays dialog), and enter details:



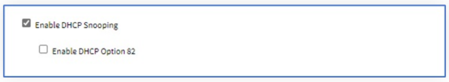
Network :: Switch :: DHCP Snooping :: 0

Settings

VLAN: 18

☐ Enable DHCP Snooping

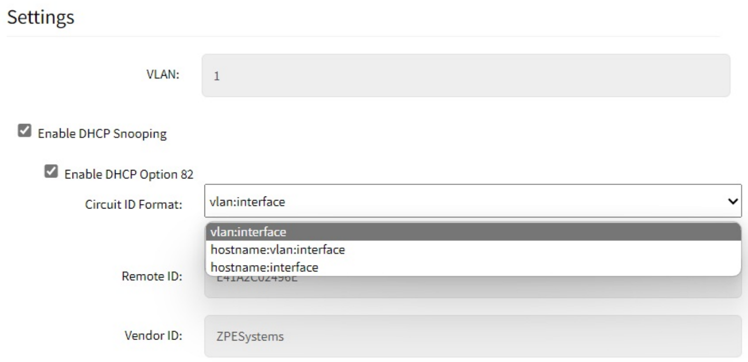
4. Select **Enable DHCP Snooping** (expands dialog).



☑ Enable DHCP Snooping

☐ Enable DHCP Option 82

   a. **Enable DHCP Option 82** (expands dialog). (v5.6+)



Settings

VLAN: 1

☑ Enable DHCP Snooping

☑ Enable DHCP Option 82

Circuit ID Format: vlan:interface

Remote ID: E41A2C02496E

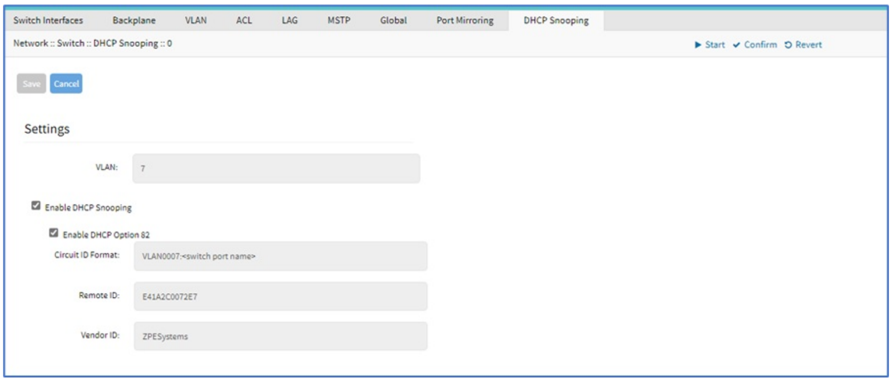
Vendor ID: ZPESystems

5. Review the Circuit ID format details.
6. If changes are made, click **Save**.

Disable DHCP Snooping

(available in v5.6+)

1. Go to *Network :: Switch :: DHCP Snooping*.
2. Select a checkbox with an enabled VLAN.
3. Click **Edit** (displays dialog).



Network :: Switch :: DHCP Snooping :: 0

Settings

VLAN: 7

☑ Enable DHCP Snooping

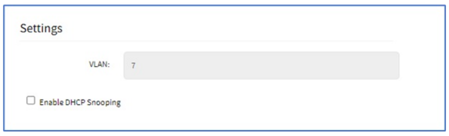
☑ Enable DHCP Option 82

Circuit ID Format: VLAN0007:<switch port name>

Remote ID: E41A2C0072E7

Vendor ID: ZPESystems

4. If **Enable DHCP Snooping** is unselected (expands dialog).



Settings

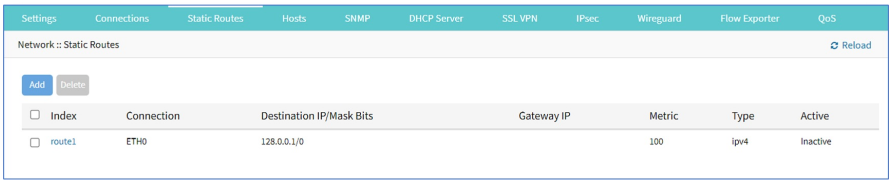
VLAN: 7

☐ Enable DHCP Snooping

5. If changes are made, click **Save**.

Routing tab

Administrators can define and manage static routes. Routes can be created for IPv4 and IPv6, assigned to specific network interfaces.



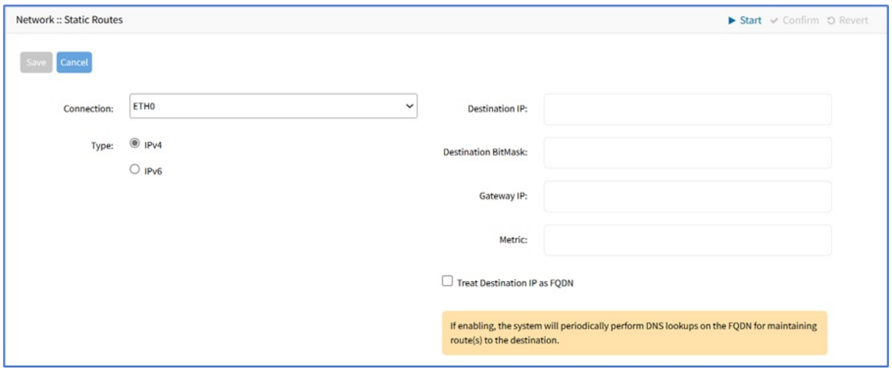
Network :: Static Routes

□	Index	Connection	Destination IP/Mask Bits	Gateway IP	Metric	Type	Active
□	route1	ETH0	128.0.0.1/0		100	ipv4	Inactive

Manage Static Routes

Add Static Route

1. Go to *Network :: Routing*.
2. Select Static Routes from the **Routing** dropdown list.
3. Click **Add** (displays dialog).



Connection: ETH0

Type: ● IPv4 ○ IPv6

Destination IP:

Destination BitMask:

Gateway IP:

Metric:

□ Treat Destination IP as FQDN

If enabling, the system will periodically perform DNS lookups on the FQDN for maintaining route(s) to the destination.

4. On **Connection** drop-down, select one (ETH0, ETH1, hotspot)
5. On *Type*menu, select one:
   - **IPv4** radio button
   - **IPv6** radio button
6. Enter details:
   a. **Destination IP**
   b. **Destination BitMask**
   c. **Gateway IP**
   d. **Metric** (routing metric value – for normal routes, default: 100)
   e. **Treat Destination IP as FQDN** checkbox (if selected, closes **Destination BitMask** field).
7. Click **Save**.

Edit Static Route

1. Go to *Network :: Static Routes*.
2. In the *Index* column, click on the name (displays dialog).
3. Make changes as needed.
4. Click **Save**.

Delete Static Route

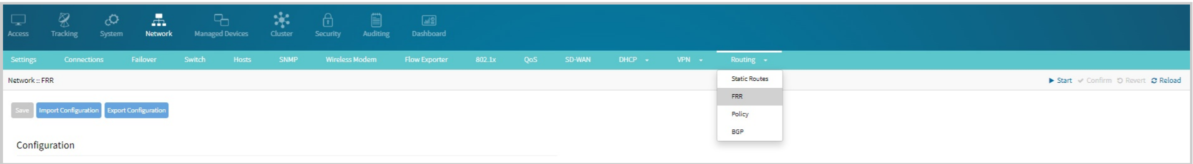
1. Go to *Network :: Static Routes*.
2. In the list, select a checkbox.
3. Click **Delete**.

FRR Configuration Management

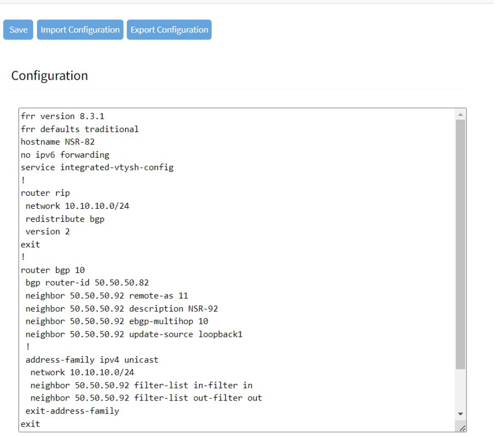
The **FRR** page allows users to view and modify all Free Range Routing (FRR) protocol configurations in a single place. Since FRR configuration is quite extensive and complex to remember the command involved in execution, this page is very useful for reviewing protocol configuration, executing configuration adjustments, and creating configuration backup.

Configuring FRR

1. Go to *Network :: Routing.*
2. Select **FRR** from the **Routing** dropdown list.



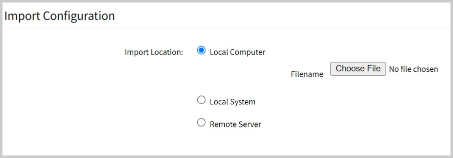
3. In the **Configuration** section, enter the required configuration.
   a. Enter FRR Configuration.



```
frr version 8.3.1
frr defaults traditional
hostname NSR-82
no ipv6 forwarding
service integrated-vtysh-config
!
router rip
 network 10.10.10.0/24
 redistribute bgp
 version 2
exit
!
router bgp 10
 bgp router-id 50.50.50.82
 neighbor 50.50.50.92 remote-as 11
 neighbor 50.50.50.92 description NSR-92
 neighbor 50.50.50.92 ebgp-multihop 10
 neighbor 50.50.50.92 update-source loopback1
 !
 address-family ipv4 unicast
  network 10.10.10.0/24
  neighbor 50.50.50.92 filter-list in-filter in
  neighbor 50.50.50.92 filter-list out-filter out
 exit-address-family
exit
```

   b. Click **Save**.

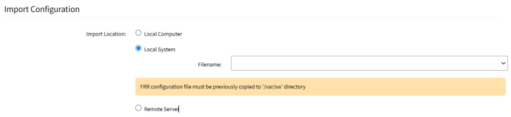
4. To import configuration, click **Import Configuration.**
   a. **Local Computer:** If the *FRR.conf* file is located on the Local Computer, click *Choose File* to browse to the location where the file is present.
      i. Select the file.
      ii. Click **Open.**


Import Configuration

Import Location: ● Local Computer ○ Local System ○ Remote Server

Filename: Choose File No file chosen

   b. **Local System:** Ensure that the FRR.conf file is already available in the local System. Once the file is available, select the file from the **Filename** drop-down list.


Import Configuration

Import Location: ○ Local Computer ● Local System ○ Remote Server

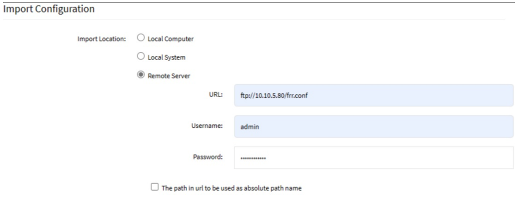
Filename:

FRR configuration file must be previously copied to '/var/sw' directory

   c. **Remote Server:** Configure the remote location where the *FRR.conf* file is available:
      i. **URL:** Enter the URL to the *FRR.conf* file. The supported URL formats are:
         - PROTOCOL://SERVER_ADDRESS/REMOTEFILE
         - PROTOCOL://SERVER_ADDRESS:SERVER_PORT/REMOTEFILE

         where, PROTOCOL can be TFTP, FTP, HTTP, HTTPS, SCP, and SFTP

         SERVER_ADDRESS can be IPv4, IPv6, or name
      ii. **Username:** Username to log in to the remote server.
      iii. **Password:** Password to log in to the remote server.


Import Configuration

Import Location: ○ Local Computer ○ Local System ● Remote Server

URL: ftp://10.10.5.80/frr.conf

Username: admin

Password: ••••••••••••

□ The path in url to be used as absolute path name

5. Click **Save.**

Verifying the Router Configuration Changes

To verify the changes performed using the FRR configuration:

1. Go to **Access:: Console.**

   ActionScript Copy

   ```
   exec frr
   do show running-config
   ```

2. Enter the following command:

The command displays the newly configured FRR details as a response.

Configuring BGP Policies

This section explains how to configure the Border Gateway Protocol (BGP) routing policy IP prefix list. A prefix list identifies which routes must be accepted or denied in a BGP network. The prefixes represent the match criteria to apply the filter. Routes are then either permitted or denied based on these specified criteria. For example, if there is a need for a BGP network to disallow the distribution of a route with the IP address 10.1.1.3, this prefix can be included in the match criteria within the route map to block connections for this IP. To configure the prefix list:

1. Log into the Nodegrid Web UI.
2. Navigate to *Network::Routing::Policy.*
3. Click **Add**.
4. Specify a name for the prefix list.
5. Select the IPv4 or IPv6 address family.
6. Specify a meaningful description of the prefix list.
7. Specify the sequence in which the prefix entries will be processed. You can include multiple sequences in the prefix list. For more information, see Adding Multiple Sequences to the Prefix List.
8. Select the action **Deny** or **Permit** based on whether you want to deny or allow the route in the BGP network for redistribution.
9. Select the match criteria **Any** or **Custom** to apply the prefix rule.
    a. Option **Any** filters the route without any network parameters defined.
    b. The Custom option applies prefix rules based on the network length and parameters LE and GE. If the parameter is LE, the prefix rules are only applied to routes whose subnets are equal to or smaller than the specified value. If the parameter is GE, the prefix rules are only applied to routes whose subnets are equal to or larger than the specified value.
10. Click **Save**.

CLI Configuration Example

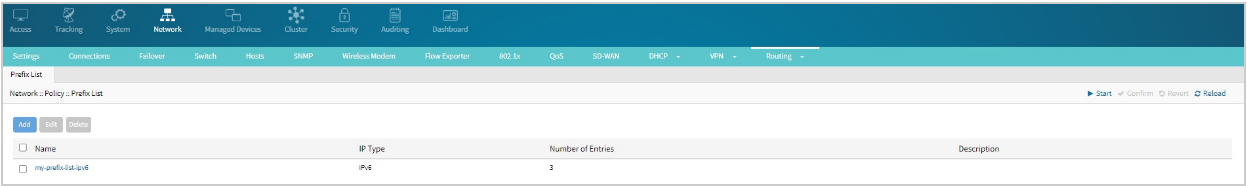
ActionScript Copy

```
[admin@nodegrid /]# cd settings/routing/policy/prefix_list/
[admin@nodegrid prefix_list]# add
[admin@nodegrid {prefix_list}]# set name=test-ipv4
[admin@nodegrid {prefix_list}]# set ip_type=ipv4
[admin@nodegrid {prefix_list}]# set description=docu-testing
[admin@nodegrid {prefix_list}]# set sequence=5
[admin@nodegrid {prefix_list}]# set action=permit
[admin@nodegrid {prefix_list}]# set match=custom network|length=10.0.0.0/24 le=30 ge=28
[admin@nodegrid {prefix_list}]# commit
```

Adding Multiple Sequences to the Prefix List

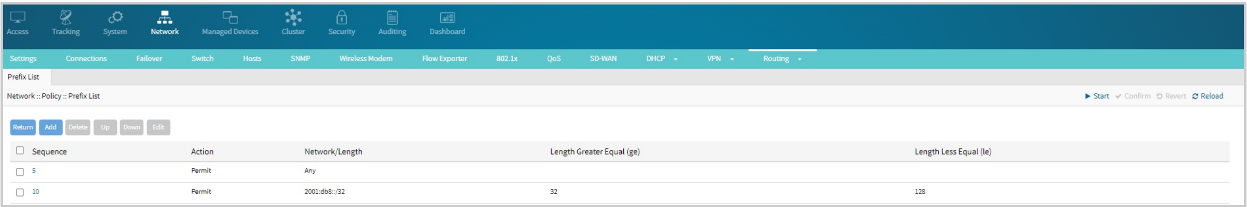
Follow this procedure to include multiple sequences.

1. Navigate to *Network::Routing::Policy.*



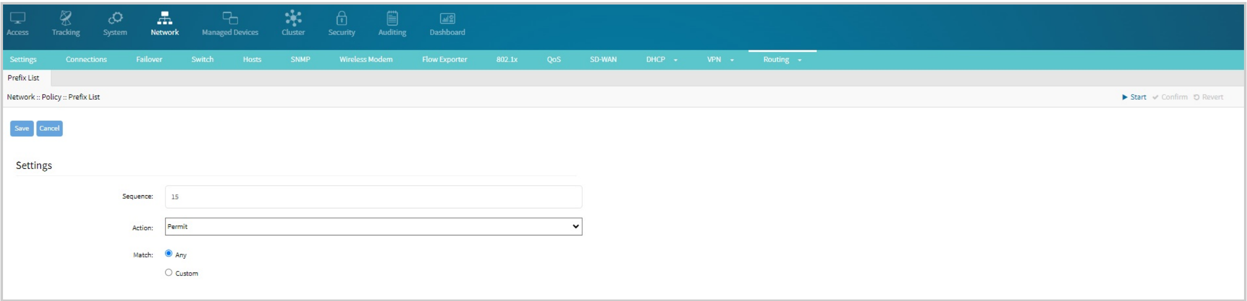
Name	IP Type	Number of Entries	Description
my-prefix-list-ipv6	IPv6	3	

2. Click on the configured prefix list in the table.



Sequence	Action	Network/Length	Length Greater Equal (ge)	Length Less Equal (le)
5	Permit	Any		
10	Permit	2001:db8::/32	32	128

3. Click **Add**.



Settings

Sequence: 15

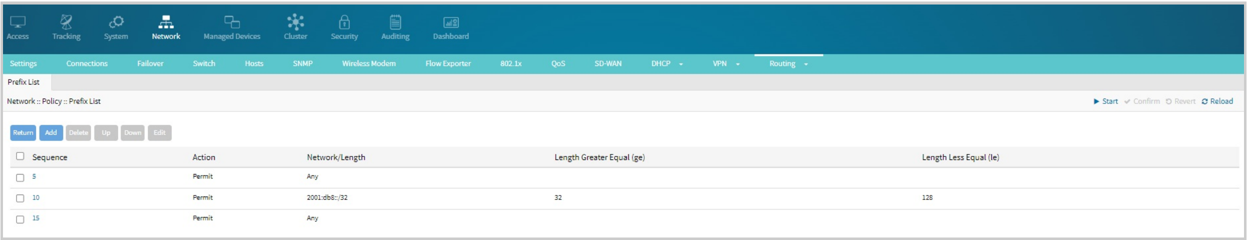
Action: Permit

Match: ● Any ○ Custom

4. Specify the new sequence number to be included in the list and specify Action and Match criteria to be applied to the prefix rule.

5. Click **Save**.

The newly created sequence is included in the prefix list.



Network :: Policy :: Prefix List

□ Sequence	Action	Network/Length	Length Greater Equal (ge)	Length Less Equal (le)
□ 5	Permit	Any		
□ 10	Permit	2001:db8::/32	32	128
□ 15	Permit	Any		

CLI Configuration Example

ActionScript Copy

```
[admin@nodegrid /]# cd /settings/routing/policy/prefix_list/
[admin@nodegrid prefix_list]# cd my-prefix-list-ipv6-ipv6/
[admin@nodegrid my-prefix-list-ipv6-ipv6]# ls
settings/
sequence/
[admin@nodegrid my-prefix-list-ipv6-ipv6]# cd sequence
[admin@nodegrid sequence]# add
[admin@nodegrid {sequence}]# set sequence=15
[admin@nodegrid {sequence}]# set action=permit
[admin@nodegrid {sequence}]# set match=any
[admin@nodegrid {sequence}]# commit
[admin@nodegrid sequence]# show
  sequence  action  network/length  ge  le
  ========  ======  ==============  ==  ===
  5         Permit  Any
  10        Permit  2001:db8::/32   32  128
  15        Permit  Any
```

Configuring BGP Routing for a Nodegrid Device

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol that exchanges routing information between different autonomous systems (ASes) on the Internet. This section explains the tasks to configure a BGP network for a Nodegrid device. To Configure BGP routing for a Nodegrid device, perform the following configurations:

1. Adding a BGP Router
2. Configuring the Neighbors
3. Setting up Neighbor Groups
4. Configuring the Network Settings
5. Configuring the Route Redistribution

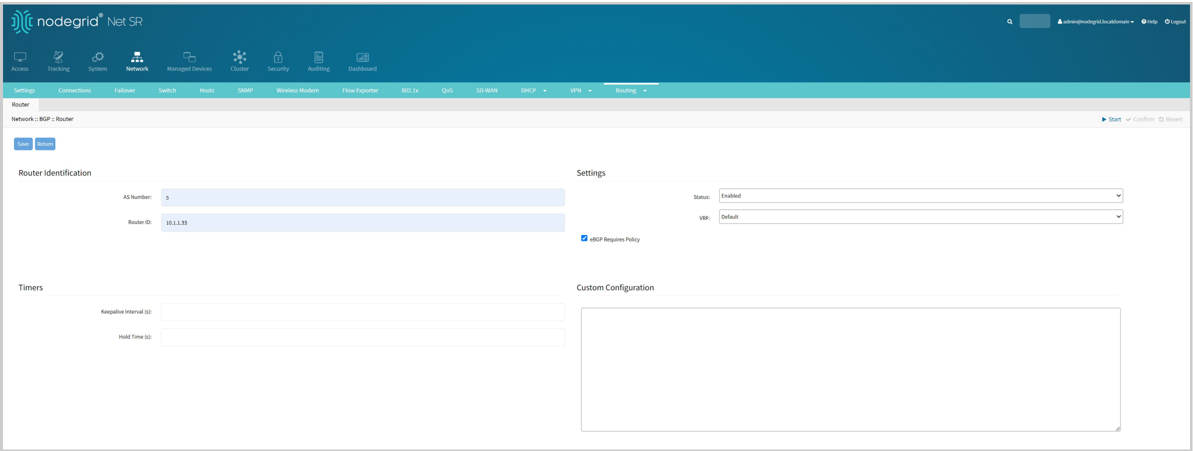
Prerequisite

Before configuring the BGP router, make sure that the IPv4 and IPv6 forwarding are enabled. To enable IPv4 and IPv6 forwarding, go to *Network:: Settings:: IPv4 and IPv6 profile* and select the checkboxes **Enable IPv4 IP Forward** and **Enable IPv6 IP Forward**.

Adding a BGP Router

To initiate the BGP routing process, you must add a BGP router. To configure the BGP router:

1. Log in to the Nodegrid OS Manager.
2. Go to *Network:: Routing:: BGP* and click **Add**.



Network :: BGP :: Router

Router Identification

AS Number: 5

Router ID: 10.1.1.33

Settings

Status: Enabled

VRF: Default

☑ eBGP Requires Policy

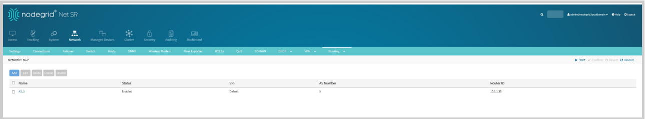
Timers

Keepalive Interval (s):

Hold Time (s):

Custom Configuration

3. Enter the AS number corresponding to the router's autonomous system.
4. Enter the **BGP Router ID**. The router ID should be a unique 32-bit IPv4 address. This ID uniquely identifies the router within the BGP domain and helps to identify the BGP neighbors.
5. Specify the time duration of the Keepalive interval and hold time for BGP neighbors.
   The minimum Keepalive interval is 0 to 65535 seconds. The hold time interval is 0 to `65535` seconds.
6. Select the Status as **Enabled**.
7. Select virtual routing and forwarding (VRF) as Default.
8. Select **eBGP Requires Policy** if you want to apply incoming and outgoing policies to the eBGP sessions. Without incoming policies, no routes will be accepted and without outgoing policies, no routes will be advertised. This option is enabled by default.
9. Click **Save**. The newly created router is listed in the table.
   The BGP router is now configured, and you will be able to see options to configure neighbor groups, neighbors, networks, and redistribution.



Network :: BGP

Name	Status	VRF	AS Number	Router ID
AS_5	Enabled	Default	5	10.1.1.33

CLI Configuration Example

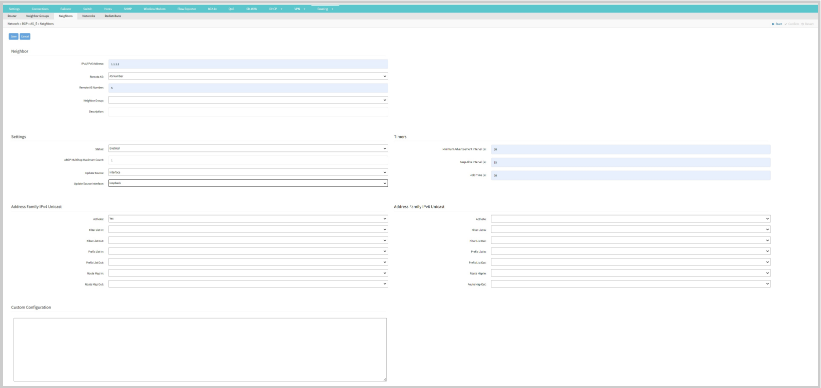
ActionScript Copy

```
[admin@nodegrid /]# cd /settings/routing/bgp
[admin@nodegrid bgp]# add
[admin@nodegrid {bgp}]# set as_number=1
[admin@nodegrid {bgp}]# set router_id=20.1.1.33
[admin@nodegrid {bgp}]# commit
```

Configuring the Neighbors

BGP routers establish TCP sessions with neighboring routers to exchange routing information. The BGP neighbors play a crucial role in maintaining accurate routing within autonomous systems, ensuring proper connectivity. To establish a connection between the BGP neighbors, you must configure the parameters as mentioned in the following procedure:

1. Click on the router entry from the table and click **Neighbor**.
2. Click **Add** to configure a new BGP neighbor.



Network :: BGP :: AS_5 :: Neighbors

Neighbor

IPv4/IPv6 Address: 1.1.1.1
Remote AS: AS Number
Remote AS Number: 5
Neighbor Group:
Description:

Settings

Status: Enabled
eBGP Multihop Maximum Count: 1
Update Source: Interface
Update Source Interface: loopback

Timers

Minimum Advertisement Interval (s): 30
Keep Alive Interval (s): 15
Hold Time (s): 30

Address Family IPv4 Unicast

Activate: Yes
Filter List In:
Filter List Out:
Prefix List In:
Prefix List Out:
Route Map In:
Route Map Out:

Address Family IPv6 Unicast

Activate:
Filter List In:
Filter List Out:
Prefix List In:
Prefix List Out:
Route Map In:
Route Map Out:

Custom Configuration

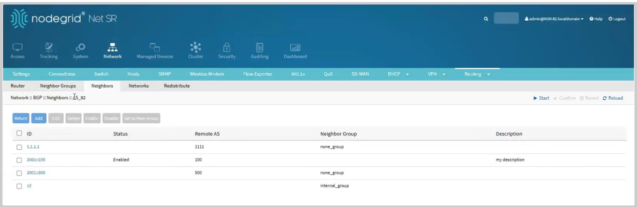
3. Configure the following neighbor parameters:
   a. Specify the **IP address** of the neighbor.
   b. Select the **Autonomous System number** of the neighboring BGP router with which you are establishing a BGP neighbor session.
      i. Select the AS number if you want to assign a numerical identifier to the autonomous system of the neighboring BGP router.
      ii. Select **External** if the neighbor with which you are establishing the connection is an external BGP router. When you have selected this option and if the AS number is identified in the local autonomous system the connection gets rejected.
      iii. Select **Internal** if the neighbor with which you are establishing the connection is an internal BGP router. When you have selected this option and if the AS number is identified in the local autonomous system the connection gets accepted.

   c. Select the neighbor group from which you want to replicate the configuration policies for this specific neighbor.
   d. Specify a meaningful **description** of the neighbor. This description assists network administrators in understanding the neighbor's role in a network topology.

4. Configure the following settings:
   a. Select if the BGP session with the specified neighbor is enabled or disabled.
   b. Specify the **maximum hop count** to establish BGP sessions with the neighbors that are not directly connected. Note that the more the hop count the lesser the network latency.
   c. Specify the **source address** of the interface or the interface type to reach the neighbor. A BGP connection can be established if there are active paths between the neighbors. If there are multiple paths between the neighbors specifying the update source initiates the Nodegrid device to establish the BGP peering itself through that interface or the source IP.

5. Configure the following timer settings:
   a. Specify the minimum router advertisement interval (per neighbor). BGP determines the interval determines the time gap between sending route advertisements or withdrawals to a BGP neighbor. The duration can be a maximum of 30 seconds.
   b. Specify the time duration between consecutive Keepalive messages sent by the BGP router to its neighbors. The duration can be from 10 to 60 seconds; however, it must not exceed half of the time set as the Hold time.
   c. Specify the maximum time duration that a BGP router should wait to receive a Keepalive message from its neighbor. The duration can be from 30 to 90 seconds.

6. Configure the IPv4/IPv6 address families.
   Specify which address families should be exchanged with neighbors that support the same address families. You could activate an address family to select that address family for a BGP neighbor. If you are defining an IPv4/IPv6 unicast neighbor, you exchange the IPv4/IPv6 unicast routes with that neighbor. Additionally, you can set up filter lists, prefix lists, and route maps, to specify which routes should be accepted from or advertised to specific neighbors.
7. A list of available neighbors is displayed in a tabular format. The table shows the following details:
   - ID: Neighbor ID, which is IPv4 or IPv6 address of the router.
   - Status: Enabled or Disabled status of the neighbor.
   - Remote AS: AS system number of the neighbor.
   - Neighbor Group: The Group to which the neighbor belongs. See the Neighbor Groups section for more information. The configurations defined in the Neighbor Groups are inherited by all the neighbors of the group. This is useful if you have the same configuration for multiple neighbors.



Network :: BGP :: Neighbors :: AS_82

ID	Status	Remote AS	Neighbor Group	Description
1.1.1.1		1111	none_group	
2001::100	Enabled	100		my description
2001::500		500	none_group	
::2			internal_group	

You can set a neighbor as a peer group by clicking the **Set as Peer Group** option. Setting a neighbor as a peer group includes it in the Neighbor Groups as peers share the same update policies.

CLI Configuration Example

ActionScript Copy

```
[admin@nodegrid routing]# cd bgp
[admin@nodegrid bgp]# cd 1-default/
[admin@nodegrid 1-default]# cd neighbor
[admin@nodegrid 1-default]# add
[admin@nodegrid {neighbors}]# set ip_address=10.1.1.33
[admin@nodegrid 10.1.1.33]# set remote_as=as_number
[admin@nodegrid 10.1.1.33 ]# set remote_as_number=10
[admin@nodegrid 10.1.1.33 ]# set description=testing
[admin@nodegrid 10.1.1.33 ]# set status=enabled
[admin@nodegrid 10.1.1.33 ]# set ebgp_multihop_maximum_count=10
[admin@nodegrid 10.1.1.33 ]# set update_source=interface
[admin@nodegrid 10.1.1.33 ]# set update_source_interface=backplane0
[admin@nodegrid 10.1.1.33 ]# set minimum_advertisement_interval=30
[admin@nodegrid 10.1.1.33 ]# set keep_alive_interval=60 hold_time=100
[admin@nodegrid 10.1.1.33]# set ipv4_unicast_activate=yes
[admin@nodegrid 10.1.1.33]# commit
```

Setting up the Neighbor Groups

You can set up neighbor groups with the same set of configurations to simplify and effectively update the configurations. This approach simplifies the configurations in cases where there are many neighbors.

1. Click on the router entry from the table and click **Neighbor Groups**.
2. Click **Add**.
3. Specify a neighbor group name.
4. Under Group Members, choose the member you want to include in the group and click **Add**. To remove a member from the group, select the member and click **Remove**.
5. Configure the necessary parameters that you want to apply to all members of the group. Refer to the procedure *Configuring the Neighbors* for information on configuration parameters.
6. Click **Save**.

> **Note:**
> After you include a member in a group, you can also override the configuration settings for that member by navigating to the Neighbors tab.

CLI Configuration Example

ActionScript Copy

```
[admin@BSR-80 /]# cd /settings/routing/bgp/1-default/neighbor_groups/
[admin@BSR-80 neighbor_groups]# add
[admin@BSR-80 {neighbor_groups}]# set name=my_group
[admin@BSR-80 {neighbor_groups}]# set remote_as_number=10
[admin@BSR-80 {neighbor_groups}]# set description="My group description"
[admin@BSR-80 {neighbor_groups}]# set members=10.1.1.33
[admin@BSR-80 {neighbor_groups}]# set status=enabled
[admin@BSR-80 {neighbor_groups}]# set ebgp_multihop_maximum_count=5
[admin@BSR-80 {neighbor_groups}]# set update_source=interface
[admin@BSR-80 {neighbor_groups}]# set update_source_interface=backplane0
[admin@BSR-80 {neighbor_groups}]# set keep_alive_interval=30
[admin@BSR-80 {neighbor_groups}]# set hold_time=90
[admin@BSR-80 {neighbor_groups}]# set ipv4_unicast_activate=yes
[admin@BSR-80 {neighbor_groups}]# commit
```

Configuring BGP Network Parameters

You need to specify the IPv4 or IPv6 routes that need to be advertised by the BGP routers to ensure routing information propagates via the network. To configure the network settings, follow these steps:

1. Enter the IP prefix of the device. The IP prefix allows the advertising of the device to its neighbors.
2. Select the IPv4 unicast or IPv6 unicast address family from the drop-down.
3. Select the **route map** for the inbound or the outbound routes. Route maps can be used to set the filters for the routes or to redistribute routes to avoid loops when the same routes are advertised.
4. (optional) Enter the **label index** number identifier for the route.
5. Select the checkbox **Backdoor Route** to route a network through the backdoor route. Applicable for IPv4 Unicast address type only. The backdoor route and the local route are the same except that the backdoor route IPs are not advertised.
6. Click **Save.**

CLI Configuration Example

ActionScript Copy

```
[admin@nodegrid {networks}]# cd /settings/routing/bgp/80-default/networks/
[admin@nodegrid networks]# add
[admin@nodegrid {networks}]# set ip_prefix=10.1.1.32
[admin@nodegrid {networks}]# set address_family=ipv4_unicast
[admin@nodegrid {networks}]# set label_index=100
[admin@nodegrid {networks}]# set backdoor_route=yes
[admin@nodegrid {networks}]# commit
```

Configuring Route Redistribution

BGP routes can advertise routes to the neighbors that are learned by other routing protocols. Follow these steps to set the redistribution parameters:

1. Select the **routing protocol** to be used during the route redistribution.
2. Select the IPv4 unicast or IPv6 unicast address family from the drop-down.
3. Select the **route map** for the inbound or the outbound routes. Route maps can be used to set the filters for the routes or to redistribute routes to avoid loops when the same routes are advertised.
4. Enter the **metric** attribute based on which the shortest path is selected for the routing purpose.
5. Click **Save**.

CLI Configuration Example

ActionScript Copy

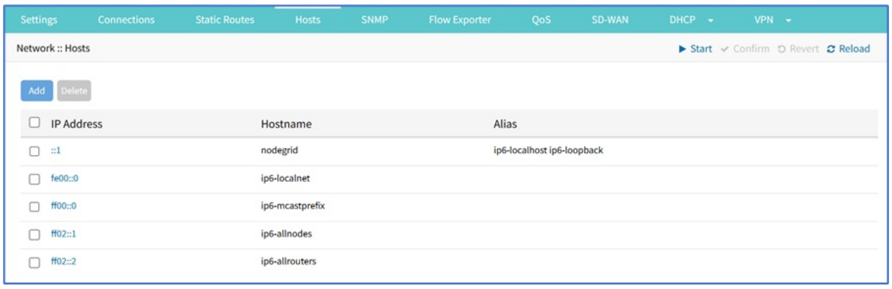
```
[admin@nodegrid /]# cd settings/routing/bgp/1-default/redistribute/
[admin@nodegrid redistribute]# add
[admin@nodegrid {redistribute}]# set protocol=ospf
[admin@nodegrid {redistribute}]# set address_family=ipv4_unicast
[admin@nodegrid {redistribute}]# set metric=10
[admin@nodegrid {redistribute}]# commit
```

Managing Route Configuration

You can edit, delete, enable, or disable BGP route configurations by choosing the corresponding configuration entry and selecting the appropriate options.

Hosts tab

Administrators can configure and manage manual hostname definitions (equivalent to entries in the host's file).

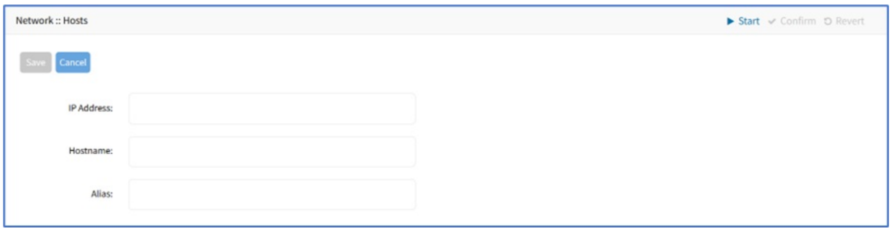


□	IP Address	Hostname	Alias
□	::1	nodegrid	ip6-localhost ip6-loopback
□	fe00::0	ip6-localnet	
□	ff00::0	ip6-mcastprefix	
□	ff02::1	ip6-allnodes	
□	ff02::2	ip6-allrouters	

Manage Hosts

Add Host

1. Go to *Network :: Hosts*.
2. Click **Add** (displays dialog).



   a. Enter **IP Address** (IPv4, IPv6 formats supported)
   b. Enter **Hostname**
   c. Enter **Alias**

3. Click **Save**.

Edit Host

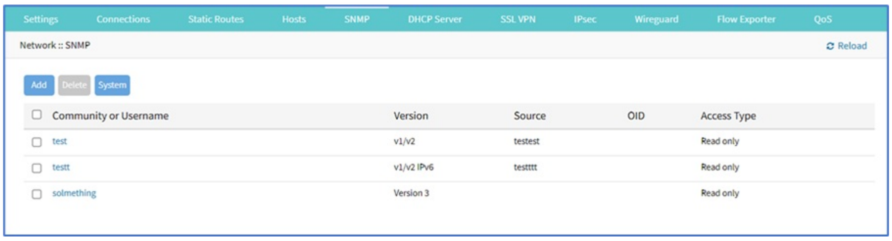
1. Go to *Network :: Hosts*.
2. In the *Index* column, click on the name (displays dialog).
3. Make changes as needed.
4. Click **Save**.

Delete Host

1. Go to *Network :: Hosts*.
2. In the list, select a checkbox.
3. Click **Delete**.

SNMP tab

Administrators can configure SNMP settings here.

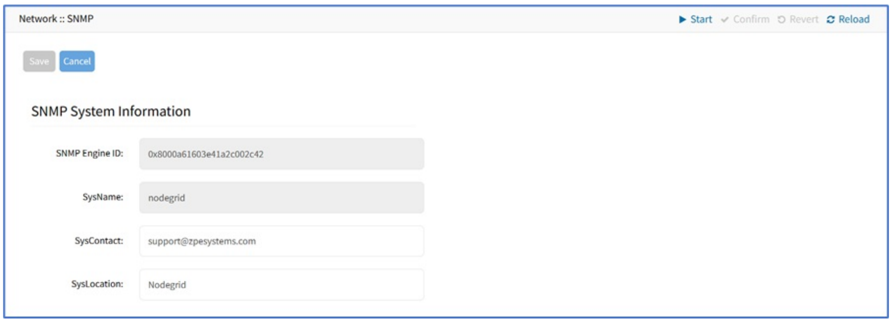


□ Community or Username	Version	Source	OID	Access Type
□ test	v1/v2	testest		Read only
□ testt	v1/v2 IPv6	testttt		Read only
□ solmething	Version 3			Read only

Manage SNMP

Review/edit System Information

1. Go to *Network :: SNMP*.
2. Click **System** (displays dialog).



SNMP System Information

SNMP Engine ID: 0x8000a61603e41a2c002c42

SysName: nodegrid

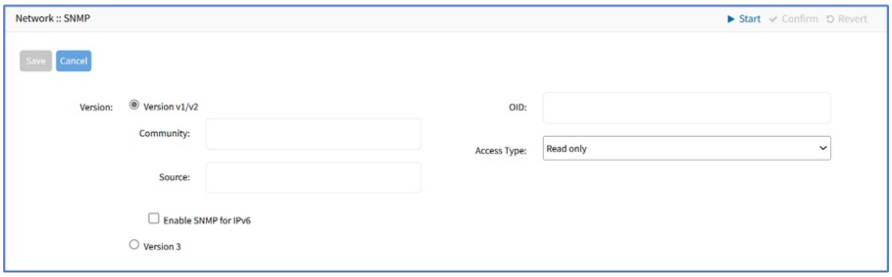
SysContact: support@zpesystems.com

SysLocation: Nodegrid

3. Two fields can be edited:
   a. **SysContact** (email address)
   b. **SysLocation** (location name)
4. If changed, click **Save**.
5. If not, click **Cancel** to return to table.

Add SNMP Community/Username Configuration

1. Go to *Network :: SNMP*.
2. Click **Add** (displays dialog).



Version: ● Version v1/v2

Community:

Source:

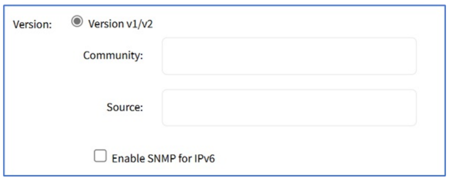
□ Enable SNMP for IPv6

○ Version 3

OID:

Access Type: Read only

3. In the *Version* menu (select one):
   - **Version V1/V2** radio button (expands dialog). Enter **Community** and **Source**. (if applicable) **Enable SNMP for IPv6** checkbox.



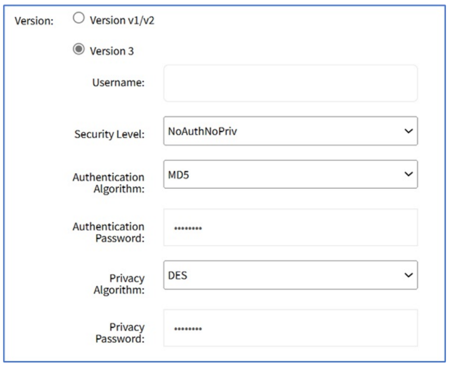
Version: ● Version v1/v2

Community:

Source:

□ Enable SNMP for IPv6

   - **Version 3** radio button (expands dialog):



Version: ○ Version v1/v2

● Version 3

Username:

Security Level: NoAuthNoPriv

Authentication Algorithm: MD5

Authentication Password: ••••••••

Privacy Algorithm: DES

Privacy Password: ••••••••

Enter **Username**.
On **Security** Level drop-down, select one (NoAuthNoPriv, AuthNoPriv, AuthPriv).
On **Authentication Algorithm** drop-down, select one (MD5, SHA, SHA-224, SHA-256, SHA-384, SHA-512).
Enter **Authentication Password**.
On **Privacy Algorithm** drop-down, select one (DES, AES, AES-192, AES-256).
Enter **Privacy Password**

4. On *OID* menu:
   a. OIDs and Descriptions are:
      - ngCellularConnections (OID: .1.3.6.1.4.1.42518.4.2.1.1.7)
        DESCRIPTION: This is the root for cellular connections.
      - ngCellularNumOfConnections (OID: .1.3.6.1.4.1.42518.4.2.1.1.7.1.0)
        DESCRIPTION: This object contains number of Cellular Connections. This identifies the number of Cellular Connections.
      - ngCellularConnectionsTable (OID: .1.3.6.1.4.1.42518.4.2.1.1.7.2)
        DESCRIPTION: This table has information about Cellular Connections in this unit.

- ngCellularConnectionsEntry (OID: .1.3.6.1.4.1.42518.4.2.1.1.7.2.1)
  DESCRIPTION: An entry for each Cellular Connection plugged in this unit. Each entry contains information on connection status, slot, SIM, data consumption and signal strength.
- ngCellularConnectionNumber (OID: .1.3.6.1.4.1.42518.4.2.1.1.7.2.1.1)
  DESCRIPTION: This object unique identifies Cellular Connection Index.
- ngCellularConnectionSlot (OID: .1.3.6.1.4.1.42518.4.2.1.1.7.2.1.2)
  DESCRIPTION: Slot of the Cellular Connection.
- ngCellularConnectionInterface (OID: .1.3.6.1.4.1.42518.4.2.1.1.7.2.1.3)
  DESCRIPTION: Interface of the Cellular Connection.
  ngCellularConnectionStatus (OID: .1.3.6.1.4.1.42518.4.2.1.1.7.2.1.4)
  DESCRIPTION: Status of the Cellular Connection.
- ngCellularConnectionSIMState (OID: .1.3.6.1.4.1.42518.4.2.1.1.7.2.1.5)
  DESCRIPTION: State of the SIM Card of the Cellular Connection.
- ngCellularConnectionSIMActive (OID: .1.3.6.1.4.1.42518.4.2.1.1.7.2.1.6)
  DESCRIPTION: Number of the Active SIM Card of the Cellular Connection.
- ngCellularConnectionDataConsumption (OID: .1.3.6.1.4.1.42518.4.2.1.1.7.2.1.7)
  DESCRIPTION: Data Consumption in kBytes of the Cellular Connection.
- ngCellularConnectionOperator (OID: .1.3.6.1.4.1.42518.4.2.1.1.7.2.1.8)
  DESCRIPTION: Operator of the Cellular Connection.
- ngCellularConnectionRadioMode (OID: .1.3.6.1.4.1.42518.4.2.1.1.7.2.1.9)
  DESCRIPTION: Radio Mode of the Cellular Connection.
- ngCellularConnectionSignalStrength (OID: .1.3.6.1.4.1.42518.4.2.1.1.7.2.1.10)
  DESCRIPTION: Signal Strength of the Cellular Connection in percent.
- ngCellularConnectionTemperature (OID: .1.3.6.1.4.1.42518.4.2.1.1.7.2.1.11)
  DESCRIPTION: Temperature of the Cellular Connection device.

b. On **Access Type** drop-down, select one (Read and Write, Read Only)

5. Click **Save**.

Edit Community/Username

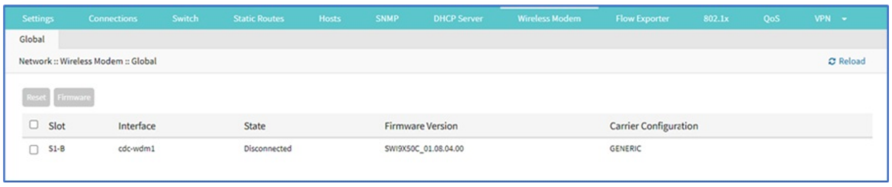
1. Go to *Network :: SNMP*.
2. On *Community or Username* column, click a name (displays dialog).
3. Make changes, as needed.
4. Click **Save**.

Delete Community/Username

1. Go to *Network :: SNMP*.
2. Select checkbox to be deleted.
3. Click **Delete**.

Wireless Modem tab

This provides details on the Wireless Modem (if installed).



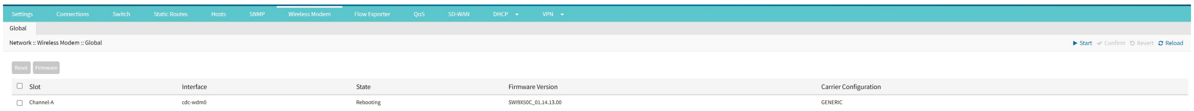
Network :: Wireless Modem :: Global

□	Slot	Interface	State	Firmware Version	Carrier Configurztion
□	S1-B	cdc-wdm1	Disconnected	SWI9X50C_01.08.04.00	GENERIC

Manage Wireless Modem

Reset Wireless Modem

1. Go to *Network :: Wireless Modem*.
2. Select the checkbox next to the *Slot* name.
3. Click **Reset**. The state of the modem changes to Rebooting.



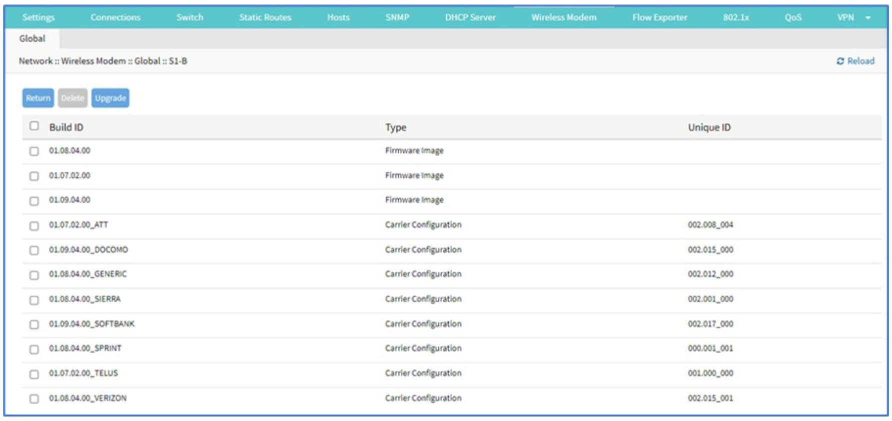
Network :: Wireless Modem :: Global

□ Slot	Interface	State	Firmware Version	Carrier Configuration
□ Channel-A	cdc-wdm0	Rebooting	SWI9X50C_01.14.13.00	GENERIC

Note: When a reset, power cycle, or sim swap operation is called, the Status of the cellular modem is changed to **rebooting**.

Upgrade Wireless Modem Firmware

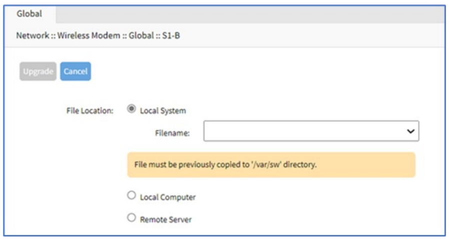
1. Go to *Network :: Wireless Modem*.
2. Select the checkbox next to the *Slot* name.
3. Click **Firmware** (displays dialog).



Network :: Wireless Modem :: Global :: S1-B

□ Build ID	Type	Unique ID
□ 01.08.04.00	Firmware Image	
□ 01.07.02.00	Firmware Image	
□ 01.09.04.00	Firmware Image	
□ 01.07.02.00_ATT	Carrier Configuration	002.008_004
□ 01.09.04.00_DOCOMO	Carrier Configuration	002.015_000
□ 01.08.04.00_GENERIC	Carrier Configuration	002.012_000
□ 01.08.04.00_SIERRA	Carrier Configuration	002.001_000
□ 01.09.04.00_SOFTBANK	Carrier Configuration	002.017_000
□ 01.08.04.00_SPRINT	Carrier Configuration	000.001_001
□ 01.07.02.00_TELUS	Carrier Configuration	001.000_000
□ 01.08.04.00_VERIZON	Carrier Configuration	002.015_001

4. Click **Upgrade**.



Network :: Wireless Modem :: Global :: S1-B

File Location: ● Local System

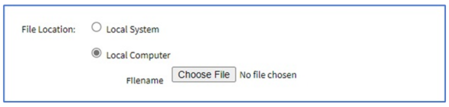
Filename:

File must be previously copied to '/var/sw' directory.

○ Local Computer

○ Remote Server

5. In the *File Location* menu, select one:
   - **Local Computer** radio button (expands dialog). Click **Choose File**. Locate and select the file.

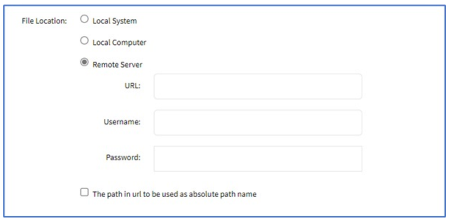


File Location: ○ Local System

● Local Computer

Filename Choose File No file chosen

   - **Remote Server** radio button (expands dialog).



File Location: ○ Local System

○ Local Computer

● Remote Server

URL:

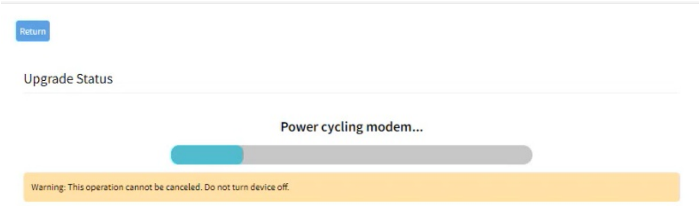
Username:

Password:

□ The path in url to be used as absolute path name

     - Enter **URL** (URL can be the IP address or hostname/FQDN. If using IPv6, use brackets [...]. Supported protocols: FTP, TFTP, SFTP, and SCP.)
     - Enter **Username** and **Password**.
     - (optional) Select **The path in the URL to be used as the absolute path name** checkbox.

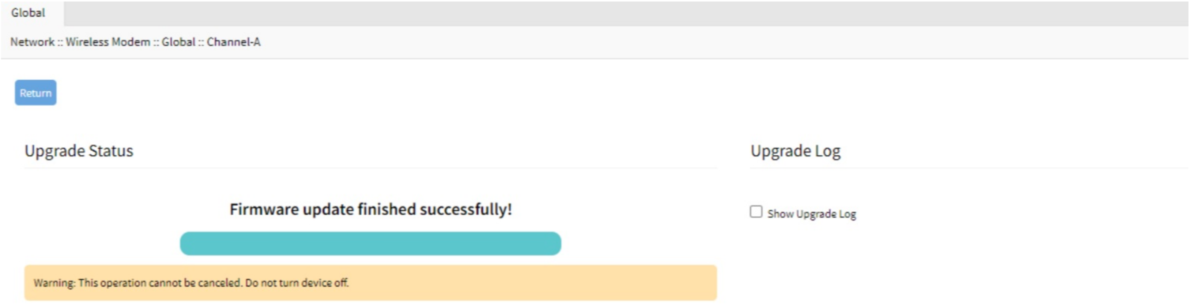
6. Click **Upgrade**.
   In the **Upgrade Status** user can view the track progress of the upgrade.



Power cycling modem...

Warning: This operation cannot be canceled. Do not turn device off.

When the upgrade completes the system displays that the firmware update is complete as shown in the following image:



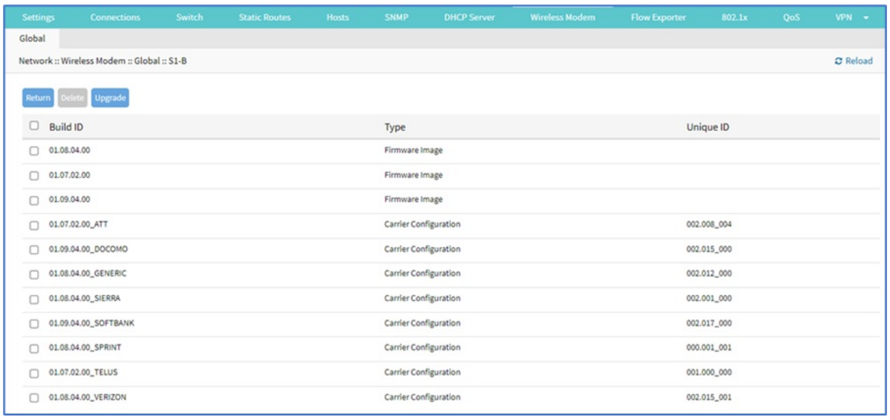
Firmware update finished successfully!

Warning: This operation cannot be canceled. Do not turn device off.

7. You can check the **Show upgrade log** field to view the detailed log information related to the upgrade. When a firmware upgrade is in progress the system doesn't allow another upgrade on the same modem.

Delete Wireless Modem Build Version

1. Go to *Network :: Wireless Modem*.
2. Select the checkbox next to the *Slot* name.
3. Click **Firmware** (displays dialog).

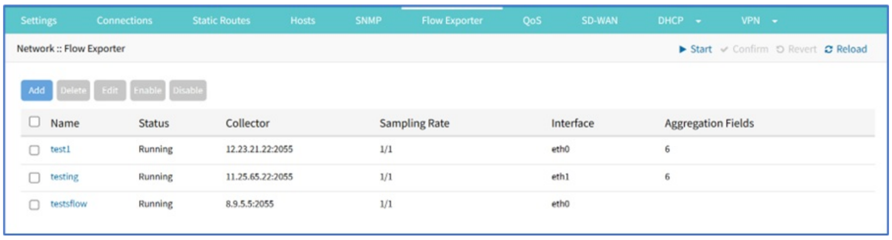


□ Build ID	Type	Unique ID
□ 01.08.04.00	Firmware Image	
□ 01.07.02.00	Firmware Image	
□ 01.09.04.00	Firmware Image	
□ 01.07.02.00_ATT	Carrier Configuration	002.008_004
□ 01.09.04.00_DOCOMO	Carrier Configuration	002.015_000
□ 01.08.04.00_GENERIC	Carrier Configuration	002.012_000
□ 01.08.04.00_SIERRA	Carrier Configuration	002.001_000
□ 01.09.04.00_SOFTBANK	Carrier Configuration	002.017_000
□ 01.08.04.00_SPRINT	Carrier Configuration	000.001_001
□ 01.07.02.00_TELUS	Carrier Configuration	001.000_000
□ 01.08.04.00_VERIZON	Carrier Configuration	002.015_001

4. To delete the version, select the checkbox next to *Build ID*.
5. Click **Delete**.

Flow Exporter tab

Netflow streaming telemetry data is supported for all network interfaces, including the switch interface.



Network :: Flow Exporter

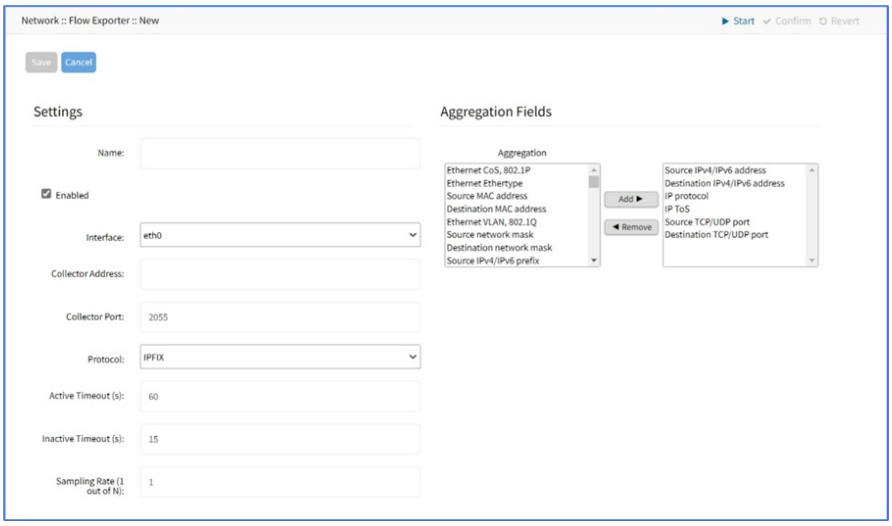
☐	Name	Status	Collector	Sampling Rate	Interface	Aggregation Fields
☐	test1	Running	12.23.21.22:2055	1/1	eth0	6
☐	testing	Running	11.25.65.22:2055	1/1	eth1	6
☐	testsflow	Running	8.9.5.5:2055	1/1	eth0	

Manage Flow Export

Add a new Flow Export

WebUI Procedure

1. Go to *Network :: Flow Exporter*.
2. Click **Add** (displays dialog).



Name:

☑ Enabled

Interface: eth0

Collector Address:

Collector Port: 2055

Protocol: IPFIX

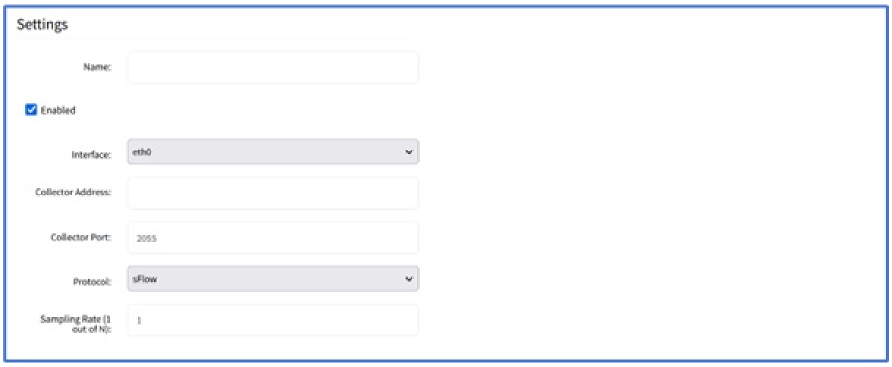
Active Timeout (s): 60

Inactive Timeout (s): 15

Sampling Rate (1 out of N): 1

3. In *Settings* menu, enter details:
   a. **Name**
   b. **Enabled** checkbox
   c. **Interface** drop-down, select one (eth0, eth1)
   d. **Collector Address**
   e. **Collector Port** (default: 2055)
4. On **Protocol** drop-down, select one (IPFIX, NetFlow v9, NetFlow v5, sFlow). (available in v5.8+)
   a. **IPFIX**, **NetFlow v9**, **NetFlow v5**, enter details:
      - **Active Timeouts (s)** (default: 60)
      - **Inactive Timeout (s)** (default: 15)
      - **Sampling Rate (1 out of N)** (default: 1)
      - In *Aggregation Fields* menu: to add an item, select item on left-side panel. Click **Add►** (item is moved). To remove an item, select item on right-side panel. Click **◄Remove** (item is moved).

   b. **sFlow** (expands dialog): (available in v5.8+) Enter details.



Name:

☑ Enabled

Interface: eth0

Collector Address:

Collector Port: 2055

Protocol: sFlow

Sampling Rate (1 out of N): 1

      - **Enabled** checkbox
      - **Collector Address**
      - **Collector Port**
      - **Sampling Rate (1 out of N)** (default: 1)

> **NOTE**
>
> The sFlow can also be viewed on *Tracking :: Network :: Flow Exporter*. (available in v5.8+)

5. Click **Save**.

Edit Flow Export

1. Go to *Network :: Flow Exporter*.
2. Select checkbox to be edited (displays dialog).
3. Make changes, as needed.
4. Click **Save**.

Delete Flow Export

1. Go to *Network :: Flow Exporter*.
2. Select checkbox to be deleted.
3. Click **Delete**.

Enable Flow Export

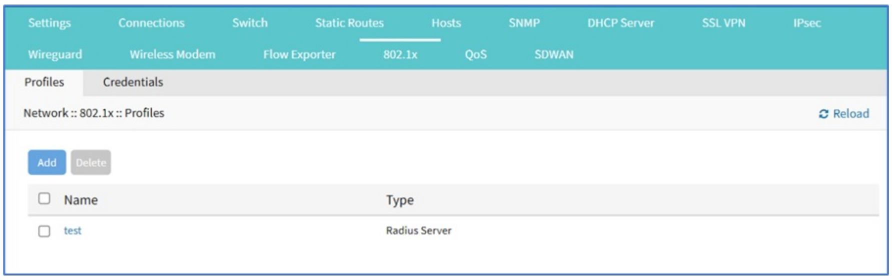
1. Go to *Network :: Flow Exporter*.
2. Select checkbox to be enabled.
3. Click **Enable**.

Disable Flow Export

1. Go to *Network :: Flow Exporter*.
2. Select checkbox to be disabled.
3. Click **Disable**.

802.1x tab (Net SR only)

These functions are only available on Nodegrid Net SR device.

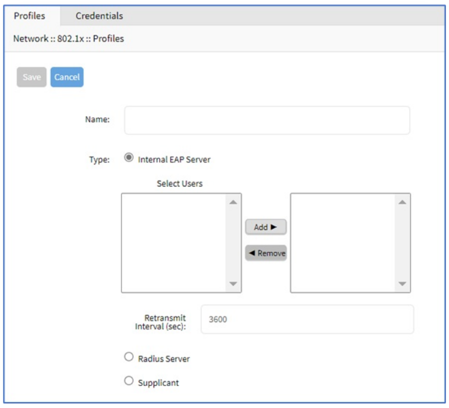


□ Name	Type
□ test	Radius Server

Profiles sub-tab

Add Profile

1. Go to *Network :: 802.1x :: Profile*.
2. Click **Add** (displays dialog). Enter **Name**.



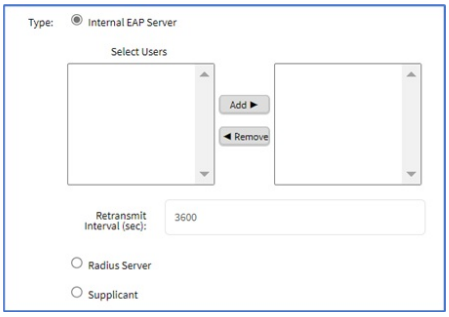
Type: ● Internal EAP Server

Retransmit Interval (sec): 3600

○ Radius Server

○ Supplicant

3. On *Type* menu, select one:
   - On **Internal EAP Server** radio button (expands dialog):



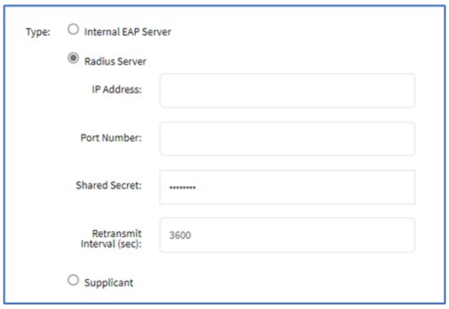
Type: ● Internal EAP Server

Retransmit Interval (sec): 3600

○ Radius Server

○ Supplicant

     - In *Select Users*: To add, select item on left-side panel and click **Add ►** (item is moved). To remove, select item on right-side panel and click **◄Remove** (item is moved).
     - Enter **Retransmit Interval (sec)** (default: 3600).
   - **Radius Server** radio button (expands dialog), enter details:



Type: ○ Internal EAP Server

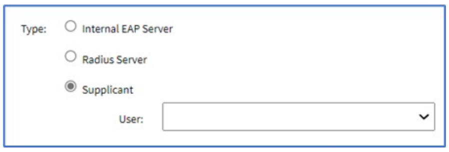
● Radius Server

Shared Secret: ••••••••

Retransmit Interval (sec): 3600

○ Supplicant

     - **IP Address**
     - **Port Number**
     - **Shared Secret**
     - **Retransmit Interval (sec)**
   - **Supplicant** radio button (expands dialog). On **User** drop-down, select one.



Type: ○ Internal EAP Server

○ Radius Server

● Supplicant

4. Click **Save**.

Edit a Profile

1. Go to *Network :: 802.1x :: Profile*.
2. In the *Name* column, click on a name (opens dialog).
3. Make changes, as needed.
4. Click **Save**.

Delete an Interface

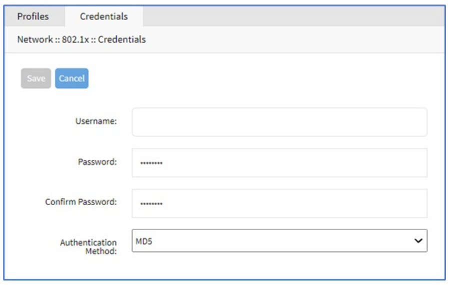
1. Go to *Network :: 802.1x :: Profile*.
2. Select checkbox to be deleted.
3. Click **Delete**.

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

Credentials sub-tab

Add Credential

1. Go to *Network :: 802.1x :: Credentials*.
2. Click **Add** (displays dialog).



Username:

Password: ••••••••

Confirm Password: ••••••••

Authentication Method: MD5

3. Enter details:
   a. **Username**
   b. **Password**
   c. **Confirm Password**
   d. **Authentication** drop-down, select one (MD5, TLS, PEAP, TTLS).

4. Click **Save**.

Edit Credential

1. Go to *Network :: 802.1x :: Credentials*.
2. In *Username* column, click on name (opens dialog).
3. Make changes, as needed.
4. Click **Save**.

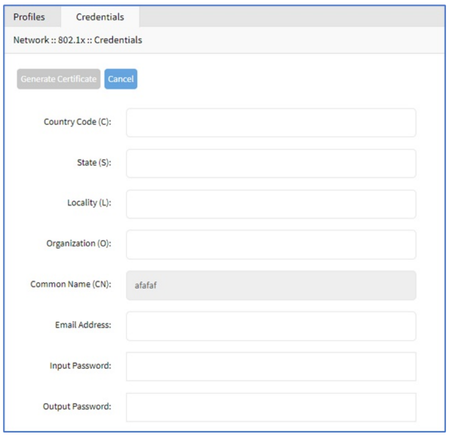
Delete Credential

1. Go to *Network :: 802.1x :: Credentials*.
2. Select checkbox.
3. Click **Delete**.
4. On confirmation dialog, click **OK**.

Include Certificate

User must have TLS authentication.

1. Go to *Network :: 802.1x :: Credentials*.
2. Select checkbox and click **Certificate** (displays dialog).



Country Code (C):

State (S):

Locality (L):

Organization (O):

Common Name (CN): afafaf

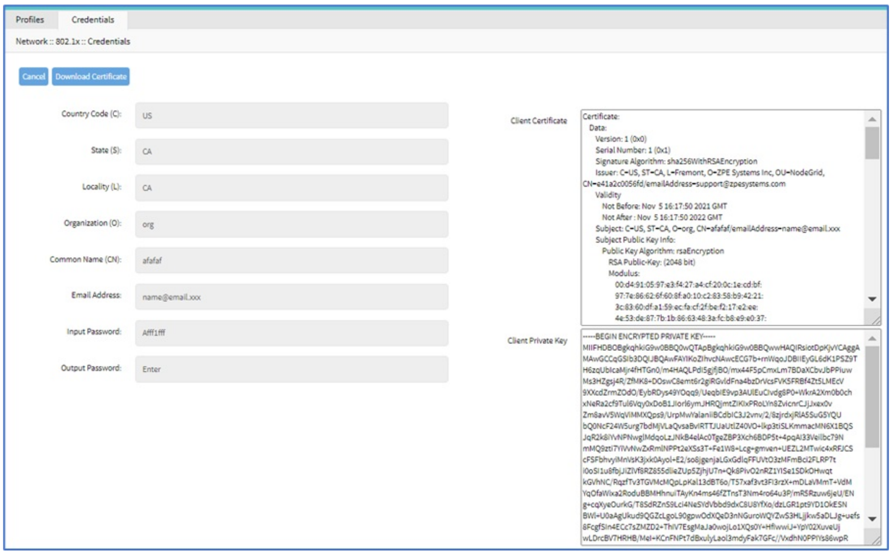
Email Address:

Input Password:

Output Password:

3. Enter details:
   a. **Country Code (C)**
   b. **State (S)**
   c. **Locality (L)**
   d. **Organization (O)**
   e. **Email Address**
   f. **Input Password**
   g. **Output Password**

4. Click **Generate Certificate** (displays dialog).



Country Code (C):	US
State (S):	CA
Locality (L):	CA
Organization (O):	org
Common Name (CN):	afafaf
Email Address:	name@email.xxx
Input Password:	Afff1fff
Output Password:	Enter

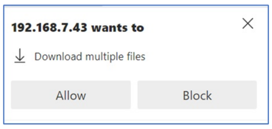
Client Certificate

```
Certificate:
  Data:
    Version: 1 (0x0)
    Serial Number: 1 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, ST=CA, L=Fremont, O=ZPE Systems Inc, OU=NodeGrid,
CN=e41a2c0056fd/emailAddress=support@zpesystems.com
    Validity
      Not Before: Nov  5 16:17:50 2021 GMT
      Not After : Nov  5 16:17:50 2022 GMT
    Subject: C=US, ST=CA, O=org, CN=afafaf/emailAddress=name@email.xxx
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        RSA Public-Key: (2048 bit)
        Modulus:
          00:d4:91:05:97:e3:f4:27:a4:cf:20:0c:1e:cd:bf:
          97:7e:86:62:6f:60:8f:a0:10:c2:83:58:b9:42:21:
          3c:83:60:df:a1:59:ec:fa:cf:2f:be:f2:17:e2:ee:
          4e:53:de:87:7b:1b:86:63:48:3a:fc:b8:e9:e0:37:
```

Client Private Key

-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFHDBOBgkqhkiG9w0BBQ0wQTApBgkqhkiG9w0BBQwwHAQIRsiotDpKjvYCAggA
MAwGCCqGSIb3DQIJBQAwFAYIKoZIhvcNAwcECG7b+rnWqoJDBIIEyGL6dK1PSZ9T
H6zqUbIcaMjr4fHTGn0/m4HAQLPdI5gjfjBO/mx44F5pCmxLm7BDaXCbvJbPPiuw
Ms3HZgsj4R/ZfMK8+DOswC8emt6r2giRGvldFna4bzDrVcsFVKSFRBf4Zt5LMEcV
9XXcdZrmZOdO/EybRDys49YOqq9/UeqbIE9vp3AUlEuClvdg8P0+WkrA2Xm0b0ch
xNeRa2cf9Tul6Vqy0xDoB1JIorl6ymJHRQjmtZIKIxPRoLYn8ZvicnrCJjJxex0v
Zm8avV5WqVIMMXQps9/UrpMwYalanIIBCdbIC3J2vnv/2/8zjrdxjRIA5SuG5YQU
bQ0NcF24W5urg7bdMjVLaQvsaBvIRTTJUaUtlZ40VO+lkp3tiSLKmmacMN6X1BQS
JqR2k8iYvNPNwglMdqoLzJNkB4elAc0TgeZBP3Xch6BDP5t+4pqAI33Veilbc79N
mMQ9zti7YIVvNwZxRmlNPPt2eXSs3T+Fe1W8+Lcg+gmven+UEZL2MTwic4xRFJCS
cFSFbhvyiMnVsK3jxk0Ayol+E2/so8jgenjaLGxGdlqFFUVtO3zMFmBci2FLRP7t
i0oSI1u8fbjJiZlVf8RZ855dlieZUp5ZjhjU7n+Qk8PlvO2nRZ1YISe1SDkOHwqt
kGVhNC/RqzfTv3TGVMcMQpLpKal13dBT6o/T57xaf3vt3FI3rzX+mDLaVMmT+VdM
YqOfaWixa2RoduBBMHhnuiTAyKn4ms46fZTnsT3Nm4ro64u3P/mR5Rzuw6jeU/EN
g+cqXyeOurkG/T8SdRZnS9Lci4NeSYdVbbd9dxC8U8YfXo/dzLGR1pt9YD1OkESN
BWl+U0aAgUkud9QGZcLgoL90gpwOdXQeD3nNGuroWQYZwS3HLjjkw5aDLJg+uefs
8FcgfSIn4ECc7sZMZD2+ThIV7EsgMaJa0wojLo1XQs0Y+HflwwIJ+YpY02XuveUj
wLDrcBV7HRHB/MeI+KCnFNPt7dBxulyLaol3mdyFak7GFc//VxdhN0PPIYs86wpR

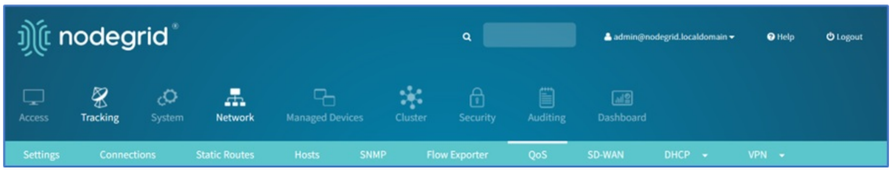
5. Click **Download Certificate**.
6. On pop-up dialog, click **Allow**.



7. Certificate is saved to the local computer download location.

QoS tab

QoS (Quality of Service) rules can be configured. Three configuration levels are available: Interface, Classes, Rules.

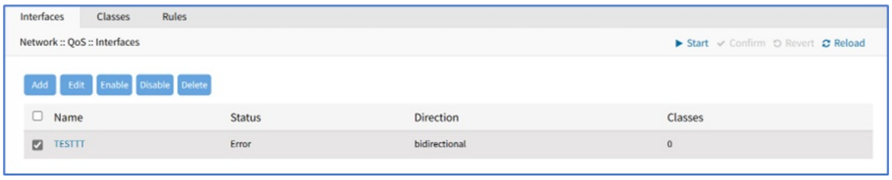


Interfaces sub-tab

The Interface tab allows you to manage QoS on each available interface. The main table displays information regarding the Name, Status, Direction, and Classes for each interface.

NOTE

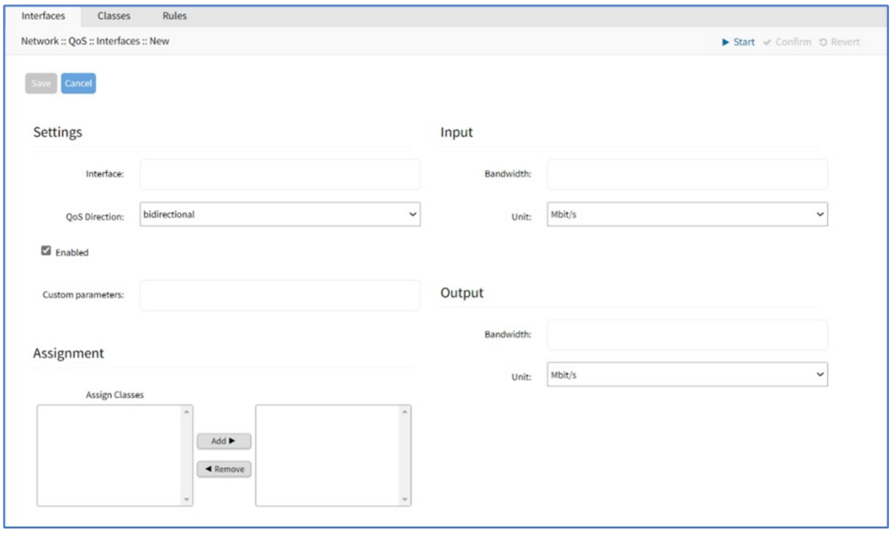
Status can be Disabled, Running, or Error



□	Name	Status	Direction	Classes
☑	TESTTT	Error	bidirectional	0

Add an Interface

1. Go to *Network :: QoS :: Interfaces*.
2. Click **Add** (displays dialog).



Interface:

QoS Direction: bidirectional

☑ Enabled

Custom parameters:

Bandwidth:

Unit: Mbit/s

Bandwidth:

Unit: Mbit/s

3. In *Settings* menu:
   a. Enter **Interface** (must match existing interface name).
   b. On **QoS Direction** drop-down, select one (Input, Output, Bidirectional).
   c. As needed, select **Enabled** checkbox.
4. On **Custom parameters** (advanced users only – enter FireQOS commands).
5. In *Assignment* menu, to add a Class, select item on left-side panel. Click **Add►** (item is moved). To remove a Class, select item on right-side panel. Click **◄Remove** (item is moved).
6. In *Input* menu: (Input menu details must match *Output* menu details) Enter **Bandwidth**. On **Unit** drop-down, select one (GB/s, MB/s, KB/s, B/s, Gbit/s, Mbit/s, Kbit/s, bit/s)
7. In *Output* menu, enter **Bandwidth.** On **Unit** drop-down, select one (GB/s, MB/s, KB/s, B/s, Gbit/s, Mbit/s, Kbit/s, bit/s)
8. Click **Save**.

Edit Interface

1. Go to *Network :: QoS :: Interfaces.*
2. In the *Name* column, locate and select checkbox,
3. Click **Edit** (opens dialog).
4. Make changes, as needed.
5. Click **Save**.

Delete Interface

1. Go to *Network :: QoS :: Interfaces.*
2. Select checkbox to be deleted.
3. Click **Delete**.
4. On confirmation dialog, click **OK**.

Enable Interface

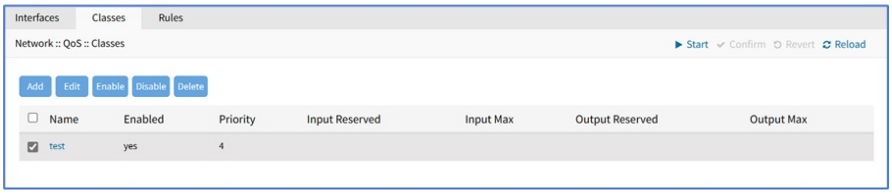
1. Go to *Network :: QoS :: Interfaces.*
2. Select checkbox to be enabled.
3. Click **Enable**.

Disable Interface

1. Go to *Network :: QoS :: Interfaces.*
2. Select checkbox to be disabled.
3. Click **Disable**.

Classes sub-tab

This manages QoS classes.

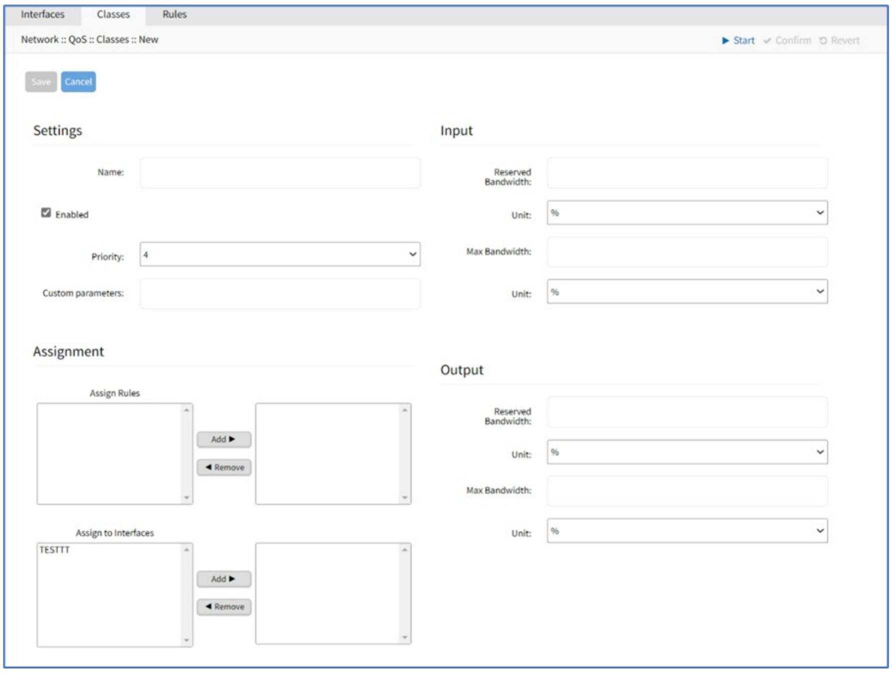


Interfaces
Classes
Rules
Network :: QoS :: Classes
▶ Start ✓ Confirm ⟲ Revert ⟳ Reload
Add
Edit
Enable
Disable
Delete

□	Name	Enabled	Priority	Input Reserved	Input Max	Output Reserved	Output Max
☑	test	yes	4				

Add a Class

1. Go to *Network :: QoS :: Classes*.
2. Click **Add** (displays dialog).



Name:

☑ Enabled

Priority: 4

Custom parameters:

Reserved Bandwidth:

Unit: %

Max Bandwidth:

Unit: %

Reserved Bandwidth:

Unit: %

Max Bandwidth:

Unit: %

3. In *Settings* menu, enter details:
    a. **Name** (descriptive name for this class)
    b. **Enabled** checkbox
    c. **Priority** drop-down, select one (0, 1, 2, 3, 4, 5, 6, 7) (0=highest priority).
4. In *Assignment* menu (enter details):
    a. On *Assign Rules* menu, to add a Rule, select item on left-side panel. Click **Add►** (item is moved). To remove a Rule, select item on right-side panel. Click **◄Remove** (item is moved).

    > **NOTE**
    >
    > If multiple rules are added, they are applied as OR (for example, if two rules are added, whichever rule applies is the rule used for the class.

    b. In *Assign Interfaces* menu, to add an Interface, select item on left-side panel. Click **Add►** (item is moved). To remove an Interface, select item on right-side panel. Click **◄Remove** (item is moved).
5. In *Input* menu, enter details: (Input menu details must match *Output* menu details)
    a. Enter **Reserved Bandwidth**. On **Unit** drop-down, select one (%, GB/s, MB/s, KB/s, B/s, Gbit/s, Mbit/s, Kbit/s, bit/s).
    b. Enter **Max Bandwidth**. On **Unit** drop-down, select one (%, GB/s, MB/s, KB/s, B/s, Gbit/s, Mbit/s, Kbit/s, bit/s).
6. In *Output* menu, enter details:
    a. Enter **Reserved Bandwidth**. On **Unit** drop-down, select one (%, GB/s, MB/s, KB/s, B/s, Gbit/s, Mbit/s, Kbit/s, bit/s).
    b. Enter **Max Bandwidth**. On **Unit** drop-down, select one (%, GB/s, MB/s, KB/s, B/s, Gbit/s, Mbit/s, Kbit/s, bit/s).
7. Click **Save**.

    > **NOTE**
    >
    > The “Input” and “Output” sections only apply to interfaces with that corresponding direction. For example, if a class has “Input” and “Output” limits but is assigned to an interface with “output”, only “Output” limits apply.

Edit a Class

1. Go to *Network :: QoS :: Classes*.
2. In the *Name* column, locate and select checkbox,
3. Click **Edit** (opens dialog).
4. Make changes, as needed.
5. Click **Save**.

Delete a Class

1. Go to *Network :: QoS :: Classes*.

2. Select checkbox to be deleted.
3. Click **Delete**.

Enable a Class

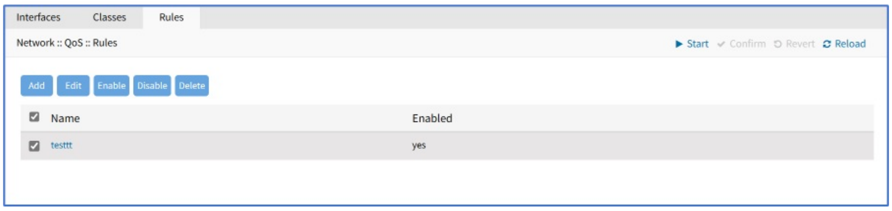
1. Go to *Network :: QoS :: Classes*.
2. Select checkbox to be enabled/disabled.
3. Click **Enable** (to enable class).

Disable a Class

1. Go to *Network :: QoS :: Classes*.
2. Select checkbox to be enabled/disabled.
3. Click **Disable** (to disable class).

Rules sub-tab

Customer QoS rules are managed with these actions: Add, Edit, Enable/Disable, and Delete. The main table contains information on existing rules.



Interfaces Classes Rules

Network :: QoS :: Rules

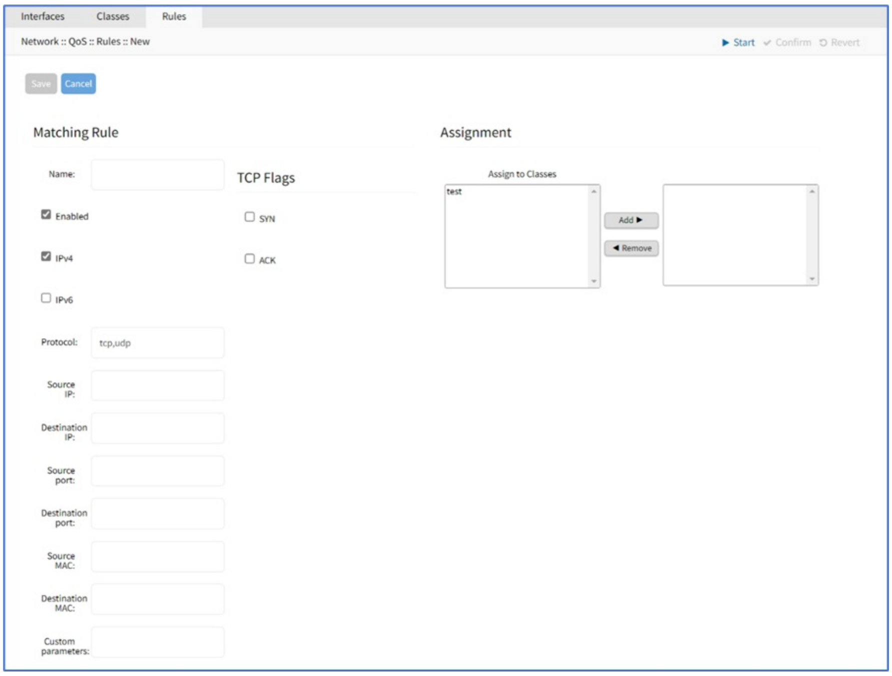
▶ Start ✓ Confirm ⟲ Revert ⟳ Reload

Add Edit Enable Disable Delete

☑	Name	Enabled
☑	testtt	yes

Add Rule

1. Go to *Network :: QoS :: Rules*.
2. Click **Add** (displays dialog).



Interfaces Classes Rules

Network :: QoS :: Rules :: New

▶ Start ✓ Confirm ⟲ Revert

Save Cancel

Matching Rule

Name:

☑ Enabled

☑ IPv4

☐ IPv6

Protocol: tcp,udp

Source IP:

Destination IP:

Source port:

Destination port:

Source MAC:

Destination MAC:

Custom parameters:

TCP Flags

☐ SYN

☐ ACK

Assignment

Assign to Classes

test

Add ▶

◀ Remove

3. In *Matching Rule* menu, enter details:
    a. **Name** (descriptive name for this rule)
    b. **Enabled** checkbox
    c. **IPv4** checkbox
    d. **IPv6** checkbox
    e. **Protocol**

    > **NOTE**
    >
    > Options for "Protocol" include the majority of protocol types. Entry can be by protocol number or lower-case protocol keyword. Multiple protocols can be input using comma-separated entries. Official source is at Internet Assigned Numbers Authority.

    f. **Source IP**
    g. **Destination IP**
    h. **Source Port**
    i. **Destination Port**
    j. **Source MAC**
    k. **Destination MAC**
    l. **Custom parameters** (advanced users only – enter FireQOS commands)
4. In *TCP Flags* menu, select (as needed):
    a. **SYN** checkbox
    b. **ACK** checkbox
5. In *Assignment* menu: to add a Rule, select item on left-side panel. Click **Add**► (item is moved). To remove a Rule, select item on right-side panel. Click ◄**Remove** (item is moved).
6. Click **Save**.

    > **NOTE**
    >
    > All parameters in a rule will be applied as an “AND” operation.

For fields that support multiple values, enter comma separated values. Numeric fields support ranges, separated with a dash (i.e., 22-100).

Edit Rule

1. Go to *Network :: QoS :: Rules*.
2. In the *Name* column, locate and select checkbox,
3. Click **Edit** (opens dialog).
4. Make changes, as needed.
5. Click **Save**.

Delete Rule

1. Go to *Network :: QoS :: Rules*.
2. Select checkbox to be deleted.
3. Click **Delete**.
4. On confirmation dialog, click **OK**.

Enable Rule

1. Go to *Network :: QoS :: Rules*.
2. Select checkbox to be enabled.
3. Click **Enable**.

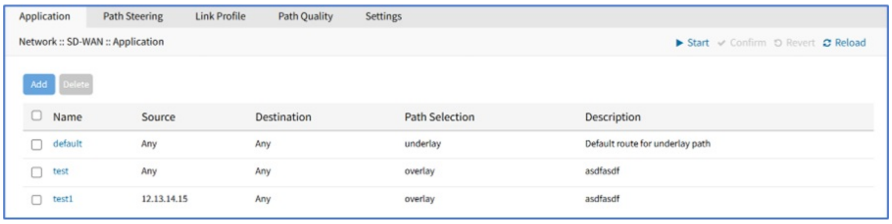
Disable Rule

1. Go to *Network :: QoS :: Rules*.
2. Select checkbox to be disabled.
3. Click **Disable**.

SD-WAN tab

ZPE recommends working with SD-WAN only with the ZPE Cloud application. Modifying directly on the Nodegrid device loses synchronization with ZPE Cloud.

Application sub-tab

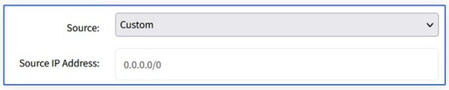


Network :: SD-WAN :: Application

□	Name	Source	Destination	Path Selection	Description
□	default	Any	Any	underlay	Default route for underlay path
□	test	Any	Any	overlay	asdfasdf
□	test1	12.13.14.15	Any	overlay	asdfasdf

Add Application

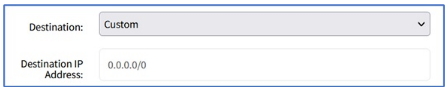
1. Go to *Network :: SD-WAN :: Application*.
2. Click **Add** (displays dialog).
3. Enter **Name** and **Description**.
4. In *Match* menu:
   a. On **Source** drop-down, select one (Any, Custom)
      - If **Custom** selected dialog expands. Enter **Source IP Address**.



Source: Custom

Source IP Address: 0.0.0.0/0

   b. On **Destination** drop-down, select one (Any, Custom)
      - If **Custom** checkbox is selected, dialog expands. Enter **Source IP Address**.



Destination: Custom

Destination IP Address: 0.0.0.0/0

5. In *Action* menu, select one:
   a. **Underlay** radio button
   b. **Overlay** radio button
6. Click **Save**.

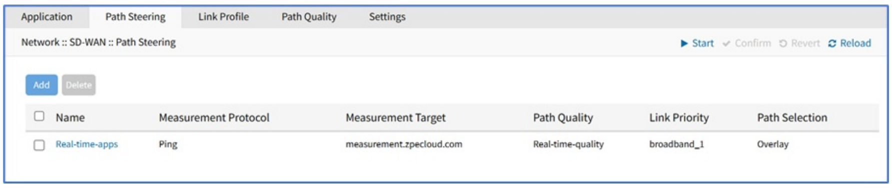
Edit Application

1. Go to *Network :: SD-WAN :: Application*.
2. In the *Name* column, locate and select checkbox,
3. Click **Edit** (opens dialog).
4. Make changes, as needed.
5. Click **Save**.

Delete Application

1. Go to *Network :: SD-WAN :: Application*.
2. Select checkbox to be deleted.
3. Click **Delete**.
4. On confirmation dialog, click **OK**.

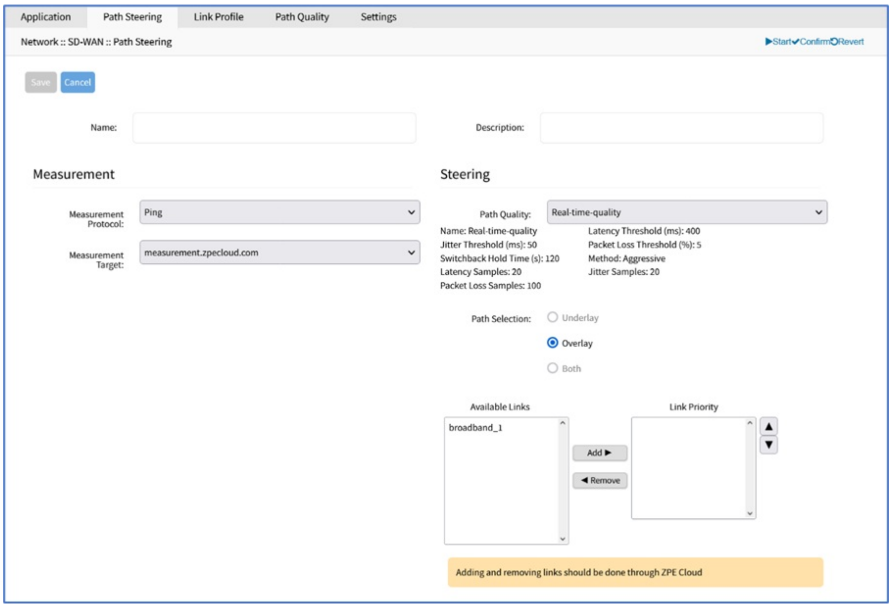
Path Steering sub-tab



□	Name	Measurement Protocol	Measurement Target	Path Quality	Link Priority	Path Selection
□	Real-time-apps	Ping	measurement.zpecloud.com	Real-time-quality	broadband_1	Overlay

Add Path Steering

1. Go to *Network :: SD-WAN :: Path Steering*.
2. Click **Add** (displays dialog).



Measurement Protocol: Ping

Measurement Target: measurement.zpecloud.com

Path Quality: Real-time-quality

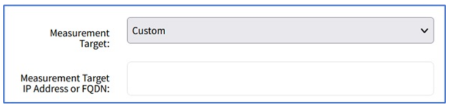
Name: Real-time-quality
Jitter Threshold (ms): 50
Switchback Hold Time (s): 120
Latency Samples: 20
Packet Loss Samples: 100
Latency Threshold (ms): 400
Packet Loss Threshold (%): 5
Method: Aggressive
Jitter Samples: 20

Path Selection: ○ Underlay ● Overlay ○ Both

Available Links: broadband_1

Adding and removing links should be done through ZPE Cloud

3. Enter **Name** and **Description**.
4. In *Measurement* menu:
   a. On **Measurement Protocol** drop-down, select one (Ping).
   b. On **Measurement Target** drop-down, select one.
      - If **Custom** (expands dialog), enter **Measurement Target IP Address or FQDN**.



Measurement Target: Custom

Measurement Target IP Address or FQDN:

5. In *Steering* menu:
   a. On **Path Quality** drop-down, select one.
   b. On *Port Selection* menu, select one.
      - **Underlay** radio button
      - **Overlay** radio button
      - **Both** radio button
6. In *Available Links* section, select from left-side panel, click **Add**▶ to move to right-side panel. To remove from right-side panel, select, and click ◀**Remove**.

   > **NOTE**
   >
   > If device is enrolled in ZPE Cloud, these links should be changed on the ZPE Cloud application.

7. Click **Save**.

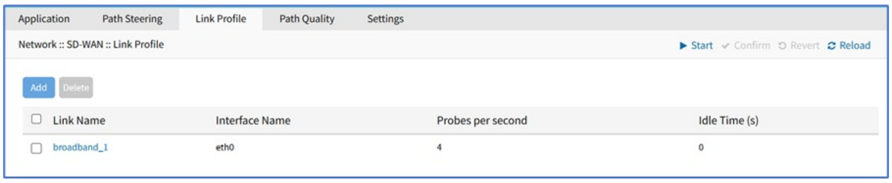
Edit Path Steering

1. Go to *Network :: SD-WAN :: Path Steering*.
2. Click on Name (opens dialog).
3. Make changes, as needed.
4. Click **Save**.

Delete Path Steering

1. Go to *Network :: SD-WAN :: Path Steering*.
2. Select checkbox next to **Name**.
3. Click **Delete**.
4. On confirmation dialog, click **OK**.

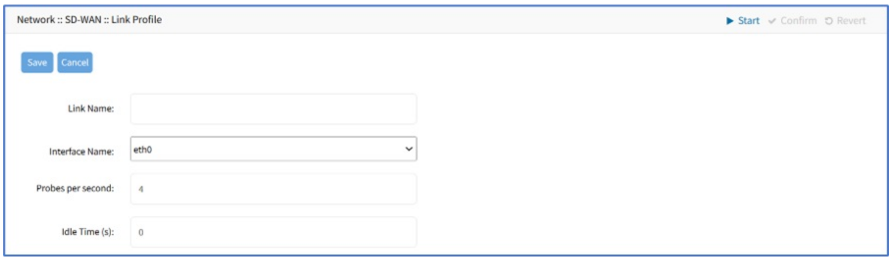
Link Profile sub-tab



□	Link Name	Interface Name	Probes per second	Idle Time (s)
□	broadband_1	eth0	4	0

Add Link Profile

1. Go to *Network :: SD-WAN :: Link Profile*.
2. Click **Add** (displays dialog).



Link Name:

Interface Name: eth0

Probes per second: 4

Idle Time (s): 0

3. Enter details:
   a. Enter **Link Name**.
   b. On **Interface Name** drop-down, select one.
   c. Set **Probes per second** (default: 4).
   d. Set **Idle Time**. (seconds) (default: 0).
4. Click **Save**.

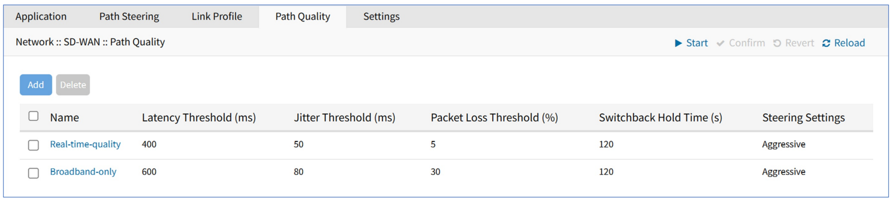
Edit Link Profile

1. Go to *Network :: SD-WAN :: Link Profile*.
2. In **Name** column, click on name.
3. Make changes, as needed.
4. Click **Save**.

Delete Link Profile

1. Go to *Network :: SD-WAN :: Link Profile*.
2. Select checkbox to be deleted.
3. Click **Delete**.
4. On confirmation dialog, click **OK**.

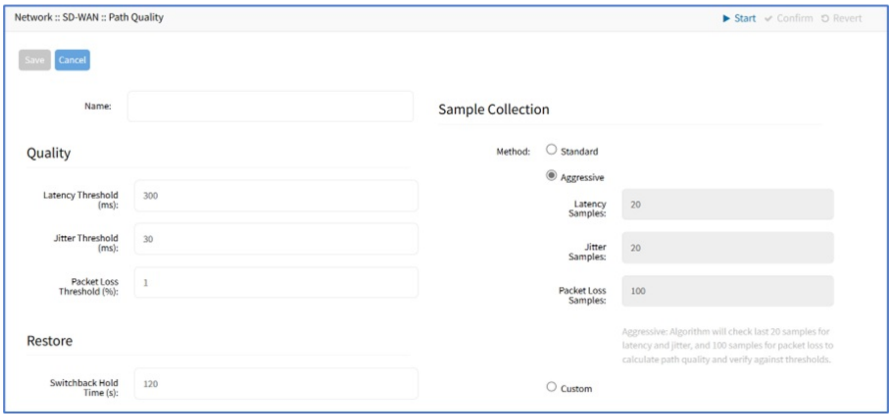
Path Quality sub-tab



□	Name	Latency Threshold (ms)	Jitter Threshold (ms)	Packet Loss Threshold (%)	Switchback Hold Time (s)	Steering Settings
□	Real-time-quality	400	50	5	120	Aggressive
□	Broadband-only	600	80	30	120	Aggressive

Add Path Quality

1. Go to *Network :: SD-WAN :: Link Profile*.
2. Click **Add** (displays dialog).



Name:

Latency Threshold (ms): 300

Jitter Threshold (ms): 30

Packet Loss Threshold (%): 1

Switchback Hold Time (s): 120

Method: ○ Standard ● Aggressive

Latency Samples: 20

Jitter Samples: 20

Packet Loss Samples: 100

Aggressive: Algorithm will check last 20 samples for latency and jitter, and 100 samples for packet loss to calculate path quality and verify against thresholds.

○ Custom

3. Enter **Name**.
4. In *Quality* menu, enter details:
   a. **Latency Threshold (ms)** (default: 300)
   b. **Jitter Threshold (ms)** (default: 30)
   c. **Packet Loss Threshold (%)** (default: 1)
5. In *Restore* menu, enter **Switchback Hold Time (s)** (default: 120)
6. In *Sample Collection* menu, **Method**, select one:
   - **Standard** radio button (fields are read-only):
     - **Latency Samples** (default: 50)
     - **Jitter Samples**: (default: 50)
     - **Packet Loss Samples** (default: 100)
   - **Aggressive** radio button (fields are read-only)
     - **Latency Samples** (default: 50)
     - **Jitter Samples** (default: 50)
     - **Packet Loss Samples** (default: 100)
   - **Custom** radio button (fields are editable)
7. Enter values for:
   a. **Latency Samples**
   b. **Jitter Samples**
   c. **Packet Loss Samples**
8. Click **Save**.

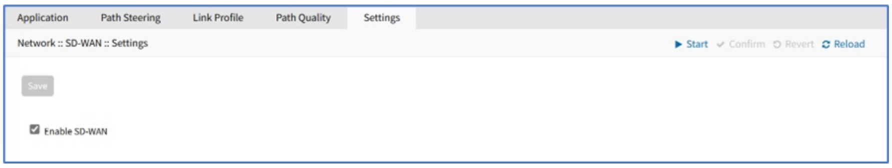
Edit Path Quality

1. Go to *Network :: SD-WAN :: Path Quality*.
2. In **Name** column, click on name.
3. Make changes, as needed.
4. Click **Save**.

Delete Path Quality

1. Go to *Network :: SD-WAN :: Path Quality*.
2. Select checkbox to be deleted.
3. Click **Delete**.
4. On confirmation dialog, click **OK**.

Settings sub-tab



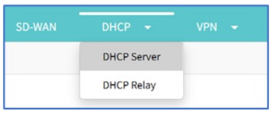
☑ Enable SD-WAN

Enable SD-WAN

(available in v5.4.6+)

1. Go to *Network :: SD-WAN :: Settings*.
2. Select **Enable SD-WAN**.
3. Click **Save**.

DHCP :: DHCP Server tab

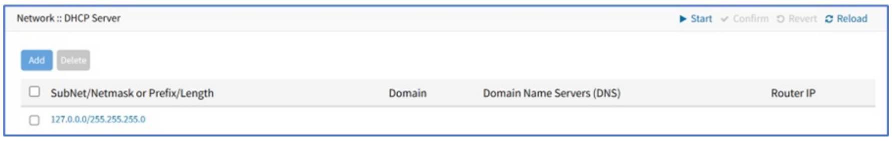


The DHCP server for devices can be configured and managed. By default, the DHCP server is not configured or active. When a DHCP scope is defined, the system serves IP addresses to all devices connected to the interface and which match the general DHCP scope.

Configuration is a two-step process.

First, the general DHCP scope and configuration is configured and created.

Second, IP address ranges (Network Range) are defined to be used as server IP addresses and as IP address reservations for specific hosts.



