zpe

nodegrid

User Guide

ZPE Systems, Inc.

4.2

About This User Guide

The Nodegrid 4.2 user manual covers the Nodegrid Platform version 4.2 and the supporting units including the Nodegrid Serial Console Series, Nodegrid Services Router, Nodegrid Gate SE, Nodegrid Bold SR and 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.

> NOTE: 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.

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 made to fit any modern and legacy mixed environment. With auto-sensing ports, you can use the S Series Console Servers within any environment using straight-through cables or with legacy adapters.

- Auto-Switching (Cisco or Legacy Pin-out)
- 16/32/48 Serial Ports
- Additional USB ports
- Factory upgradeable CPU and RAM
- 1U 19" Rack Standard Unit
- Single AC, Dual AC, and Dual DC

Table 1: 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	2 Gigabit (10/100/1000BT) Ethernet interfaces on RJ45 or 2 SFP+ Fiber interfaces compatible with 1Gb / 2.5Gb / 10Gb modules16, 32, 48 RS-232 serial ports on RJ45 @ 230,400 bps max/port.1 RS-232 serial console port on RJ45 1 USB 3.0 Host,1 USB 2.0 Host and 12 USB 2.0 Hosts on Type A connector1 HDMI
Power	Single/Dual AC 100-240 VAC, 50/60 HzDual DC: 40-63 VDCPower consumption 45 W typical
Physical	Front-Rear mounting brackets Size (L x W x H): 443 x 312 x 43 mm (17.4 x 12.3 x 1.7 in), 1UWeight: 4.9 kg (10.8 lb), depending on options Front-to-Back or Back-to-Front Fans (Swappable)
Environmental	Operation: 0 to 50° C (32 to 122° F), 5-95% RH, non-cond. Storage: -20 to 67° C (-4 to 153° F), 10-90% RH, non-cond.

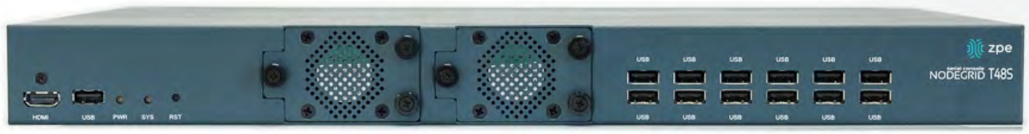


Table 2: Nodegrid Serial Console - S Series Front Interfaces

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	Fans
USB	1 x USB 2.0 Port, 12 x USB 1.1 Ports

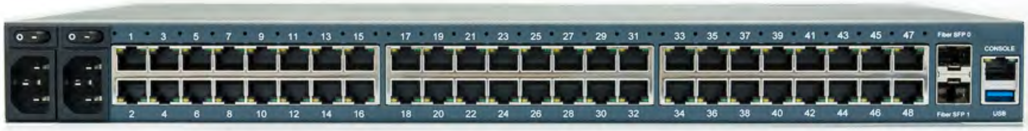


Table 3: Nodegrid Serial Console - S Series Rear Interfaces

PORT	DESCRIPTION
Power	Single or Dual Power Sockets
Serial	Serial Interfaces ·Right/Orange DCD/DTR - On: port open and/or cable connected, Off: not ready·Left/Green RX/TX - Blinking: data activity, Off: no activity

Table 3: Nodegrid Serial Console - S Series Rear Interfaces

PORT	DESCRIPTION
ETH0/SFP0	Network InterfaceCopper:·Left/Green - Blinking: data activity, Solid: ready, Off: no link/cable disconnected/Ethernet fault·Right/Green - 1000BaseT 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 InterfaceCopper:·Left/Green - Blinking: data activity, Solid: ready, Off: no link/cable disconnected/Ethernet fault·Right/Green - 1000BaseT 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 ·Right/Orange LED Power Failure - Blinking: Power supply failure/off (for dual power supply models), Off: normal·Left/Green LED System Activity - Blinking: normal, Off or Solid: no activity
USB	1 x USB 3.0

Nodegrid Serial Console - R Series

The NODEGRID SERIAL CONSOLE (R Series) is made to fit into major hardware environments like Cisco, Arista, Dell, Palo Alto Networks, and Juniper. R Series Serial Consoles are perfect for retrofits and to upgrade Rack Standards of existing builds.

