



nodegrid

User Guide v5.4

Contents

About the Nodegrid v5.4 User Guide.....	1
Notifications	1
Credits	2
Product Overview	2
Nodegrid Serial Console	2
Nodegrid Serial Console - S Series	2
Nodegrid Serial Console - R Series.....	5
Nodegrid Serial Console - T Series	7
Nodegrid Serial Console Plus.....	9
Nodegrid Net Services Router Family.....	12
Nodegrid Net Services Router.....	13
Nodegrid Net Services Router Expansion Modules.....	15
Nodegrid Gate SR	18
Nodegrid Hive SR.....	22
Nodegrid Bold SR.....	25
Nodegrid Link SR	29
Nodegrid Mini SR	33
Nodegrid Manager	36
Installation	37
Hardware Installation	37
Shipping Box Contents.....	37
Installation of Modules for Nodegrid Net Services Router	38
M.2 Cellular Antenna Placement	39
Device Power Connections	40
Rack Mounting	44
Network Connection	48
Power Cord(s) Connection	48
Connect Devices.....	48
Serial Devices	48
IP Devices	49
Connect to a Nodegrid Device	49
Connect to the Console Port	50
ETH0 Connection	50
WiFi Connection	50
Bluetooth® Connection	51
KVM Port Connection	51
I/O Ports (GPIO).....	51
Import / Export Configuration	52
Import Configuration Settings	52
Export Configuration Settings.....	53
Nodegrid Manager Installation	53
Create a VMware Virtual Machine	53
Install Nodegrid Manager	56
Enroll Nodegrid Manager to ZPE Cloud	58
System Profile.....	59
Gateway Profile	60
Out of Bounds Profile	60
Initial Network Configuration	61
Access the CLI Window.....	61
Identify Current IP Address	61
Define Static IP Address.....	62

- Configure Loopback Address 63
- WiFi Module 64
- General Information..... 65
 - User Interfaces..... 65
 - WebUI Banner..... 65
 - CLI Interface..... 68
 - Shell Access..... 70
 - Access to Devices..... 70
 - Device Sessions..... 70
 - CLI Device Sessions 73
 - Search Functionality 74
 - Device Search 74
 - Global Search..... 77
- Access Section..... 77
 - Table tab 78
 - Function Descriptions 78
 - View Device Details..... 81
 - Manage Power 82
 - Tree tab 83
 - View Column Branches 84
 - Node tab 85
 - Map tab 86
 - Image tab..... 86
- Tracking Section 87
 - Open Sessions tab..... 87
 - Sessions Table sub-tab 87
 - Devices Table sub-tab..... 87
 - Event List tab 88
 - Statistics sub-tab 88
 - Events sub-tab 88
 - System Usage tab..... 93
 - Memory Usage sub-tab 94
 - CPU Usage sub-tab 94
 - Disk Usage sub-tab 94
 - Discovery Logs tab 95
 - Manage Logs..... 95
 - Network tab..... 95
 - Interface sub-tab 95
 - Switch Interfaces sub-tab 97
 - MSTP sub-tab 98
 - LLDP sub-tab 98
 - Routing Table sub-tab 99
 - MAC Table sub-tab 100
 - IPsec sub-tab 100
 - Wireguard sub-tab 101
 - Hotspot sub-tab 101
 - QoS sub-tab 102
 - DHCP sub-tab 103
 - Flow Exporter sub-tab 103
 - Devices tab 103
 - Serial Statistics sub-tab 103
 - USB devices sub-tab 104

- Bluetooth sub-tab 106
- Wireless Modem sub-tab 107
- GPS sub-tab 109
- GEO Fence sub-tab 109
- Scheduler tab 109
- HW Monitor tab 110
 - Thermal sub-tab 110
 - Power sub-tab 111
 - USB Sensors sub-tab 111
 - I/O Ports (GPIO) sub-tab (Gate SR/Link SR only) 113
- ZPE Cloud tab 114
- SD-WAN tab 115
 - Underlay sub-tab 115
 - Overlay sub-tab 116
- System Section 116
 - License tab 116
 - Manage Licenses 117
 - Preferences tab 117
 - Manage Preferences 118
 - Slots tab (SR only) 124
 - Manage Slots 125
 - Date and Time tab 125
 - Local Settings sub-tab 126
 - NTP Server sub-tab 128
 - NTP Authentication sub-tab 128
 - Toolkit tab 130
 - Reboot tool 130
 - Shutdown tool 130
 - Software Upgrade tool 131
 - Save Settings tool 132
 - Apply Settings tool 133
 - Restore to Factory Default Settings tool 135
 - System Certificate tool 136
 - System Configuration Checksum tool 138
 - Network Tools tool 140
 - API tool 142
 - File Manager tool 145
 - Diagnostic Data tool 149
 - Cloud Enrollment tool 150
 - Logging tab 151
 - Custom Fields tab 152
 - Dial-Up tab 153
 - Services sub-tab 154
 - Callback Users sub-tab 154
 - Scheduler tab 155
 - Manage Tasks 156
 - SMS tab (only with installed cellular module) 159
 - Settings sub-tab 159
 - Whitelist sub-tab 162
 - Remote File System tab 162
 - Manage Remote File System 163
 - I/O Ports tab (only with GPIO) 166

Configure I/O Port Settings.....	167
Network Section	168
Settings tab	168
Manage Settings	169
Connections tab	173
Manage Network Connections	174
Create Interface Connections	175
Switch tab (NSR, GSR, BSR)	197
Switch Interfaces sub-tab	198
Backplane sub-tab	202
VLAN sub-tab	202
ACL sub-tab	205
LAG sub-tab	206
MSTP sub-tab	208
Global sub-tab	211
Port Mirroring sub-tab	212
Static Routes tab	214
Manage Static Routes	214
Hosts tab	216
Manage Hosts	216
SNMP tab	217
Manage SNMP	217
DHCP Server tab	219
Manage DHCP Server	220
Wireless Modem tab	224
Manage Wireless Modem	224
Flow Exporter tab	226
Add a new Flow Export	226
802.1x tab (SR only)	228
Profiles sub-tab	228
Credentials sub-tab	230
QoS tab	233
Interfaces sub-tab	233
Classes sub-tab	236
Rules sub-tab	238
SD-WAN tab	241
Application sub-tab	241
Path Steering sub-tab	242
Link Profile sub-tab	244
Path Quality sub-tab	245
Settings sub-tab	247
VPN drop-down > SSL VPN tab	248
Client sub-tab	248
Server sub-tab	252
Server Status sub-tab	255
VPN drop-down > IPsec tab	255
Overview	256
IPsec Configuration Process	259
Tunnel sub-tab	259
IKE Profile sub-tab	264
Global sub-tab	267
VPN drop-down > Wireguard tab	268

- Manage Wireguard Configurations.....269
- Managed Devices Section.....275
 - General Information275
 - Supported Protocols.....275
 - Device Types.....275
 - Devices tab277
 - Device Types.....279
 - Device Procedures282
 - Configure Individual Device Settings293
 - Access sub-tab.....293
 - Management sub-tab304
 - Logging sub-tab.....306
 - Custom Fields sub-tab.....310
 - Commands sub-tab312
 - Views tab316
 - Tree sub-tab316
 - Image sub-tab318
 - Types tab322
 - Manage Types.....323
 - Auto Discovery tab.....324
 - Auto Discovery Configuration Process324
 - Auto Discovery Configurations325
 - Network Scan sub-tab340
 - VM Manager sub-tab343
 - Discovery Rules sub-tab.....345
 - Hostname Detection sub-tab348
 - Discovery Logs sub-tab352
 - Discover Now sub-tab352
 - Preferences tab.....353
 - Power Menu sub-tab353
 - Session Preferences sub-tab354
 - Views sub-tab354
- Cluster Section356
 - Peers tab.....357
 - Settings tab357
 - Enrollment sub-tab358
 - Automatic Enrollment Range sub-tab360
 - Management tab361
 - Software Upgrade361
- Security Section363
 - Local Accounts tab.....363
 - Manage Local Users363
 - Password Rules tab366
 - Manage Password Rules.....366
 - User Response to Expired Password367
 - Authorization tab367
 - User Group Configuration Process.....368
 - User Group: Members sub-tab369
 - User Group: Profile sub-tab369
 - User Group: Remote Groups sub-tab371
 - User Group: Devices sub-tab371
 - User Group: Outlets sub-tab.....375

- Configure SSH Key Authentication..... 376
- Authentication tab 376
 - Servers sub-tab 377
 - 2-Factor sub-tab 385
 - SSO sub-tab 389
- Firewall tab..... 395
 - Manage Chains 395
- NAT tab 401
 - Manage Chains 402
 - Manage Chain Settings 403
- Services tab 408
 - General Services sub-tab 408
 - Intrusion Prevention sub-tab 414
- GEO Fence tab 415
 - Manage GEO Fence 415
 - SED Pre-Boot Authenticator (PBA) 417
- RFID Tag tab 417
 - Manage RFID Tag 417
- Auditing Section 418
 - Settings tab 419
 - Data Logging Settings 419
 - Events tab 420
 - Event List sub-tab 420
 - Categories sub-tab 421
 - Destinations tab 424
 - File sub-tab 425
 - Syslog sub-tab 426
 - SNMP Trap sub-tab 428
 - Email sub-tab 429
- Dashboard Section 431
 - Description 431
 - Navigation Tabs 431
 - Toolbar Description 431
 - Configuration Expressions of Data Points 434
 - Discover tab 435
 - Data Point Exploration 435
 - Visualize tab 436
 - Line Charts 436
 - Area Charts 442
 - Dashboard tab 444
 - Manage Dashboards 445
 - Timelion tab 447
 - Toolbar tabs 447
 - Management tab 450
 - Index Patterns sub-tab 451
 - Saved Objects sub-tab 451
 - Advanced Settings sub-tab 452
- Applications Section 452
 - Docker tab 452
 - Docker Images 454
 - Virtual Machines tab 455
 - Libvirt VM Tool 455

- Links tab.....456
 - Manage Links456
- Network Function Virtualization.....457
- Appendix A – General Information457
 - Technical Support457
 - Support Ticket459
 - Updates and Patches459
 - Manage Virtual Machines459
 - Virtual Serial Port (vSPC) on VM Servers460
 - Serial Port Pinout462
 - Safety.....463
 - Quick Install Guide.....463
 - RoHS464
 - Data Persistence.....464
 - Nodegrid Device Memory464
 - Remove Data from Nonvolatile Memory464
 - Soft Removal of User Data from Nonvolatile Memory464
 - Hard Removal - Secure Erase.....465
 - Mount Remote Shares for Virtual Media467
 - Monitoring Templates467
 - Customize a Monitoring Template467
 - SNMP Template468
 - IPMI Discovery Template469
 - Supported Nodegrid Devices470
 - USB Passthrough.....470
 - USB Power.....470
 - USB Type471
 - KVM Dongle471
 - Bluetooth471
 - 5G Support.....472
 - PXE Boot474
 - VRRP (Virtual Router Redundancy Protocol).....476
 - Example Configuration476
- Appendix B – UEFI Implementation479
 - UEFI Upgrade/Downgrade Concerns479
 - Enable Secure Boot (optional).....480
 - Downgrade to Legacy480
 - Self-Encrypting Drive481
 - Minimum BIOS Versions481
 - Device Conditions482
 - Security Adjustments to System.....482
 - Secure Boot482
 - Requirements482
 - Intrusion Prevention482

About the Nodegrid v5.4 User Guide

Document updated: September 10, 2022.

All manuals ([PDF or HTML format](#)) are available here.

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

This document provides user information and details on the Nodegrid Platform and the supporting units:

- Nodegrid Serial Console Series
- Nodegrid Net Services Router
- Nodegrid Gate SR
- Nodegrid Bold SR
- Nodegrid Link SR
- Nodegrid Hive SR

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 user will be required to correct the interference at his/her 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

ZPE Systems, the ZPE logo, Nodegrid Manager, Nodegrid, FireTrail, Cloud Clustering, DeviceURL and NodeIQ are either registered trademarks or trademarks of ZPE Systems. Other company and product names may be trademarks of their respective owners.

©2022 ZPE Systems, Inc.

Contact us

Sales: sales@zpesystems.com

Support: support@zpesystems.com

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

www.zpesystems.com

Product Overview

Nodegrid Serial Console

The Nodegrid Serial Console product line consolidates and manages attached devices via a Serial Port Connection including servers, network routers and switches, storage, PDUs, UPSs, and any other device with a serial port.

Nodegrid Serial Console - S Series

The Nodegrid Serial Console (S Series) is designed to fit modern and legacy mixed environment. With auto-sensing ports, the S Series Console Servers can be used within any environment with straight-through cables or legacy adapters.

Features include:

- Auto-Switching (Cisco or Legacy Pin-out)
- 16/32/48/96 Serial Ports
- Additional USB ports

- Factory upgradeable CPU and RAM
- 1U 19" Rack Standard Unit
- Single AC, Dual AC, and Dual DC
- Fan options

Nodegrid Serial Console - S Series Hardware Specifications

Item	Description
CPU	Intel x86_64 dual core CPU
Memory & Storage	4 GB of DDR3 DRAM 32 GB mSATA SSD
Interfaces	16, 32, 48, 96 RS-232 serial ports on RJ45 @ 230,400 bps max/port 2 Gb (10/100/1000BT) Ethernet interfaces on RJ45 or (optional) 2 SFP+ 1/2.5/10GB compatible 1 RS-232 serial console port on RJ45 1 USB 3.0 Host and 2 USB 2.0 Hosts on Type A connector 1 HDMI output port
Power	40V-63 VDC dual power input (redundant) Power consumption 45 W typical Single or Dual AC: 100-240 VAC, 50/60 Hz
Physical	Front-Rear mounting brackets Size (L x W x H): 443 x 312 x 43 mm (17.4 x 12.3 x 1.7 in), 1U Weight: 4.9 kg (10.8 lb), depending on options Shipping weight: 7.65 kg (17 lb) Shipping (L x W x H): 600 x 440 x 210 mm (23.6 x 17.3 x 8.3 in) F: front-to-back or back-to-front fans (Swappable) B: no fans
Environmental	Operation: 0 to 50° C (32 to 122° F), 5-95% RH, non-cond. Storage: -20 to 67° C (-4 to 153° F), 5-95% RH, non-cond.

Nodegrid Serial Console - S Series Front Interfaces (F: with fan)



Nodegrid Serial Console - S Series Front Interfaces (B: without fan)



Port	Description
HDMI	HDMI Interface
USB	USB 2.0 Port
PWR	Power LED Green:·Solid - normal,· Off - power is off
SYS	System LED Green:· Blinking – normal,· Fast Blink - RST button Acknowledgment,· Off or Solid - no activity
RST	Reset button: <3s system reset,>10s configuration factory reset and system reset
FAN	Fan options: F (with fan), B (without fan)
USB	1 USB 2.0 Port, 12 USB 1.1 Ports

Nodegrid Serial Console - S Series Rear Interfaces



Port	Description
Power	Single or Dual Power Sockets
Serial	Serial Interfaces: Left/Orange DCD/DTR – On (port open and/or cable connected), Off (not ready) Right/Green RX/T- Blinking (data activity), Off (no activity)

Port	Description
ETH0/SFP0	<p>Network Interface</p> <p>Copper:-Left/Green: Blinking (data activity), Solid (ready), Off (no link/cable disconnected Ethernet fault):-Right/Green (1000Base-T link speed), Right/Orange (100BaseT link speed). Right/Off (no link/cable disconnected/Ethernet fault)</p> <p>SFP 1Gb/10Gb:-Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault)</p> <p>Right/Green - 10Gb link speed:-Right/Orange (1Gb link speed),Right/Off (no link/cable disconnected/Ethernet fault)</p>
ETH1/SFP1	<p>Network Interface</p> <p>Copper:-Left/Green: Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault)</p> <p>Right/Green (1000Base-T link speed),-Right/Orange (100BaseT link speed),-Right/Off (no link/cable disconnected/Ethernet fault)</p> <p>SFP 1Gb/10Gb:-Left/Green: Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault)</p> <p>Right/Green (10Gb link speed),-Right/Orange (1Gb link speed),-Right/Off (no link/cable disconnected/Ethernet fault)</p>
Console	<p>Console MGMT Interface</p> <p>Left/Orange (LED Power Failure), Blinking (Power supply failure/off - for dual power supply models), Off (normal)</p> <p>Right/Green (LED System Activity) – Blinking (normal), Off or Solid (no activity)</p>
USB	1 USB 3.0

Nodegrid Serial Console - R Series

The Nodegrid Serial Console (R Series) fits into major hardware environments like Cisco, Arista, Dell, Palo Alto Networks, and Juniper. The R Series Serial Consoles are perfect for retrofits and to upgrade rack standards of existing builds.

Features include:

- For Cisco Pin-out Devices
- 16/32/48/96 Serial Ports
- 1U 19" Rack Standard Unit
- Single AC, Dual AC, and Dual DC

Nodegrid Serial Console - R Series Hardware Specifications

Item	Description
CPU	Intel Atom x86_64 dual core @ 1.75 GHz CPU
Memory & Storage	4 GB of DDR3 DRAM 32 GB mSATA SSD

Item	Description
Interfaces	16, 32, 48, 96 RS-232 serial ports on RJ45 @ 230,400 bps max/port. 2 Gigabit (10/100/1000BT) Ethernet interfaces on RJ45 or optionally 2 SFP+ 1/2.5/10GB compatible 1 RS-232 serial console port on RJ45 1 USB 3.0 Host and 2 USB 2.0 Hosts on Type A connector 1 HDMI output port
Power	40V-63 VDC dual power input (redundant) Power consumption 45 W typical Single or Dual AC: 100-240 VAC, 50/60 Hz
Physical	Front-Rear mounting brackets Size (L x W x H): 443 x 312 x 43 mm (17.4 x 12.3 x 1.7 in), 1U Weight: 4.9 kg (10.8 lb), depending on options Shipping weight: 9.5 kg (20.9 lb) Shipping (L x W x H): 600 x 440 x 210 mm (23.6 x 17.3 x 8.3 in)
Environmental	Operation: 0 to 50° C (32 to 122° F), 5-95% RH, non-cond. Storage: -20 to 67° C (-4 to 153° F), 5-95% RH, non-cond.

Nodegrid Serial Console - R Series Front Interfaces



Port	Description
HDMI	HDMI Interface
USB	2 USB 2.0 Port
PWR	Power LED Green:· Solid - normal,· Off - power is off
SYS	System LED Green:· Blinking – normal, Fast Blink - RST button Acknowledgment, Off or Solid - no activity
RST	Reset button:<3s system reset,>10s configuration factory reset and system reset

Nodegrid Serial Console - R Series Rear Interfaces



Port	Description
Power	Single or Dual Power Sockets
Serial	Serial Interfaces: Left/Orange DCD/DTR – On (port open and/or cable connected), Off (not ready) Right/Green RX/T- Blinking (data activity), Off (no activity)
ETH0/SFP0	Network Interface Copper:·Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault) Right/Green (1000Base-T link speed), Right/Orange (100BaseT link speed), Right/Off (no link/cable disconnected/Ethernet fault) SFP 1Gb/10Gb:·Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault) Right/Green (10Gb link speed),·Right/Orange (1Gb link speed),·Right/Off (no link/cable disconnected/Ethernet fault)
ETH1/SFP1	Network Interface Copper:·Left/Green – Blinking (data activity), Solid (ready), Off:(no link/cable disconnected/Ethernet fault) Right/Green (1000Base-T link speed), Right/Orange (100BaseT link speed), Right/Off (no link/cable disconnected/Ethernet fault) SFP 1Gb/10Gb:·Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault) Right/Green (10Gb link speed), Right/Orange (1Gb link speed), Right/Off (no link/cable disconnected/Ethernet fault)
Console	Console MGMT Interface Left/Orange (LED Power Failure), Blinking (Power supply failure/off - for dual power supply models), Off (normal) Right/Green (LED System Activity) – Blinking (normal), Off or Solid (no activity)
USB	USB 3.0

Nodegrid Serial Console - T Series

The Nodegrid Serial Console (T Series) fits into environments that still utilize legacy devices and can be a direct replacement for any legacy console server.

Features include:

- For Legacy Devices
- 16/32/48/96 Serial Ports
- 1U 19" Standard Unit
- Single AC, Dual AC, and Dual DC

Nodegrid Serial Console - T Series Hardware Specifications

Item	Description
CPU	Intel Atom x86_64 dual core @ 1.75 GHz CPU

Item	Description
Memory & Storage	4 GB of DDR3 DRAM 32 GB mSATA SSD
Interfaces	2 Gigabit (10/100/1000BT) Ethernet interfaces on RJ45 or 2 SFP+ Fiber interfaces compatible with 1Gb 2.5Gb / 10Gb modules 16, 32, 48, 96 RS-232 serial ports on RJ45 @ 230,400 bps max/port 1 RS-232 serial console port on RJ45 1 USB 3.0 Host 2 USB 2.0 Hosts on Type A connector HDMI
Power	Single/Dual AC 100-240 VAC, 50/60 Hz Dual DC: 40-63 VDC Power consumption 45 W (on 96 ports)
Physical	Front-Rear mounting brackets Size (L x W x H): 443 x 312 x 43 mm (17.4 x 12.3 x 1.7 in), 1U Weight: 4.9 kg (10.8 lb), depending on options Shipping weight: 9.5 kg (20.9 lb) Shipping (L x W x H): 600 x 440 x 210 mm (23.6 x 17.3 x 8.3 in)
Environmental	Operation: 0 to 50° C (32 to 122° F), 5-95% RH, non-cond. Storage: -20 to 67° C (-4 to 153° F), 5-95% RH, non-cond.

Nodegrid Serial Console - T Series Front Interfaces



Port	Description
HDMI	HDMI Interface
USB	2 USB 2.0 Port
PWR	Power LED Green:· Solid - normal,· Off - power is off
SYS	System LED Green:· Blinking – normal, Fast Blink - RST button Acknowledgment, Off or Solid - no activity
RST	Reset button:<3s system reset,>10s configuration factory reset and system reset
HDMI	HDMI Interface

Nodegrid Serial Console - T Series Rear Interfaces



Port	Description
Power	Single or Dual Power Sockets
Serial	Serial Interfaces: Left/Orange DCD/DTR – On (port open and/or cable connected), Off (not ready) Right/Green RX/T- Blinking (data activity), Off (no activity)
ETH0/SFP0	Network Interface Copper:·Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault) Right/Green (1000Base-T link speed), Right/Orange (100BaseT link speed), Right/Off (no link/cable disconnected/Ethernet fault) SFP 1Gb/10Gb:·Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault) Right/Green (10Gb link speed),·Right/Orange (1Gb link speed),·Right/Off (no link/cable disconnected/Ethernet fault)
ETH1/SFP1	Network Interface Copper:·Left/Green – Blinking (data activity), Solid (ready), Off:(no link/cable disconnected/Ethernet fault) Right/Green (1000Base-T link speed), Right/Orange (100BaseT link speed), Right/Off (no link/cable disconnected/Ethernet fault) SFP 1Gb/10Gb:·Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault) Right/Green (10Gb link speed), Right/Orange (1Gb link speed), Right/Off (no link/cable disconnected/Ethernet fault)
Console	Console MGMT Interface Left/Orange (LED Power Failure), Blinking (Power supply failure/off - for dual power supply models), Off (normal) Right/Green (LED System Activity) – Blinking (normal), Off or Solid (no activity)
USB	USB 3.0

Nodegrid Serial Console Plus

Nodegrid Serial Console Plus provides fast, secure and reliable InBand and Out-of-Band access to server, network, storage, power and other serial console devices for faster problem resolution. In addition, when coupled with ZPE’s vendor-neutral Nodegrid Manager software, IT staff immediately have centralized access to NSCP devices and all other physical and virtual devices (VM, Service Processor and KVM/IP) managed by the software, providing a truly hyper-converged infrastructure management solution.

Features include:

- Zero Touch Provisioning (ZTP) over the LAN and WAN
- Modern x86-64bit Linux Kernel
- Failover to 5G/4G/LTE and Wi-Fi
- Gateway and multi-routing table capability
- SSL VPN and Secure Tunnel
- DHCP server
- Built-in firewall
- Selectable encrypted cryptographic protocols and cypher suite levels

Nodegrid Serial Console Plus Hardware Specifications

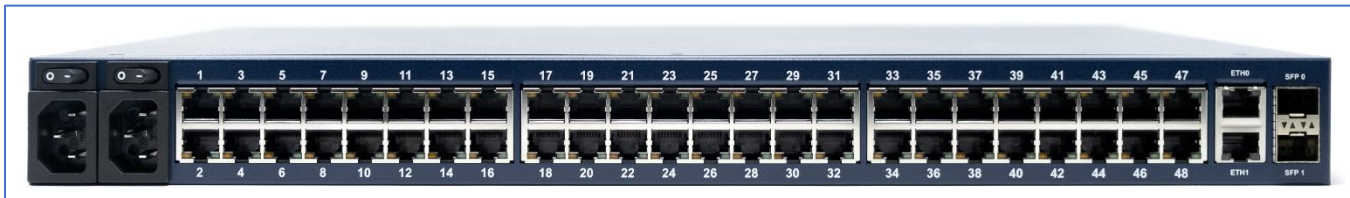
Item	Description
CPU	Intel x86_64 multi-cores
Memory & Storage	4GB of DDR4 DRAM 32GB FLASH (mSATA SSD)
Interfaces	16, 32, 96 RS-232 serial ports on RJ45 @ 230,400 bps max/port. 2 SFP+ 1/2.5/10GB and 2 Gigabit (10/100/1000BT) Ethernet interfaces on RJ45 1 RS-232 serial console port on RJ45 2 USB 3.0 Host on Type A connector 1 HDMI output port 1 5G/4G/LTE Slot (optional) 1 Wi-Fi Slot (optional)
Power	40V-63 VDC dual power input (redundant) Single or Dual AC: 100-240 VAC, 50/60 Hz Power consumption 45 W typical
Physical	Front-Rear mounting brackets Size (L x W x H): 443 x 312 x 43 mm (17.4 x 12.3 x 1.7 in), 1U weight: 5.265 kg (11.6 lb), depending on options Shipping weight: 8.745 kg (19.3 lb) Shipping (L x W x H): 533 x 497 x 209 mm (21 x 19.6 x 8.3 in)
Environmental	Operation: 0 to 50° C (32 to 122° F), 5-95% RH, non-cond. Storage: -20 to 67° C (-4 to 153° F), 5-95% RH, non-cond.

Nodegrid Serial Console Plus Front Interfaces



Port	Description
HDMI	HDMI Interface
USB	2 USB 3.0 Port
Console	Console MGMT Interface Left/Orange (LED Power Failure), Blinking (Power supply failure/off - for dual power supply models), Off (normal) Right/Green (LED System Activity) – Blinking (normal), Off or Solid (no activity)
PWR	Power LED Green:· Solid - normal,· Off - power is off
SYS	System LED Green:· Blinking – normal, Fast Blink - RST button Acknowledgment, Off or Solid - no activity
RST	Reset button:<3s system reset,>10s configuration factory reset and system reset

Nodegrid Serial Console Plus Rear Interfaces



Port	Description
Power	Single or Dual Power Sockets
Serial	Serial Interfaces: Left/Orange DCD/DTR – On (port open and/or cable connected), Off (not ready) Right/Green RX/T- Blinking (data activity), Off (no activity)
ETH0	Network Interface- Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault) Right/Green (1000Base-T link speed),·Right/Orange (100BaseT link speed),·Right/Off (no link/cable disconnected/Ethernet fault)
ETH1	Network Interface- Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault) Right/Green (1000Base-T link speed),·Right/Orange (100BaseT link speed),·Right/Off (no link/cable disconnected/Ethernet fault)
SFP+ 0	Network Interface- Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault) Right/Green (10Gb link speed),·Right/Orange (1Gb link speed),·Right/Off (no link/cable disconnected/Ethernet fault)

Port	Description
SFP+ 1	Network Interface- Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault) Right/Green (10Gb link speed),-Right/Orange (1Gb link speed),-Right/Off (no link/cable disconnected/Ethernet fault)
USB	USB 3.0

Nodegrid Serial Console Plus DOC Side Interfaces



Port	Description
Ground	GND terminal

Nodegrid Serial Console Plus SIM Side Interfaces



Port	Description
SIM-A1, SIM-A2	Sim slots

Nodegrid Net Services Router Family

The Nodegrid Net Services Router (NSR) is a platform appliance designed for software-defined networking (SDN), out of band (OOB) management, DevOps, cellular failover, docker, SD-WAN, remote/branch offices, retail locations, and network function virtualization (NFV) capabilities.

Nodegrid Net Services Router

The Nodegrid Net Services Router is a modular, open platform appliance designed for software-defined networking (SDN), out of band (OOB) management, DevOps, cellular failover, docker, SD-WAN, remote/branch offices, retail locations, and network function virtualization (NFV) capabilities.

Features include:

- Open Framework, Modular Services Router
- Pluggable Expansion Modules - 5 slots available
- Modules for GbE, Serial, SFP+ 10GbE, PoE+, USB, M.2/SATA + Antenna, Storage, Extra Compute
- 1U 19" Standard Unit
- Separation of Control Plane and Data Plane

Nodegrid Net Services Router Hardware Specifications

Item	Description
CPU	Intel Multi-core x86_64 CPU
Memory & Storage	8 GB of DDR4 DRAM (Upgradeable) 32 GB FLASH (mSATA SSD) (Upgradeable) Self-Encrypted Drive (SED)
Interfaces	2 SFP+ Ethernet 2 Gigabit Ethernet 1 RS-232 serial console port on RJ45 1 USB 3.0 1 USB 2.0 1 HDMI
Power	Dual AC 100-240 VAC, 50/60 Hz or Dual DC 36-75 VDC Power Consumption 90W-150W typical
Physical	Front-Rear mounting brackets Size (L x W x H): 438 x 332 x 43mm (17.2 x 13.1 x 1.7 in), 1U Weight: 4.9 kg (10.8 lb), depending on options Air Exhaust or Air Intake Fans (Swappable)
Environmental	Operation: 0 to 45° C (32 to 113° F), 5-95% RH, non-cond. Storage: -20 to 67° C (-4 to 153° F), 10-90% RH, non-cond.

Nodegrid Net Services Router Front Interfaces



Port	Description
Slot 1	Slot for Module
Slot 2	Slot for Module
Slot 3	Slot for Module
SFP+ 0	Network Interface- Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault) Right/Green (10Gb link speed), Right/Orange (1Gb link speed), Right/Off (no link/cable disconnected/Ethernet fault)
SFP+ 1	Network Interface- Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault) Right/Green (10Gb link speed), Right/Orange (1Gb link speed), Right/Off (no link/cable disconnected/Ethernet fault)
ETH0	Network Interface- Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault) Right/Green (1000Base-T link speed), Right/Orange (100BaseT link speed), Right/Off (no link/cable disconnected/Ethernet fault)
ETH1	Network Interface- Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault) Right/Green (1000Base-T link speed), Right/Orange (100BaseT link speed), Right/Off (no link/cable disconnected/Ethernet fault)
Console	Console MGMT Interface Left/Orange (LED Power Failure), Blinking (Power supply failure/off for dual power supply models), Off (normal) Right/Green (LED System Activity), Blinking (normal), Off or Solid (no activity)
USB	USB 3.0
RST	Reset button: <3s (system reset) >10s (configuration factory reset and system reset)

Nodegrid Net Services Router Rear Interfaces













Port	Description
Slot 4	Slot for Module (depending on the Model)
Slot 5	Slot for Module (depending on the Model)
USB	2 USB 2.0 Port
HDMI	HDMI Interface
PWR	Power LED Green:· Solid - normal,· Off - power is off
SYS	System LED Green:· Blinking – normal, Fast Blink - RST button Acknowledgment, Off or Solid - no activity
FAN	Fans
Power Socket	Dual Power Sockets
Power	Single or Dual Power Sockets

Nodegrid Net Services Router Expansion Modules

The Nodegrid Net Services Router has up to five slots for modules that provide extreme flexibility and expanded functionality.

Nodegrid Net Services Router Expansion Modules

Module	Image	Specification
16-Port 1GbE		1000BASE-T Cat5e or better
16-Port SFP 1GbE		Supports all SFP Modules

Module	Image	Specification
8-Port SFP+ 10GbE		Supports all SFP+ Modules
8-Port PoE+		25.5W mapower per port Total ma150W PoE+ available Configurable power budget
16-Port Serial		RJ45 Serial Rolled port ma230,400 bps
16-Port USB		USB 2.0 interfaces Type A
M.2 Cellular + Antenna		For up to 24G/LTE modems
M.2 SATA		For up to 2mSATA storage modules
Storage		For 2.5" SATA (HDD/SDD) storage
Compute		Compute module (server on a card), provides independent compute capabilities.

Expansion Module Compatibility Chart

Expansion card	Slot 1	Slot 2	Slot 3	Slot 4	Slot 5
16-Port GbE Ethernet	✓	✓	✓	Secure Isolated Mode **	Secure Isolated Mode **
16-Port SFP	✓	✓	✓	Secure Isolated Mode **	Secure Isolated Mode **
16-Port Serial	✓	✓	✓	✓	✓
16-Port USB	✓	✓	✓	✓	✓
M.2 Cellular / WiFi	✓	✓	✓	✓	✓

Expansion card	Slot 1	Slot 2	Slot 3	Slot 4	Slot 5
8-Port SFP+	✓	✓	✓	Secure Isolated Mode **	Secure Isolated Mode **
8-Port POE+	✓	✓	✓	—	—
Compute	✓	✓	✓	Secure Isolated Mode **	Secure Isolated Mode **
Storage *	—	—	—	✓	✓
M.2 SATA *	—	—	—	✓	✓

NOTES:

(*) The Nodegrid Net Services Router supports a maximum of 2 SATA drives, which can be divided into 2 Storage cards or in one M.2 SATA card.

(**) The Secure Isolated Mode allows for the management of the cards as if they would be located in a normal Slot, but the network traffic is isolated from any other slot.

Configure Extra Storage Devices on NSR

IMPORTANT: When additional storage is added, special steps are required to allow the system to see more than one disk (i.e., use both storage and an LTE/M2.SATA module).

If using Storage and LTE/M2.SATA:

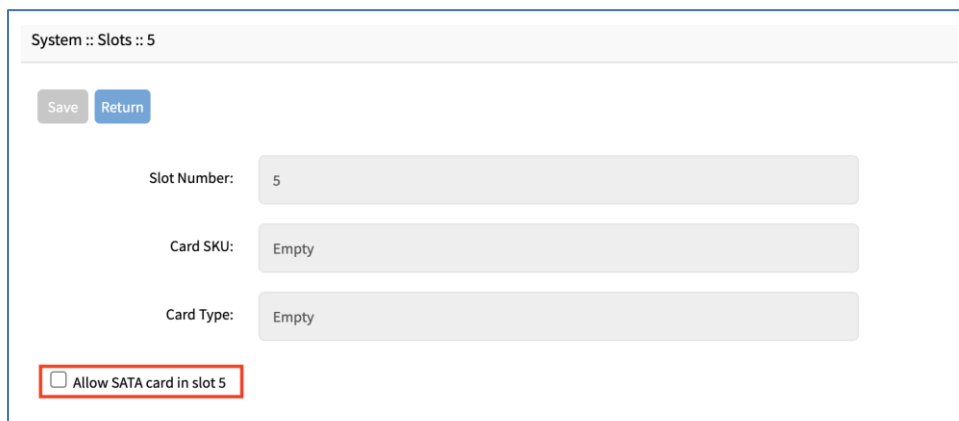
LTE/M2.SATA must be installed in slot 4.

Storage module must be installed in slot 5.

M2.SATA must be installed in Channel A.

Modem must be installed in Channel B.

1. In the WebUI, go to *System :: Slots :: 5*.



The screenshot shows the configuration page for Slot 5. At the top, there are 'Save' and 'Return' buttons. Below them are three input fields: 'Slot Number' with the value '5', 'Card SKU' with the value 'Empty', and 'Card Type' with the value 'Empty'. At the bottom of the form, there is a checkbox labeled 'Allow SATA card in slot 5', which is currently unchecked and highlighted with a red rectangular box.

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

Nodegrid Gate SR

The Nodegrid Gate SR brings agility to any network. Perfect for both data center and branch, Nodegrid Gate SR packs tremendous power in a small form factor – to provide a truly robust and dynamic, secure infrastructure management solution. Configuration and management of the Nodegrid Gate SR is easily done on the ZPE Cloud application.



Features include:

- Secure, fast, and consistent deployments across all your branches with ZPE Cloud
- Software Defined Networking, Network Function Virtualization, Guest OS, Kubernetes, and Docker capabilities
- Minimizes MTTR, downtime and expenses with secure, centralized remote device access & control
- Increases site reliability with open industry standard hardware and easy-to-use software
- Zero Touch Provisioning (ZTP) for fast and easy setup in remote locations
- Integrates with ZPE Cloud and ZPE Systems Nodegrid Manager for a vendor-neutral, unified management solution
- Direct Linux shell, HTML5 cross-device web access, and command line interface
- Modern 64-bit Linux Kernel for fast security patching and widespread software availability
- Kubernetes and Docker-optimized for quick, flexible script and application integration
- Extended Automation based on actionable real-time data
- Failover to 4G/LTE modem

- Gateway and multi-routing table capability
- VPN and IPsec
- DHCP server – extra IPs for your remote site or replace your current router altogether
- Firewall – built-in and turns on with a check box
- Secure – selectable encrypted cryptographic protocols and cipher suite levels, and a configuration checksum™
- Power control and monitoring – get alerts on suboptimal IT device health before malfunctions occur and solve problems automatically
- Orchestration - Puppet, Chef, Ansible, RESTful and ZPE Cloud
- WiFi hotspot ready via internal card or add your AP (Access Point) via a PoE+ port
- High density and flexible interfaces for greater connectivity

Nodegrid Gate SR Hardware Specifications

Item	Description
CPU	Intel Multi-core x86_64 CPU
Memory & Storage	8-32GB DDR4 DRAM 32GB Hardware encrypted SSD
Interfaces	8 RJ45 Serial ports 2 SFP+ (10G) 1 Gigabit (10/100/1000BT) Ethernet interfaces on RJ45 4 Gigabit (10/100/1000BT) Ethernet interfaces on RJ45 with Built-in Switch 4 PoE+ Gigabit (10/100/1000BT) Ethernet interfaces on RJ45 with Built-in Switch 2 GPIO (Digital I/O TTL level 5.5V max @ 64mA) 1 Digital Out Port (Signal MOSFET Digital Output 2.5V to 60V @ 500mA max) 1 Relay Port (NC relay contact max 24V @ 1A) 2 USB 3.0 Host on Type A 2 USB 2.0 Hosts on Type A 1 Wi-Fi (optional) 2 Cellular Slots with Dual SIM (optional) 1 HDMI port
Power	36V-75 VDC dual power input (redundant) Power consumption 45 W typical AC Power adapter (add-on), 100-240V~, 1.2A, 50-60Hz (operating temperature: -25C – 60C)
Physical	Front-Rear mounting brackets Size (L W H): 241.3 x 260.4 x 44.5 mm (9.5 x 10.25 x 1.75 in) Weight: .9 kg (2 lb) Shipping weight: 3.6 kg (8.0 lb) Shipping (L W H): 349.2 x 374.7 x 177.8 mm (13.75 x 14.75 x 7 in)
Environmental	Operation: 0 to 60° C (32 to 140° F), 5-95% RH, non-cond. Storage: -20 to 67° C (-4 to 153° F), 5-95% RH, non-cond.

Nodegrid Gate SR Front Interfaces



Interface	Description
DIO0	Digital I/O TTL level 5.5V ma@ 64mA
DIO1	Digital I/O TTL level 5.5V ma@ 64mA
OUT0	Signal MOSFET Digital Output 2.5V to 60V @ 500mA max
Relay Output	NC relay contact ma24V @ 1A
Console	Console MGMT Interface
USB	2 USB 2.0
HDMI	Monitor Interface
Channel A	Signal Strength indicator for Channel A
Channel B	Signal Strength indicator for Channel B
PWR	Power LED Green:· Solid - normal· Off - power is off
SYS	System LED Green:· Blinking – normal, Fast Blink - RST button Acknowledgment, Off or Solid - no activity
RST	Reset button:<3s system reset>10s reset to factory default and system reset
Power Switch	Power on/off Switch

Nodegrid Gate SR Rear Interfaces



Port	Description
PWR	Power LED Green:- Solid – normal, Off - power is off
V2- / GND / V2+	Power Connector for External Power Supply: 36V - 75VDC dual power input (redundant)
V1- / GND / V1+	Power Connector for External Power Supply: 36V - 75VDC dual power input (redundant)
PoE+	4 PoE+ Network Interface numbered 1 to 4- Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault) Right/Green (1000Base-T link speed),-Right/Orange (100BaseT link speed),-Right/Off (no link/cable disconnected/Ethernet fault)
NET	4 Network Interface numbered 5 to 8 Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault) Right/Green (1000Base-T link speed),-Right/Orange (100BaseT link speed),-Right/Off (no link/cable disconnected/Ethernet fault)
SFP+ 0	SFP+ Network Interface 0 Left/Yellow – Solid (Link UP), Off (no link/cable disconnected)- Right/Green – Solid (Link UP), Blinking (Activity), Off (no link/cable disconnected)
SFP+ 1	SFP+ Network Interface 1- Left/Yellow – Solid (Link UP), Off (no link/cable disconnected)- Right/Green – Solid (Link UP), Blinking (Activity), Off (no link/cable disconnected)
ETH0	Network Interface- Left/Yellow – Solid (Link UP), Blinking (data activity), Off (no link/cable disconnected/Ethernet fault)- Right/Green – Solid (1000Base-T link speed), Off (100/10BaseT link speed or off)
USB	2 USB 3.0 Port
Serial	Serial Interfaces 1-8- Left/Orange DCD/DTR – On (port open and/or cable connected), Off (not ready) Right/Green RX/T- Blinking (data activity), Off (no activity)

Nodegrid Hive SR

The Nodegrid Hive SR is used for SD-WAN and SD-Branch applications.



NOTE; Hive SR default system profile is Gateway Profile.

Features include:

- Three M.2 slots for flexible combinations of up to Wifi 6, 5G and NVMe drives
- Four SIM card slots for up to two cellular modems
- Four RJ-45 Network Ports (2.5G)
- Two SFP+
- Two 1GbE Combo (RJ45/SFP)
- +12V DC power
- Fan-cooled
- Rack or wall mountable
- Five antenna slots.
- Zero Touch Provisioning (ZTP) for fast and easy setup in remote locations

- Integrates with ZPE Cloud and ZPE Systems Nodegrid Manager for a vendor-neutral, unified management solution

Nodegrid Hive SR Hardware Specifications

Item	Description
CPU	Intel Atom C3558 - 4 cores
Memory & Storage	DDR4 16 GB, bus 64-bit, with ECC 16GB eMMC 128 GB NVMe SSD
Interfaces	4 RJ-45 Network Ports (2.5G) 2 SFP+ 2 1GbE Combo (RJ45/SFP) Console: Cisco RJ45 and micro-USB 2 USB 3.0 Host on Type A 4 SIM card slots Expansion Slot-0: M.2 Key-M (x2 PCIe Gen3), 128GB NVMe Channel-A (expansion slot-2): M.2 Key-B (x1 PCIe Gen3, USB3/2) optional cards: 5G cellular card or EM7565 Channel-B (expansion slot-1): M.2 Key-B (x1 PCIe Gen3, USB3/2) optional cards: Enli Wi-Fi 6 card, Wi-Fi 5 card, NVMe card or EM7565 second card.
Power	+12V DC Locking Barrel Jack External 60W PSU Power consumption 20W max (board only), 40W (includes max peripheral power)
Physical	Fan cooled. Rackmount accessory kit: Rackmount bracket, USB patch cables Wall-mount accessory kit: Unit mounting brackets, PSU mounting bracket – with hardware Size (L W H): 200 x 256 x 44 mm (7.87.x-10.07-x.1.73 in) Weight: .9 kg (2 lb) Shipping weight: 3.6 kg (8.0 lb) Shipping (L W H): 349.2 x 374.7 1x 77.8 mm (13.75 x 14.75 x 7 in)
Environmental	Operation: 0 to 60° C (32 to 140° F), 5-95% RH, non-cond. Storage: -20 to 67° C (-4 to 153° F), 5-95% RH, non-cond.

Nodegrid Hive SR Side Interfaces



Interface	Description
Left LED (PWR/Status)	AMBER (has power, standby). During BOOT: BLUE (unit starts boot) Operating: GREEN (system booted), blinking RED (alarm), solid RED (reset button pressed more than 10sec)
Middle LED	During BOOT: OFF Operating: M.2 - Channel A signal strength – OFF (no signal), solid RED (poor), solid AMBER (fair), solid BLUE (good), solid GREEN (excellent)
Right LED	During BOOT: OFF Operating: M.2 - Channel B signal strength – OFF (no signal), solid RED (poor), solid AMBER (fair), solid BLUE (good), solid GREEN (excellent)
(optional) SIM CARDS	SIM Slot-A1 SIM Slot-A2 SIM Slot-B1 SIM Slot-B2
USB	2 USB 3.0
Protruding Button	2-7s (graceful OS shutdown and set status bit) <4s (no action) 4-7s (graceful OS shutdown) >7s (immediate CPU shutdown)
Recessed Button	<10s (hardware reset) >10s (Factory default unit and reboot)

Nodegrid Hive SR Rear Interfaces



Port	Description
MicroUSB	Console Port
Console Port	Cisco RJ-45 Left LED (not used) Right LED: Green Solid (RJ-45 cable connected); Off (microUSB)

Port	Description
WAN0 (1G)	CAT 5e or CAT 6 cable. Left LED (speed) Solid Amber (1G); Solid Green (100Mb); Off (10Mb). Right LED (data traffic): Solid Green (Link Up); Blinking Green (data traffic).
WAN1 (1G)	CAT 5e or CAT 6 cable Left LED (speed) Solid Amber (1G); Solid Green (100Mb); Off (10Mb). Right LED (data traffic): Solid Green (Link Up); Blinking Green (data traffic).
SFP0 (10G)	SFP+ Network Interface 0 Left LED: Solid Green (link ready), Off (no link). Right LED (data traffic): Solid Green (Link Up); Blinking Green (data traffic).
SFP1 (10G)	SFP+ Network Interface 1 Left LED: Solid Green (link ready), Off (no link). Right LED (data traffic): Solid Green (Link Up); Blinking Green (data traffic).
LAN[0-3]	Network Ports Left LED (speed) Solid Green(2.5G); Solid Amber (1G); Off (10/100M). Right LED (data traffic): Solid Green (Link Up); Blinking Green (data traffic).
Antenna Connection	(optional) 5G/LTE
Antenna Connection	(optional) WiFi Antenna
DC Power Adaptor	12VDC for External Power Supply

Nodegrid Bold SR

The Nodegrid Bold SR is an open platform appliance designed for secure access and control over remote and IoT devices at the EDGE of your network. The Bold SR supports cellular failover, Network Function Virtualization (NFV), and Software Defined Networking with a focus on SD-WAN.



Features include:

- 1U high, compact size, high processing power
- Ideal for Software Defined Networking
- Network Function Virtualization
- Cellular failover
- WiFi hotspot & client
- Multiple Interfaces

Nodegrid Bold SR Hardware Specifications

Item	Description
CPU	Intel Multi-core x86_64 CPU
Memory & Storage	4 GB of DDR3 DRAM 32 GB SATADOM SSD (Upgradeable)
Interfaces	8 RJ45 Serial ports 1 Gigabit (10/100/1000BT) Ethernet interfaces on RJ45 4 Gigabit (10/100/1000BT) Ethernet interfaces on RJ45 with Built-in Switch 2 USB 3.0 Host on Type A 2 USB 2.0 Hosts on Type A 1 Wi-Fi and Bluetooth Slot (optional) 2 Cellular CAT-12 Slots with Dual SIM (optional) 1 VGA port

Item	Description
Power	12VDC via external 100-240 VAC, 50/60 Hz adapter Power consumption 25 W typical
Physical	Front-Rear mounting brackets Size (L x W x H): 142 x 201 x 44 mm (5.5 x 7.9 x 1.73 in) Weight: 1.2 kg (2.6 lb) Shipping weight: 2.3 kg (5.0 lb) Shipping (L x W x H): 313 x 313 x 140 mm (12.3 x 12.3 x 5.5 in)

Nodegrid Bold SR Front Interfaces



Port	Description
Channel A	Signal Strength indicator for Channel A
Channel B	Signal Strength indicator for Channel B
Console	Console MGMT Interface
PWR	Power LED Green:· Solid - normal,· Off - power is off
SYS	System LED Green:· Blinking - normal· Fast Blink - RST button Acknowledgment· Off or Solid - no activity
RST	Reset button:<3s system reset,>10s configuration factory reset and system reset
Power Switch	Power on/off Switch

Nodegrid Bold SR Rear View



Port	Description
PWR IN	Power Socket for external Power Supply
Monitor	VGA Interface
ETH0	Network Interface Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault) Right/Green (1000Base-T link speed), Right/Orange (100BaseT link speed), Right/Off (no link/cable disconnected/Ethernet fault)
USB	2 USB 2.0 Port 2 USB 3.0 Port
ETH1	Network Interface(NET) Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault) Right/Green (1000Base-T link speed), Right/Orange (100BaseT link speed), Right/Off (no link/cable disconnected/Ethernet fault)
ETH2	Network Interface(NET) Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault) Right/Green (1000Base-T link speed), Right/Orange (100BaseT link speed), Right/Off (no link/cable disconnected/Ethernet fault)
ETH3	Network Interface(NET) Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault) Right/Green (1000Base-T link speed), Right/Orange (100BaseT link speed), Right/Off (no link/cable disconnected/Ethernet fault)
ETH4	Network Interface(NET) Left/Green – Blinking (data activity), Solid (ready), Off (no link/cable disconnected/Ethernet fault) Right/Green (1000Base-T link speed), Right/Orange (100BaseT link speed), Right/Off (no link/cable disconnected/Ethernet fault)

Port	Description
Serial	Serial Interfaces 1-8 Left/Orange DCD/DTR – On (port open and/or cable connected), Off (not ready) Right/Green RX/T – Blinking (data activity), Off (no activity)

Nodegrid Link SR

The Nodegrid Link SR brings agility to the branch network and packs tremendous power in a compact design. Truly robust and dynamic, secure infrastructure management. Configure and manage Link SR via the ZPE Cloud to get your Branch / IoT / M2M / Kiosk / ATM / Remote Locations up and running quickly and easily.



Features include:

- Secure, fast and consistent deployments across your branches with the ZPE Cloud
- Combines Cellular gateway and WiFi Access Point (AP) with power input via PoE or Power Adapter
- Software Defined Networking, Network Function Virtualization, Guest OS, Kubernetes, and Docker capabilities
- Minimizes MTTR, downtime and expenses with secure, centralized remote device access & control
- Increases site reliability with open industry standard hardware, and easy-to-use software

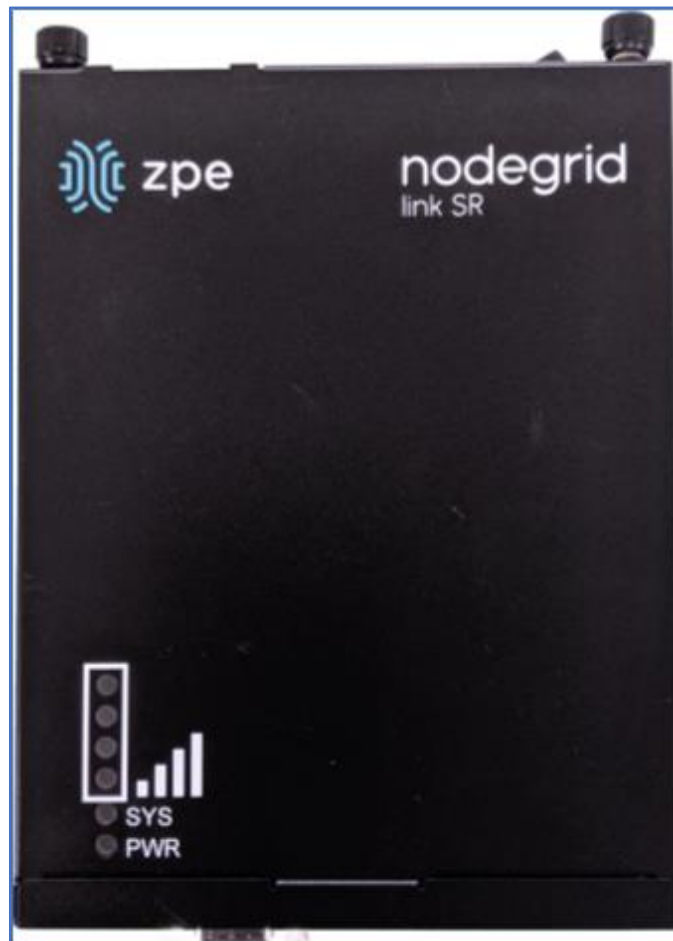
- Zero Touch Provisioning (ZTP) for fast and easy setup in remote locations
- Integrates with ZPE Cloud and ZPE Systems Nodegrid Manager vendor-neutral, unified management solution
- Direct Linux shell, HTML5 cross-device web access and command line interface
- Modern 64-bit Linux Kernel for fast security patching and widespread software availability
- Kubernetes and Docker-optimized for quick, flexible script and application integration
- Extended Automation based on actionable real-time data
- Failover to 4G/LTE modem
- Linkway and multi-routing table capability
- VPN and IPsec
- DHCP server – extra IPs for your remote site or replace your current router altogether
- Firewall – built-in and turns on with a checkbox
- Secure – selectable encrypted cryptographic protocols and cypher suite levels, configuration checksum™
- Power control and monitoring – get alerts on suboptimal IT device health before malfunctions occur and solve problems automatically
- Orchestration - Puppet, Chef, Ansible, RESTful and ZPE Cloud
- High density and flexible interfaces for greater connectivity

Nodegrid Link SR Hardware Specifications

Item	Description
CPU	Intel Multi-core x86_64 CPU
Memory & Storage	4-8GB of DDR3 DRAM 16GB Self Encrypted Disk (SED) 32 GB SATADOM SSD (Upgradeable)
Interfaces	1 RJ45 Serial ports 1 SFP (1G) 1 Gigabit (10/100/1000BT) Ethernet interfaces on RJ45 with PoE in 2 GPIO Port (Digital I/O TTL level 5.5V max @ 64mA) 2 Digital Out Port (Signal MOSFET Digital Output 2.5V to 60V @ 500mA max) 2 USB 2.0 Hosts on Type A 1 Wi-Fi (optional) 1 Cellular Slots with Dual SIM (optional) 1 VGA port

Item	Description
Power	10V - 57VDC power input AC Power adapter (add-on) 100-240V~ 50-60Hz 1.5A PoE power input Power consumption 15 W typical
Physical	DIM Rail and Wall Mountable Size (L x W x H): 170 130 55 mm (6.69 x 5.11 x 2.16 in) Weight: 1.58 kg (2.3 lb) Shipping weight: 1.58 kg (3.5 lb) Shipping (L x W x H): 228.6 x 342.9 x 88.9 mm (9 x 13.5 x 3.5 in)
Environmental	Operating: 0 to 60°C (32 to 140° F), 5-95% RH, non-cond. Storage: -20 to 67° C (-4 to 153° F), 10-90% RH, non-cond.

Nodegrid Link SR Top View



Designation	Description
BARS	Signal Strength indicator

Designation	Description
PWR	Power LED Green:- Solid - normal- Off - power is off
SYS	System LED Green:- Blinking - normal- Fast Blink - RST button Acknowledgment- Off or Solid - no activity

Nodegrid Link SR Front Interfaces



Designation	Description
SFP 0	SFP Network Interface 0 Left/Yellow – Blinking (data activity), Solid (link up), Off (no link/cable disconnected) Right/Green – Solid (1000Base-T link speed), Off (no link/cable disconnected)
Serial	Serial Interface 1- Left/Orange DCD/DTR – Solid (port open and/or cable connected), Off (not ready) Right/Green RX/T- Blinking (data activity), Off (no activity)
Console	Console MGMT Interface
USB	2 USB 2.0
VGA	Monitor Interface

Nodegrid Link SR Rear Interfaces



Item	Description
Power Switch	Power on/off Switch
V1- / GND / V1+	Power Connector for External Power Supply: 10V - 57VDC power input
ETH0	1 Gigabit (10/100/1000BT) Ethernet with PoE in Left/Yellow – Solid (link up), Blinking (data activity), Off (no link/cable) Right/Green - Solid: (1000Base-T link speed), Off (10/100BaseT link speed)
DIO0	Digital I/O TTL level 5.5V ma @ 64mA
DIO1	Digital I/O TTL level 5.5V ma @ 64mA
OUT0	Signal MOSFET Digital Output 2.5V to 60V @ 500mA max
OUT1	Signal MOSFET Digital Output 2.5V to 60V @ 500mA max
RST	Reset button:<3s system reset>10s reset to factory default and system reset

Nodegrid Mini SR

The Nodegrid Mini SR is a miniature PC designed to be tough, capable, versatile and user-friendly. The unique fan-less design eliminates the need for any maintenance after installation. The device is designed to minimize size and maximize capabilities, durability and thermal performance.



Nodegrid Mini SR Hardware Specifications

Item	Description
CPU	Intel Apollo Lake CPU
Memory & Storage	1x SO-DIMM 204-pin DDR3L SDRAM Up to 16 GB RAM eMMC M.2 SATA 2.5" storage*
Interfaces	1 HDMI 1.4b up to 3840 x 2160 @ 30Hz 1 Display Port 1.2 up to 4096 x 2160 @ 60 Hz (via Mini DP connector) 1 LAN1: Intel I211 GbE controller (RJ-45) 1 LAN2: Intel I211 GbE controller (RJ-45) 2 USB 3.0 2 USB 2.0 1 Serial communication ports 1 COM1: RS232 via mini serial connector
Power	Unregulated 7 - 20VDC input Power consumption 5W to 15W depending on configuration and system load
Physical	Size (L x W x H): 112 mm X 84 mm X 34 mm (4.41 x 3.31 x 1.34 in) Weight: 0.35 kg (0.77 lb) Shipping weight: 0.91 kg (2 lb) Shipping (L x W x H): 305 x 127 x 63.5 mm (12 x 5 x 2.5 in)

Item	Description
Environmental	Operating: 0 to 45°C (32 to 113° F), 5-95% RH, non-cond. Storage: -20 to 67° C (-4 to 153° F), 10-90% RH, non-cond.

Nodegrid Mini SR Rear Interfaces



Designation	Description
USB	2 USB 2.0
USB	2 USB 2.0
HDMI	1 HDMI 1.4b up to 3840 x 2160 @ 30Hz
Mini DP	1 Display Port 1.2 up to 4096 x 2160 @ 60 Hz (via Mini DP connector)
DC In	DC Power In connector (Unregulated 7 - 20VDC input)
RS232	COM1: RS232 via mini serial connector
LAN1	1 LAN1: Intel I211 GbE controller (RJ-45)
LAN2	1 LAN2: Intel I211 GbE controller (RJ-45)

Nodegrid Mini SR Front Interfaces



Item	Description
Power button	Power on/off Switch
USB 3.0	USB 3.0 connector
Line-in	
Line-out	
LED1	Yellow – Solid (link up), Blinking (data activity), Off (no link/cable) Green – Solid: (1000Base-T link speed), Off (10/100BaseT link speed)
USB 3.0	USB 3.0 connector.
LED2	Yellow – Solid (link up), Blinking (data activity), Off (no link/cable) Green – Solid: (1000Base-T link speed), Off (10/100BaseT link speed)

Nodegrid Manager

The Nodegrid Manager provides you with a unified solution to control compute, network, storage, and smart power assets.

Nodegrid Manager Hardware Requirements (physical or virtual devices)

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-- LinuOS




Installation





Hardware Installation

Refer to the “Quick Install Guide” provided with the boxed unit.

Shipping Box Contents

Accessories

Model	Mounting brackets	Power cables	Loop-back adapter	Console adapter	Network cable	Quick start guide & safety sheet
Nodegrid Serial Console - T Series	Yes	Yes	Legacy 	Z000036	Yes	Yes
Nodegrid Serial Console - R Series - TxxR	Yes	Yes	Cisco 	Z000014	Yes	Yes
Nodegrid Serial Console - S Series - TxxS	Yes	Yes	Legacy/Cisco 	Z000015Z000036	Yes	Yes

Model	Mounting brackets	Power cables	Loop-back adapter	Console adapter	Network cable	Quick start guide & safety sheet
Nodegrid Net Services Router	Yes	Yes	Cisco 	Z000014	Yes	Yes
Nodegrid Bold Services Router	Yes	External Power Supply	Cisco 	Z000014	Yes	Yes
Nodegrid Link Services Router	No	Optional External Power Supply	Cisco 	Z000014	Yes	Yes
Nodegrid Gate Services Router	Yes	Optional External Power Supply	Cisco 	Z000014	Yes	Yes

Each unit is shipped with multiple accessories. The table below lists the contents of the box.

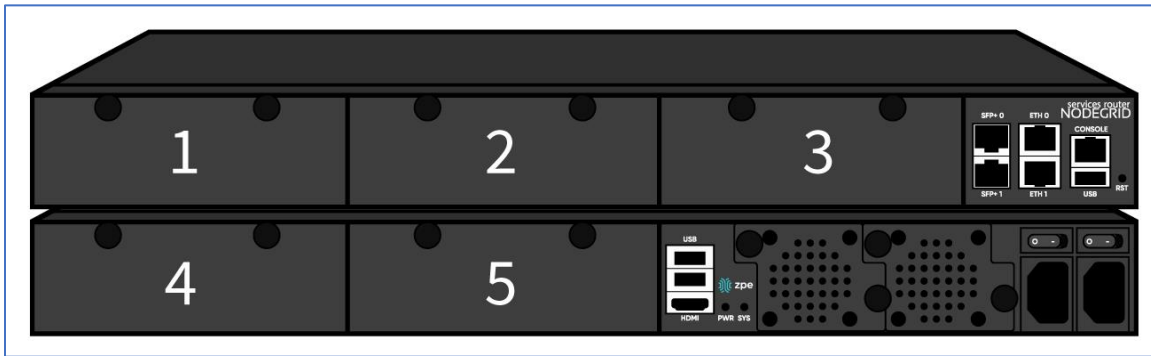
Installation of Modules for Nodegrid Net Services Router

The Nodegrid Net Services Router supports a variety of different modules. All modules are not hot-swappable and need to be installed before the unit is powered up. The modules should be installed in an ESD protected environment to avoid damage. To install a card, follow the steps below:

1. Ensure that the Nodegrid Net Services Router is powered off.
2. Turn off the power supplies on the Nodegrid Net Services Router.
3. Unscrew the blanking panel which covers the slot in which the module should be installed.
4. Unbox the card and insert it into the appropriate slot.
5. Fix the card with the provided screws.
6. The Nodegrid Net Services Router can now be turned on.

NOTE: The blanking panel should be kept for later use. For thermal efficiency and safety, each unused slot needs to be covered with a blanking panel.

Module Compatibility Layout



Nodegrid Net Services Router Expansion Module Compatibility Chart

Expansion card	Slot 1	Slot 2	Slot 3	Slot 4	Slot 5
16-Port GbE Ethernet	✓	✓	✓	Secure Isolated Mode **	Secure Isolated Mode **
16-Port SFP	✓	✓	✓	Secure Isolated Mode **	Secure Isolated Mode **
16-Port Serial	✓	✓	✓	✓	✓
16-Port USB	✓	✓	✓	✓	✓
M.2 Cellular / WiFi	✓	✓	✓	✓	✓
8-Port SFP+	✓	✓	✓	Secure Isolated Mode **	Secure Isolated Mode **
8-Port POE+	✓	✓	✓	–	–
Compute	✓	✓	✓	Secure Isolated Mode **	Secure Isolated Mode **
Storage *	–	–	–	✓	✓
M.2 SATA *	–	–	–	✓	✓

NOTES:

(*) The Nodegrid Net Services Router supports a maximum of 2 SATA drives, which can be divided into 2 Storage cards or in one M.2 SATA card.

(**) The Secure Isolated Mode allows for the management of the cards as if they would be located in a normal Slot, but the network traffic is isolated from any other slot.

M.2 Cellular Antenna Placement

Correct antenna placement is critical to ensure proper functionality of the M.2 Cellular expansion card. Two antennas (main and auxiliary) are required for each card and should be separated to improve signal quality.

Single Card Configuration

For single card applications, antenna placement is as follows:

Channel A

Main in slot 1

Auxiliary in slot 6

The A and B channel strength indicators do not directly correspond to the antenna slot positions (Slots 4-6 are not specifically reserved for channel B).

Dual Card Configuration

For dual card applications, four antennas (2 main and 2 auxiliary) will be used. Antenna placement is as follows:

Channel A

Main in slot 1

Auxiliary in slot 4

Channel B

Main in slot 3

Auxiliary in slot 6

Device Power Connections

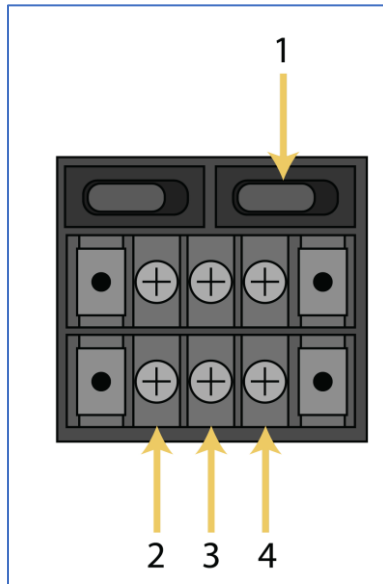
DC Power

DC power is connected to DC-powered equipment with three wires: Return (RTN), Ground and 48 VDC.

WARNING: It is critical that the power source supports the DC power requirements of your Nodegrid. Make sure that the power source is the correct type and that the DC power cables are in good condition before proceeding. Failure to do so could result in personal injury or damage to the equipment.

WARNING: Wiring to power from a DC supply may be confusing, especially in telecom racks, where the supply's positive wire (usually of red color) goes to the ground, and the hot wire (usually of black color) carries the -48VDC. In case of any doubt, consult a certified electric technician before proceeding with connections. Failure to do the right connections could result in personal injury or damage to the equipment.

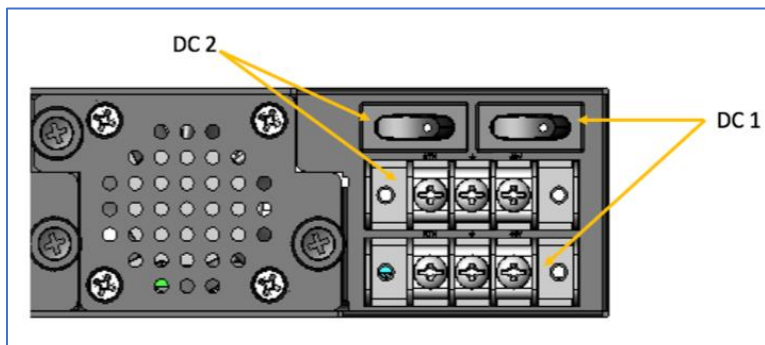
Dual DC Power Connection Terminal Block



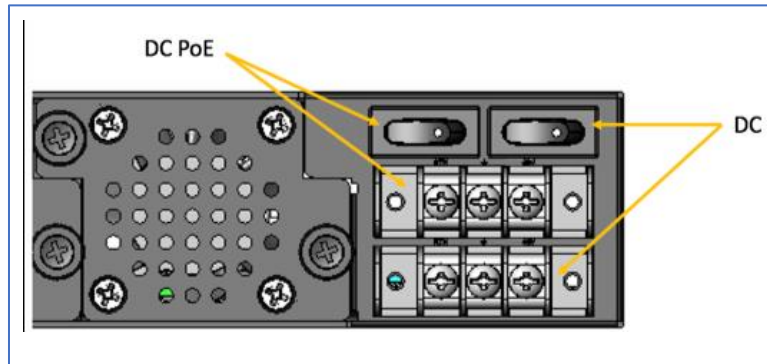
DC Power Block Terminals

Number	Description
1	Power Switch
2	RTN (Return)
3	Ground
4	48 VDC

DC association - terminal power source and switch



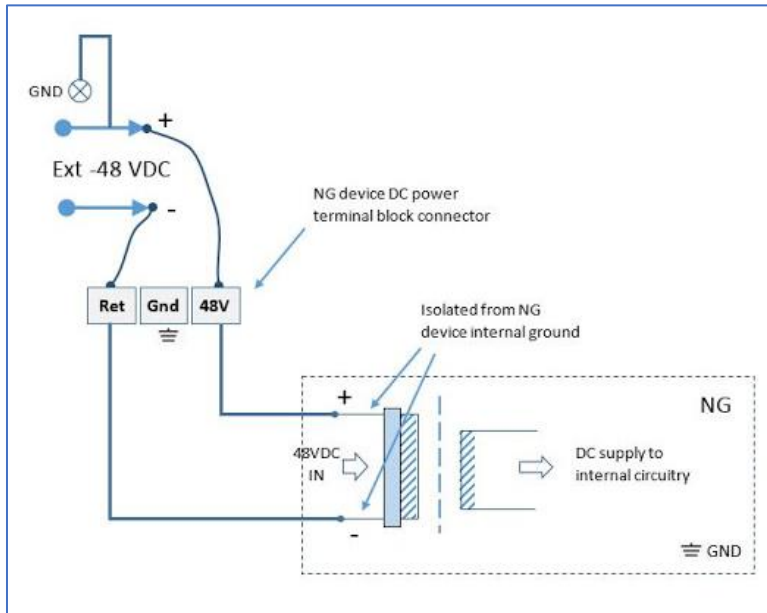
NSR Single DC + PoE Power Connection Terminal Block



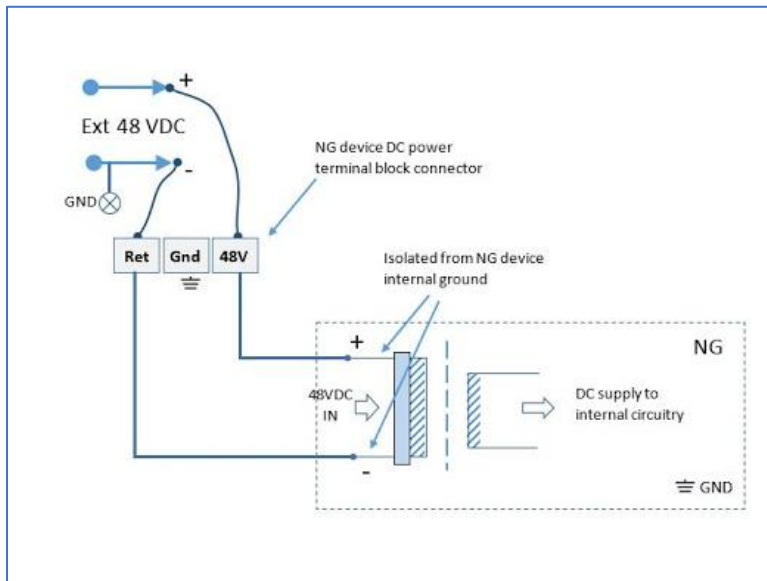
Connect a Nodegrid device to DC Power

1. Make sure the device is turned off.
2. Make sure DC power cables are **not** connected to a power source.
Never work on powered wires.
3. On the DC power block, remove the protective cover. (Slide to the left or right to remove.)
4. Loosen all three DC power connection terminal screws.
Connect return lead to the RTN terminal.
Connect ground lead to the GND \perp terminal.
Connect 48 VDC lead to the 48 VDC terminal.
5. Tighten the screws.
6. Slide the DC terminal block protective cover back into place.
7. If device has dual-input DC terminals, repeat DC power connection steps for the second terminal block.
8. Connect the DC power cables to the DC power source.
9. Turn on the DC power source.
10. (optional) Connect a serial client (set as 115200 8N1) to the console port (Teraterm, puTTY, etc).
11. Turn power on to the serial client.
12. On the connected serial client, double-check booting messages.
13. For the connected devices, turn on the power switches.
14. Connect the DC power cables to the DC power source.
15. Turn on the DC power source.
16. Turn on the unit.
17. Turn on the power switches of the connected devices.

-48VDC supply

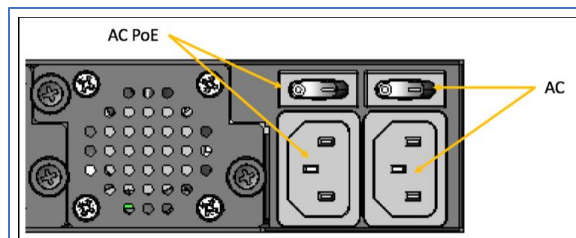


+48VDC supply



AC Power

This is the AC diagram for the NSR models with PoE+ support.







Rack Mounting

All units shipped with rack mounting brackets can be mounted to fit a standard 19" rack. Two rack mounting brackets are provided in the box as outlined in the What is in the box section. The remainder of this document will refer to "rack or cabinet" as "rack".

Some units are actively cooled by fans. These units must be properly mounted into the rack to ensure the fans blow into the correct direction. The fan direction can be determined from the part number of the unit.

Rack Mounting

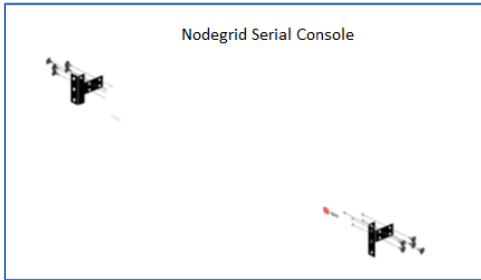
Model	Part Number	Cooled	Airflow
Nodegrid Serial Console - T Series	NSC-Txx-xxxx-xxx	Passive	N/A
Nodegrid Serial Console - R Series	NSC-TxxR-xxxx-xxx	Passive	N/A
Nodegrid Serial Console - S Series	NSC-TxxS-xxxx-xxx-F	Active	Front-Back (air in) 
Nodegrid Serial Console - S Series	NSC-TxxS-xxxx-xxx-B	Active	Back-Front (air out) 
Nodegrid Net Services Router	NSR-xxxx-xxx	Active	Front-Back (air out) 
Nodegrid Net Services Router	NSR-xxxx-xxx	Active	Back-Front (air in) 
Nodegrid Bold Services Router	BSR-xx-xxxx	Passive	N/A
Nodegrid Link Services Router	LSR-xx-xxxx	Passive	N/A
Nodegrid Gate Services Router	GSR-xx-BASE	Passive	N/A

Model	Part Number	Cooled	Airflow
Nodegrid Gate Services Router	GSR-xx-UPGx	Active	Front-Back (air out)

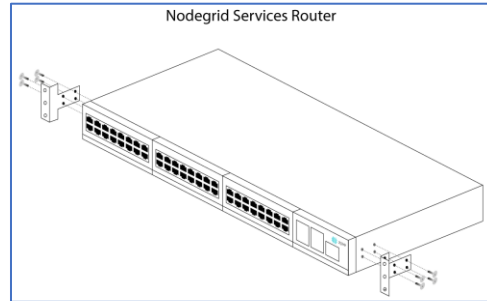
Rack Installation

1. Install the rack mounting brackets with the provided screws as shown in the diagrams below

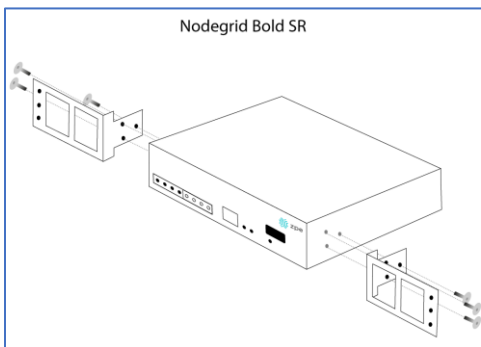
Nodegrid Serial Console



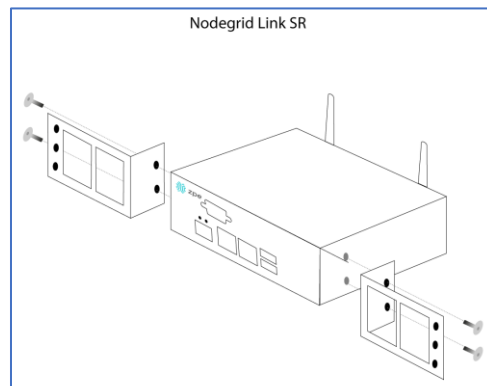
Nodegrid Net Services Router



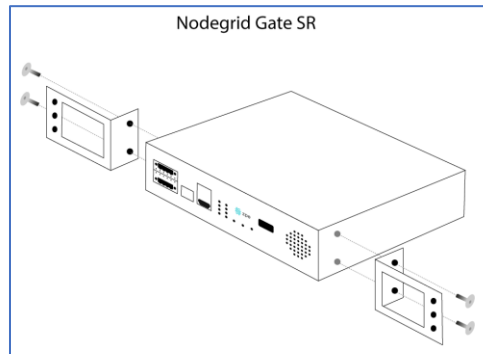
Nodegrid Bold SR



Nodegrid Link SR

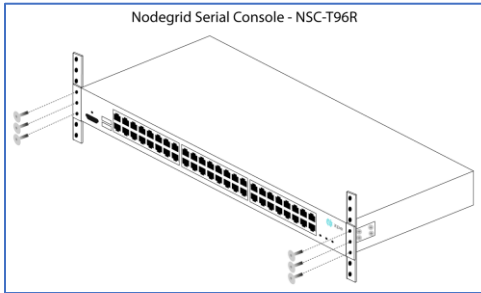


Nodegrid Gate SR

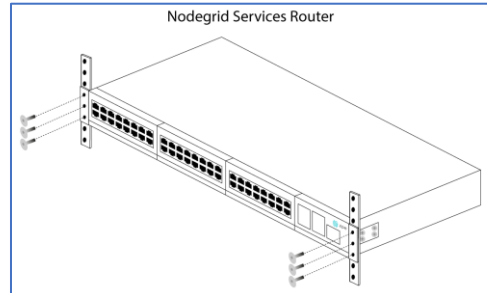


2. Locate the position on the rack where you would like to mount the unit and ensure the slot is clear of any obstructions.
3. Slide the unit into the rack and align the mounting bracket screw holes with the screw holes on the rack as shown below:

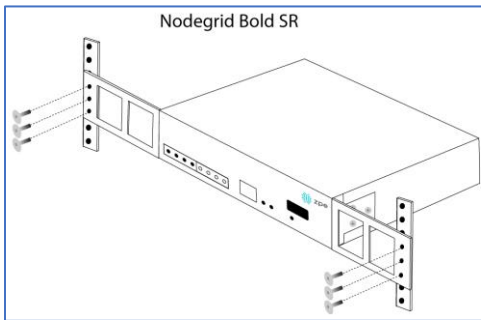
Nodegrid Serial Console



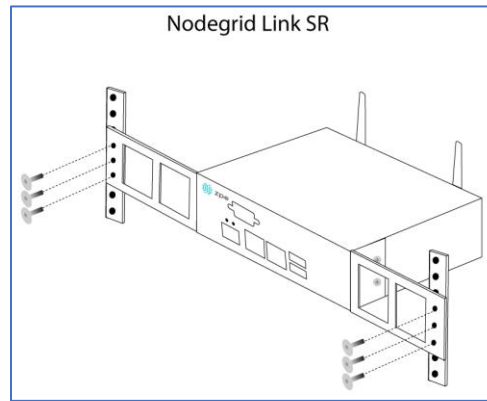
Nodegrid Net Services Router



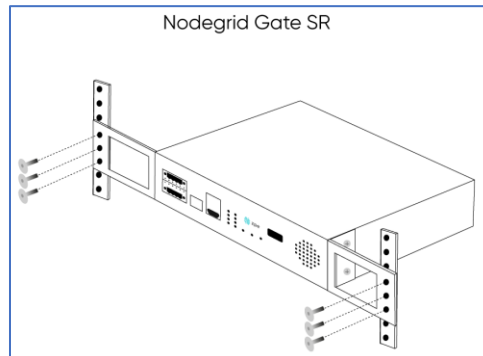
Nodegrid Bold SR



Nodegrid Link SR



Nodegrid Gate SR



4. While holding the unit in position, insert the rack mount screws (not included) and turn them clockwise until they are snug, but not tight.
5. Once all the screws are installed, check to ensure that the unit is supported and still in the correct position.
6. Tighten the screws securely in place to complete the installation.

Network Connection

Depending on model and version, the unit has a minimum of two copper Ethernet ports or two SFP+ ports. Connect the proper network cables (CAT5e, CAT6, CAT6A) from the network switch port to any available unit network ports. For models with SFP+ ports, before the unit is turned on, install the SFP+ module and connect the appropriate cables.

Power Cord(s) Connection

The Nodegrid unit can have one or multiple power supplies (AC or DC). Connect all the power supplies with appropriate cables to an available power source (usually a Rack PDU. If the unit was shipped with one power supply, that unit has no power failure redundancy. Units with two power supplies provide redundancy against power failures. Make sure these power supplies are connected to two independent power sources.

NOTE: On the Nodegrid Net Services Router with PoE support, the second power supply specifically powers the PoE feature – and does not provide power outage redundancy.

When all power supplies are appropriately connected to a power source, power can be turned on.

Connect Devices

Serial Devices

NOTE: To avoid EMC issues, always use good quality network cable for all port connections.

The cabling and adapters needed between the unit serial ports and the serial devices' console port are determined by their pin-outs.

Newer serial devices (routers, switches, and servers) use either a DB9, RJ45 or USB port as console ports. See the manufacturer's manual for serial device port pin-out specs. Generally, the RJ45 console port uses the Cisco-like pin-out.

Required Cabling Ports/Pin-outs

Model	Port type	Pin-out	Device port - RJ45 (Legacy)	Device port - RJ45 (cisco)	Device port - DB9	Device port - USB
Nodegrid Serial Console - T Series	RJ45	Legacy	CAT5e cable	CAT5e cable plus Z000039 crossover adapter	CAT5e cable plus Z000036 crossover adapter	USB
Nodegrid Serial Console - R Series	RJ45	Cisco	-	CAT5e cable	CAT5e cable plus Z000015 crossover adapter	USB
Nodegrid Serial Console - S Series	RJ45	Auto-Sensing (Legacy/Cisco)	CAT5e cable	CAT5e cable	CAT5e cable plus Z000015 crossover adapter	USB

Model	Port type	Pin-out	Device port - RJ45 (Legacy)	Device port - RJ45 (cisco)	Device port - DB9	Device port - USB
Nodegrid Net Services Router	RJ45	Cisco	-	CAT5e cable	CAT5e cable plus Z000015 crossover adapter	USB
Nodegrid Bold Services Router	RJ45	Cisco	-	CAT5e cable	CAT5e cable plus Z000015 crossover adapter	USB
Nodegrid Link Services Router	RJ45	Cisco	-	CAT5e cable	CAT5e cable plus Z000015 crossover adapter	USB
Nodegrid Gate Services Router	RJ45	Cisco	-	CAT5e cable	CAT5e cable plus Z000015 crossover adapter	USB

If the serial device's RJ45 does not have the Cisco-like pin-out, or there is a question on connecting a serial device to the unit, contact [ZPE Systems Technical Support](#) for assistance.

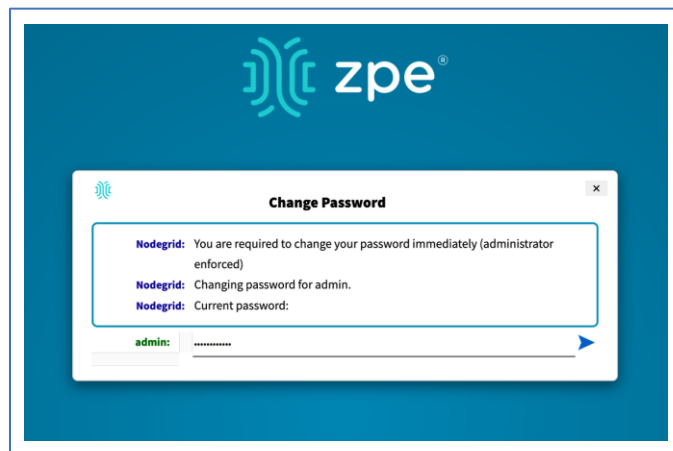
IP Devices

NOTE: To avoid EMC issues, always use good quality network cable for all port connections.

All IP based devices are directly connected to a network interface on a Nodegrid unit, or connected through an existing network infrastructure. If the devices are directly connected, use standard network cables (CAT 5, CAT6, CAT6e) for Ethernet connections, or an appropriate fiber cable.

Connect to a Nodegrid Device

On the first connection to a Nodegrid device, the login prompt requires an immediate password change.



NOTE: On new devices, SSH is disabled by default.

Connect to the Console Port

Use the provided CAT5e and RJ45-DB9 Z000036 adapter/cable to communicate with the Nodegrid unit.

1. Connect one end of the CAT5e cable to the Nodegrid console port.
2. Connect the other end to the RJ45-DB9 adapter.
3. Plug the adapter into the PC's DB9 COM port.

If no DB9 COM port, use a USB-DB9 adapter (not provided).

4. On the PC, use a serial application (Xterm, TeraTerm, PuTTY, SecureCRT) to open a terminal session to the COM port:
5. Set it to: 115200bps, 8 bits, no parity, 1 stop bit, no flow control settings.

NOTE: See system information to find the COM port.

ETH0 Connection

By default, the ETH0 interface is configured to listen for DHCP requests. If no DHCP Server is available, the unit uses the default IP address: 192.168.160.10. Use a browser to access the unit: [https://\[DHCP ASSIGNED IP\]](https://[DHCP ASSIGNED IP]) or <https://192.168.160.10>. If needed, a SSH client can be an alternative access.

Connection through ETH0

Setting	Value
DHCP	enabled
Fall-back IP	yes
Default IP	192.168.160.10/24
Default URL	https://192.168.160.10
Default SSH	SSH admin@192.168.160.10
DHCP	enabled

WiFi Connection

The Nodegrid device is pre-configured to act as a WiFi hotspot with a built-in WiFi module or a USB WiFi adapter. When turned on, the device automatically presents a WiFi network with the SSID = **Nodegrid**. The password is the device's serial number.

The Nodegrid device provides the IP address to clients in the network 192.168.162.0/24. The client can be configured statically with a valid IP address in the 192.168.162.<2-254> range, bitmask 24.

Bluetooth® Connection

Zero Touch Provisioning (ZTP) via Bluetooth allows faster deployment, even when the network infrastructure is not in place. The only additional equipment needed is a smartphone or laptop with Bluetooth tethering enabled.

On Nodegrid devices configured with Bluetooth hardware, this is enabled by default. Bluetooth is enabled/disabled via the **Security** tab or **Network Settings**.

NOTE: For devices without Bluetooth, configure an adapter. Contact ZPE Support for the latest list of compatible adapters.

To connect via Bluetooth:

1. On your smartphone or laptop, enable tethering.
2. On the Bluetooth screen, locate and click on the new Nodegrid device.
3. Once paired, Nodegrid connects to the ZPE Cloud and automatically begins the ZTP process.

KVM Port Connection

The Nodegrid unit can be directly configured with KVM.

1. Connect a HDMI cable to the monitor and the device's HDMI interface.

NOTE: The Nodegrid Bold SR uses a VGA port. If monitor only has HDMI, use a HDMI to DVI-D adapter to connect.

2. Connect a USB Keyboard and Mouse to the USB ports.

NOTE: The keyboard and mouse must support Linux. Windows-only devices are not supported. This limitation generally affects devices which use a USB wireless dongle.

3. The login prompt indicates the connection is active.

I/O Ports (GPIO)

Nodegrid Gate SR supports two digital I/O ports (DIO0, DIO1), one digital output port (OUT0) and one relay port (1A@24V).

Nodegrid Link SR supports two digital I/O ports (DIO0, DIO1) and two digital output ports (OUT0, OUT1).

DIO0 and DIO1 can be independently configured as input or output. The DIO0 and DIO1 are open-drain digital I/O ports with TTL level (5.5V max @ 64mA). ESD protection exceeds JESD 22.

When DIO port is configured as input:

contact is open, senses High (1)

contact is closed, senses Low (0)

NOTE: DIO0 and DIO1 port configuration as input is ideal for dry contact applications (door close, vibration, water, smoke sensors).

When DIO port is configured as output:

set to high, outputs TTL high

set to low, outputs TTL low

NOTE: DIO0 and DIO1 port configuration as output can control low voltage/current applications.

The OUT0 and OUT1 are high voltage digital outputs. Each port is internally attached to a Signal MOSFET. The output port is normally open (NO) and capable of supporting a voltage range from 2.5V to 60V @ 500mA.

When OUT port is set to:

High (enabled/active and pulls OUT to ground)

Low (disabled/inactive and keeps OUT open)

NOTE: OUT0 and OUT1 can pull a power-connected line to ground (i.e., relay circuit).

On Nodegrid Gate SR, the RELAY port is normally a closed (NC) relay (rated max value of 24V @ 1A). The RELAY specification supports a maximum switching power of 60W, 125VA; maximum switching voltage of 220VDC, 250VAC; maximum switching current of 2A, with restive load.

The RELAY's primary function is a Power Source Control Alarm. When closed, it indicates that Nodegrid Gate SR is powered by a single power source or has no power. If the Nodegrid Gate SR is powered by both power input sources, when RELAY is closed, it indicates a FAILURE on at least one power input sources.

(optional), RELAY can be changed to follow software control (Open / Close), to control an external device. Possible relay states are:

open (opens relay contact)

close (closes relay contact)

The I/O Port configuration is under *System :: I/O Ports*. I/O Port status and other hardware details is under *Tracking :: HW Monitor*.

WARNING! For Safety Reasons, do not exceed max voltage or current defined on each port.

Import / Export Configuration

The CLI can import the entire (or partial) Nodegrid configuration.

Import Configuration Settings

```
import_settings [arguments]
```

where arguments can be:

--file <local-pathname> (local file input)

--overwrite-tables (overwrite table when its configuration is given)

--quiet (suppress report of success/failure per path, just output final counters)

NOTE: In interactive mode (no --file given), the lines can be typed or copied/pasted. Enter **<ctrl>D** to finalize.

Export Configuration Settings

```
export_settings [cli-path] [arguments]
```

where arguments can be:

- with-options (provide a list of choices for value)
- include-empty (generate parameter line even if no value)
- not-enabled (generate parameter line even if parameter not active)
- plain-password (plain/hash password)
- file <local-pathname> (output to a local file)

Nodegrid Manager Installation

Install Nodegrid Manager from an ISO file. This is the three-step process:

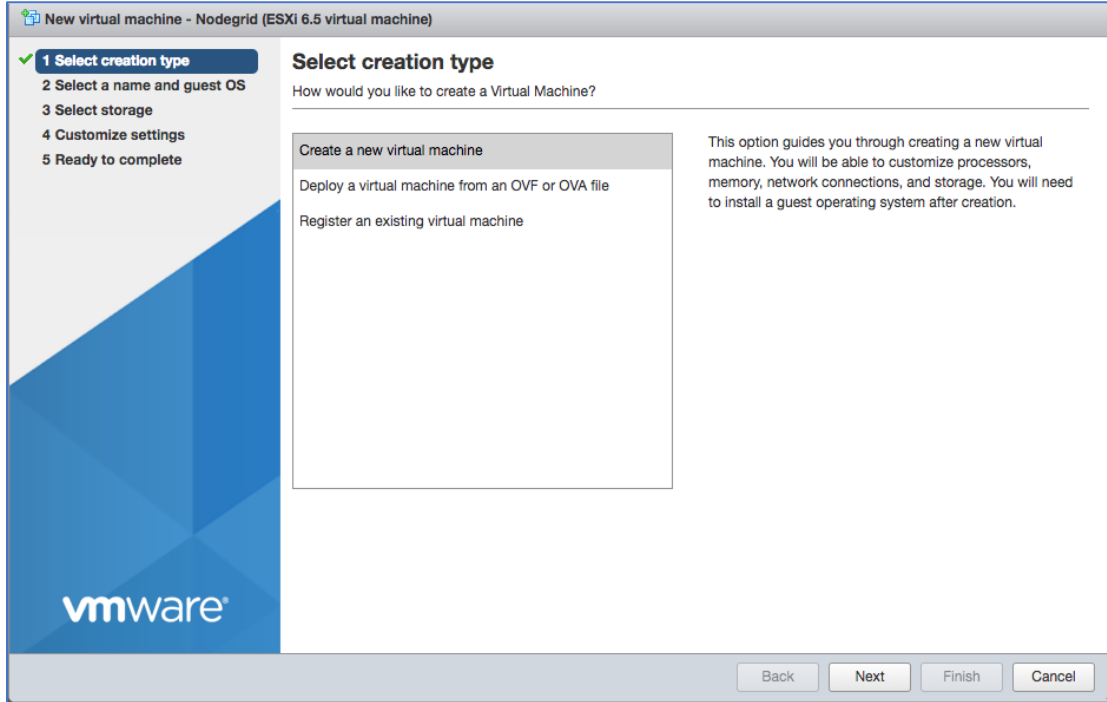
1. Create a virtual machine.
2. To install, boot from the ISO file/CD.
3. Restart and boot from the new virtual machine.

Minimum Requirements:

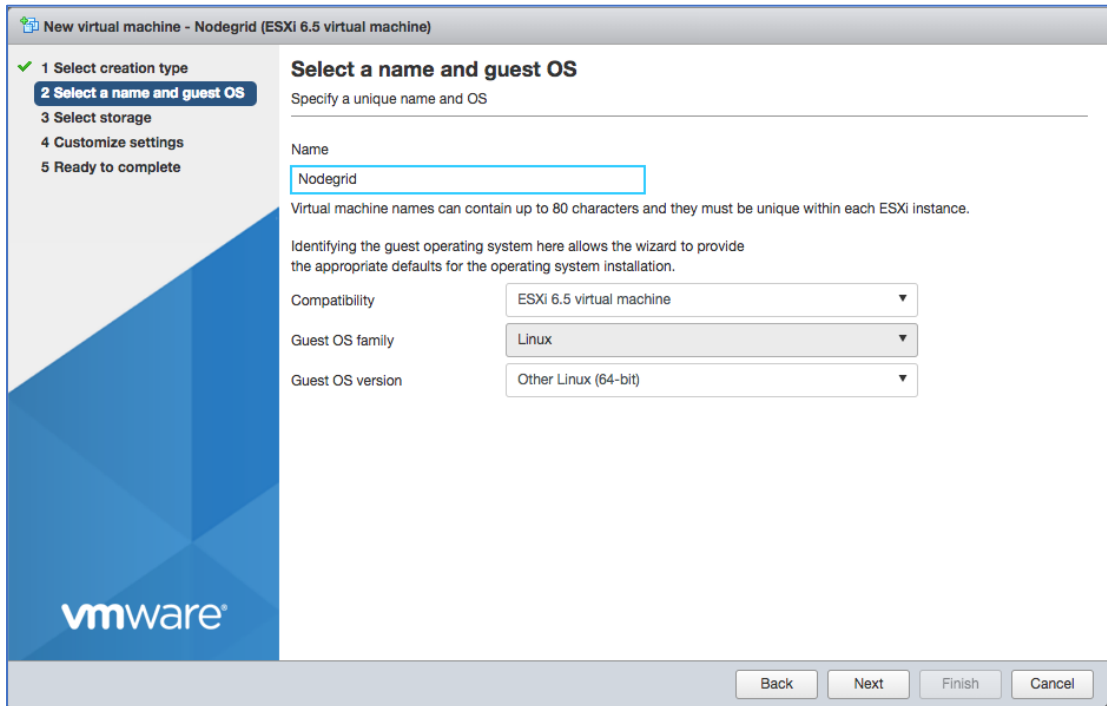
- ESXi 4.1 or above
- 32 GB hard drive (connected through the LSI Logic Parallel Controller)
- 4 GB memory (8GB is recommended)
- 2 Network adapters (E1000 adapters are recommended)

Create a VMware Virtual Machine

1. On the ESXi vSphere application, click **Create a new virtual machine**.
2. On the *Create a new virtual machine* dialog, click **Next**.



3. On *Select a name and guest OS* dialog:



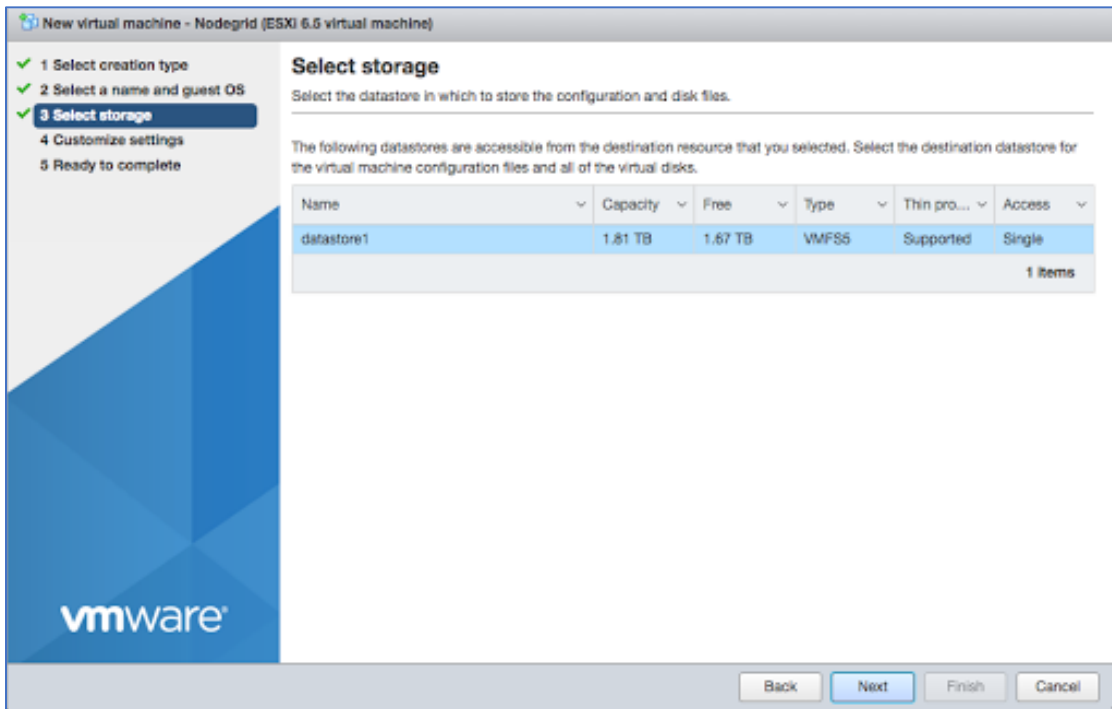
Enter **Name** for the Nodegrid Manager virtual machine.

For **Guest OS family**, select **Linux**.

For **Guest OS version**, select **Other Linux (64-Bit)**.

Click **Next**.

- On *Select storage* dialog table, select the virtual machine’s data storage volume. Click **Next**.



- On the *Customize settings* dialog, enter these settings (these are minimum settings – adjust as needed). Then click **Next**.

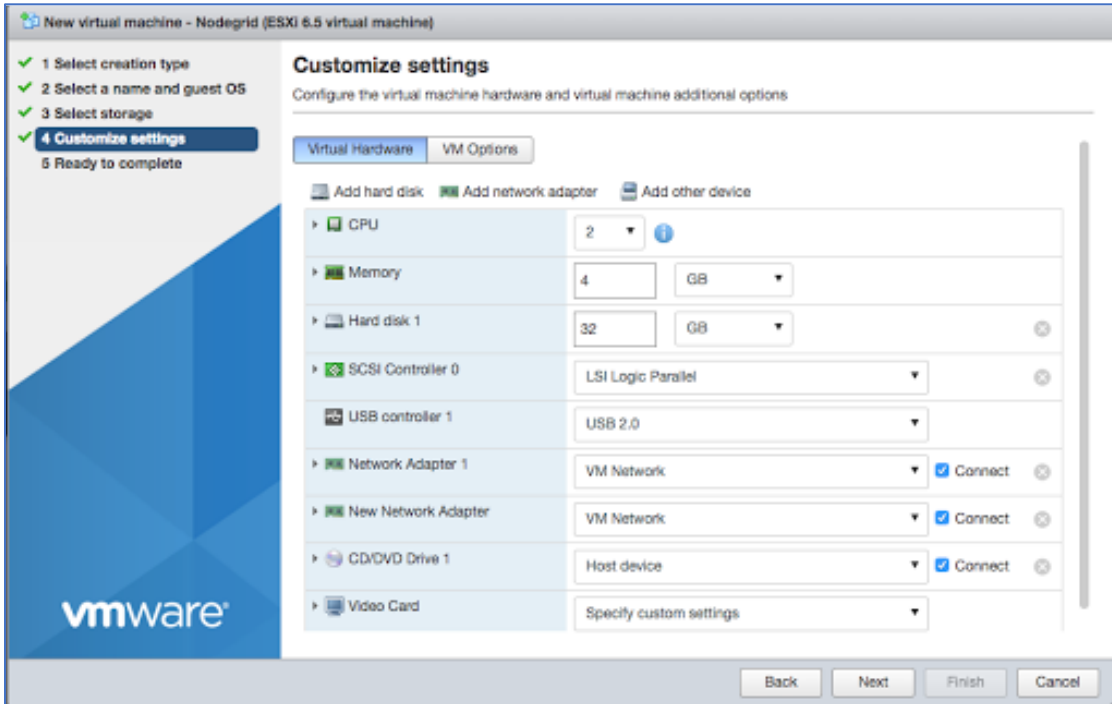
CPU: 2

Memory: 4GB

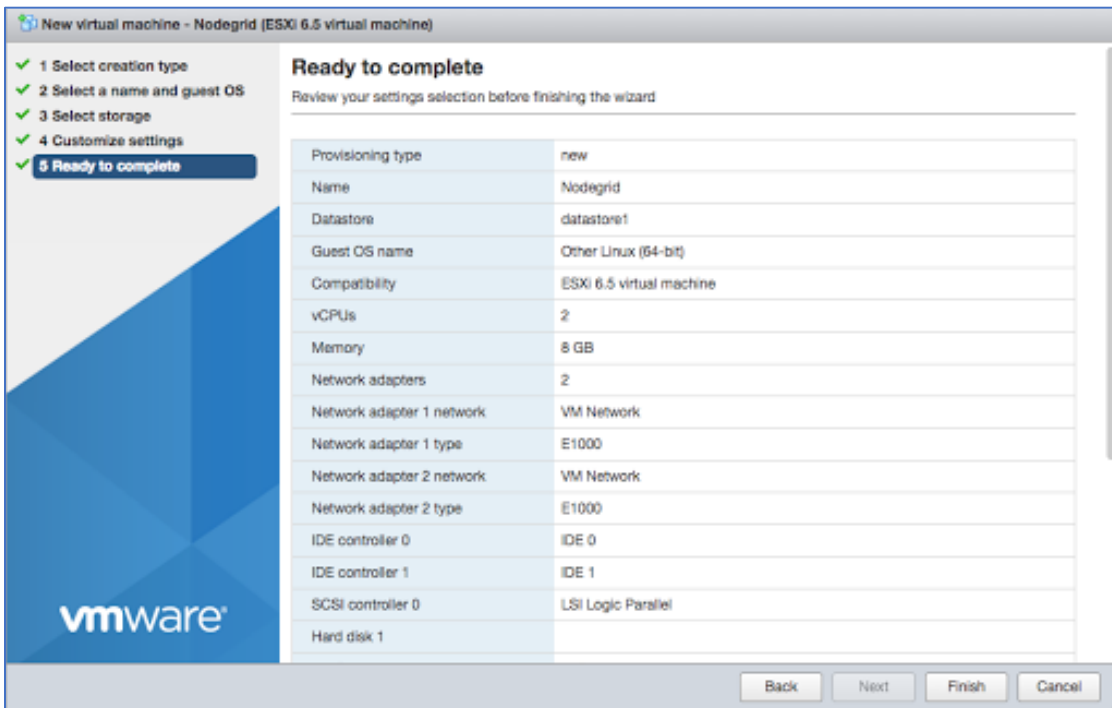
Hard disk: 32GB

SCSI Controller: LSI Logic Parallel

Network adapters: 2 of type E1000



6. On the *Ready to complete* dialog, review the details. Click **Finish**

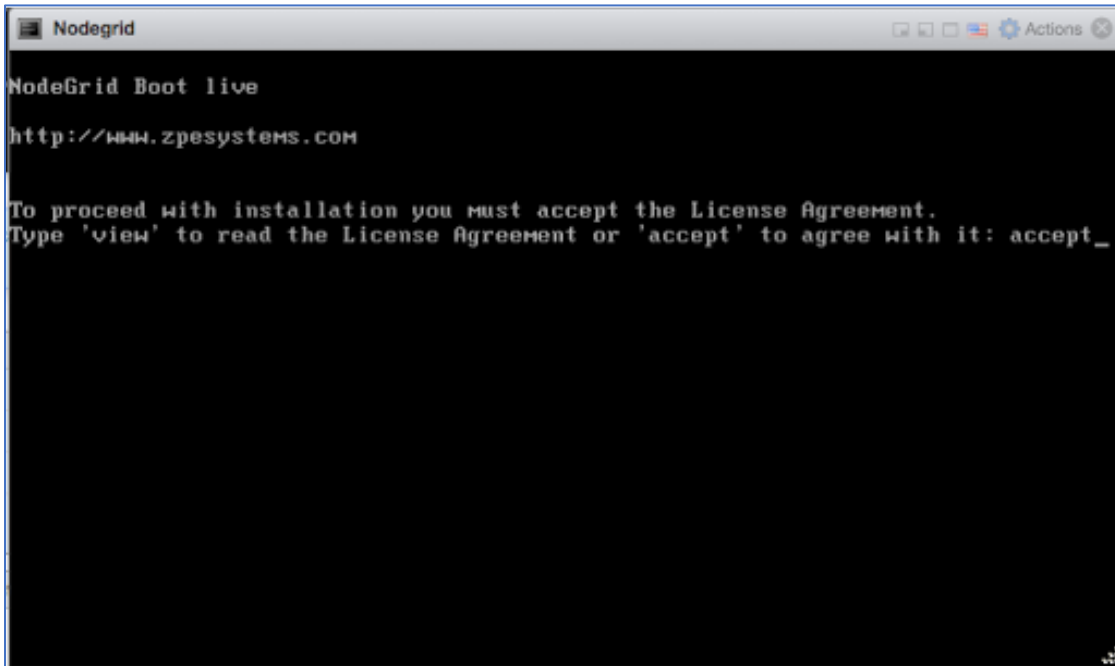


This completes the virtual machine configuration on the ESXi server.

Install Nodegrid Manager

To install the software:

1. On the virtual machine *Summary* screen, click the **Console** tab.
2. Turn on power to the virtual machine. Because there is no installed OS, the boot will fail.
3. Click on the CD/DVD icon and locate the Nodegrid Manager ISO file.
4. In the Console area, click CTL-ALT-INSERT. This reboots the virtual machine.
5. The virtual machine console server opens with a boot prompt. The image is decompressed and then loaded.
6. When the image boots, follow the console instructions. To accept the EULA, type **accept**.



7. When complete, the virtual machine reboots.

```

Nodegrid
Disk /dev/sda: 34.4GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos

Number  Start   End     Size    Type        File system  Flags
  1      1049kB  99.6MB  98.6MB  primary     ext4
  2      101MB   201MB   101MB   primary
  3      201MB   3202MB  3001MB  primary     boot
  4      3202MB  34.4GB  31.2GB  extended    lba
  5      3204MB  3304MB  99.6MB  logical
  6      3305MB  3315MB  9437kB  logical
  7      3316MB  3816MB  500MB   logical
  8      3817MB  34.4GB  30.5GB  logical

Checking current file system
Probe HD: Directory /var or root home directory not found.
Formatting partitions to ext4 ...
Mounting all partitions before start copy
Creating swap areas
Copying rootfs files...
Generating factory default settings files
Preparing second boot partition...
Installing grub on /dev/sda7
Remove your installation media, and press ENTER
    
```

- On reboot, the Nodegrid Manager application is ready to be configured.

```

Nodegrid
Booting 'NodeGrid Platform 4.0 Cirrus'

input_data: 0x00000000019ba276
input_len: 0x000000000429974
output: 0x0000000001000000
output_len: 0x000000000dd28c8
kernel_total_size: 0x000000000a6e000

Decompressing Linux... Parsing ELF... done.
Booting the kernel.
INIT: version 2.88 booting

Please wait: booting...
INIT: Entering runlevel: 5

Event Notification from nodegrid. Reported on 2018-08-02T11:48:33Z. Event ID 101
: The system has started.

NodeGrid 4.0.0 Feb 26 2018 - 04:46:01 nodegrid /dev/tty1 0.0.0.0
nodegrid login: _
    
```

Enroll Nodegrid Manager to ZPE Cloud

WebUI Procedure

- Log into ZPE Cloud.
- For enrollment information, go to *SETTINGS :: ENROLLMENT :: CLOUD*.
- Locate the device and open the WebUI.

4. Go to *Security :: Services* and select **Enable ZPE Cloud** checkbox.
To enroll the device in one on-premise instance of ZPE Cloud, select **Enable Remote Access** checkbox.
5. Make other changes, as needed.
6. Click **Save**.
7. To enroll device, go to *System :: Toolkit* and click **Cloud Enrollment**. Enter **Customer Code** and **Enrollment Key**.
To enroll the device in one on-premise instance of ZPE Cloud, enter **On-premise URL**.
8. Click **ENROLL**.

CLI Procedure

1. Log into ZPE Cloud.
2. For enrollment information, go to: *SETTINGS :: ENROLLMENT :: CLOUD*.
Open the vSphere Client.
On the **Menu** dropdown, select **Hosts and Clusters**.
On the *Hosts and Clusters* list, select the Nodegrid Manager VM
3. Click **Launch Web Console**.
4. On the CLI, enter admin credentials.
5. To enable ZPE Cloud, enter:

```
cd settings/zpe_cloud
set enable_zpe_cloud=yes
```


To enable the remote access feature, enter:

```
set enable_remote_access=yes
commit
```
6. To complete, enter:

```
commit
```

System Profile

The system profile handle interactions between local network and remote network/internet. Two system profile configurations (OOB, Gateway) are available for the following devices.

Device System Profile Configuration

Device	WAN/Uplink	LAN
Hive SR	wan[0-1], sfp[0-1], wwan[0-1]	lan[0-3], wlan0
Bold SR	eth0, wwan[0-1]	net[0-3], wlan0

Device	WAN/Uplink	LAN
Gate SR	eth0, sfp[0-1], wwan[0-1]	net[0-7], wlan0
Link SR	eth0, wwan0	sfp0, wlan0

On these devices, two system profile options are: Out of Band Profile and Gateway Profile. Administrator can update the profile at *System :: Toolkit :: Restore to Factory Default Settings*.

NOTE: When set, the System Profile is persistent.

Gateway Profile

When the System Profile selection is Gateway Profile, the following settings are configured:

- Block Unsolicited Incoming Packets enabled for all WAN ports
- IPv4 Forwarding and IPv6 Forwarding set to enabled
- Reverse Path Filtering set to Loose Mode
- Connection BRIDGE created for LAN interfaces
- Firewall rules and NAT rules are created
- If cellular card is detected:

Connection is created with name: CELLULAR-<channel>

Failover is enabled with these settings:

Primary Connection: ETH0 or WAN0

Secondary Connection: CELLULAR-<channel>

Trigger IP address: api.zpecloud.com

Out of Bounds Profile

Out Of Band Profile is set with the following configuration:

- Block Unsolicited Incoming Packets set to disabled (all network connections)
- Network Settings configuration:
 - IPv4 Forwarding set to disabled
 - IPv6 Forwarding set to disabled
 - Reverse Path Filtering set to Restrict Mode
- Firewall rules created to allow traffic to/from "lo" device
- If cellular card detected, connection is not created
- Failover is disabled
- For hotspot, DHCP server is enabled

NOTE: If the device's DHCP server fails or is unavailable, Nodegrid Platform responds on ETH0 at 192.168.160.10

Initial Network Configuration

Access the CLI Window

On the Nodegrid Platform's CLI window, after the boot messages, the login prompt is displayed.

Admin user:

Initial username = **admin**

Initial password = **admin** (after first login, default password must be changed)

Super User:

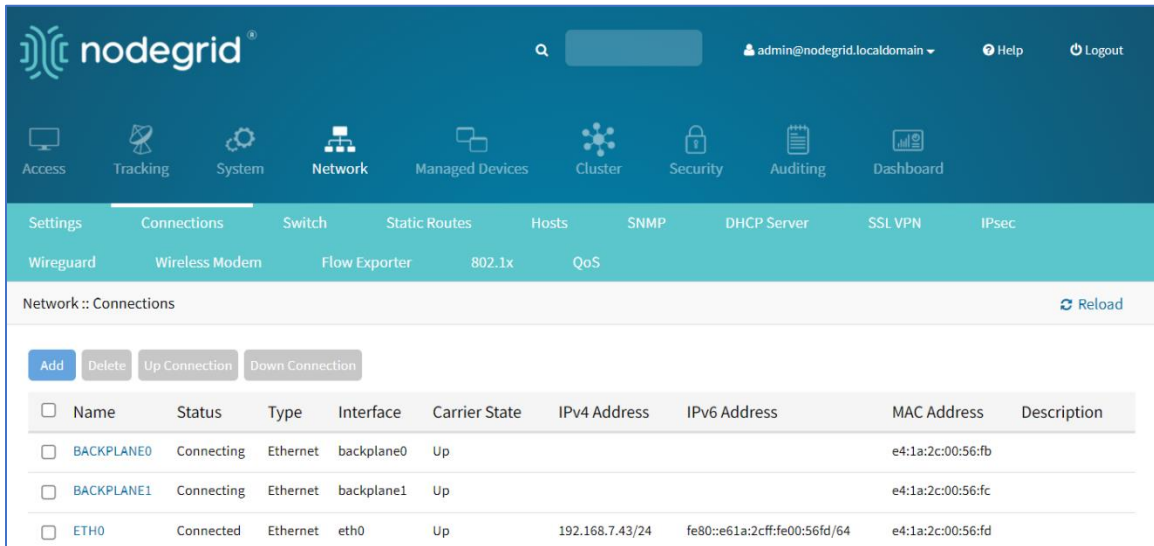
Username = **root** (SHELL access to Linux OS, but not web interface)

Default password = **root**

Identify Current IP Address

WebUI Procedure

1. Use admin login to device's Nodegrid Platform.
2. Go to *Network :: Connections*.



3. Review assigned IP addresses (save for later use).

CLI Procedure

1. Log into device as admin.

2. Enter:

```
show /system/network_connections/
```

Example output:

```
[admin@nodegrid /]# show /settings/network_connections/
name          status      type        interface   carrier state  ipv4 address      ipv6
address       mac address description
=====
BACKPLANE0    connected  ethernet    eth0        up      192.168.10.252/24 fe80 ::
290:fbff:fe5b:72bc/64 e4:1a:2c:5b:72:bc ETH0        connected ethernet backplane0
up            192.168.29.3/24 fe80 :: 290:fbff:fe5b:72bd/64 e4:1a:2c:5b:72:bd
hotspot       not active  WiFi        down
```

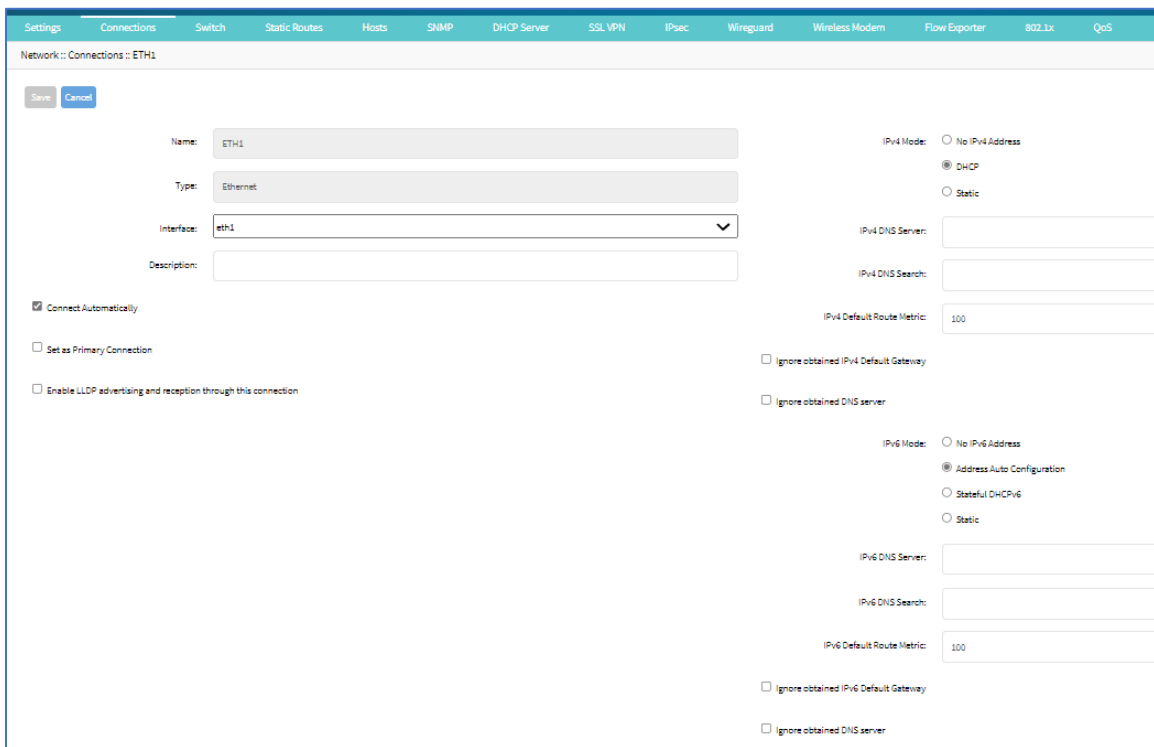
Define Static IP Address

If no DHCP server is available on the network, or to change from a dynamic to static IP, configure the network parameters.

NOTE: The examples below use IPv4 for communication. IPv6 is fully supported on the Nodegrid Platform. Settings are available in the same menus.

WebUI Procedure

1. Go to *Network :: Connections*.
2. Click on the Interface to be configured (displays *Network Connections* dialog for the .interface).
3. Enter the required details.