□ SubNet/Netmask or Prefix/Length	Domain	Domain Name Servers (DNS)	Router IP
□ 127.0.0.0/255.255.255.0			

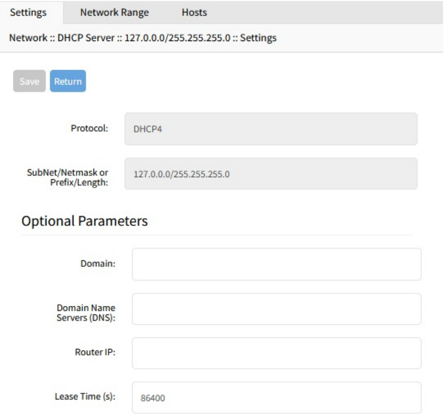
Manage DHCP Server

Add DHCP Server

1. Go to *Network :: DHCP drop-down :: DHCP Server*.
2. Click **Add** (displays dialog):
3. On *Protocol* menu, select one:
    a. **DHCP4** radio button (expands dialog) enter:
       Subnet (must match the settings of a configured interface)
       Netmask (defined subnet – format: xxx.xxx.xxx.xxx)
    b. **DHCP6** radio button (expands dialog) enter:
       Prefix
       Length
4. In *Optional Parameters* menu, enter:
    a. **Domain**
    b. **Domain Name Services (DNS)**
    c. **Router IP** (DHCP4 only)
    d. **Lease Time (s)** (default: 86400).
5. Click **Save**.

Edit DHCP Server Configuration

1. Go to *Network :: DHCP drop-down :: DHCP Server*.
2. On *Subnet/Netmask* column, click a name. This displays three sub-tabs: Settings, Network Range, Hosts.
3. On **Settings** sub-tab, make changes as needed, then click **Save**.



Network :: DHCP Server :: 127.0.0.0/255.255.255.0 :: Settings

Protocol: DHCP4

SubNet/Netmask or Prefix/Length: 127.0.0.0/255.255.255.0

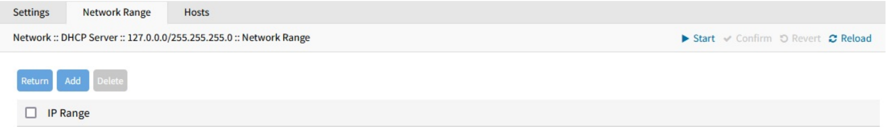
Domain:

Domain Name Servers (DNS):

Router IP:

Lease Time (s): 86400

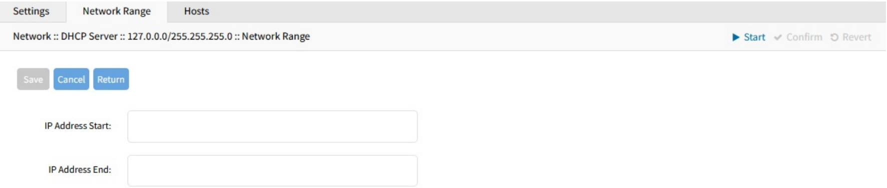
4. On **Network Range** sub-tab, the user can define one or more ranges of dynamic addresses to be allocated within the network:



Network :: DHCP Server :: 127.0.0.0/255.255.255.0 :: Network Range

☐ IP Range

    a. *Add Network Range*: click **Add** (displays dialog):



Network :: DHCP Server :: 127.0.0.0/255.255.255.0 :: Network Range

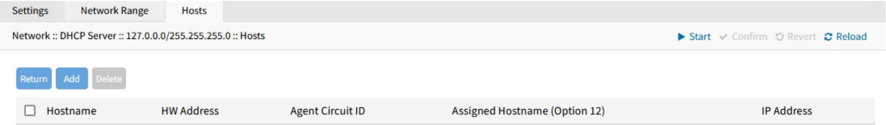
IP Address Start:

IP Address End:

- Enter **IP Address Start** (first IP address to be served)
- Enter **IP Address End** (last IP address to be served)
- Click **Save**.

    b. To edit network range, click on the **IP Range** name (expands dialog). Make changes, as needed. Click **Save**.
    c. To delete a network range, select the *IP Range* checkbox. Click **Delete**.

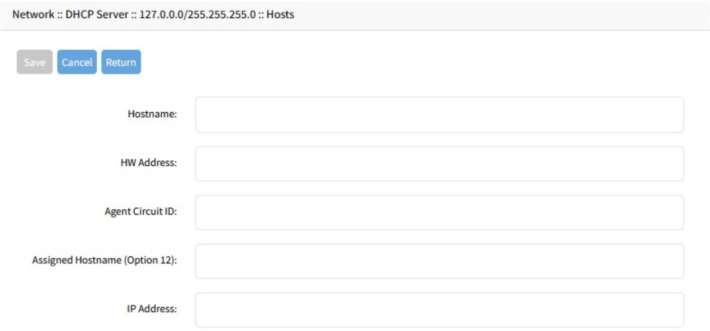
5. On **Hosts** sub-tab, a Host can be assigned a static IP address when it joins the network. It is recommended that static addresses are not within any configured dynamic Network Ranges:



Network :: DHCP Server :: 127.0.0.0/255.255.255.0 :: Hosts

☐ Hostname	HW Address	Agent Circuit ID	Assigned Hostname (Option 12)	IP Address

    a. To add Host, click **Add** (displays dialog):


Network :: DHCP Server :: 127.0.0.0/255.255.255.0 :: Hosts

b. Enter details:
   - **Hostname:** An arbitrary identifier for the host
   - **HW Address (optional):** The MAC address used to identify the host. When a device with this MAC address asks for a DHCP lease, it will be associated with this Host entry and assigned the static IP. Either **HW Address** or **Agent Circuit ID**, or both, must be configured
   - **Agent Circuit ID (optional):** A vendor-defined "circuit" identifier. Either **HW Address** or **Agent Circuit ID**, or both, must be configured
   - **Assigned Hostname (Option 12) (optional):** A hostname that will be sent and may or may not be honored by the requesting client
   - **IP Address:** The static address to assign to this host. It is recommended that this address does not fall within any configured dynamic Network Range
   - Click **Save**

c. To edit host, click on the **Hostname** (expands dialog). Make changes, as needed. Click **Save**.

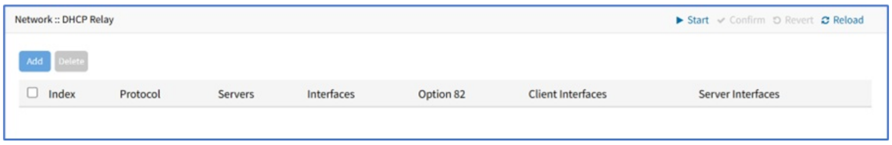
d. To delete a Host, select the Hostname checkbox. Click **Delete**.

Delete DHCP Server

1. Go to *Network :: DHCP drop-down :: DHCP Server*.
2. Select checkbox to be deleted.
3. Click **Delete**.
4. On the confirmation dialog, click **OK**.

DHCP :: DHCP Relay tab

(available in v5.6+)



Network :: DHCP Relay

□	Index	Protocol	Servers	Interfaces	Option 82	Client Interfaces	Server Interfaces

Manage DHCP Relay

Add DHCP Relay

1. Go to *Network :: DHCP drop-down :: DHCP Relay*.
2. Click **Add** . On *Add* dialog, enter details:
3. In *Protocol* menu, select one:
   a. **DHCPv4** radio button, enter details:
      - **Servers**
      - (optional) **Interfaces**
      - **Enable Option** (expands dialog). On **Incoming Option 82 Policy** drop-down, select one (Replace Option 82, Append Option 82, Forward Packet, Discard Packet)

   b. **DHCPv6** radio button (expands dialog), Enter details:
      - **Server Interfaces**
      - **Client Interfaces**

4. Click **Save**.

Edit DHCP Relay

1. Go to *Network :: DHCP drop-down :: DHCP Relay*.
2. Click on the name (displays dialog).
3. Make changes as needed.
4. Click **Save**.

Delete DHCP Relay

1. Go to *Network :: DHCP drop-down :: DHCP Relay*.
2. Select checkbox of Index to delete.
3. Click **Delete**.

VPN :: Wireguard tab

Wireguard VPN

Wireguard is a modern open-source VPN solution that provides point-to-point and site-to-site VPN/Overlay tunnels. The protocol is already widely adopted in Public Cloud and Kubernetes deployments and is starting to be adapted in Enterprise networks. It provides an easy-to-implement and operate VPN alternative to IPSec. Due to its modern architecture, Wireguard is the ideal VPN/Overlay network for management networks, like ZPE Systems Isolated Management Infrastructure Networks (IMI).

How this Feature could be Useful?

Overlay networks are a requirement for many branch or multi-site deployments. While the main connectivity between locations might be provided through an existing infrastructure, are looking at many customers for backup connectivity in case the main connection is interrupted. In most cases, it utilizes the backup connection via a 4G/5G connection using the Public internet. Providing a secure backup network connection via the public internet requires an enterprise-grade VPN/overlay solution that is easy to maintain and operate while supporting a wide variety of connection options and limitations, including no public IP address, carrier-grade NAT, IPv4 and IPv6 support, and OSPF or BGP support.

Feature Benefits and Advantages

- Simple to implement and Operate.
- WireGuard uses state-of-the-art cryptography, like the Noise protocol framework, Curve25519, ChaCha20, Poly1305, BLAKE2, SipHash24, HKDF, and secure trusted constructions. It makes conservative and reasonable choices and has been reviewed by cryptographers.
- Minimal Attack Surface.
- High Performance: A combination of extremely high-speed cryptographic primitives and the fact that WireGuard lives inside the Linux kernel means that secure networking can be very high-speed. It is suitable for both small embedded devices like smartphones and fully loaded backbone routers.
- Uses RSA keys and optional PSKs for authentication.
- Roaming of End Points is an integrated part of the solution.
- Good Client support, with native Windows, MacOS, Linux, iOS, and Android support.
- Native support for tunnel interfaces to allow for Multicast traffic.
- Support for IPv6 and IPv4 over the same interface.
- Part of the Linux kernel ensures long-term support.
- Support in Nodegrid since Version 5.2.0+

Manage Wireguard Configurations

How to Create a Site-to-Site VPN/Overlay Network using Wireguard

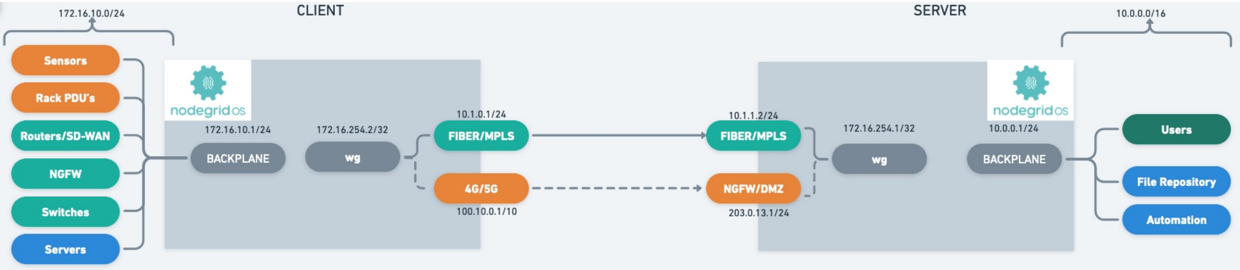
Wireguard supports a wide range of overlay architecture designs. The most common architecture used with Nodegrids is the Server-Client architecture, which supports host-to-host and site-to-site communication. Wireguard does not directly differentiate between clients and servers. The main difference is that a server actively listens for incoming connections on a specified UDP port.

Another aspect that must be mentioned is the native support for roaming connections, which sets Wireguard apart from other VPN technologies like IPSec and OpenVPN. Wireguard sessions are not bound to a specific interface or network on either the client or the server site. Tunnels can dynamically change interfaces and networks without closing the session. This process is supported from both ends by dynamically updating the other side over changing endpoint details, like roaming IP Addresses or dynamically assigned ports. The result is a dynamic failover of the overlay network without impact on existing sessions or the need to re-establish connections which utilize the tunnel.

> Routing
>
> For a site-to-site VPN/Overlay design, is it required to enable routing on each device in the Network **Settings tab**.
> Nodegrid OS supports more advanced routing options, including dynamic routing, for example, BGP and OSPF.
> Please contact support for more details and guidance.

Overview

The guide uses the following network layout as an example configuration.



Quick Step-by-step Walkthrough

- *Server-Side:*
  - *Configure a Server Configuration under **Network** :: **VPN** :: **Wireguard***
  - *Take note of the server's public key*
- *Repeat the following steps for each Client*
  - *Client Side:*
    - *Configure a Client Configuration under Network :: VPN drop-down :: Wireguard*
    - *Take note of the client's public key*
    - *Configure the server as a peer in the Client Configuration under Network :: VPN drop-down :: Wireguard :: <CLIENT CONFIGURATION>*
    - *Provide the Public IP, Port, and public key of the server*
- *Server-Side:*
  - Configure the client as a peer in the Server Configuration under *Network :: VPN drop-down :: Wireguard :: <SERVER CONFIGURATION>*
    - *public key of the client*

Server-Side Configuration

Server-side configuration is most commonly done on Nodegrid appliances, which act as central access points or VPN concentrators. Typically, these are Nodegrid VSR (Virtual Service Router) or NetSR appliances hosted in a Data Center or Public Cloud.

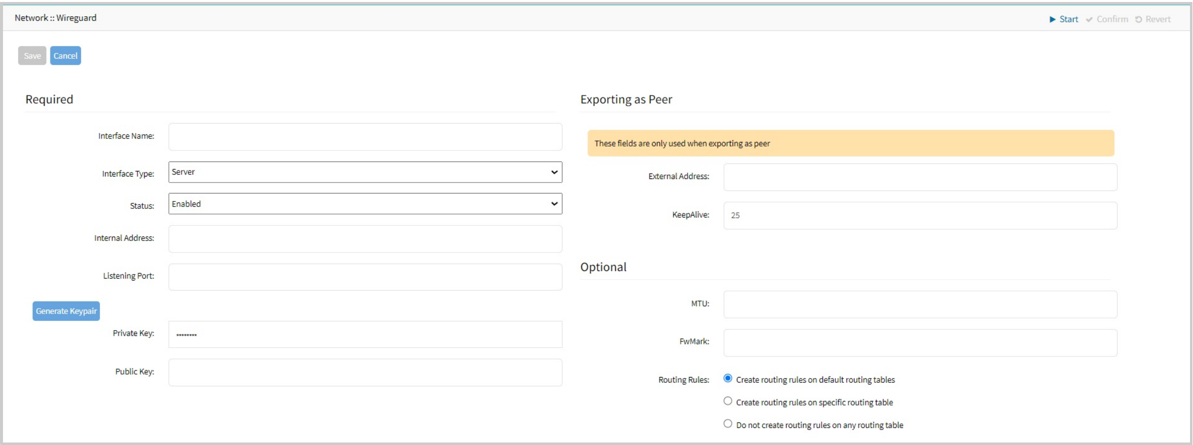
A Nodegrid instance can handle multiple Server configurations at the same time. This allows for traffic separation, for example, separation of Nodegrid to Nodegrid communication and User to Nodegrid configuration and more.

Server Interface Configuration

This part of the configuration is only required once for each overlay network. The configuration creates a server interface and allows them to authorize clients to connect to the server configuration.

To configure a server interface, use the following steps (for a full list of options, look here):

1. Go to **Network** :: **VPN** :: **Wireguard**.
2. Click **Add** (opens dialog).
3. Enter an **Interface Name** (*Example: EMEA*); this name is used for the network interface.
4. From the **Interface Type** drop-down list, select Server.



Required

Interface Name:

Interface Type: Server

Status: Enabled

Internal Address:

Listening Port:

Private Key: ••••••••

Public Key:

Exporting as Peer

These fields are only used when exporting as peer

External Address:

KeepAlive: 25

Optional

MTU:

FwMark:

Routing Rules:
● Create routing rules on default routing tables
○ Create routing rules on specific routing table
○ Do not create routing rules on any routing table

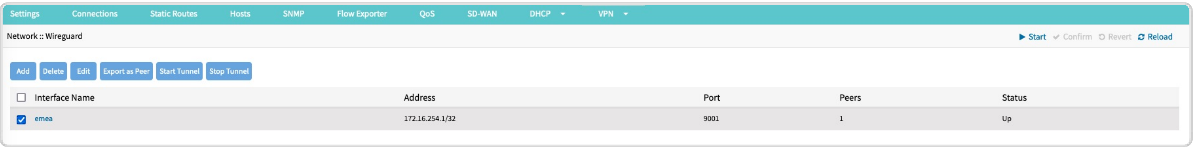
5. From the **Status** drop-down, select **Enabled.**
6. Enter an **Internal Address** (*Example: 172.16.254.1/32*); this IP Address is used as an internal interface IP Address**.** In most cases, you can use a /32 IP address.

> **Internal Address**
>
> The internal IP address assigned to the Wireguard interface is used for Cluster configuration and BPG and OSP peering configurations.

7. Enter a UDP **Listening Port** (*Example: 9001*)**,** and the server will listen to this UDP for incoming client sessions. The UDP port must be openend on teh firewall.
8. Click **Generate Keypair,** to create a new Private/Public RSA key pair. This key pair is used to secure the connection.
   The Public key is exchanged with authorized Wireguard Clients.
9. In the **Exporting as Peer**section:
   a. Define the **External Address** (*Example: 10.1.1.2*) through which the server is reachable
   b. Enter the **KeepAlive** value. The value is in seconds and provides a keep-alive functionality for the overlay network. The value should be between 10 - 120 sec, and the recommended value is **25** sec.
10. You can leave the **Optional settings** on default.
11. The Server configuration can be exported to a file for easy import into clients as a peer.

> **Note**
>
> When you export a configuration, the hostname of the device is prefixed to the interface name. For example, *Nodegrid_NG2.conf* is the name of a sample exported conf file where Nodegrid is the hostname and NG2 is the name of the interface

12. Go to **Network** *::* **VPN** *::* **Wireguard**.



☐	Interface Name	Address	Port	Peers	Status
☑	emea	172.16.254.1/32	9001	1	Up

13. Select the Interface Name.
14. Click **Export Peer**.
15. The file is downloaded to the local download location.

Client (Peer) Configuration

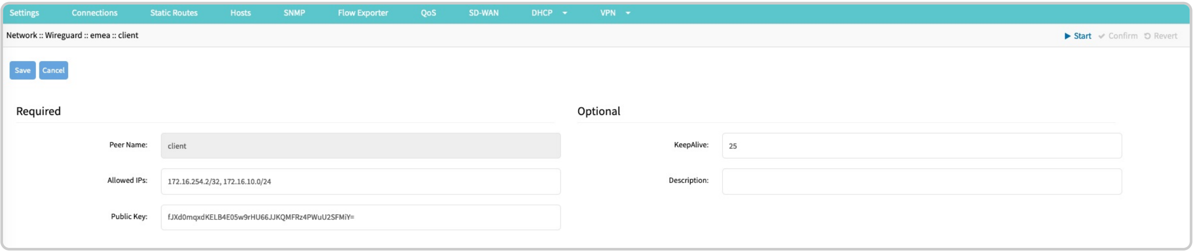
- Wireguard's security is based on a mutually trusted RSA Keypair exchange, which requires exchanging public key information in both directions.
- This means that every client must be specifically allowed and trusted on the server. This differs from most IPSec implementations, which are based on Pre-Shared key authentication, and the server might accept multiple connections with a valid preshared key without explicitly whitelisting clients. Wireguard does not support this method.
- The exchange of public keys dramatically improves security, specifically on the client side. No Client has the required information to intercept or imitate other clients, and clients can be individually removed and disabled from the configuration without impacting any other client. This eliminates the requirement to rotate preshared keys regularly.
- Clients can be created manually or by importing a Peer Export File, which can be made on the client.

> **Compleat Client-side configuration first**
>
> Due to the mutual exchange of Public Keys, it is recommended first to complete the Client-side configuration and then authorize the client on the server-side

Manual Peer Configuration

To allow a client/peer to connect to the server, create a peer using the following steps (for a full list of options, look here):

1. Go to *Network :: VPN drop-down :: Wireguard*
2. Click on the Server Interface (*Example: emea*) configuration that was created in the previous step
3. Click on **Add** (opens dialog).



Network :: Wireguard :: emea :: client

Required

Peer Name: client

Allowed IPs: 172.16.254.2/32, 172.16.10.0/24

Public Key: fJXd0mqxdKELB4E05w9rHU66JJKQMFRz4PWuU2SFMiY=

Optional

KeepAlive: 25

Description:

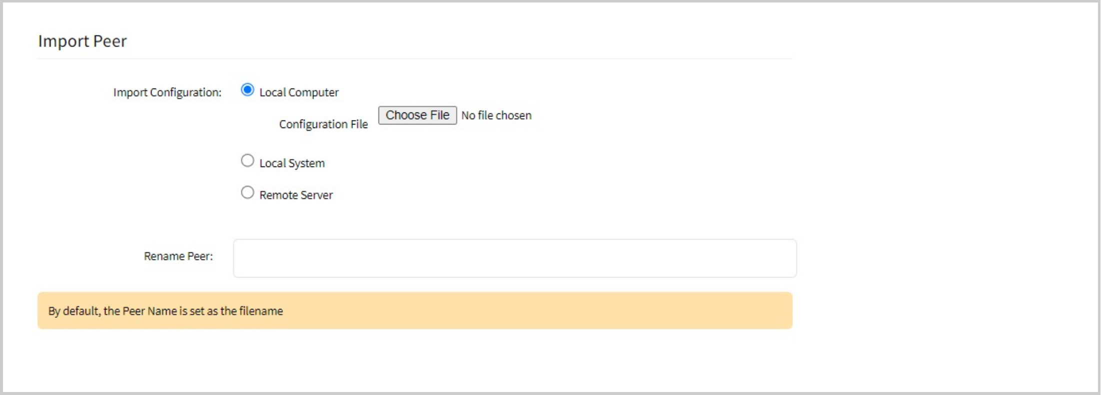
4. Enter a **Peer Name** (*Example: client*); this name is used to identify the client and must be a string without spaces or special characters.
5. Provide a list of **Allowed IP** addresses or ranges (*Example: 172.16.234.2/32, 172.16.10.0/24*). This list is used in the default configuration to create the required routing information. For Host-to-Host communication, the list should contain only the internal IP address of the client. For site-to-site configurations, it should contain the remote IP network range
6. Provide the client **Public Key,** which was created during the client-side setup.
7. It is *recommended* that a **KeepAlive** value is provided. The value is in seconds and provides a keep-alive functionality for the overlay network. The value should be between 10 - 120 sec, and the recommended value is **25** sec.

> **KeepAlive and Handshake**
>
> Wireguard uses a " Handshakes " concept, similar to heartbeats. Handshakes are renewed every 2 minutes but are passive. This means handshakes are not proactively exchanged; for this, the KeepAlive feature is used. If no handshake is available or older than 2 minutes, this indicates a connection issue.
> For this reason, it is recommended to always define a KeepAlive value.

8. Option: Provide a **Description** for the Client; this is a free text field that supports spaces and special characters

Import Peer from Client Export File

1. Go to *Network :: VPN drop-down :: Wireguard*
2. Click on the Server Interface (*Example: **emea***) configuration that was created in the previous step.
3. Click **Import Peer** (displays dialog).



Import Peer

Import Configuration: ● Local Computer

Configuration File No file chosen

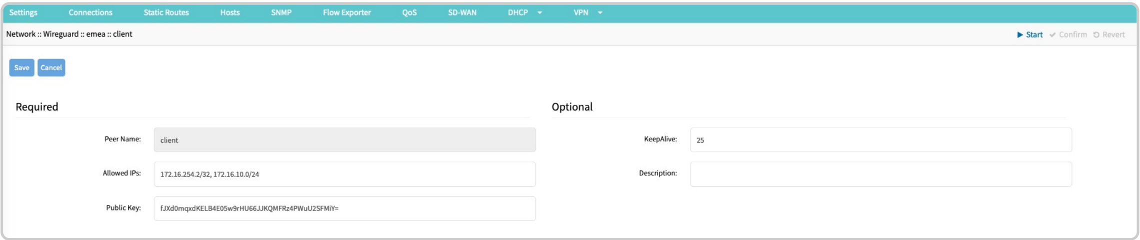
○ Local System

○ Remote Server

Rename Peer:

By default, the Peer Name is set as the filename

4. Provide the file location, which can be located locally (**Local System**) on the server, on a workstation (**Local Computer**), or on a **Remote Server.**
5. In the Rename Peer field, enter a Peer Name (*Example: client*); this name is used to identify the client and must be a string without spaces or special characters. If you do not provide a Name the default name is taken from the imported file.
6. Click **Save**.
7. After the Peer was imported, click on the newly created ***peer** (Example: Client)*
    - Update the **Allowed IP** *(Example: 172.16.254.2/32, 172.16.10.0/24)* configuration and include the client's network range
    - Validate the **KeepAlive** setting. The value is in seconds and provides a keep-alive functionality for the overlay network. The value should be between 10 - 120 sec, and the recommended value is **25** sec.



Network :: Wireguard :: emea :: client

Required

Peer Name: client

Allowed IPs: 172.16.254.2/32, 172.16.10.0/24

Public Key: fJXd0mqxdKELB4E05w9rHU66JJKQMFRz4PWuU2SFMiY=

Optional

KeepAlive: 25

Description:

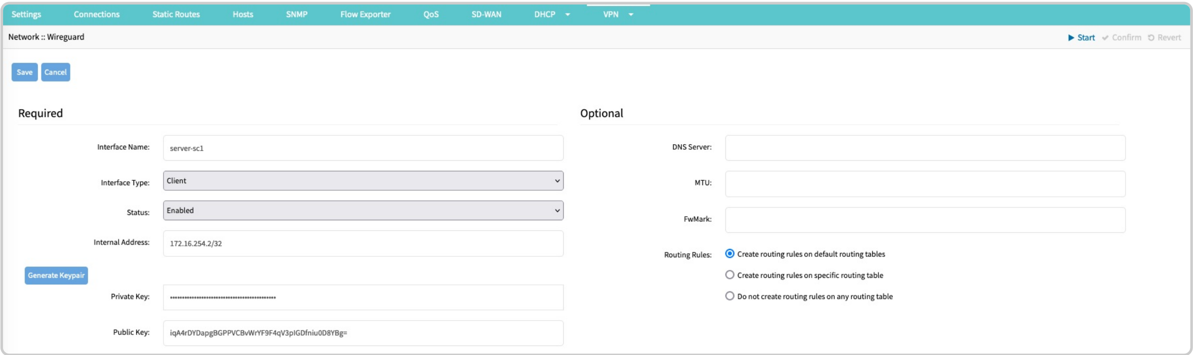
Client-Side Configuration

The following configuration steps are required for each client to take part in the Wireguard VPN/Overlay network.

Client Interface Configuration

To configure a client interface, use the following steps (for a full list of options, look here):

1. Go to **Network** *::* **VPN** *::* **Wireguard**.
2. Click **Add**.
3. Enter an **Interface Name** (*Example: server*-sc1), this name is used for the network interface.
4. On the **Interface Type** drop-down, select one **Client.**



Network :: Wireguard

Required

Interface Name: server-sc1

Interface Type: Client

Status: Enabled

Internal Address: 172.16.254.2/32

Private Key: ••

Public Key: iqA4rDYDapgBGPPVCBvWrYF9F4qV3pIGDfniu0D8YBg=

Optional

DNS Server:

MTU:

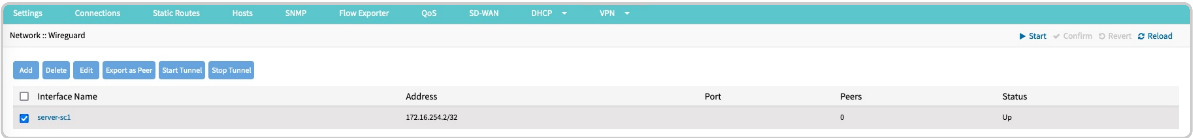
FwMark:

Routing Rules:
● Create routing rules on default routing tables
○ Create routing rules on specific routing table
○ Do not create routing rules on any routing table

5. On the **Status** drop-down, select **Enabled.**
6. Enter an **Internal Address** (*Example: 172.16.254.2/32*); this IP Address is used as an internal IP Address that is assigned to the interface.

> **Internal Address**
>
> **The internal IP address assigned to the Wireguard interface is used for Cluster configuration and BPG and OSP peering configurations.**

7. Click on **Generate Keypair,** to create a new Private/Public RSA key pair. This key pair is used to secure the connection. The Public key is exchanged with the server.
8. Leave other settings on default.
9. The Client configuration can be exported to a file for easy import into the server as a peer.
10. Go to **Network** *::* *VPN* *::* **Wireguard**.



Network :: Wireguard

☐ Interface Name	Address	Port	Peers	Status
☑ server-sc1	172.16.254.2/32		0	Up

11. Select the Interface Name
12. Click **Export Peer**.
13. The file is downloaded to the local download location.

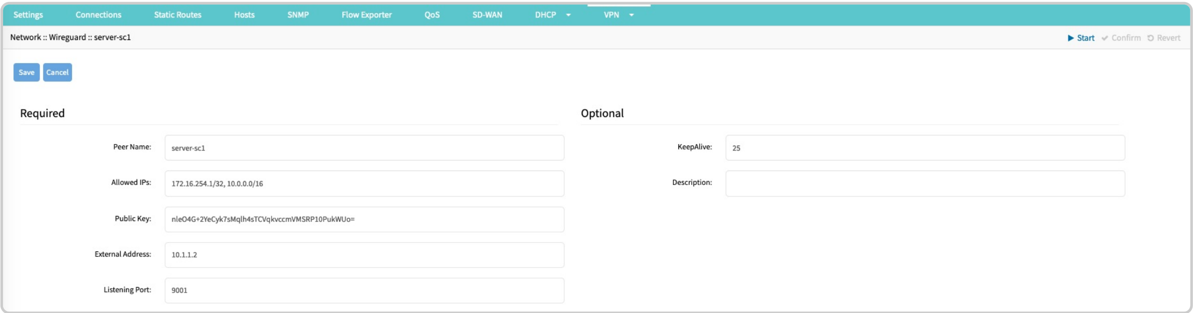
Server (Peer) Configuration

Wireguard's security is based on a mutually trusted RSA Keypair exchange, which requires exchanging public key information in both directions. This means that every client must be specifically allowed and trusted on the server.

Manual Server (Peer) Configuration

To allow a client/peer to connect to the server, create a peer using the following steps (for a full list of options, look here):

1. Go to *Network :: VPN drop-down :: Wireguard*
2. Click on the **Client Interface** (*Example: **server-sc1***) configuration that was created in the previous step
3. Click on **Add** (opens dialog).



Network :: Wireguard :: server-sc1

Required

Peer Name: server-sc1

Allowed IPs: 172.16.254.1/32, 10.0.0.0/16

Public Key: nleO4G+2YeCyk7sMqlh4sTCVqkvccmVMSRP10PukWUo=

External Address: 10.1.1.2

Listening Port: 9001

Optional

KeepAlive: 25

Description:

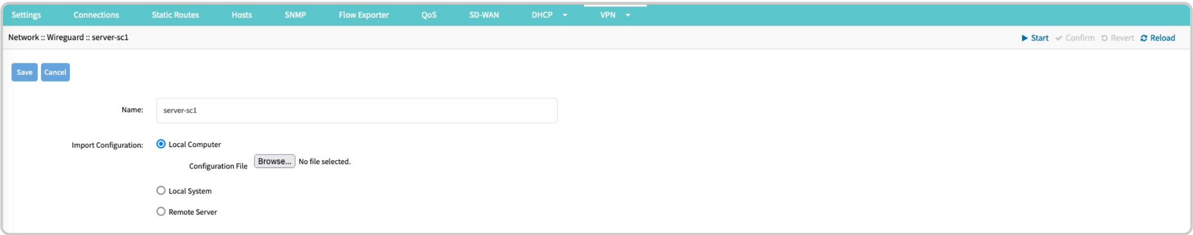
4. Enter a **Peer Name** (*Example: **server-sc1***); this name is used to identify the server and must be a string without spaces or special characters.
5. Provide a list of **Allowed IP** addresses or ranges (*Example: **172.16.254.1/32,10.0.0.0/16***). This list is used in the default configuration to create the required routing information. For Host-to-Host communication, the list should contain only the internal IP address of the server. For site-to-site configurations, it should contain the remote IP network range.
6. Provide the client **Public Key,** which was created during the server-side setup.
7. Provide the Public IP or FQDN of the server as an **External Address** (*Example: **10.1.1.2***)
8. Provide the UDP **Listening Port** (*Example: **9001***) on which the server is reachable.
9. It is recommended that a **KeepAlive** value of **25** is provided. The value is in seconds and provides a keep-alive functionality for the overlay network.

> **KeepAlive and Handshake**
>
> Wireguard uses a " Handshakes " concept, similar to heartbeats. Handshakes are renewed every 2 minutes but are passive. This means handshakes are not proactively exchanged; for this, the KeepAlive feature is used. If no handshake is available or older than 2 minutes, this indicates a connection issue.
> For this reason, it is recommended always to define a KeepAlive value.

10. Option: Provide a **Description** for the Client; this is a free text field that supports spaces and special characters

Import Peer from Server Export File

1. Go to *Network :: VPN drop-down :: Wireguard*
2. Click on the Client Interface (***Example: server-sc1***) configuration that was created in the previous step.
3. Click **Import Peer** (displays dialog).
4. Enter a Peer **Name**; this name is used to identify the client and must be a string without spaces or special characters.
5. Provide the file location, which can be located locally (**Local System**) on the server, on a workstation (**Local Computer**), or a **Remote Server.**



Network :: Wireguard :: server-sc1

Name: server-sc1

Import Configuration: ● Local Computer

Configuration File No file selected.

○ Local System

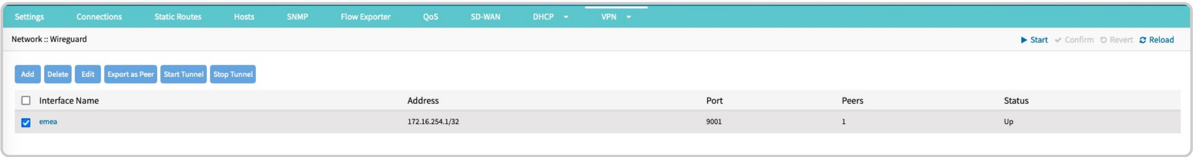
○ Remote Server

6. Click **Save**.
7. After the Peer was imported, click on the newly created ***peer*** *(Example: server-sc1)*
   - Update the **Allowed IP** *(Example: 172.16.254.1/32, 10.0.0.0/16)* configuration and include the client's network range
   - Validate the **KeepAlive** setting. The value is in seconds and provides a keep-alive functionality for the overlay network. The value should be between 10 - 120 sec, and the recommended value is **25** sec.

Appendix

Start Tunnel

1. Go to **Network** :: **VPN** :: **Wireguard**.
2. On the table, select the interface.



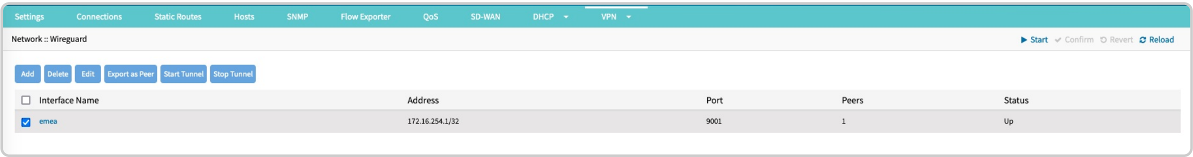
Network :: Wireguard

□ Interface Name	Address	Port	Peers	Status
☑ emea	172.16.254.1/32	9001	1	Up

3. Click **Start Tunnel** (Post Up)

Stop Tunnel

1. Go to **Network** :: **VPN** :: **Wireguard**.
2. On the table, select the interface.



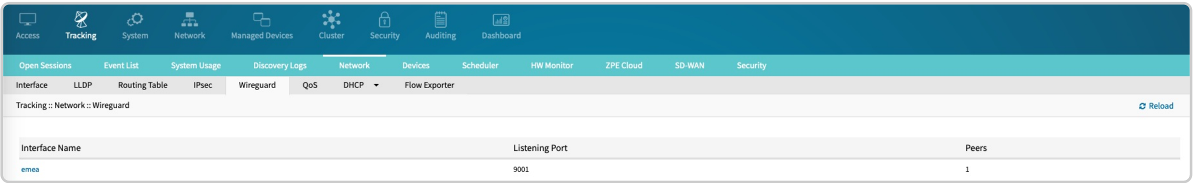
Network :: Wireguard

□ Interface Name	Address	Port	Peers	Status
☑ emea	172.16.254.1/32	9001	1	Up

3. Click **Stop Tunnel** (Post Down).

Tunnel Status

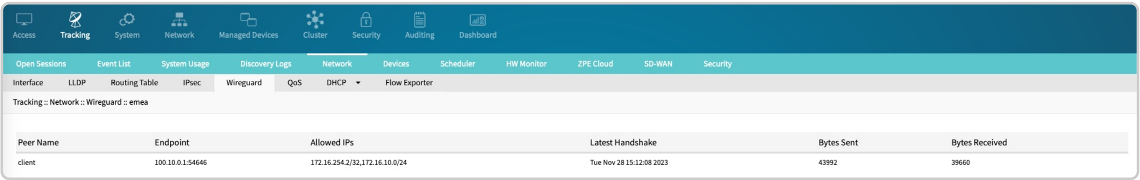
1. Go to Tracking *:: Network :: Wireguard.*



Tracking :: Network :: Wireguard

Interface Name	Listening Port	Peers
emea	9001	1

2. To review peer details and identify the overlay status, click on the interface name to drill down to the peer details.
   The table will identify:
   a. The **Peer Name**
   b. Current **End Point** (public IP address and port number) details. This information can dynamically change, depending on roaming information provided by the peer/client
   c. The latest **Handshake** timestamp. If this is older than 2 minutes or blank, this indicates an issue with the connection; if it was recently updated, is the tunnel up and working
   d. **Bytes Sent**
   e. **Bytes Received**



Tracking :: Network :: Wireguard :: emea

Peer Name	Endpoint	Allowed IPs	Latest Handshake	Bytes Sent	Bytes Received
client	100.10.0.1:54646	172.16.254.2/32,172.16.10.0/24	Tue Nov 28 15:12:08 2023	43992	39660

Full List of Server Interface Options

Setting	Value	Comment
Interface Name	network interface name	interface name must be string without spaces or special characters
Interface Type	Options: • Server (Default) • Client • Mesh	
Status	Options: • Enabled • Disabled	
Internal Address	<IP Address>/<Bit Mask>	IP Address (IPv4 or IPv6) that is assigned to the network interface
Listening Port	UDP port on which the server is listening for incoming connections	Only required for Server configuration
Private Key	Private Key	Users can either auto-generate a Private/Public keypair, by using the "Generate Keypair" option (recommended), or manually provide a Private Key
Public Key	Public Key	Users can either auto-generate a Private/Public keypair, by using the "Generate Keypair" option (recommended), or manually provide a Public Key
External Address	Optional: Public IP address	This setting is only used for Client configuration exports. It is used to simplify the Client Configuration
MTU	<MTU size>	
FwMark	<FwMark>	This is an advanced option that allows tagging of all traffic in the kernel with a specified FwMark. This can be used for advanced firewall or traffic steering options.
Routing Rules	Options: • Create routing rules on default routing tables • Create routing rules on the specific routing table • Do not create routing rules on any routing table	

Full List of Peer Options

Settings	Value	Comment
Peer Name	<Peer Name>	The wireguard name used to identify the peer *must be* a string without spaces or special characters
Allowed IPs	<List of IP's and IP Ranges>	Comma-separated list of IP addresses or IP networks, which are allowed to arrive from this peer or to be sent to the peer. In the default configuration, based on this list are the appropriate routing entries created
Public Key	<Public Key>	Public key from the client/peer
KeepAlive	keep alive interval in seconds (recommended value 25)	
description	description	Description
External Address	<IP or FQDN>	Only Available on Client connections
Listening Port	<PORT>	Only Available on Client connections

CLI Commands

1. Add the Wireguard interface configuration details, and apply these commands:

None Copy

```
[admin@nodegrid /]# cd /settings/wireguard/
[admin@nodegrid {wireguard}]# set
   interface_name=
   listening_port=
   public_key=
   external_address=
   interface_type=
   mtu=
   routing_rules=
   fwmark=
   internal_address=
   private_key=
   status=
[admin@nodegrid {wireguard}]# commit
```

2. Configure peers/clients:

None Copy

```
[admin@nodegrid wireguard]# cd Interface_Name/
[admin@nodegrid Server_Interface]# cd peers/
[admin@nodegrid peers]# add
[admin@nodegrid {peers}]# set
   allowed_ips=
   keepalive=
   peer_name=
   external_address=
   listening_port=
   public_key=
[admin@nodegrid {peers}]# commit
```

Failover

Wireguard natively supports roaming; this means a client can dynamically update its end-point information and inform the server about the updated details. This allows Nodegrid Clients to be connected to carrier-grade NAT connections and a wide range of other standard WAN connections. The Wireguard tunnel will also automatically follow the Nodegrid's Failover configuration without any additional configuration.

Challenges arise in situations where both end-point details change at the same time. This can happen in examples where, under normal circumstances, the overlay network uses the internal LAN to connect to the server but must switch to the server's public end-point address in case the LAN network has an outage or the server is not reachable for other reasons over the LAN.

The following script allows Nodeghrid to update the Endpoint Addresses dynamically in these situations. The example script provides an example script for a single tunnel, but can easily expanded for multiple tunnels by duplicating the Tunnel section.

Installation of Failover script file

> **Wireguard Tunnel Must Exist**
>
> It is assumed that the Wireguard tunnel was already configured and is working.

> *Network Failover Events 144 and 145*
>
> *The script specifically uses Nodegrid Events 144 and 145, triggered in case of a Network Failover. The script can also be used with other Events, but the appropriate checks must be adopted. in the script*

1. Open a console connection with the admin user
2. Enter into the root shell.

   Bash Copy

   ```bash
   shell sudo su -
   ```

3. Lookup the required details with wg show:

   Bash Copy

   ```bash
   interface: server-sc1
     public key: iqA4rDYDapgBGPPVCBvWrYF9F4qV3pIGDfniu0D8YBg=
     private key: (hidden)
     listening port: 54646

   peer: nleO4G+2YeCyk7sMqlh4sTCVqkvccmVMSRP10PukWUo=
     endpoint: 203.0.13.1:9001
     allowed ips: 172.16.254.1/32, 10.0.0.0/16
     latest handshake: 4 seconds ago
     transfer: 780 B received, 1.23 KiB sent
     persistent keepalive: every 25 seconds
   ```

4. Navigate to:

   Bash Copy

   ```bash
   cd /etc/scripts/auditing
   ```

5. create the script file *wireguard-failover.sh.*

   Bash Copy

   ```bash
   vi wireguard-failover.sh
   ```

6. copy the content into the file and adjust the following parameters:
   a. **tunnel_interface_1_name** = Tunnel Interface Name as provided in the WebUI
   b. **tunnel_interface_1_peer** = Peer Identifier, this is equal to the public key of the peer
   c. **tunnel_interface_1_endpoint** = Normal Endpoint IP address and port in the format of <IP Address>:<PORT Number>, i.e. 10.10.1.1:9001
   d. **tunnel_interface_1_backup**= Backup Endpoint IP address and port in the format of <IP Address>:<PORT Number>, i.e. 100.0.0.1:9001

Bash Copy

```bash
#!/bin/bash

# This script is meant to dynamically change a wireguard endpoint
# Whenever an event ocurrs, it will execute this script passing the Event
# number as the first argument plus all the arguments that this events
# pass to SNMP TRAP. See Nodegrid-TRAP-MIB.mib to see all args for each event.

EVENT_NUMBER="$1" #argument 1 is always the event number
LOG_FILE=/var/log/messages
DELAY=1

###### Tunnel 1 #######
# Dplicate the whole section for any additional Tunnel
tunnel_interface_1_name=<Interface Name>
tunnel_interface_1_peer=<Peer Name>
tunnel_interface_1_endpoint=<Interface Primary Endpoint ip:port>
tunnel_interface_1_backup=<Interface Backup Endpoint ip:port>

if [ ${EVENT_NUMBER} -eq 144 ]; then
  sleep ${DELAY}
  wg set ${tunnel_interface_1_name} peer ${tunnel_interface_1_peer}  endpoint ${tunnel_interface_1_backup}
  echo "Changed Wireguard Tunnel ${tunnel_interface_1_name} peer ${tunnel_interface_1_peer}  to endpoint ${tunnel_interface_1_backup}" >> ${LOG_FILE}
fi

if [ ${EVENT_NUMBER} -eq 145 ]; then
  sleep ${DELAY}
  wg set ${tunnel_interface_1_name} peer ${tunnel_interface_1_peer} endpoint ${tunnel_interface_1_endpoint}
  echo "Changed Wireguard Tunnel ${tunnel_interface_1_name} peer ${tunnel_interface_1_peer}  to endpoint ${tunnel_interface_1_endpoint}" >> ${LOG_FILE}
fi
### END Tunnel 1 ####
```

Example:

Bash Copy

```bash
#!/bin/bash

# This script is meant to dynamically change a wireguard endpoint
# Whenever an event ocurrs, it will execute this script passing the Event
# number as the first argument plus all the arguments that this events
# pass to SNMP TRAP. See Nodegrid-TRAP-MIB.mib to see all args for each event.

EVENT_NUMBER="$1" #argument 1 is always the event number
LOG_FILE=/var/log/messages
DELAY=1

tunnel_interface_1_name=server-sc1
tunnel_interface_1_peer=nleO4G+2YeCyk7sMqlh4sTCVqkvccmVMSRP10PukWUo=
tunnel_interface_1_endpoint=10.1.1.2:9001
tunnel_interface_1_backup=203.0.13.1:9001

if [ ${EVENT_NUMBER} -eq 144 ]; then
  sleep ${DELAY}
  wg set ${tunnel_interface_1_name} peer ${tunnel_interface_1_peer}  endpoint ${tunnel_interface_1_backup}
  echo "Changed Wireguard Tunnel ${tunnel_interface_1_name} peer ${tunnel_interface_1_peer}  to endpoint ${tunnel_interface_1_backup}" >> ${LOG_FILE}
fi

if [ ${EVENT_NUMBER} -eq 145 ]; then
  sleep ${DELAY}
  wg set ${tunnel_interface_1_name} peer ${tunnel_interface_1_peer} endpoint ${tunnel_interface_1_endpoint}
  echo "Changed Wireguard Tunnel ${tunnel_interface_1_name} peer ${tunnel_interface_1_peer}  to endpoint ${tunnel_interface_1_endpoint}" >> ${LOG_FILE}
fi
```

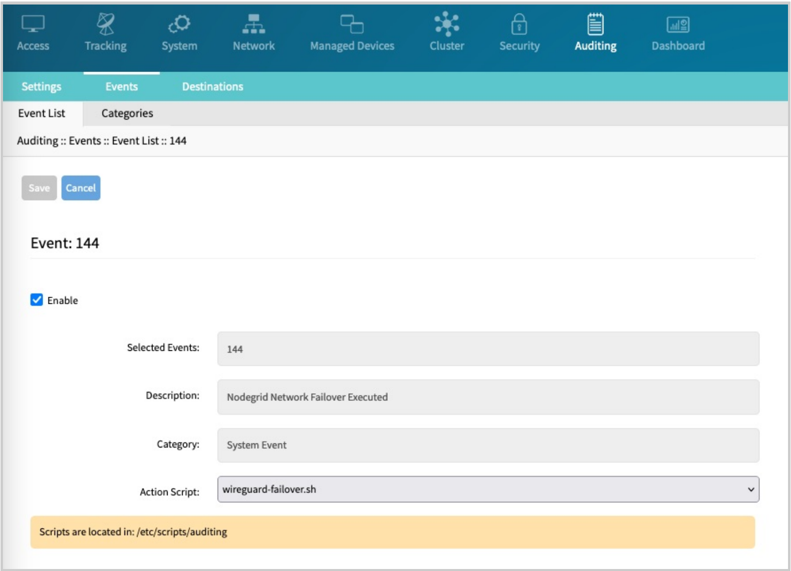
save the file with `:wq`.make the file executable.

Shell

Bash Copy

```bash
chmod +x /etc/scripts/auditing/wireguard-failover.sh
```

7. Assign script file to Events 144 and 145
    a. Open a WebUI and Navigate to **Auditing :: Events :: Event List.**
    b. Navigate to Event **144.**
    c. Click the Event ID.
    d. Assign the script to the Event ID.



Auditing :: Events :: Event List :: 144

Event: 144

☑ Enable

Selected Events: 144

Description: Nodegrid Network Failover Executed

Category: System Event

Action Script: wireguard-failover.sh

Scripts are located in: /etc/scripts/auditing

8. Repeat with Event **145.**

VPN :: IPsec tab

The Nodegrid solution supports the IPsec tunnel configuration with a variety of options for host-to-host, host-to-site, site-to-site and road warrior settings.

The Nodegrid node is directly exposed to the Internet. It is strongly recommended the device be secured. Built-in features include:

- Firewall configuration.
- Enable Fail-2-Ban.
- Change all default passwords with strong passwords.
- Disable services that are not required.

Overview

Authentication Methods

Multiple authentication methods are available. Some are simple (Pre-Shared keys and RSA keys) but with limited flexibility. Others require more initial configuration and setup which offers flexibility and consistency.

Pre-shared Keys

Pre-shared Keys provide the simplest and least secure method to secure an IPsec connection. This is a combination of characters that represent a secret. Both nodes must share the same secret. Nodegrid supports pre-shared keys with a minimum length of 32 characters. The maximum length is much higher. Due to compatibility reasons with other vendors, Nodegrid uses a 64-bit length for the examples. The longer the pre-shared key is, the more secure it is.

RSA Keys

RSA Keys or Raw RSA keys are commonly used for static configurations between single or a few hosts. The nodes are manually configured with each other's RSA keys.

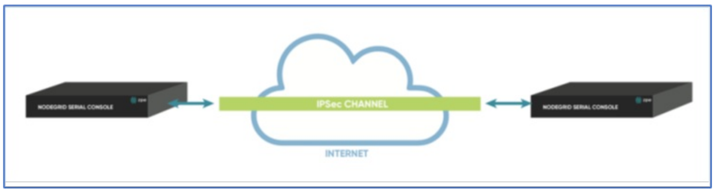
X.509 Certificates

Typically, X.509 Certificate authentications are used for larger deployments with a few to many nodes. The RSA keys of the individual nodes are signed by a central Certificate Authority (CA). The Certificate Authority maintains the trust relationship between the nodes. As needed, specific nodes can include revocation of trust. Nodegrid supports both public and private CA's. As needed, the Nodegrid Platform can host and manage its own Certificate Authority for IPsec communication.

Connection Scenarios

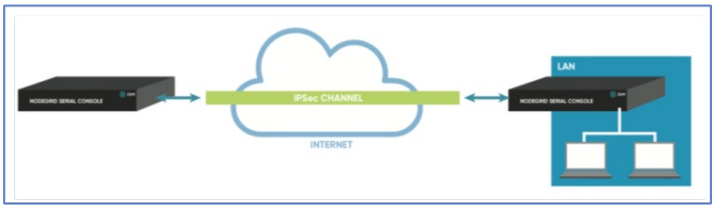
IPsec supports many connection scenarios, from the basic one-to-one nodes and the more complex one-to-many nodes. Communication can be limited to the directly involved nodes. If needed, communication can be expanded to the networks access table behind the nodes. Examples are provided for some of the most common scenarios.

Host-to-Host



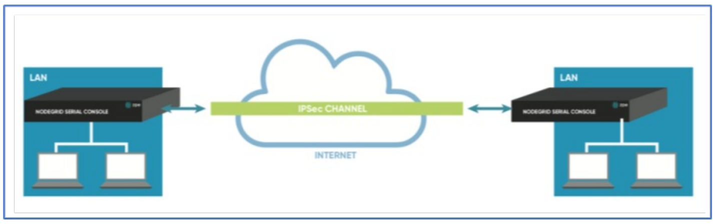
Host-to-Host communication is two nodes directly connected with a VPN tunnel. The communication is limited to direct communication between them. None of the packages are routed or forwarded. This is a point-to-point communication tunnel between two nodes.

Host-to-Site



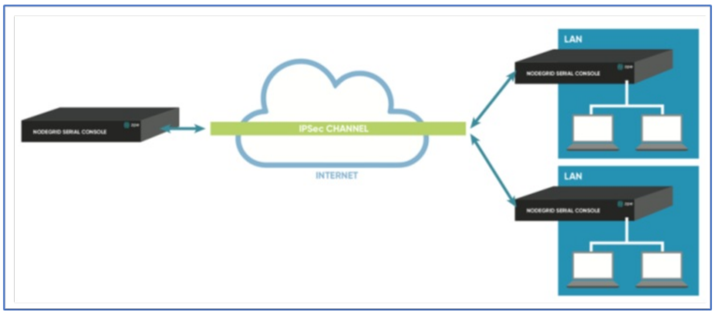
With host-to-Site, one node establishes a VPN tunnel to a second node. Communication is limited on one site to the specific node; and on the other side, limited to all devices in a range of subnet accessible by the second node.

Site-to-Site



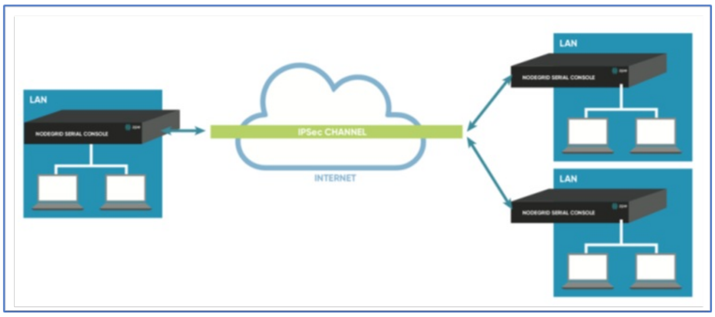
In site-to-site, the tunnel is established between two nodes. Communication can specify the subnet on both sides. This allows communication between devices on either side of the connection.

Host-to-Multi-Site



Host-to-multi-site communication is created with individual VPN connections. This is done between hosts or with specific multi-site configurations (which greatly improves scalability). Multiple nodes can connect to the same node. A typical use would be remote offices with a VPN connection to the main office. This would limit communications to the one node and devices on specified subnets in the remote locations.

Site-to-Multi-Site



Site-to-multi-site is most common for enterprise VPN setups. Similar to host-to-multi-site, communication is allowed to the specific subnet on either side. The West node would have access to all specified subnet on any of the sites. The remote sites only can access the subnet exposed by the West node.

Keys and Certificates

Keys and Certificates

	Host to Host	Host to Site	Site to Site	Host to Multi-Site	Site to Multi-Host
Pre-shared Keys	Possible	Possible	Possible	Possible	Possible
RSA Key	Recommended	Recommended	Recommended	Possible	Possible
X.509 Certificates	Recommended	Recommended	Recommended	Recommended	Recommended

IPsec Configuration Process

These are the general configuration steps to configure the desired connection.

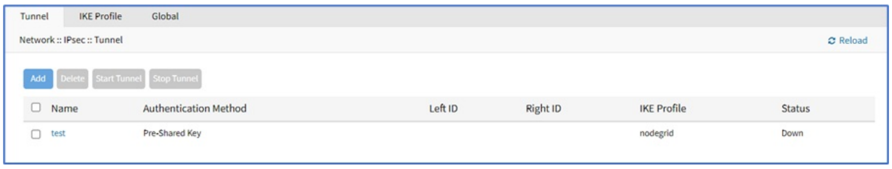
1. To prepare the Nodegrid, see How to Prepare a Nodegrid Node for IPsec
2. Ensure that one of the authentication methods is prepared:
   - How to create Pre-shared Keys for IPsec
   - How to create RSA Keys for IPsec
   - How to Create Certificates for IPsec

     > **NOTE**
     >
     > For Production environments, it is recommended to use RSA Keys or Certificate Authentication. For a test environment, Pre-Shared Keys are easy to set up.
3. Create an IPsec configuration file. Configuration examples can be found here:
   - **Pre-Shared Keys**
     - How to Configure IPsec Host to Host Tunnel with Pre-Shared Key
     - How to configure IPsec Host to Site tunnel with Pre-Shared Key
     - How to Configure IPsec Site to Site Tunnel with Pre-Shared Key
   - **RSA Keys**
     - How to Configure IPsec Host to Host Tunnel with RSA Keys
     - How to Configure IPsec Host to Site tunnel with RSA Keys
     - How to Configure IPsec Site to Site Tunnel with RSA Keys
   - **Certificates**
     - How to Configure IPsec Host to Host Tunnel with Certificate
     - How to Configure IPsec Host to Site Tunnel with Certificate
     - How to Configure IPsec Site to Site Tunnel with Certificate
4. As required, distribute and exchange configuration files and keys to all nodes
5. Test the connection.

For more detailed guides on how to use IPsec with the Nodegrid Platform, visit the Knowledge Base.

Tunnel sub-tab

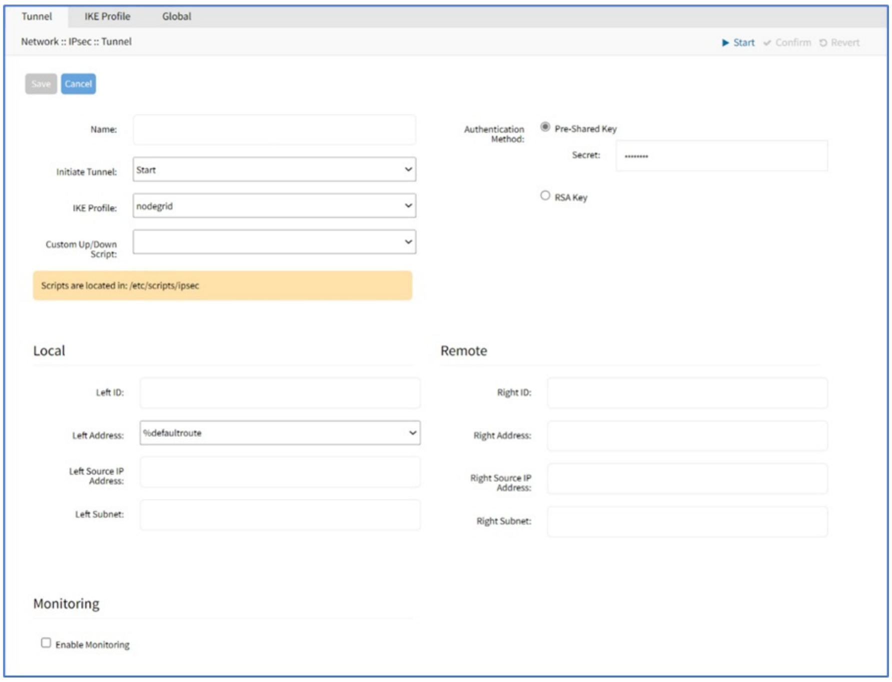
The main table displays available tunnels.



	Name	Authentication Method	Left ID	Right ID	IKE Profile	Status
□	test	Pre-Shared Key			nodegrid	Down

Add New Tunnel

1. Go to *Network :: VPN drop-down :: IPsec :: Tunnel*.
2. Click **Add** (displays dialog).



Name:

Initiate Tunnel: Start

IKE Profile: nodegrid

Custom Up/Down Script:

Scripts are located in: /etc/scripts/ipsec

Authentication Method: ● Pre-Shared Key

Secret: ••••••••

○ RSA Key

Local

Left ID:

Left Address: %defaultroute

Left Source IP Address:

Left Subnet:

Remote

Right ID:

Right Address:

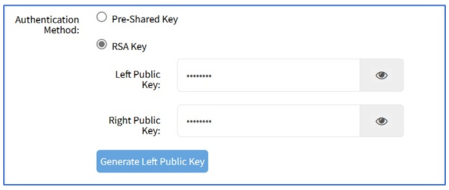
Right Source IP Address:

Right Subnet:

Monitoring

□ Enable Monitoring

3. Enter **Name.**
4. On **Initiate Tunnel** drop-down, select one (Start, Ignore, On-Demand)
5. On **IKE Profile** drop-down, select one (Cisco_ASA, PaloAlto, nodegrid)
6. (optional) On **Custom Up/Down Script** drop-down, select one (this customized script can set configuration changes and activities, when the tunnel is up or down).
7. In *Authentication Method* menu, select either of the following options.
   a. **Pre-Shared Key** radio button (expands dialog). Enter **Secret**.
   b. **RSA Key** radio button (expands dialog):



Authentication Method: ○ Pre-Shared Key

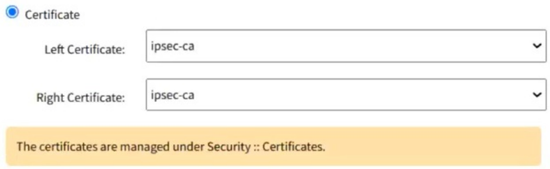
● RSA Key

Left Public Key: ••••••••

Right Public Key: ••••••••

- **Left Public Key**
- **Right Public Key**
- **Generate Left Public Key**

   c. **Certificate:** Allows you to set up a tunnel using certificates as the authentication method. This involves using certificates configured under the **Security** :: **Certificates** page.



● Certificate

Left Certificate: ipsec-ca

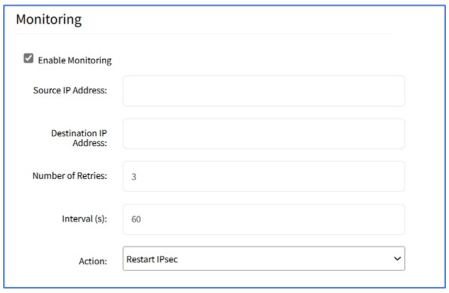
Right Certificate: ipsec-ca

The certificates are managed under Security :: Certificates.

   i. **Left Certificate:** Choose the necessary certificate for the sides that are connected to your tunnel.

ii. **Right Certificate**: Select a value when you intend to establish a side-to-side configuration with up to two nodes. In cases where there are more than two nodes, you should not enter any value into this field.

8. In the *Local* menu, enter:
    a. **Left ID**
    b. **Left Address** drop-down, select one (selection depends on the system configuration)
    c. **Left Source IP Address**
    d. **Left Subnet**
9. In the *Remote* menu, enter:
    a. **Right ID**
    b. **Right Address**
    c. **Right Source IP Address**
    d. **Right Subnet**
10. (optional) In the *Monitoring* menu, select **Enable Monitoring** checkbox (expands dialog).



Monitoring

☑ Enable Monitoring

Source IP Address:

Destination IP Address:

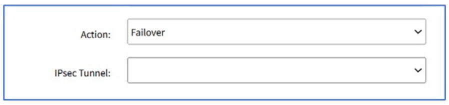
Number of Retries: 3

Interval (s): 60

Action: Restart IPsec

    a. **Source IP Address**(ping from)
        - **Destination IP Address** (ping to)
        - **Number of Retries** (pings before triggering Action)
        - **Interval (seconds)** (time between retries)

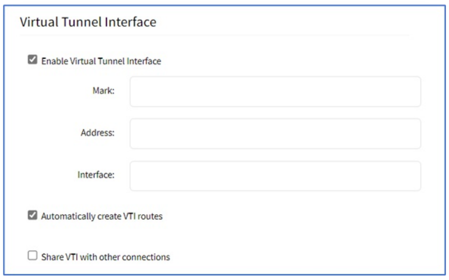
    b. On **Action** drop-down, select one (if the tunnel does not respond):
        - **Restart IPsec** (to resolve issues with key negotiation)
        - **Restart Tunnel** (to resolve issues with key negotiation)
        - **Failover** (fails over to another IPsec tunnel) (expands dialog). On **IPsec Tunnel** drop-down, select one.



Action: Failover

IPsec Tunnel:

11. (optional) In *Virtual Tunnel Interface* menu, select **Enable Virtual Tunnel**



Virtual Tunnel Interface

☑ Enable Virtual Tunnel Interface

Mark:

Address:

Interface:

☑ Automatically create VTI routes

□ Share VTI with other connections

    a. **Interface** checkbox (expands dialog), enter details:
    b. **Mark**
    c. **Address**
    d. **Interface**
    e. **Automatically create VTI routes** checkbox
    f. **Share VTI with other connections** checkbox

12. Click **Save**.

Edit Tunnel

1. Go to *Network :: VPN drop-down :: IPsec :: Tunnel*.
2. In the *Name* column, click a name (displays dialog).
3. Make changes, as needed.
4. Click **Save**.

Delete Tunnel

1. Go to *Network :: VPN drop-down :: IPsec :: Tunnel*.
2. In the table, select checkbox of tunnel to delete.
3. Click **Delete**.

Start Tunnel

1. Go to *Network :: VPN drop-down :: IPsec :: Tunnel*.
2. In the table, select checkbox of tunnel to start.
3. Click **Start Tunnel**.

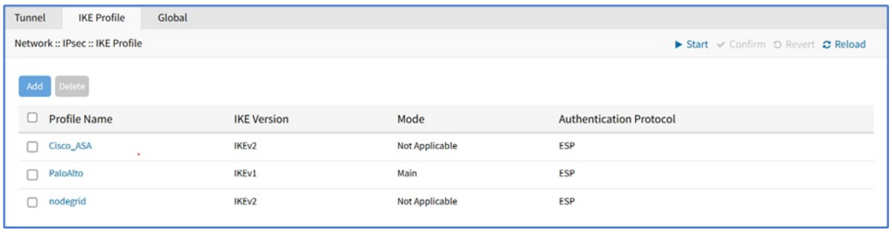
Stop Tunnel

1. Go to *Network :: VPN drop-down :: IPsec :: Tunnel*.

2. In the table, select checkbox of tunnel to stop.
3. Click **Stop Tunnel**.

IKE Profile sub-tab

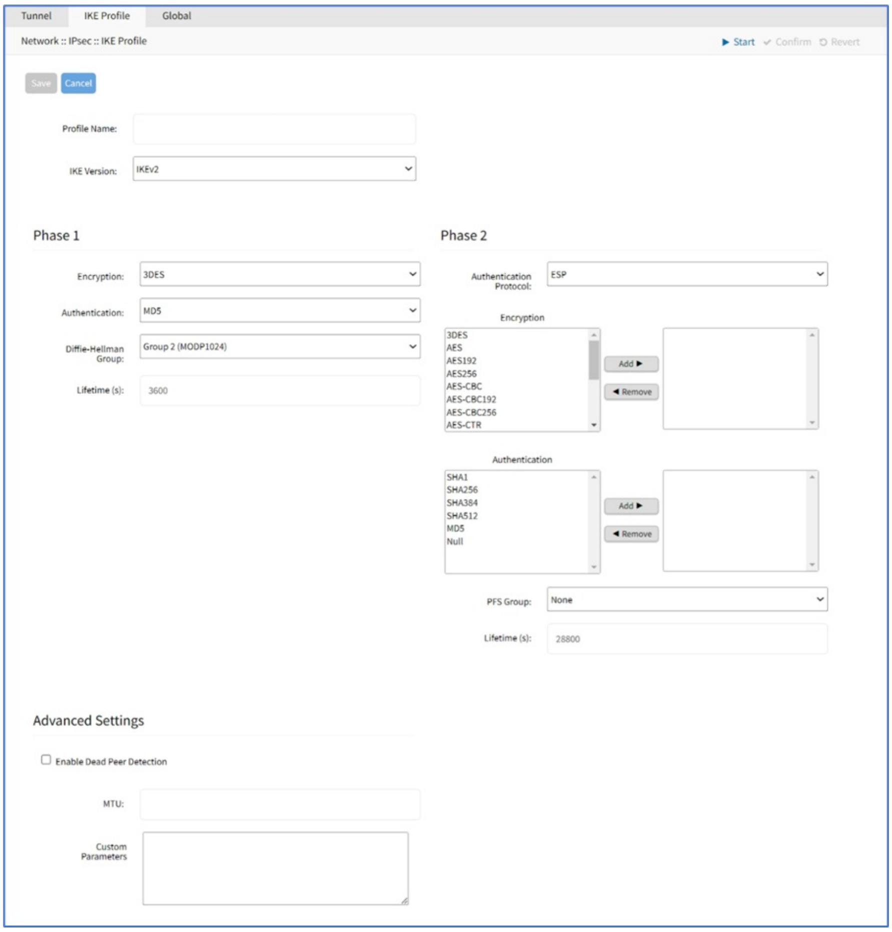
IKE Profiles are managed on this page.



□	Profile Name	IKE Version	Mode	Authentication Protocol
□	Cisco_ASA	IKEv2	Not Applicable	ESP
□	PaloAlto	IKEv1	Main	ESP
□	nodegrid	IKEv2	Not Applicable	ESP

Add New Profile

1. Go to *Network :: VPN drop-down :: IPsec :: IKE Profile*.
2. Click **Add** (displays dialog).



Profile Name:

IKE Version: IKEv2

Phase 1

Encryption: 3DES

Authentication: MD5

Diffie-Hellman Group: Group 2 (MODP1024)

Lifetime (s): 3600

Phase 2

Authentication Protocol: ESP

Encryption: 3DES, AES, AES192, AES256, AES-CBC, AES-CBC192, AES-CBC256, AES-CTR

Authentication: SHA1, SHA256, SHA384, SHA512, MD5, Null

PFS Group: None

Lifetime (s): 28800

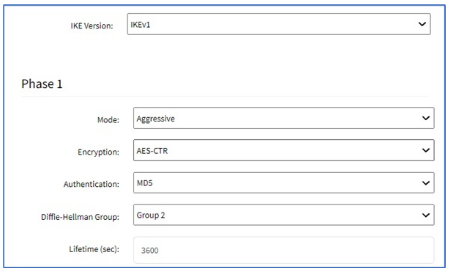
Advanced Settings

□ Enable Dead Peer Detection

MTU:

Custom Parameters

3. Enter **Profile Name**.
4. On **IKE Version** drop-down, select one (IKEv1, IKEv2) (modifies *Phase 1* selection).
   - If IKEv1 selection, on **Mode** drop-down, select one (Aggressive, Main).



IKE Version: IKEv1

Phase 1

Mode: Aggressive

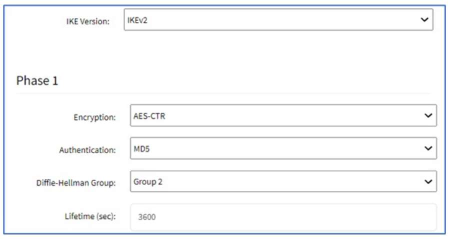
Encryption: AES-CTR

Authentication: MD5

Diffie-Hellman Group: Group 2

Lifetime (sec): 3600

   - If IKEv2 selection:



IKE Version: IKEv2

Phase 1

Encryption: AES-CTR

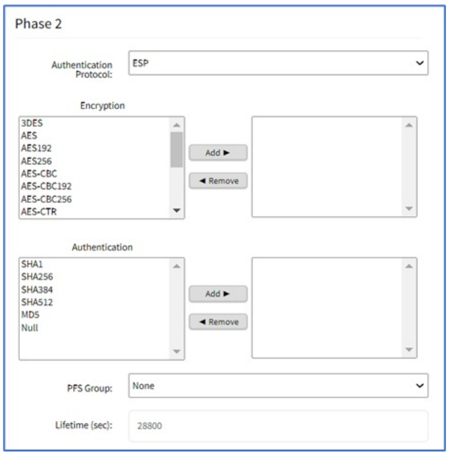
Authentication: MD5

Diffie-Hellman Group: Group 2

Lifetime (sec): 3600

- On **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).
- On **Authentication** drop-down, select one (SHA1, SHA256, SHA384, SHA512, MD5).
- On **Diffie-Hellman Group** drop-down, select one (Group 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 31).
- Enter **Lifetime (sec)** value.

5. *Phase 2* menu, **Authentication Protocol** drop-down, select one (ESP, AH).
   - If ESP selection, On *Encryption*, select from left-side panel, click **Add►** to move to right-side panel. To remove from right-side panel, select, and click **◄Remove**.



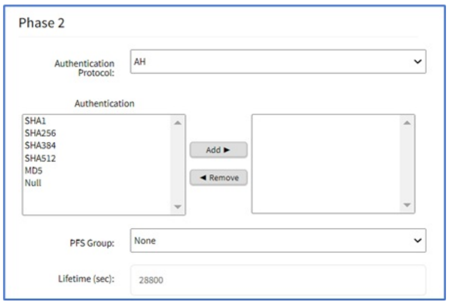
Phase 2

Authentication Protocol: ESP

PFS Group: None

Lifetime (sec): 28800

   - If AH selection, On *Authentication*, select from left-side panel, click **Add►** to move to right-side panel. To remove from right-side panel, select, and click **◄Remove**.



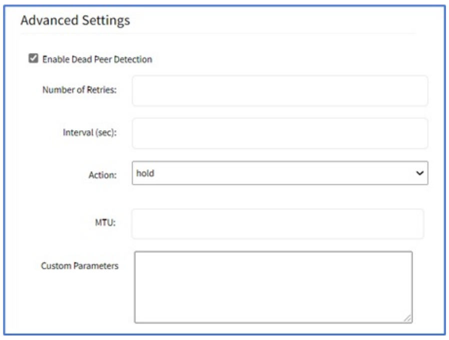
Phase 2

Authentication Protocol: AH

PFS Group: None

Lifetime (sec): 28800

6. On *Advanced Settings* menu, if **Enable Dead Peer Detection** checkbox selected:



Advanced Settings

☑ Enable Dead Peer Detection

Number of Retries:

Interval (sec):

Action: hold

MTU:

Custom Parameters

   a. Select **Enter number of retries** checkbox
   b. Enter **Interval (sec)**
   c. On **Action** drop-down, select one (hold, clear, restart)
   d. Enter **MTU**
   e. Enter **Custom Parameters** (comma separated)

7. Click **Save**.

Edit Profile

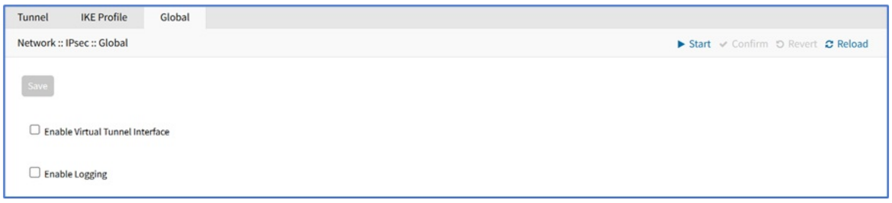
1. Go to *Network :: VPN drop-down :: IPsec :: IKE Profile*.
2. Locate and click on the Profile Name.
3. Modify details, as needed.
4. Click **Save**.

Delete Profile

1. Go to *Network :: VPN drop-down :: IPsec :: IKE Profile*.
2. Click the checkbox next to the profile to delete.
3. Click **Delete**.

Global sub-tab

Global settings are available here.



□ Enable Virtual Tunnel Interface

□ Enable Logging

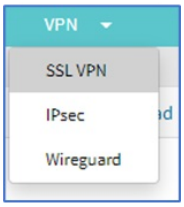
Edit Global Options

1. Go to *Network :: VPN drop-down :: IPsec :: Global*.
    a. Select **Enable Virtual Tunnel Interface** checkbox
    b. Select **Enable Logging** checkbox
2. Click **Save**

.

VPN :: SSL VPN tab

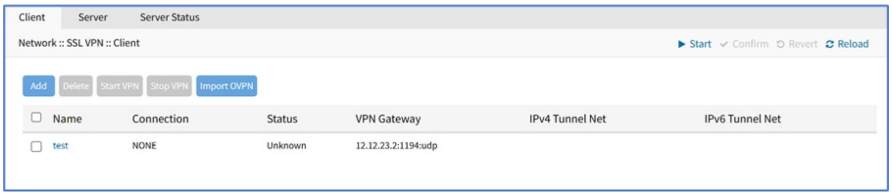
Nodegrid supports a wide variety of SSL configuration options. The System can act as either SSL client or SSL server, as needed by the customer configuration and security requirements.



Client sub-tab

The VPN client configuration settings are generally used for failover scenarios. This is when a main secure connection fails over to a less secure connection type. The VPN tunnel is used to secure traffic. When the Nodegrid device is configured as an VPN client, it is bound to a network interface (optional) and the VPN tunnel is automatically established when the bounded interface starts. Multiple client configurations can be added that support different connection and interface details.

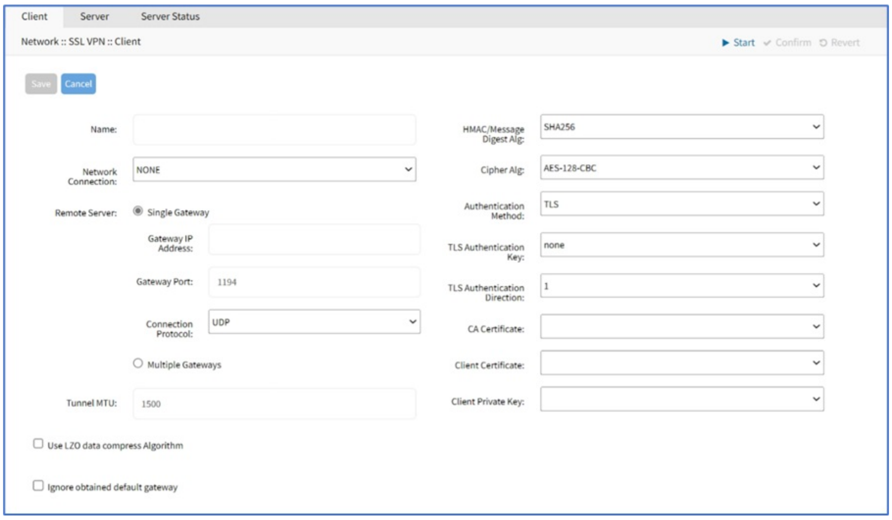
> NOTE
>
> Depending on the configuration, multiple files are required and must be available in the /etc/openvpn/CA folder.



□	Name	Connection	Status	VPN Gateway	IPv4 Tunnel Net	IPv6 Tunnel Net
□	test	NONE	Unknown	12.12.23.2:1194:udp		

Add Client

1. Go to *Network :: VPN drop-down :: SSL VPN :: Client*.
2. Click **Add** (displays dialog).



Name:

Network Connection: NONE

Remote Server: ● Single Gateway

Gateway IP Address:

Gateway Port: 1194

Connection Protocol: UDP

○ Multiple Gateways

Tunnel MTU: 1500

□ Use LZO data compress Algorithm

□ Ignore obtained default gateway

HMAC/Message Digest Alg: SHA256

Cipher Alg: AES-128-CBC

Authentication Method: TLS

TLS Authentication Key: none

TLS Authentication Direction: 1

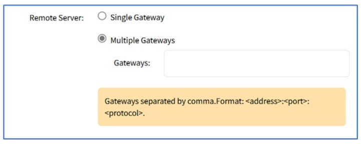
CA Certificate:

Client Certificate:

Client Private Key:

   a. Enter **Name**
   b. On **Network Connection** drop-down, select one (None, ETH0, ETH1, hotspot)

3. In *Remote Server* menu, select one:
   - **Single Gateway**radio button, enter details:
     - **Gateway IP Address**
     - **Gateway Port** (default: 1194)
     - **Connection Protocol** drop-down, select one (UDP, TCP)
   - **Multiple Gateway** radio button (expands dialog)



Remote Server: ○ Single Gateway

● Multiple Gateways

Gateways:

Gateways separated by comma.Format: <address>:<port>:<protocol>.

     - **Gateways** (comma separated).

4. Enter details:
   a. **Tunnel MTU** (MTU size for tunnel interface) (default: 1500)
   b. **Use LZO data compress Algorithm** checkbox
   c. **Ignore obtained default gateway** checkbox
   d. **HMAC/Message Digest Alg** drop-down, select one
   e. **Cipher Alg** drop-down, select one

5. On *Authentication Method* drop-down, select one.
   - **TLS**selection
     - **TLS Authentication Key** drop-down, select one
     - **TLS Authentication Direction** drop-down, select one
     - **CA Certificate** drop-down, select one
     - **Client Certificate** drop-down, select one
     - **Client Private Key** drop-down, select one
   - **Static Key**selection:
     - **Secret** drop-down, select one
     - **Local Endpoint (Local IP)**
     - **Remote Endpoint (Remote IP)**
   - **Password**selection:
     - **Username**
     - **Password**

- **CA Certificate** drop-down, select one.

- **Password plus TLS**selection:
  - **Username**
  - **Password**
  - **TLS Authentication Key** drop-down, select one
  - **TLS Authentication Direction** drop-down, select one
  - **CA Certificate** drop-down, select one
  - **Client Certificate** drop-down, select one
  - **Client Private Key** drop-down, select one

6. Click **Save**.

Edit Client

1. Go to *Network :: VPN drop-down :: SSL VPN :: Client*.
2. On *Subnet/Netmask* column, click a name.
3. Make changes, as needed.
4. Click **Save**.

Delete Client

1. Go to *Network :: VPN drop-down :: SSL VPN :: Client*.
2. Select checkbox to be deleted.
3. Click **Delete**.

Start Client VPN

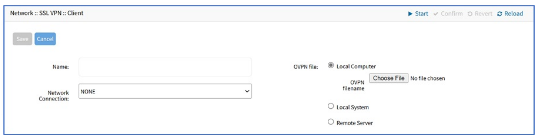
1. Go to *Network :: VPN drop-down :: SSL VPN :: Client*.
2. Select checkbox next to client to be started.
3. Click **Start VPN**.

Stop Client VPN

1. Go to *Network :: VPN drop-down :: SSL VPN :: Client*.
2. Select checkbox next to client to be stopped.
3. Click **Stop VPN**.

Import OVPN

1. Go to *Network :: VPN drop-down :: SSL VPN :: Client*.
2. Click **Import OVPN** (displays dialog).



Network :: SSL VPN :: Client

Name:

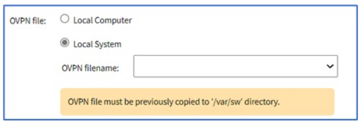
Network Connection: NONE

OVPN file: ● Local Computer ○ Local System ○ Remote Server

OVPN filename: No file chosen

   a. Enter **Name**
   b. On **Network Connection** drop-down, select one (NONE, ETH0, ETH1, hotspot)

3. In *OVPN File* menu, select one
   - **Local Computer** radio button (expands dialog), click **Choose File**. Locate and select the file.
   - **Local System** radio button (expands dialog). On **OVPN filename** drop-down, select one.

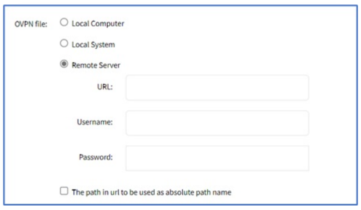


OVPN file: ○ Local Computer ● Local System

OVPN filename:

OVPN file must be previously copied to '/var/sw' directory.

   - **Remote Server** radio button (expands dialog), enter details:



OVPN file: ○ Local Computer ○ Local System ● Remote Server

URL:

Username:

Password:

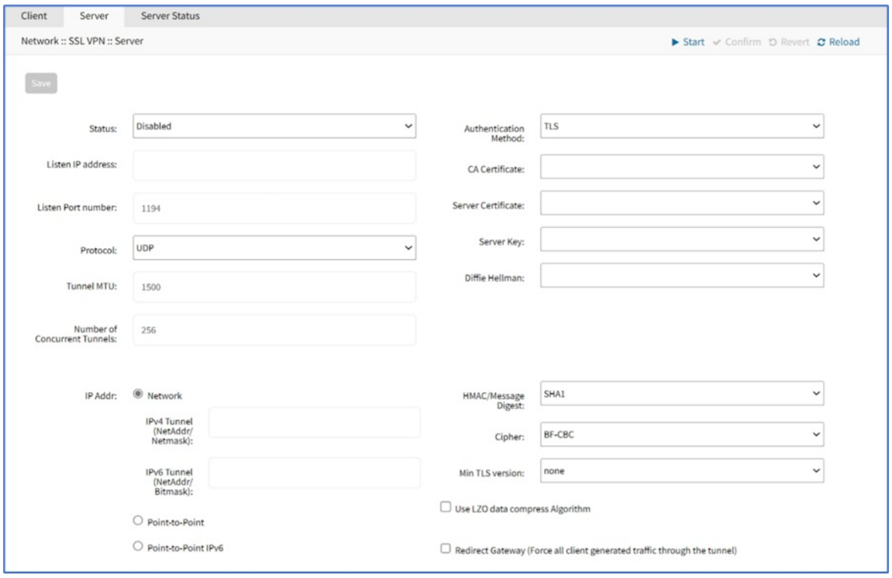
□ The path in url to be used as absolute path name

Enter **URL** (URL can be the IP address or hostname/FQDN. If using IPv6, use brackets [...]. Supported protocols: FTP, TFTP, SFTP, and SCP.)
Enter **Username** and **Password**
(optional) Select **The path in url to be used as absolute path name** checkbox.

4. Click **Save**.

Server sub-tab

Nodegrid can be configured as a VPN server. By default, this is disabled. Depending on the configuration, multiple files are required and must be available in the /etc/openvpn/CA folder.



Network :: SSL VPN :: Server

Status: Disabled

Listen IP address:

Listen Port number: 1194

Protocol: UDP

Tunnel MTU: 1500

Number of Concurrent Tunnels: 256

IP Addr: ● Network

IPv4 Tunnel (NetAddr/Netmask):

IPv6 Tunnel (NetAddr/Bitmask):

○ Point-to-Point

○ Point-to-Point IPv6

Authentication Method: TLS

CA Certificate:

Server Certificate:

Server Key:

Diffie Hellman:

HMAC/Message Digest: SHA1

Cipher: BF-CBC

Min TLS version: none

□ Use LZO data compress Algorithm

□ Redirect Gateway (Force all client generated traffic through the tunnel)

Configure SSL VPN Server Details

1. Go to *Network :: VPN drop-down :: VPN :: Server*.
2. On **Status** drop-down, select one (after configuration as a VPN server, must be enabled).
   - **Enabled**
   - **Disabled** (default)
3. Enter details:
   a. **Listen IP address** (if defined, server only responds to client requests coming in this interface)
   b. **Listen Port number** (listening port for incoming connections - default: 1194)
   c. **Protocol** drop-down, select one (UDP, TCP, UDP IPv6, TCP IPv6)
   d. **Tunnel MTU** (default: 1500)
   e. **Number of Concurrent Tunnels** (default: 256)
4. On *Authentication Method* menu, enter details (different fields are displayed according to selection).
   a. **TLS**selection:
      - **CA Certificate** drop-down, select one
      - **Server Certificate** drop-down, select one
      - **Server Key** drop-down, select one
      - **Diffie Hellman** drop-down, select one

   b. **Static Key**selection:
      - **Secret** drop-down, select one
      - **Diffie Hellman** drop-down, select one

   c. **Password**selection:
      - **CA Certificate** drop-down, select one
      - **Server Certificate** drop-down, select one
      - **Server Key** drop-down, select one
      - **Diffie Hellman** drop-down, select one

   d. **Password plus TLS**selection:
      - **CA Certificate** drop-down, select one
      - **Server Certificate** drop-down, select one
      - **Server Key** drop-down, select one
      - **Diffie Hellman** drop-down, select one
5. On *IP Address* menu (display changes based on selection) this configures IP address settings for the tunnel:
   a. **Network**radio button:
      - **IPv4 Tunnel** (NetAddr/Netmask)
      - **IPv6 Tunnel** (NetAddr/Netmask)

   b. **Point to Point**radio button:
      - **Local Endpoint** (Local IP)
      - **Remote Endpoint** (Remote IP)

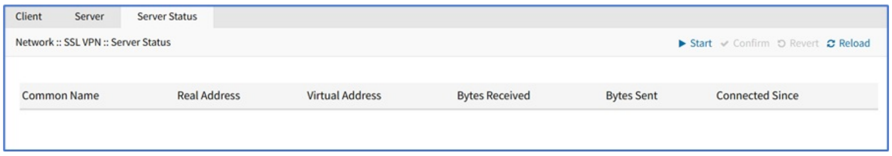
   c. **Point To Point IPv6**radio button:
      - **Local Endpoint** (Local IPv6)
      - **Remote Endpoint** (Remote IPv6)
6. Enter details:
   a. **HMAC/Message Digest** drop-down (select HMAC connection algorithm)
   b. **Cipher** drop-down (select connection cipher algorithm)
   c. **Min TLS version** drop-down, select one (None, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3)
   d. **Use LZO data compress Algorithm** checkbox (all tunnel traffic is compressed)
   e. **Redirect Gateway (Force all client generated traffic through the tunnel)** checkbox (all traffic from client is forced through the tunnel).
7. Click **Save**.

Edit VPN Server Details

1. Go to *Network :: VPN drop-down :: VPN :: Server*.
2. Make modifications, as needed.
3. Click **Save**.

Server Status sub-tab

When the device is configured and started as a VPN server, this page provides an overview of the general server status and connected clients.



Common Name	Real Address	Virtual Address	Bytes Received	Bytes Sent	Connected Since

Setting Up SSL VPN on Nodegrid

This section provides detailed instructions to set up SSL VPN on Nodegrid, enabling secure remote access. Follow the steps below to generate the required certificates and configure the VPN server and client.

- Configuring Nodegrid as a VPN server
- Configuring Nodegrid as a VPN Client
- Testing the VPN Connection
- Checking the server Status

Configuring Nodegrid as a VPN Server

Pre-requisites

Before you begin configuring a VPN using SSL, ensure that you meet the following pre-requisites:

- You have the requiered certificates (CA, Client, and server)
- Place the CA, Server, and Client certificates in the correct location
  - Copy the required files to the following location on the server: */etc/openvpn/CA/*
  - In the case of TLS authentication, copy the **tls-auth.key** file to the ***/etc/openvpn/CA/*** location
    - Copy the ***ca.crt*** file to the Nodegrid client:

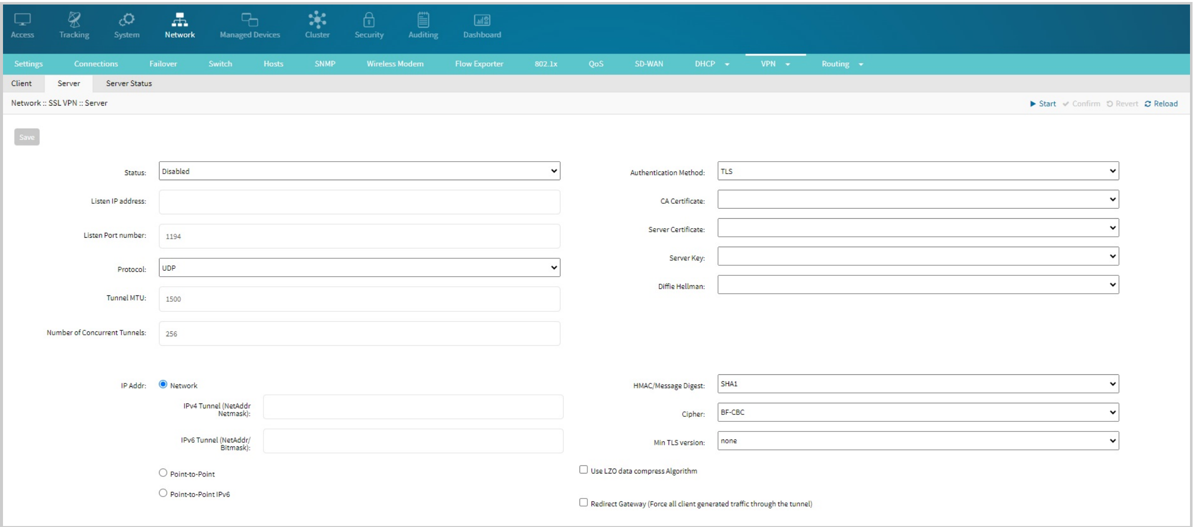
ActionScript Copy

```
scp keys/ca.crt admin@192.168.1.2
```

Configuring Nodegrid as a VPN Server

Once you have the required server certificates placed in the */etc/openvpn/CA/* /location, perform the following actions to configure Nodegrid as a VPN server:

1. Login to the Nodegrid Web UI.
2. Go to *Network :: SSL* VPN.
3. Click the **Server** tab.



Network :: SSL VPN :: Server

Status: Disabled

Listen IP address:

Listen Port number: 1194

Protocol: UDP

Tunnel MTU: 1500

Number of Concurrent Tunnels: 256

IP Addr: ● Network

IPv4 Tunnel (NetAddr Netmask):

IPv6 Tunnel (NetAddr/ Bitmask):

○ Point-to-Point

○ Point-to-Point IPv6

Authentication Method: TLS

CA Certificate:

Server Certificate:

Server Key:

Diffie Hellman:

HMAC/Message Digest: SHA1

Cipher: BF-CBC

Min TLS version: none

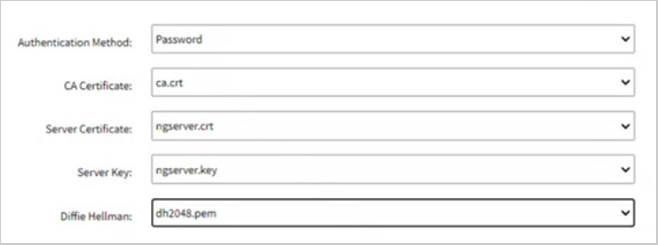
□ Use LZO data compress Algorithm

□ Redirect Gateway (Force all client generated traffic through the tunnel)

Configure the following details:

   a. **Status:** From the drop-down list select enabled to enable the VPN server.
   b. **Listen IP address:** The IP address the VPN server listens to for incoming connections. Specify the IP address that the server will use to accept VPN connections.

4. **Listen Port number:** The port number on which the VPN server listens for incoming connections. The Default is 1194 for OpenVPN. If you change the port number, ensure you also configure the same one for the client.
5. **Protocol:** The protocol used for VPN communication. To make your connection more secure, recommend using TCP.
6. **Tunnel MTU: 1500:** The maximum transmission unit (MTU) size for the VPN tunnel. This defines the largest packet size transmitted over the VPN tunnel.
7. **Number of Concurrent Tunnels: 256:** The maximum number of concurrent VPN connections the server can handle.
8. **Authentication Method:** Select one of the Authentication Method. If you have placed your files correctly in the requiered location, the following fields are populated.
   a. **Password:**
      i. **CA Certificate:** The certificate authority (CA) certificate validates the server and client certificates.
      ii. **Server Certificate:** The certificate used to authenticate the VPN server to the clients
      iii. **Server Key:** The private key corresponding to the server certificate. This key should be kept secure and not shared.
      iv. **Diffie Hellman:** The Diffie-Hellman parameters used for key exchange. These parameters help establish a secure connection.



Authentication Method: Password

CA Certificate: ca.crt

Server Certificate: ngserver.crt

Server Key: ngserver.key

Diffie Hellman: dh2048.pem

   b. **TLS:**TLS (Transport Layer Security) is a common choice for secure communication.
      i. **CA Certificate:** From the drop-down list select the requiered CA certificate.
         The certificate authority (CA) certificate validates the server and client certificates.
      ii. **Server Certificate:** The certificate used to authenticate the VPN server to the clients. From the drop-down list select the requiered Server certificate.
      iii. **Server Key:** The private key corresponding to the server certificate. This key should be kept secure and not shared.
      iv. **Diffie Hellman:** The Diffie-Hellman parameters used for key exchange. These parameters help establish a secure connection.

   c. **Static key**:
      i. Select Static Key from the Authentication drop-down list.
      ii. Select secret from the drop-down list.
      iii. Select the **Diffie Hellman** from the list. The Diffie-Hellman parameters are used for key exchange. These parameters help establish a secure connection.

9. **IP Addr:** The IP address assigned to the VPN server within the VPN network.
   a. **Network:** The network settings for the VPN server, including IPv4 and IPv6 configurations.
      i. **IPv4 Tunnel (NetAddr Netmask):** The network address and netmask for the IPv4 VPN tunnel. This defines the range of IP addresses used for the VPN tunnel.
      ii. **IPv6 Tunnel (NetAddr/ Bitmask):** The network address and bitmask for the IPv6 VPN tunnel. This defines the range of IPv6 addresses used for the VPN tunnel.
   b. **Point-to-Point:** The configuration for point-to-point connections within the VPN. This setting specifies the IP addresses for direct connections between VPN endpoints.
   c. **Point-to-Point IPv6:** The configuration for point-to-point IPv6 connections within the VPN. This setting specifies the IPv6 addresses for direct connections between VPN endpoints.
10. **HMAC/Message Digest:** Select the requiered algorithm from the drop-down list.
11. **Cipher: BF-CBC:** Select the requiered encryption algorithm for securing the VPN traffic.
12. **Min TLS version:** The minimum version of TLS required for the connection. **None** indicates no minimum version, specifying a version can enhance security.
13. **Use LZO data compress Algorithm:** Option to enable or disable LZO compression for the VPN data. Compression can improve performance but may have an impact on security.
14. **Redirect Gateway (Force all client-generated traffic through the tunnel):** Enabling this option forces all client traffic to be routed through the VPN tunnel, providing a higher level of privacy and security by routing all traffic through the VPN server.
15. Click **Save.**

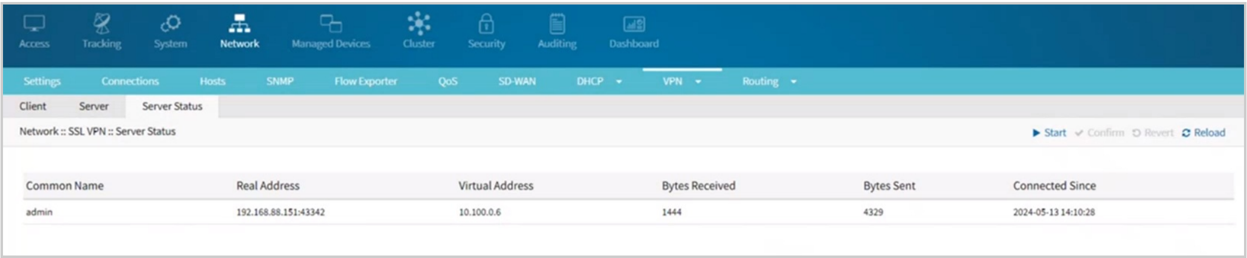
Your server is now successfully configured.

Once you establish Nodegrid as a server, you can configure any other Nodegrid as a client to connect to the server using the steps mentioned in the next section. Once the client is configured, you can see the details of the connected clients in the **Server Status** tab.

Server Status

Once your server is configured, you can go to the *Server:: Status* tab, to see the clients that are connected to the server:

- **Common Name**: The identifier or name assigned to the VPN client or user. This is extracted from the client's certificate and is used to uniquely identify each VPN client in the server's logs and configuration.
- **Real Address**: The IP address from which the VPN client connects. This is the public IP address assigned to the client by their ISP, and it is visible to the VPN server.
- **Virtual Address**: The IP address assigned to the VPN client within the VPN network. This address is used for communication within the VPN tunnel and is part of the virtual private network's IP range.
- **Bytes Received**: The total amount of data (in bytes) that the VPN client has received from the VPN server. This metric helps monitor the data usage and traffic flow from the server to the client.
- **Bytes Sent**: The total amount of data (in bytes) that the VPN client has sent to the VPN server. This metric helps monitor the data usage and traffic flow from the client to the server.
- **Connected Since**: The timestamp indicates when the VPN client established the current connection with the VPN server. This information helps track the duration of the client's session and can be useful for troubleshooting and monitoring purposes.



Network :: SSL VPN :: Server Status

Common Name	Real Address	Virtual Address	Bytes Received	Bytes Sent	Connected Since
admin	192.168.88.151:43342	10.100.0.6	1444	4329	2024-05-13 14:10:28

Configuring Nodegrid as a Client

You can configure Nodegrid as a Client, using either of the following methods:

- Adding a new client configuration
- Importing a client configuration

When you configure Nodegrid as a client, you need the CA, client, and server certificate for authentication. Ensure that the required certificate and keys are placed in the correct location before beginning the configuration:

Adding a New Client Configuration

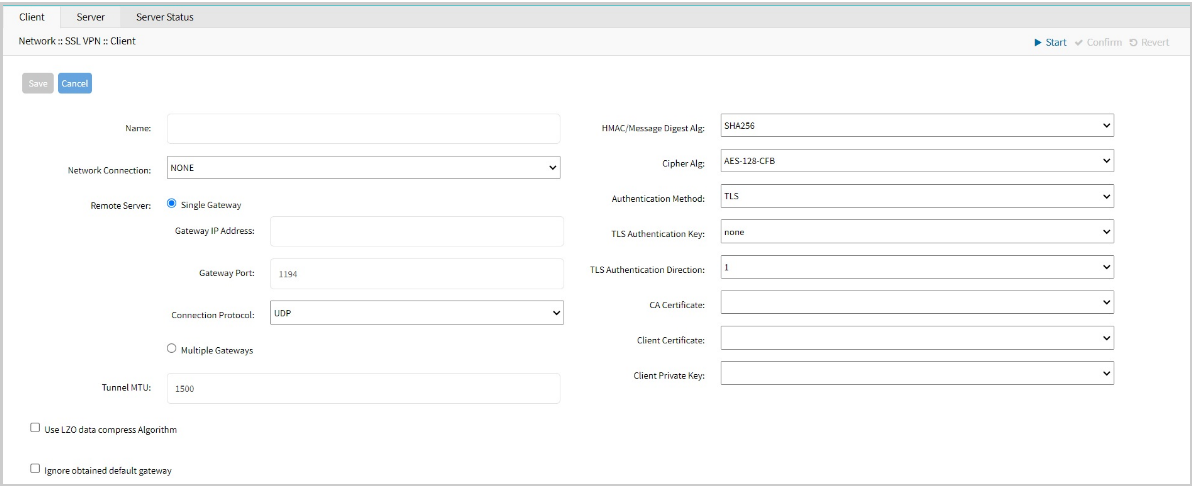
Perform the following actions to configure Nodegrid as a Client.

1. **Name**: The name assigned to this VPN configuration. This can be used to identify and manage multiple VPN configurations.
2. **Network Connection:** Select **ETHO** from the drop-down list.
3. **Remote Server**: The remote server configuration details for the VPN connection.
4. **Single Gateway**: Indicates that the VPN connection will use a single gateway for connecting to the remote server.
   a. **Gateway IP Address**: The IP address of the remote VPN server's gateway.
   b. **Gateway Port**: The port number on which the remote VPN server is listening. The default is 1194 for OpenVPN. Select the same port that you selected while

configuring a server.

c. **Connection Protocol**: Select TCP to make your connection more secure.

5. **Multiple Gateways**: Indicates that the VPN connection can use multiple gateways for connecting to the remote server. This can provide redundancy and load balancing.
6. **Tunnel MTU**: The maximum transmission unit (MTU) size for the VPN tunnel. This defines the largest packet size transmitted over the VPN tunnel.
7. **Use the LZO data compress Algorithm**: Option to enable or disable LZO compression for the VPN data. Compression can improve performance but may have an impact on security.
8. **Ignore the obtained default gateway**: If enabled, the client will ignore the default gateway obtained from the VPN server, allowing the use of a different gateway.
9. **HMAC/Message Digest Alg**: SHA256: The hash algorithm used for HMAC (Hash-based Message Authentication Code) to ensure data integrity. SHA256 provides a strong level of security.
10. **Cipher Alg:** AES-128-CFB: The encryption algorithm used for securing the VPN traffic. AES-128-CFB (Advanced Encryption Standard with 128-bit key in Cipher Feedback mode) is a common and secure choice.



Name:

Network Connection: NONE

Remote Server: ● Single Gateway

Gateway IP Address:

Gateway Port: 1194

Connection Protocol: UDP

○ Multiple Gateways

Tunnel MTU: 1500

□ Use LZO data compress Algorithm

□ Ignore obtained default gateway

HMAC/Message Digest Alg: SHA256

Cipher Alg: AES-128-CFB

Authentication Method: TLS

TLS Authentication Key: none

TLS Authentication Direction: 1

CA Certificate:

Client Certificate:

Client Private Key:

11. **Authentication Method:**

a. **TLS:** The method used for authenticating the VPN client. TLS (Transport Layer Security) is a common choice for secure communication.

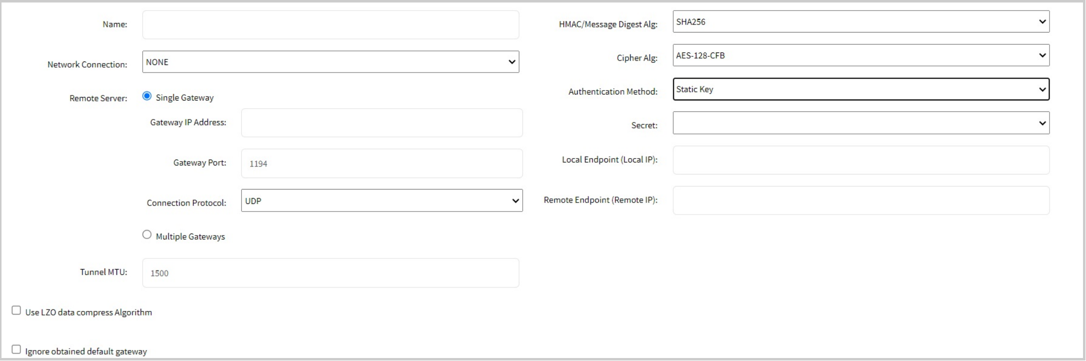
i. **TLS Authentication Key**: none: The key used for additional authentication via TLS. **None** indicates that no specific key is set, though specifying a key can enhance security.

ii. **TLS Authentication Direction**: The direction of TLS authentication. This indicates whether the key is used for incoming (1) or outgoing (0) authentication.

iii. **CA Certificate**: The certificate authority (CA) certificate validates the server and client certificates.

iv. **Client Certificate**: The certificate used to authenticate the VPN client to the server

v. Client Private Key: The private key corresponding to the client certificate. This key should be kept secure and not shared.



