



nodegrid

User Guide v5.0

Contents

About the Nodegrid v5.0 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 Net Services Router Family.....	9
Nodegrid Net Services Router.....	10
Nodegrid Net Services Router Expansion Modules.....	12
Nodegrid Gate SR	15
Nodegrid Hive SR.....	19
Nodegrid Bold SR.....	22
Nodegrid Link SR	26
Nodegrid Mini SR	30
Nodegrid Manager	33
Installation	34
Hardware Installation	34
Shipping Box Contents.....	34
Installation of Modules for Nodegrid Services Router.....	35
M.2 Cellular Antenna Placement	36
Device Power Connections	37
Rack Mounting	41
Network Connection	45
Power Cord(s) Connection	45
Connect Target Devices	45
Serial Target Devices	45
IP Target Devices.....	46
Connect to a Nodegrid Device	46
Connect to the Console Port	47
ETH0 Connection	47
WiFi Connection	47
Bluetooth® Connection	48
KVM Port Connection.....	48
I/O Ports (GPIO).....	48
Import / Export Configuration	49
Export Configuration Settings.....	49
Import Configuration Settings	50
Nodegrid Manager Installation	50
Create a VMware Virtual Machine.....	50
Install Nodegrid Manager Software	53
Initial Network Configuration	55
Access the CLI Window.....	56
Identify Current IP Address	56
Define Static IP Address.....	57
General Information.....	58
User Interfaces.....	58
WebUI View.....	58
CLI Interface.....	59
Shell Access.....	61
Access to Devices.....	61
Device Sessions.....	61

- CLI Device Sessions 63
- Search Functionality 65
 - Device Search 65
 - Global Search 68
- Access Section 68
 - Table tab 69
 - Function Descriptions 69
 - View Device Details 72
 - View Device Power Details 73
 - Tree tab 74
 - Expand View Column Branches 74
 - Node tab 75
 - Map tab 76
 - Image tab 76
- Tracking Section 76
 - Open Sessions tab 77
 - Sessions Table sub-tab 77
 - Devices Table sub-tab 77
 - Event List tab 77
 - Statistics sub-tab 77
 - Events sub-tab 78
 - System Usage tab 83
 - Memory Usage sub-tab 83
 - CPU Usage sub-tab 83
 - Disk Usage sub-tab 84
 - Discovery Logs tab 84
 - Reset Logs 84
 - Network tab 85
 - Interface sub-tab 85
 - Switch Interface sub-tab 85
 - LLDP sub-tab 85
 - Routing Table sub-tab 85
 - Devices tab 86
 - Serial Statistics sub-tab 86
 - USB Devices sub-tab 87
 - Wireless Modem sub-tab 87
 - Scheduler tab 87
 - HW Monitor tab 87
 - Thermal sub-tab 88
 - Power sub-tab 88
 - USB Sensors (or I/O Ports) sub-tab 88
 - I/O Ports (GPIO) sub-tab 89
- System Section 89
 - License tab 90
 - Manage Licenses 90
 - Preferences tab 90
 - Nodegrid Location 91
 - Session Idle Timeout 91
 - Nodegrid Configuration 92
 - Login Page Logo Image 93
 - Login Banner Message 94
 - Utilization Rate Events 95
 - Serial Console 95
 - Power Supplies 96
 - Network Boot 96

- PXE Boot..... 96
- Date and Time tab 98
 - Local Settings sub-tab..... 98
 - NTP Authentication sub-tab..... 100
- Toolkit tab 102
 - Reboot..... 103
 - Shutdown 103
 - Software Upgrade 103
 - Save Settings 104
 - Apply Settings 105
 - Restore to Factory Default Settings..... 106
 - System Configuration Checksum 107
 - System Certificate 109
 - Network Tools 111
 - API 113
 - Diagnostic Data 116
 - Cloud Enrollment 117
- Logging tab 119
- Custom Fields tab 120
- Dial-Up tab 121
 - Services sub-tab..... 122
 - Callback Users sub-tab 122
- Scheduler tab 123
 - Manage Tasks..... 124
- SMS tab (only with installed cellular module)..... 127
 - SMS Settings sub-tab..... 127
 - CLI Examples: SMS Actions and Messages 128
 - Whitelist sub-tab 130
- I/O Ports tab (only with GPIO)..... 130
- Network Section 131
 - Settings tab 131
 - Hostname and Domain Name 131
 - Network Failover 131
 - Network Failover for Wireless Connections..... 132
 - IPv4 and IPv6 Profile 133
 - Connections tab 133
 - Bonding Interfaces 135
 - Ethernet Interfaces 136
 - Mobile Broadband GSM Interface 137
 - Enable Data Usage Monitoring..... 137
 - Enable IP Passthrough..... 138
 - VLAN Interface 139
 - WiFi Interface 139
 - Bridge Interface 140
 - Analog Modem Interface 140
 - Static Routes tab..... 141
 - Hosts tab..... 141
 - DHCP Server tab 142
 - Network Switch Configuration 142
 - Switch Interfaces 143
 - VLAN Configuration..... 143
 - ACL 143
 - Untagged/Access Ports..... 143
 - Tagged/Trunk Ports..... 143
 - Backplane Ports 143

- LAG 143
- SSL VPN tab..... 144
 - VPN SSL 144
- IPsec tab 147
 - Overview 147
 - IPsec Configuration Process 150
 - Tunnel sub-tab 151
 - IKE Profile sub-tab 152
 - Global sub-tab 153
- Flow Exporter tab 154
 - Add a new flow export: 155
- QoS tab 155
 - Interfaces sub-tab 155
 - Classes sub-tab 156
 - Rules sub-tab 157
- Managed Devices Section 158
 - General Information 158
 - Supported Protocols 158
 - Device Types 158
 - Devices tab 160
 - Configure Serial Connections 160
 - Service Processor Devices 163
 - Device Management with SSH 165
 - Third-Party Console Servers 167
 - KVM Switches 171
 - Rack PDUs 175
 - Cisco UCS 179
 - Netapp 181
 - Infrabox 183
 - Virtual Machines 186
 - Configure Auto Discovery of VMware Virtual Machine 187
 - Device Management 192
 - Authenticate with SSH Keys 192
 - Auto-Discovery 194
 - Auto Discovery of Console Server and KVM Switch Ports 195
 - Auto Discovery of Network Devices 199
 - Auto Discovery of Virtual Machines 204
 - Auto Discovery of DHCP Clients 209
 - Configure Individual Device Settings 212
 - Hostname Detection 213
 - Create a Probe or Match 214
 - Multi sessions 215
 - Break Signal 217
 - Escape Sequences 217
 - Disable User Authentication 218
 - SSH / Telnet Port 219
 - Binary Socket 220
 - IP Aliases 221
 - Location 222
 - Device Web URL Options 223
 - Assign Icon to Device 224
 - Device Mode 225
 - Device Expiration 226
 - Device State Detection 227
 - Triggered Custom Scripts on Device Status Change 228

- Data Logging 229
- Event Logging 230
- Triggered Alert Strings and Custom Scripts 231
- Custom Fields 234
- Commands and Custom Commands 234
- Console-like Access 238
- Views tab 239
- Preferences tab..... 239
 - Power Menu sub-tab 239
 - Session Preferences sub-tab 240
 - Views sub-tab 240
- Cluster Section 242
 - Peers tab..... 243
 - Cluster Settings tab..... 243
 - Enable Cluster..... 243
 - Automatic Enrollment 243
 - License Pool..... 244
 - Peer Management..... 244
 - Downgrading 244
- Security Section 245
 - Local Accounts tab..... 245
 - Manage Local Users 246
 - Hash Format Password..... 246
 - API Keys..... 246
 - Password Rules tab 248
 - Authorization tab 249
 - Manage Groups..... 249
 - Group Permissions..... 249
 - External Authentication Provider 253
 - SSH Key Authorization..... 254
 - Authentication tab 255
 - Add a server 255
 - SSO (Single Sign-On) 256
 - LDAP and Active Directory 257
 - TACACS +..... 260
 - RADIUS..... 262
 - Kerberos..... 264
 - RSA SecurID, 2-factor authentication..... 264
 - Firewall tab..... 270
 - NAT tab..... 272
 - Services tab 275
 - General Services sub-tab..... 275
 - Intrusion Prevention sub-tab..... 280
- Auditing Section 281
 - Event tab..... 281
 - Categories sub-tab 281
 - Settings tab 282
 - Events tab 282
 - Destinations..... 283
- Monitoring Section..... 286
 - Monitoring Templates 286
 - SNMP Template 286
 - IPMI Discovery Template 287
 - Supported Nodegrid Devices 288
 - USB Sensors..... 288

KVM Dongle	288
Bluetooth	288
VRRP (Virtual Router Redundancy Protocol).....	289
Dashboard Section.....	290
Data Point Exploration	290
Create a Visualization	292
Line Charts	292
Area Charts	296
Create a Dashboard.....	299
Inspect a Dashboard	300
Applications Section.....	302
Docker Applications	302
Docker Images	303
Docker Containers.....	304
Application Links	304
Network Function Virtualization.....	305
Appendix A – General Information	305
Technical Support	305
Support Ticket	306
Updates and Patches	306
Virtual Serial Port (vSPC) on VM Servers	306
Serial Port Pinout.....	308
Safety.....	309
Quick Install Guide.....	310
RoHS	310
Data Persistence.....	310
Remove Data from Nonvolatile Memory	311
Soft Removal of User Data from Nonvolatile Memory	311
Hard Removal - Secure Erase.....	312

About the Nodegrid v5.0 User Guide

Document updated: July 13, 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

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 Part15 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 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:

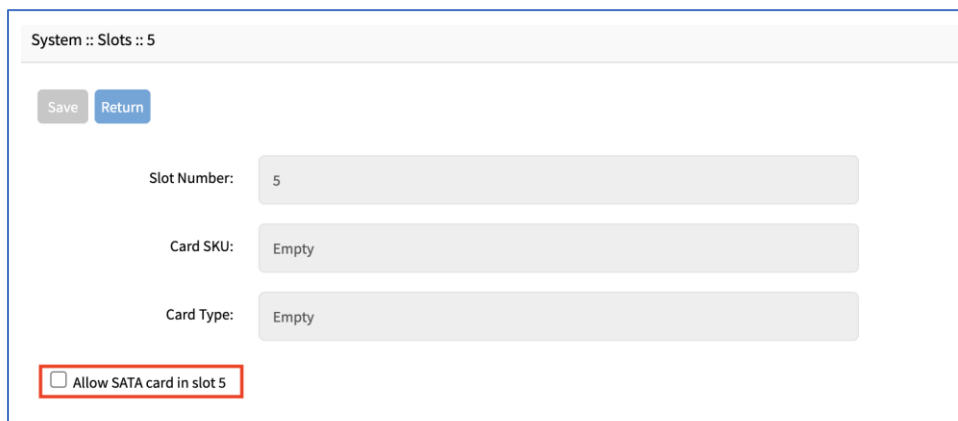
LTE/M2.SATA must be installed in slot 4.

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*.



System :: Slots :: 5

Save Return

Slot Number: 5

Card SKU: Empty

Card Type: Empty

Allow SATA card in slot 5

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

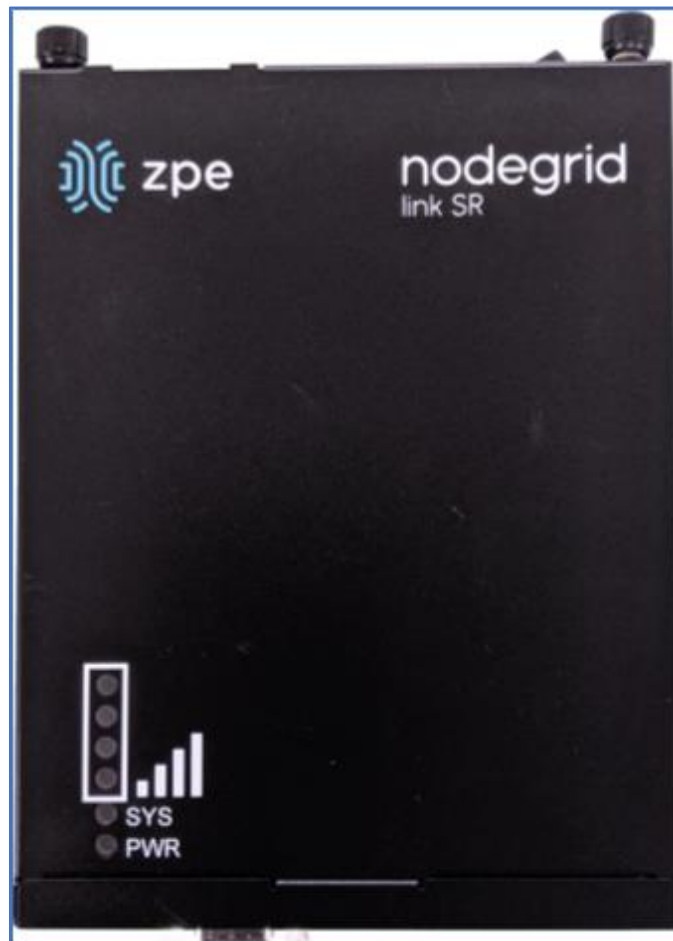
- Zero Touch Provisioning (ZTP) for fast and easy setup in remote locations
- Integrates with ZPE Cloud and ZPE Systems Nodegrid Manager vendor-neutral, unified management solution
- Direct Linux shell, HTML5 cross-device web access and command line interface
- Modern 64-bit Linux Kernel for fast security 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

Please refer to the “Quick Install Guide provided with the unit in the box for quick instructions on how to start your box.

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.

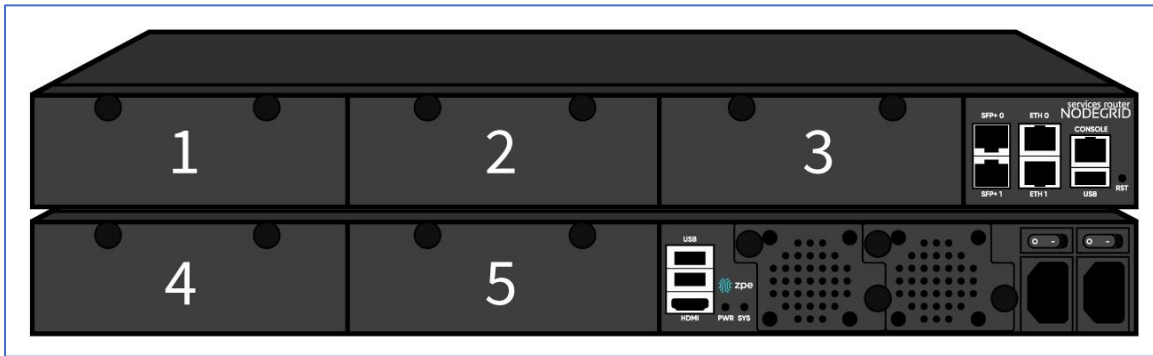
Installation of Modules for Nodegrid Services Router

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, please 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 car and they 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

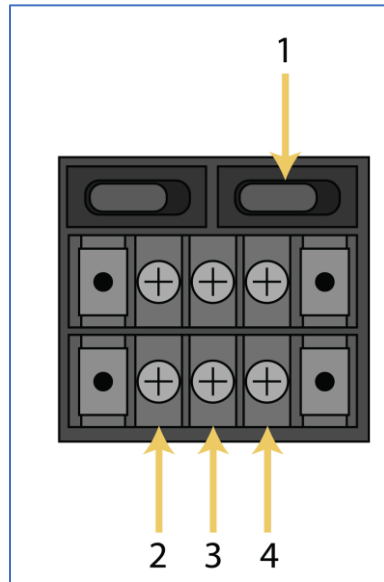
DC Power

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.

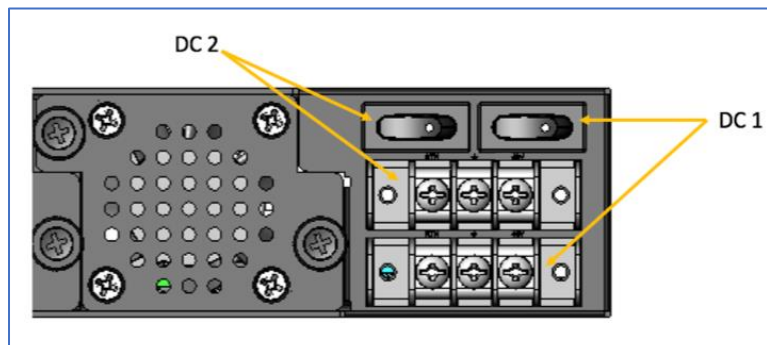
Dual DC Power Connection Terminal Block



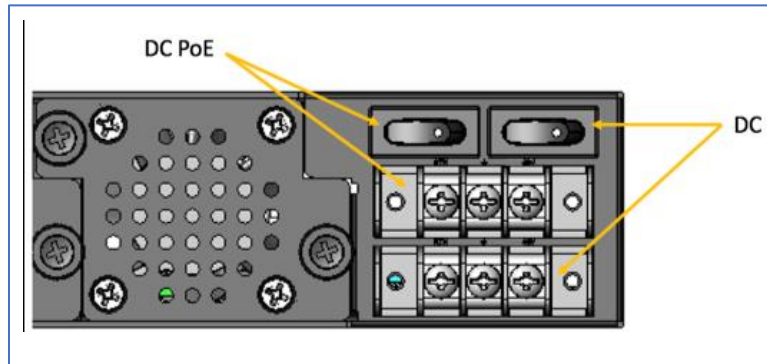
DC Power Block Terminals

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

DC association - terminal power source and switch



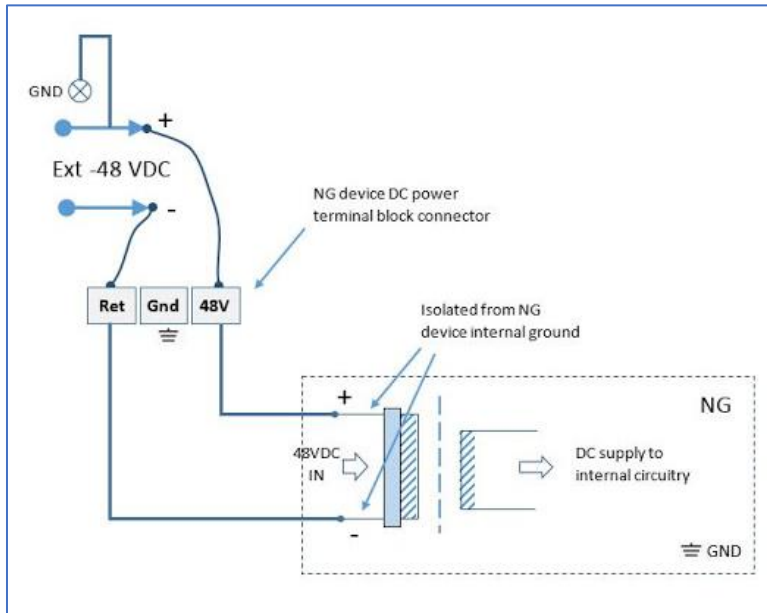
NSR Single DC + PoE Power Connection Terminal Block



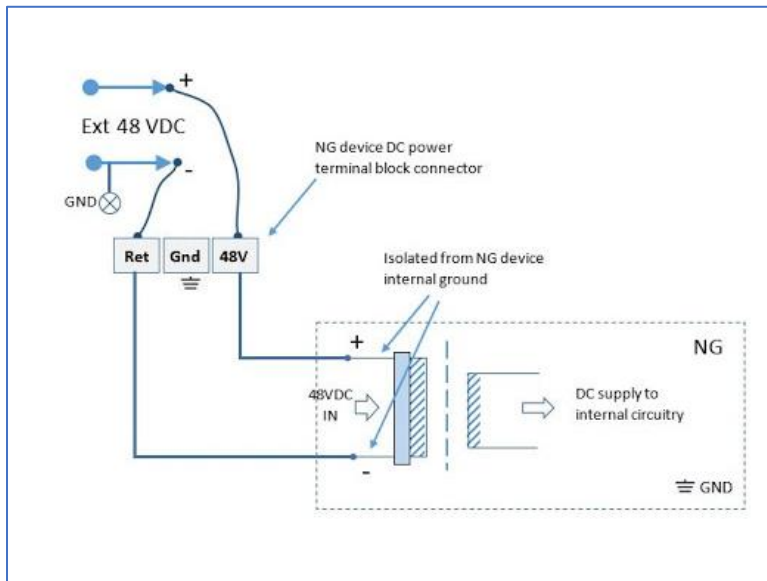
Connect a Nodegrid device to DC Power

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

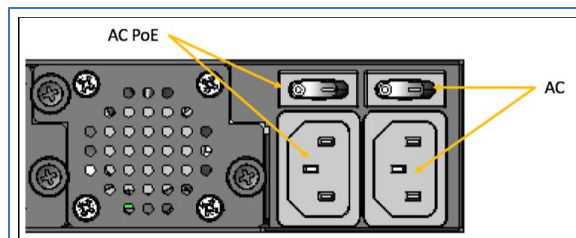


+48VDC supply



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 that the fans blow into the correct direction. The fan direction can be determined from the part number of the unit.

Rack Mounting

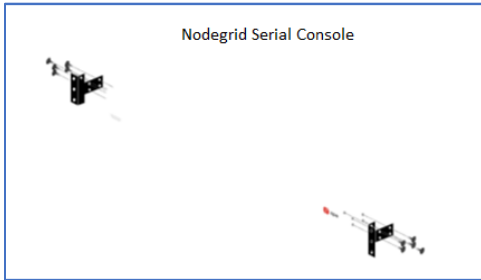
Model	Part Number	Cooled	Airflow
Nodegrid Serial Console - T Series	NSC-Txx-xxxx-xxx	Passive	N/A
Nodegrid Serial Console - R Series	NSC-TxxR-xxxx-xxx	Passive	N/A
Nodegrid Serial Console - S Series	NSC-TxxS-xxxx-xxx-F	Active	Front-Back (air in) 
Nodegrid Serial Console - S Series	NSC-TxxS-xxxx-xxx-B	Active	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)

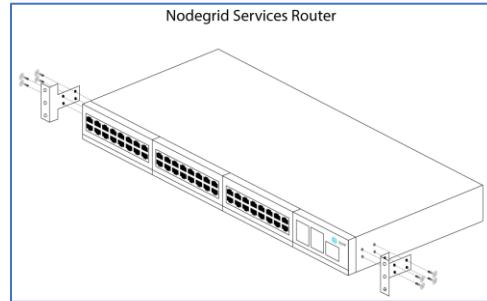
Rack Installation

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

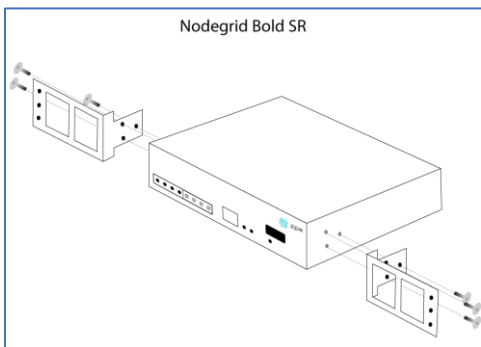
Nodegrid Serial Console



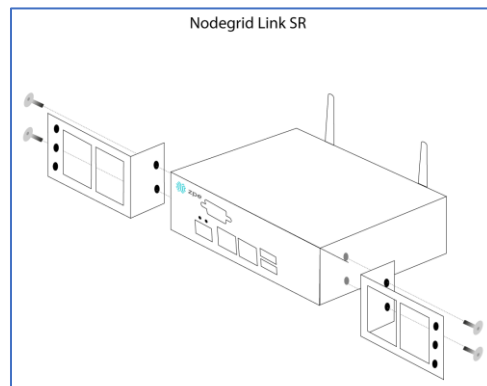
Nodegrid Net Services Router



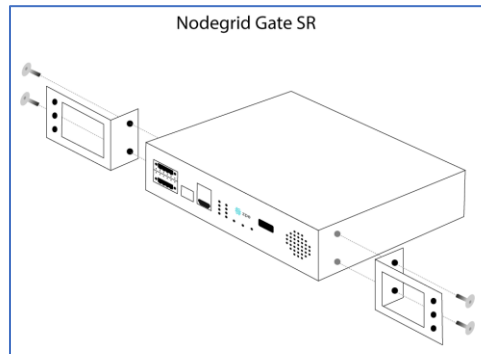
Nodegrid Bold SR



Nodegrid Link SR

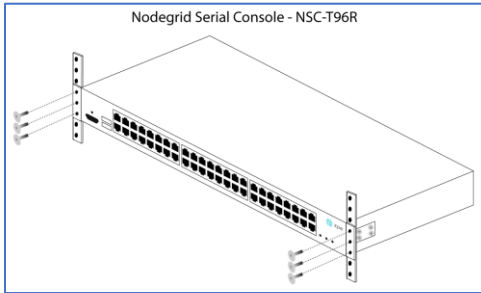


Nodegrid Gate SR

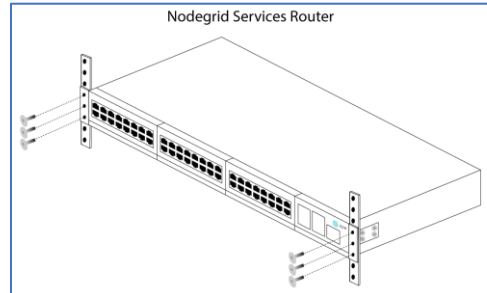


2. Locate the position on the rack where you would like to mount the unit and ensure the slot is clear of any obstructions.
3. Slide the unit into the rack and align the mounting bracket screw holes with the screw holes on the rack as shown below:

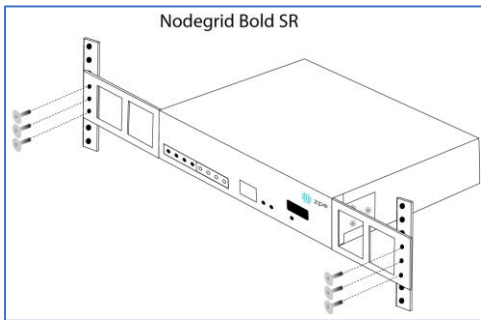
Nodegrid Serial Console



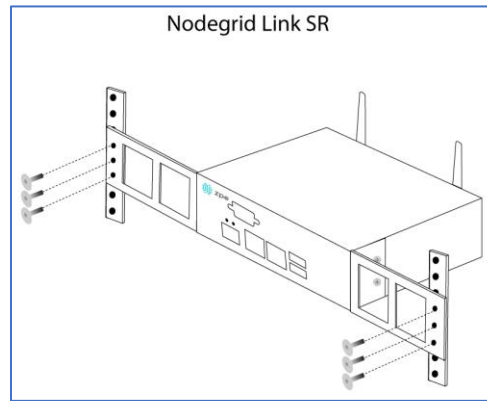
Nodegrid Net Services Router



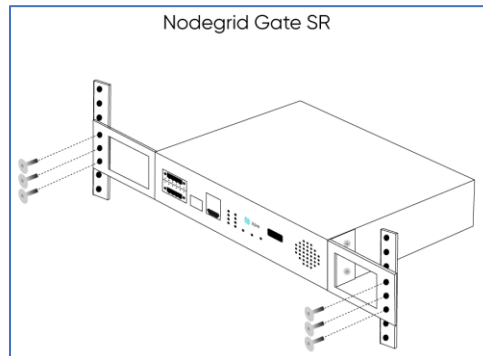
Nodegrid Bold SR



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 to complete the installation.

Network Connection

Depending on the 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. (See “DC Power” for information on the DC power supply ports).

Connect Target Devices

Serial Target 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.

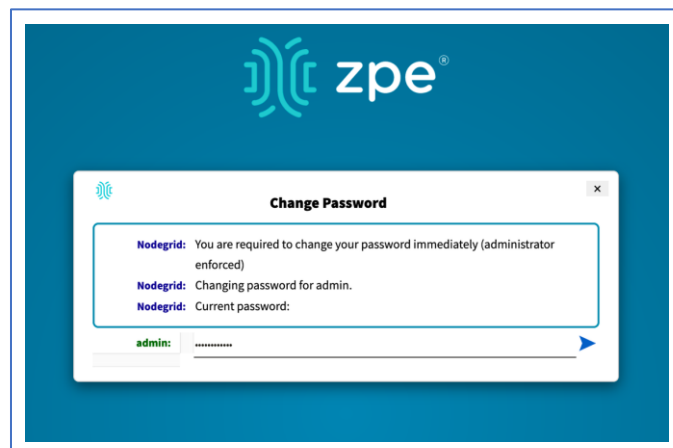
IP Target Devices

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

All IP based target devices are directly connected to a network interface on a Nodegrid unit, or connected through an existing network infrastructure. If the target 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.

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)

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.

Nodegrid Manager Installation

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

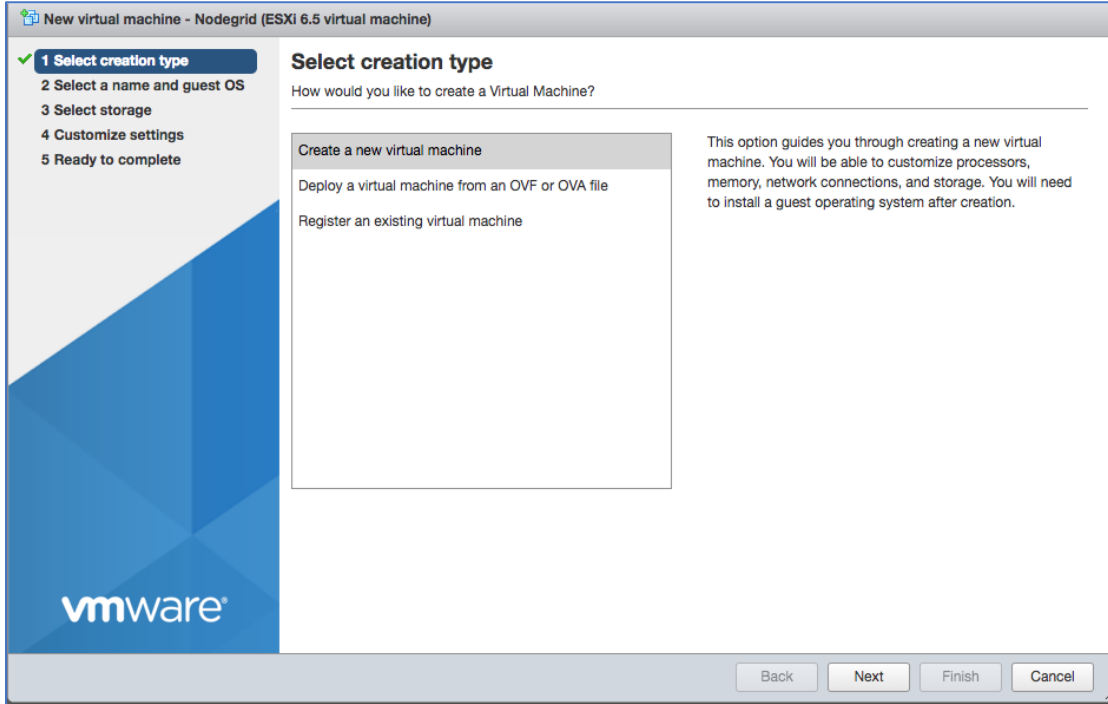
1. Create a virtual machine.
2. To install, boot from the ISO file/CD.
3. Restart and boot from the new virtual machine.

Minimum Requirements:

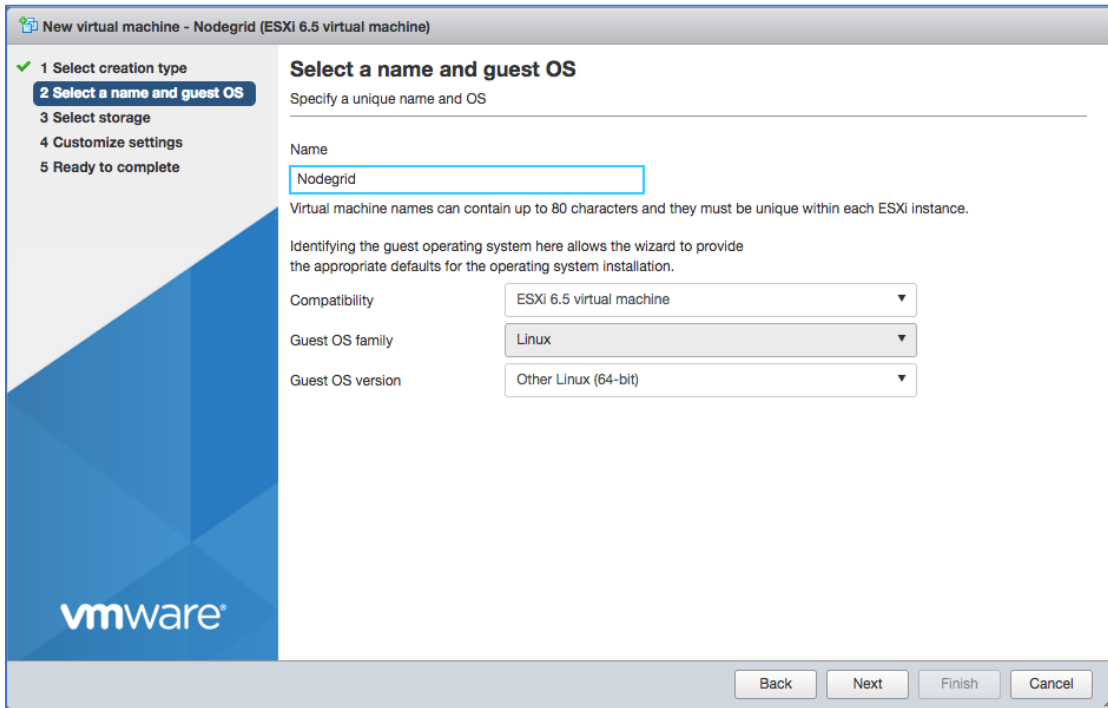
- ESXi 4.1 or above
- 32 GB hard drive (connected through the LSI Logic Parallel Controller)
- 4 GB memory (8GB is recommended)
- 2 Network adapters (E1000 adapters are recommended)

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:



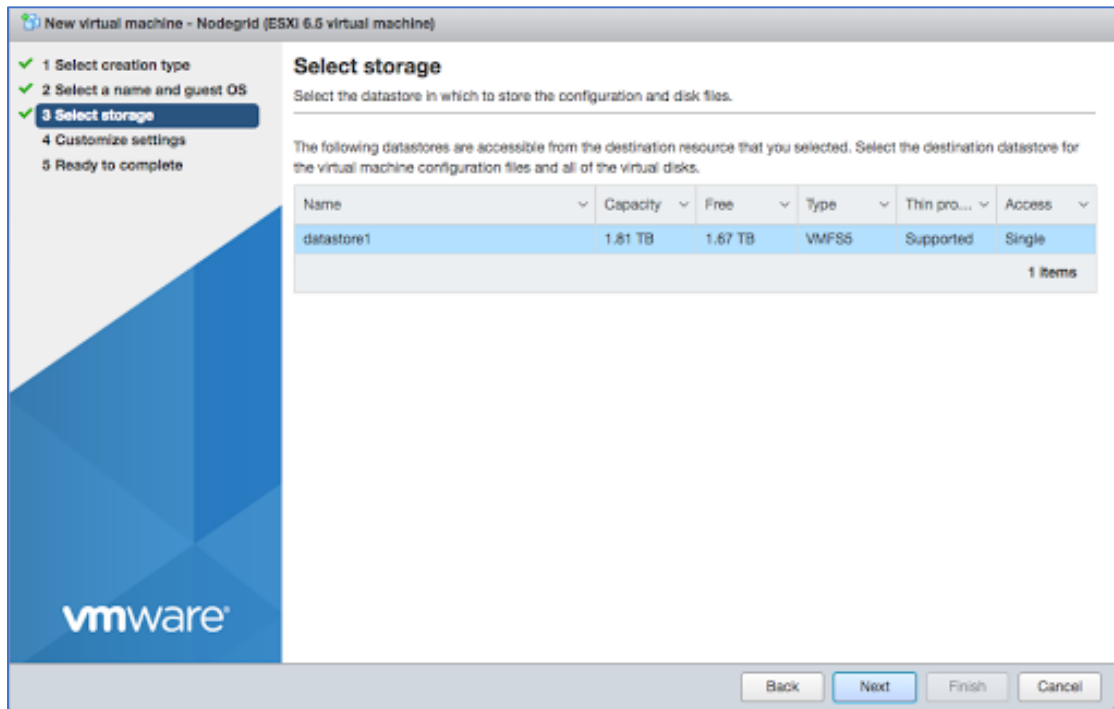
Enter **Name** for the Nodegrid Manager virtual machine.

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**.

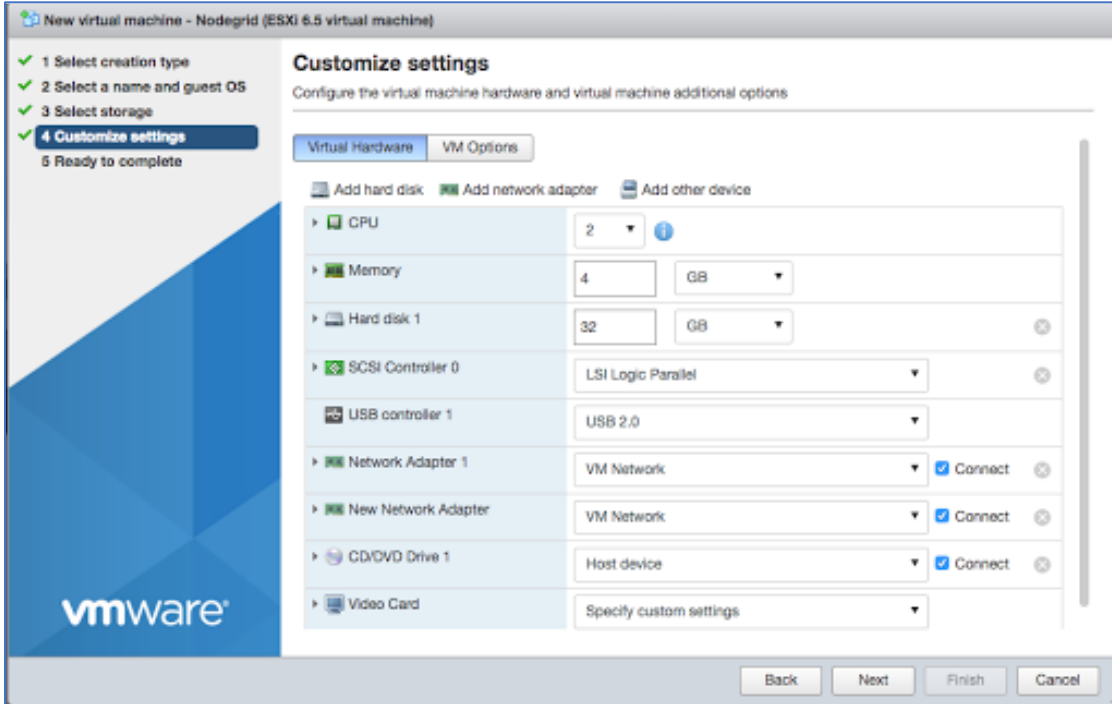
CPU: 2

Memory: 4GB

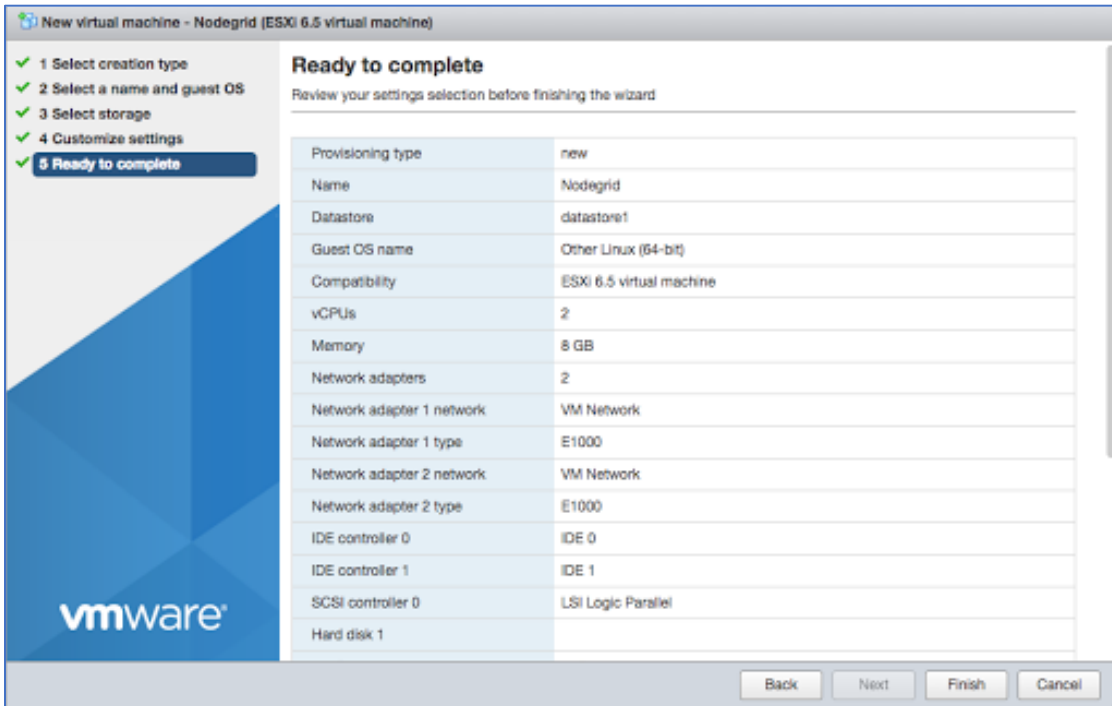
Hard disk: 32GB

SCSI Controller: LSI Logic Parallel

Network adapters: 2 of type E1000



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

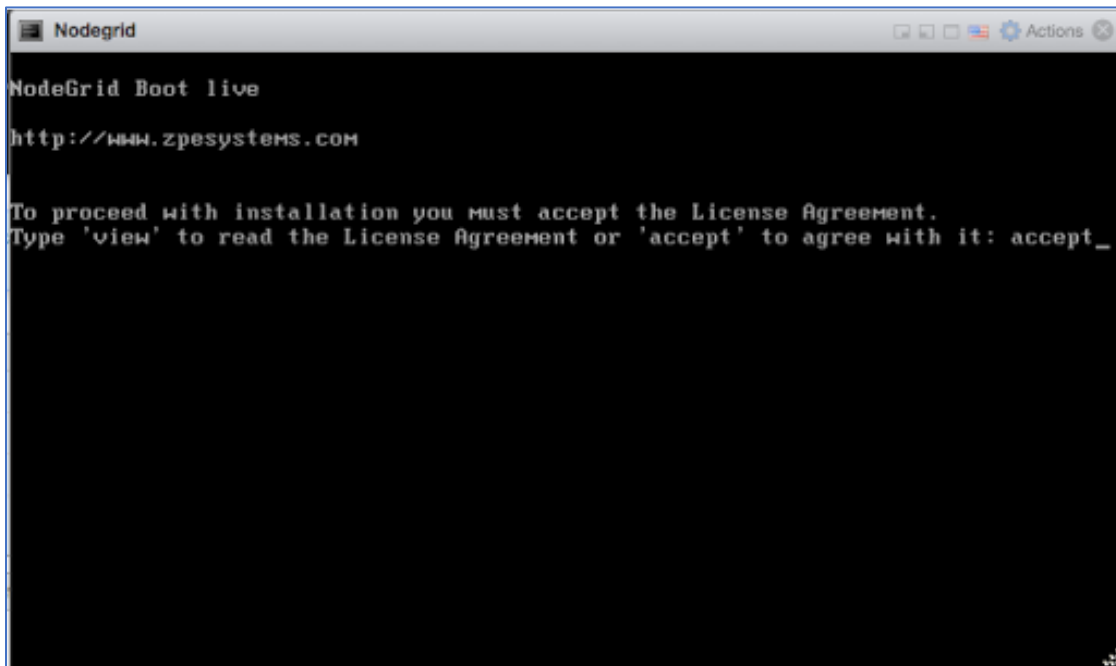


This completes the virtual machine configuration on the ESXi server.

Install Nodegrid Manager Software

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**.



```
NodeGrid Boot live
http://www.zpesystems.com

To proceed with installation you must accept the License Agreement.
Type 'view' to read the License Agreement or 'accept' to agree with it: 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: 0x000000000019ba276
input_len: 0x0000000000429974
output: 0x00000000001000000
output_len: 0x0000000000dd28c8
kernel_total_size: 0x0000000000a6e000

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: _
    
```

Initial Network Configuration

The Nodegrid Platform can be accessed through a console port in HTTPS (web interface) or SSH (CLI). Other methods can be enabled later.

By default, the Nodegrid Platform is set up with DHCP IP configuration enabled.

NOTE: The Nodegrid Platform will respond on ETH0 at 192.168.160.10 if your DHCP server fails or is unavailable.

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:

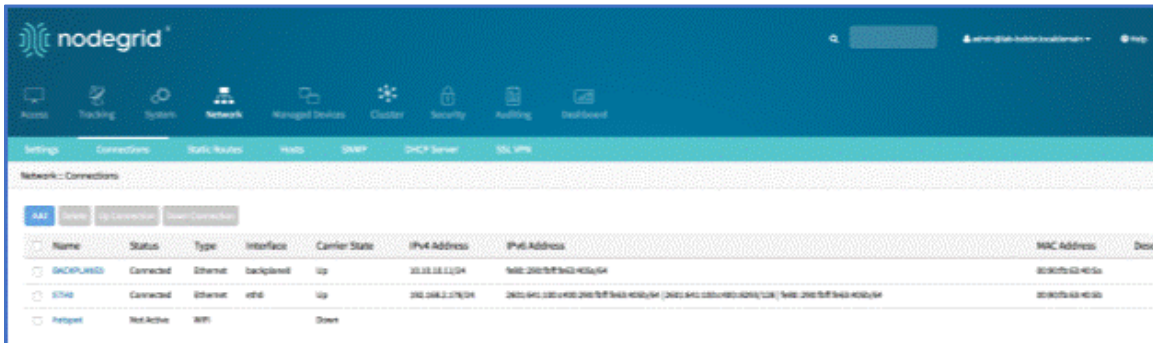
Username = **root** (SHELL access to Linux OS, but not web interface)

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 IP address(es).

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
    
```

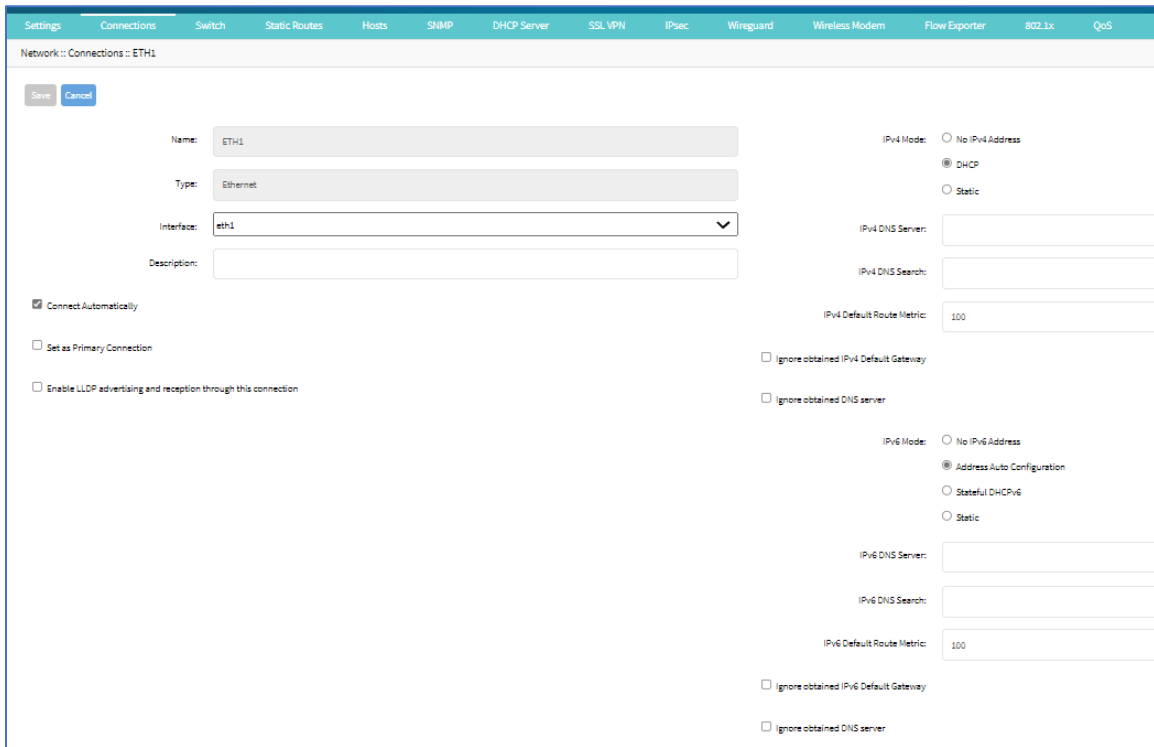
Define Static IP Address

If no DHCP server is available on your 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.
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.

General Information


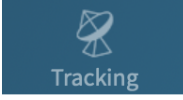
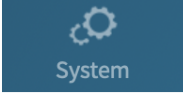

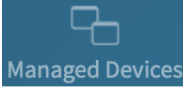


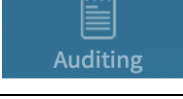
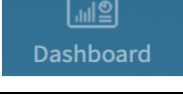
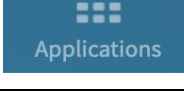
User Interfaces

WebUI View

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 Buttons

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

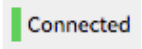

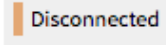
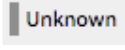
Access to Devices

This provides an overview of all available target 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

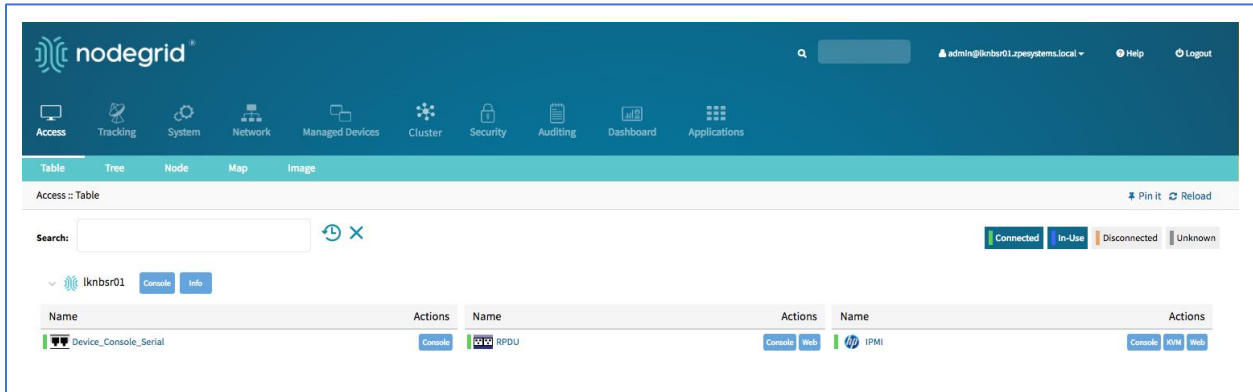
When a user logs into the WebUI, the first page is the Access section. This is overview of all available user-accessible targets. Each device current connection status and available connection types are shown.

Device Sessions

State	Indicator color	Icon	Description
Connected	Green		Nodegrid can successfully connect to the target 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 target device and it is not available for sessions
Unknown	Grey		The connection status is unknown. This is the default state for target devices with the connection mode On-Demand or for new target 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 target session and target 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.
Power Off	Performs a power off on the target device through a connected Rack PDU or IPMI device.

Options	Description
Power On	Performs a power on for the target device through a connected Rack PDU or IPMI device.
Reset	Initiates a power cycle on the target device through a connected Rack PDU or IPMI device.
Power Status	Display device's current power status (as returned by a connected Rack PDU or IPMI device).
Close Session	Closes the active session.
+	Expands or minimizes the command line options at the window's lower center.

Closing the CLI window closes the target device session.

Copy & Paste Functionality

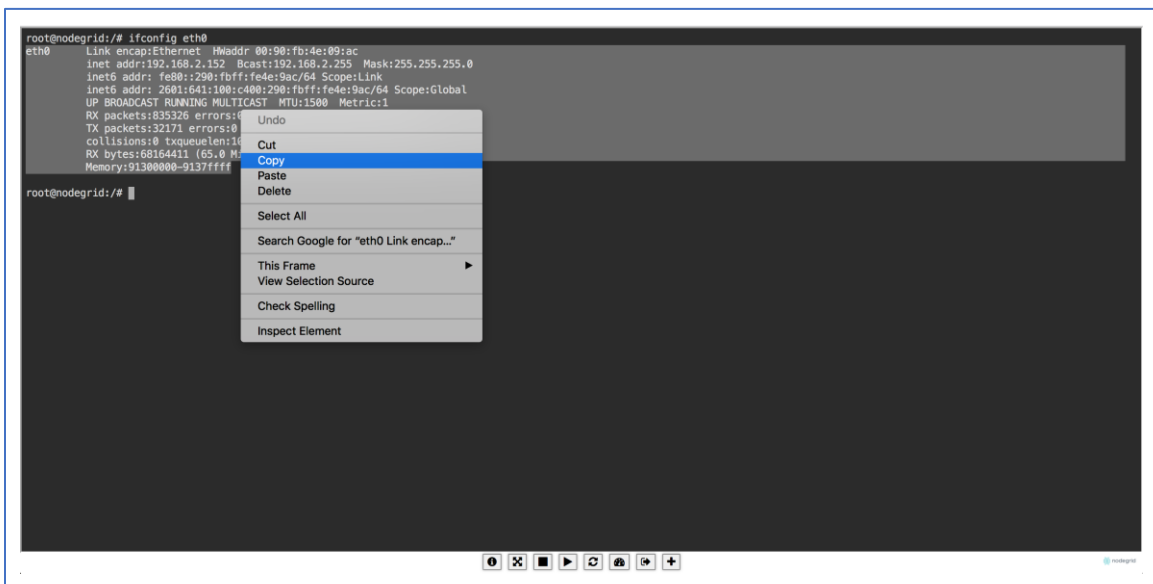
NOTE: TTYD terminal copy and paste is not currently supported within Windows and Linux.

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.
<cr>	^Ec<cr>	Send ignore/abort command signal.
k	^Eck	Serial port (speed data bits parity stop bits flow).

Option	Escape sequence	Description
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

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 Platform provides advanced search capabilities to locate and view information on target devices they require.

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

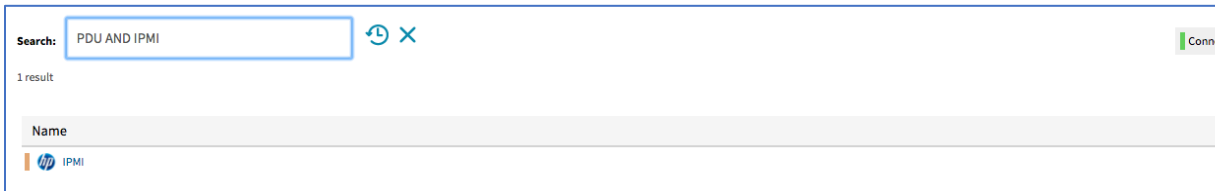
Field	Description
[search string]	A search string that represents part of or a complete string.
AND	Combines multiple search strings with an Boolean AND.
OR	Combines multiple search strings with a Boolean OR. Default search behavior for more than one search string.
NOT	Targets matching the search string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

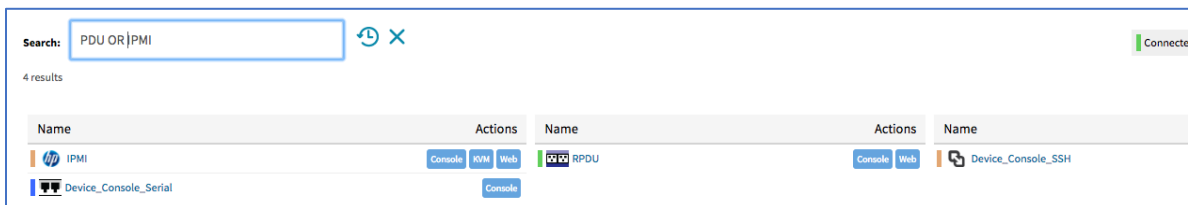


```
[admin@nodegrid search]# search "PDU AND IPMI"

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"

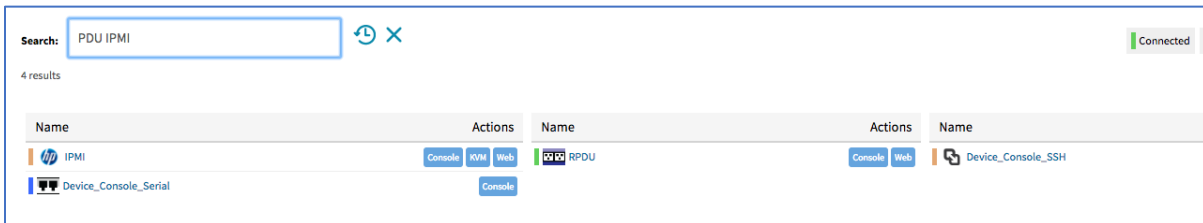


```
[admin@nodegrid access]# search "PDU OR IPMI"
```

```
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

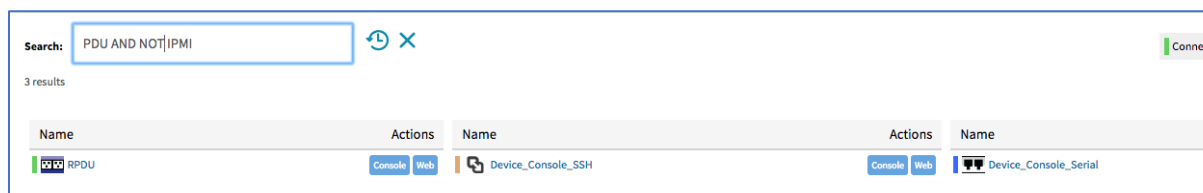
Name	Actions	Name	Actions	Name
IPMI	Console KVM Web	RPDU	Console Web	Device_Console_SSH
Device_Console_Serial	Console			