4. Click **Save**.

CLI Procedure

1. Go to the desired network Interface:

```
cd settings/network_connections/ETH0/
```

2. Configure the Network interface:

```
set ipv4_mode=static
set ipv4_address=<IP_ADDRESS> ipv4_bitmask=<BITMASK> ipv4_gateway=<GATEWAY>
commit
```

Example:

```
[admin@Nodegrid /]# cd settings/network_connections/ETH0/
[admin@Nodegrid ETH0]# set ipv4_mode=static
[admin@Nodegrid ETH0]# set ipv4_address=10.0.0.10 ipv4_bitmask=24
ipv4_gateway=10.0.0.1
[admin@Nodegrid ETH0]# show
name: ETH0
type: ethernet
ethernet_interface = eth0
connect_automatically = yes
set_as_primary_connection = no
enable_lldp = no
ipv4_mode = static
ipv4_address = 10.0.0.10
ipv4_bitmask = 24
ipv4_gateway = 10.0.0.1
ipv4_dns_server =
ipv4_dns_search =
ipv6_mode = address_auto_configuration
ipv6_dns_server =
ipv6_dns_search =
[admin@Nodegrid ETH0]# commit
```

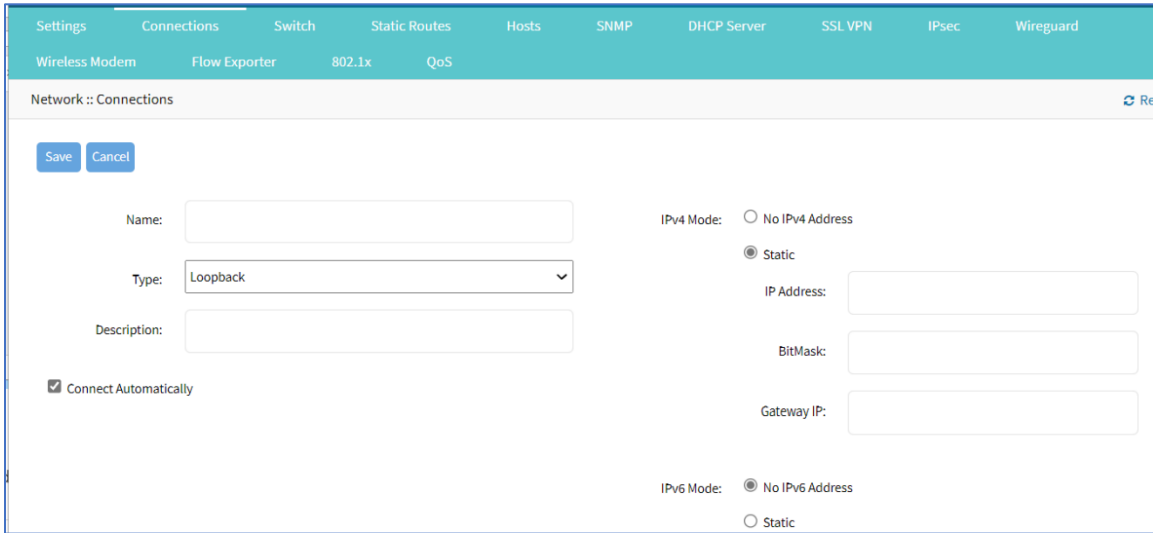
3. Follow the same steps for other interfaces.

Configure Loopback Address

WebUI Procedure

Multiple loopback addresses can be created with assigned IP addresses from within Network :: Connections.

1. Go to *Network :: Connections*.
2. Click **Add** (displays dialog).
3. On **Type** drop-down, select **Loopback** (modifies the UI).



4. Enter required details.
5. Click **Save**.

CLI Procedure

This is a minimal example. Other settings may be required (i.e., IP address is static or uses DHCP).

```
[admin@nodegrid /]# cd settings/network_connections/
[admin@nodegrid network_connections]# add
[admin@nodegrid {network_connections}]# set name=test
[admin@nodegrid {network_connections}]# set type=loopback
[admin@nodegrid {network_connections}]# commit
```

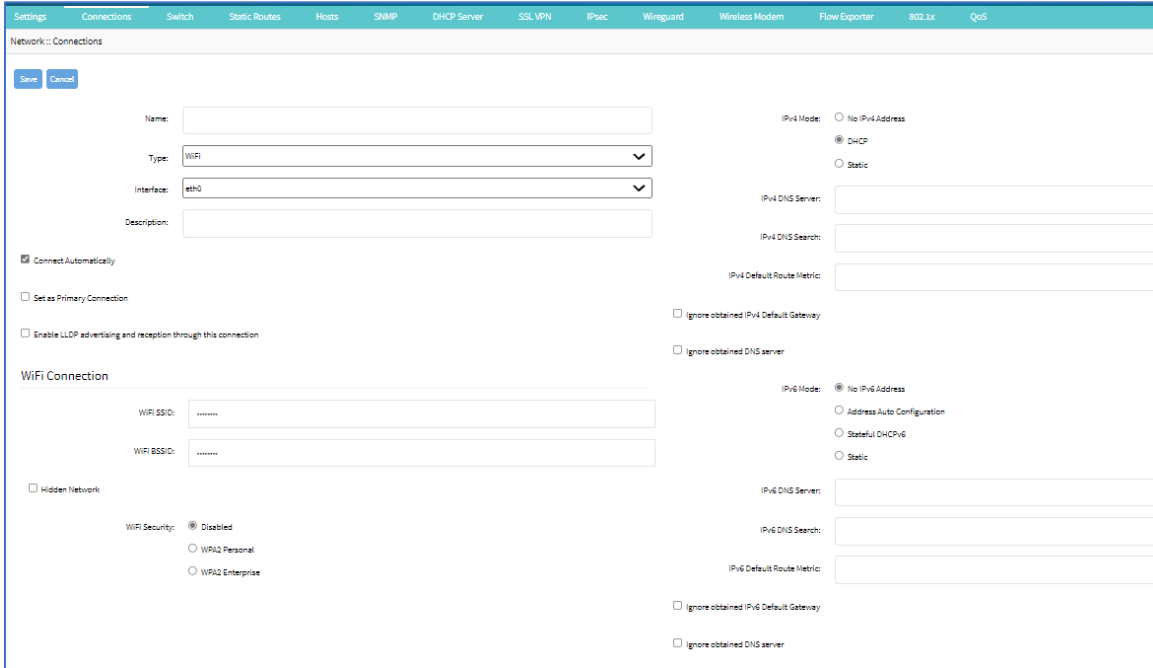
WiFi Module

When the WiFi module is installed, Nodegrid automatically creates an SSID named “Nodegrid” on the 192.168.162.x/24 network with an IP address of 192.168.162.1. Any WiFi enabled device can be connected to this network to access the Nodegrid device.

NOTE: The device can also be accessed through the Internet with properly configured routing and network settings.

To connect the Nodegrid device to another client through any available SSID:

1. Go to *Network :: Connections*.
2. Click **Add** (displays dialog).



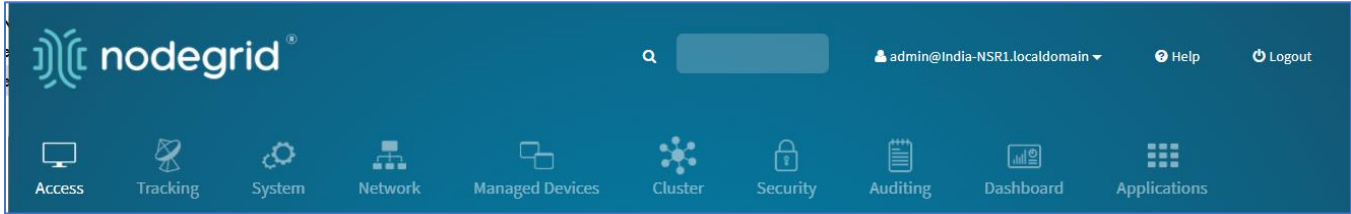
3. Enter **Name** (of the module).
4. On the **Type** drop-down, select **WiFi** (modifies UI).
5. On **Interface** drop-down, select **wlan0**.
6. (optional) Enter a **Description**
7. In *WiFi Connection* menu
 - Enter **SSID**
 - Enter **BSSID**
8. On *WiFi Security* menu, select appropriate radio button.
9. Enter Security settings (required for the selected connection)
10. Click **Save**.

General Information

User Interfaces

WebUI Banner

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



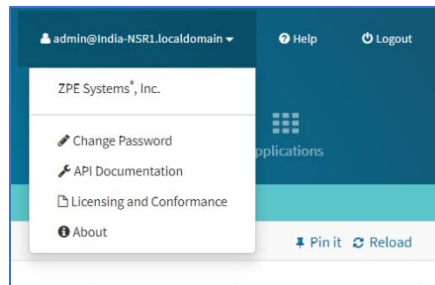
Each icon opens options to view and modify settings. Details on each section are available in the User Guide.

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 the required fields:

3. Enter **Old Password**.
4. Enter **New Password** and **Confirm Password**.
5. 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
androidudev (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+
atk-locale-en-gb (v2.34.1)                                             GPL-2.0+ & LGPL-2.0+

```

About

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



```

nodegrid

System:      Nodegrid Net SR
Version:    v5.4.0 (Nov 5 2021 - 14:28:59)
Licenses:   48
CPU:        Intel(R) Atom(TM) CPU C3758 @ 2.20GHz
CPU Cores:  8
Bogomips per core: 4400.00
Serial Number: 400843918
Uptime:     11 days, 42 hours, 0 minutes
Boot Mode:  Legacy
Secure Boot: Disabled
Model:      NSR
Part Number: NSR-TOP1-DAC
BIOS Version: 80919T00
PSU:        2
Revision Tag: r1
BIOS SED Compatible: no
SSD SED Compatible: no


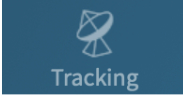
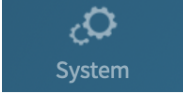

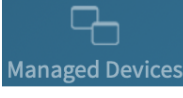
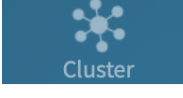

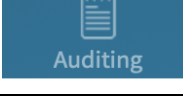
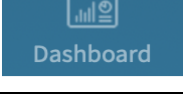
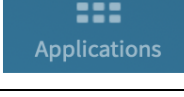
```

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	Item	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.

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 status, 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 cd - (cd<space><dash>	Returns user to root/home directory. Moves location up on level (i.e., if at <i>/settings/authentication</i> , enter cd - to go to <i>/settings</i> folder).
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	Either command can restore a setting from the most recent “commit” command.

Examples

```
[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.



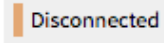
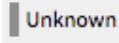
Access to Devices

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 current state of Nodegrid Cluster nodes determine which devices are displayed.

Device Sessions

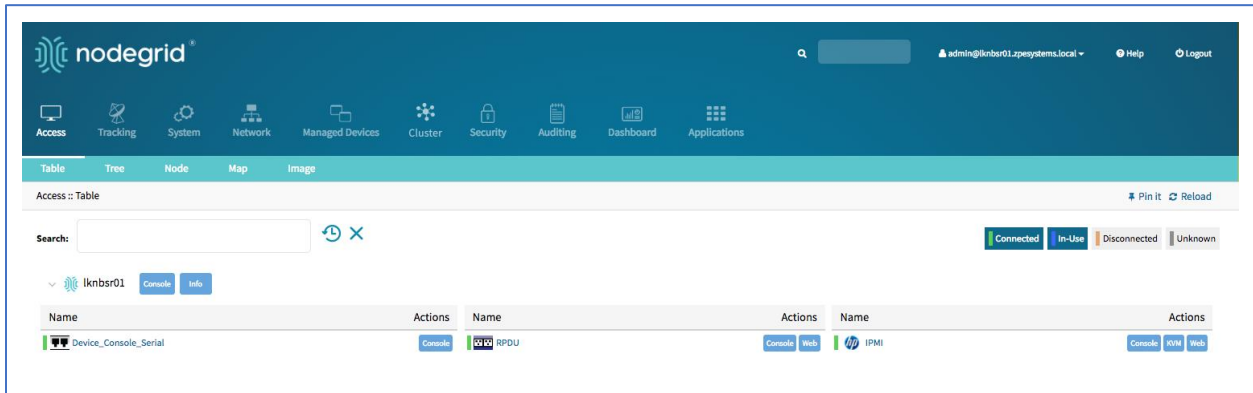
When a user logs into the WebUI, the first page is the Access section. This is overview of all available user-accessible targets. Each device current connection status and available connection types are shown.

Device Sessions

State	Indicator color	Icon	Description
Connected	Green		Nodegrid can successfully connect to the device and it is available for sessions
In-Use	Blue		The Device is currently in use
Disconnected	Orange		Nodegrid could not successfully connect to the device and it is not available for sessions
Unknown	Grey		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



Console (CLI) View

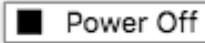
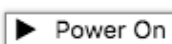
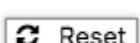
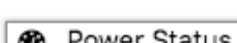


Click **Console** to display a new target session window.



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

Session Options

Options	Description
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.

Options	Description
	Performs a power off on the device through a connected Rack PDU or IPMI device.
	Performs a power on for the device through a connected Rack PDU or IPMI device.
	Initiates a power cycle on the device through a connected Rack PDU or IPMI device.
	Display device's current power status (as returned by a connected Rack PDU or IPMI device).
	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

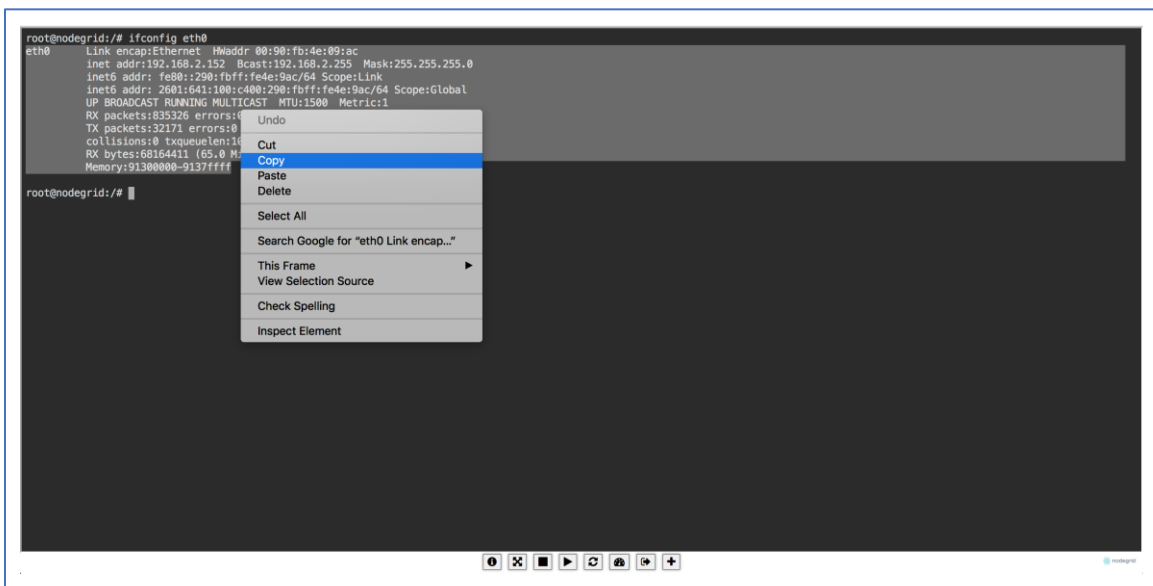
NOTE: TTYD terminal copy and paste is not currently supported within Windows and Linux.

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 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.



CLI Device Sessions

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

View currently available targets

`show`.

Example:

```
[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:

```
[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.

Option	Escape sequence	Description
<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.

```

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

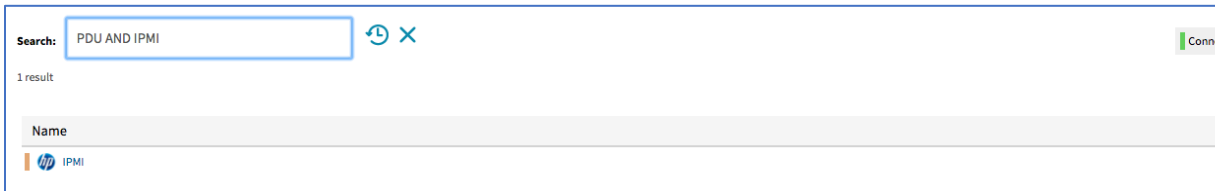
Field	Description
[search string]	A search string that represents part of or a complete string.
AND	Combines multiple search strings with an Boolean AND.
OR	Combines multiple search strings with a Boolean OR. Default search behavior for more than one search string.
NOT	Targets matching the search string 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”

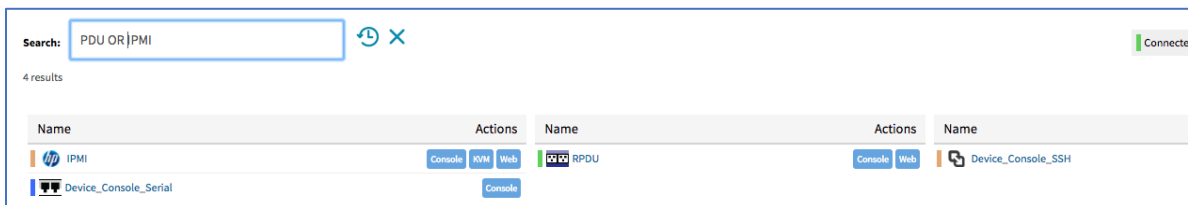


```
[admin@nodegrid search]# search "PDU AND IPMI"

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"

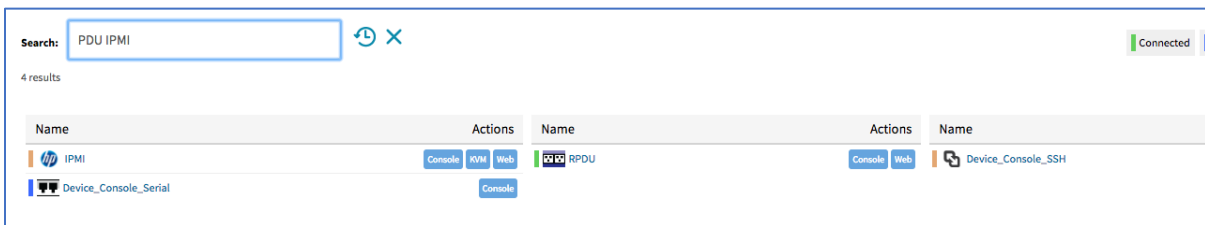


```
[admin@nodegrid access]# search "PDU OR IPMI"
```

```
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 Refresh Close Connected

4 results

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

```
[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 Refresh Close Conne

3 results

Name	Actions	Name	Actions	Name
RPDU	Console Web	Device_Console_SSH	Console Web	Device_Console_Serial

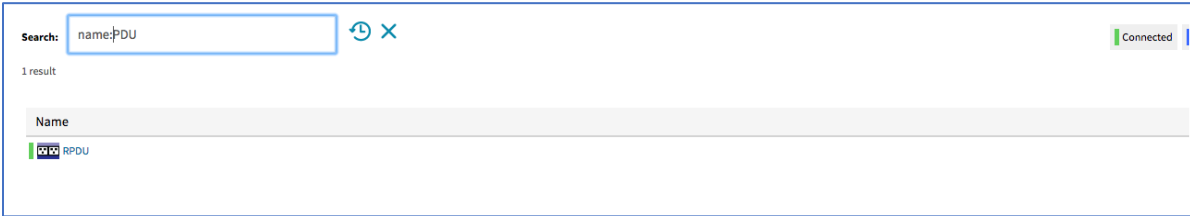
```
[admin@nodegrid search]# search "PDU AND NOT IPMI"
```

```

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"



```

[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. The following views are available:

- Table View
- Tree View
- Node View
- Map View
- Image View

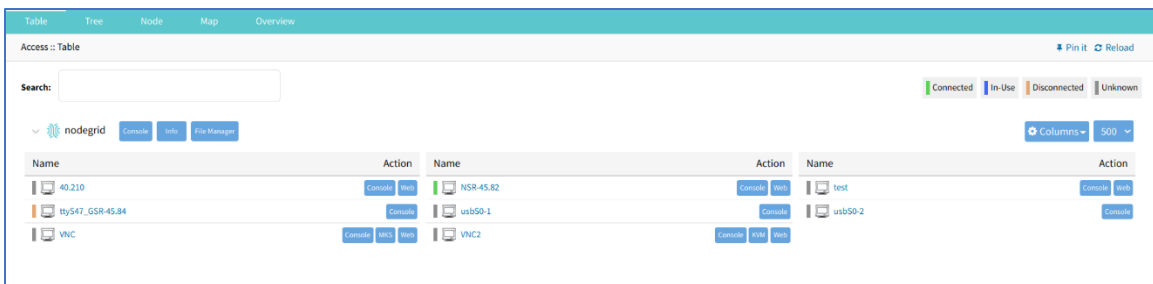
Each user can change the default view after login. To change the default view, display the preferred view and click **Pin It**.

Table tab

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.

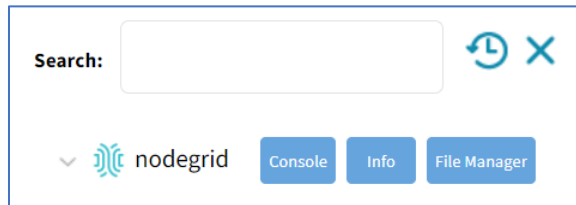
In the table, the *Action* column shows buttons to access that device. Type of button depends on device: **Console, SSH, Telnet, KVM, MKS**.



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

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)

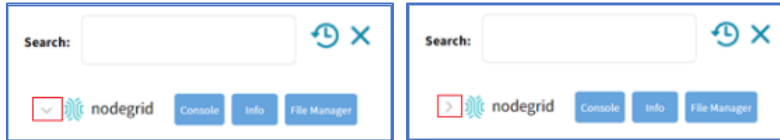
Boolean (AND, OR, NOT – caps only)

[field name] (limits results to a specific Field Name).

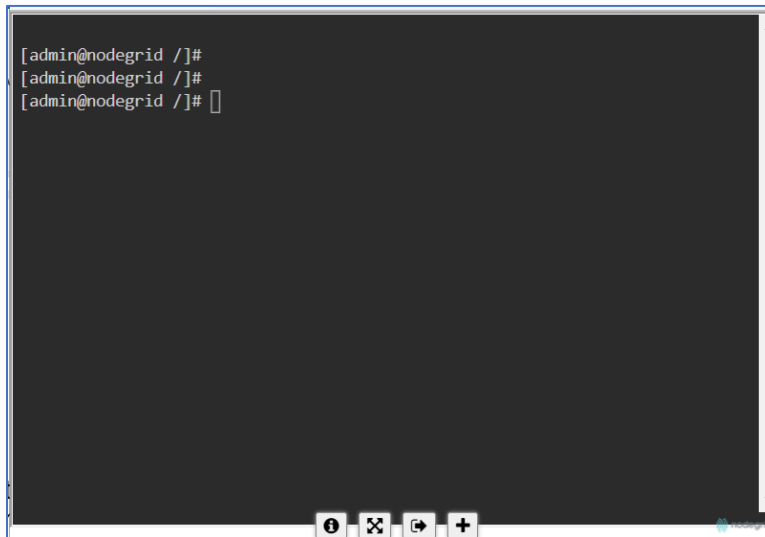
Clock icon (shows a history of past searches)

"X" (clears the search field)

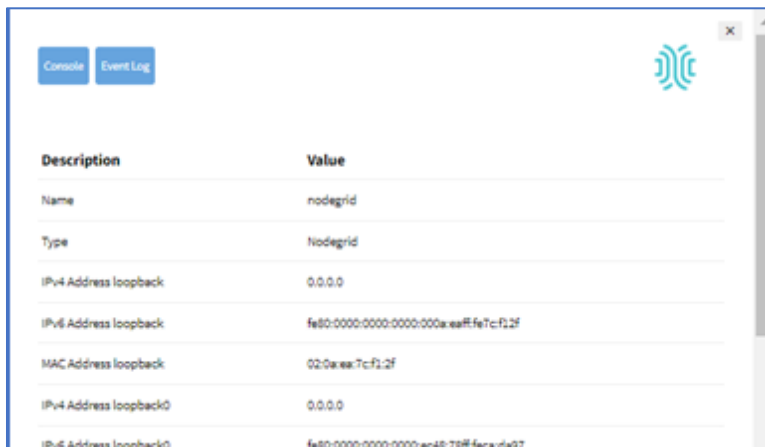
- **Arrow** (show/hide table – click down arrow to hide table, click up arrow to show table)



- **Console** (display CLI window)



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



Pop-up dialog buttons:

Console button – opens the Console (CLI) window (see above).

Event Log button – displays the raw log details.

```

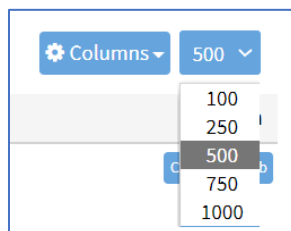
Page 1 - 10/05/2021 18:22:55

<2021-10-05T13:21:03Z> Event ID 103: Software upgrade completed, Status: 1, New software version: 5.1.2.
<2021-10-05T13:21:03Z> Event ID 101: The system has started.
<2021-10-05T13:21:04Z> Event ID 140: Connection up, Connection: ETH0, Interface: eth0, Type: ethernet, IP Address: 192.168.7.43/24.
<2021-10-05T13:21:55Z> Event ID 520: A Extended Storage started.
<2021-10-05T15:58:05Z> Event ID 202: User authentication failed, User: admin@192.168.14.46.
<2021-10-05T15:58:28Z> Event ID 202: User authentication failed, User: admin@192.168.14.46.
<2021-10-05T16:29:28Z> Event ID 202: User authentication failed, User: admin@192.168.14.46.
<2021-10-05T16:29:48Z> Event ID 202: User authentication failed, User: admin@192.168.14.46.
<2021-10-05T17:07:39Z> Event ID 202: User authentication failed, User: admin@192.168.14.46.
<2021-10-05T17:07:57Z> Event ID 202: User authentication failed, User: admin@192.168.14.46.
<2021-10-05T17:09:46Z> Event ID 202: User authentication failed, User: admin@192.168.14.39.
<2021-10-05T17:09:56Z> Event ID 202: User authentication failed, User: admin@192.168.14.39.
<2021-10-05T17:10:17Z> Event ID 200: A user logged into the system, User: admin@192.168.14.39, Session type : HTTPS, Authentication Method: Local.
<2021-10-05T17:11:30Z> Event ID 200: A user logged into the system, User: admin@192.168.14.46, Session type : HTTPS, Authentication Method: Local.
<2021-10-05T17:11:45Z> Event ID 201: A user logged out of the system, User: admin, Session type: unknown.
<2021-10-05T17:16:25Z> Event ID 201: A user logged out of the system, User: admin@192.168.14.39, Session type: HTTPS.
<2021-10-05T17:16:25Z> Event ID 201: A user logged out of the system, User: admin@192.168.14.46, Session type: HTTPS.
<2021-10-05T17:17:10Z> Event ID 202: User authentication failed, User: admin@192.168.14.39.
<2021-10-05T17:17:19Z> Event ID 200: A user logged into the system, User: admin@192.168.14.39, Session type : HTTPS, Authentication Method: Local.
<2021-10-05T17:19:45Z> Event ID 200: A user logged into the system, User: admin@192.168.14.21, Session type : HTTPS, Authentication Method: Local.
<2021-10-05T17:23:08Z> Event ID 102: Software upgrade started, User: root, Current version: 5.1.2, New version: 5.2.3.
<2021-10-05T17:30:27Z> Event ID 140: Connection up, Connection: ETH0, Interface: eth0, Type: ethernet, IP Address: 192.168.7.43/24.
    
```

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

Type	Name	Size	Time
Folder	admin_group	4.00 KB	3/9/2018 4:34:56 AM
Folder	admin_home	4.00 KB	3/9/2018 4:34:56 AM
Folder	dataalog	4.00 KB	9/29/2021 11:04:19 AM
Folder	datastore	4.00 KB	3/9/2018 4:34:56 AM
Folder	eventlog	4.00 KB	9/30/2021 6:40:55 AM
Folder	nodegrid_ap	4.00 KB	3/9/2018 4:34:56 AM
Folder	remote_file_system	4.00 KB	3/9/2018 4:34:56 AM
Folder	sed	4.00 KB	3/9/2018 4:34:56 AM
Folder	software	4.00 KB	9/30/2021 6:39:32 AM

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

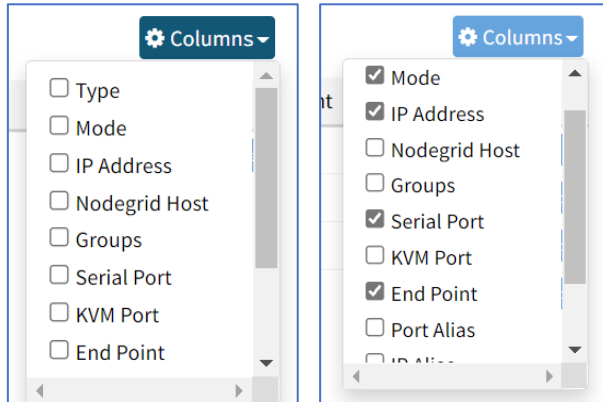


Display Table Columns

WebUI Procedure

Details on each device can be viewed by selecting columns.

1. Go to *Access :: Table*.
2. On the right side, click **Columns** (displays a drop-down dialog of available table columns).



3. As columns are selected, they are displayed in the table.

Peers Settings Management

Cluster :: Peers Reload

Search: Refresh Close

Connected
In-Use
Disconnected
Unknown

nodegrid Console Info File Manager Columns

Name	Type	Mode	IP Address	Serial Port	End Point	Action
console_server_acs	console_server_acs	Enabled			appliance	Console Web
ttyS13	local_serial	Enabled		ttyS13		Console
usbS0-1	usb_serialB	Enabled		usbS0-1		Console
usbS0-3	usb_serialB	On-demand		usbS0-3		Console

View Device Details

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

Console
SSH
Telnet
KVM
WEB

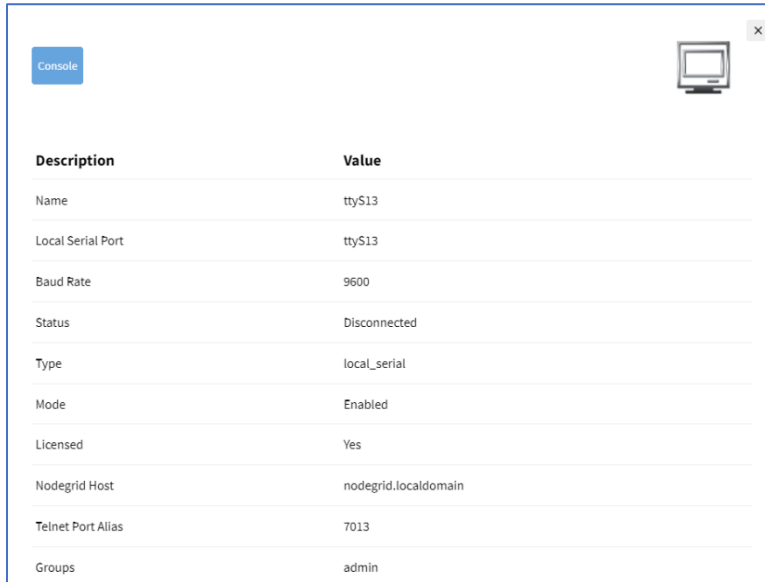
Description	Value
Name	NSR-test
Alias	DeviceAlias1
Status	Unknown
Type	device_console
Mode	Enabled
Licensed	Yes
Nodegrid Host	nodegrid.localdomain
Groups	default, admin, user

Manage Power

View Device Power Details

WebUI Procedure

1. Go to *Access :: Table*.
2. In the **Name** column, locate and click the name (displayed dialog details change according to the type).



Description	Value
Name	ttyS13
Local Serial Port	ttyS13
Baud Rate	9600
Status	Disconnected
Type	local_serial
Mode	Enabled
Licensed	Yes
Nodegrid Host	nodegrid.localdomain
Telnet Port Alias	7013
Groups	admin

CLI Procedure

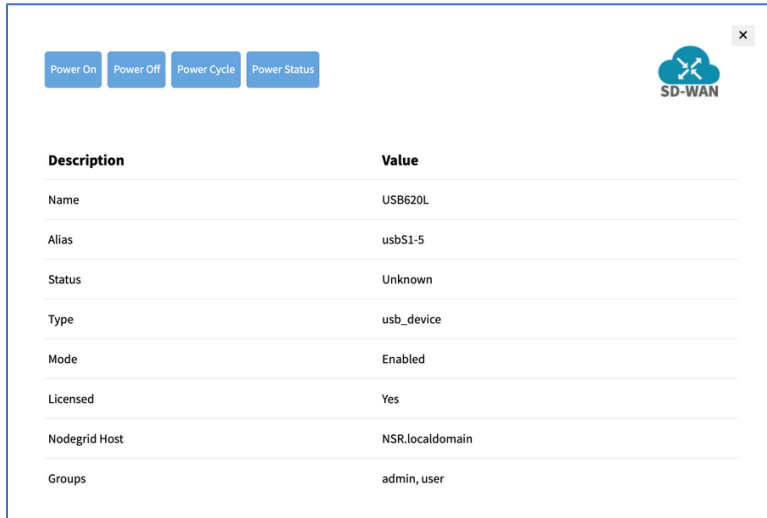
Example:

```
[admin@nodegrid /]# cd /access/
[admin@nodegrid access]# show Device_Console_Serial/
name: Device_Console_Serial
status: Connected
```

Set Device USB Power Option

WebUI Procedure

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.



The screenshot shows a web interface with four buttons: 'Power On', 'Power Off', 'Power Cycle', and 'Power Status'. To the right is an 'SD-WAN' logo with a close button 'x'. Below is a table with the following data:

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)

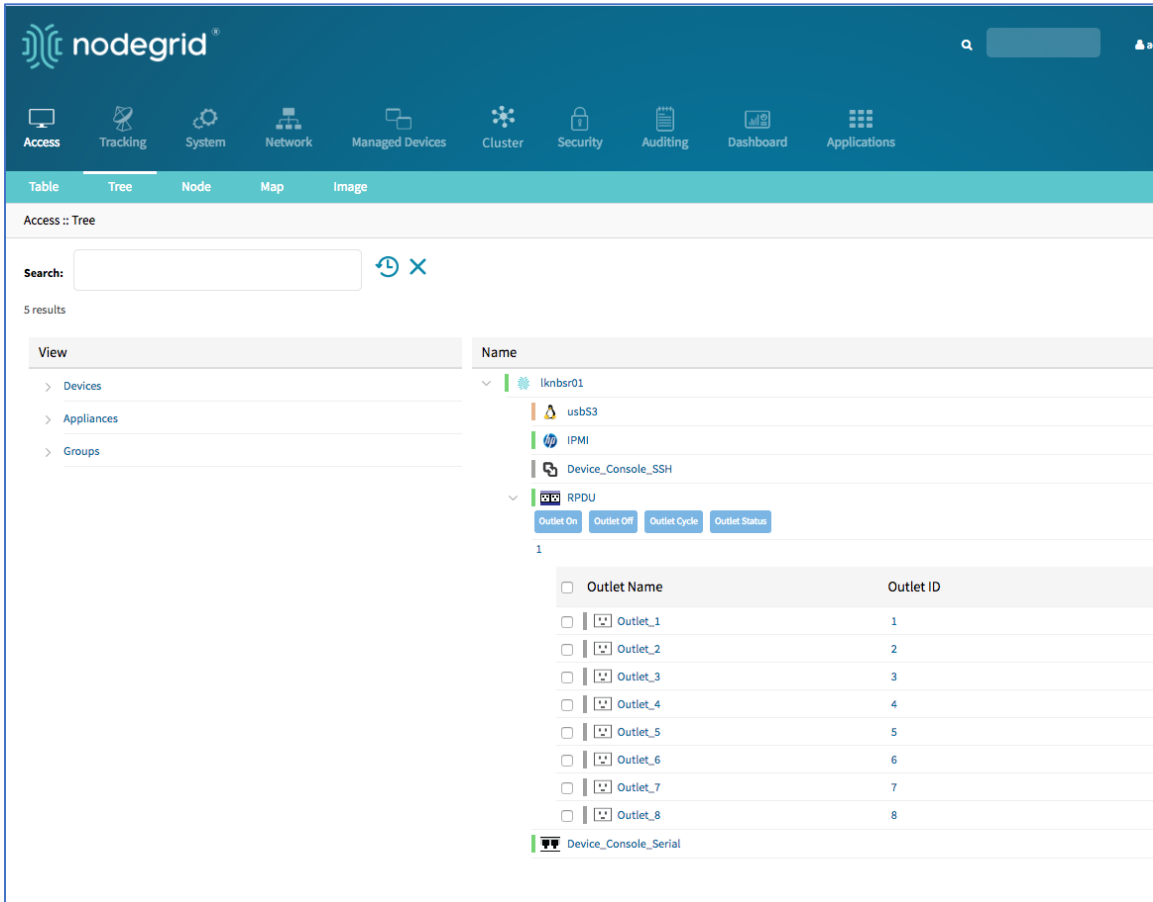
Power Off (turns power off)

Power Cycle (cycles power on and off)

Power Status (current status)

Tree tab

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*.



View Column Branches

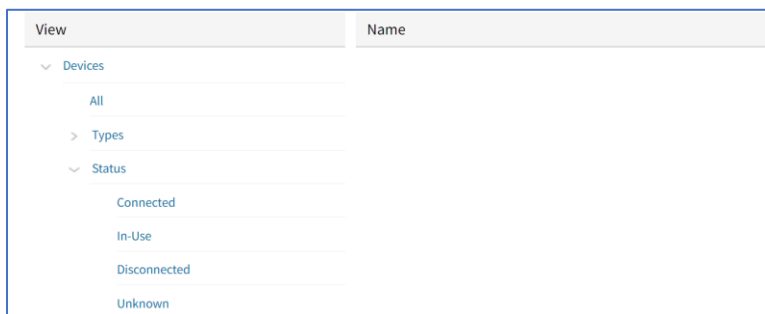
There are three trees in the View columns: **Devices**, **Appliances**, Groups. Details can be observed by clicking the ">".

Expand Individual Tree

WebUI Procedure

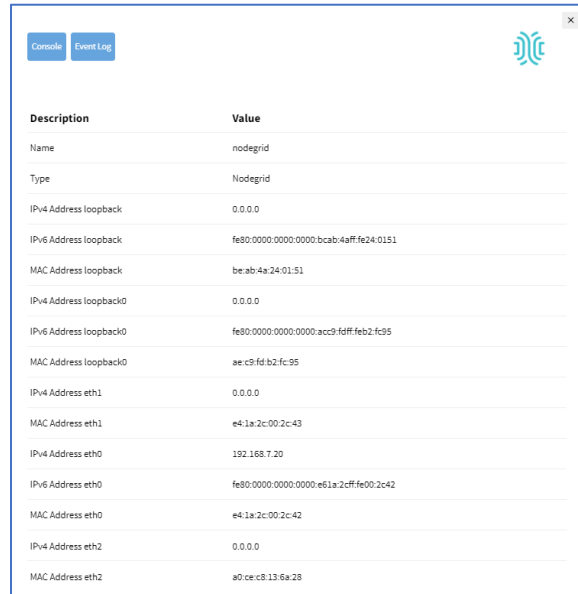
This example uses *Devices*.

1. Click the right icon to display the next branch level.



2. If further branch levels are available, click the right icon to expand the branch.

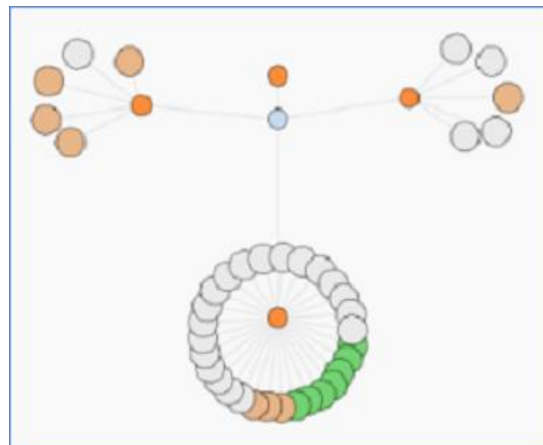
3. To contract the branch, click the down icon.
4. To see every item in the tree, click on **All**. Click on other items to see associated names (some clicked items may not have names).
5. Click on a name to display a pop-up dialog of details.



Description	Value
Name	nodegrid
Type	Nodegrid
IPv4 Address loopback	0.0.0.0
IPv6 Address loopback	fe80:0000:0000:0000:bcab:4aff:fe24:0151
MAC Address loopback	be:ab:4a:24:01:51
IPv4 Address loopback0	0.0.0.0
IPv6 Address loopback0	fe80:0000:0000:0000:acc9:f0ff:feb2:fe95
MAC Address loopback0	ae:c3:fd:b2:fc:95
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
IPv4 Address eth2	0.0.0.0
MAC Address eth2	a0:ce:c8:13:6a:28

Node tab

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



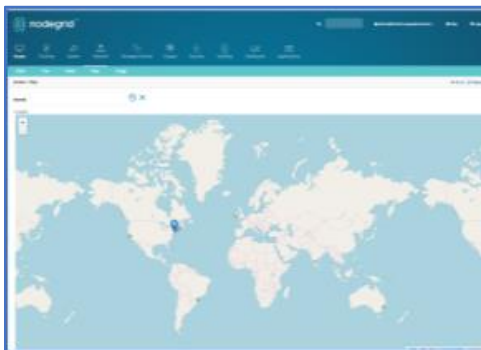
Click on a node to display a pop-up dialog of details.

Description	Value
Name	nodegrid
Type	Nodegrid
IPv4 Address loopback	0.0.0.0
IPv6 Address loopback	fe80:0000:0000:0000:bcab:4aff:fe24:0151
MAC Address loopback	be:ab:4a:24:01:51
IPv4 Address loopback0	0.0.0.0
IPv6 Address loopback0	fe80:0000:0000:0000:acc9:fdf5:feb2:fc95
MAC Address loopback0	ae:c9:fd:b2:fc:95
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:2cfff:fe00:2c42
MAC Address eth0	e4:1a:2c:00:2c:42
IPv4 Address eth2	0.0.0.0
MAC Address eth2	a0:ce:c8:13:6a:28

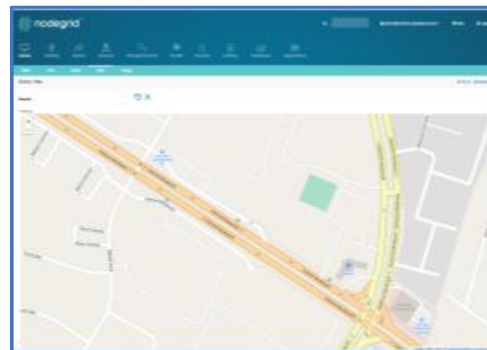
Map tab

This shows device status on a global-based map. This provides an overview of all targets and Nodegrid units in a Cluster. Precise device location details are included down to a building level. Click on a marker to display information and connections.

Global View



Zoomed in Street View



To move the map position, use click and drag.

Image tab

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

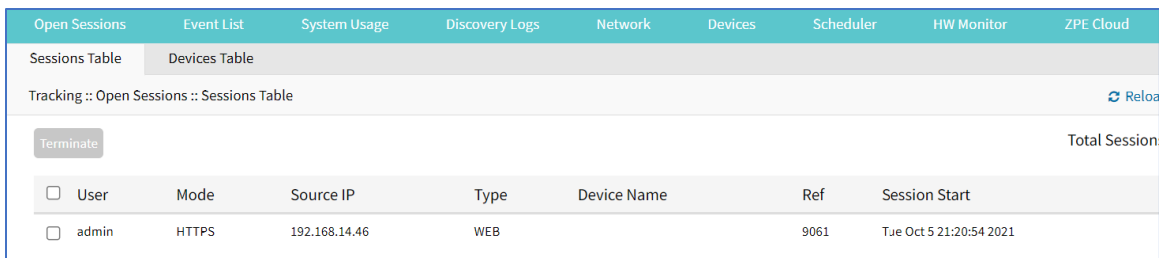
This provides information about the System and connected devices. This includes Open Sessions, Event List, Routing Table, System Usage, Discovery Logs, LLDP, and Serial Statistics.

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.



<input type="checkbox"/>	User	Mode	Source IP	Type	Device Name	Ref	Session Start
<input type="checkbox"/>	admin	HTTPS	192.168.14.46	WEB		9061	Tue Oct 5 21:20:54 2021

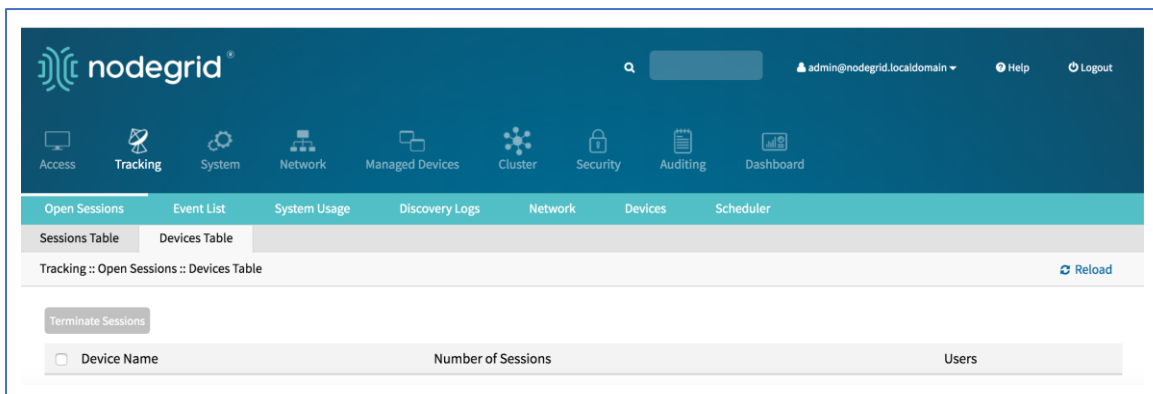
Terminate Session

WebUI Procedure

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



<input type="checkbox"/>	Device Name	Number of Sessions	Users
--------------------------	-------------	--------------------	-------

Terminate Session

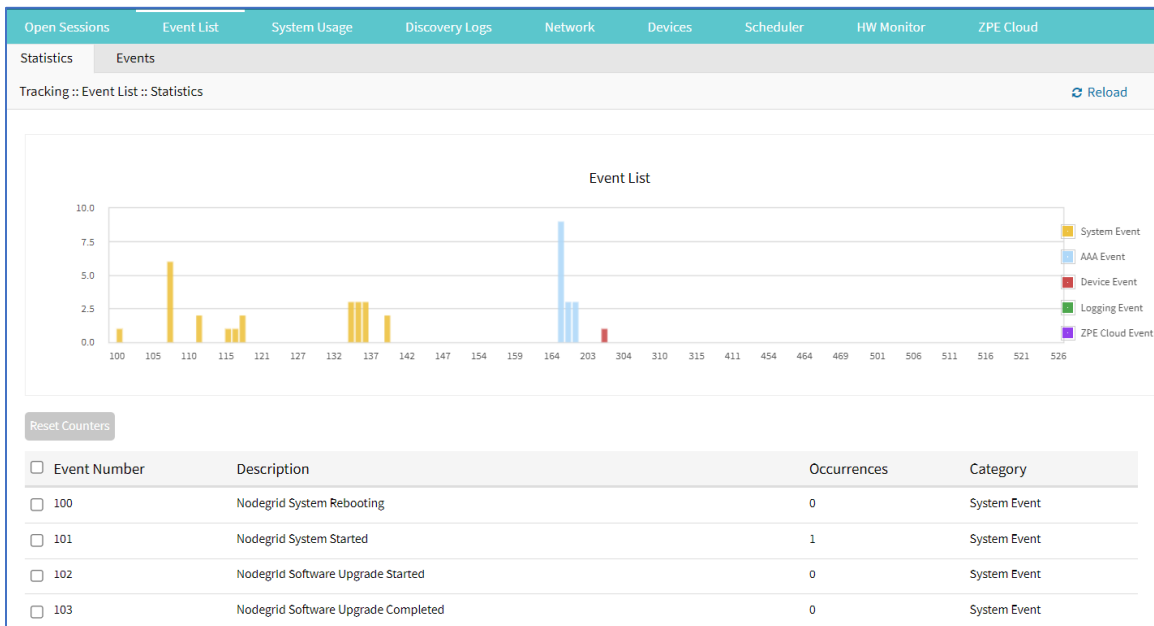
WebUI Procedure

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

Event List tab

Statistics sub-tab

This provides statistical information on the system event occurrences.



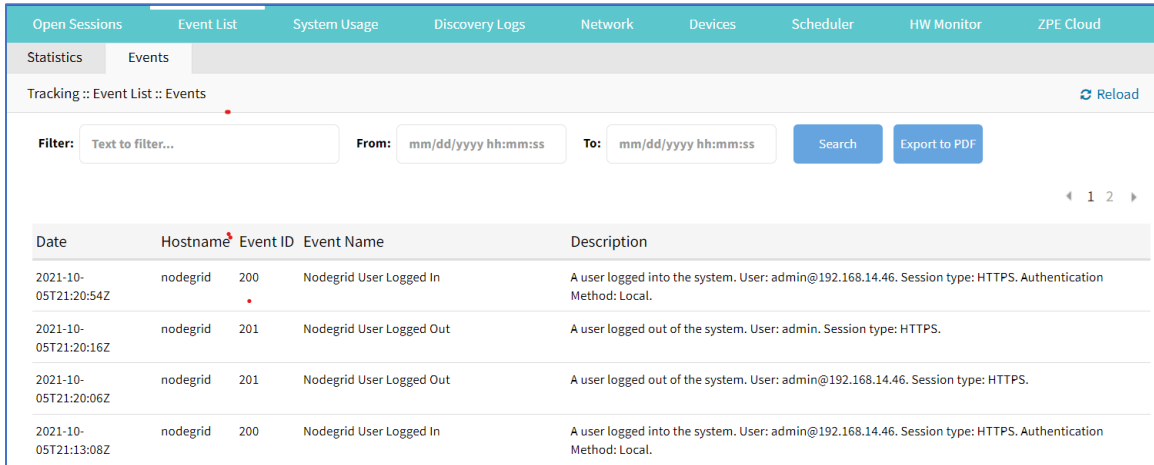
Reset Event Counter

WebUI Procedure

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**.

Events sub-tab

This displays event details (read only).



Date	Hostname	Event ID	Event Name	Description
2021-10-05T21:20:54Z	nodegrid	200	Nodegrid User Logged In	A user logged into the system. User: admin@192.168.14.46. Session type: HTTPS. Authentication Method: Local.
2021-10-05T21:20:16Z	nodegrid	201	Nodegrid User Logged Out	A user logged out of the system. User: admin. Session type: HTTPS.
2021-10-05T21:20:06Z	nodegrid	201	Nodegrid User Logged Out	A user logged out of the system. User: admin@192.168.14.46. Session type: HTTPS.
2021-10-05T21:13:08Z	nodegrid	200	Nodegrid User Logged In	A user logged into the system. User: admin@192.168.14.46. Session type: HTTPS. Authentication Method: Local.

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.

WebUI Procedure

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 location and click **Save**.

List Events Main Table

Column name	Description
Date	Date the event took place.
Hostname	Name of the host where the event took place.
Event ID	Event code.
Event Name	Name of the event.
Description	Description of the event.

Registered Events Description

Event #	Description	Category
100	Nodegrid System Rebooting	System Event
101	Nodegrid System Started	System Event

Event #	Description	Category
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

Event #	Description	Category
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

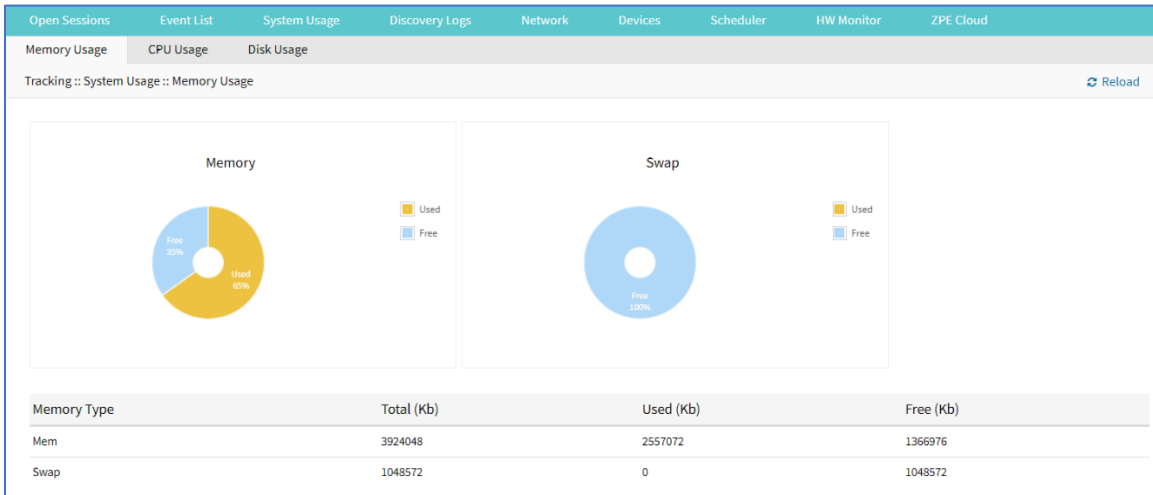
Event #	Description	Category
159	Nodegrid Cluster Peer Configured	System Event
160	Nodegrid Search Unavailable	System Event
161	Nodegrid Search Restored	System Event
200	Nodegrid User Logged In	AAA Event
201	Nodegrid User Logged Out	AAA Event
202	Nodegrid System Authentication Failure	AAA Event
300	Nodegrid 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

Event #	Description	Category
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

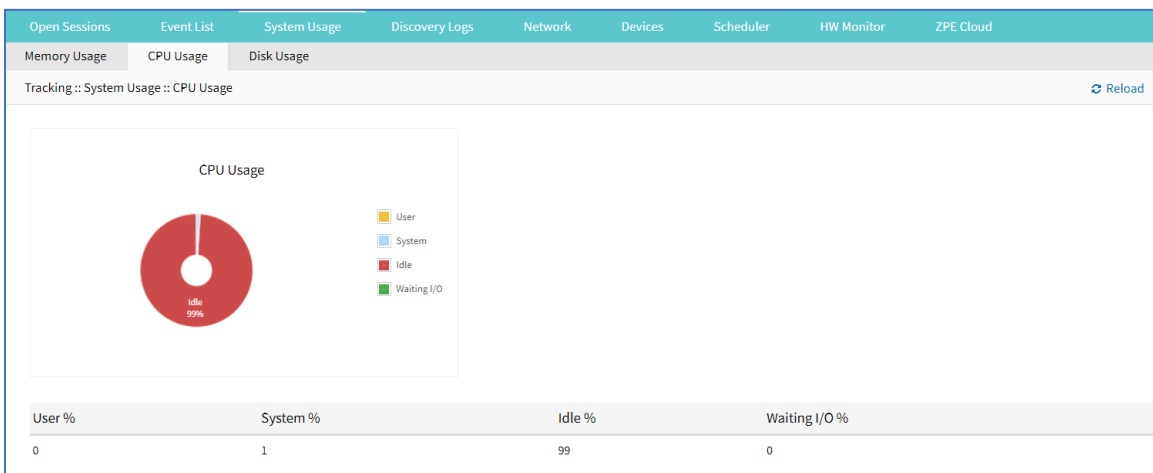
System Usage tab

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

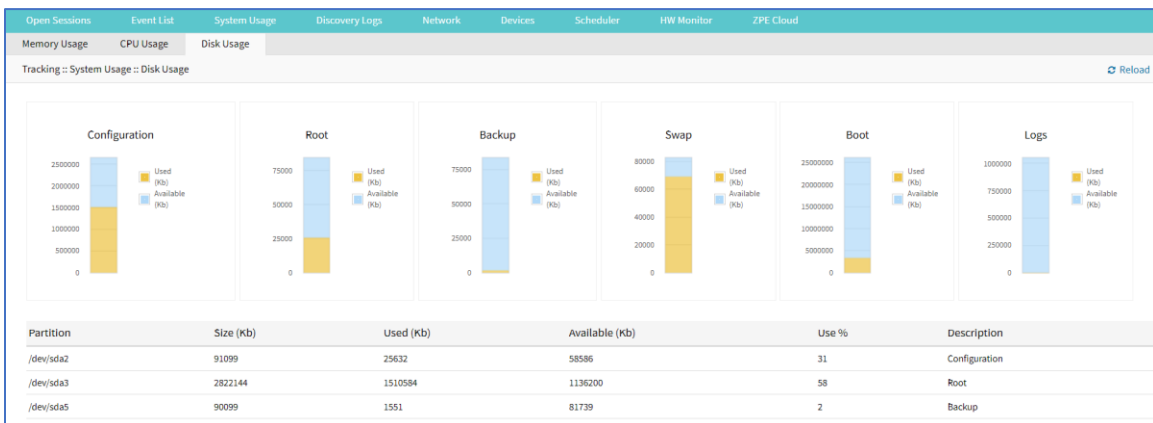
Memory Usage sub-tab



CPU Usage sub-tab

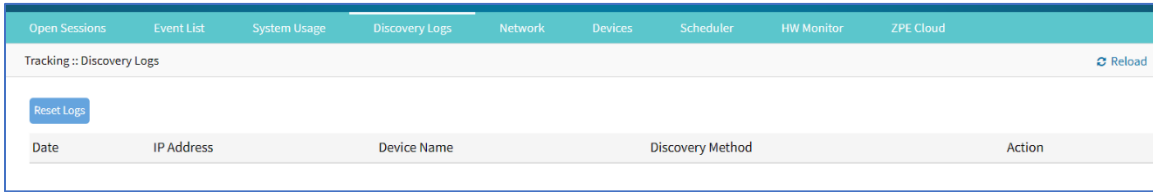


Disk Usage sub-tab



Discovery Logs tab

This shows the logs of the discovery processes set on the Managed Devices setting for auto discovery.



Discovery Logs Table

Column name	Description
Date	Date of the log entry.
IP Address	IP address of device.
Device Name	Name of the device.
Discovery Method	Discovery method used to identify the log entry.
Action	The action that occurred that generated the log entry.

Manage Logs

Reset Logs

WebUI Procedure

1. Go to *Tracking :: Discovery Logs*.
2. Click **Reset Logs**.

The table is cleared.

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.

Interface sub-tab

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

Open Sessions	Event List	System Usage	Discovery Logs	Network	Devices	Scheduler	HW Monitor	ZPE Cloud
Interface	LLDP	Routing Table	IPsec	Wireguard	Hotspot	QoS		
Tracking :: Network :: Interface								Reload
IfName	IfIndex	State	Rx Packets	Tx Packets	Collisions	Dropped	Errors	
eth0	6	Up	40763	25914	0	0	0	
eth1	5	Down	0	0	0	0	0	
eth2	7	Up	25311	0	0	0	0	
loopback	3	Up	0	148	0	0	0	
loopback0	4	Up	0	147	0	0	0	

Interface Table

Column name	Description
IfName	Name of interface.
IfIndex	Name of index.
State	Status of the interface.
Rx Packets	Number of receive packets.
Tx Packets	Number of transmit packets,
Collisions	Number of collisions.
Dropped	Number of dropped packets.
Errors	Number of Errors

Review Interface Details

WebUI Procedure

1. Go to *Tracking :: Network :: Interface*.
2. Click on an Interface (displays dialog of details):

Cancel

Detailed Statistics

IfName:

Speed(Mb/s):

Duplex:

Collisions:

Rx Statistics

Rx Packets:

Rx Bytes:

Rx Errors:

Rx CRC Errors:

Rx Dropped:

Rx FIFO Errors:

Rx Compressed:

Rx Frame Errors:

Rx Length Errors:

Rx Missed Errors:

Rx Over Errors:

Tx Statistics

Tx Packets:

Tx Bytes:

Tx Errors:

Tx Carrier errors:

Tx Dropped:

Tx FIFO Errors:

Tx Compressed:

Tx Aborted Errors:

Tx Heartbeat Errors:

Tx Window Errors:

Detailed Statistics (IfName, Speed, Duplex, Collisions)

Rx Statistics (Rx Packets, Rx Bytes, Rx Errors, Rx CRC Errors, Rx Dropped, Rx FIFO Errors, Rx Compressed, Rx Frame Errors, Rx Length Errors, Rx Missed Errors, Rx Over Errors)

Tx Statistics (Tx Packets, Tx Bytes, Tx Errors, Tx Carrier errors, Tx Dropped, Tx FIFO Errors, Tx Compressed, Tx Aborted Errors, Tx Heartbeat Errors, Tx Window Errors)

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

Switch Interfaces sub-tab

Open Sessions	Event List	System Usage	Discovery Logs	Network	Devices	Scheduler	HW Monitor	ZPE Cloud			
Interface	Switch Interfaces	MSTP	LLDP	Routing Table	MAC Table	IPsec	Wireguard	Hotspot	QoS	DHCP	Flow Exporter
Tracking :: Network :: Switch Interfaces Reload											
Unauthorize 802.1x Session											
<input type="checkbox"/>	Interface	Status	State	Speed	Rx Packets	Tx Packets	802.1x State	Description			
<input type="checkbox"/>	sfp0	Enabled	Down	10G	0	0	Disabled				
<input type="checkbox"/>	sfp1	Enabled	Up	1G	10036	69216	Disabled				
<input type="checkbox"/>	netS2-1	Disabled	Down	-	0	0	Disabled				
<input type="checkbox"/>	netS2-2	Disabled	Down	-	0	0	Disabled				
<input type="checkbox"/>	netS2-3	Disabled	Down	-	0	0	Disabled				
<input type="checkbox"/>	netS2-4	Disabled	Down	-	0	0	Disabled				

Set as Unauthorize 802.1x Session

WebUI Procedure

1. Go to *Tracking :: Network :: Switch Interfaces*.
2. In *Interface* column, locate and select checkbox.
3. Click **Unauthorized 802.1x Session**.

MSTP sub-tab

Open Sessions		Event List		System Usage		Discovery Logs		Network		Devices		Scheduler		HW Monitor		ZPE Cloud							
Interface		Switch Interfaces		MSTP		LLDP		Routing Table		MAC Table		IPsec		Wireguard		Hotspot		QoS		DHCP		Flow Exporter	
Tracking :: Network :: MSTP Reload																							
Notice: Spanning Tree is Disabled in Switch :: Global																							
MST Instance						VLAN List						Priority											
0						1-2						32768											

View MST Instance Details

WebUI Procedure

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

Interface		Switch Interfaces		MSTP		LLDP		Routing Table		MAC Table		IPsec		Wireguard		Hotspot		QoS		DHCP		Flow Exporter	
Tracking :: Network :: MSTP :: 0 Reload																							
Return																							
Interface						MST State						MST Role											

3. Click **Return**.

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.

Open Sessions		Event List		System Usage		Discovery Logs		Network		Devices		Scheduler		HW Monitor		ZPE Cloud	
Interface		LLDP		Routing Table		IPsec		Wireguard		Hotspot		QoS					
Tracking :: Network :: LLDP Reload																	
Connection	Type	Chassis ID	Port ID	Port Description	Age	System Name	IPv4 Mgmt Addr	IPv6 Mgmt Addr									
Local Chassis	TX	mac e4:1a:2c:00:2c:42	ifname	ifname		nodegrid.localdomain	192.168.7.20	fe80::bcab:4aff:fe24:151,fe80::acc9:fdff:feb2:fc95,fe80::e61a:2cff:fe0c									

LLDP Table

Column name	Description
Connection	Type of connection.
Type	Type of transmission (Tx, Rx).
Chassis ID	Chassis identification number.
Port ID	Port identification.
Port Description	Description of the port.
Age	Age of the LLDP
System Name	Name of the system.
IPv4 Mgmt Addr	IPv4 management address.
IPv6 Mgmt Addr	IPv6 management address.

Routing Table sub-tab

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

Open Sessions	Event List	System Usage	Discovery Logs	Network	Devices	Scheduler	HW Monitor	ZPE Cloud
Interface	LLDP	Routing Table	IPsec	Wireguard	Hotspot	QoS		
Tracking :: Network :: Routing Table								Reload
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:2c:ff:fe00:2c42	eth0			

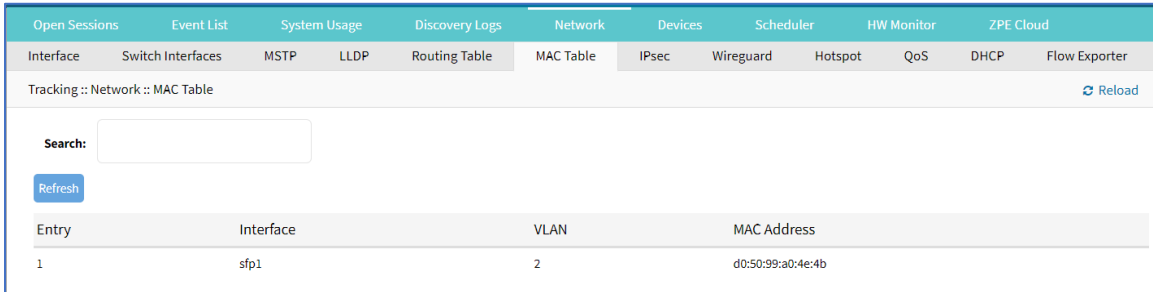
Routing Table

Column name	Description
Destination	Destination IP address.
Gateway	Gateway IP address.
Metric	Metric value.
Interface	Type of interface.

Column name	Description
From	From IP address.
Table	Table interface.

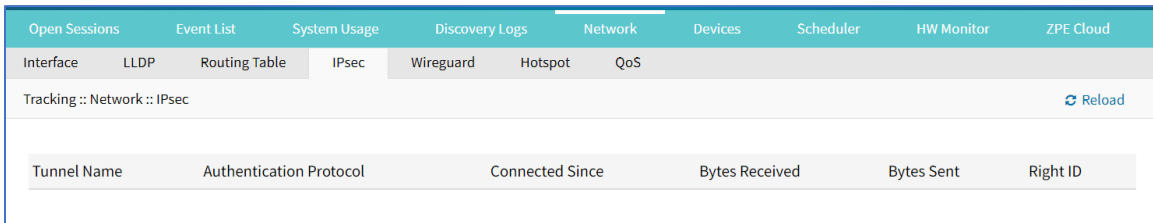
MAC Table sub-tab

(read only) This displays information in MAC settings.



IPsec sub-tab

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



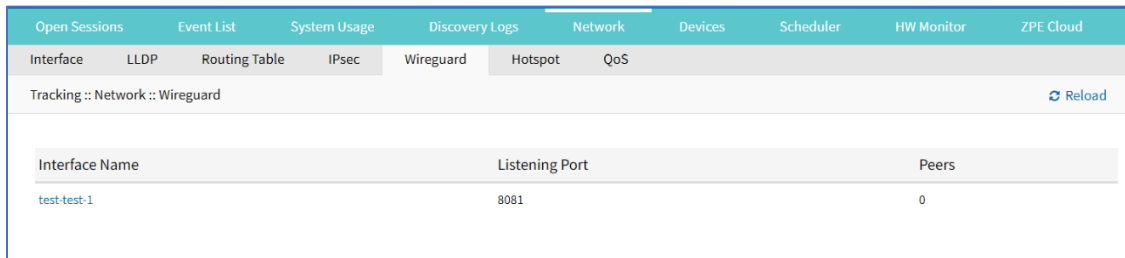
To appear on the IPsec list, Monitoring must be enabled for each IPsec tunnel.

IPsec Table

Column name	Description
Tunnel Name	Name of the tunnel.
Authentication Protocol	Protocols used for authentication.
Connected Since	Current connection time
Bytes Received	Bytes received by IPsec.
Bytes Sent	Bytes sent by IPsec.
Right ID	Tunnel right ID.

Wireguard sub-tab

This shows the Wireguard connection details.



Interface Name	Listening Port	Peers
test-test-1	8081	0

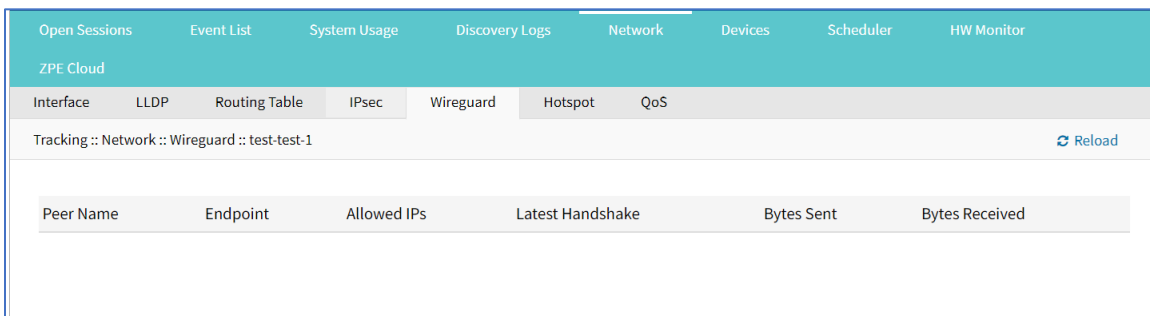
Wireguard Table

Column name	Description
Interface Name	Name of the Interface.
Listening Port	Port that Wireguard is listening.
Peers	Associated Wireguard peers

View Details on Wireguard Configuration

WebUI Procedure

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

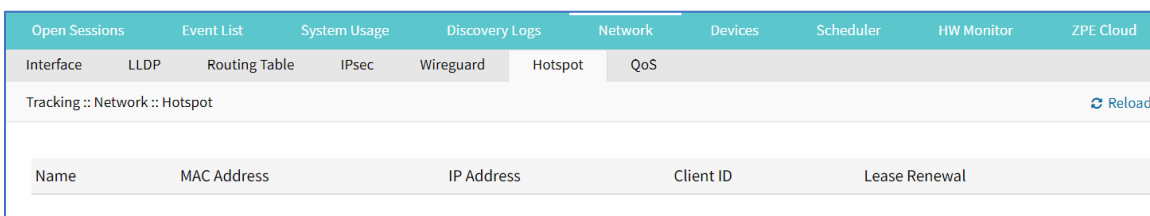


Peer Name	Endpoint	Allowed IPs	Latest Handshake	Bytes Sent	Bytes Received

3. Review details.

Hotspot sub-tab

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



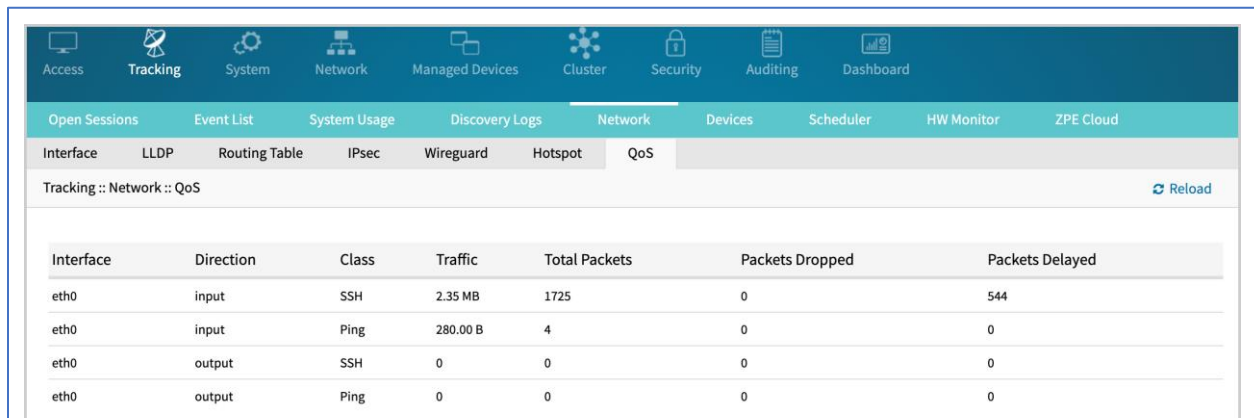
Name	MAC Address	IP Address	Client ID	Lease Renewal

Hotspot Table

Column name	Description
Name	Name of hotspot.
MAC Address	MAC address of hotspot
IP Address	IP address of hotspot.
Client ID	ID of the client.
Lease Renewal	Renewal date.

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
eth0	input	SSH	2.35 MB	1725	0	544
eth0	input	Ping	280.00 B	4	0	0
eth0	output	SSH	0	0	0	0
eth0	output	Ping	0	0	0	0

QoS Table

Column name	Description
Interface	Name of interface.
Direction	Direction (Input, Output).
Class	Class (SSH, Ping)
Traffic	Amount of traffic (MB).
Total Packets	Total number of packets.
Packets dropped	Number of dropped packets.
Packets delayed	Number of delayed packets.

DHCP sub-tab

(read-only) This displays DHCP information.

Open Sessions		Event List		System Usage		Discovery Logs		Network		Devices		Scheduler		HW Monitor		ZPE Cloud	
Interface	Switch Interfaces	MSTP	LLDP	Routing Table	MAC Table	IPsec	Wireguard	Hotspot	QoS	DHCP	Flow Exporter						
Tracking :: Network :: DHCP ↻ Reload																	
IP Address				MAC Address				Hostname				Lease Expiration					

Flow Exporter sub-tab

(read-only) This displays Flow Exporter details.

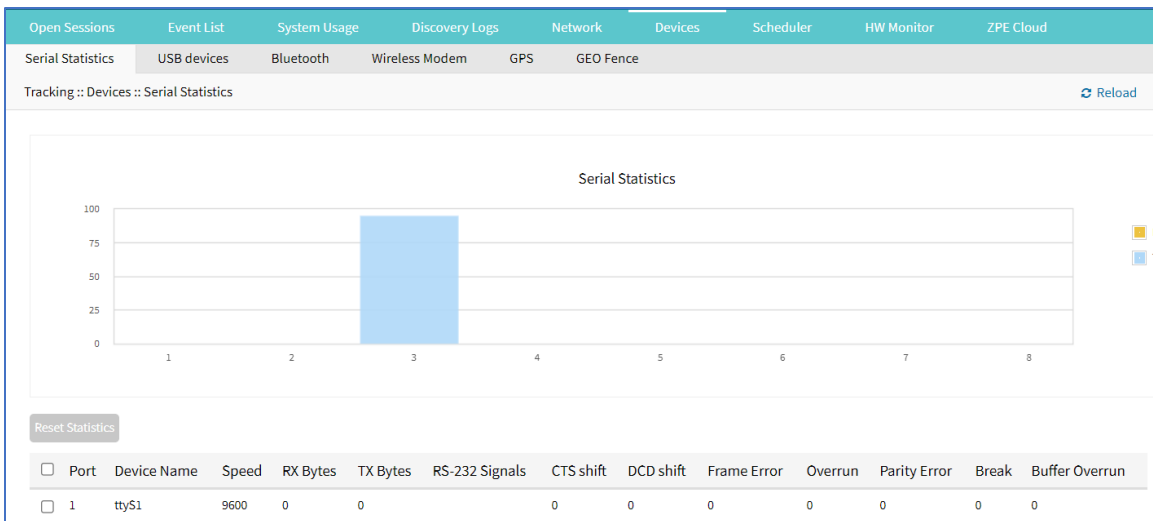
Open Sessions		Event List		System Usage		Discovery Logs		Network		Devices		Scheduler		HW Monitor		ZPE Cloud	
Interface	Switch Interfaces	MSTP	LLDP	Routing Table	MAC Table	IPsec	Wireguard	Hotspot	QoS	DHCP	Flow Exporter						
Tracking :: Network :: Flow Exporter ↻ Reload																	
Name			Interface			Flows			Packets			Bytes					

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.



Reset Statistics Table

Column name	Description
Port	Port number.
Device Name	Name of device.
Speed	Speed (bps).
RX Bytes	Amount of received bytes.
TX Bytes	Amount of transmitted bytes.
RS-232 Signals	Type of RS-232 signals.
CTS shift	Number of CTS shifts.
DCD shift	Number of DCD shifts.
Frame Error	Number of frame errors.
Overrun	Number of overruns.
Parity Error	Number of parity errors.
Break	Number of breaks.
Buffer Overrun	Number of buffer overruns.

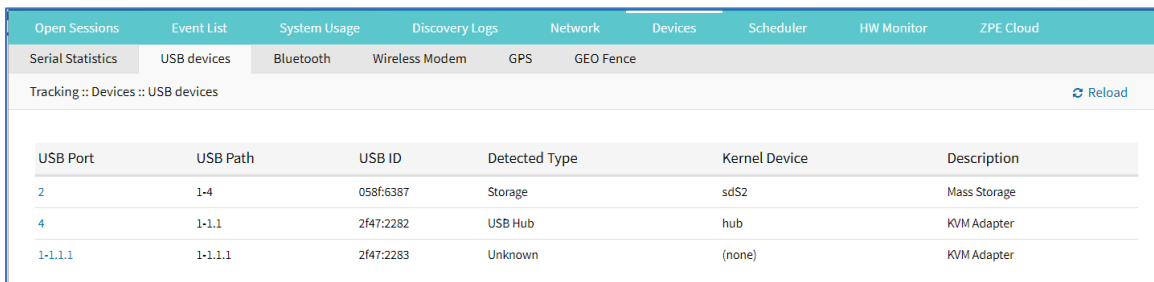
Reset Statistics

WebUI Procedure

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

USB devices sub-tab

This provides details about connected USB devices and initialized drivers.



USB Port	USB Path	USB ID	Detected Type	Kernel Device	Description
2	1-4	058f:6387	Storage	sdS2	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

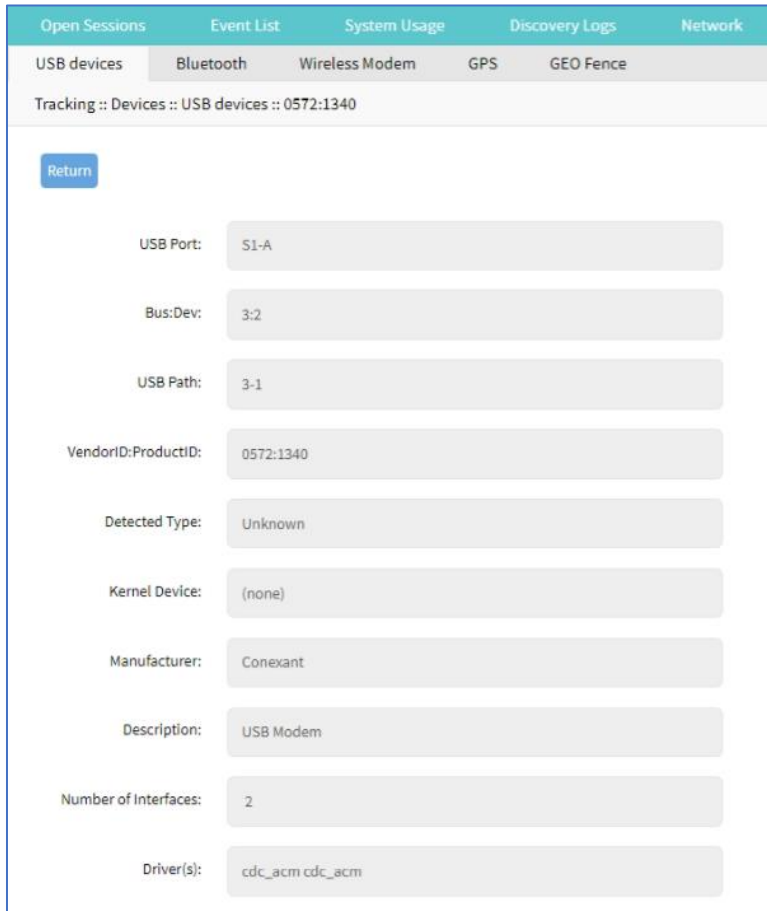
USB Devices Table

Column name	Description
USB Port	USB port number
USB Path	USB path.
USB ID	USB identification.
Detected Type	Type of interface.
Kernel Device	Kernel interface type.
Description	Description of USB.

View USB Device Details

WebUI Procedure

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



The screenshot shows a web interface with a navigation bar at the top containing 'Open Sessions', 'Event List', 'System Usage', 'Discovery Logs', and 'Network'. Below this is a sub-menu with 'USB devices', 'Bluetooth', 'Wireless Modem', 'GPS', and 'GEO Fence'. The main content area is titled 'Tracking :: Devices :: USB devices :: 0572:1340' and features a 'Return' button. The device details are displayed as follows:

- USB Port: 51-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 M.2 Analog Modem to USB Serial Device

WebUI Procedure

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

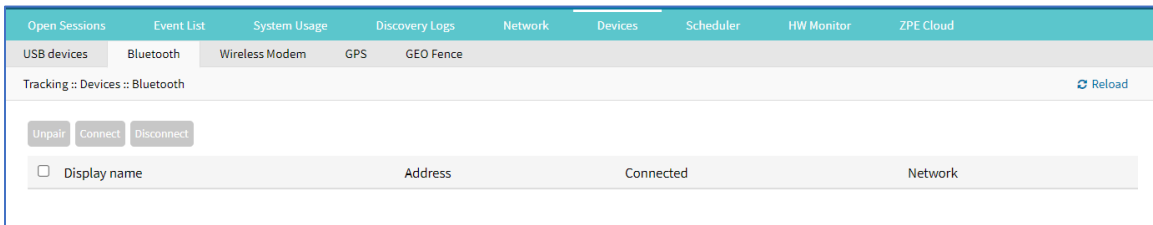
Convert USB Analog Modem to USB Serial Device

WebUI Procedure

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

Bluetooth sub-tab

This displays information about Bluetooth devices.



Bluetooth Table

Column name	Description
Display Name	Displayed name of Bluetooth.
Address	IP Address of Bluetooth.
Connected	Connection status.
Network	Network of Bluetooth.

Unpair Bluetooth

WebUI Procedure

1. Go to *Tracking :: Devices :: Bluetooth*.

2. Select checkbox.
3. Click **Unpair**.

Connect Bluetooth

WebUI Procedure

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


Disconnect Bluetooth

WebUI Procedure

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

Wireless Modem sub-tab

This displays information about wireless modem.

Open Sessions		Event List		System Usage		Discovery Logs		Network		Devices		Scheduler		HW Monitor		ZPE Cloud	
USB devices		Bluetooth		Wireless Modem		GPS		GEO Fence									
Tracking :: Devices :: Wireless Modem ↻ Reload																	
Slot	Interface	Status	SIM State	Active	Data Consumption	Operator	Radio Mode	Signal Strength									
S1-B	cdc-wdm1	Disconnected	Registered	SIM 1	0 B / --GB	AT&T	LTE	70% 									

View Wireless Modem Details

WebUI Procedure

1. Go to *Tracking :: Devices :: Wireless Modem*.
2. In *Slot* column, click on name (displays dialog).

Open Sessions | Event List | System Usage | Discovery Logs | Network | Devices | Scheduler | HW Monitor | ZPE Cloud

Serial Statistics | USB devices | Bluetooth | Wireless Modem | GPS | GEO Fence

Tracking :: Devices :: Wireless Modem :: Channel-A

[Return](#)

Modem Information

Slot: Channel-A

Modem Model: EM7565

Firmware Version: SW9X50C_01.14.02.00

Hardware Version: 1.0

Carrier Configuration: ATT

Equipment ID (IMEI): 353533101043225

Interface: cdc-wdm0

Status: Disconnected

Current Operator: AT&T MicroCell

Temperature (Celsius): 55

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

SIM data usage monitoring should be enabled in Network :: Connections.

SIM 1 Information

Data Usage Signal Strength

[Reset](#)

Last Update: Tue Nov 23 13:18:53 2021

SIM Status: Active

Subscriber ID: 310410256791820

Circuit Card ID: 89014103272567918202

Operator: AT&T MicroCell

Phone Number Discovered:

SIM State: Registered

Connection: LTE

Signal Strength: 67%

SIM 2 Information

Data Usage Signal Strength

[Reset](#)

Last Update:

SIM Status: Inactive

Subscriber ID:

Circuit Card ID:

Operator:

Phone Number Discovered:

SIM State:

Connection:

Signal Strength: 0%

3. Review details.

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

GPS sub-tab

This provides information about GPS details (when installed).

Open Sessions		Event List		System Usage		Discovery Logs		Network		Devices		Scheduler		HW Monitor		ZPE Cloud	
USB devices		Bluetooth		Wireless Modem		GPS		GEO Fence									
Tracking :: Devices :: GPS :: S1-B ↻ Reload																	
Configured Coordinates (Lat,Lon): 0,0																	
Slot	Coordinates (Lat,Lon)		Distance (m)		Update Time (UTC)		Device Name										

GEO Fence sub-tab

(if enabled) This provides map of GEO Fence location. View can be zoomed in or out.

Open Sessions		Event List		System Usage		Discovery Logs		Network		Devices		Scheduler		HW Monitor		ZPE Cloud	
Serial Statistics		USB devices		Bluetooth		Wireless Modem		GPS		GEO Fence							
Tracking :: Devices :: GEO Fence ↻ Reload																	
Update Time (UTC)	Coordinates (Lat,Lon)		Distance (m)		Device Name												

Scheduler tab

This provides information about scheduled tasks.

Open Sessions		Event List		System Usage		Discovery Logs		Network		Devices		Scheduler		HW Monitor		ZPE Cloud	
Tracking :: Scheduler ↻ Reload																	
<div style="border: 1px solid #ccc; padding: 2px; display: inline-block; margin-bottom: 5px;">Reset Log</div>																	
Task Name	User	Date	PID	Event	Error												

Scheduler Table

Column name	Description
Task Name	Name of scheduled task.
User	User who initiated task.
Date	Date of task.
PID	Product identification.
Event	Event name.
Error	Error description.

Reset Log

WebUI Procedure

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

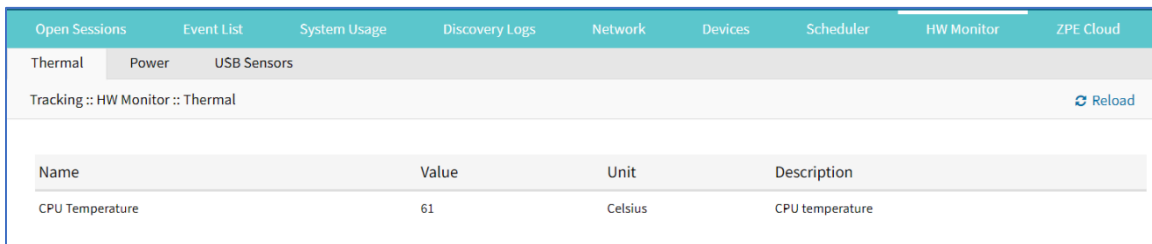
HW Monitor tab

This displays Nodegrid system information. Content is read only.

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	61	Celsius	CPU temperature

Thermal Table

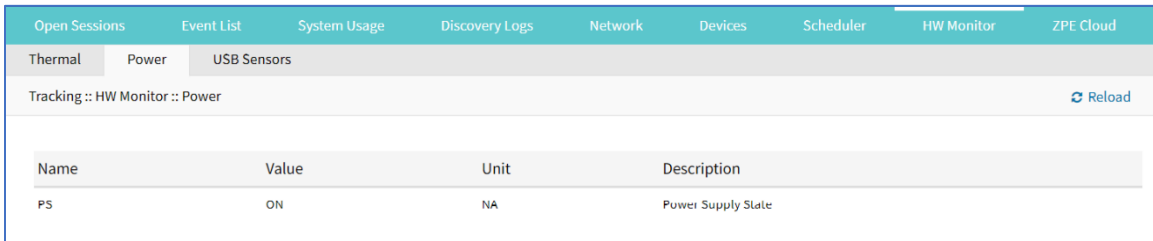
Column name	Description
Name	Name of thermal measurement.
Value	Current value

Column name	Description
Unit	Type of measurement (i.e., C).
Description	Description of thermal type.

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

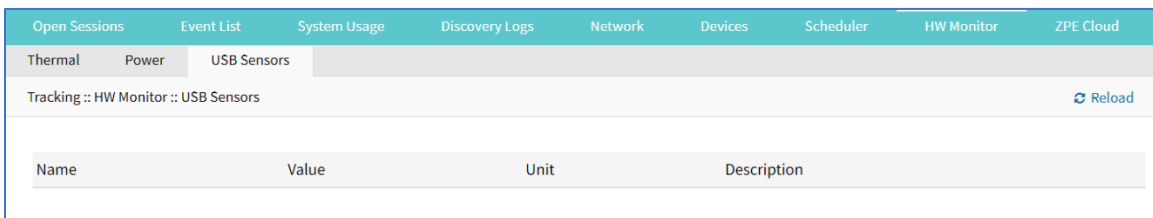
Power Table

Column name	Description
Name	Name of power source.
Value	Current value
Unit	Type of measurement
Description	Description of power source.

USB Sensors sub-tab

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


NOTE: The details shown depend on the Nodegrid model.



Name	Value	Unit	Description
------	-------	------	-------------

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.


x

Sensors Status

Name	Value	Unit	Description
Description		Value	
Name	usbS3-8		
Status	Unknown		
Type	usb_sensor		
Mode	Enabled		
Licensed	Yes		
Nodegrid Host	nodegrid-JamieNSR2.175.localdomain		
Groups	admin		

Supported USB Sensors

USB Device	Vendor
USB Serial	FTDI, CP2105, CP210X
USB KVM	ZPE's KVM-U01 - KVM over USB dongle (VGA, USB kb, USB mouse)
USB Sensor	ZPE's THS-U01 - temperature & humidity, Degree Controls F200 - Air Velocity Sensor (paired with TTL-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

NOTE: 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 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 - °C
Degree Controls F200	Air temperature and velocity sensors	No	1 Air Temperature - °C 1 Air Velocity - m/s
Homologated Generic USB I/O Device	All in one	100-On/Off	100 generic - any

Additional Supported USB Devices

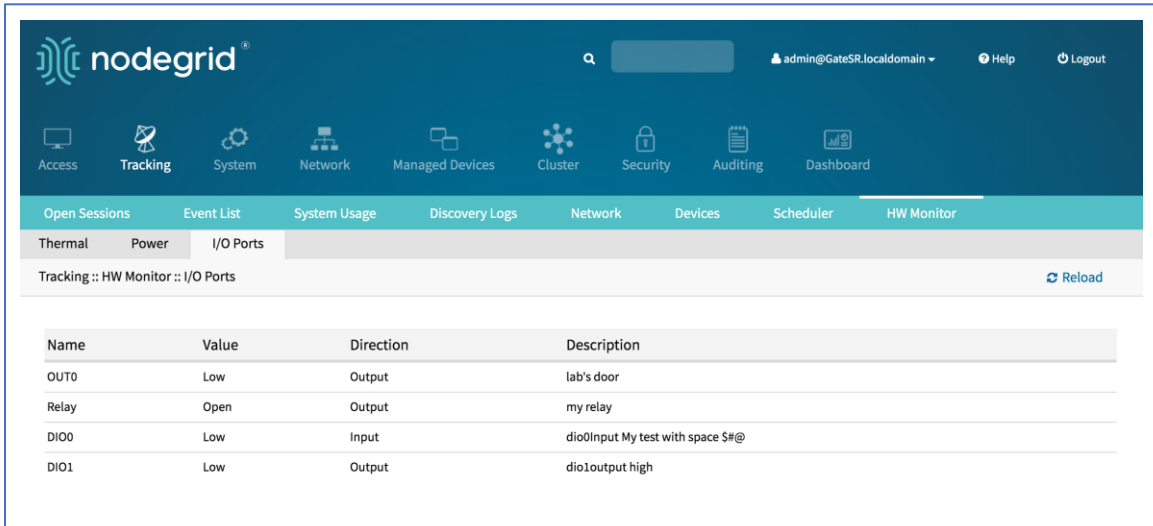
USB i/O Device	GPIO output	Relay	Light	Buzzer
Numato GP80001E	UP TO 8 – On, Off	No	No	No
Numato USBPOWRL001	UP TO 4 – On, Off	2 – On, Off	No	No
Delcom USB HID 9040XX	No	No	3 – On, Off, continuous cycle	1 – On, Off, continuous cycle
Patlite LR6-USB-W/K	No	No	1 – On, Off, continuous cycle	1 – On, Off, 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)

NOTE: This is specific to Gate SR and Link SR.

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

Example – Nodagrid Gate SR WebUI



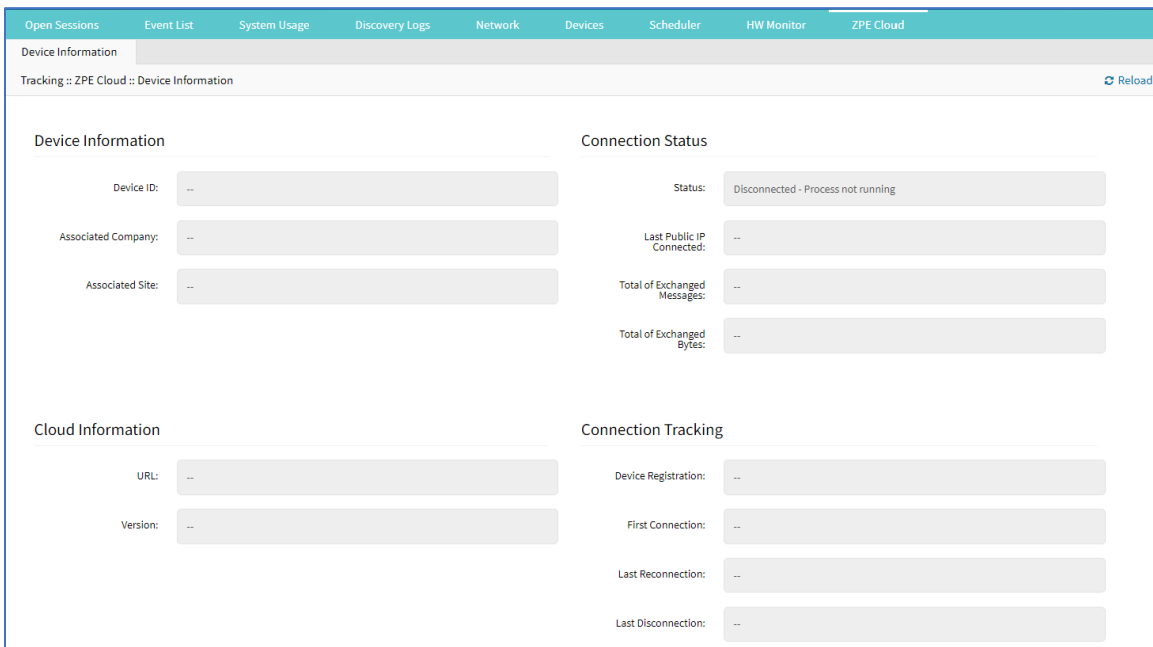
The screenshot shows the Nodegrid interface with the 'HW Monitor' tab selected. Under 'HW Monitor', the 'I/O Ports' sub-tab is active. The page title is 'Tracking :: HW Monitor :: I/O Ports'. Below the title is a table with the following data:

Name	Value	Direction	Description
OUT0	Low	Output	lab's door
Relay	Open	Output	my relay
DIO0	Low	Input	dio0Input My test with space S#@
DIO1	Low	Output	dio1output high

ZPE Cloud tab

This is used to configure connections with the ZPE Cloud application. Details groups are:

- Device Information
- Connection Status
- Cloud Information
- Connection Tracking



The screenshot shows the Nodegrid interface with the 'ZPE Cloud' tab selected. The page title is 'Tracking :: ZPE Cloud :: Device Information'. The content is organized into four sections:

- Device Information:** Fields for Device ID, Associated Company, and Associated Site, all showing "--".
- Connection Status:** Fields for Status (Disconnected - Process not running), Last Public IP Connected, Total of Exchanged Messages, and Total of Exchanged Bytes, all showing "--".
- Cloud Information:** Fields for URL and Version, both showing "--".
- Connection Tracking:** Fields for Device Registration, First Connection, Last Reconnection, and Last Disconnection, all showing "--".

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** (All SLA metrics are violated, or 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, the following message displays.



If topology is not yet configured inside the device, the following message displays.



If there is an error communicating with the SD-WAN daemon, the following message displays.



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_f10608 1 up 22.6ms / 400ms 0.1ms / 50ms 0.0% / 5% 788788 2295720 0 0
eth1 l2_eth_f10608 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.

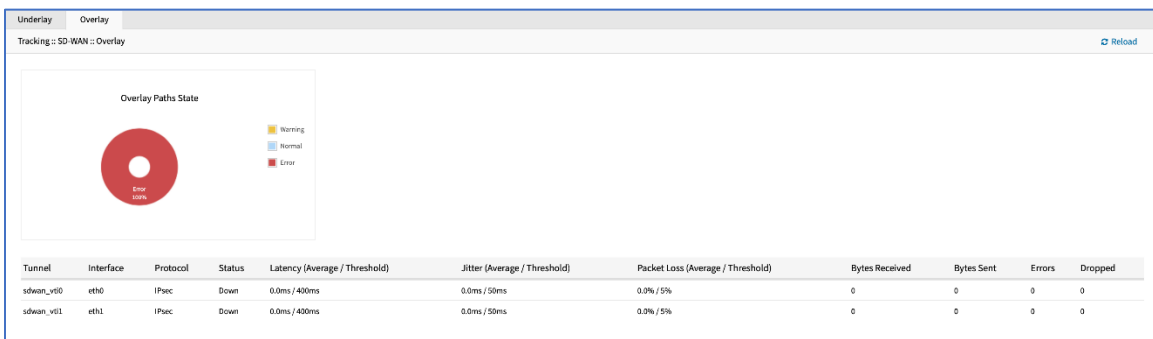
Underlay sub-tab

This shows the status of the Underlay path.



Overlay sub-tab

This shows the status of the Overlay path.



System Section

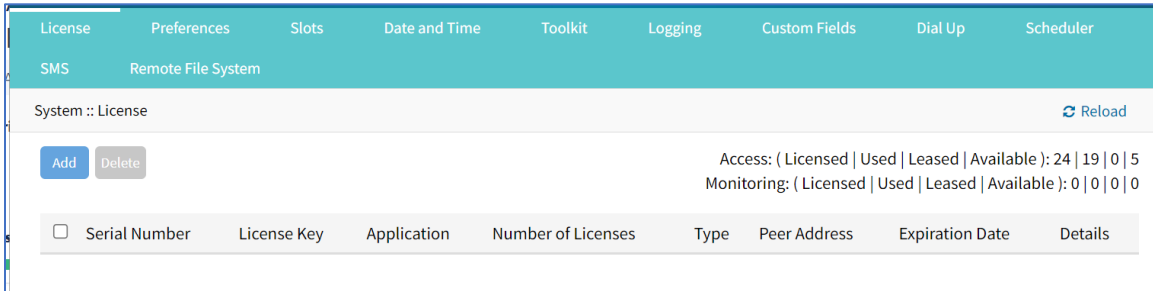
System settings are configured for each device, including license keys, general system settings, firmware updates, backup and restore, and more.

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.



The right side lists available license details:

Access: (Licensed | Used | Leased | Available): 17 | 12 | 0 | 5

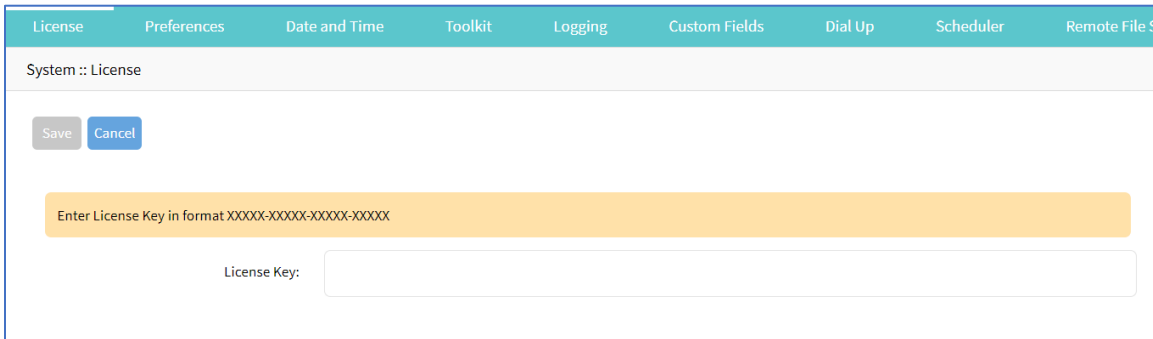
Monitoring: (Licensed | Used | Leased | Available): 0 | 0 | 0 | 0

Manage Licenses

Add a License

WebUI Procedure

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



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

Delete a License

WebUI Procedure

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

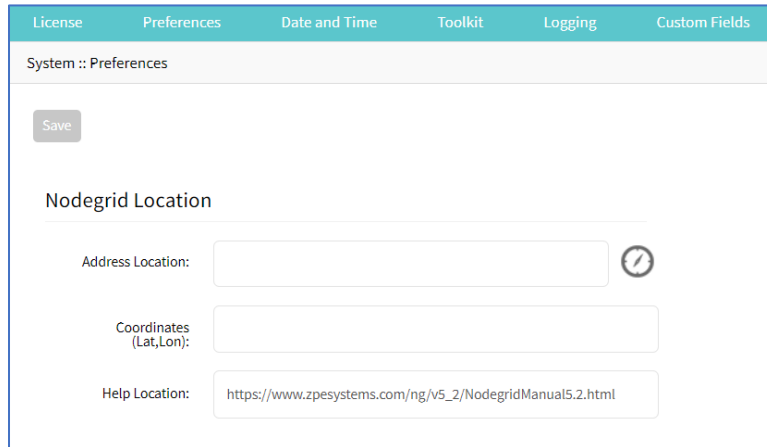
Preferences tab

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

Manage Preferences

Modify Nodegrid Location

This is the device location, shown on the Device Map.




WebUI Procedure

1. Go to *System :: Preferences*.

2. In the *Nodegrid Location* menu:

Enter **Address Location** (a valid address for the device location).

Enter **Coordinates (Lat, Lon)** (if GPS is available, click **Compass** icon  or manually enter GPS coordinates).

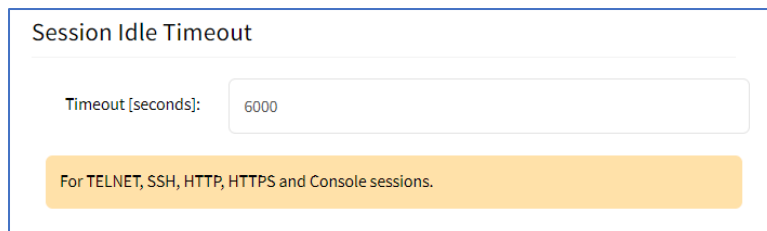
For **Help Location**, enter alternate URL location for the User Guide.

NOTE: The administrator can download the documentation from ZPE (HTML5 or PDF, as preferred) to be available for users (when **Help** icon is clicked).

3. When done, click **Save**.

Modify Session Idle Timeout

This is the number of seconds of session inactivity until the session times out and logs the user off.



WebUI Procedure

1. Go to *System :: Preferences*.

- 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.

NOTE: Any change in value is applied on the next login.

In **Timeout (seconds)**, enter one of these:

zero (0) – the session will never expire.

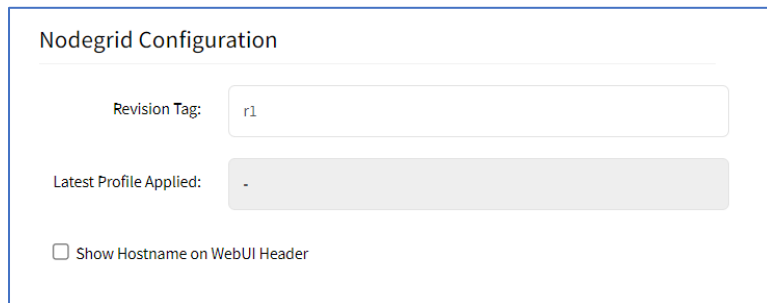
Value (i.e., 6000 keeps session active for 100 minutes).

- Click **Save**.

Modify Nodegrid Configuration

The Revision Tag field is a free format string used as a configuration reference tag. This field can be manually updated or updated with an automated change management process.

The **Latest Profile Applied** (read-only) is the last applied profile (ZTP process or on ZPE Cloud).



The screenshot shows a 'Nodegrid Configuration' form with the following fields:

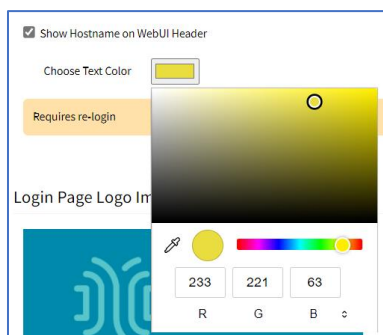
- Revision Tag:** A text input field containing 'r1'.
- Latest Profile Applied:** A read-only text field containing '-'.
- Show Hostname on WebUI Header:** An unchecked checkbox.

WebUI Procedure

- Go to *System :: Preferences*.
- In the *Nodegrid Configuration* menu:

Enter **Revision Tag**.

(optional) Select **Show Hostname on WebUI Header** checkbox (displays the device hostname on the WebUI banner. Select color (click in color grid or enter RGB or CYMK).

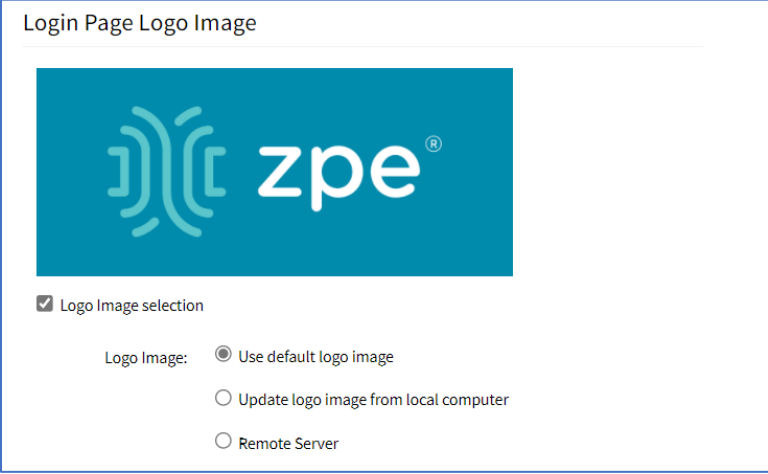


The screenshot shows the 'Show Hostname on WebUI Header' checkbox checked. Below it is a 'Choose Text Color' section with a color picker. The color picker shows a yellow color selected. Below the color picker is a color grid and an RGB input field with values 233, 221, and 63 for R, G, and B respectively.

- Click **Save**.

Modify Login Page Logo Image

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>://<ServerAddress>/<Remote File>.



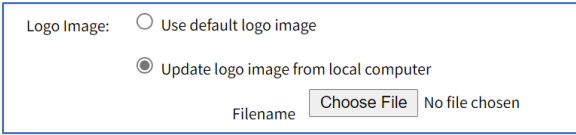
WebUI Procedure

1. Go to *System :: Preferences*.
2. In the *Logo Page Logo Image* menu:
3. (optional) Select **Logo Image selection** checkbox.

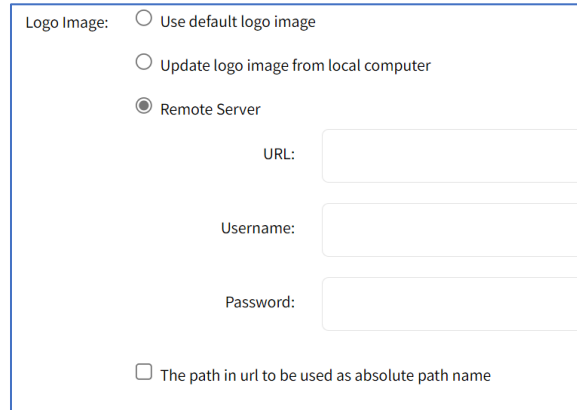
In *Logo Image* menu, select one:

Use default logo image radio button.

Update log image from local computer radio button. Click **Choose File** to locate and select logo (jpg, png).



Remote Server radio button. Enter **URL, Username, Password**. (as needed) Select **The path in url to be used as absolute pathname** checkbox.

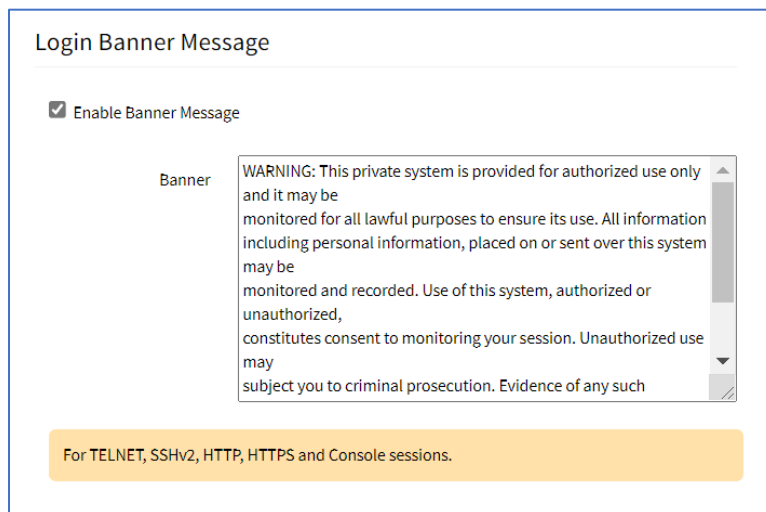


4. Click **Save**.
5. After upload, refresh the browser cache to display the new image.

Modify Login Banner Message

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.

WARNING: This private system is provided for authorized use only and it may be monitored for all lawful purposes to ensure its use. All information including personal information, placed on or sent over this system may be monitored and recorded. Use of this system, authorized or unauthorized, constitutes consent to monitoring your session. Unauthorized use may subject you to criminal prosecution. Evidence of any such unauthorized use may be used for administrative, criminal and/or legal actions.



The message can include device-specific information, such as Device Alias or other device identifier detail.

WebUI Procedure

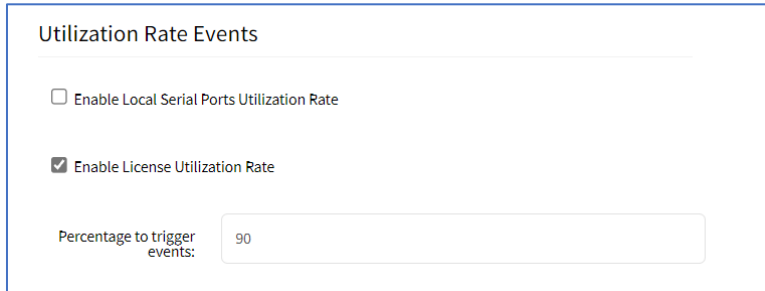
1. Go to *System :: Preferences*.
2. In the *Login Banner Message* menu:
 - Click in **Banner**.

Modify text, as needed (to control line length, use *Enter* for hard returns).

3. Click **Save**.

Modify Utilization Rate Events

This sets up event notifications for utilization rates.

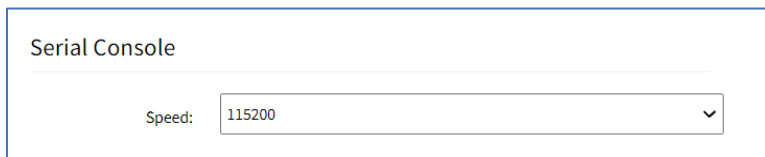


WebUI Procedure

1. Go to *System :: Preferences*.
2. In the *Utilization Rate Events* menu:
 (optional) Select **Enable Local Serial Ports Utilization Rate** checkbox.
 Select **Enable License Utilization Rate** checkbox and enter **Percentage to trigger events**. (An event notification is generated when the entered percentage is reached.)
3. Click **Save**.

Modify Serial Console

This displays the baud speed of the device.



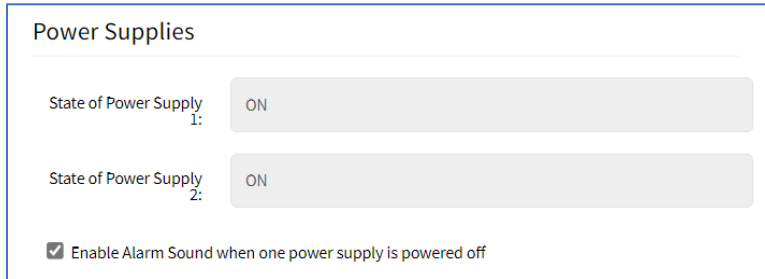
WebUI Procedure

1. Go to *System :: Preferences*.
2. In the *Serial Console* menu:
 On **Speed** drop-down, select baud rate (**9600, 19200, 38400, 57600, 115200**).
3. Click **Save**.

Modify Power Supplies

NOTE: This displays only when device is equipped with 2 power supplies)

Option to enable alarm when powered off.



Power Supplies

State of Power Supply 1: ON

State of Power Supply 2: ON

Enable Alarm Sound when one power supply is powered off

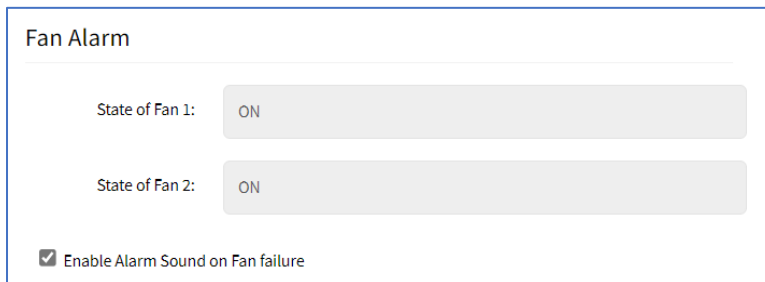
WebUI Procedure

1. Go to *System :: Preferences*.
2. In the *Power Supplies* menu:
 Select **Enable Alarm Sound when one power supply is powered off** checkbox.
3. Click **Save**.

Modify Fan Alarm

NOTE: This displays only when device is equipped with fans.

Option to sound alarm on fan failure.



Fan Alarm

State of Fan 1: ON

State of Fan 2: ON

Enable Alarm Sound on Fan failure

WebUI Procedure

1. Go to *System :: Preferences*.
2. In the *Fan Alarm* menu:
 Select **Enable Alarm Sound on Fan Failure** checkbox.
3. Click **Save**.

Modify Network Boot

Nodegrid can boot from a network ISO image. Enter the unit's IPv4 address and netmask, ethernet interface (eth0 or eth1), and ISO image URL. Use this URL format:
 http://ServerIPAddress/PATH/FILENAME.ISO

Network Boot

Unit IPv4 Address:

Unit Netmask:

Unit Interface:

ISO URL:

WebUI Procedure


1. Go to *System :: Preferences*.
2. In the *Network Boot* menu:
 - Enter **Unit IPv4 Address**.
 - Enter **Unit Netmask**.
 - On **Unit Interface** drop-down, select one (**eth0**, **eth1**).
 - Enter **ISO URL**.
3. Click **Save**.

Slots tab (SR only)

This information identifies slots on SR devices with installed modules.

License Preferences **Slots** Date and Time Toolkit Logging Custom Fields Dial Up Scheduler SMS Remote File System

System :: Slots ↻ Reload

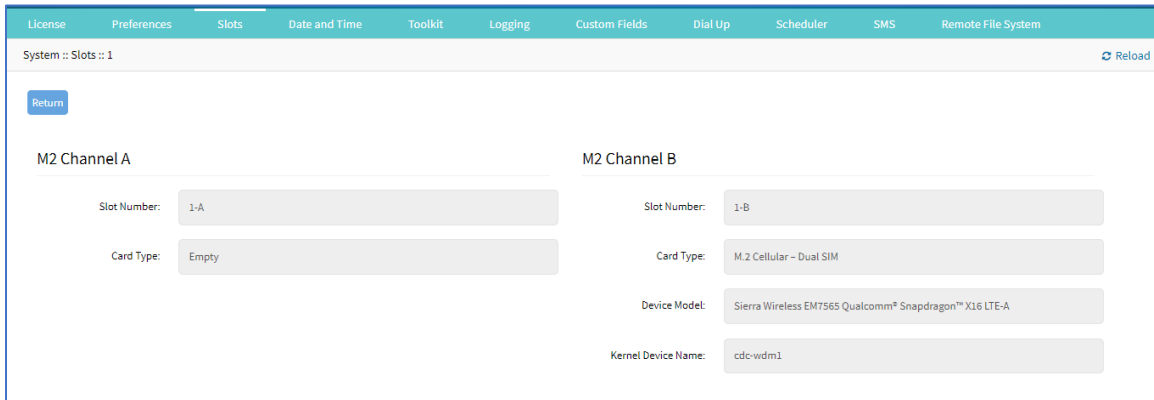


Slot Number	Card SKU	Card Type	Add-ons
slot-1	NSR-COMP-EXPN	NSR Compute Expansion Card	
slot-2	NSR-16ETH-EXPN	NSR 16-Port 1G Ethernet Expansion Card	
slot-3	NSR-8SFP-EXPN	NSR 8-Port 10G SFP Expansion Card	
slot-4	NSR-16ETH-EXPN	NSR 16-Port 1G Ethernet Expansion Card	
slot-5	Empty	Empty	

Manage Slots

Review Slot Details

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



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

Enable SATA Card in Slot 5

WebUI Procedure

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

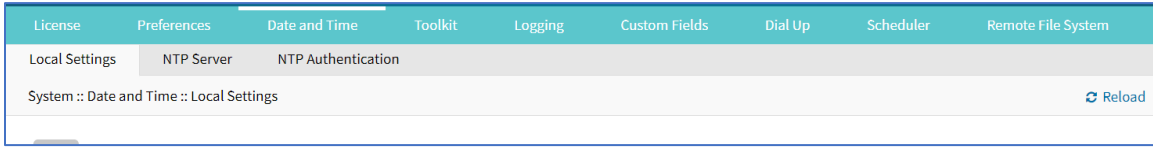


3. Select **Allow SATA card in slot 5** checkbox.
4. Click **Save**.

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).

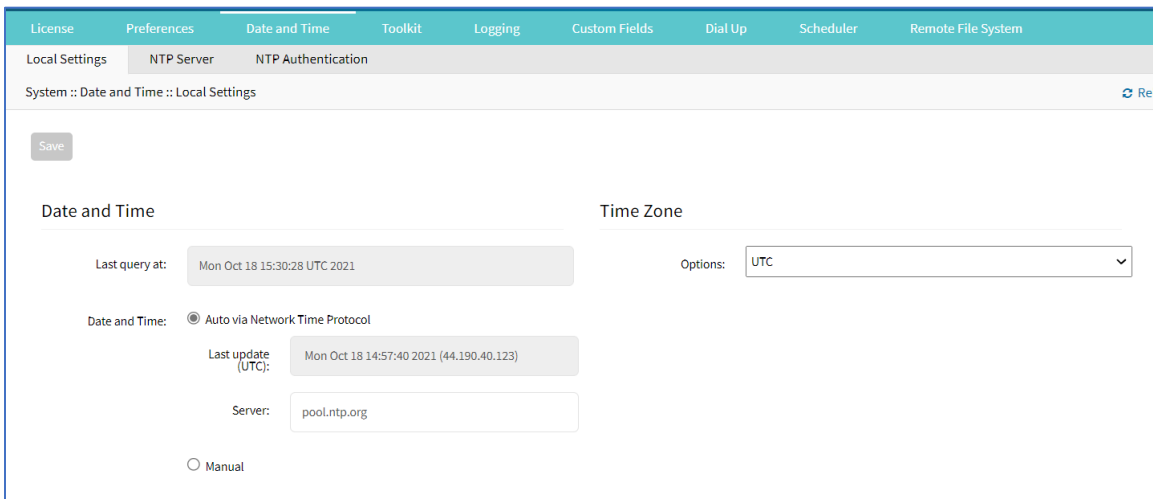
NOTE: All timestamps in Event Logs are in UTC.

Configure Local Time

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

WebUI Procedure

1. Go to *System :: Date and Time :: Local Settings*.



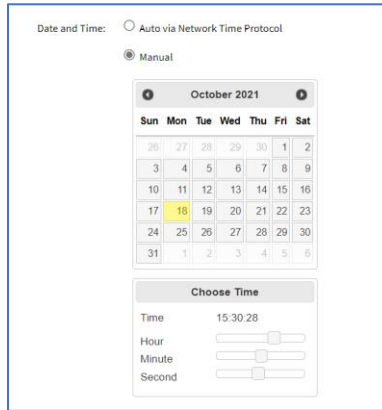
2. In *Date and Time* menu:

In *Date and Time*, select one:

Auto via Network Time Protocol radio button:

Enter **Server**.

Manual radio button:



Scroll through **Calendar** and select date.

In **Choose Time**, enter hour, minute, second.

3. In *Time Zone* menu:

On **Options** drop-down, select the appropriate time zone.