Name:

Network Connection: NONE

Remote Server: ● Single Gateway

Gateway IP Address:

Gateway Port: 1194

Connection Protocol: UDP

○ Multiple Gateways

Tunnel MTU: 1500

□ Use LZO data compress Algorithm

□ Ignore obtained default gateway

HMAC/Message Digest Alg: SHA256

Cipher Alg: AES-128-CFB

Authentication Method: Static Key

Secret:

Local Endpoint (Local IP):

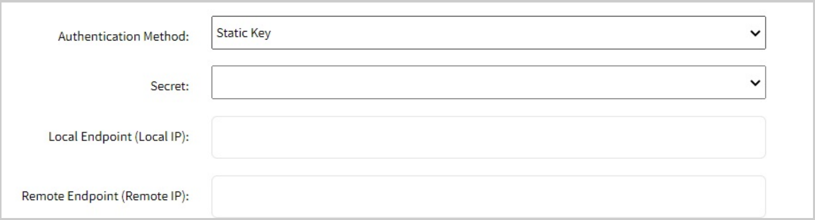
Remote Endpoint (Remote IP):

b. **Static Key**:

i. **Secret**: The pre-shared static key is used to authenticate the VPN client and server. Select the key from the drop-down list.

ii. **Local Endpoint (Local IP)**: The local IP address assigned to the VPN interface on the client side. This IP address is used within the VPN network to identify the local endpoint of the VPN connection.

iii. **Remote Endpoint (Remote IP)**: The remote IP address is assigned to the VPN interface on the server side. This IP address is used within the VPN network to identify the remote endpoint of the VPN connection.



Authentication Method: Static Key

Secret:

Local Endpoint (Local IP):

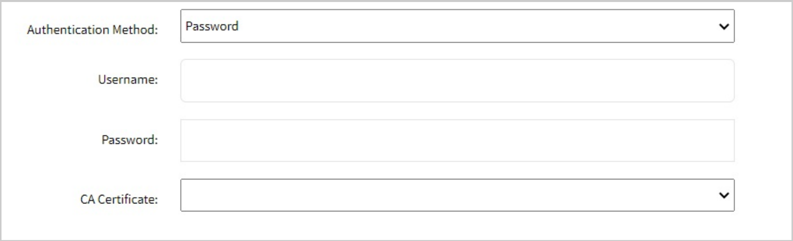
Remote Endpoint (Remote IP):

c. **Password:** Enter the following details:

i. **Username**: The username used for authenticating the VPN client. This is typically provided by the VPN administrator and is required for connecting to the VPN server.

ii. **Password**: The password associated with the username for authenticating the VPN client. This should be kept secure and not shared with others.

iii. **CA Certificate**: The certificate authority (CA) certificate is used to validate the server certificate. This ensures that the VPN client connects to a trusted server, preventing man-in-the-middle attacks.



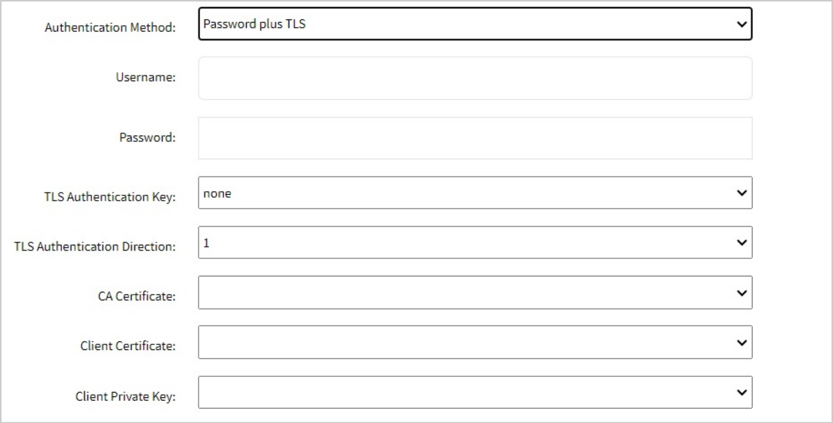
Authentication Method: Password

Username:

Password:

CA Certificate:

12. **Password plus TLS**: This method uses both a username and password for authentication and TLS (Transport Layer Security) for secure communication. This adds an extra layer of security by combining both types of authentication.
    a. **Username:** The username used for authenticating the VPN client. This is typically provided by the VPN administrator and is required for connecting to the VPN server.
    b. **Password**: The password associated with the username used for authenticating the VPN client. This should be kept secure and not shared with others.
    c. **TLS Authentication Key**: The key used for additional authentication via TLS. "None" indicates that no specific key is set, though specifying a key can enhance security by ensuring that the client and server use the same pre-shared key for the TLS handshake.
    d. **TLS Authentication Direction**: The direction of TLS authentication. This typically indicates whether the key is used for incoming (1) or outgoing (0) **authentication**. Setting this ensures proper use of the TLS authentication key.
    e. **CA Certificate**: The certificate authority (CA) certificate is used to validate the server certificate. This ensures that the VPN client is connecting to a trusted server, preventing man-in-the-middle attacks.
    f. **Client Certificate**: The certificate used to authenticate the VPN client to the server. This certificate is issued by the CA and is required for establishing a secure TLS connection.
    g. **Client Private Key**: The private key corresponding to the client certificate. This key should be kept secure and not shared with others. It is used to establish the client's identity and enable encrypted communication.



Authentication Method: Password plus TLS

Username:

Password:

TLS Authentication Key: none

TLS Authentication Direction: 1

CA Certificate:

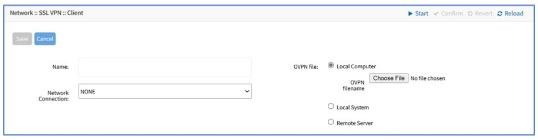
Client Certificate:

Client Private Key:

Importing OVPN Client Configuration

Before you begin to import the OVPN configuration, ensure that you have the requiered ovpn file and place it in the requiered location. You can request the ovpn file from the IT administrator.

1. Go to *Network :: VPN :: SSL VPN :: Client*.
2. Click **Import OVPN** (displays dialog).



Network :: SSL VPN :: Client

Name:

Network Connection: NONE

OVPN file: ● Local Computer

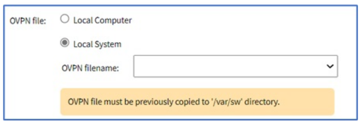
OVPN filename: Choose File No file chosen

○ Local System

○ Remote Server

   a. Enter **Name.**
   b. On **Network Connection** drop-down, select one (NONE, ETH0, ETH1, hotspot).

3. In *OVPN File* menu, select one
   - **Local Computer** radio button (expands dialog), click **Choose File**. Locate and select the file.
   - **Local System** radio button (expands dialog). On **OVPN filename** drop-down, select one.



OVPN file: ○ Local Computer

● Local System

OVPN filename:

OVPN file must be previously copied to '/var/sw' directory.

   - **Remote Server** radio button (expands dialog), enter details:
     - Enter **URL:** URL can be the IP address or hostname/FQDN. If using IPv6, use brackets [...]. Supported protocols: FTP, TFTP, SFTP, and SCP.)
     - Enter **Username** and **Password**
     - (optional) Select **The path in url to be used as the absolute path name** checkbox.

4. Click **Save**.

Testing the VPN connection as a Client

Once you configure the Client, you can test whether the connection is working.

1. Log in as a root user on the client machine from the CLI. This ensures you have the necessary permissions to run network commands and check the VPN connection.
2. Ping the server using the following command: ping <IP address of the server> Replace <IP address of the server> with the actual IP address of your VPN server. Example:

ActionScript

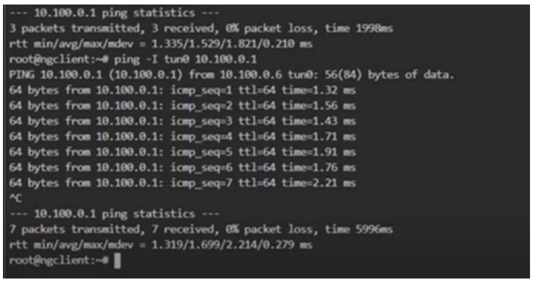
```
ping 192.168.1.1
```

3. This step verifies that the client can reach the VPN server over the network.
4. Once the connection is verified, check if the VPN tunnel is established by pinging through the tunnel interface:

ActionScript

```
ping -I tun0 10.100.0.1
```

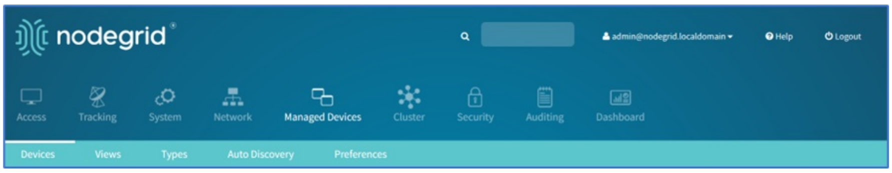
5. This command specifies the tunnel interface (typically tun0) and the internal IP address assigned within the VPN. Example: Replace 10.100.0.1 with the actual internal IP address of the VPN server or another client within the VPN network.



```
--- 10.100.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 1.335/1.529/1.821/0.210 ms
root@ngclient:~# ping -I tun0 10.100.0.1
PING 10.100.0.1 (10.100.0.1) from 10.100.0.6 tun0: 56(84) bytes of data.
64 bytes from 10.100.0.1: icmp_seq=1 ttl=64 time=1.32 ms
64 bytes from 10.100.0.1: icmp_seq=2 ttl=64 time=1.56 ms
64 bytes from 10.100.0.1: icmp_seq=3 ttl=64 time=1.43 ms
64 bytes from 10.100.0.1: icmp_seq=4 ttl=64 time=1.71 ms
64 bytes from 10.100.0.1: icmp_seq=5 ttl=64 time=1.91 ms
64 bytes from 10.100.0.1: icmp_seq=6 ttl=64 time=1.76 ms
64 bytes from 10.100.0.1: icmp_seq=7 ttl=64 time=2.21 ms
^C
--- 10.100.0.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 5996ms
rtt min/avg/max/mdev = 1.319/1.699/2.214/0.279 ms
root@ngclient:~#
```

Managed Devices Section

In this section, users can configure, create, and delete devices. The Nodegrid Platform supports devices connected through a serial, USB, or network connection.



General Information

Supported Protocols

These protocols are currently supported for network-based devices:

- Telnet
- SSH
- HTTP/S
- IPMI variations
- SNMP

Devices are managed with multiple options (enable, create, add). These can be done manually or automatically with Discovery.

When a managed device is added in the System, one license is pulled from the License Pool. Each unit is shipped with enough perpetual licenses for all physical ports. Additional licenses can be added to a unit to manage additional devices.

If licenses expire or are deleted from the system, the status of any device that exceeds the total licenses is changed to “Unlicensed”. The System maintains information on unlicensed devices but are only shown on *Access :: Table*. Licensed devices are listed and available for access and management. On the *Managed Devices* page (upper right), total licenses, total in-use licenses, and total available licenses are shown.

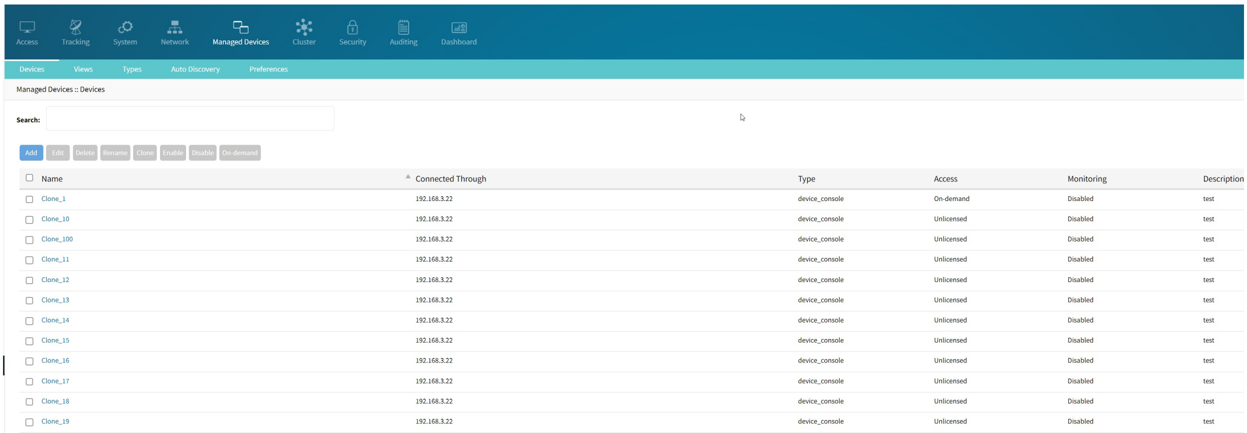
Device Types

These managed device types are supported:

- Console connections that utilize RS-232 protocol.
  - Nodegrid Console Servers
  - Nodegrid Net Services Routers
- Service Processor Devices that use:
  - IPMI 1.5
  - IPMI 2.0
  - HP iLO
  - Oracle/SUN iLOM
  - IBM IMM
  - Dell DRAC
  - Dell iDRAC
  - Intel BMC
  - Open BMC (available in v5.8+)
- Console Server connections that utilize SSH protocol
- Console Server connections that utilize:
  - Vertiv ACS Classic family
  - Vertiv ACS6000 family
  - Lantronix Console Server family
  - Opengear Console Server family
  - Digi Console Server family
  - Nodegrid Console Server family
- KVM (Keyboard, Video, Mouse) Switches that utilize:
  - Vertiv DSR family
  - Vertiv MPU family
  - Atem Enterprise KVM family
  - Raritan KVM family
  - ZPE Systems KVM module
- Rack PDUs from:
  - APC
  - CPI
  - Cyberpower
  - Baytech
  - Eaton
  - Enconnex
  - Vertiv (PM3000 and MPH2)
  - Raritan
  - Ritttal
  - Servertech
  - Austin Hughes
- Cisco UCS
- Netapp
- Infrabox
- Virtual Machine sessions from:
  - VMWare
  - KVM
- Sensors (auto-detected)
  - ZPE Systems Temperature and Humidity Sensor
- EdgeCore Access Points (auto-detected)

Devices tab

These are all actions that can be performed on this page.

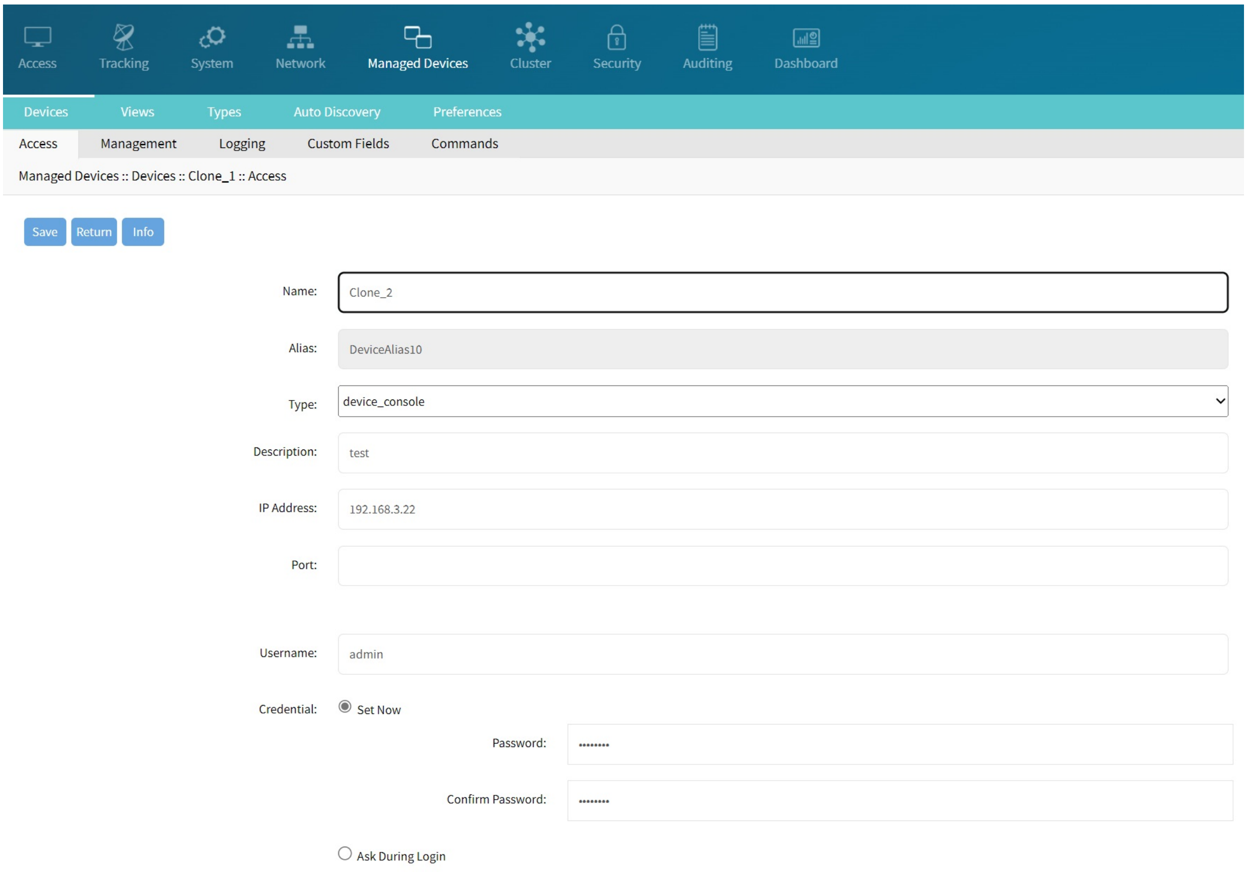


Managed Devices :: Devices

Search:

□	Name	Connected Through	Type	Access	Monitoring	Description
□	Clone_1	192.168.3.22	device_console	On-demand	Disabled	test
□	Clone_10	192.168.3.22	device_console	Unlicensed	Disabled	test
□	Clone_100	192.168.3.22	device_console	Unlicensed	Disabled	test
□	Clone_11	192.168.3.22	device_console	Unlicensed	Disabled	test
□	Clone_12	192.168.3.22	device_console	Unlicensed	Disabled	test
□	Clone_13	192.168.3.22	device_console	Unlicensed	Disabled	test
□	Clone_14	192.168.3.22	device_console	Unlicensed	Disabled	test
□	Clone_15	192.168.3.22	device_console	Unlicensed	Disabled	test
□	Clone_16	192.168.3.22	device_console	Unlicensed	Disabled	test
□	Clone_17	192.168.3.22	device_console	Unlicensed	Disabled	test
□	Clone_18	192.168.3.22	device_console	Unlicensed	Disabled	test
□	Clone_19	192.168.3.22	device_console	Unlicensed	Disabled	test

Additionaly, you can click the device name link to rename a device. The **Name** field is editable and allows you to rename the device. Click **Save** to save the changes.



Managed Devices :: Devices :: Clone_1 :: Access

Name: Clone_2

Alias: DeviceAlias10

Type: device_console

Description: test

IP Address: 192.168.3.22

Port:

Username: admin

Credential: ● Set Now

Password: ••••••••

Confirm Password: ••••••••

○ Ask During Login

Device Type Selections

When a device is added, the *Add* dialog is modified by the **Type** selection.

> NOTE
>
> If NSR-16USB-OCP-EXPN card is added, it is automatically recognized when device is booted. (available v5.8+)

Service Processor Devices

The Nodegrid Platform supports multiple IPMI-based Service Processors (IPMI 1.5, IMPI 2.0, Hewlett Packard ILO's, Oracle/SUN iLOM's, IBM IMM's, Dell DRAC and iDRAC).

To manage these devices, Nodegrid requires a valid network connection to each device. This can be without dedicated network interface on Nodegrid, or through an existing network connection.

These features are available:

- Serial Over LAN (SOL)
- Web Interface
- KVM sessions
- Virtual Media
- Data Logging
- Event Logging
- Power Control (through Rack PDU)

Some features might not be available, depending on the Service Processor's capabilities.

For console access via SOL, on the server make sure to enable BIOS console redirect and OS console redirect (typically for Linux OS).

Switch

(available v5.8+)

This provides switch port details: Interface Type, Admin Status, and Link Status. When added, Auto-Discovery will identify the ports.

Supported switches:

- switch_edgecore
- switch_zpe

Infrabox

Smart Access Control is supported for Rack's solution appliances (Infrabox) from InfraSolution. Communication requires SNMP to be configured.

These features are available:

- Door Control
- Web Session
- Power Control through Rack PDU

Netapp

Netapp appliances are supported through their management interfaces. These features are available:

- Console Session
- Data Logging
- Event Logging
- Power Control through Netapp appliance
- Web Session
- Custom Commands
- Power Control through Rack PDU

Cisco UCS

Management of Cisco UCS is supported through Console Ports, as well as management interfaces. These features are available:

- Console Session
- Logging
- Event Logging
- Power Control through Cisco UCS appliance
- Web Session
- Custom Commands

Devices with SSH

Management of devices through SSH is supported. These features are available:

- Console Session
- Data Logging
- Custom Commands
- Web Sessions
- Power Control through Rack PDU

Third-Party Console Servers

Multiple third-party Console Servers from different vendors are supported (including consoles from Avocent and Servertech). These can be added to allow connected targets to be directly connected to a Nodegrid device.

This is a two-step process. First, the third party unit is added to the Nodegrid Platform. Then all enabled ports are added to the Nodegrid Platform.

These features are available:

- Console Session
- Data Logging
- Custom Commands
- Web Sessions
- Power Control through Rack PDU

Rack PDUs

Multiple third-party Rack PDUs from different vendors are supported (including products from APC, Avocent, Baytech, CPI, Cyberpower, Eaton, Enconnex, Geist, Liebert, Raritan, Rittal, and Servertech). When these devices are added to the Nodegrid Platform, users can connect to the Rack PDU and control the power outlets (only if supported by the Rack PDU). Outlets can be associated to specific devices, allowing direct control of specific power outlets for this device.

These features are available:

- Console Sessions
- Data Logging
- Custom Commands
- Web Sessions
- Power Control of outlets

The Power Control feature needs to be supported by the Rack PDU. Check the Rack PDU manual to determine if this feature is available on a specific model.

> NOTE
>
> By default, Nodegrid communicates with the Rack PDU with SSH/telnet. The reaction time is typically very slow. If possible, use SNMP to communicate with the Rack PDU.

Rack PDUs include (other PDUs may be available on the list):

- pdu_apc
- pdu_baytech
- pdu_digital_loggers (v5.6+)
- pdu_eaton
- pdu_mph2
- pdu_pm3000
- pdu_cpi_serial (must be physically connected via serial port or USB) (available v5.6+)
- pdu_raritan
- pdu_geist
- pdu_servertech
- pdu_enconnex
- pdu_cyberpower
- pdu_rittal
- pdu_tripplite

KVM Switches

Multiple third party KVM switches are supported (including those from Avocent and Raritan). When added, the switches act as if directly connected.

This is a two-step process, First, the third-party KVM switch is added to the Nodegrid Platform. Then all enabled ports are added.

These features are available:

- KVM Session
- Web Sessions
- Power Control through Rack PDU

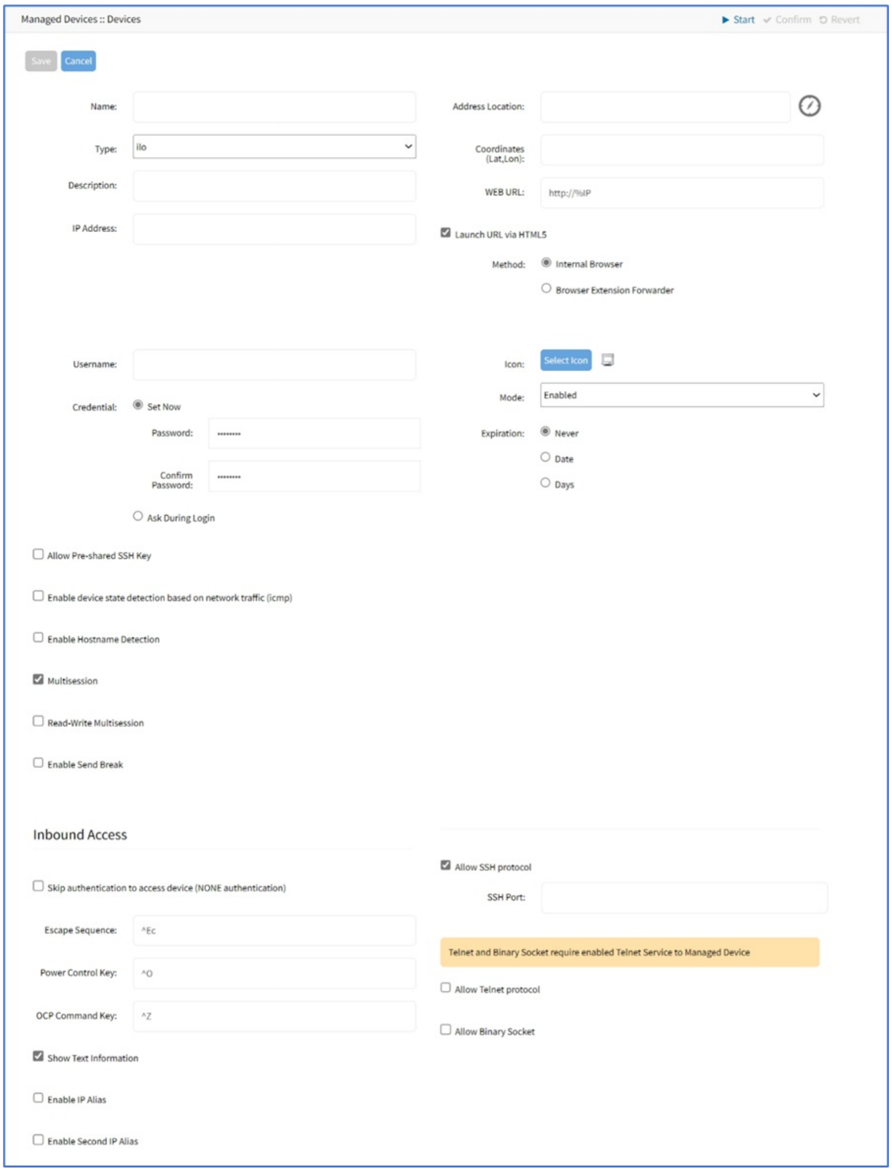
On the **Add** dialog, make sure these two settings are selected:

- **End Point**, select **Appliance** radio button.
- **End Point**, select **KVM Port** radio button.

Manage Devices

Add Device

1. Go to *Managed Devices :: Devices*.
2. Click **Add** (displays dialog).



Managed Devices :: Devices

Name:

Type: ilo

Description:

IP Address:

Username:

Credential: ● Set Now

Password: ••••••••

Confirm Password: ••••••••

○ Ask During Login

Address Location:

Coordinates (Lat,Lon):

WEB URL: http://%IP

☑ Launch URL via HTML5

Method: ● Internal Browser ○ Browser Extension Forwarder

Icon:

Mode: Enabled

Expiration: ● Never ○ Date ○ Days

□ Allow Pre-shared SSH Key

□ Enable device state detection based on network traffic (icmp)

□ Enable Hostname Detection

☑ Multisession

□ Read-Write Multisession

□ Enable Send Break

Inbound Access

□ Skip authentication to access device (NONE authentication)

Escape Sequence: ^Ec

Power Control Key: ^O

OCP Command Key: ^Z

☑ Show Text Information

□ Enable IP Alias

□ Enable Second IP Alias

☑ Allow SSH protocol

SSH Port:

Telnet and Binary Socket require enabled Telnet Service to Managed Device

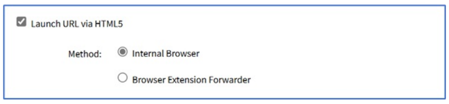
□ Allow Telnet protocol

□ Allow Binary Socket

3. Enter **Name**.
4. In the **Type** drop-down, select one.
   - Service Processor devices (ilo, imm, drac, drac6, idrac7, ilom, ipmi_1.5, ipmi_2.0, intel_bmc, openbmc)
     IP Address (reachable by the Nodegrid Platform)
   - Switch devices (switch_edgecore)
     IP Address (reachable by the Nodegrid Platform)
   - Infrabox devices (infrabox)
     IP Address (reachable by the Nodegrid Platform)
   - Netapp devices (netapp)
     IP Address (reachable by the Nodegrid Platform)
   - Cisco UCS Blade devices (cimc_ucs)
     IP Address (reachable by the Nodegrid Platform)
     ChassisID
     Blade ID
   - Virtual Console KVM devices (virtual_console_kvm)
     IP Address (reachable by the Nodegrid Platform)
     Port
   - Console Server devices (console_server_nodegrid, console_server_acs, console_server_acs6000, console_server_lantronix, console_server_opengear, console_server_digicp, console_server_raritan, console_server_perle)
     IP Address (reachable by the Nodegrid Platform)
     Port
   - PDU devices (pdu_apc, pdu_baytech, pdu_digital_logger, pdu_eaton, pdu_mph2, pdu_pm3000, pdu_cpi, pdu_raritan, pdu_geist, pdu_servertech, pdu_enconnex, pdu_cyberpower, pdu_rittal, pdu_hpe_g2)
     IP Address (reachable by the Nodegrid Platform)
   - KVM Virtual Machine devices (virtual_console_kvm)
     Name (must match the hypervisor name)
     IP Address (reachable by the Nodegrid Platform)

- KVM devices (kvm_dsr, kvm_mpu, kvm_aten, kvm_raritan)
  IP Address (reachable by the Nodegrid Platform)

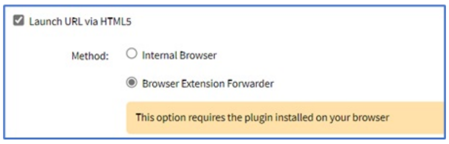
5. **Address Location** (a valid address for the device location).
   Coordinates (Lat, Lon) (if GPS is available, click **Compass** icon) or manually enter GPS coordinates.
6. **Web URL**
   Launch URL via HTML5 checkbox (expands options). In *Method* menu, select one:

   ☑ Launch URL via HTML5

   Method: ● Internal Browser
   ○ Browser Extension Forwarder

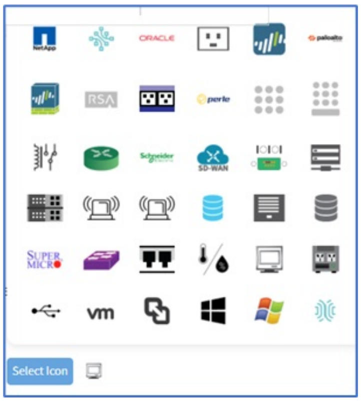
   Internet Browser radio button
   Browser Extension Forwarder radio button (read note)

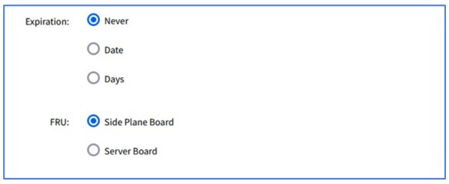
   ☑ Launch URL via HTML5

   Method: ○ Internal Browser
   ● Browser Extension Forwarder

   This option requires the plugin installed on your browser
7. **Username**
   In the *Credential* menu, select one:
   Set Now radio button. Enter the Password and Confirm the Password.
   Ask During Login radio button (user credentials are entered during login).
8. Select checkboxes, as needed:
   a. **Allow Pre-shared SSH Key** checkbox.
   b. **Enable device state detection based on network traffic (icmp)** checkbox
   c. **Enable Hostname Detection** checkbox
   d. **Multisession** checkbox
   e. **Read-Write Multisession** checkbox
   f. **Enable Send Break** checkbox
9. **Select Icon**. On the pop-up dialog, select an icon.

10. **Mode** drop-down, select one (Enabled, On-demand, Disabled).
11. On the *Expiration* menu, select one:
    a. **Mode** drop-down, select one (Enabled, On-demand, Disabled).
    b. *Expiration* menu, select one:
       i. **Never** radio button
       ii. **Date** radio button. Enter **Date (YYYY-MM-DD)**
       iii. **Days** radio button. Enter **Duration**.
12. On **Type** drop-down:
    a. If **openbmc** is selected, the *FRU* menu displays (below the *Expiration* menu).

    Expiration: ● Never
    ○ Date
    ○ Days

    FRU: ● Side Plane Board
    ○ Server Board

    > **NOTE**
    > The OpenBMC platform contains various Field Replaceable Units (FRUs) like Side Plane Board (spb), OCP Mezzanine Card, and four 1S server boards.

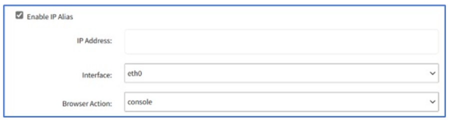
    b. In the *FRU* menu, select one:
    Side Plane Board radio button
    Server Board radio button (expands dialog). For **Slot Number**, specify which 1 of 4 1S server boards to control.
    c. If **console_server_xxx** is selected, the *Endpoint* menu displays (below the *Expiration* menu).

    > **NOTE**
    > Depending on the selection of the console server, the **Expiration** and **End Point** radio button selections can change.

    From the *End Point* menu, select one:
    Appliance radio button, enter **Port Number**
    Serial Port radio button, enter **Port Number**
    USB Port radio button (if available), enter **Port Number**
    KVM Port radio button, enter **Port Number**
13. In the *End Point* menu, select one (*not available for service processors, virtual consoles*);

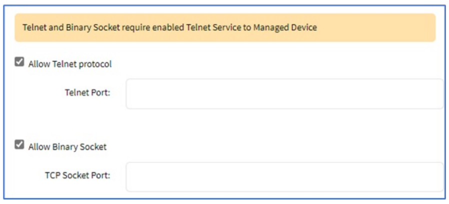
a. **Appliance** radio button, enter **Port Number**
b. **Serial Port** radio button, enter **Port Number**
c. **USB Port** radio button (if available), enter **Port Number**
d. **KVM Port** radio button, enter **Port Number**

14. In the *Inbound Access* menu:
    a. **Skip Authentication to access device (NONE authentication)** checkbox (if unselected, enter the following details).
    Escape Sequence (prefix for Console commands – i.e., "^Ec." to close Console)
    Power Control Key (*Power Control* menu for the device displays)
    b. **Show Text Information** checkbox
    c. **Enable IP Alias** checkbox (expands dialog)



☑ Enable IP Alias
IP Address:
Interface: eth0
Browser Action: console

IP Address
Interface drop-down, select one (eth0, eth1, loopback, loopback1)
Browser Action drop-down, select one (console, web)
d. **Allow Telnet Protocol** checkbox, enter **TCP Socket Port**
e. **Allow Binary Socket** checkbox, enter **TCP Socket Port**
f. (optional) **Enable Second IP Alias** checkbox
IP Address
Interface drop-down, select one (eth0, eth1, loopback, loopback1)
Browser Action drop-down, select one (console, web)
g. **Allow Telnet Protocol** checkbox, enter, enter **TCP Socket Port**
h. **Allow Binary Socket** checkbox, enter **TCP Socket Port**
i. **Allow SSH protocol** checkbox, enter **SSH Port**
j. At this location:



Telnet and Binary Socket require enabled Telnet Service to Managed Device
☑ Allow Telnet protocol
Telnet Port:
☑ Allow Binary Socket
TCP Socket Port:

Allow Telnet Protocol. checkbox, enter **TCP Socket Port**
Allow Binary Socket checkbox, enter **TCP Socket Port**

15. Click **Save**.

CLI Procedure

1. Go to /settings/devices.
2. Use the add command to create a new device.
3. Use the set command to define the following settings, and save the changes with commit.

Plaintext | Copy

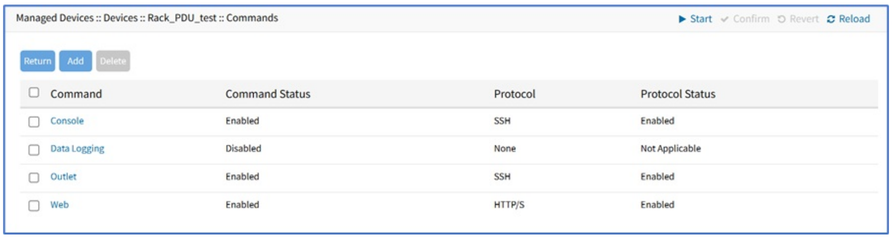
```
[admin@nodegrid /]# cd /settings/devices
[admin@nodegrid devices]# add
[admin@nodegrid {devices}]# set name=IPMI
[admin@nodegrid {devices}]# set type=ipmi_2.0
[admin@nodegrid {devices}]# set ip_address=192.168.10.11
[admin@nodegrid {devices}]# set credential=ask_during_login

or

[admin@nodegrid {devices}]# set credential=set_now
[admin@nodegrid {devices}]# set username=admin password=admin

[admin@nodegrid {devices}]# commit
```

Configure Rack PDU

This process requires two steps:

- Add the PDU device. See *Add Device*.
- Configure the PDU with the procedure below.

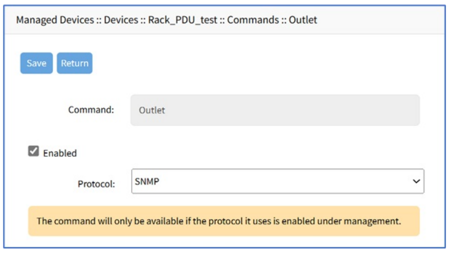
1. Go to *Managed Devices :: Devices*.
2. Locate and click the **Name** of the newly added Rack PDU.
3. On the **Commands** tab, *Command* column, click **Outlets**.



Managed Devices :: Devices :: Rack_PDU_test :: Commands

☐ Command	Command Status	Protocol	Protocol Status
☐ Console	Enabled	SSH	Enabled
☐ Data Logging	Disabled	None	Not Applicable
☐ Outlet	Enabled	SSH	Enabled
☐ Web	Enabled	HTTP/S	Enabled

4. On the *Outlet* dialog, **Protocol** drop-down, select **SNMP**.



Managed Devices :: Devices :: Rack_PDU_test :: Commands :: Outlet

Command: Outlet

☑ Enabled

Protocol: SNMP

The command will only be available if the protocol it uses is enabled under management.

5. Click **Save**.
6. On the **Management** tab, in the *SNMP* menu, update values to match the Rack PDU settings (see manufacturer’s manual).
7. This will modify the default settings, enabling the "private" community to handle both read and write operations.

> **NOTE:**
> **When you select the type as PDU HPE G2, by default, the HPE G2 PDU is set up with the public community for read-only access and the private community for write-only access. This setup means the private community can't be used for reading and writing. To fix this, you may need to change the PDU's configuration to allow the private community to have both read and write access. Here's how you do it:**
>
> 1. Log in to the PDU's management interface.
> 2. Go to the SNMP settings.
> 3. Change the "private" community permissions to allow both reading and writing.
> 4. Save the configuration.

8. Click **Save**.

> NOTE
>
> Use SNMP settings to provide read and write access. Read-only credentials can not control power outlets.

The Rack PDU Outlets are automatically discovered (may need a few minutes, depending on the Rack PDU).

CLI Procedure

1. Go to /settings/devices/<device name>/commands/outlet.
2. Change the protocol to SNMP.
3. Go to /settings/devices/<device name>/management.
4. Enable SNMP and select the desired SNMP version and details.
5. Save the changes with commit.

> NOTE
>
> Use SNMP settings to provide read and write access. Read-Only credentials can not control power outlets.

The Rack PDU Outlets are automatically discovered (may need a few minutes, depending on the Rack PDU).

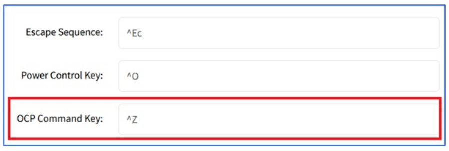
Plaintext Copy

```
[admin@nodegrid /]# cd /settings/devices
[admin@nodegrid devices]# add
[admin@nodegrid {devices}]# set name=Rack_PDU
[admin@nodegrid {devices}]# set type=pdu_servertech
[admin@nodegrid {devices}]# set ip_address=192.168.2.39
[admin@nodegrid {devices}]# set credential=ask_during_login

or

[admin@nodegrid {devices}]# set credential=set_now
[admin@nodegrid {devices}]# set username=admin password=admin

[admin@nodegrid {devices}]# commit
[admin@nodegrid /]# cd /settings/devices/Rack_PDU/commands/outlet
[admin@nodegrid outlet]# set protocol=snmp
[admin@nodegrid outlet]# cd /settings/devices/Rack_PDU/management/
[admin@nodegrid management]# set snmp=yes
[+admin@nodegrid management]# snmp_version = v2
[+admin@nodegrid management]# snmp_commmunity = private
[+admin@nodegrid management]# commit
```

Edit Device

1. Go to *Managed Devices :: Devices*.
2. In the *Name* column, locate device and select checkbox.
3. Click **Edit** (displays dialog).

> NOTE
>
> If the device type is USB OCP, this additional field displays. Modify **OCP Command Key** as needed. (available in v5.8+)



Escape Sequence: ^Ec

Power Control Key: ^O

OCP Command Key: ^Z

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

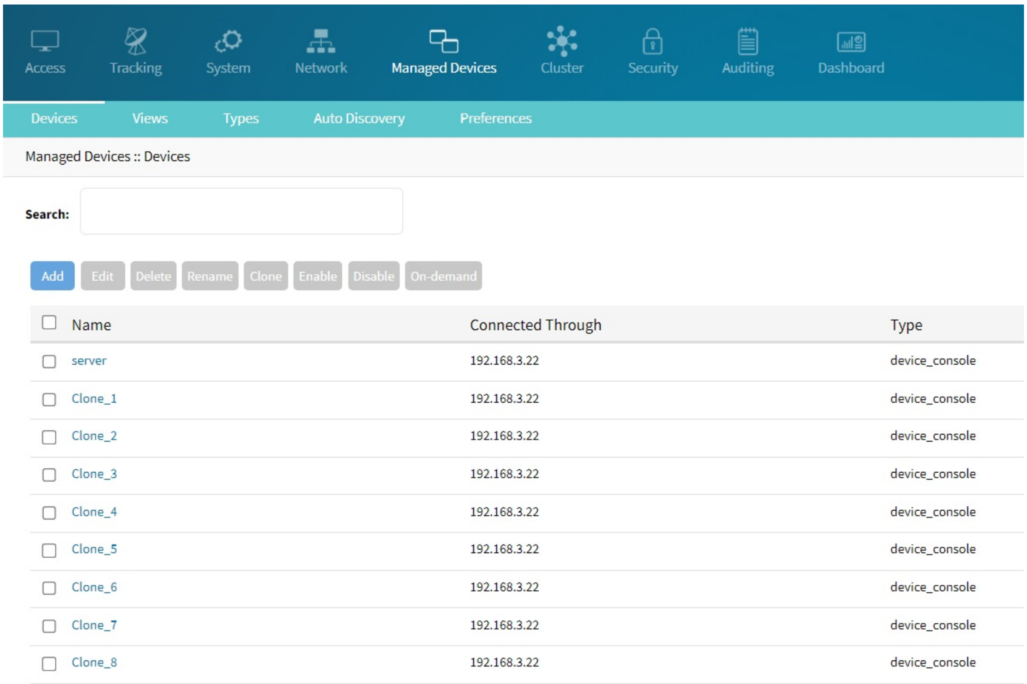
Delete Device

1. Go to *Managed Devices :: Devices*.

2. In the *Name* column, locate the device and select the checkbox.
3. Click **Delete**.
4. On the Confirmation dialog, click **OK**.

Managing devices individually

1. Go to *Managed Devices :: Devices*. All the devices are listed on this page.
2. Click the link to any device.

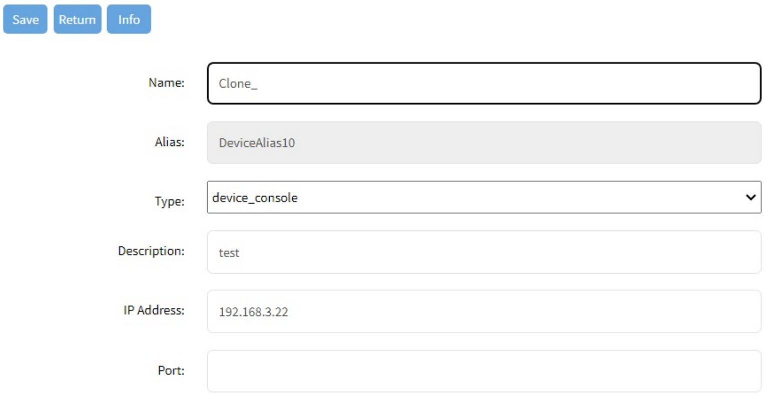


Managed Devices :: Devices

Search:

□	Name	Connected Through	Type
□	server	192.168.3.22	device_console
□	Clone_1	192.168.3.22	device_console
□	Clone_2	192.168.3.22	device_console
□	Clone_3	192.168.3.22	device_console
□	Clone_4	192.168.3.22	device_console
□	Clone_5	192.168.3.22	device_console
□	Clone_6	192.168.3.22	device_console
□	Clone_7	192.168.3.22	device_console
□	Clone_8	192.168.3.22	device_console

3. You can update any device configuration. For example, rename a device by overwriting a new name in the Name field.



Name: Clone_

Alias: DeviceAlias10

Type: device_console

Description: test

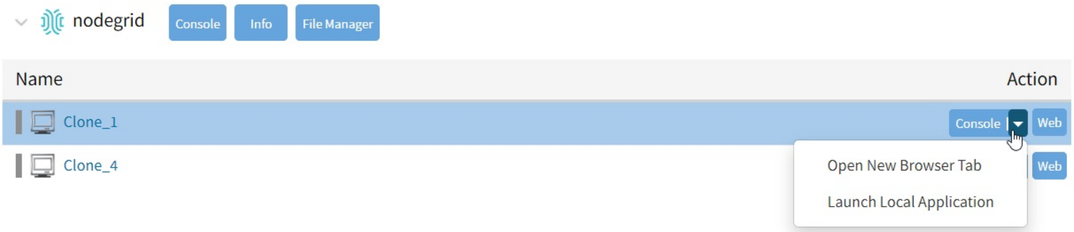
IP Address: 192.168.3.22

Port:

4. Once you make changes the **Save** button becomes active. Click **Save** to save the changes.
5. The **Return** button takes you back to the Devices tab page where all the devices are listed.
6. Click **Info,** and the user is directed to **Access** :: *Table* to view the device description and additionally perform the actions as described in the **TableTab** section.

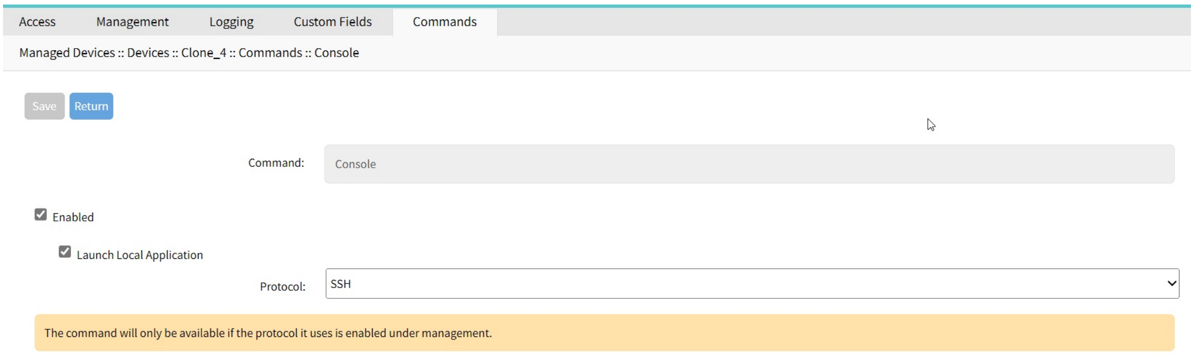
Launching the Local Application field

The Console drop-down list is visible only when you enable the Launch Local Application for the selected device. You can select the Launch Local Application option when you want to launch the local ssh or telnet instead of opening a new browser tab to handle the connection.



To enable the Console option and Launch Local Application, perform the following actions :

1. Go to **Managed Devices> Devices**, and select the required device from the list.
2. Go to the **Commands** tab.
3. Select the **Launch Local Application** field.
4. Click **Save**.



Managed Devices :: Devices :: Clone_4 :: Commands :: Console

Command: Console

☑ Enabled

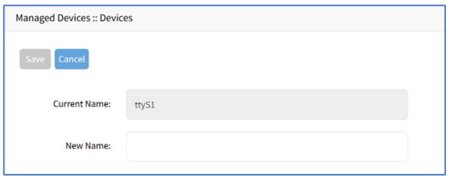
☑ Launch Local Application

Protocol: SSH

The command will only be available if the protocol it uses is enabled under management.

Rename Device

1. Go to *Managed Devices :: Devices*.
2. In the *Name* column, locate the device and select the checkbox.
3. Click **Rename** (displays dialog). Enter **New Name**.



Managed Devices :: Devices

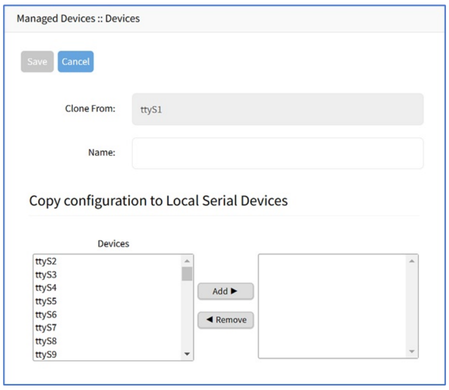
Current Name: ttyS1

New Name:

4. Click **Save**.

Clone Device

1. Go to *Managed Devices :: Devices*.
2. In the *Name* column, locate the device and select the checkbox.
3. Click **Clone** (displays dialog).



Managed Devices :: Devices

Clone From: ttyS1

Name:

Copy configuration to Local Serial Devices

Devices

ttyS2
ttyS3
ttyS4
ttyS5
ttyS6
ttyS7
ttyS8
ttyS9

4. Enter **Name**.
5. In *Copy configuration to Local Serial Devices* section:
   Select from the left-side panel, click **Add►** to move to the right-side panel.
   To remove from the right-side panel, select, and click **◄Remove**.
6. Click **Save**.

Enable Device

1. Go to *Managed Devices :: Devices*.
2. In the *Name* column, locate the device and select the checkbox.
3. Click **Enable**.

Disable Device

1. Go to *Managed Devices :: Devices*.
2. In the *Name* column, locate device and select checkbox.
3. Click **Disable**.

Set Device to On-Demand

1. Go to *Managed Devices :: Devices*.
2. In the *Name* column, locate device and select checkbox.
3. Click **On-Demand**.

Set Device as Default

> WARNING
>
> This restores the selected device back to the original factory settings.

1. Go to *Managed Devices :: Devices*.
2. In the *Name* column, locate device and select checkbox.
3. Click **Default**.

Run Bounce DTR

This puts the DTR and RTS pins DOWN – waits 500ms, then put those pins UP.

1. Go to *Managed Devices :: Devices*.
2. In the *Name* column, locate device and select checkbox.
3. Click **Bounce DTR**.

Configure Chatsworth (CPI) eConnect PDU

(available in v5.6+)

This unit must be physically connected to a serial port or USB port of a Nodegrid device. This PDU can merge IT devices to PDU outlets for more intuitive power control. Console access is included. Activities are recorded on the serial data log. Features include Outlet Auto Discovery and Outlet Control (Power On, Off, Cycle, Status).

> **NOTE**
>
> Console + CLI should be available on the PDU device - find your model in the **CPI Quick Reference**.

1. Go to *Managed Devices :: Devices*.
2. Click on the serial device the PDU is connected.
    a. On **Type** drop-down, select **pdu_cpi_serial**
    b. Enter **Username**.
    c. Enter **Password** and **Confirm Password**
    d. (as needed) Review and adjust serial configuration details (**Baud Rate**, **Parity**, etc.)
3. Click **Save**.

Auto Discovery

Auto-Discovery automatically detects the CPI PDU. The CPI PDU details are available in device's **Outlets** sub-tab.

1. Go to *Auto-Discovery :: Discover Now*.
2. Select **PDU serial device name** checkbox.
3. Click **Discover Now**.
4. To confirm, go to *Access :: Table*.
5. Click on the **PDU serial device name** and check the *Discovered Outlets* in the table.

Merged Outlets

To see merged outlets.

1. Go to *Managed Devices :: Devices :: <device name> :: Commands*.
2. Review *Merged* panel details (this example shows eConnect PDU attached with two devices).

Accessing Jetson Card as a Managed Device

Introduction

The Jetson Orin Nano is supported on the Nodegrid Gate SR device model with the minimum supported version of 6.0.15. The NVIDIA Jetson Orin is a powerful platform that enables AI-driven applications and edge computing. The ZPE carrier board setup uses a USB connection for serial access via an FTDI chip, and dedicated control pins for managing recovery and reset functionalities. It is also possible to toggle the USB connection to directly connect to the Jetson Card, allowing flashing from recovery mode.

Available interfaces between Jetson and Nodegrid Gate SR

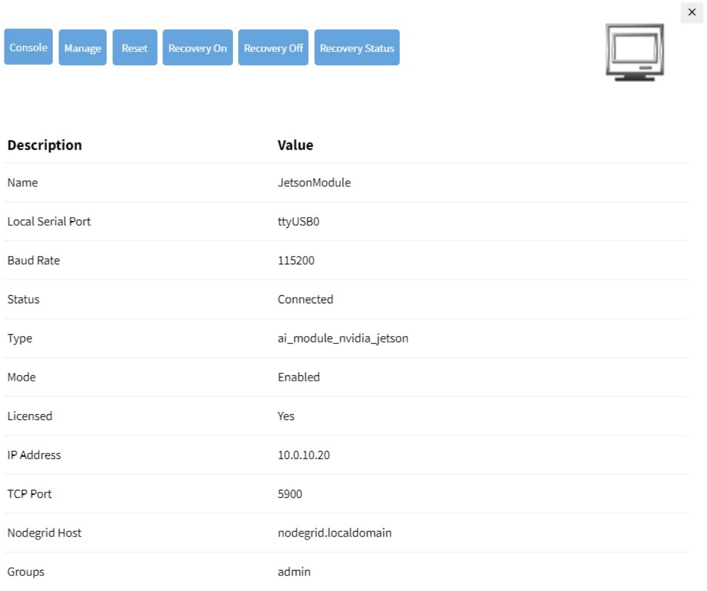
The Nodegrid OS automatically detects and creates the Managed Device called **JetsonModule** when it detects a Jetson Card. You can access the Jetson carrier board using the Serial, KVM, or USB connections.

Serial Connection

In the **JetsonModule**-managed device, you can connect through a serial connection.

Using Web UI:

1. Navigate to *Access :: Table, select the JetsonModule as the managed device,* and click **Manage**.



Description	Value
Name	JetsonModule
Local Serial Port	ttyUSB0
Baud Rate	115200
Status	Connected
Type	ai_module_nvidia_jetson
Mode	Enabled
Licensed	Yes
IP Address	10.0.10.20
TCP Port	5900
Nodegrid Host	nodegrid.localdomain
Groups	admin

Using CLI:

Plaintext Copy

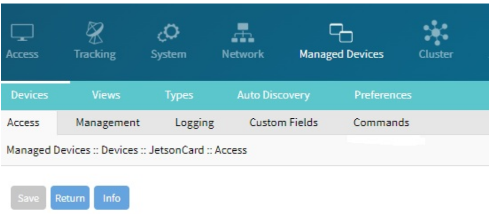
```
[admin@nodegrid /]# cd access/JetsonModule/
[admin@nodegrid JetsonModule]# show name: JetsonModule
Status: Connected
[admin@nodegrid JetsonModule]# connect
```

KVM Connection

To support KVM over VNC, the IP address of the Jetson must be added to the managed device, together with the port 5900. This was already done in the steps seen above.

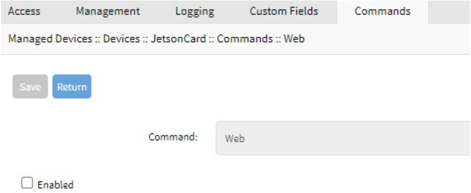
After creating the Managed Device as seen above:

1. Navigate to *Managed Devices :: [Your Device Name]*.
2. Click on the **Commands** tab.



Managed Devices :: Devices :: JetsonCard :: Access

3. Go to Web and uncheck the **Enabled** checkbox.
4. Click on **Save**.

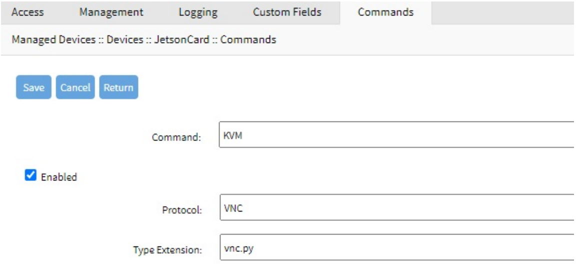


Managed Devices :: Devices :: JetsonCard :: Commands :: Web

Command: Web

☐ Enabled

5. Click on **Add** and configure the KVM over VNC as it follows:



Managed Devices :: Devices :: JetsonCard :: Commands

Command: KVM

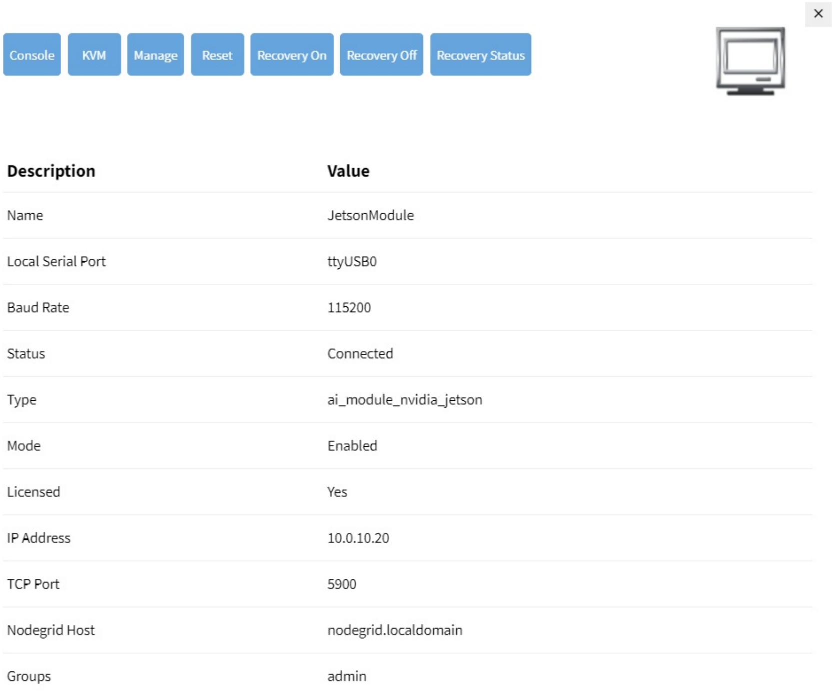
☑ Enabled

Protocol: VNC

Type Extension: vnc.py

6. Click on **Save**.

Your device now has KVM access to Jetson.



Description	Value
Name	JetsonModule
Local Serial Port	ttyUSB0
Baud Rate	115200
Status	Connected
Type	ai_module_nvidia_jetson
Mode	Enabled
Licensed	Yes
IP Address	10.0.10.20
TCP Port	5900
Nodegrid Host	nodegrid.localdomain
Groups	admin

> You must also follow the procedure at Running a VNC Server on Jetson Card to enable the VNC server in the Jetson.

USB Connection

The following modes are available to manage reset and recovery modes:

- module_recovery_off
- module_recovery_on
- module_recovery_status
- module_reset

Execute the following command to access these modes via CLI:

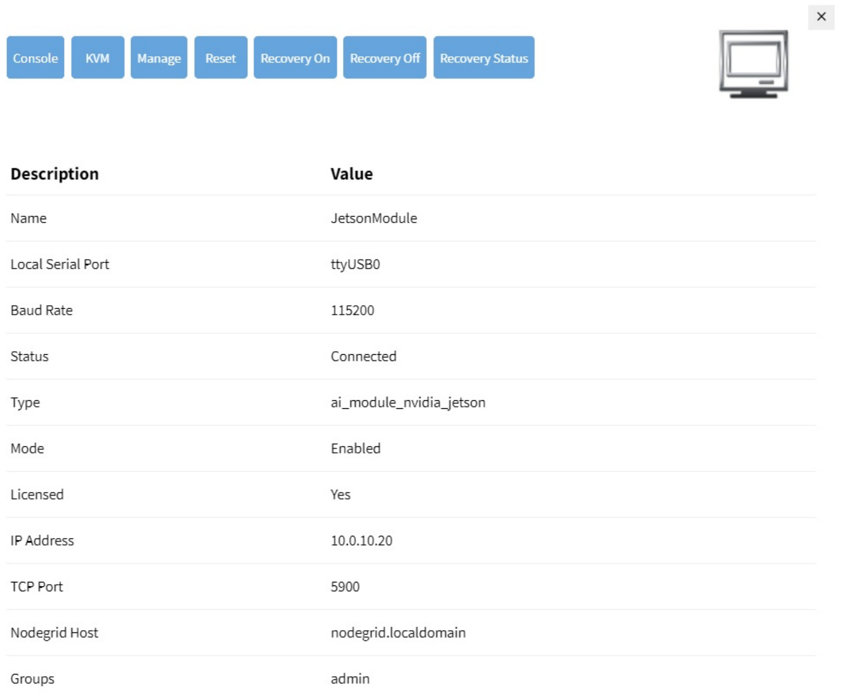
Plaintext Copy

```
[admin@nodegrid /]# cd access/JetsonModule/
[admin@nodegrid JetsonModule]# module_recovery
module_recovery_off     module_recovery_on      module_recovery_status  module_reset
[admin@nodegrid JetsonModule]#
```

To connect to Jetson USB, your device first need to be in recovery mode. This is done in such way that one can flash the Bootloader and Nodegrid OS to Jetson.

Recovery On Using Web UI:

Click on the **Recovery On** button in the WebUI.



Description	Value
Name	JetsonModule
Local Serial Port	ttyUSB0
Baud Rate	115200
Status	Connected
Type	ai_module_nvidia_jetson
Mode	Enabled
Licensed	Yes
IP Address	10.0.10.20
TCP Port	5900
Nodegrid Host	nodegrid.localdomain
Groups	admin

Recovery On Using CLI:

Execute the command from the CLI by using **module_recovery_on**:

Plaintext Copy

```
[admin@nodegrid /]# cd access/JetsonModule/
[admin@nodegrid JetsonModule]# module_recovery_on
Recovery Enabled
[admin@nodegrid JetsonModule]#
```

This will force Jetson into recovery mode and reset it.

After putting the Jetson Card in to Force Recovery Mode, a new USB device appears. You can view this by running the command **lsusb** on root shell.

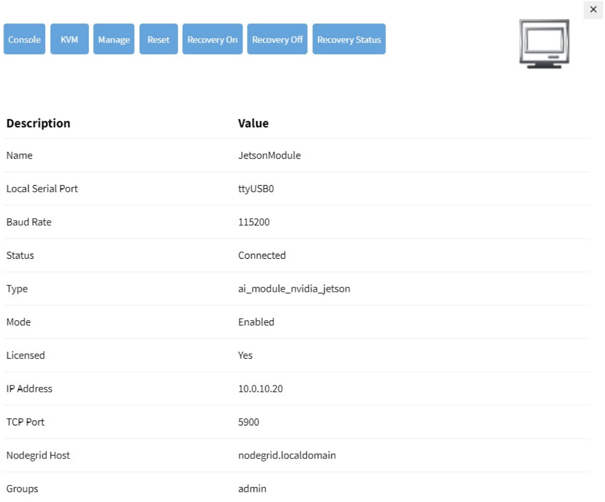
Plaintext Copy

```
[admin@nodegrid /]# shell sudo su -
root@nodegrid:~# lsusb
Bus 004 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 002: ID 05e3:0620 Genesys Logic, Inc. USB3.2 Hub
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 007: ID 0955:7523 NVIDIA Corp. APX
Bus 001 Device 003: ID 0fc5:b080 Delcom Engineering USB FS IO
Bus 001 Device 002: ID 05e3:0610 Genesys Logic, Inc. 4-port hub
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
```

> In this case, the device that should appear is the NVIDIA Corp, with ID 0955:7523.

To remove Jetson from recovery mode, you can execute **module_recovery_off** on CLI or do it from the WebUI:

Recovery Off Using Web UI:



Description	Value
Name	JetsonModule
Local Serial Port	ttyUSB0
Baud Rate	115200
Status	Connected
Type	ai_module_nvidia_jetson
Mode	Enabled
Licensed	Yes
IP Address	10.0.10.20
TCP Port	5900
Nodegrid Host	nodegrid.localdomain
Groups	admin

Recovery Off Using CLI:

Execute the command **module_recovery_off**:

Plaintext Copy

```
[admin@nodegrid /]# cd access/JetsonModule/
[admin@nodegrid JetsonModule]# module_recovery_off
Recovery Disabled
[admin@nodegrid JetsonModule]#
```

The Serial Connection is enabled after this operation.

Configure Individual Device Settings

Each device in the *Managed Devices :: Devices* table are individually configured. To gain access to a device's settings, locate it in the table, and click the **Name**. This displays the individual device settings in sub-tabs: **Access**, **Management**, **Logging**, **Custom Fields**, **Commands**.

In the procedures, the path is shown as:
Go to *Device Management :: Devices :: <device name> :: <sub-tab>*.

Alternately, select the checkbox next to the device name and click **Edit**.

Configuring Auto-Login for Managed Devices via Serial Port

The auto-login feature allows users to automatically log into managed devices without manually entering login credentials each time they access a device via a serial port. This is particularly useful when devices are frequently accessed for monitoring, configuration, or troubleshooting.

Understanding the auto-login workflow:

- **Pre-Configured Credentials:** The system administrator pre-configures the login credentials (username and password) for each managed device connected via the serial port.
- **Serial Port Configuration:** The managed device is associated with a specific serial port type (e.g., local_serial, usb_serialB). This configuration includes the necessary details such as the login prompt, password prompt, and command prompt that the system expects during the login process.
- **Auto-Login Execution:** When a user attempts to access the managed device via the serial port, the Nodegrid Manager automatically sends the pre-configured credentials to the device. This eliminates the need for the user to manually input the username and password each time.
- **Seamless Access:** The user is logged into the device automatically, allowing them to begin their tasks immediately without the repetitive task of entering credentials.

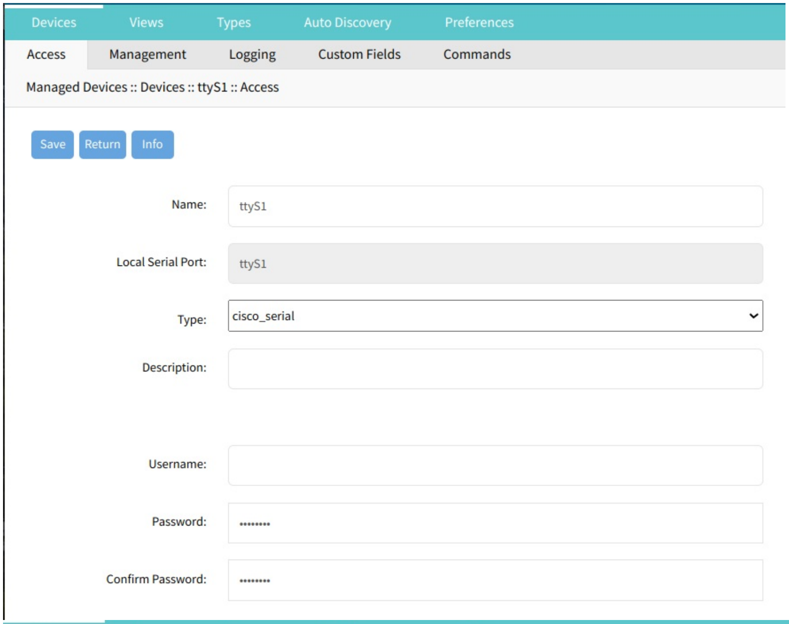
Prerequisites

- Access to the Nodegrid Manager with appropriate permissions to configure managed devices.
- Ensure that the serial port types (e.g., local_serial, usb_serialB) have been predefined in the system.

Procedure

This procedure outlines the steps to configure auto-login credentials for managed devices using the serial port in the Nodegrid WebUI.

1. Log in to the Nodegrid Manager WebUI.
2. Navigate to the *Managed Devices :: Devices:: <port> :: Access*.



Managed Devices :: Devices :: ttyS1 :: Access

Name: ttyS1

Local Serial Port: ttyS1

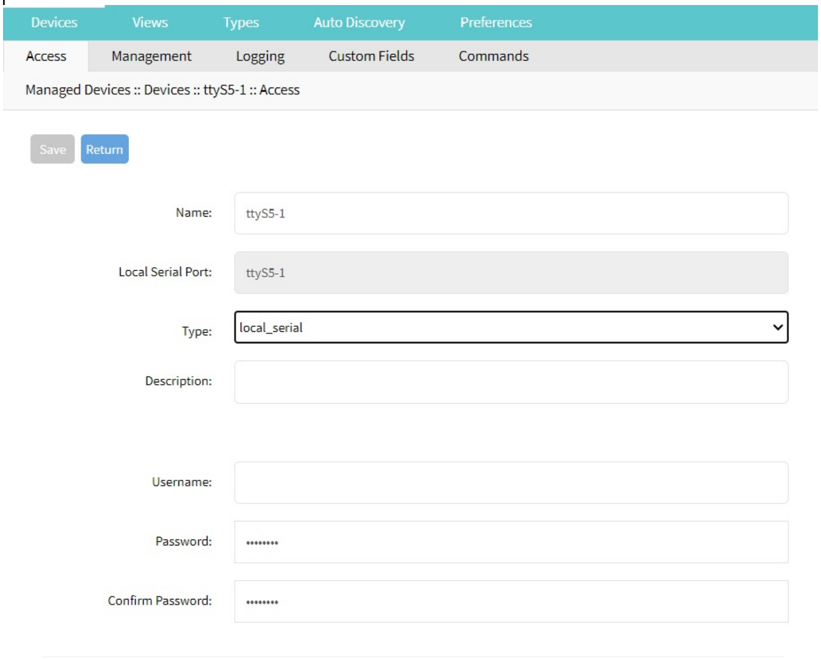
Type: cisco_serial

Description:

Username:

Password: ••••••••

Confirm Password: ••••••••



Managed Devices :: Devices :: ttyS5-1 :: Access

Name: ttyS5-1

Local Serial Port: ttyS5-1

Type: local_serial

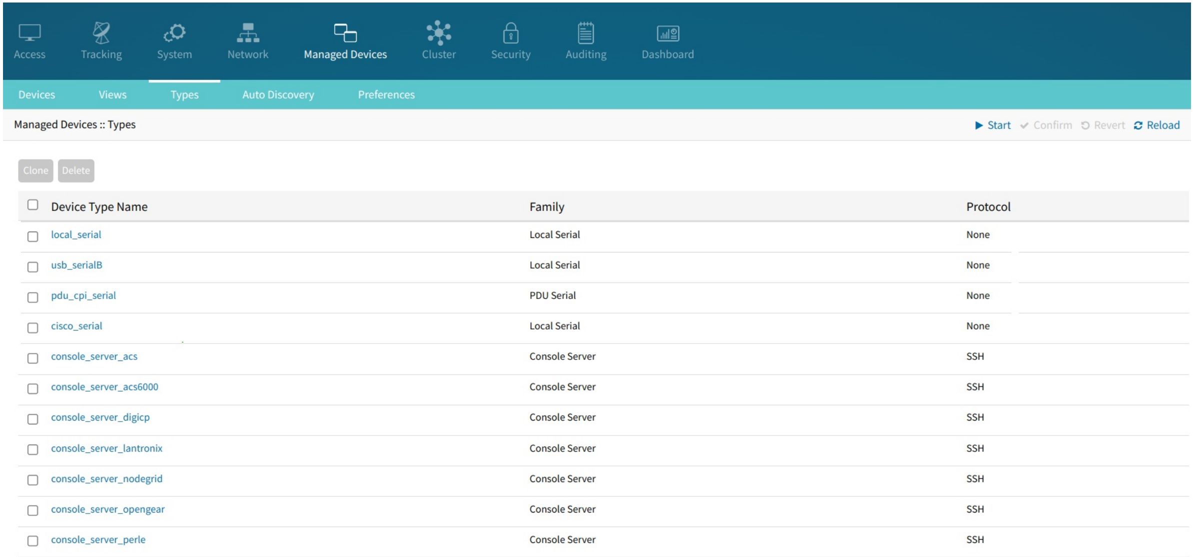
Description:

Username:

Password: ••••••••

Confirm Password: ••••••••

3. Enter the username, password, and confirm password that should be used during the managed device login. After the credentials are configured, the Console session of the serial port is automatically logged in.



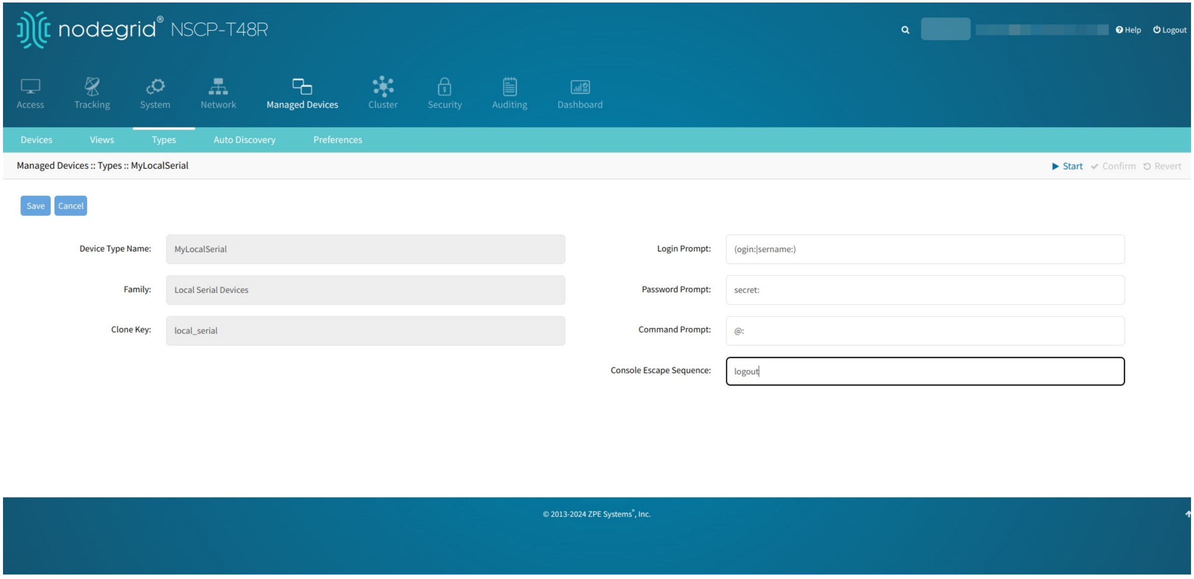
Managed Devices :: Types

	Device Type Name	Family	Protocol
□	local_serial	Local Serial	None
□	usb_serialB	Local Serial	None
□	pdu_cpi_serial	PDU Serial	None
□	cisco_serial	Local Serial	None
□	console_server_acs	Console Server	SSH
□	console_server_acs6000	Console Server	SSH
□	console_server_digicp	Console Server	SSH
□	console_server_lantronix	Console Server	SSH
□	console_server_nodegrid	Console Server	SSH
□	console_server_opengear	Console Server	SSH
□	console_server_perle	Console Server	SSH

4. ## Cloning a Port Type

The main reference types for serial ports are the *local_serial* and *usb_serialB*. You can clone a Type if you need to change any of the login prompts, password prompts, command prompt, or console escape sequence. To clone a Type:

1. Navigate to *Managed Devices :: Types.*
2. Select the device type name from the table and click **Clone**. Clone the local_serial or other _serial (name ends with "_serial") type.
3. Configure the cloned type as indicated in the following figures.



Managed Devices :: Types :: MyLocalSerial

Device Type Name: MyLocalSerial

Family: Local Serial Devices

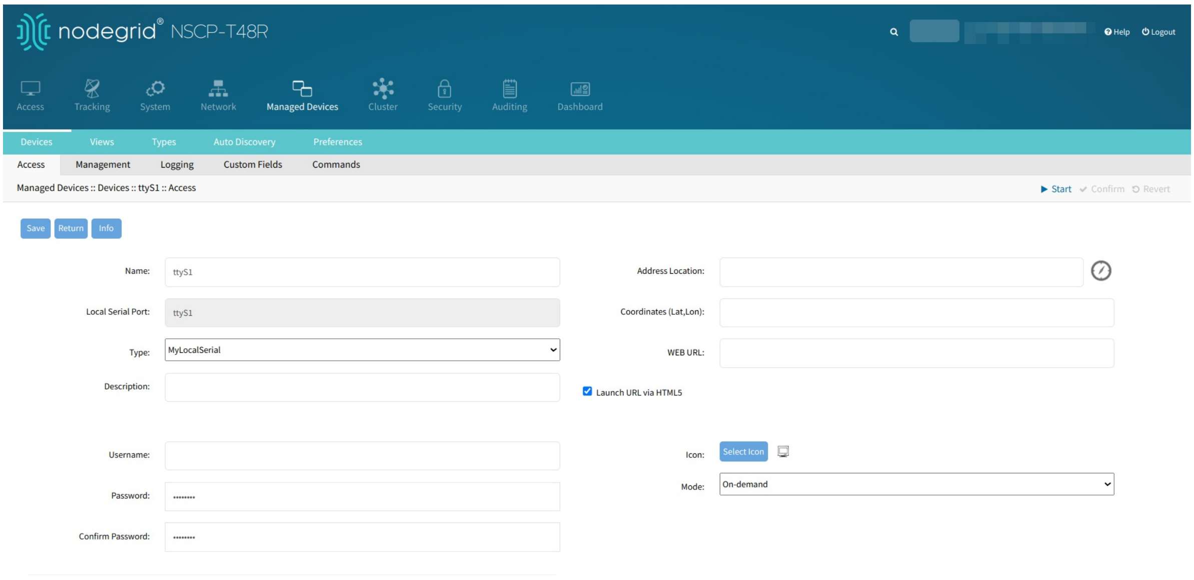
Clone Key: local_serial

Login Prompt: (ogin:|sername:)

Password Prompt: secret:

Command Prompt: @:

Console Escape Sequence: logout



Managed Devices :: Devices :: ttyS1 :: Access

Name: ttyS1

Local Serial Port: ttyS1

Type: MyLocalSerial

Description:

Username:

Password: ••••••••

Confirm Password: ••••••••

Address Location:

Coordinates (Lat,Lon):

WEB URL:

☑ Launch URL via HTML5

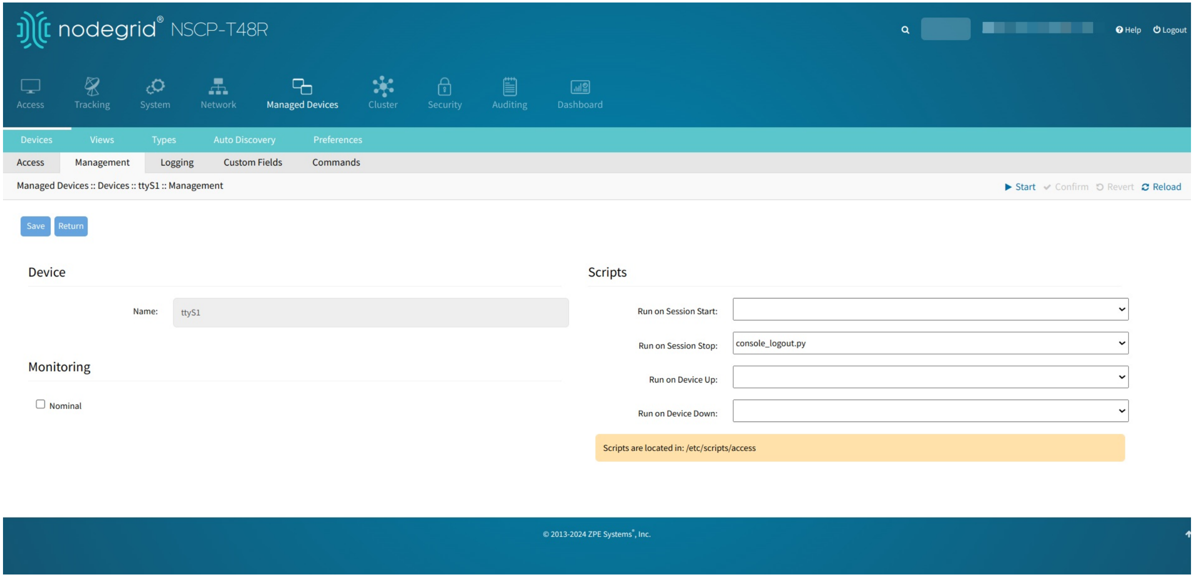
Icon:

Mode: On-demand

Configuring Auto Logout

If want to have the console automatically logged out when the Console session is closed:

1. Navigate to the path *Managed Devices :: Devices :: <port> :: Management*.
2. In the Run on Session Stop field, select the console_logout.py script.



Managed Devices :: Devices :: ttyS1 :: Management

Name: ttyS1

Run on Session Start:

Run on Session Stop: console_logout.py

Run on Device Up:

Run on Device Down:

Scripts are located in: /etc/scripts/access

Verify the Configuration:

1. Navigate back to the Devices tab.
2. Select the Types sub-tab to ensure the serial types are correctly listed under the Family column, with protocols set to None. You can also clone a Type for another device and modify the password if required.

Troubleshooting (if required):

- If the auto-login fails, revisit the Access tab and ensure that the credentials are correct.
- Check the Types configuration under Managed Devices to confirm that the correct serial type is being used.
- If necessary, consult the Nodegrid logs for any error messages related to serial port access.

Caution:

- **Ensure that all configurations adhere to your organization's security protocols to prevent unauthorized access.**

Access sub-tab

The Nodegrid Platform supports RS-232 Serial connections with the available Serial and USB interfaces. Ports are automatically detected and shown in the Devices menu. To provide access to the device, each port needs to be enabled and configured.

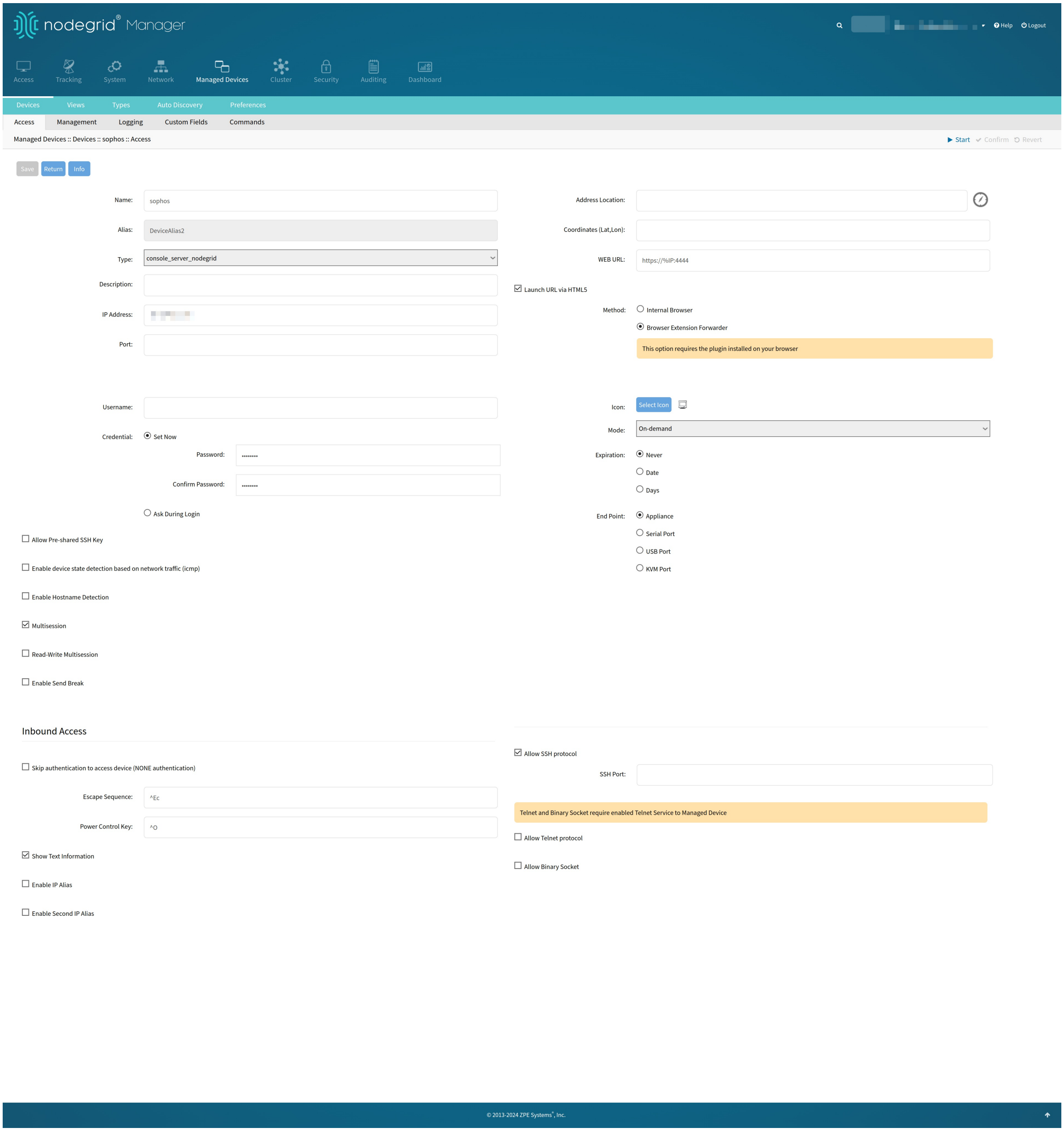
Before configuring the Nodegrid port, check the device manufacturer's console port settings. Most devices use default port settings: 9600,8,N,1

The Nodegrid Console Server S Series supports advanced auto-detection. This simplifies configuration with automatic detection of the cable pinout (Legacy and Cisco) and connection speed.

Configure Device Type

This is a general description of the procedure. Based on the type of device, the details will change. Details provided here are the serial port configuration.

1. Go to *Managed Devices :: Devices :: <device name> :: Access*.



Managed Devices :: Devices :: sophos :: Access

Name: sophos

Alias: DeviceAlias2

Type: console_server_nodegrid

Description:

IP Address: [redacted]

Port:

Username:

Credential: ● Set Now

Password: ••••••••

Confirm Password: ••••••••

○ Ask During Login

□ Allow Pre-shared SSH Key

□ Enable device state detection based on network traffic (icmp)

□ Enable Hostname Detection

☑ Multisession

□ Read-Write Multisession

□ Enable Send Break

Address Location:

Coordinates (Lat,Lon):

WEB URL: https://%IP:4444

☑ Launch URL via HTML5

Method: ○ Internal Browser

● Browser Extension Forwarder

This option requires the plugin installed on your browser

Icon:

Mode: On-demand

Expiration: ● Never

○ Date

○ Days

End Point: ● Appliance

○ Serial Port

○ USB Port

○ KVM Port

Inbound Access

□ Skip authentication to access device (NONE authentication)

Escape Sequence: ^Ec

Power Control Key: ^O

☑ Show Text Information

□ Enable IP Alias

□ Enable Second IP Alias

☑ Allow SSH protocol

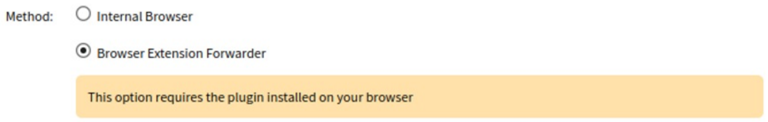
SSH Port:

Telnet and Binary Socket require enabled Telnet Service to Managed Device

□ Allow Telnet protocol

□ Allow Binary Socket

2. Configure location details:
   a. **Address Location** (can use **Compass** icon)
   b. **Coordinates**
   c. **Web URL**
   d. **Launch URL via HTML5** checkbox (default: enabled)
   e. **Method**: Select **Internal Browser** or **Browser Extension Forwarder**. When you select the Internal Browser option, the device session opens the usual setting with TTYD allowing you to interact with the device terminal remotely via a web interface. When you select the Browser Extension Forwarder option, the request path is changed and the browser plugin is activated for your device session. This allows you to navigate the managed device web interface, providing you with a seamless browsing experience of the device.



Method: ○ Internal Browser

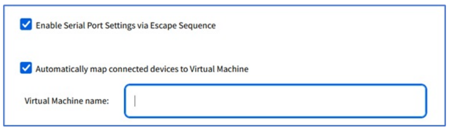
● Browser Extension Forwarder

This option requires the plugin installed on your browser

f. **Allow Pre-shared SSH Key** checkbox

3. Configure port settings:
   a. **Baud Rate** drop-down, select one (speed matching device settings) or (Auto, 9600, 19200, 38400, 57600, 115200).
   b. **Parity** drop-down, select one (None-default, Odd, Even).
   c. **Flow Control** drop-down, select one (None-default, Software, Hardware).
   d. **Data Bits** drop-down, select one (5,6,7,8-default).
   e. **Stop Bits** drop-down, select one (1-default, 2).
   f. **RS-232 signal for device state detection** drop-down, select one (Auto, DCD, CTS, None).

4. Set Serial settings:
   a. **Enable device state detection based in data flow** checkbox
   b. **Enable Hostname Detection** checkbox
   c. **Multisession** checkbox (several users can access the same device at the same time, and see the same output. First user has read-write access, others have read-only.)
   d. **Read-Write Multisession** checkbox (if enabled, all connected users have read-write access to the session)
   e. **Enable Serial Port Settings via Escape Sequence** checkbox
   f. (optional) Select **Enable Send Break** (configured per device. Not available on: usb_kvm, usb_sensor, usb_device, local_serial). If selected, enter a new **Break Sequence** (sent via SSH console session).
   g. If selected device is USB, this flag is shown: (available in v5.8+)
      - Select **Automatically map connected devices to Virtual Machine** checkbox (expands dialog), enter **Virtual Machine name**.



☑ Enable Serial Port Settings via Escape Sequence

☑ Automatically map connected devices to Virtual Machine

Virtual Machine name:

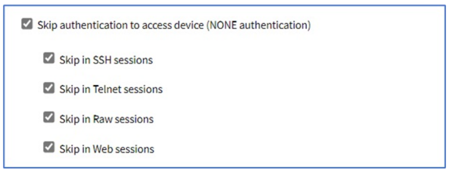
   h. On **Select Icon** pop-up, select an icon.
   i. On **Mode** drop-down, select one (Enabled, On-Demand, Disabled).

5. In the *Expiration* menu, select a radio button: **Never**, **Expiration Date** or **Expiration Days** and provide an appropriate value.

> **NOTE**
>
> With VM devices, both Date and Days are synced with the ESXi Servers where the VMs are constantly being added, moved, and deleted, or if the Nodegrid managed device license becomes available.

   a. **Date (YYYY-MM-DD)** Device available until the specified date. After that date, set to Disabled mode. Admin user has 10 days to take action. After 10 days, the device and its data are removed from the system.
   b. **Days** (between 1 and 9999999999) If no update on the device's configuration after specified days, device and data is removed from the System (similar to a timeout).

6. In *Inbound Access* menu, enter details:
   a. **Skip authentication to access device (NONE authentication)** checkbox (displays dialog).



☑ Skip authentication to access device (NONE authentication)

☑ Skip in SSH sessions

☑ Skip in Telnet sessions

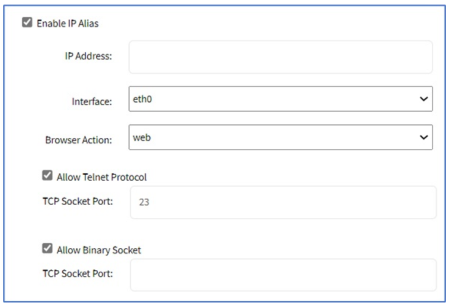
☑ Skip in Raw sessions

☑ Skip in Web sessions

      - **Skip in SSH sessions** checkbox (default: enabled)
      - **Skip in Telnet sessions** checkbox (default: enabled)
      - **Skip in Raw sessions** checkbox (default: enabled)
      - **Skip in Web sessions** checkbox (default: enabled)

   b. **Escape Sequence** (default: ^Ec – Ctrl+Shift+E+c)
   c. **Power Control Key** (default: ^O – Ctrl+Shift+O)
   d. **Show Text Information** checkbox

7. Select **Enable IP Alias** checkbox (user can connect to a device with IP addresses).



☑ Enable IP Alias

IP Address:

Interface: eth0

Browser Action: web

☑ Allow Telnet Protocol

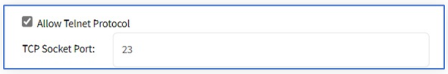
TCP Socket Port: 23

☑ Allow Binary Socket

TCP Socket Port:

   a. Enter **IP Address.**

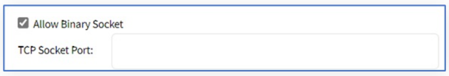
   b. On **Interface** drop-down, select one (backplane0, eth0, loopback).
   c. On **Browser Action** drop-down, select one (console, web).
   d. Select **Allow Telnet Protocol** checkbox. Enter **TCP Socket Port** (default: 23).



☑ Allow Telnet Protocol

TCP Socket Port: 23

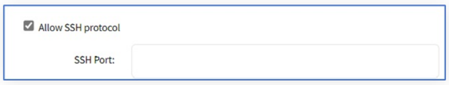
   e. Select **Allow Binary Socket** checkbox. Enter **TCP Socket Port.**



☑ Allow Binary Socket

TCP Socket Port:

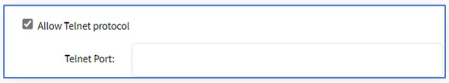
f. Select **Allow SSH protocol** checkbox. Enter **SSH Port.**



☑ Allow SSH protocol

SSH Port:

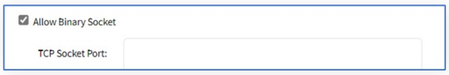
g. Select **Allow Telnet protocol** checkbox. Enter **Telnet Port.**



☑ Allow Telnet protocol

Telnet Port:

h. Select **Allow Binary Socket** checkbox. Enter **TCP Socket Port.**



☑ Allow Binary Socket

TCP Socket Port:

8. Select **Enable Second IP Alias** checkbox (same dialog as **Enable IP Alias**).
9. Click **Save.**

CLI Procedure

This example provides some of the configurations provided above.

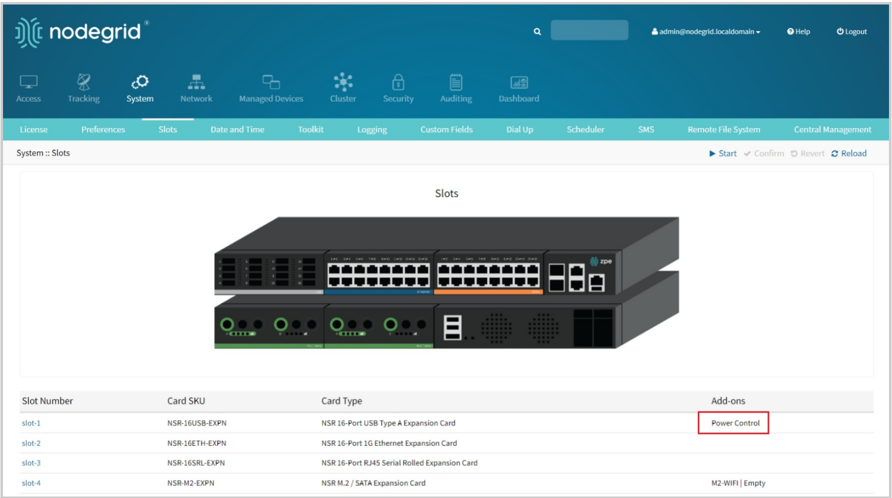
1. Go to /settings/devices
2. Use the edit command with the port name to change the port configuration. Multiple ports can be defined.
3. Use the show command to display current values.
4. Use the set command for:
   baud_rate (set to the correct speed matching device settings or to Auto)
   parity (None (default), Odd, or Even)
   flow_control (None (default), Software, Hardware)
   data_bits (5, 6, 7, 8 (default))
   stop_bits (1)
   rs-232_signal_for_device_state_detection (DCD (default), None, CTS)
   mode (Enabled, On-Demand, Disabled)
5. Use the commit command to change the settings.

Plaintext Copy

```
[admin@nodegrid /]# cd /settings/devices
[admin@nodegrid devices]# edit ttyS2
[admin@nodegrid {devices}]# show
name: ttyS2
type: local_serial
address_location =
coordinates =
web_url =
launch_url_via_html5 = yes
baud_rate = 9600
parity = None
flow_control = None
data_bits = 8
stop_bits = 1
rs-232_signal_for_device_state_detection = DCD
enable_device_state_detection_based_in_data_flow = no
enable_hostname_detection = no
multisession = yes
read-write_multisession = no
icon = terminal.png
mode = disabled
skip_authentication_to_access_device = no
escape_sequence = ^Ec
power_control_key = ^O
show_text_information = yes
enable_ip_alias = no
enable_second_ip_alias = no
allow_SSH_protocol = yes
SSH_port =
allow_telnet_protocol = yes
telnet_port = 7002
allow_binary_socket = no
data_logging = no
[admin@nodegrid {devices}]# set mode=enabled baud_rate=Auto
[admin@nodegrid {devices}]# commit
```

Configure USB Mode

1. To confirm the USB card supports USB Passthrough, go to *System :: Slots* . Check the *Add-ons* column for an entry: **Power Control**.

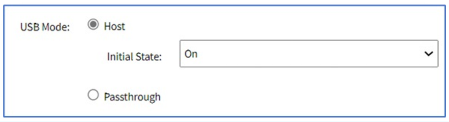


System :: Slots

Slots

Slot Number	Card SKU	Card Type	Add-ons
slot-1	NSR-16USB-EXPN	NSR 16-Port USB Type A Expansion Card	Power Control
slot-2	NSR-16ETH-EXPN	NSR 16-Port 1G Ethernet Expansion Card	
slot-3	NSR-16SRL-EXPN	NSR 16-Port RJ45 Serial Rolled Expansion Card	
slot-4	NSR-M2-EXPN	NSR M.2 / SATA Expansion Card	M2-WIFI | Empty

2. Go to *Managed Devices :: Devices*.
3. On the list, locate the USB and click the **Name** (displays dialog).
4. On the **Access** tab, *USB Mode* menu, select one:
   - **Host** radio button (expands dialog), **Initial State** drop-down, select one (On, Off, Last State)



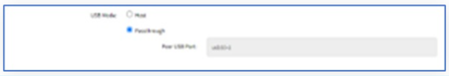
USB Mode: ● Host

Initial State: On

○ Passthrough

> **NOTE**
> The device with an internal USB serial adapter provides the power for the adapter. Power control setting does not affect power to the USB.

   - **Passthrough** radio button (expands dialog).



USB Mode: ○ Host

● Passthrough

Peer USB Port: [illegible]

> **NOTE**
> When a device's Passthrough mode is enabled, its peer is also set to Passthrough mode.

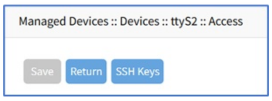
5. Click **Save**.

Configure SSH Key Authentication

For added security, devices can be configured to authenticate via SSH keys. When enabled, SSH is connected with key pairs (user does not require password).

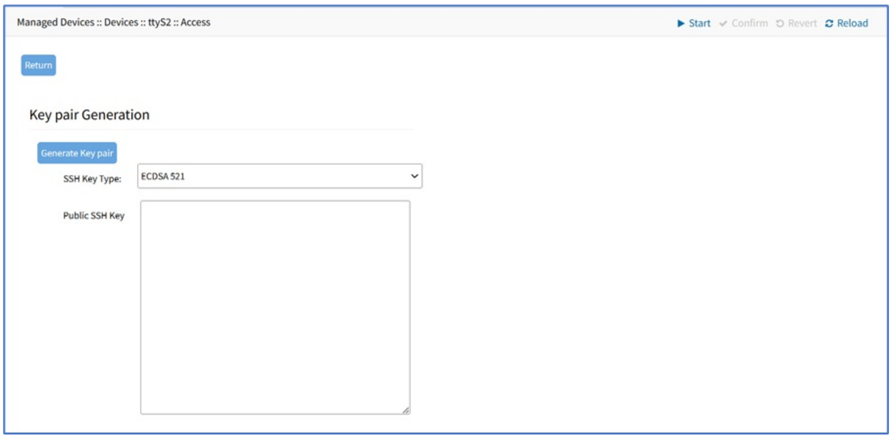
> **NOTE**
>
> Not all devices support this feature.

1. Go to *Managed Devices :: Devices :: <device name> :: Access*.
2. Select **Allow Pre-shared SSH Key** checkbox.
3. Click **Save**.
4. The **SSH Keys** button displays next to the **Save** and **Return** buttons.



Managed Devices :: Devices :: ttyS2 :: Access

5. Click **SSH Keys** (expands dialog).
6. On **SSH Key Type** drop-down, select one (ECDSA 521, ECDSA 384, ECDSA 256, ED25519, DSA 1024, RSA 4096, RSA 2048, RSA 1024).