```
[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

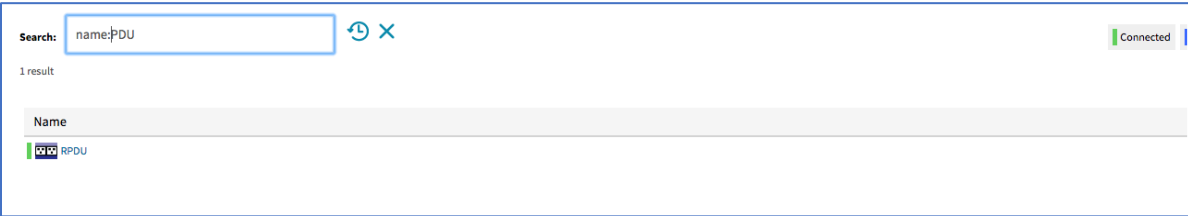
```
[admin@nodegrid search]# search "PDU AND NOT IPMI"
```

```

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 a device information stored in the system. This information is visible to users and is fully searchable in the system. These details are useful to help identify specific targets.

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 target 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**.

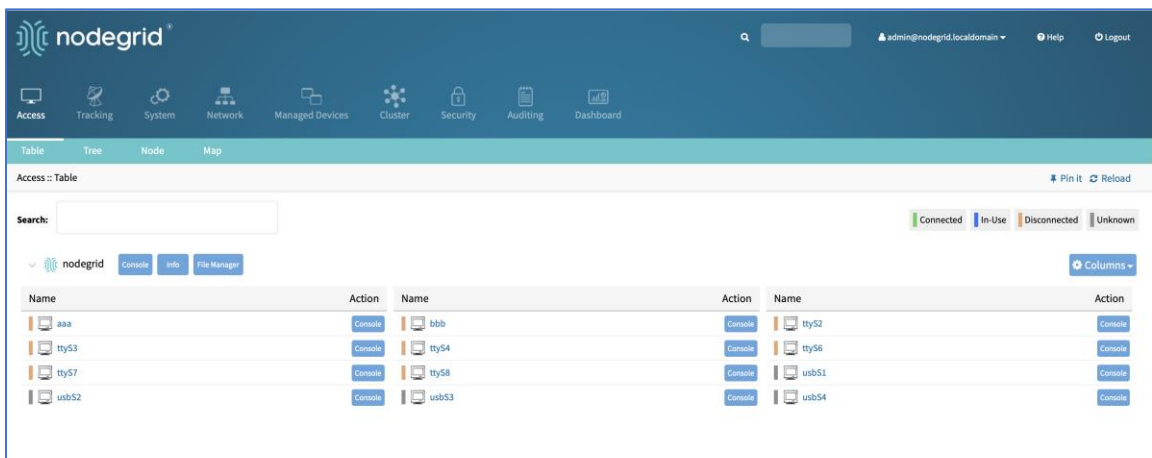
NOTE: The Table view is the only CLI view.

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.

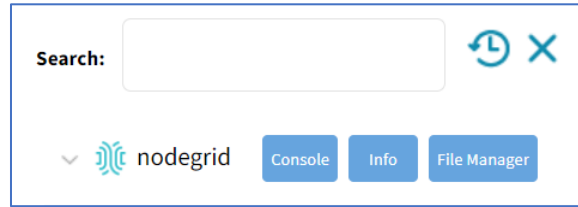
In the table, the *Action* column shows buttons to access that device. Type of button depends on device: **Console, SSH, Telnet, KVM, MKS**.



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)

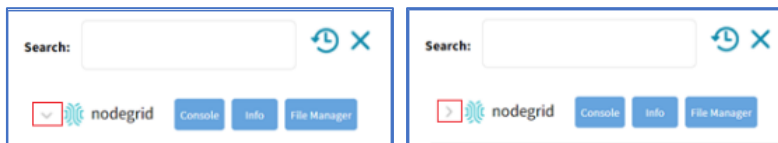
Boolean (AND, OR, NOT – caps only)

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

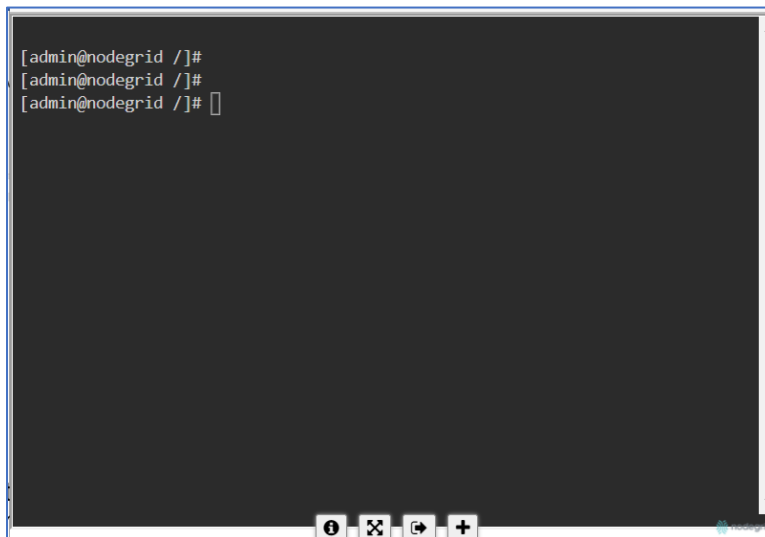
Clock icon (shows a history of past searches)

"X" (clears the search field)

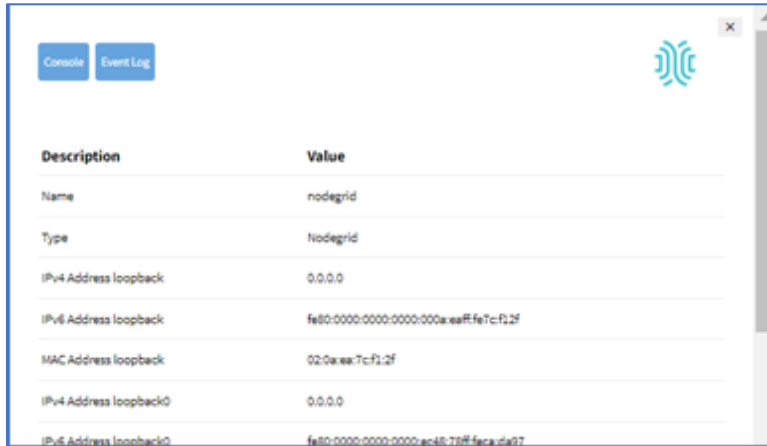
- **Arrow** (show/hide table – click down arrow to hide table, click up arrow to show table)



- **Console** (display CLI window)



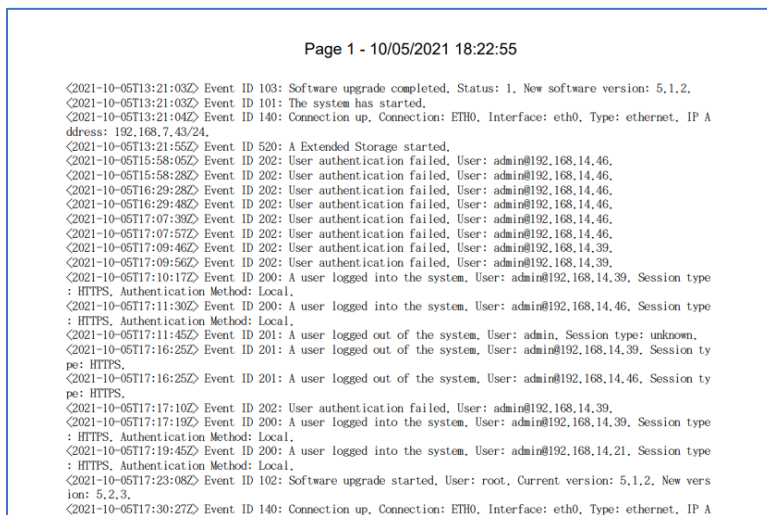
- **Info** (pop-up dialog provides device-specific details)



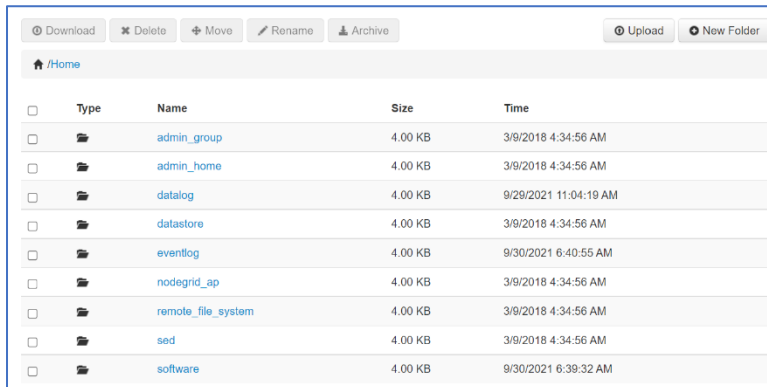
Pop-up dialog buttons:

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

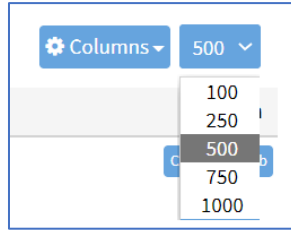
Event Log button – displays the raw log details.



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



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

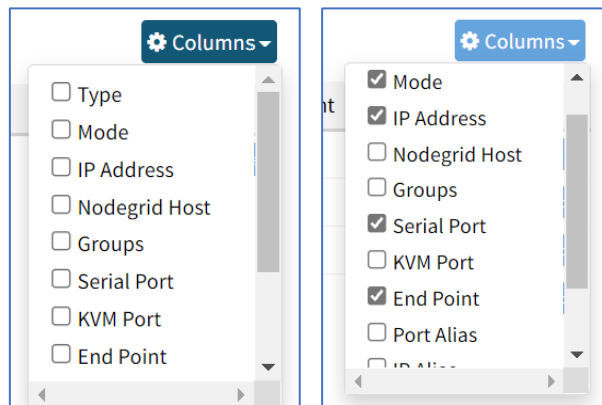


Display Table Columns

WebUI Procedure

Details on each device can be viewed by selecting columns.

4. Go to *Cluster :: Peers*.
5. On the right side, click **Columns** (displays a drop-down dialog of available table columns).

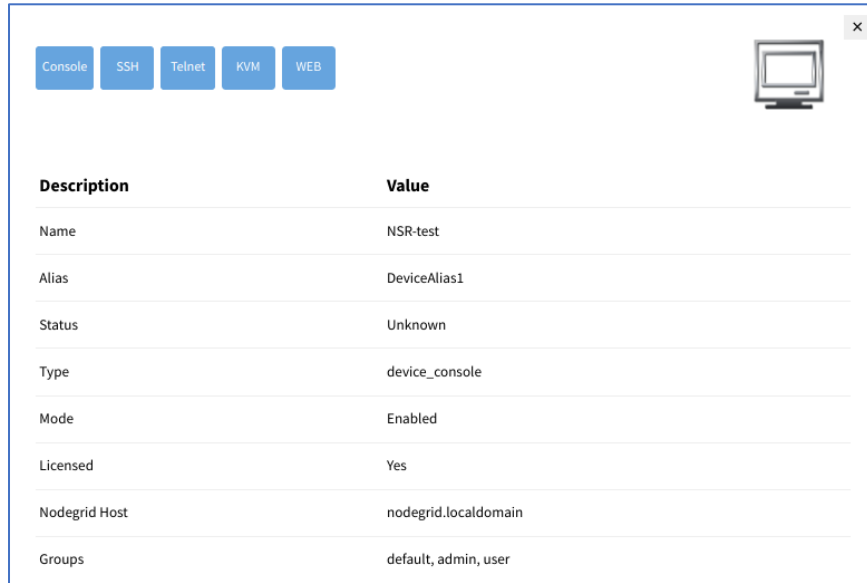


6. As columns are selected, they are displayed in the table.

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.



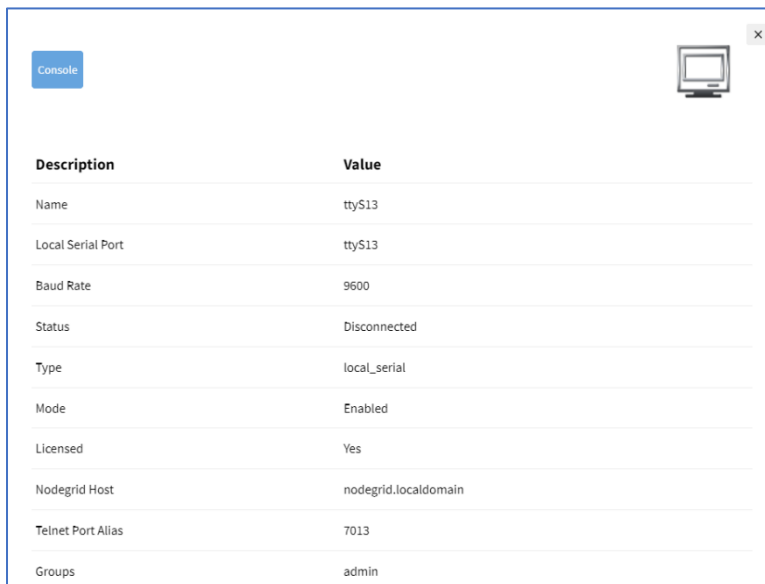
The screenshot shows a WebUI window with a title bar containing a monitor icon and a close button. Below the title bar are five tabs: Console, SSH, Telnet, KVM, and WEB. The main content area displays a table with the following data:

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

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).



The screenshot shows a WebUI window with a title bar containing a monitor icon and a close button. Below the title bar is a single tab labeled 'Console'. The main content area displays a table with the following data:

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

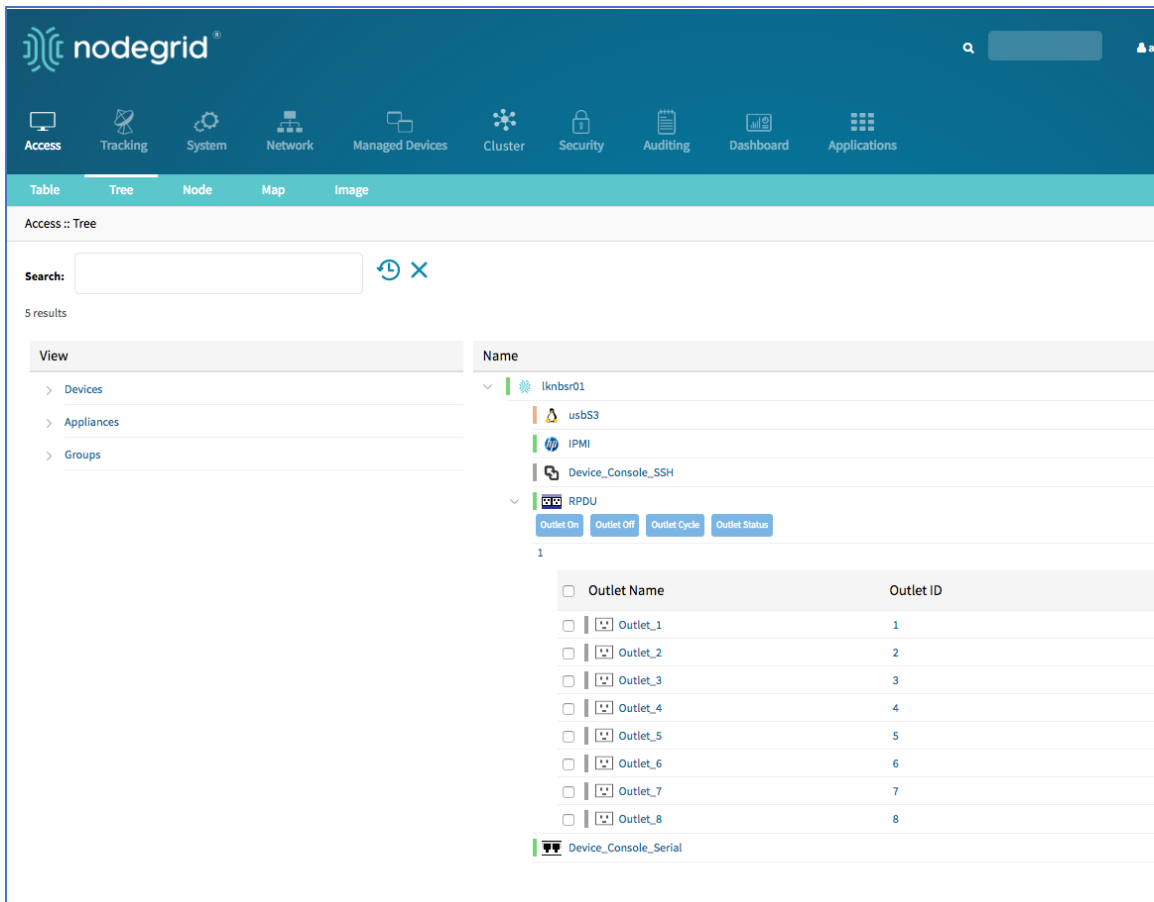
1. Go to the access folder.
2. Type the show command.

Example:


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

Tree tab

This displays the physical hierarchies of the Nodegrid setup. Start connections can be applied to each target device. Target 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. For more details, expand the *Devices*, *Appliances*, *Groups* branches.




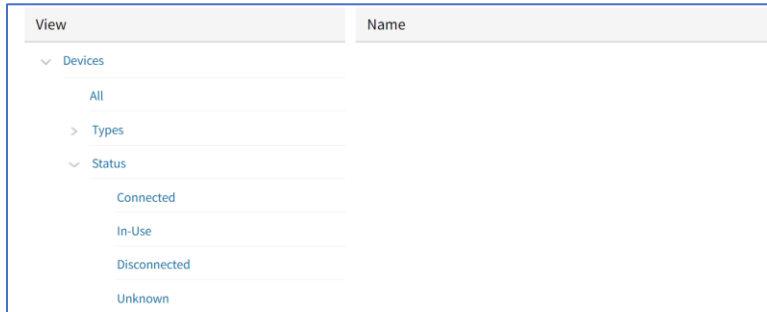
Expand View Column Branches



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

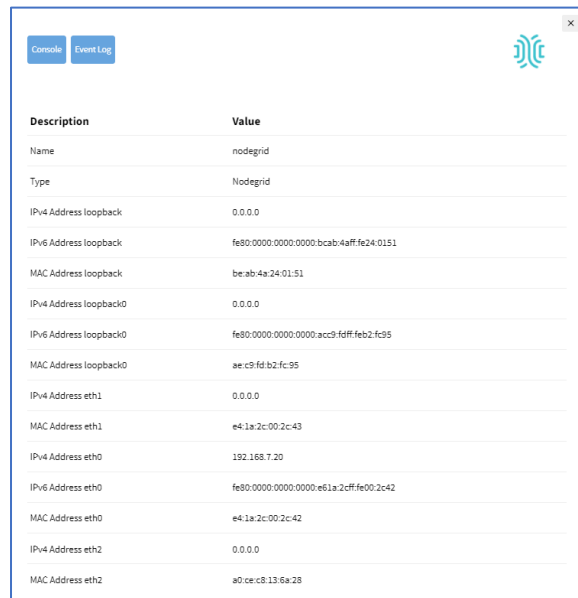
Expand Individual Tree

(For this example, Devices)

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



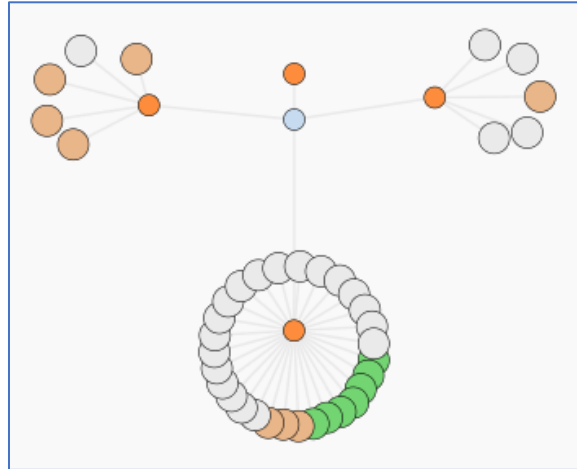
2. If further branch levels are available, click the right  icon to expand the branch.
3. To contract the branch, click the down  icon.
4. To see every item in the tree, click on **All**. Click on other items to see associated names (some clicked items may not have names).
5. Click on a name to display 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:fdff:feb2:fe95
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: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

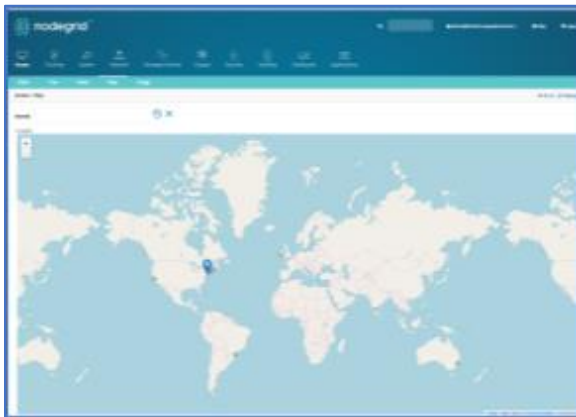
This arranges all target devices around connected Nodegrid units. It provides a complete overview of all targets and Nodegrid units in a Cluster. Click on a node to review device details and connections.



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

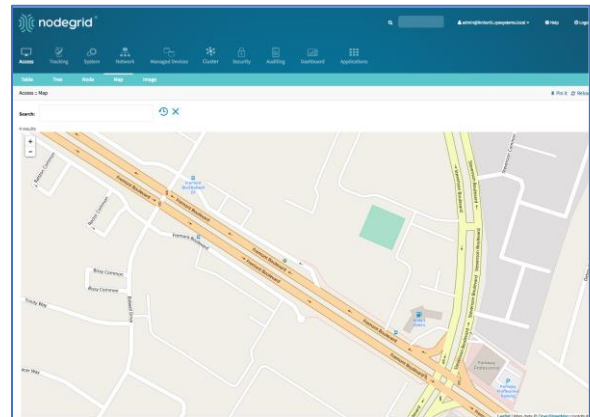


Image tab

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

This displays a custom view of Nodegrid units and target devices with associated information.

Tracking Section

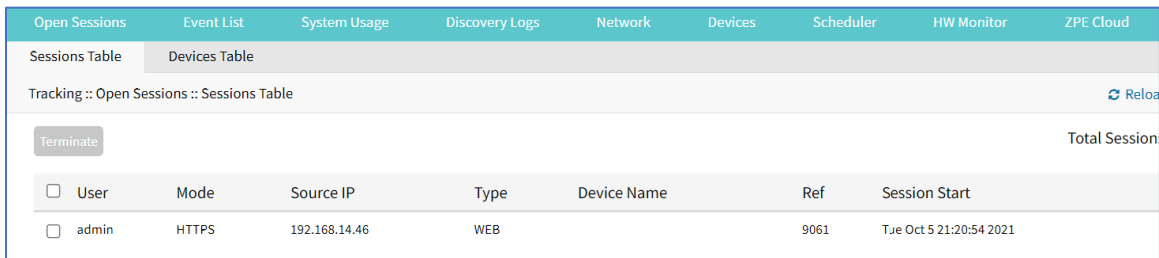
This provides information about the System and connected devices. This includes Open Sessions, Event List, Routing Table, System Usage, Discovery Logs, LLDP, and Serial Statistics.

Open Sessions tab

This provides an overview of connected users and devices sessions.

Sessions Table sub-tab

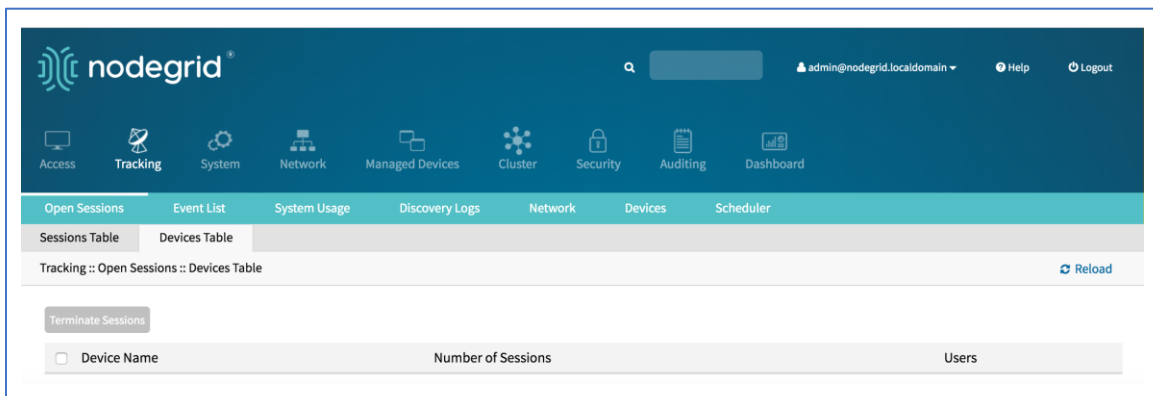
The Sessions table menu shows all users actively connected to the system, from where they are connecting from, and for how long.



Open Sessions							
Sessions Table							
Tracking :: Open Sessions :: Sessions Table							
Terminate							Total Session
<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

Devices Table sub-tab

The Device table menu shows information about active device sessions, the amount of connected session and the users which are connected.



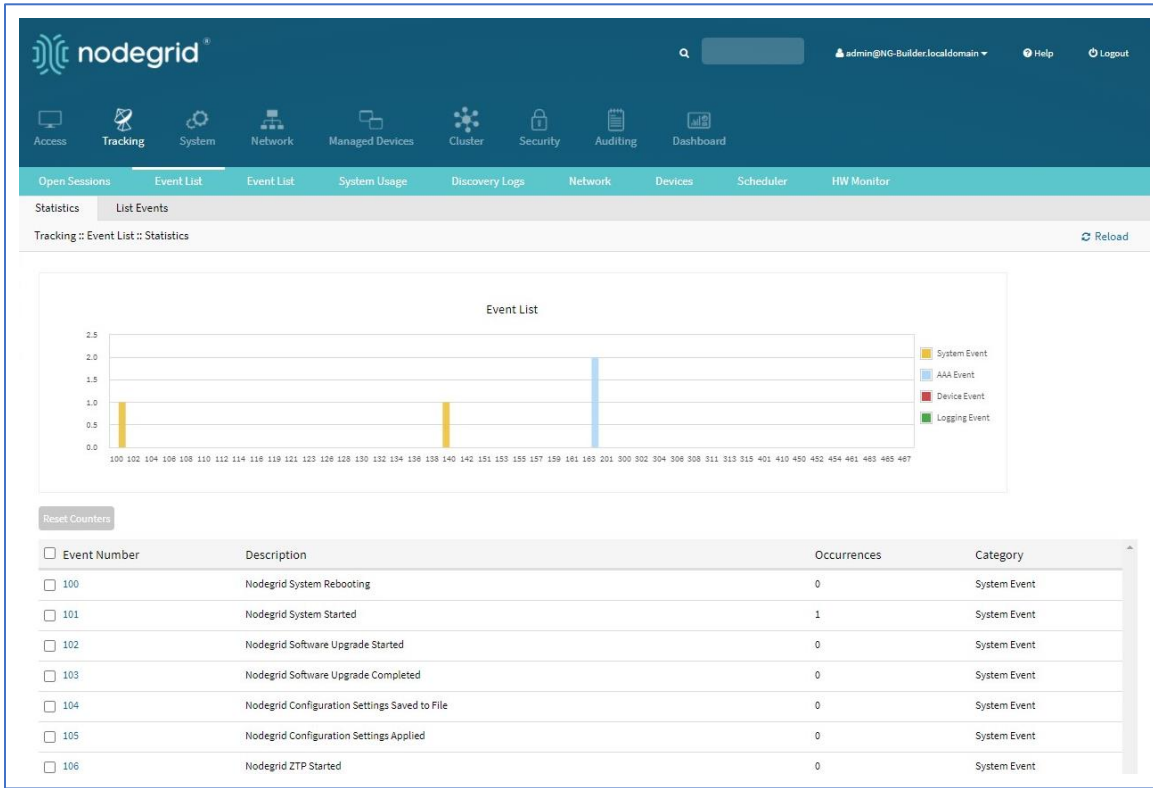
nodegrid							
Tracking :: Open Sessions :: Devices Table							
Terminate Sessions							Reload
<input type="checkbox"/>	Device Name	Number of Sessions				Users	

If a user has permission (based on an authorization group), sessions can be terminated.

Event List tab

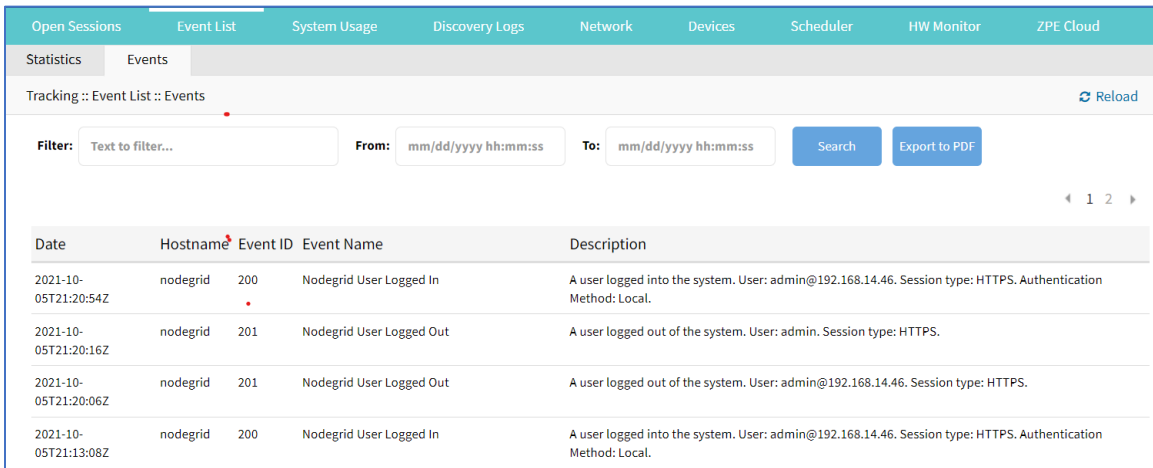
Statistics sub-tab

This provides statistical information on the system event occurrences.



Events sub-tab

This displays event details.



List Events Main Table

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

Column name	Description
Event ID	Event code.
Event Name	Name of the event.
Description	Description of the event.

Events may also be filtered by start and end date, as well as by keyword via the Filter field.

To download *Filtered Event List*, click **Export to PDF**.

NOTE: 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.

Registered Events Listing

Registered Events

Event #	Description	Occurrences	Category
100	Nodegrid System Rebooting	0	System Event
101	Nodegrid System Started	1	System Event
102	Nodegrid Software Upgrade Started	0	System Event
103	Nodegrid Software Upgrade Completed	0	System Event
104	Nodegrid Configuration Settings Saved to File	0	System Event
105	Nodegrid Configuration Settings Applied	0	System Event
106	Nodegrid ZTP Started	0	System Event
107	Nodegrid ZTP Completed	0	System Event
108	Nodegrid Configuration Changed	0	System Event
109	Nodegrid SSD Life Left	0	System Event
110	Nodegrid Local User Added to System Datastore	0	System Event
111	Nodegrid Local User Deleted from System Datastore	0	System Event
112	Nodegrid Local User Modified in System Datastore	0	System Event
113	Nodegrid ZTP execution success	0	System Event
114	Nodegrid ZTP execution failure	0	System Event

Event #	Description	Occurrences	Category
115	Nodegrid Session Terminated	0	System Event
116	Nodegrid Session Timed Out	0	System Event
118	Nodegrid Power Supply State Changed	0	System Event
119	Nodegrid Power Supply Sound Alarm Stopped by User	0	System Event
120	Nodegrid Utilization Rate Exceeded	0	System Event
121	Nodegrid Thermal Temperature ThrottleUp	0	System Event
122	Nodegrid Thermal Temperature Dropping	0	System Event
123	Nodegrid Thermal Temperature Warning	0	System Event
124	Nodegrid Thermal Temperature Critical	0	System Event
126	Nodegrid Fan Status Changed	0	System Event
127	Nodegrid Fan Sound Alarm Stopped by User	0	System Event
128	Nodegrid Total number of local serial ports mismatch	0	System Event
129	Nodegrid dry contact change state	0	System Event
130	Nodegrid License Added	0	System Event
131	Nodegrid License Removed	0	System Event
132	Nodegrid License Conflict	0	System Event
133	Nodegrid License Scarce	0	System Event
134	Nodegrid License Expiring	0	System Event
135	Nodegrid Shell Started	0	System Event
136	Nodegrid Shell Stopped	0	System Event
137	Nodegrid Sudo Executed	0	System Event
138	Nodegrid SMS Executed	0	System Event
139	Nodegrid SMS Invalid	0	System Event
140	Nodegrid Connection Up	2	System Event

Event #	Description	Occurrences	Category
141	Nodegrid Connection Down	0	System Event
142	Nodegrid SIM Card Swap	0	System Event
150	Nodegrid Cluster Peer Online	0	System Event
151	Nodegrid Cluster Peer Offline	0	System Event
152	Nodegrid Cluster Peer Signed On	0	System Event
153	Nodegrid Cluster Peer Signed Off	0	System Event
154	Nodegrid Cluster Peer Removed	0	System Event
155	Nodegrid Cluster Peer Became Coordinator	0	System Event
156	Nodegrid Cluster Coordinator Became Peer	0	System Event
157	Nodegrid Cluster Coordinator Deleted	0	System Event
158	Nodegrid Cluster Coordinator Created	0	System Event
159	Nodegrid Cluster Peer Configured	0	System Event
160	Nodegrid Search Unavailable	0	System Event
161	Nodegrid Search Restored	0	System Event
200	Nodegrid User Logged In	3	AAA Event
201	Nodegrid User Logged Out	1	AAA Event
202	Nodegrid System Authentication Failure	4	AAA Event
300	Nodegrid Device Session Started	0	Device Event
301	Nodegrid Device Session Stopped	0	Device Event
302	Nodegrid Device Created	0	Device Event
303	Nodegrid Device Deleted	0	Device Event
304	Nodegrid Device Renamed	0	Device Event
305	Nodegrid Device Cloned	0	Device Event
306	Nodegrid Device Up	0	Device Event
307	Nodegrid Device Down	0	Device Event

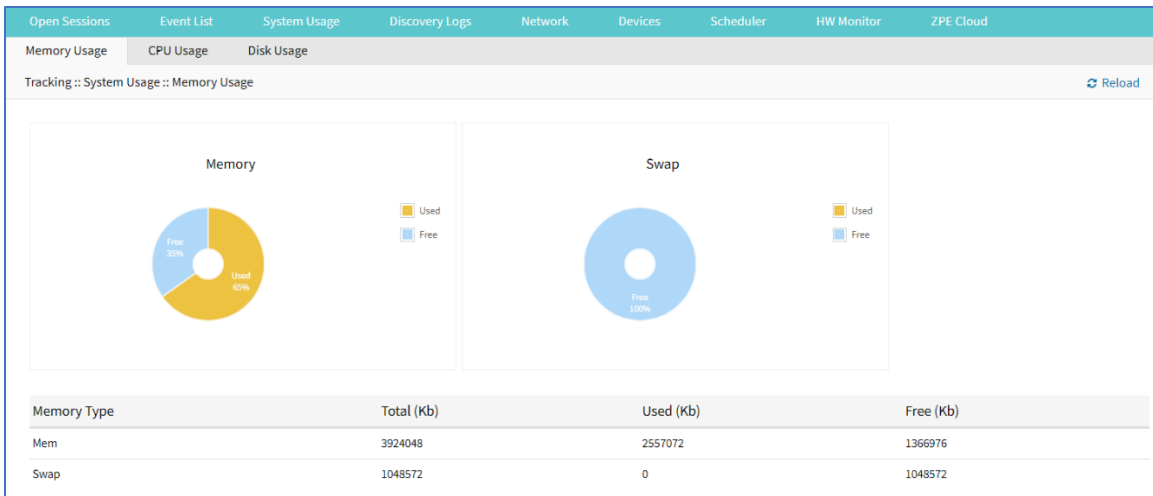
Event #	Description	Occurrences	Category
308	Nodegrid Device Session Terminated	0	Device Event
310	Nodegrid Power On Command Executed on a Device	0	Device Event
311	Nodegrid Power Off Command Executed on a Device	0	Device Event
312	Nodegrid Power Cycle Command Executed on a Device	0	Device Event
313	Nodegrid Suspend Command Executed on a Device	0	Device Event
314	Nodegrid Reset Command Executed on a Device	0	Device Event
315	Nodegrid Shutdown Command Executed on a Device	0	Device Event
400	Nodegrid System Alert Detected	0	Logging Event
401	Nodegrid Alert String Detected on a Device Session	0	Logging Event
402	Nodegrid Event Log String Detected on a Device Event Log	0	Logging Event
410	Nodegrid System NFS Failure	0	Logging Event
411	Nodegrid System NFS Recovered	0	Logging Event
450	Nodegrid Datapoint State High Critical	0	Logging Event
451	Nodegrid Datapoint State High Warning	0	Logging Event
452	Nodegrid Datapoint State Normal	0	Logging Event
453	Nodegrid Datapoint State Low Warning	0	Logging Event
454	Nodegrid Datapoint State Low Critical	0	Logging Event
460	Nodegrid Door Unlocked	0	Logging Event
461	Nodegrid Door Locked	0	Logging Event
462	Nodegrid Door Open	0	Logging Event
463	Nodegrid Door Close	0	Logging Event
464	Nodegrid Door Access Denied	0	Logging Event
465	Nodegrid Door Alarm Active	0	Logging Event
466	Nodegrid Door Alarm Inactive	0	Logging Event

Event #	Description	Occurrences	Category
467	Nodegrid PoE Power Fault	0	Logging Event
468	Nodegrid PoE Power Budget Exceeded	0	Logging Event

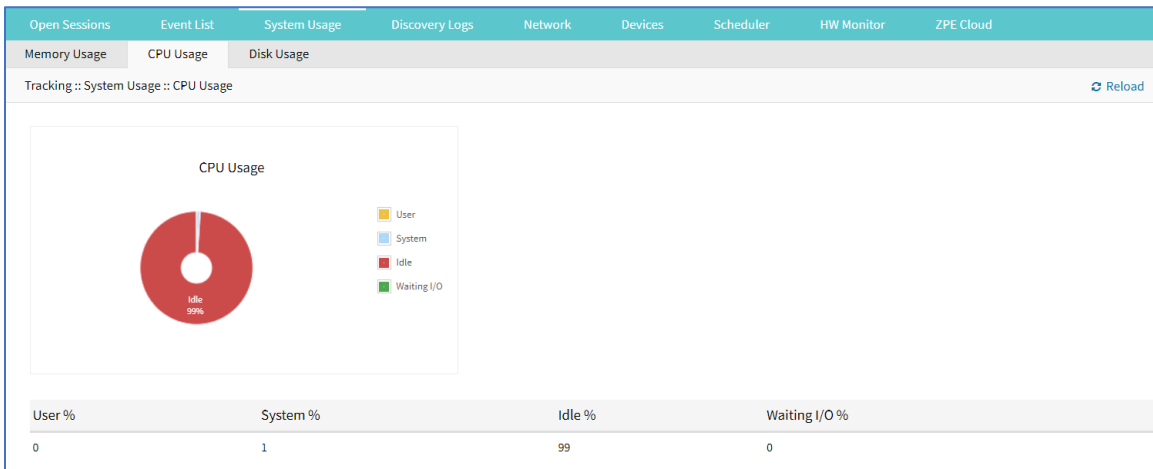
System Usage tab

This presents information usage details.

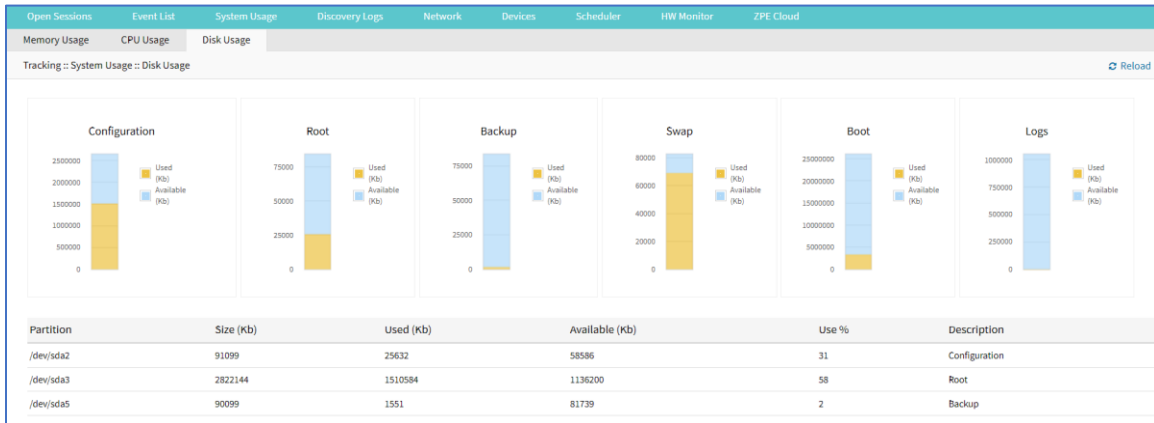
Memory Usage sub-tab



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.

Date	IP Address	Device Name	Discovery Method	Action
Fri Aug 16 16:19:47 2019	N/A	usbS0-2	KVM USB	Device Connected
Fri Aug 16 16:19:47 2019	N/A	usbS3-16	KVM USB	Device Connected
Fri Aug 16 16:19:47 2019	N/A	usbS0-1	SENSOR USB	Device Connected
Fri Aug 16 16:19:48 2019	N/A	usbS1-1	Serial USB	Device Connected
Fri Aug 16 16:19:48 2019	N/A	usbS0-3	Serial USB	Device Connected
Fri Aug 16 16:19:48 2019	N/A	usbS1-13	Serial USB	Device Connected

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.

Reset Logs

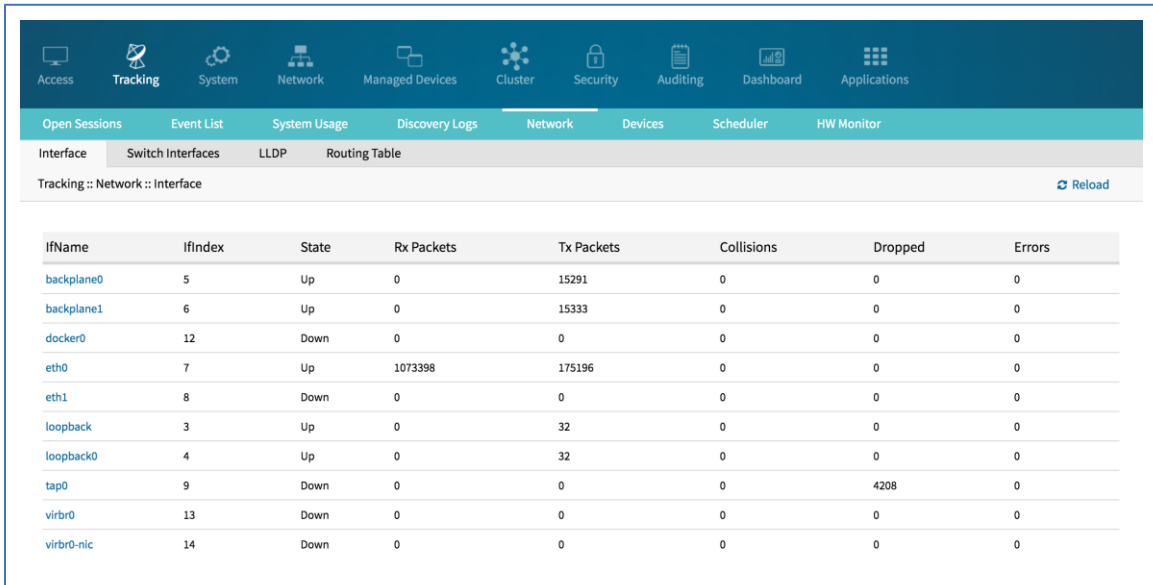
WebUI Procedure

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

The table will clear.

Network tab

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



IfName	IfIndex	State	Rx Packets	Tx Packets	Collisions	Dropped	Errors
backplane0	5	Up	0	15291	0	0	0
backplane1	6	Up	0	15333	0	0	0
docker0	12	Down	0	0	0	0	0
eth0	7	Up	1073398	175196	0	0	0
eth1	8	Down	0	0	0	0	0
loopback	3	Up	0	32	0	0	0
loopback0	4	Up	0	32	0	0	0
tap0	9	Down	0	0	0	4208	0
virbr0	13	Down	0	0	0	0	0
virbr0-nic	14	Down	0	0	0	0	0

Interface sub-tab

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

Switch Interface sub-tab

This shows switch interfaces.

LLDP sub-tab

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

Routing Table sub-tab

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

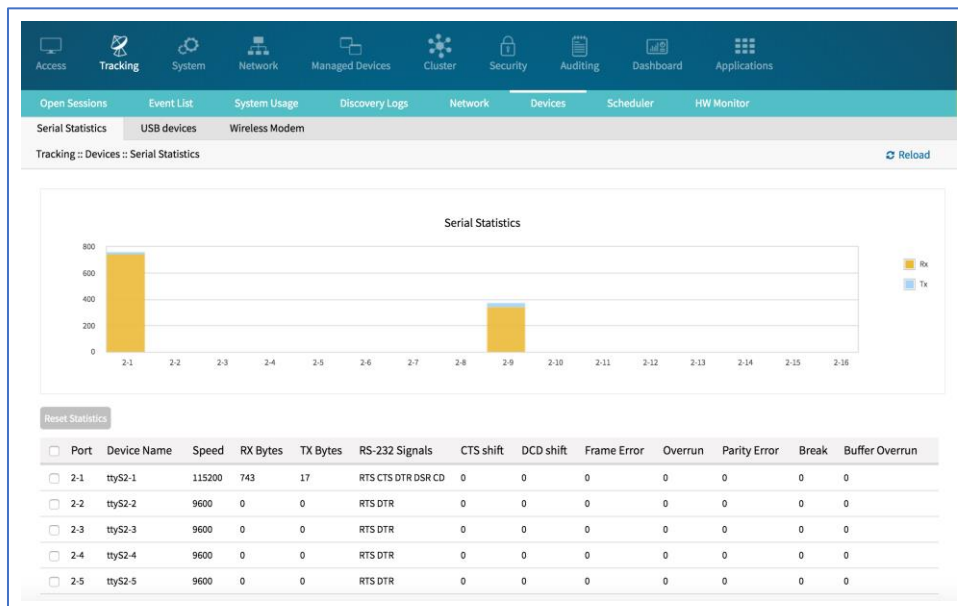
Destination	Gateway	Metric	Interface	From	Table
0.0.0.0/0	192.168.2.202	0	eth0	192.168.2.146	eth0
0.0.0.0/0	192.168.2.202	90	eth0	all	main
172.17.0.0/16	-	0	docker0	all	main
192.168.122.0/24	-	0	virbr0	all	main
192.168.2.0/24	-	0	eth0	192.168.2.146	eth0
192.168.2.0/24	-	90	eth0	192.168.2.146	eth0
192.168.2.0/24	-	90	eth0	all	main
2601:641:100:c400::/64	-	1024	eth0	2601:641:100:c400:290:fbff:fe60:2cc0	eth0
2601:641:100:c400::/64	-	90	eth0	2601:641:100:c400:290:fbff:fe60:2cc0	eth0
2601:641:100:c400::/64	-	90	eth0	all	main
::/0	fe80::225:90ff:fe23:c0b4	1024	eth0	2601:641:100:c400:290:fbff:fe60:2cc0	eth0
::/0	fe80::225:90ff:fe23:c0b4	90	eth0	all	main
fe80::/64	-	256	eth0	2601:641:100:c400:290:fbff:fe60:2cc0	eth0
fe80::/64	-	256	eth0	all	main
fe80::/64	-	256	loopback	all	main

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, etc.



USB Devices sub-tab

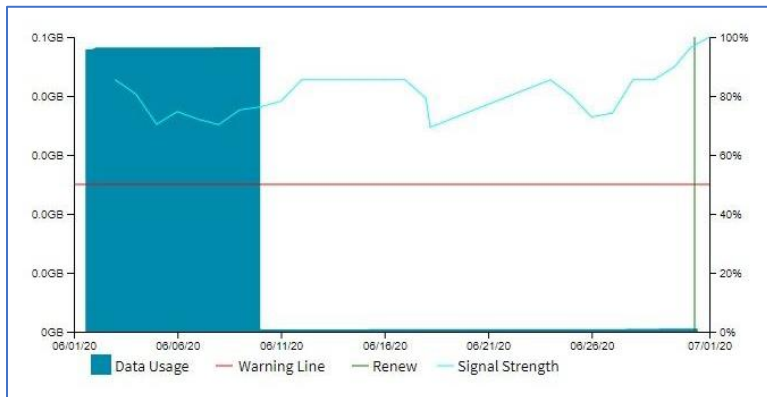
This provides details about connected USB devices and initialized drivers.

USB Port	USB Path	USB ID	Detected Type	Kernel Device	Description
S3-16	10-4	2f47:2285	KVM Device	usb53-16	KVM Adapter
S1-1	11-1	067b:2303	Serial Device	usb51-1	USB-Serial Controller D
S1-13	17-1	0403:6001	Serial Device	usb51-13	FT232R USB UART
0-2	1-1	2f47:2285	KVM Device	usb50-2	KVM Adapter
0-3	1-2	0403:6001	Serial Device	usb50-3	FT232R USB UART
0-1	1-3	289b:0503	Sensor Device	usb50-1	TRH320

Wireless Modem sub-tab

This displays information about slot, SIM status, and signal strength.

If Data Usage Monitoring is enabled, mobile data usage statistics for each SIM can be viewed, on the graphs.



To manually reset Usage statistics, click **Reset**.

Scheduler tab

This provides information about scheduled tasks.

HW Monitor tab

This displays Nodegrid system information. Three sub-tabs provide critical system information.

Thermal sub-tab

Name	Value	Unit	Description
CPU Temperature	57	Celsius	CPU temperature
System Temperature	52	Celsius	System temperature
CPU Fan	0	RPM	CPU FAN speed
System Fan 1	7187	RPM	System FAN 1 speed
System Fan 2	7187	RPM	System FAN 2 speed
Switch Fan	0	RPM	Switch FAN speed

Details displayed:

- CPU Temperature (C)
- System Temperature (C)
- CPU Fan (RPM)
- System Fan 1 (RMP)
- System Fan 2 (RPM)
- Switch Fan (RPM)

Power sub-tab

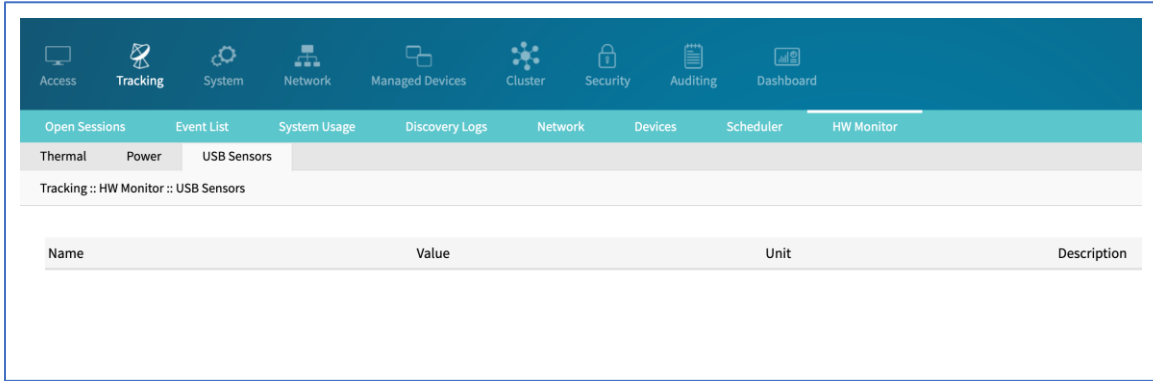
Name	Value	Unit	Description
PS1	ON	NA	Power Supply 1 State
PS2	OFF	NA	Power Supply 2 State

Details displayed:

- PS1
- PS2

USB Sensors (or I/O Ports) sub-tab

The details shown depend on the model.



Additional USB sensors (or I/O ports in use) are displayed here.

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

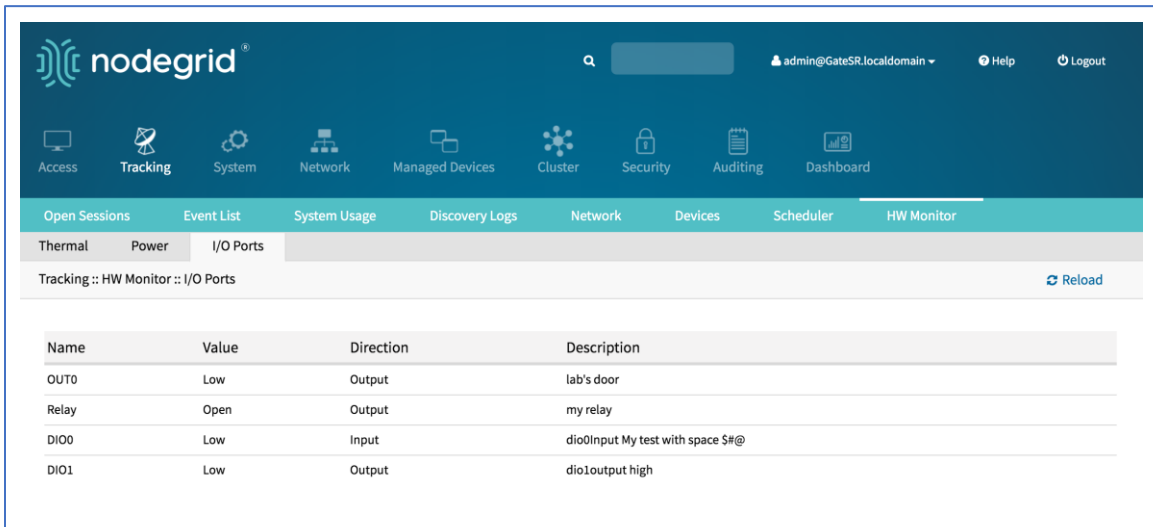
Power menu displays information about current Power sources (current state and power consumption).

I/O Ports menu is only available on devices with GPIO ports, like the Nodegrid Gate SR and Nodegrid Link SR. It will show the current status of GPIO ports.

I/O Ports (GPIO) sub-tab

This shows the status of GPIO ports (only displayed for models with GPIO ports, i.e., Nodegrid Gate SR and Nodegrid Link SR).

Example shown – Nodegrid Gate SR



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.

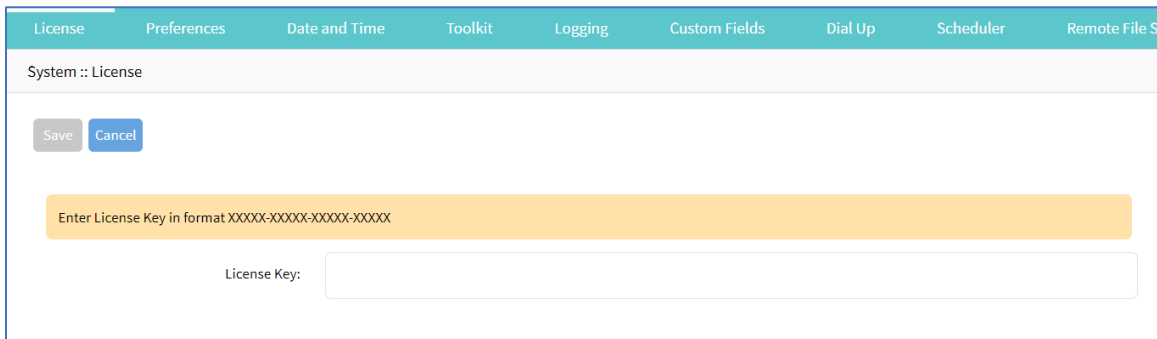
NOTE: A managed device is any physical or virtual device defined under Nodegrid for access and control.

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

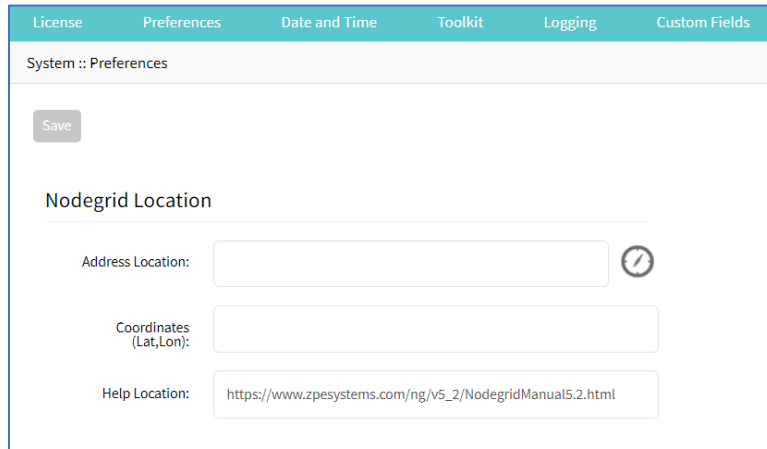
WebUI Procedure

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.

Nodegrid Location



The screenshot shows the 'System :: Preferences' page with a teal header containing tabs for License, Preferences, Date and Time, Toolkit, Logging, and Custom Fields. The 'Nodegrid Location' section includes a 'Save' button, an 'Address Location' input field with a compass icon, a 'Coordinates (Lat,Lon):' input field, and a 'Help Location' input field containing the URL 'https://www.zpesystems.com/ng/v5_2/NodegridManual5.2.html'.

Edit Location Preferences

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).

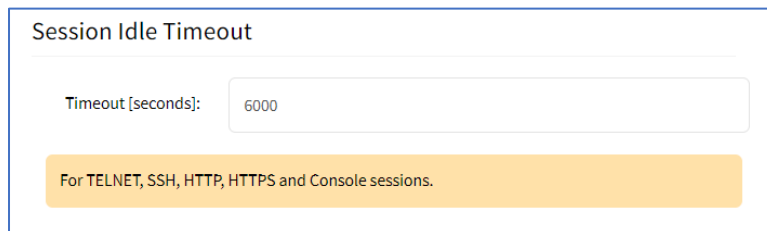
For **Help Location**, enter alternate URL location for the User Guide.

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

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

Session Idle Timeout

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



The screenshot shows the 'Session Idle Timeout' configuration page with a text input field for 'Timeout [seconds]' containing the value '6000'. Below the input field is a yellow callout box with the text 'For TELNET, SSH, HTTP, HTTPS and Console sessions.'

Change Timeout

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.

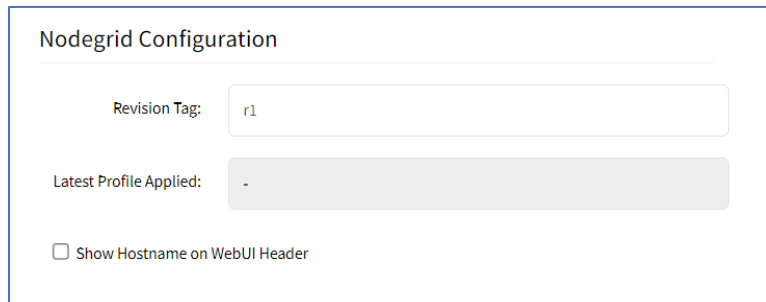
Value (i.e., 6000 keeps session active for 100 minutes).

- Click **Save**.

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** shows the last applied profile (through a ZTP process or the ZPE Cloud).



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

- Revision Tag:** A text input field containing the value 'r1'.
- Latest Profile Applied:** A dropdown menu showing a hyphen '-' as the selected option.
- Show Hostname on WebUI Header:** An unchecked checkbox.

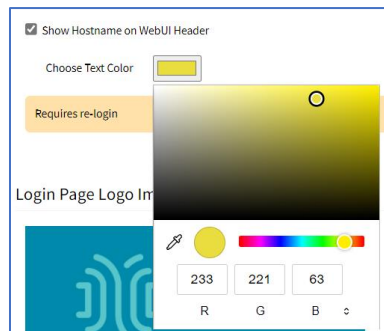
Modify Nodegrid Configuration

WebUI Procedure

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

Enter **Revision Tag**.

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



The screenshot shows a color selection interface with the following elements:

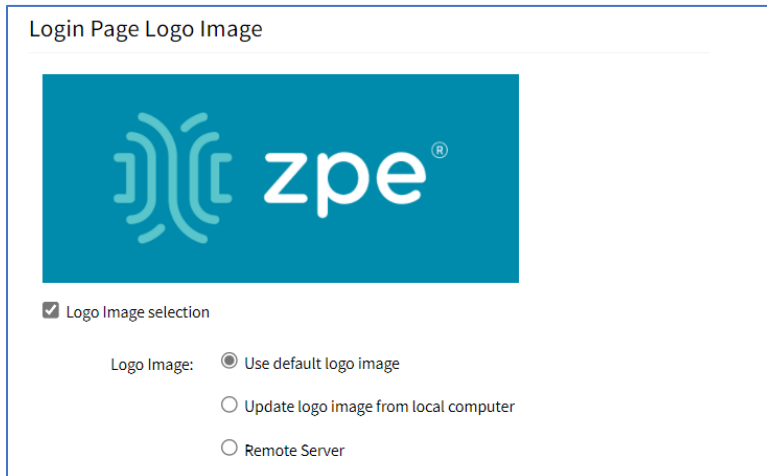
- Show Hostname on WebUI Header:** A checked checkbox.
- Choose Text Color:** A color selection area showing a yellow color swatch.
- Requires re-login:** A yellow banner indicating that the user must log in again.
- Login Page Logo Im:** A partially visible label for the logo image.
- Color Grid:** A large color grid with a yellow circle indicating the selected color.
- Color Picker:** A color picker tool with a brush icon and a color spectrum.
- RGB Values:** Input fields for Red (233), Green (221), and Blue (63).

- Click **Save**.

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>.

After upload, refresh the browser cache to display the new image.



Update Logo Image Selection

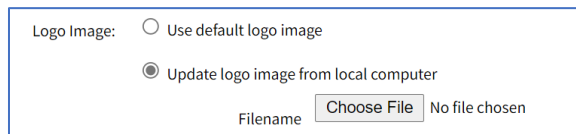
WebUI Procedure

4. Go to *System :: Preferences*.
5. In the *Logo Page Logo Image* menu:
6. (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.

Logo Image: Use default logo image

Update logo image from local computer

Remote Server

URL:

Username:

Password:

The path in url to be used as absolute path name

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.

Login Banner Message

Enable Banner Message

Banner

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

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

Change Message to appear on Login Page

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

WebUI Procedure

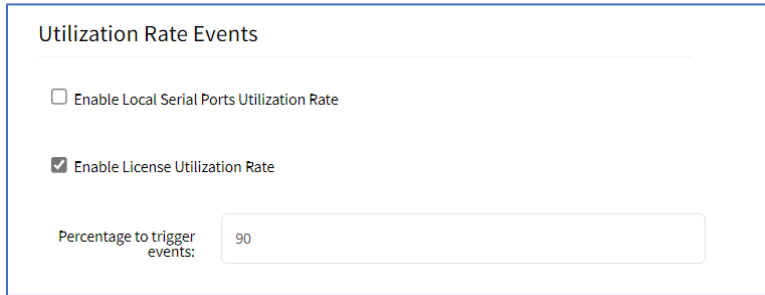
1. Go to *System :: Preferences*.
2. In the *Login Banner Message* menu:
 - Click in **Banner**.

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

3. Click **Save**.

Utilization Rate Events

This sets up event notifications for utilization rates.



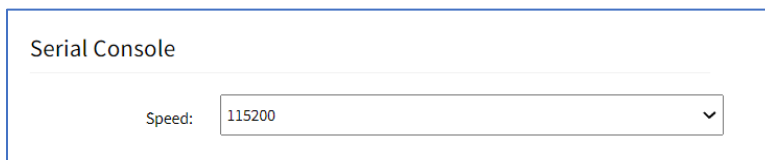
Set Utilization Rate

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**.

Serial Console

This displays the baud speed of the device.



Set Serial Console Speed

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**.

Power Supplies

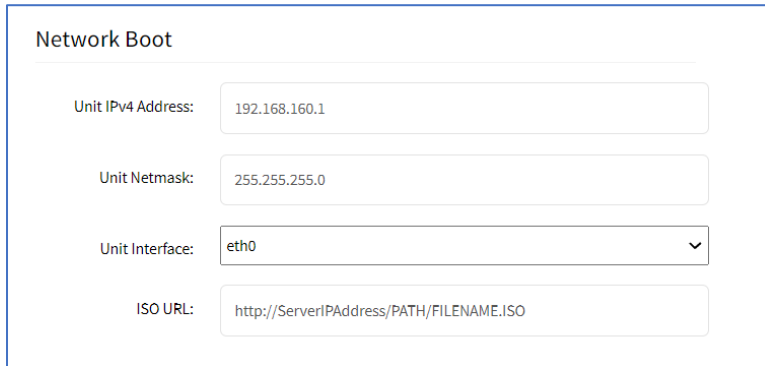
This displays the state of dual power supplies (ON/OFF).

To get an alarm when one power supply goes down, select **Enable alarm sound** checkbox.

To acknowledge an alarm state, click **Acknowledge Alarm State** (top left).

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>



The screenshot shows a web form titled "Network Boot" with the following fields and values:

- Unit IPv4 Address: 192.168.160.1
- Unit Netmask: 255.255.255.0
- Unit Interface: eth0 (selected from a dropdown menu)
- ISO URL: http://ServerIPAddress/PATH/FILENAME.ISO

Set Network Boot

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**.

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 5.0.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 5.0.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-5.0.1.xx
root@ubuntu-srv1:/var/lib/tftpboot# ls -l nodegrid-5.0.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. 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.

```
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 bootfile-name "nodegrid-5.0.xx/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;
}
```

5. 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-5.0.xx/ nodegrid-5.0.xx
```

6. Restart the DHCP server.

```
sudo service isc-dhcp-server restart
```


7. Restart tftpd-hpa process.
8. Start the Nodegrid device. This installs the Nodegrid netboot image on device.

Date and Time tab

Nodegrid devices supports NTP (Network Time Protocol) Authentication and Cellular Tower Synchronization. This default configuration is set to automatically retrieve 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).

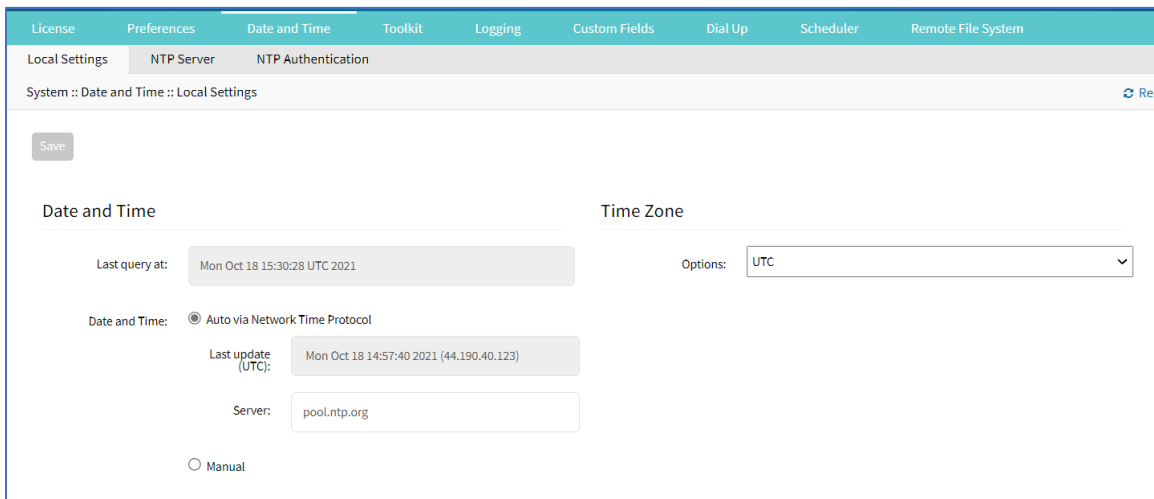
NOTE: All timestamps in Event Logs are in UTC.

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*.