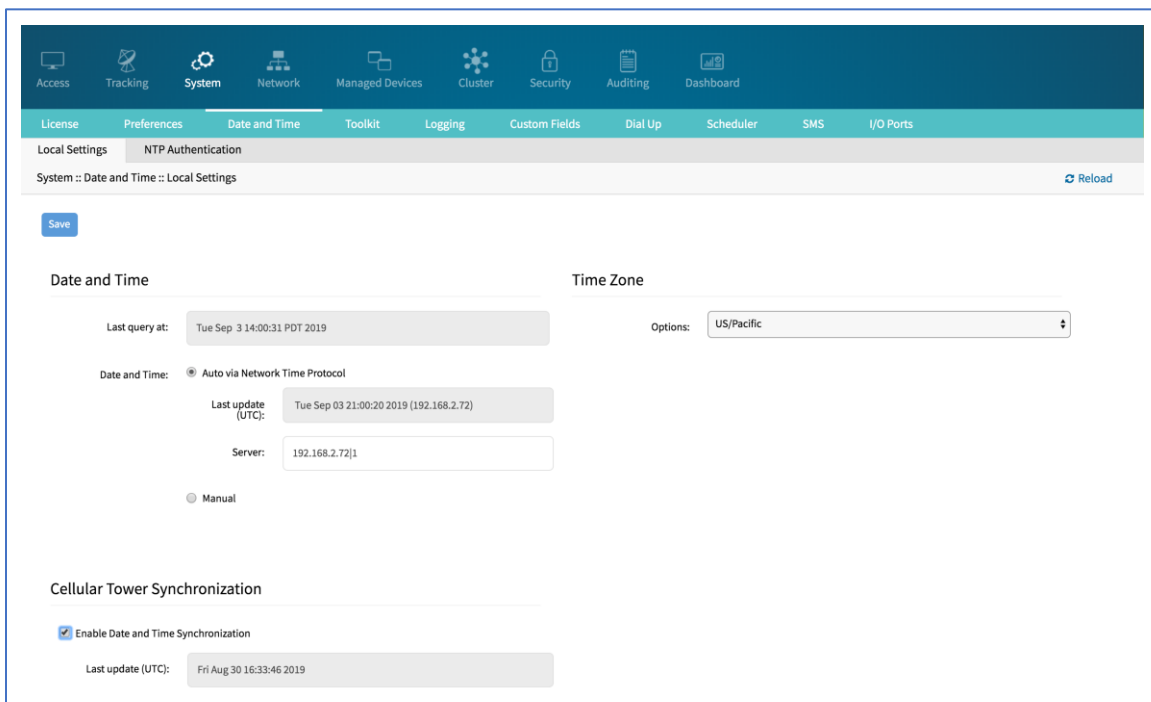
4. Click **Save**.

Cellular Tower Synchronization

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).

WebUI Procedure

1. Go to *System :: Date and Time :: Local Settings*.

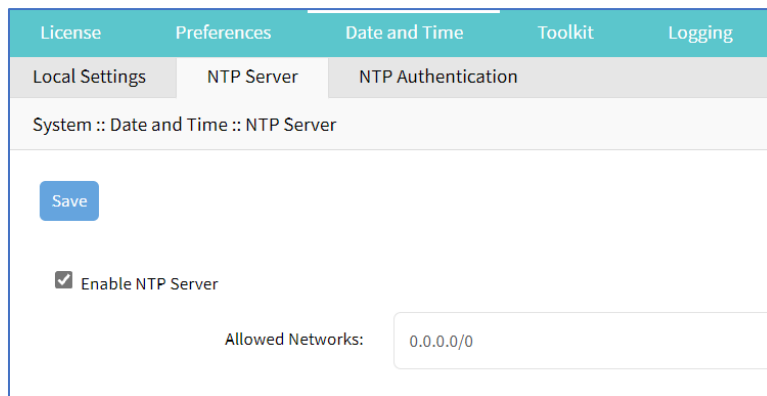


2. In *Cellular Tower Synchronization* menu:
 Select **Enable Date and Time Synchronization** checkbox.
3. Make other changes, as needed.
4. Click **Save**.

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.

NTP Server sub-tab

This page enables the NTP Server.



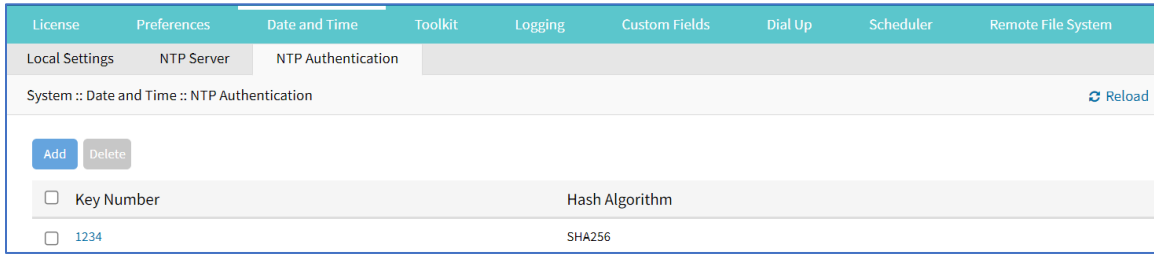
Configure the local NTP server

WebUI Procedure

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.

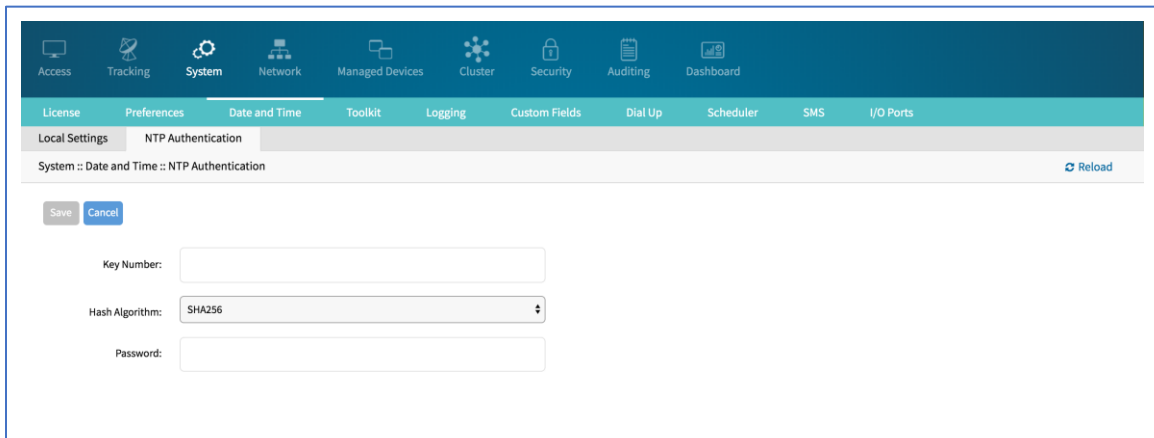


Configure Key Number Set

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

WebUI Procedure

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



3. For **Key Number**, enter 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. For **Password**, enter a character string (space character not allowed).
Alternatively, enter a hexadecimal number with prefix **HEX** followed by the number **#####**.
6. Click **Save**.

Delete Key Number

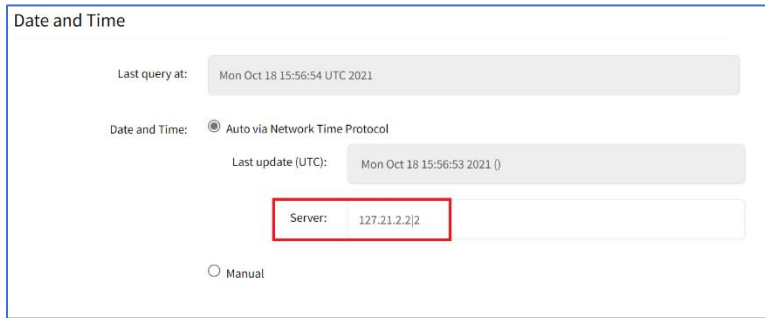
WebUI Procedure

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

WebUI Procedure

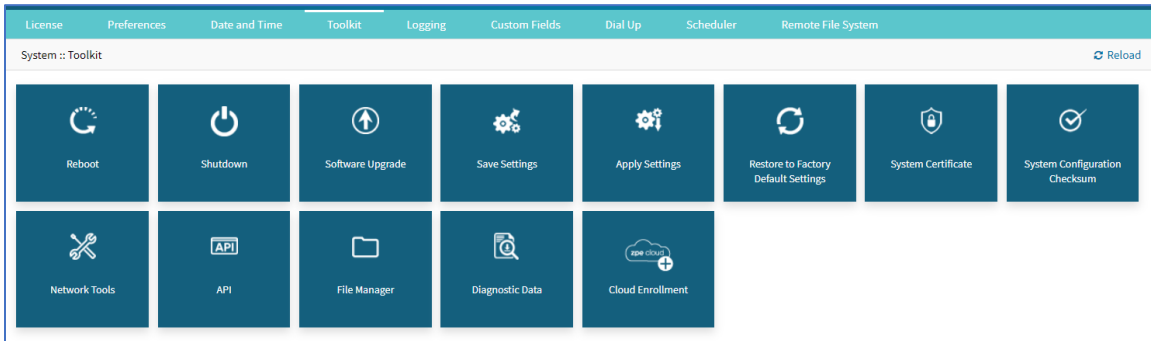
1. Go to *System :: Date and Time :: Local Settings*.
2. Use separator '|' (pipe) between server address and its key number.



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

Toolkit tab

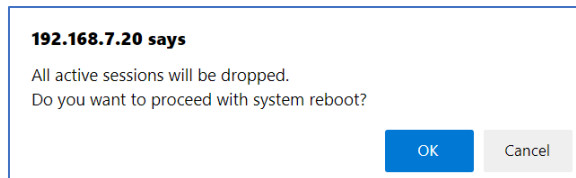
System maintenance features are available in *System :: Toolkit* page.



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.

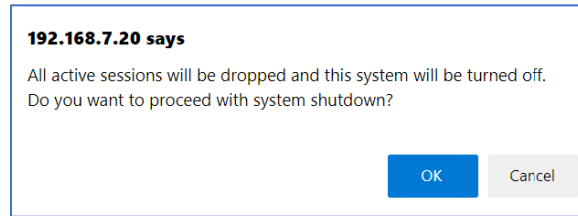
On click, displays pop-up dialog. Click **OK** to continue.



Shutdown tool

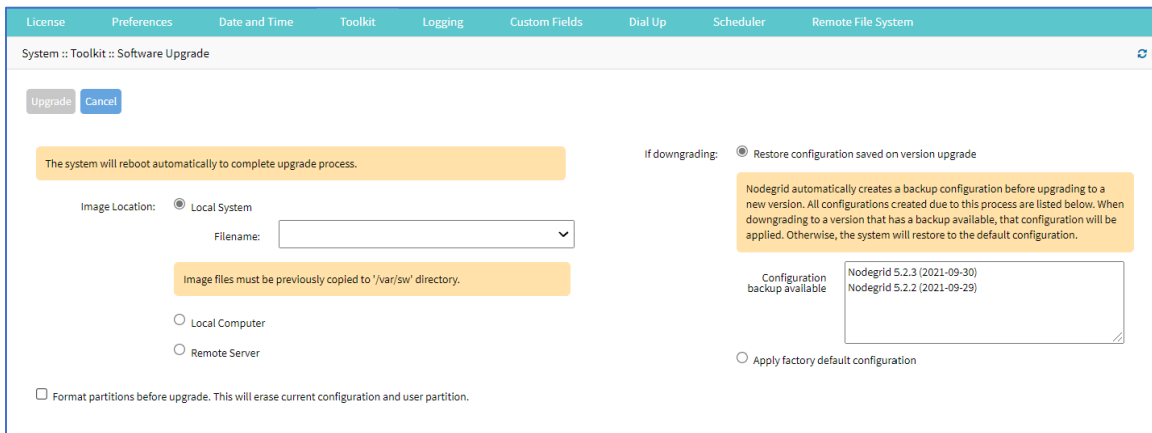
On a shutdown, the operating system will be brought to a halted state. At this point, it is safe to drop the power supply to the unit (turn off power supplies or removing power cords). To turn the unit back on, the power supply must be stopped and then restarted.

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



Software Upgrade tool

Nodegrid can be updated via the WebUI or with the CLI.



This version can be upgraded from 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 v5.8.0.

Downgrade is only allowed to v4.2.4 or newer. UEFI mode and Secure Boot must be disabled prior to downgrading to v5.0 or older.

There are three methods for device software upgrades:

- From the Nodegrid device
- From the connected local computer
- From a remote server

The new software ISO image must be previously loaded.

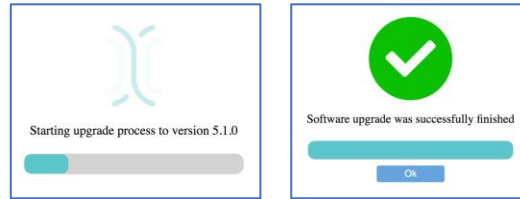
To upgrade from the Nodegrid device itself, place the new software ISO file in /var/sw.

To upgrade from a connected local computer, click on the **Local Computer** radio button. Locate and select the file.

To upgrade from a remote server, click **Remote Server** radio button. Enter the server URL and required username and password. Supported protocols: FTP, TFTP, SFTP, SCP, HTTP, and HTTPS. The URL can be the IP address or hostname/FQDN. (If using IPv6, include brackets [].)

```
ftp://192.168.22.21/downloads/Nodegrid_v5.4.1.iso
```

A status bar (WebUI only) displays progress of the software upgrade. When complete, a success dialog is displayed.



CLI Procedure

To upgrade via the CLI, execute these commands:

```
[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 5.2.1 (2020-08-16)
```

```
Nodegrid 5.0.0 (2018-05-02)
```

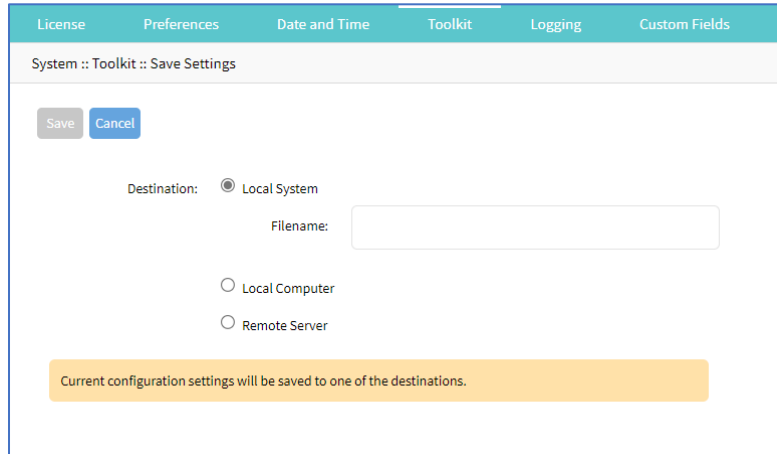
Software Downgrade

If downgrading, options are:

- Format partitions before downgrade.
- Apply factory default configuration.
- Restore a saved configuration.

Save Settings tool

This saves current configuration. Displays this dialog.



WebUI Procedure

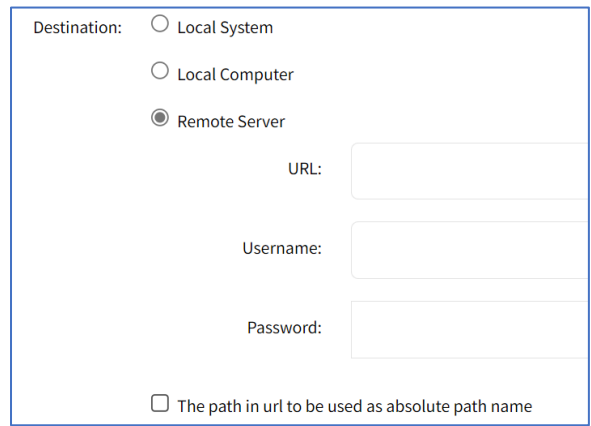
1. Go to *System :: Toolkit*.
2. Click **Save Settings** icon (displays dialog).
3. In *Destination* menu, select one.

Local System radio button. Enter **File Name**.

Local Computer radio button. Click **Save** (file is saved on the local computer *Download* folder).

Remote Server radio button. Enter **URL**, **Username**, and **Password**. (as needed) Select **Download path is absolute path name** checkbox.

The URL can be the IP address or hostname/FQDN. If using IPv6, use brackets [...].
Supported protocols: FTP, TFTP, SFTP, and SCP.



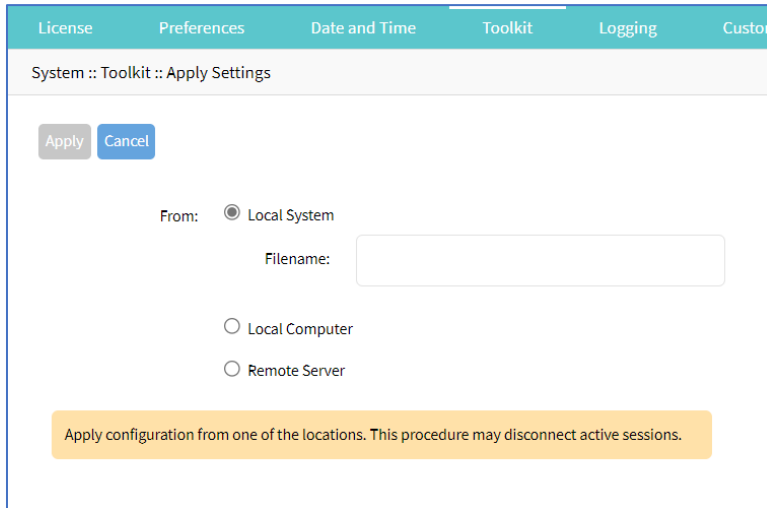
4. Click **Save**.

NOTE: The option to save to ZPE Cloud is only available if ZPE Cloud is enabled.

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.

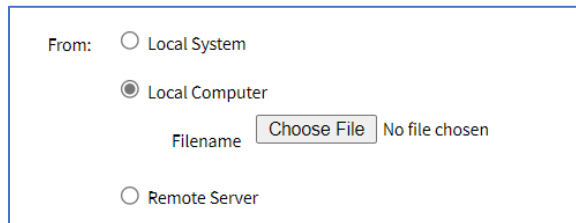


WebUI Procedure

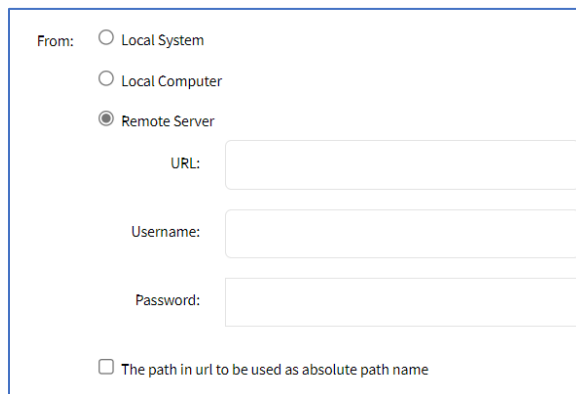
1. Go to *System :: Toolkit*.
2. Click **Apply Settings** icon (displays dialog).
3. In *From* menu, select one:

Local System radio button. Enter **File Name**.

Local Computer radio button. Click **Choose File** (locate and select the file).



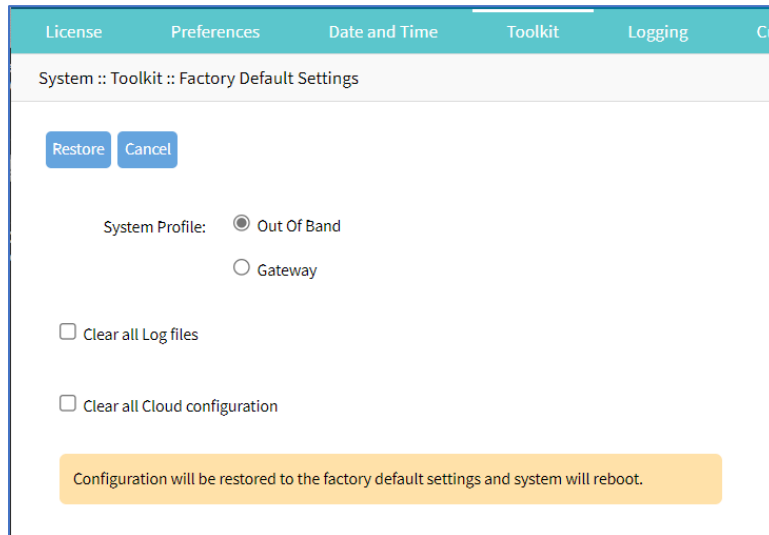
Remote Server radio button. Enter **URL**, **Username**, and **Password**. (as needed) Select **Download path is absolute path name** checkbox.



4. Click **Apply**.

Restore to Factory Default Settings tool

The Nodegrid solution offers multiple options to reset the unit back to factory default settings. Displays this dialog. The *System Profile* menu is available on: Link SR, Bold SR, Gate SR, and Hive SR.



During this action, all configuration files are set to factory default. There is an option to save or clear all log files.

NOTE: 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.

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.

WebUI Procedure

1. Go to *System :: Toolkit*.
2. Click **Restore to Factory Default Settings** icon (displays dialog).
3. In the *System Profile* menu, select one: (for more information, see [System Profile](#)).

Out of Band radio button.

Gateway radio button.

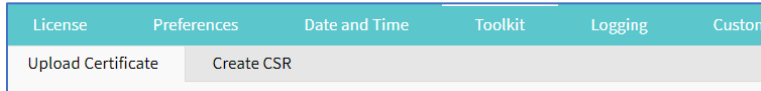
(optional) Select **Clear all Log files** checkbox.

(optional) Select **Clear all Cloud Configuration** checkbox

4. Click **Restore**.

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**.



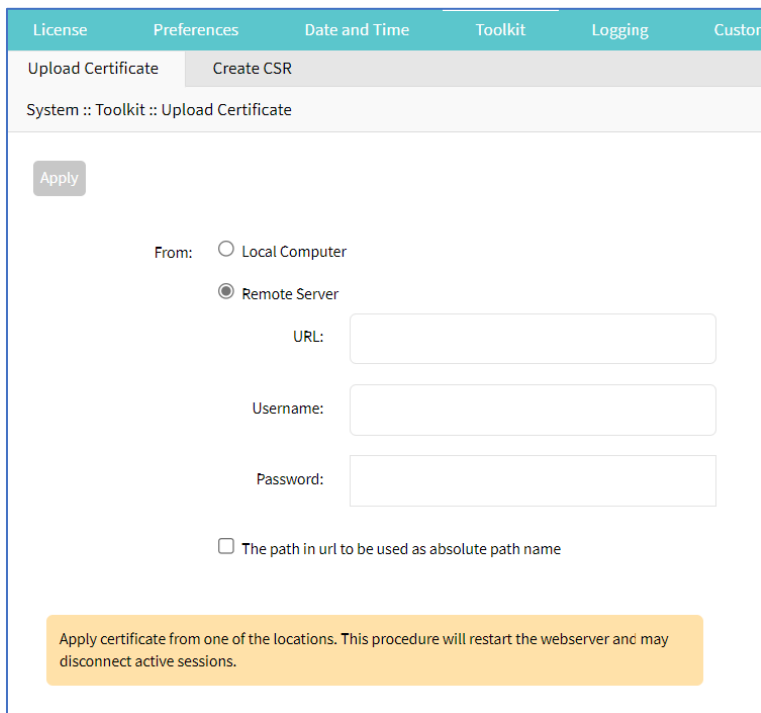
WARNING! When the certificate is applied, the web server is restarted and active sessions are disconnected.

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

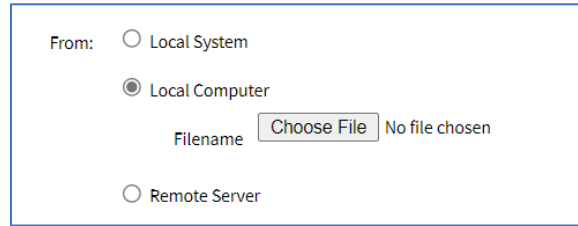
Upload Certificate

WebUI Procedure

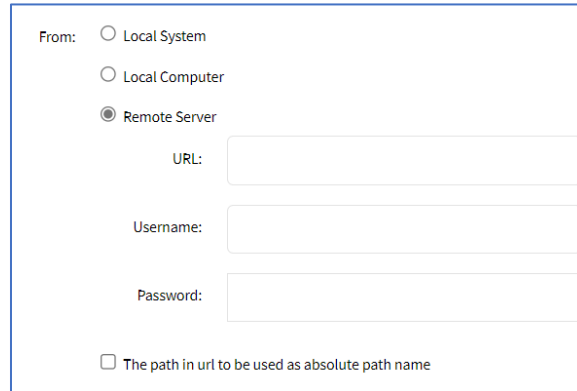
1. Go to *System :: Toolkit*.
2. Click **System Certificate** icon (displays dialog).



3. On the **Upload Certificate** sub-tab, *From* menu, select one.
 - Local System** radio button. Enter **File Name**.
 - Local Computer** radio button. Click **Choose File** (locate and select the file).



Remote Server radio button. Enter **URL**, **Username**, **Password**, and **Passphrase** (if certificate requires). Select **Download path is absolute path name** checkbox.



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

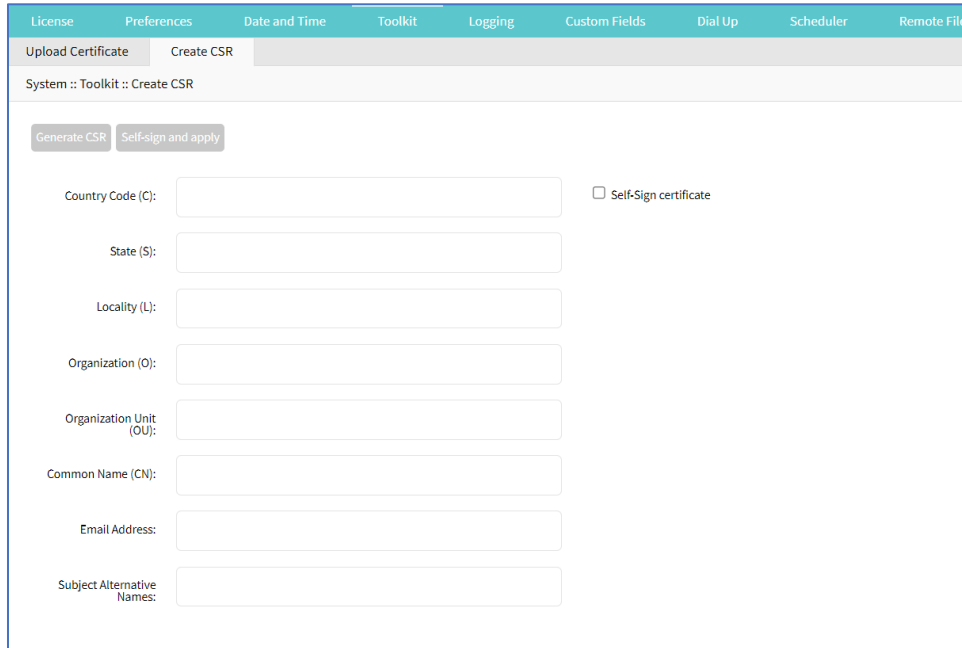
4. Click **Apply**.

Create a Self-Sign Certificate

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

WebUI Procedure

1. Go to *System :: Toolkit*.
2. Click **System Certificate** icon (displays dialog).
3. On the **Create CSR** sub-tab:



Enter **Country Code (C)**.

Enter **State (S)** .

Enter **Locality (L)** .

Enter **Organization (O)** .

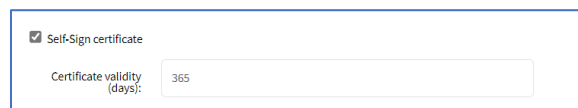
Enter **Organization Unit (OU)** .

Enter **Common Name (CN)** .

Enter **Email Address**.

(optional) **Subject Alternative Names**.

4. Select **Self-Sign certificate** checkbox and enter **Certificate validity (days)** value.

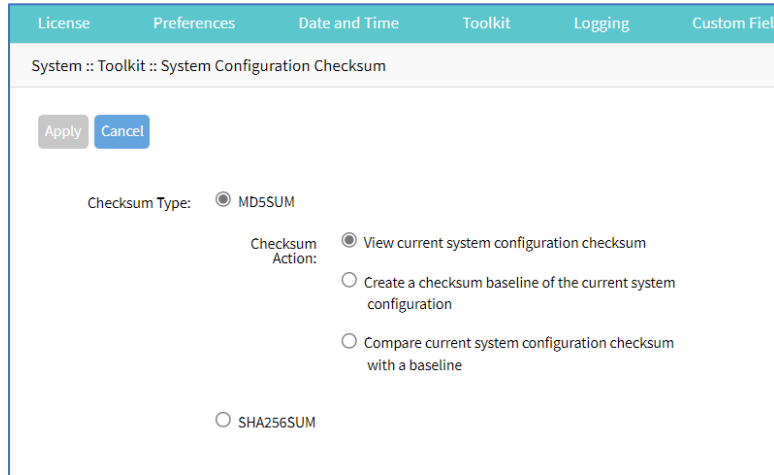


5. Click **Self-sign and apply**.

6. 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. Displays this dialog.



WebUI Procedure

1. Go to *System :: Toolkit*.
2. Click **System Configuration Checksum** icon (displays dialog).
3. In *Checksum Type* menu, select one:

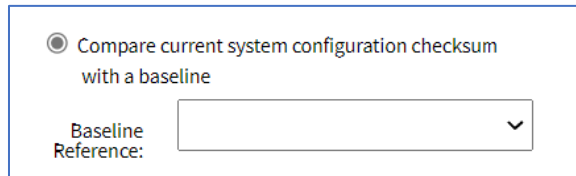
MD5SUM radio button

In *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.



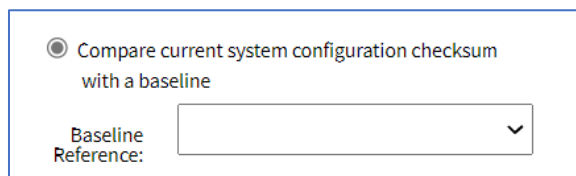
SHA256SUM radio button

In *Checksum Action* menu, select one:

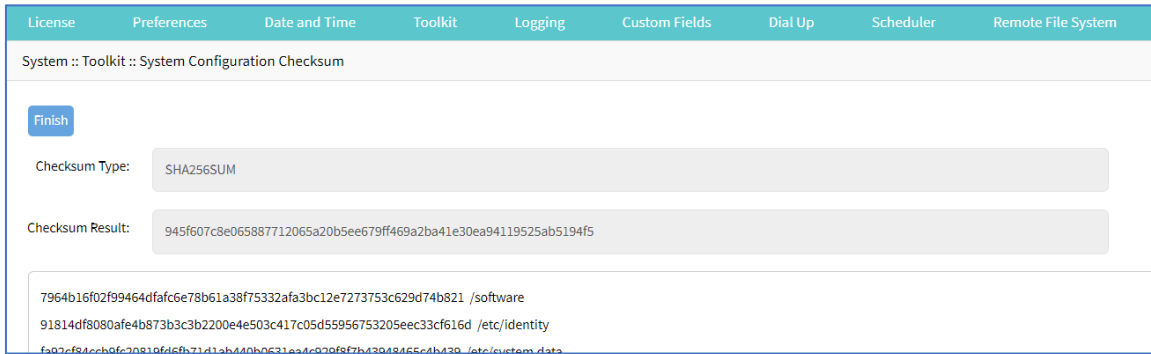
View current system configuration checksum radio button.

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.



4. Click **Apply** (display results).

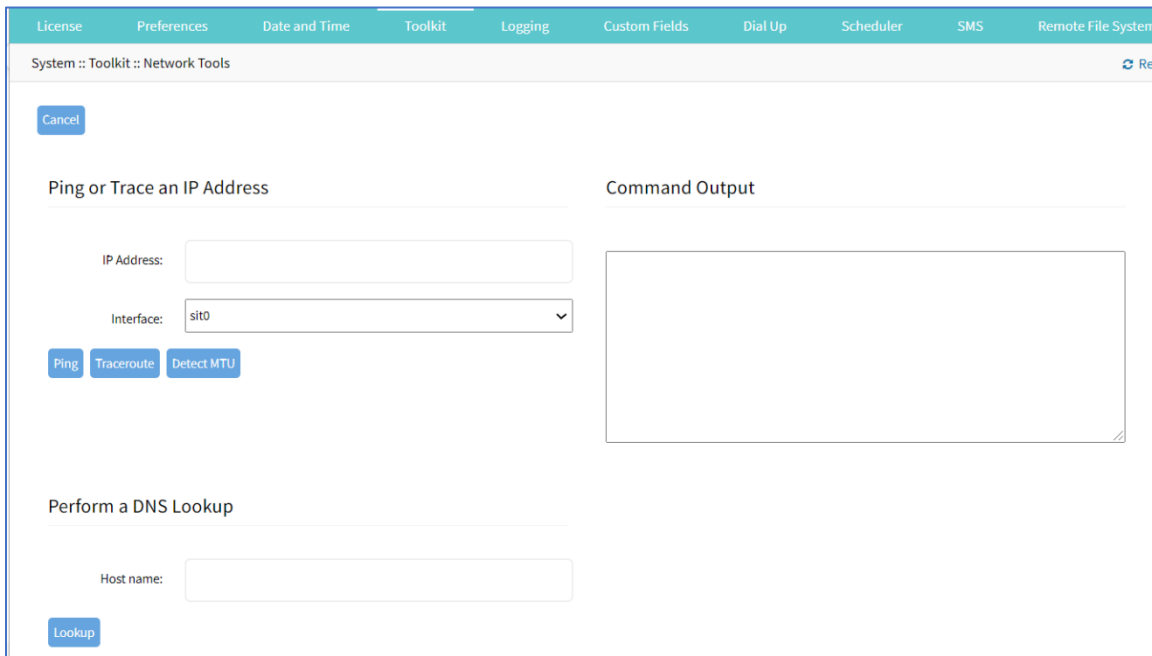


5. Review the results. If the configurations match, the main result is "Passed". If any change, altered locations are identified.

6. 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.

WebUI Procedure

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**.

On **Interface** drop-down, select one (**eth0**, **eth1**, **backplane0**, **backplane1**, **docker0**, **sit0**, **tap0**, **tap1**, **Source IP Address**).

Click **Ping**.

4. 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.

WebUI Procedure

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**.

On **Interface** drop-down, select one (**eth0**, **eth1**, **backplane0**, **backplane1**, **docker0**, **sit0**, **tap0**, **tap1**, **Source IP Address**).

Click **Traceroute**.

4. 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.

WebUI Procedure

1. Go to *System :: Toolkit*.
2. Click **Network Tools** icon (displays dialog).
3. In the *Perform a DNS Lookup* menu:

Enter **Host name**.

Click **Lookup**.

4. Review results in *Command Output* panel.

Detect MTU

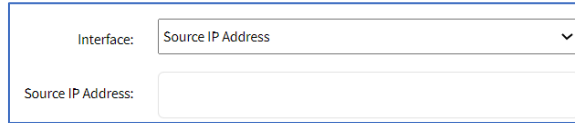
WebUI Procedure

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**.

On **Interface** drop-down, select one (**eth0**, **eth1**, **backplane0**, **backplane1**, **docker0**, **sit0**, **tap0**, **tap1**, **Source IP Address** – enter **Source IP Address**).



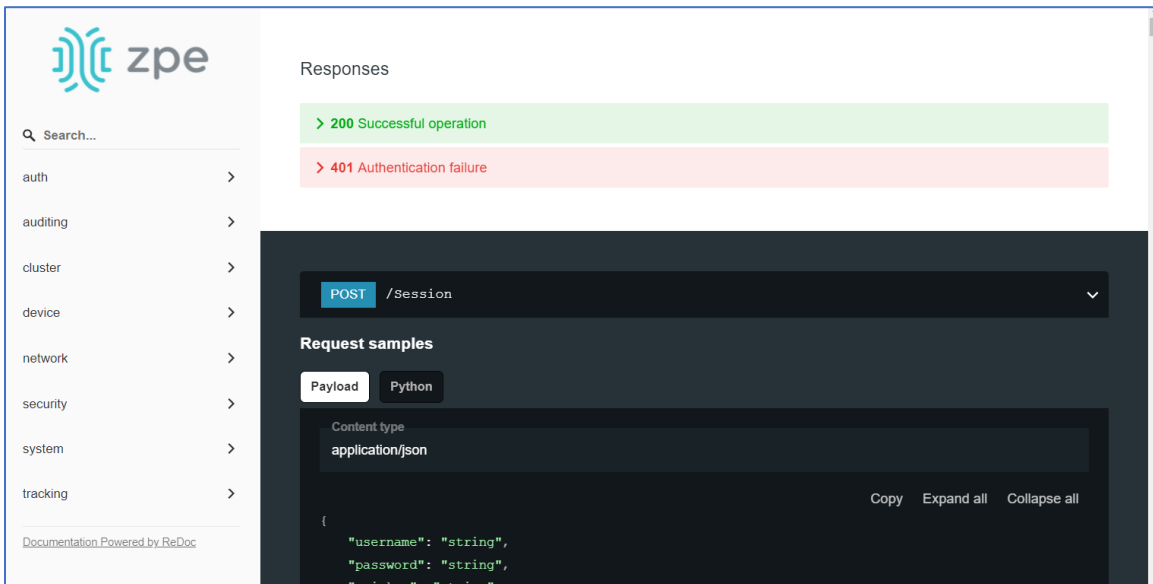
Click **Detect MTU**.

4. 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.



WebUI Procedure

1. Go to *System :: Toolkit*.
2. Click on the **API** icon.

Alternatively, on Banner, **User Name** drop-down (top right), click **API Documentation**.

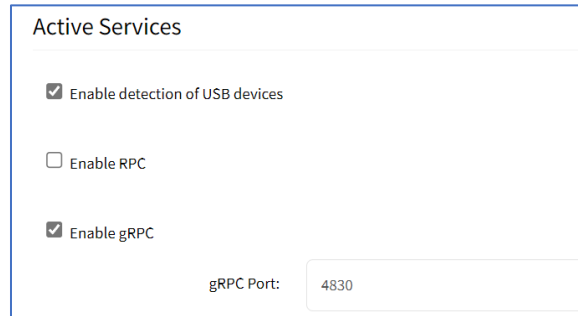
3. On the left panel, click the > arrow to display API calls for that function. Request and Response examples are included.

Example: "get auditing email destination configuration"

gRPC

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

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



2. In *Active Services* menu:

Select **Enable gRPC** checkbox.

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.

CLI Examples

`post_request (Authentication - returns a session ticket)`


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

get_request (get network connection details)

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

post_request (add a phone number to the sms whitelist)

```
post_request({path: '/v1/system/sms/whitelist', ticket: 'xxxxxxxxxxxxx', data '{"name": "phone1", "phone_number": "+11111111111"}' }, [...])
```

put_request (update an existing value on the sms whitelist)

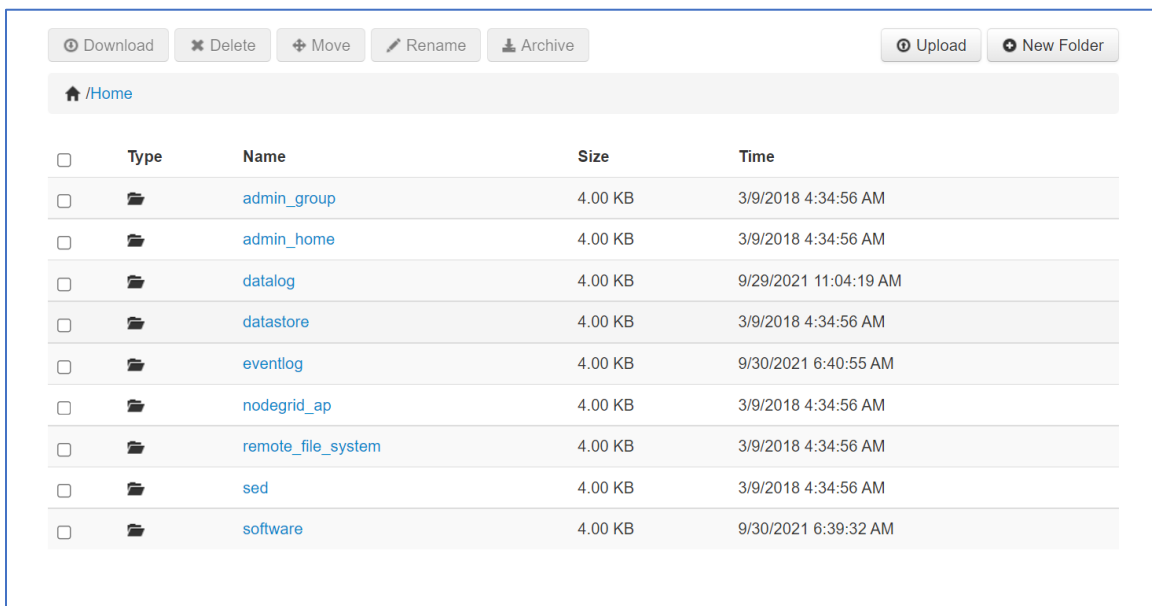
```
put_request({path: '/v1/system/sms/whitelist/phone1', ticket: 'xxxxxxxxxxxxx', data '{"phone_number": "+12222222222"}' }, [...])
```

delete_request (delete an existing value on the sms whitelist)

```
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.



The screenshot shows a file manager interface with a toolbar at the top containing buttons for Download, Delete, Move, Rename, Archive, Upload, and New Folder. Below the toolbar is a breadcrumb path: /Home. The main area displays a table of files and folders.

<input type="checkbox"/>	Type	Name	Size	Time
<input type="checkbox"/>	Folder	admin_group	4.00 KB	3/9/2018 4:34:56 AM
<input type="checkbox"/>	Folder	admin_home	4.00 KB	3/9/2018 4:34:56 AM
<input type="checkbox"/>	Folder	datalog	4.00 KB	9/29/2021 11:04:19 AM
<input type="checkbox"/>	Folder	datastore	4.00 KB	3/9/2018 4:34:56 AM
<input type="checkbox"/>	Folder	eventlog	4.00 KB	9/30/2021 6:40:55 AM
<input type="checkbox"/>	Folder	nodegrid_ap	4.00 KB	3/9/2018 4:34:56 AM
<input type="checkbox"/>	Folder	remote_file_system	4.00 KB	3/9/2018 4:34:56 AM
<input type="checkbox"/>	Folder	sed	4.00 KB	3/9/2018 4:34:56 AM
<input type="checkbox"/>	Folder	software	4.00 KB	9/30/2021 6:39:32 AM

Download File

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

WebUI Procedure

1. Go to *System :: Toolkit*.
2. Click **File Manager** icon (opens a new browser tab).
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.

Delete File or Folder

This deletes the selected files/folders.

WebUI Procedure

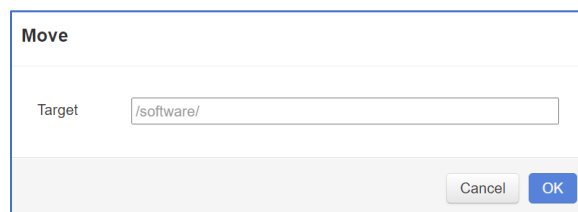
1. Go to *System :: Toolkit*.
2. Click **File Manager** icon (opens a new browser tab).
3. Go to the location.
4. Select checkbox(es).
5. Click **Delete**.

Move File or Folder

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

WebUI Procedure

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

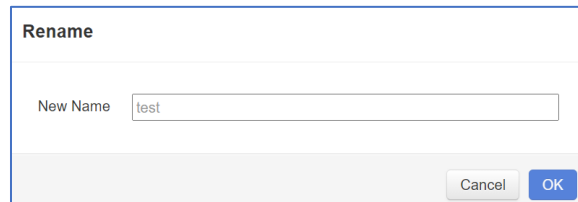


7. Click **OK**.

Rename File or Folder

WebUI Procedure

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



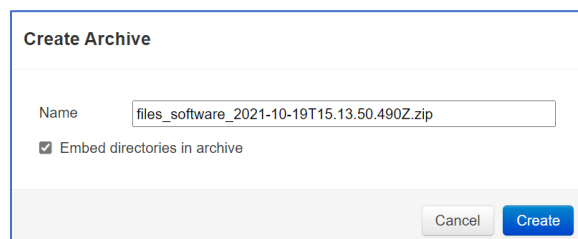
7. Click **OK**.

Archive File or Folder

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

WebUI Procedure

1. Go to *System :: Toolkit*.
2. Click **File Manager** icon (opens a new browser tab).
3. Go to the location.
4. Select checkbox(es).
5. Click **Archive**.
6. On the *Create Archive* pop-up dialog, confirm the Name (modify as needed). Select **Embed directories in archive** checkbox. Click **Create**.



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

🏠 /Home/software				
<input type="checkbox"/>	Type	Name	Size	Time
<input type="checkbox"/>	📄	files_software_2021-10-19T15.17.08.413Z.zip	22 B	10/19/2021 8:17:10 AM
<input type="checkbox"/>	📁	software	4.00 KB	10/19/2021 8:04:11 AM
<input type="checkbox"/>	📁	test	4.00 KB	10/19/2021 8:03:52 AM

Create New Folder

Cannot be done in Home location.

WebUI Procedure

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**.

New Folder

Complete Path /software/software/test/test112/

Folder Name

The new folder is added in that location.

Upload File

WebUI Procedure

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. Click **OK**.

Upload File

Upload to /software/

No file chosen

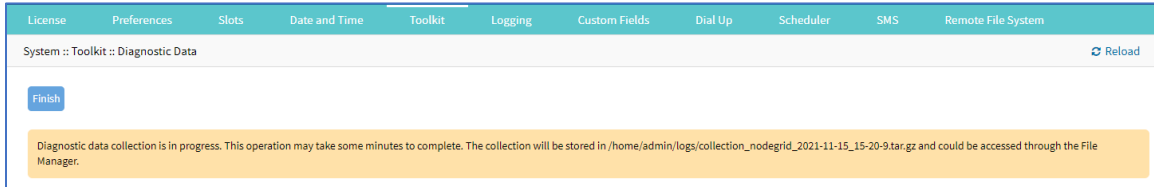
The file will upload and become available.

Diagnostic Data tool

This tool creates a report on the system status of the Nodegrid device. The contents help investigate the device functionality. A series of commands output the state of the system, collect various log files, and copies 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:

`/home/admin/logs/collection_nodegrid_XXXX-XX-XX_XX-XX-X.tar.gz`



Step 1 – Initiate Diagnostic Data

This runs the Diagnostic Data tool. The results are accessed with **File Manager**.

WebUI Procedure

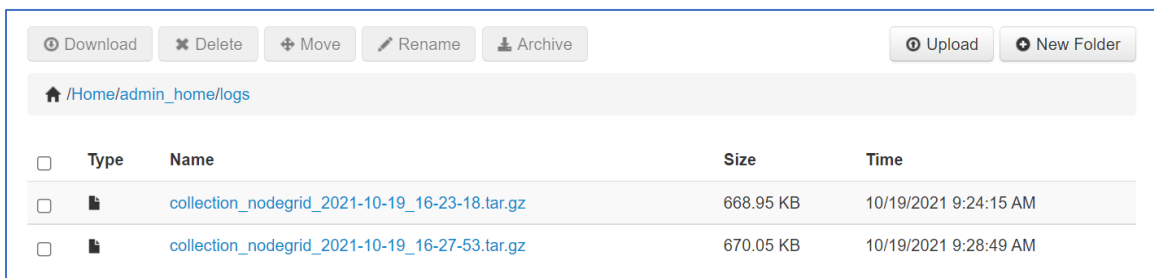
1. Go to *Systems :: Toolkit*.
2. Click **Diagnostic Data** icon.
3. The tool will run the diagnostics.
4. When done, click **Finish** (returns to the *Toolkit* page).

Step 2 – Access the Diagnostic Data Results

(Admin privileges required.)

WebUI Procedure

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

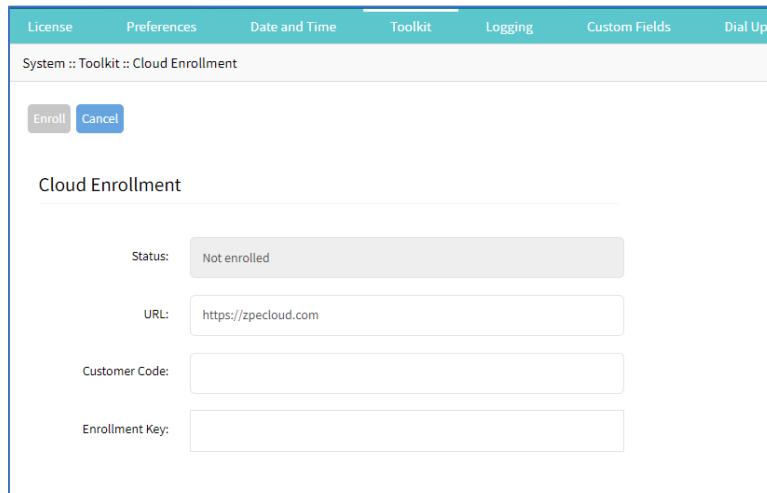


4. Locate the tarball and select checkbox.
5. Click **Download**.

Review the file, as needed.

Cloud Enrollment tool

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



Enable Cloud Enrollment

WebUI Procedure

1. Go to *System :: Toolkit*.
2. Click **Cloud Enrollment** icon.
3. In the *Cloud Enrollment* menu:
 - Enter **URL** of the Cloud application.
 - Enter **Customer Code**.
 - 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.

```
[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
```

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

To show ZPE Cloud enrollment settings:

```
[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]#
```

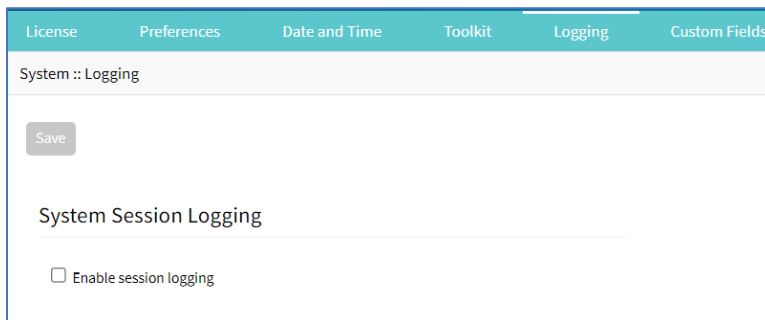
3. A confirmation is sent when the enrollment succeeds.

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.

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).

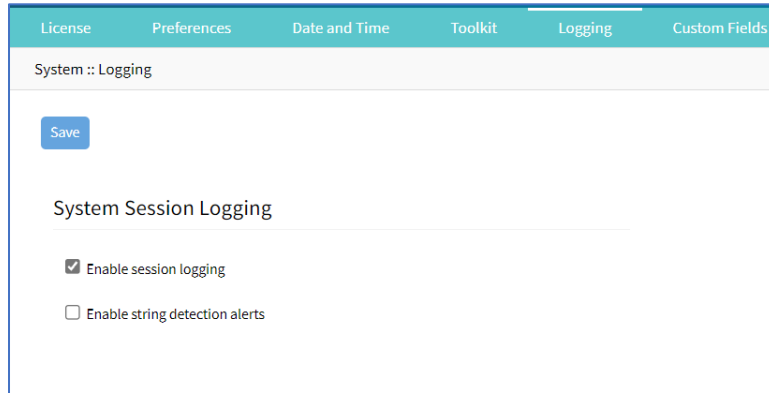


Enable Session Logging

Details can be modified, as needed.

WebUI Procedure

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



License Preferences Date and Time Toolkit Logging Custom Fields

System :: Logging

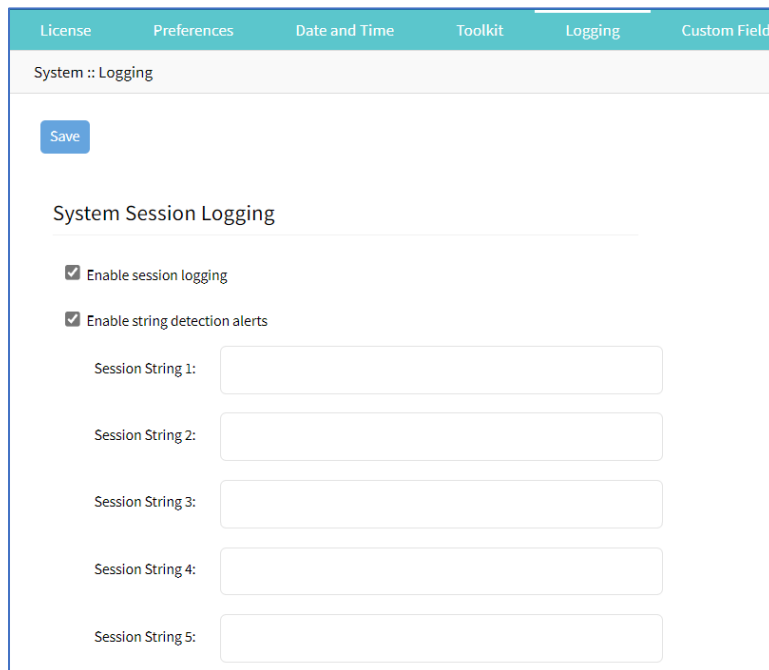
Save

System Session Logging

Enable session logging

Enable string detection alerts

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



License Preferences Date and Time Toolkit Logging Custom Fields

System :: Logging

Save

System Session Logging

Enable session logging

Enable string detection alerts

Session String 1:

Session String 2:

Session String 3:

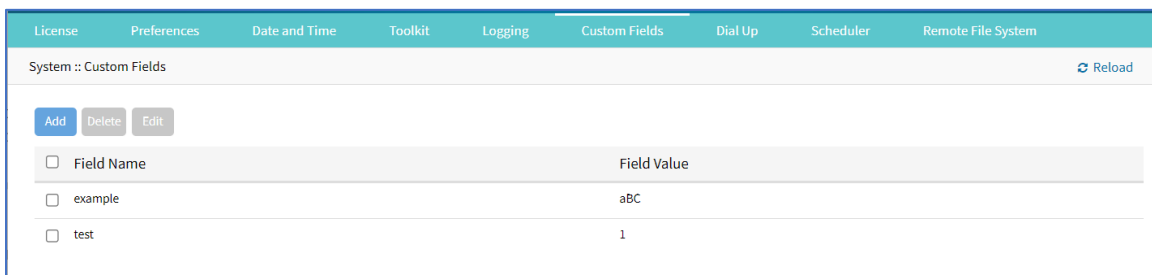
Session String 4:

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.



License Preferences Date and Time Toolkit Logging Custom Fields Dial Up Scheduler Remote File System

System :: Custom Fields Reload

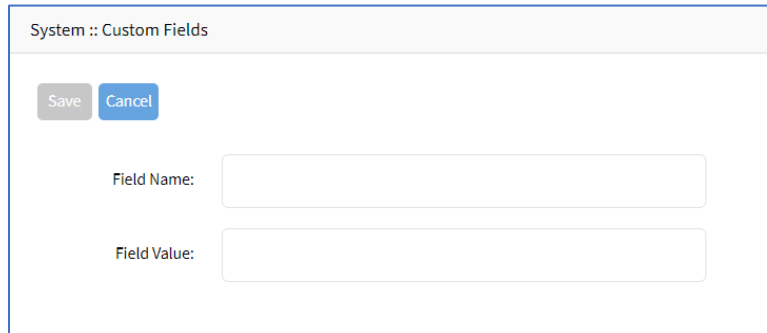
Add Delete Edit

Field Name	Field Value
<input type="checkbox"/> example	aBC
<input type="checkbox"/> test	1

Add Custom Field

WebUI Procedure

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



3. Enter **Field Name**.
4. Enter **Field Value**.
5. Click **Save**.

Edit Custom Field

WebUI Procedure

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

Delete Custom Field

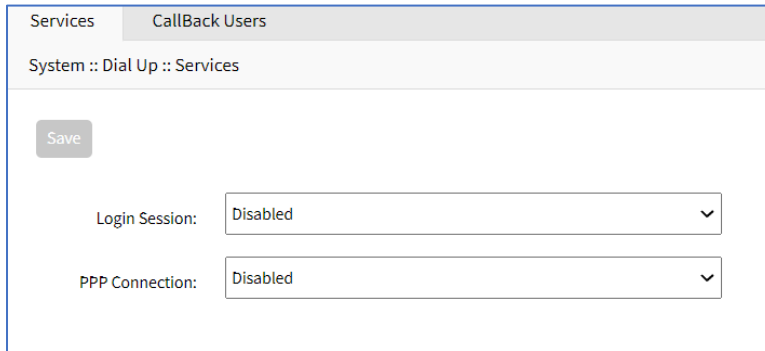
WebUI Procedure

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

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

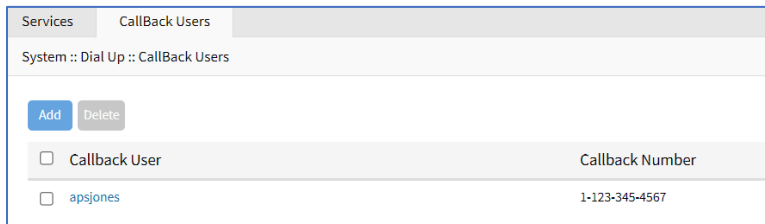


Manage Dial Up Services

WebUI Procedure

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

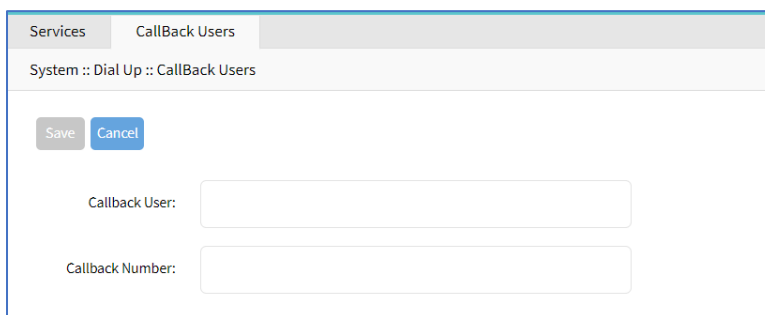


Callback User	Callback Number
<input type="checkbox"/> apsjones	1-123-345-4567

Add Callback User

WebUI Procedure

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



3. Enter **Callback User**.

4. Enter **Callback Number**.
5. Click **Save**.

Delete Callback User

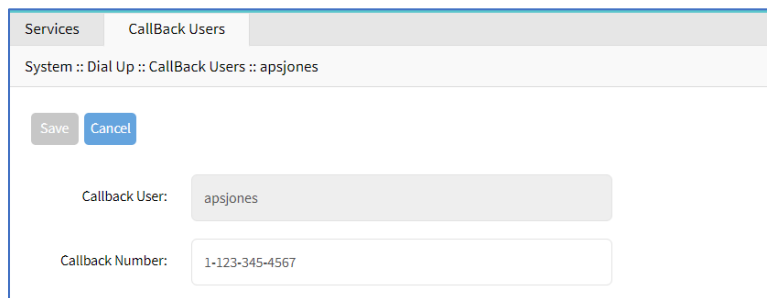
WebUI Procedure

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

Edit Callback User

WebUI Procedure

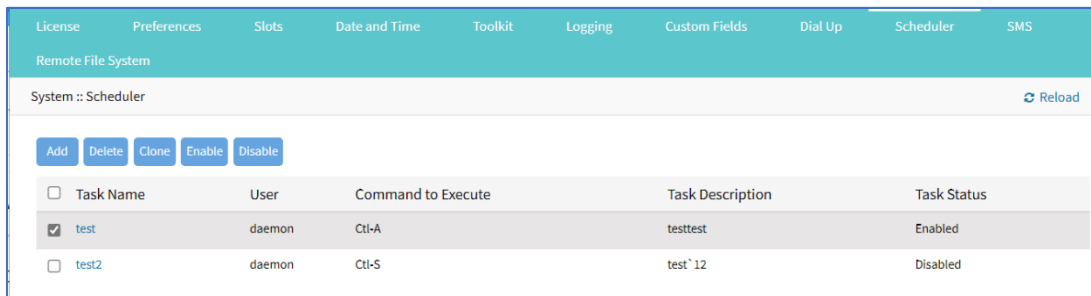
1. Go to *System :: Dial Up :: Callback Users*.
2. In *Callback User* column, click name.



3. On the dialog, make changes.
4. Click **Save**.

Scheduler 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.



<input type="checkbox"/>	Task Name	User	Command to Execute	Task Description	Task Status
<input checked="" type="checkbox"/>	test	daemon	Ctl-A	testtest	Enabled
<input type="checkbox"/>	test2	daemon	Ctl-S	test` 12	Disabled

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

Scheduler Date/Time examples

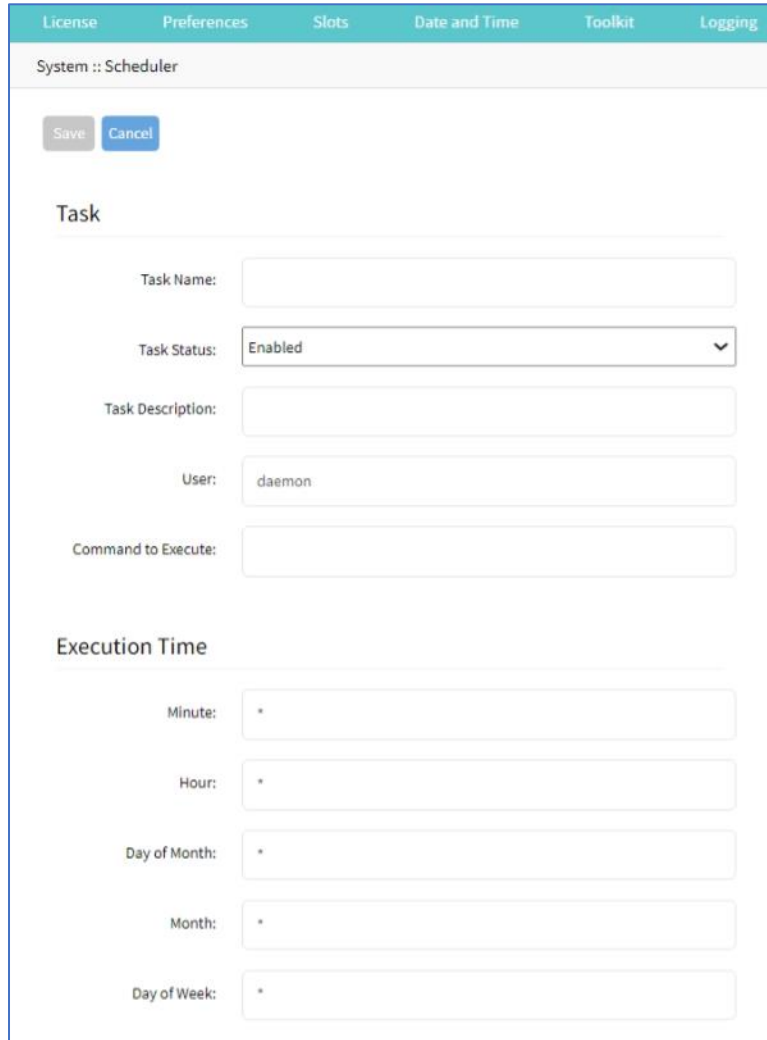
Factor	Daily Task 00:01 hours	Every Saturday: 23:45 hours	Every Hour on the Hour
Minute	1	45	0
Hour	0	23	*
Day of Month	*	*	*
Month	*	*	*
Day of Week	*	6	*

Manage Tasks

Add a Task

WebUI Procedure

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



3. In the *Task* menu:

Enter **Task Name**.

On **Task Status** drop-down, select one (**Enabled, Disabled**).

(optional) Enter **Task Description**.

For **User**, accept default.

Enter **Command to Execute** (Shell command to execute).

4. In the *Execution Time* menu, modify fields as needed.

Minute (*, numbers [0-59], ',' separated, '-' separated, '/' separated)

Hour (*, numbers [0-23], ',' separated, '-' separated, '/' separated)

Day of month (*, numbers [1-31], ',' separated, '-' separated, '/' separated)

Month (*, numbers [Jan=1, Feb=2, ..., Dec=12], ',' separated, '-' separated, '/' separated)

Day of Week (*, numbers, ',', '-', '/', ' ', '-', '/'.(Sun=0, Mon=1, ..., Sat=6))

5. Click **Save**.

Edit a Task

WebUI Procedure

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

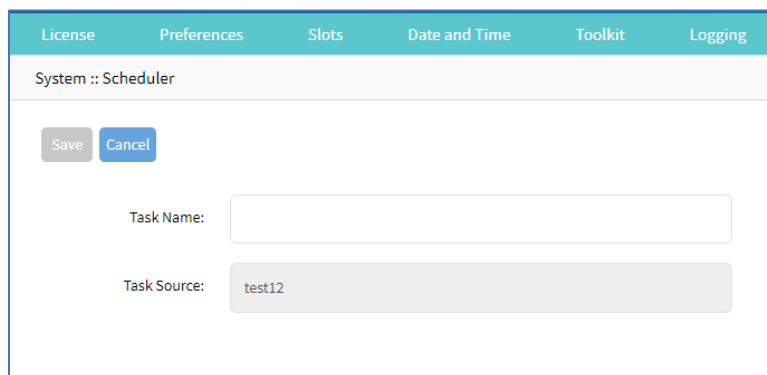
WebUI Procedure

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

Clone a Task

WebUI Procedure

1. Go to *System :: Scheduler*.
2. In the *Task Name* column, click on the name (displays dialog).
3. Select checkbox next to a task.
4. Click **Clone** (displays dialog).



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

Enable/Disable a Task

WebUI Procedure

1. Go to *System :: Scheduler*.
2. In the *Task Name* column, click on the name (displays dialog).
3. Select checkbox next to a task.
4. Click **Enable** (to enable task).
5. Click **Disable** (to disable task).

SMS tab (only with installed cellular module)

NOTE: This function is only available on devices on devices with the cellular module installed: Services Router, Bold SR, Gate SR, Link SR, and Hive SR (loaded with M2-Card EM7565 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. MAC address of ETH0 is the default password.

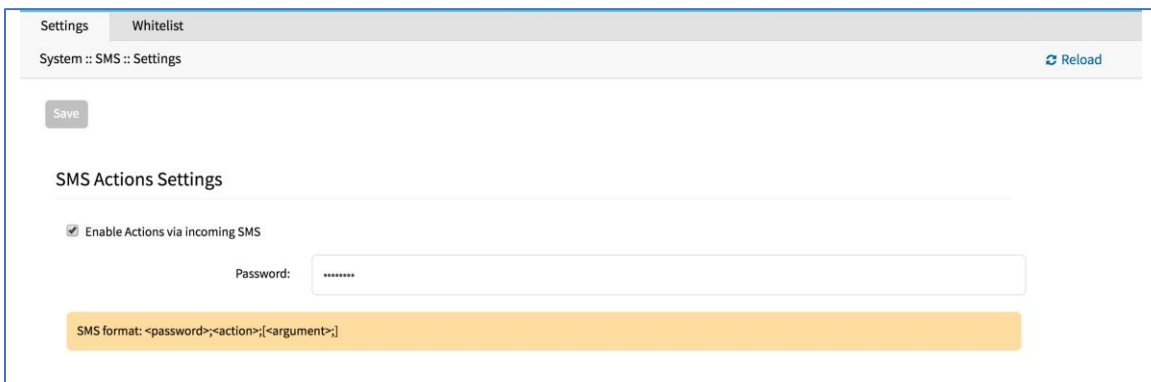
NOTE: The SMS option requires that the SIM card and plan to be SMS-enabled. This can be checked with the service provider. It is recommended to check the costs for this service, as some actions can respond with multiple SMS.

Settings sub-tab

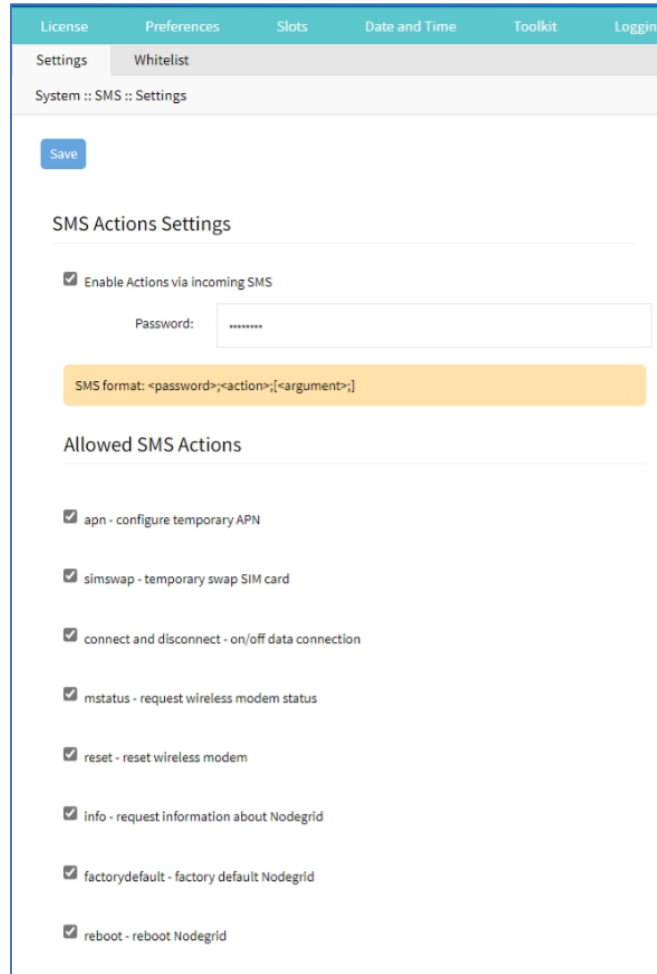
Enable Incoming SMS Actions

WebUI Procedure

1. Go to *System :: SMS :: Settings*.



2. In *SMS Actions Settings* menu, select **Enable Actions via Incoming SMS** checkbox (displays dialog).



3. Enter **Password**.
4. 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).
5. 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)

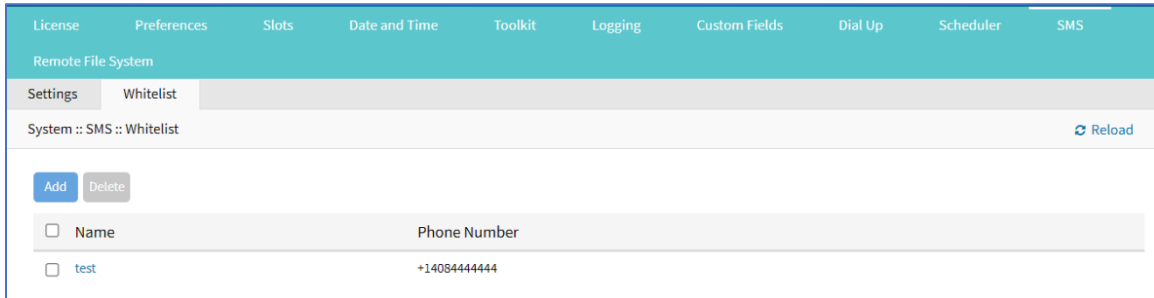
```
< password >;factorydefault;  
Nodegrid will restore configuration to factory default and reboot;
```

reboot (reboot Nodegrid device)

```
< 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.

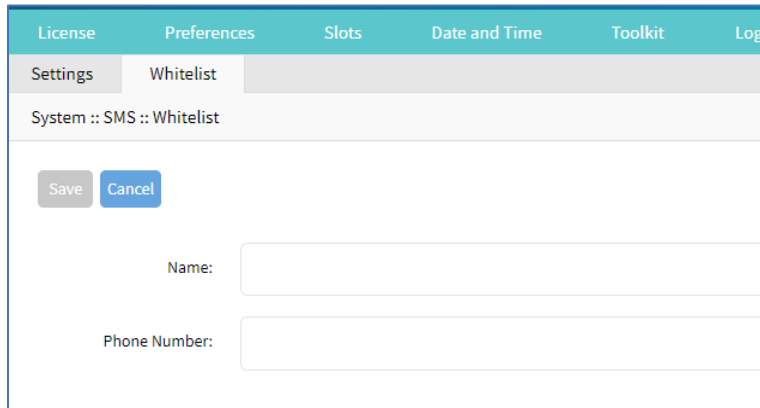


NOTE: If the whitelist table is empty, requests from all phone numbers are accepted.

Add Entry to Whitelist

WebUI Procedure

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



3. Enter **Name**.
4. Enter **Phone Number**.
5. Click **Save**.

Remote File System tab

This designates remote file system folders.

System :: Remote File System							
Mount Point	File System Type	Remote Server	Remote Directory	Include in the File Manager	Status	Error	
<input type="checkbox"/> 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

WebUI Procedure

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

System :: Remote File System	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	
Mount Point:	<input type="text"/>
File System Type:	NFS <input type="button" value="v"/>
Remote Server:	<input type="text"/>
Remote Directory:	<input type="text"/>
<input type="checkbox"/> Mount On-demand	
<input type="checkbox"/> Include in the File Manager	

3. Enter **Mount Point**.
4. On **File System Type** drop-down, select one **NFS**

File System Type:	NFS <input type="button" value="v"/>
Remote Server:	<input type="text"/>
Remote Directory:	<input type="text"/>

Enter **Remote Server**.

Enter **Remote Directory**

Windows Sharing

File System Type:	Windows Sharing
Remote Server:	
Remote Directory:	
Username:	
Password:	*****
Confirm Password:	*****

Enter **Remote Server**.

Enter **Remote Directory**.

Enter **Username**.

Enter **Password** and **Confirm Password**.

SSHFS

File System Type:	SSHFS
Remote Server:	
Remote Directory:	
Username:	
Authentication Method:	<input checked="" type="radio"/> Password
	Password: *****
	Confirm Password: *****
	<input type="radio"/> SSH Key

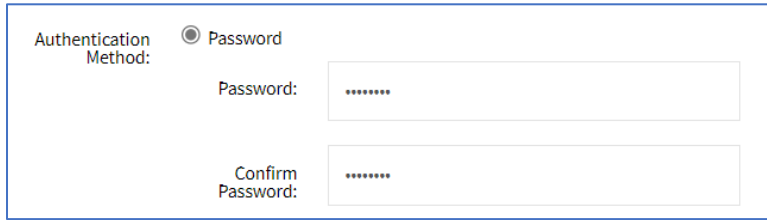
Enter **Remote Server**.

Enter **Remote Directory**.

Enter **Username**.

On *Authentication Method* menu, select one:

Password radio button. Enter **Password** and **Confirm Password**.

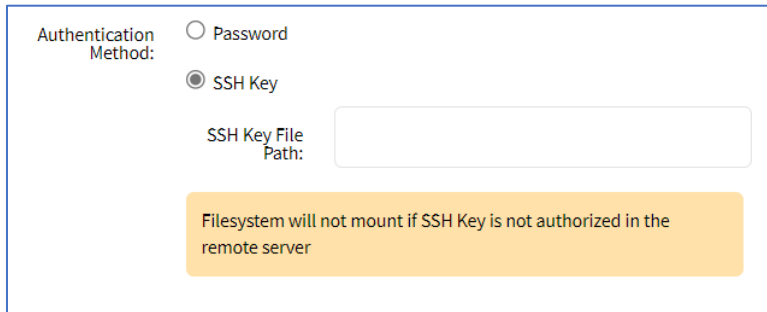


Authentication Method: Password

Password:

Confirm Password:

SSH Key radio button. Enter **SSH Key File Path**.



Authentication Method: Password

SSH Key

SSH Key File Path:

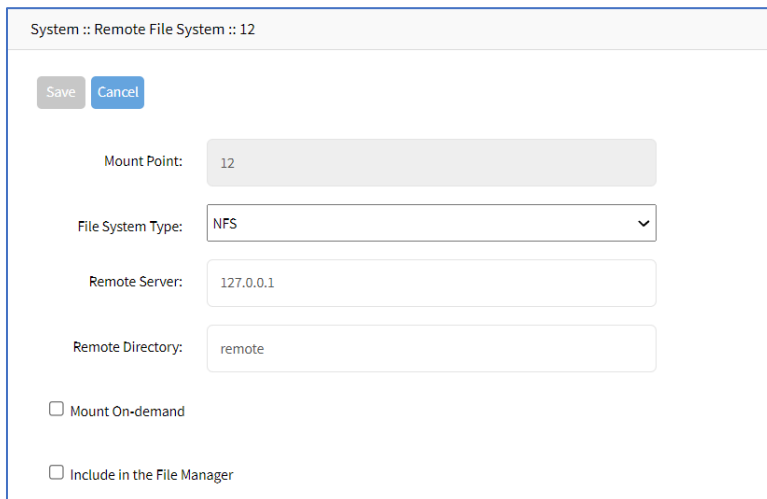
Filesystem will not mount if SSH Key is not authorized in the remote server

5. (optional) Select **Mount On-demand** checkbox.
6. (optional) Select **Include in the File Manager** checkbox.
7. Click **Save**.

Edit Remote File System

WebUI Procedure

1. Go to *System :: Remote File System*.
2. Click on the name in the *Mount Point* column (displays dialog)



System :: Remote File System :: 12

Mount Point:

File System Type:

Remote Server:

Remote Directory:

Mount On-demand

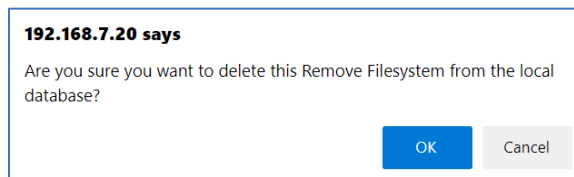
Include in the File Manager

3. Make changes.
4. Click **Save**.

Delete Remote File System

WebUI Procedure

1. Go to *System :: Remote File System*.
2. Select checkbox next to name.
3. Click **Delete** (displays confirmation dialog).



4. Click **OK**.

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.

License
Preferences
Date and Time
Toolkit
Logging
Custom Fields
Dial Up
Scheduler
SMS

I/O Ports
Remote File System

System :: I/O Ports ▶ Start ▼ Confirm ↺ Revert ↻ Reload

Save

Digital Output OUT0

Description:

State:

Alarm Relay

Description:

State: Open
 Close
 Power Source Control

Dry Contact DIO0

Description:

Direction: Input
 Output

State:

Dry Contact DIO1

Description:

Direction: Input
 Output

State:

Configure I/O Port Settings

1. In *Digital Output OUT0* menu:
 Enter **Description**.
 On **State** drop-down, select one (**Low**, **High**):
2. In *Alarm Relay* menu:
 Enter **Description**.

On *State*, select one:

Open radio button

Close radio button

Power Source Control radio button

3. In *Dry Contact DIO0* menu:

Enter **Description**.

On *Direction*, select one:

Input radio button

Output radio button

On **State** drop-down, select one (**Low, High**)

4. In *Dry Contact DIO1* menu:

Enter **Description**.

On *Direction*, select one:

Input radio button

Output radio button

On **State** drop-down, select one (**Low, High**)

5. Click **Save**.

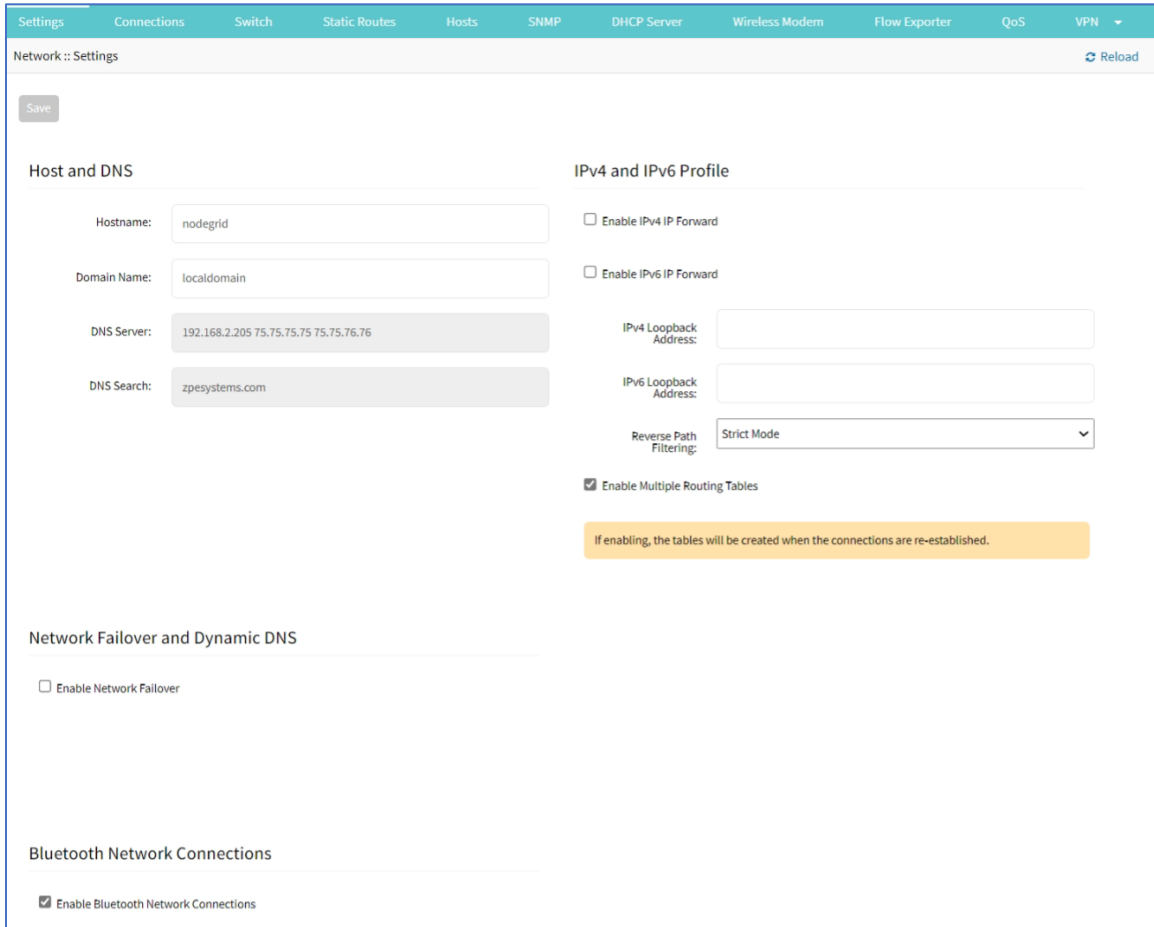
Network Section

Administrators can configure and adjust all network-related settings, including network configuration, LTE, WIFI interfaces, bonding, 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, including failover.



Manage Settings

Configure Settings

WebUI Procedure

1. Go to *Network :: Settings*.
2. In the *Host & DNS* menu:
 - Enter **Hostname**.
 - Enter **Domain Name**.
 - (**DNS Server** and **DNS Search** are read-only.)
3. In *IPv4 and IPv6 Profile* menu (select one or both IP Forwards to route network traffic between network interfaces):

IPv4 and IPv6 Profile

Enable IPv4 IP Forward

Enable IPv6 IP Forward

IPv4 Loopback Address:

IPv6 Loopback Address:

Reverse Path Filtering:

Enable Multiple Routing Tables

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

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

Select **Enable IPv4 IP Forward** checkbox

Select **Enable IPv6 IP Forward** checkbox

Enter **IPv4 Loopback Address** (address is assigned a bitmask of /32)

Enter **IPv6 Loopback Address** (address is assigned a bitmask of /128)

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 route table. If the packet cannot be routed, it gets dropped. This allows for asymmetric routing scenarios.)

NOTE: With Reverse Path Filtering, administrators can configure device behavior. By default, this is set to Strict Mode (recommended for most environments with protection against some forms of DDoS attacks). This value may need to change because of dynamic routing protocols or other network setup scenarios.

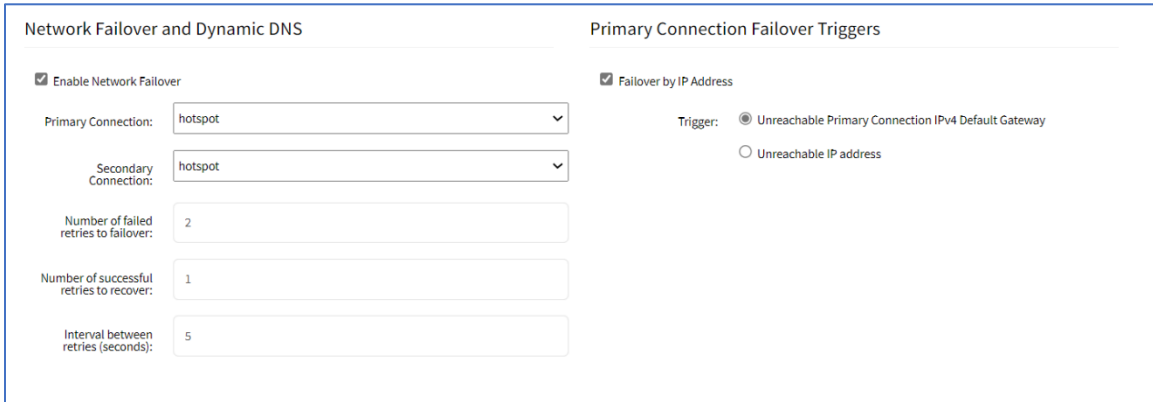
Select **Enable Multiple Routing Tables** checkbox (if selected, tables are created when connections re-established).

4. In *Network Failover and Dynamic DNS* menu:

The network failover option allows administrators to automatically failover between two and three different network interfaces.

Select **Enable Network Failover** checkbox (displays expanded dialog).

NOTE: If SD-WAN is enabled, the **Enable Network Failure** checkbox is disabled.



On **Primary Connection** drop-down, select one (**BACKPLANE0, BACKPLANE1, ETH0, ETH1, hotspot**).

On **Secondary Connection** drop-down, select one (**BACKPLANE0, BACKPLANE1, ETH0, ETH1, hotspot**).

Enter **Number of failed retries to failover** (default: 2).

Enter **Number of successful retries to recover** (default: 1)

Enter **Interval between retries (seconds)** (default: 5)

In *Primary Connection Failover Triggers* menu (the selection depends on type of Nodegrid device):

Select **Failover by IP Address** checkbox.



In *Trigger* menu, select one:

Unreachable Primary Connection IPv4 Default Gateway radio button

Unreachable IP address radio button - enter **Address**.

In *Dynamic DNS* menu, select **Enable Dynamic DNS** checkbox (displays dialog).

Dynamic DNS

Enable Dynamic DNS

DDNS server name:

DDNS server TCP port:

ZONE:

Failover Hostname (FQDN):

Key Information for dnssec:

Username:

Algorithm:

Key Size:

Enter **DDNS server name**.

Enter **DDNS server TCP port** (default: 53).

Enter **ZONE**.

Enter **Failover Hostname (FQDN)**.

Enter **Username**.

On **Algorithm** drop-down, select one (**HMAC-MD5, HMAC-SHA1, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512**).

Enter **Key Size** (default: 512).

(Following displays only when wireless connections are available.)

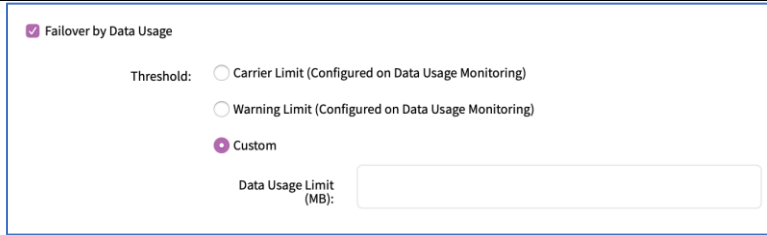
Select **Failover by Signal Strength** checkbox (triggered when signal strength drops below a user-defined percentage).

Failover by Signal Strength

Signal Strength (%):

Enter **Signal Strength (%)** value.

Select **Failover by Data Usage** checkbox (triggered when one of these limits are met):



In *Threshold* menu, select one:

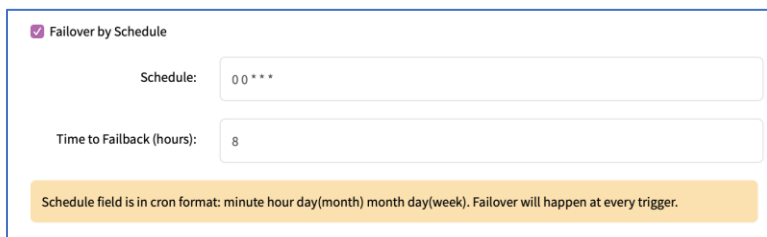
Carrier Limit (Configured on Data Usage Monitoring) radio button

Warning Limit (Configured on Data Usage Monitoring) radio button

Custom radio button – enter **Data Usage Limit (MB)** value.

NOTE: 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> for details on how to configure Carrier and Warning limits.

Select **Failover by Schedule** checkbox (triggers on a set schedule).



Enter **Schedule** value

(# # # # #, separated by word space) Sequence: *minute* (0-59), *hour* (0-23), *day of month* (0-30), *month* (0-11), *day of week* (0-6)

Enter **Time to Failback (hours)** value.

5. In *Blue Tooth Network Connections* (applies only if Bluetooth is enabled):

Select **Enable Bluetooth Network Connections** checkbox.

6. Click **Save**.

Connections tab

Administrators can edit, add, and delete existing network configurations. All existing physical interfaces are automatically added.

Network :: Connections									
Name	Status	Type	Interface	Carrier State	IPv4 Address	IPv6 Address	MAC Address	Description	
<input type="checkbox"/> BACKPLANE0	Not Active	Ethernet	backplane0	Up			00:90:fb:63:40:62		
<input type="checkbox"/> ETH0	Connected	Ethernet	eth0	Up	192.168.7.25/24	fe80::290:fbff:fe63:4063/64	00:90:fb:63:40:63		
<input type="checkbox"/> hotspot	Not Active	WiFi		Down					

Manage Network Connections

Edit Network Connection

WebUI Procedure

1. Go to *Network :: Connections*.
1. In the *Name* column, click on the connection to be edited.
2. Make changes, as needed.
3. Click **Save**.

Delete Network Connection

WebUI Procedure

1. Go to *Network :: Connections*.
2. Select a connection checkbox.
3. Click **Delete**.

Move Connection Carrier State Up or Down

WebUI Procedure

1. Go to *Network :: Connections*.
2. Select a connection checkbox.
3. To make it active, click **Up**.
4. To make it inactive, click **Down**.

Set Device to be a WiFi Client

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

WebUI Procedure

1. Go to *Network :: Connections*.
2. In the *Name* column, click on hotspot connection.
3. Unselect the **Connect Automatically** checkbox.

4. Click **Save**.
5. On the table, verify the hotspot interface is down.
6. The system creates a new WiFi interface to allow the device to act as a client.

Create Interface Connections

Add Bonding Interface

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

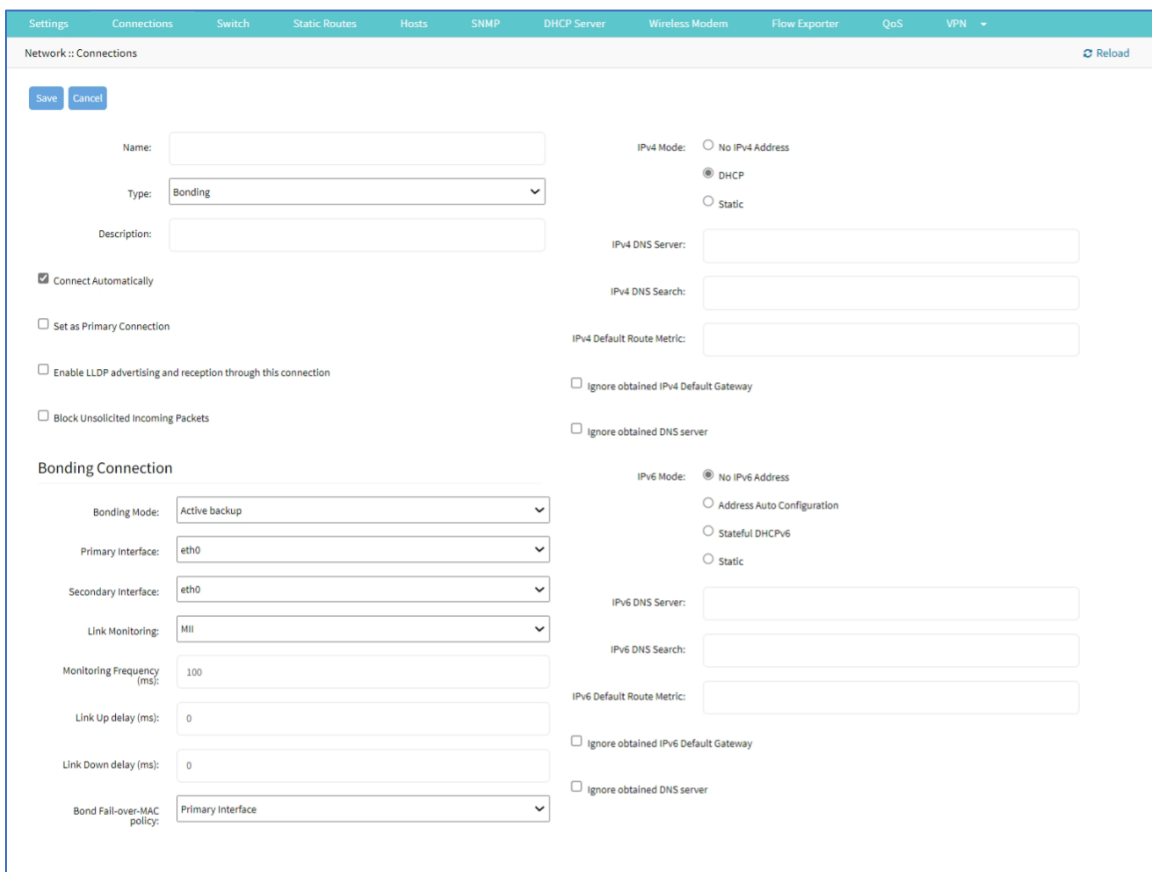
The built-in Network Failover can do the same. The main difference is that the built-in feature Network Failover works on the IP layer for more functionality. A bonding interface works on the link layer.

NOTE: The build function Network Failover and Bonding can be combined.

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

WebUI Procedure

1. Go to *Network :: Connections*.
2. Click **Add** (displays dialog).



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

Enable LLDP advertising and reception through this connection

Port ID:

Port Description:

On **Port ID** drop-down, select one (Interface Name, Interface Index).

On **Port Description** drop-down, select one (Interface Description, Interface Name).

9. Select **Block Unsolicited Incoming Packets** checkbox.
10. In *Bonding Connection* menu, the dialog modifies on the **Bonding Mode** drop-down selection:
 - Round Robin** (packets transmitted in sequential order from first available slave through the last)

Enter **Slave(s)** interface (comma separated).

On **Link Monitoring** drop-down, select one (**MII, ARP**).

Enter **Monitoring Frequency (ms)** value (MII only).

Enter **Link Up delay (ms)** value (MII only).

Enter **Link Down delay (ms)** value (MII only).

On **Bond Fail-over-MAC policy** drop-down, select one (**Primary Interface, Current Active Interface, Follow Active Interface**).

Active Backup (Only one slave in the bond is active. A different slave becomes active if, and only if, the active slave fails.)

On **Primary Interface** drop-down, select interface.

On **Secondary Interface** drop-down, select interface.

On **Link Monitoring** drop-down, select one (**MII, ARP**).

Enter **Monitoring Frequency (ms)** value (MII only).

Enter **Link Up delay (ms)** value (MII only).

Enter **Link Down delay (ms)** value (MII only).

On **Bond Fail-over-MAC policy** drop-down, select one (**Primary Interface, Current Active Interface, Follow Active Interface**).

XOR load balancing (Transmit based on the selected transmit hash policy.)

Enter **Slave(s)** interface (comma separated).

On **Link Monitoring** drop-down, select one (**MII, ARP**).

Enter **Monitoring Frequency (ms)** value (MII only).

Enter **Link Up delay (ms)** value (MII only).

Enter **Link Down delay (ms)** value (MII only).

On **Bond Fail-over-MAC policy** drop-down, select one (**Primary Interface, Current Active Interface, Follow Active Interface**).

On **Transmit Hash Policy** drop-down, select one (**Layer 2, Layer 2 and 3, Layer 3 and 4, Layer 2 and 3 and Encap, Layer 3 and 4 and Encap**)

Broadcast (Transmits everything on all slave interfaces. This mode provides fault tolerances.)

Enter **Slave(s)** interface (comma separated).

On **Link Monitoring** drop-down, select one (**MII, ARP**).

Enter **Monitoring Frequency (ms)** value (MII only).

Enter **Link Up delay (ms)** value (MII only).

Enter **Link Down delay (ms)** value (MII only).

On **Bond Fail-over-MAC policy** drop-down, select one (**Primary Interface, Current Active Interface, Follow Active Interface**).

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.)

Enter **Slave(s)** interface (comma separated).

On **Link Monitoring** drop-down, select one (**MII, ARP**).

Enter **Monitoring Frequency (ms)** value (MII only).

Enter **Link Up delay (ms)** value (MII only).

Enter **Link Down delay (ms)** value (MII only).

On **Bond Fail-over-MAC policy** drop-down, select one (**Primary Interface, Current Active Interface, Follow Active Interface**).

Enter **System Priority** value.

Enter **Actor MAC address**.

Enter **User Port Key**.

On **LACP rate** drop-down, select one (**Slow, Fast**).

On **Aggregation Selection Logic** drop-down, select one (**Stable, Bandwidth, Count**).

On **Transmit Hash Policy** drop-down, select one (**Layer 2, Layer 2 and 3, Layer 3 and 4, Layer 2 and 3 and Encap, Layer 3 and 4 and Encap**)

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.)

Enter **Slave(s)** interface (comma separated).

On **Link Monitoring** drop-down, select one (**MII, ARP**).

Enter **Monitoring Frequency (ms)** value (MII only).

Enter **Link Up delay (ms)** value (MII only).

Enter **Link Down delay (ms)** value (MII only).

On **Bond Fail-over-MAC policy** drop-down, select one (**Primary Interface, Current Active Interface, Follow Active Interface**).

On **Transmit Hash Policy** drop-down, select one (**Layer 2, Layer 2 and 3, Layer 3 and 4, Layer 2 and 3 and Encap, Layer 3 and 4 and Encap**)

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.)

Enter **Slave(s)** interface (comma separated).

On **Link Monitoring** drop-down, select one (**MII, ARP**).

Enter **Monitoring Frequency (ms)** value (MII only).

Enter **Link Up delay (ms)** value (MII only).

Enter **Link Down delay (ms)** value (MII only).

On **Bond Fail-over-MAC policy** drop-down, select one (**Primary Interface, Current Active Interface, Follow Active Interface**).

11. In *IPv4 Mode* menu:

No IPv4 Address radio button.

DHCP radio button.

Static radio button (if selected, displays):

Enter **IP Address**.

Enter **BitMask**.

(optional) Enter **Gateway IP**:

(optional) Enter **IPv4 DNS Server**.

Enter **IPv4 DNS Search** (defines a domain name for DNS lookups).

Enter **IPv4 Default Route Metric**.

Select **Ignore obtained IPv4 Default Gateway** checkbox.

Select **Ignore obtained DNS server** checkbox

12. In *IPv6 Mode* menu:

No IPv6 Address radio button

Address Auto Configuration radio button

Stateful DHCPv6 radio button.

Static radio button (if selected, displays):

Enter **IP Address**.

Enter **Prefix Length**.

(optional) Enter **Gateway IP**.

(optional) Enter **IPv6 DNS Server**.

Enter **IPv6 DNS Search** (defines a domain name for DNS lookups).

Enter **IPv6 Default Route Metric**.

Select **Ignore obtained IPv6 Default Gateway** checkbox.

Select **Ignore obtained DNS server** checkbox.

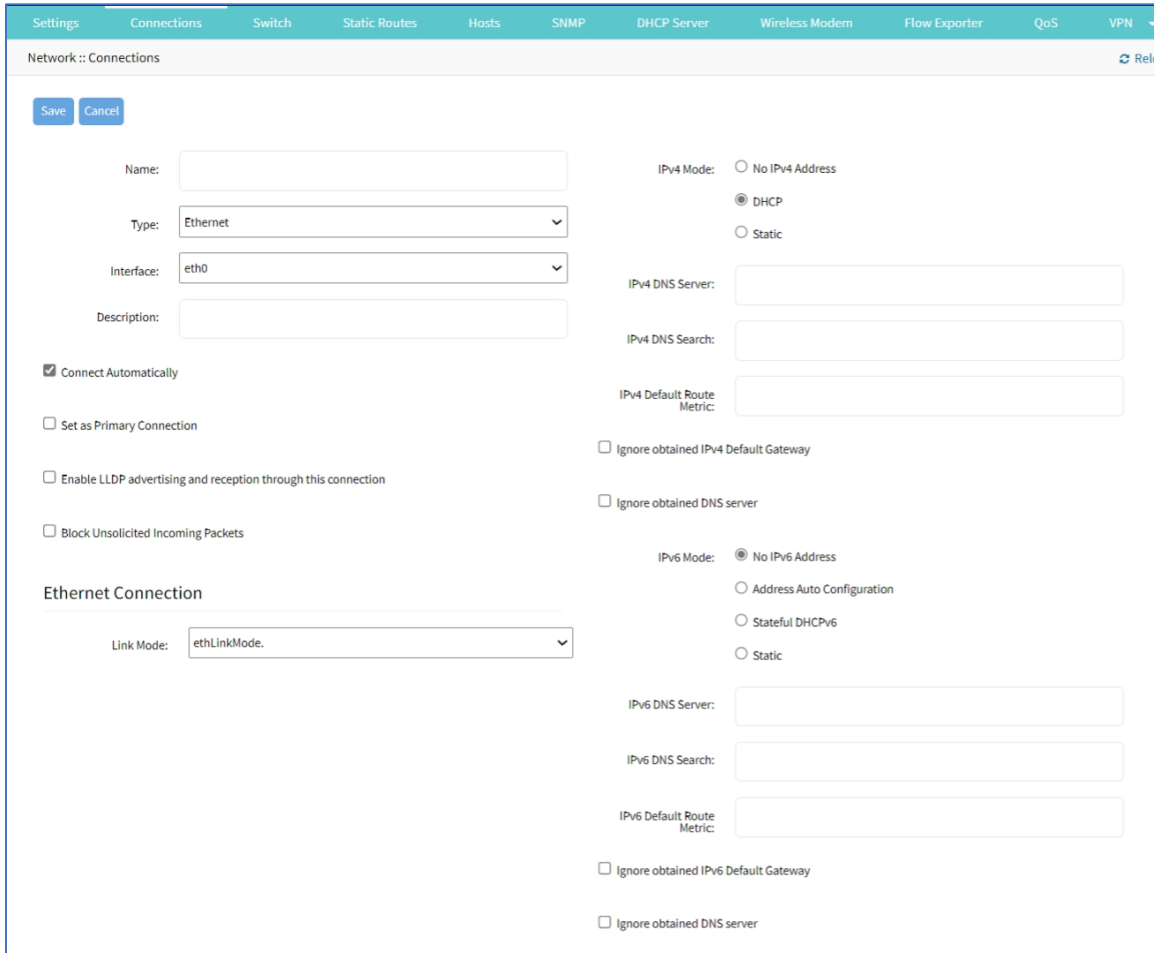
13. Click **Save**.

Add Ethernet Interface

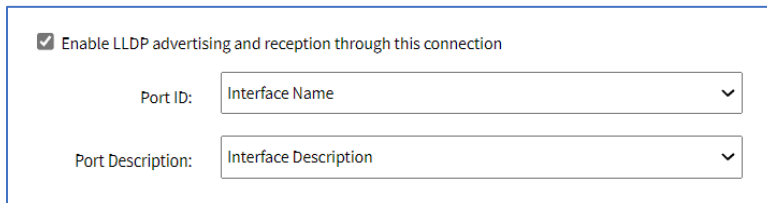
Additional Ethernet interfaces can be added and configured when an additional physical interface is added. This can occur during a Nodegrid Manager installation, where the System might have more than two interfaces to better support network separation.

WebUI Procedure

1. Go to *Network :: Connections*.
2. Click **Add** (displays dialog).



3. Enter **Name**.
4. On **Type** drop-down, select **Ethernet**.
5. On **Interface** drop-down, select one.
6. Enter **Description**.
7. Select **Connect Automatically** checkbox (connection is automatically established at startup).
8. Select **Set as Primary Connection** (defines interface as the primary connection. Only one interface can be the primary.)
9. Select **Enable LLD advertising and reception through this connection** checkbox.



On **Port ID** drop-down, select one (**Interface Name, Interface Index**).

On **Port Description** drop-down, select one (**Interface Description, Interface Name**).

10. Select **Block Unsolicited Incoming Packets** checkbox.
11. In *Ethernet Connection* menu (availability depends on device):
 - On **Link Mode** drop-down, select one (**Auto**, **10M/Half**, **10M/Full**, **100M/Half**, **100M/Full**, **1G/Full**).
 - NOTE:** Only available for copper interfaces. If one of these speeds is selected (not Auto), auto-negotiation (autoneg) is set to off. The selected speed/duplex becomes the default.
12. In *IPv4 Mode* menu:
 - No IPv4 Address** radio button.
 - DHCP** radio button.
 - Static** radio button (if selected, displays):
 - Enter **IP Address**.
 - Enter **BitMask**.
 - (optional) Enter **Gateway IP**:
 - (optional) Enter **IPv4 DNS Server**.
 - Enter **IPv4 DNS Search** (defines a domain name for DNS lookups).
 - Enter **IPv4 Default Route Metric**.
 - Select **Ignore obtained IPv4 Default Gateway** checkbox.
 - Select **Ignore obtained DNS server** checkbox
13. In *IPv6 Mode* menu:
 - No IPv6 Address** radio button
 - Address Auto Configuration** radio button
 - Stateful DHCPv6** radio button.
 - Static** radio button (if selected, displays):
 - Enter **IP Address**.
 - Enter **Prefix Length**.
 - (optional) Enter **Gateway IP**.
 - (optional) Enter **IPv6 DNS Server**.
 - Enter **IPv6 DNS Search** (defines a domain name for DNS lookups).
 - Enter **IPv6 Default Route Metric**.
 - Select **Ignore obtained IPv6 Default Gateway** checkbox.
 - Select **Ignore obtained DNS server** checkbox.
14. 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).

NOTE: Built-in modems support Active-Passive SIM failover. SIM-2 settings are only supported for the built-in modems.

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>.

WebUI Procedure

1. Go to *Network :: Connections*.
2. Click **Add** (displays dialog).

Settings | Connections | Switch | Static Routes | Hosts | SNMP | DHCP Server | Wireless Modem | Flow Exporter | 802.1x | QoS

VPN

Network :: Connections Reload

Save Cancel

Name:

Type: **Mobile Broadband GSM**

Interface: **backplane0**

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 User name:

SIM-1 Password:

SIM-1 Access Point Name (APN):

SIM-1 Personal Identification Number (PIN):

SIM-1 MTU:

Enable Data Usage Monitoring

Enable IP Passthrough

Enable Global Positioning System (GPS)

3. Enter **Name**.
4. On **Type** drop-down, select **Mobile Broadband GSM**.
5. On **Interface** drop-down, select one.
6. Enter **Description**.

7. Select **Connect Automatically** checkbox (connection is automatically established at startup).
8. Select **Set as Primary Connection** (defines interface as the primary connection. Only one interface can be the primary.)
9. Select **Enable LLDP advertising and reception through this connection** checkbox.

Enable LLDP advertising and reception through this connection

Port ID:

Port Description:

On **Port ID** drop-down, select one (Interface Name, Interface Index).

On **Port Description** drop-down, select one (Interface Description, Interface Name).

10. Select **Block Unsolicited Incoming Packets** checkbox.
11. Select **Enable Connection Health Monitoring** checkbox (expands dialog).

Enable Connection Health Monitoring

Ensure Connection is Up

IP Address:

Interval (hours):

Select **Ensure Connection is Up** checkbox.

Enter **IP Address**.

Enter **Interval (hours)**.

12. In *IPv4 Mode* menu:

No IPv4 Address radio button.

DHCP radio button.

(optional) Enter **IPv4 DNS Server**.

Enter **IPv4 DNS Search** (defines a domain name for DNS lookups).

Enter **IPv4 Default Route Metric**.

Ignore obtained IPv4 Default Gateway checkbox.

Ignore obtained DNS server checkbox.

13. In *IPv6 Mode* menu:

No IPv4 Address radio button.

Address Auto Configuration radio button.

(optional) Enter **IPv6 DNS Server**.

Enter **IPv6 DNS Search** (defines a domain name for DNS lookups).

Enter **IPv6 Default Route Metric**.

Ignore obtained IPv6 Default Gateway checkbox.

Ignore obtained DNS server checkbox.

14. In *Mobile Broadband Connection* menu:

Enter **SIM-1 Phone Number**.

Enter **SIM-1 User name** (User name to unlock the SIM).

Enter **SIM-1 Password**.

Enter **SIM-1 Access Point Name (APN)**.

Enter **SIM-1 Personal Identification Number (PIN)**.

Enter **SIM-1 MTU**. (bytes – can be set to 'auto' – equal to 1500 bytes).

Select **Enable Data Usage Monitoring** checkbox.

Enter **SIM-1 Data Limit Value (GB)** (monthly data limit).

Enter **SIM-1 Data Warning (%)** (percentage that triggers an alarm).

Enter **SIM-1 Renew Day** (day to reset accumulated data).

Select **Enable IP Passthrough** checkbox.

On **Ethernet Connection** drop-down, select one.

Enter **MAC Address** (if blank, the system uses DHCP to get the device).

Enter **Port Intercepts** (any ports that should NOT pass through the Nodegrid device).

Select **Enable Global Positioning System (GPS)** checkbox.

Enter **Polling Time (min)**.

On **GPS Antenna** drop-down, select one

Shared GPS/Rx diversity(aux) antenna

Dedicated Active GPS antenna

Dedicated Passive GPS antenna

(if applicable) Select **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.

15. Click **Save**.

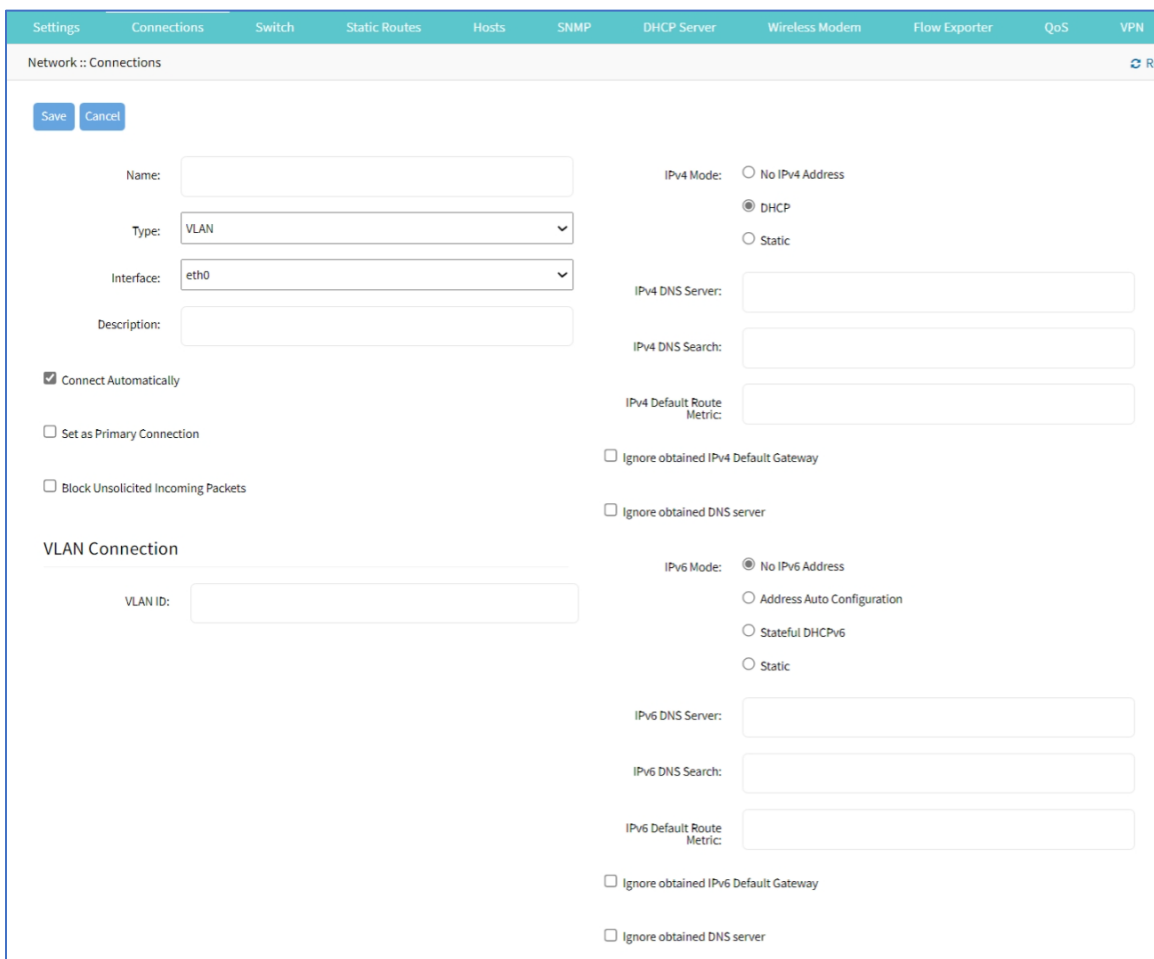
Add VLAN Interface

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).

WebUI Procedure

1. Go to *Network :: Connections*.
2. Click **Add** (displays dialog).



The screenshot shows the 'Network :: Connections' configuration page. At the top, there are navigation tabs: Settings, Connections, Switch, Static Routes, Hosts, SNMP, DHCP Server, Wireless Modem, Flow Exporter, QoS, and VPN. The main content area has a 'Network :: Connections' header with a refresh icon. Below the header are 'Save' and 'Cancel' buttons. The configuration form is divided into several sections:

- General Settings:**
 - Name: [Text Input]
 - Type: [VLAN (Dropdown)]
 - Interface: [eth0 (Dropdown)]
 - Description: [Text Input]
 - Connect Automatically
 - Set as Primary Connection
 - Block Unsolicited Incoming Packets
- IPv4 Settings:**
 - IPv4 Mode:
 - No IPv4 Address
 - DHCP
 - Static
 - IPv4 DNS Server: [Text Input]
 - IPv4 DNS Search: [Text Input]
 - IPv4 Default Route Metric: [Text Input]
 - Ignore obtained IPv4 Default Gateway
 - Ignore obtained DNS server
- IPv6 Settings:**
 - IPv6 Mode:
 - No IPv6 Address
 - Address Auto Configuration
 - Stateful DHCPv6
 - Static
 - IPv6 DNS Server: [Text Input]
 - IPv6 DNS Search: [Text Input]
 - IPv6 Default Route Metric: [Text Input]
 - Ignore obtained IPv6 Default Gateway
 - Ignore obtained DNS server
- VLAN Connection:**
 - VLAN ID: [Text Input]

3. Enter **Name**.
4. On **Type** drop-down, select **VLAN**.
5. On **Interface** drop-down, select one.
6. Enter **Description**.
7. Select **Connect Automatically** checkbox (connection is automatically established at startup).

8. Select **Set as Primary Connection** (defines interface as the primary connection. Only one interface can be the primary.)
9. Select **Block Unsolicited Incoming Packets** checkbox.
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, displays):
 - Enter **IP Address**.
 - Enter **BitMask**.
 - (optional) Enter **Gateway IP**:
 - (optional) Enter **IPv4 DNS Server**.
 - Enter **IPv4 DNS Search** (defines a domain name for DNS lookups).
 - Enter **IPv4 Default Route Metric**.
 - Select **Ignore obtained IPv4 Default Gateway** checkbox.
 - Select **Ignore obtained DNS server** checkbox
12. In *IPv6 Mode* menu:
 - No IPv6 Address** radio button
 - Address Auto Configuration** radio button
 - Stateful DHCPv6** radio button.
 - Static** radio button (if selected, displays):
 - Enter **IP Address**.
 - Enter **Prefix Length**.
 - (optional) Enter **Gateway IP**.
 - (optional) Enter **IPv6 DNS Server**.
 - Enter **IPv6 DNS Search** (defines a domain name for DNS lookups).
 - Enter **IPv6 Default Route Metric**.
 - Select **Ignore obtained IPv6 Default Gateway** checkbox.
 - Select **Ignore obtained DNS server** checkbox.
13. Click **Save**.

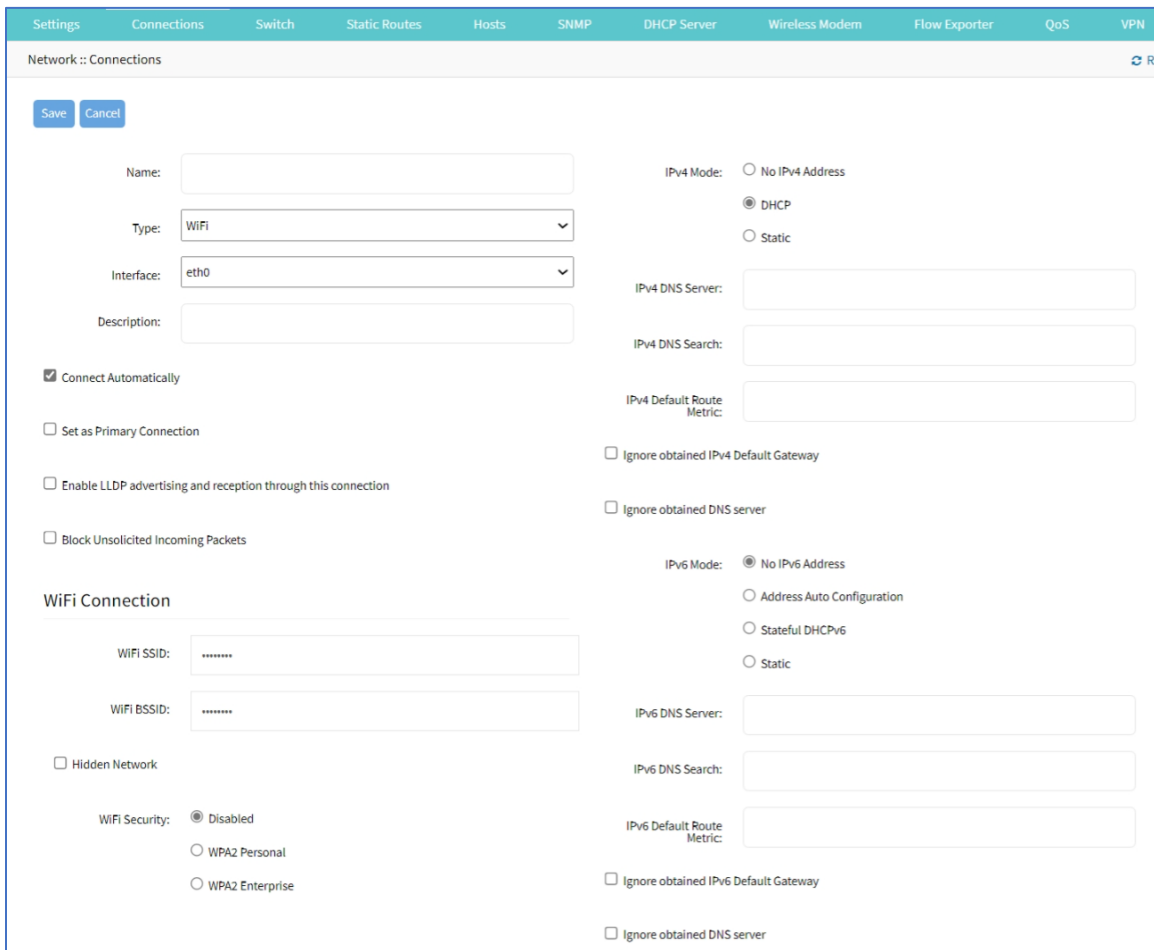
Add WiFi Interface

The System support a Nodegrid device as a WiFi client or access point. A compatible WiFi module must be installed.