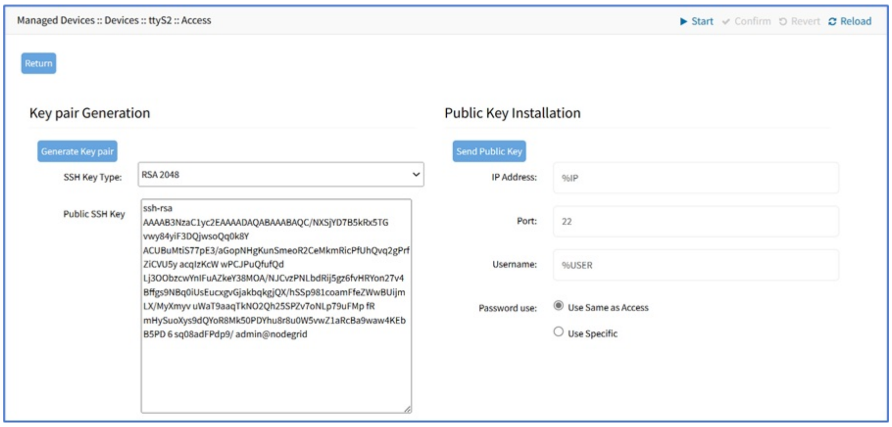
Managed Devices :: Devices :: ttyS2 :: Access

Key pair Generation

SSH Key Type: ECDSA 521

Public SSH Key

7. Click **Generate Key Pair**.



SSH Key Type: RSA 2048

Public SSH Key

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC/NXSjYD7B5kRx5TG
vwy84yiF3DQjwsoQq0k8Y
ACUBuMtiS77pE3/aGopNHgKunSmeoR2CeMkmRicPfUhQvq2gPrf
ZiCVU5y acqIzKcW wPCJPuQfufQd
Lj3OObzcwYnIFuAZkeY38MOA/NJCvzPNLbdRij5gz6fvHRYon27v4
Bffgs9NBq0iUsEucxgvGjakbqkgjQX/hSSp981coamFfeZWwBUijm
LX/MyXmyv uWaT9aaqTkNO2Qh25SPZv7oNLp79uFMp fR
mHySuoXys9dQYoR8Mk50PDYhu8r8u0W5vwZ1aRcBa9waw4KEb
B5PD 6 sq08adFPdp9/ admin@nodegrid
```

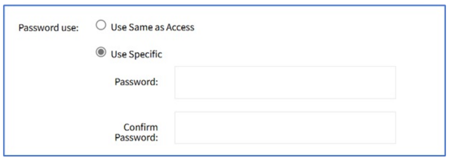
IP Address: %IP

Port: 22

Username: %USER

Password use: ● Use Same as Access ○ Use Specific

8. In *Public Key Installation* menu, enter details:
    a. **IP Address** (default: %IP)
    b. **Port** (default: 22)
    c. **Username** (default: %USER)
    d. On *Passport Use* menu (select one)
        - **Use Same as Access** radio button
        - **Use Specific** radio button (expands dialog), enter **Password** and **Confirm Password**.



Password use: ○ Use Same as Access ● Use Specific

Password:

Confirm Password:

9. **Send Public Key** (sends key to the device). On a connection to a Managed Device with Pre-shared SSH Key enabled, username is still required. If the device fails to authenticate, at the prompt, enter the password. If an error message displays, resolve and click again.

    NOTE

    Not all devices support the **Send Public Key** feature. If not, manually copy the **Public SSH Key** textbox contents to the device.

10. Click **Return** (goes back to the **Access** sub-tab view).

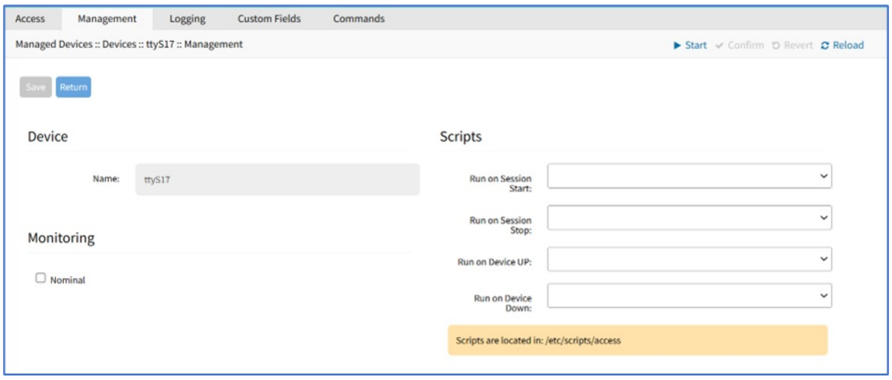
Enable Launch URL with Chrome Forwarder extension

(Chrome browser only) This requires Chrome Forwarder extension. This reduces resource usage by redirecting to a web server. This provides the same behavior as the HTML5 frame. The device’s interface can be viewed in full-screen mode rather than a windowed frame.

Install Chrome Forwarder Extension and Activate

1. Open Google Chrome and go to https://chrome.google.com/webstore/detail/nodegrid-web-access-exten/cmcpkbfnablakhllgdmbhkedpoengpik
2. Click **Add to Chrome**.
3. When the extension is installed, go to *Managed Devices :: Devices :: <device name> :: Access*.
4. Select **Launch URL via Forwarder** checkbox.
5. Click **Save**.

Management sub-tab



Managed Devices :: Devices :: ttyS17 :: Management

Device

Name: ttyS17

Monitoring

□ Nominal

Scripts

Run on Session Start:

Run on Session Stop:

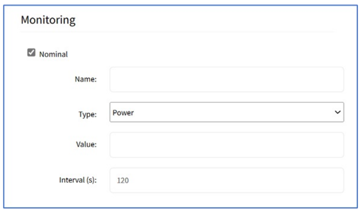
Run on Device UP:

Run on Device Down:

Scripts are located in: /etc/scripts/access

Configure Management of Device

1. Go to *Managed Devices :: Devices :: <device name> :: Management*.
2. On *Device* menu, **Name** is read-only.
3. On *Monitoring* menu, select **Nominal** checkbox (expands dialog).



Monitoring

☑ Nominal

Name:

Type: Power

Value:

Interval (s): 120

   a. Enter **Name.**
   b. On **Type** drop-down, select one (Power, Apparent Power, Current, Voltage, Frequency, etc.).
   c. Enter **Value.**
   d. Enter **Interval (s)** (default: 120).

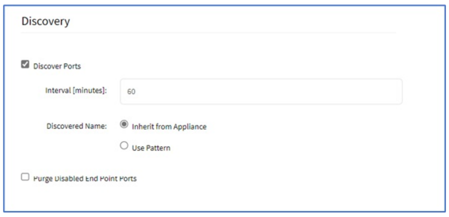
4. In the *Scripts* menu, select an available script for the appropriate device status drop-down list: Copy the scripts to **/etc/scripts/access** folder before assignment to a device status condition. Each script must be executable with user privileges. The customer or a professional services provider can create the custom script.
   a. **Run on Session Start** drop-down, select one
   b. **Run on Session Stop** drop-down, select one
   c. **Run on Device Up** drop-down, select one
   d. **Run on Device Down** drop-down, select one

5. Click **Save**.

Configure Discovery (Appliances only)

This configures the discovery process for the Appliance (i.e., Console Server).

1. Go to *Managed Devices :: Devices :: <device name> :: Management*.
2. Scroll to *Discovery* menu, enter details:



Discovery

☑ Discover Ports

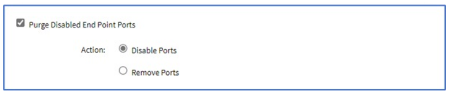
Interval (minutes): 60

Discovered Name: ● Inherit from Appliance ○ Use Pattern

□ Purge Disabled End Point Ports

   a. Select **Discovery Ports** checkbox.
   b. Enter **Set Interval (minutes).**

3. In *Discovered Name* menu, select one:
   a. **Inherit from Appliance** radio button
   b. **Use Pattern** radio button
   c. (optional) **Purge Disabled End Point Ports** checkbox (expands dialog). In *Action* menu, select one:



☑ Purge Disabled End Point Ports

Action: ● Disable Ports ○ Remove Ports

- **Disable Ports** radio button
- **Remove Ports** radio button

4. Click **Save**.

Logging sub-tab

Data logs capture all session information sent and received from a device. This feature is available to log all text-based sessions (serial or SSH-based).

Data Logging and Event Logging can be configured to collect information and create event notifications, based on custom scripts triggered by events. Defined alert strings (simple text match or regular expression pattern) are evaluated against the data source stream (during data collection). Events are generated for each match.

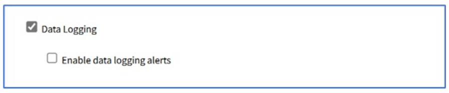
> NOTE
>
> Custom scripts can be created by the customer or a professional services provider.

For data log events, copy scripts to the */etc/scripts/datalog* folder. For event logs, copy scripts to */etc/scripts/events* folder. Each script must be executable with user privileges.

Enable Data Logging and Triggered Alerts

Session data is recorded even if no user is connected. System messages are logged when pushed to console sessions. Location of data logs (local or remote) is based on Auditing settings.

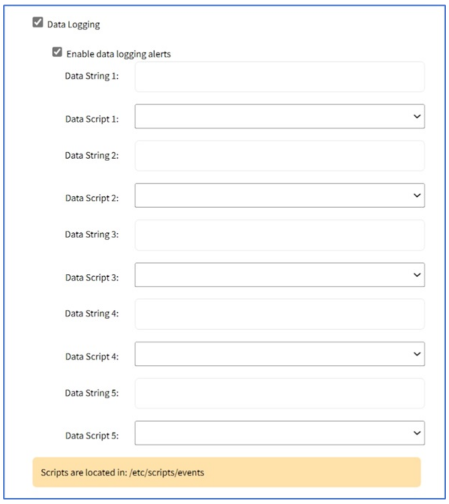
1. Go to *Managed Devices :: Devices :: <device name> :: Logging*.
2. Select **Data Logging** checkbox (expands dialog). Select **Enable data logging alerts** checkbox.



☑ Data Logging

☐ Enable data logging alerts

3. Select **Enable data logging alerts** checkbox (expands dialog).



☑ Data Logging

☑ Enable data logging alerts

Data String 1:

Data Script 1:

Data String 2:

Data Script 2:

Data String 3:

Data Script 3:

Data String 4:

Data Script 4:

Data String 5:

Data Script 5:

Scripts are located in: /etc/scripts/events

   a. Enter **Data String 1** (that triggers alert).
   b. On **Data Script 1** drop-down, select a script that executes on occurrence.

4. Repeat for additional triggers.
5. Click **Save**.

CLI Procedure

1. Go to /settings/devices/<device name>/logging
2. Use the set command to change the data_logging value to yes.
3. Use the set command to change the enable_data_logging_alerts value to yes.
4. Define for data_string_1 string or regular expression which will be matched against the data stream.
5. Define for data_script_1 an available script in case a custom script should be executed.
6. If needed, repeat for data_string_2 and data_script_2.
7. Save the changes with commit

None Copy

```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/logging/
[admin@nodegrid /]#set data_logging=yes
[+admin@nodegrid logging]#set enable_data_logging_alerts=yes
[+admin@nodegrid logging]#set data_string_1="String"
[+admin@nodegrid logging]#set data_script_1=ShutdownDevice_sample.sh
[+admin@nodegrid logging]#commit
```

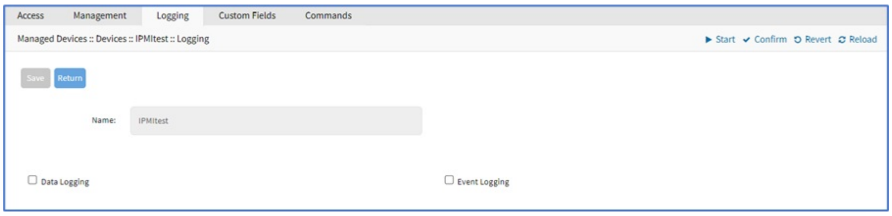
Enable Event Logging and Triggered Alerts

> NOTE
>
> If *Event Logging* does not appear on the **Logging** sub-tab, it is not available on the selected device.

This feature logs events for Service Processor and IPMI sessions. When enabled, the System collects Service Processor Event Log data. The type of collected data depends on the Service Process functions and configuration.

The settings control the interval of collected information (# = 1-999, and time = minutes-hour). Location of data logs (local or remote) is based on *Auditing* section settings.

1. Go to *Managed Devices :: Devices :: <device name> :: Logging*.



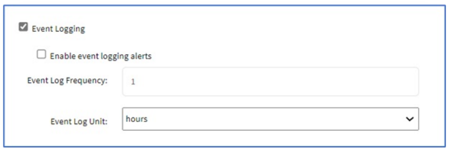
Managed Devices :: Devices :: IPMItest :: Logging

Name: IPMItest

□ Data Logging

□ Event Logging

2. **Event Logging** checkbox (expands dialog).



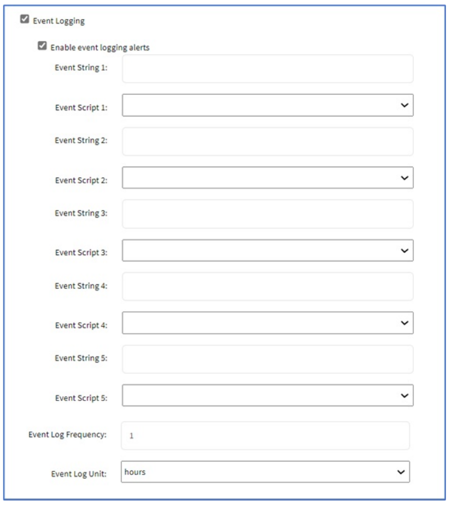
☑ Event Logging

□ Enable event logging alerts

Event Log Frequency: 1

Event Log Unit: hours

3. **Enable Event Logging Alerts** checkbox (expands dialog).



☑ Event Logging

☑ Enable event logging alerts

Event String 1:

Event Script 1:

Event String 2:

Event Script 2:

Event String 3:

Event Script 3:

Event String 4:

Event Script 4:

Event String 5:

Event Script 5:

Event Log Frequency: 1

Event Log Unit: hours

   a. Enter **Event String 1** (that triggers alert)
   b. Select **Event Script 1** drop-down, select one
   c. Repeat for additional triggers.

4. Adjust **Event Log Frequency** (1-9999)
5. On **Event Log Unit** drop-down, select one (hours, minutes).
6. Click **Save**.

CLI Procedure

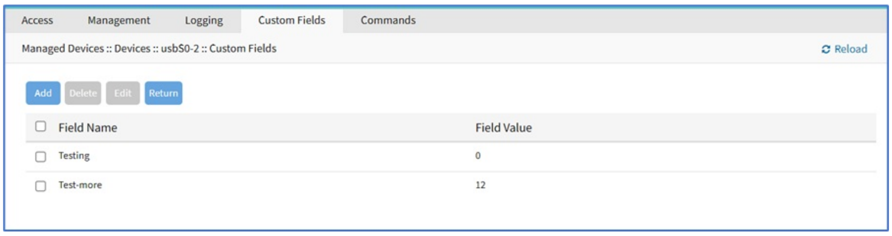
1. Go to /settings/devices/<device name>/logging
2. Use the set command to change the event_logging value to yes
3. Use the set command to adjust event_log_frequency and event_log_unit as needed:
   event_log_frequency range from 1 – 9999
   event_log_unit options hours or minutes
4. Use the set command to change the enable_event_logging_alerts value to yes
5. For event_string_1, define the text string or regular expression (to be matched against the data stream).
6. For event_script_1 define an available script (if a custom script should be executed).
7. As needed, define event_string_2 and event_script_2.
8. Save the changes with commit

None Copy

```
[admin@nodegrid /]# /settings/devices/ipmi/logging/
[admin@nodegrid /]#set event_logging=yes
[+admin@nodegrid logging]#set event_log_frequency=1
[+admin@nodegrid logging]#set event_log_unit=hours
[+admin@nodegrid logging]#set enable_event_logging_alerts=yes
[+admin@nodegrid logging]#set event_string_1="String"
[+admin@nodegrid logging]#set event_script_1=PowerCycleDevice_sample.sh
[+admin@nodegrid logging]#commit
```

Custom Fields sub-tab

Each device type has a collection of commands to access device of that type. Generally, the default configuration is sufficient and is the recommended option.



Managed Devices :: Devices :: usbS0-2 :: Custom Fields

☐	Field Name	Field Value
☐	Testing	0
☐	Test-more	12

As needed, admin users can:

- Disable or change existing commands.
- Enable any (by default) disabled commands.
- Assign custom commands to a device.
- Remove access to specific commands from certain users or groups (with user and group authorization).

Changes to the default command settings affect all users and require careful consideration.

Commands available depend on the device type. For example, the KVM command (enable Service Processor KVM session support) is only available to Service Processor devices. The Outlet command is available to all device types.

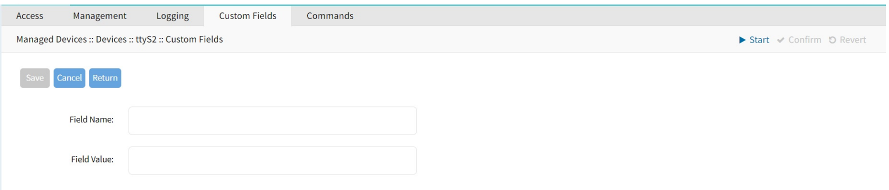
Custom Commands can be created with custom scripts, for all device types. Custom Commands can support for a wide range of different functions (such as additional session options and specific custom device tasks).

NOTE

Custom scripts can be created by the customer or a professional services provider.

Add Custom Field

1. Go to *Managed Devices :: Devices :: <device name> :: Custom Fields*.
2. Click **Add** (displays dialog).



Managed Devices :: Devices :: ttyS2 :: Custom Fields

Field Name:

Field Value:

   a. Enter **Field Name**.
   b. Enter **Field Value**.

3. Click **Save**.

Edit Custom Field

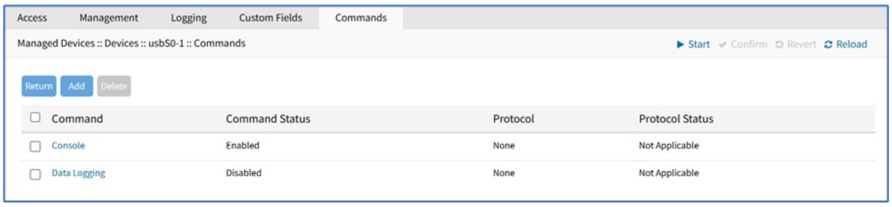
1. Go to *Managed Devices :: Devices :: <device name> :: Custom Fields*.
2. Locate the custom field and select the checkbox.
3. Click **Edit** (displays dialog).
4. Edit the **Field Value**, as needed.
5. Click **Save**.

Delete Custom Field

1. Go to *Managed Devices :: Devices :: <device name> :: Custom Fields*.
2. Locate the custom field and select the checkbox.
3. Click **Delete**.
4. On confirmation dialog, click **OK**.

Commands sub-tab

While Custom Commands can be executed through the WebUI and CLI, feedback and output of Custom Commands is only available on the CLI and not on the WebUI.



Managed Devices :: Devices :: usbS0-1 :: Commands

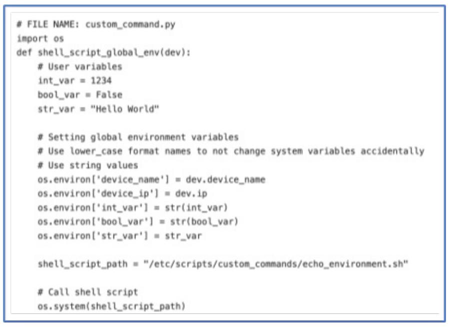
□	Command	Command Status	Protocol	Protocol Status
□	Console	Enabled	None	Not Applicable
□	Data Logging	Disabled	None	Not Applicable

About Custom Scripts

Custom scripts required the following conditions:

- Written in Python
- “Command label” must match a function within the script
- Located in */etc/scripts/custom_commands*

Custom script example



```
# FILE NAME: custom_command.py
import os
def shell_script_global_env(dev):
    # User variables
    int_var = 1234
    bool_var = False
    str_var = "Hello World"

    # Setting global environment variables
    # Use lower_case format names to not change system variables accidentally
    # Use string values
    os.environ['device_name'] = dev.device_name
    os.environ['device_ip'] = dev.ip
    os.environ['int_var'] = str(int_var)
    os.environ['bool_var'] = str(bool_var)
    os.environ['str_var'] = str_var

    shell_script_path = "/etc/scripts/custom_commands/echo_environment.sh"

    # Call shell script
    os.system(shell_script_path)
```

Create Commands

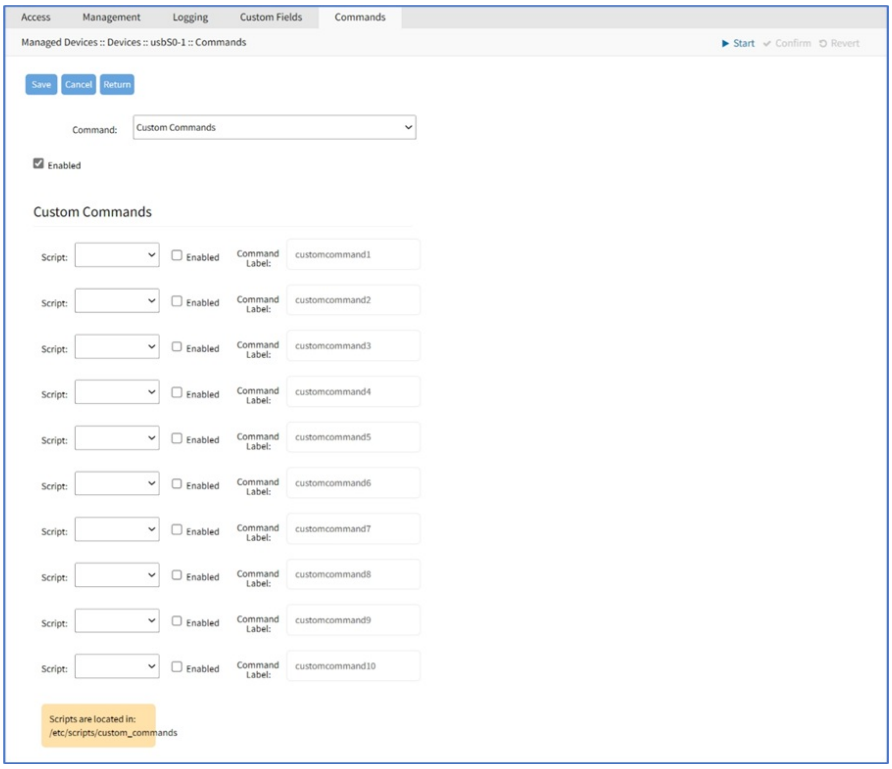
This integrates Out-of-Band and Console-like configurations with the In-Band command.

This can create specific types of commands:

- Custom
- Outlet
- SSH
- Telnet
- Web

Create Custom Command

1. Copy the custom script into */etc/scripts/custom*_commands.
2. Go to *Managed Devices :: Devices :: <device name> :: Commands*.
3. Click **Add**.
4. In **Command** drop-down, select **Custom Commands**.



Managed Devices :: Devices :: usbS0-1 :: Commands

Command: Custom Commands

☑ Enabled

Custom Commands

Script: □ Enabled Command Label: customcommand1

Script: □ Enabled Command Label: customcommand2

Script: □ Enabled Command Label: customcommand3

Script: □ Enabled Command Label: customcommand4

Script: □ Enabled Command Label: customcommand5

Script: □ Enabled Command Label: customcommand6

Script: □ Enabled Command Label: customcommand7

Script: □ Enabled Command Label: customcommand8

Script: □ Enabled Command Label: customcommand9

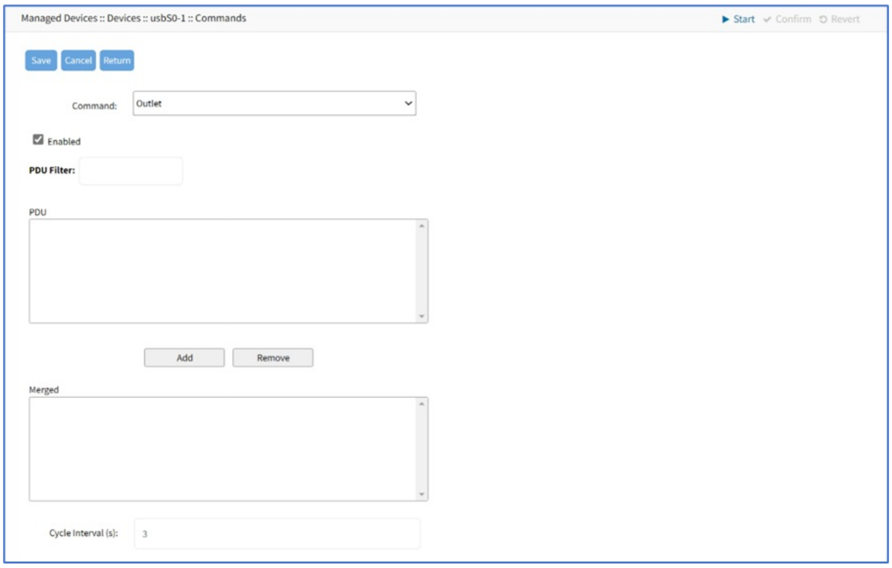
Script: □ Enabled Command Label: customcommand10

Scripts are located in: /etc/scripts/custom_commands

5. Select **Enabled** checkbox.
6. In *Custom Commands* menu:
   a. On **Script** drop-down, select one.
   b. Select **Enabled** checkbox.
   c. Enter **Comment Label** (short description).
7. Repeat, as needed.
8. Click **Save**.

Create Outlet Command

1. Copy the custom script into */etc/scripts/custom*_commands.
2. Go to *Managed Devices :: Devices :: <device name> :: Commands*.
3. Click **Add**.
4. In **Command** drop-down, select **Outlet**.



Managed Devices :: Devices :: usbS0-1 :: Commands

Command: Outlet

☑ Enabled

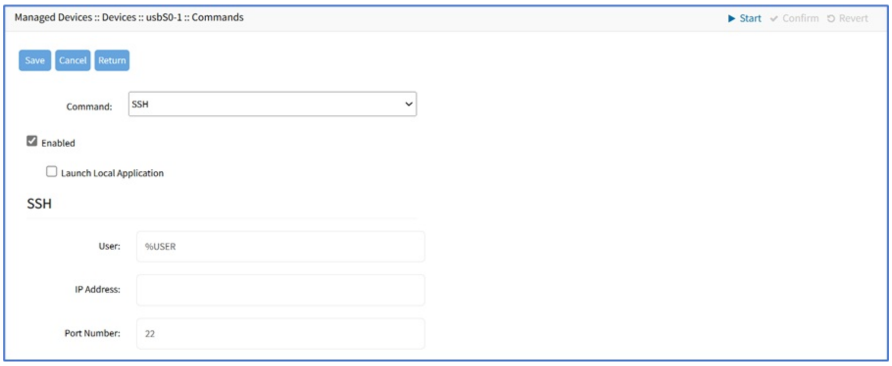
PDU Filter:

Cycle Interval (s): 3

5. Select **Enabled** checkbox.
6. To add, select in **PDU** textbox, click **Add** (moves to **Merged** textbox).
7. To remove, select in **Merged** textbox, click **Remove** (moves to **PDU** textbox).
8. Set **Cycle Interval (s)** (default: 3).
9. Click **Save**.

Create SSH Command

1. Copy the custom script into */etc/scripts/custom*_commands.
2. Go to *Managed Devices :: Devices :: <device name> :: Commands*.
3. Click **Add**.
4. In **Command** drop-down, select **SSH**.


Managed Devices :: Devices :: usbS0-1 :: Commands
▶ Start ✓ Confirm ↻ Revert
Save
Cancel
Return

Command: SSH

☑ Enabled

□ Launch Local Application

SSH

User: %USER

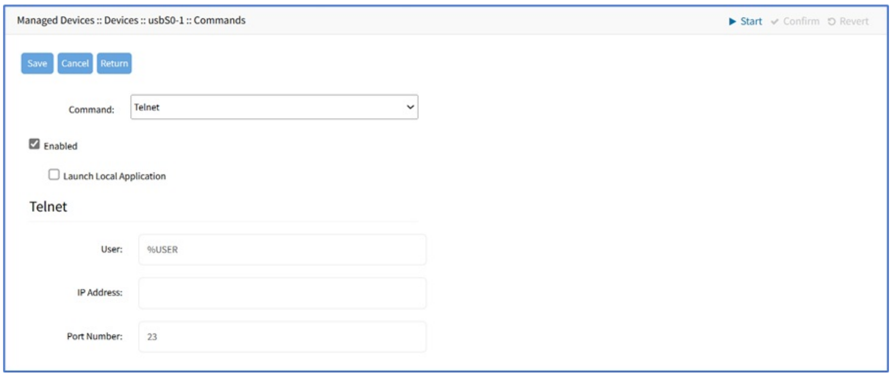
IP Address:

Port Number: 22

5. Select **Enabled** checkbox.
6. Select **Launch Local Application**.
7. In *SSH* menu, enter:
    a. **User**
    b. **IP Address**
    c. **Port Number** (default: 22)
8. Click **Save**.

Create Telnet Command

1. Copy the custom script into */etc/scripts/custom*_commands.
2. Go to *Managed Devices :: Devices :: <device name> :: Commands*.
3. Click **Add**.
4. In **Command** drop-down, select **Telnet**.


Managed Devices :: Devices :: usbS0-1 :: Commands
▶ Start ✓ Confirm ↻ Revert
Save
Cancel
Return

Command: Telnet

☑ Enabled

□ Launch Local Application

Telnet

User: %USER

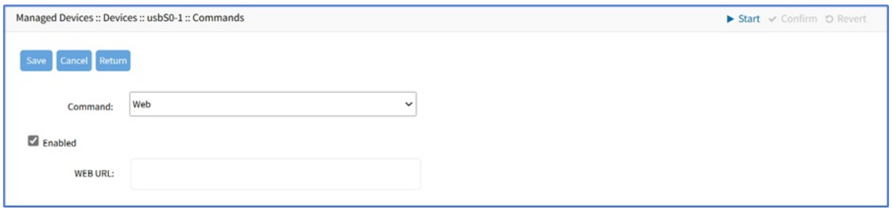
IP Address:

Port Number: 23

5. Select **Enabled**. checkbox.
6. Select **Launch Local Application**.
7. In *Telnet* menu, enter:
    a. **User**
    b. **IP Address**
    c. **Port Number** (default: 22)
8. Click **Save**.

Create Web Command

1. Copy the custom script into */etc/scripts/custom*_commands.
2. Go to *Managed Devices :: Devices :: <device name> :: Commands*.
3. Click **Add**.
4. In **Command** drop-down, select **Web**.


Managed Devices :: Devices :: usbS0-1 :: Commands
▶ Start ✓ Confirm ↻ Revert
Save
Cancel
Return

Command: Web

☑ Enabled

WEB URL:

    a. Select **Enabled**.
    b. Enter **WEB URL**
5. Click **Save**.

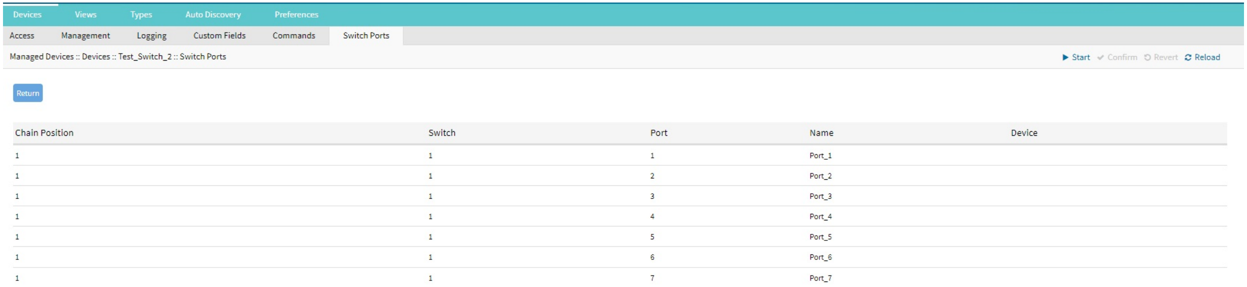
Device Access via RDP

1. Go to *Managed Devices :: Devices :: <device name> :: Commands*.
2. Click **Add** (displays dialog).
3. In **Command** drop-down, select **KVM**.
    a. Select **Enabled** checkbox.
    b. On **Protocol** drop-down, select one.
    c. On **Type Extension** drop-down, select one.
4. Click **Save**.

Switch Port tab

Switch Port tab

When you add a Switch, like other devices it is listed on the **Managed Devices** :: **Devices** page. When you click the name link, the **Switch Port** tab appears next to the **Command** tab. This tab is displayed only when the device family is Switch. On this tab you can view the port related details as shown in the following image:



Managed Devices :: Devices :: Test_Switch_2 :: Switch Ports

Chain Position	Switch	Port	Name	Device
1	1	1	Port_1	
1	1	2	Port_2	
1	1	3	Port_3	
1	1	4	Port_4	
1	1	5	Port_5	
1	1	6	Port_6	
1	1	7	Port_7	

You can view the following details related to a switch:

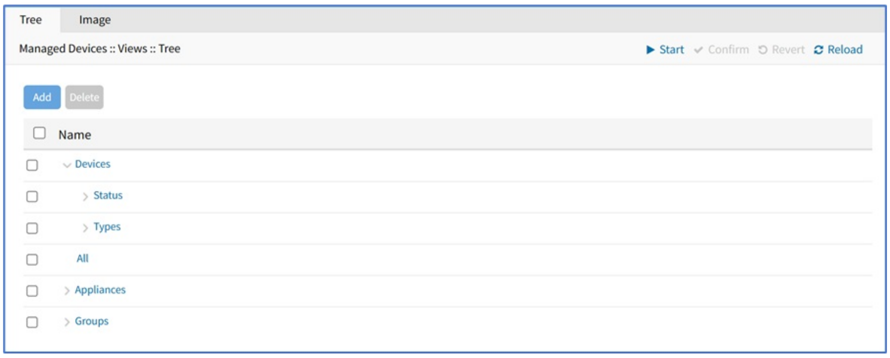
- **Chain position**: if the switch is connected to other switches
- **Switch**: Indicates the Switch ID
- **Port**: Number of switch ports
- **Name**: Name of the switch port
- **Devices**: The devices connected to the switch port

Views tab

On this page, an admin can create and manage a device-based tree structure. This can be configured for specific organizational or physical structure layouts. Groups may also be used to aggregate monitoring values like a rack or room level.

Trees Sub-tab

This displays the tree structure. On first opening, the root locations are shown.

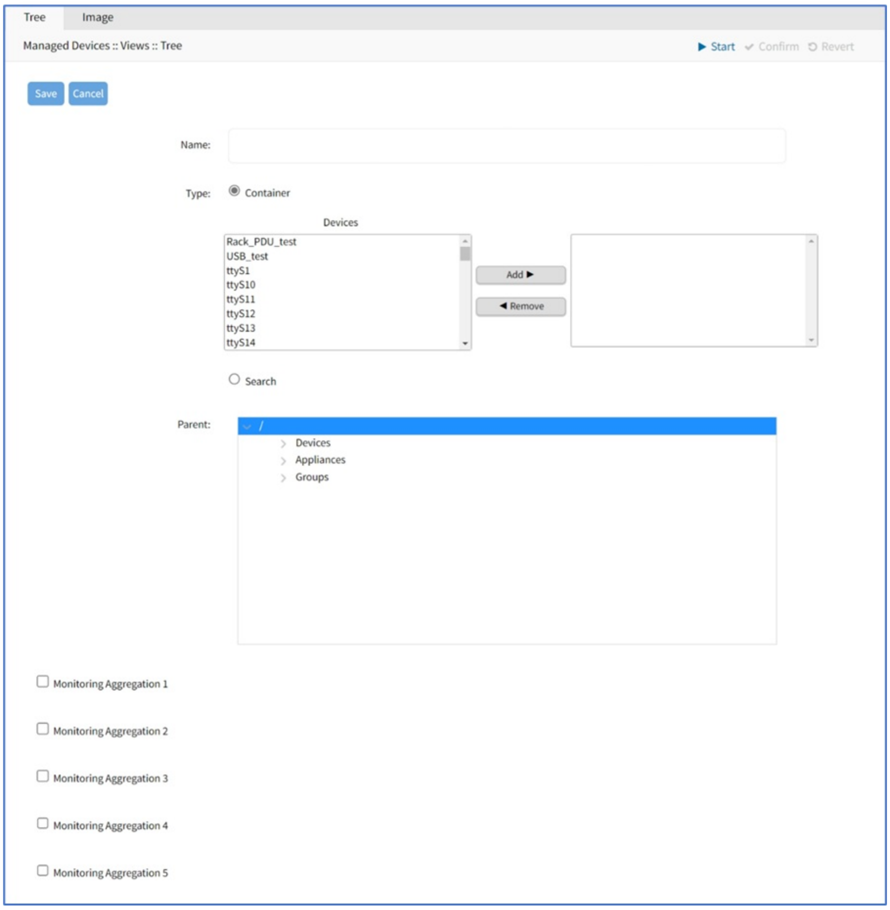


View Tree Branches

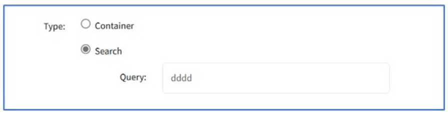
1. Click the right arrow ▷ icon to display the next branch level.
2. If further branch levels are available, expand the branch.
3. To contract the branch, click the down arrow icon.

Add a Branch Item

1. Go to *Managed Devices :: Views :: Tree*.
2. Click **Add** (displays dialog).

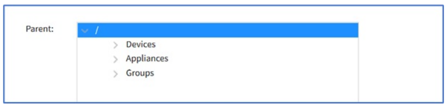


3. Enter **Name.**
4. In *Type* menu, select one:
   - **Container** radio button. In *Devices* panel, select from left-side panel, click **Add►** to move to right-side panel. To remove from right-side panel, select, and click **◄Remove**.
   - **Search** radio button (expands dialog). Enter **Query** to locate and select.

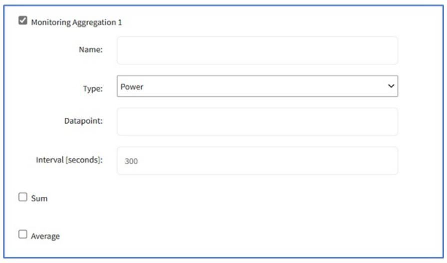


Query: dddd

5. To select a **Parent**, click on the solid bar, expand the tree to locate the parent for this addition.



6. Select **Monitoring Aggregation** checkbox (expands dialog).



Type: Power

Interval (seconds): 300

a. Enter **Name.**

b. On **Type** drop-down, select one (Power, Apparent Power, Power Factor, Current, Voltage, Frequency, Temperature, Humidity, Fan Speed, Time Left, Counter, Percent).
c. Enter **Datapoint.**
d. Set **Interval (seconds)** (default: 300).
e. Select **Sum** checkbox.
f. Select **Average** checkbox.
(as needed) Repeat for other **Aggregations**.

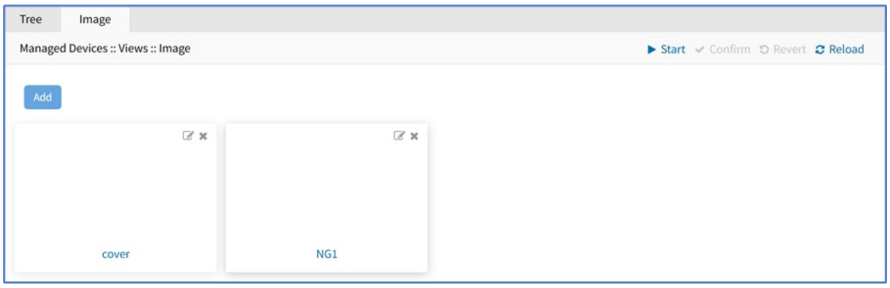
7. When done, click **Save**.

Delete a Branch Item

1. Go to *Managed Devices :: Views :: Tree*.
2. Expand tree to locate item.
3. Select checkbox.
4. Click **Delete**.
5. On confirmation dialog, click **OK**.

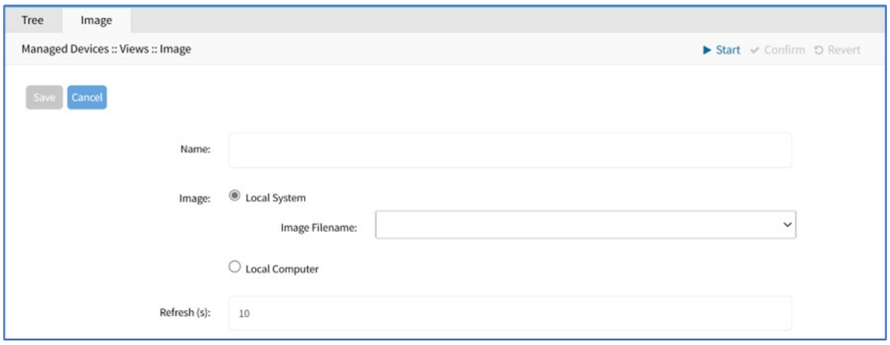
Image Sub-Tab

Available images are shown on this page.



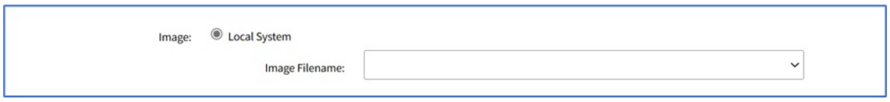
Add Image

1. Go to *Managed Devices :: Views :: Image*.
2. Click **Add** (displays dialog).

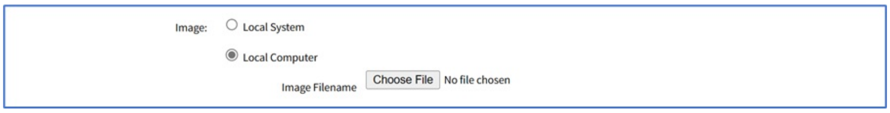


Refresh (s): 10

3. Enter **Name**.
4. In *Image* menu, select one:
- **Local System** radio button, select from the **Image Filename** drop-down.



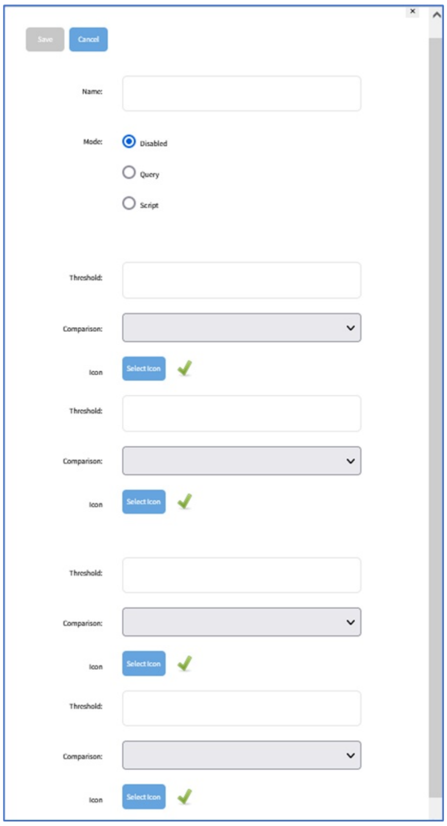
- **Local Computer** radio button. Click **Choose File**, then locate and select the graphic file.



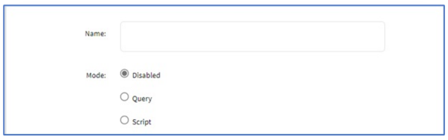
5. In **Refresh**, enter value (seconds).
6. Click **Save**.

Add Image Property Details

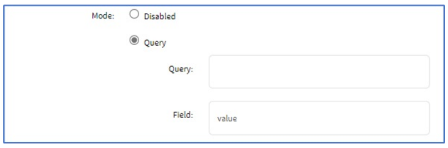
1. Go to *Managed Devices :: Views :: Image*.
2. Click on an image (displays dialog).
3. Right-click on the image (displays properties dialog).



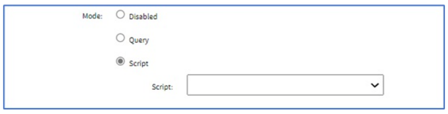
4. Enter **Name**.
5. In *Mode* menu, select one:
   - **Disabled** radio button (dialog expands).



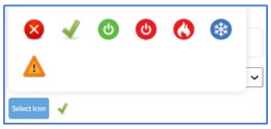
   - **Query** radio button (dialog expands). Enter **Query**. Enter **Field**.



   - **Script** radio button (dialog expands). On **Script** drop-down, select one.



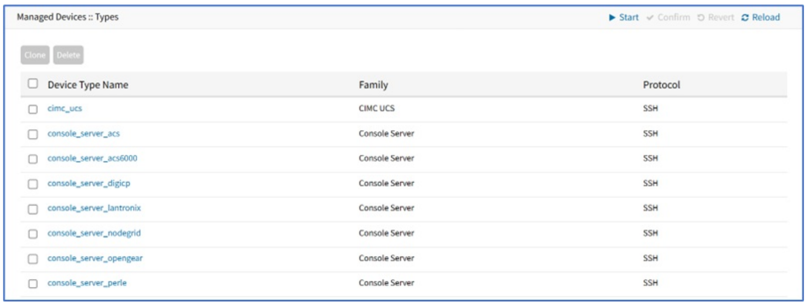
6. In *Threshold* menu, enter details:
   a. Enter **Threshold** value.
   b. On **Comparison** drop-down select one.
   c. On **Icon**, select from the pop-up dialog.



7. (as needed) Enter details for another Threshold (up to 4).
8. Click **Save**.

Types tab

Administrators can manage Device Type settings for customized versions of existing device types. There are situations when the device type default value does not match with customer's default values. The admin can clone, edit, or delete existing device types. Settings can be adjusted as needed. When saved, new settings are immediately effective for all devices with that device type.

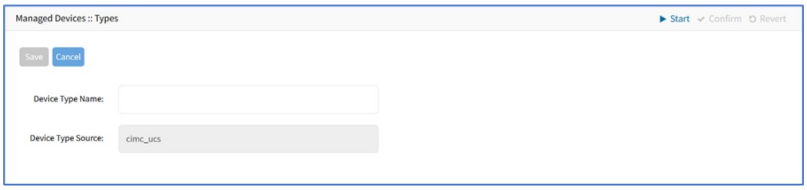


□ Device Type Name	Family	Protocol
□ cimc_ucs	CIMC UCS	SSH
□ console_server_acs	Console Server	SSH
□ console_server_acs6000	Console Server	SSH
□ console_server_digicp	Console Server	SSH
□ console_server_lantronix	Console Server	SSH
□ console_server_nodegrid	Console Server	SSH
□ console_server_opengear	Console Server	SSH
□ console_server_perle	Console Server	SSH

Manage Device Types

Clone Device Type

1. Go to *Managed Devices :: Types*.
2. Locate and select the checkbox of the type to be cloned.
3. Click **Clone** (displays dialog).



Device Type Name:

Device Type Source: cimc_ucs

4. Enter **Device Type Name**.
5. Click **Save**.

Clone Validation

Ensure the source device is correctly configured. After the clone is created, use this verification process:

1. Access the clone to verify username, password and IP address is correct.
2. Audit the log files to verify data logging and event logging settings are correct.
3. Simulate events and check if any notification is created.
4. Verify events are detected on the data and event logs.
5. Verify that the device is in the correct authorization group with proper access rights.

Edit Device Type

1. Go to *Managed Devices :: Types*.
2. In the *Device Type Name* column, locate and click on the name.
3. On the dialog, modify details as needed:
4. Click **Save**.

Delete Device Type

1. Go to *Managed Devices :: Types*.
2. Locate and select the checkbox to be deleted.
3. Click **Delete**.
4. On the confirmation dialog, click **OK**.

Configuring Auto Discovery

The System automatically discovers and adds network devices, enabled ports on console servers, KVM switches, and VMware (virtual serial ports and virtual machines). This section describes the following device auto-discovery processes:

- Auto Discovery: Configuration Process
- Auto Discovery: Configure Console Server
- Auto Discovery: Configure Network Devices
- Auto Discovery: Configure Virtual Machines
- Auto Discovery: Configure DHCP Clients

Auto Discovery: Configuration Process

This is the process of configuring auto-discovery on various devices.

1. Create a template device. (For each device type, a template device must be created.)
   Clone is recommended. The template needs to include all the settings for an end device, except connection details to the discovered devices.
2. For network devices, create a Network Scan.
3. For virtual machines, create a Virtual Manager.
4. For all devices, create a Discovery Rule.
   Discovery rules must be associated with the template device. These rules determine the action taken on every discovered device.
5. Start the discovery process.
   This process automatically starts when a device is added to the Nodegrid Platform. A manual discovery process can be started from the WebUI (*Managed Devices :: Auto Discovery :: Discover Now*) or CLI (/settings/auto_discovery/discover_now/).

Auto Discovery: Configure Console Server

The Console Server appliances can be discovered using the Network Devices process. Use the Auto Discovery process to automatically add and configure managed devices for third-party console server ports and KVM switch ports.

Step 1 – Create a Template Device

The template device must be created first. In this process, only enter the details listed.

1. Go to *Managed Devices :: Devices*.
2. Click **Add**.
3. On the *Add* dialog, enter **Name** (of the template).
4. On **Type** drop-down, select one (console_server_acs, console_server_acs6000, console_server_lantronix, console_server_opengear, console_server_digicp, console_server_raritan, console_server_perle).
5. For **IP Address**, enter **127.0.0.1**
6. Select **Ask During Login** checkbox
7. On *End Point*menu, select one
    - **Serial Port** radio button
    - **KVM Port** radio button
    - **Port Number**
8. On **Mode** drop-down, select **Disabled** (ensures the device is not displayed on the *Access* page).
9. Click **Save**.

CLI Procedure

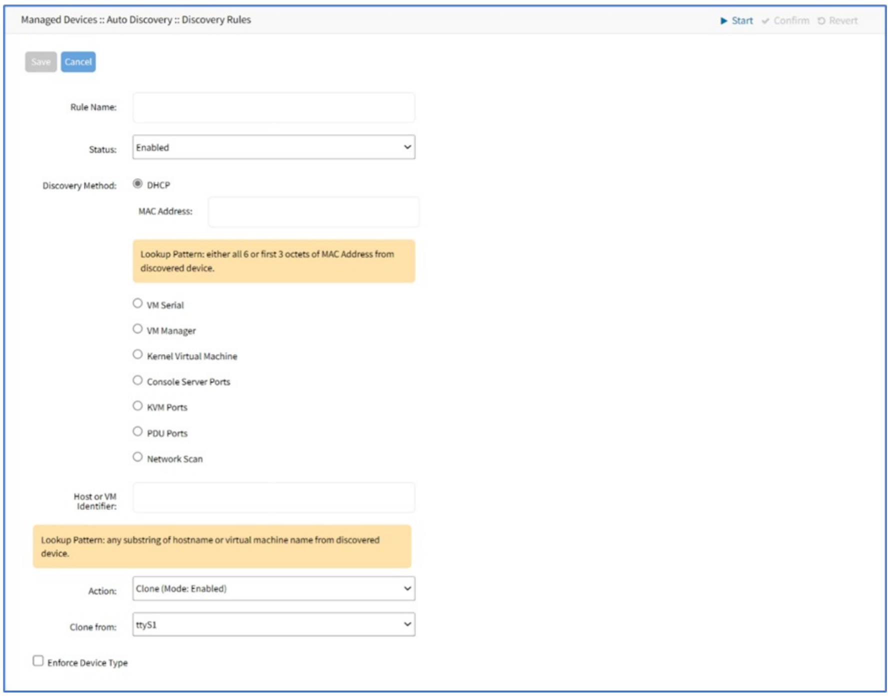
1. Go to /settings/devices
2. Use the add command to create a new device.
3. Use the set command to define the following:
name
type (console_server_acs, console_server_acs6000, console_server_lantronix, console_server_opengear, console_server_digicp, console_server_raritan, console_server_perle)
ip_address as 127.0.0.1
Set credential to Ask During Login
endpoint (serial_port or kvm_port)
port_number (port number)
Set mode to disabled
4. Save the changes with commit.

None Copy

```
[admin@nodegrid /]# cd /settings/devices
[admin@nodegrid devices]# add
[admin@nodegrid {devices}]# set name=Console_Server_Port_Template
[admin@nodegrid {devices}]# set type=console_server_acs6000
[admin@nodegrid {devices}]# set ip_address=127.0.0.1
[admin@nodegrid {devices}]# set end_point=serial_port
[admin@nodegrid {devices}]# set port_number=1
[admin@nodegrid {devices}]# set credential=ask_during_login
[admin@nodegrid {devices}]# set mode=disabled
[admin@nodegrid {devices}]# commit
```

Step 2 – Create a Discovery Rule

1. Go to *Managed Devices :: Auto Discovery :: Discovery Rules*.
2. Click **Add** (displays dialog).



Status: Enabled

Discovery Method: ● DHCP

MAC Address:

Lookup Pattern: either all 6 or first 3 octets of MAC Address from discovered device.

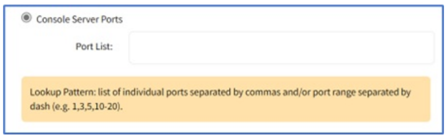
Lookup Pattern: any substring of hostname or virtual machine name from discovered device.

Action: Clone (Mode: Enabled)

Clone from: ttyS1

3. Enter **Rule Name**

4. On **Status** drop-down, select one (Enabled, Disabled)
5. On *Discovery Method*menu, select one:
    - **Console Server Ports** radio button. Enter **Port List** (list of ports to scan (i.e., 1,3,5,10-20).

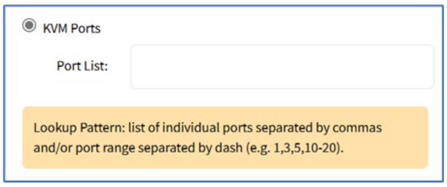


● Console Server Ports

Port List:

Lookup Pattern: list of individual ports separated by commas and/or port range separated by dash (e.g. 1,3,5,10-20).

    - **KVM Ports** radio button. Enter **Port List** (list of ports to scan (i.e., 1,3,5,10-20).



● KVM Ports

Port List:

Lookup Pattern: list of individual ports separated by commas and/or port range separated by dash (e.g. 1,3,5,10-20).

6. (optional) In *Host or VM Identifier* menu, enter parameter to further filter (if provided, part of port name must match value).
7. On **Action** drop-down, select what to do when a new device is discovered: Clone (Mode: Enabled), Clone (Mode: On-Demand), Clone (Mode: Discovered), Discard Discovered Devices.
8. On **Clone from** drop-down, select the template device (created earlier).
9. Click **Save**.

After the appliance is created, the Nodegrid Platform automatically starts discovering attached devices (based on the created Discovery Rules).

This process takes several minutes.

CLI Procedure

1. Go to /settings/auto_discovery/discovery_rules/
2. Use the add command to create a Discovery Rule.
3. Use the set command to define the following settings:
rule_name (for the Discovery Rule)
status for the rule (enabled, disabled)
method set to console_server_ports or kvm_ports
port_list (list of ports which should be scanned – i.e., 1,3,5,10-20)
host_identifier parameter (apply as a filter) (If a value is provided, part of the port name must match the value.)
4. For action (enter action taken when a new device is discovered) (clone_mode_enabled, clone_mode_on-demand, clone_mode_discovered, discard_device).
5. clone_from (template device created earlier).
6. Save the changes with commit.

None Copy

```
[admin@nodegrid /]# cd /settings/auto_discovery/discovery_rules/
[admin@nodegrid discovery_rules]# add
[admin@nodegrid {discovery_rules}]# set rule_name=Console_Server_Ports
[admin@nodegrid {discovery_rules}]# set status=enabled
[admin@nodegrid {discovery_rules}]# set method=console_server_ports
[admin@nodegrid {discovery_rules}]# set port_list=1-48
[admin@nodegrid {discovery_rules}]# set action=clone_mode_enabled
[admin@nodegrid {discovery_rules}]# set clone_from=Console_Server_Ports_Template
[admin@nodegrid {discovery_rules}]# commit
```

After the appliance was created, the Nodegrid Platform automatically starts discovery of attached devices based on the created Discovery Rules.

This process takes several minutes.

Auto Discovery: Configure Network Devices

Network appliances can be automatically discovered and added to the Nodegrid Platform. This includes appliances which support Telnet, SSH, ICMP, Console Servers, KVM Switches or IMPI protocols plus others.

Appliances can be discovered through various methods, in combination or singly:

- Similar Devices (select one of the devices from the drop-down)
- Port Scan and enter a list of ports in the Port List field,
- Ping
- DHCP (via MAC Address)

Setup is a three-step process.

Step 1 – Create a Template Device

The template device must be created first. In this process, only enter the details listed.

1. Managed Devices :: Devices.
2. Click **Add**.
3. On *Add* dialog, enter **Name** (of the template).
4. On **Type** drop-down, select one (device_console, ilo, imm, drac, idrac6, ipmi1.5, impi2.0, ilom, cimc_ucs, netapp, infrabox, pdu)..
5. On **IP Address**, enter **127.0.0.1.**

6. Enter **Username**, **Password** and **Confirm Password.**
   Alternatively, select **Ask During Login** checkbox (user credentials are entered during login).
7. On **Mode** drop-down, select **Disabled** (ensures the device is not displayed on the Access page).
8. Click **Save**.

CLI Procedure

1. Go to /settings/devices
2. Use the add command to create a new device.
3. Use the set command to define the following settings:
   a. name
   b. type (device_console, ilo, imm, drac, idrac6, ipmi1.5, impi2.0, ilom, cimc_ucs, netapp, infrabox, pdu*)
   c. ip_address as 127.0.0.1
   d. username and password (of the device) or set credential ask_during_login
   e. set mode to disabled

4. Save the changes with commit.

None Copy

```
[admin@nodegrid /]# cd /settings/devices
[admin@nodegrid devices]# add
[admin@nodegrid {devices}]# set name=Network_Template
[admin@nodegrid {devices}]# set type=device_console
[admin@nodegrid {devices}]# set ip_address=127.0.0.1
[admin@nodegrid {devices}]# set credential=ask_during_login

or

[admin@nodegrid {devices}]# set credential=set_now
[admin@nodegrid {devices}]# set username=admin password=admin

[admin@nodegrid {devices}]# set mode=disabled
[admin@nodegrid {devices}]# commit
```

1. ### Step 2 – Create a Network Scan
2. Go to *Managed Devices :: Auto Discovery :: Network Scan*.
3. Click **Add**.
4. On *Add* dialog, enter **Name** (of Scan ID).
5. Enter **IP Range Start** and **IP Range End.**
6. Select **Similar Devices** checkbox.
   - On **Device** drop-down, select an existing template (to identify devices).

7. Select **Enable Scanning** checkbox.
8. Select **Port Scan** checkbox.
9. Enter **Port List** (ports to be scanned, i.e., “2”, “3,104”, 11-20).
10. Select **Ping** checkbox (enables Ping function).
11. On **Scan interval (in minutes)**, enter a value.
12. Click **Save**.

CLI Procedure

1. Go to /settings/auto_discovery/network_scan/
2. Use the add command to create a Network Scan.
3. Use the set command to define the following settings:
   scan_id (name for the Network Scan)
   ip_range_start and ip_range_end (define a network range to be scanned)
   Set enable_scanning to yes to enable the scan

4. Define one or more of the three scan methods:
   similar_devices (set device to match one of the existing devices or templates
   port_scan (set to yes)
   set port_list (to a list of ports reachable on the device)
   ping (no further settings are required)
5. Set scan_interval (when to scan, in minutes).
6. Save the changes with commit.

None Copy

```
[admin@nodegrid /]# cd /settings/auto_discovery/network_scan/
[admin@nodegrid network_scan]# add
[+admin@nodegrid {network_scan}]# set scan_id=SSH_Console
[+admin@nodegrid {network_scan}]# set ip_range_start=192.168.10.1
[+admin@nodegrid {network_scan}]# set ip_range_end=192.168.10.254
[+admin@nodegrid {network_scan}]# set enable_scanning=yes
[+admin@nodegrid {network_scan}]# set similar_devices=yes
[+admin@nodegrid {network_scan}]# set device= network_template
[+admin@nodegrid {network_scan}]# set port_scan=yes
[+admin@nodegrid {network_scan}]# set port_list=22
[+admin@nodegrid {network_scan}]# set ping=no
[+admin@nodegrid {network_scan}]# set scan_interval=100
[+admin@nodegrid {network_scan}]# commit
```

Step 3 – Create a Discovery Rule

1. Go to *Managed Devices :: Auto Discovery :: Discovery Rules*.
2. Click **Add**.
3. On the *Add* dialog, enter **Name** (of the Discovery Rule).
4. On **Status** drop-down, select (Enabled, Disabled).
5. On *Discovery Method* menu, select **Network Scan** checkbox.
6. On **Scan ID** drop-down, select the created Network Scan ID.
7. (optional) In *Host or VM Identifier* menu, enter parameter to further filter (if provided, part of port name must match value).
8. On **Action** drop-down, select what to do when a new device is discovered (Clone (Mode: Enabled), Clone (Mode: On-Demand), Clone (Mode: Discovered), Discard Discovered Devices).
9. On **Clone from** drop-down, select the template device created earlier.
10. Click **Save**.

The Nodegrid Platform automatically starts discovering devices, based on the created Discovery Rules.

This process takes several minutes.

CLI Procedure

1. Go to /settings/auto_discovery/discovery_rules/
2. Use the add command to create a Discovery Rule.
3. Use the set command to define the following settings:
   rule_name for the Discovery Rule
   status for the discovered rule (enabled, disabled)
   method set to network_scan
   scan_id select a Network Scan ID created earlier
   host_identifier parameter to further filer, if provided - part of the port name must match the value)
4. For action, select what should be done on a new device discovery (clone_mode_enabled, clone_mode_on-demand, clone_mode_discovered, discard_device).
5. clone_from set to the template device created earlier.
6. Save the changes with commit.

None Copy

```
[admin@nodegrid /]# cd /settings/auto_discovery/discovery_rules/
[admin@nodegrid discovery_rules]# add
[admin@nodegrid {discovery_rules}]# set rule_name=Network_Scan
[admin@nodegrid {discovery_rules}]# set status=enabled
[admin@nodegrid {discovery_rules}]# set method=network_scan

[admin@nodegrid {discovery_rules}]# set scan_id=SSH_Console
[admin@nodegrid {discovery_rules}]# set action=clone_mode_enabled
[admin@nodegrid {discovery_rules}]# set clone_from=Network_Template
[admin@nodegrid {discovery_rules}]# commit
```

The Nodegrid Platform automatically starts discovering devices, based on the created Discovery Rules.

This process takes several minutes.

Auto Discovery: Configure Virtual Machines

Virtual Machines which are managed by VMWare vCenter or run on ESXi can be discovered and managed directly on Nodegrid. The process will regularly scan vCenter or the ESXi host and detect newly added Virtual Machines. The virtual machines can be added as type virtual_console_vmware or virtual_serial_port.

> **NOTE**
>
> The free version of ESXi is not supported.

Step 1 – Create a Template Device

The device must be created first. In this process, only enter the details listed.

1. Go to *Managed Devices :: Devices*.
2. Click **Add.**
3. On *Add* dialog, enter **Name** (of the template).
4. On **Type** drop-down, select **virtual_console_vmware**
5. Enter **IP Address**, enter **127.0.0.1**
6. Enter **Username**, **Password** and **Confirm Password.**
   Alternatively, select **Ask During Login** checkbox (user credentials are entered during login).
7. Select **Mode Disabled** checkbox (ensures device is not displayed on *Access* page).
8. Click **Save**.

CLI Procedure

1. Go to /settings/devices
2. Use the add command to create a new device.
3. Use the set command to define the following settings:
   name
   type (virtual_console_vmware)
   ip_address as 127.0.0.1
   set mode to disabled
4. Save the changes with commit.

None Copy

```
[admin@nodegrid /]# cd /settings/devices
[admin@nodegrid devices]# add
[admin@nodegrid {devices}]# set name=Virtual_Machine_Template
[admin@nodegrid {devices}]# set type=virtual_console_vmware
[admin@nodegrid {devices}]# set ip_address=192.168.2.151
[admin@nodegrid {devices}]# set mode=disabled
[admin@nodegrid {devices}]# commit
```

Step 2 – Create a Discovery Rule

1. Go to *Managed Devices :: Auto Discovery :: Discovery Rules*.
2. Click **Add**.
3. On *Add* dialog, enter **Rule Name.**
4. On **Status** drop-down, select an item (Enabled, Disabled).
5. In *Discovery Method* menu, select **VM Manager.**
6. (optional) To filter the scan, enter **Datacenter** and **Cluster.**
7. (optional) In *Host or VM Identifier* menu, enter parameter to further filter (if provided, part of port name must match value).
8. On **Action** drop-down, select what to do when a new device is discovered - Clone (Mode: Enabled), Clone (Mode: On-Demand), Clone (Mode: Discovered), Discard Discovered Devices.
9. On **Clone from** drop-down, select the template device created earlier.
10. Click **Save**.

CLI Procedure

1. Go to /settings/auto_discovery/discovery_rules/
2. Use the add command to create a Discovery Rule.
3. Use the set command to define the following settings:
   rule_name for the Discovery Rule
   status for the discovered rule (enabled, disabled)
   method set to vm_manager
   Use datacenter and cluster to define filters based on Data Center and or Cluster
   host_identifier parameter (apply as a filter) (If a value is provided, part of the port name must match the value.)
4. For action (enter action taken when a new device is discovered) (clone_mode_enabled, clone_mode_on-demand, clone_mode_discovered, discard_device).
5. clone_from (template device created earlier).
6. Save the changes with commit.

None Copy

```
[admin@nodegrid /]# cd /settings/auto_discovery/discovery_rules/
[admin@nodegrid discovery_rules]# add
[admin@nodegrid {discovery_rules}]# set rule_name=Virtual_Machine
[admin@nodegrid {discovery_rules}]# set status=enabled
[admin@nodegrid {discovery_rules}]# set method=vm_manager
[admin@nodegrid {discovery_rules}]# set action=clone_mode_enabled
[admin@nodegrid {discovery_rules}]# set clone_from=Vitual_Machine_Template
[admin@nodegrid {discovery_rules}]# commit
```

Step 3 – Define a VM Manager

1. Go to *Managed Devices :: Auto Discovery :: VM Managers*.
2. Click **Add**.
3. On *Add* dialog, on **VM Server**, enter the vCenter/ESXi IP or FQDN.
4. Enter **Username.**
5. On **Virtualization Type** drop-down, select **VMware.**
6. Enter **Password** and **Confirm Password.**
7. Enter **HTML console port** (if needed).
8. Click **Save**.

The Nodegrid Platform connects to the vCenter or ESXi system.

This process takes several minutes.

CLI Procedure

1. Go to /settings/auto_discovery/vm_managers/
2. Use the add command to create a VM Manager.
3. Use the set command to define the following settings:
   vm_server (vCenter/ESXi IP or FQDN)
   Define username and password
   Adjust the html_console_port (if needed)
4. Save the changes with commit.

None Copy

```
[admin@nodegrid /]# cd /settings/auto_discovery/vm_managers/
[admin@nodegrid vm_managers]# add
[admin@nodegrid {vm_managers}]# set vm_server=vCenter
[admin@nodegrid {vm_managers}]# set username=admin
[admin@nodegrid {vm_managers}]# set password=password
[admin@nodegrid {vm_managers}]# commit
```

The Nodegrid Platform connects to the vCenter or ESXi system.

This process takes several minutes.

Step 4 – Enable Discover Virtual Machines

1. Click on the newly created and connected VM Manager.
2. Select **Discover Virtual Machines** checkbox.
3. On **Discovery Polling Interval (minutes)**, enter a value.
4. Click **Save**.

CLI Procedure

1. Log into the newly created VM Manager
2. Enable Discover Virtual Machines option.
3. Define the Data Center and Discovery Polling Interval.
4. Save the changes with commit.

None Copy

```
[admin@nodegrid 192.168.2.217]# set html_console_port=7331,7343
[admin@nodegrid 192.168.2.217]# set discover_virtual_machines=yes
[admin@nodegrid 192.168.2.217]# set interval_in_minutes=15
[admin@nodegrid 192.168.2.217]# set discovery_scope=Demo-DC!
[admin@nodegrid 192.168.2.217]# commit
```

Auto Discovery: Configure DHCP Clients

The Nodegrid Platform can be used as a DHCP Server for Clients within the management network. These devices can be automatically discovered and added to the Nodegrid platform. This feature only supports DHCP Clients that receive DHCP lease from the local Nodegrid Platform.

Step 1 – Create a Template Device

1. Go to *Managed Devices :: Devices.*
2. Click **Add** .
3. Enter **Name** (of the template).
4. For **IP Address**, enter **127.0.0.1**
5. On **Type** drop-down, select one (device_console, ilo, imm, drac, idrac6, ipmi1.5, impi2.0, ilom, cimc_ucs, netapp, infrabox, pdu*).
6. Enter **Username**, **Password** and **Confirm Password.**
   Alternatively, **Ask During Login** checkbox (user credentials are entered during login).
7. Select **Mode Disabled** checkbox (ensures device is not displayed on *Access* page).
8. Click **Save**.

CLI Procedure

1. Go to /settings/devices
2. Use the add command to create a new device,
3. Use the set command to define the following settings:
   name
   type (device_console, ilo, imm, drac, idrac6, ipmi1.5, impi2.0, ilom, cimc_ucs, netapp, infrabox, pdu*)
   ip_address as 127.0.0.1
   username and password (of the device)
   or set credential ask_during_login
   set mode to disabled
4. Save the changes with commit.

None Copy

```
[admin@nodegrid /]# cd /settings/devices
[admin@nodegrid devices]# add
[admin@nodegrid {devices}]# set name=Network_Template
[admin@nodegrid {devices}]# set type=device_console
[admin@nodegrid {devices}]# set ip_address=127.0.0.1
[admin@nodegrid {devices}]# set credential=ask_during_login

or

[admin@nodegrid {devices}]# set credential=set_now
[admin@nodegrid {devices}]# set username=admin password=admin

[admin@nodegrid {devices}]# set mode=disabled
[admin@nodegrid {devices}]# commit
```

Step 2 – Create a Discovery Rule

1. Go to *Managed Devices :: Auto Discovery :: Discovery Rules*
2. Click **Add**.
3. On *Add* dialog, enter **Name**.
4. On **Status** drop-down, select (Enabled, Disabled).
5. On *Discovery Method* menu, select **DHCP** checkbox.
6. (optional) To filter specific entries, enter **MAC Address.**
7. (optional) In *Host or VM Identifier* menu, enter parameter to further filter (if provided, part of port name must match value).
8. On **Action** drop-down, select what to do when a new device is discovered - Clone (Mode: Enabled), Clone (Mode: On-Demand), Clone (Mode: Discovered), Discard Discovered Devices.
9. On **Clone from** drop-down, select template device created earlier.
10. Click **Save**.

After the rule is created, the device is automatically added to the system as soon as it receives a DHCP address or renews its DHCP address lease. The default for the address lease renewal is every 10 minutes.

CLI Procedure

1. Go to /settings/auto_discovery/discovery_rules/
2. Use the add command to create a Discovery Rule.
3. Use the set command to define the following settings:
   rule_name for the Discovery Rule
   status for the discovered rule (enabled, disabled)
   method set to dhcp
   (optional) use the mac_address field to filter to these specific entries
   host_identifier parameter can be used to further apply a filter if a value is provided then part of the port name has to match the value
   action - select what should be performed when a new device is discovered (clone_mode_enabled, clone_mode_on-demand, clone_mode_discovered, discard_device)
4. clone_from set to the template device created earlier.
5. Save the changes with commit.

None Copy

```
[admin@nodegrid /]# cd /settings/auto_discovery/discovery_rules/
[admin@nodegrid discovery_rules]# add
[admin@nodegrid {discovery_rules}]# set rule_name=Network_Scan
[admin@nodegrid {discovery_rules}]# set status=enabled
[admin@nodegrid {discovery_rules}]# set method=dhcp
[admin@nodegrid {discovery_rules}]# set mac_address=00:0C:29
[admin@nodegrid {discovery_rules}]# set action=clone_mode_enabled
[admin@nodegrid {discovery_rules}]# set clone_from=Network_Template
[admin@nodegrid {discovery_rules}]# commit
```

Auto Discovery: Configure Service Account Credentials

This section provides information on configuring service account credentials that can be used for Nodegrid automated tasks, such as auto-discovery by using the second set of credentials for discovering Console and KVM Servers' ports.

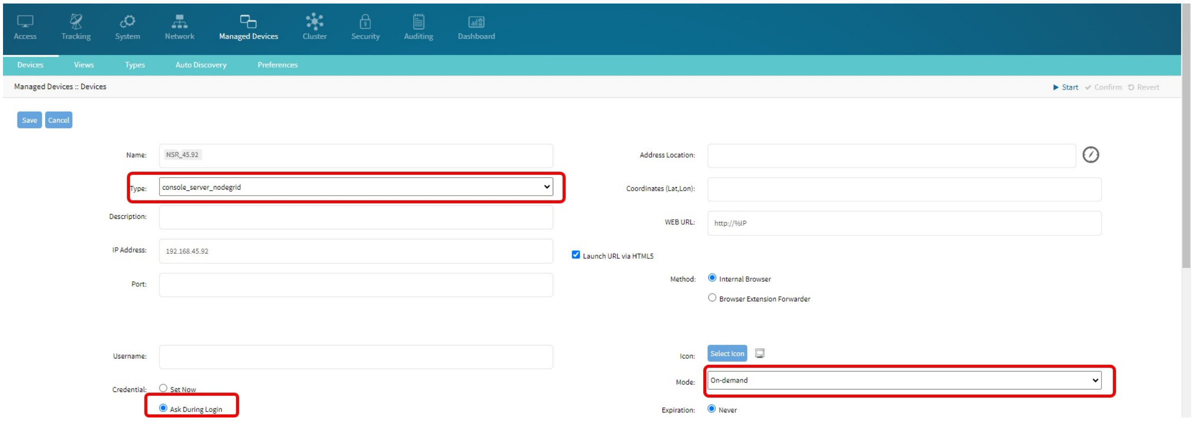
The discovery process requires logging into the appliance, and by default, it uses the credentials configured under *Device :: Access*, which are primarily intended for Console sessions. However, due to security policies, the same credentials cannot be used for both Console sessions and the discovery process. To align with these policies, we must define a dedicated authentication method, such as a service account specifically for automated tasks such as discovery. This ensures the credentials used for discovery are separate from those used for Console sessions.

- Discovery Process: Typically requires Administrator-level credentials to access system information.
- Console Sessions: Can be performed with User-level credentials, which can either be stored in *Device :: Access* or prompted at login.

Step 1: Create a Managed Device

To add a Console server managed device, follow these steps:

1. Navigate to *Managed Devices :: Devices*.



Managed Devices :: Devices

Name: NSR_45.92

Type: console_server_nodegrid

Description:

IP Address: 192.168.45.92

Port:

Username:

Credential: ○ Set Now ● Ask During Login

Address Location:

Coordinates (Lat,Lon):

WEB URL: http://%IP

☑ Launch URL via HTML5

Method: ● Internal Browser ○ Browser Extension Forwarder

Icon:

Mode: On-demand

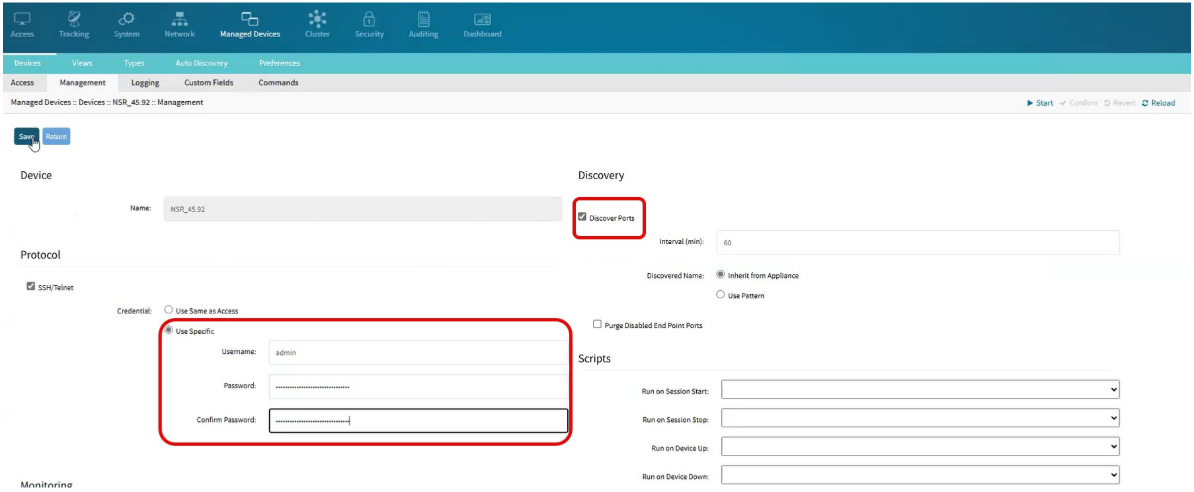
Expiration: ● Never

2. Click **Add**.
3. Enter a name for the managed device.
4. Select Type as **console_server_nodegrid**.
5. Enter the IP address of the managed device.
6. Under Credential select **Ask During Login**.
7. Select **On-demand** in the Mode drop-down.
8. Click **Save**.

Step 2: Set up the Console Server Credentials

After adding a Console server, you need to set up the credentials. Follow these steps to perform this task:

1. Click on the managed device name created in the above procedure.
2. Click **Management**.



Managed Devices :: Devices :: NSR_45.92 :: Management

Device

Name: NSR_45.92

Protocol

☑ SSH/Telnet

Credential: ○ Use Same as Access ● Use Specific

Username: admin

Password: ••••••••••••••••••••••

Confirm Password: ••••••••••••••••••••••

Monitoring

Discovery

☑ Discover Ports

Interval (min): 60

Discovered Name: ● Inherit from Appliance ○ Use Pattern

☐ Purge Disabled End Point Ports

Scripts

Run on Session Start:

Run on Session Stop:

Run on Device Up:

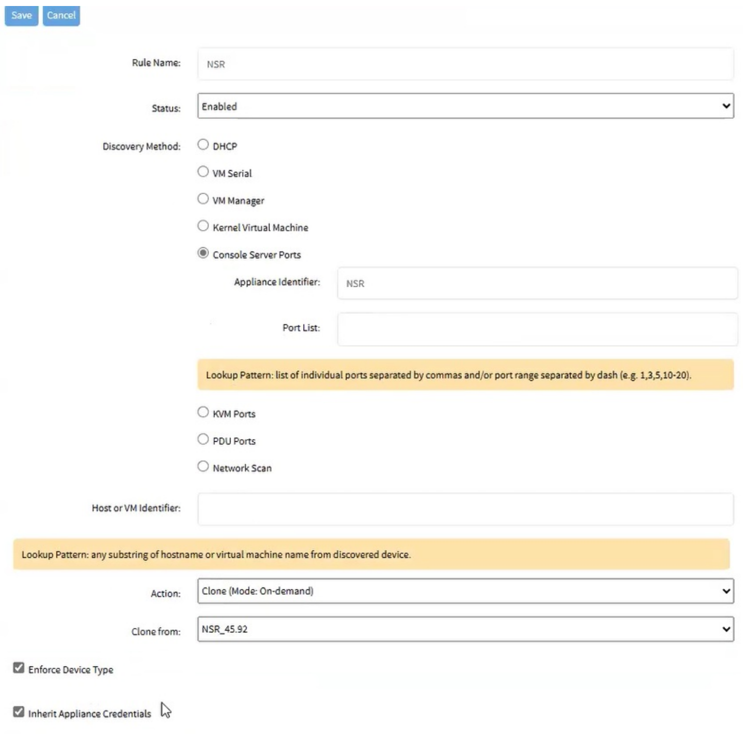
Run on Device Down:

3. The Discovery Ports will be selected by default. Leave the setting to enabled.
4. Provide username and password for logging in to the console server.
5. Click **Save**.

Step 3: Set up Discovery Rules

Create a rule to apply the cloning on the managed device. Follow these steps to perform this task:

1. Navigate to *Managed Device :: AutoDiscovery :: Discovery Rules*.
2. Click **Add**.



Rule Name: NSR

Status: Enabled

Discovery Method:
○ DHCP
○ VM Serial
○ VM Manager
○ Kernel Virtual Machine
● Console Server Ports

Appliance Identifier: NSR

Port List:

Lookup Pattern: list of individual ports separated by commas and/or port range separated by dash (e.g. 1,3,5,10-20).

○ KVM Ports
○ PDU Ports
○ Network Scan

Host or VM Identifier:

Lookup Pattern: any substring of hostname or virtual machine name from discovered device.

Action: Clone (Mode: On-demand)

Clone from: NSR_45.92

☑ Enforce Device Type

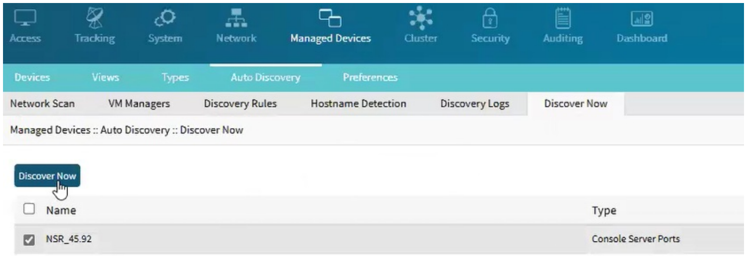
☑ Inherit Appliance Credentials

3. Enter a name for the discovery rule.
4. Select mode as **Enabled**.
5. Select the radio button Console Server Ports.
6. Select the Action as Clone (Mode On-demand).
7. From the drop-down Clone from: select the managed device name (created in the above procedure).
8. (Optional): Enable **Enforce Device Type** and **Inherit Appliance Credentials**.
9. Click **Save**.

Step 4: Start the Discovery Process

The discovery process runs at the configured interval but is triggered automatically when a new appliance is added to the platform. It can also be started manually if needed.

1. Navigate to *Managed Devices:: Auto Discovery:: Discover Now.*



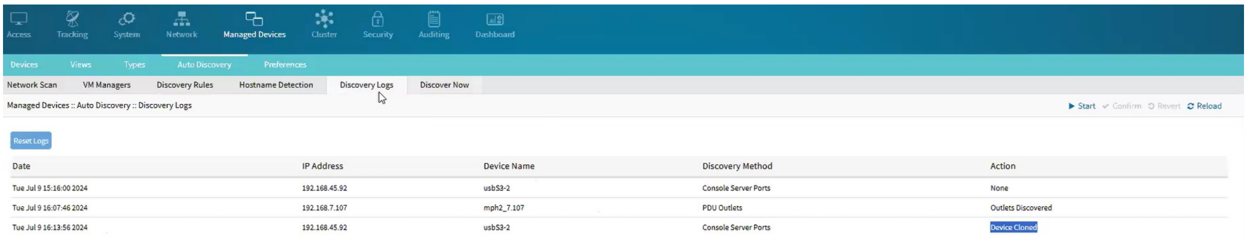
Managed Devices :: Auto Discovery :: Discover Now

☐	Name	Type
☑	NSR_45.92	Console Server Ports

2. Select the console server name.
3. Click **Discover Now**.

Step 5: View Discovery Logs

The Discovery Logs page shows the logs of the discovery processes set on the Managed Devices' setting for auto discovery. In this example, you can see that the Action is **Device Cloned** for the Console Server Port.



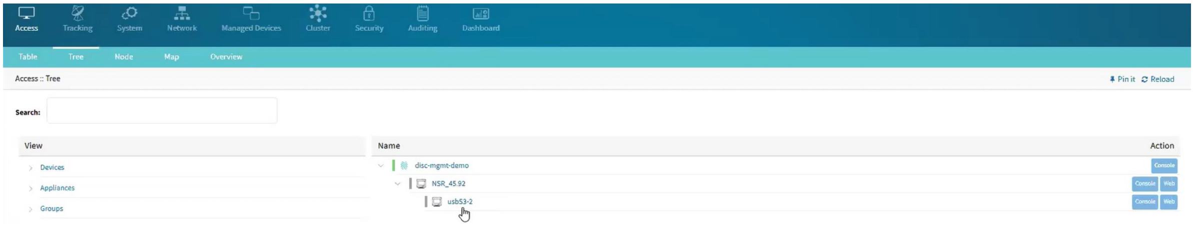
Managed Devices :: Auto Discovery :: Discovery Logs

Date	IP Address	Device Name	Discovery Method	Action
Tue Jul 9 15:16:00 2024	192.168.45.92	usbS3-2	Console Server Ports	None
Tue Jul 9 16:07:46 2024	192.168.7.107	mph2_7.107	PDU Outlets	Outlets Discovered
Tue Jul 9 16:13:56 2024	192.168.45.92	usbS3-2	Console Server Ports	Device Cloned

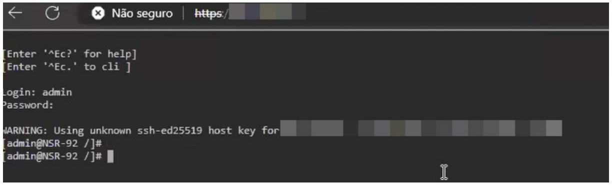
Step 6: Access the Managed Device Appliance and Appliance Port

To access the managed device appliance (console server port), follow these steps:

1. Navigate to *Access :: Tree*. In the following figure, the managed device appliance has usbS3-2 port enabled that is cloned.



2. Click on **Console** button next to the managed device to access console session of the device. The session will request for access credentials to log in to the device.



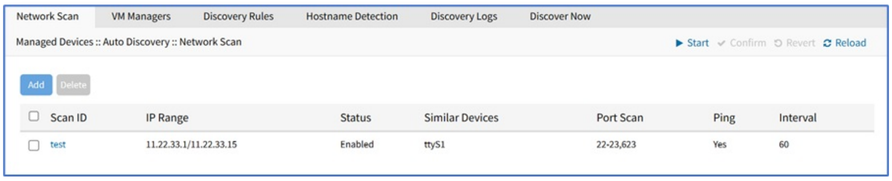
```
[Enter '^Ec?' for help]
[Enter '^Ec.' to cli ]

Login: admin
Password:

WARNING: Using unknown ssh-ed25519 host key for[redacted]
[admin@NSR-92 /]#
[admin@NSR-92 /]#
```

3. Enter the login credentials to get access to the device.

> **Note**
>
> Similarly when you access the usbS3-2 port, you will be required enter the credentials (due to Access configuration **Ask During Login**).

Network Scan sub-tab

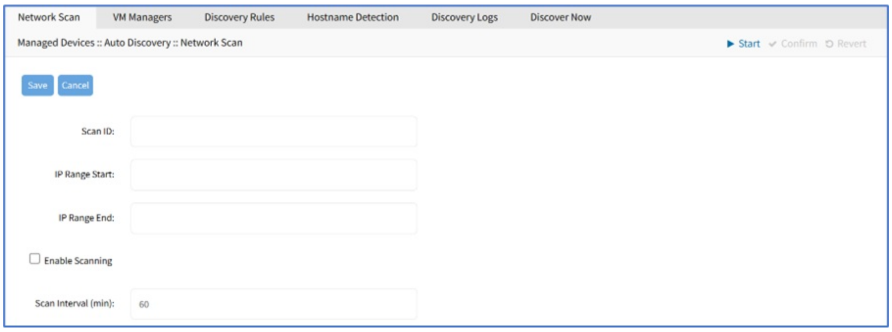
This lists available network scan setups.



□	Scan ID	IP Range	Status	Similar Devices	Port Scan	Ping	Interval
□	test	11.22.33.1/11.22.33.15	Enabled	ttyS1	22-23,623	Yes	60

Add Network Scan

1. Go to *Managed Devices :: Auto Discovery :: Network Scan*.
2. Click **Add** (displays dialog).



Scan ID:

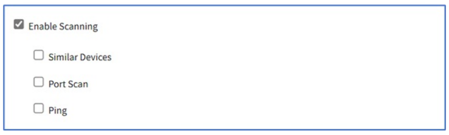
IP Range Start:

IP Range End:

□ Enable Scanning

Scan Interval (min): 60

3. Enter **Scan ID**
4. Enter **IP Range Start** and **IP Range End**
5. Select **Enable Scanning** checkbox (expands dialog).



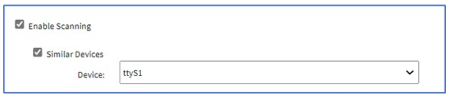
☑ Enable Scanning

□ Similar Devices

□ Port Scan

□ Ping

   a. Select **Similar Devices** checkbox (expands dialog). On **Device** drop-down, select an existing template (to identify devices).

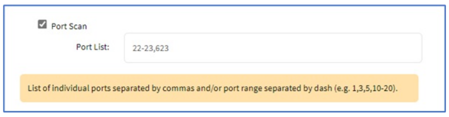


☑ Enable Scanning

☑ Similar Devices

Device: ttyS1

   b. Select **Port Scan** checkbox (expands dialog). Enter **Port List** (ports to be scanned, i.e., 2, 3, 11-20).



☑ Port Scan

Port List: 22-23,623

List of individual ports separated by commas and/or port range separated by dash (e.g. 1,3,5,10-20).

   c. Select **Ping** checkbox (enables Ping function).

6. On **Scan interval (in minutes)**, enter a value.
7. Click **Save**.

Edit Network Scan

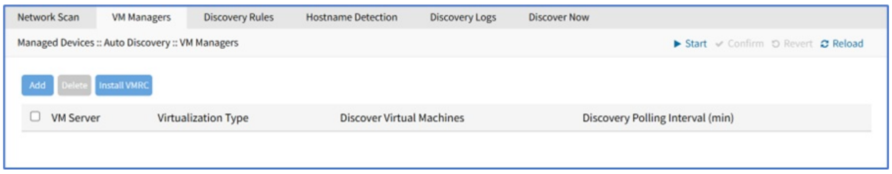
1. Go to *Managed Devices :: Auto Discovery :: Network Scan*.
2. In *Scan ID* column, click on the name (displays dialog).
3. Make changes as needed.
4. Click **Save**.

Delete Network Scan

1. Go to *Managed Devices :: Auto Discovery :: Network Scan*.
2. Select the checkbox(es) to be deleted.
3. Click **Delete**.
4. On the confirmation dialog, click **OK**.

VM Manager sub-tab

This lists VM Managers.

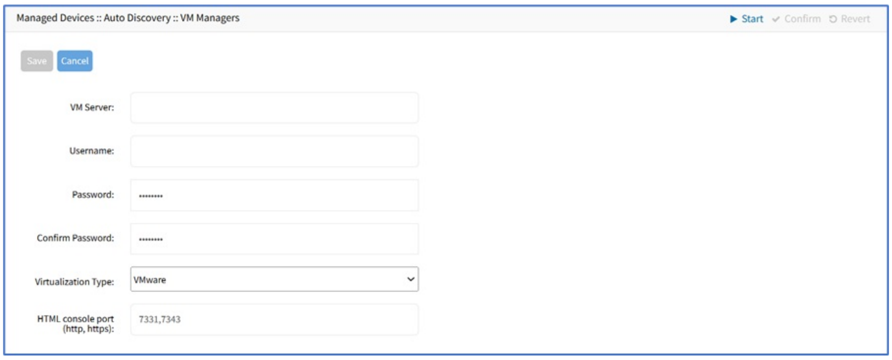


Managed Devices :: Auto Discovery :: VM Managers

□	VM Server	Virtualization Type	Discover Virtual Machines	Discovery Polling Interval (min)

Add VM Manager

1. Go to *Managed Devices :: Auto Discovery :: VM Managers*.
2. Click **Add** (displays dialog).



Managed Devices :: Auto Discovery :: VM Managers

VM Server:

Username:

Password: ••••••••

Confirm Password: ••••••••

Virtualization Type: VMware

HTML console port (http, https): 7331,7343

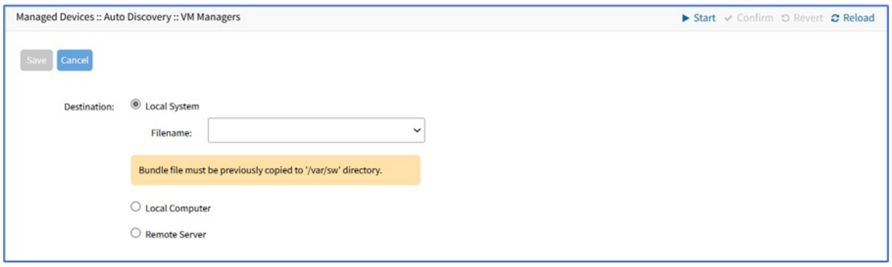
3. On **VM Server**, enter the *vCenter/ESXi* **IP** or **FQDN.**
4. Enter **Username.**
5. On **Virtualization Type** drop-down, select **VMware.**
6. Enter **Password** and **Confirm Password.**
7. Enter **HTML console port** (if needed).
8. Click **Save**.

Delete VM Manager

1. Go to *Managed Devices :: Auto Discovery :: VM Managers*.
2. Select the checkbox(es) of items to delete.
3. Click **Delete**.
4. On the confirmation dialog, click **OK**.

Install VMRC

1. Go to *Managed Devices :: Auto Discovery :: VM Managers*.
2. Click **Install VMRC** (displays dialog).



Managed Devices :: Auto Discovery :: VM Managers

Destination: ● Local System

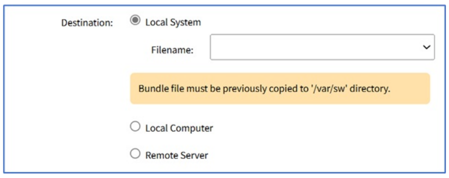
Filename:

Bundle file must be previously copied to '/var/sw' directory.

○ Local Computer

○ Remote Server

3. On *Destination* menu, select one:
   - **Local System** radio button. **Filename** drop-down, select one.



Destination: ● Local System

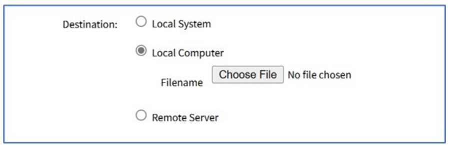
Filename:

Bundle file must be previously copied to '/var/sw' directory.

○ Local Computer

○ Remote Server

   - **Local Computer** radio button. On **File Name**, click **Choose File** (locate and select).



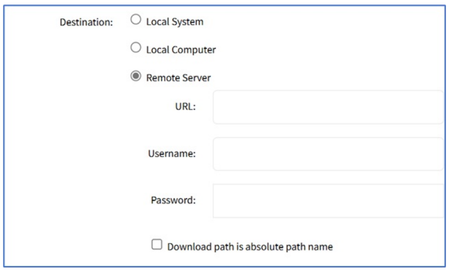
Destination: ○ Local System

● Local Computer

Filename No file chosen

○ Remote Server

   - **Remote Server** radio button.



Destination: ○ Local System

○ Local Computer

● Remote Server

URL:

Username:

Password:

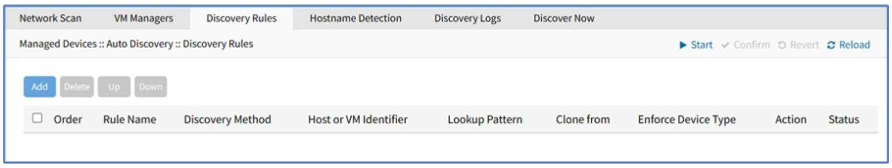
□ Download path is absolute path name

- Enter **URL**, **Username**, and **Password**.
- (optional) **Download path is absolute path name** checkbox.

4. Click **Save**.

Discovery Rules sub-tab

This lists all available discovery rules.



Network Scan | VM Managers | Discovery Rules | Hostname Detection | Discovery Logs | Discover Now

Managed Devices :: Auto Discovery :: Discovery Rules

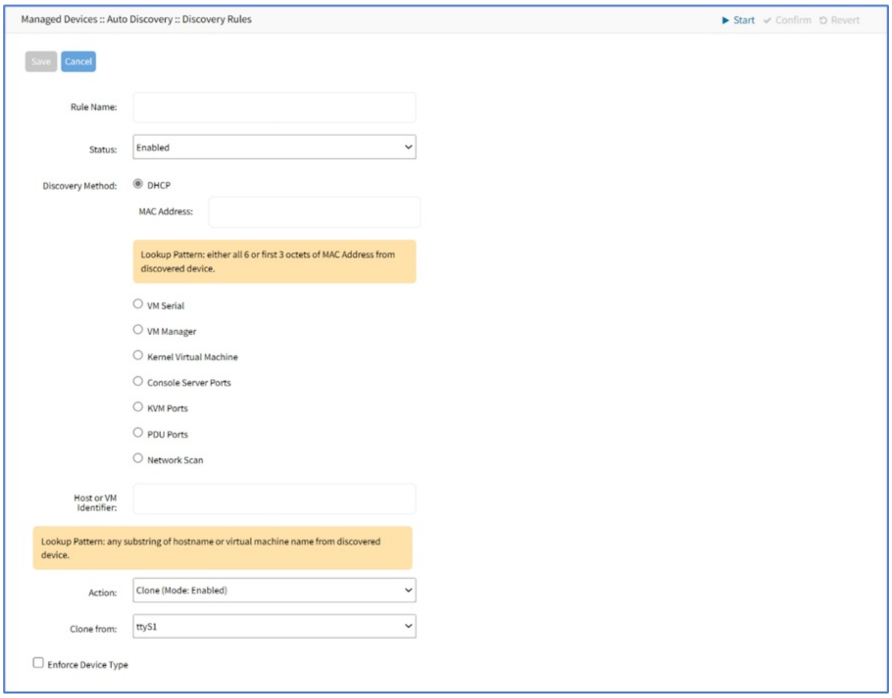
▶ Start ✔ Confirm ↺ Revert ↻ Reload

Add | Delete | Up | Down

□	Order	Rule Name	Discovery Method	Host or VM Identifier	Lookup Pattern	Clone from	Enforce Device Type	Action	Status

Add Discovery Rule

1. Go to *Managed Devices :: Auto Discovery :: Discovery Rules*.
2. Click **Add** (displays dialog).



Managed Devices :: Auto Discovery :: Discovery Rules

▶ Start ✔ Confirm ↺ Revert

Save | Cancel

Rule Name:

Status: Enabled

Discovery Method: ● DHCP

MAC Address:

Lookup Pattern: either all 6 or first 3 octets of MAC Address from discovered device.

○ VM Serial

○ VM Manager

○ Kernel Virtual Machine

○ Console Server Ports

○ KVM Ports

○ PDU Ports

○ Network Scan

Host or VM Identifier:

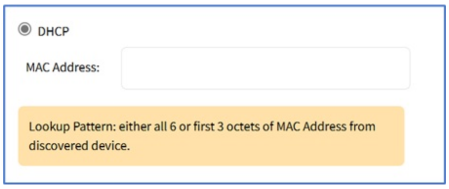
Lookup Pattern: any substring of hostname or virtual machine name from discovered device.

Action: Clone (Mode: Enabled)

Clone from: ttyS1

□ Enforce Device Type

3. Enter **Rule Name.**
4. On **Status** drop-down, select (Enabled, Disabled).
5. On the *Discovery Method* menu, select either of the following options:
   - If you select **DHCP,** enter the following details:
     - Enter **MAC Address**

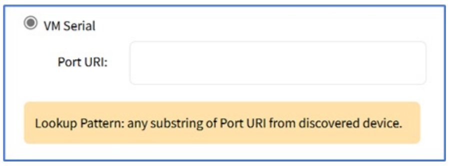


● DHCP

MAC Address:

Lookup Pattern: either all 6 or first 3 octets of MAC Address from discovered device.

   - If you select **VM Serial,** enter the following details:
     - **Port URI**.

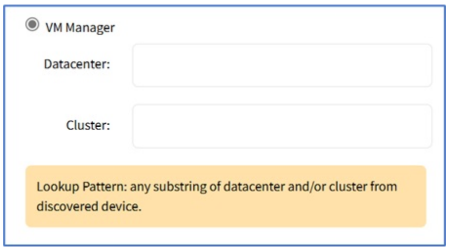


● VM Serial

Port URI:

Lookup Pattern: any substring of Port URI from discovered device.

   - If you select **VM Manager,** enter the following details:
     - Enter **Datacenter** and **Cluster**.



● VM Manager

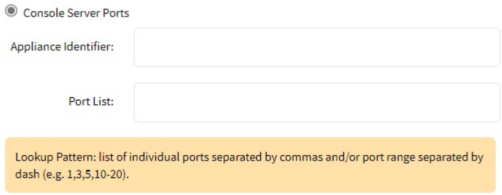
Datacenter:

Cluster:

Lookup Pattern: any substring of datacenter and/or cluster from discovered device.

   - If you select **Kernel Virtual Machine,** specify the **Host or VM Identifier** and proceed further to step 6.
   - If you select **Console Server Ports,** enter the following details:
     - **Appliance Identifier**: allows filtering to discover ports from multiple appliances that are of the same or different type by matching any substring of the

appliance name
    - **Port List** (list of ports to scan (i.e., 1,3,5,10-20).



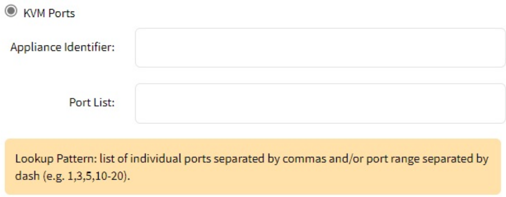
○ Console Server Ports

Appliance Identifier:

Port List:

Lookup Pattern: list of individual ports separated by commas and/or port range separated by dash (e.g. 1,3,5,10-20).

- If you select **KVM Ports,** enter the following details:
    - **Appliance Identifier**: allows filtering to discover ports from multiple appliances that are of the same or different type by matching any substring of the appliance name
    - **Port List** (list of ports to scan; i.e., 1,3,5,10-20)



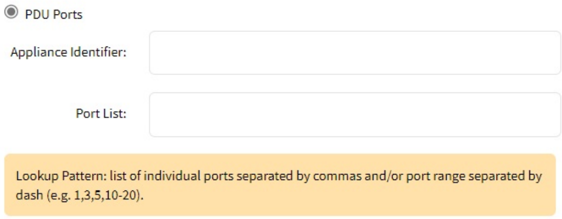
○ KVM Ports

Appliance Identifier:

Port List:

Lookup Pattern: list of individual ports separated by commas and/or port range separated by dash (e.g. 1,3,5,10-20).

- If you select **PDU Ports,** enter the following details:
    - **Appliance Identifier**: allows filtering to discover ports from multiple appliances that are of the same or different type by matching any substring of the appliance name
    - **Port List** (list of ports to scan; i.e., 1,3,5,10-20)



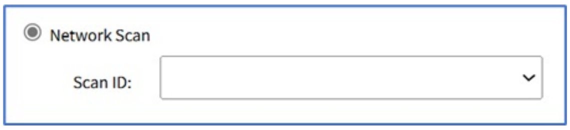
○ PDU Ports

Appliance Identifier:

Port List:

Lookup Pattern: list of individual ports separated by commas and/or port range separated by dash (e.g. 1,3,5,10-20).

- If you select the **Network Scan** radio button. From the **Scan ID** drop-down, select the required option:



○ Network Scan

Scan ID:

- (optional) In *Host or VM Identifier* menu, enter the parameter to further filter (if provided, part of the port name must match the value).

6. On **Action** drop-down, select what to do when a new device is discovered (Clone (Mode: Enabled), Clone (Mode: On-Demand), Clone (Mode: Discovered), Discard Discovered Devices).
7. On **Clone from** the drop-down, select the appropriate template device.
8. Select **Enforce Device Type** checkbox.
9. Select the **Inherit Appliance Credentials** field, which uses appliance or device credentials to discover ports and syncs over time, whether username, password, or SSH Keys is changed, ports sync appliance credentials in the upcoming scans of Ports Discovery.
   Note: *This field only applies to Console Server Ports, KVM Ports, and PDU Ports Discovery Methods.*
10. Click **Save**.

Edit Discovery Rule

1. Go to *Managed Devices :: Auto Discovery :: Discovery Rules*.
2. In the *Order* column, click on the name (displays dialog).
3. Make changes as needed.
4. Click **Save**.

Delete Discovery Rule

1. Go to *Managed Devices :: Auto Discovery :: Discovery Rules*.
2. Select the checkbox(es) of items to delete.
3. Click **Delete**.
4. On the confirmation dialog, click **OK**.

Move Discovery Rule Priorities Up

1. Go to *Managed Devices :: Auto Discovery :: Discovery Rules*.
2. Select the checkbox(es) of items.
3. Click **Up**.

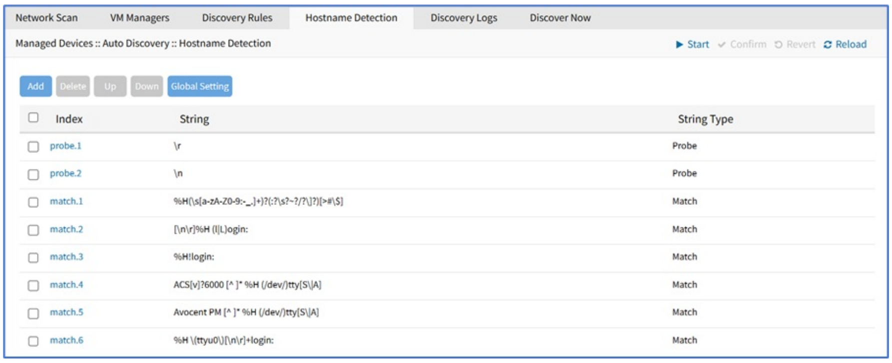
Move Discovery Rule Priorities Down

1. Go to *Managed Devices :: Auto Discovery :: Discovery Rules*.
2. Select the checkbox(es) of items.
3. Click **Down**.

Hostname Detection sub-tab

Hostname (network or serial) is automatically discovered when logged into the Nodegrid Platform, based on user access permissions. By default, Nodegrid devices include probes and matches for these device types: PDUs, NetApp, Console Servers, Device Consoles, and Service Processors.

Nodegrid sends a probe and waits for a match. If no match, a second probe is sent. This is repeated until a match occurs, then the probe process stops.



☐	Index	String	String Type
☐	probe.1	\r	Probe
☐	probe.2	\n	Probe
☐	match.1	%H(\s[a-zA-Z0-9:-_.]+)?(:?\s?~?/?\]?)[>#\$]	Match
☐	match.2	[\n\r]%H (l|L)ogin:	Match
☐	match.3	%H!login:	Match
☐	match.4	ACS[v]?6000 [^]* %H (/dev/)tty[S\\|A]	Match
☐	match.5	Avocent PM [^]* %H (/dev/)tty[S\\|A]	Match
☐	match.6	%H \(ttyu0\)[\n\r]+login:	Match

Enable Hostname Detection

After hostname detection is enabled, it runs only once and then reverts to disabled.

1. Go to *Managed Devices :: Devices*.
2. Click on the device **Name** (displays dialog).
3. On the **Access** sub-tab, scroll down to locate and select **Enable Hostname Detection** checkbox.

☑ Enable Hostname Detection

4. Click **Save**.

CLI Procedure

1. Go to /settings/devices/<device name>/access
2. Set enable_hostname_detection to yes
3. Save the changes with commit

Plaintext Copy

```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/access/
[admin@nodegrid /]# set enable_hostname_detection=yes
[+admin@nodegrid /]# commit
```

Create a Probe or Match

1. Go to *Managed Devices :: Auto Discovery :: Hostname Detection*.
2. Click **Add** (displays dialog).
3. On **String Type** drop-down, select one (Match, Probe).
4. On **String**, enter characters for Match or Probe.

> **NOTE**
> For String Type: Matches, RegEx expressions are allowed. Use the variable %H to indicate the location of the hostname.

5. Click **Save**.

CLI Procedure

1. Go to /settings/auto_discovery/hostname_detection/string_settings
2. Type add
3. Use the set command to define string_type (match, probe)
4. Use the set command to define a probe or match string
5. Make active
6. Save the changes with commit

> **NOTE**
> For Matches RegEx expressions are allowed. Use the variable %H to indicate the location of the hostname

Plaintext Copy