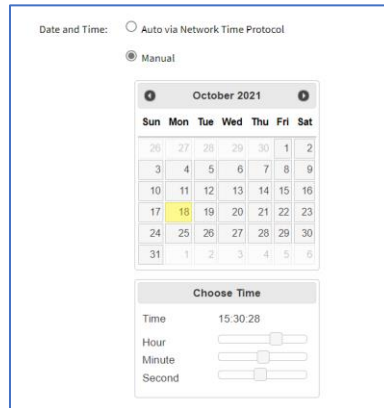
2. In *Date and Time* menu:

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.

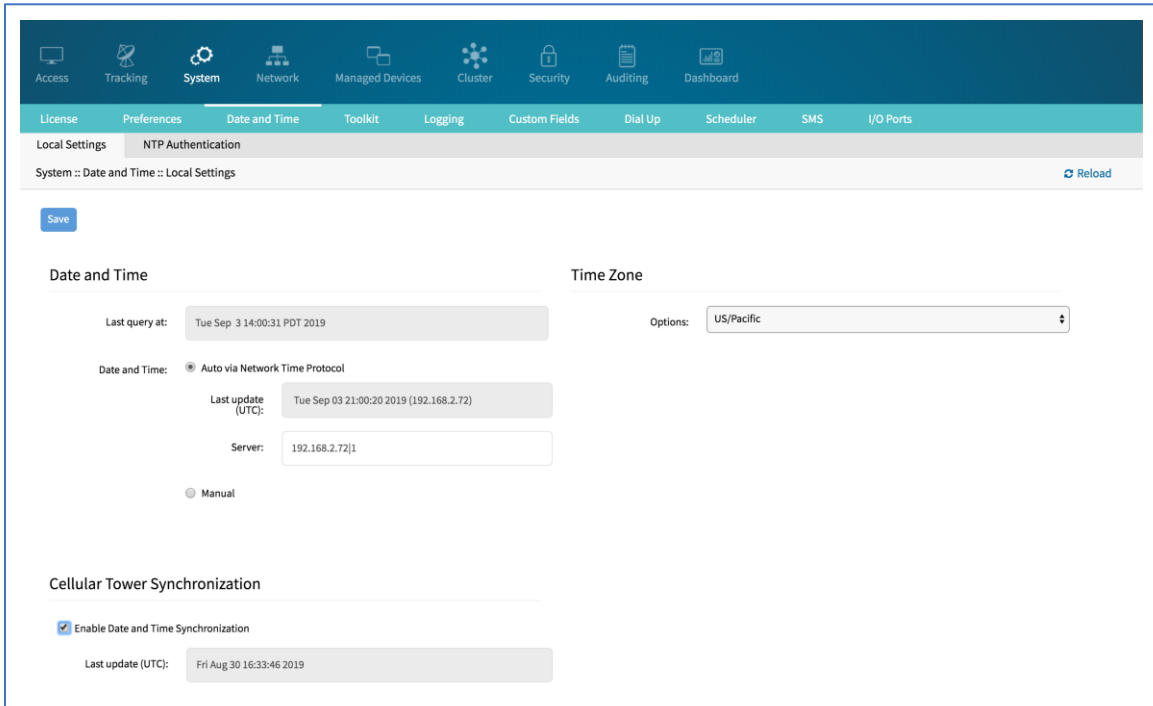
4. Click **Save**.

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.

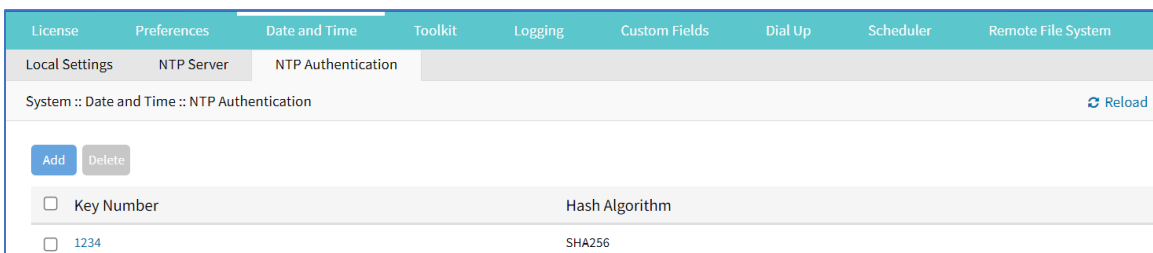
3. Make other changes, as needed.

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 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.

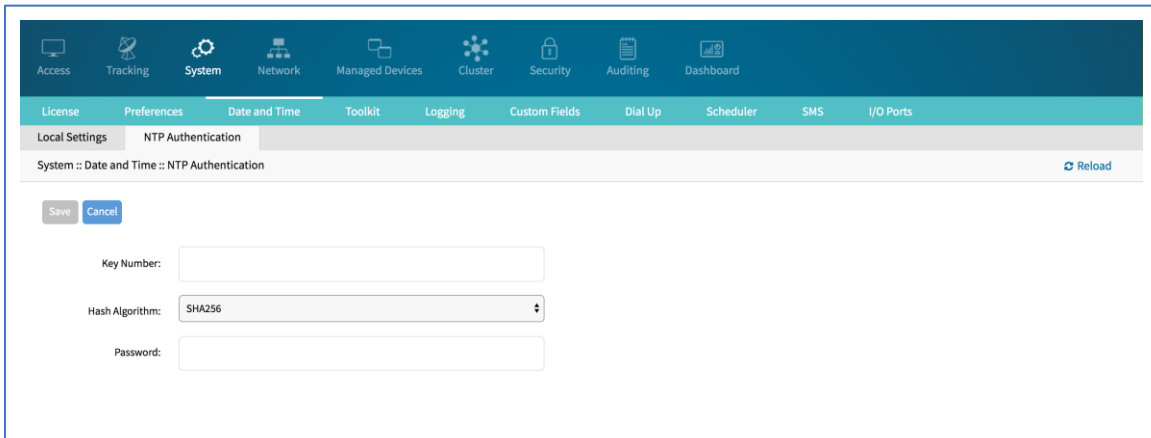


Configure Key Number Set

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#####**.
6. Click **Save**.

Delete Key Number

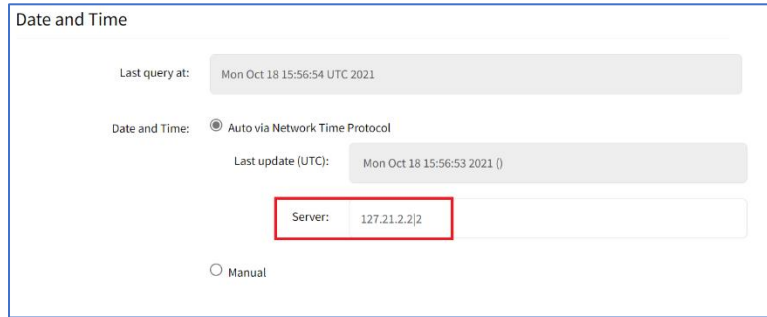
WebUI Procedure

1. Go to *System :: Date and Time :: NTP Authentication*.
2. Select checkbox next to Key Number to be deleted.
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.

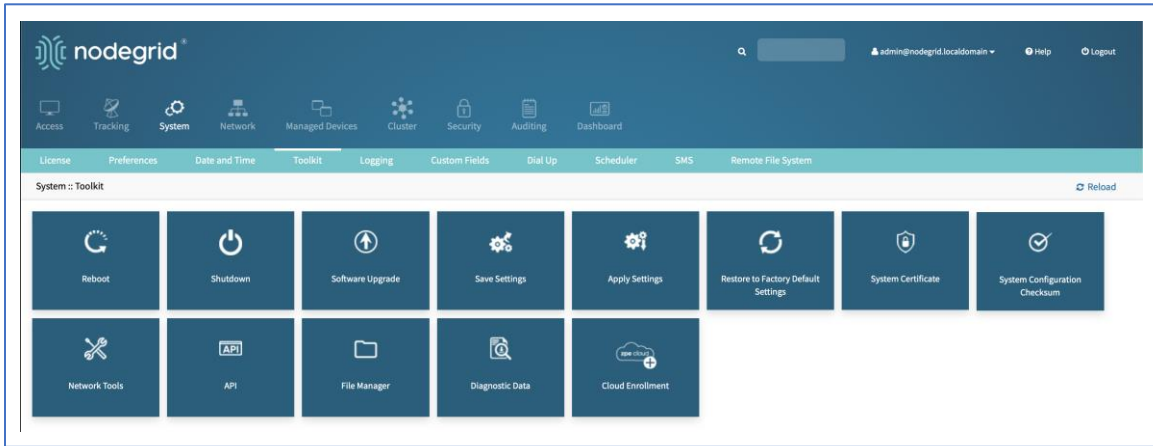


3. Make other changes, as needed.
4. Click **Save**.

Toolkit tab

System maintenance features are available in System::Toolkit page. This toolkit is used to run the following:

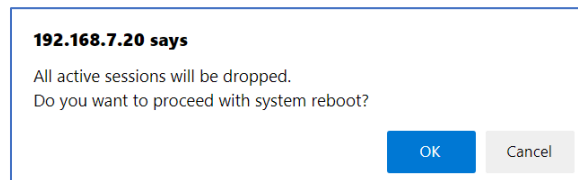
- Reboot
- Shutdown
- Software upgrade
- Save Settings
- Apply Settings
- Restore to Factory Default Settings
- System Certificate
- System Configuration Checksum
- Network tools
- API
- File Manager (only accessible with Admin privileges)
- Diagnostic Data
- Cloud Enrollment



Reboot

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.

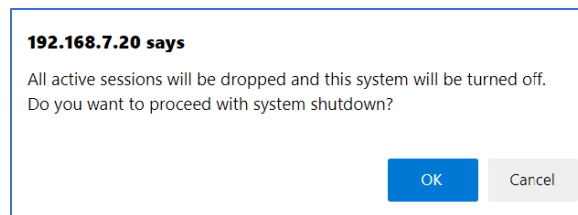
On click, displays pop-up dialog. Click **OK** to continue.



Shutdown

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

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 [].)

Example:

```
ftp://<your-ftp-server>/downloads/Nodegrid_v5.0.1.iso
```

If downgrading, the options are:

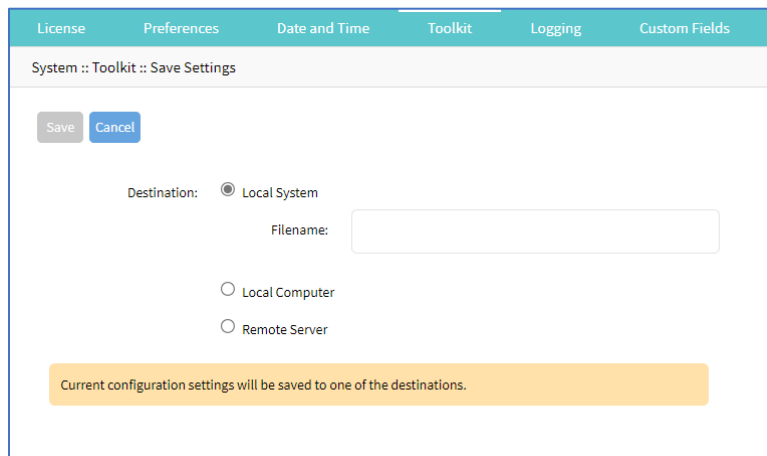
- Apply factory default configuration.
- Restore a saved configuration.

Save Settings

This saves current configuration.

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.

Destination: Local System
 Local Computer
 Remote Server

URL:

Username:

Password:

The path in url to be used as absolute path name

4. Click **Save**.

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

Apply Settings

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.

License
Preferences
Date and Time
Toolkit
Logging
Custom

System :: Toolkit :: Apply Settings

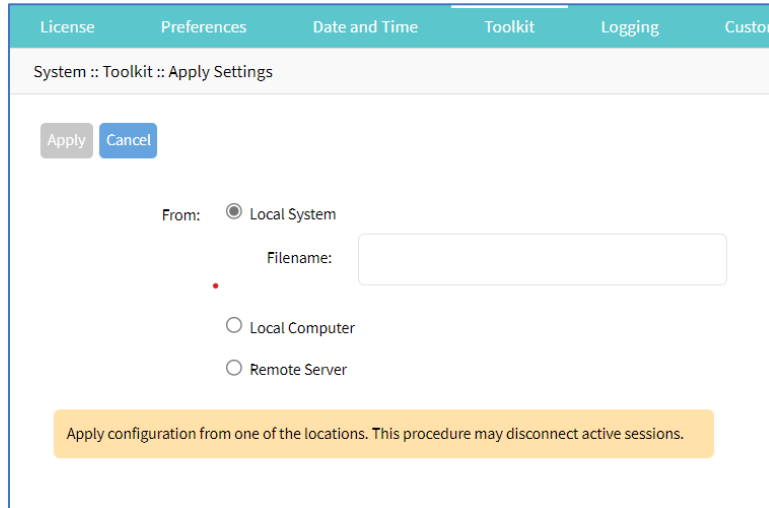
From: Local System

Local Computer
 Remote Server

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

WebUI Procedure

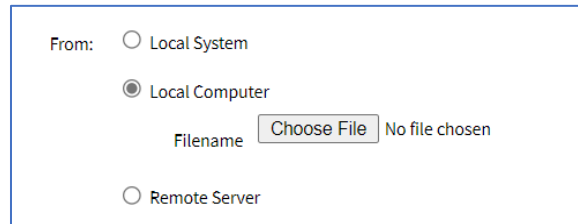
1. Go to *System :: Toolkit*.
2. Click **Apply Settings** icon (displays dialog).



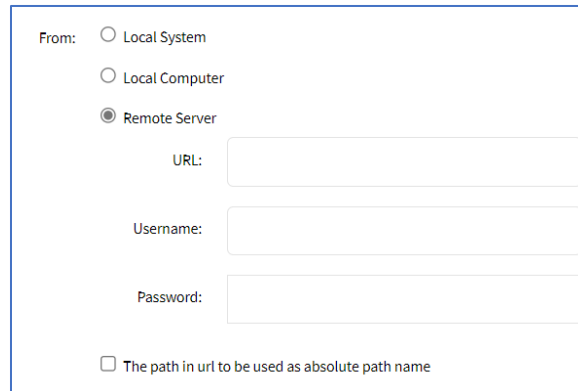
3. In *From* menu, select one:

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

The Nodegrid solution offers multiple options to reset the unit back to factory default settings.

If restore to factory default, all configuration files are set to factory default. There is an option to save or clear all log files.

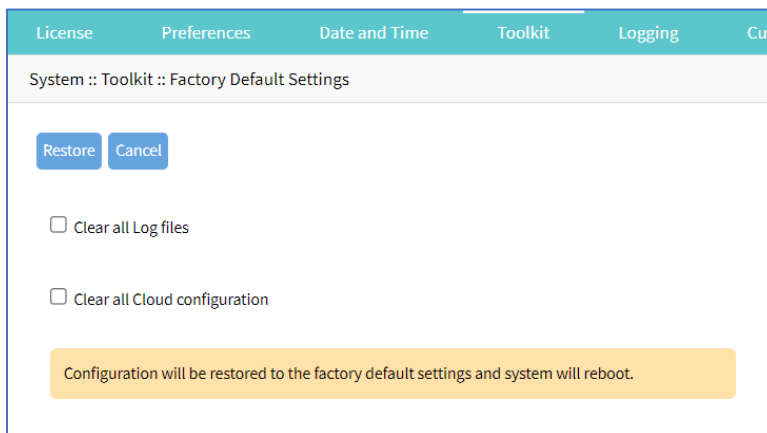
Hard restore is available on the Nodegrid device. To use, locate the RST button on the chassis. Press the RST button down for at least 10 seconds. All configuration files are reset to defaults and log files are cleared.

NOTE: Reset to factory default through the RST button requires a minimum ET version of 80814T00. See *About* page for the current version.

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

WebUI Procedure

1. Go to *System :: Toolkit*.
2. Click **Restore to Factory Default Settings** icon (displays dialog).



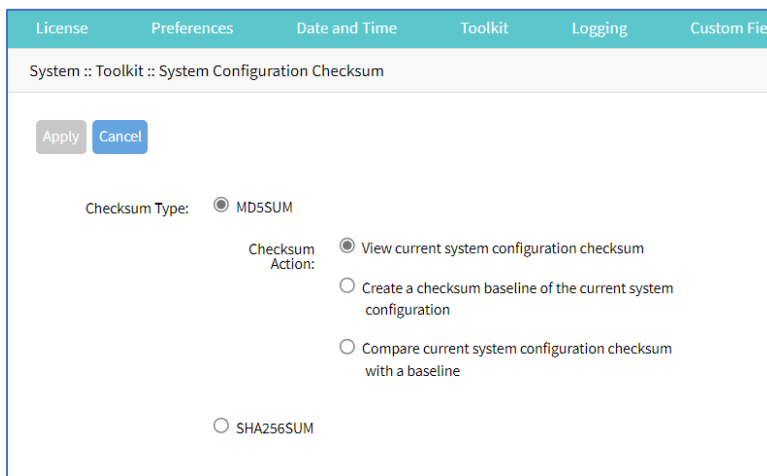
(optional) Select **Clear all Log files** checkbox.

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

3. Click **Restore**.

System Configuration Checksum

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



WebUI Procedure

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

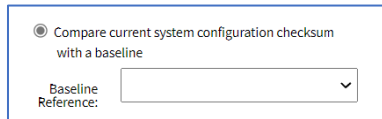
MD5SUM radio button

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.



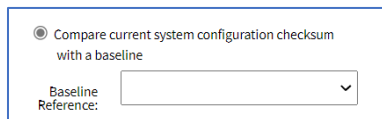
SHA256SUM radio button

In *Checksum Action* menu, select one:

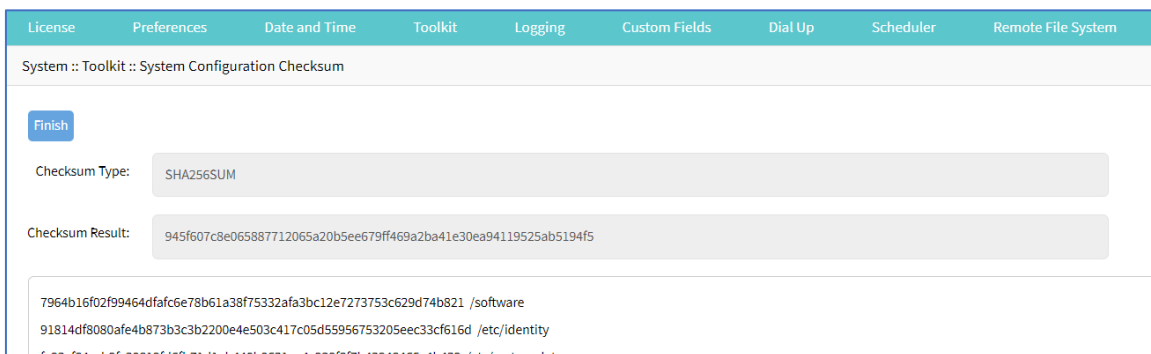
View current system configuration checksum radio button.

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**.

System Certificate

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**.



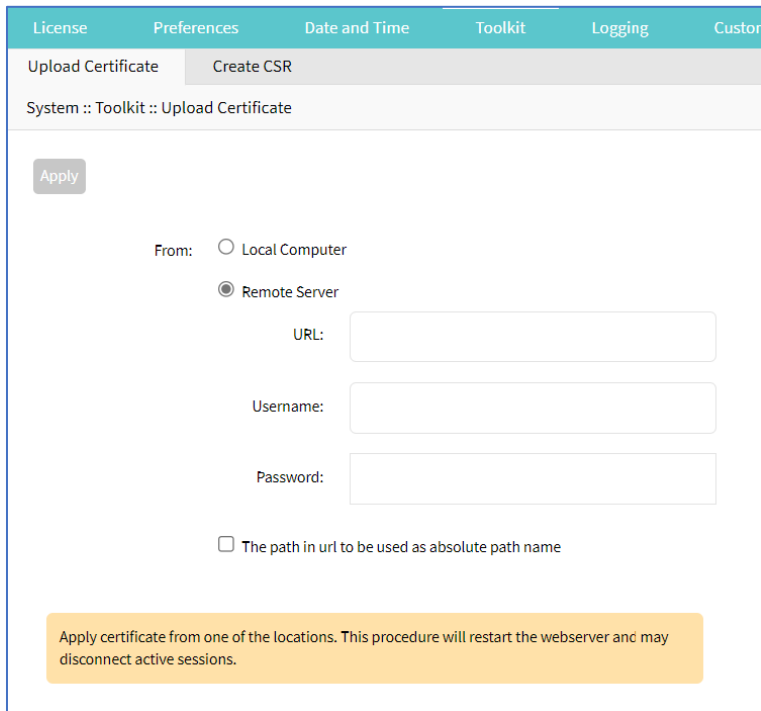
WARNING! When the certificate is applied, the web server is restarted and active sessions are disconnected.

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

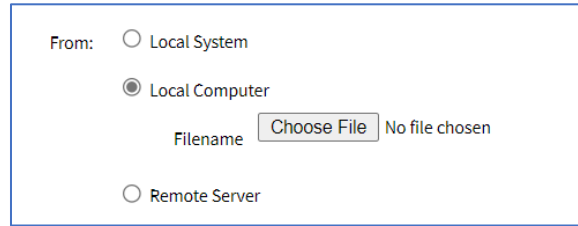
Upload Certificate

WebUI Procedure

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

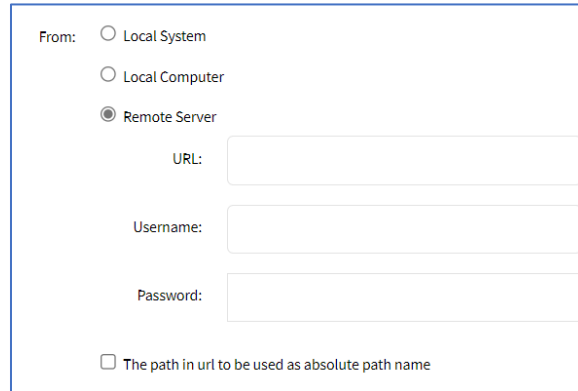


3. On the **Upload Certificate** sub-tab, *From* menu, select one.
 - Local System** radio button. Enter **File Name**.
 - Local Computer** radio button. Click **Choose File** (locate and select the file).



From: Local System
 Local Computer
 Filename No file chosen
 Remote Server

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



From: Local System
 Local Computer
 Remote Server
 URL:
 Username:
 Password:
 The path in url to be used as absolute path name

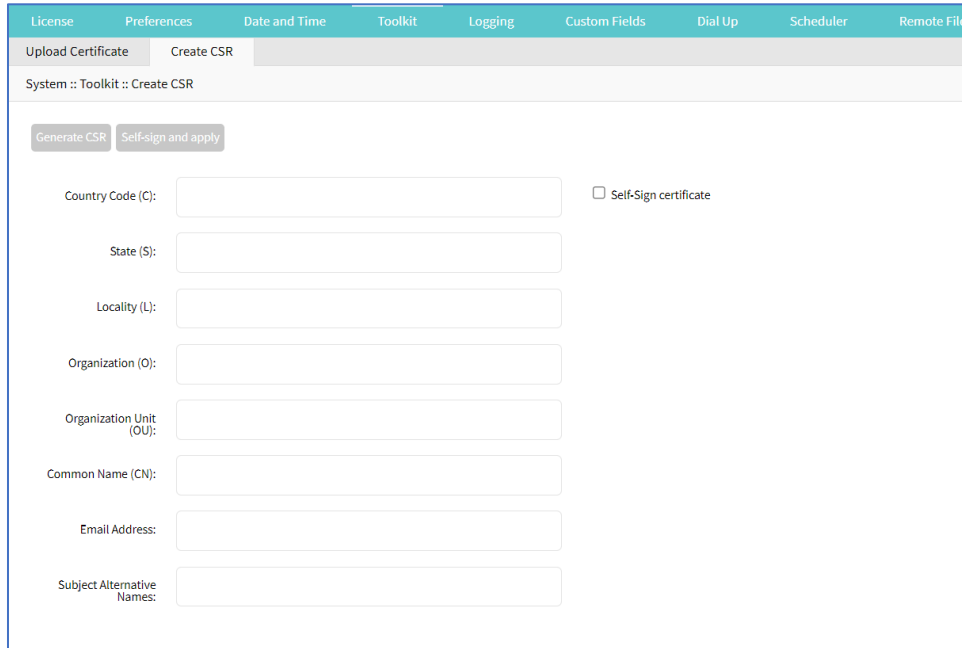
4. Click **Apply**.

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)** .

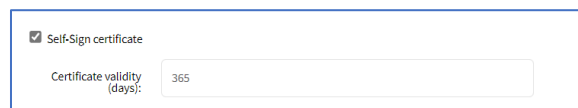
Enter **Organization Unit (OU)** .

Enter **Common Name (CN)** .

Enter **Email Address**.

(optional) **Subject Alternative Names**.

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

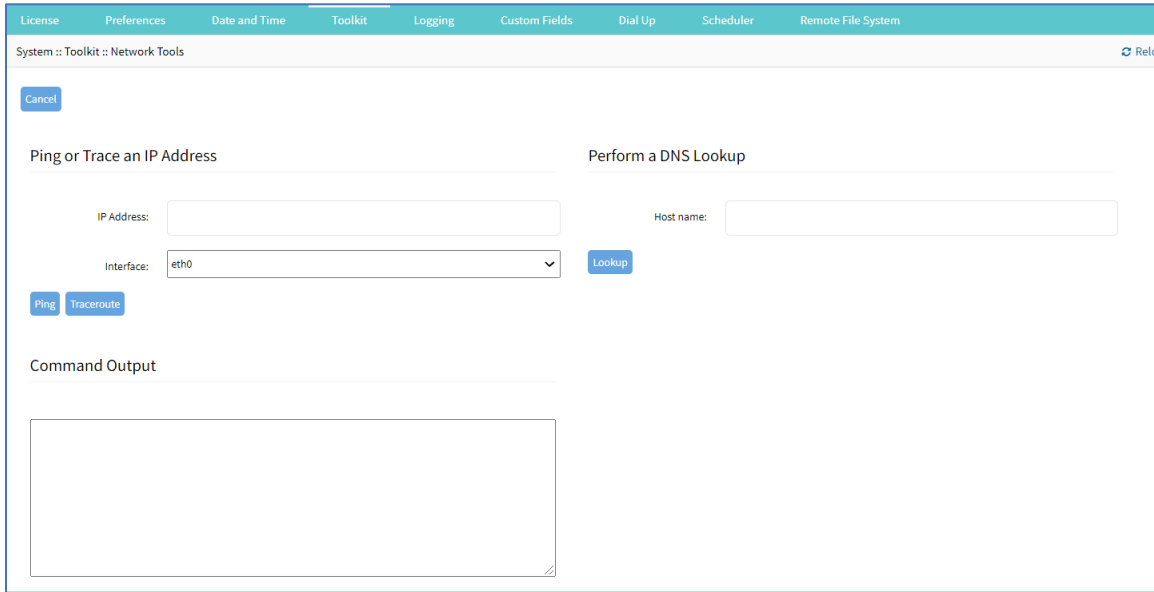


5. Click **Self-sign and apply**.

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

Network Tools

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



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**).
4. Click **Ping**.
5. 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**).

4. Click **Traceroute**.
5. Review results in *Command Output* panel.

Do 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.

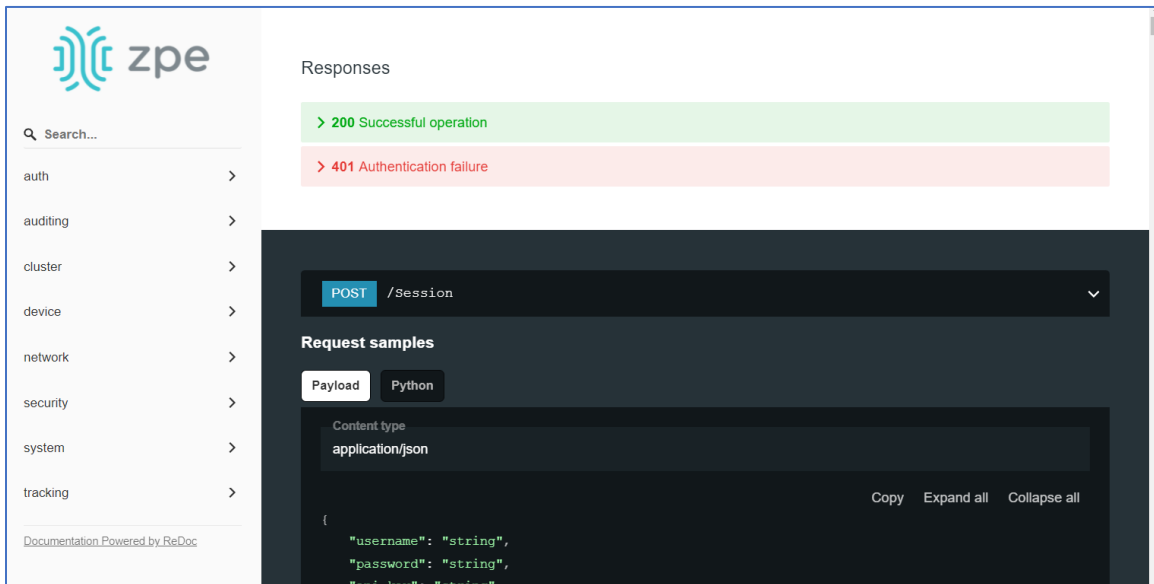
WebUI Procedure

1. Go to *System :: Toolkit*.
2. Click **Network Tools** icon (displays dialog).
3. In the *Perform a DNS Lookup* menu:
 - Enter **Host name**.
4. Click **Lookup**.
5. Review results in *Command Output* panel.

API

RESTful API

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



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**.

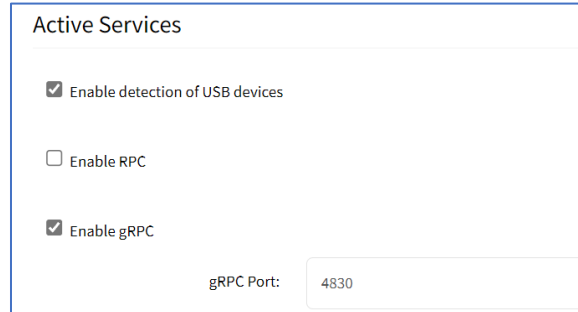
- On the left panel, click the > arrow to display API calls for that function. Request and Response examples are included.

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" ]}' }, [...]
```

Diagnostic Data

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:

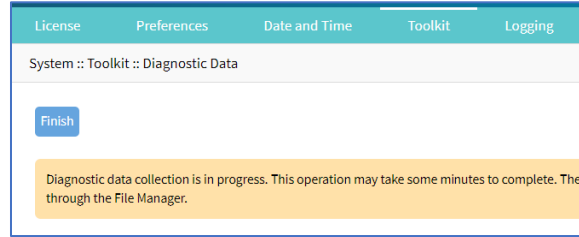
```
/home/admin/logs/collection_nodegrid_XXXX-XX-XX_XX-XX-X.tar.gz
```

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**.

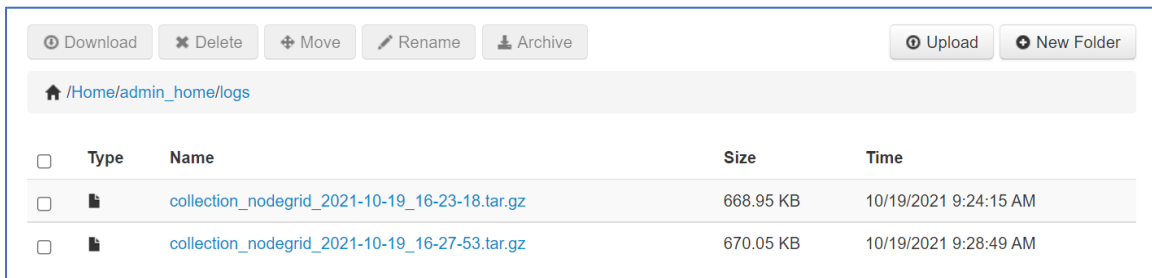


Step 2 – Access the Diagnostic Data Results

(Admin privileges required.)

WebUI Procedure

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

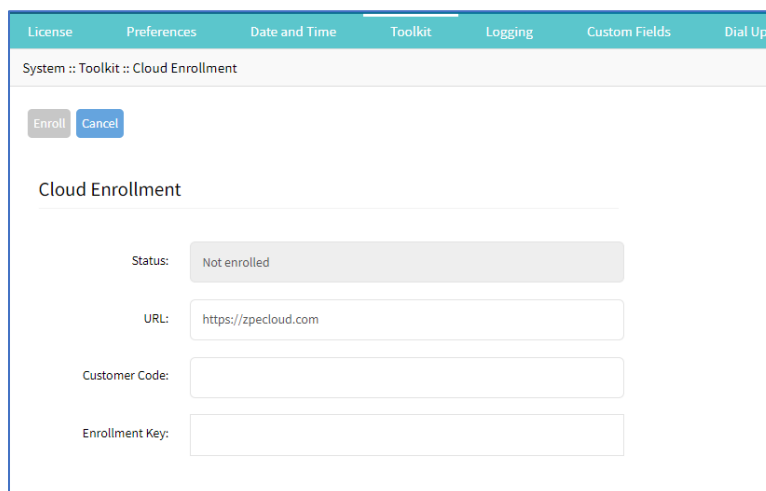


4. Locate the tarball and select checkbox.
5. Click **Download**.

Review the file, as needed.

Cloud Enrollment

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 (displays dialog)
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]#
```

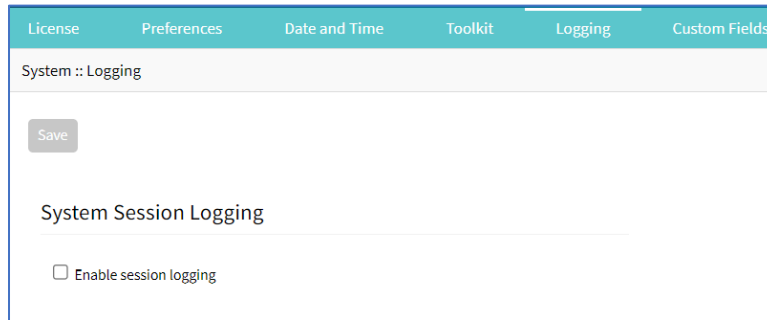
3. A confirmation is sent when the enrollment succeeds.

Once the ZPE Cloud is enabled on the device, access www.zpecloud.com 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).



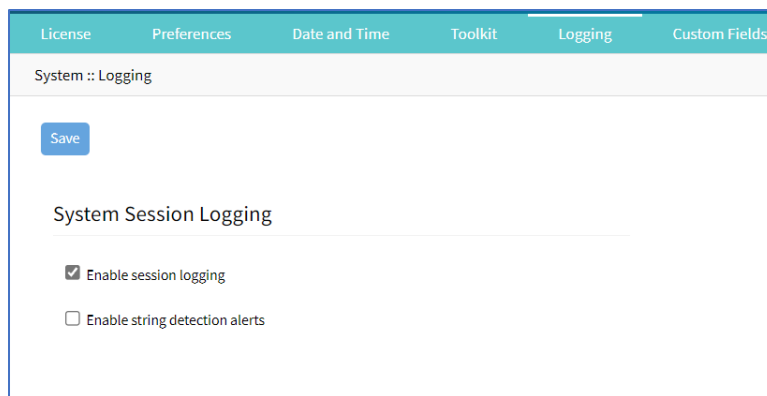
Enable Session Logging

Details can be modified, as needed.

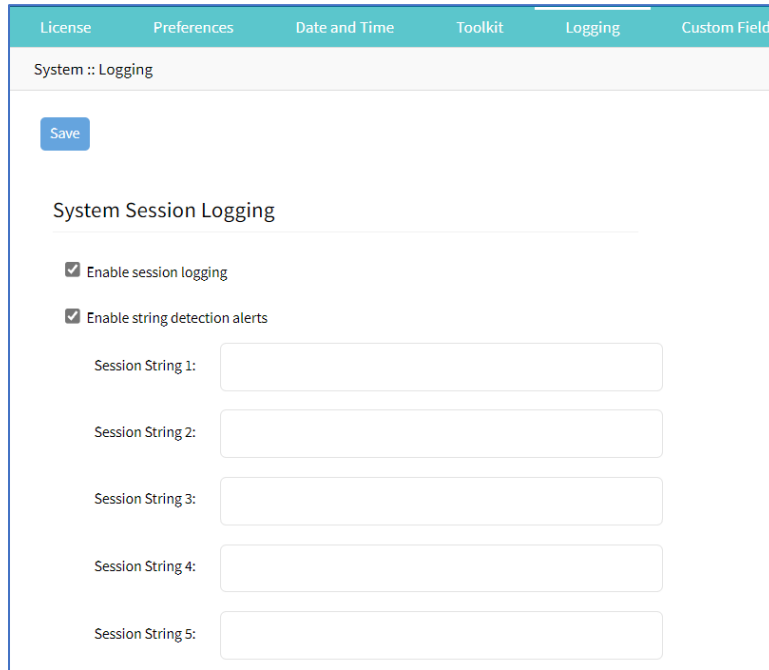
WebUI Procedure

1. Go to *System :: Logging*.
2. In *System Session Logging* menu:

Select **Enable session logging** checkbox (expands dialog).



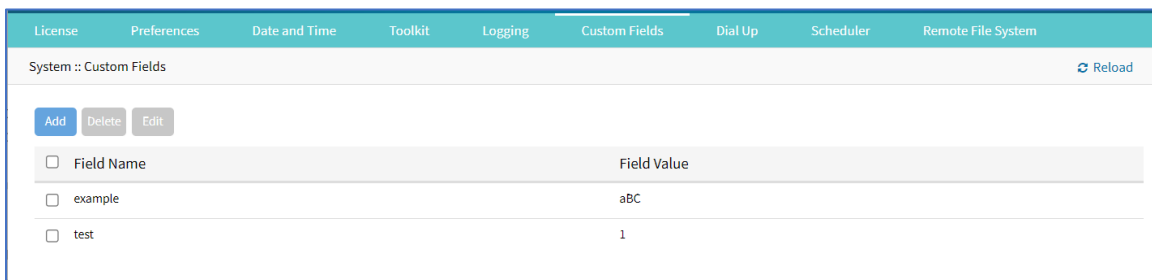
(optional) Select **Enable string detection alerts** checkbox (expands dialog). Enter **Session String** sets, as needed) that sends a notification alert upon occurrence.



3. Click **Save**.

Custom Fields tab

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

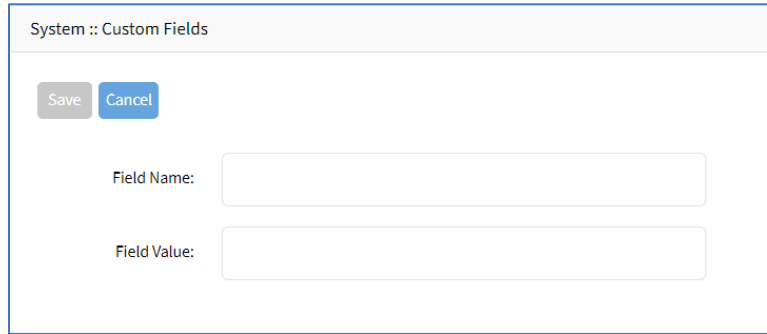


Field Name	Field Value
example	aBC
test	1

Add Custom Field

WebUI Procedure

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



The screenshot shows a web-based dialog box titled "System :: Custom Fields". At the top left, there are two buttons: "Save" (disabled) and "Cancel" (active). Below the buttons are two text input fields. The first is labeled "Field Name:" and the second is labeled "Field Value:". Both fields are currently empty.

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

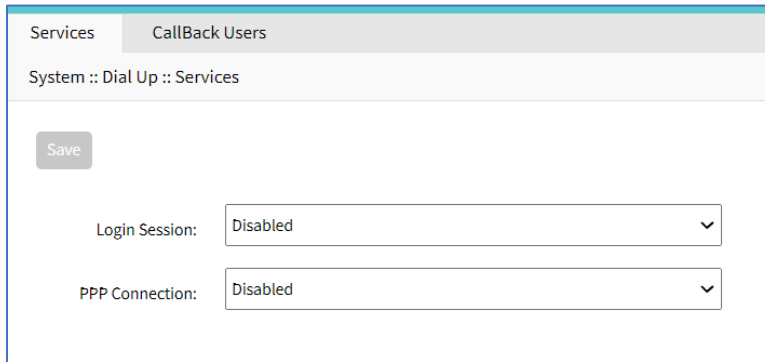
WebUI Procedure

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

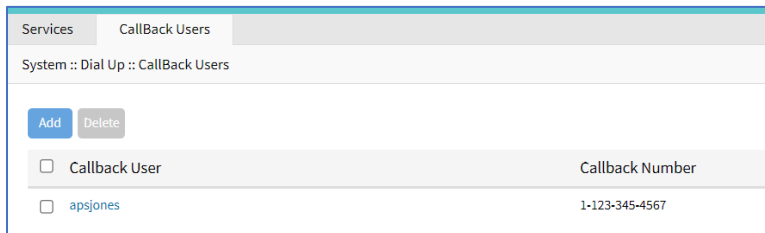


Manage Dial Up Services

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

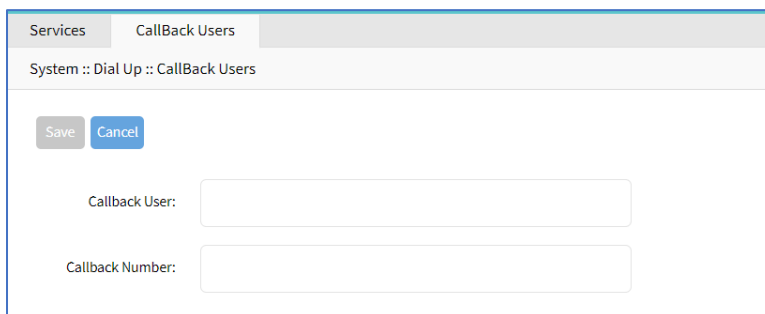


Callback User	Callback Number
<input type="checkbox"/> apsjones	1-123-345-4567

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

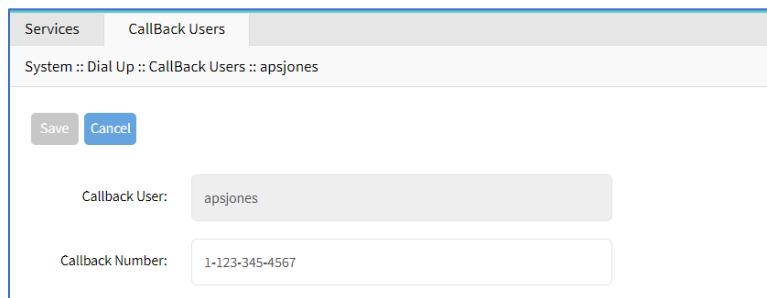
WebUI Procedure

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

Edit Callback User

WebUI Procedure

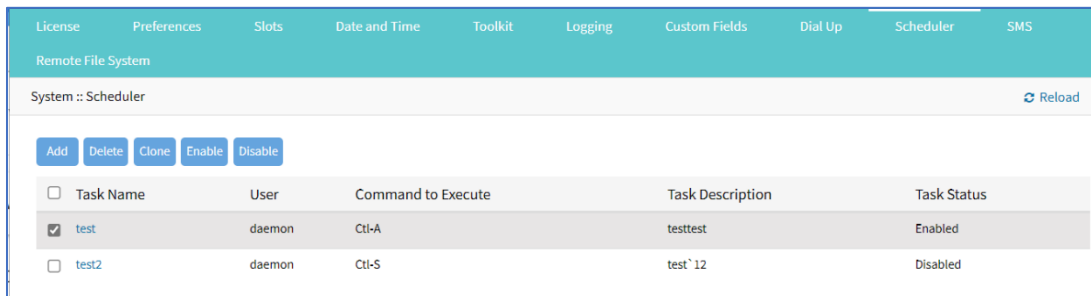
1. Go to *System :: Dial Up :: Callback Users*.
2. In *Callback User* column, click name.



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

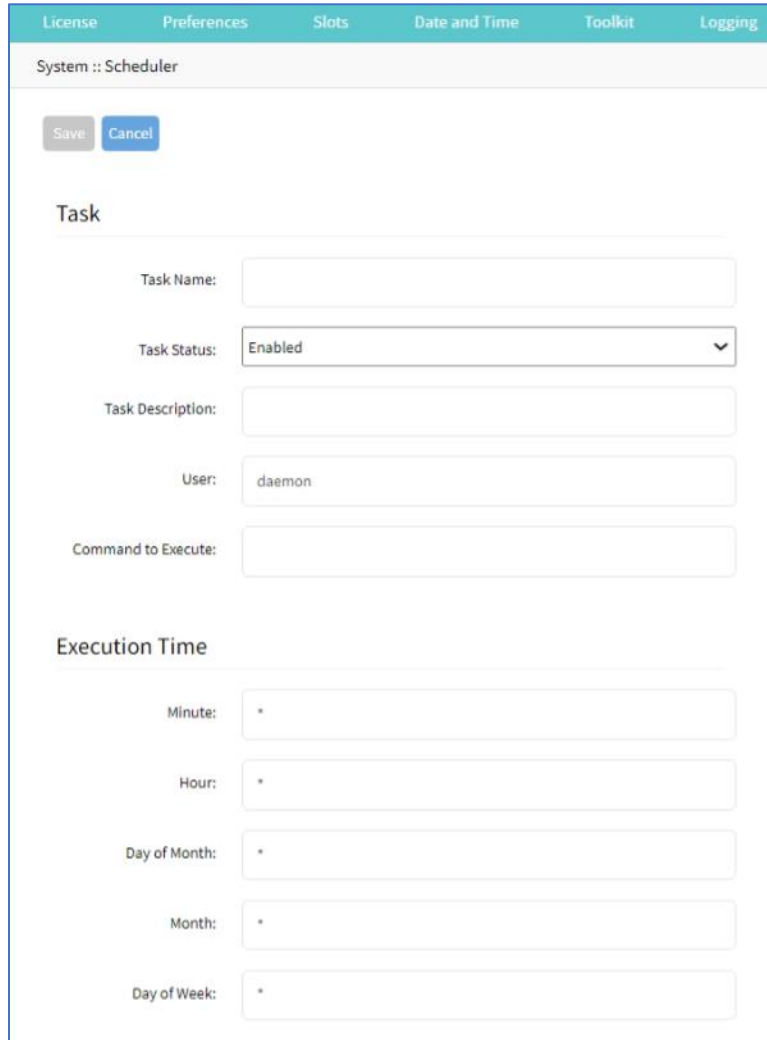
Factor	Daily Task 00:01 hours	Every Saturday: 23:45 hours	Every Hour on the Hour
Minute	1	45	0
Hour	0	23	*
Day of Month	*	*	*
Month	*	*	*
Day of Week	*	6	*

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 **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

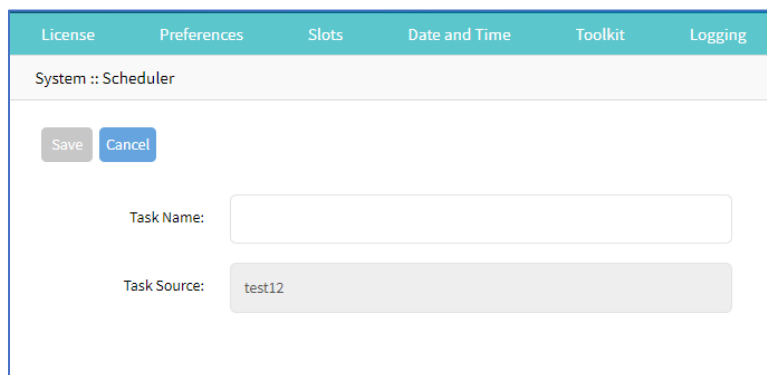
WebUI Procedure

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, and Link 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.

SMS Settings sub-tab

SMS Settings

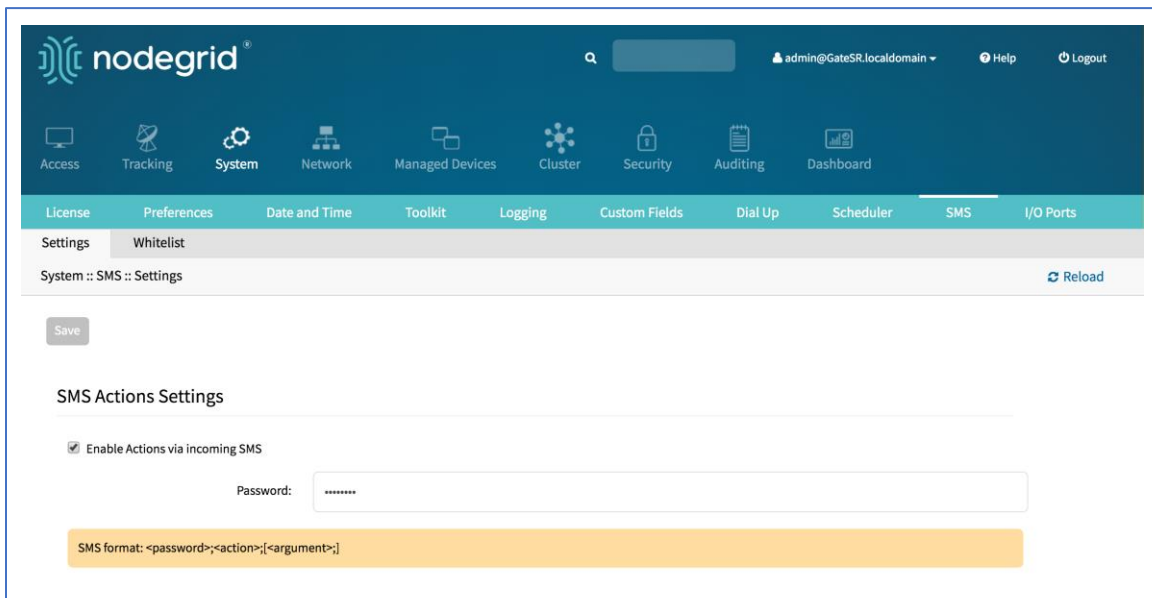
Action	Data type	Description
Enable Actions via incoming SMS	String	Disabled by default.
Allowed SMS Action		Actions allowed to be triggered by SMS.
apn - configure temporary APN	True/False	Configure a temporary APN.
simswap - temporary swap SIM card	True/False	Triggers a SIM card failover.
connect and disconnect - on/off data connection	True/False	Triggers a modem to connect or disconnect.
mstatus - request wireless modem status	True/False	Returns current modem status.
reset - reset wireless modem	True/False	Triggers a modem reset.

Action	Data type	Description
info - request information about Nodegrid	True/False	Returns About information.
factorydefault - factory default Nodegrid	True/False	Factory default of the Nodegrid device is triggered.
reboot - reboot Nodegrid	True/False	Triggers device reboot.

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.
3. Enter **Password**.
4. Click **Save**.

CLI Examples: SMS Actions and Messages

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

Format

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

connect (try to power on data connection)

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

disconnect (drop current data connection)

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

reset (reset wireless modem)

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

apn (configure temporary APN)