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

Table 4: 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

Table 4: Nodegrid Serial Console - R Series Hardware Specifications

ITEM	DESCRIPTION
Interfaces	2 Gigabit (10/100/1000BT) Ethernet interfaces on RJ45 or 2 SFP+ Fiber interfaces compatible with 1Gb / 2.5Gb / 10Gb modules16, 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 and 2 USB 2.0 Hosts on Type A connector1 HDMI
Power	Single/Dual AC 100-240 VAC, 50/60 HzDual DC: 40-63 VDCPower consumption 45 W (on 96 ports)
Physical	Front-Rear mounting bracketsSize (L x W x H): 443 x 312 x 43 mm (17.4 x 12.3 x 1.7 in), 1UWeight: 4.9 kg (10.8 lb), depending on options
Environmental	Operation: 0 to 50° C (32 to 122° F), 5-95% RH, non-cond. Storage: -20 to 67° C (-4 to 153° F), 10-90% RH, non-cond.

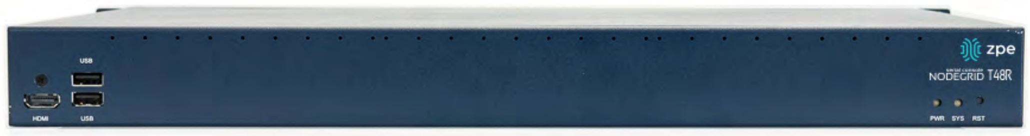


Table 5: Nodegrid Serial Console - R Series Front Interfaces

PORT	DESCRIPTION
HDMI	HDMI Interface
USB	2 x 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

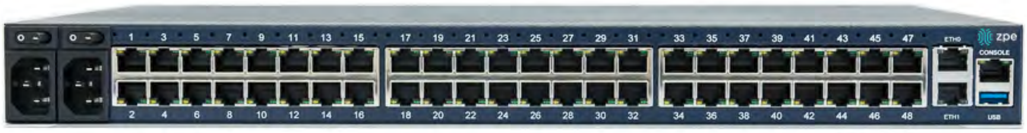


Table 6: Nodegrid Serial Console - R Series Rear Interfaces

PORT	DESCRIPTION
Power	Single or Dual Power Sockets
Serial	Serial Interfaces ·Right/Orange DCD/DTR - On: port open and/or cable connected, Off: not ready·Left/Green RX/TX - Blinking: data activity, Off: no activity
ETH0/SFP0	Network InterfaceCopper:·Left/Green - Blinking: data activity, Solid: ready, Off: no link/cable disconnected/Ethernet fault·Right/Green - 1000BaseT 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 InterfaceCopper:·Left/Green - Blinking: data activity, Solid: ready, Off: no link/cable disconnected/Ethernet fault·Right/Green - 1000BaseT 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 ·Right/Orange LED Power Failure - Blinking: Power supply failure/off (for dual power supply models), Off: normal·Left/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) is made to fit into environments which are still utilizing legacy devices and can be a direct replacement for any legacy console server.

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

Table 7: Nodegrid Serial Console - T 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
Interfaces	2 Gigabit (10/100/1000BT) Ethernet interfaces on RJ45 or 2 SFP+ Fiber interfaces compatible with 1Gb / 2.5Gb / 10Gb modules16, 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 and 2 USB 2.0 Hosts on Type A connector1 HDMI
Power	Single/Dual AC 100-240 VAC, 50/60 HzDual DC: 40-63 VDCPower consumption 45 W (on 96 ports)
Physical	Front-Rear mounting bracketsSize (L x W x H): 443 x 312 x 43 mm (17.4 x 12.3 x 1.7 in), 1UWeight: 4.9 kg (10.8 lb), depending on options
Environmental	Operation: 0 to 50° C (32 to 122° F), 5-95% RH, non-cond. Storage: -20 to 67° C (-4 to 153° F), 10-90% RH, non-cond.