By default, a hotspot interface is defined which configures the device as an access point (if a WiFi module is present). To use the Nodegrid as an access point, update the values. The default password of the hotspot connection is the device serial number.

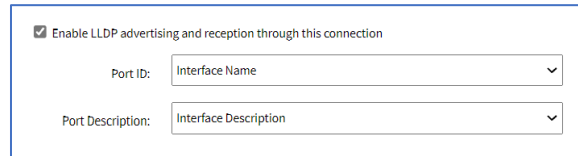
WebUI Procedure

1. Go to *Network :: Connections*.
2. Click **Add** (displays dialog).



3. Enter **Name**.
4. On **Type** drop-down, select **WiFi**.
5. On **Interface** drop-down, select one.
6. Enter **Description**.
7. Select **Connect Automatically** checkbox (connection is automatically established at startup).

8. Select **Set as Primary Connection** (defines interface as the primary connection. Only one interface can be the primary.)
9. Select **Enable LLD advertising and reception through this connection** checkbox.



On **Port ID** drop-down, select one (Interface Name, Interface Index).

On **Port Description** drop-down, select one (**Interface Description, Interface Name**).

10. Select **Block Unsolicited Incoming Packets** checkbox.

11. In *WiFi Connection* menu:

Enter **WiFi SSID**.

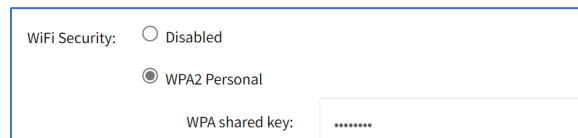
Enter **WiFi BSSID** (MAC address of the Access Point)

Select **Hidden Network** checkbox (if applicable).

In *WiFi Security* menu (select one):

Disabled radio button

WPA2 Personal radio button (if selected, displays). Enter **WPA shared key**.



WPA2 Enterprise radio button (if selected, displays):

Enter **Username**.

Enter **Password**.

On **Method** drop-down, select one.

On **Phase 2 Authentication** drop-down, select one.

Select **Validate server certificate** checkbox.

12. In *IPv4 Mode* menu, select one:

No IPv4 Address radio button.

DHCP radio button.

Static radio button (if selected, displays):

Enter **IP Address**.

Enter **BitMask**.

(optional) Enter **Gateway IP**:

(optional) Enter **IPv4 DNS Server**.

Enter **IPv4 DNS Search** (defines a domain name for DNS lookups).

Enter **IPv4 Default Route Metric**.

Select **Ignore obtained IPv4 Default Gateway** checkbox.

Select **Ignore obtained DNS server** checkbox

13. In *IPv6 Mode* menu:

No IPv6 Address radio button

Address Auto Configuration radio button

Stateful DHCPv6 radio button.

Static radio button (if selected, displays):

Enter **IP Address**.

Enter **Prefix Length**.

(optional) Enter **Gateway IP**.

(optional) Enter **IPv6 DNS Server**.

Enter **IPv6 DNS Search** (defines a domain name for DNS lookups).

Enter **IPv6 Default Route Metric**.

Ignore obtained IPv6 Default Gateway checkbox.

Ignore obtained DNS server checkbox.

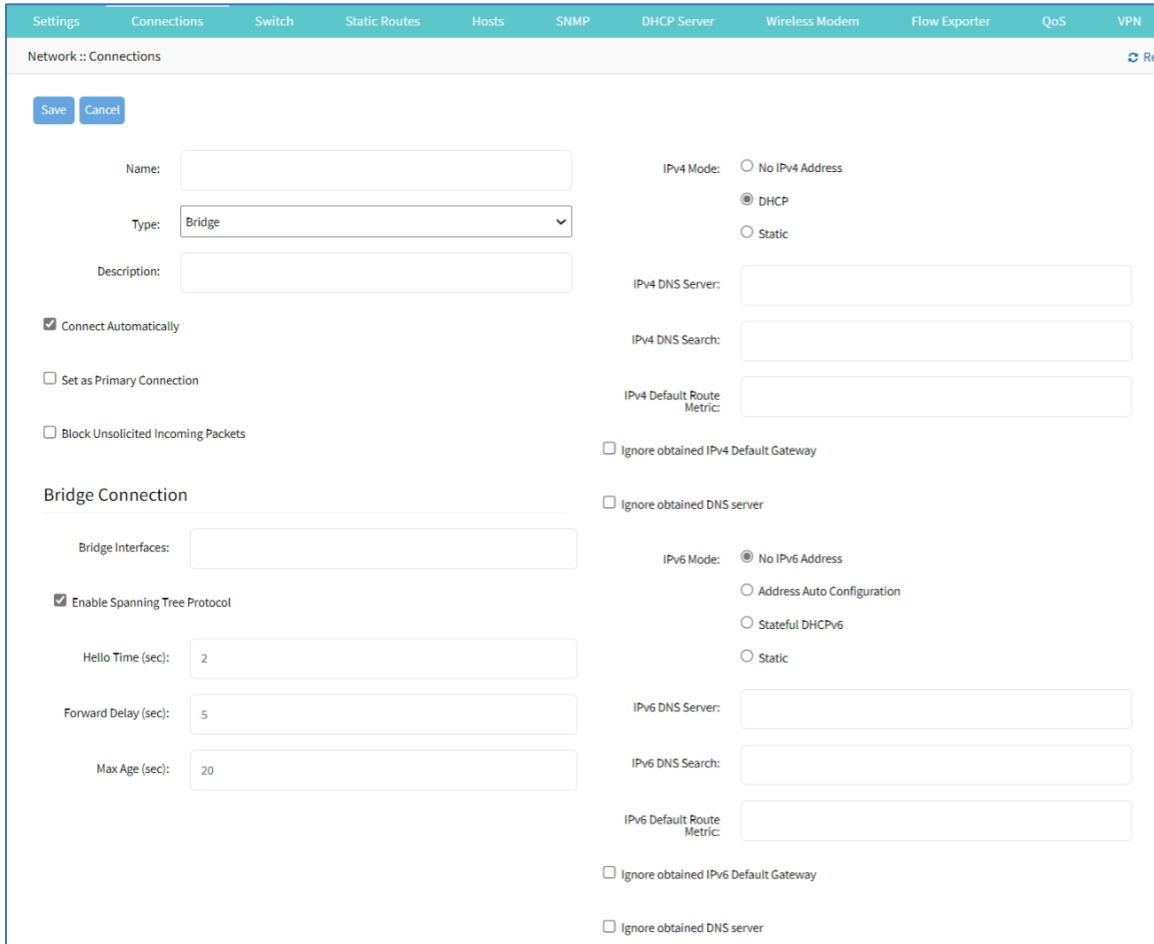
14. Click **Save**.

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.

WebUI Procedure

1. Go to *Network :: Connections*.
2. Click **Add** (displays dialog).



3. Enter **Name**.
4. On **Type** drop-down, select **Bridge**.
5. Enter **Description**.
6. Select **Connect Automatically** checkbox (connection is automatically established at startup).
7. Select **Set as Primary Connection** (defines interface as the primary connection. Only one interface can be the primary.)
8. Select **Block Unsolicited Incoming Packets** checkbox.
9. In *Bridge Connection* menu:
 - Enter **Bridge Interfaces** (comma-separated list of physical interfaces).
 - Select **Enable Spanning Tree Protocol** checkbox.
 - Enter **Hello Time (sec)** (number of seconds a HELLO packet is sent when Spanning Tree is enabled).
 - Enter **Forward Delay (sec)** (packet forward delay when Spanning Tree is enabled).
 - Enter **Max Age (sec)** (maximum age for packages when Spanning Tree is enabled).

10. In *IPv4 Mode* menu, select one:

No IPv4 Address radio button.

DHCP radio button.

Static radio button (if selected, displays):

Enter **IP Address**.

Enter **BitMask**.

(optional) Enter **Gateway IP**:

(optional) Enter **IPv4 DNS Server**.

Enter **IPv4 DNS Search** (defines a domain name for DNS lookups).

Enter **IPv4 Default Route Metric**.

Select **Ignore obtained IPv4 Default Gateway** checkbox.

Select **Ignore obtained DNS server** checkbox

11. In *IPv6 Mode* menu:

No IPv6 Address radio button

Address Auto Configuration radio button

Stateful DHCPv6 radio button.

Static radio button (if selected, displays):

Enter **IP Address**.

Enter **Prefix Length**.

(optional) Enter **Gateway IP**.

(optional) Enter **IPv6 DNS Server**.

Enter **IPv6 DNS Search** (defines a domain name for DNS lookups).

Enter **IPv6 Default Route Metric**.

Select **Ignore obtained IPv6 Default Gateway** checkbox.

Select **Ignore obtained DNS server** checkbox.

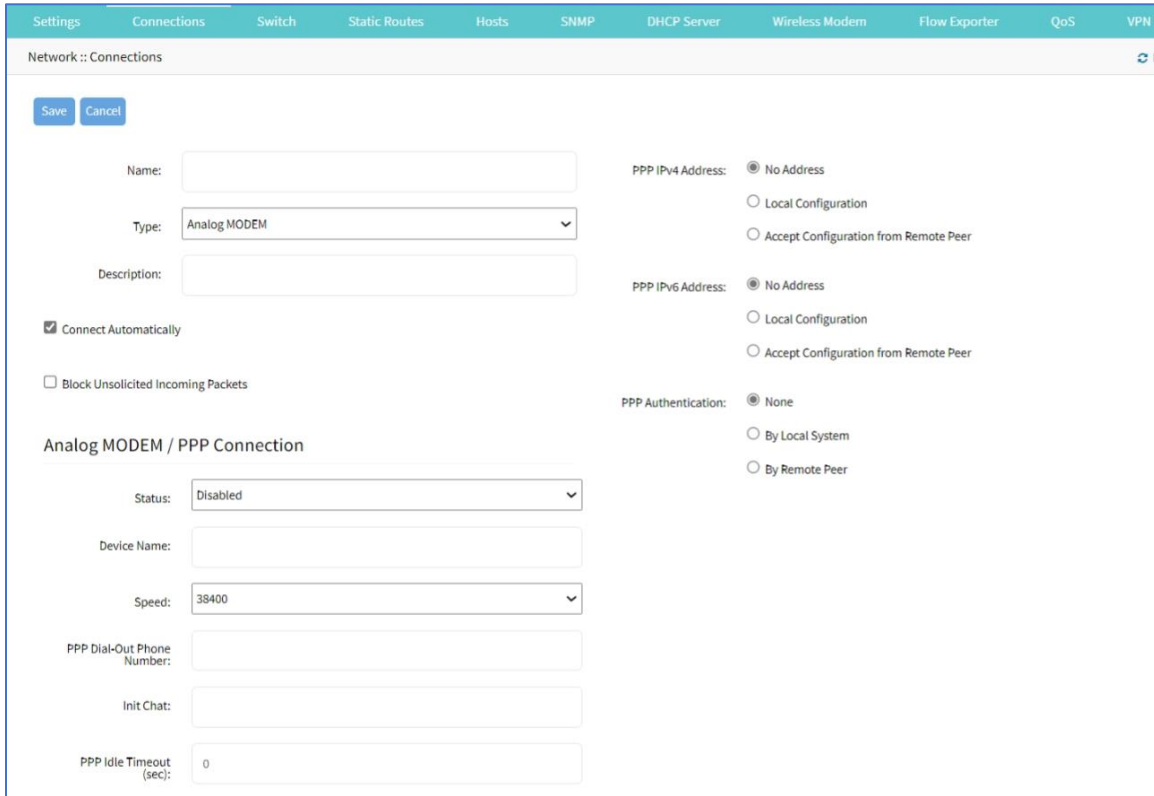
12. Click **Save**.

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.

WebUI Procedure

1. Go to *Network :: Connections*.
2. Click **Add** (displays dialog).



3. Enter **Name**.
4. On **Type** drop-down, select **Analog MODEM**.
5. Enter **Description**.
6. Select **Connect Automatically** checkbox (connection is automatically established at startup).
7. Select **Block Unsolicited Incoming Packets** checkbox.
8. In *Analog MODEM / PPP Connection* menu:
 - On **Status** drop-down, select one (**Enabled, Disabled**).
 - Enter **Device Name**.
 - On **Speed** drop-down, select one (**9600, 19200, 38400, 57600, 115200**).
 - Enter **PPP Dial-Out Phone Number**.
 - Enter **Init Chat** (a specific AT init string, if required).
 - Enter **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):
 - No Address** radio button
 - Local Configuration** radio button (displays):
 - Enter **Local Address**.

Enter **Remote Address**.

Accept Configuration from Remote Peer radio button

10. In *PPP IPv6 Address* menu (select one):

No Address radio button

Local Configuration radio button (displays)

Enter **Local Address (LL)**.

Enter **Remote Address (LL)**.

Accept Configuration from Remote Peer radio button

11. In *PPP Authentication* menu:

None radio button

By **Local System** radio button (displays):

On **Authentication Protocol** drop-down, select one (**PAP, CHAP, EAP**).

By **Remote Peer** radio button (displays):

Enter **Remote Username**.

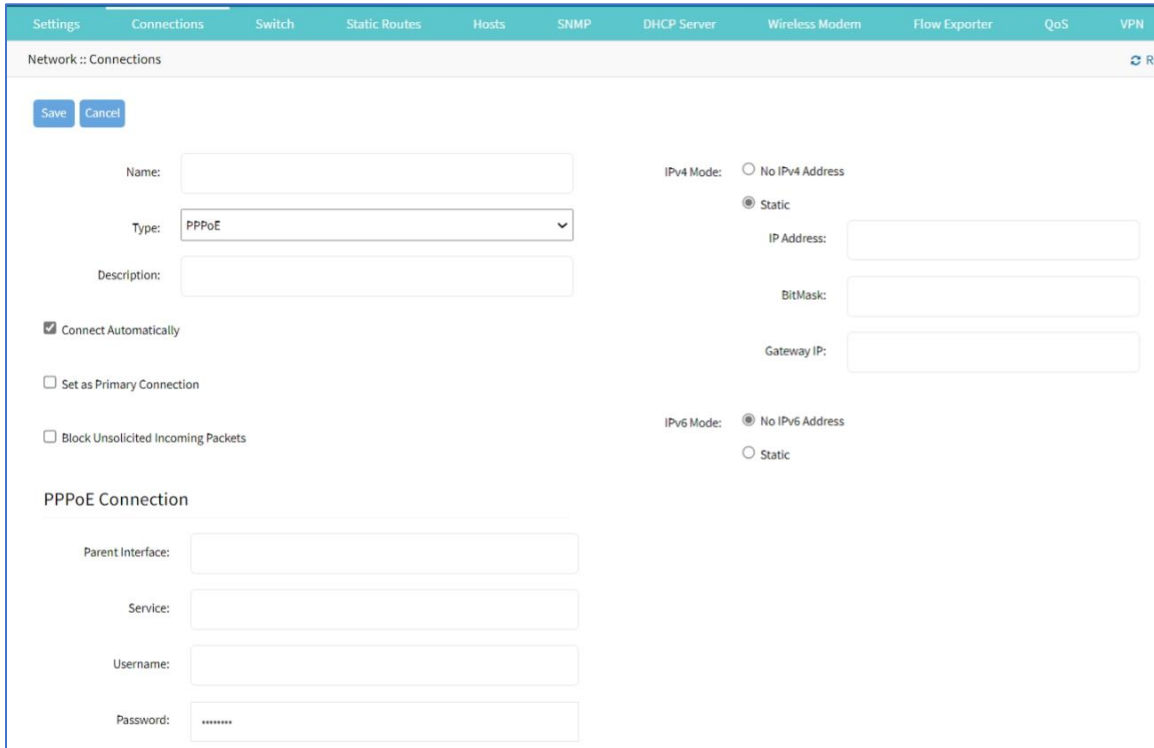
Enter **Remote Passphrase**.

12. Click **Save**.

Add PPPoE Interface

WebUI Procedure

1. Go to *Network :: Connections*.
2. Click **Add** (displays dialog).



3. Enter **Name**.
4. On **Type** drop-down, select **PPPoE**.
5. Enter **Description**.
6. Select **Connect Automatically** checkbox (connection is automatically established at startup).
7. Select **Set as Primary Connection** (defines interface as the primary connection. Only one interface can be the primary.)
8. Select **Block Unsolicited Incoming Packets** checkbox.
9. In *PPPoE Connection* menu:

Enter **Parent Interface** (default: blank)

If entered, specifies the parent interface name on which this PPPoE connection should be created. If blank, connection is activated on the ethernet interface. (default: blank)

Enter **Service** (default: blank)

If specified, 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.

Enter **Username**.

Enter **Password**.

10. In *IPv4 Mode* menu, select one:

No IPv4 Address radio button.

Static radio button (if selected, displays):

Enter **IP Address**.

Enter **BitMask**.

(optional) Enter **Gateway IP**:

11. In *IPv6 Mode* menu:

No IPv6 Address radio button

Static radio button (if selected, displays):

Enter **IP Address**.

Enter **Prefix Length**.

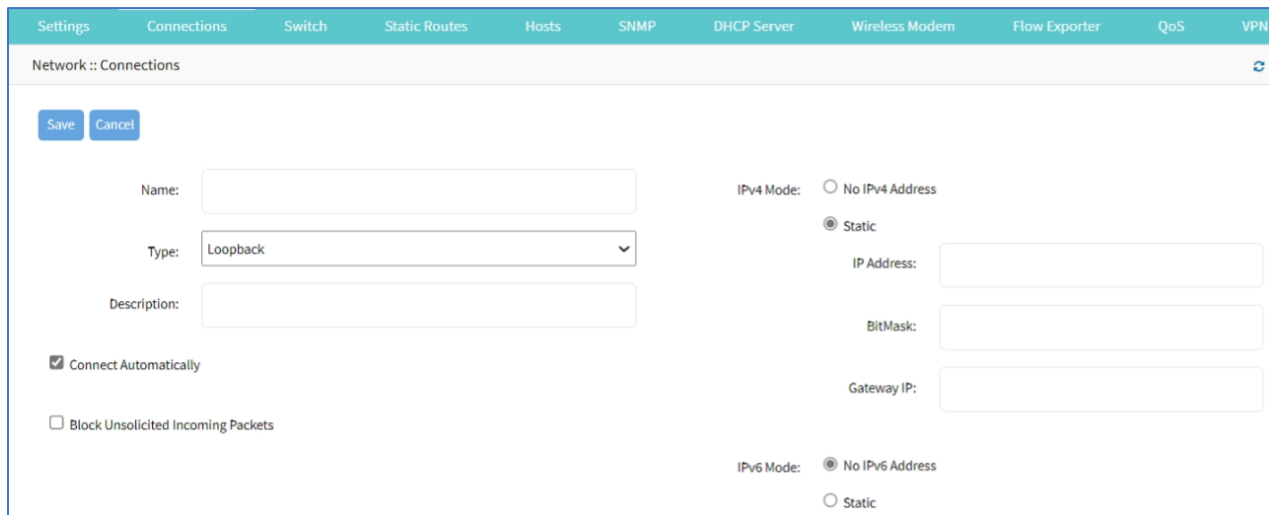
(optional) Enter **Gateway IP**.

12. Click **Save**.

Add Loopback Interface

WebUI Procedure

1. Go to *Network :: Connections*.
2. Click **Add** (displays dialog).



The screenshot shows the 'Network :: Connections' configuration dialog. At the top, there are navigation tabs: Settings, Connections, Switch, Static Routes, Hosts, SNMP, DHCP Server, Wireless Modem, Flow Exporter, QoS, and VPN. The dialog has a 'Save' button and a 'Cancel' button. The 'Name' field is empty. The 'Type' dropdown is set to 'Loopback'. The 'Description' field is empty. There are two checkboxes: 'Connect Automatically' (checked) and 'Block Unsolicited Incoming Packets' (unchecked). On the right side, there are two sections for IP modes. The 'IPv4 Mode' section has two radio buttons: 'No IPv4 Address' (unselected) and 'Static' (selected). Below it are three input fields: 'IP Address', 'BitMask', and 'Gateway IP'. The 'IPv6 Mode' section has two radio buttons: 'No IPv6 Address' (selected) and 'Static' (unselected).

3. Enter **Name**.

4. On **Type** drop-down, select **Loopback**.

5. Enter **Description**.

6. Select **Connect Automatically** checkbox (connection is automatically established at startup).

7. Select **Block Unsolicited Incoming Packets** checkbox.
8. In *IPv4 Mode* menu, select one:
 - No IPv4 Address** radio button.
 - Static** radio button (if selected, displays):
 - Enter **IP Address**.
 - Enter **BitMask**.
 - (optional) Enter **Gateway IP**:
9. In *IPv6 Mode* menu:
 - No IPv6 Address** radio button
 - Static** radio button (if selected, displays):
 - Enter **IP Address**.
 - Enter **Prefix Length**.
 - (optional) Enter **Gateway IP**.
10. Click **Save**.

Switch tab (NSR, GSR, BSR)

These functions are only available on Nodegrid NSR, GSR, BSR devices.

Users can configure the built-in network switch. Supported functions include enable/disable individual ports, as well as creation of tagged (trunk) and untagged (access) ports.

Each card that provides network connectivity (Backplane 0/1 and SFP0/1) are directly connected to the switch. By default, the interfaces Backplane0/1 and SFP0/1 are active. By default, these can provide or consume ZTP, PXE and DHCP requests. By default, all other network interfaces are disabled.

All ports belong to VLAN1 and provide direct communication between enabled interfaces, except Backplane1 and SFP1 (which belong to VLAN2).

Physical Interfaces

Connection	Model	Physical interface
ETH0	all	eth0
ETH1	Nodegrid NSC, NSR	eth1
BACKPLANE0	Nodegrid NSR, BSR, GSR	NSR: backplane0 is in the same VLAN as SFP0 and switch ports by default GSR, BSR: backplane0 is in the same VLAN as SFP0 and switch ports by default
BACKPLANE1	Nodegrid NSR, GSR	NSR: backplane1 is in the same VLAN as SFP1 by default GSR: backplane1 is not in any VLAN by default

Connection	Model	Physical interface
SFP0	Nodegrid GSR, NSR	GSR: sfp0 NSR: SFP0 is in the same VLAN as backplane0 and switch ports by default
SFP1	Nodegrid GSR, NSR	GSR: sfp1 NSR: SFP1 is connected to backplane1 by default
hotspot	all	Interface is bound to wireless adapter (if available).

Switch Interfaces sub-tab

These provide an overview of all switch ports, current status, and allow enable/disable. Current VLAN associates (tagged and untagged) are shown and Port VLAN IDs can be configured.

NSR

Interface	Status	Speed	Port VLAN ID	Jumbo Frame	ACL Ingress	ACL Egress	MSTP Status	802.1x Status	Description
<input checked="" type="checkbox"/> sfp0	Enabled	Auto	1	Disabled	None	None	Disabled	Disabled	
<input type="checkbox"/> sfp1	Enabled	Auto	2	Disabled	None	None	Disabled	Disabled	

GSR

Switch Interfaces Backplane VLAN PoE Global

Network :: Switch :: Switch Interfaces ▶ Start ✓ Confirm ⊖ Revert ↻ Reload

Switch Interfaces

Legend:

- Speed: Auto (red), 10 MbE (orange), 100 MbE (green), 1 GbE (yellow), 2.5 GbE (purple), 10 GbE (blue)
- Status: Enabled (green), Disabled (grey)

Edit

<input type="checkbox"/>	Interface	Status	Speed	Port VLAN ID	Jumbo Frame	Description
<input type="checkbox"/>	netS1	Enabled	Auto	1	Enabled	
<input type="checkbox"/>	netS2	Enabled	Auto	1	Enabled	
<input type="checkbox"/>	netS3	Enabled	Auto	1	Enabled	
<input type="checkbox"/>	netS4	Enabled	Auto	1	Enabled	

BSR

Switch Interfaces Backplane VLAN Global

Network :: Switch :: Switch Interfaces ▶ Start ✓ Confirm ⊖ Revert ↻ Reload

Switch Interfaces

Legend:

- Speed: Auto (red), 10 MbE (orange), 100 MbE (green), 1 GbE (yellow), 2.5 GbE (purple), 10 GbE (blue)
- Status: Enabled (green), Disabled (grey)

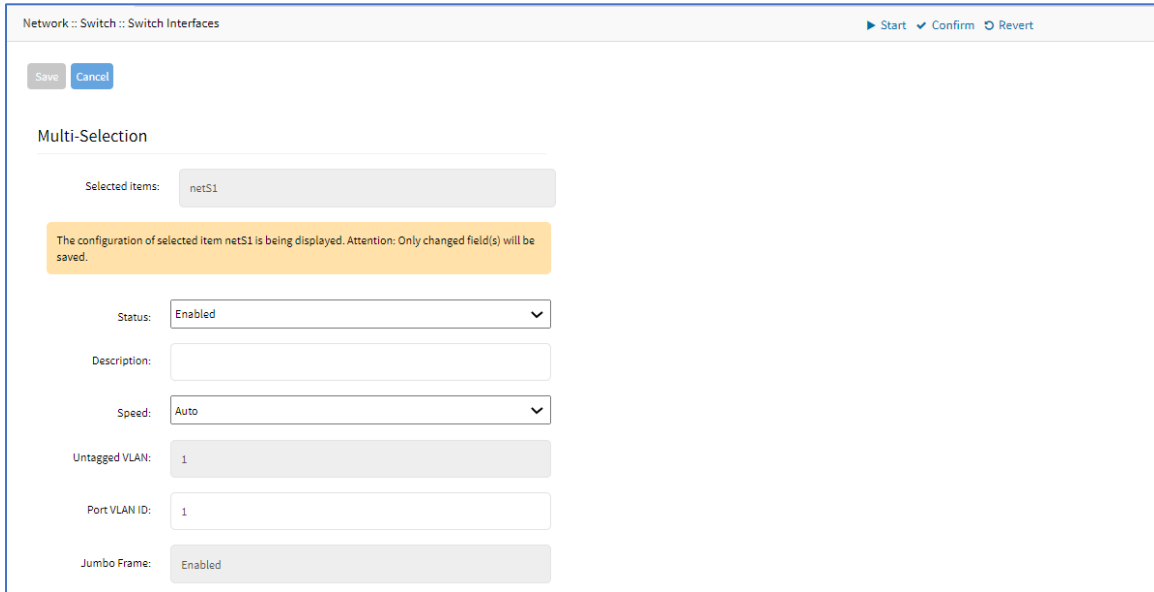
Edit

<input type="checkbox"/>	Interface	Status	Speed	Port VLAN ID	Jumbo Frame	Description
<input type="checkbox"/>	netS1	Enabled	Auto	1	Enabled	
<input type="checkbox"/>	netS2	Enabled	Auto	1	Enabled	
<input type="checkbox"/>	netS3	Enabled	Auto	1	Enabled	
<input type="checkbox"/>	netS4	Enabled	Auto	1	Enabled	

Edit Switch Port Interface (BSR, GSR)

WebUI Procedure

1. Go to *Network :: Switch :: Switch Interfaces*.
2. In the table, select checkbox.
3. Click **Edit** (displays dialog).

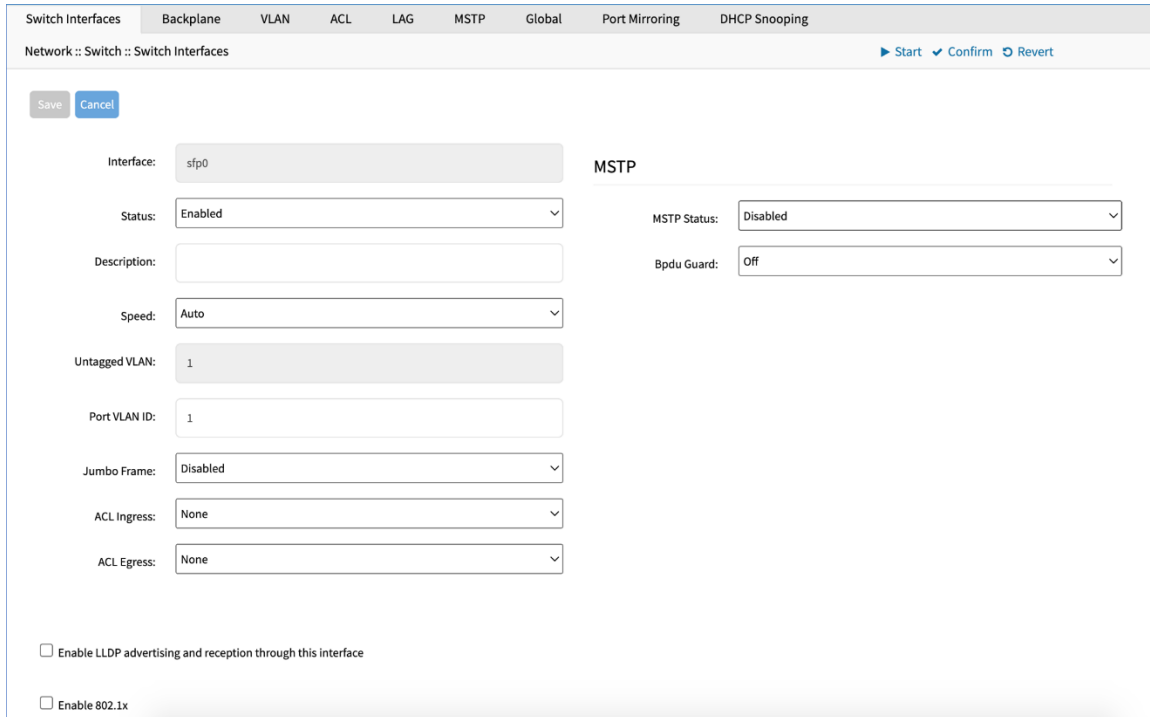


4. As needed, make changes:
 - Status** drop-down (**enabled, disabled**).
 - Description**.
 - Speed** drop-down (**Auto, 10M, 100M, 1G**).
 - Port VLAN ID**.
5. Click **Save**.

Edit Switch Port Interface (NSR)

WebUI Procedure

6. Go to *Network :: Switch :: Switch Interfaces*.
7. In the table, select checkbox.
8. Click **Edit** (displays dialog).



Switch Interfaces | Backplane | VLAN | ACL | LAG | MSTP | Global | Port Mirroring | DHCP Snooping

Network :: Switch :: Switch Interfaces ▶ Start ▼ Confirm ↺ Revert

Save Cancel

Interface: sfp0 **MSTP**

Status: Enabled ▼

Description:

Speed: Auto ▼

Untagged VLAN: 1

Port VLAN ID: 1

Jumbo Frame: Disabled ▼

ACL Ingress: None ▼

ACL Egress: None ▼

MSTP Status: Disabled ▼

Bpdu Guard: Off ▼

Enable LLDP advertising and reception through this interface

Enable 802.1x

9. As needed, make changes:

Status drop-down (**enabled, disabled**).

Description.

Speed drop-down (**Auto, 10M, 100M, 1G, 10G**).

Port VLAN ID.

Jumbo Frame drop-down (**enabled, disabled**).

(if available) **ACL Ingress** drop-down (select one).

(if available) **ACL Egress** drop-down (select one).

Enable LLDP advertising and reception through this interface checkbox.

Enable 802.1x checkbox.

10. In *MSTP* menu, select:

MSTP Status drop-down (**enabled, disabled**)

(To be active, *Network :: Switch :: Global :: Spanning Tree* status must be enabled).

BPDU Guard drop-down (selection varies). Protects Layer 2 Spanning Tree Protocol (STP) Topology from BPDU related attacks.

(To be active, *Network :: Switch :: Global :: Spanning Tree* status must be enabled).

11. Click **Save**.

Backplane sub-tab

Backplane settings control the switch interfaces directly exposed to the Nodegrid Platform. For the Nodegrid to communicate with any existing switch ports or VLANs, at least one of the backplane interfaces must be part of the specific VLAN. The backplane settings display the current VLAN associations. The Port VLAN IDs can be set for the backplane interfaces.

NOTE: Display varies depending on device – GSR, BSR, or NSR).

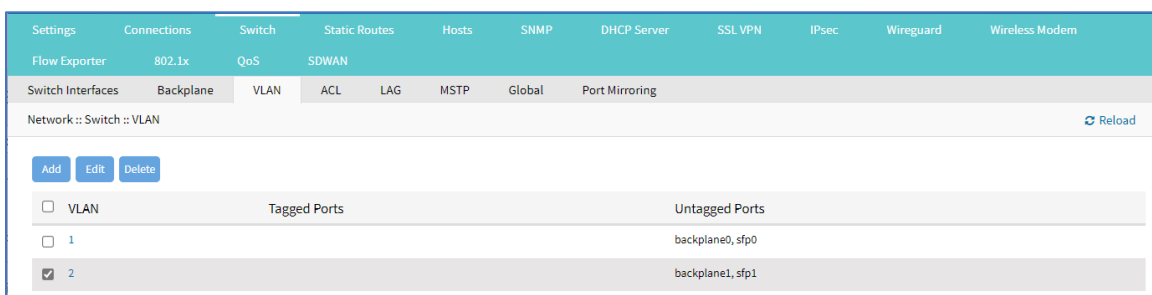
Edit Backplane Settings

WebUI Procedure

1. Go to *Network :: Switch :: Backplane*.
2. In *backplane0*, make changes, as needed:
Enter **Port VLAN ID**.
(if active) On **Jumbo Frame** drop-down, select one (**Enabled, Disabled**).
3. In *backplane1*, make changes, as needed:
Enter **Port VLAN ID**.
(if active) On **Jumbo Frame** drop-down, select one (**Enabled, Disabled**).
4. (if shown) In *Slot1-0*, make changes, as needed (displays if a compute card is present in slot 1):
Enter **Port VLAN ID**.
(if active) On **Jumbo Frame** drop-down, select one (**Enabled, Disabled**).
5. (if shown) In *Slot1-1*, make changes, as needed (displays if a compute card is present in slot 1):
Enter **Port VLAN ID**.
(if active) On **Jumbo Frame** drop-down, select one (**Enabled, Disabled**).
6. Click **Save**.

VLAN sub-tab

The Port VLAN ID is assigned to all incoming untagged packets. Then, the Port VLAN ID is used to forward packets to other ports which match that VLAN ID.



VLAN	Tagged Ports	Untagged Ports
<input type="checkbox"/> 1		backplane0, sfp0
<input checked="" type="checkbox"/> 2		backplane1, sfp1

The switch port interface identifies the VLAN interfaces to which a port belongs. For most situations, a port is either an untagged port (equivalent to an access port) or a tagged port (equivalent to a trunk port).

802.1 support is available with the “Enable 802.1X” checkbox. Use the drop down menu to select the desired 802.1 profile. Profiles can be created within *Network :: Switch :: 802.1* configuration.

The following speeds are configurable within the NSR SFP0/SFP1 and 8-SFP card (depending on which transceivers are inserted):

Auto (reads SFP to configure 1G or 10G)

10G

1G (used with fiber or copper 1000BASE-T transceivers. Supports auto-negotiation: enabled or disabled)

10/100/1000 – (used with copper 10/100/1000BASE-T transceivers. Auto-negotiation is enabled.)

100M (used with copper 10/100/1000BASE-T transceivers. Auto-negotiation is disabled and speed is forced 100M.)

10M (used with copper 10/100/1000BASE-T transceivers. Auto-negotiation is disabled and speed is forced 10M.)

Untagged/Access Ports

To assign a port to a specific VLAN as an untagged or access port, enable the port and change the PORT VLAN ID to the desired VLAN. The port is automatically assigned to VLAN and untagged port.

NOTE: the VLAN must exist before the port can be assigned.

Tagged/Trunk Ports

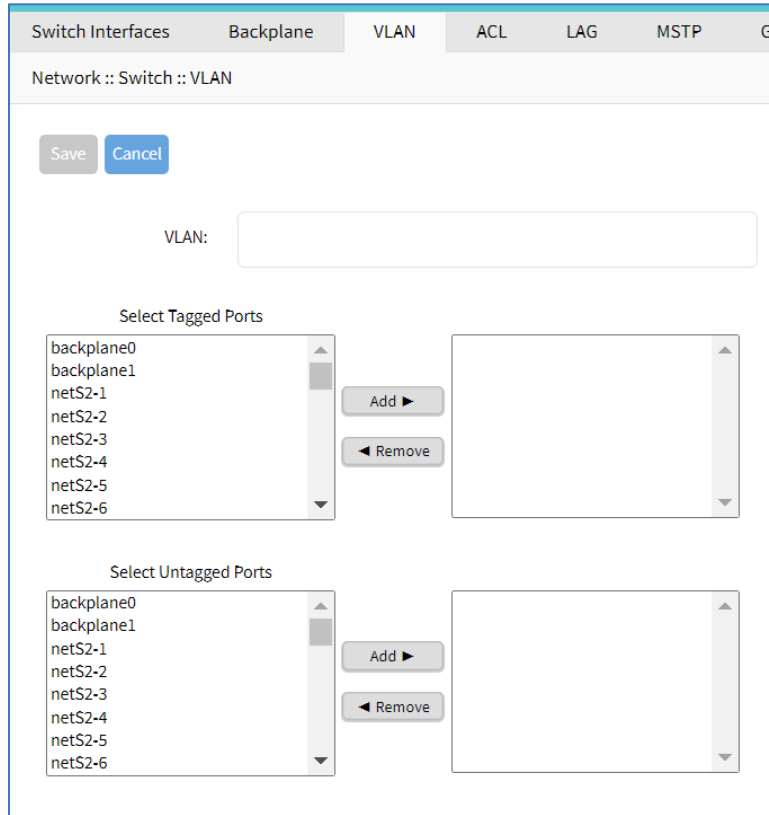
Tagged ports accept incoming packets with VLAN tags. Tagged ports will accept any packet which belongs to an assigned VLAN. They are used to create a trunk connection between multiple switches. To assign a port as a tagged port, a minimum of one VLAN must be added to a port as tagged VLAN. This can be done on the VLAN configuration. The Port VLAN ID for a tagged port should match one of the assigned VLANs or be blank. Untagged traffic is not accepted by the port.

NOTE: the VLAN must exist before the port can be assigned.

Add VLAN

WebUI Procedure

1. Go to *Network :: Switch :: VLAN*.
2. Click **Add** (displays dialog).



3. Enter **VLAN**.
4. In *Select Tagged Ports*, select from left-side panel, click **Add ►** to move to right-side panel.
To remove from right-side panel, select and click **◀ Remove**.
5. In *Select Untagged Ports*, select from left-side panel, click **Add ►** to move to right-side panel.
To remove from right-side panel, select and click **◀ Remove**.
6. Click **Save**.

Edit VLAN

WebUI Procedure

1. Go to *Network :: Switch :: VLAN*.
2. Select checkbox next to item to edit.
3. Click **Edit** (displays dialog).
4. Make changes, as needed.
5. Click **Save**.

Delete VLAN

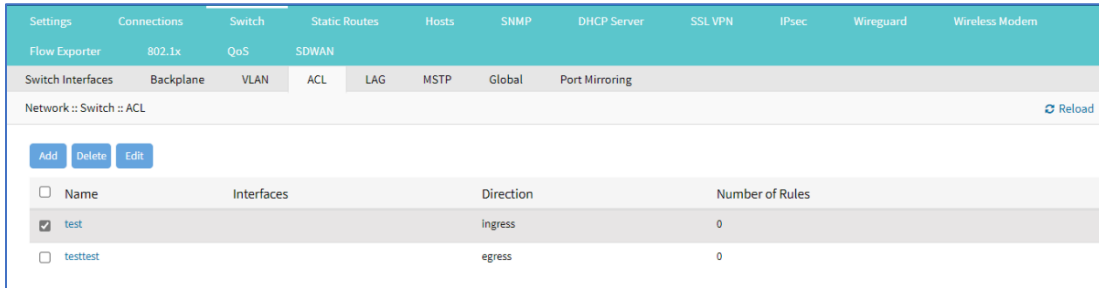
WebUI Procedure

1. Go to *Network :: Switch :: VLAN*.

2. Select checkbox next to item to delete.
3. Click **Delete**.
4. On the confirmation pop-up dialog, click **OK**.

ACL sub-tab

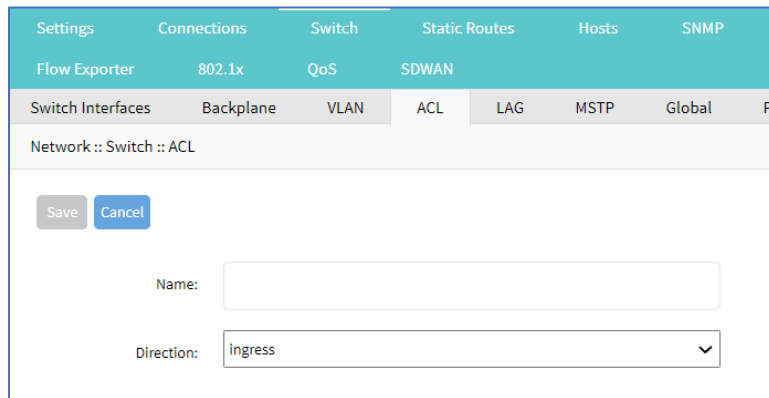
With the ACL (access control list) option, custom ACL rules can be managed (add, delete, edit) for each interface.



Add ACL

WebUI Procedure

1. Go to *Network :: Switch :: ACL*.
2. Click **Add** (displays dialog).



3. Enter **Name**.
4. On **Direction** drop-down, select one (**ingress**, **egress**).
5. Click **Save**.

Edit ACL

WebUI Procedure

1. Go to *Network :: Switch :: ACL*.
2. Select checkbox next to item to edit.
3. Click **Edit** (displays dialog).

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

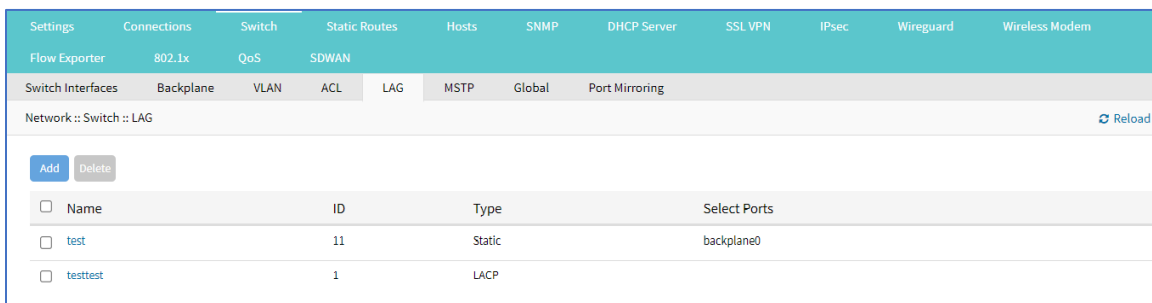
Delete ACL

WebUI Procedure

1. Go to *Network :: Switch :: ACL*.
2. Select checkbox next to item to delete.
3. Click **Delete**.
4. On the confirmation pop-up dialog, click **OK**.

LAG sub-tab

Link aggregation allows 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.

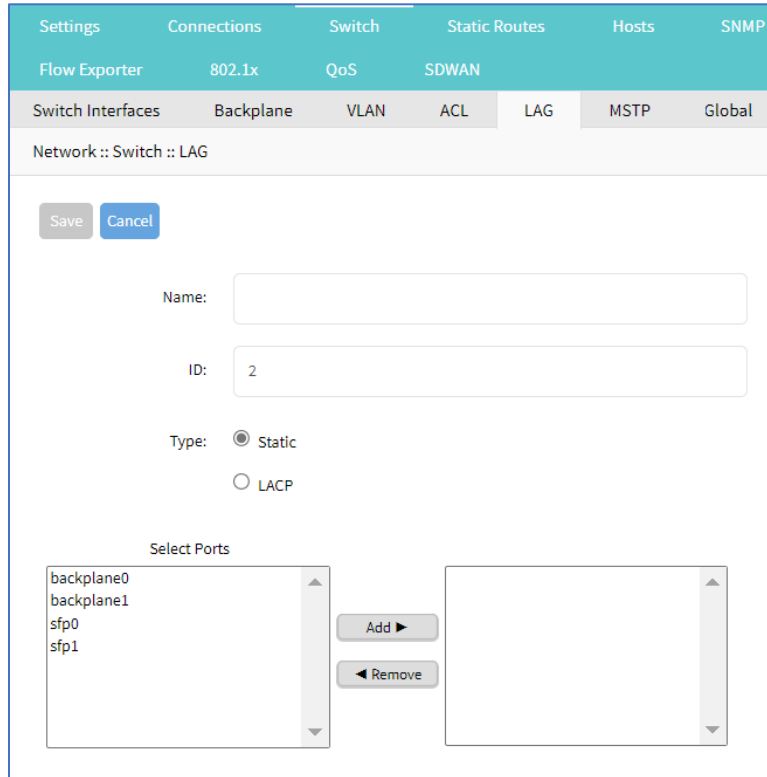


Settings				
Flow Exporter	802.1x	QoS	SDWAN	
Switch				
Switch Interfaces	Backplane	VLAN	ACL	LAG
MSTP				Global
Port Mirroring				
Network :: Switch :: LAG Reload				
Add Delete				
<input type="checkbox"/>	Name	ID	Type	Select Ports
<input type="checkbox"/>	test	11	Static	backplane0
<input type="checkbox"/>	testtest	1	LACP	

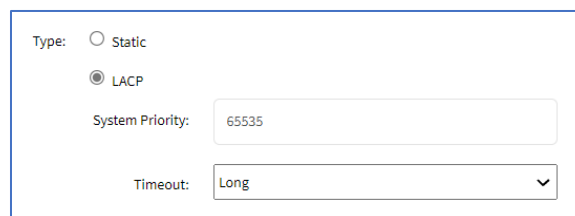
Add LAG

WebUI Procedure

1. Go to *Network :: Switch :: LAG*.
2. Click **Add** (displays dialog).



3. Enter **Name**.
4. Enter **ID**.
5. On *Type* menu, select one:
 - Static** radio button.
 - LACP** radio button (displays dialog).



Enter **System Priority**.

On **Timeout** drop-down, select one (**Long**, **Short**).

6. In *Select Ports*, select from left-side panel, click **Add** to move to right-side panel.
To remove from right-side panel, select and click **Remove**.
7. Click **Save**.

Edit LAG

WebUI Procedure

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**.

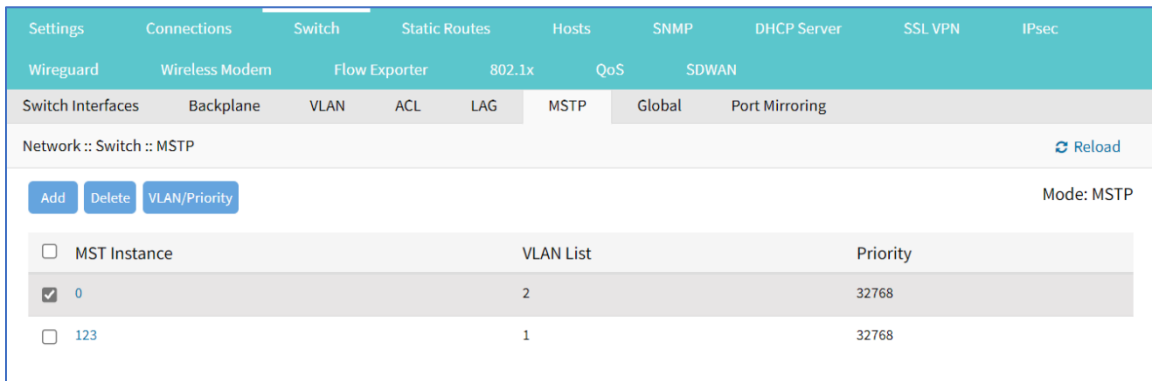
Delete LAG

WebUI Procedure

1. Go to *Network :: Switch :: LAG*.
2. Select checkbox next to item to delete.
3. Click **Delete**.
4. On the confirmation pop-up dialog, click **OK**.

MSTP sub-tab

MSTP (Multiple Spanning Tree Protocol) provides connectivity (simple and full) assigned to any VLAN throughout a Bridged Local Area Network. Bridge Protocol Data Units (BPDU) exchange information between spanning-tree compatible devices. This prevents loops in each Multiple Spanning Tree Instances (MSTI) and the Common and Internal Spanning Tree (CIST) configuration. Active and blocked paths are selected, without needing manually enabled backup links, and gets rid of bridge loop problems.



MST Instance	VLAN List	Priority
<input checked="" type="checkbox"/> 0	2	32768
<input type="checkbox"/> 123	1	32768

Add MSTB

WebUI Procedure

1. Go to *Network :: Switch :: MSTB*.
2. Click Add (displays dialog).

3. Enter MST Instance ID.
4. Enter VLAN.
5. On **Priority** drop-down, select one (**0, 4096, 8192, 12288, 16384, 20480, 24594, 28672, 32768, 40960, 45056, 49152, 53248, 57344, 61440**).
6. Click **Save**.

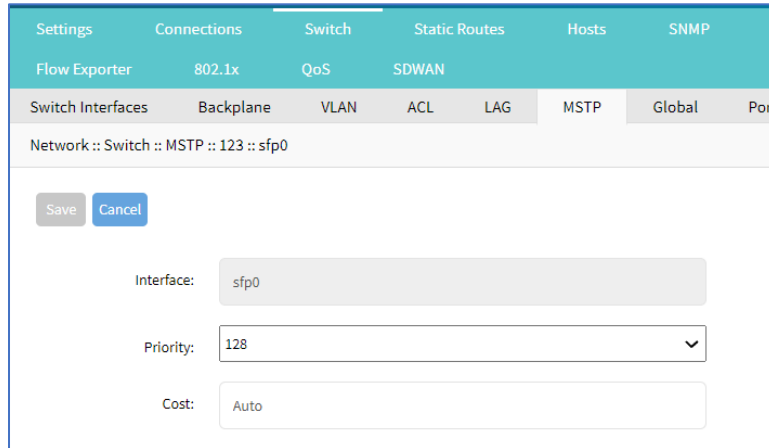
Edit MSTB

WebUI Procedure

1. Go to *Network :: Switch :: MSTB*.
2. In the *MST Interface* column, click on a name (displays dialog).

Interface	Priority	Cost
<input type="checkbox"/> sfp0	128	Auto
<input type="checkbox"/> sfp1	128	Auto

3. In *Interface* column, click a name (displays dialog).



4. As needed, make changes:

On **Priority** drop-down, select one (**0, 16, 32, ;48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240**).

Enter **Cost** (default: Auto).

5. Click **Save**.

Delete MSTB

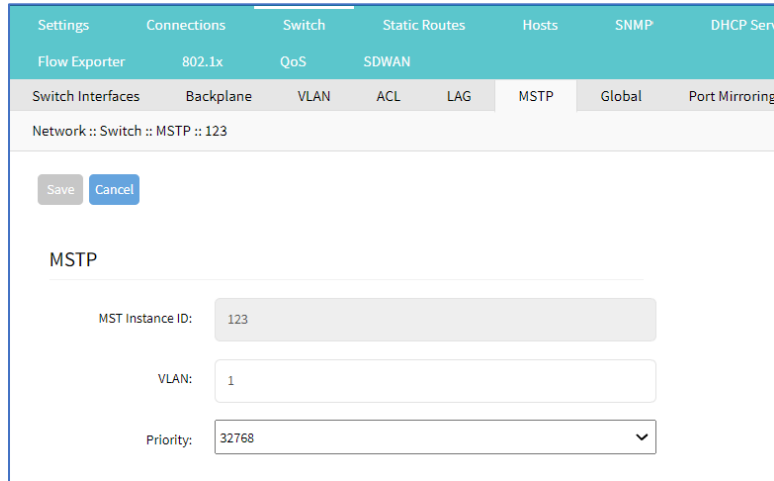
WebUI Procedure

1. Go to *Network :: Switch :: MSTB*.
2. In the *MST Interface* column, select checkbox.
3. Click **Delete**.
4. On confirmation pop-up dialog, click **OK**.

Set VLAN/Priority

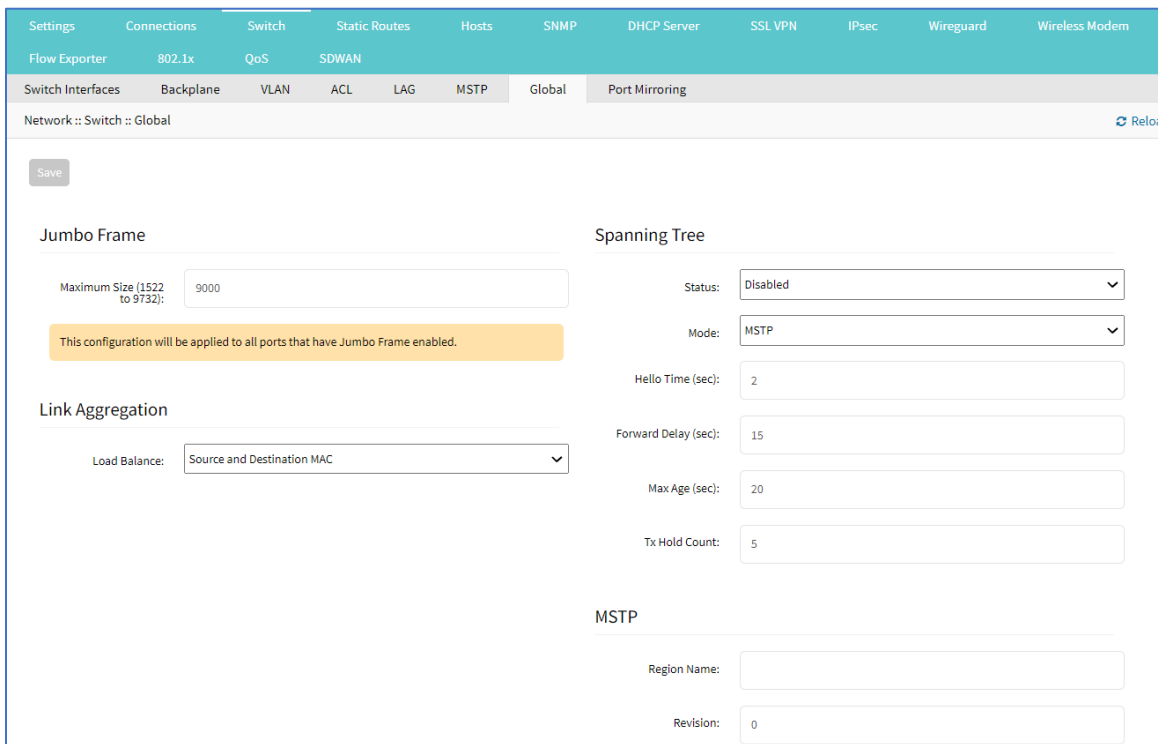
WebUI Procedure

1. Go to *Network :: Switch :: MSTB*.
2. In the *MST Interface* column, select checkbox.
3. Click **VLAN/Priority** (displays dialog).



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

Global sub-tab



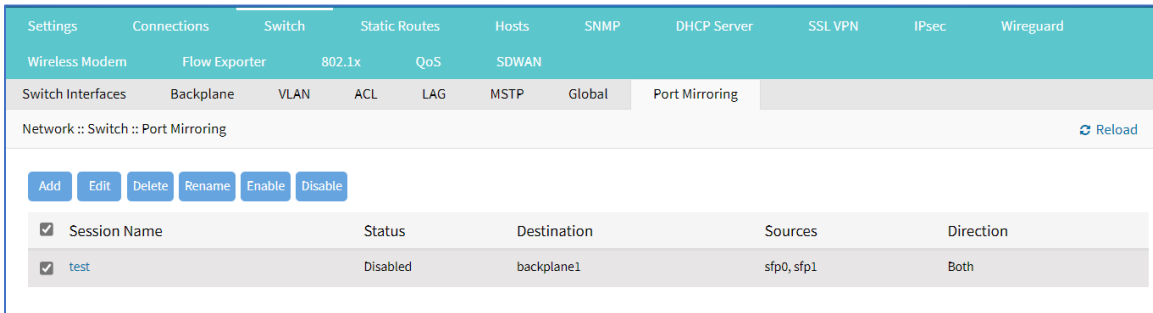
Edit Global Settings

WebUI Procedure

1. Go to *Network :: Switch :: Global*.
2. In *Jumbo Frame* menu:
Enter **Maximum Size (1522 to 9732)**.

3. In *Link Aggregation* menu:
 In **Load Balance** drop-down, select one (**Source and Destination IP, Source and Destination MAC, Source and Destination MAC and IP, Source and Destination MAC and IP and TCP/UDP Ports**).
4. In *Spanning Tree* menu:
 In **Status** drop-down, select one (**Enabled, Disabled**).
 In **Mode** drop-down, select one (**MSTP**).
 Enter **Hello Time (sec)**.
 Enter **Forward Delay (sec)**.
 Enter **Max Age (sec)**.
 Enter **Tx Hold Count**.
5. In *MTSP* menu:
 Enter Region Name.
 Enter Revision.
6. Click **Save**.

Port Mirroring sub-tab

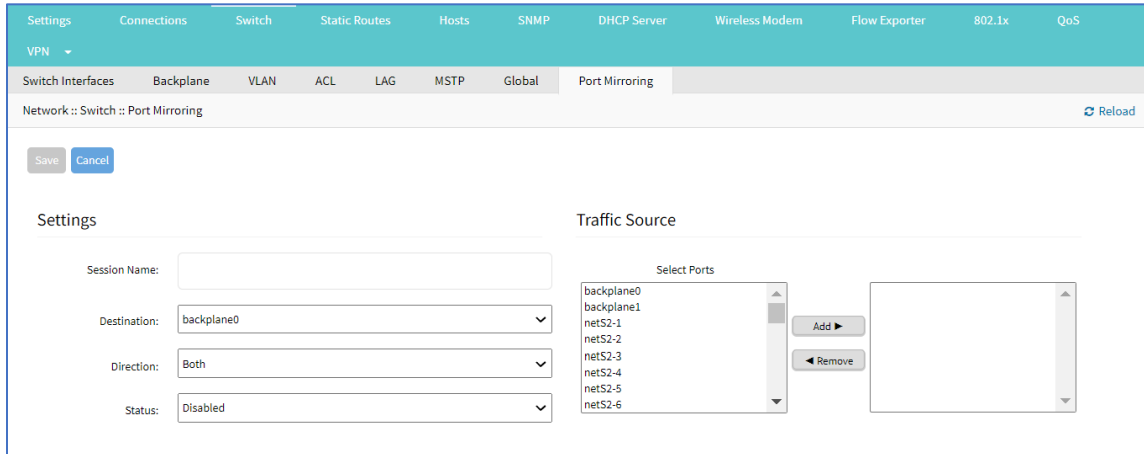


Session Name	Status	Destination	Sources	Direction
test	Disabled	backplane1	sfp0, sfp1	Both

Add Port Mirroring

WebUI Procedure

1. Go to *Network :: Switch :: Port Mirroring*.
2. Click **Add** (displays dialog).



3. In *Settings* menu:

Enter **Session Name**.

On **Destination** drop-down, select one (**backplane0**, **backplane1**, **netS2-(1-16)**, **netS3-(1-8)**, **netS4-(1-16)**, **sfp0**, **sfp1**, **slot1-0**, **slot1-1**).

On **Direction** drop-down, select one (**Both**, **Egress**, **Ingress**).

On **Status** drop-down, select one (**Disabled**, **Enabled**).

4. In *Traffic Source* menu:

On *Traffic Source*, 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

WebUI Procedure

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

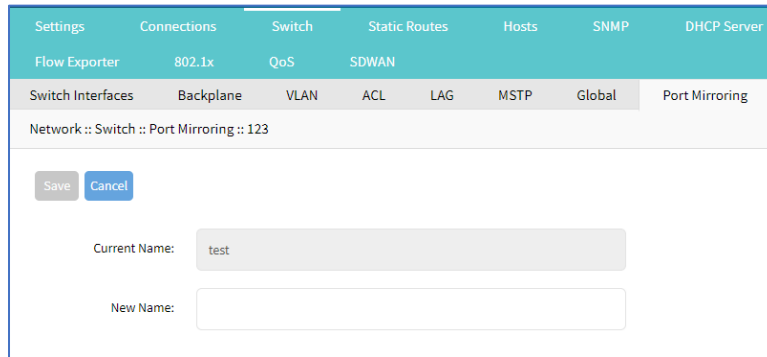
WebUI Procedure

1. Go to *Network :: Switch :: Port Mirroring*.
2. In *Session Name* column, select checkbox.
3. Click **Delete**.
4. On confirmation pop-up dialog, click **OK**.

Rename Port Mirroring

WebUI Procedure

1. Go to *Network :: Switch :: Port Mirroring*.
2. In *Session Name* column, select checkbox.
3. Click **Rename** (displays dialog).



4. Enter **New Name**.
5. Click **Save**.

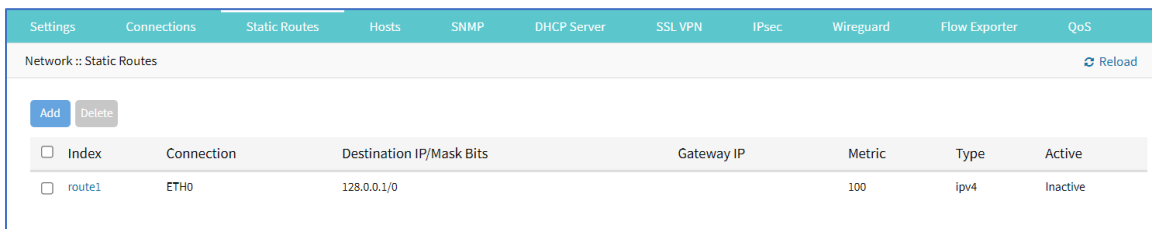
Enable/Disable Port Mirroring

WebUI Procedure

1. Go to *Network :: Switch :: Port Mirroring*.
2. In *Session Name* column, select checkbox.
3. Click **Enable**. (to enable port mirroring).
4. Click **Disable** (to disable port mirroring).

Static Routes tab

Administrators can define and manage static routes. Routes can be created for IPv4 and IPv6, assigned to specific network interfaces.



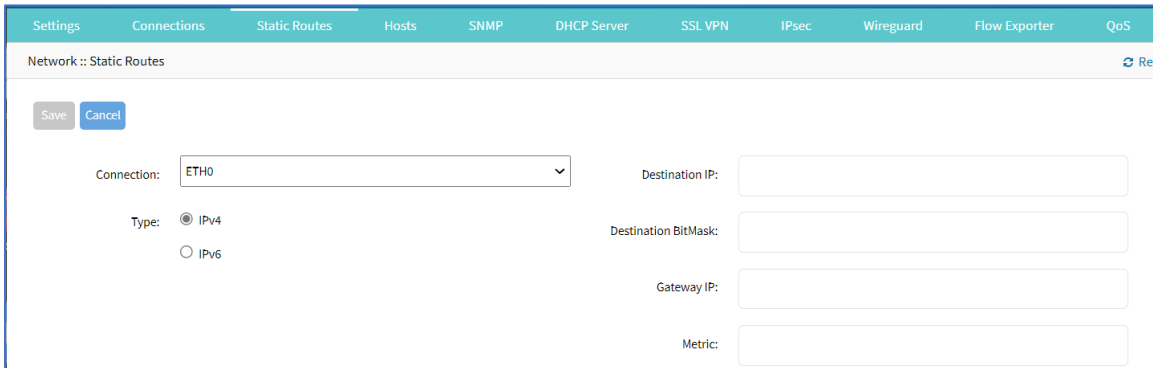
Index	Connection	Destination IP/Mask Bits	Gateway IP	Metric	Type	Active
<input type="checkbox"/> route1	ETH0	128.0.0.1/0	128.0.0.1/0	100	ipv4	Inactive

Manage Static Routes

Add Static Route

WebUI Procedure

1. Go to *Network :: Static Routes*.
2. Click **Add** (displays dialog).



3. On **Connection** drop-down, select one (**ETH0, ETH1, hotspot**).
4. In *Type* menu, select one:
 - IPv4** radio button.
 - IPv6** radio button.
5. Enter **Destination IP**.
6. Enter **Destination BitMask**.
7. Enter **Gateway IP**.
8. Enter **Metric** (routing metric value – for normal routes default = 100)
9. Click **Save**.

Edit Static Route

WebUI Procedure

1. Go to *Network :: Static Routes*.
2. In the *Index* column, click on the name.
3. On the dialog, make changes as needed.
4. Click **Save**.

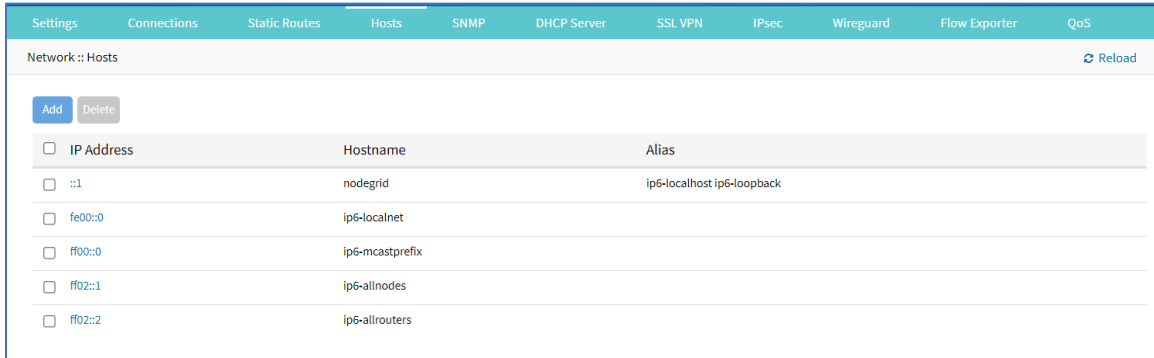
Delete Static Route

WebUI Procedure

1. Go to *Network :: Static Routes*.
2. In the list, select a checkbox.
3. Click **Delete**.

Hosts tab

Administrators can configure and manage manual hostname definitions (equivalent to entries in the host's file).



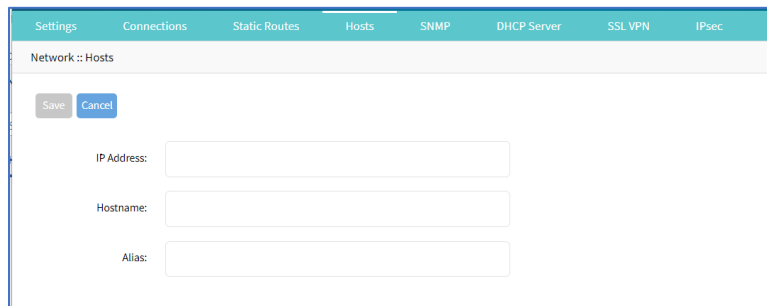
IP Address	Hostname	Alias
<input type="checkbox"/> ::1	nodegrid	ip6-localhost ip6-loopback
<input type="checkbox"/> fe00::0	ip6-localnet	
<input type="checkbox"/> ff00::0	ip6-mcastprefix	
<input type="checkbox"/> ff02::1	ip6-allnodes	
<input type="checkbox"/> ff02::2	ip6-allrouters	

Manage Hosts

Add Host

WebUI Procedure

1. Go to *Network :: Hosts*.
2. Click **Add** (displays dialog).



3. Enter **IP Address** (IPv4, IPv6 formats supported.)
4. Enter **Hostname**.
5. Enter **Alias**.
6. Click **Save**.

Edit Host

WebUI Procedure

1. Go to *Network :: Hosts*.
2. In the *Index* column, click on the name.
3. On the dialog, make changes as needed.
4. Click **Save**.

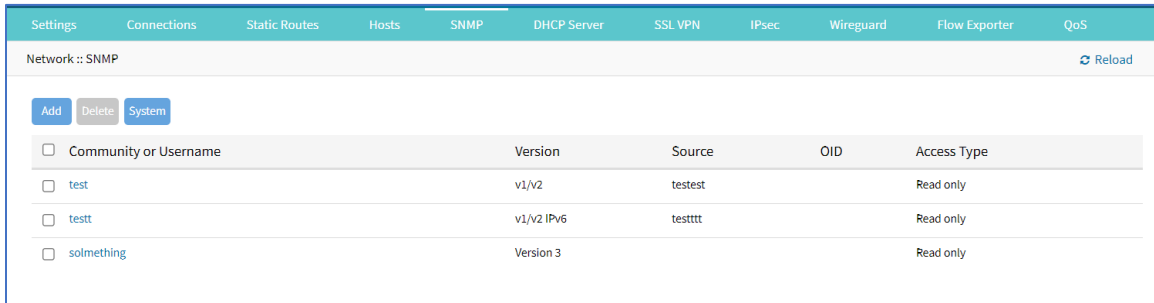
Delete Host

WebUI Procedure

1. Go to *Network :: Hosts*.
2. In the list, select a checkbox.
3. Click **Delete**.

SNMP tab

Administrators can configure SNMP settings here.



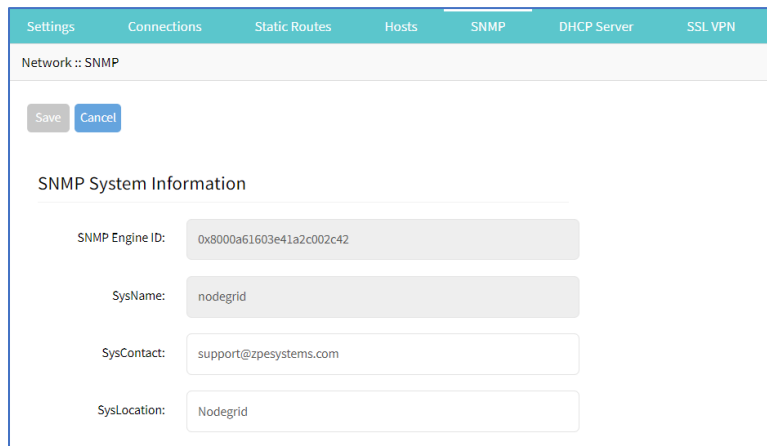
<input type="checkbox"/> Community or Username	Version	Source	OID	Access Type
<input type="checkbox"/> test	v1/v2	testest		Read only
<input type="checkbox"/> testt	v1/v2 IPv6	testttt		Read only
<input type="checkbox"/> solomething	Version 3			Read only

Manage SNMP

Review/edit System Information

WebUI Procedure

1. Go to *Network :: SNMP*.
2. Click **System**.



SNMP System Information

SNMP Engine ID: 0x8000a61603e41a2c002c42

SysName: nodegrid

SysContact: support@zpesystems.com

SysLocation: Nodegrid

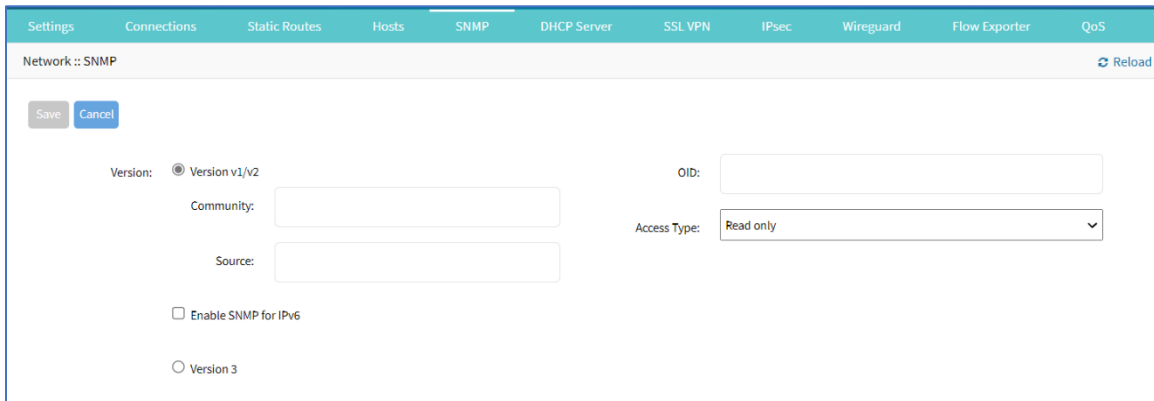
3. Two fields can be edited:
 - SysContact** (email address)
 - SysLocation** (location name)
4. If changed, click **Save**.

5. If not, click **Cancel** to return to table.

Add Community/Username

WebUI Procedure

1. Go to *Network :: SNMP*.
2. Click **Add** (displays dialog).



3. In *Version* menu (select one):

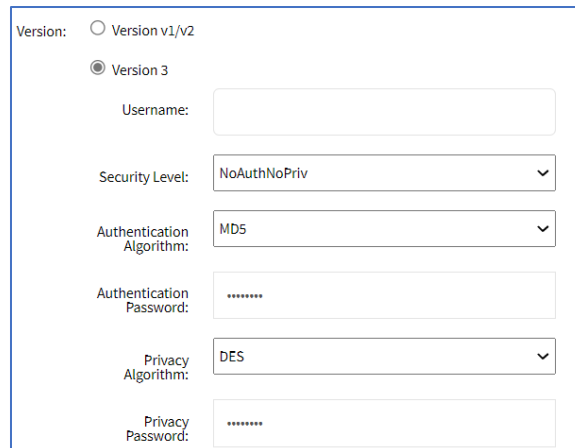
Version V1/V2 radio button

Enter **Community**.

Enter **Source**.

(if applicable) Select **Enable SNMP for IPv6** checkbox

Version 3 radio button



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. Enter **OID**.
5. On **Access Type** drop-down, select one (**Read and Write, Read Only**).
6. Click **Save**.

Edit Community/Username

WebUI Procedure

1. Go to *Network :: SNMP*.
2. On *Community or Username* column, click a name.
3. Make changes, as needed.
4. Click **Save**.

Delete Community/Username

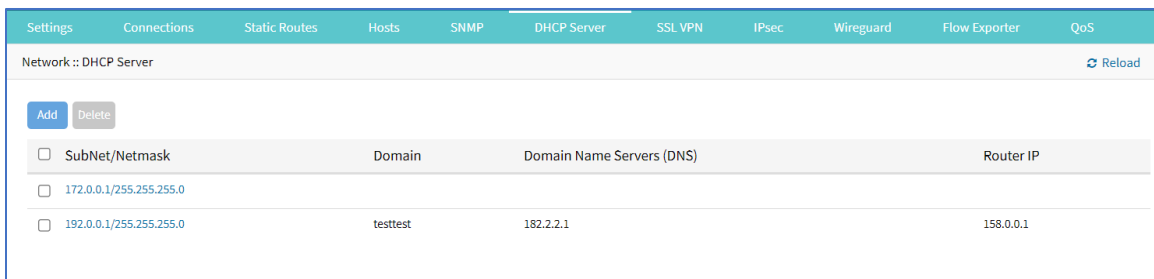
WebUI Procedure

1. Go to *Network :: SNMP*.
2. Select checkbox to be deleted.
3. Click **Delete**.

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. Then, IP address ranges (Network Range) are defined to be used as server IP addresses and as IP address reservations for specific hosts.



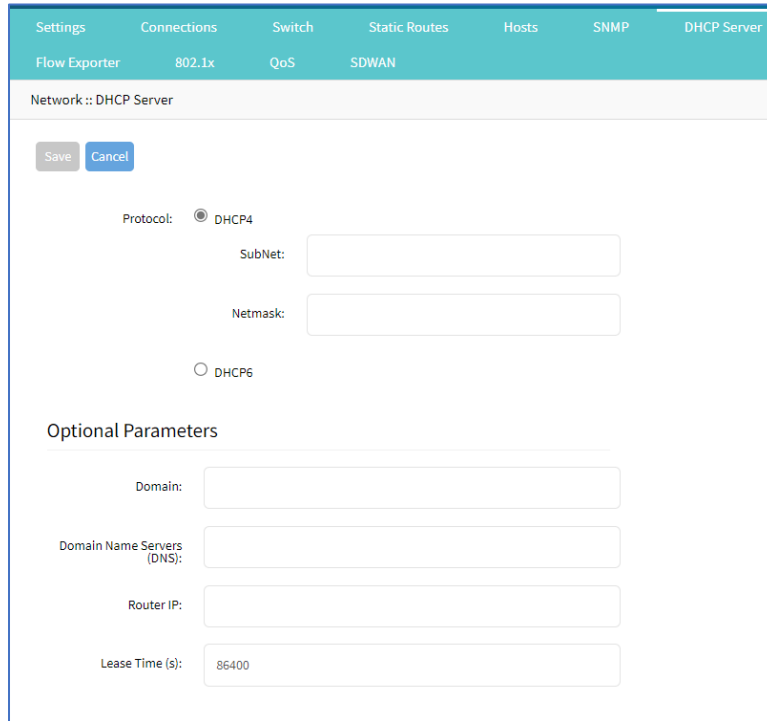
<input type="checkbox"/>	SubNet/Netmask	Domain	Domain Name Servers (DNS)	Router IP
<input type="checkbox"/>	172.0.0.1/255.255.255.0			
<input type="checkbox"/>	192.0.0.1/255.255.255.0	testtest	182.2.2.1	158.0.0.1

Manage DHCP Server

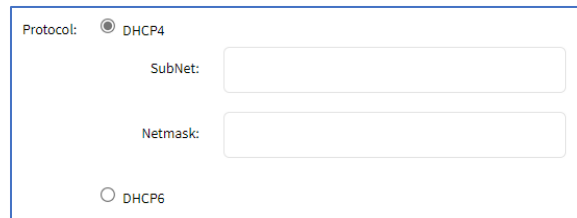
Add DHCP Server

WebUI Procedure

1. Go to *Network :: DHCP Server*
2. Click **Add** (displays dialog)



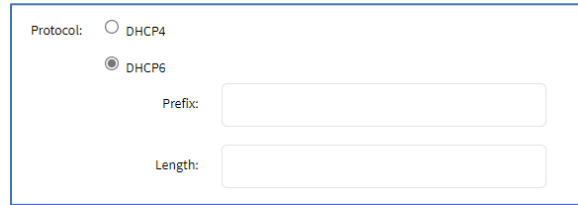
3. On *Protocol* menu, select one:
DHCP4 radio button



Enter **Subnet** (must match the settings of a configured interface)

Enter **Netmask** (defined subnet – format: xxx.xxx.xxx.xxx)

DHCP6 radio button



The screenshot shows a configuration form for DHCP6. It includes a 'Protocol' section with two radio buttons: 'DHCP4' (unselected) and 'DHCP6' (selected). Below this are two input fields: 'Prefix' and 'Length', both currently empty.

Enter **Prefix**

Enter **Length**

4. In *Optional Parameters* menu:

Enter **Domain**

Enter **Domain Name Services (DNS)**

Enter **Router IP** (DHCP4 only)

Enter **Lease Time (s)** (default: 86400)

5. Click **Save**

Edit DHCP Server

WebUI Procedure

1. Go to *Network :: DHCP Server*.
2. On *Subnet/Netmask* column, click a name.
3. Make changes, as needed.
4. Click **Save**.

Delete DHCP Server

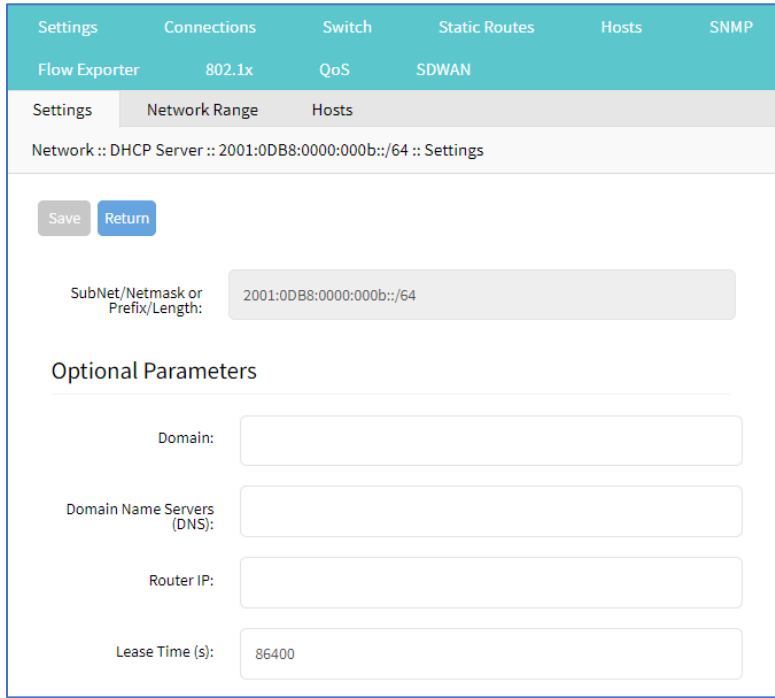
WebUI Procedure

1. Go to *Network :: DHCP Server*.
2. Select checkbox to be deleted.
3. Click **Delete** (displays confirmation dialog).
4. Click **OK**.

Edit DHCP Server Settings, IP Range, and Hosts

WebUI Procedure

1. Go to *Network :: DHCP Server*.
2. In the *Subnet/Netmask* column, click name (displays dialog).



Settings Connections Switch Static Routes Hosts SNMP
Flow Exporter 802.1x QoS SDWAN

Settings Network Range Hosts

Network :: DHCP Server :: 2001:0DB8:0000:000b::/64 :: Settings

Save Return

SubNet/Netmask or Prefix/Length: 2001:0DB8:0000:000b::/64

Optional Parameters

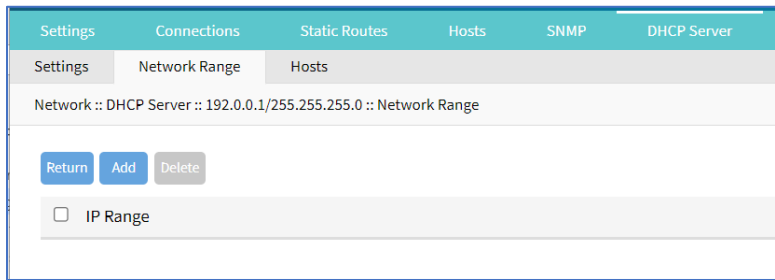
Domain:

Domain Name Servers (DNS):

Router IP:

Lease Time (s): 86400

3. On **Settings** sub-tab, review details. Make changes, as needed.
4. Click on **Network Range** sub-tab (displays dialog).



Settings Connections Static Routes Hosts SNMP DHCP Server

Settings Network Range Hosts

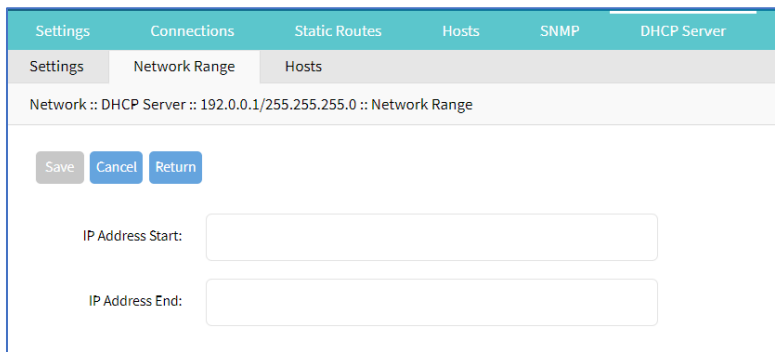
Network :: DHCP Server :: 192.0.0.1/255.255.255.0 :: Network Range

Return Add Delete

IP Range

To add IP Range:

Click **Add** (displays dialog).



Settings Connections Static Routes Hosts SNMP DHCP Server

Settings Network Range Hosts

Network :: DHCP Server :: 192.0.0.1/255.255.255.0 :: Network Range

Save Cancel Return

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**.

To edit IP Range

In column, click on *IP Range* name.

Make changes, as needed.

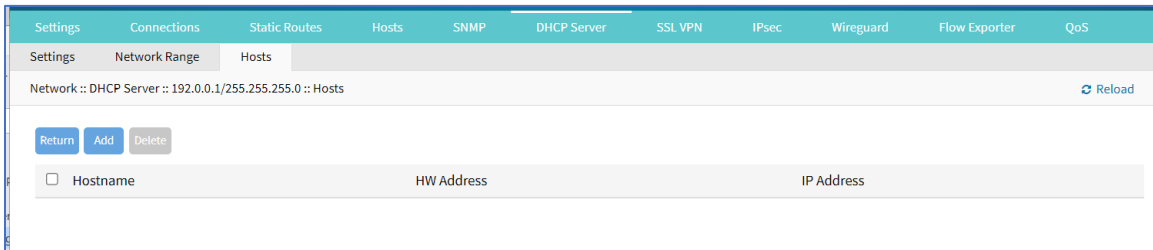
Click **Save**.

To delete IP Range

Select checkbox next to name.

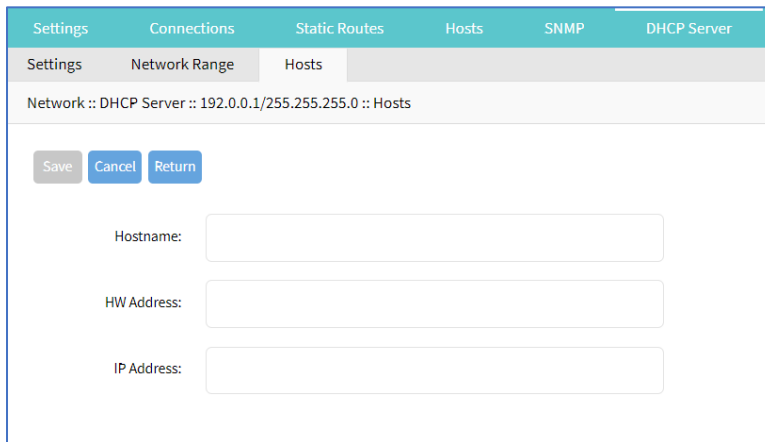
Click **Delete**.

5. Click on **Hosts** sub-tab (displays dialog)



To add a host:

Click **Add** (opens dialog)



Enter **Hostname**

Enter **HW Address**. (MAC address to which an IP address reservation applies).

Enter **IP Address** (IP address assigned to specific host matching the MAC address).

Click **Save**.

To edit host:

In *Host* column, click on name.

Make changes, as needed.

Click **Save**.

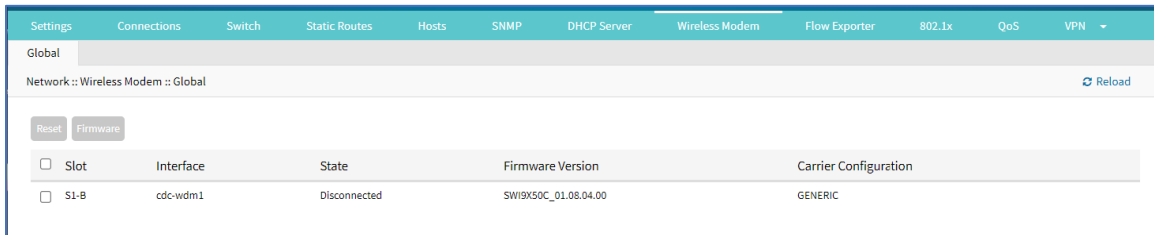
To delete host:

In Host column, select checkbox.

Click **Delete**.

Wireless Modem tab

This provides details on the Wireless Modem (if installed).



Slot	Interface	State	Firmware Version	Carrier Configuration
<input type="checkbox"/> S1-B	cdc-wdm1	Disconnected	SW19X50C_01.08.04.00	GENERIC

Manage Wireless Modem

Reset Wireless Model

WebUI Procedure

1. Go to *Network :: Wireless Modem*.
2. Select checkbox next to *Slot* name.
3. Click **Reset**.

Manage Wireless Modem Firmware

WebUI Procedure

1. Go to *Network :: Wireless Modem*.
2. Select checkbox next to *Slot* name.
3. Click **Firmware** (displays dialog).

Build ID	Type	Unique ID
<input type="checkbox"/> 01.08.04.00	Firmware Image	
<input type="checkbox"/> 01.07.02.00	Firmware Image	
<input type="checkbox"/> 01.09.04.00	Firmware Image	
<input type="checkbox"/> 01.07.02.00_ATT	Carrier Configuration	002.008_004
<input type="checkbox"/> 01.09.04.00_DOCOMO	Carrier Configuration	002.015_000
<input type="checkbox"/> 01.08.04.00_GENERIC	Carrier Configuration	002.012_000
<input type="checkbox"/> 01.08.04.00_SIERRA	Carrier Configuration	002.001_000
<input type="checkbox"/> 01.09.04.00_SOFTBANK	Carrier Configuration	002.017_000
<input type="checkbox"/> 01.08.04.00_SPRINT	Carrier Configuration	000.001_001
<input type="checkbox"/> 01.07.02.00_TELUS	Carrier Configuration	001.000_000
<input type="checkbox"/> 01.08.04.00_VERIZON	Carrier Configuration	002.015_001

4. To delete firmware:

Select checkbox next to *Build ID*.

Click **Delete**.

5. To upgrade firmware.

Select checkbox next to *Build ID*.

Click **Upgrade** (displays dialog).

Global

Network :: Wireless Modem :: Global :: S1-B

File Location: Local System

Filename:

File must be previously copied to '/var/sw' directory.

Local Computer

Remote Server

In *File Location* menu, select one:

Local System radio button. On **Filename** drop-down, select file.

Select **Local Computer** radio button:

Click **Choose File**. Locate and select the file.

File Location: Local System

Local Computer

Filename: No file chosen

Select **Remote Server** radio button:

File Location:

Local System

Local Computer

Remote Server

URL:

Username:

Password:

The path in url to be used as absolute path name

Enter **URL**.

Enter **Username**.

Enter **Password**.

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

6. Click **Upgrade**.

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	Interfaces	Aggregation Fields	
<input type="checkbox"/> Flow2	Error	192.168.56.2:2055	1/12	eth0,eth1	dst_host,dst_port,proto,src_host,src_mac,src_mask,src_port,tos	
<input type="checkbox"/> Flow3	Disabled	192.168.56.3:2055	1/1	eth0	dst_host,dst_port,proto,src_host,src_port,tos	
<input type="checkbox"/> MyFlow	Running	127.0.0.1:2055	1/1	eth0	dst_host,dst_port,proto,src_host,src_port,tos	

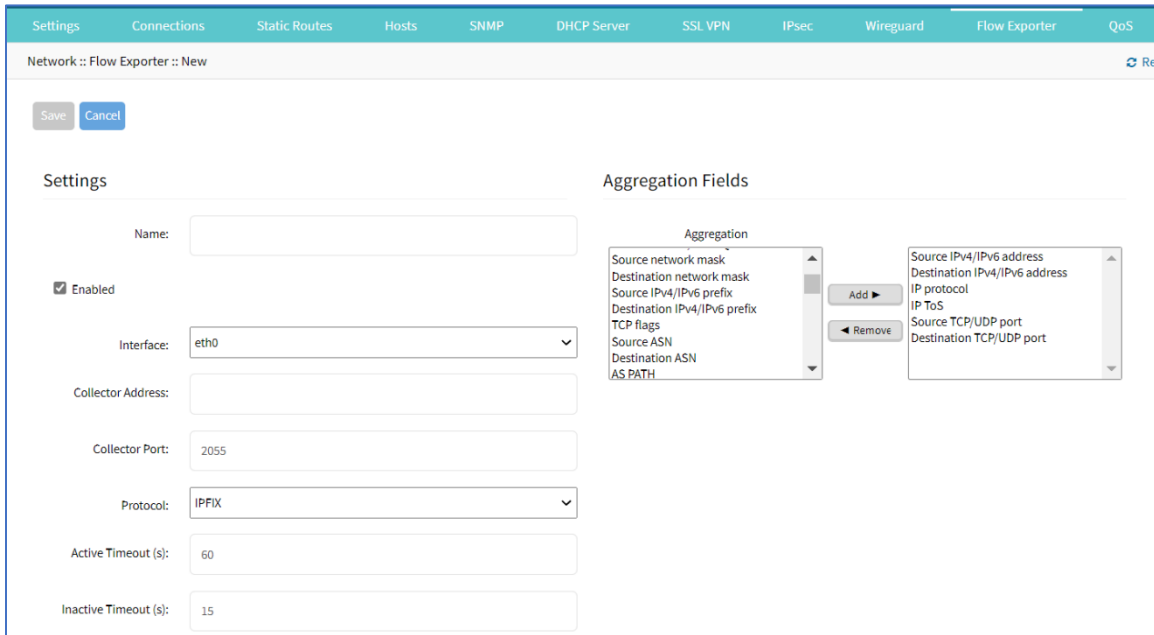
Flow Exporter Main Table

Column names	Description
Name	Name of the flow.
Status	Status of the flow (Running, Disabled, Error).
Collector	IP address and port.
Sampling rate	Sampling ratio.
Interfaces	Interfaces used.
Aggregation Fields	Aggregation fields that have been added.

Add a new Flow Export

WebUI Procedure

1. Go to *Network :: Flow Exporter*.
2. Click **Add** (displays dialog).



3. In *Settings* menu:

Enter **Name**.

Select **Enabled** checkbox.

On **Interface** drop-down, select one (**eth0, eth1**).

Enter **Collector Address**.

Enter **Collector Port**.

On **Protocol** drop-down, select one (**IPFIX, NetFlow v9, NetFlow v5**).

Enter **Active Timeouts (s)** in seconds.

Enter **Inactive Timeout (s)** in seconds.

Enter **Sampling Rate (1 out of N)**.

4. In *Aggregation Fields* menu:

To add an item to the *Aggregation*:

Select item on left-side panel.

Click **Add ►** (item is moved).

To remove an item from the *Aggregation*:

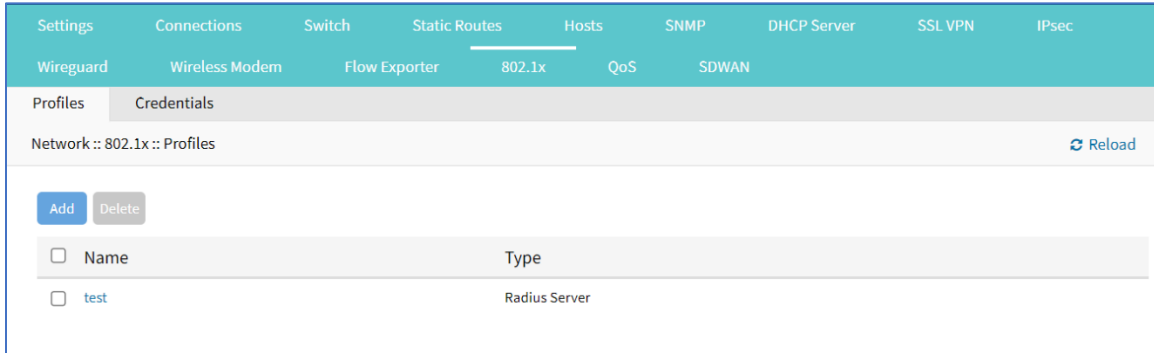
Select item on right-side panel.

Click **◀ Remove** (item is moved).

5. Click **Save**.

802.1x tab (SR only)

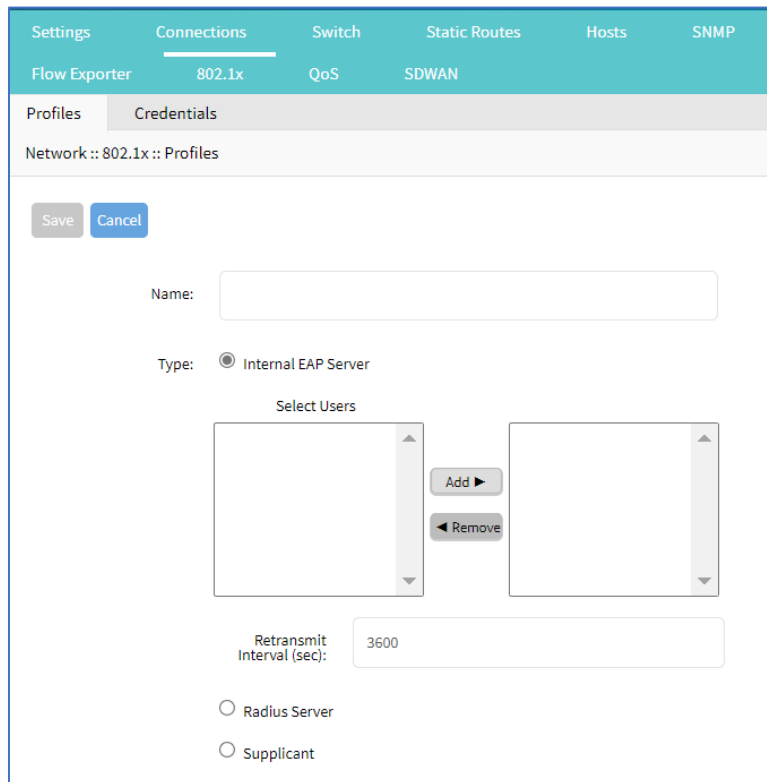
These functions are only available on Nodegrid Gate SR, Bold SR, Link SR, Net SR, and Hive SR devices.



Profiles sub-tab

Add Profile

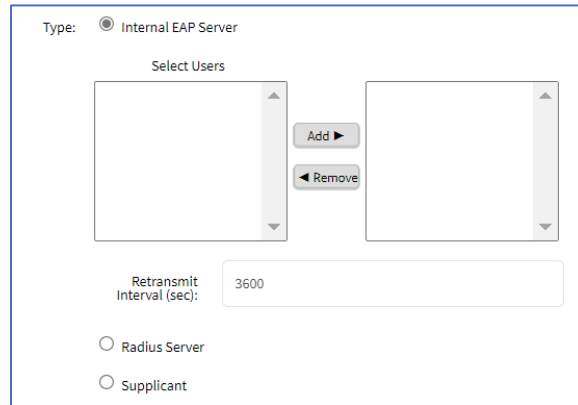
1. Go to *Network :: 802.1x :: Profile*.
2. Click **Add** (displays dialog).



3. Enter **Name**.

4. On *Type* menu, select one:

Internal EAP Server radio button (expands dialog).



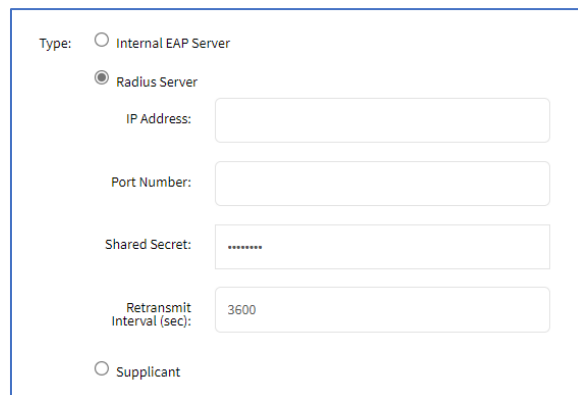
In *Select Users*:

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).



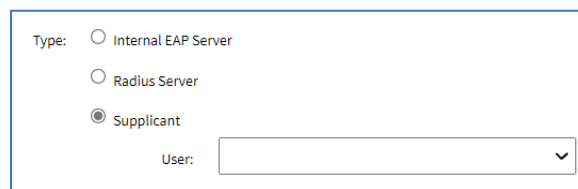
Enter **IP Address**.

Enter **Port Number**.

Enter **Shared Secret**.

Enter **Retransmit Interval (sec)**.

Supplicant radio button (expands dialog). On **User** drop-down, select one.



5. Click **Save**.

Edit a Profile

WebUI Procedure

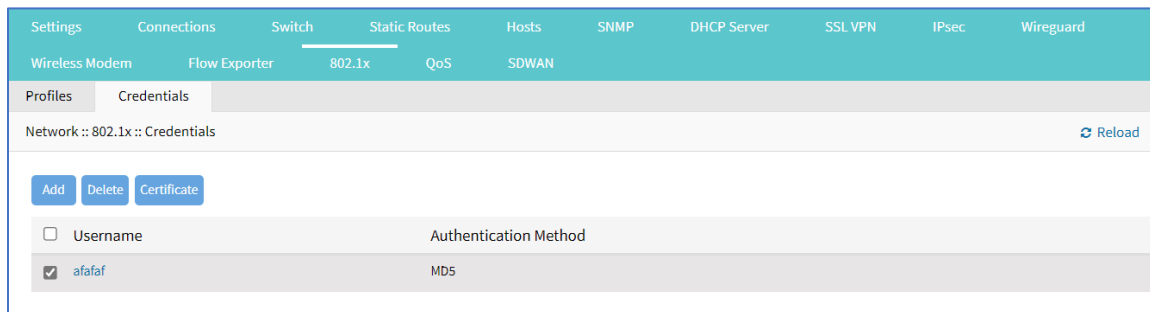
1. Go to *Network :: 802.1x :: Profile*.
2. In the *Name* column, click on a name (opens dialog).
3. Make changes, as needed.
4. Click **Save**.

Delete an Interface

WebUI Procedure

1. Go to *Network :: 802.1x :: Profile*.
2. Select checkbox to be deleted.
3. Click **Delete**.
4. On confirmation pop-up dialog, click **OK**.

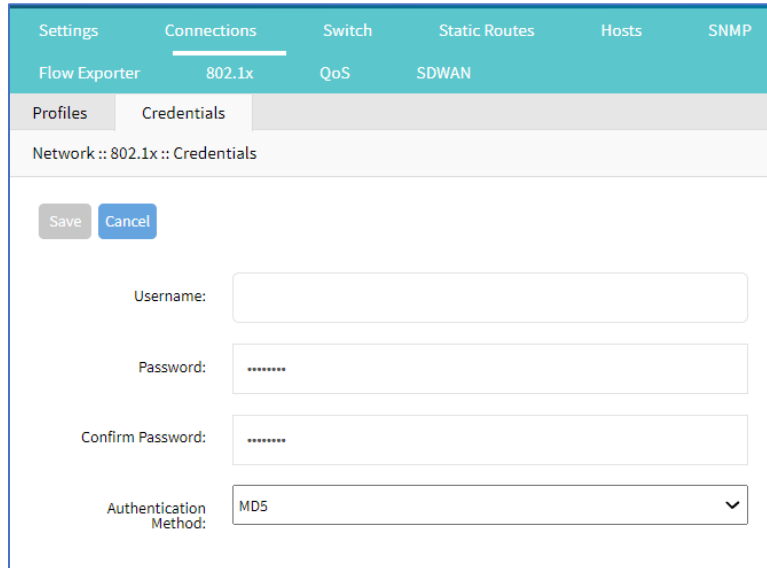
Credentials sub-tab



Add Credential

WebUI Procedure

1. Go to *Network :: 802.1x :: Credentials*.
2. Click **Add** (displays dialog).



3. Enter **Username**.
4. Enter **Password** and **Confirm Password**.
5. On **Authentication** drop-down, select one (**MD5, TLS, PEAP, TTLS**).
6. Click **Save**.

Edit Credential

WebUI Procedure

7. Go to *Network :: 802.1x :: Credentials*.
8. In *Username* column, click on name (opens dialog).
9. Make changes, as needed.
10. Click **Save**.

Delete Credential

WebUI Procedure

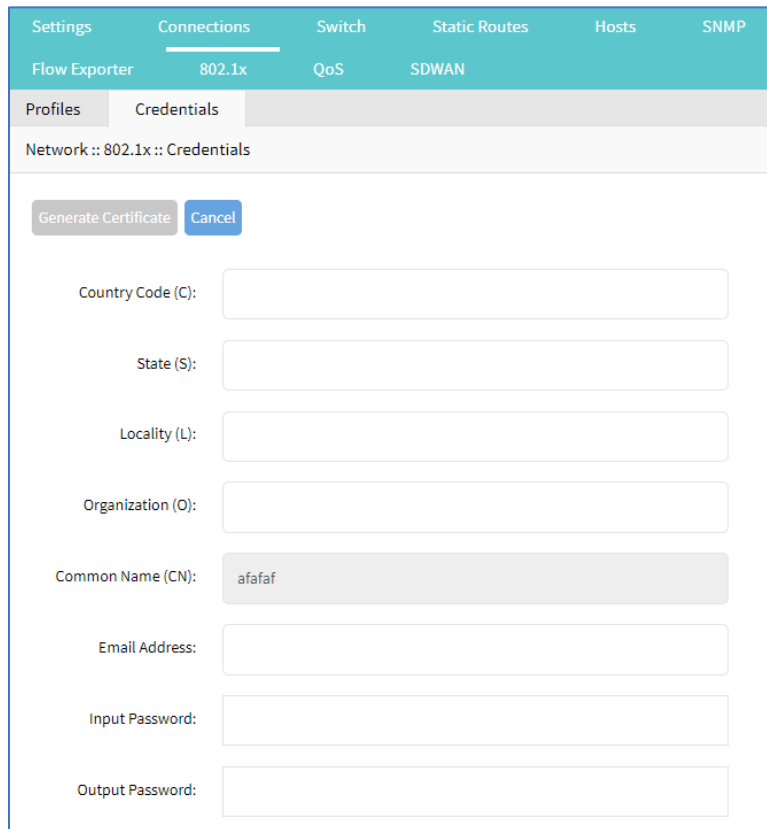
1. Go to *Network :: 802.1x :: Credentials*.
2. Select checkbox.
3. Click **Delete**.
4. On confirmation pop-up dialog, click **OK**.

Include Certificate

WebUI Procedure

1. Go to *Network :: 802.1x :: Credentials*.
2. Select checkbox.

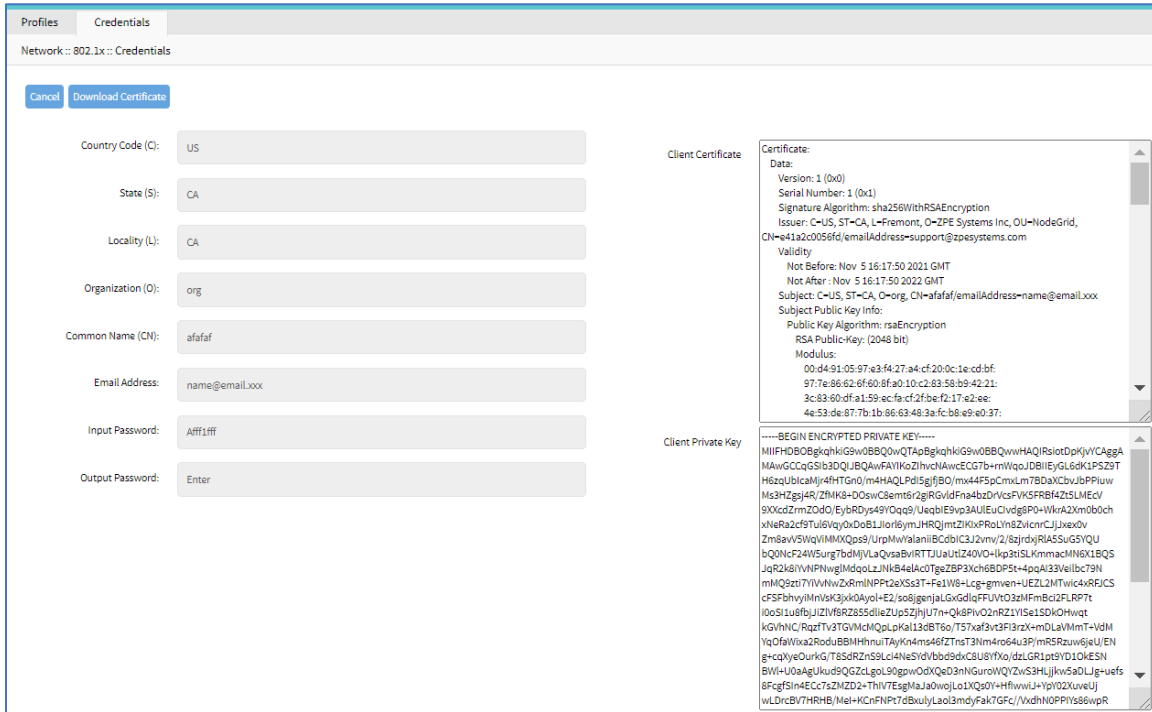
3. Click **Certificate** (displays dialog). User must have TLS authentication.



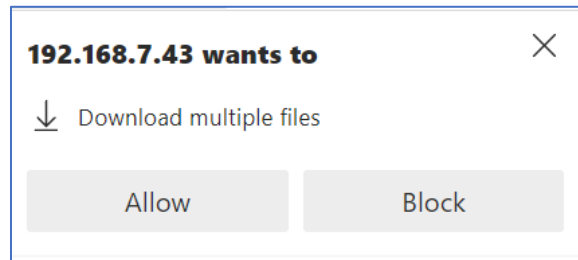
The screenshot shows a web interface with a teal header. The main navigation bar includes 'Settings', 'Connections', 'Switch', 'Static Routes', 'Hosts', and 'SNMP'. Under 'Connections', '802.1x' is selected, with sub-options 'Flow Exporter', 'QoS', and 'SDWAN'. Below this, 'Profiles' and 'Credentials' are visible, with 'Network :: 802.1x :: Credentials' as the current view. A dialog box titled 'Generate Certificate' is open, featuring a 'Generate Certificate' button and a 'Cancel' button. The dialog contains the following fields:

- Country Code (C):
- State (S):
- Locality (L):
- Organization (O):
- Common Name (CN):
- Email Address:
- Input Password:
- Output Password:

4. Enter the following details:
 - Country Code (C).**
 - State (S).**
 - Locality (L).**
 - Organization (O).**
 - Email Address.**
 - Input Password.**
 - Output Password.**
5. Click **Generate Certificate** (displays dialog).



6. Click **Download Certificate**.
7. On pop-up dialog, click **Allow**.



8. Certificate is saved to the local download location.

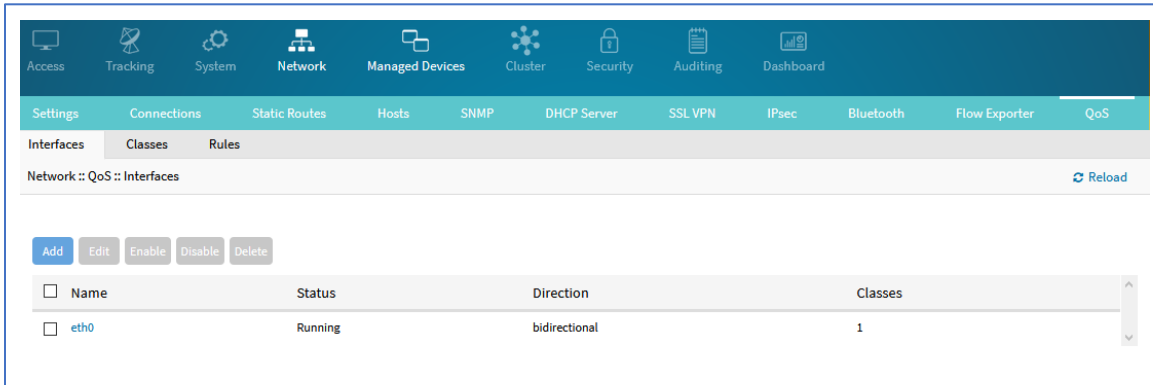
QoS tab

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 Add, Edit, Delete, and Enable/Disable QoS on each available interface. The main table displays information regarding the Name, Status, Direction, and Classes for each interface.

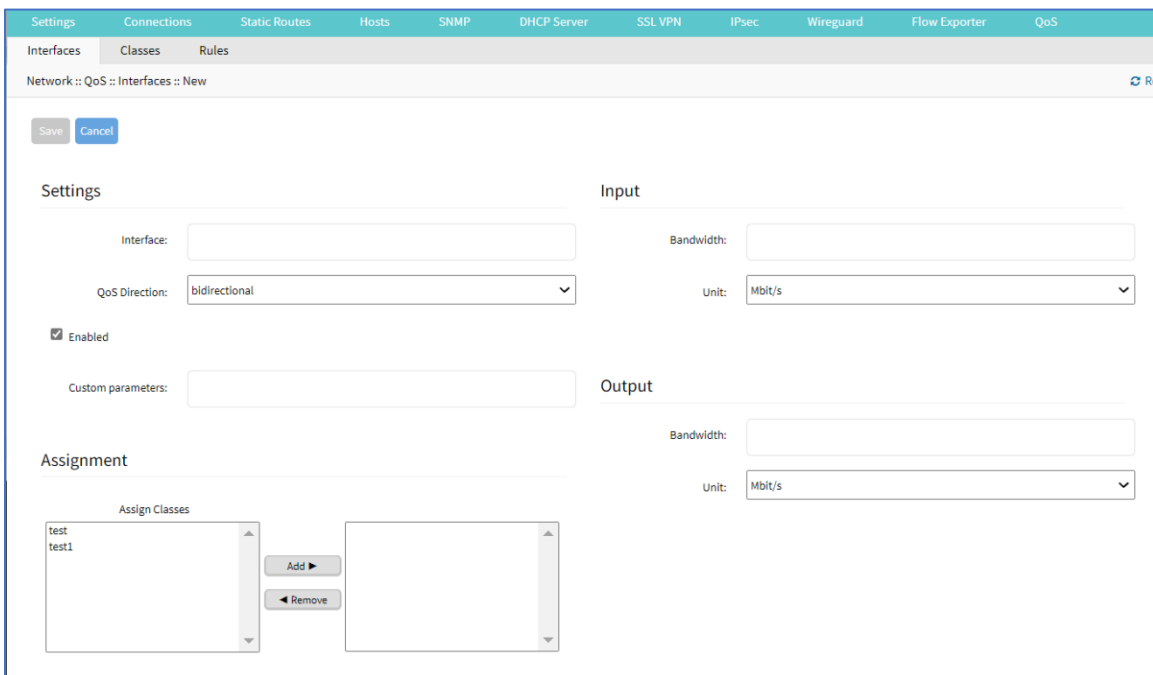
NOTE: Status can be Disabled, Running, or Error



Add an Interface

WebUI Procedure

1. Go to *Network :: QoS :: Interfaces*.
2. Click **Add** (displays dialog).



3. In *Settings* menu:
 - Enter **Interface** (must match existing interface name).
 - On **QoS Direction** drop-down, select one (**Input**, **Output**, **Bidirectional**).
 - Select **Enabled** checkbox.
4. Enter **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 an Interface

WebUI Procedure

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 an Interface

WebUI Procedure

1. Go to *Network :: QoS :: Interfaces*.
2. Select checkbox to be deleted.
3. Click **Delete**.
4. On confirmation pop-up dialog, click **OK**.

Enable/Disable an Interface

WebUI Procedure

1. Go to *Network :: QoS :: Interfaces*.
2. Select checkbox to be enabled/disabled.
3. Click **Enable** (to enable interface).
4. Click **Disable** (to disable interface).

Classes sub-tab

Classed management includes: Add, Edit, Delete, and Enable/Disable QoS classes. The main table displays information regarding Name, Enabled (yes/no), Priority, Input Reserved, Input Max, Output Reserved, and Output Max.

<input type="checkbox"/>	Name	Enabled	Priority	Input Reserved	Input Max	Output Reserved	Output Max
<input type="checkbox"/>	SSH	yes	0		50%		50%
<input type="checkbox"/>	WebUI	no	6	10%	100MB/s		

Add a Class

WebUI Procedure

1. Go to *Network :: QoS :: Classes*.
2. Click **Add** (displays dialog).

The dialog box is titled "Network :: QoS :: Classes :: New" and contains the following sections:

- Settings:**
 - Name:
 - Enabled
 - Priority:
 - Custom parameters:
- Input:**
 - Reserved Bandwidth:
 - Unit: %
 - Max Bandwidth:
 - Unit: %
- Assignment:**
 - Assign Rules:**
 - test11, test2
 - Add / Remove buttons
 - Assign to interfaces:**
 - eth0, eth1
 - Add / Remove buttons
- Output:**
 - Reserved Bandwidth:
 - Unit: %
 - Max Bandwidth:
 - Unit: %

3. In *Settings* menu:
 - Enter **Name** (descriptive name for this class).

Select **Enabled** checkbox.

On **Priority** drop-down, select one (**0, 1, 2, 3, 4, 5, 6, 7**) (0 is highest priority).

4. In *Assignment* menu:

In *Assign Rules*:

To add a Rule:

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).

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).

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: (Input menu details must match Output menu details)

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**).

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 **Reserved Bandwidth**.

On **Unit** drop-down, select one (**%, GB/s, MB/s, KB/s, B/s, Gbit/s, Mbit/s, Kbit/s, bit/s**).

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

WebUI Procedure

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

WebUI Procedure

1. Go to *Network :: QoS :: Classes*.
2. Select checkbox to be deleted.
3. Click **Delete**.

Enable/Disable a Class

WebUI Procedure

1. Go to *Network :: QoS :: Classes*.
2. Select checkbox to be enabled/disabled.
3. Click **Enable** (to enable class).
4. 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.



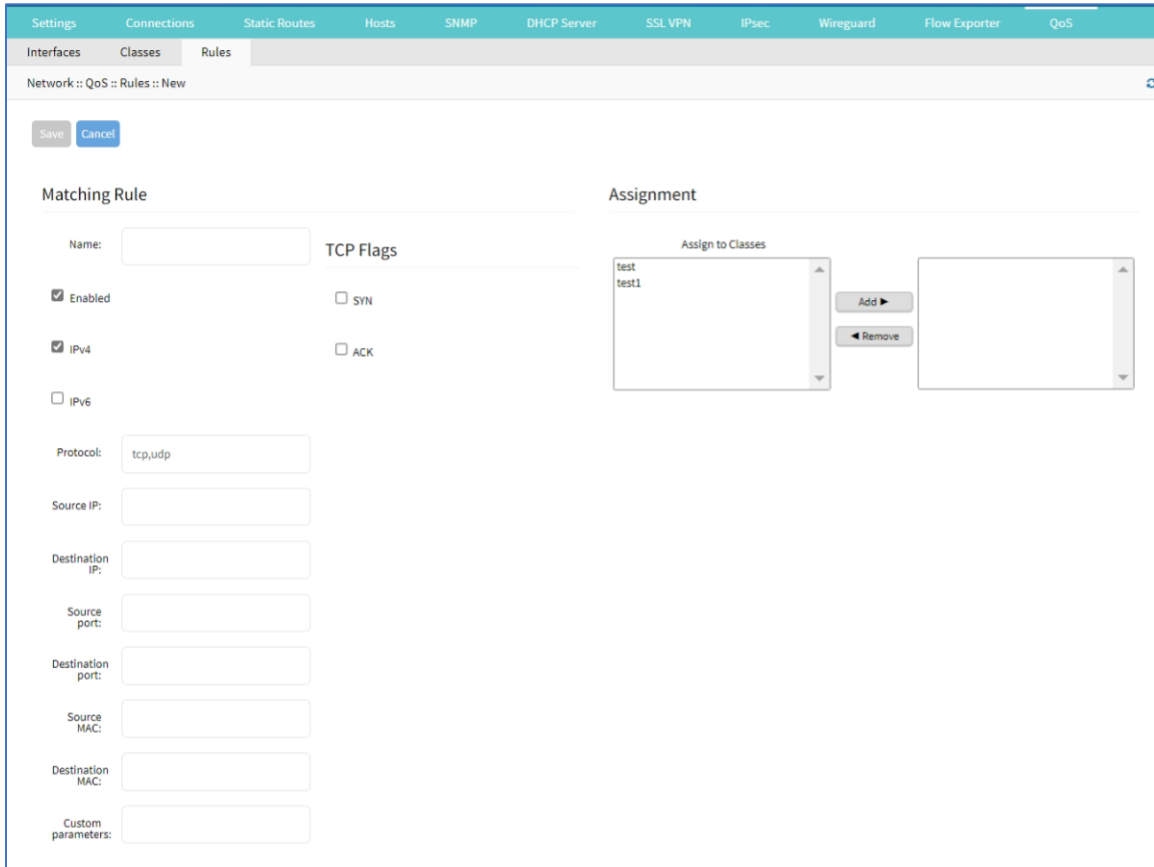
The screenshot shows the 'Rules' sub-tab in the WebUI. At the top, there are tabs for 'Interfaces', 'Classes', and 'Rules'. Below the tabs, the breadcrumb is 'Network :: QoS :: Rules' and there is a 'Reload' button. A row of action buttons includes 'Add', 'Edit', 'Enable', 'Disable', and 'Delete'. Below the buttons is a table with two columns: 'Name' and 'Enabled'. The table contains three rows of rules.