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

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 >
```

simswap (swap sim card temporary)

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

info (request device information)

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

reboot (reboot Nodegrid device)

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

factorydefault (restore Nodegrid configuration to factory default)

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


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.

SMS Whitelist

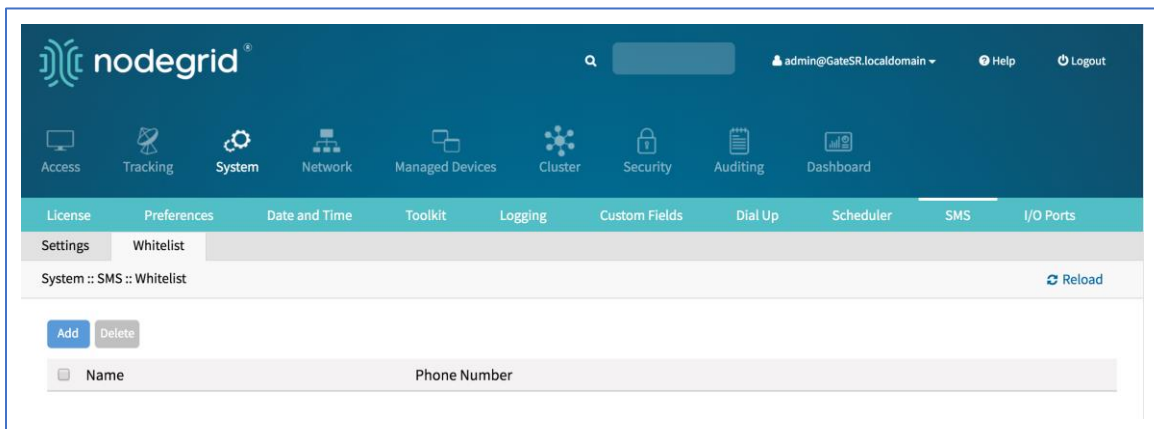
Setting	Data type	Description
Name	String	Name
Phone Number	Phone Number	Allowed Phone Number

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

Add Entry to Whitelist

WebUI Procedure

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

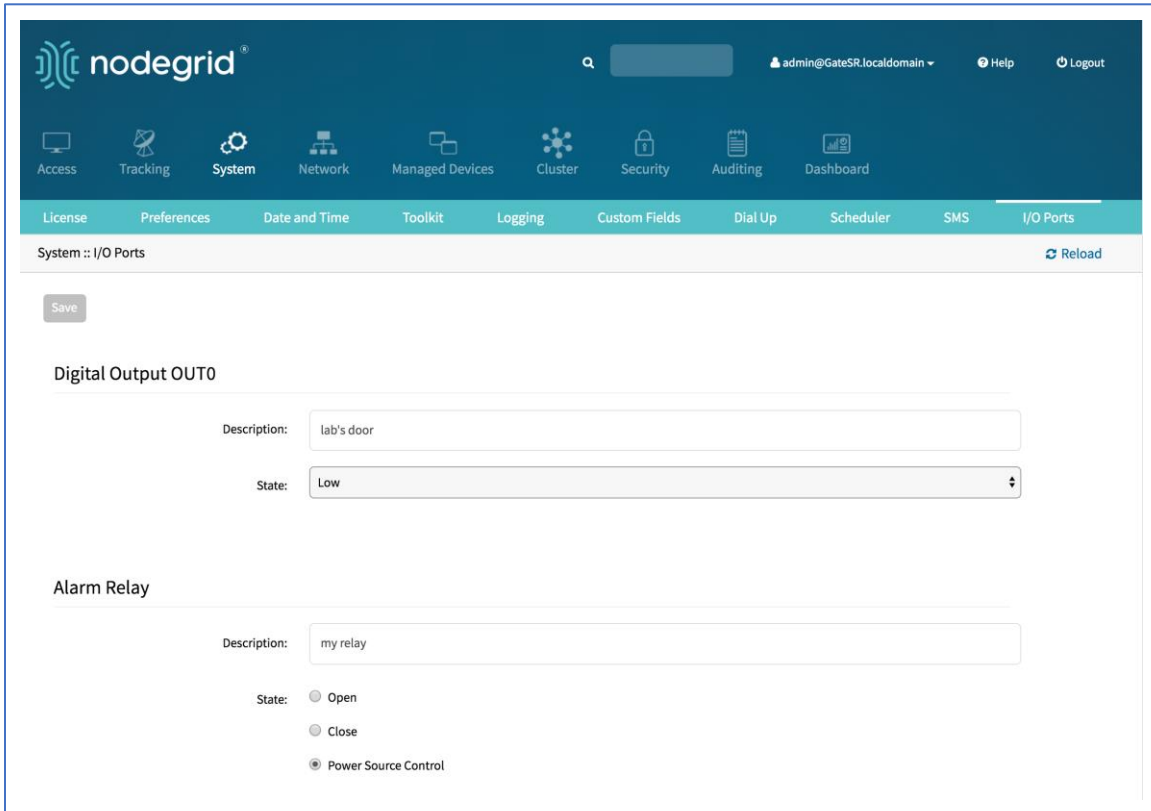


2. Click **Add** (displays dialog).
3. Enter **Name**.
4. Enter **Phone Number**.
5. Click **Save**.

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.



Network Section

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

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

Settings tab

Administrators can define the units host and domain name, configure Network Failover between multiple interfaces, enable IP Forwarding and configure a loopback address.

Hostname and Domain Name

The device hostname and domain name is defined in the *Network Settings* menu. Appropriate values for both settings must be provided.

Network Failover

The network failover option allows administrators to automatically failover between two and three different network interfaces. Each failover setting can be defined.

Failover Settings

Setting	Options	Description
Primary Connection	Interfaces	List of all available network interfaces. One must be selected.
Secondary Connection - Tertiary Connection	Interfaces	List of all available network interfaces. One must be selected.
Trigger	Unreachable Primary Connection IPv4 Default GatewayUnreachable IP address	Based on the setting, the System will check availability of the default gateway or a specified address.
Number of failed retries to failover	Number	Number of failed attempts to reach the trigger address. This is used to trigger a failover.
Number of successful retries to recover	Number	Number of successful tries to reach the trigger address. This is used to trigger a fallback.
Interval between retries (seconds)	Number	Amount of time to wait between tries.

The Nodegrid Platform supports configuration of a Dynamic DNS for failover interfaces.

Network Failover for Wireless Connections

Additional failover options are available for wireless connections:

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

Failover by Signal Strength

Signal Strength (%):

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

Carrier Limit

Warning Limit

Custom (Data Usage Limit (MB))

Failover by Data Usage

Threshold:

Carrier Limit (Configured on Data Usage Monitoring)

Warning Limit (Configured on Data Usage Monitoring)

Custom

Data Usage Limit (MB):

Failover by Schedule (triggered on a set schedule).

Failover by Schedule

Schedule:

Time to Failback (hours):

Schedule field is in cron format: minute hour day(month) month day(week). Failover will happen at every trigger.

NOTE: See “Scheduler Date and Time examples” for schedule format examples.

IPv4 and IPv6 Profile

IP Forwarding

IP Forwarding can route network traffic between network interfaces. Behavior of the routing traffic can be further adjusted with firewall settings. IP Forwarding is enabled independently for IPv4 and IPv6.

Loopback Address

If required, a Loopback address can be configured for IPv4 and IPv6. The address is assigned a bitmask of /32 (IPv4) or /128 (IPv6).

Reverse Path Filtering

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 be changed because of dynamic routing protocols or other network setup scenarios.

Reverse Path Filtering Options

Value	Description
Disabled	No source address validation is performed.
Strict Mode	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 Mode	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.

Multiple Routing Tables

Nodegrid supports multiple routing tables to assign specific routing details to specific network interfaces or IP clients. This is enabled by default. Administrators can disable, if required.

Connections tab

Administrators can edit, add, and delete existing network configurations. All existing physical interfaces are automatically added. The following physical interfaces exist, depending on the model.

Physical Interfaces

Interface	Model	Physical interface
ETH0	all	eth0
ETH1	Nodegrid Serial Consoles, Services Router	eth1
BACKPLANE0	Nodegrid Bold SR, Services Router, Gate SR	Backplane0 provides the connection to switch ports and sfp0 (Nodegrid Services Router).
BACKPLANE1	Nodegrid Services Router, Gate SR	Backplane1 provides the connection to sfp1.
SFP0	Nodegrid Gate SR	sfp0
SFP1	Nodegrid Gate SR	sfp1
hotspot	all	Interface is bound to wireless adapter (if available).

The administrator can define settings for each interface.

Physical Interface Settings

Settings	Description
Set as Primary Connection	Defines the interface as the primary connection. (Only one interface can be the primary.)
Enable LLDP advertising and reception through this connection	Enables LLDP advertisement through the interface.
(IPv4/IPv6) mode	Defines the IP mode for the interface, available are: No (IPv4/IPv6) Address DHCP (IPv4)Address Auto Configuration (IPv6) Stateful DHC (IPv6) Static (IPv4/IPv6)
(IPv4/IPv6) address	Defines a static IP address, if the mode is set to static.
(IPv4/IPv6) bitmask	Defines a static IP bitmask, if the mode is set to static.
(IPv4/IPv6) gateway	(optional) Defines a static IP gateway, if the mode is set to static.
(IPv4/IPv6) DNS Server	(optional) Defines a DNS Server for this connection Defines a static IP gateway, if mode is set to static.
(IPv4/IPv6) DNS Search	Defines a domain name for DNS lookups.

Additional interfaces can be defined to the existing physical interfaces – for more advanced configuration options.

Supported Interface Types

Interface	Description
Bonding	Allows bonding of multiple interfaces for Failover purposes.
Ethernet	Allows configuration of additional physical interfaces.
Mobile Broadband GSM	Allows configuration of available LTE modem connections.
VLAN	(optional) Allows configuration of VLAN interfaces (bound to physical interfaces).
WiFi	(optional) Allows configuration of WiFi interfaces, as WIFI client or hotspot. By default, a WiFi interface already exists with the name "hotspot".
Bridge	Allows creation of a bridge interface of one or multiple physical interfaces.

Bonding Interfaces

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).

Bonding Interface Options

Setting	Description
Primary Interface	Primary network interface.
Secondary Interface	Secondary network interface.

Setting	Description
Bonding Mode	<p>Allows use of the Bond mode. Valid options are:</p> <p>(0) Round Robin (Packets transmitted in sequential order from first available slave through the last).</p> <p>(1) Active Backup (Only one slave in the bond is active. A different slave becomes active if, and only if, the active slave fails.)</p> <p>(2) Balance XOR (Transmit based on the selected transmit hash policy.)</p> <p>(3) Broadcast (Transmits everything on all slave interfaces. This mode provides fault tolerances.)</p> <p>(4) 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.)</p> <p>(5) Balance TLB (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.)</p> <p>(6) Balance ALB (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.)</p>
Link Monitoring	Allows Link monitoring mode to be specified. Options are: MII, ARP.
Monitoring Frequency (ms)	Allows defining a link-state monitoring frequency in ms for the interfaces. Value is only valid for MII mode.
Link Up delay (ms)	Allows defining a delay in ms before an interface is brought up after a link is detected. Value is only valid for MII mode.
Link Down delay (ms)	Allows defining a delay in ms before an interface is brought down after link down is detected. Value is only valid for MII mode.
ARP target	Allows defining an IP target which will be used to send ARP monitoring requests to. ARP mode value must be defined.
ARP validate	Allows defining which interfaces to use for the ARP validation. Options: None, Active, Backup, All
Bond Fail-over-MAC policy	Allows the definition of the MAC address failover policy. Options are: Primary Interface, Current Active Interface, Follow Active Interface.
Primary Interface	Primary network interface.

Ethernet Interfaces

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.

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, and LSR) 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.

Mobile Broadband GSM Interface Options

Setting	Description
SIM-1 User name	User name to unlock the SIM.
SIM-1 Password	Password to unlock the SIM.
SIM-1 Access Point Name (APN)	Access Point Name.
SIM-1 Personal Identification Number (PIN)	PIN to unlock the SIM.
Enable Second SIM card	(optional) Allows a 2nd SIM card to be configured.
Active SIM card	Allows definition of the primary SIM card to be used.
SIM-2 User name	User name to unlock the SIM.
SIM-2 Password	Password to unlock the SIM.
SIM-2 Access Point Name (APN)	Access Point Name.
SIM-2 Personal Identification Number (PIN)	PIN to unlock the SIM.
MTU	Allows the MTU value to be set (in bytes). Field can be set to 'auto' (equal to 1500 bytes).

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

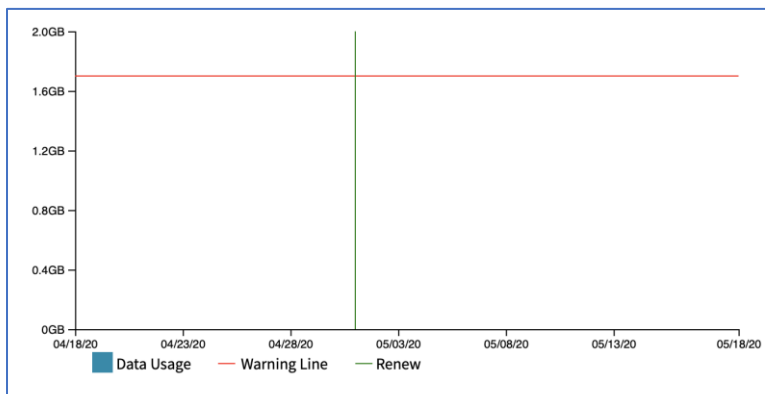
Enable Data Usage Monitoring

Data Usage Monitoring can be enabled to trigger an alarm once your mobile data usage has reached a set percentage of your monthly allowance.

WebUI Procedure

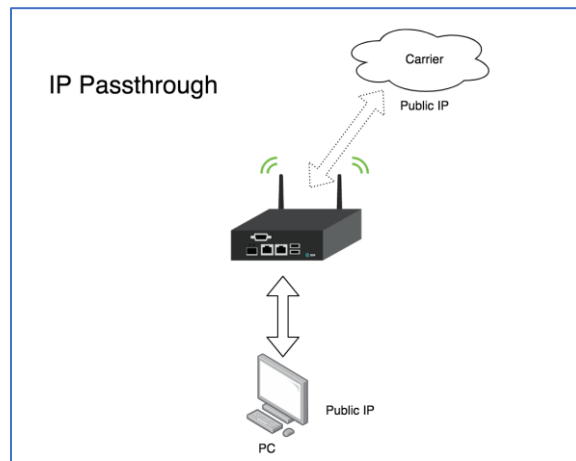
1. Go to *Network :: Connections*.
2. Click on the Mobile Broadband GSM connection to be enabled for Data Usage Monitoring.
3. Select **Enable Data Usage Monitoring** checkbox.
4. Enter these details:
 - SIM-1 Data Limit Value (GB)** (monthly data limit).
 - SIM-1 Data Warning (%)** (percentage that triggers an alarm).
 - SIM-1 Renew Day** (day to reset accumulated data).
5. Click **Save**.

A graph is displayed with lines set based on the parameters entered.

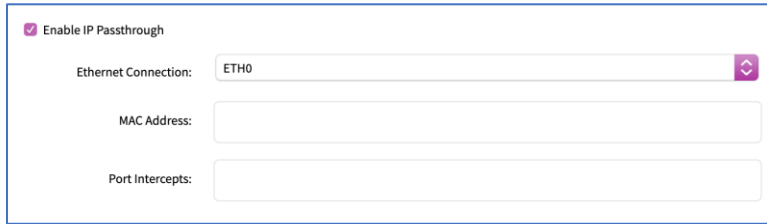


Enable IP Passthrough

IP Passthrough allows a connected device to be reachable via a public IP.



1. Go to *Network :: Connections*.
2. Click on the Mobile Broadband GSM connection to be enabled for IP Passthrough.
3. Select **Enable IP Passthrough** checkbox.
4. On the **Ethernet Connection** drop-down, select one.



The screenshot shows a configuration form for IP Passthrough. At the top, there is a checked checkbox labeled "Enable IP Passthrough". Below this, there are three input fields: "Ethernet Connection:" with a dropdown menu showing "ETH0", "MAC Address:" with an empty text box, and "Port Intercepts:" with an empty text box.

5. For **MAC Address**, enter the target device MAC address. If blank, the system uses DHCP to get the target device.
6. For **Port Intercepts**, enter any ports that should NOT pass through the Nodegrid device.
7. Click **Save**.

VLAN Interface

VLAN Interfaces can natively tag network traffic with a specific VLAN ID. The VLAN Interface needs to be created. The VLAN interface has the same settings as any other network interface and behaves the same way. It is bound to a specific physical interface with an administrator-defined VLAN ID.

WiFi Interface

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

WiFi Access Point

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.

WiFi Client

To use the device as a WiFi client, the existing hotspot connection must be disabled.

1. Go to the settings and disable the **Connect Automatically** option.
2. Ensure that the hotspot interface is down.
3. The system creates a new WiFi interface to allow the device to act as a client.

WiFi Settings

The WiFi configuration security configuration options support No Security or WPA2 Personal.

WiFi Specific Settings

Setting	Description
WiFi SSID	SSID to be used.
WiFi BSSID	MAC address of the Access Point to be used.

Hidden Network	When enabled, the SSID will not be broadcasted.
WiFi Security	Allows security to be set up (No Security, WPA2 Personal).
WPA shared key	If WPA2 Personal is defined as security, a shared key can be defined.

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.

Bridge Network Options

Setting	Description
Bridge Interfaces	Comma-separated list of physical interfaces.
Enable Spanning Tree Protocol	Enable the Spanning Tree Protocol for the interface.
Hello Time (sec)	Number of seconds a HELLO packet is sent (used when Spanning Tree is enabled).
Forward Delay (sec)	Defines a packet forward delay (used when Spanning Tree is enabled).
Max Age (sec)	Defines maximum age for packages (used when Spanning Tree is enabled).

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.

Analog Modem Options

Setting	Description
Status	Connection status (enabled, disabled).
Device Name	Name of detected modem (i.e., tty, USB0).
Speed	Serial connection speed to the modem.
PPP Dial-Out Phone Number	
Init Chat	Define a specific AT init string (if required).

Setting	Description
PPP Idle Timeout (sec)	Define the connection idle timeout after which the connection is automatically disconnected. 0 sec = connection does not get automatically disconnected.
PPP IPv4/IPv6Address	Definition of IPv4 addresses for the PPP connection. Options are: No Address Local Configuration (Configuration of a local and remote IP address). Accept Configuration from Remote Peer.
PPP Authentication	Definition of PPP authentication options. Possible options are: None By Local System (allows a definition of authentication protocol of PAP, CHAP, EAP) By Remote Peer (allows a definition of a remote username and password)

Static Routes tab

Administrators can define and manage static routes. Routes can be created for IPv4 and IPv6, assigned to specific network interfaces.

Static Route Options

Setting	Description
Connection	Selection of the network connection associated with the route.
Type	Definition of IP type. Options are: IPv4,IPv6.
Destination IP	Definition of the destination IP or network.
Destination BitMask	Definition of the associated bitmask (xxx.xxx.xxx.xxx or xx Example: 255.255.255.0 24
Gateway IP	Definition of the gateway address.
Metric	Definition of the routing metric value. Normal routes have a default value: 100.

Hosts tab

Administrators can configure and manage manual hostname definitions (equivalent to entries in the host's file).

Manual Hostname Options

Setting	Description
IP Address	Target hosts IP address. (IPv4 and IPv6 formats are supported.)
Hostname	Hostname of the target.

Setting	Description
Alias	Additional hostname aliases.

DHCP Server tab

The DHCP server for target 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 target 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.

DHCP Server Options

Setting	Description
SubNet	IP address subnet network are used. Must match the settings of a configured interface.
Netmask	Network mask for the defined subnet – format: xxx.xxx.xxx.xxx
Domain	Domain name for the scope.
Domain Name Servers (DNS)	DNS servers for the scope.
Router IP	Default gateway for the scope.
Network Range - IP Address Start	First IP address to be served.
Network Range - IP Address End	Last IP address to be served.
Hosts - Hostname	Hostname for IP address reservation.
Hosts - HW Address	MAC address to which an IP address reservation applies
Hosts - IP Address	IP address assigned to specific host matching the defined MAC address.

Network Switch Configuration

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

Switch Interfaces

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).

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.

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).

VLAN Configuration

Administrators can create, delete, and manage VLAN's. Ports can be assigned, as needed. By default, VLAN 1 and VLAN 2 exist. By default, all ports belong to VLAN 1 except BACKPLANE1 and SFP1 which belong by default to VLAN 2.

ACL

With the ACL (access control list) option, user can add, delete, and edit custom ACL rules for each interface. The main table displays details: Name, Interfaces, Direction, and number of rules.

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. In this case, no untagged traffic is accepted by the port.

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

Backplane Ports

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.

LAG

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.

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.

VPN SSL

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.

VPN Client

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.

VPN Client Options

Setting	Description
Name	Connection name.
Network Connection	Network interface the tunnel is bound.
Gateway IP Address	IP address or FQDN of the VPN server.
Gateway TCP Port	TCP port for the connection (default: 1194).
Connection Protocol	Supported connection protocols. Options: UTP, TCP.
Tunnel MTU	MTU size for the tunnel interface.
HMAC/Message Digest Alg	Selected HMAC connection algorithm from a list.
Cipher Alg	Selected connection cipher algorithm from a list.
Use LZO data compress Algorithm	If enabled, supports data compression.
Authentication Method	User authentication method. Options: TLS, Static Key, Password, Password plus TLS.
TLS - CA Certificate	CA certificate used by the SSL server.
TLS - Client Certificate	The certificate recognized by the SSL server.

Setting	Description
TLS - Client Private Key	Client certificates private key.
Static Key - Secret	Static key for the Secret.
Static Key - Local Endpoint (Local IP)	Local IP address for the VPN connection.
Static Key - Remote Endpoint (Remote IP)	Remote IP address for the VPN connection.
Password - Username	Connection username.
Password - Password	Connection password.
Password - CA Certificate	CA certificate file used by the SSL server.
Password plus TLS - Username	Connection username.
Password plus TLS - Password	Connection password.
Password plus TLS - CA Certificate	CA certificate file used by the SSL server.
Password plus TLS - Client Certificate	Client certificate recognized by the SSL server.
Password plus TLS - Client Private Key	Client certificates private key.

VPN Server

Nodegrid can be configured as a VPN server. By default, this is disabled. When configured as a VPN server and started, the *SSL Server Status* page provides an overview of the general server status and connected clients.

NOTE: Depending on the configuration, multiple files are required and must be available in the `/etc/openvpn/CA` folder.

VPN Server Options

Setting	Description
Status	After configured, must be enabled to start the server (default: disabled).
Listen IP address	Listening IP address. If defined, the server only responds to client requests coming in on this interface.

Setting	Description
Listen Port number	Listening port for incoming connections (default: 1194).
Protocol	Protocol to be used. Options: UDP, TCP.
Tunnel MTU	MTU used for the tunnel (default: 1500).
Number of Concurrent Tunnels	Total amount of concurrent SSL client sessions (default: 256).
IP Address	IP address settings for the tunnel. Options: Network, Point to Point, Point To Point IPv6.
IP Address - Network - IPv4 Tunnel(NetAddr Netmask)	IPv4 network address and network mask for the tunnel.
IP Address - Network - IPv6 Tunnel(NetAddr/Bitmask):	IPv4 network address and network mask for the tunnel.
IP Address - Point-to-Point - Local Endpoint (Local IP)	Local IPv4 IP address for Point-to-Point connection.
IP Address - Point-to-Point - Remote Endpoint (Remote IP)	Remote IPv4 IP address for Point-to-Point connection.
IP Address - Point-to-Point IPv6 - Local Endpoint (Local IP)	Local IPv6 IP address for Point-to-Point connection.
IP Address - Point-to-Point IPv6 - Remote Endpoint (Remote IP)	Remote IPv6 IP address for Point-to-Point connection.
Authentication Method	Authentication method. Options: TLS, Static Key, Password, Password plus TLS.
TLS - CA Certificate	CA certificate TLS.
TLS - Server Certificate	Server certificate TLS.
TLS - Server Key	Private TLS key of the server certificate.
TLS - Diffie Hellman	Diffie Hellman TLS.
Static Key - Secret	Secret static key.
Static Key - Diffie Hellman	Diffie Hellman static key.
Password - CA Certificate	CA certificate to use.
Password - Server Certificate	Password for server certificate to use.
Password - Server Key	Password for server key.

Setting	Description
Password - Diffie Hellman	Diffie Hellman password,
Password plus TLS - CA Certificate	CA certificate Password plus TLS.
Password plus TLS- Server Certificate	Server certificate Password plus TLS.
Password plus TLS- Server Key	Private server key Password plus TLS.
Password plus TLS- Diffie Hellman	Diffie Hellman Password plus TLS.
HMAC/Message Digest	HMAC connection algorithm selected from a list.
Cipher	Connection cipher algorithm selected from a list.
Min TLS version	Connection TLS minimum version. Options: None, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.
Use LZO data compress Algorithm	If enabled, all tunnel traffic is compressed.
Redirect Gateway (Force all client generated traffic through the tunnel)	If enabled, all traffic from a client is forced through the tunnel.

IPsec tab

The Nodegrid solution supports the IPsec tunnel configuration with a variety of options for host-to-host, host-to-site, site-to-site and road warrior settings. The Nodegrid node is directly exposed to the Internet. It is strongly recommended the device be secured. Built-in features include:

- Firewall configuration
- Enable Fail-2-Ban
- Change all default passwords with strong passwords
- Disable services not required

Overview

Authentication Methods

Multiple authentication methods are available. Some are simple (Pre-Shared keys and RSA keys) but with limited flexibility. Others require more initial configuration and setup which offers flexibility and consistency.

Pre-shared Keys

Pre-shared Keys provide the simplest and least secure method to secure an IPsec connection. This is a combination of characters that represent a secret. Both nodes must share the same secret. Nodegrid supports pre-shared keys with a minimum length of 32 characters. The maximum length is much higher. Due to compatibility reasons with other vendors, Nodegrid uses a 64-bit length for the examples. The longer the pre-shared key is, the more secure it is.

RSA Keys

RSA Keys or Raw RSA keys are commonly used for static configurations between single or a few hosts. The nodes are manually configured with each other's RSA keys.

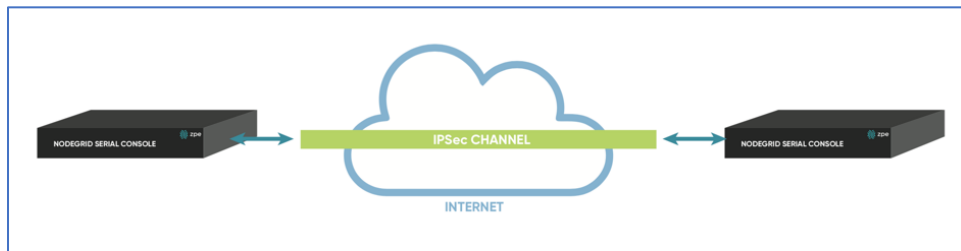
X.509 Certificates

Typically, X.509 Certificate authentications are used for larger deployments with a few to many nodes. The RSA keys of the individual nodes are signed by a central Certificate Authority (CA). The Certificate Authority maintains the trust relationship between the nodes. As needed, specific nodes can include revocation of trust. Nodegrid supports both public and private CA's. As needed, the Nodegrid Platform can host and manage its own Certificate Authority for IPsec communication.

Connection Scenarios

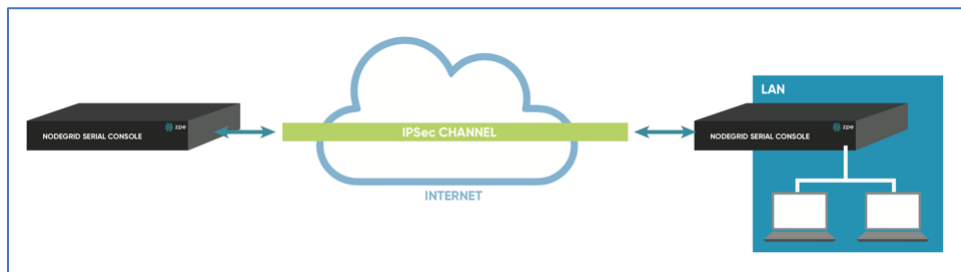
IPsec supports many connection scenarios, from the basic one-to-one nodes and the more complex one-to-many nodes. Communication can be limited to the directly involved nodes. If needed, communication can be expanded to the networks access table behind the nodes. Examples are provided for some of the most common scenarios.

Host-to-Host



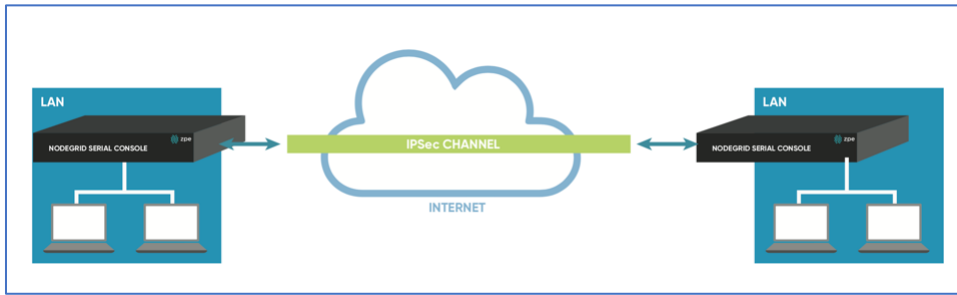
Host-to-Host communication is two nodes directly connected with a VPN tunnel. The communication is limited to direct communication between them. None of the packages are routed or forwarded. This is a point-to-point communication tunnel between two nodes.

Host-to-Site



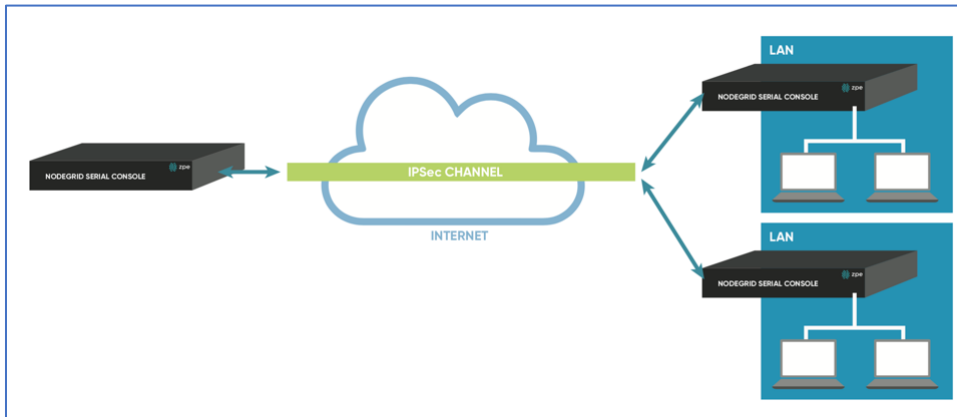
With host-to-Site, one node establishes a VPN tunnel to a second node. Communication is limited on one site to the specific node; and on the other side, limited to all devices in a range of subnet accessible by the second node.

Site-to-Site



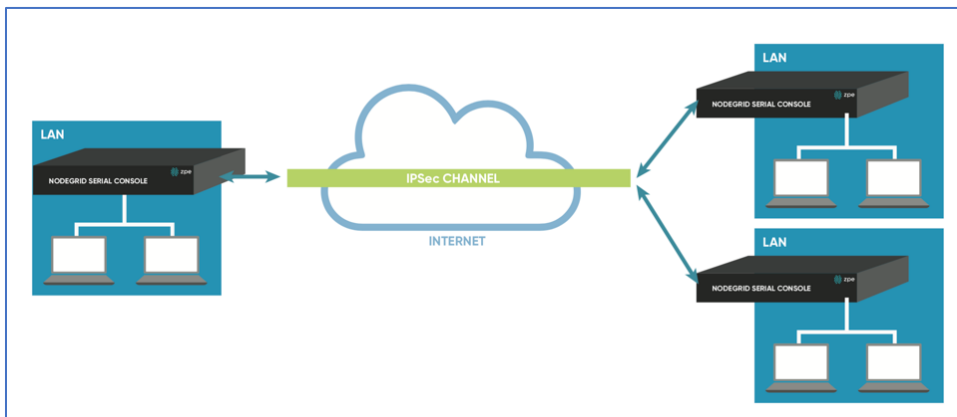
In site-to-site, the tunnel is established between two nodes. Communication can specify the subnet on both sides. This allows communication between devices on either side of the connection.

Host-to-Multi-Site



Host-to-multi-site communication is created with individual VPN connections. This is done between hosts or with specific multi-site configurations (which greatly improves scalability). Multiple nodes can connect to the same node. A typical use would be remote offices with a VPN connection to the main office. This would limit communications to the one node and devices on specified subnets in the remote locations.

Site-to-Multi-Site



Site-to-multi-site is most common for enterprise VPN setups. Similar to host-to-multi-site, communication is allowed to the specific subnet on either side. The West node would have access

to all specified subnet on any of the sites. The remote sites only can access the subnet exposed by the West node.

Keys and Certificates

Keys and Certificates

	Host to Host	Host to Site	Site to Site	Host to Multi-Site	Site to Multi-Host
Pre-shared Keys	Possible	Possible	Possible	Possible	Possible
RSA Key	Recommended	Recommended	Recommended	Possible	Possible
X.509 Certificates	Recommended	Recommended	Recommended	Recommended	Recommended

IPsec Configuration Process

These are the general configuration steps to configure the desired connection.

1. To prepare the Nodegrid, see [How to Prepare a Nodegrid Node for IPsec](#)
2. Ensure that one of the authentication methods is prepared:

[How to create Pre-shared Keys for IPsec](#)

[How to create RSA Keys for IPsec](#)

[How to Create Certificates for IPsec](#)

NOTE: For Production environments, it is recommended to use RSA Keys or Certificate Authentication. For a test environment, Pre-Shared Keys are easy to set up.

3. Create an IPsec configuration file. Configuration examples can be found here:

Pre-Shared Keys

[How to Configure IPsec Host to Host Tunnel with Pre-Shared Key](#)

[How to configure IPsec Host to Site tunnel with Pre-Shared Key](#)

[How to Configure IPsec Site to Site Tunnel with Pre-Shared Key](#)

RSA Keys

[How to Configure IPsec Host to Host Tunnel with RSA Keys](#)

[How to Configure IPsec Host to Site tunnel with RSA Keys](#)

[How to Configure IPsec Site to Site Tunnel with RSA Keys](#)

Certificates

[How to Configure IPsec Host to Host Tunnel with Certificate](#)

[How to Configure IPsec Host to Site Tunnel with Certificate](#)

[How to Configure IPsec Site to Site Tunnel with Certificate](#)

4. As required, distribute and exchange configuration files and keys to all nodes
5. Test the connection.

For more detailed instruction on how to use IPsec with the Nodegrid Platform, visit the [Knowledge Base](#).

Tunnel sub-tab

The main table displays available tunnels.

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.

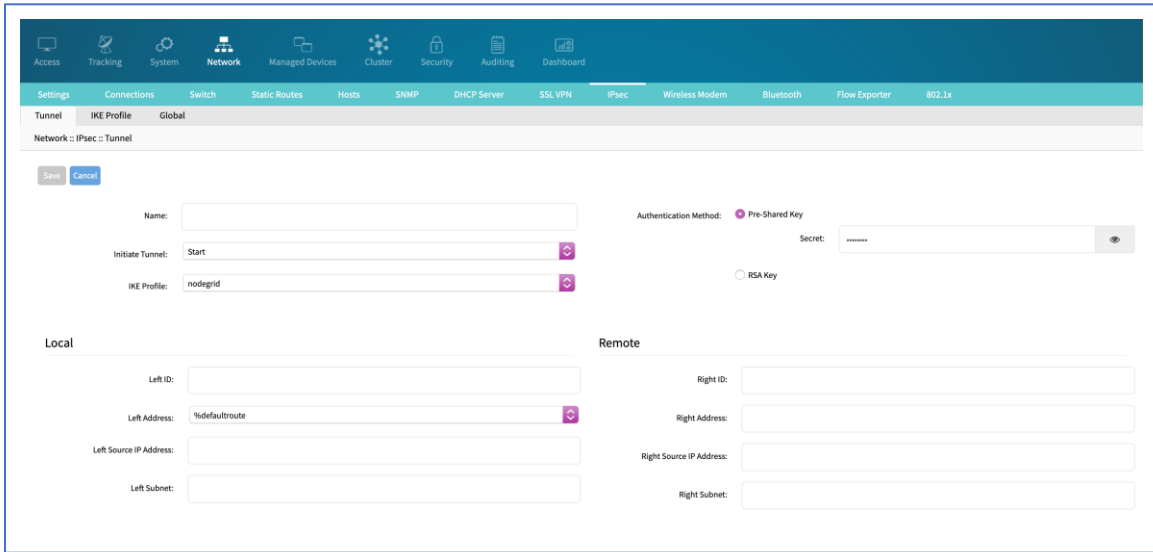
Tunnels can be managed with these actions:

- Add
- Delete
- Start Tunnel
- Stop Tunnel

WebUI Procedure

Add a new tunnel

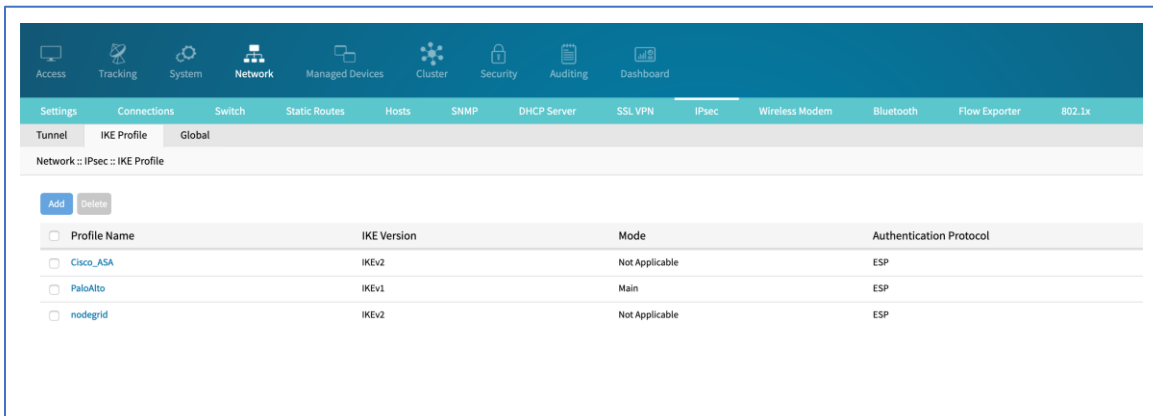
1. Go to *Network :: IPsec :: Tunnel*.
2. Click **Add**.
3. Enter configuration details.



4. Click **Save**.

IKE Profile sub-tab

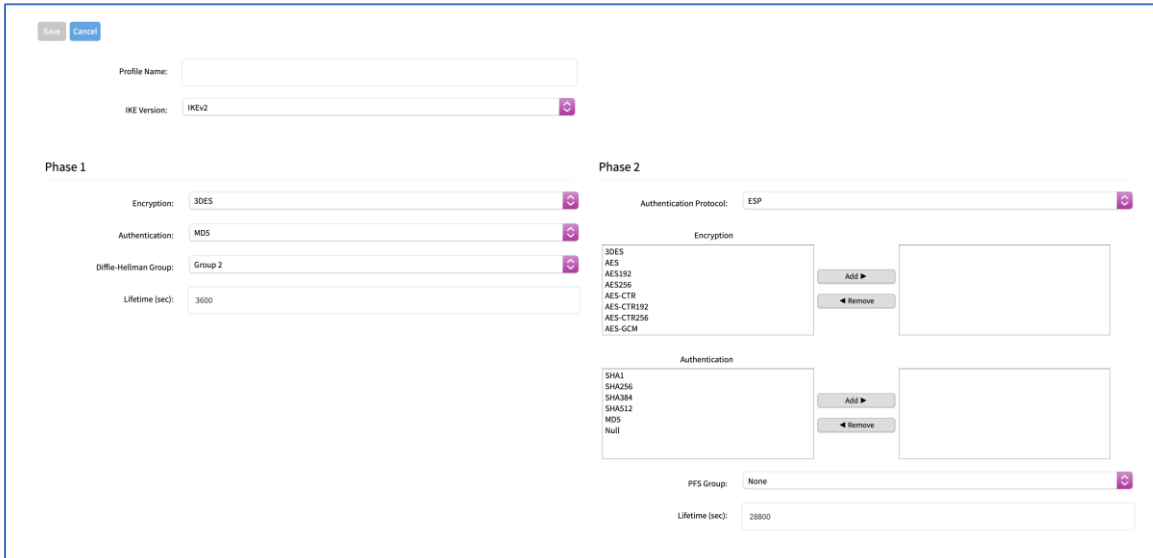
IKE Profiles activities are: Add, Delete, or Edit.



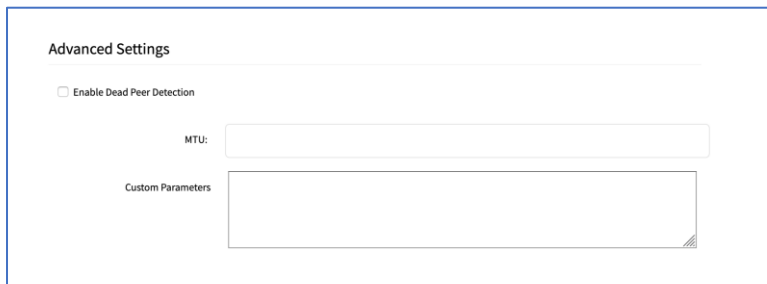
WebUI Procedure

To add a new profile:

1. Go to *Network :: IPsec :: IKE Profile*.
2. Click **Add**.
3. Enter configuration details.



4. In *Advanced Settings* menu, modify details as needed.



5. Click **Save**.

WebUI Procedure

To edit a profile:

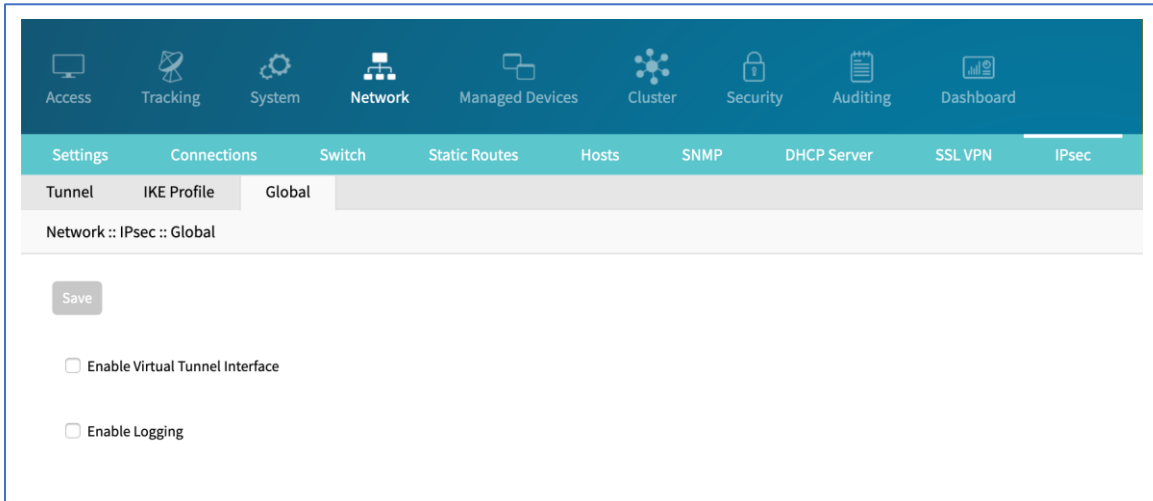
1. Go to *Network :: IPsec :: IKE Profile*.
2. Locate and click on the **Profile Name**.
3. Modify configuration details, as needed.
4. Click **Save**.

Global sub-tab

WebUI Procedure

On this page, edit the options:

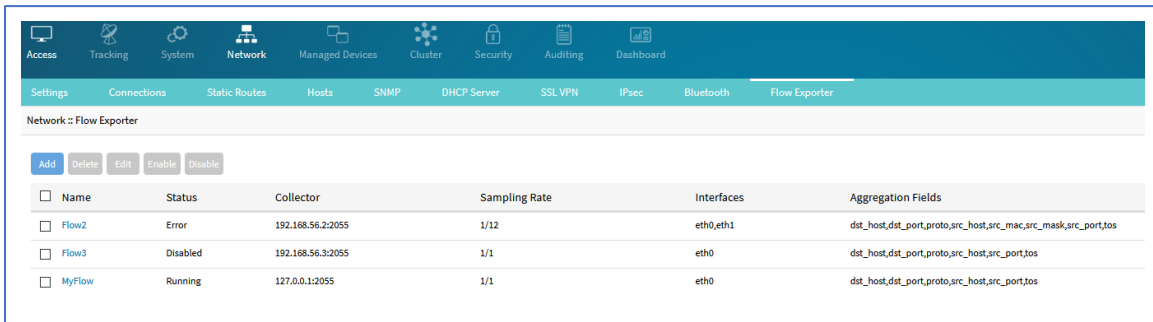
1. Go to *Network :: IPsec :: Global*.



2. Select/unselect **Enable Virtual Tunnel Interface** checkbox.
3. Select/unselect **Enable Logging** checkbox.
4. Click **Save**.

Flow Exporter tab

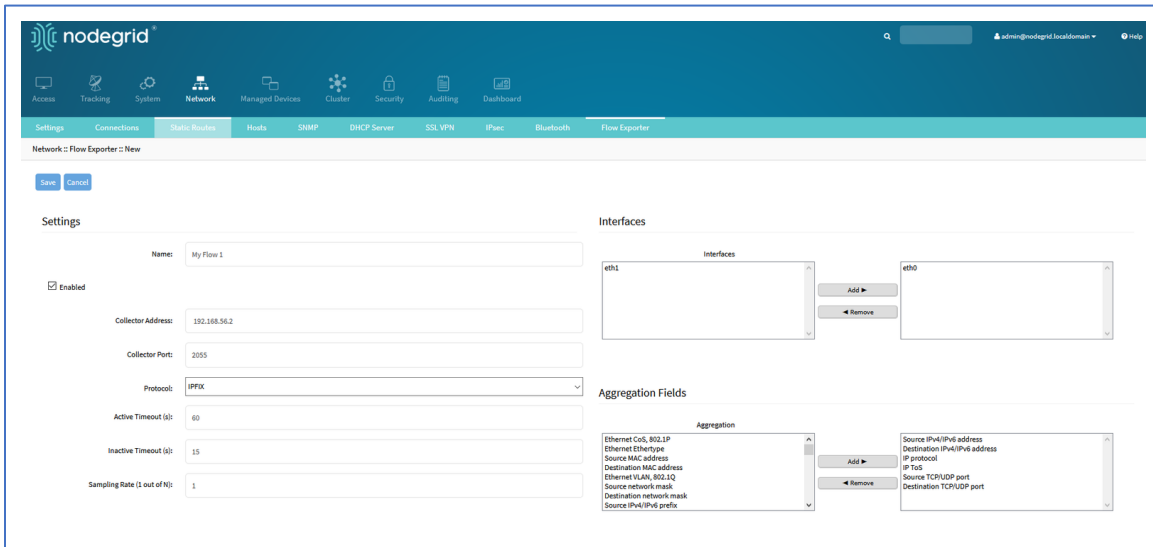
Netflow streaming telemetry data is supported for all network interfaces including the switch interface.



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:



The following fields are needed:

- Name
- Collector Address
- Collector Port
- Protocol
- Active Timeout (seconds)
- Inactive Timeout (seconds)
- Sampling Rate (1 out of N)
- Interfaces
- Aggregation Fields

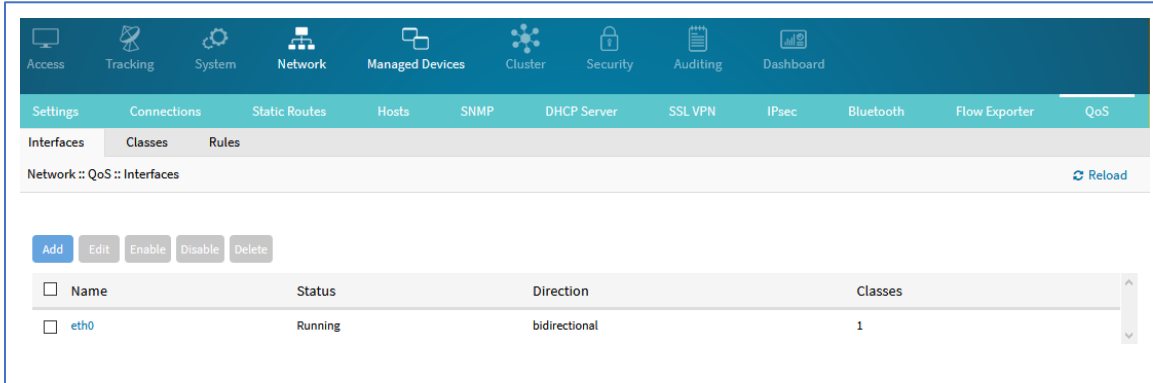
QoS tab

Under the QoS tab, you are able to configure rules directly from the web interface. 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 a new Interface

WebUI Procedure

1. Click **Add**.
2. Enter the details:

Interface

QoS Direction

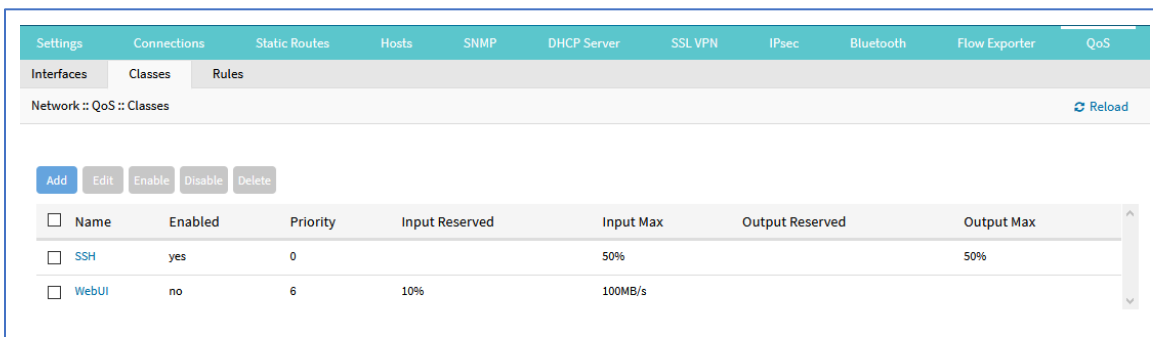
Assignment

Bandwidth

3. Click **Save**.

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.



Add a new Class

WebUI Procedure

1. Click **Add**.
2. Enter the details:

Name

Priority

Assignment

Input Reserved and Max Bandwidth

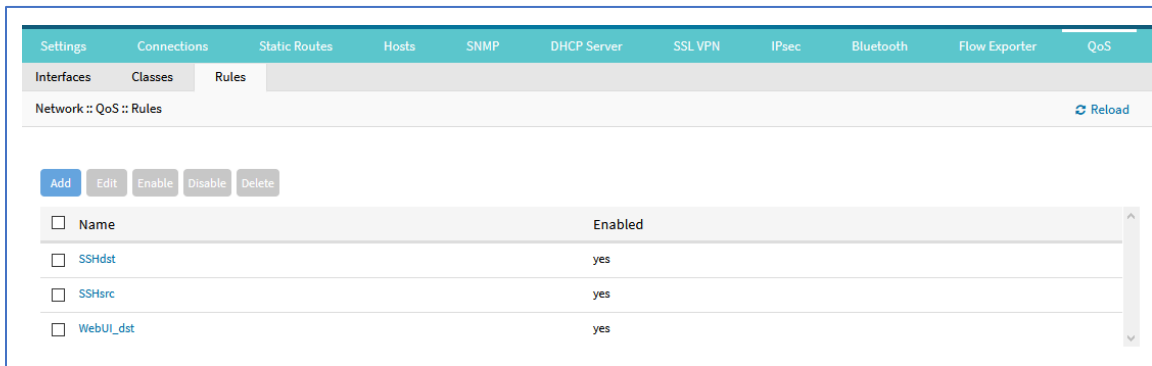
Output Reserved and Max Bandwidth

3. 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.

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.



Add a Rule

WebUI Procedure

1. Click **Add**.
2. Enter the details:

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](http://www.iana.org).

Source and Destination IP

Source and Destination Port

Source and Destination MAC

Custom Parameters

Assignment

3. Click **Save**.

NOTE: All parameters in a rule will be applied as an “AND” operation.

For all fields that support multiple values, enter comma separated values. Numeric fields support ranges, separated with a dash (i.e., 22-100).

Managed Devices Section

In this section, users can configure, create, and delete target devices. The Nodegrid Platform supports target devices connected through a serial, USB, or network connection.

General Information

Supported Protocols

The following protocols are currently supported for network-based devices:

- Telnet
- SSH
- HTTP/S
- IPMI variations
- SNMP

The user has multiple options to manage target devices (enable, create, add). These can be done manually or automatically discover.

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, status of any devices that exceed the total licenses is changed to “Unlicensed”. The System maintains information on unlicensed devices but are now shown on the Access page. Only licensed devices are listed and available for access and management. On the Managed Devices page, upper right, total licenses, total in-use, and total available is shown. See “Licenses” for more details.

Device Types

These managed device types are supported:

- Console connections utilizing RS232 protocol.
 - Nodegrid Console Servers
 - Nodegrid Net Services Routers
- Service Processor Devices using:
 - IPMI 1.5

IPMI 2.0

HP iLO

Oracle/SUN iLOM

IBM IMM

Dell DRAC

Dell iDRAC

- Console Server connections utilizing SSH protocol
- Console Server connections utilizing
 - 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 utilizing
 - 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

Configure Serial Connections

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 target 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.

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click on the port – or select the port and click **Edit**.

Multiple ports can be selected.

The screenshot shows the Nodegrid web interface for configuring a device. The breadcrumb trail is: Managed Devices > Devices :: ttyS2 :: Access. The configuration form includes the following fields and options:

- Name:** ttyS2
- Local Serial Port:** ttyS2
- Type:** local_serial
- Address Location:** [Empty field]
- Coordinates (Lat, Lon):** [Empty field]
- WEB URL:** [Empty field]
- Launch URL via HTML5**
- 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
- Enable Hostname Detection
- Multisession**
- Read-Write Multisession
- Icon:** Select icon
- Mode:** Disabled

3. Enter values for:

Baud Rate (set to speed matching target device settings, or to Auto)

Parity (None (default), Odd, 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)

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings” for more details.

CLI Procedure

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 target 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)

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings” for more details.

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
```

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 the target device. This can be without dedicated network interface on Nodegrid, or through an existing network connection.

These features are available:

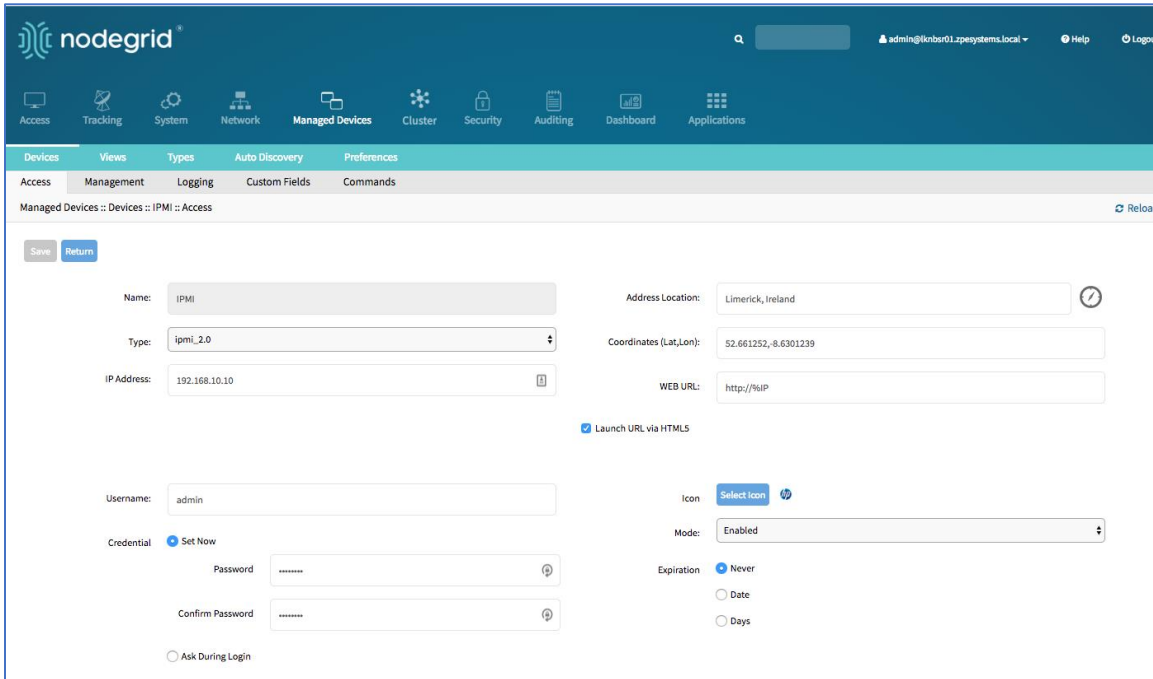
- Serial Over LAN (SOL)
- Web Interface
- KVM sessions
- Virtual Media
- Data Logging
- Event Logging
- Power Control (through Rack PDU)

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).

WebUI Procedure

1. Go to *Managed Devices :: Devices*,
2. Click **Add**.



3. Enter the **Name** (of the server).
4. In the **Type** drop-down, select type (ipmi1.5, ipmi2.0, ilo, ilom, imm, drac, idrac6, intel_bmc)
5. Enter **IP Address** (make sure it is reachable by the Nodegrid Platform).
6. Enter **Username**.
7. Enter **Password** and **Confirm Password**.

Alternatively, select **Ask During Login** checkbox (user credentials are entered during login).

8. Click **Save**.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See "Device Settings".

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 (ipmi1.5, ipmi2.0, ilo, ilom, imm, drac, idrac6)
 - ip_address
 - username and password (of service processor)
 - or set credential ask_during_login
4. Save the changes with commit.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings” for more details.

```
[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
```

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
```

Device Management with SSH

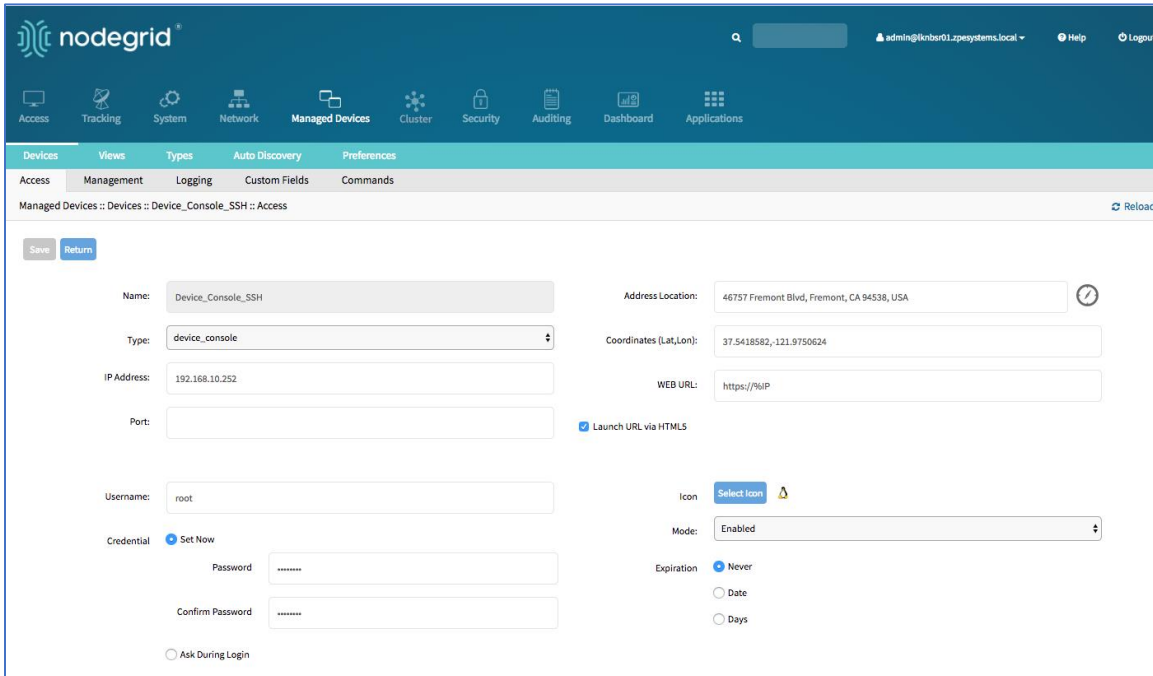
Management of target devices through SSH is supported:

These features are available:

- Console Session
- Data Logging
- Custom Commands
- Web Sessions
- Power Control through Rack PDU

WebUI Procedure

1. Go to *Managed Devices :: Devices*,
2. Click **Add**.



3. Enter **Name** (of the server).
4. In the **Type** drop-down, select type (device_console).
5. Enter **IP Address** (make sure it is reachable by the Nodegrid Platform).
6. Enter **Username**
7. Enter **Password** and **Confirm Password**.

Alternatively, select **Ask During Login** checkbox (user credentials are entered during login).

8. Click **Save**.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See "Device Settings".

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
 - name alias
 - type (device_console)

ip_address

username and password (of the device)
or set credential ask_during_login

4. Save the changes with commit

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings”

```
[admin@nodegrid /]# cd /settings/devices
[admin@nodegrid devices]# add
[admin@nodegrid {devices}]# set name=Device_Console_SSH
[admin@nodegrid {devices}]# set name_alias=aliasname
[admin@nodegrid {devices}]# set type=device_console
[admin@nodegrid {devices}]# set ip_address=192.168.10.252
[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
```

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.

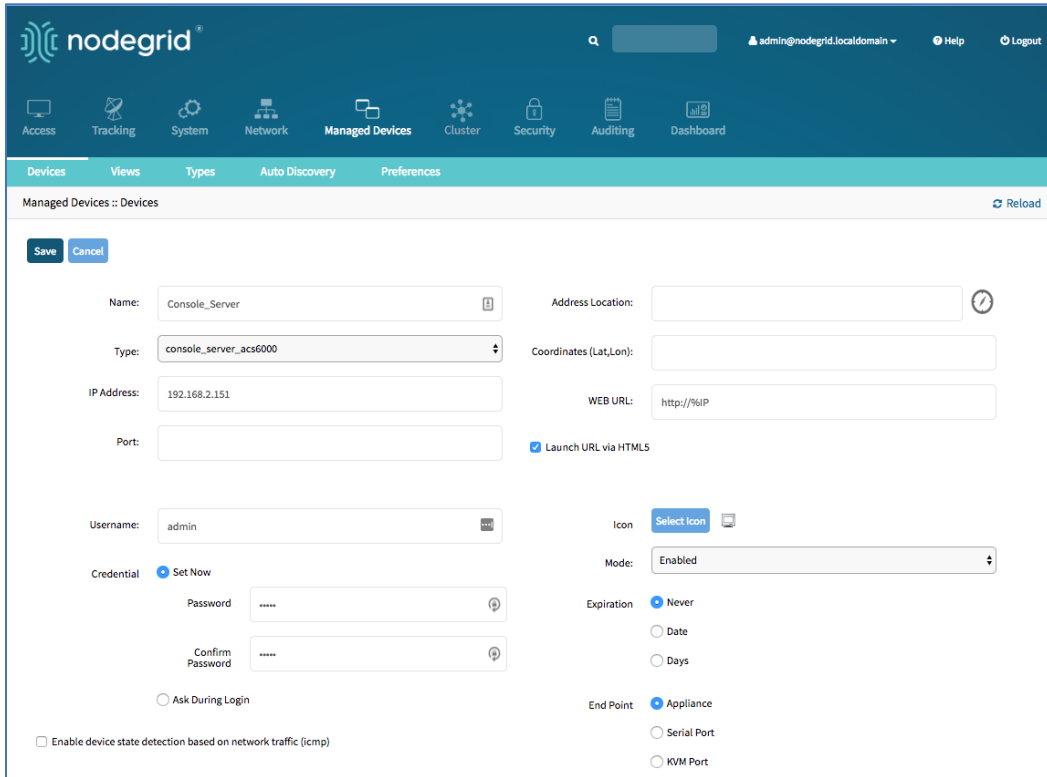
These features are available:

- Console Session
- Data Logging
- Custom Commands
- Web Sessions
- Power Control through Rack PDU

Step 1 – Add Third-Party Console Servers

WebUI Procedure

1. Go to *Managed Devices :: Devices*,
2. Click **Add**.



3. Enter **Name** (of the console server).
4. In the **Type** drop-down, select type (console_server_nodegrid, console_server_acs, console_server_acs6000, console_server_lantronix, console_server_opengear, console_server_digicp, console_server_raritan, console_server_perle)
5. Enter **IP Address** (make sure the IP address is reachable by the Nodegrid Platform).
6. Enter **Username**
7. Enter **Password** and **Confirm Password**.
Alternatively, select **Ask During Login** checkbox (user credentials are entered during login).
8. For **End Point**, select **Appliance** radio button.
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

username and password (of the device)
or set credential ask_during_login

endpoint (appliance)

4. Save the changes with commit

```
[admin@nodegrid /]# cd /settings/devices
[admin@nodegrid devices]# add
[admin@nodegrid {devices}]# set name=Console_Server
[admin@nodegrid {devices}]# set type=console_server_acs6000
[admin@nodegrid {devices}]# set ip_address=192.168.2.151
[admin@nodegrid {devices}]# set end_point = appliance
[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
```

Step 2 – Add Third Party Console Server Ports

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click **Add**.

3. Enter the **Name** (of the console server port).
4. In the **Type** drop-down, select type (console_server_nodegrid, console_server_acs, console_server_acs6000, console_server_lantronix, console_server_opengear, console_server_digicp, console_server_raritan, console_server_perle)
5. Enter **IP Address** (make sure it is reachable by the Nodegrid Platform).
6. Enter **Username**
7. Enter **Password** and **Confirm Password**.
Alternatively, select **Ask During Login** checkbox (user credentials are entered during login).
8. For **End Point**, select **Serial Port** radio button.
9. Enter **Port Number**.
10. Click **Save**.

NOTE: Ports can be automatically detected and added. See “Auto-Discovery” for more details.

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

username and password (of the device)
or set credential ask_during_login

endpoint (serial_port)

port_number (port number)

4. Save the changes with commit

NOTE: Ports can be automatically detected and added. See “Auto-Discovery” for details.

```
[admin@nodegrid /]# cd /settings/devices
[admin@nodegrid devices]# add
[admin@nodegrid {devices}]# set name=Console_Server_Port_5
[admin@nodegrid {devices}]# set type=console_server_acs6000
[admin@nodegrid {devices}]# set ip_address=192.168.2.151
[admin@nodegrid {devices}]# set end_point = serial_port
[admin@nodegrid {devices}]# set port_number = 5
[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
```

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.

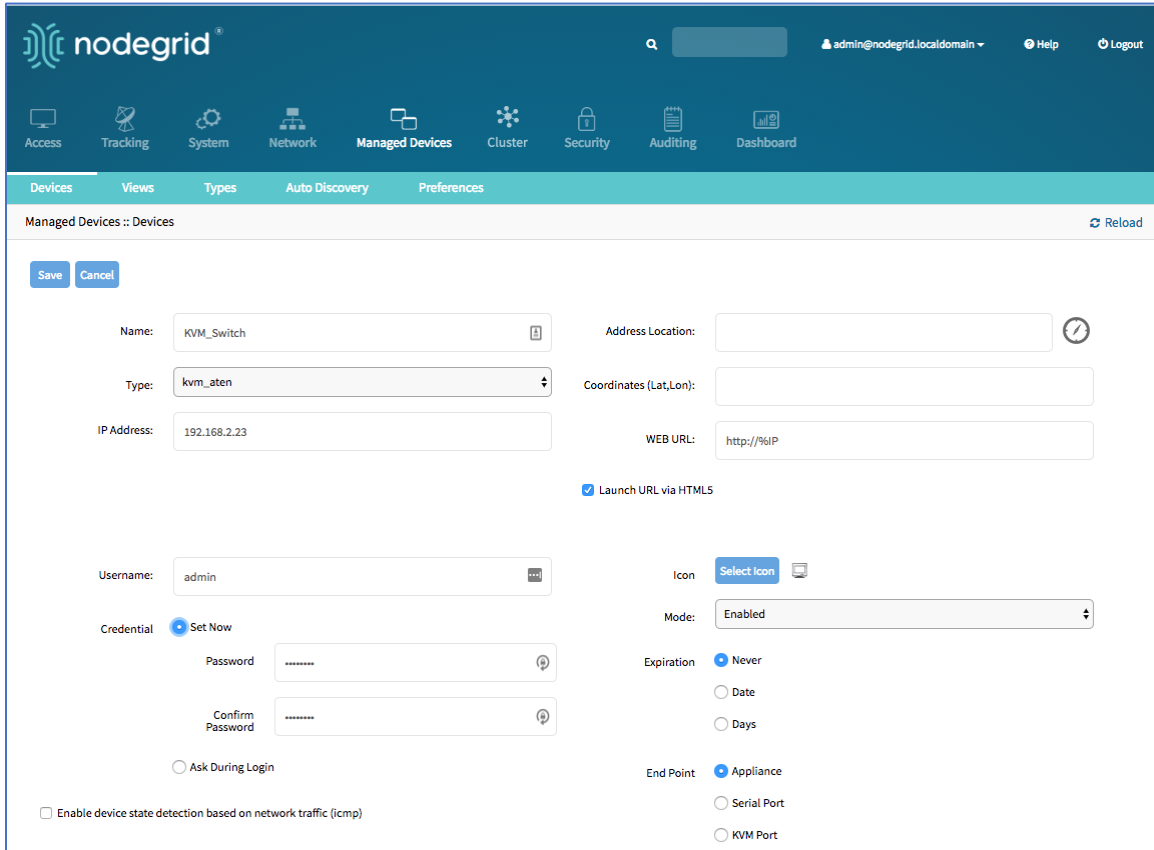
These features are available:

- KVM Session
- Web Sessions
- Power Control through Rack PDU

Step 1 – Add KVM Switches

WebUI Procedure

1. Go to *Managed Devices :: Devices*,
2. Click **Add**.



3. Enter the **Name** (of the KVM switch).
4. In the **Type** drop-down, select type (kvm_dsr, kvm_mpu, kvm_aten, kvm_raritan)
5. Enter **IP Address** (make sure it is reachable by the Nodegrid Platform).
6. Enter **Username**
7. Enter **Password** and **Confirm Password**.
Alternatively, select **Ask During Login** checkbox (user credentials are entered during login).
8. For **End Point**, select **Appliance** radio button.
9. Click **Save**.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See "Device Settings".

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 (kvm_dsr, kvm_mpu, kvm_aten, kvm_raritan)

ip_address

username and password (of the device)
or set credential ask_during_login

endpoint (appliance)

4. Save the changes with commit

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings”.

```
[admin@nodegrid /]# cd /settings/devices
[admin@nodegrid devices]# add
[admin@nodegrid {devices}]# set name=KVM_Switch
[admin@nodegrid {devices}]# set type=kvm_aten
[admin@nodegrid {devices}]# set ip_address=192.168.2.151
[admin@nodegrid {devices}]# set end_point = appliance
[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
```

Step 2 – Add KVM Switch Ports

WebUI Procedure

1. Go to *Managed Devices :: Devices*,
2. Click **Add**.

3. Enter the **Name** (of the KVM switch port).
4. In the **Type** drop-down, select type (kvm_dsr, kvm_mpu, kvm_aten, kvm_raritan)
5. Enter **IP Address** (make sure it is reachable by the Nodegrid Platform).
6. Enter **Username**
7. Enter **Password** and **Confirm Password**.
Alternatively, select **Ask During Login** checkbox (user credentials are entered during login).
8. For **End Point**, select **KVM Port** radio button.
9. Enter **Port Number**.
10. Click **Save**.

NOTE: Ports can be automatically detected and added see “Auto-Discovery” for details.

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 (kvm_dsr, kvm_mpu, kvm_aten, kvm_raritan)

ip_address

username and password (of the device)
or set credential ask_during_login

endpoint (kvm_port)

port_number (port number)

4. Save the changes with commit

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings”.

NOTE: Ports can be automatically detected and added. See “Auto Discovery” for details.