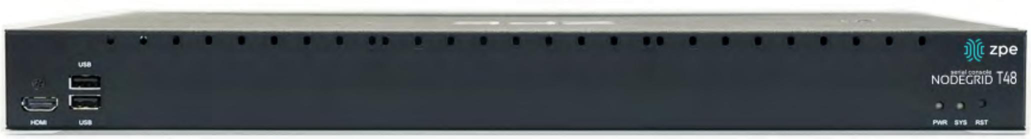


Table 8: Nodegrid Serial Console - T Series Front Interfaces

PORT	DESCRIPTION
HDMI	HDMI Interface
USB	2 x USB 2.0 Port

Table 8: Nodegrid Serial Console - T Series Front Interfaces

PORT	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
RST	Reset button:<3s system reset,>10s configuration factory reset and system reset
HDMI	HDMI Interface

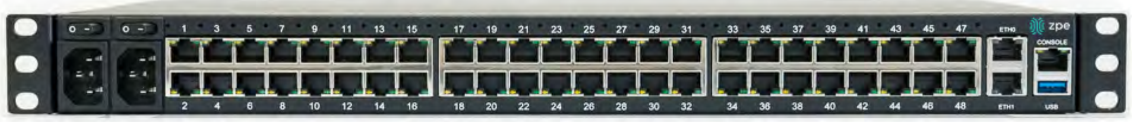


Table 9: Nodegrid Serial Console - T Series Rear Interfaces

PORT	DESCRIPTION
Power	Single or Dual Power Sockets
Serial	Serial Interfaces ·Right/Orange DCD/DTR - On: port open and/or cable connected, Off: not ready·Left/Green RX/TX - Blinking: data activity, Off: no activity
ETH0/SFP0	Network InterfaceCopper:·Left/Green - Blinking: data activity, Solid: ready, Off: no link/cable disconnected/Ethernet fault·Right/Green - 1000BaseT 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 InterfaceCopper:·Left/Green - Blinking: data activity, Solid: ready, Off: no link/cable disconnected/Ethernet fault·Right/Green - 1000BaseT 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

Table 9: Nodegrid Serial Console - T Series Rear Interfaces

PORT	DESCRIPTION
Console	Console MGMT Interface ·Right/Orange LED Power Failure - Blinking: Power supply failure/off (for dual power supply models), Off: normal·Left/Green LED System Activity - Blinking: normal, Off or Solid: no activity
USB	USB 3.0

Nodegrid Services Router Family

The Nodegrid Services Router 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 Services Router

The NODEGRID 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.

- Open Framework, Modular Services Router
- Plugable 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

Table 10: Nodegrid Services Router Hardware Specifications

ITEM	DESCRIPTION
CPU	Intel Multi-core x86_64 CPU
Memory & Storage	8 GB of DDR4 DRAM, 32 GB mSATA SSD (Factory upgradable)
Interfaces	2 SFP+ Ethernet 2 Gigabit Ethernet 1 RS-232 serial console port on RJ45 1 USB 3.01 USB 2.01 HDMI
Power	Single/Dual AC 100-240 VAC, 50/60 HzDual DC: 36-75 VDCPower Consumption 90W typical

Table 10: Nodegrid Services Router Hardware Specifications

ITEM	DESCRIPTION
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), 1UWeight: 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.

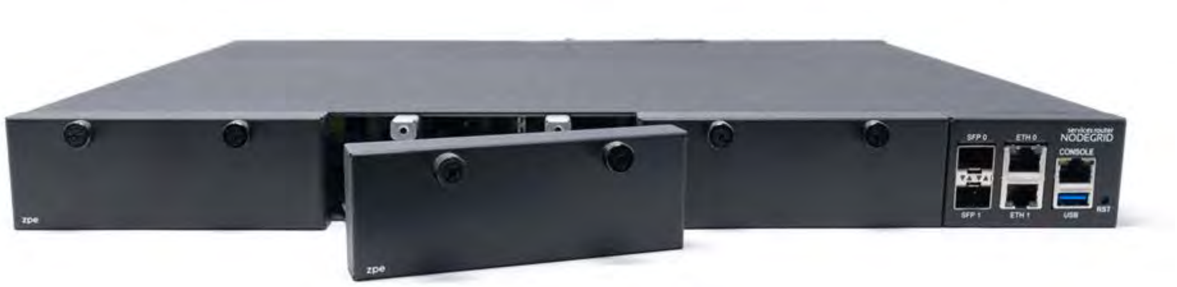


Table 11: Nodegrid Services Router Front Interfaces

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 - 1000BaseT 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 - 1000BaseT link speed·Right/Orange - 100BaseT link speed·Right/Off - no link/cable disconnected/Ethernet fault