Name	Enabled
<input type="checkbox"/> SSHdst	yes
<input type="checkbox"/> SSHsrc	yes
<input type="checkbox"/> WebUI_dst	yes

Add a Rule

WebUI Procedure

1. Go to *Network :: QoS :: Rules*.
2. Click **Add** (displays dialog).



3. In *Matching Rule* menu:
4. Enter **Name** (descriptive name for this rule).

Select **Enabled** checkbox.

Select **IPv4** checkbox.

Select **IPv6** checkbox.

Enter **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](https://www.iana.org/).

Enter **Source IP**.

Enter **Destination IP**.

Enter **Source Port**.

Enter **Destination Port**.

Enter **Source MAC**.

Enter **Destination MAC**.

Enter **Custom parameters** (advanced users only – enter FireQoS commands).

5. In *TCP Flags* menu:

Select **SYN** checkbox.

Select **ACK** checkbox.

6. 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).

7. 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 a Rule

WebUI Procedure

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 a Rule

WebUI Procedure

1. Go to *Network :: QoS :: Rules*.
2. Select checkbox to be deleted.
3. Click **Delete**.
4. On confirmation pop-up dialog, click **OK**.

Enable/Disable a Rule

WebUI Procedure

1. Go to *Network :: QoS :: Rules*.
2. Select checkbox to be enabled/disabled.

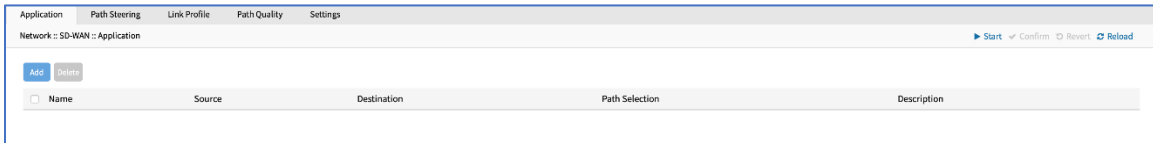
3. Click **Enable** (to enable rule).
4. Click **Disable** (to disable rule).

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.

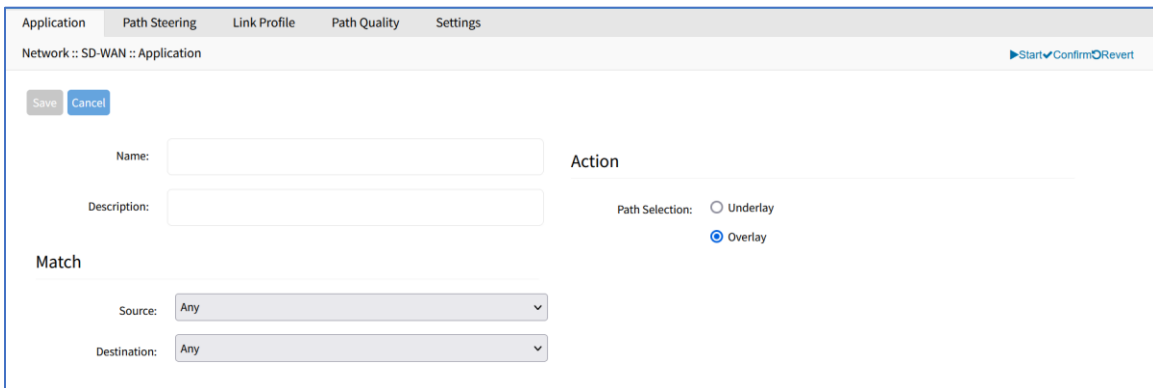
Application sub-tab

Go to *Network :: SD-WAN :: Application*.



Add Application

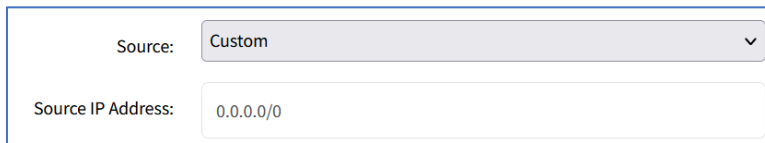
1. Go to *Network :: SD-WAN :: Application*.
2. Click **Add** (displays dialog).



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

On **Source** drop-down, select one (**Any, Custom**)

If **Custom** (expands dialog)



Enter **Source IP Address**.

On **Destination** drop-down, select one (**Any, Custom**)

If **Custom** (expands dialog)

Destination: Custom ▼

Destination IP Address: 0.0.0.0/0

Enter **Destination IP Address**.

6. In *Action* menu, select one:

Underlay radio button

Overlay radio button

7. Click **Save**.

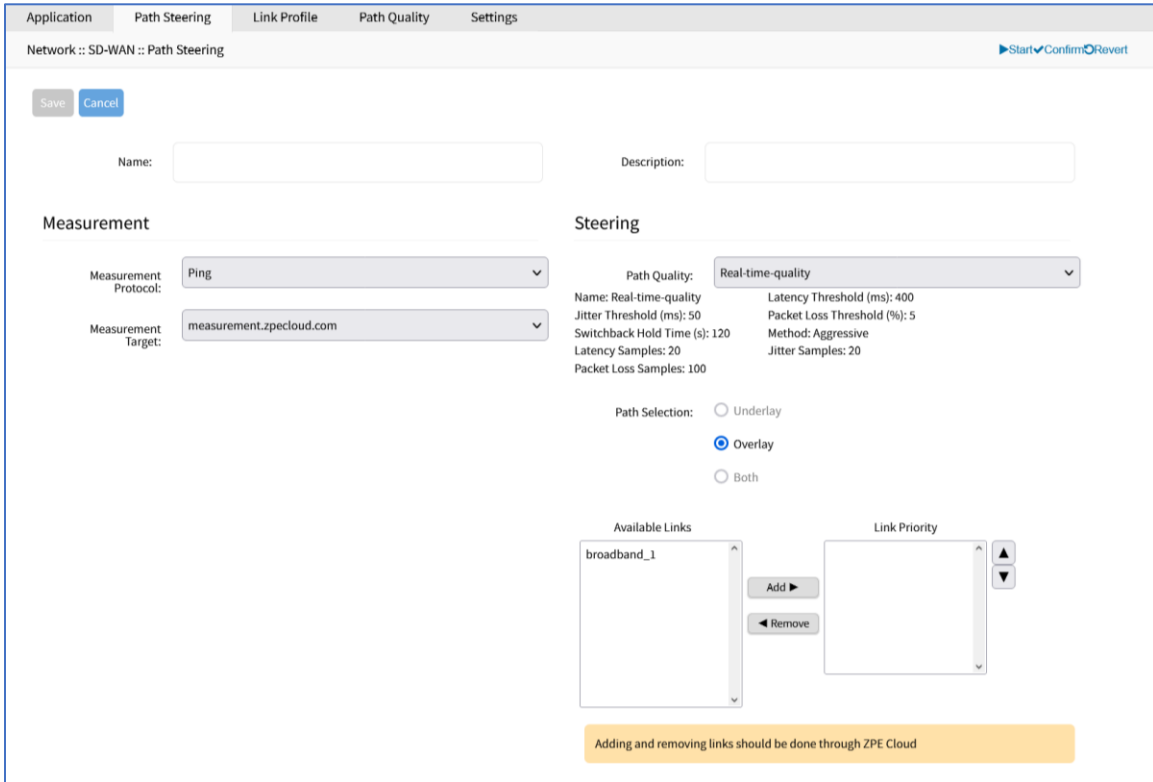
Path Steering sub-tab

Application						
Path Steering						
Link Profile						
Path Quality						
Settings						
Network :: SD-WAN :: Path Steering					Reload	
<div style="display: flex; gap: 5px;"> Add Delete </div>						
<input type="checkbox"/>	Name	Measurement Protocol	Measurement Target	Path Quality	Link Priority	Path Selection
<input type="checkbox"/>	Real-time-apps	Ping	measurement.zpecloud.com	Real-time-quality	broadband_1	Overlay

Add Path Steering

8. Go to *Network :: SD-WAN :: Path Steering*.

9. Click **Add** (displays dialog).



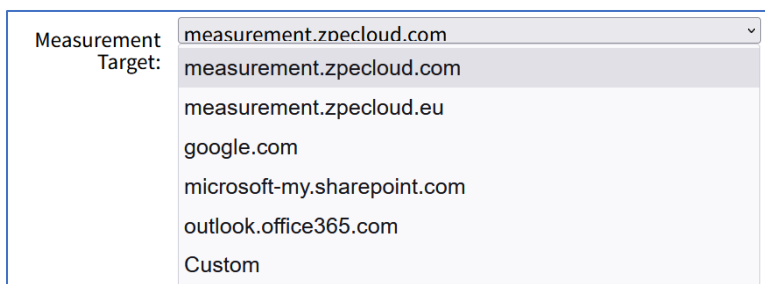
10. Enter **Name**.

11. Enter **Description**.

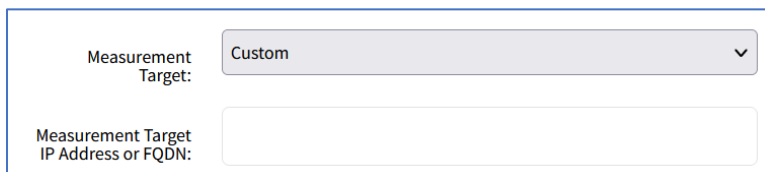
12. In *Measurement* menu:

On **Measurement Protocol** drop-down, select one (**Ping**);

On **Measurement Target** drop-down, select one.



If **Custom** (expands dialog), enter **Measurement Target IP Address or FQDN**.



13. In *Steering* menu:

On **Path Quality** drop-down, select one.

On **Port Selection**, select one.

Underlay radio button

Overlay radio button

Both radio button

In *Available Links* section:

NOTE: If device is enrolled in ZPE Cloud, these links should be changed on the ZPE Cloud application.

Select from left-side panel, click **Add▶** to move to right-side panel.

To remove from right-side panel, select, and click **◀Remove**.

14. Click **Save**.

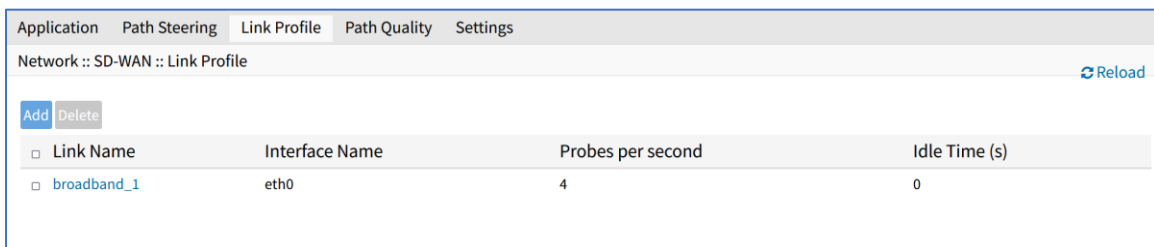
Edit Path Steering

1. Go to *Network :: SD-WAN :: Path Steering*.
2. Click on **Name**.
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)
<input type="checkbox"/> broadband_1	eth0	4	0

Add Link Profile

WebUI Procedure

5. Go to *Network :: SD-WAN :: Link Profile*.
1. Click **Add** (displays dialog).

2. Enter **Link Name**.
3. On **Interface Name** drop-down, select one.
4. Enter **Probes per second** (default: 4).
5. Enter **Idle Time**. (seconds) (default: 0).
6. Click **Save**.

Edit Link Profile

WebUI Procedure

7. Go to *Network :: SD-WAN :: Link Profile*.
 1. In **Name** column, click on name.
 2. Make changes, as needed.
 3. Click **Save**.

Delete Link Profile

WebUI Procedure

4. Go to *Network :: SD-WAN :: Link Profile*.
 1. Select checkbox to be deleted.
 2. Click **Delete**.
 3. On confirmation pop-up dialog, click **OK**.

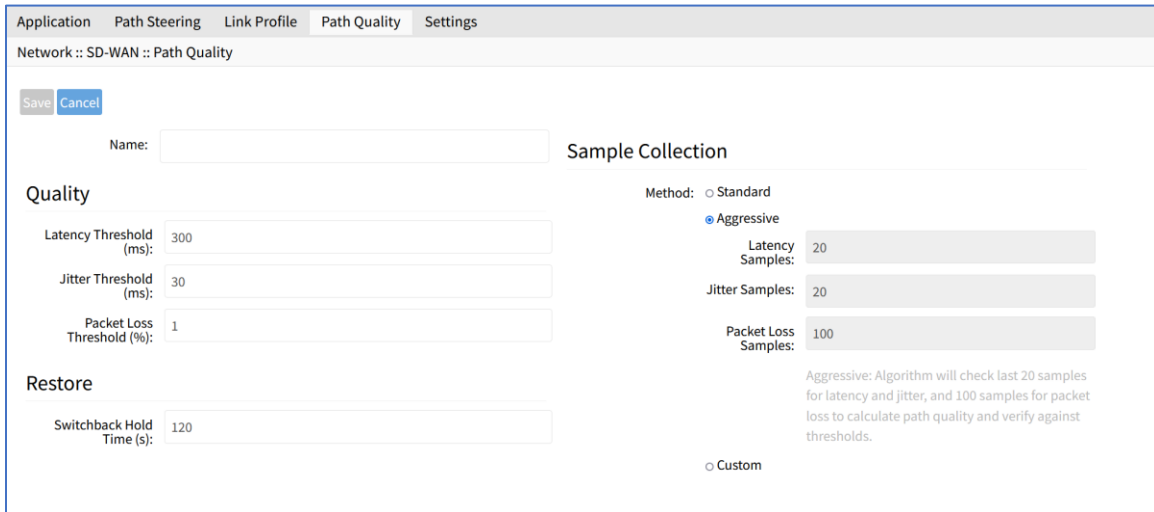
Path Quality sub-tab

<input type="checkbox"/> Name	Latency Threshold (ms)	Jitter Threshold (ms)	Packet Loss Threshold (%)	Switchback Hold Time (s)	Steering Settings
<input type="checkbox"/> Real-time-quality	400	50	5	120	Aggressive
<input type="checkbox"/> Broadband-only	600	80	30	120	Aggressive

Add Path Quality

WebUI Procedure

1. Go to *Network :: SD-WAN :: Link Profile*.
2. Click **Add** (displays dialog).



3. Enter **Name**.
4. In *Quality* menu:
 - Enter **Latency Threshold (ms)** (default: 300)
 - Enter **Jitter Threshold (ms)** (default: 30)
 - Enter **Packet Loss Threshold (%)** (default: 1)
5. In *Restore* menu:
 - Enter **Switchback Hold Time (s)** (default: 120)
6. In *Sample Collection* menu:
 - On **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)

Enter **Latency Samples**

Enter **Jitter Samples**

Enter **Packet Loss Samples**

7. Click **Save**.

Edit Path Quality

WebUI Procedure

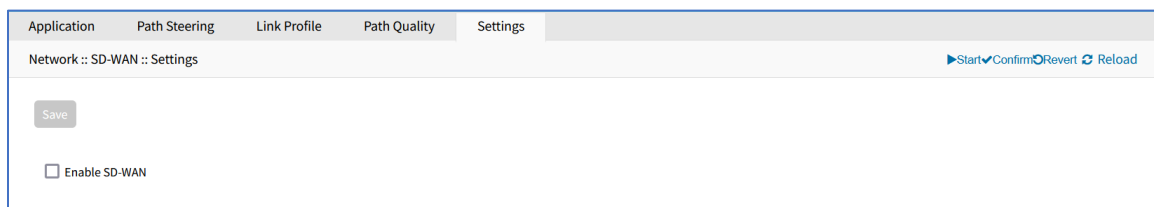
1. Go to *Network :: SD-WAN :: Path Quality*.
2. In **Name** column, click on name.
3. Make changes, as needed.
4. Click **Save**.

Delete Path Quality

WebUI Procedure

1. Go to *Network :: SD-WAN :: Path Quality*.
2. Select checkbox to be deleted.
3. Click **Delete**.
4. On confirmation pop-up dialog, click **OK**.

Settings sub-tab



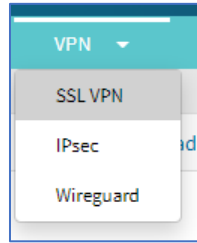
Enable SD-WAN

The minimum Nodegrid supported version to enable SD-WAN is v5.4.6+.

WebUI Procedure

5. Go to *Network :: SD-WAN :: Settings*.
6. Select **Enable SD-WAN**.
7. Click **Save**.

VPN drop-down > SSL VPN tab



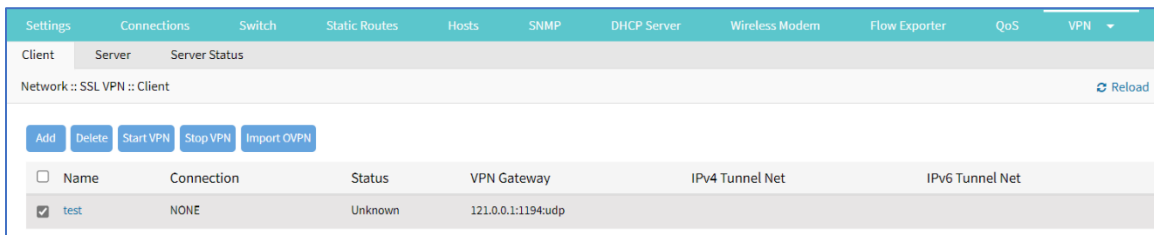
Multiple VPN options are supported. This includes VPN client and server options plus IPsec configurations for host to host, site to site, and others. Also available is IPsec with asymmetric PSL auth support for IKEv2 tunnel. This allows the System to act as VPN servers or clients.

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.



Settings	Connections	Switch	Static Routes	Hosts	SNMP	DHCP Server	Wireless Modem	Flow Exporter	QoS	VPN
Client	Server	Server Status								
Network :: SSL VPN :: Client										Reload
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Start VPN"/> <input type="button" value="Stop VPN"/> <input type="button" value="Import OVPN"/>										
<input type="checkbox"/>	Name	Connection	Status	VPN Gateway	IPv4 Tunnel Net	IPv6 Tunnel Net				
<input checked="" type="checkbox"/>	test	NONE	Unknown	121.0.0.1:1194:udp						

VPN Client Table

Column name	Description
Name	Connection name.
Connection	Network interface the tunnel is bound.
Status	Status of client.
VPN Gateway	VPN Gateway IP address.
IPv4 Tunnel Net	IPv4 Tunnel IP address.
IPv6 Tunnel Net	IPv6 Tunnel IP address.

Add Client

WebUI Procedure

1. Go to *Network :: VPN drop-down :: SSL VPN :: Client*.
2. Click **Add** (displays dialog).

3. Enter **Name**.
4. On **Network Connection** drop-down, select one (**None, ETH0, ETH1, hotspot**).
5. In *Remote Server* menu, select:
 - Single Gateway** radio button
 - Enter **Gateway IP Address**.
 - Enter **Gateway Port** (default: 1194).
 - On **Connection Protocol** drop-down, select one (**UDP, TCP**).

Multiple Gateway radio button

Enter **Gateways** (comma separated).

6. Enter **Tunnel MTU** (MTU size for the tunnel interface. Default: 1500).

7. Select **Use LZO data compress Algorithm** checkbox.
8. Select **Ignore obtained default gateway** checkbox.
9. On **HMAC/Message Digest Alg** drop-down, select one.
10. On **Cipher Alg** drop-down, select one.
11. On *Authentication Method* drop-down, select one.
 - On **TLS** selection:
 - For **TLS Authentication Key** drop-down, select one.
 - For **TLS Authentication Direction** drop-down, select one.
 - For **CA Certificate** drop-down, select one.
 - For **Client Certificate** drop-down, select one.
 - For **Client Private Key** drop-down, select one.
 - On **Static Key** selection:
 - For **Secret** drop-down, select one.
 - Enter **Local Endpoint (Local IP)**.
 - Enter **Remote Endpoint (Remote IP)**.
 - On **Password** selection:
 - Enter **Username**.
 - Enter **Password**.
 - For **CA Certificate** drop-down, select one.
 - On **Password plus TLS** selection:
 - Enter **Username**.
 - Enter **Password**.
 - For **TLS Authentication Key** drop-down, select one.
 - For **TLS Authentication Direction** drop-down, select one.
 - For **CA Certificate** drop-down, select one.
 - For **Client Certificate** drop-down, select one.
 - For **Client Private Key** drop-down, select one.
12. Click **Save**.

Edit Client

WebUI Procedure

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

WebUI Procedure

1. Go to *Network :: VPN drop-down :: SSL VPN :: Client*.
2. Select checkbox to be deleted.
3. Click **Delete**.

Start Client VPN

WebUI Procedure

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

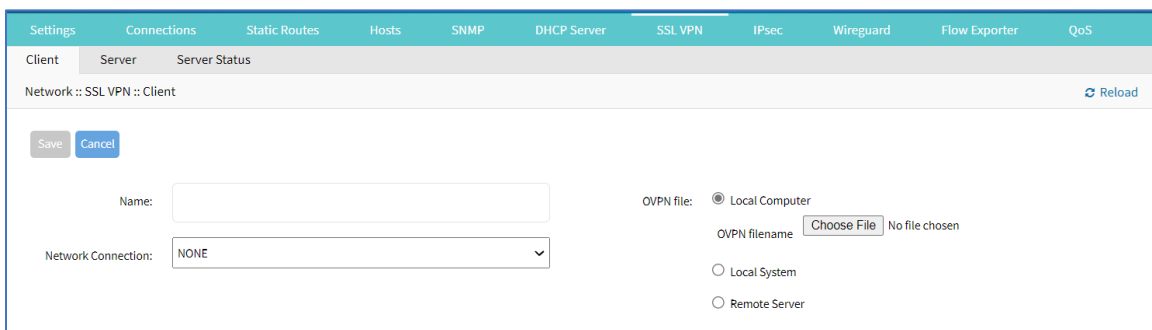
WebUI Procedure

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

WebUI Procedure

1. Go to *Network :: VPN drop-down :: SSL VPN :: Client*.
2. Click **Import OVPN** (displays dialog).



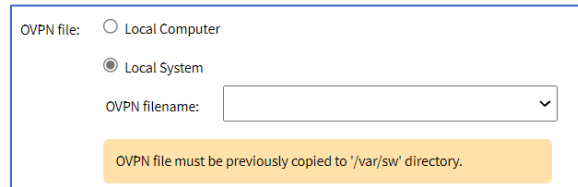
3. Enter **Name**.
4. On **Network Connection** drop-down, select one (**NONE, ETH0, ETH1, hotspot**).

5. In *OVPN File* menu:

Select **Local Computer** radio button:

Click **Choose File**. Locate and select the file.

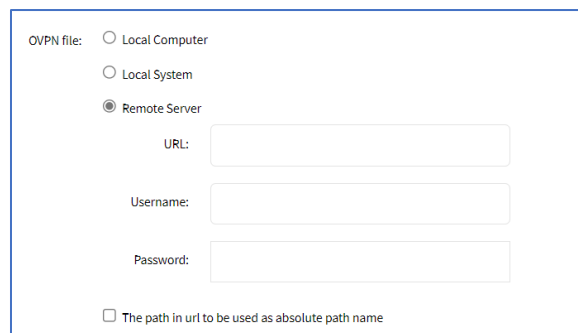
Select **Local System** radio button:



The screenshot shows the 'OVPN file:' section of a configuration form. It has three radio buttons: 'Local Computer' (unselected), 'Local System' (selected), and 'Remote Server' (unselected). Below the radio buttons is a text input field labeled 'OVPN filename:' with a dropdown arrow. At the bottom, there is a yellow warning box with the text: 'OVPN file must be previously copied to '/var/sw' directory.'

On **OVPN filename** drop-down, select one.

Select **Remote Server** radio button:



The screenshot shows the 'OVPN file:' section of a configuration form. It has three radio buttons: 'Local Computer' (unselected), 'Local System' (unselected), and 'Remote Server' (selected). Below the radio buttons are three text input fields labeled 'URL:', 'Username:', and 'Password:'. At the bottom, there is a checkbox labeled 'The path in url to be used as absolute path name' which is currently unchecked.

Enter **URL**.

Enter **Username**.

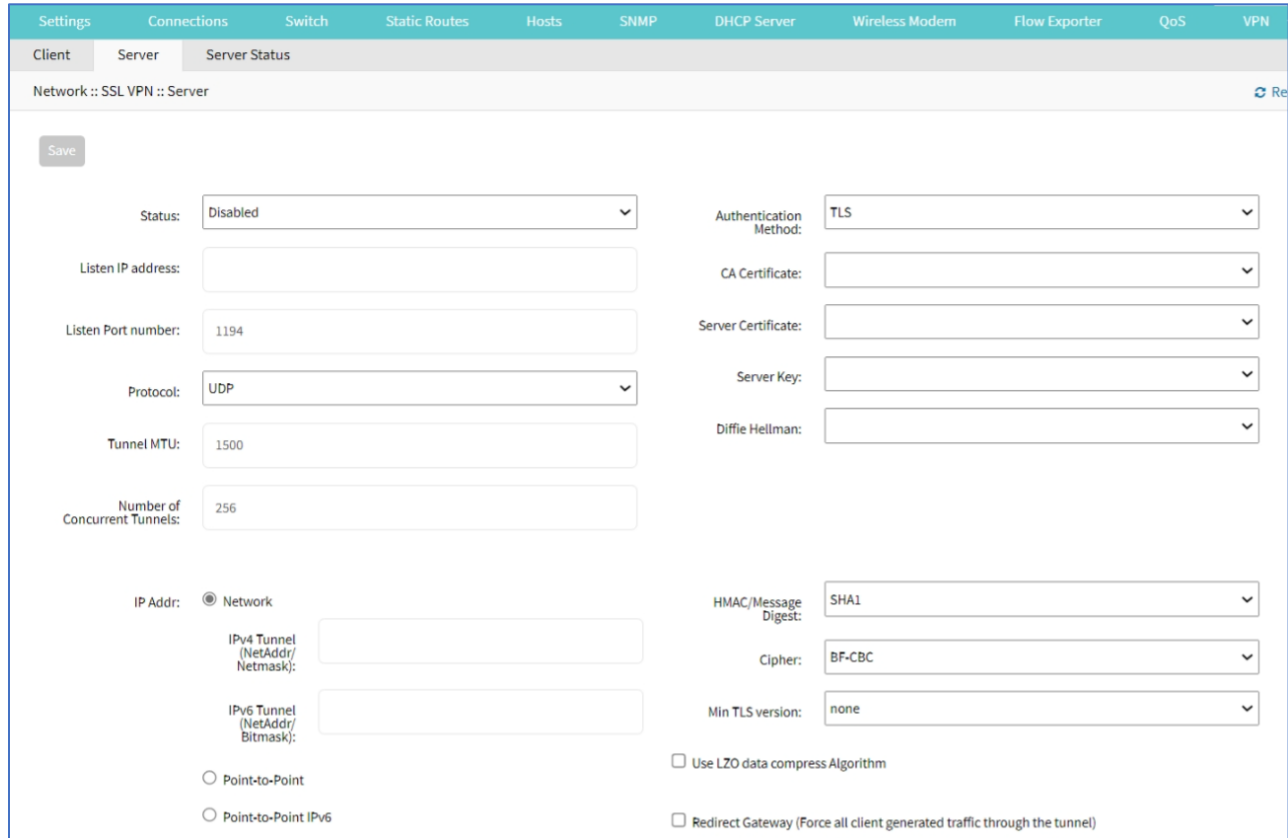
Enter **Password**.

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

6. 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/openssl/CA folder.



Configure SSL VPN Server Details

WebUI Procedure

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 **Listen IP address** (if defined, the server only responds to client requests coming in this interface)

Enter **Listen Port number** (listening port for incoming connections - default: 1194).
4. On **Protocol** drop-down, select one (**UDP, TCP, UDP IPv6, TCP IPv6**).

Enter **Tunnel MTU** (default: 1500).

Enter **Number of Concurrent Tunnels** (default: 256).
5. *Authentication Method* menu – enter details (different fields are displayed according to selection)

On **TLS** selection:

For **CA Certificate** drop-down, select one.

For **Server Certificate** drop-down, select one.

For **Server Key** drop-down, select one.

For **Diffie Hellman** drop-down, select one.

On **Static Key** selection

For **Secret** drop-down, select one.

For **Diffie Hellman** drop-down, select one.

On **Password** selection

For **CA Certificate** drop-down, select one.

For **Server Certificate** drop-down, select one.

For **Server Key** drop-down, select one.

For **Diffie Hellman** drop-down, select one.

On **Password plus TLS** selection

For **CA Certificate** drop-down, select one.

For **Server Certificate** drop-down, select one.

For **Server Key** drop-down, select one.

For **Diffie Hellman** drop-down, select one.

6. *IP Address* menu (display changes based on selection) IP address settings for the tunnel:

Select **Network** radio button:

Enter **IPv4 Tunnel** (NetAddr/ Netmask)

Enter **IPv6 Tunnel** (NetAddr/ Netmask):

Select **Point to Point** radio button:

Enter **Local Endpoint** (Local IP)

Enter **Remote Endpoint** (Remote IP)

Select **Point To Point IPv6** radio button:

Enter **Local Endpoint** (Local IPv6)

Enter **Remote Endpoint** (Remote IPv6)

On **HMAC/Message Digest** drop-down (select HMAC connection algorithm)

On **Cipher** drop-down (select connection cipher algorithm)

On **Min TLS version** drop-down, select one (**None, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3**).

Select **Use LZO data compress Algorithm** checkbox (all tunnel traffic is compressed)

Select **Redirect Gateway (Force all client generated traffic through the tunnel)** checkbox (all traffic from a client is forced through the tunnel)

7. Click **Save**.

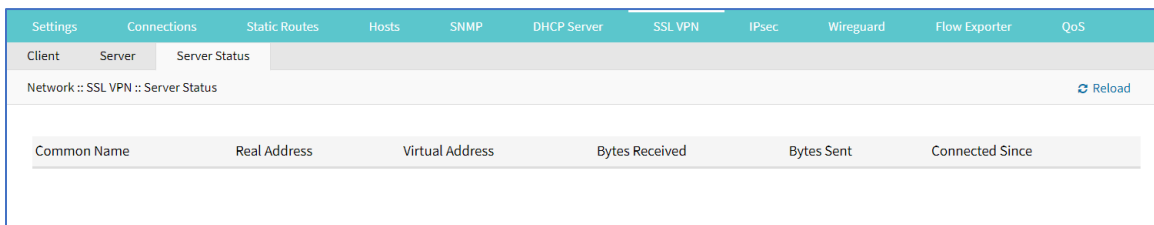
Edit VPN Server Details

WebUI Procedure

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.

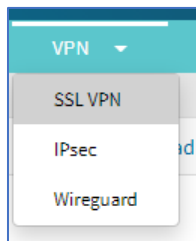


Server Status Table

Column name	Description
Common Name	Connection name.
Real Address	Real IP address.
Virtual Address	Virtual IP address.
Bytes Received	Bytes received by client.
Bytes Sent	Bytes sent from client.
Connect Since	Continuous connection from <date/time>.

VPN drop-down > IPsec tab

NOTE: Access on VPN tab drop-down.



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 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.

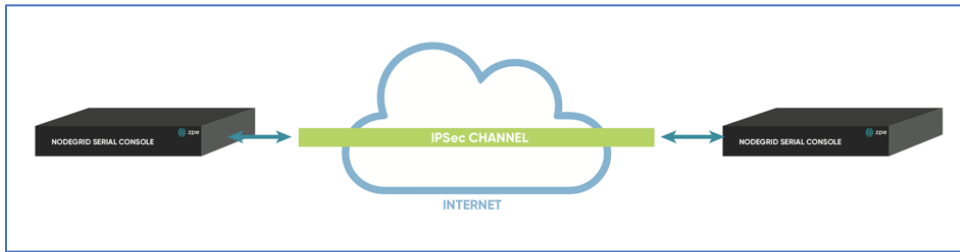
X.509 Certificates

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

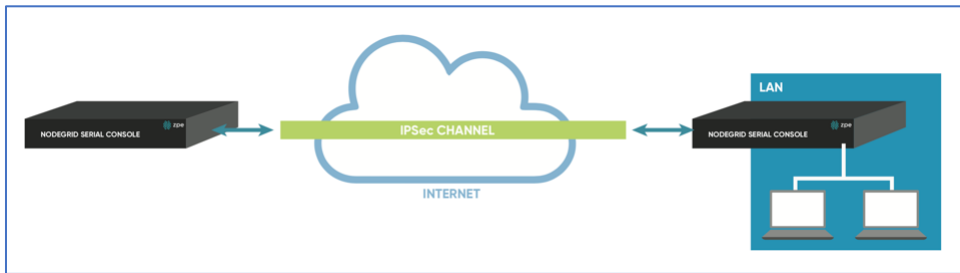
IPsec supports many connection scenarios, from the basic one-to-one nodes and the more complex one-to-many nodes. Communication can be limited to the directly involved nodes. If needed, communication can be expanded to the networks access table behind the nodes. Examples are provided for some of the most common scenarios.

Host-to-Host



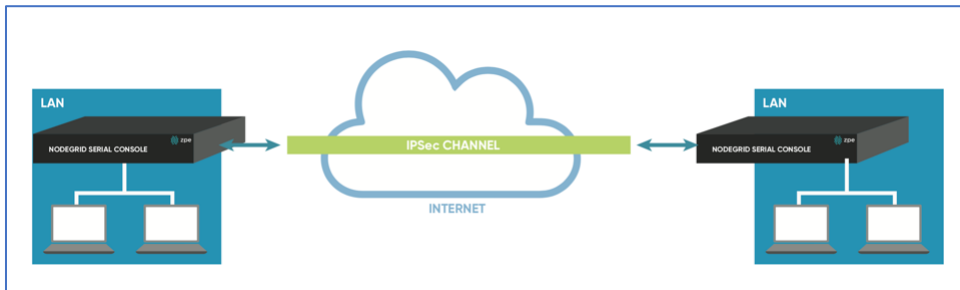
Host-to-Host communication is two nodes directly connected with a VPN tunnel. The communication is limited to direct communication between them. None of the packages are routed or forwarded. This is a point-to-point communication tunnel between two nodes.

Host-to-Site



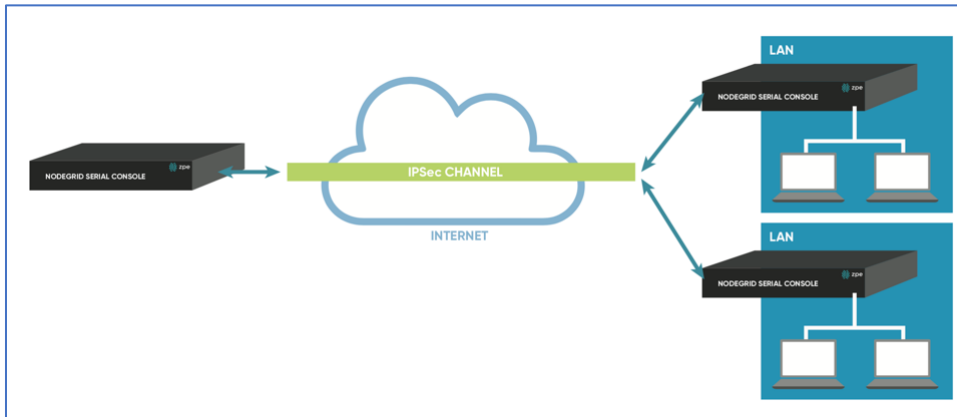
With host-to-Site, one node establishes a VPN tunnel to a second node. Communication is limited on one site to the specific node; and on the other side, limited to all devices in a range of subnet accessible by the second node.

Site-to-Site



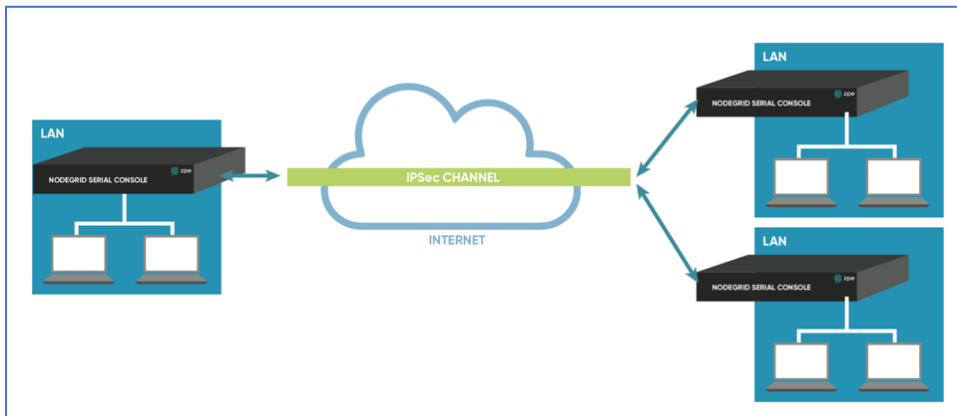
In site-to-site, the tunnel is established between two nodes. Communication can specify the subnet on both sides. This allows communication between devices on either side of the connection.

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

	Host to Host	Host to Site	Site to Site	Host to Multi-Site	Site to Multi-Host
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](#)

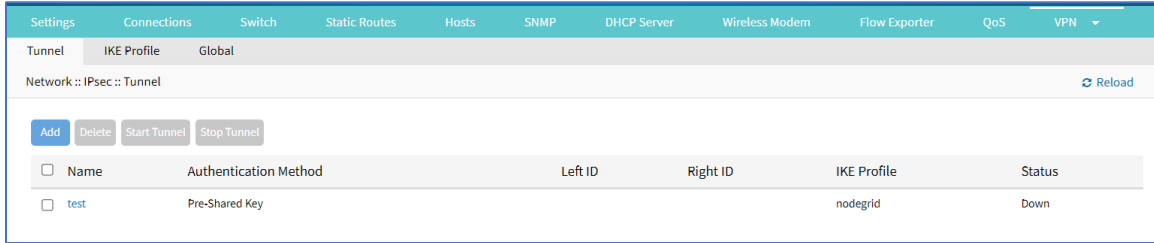
[How to Configure IPsec Site to Site Tunnel with Certificate](#)

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.



Column name	Description
Name	Tunnel name.
Authentication Method	Method of authentication.
Left ID	Tunnel left ID.
Right ID	Tunnel right ID.
IKE Profile	Profile information.
Status	Current tunnel status.

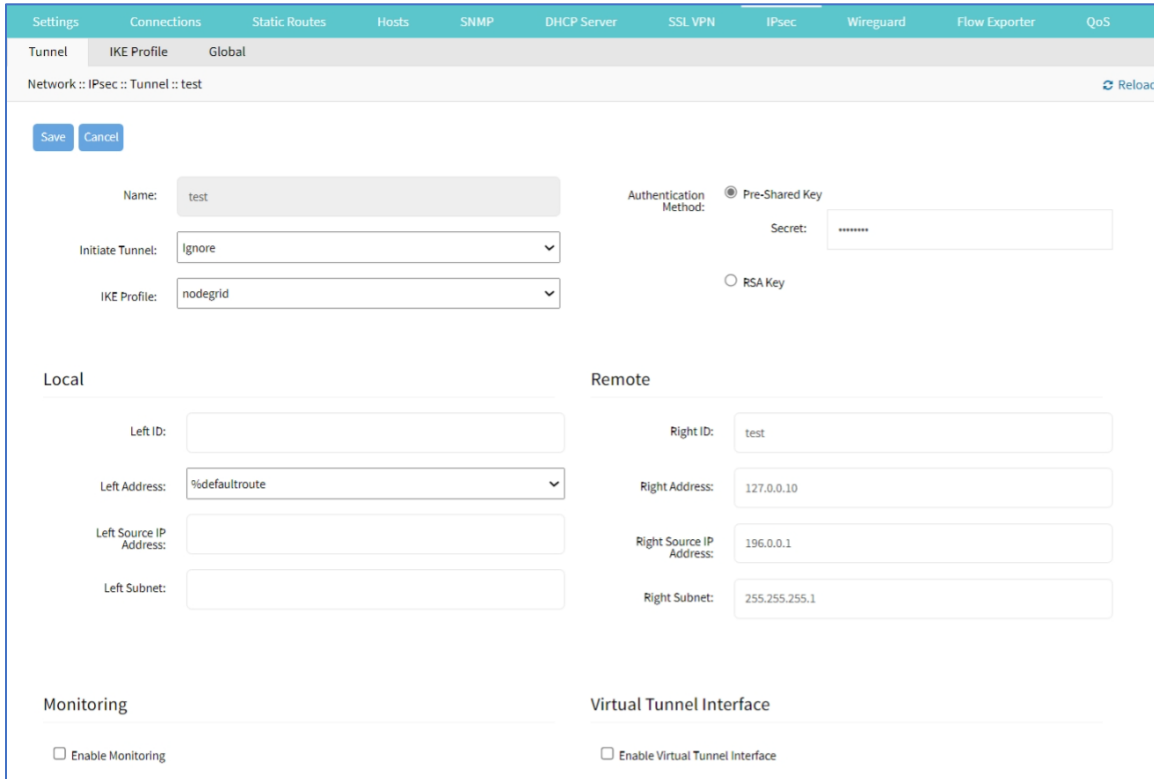
Tunnel Main Table

Column name	Description
Name	Tunnel name.
Authentication Method	Method of authentication.
Left ID	Tunnel left ID.
Right ID	Tunnel right ID.
IKE Profile	Profile information.
Status	Current tunnel status.

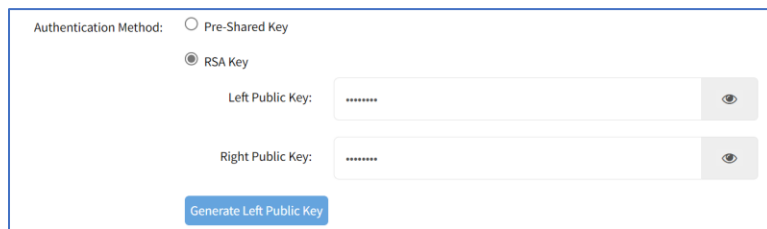
Add a New Tunnel

WebUI Procedure

1. Go to *Network :: VPN drop-down :: IPsec :: Tunnel*.
2. Click **Add** (displays dialog).



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. In *Authentication Method* menu, select one:
 Select **Pre-Shared Key** radio button.
 Enter **Secret**.
 Select **RSA Key** radio button (displays dialog)



- Enter **Left Public Key**.
- Enter **Right Public Key**.
- Click **Generate Left Public Key**.

7. In *Local* menu:
 Enter **Left ID**.

On **Left Address** drop-down, select one (selection depends on the system configuration).

Enter **Left Source IP Address**.

Enter **Left Subnet**.

8. In *Remote* menu:

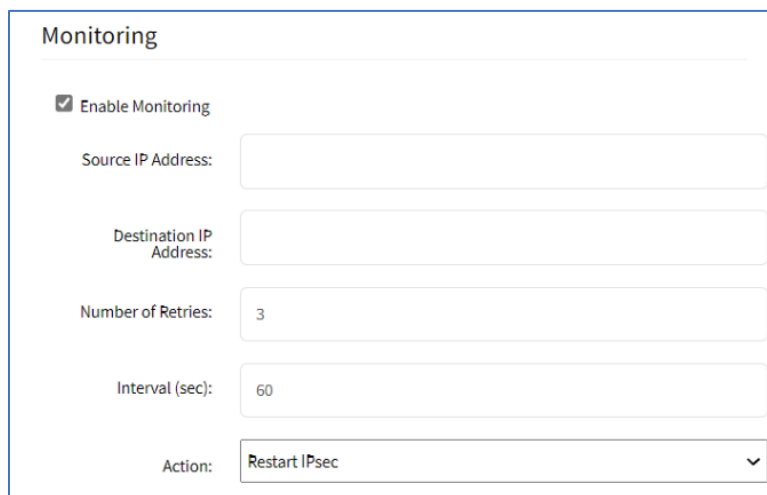
Enter **Right ID**.

Enter **Right Address**.

Enter **Right Source IP Address**.

Enter **Right Subnet**.

9. (optional) In *Monitoring* menu, select **Enable Monitoring** checkbox (expands dialog).



Enter **Source IP Address** (to ping from).Enter

Enter **Destination IP Address** (to ping to).

Enter **Number of Retries** (pings before triggering Action)

Enter **Interval (seconds)** (time between retries)

On **Action** drop-down, select one (if 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)

NOTE: The number of retries and interval should be greater than that of the dead peer detection configuration within the IKE profile.

10. (optional) In *Virtual Tunnel Interface* menu, select **Enable Virtual Tunnel Interface** checkbox (displays dialog).

Virtual Tunnel Interface

Enable Virtual Tunnel Interface

Mark:

Address:

Interface:

Automatically create VTI routes

Share VTI with other connections

Enter **Mark**.

Enter **Address**.

Enter **Interface**.

Select **Automatically create VTI routes**.

Select **Share VTI with other connections**.

11. Click **Save**.

Edit a Tunnel

WebUI Procedure

1. Go to *Network :: VPN drop-down :: IPsec :: Tunnel*.
2. In the *Name* column, click a name (opens dialog).
3. Make changes, as needed.
4. Click **Save**.

Delete a Tunnel

WebUI Procedure

1. Go to *Network :: VPN drop-down :: IPsec :: Tunnel*.
2. In the table, select checkbox of tunnel to delete.
3. Click **Delete**.

Start a Tunnel

WebUI Procedure

1. Go to *Network :: VPN drop-down :: IPsec :: Tunnel*.
2. In the table, select checkbox of tunnel to start.
3. Click **Start Tunnel**.

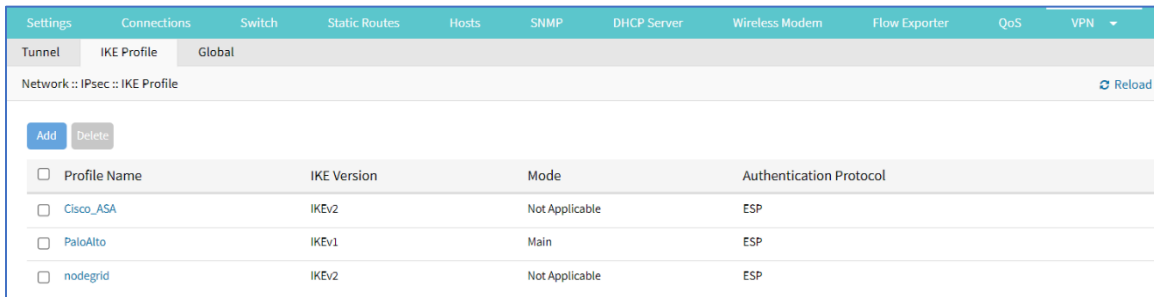
Stop a Tunnel

WebUI Procedure

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.



<input type="checkbox"/>	Profile Name	IKE Version	Mode	Authentication Protocol
<input type="checkbox"/>	Cisco_ASA	IKEv2	Not Applicable	ESP
<input type="checkbox"/>	PaloAlto	IKEv1	Main	ESP
<input type="checkbox"/>	nodegrid	IKEv2	Not Applicable	ESP

Add a New Profile

WebUI Procedure

1. Go to *Network :: VPN drop-down :: IPsec :: IKE Profile*.
2. Click **Add** (displays dialog).

3. Enter **Profile Name**.
4. On **IKE Version** drop-down, select one (**IKEv1**, **IKEv2**) (modifies *Phase 1* selection).

(IKEv1 selection)

(IKEv2 selection)

(if **IKEv1**) On **Mode** drop-down, select one (**Aggressive**, **Main**).

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.

- In *Phase 2* menu, **Authentication Protocol** drop-down, select one (**ESP, AH**).

(ESP selection)

(AH selection)

(ESP selection only) 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**.

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**.

- In *Advanced Settings* menu, dialog changes if **Enable Dead Peer Detection** checkbox is selected.

(unselected)

(selected)

Advanced Settings

Enable Dead Peer Detection

Number of Retries:

Interval (sec):

Action:

MTU:

Custom Parameters

(if selected) Enter value on **Enter number of retries**.

Enter **Interval (sec)**.

On **Action** drop-down, select one (**hold, clear, restart**).

Enter **MTU**.

Enter **Custom Parameters** (comma separated).

7. Click **Save**.

Edit a Profile

WebUI Procedure

1. Go to *Network :: VPN drop-down :: IPsec :: IKE Profile*.
2. Locate and click on the **Profile Name**.
3. Modify configuration details, as needed.
4. Click **Save**.

Delete a Profile

WebUI Procedure

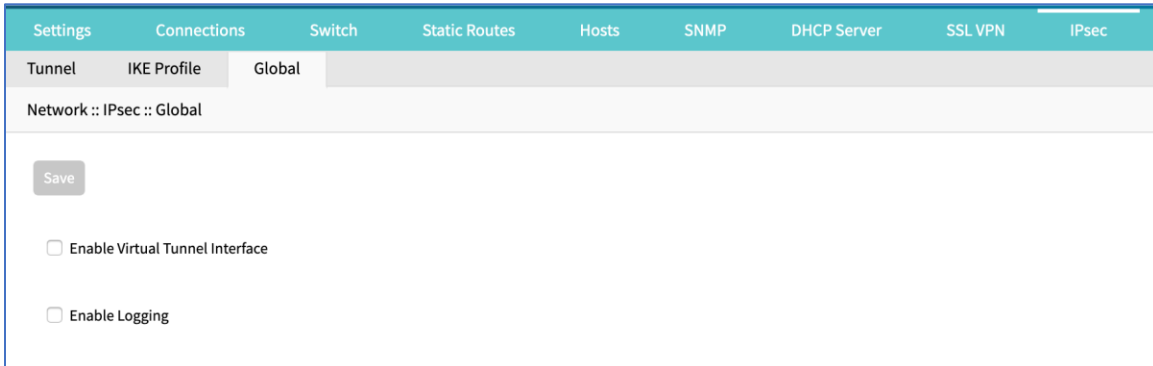
1. Go to *Network :: VPN drop-down :: IPsec :: IKE Profile*.
2. Click the checkbox next to the profile to delete.
3. Click **Delete**.

Global sub-tab

Edit Global Options

WebUI Procedure

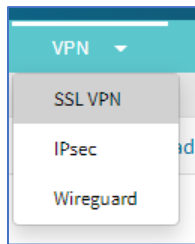
1. Go to *Network :: VPN drop-down :: IPsec :: Global*.



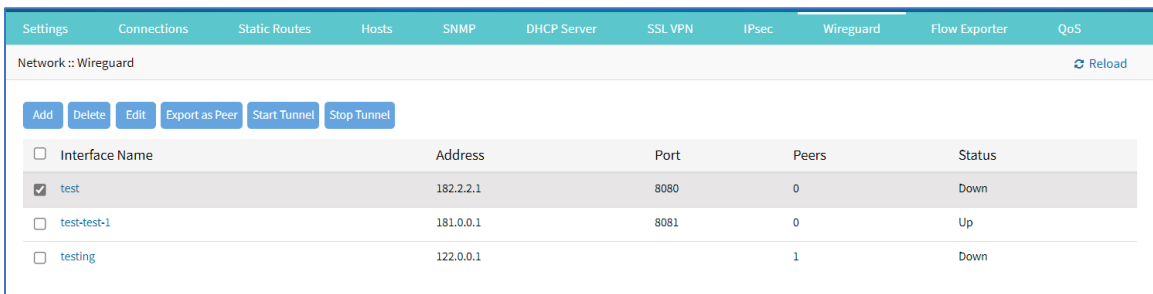
2. Select/unselect **Enable Virtual Tunnel Interface** checkbox.
3. Select/unselect **Enable Logging** checkbox.
4. Click **Save**.

VPN drop-down > Wireguard tab

NOTE: Access on VPN tab drop-down.



Wireguard establishes a site to site tunnel. Wireguard is supported in the admin CLI and GUI on Nodegrid devices v5.2+.



Advantages

- Uses a current elliptic curve algorithm for the encryption
- Uses RSA keys and optional PSK's for authentication
- Roaming of End Points is an integrated part of the solution
- Good Client support, with native support for Windows, MacOS, Linux, iOS and Android
- 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

Manage Wireguard Configurations

Add a Wireguard Configuration

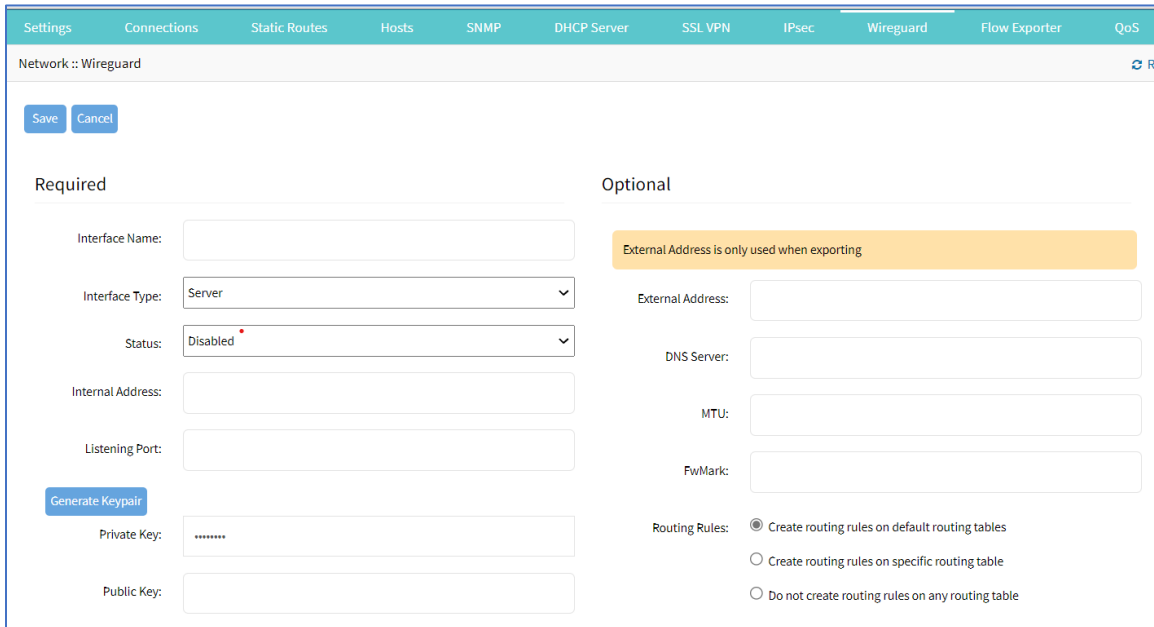
WebUI Procedure

1. Go to *Network :: VPN drop-down :: Wireguard*.
2. Click **Add** (dialog changes, based on **Interface Type** drop-down selection).

Enter **Interface Name**.

On **Interface Type** drop-down, select one (display is modified, based on selection).

Server interface type



On **Status** drop-down, select one (**Enabled, Disabled**).

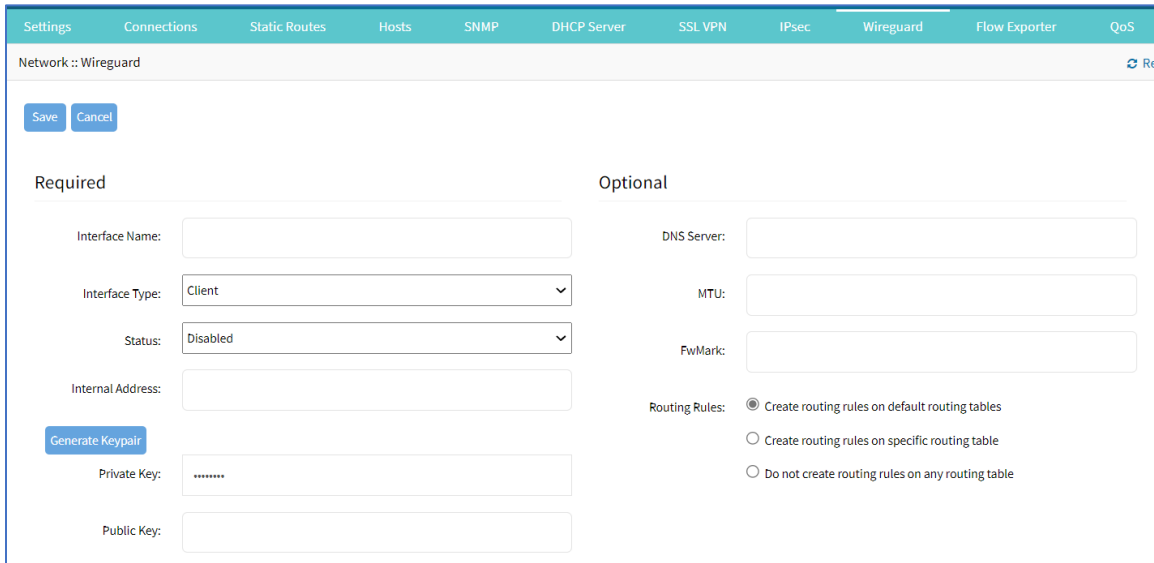
Enter **Internal Address**.

Enter **Listening Port**.

Click **Generate Keypair**.

In *Optional* menu, enter **External Address**.

Client interface type



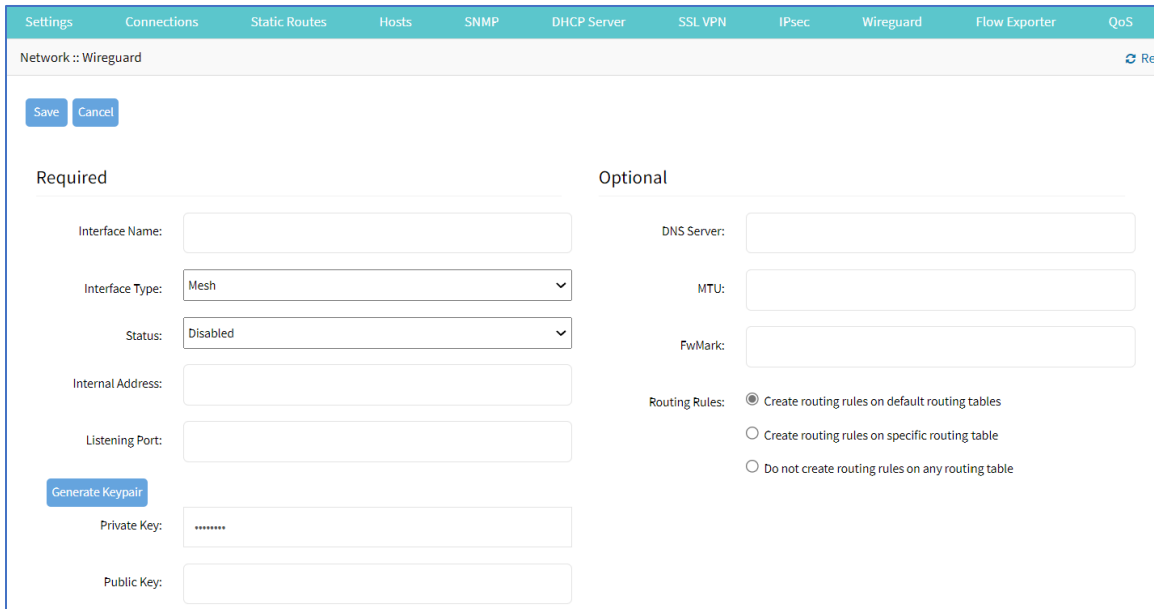
The screenshot shows the 'Wireguard' configuration page. The 'Required' section includes fields for 'Interface Name', 'Interface Type' (set to 'Client'), 'Status' (set to 'Disabled'), 'Internal Address', 'Private Key', and 'Public Key'. A 'Generate Keypair' button is located between the 'Internal Address' and 'Private Key' fields. The 'Optional' section includes 'DNS Server', 'MTU', 'FwMark', and 'Routing Rules' (with three radio button options: 'Create routing rules on default routing tables', 'Create routing rules on specific routing table', and 'Do not create routing rules on any routing table').

On **Status** drop-down, select one (**Enabled, Disabled**).

Enter **Internal Address**.

Click **Generate Keypair**.

Mesh interface type



The screenshot shows the 'Wireguard' configuration page. The 'Required' section includes fields for 'Interface Name', 'Interface Type' (set to 'Mesh'), 'Status' (set to 'Disabled'), 'Internal Address', 'Listening Port', 'Private Key', and 'Public Key'. A 'Generate Keypair' button is located between the 'Internal Address' and 'Private Key' fields. The 'Optional' section includes 'DNS Server', 'MTU', 'FwMark', and 'Routing Rules' (with three radio button options: 'Create routing rules on default routing tables', 'Create routing rules on specific routing table', and 'Do not create routing rules on any routing table').

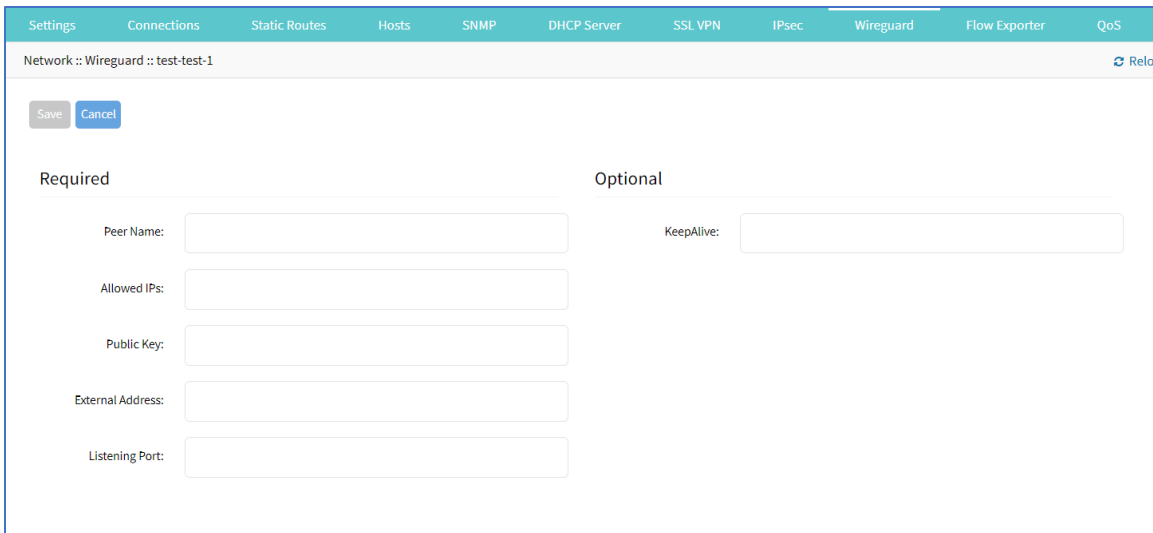
On **Status** drop-down, select one (**Enabled, Disabled**).

Enter **Internal Address**.

Enter **Listening Port**.

Click **Generate Keypair**.

3. In *Optional* menu:
 Enter **DNS Server**.
 Enter **MTU**.
 Enter **FwMark**.
4. In *Routing Rules* menu, select one.
Create routing rules on default routing tables radio button.
Create routing rules on specific routing table radio button.
Do not create routing rules on any routing table radio button.
5. Click **Save**.
 Next is to configure the Peer.
6. On the table, click the **Name** of the new configuration (displays dialog).



7. In the *Required* menu:
 Enter **Peer Name**.
 Enter **Allowed IPs** (comma-separated).
 Enter **Public Key**.
 Enter **External Address**.
 Enter **Listening Port**.
8. In the *Optional* menu, enter **Keepalive** value.
9. Click **Save**.

CLI Procedure

1. Add the Wireguard configuration details, apply these commands:

```
[admin@nodegrid /]# cd /settings/wireguard/
[admin@nodegrid {wireguard}]# set <to configure these parameters>
  dns_server=<value>
  interface_name=<value>
  listening_port=<value>
  public_key=<value>
  external_address=<value>
  interface_type=<value>
  mtu=<value>
  routing_rules=<value>
  fwmark=<value>
  internal_address=<value>
  private_key=<value>
  status=<value>
[admin@nodegrid {wireguard}]# commit
```

2. Configure peers:

```
[admin@nodegrid wireguard]# cd Interface_Name/
[admin@nodegrid Server_Interface]# cd peers/
[admin@nodegrid peers]# add
[admin@nodegrid {peers}]# set <to configure these parameters>
  allowed_ips=<value>
  keepalive=<value>
  peer_name=<value>
  external_address=<value>
  listening_port=<value>
  public_key=<value>
[admin@nodegrid {peers}]# commit
```

Delete a Wireguard Configuration

WebUI Procedure

1. Go to *Go to Network :: VPN drop-down :: Wireguard*.
2. On the table, select checkbox of configuration to delete.
3. Click **Delete**.

Edit a Wireguard Configuration

WebUI Procedure

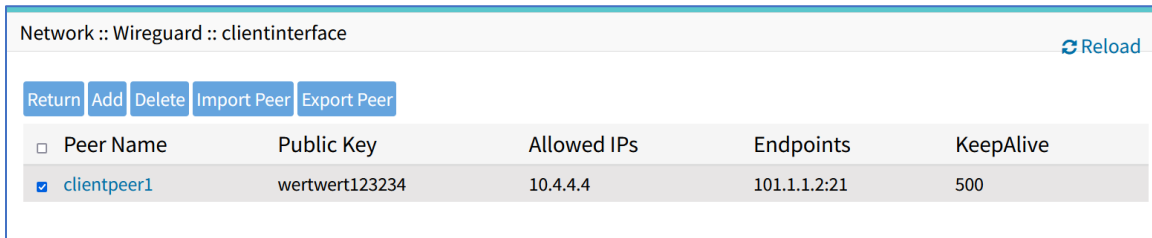
1. Go to *Network :: VPN drop-down :: Wireguard*.
2. On the table, select checkbox of configuration to edit.
3. Click **Edit** (displays dialog).
4. Make changes as needed.

5. Click **Save**.

Export Peer

WebUI Procedure

1. Go to *Network :: VPN drop-down :: Wireguard*.



<input type="checkbox"/>	Peer Name	Public Key	Allowed IPs	Endpoints	KeepAlive
<input checked="" type="checkbox"/>	clientpeer1	wertwert123234	10.4.4.4	101.1.1.2:21	500

2. On the table, select checkbox of configuration to export.

3. Click **Export Peer**.

The file is downloaded to the local download location.

Import Peer

WebUI Procedure

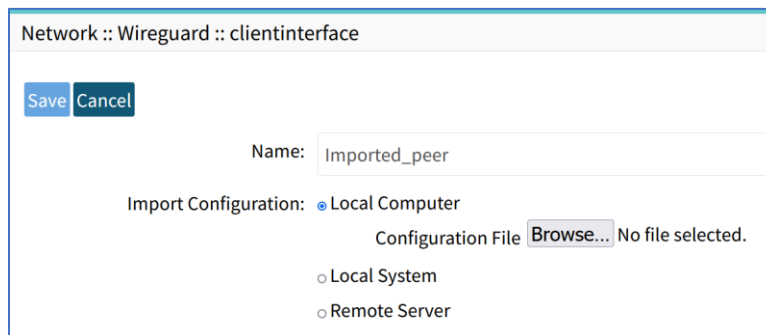
1. Go to *Network :: VPN drop-down :: Wireguard*.

2. Click **Import Peer** (displays dialog).

3. Enter **Name**.

4. Select one:

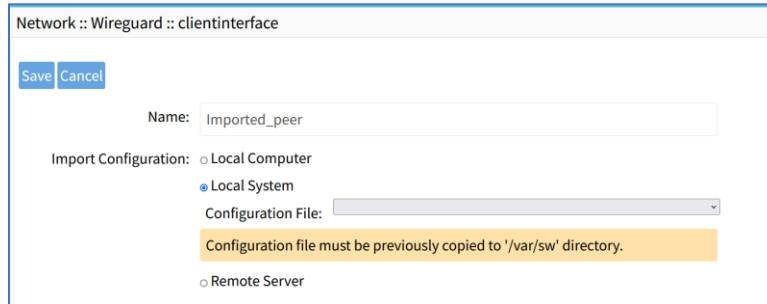
Local Computer radio button



Enter **Name**.

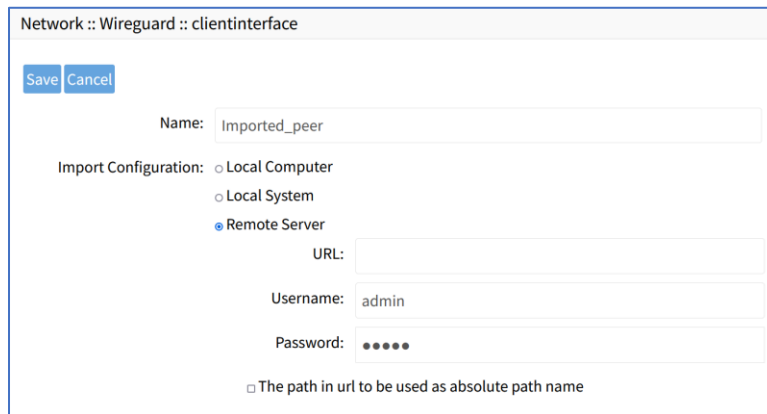
Click **Browse** to locate and select the file.

Local System radio button:



On the **Configuration File** drop-down, select one.

Remote Server radio button:



Enter **URL**

Enter **Username**

Enter **Password**

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

5. Click **Save**.

Start Tunnel\

WebUI Procedure

1. Go to *Network :: VPN drop-down :: Wireguard*.
2. On the table, select checkbox to start configuration.
3. Click **Start Tunnel**.

Stop Tunnel

WebUI Procedure

1. Go to *Network :: VPN drop-down :: Wireguard*.
2. On the table, select checkbox to stop configuration.
3. Click **Stop Tunnel**.

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 the *Access* page. 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
- 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
- Cisco UCS
- Netapp
- Infrabox
- Virtual Machine sessions from:

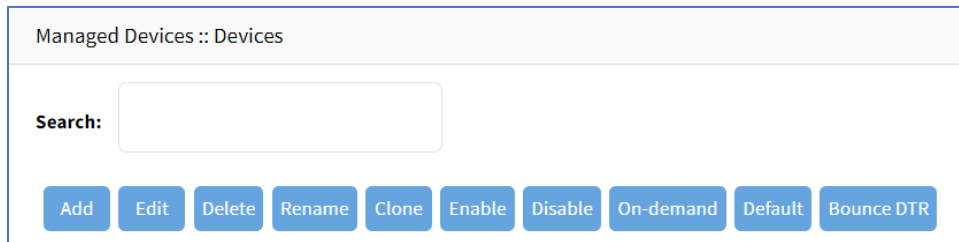
VMWare

KVM

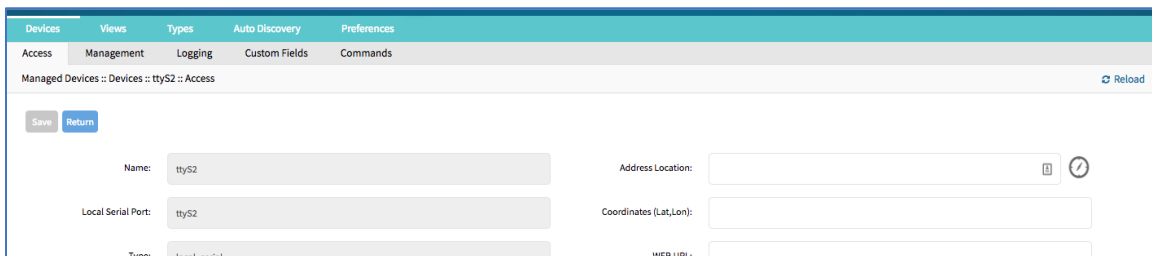
- Sensors:
 - ZPE Systems Temperature and Humidity Sensor
- EdgeCore Access Points

Devices tab

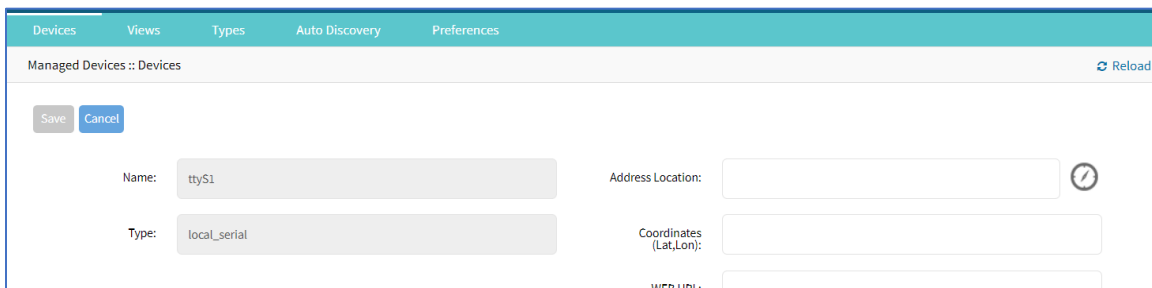
These are all actions that can be performed on this page.



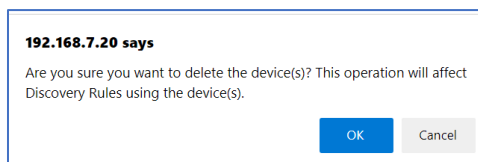
Add – add a device configuration.



Edit – edit settings on the selected device



Delete – displays a pop-up delete confirmation dialog



Rename – change name of selected device

Managed Devices :: Devices

Save Cancel

Current Name:

New Name:

Clone – clone the selection

Managed Devices :: Devices

Save Cancel

Clone From:

Name:

Copy configuration to Local Serial Devices

Devices

- ttyS2
- ttyS3
- ttyS4
- ttyS5
- ttyS6
- ttyS7
- ttyS8
- ttyS9

Add Remove

Enable – changes device use from disabled to enabled

Managed Devices :: Devices Reload

Search:

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

Add Edit Delete Rename Clone Enable Disable On-demand Default Bounce DTR

<input type="checkbox"/>	Name	Connected Through	Type	Access	Monitoring
<input type="checkbox"/>	ttyS1	ttyS1	local_serial	Enabled	Not Supported
<input checked="" type="checkbox"/>	ttyS2	ttyS2	local_serial	Disabled	Not Supported

Disable – changes device use from enabled to disabled

Managed Devices :: Devices Reload

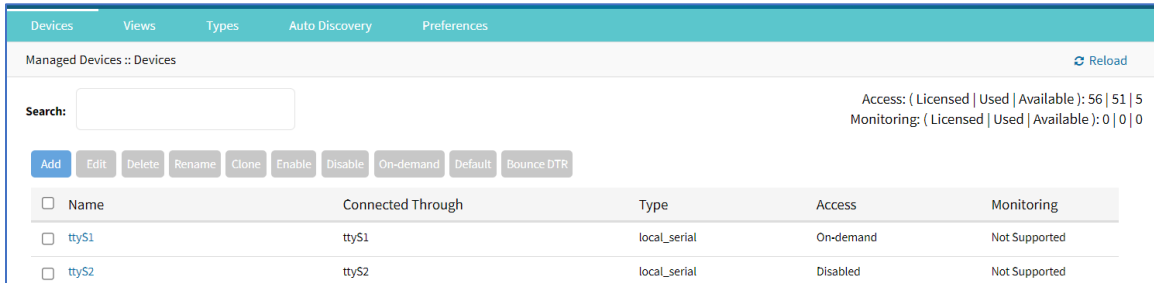
Search:

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

Add Edit Delete Rename Clone Enable Disable On-demand Default Bounce DTR

<input type="checkbox"/>	Name	Connected Through	Type	Access	Monitoring
<input type="checkbox"/>	ttyS1	ttyS1	local_serial	Disabled	Not Supported
<input type="checkbox"/>	ttyS2	ttyS2	local_serial	Disabled	Not Supported

On-demand – changes device use to On-Demand



<input type="checkbox"/>	Name	Connected Through	Type	Access	Monitoring
<input type="checkbox"/>	ttyS1	ttyS1	local_serial	On-demand	Not Supported
<input type="checkbox"/>	ttyS2	ttyS2	local_serial	Disabled	Not Supported

Default – make this the default

Bounce DTR – puts the DTR and RTS pins DOWN – waits 500ms, then put those pins UP.

Device Types

When a device is added, the *Add* dialog is modified by the **Type** selection.

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 capabilities.

For console access via SOL, on the server make sure to enable BIOS console redirect and OS console redirect (typically for Linux OS).

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
- Data 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.

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 set:

For **End Point**, select **Appliance** radio button.

On **End Point**, select **KVM Port** radio button.

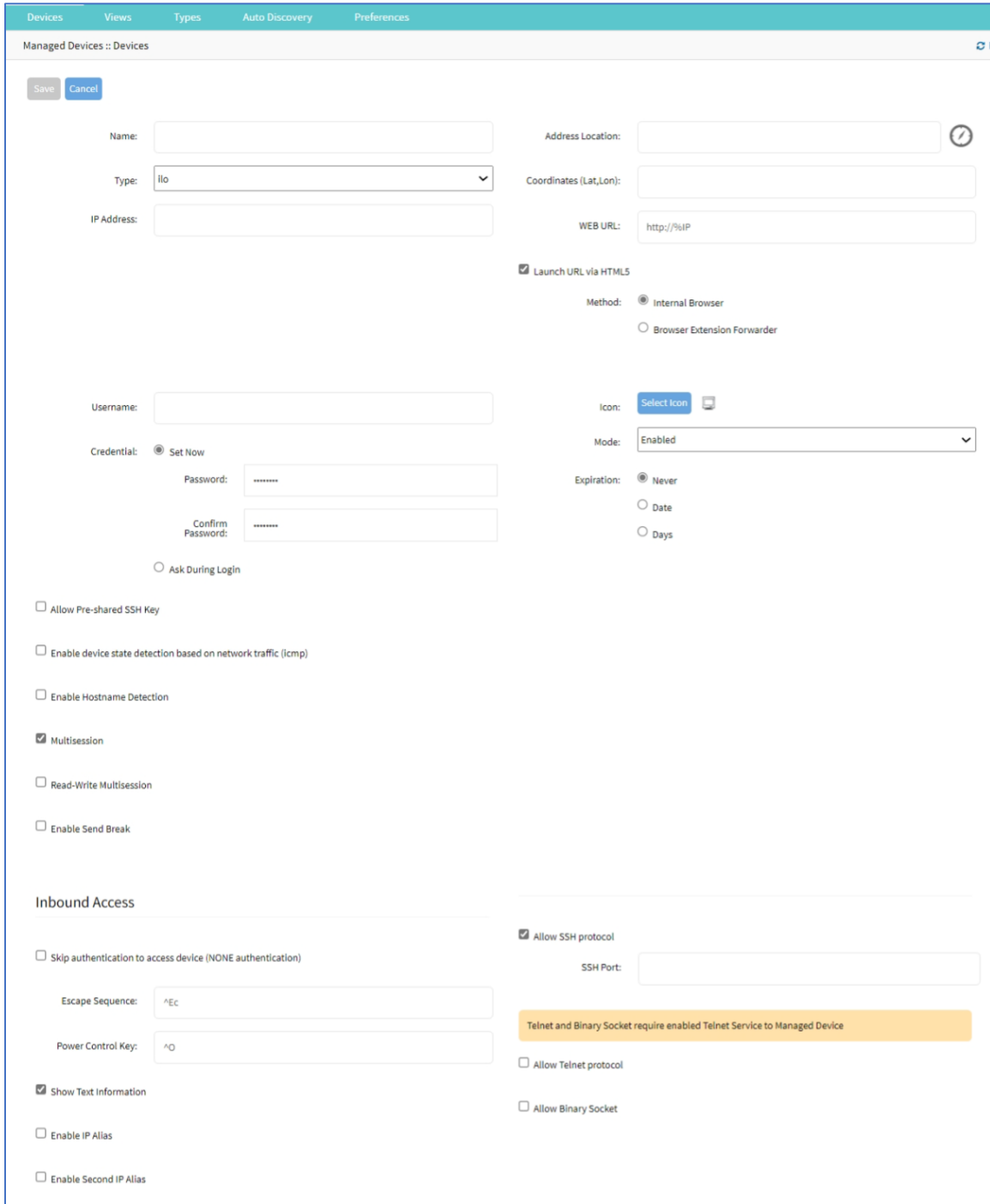
Device Procedures

Add Device

NOTE: *Add* dialog changes based on **Type** drop-down selection.

WebUI Procedure

1. Go to *Managed Devices :: Devices*,
2. Click **Add** (displays dialog).



3. Enter the **Name** (of the server).
4. In the **Type** drop-down, select one (see options, based on selection).

+++++

Service Processor devices (ilo, imm, drac, drac6, idrac7, ilom, ipmi_1.5, ipmi_2.0, intel_bmc).

Enter **IP Address** (reachable by the Nodegrid Platform).

+++++

Infrabox devices (infrabox)

Enter **IP Address** (reachable by the Nodegrid Platform).

+++++

Netapp devices (netapp)

Enter **IP Address** (reachable by the Nodegrid Platform).

+++++

Cisco UCS Blade devices (cimc_ucs)

Enter **IP Address** (reachable by the Nodegrid Platform).

Enter the **Chassis ID**.

Enter the **Blade ID**.

+++++

Virtual Console KVM devices (virtual_console_kvm)

Enter **IP Address** (reachable by the Nodegrid Platform).

Enter **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)

Enter **IP Address** (reachable by the Nodegrid Platform).

Enter **Port**.

+++++

PDU devices (pdu_apc, pdu_baytech, pdu_eaton, pdu_mph2, pdu_pm3000, pdu_cpi, pdu_raritan, pdu_geist, pdu_servertech, pdu_enconnex, pdu_cyberpower, pdu_rittal)

Enter **IP Address** (reachable by the Nodegrid Platform).

+++++

KVM Virtual Machine devices (virtual_console_kvm)

Name must match the hypervisor name.

Enter **IP Address** (reachable by the Nodegrid Platform).

+++++

KVM devices (kvm_dsr, kvm_mpu, kvm_aten, kvm_raritan)

Enter **IP Address** (reachable by the Nodegrid Platform).

+++++

5. Enter **Address Location** (a valid address for the device location).

Enter **Coordinates (Lat, Lon)** (if GPS is available, click **Compass** icon – or manually enter GPS coordinates).

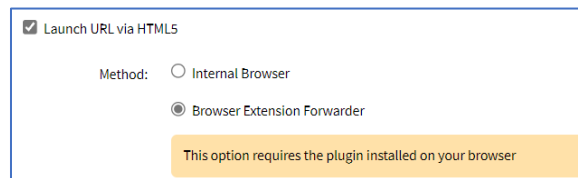
6. Enter **Web URL**.

7. Select **Launch URL via HTML5** checkbox (expands options).

In *Method* menu, select one:

Internet Browser radio button

Browser Extension Forwarder radio button (apply note instructions).



8. Enter **Username**

In *Credential* menu, select one:

Set Now radio button

Enter **Password** and **Confirm Password**.

Ask During Login radio button (user credentials are entered during login).

9. Select checkboxes, as needed:

Allow Pre-shared SSH Key checkbox.

Enable device state detection based on network traffic (icmp) checkbox.

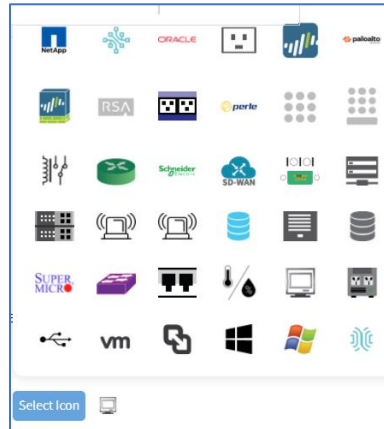
Enable Hostname Detection checkbox.

Multisession checkbox.

Read-Write Multisession checkbox.

Enable Send Break checkbox.

10. Click **Select Icon** .On the pop-up dialog, select an icon.



11. On **Mode** drop-down, select one (**Enabled, On-demand, Disabled**).

12. In *Expiration* menu, select one:

Never radio button

Date radio button

Enter **Date (YYYY-MM-DD)**.

Days radio button

Enter **Duration**.

13. In *End Point* menu, select one (*not available for service processors, virtual consoles*);

Appliance radio button

Serial Port radio button

Enter **Port Number**.

KVM Port radio button

Enter **Port Number**.

14. In *Inbound Access* menu:

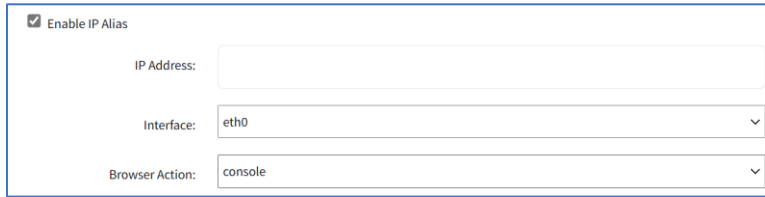
Select **Skip Authentication to access device (NONE authentication)** checkbox (if unselected, enter the following details).

Enter **Escape Sequence**.

Enter **Power Control Key**.

Select **Show Text Information** checkbox.

Select **Enable IP Alias**.



Enter **IP Address**.

On **Interface** drop-down, select one (**eth0, eth1, loopback, loopback1**).

On **Browser Action** drop-down, select one (**console, web**).

Select **Allow Telnet Protocol**.

Enter **TCP Socket Port**.

Select **Allow Binary Socket**.

Enter **TCP Socket Port**.

(optional) Select **Enable Second IP Alias** checkbox.

Enter **IP Address**.

On **Interface** drop-down, select one (**eth0, eth1, loopback, loopback1**).

On **Browser Action** drop-down, select one (**console, web**).

Select **Allow Telnet Protocol**.

Enter **TCP Socket Port**.

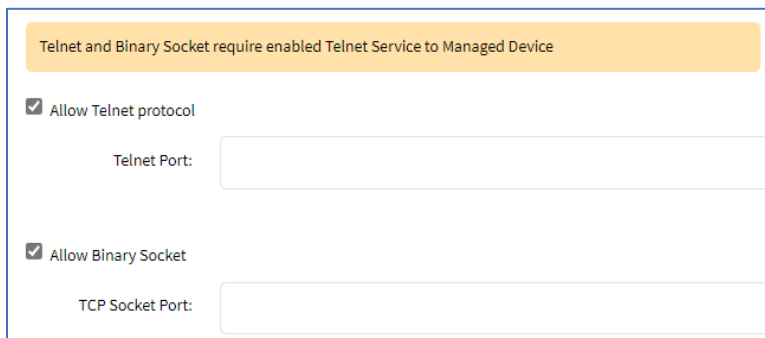
Select **Allow Binary Socket**.

Enter **TCP Socket Port**.

Select **Allow SSH protocol**.

Enter **SSH Port**.

At this location:



Select **Allow Telnet Protocol**.

Enter **TCP Socket Port**.

Select **Allow Binary Socket**.

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:

name

type

ip_address

username and password (of service processor)
or set credential ask_during_login

4. Save the changes with commit.

```
[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 requires two steps.

1. Add the PDU device. See *Add Device*.
2. Configure the PDU with the procedure below.

WebUI Procedure

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**.

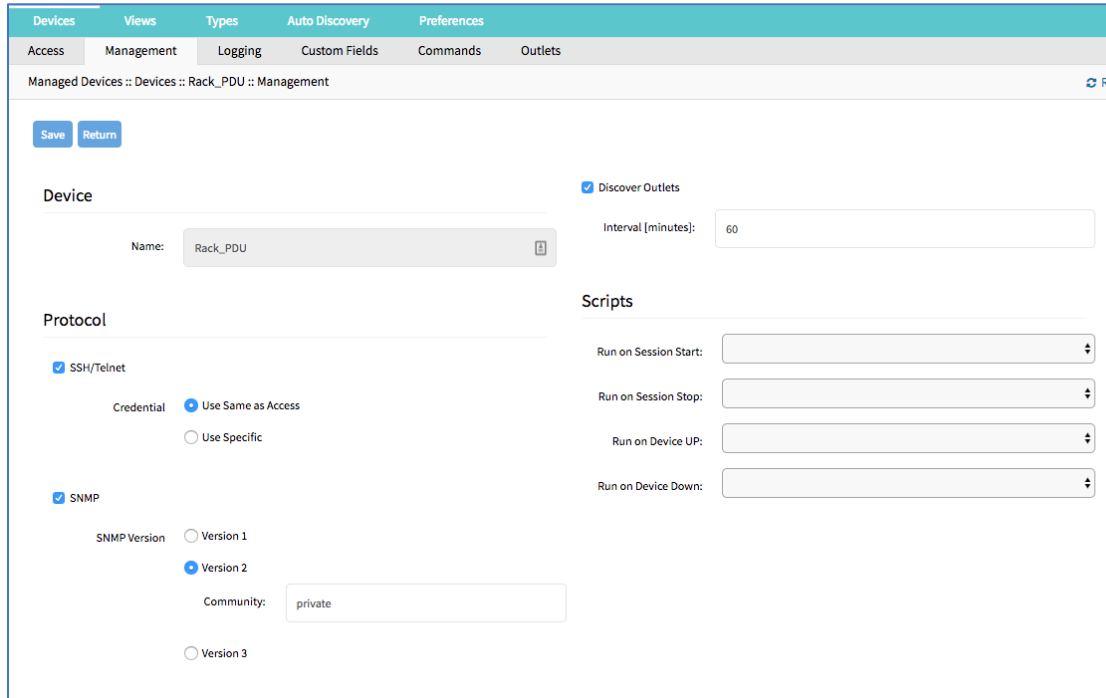
Devices		Views	Types	Auto Discovery	Preferences
Access	Management	Logging	Custom Fields	Commands	Outlets
Managed Devices :: Devices :: Rack_PDU :: Commands					
<input type="button" value="Return"/> <input type="button" value="Add"/> <input type="button" value="Delete"/>					
<input type="checkbox"/>	Command	Command Status	Protocol	Protocol Status	
<input type="checkbox"/>	Console	Enabled	SSH	Enabled	
<input type="checkbox"/>	Data Logging	Disabled	None	Not Applicable	
<input type="checkbox"/>	Outlet	Enabled	SSH	Enabled	
<input type="checkbox"/>	Web	Enabled	HTTP/S	Enabled	

4. On the **Protocol** drop-down, select **SNMP**.
5. Click **Save**.

Devices		Views	Types	Auto Discovery	Preferences
Access	Management	Logging	Custom Fields	Commands	Outlets
Managed Devices :: Devices :: Rack_PDU :: Commands					
<input type="button" value="Save"/> <input type="button" value="Return"/>					
	Command:	Outlet			
	<input checked="" type="checkbox"/> Enabled				
	Protocol:	SNMP			
<div style="background-color: #fff9c4; padding: 5px;">The command will only be available if the protocol it uses is enabled under management.</div>					

6. On the **Management** tab:
In the *SNMP* menu, update values to match the Rack PDU settings (see manufacturer’s manual).
7. Click **Save**.

NOTE: Use SNMP settings to provide read and write access. Read-Only credentials can not control power outlets.



The screenshot shows the configuration page for a device named 'Rack_PDU'. The 'Management' tab is selected, and the 'Discover Outlets' checkbox is checked. The interval for discovering outlets is set to 60 minutes. Under the 'Protocol' section, 'SSH/Telnet' and 'SNMP' are both checked. For 'SNMP', 'Version 2' is selected, and the community string is 'private'. There are also dropdown menus for 'Run on Session Start', 'Run on Session Stop', 'Run on Device UP', and 'Run on Device Down'.

8. 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.

6. The Rack PDU Outlets are automatically discovered (may need a few minutes, depending on the Rack PDU).

```
[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_community = private
[+admin@nodegrid management]# commit
```

Edit Device

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. In the *Name* column, locate device and select checkbox.
3. Click **Edit** (displays dialog).
4. Make changes, as needed.
5. Click **Save**.

Delete Device

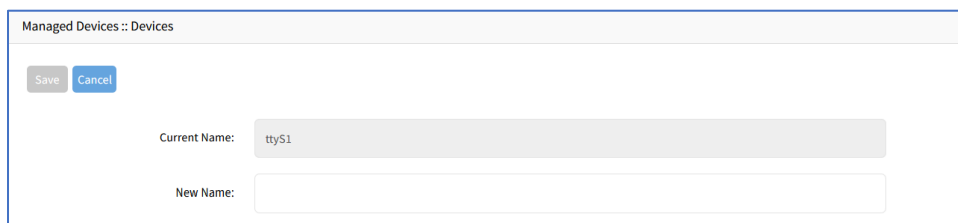
WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. In the *Name* column, locate device and select checkbox.
3. Click **Delete**.
4. On confirmation pop-up dialog, click **OK**.

Rename Device

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. In the *Name* column, locate device and select checkbox.
3. Click **Rename** (displays dialog).



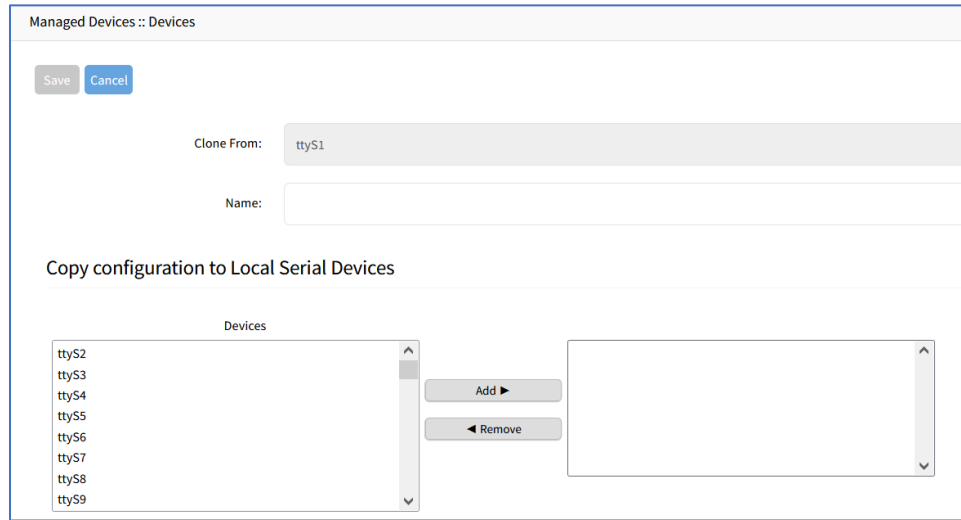
4. Enter **New Name**.

5. Click **Save**.

Clone Device

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. In the *Name* column, locate device and select checkbox.
3. Click **Clone** (displays dialog).



4. Enter **Name**.
5. In *Copy configuration to Local Serial Devices* section:
 - Select from left-side panel, click **Add ►** to move to right-side panel.
 - To remove from right-side panel, select, and click **◀ Remove**.
6. Click **Save**.

Enable/Disable Device

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. In the *Name* column, locate device and select checkbox.
3. Click **Enable**. (to enable device).
4. Click **Disable** (to disable device).

Set Device to On-Demand

WebUI Procedure

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 it's original factory settings.

WebUI Procedure

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.

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. In the *Name* column, locate device and select checkbox.
3. Click **Bounce DTR**.

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**.

Devices	Views	Types	Auto Discovery	Preferences
Access	Management	Logging	Custom Fields	Commands
Managed Devices :: Devices :: ttyS2 :: Access				

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**.

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 type of device, the details will change. Details provided here is the serial port configuration.

WebUI Procedure

1. Go to *Managed Devices :: Devices :: <device name> :: Access*.

Devices
Views
Types
Auto Discovery
Preferences

Access
Management
Logging
Custom Fields
Commands

Managed Devices :: Devices :: ttyS1 :: Access

Save Return

Name:

Local Serial Port:

Type:

Address Location:

Coordinates (Lat,Lon):

WEB URL:

Launch URL via HTML5

Icon: Select Icon

Mode:

Allow Pre-shared SSH Key

Baud Rate:

Parity:

Flow Control:

Data Bits:

Stop Bits:

RS-232 signal for device state detection:

Enable device state detection based in data flow

Enable Hostname Detection

Multisession

Read-Write Multisession

Enable Serial Port Settings via Escape Sequence

Inbound Access

Skip authentication to access device (NONE authentication)

Escape Sequence:

Power Control Key:

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

Telnet Port:

Allow Binary Socket

2. Configure location details:

Enter **Address Location** (can use **Compass** icon).

Enter **Coordinates**.

Enter **Web URL**.

Select **Launch URL via HTML5** checkbox (default: enabled).

3. Select **Allow Pre-shared SSH Key** checkbox.

4. Configure port settings:

On **Baud Rate** drop-down, select one (speed matching device settings) or (**Auto, 9600, 19200, 38400, 57600, 115200**).

On **Parity** drop-down, select one (**None**-default, **Odd, Even**)

On **Flow Control** drop-down, select one (**None**-default, **Software, Hardware**)

On **Data Bits** drop-down, select one (**5,6,7,8**-default).

On **Stop Bits** drop-down, select one (**1**-default, **2**).

On **RS-232 signal for device state detection** drop-down, select one (**Auto, DCD, CTS, None**).

5. Serial settings:

Select **Enable device state detection based in data flow** checkbox.

Select **Enable Hostname Detection** checkbox.

Select **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.).

Select **Read-Write Multisession** checkbox (If enabled, all connected users have read-write access to the session).

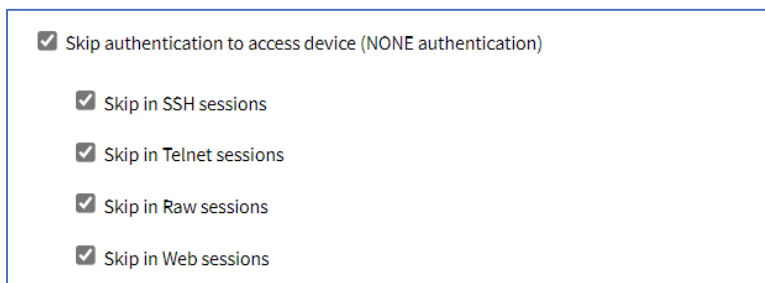
Select **Enable Serial Port Settings via Escape Sequence** checkbox.

6. Click **Select Icon** .On the pop-up dialog, select an icon.

7. On **Mode** drop-down, select one (**Enabled, On-Demand, Disabled**)

8. In *Inbound Access* menu:

Select **Skip authentication to access device (NONE authentication)** checkbox (displays dialog).



Select **Skip in SSH sessions** checkbox (default: enabled).

Select **Skip in Telnet sessions** checkbox (default: enabled).

Select **Skip in Raw sessions** checkbox (default: enabled).

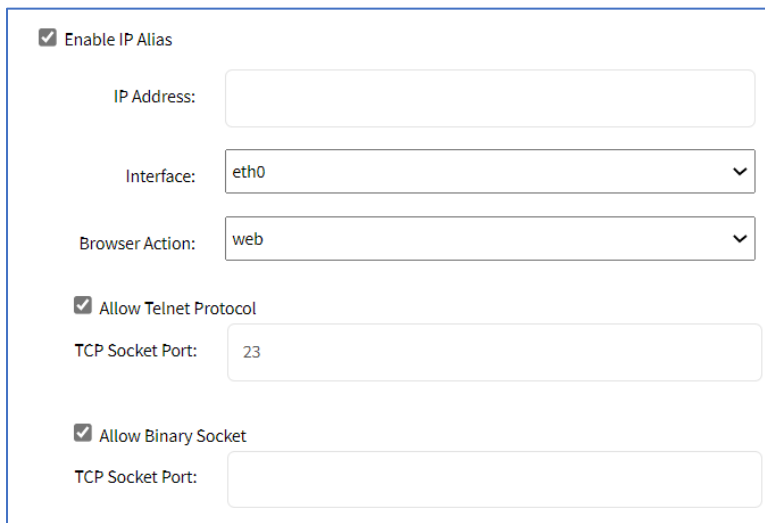
Select **Skip in Web sessions** checkbox (default: enabled).

Enter **Escape Sequence** (default: ^Ec – Ctrl+Shift+E+c).

Enter **Power Control Key** (default: ^O – Ctrl+Shift+O).

Select **Show Text Information** checkbox.

Select **Enable IP Alias** checkbox (user can connect to a device with IP addresses).

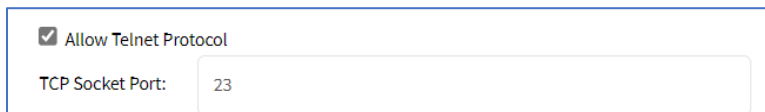


Enter **IP Address**.

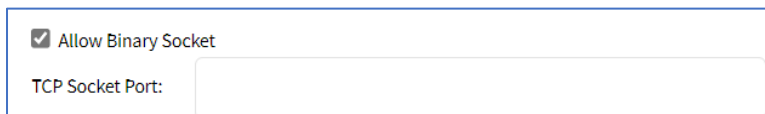
On **Interface** drop-down, select one (**backplane0**, **eth0**, **loopback**).

On **Browser Action** drop-down, select one (**console**, **web**).

Select **Allow Telnet Protocol**. Enter **TCP Socket Port** (default: 23).

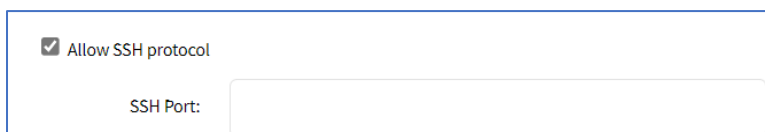


Select **Allow Binary Socket** checkbox. Enter **TCP Socket Port**.



Select **Enable Second IP Alias** checkbox (same dialog as **Enable IP Alias**).

Select **Allow SSH protocol** checkbox. Enter **SSH Port**.



Select **Allow Telnet protocol** checkbox. Enter **Telnet Port**.

Allow Telnet protocol
 Telnet Port:

Select **Allow Binary Socket** checkbox. Enter **TCP Socket Port**.

Allow Binary Socket
 TCP Socket Port:

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.

```
[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
```

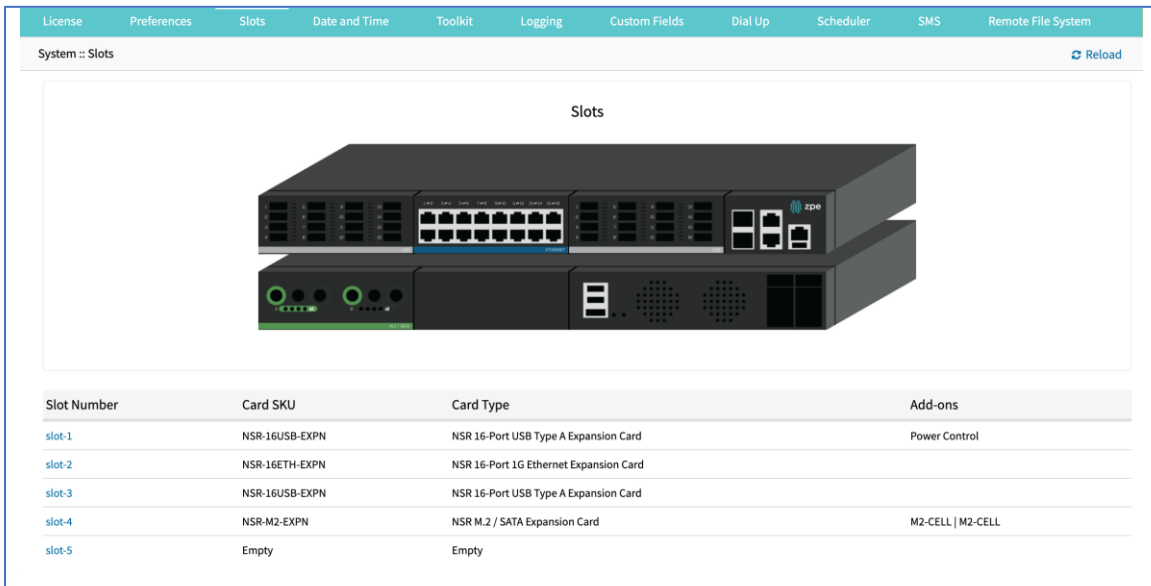
```

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 = ^0
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

WebUI Procedure

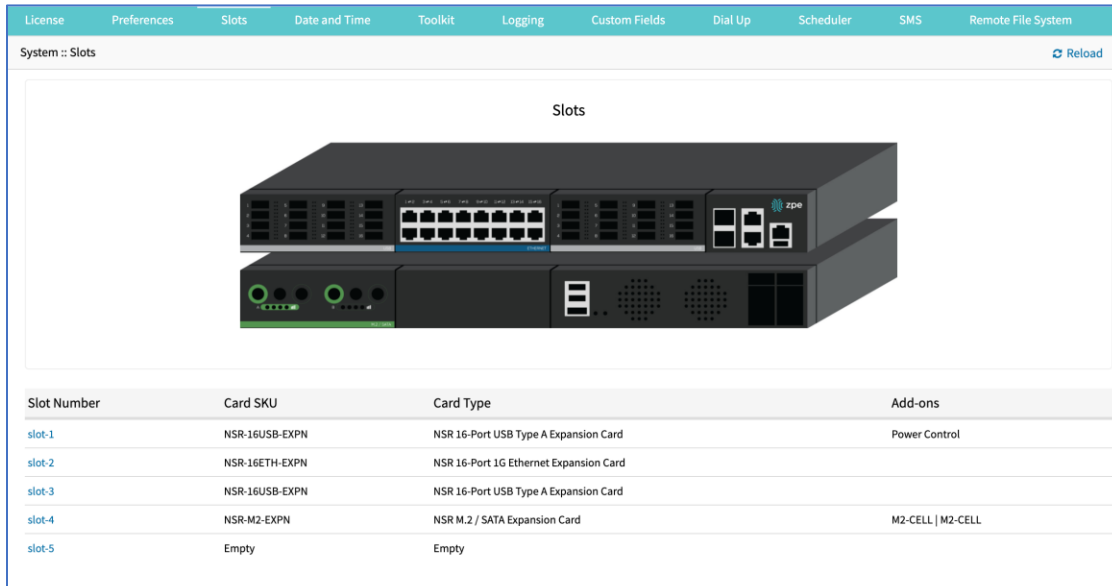
1. To confirm the USB card supports USB Passthrough, go to *System :: Slots :: Supported cards* . Check the *Add-ons* column for an entry: **Power Control**.



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-16USB-EXPN	NSR 16-Port USB Type A Expansion Card	
slot-4	NSR-M2-EXPN	NSR M.2 / SATA Expansion Card	M2-CELL M2-CELL
slot-5	Empty	Empty	

2. Go to *Managed Devices :: Devices*.

- On the list, locate the USB and click the **Name** (displays dialog).
- On the **Access** tab, *USB Mode* menu:



Select **Host** radio button:

USB Mode: Host

Initial State:

Passthrough

On **Initial State** drop-down, select one (**On, Off, Last State**).

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.

Select **Passthrough** radio button:

Type:

USB Mode: Host

Passthrough

Peer USB Port:

NOTE: When a device’s Passthrough mode is enabled, its peer is also set to Passthrough mode.

- Click **Save**.

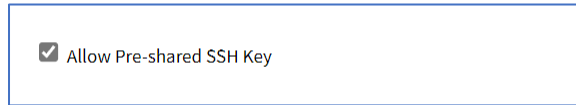
Configure SSH Key Authentication

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).

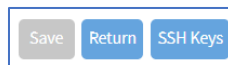
NOTE: Not all devices support this feature

Enable SSK Key Authentication WebUI Procedure

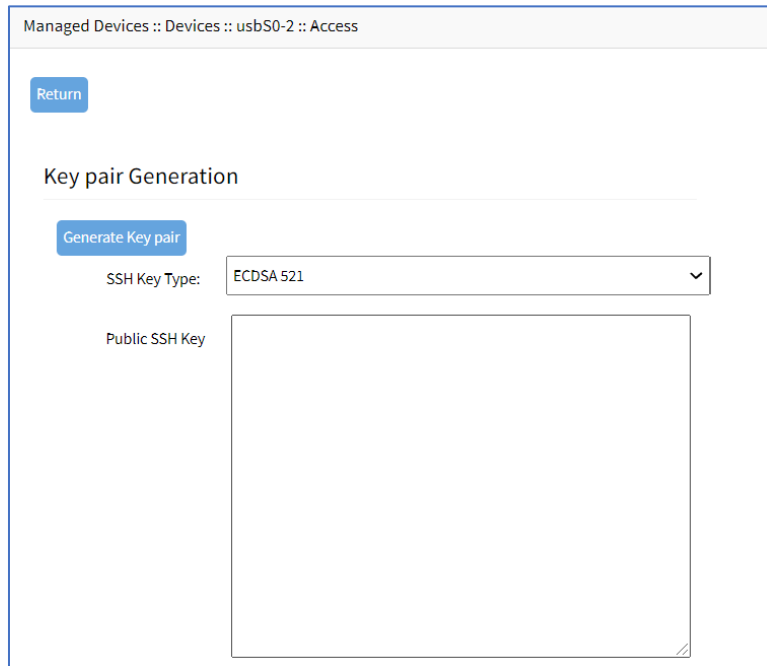
1. Go to *Managed Devices :: Devices :: <device name> :: Access*.
2. Select **Allow Pre-shared SSH Key** checkbox.



3. Click **Save**.
4. The **SSH Keys** button appears next to the **Save** and **Return** buttons.



5. Click **SSH Keys** (displays 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**).
7. Click **Generate Pair Keys**.

- For **Password Use** setting, select **Use Same as Access** for the current account. Alternatively, select **Use Specific** and set new **Password** with **Confirm Password**.

- Click **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.

- Click **Return** (goes back to the **Access** sub-tab view).

Enable Break Signal

NOTE: Not available for: usb_kvmm, usb_sensor, usb_device, local_serial.

When this is enabled, users can send a break signal via the SSH console session. This is enabled on a per-device basis. The break sequence is configurable.

WebUI Procedure

- Go to *Managed Devices :: Devices :: <device name> :: Access*.
- Scroll down to this section.

- Select the **Enable Send Break** checkbox.
- (optional) Enter a new **Break Sequence**.
- Click **Save**.

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/cmcpkbfablakhlhgdmhkedpoengpik>
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**.

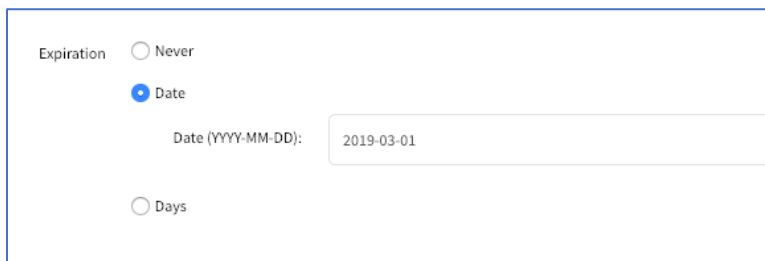
Set Device Expiration (IP-based devices only)

Each device has a defined expiration date or days. Once expired, the device automatically becomes unavailable (default: Never). The device and data remains in the system until removed by an admin.

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.

WebUI Procedure

1. Go to *Managed Devices :: Devices :: <device name> :: Access*.
2. Scroll to this section.



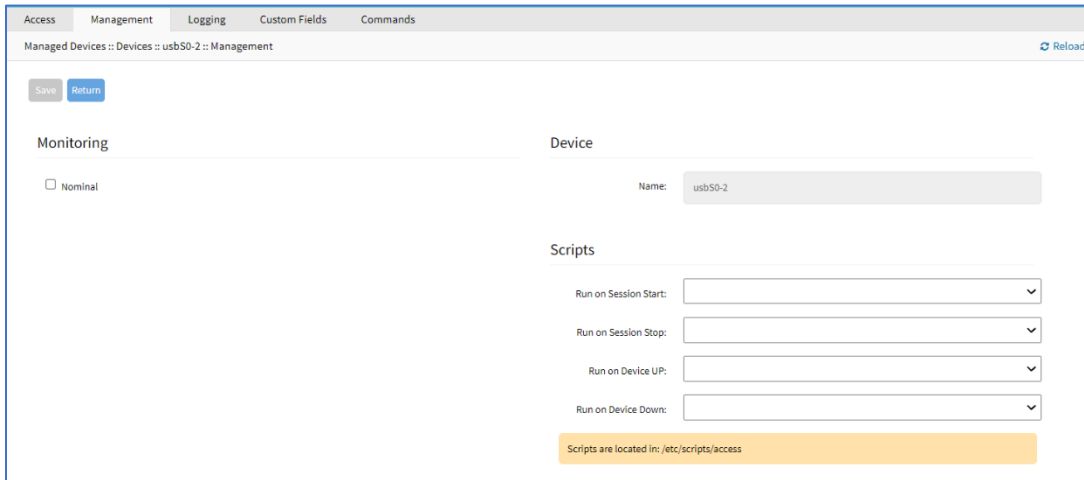
3. In the *Expiration* menu, select radio button for: **Never**, **Expiration Date** or **Expiration Days** and provide an appropriate value.

Date (YYYY-MM-DD) The device is available until the specified date. After that date, it is set to Disabled mode, and the admin user has 10 days to take action. After 10 days, the device and its data is removed from the system.

Days (between 1 and 9999999999) If no update on the device's configuration after the specified days, the device and its data is removed from the System (similar to a timeout).

4. Click **Save**.

Management sub-tab

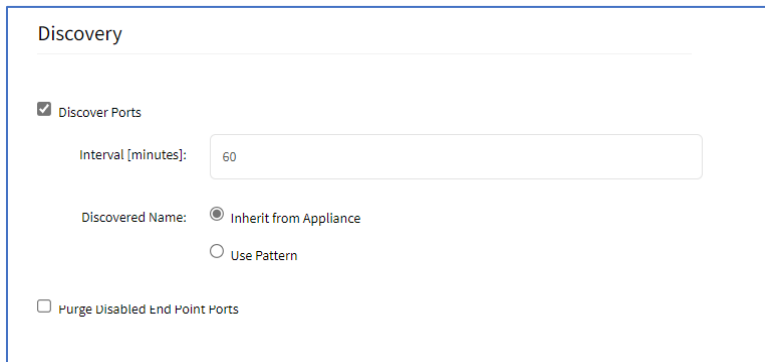


Configure Discovery (Appliances only)

This configures the discovery process for the Appliance (i.e., Console Server).

WebUI Procedure

1. Go to *Managed Devices :: Devices :: <device name> :: Management*.
2. Scroll to this section.



3. Select **Discovery Ports** checkbox.

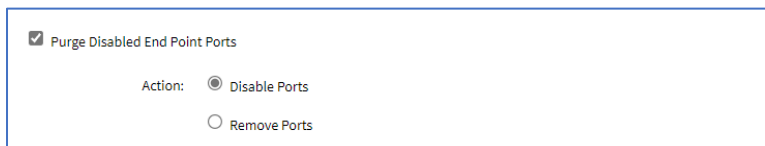
Enter **Set Interval (minutes)**.

In *Discovered Name* menu, select one:

Inherit from Appliance radio button

Use Pattern radio button

4. (optional) Select **Purge Disabled End Point Ports** checkbox.



5. Click **Save**.

Run Custom Scripts on Device Status Change

Users can assign custom scripts to specific device status changes. This is normally used when a specific status change occurs, and a pre-defined action is needed. The customer or a professional services provider can create the custom script.

Copy the scripts to `/etc/scripts/access` folder before assignment to a device status condition. Each script must be executable with user privileges.

WebUI Procedure

1. Go to *Managed Devices :: Devices :: <device name> :: Management*.
2. Scroll to this section.



3. In the *Scripts* menu, select an available script for the appropriate device status drop-down list:
 - On **Run on Session Start** drop-down, select one.
 - On **Run on Session Stop** drop-down, select one.
 - On **Run on Device UP** drop-down, select one.
 - On **Run on Device Down** drop-down, select one.
4. Click **Save**.

CLI Procedure

1. Go to `/settings/devices/<device name>/management`
2. Use the set command to assign a script to a device status
 - `on_session_start`
 - `on_session_stop`
 - `on_device_up`
 - `on_device_down`
3. Save the changes with commit.

```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/management/
[admin@nodegrid /]#set on_session_start=sessionstart.sh
```

```
[+admin@nodegrid management]#commit
```

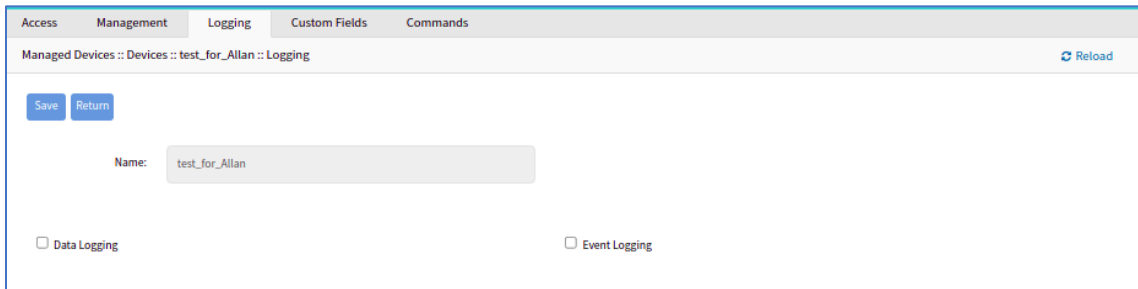
Logging sub-tab

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.

WebUI Procedure

1. Go to *Managed Devices :: Devices :: <device name> :: Logging*.
2. Scroll to this section.

Devices	Views	Types	Auto Discovery	Preferences
Access	Management	Logging	Custom Fields	Commands

Managed Devices :: Devices :: ttyS3 :: Logging

Name:

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

3. Select **Data Logging** checkbox.
4. Select **Enable data logging alerts** checkbox.
 Enter **Data String 1** (that triggers alert).
 On **Data Script 1** drop-down, select a script.
 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

```
[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.

WebUI Procedure

1. Go to *Managed Devices :: Devices :: <device name> :: Logging*.
2. Scroll to this section.

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:

Event Log Unit:

3. Select **Event Logging** checkbox.
4. Select **Enable Event Logging Alerts** checkbox.
 Enter **Event String 1** (that triggers alert).
 On **Event Script 1** drop-down, select one.
 Repeat for additional triggers.
5. Adjust **Event Log Frequency** (1 min to 9999 hours) or **Event Log Unit** values, as needed
6. Click **Save**.

CLI Procedure

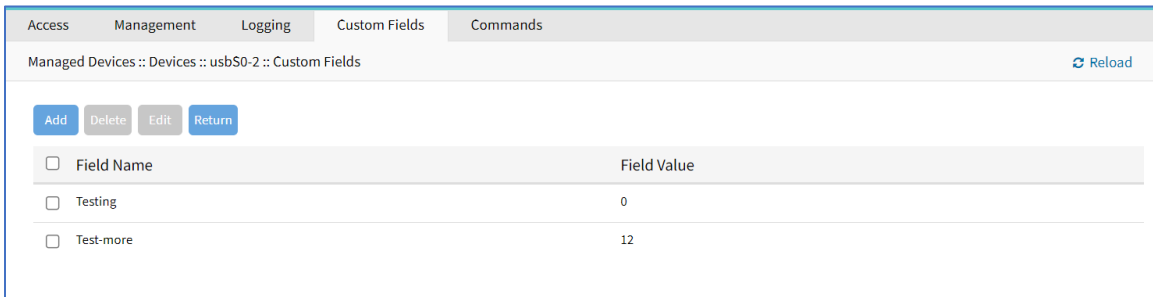
1. Go to /settings/devices/<device name>/logging
2. Use the set command to change the event_logging value to yes
3. Use the set command to adjust event_log_frequency and event_log_unit as needed:
 event_log_frequency range from 1 - 9999
 event_log_unit options hours or minutes
4. Use the set command 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

```
[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.