```
[admin@nodegrid /]# cd /settings/devices
[admin@nodegrid devices]# add
[admin@nodegrid {devices}]# set name=Console_Server_Port_5
[admin@nodegrid {devices}]# set type=kvm_aten
[admin@nodegrid {devices}]# set ip_address=192.168.2.151
[admin@nodegrid {devices}]# set end_point = kvm_port
[admin@nodegrid {devices}]# set port_number = 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}]# commit
```

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 target devices, allowing direct control of specific power outlets for this target device.

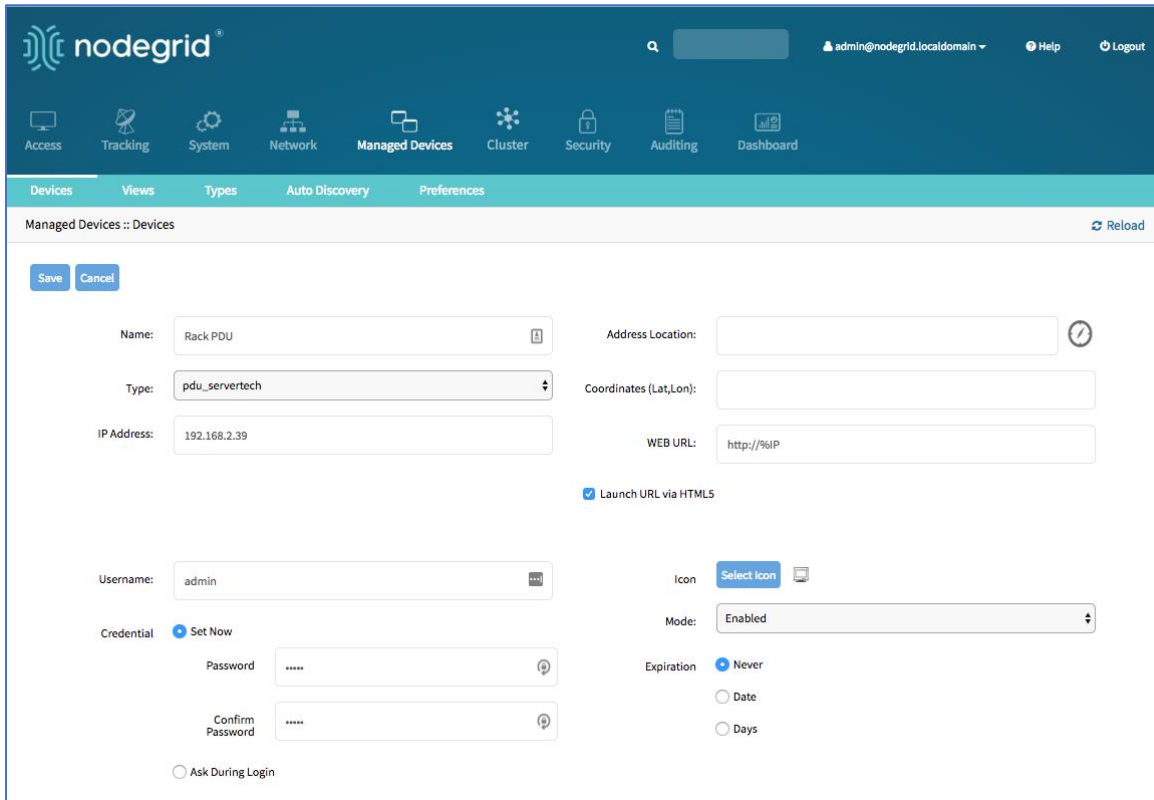
These features are available:

- 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.

WebUI Procedure

1. Go to *Managed Devices :: Devices*,
2. Click **Add**.



3. Enter the **Name** (of the Rack PDU).
4. In the **Type** drop-down, select type (pdu_apc, pdu_baytech, pdu_eaton, pdu_mph2, pdu_pm3000, pdu_cpi, pdu_raritan, pdu_geist, pdu_servertech, pdu_enconnex, pdu_cyberpower, pdu_rittal)
5. Enter **IP Address** (make sure it is reachable by the Nodegrid Platform).
6. Enter **Username**
7. Enter **Password** and **Confirm Password**.

Alternatively, select **Ask During Login** checkbox (user credentials are entered during login).

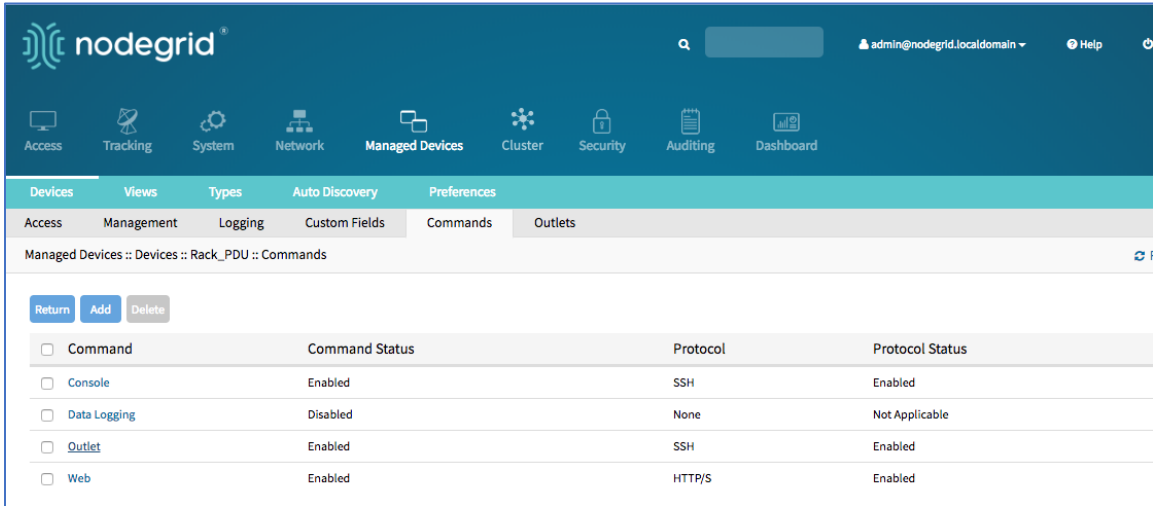
8. Click **Save**.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See "Device Settings".

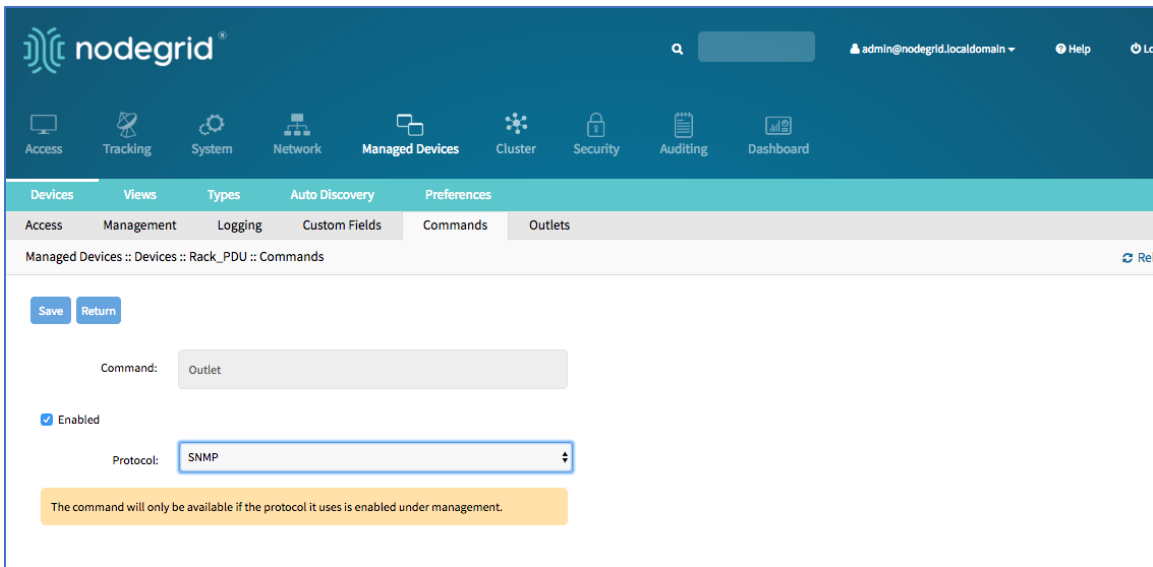
NOTE: By default, Nodegrid communicates with the Rack PDU with SSH/telnet. The reaction time is typically very slow. If possible, use SNMP to communicate with the Rack PDU.

WebUI – Change Communication to SNMP

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**.



4. On the new page, change **Protocol** to **SNMP**.
Click **Save**.

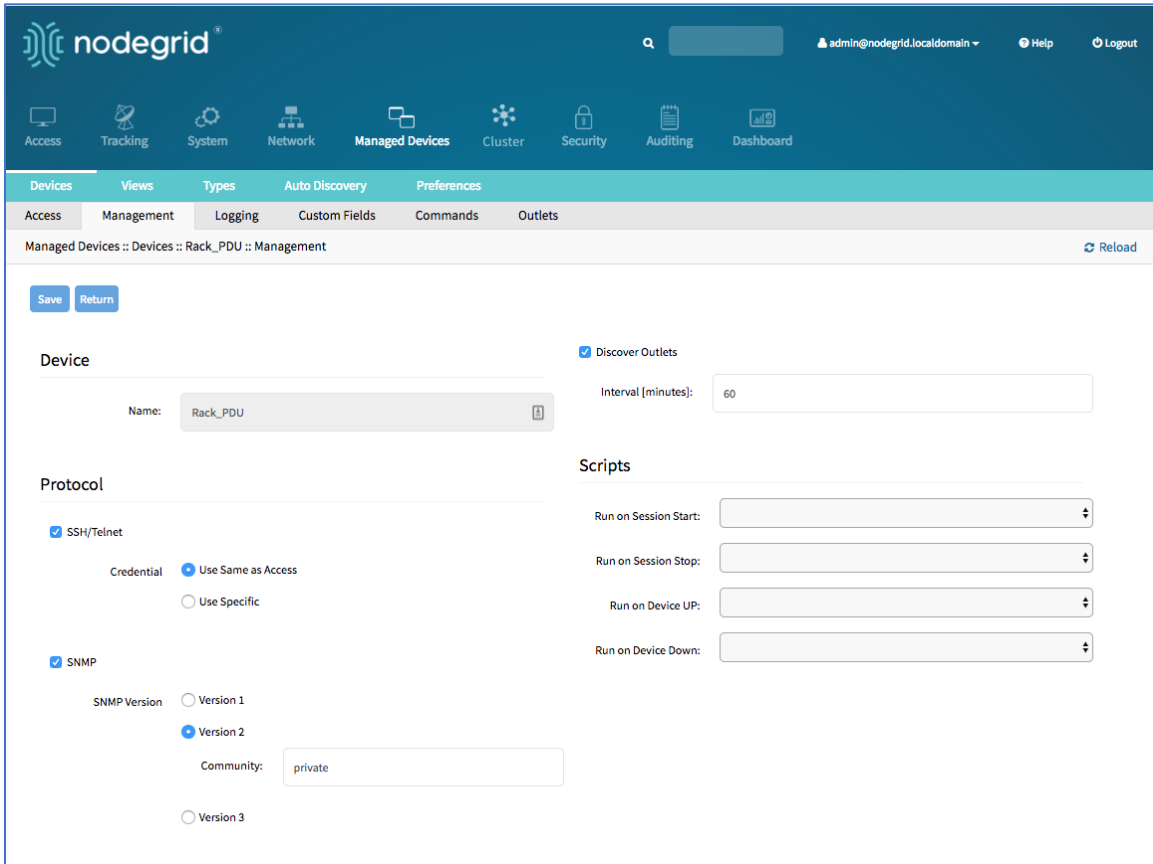


5. On the **Management** tab:

In the *SNMP* menu, update values to match the settings on the Rack PDU (see manufacturer’s manual).

Click **Save**.

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).

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 (pdu_apc, pdu_baytech, pdu_eaton, pdu_mph2, pdu_pm3000, pdu_cpi, pdu_raritan, pdu_geist, pdu_servertech, pdu_enconnex, pdu_cyberpower, pdu_rittal)

ip_address

username and password (of the device)
or set credential ask_during_login

endpoint should be defined as appliance

4. Save the changes with commit

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings”.

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.

CLI – Change Communication to SNMP

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
```

Cisco UCS

Management of Cisco UCS is supported through Console Ports, as well as management interfaces.

These features are available:

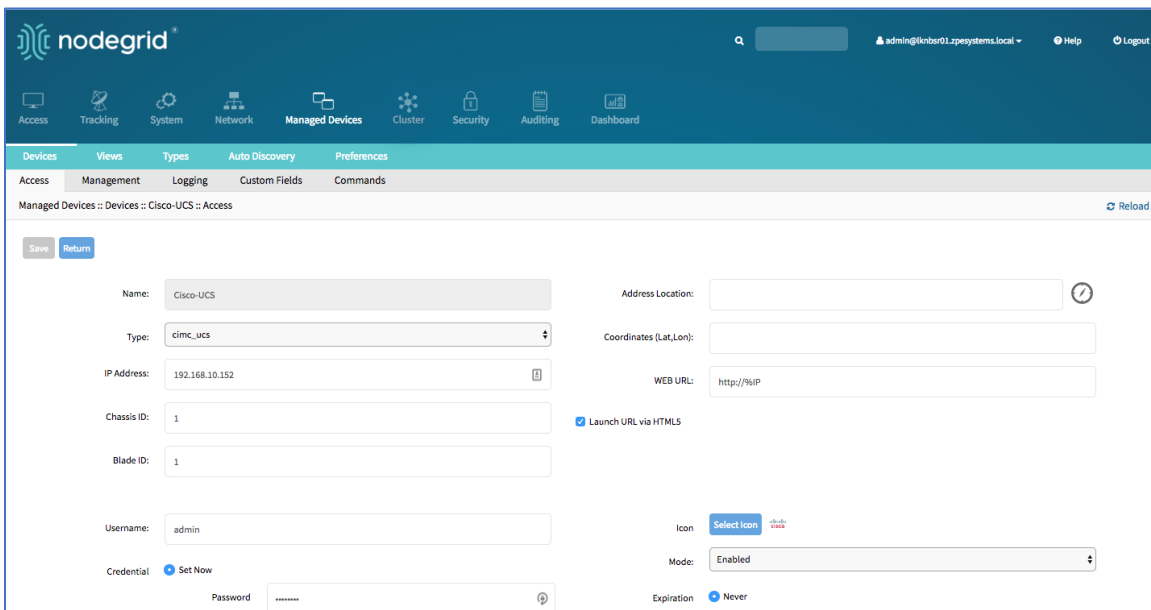
- Console Session
- Data Logging

- Event Logging
- Power Control through Cisco UCS appliance
- Web Session
- Custom Commands

Add Cisco UCS

WebUI Procedure

1. Go to *Managed Devices :: Devices*,
2. Click **Add**.



The screenshot shows the Nodegrid WebUI interface for adding a new device. The breadcrumb path is 'Managed Devices :: Devices :: Cisco-UCS :: Access'. The form contains the following fields and options:

- Name:** Cisco-UCS
- Type:** cimc_ucs (selected from a dropdown)
- IP Address:** 192.168.10.152
- Chassis ID:** 1
- Blade ID:** 1
- Username:** admin
- Credential:** Set Now (radio button selected)
- Password:** [Redacted]
- Address Location:** [Empty field]
- Coordinates (Lat,Lon):** [Empty field]
- WEB URL:** http://%IP
- Launch URL via HTML5:**
- Icon:** Select icon (dropdown menu)
- Mode:** Enabled (dropdown menu)
- Expiration:** Never (radio button selected)

3. Enter the **Name** (of the Cisco UCS Blade).
4. In the **Type** drop-down, select type (cimc_ucs).
5. Enter **IP Address** (make sure it is reachable by the Nodegrid Platform).
6. Enter **Chassis ID**.
7. Enter **Blade ID**.
8. Enter **Username**
9. Enter **Password** and **Confirm Password**.

Alternatively, select **Ask During Login** checkbox (user credentials are entered during login).

10. Click **Save**.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See "Device Settings".

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 (of the blade)

type (cimc_ucs)

ip_address

chassis_id

blade_id

username and password (of the device)

or set credential ask_during_login

4. Save the changes with commit.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings”.

```
[admin@nodegrid /]# cd /settings/devices
[admin@nodegrid devices]# add
[admin@nodegrid {devices}]# set name=Cisco-UCS
[admin@nodegrid {devices}]# set type=cimc_ucs
[admin@nodegrid {devices}]# set ip_address=192.168.10.151
[admin@nodegrid {devices}]# set chassis_id=1 blade_id=1s
[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
```

Netapp

Netapp appliances are supported through their management interfaces.

These features are available:

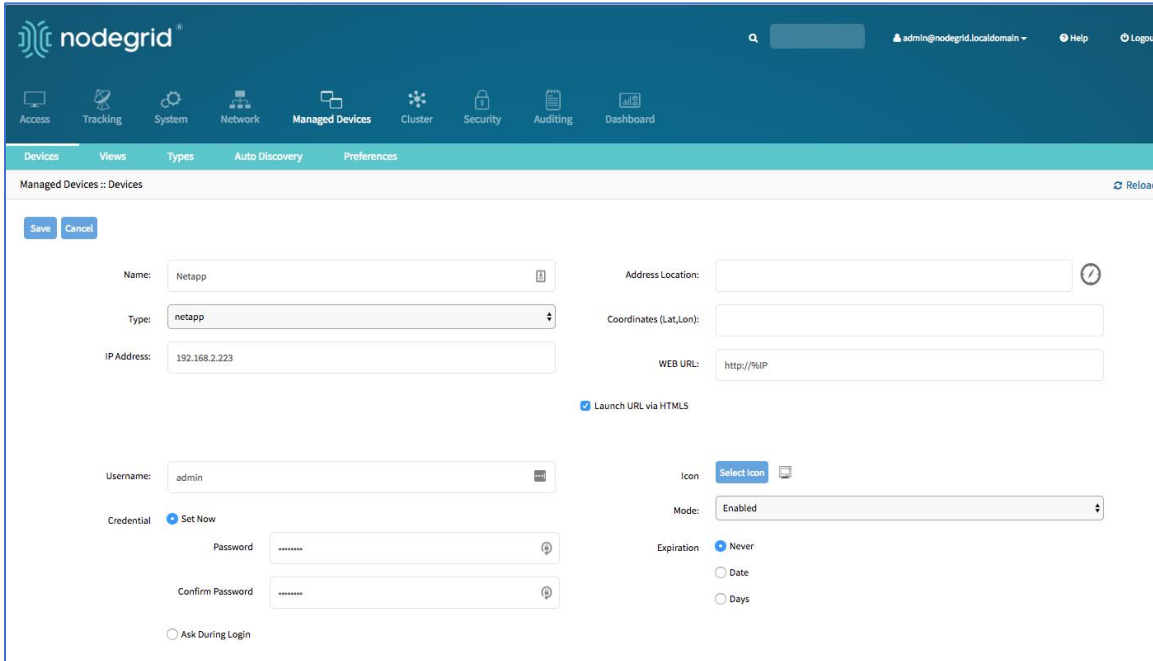
- Console Session
- Data Logging
- Event Logging
- Power Control through Netapp appliance
- Web Session

- Custom Commands
- Power Control through Rack PDU

Add Netapp

WebUI Procedure

1. Go to *Managed Devices :: Devices*,
2. Click **Add**.



The screenshot shows the 'Managed Devices :: Devices' page in the Nodegrid WebUI. The form is for adding a new device of type 'netapp'. The fields are filled with the following information:

- Name:** Netapp
- Type:** netapp
- IP Address:** 192.168.2.223
- Address Location:** (empty)
- Coordinates (Lat, Lon):** (empty)
- WEB URL:** http://%iP
- Launch URL via HTML5:**
- Username:** admin
- Credential:** Set Now
 - Password:** (masked)
 - Confirm Password:** (masked)
- Ask During Login:**
- Icon:** Select icon
- Mode:** Enabled
- Expiration:** Never
 - Date
 - Days

3. Enter the **Name**.
4. In the **Type** drop-down, select type (netapp).
5. Enter **IP Address** (make sure it is reachable by the Nodegrid Platform).
6. Enter **Password** and **Confirm Password**.
Alternatively, select **Ask During Login** checkbox (user credentials are entered during login).
7. Click **Save**.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See "Device Settings".

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 (netapp)
ip_address
username and password (of the device)
or set credential ask_during_login

4. Save the changes with commit

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings”.

```
[admin@nodegrid /]# cd /settings/devices
[admin@nodegrid devices]# add
[admin@nodegrid {devices}]# set name=Netapp
[admin@nodegrid {devices}]# set type=netapp
[admin@nodegrid {devices}]# set ip_address=192.168.10.250
[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
```

Infrabox

Smart Access Control is supported for Rack's solution appliances (Infrabox) from InfraSolution. Communication requires SNMP to be configured.

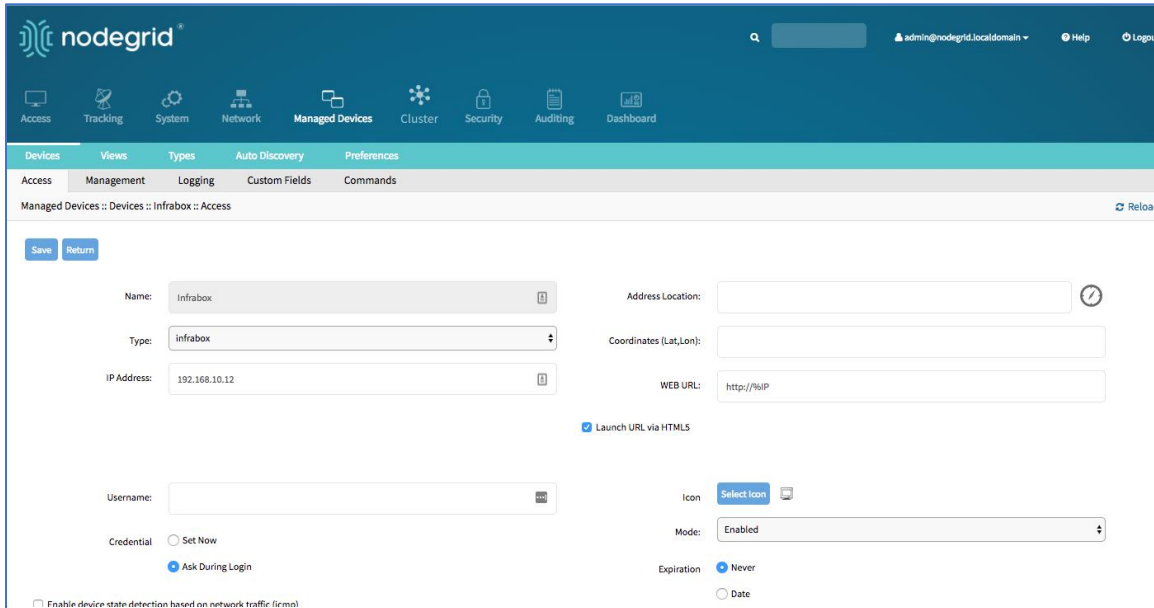
These features are available:

- Door Control
- Web Session
- Power Control through Rack PDU

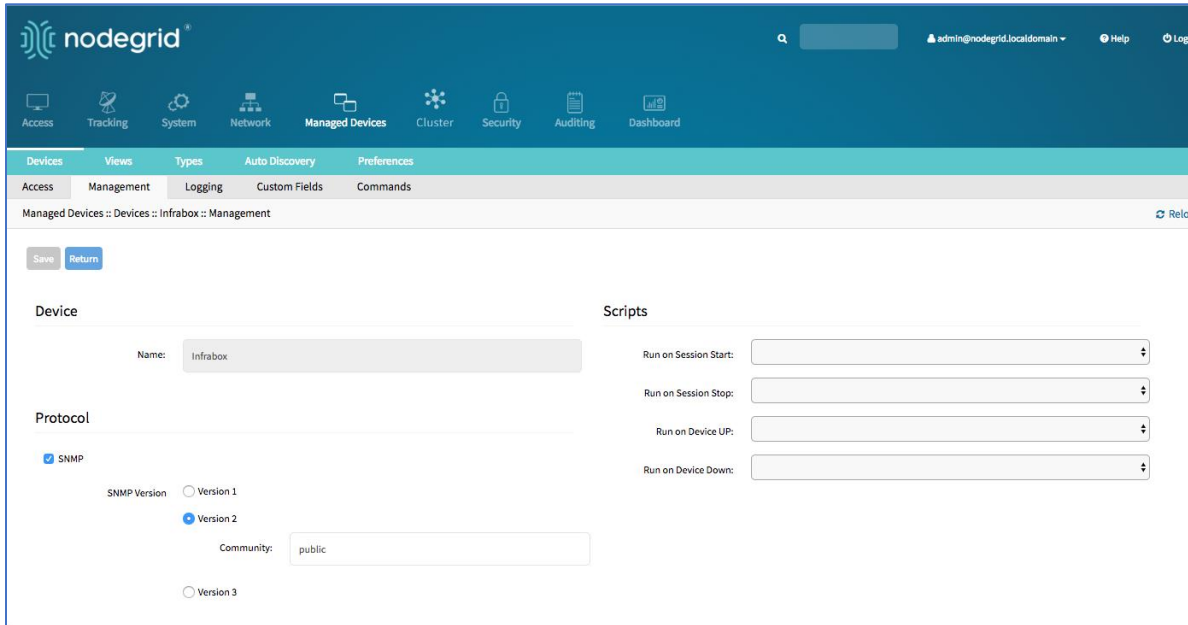
Add Infrabox

WebUI Procedure

1. Go to *Managed Devices :: Devices*,
2. Click **Add**.



3. Enter **Name**.
4. In the **Type** drop-down, select type (infrabox).
5. Enter **IP Address** (make sure it is reachable by the Nodegrid Platform).
6. Enter **Password** and **Confirm Password**.
Alternatively, select **Ask During Login** checkbox (user credentials are entered during login).
7. Click **Save**.
Optional: Settings which control the display and behavior of the device can be adjusted at this time. See "Device Settings".
8. On the **Management** tab
Update the SNMP values to match the appliance settings.
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 (infrabox)
ip_address
username and password (of the device)
or set credential ask_during_login
```

4. Save the changes with commit

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings”.

5. Go to /settings/devices/<Device>/management/
6. Use the set command to define SNMP values:

```
snmp_version
snmp_community
```

7. Save the changes with commit.

```
[admin@nodegrid /]# cd /settings/devices
[admin@nodegrid devices]# add
[admin@nodegrid {devices}]# set name=Infrabox
[admin@nodegrid {devices}]# set type=infrabox
```



```
[admin@nodegrid {devices}]# set ip_address=192.168.10.250
[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 outlet]# cd /settings/devices/Infrabox/management/
[admin@nodegrid management]# set snmp=yes
[+admin@nodegrid management]# snmp_version=v2
[+admin@nodegrid management]# snmp_community=private
[+admin@nodegrid management]# commit
```

Virtual Machines

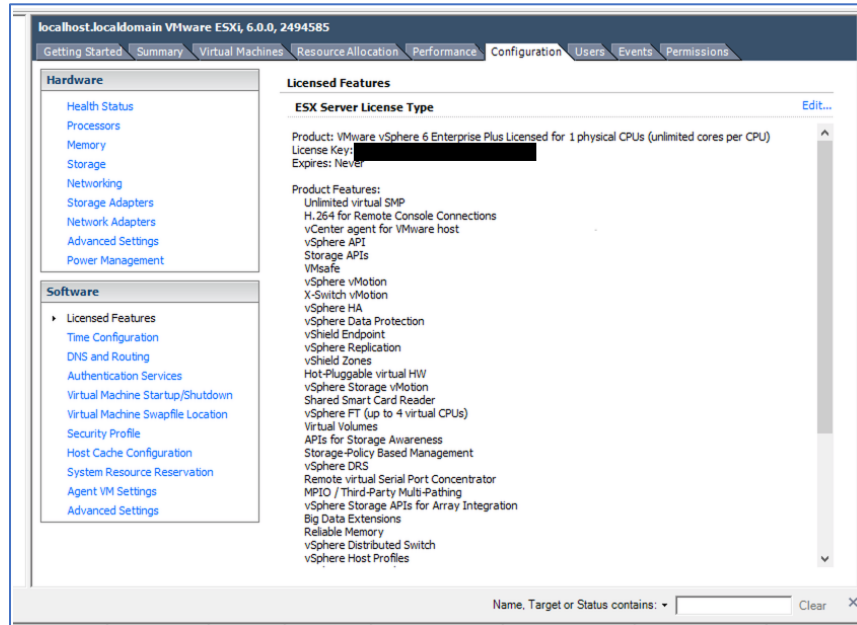
Management of VMware virtual machines are supported, including KVM Virtual Machines.

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.



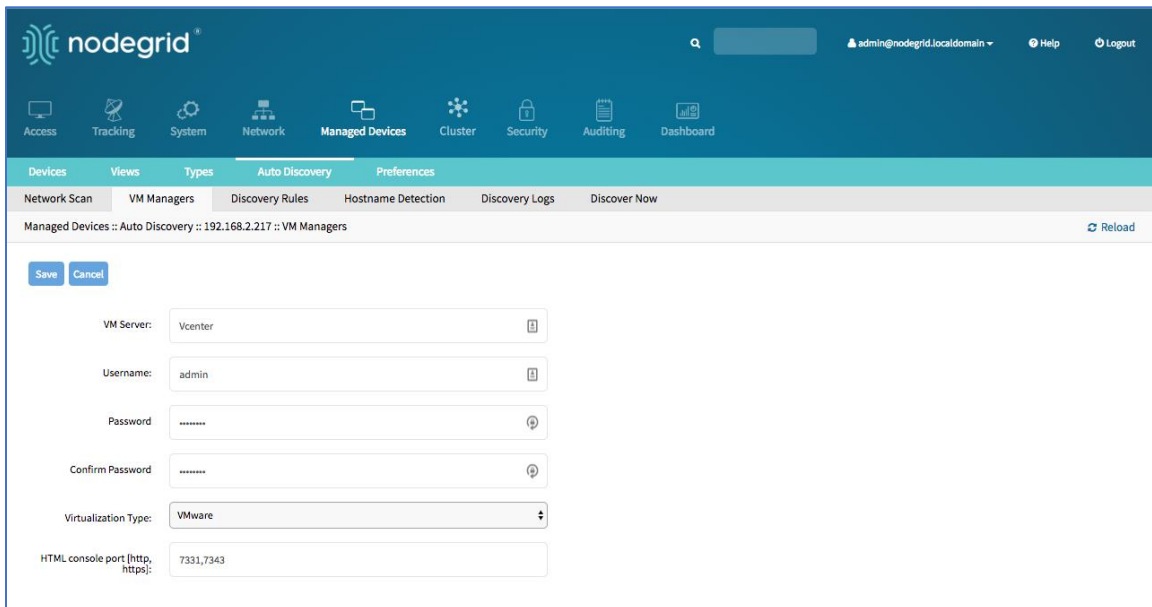
NOTE: To utilize the vSPC option with VMware virtual machines, the port must be configured on the Virtual Machine. See “Configuring Virtual Serial Port (vSPC)”.

Configure Auto Discovery of VMware Virtual Machine

Step 1 – Add VMware Virtual Machine

Step 1 – WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: VM Managers*.
2. Click **Add**.



3. In **VM Server**, enter *vCenter/ESXi IP or FQDN*.

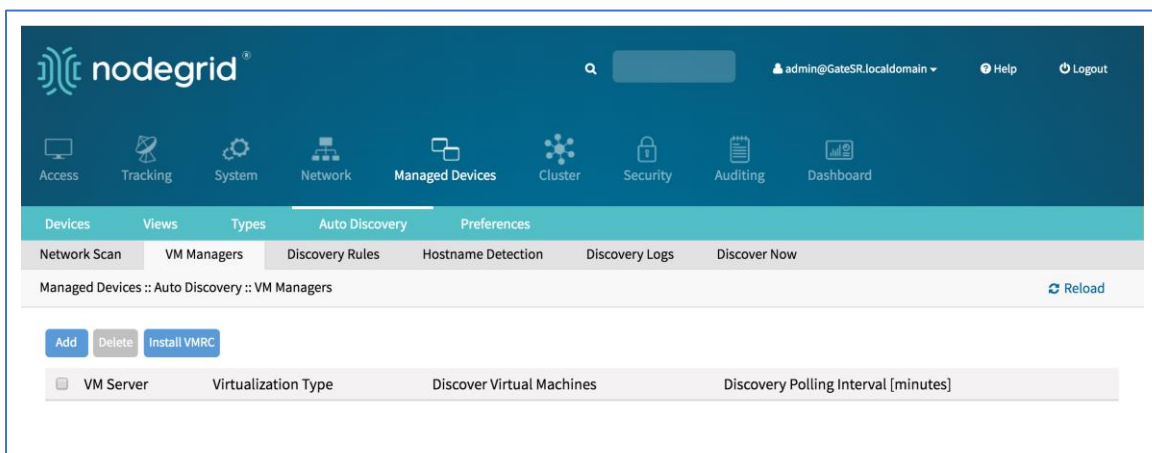
4. Enter **Username**.
5. Enter **Password** and **Confirm Password**.
6. (if needed) Enter **HTML console port**.
7. Click **Save**.

Step 2 – install VMRC

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: VM Managers*.
2. Click **Install VMRC**.

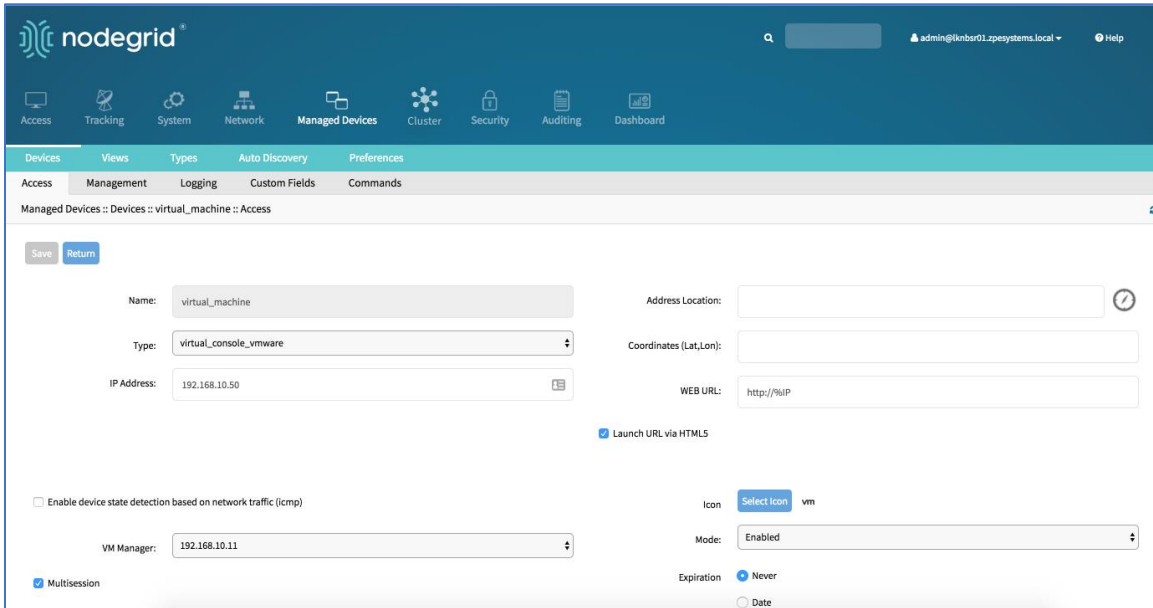
This sets up graphical device connections and console access to virtual machines.



Step 3 –Add VMware virtual machine

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click **Add**.



3. Enter **Name** (of the Virtual Machine).
This must match the Hypervisor Name.
4. In the **Type** drop-down, select type (virtual_console_vmware).
5. (optional) Enter **IP Address**.
6. In **VM Manager** drop-down, select the correct hypervisor.
7. Click **Save**.

CLI Procedure – define VM Manager

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)
username and password (of the device)
or set credential ask_during_login
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
```

CLI Procedure – add VMware Virtual Machine

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)

(optional) ip_address

vm_manager (existing VM Manager)

4. Save the changes with commit

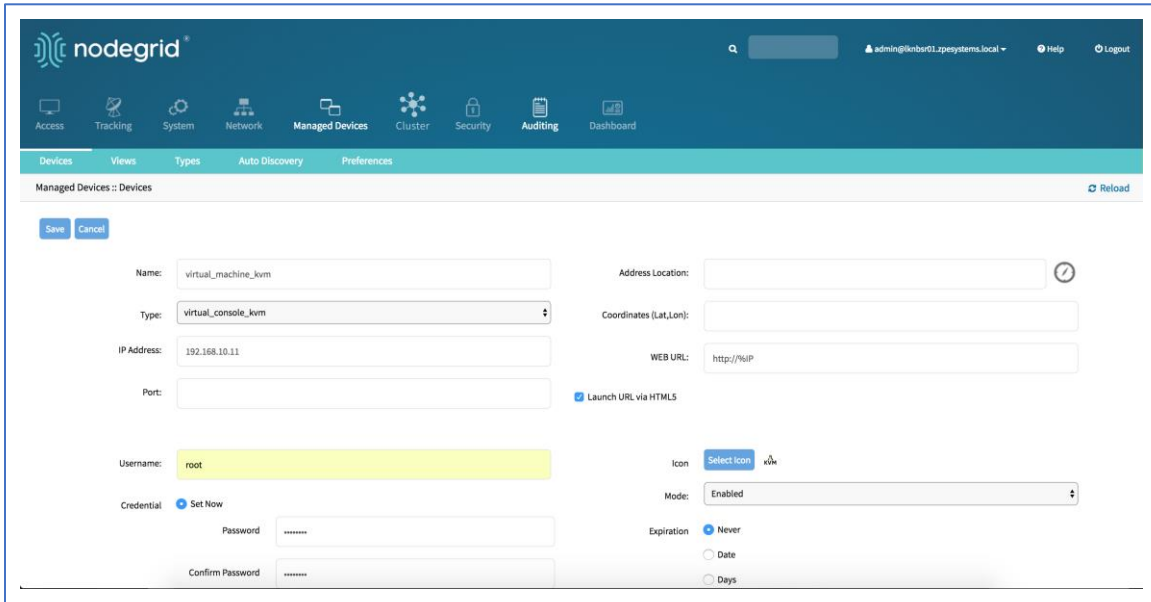
Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings”.

```
[admin@nodegrid /]# cd /settings/devices
[admin@nodegrid devices]# add
[admin@nodegrid {devices}]# set name=Virtual_Machine
[admin@nodegrid {devices}]# set type=virtual_console_vmware
[admin@nodegrid {devices}]# set ip_address=192.168.2.151
[admin@nodegrid {devices}]# set vm_manager=192.168.10.11
[admin@nodegrid {devices}]# commit
```

Add KVM Virtual Machine

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click **Add**.



3. Enter **Name**.
Must match the hypervisor name.
4. In the **Type** drop-down, select type (virtual_console_kvm).
5. Enter **IP Address**.
6. Enter **Username**.
7. Enter **Password** and **Confirm Password**.
8. Click **Save**.

CLI Procedure

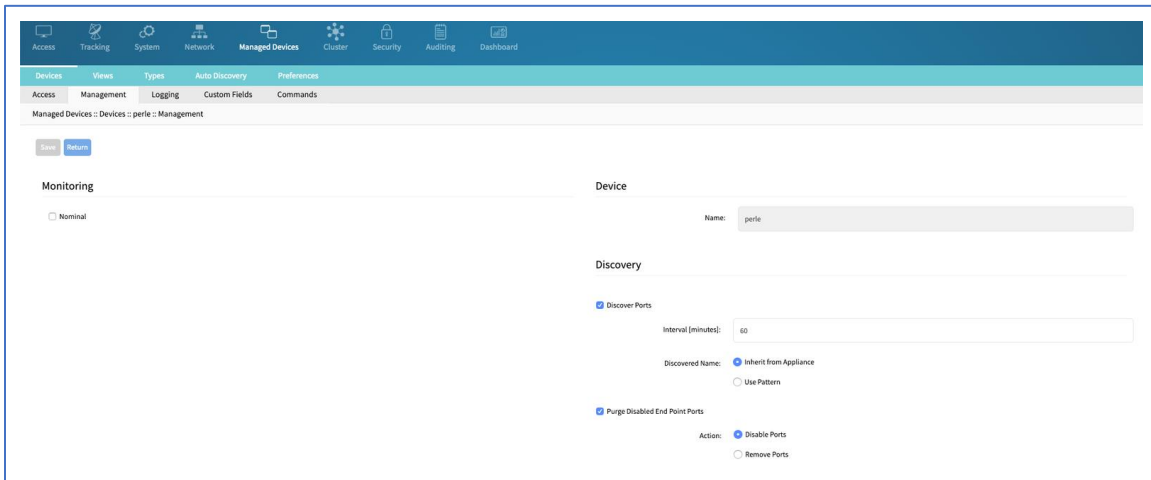
1. Go to /settings/devices
2. Use the add command to create a new device.
3. Use the set command to define the following settings:
name (must match the machine's hypervisor name)
type (virtual_console_kvm)
ip_address
username (for KVM hypervisor)
password (for KVM hypervisor)
4. Save the changes with commit.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See "Device Settings".

```
[admin@nodegrid /]# cd /settings/devices
```

```
[admin@nodegrid devices]# add
[admin@nodegrid {devices}]# set name=virtual_machine_kvm
[admin@nodegrid {devices}]# set type=virtual_console_vmware
[admin@nodegrid {devices}]# set ip_address=192.168.10.11
[admin@nodegrid {devices}]# set username=root
[admin@nodegrid {devices}]# set password=password
[admin@nodegrid {devices}]# commit
```

Device Management



On the **Management** tab, the following settings are available:

- *Monitoring* menu (enable/disable Nominal monitoring)
- *Device* menu (Name of the device)
- *Discovery* menu
 - Discovery Ports (enable/disable)
 - Interval (minutes)
 - Discovered Name (options to *Inherit from Appliance* or *Use Pattern*)
 - Purge Disabled End Point Ports (options are *Disable Ports* or *Remove Ports*)

Authenticate with SSH Keys

For added security, devices can be configured to authenticate via SSH keys. When enabled, The 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 :: <nameofdevice> :: Access.*

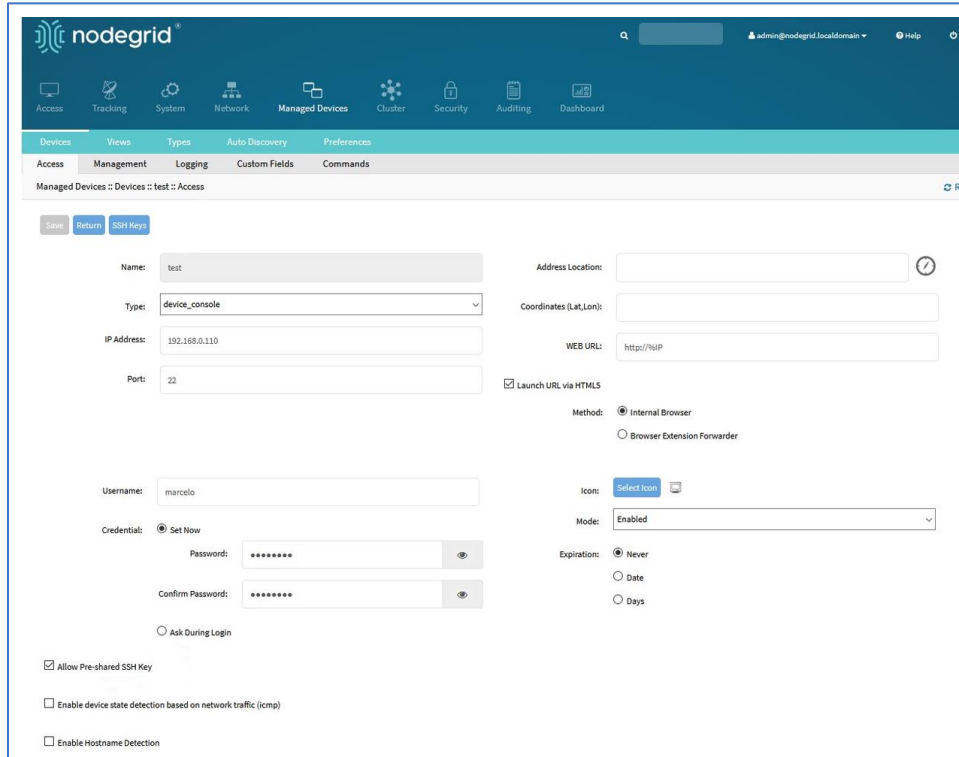
2. Select **Allow Pre-shared SSH Key** checkbox.
3. Click **Save**.

The SSH Keys button will now appear next to the Save and Return buttons.

Generate a new SSH Key

WebUI Procedure

1. Click **SSH Keys**.



The screenshot shows the Nodegrid WebUI interface for configuring an SSH key. The breadcrumb trail is: Managed Devices > Devices > test > Access. The form contains the following fields and options:

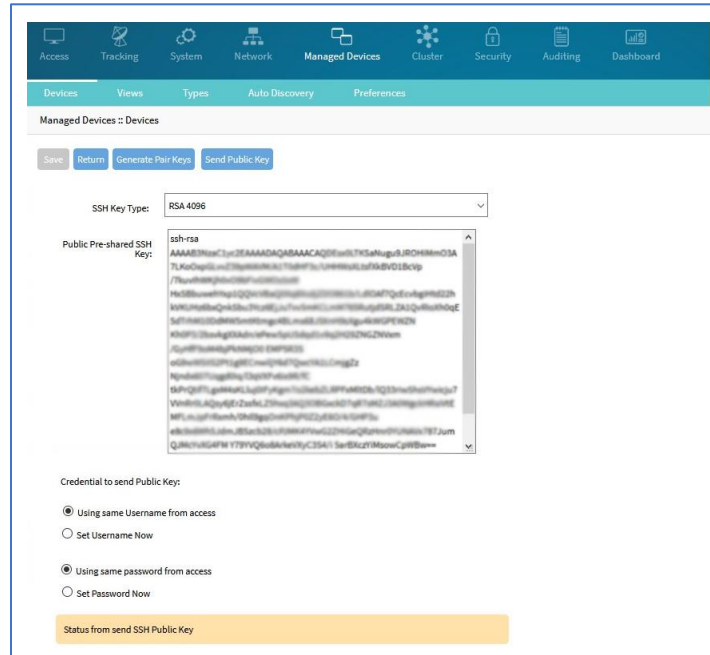
- Name:** test
- Type:** device_console (dropdown menu)
- IP Address:** 192.168.0.110
- Port:** 22
- Address Location:** (empty field)
- Coordinates (Lat, Lon):** (empty field)
- WEB URL:** http://%IP
- Launch URL via HTML5:**
- Method:** Internal Browser (selected), Browser Extension Forwarder
- Icon:** Select Icon (button)
- Mode:** Enabled (dropdown menu)
- Expiration:** Never (selected), Date, Days
- Credential:** Set Now (selected), Ask During Login
- Password:** (masked with dots)
- Confirm Password:** (masked with dots)
- Allow Pre-shared SSH Key:**
- Enable device state detection based on network traffic (icmp):**
- Enable Hostname Detection:**

2. On **SSH Key Type** drop-down, select type.
3. Click **Generate Pair Keys**.

NOTE: The same username and password as the current account can be used. Alternatively, these can be set now (at the bottom of the page).

4. Click **Send Public Key** . This sends the key to the device.

NOTE: Not all devices support the Send Public Key feature. If not, manually copy the Public key to the device.



NOTE: 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.

Auto-Discovery

The System automatically discovers and adds network devices, enabled ports on console servers, KVM switches, and VMware (Virtual Serial Ports and Virtual Machines).

Clones of existing devices can be created. Make sure 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.

Auto Discovery General Process

1. Create a template device.

This device is a clone that includes all the settings, except connection details to the discovered devices. It is recommended the clone be configured with all settings as on end devices.

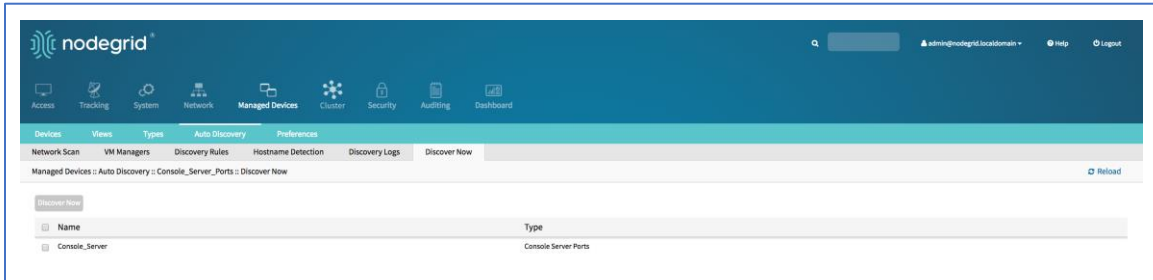
NOTE: For each target device type, a template device must be created.

2. For network devices, create a Network Scan.
3. For virtual machines, create a Virtual Manager.
4. For all devices, create a Discovery Rule

This links the template device with discovery rules. 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. The process can be manually started at any point from the WebUI (*Managed Devices :: Auto Discovery :: Discover Now*) or CLI (/settings/auto_discovery/discover_now/).



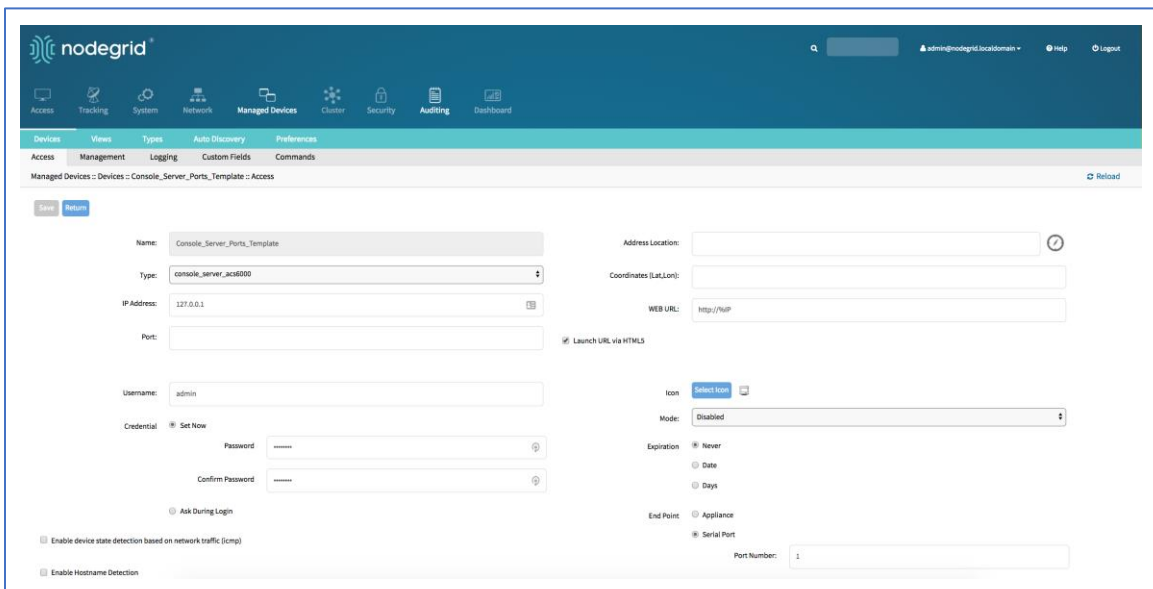
Auto Discovery of Console Server and KVM Switch Ports

The Console Server appliance and KVM Switches 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. See “Auto Discover of Network Devices”.

Create a Template Device

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click **Add**.



3. Enter a **Name** (of the template).

4. In the **Type** drop-down, select a type (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. For **End Point** menu, select **Serial Port** or **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**.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings”.

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

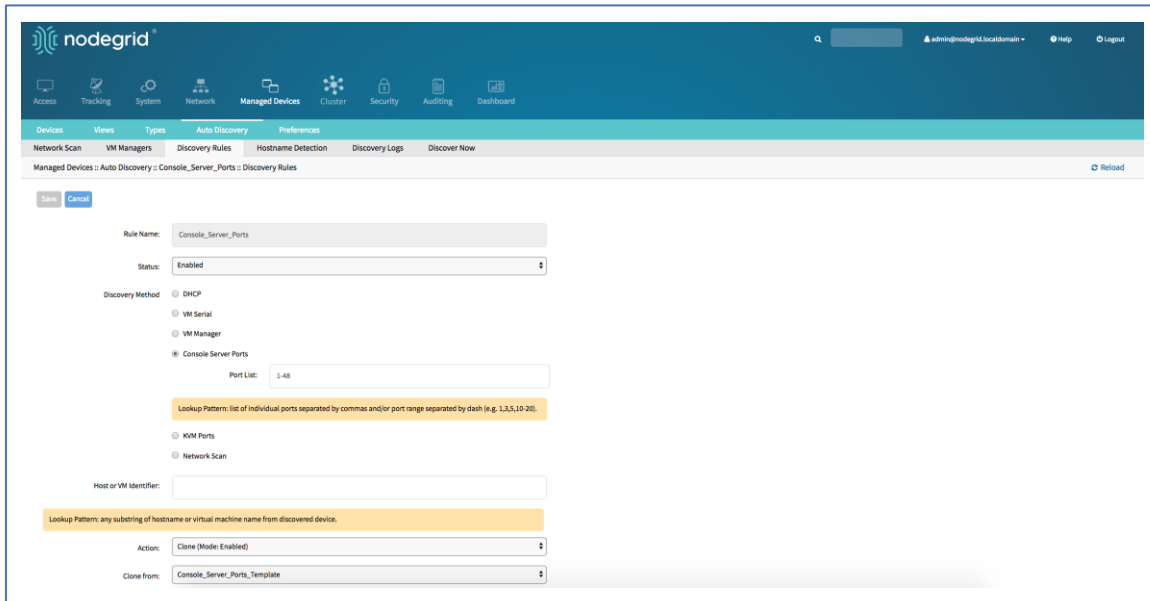
4. Save the changes with commit

```
[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=192.168.2.151
[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
```

Create a Discovery Rule

WebUI Procedure

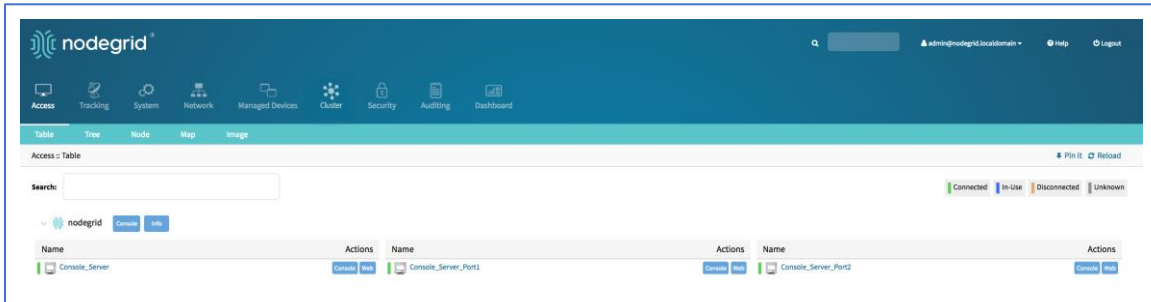
1. Go to *Managed Devices :: Auto Discovery :: Discovery Rules*
2. Click **Add**.



3. Enter **Rule Name** (of Discovery Rule).
4. On **Status** drop-down, select an item (Enabled, Disabled)
5. In **Discovery Method** menu, select **Console Server Ports** or **KVM Ports** radio button.
6. For **Port List**, enter a list of ports to be scanned (i.e., 1,3,5,10-20).
7. For **Host or VM Identifier**, enter a parameter to apply as an additional filter.
If a value is provided, part of the port name must match the value.
8. On **Action** drop-down, select an action item to be performed 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**.
11. Create a Console Server or KVM Switch appliance (See “Add Console Servers”).

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
```

7. Create a Console Server or KVM Switch appliance See “Add Console Servers”.

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 of 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 menu),
- Port Scan and enter a list of ports in the Port List field,
- Ping
- DHCP (via MAC Address)

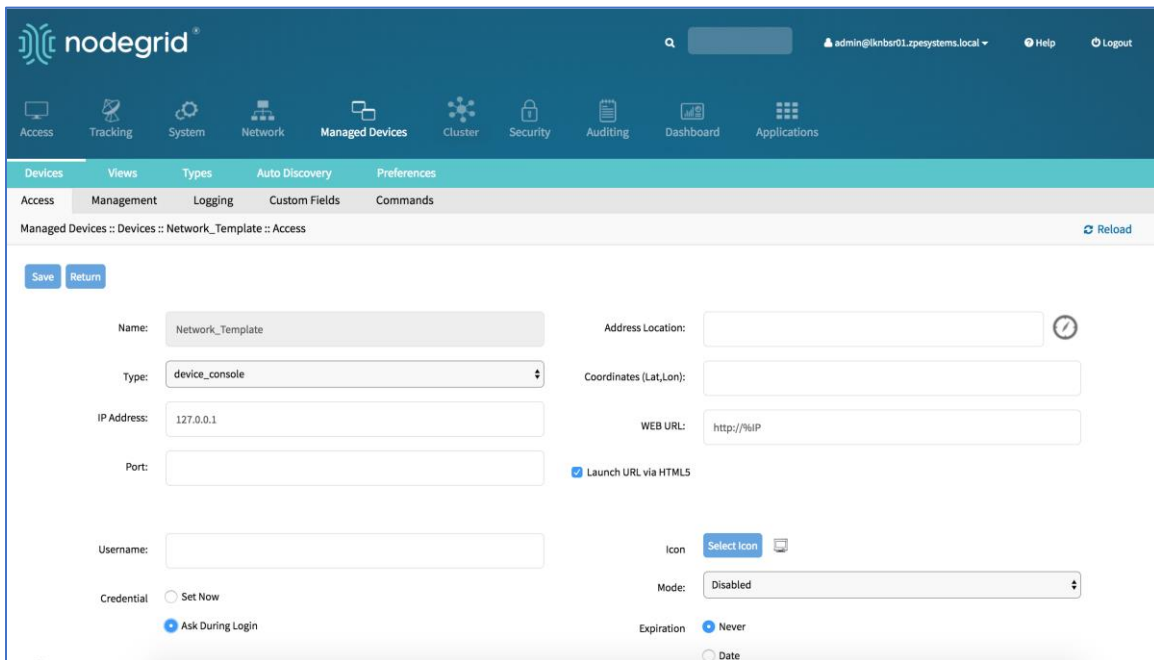
Setup is a three-step process:

1. Create a Template Device
2. Create a Network Scan
3. Create a Discovery Rule.

Create a Template Device

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click **Add**.



The screenshot shows the Nodegrid WebUI interface for adding a new device template. The breadcrumb path is 'Managed Devices :: Devices :: Network_Template :: Access'. The form contains the following fields and options:

- Name:** Network_Template
- Type:** device_console (selected from a dropdown menu)
- IP Address:** 127.0.0.1
- Port:** (empty)
- Username:** (empty)
- Credential:** Set Now, Ask During Login
- Address Location:** (empty)
- Coordinates (Lat, Lon):** (empty)
- WEB URL:** http://%iP
- Launch URL via HTML5:**
- Icon:** Select Icon (button)
- Mode:** Disabled (selected from a dropdown menu)
- Expiration:** Never, Date

3. Enter **Name** (of the template).
4. In the **Type** drop-down, select a type (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**.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings”.

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

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings”.