Table 11: Nodegrid Services Router Front Interfaces

PORT	DESCRIPTION
Console	Console MGMT Interface ·Right/Orange LED Power Failure - Blinking: Power supply failure/off (for dual power supply models), Off: normal·Left/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

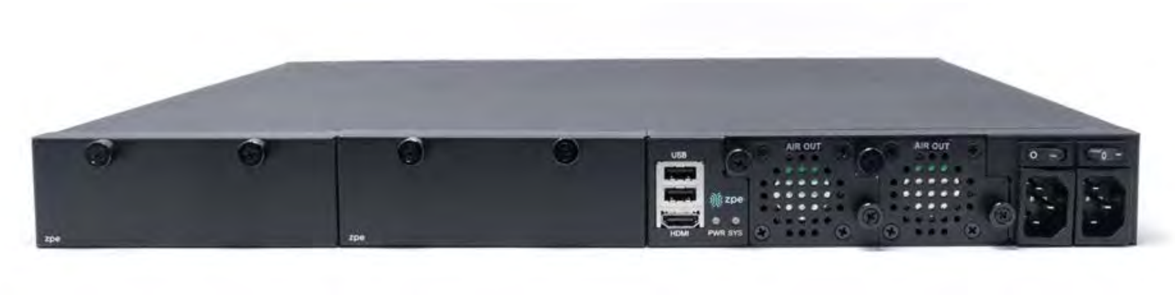


Table 12: Nodegrid Services Router Rear Interfaces

PORT	DESCRIPTION
Slot 4	Slot for Module (depending on the Model)
Slot 5	Slot for Module (depending on the Model)
USB	2 x 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	Fan's
Power Socket	Dual Power Sockets
Power	Single or Dual Power Sockets

Nodegrid Services Router Expansion Modules

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

Table 13: Nodegrid Services Router Expansion Modules

MODULE	IMAGE	SPECIFICATION
16-Port 1GbE		1000BASE-T Cat5e or better
16-Port SFP 1GbE		Supports all SFP Modules
8-Port SFP+ 10GbE		Supports all SFP+ Modules
8-Port PoE+		25.5W max power per port Total max 150W PoE+ available Configurable power budget
16-Port Serial		RJ45 Serial Rolled port max 230,400 bps
16-Port USB		USB 2.0 interfaces Type A
M.2 Cellular + Antenna		For up to 2x 4G/LTE modems
M.2 SATA		For up to 2x mSATA storage modules

Table 13: Nodegrid Services Router Expansion Modules

MODULE	IMAGE	SPECIFICATION
Storage		For 2.5" SATA (HDD/SDD) storage
Compute		Compute module (server on a card), provides independent compute capabilities.

Table 14: 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 / Wi-Fi	√	√	√	√	√
8-Port SFP+	√	√	√	Secure Isolated Mode **	Secure Isolated Mode **
8-Port POE+	√	√	√	–	–
Compute	√	√	√	Secure Isolated Mode **	Secure Isolated Mode **
Storage *	–	–	–	√	√
M.2 SATA *	–	–	–	√	√

Note:
(*) The Nodegrid 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.