```
[admin@nodegrid /]# /settings/auto_discovery/hostname_detection/string_settings
[admin@nodegrid /]# add
[admin@nodegrid /]# set string_type=match
[+admin@nodegrid /]# set match_string=[\a\r]%H{I|L)ogin:
[+admin@nodegrid /]# active
[+admin@nodegrid /]# commit
```

Delete a Probe or Match

1. Go to *Managed Devices :: Auto Discovery :: Hostname Detection*.
2. Select checkbox(es).
3. Click **Delete**.
4. On confirmation dialog, click **OK**.

Move Hostname Detection Priorities Up

1. Go to *Managed Devices :: Auto Discovery :: Hostname Detection*.
2. Select the checkbox(es) of items.
3. Click **Up** to move the sequence.

Move Hostname Detection Priorities Down

1. Go to *Managed Devices :: Auto Discovery :: Hostname Detection*.
2. Select the checkbox(es) of items.
3. Click **Down** to move the sequence.

Modify Hostname Detection Global Setting

1. Go to *Managed Devices :: Auto Discovery :: Hostname Detection*.
2. Click **Global Settings** (displays dialog).
3. Enter **Probe timeout (sec)** (max time to wait for output) (default: 5)
4. Enter **Number of retries** (number of times probe is resent if no output) (default: 3).
5. Enter **Discovered name updates device name** checkbox (enabled by default).

   > **NOTE**
   >
   > If disabled, no devices names are updated, even if a match is found.)

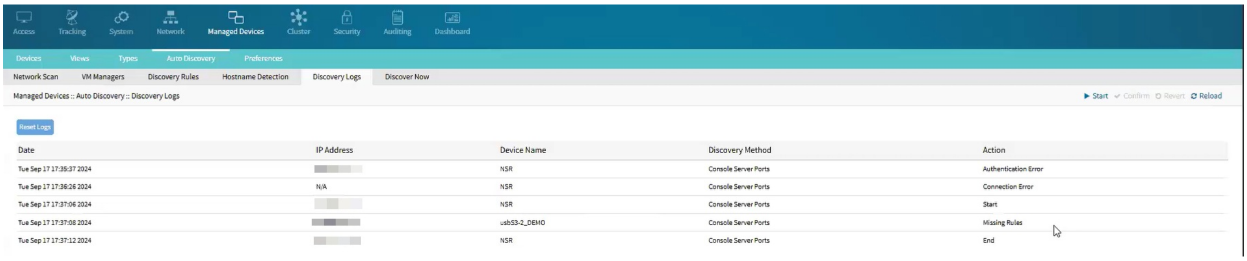
6. Select **New discovered device receives the name during conflict** checkbox.

   > **NOTE**
   >
   > If enabled, and multiple devices have the same name, the latest discovered device receives the name.

7. Click **Save**.

Discovery Logs sub-tab

A device discovery log records the details of the managed devices connected to the Nodegrid device during a device discovery process. The Discovery Logs tab displays the available Auto Discovery logs.



Date	IP Address	Device Name	Discovery Method	Action
Tue Sep 17 17:35:37 2024	[redacted]	NSR	Console Server Ports	Authentication Error
Tue Sep 17 17:36:26 2024	N/A	NSR	Console Server Ports	Connection Error
Tue Sep 17 17:37:06 2024	[redacted]	NSR	Console Server Ports	Start
Tue Sep 17 17:37:08 2024	[redacted]	usbS3-2_DEMO	Console Server Ports	Missing Rules
Tue Sep 17 17:37:12 2024	[redacted]	NSR	Console Server Ports	End

The logs table shows the following details:

Discovery Log Name	Description
Date	Discovery time stamp to track the latest discovery state of a device.
IP Address	IP address and device name using which the device was discovered.
Device Name	Name of the managed device associated with the IP address.
Discovery Method	Managed device discovery method to indicate how the devices were identified. The devices can be discovered via: • DHCP • VM Serial • VM Manager • Kernel Virtual Machine • Console Server Ports • KVM Ports • PDU Ports • Network Scan PDU Outlets • Switch Ports • Hostname Detection
Action	Actions or latest state processed by the discovery tool on the managed device during the discovery process. The common actions include: • Start and End state of the discovery process • Discovery errors such as • Connection error (incorrect or unreachable IP address) • Authentication error (incorrect credentials) • Communication error (integration error, misconfiguration or unsupported appliance) • Configuration failures (invalid device name) • Missing discovery rules • No rule matched • No ports found • Device Updated • Device Renamed • Device Cloned – Rule: <RULENAME> • Discarded • Discovery Disabled • No License Available • Device Disabled • Device Removed • None (no rules, already discovered or no updates)

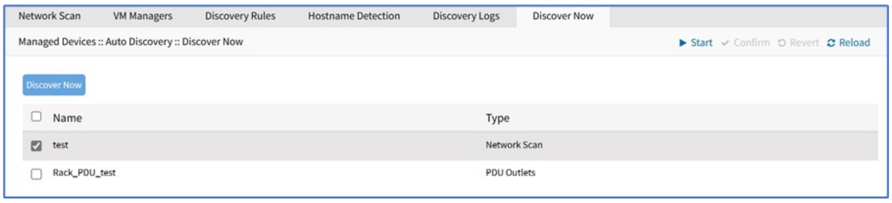
Reset Logs

At any point, you can reset the discovery logs by using the following procedure.

1. Go to *Managed Devices :: Auto Discovery :: Discovery Logs.*
2. Click **Reset Logs** (clears the table listing).

Discover Now sub-tab

This manually runs the auto discovery process for the selected item(s).



	Name	Type
☑	test	Network Scan
□	Rack_PDU_test	PDU Outlets

Start Discovery

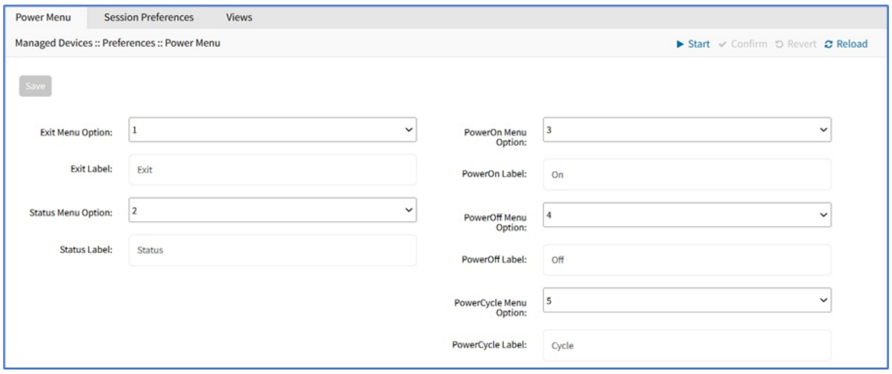
1. Go to *Managed Devices :: Auto Discovery :: Discover Now*.
2. On the list, select checkboxes.
3. Click **Discover Now**.

Preferences tab

Administrators can define various preferences options that are applied to all sessions.

Power Menu sub-tab

This configures preferences for defined order and labeling of the power menu as it appears in a console session.



Exit Menu Option: 1

Exit Label: Exit

Status Menu Option: 2

Status Label: Status

PowerOn Menu Option: 3

PowerOn Label: On

PowerOff Menu Option: 4

PowerOff Label: Off

PowerCycle Menu Option: 5

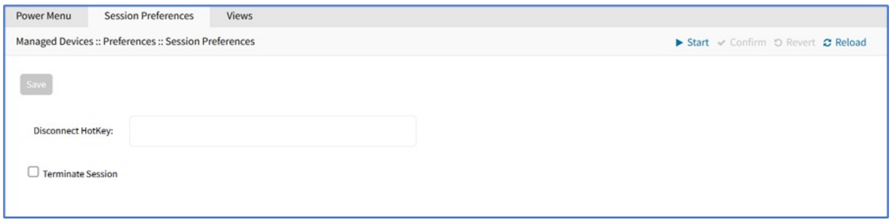
PowerCycle Label: Cycle

Edit Power Menu Settings

1. Go to *Managed Devices :: Preferences :: Power Menu*.
2. On **Exit Menu Option** drop-down, select one (0, 1, 2, 3, 4, 5, 6, 7, 8, 9). Enter **Exit Label**.
3. On **Status Menu Option** drop-down, select one (0, 1, 2, 3, 4, 5, 6, 7, 8, 9). Enter **Status Label**.
4. On **PowerOn Menu Option** drop-down, select one (0, 1, 2, 3, 4, 5, 6, 7, 8, 9). Enter **PowerOn Label**.
5. On **PowerOff Menu Option** drop-down, select one (0, 1, 2, 3, 4, 5, 6, 7, 8, 9). Enter **PowerOff Label**.
6. On **PowerCycle Menu Option** drop-down, select one (0, 1, 2, 3, 4, 5, 6, 7, 8, 9). Enter **PowerCycle Label**.
7. Click **Save**.

Session Preferences sub-tab

This defines session preferences. Often, it is difficult to exist a specific console session without affecting other sessions in the chain. The Disconnect HotKey closes the current active session in a chain. Configuring this hot key is useful when multiple sessions are open, i.e., a console session started from within a console session; or cascaded console sessions.

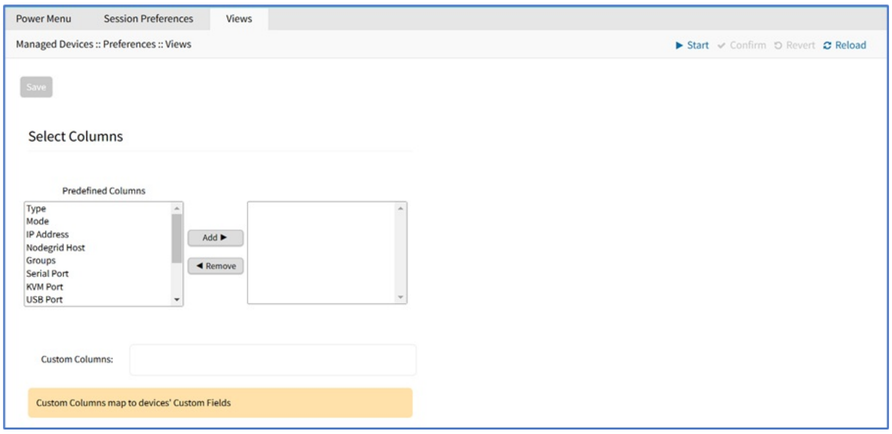


Configure Disconnect HotKey to Terminate Session

1. Go to *Managed Devices :: Preferences :: Session Preferences*.
2. On **Disconnect HotKey** (a key sequence that terminates the session).
3. Select **Terminate session** checkbox (if enabled, on Disconnect HotKey, all connected sessions are closed – and the user is returned to the main shell prompt. If disabled, on Disconnect HotKey, only the current session is closed.
4. Click **Save**.

Views sub-tab

This changes how columns are displayed, as well as creating custom columns.



Custom Columns map to devices' Custom Fields

Change Table Column Preferences

Column selections and arrangements are stored on the local computer. This column layout is not available when logged into another device.

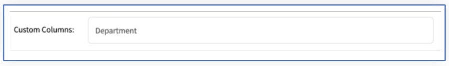
1. Go to *Managed Devices :: Preferences :: Views*.
2. To add columns to right panel, in *Predefined Columns*, select and click **Add►** .
3. To remove columns from right panel, in right side panel, select and click **◄Remove**.
4. Click **Save**.

Step 1 – Create Custom Columns (per Device)

These provide additional organization of data on connected devices, custom columns can be created and enabled. This is a two-step process. First create the custom column, then add the custom column(s) to the individual device.

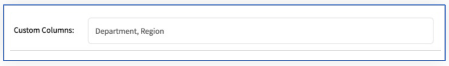
This two-step procedure connects the device's custom column to the device's custom field displayed in tables that contain that device's settings/values.

1. Go to *Managed Devices :: Preferences :: Views*.
2. In the **Custom Columns** text box, enter the column name.



Custom Columns: Department

3. To add multiple columns, separate each name with a comma.



Custom Columns: Department, Region

4. Click **Save**.

NOTE

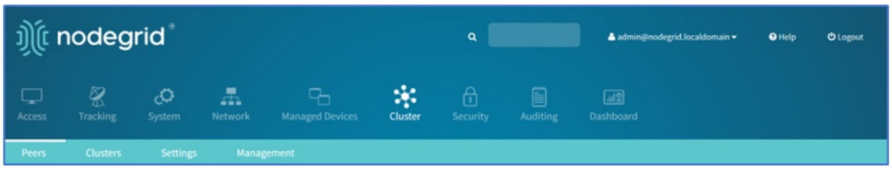
The new custom column(s) do not appear on the *Access :: Devices* page until the associated device and column is enabled.

Step 2 – Associate Device to the new Custom Field

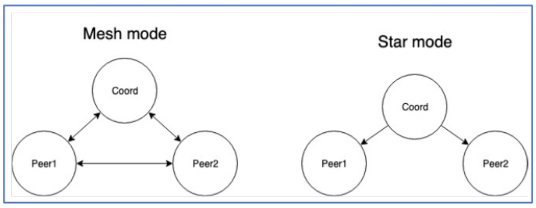
1. Go to *Managed Devices :: Devices*.
2. Click the device name to be associated with the custom field.
3. On **Custom Fields** sub-tab, click **Add** (displays dialog).
4. Enter **Field Name** (must exactly match name entered in the *Custom Columns* dialog).
5. Enter **Field Value**.
6. Click **Save**.

Cluster Section

Cluster establishes a secure and resilient connection with a set of Nodegrid devices. When enabled, a Nodegrid device that is part of the Cluster can access and manage other devices. By logging into any Nodegrid device, all devices in the Cluster can be reached with a single interface. This allows for vertical and horizontal scalability.



There are two types of clustering topologies:



Star

This is the default option. In a star configuration, one Nodegrid unit acts as the coordinator and central node. All other peers connect to the coordinator in a star formation. Only the coordinator has the list of all peers and attached devices within the configuration. This option allows centralized access and visibility from the coordinator Nodegrid device.

Mesh

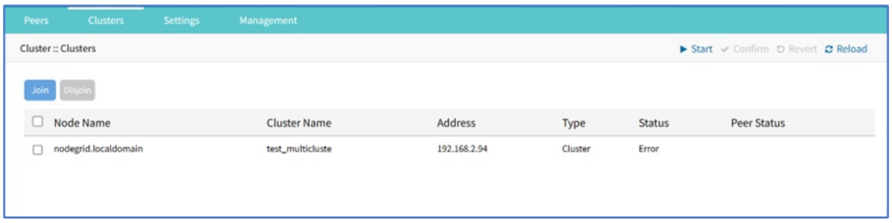
In this configuration, one Nodegrid unit acts as the coordinator and all Nodegrid units (coordinator and peers) see each other (and all attached devices). This option allows for distributed access. Each unit keeps a list of all peers and attached devices and demands equal system resources of all devices. This configuration is recommended for clusters of less than 50 units.

Clusters tab

This table lists remote clusters the local node has joined, as well as remote clusters that have joined this cluster. Nodes listed as remote peers initiated the Join.

NOTE

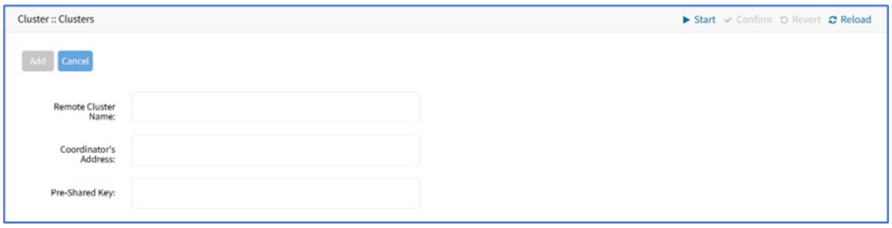
Remote Peers don't show Status or Peer Status, because there is no connection from the coordinator to the remote peers that have been joined.



□	Node Name	Cluster Name	Address	Type	Status	Peer Status
□	nodegrid.localdomain	test_multicluste	192.168.2.94	Cluster	Error	

Join a Cluster

1. Go to *Cluster :: Clusters*.
2. Click **Join** (displays dialog).



Remote Cluster Name:

Coordinator's Address:

Pre-Shared Key:

   a. Enter **Remote Cluster Name**
   b. Enter **Coordinator's Address**
   c. Enter **Pre-Shared Key**

3. Click **Save**.

Disjoin a Cluster

This leaves a remote cluster that was joined or removes a remote peer that has joined the cluster.

1. Go to *Cluster :: Clusters*.
2. Select checkbox next to Remote Cluster to be disjoined.
3. Click **Disjoin**.

Enable Cluster

Cloud is a NodeGrid feature that establishes a secure and resilient connection among other NodeGrid platforms. When Clustering is enabled, multiple NodeGrid systems can easily manage and access all managed devices from different nodes.

NodeGrid makes cloud access management even easier with cloud asset search. By logging into any NodeGrid node users can search the entire NodeGrid-managed enterprise network and cluster with a single interface.

This allows vertical and horizontal scalability.

> **Note: Ensure the cluster license is added to the Coordinator under System::License.**

The following are the steps to configure clustering in NodeGrid:

1. Log in to your first NodeGrid's WebUI as admin
2. Go to **Cluster** :: **Settings** page.
3. Check the **Enable Cluster** checkbox.
4. Enter a **Cluster** Name
5. Select **Type** as **Coordinator**, and enter a **Pre-Shared** Key
6. Select the **Cluster** mode, Star, or Mesh. Change the polling rate if you require. default is 30 sec.
7. Check the **Enable Clustering Access** checkbox.
8. Click **Save.**
9. Go to your second Nodegrid and log in as admin.
10. Go to **Cluster** :: **Settings** page, and enable Cluster.
11. Enter the same **Cluster** name from the Coordinator NodeGrid.
12. Select **Type** as **Peer**, and enter the IP address and the same Pre-Shared Key of the first NodeGrid
13. Check the **Enable Clustering Access** checkbox.
14. Click **Save**.
15. Repeat steps 8 through 13 for other NodeGrids that you want to be part of the Clustering
16. Go to the Cluster :: Peers page and wait until all units establish internal communication and get Status **Online.**
17. Go to the **Access** page and all the nodes should be listed there. You will also see the leased cluster license under **System** :: **License**.

Example of Configuration via CLI

> **Note: replace the values of the parameters with your own**

1. Access the first NodeGrid via SSH or local port (Console or HDMI) and log in as admin
2. Type the following commands:

ActionScript Copy

```
[admin@nodegrid /]# cd /settings/cluster/settings
[admin@nodegrid   settings/] edit
[admin@nodegrid {settings}]# set enable_cluster=yes type=coordinator
[admin@nodegrid {settings}]# set cluster_name=clustername
[admin@nodegrid {settings}]# set psk=presharedkey
[admin@nodegrid {settings}]# set cluster_mode=star
[admin@nodegrid {settings}]# set lps_type=server
[admin@nodegrid {settings}]# set enable_license_pool=yes
[admin@nodegrid {settings}]# set enable_clustering_access=yes
[admin@nodegrid {settings}]# commit
```

Copy

3. Access the second Nodegrid via SSH or local port, and log in as admin.
4. Type the following commands:

ActionScript Copy

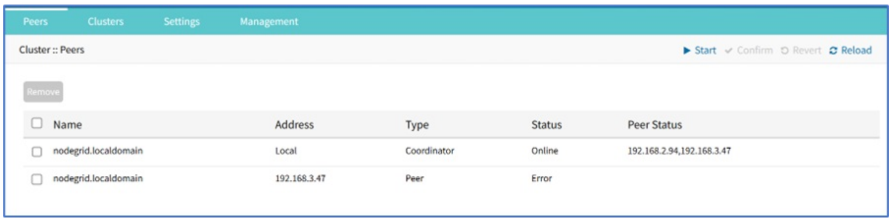
```
[admin@nodegrid /]# cd /settings/cluster/settings
[admin@nodegrid   settings/] edit
[admin@nodegrid {settings}]# set enable_cluster=yes type=peer
[+admin@nodegrid {settings}]# set cluster_name=cloudname
[+admin@nodegrid {settings}]# set coordinator_address=1.1.1.1
[+admin@nodegrid {settings}]# set psk=presharedkey
[+admin@nodegrid {settings}]# set enable_clustering_access=yes
[+admin@nodegrid {settings}]# commit
```

Copy

5. Repeat the commands for other NodeGrids for the Clustering.

Peers tab

This table lists Nodegrid devices enrolled in the cluster. The table shows information on each device.



Cluster :: Peers

□	Name	Address	Type	Status	Peer Status
□	nodegrid.localdomain	Local	Coordinator	Online	192.168.2.94,192.168.3.47
□	nodegrid.localdomain	192.168.3.47	Peer	Error	

Remove a Peer

1. Go to *Cluster :: Peers*.
2. Locate name to be removed.
3. Select checkbox.
4. Click **Remove**.

Settings tab

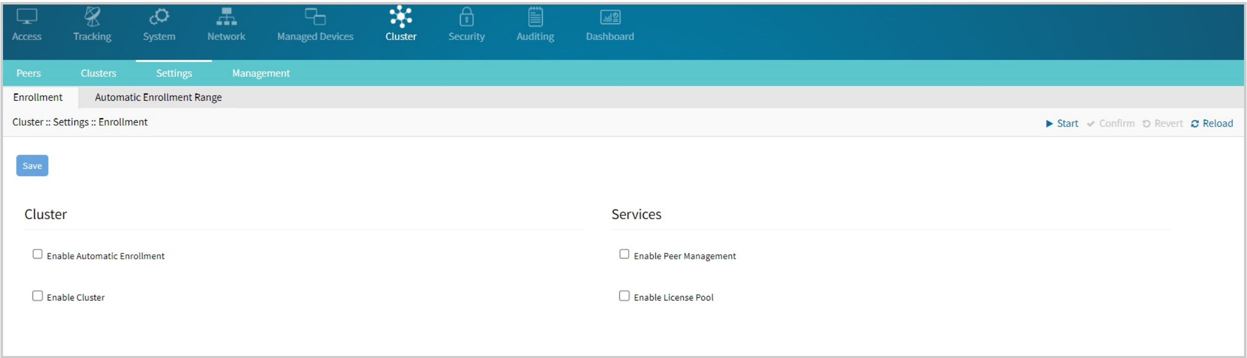
This configures Cluster settings and additional services such as Peer Management and License Pool.

NOTE

The Cluster feature requires a software license for each node in the cluster.

Enrollment sub-tab

This section provides information on the cluster settings required during enrolling cluster automatically, enabling cluster, managing peers in a cluster, and managing licenses within a cluster.



Cluster

□ Enable Automatic Enrollment

□ Enable Cluster

Services

□ Enable Peer Management

□ Enable License Pool

Description of Settings

Automatic Enrollment

With Automatic Enrollment, new Nodegrid devices can automatically become available to an existing cluster. For Peers, this is enabled by default. The Pre-Shared Key setting must be the same on the Coordinator (set by default to **nodegrid-key**). The Interval setting only applies to the Coordinator and regulates how often invitations are sent to potential peers.

Enable Cluster

When enabled, each Cluster requires one Coordinator that controls the enrollment of peer systems. The first unit in the Cluster must be the Coordinator. All other units are Peers. When a Peer device is set to the Coordinator role, the change is automatically propagated. The previous Coordinator device is changed to Peer. Ensure the Coordinator device has Allow Enrollment selected. This provides a Cluster Name and Pre-Shared Key to enroll peers (and used in each Peer's settings). The Cluster Mode can be Star or Mesh.

In MESH, the Coordinator is only required for the enrollment of the peers. Once all Nodegrid systems are enrolled in the Cluster, the Coordinator can be set to Peer (prevents enrollment of other devices.)

Peer Management

Any peers with enabled peer management, are shown under the Central Management tab of the Coordinator.

Allows Nodegrid device hardware to be centrally upgraded. The upgrade process for remote devices is done on the cluster's Management page. The firmware applied to the units must be hosted on a central location, available through a URL (URL should include the remote server's IP or hostname, file path, and the ISO file. If the status shows Disabled, that device is Peer Management disabled.

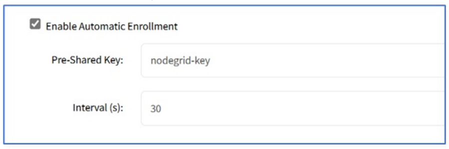
License Pool

The License Pool allows central management of all software licenses within a cluster when enabled. At least one device must be configured as the License Pool Server. In STAR mode, this must be the Coordinator. License Pool Clients automatically request required licenses from the License Pool Server. The Server checks availability and assigns as needed. The client sends a renewal request based on the renewal time. If a client is unavailable for an extended time (exceeding the server's Lease Time), the client's licenses become invalid. The license is returned to the pool.

> **NOTE**
>
> Each Nodegrid device is shipped with five additional test target licenses. A test license is used automatically when a target license is added to the system. This applies if a target license is applied on the License Pool Server. The first time a device requests target licenses, it requests five additional licenses to cover the currently used test licenses.

Configure Cluster

1. Go to *Cluster:: Settings:: Enrollment*.
2. On the *Cluster* menu, select the **Enable Automatic Enrollment** checkbox (expands dialog).



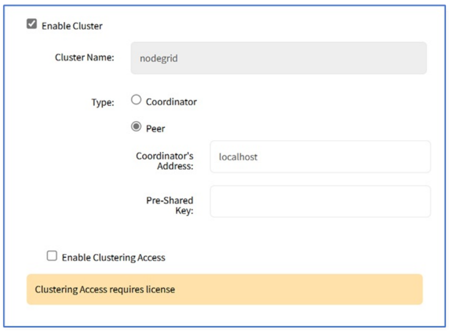
☑ Enable Automatic Enrollment

Pre-Shared Key: nodegrid-key

Interval (s): 30

   a. Enter **Pre-shared Key** (default: nodegrid-key)
   b. Enter **Interval (s)** (default: 30)

3. Select the **Enable Cluster** checkbox (allows other Nodegrid systems to manage, access, and search managed devices from other nodes) (expands dialog).



☑ Enable Cluster

Cluster Name: nodegrid

Type: ○ Coordinator
● Peer

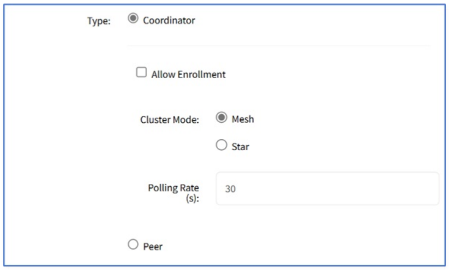
Coordinator's Address: localhost

Pre-Shared Key:

☐ Enable Clustering Access

Clustering Access requires license

a. On *Type* menu, select one:
   - **Coordinator** radio button (expands dialog)



Type: ● Coordinator

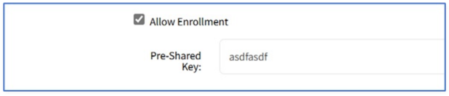
☐ Allow Enrollment

Cluster Mode: ● Mesh
○ Star

Polling Rate (s): 30

○ Peer

   - **Allow Enrollment** checkbox (expands dialog). Enter **Pre-Shared Key**.

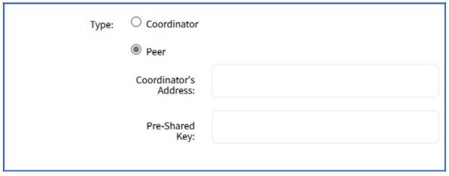


☑ Allow Enrollment

Pre-Shared Key: asdfasdf

     - On the *Cluster Mode* menu, select one radio button (Star, Mesh).
     - Enter **Polling Rate (s)**. (default: 30).

b. **Peer** radio button (expands dialog)



Type: ○ Coordinator
● Peer

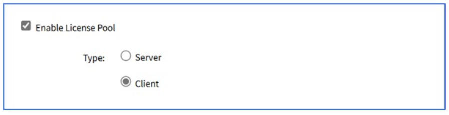
Coordinator's Address:

Pre-Shared Key:

   - **Coordinator's Address** (default: blank)
   - **Pre-Shared Key**

c. Select **Enable Clustering Access** checkbox.

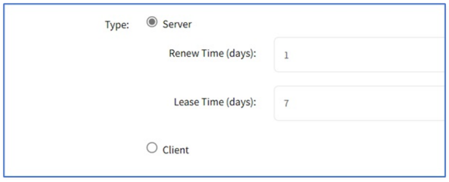
4. On *Services* menu:
   a. Select **Enable Peer Management** checkbox.
   b. Select **Enable License Pool** checkbox (expands dialog).



☑ Enable License Pool

Type: ○ Server
● Client

   c. On *Type* menu, select one:
      - **Server** radio button (expands dialog). Enter **Renew Time (days)** (default 1). Enter **Lease Time (days)** (default 7) (range: 7-30 days).



Type: ● Server

Renew Time (days): 1

Lease Time (days): 7

○ Client

      - **Client** radio button

5. Click **Save**.

Automatic Enrollment Range sub-tab

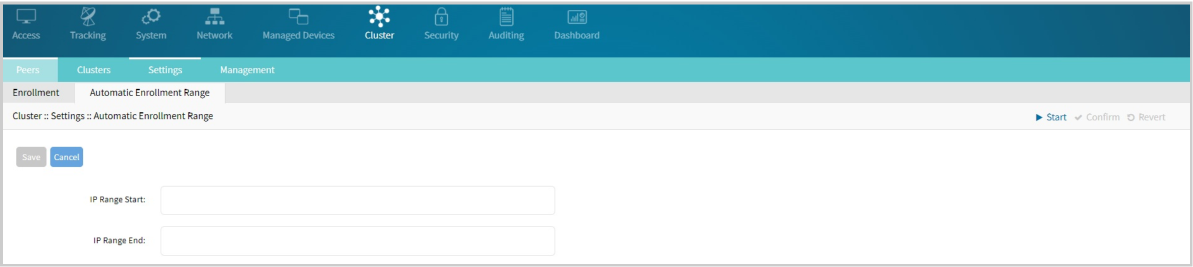
After the Coordinator is enabled and configured, the admin user can add a range of IPs for other Nodegrid devices on the network. This range eliminates the need to go to each Nodegrid node and manually set each as peers.

It is recommended to only add IP's to the Automatic Enrollment Range which are potentially Nodegrid units. When set, invitations are continually sent to all IP's until a Nodegrid device is identified on a specific IP, and then is added to the Cluster.

An existing IP range setting cannot be modified. If an adjustment is needed, create a new IP range and delete the old IP range.

Add Automatic Enrollment Range

1. Go to *Cluster :: Settings :: Automatic Enrollment Range*.
2. Click **Add** (displays dialog).



Cluster :: Settings :: Automatic Enrollment Range

IP Range Start:

IP Range End:

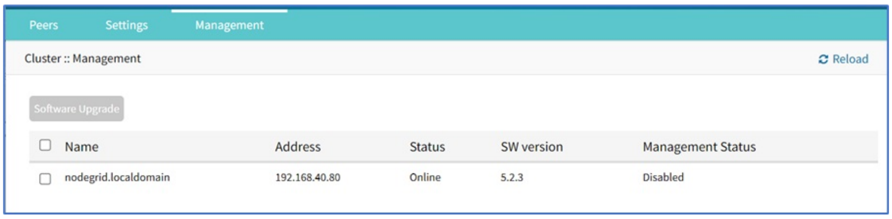
   a. Enter **IP Range Start**.
   b. Enter **IP Range End**.

3. Click **Save**.

Delete Automatic Enrollment Range

1. Go to *Cluster :: Settings :: Automatic Enrollment Range*.
2. Select checkbox next to IP range to delete.
3. Click **Delete**.
4. On confirmation dialog, click **OK**.

Management tab



Cluster :: Management

☐ Name	Address	Status	SW version	Management Status
☐ nodegrid.localdomain	192.168.40.80	Online	5.2.3	Disabled

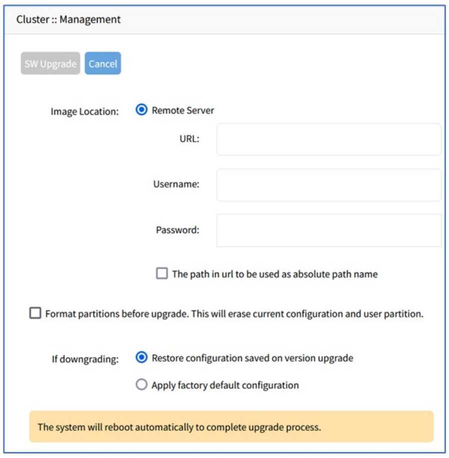
Software Upgrade

Nodegrid can be updated on the WebUI or CLI.

> **NOTE**
>
> Software upgrade/downgrade requires several minutes to process. Be patient.

Software can be upgraded or downgraded on this procedure.

1. Go to *Cluster :: Management*.
2. Select checkbox next to the name for software management.
3. Click **Upgrade Software** (displays dialog).



Cluster :: Management

Image Location: ● Remote Server

URL:

Username:

Password:

☐ The path in url to be used as absolute path name

☐ Format partitions before upgrade. This will erase current configuration and user partition.

If downgrading: ● Restore configuration saved on version upgrade

○ Apply factory default configuration

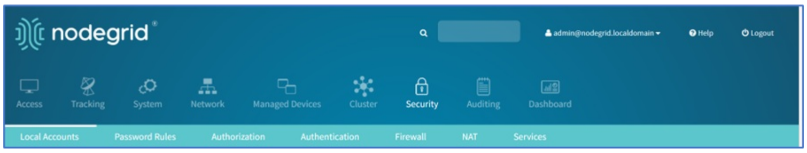
The system will reboot automatically to complete upgrade process.

4. On *Image Location* menu, select **Remote Server**.
   a. Enter **URL** (URL can be the IP address or hostname/FQDN. If using IPv6, use brackets [...]. Supported protocols: FTP, TFTP, SFTP, and SCP.)
   b. Enter **Username and Password**.
   c. (optional) Select **The path in url to be used as absolute path name** checkbox.
   (optional) Select **Format partitions before upgrade. This will erase current configuration and user partition** checkbox.
5. (if applicable) *If downgrading* menu (select one):
   - **Restore configuration saved on version upgrade** radio button
   - **Apply factory default configuration** radio button
6. Review details.
7. Click **SW Upgrade**.

Security Section

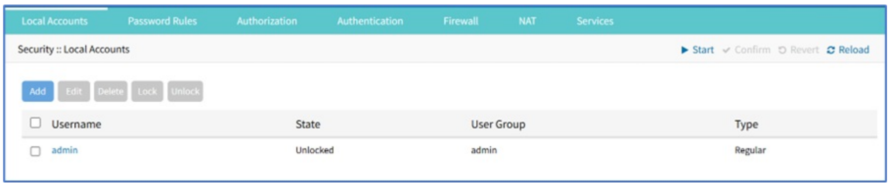
This section provides information on the essential components of Nodegrid device security, covering:

- Local accounts
- Password rules
- Authentication
- Authorization
- Firewall configurations
- NAT settings
- Service settings



Local Accounts tab

New local users can be added, deleted, changed, and locked. Administrators can force passwords to be changed upon next login; and can set expiration dates for user accounts. Administrators can manage API keys for each account. The following sections show provides details on how to manage local user accounts.



Security :: Local Accounts

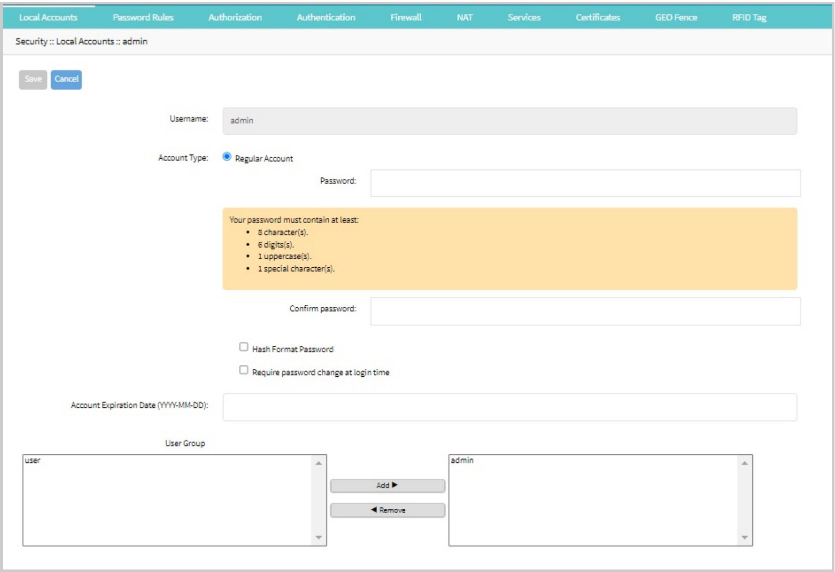
□ Username	State	User Group	Type
□ admin	Unlocked	admin	Regular

Manage Local Users

> **NOTE**
>
> Regardless of activation options, users can change their passwords at any time.

Add Local User

1. Go to *Security :: Local Accounts*.
2. Click **Add** (displays dialog).



Security :: Local Accounts :: admin

Username: admin

Account Type: ● Regular Account

Password:

Your password must contain at least:
- 8 character(s).
- 6 digits(s).
- 1 uppercase(s).
- 1 special character(s).

Confirm password:

□ Hash Format Password

□ Require password change at login time

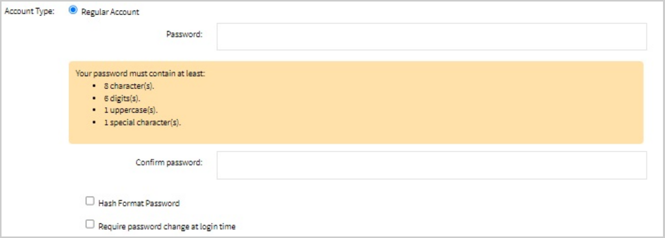
Account Expiration Date (YYYY-MM-DD):

User Group

user

admin

3. Enter **Username.**
4. On the *Account Type* menu, select one.
   - **Regular Account** radio button (expands dialog).



Account Type: ● Regular Account

Password:

Your password must contain at least:
- 8 character(s).
- 6 digits(s).
- 1 uppercase(s).
- 1 special character(s).

Confirm password:

□ Hash Format Password

□ Require password change at login time

     - Enter **Password** and **Confirm Password** (If the password is in a hash format, select the **Hash Format Password** checkbox.). Alternatively, select **Require password change at the login time** checkbox.

> *Note:*
>
> *Set the password based on the rules defined under the Security :: Password Rules tab. You can change the rules from the same tab.*

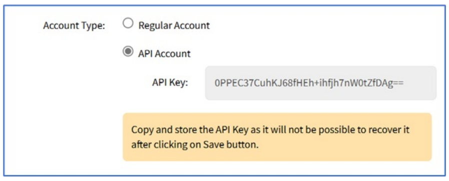
   - **API Account** radio button
     - An API Account will only have access to API requests (not CLI nor WebUI). The API Key can be used directly for API requests authentication in any endpoint, using the `api_key` and `username` headers instead of authenticating to get a ticket and then using the `ticket` header. For example:

Shell

Bash   Copy

```
curl -X GET "https://nodegrid/api/v1/system/preferences" \
    -H "accept: application/json" -H "Content-Type: application/json" \
    -H "api_key: 0PPEC37CuhKJ68fHEh+ihfjh7nW0tZfDAg==" \
    -H "username: myapiuser" -k
```

     - To turn the user into an API Account, select the **API Account** option. The API Key will be automatically generated and displayed.



Account Type: ○ Regular Account

● API Account

API Key: 0PPEC37CuhKJ68fHEh+ihfjh7nW0tZfDAg==

Copy and store the API Key as it will not be possible to recover it after clicking on Save button.

- On the **API Key**, follow this instruction: "*Copy and store the API Key as it will not be possible to recover it after clicking on Save button.*"

5. (optional) **Account Expiration Date (YYYY-MM-DD)**.
6. On the *User Group* panel, select from the left-side panel, and click **Add►** to move to the right-side panel. To remove from the right-side panel, select, and click **◄Remove**.
7. Click **Save**.

Edit Local User

1. Go to *Security :: Local Accounts*.
2. Locate and select checkbox next to username.
3. Click **Edit** (displays dialog).
4. Make changes as needed.
5. Click **Save**.

Delete Local User

Deleting a local user account on your Nodegrid device involves removing a user profile and all associated data, such as files, settings, and installed applications. This step is crucial when a user no longer requires access to the device. Removing unused accounts helps protect your device from unauthorized access, safeguarding sensitive information.

Web UI Procedure

1. Go to *Security :: Local Accounts*.
2. Locate and select checkbox next to username.
3. Click **Delete**.
4. On the confirmation dialog, click **OK**.

CLI Procedure

Use the delete command to delete the user account using CLI.

Syntax

Plaintext Copy

```
[admin@nodegrid /]# delete
```

Parameters

Parameter	Description
delete <target>	Delete one target
delete -	Deletes ALL targets
delete <target1>,<target2>	Deletes multiple targets

Arguments

Arguments	Description
-f, --force	Skips all confirmation prompts
-q, --quiet	Hides all error and warning messages
-fq, -qf	Arguments can be combined for simultaneous functionality

Examples

To delete users:

Plaintext Copy

```
[admin@nodegrid local_accounts]# show
  username  state     user group  type
  ========  ========  ==========  =======
  admin     Unlocked  admin       Regular
  user1     Unlocked  user        Regular
  user2     Unlocked  user        Regular
[admin@nodegrid local_accounts]# delete -
are you sure you want to delete this user from the local database? (yes, no) : yes
Warning: Protected users cannot be deleted
[+admin@nodegrid local_accounts]# show
  username  state     user group  type
  ========  ========  ==========  =======
  admin     Unlocked  admin       Regular
```

To delete users by including - -force and - -quiet arguments. The - -force argument deletes the users without a confirmation message and the - -quiet argument suppresses error and warning messages, making it ideal for automation deployment.

To delete users by including - -force argument:

Plaintext Copy

```
[admin@nodegrid local_accounts]# show
  username  state     user group  type
  ========  ========  ==========  =======
  admin     Unlocked  admin       Regular
  user1     Unlocked  user        Regular
  user2     Unlocked  user        Regular
[admin@nodegrid local_accounts]# delete - --
--force  --quiet
[+admin@nodegrid local_accounts]# delete - --force
Warning: Protected users cannot be deleted
  [+admin@nodegrid local_accounts]# show
  username  state     user group  type
  ========  ========  ==========  =======
  admin     Unlocked  admin       Regular
```

To delete users by including - -quiet argument:

Plaintext Copy

```
[admin@nodegrid local_accounts]# show
  username  state     user group  type
  ========  ========  ==========  =======
  admin     Unlocked  admin       Regular
  user1     Unlocked  user        Regular
  user2     Unlocked  user        Regular
[admin@nodegrid local_accounts]# delete - --
--force  --quiet
[+admin@nodegrid local_accounts]# delete - --quiet
are you sure you want to delete this user from the local database? (yes, no) : yes
  [+admin@nodegrid local_accounts]# show
  username  state     user group  type
  ========  ========  ==========  =======
  admin     Unlocked  admin       Regular
```

To delete users by combining both the - -force and - -quiet arguments:

Plaintext Copy

```
[admin@nodegrid local_accounts]# show
  username  state     user group  type
  ========  ========  ==========  =======
  admin     Unlocked  admin       Regular
  user1     Unlocked  user        Regular
  user2     Unlocked  user        Regular
[admin@nodegrid local_accounts]# delete - --
--force  --quiet
[+admin@nodegrid local_accounts]# delete - --force --quiet
[+admin@nodegrid local_accounts]# show
  username  state     user group  type
  ========  ========  ==========  =======
  admin     Unlocked  admin       Regular
```

NOTE:

There are also short forms for the - -force and - -quiet arguments. The following are these arguments:

-f	- -force argument
-q	- -quiet argument
-fq -qf	- -force - -quiet arguments combined

Lock Local User

The administrator can lock a user out of the device.

1. Go to *Security :: Local Accounts*.
2. Locate and select checkbox next to username.
3. Click **Lock** (locks user out of device).

Unlock Local User

As needed, the administrator can unlock a user.

1. Go to *Security :: Local Accounts*.
2. Locate and select checkbox next to username.
3. Click **Unlock** (allows user access)

There is a function whereby the user is authorized by an external authentication provider (LDAP, AD, or TACACS+) and the Local user account is locked. The user can authenticate with the sshkey, but permissions are enforced based on his group permissions with the external authentication provider.

Hash Format Password

As needed, the administrator can use a hash format password, rather than plain password. This can be used for scripts (avoids requiring scripts to use actual user passwords). The hash password must be generated separately beforehand. Use a hash password generator. These applications (OpenSSL, chpasswd, mkpasswd) use MD5, SHA256, SHA512 engines.

Hash Format

CLI Procedure

The Nodegrid Platform has an OpenSSL version. In the Console, use this:

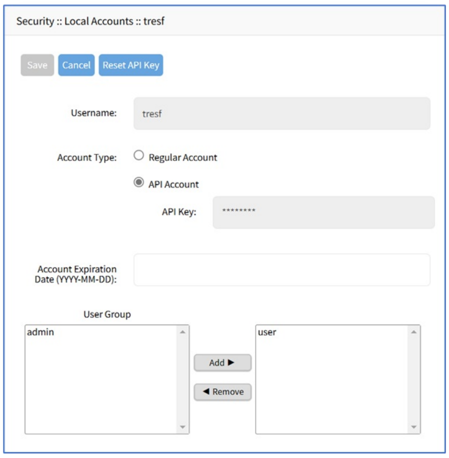
Plaintext Copy

```
root@nodegrid:~# openssl passwd -1 -salt mysall
Password:
$1$mysall$YBFr9On0wjde5be32mC1g1
```

Generate a new API key for a User

In the *Type* column, the user must have a value of **API**.

1. Go to *Security :: Local Accounts*.
2. Locate and click the user's name – *Type* column must be **API** (displays dialog). (Alternatively, select checkbox and click **Edit**.)



Security :: Local Accounts :: tresf

Username: tresf

Account Type: ○ Regular Account ● API Account

API Key: ********

Account Expiration Date (YYYY-MM-DD):

User Group

admin

user

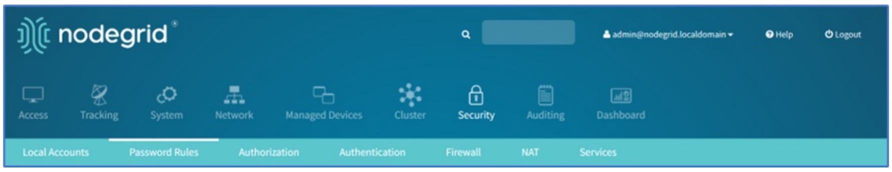
3. Click **Reset API Key**.

> **IMPORTANT**
>
> The new key is displayed in the API Key field. Copy the key and save in a secure location.

4. Click **Save**.

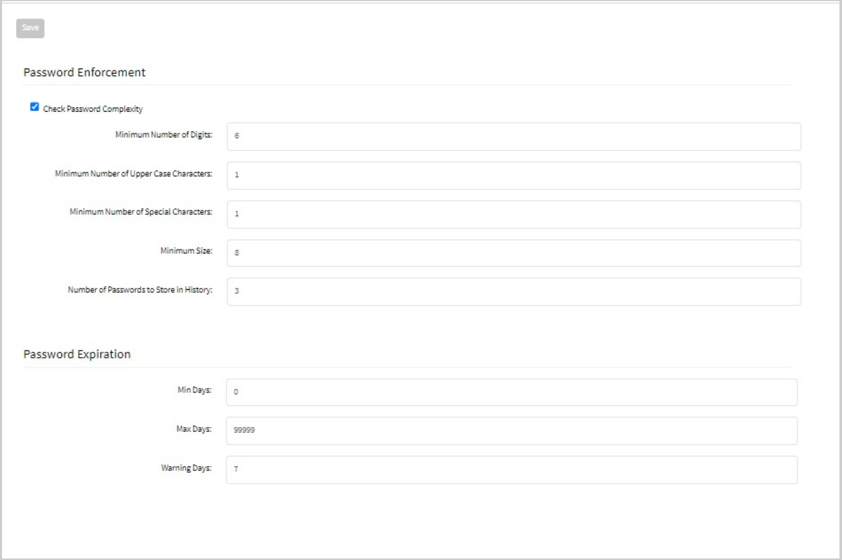
Password Rules tab

When password rules are configured for the Nodegrid Platform, all local user accounts are subject. The administrator can set password complexity as well as password expiration.



Modify Password Rules

1. Go to *Security :: Password Rules*.
2. On the *Password Enforcement* menu, enter the details:



Password Enforcement

☑ Check Password Complexity

Minimum Number of Digits: 6

Minimum Number of Upper Case Characters: 1

Minimum Number of Special Characters: 1

Minimum Size: 8

Number of Passwords to Store in History: 3

Password Expiration

Min Days: 0

Max Days: 99999

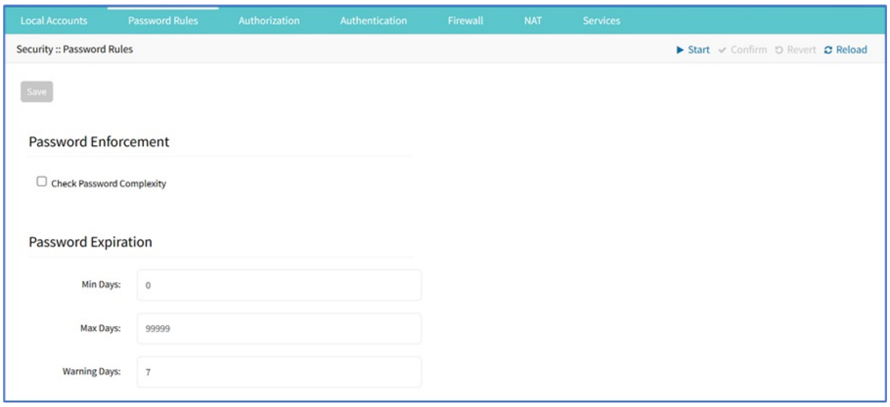
Warning Days: 7

   a. **Check the Password Complexity**checkbox (expands dialog).
      i. **Minimum Number of Digits** (default: 0)
      ii. **Minimum Number of Upper Case Characters** (default: 0)
      iii. **Minimum Number of Special Characters** (default: 0)
      iv. **Minimum Size**. (default: 8)

   b. **Number of Passwords to Store in History** (default: 1)

3. On the *Password Expiration* menu, enter the details:
   a. **Min Days** (default: 0)
   b. **Max Days** (default: 99999)
   c. **Warning Days** (default: 7)

4. Click **Save**.



Password Enforcement

□ Check Password Complexity

Password Expiration

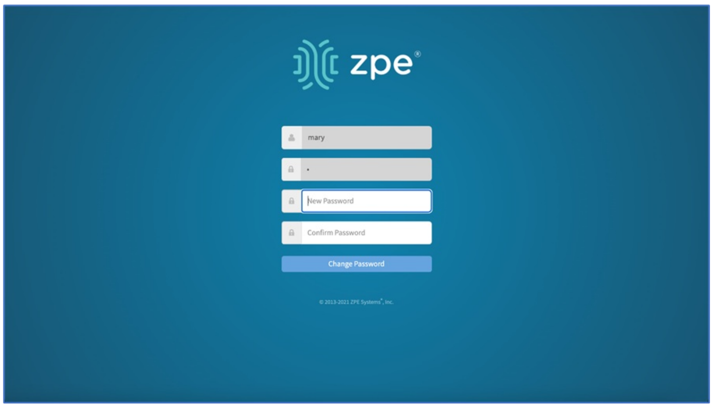
Min Days: 0

Max Days: 99999

Warning Days: 7

User Response to Expired Password

When the password is configured to expire after a specified time, on user login, this is the response on the WebUI.



mary

•

When this displays, enter **New Password** and **Confirm Password**, then click **Change Password**.

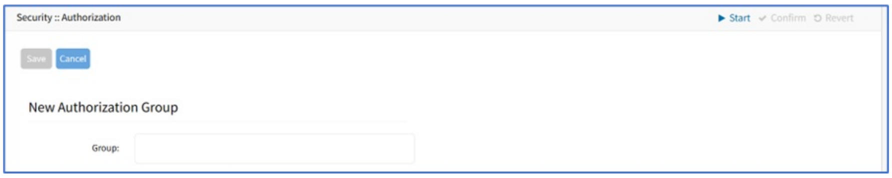
Authorization tab

User groups combine multiple local and remote users into a single local group. Members are assigned group-specific roles/permissions. Members have access to devices assigned to that group. Groups which are authenticated against an external authentication provider are mapped to local groups. When a user is assigned to a group, that user received the combined access rights. Administrators can add and delete groups, as well as change permissions. On the device's original configuration, two default groups are available: Admin and Users. The Admin group grants full system and target access.

Manage User Groups

Add User Group

1. Go to *Security :: Authorization*.
2. Click **Add** (displays dialog).



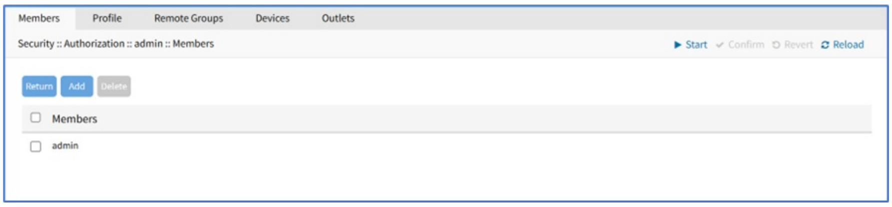
3. Enter **Group Name**.
4. Click **Save**.

Delete User Group

1. Go to *Security :: Authorization*.
2. Select checkbox next to group to be deleted.
3. Click **Delete**.
4. On the confirmation dialog, click **OK**.

Manage User Group Configuration

Groups are configured in this section. To access, click on an existing user group.



User Group Configuration Process

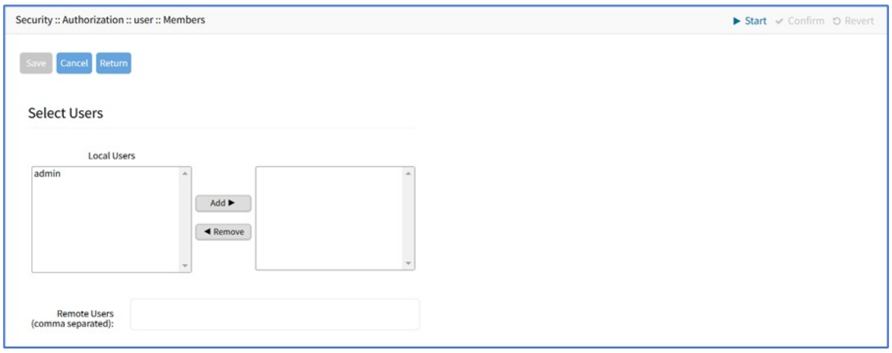
This is the configuration process for a User Group.

1. Create a user group.
2. Add local and remote users to the group.
3. Configure group system permissions and settings.
4. Assign access to remote server groups.
5. Add devices and configure permissions.
6. Add and configure power outlet details.

Members sub-tab

Add Members to User Group

1. Go to *Security :: Authorization*.
2. Click the **Group Name**.
3. On **Members** sub-tab, click **Add** (displays dialog).

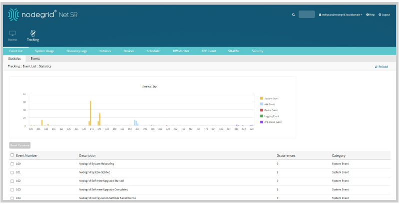
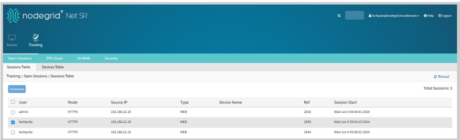
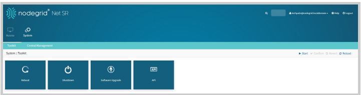
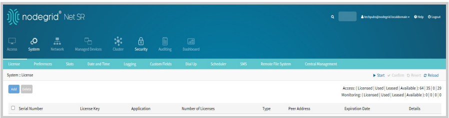


4. In the *Local Users* (left) panel, to add, select from left-side panel, click **Add**► to move to right-side panel. To remove from right-side panel, select, and click ◄**Remove**.
5. Click **Save**.

Configuring Group Profiles Permissions

This section explains how to assign system permissions to group profiles. You can manage user access using permission sets without changing the user profiles. The following table lists:

- Available permissions for users.
- Description of the permission.
- Web UIs and commands demonstrating the functions enabled for the user when each corresponding permission is enabled.

Permission	Description	Commands Enabled
Track System Information	Allows access to track information about the Nodegrid devices and the devices connected to them. The information includes the Event List, System Usage, Discovery Logs, and so on as indicated in the following figure. 	Plaintext Copy event_list routing_table system_usage sdwan discovery_logs serial_statistics serial_ports_summary lldp ipsec_table mac_table wireguard hotspot qos dhcp dhcp_ranges flow_exporter network_statistics network_failover_status network_failover_history switch_statistics mstp_statistics usb_devices usb_serial_stats wireless_modem gps geo_fence bluetooth scheduler_logs hw_monitor zpe_cloud about firewall_table nat_table
Terminate Sessions	Allows to terminate any open Nodegrid sessions. 	Plaintext Copy cluster_peers cluster_clusters open_sessions device_sessions about
Software Upgrade and Reboot System	Allows to upgrade and reboot the Nodegrid software. 	Plaintext Copy toolkit about
Configure System	Allows to configure the system. 	

Plaintext Copy

```
system/about/
system/fips/
settings/zpe_cloud
settings/fips_140
settings/license
settings/flow_exporter
settings/qos
settings/system_preferences
settings/slots
settings/custom_fields
settings/remote_file_system
settings/system_logging
settings/date_and_time
settings/ntp_authentication
settings/ntp_server
settings/dial_up
settings/sms_settings
settings/sms_whitelist
settings/scheduler
settings/devices
settings/types
settings/auto_discovery
settings/power_menu
settings/devices_session_preferences
settings/devices_views_preferences
settings/cluster
settings/network_settings
settings/network_connections
settings/network_failover
settings/switch_interfaces
settings/switch_backplane
settings/switch_vlan
settings/switch_global
settings/switch_acl
settings/switch_lag
settings/switch_mstp
settings/switch_port_mirroring
settings/switch_dhcp_snooping
settings/802.1x
settings/static_routes
settings/hosts
settings/snmp
settings/dhcp_server
settings/dhcp_relay
settings/authentication
settings/ipv4_firewall
settings/ipv6_firewall
settings/ipv4_nat
settings/ipv6_nat
settings/ssl_vpn
settings/central_management
settings/ipsec
settings/wireguard
settings/frr
settings/routing
settings/sdwan
settings/wireless_modem
settings/services
settings/certificates
settings/geo_fence
settings/auditing
```

Note:

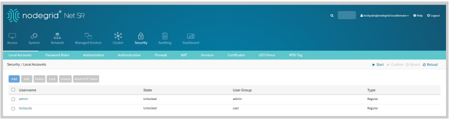
If you select the option **Restrict Configure System Permission to Read Only**, all commands from the above list are disabled except for:

Plaintext Copy

```
acknowledge_alarm_state
edit
event_system_audit
```

Configure User Accounts

Allows to configure users and groups such as admin users, root users, and so on. To enable Configure User Accounts, Configure System Settings must also be enabled.

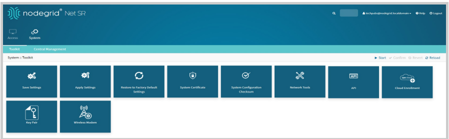


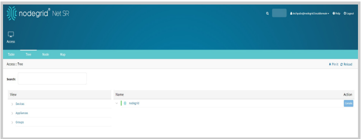
Security :: Local Accounts

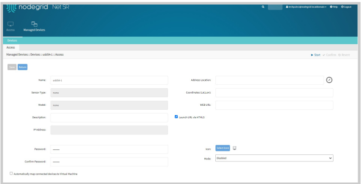
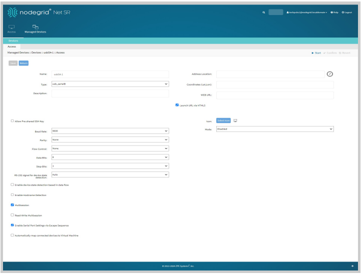
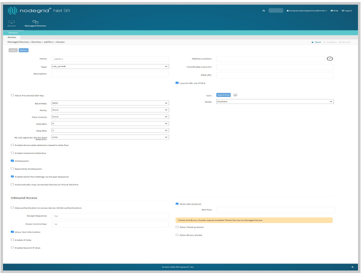
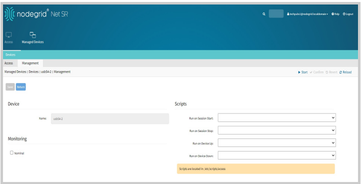
□	Username	State	User Group	Type
□	admin	Unlocked	admin	Regular
□	techpubs	Unlocked	user	Regular

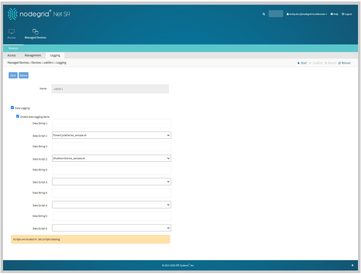
Plaintext Copy

```
system/about/
system/fips/
settings/zpe_cloud
settings/fips_140
settings/license
settings/flow_exporter
settings/qos
settings/system_preferences
settings/slots
settings/custom_fields
settings/remote_file_system
settings/system_logging
settings/date_and_time
settings/ntp_authentication
settings/ntp_server
settings/dial_up
settings/sms_settings
settings/sms_whitelist
settings/scheduler
settings/devices
settings/types
settings/auto_discovery
settings/power_menu
settings/devices_session_preferences
settings/devices_views_preferences
settings/cluster
settings/network_settings
settings/network_connections
settings/network_failover
settings/switch_interfaces
settings/switch_backplane
settings/switch_vlan
settings/switch_global
settings/switch_acl
settings/switch_lag
settings/switch_mstp
settings/switch_port_mirroring
settings/switch_dhcp_snooping
settings/802.1x
settings/static_routes
settings/hosts
settings/snmp
settings/dhcp_server
settings/dhcp_relay
settings/local_accounts
settings/password_rules
settings/authorization
settings/authentication
settings/ipv4_firewall
settings/ipv6_firewall
settings/ipv4_nat
settings/ipv6_nat
settings/ssl_vpn
settings/central_management
settings/ipsec
settings/wireguard
settings/frr
settings/routing
settings/sdwan
settings/wireless_modem
settings/services
settings/certificates
settings/geo_fence
settings/auditing
```

Apply & Save Settings	Executes Nodegrid device configurations Apply settings and Save Settings.
	
	 nodegrid Net SR
	Access
	System
	Toolkit
	Central Management
	System :: Toolkit
	Start
	Confirm
	Revert
	Reload
	Save Settings
	Apply Settings
	Restore to Factory Default Settings
	System Certificate
	System Configuration Checksum
	Network Tools
	API
	Cloud Enrollment
	Key Pair
	Wireless Modem
		Plaintext Copy
		`toolkit`
		`about`

Shell Access	Enables shell access to the Nodegrid device. 	Plaintext Copy `about`

Manage Devices	Enables access to devices connected to the Nodegrid device. Enabling manage devices will require enabling at least one of the following permissions at the device level. Device permissions include:
	• General Settings
	
	• Connection Settings
	
	• Inbound Settings
	
	• Management
	
	• Logging
		Plaintext Copy
		`access/`
		`management/`
		`logging/`
		`custom_fields/`
		`commands/`



Managed Devices :: Devices :: usbS4-1 :: Logging

Name: usbS4-1

☑ Data Logging

☑ Enable data logging alerts

Data String 1:

Data Script 1: PowerCycleDevice_sample.sh

Data String 2:

Data Script 2: ShutdownDevice_sample.sh

Data String 3:

Data Script 3:

Data String 4:

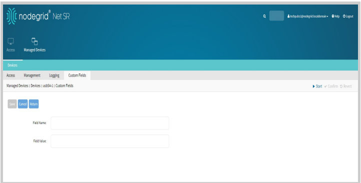
Data Script 4:

Data String 5:

Data Script 5:

Scripts are located in: /etc/scripts/datalog

- Custom Fields

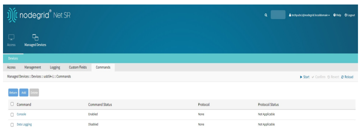


Managed Devices :: Devices :: usbS4-1 :: Custom Fields

Field Name:

Field Value:

- Commands



Managed Devices :: Devices :: usbS4-1 :: Commands

Command	Command Status	Protocol	Protocol Status
Console	Enabled	None	Not Applicable
Data Logging	Disabled	None	Not Applicable

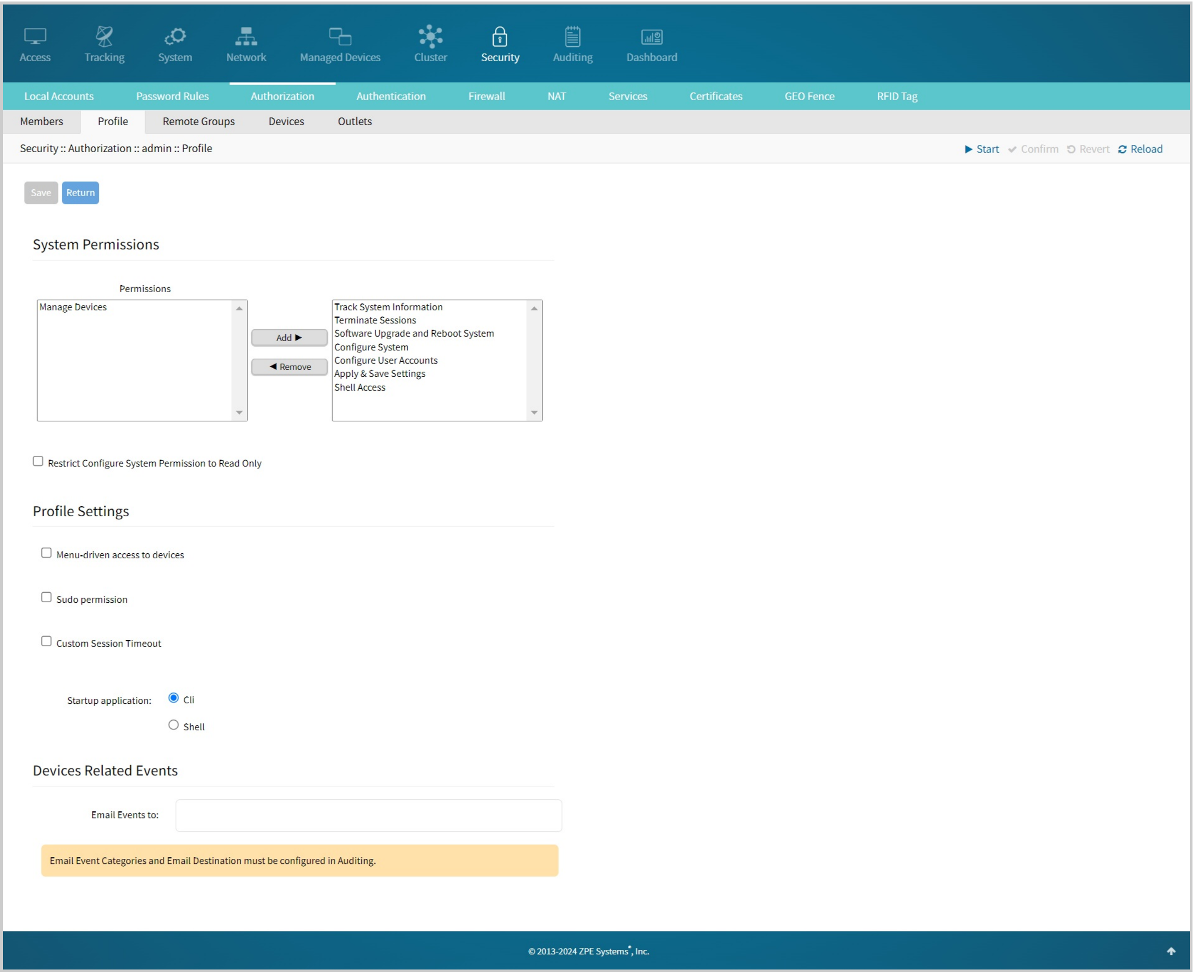
- Outlets
- Sensor Channels

You can enable either Manage Devices or Configure System permission. Both these permissions cannot be selected together for a device.

Procedure

To configure a user profile:

1. Go to *Security :: Authorization*.
2. Click on the **Group Name**.
3. Click on the **Profile** sub-tab.



Security :: Authorization :: admin :: Profile

System Permissions

Permissions

Manage Devices

Track System Information
Terminate Sessions
Software Upgrade and Reboot System
Configure System
Configure User Accounts
Apply & Save Settings
Shell Access

□ Restrict Configure System Permission to Read Only

Profile Settings

□ Menu-driven access to devices

□ Sudo permission

□ Custom Session Timeout

Startup application: ● Cli ○ Shell

Devices Related Events

Email Events to:

Email Event Categories and Email Destination must be configured in Auditing.

4. In the *System Permissions* menu:
   a. To add, select from the left-side panel, and click **Add ▶** to move to the right-side panel. To remove from the right-side panel, select, and click **◀Remove**.
   b. Select **Restrict Configure System Permission to Read Only** checkbox (granted system settings are visible but cannot be changed)

5. In the *Profile Settings* menu:
   a. Select the **Menu-driven access to devices** checkbox (group members presented a target menu when SSH connection to the Nodegrid device is established).
   b. Select the **Sudo permission** checkbox (users can execute sudo commands).
   c. Select the **Custom Session Timeout** checkbox (enables a custom session time).
   d. Set **Timeout [seconds]**.
   e. On the *Startup application* menu, select one (**Cli**, **Shell**).

6. In the *Devices Related Events* menu, enter **Email Events to** (comma-separated)

> **NOTE**
>
> *Email Event Categories* and *Email Destinations* are configured in the *Auditing* section.

7. Click **Save**.

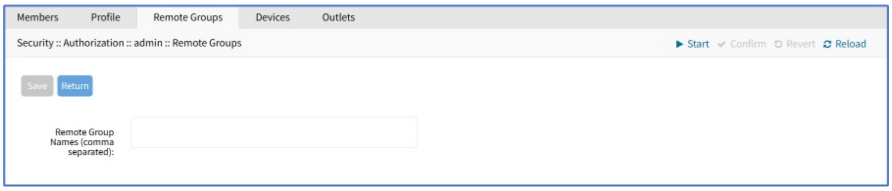
Remote Groups sub-tab

Assign Remote Groups

External remote groups must be assigned to a local group. This ensures the remote group gets the correct permissions.

> **NOTE**
>
> This step is required for LDAP, AD, and Kerberos groups. Radius and TACACS+ authentication providers use other methods to link external groups/users to local groups.

1. Go to *Security :: Authorization*.
2. Click on the **Group Name**,
3. On the **Remote Groups** sub-tab, enter **Remote Group Names** (comma-separated).



Remote Group Names (comma separated):

4. Click **Save**.

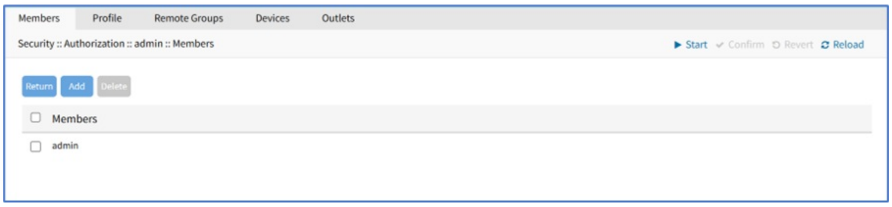
Depending on system permission, access to specific devices can be assigned to groups. Devices must be added to the group. Appropriate access rights can be set. Multiple devices can be added at the same time.

> **NOTE**
>
> Access permissions to control power outlets are granted through the Outlets permissions and not through Devices

Devices sub-tab

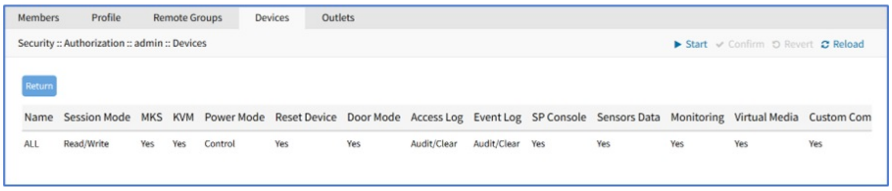
Assign Devices (Admin)

1. Go to *Security :: Authorization :: Members*.



□ Members
□ admin

2. Click on **Admin** name and go to **Devices** sub-tab.



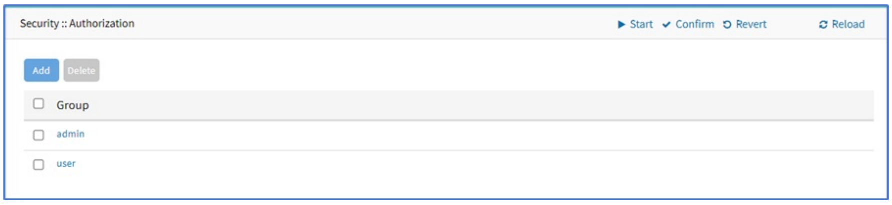
Name	Session Mode	MKS	KVM	Power Mode	Reset Device	Door Mode	Access Log	Event Log	SP Console	Sensors Data	Monitoring	Virtual Media	Custom Com
ALL	Read/Write	Yes	Yes	Control	Yes	Yes	Audit/Clear	Audit/Clear	Yes	Yes	Yes	Yes	Yes

With the **ALL** configuration, admin users have all permissions to devices: Read/Write, Power, Command, etc.

> NOTE
>
> No additions/changes can be made to available devices or device permissions.

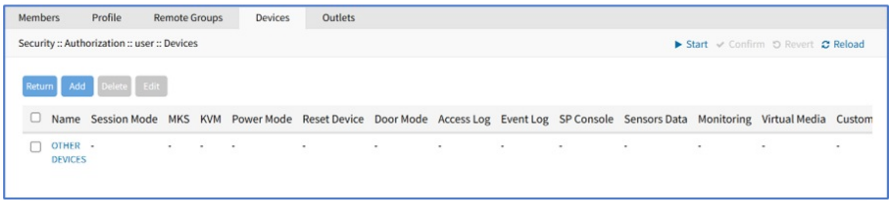
Assign Devices (other groups)

1. Go to *Security :: Authorization*.



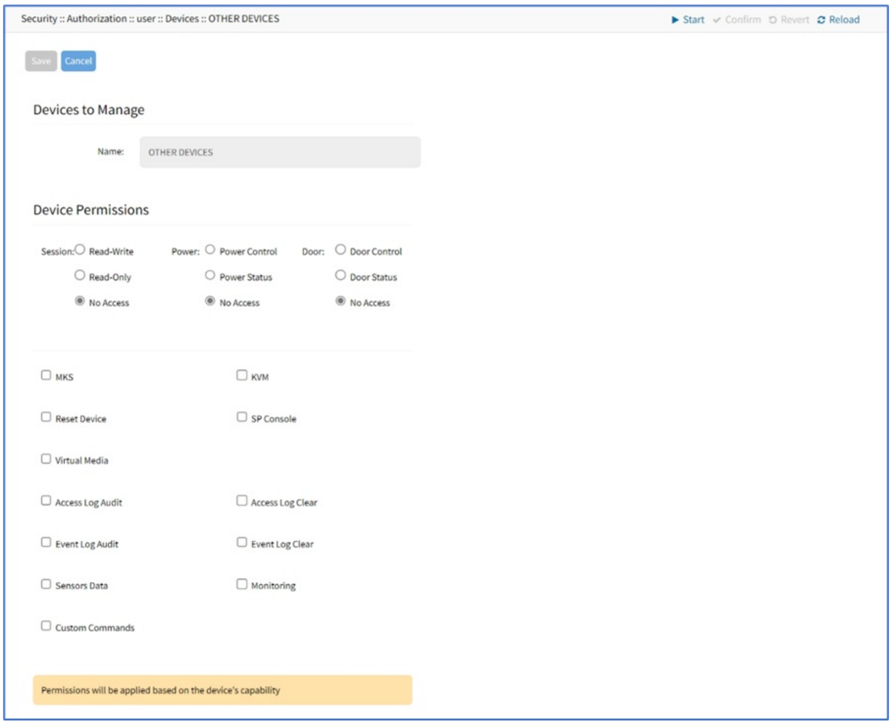
□ Group
□ admin
□ user

2. Click on **Users** (or other group name) and go to **Devices** sub-tab.



□	Name	Session Mode	MKS	KVM	Power Mode	Reset Device	Door Mode	Access Log	Event Log	SP Console	Sensors Data	Monitoring	Virtual Media	Custom
□	OTHER DEVICES	-	-	-	-	-	-	-	-	-	-	-	-	-

3. Click on **OTHER DEVICES** (displays dialog).


Security :: Authorization :: user :: Devices :: OTHER DEVICES
▶ Start
✓ Confirm
Revert
Reload
Save
Cancel

Devices to Manage

Name: OTHER DEVICES

Device Permissions

Session: ○ Read-Write ○ Read-Only ● No Access

Power: ○ Power Control ○ Power Status ● No Access

Door: ○ Door Control ○ Door Status ● No Access

□ MKS □ KVM

□ Reset Device □ SP Console

□ Virtual Media

□ Access Log Audit □ Access Log Clear

□ Event Log Audit □ Event Log Clear

□ Sensors Data □ Monitoring

□ Custom Commands

Permissions will be applied based on the device's capability

4. *Device Permissions* menu, select checkbox in each section:

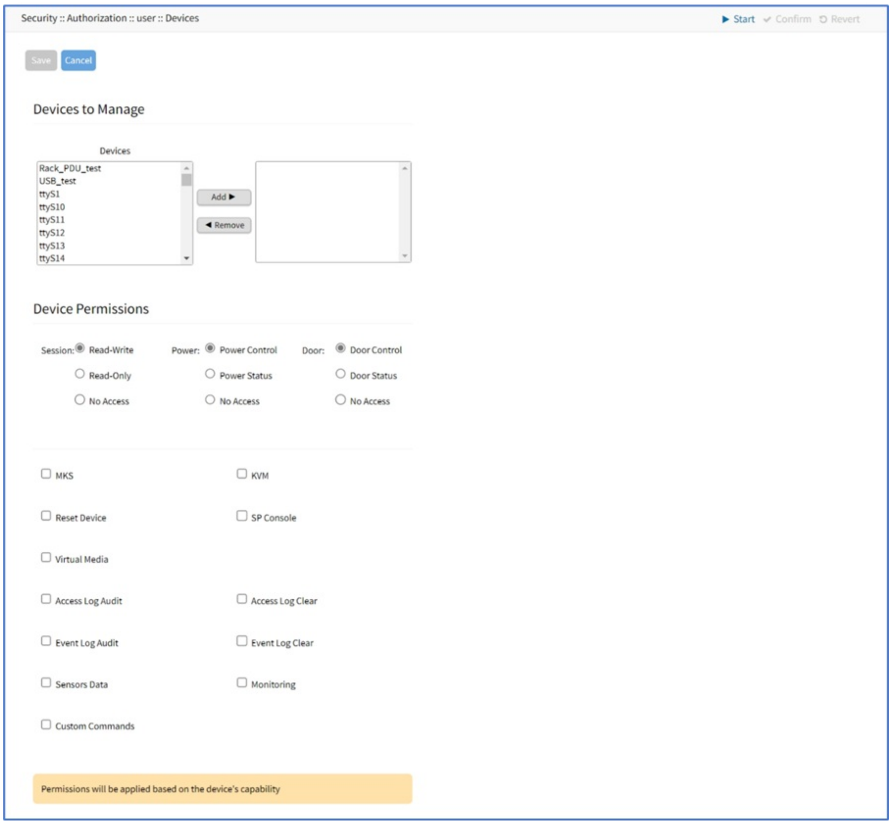
5. On *Sessions* menu, select one (Read-Write, Read-Only, No Access).
6. On *Power* menu, select one (Power Control, Power Status, No Access).
7. On *Door* menu, select one (Door Control, Door Status, No Access)
8. Select checkboxes, as appropriate:
   - **MKS** (access to MKS sessions)
   - **KVM** (access to KVM sessions)
   - **Reset Device** (permission to reset a device session)
   - **SP Console** (access to IPMI console sessions - serial over LAN)
   - **Virtual Media** (access to start a Virtual Media session to an IPMI device)
   - **Access Log Audit** (access to read the access log of an IPMI device)
   - **Access Log Clear** (permission to clear the access log of an IPMI device)
   - **Event Log Audit** (permission to read the device-specific event log)
   - **Event Log Clear** (permission to clear the device-specific Event Log)
   - **Sensors Data** (permission to access monitoring features)
   - **Monitoring** (permission to read sensor data)
   - **Custom Commands** (permission to execute custom commands).
9. Click **Save**.

NOTE

To add individual devices and set permissions, use the *Add Devices and Configure Permissions* procedure.

Add Devices and Configure Permissions

1. Go to *Security :: Authorization*.
2. Click on the **Group Name**.
3. On the **Devices** sub-tab, click **Add** (displays dialog).



Session: ● Read-Write ○ Read-Only ○ No Access

Power: ● Power Control ○ Power Status ○ No Access

Door: ● Door Control ○ Door Status ○ No Access

□ MKS □ KVM

□ Reset Device □ SP Console

□ Virtual Media

□ Access Log Audit □ Access Log Clear

□ Event Log Audit □ Event Log Clear

□ Sensors Data □ Monitoring

□ Custom Commands

Permissions will be applied based on the device's capability

4. On *Devices to Manage* menu, on *Devices* panel: To add, select from left-side panel, click **Add►** to move to right-side panel. To remove from right-side panel, select, and click **◄Remove**.
5. On *Device Permissions* menu, select as needed:
   a. On *Sessions* menu, select one (Read-Write, Read-Only, No Access).
   b. On *Power* menu, select one (Power Control, Power Status, No Access).
   c. On *Door* menu, select one (Door Control, Door Status, No Access)
6. Select/unselect the following settings (as needed):
   - **MKS** (access to MKS sessions)
   - **KVM** (access to KVM sessions)
   - **Reset Device** (permission to reset a device session)
   - **SP Console** (access to IPMI console sessions - serial over LAN)
   - **Virtual Media** (access to start a Virtual Media session to an IPMI device)
   - **Access Log Audit** (access to read the access log of an IPMI device)
   - **Access Log Clear** (permission to clear the access log of an IPMI device)
   - **Event Log Audit** (permission to read the device-specific event log)
   - **Event Log Clear** (permission to clear the device-specific Event Log)
   - **Sensors Data** (permission to access monitoring features)
   - **Monitoring** (permission to read sensor data)
   - **Custom Commands** (permission to execute custom commands).
7. Click **Save**.

Edit Device in Group

1. Go to *Security :: Authorization*.
2. Click on the **Group Name**.
3. Click on the **Devices** sub-tab.
4. In the **Name** column, click on the device name. Alternatively, select checkbox and click **Edit**.
5. Make changes as needed.
6. Click **Save**.

Delete Device from Group

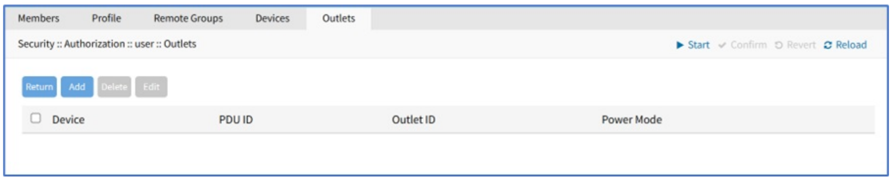
1. Go to *Security :: Authorization*.
2. Click on the **Group Name**.
3. Click on the **Devices** sub-tab.
4. Select checkbox and click **Delete**.

Outlets sub-tab

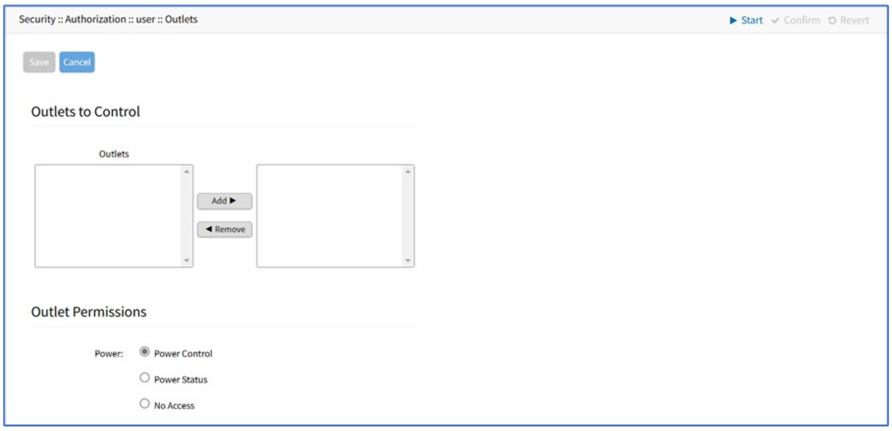
Add and Configure Power Outlets

Access permissions for power outlets from Rack PDUs are controlled individually as the power to turn on or off a device can have severe consequences for the running of a data center or remote location. The assignment of permissions is analogous to device's access permissions.

1. Go to *Security :: Authorization*.
2. Click on the **Group Name**.
3. Click **Outlets** sub-tab.



4. Click **Add** (displays dialog).



5. On *Outlets to Control* menu, *Outlets* panel: To add, select from left-side panel, click **Add►** to move to right-side panel. To remove from right-side panel, select, and click **◄Remove**.
6. On *Outlet Permissions* menu, select one:
   - **Power Control** radio button (permission to turn on or off an outlet)
   - **Power Status** radio button (permission to see the current outlet status)
   - **No Access** radio button (no access to outlet)
7. Click **Save**.

Configure SSH Key Authentication

The Nodegrid platform allows use of SSH keys for authorization. The feature is often used to allow automation systems to gain secure access without a password. It works well with direct Shell access and users who want to use SSH keys for a local home directory. This feature is available for all local, LDAP, AD, and TACACS+ users. Radius users cannot use SSH keys for authentication.

Configure SSH Key Authorization

1. Go to *Security :: Authorization*.
2. In the Group column, click on a name.
3. On the group's **Profile** sub-tab, in *Startup application* menu:
    a. Select **Shell** radio button (gives group members default shell access, and not CLI access, on connection via SSH).
    b. Click **Save**.
4. Go to *Security :: Local Accounts*.
5. Create a local user and add to the new group.

The SSH key can be used for authentication. The default SSH tools can copy the SSH key to the Nodegrid device (i.e., SSH-copy-id).

> NOTE
>
> If the user needs default CLI access, and not Shell access, remove the user from the newly created Group.

Authentication tab

Authentication validates the user, usually with credentials that, most often, take the form of a username and password. Authorization is an essential security feature that complements authentication. Once authenticated with credentials, authorization determines access (i.e., directories, functions, features, and displays).

Nodegrid devices have a built-in admin user account named 'admin'. This has full access and rights to all configurable unit functions: network, security, authentication, authorization, managed devices, including other users. The admin account cannot be deleted (initial default password: admin).

> NOTE
>
> For security reasons, during the first login, administrators are immediately required to change the default password. Use the Change Password option on the pull-down menu under the username (upper right corner of the WebUI).

Authentication of local users and groups is fully supported, as well as external users and groups. External authentication of users and groups can be done through LDAP/AD, TACACS+, Radius and Kerberos.

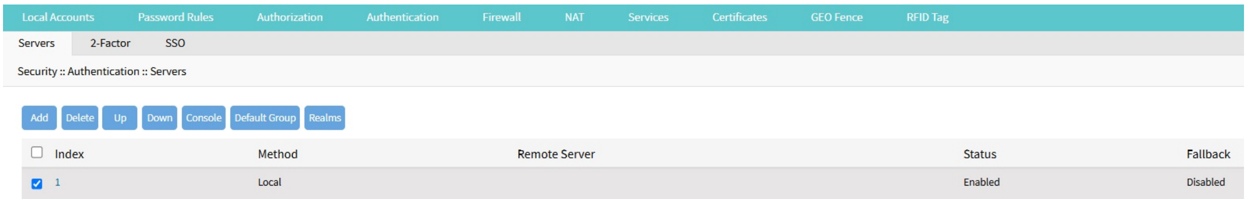
By default, all users have access to enabled managed devices. Based on assigned groups, users have limited access to Nodegrid Web portal management attributes. User privileges can be modified with profile and access rights in an authorization group.

A user in the Admin group has the same administrative privileges as the initial admin user. Each user must have a specific user account on a Nodegrid device. An external authentication server can provide authenticated access. A user can be assigned to one or more groups.

> NOTE
>
> The device's root user and Admin group users can still bypass 2-Factor Authentication in Console and WebUI, in case the remote server is unreachable.

Servers sub-tab

Authentication server configuration is done on this page.

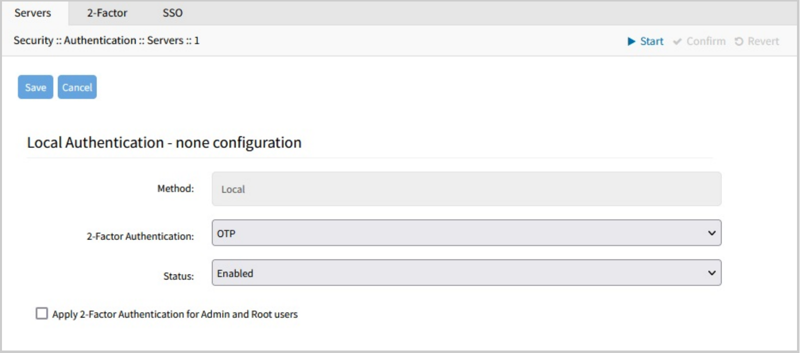


Security :: Authentication :: Servers

☐ Index	Method	Remote Server	Status	Fallback
☑ 1	Local		Enabled	Disabled

Edit Local Authentication

Click on the Index of the *Local* authentication server to enable/disable it, or set 2-Factor Authentication if a method is configured in the *2-Factor* tab:



Security :: Authentication :: Servers :: 1

Local Authentication - none configuration

Method: Local

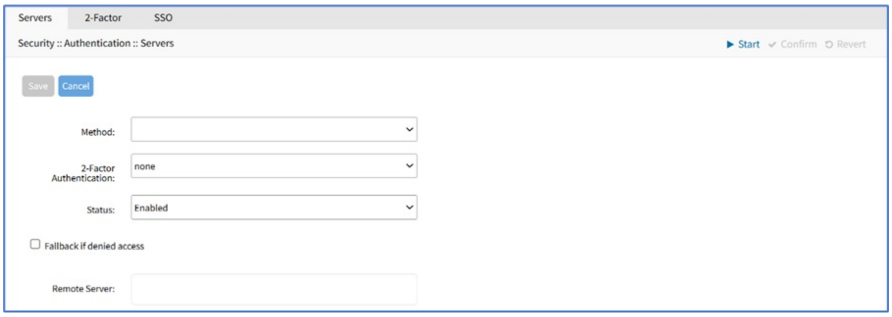
2-Factor Authentication: OTP

Status: Enabled

☐ Apply 2-Factor Authentication for Admin and Root users

Add Remote Server

1. Go to *Security :: Authentication :: Servers*.
2. Click **Add** (displays dialog):



Security :: Authentication :: Servers

Method:

2-Factor Authentication: none

Status: Enabled

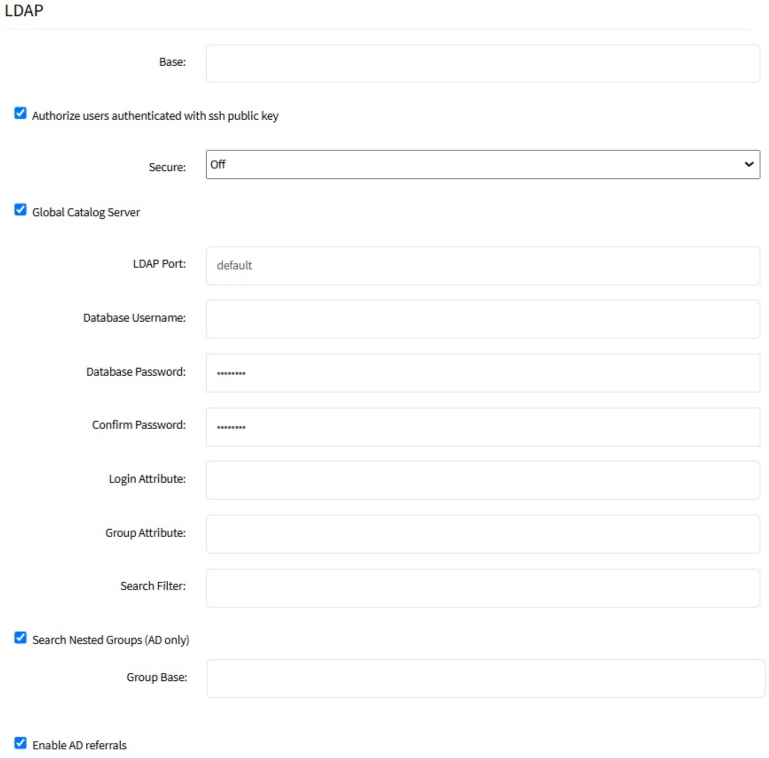
☐ Fallback if denied access

Remote Server:

3. On **Method** drop-down, select one of the following authentication methods:
   - LDAP or AD, see Method: LDAP or AD
   - RADIUS, see Method: RADIUS authentication and authorization - TACACS+, see Method: TACACS+
   - Kerberos, see Method: Kerberos
4. On **2 Factor Authentication** drop-down, select one (None, Enabled).
5. On **Status** drop-down, select one (Enabled, Disabled).
6. Select **Fallback if denied access** checkbox.
7. Enter **Remote Server** (IP address of remote server).
8. Click **Save**.

Method: LDAP or AD

1. Enter **Base** (root DN or a sublevel DN – highest point used to search for users or groups).



LDAP

Base:

☑ Authorize users authenticated with ssh public key

Secure: Off

☑ Global Catalog Server

LDAP Port: default

Database Username:

Database Password: ••••••••

Confirm Password: ••••••••

Login Attribute:

Group Attribute:

Search Filter:

☑ Search Nested Groups (AD only)

Group Base:

☑ Enable AD referrals

2. Select/unselect **Authorize users authenticated with ssh public key** checkbox (default: disabled).
3. On **Secure** drop-down, select one (On, Off, Start_TLS) (default: Off).
4. Select/unselect **Global Catalog Server** checkbox (if enabled, uses an Active Directory Global Catalog Server).
5. Enter **LDAP Port** (or accept "default").
6. Enter **Database Username**, **Database Password** and **Confirm Password.**
7. Enter **Login Attribute** (contains username - for AD, default: sAMAccountName).
8. Enter **Group Attribute** (group identifier - for AD, default: memberOf).
9. Enter **Search Filter.**
10. Select/unselect **Search Nested Groups (AD only)** checkbox (default: disabled).
11. Enter **Group Base**.

> **Example: OpenLDAP Configuration**
>
> Status: True; Fallback if denied access: True; Remote Server: 192.168.1.1; Base: dc=zpe, dc=net; Secure: Off; Global Catalog Server: False; Database Username: cn=admin, dc=zpe, dc=net; Login Attribute: cn; Group Attribute: Member, UID

> **Example: Active Directory Configuration**
>
> Status: True; Fallback if denied access: True; Remote Server: 192.168.1.1; Base: dc=zpesystems, dc=com; Secure: Start TLSl; Global Catalog Server: True; Database Username: cn=Administrator, cn=Users, dc=zpesystems, dc=com; Login Attribute: sAMAccountName; Group Attribute: memberOf

Method: RADIUS authentication and authorization

RADIUS (Remote Access Dial In User Service) provides central authentication for users.

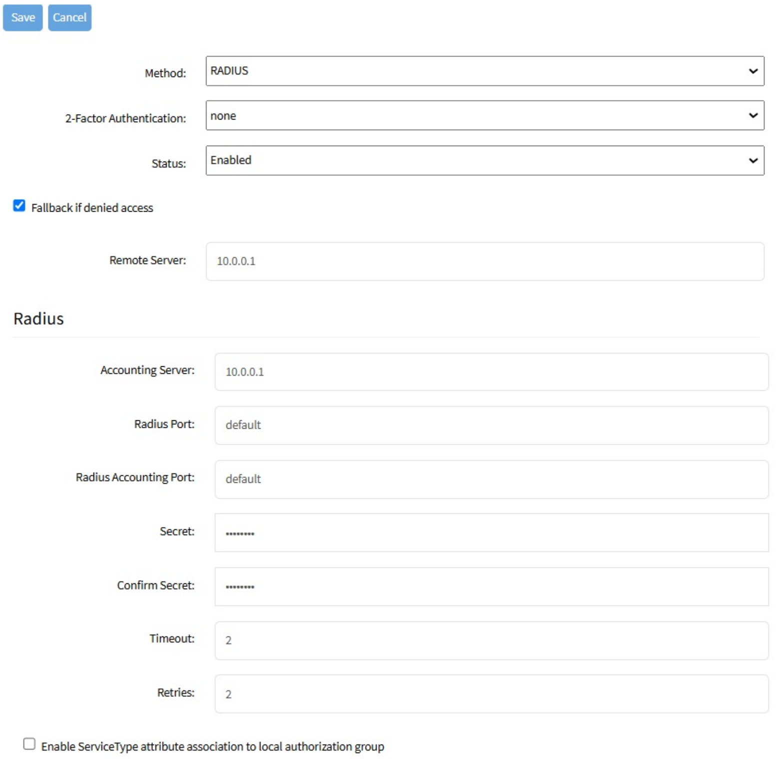
It is a client server protocol that runs on application layer. It can use either TCP or UDP as transport. Normally, all users have access to use all devices without restriction.

Configuration

Step 1 - On the Nodegrid side:

1. Login in as admin into Nodegrid and go to **Security**.
2. Select Authentication and click **Add**.

3. Select Radius as method and enter the IP address of remote server.



Method: RADIUS

2-Factor Authentication: none

Status: Enabled

☑ Fallback if denied access

Remote Server: 10.0.0.1

Radius

Accounting Server: 10.0.0.1

Radius Port: default

Radius Accounting Port: default

Secret: ••••••••

Confirm Secret: ••••••••

Timeout: 2

Retries: 2

☐ Enable ServiceType attribute association to local authorization group

4. Enter IP address of Radius accounting server.
5. Enter the secret key and confirm it.
6. Select Fallback if denied access option.
7. Click **Save**.

> **NOTE:**
>
> The "Fall-back if denied access" option enables you to log-in to the Nodegrid with local accounts in case you cannot authenticate with the Radius users.
> In the case there is no accounting server on the Radius side, it is recommended to leave the field 'Accounting Server' above empty (i.e. no IP address).

8. Go back to **Security** and select **Services**.
9. Look in to Manage devices portion and select **Device access enforced via user group authentication** option.
10. Click **Save**.

Log in as a user and one can see that user does not have access to any devices. To give access to a user:

1. Log in as admin and go to **Security**.
2. Select **Authorization** and select the group needed and click **Add**.
3. Enter the user one wants to add. If more users needs to be added then separate each username with a comma.
4. Click **Save**.

Log in back as user and one can see that user will have access to devices allowed by the group.

To match the Radius group, Go to *Security :: Authorization*, select or create a new group. In Profile, assign the permissions of that group. In Remote Groups, enter the name of group as per declared on the Radius server.

Step 2 - On the RADIUS server side

In this example, the free radius server (opensource) is used. It is assumed that the free radius server is installed.

1. Go to the location /etc/freeradius/3.0/clients.conf.
2. Declare the Nodegrid, following the format:

Plaintext Copy