```
[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

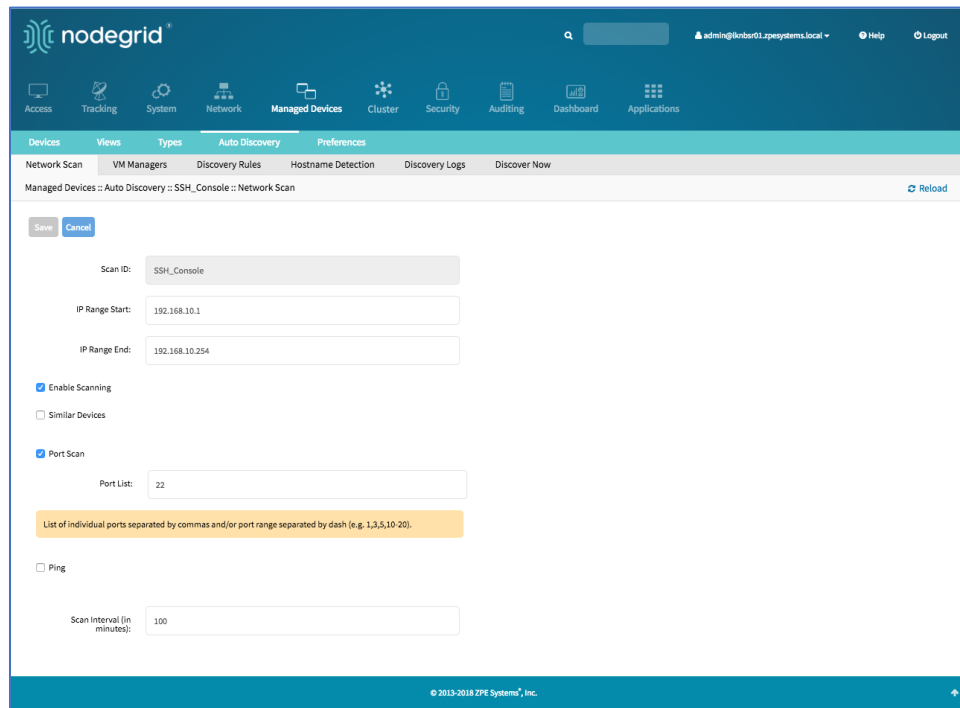
[admin@nodegrid {devices}]# set credential=set_now
[admin@nodegrid {devices}]# set username=admin password=admin

[admin@nodegrid {devices}]# set mode=disabled
[admin@nodegrid {devices}]# commit
```

Create a Network Scan

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: Network_Scan*
2. Click **Add**.



The screenshot shows the 'Add' form for a Network Scan in the Nodegrid web interface. The form is titled 'Managed Devices :: Auto Discovery :: SSH_Console :: Network Scan'. It includes the following fields and options:

- Scan ID:** SSH_Console
- IP Range Start:** 192.168.10.1
- IP Range End:** 192.168.10.254
- Enable Scanning:**
- Similar Devices:**
- Port Scan:**
 - Port List:** 22
 - List of individual ports separated by commas and/or port range separated by dash (e.g. 1,3,5,10-20).
- Ping:**
- Scan Interval (in minutes):** 100

3. Enter **Name** (of Scan ID)
4. Enter **IP Range Start** (to be scanned).
5. Enter **IP Range End** (to be scanned).
6. For scan methods, select checkbox and define one or more of the three scan methods:
 - Similar Devices** (select an existing template used to identify devices)
 - Port Scan** (define a list of ports which should be reachable on the device)
 - Ping** (no further settings required)
7. Select **Enable Scanning** checkbox
8. In **Scan interval (in minutes)**, enter a value.
9. 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)

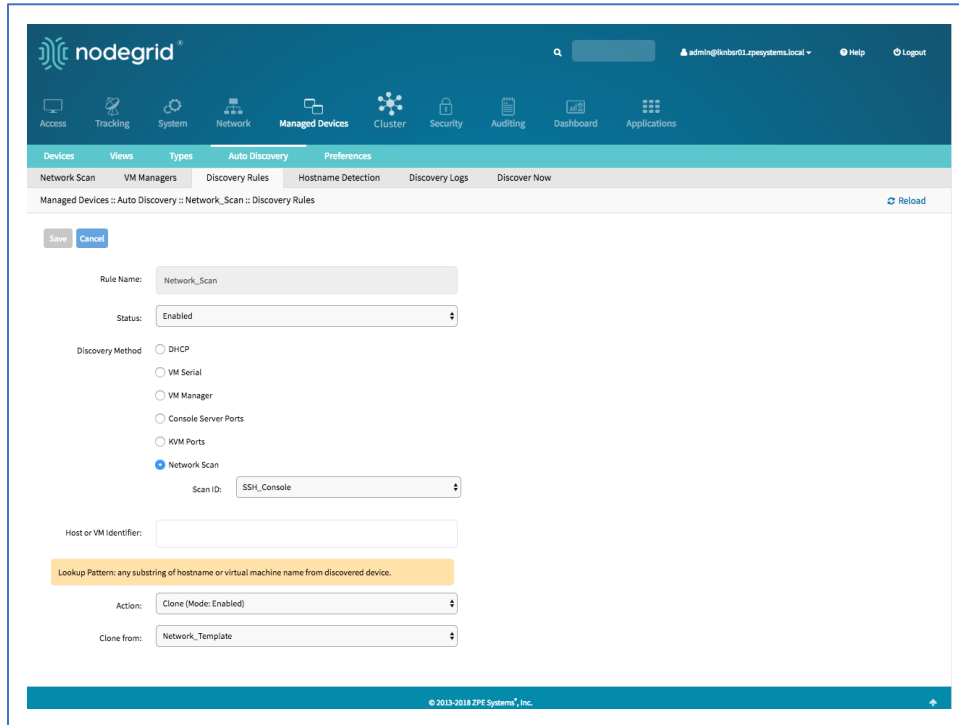
6. Save the changes with commit

```
[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
```

Create a Discovery Rule

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: Discovery Rules*
2. Click **Add**.



3. Enter **Name** (of the Discovery Rule)
4. On **Status** drop-down, select (Enabled, Disabled)
5. On **Discovery Method** menu, select **Network Scan** checkbox.
6. On **Scan ID** drop-down, select (the created Network Scan ID).
7. 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 action to be performed 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 will take a few minutes to complete.

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 a few minutes to complete.

Auto Discovery of 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. (See “Configuring Virtual Serial Port (vSPC) on VM Servers”.)

NOTE: The free version of ESXi is not supported.

Create a Template Device

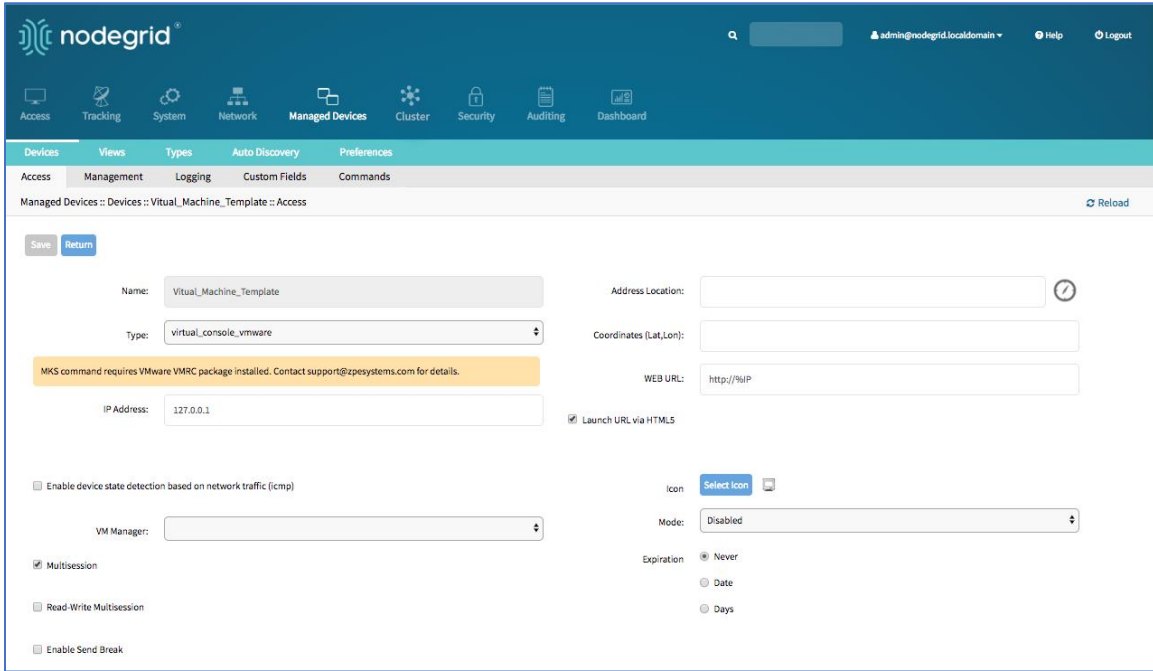
WebUI Procedure

1. Go to *Managed Devices :: Devices*
2. Click **Add** button.
3. Enter **Name** (of the template).
4. In the **Type** drop-down, select a type (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**.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings”.



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

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings”.

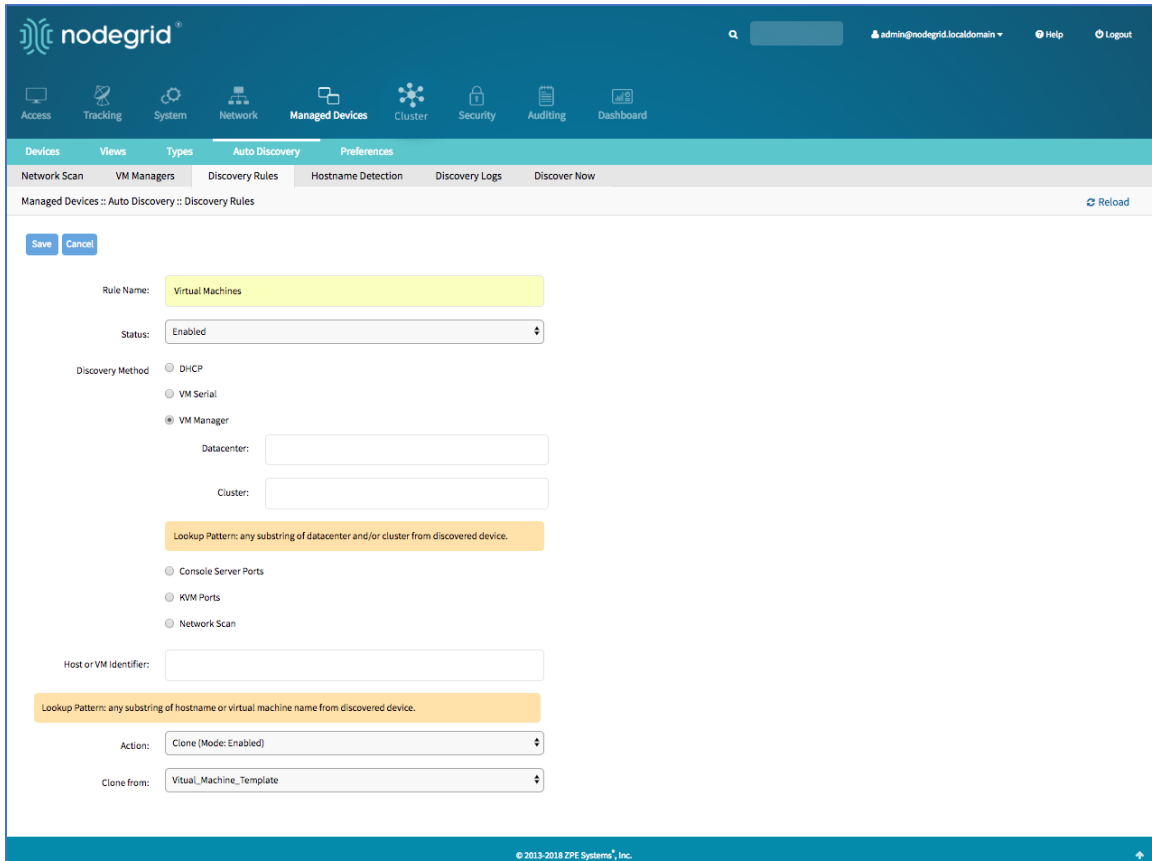
```
[admin@nodegrid /]# cd /settings/devices
[admin@nodegrid devices]# add
[admin@nodegrid {devices}]# set name=Virtual_Machine_Template
[admin@nodegrid {devices}]# set type=virtual_console_vmware
[admin@nodegrid {devices}]# set ip_address=192.168.2.151
```

```
[admin@nodegrid {devices}]# set mode=disabled
[admin@nodegrid {devices}]# commit
```

Create a Discovery Rule

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: Discovery Rules*
2. Click **Add**.



3. Enter **Rule Name** (of Discovery Rule).
4. On **Status** drop-down, select an item (Enabled, Disabled)
5. In **Discovery Method** menu, select **VM Manager**.
6. (optional) Use the fields **Datacenter** and **Cluster** to filter the scan to these specific entries.
7. For **Host or VM Identifier**, enter a parameter to apply as an additional filter.
If a value is provided, part of the port name must match the value.
8. On **Action** drop-down, select an action item to be performed 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**.

CLI Procedure

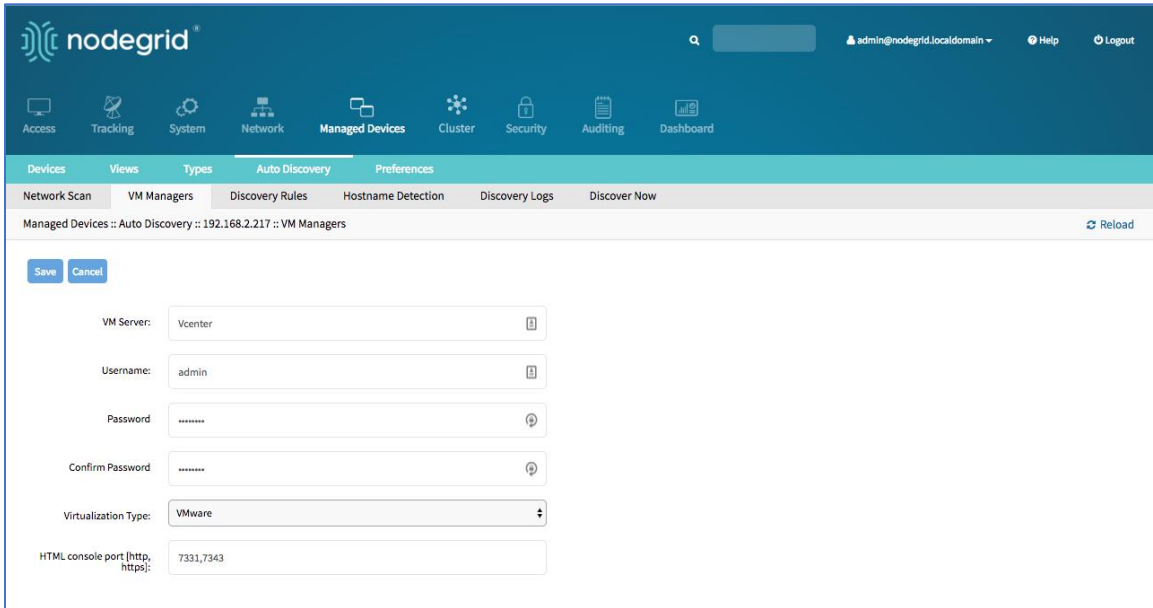
1. Go to `/settings/auto_discovery/discovery_rules/`
2. Use the `add` command to create a Discovery Rule
3. Use the `set` command to define the following settings:
 - `rule_name` for the Discovery Rule
 - `status` for the discovered rule (enabled, disabled)
 - `method` set to `vm_manager`
 - Use `datacenter` 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
```

Define a VM Manager

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: VM Managers*
2. Click **Add**.



3. In **VM Server**, enter the **vCenter/ESXi IP** or **FQDN**.
4. Enter **Username**.
5. Enter **Password**.
6. Enter **HTML console port** (if needed).
7. Click **Save**.

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

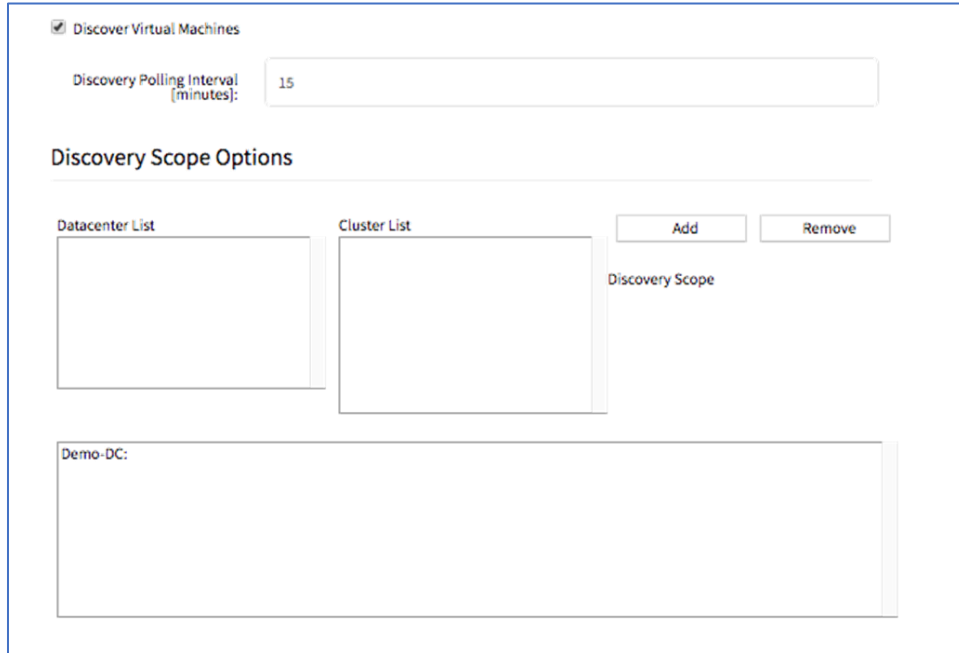
```
[admin@nodegrid /]# cd /settings/auto_discovery/vm_managers/
[admin@nodegrid vm_managers]# add
[admin@nodegrid {vm_managers}]# set vm_server=vCenter
[admin@nodegrid {vm_managers}]# set username=admin
[admin@nodegrid {vm_managers}]# set password=password
[admin@nodegrid {vm_managers}]# commit
```

5. The Nodegrid Platform connects to the vCenter or ESXi system.
 This can take several minutes).

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
```

Auto Discovery of 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. See “DHCP Server for details.

Create a Template Device

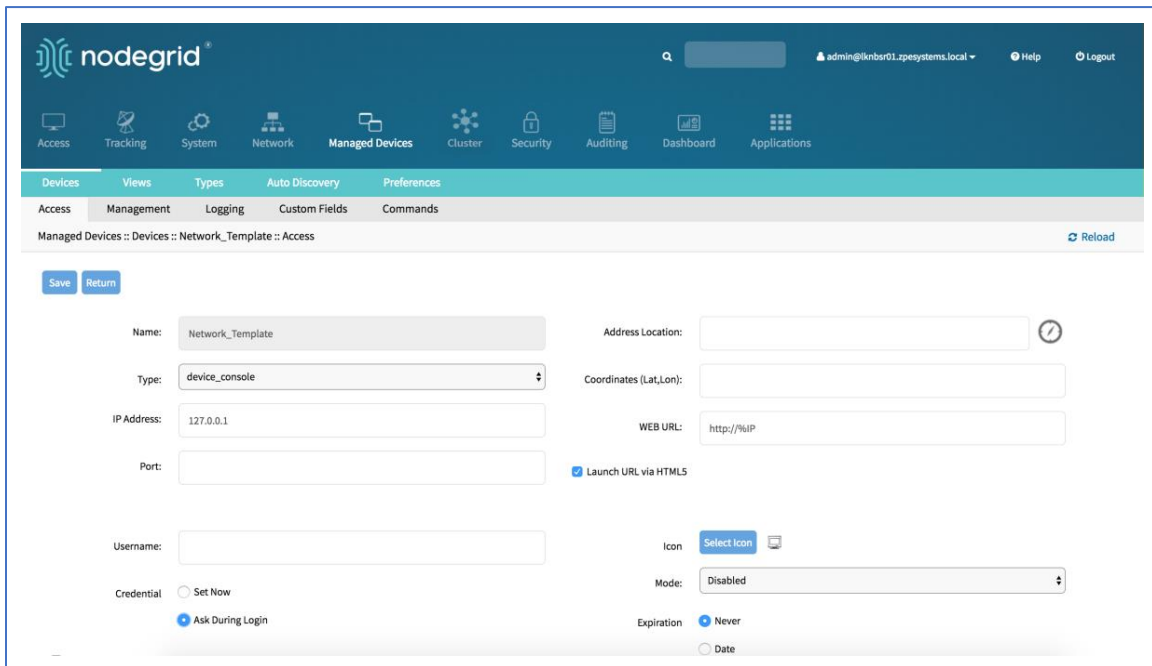
WebUI Procedure

1. Go to *Managed Devices :: Devices*
2. Click **Add**.
3. Enter **Name** (of the template).
4. For **IP Address**, enter 127.0.0.1
5. In the **Type** drop-down field, select a type (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**.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings”.



CLI Procedure

1. Go to /settings/devices
2. Use the add command to create a new device,

- 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

- Save the changes with commit

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings”.

```
[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
```

Create a Discovery Rule

WebUI Procedure

- Go to *Managed Devices :: Auto Discovery :: Discovery Rules*
- Click **Add**.
- Enter **Name** (of the Discovery Rule)
- On **Status** drop-down, select (Enabled, Disabled)
- On **Discovery Method** menu, select **DHCP** checkbox.
- (optional) To filter specific entries, enter **MAC Address**.
- 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 action to be performed 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
```

Configure Individual Device Settings

Most devices support additional configuration options and settings. This section provides details and procedures on configuration.

Hostname Detection

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.

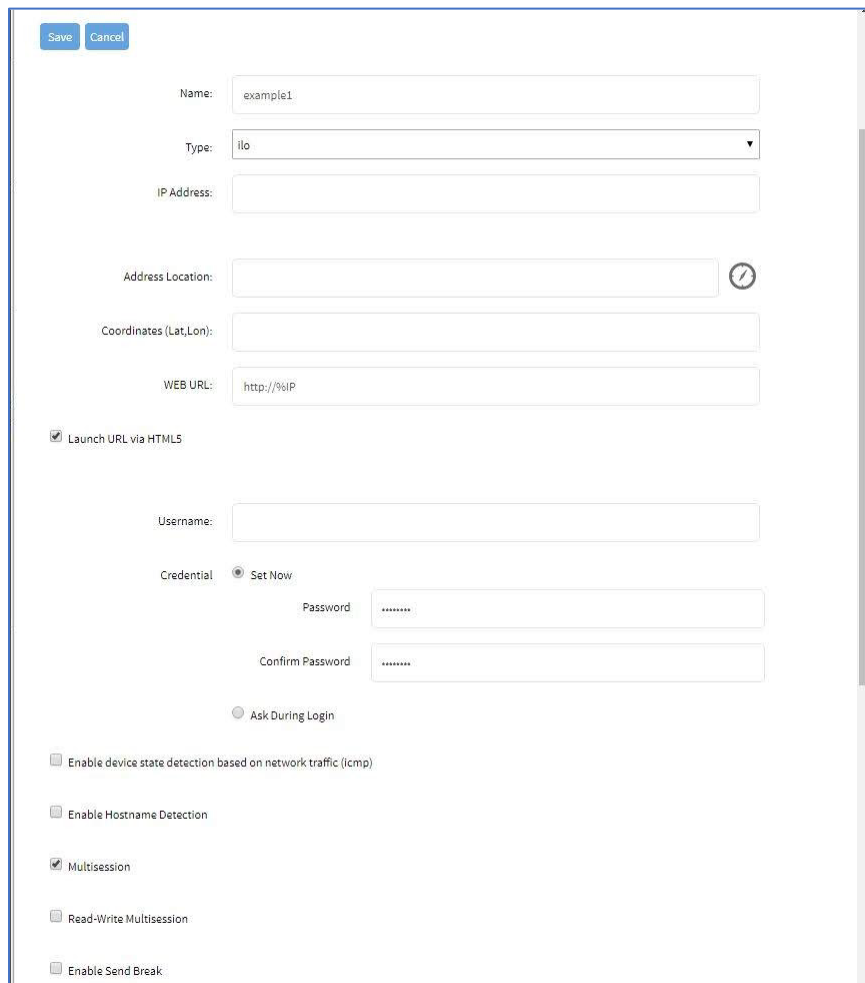
Nodegrid sends a probe and waits for a match. If no match, a second probe is sent. This is repeated until a match occurs, then the probe process stops.

Configure Hostname Detection

Hostname detection must be enabled on the target device. After hostname detection is enabled, it runs only once and then reverts to disabled.

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Locate and click on the device name. This displays the device details page.



The screenshot shows a configuration form for a device. At the top left are 'Save' and 'Cancel' buttons. The form contains the following fields and options:

- Name:
- Type:
- IP Address:
- Address Location: (with a location pin icon)
- Coordinates (Lat, Lon):
- WEB URL:
- Launch URL via HTML5
- Username:
- Credential:
 - Set Now
 - Password:
 - Confirm Password:
 - Ask During Login
- Enable device state detection based on network traffic (icmp)
- Enable Hostname Detection
- Multisession
- Read-Write Multisession
- Enable Send Break

3. Select **Enable Hostname Detection** checkbox.
4. Click **Save**.

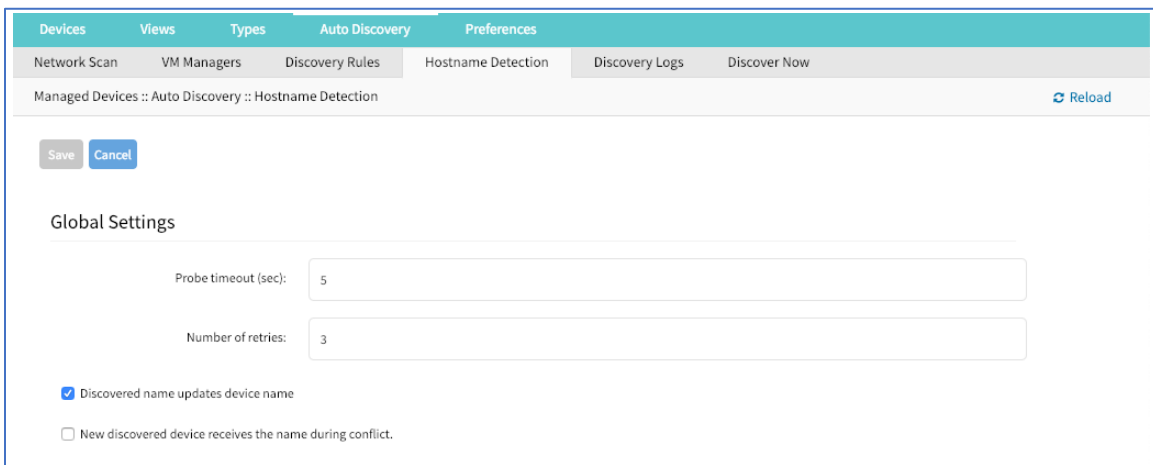
CLI Procedure

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
```

Hostname Detection Settings

On each target device, settings can be adjusted – WebUI (*Managed Devices :: Auto Discovery :: Hostname Detection*) or CLI (*/settings/auto_discovery/hostname_detection*).



Probe timeout (sec) (timeout to wait for output)

Number of retries (number of times probe is resent if no output available)

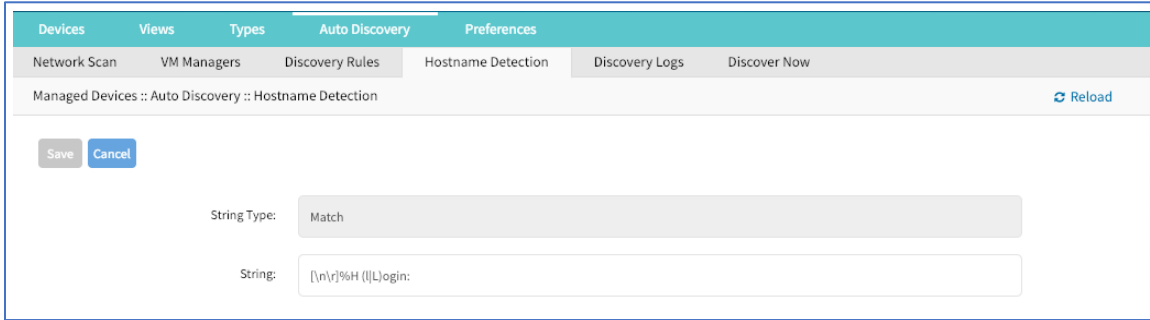
Discovered name updates device name checkbox (enabled by default – if disabled, no device names are updated, even if a match was found.)

New discovered device receives the name during conflict checkbox (if enabled and multiple devices have the same name, the latest discovered device is receives the name.)

Create a Probe or Match

WebUI Procedure

1. Go to *Managed Devices :: Auto Discovery :: Hostname Detection*
2. Click **Add**.



3. For **String Type**, enter a type (Match or Probe).
4. In **String**, enter characters to be the 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
```

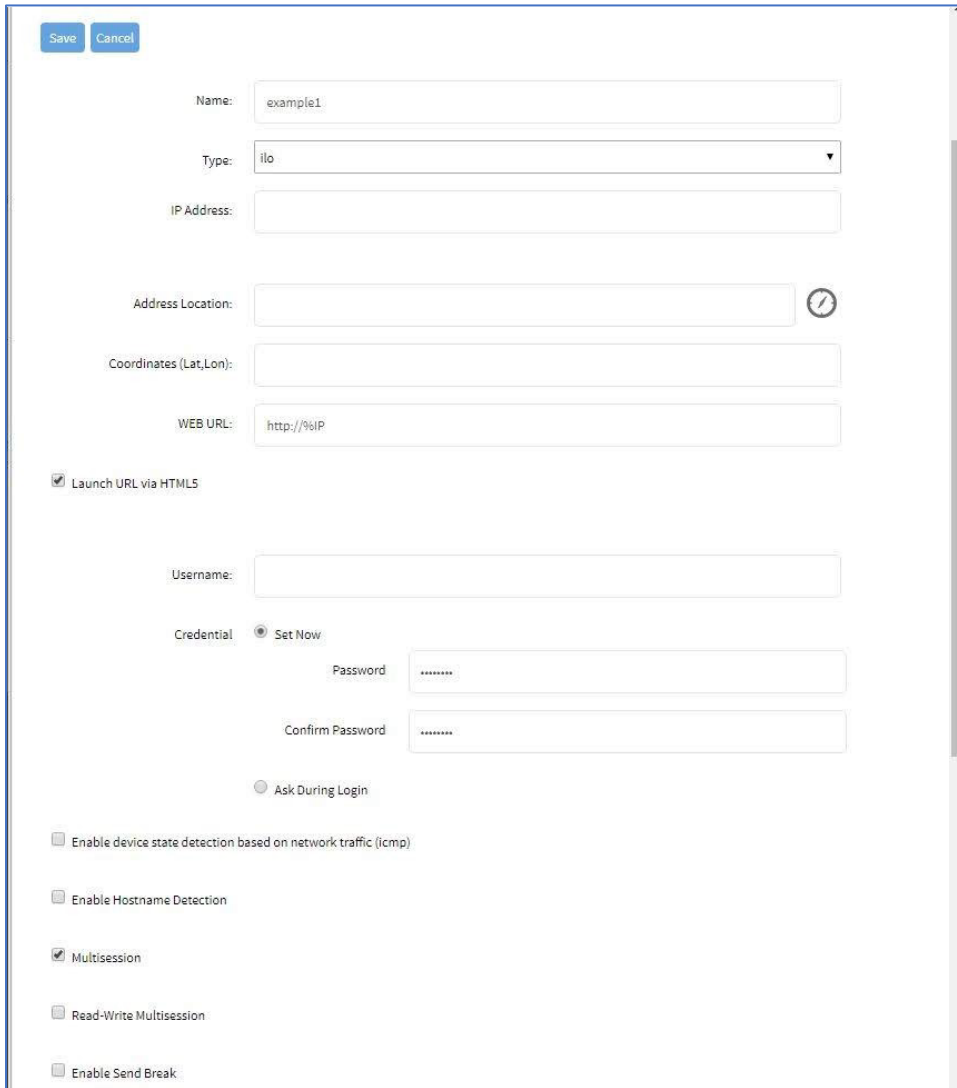
Multi sessions

With multi-sessions enabled, several users can access the same device at the same time. All users see the same output. By default, the first user has read-write access, and all other users have read access. When the Read-Write Multisession option is enabled, all connected users have read-write access to the session. Because only one user at a time has write access, the system automatically switches to the first user who is entering keystrokes.

On the console session menu, all connected users can be viewed. (see “Break Signal”). This is also available for device console sessions.

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Locate and click the target device name. This displays device details.



The screenshot shows a configuration form for a device. At the top left are 'Save' and 'Cancel' buttons. The form contains the following fields and options:

- Name: example1
- Type: ilo
- IP Address: (empty)
- Address Location: (empty) with a location pin icon
- Coordinates (Lat, Lon): (empty)
- WEB URL: http://%IP
- Launch URL via HTML5
- Username: (empty)
- Credential:
 - Set Now
 - Password: (masked with dots)
 - Confirm Password: (masked with dots)
 - Ask During Login
- Enable device state detection based on network traffic (icmp)
- Enable Hostname Detection
- Multisession
- Read-Write Multisession
- Enable Send Break

3. Select the **Multi-sessions** checkbox.
4. (optional) **Select Read-Write Multi-session** checkbox.
5. Click **Save**.

CLI Procedure

1. Go to `/settings/devices/<Device Name>/access`
2. Set multisession to yes
3. (optional) set write_multisession to yes
4. Save the changes with commit

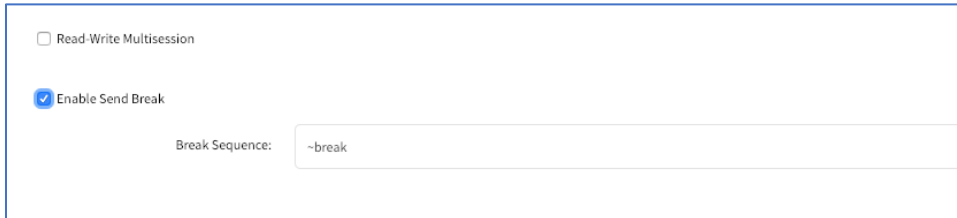
```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/access/
[admin@nodegrid /]# set multisession=yes
[+admin@nodegrid /]# set read-write_multisession=yes
[+admin@nodegrid /]# commit
```

Break Signal

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

1. Go to *Managed Devices :: Devices*.
2. Click on the Target Device name. This opens the details page.



3. Select the **Enable Send Break** checkbox.
4. Change **Break Sequence**, as needed.
5. Click **Save**.

CLI Procedure

1. Go to `/settings/devices/<Device Name>/access`
2. Set `enable_send_break` to `yes`
3. Adjust `break_sequence`, as needed
4. Save the changes with `commit`

```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/access/
[admin@nodegrid /]# set enable_send_break=yes
[+admin@nodegrid access]# set break_sequence=~break
[+admin@nodegrid access]# commit
```

Escape Sequences

Escape Sequences allow users to keep the current session active, and open another session. There are two types of escape sequences: open another normal session menu or open the power menu (for direct power control of a target device). See “Power Menu Preferences”.

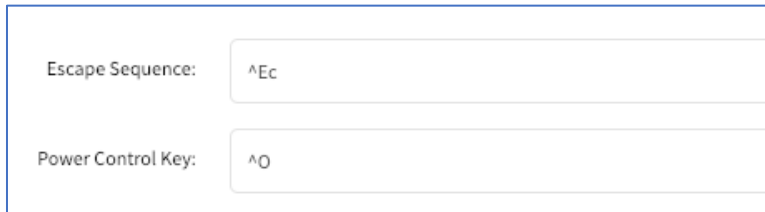
Both escape sequences are preset with a default value. This value can be changed, if needed.

Escape Sequences

Item	Default sequence	Key combination
Escape Sequence	^Ec	CTRL+SHIFT+E c
Power Control Key	^O	CTRL+SHIFT+O

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click on the Target Device name. This opens device details.



The screenshot shows a configuration form with two input fields. The first field is labeled 'Escape Sequence:' and contains the value '^Ec'. The second field is labeled 'Power Control Key:' and contains the value '^O'.

3. In **Escape Sequence**, enter new value.
4. In **Power Control Key**, enter new value.
5. Click **Save**.

CLI Procedure

1. Go to `/settings/devices/<Device Name>/access`
2. Adjust the `escape_sequence` or `power_control_key`, as needed.
3. Save the changes with `commit`

```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/access/
[admin@nodegrid /]# set escape_sequence=^Ec
[+admin@nodegrid access]# set power_control_key=^O
[+admin@nodegrid access]# commit
```

Disable User Authentication

By default, user authentication is required to access a target device. If not required, Nodegrid authentication can be disabled for specific devices.

NOTE: This disables any Nodegrid authentication method for this device. It is recommended to configure an appropriate authentication mechanism.

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click on the Target Device name. This opens device details.
3. Select the **Skip authentication to access device (NONE authentication)** checkbox.

4. Click **Save**.

CLI Procedure

1. Go to /settings/devices/<Device Name>/access
2. Set the skip_authentication_to_access_device to yes to disable authentication
3. Save the changes with commit

```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/access/
[admin@nodegrid /]# set skip_authentication_to_access_device=yes
[+admin@nodegrid access]# commit
```

SSH / Telnet Port

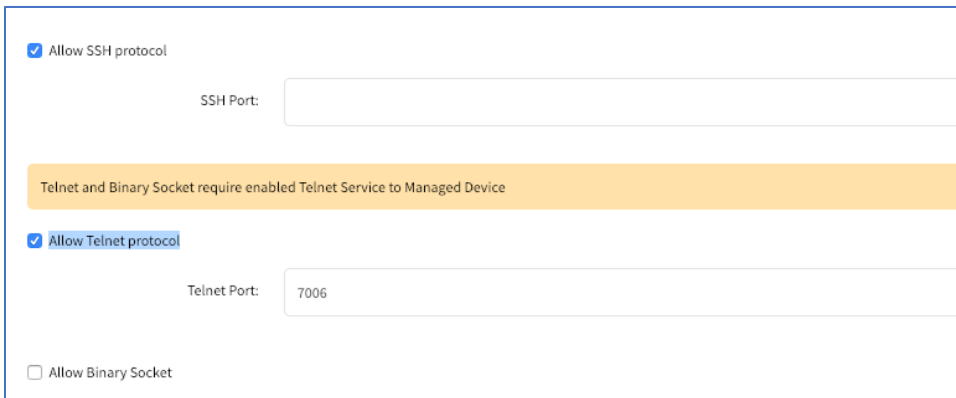
Administrators can define a specific SSH or telnet port for target devices. By default, each target device has a unique assigned telnet port. Port 7000 is used as a base port, plus the port number. For SSH connections, the default port is used for all connections.

SSH and Telnet ports can be adjusted, as needed.

NOTE: SSHv1 is deprecated. Only SSHv2 is supported.

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click on the Target Device name. This opens device details.



3. Select **Allow SSH protocol** checkbox or **Allow Telnet protocol** checkbox.

NOTE: Both options are enabled by default.

4. Enter the **Port Number**.

CLI Procedure - SSH

1. Go to /settings/devices/<Device Name>/access
2. Use the set command set allow_SSH_protocol to yes.
3. Use the set command to define a SSH_port number.

4. Save the changes with commit

CLI Procedure - Telnet

1. Go to /settings/devices/<Device Name>/access
2. Use the set command set allow_telnet_protocol to yes
3. Use the set command to define a telnet_port number
4. Save the changes with commit

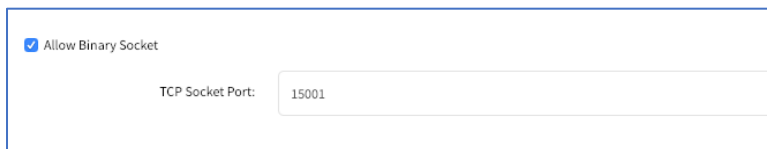
```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/access/
[admin@nodegrid /]# set allow_SSH_protocol=yes
[+admin@nodegrid access]#set SSH_port=17001
[+admin@nodegrid access]#set allow_telnet_protocol=yes
[+admin@nodegrid access]#set telnet_port=7001
[+admin@nodegrid access]#commit
```

Binary Socket

With Binary Socket, third-party systems can directly access the device as if physically connected. Signals are transmitted directly and are not encapsulated in the telnet or SSH protocol. A specific port needs to be assigned.

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click on the Target Device name. This opens device details.
3. Select **Allow Binary Socket** checkbox.
4. Enter **Port Number**.



The screenshot shows a configuration form with a checked checkbox labeled 'Allow Binary Socket' and a text input field labeled 'TCP Socket Port:' containing the value '15001'.

CLI Procedure

1. Go to /settings/devices/<Device Name>/access
2. Use the set command set allow_binary_socket to yes
3. Use the set command to define a tcp_socket_port number
4. Save the changes with commit

```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/access/
[admin@nodegrid /]# set allow_binary_socket=yes
[+admin@nodegrid access]#set tcp_socket_port=15001
[+admin@nodegrid access]#commit
```

IP Aliases

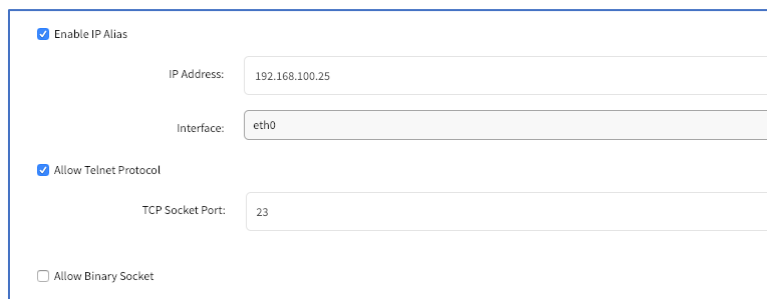
Console sessions can be started from the WebUI, CLI console, or a SSH/telnet client. For a SSH client, the default method to access is to pass the target device name (as a parameter).

Port Aliases allow the user to connect to a target device with IP addresses. Each IP Alias supports the definition of a telnet with binary port.

The allocation of up to two IP address alias are supported for each target device (IPv4 and IPv6 addresses).

WebUI Procedure

1. Go to *Managed Devices:: Devices*.
2. Click on the Target Device name. This opens device details.



3. Select **Enable IP Alias** checkbox.
4. Enter a valid **IP Address**.
5. On **Interface** drop-down, select from list.
6. Select **Allow the Telnet Protocol** checkbox.
Enter **TCP Socket Port**.
7. (if interface supports) Select **Allow Binary Socket** checkbox.
Enter **Port Number**.
8. (optional) Select **Enable Second IP Alias** checkbox.
Repeat above steps.
9. Click **Save**.

CLI Procedure

1. Go to `/settings/devices/<Device Name>/access`
2. Use the set command `set enable_ip_alias` to yes
3. Use the set command to define the following values:
 - `ip_alias` - IP address
 - Interface (network interface to used)
 - `ip_alias_telnet` - enable/disable telnet

ip_alias_telnet_port - Telnet port to be used

ip_alias_binary - If the interface should support binary socket connections

4. Repeat these steps for enable_second_ip_alias
5. Save the changes with commit

```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/access/
[admin@nodegrid /]# set enable_ip_alias=yes
[+admin@nodegrid access]#set ip_alias=192.168.10.249
[+admin@nodegrid access]#set interface=eth0
[+admin@nodegrid access]#set ip_alias_telnet=yes
[+admin@nodegrid access]#set ip_alias_telnet_port=23
[+admin@nodegrid access]#set ip_alias_binary=no
[+admin@nodegrid access]#set ip_alias_binary_port=15001
[+admin@nodegrid access]#commit
```

Location

Each Device can be associated with a location, displayed in the Map view. The location can be defined through address details or directly through Longitude and Latitude values. If provided with an address, the device requires an Internet connection to determine the longitude and latitude.

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click on the Target Device name. This opens device details.

Address Location:	46757 Fremont Blvd, Fremont, CA 94538, USA
Coordinates (Lat,Lon):	37.5418582, -121.9750624

3. In **Address Location**, enter the full address. Click the **Locater** icon (to the right) to identify the latitude and longitude.
4. Alternatively, in **Coordinates (Lat., Lon)**, enter valid coordinates.
5. Click **Save**.

CLI Procedure

1. Go to /settings/devices/<Device Name>/access
2. Use the set command to provide valid latitude and longitude coordinates
3. Alternatively, provide an address.
4. Save the changes with commit

```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/access/
```

```
[admin@nodegrid /]# set coordinates="37.5418582,-121.9750624"
[+admin@nodegrid access]# set address_location="46757 Fremont Blvd, Fremont, CA 94538, USA"
[+admin@nodegrid access]# commit
```

NOTE: The CLI does not support the look-up address function.

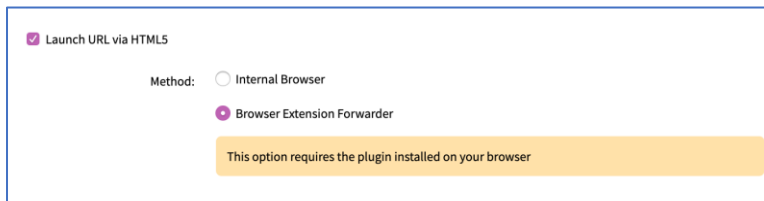
Device Web URL Options

A Web URL can be defined for each device. The URL is used for the WebUI, available for each device by default. The default URL (for all IP based sessions) is `http://%IP` where `%IP` will be replaced by the IP Address values defined for that device. By default, the URL opens inside an HTML5 frame which is forwarded to the client. This allows unsecured device web interfaces to be passed through without exposing the device to the network.

This is controlled by the setting Launch URL via HTML5.

Another option is to launch the URL via Forwarder. 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.

This is controlled by the setting: Launch URL via Forwarder.



NOTE: The Forwarder extension must be installed on the client's browser.

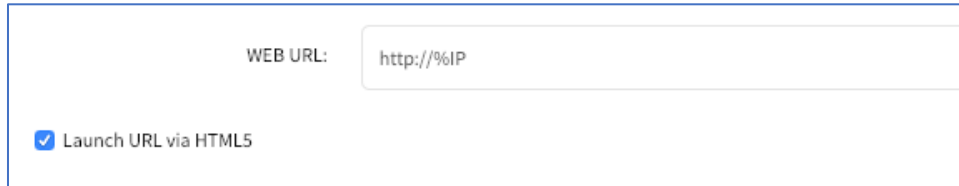
Install Chrome Forwarder Extension

1. Open Google Chrome and go to <https://chrome.google.com/webstore/detail/nodegrid-web-access-extern/cmcpkbfnaqlakhlhgdmhkedpoengpik>
2. Click **Add to Chrome**.
3. When the extension is installed, it is ready to use.

Launch URL in HTML5

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click on the Target Device name.
3. Go to the *Launch URL in HTML5* menu.



4. For **WEB URL**, adjust as needed.
5. Select **Launch URL via HTML5 checkbox**.
6. Click **Save**.

CLI Procedure

1. Go to /settings/devices/<Device Name>/access
2. Use the set command to adjust the web_url
3. Enable or disable the launch of the URL in HTML5 window by setting launch_url_via_html5
4. Save the changes with commit

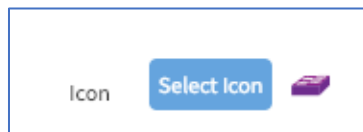
```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/access/
[admin@nodegrid /]# set web_url=https://%IP
[+admin@nodegrid access]# set launch_url_via_html5=yes
[+admin@nodegrid access]# commit
```

Assign Icon to Device

An icon can be defined for each device. Different icons can define different device types.

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click on the Target Device name.
3. Go to the *Icon* menu.



4. Click **Select Icon** and select an icon.
5. Click **Save**.

CLI Procedure

1. Go to /settings/devices/<Device Name>/access
2. Use the set command to adjust the icon to a valid value. Use tab-tab at this point to see a list of valid values.
3. Save the changes with commit

```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/access/
[admin@nodegrid /]# set icon=switch.png
[+admin@nodegrid access]# commit
```

Device Mode

Mode defines how the device is managed by the Nodegrid Platform and how device status is confirmed. Four different modes are supported.

Disabled

Device is disabled. No sessions can be opened to it and Nodegrid does not check if the device is reachable.

Enabled

Device is enabled. Sessions can be started and Nodegrid actively checks if it is reachable.

On-Demand

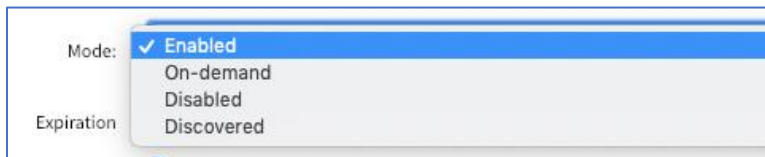
On-Demand is device enabled. A session can be started. Nodegrid does not check if a device is reachable

Discovered

Device is disabled. No sessions can be opened. Nodegrid does not check if the device is reachable. This mode indicates the device was added to the system through a discovery process.

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click on the Target Device name. Go to *Mode* menu.



3. On the **Mode** drop-down, select a mode.

NOTE: Discovered mode is a system status and can not be selected.

4. Click **Save**.

CLI Procedure

1. Go to `/settings/devices/<Device Name>/access`
2. Use the set command to adjust the mode to either:
 - enabled
 - disabled
 - on-demand

3. Save the changes with commit

```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/access/
[admin@nodegrid /]# set mode=enabled
[+admin@nodegrid access]# commit
```

Device Expiration

Each device has a defined expiration date or days. Once expired, the device automatically becomes unavailable. The default value is Never. The device and data stays in the system until removed by an admin user.

Date

The device will be available until the date specified. After that date, it will be set to Disabled mode and admin user has 10 days to take action. After 10 days, the device and its data will be removed from the system.

Days

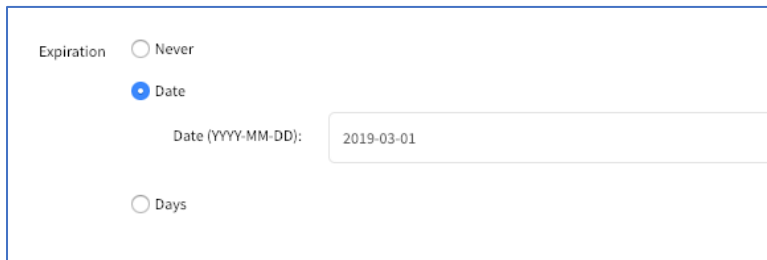
This is similar to a timeout. If no update on the device's configuration after the specified days, the device and its data is removed from the System. This is independent of the use of the device.

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.

NOTE: This feature is only available for IP-based devices.

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click on the Target Device name. Go to the *Expiration* menu.



3. Select radio button for: **Never**, **Expiration Date** or **Expiration Days** and provide an appropriate value.

Date (format: YYYY-MM-DD)

Days (between 1 and 9999999999)

4. Click **Save**.

CLI Procedure

1. Go to `/settings/devices/<Device Name>/access`
2. Use the set command to adjust expiration:

never

date

set expiration_date with valid entry YYYY-MM-DD

days

set expiration_days with a valid number 0 and 9999999999

3. Save the changes with commit

```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/access/
[admin@nodegrid /]#set expiration=date
[+admin@nodegrid access]#set expiration_date=2020-01-01
[+admin@nodegrid access]#commit
```

or

```
[admin@nodegrid /]#set expiration=days
[+admin@nodegrid access]#set expiration_days=5
[+admin@nodegrid access]#commit
```

or

```
[admin@nodegrid /]#set expiration=never
```

Device State Detection

This is a device state detection that indicates if a device is currently available.

Serial Devices

By default, Nodegrid uses DCD or CTS signals for serial devices. If these signals do not exist for a specific device, the device state detection can be changed to use data flow. For data flow, the state is based on actual data transmitted by the device. To function, this must be enabled.

IP Devices

For IP-based devices, the default mechanism is a monitored active SSH session. Additionally, an ICMP (ping) check can be enabled to check if active. To function, the Enable device state detection based on network traffic (icmp) must be enabled.

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click on the Target Device name. Go to *Device State Detection* menu.
3. Select the appropriate checkbox:

For serial: select **Enable device state detection based in data flow** checkbox.

Enable device state detection based in data flow

For other devices: Select **Enable device state detection based on network traffic (icmp)** checkbox.

Enable device state detection based on network traffic (icmp)

4. Click **Save**.

CLI Procedure

1. Go to /settings/devices/<Device Name>/access
2. Use the set command to enable the device state detection

For serial:

```
enable_device_state_detection_based_in_data_flow
```

For other devices:

```
enable_device_state_detection_based_on_network_traffic
```

3. Save the changes with commit

```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/access/
[admin@nodegrid /]#set enable_device_state_detection_based_in_data_flow=yes

or

[admin@nodegrid /]#set enable_device_state_detection_based_on_network_traffic=yes

[+admin@nodegrid access]#commit
```

Triggered 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.

NOTE: Custom scripts can be created by the customer or a professional services provider.

The following status changes can be used as triggers for custom scripts:

- Session Start
- Session Stop
- Device Up
- Device Down

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*.
2. Click on the Target Device name.
3. On the details page, go to the **Management** sub-tab.



4. In the *Scripts* menu, select an available script for the appropriate device status drop-down list:
 - Run on Session Start** drop-down
 - Run on Session Stop** drop-down
 - Run on Device UP** drop-down
 - Run on Device Down** drop-down
5. 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
```

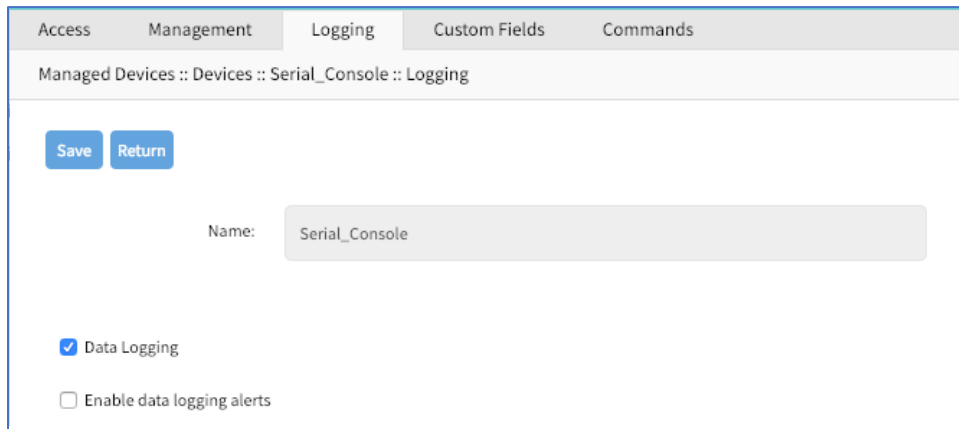
Data Logging

NOTE: This feature is available to log all text-based sessions (serial or SSH-based).

When enabled, data logs capture all session information sent and received from a device. 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*.
2. Click on the Target Device name.
3. Go to **Logging** sub-tab.
4. Select **Data Logging** checkbox.



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 or no.
3. Save the changes with `commit`

```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/logging/
[admin@nodegrid /]#set data_logging=yes
[+admin@nodegrid logging]#commit
```

Event Logging

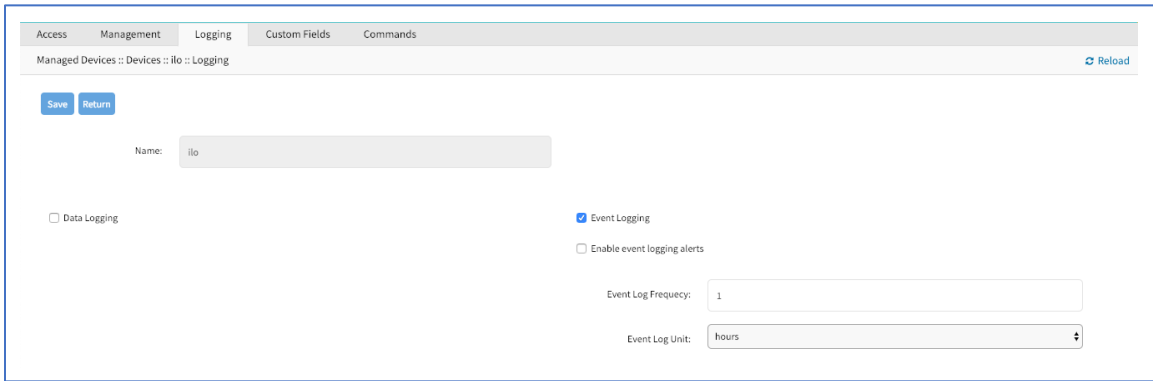
This feature logs events for Service Processor and IPMI sessions. When enabled, the System collects Service Processor Event Log data. The type of collected data depends on the Service Process functions and configuration.

The settings control the interval of collected information (1 min to 9999 hours). Location of data logs (local or remote) is based on Auditing settings.

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click on the Target Device name.

3. Go to **Logging** sub-tab.



4. Select **Event Logging** checkbox.
5. Adjust **Event Log Frequency** or **Event Log Unit** values, as needed
6. Click **Save**.

CLI Procedure

1. Gi to /settings/devices/<Device Name>/logging
2. Use the set command to change the event_logging value to yes or no.
3. Use the set command to adjust values, as needed
 - event_log_frequency (range 1 – 9999)
 - event_log_unit (hours or minutes)
4. 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]#commit
```

Triggered Alert Strings and Custom Scripts

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.

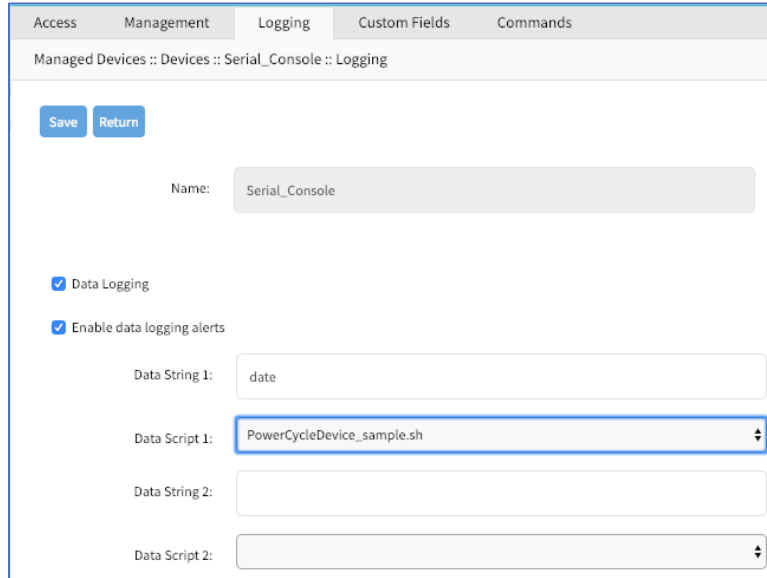
NOTE: Custom scripts can be created by the customer or a professional services provider.

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.

Data Logging Alerts

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click on the Target Device name.
3. Go to **Logging** sub-tab.



4. Select **Data Logging** checkbox.
5. Select **Enable data logging alerts** checkbox.
6. In **Data String 1** field, enter text to be matched against the data stream.
7. In **Data Script 1** drop-down, select a script.
8. If needed, repeat in **Data String 2** and **Data Script 2**.
9. 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

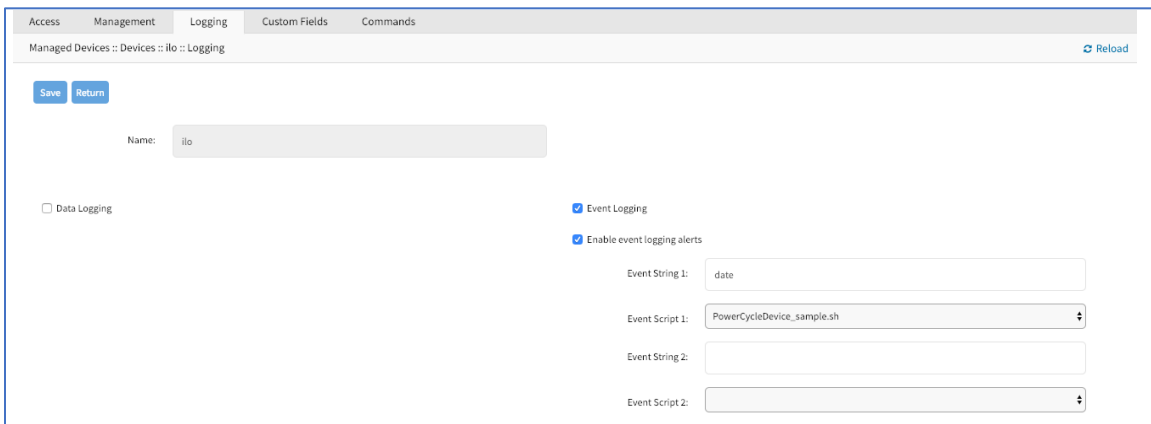
```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/logging/
[admin@nodegrid /]#set data_logging=yes
[+admin@nodegrid logging]#set enable_data_logging_alerts=yes
[+admin@nodegrid logging]#set data_string_1="String"
```

```
[+admin@nodegrid logging]#set data_script_1=ShutdownDevice_sample.sh
[+admin@nodegrid logging]#commit
```

Event Logging Alerts

WebUI Procedure

1. Go to *Managed Devices:: Devices*
2. Click on the Target Device.
3. Go to **Logging** sub-tab.
4. Select **Event Logging** checkbox.
5. Select **Enable event logging alerts** checkbox.
6. Define a min of one Event String to be matched against the data stream.
7. For a custom script, select an available script for the defined Event.



8. 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

With Custom Fields, additional information can be assigned to devices. This information is displayed on each device overview page and is searchable.

NOTE: Custom information is stored as a key/value pair.

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click on the Target Device name.
3. Go to **Custom Fields** sub-tab.
4. Click **Add**.
5. Enter a **Field Name**.
6. Enter a **Field Value**.
7. Click **Save**.

CLI Procedure

1. Go to /settings/devices/<Device Name>/custom_fields
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/custom_fields/
[admin@nodegrid /]#add
[+admin@nodegrid custom_fields]#set field_name=Custom_Field_Example
[+admin@nodegrid custom_fields]#set field_value="A Value"
[+admin@nodegrid custom_fields]#commit
```

Commands and Custom Commands

Each device type has a collection of commands to allow access to a 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.

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.

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"

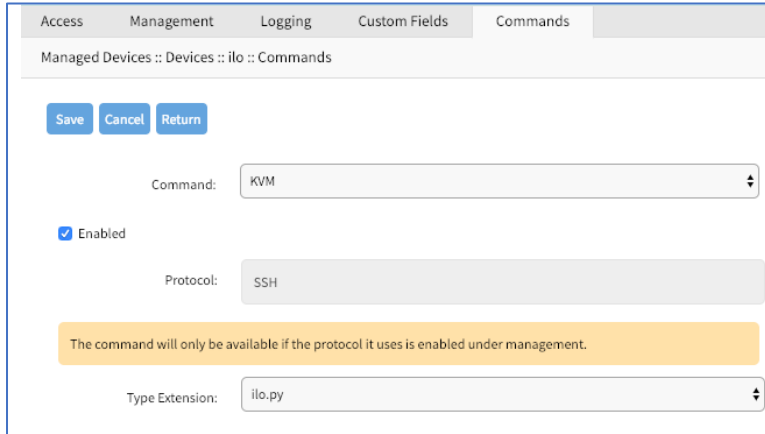
    # Call shell script
    os.system(shell_script_path)
```

Generic Change

WebUI Procedure

1. Copy the custom script into /etc/scripts/custom_commands

2. Go to *Managed Devices :: Devices*.
3. Click on the Target Device name.
4. Go to **Commands** sub-tab.

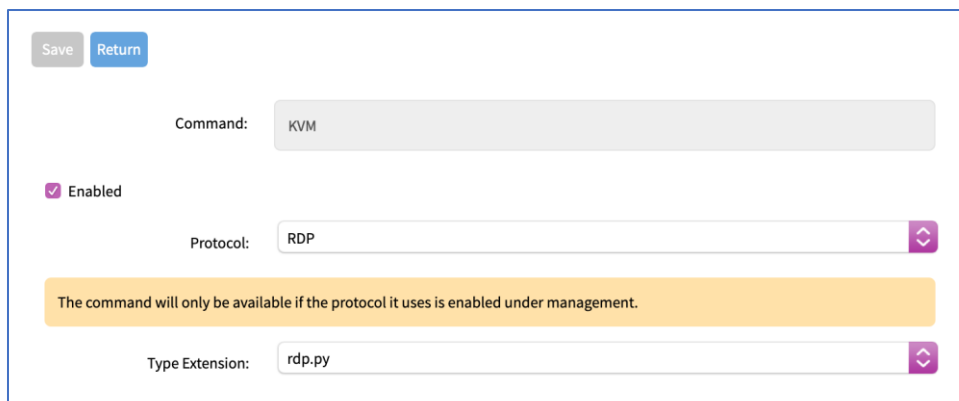


5. Click **Add**
6. To change or disable a command, click the **Command** and modify.
7. When done, click **Save**.

Device Access via RDP

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click on the Target Device name.
3. Go to **Commands** sub-tab.



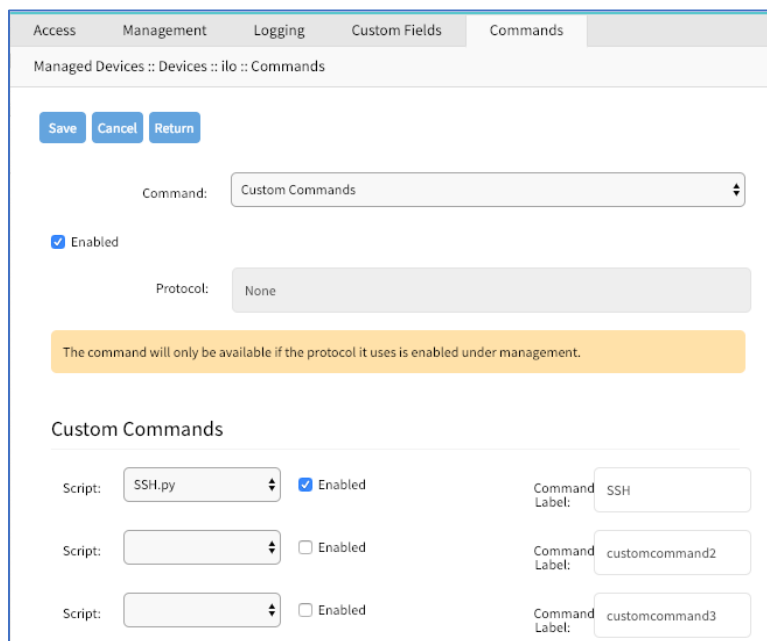
4. Click **Add**.
5. In **Command** drop-down, select KVM.
6. Select **Enabled** checkbox.
7. On **Protocol** drop-down, select one:

8. On **Type Extension** drop-down, select one.
9. Click **Save**.

Custom Commands

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click on the Target Device name.
3. Go to **Commands** sub-tab.
4. Click **Add**.