Nodegrid Gate SR

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

- 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
- SSL 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
- Wi-Fi hotspot ready via internal card or add your AP (Access Point) via a PoE+ port
- High density and flexible interfaces for greater connectivity

Table 15: Nodegrid Gate SR Hardware Specifications

ITEM	DESCRIPTION
CPU	Intel Multi-core x86_64 CPU
Memory & Storage	8-32 GB of DDR4 DRAM, 32 GB SATADOM SSD (Upgradeable)

Table 15: Nodegrid Gate SR Hardware Specifications

ITEM	DESCRIPTION
Interfaces	4 PoE+ Gigabit (10/100/1000BT) Ethernet interfaces on RJ45 with Built-in Switch4 Gigabit (10/100/1000BT) Ethernet interfaces on RJ45 with Built-in Switch 8 RJ45 serial ports 2 SFP+ (10G)1 Console port on RJ45 2 USB 3.0 Hosts on Type A 2 USB 2.0 Hosts on Type A 2 GPIO 1 Digital Out Port 1 Relay Port 1 Wi-Fi slot (client or server) optional2 Cellular Slots (4G/LTE) with Dual SIM - optional1 HDMI port
Power	36V - 75VDC dual power input - redundant active/passive input, the highest voltage will be active.AC Power adapter (add-on) 100-240V ~50-60Hz, 1.2A, Operating Temperature -25 to 60°C Power consumption 45 W typical
Physical	Front-Rear mounting brackets Size (L x W x 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 x W x H): 349.2 x 374.7 x 177.8 mm (13.75 x 14.75 x 7 in)
Environmental	Operating: -20°C to 60°C (-4 to 140° F), 5-95% RH, non-cond. Storage: -20 to 67° C (-4 to 153° F), 10-90% RH, non-cond.

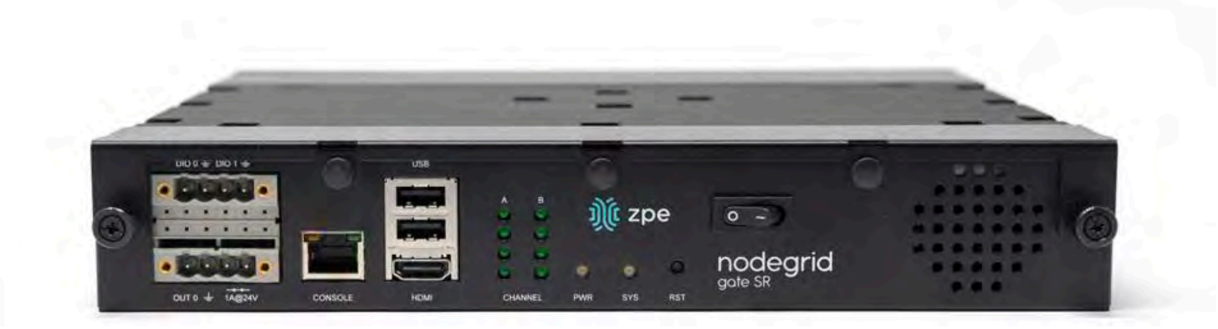


Table 16: Nodegrid Gate SR Front Interfaces

DESIGNATION	DESCRIPTION
DIO0	Digital I/O TTL level 5.5V max @ 64mA
DIO1	Digital I/O TTL level 5.5V max @ 64mA
OUT0	Signal MOSFET Digital Output 2.5V to 60V @ 500mA max
Relay Output	NC relay contact max 24V @ 1A
Console	Console MGMT Interface
USB	2 x USB 2.0

Table 16: Nodegrid Gate SR Front Interfaces

DESIGNATION	DESCRIPTION
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

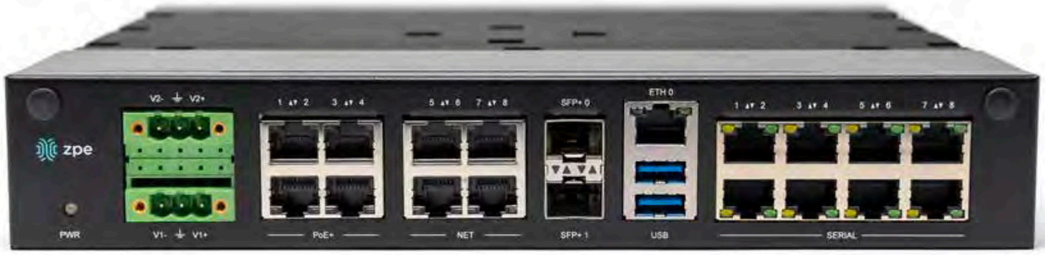


Table 17: Nodegrid Gate SR Interfaces Back

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 x PoE+ Network Interface numbered 1 to 4·Left/Green - Blinking: data activity, Solid: ready, Off: no link/cable disconnected/Ethernet fault·Right/Green - 1000BaseT link speed·Right/Orange - 100BaseT link speed·Right/Off - no link/cable disconnected/Ethernet fault