```
client your_nodegrid_device {
    ipaddr = 10.10.10.6
    secret = your_secret_password
    require_message_authenticator = no
    nastype = other
}
```

> The secret must match the secret entered, during the first step, on the Nodegrid side.

3. Create the file "usr/share/freeradius/dictionnary.zpe" with the content listed below:
   VENDOR ZPE 42518
   BEGIN-VENDOR ZPE
   ATTRIBUTE ZPE-User-Groups 1 string
   END-VENDOR ZPE
4. Edit the file "usr/share/freeradius/dictionnary".
5. Add a line with the dictionary.zpe:
   $INCLUDE dictionary.zpe
6. Then, in /etc/freeradius/users, assign user groups.
7. Define the "Framed-Filter-ID" attribute (as before) or define a new attribute "ZPE-User-Groups".
   user_radius Cleartext-Password := "password_user_radius"

ZPE-User-Groups = "radius_network_admin"
Restart the radius server: systemctl restart freeradius

> NOTE: If both attributes are defined, "ZPE-User-Groups" takes precedence:

Troubleshooting

1. Make a local test, on the Radius server, with the command:

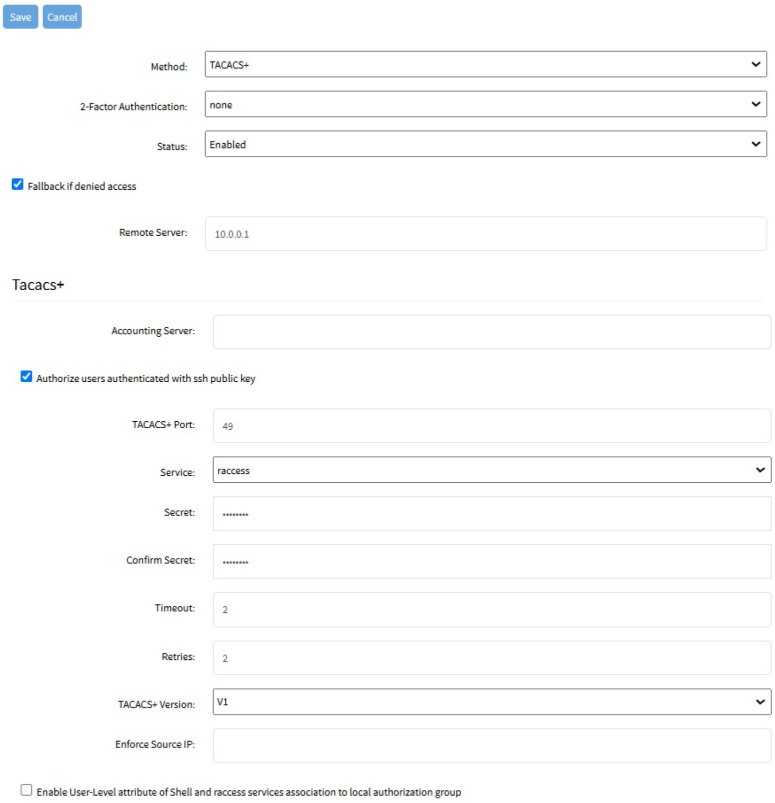
```
radtest user_radius password_user_radius localhost 0 your_secret_password
```

2. Log in to the Nodegrid, using the Radius user of the Radius group:

The permissions of that user shall match the ones of the local and associated group.

Method: TACACS+

1. Enter **Accounting Server**.



Method: TACACS+

2-Factor Authentication: none

Status: Enabled

☑ Fallback if denied access

Remote Server: 10.0.0.1

Tacacs+

Accounting Server:

☑ Authorize users authenticated with ssh public key

TACACS+ Port: 49

Service: raccess

Secret: ••••••••

Confirm Secret: ••••••••

Timeout: 2

Retries: 2

TACACS+ Version: V1

Enforce Source IP:

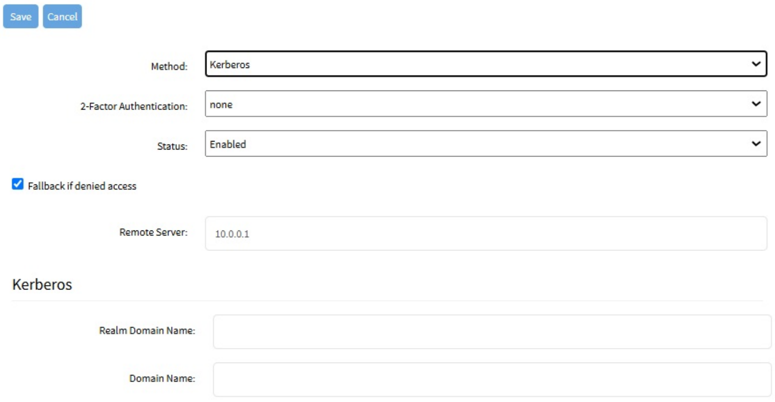
☐ Enable User-Level attribute of Shell and raccess services association to local authorization group

2. Select **Authorize users authenticated with ssh public key** checkbox.
3. Enter **TACACS+ Port** (default: 49).
4. On **Service** drop-down, select one (PPP, Shell, raccess) (default: raccess).
5. Enter **Secret** and **Confirm Secret.**
6. Enter **Timeout** (default: 2).
7. Enter **Retries** (default: 2).
8. On **TACACS+ Version** drop-down, select one (V0, V1, V0_V1, V1_V0) (default: V1).
9. Enter **Enforce Source IP** for AAA authentication (available in v5.8+).
10. Select **Enable User-Level attribute of Shell and raccess services association to local authorization group** checkbox (expands dialog with 15 User Levels). Per instruction, “Enter local authorization group name for each User Level.”

> **NOTE**
>
> User Level displays User Level 1 through User Level 15.

Method: Kerberos

1. Enter **Realm Domain Name**.



Method: Kerberos

2-Factor Authentication: none

Status: Enabled

☑ Fallback if denied access

Remote Server: 10.0.0.1

Kerberos

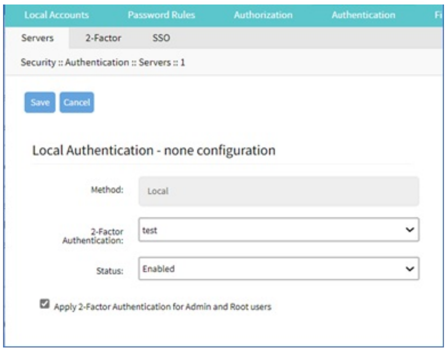
Realm Domain Name:

Domain Name:

2. Enter **Domain Name**.

Configure 2-Factor Authentication for Admin/Root Users

1. Go to *Security :: Authentication :: Servers*.
2. In *Index* column, click the index to be updated (displays dialog).



Security :: Authentication :: Servers :: 1

Local Authentication - none configuration

Method: Local

2-Factor Authentication: test

Status: Enabled

☑ Apply 2-Factor Authentication for Admin and Root users

3. Select **Apply 2-Factor Authentication for Admin and Root users** checkbox (if not selected, Admin and Root roles can use single logon).
4. Click **Save**.

Edit a Server

1. Go to *Security :: Authentication :: Servers*.
2. In *Index* column, click the index to be updated (displays dialog).
3. Make changes, as needed.
4. Click **Save**.

Delete a Server

1. Go to *Security :: Authentication :: Servers*.
2. Locate and select checkbox.
3. Click **Delete**.
4. On the confirmation dialog, click **OK**.

Move Index Priority Up

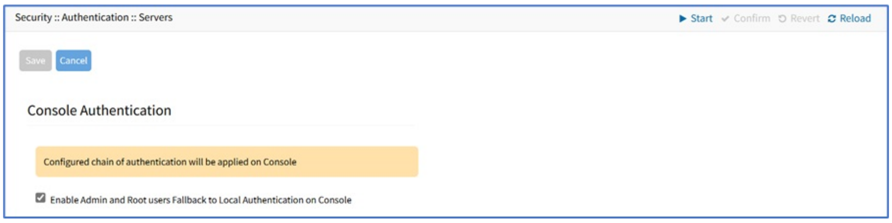
1. Go to *Security :: Authentication :: Servers*.
2. Locate and select checkbox.
3. Click **Up** to move the selection up in the table.
4. Click **Save**.

Move Index Priority Down

1. Go to *Security :: Authentication :: Servers*.
2. Locate and select checkbox.
3. Click **Down** to move the selection down in the table.
4. Click **Save**.

Enable/disable Console Authentication

1. Go to *Security :: Authentication :: Servers*.
2. Locate and select checkbox).
3. Click **Console** (displays dialog).



Console Authentication

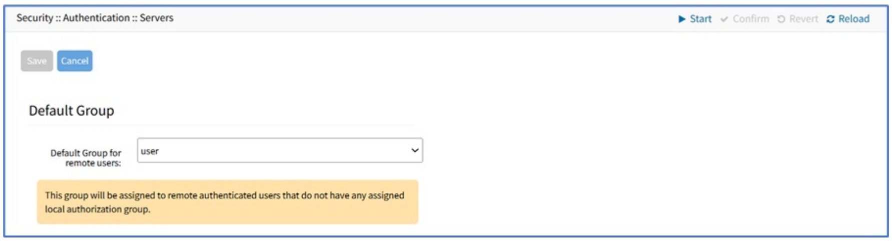
Configured chain of authentication will be applied on Console

☑ Enable Admin and Root users Fallback to Local Authentication on Console

4. Select **Enable Admin and Root users Fallback to Local Authentication on Console** checkbox.
5. Click **Save**.

Set Default Group

1. Go to *Security :: Authentication :: Servers*.
2. Locate and select checkbox.
3. Click **Default Group** (displays dialog).



Default Group

Default Group for remote users: user

This group will be assigned to remote authenticated users that do not have any assigned local authorization group.

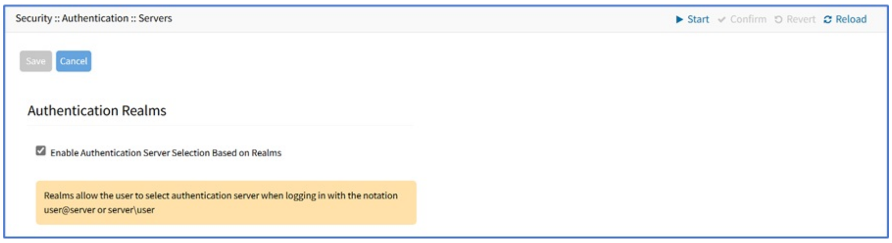
4. On **Default Group for Remote Server** drop-down, select one.
5. Click **Save**.

Set Realms

(available in v5.6+)

Realms allow the user to select authentication server when logging in with the notation user@server or server\user.

1. Go to *Security :: Authentication :: Servers*.
2. Locate and select checkbox.
3. Click **Realms** (displays dialog).



Authentication Realms

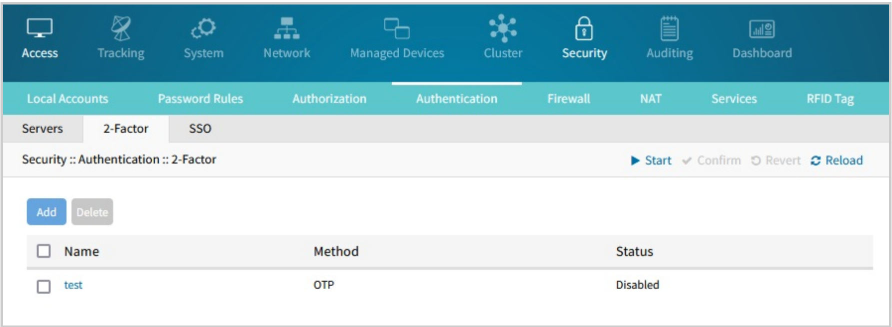
☑ Enable Authentication Server Selection Based on Realms

Realms allow the user to select authentication server when logging in with the notation user@server or server\user

4. Select **Enable Authentication Server Selection Based on Realms** checkbox.
5. Click **Save**.

2-Factor sub-tab

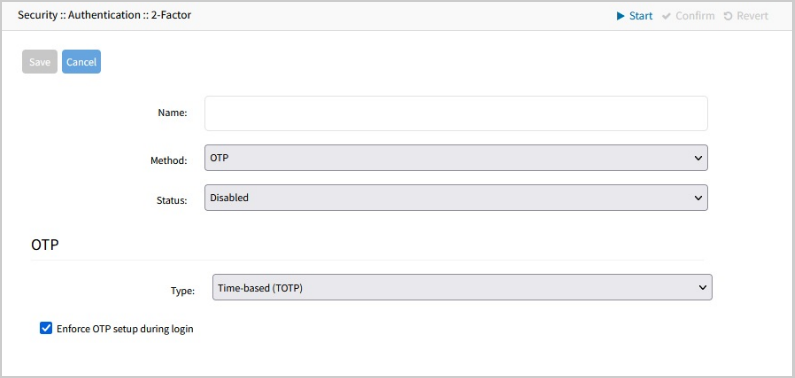
This sets up 2-factor authentication (2FA) with RSA or OTP methods. 2FA requires Nodegrid to pair with an external service that provides the corresponding method. The service is consulted at each login for users with 2FA enabled.



Name	Method	Status
test	OTP	Disabled

Add 2-Factor Configuration

1. Go to *Security :: Authentication :: 2-Factor*.
2. Click **Add** (displays dialog):



Name:

Method: OTP

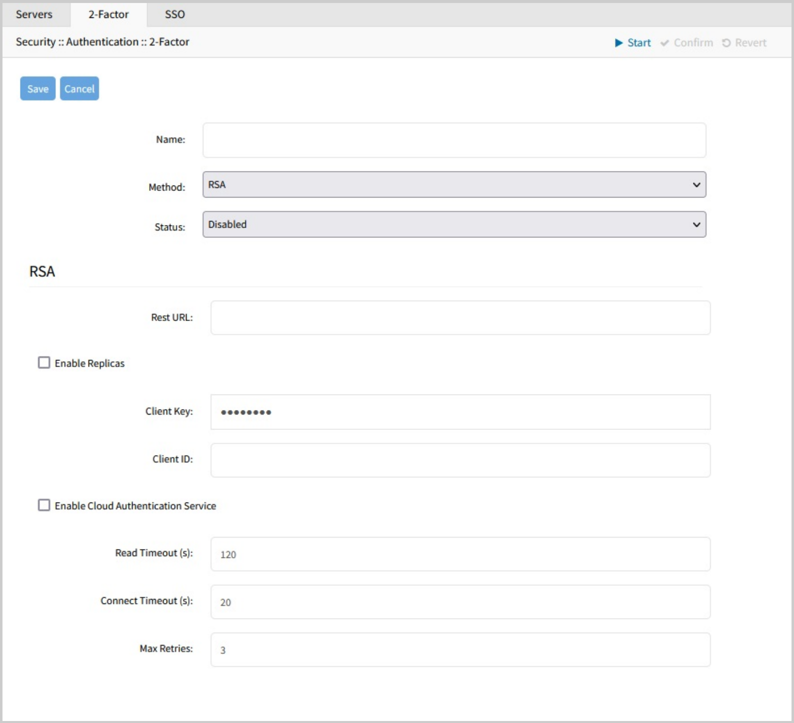
Status: Disabled

OTP

Type: Time-based (TOTP)

☑ Enforce OTP setup during login

3. Enter **Name** as an arbitrary identifier.
4. On **Method** drop-down, select one (OTP, RSA). Dialog changes.
5. On **Status** drop-down, select one (Enabled, Disabled). The authentication method will only apply when Enabled.
6. If configuring the *OTP* method (see additional steps in the "Configure OTP for a user" section below):
    a. OTP (One-Time Password) 2FA works by setting up an initial pairing between a Nodegrid user and an external service supporting the chosen *Type* (such as Google Authenticator, Microsoft Authenticator, Free OTP, etc.). After the initial pairing, upon each login, the user with OPT configured will be required to enter their password as well as a code provided by the external authenticator service.
    b. Select a **Type** depending on the external authenticator service selected:
        i. Time-based (TOTP): the provided code is time-sensitive, changing periodically
        ii. Counter-based (HOTP): the provided code changes at every use, and only when used
    c. Choose whether or not to *Enforce OTP setup during login.* If selected, all users will be prompted and forced to setup OTP on their next login. If not selected, users can choose to setup OTP on the "Change Password" screen.
7. If configuring the *RSA* method (see additional steps in "Configure RSA SecurID (2-Factor)" section below):



Security :: Authentication :: 2-Factor

Name:

Method: RSA

Status: Disabled

RSA

Rest URL:

□ Enable Replicas

Client Key: ••••••••

Client ID:

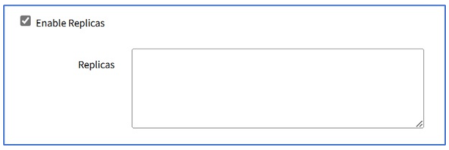
□ Enable Cloud Authentication Service

Read Timeout (s): 120

Connect Timeout (s): 20

Max Retries: 3

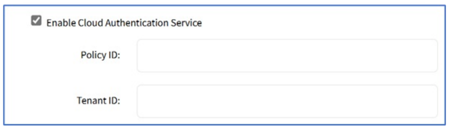
   a. Enter **Rest URL.**
   b. Select **Enable Replicas** checkbox (expands dialog). Enter **Replicas**.



☑ Enable Replicas

Replicas

8. Enter **Client Key.**
9. Enter **Client ID.**
10. Select **Enable Cloud Authentication Service** checkbox (expands dialog).



☑ Enable Cloud Authentication Service

Policy ID:

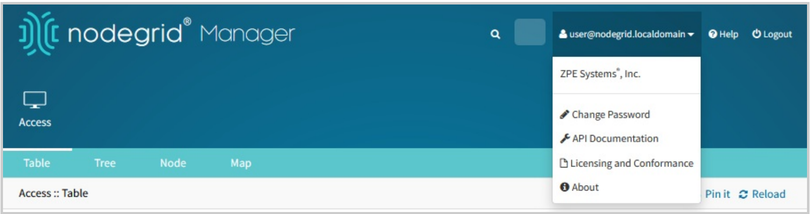
Tenant ID:

   a. Enter **Policy ID.**
   b. Enter **Tenant ID.**

11. Enter **Read Timeout [seconds]** (default: 120).
12. Enter **Connect Timeout [seconds]** (default: 20).
13. Enter **Max Retries** (default: 3).
14. Click **Save**.

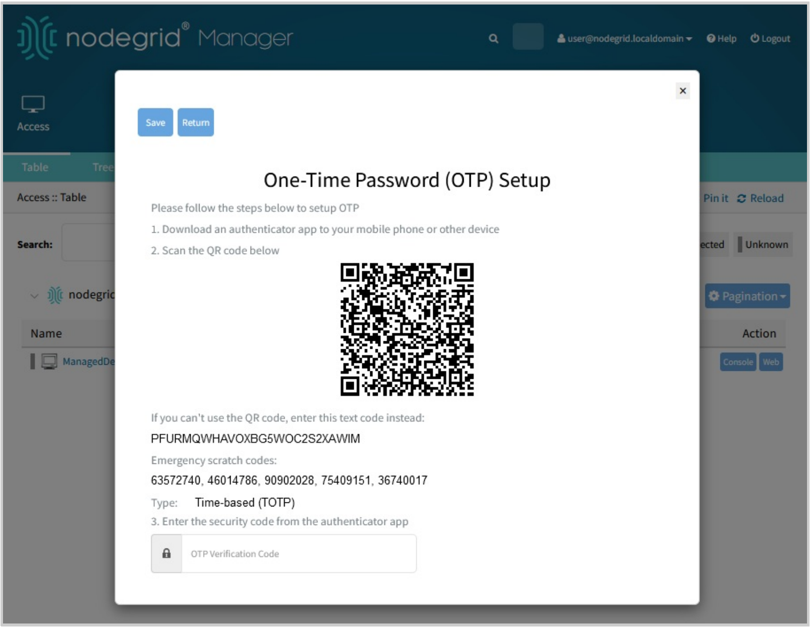
Configure OTP authentication for a user

1. Add and enable an OTP authentication provider (see "Add 2-Factor Configuration" above for the OTP method)
2. Go to *Security :: Authentication :: Servers* and set the 2-Factor Authentication option of the local server to the configured OTP provider (see *Authentication tab / Servers sub-tab, Edit Local Authentication*)
3. Login as the user that will configure 2FA
4. Click on *user@nodegrid.localdomain* at the top banner, and select *Change Password:*



5. Click on *Generate OTP Token*
   a. Note: if clicking on *Reset OTP Token*, the current configuration will be erased and a new one will **not** be set. Useful for enforcing a new setup at next login.

6. Follow the instructions on the dialog (shown below)
   a. If OTP is enforced at login, this dialog will also be shown when the user tries to login
   b. If desired, note down the "Emergency scratch codes". These can be used instead of an OTP, but only once per code



One-Time Password (OTP) Setup

Please follow the steps below to setup OTP

1. Download an authenticator app to your mobile phone or other device

2. Scan the QR code below

If you can't use the QR code, enter this text code instead:

PFURMQWHAVOXBG5WOC2S2XAWIM

Emergency scratch codes:

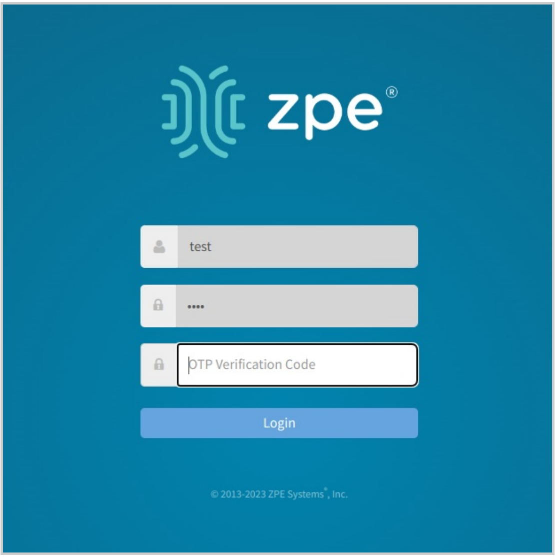
63572740, 46014786, 90902028, 75409151, 36740017

Type: Time-based (TOTP)

3. Enter the security code from the authenticator app

OTP Verification Code

7. Upon each new login, after correctly entering their password, the user will be prompted for an OTP verification code:



The same applies to CLI:

Shell

✏🗑

Bash Copy

```bash
$ ssh test@nodegrid
(test@nodegrid) Password:
(test@nodegrid) Verification code:
```

And API:

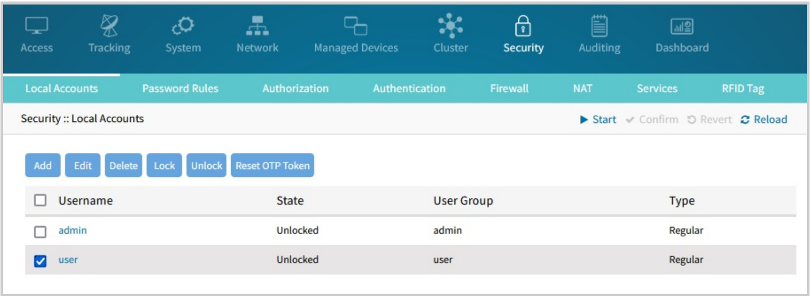
Python

✏🗑

Python Copy

```python
url = f'https://{NG_IP}/api/v1/Session'
headers = {"Content-Type": "application/json", "accept": "application/json"}
data = f'{{ "username": "{USERNAME}", "password": "{PASSWD}", "verification_code": "824584" }}'

requests.post(url, data=data, headers=headers, verify=False)
```

8. (Optional) System administrators can reset any user's OTP tokens using the *Reset OTP Token* button in *Security :: Local Accounts*:



	Username	State	User Group	Type
□	admin	Unlocked	admin	Regular
☑	user	Unlocked	user	Regular

Configure RSA SecurID (2-Factor)

Step 1 – Add SecurID (WebUI Procedure)

1. Go to *Security :: Authentication :: 2-Factor*.
2. Click **Add**.
3. On the *Add* dialog, enter **Name** (name to identify the SecurID system, i.e., SecurID)
4. Enter **Rest URL** (URL to access the SecurID Authentication API – format: https://5555/mfa/v1_1/authn).
5. Enter **Enable Replicas**(Rest Service URL to failover to the server (up to 15 replicas). One per line).
    a. Enter **Client Key** (available through RSA Security Console. Copy/paste the **Access Key** from the *SecurID Security Console*. The Access Key is also available at RSA SecurID Authentication API (under System Settings).
    b. Enter **Client ID** (retrieve the Server Node name from the *Authentication Manager Contact List*.).
6. Select the **Enable Cloud Authentication Service** checkbox:
    a. Enter **Policy ID**: Enter the name of the access policy you want to authenticate with as specified in the RSA Cloud Administration Console.
    b. Enter **Tenant ID:** Enter the RSA Cloud Authentication Service Company ID.
7. Click **Save**.

Step 2 – Set Certificate to access SecurID Server (WebUI Procedure)

1. If the RSA server is through ZPE Cloud Authentication, go to RSA SecurID Access and click the **Lock** icon (next to the URL).
    a. Locate and click on the Certificate.
    b. Click the first/top certificate on the pop-up dialog, and drag it to your desktop.
    c. Upload certificate to Nodegrid (certificate is automatically converted to the expected format).
2. If not via ZPE Cloud:
    a. Go to the *RSA Operations Console.*
    b. Download the Signing Root Certificate.
    c. Go to *Security :: Authentication :: 2-Factor*.
    d. Click the link representing the SecurID server (added above).
    e. Click **Certificate**.
    f. Select **Local Computer** checkbox. Click **Choose File** and select the file (i.e. RootCA.cer file).
    g. Click **Apply**,
3. Click **Save**.

Edit 2-Factor Configuration

1. Go to *Security :: Authentication :: 2-Factor*.
2. In the *Name* column, click the name to be updated (displays dialog).
3. Make changes, as needed.
4. Click **Save**.

Delete 2-Factor Configuration

1. Go to *Security :: Authentication :: 2-Factor*.
2. Locate and select the checkbox.
3. Click **Delete**.
4. On the confirmation dialog, click **OK**.

Assign 2-factor to an Authentication Method

RSA SecurID 2-factor authentication can be added to any Nodegrid-supported authentication method: Local, LDAP/AD, Radius, TACACS+, or Kerberos.

Nodegrid authenticates users following the order of the authentication servers, as configured. When a method succeeds (user authenticated), Nodegrid initiates the 2-factor authentication (if configured).

The user receives a request from RSA SecurID to provide the token code and PIN (according to the setup on the user's RSA Security Console). The process is applied on user login via Web Browser, SSH, Telnet or Console port.

> NOTE
>
> For the Local authentication method, 2-factor can be enforced or skipped. This allows local administrators to login without needing to configure counterpart users in the RSA Security Console.

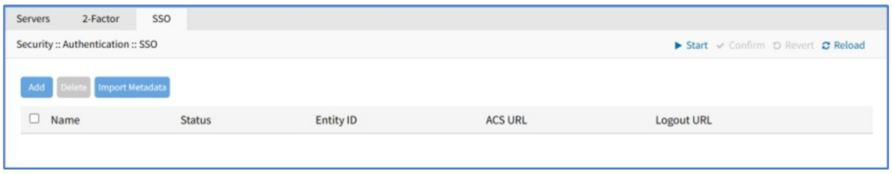
RSA Authenticate App

This applies only to ZPE Cloud Authentication Services.

1. Download the *RSA SecurID Authenticate* app.
2. Go to **RSA SecurID Access** and login.
3. Follow the steps to register the device.

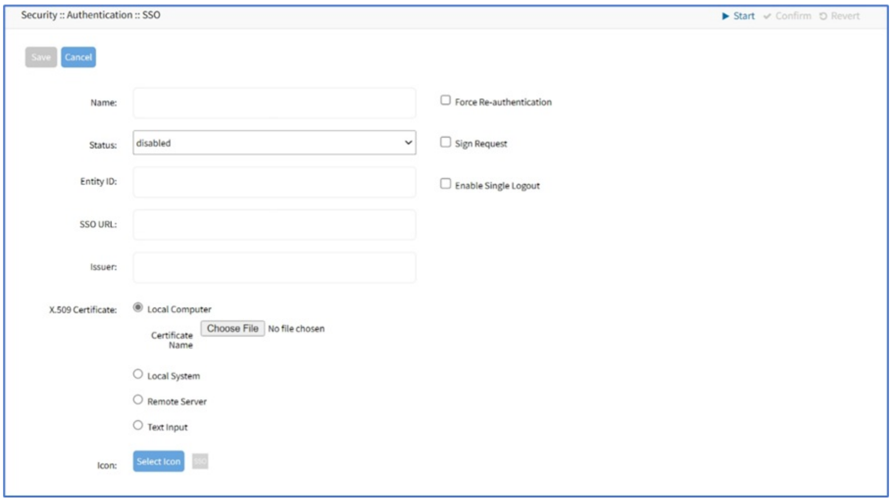
SSO sub-tab

With Single Sign-On (SSO), users authenticate once to gain access to multiple secured systems without resubmitting credentials. Nodegrid currently supports multiple identify providers.

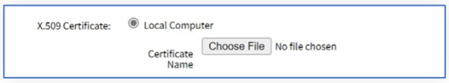


Add SSO

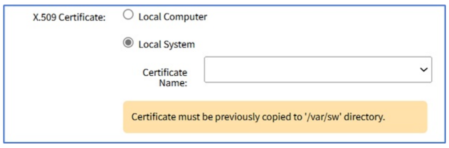
1. Go to *Security :: Authentication :: SSO*.
2. Click **Add** (displays dialog).



3. Enter **Name.**
4. On **Status** drop-down, select one (Enabled, Disabled).
5. Enter **Entity ID** (globally unique name).
6. Enter **SSO URL.**
7. Enter **Issuer.**
8. On *X-509 Certificate* menu, select one:
   - **Local Computer** radio button (expands dialog). Click **Choose File** to locate and select file.

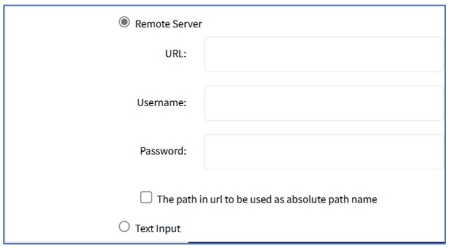


   - **Local System** radio button (expands dialog). On **Certificate Name** drop-down, select one.



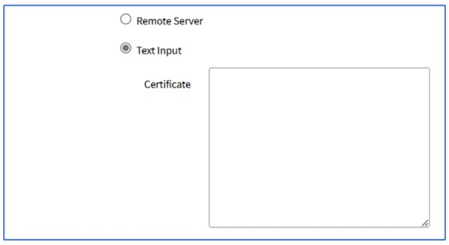
Certificate must be previously copied to '/var/sw' directory.

   - **Remote Server** radio button (expands dialog).



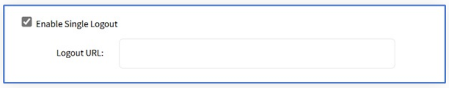
     - Enter **URL** (URL can be the IP address or hostname/FQDN. If using IPv6, use brackets [...]. Supported protocols: FTP, TFTP, SFTP, and SCP.).
     - Enter **Username** and **Password.**
     - (optional) Select **The path in url to be used as absolute path name** checkbox.

   - **Text Input** radio button (expands dialog). Enter in **Certificate** text box.



9. Select **Force Re-authentication** checkbox.

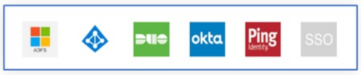
10. Select **Sign Request** checkbox.
11. Select **Enable Single Logout** checkbox (expands dialog). Enter **Logout URL**.



☑ Enable Single Logout

Logout URL:

12. (optional) **Icon**, click **Select Icon** (expands dialog). Click on a logo to set as 2-Factor icon.



13. Click **Save**.

The following fields are required to configure a successful SAML flow for each Identity Provider:

SAML Requirements

Identity Provider (IDP)	Copy Fields from Nodegrid to IdP	Paste Fields from IDP to Nodegrid
Duo	Login URL Entity ID	SSO URL Entity ID Download Certificate
Okta	Single Sign On URL Audience URI (SP Entity ID)	Identity Provider SSO URL Identity Provider Issuer X.509 Certificate
G Suite	ACS URL Entity ID	SSO URL Entity ID Certificate
Ping	Entity ID ACS URL	Issuer Idpid The idpid from Ping is used as the SSO URL field in Nodegrid: https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid= + the idpid
ADFS	Entity ID (maps to Relying party trust identifier) ACS URL (maps to Trusted URL)	Entity ID (maps to Issuer on Nodegrid)

IdP configuration fields:

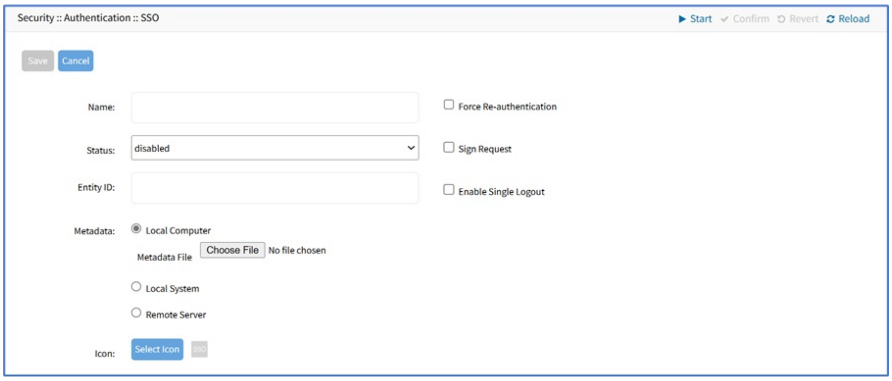
- *Entity ID* (globally unique name for the SP URL)
- *ACS URL* (Assertion Consumer Service URL in which the Identity Provider redirects the user and sends the SAML assertion after its authentication process.)
- *Attributes* (attributes that IdP sends back with the SAML assertion. SP can have more than one attribute, nameID is the most common.)
- *SAML Signature Algorithm* (either SHA-1 or SHA-256. Used with X.509 certificate. Default: SHA-256.)

SP configuration fields:

- *X.509 Certificate* (certificate provided by the IdP to allow the SP to verify that the SAML assertion is from the IdP)
- *Issuer URL/Entity ID* (unique identifier of the IdP)
- *Single Sign On URL* (IdP endpoint that starts the authentication process)
- *RelayState:* (optional) (deep linking for SAML for <ip>/direct/<device>/console)
- For more information on SSO, please see https://support.zpesystems.com/portal/kb/articles/single-sign-on-sso

Import Metadata

1. Go to *Security :: Authentication :: SSO*.
2. Click **Import Metadata** (displays dialog).



Security :: Authentication :: SSO

Name:

Status: disabled

Entity ID:

☐ Force Re-authentication

☐ Sign Request

☐ Enable Single Logout

Metadata: ● Local Computer

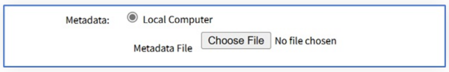
Metadata File Choose File No file chosen

○ Local System

○ Remote Server

Icon: Select Icon

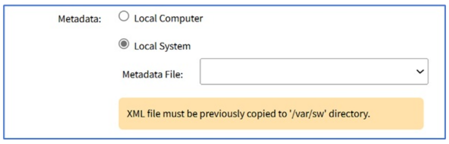
3. Enter **Name.**
4. On **Status** drop-down, select one (Enabled, Disabled).
5. Enter **Entity ID** (globally unique name).
6. On *Metadata* menu, select one:
   - **Local Computer** radio button (expands dialog). Click **Choose File**, locate and select.



Metadata: ● Local Computer

Metadata File Choose File No file chosen

   - **Local System** radio button (expands dialog). On **Metadata File** drop-down, select one.



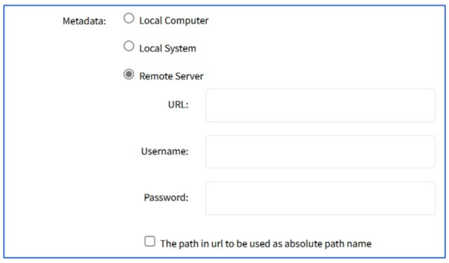
Metadata: ○ Local Computer

● Local System

Metadata File:

XML file must be previously copied to '/var/sw' directory.

- **Remote Server** radio button (expands dialog):

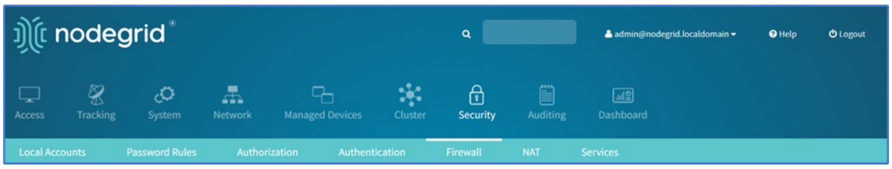
  Metadata: ○ Local Computer
  ○ Local System
  ● Remote Server
  URL:
  Username:
  Password:
  □ The path in url to be used as absolute path name

  - Enter **URL** (URL can be the IP address or hostname/FQDN. If using IPv6, use brackets [...]. Supported protocols: FTP, TFTP, SFTP, and SCP.)
  - Enter **Username** and **Password.**
  - (optional) Select **The path in url to be used as absolute path name** checkbox.

7. (optional) **Icon**, click **Select Icon**. Click on a logo to set as 2-Factor icon.
8. Select **Force Re-authentication** checkbox.
9. Select **Sign Request** checkbox.
10. Select **Enable Single Logout** checkbox.
11. Click **Save**.

Firewall tab

When configured, the Nodegrid device functions as a Firewall. There are six built-in default chains (three for IPv4, three for IPv6). These accept packets (Output, Input, and Forward). As needed, additional user chains can be created. (Default chains cannot be deleted.)



The Nodegrid platform comes with its own firewall which is based on iptables. The WebUI and the CLI provide an easy way of creating and managing the firewall. By default, the firewall accepts all incoming traffic. Specifically, if the Nodegrid is exposed to an internet connection either directly or indirectly is it recommended to secure the Nodegrid with a valid firewall configuration.

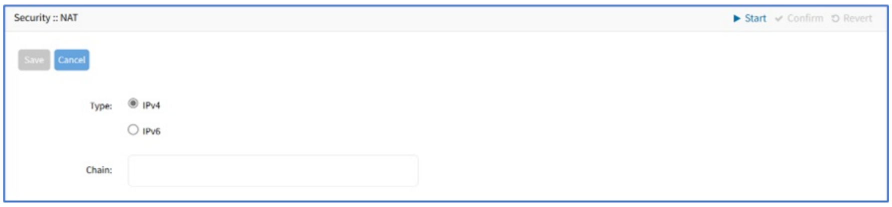
Manage Chains

The Firewall table displays all the firewall rules configured for different interfaces.

> Note: If you import a configuration for a chain through CLI, the rules defined for the specified chain(s) will be overridden by the imported configuration. For example, if you are importing configuration For the INPUT and OUTPUT chains, the FORWARD chain will not be changed, only the INPUT and OUTPUT chains are updated.

Add a Chain

1. Go to *Security :: Firewall*.
2. Click **Add** (displays dialog).



Security :: NAT

Type: ● IPv4 ○ IPv6

Chain:

3. On *Type* menu, select one:
   - **IPv4** radio button
   - **IPv6** radio button
4. Enter **Chain** (name of this chain).
5. Click **Save**.

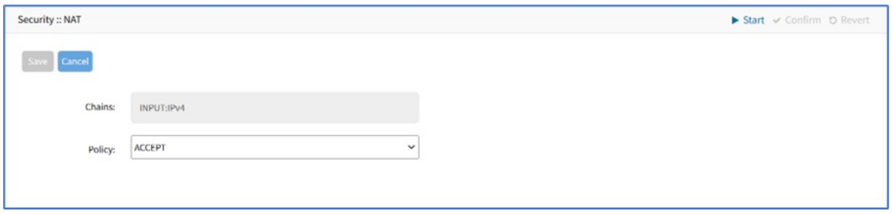
Delete a Chain

1. Go to *Security :: Firewall*.
2. Select the checkbox next to the name to be deleted.
3. Click **Delete**.
4. On the confirmation dialog, click **OK**.

Change Chain Policy

> NOTE
>
> The policy cannot be changed for user custom chains. The policy can only be changed for default chains.

1. Go to *Security :: Firewall*.
2. In the *Chain* column, select the checkbox of Chain.
3. Click **Change Policy** (displays dialog). On **Policy** drop-down, select one (ACCEPT, DROP).



Security :: NAT

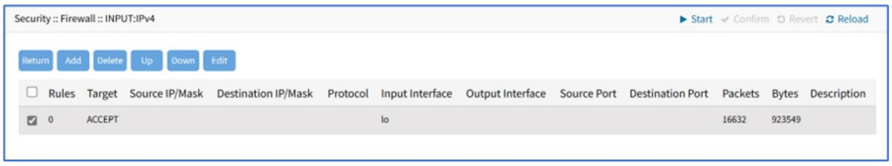
Chains: INPUT:IPv4

Policy: ACCEPT

4. Click **Save**.

Manage a Chain

To manage chain functions/settings, click on the name in the *Chain* column (displays dialog).

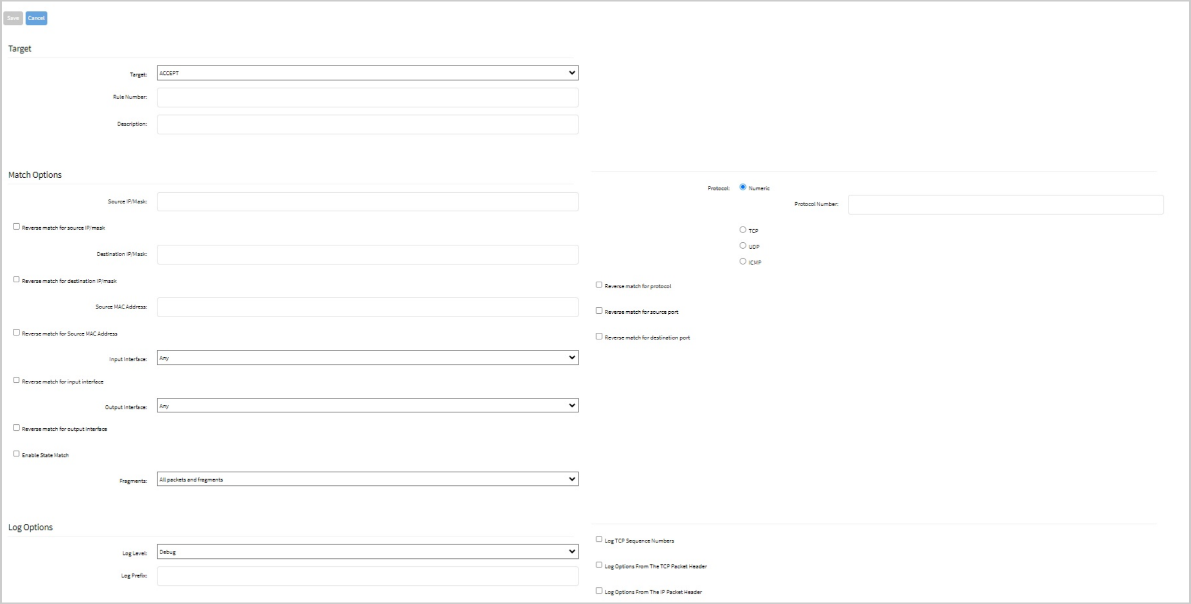


Security :: Firewall :: INPUT:IPv4

□	Rules	Target	Source IP/Mask	Destination IP/Mask	Protocol	Input Interface	Output Interface	Source Port	Destination Port	Packets	Bytes	Description
☑	0	ACCEPT				lo				16632	923549	

Add Rule

1. Go to *Security :: Firewall*.
2. In the *Chain* column, locate and click on the name (displays dialog).
3. Click **Add** (displays dialog).



Target

Target: ACCEPT

Rule Number:

Description:

Match Options

Source IP/Mask:

□ Reverse match for source IP/mask

Destination IP/Mask:

□ Reverse match for destination IP/mask

Source MAC Address:

□ Reverse match for Source MAC Address

Input Interface: Any

□ Reverse match for input interface

Output Interface: Any

□ Reverse match for output interface

□ Enable State Match

Fragments: All packets and fragments

Protocol: ● Numeric

Protocol Number:

○ TCP

○ UDP

○ ICMP

□ Reverse match for protocol

□ Reverse match for source port

□ Reverse match for destination port

Log Options

Log Level: Debug

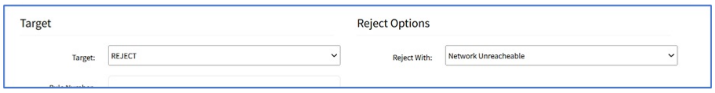
Log Prefix:

□ Log TCP Sequence Numbers

□ Log Options From The TCP Packet Header

□ Log Options From The IP Packet Header

4. On the *Target* menu, on the **Target** drop-down, select one (ACCEPT, DROP, REJECT, LOG, RETURN). Enter the **Rule Number** and **Description.**
   - If **REJECT** is selected, the *Reject Options* menu displays:



Target

Target: REJECT

Reject Options

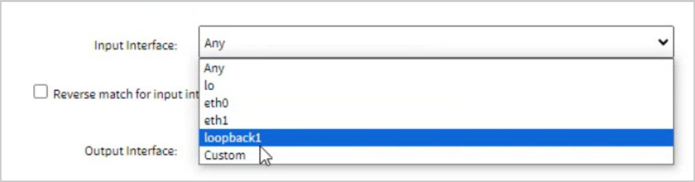
Reject With: Network Unreachable

   - On **Reject With** drop-down, select one (Network Unreachable, Host Unreachable, Port Unreachable, Protocol Unreachable, Network Prohibited, Host Prohibited, Administratively Prohibited, TCP Reset).

5. On the *Match Options* menu:
   a. Enter **Source IP/Mask**
   b. Select **Reverse match for source IP/mask** checkbox
      i. Enter **Destination IP/Mask**
   c. Select **Reverse match for destination IP/mask** checkbox
   d. Enter **Source MAC Address**
   e. Select **Reverse match for source MAC address** checkbox

Note: The Source MAC Address and Reverse Match for the source MAC Address fields are applicable only for Input, PREROUTING, and FORWARD chains.

   f. From the **Input Interface** drop-down list, select one. The list contains all the available interfaces such as eth0, eth1, loopback1, custom, etc.



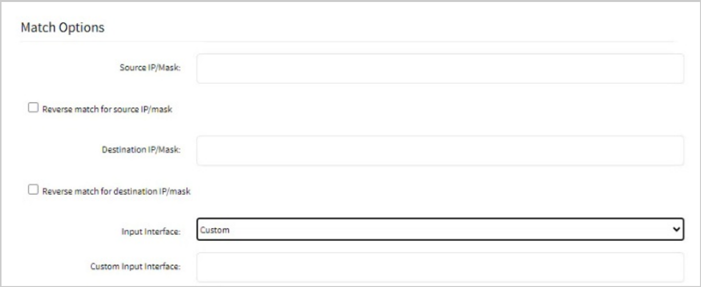
Input Interface: Any

□ Reverse match for input int

Output Interface:

Note: The Source MAC Address and Reverse Match for the source MAC Address fields are applicable only for Input, PREROUTING, and FORWARD chains.

      i. If you want to add an interface that is not listed, select **Custom**. You can create any custom interface.
      ii. In the **Custom Input Interface** field, specify the name of the interface.



Match Options

Source IP/Mask:

□ Reverse match for source IP/mask

Destination IP/Mask:

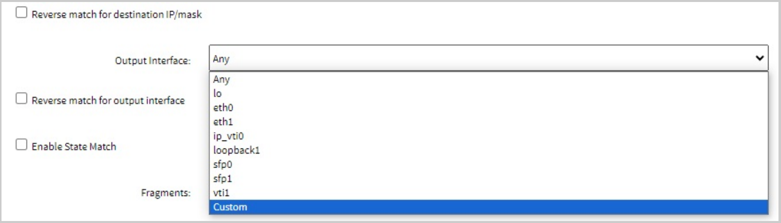
□ Reverse match for destination IP/mask

Input Interface: Custom

Custom Input Interface:

The user can later go to **Network**::**Connections** and click **Add**, to add the **Custom Input Interface** mentioned under the **Custom Input Interface**

   g. Select **Reverse match for the input interface** checkbox
   h. On the **Output Interface** drop-down, select the required interface. If an interface is not listed or does not exist, you can use the **Custom** option from the drop-down list to specify the name of the interface:



☐ Reverse match for destination IP/mask

Output Interface: Any

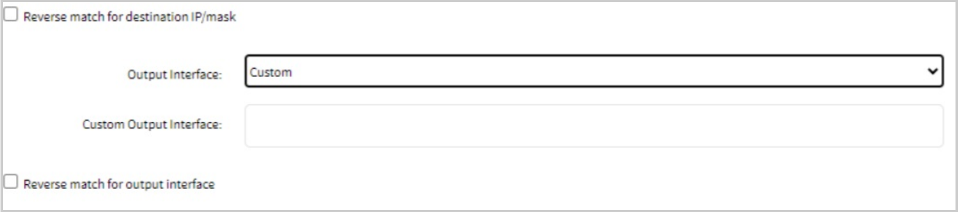
☐ Reverse match for output interface

☐ Enable State Match

Fragments:

Note: The Source MAC Address and Reverse Match for the source MAC Address fields are applicable only for Output, POSTROUTING, and FORWARD chains.

i. In the **Custom Output Interface** field, specify the name of the interface.



☐ Reverse match for destination IP/mask

Output Interface: Custom

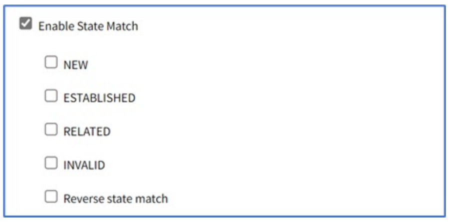
Custom Output Interface:

☐ Reverse match for output interface

The user can later go to **Network::Connections** and click **Add**, to add the Interface mentioned under the **Custom Output Interface**.

j. Select **Reverse match for the output interface** checkbox

k. Select **Enable State Match** checkbox (displays options – one or more can be selected):



☑ Enable State Match

☐ NEW

☐ ESTABLISHED

☐ RELATED

☐ INVALID

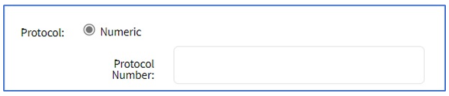
☐ Reverse state match

- **NEW** checkbox
- **ESTABLISHED** checkbox
- **RELATED** checkbox
- **INVALID** checkbox
- **Reverse state match** checkbox

l. On **Fragments** drop-down, select one (All packets and fragments, Unfragmented packets and 1st packets, 2nd and further packets)

6. On the *Protocol* menu, select one:

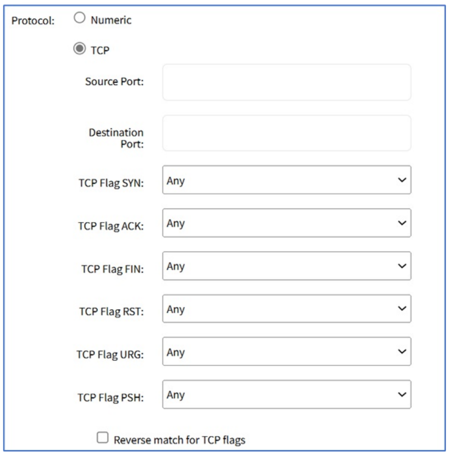
a. **Numeric** radio button (expands dialog). Enter the **Protocol Number**.



Protocol: ● Numeric

Protocol Number:

b. **TCP** radio button (expands dialog).



Protocol: ○ Numeric

● TCP

Source Port:

Destination Port:

TCP Flag SYN: Any

TCP Flag ACK: Any

TCP Flag FIN: Any

TCP Flag RST: Any

TCP Flag URG: Any

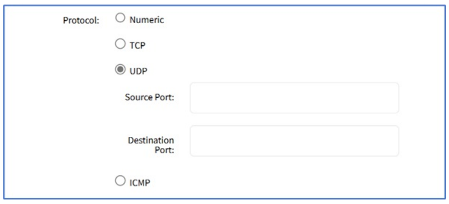
TCP Flag PSH: Any

☐ Reverse match for TCP flags

- Enter **Source Port.**
- Enter **Destination Port.**
- **TCP Flag SYN** drop-down, select one (Any, Set, Unset)
- **TCP Flag ACK** drop-down, select one (Any, Set, Unset)

        - **TCP Flag FIN** drop-down, select one (Any, Set, Unset)
        - **TCP Flag RST** drop-down, select one (Any, Set, Unset)
        - **TCP Flag URG** drop-down, select one (Any, Set, Unset)
        - **TCP Flag PSH** drop-down, select one (Any, Set, Unset)
        - **Reverse Match for TCP Flags** checkbox

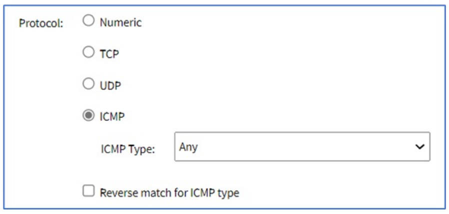
    c. **UDP** radio button (expands dialog)



Protocol:
○ Numeric
○ TCP
● UDP
Source Port:
Destination Port:
○ ICMP

        - Enter **Source Port**
        - Enter **Destination Port**

    d. **ICMP** radio button (expands dialog)



Protocol:
○ Numeric
○ TCP
○ UDP
● ICMP
ICMP Type: Any
□ Reverse match for ICMP type

        - On **ICMP Type** drop-down, select one (Any, Echo-Reply, Destination Unreachable, Network Unreachable, Host Unreachable, Protocol Unreachable, Port Unreachable, Fragmentation Needed, Source Route Failed, Network Unknown, Host Unknown, Network Prohibited, Host Prohibited, TOS Network Unreachable, TOS Host Unreachable, Communication Prohibited, Host Precedence Violation, Precedence Cutoff, Source Quench, Redirect, Network Redirect, Host Redirect, TOS Network Redirect, TOS Host Redirect, Echo Request, Router Advertisement, Router Solicitation, Time Exceeded, TTL Zero During Transit, TTL Zero During Reassembly, Parameter Problem, Bad IP Header, Required Option Missing, Timestamp Request, Timestamp Reply, Address Mask Request, Address Mask Reply)
        - Select **Reverse match for ICMP type** checkbox
        - Select **Reverse match for the protocol** checkbox
        - Select **Reverse match for source port** checkbox
        - Select **Reverse match for destination port** checkbox

7. From the *Log Options* menu:
    a. From the **Log Level** drop-down list, select one (Debug, Info, Notice, Warning, Error, Critical, Alert, Emergency)
    b. Enter **Log Prefix**
    c. Select the **Log TCP Sequence Numbers** checkbox
    d. Select the **Log Options from the TCP Packet Header** checkbox
    e. Select the **Log Options from the IP Packet Header** checkbox

8. Click **Save**.

Edit Chain

1. Go to *Security :: Firewall*.
2. In the *Chain* column, locate and click on the checkbox.
3. Click **Edit** (displays dialog).
4. Make changes, as needed.
5. Click **Save**.

Delete Chain

1. Go to *Security :: Firewall*.
2. In the *Chain* column, locate and select the checkbox on the name.
3. Click **Delete**.
4. On the confirmation dialog, click **OK**.

Move Chain Up

1. Go to *Security :: Firewall*.
2. In the *Chain* column, locate and select the checkbox on the name.
3. Click **Up** to move up.

Move Chain Down

1. Go to *Security :: Firewall*.
2. In the *Chain* column, locate and select the checkbox on the name.
3. Click **Down** to move down.

How to Configure a new Firewall rule

The WebUI and CLI provide a simple interface to create, edit and remove firewall rules. All changes made through either interface will be effective immediately. It is therefore important that before the default policies are set to DROP that the required ACCEPT rules have been configured.

All defined rules will persist through a reboot. In case that a rule prevents access to the node, the rules can be adjusted through the local console port of the node.

The following rules must always be applied to a Nodegrid as they are required for a normal operation:

Source	Direction	Comments
loopback	INBOUND	IPv4
loopback	OUTBOUND	IPv4
loopback	INBOUND	IPv6
loopback	OUTBOUND	IPv6

A list of commonly used Firewall Rules on a Nodegrid can be found in Firewall Rules for the Nodegrid platform.

Create a new Rule

Create a new Rule through CLI

1. Log in to the Nodegrid device CLI using admin account.
2. Navigate to the desired firewall chain. By default, the following 6 Chains are available:

IPv4 INPUT

Plaintext Copy

```
[admin@nodegrid /]# cd /settings/ipv4_firewall/chains/INPUT/
```

IPv4 FORWARD

Plaintext Copy

```
[admin@nodegrid /]# cd /settings/ipv4_firewall/chains/FORWARD/
```

IPv4 OUTPUT

Plaintext Copy

```
[admin@nodegrid /]# cd /settings/ipv4_firewall/chains/OUTPUT/
```

IPv6 INPUT

Plaintext Copy

```
[admin@nodegrid /]# cd /settings/ipv6_firewall/chains/INPUT/
```

IPv6 FORWARD

Plaintext Copy

```
[admin@nodegrid /]# cd /settings/ipv6_firewall/chains/FORWARD/
```

IPv6 OUTPUT

Plaintext Copy

```
[admin@nodegrid /]# cd /settings/ipv6_firewall/chains/OUTPUT/
```

Type **add** to create a new rule

Plaintext Copy

```
[admin@nodegrid INPUT]# add
```

Use the **set** command to create the new rule settings. Press **TAB twice** to see all available options

Plaintext Copy

```
[admin@nodegrid {INPUT}]# set target=ACCEPT source_net4=192.168.1.1
```

Use the **save** command to create and activate the new rule

Plaintext Copy

```
[admin@nodegrid {INPUT}]# save
```

Use the **show** command to see the current values for the rule:

Plaintext Copy

```
[admin@nodegrid 2]# show
target = ACCEPT
source_net4 = 192.168.1.1
destination_net4 =
protocol = tcp
source_port =
destination_port = 443
tcp_flag_syn = any
tcp_flag_ack = any
tcp_flag_fin = any
tcp_flag_rst = any
tcp_flag_urg = any
tcp_flag_psh = any
input_interface = any
output_interface = any
fragments = all_packets_and_fragments
reverse_match_for_source_ip|mask = no
reverse_match_for_destination_ip|mask = no
reverse_match_for_source_port = no
reverse_match_for_destination_port = no
reverse_match_for_protocol = no
reverse_match_for_tcp_flags = no
reverse_match_for_icmp_type = no
reverse_match_for_input_interface = no
reverse_match_for_output_interface = no
reject_with = port_unreacheable
log_level = debug
log_prefix =
log_tcp_sequence_numbers = no
log_options_from_the_tcp_packet_header = no
log_options_from_the_ip_packet_header = no
```

A list of currently active IPv4 rules can be see with the command **shell sudo /usr/sbin/iptables -L -nvx**

Plaintext Copy

```
[admin@nodegrid /]# shell sudo /usr/sbin/iptables -L -nvx

Chain INPUT (policy ACCEPT 110 packets, 13509 bytes)
    pkts      bytes  target     prot opt in     out     source               destination
    1182   132492 ACCEPT     all  --  *      *       127.0.0.1            0.0.0.0/0
       0        0 ACCEPT     all  --  *      *       192.168.56.101       0.0.0.0/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)
    pkts      bytes  target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
    pkts      bytes  target     prot opt in     out     source               destination
    1182   132492 ACCEPT     all  --  *      *       127.0.0.1            0.0.0.0/0
      59    32478 ACCEPT     all  --  *      *       192.168.56.101       0.0.0.0/0
```

A list of currently active IPv6 rules can be see with the command **shell sudo /usr/sbin/ip6tables -L -nvx**

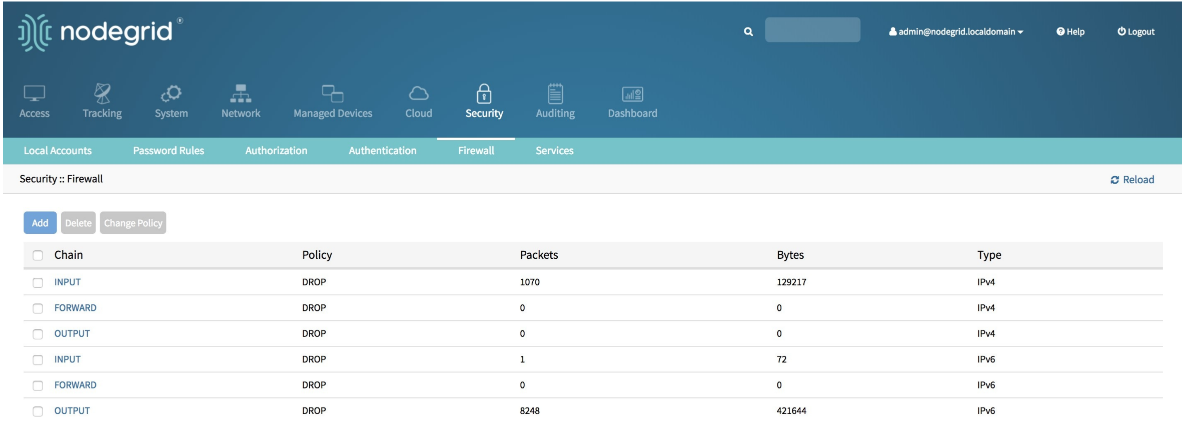
Plaintext Copy

```
[admin@nodegrid /]# shell sudo /usr/sbin/ip6tables -L -nvx

Chain INPUT (policy DROP 1 packets, 72 bytes)
    pkts      bytes  target     prot opt in     out     source               destination
       2      132 ACCEPT     all      lo     *       ::/0                 ::/0
       0        0 ACCEPT     all      *      *       ::1                  ::/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)
    pkts      bytes  target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 8384 packets, 428444 bytes)
    pkts      bytes  target     prot opt in     out     source               destination
       2      132 ACCEPT     all      *      *       ::1                  ::/0
```

Create a new Rule through WebUI

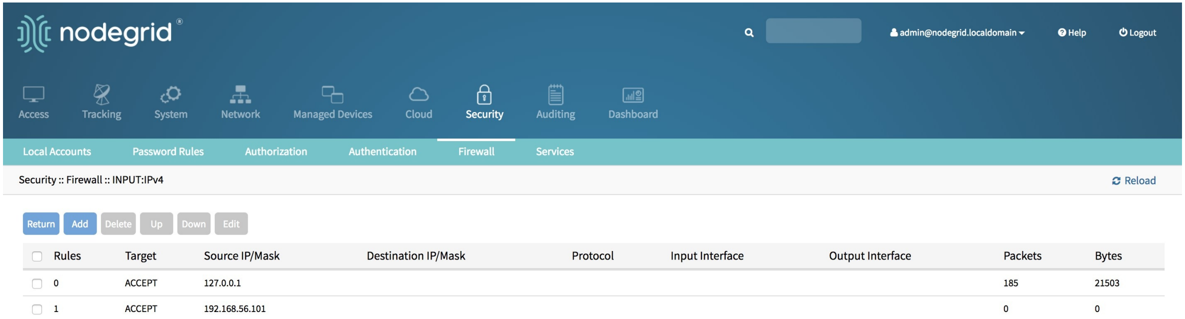
1. Log in to the Nodegrid Manager Web UI with an **admin** account.

2. Go to **Security::Firewall**.



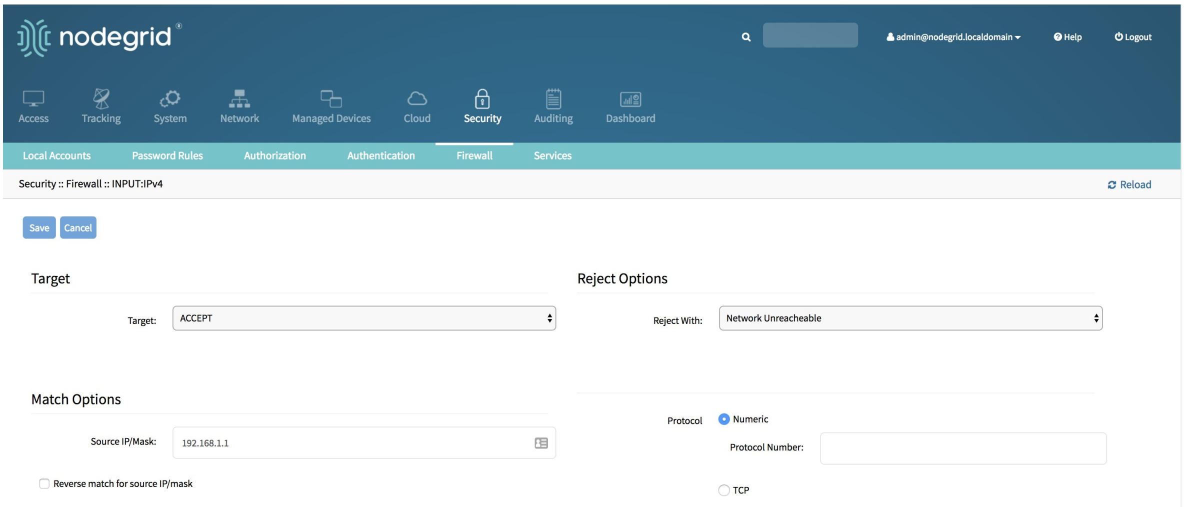
□	Chain	Policy	Packets	Bytes	Type
□	INPUT	DROP	1070	129217	IPv4
□	FORWARD	DROP	0	0	IPv4
□	OUTPUT	DROP	0	0	IPv4
□	INPUT	DROP	1	72	IPv6
□	FORWARD	DROP	0	0	IPv6
□	OUTPUT	DROP	8248	421644	IPv6

3. Click on the desired **Chain**, by default the following 6 chains are available:
   - INPUT - Type IPv4
   - FORWARD - Type IPv4
   - OUTPUT - Type IPv4
   - INPUT - Type IPv6
   - FORWARD - Type IPv6
   - OUTPUT - Type IPv6



□	Rules	Target	Source IP/Mask	Destination IP/Mask	Protocol	Input Interface	Output Interface	Packets	Bytes
□	0	ACCEPT	127.0.0.1					185	21503
□	1	ACCEPT	192.168.56.101					0	0

4. Click **Add** to create a new rule.



Target

Target: ACCEPT

Reject Options

Reject With: Network Unreachable

Match Options

Source IP/Mask: 192.168.1.1

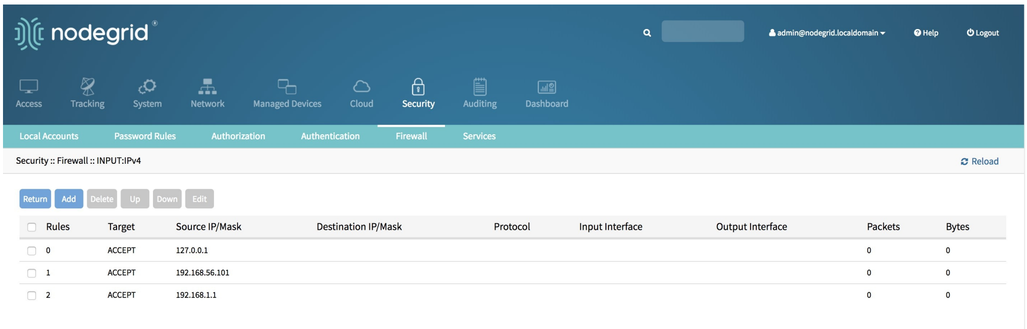
□ Reverse match for source IP/mask

Protocol ● Numeric

Protocol Number:

○ TCP

5. Enter the desired values for the new rule and click **Save**. The new rule will saved and will be effective immediately



□	Rules	Target	Source IP/Mask	Destination IP/Mask	Protocol	Input Interface	Output Interface	Packets	Bytes
□	0	ACCEPT	127.0.0.1					0	0
□	1	ACCEPT	192.168.56.101					0	0
□	2	ACCEPT	192.168.1.1					0	0

Edit an existing Rule

Edit an existing Rule through CLI

1. Log in to the Nodegrid device CLI console with an **admin** account.
2. Navigate to the firewall **Chain** which contains the rule.
3. List all available rules with the **show** command:

Plaintext Copy

```
[admin@nodegrid INPUT]# show
  rules  target  source net4      destination net4  protocol  input interface  output interface  packets  bytes
  =====  ======  ==============  ================  ========  ===============  ================  =======  ======
  0      ACCEPT  127.0.0.1                                                                       3979     251243
  1      ACCEPT  192.168.56.101                                                                  0        0
  2      ACCEPT  192.168.1.1                                                                     0        0
```

4. Navigate into the rule to be change with its rule number.

Plaintext Copy

```
[admin@nodegrid INPUT]# cd 2/
```

5. Use the **set** command to create the new rule settings. Press **TAB twice** to see all available options.

Plaintext Copy

```
[admin@nodegrid 2]# set protocol=tcp destination_port=443
```

6. Use the **commit** command to save and activate the changes.

Plaintext Copy

```
[+admin@nodegrid 2]# commit
```

7. Use the **show** command to see the current values for the rule.

Plaintext Copy

```
[admin@nodegrid 2]# show
target = ACCEPT
source_net4 = 192.168.1.1
destination_net4 =
protocol = tcp
source_port =
destination_port = 443
tcp_flag_syn = any
tcp_flag_ack = any
tcp_flag_fin = any
tcp_flag_rst = any
tcp_flag_urg = any
tcp_flag_psh = any
input_interface = any
output_interface = any
fragments = all_packets_and_fragments
reverse_match_for_source_ip|mask = no
reverse_match_for_destination_ip|mask = no
reverse_match_for_source_port = no
reverse_match_for_destination_port = no
reverse_match_for_protocol = no
reverse_match_for_tcp_flags = no
reverse_match_for_icmp_type = no
reverse_match_for_input_interface = no
reverse_match_for_output_interface = no
reject_with = port_unreacheable
log_level = debug
log_prefix =
log_tcp_sequence_numbers = no
log_options_from_the_tcp_packet_header = no
log_options_from_the_ip_packet_header = no
```

- A list of currently active IPv4 rules can be see with the command **shell sudo /usr/sbin/iptables -L -nvx**

Plaintext

Copy

```
[admin@nodegrid 2]# shell sudo /usr/sbin/iptables -L -nvx
Chain INPUT (policy ACCEPT 38 packets, 2372 bytes)
    pkts      bytes target     prot opt in     out     source               destination
     385    38206 ACCEPT     all  --  *      *       127.0.0.1            0.0.0.0/0
       0        0 ACCEPT     all  --  *      *       192.168.56.101       0.0.0.0/0
       0        0 ACCEPT     tcp  --  *      *       192.168.1.1          0.0.0.0/0            tcp dpt:443

Chain FORWARD (policy DROP 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
     385    38206 ACCEPT     all  --  *      *       127.0.0.1            0.0.0.0/0
      24     2828 ACCEPT     all  --  *      *       192.168.56.101       0.0.0.0/0
```

- A list of currently active IPv6 rules can be see with the command **shell sudo /usr/sbin/ip6tables -L -nvx**

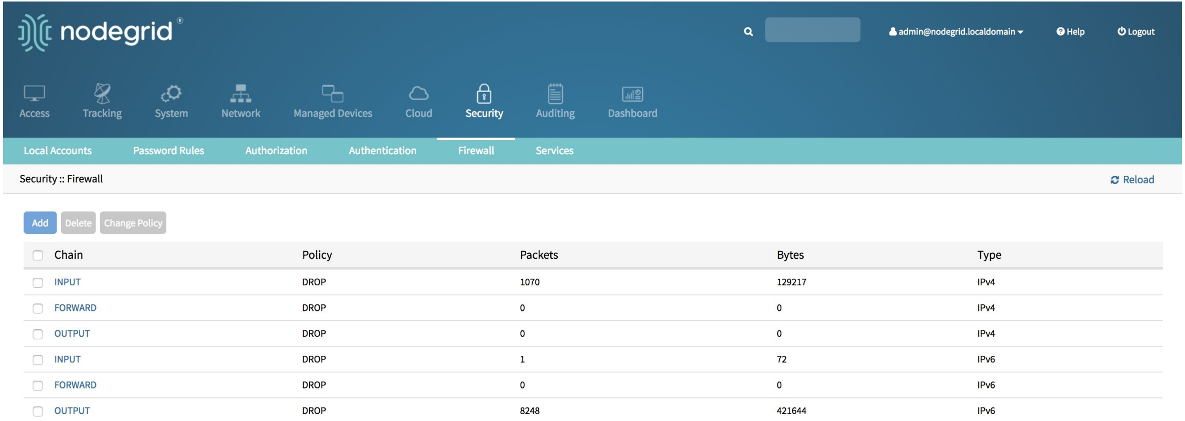
Plaintext

Copy

```
[admin@nodegrid 2]# shell sudo /usr/sbin/ip6tables -L -nvx
Chain INPUT (policy DROP 1 packets, 72 bytes)
     pkts      bytes target     prot opt in     out     source               destination
        2      132 ACCEPT     all      lo      *       ::/0                 ::/0
        0        0 ACCEPT     all      *       *       ::1                  ::/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)
     pkts      bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 8822 packets, 451048 bytes)
     pkts      bytes target     prot opt in     out     source               destination
        2      132 ACCEPT     all      *       *       ::1                  ::/0
```

Edit an existing Rule through WebUI

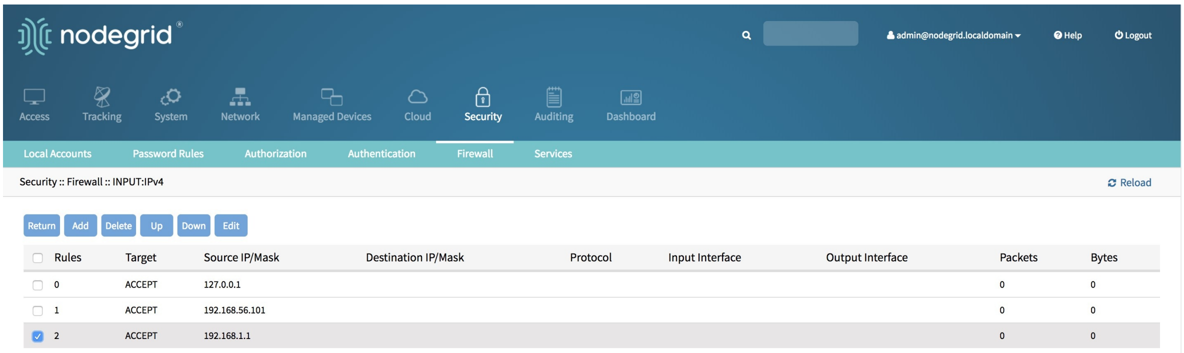
1. Log in to the Nodegrid Manager Web UI with an admin account.



Security :: Firewall

□	Chain	Policy	Packets	Bytes	Type
□	INPUT	DROP	1070	129217	IPv4
□	FORWARD	DROP	0	0	IPv4
□	OUTPUT	DROP	0	0	IPv4
□	INPUT	DROP	1	72	IPv6
□	FORWARD	DROP	0	0	IPv6
□	OUTPUT	DROP	8248	421644	IPv6

2. Go to **Security::Firewall.**
3. Click on the **Chain** which contains the rule to see a list of current rules.

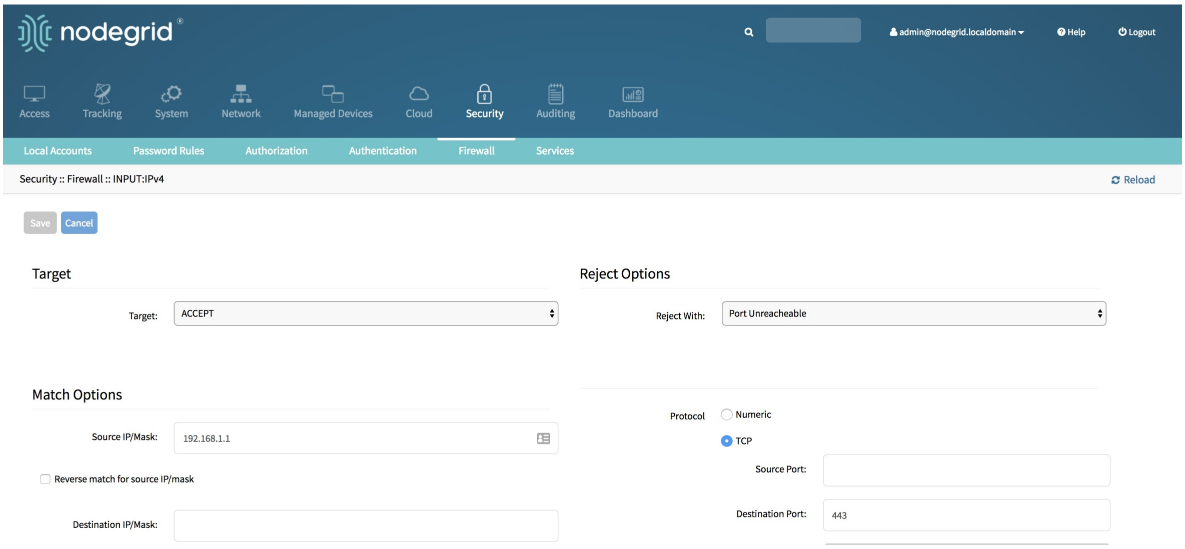


Security :: Firewall :: INPUT:IPv4

□	Rules	Target	Source IP/Mask	Destination IP/Mask	Protocol	Input Interface	Output Interface	Packets	Bytes
□	0	ACCEPT	127.0.0.1					0	0
□	1	ACCEPT	192.168.56.101					0	0
☑	2	ACCEPT	192.168.1.1					0	0

4. **Select** the rule to be changed.

5. Click **Edit**.



Security :: Firewall :: INPUT:IPv4

Target

Target: ACCEPT

Reject Options

Reject With: Port Unreacheable

Match Options

Source IP/Mask: 192.168.1.1

□ Reverse match for source IP/mask

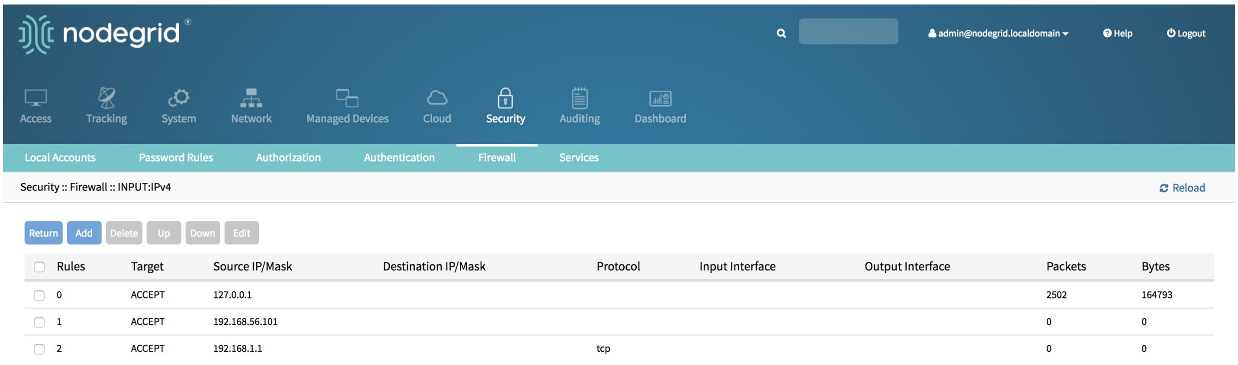
Destination IP/Mask:

Protocol ○ Numeric ● TCP

Source Port:

Destination Port: 443

6. Specify the settings as required and click **Save**. The new rule gets saved and will be effective immediately



Security :: Firewall :: INPUT:IPv4

□	Rules	Target	Source IP/Mask	Destination IP/Mask	Protocol	Input Interface	Output Interface	Packets	Bytes
□	0	ACCEPT	127.0.0.1					2502	164793
□	1	ACCEPT	192.168.56.101					0	0
□	2	ACCEPT	192.168.1.1		tcp			0	0

Delete a Rule

Delete a Rule through CLI

1. Log in to the Nodegrid device CLI console with an **admin** account.
2. Navigate to the firewall **Chain** which contains the rule:

   Plaintext Copy

   ```
   [admin@nodegrid /]# cd /settings/ipv4_firewall/chains/INPUT/
   ```

3. List all available rules with the **show** command.

   Plaintext Copy

   ```
   [admin@nodegrid INPUT]# show
     rules  target  source net4     destination net4  protocol  input interface  output interface  packets  bytes
     =====  ======  ==============  ================  ========  ===============  ================  =======  =======
     0      ACCEPT  127.0.0.1                                                                      0        0
     1      ACCEPT  192.168.56.101                                                                 0        0
     2      ACCEPT  192.168.1.1                       tcp                                          104007   5150785
   ```

4. Type **delete** together with the rule number to delete a rule and to activate the change.

   Plaintext Copy

   ```
   [admin@nodegrid INPUT]# delete 2
   ```

A list of currently active IPv4 rules can be see with the command **shell sudo /usr/sbin/iptables -L -nvx**

Plaintext Copy

```
[admin@nodegrid /]# shell sudo /usr/sbin/iptables -L -nvx
Chain INPUT (policy ACCEPT 110 packets, 13509 bytes)
    pkts      bytes target     prot opt in     out     source               destination
    1182   132492 ACCEPT     all  --  *      *       127.0.0.1            0.0.0.0/0
       0        0 ACCEPT     all  --  *      *       192.168.56.101       0.0.0.0/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
    1182   132492 ACCEPT     all  --  *      *       127.0.0.1            0.0.0.0/0
      59    32478 ACCEPT     all  --  *      *       192.168.56.101       0.0.0.0/0
```

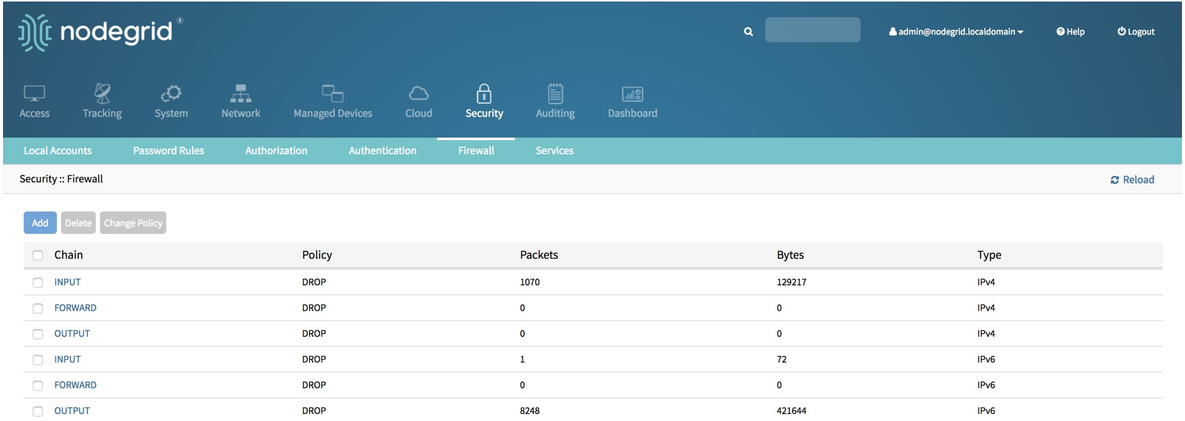
A list of currently active IPv6 rules can be see with the command **shell sudo /usr/sbin/ip6tables -L -nvx**

Plaintext Copy

```
[admin@nodegrid /]# shell sudo /usr/sbin/ip6tables -L -nvx
Chain INPUT (policy DROP 1 packets, 72 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       2      132 ACCEPT     all      lo     *       ::/0                 ::/0
       0        0 ACCEPT     all      *      *       ::1                  ::/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 8384 packets, 428444 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       2      132 ACCEPT     all      *      *       ::1                  ::/0
```

Delete a Rule through WebUI

1. Log in to the Nodegrid Manager Web UI with an admin account.

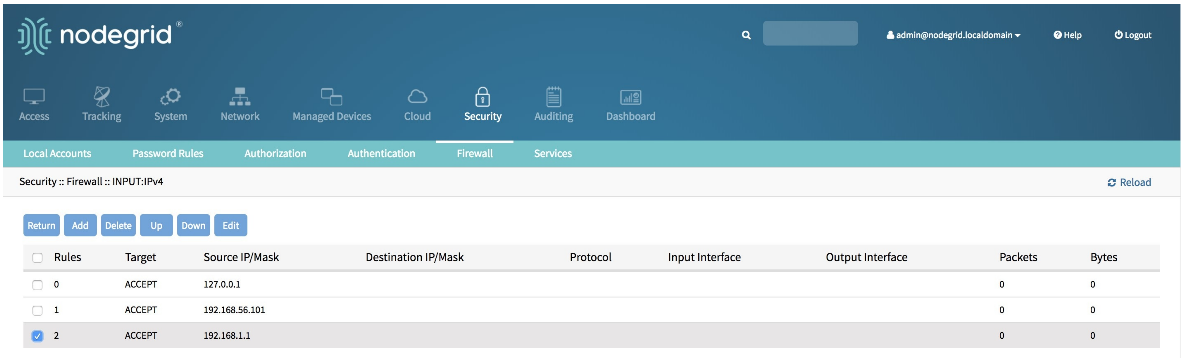


Security :: Firewall

□ Chain	Policy	Packets	Bytes	Type
□ INPUT	DROP	1070	129217	IPv4
□ FORWARD	DROP	0	0	IPv4
□ OUTPUT	DROP	0	0	IPv4
□ INPUT	DROP	1	72	IPv6
□ FORWARD	DROP	0	0	IPv6
□ OUTPUT	DROP	8248	421644	IPv6

2. Go to *Security::Firewall*.

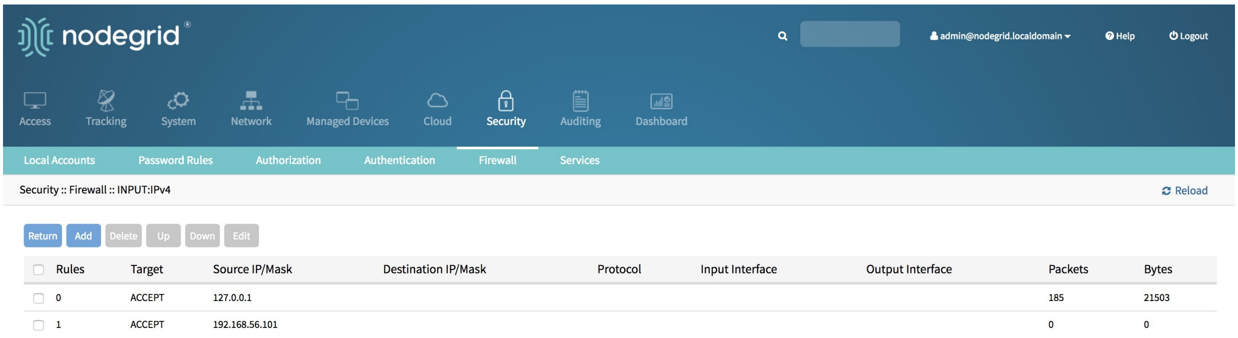
3. Click on the **Chain** which contains the rule to see a list of current rules.



Security :: Firewall :: INPUT:IPv4

□	Rules	Target	Source IP/Mask	Destination IP/Mask	Protocol	Input Interface	Output Interface	Packets	Bytes
□	0	ACCEPT	127.0.0.1					0	0
□	1	ACCEPT	192.168.56.101					0	0
☑	2	ACCEPT	192.168.1.1					0	0

4. Select the rule to be deleted.
5. Click **Delete.** The rule gets deleted and the change will be effective immediately



Security :: Firewall :: INPUT:IPv4

□	Rules	Target	Source IP/Mask	Destination IP/Mask	Protocol	Input Interface	Output Interface	Packets	Bytes
□	0	ACCEPT	127.0.0.1					185	21503
□	1	ACCEPT	192.168.56.101					0	0

Set Default Policy for a Chain

Set default Policy for a Chain through CLI

Before changing the default policy for a chain to drop ensure that all required accept rules have been entered. After the change takes effect all not allowed access will be dropped.

1. Log in to the Nodegrid device CLI console with an admin account.
2. Navigate to the firewall policy to changed.
   IPv4 Policies are located at:

   Plaintext Copy
   ```
   [admin@nodegrid /]# cd /settings/ipv4_firewall/policy/
   ```

   IPv6 Policies are located:

   Plaintext Copy
   ```
   [admin@nodegrid /]# cd /settings/ipv6_firewall/policy/
   ```

3. Use the **show** command to list the current settings.

   Plaintext Copy
   ```
   [admin@nodegrid policy]# show input = accept
   output = accept forward = accept
   ```

4. Change the default policy for a chain with the set command.

   Plaintext Copy
   ```
   [admin@nodegrid policy]# set input=drop
   ```

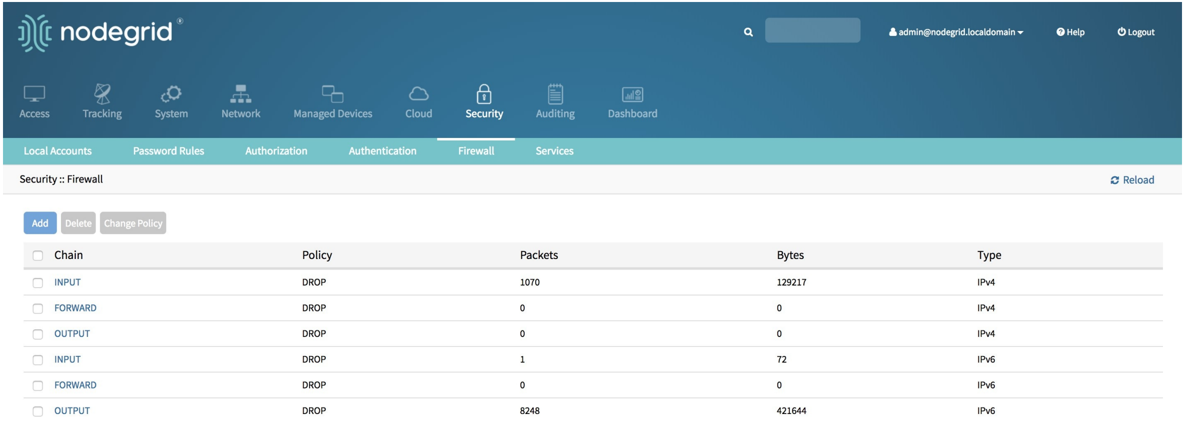
5. Use the **commit** command to save and activate the changes.

   Plaintext Copy
   ```
   [+admin@nodegrid policy]#commit
   ```

Set default Policy for a Chain through WebUI

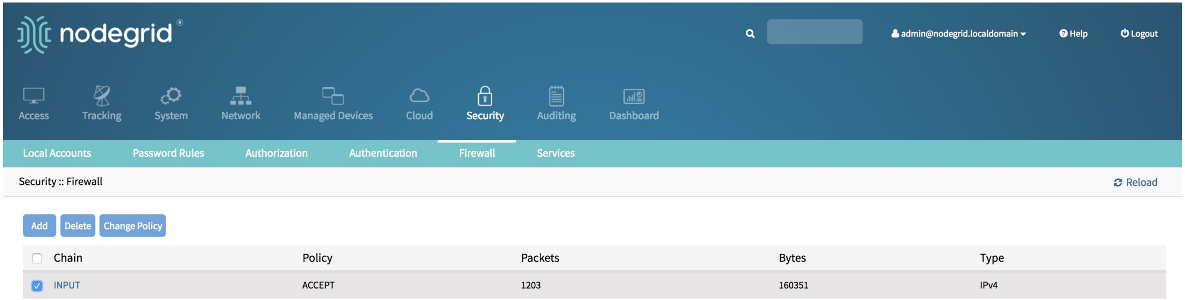
Before changing the default policy for a chain to drop ensure that all required accept rules have been entered. After the change takes effect all not allowed access will be dropped.

1. Log in with an admin account and go to *Security::Firewall*.



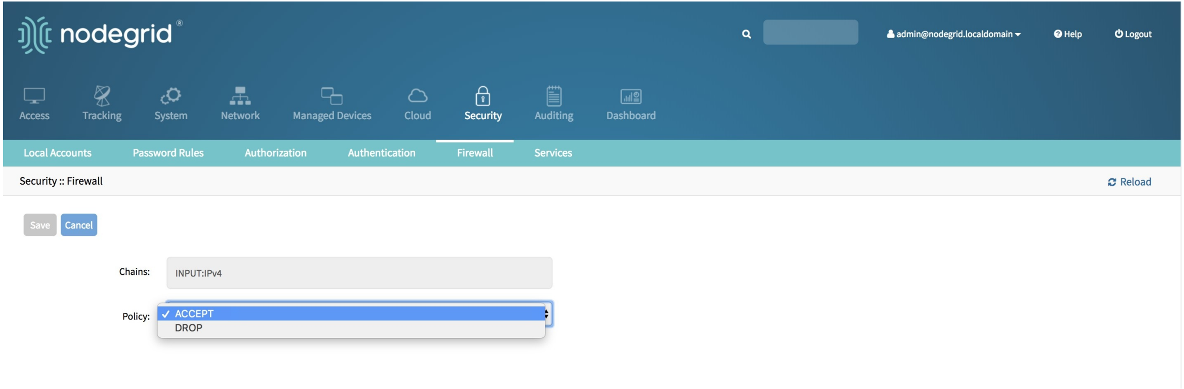
□	Chain	Policy	Packets	Bytes	Type
□	INPUT	DROP	1070	129217	IPv4
□	FORWARD	DROP	0	0	IPv4
□	OUTPUT	DROP	0	0	IPv4
□	INPUT	DROP	1	72	IPv6
□	FORWARD	DROP	0	0	IPv6
□	OUTPUT	DROP	8248	421644	IPv6

2. Select the Chain for which the default policy should be changed.



□	Chain	Policy	Packets	Bytes	Type
☑	INPUT	ACCEPT	1203	160351	IPv4

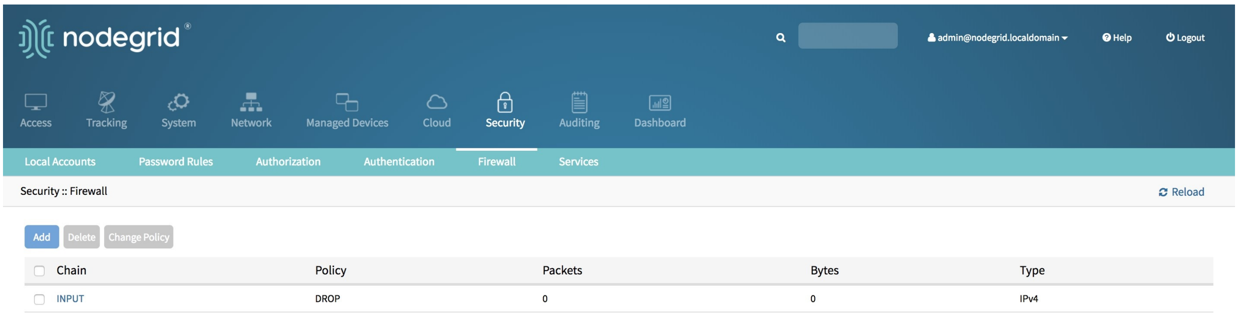
3. Click on **Change Policy.**



Chains: INPUT:IPv4

Policy: ✓ ACCEPT
DROP

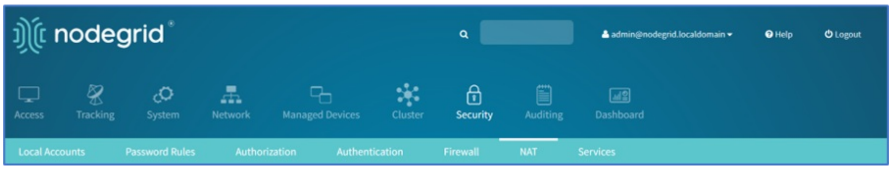
4. Set the new default policy and accept the change with **Save**. The new Policy gets saved and will be effective immediately



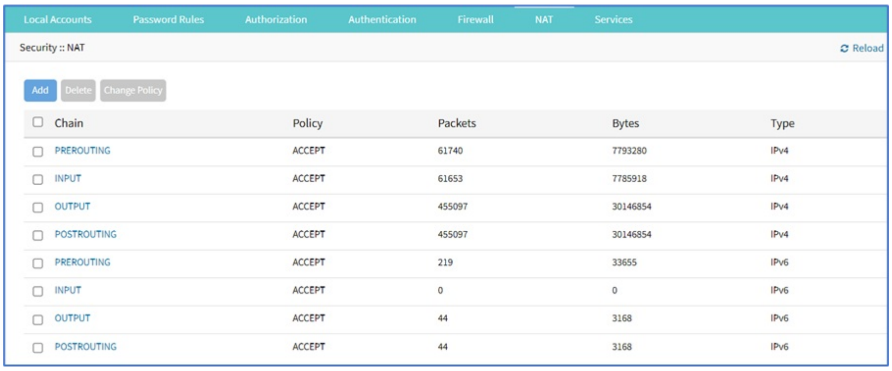
☐ Chain	Policy	Packets	Bytes	Type
☐ INPUT	DROP	0	0	IPv4

NAT tab

There are eight built-in default chains (cannot be deleted): IPv4 with four, IPv6 with four. These accept Pre-routing, Output, Input, and Post-routing packets. Rules can be created for each chain.



Manage NAT Chains

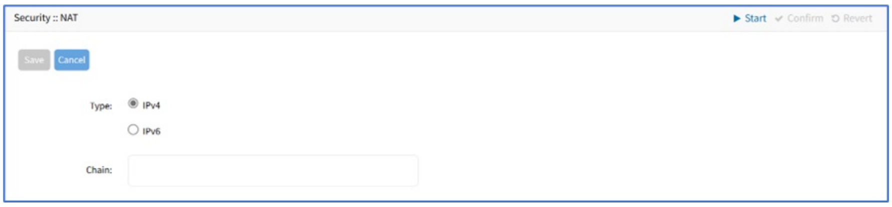


Security :: NAT

□ Chain	Policy	Packets	Bytes	Type
□ PREROUTING	ACCEPT	61740	7793280	IPv4
□ INPUT	ACCEPT	61653	7785918	IPv4
□ OUTPUT	ACCEPT	455097	30146854	IPv4
□ POSTROUTING	ACCEPT	455097	30146854	IPv4
□ PREROUTING	ACCEPT	219	33655	IPv6
□ INPUT	ACCEPT	0	0	IPv6
□ OUTPUT	ACCEPT	44	3168	IPv6
□ POSTROUTING	ACCEPT	44	3168	IPv6

Add a Chain

1. Go to *Security :: NAT*.
2. Click **Add** (displays dialog).



Security :: NAT

Type: ● IPv4 ○ IPv6

Chain:

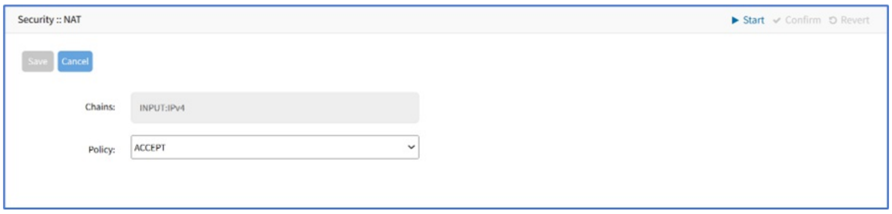
3. On Type menu, select one:
   - **IPv4** radio button
   - **IPv6** radio button
4. Enter **Chain** (name of this chain).
5. Click **Save**.

Delete a Chain

1. Go to *Security :: NAT*.
2. Select checkbox next to name to be deleted.
3. Click **Delete**.
4. On confirmation dialog, click **OK**.

Change Chain Policy

1. Go to *Security :: NAT*.
2. In the *Chain* column, select checkbox next to a chain.
3. Click **Change Policy** (displays dialog). On **Policy** drop-down, select one (ACCEPT, DROP).



Security :: NAT

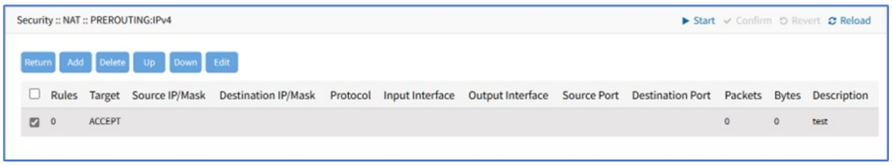
Chains: INPUT:IPv4

Policy: ACCEPT

4. Click **Save**.

Manage NAT Chain Settings

To manage chain functions/settings, click on the name in the *Chain* column (displays dialog).

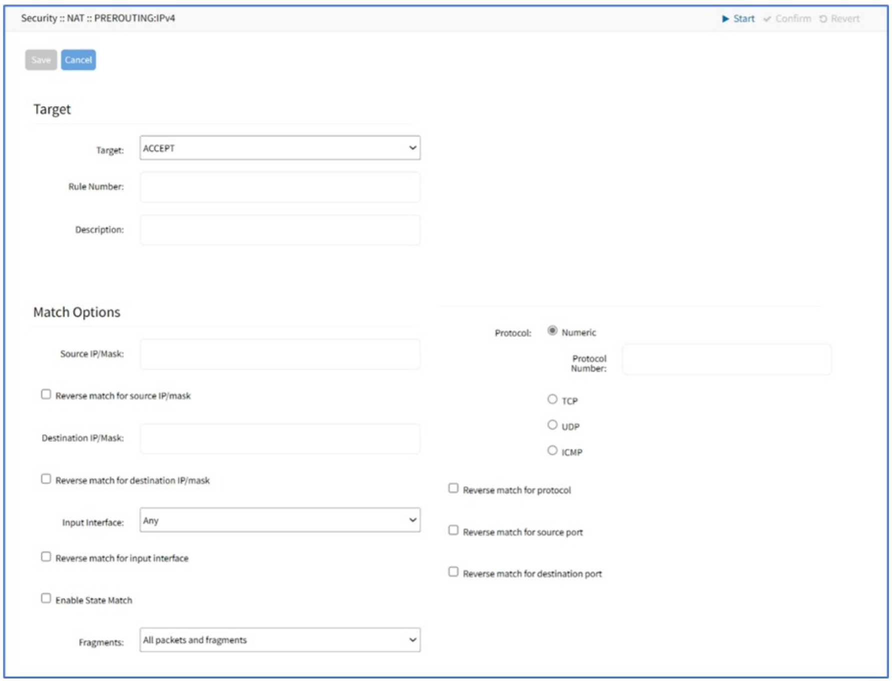

Security :: NAT :: PREROUTING:IPv4
▶ Start ✓ Confirm ↻ Revert ↻ Reload
Return
Add
Delete
Up
Down
Edit

☐	Rules	Target	Source IP/Mask	Destination IP/Mask	Protocol	Input Interface	Output Interface	Source Port	Destination Port	Packets	Bytes	Description
☑	0	ACCEPT								0	0	test

Note: If you import a configuration for a chain through CLI, the rules defined for the specified chain(s) will be overridden by the imported configuration. For example, if you are importing configuration For the INPUT and OUTPUT chains, the FORWARD chain will not be changed, only the INPUT and OUTPUT chains are updated.

Add Chain Setting (all Type selections)

1. Go to *Security :: NAT*.
2. In the *Chain* column, locate and click on the name (displays dialog).
3. Click **Add** (displays dialog).


Security :: NAT :: PREROUTING:IPv4
▶ Start ✓ Confirm ↻ Revert
Save
Cancel
Target
Match Options

Target: ACCEPT

Rule Number:

Description:

Source IP/Mask:

☐ Reverse match for source IP/mask

Destination IP/Mask:

☐ Reverse match for destination IP/mask

Input Interface: Any

☐ Reverse match for input interface

☐ Enable State Match

Fragments: All packets and fragments

Protocol: ● Numeric

Protocol Number:

○ TCP

○ UDP

○ ICMP

☐ Reverse match for protocol

☐ Reverse match for source port

☐ Reverse match for destination port

4. On *Target* menu:
   a. On **Target** drop-down, select one (ACCEPT, DNAT, REDIRECT, LOG, RETURN).
   b. Enter **Rule Number.**
   c. Enter **Description.**
5. On the *Match Options* menu:
   a. Enter **Source IP/Mask.**
   b. Select **Reverse match for source IP/mask** checkbox.
   c. Enter **Destination IP/Mask.**
   d. Enter **Source MAC Address.**
   e. Select **Reverse match for source MAC address** checkbox.

   Note: The Source MAC Address and Reverse Match for the source MAC Address fields are applicable only for Input, PREROUTING, and FORWARD chains.

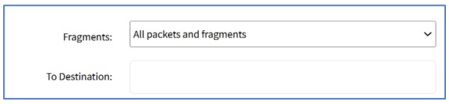
   f. Select **Reverse match for destination IP/mask** checkbox.
   g. Select the required Input Interface from the drop-down list. (Any, lo, eth0, eth1).

   Note: The Source MAC Address and Reverse Match for the source MAC Address fields are applicable only for Input, PREROUTING, and FORWARD chains

   Select **Reverse match for the input interface** checkbox.
   h. Select **Enable State Match**checkbox (displays options – one or more can be selected):
      - **NEW** checkbox
      - **ESTABLISHED** checkbox
      - **RELATED** checkbox

- **INVALID** checkbox
- **SNAT** checkbox
- **DNAT** checkbox
- **Reverse state match** checkbox

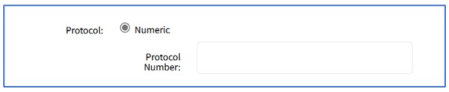
6. On the **Fragments** drop-down, select one (All packets and fragments, Unfragmented packets and 1st packets, 2nd and further packets). (if **Type** selection: **DNAT**) Enter **To Destination**.



Fragments: All packets and fragments

To Destination:

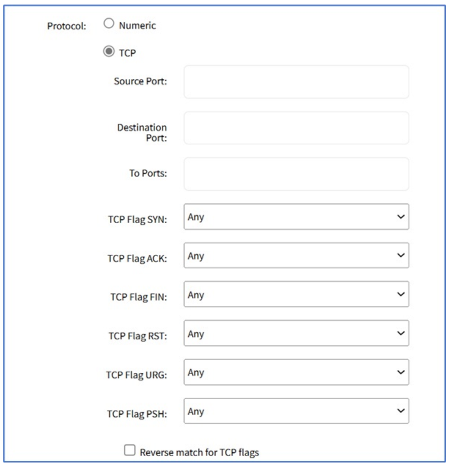
7. On the *Protocol* menu, select one:
   - **Numeric** radio button (expands dialog). Enter the **Protocol Number**.



Protocol: ● Numeric

Protocol Number:

   - **TCP** radio button (expands dialog).



Protocol: ○ Numeric

● TCP

Source Port:

Destination Port:

To Ports:

TCP Flag SYN: Any

TCP Flag ACK: Any

TCP Flag FIN: Any

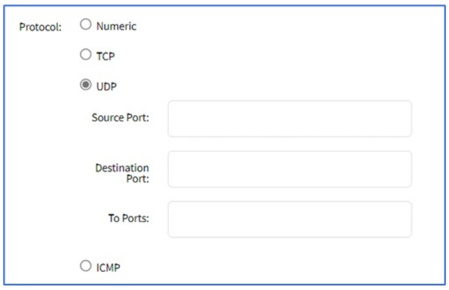
TCP Flag RST: Any

TCP Flag URG: Any

TCP Flag PSH: Any

□ Reverse match for TCP flags

     - Enter **Source Port.**
     - Enter **Destination Port.**
     - Enter **To Ports.**
     - **TCP Flag SYN** drop-down, select one (Any, Set, Unset).
     - **TCP Flag ACK** drop-down, select one (Any, Set, Unset).
     - **TCP Flag FIN** drop-down, select one (Any, Set, Unset).
     - **TCP Flag RST** drop-down, select one (Any, Set, Unset).
     - **TCP Flag URG** drop-down, select one (Any, Set, Unset).
     - **TCP Flag PSH** drop-down, select one (Any, Set, Unset).
     - Select **Reverse Match for the TCP Flags** checkbox.
   - **UDP** radio button (expands dialog):



Protocol: ○ Numeric

○ TCP

● UDP

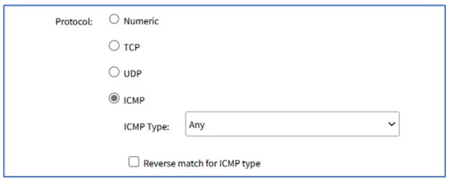
Source Port:

Destination Port:

To Ports:

○ ICMP

     - Enter **Source Port.**
     - Enter **Destination Port.**
     - Enter **To Ports.**
   - **ICMP** radio button (expands dialog):



Protocol: ○ Numeric

○ TCP

○ UDP

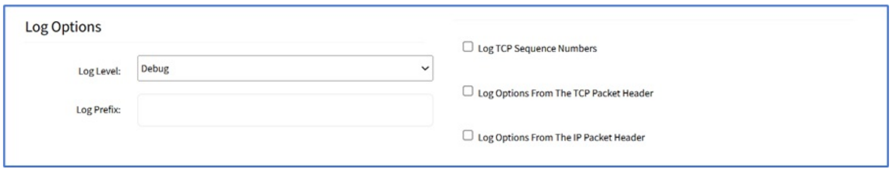
● ICMP

ICMP Type: Any

□ Reverse match for ICMP type

     - On **ICMP Type** drop-down, select one.
     - Select **Reverse match for ICMP type** checkbox.

8. Select **Reverse match for the protocol** checkbox.
9. Select **Reverse match for the source port** checkbox.
10. Select **Reverse match for the destination port** checkbox.
11. On the *Log Options* menu (shows when **Type** selection: **LOG**).


Log Options

Log Level: Debug

Log Prefix:

□ Log TCP Sequence Numbers

□ Log Options From The TCP Packet Header

□ Log Options From The IP Packet Header

a. On the **Log Level** drop-down, select one (Debug, Info, Notice, Warning, Error, Critical, Alert, Emergency).
b. Enter **Log Profile** (name of this profile).
c. Select **Log TCP Sequence Numbers** checkbox.
d. Select **Log Options From The TCP Packet Header** checkbox.
e. Select **Log Options From The IP Packet Header** checkbox.

12. Click **Save**.

Edit Chain Setting

1. Go to *Security :: NAT*.
2. In the *Chain* column, locate and click on the checkbox.
3. Click **Edit** (displays dialog).
4. Make changes, as needed.
5. Click **Save**.

Delete Chain Setting

1. Go to *Security :: NAT*.
2. In the *Chain* column, locate and select the checkbox next to the name.
3. Click **Delete**.
4. On the confirmation dialog, click **OK**.

Move Chain Up

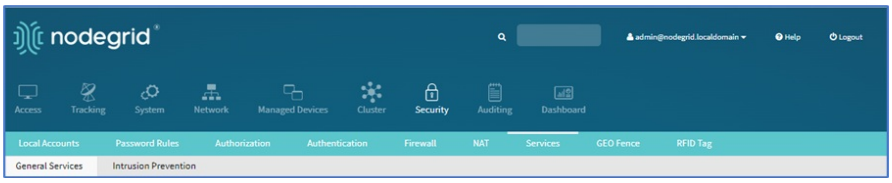
1. Go to *Security :: NAT*.
2. In the *Chain* column, locate and select the checkbox on the name.
3. Click **Up** to move up.

Move Chain Down

1. Go to *Security :: NAT*.
2. In the *Chain* column, locate and select the checkbox on the name.
3. Click **Down** to move down.

Services tab

The device's security level is configured here. This includes active service settings for ZPE Cloud, managed devices, intrusion prevention, SSH, web service settings, and cryptographic protocols.



General Services sub-tab

General security service settings are configured on this page. Because of this complexity, it is recommended to prepare a document that defines how the company security requirements are implemented with the device security settings.

Configure General Services

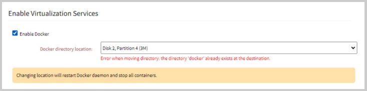
1. Go to *Security :: Services :: General Services*. Enter details:
2. In the *ZPE Cloud section*(cloud-based management platform for Nodegrid products):
    a. Select **Enable ZPE Cloud** checkbox (Nodegrid NSR, GSR, BSR, LSR, HSR - default: enabled. Nodegrid Serial Console - default: disabled). When Once enabled you can access this device from the ZPE cloud.
    b. **ZPE Cloud URL:** This is a read-only field, that automatically populates the URL to the ZPE cloud.
    c. **Enable Remote Access**: Check this field to remotely access the device, this is useful when you want to take the backup of the data.
    d. (optional) **Enable File Protection:** If enabled, file transfer requires an authentication hash based on this password to validate file integrity and origin. The field is disabled by default. If enabled, enter **Passcode** and **Confirm Passcode**.
3. Select **Enable File Encryption** checkbox (expands dialog)
    a. On the *File Encryption Mode* menu (select one):
        - **Encryption by Passcode** radio button. Enter the **Encryption Passcode** and **Confirm the Encryption Passcode**.
        - **Encryption by an Asymmetric Key** radio button. Select **Encryption with Base64** checkbox.
4. In the *Active Services* section (select all that apply):
    a. **Enable detection of USB devices:** If enabled, detect if any USB is attached to the device.
    b. **Enable RPC:** Enable if you want to request services from other programs on a different machine in a network.
    c. **Enable gRPC** checkbox: If enabled, enter **gRPC Port** (default: 4830)
    d. **Enable FTP Service** checkbox.
    e. **Enable SNMP Service** checkbox (default: enabled)
    f. **Enable Telnet Service to Nodegrid** checkbox (expands dialog). Enter **Telnet TCP Port** (default: 23).
    g. **Enable Telnet Service to Managed Devices** checkbox.
    h. **Enable ICMP echo reply** checkbox.
    i. **Enable ICMP secure redirects** checkbox.
    j. **Enable USB over IP** checkbox.
    k. **Enable Search Engine** checkbox (expands dialog). Select the **Enable Dashboards** checkbox.
    l. **Enable Telegraf** checkbox.
    m. **Enable Services Status Page** (<NG URL>/services/status) used to determine functioning services.
    n. **Enable reboot on Services Status Page** checkbox (allows device reboot on the /services/status page).
    o. **Enable keepalived** checkbox to enable a keepalive session for a Nodegrid device. Enabling this option ensures that the keepalive session starts during the system reboot and remains active throughout the session. With the option enabled, the keepalived settings can also be exported and imported along with the other Nodegrid configurations.

You can also enable the keepalived setting via the CLI by entering the following command:

```
[admin@nodegrid services]# set enable_keepalived=yes
```

1. In the *Enable Virtualization Services section*(select all that apply):
    a. **Enable Docker:** When you enable the field, the **Docker directory location** drop-down list is displayed. It lists all the suitable locations to which the Docker daemon and its files can be moved and lists any disk or partition that is formatted and mounted. The Default option points to the primary disk location; */var/lib*.

    If there is not enough space in the selected folder, an error is displayed:

    Enable Virtualization Services

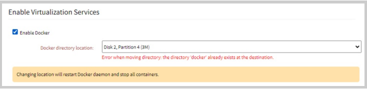
    ☑ Enable Docker

    Docker directory location: Disk 2, Partition 4 (3M)

    Error when moving directory: the directory 'docker' already exists at the destination.

    Changing location will restart Docker daemon and stop all containers.

    b. If there is an existing folder called **Docker,** an error is displayed:

    Enable Virtualization Services

    ☑ Enable Docker

    Docker directory location: Disk 2, Partition 4 (3M)

    Error when moving directory: the directory 'docker' already exists at the destination.

    Changing location will restart Docker daemon and stop all containers.

    c. **Enable Qemu/KVM** checkbox.
    d. **Enable VMware Manager** checkbox.
    e. **Cluster TCP Port** (default: 9966).
    f. **Enable Automatic Cluster Enrollment** checkbox.
    g. **Search Engine TCP Port** (default: 9300).
    h. **Enable Search Engine High Level Cipher Suite** checkbox.
        i. VM Serial Port (default: 9977)
        ii. vMotion timeout [seconds] (default: 300)
    i. **Enable VM Serial access** checkbox (default: enabled).
    j. **Enable Zero Touch Provisioning** checkbox (default: enabled).
    k. **Enable Bluetooth** checkbox.

    > **NOTE**
    >
    > (default: enabled) Completely enables/disables Bluetooth on the device. When enabled, tethers the network connection via Bluetooth to the device without any configuration. This tethers the network connection via Bluetooth to be the first device deployed on the network. This temporary connection reaches ZPE Cloud to download its full configuration.

    l. **Display name** (Default format: <ProductName_SerialNumber> This name is displayed on other devices paired with this device via Bluetooth.
    m. **Enable Bluetooth Discoverable mode** checkbox (default: Enabled).

> **NOTE**
> Enables discovery and pairing of this device to an external device. This tethers the network connection via Bluetooth to be the first device deployed on the network. This temporary connection reaches ZPE Cloud to download its full configuration. When a connection is established to a trusted device, this discoverable mode can be disabled to ensure other devices cannot pair with this device.

n. **Enable PXE (Preboot eXecution Environment)** checkbox (default: enabled).
o. **Block Host with multiple authentication failures** checkbox (expands dialog).
   i. Period Host will stay blocked (min) (default: 10).
   ii. Enter Timeframe to monitor authentication fails (min) (default: 10).
   iii. The number of authentication fails to block the host (default: 5).
   iv. Whitelisted IP Addresses (comma-separated).

p. **Block Account with multiple authentication failures**: Enable this field if you want to lock the account when the credentials are entered incorrectly multiple times. If you enable the field enter the following details:
   i. Period Account will stay blocked (min): The duration for which you want to keep the account locked out.
   ii. Timeframe to monitor authentication fails (min): the time frame for which the authentication failure is monitored.
   iii. Number of Authentication failed to block account: The account will be locked out after the specified number of attempts.
   iv. Show message when the account is blocked: If the account gets locked, a relevant message is displayed in the UI.

q. **Enable Console Access**: provides administrators the ability to control access to the primary console interface, which includes both the Console Serial Port and the Video VGA/HDMI and USB Keyboard ports.
   To allow root console access, select both **Enable console access** and **Allow root console access** fields.
   When you disable the console access:
   i. Critical system components such as Console Live system authentication, Bootloaders, and root console access are not accessible anymore.
   ii. BIOS settings are accessible, to make it inaccessible use the **Password protected boot** feature.
   iii. Unchecking **Allow root console access** disables access to the root users as well and they will encounter a login incorrect error message as shown in the following example.

Plaintext | Copy

```
nodegrid login: root

Login incorrect
nodegrid login: Event Notification from nodegrid. Reported on 2024-04-17T11:51:04z. Event ID 202: User authentication failed. User: root on 'ttyS0'.
```

System Console Events is turned off.

> **Note:**
>
> It's crucial to carefully consider the implications of disabling the main console port. This action may impact low-level maintenance tasks that necessitate direct access to the system. Make sure to evaluate your specific requirements for maintenance and security before disabling Console Access.

On the *Managed Devices* menu (select all that apply):

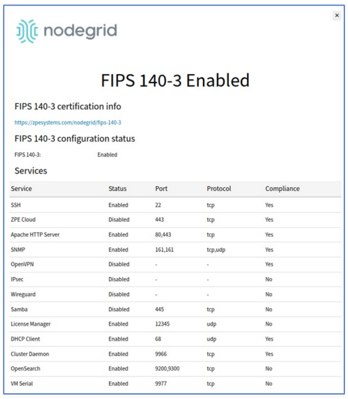
1. **Device access is enforced via user group authorization** checkbox (If enabled, users can only access devices listed in the user's authorization groups. If not enabled, all enrolled devices are available).
2. **Enable the Autodiscovery** checkbox. Select **the DHCP lease controlled by the autodiscovery rules** checkbox (default: disabled).

On *FIPS 140-3* menu: (available in v5.8+)

1. Select the **Enable FIPS 140-3** checkbox. Enabling FIPS 140-3 on a Nodegrid device ensures FIPS compliance, limiting cryptographic services to the FIPS provider for the applications that rely on OpenSSL for these services.
   Network services and ports that rely on OpenSSL for cryptographic services will be FIPS 140-3 compliant when enabled, including:
   - HTTPS (TCP port 443)
   - SSH client and server (TCP port 22)
   - SNMP (TCP port 161)
   - Cluster (TCP port 9966)
   For a more detailed list, refer to the FIPS 140-3 status page (Click on the FIPS 140-3 button on the top right of the web UI).

   > **NOTE**
   > Enabling or disabling FIPS 140-3 requires the Nodegrid device to be rebooted for all changes to take effect.

2. In the user interface, the *Banner* (right side) shows FIPS 140-3 is active.
3. Click the **FIPS 140-3** button to display the status.



FIPS 140-3 Enabled

FIPS 140-3 certification info

https://zpesystems.com/nodegrid/fips-140-3

FIPS 140-3 configuration status

FIPS 140-3: Enabled

Services

Service	Status	Port	Protocol	Compliance
SSH	Enabled	22	tcp	Yes
ZPE Cloud	Disabled	443	tcp	Yes
Apache HTTP Server	Enabled	80,443	tcp	Yes
SNMP	Enabled	161,161	tcp,udp	Yes
OpenVPN	Disabled	-	-	Yes
IPsec	Disabled	-	-	No
Wireguard	Disabled	-	-	No
Samba	Disabled	445	tcp	No
License Manager	Enabled	12345	udp	No
DHCP Client	Enabled	68	udp	Yes
Cluster Daemon	Enabled	9966	tcp	Yes
OpenSearch	Enabled	9200,9300	tcp	No
VM Serial	Enabled	9977	tcp	No

4. You may also verify that FIPS is enabled from the root shell using the following command:

Plaintext Copy

```
root@nodegrid:~# openssl list -providers
Providers:
  base
    name: OpenSSL Base Provider
    version: 3.0.12
    status: active
  fips
    name: OpenSSL FIPS Provider
    version: 3.0.10
    status: active
```

5. On the *SSH* menu:
   - Select **SSH allow root access** checkbox (default: disabled).
   - Enter **SSH TCP Port** (default: 22).
   - Enter **SSH Ciphers** (comma-separated) (default: blank).
   - Enter **SSH MACs** (comma-separated) (default: blank).
   - Enter **SSH Kex Algorithms** (comma-separated) (default: blank).
6. On the *Web Service* menu:
   a. Select **Enable HTTP access** checkbox (default: enabled). Enter **HTTP Port** (default: 80).
      - Select **Enable HTTPS access** checkbox (default: enabled).
      - Enter **HTTP Port** (default: 443).
      - Select **Redirect HTTP to HTTPS** checkbox (default: enabled).
7. Select the **Enable HTTP/S File Repository** checkbox (default: disabled).

   > **NOTE:**
   > When enabled, provide public access to files uploaded in the File Manager/datastore folder (to access the file publicly, use https://<Nodegrid URL>/datastore/<filename.ext>). For security reasons, the full path of the file is required. In addition, "list", "edit", and "post" commands are disabled.

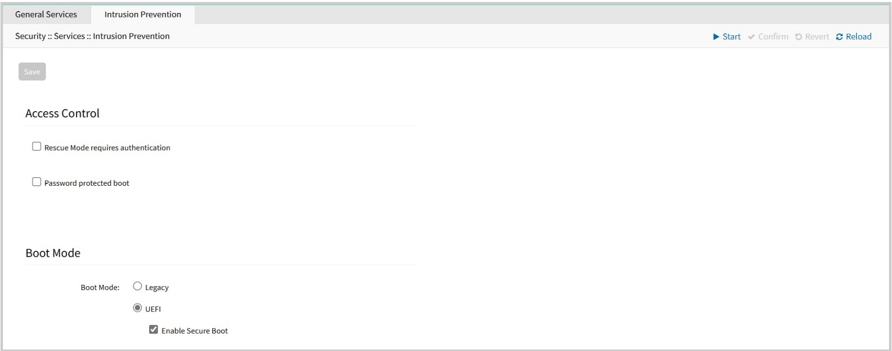
   You can enable access to the Web UI using the CLI. To do this, access the Console and run the following commands. This method is useful if a user gets locked out of the Web UI and when HTTP and HTTPS are disabled.

   Plaintext Copy

   ```
   cd/settings/services
   enable_http_access = yes
   http_port = 80
   enable_https_access = yes
   http_port = 443
   redirect_http_to_https = no
   commit
   ```
8. On *FRR* menu, select as needed:
   - **Enable BGP** checkbox
   - **Enable OSPFv2** checkbox
   - **Enable OSPFv3** checkbox
   - **Enable RIP** checkbox
   - **Enable VRRP** checkbox
9. On *Cryptographic Protocols* menu, select as needed:
   - **TLSv1.3** checkbox (default: enabled)
   - **TLSv1.2** checkbox (default: enabled)
   - **TLSv1.1** checkbox (default: disabled)
   - **TLSv1**checkbox (default: disabled)
10. On *Cipher Suite Level* menu, select one:
    - **High** radio button
    - **Medium** radio button (default)
    - **Low** radio button
    - **Custom** radio button (expands dialog). Enter **Custom Cipher Suite.**
11. Click **Save**. ZPE Cloud ensures all deployment activity is done at the device location.

Intrusion Prevention sub-tab

This configures intrusion prevention settings.



General Services | Intrusion Prevention

Security :: Services :: Intrusion Prevention

▶ Start ✓ Confirm ⟲ Revert ⟳ Reload

Save

Access Control

☐ Rescue Mode requires authentication

☐ Password protected boot

Boot Mode

Boot Mode: ○ Legacy

● UEFI

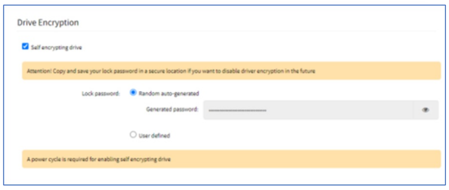
☑ Enable Secure Boot

Configure Intrusion Prevention

WARNING

On Boot Mode menu, do NOT select Legacy radio button. It is a weaker configuration.

1. Go to *Security :: Services :: Intrusion Prevention*.
2. In *Access Control* menu:
   a. Select **Rescue Mode requires authentication** checkbox.
   b. Select **Password protected boot** checkbox (password required to reboot).
3. In *Drive Encryption* menu (only available if drive is OPAL 2 compliant), select **Self encrypting drive** checkbox. If enabled, the device must be restarted for the change to take effect.



Drive Encryption

☑ Self encrypting drive

Attention! Copy and save your lock password in a secure location if you want to disable driver encryption in the future

Lock password: ● Random auto-generated

Generated password: ---------------------------

○ User defined

A power cycle is required for enabling self encrypting drive

   a. On *Lock Password* menu, select one:
      - **Random auto-generated** radio button.

        IMPORTANT

        Save this Password in a secure location. If lost, it cannot be recovered.

      - **User defined** radio button. Enter **Password**.
4. Click **Save**.

Change Boot Mode to Legacy

1. Go to *Security :: Services :: Intrusion Prevention*.
2. In *Boot Mode* menu:
3. In Boot Mode, select **Legacy** radio button.
4. Click **Save**.

SED Pre-Boot Authenticator (PBA)

Install or upgrade SED Pre-Boot authenticator

SED must be disabled before upgrading or installing the SED PBA. If currently enabled, enter the unlock password and disable it.

1. Contact a ZPE representative to get valid copies of these PBA image files:
   - pba.img
   - pba.img.sha256
2. Copy the files to /var/sed
3. Restart system and boot into Rescue Mode.
4. Execute the script:

   None Copy

   ```
   /usr/sbin/sed_install.sh
   ```

5. When prompted, type:

   None Copy

   ```
   continue.\
   ```

6. Enter path to the SED PBA image file.
7. Enter path to the SED PBA Image hash file.
8. Accept SED PBA version check.
9. Wait for installation to complete.
10. Once complete, power cycle the device for changes to take effect.

Certificates Tab

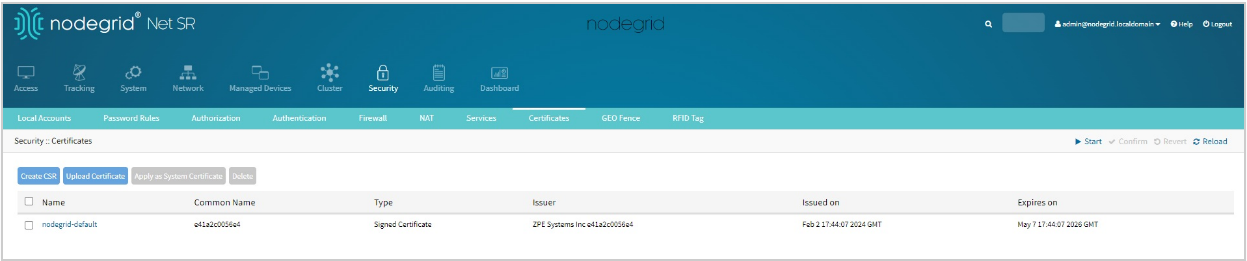
The **Certificates** tab serves as a central hub for creating and managing certificates. Certificates for the following two functions are managed on this page:

- **Certificate for Web server:**
    - You can create certificates that can be applied to the web server for secure communication.
    - The **Nodegrid-default certificate** is the default web server certificate generated by the system.
- **Certificates for IPsec tunnel:**
    - You can create certificates that you can use while creating IPsec tunnels to ensure secure authentication, encrypted data transfer, and trust between VPN endpoints.

      ZPE supports X.509 encoded certificates. This includes PCKS, PFX, DEM, and PEM formats.

The Webserver Certificate

- You can create a web server certificate or upload one created outside of the Nodegrid. The web server in the Nodegrid uses this certificate for all the HTTP and HTTPS communication via the web interface.
- For Nodegrid version 6.0.2 and above, a **default webserver certificate is installed. This certificate is listed under the Certificates** tab.
- If you have the certificate applied to the system, and you delete the certificate, the certificate will continue to remain applied to the system.



Security :: Certificates

□	Name	Common Name	Type	Issuer	Issued on	Expires on
□	nodegrid-default	e41a2c0056e4	Signed Certificate	ZPE Systems Inc e41a2c0056e4	Feb 2 17:44:07 2024 GMT	May 7 17:44:07 2026 GMT

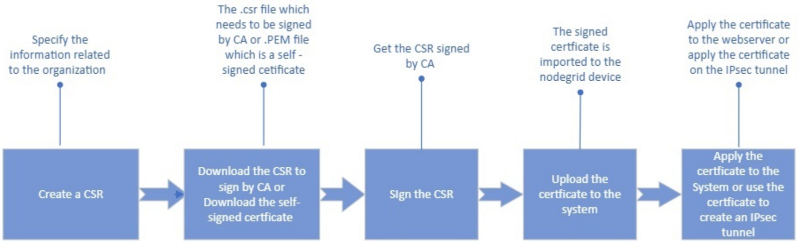
See the following sections for information on creating a new certificate, uploading a certificate, applying a certificate, and deleting a certificate.

Creating a New Certificate

You can import a certificate or generate a Certificate Signing Request (CSR) and use that certificate on the web server or an IPsec tunnel.

To create a certificate:

1. You must first create a CSR; and complete all the required information related to the certificate, including details such as Common Name, Organization, Organization Unit, and more. For more information, see the Create a CSR section.
2. After creating the CSR, you can either self-sign it or send it to a Certificate Authority (CA) for signature, and the CA will then generate the certificate.
3. Once you upload the certificate to the system, you can either use it as a web server certificate or use it while creating an IPsec tunnel.


Specify the information related to the organization
The .csr file which needs to be signed by CA or .PEM file which is a self - signed cetificate
Get the CSR signed by CA
The signed certficate is imported to the nodegrid device
Apply the certificate to the webserver or apply the certificate on the IPsec tunnel
Create a CSR
Download the CSR to sign by CA or Download the self-signed certficate
SIgn the CSR
Upload the certficate to the system
Apply the certficate to the System or use the certficate to create an IPsec tunnel

Create a CSR

You can either generate a CSR and get it signed by a Certificate Authority or self-sign it.

To create a CSR:

1. Go to *Security :: Certificates*.
2. Click **Create CSR**.
3. To generate a CSR to be signed by a CA:
   a. Enter the details.

      > DO NOT check the Self-signed field.

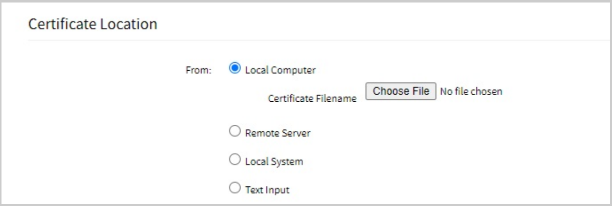
   b. Click **Generate CSR**. Download the CSR and send it to a CA.
   c. To download the CSR, go to the Certificate table, and click the CSR name link.
   d. Click **Download**.
4. To generate a self-signed certificate for the webserver:
   a. Select the Self-Sign Certificate field.
   b. Specify the Certificate validity in days.
   c. Select the Self-Sign Certificate field.
   d. Click **Generate CSR**. A self-signed certificate is listed in the Certificate tab.
5. To generate a self-signed certificate for the IPsec tunnel:
   a. Specify the Certificate validity in days.
   b. Select the User SSL Certificate Trust Attribute field.
      i. Trusted Peer (P): Select this field if the Nodegrid device can act as a trusted peer and be used in the authentication phase in an IPsec network.
      ii. In the case of self-signed certificates, where there's no external CA involved, these attributes are used to establish trust within the IPsec network.
         α. Trusted CA to issue client certificates (T): This attribute ensures that the self-signed CA certificate is trusted to issue client certificates. Select the field to allow the IPsec to be validated against this CA certificate to prove their identity and securely gain access to the IPsec network.
         β. Trusted CA to issue server certificates (C): This attribute ensures that the self-signed CA certificate is trusted to issue server certificates. Select the field to allow the IPsec servers to validate against this CA certificate to prove their identity and securely gain access to the IPsec.
6. Click **Generate CSR**.
7. A self-signed certificate is generated and listed under the Certificates tab.

Uploading a Certificate

You can use this option to upload certificates generated in a Nodegrid device or certificates generated outside Nodegrid device.

To upload a signed certificate to the Nodegrid device:

1. Go to **Security** :: **Certificates**.
2. Click **Upload Certificate**.
3. When you upload a certificate to use for IPsec, select the **User SSL Certificate Trust Attribute** field.
   a. **Trusted Peer (P)**: Select this field if the Nodegrid device can act as a trusted peer and be used in the authentication phase in an IPsec network.
   b. In the case of self-signed certificates, where there's no external CA involved, these attributes are used to establish trust within the IPsec network.
      α. **Trusted CA to issue client certificates (T)**: This attribute ensures that the self-signed CA certificate is trusted to issue client certificates. Select the field to allow the IPsec to be validated against this CA certificate to prove their identity and securely gain access to the IPsec network.
      β. **Trusted CA to issue server certificates (C)**: This attribute ensures that the self-signed CA certificate is trusted to issue server certificates. Select the field to allow the IPsec servers to validate against this CA certificate to prove their identity and securely gain access to the IPsec.
4. **Certificate Location**: This section allows you to upload the certificate using either of the following options:
   a. **Local Computer**: Select this option if the certificate is available on your system locally.



Certificate Location

From: ● Local Computer

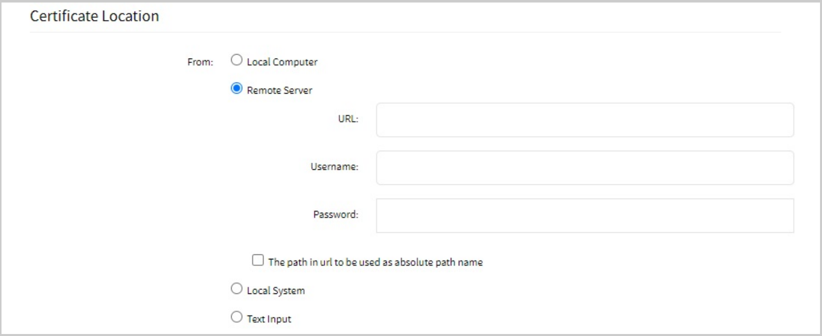
Certificate Filename [Choose File] No file chosen

○ Remote Server

○ Local System

○ Text Input

   b. **Remote Server**: Select this option if the certificate is available on the remote server. Enter the URL, Username, and Password to connect to the remote server.



Certificate Location

From: ○ Local Computer

● Remote Server

URL:

Username:

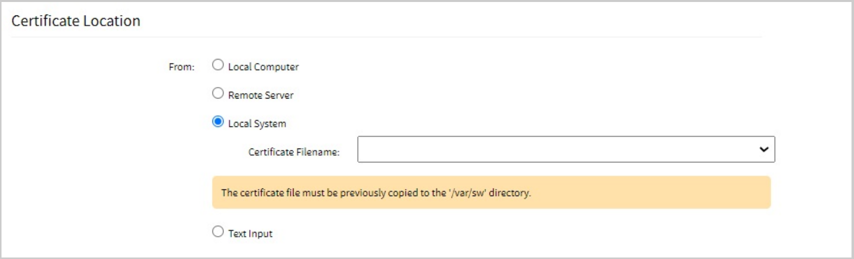
Password:

□ The path in url to be used as absolute path name

○ Local System

○ Text Input

   c. **The path in the URL to be used as the absolute path name**: The path on the remote server is an absolute path instead of a relative path. Absolute paths always start with the root directory and provide the full path to the file or directory.
   d. **Local System**: Uses certificate files stored on /var/sw on Nodegrid device.



Certificate Location

From: ○ Local Computer

○ Remote Server

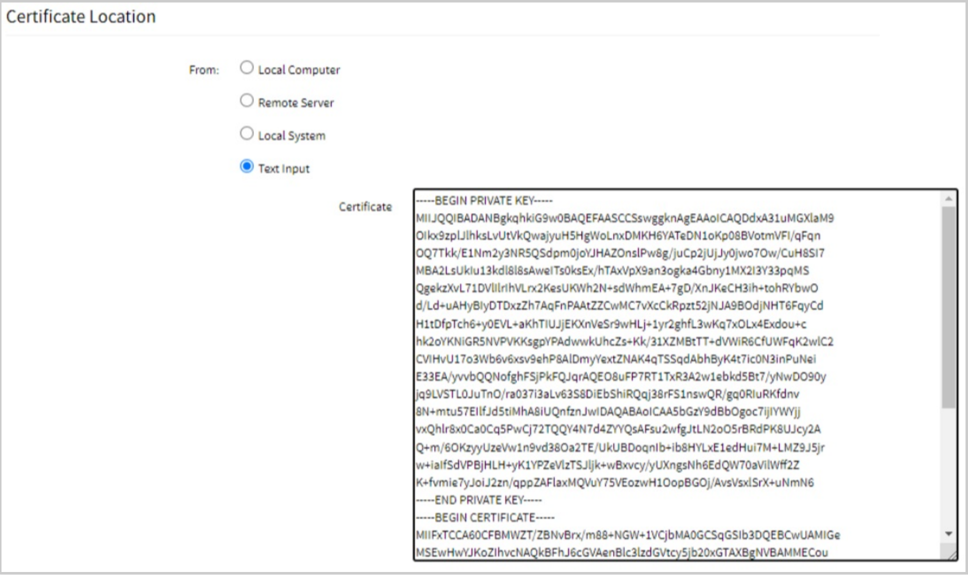
● Local System

Certificate Filename:

The certificate file must be previously copied to the '/var/sw' directory.

○ Text Input

   e. **Text input**: Paste the content of the certificate here instead of uploading a file.



Certificate Location

From: ○ Local Computer

○ Remote Server

○ Local System

● Text Input

Certificate

```
-----BEGIN PRIVATE KEY-----
MIIJQQIBADANBgkqhkiG9w0BAQEFAASCCSswggknAgEAAoICAQDdxA31uMGXlaM9
OIkx9zplJlhksLvUtVkQwajyuH5HgWoLnxDMKH6YATeDN1oKp08BVotmVFI/qFqn
OQ7Tkk/E1Nm2y3NR5QSdpm0joYJHAZOnslPw8g/juCp2jUjJy0jwo7Ow/CuH8SI7
MBA2LsUklu13kdl8l8sAweITs0ksEx/hTAxVpX9an3ogka4Gbny1MX2I3Y33pqMS
QgekzXvL71DVlIlrIhVLrx2KesUKWh2N+sdWhmEA+7gD/XnJKeCH3ih+tohRYbwO
d/Ld+uAHyBIyDTDxzZh7AqFnPAAtZZCwMC7vXcCkRpzt52jNJA9BOdjNHT6FqyCd
H1tDfpTch6+y0EVL+aKhTIUJjEKXnVeSr9wHLj+1yr2ghfL3wKq7xOLx4Exdou+c
hk2oYKNiGR5NVPVKKsgpYPAdwwkUhcZs+Kk/31XZMBtTT+dVWiR6CfUWFqK2wlC2
CVIHvU17o3Wb6v6xsv9ehP8AlDmyYextZNAK4qTSSqdAbhByK4t7ic0N3inPuNei
E33EA/yvvbQQNofghFSjPkFQJqrAQEO8uFP7RT1TxR3A2w1ebkd5Bt7/yNwDO90y
jq9LVSTL0JuTnO/ra037i3aLv63S8DiEbShiRQqj38rFS1nswQR/gq0RIuRKfdnv
8N+mtu57EIlfJd5tiMhA8iUQnfznJwIDAQABAoICAA5bGzY9dBbOgoc7ijIYWYjj
vxQhlr8x0Ca0Cq5PwCj72TQQY4N7d4ZYYQsAFsu2wfgJtLN2oO5rBRdPK8UJcy2A
Q+m/6OKzyyUzeVw1n9vd38Oa2TE/UkUBDoqnIb+ib8HYLxE1edHui7M+LMZ9J5jr
w+iaIfSdVPBjHLH+yK1YPZeVlzTSJljk+wBxvcy/yUXngsNh6EdQW70aVilWff2Z
K+fvmie7yJoiJ2zn/qppZAFlaxMQVuY75VEozwH1OopBGOj/AvsVsxlSrX+uNmN6
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIFxTCCA60CFBMWZT/ZBNvBrx/m88+NGW+1VCjbMA0GCSqGSIb3DQEBCwUAMIGe
MSEwHwYJKoZIhvcNAQkBFhJ6cGVAenBlc3lzdGVtcy5jb20xGTAXBgNVBAMMECou
```

Note: **If you are uploading a certificate whose CSR was not generated in Nodegrid, ensure that the private key of that certificate is included while uploading the certificate. This can be done by concatenating the private key with the certificate content or by using a PKCS12 file containing both the private key and the certificate.**

Certificate File Password: Some certificates are encrypted using a password, such as the PKCS12 (.p12) files. In this case, you must specify the password to decrypt the file.

5. Click **Save**.
   The certificate is successfully uploaded to the system.

Applying the Certificate

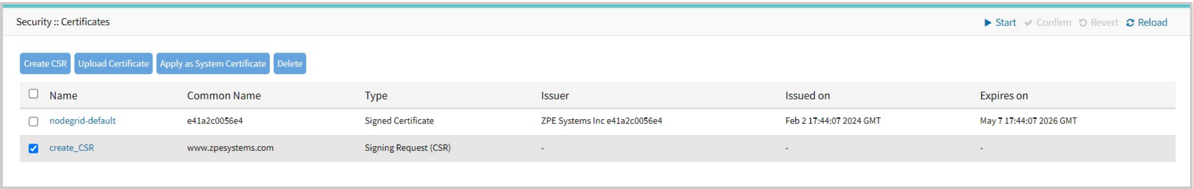
Applying the Certificate to the System or Webserver

You can use a valid certificate as the system certificate in the following cases:

- CSR was generated in Nodegrid sent to a CA, signed, and uploaded again to the device.
- CSR was generated in Nodegrid and self-signed.
- A valid certificate is uploaded to the device bundled with its private key.

To apply a certificate on the system (webserver)

1. Log in to the Nodegrid Device.
2. Go to **Systems** :: **Certificates.**
3. Select the required certificate.
4. Click **Apply as a System Certificate.**
5. Click **Finish.**
   You will be logged out of Nodegrid. Enter the credentials again and the new certificate will be applied to the system.



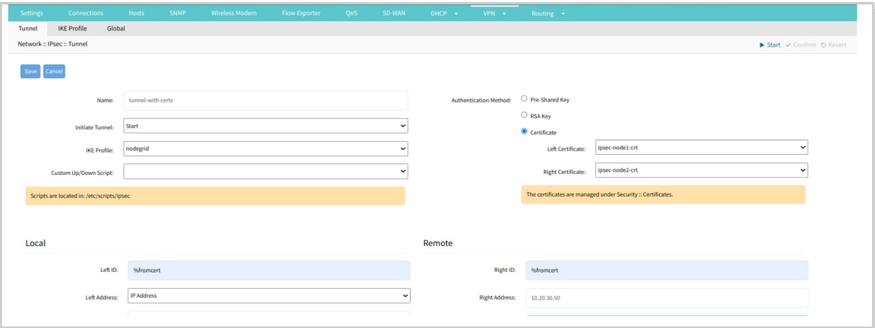
□	Name	Common Name	Type	Issuer	Issued on	Expires on
□	nodegrid-default	e41a2c0056e4	Signed Certificate	ZPE Systems Inc e41a2c0056e4	Feb 2 17:44:07 2024 GMT	May 7 17:44:07 2026 GMT
☑	create_CSR	www.zpesystems.com	Signing Request (CSR)	-	-	-

Applying the Certificate while creating an IPsec Tunnel

The certificate created in the **Certificates** tab can be used while creating an IPSec tunnel. IPsec on Nodegrid supports authentication using X.509 certificates, which is a more secure way to establish a tunnel and identify the systems participating in the tunnel.

To create an IPsec Tunnel using the Certificate:

1. Go to **Network**:: **IPsec** :: **Tunnel** table.
2. Click the **Add** button.
3. In the **Authentication** Method, select **Certificate**.
4. select the **Left** and **Right** Certificates.
5. The Local and Remote sections are populated once you upload the certificates:



Name: tunnel-with-certs

Initiate Tunnel: Start

IKE Profile: nodegrid

Custom Up/Down Script:

Scripts are located in: /etc/scripts/ipsec

Authentication Method: ○ Pre-Shared Key ○ RSA Key ● Certificate

Left Certificate: ipsec-node1-crt

Right Certificate: ipsec-node2-crt

The certificates are managed under Security :: Certificates.

Local

Left ID: %fromcert

Left Address: IP Address

Remote

Right ID: %fromcert

Right Address: 10.20.30.50

6. Click **Save**.

The certificate is used to ensure secure authentication, encrypted data transfer, and trust between VPN endpoints.

Deleting the Certificate

To delete a certificate:

1. Log in to the Nodegrid Device
2. Go to **Systems**:: **Certificates.**
3. Select the required certificate.
4. Click **Delete**.

The certificate is no longer listed on this tab.

Generating and Managing Certificates Using ACME in Nodegrid

The **Sign with ACME** feature in Nodegrid simplifies the process of obtaining and managing SSL/TLS certificates for secure network communication. By leveraging the Automatic Certificate Management Environment (ACME) protocol, this feature automates the traditionally complex task of certificate generation, validation, and renewal. Whether you're securing a website or internal network services, ACME provides an efficient and user-friendly way to ensure your communications remain encrypted and authenticated. This section walks you through using the ACME feature in Nodegrid, including handling both HTTP-01 and DNS-01 challenges, to help you maintain a secure and compliant network environment. It also provides steps if you would want to renew or revoke the certificate.

For more information, refer to the following sections:

- Signing in with ACME
- Renewing ACME Certificates
- Revoking ACME Certificates
- Troubleshooting and Logs

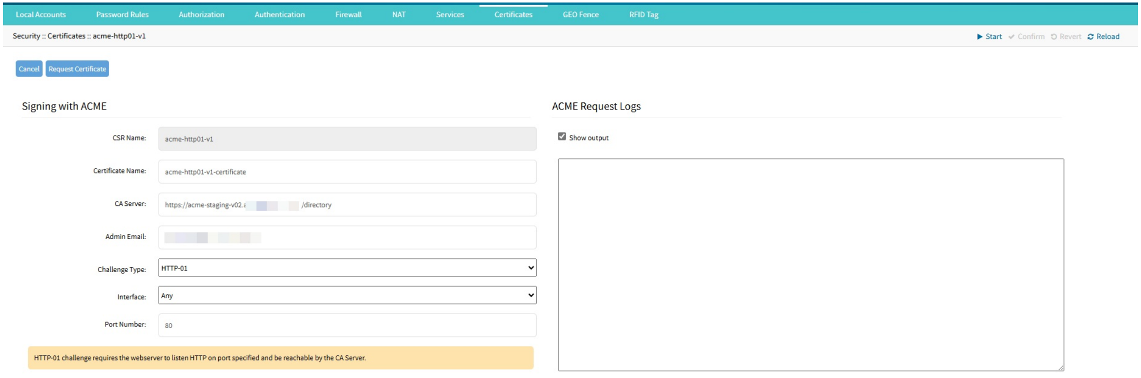
Signing in with ACME

This section outlines the steps for generating certificates using the ACME protocol in Nodegrid. The process includes creating a Certificate Signing Request (CSR), submitting it for signing through a Certificate Authority (CA), and handling the HTTP-01 and DNS-01 challenges.

Using Web UI:

Sign in with ACME (HTTP-01)

1. Log in to the Nodegrid web UI.
2. Navigate to *Security:: Certificates*.
3. Create a Certificate Signing Request (CSR).
4. Navigate to the recently created CSR.
5. Click **Sign with ACME**.
6. Enter the following fields. Some of the fields are auto-populated from the CSR.
   a. CSR Name: Auto-populated from the CSR(read-only).
   b. Certificate Name: Name of the certificate after signing in.
   c. CA Server: The Certificate Authority server URL is used for the certificate validation.
   d. Admin Email: Email address of the user to issue the certificate.
   e. Interface: The network interface on Nodegrid that CA should reach to validate the certificate.
   f. Port Number: The port number (on the specified interface) that CA should reach to validate the certificate.



Security :: Certificates :: acme-http01-v1

Signing with ACME

CSR Name: acme-http01-v1

Certificate Name: acme-http01-v1-certificate

CA Server: https://acme-staging-v02.[redacted]/directory

Admin Email: [redacted]

Challenge Type: HTTP-01

Interface: Any

Port Number: 80

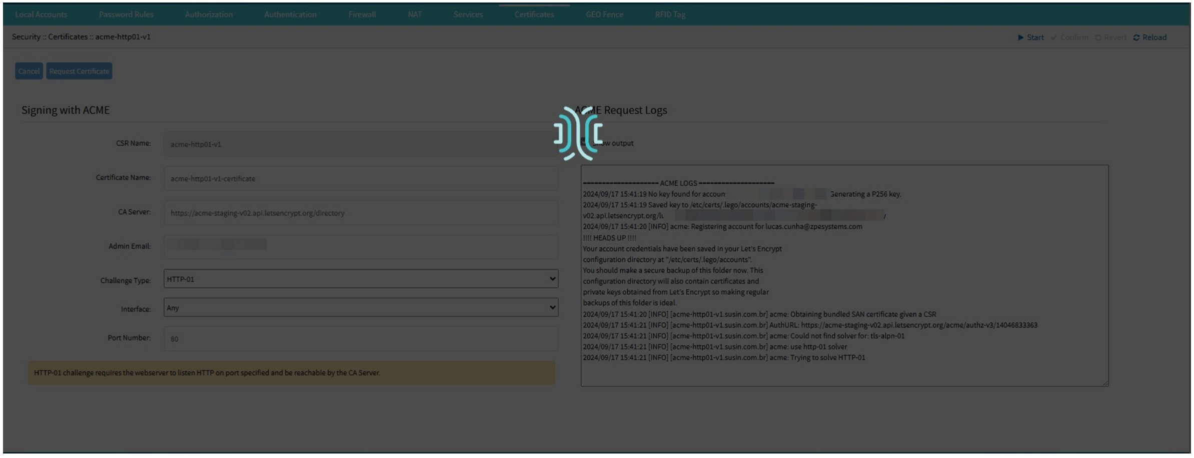
HTTP-01 challenge requires the webserver to listen HTTP on port specified and be reachable by the CA Server.

ACME Request Logs

☑ Show output

> **NOTE**
>
> Users can enable the ACME Request Logs if needed (Recommended).

7. Click **Request Certificate**. The user is redirected to the Certificates Table with the new certificate generated.



Security :: Certificates :: acme-http01-v1

Signing with ACME

CSR Name: acme-http01-v1

Certificate Name: acme-http01-v1-certificate

CA Server: https://acme-staging-v02.api.letsencrypt.org/directory

Admin Email: [redacted]

Challenge Type: HTTP-01

Interface: Any

Port Number: 80

HTTP-01 challenge requires the webserver to listen HTTP on port specified and be reachable by the CA Server.

ACME Request Logs

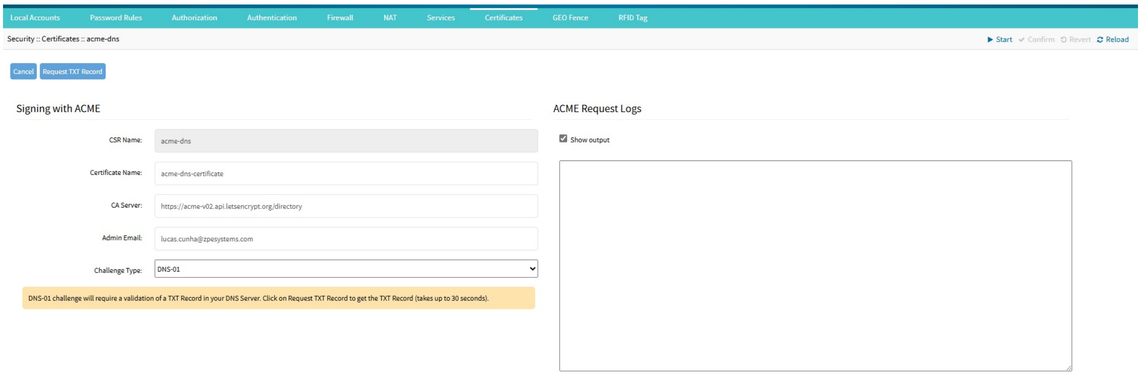
☑ Show output

```
-------------------- ACME LOGS --------------------
2024/09/17 15:41:19 No key found for accoun [redacted] Generating a P256 key.
2024/09/17 15:41:19 Saved key to /etc/certs/.lego/accounts/acme-staging-
v02.api.letsencrypt.org/lu [redacted] /
2024/09/17 15:41:20 [INFO] acme: Registering account for lucas.cunha@zpesystems.com
!!!! HEADS UP !!!!
Your account credentials have been saved in your Let's Encrypt
configuration directory at "/etc/certs/.lego/accounts".
You should make a secure backup of this folder now. This
configuration directory will also contain certificates and
private keys obtained from Let's Encrypt so making regular
backups of this folder is ideal.
2024/09/17 15:41:20 [INFO] [acme-http01-v1.susin.com.br] acme: Obtaining bundled SAN certificate given a CSR
2024/09/17 15:41:21 [INFO] [acme-http01-v1.susin.com.br] AuthURL: https://acme-staging-v02.api.letsencrypt.org/acme/authz-v3/14046833363
2024/09/17 15:41:21 [INFO] [acme-http01-v1.susin.com.br] acme: Could not find solver for: tls-alpn-01
2024/09/17 15:41:21 [INFO] [acme-http01-v1.susin.com.br] acme: use http-01 solver
2024/09/17 15:41:21 [INFO] [acme-http01-v1.susin.com.br] acme: Trying to solve HTTP-01
```

Sign in with ACME (DNS-01)

1. Log in to the Nodegrid web UI.
2. Navigate to *Security :: Certificates*.
3. Create a Certificate Signing Request (CSR).
4. Navigate to the recently created CSR.
5. Click **Sign with ACME**.
6. Enter the following fields. Some of the fields are auto-populated from the CSR.
   a. CSR Name: Auto-populated from the CSR(read-only).
   b. Certificate Name: Name of the certificate after signing in.
   c. CA Server: The Certificate Authority server URL is used for the certificate validation.

d. Admin Email: Email address of the user to issue the certificate.



Security :: Certificates :: acme-dns

Signing with ACME

CSR Name: acme-dns

Certificate Name: acme-dns-certificate

CA Server: https://acme-v02.api.letsencrypt.org/directory

Admin Email: lucas.cunha@zpesystems.com

Challenge Type: DNS-01

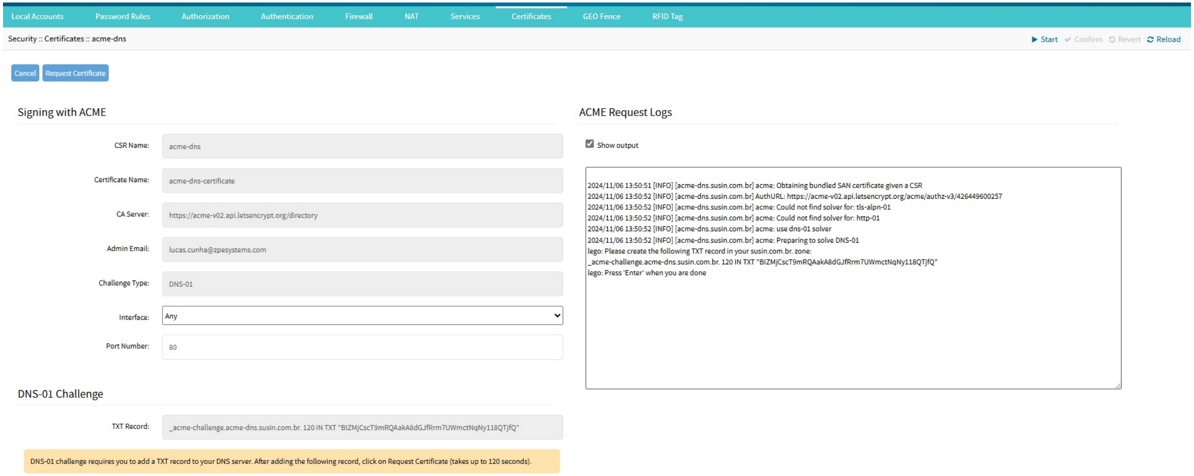
DNS-01 challenge will require a validation of a TXT Record in your DNS Server. Click on Request TXT Record to get the TXT Record (takes up to 30 seconds).

ACME Request Logs

☑ Show output

> **NOTE**
>
> Users can enable the ACME Request Logs if needed (Recommended).

7. Click on **Request TXT Record**. The page will reload with a new field named TXT Record.



Security :: Certificates :: acme-dns

Signing with ACME

CSR Name: acme-dns

Certificate Name: acme-dns-certificate

CA Server: https://acme-v02.api.letsencrypt.org/directory

Admin Email: lucas.cunha@zpesystems.com

Challenge Type: DNS-01

Interface: Any

Port Number: 80

DNS-01 Challenge

TXT Record: _acme-challenge.acme-dns.susin.com.br. 120 IN TXT "BIZMjCscT9mRQAakA8dGJfRrm7UWmctNqNy118QTjfQ"

DNS-01 challenge requires you to add a TXT record to your DNS server. After adding the following record, click on Request Certificate (takes up to 120 seconds).

ACME Request Logs

☑ Show output

```
2024/11/06 13:50:51 [INFO] [acme-dns.susin.com.br] acme: Obtaining bundled SAN certificate given a CSR
2024/11/06 13:50:52 [INFO] [acme-dns.susin.com.br] AuthURL: https://acme-v02.api.letsencrypt.org/acme/authz-v3/426449600257
2024/11/06 13:50:52 [INFO] [acme-dns.susin.com.br] acme: Could not find solver for: tls-alpn-01
2024/11/06 13:50:52 [INFO] [acme-dns.susin.com.br] acme: Could not find solver for: http-01
2024/11/06 13:50:52 [INFO] [acme-dns.susin.com.br] acme: use dns-01 solver
2024/11/06 13:50:52 [INFO] [acme-dns.susin.com.br] acme: Preparing to solve DNS-01
lego: Please create the following TXT record in your susin.com.br. zone:
_acme-challenge.acme-dns.susin.com.br. 120 IN TXT "BIZMjCscT9mRQAakA8dGJfRrm7UWmctNqNy118QTjfQ"
lego: Press 'Enter' when you are done
```

User should use the given TXT Record and paste on the DNS provider so that DNS-01 request the certificate to the CA server.

8. Once you paste the TXT Record and save it, click **Request Certificate**. The page reloads with a new field named TXT Record. Enabling the ACME Request Logs makes easier to understand on which process the ACME is running.
9. If successful, you will be redirected to the Certificates Table with the new certificate generated.

Using CLI

acme_sign (HTTP-01)

1. Access /settings/certificates:

Plaintext Copy

```
[admin@nodegrid acme-http]# cd /settings/certificates
[admin@nodegrid certificates]# show
  name                   common name                  status  type                   issuer
issued on                  expires on                 used by
  ====================  ===========================  ======  =====================
====================================================================  ========================  ========================
=========
  nodegrid-default      e41a2c00752c                  Valid   Signed Certificate     ZPE Systems Inc e41a2c00752c
Nov  1 14:55:21 2024 GMT  Feb  4 14:55:21 2027 GMT  Webserver
  acme-http             acme-http.example.com         Valid   Signing Request (CSR)  -
-                          -
```

2. Create a valid CSR (Certificate Signing Request).
3. Navigate to the recently created CSR.
4. Type acme_sign.

Plaintext Copy

```
[admin@nodegrid certificates]# cd acme-http
[admin@nodegrid acme-http]# acme_sign
```

5. Select the ACME Challenge type (default is HTTP-01) and acme_sign again.

Plaintext Copy

```
[admin@nodegrid {acme-http}]# show
challenge_type = http-01
Set the ACME challenge type before proceeding with 'next' command.
[admin@nodegrid {acme-http}]# next
```

6. Enter all the fields (some are read from the CSR):
    a. CSR Name: Auto-populated from the CSR(read-only).
    b. Certificate Name: Name of the certificate after signing in.
    c. CA Server: The Certificate Authority server URL used for the certificate validation.
    d. Admin Email: Email address of the user to issue the certificate.
    e. Interface: The network interface on Nodegrid that CA should reach to validate the certificate.
    f. Port Number: The port number (on the specified interface) that CA should reach to validate the certificate.

Plaintext Copy

```
[admin@nodegrid {acme-http}]# set certificate_name=acme-http-certificate
[admin@nodegrid {acme-http}]# show
csr name: acme-http
certificate_name = acme-http-certificate
ca_server = https://acme-staging-v02.api.letsencrypt.org/directory
admin_email = lucas.cunha@zpesystems.com
challenge type: HTTP-01
interface = any
port_number = 80
HTTP-01 challenge requires the webserver to listen HTTP on port specified and be reachable by the CA Server.
DNS-01 challenge will require a validation of a TXT Record in your DNS Server. Click on Request TXT Record to get the TXT
Record (takes up to 30 seconds).
```

7. Type request_certificate.

Plaintext Copy

```
[admin@nodegrid {acme-http}]# request_certificate
[admin@nodegrid acme-http]# cd ..
[admin@nodegrid certificates]# show
  name                   common name                  status  type                       issuer
issued on                 expires on                used by
  =====================  ===========================  ======  =========================
=====================================================================  ========================  ========================
=========
  nodegrid-default       e41a2c00752c                 Valid   Signed Certificate         ZPE Systems Inc e41a2c00752c
Nov  1 14:55:21 2024 GMT  Feb  4 14:55:21 2027 GMT  Webserver
  acme-http-certificate  acme-http.example.com        Valid   Signed Certificate (ACME)  (STAGING) Let's Encrypt (STAGING)
Counterfeit Cashew R10               Nov  6 16:01:53 2024 GMT  Feb  4 16:01:52 2025 GMT  -
  acme-http             acme-http.example.com         Valid   Signing Request (CSR)      -
-                         -
[admin@nodegrid certificates]#                                                     -                         -
-
```

acme_sign (DNS-01)

1. Access /settings/certificates.

Plaintext Copy

```
[admin@nodegrid certificates]# cd /settings/certificates
[admin@nodegrid certificates]# show
  name                   common name                  status  type                       issuer
issued on                 expires on                used by
  =====================  ===========================  ======  =========================
=====================================================================  ========================  ========================
=========
  nodegrid-default       e41a2c00752c                 Valid   Signed Certificate         ZPE Systems Inc e41a2c00752c
Nov  1 14:55:21 2024 GMT  Feb  4 14:55:21 2027 GMT  Webserver
  acme-dns               acme-dns.example.com         Valid   Signing Request (CSR)      -
```

2. Create a valid CSR (Certificate Signing Request).
3. Navigate to the recently created CSR.
4. Type acme_sign.

Plaintext Copy

```
[admin@nodegrid certificates]# cd acme-dns
[admin@nodegrid acme-dns]# acme_sign
```

5. Select the ACME Challenge type (default is HTTP-01) and acme_sign again.

Plaintext Copy

```
[admin@nodegrid {acme-dns}]# show
challenge_type = http-01
Set the ACME challenge type before proceeding with 'next' command.
[admin@nodegrid {acme-dns}]# set challenge_type=dns-01
[admin@nodegrid {acme-dns}]# next
```

6. Enter all the fields (some are read from the CSR):
    a. CSR Name: Auto populated from the CSR(read-only).
    b. Certificate Name: Name of the certificate after signing in.
    c. CA Server: The Certificate Authority server URL used for the certificate validation.
    d. Admin Email: Email address of the user to issue the certificate.

Plaintext Copy

```
[admin@nodegrid {acme-dns}]# set certificate_name=acme-dns-certificate
[admin@nodegrid {acme-dns}]# show
csr name: acme-dns
certificate_name = acme-dns-certificate
ca_server = https://acme-staging-v02.api.letsencrypt.org/directory
admin_email = lucas.cunha@zpesystems.com
challenge type: DNS-01
interface = any
port_number = 80
HTTP-01 challenge requires the webserver to listen HTTP on port specified and be reachable by the CA Server.
DNS-01 challenge will require a validation of a TXT Record in your DNS Server. Click on Request TXT Record to get the TXT
Record (takes up to 30 seconds).
```

7. Type request_certificate. The page reloads with a new field named TXT Record.

Plaintext Copy

```
[admin@nodegrid {acme-dns}]# request_txt_record
[admin@nodegrid {acme-dns}]# show
csr name: acme-dns
certificate name: acme-dns-certificate
ca server: https://acme-staging-v02.api.letsencrypt.org/directory
admin email: lucas.cunha@zpesystems.com
challenge type: DNS-01
interface = any
port_number = 80
txt record: _acme-challenge.acme-dns.example.com. 120 IN TXT "WBtpuD6iqqjXIpnHqX3yhg03QzWT66SiZ1F0zyAitmY"
DNS-01 challenge requires you to add a TXT record to your DNS server. After adding the following record, click on Request
Certificate (takes up to 120 seconds).
request log:
2024/11/06 14:08:29 [INFO] [acme-dns.example.com] acme: Obtaining bundled SAN certificate given a CSR
2024/11/06 14:08:30 [INFO] [acme-dns.example.com] AuthURL: https://acme-staging-v02.api.letsencrypt.org/acme/authz-v3/14779174313
2024/11/06 14:08:30 [INFO] [acme-dns.example.com] acme: Could not find solver for: tls-alpn-01
2024/11/06 14:08:30 [INFO] [acme-dns.example.com] acme: Could not find solver for: http-01
2024/11/06 14:08:30 [INFO] [acme-dns.example.com] acme: use dns-01 solver
2024/11/06 14:08:30 [INFO] [acme-dns.example.com] acme: Preparing to solve DNS-01
lego: Please create the following TXT record in your example.com. zone:
_acme-challenge.acme-dns.example.com. 120 IN TXT "WBtpuD6iqqjXIpnHqX3yhg03QzWT66SiZ1F0zyAitmY"
lego: Press 'Enter' when you are done
```

> NOTE
> Copy and paste the TXT Record here on the DNS provider so that the DNS-01 requests the certificate to the CA server.

> The ACME logs are activated by default in CLI. Users can however double check the ACME client logs and as well the same TXT record provided.

8. After copying and pasting the TXT Record, type **Request Certificate** again. The user is redirected to the Certificates Table with the new certificate generated.

Plaintext Copy

```
[admin@nodegrid {acme-dns}]# request_certificate
[admin@nodegrid acme-dns]# cd ..
[admin@nodegrid certificates]# show
  name                   common name                   status  type                       issuer
issued on                 expires on                used by
  =====================  ===========================  ======  =========================
=====================================================================  ========================  ========================
=========
  nodegrid-default       e41a2c00752c                 Valid   Signed Certificate         ZPE Systems Inc e41a2c00752c
Nov  1 14:55:21 2024 GMT  Feb  4 14:55:21 2027 GMT  Webserver
  acme-dns-certificate   acme-dns.example.com         Valid   Signed Certificate (ACME)  (STAGING) Let's Encrypt (STAGING)
Counterfeit Cashew R10               Nov  6 16:16:44 2024 GMT  Feb  4 16:16:43 2025 GMT  -
  acme-dns               acme-dns.example.com         Valid   Signing Request (CSR)      -
-                         -                         -
[admin@nodegrid certificates]#
```

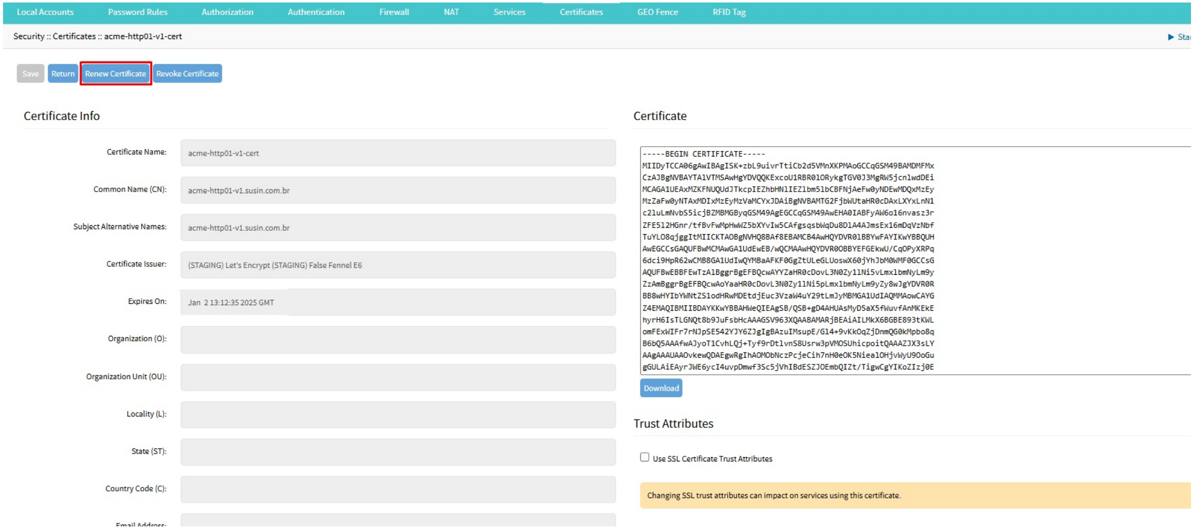
Renewing ACME Certificates

Renewing a certificate involves acquiring a new one to extend the validity of an existing certificate before it expires. This ensures that secure connections (such as HTTPS) remain uninterrupted, and the certificate continues to be trusted by browsers and systems.

Using Web UI:

To renew an ACME certificate:

1. Navigate to *Security :: Certificates*.
2. In the Certificate Table, locate the Signed Certificate (ACME) that you want to renew.
3. Verify the certificate expiry date and click **Renew Certificate**. The page gets redirected to Certificates Table where you can check the new expiry date.



Security :: Certificates :: acme-http01-v1-cert

Certificate Info

Certificate Name: acme-http01-v1-cert
Common Name (CN): acme-http01-v1.susin.com.br
Subject Alternative Names: acme-http01-v1.susin.com.br
Certificate Issuer: (STAGING) Let's Encrypt (STAGING) False Fennel E6
Expires On: Jan 2 13:12:35 2025 GMT
Organization (O):
Organization Unit (OU):
Locality (L):
State (ST):
Country Code (C):
Email Address:

Certificate

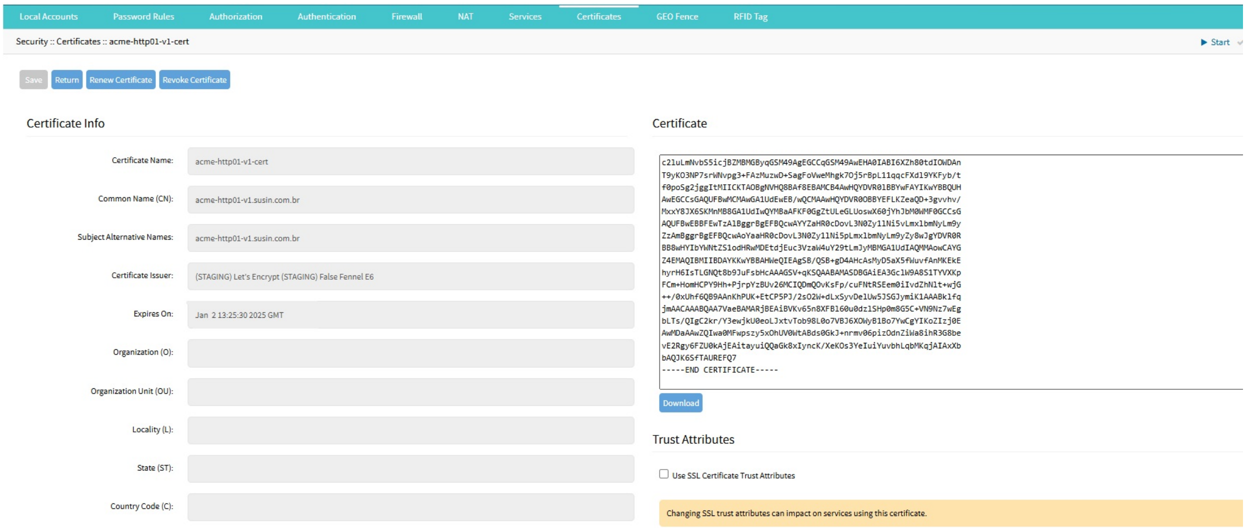
```
-----BEGIN CERTIFICATE-----
MIIDyTCCA06gAwIBAgISK+zbL9uivrTtiCb2d5VMnXKPMAoGCCqGSM49BAMDMFMx
CzAJBgNVBAYTAlVTMSAwHgYDVQQKExcoU1RBR0lORykgTGV0J3MgRW5jcnlwdDEi
MCAGA1UEAxMZKFNUQUdJTkcpIEZhbHNlIEZlbm5lbCBFNjAeFw0yNDEwMDQxMzEy
MzZaFw0yNTAxMDIxMzEyMzVaMCYxJDAiBgNVBAMTG2FjbWUtaHR0cDAxLXYxLnN1
c2luLmNvbS5icjBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABFyAW6o16nvasz3r
ZFE5l2HGnr/tfBvFwMpHwWZ5bXYvIw5CAfgsqsbWqDu8DlA4AJmsEx16mDqVzNbf
TuYLO8qjggItMIICKTAOBgNVHQ8BAf8EBAMCB4AwHQYDVR0lBBYwFAYIKwYBBQUH
AwEGCCsGAQUFBwMCMAwGA1UdEwEB/wQCMAAwHQYDVR0OBBYEFGEkwU/CqOPyXRPq
6dci9HpR62wCMB8GA1UdIwQYMBaAFKF0GgZtULeGLUoswX60jYhJbM0WMF0GCCsG
AQUFBwEBBFEwTzAlBggrBgEFBQcwAYYZaHR0cDovL3N0Zy1lNi5vLmxlbmNyLm9y
ZzAmBggrBgEFBQcwAoYaaHR0cDovL3N0Zy1lNi5pLmxlbmNyLm9yZy8wJgYDVR0R
BB8wHYIbYWNtZS1odHRwMDEtdjEuc3VzaW4uY29tLmJyMBMGA1UdIAQMMAowCAYG
Z4EMAQIBMIIBDAYKKwYBBAHWeQIEAgSB/QSB+gD4AHUAsMyD5aX5fWuvfAnMKEkE
hyrH6IsTLGNQt8b9JuFsbHcAAAGSV963XQAABAMARjBEAiAILMkX6BGBE893tKWL
omFExWIFr7rNJpSE542YJY6ZJgIgBAzuIMsupE/Gl4+9vKkOqZjDnmQG0kMpbo8q
B6bQ5AAAfwAJyoT1CvhLQj+Tyf9rDtlvnS8Usrw3pVMOSUhicpoitQAAAZJX3sLY
AAgAAAUAAOvkewQDAEgwRgIhAOMObNczPcjeCih7nH0eOK5Nieal0HjvWyU9OoGu
gGULAiEAyrJWE6ycI4uvpDmwf3Sc5jVhIBdESZJOEmbQIZt/TigwCgYIKoZIzj0E
```

Trust Attributes

□ Use SSL Certificate Trust Attributes

Changing SSL trust attributes can impact on services using this certificate.

4. Verify the new certificate expiry date.



Security :: Certificates :: acme-http01-v1-cert

Certificate Info

Certificate Name: acme-http01-v1-cert
Common Name (CN): acme-http01-v1.susin.com.br
Subject Alternative Names: acme-http01-v1.susin.com.br
Certificate Issuer: (STAGING) Let's Encrypt (STAGING) False Fennel E6
Expires On: Jan 2 13:25:30 2025 GMT
Organization (O):
Organization Unit (OU):
Locality (L):
State (ST):
Country Code (C):

Certificate

```
c2luLmNvbS5icjBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABI6XZh80tdIOWDAn
T9yKO3NP7srWNvpg3+FAzMuzwD+SagFoVweMhgk7Oj5rBpL11qqcFXdl9YKFyb/t
f0poSg2jggItMIICKTAOBgNVHQ8BAf8EBAMCB4AwHQYDVR0lBBYwFAYIKwYBBQUH
AwEGCCsGAQUFBwMCMAwGA1UdEwEB/wQCMAAwHQYDVR0OBBYEFLKZeaQD+3gvvhv/
MxxY8JX6SKMnMB8GA1UdIwQYMBaAFKF0GgZtULeGLUoswX60jYhJbM0WMF0GCCsG
AQUFBwEBBFEwTzAlBggrBgEFBQcwAYYZaHR0cDovL3N0Zy1lNi5vLmxlbmNyLm9y
ZzAmBggrBgEFBQcwAoYaaHR0cDovL3N0Zy1lNi5pLmxlbmNyLm9yZy8wJgYDVR0R
BB8wHYIbYWNtZS1odHRwMDEtdjEuc3VzaW4uY29tLmJyMBMGA1UdIAQMMAowCAYG
Z4EMAQIBMIIBDAYKKwYBBAHWeQIEAgSB/QSB+gD4AHcAsMyD5aX5fWuvfAnMKEkE
hyrH6IsTLGNQt8b9JuFsbHcAAAGSV+qKSQAABAMASDBGAiEA3GclW9A8S1TYVXKp
FCm+HomHCPY9Hh+PjrpYzBUv26MCIQDmQOvKsFp/cuFNtRSEem0iIvdZhNlt+wjG
++/0xUhf6QB9AAnKhPUK+EtCP5PJ/2sO2W+dLxSyvDelUw5JSGJymiK1AAABklfq
jmAACAAABQAA7VaeBAMARjBEAiBVKv65n8XFBl60u0dzlSHp0m8G5C+VN9Nz7wEg
bLTs/QIgC2kr/Y3ewjkU0eoLJxtvTob98L0o7VBJ6XOWyB1Bo7YwCgYIKoZIzj0E
AwMDaAAwZQIwa0MFwpszy5xOhUV0WtABds0GkJ+nrmv06pizOdnZiWa8ihR3G8be
vE2Rgy6FZU0kAjEAitayuiQQaGk8xIyncK/XeKOs3YeIuiYuvbhLqbMKqjAIAxXb
bAQJK6SfTAUREFQ7
-----END CERTIFICATE-----
```

Trust Attributes

□ Use SSL Certificate Trust Attributes

Changing SSL trust attributes can impact on services using this certificate.

Using CLI:

Run the following commands to renew an ACME certificate:

1. Access /settings/certificates:
2. Locate the Signed Certificate (ACME):

Plaintext Copy

```
[admin@ACME /]# cd /settings/certificates/
[admin@ACME certificates]# show
  name                 common name                  status  type                       issuer
issued on                 expires on                used by
  ===================  ===========================  ======  ========================
==================================================  ========================  ========================  ============
  nodegrid-default     e41a2c00752c                 Valid   Signed Certificate         ZPE Systems Inc e41a2c00752c
Sep 13 00:37:45 2024 GMT  Dec 17 00:37:45 2026 GMT  Webserver
  acme-http01-v1-cert  acme-http01-v1.example.com   Valid   Signed Certificate (ACME)  (STAGING) Let's Encrypt (STAGING) False
Fennel E6  Oct  4 13:10:12 2024 GMT  Jan  2 13:10:11 2025 GMT  -
[admin@ACME certificates]# cd acme-http01-v1-cert
```

3. Check the current Expiration Date.

Plaintext Copy

```
[admin@ACME acme-http01-v1-cert]# show
certificate name: acme-http01-v1-cert
status: Valid
common name: acme-http01-v1.example.com.br
subject alternative names: acme-http01-v1.example.com.br
certificate issuer: (STAGING) Let's Encrypt (STAGING) False Fennel E6
expires on: Jan  2 13:10:11 2025 GMT                                   <<<<<< Expiration Date
key size: 256 bit
certificate:
-----BEGIN CERTIFICATE-----
MIIDtTCCAzygAwIBAgISKxytfvHqoeskmhnEm2f5MDz8MAoGCCqGSM49BAMDMFMx
...
use_ssl_certificate_trust_attributes = no
```

4. Type renew_certificate.

Plaintext Copy

```
[admin@ACME acme-http01-v1-cert]# renew_certificate
```

5. Verify the expiry date again.

Plaintext Copy

```
 [admin@ACME acme-http01-v1-cert]# show
certificate name: acme-http01-v1-cert
status: Valid
common name: acme-http01-v1.example.com.br
subject alternative names: acme-http01-v1.example.com.br
certificate issuer: (STAGING) Let's Encrypt (STAGING) False Fennel E6
expires on: Jan  2 13:15:22 2025 GMT                                   <<<<<< Expiration Date
key size: 256 bit
certificate:
-----BEGIN CERTIFICATE-----
MIIDtTCCAzygAwIBAgISKxytfvHqoeskmhnEm2f5MDz8MAoGCCqGSM49BAMDMFMx
...
use_ssl_certificate_trust_attributes = no
```

ACME certificates can also be automatically renewed using the same credentials that were used to create the CA server. For the **Let's Encrypt** CA server, the default threshold for auto-renewal is when the certificate has 30 days remaining before expiration. In other words, if an ACME certificate has 29 days left before it expires, the auto-renew feature will automatically renew it. Other certificate authorities (CAs) may have different timeframes for their certificate renewal process. You can edit the renewal interval by navigating to *System :: Scheduler*. For more information, refer to the section Manage Scheduled Tasks.

Revoking ACME Certificates

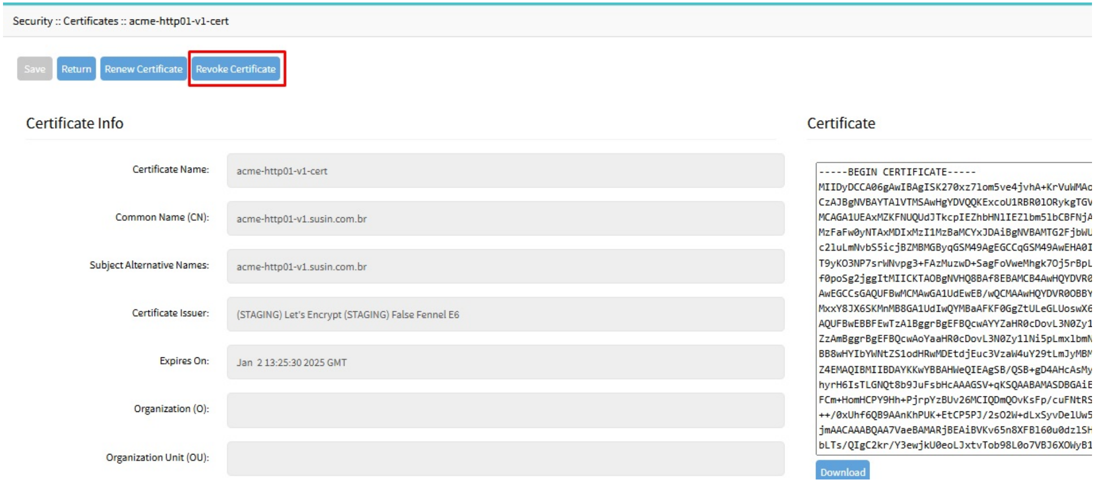
When a certificate is revoked, it is permanently invalid and cannot be reused or restored. This is a final action, usually taken because the certificate's private key has been compromised, the domain has changed ownership, or a serious security issue has occurred.

> - Signed Certificates with ACME that are being used by Webserver or IPsec cannot be Revoked.
> - Once a ACME Certificate is revoked, it cannot be renewed again. The Renew or Revoke buttons won’t show for the revoked certificate.

Using Web UI:

To revoke an ACME certificate:

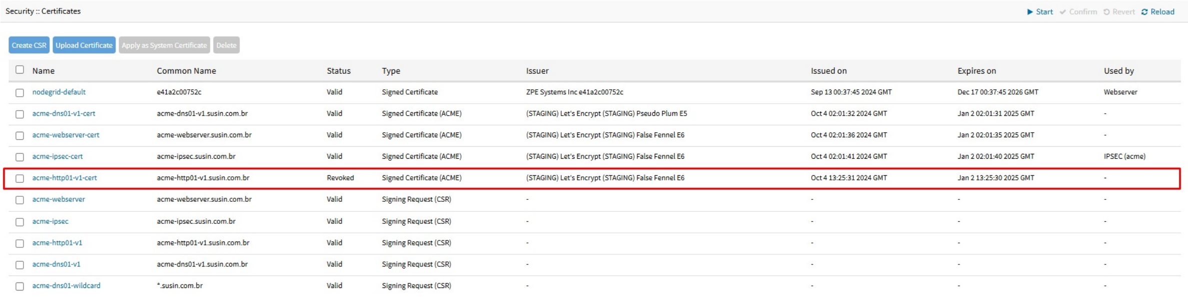
1. Navigate to *Security :: Certificates*.
2. In the Certificate Table, locate the Signed Certificate (ACME) that you want to revoke.
3. Click **Revoke Certificate**. The page gets redirected to the Certificate Table.



Certificate Name:	acme-http01-v1-cert
Common Name (CN):	acme-http01-v1.susin.com.br
Subject Alternative Names:	acme-http01-v1.susin.com.br
Certificate Issuer:	(STAGING) Let's Encrypt (STAGING) False Fennel E6
Expires On:	Jan 2 13:25:30 2025 GMT
Organization (O):	
Organization Unit (OU):	

-----BEGIN CERTIFICATE-----
MIIDyDCCA06gAwIBAgISK270xz7lom5ve4jvhA+KrVuWMAc
CzAJBgNVBAYTAlVTMSAwHgYDVQQKExcoU1RBR0lORykgTGV
MCAGA1UEAxMZKFNUQUdJTkcpIEZhbHNlIEZlbm5lbCBFNjA
MzFaFw0yNTAxMDIxMzI1MzBaMCYxJDAiBgNVBAMTG2FjbWU
c2luLmNvbS5icjBZMBMGByqGSM49AgEGCCqGSM49AwEHA0I
T9yKO3NP7srWNvpg3+FAzMuzwD+SagFoVweMhgk7Oj5rBpL
f0poSg2jggItMIICKTAOBgNVHQ8BAf8EBAMCB4AwHQYDVR0
AwEGCCsGAQUFBwMCMAwGA1UdEwEB/wQCMAAwHQYDVR0OBBY
MxxY8JX6SKMnMB8GA1UdIwQYMBaAFKF0GgZtULeGLUoswX6
AQUFBwEBBFEwTzAlBggrBgEFBQcwAYYZaHR0cDovL3N0Zy1
ZzAmBggrBgEFBQcwAoYaaHR0cDovL3N0Zy1lNi5pLmxlbmN
BB8wHYIbYWNtZS1odHRwMDEtdjEuc3VzaW4uY29tLmJyMBM
Z4EMAQIBMIIBDAYKKwYBBAHWeQIEAgSB/QSB+gD4AHcAsMy
hyrH6IsTLGNQt8b9JuFsbHcAAAGSV+qKSQAABAMASDBGAiE
FCm+HomHCPY9Hh+PjrpYzBUv26MCIQDmQOvKsFp/cuFNtRS
++/0xUhf6QB9AAnKhPUK+EtCP5PJ/2sO2W+dLxSyvDelUw5
jmAACAAABQAA7VaeBAMARjBEAiBVKv65n8XFBl60u0dzlSH
bLTs/QIgC2kr/Y3ewjkU0eoLJxtvTob98L0o7VBJ6XOWyB1

4. Verify the updated status (Revoked) of the certificate.



□	Name	Common Name	Status	Type	Issuer	Issued on	Expires on	Used by
□	nodegrid-default	e41a2c00752c	Valid	Signed Certificate	ZPE Systems Inc e41a2c00752c	Sep 13 00:37:45 2024 GMT	Dec 17 00:37:45 2026 GMT	Webserver
□	acme-dns01-v1-cert	acme-dns01-v1.susin.com.br	Valid	Signed Certificate (ACME)	(STAGING) Let's Encrypt (STAGING) Pseudo Plum E5	Oct 4 02:01:32 2024 GMT	Jan 2 02:01:31 2025 GMT	-
□	acme-webserver-cert	acme-webserver.susin.com.br	Valid	Signed Certificate (ACME)	(STAGING) Let's Encrypt (STAGING) False Fennel E6	Oct 4 02:01:36 2024 GMT	Jan 2 02:01:35 2025 GMT	-
□	acme-ipsec-cert	acme-ipsec.susin.com.br	Valid	Signed Certificate (ACME)	(STAGING) Let's Encrypt (STAGING) False Fennel E6	Oct 4 02:01:41 2024 GMT	Jan 2 02:01:40 2025 GMT	IPSEC (acme)
□	acme-http01-v1-cert	acme-http01-v1.susin.com.br	Revoked	Signed Certificate (ACME)	(STAGING) Let's Encrypt (STAGING) False Fennel E6	Oct 4 13:25:31 2024 GMT	Jan 2 13:25:30 2025 GMT	-
□	acme-webserver	acme-webserver.susin.com.br	Valid	Signing Request (CSR)	-	-	-	-
□	acme-ipsec	acme-ipsec.susin.com.br	Valid	Signing Request (CSR)	-	-	-	-
□	acme-http01-v1	acme-http01-v1.susin.com.br	Valid	Signing Request (CSR)	-	-	-	-
□	acme-dns01-v1	acme-dns01-v1.susin.com.br	Valid	Signing Request (CSR)	-	-	-	-
□	acme-dns01-wildcard	*.susin.com.br	Valid	Signing Request (CSR)	-	-	-	-

Using CLI:

Run the following commands to revoke an ACME certificate:

1. Access /settings/certificates:
2. Locate the Signed Certificate (ACME):

Plaintext

```
[admin@nodegrid acme-http]# cd /settings/certificates
[admin@nodegrid certificates]# show
  name                  common name                  status  type                   issuer
issued on                 expires on                used by
  ====================  ===========================  ======  =====================
=====================================================================  ========================  ========================
=========
  nodegrid-default      e41a2c00752c                 Valid   Signed Certificate     ZPE Systems Inc e41a2c00752c
Nov  1 14:55:21 2024 GMT  Feb  4 14:55:21 2027 GMT  Webserver
  acme-http             acme-http.example.com        Valid   Signing Request (CSR)  -
-                         -
```

3. Check the certificate status.

Plaintext Copy

```
[admin@ng-bugbuster acme-http01-v1-cert]# show
certificate name: acme-http01-v1-cert
status: Valid                                         <<<<<<<< Status
common name: acme-http01-v1.example.com.br
subject alternative names: acme-http01-v1.example.com.br
certificate issuer: (STAGING) Let's Encrypt (STAGING) False Fennel E6
issued on: Oct 29 15:48:50 2024 GMT
expires on: Jan  2 13:10:11 2025 GMT
key size: 256 bit
certificate:
-----BEGIN CERTIFICATE-----
MIIDtTCCAzygAwIBAgISKxytfvHqoeskmhnEm2f5MDz8MAoGCCqGSM49BAMDMFMx
...
-----END CERTIFICATE-----
use_ssl_certificate_trust_attributes = no
```

4. Type revoke_certificate.

Plaintext Copy

```
[admin@ACME acme-http01-v1-cert]# revoke_certificate
```

5. Verify the revoked status again

Plaintext Copy

```
[admin@ACME acme-http01-v1-cert]# show
certificate name: acme-http01-v1-cert
status: Revoked                                                       <<<<<<<< Status
common name: acme-http01-v1.example.com.br
subject alternative names: acme-http01-v1.example.com.br
certificate issuer: (STAGING) Let's Encrypt (STAGING) False Fennel E6
issued on: Oct 29 15:48:50 2024 GMT
expires on: Jan  2 13:10:11 2025 GMT
key size: 256 bit
certificate:
-----BEGIN CERTIFICATE-----
MIIDtTCCAzygAwIBAgISKxytfvHqoeskmhnEm2f5MDz8MAoGCCqGSM49BAMDMFMx
...
-----END CERTIFICATE-----
use_ssl_certificate_trust_attributes = no
```

Troubleshooting and Logs

The ACME client generates log messages when requesting, renewing, or revoking a certificate. These ACME logs typically appear in the response message (e.g., success or error notifications).

> However, the logs may not always be visible in the Nodegrid user interface. If an unknown error occurs, users may need to manually check the logs at */tmp/acme/acme-lego.log*.

It is important to carefully verify that the fields entered on the CSR and ACME signing page match those saved with the DNS provider.

Obtaining a certificate for the first time usually takes a few minutes. This process can be made fast by reducing the DNS record's Time to Live (TTL).

Viewing and Validating device identity with Platform Certificate

An X.509 certificate (platform certificate) is a digital certificate stored in a Trusted Platform Module (TPM). It is used to verify the identity of Nodegrid devices, ensuring the device's authenticity. The certificate is preinstalled on the Nodegrid device as a factory default. Users can view and validate these certificates. For more information refer to the following sections:

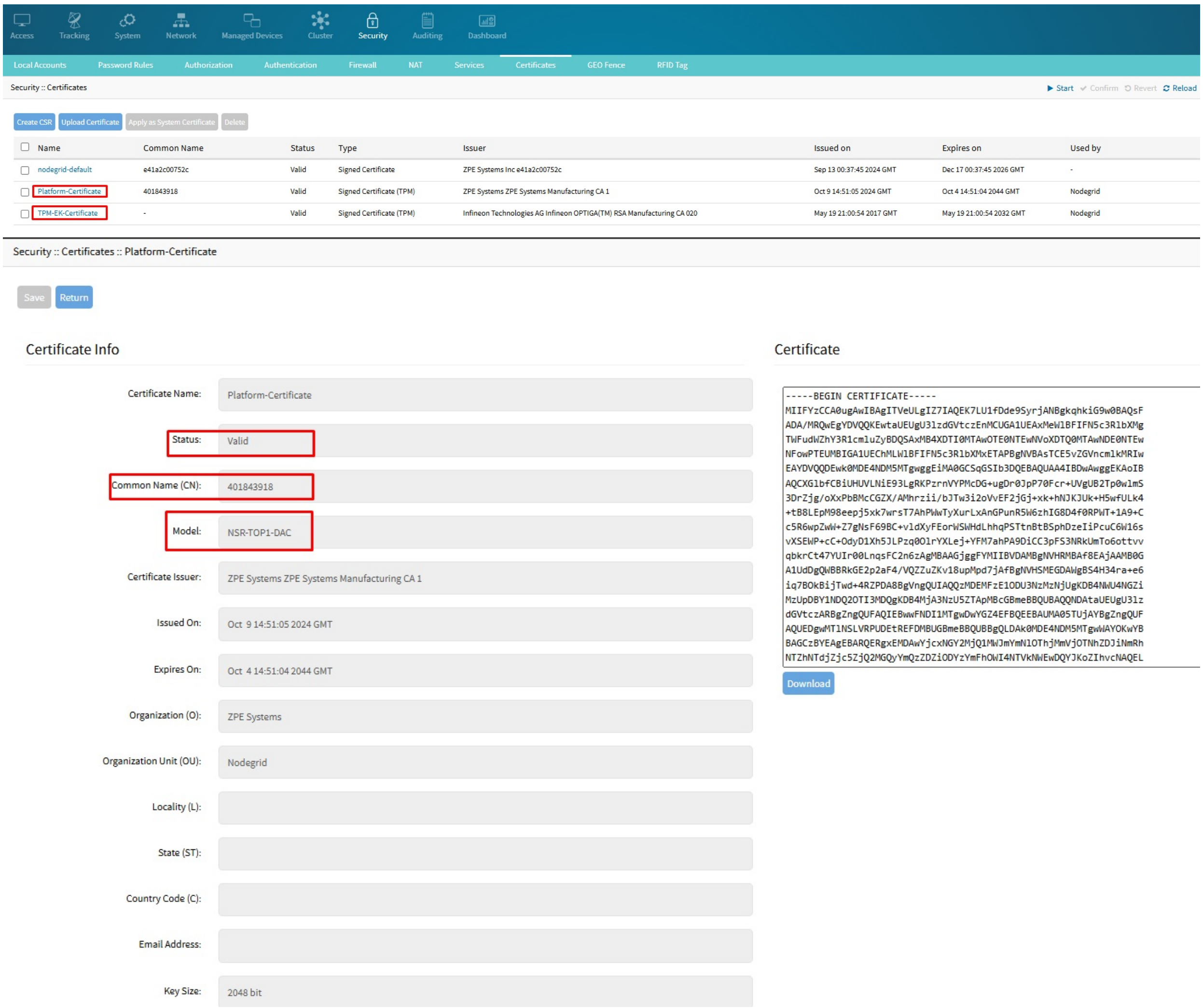
- Viewing the X.509 Certificate
- Validating the X.509 Certificate

Viewing the X.509 Certificate

Users can view Platform Certificate on the Certificates Table in a Nodegrid application. Two certificates related to the platform certificate solution are displayed:

- Platform Certificate (TPM Attestation Certificate): This certificate is created and signed by the ZPE manufacturing facility and installed in the TPM. It includes information about the EK (Endorsement Key) certificate, manufacturer name, manufacturer ID, device model, device version, device serial number, and attestation key name.
- TPM-EK Certificate (TPM Endorsement Certificate): This certificate is installed and signed by the TPM hardware vendor.

The following images display these certificates in the Certificates table within the Nodegrid Web UI.



Security :: Certificates

□	Name	Common Name	Status	Type	Issuer	Issued on	Expires on	Used by
□	nodegrid-default	e41a2c00752c	Valid	Signed Certificate	ZPE Systems Inc e41a2c00752c	Sep 13 00:37:45 2024 GMT	Dec 17 00:37:45 2026 GMT	-
□	Platform-Certificate	401843918	Valid	Signed Certificate (TPM)	ZPE Systems ZPE Systems Manufacturing CA 1	Oct 9 14:51:05 2024 GMT	Oct 4 14:51:04 2044 GMT	Nodegrid
□	TPM-EK-Certificate	-	Valid	Signed Certificate (TPM)	Infineon Technologies AG Infineon OPTIGA(TM) RSA Manufacturing CA 020	May 19 21:00:54 2017 GMT	May 19 21:00:54 2032 GMT	Nodegrid

Security :: Certificates :: Platform-Certificate

Certificate Info

Certificate Name:	Platform-Certificate
Status:	Valid
Common Name (CN):	401843918
Model:	NSR-TOP1-DAC
Certificate Issuer:	ZPE Systems ZPE Systems Manufacturing CA 1
Issued On:	Oct 9 14:51:05 2024 GMT
Expires On:	Oct 4 14:51:04 2044 GMT
Organization (O):	ZPE Systems
Organization Unit (OU):	Nodegrid
Locality (L):	
State (ST):	
Country Code (C):	
Email Address:	
Key Size:	2048 bit

Certificate

```
-----BEGIN CERTIFICATE-----
MIIFYzCCA0ugAwIBAgITVeULgIZ7IAQEK7LU1fDde9SyrjANBgkqhkiG9w0BAQsF
ADA/MRQwEgYDVQQKEwtaUEUgU3lzdGVtczEnMCUGA1UEAxMeWlBFIFN5c3RlbXMg
TWFudWZhY3R1cmluZyBDQSAxMB4XDTI0MTAwOTE0NTEwNVoXDTQ0MTAwNDE0NTEw
NFowPTEUMBIGA1UEChMLWlBFIFN5c3RlbXMxETAPBgNVBAsTCE5vZGVncmlkMRIw
EAYDVQQDEwk0MDE4NDM5MTgwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQCXGlbfCBiUHUVLNiE93LgRKPzrnVYPMcDG+ugDr0JpP70Fcr+UVgUB2Tp0wlmS
3DrZjg/oXxPbBMcCGZX/AMhrzii/bJTw3i2oVvEF2jGj+xk+hNJKJUk+H5wfULk4
+tB8LEpM98eepj5xk7wrsT7AhPWwTyXurLxAnGPunR5W6zhIG8D4f0RPWT+1A9+C
c5R6wpZwW+Z7gNsF69BC+vldXyFEorWSWHdLhhqPSTtnBtBSphDzeIiPcuC6W16s
vXSEWP+cC+OdyD1Xh5JLPzq0OlrYXLej+YFM7ahPA9DiCC3pFS3NRkUmTo6ottvv
qbkrCt47YUIr00LnqsFC2n6zAgMBAAGjggFYMIIBVDAMBgNVHRMBAf8EAjAAMB0G
A1UdDgQWBBRkGE2p2aF4/VQZZuZKv18upMpd7jAfBgNVHSMEGDAWgBS4H34ra+e6
iq7BOkBijTwd+4RZPDA8BgVngQUIAQQzMDEMFzE1ODU3NzMzNjUgKDB4NWU4NGZi
MzUpDBY1NDQ2OTI3MDQgKDB4MjA3NzU5ZTApMBcGBmeBBQUBAQQNDAtaUEUgU3lz
dGVtczARBgZngQUFAQIEBwwFNDI1MTgwDwYGZ4EFBQEEBAUMA05TUjAYBgZngQUF
AQUEDgwMT1NSLVRPUDEtREFDMBUGBmeBBQUBBgQLDAk0MDE4NDM5MTgwWAYOKwYB
BAGCzBYEAgEBARQERgxEMDAwYjcxNGY2MjQ1MWJmYmNlOThjMmVjOTNhZDJiNmRh
NTZhNTdjZjc5ZjQ2MGQyYmQzZDZiODYzYmFhOWI4NTVkNWEwDQYJKoZIhvcNAQEL
```

> The common name for a Platform Certificate is the serial number of the device.

The following commands shows an example of Platform Certificate in the Certificate table and its details:

Certificate Table:

Plaintext

Copy

```
[admin@nodegrid /]# cd /settings/certificates
[admin@nodegrid certificates]# show
  name                  common name   status  type                                     issuer                                     issued on
expires on               used by
  ====================  ============  ======  ========================================  ==========================================
========================  ========================  =========
  nodegrid-default      e41a2c00752c  Valid   Signed Certificate                        ZPE Systems Inc e41a2c00752c               Sep 13 00:37:45 2024
GMT  Dec 17 00:37:45 2026 GMT  Webserver
  Platform-Certificate  404803920     Valid   Signed Certificate (TPM)                  ZPE Systems ZPE Systems Manufacturing CA 1  Sep 13 11:09:04 2024
GMT  Sep  8 11:09:03 2044 GMT  Nodegrid
```

Platform Certificate Details:

Plaintext Copy

```
[admin@nodegrid certificates]# cd Platform-Certificate/
[admin@ACME Platform-Certificate]# show
certificate name: Platform-Certificate
status: Valid
common name: 404803920
Model: NSR-TOP1-DAC
certificate issuer: ZPE Systems ZPE Systems Manufacturing CA 1
issued on: Sep 13 11:09:04 2024 GMT
expires on: Sep  8 11:09:03 2044 GMT
organization: ZPE Systems
organization unit: Nodegrid
key size: 2048 bit
certificate:
-----BEGIN CERTIFICATE-----
MIIFYjCCA0qgAwIBAgITcBjzMqubIYPOa3dJBACNjQp3gDANBgkqhkiG9w0BAQsF
ADA/MRQwEgYDVQQKEwtaUEUgU3lzdGVtczEnMCUGA1UEAxMeWlBFIFN5c3RlbXMg
TWFudWZhY3R1cmluZyBDQSAxMB4XDTI0MDkxMzExMDkwNFoXDTQ0MDkwODExMDkw
M1owPTEUMBIGA1UEChMLWlBFIFN5c3RlbXMxETAPBgNVBAsTCE5vZGVncmlkMRIw
EAYDVQQDEwk0MDQ4MDM5MjAwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQDQ31X7PoqERIUv7FRwMLW/fE0uAmZpRVf49EVlnUw+5+Rfgc3kCmMjJA5WygvM
+Oju7FIH2+3HQj064LxuykRQGwxK0XnnA0DZJ+DyknVDOLjGjcHtIXOvOu0SCxST
KIpS+t8Pm1cNGefBXUFfbrDLHSIXrIqecWcyHuyikbT7zkb7xy/BTAMXAArJcu5n
wgpTDbwmBFZMeVvZqv/Mv84o1ZxOx0SpsuDAP23GcK2OGP/26gOQ1pZEc0khmyOb
tao4s3HFKday656KMSuea89wejladQj4wPhd4q/Dc1ETD92SOMT1LfpmfJe6t8jG
KSxsmslS3WHzpo4gCoKQ0HjhAgMBAAGjggFXMIIBUzAMBgNVHRMBAf8EAjAAMB0G
A1UdDgQWBBQJ6KcKlwwgN2gWOxikrn0/nkvwPzAfBgNVHSMEGDAWgBS4H34ra+e6
iq7BOkBijTwd+4RZPDA7BgVngQUIAQQyMDAMFTEwOTYwNDAzNyAoMHg2ODg2Y2M1
KQwXMTUyNTAwMTc3NyAoMHg1YWU1YWUzMSkwFwYGZ4EFBQEBBA0MC1pQRSBTeXN0
ZW1zMBEGBmeBBQUBAgQHDAU0MjUxODAPBgZngQUFAQQEBQwDTlNSMBgGBmeBBQUB
BQQODAxOU1ItVE9QMS1EQUMwFQYGZ4EFBQEGBAsMCTQwNDgwMzkyMDBYBg4rBgEE
AYLMFgQCAQEBFARGDEQwMDBiNzdlZDkzYThjNzc2NTQ4ZThjNTU5MmVlMjJkNDE5
ZjE5NmM4ZThmYjliM2Y1MTdlODJkNWZiMTgzMDU0NmNiZjANBgkqhkiG9w0BAQsF
AAOCAgEAdMHJt1S59Xq8JIEFtEenn78nAYTN8itwQuPkJJkv54DoIoP7qE1fBy8g
gwavDZJeQuc9fg7Xb2lFyN7yZbmGyIVsRoZ7n54/H1MDuMBFZyQtx3/lry/Rd7bj
V9PtKKpqLEFLi93mPE9xzjnu9LhnFCzA486UiZB7AQnShNKIHWZeQ0xVVIInhIV3
vKe3HfE4k2RNcmZpz9HIQ+oIreqm5qjmLIrDtuF1t51vd7MPnYtehSBXyi3g0E9L
FTUNsBTO6L65llSfXoDetLp5lCaZoBqJMsfg/oz7nv3J8ZjePBKTn9/WViAZyho+
Av7v8YsDYWTxMau9UlSnLR7eI+Xq30g43OoL1ADwBAA6XsWyML+868kW1KDf7eoO
1kIzqmI4Usnb29yrZahlqKH6Q84N7B27iS+dRezEzs2e9FsNFA9iH6QnVnSd2P6/
PgtVUNAFM+S942YX5Eg55Hx/9b8GkEIGTq6R9Bxzh7P+dX0i2bpkhi12zhAz0MXx
c388qmsMBB/OtO+VEw7VlFdVV6xWdx8KOaqwABySn8AjUB28/qLOm2gNEnpqsKNX
IABkyXuuAgcEvG8fDC1Gg2jKpReHUbwLIOWB6JxqHvOCKhkkFAzlmXNwcdUaaPU0
iUimh1BTicDjYMG2wE8loY9XeYfNItMlfsJID2qiHYdnq/UV28I=
-----END CERTIFICATE-----
```

Validating the X.509 Certificate

This section provides information on how to validate the platform certificate. Before the validation ensure that the following requirements are met:

- The commands on this guide are to be executed on a trusted Linux system that has these commands available:tpm2_makecredential, curl, jq, scp
- It assumes "nodegrid" is the hostname of the device to be attested, for example defined in /etc/hosts. "nodegrid" can be changed to the device's IP instead.
- An active Nodegrid API ticket is stored in the variable $ticket . This command can be used to get a ticket:

```bash
# Create a Nodegrid API ticket, assuming the password is in variable $NG_ADMIN_PASSWORD
ticket=$(\
  curl -s -X POST \
  https://nodegrid/api/v1/Session \
  --insecure \
  -H 'Content-Type: application/json' \
  -H 'accept: application/json' \
  -d '{"username": "admin", "password": "'"$NG_ADMIN_PASSWORD"'"}' | \
  jq -r .session \
)
```

See the following sections for information about certificate validations:

- Validate the Platform Certificate
- Validate Endorsement Key Certificate
- Validate Attestation Key name in the Platform Certificate
- Validate that TPM can use the private part of the Attestation Key to sign

How to Validate the Platform Certificate

These steps validate that the platform certificate stored in the device's TPM NVRAM was generated by ZPE Systems.

Bash Copy

```bash
# Get platform certificate from device's TPM
curl -s -X GET \
  https://nodegrid/api/v1/security/certificates/Platform-Certificate \
  --insecure \
  -H 'Content-Type: application/json' \
  -H 'accept: application/json' \
  -H "ticket: $ticket" | \
  jq -r .certificate | \
  tr -d '\r' | \
  sed '/^[[:space:]]*$/d' > device-platform-certificate.crt

# Verify which subordinated CA signed the device platform certificate
# This device CA was signed by 'ZPE Systems Manufacturing CA 1'
openssl x509 -issuer -noout -in device-platform-certificate.crt
#issuer=O = ZPE Systems, CN = ZPE Systems Manufacturing CA 1

# Download subordinated certificate from device
scp admin@nodegrid:/usr/share/ca-certificates/platform-certificate/zpe_systems_manufacturing_ca_1.crt .

# Verify that crt is unadulterated
md5sum zpe_systems_manufacturing_ca_1.crt
#f62cd72093eff2405761df7f66f6aaad  ./zpe_systems_manufacturing_ca_1.crt

# Verify which root CA signed subordinated CA
# This subordinated was signed by 'ZPE Systems Root CA 1'
openssl x509 -issuer -noout -in zpe_systems_manufacturing_ca_1.crt
#issuer=O = ZPE Systems, CN = ZPE Systems Root CA 1

# Download root certificate from device
scp admin@nodegrid:/usr/share/ca-certificates/platform-certificate/zpe_systems_root_ca_1.crt .