5. In **Command** drop-down, select **Custom Commands**.
6. Select **Enable** checkbox.
7. In *Custom Commands* menu, **Script** drop-down, select one.
8. Next to drop-down, select **Enabled** checkbox.
9. Adjust **Command Label** to match the command option in the script.
10. As needed, repeat for additional Scripts.
11. 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
```

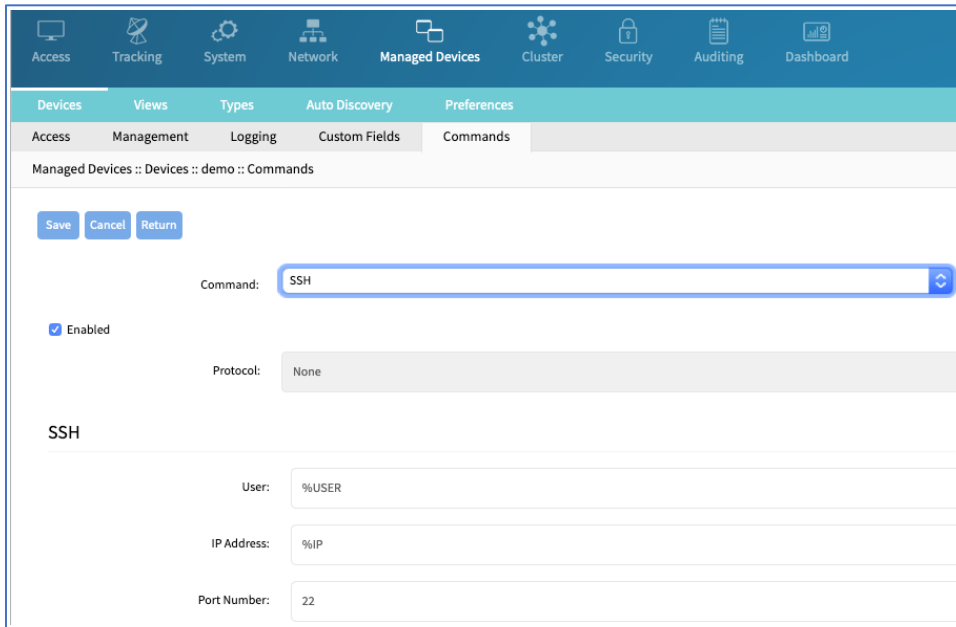
Console-like Access

This feature integrates Out-of-Band and Console-like configurations with the In-Band command.

SSH Configuration

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click on the Target Device name.
3. Go to **Commands** sub-tab.
4. On the **Command** drop-down, select **SSH**.

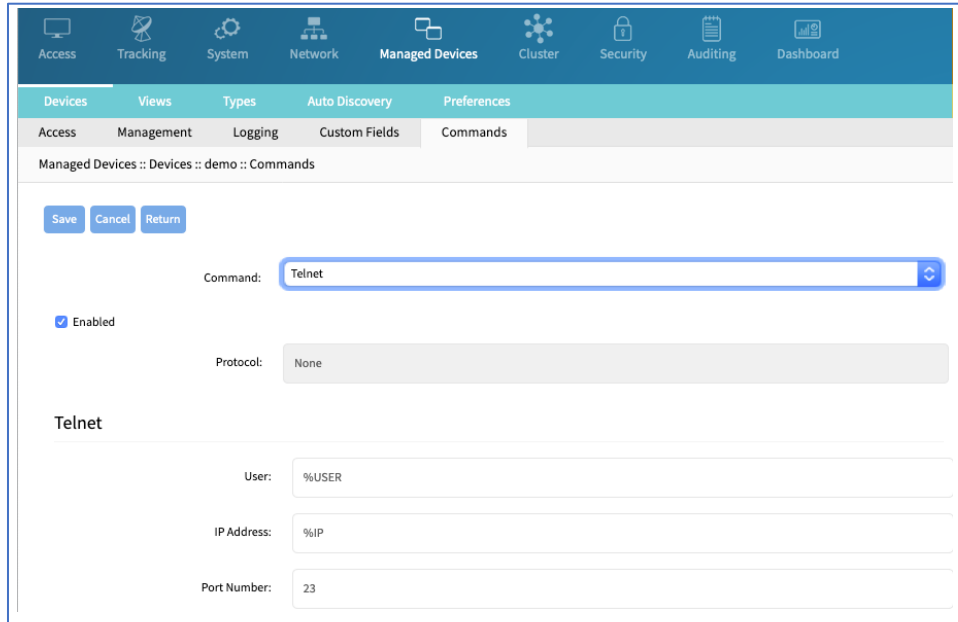


5. Select **Enabled** checkbox.
6. In the *SSH* menu, modify as needed.
7. Click **Save**.

Telnet Configuration

WebUI Procedure

1. Go to *Managed Devices :: Devices*.
2. Click on the Target Device name.
3. Go to **Commands** sub-tab.
4. On the **Command** drop-down, select **Telnet**.



5. Select **Enabled** checkbox.
6. In the *Telnet* menu, modify as needed.
7. Click **Save**.

Views tab

In *Managed Devices :: Views*, 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.

Preferences tab

The Preference menu allows administrators to further define Power Menu and Session Preferences options. These are global settings and will affect all sessions.

Power Menu sub-tab

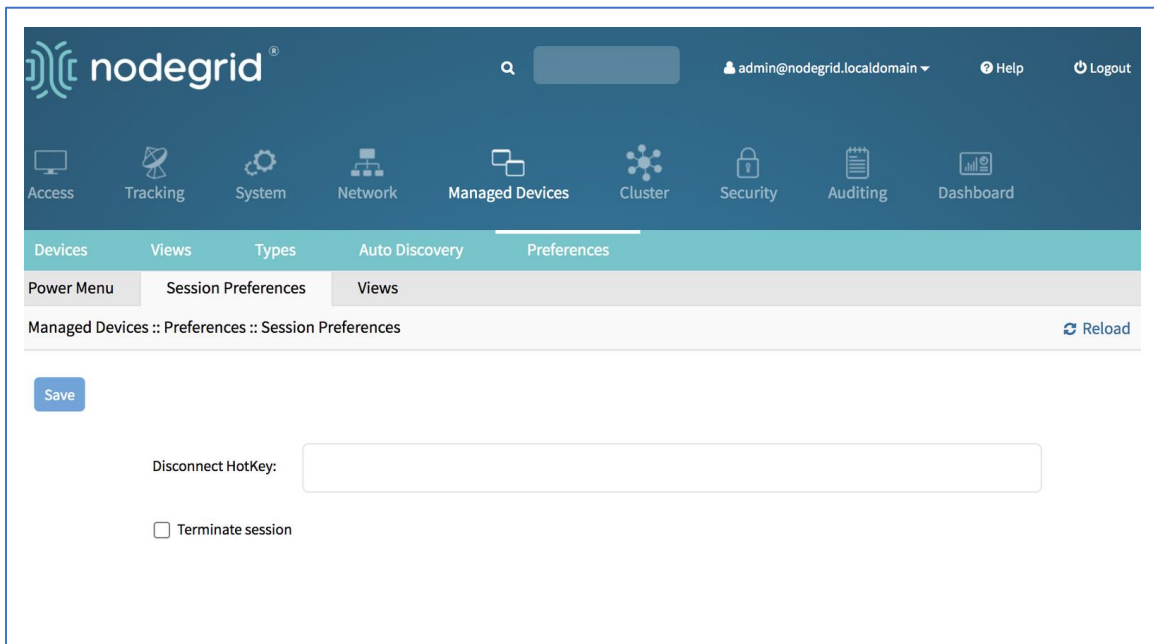
Administrators can configure preferences for defined order and labeling of the power menu as it appears in a console session.

Session Preferences sub-tab

The **Disconnect HotKey** can be defined for console sessions. This feature is useful when multiple sessions are open, i.e., a console session started from within a console session; or cascaded console sessions.

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.

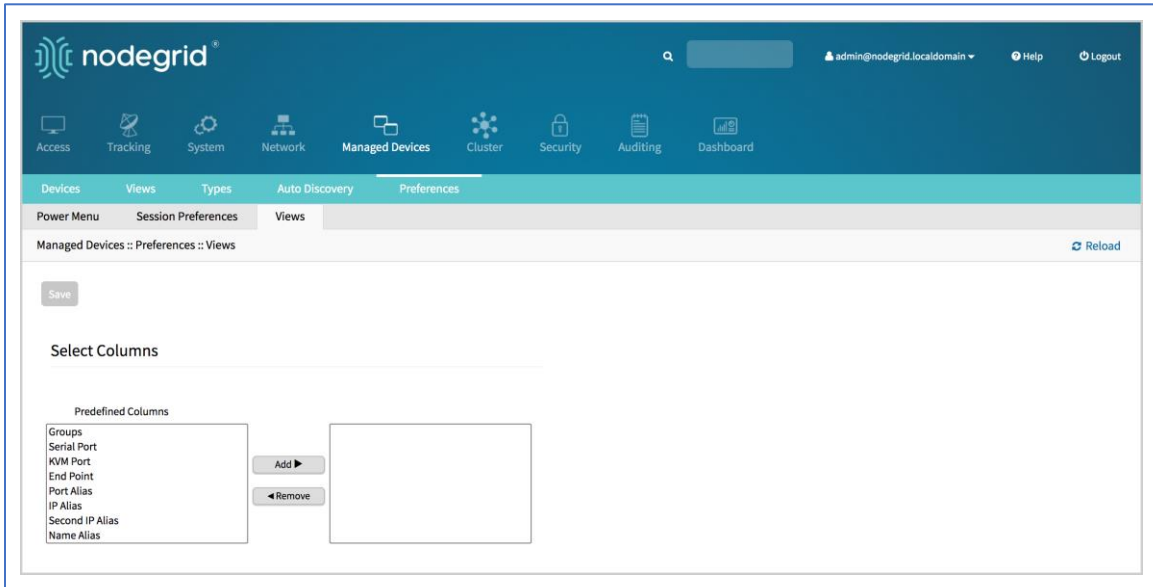
If **Terminate session** is enabled, the Disconnect HotKey closes all connected sessions – and the user is returned to the main shell prompt.



Views sub-tab

Change Column Preferences

1. Go to *Managed Devices :: Preferences :: Views*.



2. To change table column sequence, in the drop-down, select and drag a column title to the new position.

NOTE: Column selections and arrangements are stored locally on your computer. The personal column layout is not available when logged into another device.

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

Step 1 – Create a custom column

For additional organization of connected devices, custom columns can be created and enabled.

1. Go to *Managed Devices :: Preferences :: Views*.
2. In the **Custom Columns** text box, enter the name.

Custom Columns:

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 column

1. Go to *Managed Devices :: Devices*.

2. Click the device name to be associated.
3. Click **Custom Fields**.
4. Click **Add**.
5. Enter a **Field Name** and a **Field Value**.

Field Name:

Field Value:

NOTE: The Field Name must exactly match the name entered in the *Custom Columns* dialog.

6. Click **Save**.

Cluster Section

Cluster establishes a secure and resilient connection with a set of other 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.

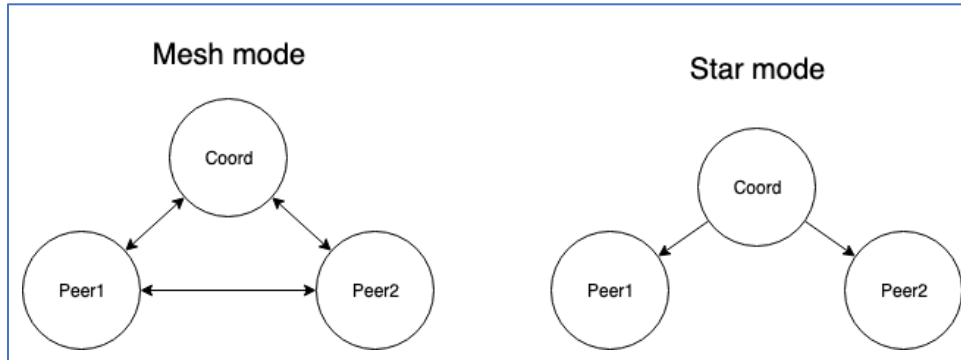
There are two types of clustering topologies:

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. To remove a peer device, select it and click **Remove**. The Coordinator device cannot be removed.

Cluster 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.

Enable Cluster

Cluster is activated when the Enable Cluster checkbox is selected.

Each Cluster requires one Coordinator (controls enrollment of peer systems).

The first unit in the Cluster must be set as type Coordinator. All other units are then set to type Peer. A Peer device can be set to the Coordinator role when the Type of Coordinator is selected. The change is automatically propagated and the previous Coordinator device is changed to Peer.

On the Coordinator device, ensure Allow Enrollment checkbox is selected. This provides a Cluster Name and Pre-Shared Key to enroll peers. For Cluster Mode, select Star or Mesh.

NOTE: The Cluster Name and the Pre-Shared Key will be used in the Peer's settings.

On the Peer device, enter the Coordinator's Cluster Name, Coordinator's Address, and the Pre-Shared Key.

Select the Enable Clustering checkbox to allow other Nodegrid systems to manage, access, and search all managed devices from other nodes.

NOTE: 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 as Peers to prevent the enrollment of other units.

Automatic Enrollment

This allows administrators to automatically add new Nodegrid systems which become available to an existing cluster. For Peers, this is enabled by default for Peers. The Pre-Shared Key setting needs to be the same on the Coordinator (set by default to nodegrid-key). The Interval [seconds] setting only

applies to the Coordinator, and regulates how often invitations are sent to potential peers. This is based on the defined network list.

After the Coordinator is enabled and configured, the admin user can add a range of IPs for other Nodegrid devices on the network. To add network ranges for the discovery process, go to the Cluster Settings tab, Automatic Enrollment Range. 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 added to the Cluster.

License Pool

This 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 which checks license availability, and assign as available). The Client sends a renew request based on the server's Renew Time [days] setting. If a client becomes unavailable for an extended period of time (exceeds the servers Lease Time [days]), that client's licenses become invalid on the client. The license is returned to the pool. Lease Time [days] option accepts values from 7-30 days. Go to System :: Licenses for a current list.

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 request five additional licenses to cover the currently used test licenses.

Peer Management

This is a function to centrally upgrade firmware of Nodegrid devices in the cluster. To enable the feature, select Enable Peer Management.

On the cluster's Management page, the software upgrade process can be started for remote devices from this central location. The firmware to be applied to the units must be hosted on a central location, available through a URL.

NOTE: The URL should include the remote server's IP or hostname, file path, and the ISO file. For example: ftp://192.168.2.200/nodegrid/Nodegrid_Platform_v3.1.0_20160127.iso

The list includes all Nodegrid systems in the Cluster. If the status shows Disabled, that device has Peer Management disabled.

To update firmware, select devices with Management Status as Idle. Then click on the Software Upgrade button. Select Remote Server and enter URL, Username, and Password. If the option Format partitions before upgrade is selected, the device's hard drive will be formatted before installing the firmware upgrade.

Downgrading

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.

To downgrade to a previous version of the Nodegrid software, two options are available:

- Restore to factory default
- Restore configuration

Security Section

Authentication validates the user, usually done with credentials. Credentials 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. This special user account, 'admin' cannot be deleted. The initial default password 'admin'.

NOTE: For security reasons, administrators are strongly advised to change the default password during the first login. Use the Change Password option on the pull-down menu under the username (upper right corner of the WebUI).

The Nodegrid Platform fully supports Authentication of local users and groups, as well as external users and groups. External authentication of users and groups can be done through LDAP/AD, Tacacs+, Radius and Kerberos.

All users have access to enabled managed devices by default. Fine Grain Authorization can be available when the option Device access enforced via user group authorization (under Services section) is enabled.

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 authorization groups.

Local Accounts tab

New local users can be added, deleted, changed, and locked under *Security :: Local Accounts*. Administrators can force passwords to be changed upon next login, and set expiration dates for user accounts. Regardless of activation options, users can change their passwords at any time. Administrators can manage API keys for each account.

- User name and password
- Hash format password (optional)
- Account expiration (optional)

- Groups, the user is a member

Manage Local Users

Local users are available at *Security :: Local Accounts*. These options are available:

- Add** (new users can be added)
- Edit** (change user settings)
- Delete** (remove a user)
- Lock** (existing users can be locked to prevent login in)
- Unlock** (locked user account can be unlocked)

Add Local User

1. Go to *Security :: Local Accounts*.
2. Click **Add**.
3. Enter **User Name**.
4. Enter **Password**.
If the password is in a hash format, select **Hash Format Password** checkbox.
5. (optional) Enter **Account Expiration Date**.
6. (optional) Select **Require password change at login time** checkbox.
7. (optional) Choose the group name from left box, click **Add**.
To remove a user group, select and click Remove.
8. Click **Save**.

Hash Format Password

The administrator can use a has format password, rather than plain password. Apply this feature if needed. This can be used for scripts, to avoids requiring scripts to use actual user passwords.

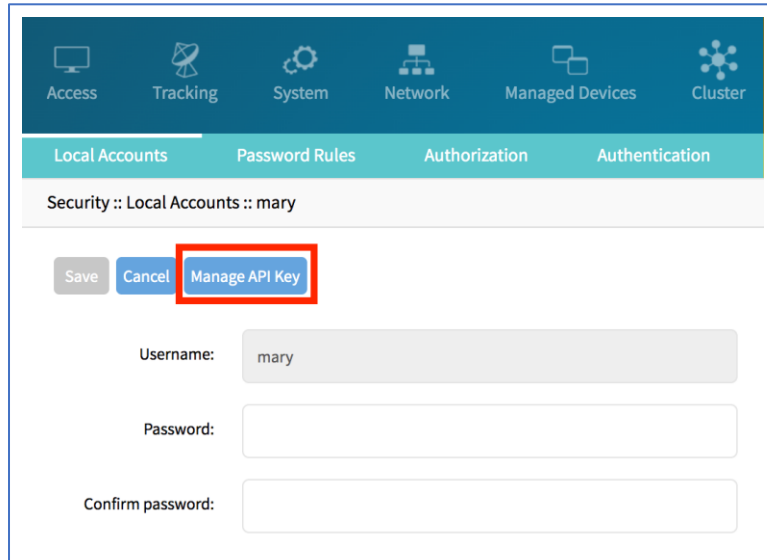
The hash password must be generated separately beforehand. Use a hash password generator. These applications (OpenSSL, chpasswd, mkpasswd) use MD5, SHA256, SHA512 engines..

The Nodegrid Platform has an OpenSSL version. In the CLI use this:

```
root@nodegrid:~# openssl passwd -1 -salt mysall  
Password:  
$1$mysall$YBFR90n0wjde5be32mC1g1
```

API Keys

Administrator can generate or revoke API keys for each user. To access, go to *Security :: Local Accounts :: <nameofuser>* and click **Manage API Key**.

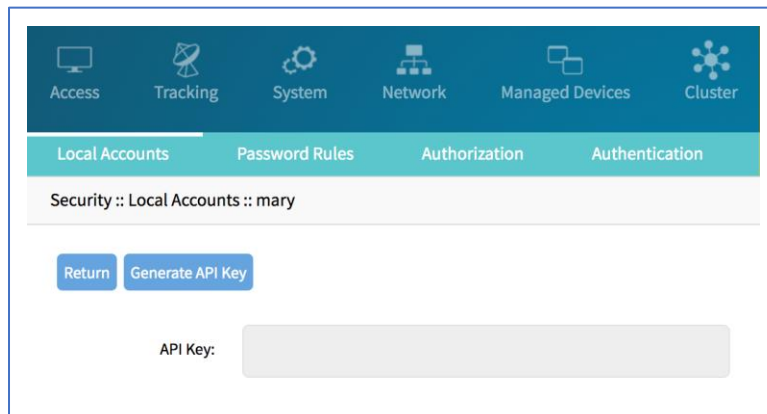


NOTE: In the example above, the name of the user is “mary”

Generate a new API key for a user

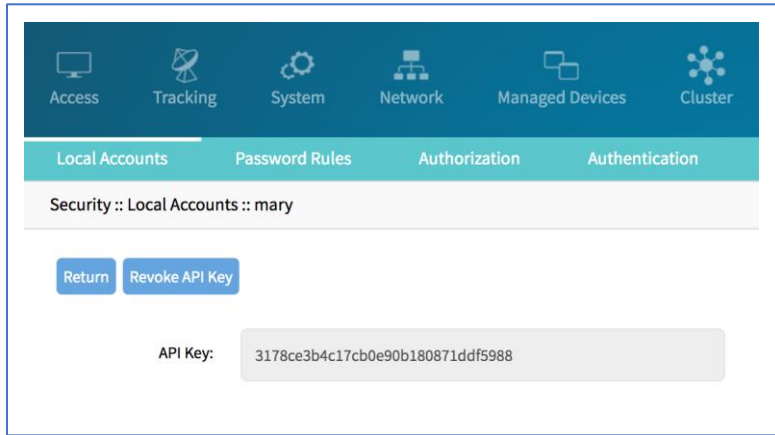
WebUI Procedure

1. Go to *Security :: Local Accounts*.
2. Locate and click the user’s name.



3. Click **Generate API Key**.

The new key is displayed in the API Key field.



NOTE: After an API key is generated for a user, the button changes to **Revoke API Key**.

Password Rules tab

When password rules are configured for the Nodegrid Platform, all local user accounts are subject. To setup, go to *Security :: Password Rules*. The administrator can set password complexity as well as password expiration.

Password Rules Options

Setting	Value	Description
Check Password Complexity	True/False	Enable/disable password complexity rules (default: disabled).
Password Complexity - Minimum Number of Digits	Number	Minimum number of digits to include in the password (default: 0).
Password Complexity - Minimum Number of Upper Case Characters	Number	Minimum number of upper cases to include in the password (default: 0).
Password Complexity - Minimum Number of Special Characters	Number	Minimum number of special characters to include in the password (default: 0).
Password Complexity - Minimum Size	Number	Minimum number of characters included in the password (default: 8).
Password Complexity - Number of Passwords to Store in History	Number	Number of passwords stored in password history. Prevents reuse of previous passwords (default: 1).
Password Expiration - Min Days	Number	Number of days the password must be valid for before it can be changed (default: 0).
Password Expiration - Max Days	Number	Maximum number of days a password can be valid for changing (default: 99999).
Password Expiration - Warning Days	Number	Number of days users is notified before password expires (default: 7).

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.

Manage Groups

During a first time login, two groups are available in the default configuration, Admin and Users. The Admin group grants the user full system and target access. The Users group grants all members full access to all targets with the disabled default of Fine Grain Authorization. When Fine Grain Authorization is enabled, User group members have no access to any target device.

Administrators can create, edit and delete groups under *Security :: Authorization*.

Group Permissions

System Permissions

Permission	Description
Track System Information	Grants access to tracking information. See "Tracking".
Terminate Sessions	Grants permission to terminal user and device sessions.
Software Upgrade and Reboot System	Grants permission to perform system upgrades and reboots.
Configure System	Grants admin rights to change the system configuration.
Configure User Account	Grants permissions to change the Authorization setting.
Apply & Save Settings	Grants permissions to save settings.
Shell Access	Grants access to the system shell.

System Permission Settings

Setting	Value	Description
Permissions	Track System Information Terminate Sessions Software Upgrade and Reboot System Configure System Configure User Account Apply & Save Settings Shell Access	System Permissions.

Setting	Value	Description
Restrict Configure System Permission to Read Only	True/False	Granted system settings are visible but cannot be changed.
Menu-driven access to devices	True/False	Group members are presented a target menu when SSH connection to the Nodegrid device is established.
Sudo permission	True/False	Allows users to execute sudo commands.
Custom Session Timeout	True/False	Enable a custom session time.
Timeout [seconds]	Number	Session timeout in seconds.
Startup application	CLI Shell	Allows administrator to set default start application when a group member connects via SSH to the Nodegrid unit (default: CLI).
Email Events to	Email Address	List of the email address to which events will be sent.

Create a User Group

WebUI Procedure

1. Go to *Security :: Authorization*.
2. Click **Add**.
3. Enter the **Group Name**.
4. Click **Save**.

The group has been created. To edit properties and permissions, click on the Group Name.

Add Local Users to a Group

WebUI Procedure

1. Go to *Security :: Authorization*.
2. Click the **Group Name**.
3. Click on **Members**.
4. Click **Add**.
5. In the left box, select the user and click Add (moves selected user to this group).

To remove a user, select in right side box, click **Remove**.

Assign Group System Permissions and Settings

WebUI Procedure

1. Go to *Security :: Authorization*.
2. Click on the **Group Name**.

3. Click **Profile**.

A user group can be assigned multiple additional system permissions. All groups have by default the user permission, granting them access to the Access table, which will allow them to connect to target devices based on the specific target permissions.

NOTE: Multiple permissions can be assigned to the same group.

4. Assign permissions.
5. Click **Save**.

Assign external groups

External groups must be assigned to a local group. This ensure the remote group gets the correct permissions.

NOTE: This step is required for LDAP, AD, and Kerberos groups. Radius and Tacacs authentication provider provide other methods to link external groups/users to local groups.

WebUI Procedure

1. Go to *Security :: Authorization*.
2. Click on the **Group Name**.
3. Click **Remote Groups**
4. List the external group names separated by a comma.
5. Click **Save**.

Assign device permissions

If Fine Grain Authorization is enabled, the permissions to access specific devices must be assigned to groups. To do this, add specific devices to a group. Then set the appropriate access rights to the target. Multiple devices can be added at the same time. Access permissions can be set together.

NOTE: access permissions to control power outlets are granted through the Outlets permissions and not through Devices

WebUI Procedure

1. Go to *Security :: Authorization*.
2. Click on the **Group Name**.
3. Click **Devices**.
4. Click **Add**.
5. Select devices on the Available list (left side) and click **Add** (moves devices to Authorized Devices list on right).

To remove one or more devices, select on the right-side box, and click **Delete**.

6. Select **Device Permissions**.
7. Click **Save**.

Access Permissions

Permission	Value	Description
Session	Read-Write Read-Only No-Access	Permission to access serial or SSH sessions (Console).
Power	Power Control Power Status No Access	Power Control permissions through IPMI.
Door	Door Control Door Status No Access	Door Control permissions.
MKS	True/False	Access to MKS sessions.
Reset Device	True/False	Permission to reset a device session.
KVM	True/False	Access to KVM sessions.
SP Console	True/False	Access to IPMI console sessions (Serial over Lan).
Virtual Media	True/False	Access to start a Virtual Media session to an IPMI device.
Access Log Audit	True/False	Access to read the access log of an IPMI device.
Access Log Clear	True/False	Permission to clear the access log of an IPMI device.
Event Log Audit	True/False	Permission to read the device-specific event log.
Event Log Clear	True/False	Permission to clear the device-specific Event Log.
Monitoring	True/False	Permission to access monitoring features.
Sensors Data	True/False	Permission to read sensor data.
Custom Commands	True/False	Permission to execute custom commands.

Assign power outlet permissions

Access permissions for power outlets from Rack PDUs are controlled individually as the power to turn on or off a device can have severe consequences for the running of a data center or remote location. The assignment of permissions is analogous to device's access permissions.

1. Go to *Security :: Authorization*.
2. Click on the **Group Name**.
3. Click **Outlets**.

4. Click **Add**,
5. Select one or more devices in the left box. Click **Add**.
To remove a device from the authorized device list, select the device and click **Delete**.
6. Select desired device permissions:
Power Control (permission to turn on or off an outlet)
Power Status (permission to see the current outlet status)
No Access
7. Click **Save**.

External Authentication Provider

External authentication is enabled on the Nodegrid Platform. This can authenticate users with:

- Active Directory and LDAP (Lightweight Directory Access Protocol),
- TACACS+ (Terminal Access Controller Access-Control System Plus),
- RADIUS (Remote Authentication Dial-In User Service)
- Kerberos (based on tickets to prove identity)

These steps must be performed independently of the specific authentication provider.

Create an Internal Group

WebUI Procedure

This creates a new internal group.

1. Go to *Security :: Authorization*.
2. Click **Add**.
3. Enter the **Group Name**.
4. Click **Save**.

Assign Permissions to Group

WebUI Procedure

1. Go to *Security :: Authorization*.
2. Click on the **Group Name**.
3. Click **Profile**.

A user group can be assigned multiple additional system permissions. All groups have by default the user permission, granting them access to the Access table, which will allow them to connect to target devices based on the specific target permissions.

NOTE: Multiple permissions can be assigned to the same group.

4. Assign permissions.
5. Click **Save**.

Assign Authentication Provider

External Authentication Provider needs to be added.

Map External Group to Internal Group

External group is mapped to an internal group.

SSH Key Authorization

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.

NOTE: Radius users can not use SSH keys for authentication.

Setup SSH key authorization

WebUI Procedure

1. Go to *Security::Authorization*.
2. Create a group or use an existing Group.
3. Click **Profile**.
4. On **Startup application**, select **Shell**.

All group members get default shell access and not CLI access on connection via SSH.

5. Go to *Security :: Local Accounts*.
6. Create a local user.
7. Add the user to the newly created group.
8. The user can now use the default SSH tools to copy his SSH key to the Nodegrid (i.e., SSH-copy-id).
9. The user can use the SSH key for authentication.

Optional

If the user needs default CLI access and not Shell access, remove the user from the newly created Group.

If the user is authorized by an external authentication provider (LDAP, AD, or TACACS+), the Local user account can be locked.

1. Go to *Security :: Local Accounts*.
2. Highlight the user.
3. Click **Lock**

The user can still use the sskkey for authentication but permissions are enforced based on his group permissions with the external authentication provider.

Authentication tab

On *Security :: Authentication*, currently configured authentication providers are listed. The order of the providers determines which is first authenticates the user.

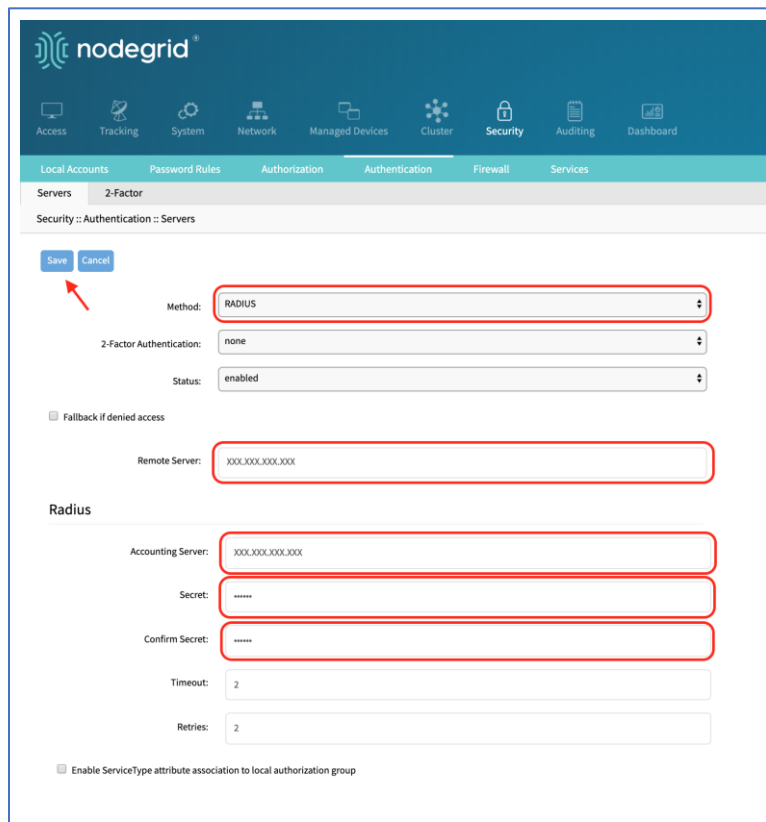
On a failed authentication, user access can be rejected, or the next provider can be tried (**Fallback if denied access** must be enabled). If disabled, user access is limited to the correct entry of authorization credentials for the first provider listed.

To access Nodegrid, the user must be a member of a group. If not, the user is checked against the default User group. Any group can be the user's default group if that group's **Default Group** setting is enabled (only one default group per user).

Add a server

WebUI Procedure

1. Go to *Security :: Authentication :: Servers*.
2. Click **Add**.



The screenshot shows the Nodegrid web interface for configuring a server. The breadcrumb path is *Security :: Authentication :: Servers*. The form includes the following fields and options:

- Method:** RADIUS
- 2-Factor Authentication:** none
- Status:** enabled
- Fallback if denied access**
- Remote Server:** XXX.XXX.XXX.XXX
- Radius Section:**
 - Accounting Server:** XXX.XXX.XXX.XXX
 - Secret:** [masked]
 - Confirm Secret:** [masked]
 - Timeout:** 2
 - Retries:** 2
- Enable ServiceType attribute association to local authorization group**

A red arrow points to the **Save** button.

3. Enter needed details.
4. Click **Save**.

SSO (Single Sign-On)

With Single Sign-On (SSO) users authenticate once and gain access to multiple secured systems without resubmitting credentials. Nodegrid currently supports these Service Providers:

- Duo
- Okta
- G Suite
- Other custom SAML Identity Providers

Configure SSO

WebUI Procedure

1. Go to *Security :: Authentication :: SSO*.
2. Click **Add**.
3. Enter these details:

Name

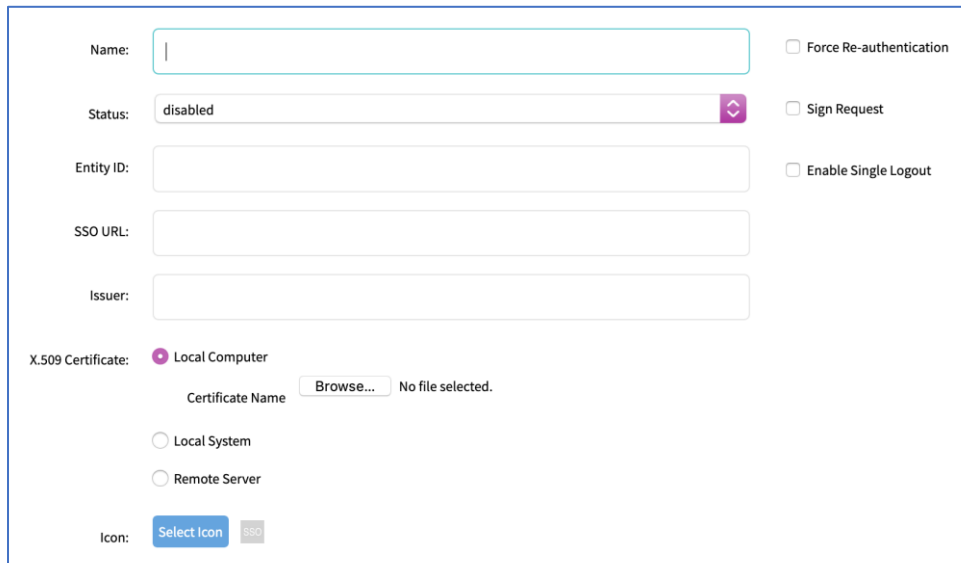
Status

Identity Provider

SSO URL

Entity ID

Certificate



The screenshot shows a configuration form for SSO. It includes the following fields and options:

- Name:** A text input field.
- Status:** A dropdown menu currently set to "disabled".
- Entity ID:** A text input field.
- SSO URL:** A text input field.
- Issuer:** A text input field.
- Force Re-authentication:** An unchecked checkbox.
- Sign Request:** An unchecked checkbox.
- Enable Single Logout:** An unchecked checkbox.
- X.509 Certificate:** A section with radio buttons for "Local Computer" (selected), "Local System", and "Remote Server". Below "Local Computer" is a "Certificate Name" field with a "Browse..." button and the text "No file selected."
- Icon:** A "Select Icon" button and a small "SSO" icon.

4. 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

IdP configuration fields:

Entity ID (globally unique name for the SP URL)

Assertion Consumer Service (ACS) (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 (an IdP endpoint that starts the authentication process)

RelayState: (optional) (deep linking for SAML. Used for <ip>/direct/<device>/console)

For more information on SSO, please see <https://support.zpesystems.com/portal/kb/articles/single-sign-on-ss0>

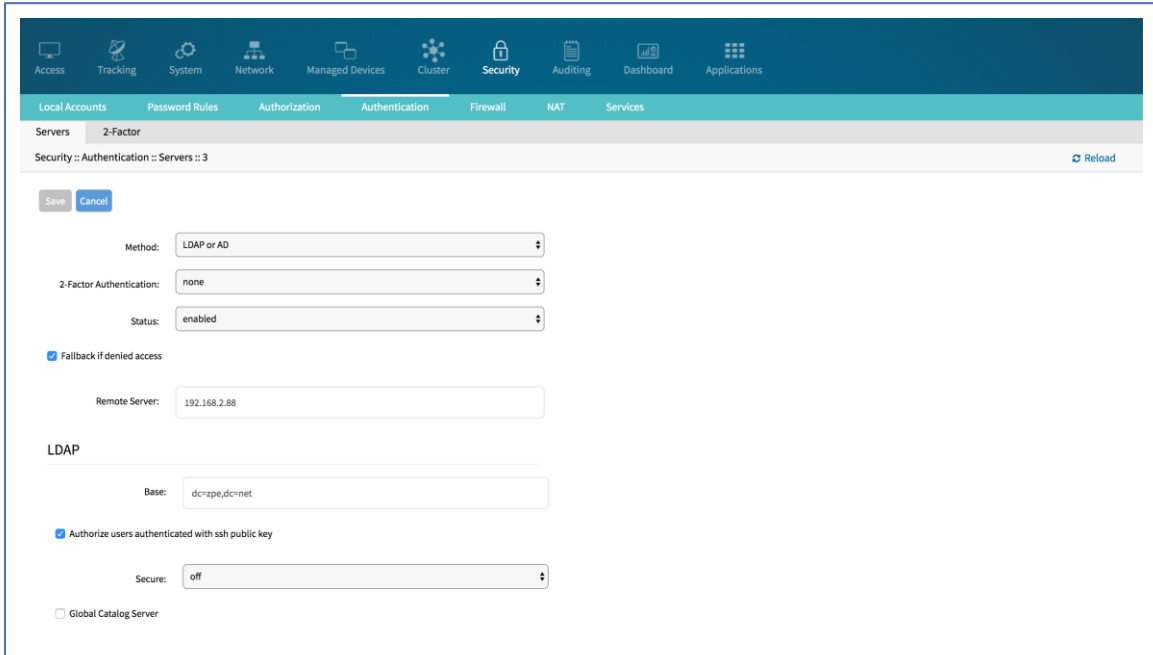
LDAP and Active Directory

The LDAP protocol is an open standard and there is a large variety of implementations, all similar, but bearing slight variations. LDAP examples shown are based on OpenLDAP implementation.

Microsoft’s Active Directory is one of the largest and widely used implementations of LDAP. Implementation is a very complex authentication structure that reflects the internal organization of companies.

To setup this provider, go to *Security :: Authentication*.

NOTE: Features can be enabled: Fallback if denied access, Authorize users authenticated with SSH public key, and Search Nested Groups (AD only).



The following information is required to set up LDAP or Active Directory authentication server.

LDAP/Active Directory Options

Field	Values	Description
Status	True/False	The provider is used to authenticate users (default: enabled).
Fallback if denied access	Enabled or Disabled	It is recommended to enable this, if the provider is not available (default: disabled).
Remote Server	FQDN or IP of LDAP server or domain	Nodegrid supports resolution of Active Directory Servers through DNS requests. This means that specific Active Directory Servers can be listed, or a valid Active Directory Domain is listed. If AD Doman is listed, the System contacts the closest server, based on the DNS results.
Base	Base DN	This can be the Root DN or a sublevel DN. This marks the highest point used to search for users or groups.
Authorize users authenticated with SSH public key	Enabled or Disabled	(default: disabled).
Secure	On, Off or Start_TLS	Traffic between the Nodegrid and LDAP server is sent unencrypted. <i>“On” is recommended.</i> (This feature must be supported by the server.) (default: off).

Field	Values	Description
Global Catalog Server	True/False	If enabled, the provider uses an Active Directory Global Catalog Server
Database Username	Search User Name	Full Qualified username (used to search through the directory). Only required if the LDAP server requires authentication for directory browsing,
Database Password and Confirm Password	Password for the search user	Only required if the LDAP server requires authentication for directory browsing
Login Attribute	Field identifies the username	Contains the username. For Active Directory, default is sAMAccountName.
Group Attribute	Field identifies the group names	Contains the group identifier. For Active Directory, default is memberOf.
Search Filter	Search Filter following the LDAP implementation	Filter used for search queries.
Search Nested Groups (AD only)	Enabled or Disabled	Disabled by Default

Example: OpenLDAP Configuration

Field	Value
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

Field	Value
Status	True

Field	Value
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

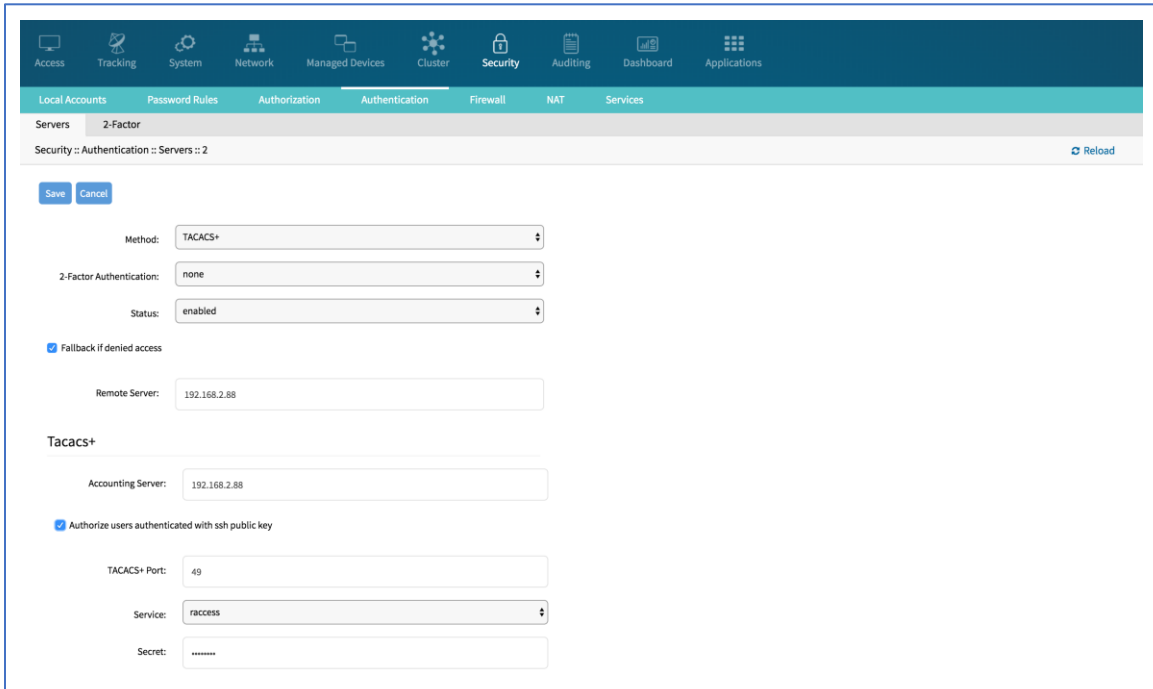
More information on how to setup LDAP and Active Directory can be found in the KB article: [How to Configure Active Directory or LDAP Authentication Provider](#).

NOTE: Permissions may be configured to restrict LDAP/AD users to access certain features within Nodegrid. Full login access cannot be blocked for specific LDAP/AD users.

TACACS +

TACACS+ (Terminal Access Controller Access-Control System Plus) is a protocol developed by Cisco and released as an open standard beginning in 1993. Although derived from TACACS, TACACS+ is a separate protocol that handles authentication, authorization, and accounting (AAA) services. TACACS+ and other flexible AAA protocols have largely replaced their predecessors.

NOTE: This page can set options such as **Fallback if denied access**, **Authorize users authenticated with SSH public key**, and **Enable User-Level attribute of Shell** and raccess services association to local authorization group.



TACACS+ Options

Field	Values	Description
Status	Enabled/Disabled	The provider will be used to authenticate users (default: enabled).
Fallback if denied access	Enabled or Disabled	Recommended: enable this feature if the provider is not available (default: disabled)..
Remote Server	IP address	
Accounting Server	IP address	
Authorize users authenticated with SSH public key	Enabled or Disabled	(default: disabled).
TACACS+ Port	TCP Port	(default port: 49).
Service	pppshellraccess	Authentication service used by TACACS (default: raccess).
Secret/Confirm Secret	Secret	
Timeout	Number	Communication timeout in seconds (default: 2)
Retries	Number	Number of retries before connection fails.
TACACS+ Version	V0V1V0_V1V1_V0	TACACS version to be used (default:V1).

Field	Values	Description
Enable User-Level attribute of Shell and raccess services association to local authorization group	True/False	
User Level 1 - 10	Nodegrid group name	

RADIUS

RADIUS is a client/server protocol that runs in the application layer and uses TCP or UDP as transport. Operating on port 1812, it provides centralized Authentication, Authorization, and Accounting (AAA) management for users.

The Nodegrid Platform allows multiple methods to assign Radius users to Nodegrid groups. Configuration settings include:

Radius Service Types can be assigned to Nodegrid groups using the settings in the Authentication provider

On the Radius server, the attribute Framed-Filter-ID may be used to assign a user to a Nodegrid group Example: Framed-Filter-ID = "group_name=<ng-groupname>[,<ng-groupname1>];"

Nodegrid supports Vendor-Specific Attributes (VSA) for authorization purposes. Two properties must be defined on the Radius server:

VENDOR ZPE 42518

ATTRIBUTE ZPE-User-Groups 1 string

Each authorized user needs the ZPE-User-Groups attribute assigned. The value is a comma-separated list of Nodegrid Group names.

FreeRadius Server Configuration

CLI Procedure

This is an 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
```