Table 17: Nodegrid Gate SR Interfaces Back

PORT	DESCRIPTION
NET	4 x Network Interface numbered 5 to 8·Left/Green - Blinking: data activity, Solid: ready, Off: no link/cable disconnected/Ethernet fault·Right/Green - 1000BaseT 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: 1000BaseT link speed, Off: 100/10BaseT link speed or off
USB	2 x USB 3.0 Port
Serial	Serial Interfaces 1-8·Right/Orange DCD/DTR - On: port open and/or cable connected, Off: not ready·Left/Green RX/TX - Blinking: data activity, Off: no activity

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.

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

Table 18: 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)

Table 18: Nodegrid Bold SR Hardware Specifications

ITEM	DESCRIPTION
Interfaces	1 Gigabit (10/100/1000BT) Ethernet interfaces on RJ454 Gigabit (10/ 100/1000BT) Ethernet interfaces on RJ45 with Built-in Switch 8 RS-232 serial ports on RJ45 1 RS-232 console port on RJ45 USB 3.0 Host on Type A2 USB 2.0 Hosts on Type A1 Wi-Fi – optional2 Cellular Slots with Dual SIM – Optional1 VGA port
Power	12 VDC via external 100–240 VAC, 50/60 Hz adapter12 VDC via external 48 VDC 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)

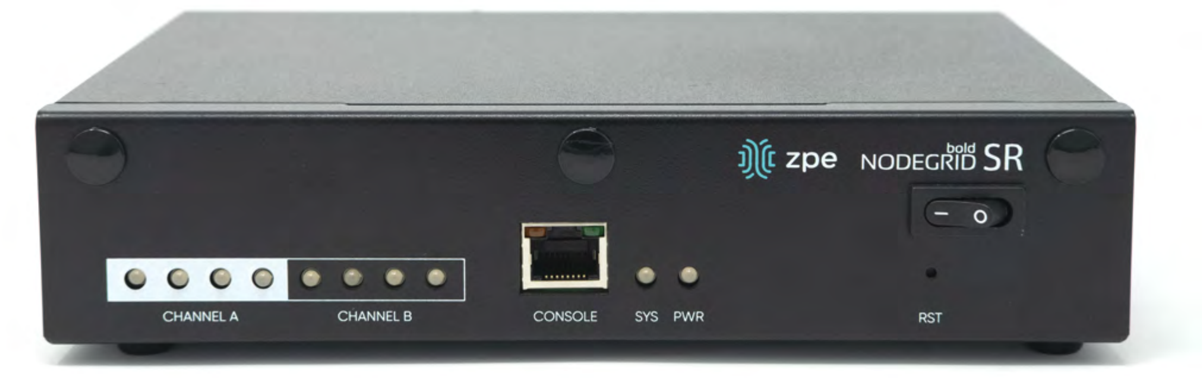


Table 19: Nodegrid Bold SR Front Interfaces

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

Table 19: Nodegrid Bold SR Front Interfaces

PORT	DESCRIPTION
RST	Reset button:<3s system reset,>10s configuration factory reset and system reset
Power Switch	Power on/off Switch