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)

Admin changes to the default command settings affect all users and require careful consideration.

Commands available on a device 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.

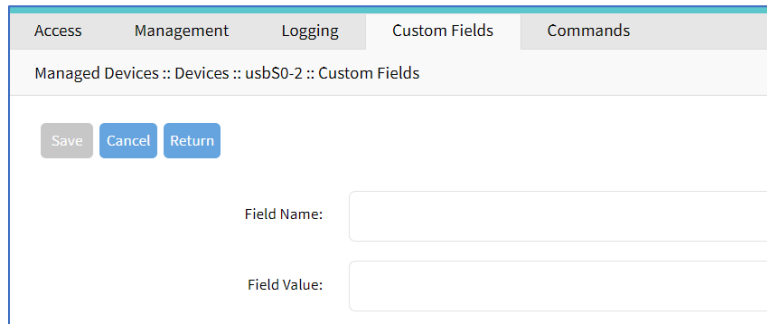
Custom Commands can be created with custom scripts, for all device types. Custom Commands can support for a wide range of different functions (such as additional session options and specific custom device tasks).

NOTE: Custom scripts can be created by the customer or a professional services provider.

Add Custom Field

WebUI Procedure

1. Go to *Managed Devices :: Devices :: <device name> :: Custom Fields*.
2. Click **Add** (displays dialog).

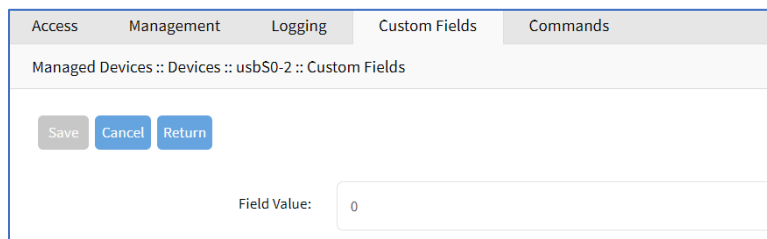


3. Enter **Field Name**.
4. Enter **Field Value**.
5. Click **Save**.

Edit Custom Field

WebUI Procedure

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

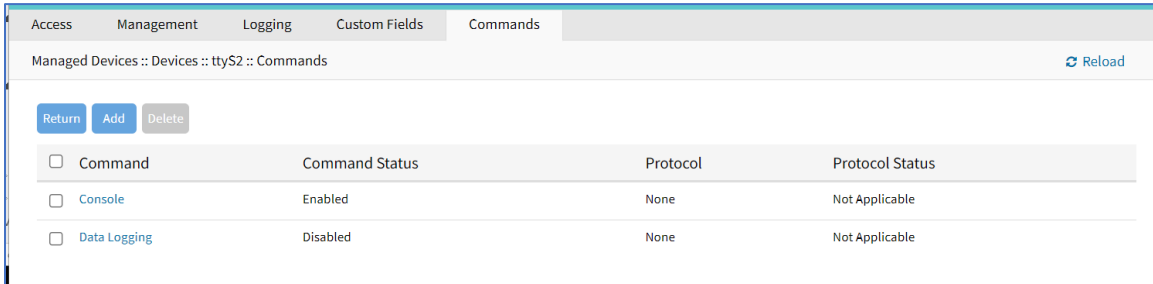
WebUI Procedure

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 pop-up 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.



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)
```

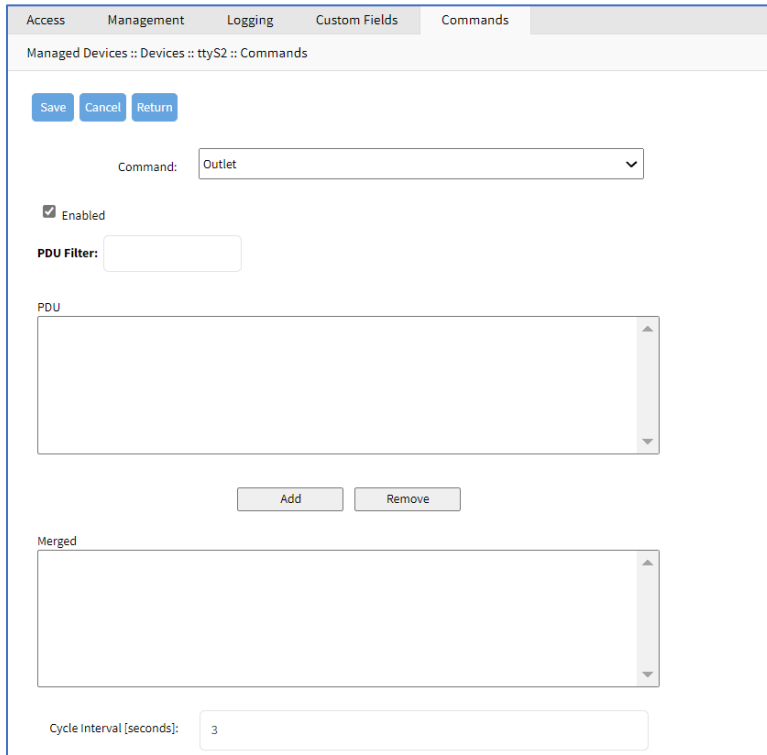
Create Commands (Outlet, SSH, Telnet, Web)

This integrates Out-of-Band and Console-like configurations with the In-Band command.

WebUI Procedure

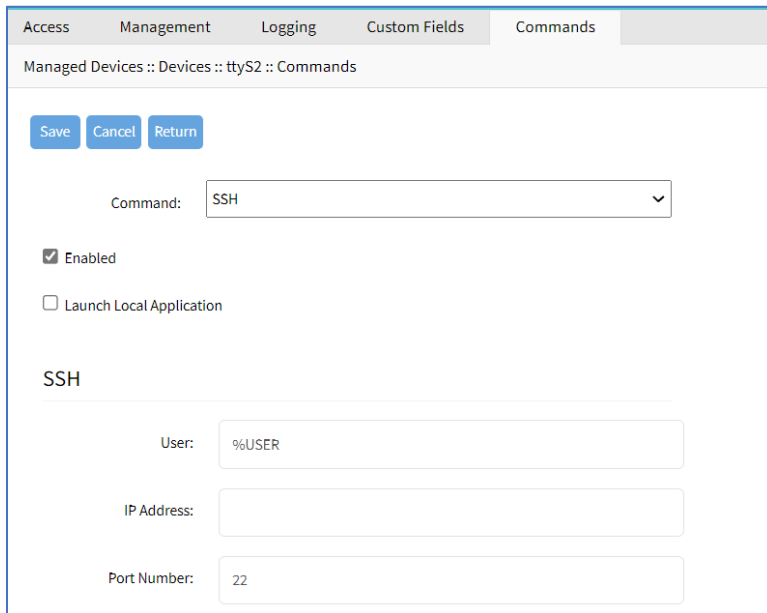
1. Copy the custom script into /etc/scripts/custom_commands
2. Go to *Managed Devices :: Devices :: <device name> :: Commands*.
3. Click **Add** (displays dialog).
4. In **Command** drop-down, select one (dialog changes depending on selection).

Command drop-down selection: **Outlet**. Enter details as needed.



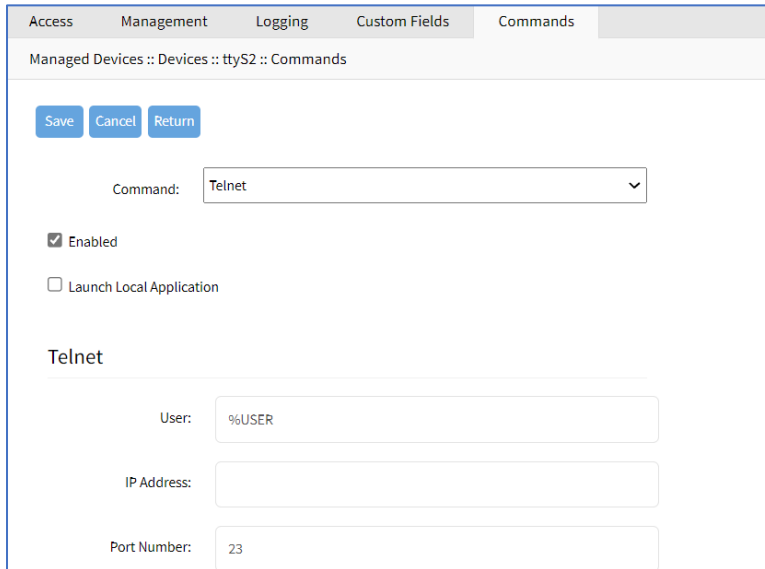
The screenshot shows the 'Commands' configuration page for a device. The breadcrumb trail is 'Managed Devices :: Devices :: ttyS2 :: Commands'. At the top, there are tabs for 'Access', 'Management', 'Logging', 'Custom Fields', and 'Commands'. Below the tabs are three buttons: 'Save', 'Cancel', and 'Return'. The 'Command' dropdown menu is set to 'Outlet'. There is a checked checkbox for 'Enabled' and an empty 'PDU Filter' text box. Below these are two large, empty text areas labeled 'PDU' and 'Merged', each with an 'Add' and 'Remove' button. At the bottom, the 'Cycle Interval [seconds]' is set to '3'.

Command drop-down selection: **SSH**. Enter details as needed.

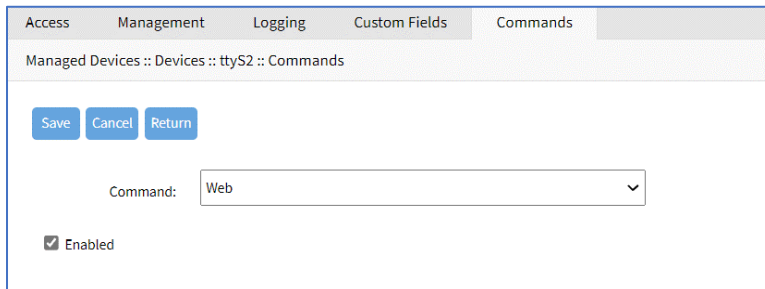


The screenshot shows the 'Commands' configuration page for a device. The breadcrumb trail is 'Managed Devices :: Devices :: ttyS2 :: Commands'. At the top, there are tabs for 'Access', 'Management', 'Logging', 'Custom Fields', and 'Commands'. Below the tabs are three buttons: 'Save', 'Cancel', and 'Return'. The 'Command' dropdown menu is set to 'SSH'. There is a checked checkbox for 'Enabled' and an unchecked checkbox for 'Launch Local Application'. Below these are three text input fields: 'User' with the value '%USER', 'IP Address' which is empty, and 'Port Number' with the value '22'.

Command drop-down selection: **Telnet**. Enter details as needed.



Command drop-down selection: **Web** (if available). Select **Enabled** checkbox.



5. When done, click **Save**.

Device Access via RDP

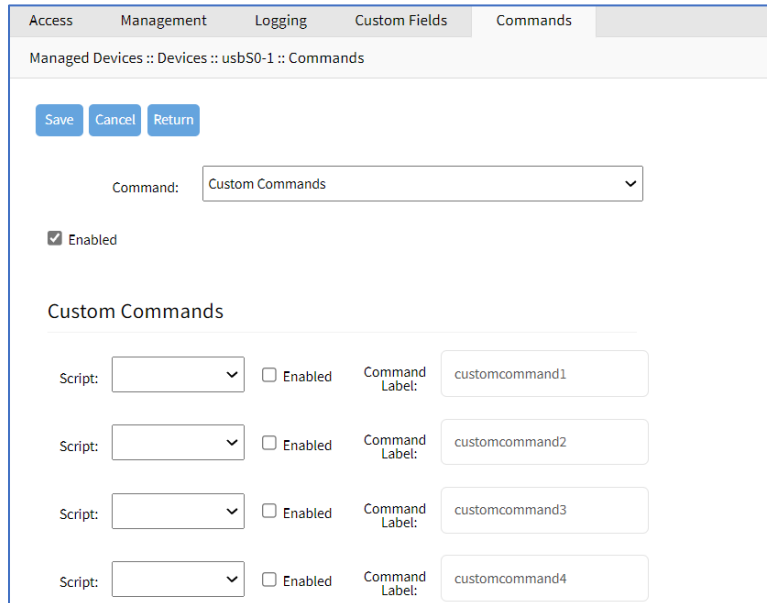
WebUI Procedure

1. Go to *Managed Devices :: Devices :: <device name> :: Commands*.
2. Click **Add** (displays dialog).
3. In **Command** drop-down, select **KVM**.
4. Select **Enabled** checkbox.
5. On **Protocol** drop-down, select one:
6. On **Type Extension** drop-down, select one.
7. Click **Save**.

Create Custom Commands

WebUI Procedure

1. Go to *Managed Devices :: Devices :: <device name> :: Commands*.
2. Click **Add** (displays dialog).



3. In **Command** drop-down, select **Custom Commands**.
4. Select **Enable** checkbox.
5. In *Custom Commands* menu
 On **Script** drop-down, select one.
 Next to drop-down, select **Enabled** checkbox.
 Adjust **Command Label** to match the command option in the script.
6. As needed, repeat for additional Scripts.
7. Click **Save**.

CLI Procedure

1. Go to `/settings/devices/<device name>/commands`
2. Use the add command to create a new custom field.
3. Use the set command to define a `field_name` and `field_value`.
4. Save the changes with `commit`

```
[admin@nodegrid /]# /settings/devices/Serial_Console/commands/
[admin@nodegrid /]#add
[+admin@nodegrid commands]#set command=custom_commands
[+admin@nodegrid commands]#set custom_command_enabled1=yes
[+admin@nodegrid commands]#set custom_command_script1=SSH.py
[+admin@nodegrid commands]#set custom_command_label1=SSH
```

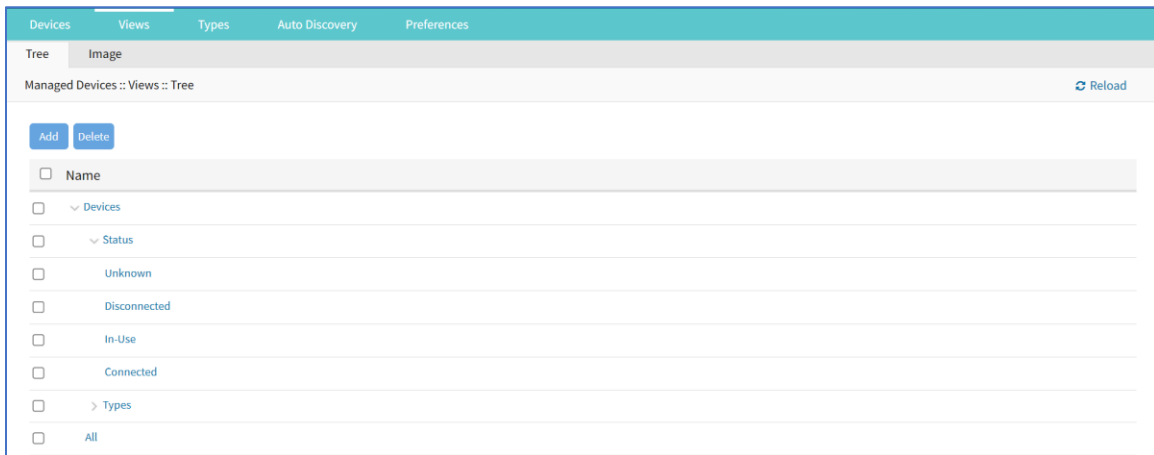
```
[+admin@nodegrid commands]#commit
```

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.




Tree sub-tab

This displays the tree structure. On first opening, the roots are shown: Devices, Appliances, Groups.



View Tree Branches

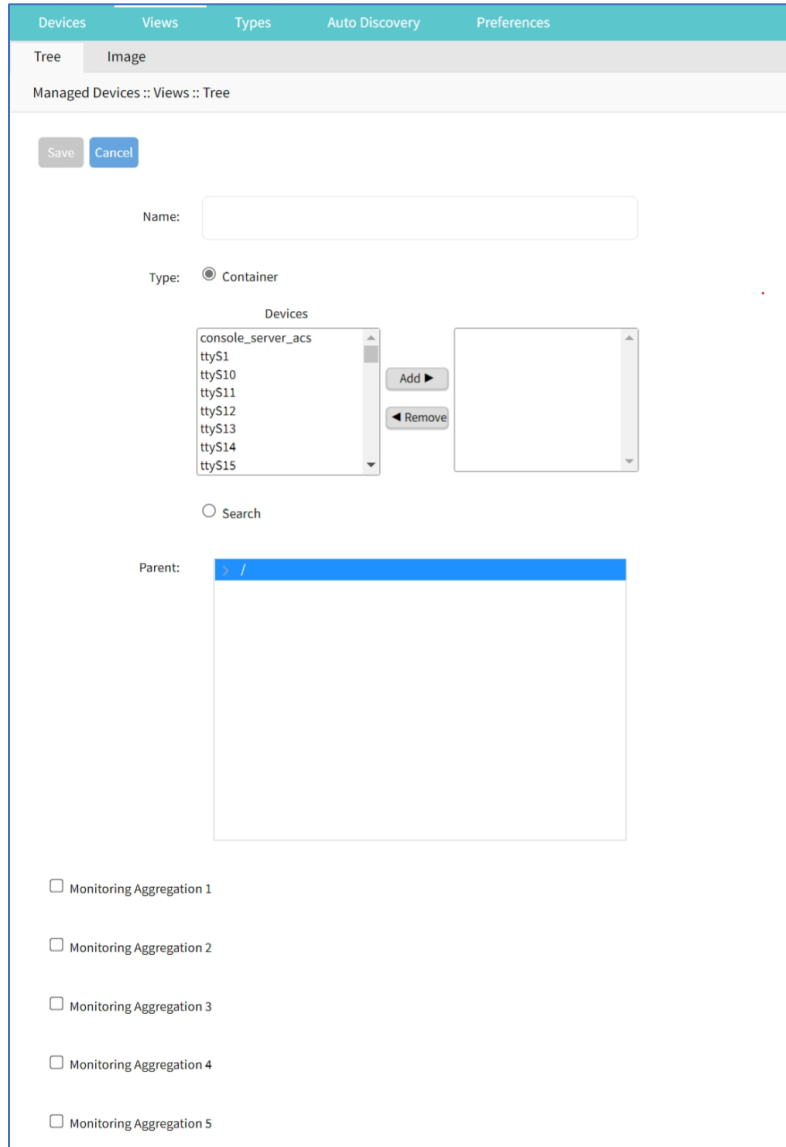
WebUI Procedure

1. Click the right  icon to display the next branch level.
2. If further branch levels are available, click the right  icon to expand the branch.
3. To contract the branch, click the down  icon.

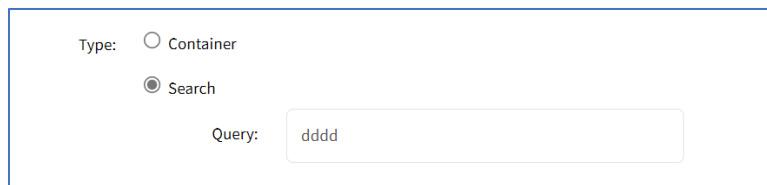
Add a Branch Item

WebUI Procedure

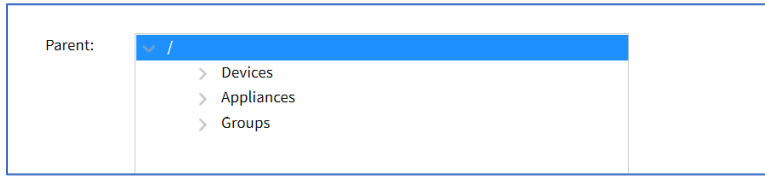
1. Go to *Managed Devices :: Views :: Tree*.
2. Click **Add** (displays dialog).



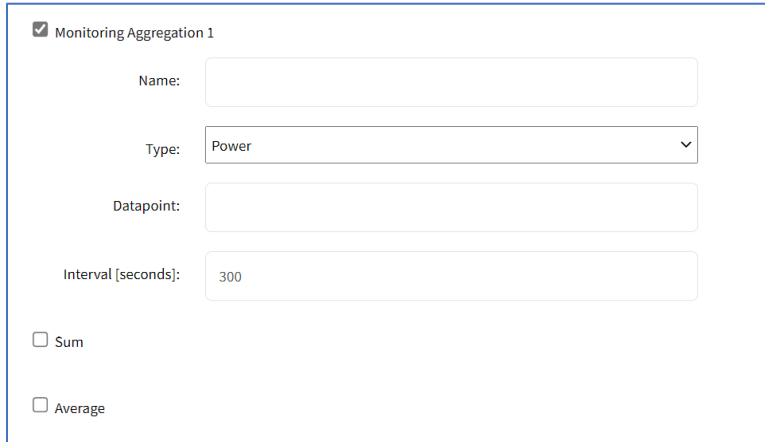
3. Enter a **Name**.
4. To include in *Contains*, in *Devices* panel:
 Select from left-side panel, click **Add** ► to move to right-side panel.
 To remove from right-side panel, select, and click **Remove** ◀.
5. To search for an item, select **Search** radio button. Opens a search dialog to locate and select.



6. To select a **Parent**, click on the solid bar, expand the tree to locate the parent for this addition.



7. As needed, select **Monitoring Aggregation** checkbox.



Enter **Name**

On **Type** drop-down, select one (**Power, Apparent Power, Power Factor, Current, Voltage, Frequency, Temperature, Humidity, Fan Speed, Time Left, Counter, Percent**).

Enter **Datapoint**.

Enter **Interval (seconds)**.

Select **Sum** checkbox or **Average** checkbox.

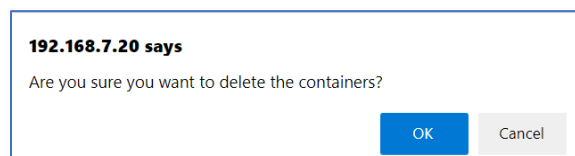
8. (as needed) Repeat for other **Aggregations**.

9. When done, click **Save**.

Delete a Branch Item

WebUI Procedure

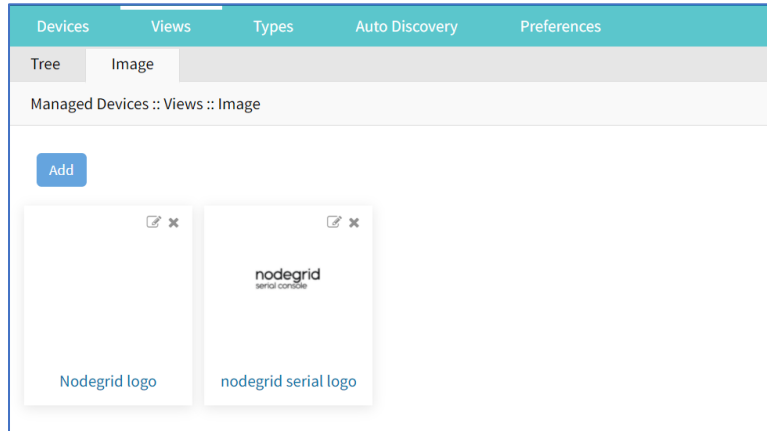
1. Go to *Managed Devices :: Views :: Tree*.
2. Click **Delete** (displays confirmation dialog).



3. Click **OK**.

Image sub-tab

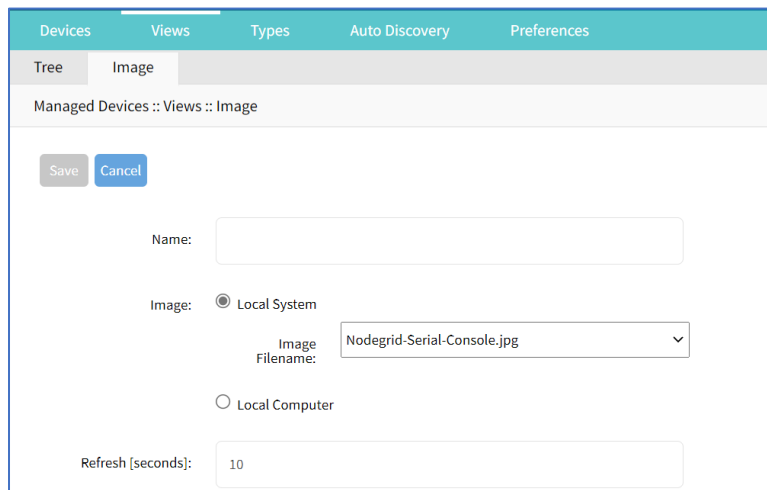
Available images are shown on this page.



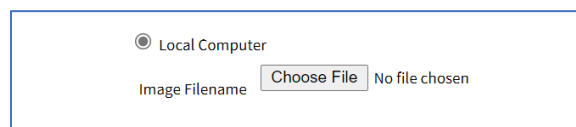
Add Image

WebUI Procedure

1. Go to *Managed Devices :: Views :: Image*.
2. Click **Add** (displays dialog).



3. Enter **Name**.
4. In *Image* menu:
 - Select **Local System** radio button, then select from the **Image Filename** drop-down.
 - Select **Local Computer** radio button.



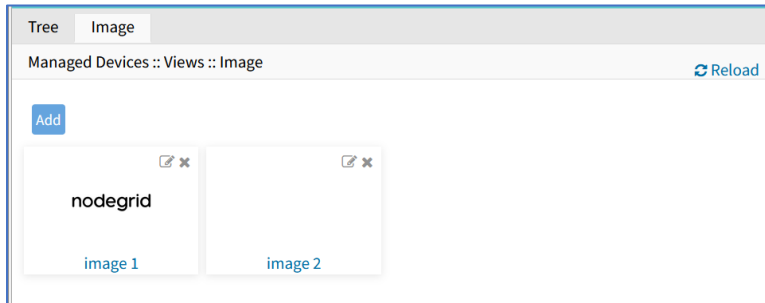
Click **Choose File**, then locate and select the graphic file.

5. Click **Save**.

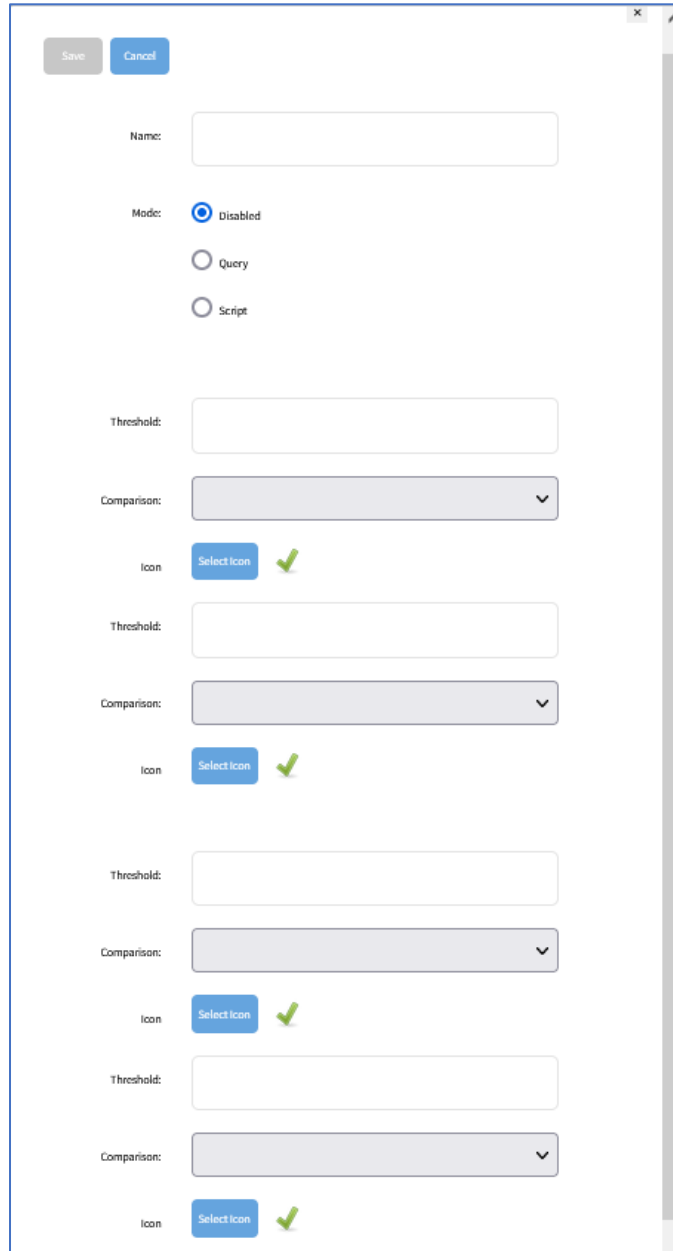
Add Image Property Details

WebUI Procedure

1. Go to *Managed Devices :: Views :: Image*.



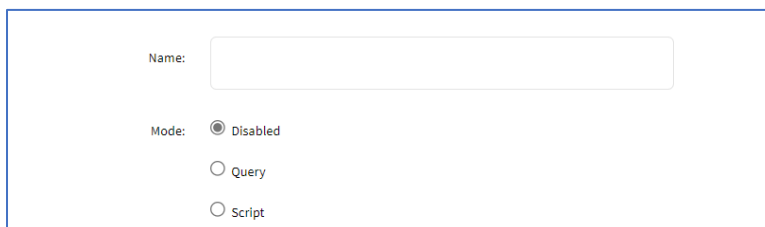
2. Click on an image to display.
3. Right-click on the image (displays properties dialog).



The screenshot shows a configuration window with a 'Save' button and a 'Cancel' button. Below these are four identical rows of configuration fields. Each row contains: a 'Name' text input field; a 'Mode' section with three radio buttons ('Disabled', 'Query', 'Script'), where 'Disabled' is selected; a 'Threshold' text input field; a 'Comparison' dropdown menu; and an 'Icon' section with a 'Select Icon' button and a green checkmark.

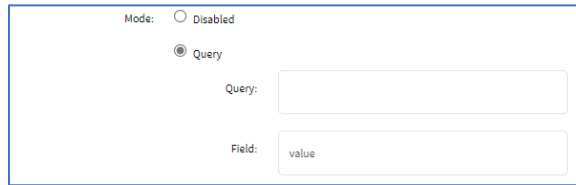
- 4. Enter **Name**.
- 5. In *Mode* menu, select one:

Disabled radio button:



This close-up shows the 'Name' text input field and the 'Mode' section. The 'Mode' section has three radio buttons: 'Disabled' (which is selected), 'Query', and 'Script'.

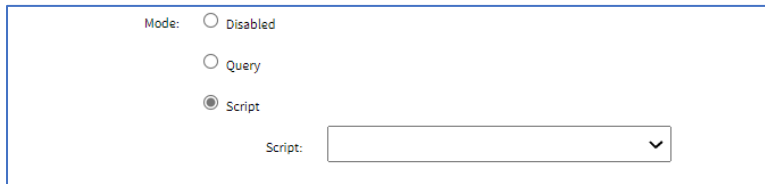
Query radio button:



Enter **Query**

Enter **Field**

Script radio button:



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

6. In *Threshold* menu:

Enter a **Threshold** value

On the **Comparison** drop-down select one

Click **Icon** and select from the dialog

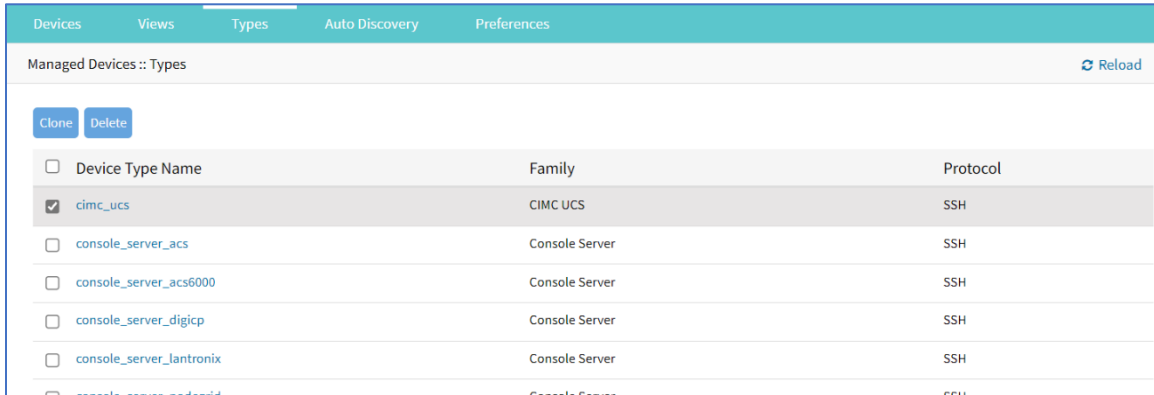


(as needed) Enter details for another Threshold (up to 4).

7. 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.

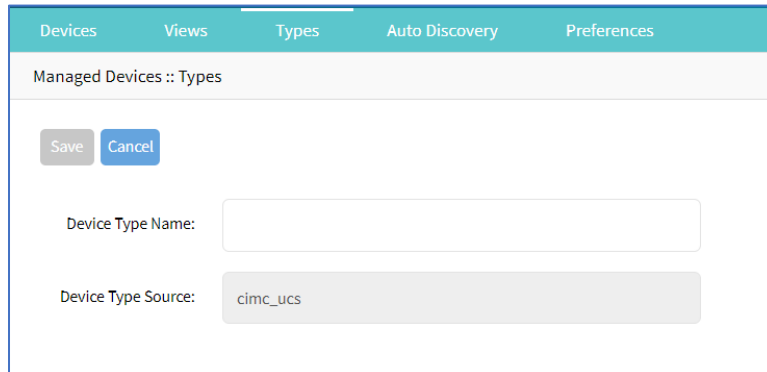


Manage Types

Clone a Type

WebUI Procedure

1. Go to *Managed Devices :: Types*.
2. Locate and select the checkbox of the type to be cloned.
3. Click **Clone** (displays dialog)



4. Enter **Device Type Name**.
5. Click **Save**.

Clone Validation

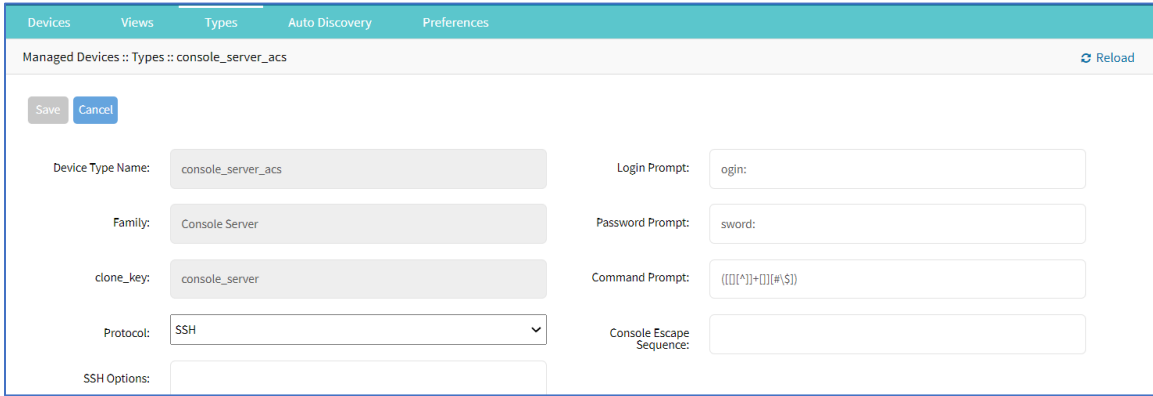
Ensure the source device is correctly configured. After the clone is created, use this verification process:

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 a Device Type

WebUI Procedure

1. Go to *Managed Devices :: Types*.
2. In the *Device Type Name* column, locate and click on the name.

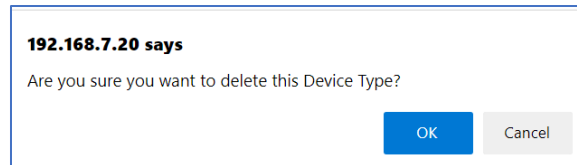


3. Modify details as needed:
4. Click **Save**.

Delete a Type

WebUI Procedure

1. Go to *Managed Devices :: Types*.
2. Locate and select the checkbox to be deleted.
3. Click **Delete** (displays confirmation dialog).



4. Click **OK**.

Auto Discovery tab

The System automatically discovers and adds network devices, enabled ports on console servers, KVM switches, and VMware (virtual serial ports and virtual machines).

Auto Discovery Configuration Process

Auto Discovery Process

This is the process to configure auto discovery on various devices.

1. Create a template device. (For each device type, a template device must be created.)

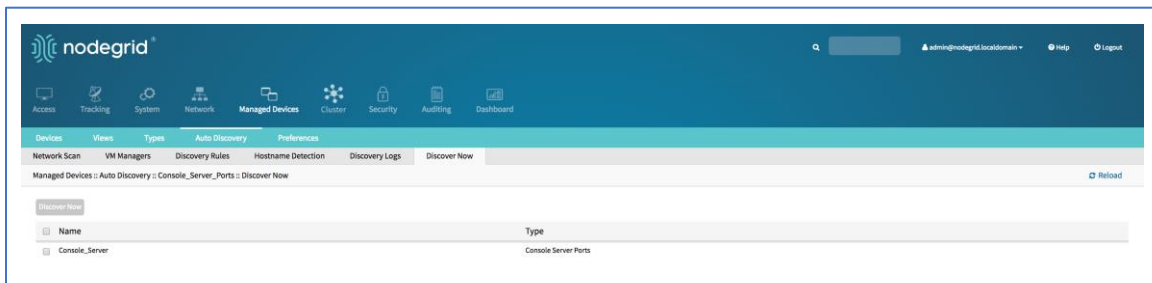
Clone is recommended. The template needs to include all the settings as for an end device, except connection details to the discovered devices.

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 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 Configurations

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.

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click **Add** (displays dialog).
3. Enter **Name** (of the template).
4. In the **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. In *End Point* menu, select one

Serial Port radio button.

KVM Port radio button.

Enter **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 settings:

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

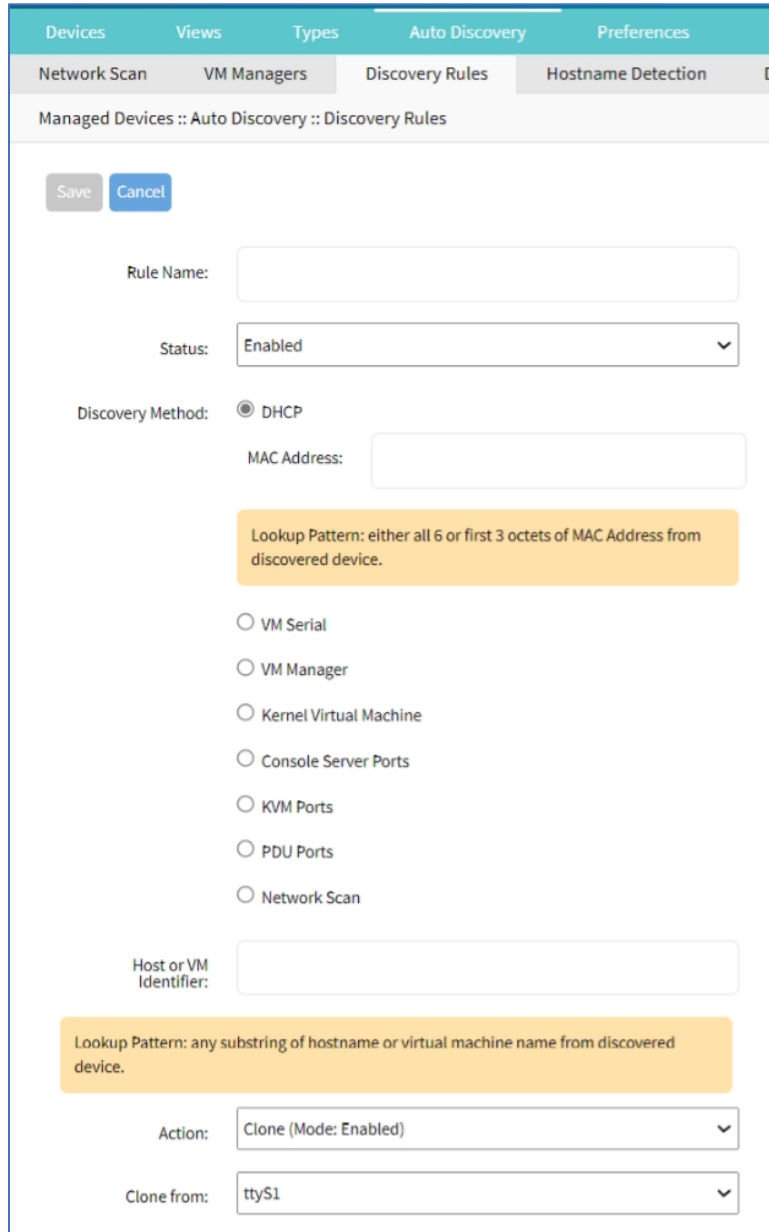
4. Save the changes with commit.

```
[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
```

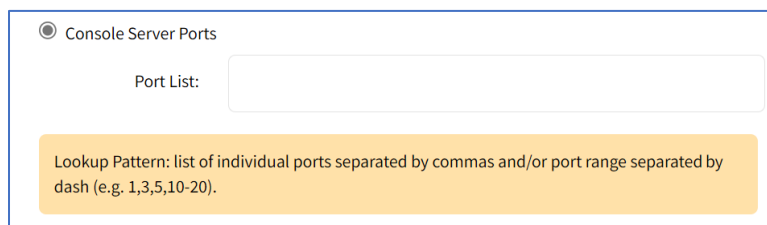
Step 2 – Create a Discovery Rule

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: Discovery Rules*.
2. Click **Add** (displays dialog).



3. Enter **Rule Name**.
4. On **Status** drop-down, select one (**Enabled, Disabled**).
5. In *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)).



KVM Ports radio button. Enter **Port List** (list of ports to scan (i.e., 1,3,5,10-20)).

KVM Ports

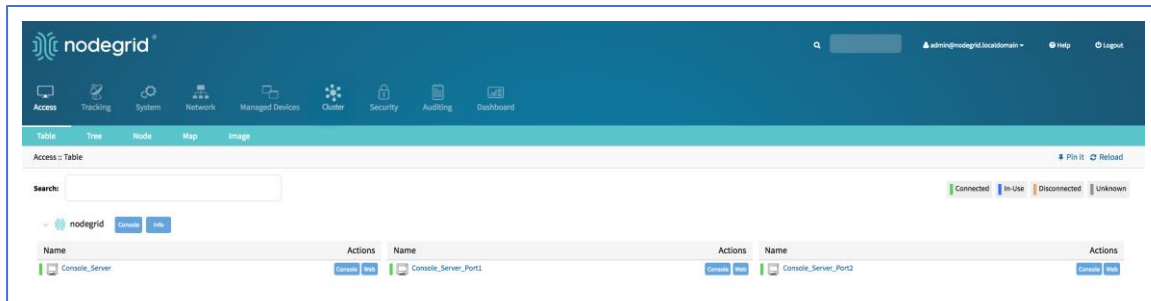
Port List:

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. In the **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.

```
[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 device must be created first. In this process, only enter the details listed.

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click **Add** (displays dialog).
3. Enter **Name** (of the template).
4. In the **Type** drop-down, select one (device_console, ilo, imm, drac, idrac6, ipmi1.5, impi2.0, ilom, cimc_ucs, netapp, infrabox, pdu).
5. For **IP Address**, enter **127.0.0.1**
6. Enter **Username**
7. Enter **Password** and **Confirm Password**.

Alternatively, select **Ask During Login** checkbox (user credentials are entered during login).

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 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.

```
[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

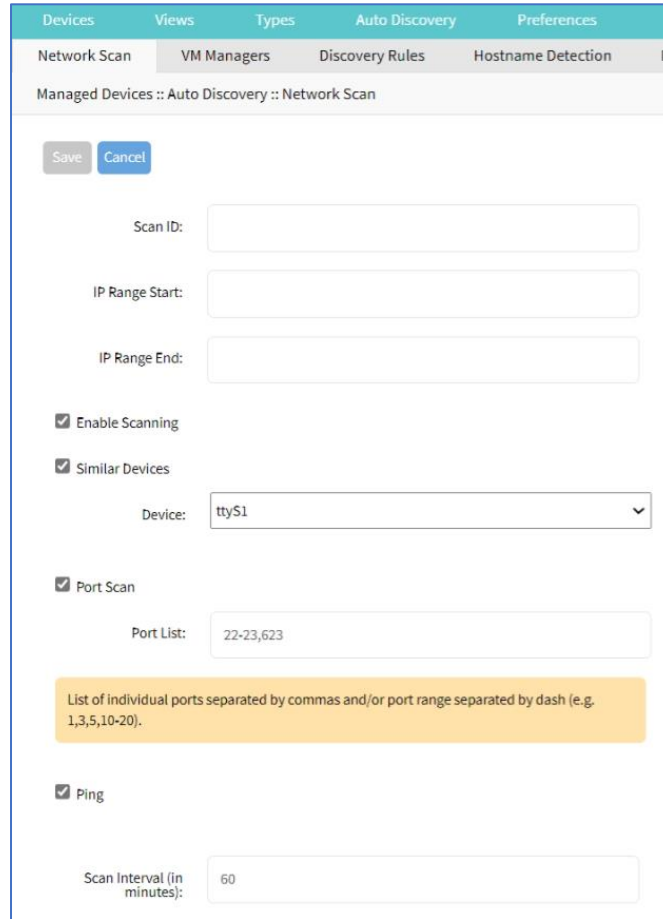
[admin@nodegrid {devices}]# set credential=set_now
[admin@nodegrid {devices}]# set username=admin password=admin

[admin@nodegrid {devices}]# set mode=disabled
[admin@nodegrid {devices}]# commit
```

Step 2 – Create a Network Scan

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: Network Scan*.
2. Click **Add** (displays dialog).



3. Enter **Name** (of Scan ID).
4. Enter **IP Range Start**.
5. Enter **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.
Enter **Port List** (ports to be scanned, i.e., 2, 3, 11-20).
9. Select **Ping** checkbox (enables Ping function).
10. In **Scan interval (in minutes)**, enter a value.
11. 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.

```
[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

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: Discovery Rules*.
2. Click **Add** (displays dialog).
3. Enter **Name** (of the Discovery Rule).
4. On **Status** drop-down, select (**Enabled, Disabled**).
5. In **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. In the **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 filter, 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`.

```
[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 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

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click **Add** (displays dialog).
3. Enter **Name** (of the template).
4. For **IP Address**, enter **127.0.0.1**
5. In the **Type** drop-down field, select one (device_console, ilo, imm, drac, idrac6, ipmi1.5, impi2.0, ilom, cimc_ucs, netapp, infrabox, pdu*).
6. Enter **Username**.
7. Enter **Password** and **Confirm Password**.
Alternatively, select **Ask During Login** checkbox (user credentials are entered during login).
8. Select **Mode Disabled** checkbox (ensures device is not displayed on 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 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.

```
[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

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: Discovery Rules*
2. Click **Add** (displays dialog).
3. 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. In the **Clone from** drop-down, select the 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.

```
[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 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.

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click **Add** (displays dialog).
3. Enter **Name** (of the template).
4. In the **Type** drop-down, select one (virtual_console_vmware).
5. For **IP Address**, enter **127.0.0.1**
6. Enter **Username**.
7. Enter **Password** and **Confirm Password**.

Alternatively, select **Ask During Login** checkbox (user credentials are entered during login).

8. Select **Mode Disabled** checkbox (ensures device is not displayed on 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 settings:

```
name
type (virtual_console_vmware)
ip_address as 127.0.0.1
set mode to disabled
```

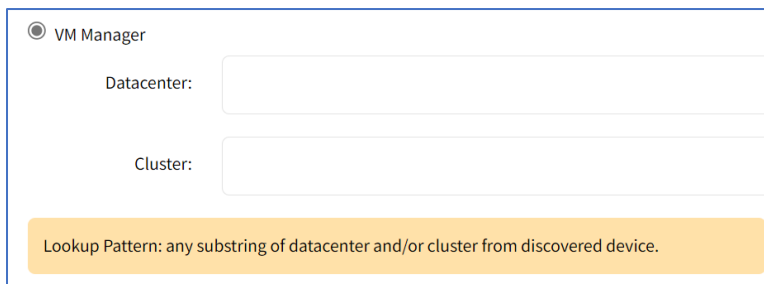
4. Save the changes with commit.

```
[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

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: Discovery Rules*.
2. Click **Add** (displays dialog).
3. Enter **Rule Name**.
4. On **Status** drop-down, select an item (**Enabled, Disabled**).
5. In *Discovery Method* menu, select **VM Manager**.



(optional) To filter the scan, enter **Datacenter** and **Cluster**.

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. In the **Clone from** drop-down, select the template device (created earlier).
9. 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.

```
[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=Virtual_Machine_Template
[admin@nodegrid {discovery_rules}]# commit
```

Step 3 – Define a VM Manager

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: VM Managers*.
2. Click **Add** (displays dialog).
3. In **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.

```
[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
```

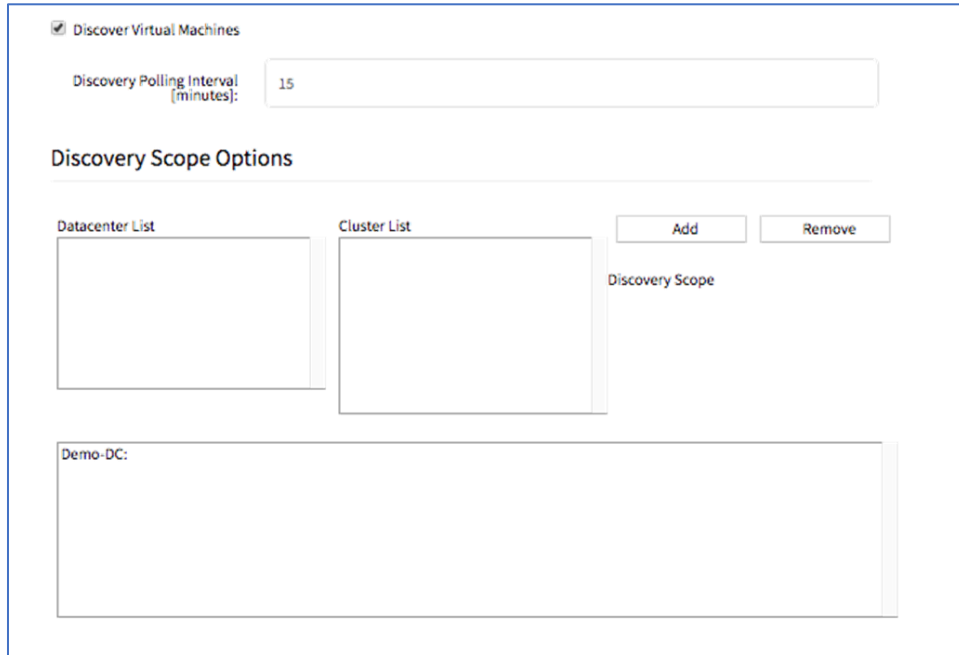
The Nodegrid Platform connects to the vCenter or ESXi system.

This process takes several minutes.

Step 4 – Enable Discover Virtual Machines

WebUI Procedure

1. Click on the newly created and connected VM Manager.



2. Select **Discover Virtual Machines** checkbox.
3. In **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.

```
[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
```

Network Scan sub-tab

This lists available network scan setups.

Devices	Views	Types	Auto Discovery	Preferences			
Network Scan	VM Managers	Discovery Rules	Hostname Detection	Discovery Logs Discover Now			
Managed Devices :: Auto Discovery :: Network Scan ↻ Reload							
<input type="button" value="Add"/> <input type="button" value="Delete"/>							
<input type="checkbox"/>	Scan ID	IP Range	Status	Similar Devices	Port Scan	Ping	Interval
<input type="checkbox"/>	testtest	127.0.0.1/127.0.0.4	Enabled	ttyS1	22-23,623	Yes	60

Add Network Scan

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: Network Scan*.
2. Click **Add** (displays dialog).

Devices	Views	Types	Auto Discovery	Preferences
Network Scan	VM Managers	Discovery Rules	Hostname Detection	Discovery Logs Discover Now
Managed Devices :: Auto Discovery :: Network Scan				
<input type="button" value="Save"/> <input type="button" value="Cancel"/>				
Scan ID: <input type="text"/>				
IP Range Start: <input type="text"/>				
IP Range End: <input type="text"/>				
<input checked="" type="checkbox"/> Enable Scanning				
<input checked="" type="checkbox"/> Similar Devices				
Device: <input type="text" value="ttyS1"/>				
<input checked="" type="checkbox"/> Port Scan				
Port List: <input type="text" value="22-23,623"/>				
List of individual ports separated by commas and/or port range separated by dash (e.g. 1,3,5,10-20).				
<input checked="" type="checkbox"/> Ping				
Scan Interval (in minutes): <input type="text" value="60"/>				

3. Enter **Name** (of Scan ID).
4. Enter **IP Range Start**.
5. Enter **IP Range End**.
6. Select **Similar Devices** checkbox.

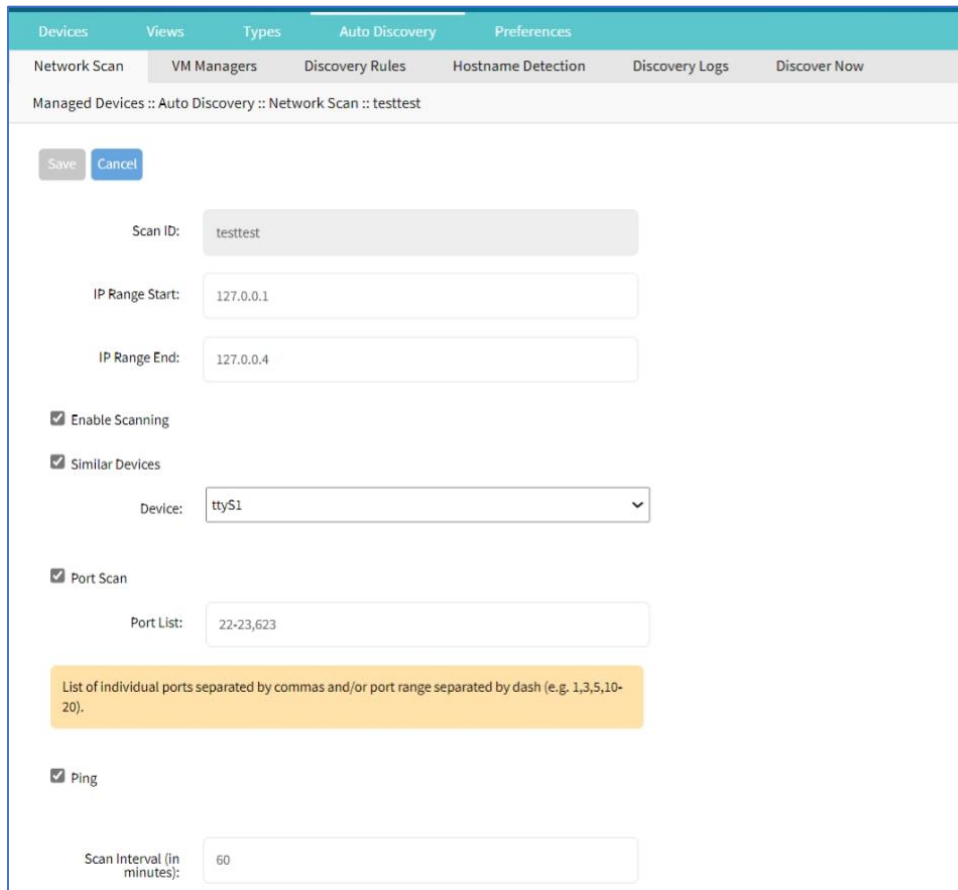
On **Device** drop-down, select an existing template (to identify devices).

7. Select **Enable Scanning** checkbox.
8. Select **Port Scan** checkbox.
Enter **Port List** (ports to be scanned, i.e., 2, 3, 11-20).
9. Select **Ping** checkbox (enables Ping function).
10. In **Scan interval (in minutes)**, enter a value.
11. Click **Save**.

Edit Network Scan

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: Network Scan*.
2. In *Scan ID* column, click on the name (displays dialog).

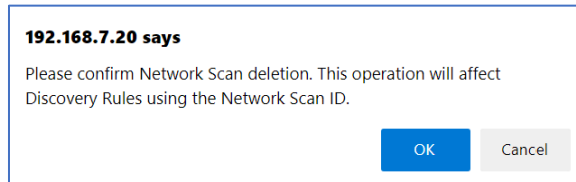


3. Make changes as needed.
4. Click **Save**.

Delete Network Scan

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: Network Scan*.
2. Select the checkbox(es) of items to delete.
3. Click **Delete** (displays confirmation dialog).



4. Click **OK**.

VM Manager sub-tab

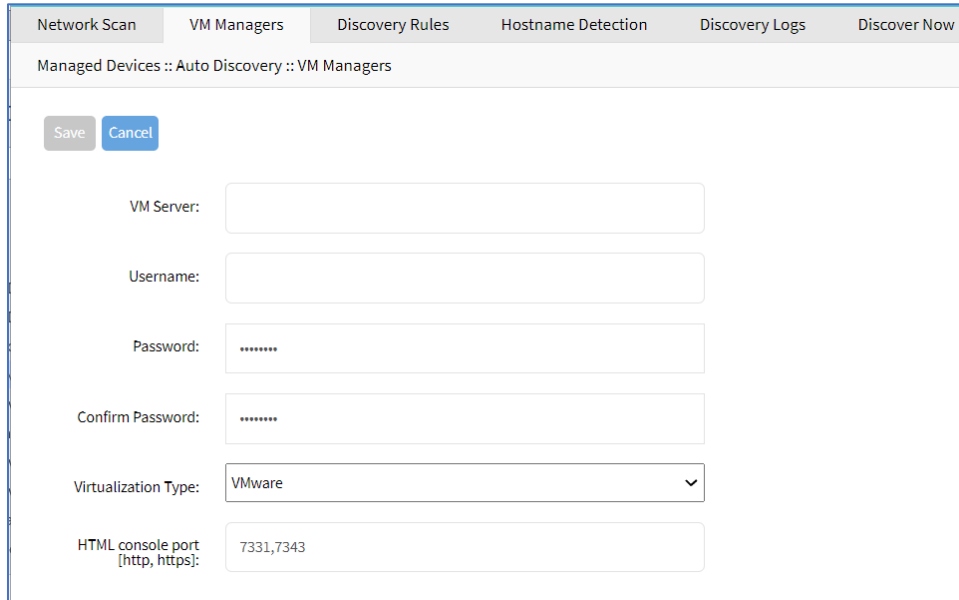
This lists VM Managers.

Devices	Views	Types	Auto Discovery	Preferences	
Network Scan	VM Managers	Discovery Rules	Hostname Detection	Discovery Logs	Discover Now
Managed Devices :: Auto Discovery :: VM Managers ↻ Reload					
<div style="display: flex; gap: 10px;"> Add Delete Install VMRC </div>					
<input type="checkbox"/>	VM Server	Virtualization Type	Discover Virtual Machines	Discovery Polling Interval [minutes]	
<input checked="" type="checkbox"/>	sdf	VMware	No	15	

Add VM Manager

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: VM Managers*.
2. Click **Add** (displays dialog).

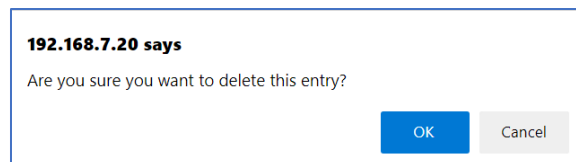


3. In **VM Server**, enter the *vCenter/ESXi IP* or **FQDN**.
4. Enter **Username**.
5. On **Virtualization Type** drop-down, select **VMware**.
6. Enter **Password** and **Confirm Password**.
7. Enter **HTML console port** (if needed).
8. Click **Save**.

Delete VM Manager

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: VM Managers*.
2. Select the checkbox(es) of items to delete.
3. Click **Delete** (displays confirmation dialog).



4. Click **OK**.

Install VMRC

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: VM Managers*.
2. Click **Install VMRC** (displays dialog).

3. In *Destination* menu, select one:

Local System radio button . On **Filename**, select from drop-down

Local Computer radio button. On **File Name**, click **Choose File** (locate and select).

Remote Server radio button. Enter **URL**, **Username**, and **Password**.

(as needed) Select **Download path is absolute path name** checkbox.

4. Click **Save**.

Discovery Rules sub-tab

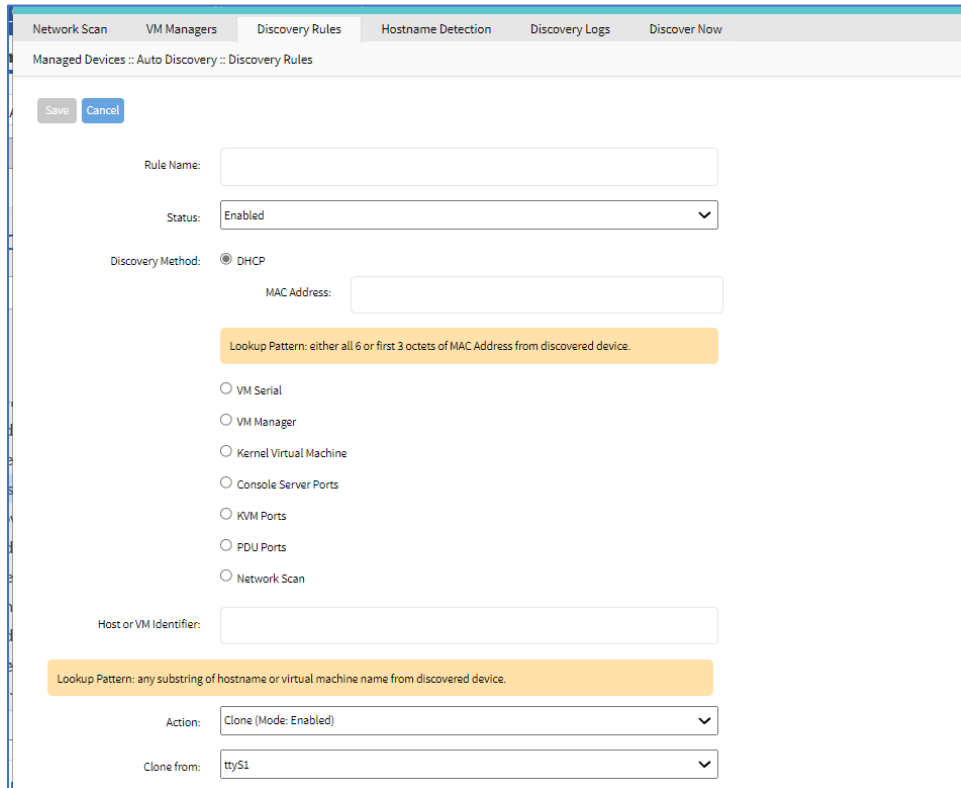
This lists all available discovery rules.

Devices		Views		Types		Auto Discovery		Preferences	
Network Scan		VM Managers		Discovery Rules		Hostname Detection		Discovery Logs	
Managed Devices :: Auto Discovery :: Discovery Rules Reload									
<div style="display: flex; justify-content: space-between; align-items: center;"> Add Delete Up Down </div>									
<input type="checkbox"/>	Order	Rule Name	Discovery Method	Host or VM Identifier	Lookup Pattern	Clone from	Action	Status	
<input checked="" type="checkbox"/>	1.0	testtest	DHCP			ttyS1	Clone (Mode: Enabled)	Enabled	

Add Discovery Rule

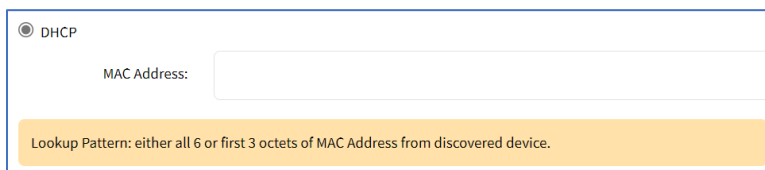
WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: Discovery Rules*.
2. Click **Add** (displays dialog).

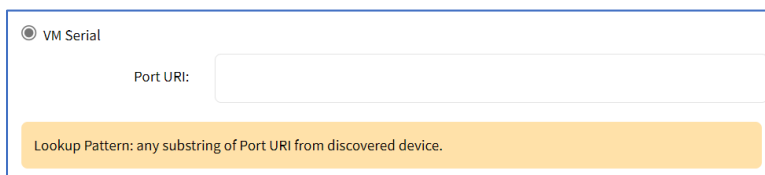


3. Enter **Rule Name**.
4. On **Status** drop-down, select (Enabled, Disabled).
5. In *Discovery Method* menu, select one and enter associated details.

DHCP radio button



VM Serial radio button



VM Manager radio button

VM Manager

Datacenter:

Cluster:

Lookup Pattern: any substring of datacenter and/or cluster from discovered device.

Kernel Virtual Machine radio button

Kernel Virtual Machine

Console Server Ports radio button

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

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).

PDU Ports radio button

PDU 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).

Network Scan radio button

Network Scan

Scan ID:

6. (optional) To filter specific entries, enter **MAC Address** (not available for some selections).
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 appropriate template device.
10. Click **Save**.

Edit Discovery Rule

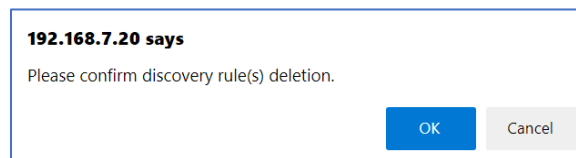
WebUI Procedure

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

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: Discovery Rules*.
2. Select the checkbox(es) of items to delete.
3. Click **Delete** (displays confirmation dialog).



4. Click **OK**.

Move Discovery Rule Priorities

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: Discovery Rules*.
2. Select the checkbox(es) of items.
3. Click **Up** or **Down** to move the sequence.

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.

Devices	Views	Types	Auto Discovery	Preferences
Network Scan	VM Managers	Discovery Rules	Hostname Detection	Discovery Logs Discover Now
Managed Devices :: Auto Discovery :: Hostname Detection Reload				
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Global Setting"/>				
<input type="checkbox"/>	Index	String		String Type
<input checked="" type="checkbox"/>	probe.1	\r		Probe
<input type="checkbox"/>	probe.2	\n		Probe
<input type="checkbox"/>	match.1	%H([a-zA-Z0-9:-_]+)?(?:[s?~?/]?)(?=>#)\$		Match
<input type="checkbox"/>	match.2	[\n\r]%H ([L]login:		Match

Enable Hostname Detection

Hostname detection must be enabled on the device. After hostname detection is enabled, it runs only once and then reverts to disabled.

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click on the device **Name** (displays dialog).
3. Select **Enable Hostname Detection** checkbox.



4. Click **Save**.

CLI Procedure

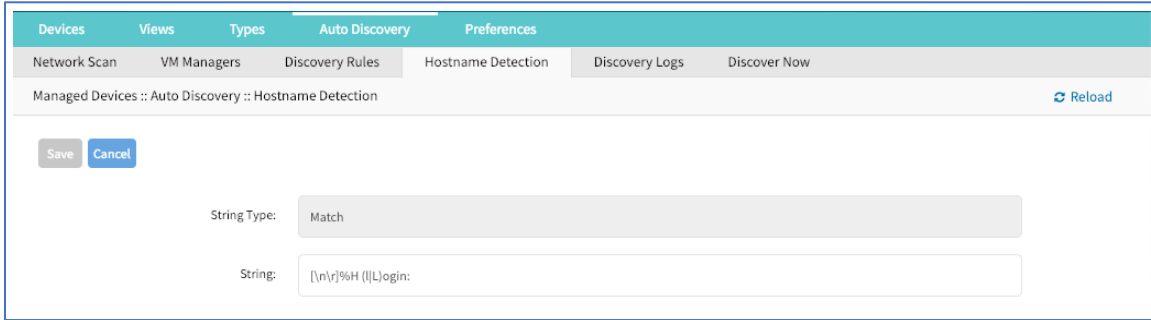
1. Go to `/settings/devices/<device name>/access`
2. Set `enable_hostname_detection` to `yes`
3. Save the changes with `commit`

```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/access/
[admin@nodegrid /]# set enable_hostname_detection=yes
[+admin@nodegrid /]# commit
```

Create a Probe or Match

WebUI Procedure

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. Enter **String** (characters for Match or Probe).

NOTE: For 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

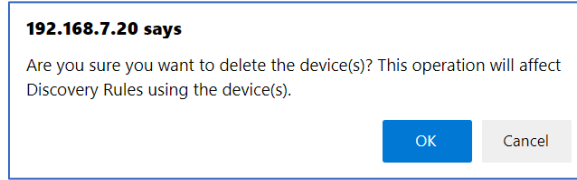
NOTE: For Matches RegEx expressions are allowed. Use the variable %H to indicate the location of the hostname

```
[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

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: Hostname Detection*.
2. Select checkbox(es).
- Click **Delete** (displays confirmation dialog).

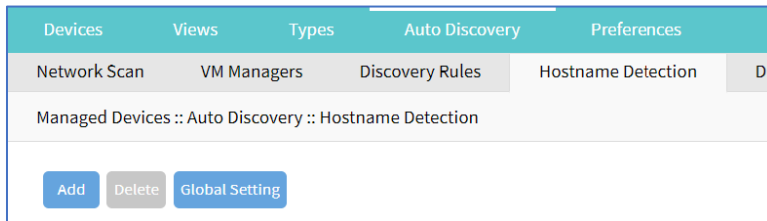


- Click **OK**.

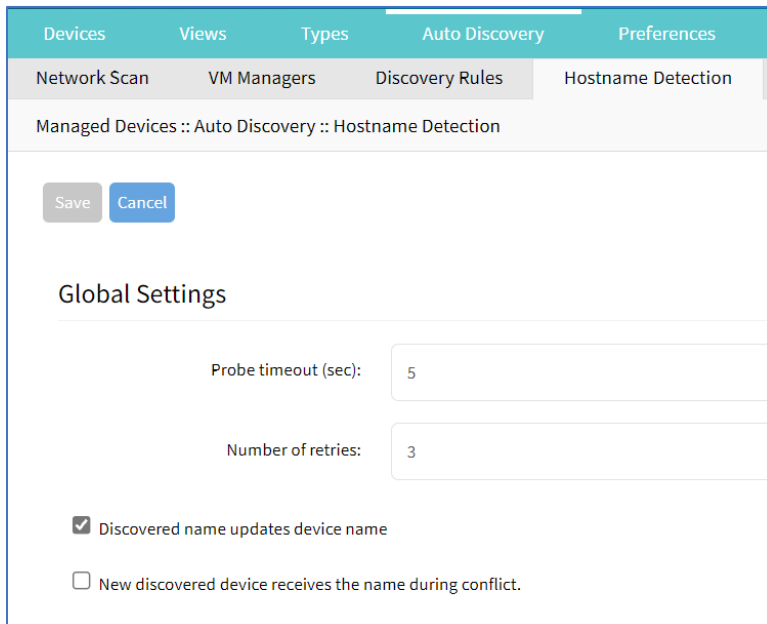
Modify Hostname Detection Global Setting

WebUI Procedure

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).
4. Enter **Number of retries** (number of times probe is resent if no output).
5. Select **Discovered name updates device name** checkbox (enabled by default)
 If disabled, no devices names are updated, even if a match was found.)
6. Select **New discovered device receives the name during conflict** checkbox.

If enabled and multiple devices have the same name, the latest discovered device receives the name.

7. Click **Save**.

Discovery Logs sub-tab

This displays the available Auto Discovery logs.

Managed Devices :: Auto Discovery :: Discovery Logs					
Reload					
Reset Logs					
Date	IP Address	Device Name	Discovery Method	Action	
Wed Oct 6 20:36:28 2021	127.0.0.1	nodegrid.localdomain	Network Scan	None	
Wed Oct 6 20:36:28 2021	127.0.0.2	whoartthou	Network Scan	None	
Wed Oct 6 20:36:29 2021	127.0.0.3	127.0.0.3	Network Scan	None	
Wed Oct 6 20:36:29 2021	127.0.0.4	127.0.0.4	Network Scan	None	

Reset Logs

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: Discovery Logs*.
2. Click **Reset Logs** (clears the table listing).

Managed Devices :: Auto Discovery :: Discovery Logs					
Reload					
Reset Logs					
Date	IP Address	Device Name	Discovery Method	Action	

Discover Now sub-tab

Managed Devices :: Auto Discovery :: Discover Now					
Reload					
Discover Now					
<input type="checkbox"/>	Name	Type			
<input checked="" type="checkbox"/>	testtest	Network Scan			

Start Discovery

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: Discover Now*.
2. On the list, select checkboxes.
3. Click **Discover Now**.

This manually runs the auto discovery process for the selected item(s).

Preferences tab

Administrators can define various preferences options that are applied to all sessions.

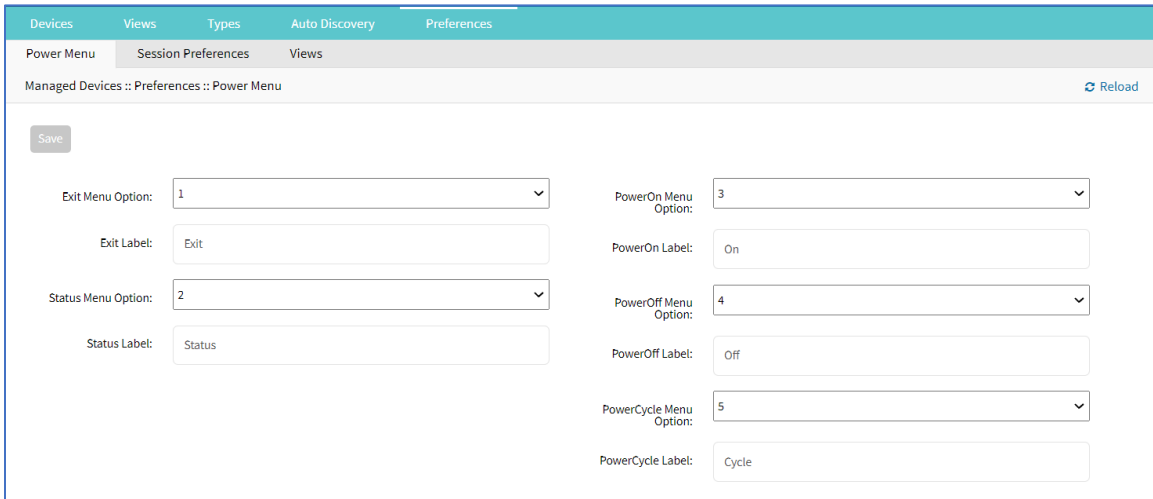
Power Menu sub-tab

This configures preferences for defined order and labeling of the power menu as it appears in a console session.

Edit Power Menu Settings

WebUI Procedure

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**.

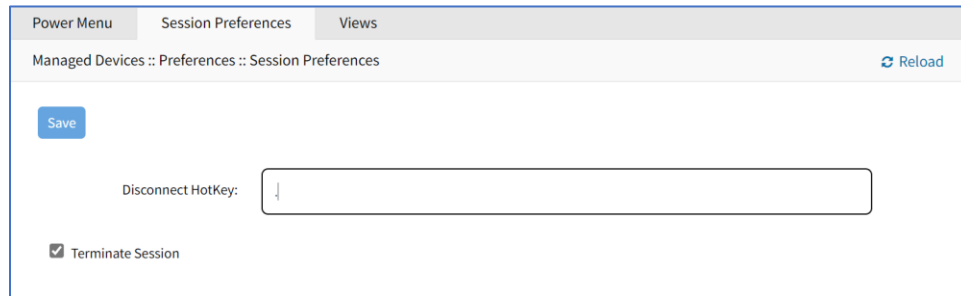
Session Preferences sub-tab

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

WebUI Procedure

1. Go to *Managed Devices :: Preferences :: Session Preferences*.



2. In **Disconnect HotKey**, create a key sequence to signals a terminate session.
3. Select **Terminate session** checkbox.

When 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

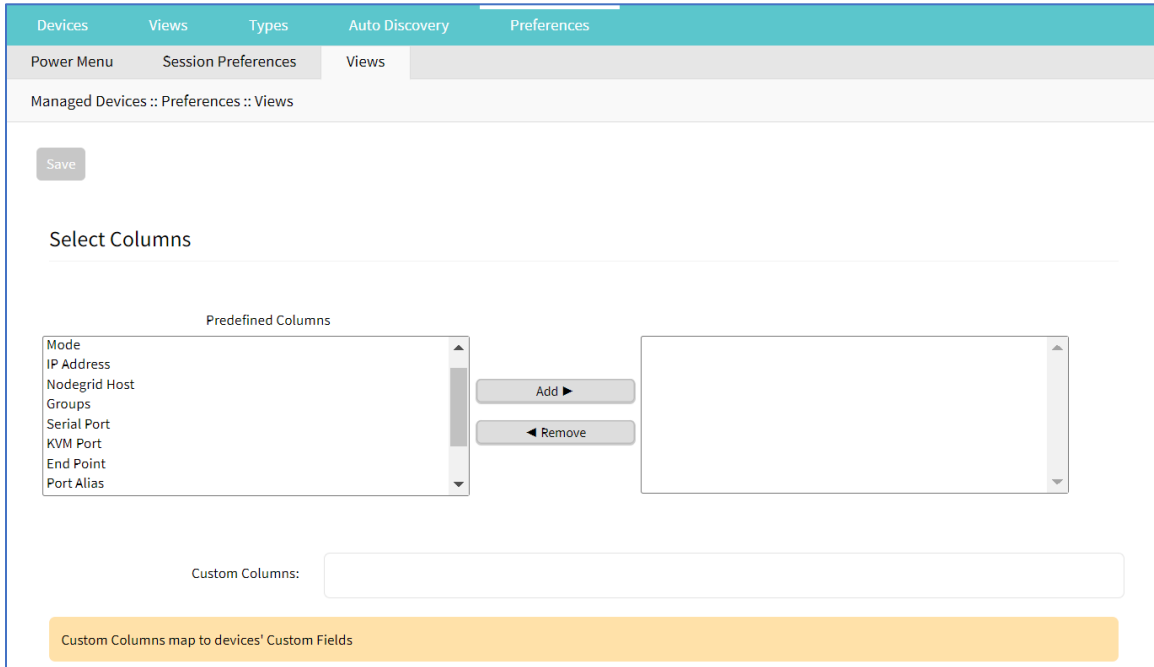
This changes how columns are displayed, as well as creating custom columns.

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.

WebUI Procedure

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**.

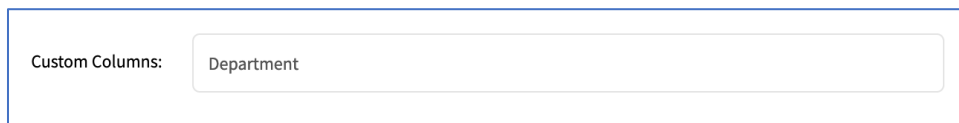
Step 1 – Create Custom Columns (per Device)

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.

WebUI Procedure

1. Go to *Managed Devices :: Preferences :: Views*.
2. In the **Custom Columns** text box, enter the name.



3. To add multiple columns, separate each name with a comma.

Custom Columns:

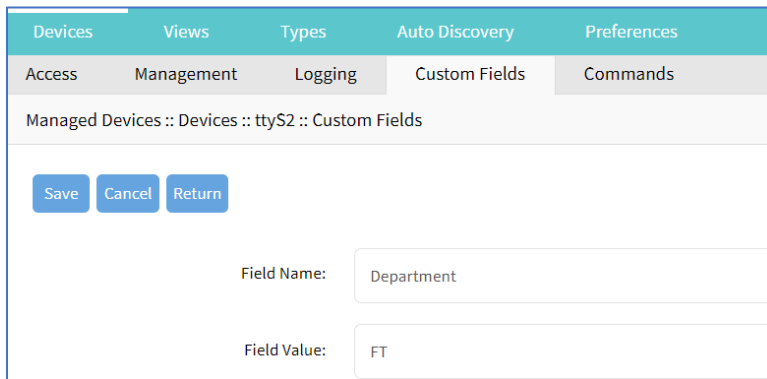
4. Click **Save**.

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

WebUI Procedure

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.

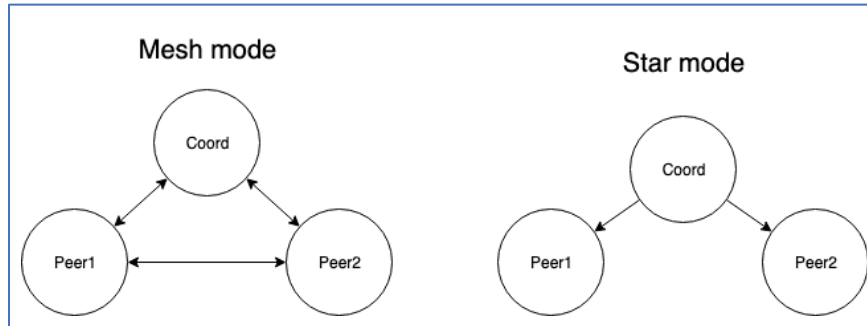
There are two types of clustering topologies:

STAR

This is the default option. In a star configuration, one Nodegrid unit acts as the coordinator and central node. All the 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.



Peers tab

This lists all Nodegrid devices enrolled in the cluster. The table shows information on each device.

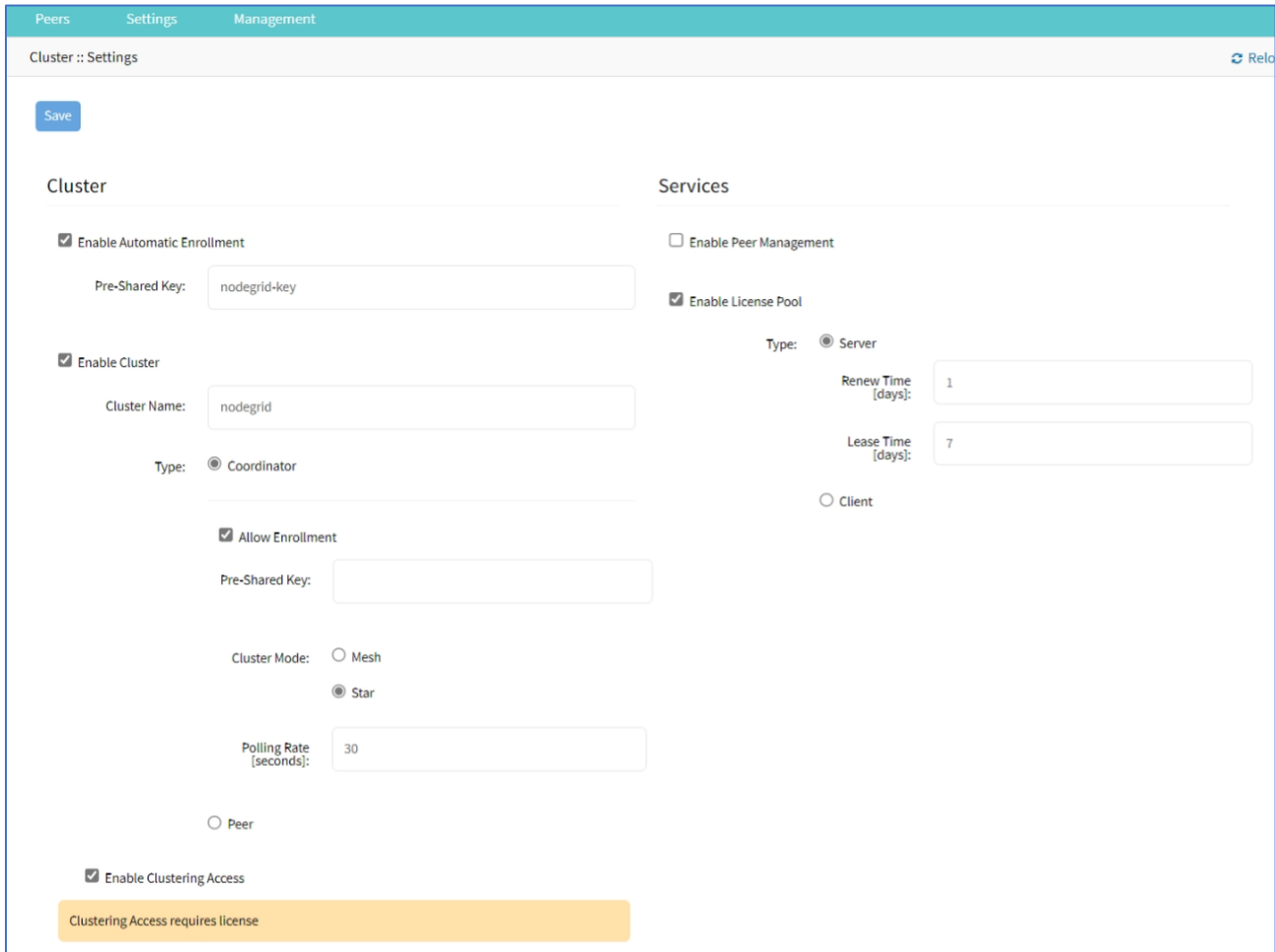
Peers					
Cluster :: Peers					
Name	Address	Type	Status	Peer Status	
<input type="checkbox"/> masterX.localdomain	Local	Coordinator	Online	192.168.3.216,192.168.3.70	
<input type="checkbox"/> peerZ.localdomain	192.168.3.216	Peer	Online	192.168.3.208,192.168.3.70	
<input type="checkbox"/> peerY.localdomain	192.168.3.70	Peer	Online	192.168.3.208,192.168.3.216	

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



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 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 were enrolled in the Cluster, the Coordinator can be set to Peer (prevents enrollment of other devices.)

Peer Management

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

When enabled, the License Pool allows central management of all software licenses within a cluster. 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 renew request based on the Renew Time. If client is unavailable for an extended time (exceeding the servers Lease Time), the client's licenses become invalid. The license is returned to the pool.

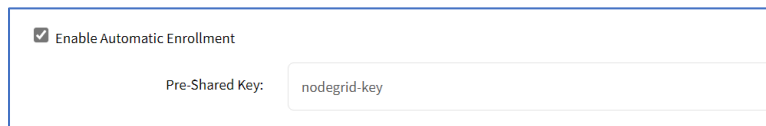
NOTE: Each Nodegrid device is shipped with five additional test target licenses. A test license is used automatically when a target license is added to the system. This also applies if a target license is applied on the License Pool Server. The first time a device requests target licenses, it requests five additional licenses to cover the currently used test licenses.

Configure Cluster

WebUI Procedure

1. Go to *Cluster :: Settings :: Enrollment*.
2. In the *Cluster* menu:

Select **Enable Automatic Enrollment** checkbox (expands to show additional fields)



The screenshot shows a configuration form with a checked checkbox labeled "Enable Automatic Enrollment". Below it, there is a label "Pre-Shared Key:" followed by a text input field containing the value "nodegrid-key".

Enter **Pre-shared Key** (default: nodegrid key).

Select **Enable Cluster** checkbox (allows other Nodegrid systems to manage, access, and search managed devices from other nodes)

In *Type* menu, select one:

Coordinator radio button

Enter **Pre-Shared Key**.

In *Cluster Mode* menu, select one (**Star**, **Mesh**).

Enter **Polling Rate (seconds)**.

Peer radio button

For **Coordinator's Address** (accept default: localhost).

Enter **Pre-Shared Key**.

Select **Enable Clustering Access** checkbox.

3. In *Services* menu:

Select **Enable Peer Management** checkbox.

Select **Enable License Pool** checkbox

In *Type* menu, select one.

Server radio button

Enter **Renew Time (days)**.

Enter **Lease Time (days)** (7-30 days)

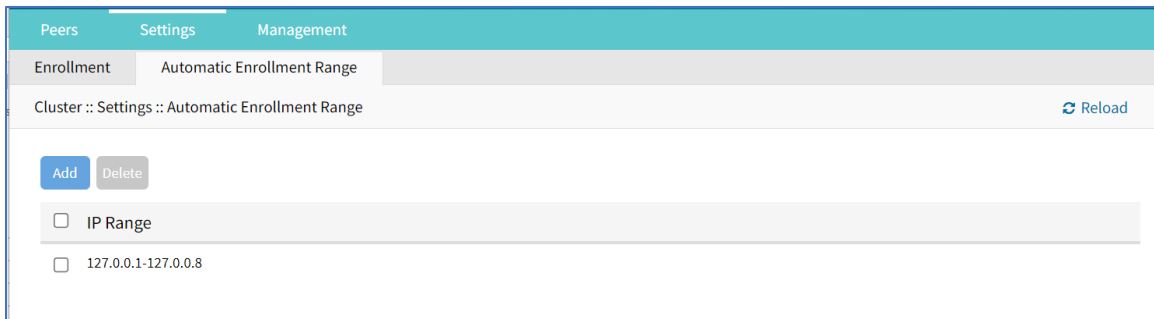
Client radio button

4. 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.

NOTE: 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.

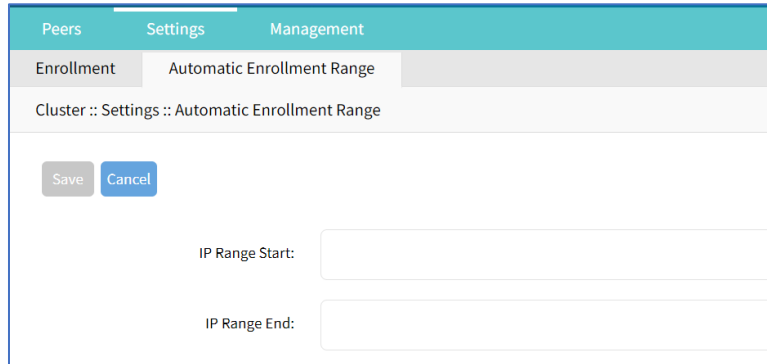


NOTE: An existing IP range setting cannot be modified. If an adjustment is needed, create a new IP range and delete the old IP range.

Add Automatic Enrollment Range

WebUI Procedure

1. Go to *Cluster :: Settings :: Automatic Enrollment Range*.
2. Click **Add** (displays dialog).



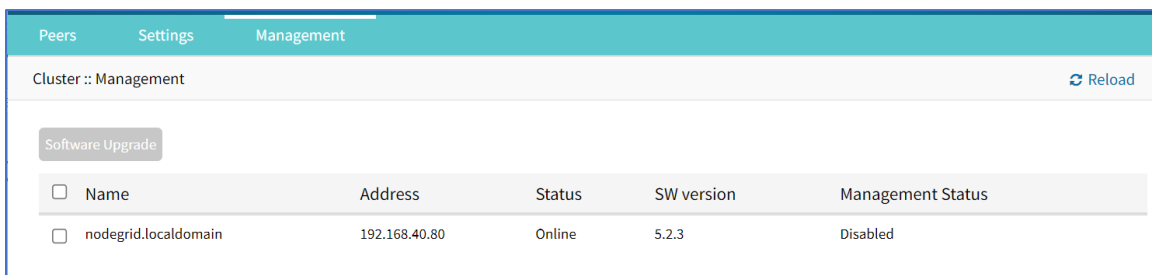
3. Enter **IP Range Start**.
4. Enter **IP Range End**.
5. Click **Save**.

Delete Automatic Enrollment Range

WebUI Procedure

1. Go to *Cluster :: Settings :: Automatic Enrollment Range*.
2. Select checkbox next to IP range to delete.
3. Click **Delete**.
4. On confirmation pop-up dialog, click **OK**.

Management tab



<input type="checkbox"/>	Name	Address	Status	SW version	Management Status
<input type="checkbox"/>	nodegrid.localdomain	192.168.40.80	Online	5.2.3	Disabled

Software Upgrade

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.

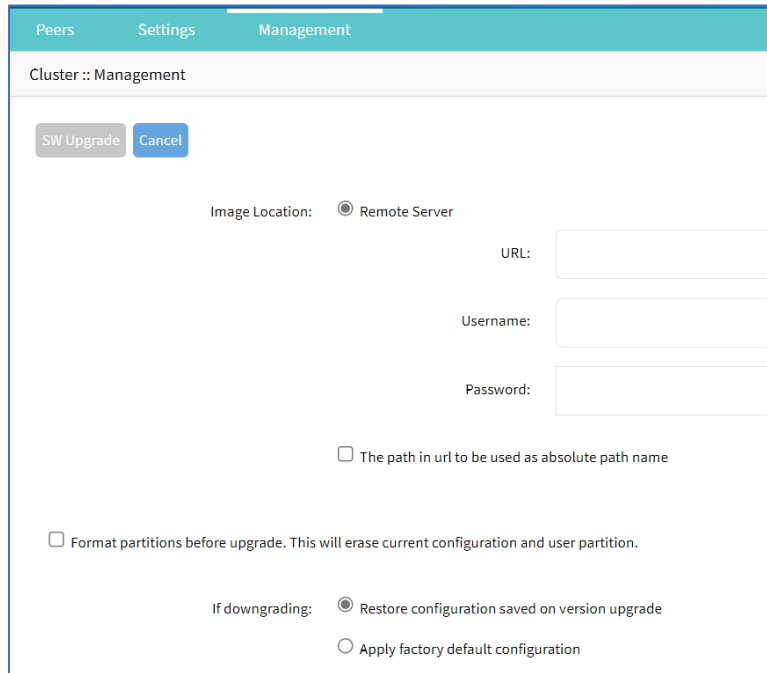
Upgrade the Software

Software can be upgraded or downgraded on this procedure.

WebUI Procedure

1. Go to *Cluster :: Management*.

2. Select checkbox next to the name for software management.
3. Click **Upgrade Software** (displays dialog).



The screenshot shows a software upgrade dialog box with the following elements:

- Buttons: SW Upgrade (disabled), Cancel
- 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

4. In *Image Location* menu, select **Remote Server**.
 Enter **URL**.
 Enter **Username**.
 Enter **Password**.
5. (as needed) Select **The path in url to be used as absolute path name** checkbox.
6. (as needed) Select **Format partitions before upgrade. This will erase current configuration and user partition** checkbox.
7. (if applicable) In *If downgrading* menu (select one):
Restore configuration saved on version upgrade radio button
Apply factory default configuration radio button.
8. Review the details.
9. Click **SW Upgrade**.

Security Section

Local Accounts tab

New local users can be added, deleted, changed, and locked. Administrators can force passwords to be changed upon next login, and set expiration dates for user accounts. Administrators can manage API keys for each account.

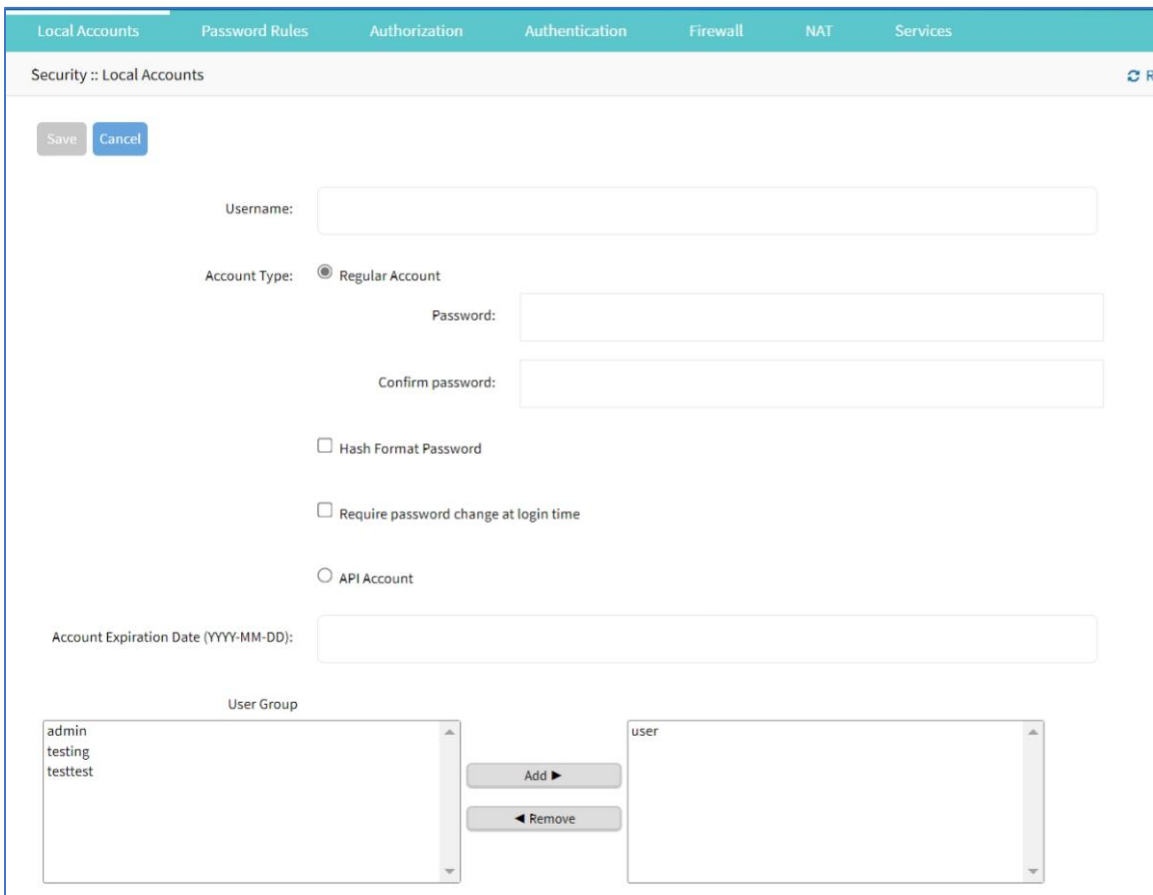
NOTE: Regardless of activation options, users can change their passwords at any time.

Manage Local Users

Add Local User

WebUI Procedure

1. Go to *Security :: Local Accounts*.
2. Click **Add** (displays dialog).



3. Enter **Username**.
4. In *Account Type* menu, select one.

Regular Account radio button

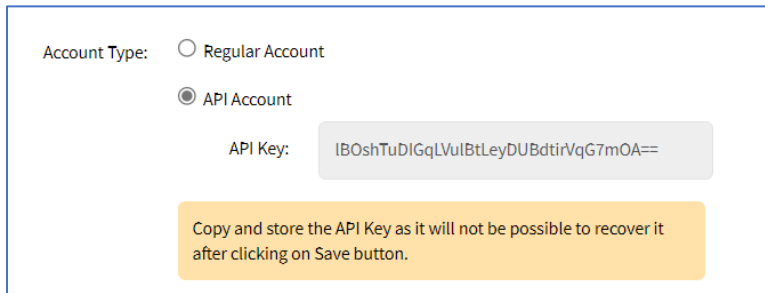
Enter **Password** and **Confirm Password**.

If the password is in a hash format, select **Hash Format Password** checkbox.

(as needed) Select **Require password change at login time** checkbox.

API Account radio 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.*"



Account Type: Regular Account
 API Account

API Key:

Copy and store the API Key as it will not be possible to recover it after clicking on Save button.

5. (optional) Enter **Account Expiration Date (YYYY-MM-DD)**.
6. In the *User Group* panel:
 Select from left-side panel, click **Add ►** to move to right-side panel.
 To remove from right-side panel, select, and click **◀ Remove**.
7. Click **Save**.

Edit Local User

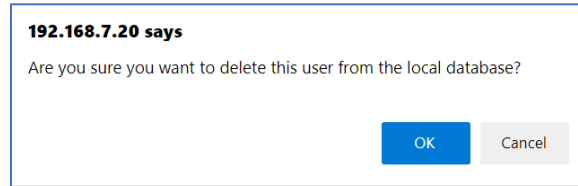
WebUI Procedure

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

WebUI Procedure

1. Go to *Security :: Local Accounts*.
2. Locate and select checkbox next to username.
3. Click **Delete** (displays confirmation dialog).



4. Click **OK**.

Lock/Unlock Local User

WebUI Procedure

Generally, 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 one:
 - Lock** (locks user out of device).
 - 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:

```

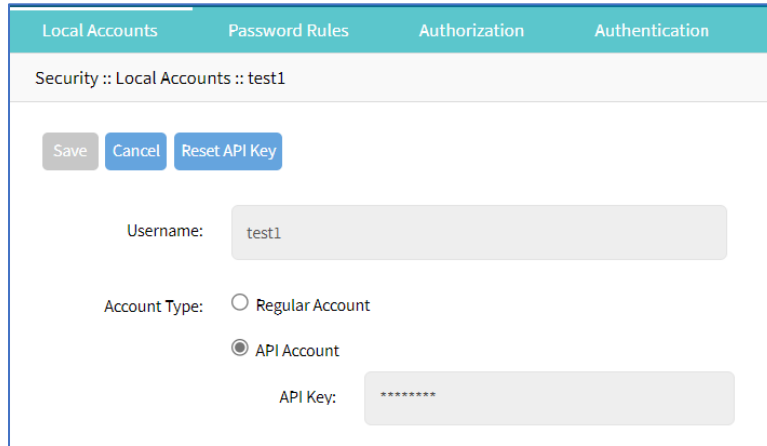
root@nodegrid:~# openssl passwd -1 -salt mysall
Password:
$1$mysall$YBFR90n0wjde5be32mC1g1
    
```

Generate a new API key for a user

In the *Type* column, the user must have a value of **API**.

WebUI Procedure

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**.



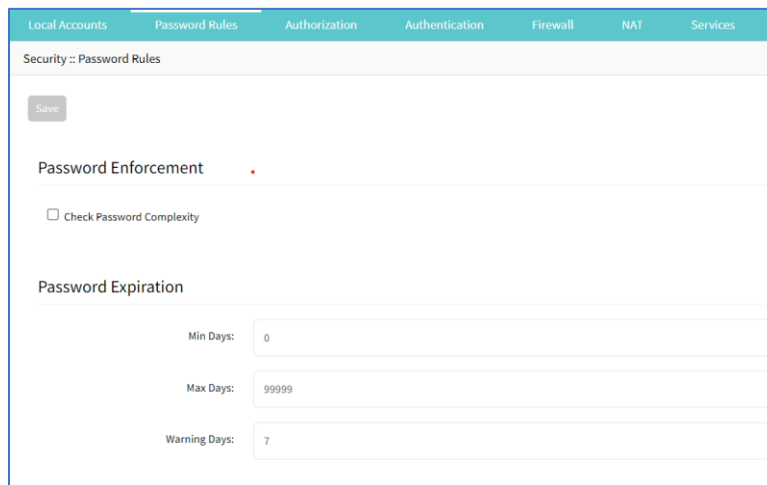
3. Click **Reset API Key**.

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.



Manage Password Rules

Modify Password Rules

WebUI Procedure

1. Go to *Security :: Password Rules*.
2. In *Password Enforcement* menu:
 - Select **Check Password Complexity** checkbox (expands options).
 - Enter **Minimum Number of Digits** (minimum characters in password).

Enter **Minimum Number of Upper Case Characters** (minimum upper case characters in password).

Enter **Minimum Number of Special Characters** (minimum special characters in password).

Enter **Minimum Size**. (minimum characters in password – default: 8).

Enter **Number of Passwords to Store in History** (the number of passwords stored in history to prevent reuse – default: 1).

3. In *Password Expiration* menu:

Enter **Min Days** (minimum days password must be valid before changed – default: 0).

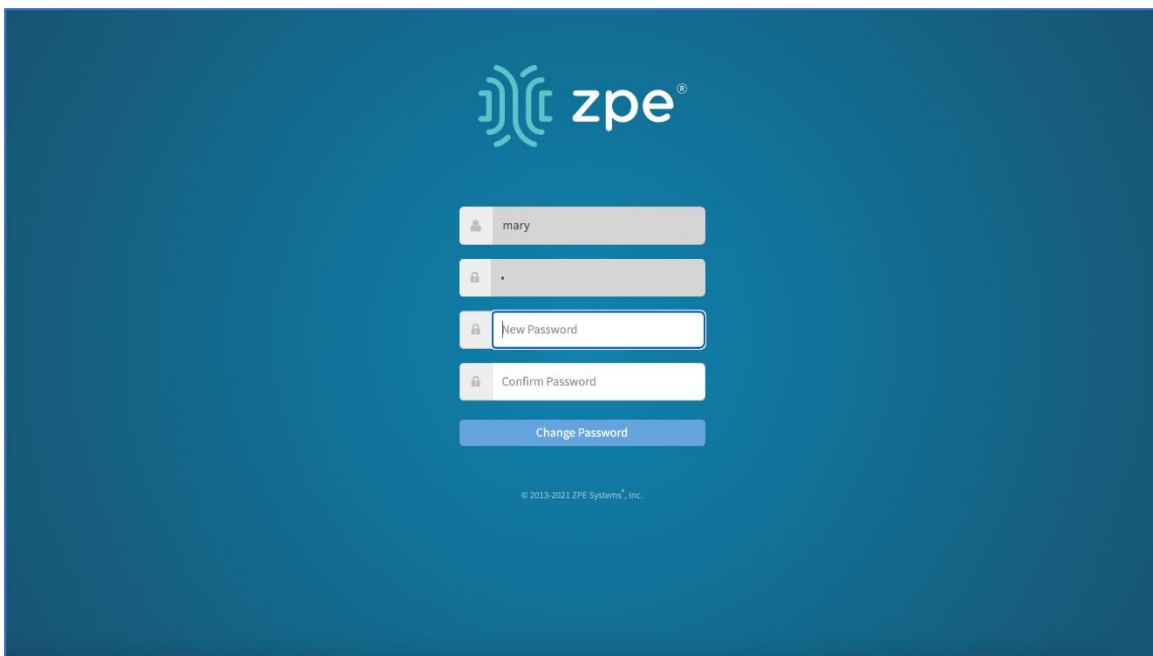
Enter **Max Days** (maximum days password is valid before forcing change – default: 99999).

Enter **Warning Days** (days that users is notified before expiration – default: 7).

4. Click **Save**.

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.



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.

User Group Configuration Process

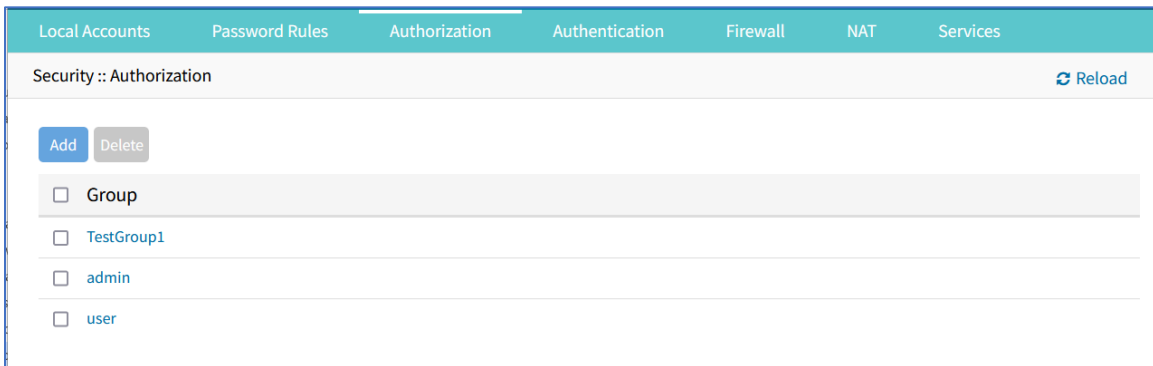
This is the process to establish a User Group.

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

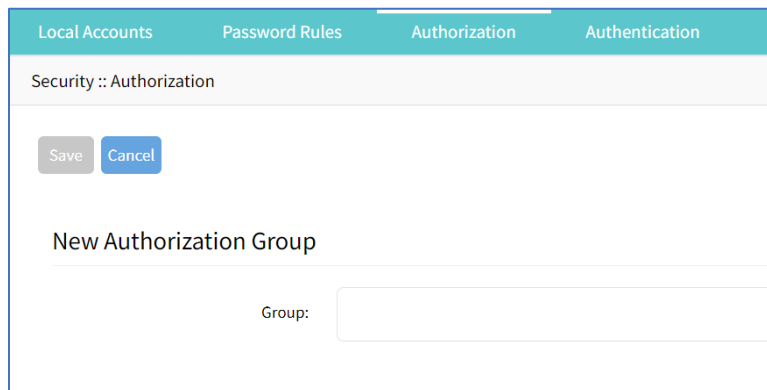
Add User Group

WebUI Procedure

1. Go to *Security :: Authorization*.



2. Click **Add** (displays dialog).



3. In **Group**, enter name of group.
4. Click **Save**.

Delete User Group

WebUI Procedure

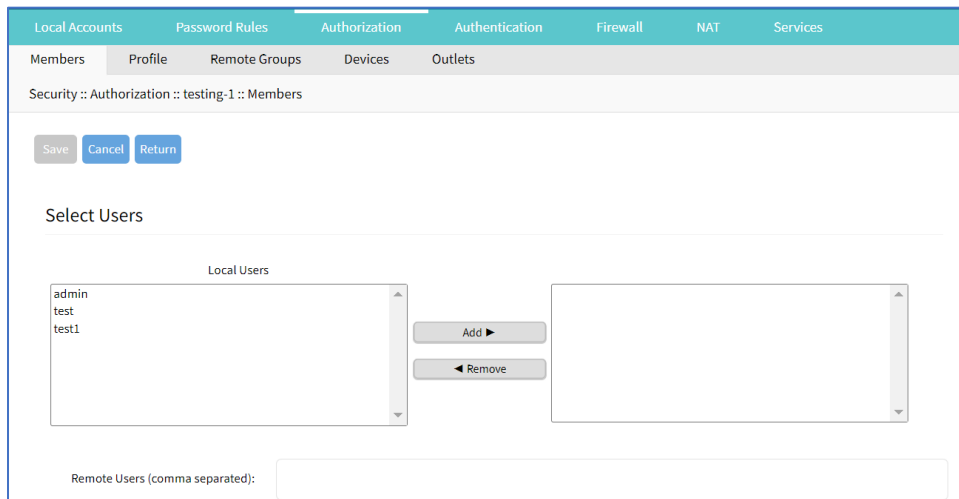
1. Go to *Security :: Authorization*.
2. Select checkbox next to group to be deleted.
3. Click **Delete**.
4. On Confirmation dialog, click **OK**.

User Group: Members sub-tab

Add Members to User Group

WebUI Procedure

5. Go to *Security :: Authorization*.
6. Click the **Group Name**.
7. On **Members** sub-tab, click **Add** (displays dialog).



8. In the *Local Users* (left) panel:
 Select from left-side panel, click **Add** to move to right-side panel.
 To remove from right-side panel, select, and click **Remove**.
9. Click **Save**.

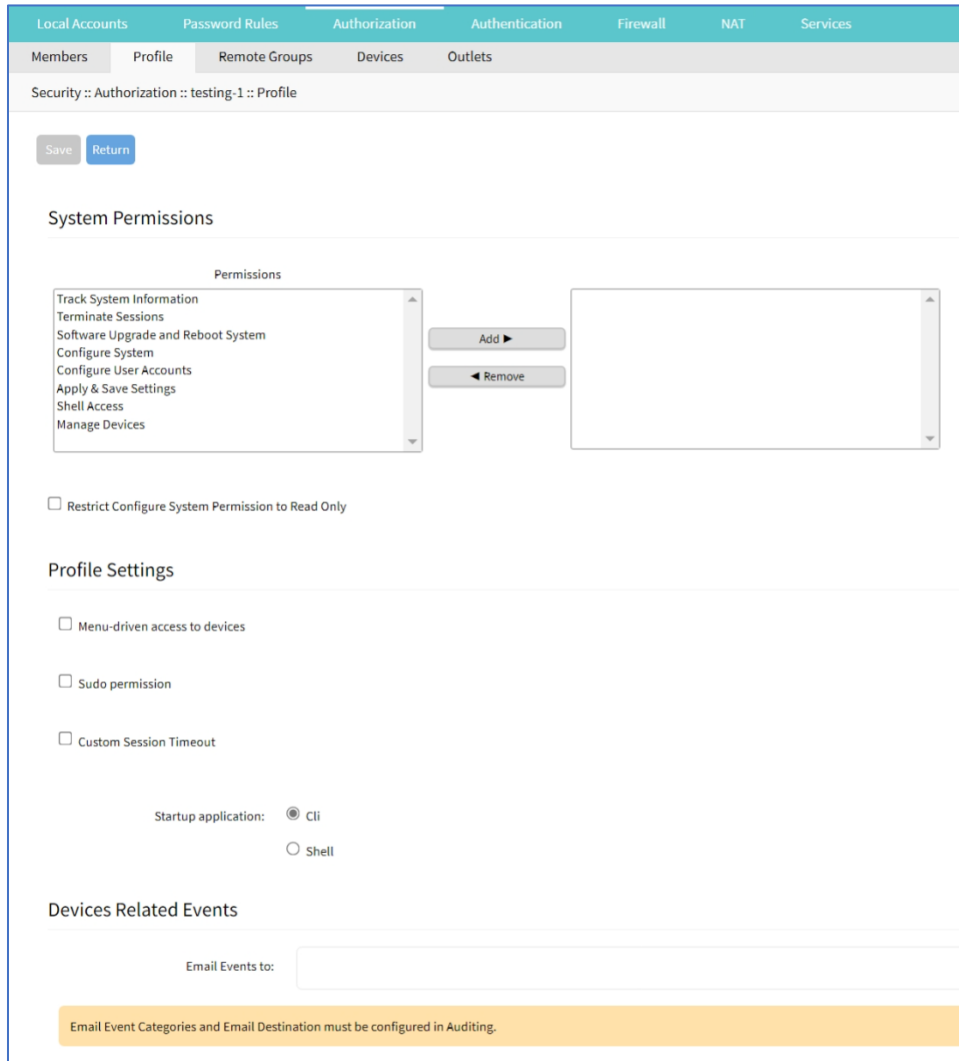
User Group: Profile sub-tab

Apply System Permissions and Profile Settings

WebUI Procedure

1. Go to *Security :: Authorization*.

2. Click on the **Group Name**.
3. Click on the **Profile** sub-tab:



4. In *System Permissions* menu:
 - Select from left-side panel, click **Add**► to move to right-side panel.
 - To remove from right-side panel, select, and click ◀**Remove**.
 - Select **Restrict Configure System Permission to Read Only** checkbox (granted system settings are visible but cannot be changed)
5. In *Profile Settings* menu:
 - Select **Menu-driven access to devices** checkbox (group members presented a target menu when SSH connection to the Nodegrid device is established).
 - Select **Sudo permission** checkbox (users can execute sudo commands).
 - Select **Custom Session Timeout** checkbox (enables a custom session time).

Enter **Timeout [seconds]**.

In *Startup application* menu, select one (**Cli, Shell**).

6. In *Devices Related Events* menu:

On **Email Events to**, enter email addresses (comma-separated).

NOTE: *Email Event Categories* and *Email Destination* are configured in the *Auditing* section.

7. Click **Save**.

User Group: Remote Groups sub-tab

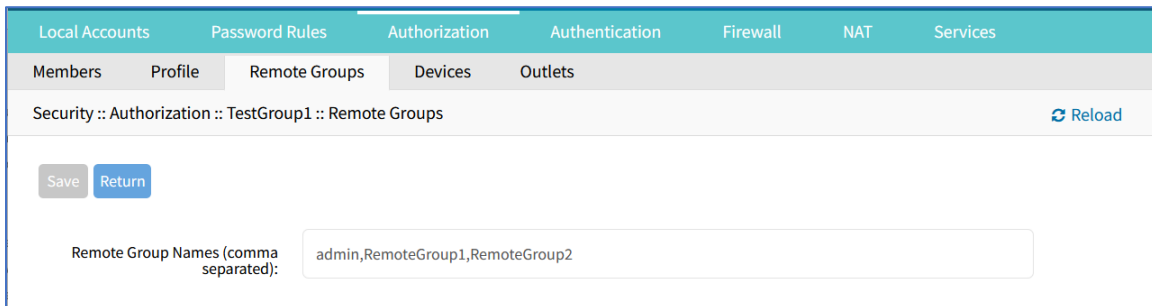
Assign Remote Groups

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.

WebUI Procedure

1. Go to *Security :: Authorization*.
2. Click on the **Group Name**,
3. On the **Remote Groups** sub-tab:



In **Remote Group Names**, enter external group names (comma-separated).

4. Click **Save**.

User Group: Devices sub-tab

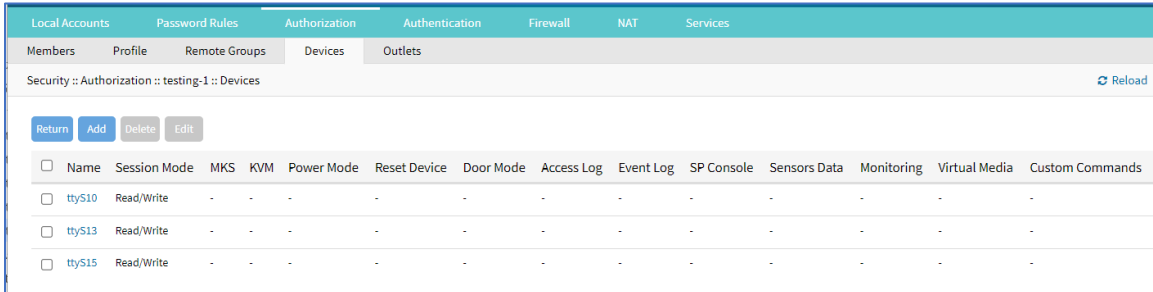
Depending on system permission, access to specific devices can be assigned to groups. Devices must be added to the group. Appropriate access rights can be set. Multiple devices can be added at the same time.

NOTE: Access permissions to control power outlets are granted through the Outlets permissions and not through Devices

Add Devices and Configure Permissions

WebUI Procedure

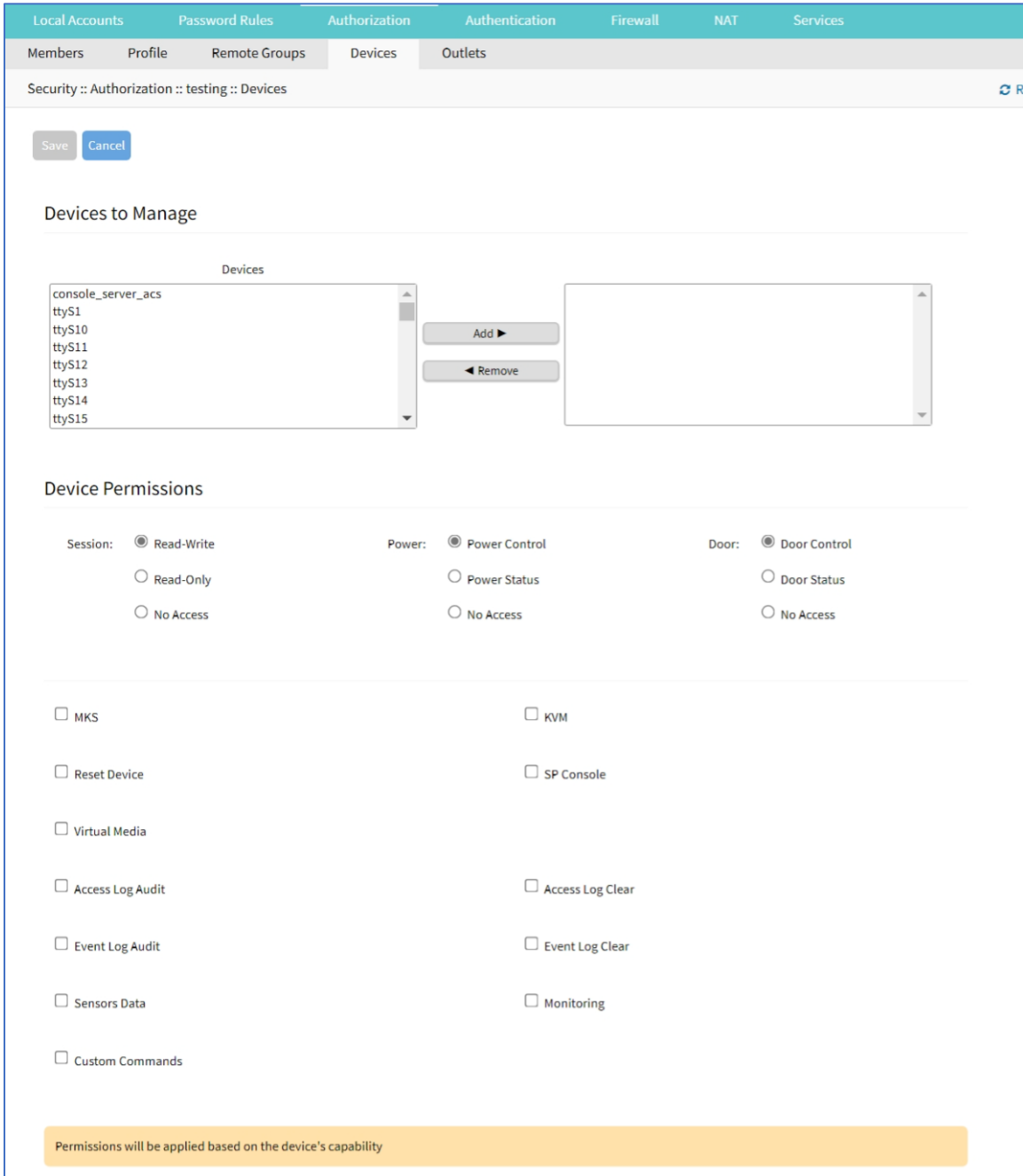
1. Go to *Security :: Authorization*.
2. Click on the **Group Name**.
3. Click on the **Devices** sub-tab.