- 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
```

Radius Options

Field	Values	Description
Status	True/False	This provider is used to authenticate users (default: enabled).
Fallback if denied access	Enabled or Disabled	Recommendation: enable this feature if the provider is not available (default: disabled).
Remote Server	IP address	
Accounting Server	IP Address	
Secret / Confirm Secret	Secret	
Timeout	Number	Communication timeout in seconds (default: 2).
Retries	Number	Number of retries before connection fails
Enable ServiceType attribute association to local authorization group	True/False	Allows assignment of Radius Service Types to Nodegrid local groups.
Service Type Login	Nodegrid group name	
Service Type Framed	Nodegrid group name	
Service Type Callback Login	Nodegrid group name	
Service Type Callback Framed	Nodegrid group name	
Service Type Outbound	Nodegrid group name	

Field	Values	Description
Service Type Administrative	Nodegrid group name	

Kerberos

Kerberos is a computer network authentication protocol that uses tickets to allow nodes to securely communicate over a non-secure network. Designed primarily as a client–server model, it provides mutual authentication between nodes. The user and the server verify each other's identity. Built on symmetric key cryptography a trusted third party is required (optionally, public-key cryptography may be used). UDP port 88 is used by default.

Kerberos Options

Field	Values	Description
Status	True/False	This provider is used to authenticate users (default: enabled).
Fallback if denied access	Enabled or Disabled	Recommendation: enable this feature if the provider is not available (default: disabled).
Remote Server	IP address	
Realm Domain Name	Kerberos realm name	
Domain Name	domain name	

RSA SecurID, 2-factor authentication

Add SecurID Server

WebUI Procedure

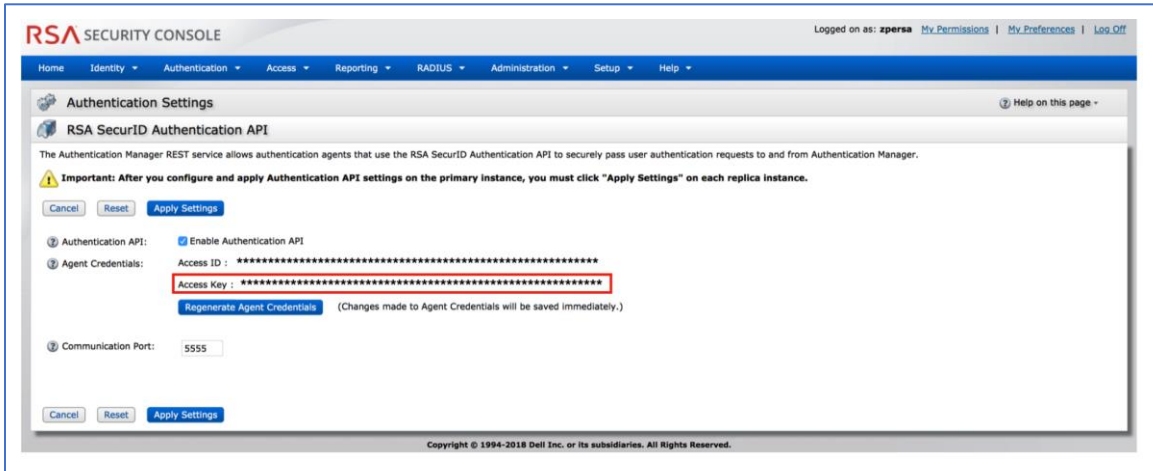
1. Login as admin and go to: *Security :: Authentication*.
2. On the **2-Factor** sub-tab, click **Add**.
3. Enter the details:

Name (name to identify the SecurID system, i.e., SecurID)

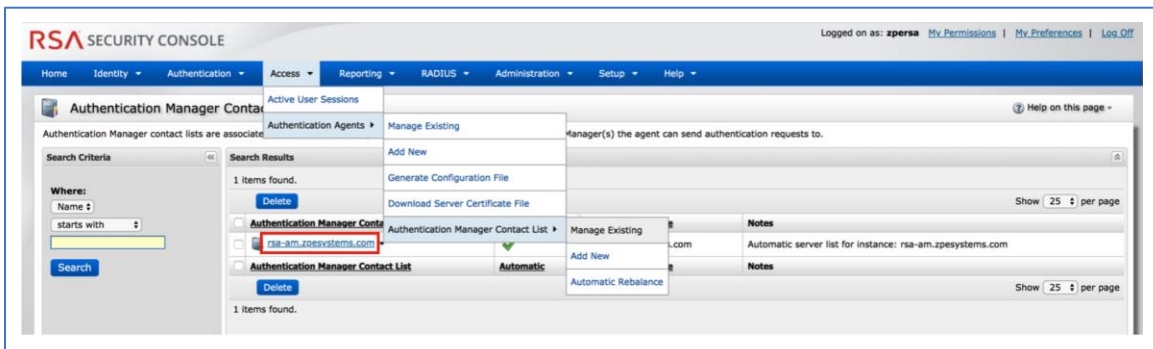
Rest URL (URL to access the SecurID Authentication API (format: https://:5555/mfa/v1_1/authn))

Enable Replicas (Rest Service URL to failover to the server. Can be up to 15 replicas. One per line, i.e., rsa-am-replica2.zpesystems.com:4444, 192.168.2.229:5555)

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*.)



4. Select Cloud Authentication Service checkbox (if enabled, two required fields display).

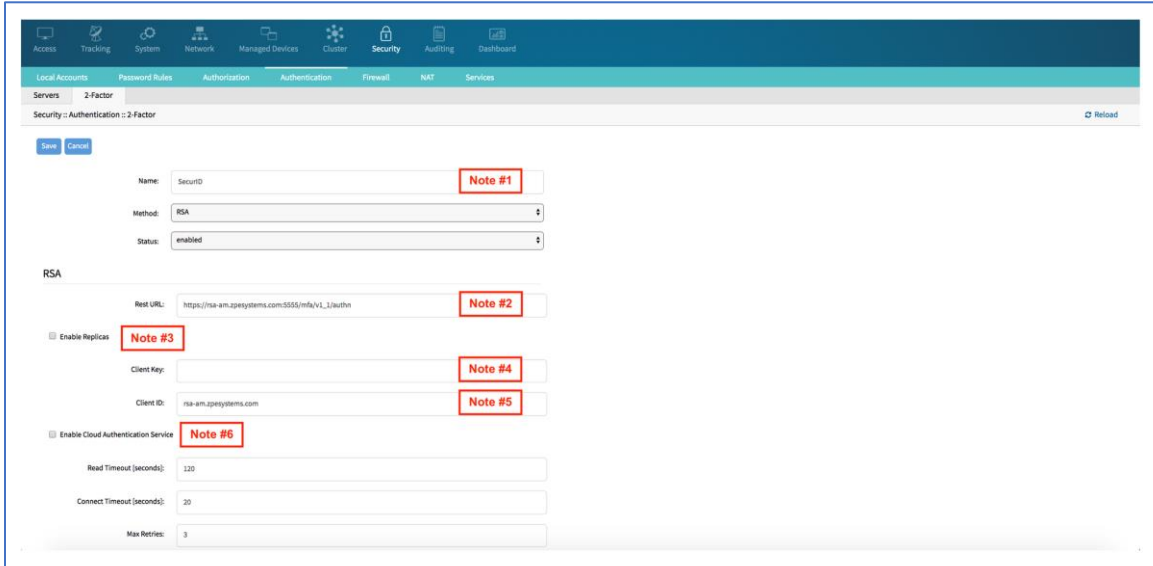
Enable Cloud Authentication Service

Policy ID:

Tenant ID:

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)

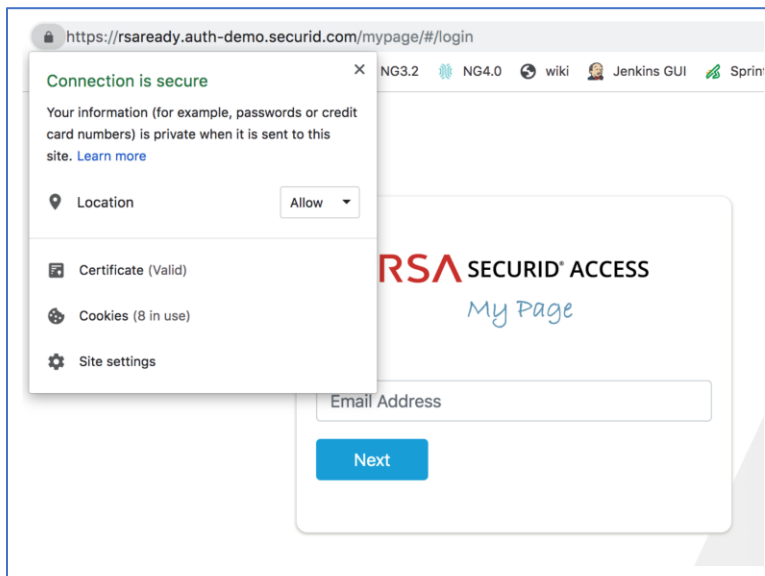


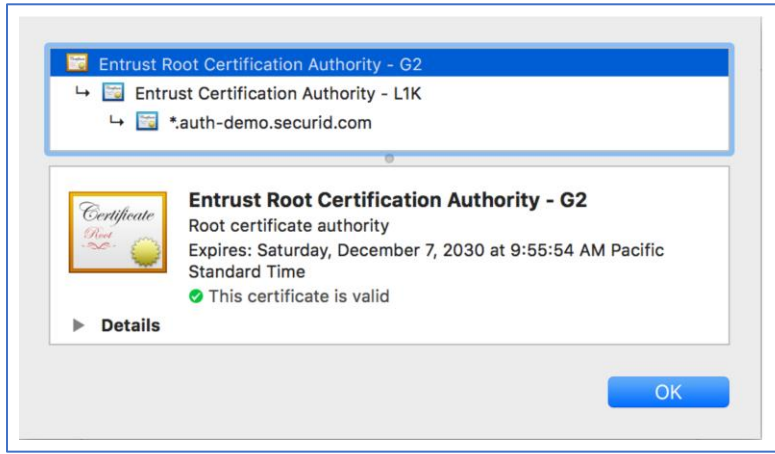
5. Click **Save**.

Set Certificate to access SecurID Server

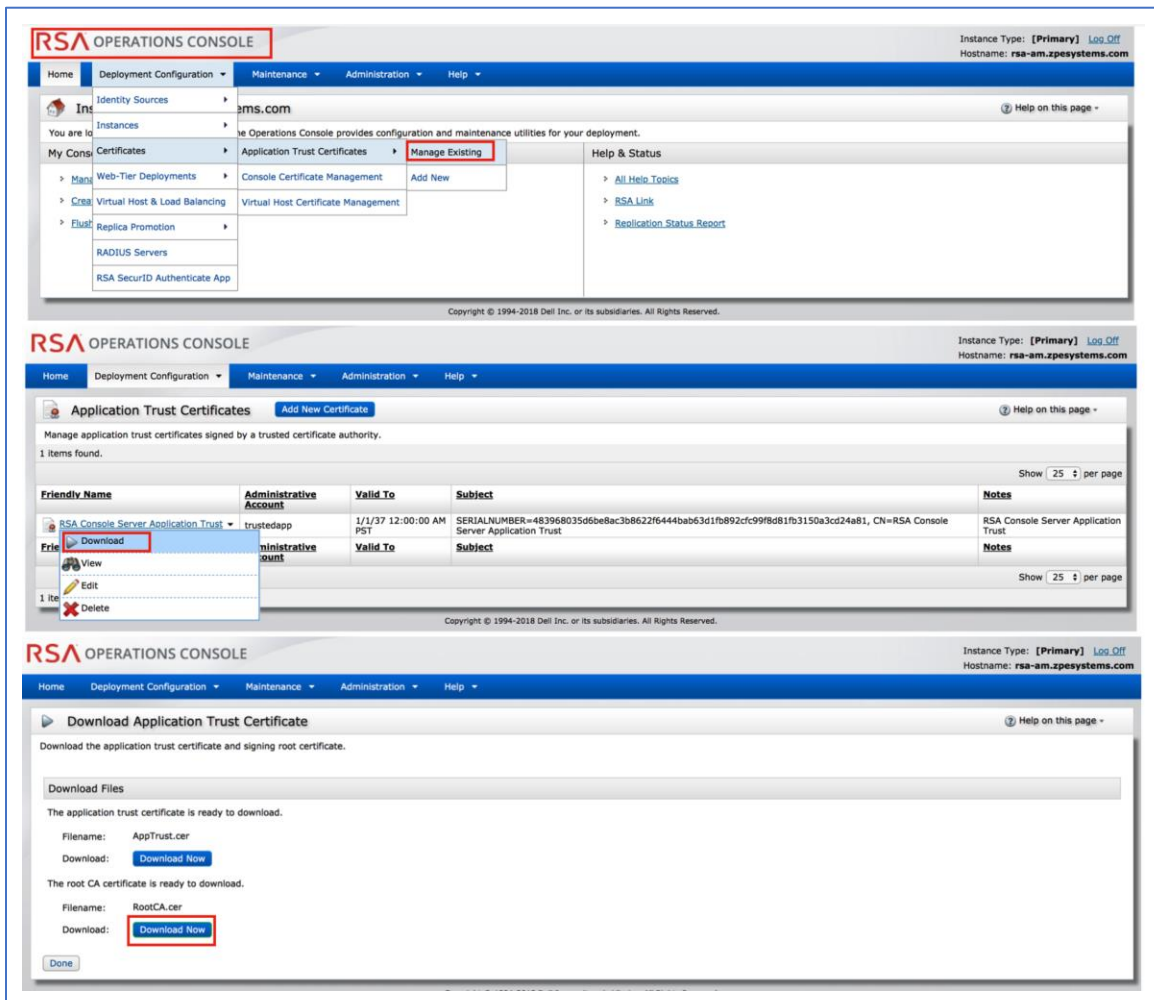
WebUI Procedure

1. If RSA server is through Cloud Authentication, go to RSA SecurID Access, and click on the **Lock** icon (next to URL).
2. Locate and click on the Certificate.
3. On the pop-up dialog, click on the first/top certificate, and drag it to your desktop (this copies it to your desktop).
4. Upload certificate Nodegrid (certificate is automatically converted to the expected format).





5. If not via Cloud, go the *RSA Operations Console* and download the Signing Root Certificate.



6. To upload certificate, login to WebUI (if needed).
7. Go to *Security :: Authentication*.
8. On the **2-Factor** sub-tab, click the link representing the SecurID server (added in step above)..

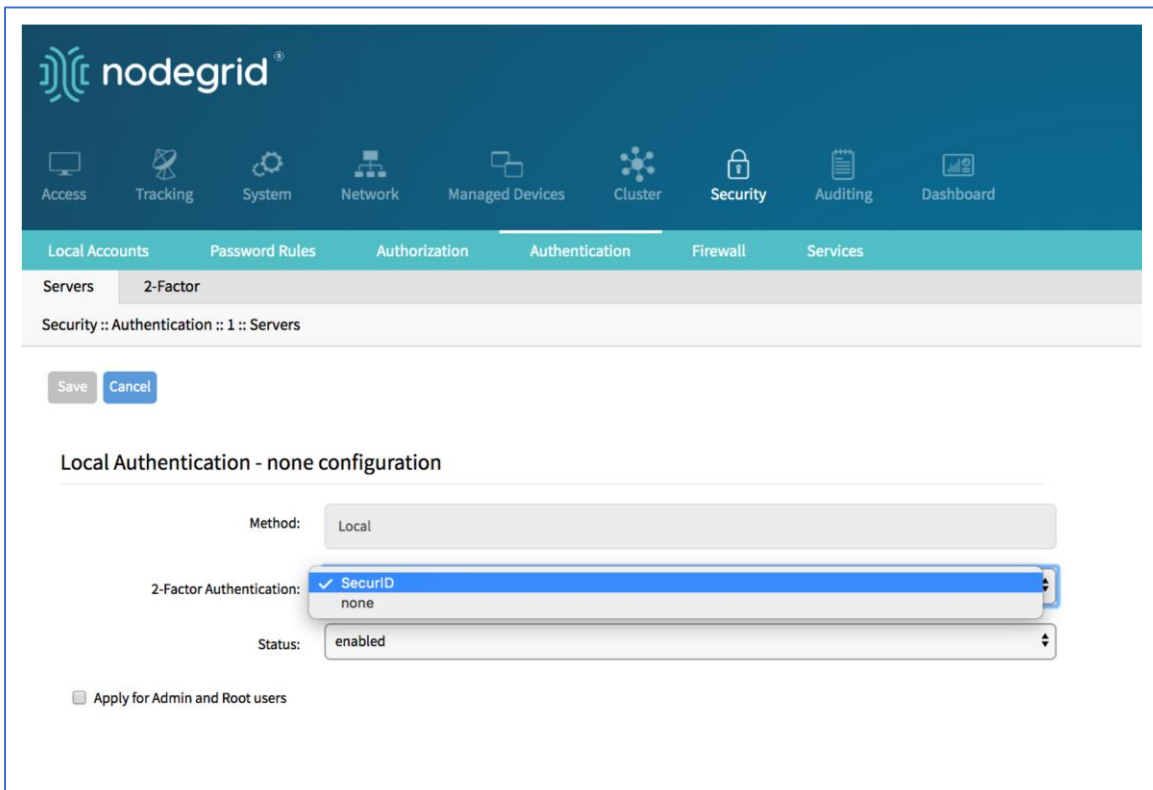
9. Click **Certificate**.
10. Select **Local Computer** checkbox, and click **Choose File**.
11. Browse to the certificate location and select it (i.e. RootCA.cer file).
12. Click **Apply**,

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.



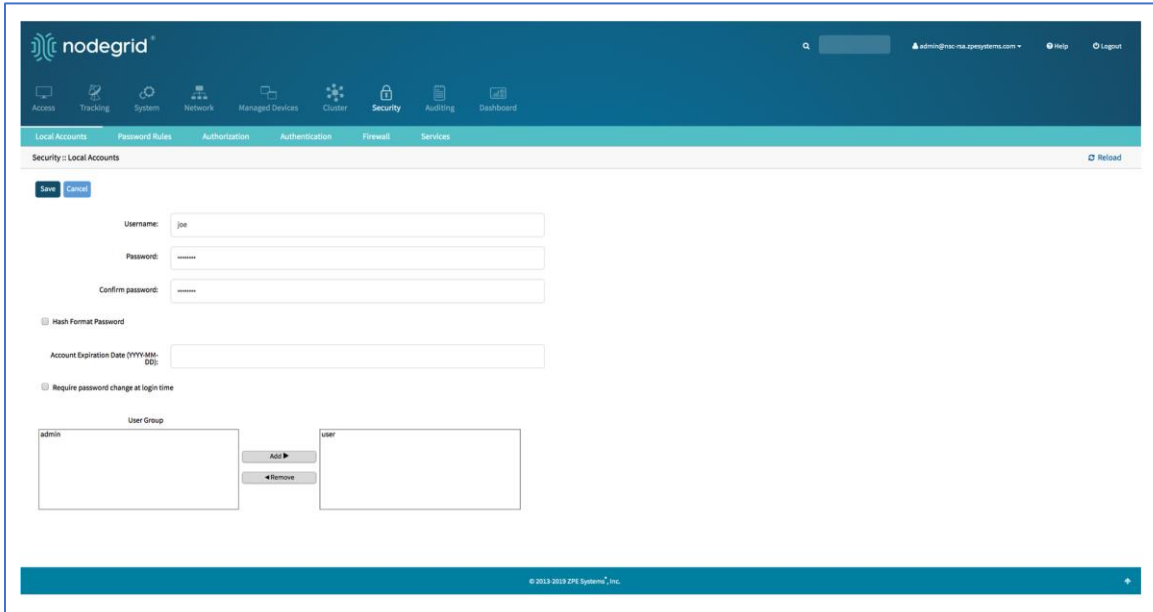
NOTE: For Local authentication method, 2-factor can be enforced or skipped. This allows local Nodegrid administrators to login without needing to configure counterpart users in the RSA Security Console.

Configure a user in Nodegrid local accounts

When 2-factor is enabled, the user provides credentials and the pass code to access Nodegrid. Users must be configured on the RSA Security Console.

WebUI Procedure

1. Go to *Security :: Local Accounts*.
2. Click **Add**.

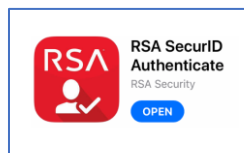


3. Enter **User Name**.
4. Enter **Password** and **Confirm Password**.
5. Click **Save**.

NOTE: The exact same users must be configured in RSA SecurID with an assigned token.

Authenticate App

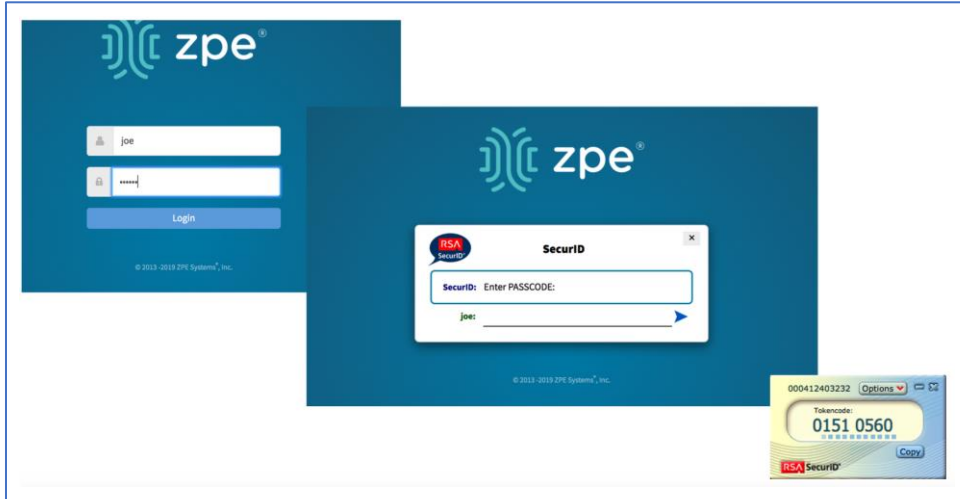
This applies only to Cloud Authentication Services.



1. Download the *RSA SecurID Authenticate* app.
2. Go to **RSA SecurID Access** and login.
3. Follow the steps to register the device.

Login Process

On login in Nodegrid, provide the user credentials. If 2-factor authentication is required, the login process prompts for the information as requested by SecurID.



Firewall tab

When configured by an administrator, the Nodegrid device functions as a Firewall. There are six built-in default chains, three for IPv4 and three for IPv6. These accept packets (Output, Input, and Forward). As needed, additional user chains can be created and deleted. (Default chains cannot be deleted.) Default policy can be set for each chain. Default policy is set to accept packages.

To manage (add, edit, delete) rules click on the chain name. Existing rules are listed. The following settings are available when configuring rules.

Firewall Settings

Setting	Values	Description
Target	Accept, Drop, Reject, Log, Return	
Source IP/Mask	IP address and mask	
Reverse match for source IP/mask	TRUE/FALSE	
Destination IP/Mask	IP address and mask	
Reverse match for destination IP/mask	TRUE/FALSE	
Input Interface	Any, Available interfaces	One value can be selected.
Reverse match for input interface	TRUE/FALSE	
Output Interface	Any, Available interfaces	One value can be selected.
Reverse match for output interface	TRUE/FALSE	
Enable State Match	New, Established, Related, Invalid	One or multiple values can be selected.

Setting	Values	Description
Reverse state match	TRUE/FALSE	
Fragments	All packets and fragments, unfragmented packets and 1st packets, 2nd and further packets	One value can be selected.
Reject With	Network Unreachable, Host Unreachable, Port Unreachable, Protocol Unreachable, Network Prohibited, Host Prohibited, Administratively Prohibited, TCP Reset	
Protocol	Numeric, TCP, UDP, ICMP	
Protocol - Numeric - Protocol Number	Protocol Number	
Protocol - TCP - Source Port	Port Number	
Protocol - TCP - Destination Port	Port Number	
Protocol - TCP - TCP Flag SYN	Any, Set, Unset	
Protocol - TCP - TCP Flag ACK	Any, Set, Unset	
Protocol - TCP - TCP Flag FIN	Any, Set, Unset	
Protocol - TCP - TCP Flag RST	Any, Set, Unset	
Protocol - TCP - TCP Flag URG	Any, Set, Unset	
Protocol - TCP - TCP Flag PSH	Any, Set, Unset	
Protocol - TCP - Reverse match for TCP flags	TRUE/FALSE	
Protocol - UDP - Source Port	Port Number	
Protocol - UDP - Destination Port	Port Number	
Protocol - ICMP - ICMP Type	Any, Echo Reply, Destination Unreachable, Network Unreachable, Host Unreachable, Protocol Unreachable, Port Unreachable, Fragmentation Needed, Source Route Failed, Network Unknown, Host Unknown, Network Prohibited, TOS Network Unreachable, TOS Host Unreachable, Communication Prohibited, Host Precedence Violation, Precedence Cutoff, Source	

Setting	Values	Description
	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	
Protocol - ICMP - Reverse match for ICMP type	TRUE/FALSE	
Reverse match for protocol	TRUE/FALSE	
Reverse match for source port	TRUE/FALSE	
Reverse match for destination port	TRUE/FALSE	
Log Level	Debug, Info, Notice, Warning, Error, Critical, Alert, Emergency	
Log Prefix	Log Prefix String	
Log TCP Sequence Numbers	TRUE/FALSE	
Log Options from The TCP Packet Header	TRUE/FALSE	
Log Options from The IP Packet Header	TRUE/FALSE	

NAT tab

The NAT section manages (add, edit, delete) defining rules for the Network Address Translation (NAT) table.

There are eight built-in default chains (four for IPv4 and four for IPv6). These accept Pre-routing, Output, Input, and Post-routing packets. Default chains cannot be deleted.

Rules can be created for each chain by clicking on the chain name. This will list all existing rules belonging to the chain. Rules can be created, deleted, and modified. The following settings exist for rules.

NAT Settings

Settings	Values	Description
Target	Accept, Drop, Reject, Log, Return	

Settings	Values	Description
Source IP/Mask	IP address and mask	
Reverse Match for Source IP/mask	TRUE/FALSE	
Destination IP/Mask	IP address and mask	
Reverse Match for Destination IP/mask	TRUE/FALSE	
Input Interface	Any, Available interfaces	One value can be selected.
Reverse Match for Input Interface	TRUE/FALSE	
Output Interface	Any, Available interfaces	One value can be selected.
Reverse Match for Output Interface	TRUE/FALSE	
Enable State Match	New, Established, Related, Invalid	One or multiple values can be selected
Reverse State Match	TRUE/FALSE	
Fragments	All packets and fragments, Unfragmented packets and 1st packets, 2nd and further packets	One value can be selected.
Reject With	Network Unreachable, Host Unreachable, Port Unreachable, Protocol Unreachable, Network Prohibited, Host Prohibited, Administratively Prohibited, TCP Reset	
Protocol	Numeric, TCP, UDP, ICMP	
Protocol - Numeric - Protocol Number	Protocol Number	
Protocol - TCP - Source Port	Port Number	
Protocol - TCP - Destination Port	Port Number	
Protocol - TCP - TCP Flag SYN	Any, Set, Unset	
Protocol - TCP - TCP Flag ACK	Any, Set, Unset	
Protocol - TCP - TCP Flag FIN	Any, Set, Unset	
Protocol - TCP - TCP Flag RST	Any, Set, Unset	
Protocol - TCP - TCP Flag URG	Any, Set, Unset	

Settings	Values	Description
Protocol - TCP - TCP Flag PSH	Any, SetU, nset	
Protocol - TCP - Reverse match for TCP flags	TRUE/FALSE	
Protocol - UDP - Source Port	Port Number	
Protocol - UDP - Destination Port	Port Number	
Protocol - ICMP - ICMP Type	Any, Echo Reply, Destination Unreachable, Network Unreachable, Host Unreachable, Protocol Unreachable, Port Unreachable, Fragmentation Needed, Source Route Failed, Network Unknown, Host Unknown, Network 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	
Protocol - ICMP - Reverse match for ICMP type	TRUE/FALSE	
Reverse match for protocol	TRUE/FALSE	
Reverse match for source port	TRUE/FALSE	
Reverse match for destination port	TRUE/FALSE	
Log Level	Debug, Info, Notice, Warning, Error, Critical, Alert, Emergency	
Log Prefix	Log Prefix String	
Log TCP Sequence Numbers	TRUE/FALSE	
Log Options from the TCP Packet Header	TRUE/FALSE	

Settings	Values	Description
Log Options from the IP Packet Header	TRUE/FALSE	

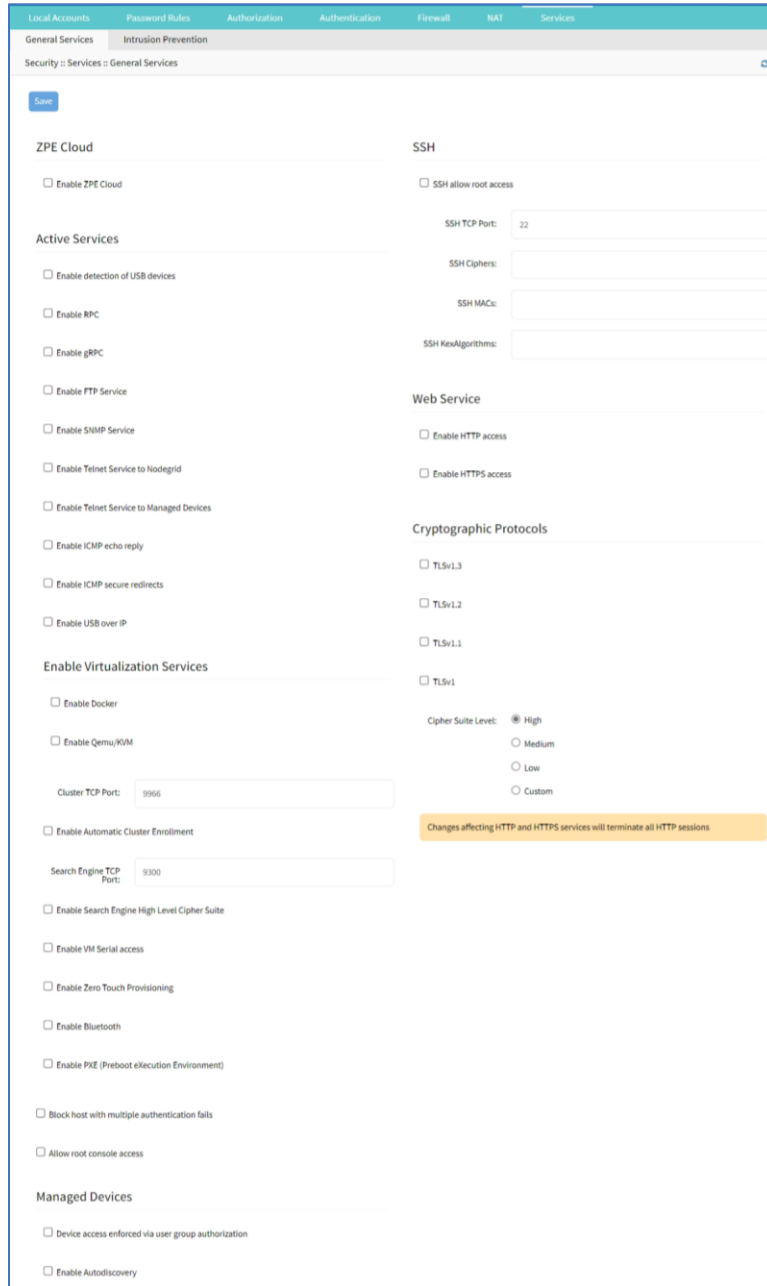
Services tab

This defines Active Services running on the System, as well as general service settings for ZPE Cloud, managed devices, intrusion prevention, SSH settings to the systems, web service settings and cryptographic protocols for the Web Service.

The system's security level is configured here. For instance, unsecured protocols like Telnet or HTTP can be disabled, or the SSH version can be selected.

General Services sub-tab

General security service settings are configured on this page. Because of this complexity, it is recommended to prepare a document that defines how the company security requirements are implemented with the device security settings.



Configure General Services

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 - default: enabled. Nodegrid Serial Console - default: disabled).

Confirm **ZPE Cloud URL** (read-only).

Select **Enable Remote Access** checkbox.

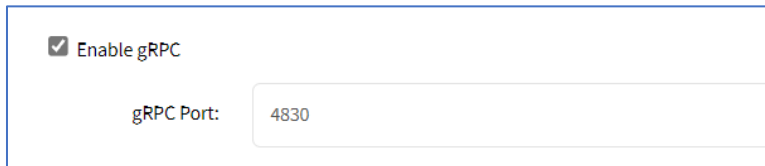
Select **Enable File Protection** checkbox (If enabled, file transfer requires authentication hash based on this password to validate file integrity and origin – default: disabled).

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**.

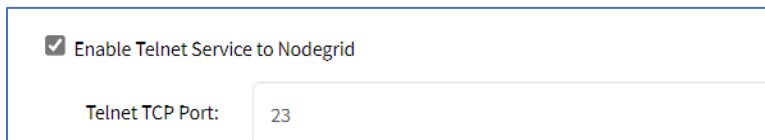


The screenshot shows a configuration panel with a checked checkbox labeled 'Enable gRPC'. Below it is a text input field labeled 'gRPC Port:' containing the value '4830'.

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).



The screenshot shows a configuration panel with a checked checkbox labeled 'Enable Telnet Service to Nodegrid'. Below it is a text input field labeled 'Telnet TCP Port:' containing the value '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.

4. In *Enable Virtualization Services* menu (select all that apply):

Select **Enable Docker** checkbox.

Select **Enable Qemu/KVM** checkbox.

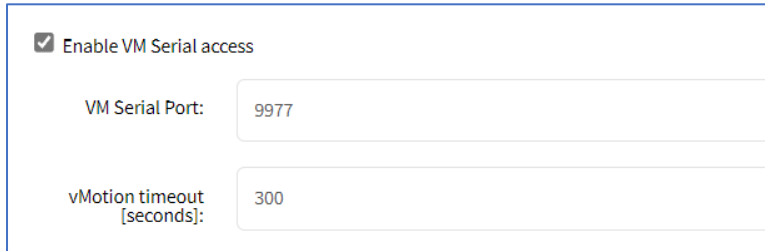
Enter **Cluster TCP Port** (default: 9966).

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).



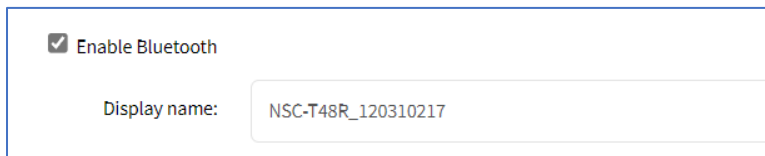
Enable VM Serial access
 VM Serial Port:
 vMotion timeout [seconds]:

Enter **VM Serial Port** (default: 9977).

Enter **vMotion timeout [seconds]** (default: 300).

Select **Enable Zero Touch Provisioning** checkbox (default: enabled).

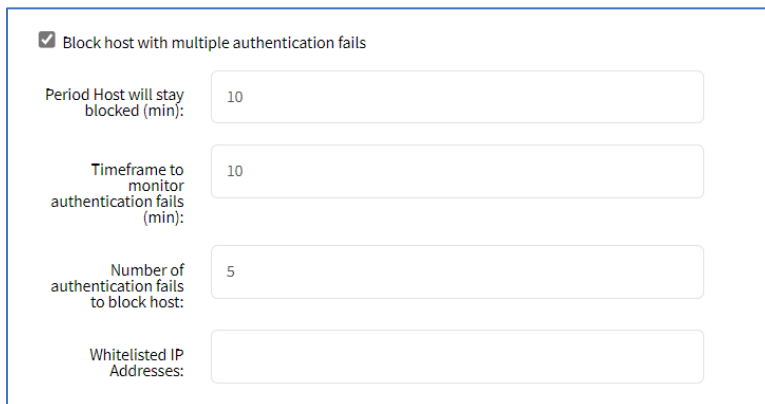
Select **Enable Bluetooth** checkbox. Enter **Display name**.



Enable Bluetooth
 Display name:

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.

Enable Autodiscovery

DHCP lease controlled by autodiscovery rules

Select **DHCP lease controlled by autodiscovery rules** checkbox (default: auto-selected)

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).

Enable HTTP access

HTTP Port:

Enter **HTTP Port** (default: 80).

Select **Enable HTTPS access** checkbox (default: enabled).

Enable HTTPS access

HTTPS Port:

Redirect HTTP to HTTPS

Enter **HTTP Port** (default: 443).

Select **Redirect HTTP to HTTPS** checkbox (default: enabled).

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).

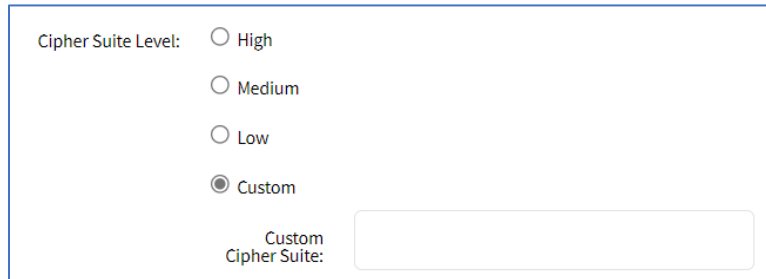
In *Cipher Suite Level* menu, select one:

High radio button.

Medium radio button (default).

Low radio button.

Custom radio button.



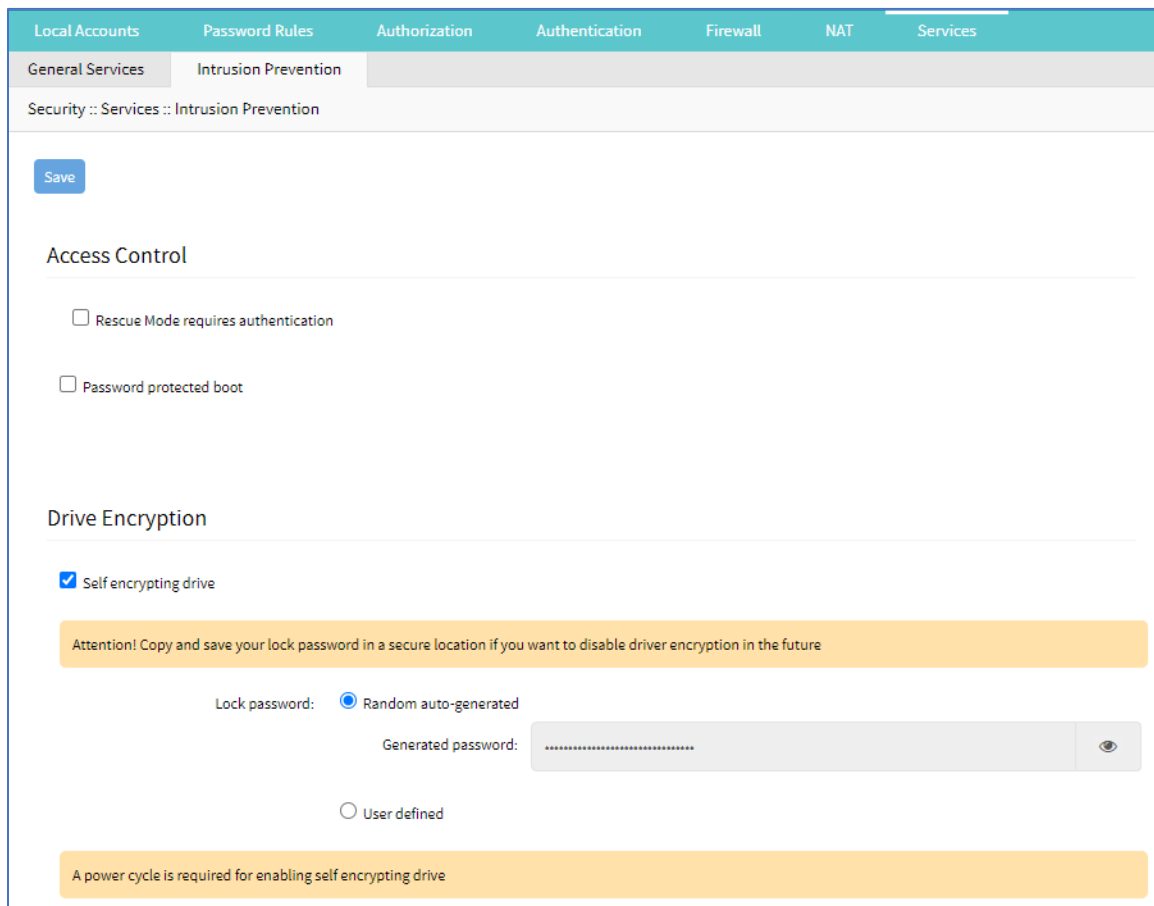
Cipher Suite Level: High
 Medium
 Low
 Custom
Custom Cipher Suite:

Enter **Custom Cipher Suite**.

9. Click **Save**.

Intrusion Prevention sub-tab

This configures intrusion prevention settings.



Local Accounts Password Rules Authorization Authentication Firewall NAT Services

General Services Intrusion Prevention

Security :: Services :: Intrusion Prevention

Save

Access Control

Rescue Mode requires authentication

Password protected boot

Drive Encryption

Self encrypting drive

Attention! Copy and save your lock password in a secure location if you want to disable driver encryption in the future

Lock password: Random auto-generated

Generated password:

User defined

A power cycle is required for enabling self encrypting drive

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**.

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.

Event tab

Categories sub-tab

To review categories of events, go to *Auditing :: Events :: Categories* . These are the categories enabled for each service.

Events	System Events	AAA Events	Device Events	Logging Events	ZPE Cloud Events
ZPE Cloud	-	-	-	-	-
Email	-	-	-	-	-
File	Yes	Yes	Yes	Yes	-
SNMP Trap	-	-	-	-	-
Syslog	Yes	Yes	Yes	Yes	-

Edit Category for an Event Type

WebUI Procedure

1. Go to *Auditing :: Events :: Categories*.
2. Click the **Event name**.
3. Select checkboxes for event categories.

4. Click **Save**.

Settings tab

Data logging captures the data stream on the device, as well as to and from target devices. General settings are available under Auditing :: Settings.

Data Logging Settings

Setting	Values	Description
Enable File Destination	TRUE/FALSE	If enabled, all Data Logs are stored at the defined File location (defined under Auditing Destinations) (default: enabled).
Enable Syslog Destination	TRUE/FALSE	If enabled, all Data Logs are sent to the defined Syslog location (defined under Auditing Destinations) (default: disabled).
Add Timestamp on every line logged	TRUE/FALSE	If enabled, a timestamp is added to each data log line.
Timestamp Format	UTC, Local Time	Timestamp or time zone (default: UTC).

Events tab

Events are automatically created 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.

Four event categories can be individually controlled:

- Systems Events
- AAA Events
- Device Events
- Logging Events

Go to *Tracking :: Event List* for all listed events and associated categories. Each event category can be configured to send the events to any of the four event destinations or to none.

Event Destinations are:

- File - This can be local File storage or NFS file storage
- Syslog - This can be local Syslog or remote
- SNMP Trap
- Email

Destinations

File

By default, data logs are written to local files. The file destination and archive settings can be set under *Auditing :: Destinations :: File*.

NOTE: NFS requires RPC service to be enabled (go to *Security :: Services*).

File Destination and Archive Settings

Setting	Values	Description
Destination	localNFS	
NFS - NFS Server	IP address of NFS Server	
NFS - NFS Path	Path to the NFS root directory	Each device should have its own root directory.
File Size [Kbytes]	File size in Kbytes	File size at which the file is rotated. Valid values are between 0 (disabled) and 2048 Kb (default: 1024).
Number of Archives	Number	Number of archive files kept before discarded (default: 0) (maximum: 99).
(NFS) Archive by Time [HH:MM]	Time in format HH:MM	Time when the file archive is rotated (default: blank).

Syslog

Support destinations are: local Syslog destination or remote IPv4 and IPv6 destination.

Syslog Options

Setting	Value	Description
System Console	TRUE/FALSE	Syslog events displayed on device console port sessions (default: enabled).
Admin Session	TRUE/FALSE	Syslog events displayed on any open admin session on the device (default: disabled).
IPv4 Remote Server	IP address	One or more IP addresses (comma-separated).
IPv4 Address or Hostname	TRUE/FALS	(default: disabled)
IPv6 Remote Server	IP address	One or more IP addresses (comma-separated).

Setting	Value	Description
IPv6 Address or Hostname	TRUE/FALSE	(default: disabled)
Event Facility	Log Local 0, Log Local 1, Log Local 2, Log Local 3, Log Local 4, Log Local 5	Syslog logging facility for Events.
Data Logging Facility	Log Local 0, Log Local 1, Log Local 2, Log Local 3, Log Local 4, Log Local 5	Syslog logging facility for data logs.

SNMP Trap

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.

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
    
```

NOTE: SNMP3 INFORM messages are currently not supported.

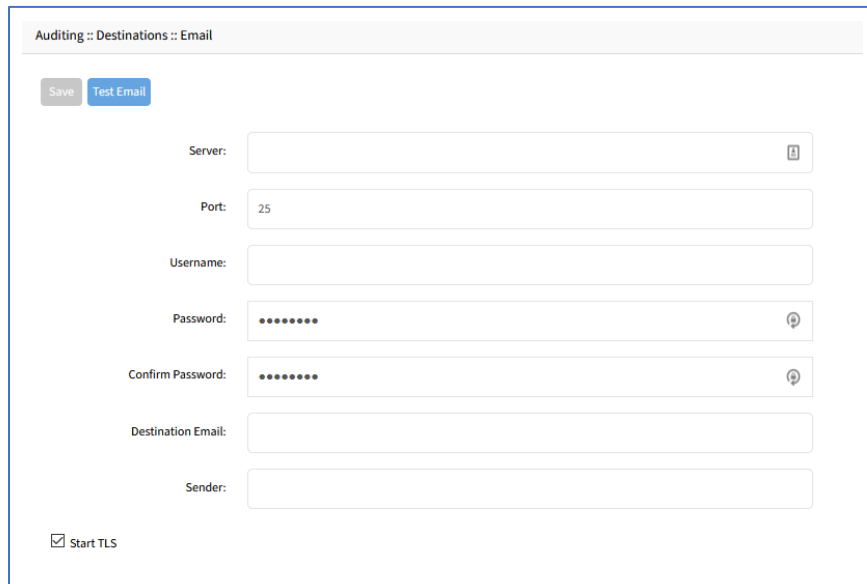
SNMP Trap Settings

Setting	Value	Description
SNMP Engine ID	none	Displays the systems Engine ID
Server	IPv4 or IPv6 IP address	
Transport Protocol	UDP-IPv4, TCP-IPv4, UDP-IPv6, TCP-IPv6	Protocol to send traps (default: UDP-IPv4).
Port	TCP port	(default: 161)
Trap Version	Version 2c, Version 3	SNMP version to be used.
Version 2c - Community	Community name	
Version 3 - User Name	User name	
Version 3 -Security Level	noAuth, NoPrivauth, NoPrivauthPriv	
Version 3 -Authentication Algorithm	MD5, SHA	

Setting	Value	Description
Version 3 -Authentication Password	Password	
Version 3 -Privacy Algorithm	DES, AES	
Version 3 -Privacy Passphrase	Pass phrase	

Email Notification

Events can be sent to an email address.



Email Notification Settings

Setting	Value	Description
Server	SMTP server address	
Port	TCP port to be used	(default: 25)
Username	Username	
Password	Password	
Confirm Password	Password	
Destination Email	Email address	Target email address for events.
Start TLS	TRUE/FALSE	If TLS is used for the communication.

Monitoring Section

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.

Monitoring Templates

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

Setting	Value	Description
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 discover 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.

Setting	Value	Description
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. In the **Managed Device** section, access the device.
2. On the device, go to *Management*.
3. Enable and configure the required monitoring protocol like SNMP or IPMI
4. Enable Monitoring and assign the template and assign the collection interval.
5. Click **Save**.

Supported Nodegrid Devices

USB Sensors

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.

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
```

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.

VRRP support is implemented through *keepalived* services. Official documentation for the service is available on the [Keep Alived web site](#).

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
```


Dashboard Section

The Dashboard allows visual presentations of Event Details, Managed Device details, and monitoring data from the device and the Managed Devices. Several dashboards can be created for different purposes. For example, one to monitor managed devices data points such as Power Consumption, Voltage (V), Current (A), Temperature, Fan speed, and many more. There are options to show data from different periods of times (i.e., last 15 minutes, last hour, last day, this week, this month, last five years).

NOTE: The Dashboard feature is only available through the WebUI

Data Point Exploration

This provides an example on how to verify collected data are stored, and details on the collected data.

Collect Raw Data Points

1. Go to *Dashboard :: Discover*.
2. Select **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 the Search field to search for a specific device or data point.
5. Verify that data points were collected, and inspect the available fields.

NOTE: Collected data is buffered before stored. A couple collection cycles can occur before the data is visualized.

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.

Field	Value	Description
type_instance	Data Point Name	Name of the element associated with measurement.

Device fields (logstash-* Index)

Field	Values	Description
name	Device Name	The name of the device being monitored.
mode	enabled, on demand, disabled	operational mode of the device.
type	device type	Device type as assigned under Managed Devices.
family	ilo, drac, ipmi_1.5, ilmi_2.0, cimc_ucs, device_console, pdu	Device family.
addr_location	Address	
coordinates	Coordinates	
ip	IP address	
mac	MAC address	The MAC address of the device, if known.
alias	IP address alias	
groups	list of groups	Authorization groups granted access to the device.
licensed	yes, no	Device license state.
status	connected, disconnected, in-use, unknown	Current status of the device.
nodegrid	Nodegrid hostname	Hostname of the Nodegrid that controls the device.
custom fields		Any custom field configured for the device.

Event fields (*_date_* Index)

Field	Value	Description
event_id	Number	Event ID number.
event_msg	Text	Event Message.
host	Nodegrid hostname	Hostname of the Nodegrid where Event occurred.
message	Text	Full message text.

Create a Visualization

Visualizations display aggregate data in a variety of options. Following are descriptions of data presentation.

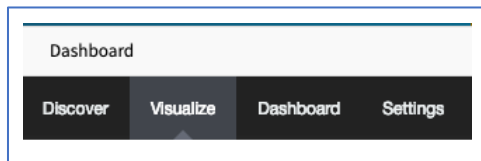
Line Charts

Line Charts allow the visualization of data points along the line graph.

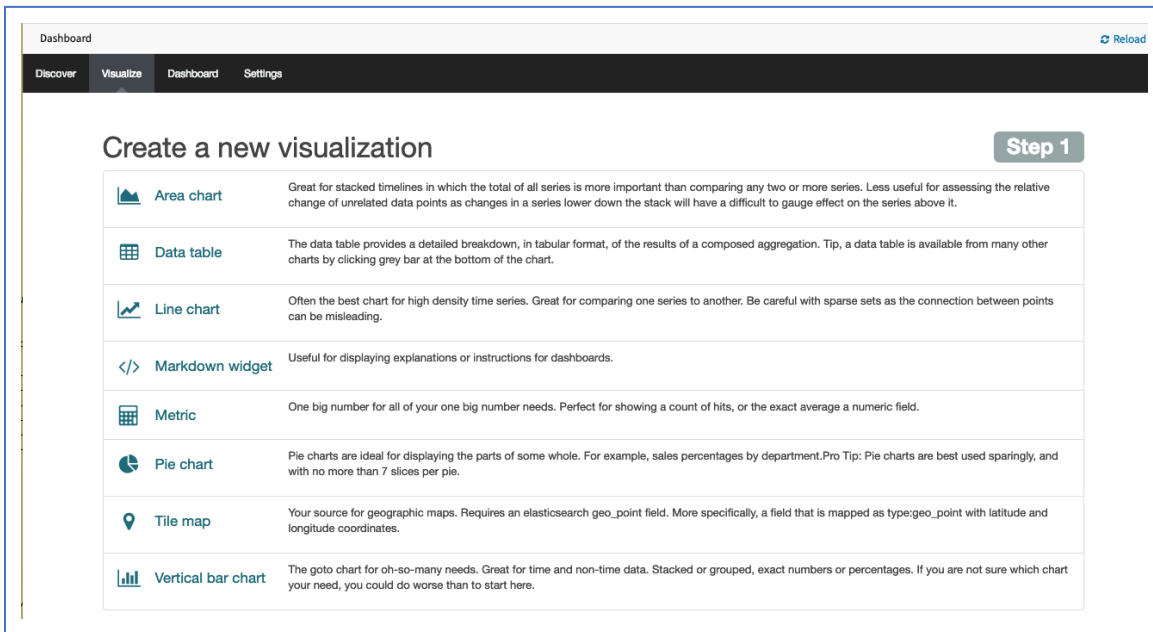
Create a Single or Multi-Line Chart

WebUI Procedure

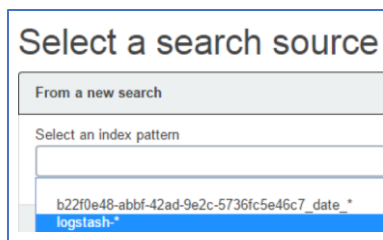
1. Click **Visualize**



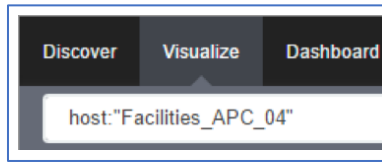
2. On the *Create a new visualization* dialog, select a **Line Chart**.



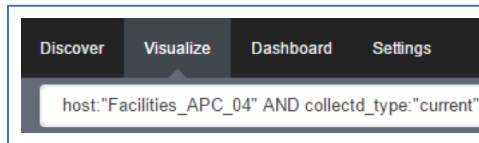
3. On the *Select a search source* menu, **From a new search** drop-down, select **logstash-*** as the index pattern



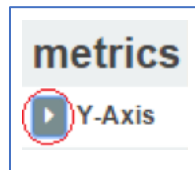
- To select the data points to visualize, enter a search expression, i.e., <device name>.



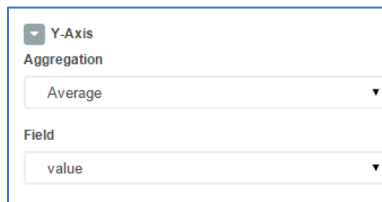
- As needed, the search expression can be extended to be more selective.



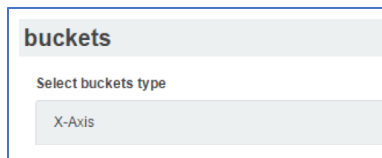
- Click on the **Y-Axis** metrics Arrow to expand it.



- On the dialog, select **Average for Aggregation** and enter a **Field** value.

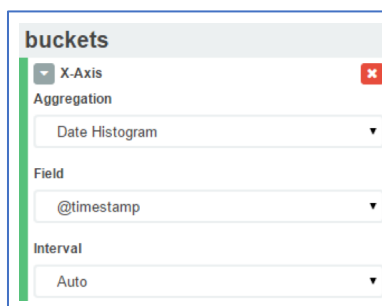


- Click on **X-Axis**.



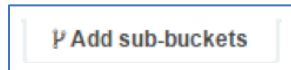
- For **Aggregation**, select **Date Histogram**. Accept **Field** and **Interval** defaults.

For a single line graph visualization, click **Save** and enter a **Title**.

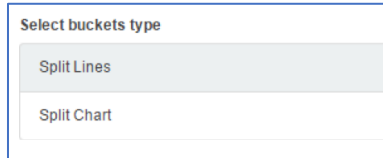


For a multi-line graph visualization, continue with the next steps.

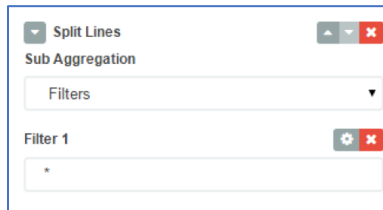
10. To add multiple data points, click Add sub-buckets.



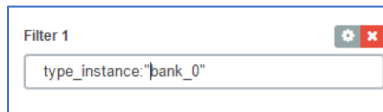
11. Click on **Split Lines**.



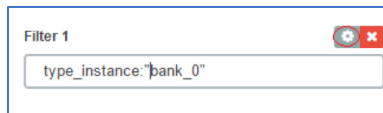
12. On **Sub Aggregation** drop-down, select **Filters**.



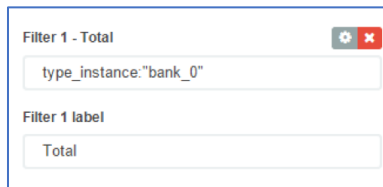
13. In **Filter 1**, enter a search expression for the elements to visualize.



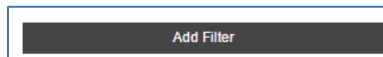
14. (optional) To associate a label, click the **Settings** icon



15. In **Filter 1 label** field, enter the label.



16. To add another element, click **Add Filter**.



17. Repeat the add filter for all additional elements.

Filter 1 - Total ⚙️ ✖️

Filter 1 label

Filter 2 - Bank 1 ⚙️ ✖️

Filter 2 label

Filter 3 - Bank 2 ⚙️ ✖️

Filter 3 label

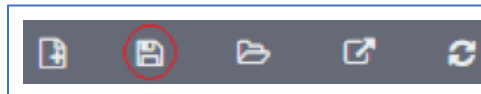
18. To refresh the graph based on the configuration, click on the green arrow.



The graph presents the configuration details. As needed tweak the entries.



19. Click **Save**.



20. Enter **Title** for the visualization and click **Save**.

Title

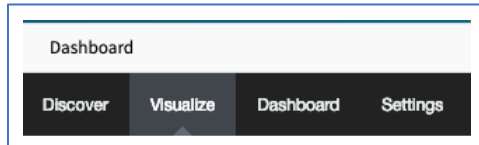
Save

Area Charts

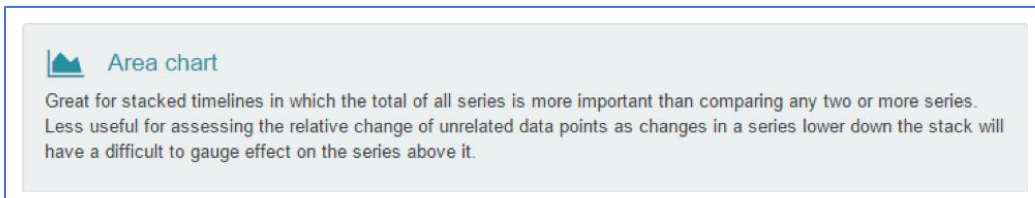
The area chart is useful for stacking measurements for different although related entities, such as the outlets of a PDU.

NOTE: Become familiar with the Line Chart procedure before creating an Area Chart,

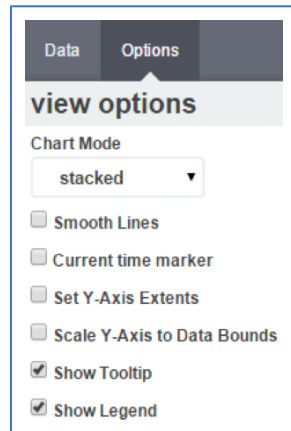
1. Click **Visualize**.



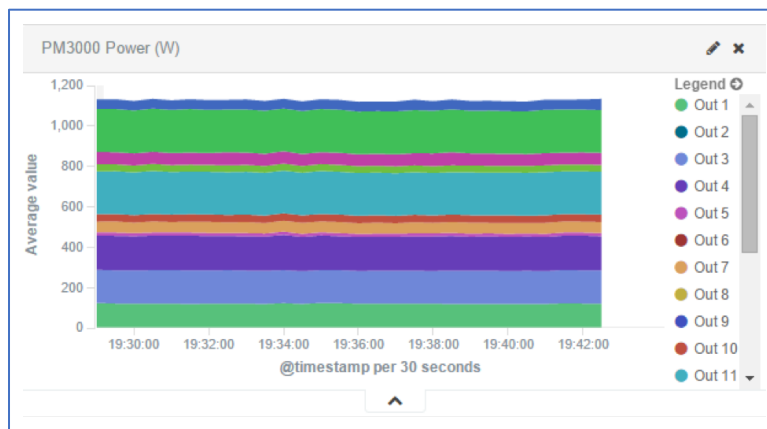
2. Select **Area chart**



3. In **Options** tab, **Chart Mode** drop-down, select **stacked**.

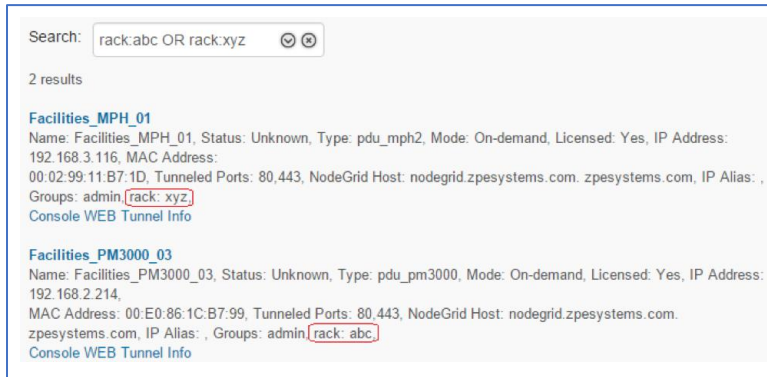


This is the appearance of such a visualization

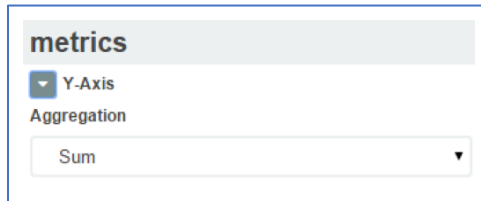


NOTE: Search expressions are used to select/limit data points on the visualization. They can be used as a filter for the whole visualization, as sub-aggregation filters, or as a filter for the whole dashboard.

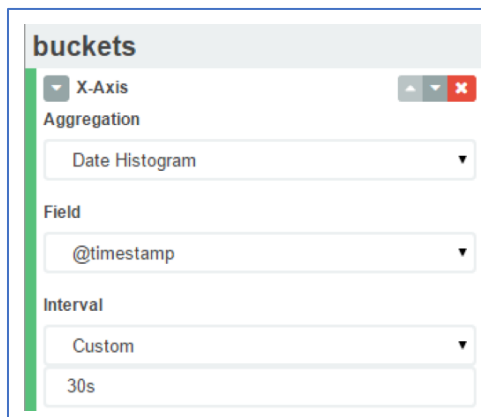
Search expressions are not restricted to data point fields. An expression can also refer to fields associated with the device (type, IP address, groups, custom fields, and more). For example, to collect current from each outlet in a selection of Rack PDUs, use one custom field “rack:abc” with another custom field “rack:xyz”.



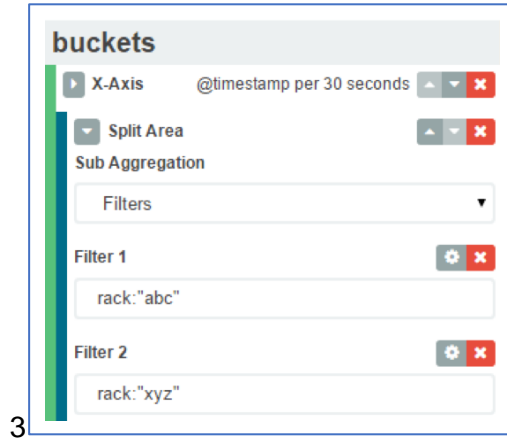
4. The following steps show the total sum of the current provided by outlets of each Rack PDU.
5. On **metrics**, Y-axis, set the **Aggregation** drop-down, select **Sum**.



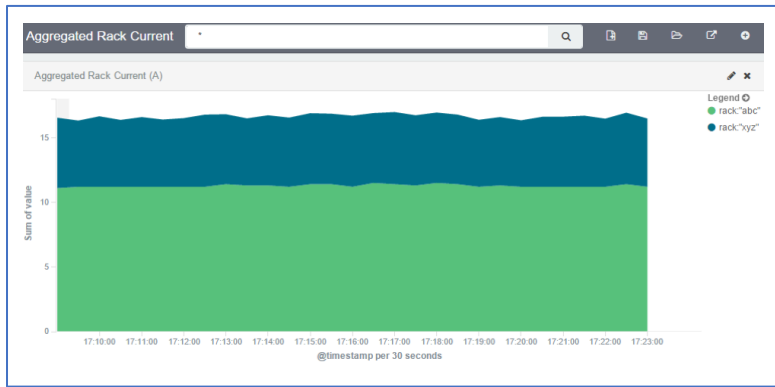
6. On **Buckets**, set the **Interval** to match the collecting period.



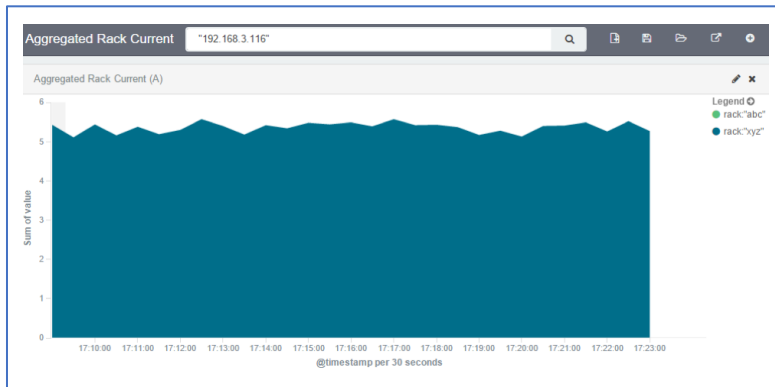
7. On **Buckets**, set **Sub-Aggregation** filters to custom fields.



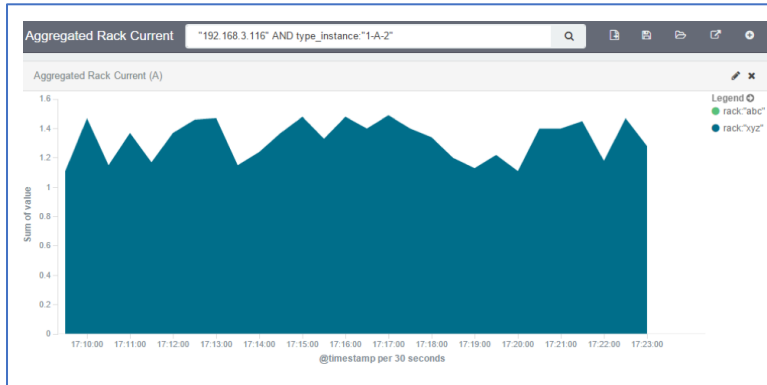
8. The resulting visualization would look like this:



9. Add Filters to display the values of only one Rack PDU with the IP address.



10. Additional filters can be used as needed, all from the same visualization.



11. Click **Save**.
12. Enter **Title** for the visualization and click **Save**.

NOTE: When using area charts be careful to not account for the same measurement twice, by mixing power consumers and power producers, or a Rack PDU’s input and output power.

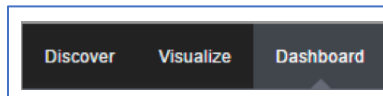
Create a Dashboard

Dashboards are a collection of one or more visualizations. These objects can be created, modified, and deleted..

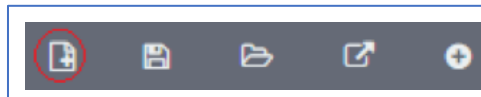
Create a New Dashboard

WebUI Procedure

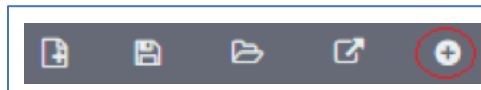
1. Click **Dashboard**.



2. Click the **New Dashboard** icon.

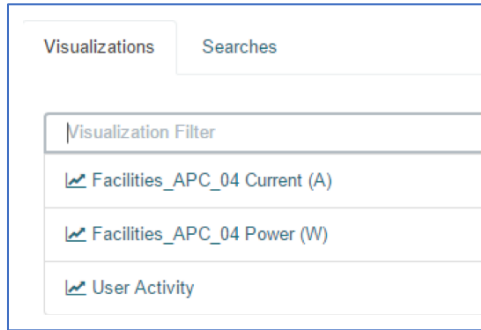


3. Click **Add Visualization** icon.



This will show the previously saved visualizations.

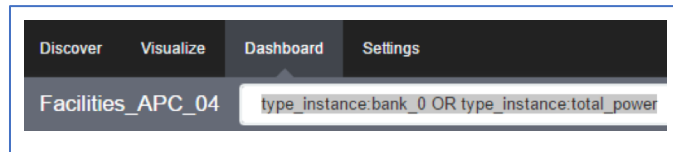
4. Click the visualization to be added to the Dashboard.
5. Add other visualizations, as needed.



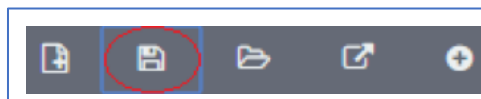
6. On the panel, resize and reposition the graphs.



7. If applicable, filters can be added to the Dashboard.



8. Click **Save** icon.



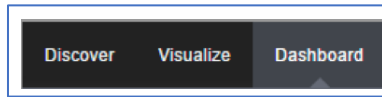
9. On **Save As**, enter the Dashboard Name, then click **Save**.

Inspect a Dashboard

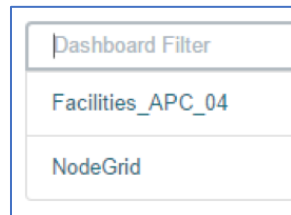
View a Dashboard

WebUI Procedure

1. Click **Dashboard**.



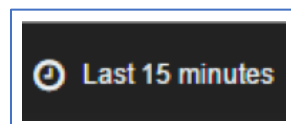
2. Click the **Folder** icon.
3. Click the Dashboard name. As needed, in **Dashboard Filter**, enter a search expression.



4. View the displayed Dashboard.



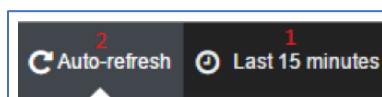
5. To adjust the time frame, click the **Clock** icon.



6. Select a new time frame.



7. To automatically refresh the Dashboard, click the **Auto-refresh** icon and select the refresh frequency.



Applications Section

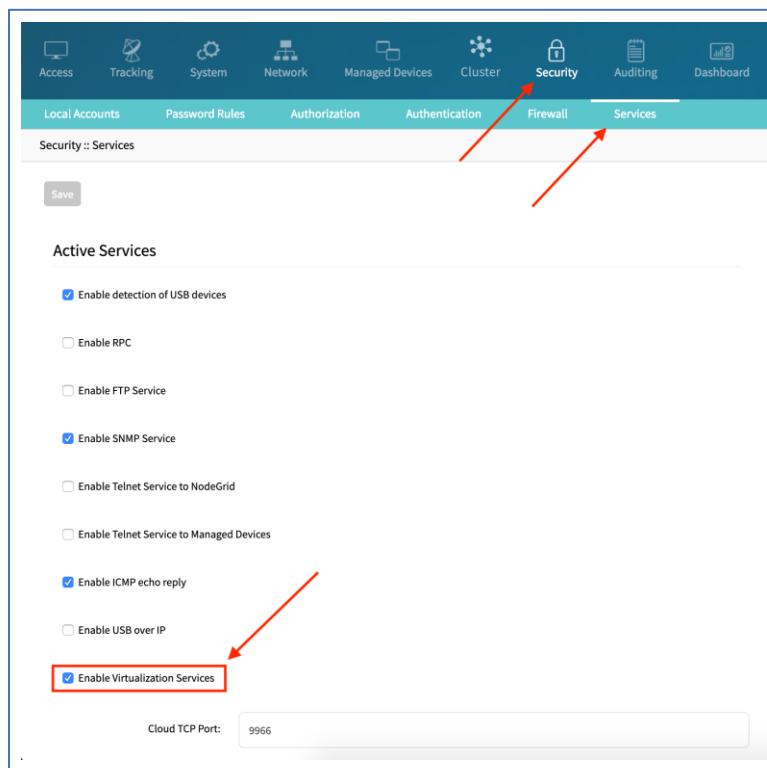
Nodegrid devices can run additional applications. These mostly expand software capabilities. The most used apps are in the areas of monitoring and SD-WAN. While all Nodegrid units support this feature, the Services Router Family is specifically designed to run applications to provide a wide variety of connectivity options.

NOTE: To run applications, additional licenses are required.

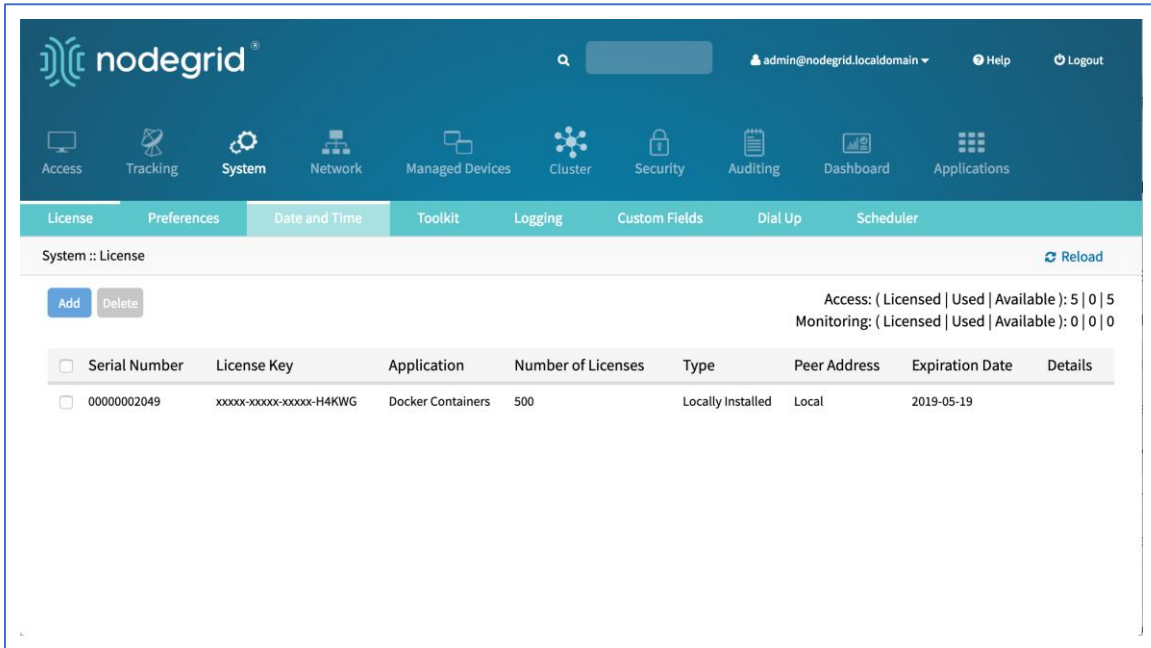
Docker Applications

Docker is an open platform to build, ship and run distributed applications. Administrators can run Docker apps on Nodegrid. Docker applications can be pulled from **Docker Hub**, starting and stopping of the Docker Containers.

NOTE: To activate virtualization, go to *Security :: Services* and select **Enable Virtualization Services**. This is necessary to run NFV's or Docker apps. Both features require licenses (System :: License).



To view licensed applications, go to *System :: Licenses*.



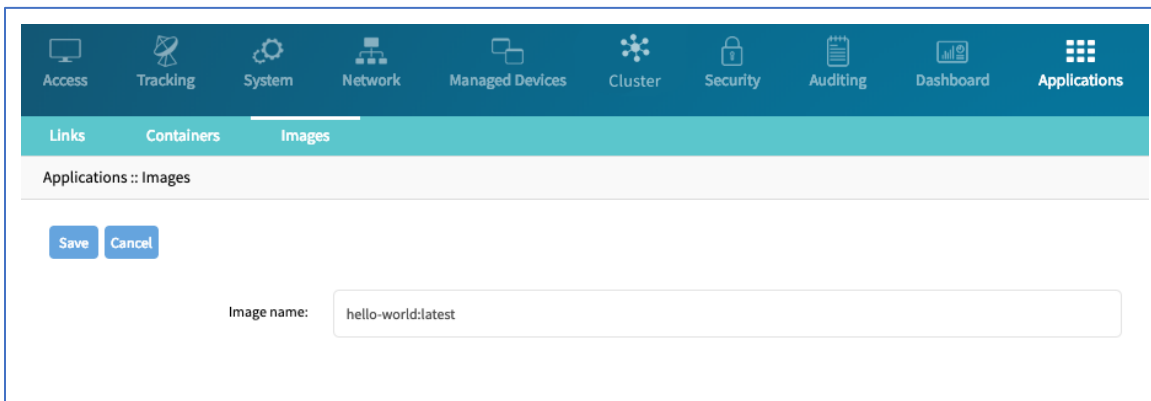
NOTE: The management of Docker Applications is currently only available through the WebUI. The WebUI provides a basic interface to manage Docker Containers. For more advanced features, administrators can use the docker command line tools.

Docker Images

To download (and delete Docker container images, go to *Applications :: Images*. To access **Docker Hub**, Nodegrid requires direct network access.

Download New Images

1. Go to *Applications :: Images*.
2. Click **Add**.
3. Provide the image to download (for specific versions, use the : separator).



4. Click on **Save**. This downloads the image.

Links Containers Images		
Applications :: Images		Reload
Add	Delete	
ID	Name	Status
<input type="checkbox"/> sha256:fce289e99eb9bca977dae136fbc2a82b6b7d4c372474c9235adc1741675f587e	hello-world:latest	Complete

Docker Containers

Administrators can add a container based on an existing image. Go to *Applications :: Containers*. The container can be started, stopped, and deleted, as needed.

For additional detail see the official [Docker create](#) documentation.

NOTE: When a container is created, is not automatically started.

Add a Container

WebUI Procedure

1. Go to *Applications :: Containers*.
2. Click **Add**.
3. Provide the following information:

Image name (name of a Docker Image)

List of valid image names can be found under *Applications :: Images*

(optional) **Command** (Command to run within the container)

Hostname (Hostname assigned to the container)

Domain (Domain name assigned to the container)

Container Name (Name of the Docker container)

CPUs (number of CPU's assigned to the container)

Memory(MB) (Amount of RAM assigned to the container)

(optional) **Arguments** (Options to be used on the container)

4. Click **Save**.

Application Links

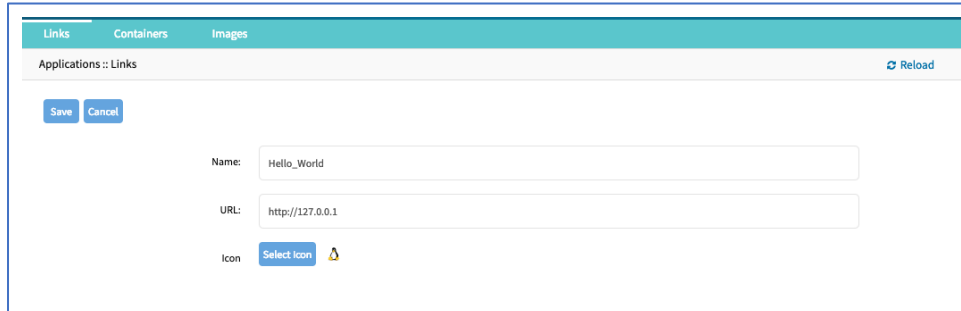
Administrators can create simple web links to run containers and other applications.

Create Application Link

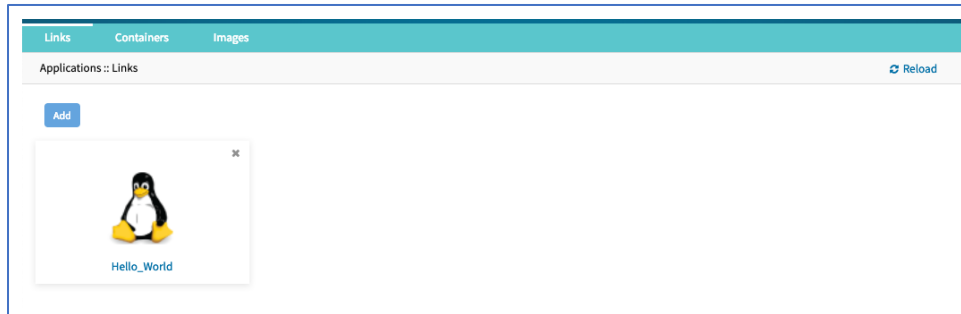
WebUI Procedure

1. Go to *Applications :: Links*.
2. Click **Add**.

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 to test.



NOTE: Depending on the Application, there can be an advantage to create a target device for the created Application.

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. 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/

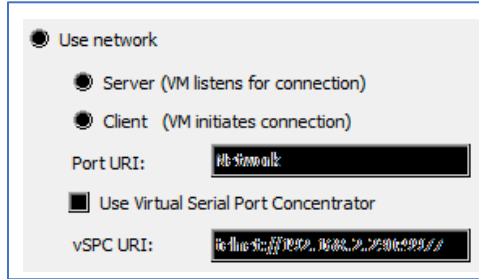
Virtual Serial Port (vSPC) on VM Servers

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**.
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**.

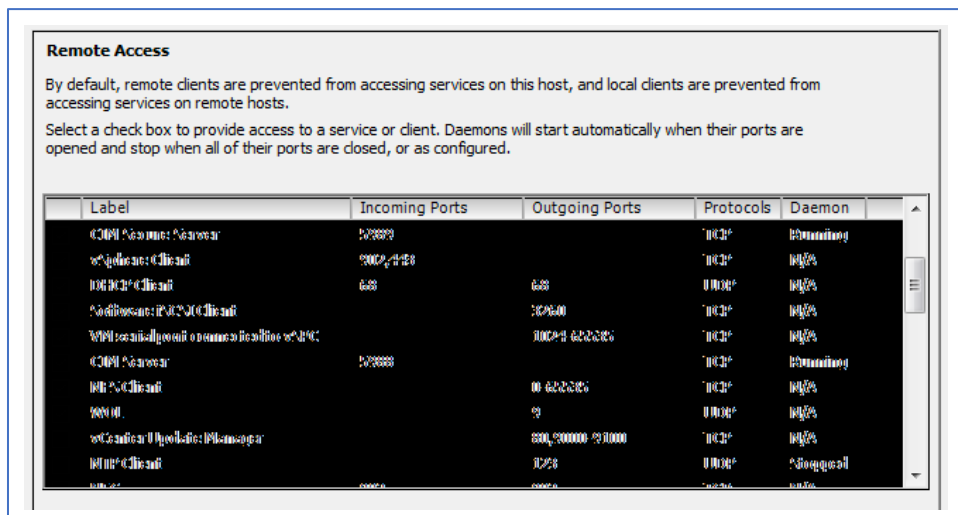


11. On the ESXi firewall, ensure the vSPC port is enabled. To confirm, go to **ESXi Configuration**, select **Security Profile** and click on **Properties**.



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.

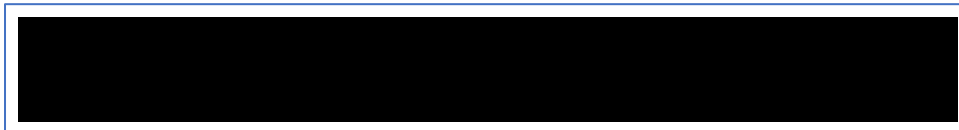
2. Execute the following commands:



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 display 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
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 Services Router](#)

[Nodegrid Gate SR](#)

[Nodegrid Bold SR](#)

[Nodegrid Link SR](#)

Quick Install Guide

Please refer to the links below for product installation information.

[Nodegrid Serial Console](#)

[Nodegrid Services Router](#)

[Nodegrid Gate SR](#)

[Nodegrid Bold SR](#)

[Nodegrid Link SR](#)

RoHS

Please refer to the links below for RoHS information.

[Nodegrid Serial Console](#)

[Nodegrid Services Router](#)

[Nodegrid Gate SR](#)

[Nodegrid Bold SR](#)

[Nodegrid Link 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, **Nodegrid - 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. On 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](#).