# Verify that root CA crt is unadulterated
md5sum zpe_systems_root_ca_1.crt
#bb48016879300c1ab97aa847f80d342e  ./zpe_systems_root_ca_1.crt

# All required certificates are now available
ls -1
#device-platform-certificate.crt
#zpe_systems_manufacturing_ca_1.crt
#zpe_systems_root_ca_1.crt

# create CA chain
cat "zpe_systems_root_ca_1.crt" > ca_chain.pem
cat "zpe_systems_manufacturing_ca_1.crt" >> ca_chain.pem

# Validate platform certificate with openssl
openssl verify --verbose -CAfile ca_chain.pem device-platform-certificate.crt
#device-platform-certificate.pem: OK
```

How to validate Endorsement Key certificate

These steps validate that the TPM's EK certificate is valid according to the TPM vendor, and extract the EK public key to later verify the Platform Certificate.

Bash Copy

```bash
# Get Endorsement Key (EK) RSA certificate from the device
curl -s -X GET \
  https://nodegrid/api/v1/security/certificates/TPM-EK-Certificate \
  --insecure \
  -H 'Content-Type: application/json' \
  -H 'accept: application/json' \
  -H "ticket: $ticket" | \
  jq -r .certificate | \
  tr -d '\r' | \
  sed '/^[[:space:]]*$/d' > ek.crt

# Verify which subordinate CA signed the EK certificate
# It was signed by 'Infineon OPTIGA(TM) RSA Manufacturing CA 042'
openssl x509 -issuer -noout -in ek.crt
#issuer=C = DE, O = Infineon Technologies AG, OU = OPTIGA(TM), CN = Infineon OPTIGA(TM) TPM 2.0 RSA CA 042

# Check URLs to download crt and crl from TPM manufacturer
openssl x509 -noout -text -in ek.crt | grep URI
#                CA Issuers - URI:http://pki.infineon.com/OptigaRsaMfrCA042/OptigaRsaMfrCA042.crt
#                  URI:http://pki.infineon.com/OptigaRsaMfrCA042/OptigaRsaMfrCA042.crl

# Download subordinated certificate and CRL from EK vendor website
# The link is present in the ek.crt file
# Note: your URL may be different from this example
curl http://pki.infineon.com/OptigaRsaMfrCA042/OptigaRsaMfrCA042.crt -o ek-subordinate.crt
curl http://pki.infineon.com/OptigaRsaMfrCA042/OptigaRsaMfrCA042.crl -o ek-subordinate.crl

# Optiga subordinate certificate and CRL are encoded in DER format
# Let's convert it to PEM encoding
openssl x509 -inform der -in ek-subordinate.crt -out ek-subordinate.pem
openssl crl -inform der -in ek-subordinate.crl -out ek-subordinate-crl.pem

# Verify which root CA signed the EK certificate
# It was signed by 'Infineon OPTIGA(TM) RSA Root CA'
openssl x509 -issuer -noout -in ek-subordinate.pem
#issuer=C = DE, O = Infineon Technologies AG, OU = OPTIGA(TM) Devices, CN = Infineon OPTIGA(TM) RSA Root CA

# Check URLs to download root CA crt and crl from TPM manufacturer
openssl x509 -noout -text -in ek-subordinate.pem | grep URI
#                CA Issuers - URI:http://pki.infineon.com/OptigaRsaRootCA/OptigaRsaRootCA.crt
#                  URI:http://pki.infineon.com/OptigaRsaRootCA/OptigaRsaRootCA.crl

# Download root certificate and CRL from EK vendor website
curl http://pki.infineon.com/OptigaRsaRootCA/OptigaRsaRootCA.crt -o ek-root.crt
curl http://pki.infineon.com/OptigaRsaRootCA/OptigaRsaRootCA.crl -o ek-root.crl

# Optiga root certificate and CRL are encoded in DER format
# Let's convert it to PEM encoding
openssl x509 -inform der -in ek-root.crt -out ek-root.pem
openssl crl -inform der -in ek-root.crl -out ek-root-crl.pem

# create CA chain
cat ek-subordinate.pem > ek-ca-chain.pem
cat ek-root.pem >> ek-ca-chain.pem

# create CRL chain
cat ek-subordinate-crl.pem > ek-crl-chain.pem
cat ek-root-crl.pem >> ek-crl-chain.pem

# Validate EK certificate chain with openssl
openssl verify --verbose -CAfile ek-ca-chain.pem -crl_check_all -CRLfile ek-crl-chain.pem ek.crt
#ek.crt: OK
```

How to validate Attestation Key name in Platform Certificate

This process uses the Endorsement Key's public key to verify that the TPM holds the attestation key, which is identified by the name in the Platform Certificate.

Bash Copy

```bash
# Extract public key from EK certificate and platform certificate
openssl x509 -pubkey -noout -in ek.crt > ek-public-key.pem
# Extract AK Name from Platform Certificate
ak_name=$(\
  openssl x509 -noout -text -in device-platform-certificate.crt | \
  grep -A 1 '1.3.6.1.4.1.42518.4.2.1.1.1.20' | tail -n 1 | \
  tr -d ' ' | sed 's/^.D//'
)

# Create a nonce (challenge)
echo "$RANDOM" > nonce.txt
# Create TPM credential using nonce as secret (challenge)
tpm2_makecredential -Q \
  -T none \
  -u ek-public-key.pem \
  -s "nonce.txt" \
  -n "$ak_name" \
  -o "credential.out" \
  -G rsa

# credential conversion to base64
credential_base64="$(cat credential.out | base64)"
# EK/TPM challenge
curl -s -X POST \
   "https://nodegrid/api/v1/system/platformcertificate/challenge" \
  --insecure \
  -H "Content-Type: text/plain" \
  -H 'accept: application/json' \
  -H "ticket: ${ticket}" \
  -d "$credential_base64" | \
  jq . > response.json

# check if replied nonce matches with nonce.txt
jq -r .data.nonce response.json | base64 -d > device-nonce.txt
cmp nonce.txt device-nonce.txt && echo "EK was successfully challenged"
#EK was successfully challenged
```

How to validate that TPM can use the private part of Attestation Key to sign

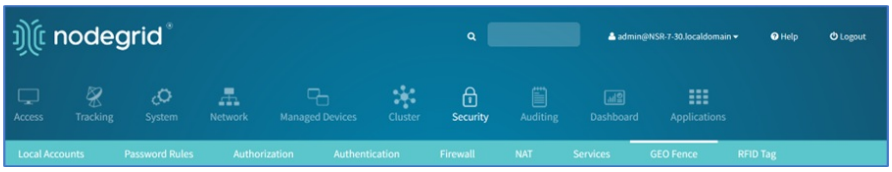
These steps validate that the TPM controls the private counterpart of the public key present in the platform certificate and can be used for signatures.

Bash Copy

```bash
# Extract the public key from the platform certificate
openssl x509 -pubkey -noout -in device-platform-certificate.crt  > ak-public-key.pem

# Nonce signed by AK was already replied in previous HTTP POST (EK/TPM challenge)
# ak_signature is replied in base64 format. Let's decode it
jq -r .data.ak_signature response.json | base64 -d > signed_ak_nonce.sig

# Verify the signature with AK public key
openssl dgst -sha256 -verify ak-public-key.pem -signature signed_ak_nonce.sig nonce.txt
#Verified OK

# Destroy NG API ticket
curl -s -X DELETE \
  https://nodegrid/api/v1/Session \
  --insecure \
  -H 'Content-Type: application/json' \
  -H 'accept: application/json' \
  -H "ticket: ${ticket}"
```

GEO Fence tab

This sets up a GEO Fence.

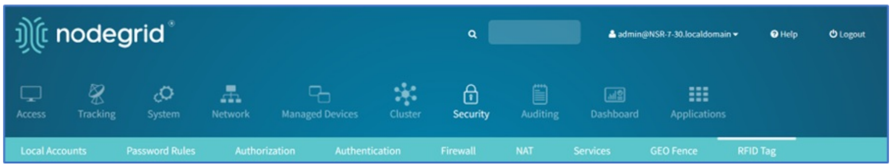


Enable GEO Fence

1. Go to *Security :: GEO Fence*.
2. Select the **Enable GEO Fence** checkbox (displays dialog).
   a. Enter the **Address Location** (a valid address for the device location).
   b. Enter **Coordinates (Lat, Lon)** (if GPS is available, click the **Compass** icon or manually enter GPS coordinates).
3. In the *Perimeter Type* menu:
   a. Select the **Circle** radio button (default).
   b. Enter **Radius (m).**
4. In the *Event Action* menu:
   a. Enter the **Number of Retries** (default: 3).
   b. Enter **Interval (sec)** (default: 60).
   c. On the **Inside Perimeter Action** drop-down, select one.
   d. On the **Outside Perimeter Action** drop-down, select one.
5. Click **Save.**

RFID Tag tab

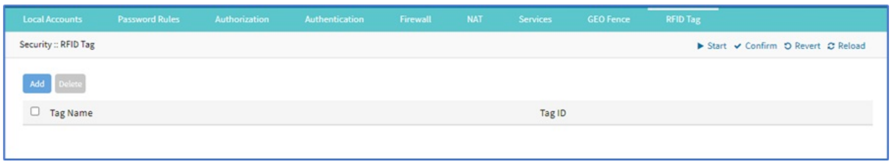
This tab lists authorized RFID Keys. Currently, these keys are linked to the RFID Door Lock. When a RIFD Reader door lock is connected to the Nodegrid device, a card with the correct RFID tag (on this list) must be inserted to unlock the door.



NOTE

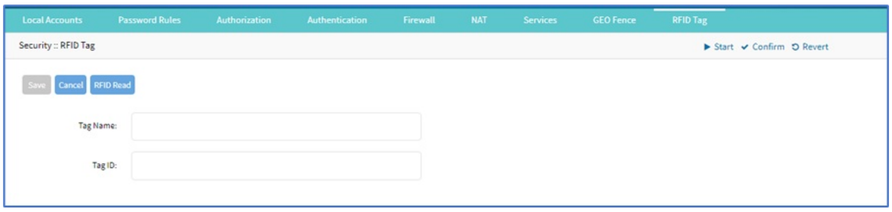
When the RIFD Reader door lock is connected to the Nodegrid device, it is automatically recognized.

Manage RFID Tag



Add RFID Tag

1. Go to *Security :: RFID Tag*.
2. Click **Add** (displays dialog).



   a. Enter **Tag Name.**
   b. Enter **Tag ID.**

3. Click **Save**.

Read RFID Tag from Card

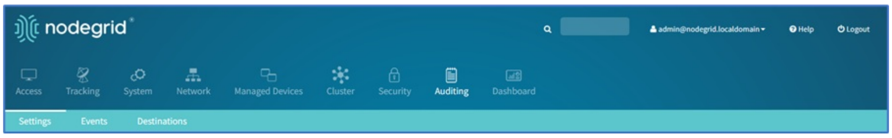
1. Go to *Security :: RFID Tag*.
2. Click **Add** (displays dialog).
3. Click **RIFD Read**.
4. Insert Card into RIFD Reader.
5. The **Tag Name** and **Tag ID** are populated.
6. Click **Save**.
7. Repeat for additional cards.

Delete RFID Tag

1. Go to *Security :: RFID Tag*.
2. Select checkbox.
3. Click **Delete**.

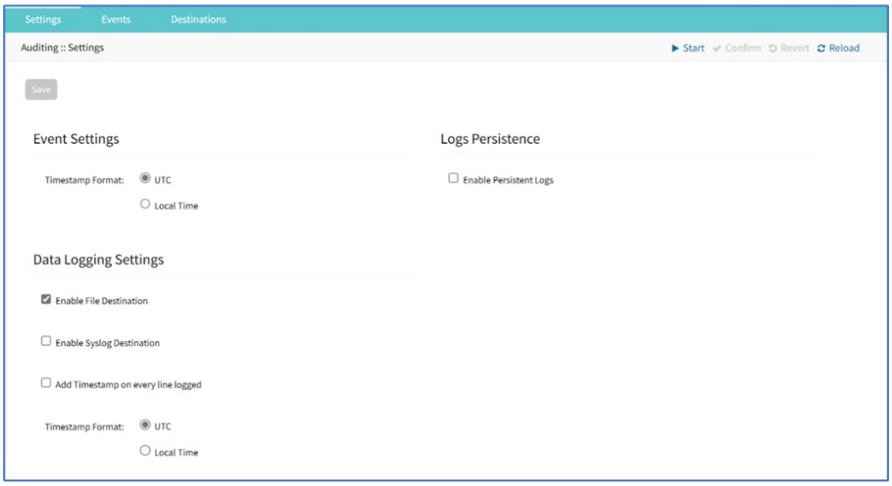
Auditing Section

This tracks events and data logging settings. Events can be distributed with four different methods: Email, File, SNMP Trap, and Syslog. Data logging and events logging can be stored locally, remotely (via NFS) or sent to a syslog server.



Settings tab

Log settings are configured here. Data logging captures the data stream on the device, as well as to and from devices.



Event Settings

Timestamp Format: ● UTC ○ Local Time

Data Logging Settings

☑ Enable File Destination

□ Enable Syslog Destination

□ Add Timestamp on every line logged

Timestamp Format: ● UTC ○ Local Time

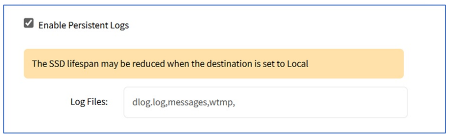
Logs Persistence

□ Enable Persistent Logs

Data Logging Settings

Update Logging Settings

1. Go to *Auditing :: Settings*.
2. On *Event Setting* menu:
   a. On **Timestamp Format**, select one:
      - **UTC** radio button (default)
      - **Local Time** radio button
3. On *Data Logging Settings* menu:
   a. Select **Enable File Destination** checkbox (if enabled, data logs stored at location defined in *Auditing :: Destination* - default: enabled).
   b. Select **Enable Syslog Destination** checkbox (if enabled, data logs stored at location defined in *Auditing :: Destination* - default: disabled).
   c. Select **Add Timestamp on every line logged** checkbox.
   d. On **Timestamp Format**, select one:
      - **UTC** radio button (default)
      - **Local Time** radio button
4. On *Logs Persistence* menu:
   a. Select **Enable Persistent Logs** checkbox (expands dialog).



☑ Enable Persistent Logs

The SSD lifespan may be reduced when the destination is set to Local

Log Files: dlog.log,messages,wtmp,

   b. **Log Files** (default values: dlog.log,messages,wtmp,), or edit, as needed.
5. Click **Save**.

Events tab

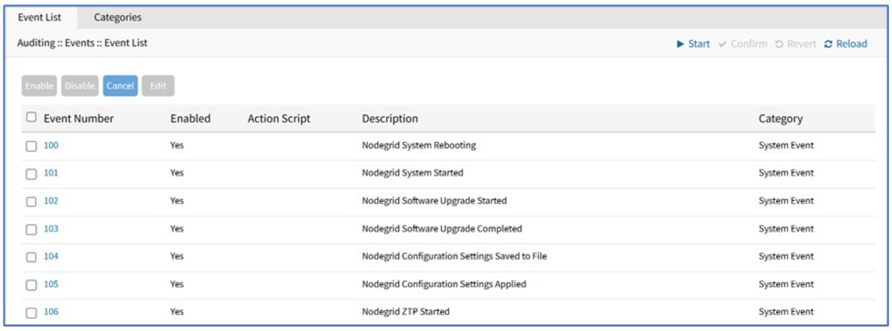
Events are automatically logged based on event and device settings. By default, all events are stored to the local file system. This behavior is adjusted under *Auditing :: Events*. The administrator can configure to which destination events and which event categories are logged.

Following are the event categories:

- Systems Events
- AAA Events
- Device Events
- Logging Events
- ZPE Cloud Events

Event List sub-tab

This is a list of events. The table lists all current event types: 100 – 527 (list can be variable).



Auditing :: Events :: Event List

□ Event Number	Enabled	Action Script	Description	Category
□ 100	Yes		Nodegrid System Rebooting	System Event
□ 101	Yes		Nodegrid System Started	System Event
□ 102	Yes		Nodegrid Software Upgrade Started	System Event
□ 103	Yes		Nodegrid Software Upgrade Completed	System Event
□ 104	Yes		Nodegrid Configuration Settings Saved to File	System Event
□ 105	Yes		Nodegrid Configuration Settings Applied	System Event
□ 106	Yes		Nodegrid ZTP Started	System Event

Enable Event

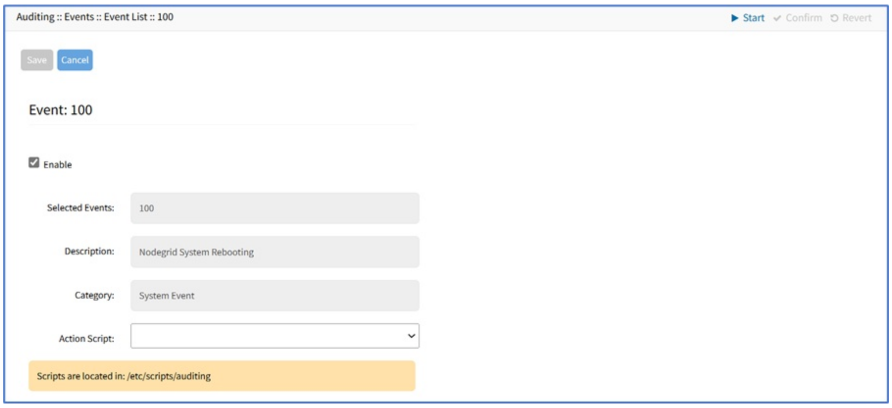
1. Go to *Auditing :: Events :: Event List*.
2. Locate and select checkbox(es).
3. Click **Enable** (enables reporting of that event type).

Disable Event

1. Go to *Auditing :: Events :: Event List*.
2. Locate and select checkbox(es).
3. Click **Disable** (disables reporting of that event type).

Edit Event

1. Go to *Auditing :: Events :: Event List*.
2. Locate and select checkbox.
3. Click **Edit** (displays dialog).



Auditing :: Events :: Event List :: 100

Event: 100

☑ Enable

Selected Events: 100

Description: Nodegrid System Rebooting

Category: System Event

Action Script:

Scripts are located in: /etc/scripts/auditing

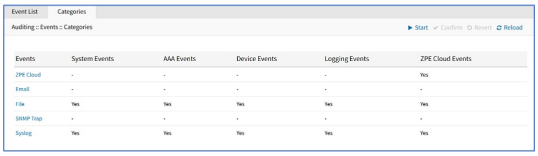
4. Select **Enable** checkbox (must be enabled to report occurrence)
5. On **Action Script** drop-down, select one (list is based on available scripts).

> **NOTE**
> If event is enabled, and an action script assigned, the script runs when the event occurs.

6. Click **Save**.

Categories sub-tab

This page shows the event category reporting. An event category groups the events occurring on a Nodegrid device. These categories are used in network monitoring. Table indicates current settings for reporting.

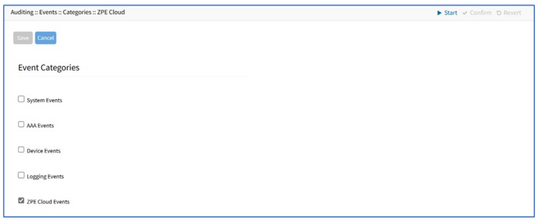


Events	System Events	AAA Events	Device Events	Logging Events	ZPE Cloud Events
ZPE Cloud	-	-	-	-	Yes
Email	-	-	-	-	-
File	Yes	Yes	Yes	Yes	Yes
SNMP Trap	-	-	-	-	-
Syslog	Yes	Yes	Yes	Yes	Yes

Set Categories for ZPE Cloud Events

The events reported in the ZPE Cloud are shown when you enable this option.

1. Go to *Auditing :: Events :: Categories*.
2. In *Events* column, click **ZPE Cloud** (displays dialog).



Event Categories

□ System Events

□ AAA Events

□ Device Events

□ Logging Events

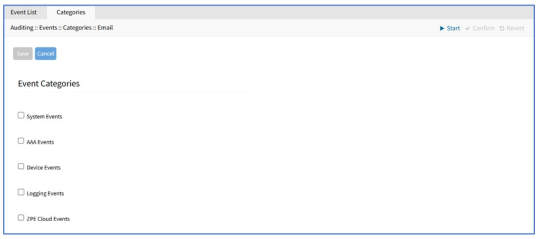
☑ ZPE Cloud Events

3. Select **ZPE Cloud Events** checkbox.
4. Select other checkboxes, as needed.
5. Click **Save**.

Set Categories for Email

When an event occurs on a device, an email is sent to the users for that specific event. To specify the event type:

1. Go to *Auditing :: Events :: Categories*.
2. In *Events* column, click **Email** (displays dialog).



Event Categories

□ System Events

□ AAA Events

□ Device Events

□ Logging Events

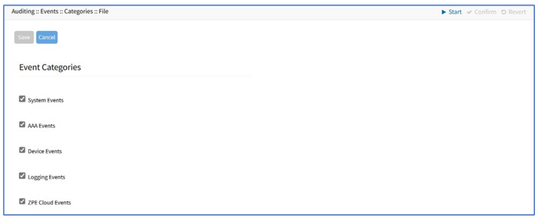
□ ZPE Cloud Events

3. Select the checkboxes, as needed.
4. Click **Save**.

Set Categories for File

You can write the event data logs to local files or to the network file system for distributed file when an event occurs on a device. To do this:

1. Go to *Auditing :: Events :: Categories*.
2. In *Events* column, click **File** (displays dialog).



Event Categories

☑ System Events

☑ AAA Events

☑ Device Events

☑ Logging Events

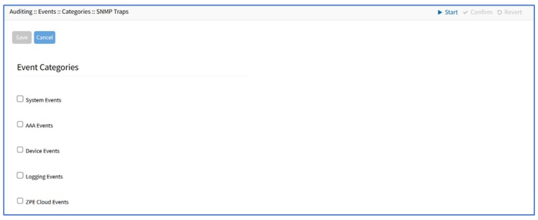
☑ ZPE Cloud Events

3. Select/unselect checkboxes, as needed.
4. Click **Save**.

Set Categories for SNMP Trap

You can send the device events via SNMP traps. To do this:

1. Go to *Auditing :: Events :: Categories*.
2. In *Events* column, click **SNMP Trap** (displays dialog).



Event Categories

□ System Events

□ AAA Events

□ Device Events

□ Logging Events

□ ZPE Cloud Events

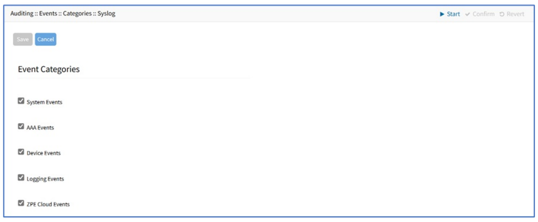
3. Select/unselect checkboxes, as needed.

4. Click **Save**.

Set Categories for Syslog

You can send the device events via system logging to the local Syslog destination or remote IPv4 and IPv6 destination. To do this:

1. Go to *Auditing :: Events :: Categories*.
2. In *Events* column, click **Syslog** (displays dialog).



☑ System Events

☑ AAA Events

☑ Device Events

☑ Logging Events

☑ ZPE Cloud Events

3. Select/unselect checkboxes, as needed.
4. Click **Save**.

Destinations tab

Event Destinations are defined here.

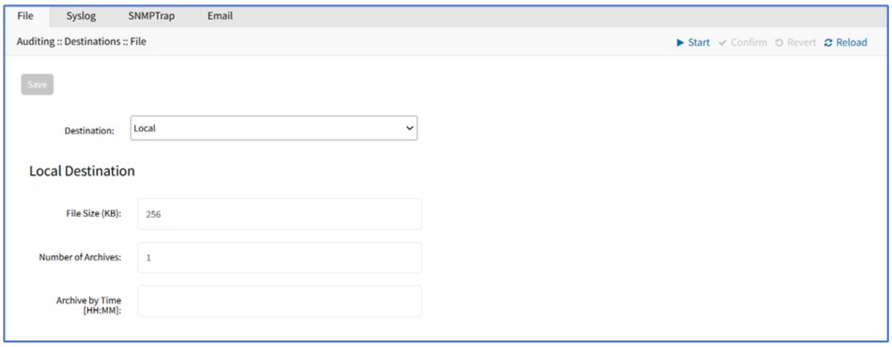
File sub-tab

File destination and archive settings are configured here. By default, data logs are written to local files.

> **NOTE**
>
> NFS requires RPC service to be enabled (*Security :: Services*).

Configure File Settings

1. Go to *Auditing :: Destinations :: File*.



Destination: Local

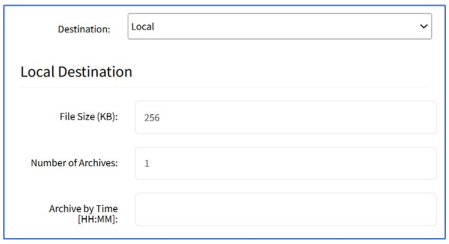
Local Destination

File Size (KB): 256

Number of Archives: 1

Archive by Time [HH:MM]:

2. On **Destination** drop-down, select **Local** (expands dialog).



Destination: Local

Local Destination

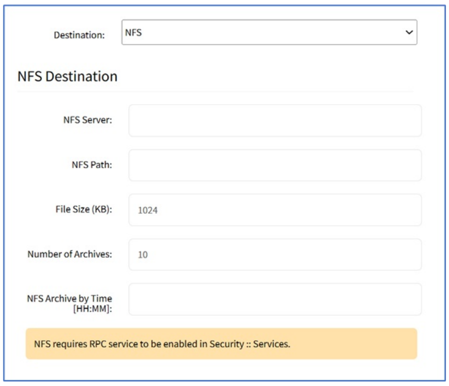
File Size (KB): 256

Number of Archives: 1

Archive by Time [HH:MM]:

   a. Enter **File Size [Kbytes]** (0=disabled, up to 2048 KB - default: 256).
   b. Enter **Number of Archives** (number of archive files before discard - default: 1, max: 9).
   c. Enter **Archive by Time [HH:MM]** (when file archive is rotated - default: blank).

3. On **Destination** drop-down, select **NFS** (expands dialog).



Destination: NFS

NFS Destination

NFS Server:

NFS Path:

File Size (KB): 1024

Number of Archives: 10

NFS Archive by Time [HH:MM]:

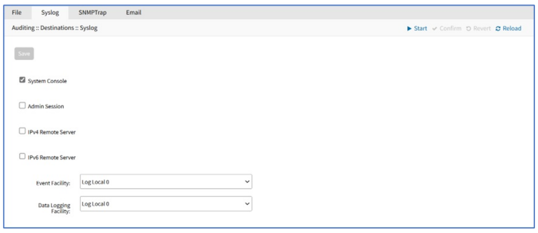
NFS requires RPC service to be enabled in Security :: Services.

   a. Enter **NFS Server** (IP address of NFS server).
   b. Enter **NFS Path** (path to NFS root directory).
   c. Enter **File Size [Kbytes]** (0=disabled, up to 2048 KB - default: 1024).
   d. Enter **Number of Archives** (number of archive files before discard - default: 10, max: 99).
   e. Enter **NFS Archive by Time [HH:MM]** (when file archive is rotated - default: blank).

4. Click **Save**.

Syslog sub-tab

Support destinations are local Syslog destination or remote IPv4 and IPv6 destination.



☑ System Console

☐ Admin Session

☐ IPv4 Remote Server

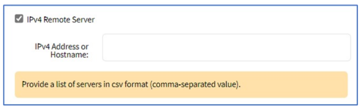
☐ IPv6 Remote Server

Event Facility: Log Local 0

Data Logging Facility: Log Local 0

Configure Syslog Settings

1. Go to *Auditing :: Destinations :: Syslog*.
2. Select **System Console** checkbox.
3. Select **Admin Session** checkbox.
4. Select **IPv4 Remote Server** checkbox. Enter **IPv4 Address or Hostname** (comma-separated list).

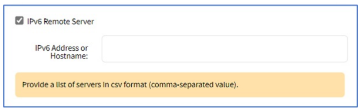


☑ IPv4 Remote Server

IPv4 Address or Hostname:

Provide a list of servers in csv format (comma-separated value).

5. Select **IPv6 Remote Server** checkbox. Enter **IPv6 Address or Hostname** (comma-separated list).



☑ IPv6 Remote Server

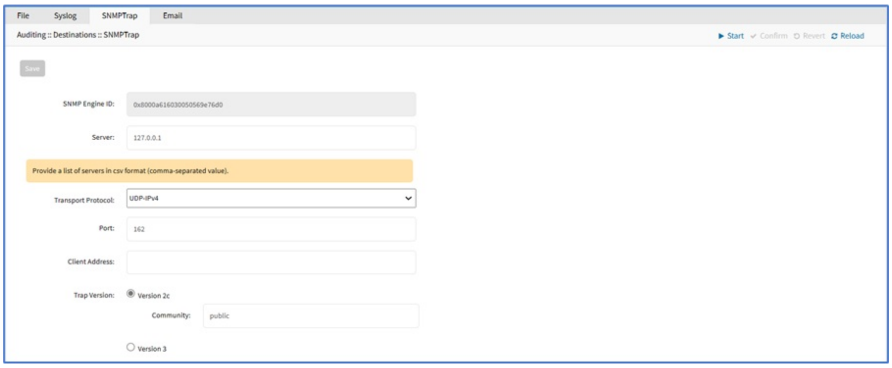
IPv6 Address or Hostname:

Provide a list of servers in csv format (comma-separated value).

6. On **Event Facility** drop-down, select one (Log Local 0, Log Local 1, Log Local 2, Log Local 3, Log Local 4, Log Local 5).
7. On **Data Logging Facility** drop-down, select one (Log Local 0, Log Local 1, Log Local 2, Log Local 3, Log Local 4, Log Local 5).
8. Click **Save**.

SNMPTrap sub-tab

Any triggered event can be sent as an SNMP trap to an existing NMS system. SNMP v2 and 3 for traps is supported. The MIB files for the device are available together with the firmware files.



SNMP Engine ID: 0x8000a616030050569e76d0

Server: 127.0.0.1

Provide a list of servers in csv format (comma-separated value).

Transport Protocol: UDP-IPv4

Port: 162

Client Address:

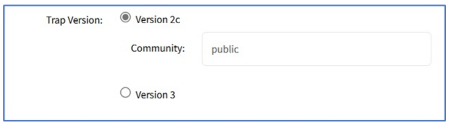
Trap Version: ● Version 2c

Community: public

○ Version 3

Configure SNMP Trap Settings

1. Go to *Auditing :: Destinations :: SNMP Trap*.
2. Enter **Server** (comma-separated list).
3. On **Transport Protocol** drop-down, select one (UDP-IPv4, TCP-IPv4, UDP-IPv6, TCP-IPv6) (protocol to send traps - default: UDP-IPv4).
4. Enter **Port** (default: 162).
5. Enter **Client Address.**
6. On *Trap Version* menu, select one:
   - **Version 2c** radio button. Enter **Community**.

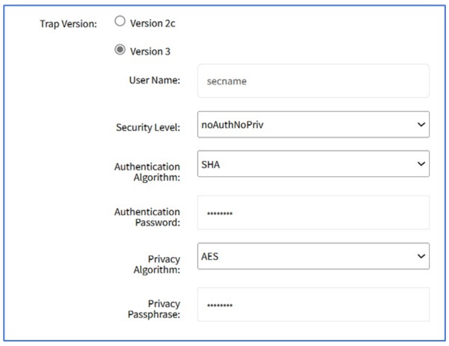
     

     Trap Version: ● Version 2c

     Community: public

     ○ Version 3

   - **Version 3** radio button (expands dialog).

     Trap Version: ○ Version 2c

     ● Version 3

     User Name: secname

     Security Level: noAuthNoPriv

     Authentication Algorithm: SHA

     Authentication Password: ••••••••

     Privacy Algorithm: AES

     Privacy Passphrase: ••••••••

     - Enter **User Name.**
     - On **Security Level** drop-down, select one (noAuthNoPriv, authNoPriv, authPriv).
     - On **Authentication Algorithm** drop-down, select one (MD5, SHA).
     - Enter **Authentication Password.**
     - On **Privacy Algorithm** drop-down, select one (DES, AES).
     - Enter **Privacy Passphrase.**
7. Click **Save**.

Access MIB files

(available in v5.6+)

CLI Procedure

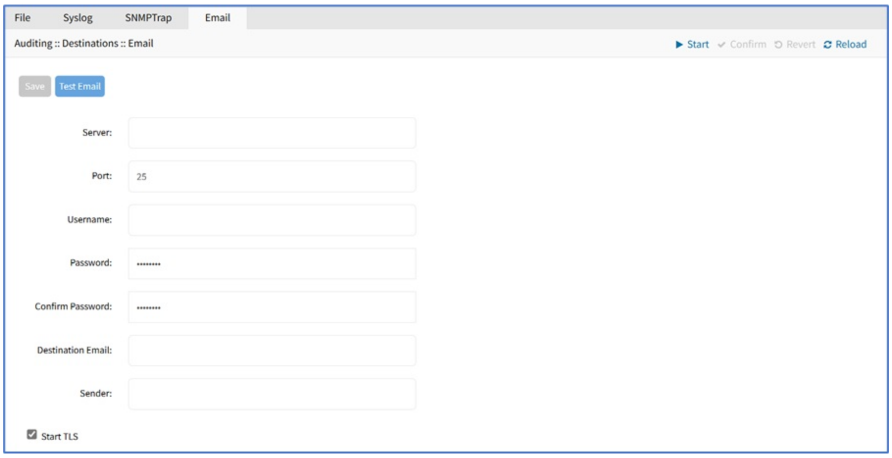
The MIB files are located as follows:

None Copy

```
root@nodegrid:~# ls -l /usr/local/mibs/
total 104
-rw-r--r-- 1 root root 36940 Nov 20  2017 NodeGrid-MIB.asn
-rw-r--r-- 1 root root 61403 Nov 20  2017 NodeGrid-TRAP-MIB.asn
-rw-r--r-- 1 root root  2732 Nov 20  2017 ZPESystems.smi
```

Email sub-tab

Events can be sent to an email address.



Auditing :: Destinations :: Email

Server:

Port: 25

Username:

Password: ••••••••

Confirm Password: ••••••••

Destination Email:

Sender:

☑ Start TLS

Configure Email Settings

1. Go to *Auditing :: Destinations :: Email*.
2. Enter **Server.**
3. Enter **Port** (default: 25).
4. Enter **Username.**
5. Enter **Password** and **Confirm Password.**
6. Enter **Destination Email.**
7. Enter **Sender.**
8. Select **Start TLS** checkbox (if TLS is used for communication).
9. Click **Save**.

Dashboard Section

(available in v5.8+)

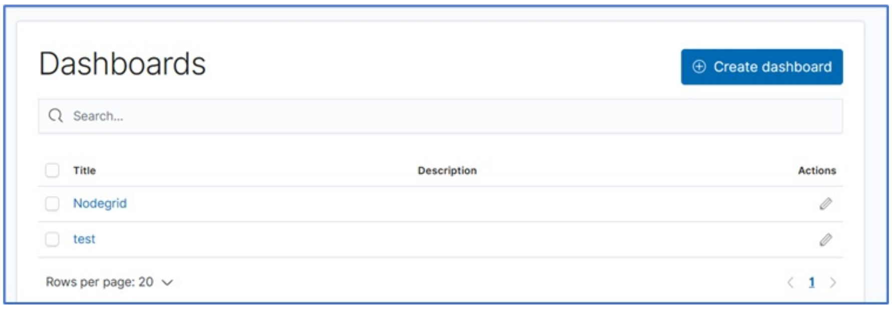
User interface updates.

The Dashboard (WebUI only) allows visual presentations of Event activities, Managed Device details, and data monitoring. Multiple dashboards can be created for different purposes. For example, one to monitor managed device data points (i.e., Power Consumption, Voltage, Current, Temperature, Fan speed, etc.) Another dashboard can monitor Nodegrid events such as authentication failures, login, and logout.

Description Details

Navigation Tabs

Navigation tabs are located on the left panel.

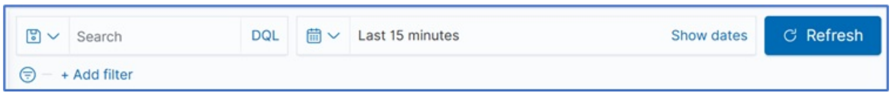


Dashboards

☐	Title	Description	Actions
☐	Nodegrid		✎
☐	test		✎

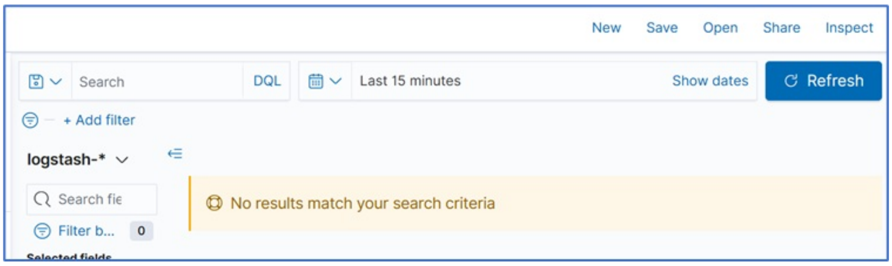
Discover Toolbar Description

Clicking on **Discover** side-tab displays this toolbar.



New

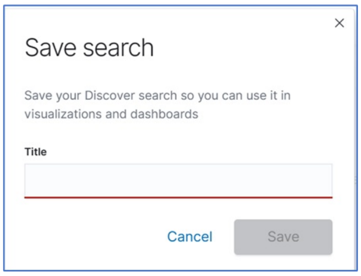
Opens a new search.



No results match your search criteria

Save

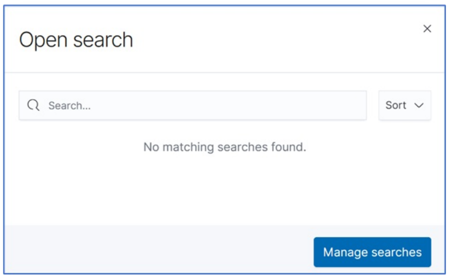
Opens dialog to save the current search. Enter **Title** and click **Save**.



Save your Discover search so you can use it in visualizations and dashboards

Open

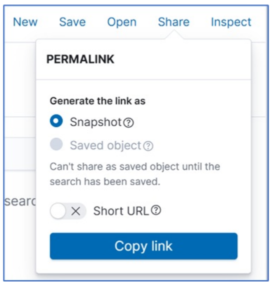
Opens a list of saved searched.



No matching searches found.

Share

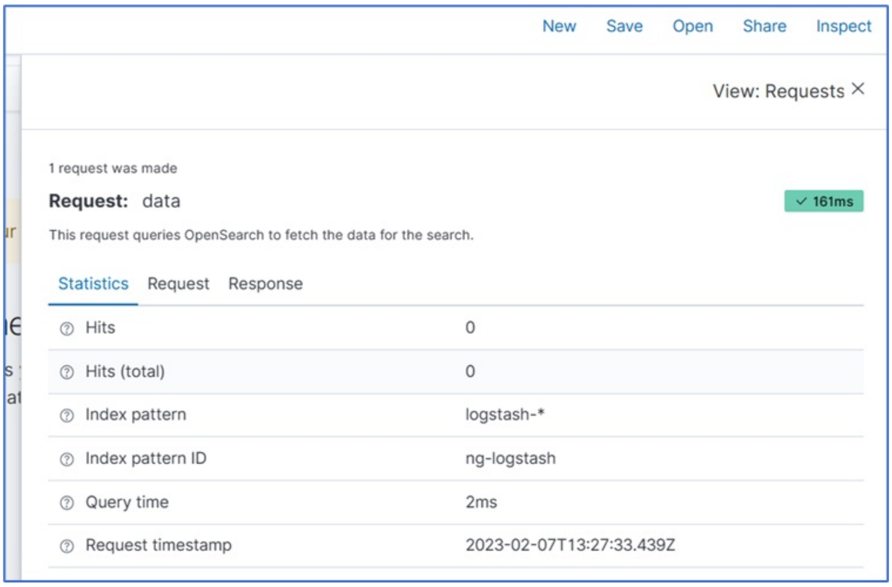
Opens dialog to share the page.



Can't share as saved object until the search has been saved.

Inspect

Opens panel with details.



1 request was made

Request: data

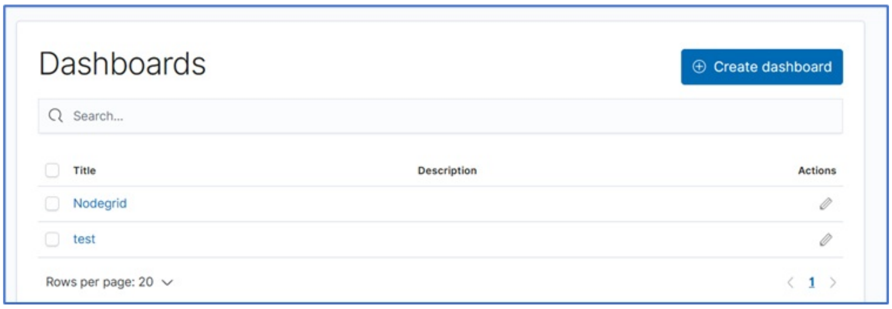
✓ 161ms

This request queries OpenSearch to fetch the data for the search.

Hits	0
Hits (total)	0
Index pattern	logstash-*
Index pattern ID	ng-logstash
Query time	2ms
Request timestamp	2023-02-07T13:27:33.439Z

Dashboards side-tab

Click on **Dashboard** side-tab.

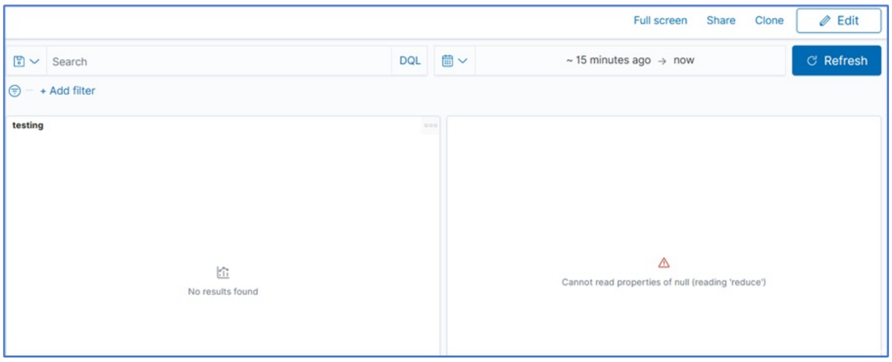


Dashboards

□ Title	Description	Actions
□ Nodegrid		
□ test		

View Dashboard

Click on a **Title** to display the Dashboard.

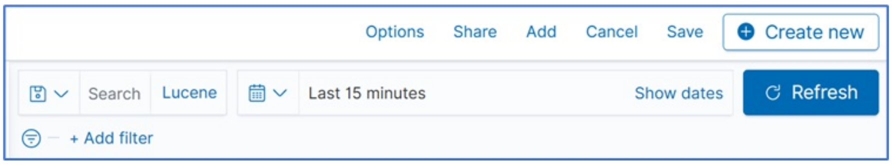


No results found

Cannot read properties of null (reading 'reduce')

Edit

Click **Edit** to display this toolbar.

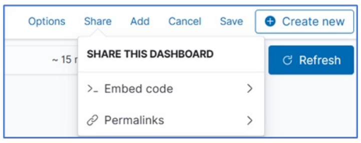


Full screen

Displays the dashboard on the full monitor width.

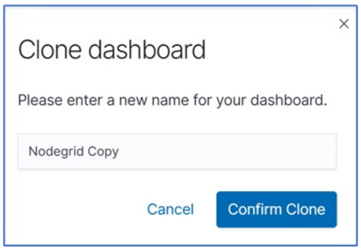
Share

Displays this pop-up dialog.



Clone

Displays *Clone dashboard* dialog. Enter new name and click **Confirm Clone**.

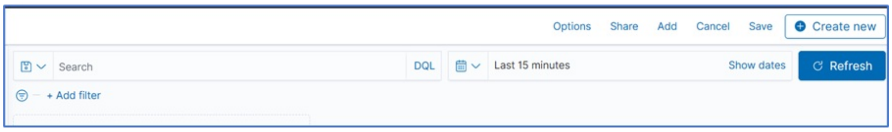


Please enter a new name for your dashboard.

Nodegrid Copy

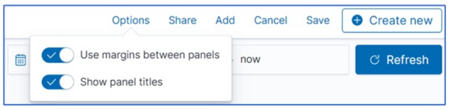
Create Dashboard

On **Dashboard** side-tab, click **Create Dashboard** to display this Toolbar.



Options

Displays this pop-up dialog.

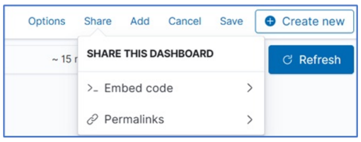


☑ Use margins between panels

☑ Show panel titles

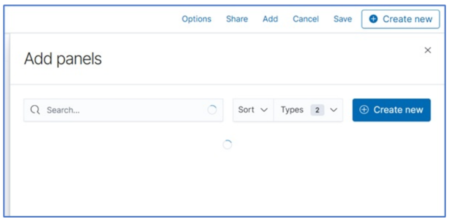
Share

Displays this pop-up dialog.



Add

Displays *Add panels* dialog.

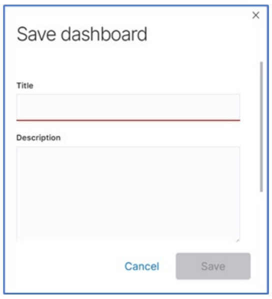


Cancel

Cancels the Create New Dashboard process.

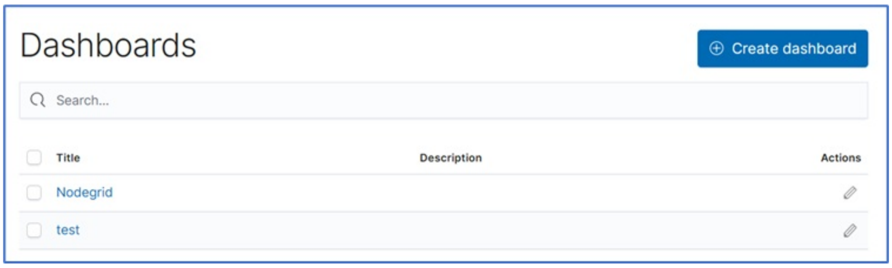
Save

Displays pop-up dialog to save dashboard. Enter **Title** and click **Save**.



Edit a Dashboard

Go to **Dashboard** side-tab, list of Dashboards. Click a pencil icon to edit that dashboard.

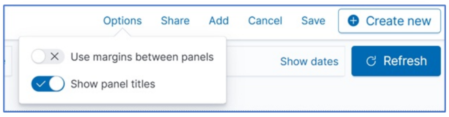


Dashboards

Title	Description	Actions
Nodegrid		
test		

Options

Provides visual display options.

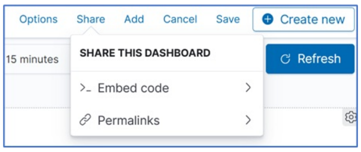


○ Use margins between panels

● Show panel titles

Share

Opens *Share* dialog options of the current saved search.



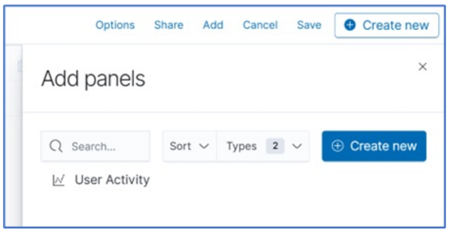
SHARE THIS DASHBOARD

Embed code

Permalinks

Add

Displays *Add Panels* dialog.

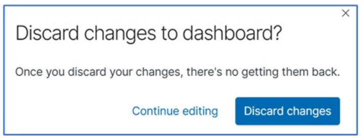


Add panels

User Activity

Cancel

Displays *Discard changes to Dashboard* dialog.

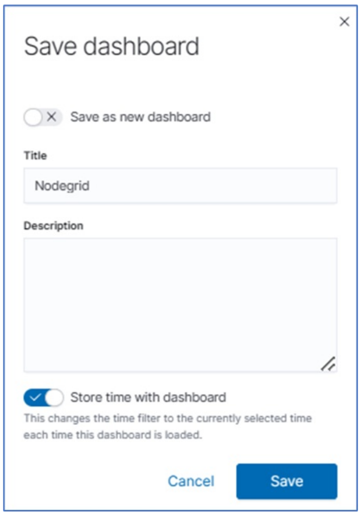


Discard changes to dashboard?

Once you discard your changes, there's no getting them back.

Save

Displays *Save dashboard* dialog.



Save dashboard

○ Save as new dashboard

Title: Nodegrid

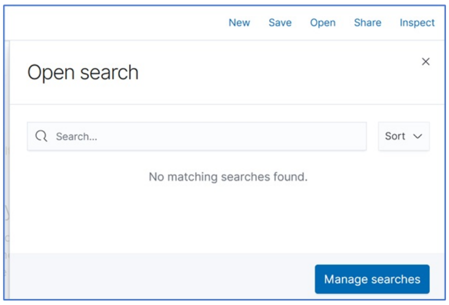
Description:

● Store time with dashboard

This changes the time filter to the currently selected time each time this dashboard is loaded.

Open

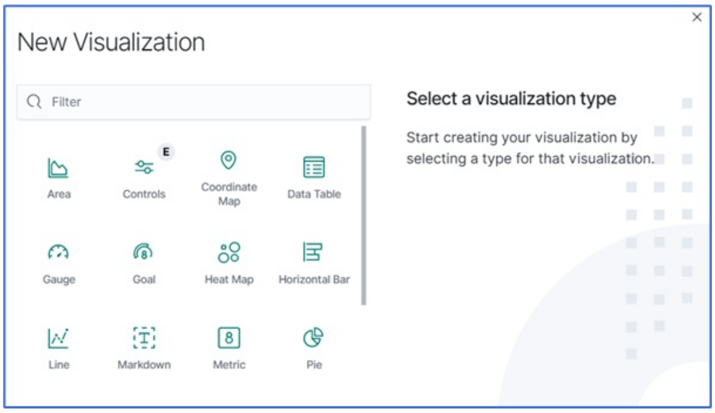
Displays *Open search* dialog.



No matching searches found.

Create New

Displays *New Visualization* dialog.



Select a visualization type

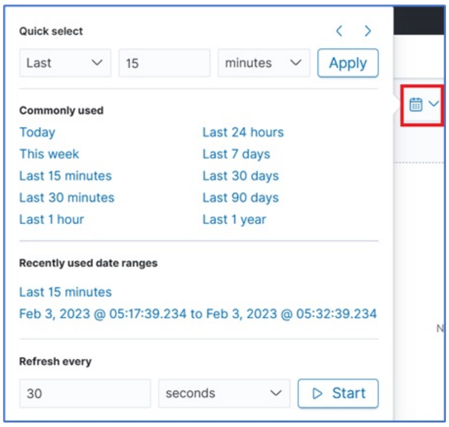
Start creating your visualization by selecting a type for that visualization.

Refresh

How often the results are checked and shown in the display.

Quick select button

Quick options to select a relative time frame to current time.



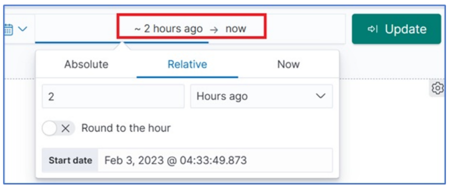
Last 15 minutes

Feb 3, 2023 @ 05:17:39.234 to Feb 3, 2023 @ 05:32:39.234

Refresh every: 30 seconds

Relative Time

Click to customize time frames of data in panels. Click **Update** when done.



2 Hours ago

Start date Feb 3, 2023 @ 04:33:49.873

Search bar

Enter search criteria to locate details. Search expressions are used to select/limit data points on the visualization. They can be used as a filter for the whole visualization, or as a filter for the whole dashboard.

Search expressions are not restricted to data point fields. An expression can also refer to fields associated with the device (type, IP address, groups, custom fields, and more). For example, to collect current from each outlet in a selection of Rack PDUs, use one custom field “rack:abc” with another custom field “rack:xyz”. Here are some search examples:

- host:"ServertechPDU"

- collectd_type:”power”
- type_instance:”AA1”
- collectd_type:”power” AND type_instance:”AA1”

Configuration Expressions of Data Points

Data Point fields (logstash-* Index)

Field	Value	Description
host	Device Name	Name of the device being monitored.
plugin	snmp, ipmi, nominal, aggregation	Name of the collection plugin.
plugin_instance	sum, average	Instance of the plugin collecting the data, if the plugin requires it. Present in the aggregation plugin.
collectd_type	temperature, fan speed, humidity, counter, percent time left, voltage, current power, apparent_power, power_factor, frequency	Type of measurement.
type_instance	Data Point Name	Name of the element associated with measurement.

Device fields (logstash-* Index)

Field	Values	Description
name	Device Name	Name of the device being monitored.
mode	enabled, on demand, disabled	Device operational mode.
type	device type	Device type (assigned under Managed Devices).
family	ilo, drac, ipmi_1.5, ilmi_2.0, cimc_ucs, device_console, pdu	Device family.
addr_location	Address	Address (street, city, country).
coordinates	Coordinates	Latitude, longitude.
ip	IP address	Device IP address.
mac	MAC address	Device MAC address (if known).
alias	IP address alias	Alias of the IP address.
groups	list of groups	Groups authorized to access the device.
licensed	yes, no	Device license state.
status	connected, disconnected, in-use, unknown	Current device status.
nodegrid	Nodegrid hostname	Device hostname that controls the device.
custom fields		Any configured custom field for the device.

Event fields (*_date_* Index)

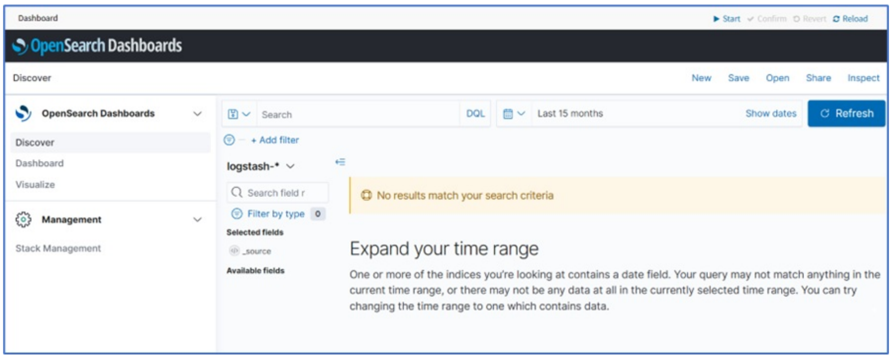
Field	Value	Description
event_id	Number	Event ID number.
event_msg	Text	Event message.
host	Nodegrid hostname	Device hostname on which the event occurred.
message	Text	Full message text.

Discover tab

This allows an inspection of the entire JSON document that was indexed.

Collect Raw Data Points

1. Go to *Dashboard :: Discover*.

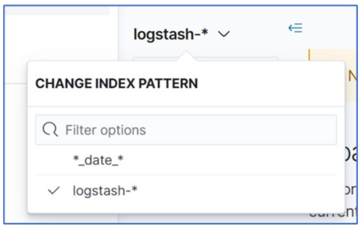


No results match your search criteria

Expand your time range

One or more of the indices you're looking at contains a date field. Your query may not match anything in the current time range, or there may not be any data at all in the currently selected time range. You can try changing the time range to one which contains data.

2. Next to the index name, click the **Down-arrow**. On the drop-down, select the *Index Pattern*:



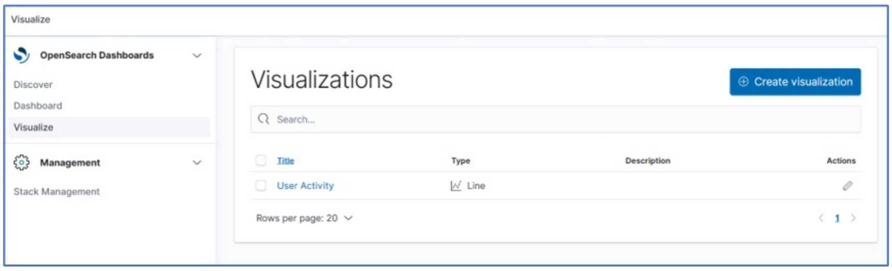
   - **logstash-*** (contains monitored data)
   - ***_date_***(contains event notifications)

3. Adjust the time frame as needed. By default, all displayed data is collected within the defined time frame.
4. Use **Search** to find a specific device or data point.
5. Verify that data points were collected.
6. Inspect the available fields.

> **NOTE**
>
> Collected data is buffered before stored. it may take up to a few minutes for data to display. If the data source produces a lot of content, buffers quickly fill up.

Visualize tab

Visualizations display aggregate data in a variety of options. Following are descriptions of data presentation.



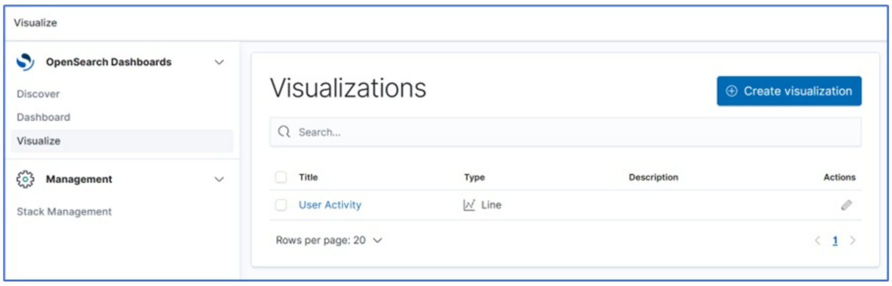
Title	Type	Description	Actions
User Activity	Line		

Line Charts

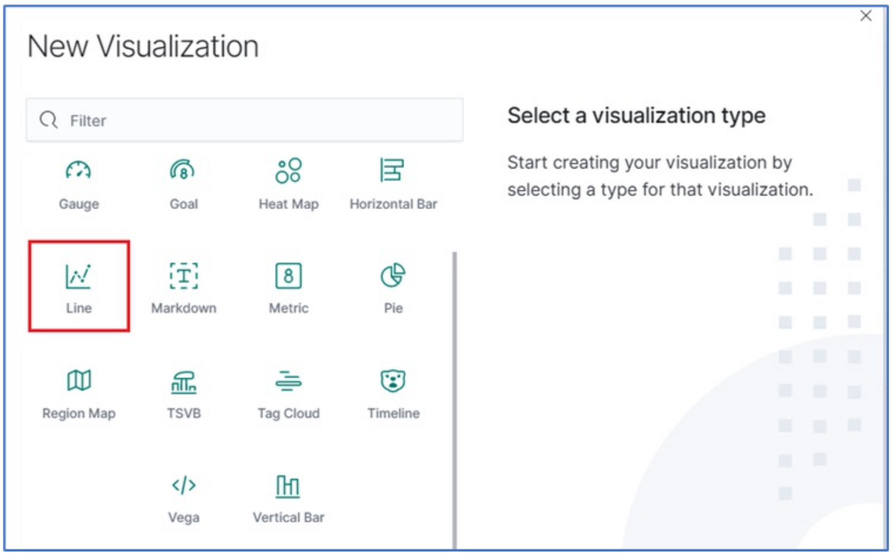
Line Charts allow the visualization of data points along the line graph.

Create a Single or Multi-Line Chart (Configuration Example)

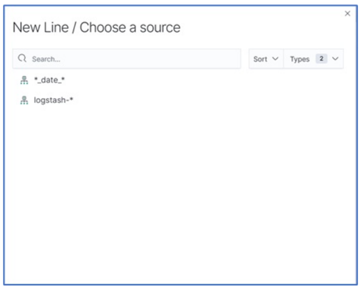
1. Go to *Dashboard :: Visualize*.
2. On the **Visualize** side-tab, click **Create Visualization**,



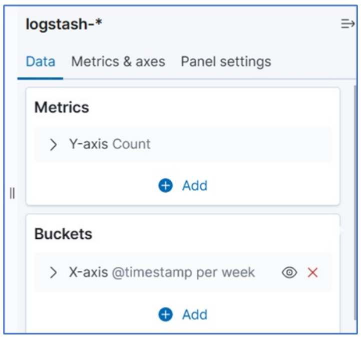
3. Click the *New Visualization* dialog, click the **Line** icon.



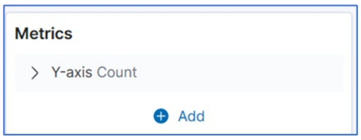
4. On the dialog, click **logstash-***.



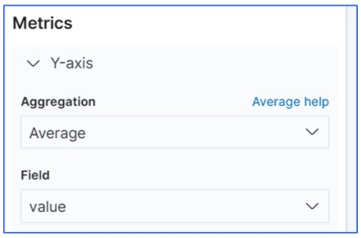
5. In the *From a New Search, Select Index* menu, click **logstash-*** (displays editor dialog).



6. In the *Metrics* section, expand the **Y-Axis** arrow.



7. On the **Aggregation** drop-down, under *Metric Aggregations* section, select **Average** . In **Field** drop-down, select **value**.



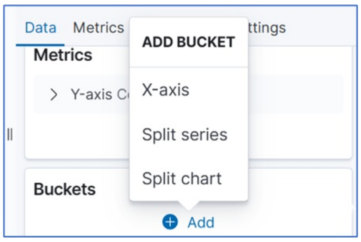
Metrics

Y-axis

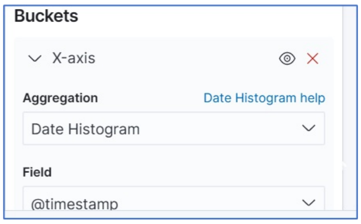
Aggregation: Average

Field: value

8. In *buckets* section, click **Add**, and click **X-Axis**.



9. On **Aggregation** drop-down, select **Date Histogram**. Accept **Field** and **Interval** defaults.



Buckets

X-axis

Aggregation: Date Histogram

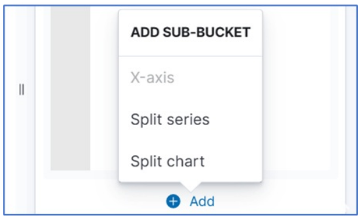
Field: @timestamp

10. On the Toolbar, click **Save**.
11. Enter a name for the visualization and click **Save**.

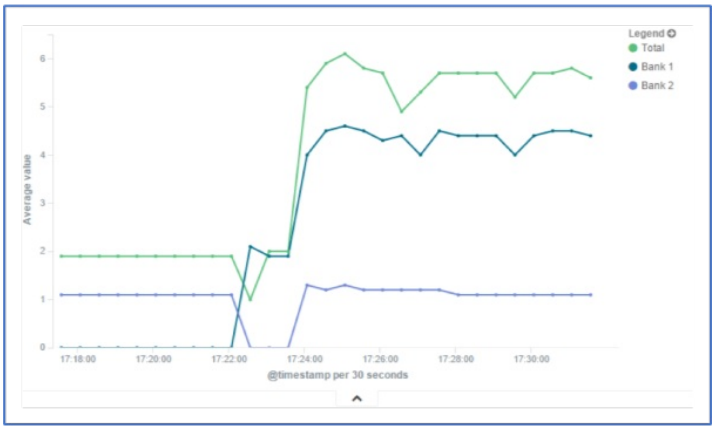
Create a Multi-Line Chart (Configuration Example)

Follow the Single-Line Chart example and continue these steps.

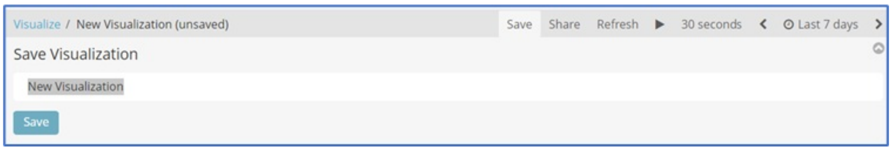
1. Below **Custom Label** field, click **+Add**. On the *Add Sub-Bucket* pop-up select **Split Series**.



2. On **Sub Aggregation** drop-down, click **Filters**.
3. In **Filter 1**, enter a search expression for the elements to visualize.
4. (optional) To associate a label, click the **Settings** icon and enter **Filter 1 label**.
5. (as needed) Click **Add Filter** and repeat.
6. (as needed) Click **Add sub-buckets** and repeat.
7. To refresh the graph, click **Refresh**. The graph example includes several sub-buckets.



8. On the Toolbar, click **Save** (displays dialog).



Visualize / New Visualization (unsaved)

Save Visualization

New Visualization

9. Enter a name for the visualization and click **Save**.

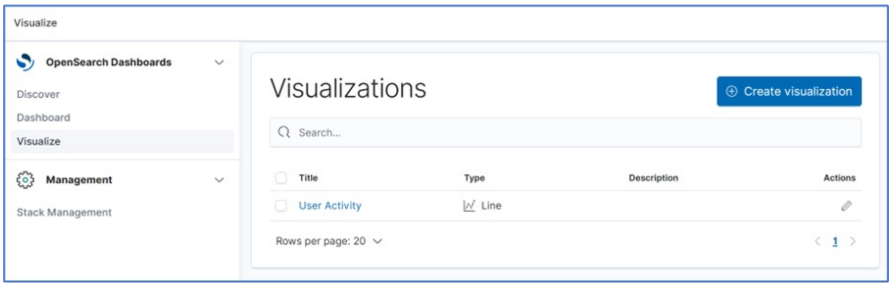
Area Charts

Create an Area Chart (Configuration Example)

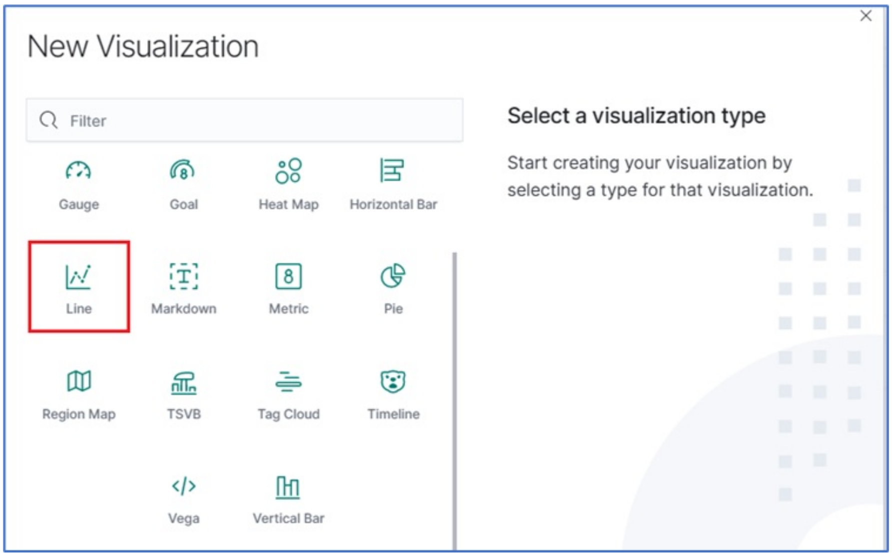
The area chart is useful for stacking measurements for different but related entities.

> NOTE
>
> Become familiar with the Line Chart procedure before creating an Area Chart.

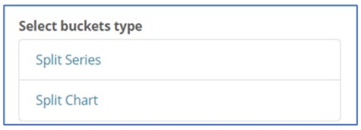
1. Go to *Dashboard :: Visualize*.
2. On the **Visualize** side-tab, click **Create Visualization**,



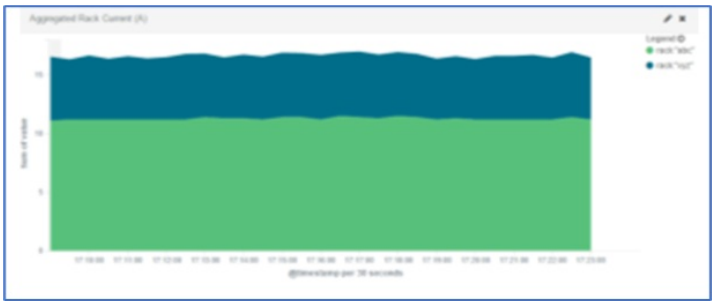
3. Click the *New Visualization* dialog, click the **Line** icon.



4. Click the **Area** icon. On the dialog, click **logstash-***.
5. In *metrics* section, click on **Y-Axis** icon. In **Aggregation** drop-down, select **Sum**.
6. On *Buckets* menu, X-Axis, on **Aggregation** pop-up, select **Data Histogram**. In **Interval** drop-down, select **Custom** then enter value (i.e., 30s).
7. Click **Add Filter** and click **Add sub-buckets**.
8. On the *Select buckets type* menu, click **Split Series**.



9. On **Sub Aggregation** drop-down, select **Filters**. In **Filter 1**, enter value. Click **Add Filter**.
10. In **Filter 2**, enter a search expression for the elements to visualize.
11. (as needed) Click **Add Filter** and repeat.
12. To refresh the graph based on the configuration, click **Refresh**.
13. The resulting visualization would look similar to this:



14. On the Toolbar, click **Save**. Enter a name for the visualization and click **Save**.

> NOTE
>
> When using area charts, be careful to not use the same measurement twice.

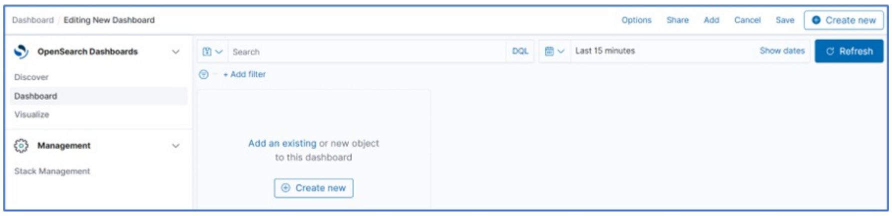
Dashboard tab

Dashboards are a collection of one or more visualizations. These objects can be created, modified, and deleted.

Manage Dashboards

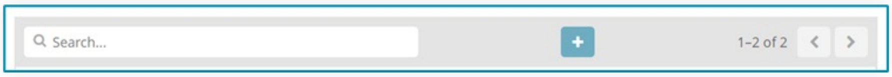
Create Dashboard

1. On the left side panel, click **Dashboard** tab (main panel lists saved visualizations).

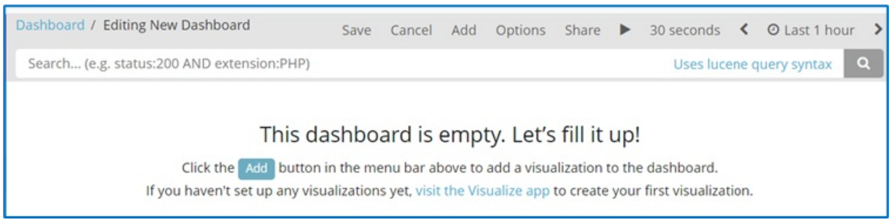


Add an existing or new object to this dashboard

2. On the *Navigation* bar, click the **Create New** icon.



3. On the *Editing New Dashboard* panel, click **Add**.

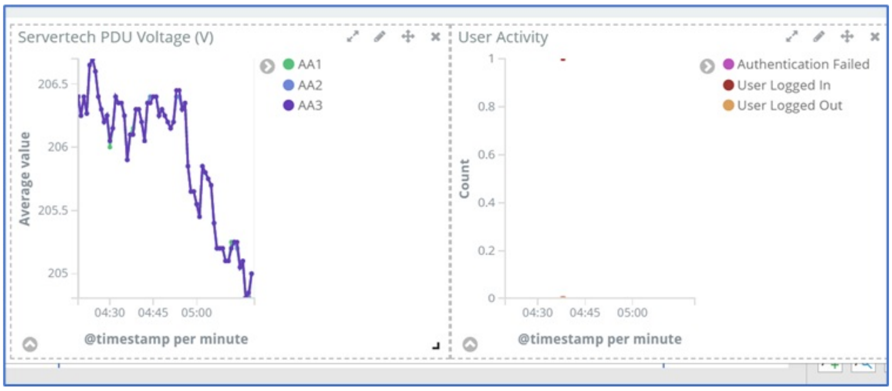

Dashboard / Editing New Dashboard
Save
Cancel
Add
Options
Share
30 seconds
Last 1 hour
Search... (e.g. status:200 AND extension:PHP)
Uses lucene query syntax

This dashboard is empty. Let's fill it up!

Click the Add button in the menu bar above to add a visualization to the dashboard.

If you haven't set up any visualizations yet, visit the Visualize app to create your first visualization.

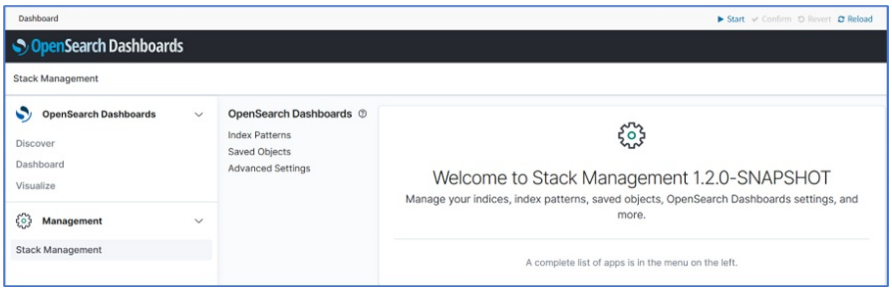
4. On the *Add Panels* dialog, top panel lists available visualizations. To the upper right is the option to create a new visualization.
5. On the visualization list, click the first one to add. The visualization displays in the *dashboard* panel. Click others to add those to the *dashboard* panel.



6. Resize (lower right corner handle) and reposition (click, drag and drop) the graphs, as needed.
7. If needed, to include a filter, click **Add a filter** (displays *Add a Filter* dialog).
   Select from **Filter** drop-down, Enter **Label**, then click **Save**.
8. When the dashboard appearance and details are ready, click **Save** icon.
9. On the *Save dashboard* dialog:
   a. Enter **Title**.
   b. Enter **Description**.
   c. Click **Save**.
10. The new dashboard is added to the list.

Management tab

This manages index patterns, saved objects. The advanced settings can tweak some points, especially visualizations.



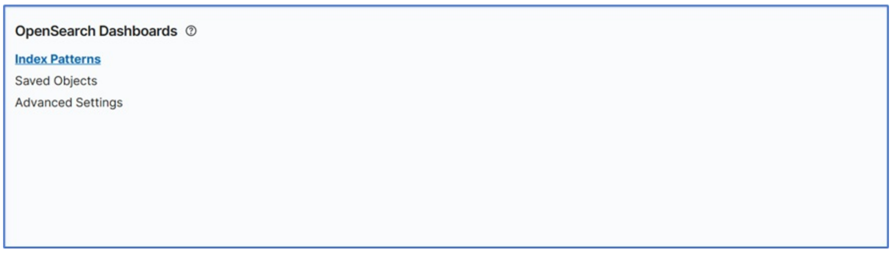
Welcome to Stack Management 1.2.0-SNAPSHOT

Manage your indices, index patterns, saved objects, OpenSearch Dashboards settings, and more.

A complete list of apps is in the menu on the left.

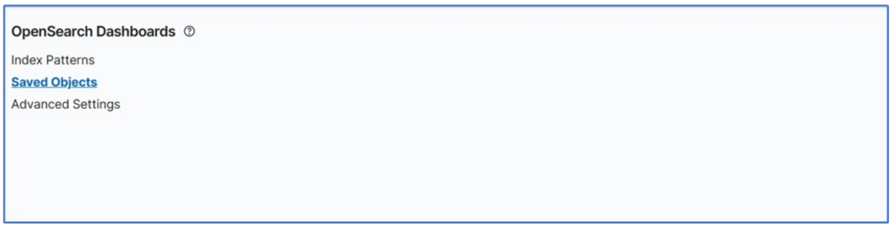
Index Patterns sub-tab

Displays details of selected index patterns (screenshot shows logstash-*).



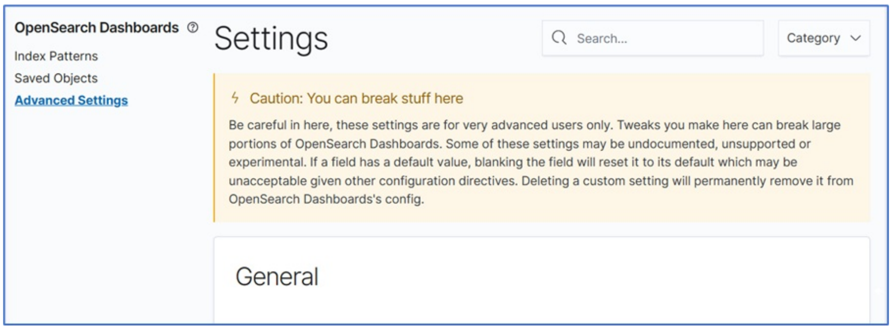
Saved Objects sub-tab

Displays Edit Saved Objects. To modify, click name on list.



Advanced Settings sub-tab

Settings can be directly edited here (admin privileges required). Carefully read the **Caution** statement, especially for the size of the history of saved search queries.



Caution: You can break stuff here

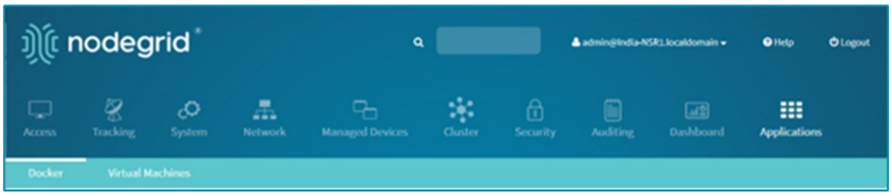
Be careful in here, these settings are for very advanced users only. Tweaks you make here can break large portions of OpenSearch Dashboards. Some of these settings may be undocumented, unsupported or experimental. If a field has a default value, blanking the field will reset it to its default which may be unacceptable given other configuration directives. Deleting a custom setting will permanently remove it from OpenSearch Dashboards's config.

General

Applications Section

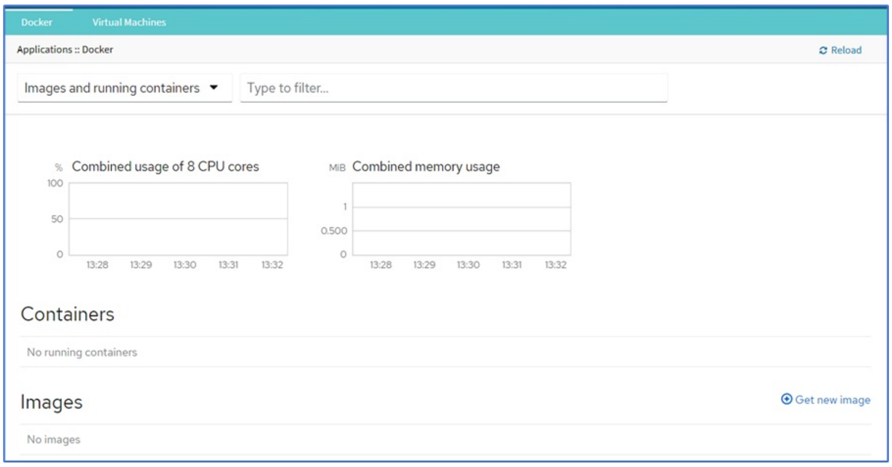
Nodegrid devices can run additional applications. These provide expanded software capabilities. The most used apps are in the areas of monitoring and SD-WAN. While all Nodegrid units support this feature, the Services Router Family is designed to run applications to enhance a wide variety of connectivity options.

> **NOTE**
>
> To run applications, additional licenses are required.



Docker tab

Docker is an open platform to build, ship and run distributed applications. With Administrator privileges, user can run Docker apps on Nodegrid. Docker applications can be pulled from **Docker Hub**, starting and stopping of the Docker Containers.



Docker supports Seccomp and Apparmor. New containers are Seccomp and Apparmor enabled by default.

To start a container without Seccomp and Apparmor, the following shell command is required:

None Copy

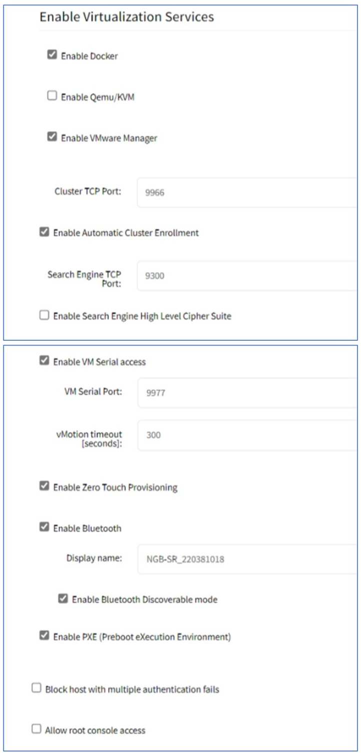
```
docker run --name <name> --security-opt seccomp=unconfined --security-opt apparmor=unconfined <image name>.
```

Containers created before v5.4 retain the same behavior prior to this Docker upgrade. For example, if the container was created with the default command, Seccomp and Apparmor is disabled.

Virtualization

Activate Virtualization

1. Go to *Security :: Services*
2. In the *Enable Virtualization Services* menu.



Enable Virtualization Services

☑ Enable Docker

☐ Enable Qemu/KVM

☑ Enable VMware Manager

Cluster TCP Port: 9966

☑ Enable Automatic Cluster Enrollment

Search Engine TCP Port: 9300

☐ Enable Search Engine High Level Cipher Suite

☑ Enable VM Serial access

VM Serial Port: 9977

vMotion timeout [seconds]: 300

☑ Enable Zero Touch Provisioning

☑ Enable Bluetooth

Display name: NGB-SR_220381018

☑ Enable Bluetooth Discoverable mode

☑ Enable PXE (Preboot eXecution Environment)

☐ Block host with multiple authentication fails

☐ Allow root console access

3. Select **Enable Docker** checkbox
4. Make other settings, as needed
5. Click **Save**.

Licenses are required. To view licensed applications, go to *System :: Licenses*.

> NOTE
>
> The management of Docker Applications is currently only available through the WebUI. The WebUI provides a basic interface to manage Docker Containers. For more advanced features, administrators can use the docker command line tools.

Docker Images

Administrators can directly download images from the Docker Hub to *Applications :: Docker*. The Nodegrid device must have access to the Docker Hub.

Each container can be configured with several parameters, including exposed ports, memory allocation, environmental variables, name, etc. When a container is created, detailed information is displayed in drop-down menus.

Add a new Docker Image

NOTE

Requires administrator privileges.

1. Ensure the virtualization license is valid, and device firmware version is 5.4 or later.
2. Go to *Security :: Services* and ensure Docker services are enabled.
3. Go to *Applications :: Docker*.
4. Click **Get new image**.
5. Type **httpd** and press **Enter**.
6. On the list, select the image and click **Download**.
7. On download, the image is listed in the *Images* table.

Add a New Docker Container

1. Select the image and click **Play**.
2. Adjust the configuration details.
3. Click **Run**.

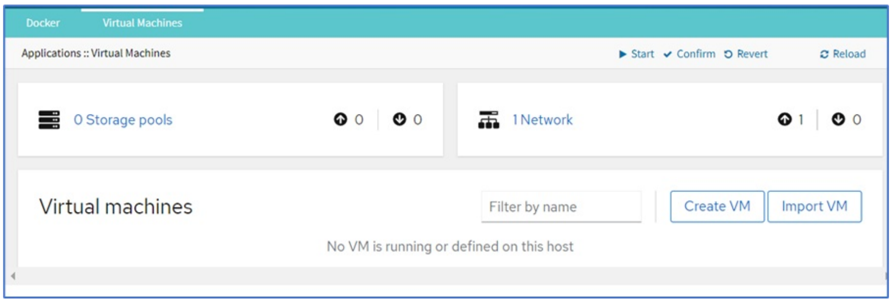
For additional details see the official Docker create documentation.

NOTE

After the container is created, it does not automatically start.

Virtual Machines tab

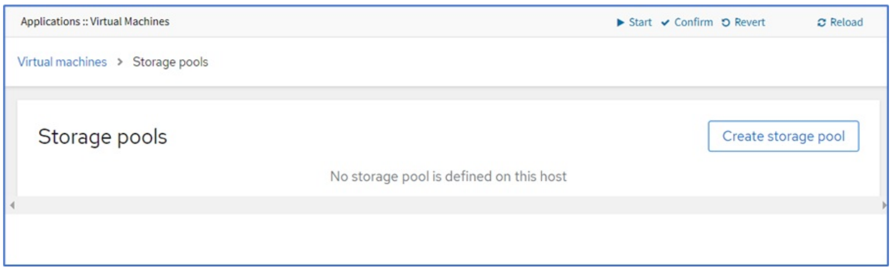
On *Applications :: Virtual Machines*, virtual machines can be created, imported, and managed. Within the drop-down menu, an embedded VNC terminal is available and automatically started with the VM.



Storage Pools

Create a Storage Pool

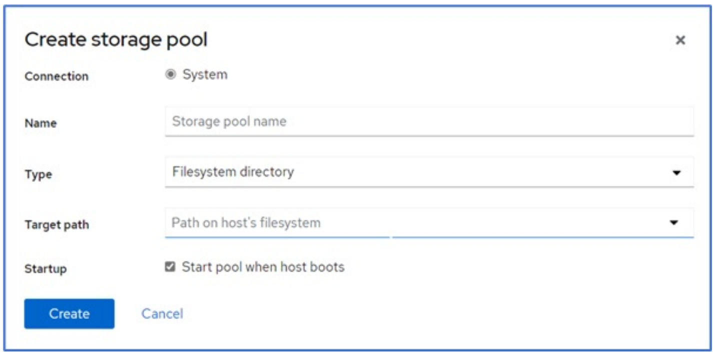
1. Go to *Applications :: Virtual Machines*.
2. Click **Storage pools** (displays dialog).



Storage pools

No storage pool is defined on this host

3. Click **Create storage pool** (displays dialog).



Create storage pool

Connection	● System
Name	Storage pool name
Type	Filesystem directory
Target path	Path on host's filesystem
Startup	☑ Start pool when host boots

   a. Enter **Name**.
   b. On **Type** drop-down, select **Filesystem directory.**
   c. On **Target path** drop-down, select **list of file folders**.

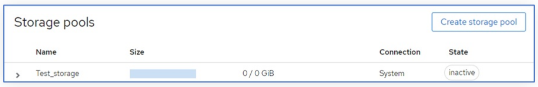
4. On **Startup**, select **Start pool when host boots** checkbox.
5. Click **Create**.

Create sdb Storage

Step 1 – Create storage pool

This is used in the *Access Additional Drive(s)/Drive Partitions* procedure.

1. Go to *Applications :: Virtual Machines*.
2. Click **Storage pools**
3. Click **Create storage pool**
4. Enter **Name**
5. On **Type** drop-down, select **Filesystem directory**
6. On **Target path** field, enter: **/var/local/file_manager/admin_group/sdb1/**
7. On **Startup**, select **Start pool when host boots** checkbox.
8. Click **Create.**

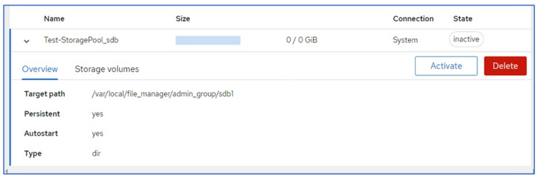


Storage pools

	Name	Size		Connection	State
›	Test_storage		0 / 0 GiB	System	inactive

Step 2 – Create Volume

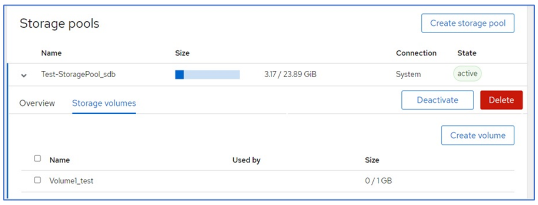
1. Expand the details (click **Right-arrow** – left side)



	Name	Size		Connection	State
⌄	Test-StoragePool_sdb		0 / 0 GiB	System	inactive

Target path	/var/local/file_manager/admin_group/sdb1
Persistent	yes
Autostart	yes
Type	dir

2. Click **Activate**.
3. On *Storage volumes* sub-tab, click **Create a Volume**.
4. Enter **Name**
5. On **Size** drop-down, select **Gib** or **MiB**.
6. On **Format** drop-down, select one (qcow2, raw).
7. Click **Create**.



Storage pools

Create storage pool

	Name	Size		Connection	State
⌄	Test-StoragePool_sdb		3.17 / 23.89 GiB	System	active

Overview | Storage volumes

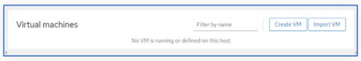
Deactivate | Delete

Create volume

□	Name	Used by	Size
□	Volume1_test		0 / 1 GB

Step 3 – Create Virtual Machine

1. On *Virtual Machine* page, go to *Virtual machines* section:

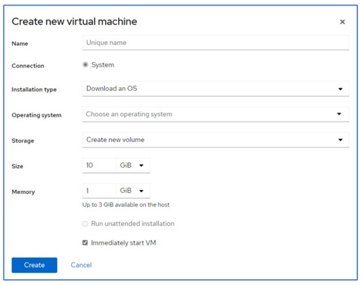


Virtual machines

Filter by name | Create VM | Import VM

No VM is running or defined on this host

2. Click **Create VM** (displays dialog). Enter details:



Create new virtual machine ×

Name: Unique name

Connection: ● System

Installation type: Download an OS

Operating system: Choose an operating system

Storage: Create new volume

Size: 10 GiB

Memory: 1 GiB

Up to 3 GiB available on the host

□ Run unattended installation

☑ Immediately start VM

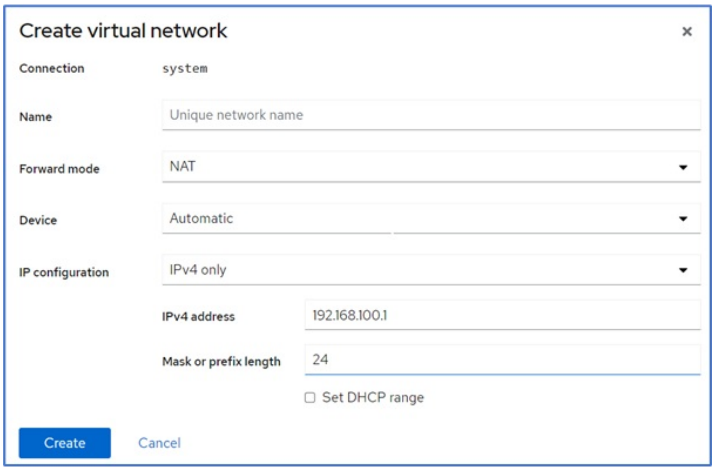
Create | Cancel

3. Enter **Name.**
4. On **Installation type** drop-down, select **Download an OS.**
5. On **Operating system** drop-down, select one (depends on **Installation type** selection).
6. On **Storage** drop-down, select the **sdb** storage pool.
7. On **Volume** drop-down, select the **sdb** volume.
8. Enter **Size** values.
9. Enter **Memory** values.
10. (if available) Select **Run unattended installation** checkbox.
11. Select **Immediately start VM** checkbox.
12. Click **Create**.

Networks

Create a Network

1. Go to *Applications :: Virtual Machines*.
2. Click **Network** (displays dialog)
3. Click **Create virtual network** (displays dialog).



Create virtual network

Connection: system

Name: Unique network name

Forward mode: NAT

Device: Automatic

IP configuration: IPv4 only

IPv4 address: 192.168.100.1

Mask or prefix length: 24

□ Set DHCP range

4. Enter **Name.**
5. On **Forward** mode drop-down, select **NAT**.
6. On **Device** drop-down, select one.
7. On **IP configuration** drop-down,
    - **IPv4 only**selection
        - Enter **IPv4 address.**
        - Enter **Mask or prefix length.**
        - Select **DHCP range** checkbox, enter **Start** and **End** values.
    - **IPv6 only** selection
        - Enter **Prefix length.**
        - **DHCP range** checkbox, enter **Start** and **End** values.
    - **IPv4 and IPv6** selection
        - Enter **IPv4 address.**
        - Enter **Mask or prefix length.**
        - **DHCP range** checkbox, enter **Start** and **End** values.
        - Enter **IPv6 address.**
        - Enter **Prefix length.**
        - **DHCP range** checkbox, enter **Start** and **End** values.
8. Click **Create**.

Libvirt VM Tool

Create a new VM via Libvirt

1. Copy the .iso image to /var/lib/libvirt/images
2. Go to *Applications :: Virtual Machines*.
3. Click **Create VM** (displays dialog).
4. Enter **Name**
5. On **Installation Type**drop-down, select Local install media (ISO image or distro install tree). Other options: URL (ISO image or distro install tree), Network boot (PXE).
    a. **Installation Source** (options adjust based on **Installation Type** selection).
    b. **Operating System** drop-down, select one (if available).
    c. **Storage** drop-down, select one (Create new volume, No storage, Storage pools).
    d. If **Create new volume** selected, enter **Size** and **Memory**.
    e. **Immediately Start VM** checkbox
6. Click **Create**.

WiFi Controller tab

This provides information on Devices, Firmware and System.

Install OpenWiFi

Get OpenWiFi Script

To get the OpenWiFi install package, contact Technical Support.

Install OpenWiFi Script

1. Copy the package to the Nodegrid device (any location is acceptable).
2. Open Shell SUDO.
3. To make it executable:
   ```
   chmod +x (package_file)
   ```
4. To execute:
   Text
   ✏🗑
   ```
   opkg install (package_file)
   ```
5. To view the OpenWiFi application, go to *Applications :: WiFi Controller*.

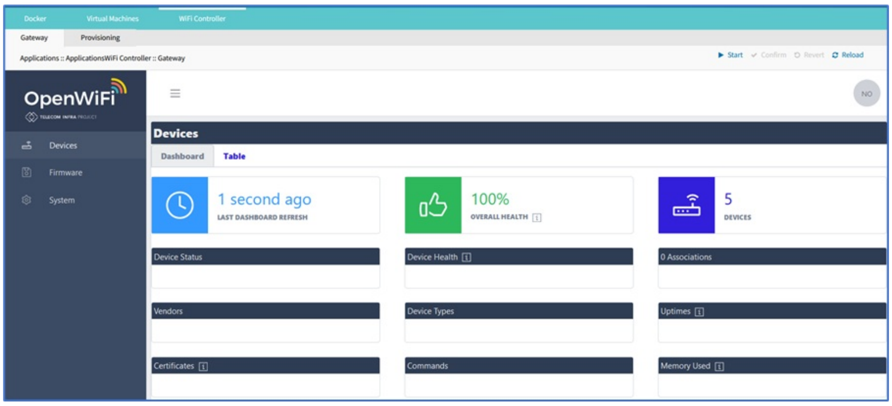
Enable/Disable WiFi Controller

1. Go to *Security :: Services*.
2. In *Active Services* menu:
3. Select/unselect **Enable WiFi Controller** checkbox.
4. Click **Save**.

Applications :: WiFi Controller :: Gateway

Devices side-tab

Go to *Applications :: WiFi Controller :: Gateway – Devices :: Dashboard*.



Applications :: ApplicationsWiFi Controller :: Gateway

Devices

1 second ago
LAST DASHBOARD REFRESH

100%
OVERALL HEALTH

5
DEVICES

Device Status

Device Health

0 Associations

Vendors

Device Types

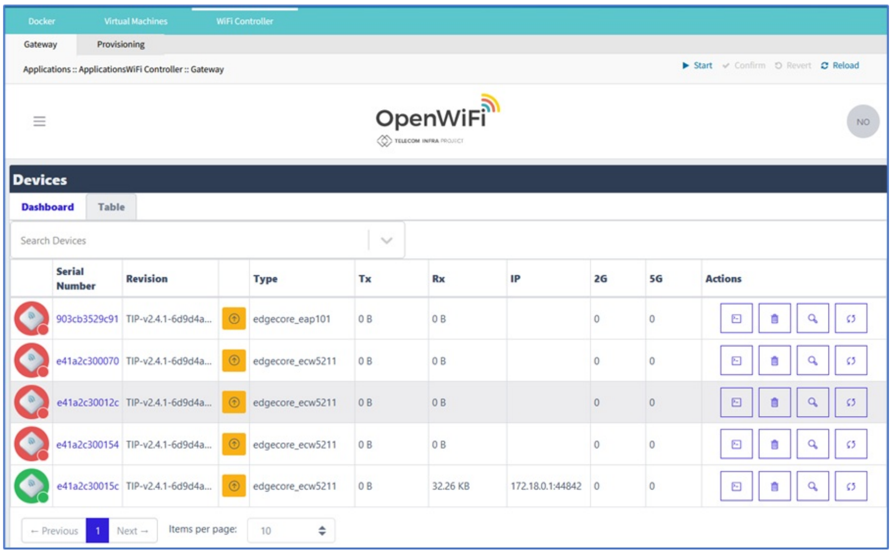
Uptimes

Certificates

Commands

Memory Used

Go to *Applications :: WiFi Controller :: Gateway – Devices :: Table*.

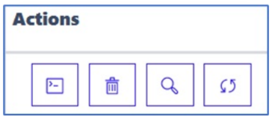


Applications :: ApplicationsWiFi Controller :: Gateway

Devices

	Serial Number	Revision		Type	Tx	Rx	IP	2G	5G	Actions
	903cb3529c91	TIP-v2.4.1-6d9d4a...		edgecore_eap101	0 B	0 B		0	0	
	e41a2c300070	TIP-v2.4.1-6d9d4a...		edgecore_ecw5211	0 B	0 B		0	0	
	e41a2c30012c	TIP-v2.4.1-6d9d4a...		edgecore_ecw5211	0 B	0 B		0	0	
	e41a2c300154	TIP-v2.4.1-6d9d4a...		edgecore_ecw5211	0 B	0 B		0	0	
	e41a2c30015c	TIP-v2.4.1-6d9d4a...		edgecore_ecw5211	0 B	32.26 KB	172.18.0.1:44842	0	0	

On the *Actions* column, click buttons, as needed.



Connect this device

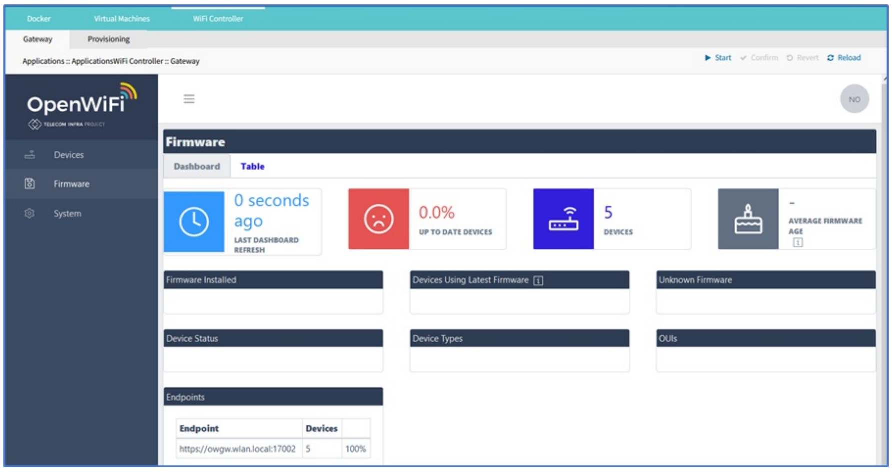
Delete this device.

Display details on this device.

Refresh this device.

Firmware side-tab

Go to *Applications :: WiFi Controller :: Gateway – Firmware :: Dashboard*.



0 seconds ago
LAST DASHBOARD REFRESH

0.0%
UP TO DATE DEVICES

5
DEVICES

-
AVERAGE FIRMWARE AGE

Firmware Installed

Devices Using Latest Firmware

Unknown Firmware

Device Status

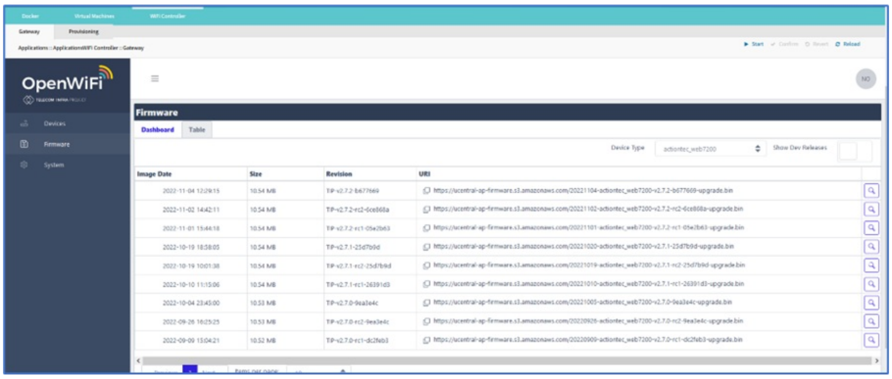
Device Types

OUIs

Endpoints

Endpoint	Devices	
https://owgw.wlan.local:17002	5	100%

Go to *Applications :: WiFi Controller :: Gateway – Firmware ::Table*.



Device Type: actiontec_web7200

Show Dev Releases

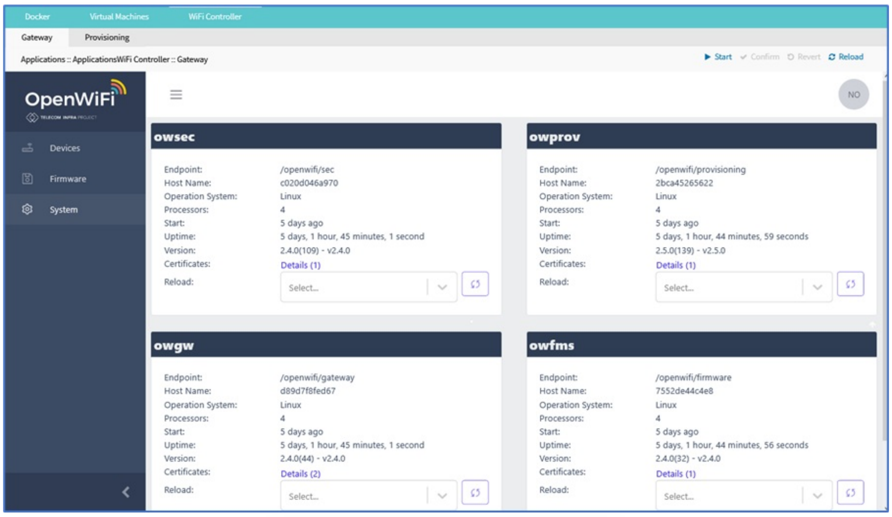
Image Date	Size	Revision	URI
2022-11-04 12:29:15	10.54 MB	TIP-v2.7.2-b677669	https://ucentral-ap-firmware.s3.amazonaws.com/20221104-actiontec_web7200-v2.7.2-b677669-upgrade.bin
2022-11-02 14:42:11	10.54 MB	TIP-v2.7.2-rc2-6ce868a	https://ucentral-ap-firmware.s3.amazonaws.com/20221102-actiontec_web7200-v2.7.2-rc2-6ce868a-upgrade.bin
2022-11-01 15:44:18	10.54 MB	TIP-v2.7.2-rc1-05e2b63	https://ucentral-ap-firmware.s3.amazonaws.com/20221101-actiontec_web7200-v2.7.2-rc1-05e2b63-upgrade.bin
2022-10-19 18:58:05	10.54 MB	TIP-v2.7.1-25d7b9d	https://ucentral-ap-firmware.s3.amazonaws.com/20221020-actiontec_web7200-v2.7.1-25d7b9d-upgrade.bin
2022-10-19 10:01:38	10.54 MB	TIP-v2.7.1-rc2-25d7b9d	https://ucentral-ap-firmware.s3.amazonaws.com/20221019-actiontec_web7200-v2.7.1-rc2-25d7b9d-upgrade.bin
2022-10-10 11:15:06	10.54 MB	TIP-v2.7.1-rc1-26391d3	https://ucentral-ap-firmware.s3.amazonaws.com/20221010-actiontec_web7200-v2.7.1-rc1-26391d3-upgrade.bin
2022-10-04 23:45:00	10.53 MB	TIP-v2.7.0-9ea3e4c	https://ucentral-ap-firmware.s3.amazonaws.com/20221005-actiontec_web7200-v2.7.0-9ea3e4c-upgrade.bin
2022-09-26 16:25:25	10.53 MB	TIP-v2.7.0-rc2-9ea3e4c	https://ucentral-ap-firmware.s3.amazonaws.com/20220926-actiontec_web7200-v2.7.0-rc2-9ea3e4c-upgrade.bin
2022-09-09 15:04:21	10.52 MB	TIP-v2.7.0-rc1-dc2feb3	https://ucentral-ap-firmware.s3.amazonaws.com/20220909-actiontec_web7200-v2.7.0-rc1-dc2feb3-upgrade.bin

⧉ Copy this URI to clipboard.

🔍 Display details on this URI.

System side-tab

Go to *Applications :: WiFi Controller :: Gateway – System*.



owsec

Endpoint: /openwifi/sec
Host Name: c020d046a970
Operation System: Linux
Processors: 4
Start: 5 days ago
Uptime: 5 days, 1 hour, 45 minutes, 1 second
Version: 2.4.0(109) - v2.4.0
Certificates: Details (1)
Reload: Select...

owprov

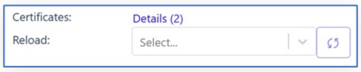
Endpoint: /openwifi/provisioning
Host Name: 2bca45265622
Operation System: Linux
Processors: 4
Start: 5 days ago
Uptime: 5 days, 1 hour, 44 minutes, 59 seconds
Version: 2.5.0(139) - v2.5.0
Certificates: Details (1)
Reload: Select...

owgw

Endpoint: /openwifi/gateway
Host Name: d89d7f8fed67
Operation System: Linux
Processors: 4
Start: 5 days ago
Uptime: 5 days, 1 hour, 45 minutes, 1 second
Version: 2.4.0(44) - v2.4.0
Certificates: Details (2)
Reload: Select...

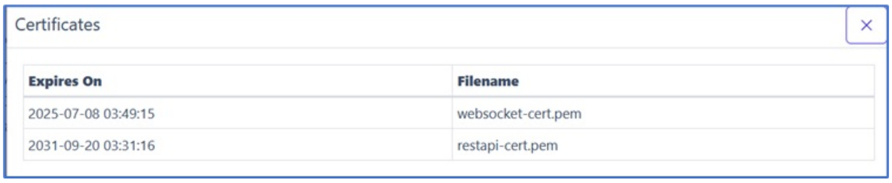
owfms

Endpoint: /openwifi/firmware
Host Name: 7552de44c4e8
Operation System: Linux
Processors: 4
Start: 5 days ago
Uptime: 5 days, 1 hour, 44 minutes, 56 seconds
Version: 2.4.0(32) - v2.4.0
Certificates: Details (1)
Reload: Select...



Certificates: Details (2)
Reload: Select...

Click **Details** link to display Certificate details.



Certificates

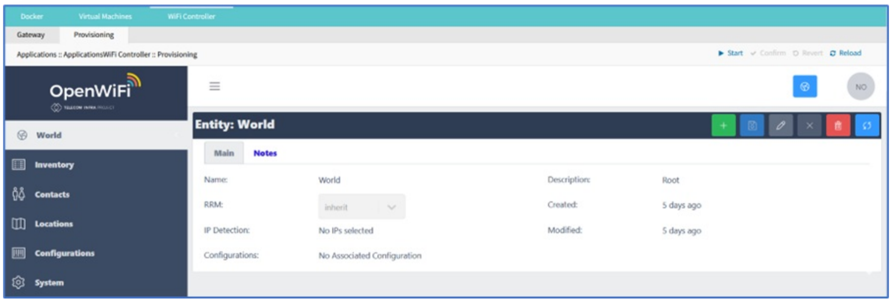
Expires On	Filename
2025-07-08 03:49:15	websocket-cert.pem
2031-09-20 03:31:16	restapi-cert.pem

To reload, on **Select** drop-down, select one, then click Refresh icon.

Applications :: WiFi Controller :: Provisioning

World side-tab

Go to *Applications :: WiFi Controller :: Provisioning – World :: Main*.



Entity: World

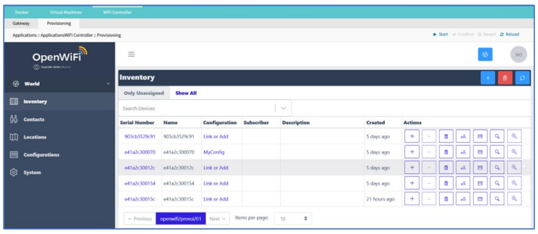
Name:	World	Description:	Root
RRM:	inherit	Created:	5 days ago
IP Detection:	No IPs selected	Modified:	5 days ago
Configurations:	No Associated Configuration		

Buttons:

- + Add Child Entity to World
- Save
- ✎ Edit
- × Close window
- Delete
- Refresh

Inventory side-tab

Go to *Applications :: WiFi Controller :: Positioning – Inventory*.

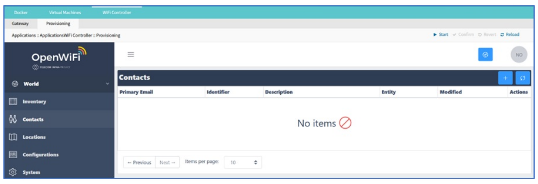


Inventory

Serial Number	Name	Configuration	Subscriber	Description	Created	Actions
903cb3529c91	903cb3529c91	Link or Add			5 days ago	
e41a2c300070	e41a2c300070	MyConfig			5 days ago	
e41a2c30012c	e41a2c30012c	Link or Add			5 days ago	
e41a2c300154	e41a2c300154	Link or Add			5 days ago	
e41a2c30015c	e41a2c30015c	Link or Add			21 hours ago	

Contacts side-tab

Go to *Applications :: WiFi Controller :: Positioning – Contacts*.



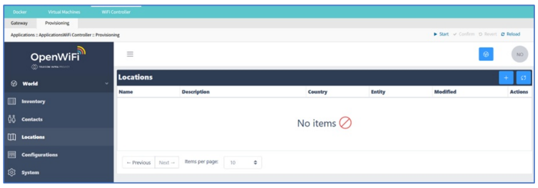
Contacts

Primary Email	Identifier	Description	Entity	Modified	Actions

No items

Locations side-tab

Go to *Applications :: WiFi Controller :: Positioning – Locations*.



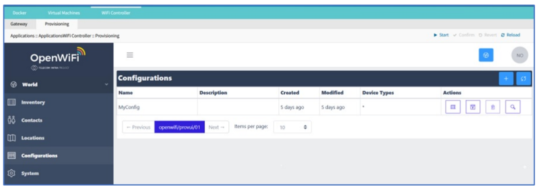
Locations

Name	Description	Country	Entity	Modified	Actions

No items

Configurations side-tab

Go to *Applications :: WiFi Controller :: Positioning – Configurations*.

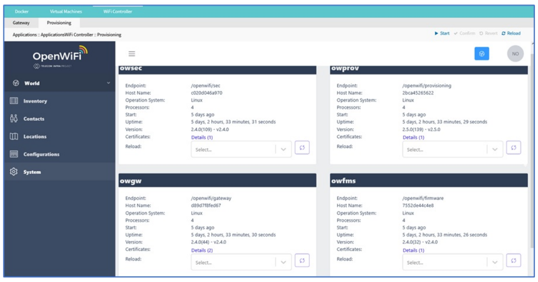


Configurations

Name	Description	Created	Modified	Device Types	Actions
MyConfig		5 days ago	5 days ago	*	

System side-tab

Go to *Applications :: WiFi Controller :: Positioning – System*.



Applications :: ApplicationsWiFi Controller :: Provisioning

owsec

Endpoint: /openwifi/sec
Host Name: c020d046a970
Operation System: Linux
Processors: 4
Start: 5 days ago
Uptime: 5 days, 2 hours, 33 minutes, 31 seconds
Version: 2.4.0(109) - v2.4.0
Certificates: Details (1)
Reload: Select...

owprov

Endpoint: /openwifi/provisioning
Host Name: 2bca45265622
Operation System: Linux
Processors: 4
Start: 5 days ago
Uptime: 5 days, 2 hours, 33 minutes, 29 seconds
Version: 2.5.0(139) - v2.5.0
Certificates: Details (1)
Reload: Select...

owgw

Endpoint: /openwifi/gateway
Host Name: d89d7f8fed67
Operation System: Linux
Processors: 4
Start: 5 days ago
Uptime: 5 days, 2 hours, 33 minutes, 30 seconds
Version: 2.4.0(44) - v2.4.0
Certificates: Details (2)
Reload: Select...

owfms

Endpoint: /openwifi/firmware
Host Name: 7552de44c4e8
Operation System: Linux
Processors: 4
Start: 5 days ago
Uptime: 5 days, 2 hours, 33 minutes, 26 seconds
Version: 2.4.0(32) - v2.4.0
Certificates: Details (1)
Reload: Select...

Network Function Virtualization

Administrators can run additional NFV's or other Virtual Machines. A large variety of configuration options are available through the command line interface.

Contact Technical Support for more information.