The screenshot shows the ZPE web interface. The top navigation bar includes 'Local Accounts', 'Password Rules', 'Authorization', 'Authentication', 'Firewall', 'NAT', and 'Services'. Under 'Authorization', there are sub-tabs: 'Members', 'Profile', 'Remote Groups', 'Devices', and 'Outlets'. The 'Devices' sub-tab is active, showing a table of devices for the group 'testing-1'. The table has columns for Name, Session Mode, MKS, KVM, Power Mode, Reset Device, Door Mode, Access Log, Event Log, SP Console, Sensors Data, Monitoring, Virtual Media, and Custom Commands. There are three rows of devices: ttyS10, ttyS13, and ttyS15, all with 'Read/Write' session mode and '-' for other attributes. Above the table are buttons for 'Return', 'Add', 'Delete', and 'Edit'. A 'Reload' button is in the top right corner.

<input type="checkbox"/>	Name	Session Mode	MKS	KVM	Power Mode	Reset Device	Door Mode	Access Log	Event Log	SP Console	Sensors Data	Monitoring	Virtual Media	Custom Commands
<input type="checkbox"/>	ttyS10	Read/Write	-	-	-	-	-	-	-	-	-	-	-	-
<input type="checkbox"/>	ttyS13	Read/Write	-	-	-	-	-	-	-	-	-	-	-	-
<input type="checkbox"/>	ttyS15	Read/Write	-	-	-	-	-	-	-	-	-	-	-	-

4. Click **Add** (displays dialog).



5. In *Devices to Manage* menu:

On *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**.

In *Device Permissions* menu:

In *Sessions* menu, select one (**Read-Write, Read-Only, No Access**).

In *Power* menu, select one (**Power Control, Power Status, No Access**).

In *Door* menu, select one (**Door Control, Door Status, No Access**)

6. (as needed) Select/unselect the following settings:

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

WebUI Procedure

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

WebUI Procedure

1. Go to *Security :: Authorization*.
2. Click on the **Group Name**.
3. Click on the **Devices** sub-tab.
4. Select checkbox and click **Delete**.

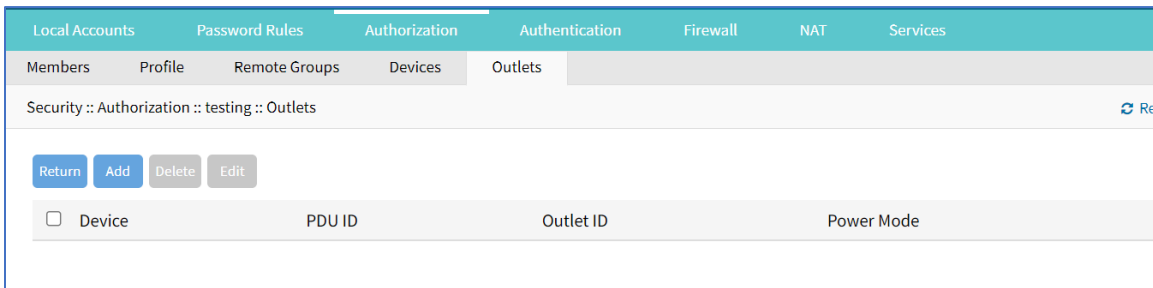
User Group: Outlets sub-tab

Add and Configure Power Outlets

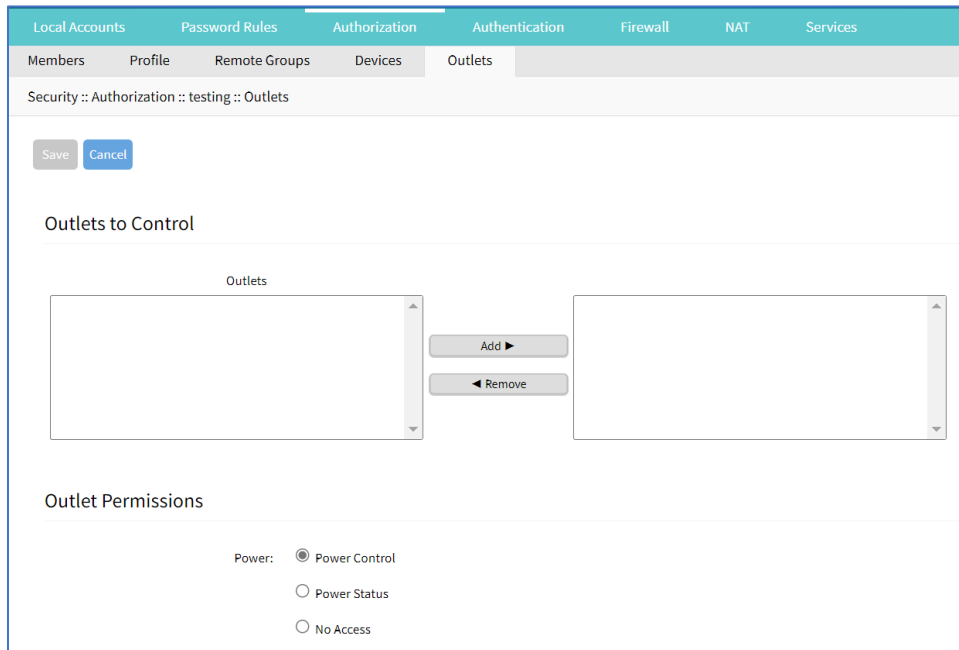
Access permissions for power outlets from Rack PDUs are controlled individually as the power to turn on or off a device can have severe consequences for the running of a data center or remote location. The assignment of permissions is analogous to device's access permissions.

WebUI Procedure

1. Go to *Security :: Authorization*.
2. Click on the **Group Name**.
3. Click **Outlets** sub-tab.



4. Click **Add** (displays dialog).



5. In *Outlets to Control* menu:

In *Outlets* panel:

Select from left-side panel, click **Add ►** to move to right-side panel.

To remove from right-side panel, select, and click **◀ Remove**.

- In *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)
- 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

WebUI Procedure

- Go to *Security :: Authorization*.
- In the Group column, click on a name.
- On the group's **Profile** sub-tab:
 - In *Startup application* menu:
 - Select **Shell** radio button (gives group members default shell access, and not CLI access, on connection via SSH).
 - Click **Save**.
- Go to *Security :: Local Accounts*.
- 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.

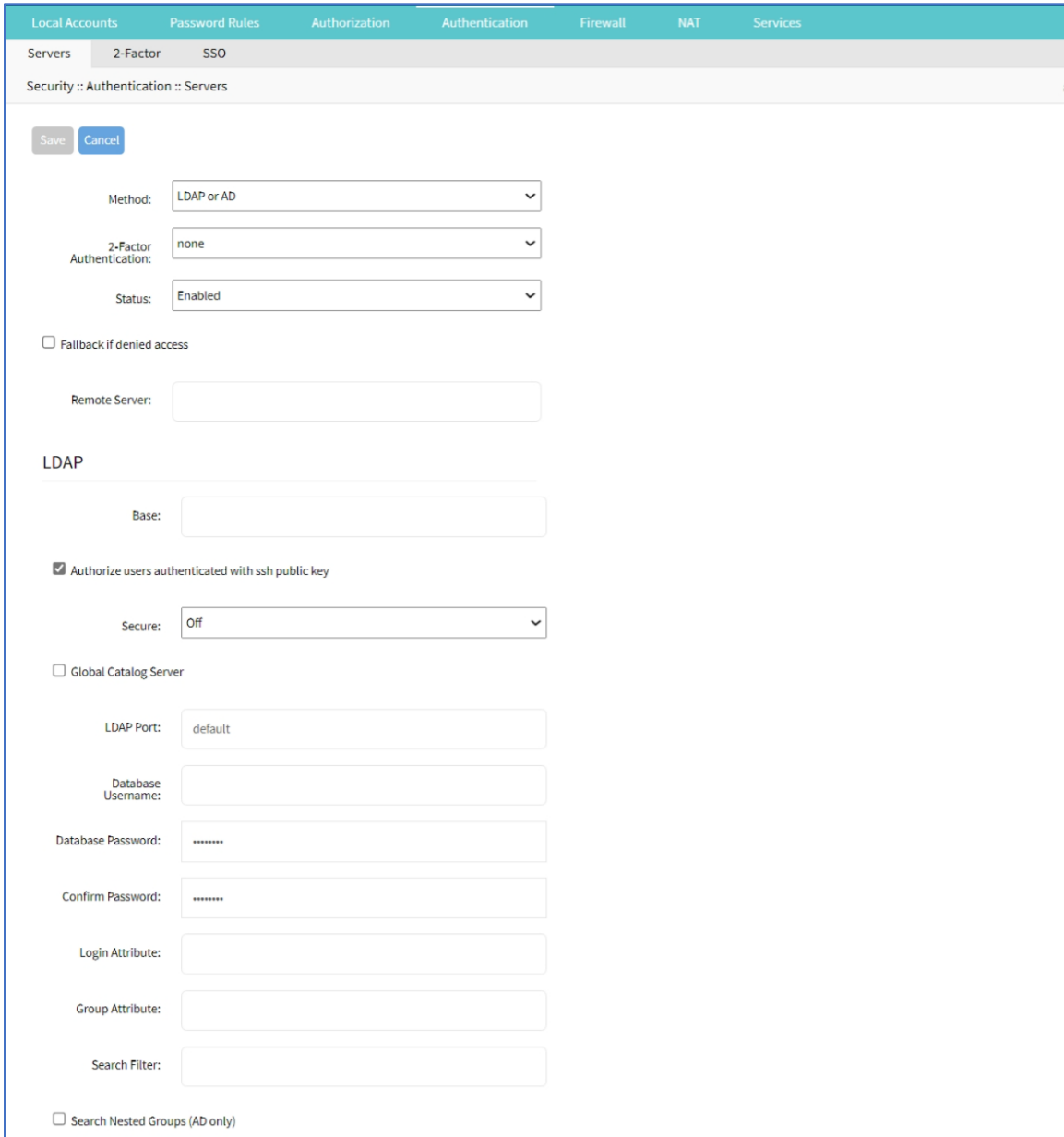
NOTE: The device's root user and Admin group users can still bypass 2-Factor Authentication in Console and WebUI, in case the remote server is unreachable.

Servers sub-tab

Add a server

WebUI Procedure

1. Go to *Security :: Authentication :: Servers*.
2. Click **Add** (displays dialog).



Local Accounts Password Rules Authorization **Authentication** Firewall NAT Services

Servers 2-Factor SSO

Security :: Authentication :: Servers

Save Cancel

Method: LDAP or AD

2-Factor Authentication: none

Status: Enabled

Fallback if denied access

Remote Server:

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)

3. On **Method** drop-down, select one (**LDAP or AD, RADIUS, TACACS+, Kerberos**). (Additional options display, depending on selection).
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. If **Method** selection is: **LDAP or AD** (displays dialog).

LDAP

Base:

Authorize users authenticated with ssh public key

Secure:

Global Catalog Server

LDAP Port:

Database Username:

Database Password:

Confirm Password:

Login Attribute:

Group Attribute:

Search Filter:

Search Nested Groups (AD only)

Enter **Base** (root DN or a sublevel DN – highest point used to search for users or groups).

Select **Authorize users authenticated with ssh public key** checkbox (default: disabled).

On **Secure** drop-down, select one (**On**, **Off**, **Start_TLS**) (default: Off).

Select **Global Catalog Server** checkbox (if enabled, uses an Active Directory Global Catalog Server).

Enter **LDAP Port** (or accept "default").

Enter **Database Username**.

Enter **Database Password**.

Enter **Confirm Password**.

Enter **Login Attribute** (contains username - for AD, default: sAMAccountName).

Enter **Group Attribute** (group identifier - for AD, default: memberOf).

Enter **Search Filter**.

Select **Search Nested Groups (AD only)** checkbox (default: disabled).

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 TLS!; Global Catalog Server: True; Database Username: cn=Administrator, cn=Users, dc=zpesystems, dc=com; Login Attribute: sAMAccountName; Group Attribute: memberOf

9. If **Method** selection is: **RADIUS** (displays dialog).

Radius

Accounting Server:

Radius Port:

Radius Accounting Port:

Secret:

Confirm Secret:

Timeout:

Retries:

Enable ServiceType attribute association to local authorization group

Enter **Accounting Server**.

Enter **Radius Port** (or accept "default").

Enter **Radius Accounting Port** (or accept "default").

Enter **Secret** and **Confirm Secret**.

Enter **Timeout**.

Enter **Retries**.

Select **Enable ServiceType attribute association to local authorization group** checkbox (allows assignment of Radius Service Types to Nodegrid local groups).

+++++

FreeRadius Server Configuration - CLI Procedure (example)

1. Create the file "/usr/share/freeradius/dictionary.zpe" with the content listed below:

```
VENDOR ZPE 42518
BEGIN-VENDOR ZPE
    ATTRIBUTE ZPE-User-Groups 1 string
END-VENDOR ZPE
```

2. Edit the file "/usr/share/freeradius/dictionary". In the file, add a line with dictionary.zpe (suggested location).

```
$INCLUDE dictionary.zpe
$INCLUDE dictionary.jradius
```

3. In /etc/freeradius/users, assign user groups. Define the "Framed-Filter-ID" attribute (as before) or define a new attribute "ZPE-User-Groups".

NOTE: If both attributes are defined, "ZPE-User-Groups" takes precedence.

```
rad-edmond      Cleartext-Password := "*****"
                Service-Type = Framed-User,
                Framed-Protocol = PPP,
                Framed-Filter-Id = "group_name=filter-grp1, filter-
grp2;",
                ZPE-User-Groups = "vsa-grp1, vsa-grp2",
                Framed-MTU = 1500,
                Framed-Compression = Van-Jacobsen-TCP-IP
```

+++++

10. If **Method** selection is: **TACACS+** (displays dialog).

Tacacs+

Accounting Server:

Authorize users authenticated with ssh public key

TACACS+ Port:

Service: ▼

Secret:

Confirm Secret:

Timeout:

Retries:

TACACS+ Version: ▼

Enable User-Level attribute of Shell and raccess services association to local authorization group

Enter **TACACS+ Port** (default: 49).

On **Service** drop-down, select one (**PPP, Shell, raccess**) (default: raccess).

Enter **Secret**.

Enter **Confirm Secret**.

Enter **Timeout**.

Enter **Retries**.

On **TACACS+ Version** drop-down, select one (**V0, V1, V0_V1, V1_V0**).

Select **Enable User-Level attribute of Shell and raccess services association to local authorization group** checkbox.

11. If **Method** selection is: **Kerberos** (displays dialog).

Kerberos

Realm Domain Name:

Domain Name:

Enter **Realm Domain Name**.

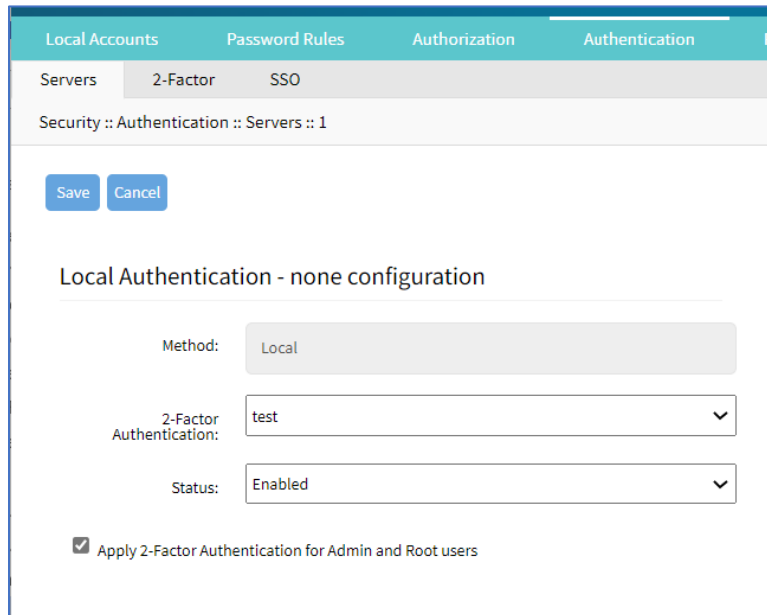
Enter **Domain Name**.

12. Click **Save**.

Set 2-Factor Authentication for Admin/Root Users

WebUI Procedure

1. Go to *Security :: Authentication :: Servers*.
2. In *Index* column, click the index to be updated (displays dialog).



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

WebUI Procedure

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

WebUI Procedure

1. Go to *Security :: Authentication :: Servers*.

2. Locate and select checkbox.
3. Click **Delete**.
4. On the confirmation pop-up dialog, click **OK**.

Move Index Up/Down

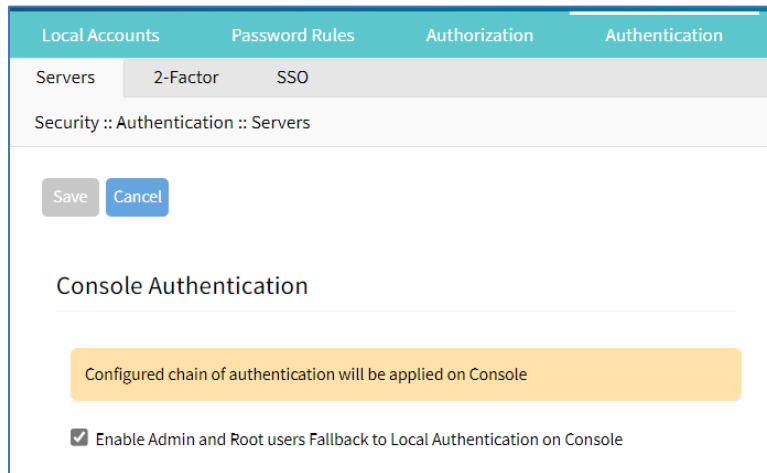
WebUI Procedure

1. Go to *Security :: Authentication :: Servers*.
2. Locate and select checkbox.
3. Click **Up** to move the selection up in the table.
4. Click **Down** to move the selection down in the table.
5. Click **Save**.

Enable/disable Console Authentication

WebUI Procedure

1. Go to *Security :: Authentication :: Servers*.
2. Locate and select checkbox).
3. Click **Console** (displays dialog).



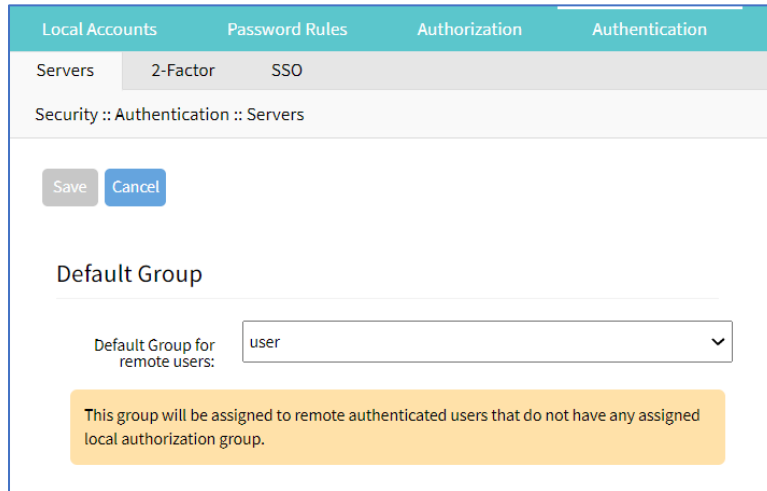
4. (as needed) Select/unselect **Enable Admin and Root users Fallback to Local Authentication on Console** checkbox.
5. Click **Save**.

Display Console

WebUI Procedure

1. Go to *Security :: Authentication :: Servers*.
2. Locate and select checkbox).

3. Click **Default Group** (displays dialog).



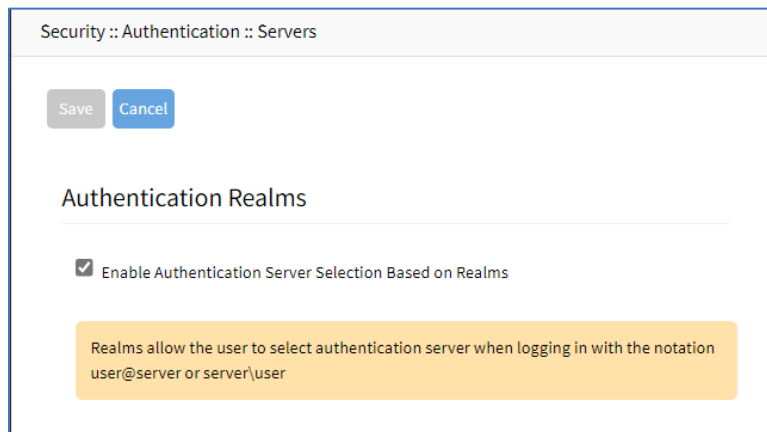
4. On the **Default Group for Remote Server** drop-down, select one.
5. Click **Save**.

Set Realms

Realms allow the user to select authentication server when logging in with the notation user@server or server\user

WebUI Procedure

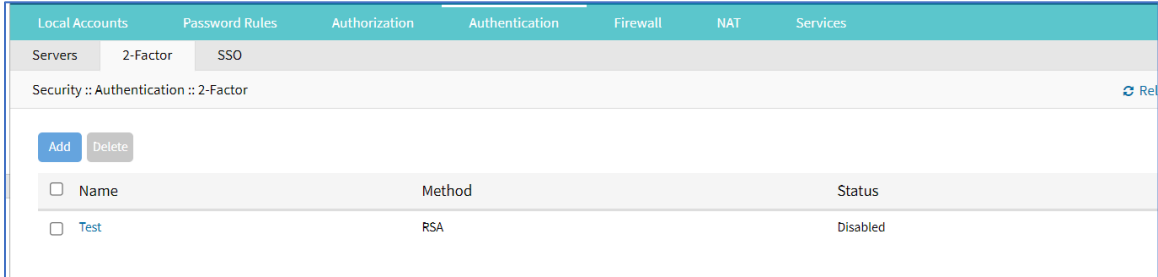
1. Go to *Security :: Authentication :: Servers*.
2. Locate and select checkbox.
3. Click **Realms** (displays dialog).



4. Click **Save**.

2-Factor sub-tab

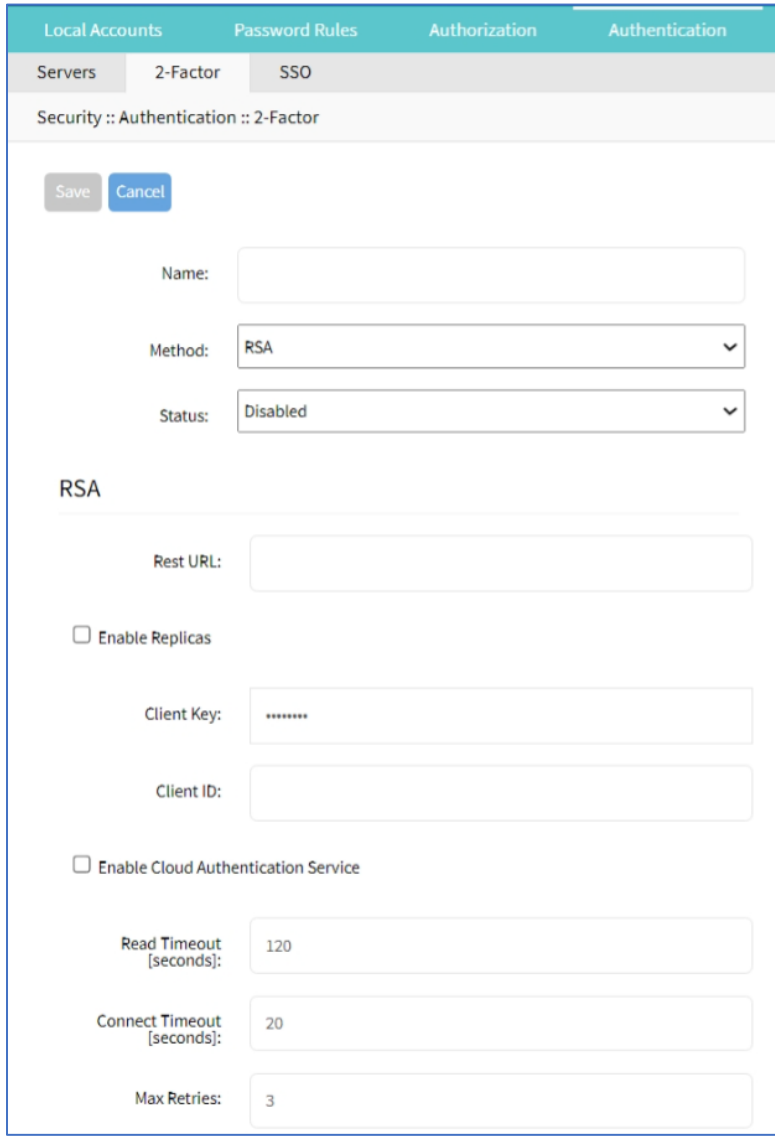
This sets up 2-factor authentication.



Add 2-Factor Configuration

WebUI Procedure

1. Go to *Security :: Authentication :: 2-Factor*.
2. Click **Add** (displays dialog)



3. Enter **Name**.

4. On **Method** drop-down, select one (**RSA**).
5. On **Status** drop-down, select one (**Enabled, Disabled**).
6. In *RSA* menu:
 - Enter **Rest URL**.
 - Select **Enable Replicas** checkbox.
 - Enter **Client Key**.
 - Enter **Client ID**.
 - Select **Enable Cloud Authentication Service** checkbox.
 - Enter **Read Timeout [seconds]** (default: 120).
 - Enter **Connect Timeout [seconds]** (default: 20).
 - Enter **Max Retries**.
7. Click **Save**.

Configure RSA SecurID (2-Factor)

Step 1 – Add SecurID (WebUI Procedure)

1. Go to *Security :: Authentication :: 2-Factor*.
2. Click **Add** (displays dialog)
3. 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. Select **Enable Replicas** (Rest Service URL to failover to the server (up to 15 replicas). One per line).
 - Client Key** (available through RSA Security Console. Copy/paste the **Access Key** from *SecurID Security Console*. The Access Key is also available at RSA SecurID Authentication API (under System Settings)
 - Client ID** (retrieve the Server Node name from the *Authentication Manager Contact List*.)
6. Select **Enable Cloud Authentication Service** checkbox (if enabled, two required fields display).
 - Policy ID** (access policy name configured in the Cloud Administration Console. Obtain this name from your Cloud Authentication Service Super Admin)
 - Tenant ID** (Tenant Id name created in the Cloud Administration Console. Obtain this name from your Cloud Authentication Service Super Admin)
7. Click **Save**.

Step 2 – Set Certificate to access SecurID Server (WebUI Procedure)

1. If RSA server is through Cloud Authentication:

Go to RSA SecurID Access and click the **Lock** icon (next to URL).

Locate and click on the Certificate.

On the pop-up dialog, click on the first/top certificate, and drag it to your desktop.

Upload certificate to Nodegrid (certificate is automatically converted to the expected format).

2. If not via Cloud:

Go the *RSA Operations Console*

Download the Signing Root Certificate.

Go to *Security :: Authentication :: 2-Factor*.

Click the link representing the SecurID server (added above).

Click **Certificate**.

Select **Local Computer** checkbox.

Click **Choose File** and select the file (i.e. RootCA.cer file).

Click **Apply**,

3. Click **Save**.

Edit 2-Factor Configuration

WebUI Procedure

1. Go to *Security :: Authentication :: 2-Factor*.
2. In *Name* column, click the name to be updated (displays dialog).
3. Make changes, as needed.
4. Click **Save**.

Delete 2-Factor Configuration

WebUI Procedure

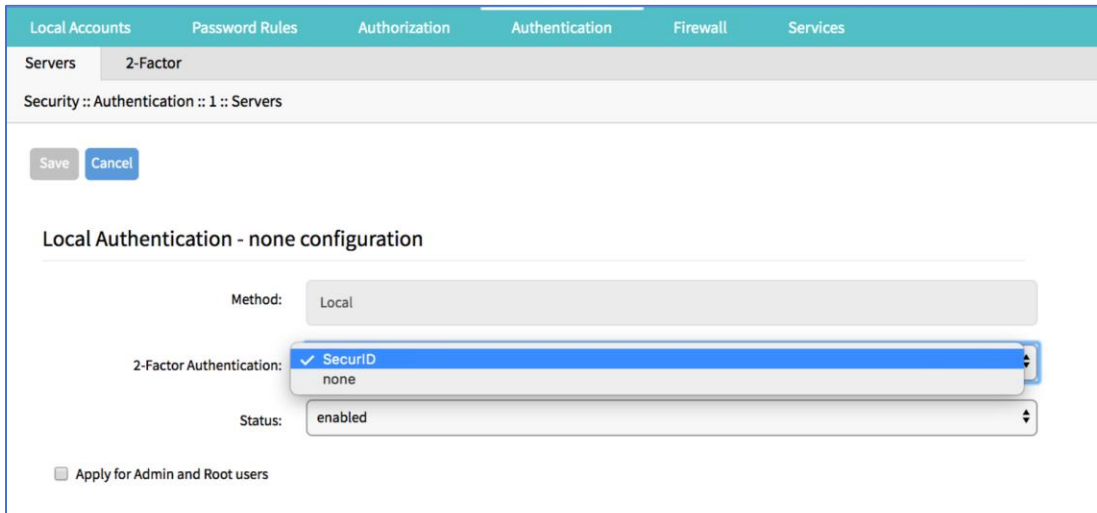
1. Go to *Security :: Authentication :: 2-Factor*.
2. Locate and select checkbox.
3. Click **Delete**.
4. On the confirmation pop-up dialog, click **OK**.

Assign 2-factor to an Authentication Method

RSA SecurID 2-factor authentication can be added to any of the Nodegrid-supported authentication methods: 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 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

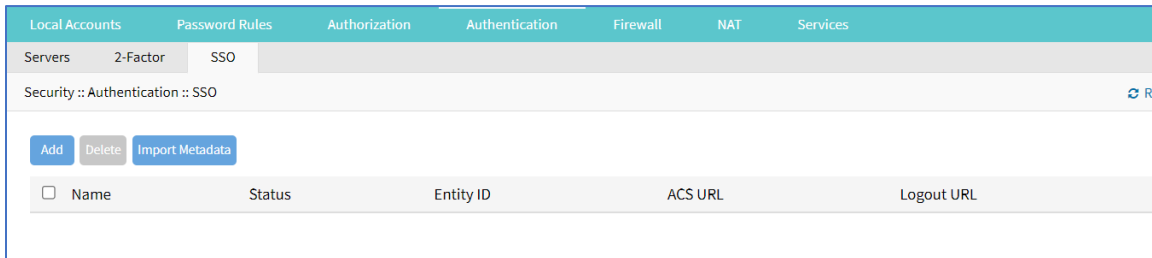
This applies only to Cloud Authentication Services.



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

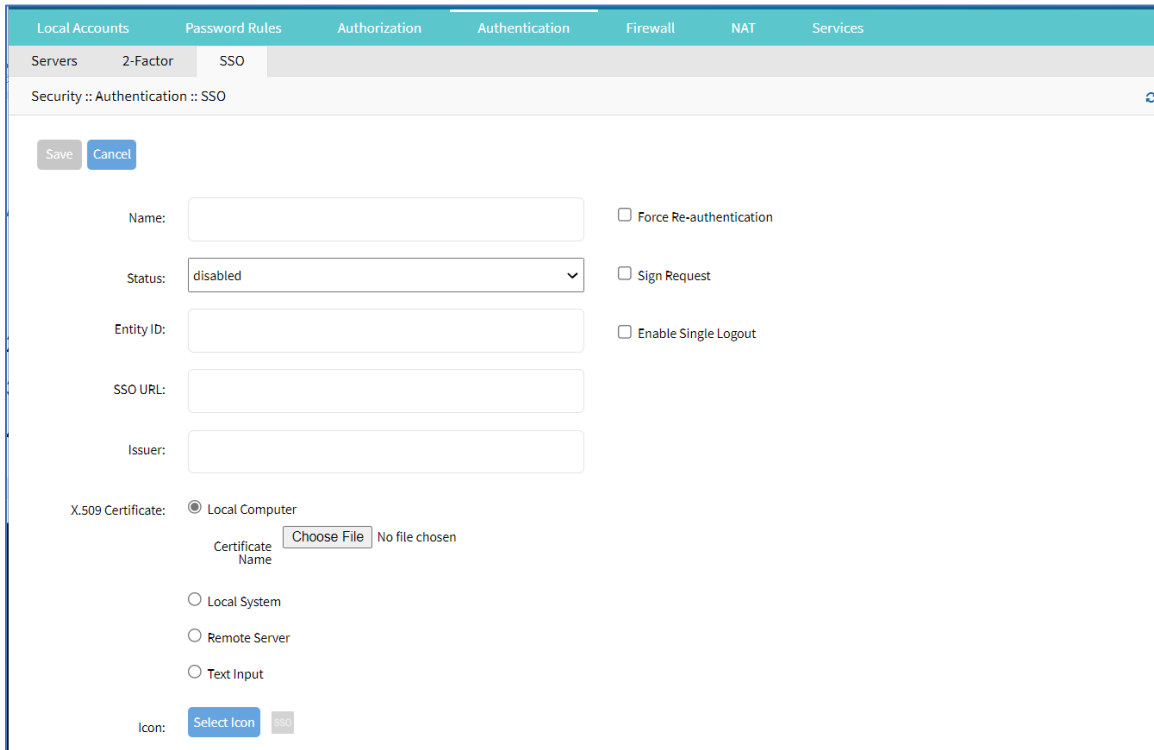
With Single Sign-On (SSO), users authenticate once to gain access to multiple secured systems without resubmitting credentials. Nodagrid currently supports multiple identify providers.



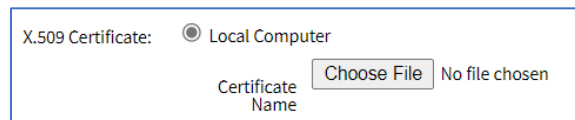
Add SSO

WebUI Procedure

1. Go to *Security :: Authentication :: SSO*.
2. Click **Add** (displays dialog).



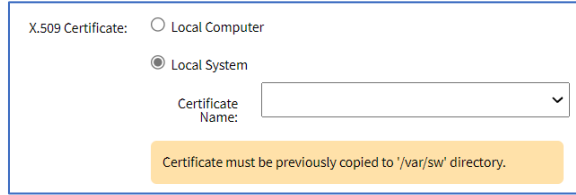
3. Enter **Name**.
4. On **Status** drop-down, select one (**Enabled, Disabled**).
5. Enter **Entity ID** (globally unique name).
6. Enter **SSO URL**.
7. Enter **Issuer**.
8. In *X-509 Certificate* menu, select one:
Local Computer radio button.



Click **Choose File**.

Locate and select file.

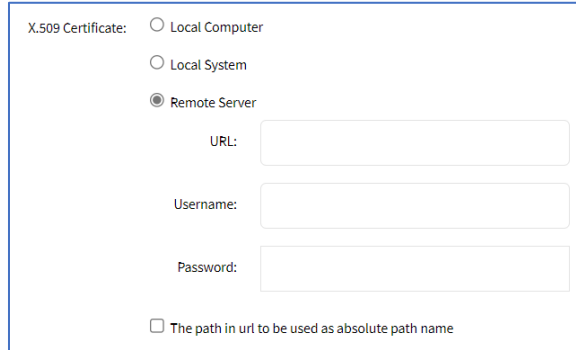
Local System radio button.



X.509 Certificate: Local Computer
 Local System
 Certificate Name:
 Certificate must be previously copied to '/var/sw' directory.

On **Certificate Name** drop-down, select one.

Remote Server radio button.



X.509 Certificate: Local Computer
 Local System
 Remote Server
 URL:
 Username:
 Password:
 The path in url to be used as absolute path name

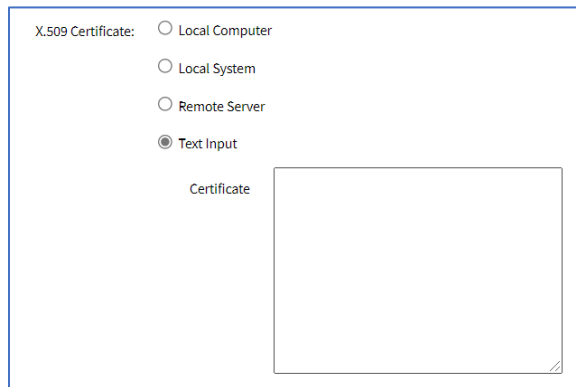
Enter **URL**.

Enter **Username**.

Enter **Password**.

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

Text Input radio button.



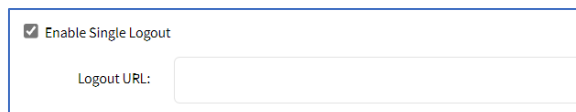
X.509 Certificate: Local Computer
 Local System
 Remote Server
 Text Input
 Certificate

In **Certificate** text box, enter details.

9. Select **Force Re-authentication** checkbox.

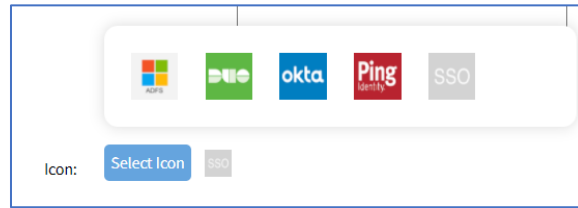
10. Select **Sign Request** checkbox.

11. Select **Enable Single Logout** checkbox. Enter **Logout URL**.



Enable Single Logout
 Logout URL:

12. (optional) In **Icon**, click **Select Icon**. 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 NOTE: The idpid from Ping is used as the SSO URL field in Nodegrid: <a +the+idpid"="" href="https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid=">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)

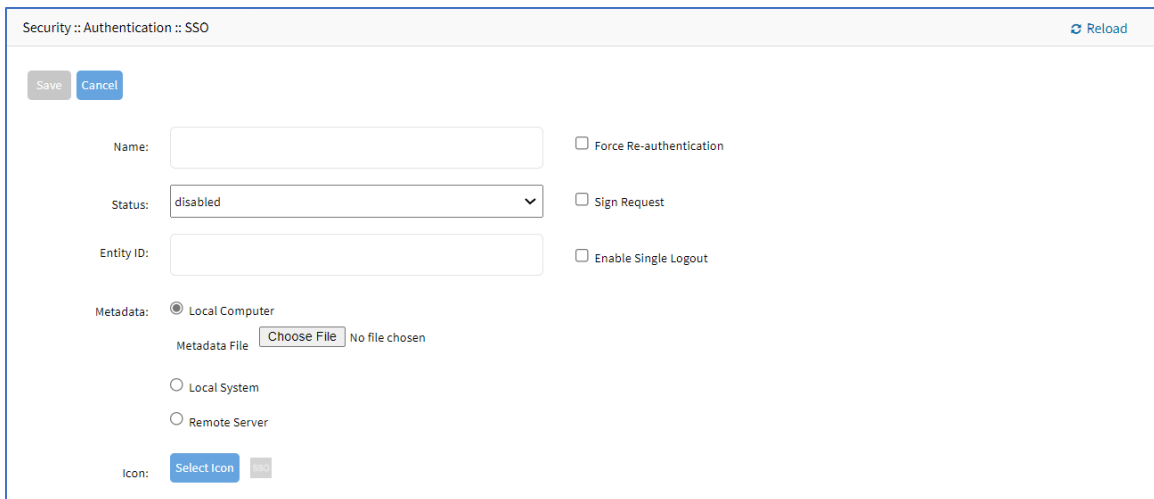
RelayState: (optional) (deep linking for SAML for <ip>/direct/<device>/console)

For more information on SSO, please see <https://support.zpesystems.com/portal/kb/articles/single-sign-on-ssso>

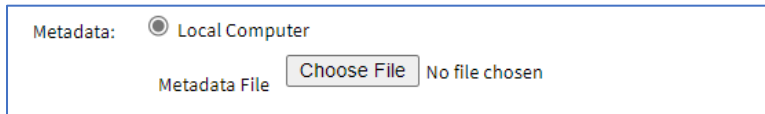
Import Metadata

WebUI Procedure

1. Go to *Security :: Authentication :: SSO*.
2. Click **Import Metadata** (displays dialog).



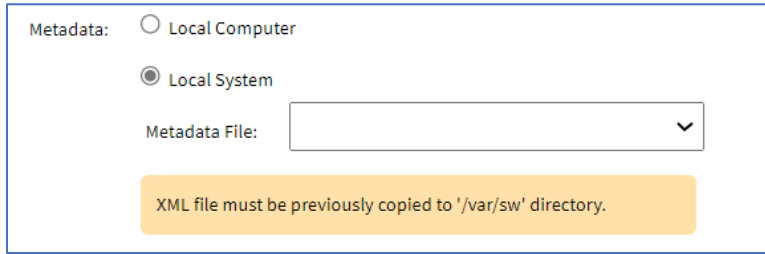
3. Enter **Name**.
4. On **Status** drop-down, select one (**Enabled, Disabled**).
5. Enter **Entity ID** (globally unique name).
6. In *Metadata* menu, select one:
Local Computer radio button.



Click **Choose File**.

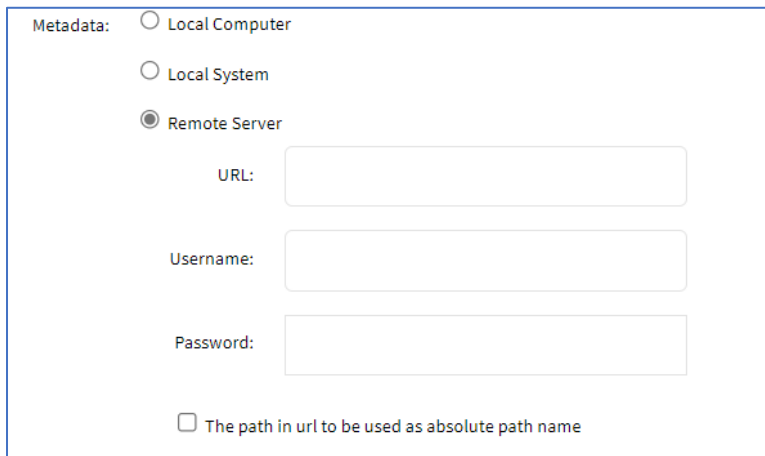
Locate and select file.

Local System radio button.



On **Metadata File** drop-down, select one.

Remote Server radio button.



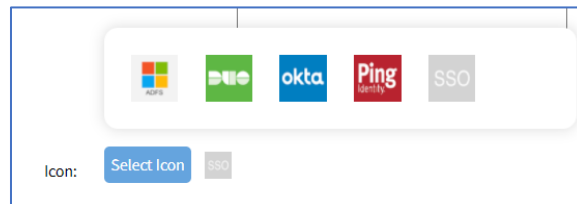
Enter **URL**.

Enter **Username**.

Enter **Password**.

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

7. (optional) In **Icon**, click **Select Icon**. Click on a logo to set as 2-Factor icon.



8. Select **Force Re-authentication** checkbox.

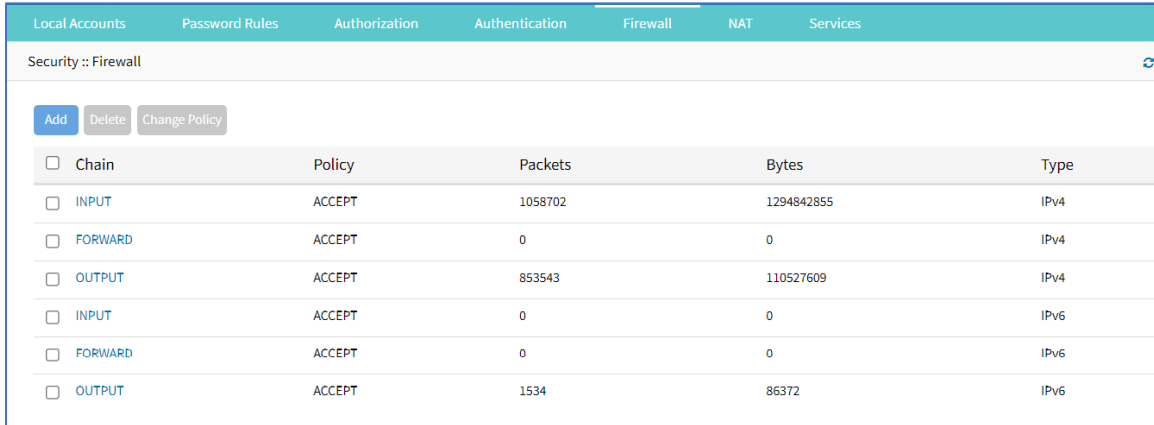
9. Select **Sign Request** checkbox.

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.)



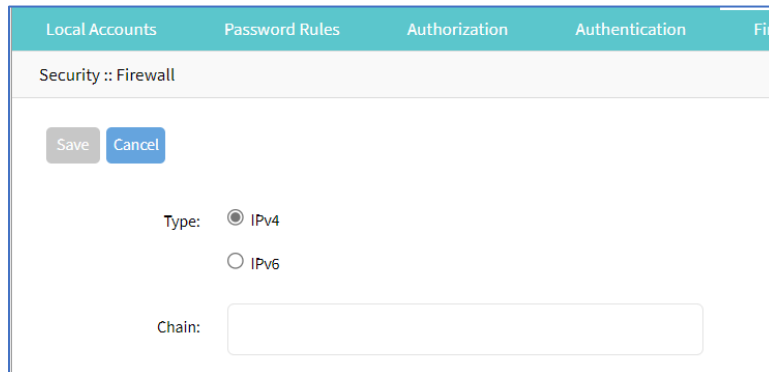
Chain	Policy	Packets	Bytes	Type
<input type="checkbox"/> INPUT	ACCEPT	1058702	1294842855	IPv4
<input type="checkbox"/> FORWARD	ACCEPT	0	0	IPv4
<input type="checkbox"/> OUTPUT	ACCEPT	853543	110527609	IPv4
<input type="checkbox"/> INPUT	ACCEPT	0	0	IPv6
<input type="checkbox"/> FORWARD	ACCEPT	0	0	IPv6
<input type="checkbox"/> OUTPUT	ACCEPT	1534	86372	IPv6

Manage Chains

Add a Chain

WebUI Procedure

1. Go to *Security :: Firewall*.
2. Click **Add** (displays dialog).



Security :: Firewall

Save Cancel

Type: IPv4
 IPv6

Chain:

3. For **Type**, select one:
 - IPv4** radio button
 - IPv6** radio button
4. Enter **Chain** (name of this chain).
5. Click **Save**.

Delete a Chain

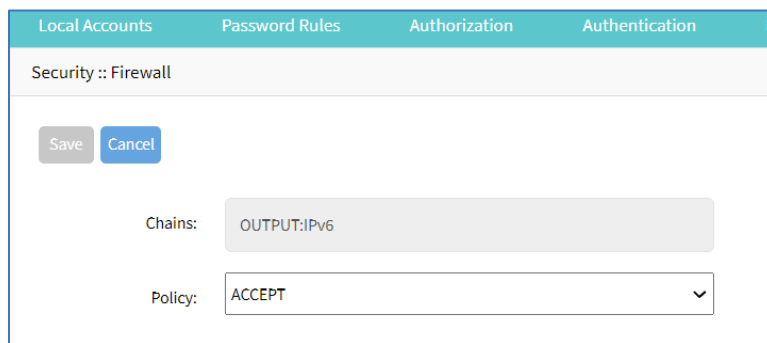
WebUI Procedure

1. Go to *Security :: Firewall*.
2. Select checkbox next to name to be deleted.
3. Click **Delete**.
4. On confirmation pop-up dialog, click **OK**.

Change Chain Policy

WebUI Procedure

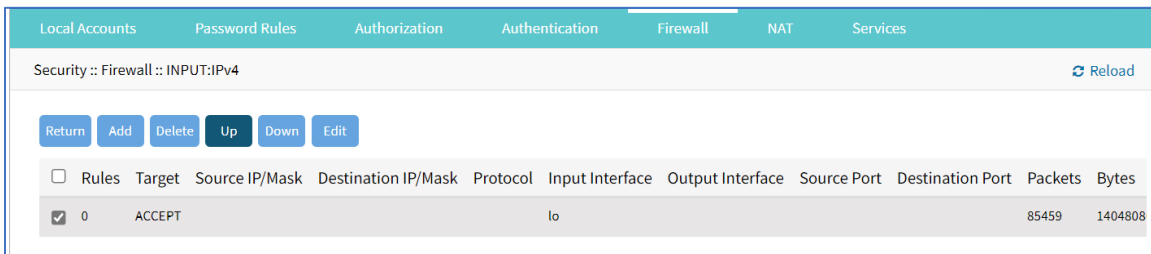
1. Go to *Security :: Firewall*.
2. In the *Chain* column, locate and click the name (displays dialog).



3. On **Policy** drop-down, select one (**ACCEPT**, **DROP**).
4. Click **Save**.

Options to Manage a Chain

To manage chain functions/settings, click on the name in the *Chain* column (displays dialog).

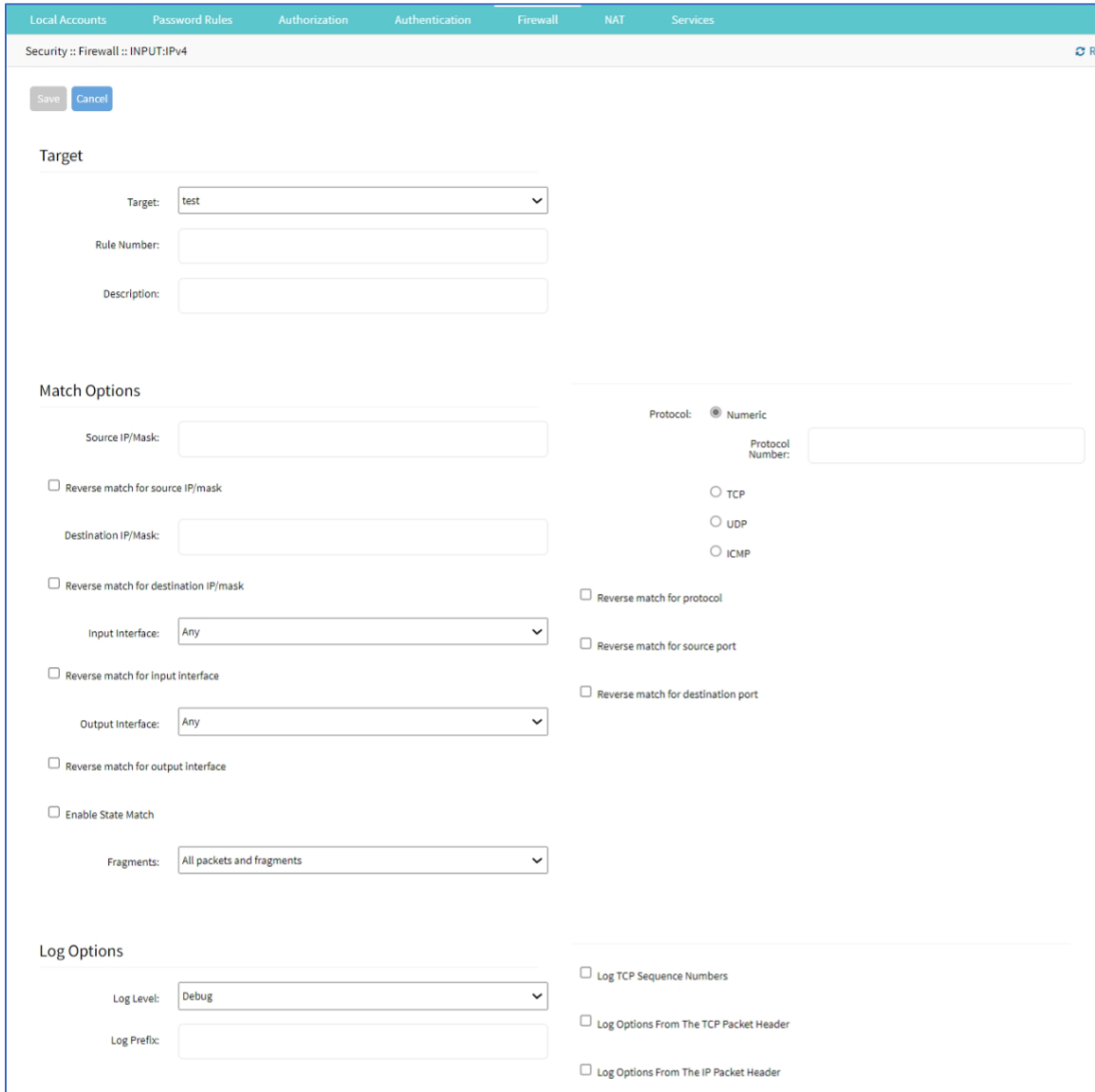


Rules	Target	Source IP/Mask	Destination IP/Mask	Protocol	Input Interface	Output Interface	Source Port	Destination Port	Packets	Bytes
<input checked="" type="checkbox"/> 0	ACCEPT				lo				85459	1404808

Add Chain

WebUI Procedure

1. Go to *Security :: Firewall*.
2. In the *Chain* column, locate and click on the name (displays dialog).
3. Click **Add** (displays dialog).



The screenshot shows the Firewall configuration page for 'Security :: Firewall :: INPUT:IPv4'. It includes sections for Target, Match Options, and Log Options. The Target section has a dropdown menu set to 'test'. Match Options include fields for Source IP/Mask, Destination IP/Mask, Input Interface (set to 'Any'), and Output Interface (set to 'Any'), along with checkboxes for reverse matching and state matching. Log Options include a dropdown for Log Level (set to 'Debug') and a field for Log Prefix. There are also checkboxes for logging TCP sequence numbers and options from packet headers.

4. In *Target* menu:

In **Target** drop-down, select one (**ACCEPT, DROP, REJECT, LOG, RETURN**).

Enter **Rule Number**.

Enter **Description**.

If **REJECT** selected, *Reject Options* menu displays:



The screenshot shows the 'Reject Options' section with a dropdown menu labeled 'Reject With' set to 'No Route'.

In **Reject With** drop-down, select one (**Network Unreachable, Host Unreachable, Port Unreachable, Protocol Unreachable, Network Prohibited, Host Prohibited, Administratively Prohibited, TCP Reset**).

5. In *Match Options* menu:

Enter **Source IP/Mask**.

Select **Reverse match for source IP/mask** checkbox.

Enter **Destination IP/Mask**.

Select **Reverse match for destination IP/mask** checkbox.

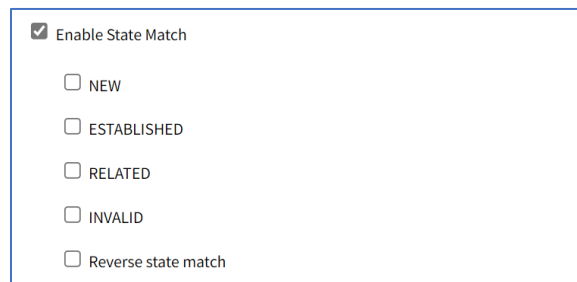
On **Input Interface** drop-down, select one (**Any, lo, eth0, eth1**).

Select **Reverse match for input interface** checkbox.

On **Output Interface** drop-down, select one (**Any, lo, eth0, eth1**).

Select **Reverse match for output interface** checkbox.

Select **Enable State Match** checkbox (displays options – one or more can be selected):



NEW checkbox.

ESTABLISHED checkbox.

RELATED checkbox.

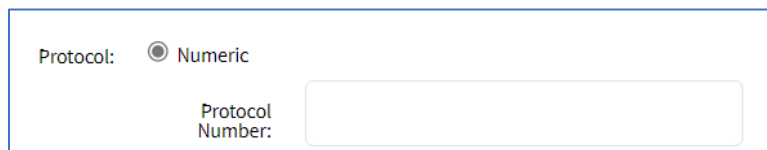
INVALID checkbox.

Reverse state match checkbox

On **Fragments** drop-down, select one (**All packets and fragments, Unfragmented packets and 1st packets, 2nd and further packets**).

In *Protocol* menu, select one:

Numeric radio button. Enter **Protocol Number**.



TCP radio button

Protocol: Numeric

TCP

Source Port:

Destination Port:

TCP Flag SYN: ▼

TCP Flag ACK: ▼

TCP Flag FIN: ▼

TCP Flag RST: ▼

TCP Flag URG: ▼

TCP Flag PSH: ▼

Reverse match for TCP flags

UDP

ICMP

Enter **Source Port**.

Enter **Destination Port**.

On **TCP Flag SYN** drop-down, select one (**Any, Set, Unset**).

On **TCP Flag ACK** drop-down, select one (**Any, Set, Unset**).

On **TCP Flag FIN** drop-down, select one (**Any, Set, Unset**).

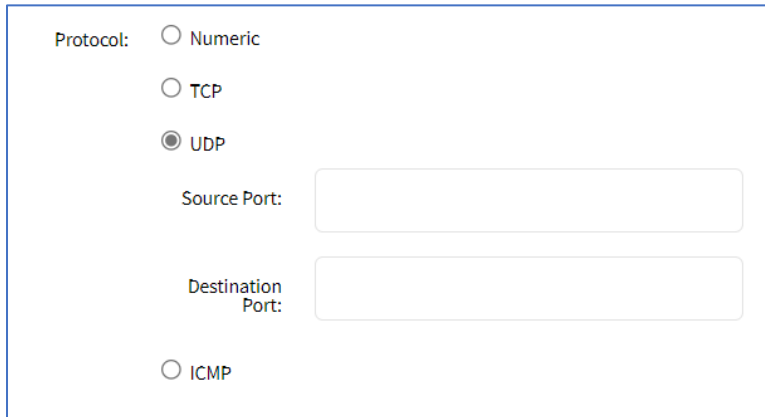
On **TCP Flag RST** drop-down, select one (**Any, Set, Unset**).

On **TCP Flag URG** drop-down, select one (**Any, Set, Unset**).

On **TCP Flag PSH** drop-down, select one (**Any, Set, Unset**).

Select **Reverse Match for TCP Flags** checkbox.

UDP radio button. Enter **Source Port**. Enter **Destination Port**.

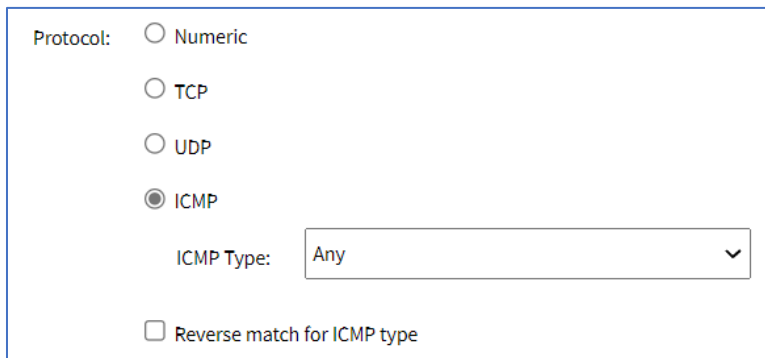


Protocol: Numeric
 TCP
 UDP
Source Port:
Destination Port:
 ICMP

Enter **Source Port**.

Enter **Destination Port**.

ICMP radio button.



Protocol: Numeric
 TCP
 UDP
 ICMP
ICMP Type:
 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 protocol** checkbox.

Select **Reverse match for source port** checkbox.

Select **Reverse match for destination port** checkbox.

6. In *Log Options* menu:

On **Log Level** drop-down, select one (**Debug**, **Info**, **Notice**, **Warning**, **Error**, **Critical**, **Alert**, **Emergency**).

Enter **Log Prefix**.

Select **Log TCP Sequence Numbers** checkbox.

Select **Log Options from the TCP Packet Header** checkbox.

Select **Log Options from the IP Packet Header** checkbox.

7. Click **Save**.

Edit Chain

WebUI Procedure

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

WebUI Procedure

1. Go to *Security :: Firewall*.
2. In the *Chain* column, locate and select checkbox on the name.
3. Click **Delete**.
4. On the confirmation pop-up dialog, click **OK**.

Move Chain Up/Down

WebUI Procedure

1. Go to *Security :: Firewall*.
2. In the *Chain* column, locate and select checkbox on the name.
3. Click **Up** to move up.
4. Click **Down** to move down.

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.

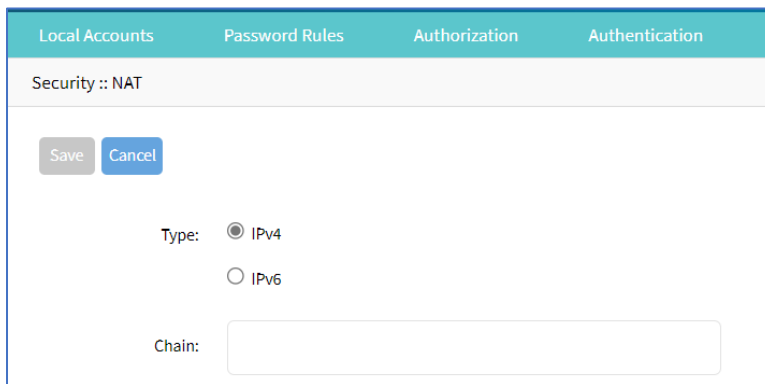
Chain	Policy	Packets	Bytes	Type
<input type="checkbox"/> Chain				
<input type="checkbox"/> PREROUTING	ACCEPT	61740	7793280	IPv4
<input type="checkbox"/> INPUT	ACCEPT	61653	7785918	IPv4
<input type="checkbox"/> OUTPUT	ACCEPT	455097	30146854	IPv4
<input type="checkbox"/> POSTROUTING	ACCEPT	455097	30146854	IPv4
<input type="checkbox"/> PREROUTING	ACCEPT	219	33655	IPv6
<input type="checkbox"/> INPUT	ACCEPT	0	0	IPv6
<input type="checkbox"/> OUTPUT	ACCEPT	44	3168	IPv6
<input type="checkbox"/> POSTROUTING	ACCEPT	44	3168	IPv6

Manage Chains

Add a Chain

WebUI Procedure

1. Go to *Security :: NAT*.
2. Click **Add** (displays dialog).



3. For **Type**, select one
 - IPv4** radio button
 - IPv6** radio button
4. Enter **Chain** (name of this chain).
5. Click **Save**.

Delete a Chain

WebUI Procedure

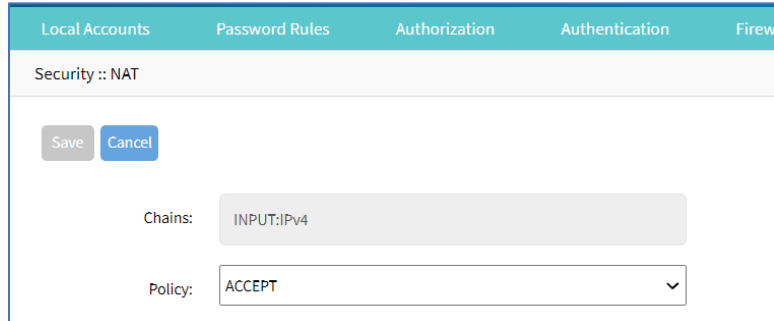
1. Go to *Security :: NAT*.
2. Select checkbox next to name to be deleted.

3. Click **Delete**.
4. On confirmation pop-up dialog, click **OK**.

Change Chain Policy

WebUI Procedure

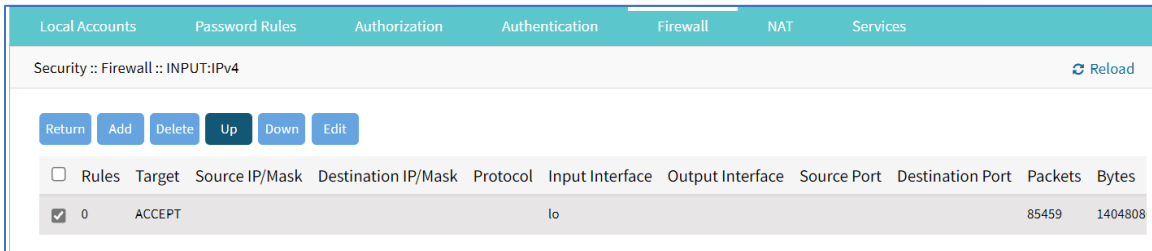
1. Go to *Security :: NAT*.
2. In the *Chain* column, locate and click the name (displays dialog).



3. On **Policy** drop-down, select one (**ACCEPT**, **DROP**).
4. Click **Save**.

Manage Chain Settings

To manage chain functions/settings, click on the name in the *Chain* column (displays dialog).

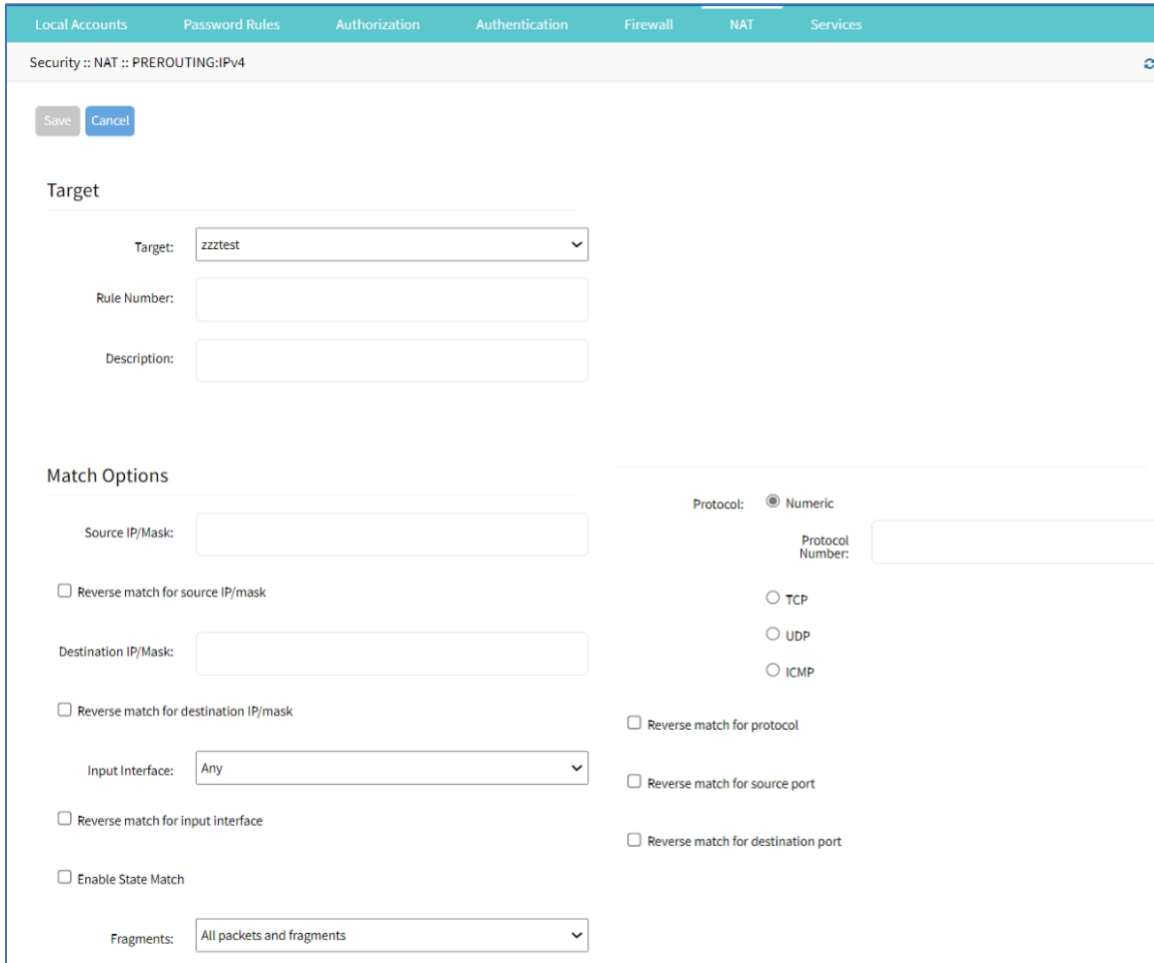


Rules	Target	Source IP/Mask	Destination IP/Mask	Protocol	Input Interface	Output Interface	Source Port	Destination Port	Packets	Bytes
<input checked="" type="checkbox"/>	0	ACCEPT			lo				85459	1404808

Add Chain Setting (all Type selections)

WebUI Procedure

1. Go to *Security :: NAT*.
2. In the *Chain* column, locate and click on the name (displays dialog).
3. Click **Add** (displays dialog).



The screenshot shows the NAT configuration page for 'Security :: NAT :: PREROUTING:IPv4'. It features a 'Target' section with a dropdown menu set to 'zzztest', and empty input fields for 'Rule Number' and 'Description'. The 'Match Options' section includes input fields for 'Source IP/Mask' and 'Destination IP/Mask', each with a corresponding 'Reverse match for source IP/mask' and 'Reverse match for destination IP/mask' checkbox. There is also an 'Input Interface' dropdown set to 'Any' with a 'Reverse match for input interface' checkbox. A 'Fragments' dropdown is set to 'All packets and fragments'. On the right, the 'Protocol' is set to 'Numeric' with a 'Protocol Number' input field, and radio buttons for 'TCP', 'UDP', and 'ICMP'. There are also checkboxes for 'Reverse match for protocol', 'Reverse match for source port', and 'Reverse match for destination port'. 'Save' and 'Cancel' buttons are at the top left.

4. In *Target* menu:

In **Target** drop-down, select one (**ACCEPT, DNAT, REDIRECT, LOG, RETURN**).

Enter **Rule Number**.

Enter **Description**.

5. In *Match Options* menu:

Enter **Source IP/Mask**.

Select **Reverse match for source IP/mask** checkbox.

Enter **Destination IP/Mask**.

Select **Reverse match for destination IP/mask** checkbox.

On **Input Interface** drop-down, select one (**Any, lo, eth0, eth1**).

Select **Reverse match for input interface** checkbox.

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

On **Fragments** drop-down, select one (**All packets and fragments**, **Unfragmented packets and 1st packets**, **2nd and further packets**).

(Type selection: **DNAT**) Enter **To Destination**.

Fragments:	All packets and fragments	▼
To Destination:	<input type="text"/>	

In *Protocol* menu, select one:

Numeric radio button. Enter **Protocol Number**.

Protocol:	<input checked="" type="radio"/> Numeric
Protocol Number:	<input type="text"/>

TCP radio button

Protocol: Numeric
 TCP

Source Port:

Destination Port:

To Ports:

TCP Flag SYN: ▼

TCP Flag ACK: ▼

TCP Flag FIN: ▼

TCP Flag RST: ▼

TCP Flag URG: ▼

TCP Flag PSH: ▼

Reverse match for TCP flags

Enter **Source Port**.

Enter **Destination Port**.

Enter **To Ports**

On **TCP Flag SYN** drop-down, select one (**Any, Set, Unset**).

On **TCP Flag ACK** drop-down, select one (**Any, Set, Unset**).

On **TCP Flag FIN** drop-down, select one (**Any, Set, Unset**).

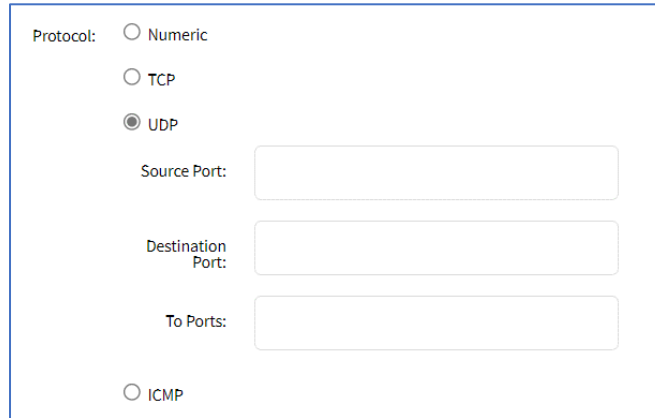
On **TCP Flag RST** drop-down, select one (**Any, Set, Unset**).

On **TCP Flag URG** drop-down, select one (**Any, Set, Unset**).

On **TCP Flag PSH** drop-down, select one (**Any, Set, Unset**).

Select **Reverse Match for TCP Flags** checkbox.

UDP radio button.



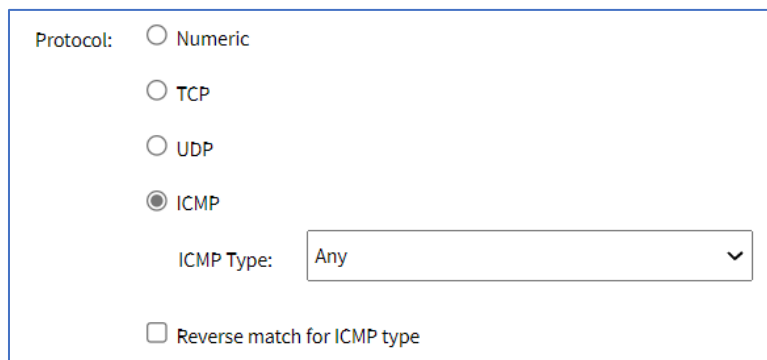
Protocol: Numeric
 TCP
 UDP
Source Port:
Destination Port:
To Ports:
 ICMP

Enter **Source Port**.

Enter **Destination Port**.

Enter **To Ports**.

ICMP radio button



Protocol: Numeric
 TCP
 UDP
 ICMP
ICMP Type:
 Reverse match for ICMP type

On **ICMP Type** drop-down, select one (

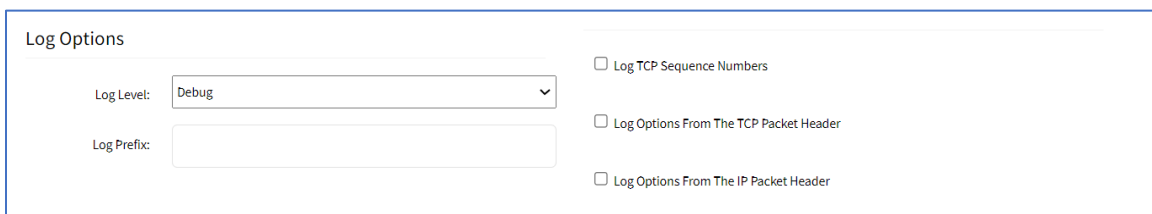
Select **Reverse match for ICMP type** checkbox.

Select **Reverse match for protocol** checkbox.

Select **Reverse match for source port** checkbox.

Select **Reverse match for destination port** checkbox.

6. In *Log Options* menu (only if **Type** selection: **LOG**).



Log Options
Log Level:
Log Prefix:
 Log TCP Sequence Numbers
 Log Options From The TCP Packet Header
 Log Options From The IP Packet Header

On **Log Level** drop-down, select one (**Debug, Info, Notice, Warning, Error, Critical, Alert, Emergency**).

Enter **Log Profile** (name of this profile).

Select **Log TCP Sequence Numbers** checkbox.

Select **Log Options From The TCP Packet Header** checkbox.

Select **Log Options From The IP Packet Header** checkbox.

7. Click **Save**.

Edit Chain Setting

WebUI Procedure

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

WebUI Procedure

1. Go to *Security :: NAT*.
2. In the *Chain* column, locate and select checkbox next to name.
3. Click **Delete**.
4. On the confirmation pop-up dialog, click **OK**.

Move Up/Down

WebUI Procedure

1. Go to *Security :: NAT*.
2. In the *Chain* column, locate and select checkbox on the name.
3. Click **Up** to move up.
4. 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.

Local Accounts Password Rules Authorization Authentication Firewall NAT Services GEO Fence

General Services Intrusion Prevention

Security :: Services :: General Services Reload

Save

ZPE Cloud

- Enable ZPE Cloud
 - ZPE Cloud URL:
 - Enable Remote Access
 - Enable File Protection
- System Profile:

Active Services

- Enable detection of USB devices
- Enable RPC
- Enable gRPC
- Enable FTP Service
- Enable S/NMP Service
- Enable Teinet Service to Nodegrid
- Enable Teinet Service to Managed Devices
- Enable ICMP echo reply
- Enable ICMP secure redirects
- Enable USB over IP
- Enable Elasticsearch
 - Enable Kibana
- Enable Telegraf

Enable Virtualization Services

- Enable Docker
- Enable Qemu/KVM
- Enable VMware Manager
 - Cluster TCP Port:
- Enable Automatic Cluster Enrollment
 - Search Engine TCP Port:
 - Enable Search Engine High Level Cipher Suite
- Enable VM Serial access
 - VM Serial Port:
 - vMotion timeout (seconds):
- Enable Zero Touch Provisioning
- Enable Bluetooth
 - Display name:
 - Enable Bluetooth Discoverable mode
- Enable PXE (Preboot execution Environment)
- Block host with multiple authentication fails
- Allow root console access

Managed Devices

- Device access enforced via user group authorization
- Enable Autodiscovery
 - DHCP lease controlled by autodiscovery rules

SSH

- SSH allow root access
- SSH TCP Port:
- SSH Ciphers:
- SSH MACs:
- SSH KeyAlgorithms:

Web Service

- Enable HTTP access
 - HTTP Port:
- Enable HTTPS access
 - HTTPS Port:
- Redirect HTTP to HTTPS

Cryptographic Protocols

- TLSv1.3
- TLSv1.2
- TLSv1.1
- TLSv1
- Cipher Suite Level:
 - High
 - Medium
 - Low
 - Custom

Changes affecting HTTP and HTTPS services will terminate all HTTP sessions

Configure General Services

WebUI Procedure

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

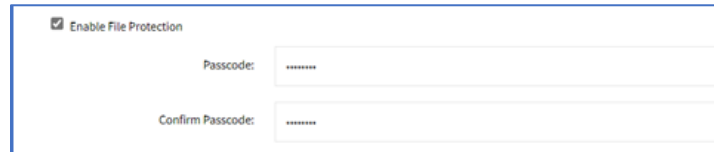
2. In *ZPE Cloud* menu (cloud-based management platform for Nodegrid products):

Select **Enable ZPE Cloud** checkbox (Nodegrid NSR, GSR, BSR, LSR, HSR - default: enabled. Nodegrid Serial Console - default: disabled).

Confirm **ZPE Cloud URL** (read-only).

Select **Enable Remote Access** checkbox.

(optional) Select **Enable File Protection** checkbox (If enabled, file transfer requires authentication hash based on this password to validate file integrity and origin – default: disabled).

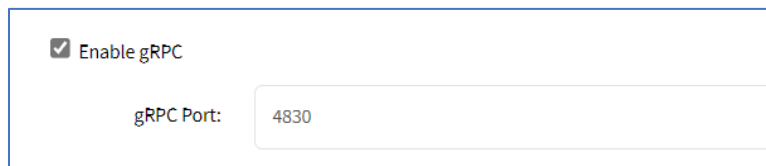


3. In *Active Services* menu (select all that apply):

Select **Enable detection of USB devices** checkbox.

Select **Enable RPC** checkbox.

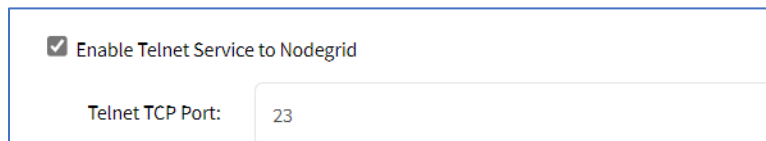
Select **Enable gRPC** checkbox. Enter **gRPC Port**.



Select **Enable FTP Service** checkbox.

Select **Enable SNMP Service** checkbox (default: enabled).

Select **Enable Telnet Service to Nodegrid** checkbox. Enter **Telnet TCP Port** (default: 23).



Select **Enable Telnet Service to Managed Devices** checkbox.

Select **Enable ICMP echo reply** checkbox.

Select **Enable ICMP secure redirects** checkbox.

Select **Enable USB over IP** checkbox.

Select **Enable Elasticsearch** checkbox. Select **Enable Kibana** checkbox.

Enable Elasticsearch

Enable Kibana

4. In *Enable Virtualization Services* menu (select all that apply):

Select **Enable Docker** checkbox.

Select **Enable Qemu/KVM** checkbox.

Select **Enable VMware Manager** checkbox.

Enter **Cluster TCP Port** (default: 9966).

Select **Enable Automatic Cluster Enrollment** checkbox.

Enter **Search Engine TCP Port** (default: 9300).

Select **Enable Search Engine High Level Cipher Suite** checkbox.

Select **Enable VM Serial access** checkbox (default: enabled).

Enable VM Serial access

VM Serial Port:

vMotion timeout [seconds]:

Enter **VM Serial Port** (default: 9977).

Enter **vMotion timeout [seconds]** (default: 300).

Select **Enable Zero Touch Provisioning** checkbox (default: enabled).

Select **Enable Bluetooth** checkbox.

Enable Bluetooth

Display name:

Enable Bluetooth Discoverable mode

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.

Enter **Display name**.

NOTE: Name displayed on other devices paired with this device via Bluetooth (default format: <ProductName_SerialNumber>.

Select **Enable Bluetooth Discoverable mode** checkbox.

NOTE: (default: enabled) Enables discovery and pairing 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.

Select **Enable PXE (Preboot eXecution Environment)** checkbox (default: enabled).

Select **Block host with multiple authentication fails** checkbox.

Block host with multiple authentication fails

Period Host will stay blocked (min):

Timeframe to monitor authentication fails (min):

Number of authentication fails to block host:

Whitelisted IP Addresses:

Enter **Period Host will stay blocked (min)** (default: 10).

Enter **Timeframe to monitor authentication fails (min)** (default: 10).

Enter **Number of authentication fails to block host** (default: 5).

Enter **Whitelisted IP Addresses** (comma-separated).

Select **Allow root console access** checkbox.

5. In *Managed Devices* menu (select all that apply):

Select **Device access enforced via user group authorization** checkbox (If enabled, users can only access devices listed in user's authorization groups. If not enabled, all enrolled devices are available.).

Select **Enable Autodiscovery** checkbox. Select **DHCP lease controlled by autodiscovery rules** checkbox (default: auto-selected).

Enable Autodiscovery

DHCP lease controlled by autodiscovery rules

6. In *SSH* menu:

Select **SSH allow root access** checkbox (default: enabled).

Enter **SSH TCP Port** (default: 22).

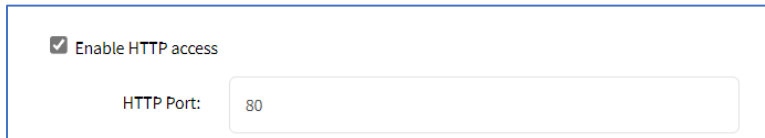
Enter **SSH Ciphers** (comma-separated) (default: blank).

Enter **SSH MACs** (comma-separated) (default: blank).

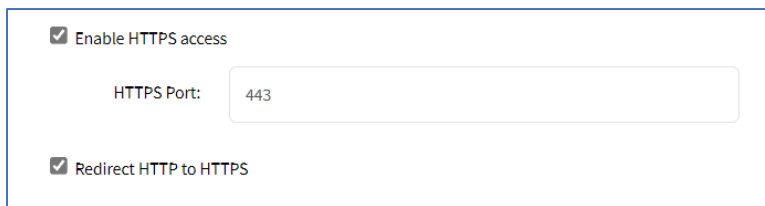
Enter **SSH KexAlgorithms** (comma-separated) (default: blank).

7. In *Web Service* menu:

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).

Select **Enable HTTP/S File Repository** checkbox (default: disabled) when enabled, provides public access of files uploaded in the File Manager/datastore (https://<Nodegrid URL>/datastore/<filename.ext>) For security reasons, full path of the file is required. For security reasons, listing, edit and post are disabled.

8. In *Cryptographic Protocols* menu:

Select **TLSv1.3** checkbox (default: enabled).

Select **TLSv1.2** checkbox (default: enabled).

Select **TLSv1.1** checkbox (default: enabled).

Select **TLSv1** checkbox (default: disabled).

In *Cipher Suite Level* menu, select one:

High radio button.

Medium radio button (default).

Low radio button.

Custom radio button. Enter **Custom Cipher Suite**.

Cipher Suite Level: High
 Medium
 Low
 Custom

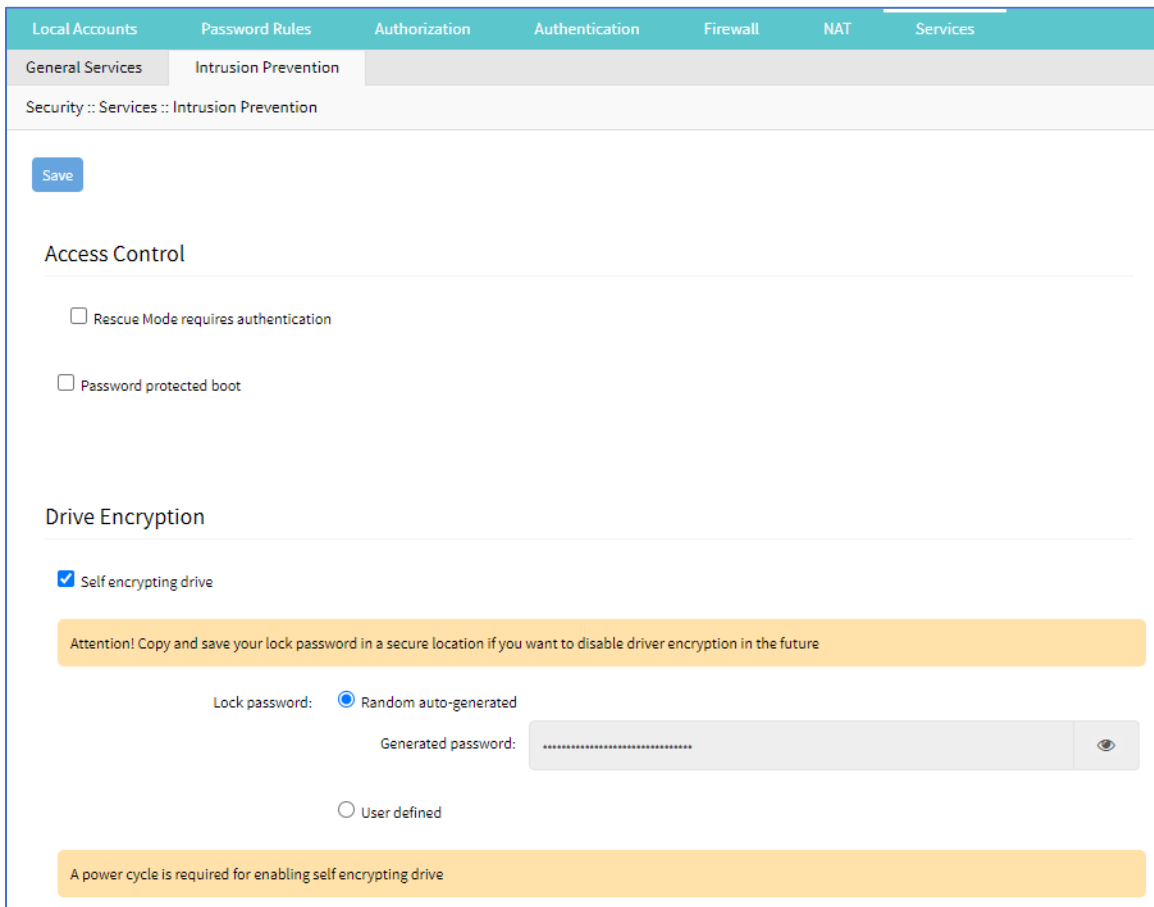
Custom Cipher Suite:

9. Click **Save**.

ZPE Cloud ensures all deployment activity is done at the device location.

Intrusion Prevention sub-tab

This configures intrusion prevention settings.



The screenshot shows the 'Intrusion Prevention' sub-tab under 'Services'. The breadcrumb path is 'Security :: Services :: Intrusion Prevention'. A 'Save' button is located at the top left. The configuration is divided into two sections: 'Access Control' and 'Drive Encryption'. Under 'Access Control', there are two unchecked checkboxes: 'Rescue Mode requires authentication' and 'Password protected boot'. Under 'Drive Encryption', the 'Self encrypting drive' checkbox is checked. A yellow warning box states: 'Attention! Copy and save your lock password in a secure location if you want to disable driver encryption in the future'. Below this, the 'Lock password' is set to 'Random auto-generated', and the 'Generated password' is displayed as a series of dots with an eye icon to toggle visibility. The 'User defined' option is also present but unchecked. A final yellow warning box at the bottom states: 'A power cycle is required for enabling self encrypting drive'.

Configure Intrusion Prevention

WebUI Procedure

1. Go to *Security :: Services :: Intrusion Prevention*.
2. In *Access Control* menu:

Select **Rescue Mode requires authentication** checkbox.

Select **Password protected boot** checkbox (password required to reboot).

3. In *Drive Encryption* menu:

NOTE: This menu is only available if the drive is OPAL 2 compliant.

Select **Self encrypting drive** checkbox. If enabled, the device must be restarted for the change to take effect.

In *Lock Password* menu, select one:

Random auto-generated radio button (save password in a secure location - cannot be recovered if lost).

User defined radio button. Enter **Password**.

4. Click **Save**.

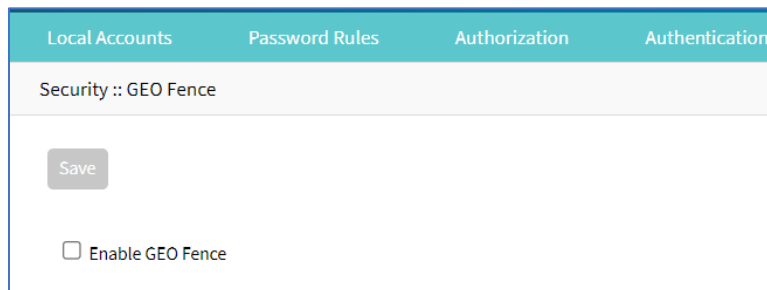
GEO Fence tab

Manage GEO Fence

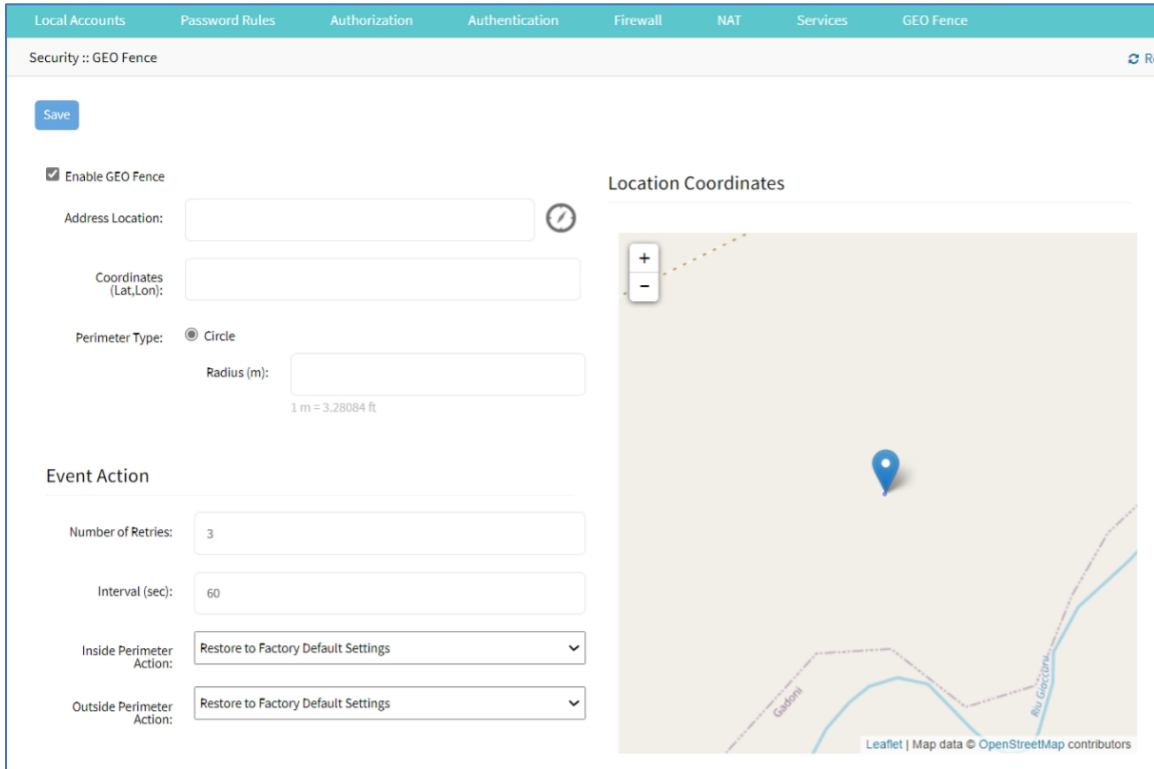
Enable GEO Fence


WebUI Procedure

1. Go to *Security :: GEO Fence*.



2. Select **Enable GEO Fence** checkbox (displays dialog).



3. Enter **Address Location** (a valid address for the device location).
4. Enter **Coordinates (Lat, Lon)** (if GPS is available, click **Compass** icon  or manually enter GPS coordinates).
5. In **Perimeter Type** menu:
 - Select **Circle** radio button (default).
 - Enter **Radius (m)**.
6. In **Event Action** menu:
 - Enter **Number of Retries** (default: 3).
 - Enter **Interval (sec)** (default: 60).
 - On **Inside Perimeter Action** drop-down, select one (**template.py**, **template.sh**, **template_change_system_init.sh**, **template_send_sms.sh**, **Restore to Factory Default Settings**).
 - On **Outside Perimeter Action** drop-down, select one (**template.py**, **template.sh**, **template_change_system_init.sh**, **template_send_sms.sh**, **Restore to Factory Default Settings**).
7. 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 the system and boot into Rescue Mode.

4. Execute the script:

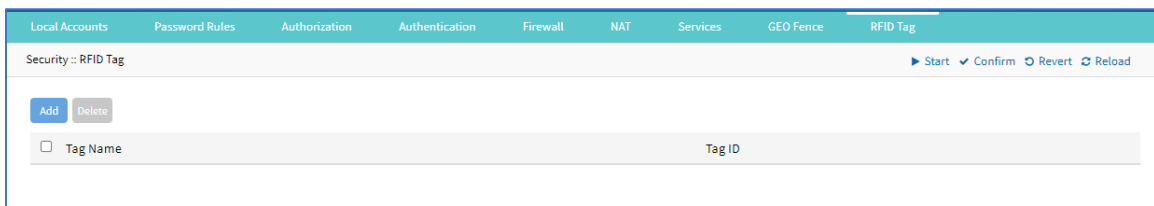
```
/usr/sbin/sed_install.sh
```

5. When prompted, type:

```
continue.\
```

6. Enter the path to the SED PBA image file.
7. Enter the path to the SED PBA Image hash file.
8. Accept the SED PBA version check.
9. Wait for the installation to complete.
10. Once complete, power cycle the device for changes to take effect.

RFID Tag tab



This tab lists authorized RFID Keys. Currently, these keys are linked to the RFID Door Lock. When a RFID 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.

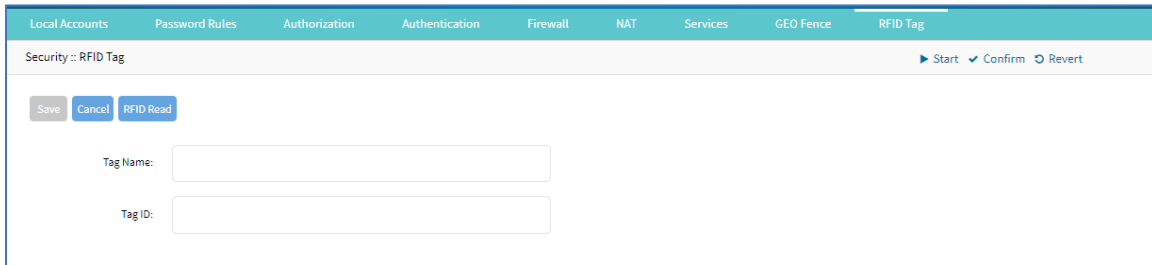
NOTE: When the RFID Reader door lock is connected to the Nodegrid device, it is automatically recognized.

Manage RFID Tag

Add RFID Tag

WebUI Procedure

1. Go to *Security :: RFID Tag*.
2. Click **Add** (displays dialog).



3. Enter **Tag Name**.
4. Enter **Tag ID**.
5. Click **Save**.

Read RFID Tag from Card

WebUI Procedure

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

WebUI Procedure

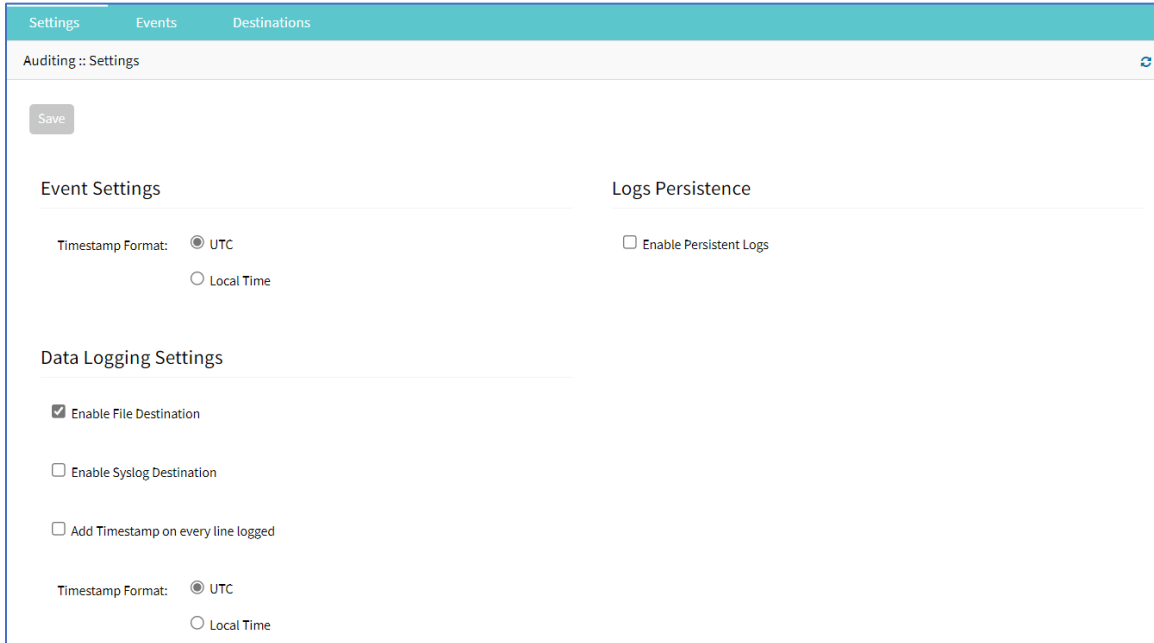
1. Go to *Security :: RFID Tag*.
2. Select checkbox.
3. Click **Delete**.

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.



Data Logging Settings

Update Logging Settings

WebUI Procedure

1. Go to *Auditing :: Settings*.
2. In *Event Setting* menu

In **Timestamp Format**, select one:

UTC radio button (default).

Local Time radio button.

3. In *Data Logging Settings* menu:

Select **Enable File Destination** checkbox (if enabled, data logs stored at location defined in *Auditing :: Destination* - default: enabled).

Select **Enable Syslog Destination** checkbox (if enabled, data logs stored at location defined in *Auditing :: Destination* - default: disabled).

Select **Add Timestamp on every line logged** checkbox.

In **Timestamp Format**, select one:

UTC radio button (default).

Local Time radio button.

4. In *Logs Persistence* menu:
Select **Enable Persistent Logs** checkbox.
5. Click **Save**.

Events tab

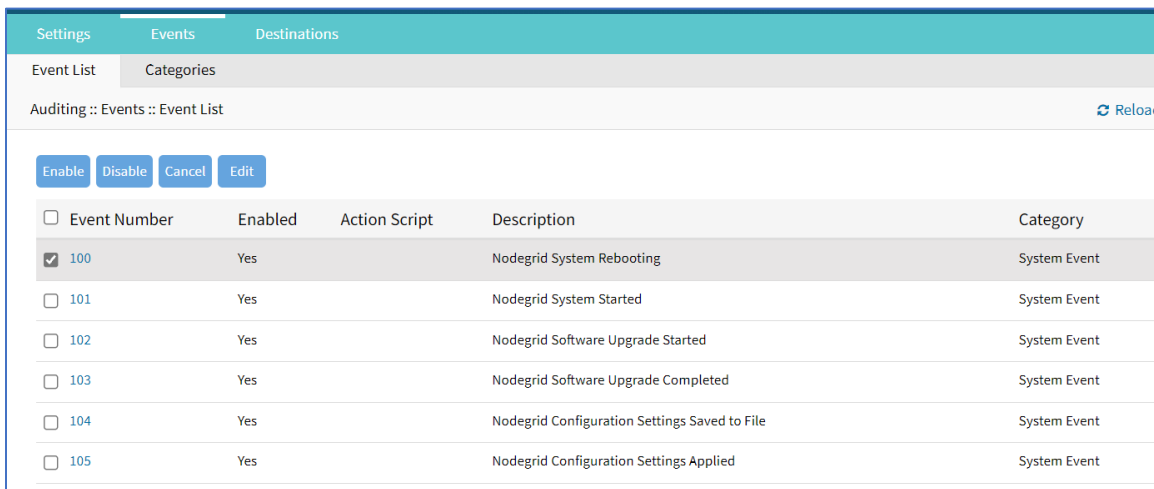
Events are automatically logged based on event and device settings. By default, all events are stored to the local file system. This behavior is adjusted under *Auditing :: Events*. The administrator can configure to which destination events and which event categories are logged.

There are four event categories:

- Systems Events
- AAA Events
- Device Events
- Logging Events

Event List sub-tab

This is a list of events. The table lists all current event types: 100 – 527 (list can be variable).



Event Number	Enabled	Action Script	Description	Category
<input checked="" type="checkbox"/> 100	Yes		Nodegrid System Rebooting	System Event
<input type="checkbox"/> 101	Yes		Nodegrid System Started	System Event
<input type="checkbox"/> 102	Yes		Nodegrid Software Upgrade Started	System Event
<input type="checkbox"/> 103	Yes		Nodegrid Software Upgrade Completed	System Event
<input type="checkbox"/> 104	Yes		Nodegrid Configuration Settings Saved to File	System Event
<input type="checkbox"/> 105	Yes		Nodegrid Configuration Settings Applied	System Event

Enable/Disable Event

WebUI Procedure

1. Go to *Auditing :: Events :: Event List*.
2. Locate and select checkbox(es).
3. Click **Enable** to enable reporting of that event type.

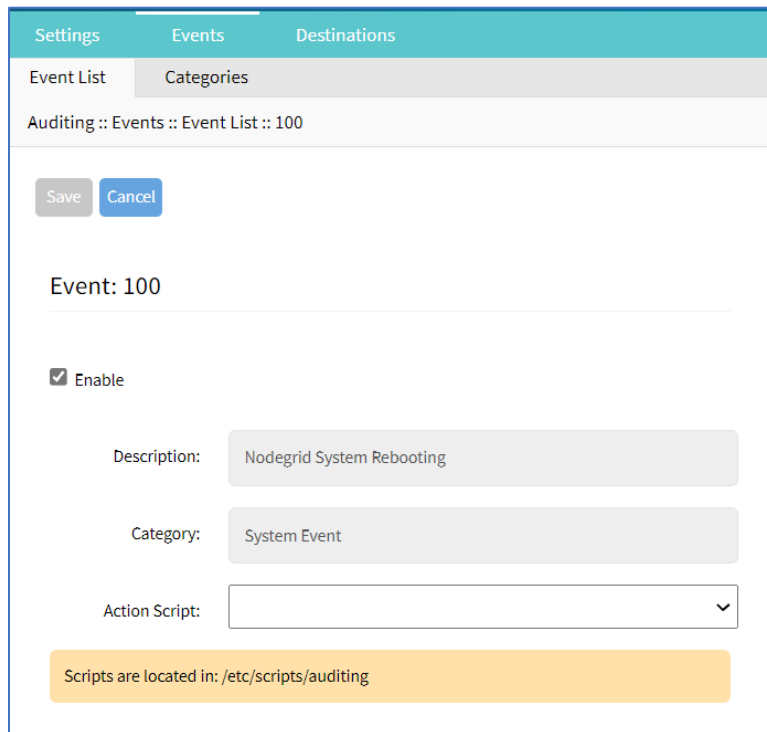
<input type="checkbox"/> Event Number	Enabled	Action Script	Description	Category
<input type="checkbox"/> 100	No		Nodegrid System Rebooting	System Event
<input type="checkbox"/> 101	Yes		Nodegrid System Started	System Event

4. Click **Disable** to disable reporting of that event type.

Edit Event

WebUI Procedure

1. Go to *Auditing :: Events :: Event List*.
2. Locate and select checkbox.
3. Click **Edit** (displays dialog).



The screenshot shows the 'Edit Event' dialog box. At the top, there are tabs for 'Settings', 'Events', and 'Destinations'. Under 'Events', there are sub-tabs for 'Event List' and 'Categories'. The current view is 'Event List' for 'Auditing :: Events :: Event List :: 100'. There are 'Save' and 'Cancel' buttons. The event is identified as 'Event: 100'. The 'Enable' checkbox is checked. The 'Description' field contains 'Nodegrid System Rebooting'. The 'Category' field contains 'System Event'. The 'Action Script' field is a dropdown menu. A yellow banner at the bottom indicates 'Scripts are located in: /etc/scripts/auditing'.

4. Select/unselect **Enable** checkbox (must be enabled to report occurrence).
5. On **Action Script** drop-down, select one (list is based on existing scripts).

NOTE: If event is enabled, and an action script assigned, the script runs when the event occurs.

6. Click **Save**.

Categories sub-tab

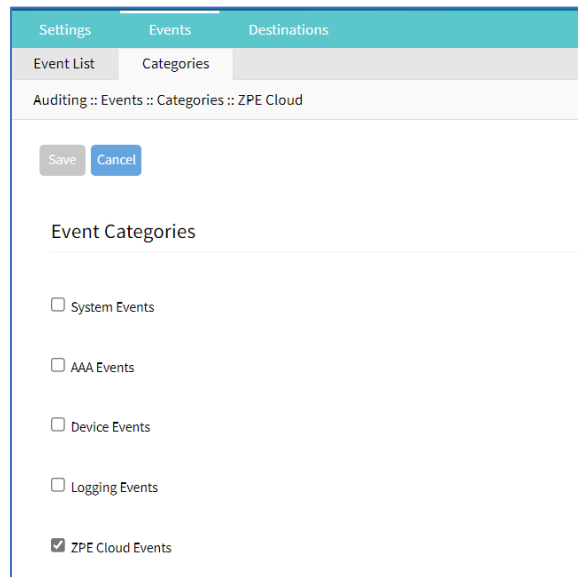
Category reporting is defined here. Table indicates current settings for reporting.

Settings						
Events						
Destinations						
Event List						
Categories						
Auditing :: Events :: Categories Rel						
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

WebUI Procedure

1. Go to *Auditing :: Events :: Categories*.
2. In *Events* column, click **ZPE Cloud** (displays dialog).



Settings Events Destinations

Event List Categories

Auditing :: Events :: Categories :: ZPE Cloud

Save Cancel

Event Categories

System Events

AAA Events

Device Events

Logging Events

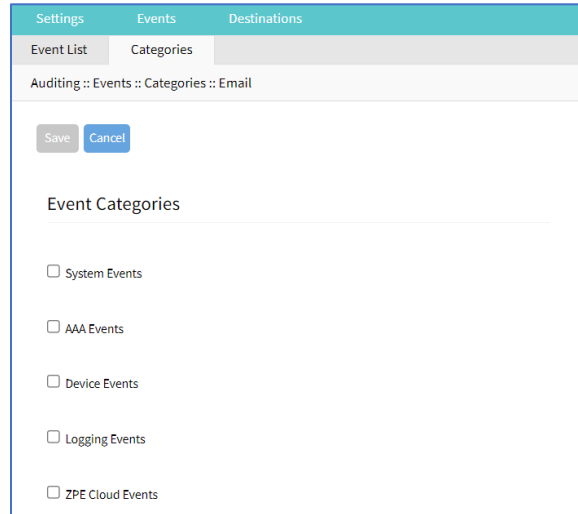
ZPE Cloud Events

3. Select **ZPE Cloud Events** checkbox (events that occur in ZPE Cloud are reported).
4. Click **Save**.

Set Categories for Email

WebUI Procedure

1. Go to *Auditing :: Events :: Categories*.
2. In *Events* column, click **Email** (displays dialog).

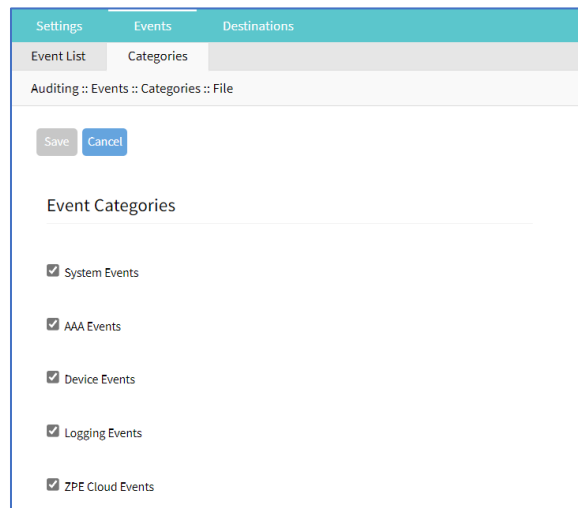


3. Select checkbox(es) that, when event occurs, email is sent (configured in *Auditing :: Destinations :: Email*).
4. Click **Save**.

Set Categories for File

WebUI Procedure

1. Go to *Auditing :: Events :: Categories*.
2. In *Events* column, click **File** (displays dialog).



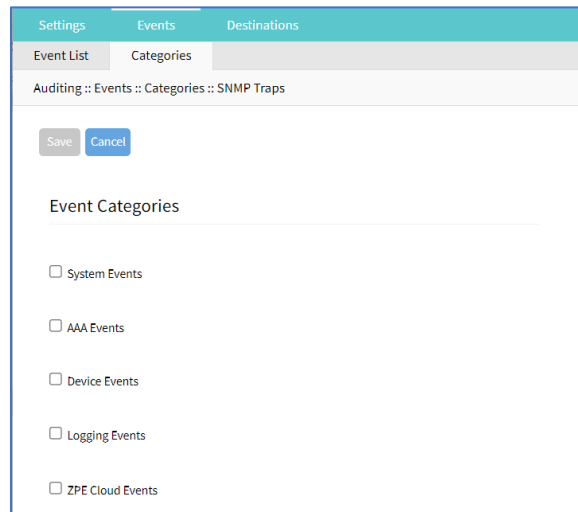
3. Select/unselect checkboxes, as needed.
4. Click **Save**.

Set Categories for SNMP Trap

WebUI Procedure

1. Go to *Auditing :: Events :: Categories*.

- In *Events* column, click **SNMP Trap** (displays dialog).

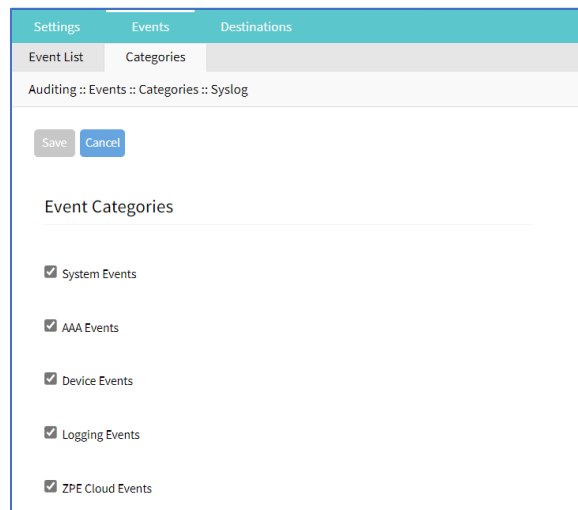


- Select/unselect checkboxes, as needed.
- Click **Save**.

Set Categories for Syslog

WebUI Procedure

- Go to *Auditing :: Events :: Categories*.
- In *Events* column, click **Syslog** (displays dialog).



- Select/unselect checkboxes, as needed.
- Click **Save**.

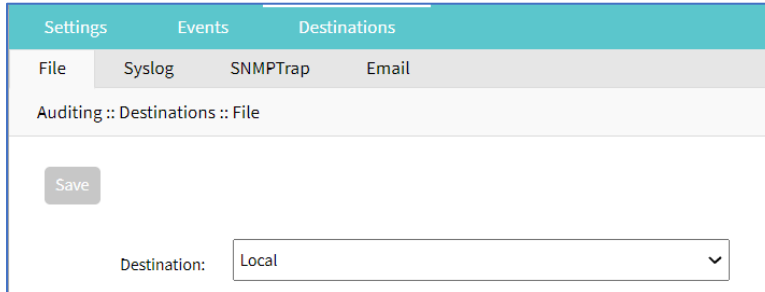
Destinations tab

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.

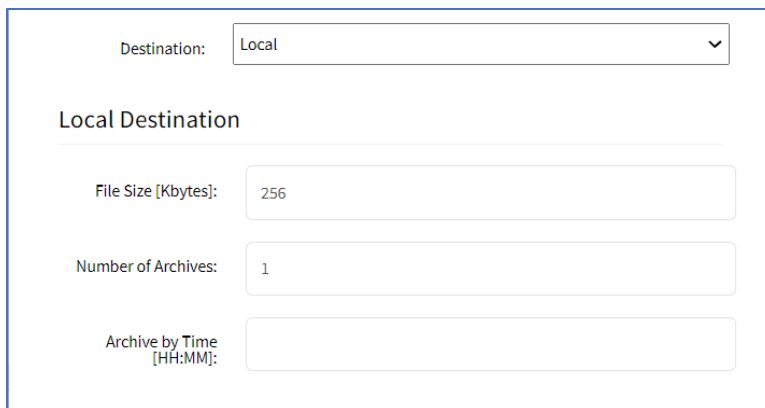
NOTE: NFS requires RPC service to be enabled (*Security :: Services*).



Configure File Settings

WebUI Procedure – Local Destination

1. Go to *Auditing :: Destinations :: File*.
2. On **Destination** drop-down, select **Local** (displays dialog):



3. In *Local Destination* menu:
 - Enter **File Size [Kbytes]** (0=disabled, up to 2048 KB - default: 1024).
 - Enter **Number of Archives** (number of archive files before discard - default: 0, max: 99).
 - Enter **Archive by Time [HH:MM]** (when file archive is rotated - default: blank).
4. Click **Save**.

WebUI Procedure – NFS Destination

1. Go to *Auditing :: Destinations :: File*.
2. On **Destination** drop-down, select **NFS** (displays dialog):

Destination:

NFS Destination

NFS Server:

NFS Path:

File Size [Kbytes]:

Number of Archives:

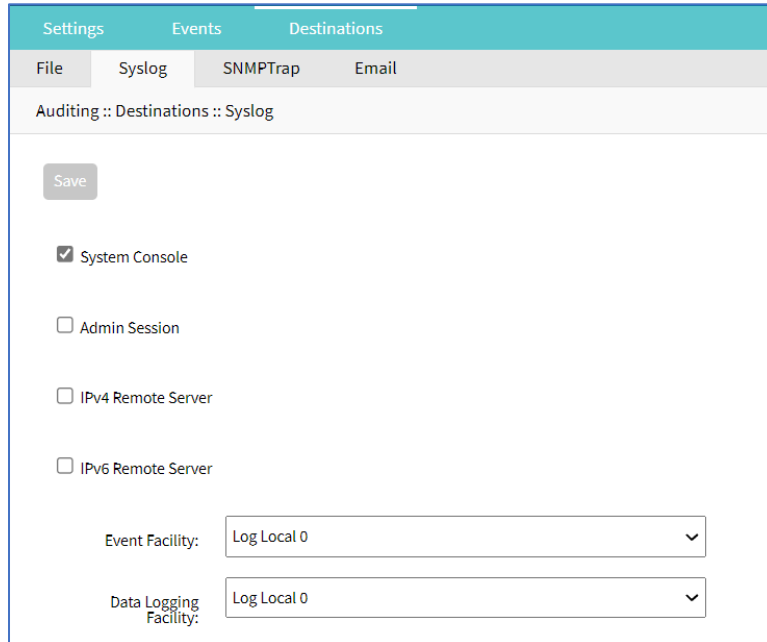
NFS Archive by Time [HH:MM]:

NFS requires RPC service to be enabled in Security :: Services.

3. In *NFS Destination* menu:
 - Enter **NFS Server** (IP address of NFS server).
 - Enter **NFS Path** (path to NFS root directory).
 - Enter **File Size [Kbytes]** (0=disabled, up to 2048 KB - default: 1024).
 - Enter **Number of Archives** (number of archive files before discard - default: 0, max: 99).
 - Enter **NFS Archive by Time [HH:MM]** (when file archive is rotated - default: blank).
4. Click **Save**.

Syslog sub-tab

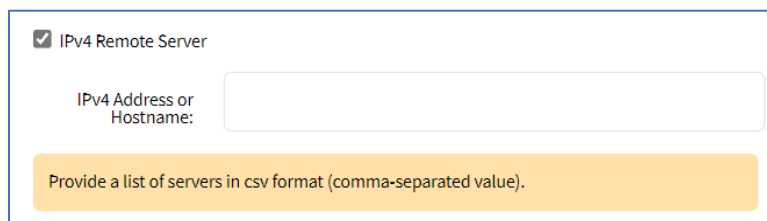
Support destinations are: local Syslog destination or remote IPv4 and IPv6 destination.



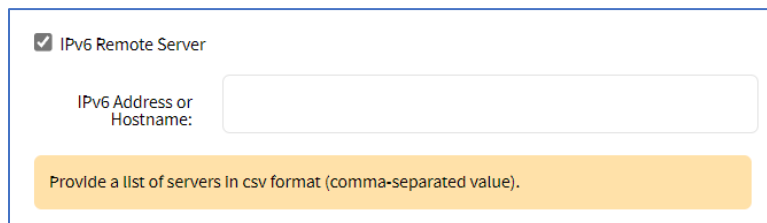
Configure Syslog Settings

WebUI Procedure

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**.



5. Select **IPv6 Remote Server** checkbox. Enter **IPv6 Address or Hostname**.



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**.

SNMP Trap 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.

Configure SNMP Trap Settings

WebUI Procedure

1. Go to *Auditing :: Destinations :: SNMP Trap*.
2. Enter **Server**.
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: 161).
5. Enter **Client Address**.
6. In *Trap Version* menu, select one:

NOTE: SNMP3 INFORM messages are currently not supported.

Version 2c radio button.

Enter **Community**.

Version 3 radio button.

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

CLI Procedure

The MIB files are located as follows:

```
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.

Settings	Events	Destinations	
File	Syslog	SNMPTrap	Email
Auditing :: Destinations :: Email			
<input type="button" value="Save"/> <input type="button" value="Test Email"/>			
Server:	<input type="text"/>		
Port:	<input type="text" value="25"/>		
Username:	<input type="text"/>		
Password:	<input type="password" value="*****"/>		
Confirm Password:	<input type="password" value="*****"/>		
Destination Email:	<input type="text"/>		
Sender:	<input type="text"/>		
<input checked="" type="checkbox"/> Start TLS			

Configure Email Settings

WebUI Procedure

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**.

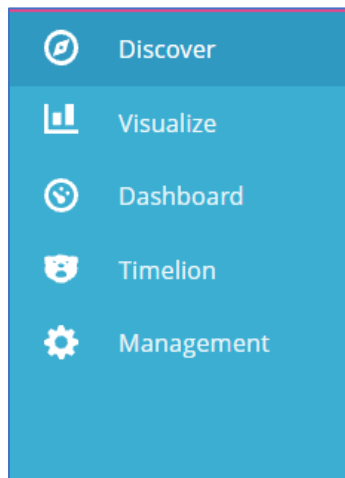
Dashboard Section

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

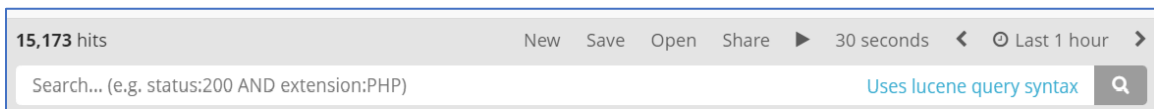
Navigation Tabs

Navigation tabs are located on the left panel.



Toolbar Description

The Toolbar is show across top of the panel.



New

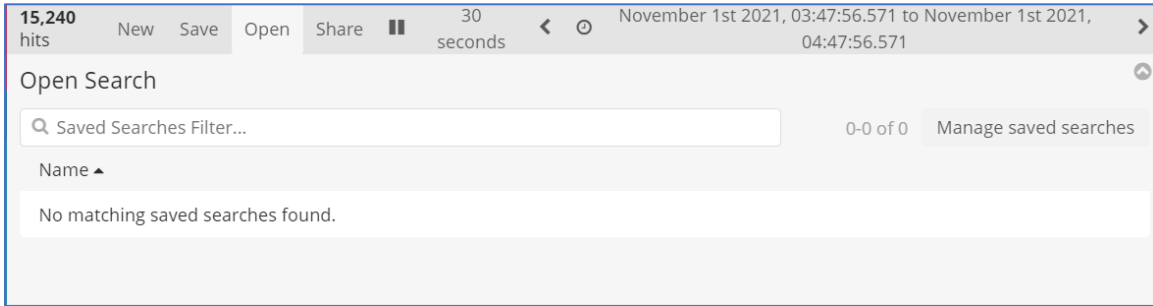
Initiates an option to create a new option – visualization, panel, etc.

Save

Saves the settings of the current configuration with any modifications.

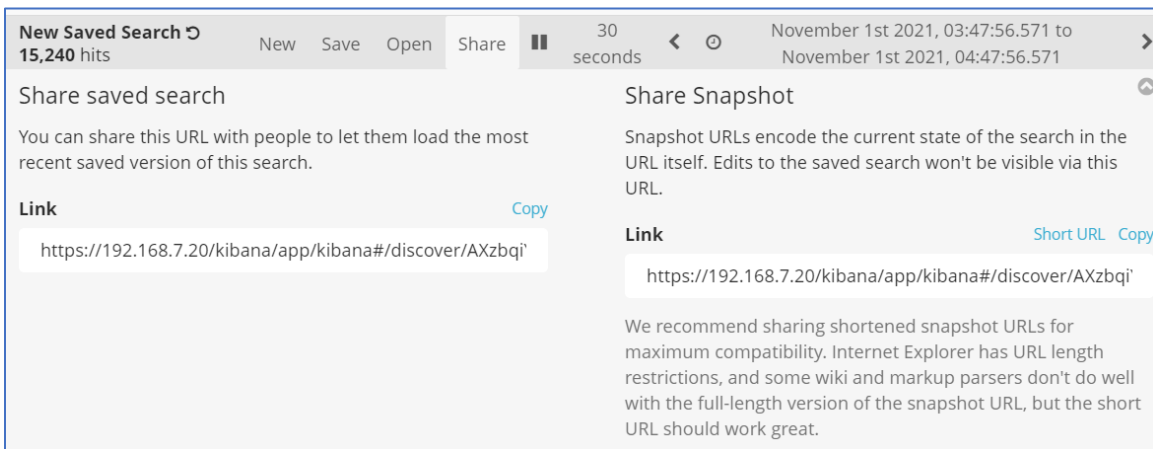
Open

Displays Open Search dialog.



Share

Opens *Share* dialog options of the current saved search.



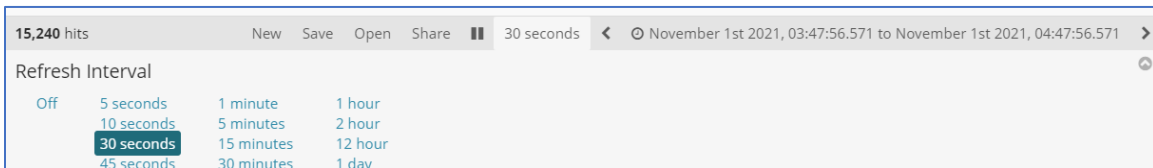
Click to play discovery to include modifications. Useful for testing parameter changes before saving.



Click to move the display back in time.

Refresh interval

How often the results are checked and shown in the display.



Quick sub-tab

Quick options to select a relative time frame to current time.

15,240 hits New Save Open Share 30 seconds ◀ November 1st 2021, 03:47:56.571 to November 1st 2021, 04:47:56.571 ▶

Time Range

- Quick**
 - Today
 - This week
 - This month
- Relative
 - This year
 - The day so far
 - Week to date
 - Month to date
 - Year to date
- Absolute
 - Yesterday
 - Day before yesterday
 - This day last week
 - Previous week
 - Previous month
 - Previous year
 - Last 15 minutes
 - Last 30 minutes
 - Last 1 hour
 - Last 4 hours
 - Last 12 hours
 - Last 24 hours
 - Last 7 days
 - Last 30 days
 - Last 60 days
 - Last 90 days
 - Last 6 months
 - Last 1 year
 - Last 2 years
 - Last 5 years

Relative sub-tab

Select custom time frames in relation to current time.

15,240 hits New Save Open Share 30 seconds ◀ November 1st 2021, 03:47:56.571 to November 1st 2021, 04:47:56.571 ▶

Time Range

- Quick
- Relative**
- Absolute

From: November 1st 2021, 04:11:02.875 Set To Now

To: November 1st 2021, 05:11:02.875 Set To Now

2 Hours ago 1 Hours ago

round to the hour round to the hour

Go

Absolute sub-tab

Select fixed dates/times.

15,240 hits New Save Open Share 30 seconds ◀ November 1st 2021, 03:47:56.571 to November 1st 2021, 04:47:56.571 ▶

Time Range

- Quick
- Relative
- Absolute**

From: Set To Now To: Set To Now

2021-11-01 03:47:56.571 2021-11-01 04:47:56.571 Go

YYYY-MM-DD HH:mm:ss.SSS YYYY-MM-DD HH:mm:ss.SSS

< November 2021 > < November 2021 >

Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat
	01	02	03	04	05	06	01	02	03	04	05	06	
07	08	09	10	11	12	13	07	08	09	10	11	12	13
14	15	16	17	18	19	20	14	15	16	17	18	19	20
21	22	23	24	25	26	27	21	22	23	24	25	26	27
28	29	30					28	29	30				

> (forward)

Click to moves the display forward in time.

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.

Field	Values	Description
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.

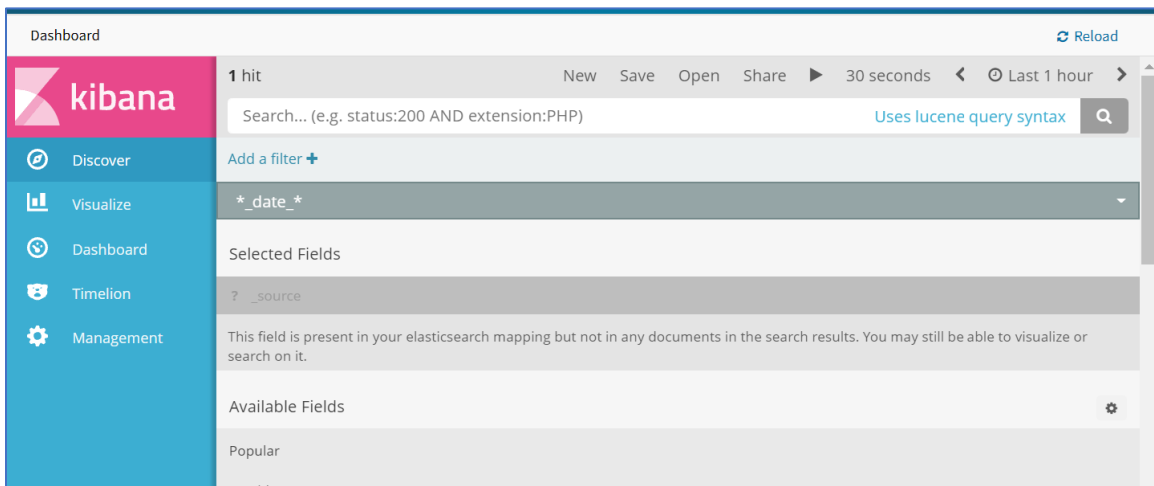
Discover tab

Data Point Exploration

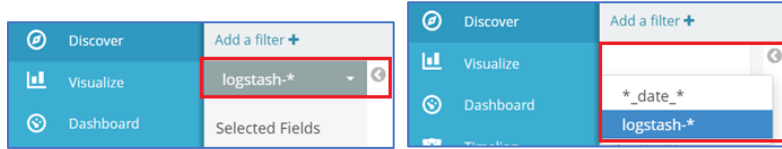
This allows an inspection of the entire json document that was indexed

Collect Raw Data Points

1. Go to *Dashboard :: Discover*.



2. Click in the dark bar. 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.

Line Charts

Line Charts allow the visualization of data points along the line graph.

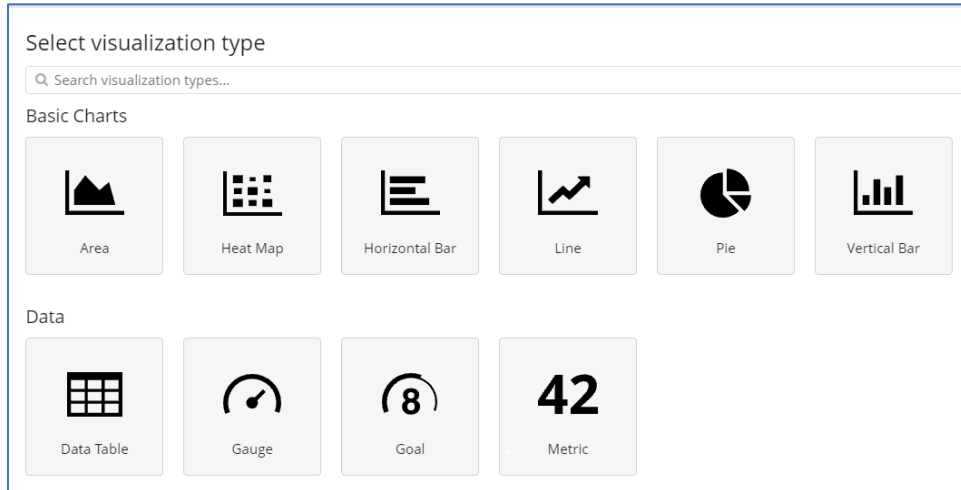
Create a Single or Multi-Line Chart (Configuration Example)

WebUI Procedure

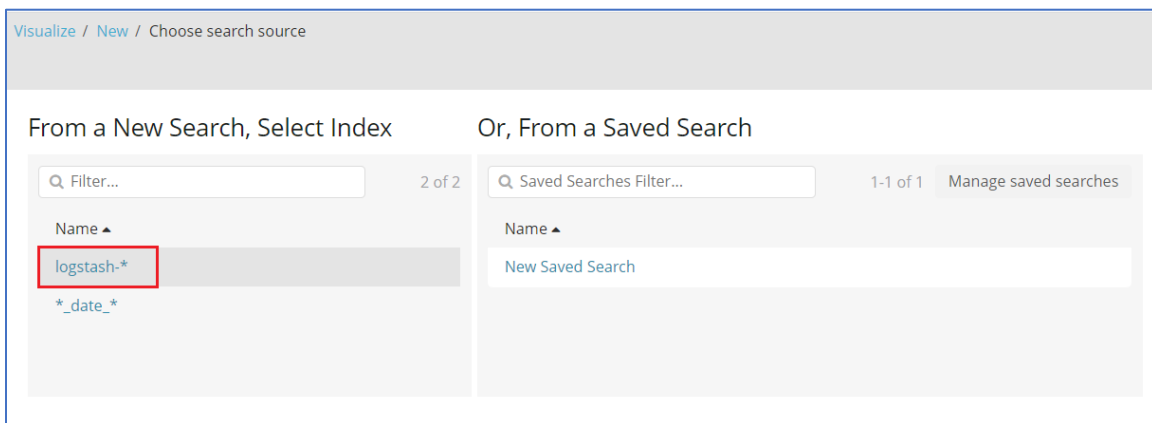
1. Go to *Dashboard :: Visualize*.
2. Click the + icon.



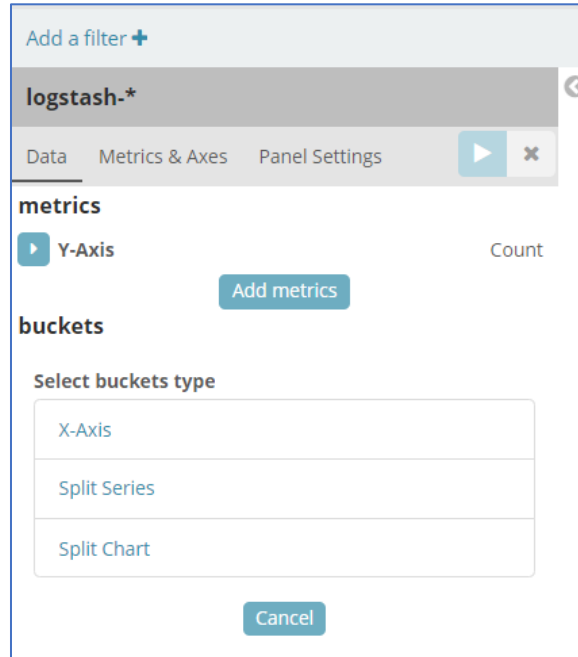
3. This displays the *Select visualization type* dialog.



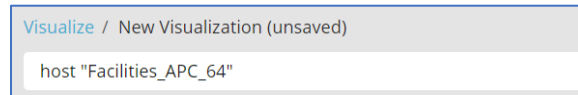
4. Click the **Line** icon. On the dialog, click **logstash-***.



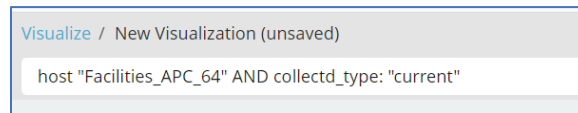
5. In the *From a New Search, Select Index* menu, click **logstash-*** (displays editor dialog).



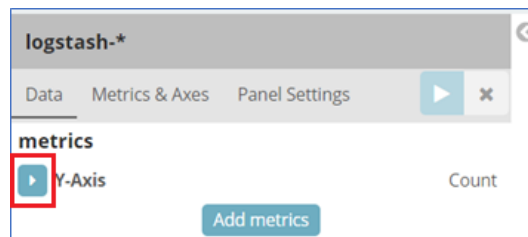
- To select the data points to visualize, enter a search expression.



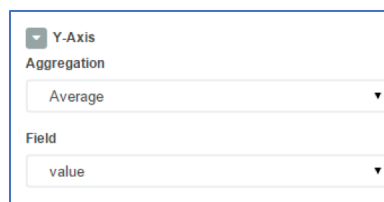
The search expression can be extended.



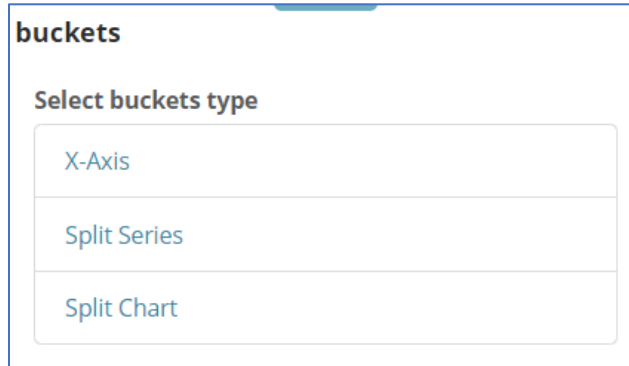
- In the *Metrics* section, click **Y-Axis** arrow.



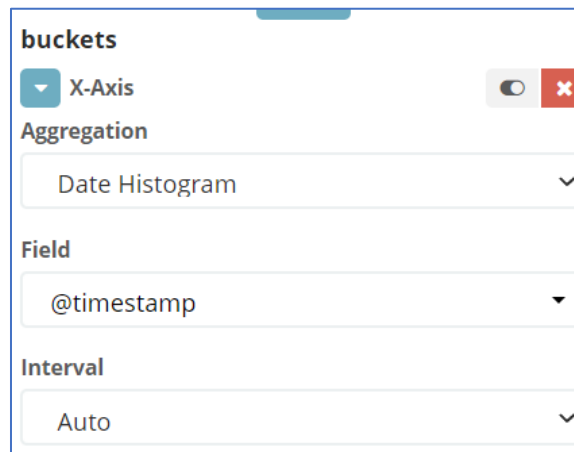
- On the **Aggregation** drop-down, under *Metric Aggregations* section, select **Average** . In **Field** drop-down, select **value**.



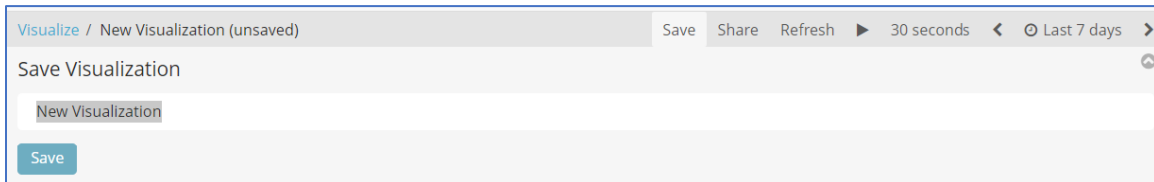
- In *buckets* section, in *Select buckets type* menu, click **X-Axis**.



10. On **Aggregation** drop-down, select **Date Histogram**. Accept **Field** and **Interval** defaults.



11. On the Toolbar, click **Save** (displays dialog).



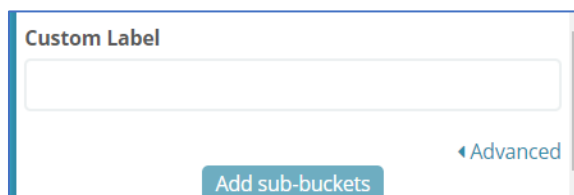
12. Enter a name for the visualization and click **Save**.

Create a Multi-Line Chart (Configuration Example)

Follow the Single-Line Chart example and continue these steps.

WebUI Procedure

1. Below **Custom Label** field, click **Add sub-buckets**.



2. On the *Select buckets type* menu, click **Split Series**.

Select buckets type

Split Series

Split Chart

- On **Sub Aggregation** drop-down, select **Filters**.

▼ Split Series
☐ ↑ ×

Sub Aggregation

Filters

Filter 1 🔍 ×

Add Filter

- In **Filter 1**, enter a search expression for the elements to visualize.

▼ Split Series
☐ ↑ ×

Sub Aggregation

Filters

Filter 1 🔍 ×

type_instance: "bank_0"

Filter 1 label

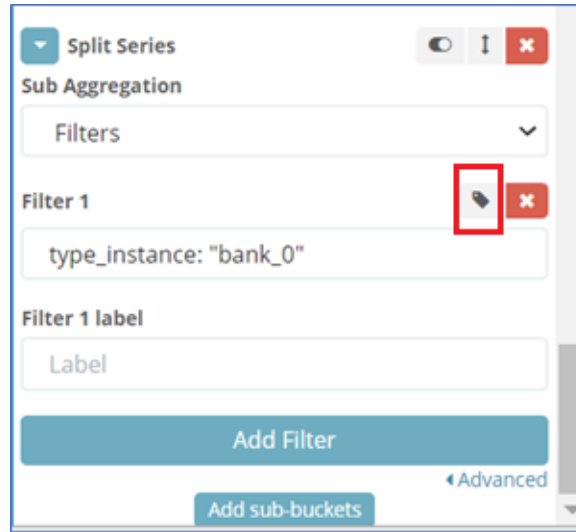
Label

Add Filter

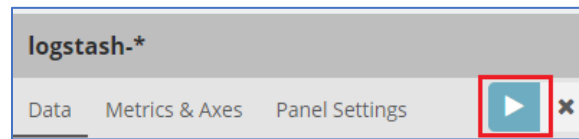
⏪ Advanced

Add sub-buckets

- (optional) To associate a label, click the **Settings** icon and enter **Filter 1 label**.



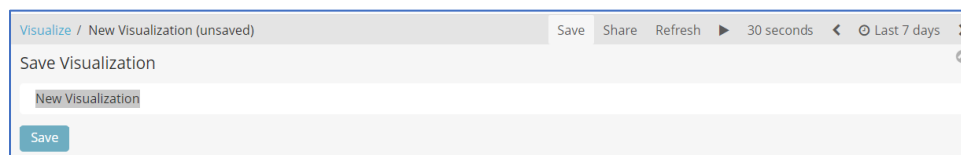
6. (as needed) Click **Add Filter** and repeat.
7. (as needed) Click **Add sub-buckets** and repeat.
8. To refresh the graph based on the configuration, click on the Play icon.



The graph example includes several sub-buckets.



9. On the Toolbar, click **Save** (displays dialog).



10. 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.

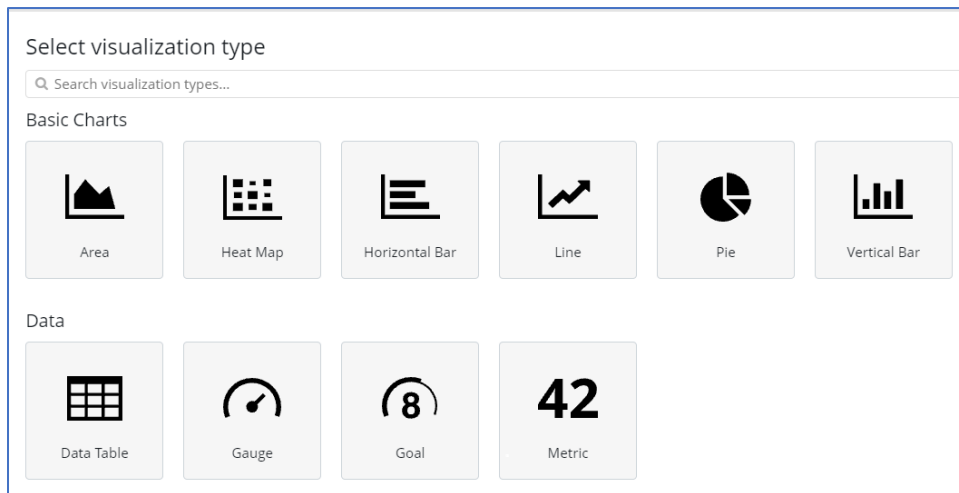
NOTE: Become familiar with the Line Chart procedure before creating an Area Chart,

WebUI Procedure

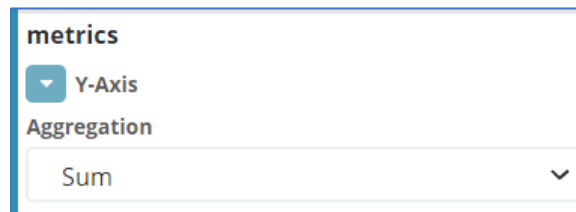
1. Go to *Dashboard :: Visualize*.
2. Click the + icon.



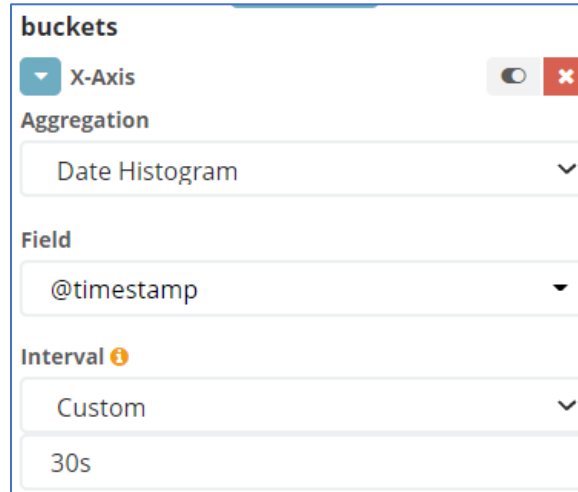
3. This displays the *Select visualization type* dialog.



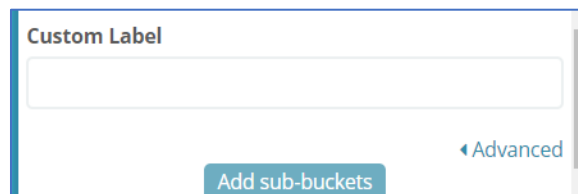
4. Click the **Area** icon. On the dialog, click **logstash-***.
5. In *metrics* section, click on **Y-Axis** icon. In **Aggregation** drop-down, select **Sum**.



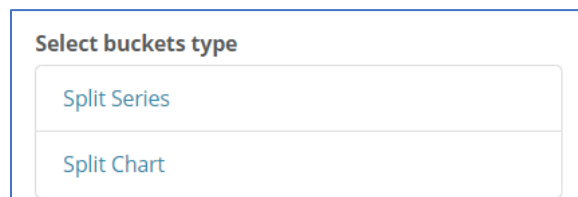
6. On *Buckets* menu, X-Axis, on **Aggregation** drop-down, select **Data Histogram**. In **Interval** drop-down, select **Custom** then enter value (i.e., 30s).



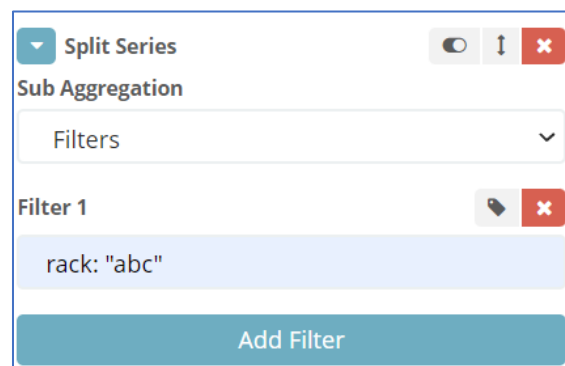
7. Below **Custom Label** field, click **Add sub-buckets**.



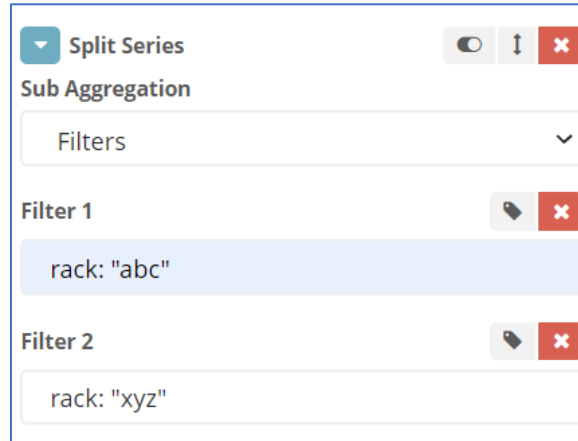
8. On the *Select buckets type* menu, click **Split Series**.



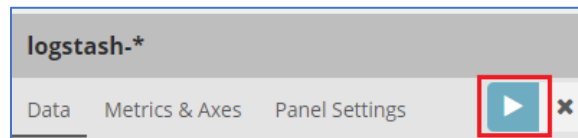
9. On **Sub Aggregation** drop-down, select **Filters**. In **Filter 1**, enter value. Click **Add Filter**.



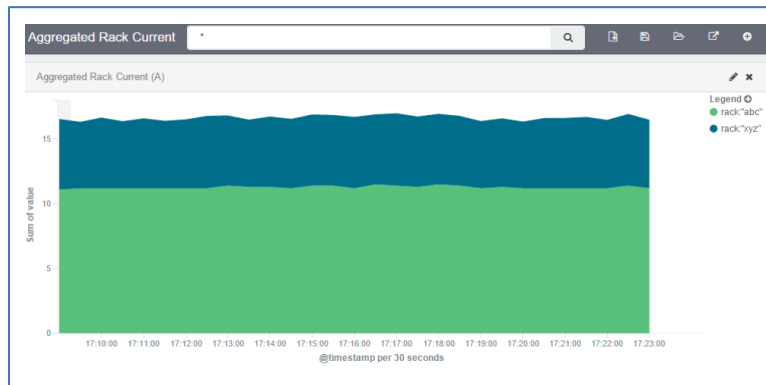
10. In **Filter 2**, enter a search expression for the elements to visualize.



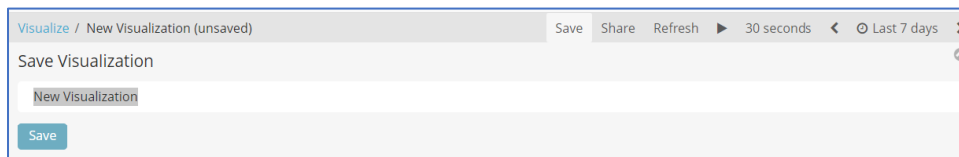
11. (as needed) Click **Add Filter** and repeat.
12. To refresh the graph based on the configuration, click on the Play icon.



The resulting visualization would look like this:



13. On the Toolbar, click **Save** (displays dialog).

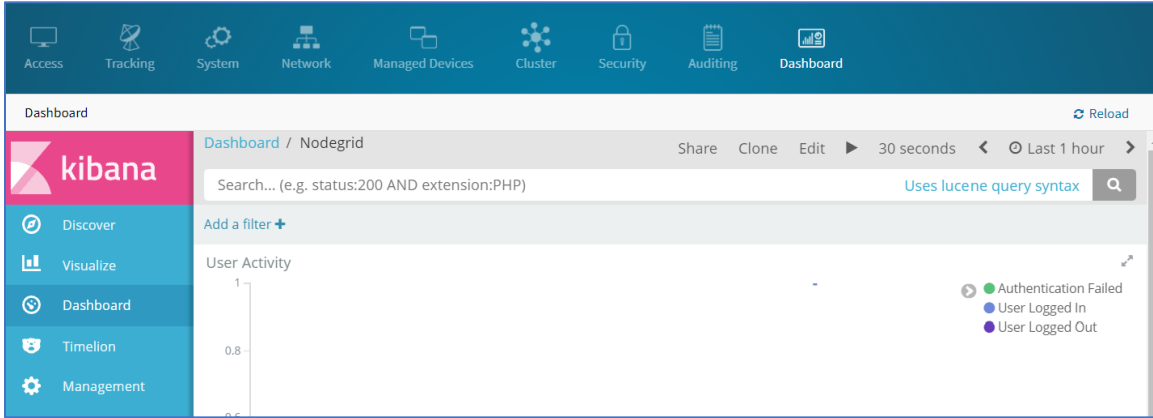


14. Enter a name for the visualization and click **Save**.

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.

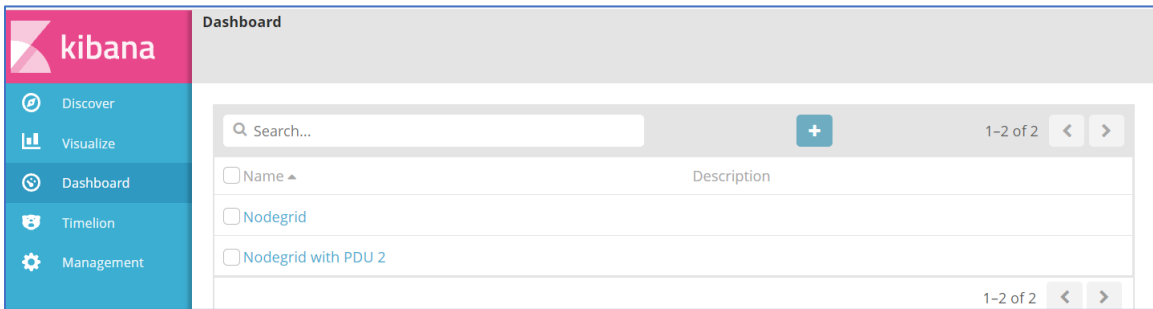


Manage Dashboards

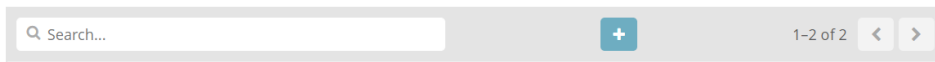
Description

WebUI Procedure

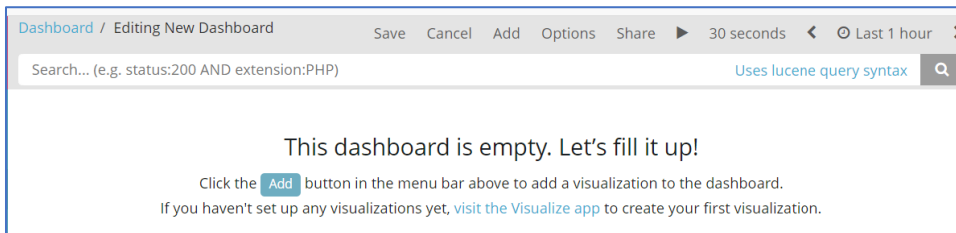
1. On the left side panel, click **Dashboard** tab (main panel lists saved visualizations).



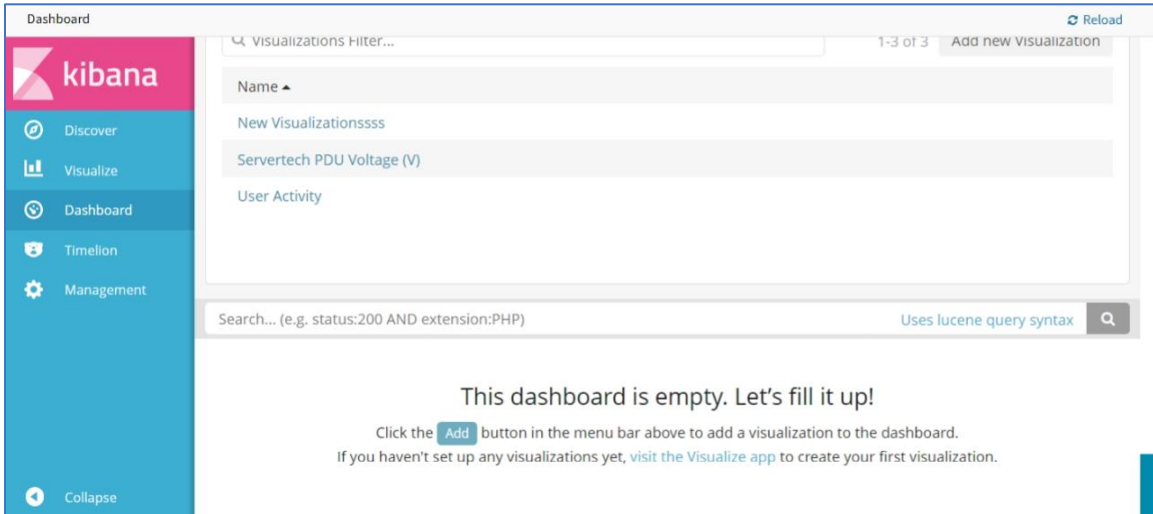
2. On the *Navigation* bar, click the **New Dashboard** icon



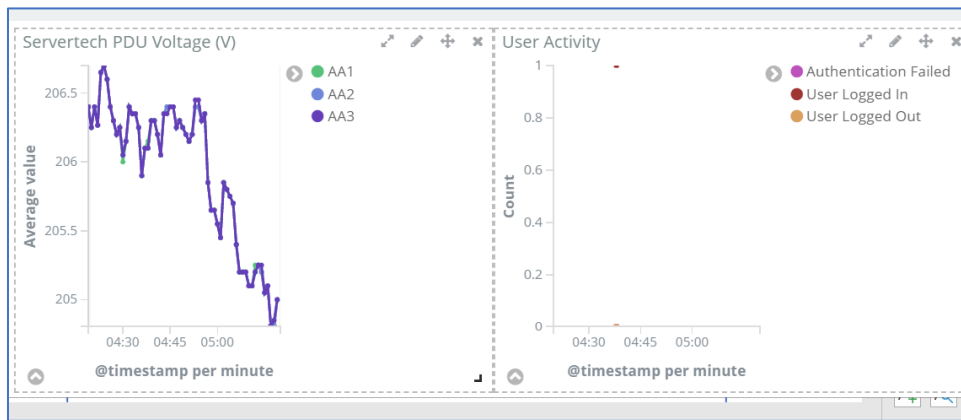
3. On the *Editing New Dashboard* panel, click **Add**.



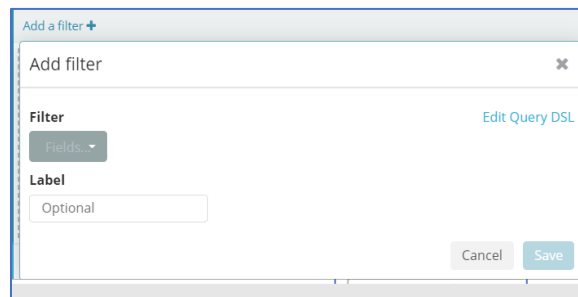
4. On the *Add Panels* dialog, top panel lists available visualizations. To the upper right is the option to create a new visualization. Below is the *dashboard* panel.



- 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.

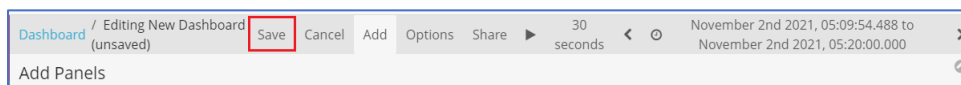


- Resize (lower right corner handle) and reposition (click, drag and drop) the graphs, as needed. .
- If needed, to include a filter, click **Add a filter** (displays *Add a Filter* dialog).

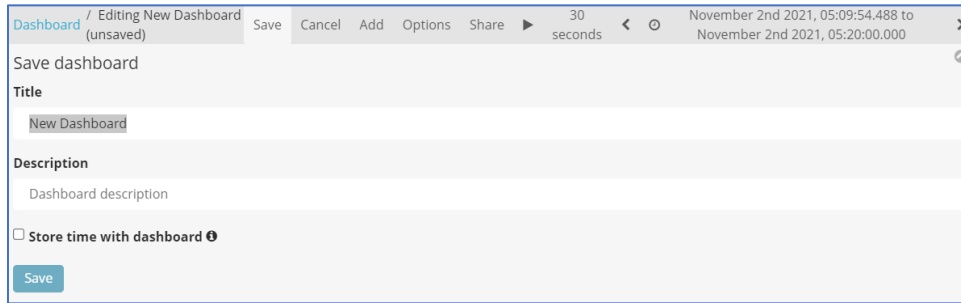


Select from **Filter** drop-down, Enter **Label**, then click **Save**.

- When the dashboard appearance and details are ready, click **Save** icon.



9. On the *Save dashboard* dialog:



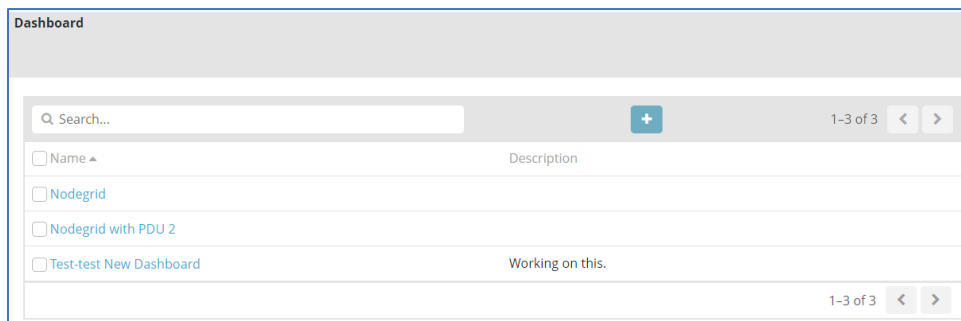
Enter **Title**.

Enter **Description**.

(optional) Select **Store time with dashboard** checkbox.

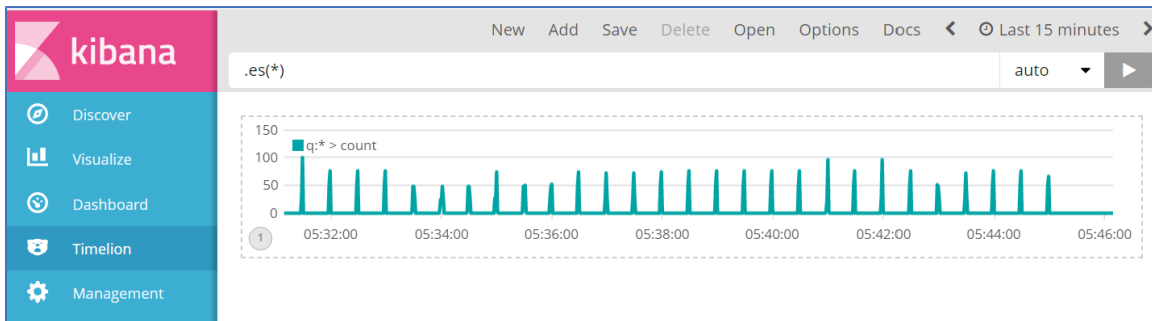
Click **Save**.

10. The new dashboard is added to the list.



Timelion tab

This is another visualization tool for time-based data analysis. For example, it can view specific data activity on a timeline basis. The chart results can be analyzed in various time segments (daily, weekly, etc.).

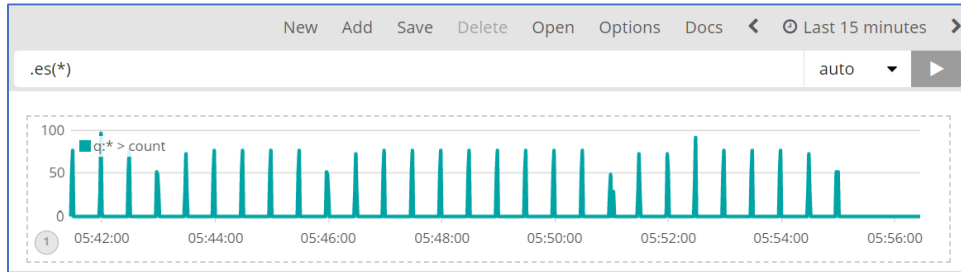


Toolbar tabs

On the Toolbar, these functions are available:

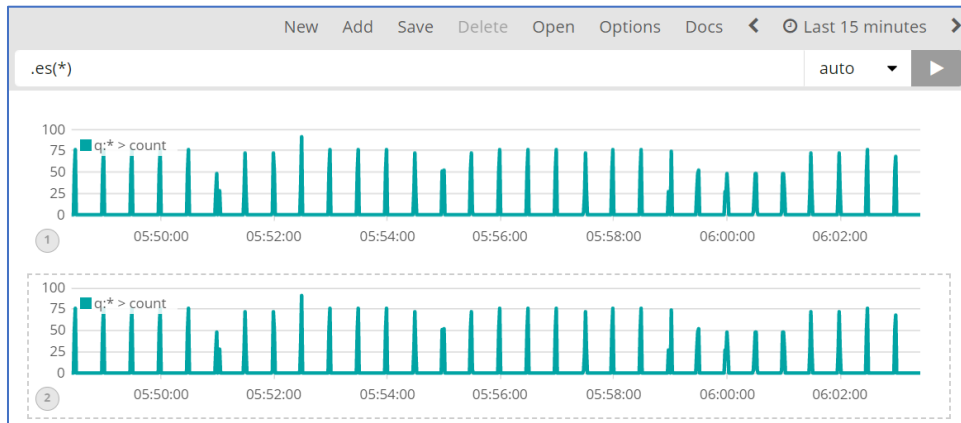
New sub-tab

Option to modify the display (change field, change time)



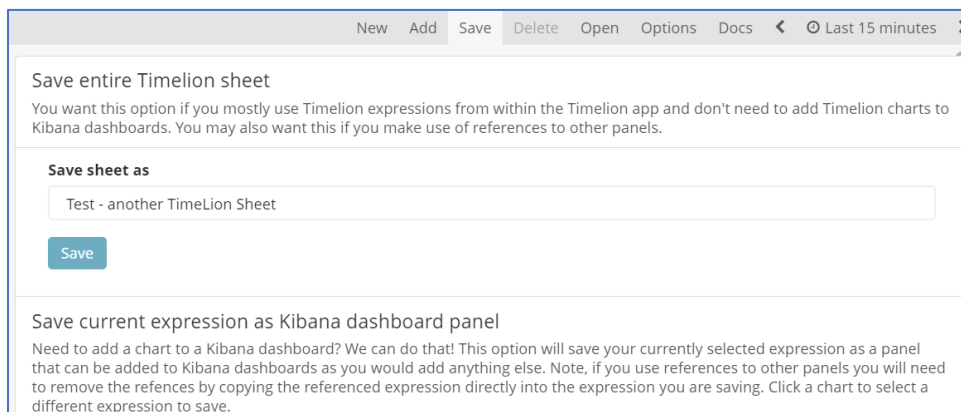
Add sub-tab

Adds another visualization chart.



Save sub-tab

Saves the current configuration. Click on one paragraph, as needed.

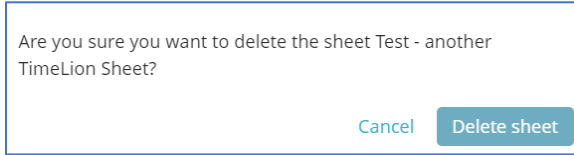


The screenshot shows a 'Save' dialog box with a menu at the top containing: New, Add, Save, Delete, Open, Options, Docs, and a refresh icon. The dialog has two sections:

- Save entire Timelion sheet**: A paragraph explaining that this option is for users who mostly use Timelion expressions from within the app and don't need to add charts to Kibana dashboards. It also notes that this option is useful if references to other panels are used.
- Save sheet as**: A text input field containing the text 'Test - another TimeLion Sheet' and a 'Save' button.
- Save current expression as Kibana dashboard panel**: A paragraph explaining that this option saves the current expression as a panel for a Kibana dashboard. It notes that if references to other panels are used, they must be removed by copying the referenced expression directly into the one being saved.

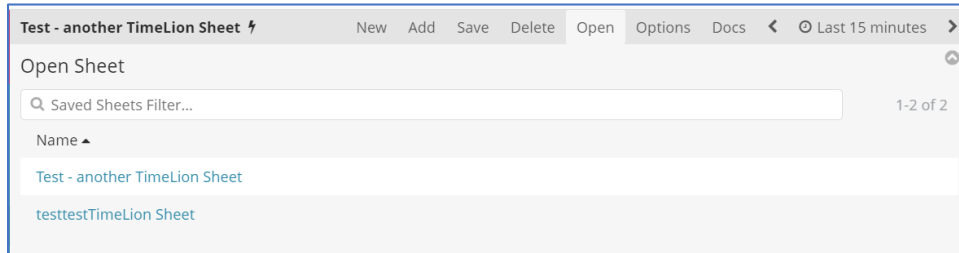
Delete sub-tab

Displays pop-up dialog to confirm deletion of the current displayed visualization.



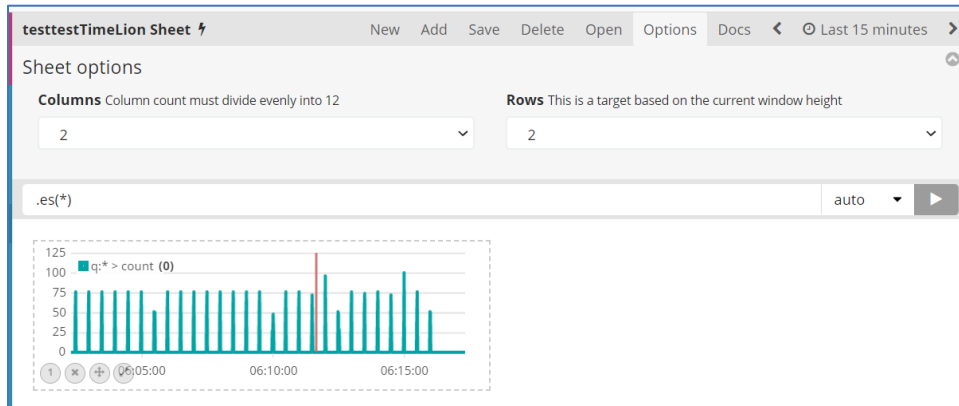
Open sub-tab

Displays *Open Sheet* dialog to select a visualization.



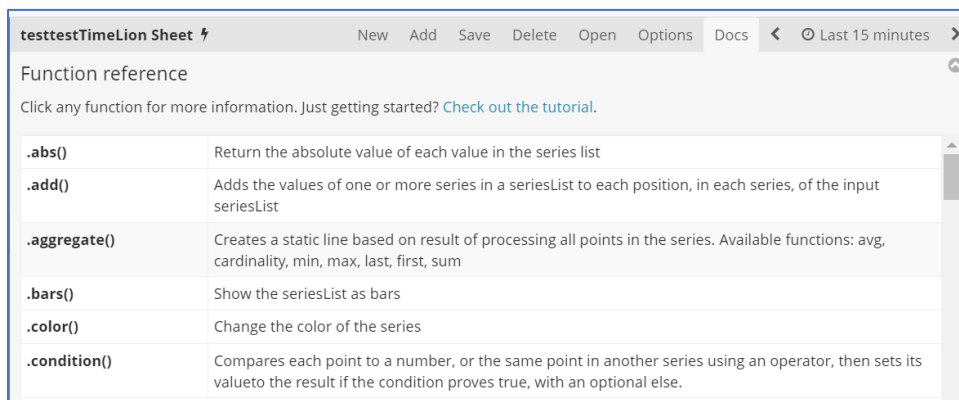
Options sub-tab

Displays options to modify display of the visualization (Columns, Rows, etc.)



Docs sub-tab

Displays the Function Reference details.

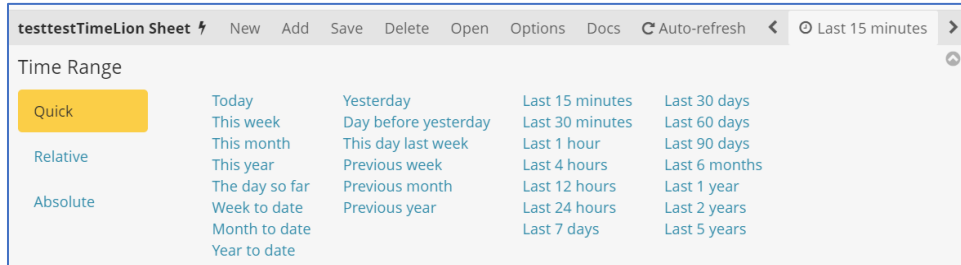


< (back)

Click to move the display back in time.

Time Range sub-tab

Option to modify the time range of the visualization.

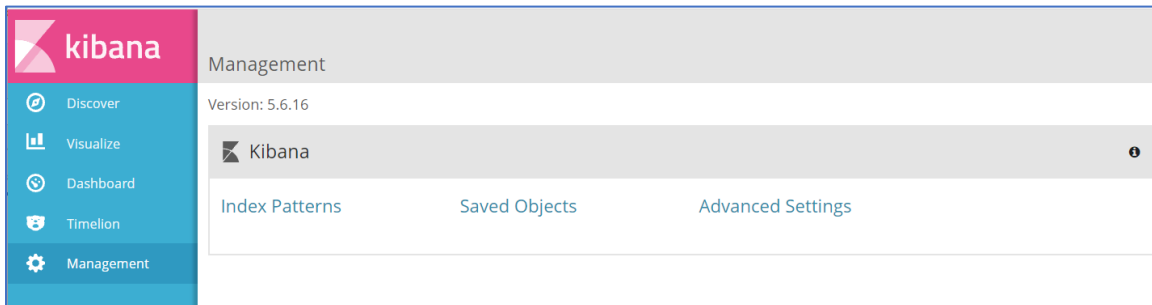


> (forward)

Click to moves the display forward in time.

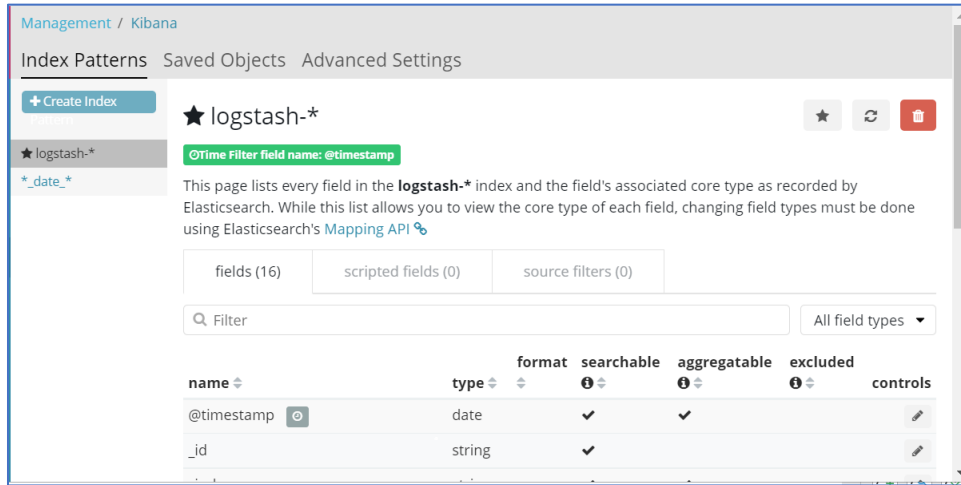
Management tab

This manage index patterns, saved objects. The advanced settings can tweak some points, especially visualizations.



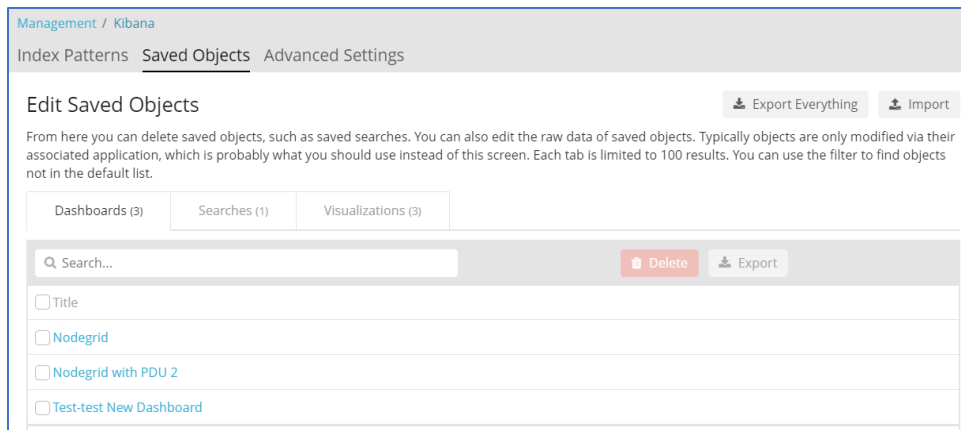
Index Patterns sub-tab

Displays details of selected index patterns (screenshot shows logstash-*).



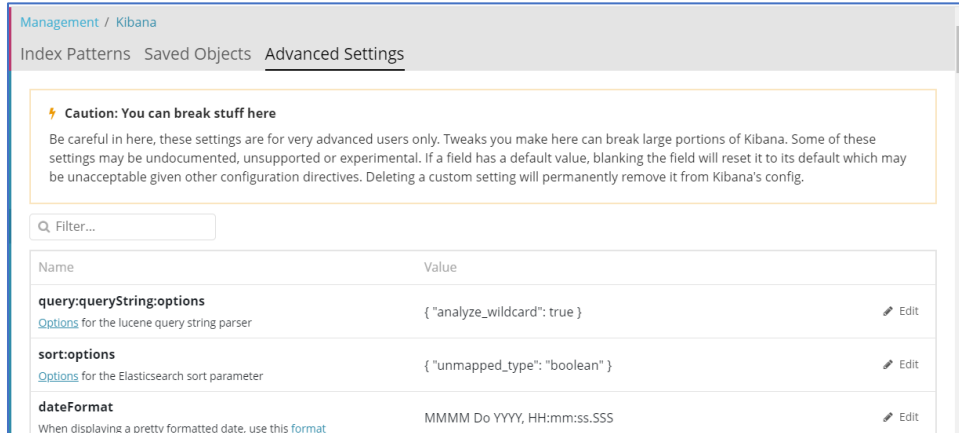
Saved Objects sub-tab

Displays Edit Saved Objects. To modify, click name on list.



Advanced Settings sub-tab

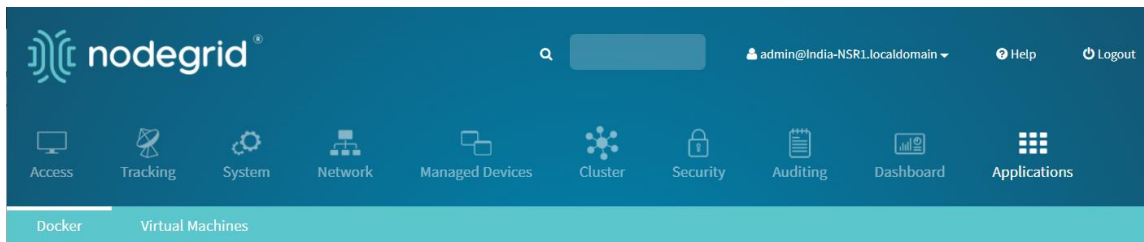
Settings can be directly edited here (admin privileges required). Carefully read the **Caution** statement, especially for the size of the history of saved search queries.



Applications Section

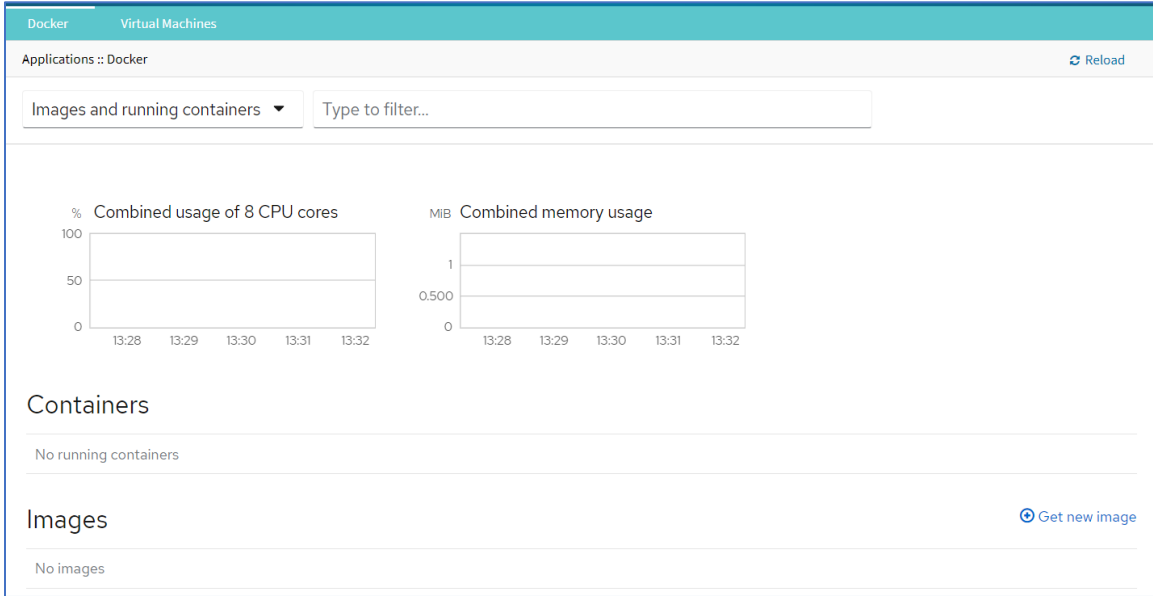
Nodegrid devices can run additional applications. These provide expanded software capabilities. The most used apps are in the areas of monitoring and SD-WAN. While all Nodegrid units support this feature, the Services Router Family is designed to run applications to enhance a wide variety of connectivity 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.

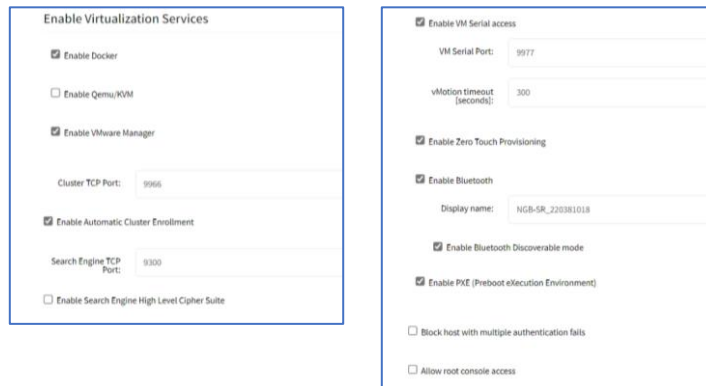
To start a container without Seccomp and Apparmor, the following shell command is required:

```
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.

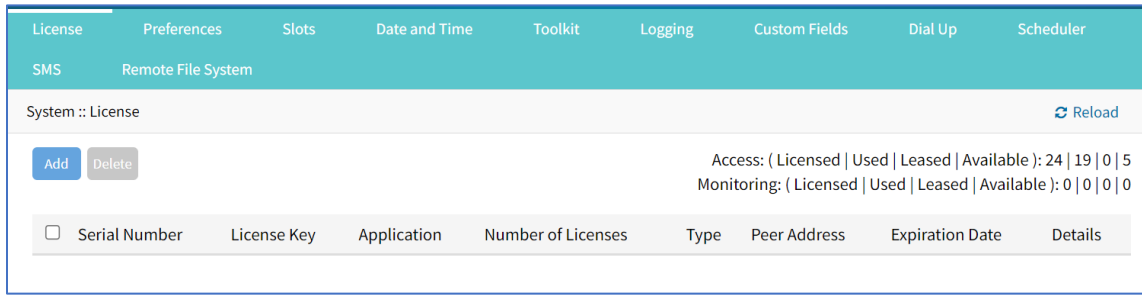
Activate Virtualization

1. Go to *Security :: Services*
2. In the *Enable Virtualization Services* menu:



3. Select **Enable Docker** checkbox.
4. Make other settings, as needed
5. Click **Save**.

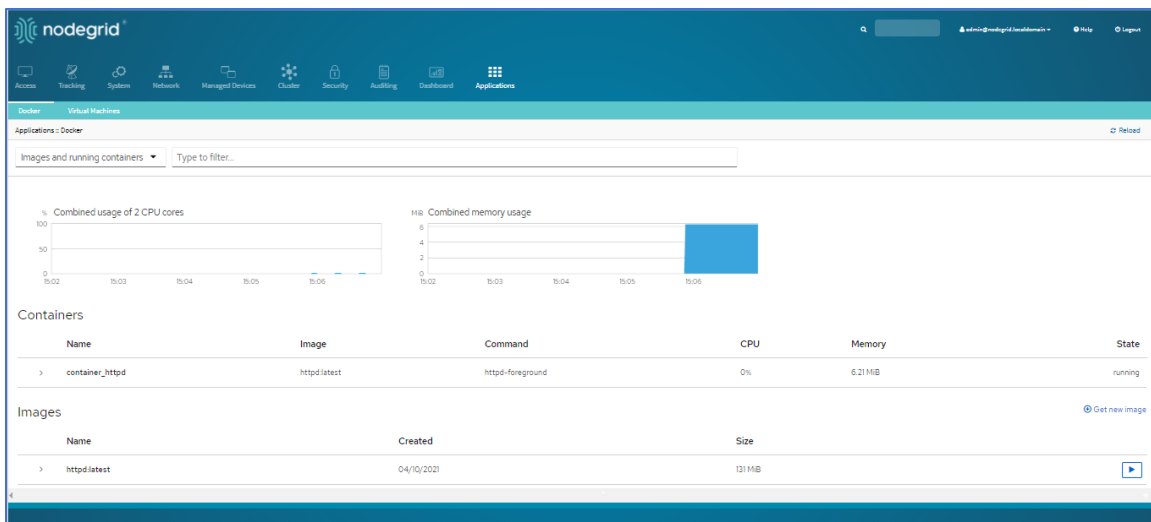
Licenses are required. To view licensed applications, go to *System :: Licenses*.



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.

WebUI Procedure

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**.

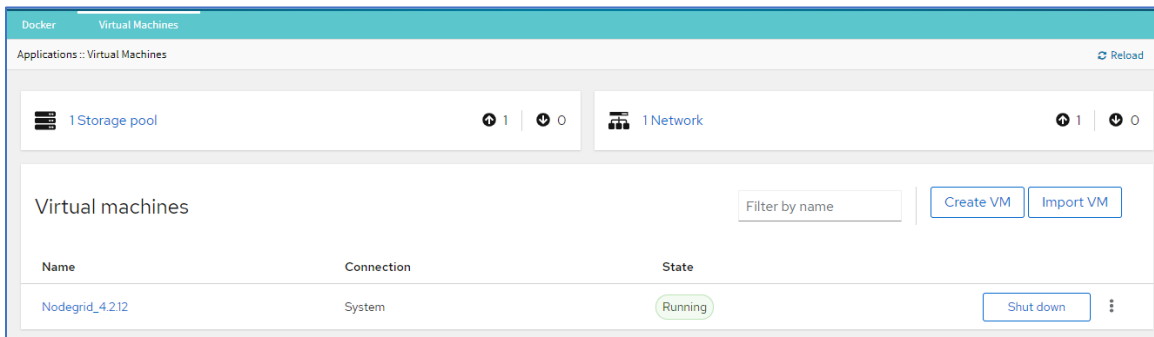
5. Type **httpd** and press enter
6. On the list, select the image and click **Download**.
7. On download, the image is listed in the *Images* table.

Add a New Docker Container

1. Select the image and click **Play**.
2. Adjust the configuration details.
3. Click **Run**.

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.



For additional details see the official [Docker create](#) documentation.

NOTE: After the container is created, it does not automatically start.

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).

Create new virtual machine ✕

Name

Connection System

Installation type

Installation source

Operating system

Storage

Size

Memory

Immediately start VM

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)**.
6. Enter **Installation Source** (options adjust based on **Installation Type** selection).
7. On **Operating System** drop-down, select one (if available).
8. On **Storage** drop-down, select one (**Create new volume**, **No storage**, **Storage pools**).
If **Create new volume** selected, enter **Size** and **Memory**.
9. Select **Immediately Start VM** checkbox.
10. Click **Create**.

Links tab

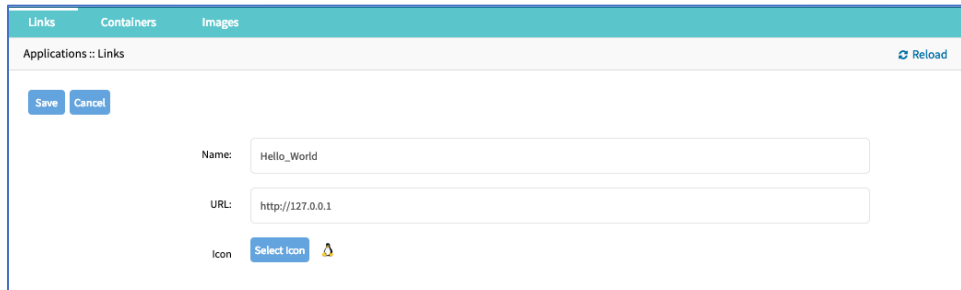
Administrators can create simple web links to run containers and other applications.

Manage Links

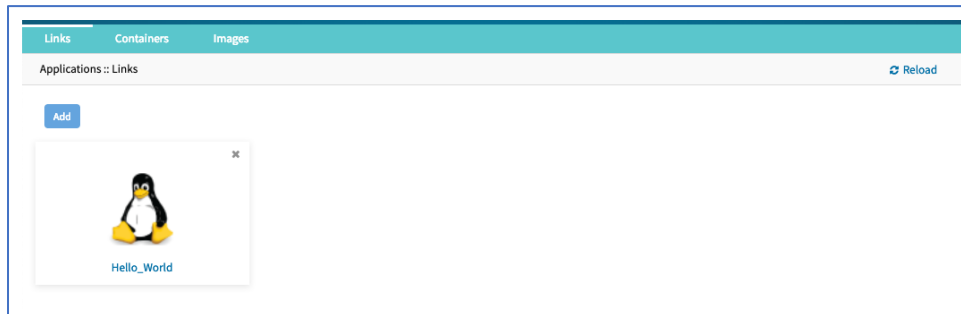
Create Application Link

WebUI Procedure

1. Go to *Applications :: Links*.
2. Click **Add** (displays dialog).
3. Enter a **Name** for the link.
4. In **URL**, provide a valid URL.
5. Click **Select Icon** to choose an icon associated with the link.



6. Click **Save**.
7. When the link is created, click the link to validate.



Network Function Virtualization

Administrators can run additional NFV's or other Virtual Machines. A large variety of configuration options is available through the command line interface.

Contact [Technical Support](#) for more information.

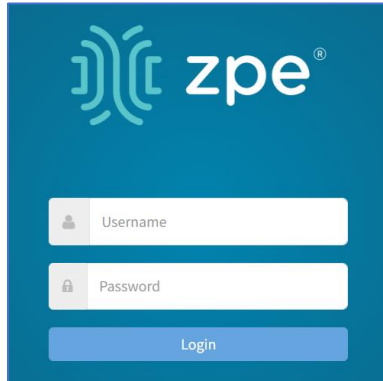
Appendix A – General Information

Technical Support

Our Technical Support staff provides assistance in any operational or installation issues for the Nodegrid products. For any question first follow this procedure:

1. From the Device WebUI, open the device help. Based on the WebUI location of the situation, go to the document location for that feature/function.

2. Check the Online help documentation at www.zpesystems.com/support
3. (admin privileges only) Access the <https://<Nodegrid URL>/services/status>.
Enter the login credentials.



On the *Status* page, review contents.

Services :: Status Table		Reload
Name	Status	
Configuration Manager	● Up	
API	● Up	
CLI	● Up	
Web Services	● Up	
Search Engine	● Up	
Dashboard	● Up	
Network	● Up	

Reboot Last updated: Wed May 18 2022 12:17:09 GMT+0000 (Coordinated Universal Time)

As needed, check the Knowledge Base or submit a Support Tickets.

+++++

To enable/disable access, go to: *Security :: Services*. In *Active Services* menu, select/unselect:

Enable Services Status Page checkbox (default: enabled)

(as needed) **Enable reboot on Service Status Page** checkbox (default: enabled)

+++++

4. Visit our [Help Center Website](#) for the Knowledge Base and other useful links.

Support Ticket

Submit an online ticket request

1. At the top-right of the WebUI, click **Submit a request**.
2. In the form, enter the required information. Provide as much detailed information as possible on the description of the problem or question.
3. If needed, a file or graphic image can be attached.
4. Select the **I'm not a robot** checkbox.
5. Click **Submit**.

A response email will be sent to you from ZPE Systems that confirms your request was received. The email includes the Support Ticket Number. This is needed as reference.

Updates and Patches

To automatically receive information about important security patch announcements, future firmware updates, and other technical information, sign up to **The Loop** at www.zpesystems.com/loop/

Manage Virtual Machines

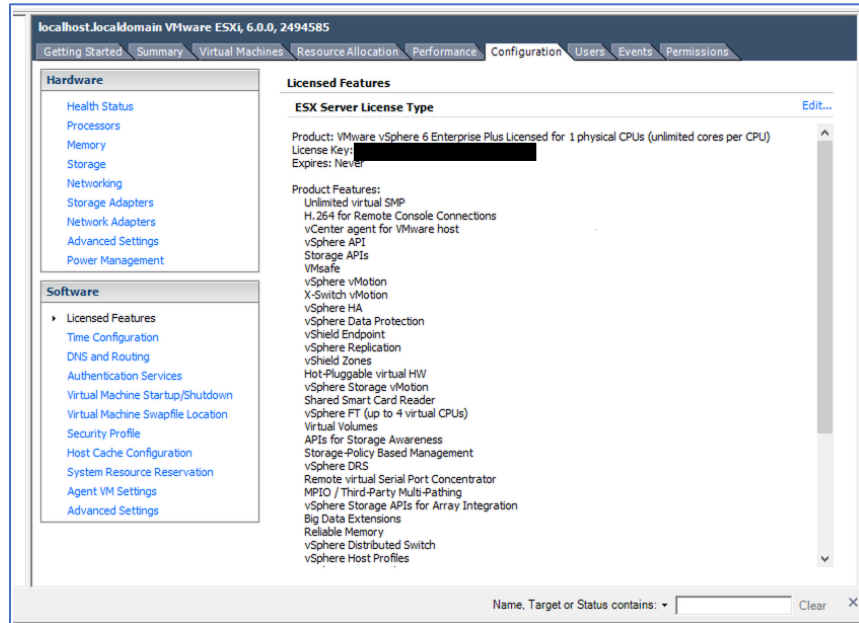
Management of VMWare virtual machines are supported, including KVM Virtual Machines.

These features are available:

- MKS Sessions (for VMWare machines only)
- Virtual Serial console session (for VMWare machines only)
- Console session (for KVM machines only)
- Power Control through the hypervisor
- Web Session to the device

Direct connections to ESX or VSphere servers are supported. When a direct connection is made, the ESX server has to support the feature: "vCenter agent for VMware Host". This is enabled through an ESX server license.

To check if the ESX server supports this feature, login to the ESX host and go to the *License Feature* section. Host supported licenses and features are listed.



NOTE: To utilize the vSPC option with VMWare virtual machines, the port must be configured on the Virtual Machine.

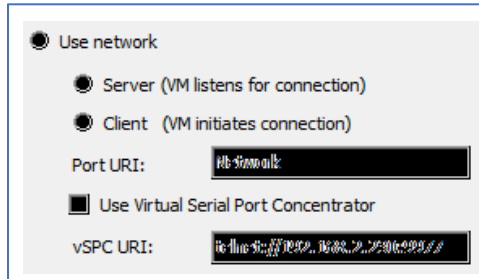
Virtual Serial Port (vSPC) on VM Servers

To redirect the VMware VM vSPC data to the Nodegrid Platform, the VM serial port needs to be configured.

Configure vSPC on VM Server

Ensure the VM is turned off.

1. Open the ESXi configuration (vSphere).
2. Select the VM and click **Edit Virtual Machine Settings**.
3. Click **Add** (displays dialog).
4. Click **Serial Manager Device**.
5. On the pop-up dialog, click **Next**.
6. Click **Connect Via Network**, then click **Next**.
7. Select **Client** (VM initiates the connection).
8. (optional) For **Port URI**, enter **<group_id>** where group_id is an identifier used during the Auto Discovery (to relate servers of the same group).
9. On **vSPC URI**, type **telnet://<IP or Nodegrid Manager hostname>:9977**.
10. Click **Finish**.

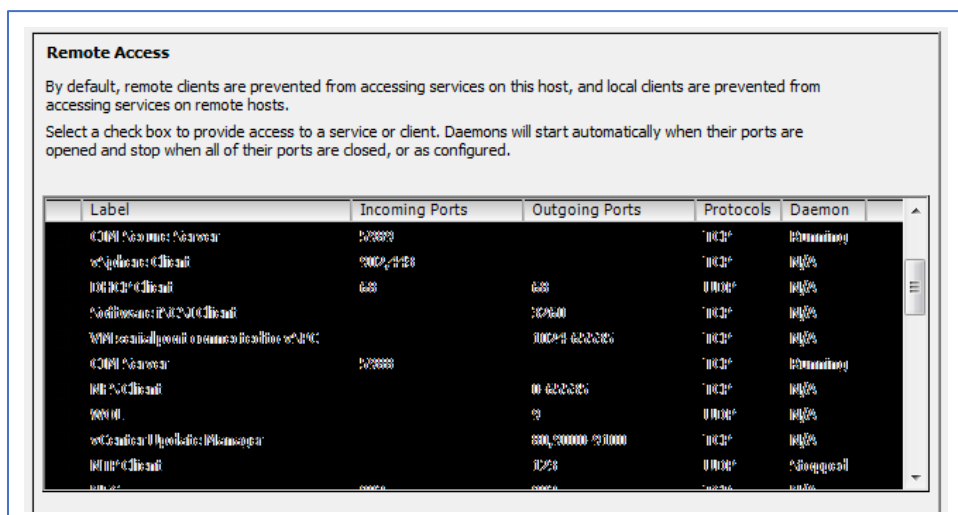


11. On the ESXi firewall, ensure the vSPC port is enabled. To confirm, go to **ESXi Configuration**, select **Security Profile** and click on **Properties**.



12. On the *Remote Access* page, review the box related to VM serial port connected to vSPC.

Outgoing Ports should have a TCP port range starting from 1024 or higher. The port range must include the TCP port used on the vSPC URI field (default 9977).



Modify Outgoing Port Range

1. Connect to the ESXi command line.

2. Execute the following commands:



3. Edit the port section:



4. Save the changes and then restart the firewall service.



For further information on VMware firewall, please refer to the [VMware Knowledge Base](#).

Serial Port Pinout

The tables below provide serial port pinout information.

Cisco-like Pinout

Pin	Signal name	Input/output
1	CTS	IN
2	DCD	IN
3	RxD	IN
4	GND	N/A
5	GND	N/A
6	TxD	OUT

Pin	Signal name	Input/output
7	DTR	OUT
8	RTS	OUT

Legacy Pinout

Pin	Signal name	Input/output
1	RTS	OUT
2	DTR	OUT
3	TxD	OUT
4	GND	N/A
5	CTS	IN
6	RxD	IN
7	DCD	IN
8	Unused	N/A

Safety

Please refer to the links below for product safety information.

[Nodegrid Serial Console](#)

[Nodegrid Net Services Router](#)

[Nodegrid Gate SR](#)

[Nodegrid Bold SR](#)

[Nodegrid Link SR](#)

[Nodegrid Hive SR](#)

Please refer to the links below for product installation information.

Quick Install Guide

Please refer to the links below for product installation information.

[Nodegrid Serial Console](#)

[Nodegrid Net Services Router](#)

[Nodegrid Gate SR](#)

[Nodegrid Bold SR](#)

[Nodegrid Link SR](#)

[Nodegrid Hive SR](#)

RoHS

Please refer to the links below for RoHS information.

[Nodegrid Serial Console](#)

[Nodegrid Net Services Router](#)

[Nodegrid Gate SR](#)

[Nodegrid Bold SR](#)

[Nodegrid Link SR](#)

[Nodegrid Hive SR](#)

Data Persistence

In normal operation, when data logging is enabled (Configuration settings), this data is stored in non-volatile memory:

- user data from keystrokes
- managed devices output
- device monitoring data passing through a Nodegrid device

Nodegrid Device Memory

Nodegrid devices contain the following separate memory devices:

BIOS

Memory Size: 64MB Memory Type: NOR Flash Volatility: Nonvolatile User Data: No

Flash Disk

Memory Size: 32 GB or 64 GB. Other custom sizes may be used. Memory Type: SSD Volatility: Nonvolatile User Data: Yes. Partition/Data: sda2 - unit configuration sda5 - backup configuration sda8 - user home directories and log files

RAM

Memory Size: 4 GB or 8 GB Memory Type: DDR3 Volatility: Volatile User Data: Yes

Remove Data from Nonvolatile Memory

Soft Removal of User Data from Nonvolatile Memory

Removes files and installs factory default configuration on flash disk.

Restore Factory Default Configuration

1. Shutdown Nodegrid device and power off.
2. To remove the device from the network, disconnect Ethernet cables.
3. Disconnect any USB storage device and USB network device connected to device.
4. To access Nodegrid unit, use one of these options:

Connect a terminal/workstation to the Nodegrid console port (RJ-45 console adapter) and a straight-through network cable.

Connect a HDMI monitor (HDMI port) and USB keyboard (USB port).

5. Power on the device.
6. On the following menu, select *Nodegrid Manager - Rescue Mode*.

```

*****
*Nodegrid Manager <version>                                     *
*Nodegrid Manager <version> - Factory Default Settings         *
*Nodegrid Manager <version> - Rescue Mode                       <-- *
*Nodegrid Manager <version> - Network boot                     *
*Nodegrid Manager <version> (verbose)                          *
*                                                                *
*                                                                *
*                                                                *
*                                                                *
*                                                                *
*****
` Use the * and * 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.`

```

7. At the prompt ("bash-4.3#"), run this command (erases all files and loads factory configuration):

```

apply_settings --factory-and-cleanlogs -f -h

```

8. Wait for this message:

```

Apply factory settings completed.  INIT:
Switching [ ... ] reboot: System halted

```

9. Power off the unit.

Hard Removal - Secure Erase

This completely erases the flash disk. This procedure destroys ALL data on flash disk and render it unrecoverable even by data recovery services. After that, the Nodegrid software must be reinstalled via network.

Fully Erase Nonvolatile Memory

1. Shutdown Nodegrid device and power off.
2. To remove the device from the network, disconnect Ethernet cables.
3. Disconnect any USB storage device and USB network device connected to device.
4. To access Nodegrid unit, use one of these options:

Connect a terminal/workstation to the Nodegrid console port (RJ-45 console adapter) and a straight-through network cable.

Connect a HDMI monitor (HDMI port) and USB keyboard (USB port).

5. Power on the device.
6. When the BIOS setup page appears, press the 'Esc' key.
7. In the Grub Menu, select *Nodegrid Platform - Secure Erase*.

```

GNU GRUB version 2.00

+-----+
|Nodegrid Platform - Chain boot          |
|Nodegrid Platform - Rescue Mode        |
|Nodegrid Platform - Secure Erase  <--  |
|                                         |
|                                         |
+-----+

`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.`

```

8. Type 'erase' to permanently erase all data from the system:

```

Nodegrid Boot live - Secure Erase
This action will completely erase the system. Using this procedure will destroy ALL
data on the SSD and render it unrecoverable even by data recovery services. After
executing this step, system software will no longer exist and must be reinstalled via
network. Type 'erase' to secure erase the SSD or 'cancel' to reboot:

```

NOTE: Secure Erase requires the unit be power cycled (powered off and powered on) prior to the erase command execution. Otherwise, the following message displays and the system halts to allow the power cycle to be done.

```

Operation not supported. Unit must be power cycled prior to erase command. Wait for
system halt and power cycle the unit. [ 4.614365] reboot: System halted

```

9. Type **yes** to confirm.

Secure erase cannot be canceled once confirmed. Type 'yes' to confirm secure erase:

10. Wait for the *System halted* message.

```
Secure erase of SDD will start now.. security_password="PasSWorD" /dev/sda: Issuing
SECURITY_SET_PASS command, password="PasSWorD", user=user, mode=high
security_password="PasSWorD" /dev/sda: Issuing SECURITY_ERASE command,
password="PasSWorD", user=user Secure erase completed. System halting.. [ 29.083186]
reboot: System halted
```

11. Power off the unit.

You can find a copy of the [Letter of Volatility here](#).

Mount Remote Shares for Virtual Media

Nodegrid supports remote shares (NFS or Windows shares) to contain files shared with Service Processor systems. Before the files can be shared out through the Virtual Media function, the remote share must be mounted to the Nodegrid device.

CLI Procedure

1. Connect to the Nodegrid shell as the root user.
2. Go to `/var/firefox/datastore/`
3. Create a folder.
4. Use the mount command to mount the remote share to the folder.

To permanently get the share mounted, the mount command can be added to the `/etc/fstab` file.

Example: NFS mount to folder VirtualMedia

```
mount -t nfs 192.168.1.1.:/NFS/NG /var/firefox/datastore/VirtualMedia
```

Monitoring Templates

This monitors and collects sensor data from Managed Devices, connected to a Nodegrid sensor or that support SNMP or IPMI protocol.

The collected data are defined and controlled through Monitoring Templates which will be assigned to a monitored device during its configuration.

Customize a Monitoring Template

Several preexisting monitoring templates are available. These typically fulfill user requirements. As needed, these templates can be customized. All templates are text files, located in sub directories at `/etc/collectd.templates` according to the protocol used to collect monitoring data (SNMP or IPMI).

`/etc/collectd.templates/snmp`

`/etc/collectd.templates/ipmi`

Any new file added to these directories automatically appear in the user interface.

SNMP Template

Create a new SNMP Template

CLI Procedure

1. Login to the Shell as root.
2. Create a copy of one existing template as a starting point for the new template.
3. Each SNMP template file has two types of subsections:
 - Data (one entry per data point, each identified by a unique ID.)
 - Host (one single entry, defined SNMP parameters, collecting interval, and data points to be collected.)
4. The template file should only include data points of general common use. All other data points can be removed from the file.
5. Use commit to save the template.

Settings and Values for Data Entry

Setting	Value	Description
Data	Internal name of the data point as it is collected. Should be unique.	Cannot have spaces. Example: "pdu_in_cur", "pdu_in_vol".
Type	Temperature, fan speed, humidity, counter, percent time left, voltage, current power, apparent_power, power_factor, frequency	Data type
Table	True/False	reflects if the OID is part of a table or not
Instance	True/False	If Table= true (SNMP OID prefix retrieves a list of names associated with the corresponding values). For example, in a PDU this could be the outlet name. If Table = false (name of the instance is associated with the value).
InstancePrefix	String	(optional) String to prepend to the Instance, enclosed in double quotes.
Values	True/False	If Table = true (SNMP OID prefix retrieves a list of values). If Table = false (SNMP OID retrieves a single value).
Scale	Decimal value	(optional) Decimal value to be multiplied to the value retrieved before persisting it.

Example:

```
<Data "pdu_in_cur">
```

```

Type "current"
Table true
Instance ".1.3.6.1.4.1.476.1.42.3.8.40.20.1.20"
Values ".1.3.6.1.4.1.476.1.42.3.8.40.20.1.130"
Scale 0.01
</Data>

```

The host entry in an SNMP template only requires an adjustment in the Collect setting. The values list should contain a list of all data entries to be collected. All listed data entries require a corresponding data entry definition.

IPMI Discovery Template

The discovery template for IPMI automatically discovers all available sensors on an IPMI device. The template has one subsection.

IPMI Options

Setting	Value	Description
AuthType	None, md2, md5, straight	Authentication type for the IPMI protocol (default: negotiate the strongest one).
Privilege	Callback, user, operator, admin	Privilege level for IPMI protocol (default: admin).
Sensor	Name of the Sensor to be collected	Selects sensors to collect or ignore, depending on "Ignore, Selected" setting. Can be defined multiple times, each for one selected sensor.
IgnoreSelected	True/False	If true, does not collect for the sensors selected by Sensor. If false, only collects for the sensors selected by Sensor.
Scale	""	(optional) A decimal value to be multiplied to the value retrieved before persisting it.

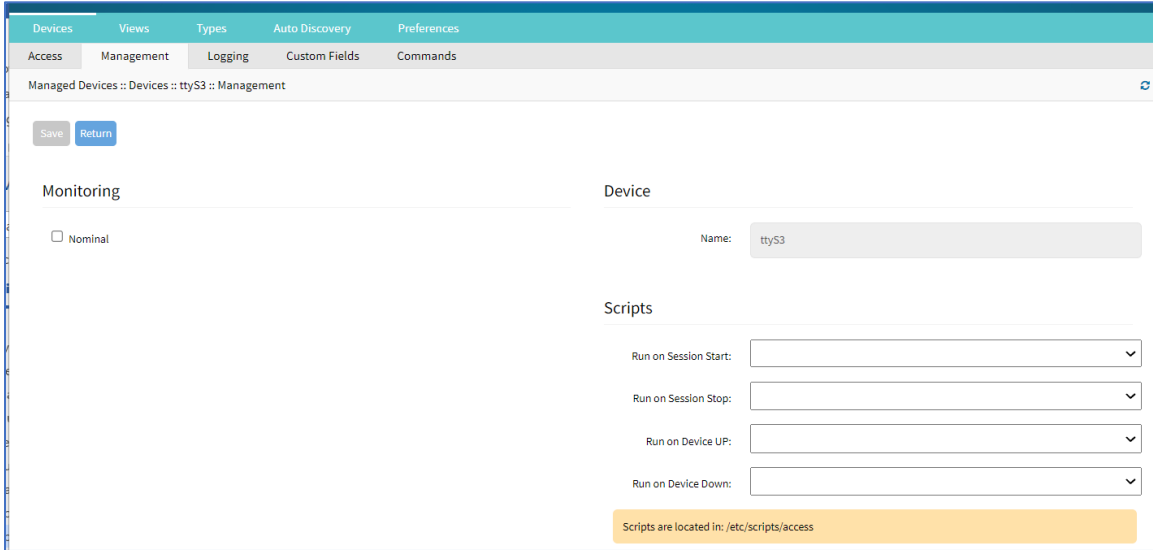
Enable Monitoring

Monitoring is enabled on a per-device basis. The settings are part of the Managed Device settings.

WebUI Procedure

1. Go to *Managed Devices :: Devices :: <device name> :: Management*.

NOTE: for <device name> on Devices table, click on a device to display the dialog with sub-tabs.



2. Enable and configure the required monitoring protocol like SNMP or IPMI
3. Select **Enable Monitoring** checkbox.
4. Assign the template
5. Assign the collection interval.
6. Click **Save**.

Supported Nodegrid Devices

USB Passthrough

This feature requires the latest USB controller (currently only available for NSR). Support for the Link SR, Bold SR, and Gate SR will become available in future releases. NSC does not support this feature.

USB Passthrough ties two consecutive ports (defined by the hardware). Two operation modes are available for USB ports:

Host Mode

USB devices connected to the port are detected. Power to the port can be controlled.

Passthrough Mode

USB devices connected to the port are not detected. Power to the port is not available.

USB Power

The USB Power feature allows control of power to specific USB ports. This requires the latest USB controller (currently only available for NSR). Support for the Link SR, Bold SR, and Gate SR will become available in future releases. NSC does not support this feature.

USB ports for the new hardware have two operation modes:

Host Mode

USB devices connected to the port are detected. Power to the port can be controlled.

Passthrough Mode

USB devices connected to the port are not detected. Power to the port is not available.

Nodegrid automatically detects if the installed USB card supports Power Control. Required configuration files are updated during boot. All USB ports are configured with USB mode set to Host. Initial state (by default) is set to On.

NOTE: Devices with internal USB Serial adapters that provide power do not allow the USB Power option to be on or off.

USB Type

If Power Control is supported, the USB Type can be configured without the device connected to the port. Three options are available:

usb_serialB (USB serial adapter)

usb_sensor (USB sensors – i.e., TRH320 for temperature and humidity)

usb_device (all other USB devices)

When **usb_device** is selected, **Management** and **Monitoring** tabs are not available.

KVM Dongle

With the KVM USB dongle, a KVM session can be established to a legacy server (VGA and USB connection). The System automatically detects the dongle when it is connected. The device must be enabled.

Bluetooth

Bluetooth devices are supported. These are primarily used for monitoring and IoT applications. The Bluetooth functionality is provided through the Nodegrid WiFi module which is available for the Nodegrid Service Router family.

By default, the Bluetooth functionality is disabled. It must be manually enabled before use.

An admin user can enable the service via the shell with these commands:

```
[admin@nodegrid /]# shell sudo su -
root@nodegrid:~#sed -i
s/^BLUETOOTH_ENABLED=0/BLUETOOTH_ENABLED=1/g/etc/default/Bluetooth
root@nodegrid:~#sed -i s/^#AutoEnable=true/AutoEnable=true/g /etc/bluetooth/main.conf
root@nodegrid:~#sed -i
s/^#InitiallyPowered=true/InitiallyPowered=true/g/etc/bluetooth/main.conf
root@nodegrid:~# /etc/init.d/bluetooth start
root@nodegrid:~# bluetoothctl
root@nodegrid:~# [bluetooth]# scan on
```

After that, Bluetooth devices can be paired to the Nodegrid, then configured for monitoring or an IoT application.

To pair to a device, use the bluetoothctl command:

```

root@nodegrid:~#bluetoothctl bluetoothctl
[bluetooth]# devices
Device 00:16:94:1A:EA:2C Sensor
[bluetooth]# pair 00:16:94:1A:EA:2C
Attempting to pair with 00:16:94:1A:EA:2C
Pairing successful
[bluetooth]# connect 00:16:94:1A:EA:2C
Attempting to connect to 00:16:94:1A:EA:2C
Connection successful
[bluetooth]# quit
    
```

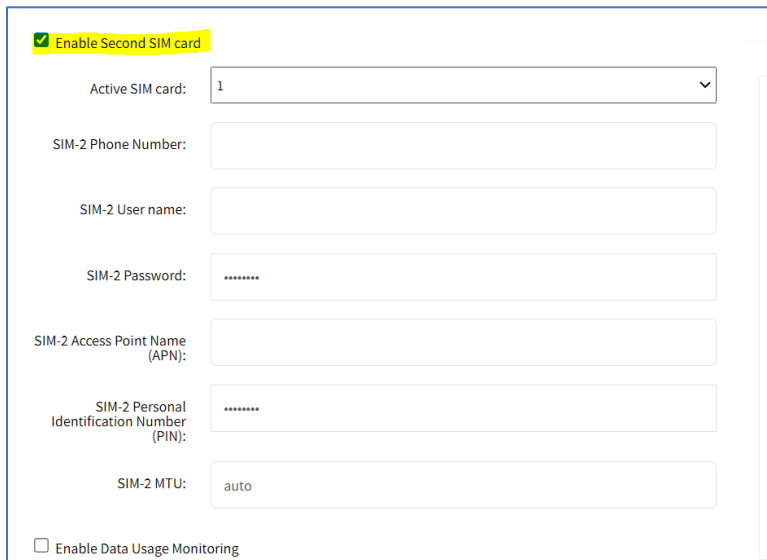
5G Support

NOTE: EM9191 modem supports 5G. EM7565 does not support 5G.

This is available when the wireless modem has dual SIMs and supports GPS dedicated antenna input.

With this device configuration, details are available in *Network :: Connections :: <connection>* (for Mobile Broad Band GSM type). The EM7565 modem and Nodegrid Hive SR (with EM9191 modem) supports dual SIM cards. The EM7565 modem supports GPS dedicated antenna options.

When dual sim is supported, it must be enabled. Go to *Network :: Connections :: <connection>* and configure the settings.



Enable Second SIM card

Active SIM card: 1

SIM-2 Phone Number:

SIM-2 User name:

SIM-2 Password:

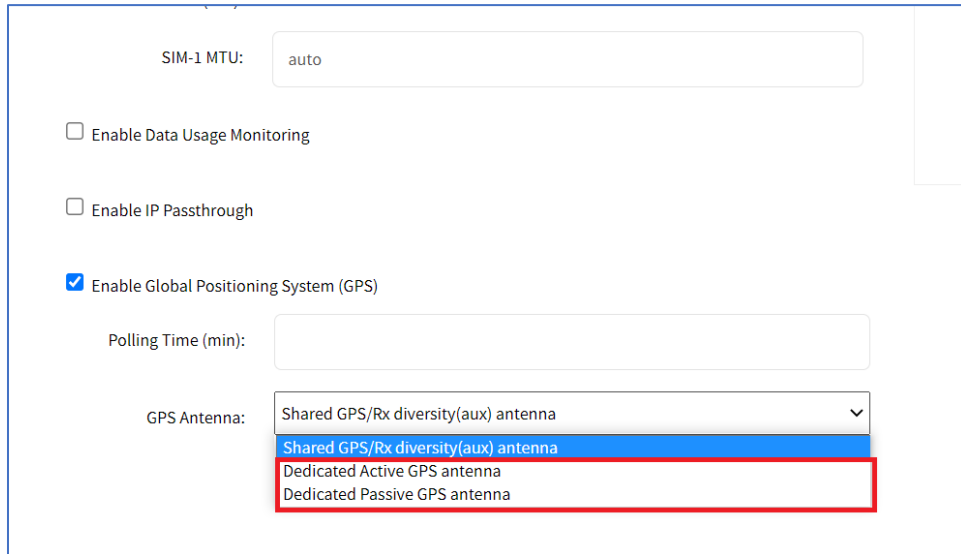
SIM-2 Access Point Name (APN):

SIM-2 Personal Identification Number (PIN):

SIM-2 MTU: auto

Enable Data Usage Monitoring

When the modem supports dedicated GPS antenna, it is shown in the GPS Antenna drop-down. (If not, only the **Shared GPS** option is available.)



SIM-1 MTU: auto

Enable Data Usage Monitoring

Enable IP Passthrough

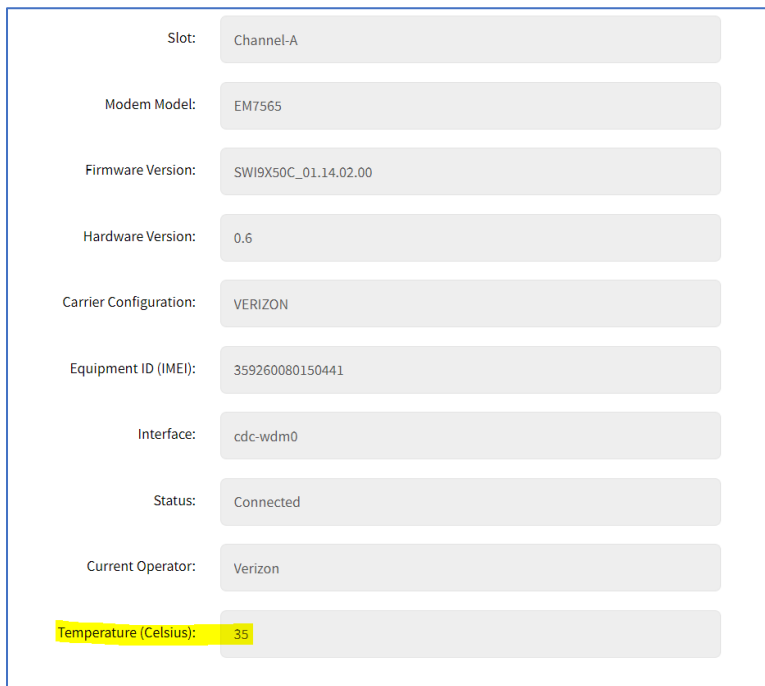
Enable Global Positioning System (GPS)

Polling Time (min):

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

- Shared GPS/Rx diversity(aux) antenna
- Dedicated Active GPS antenna
- Dedicated Passive GPS antenna

New temperature information field is displayed in *Tracking :: Devices :: Wireless Modem :: <modem>*.



Slot: Channel-A

Modem Model: EM7565

Firmware Version: SWI9X50C_01.14.02.00

Hardware Version: 0.6

Carrier Configuration: VERIZON

Equipment ID (IMEI): 359260080150441

Interface: cdc-wdm0

Status: Connected

Current Operator: Verizon

Temperature (Celsius): 35

The information is also available in *Tracking :: HW Monitor :: Thermal*.

Tracking :: HW Monitor :: Thermal			
Name	Value	Unit	Description
CPU Temperature	42	Celsius	CPU temperature
System Temperature	39	Celsius	System temperature
CPU Fan	4189	RPM	CPU FAN speed
System Fan	11550	RPM	System FAN speed
Wireless Modem Channel-A Temperature	35	Celsius	Wireless modem Channel-A temperature

PXE Boot

Nodegrid supports PXE boot (Pre-Boot Execution Environment). PXE is part of the UEFI (Unified Extensible Firmware Interface) used to boot a software image retrieved at boot time from a network server. Data centers prefer this method for OS booting, installation, and deployment.

By default, PXE boot is enabled in Nodegrid. It can be disabled on WebUI (*Security :: Services*) or CLI (/settings/services scope). The example shows how to configure the DHCP/PXE server in Linux (Ubuntu) with installed Apache web server, tftpd-hpa service and Nodegrid 5.4.x.

NOTE: PXE, DHCP and TFTP servers must be installed.

1. Download Nodegrid network boot files (tarball) - Contact Support to obtain the file
2. Copy Nodegrid network boot tar.gz(tarball) file to the DHCP server
3. Unzip the tar file (creates two directories: nodegrid 5.4.xx and boot).

Alternatively, create the directory and put tar file in that directory. Then unzip the tarball file (i.e., cd /var/lib/tftpboot/PXE directory).

Example:

```

root@ubuntu-srv1:~# cd /var/lib/tftpboot/
root@ubuntu-srv1:/var/lib/tftpboot# ls -l
drwxrwxr-x 2 root  root    4096 Apr 24 03:20 nodegrid-4.1.xx
root@ubuntu-srv1:/var/lib/tftpboot# ls -l nodegrid-4.1.xx
total 558468
-rw-r--r-- 1 root  root    22270823 Apr 24 03:19 initrd
-rw-rw-r-- 1 root  root   544343672 Apr 24 03:19 rootfs.img.gz
-rw-rw-r-- 1 root  root         7 Apr 24 03:19 version
-rw-r--r-- 1 root  root    5242832 Apr 24 03:19 vmlinuz
root@ubuntu-srv1:/var/lib/tftpboot#

```

4. (optional) To format the Hard Drive, create a file named "reformat" inside the nodegrid directory

Example:

```

touch nodegrid-5.4.xx/reformat

```

- Open **dhcpd.conf** and add these lines in the “host definition” section. The hardware ethernet value must match the Nodegrid device MAC address. The fixed-address is the Nodegrid device IP address.

Legacy Mode Example

```
host PXEboot_NSC {
    hardware ethernet e4:1a:2c:56:02:9e;
    fixed-address 192.168.22.61;
    option tftp-server-name "192.168.22.201";
    next-server 192.168.22.201;
    option bootfile-name "PXE/boot/grub/i386-pc/core.0";
    option domain-name "zpesystems.com";
    option domain-name-servers 192.168.22.205, 75.75.75.75, 75.75.76.76;
    option routers 192.168.22.202;
}
```

UEFI Mode Example:

```
host PXEboot_NSC {
    hardware ethernet e4:1a:2c:56:02:9e;
    fixed-address 192.168.22.61;
    option tftp-server-name "192.168.22.201";
    next-server 192.168.22.201;
    option bootfile-name "PXE/boot/grub/x86_64-efi/core.efi";
    option domain-name "zpesystems.com";
    option domain-name-servers 192.168.22.205, 75.75.75.75, 75.75.76.76;
    option routers 192.168.22.202;
}
```

- On Web server (i.e., Apache), cd /var/www and create a soft link to the file for the network boot:
ln -s and filename to link to the directory.

```
root@ubuntu-srv1:/var/www# pwd
root@ubuntu-srv1:/var/www#
root@ubuntu-srv1:/var/www# ln -sf /var/lib/tftpboot/PXE/nodegrid-5.4.xx/ nodegrid-5.4.xx
```

- Restart the DHCP server.

```
sudo service isc-dhcp-server restart
```

- Restart tftpd-hpa process.
- Start the Nodegrid device. This installs the Nodegrid netboot image on the device.

VRRP (Virtual Router Redundancy Protocol)

The Nodegrid Platform supports embedded Virtual Router Redundancy Protocol (VRRP). This allows Nodegrid to become part of a virtual router interface (provides router redundancy). This is used to provide automatic failover support for default gateways. By default, VRRP is not configured. To enable support, the service must first be configured by an administrator using the shell.

NOTE: VRRP can only be used with network interfaces directly exposed to the Nodegrid OS. Individual switch ports on a Nodegrid Service Router card cannot be used.

With VRRP, if there are two Nodegrid SR devices, one can be configured to be the VRRP master, and the other to be the VRRP backup. One SR is connected to the other and assigned a virtual IP address in *keepalived* configuration. The connection uses one SR (configured as master). If that SR goes down, VRRP assigns the virtual IP to the backup SR – and traffic continues on the second SR.

VRRP support is implemented through *keepalived* services. Official documentation for the service is available on the [Keep Alived web site](#).

CLI Procedure

The service configuration files are located in */etc/keepalived/*. At a minimum, the *keepalived.conf* must be a valid configuration. The service is started with this command.

```
/etc/init.d/keepalived start
```

To automatically start *keepalived* on the next system start, run this command:

```
update-rc.d -s keepalived defaults 90
```

Example Configuration

The following configuration uses IPv6 for the above topology, but IPv4 is also supported and configured in a similar process.

Router Configuration

Example:

```
sw1$ ip link add name br0 type bridge vlan_filtering 1 mcast_snooping 0
sw1$ ip link set dev swp3 master br0
sw1$ ip link set dev swp11 master br0
sw1$ ip link set dev br0 up
sw1$ ip -6 address add 2001:db8:1::2/64 dev br0
sw1$ ip link set dev swp3 up
sw1$ ip link set dev swp11 up
sw1$ ip link set dev swp7 up
sw1$ ip -6 address add 2001:db8:2::2/64 dev swp7
sw1$ ip -6 route add 2001:db8:4::/64 via 2001:db8:2::1

sw1$ cat /etc/keepalived/keepalived.conf
```

```
global_defs {
  vrrp_garp_master_refresh 60
}

vrrp_instance vrrp_test {
  state MASTER
  interface br0
  virtual_router_id 5
  priority 200
  version 3
  advert_int 0.1
  use_vmac
  vmac_xmit_base
  virtual_ipaddress {
    2001:db8:1::100
  }
  notify_master "/usr/local/bin/vmac.sh true br0 00:00:5e:00:02:05 1"
  notify_backup "/usr/local/bin/vmac.sh false br0 00:00:5e:00:02:05 1"
  notify_stop "/usr/local/bin/vmac.sh false br0 00:00:5e:00:02:05 1"
}
sw2$ ip link add name br0 type bridge vlan_filtering 1 mcast_snooping 0
sw2$ ip link set dev swp55 master br0
sw2$ ip link set dev swp54 master br0
sw2$ ip link set dev br0 up
sw2$ ip -6 address add 2001:db8:1::3/64 dev br0
sw2$ ip link set dev swp55 up
sw2$ ip link set dev swp54 up
sw2$ ip link set dev swp56 up
sw2$ ip -6 address add 2001:db8:3::2/64 dev swp56
sw2$ ip -6 route add 2001:db8:4::/64 via 2001:db8:3::1

sw2$ cat /etc/keepalived/keepalived.conf
global_defs {
  vrrp_garp_master_refresh 60
}

vrrp_instance vrrp_test {
  state BACKUP
  interface br0
  virtual_router_id 5
  priority 150
  version 3
  advert_int 0.1
  use_vmac
  vmac_xmit_base
  virtual_ipaddress {
```

```

    2001:db8:1::100
  }
  notify_master "/usr/local/bin/vmac.sh true br0 00:00:5e:00:02:05 1"
  notify_backup "/usr/local/bin/vmac.sh false br0 00:00:5e:00:02:05 1"
  notify_stop "/usr/local/bin/vmac.sh false br0 00:00:5e:00:02:05 1"
}

```

In the above configuration, the virtual router uses an advertisement interval of 0.1 seconds. A longer interval can be used – but increases the failover time. This is because the Backup router waits for three times the advertisement interval before declaring the Master as down.

The `vmac_xmit_base` option causes VRRP packets to be sent with the MAC of the underlying interface (br0 in the example) instead of the virtual MAC. (This does not conform to the VRRP specification, but is recommended in practice.)

On both switches, `vmac.sh` is the file described below. The file ensures packets whose destination MAC is the virtual MAC are locally received by the Master router. An FDB entry is configured with the virtual MAC and the local flag.

Example:

```

sw1$ cat /usr/local/bin/vmac.sh
#!/bin/bash

master=$1
bridge=$2
vmac=$3

if [[ "$#" -eq 4 ]]; then
    vlan="vlan $4"
fi

if [[ $master == "true" ]]; then
    bridge fdb replace $vmac dev $bridge self local $vlan
else
    bridge fdb del $vmac dev $bridge self local $vlan
fi

```

Host Configuration

Example:

```

host$ ip link add name bond0 type bond mode active-backup miimon 100 use_carrier 1
host$ ip link set dev ens6 master bond0
host$ ip link set dev ens7 master bond0
host$ ip link set dev ens6 up
host$ ip link set dev ens7 up
host$ ip link set dev bond0 up

```

```
host$ ip -6 address add 2001:db8:1::1/64 dev bond0
host$ ip -6 route add 2001:db8:4::/64 via 2001:db8:1::100
host$ ip link set dev bond0 type bond primary ens6
```

To avoid duplicate packets, the host uses an active-backup LAG to connect both switches. The virtual router (2001:db8:1::100) is the gateway to the 2001:db8:4::/64 network (although in actual deployments this usually is the default gateway).

The MAC address of the virtual router is the virtual router MAC (VMAC):

```
host$ ip -6 neighbour show 2001:db8:1::100
2001:db8:1::100 dev bond0 lladdr 00:00:5e:00:02:05 router REACHABLE
```

The LSB indicates that the virtual router ID is 5 (in accordance with the virtual router configuration above).

Appendix B – UEFI Implementation

The latest UEFI specification defines an entirely new interface between operating system and firmware/BIOS.

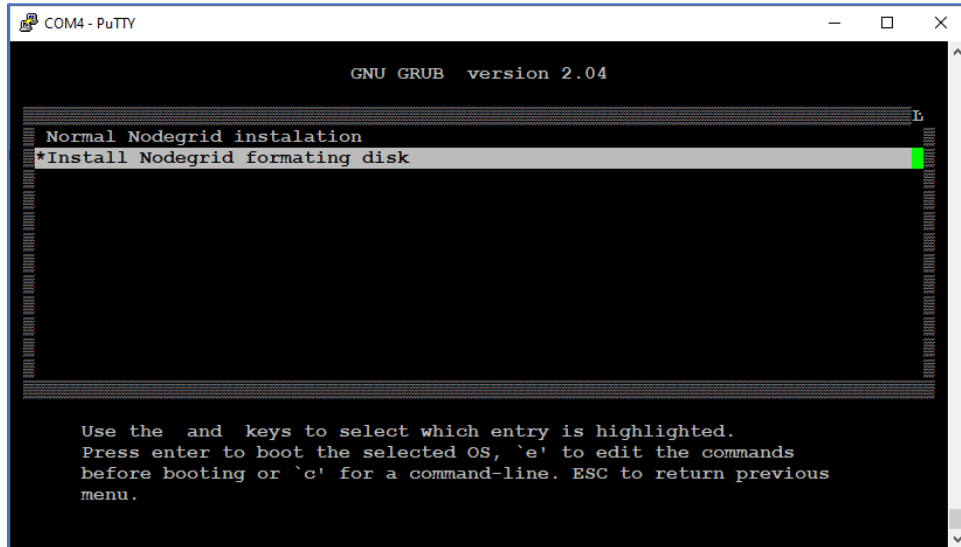
UEFI Upgrade/Downgrade Concerns

Nodegrid OSES version 5.0 or below are Legacy Only, which means those images are not capable of booting in a system configured for UEFI Boot Mode. In a system running one of those images can be upgraded to new versions but will still run in Legacy. To Upgrade a Legacy device with a new image in UEFI mode, the following procedure is required:

10. Burn an USB Drive with NG 5.X UEFI image

Or setup a PxE Server with NG5.X UEFI Netboot Tarball.

11. During installation, select Install Nodegrid formatting disk.



12. After installation, change Boot mode to UEFI Mode. Login to OS shell as root and enter the following command:

```
/usr/sbin/hwec_cmds -boot_mode set uefi
```

13. Reboot the system.

Enable Secure Boot (optional)

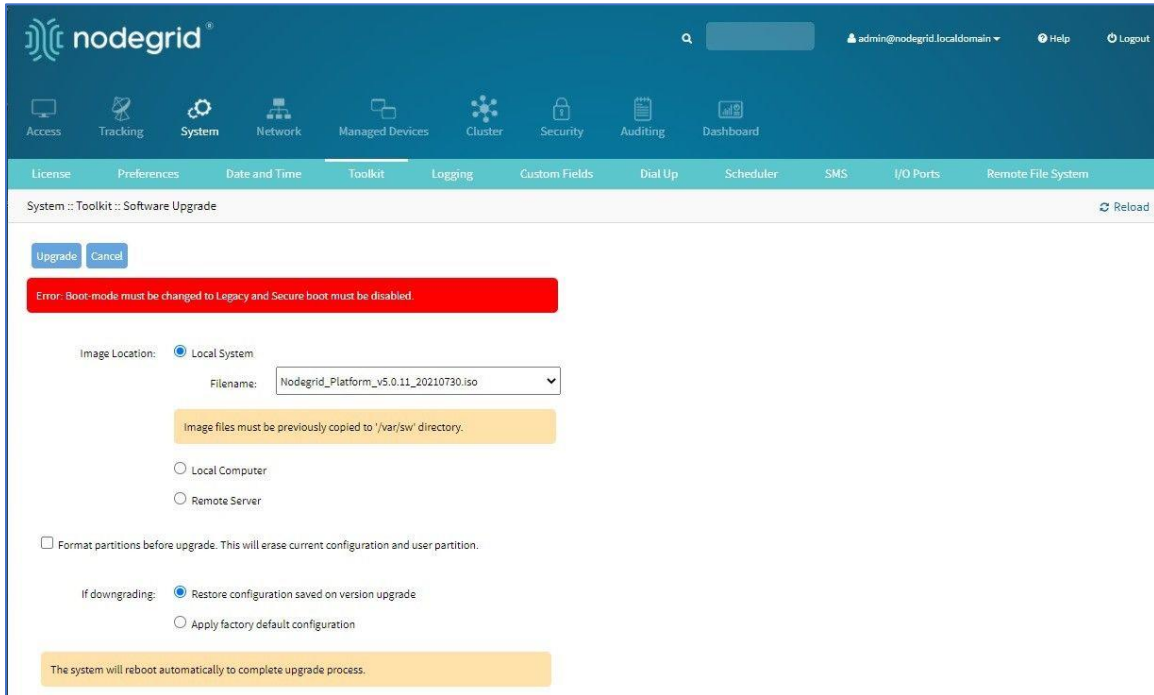
WebUI Procedure

1. Go to *Security :: Services :: Intrusion Prevention*.
2. Select **Enable Secure Boot** checkbox.
3. Click **Save**.
4. Reboot the device.

Nodegrid OS version 5.1 and above are both Legacy and UEFI compatible.

Downgrade to Legacy

When in UEFI Boot Mode (optional Secure Boot), the device cannot be downgraded to Legacy Only. If a Legacy Image downgrade is necessary (v5.0 and below), disable Secure Boot and change to Legacy Mode. Then the downgrade procedure can be done.



1. Log into OS shell as root.
2. Enter:


```
/usr/sbin/hwec_cmds -secure_boot set 00
/usr/sbin/hwec_cmds -boot_mode set legacy
```
3. Reboot the system.
4. After that, proceed normally with the reboot.

Self-Encrypting Drive

Self-Encrypting Drive (SED) refers to SSDs with built-in full-disk encryption. The SED feature provides data privacy security against SSD theft. The customer can enable SSD data encryption, based on an authentication password. The Pre-Boot Authenticator is stored in SSD's Controller MBA and unlocks the drive during the boot process.

Minimum BIOS Versions

- NSR-COMP-EXPN (10518T00)
- NSR (10518T00)
- GSR (10617T00)
- LSR (10730T00)
- BSR (10813T00)

Device Conditions

- System's Boot Mode must be UEFI.
- Self-Encrypting Drive Pre-Boot Authenticator must be installed.
- After feature is enabled, a **power cycle** is required to activate.
- Lock Password is required to disable this feature.

Security Adjustments to System

- PxE Boot is disabled.
- Boot Order is set to SSD Only.
- When Password-and Protected Boot is enabled, use of Rescue Mode requires authentication.
- Secure Boot is strongly recommended.

Secure Boot

Secure Boot is optional in UEFI, but it highly recommended. It ensures software integrity on the device. A trust relationship is established between the UEFI BIOS and the device software (bootloaders, OS, UEFI drivers and utilities). When enabled, only software or firmware signed with approved keys can be executed.. This guards the system against malicious attacks, rootkits, and unauthorized software updates that could occur prior to the device's OS launch.

The Secure Boot mechanism relies on public/private key pairs to verify the software's digital signature before execution. In the Secure Boot Standard Mode (default configuration), ZPE official public certificates are provided to validate Nodegrid OS images. To validate other device OS, the Secure Boot Custom Mode can use custom certificates installed in BIOS.

Requirements

- System's Boot Mode must be UEFI.
- Minimum BIOS version for Nodegrid devices:
 - NSR-COMP-EXPN (10518T00)
 - NSR (10518T00)
 - GSR (10617T00)
 - LSR (10730T00)
 - BSR (10813T00)

Intrusion Prevention

The Intrusion Prevention section allows configuration of preventive mechanisms (i.e., Fail 2 Ban, Rescue Mode) to prevent unauthorized access to a System. The following settings are available:

Intrusion Prevention Settings

Setting	Value	Description
Block host with multiple authentications fails	TRUE/FALSE	Blocks host from access after the maximum limit of failures occur.
Period Host will stay blocked (min)	Number in minutes	Amount of time the system is not reachable on the network (default: 10).
Timeframe to monitor authentication fails (min)	Number in minutes	Amount of time when failed authentication attempts maxed, and before the counter gets reset (default: 10).
Number of authentication fails to block host	Number	Number of failed authentication attempts before the user is blocked (default: 5).
Rescue Mode requires authentication	TRUE/FALSE	When enabled, Rescue Mode requires authentication through a local user account (i.e., root).
Password protected boot	TRUE/FALSE	When enabled, editing BIOS and Grub requires authentication based on the defined password.
Enable Secure Boot	TRUE/FALSE	When enabled, only ZPE-signed OS with ZPE standard certificates in BIOS are permitted to boot.
SED PBA Version	Read only text	Pre-Boot Authenticator Version installed in the SSD.
Self-encrypting drive	TRUE/FALSE	When enabled, all SSD data is automatically encrypted.
Lock password menu: Random Auto Generated	Radio button	Select to generate a ZPE random password.
Lock password menu: Random auto-generated	Radio button	Save the auto-generated Lock password.
Generated password	Read only text	Auto-generated Lock password. WARNING! SAVE THIS PASSWORD (Lock Password is required to disable this feature.)
User defined	Radio button	Enter user defined Lock password.
Lock password	Read only text	Enter Lock Password. WARNING! SAVE THIS PASSWORD (Lock Password is required to disable this feature.)
Confirm lock password	Read only text	Confirm Lock Password. WARNING! SAVE THIS PASSWORD (Lock Password is required to disable this feature.)

NOTES:

Password Protected Boot is a patent-pending feature that allows Nodegrid OS to communicate with BIOS to enable the BIOS password to prevent unauthorized changes. The same password also protects Grub from unauthorized changes.

The Password Protected Boot feature requires minimum BIOS version of 81122T00. On the WebUI, see About information for the current version.