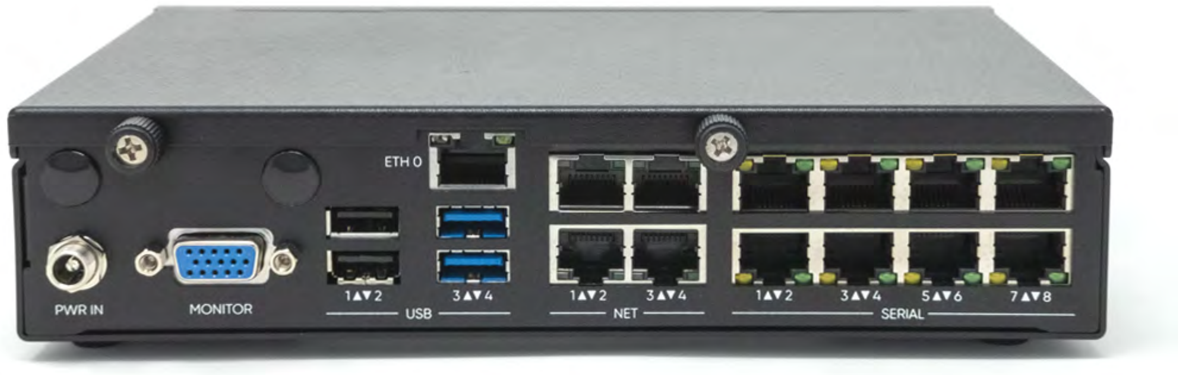


Table 20: Nodegrid Bold SR Rear Interfaces

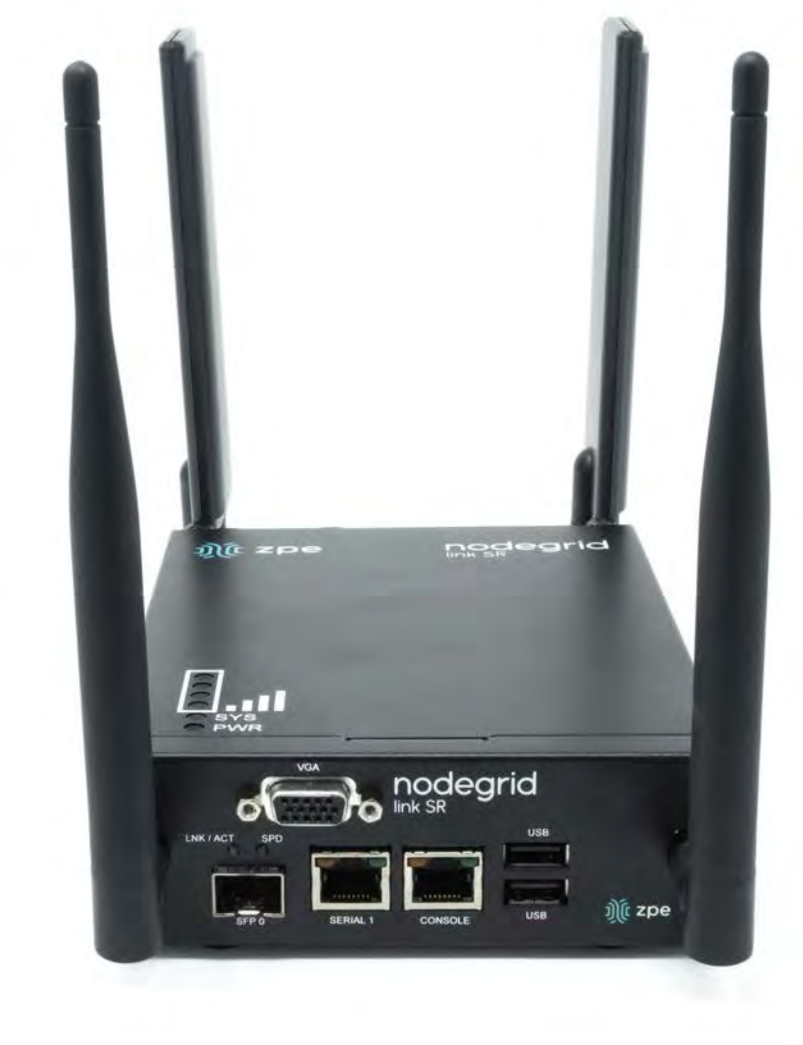
PORT	DESCRIPTION
PWR IN	Power Socket for external Power Supply
Monitor	VGA Interface
ETH0	Network Interface·Left/Green - Blinking: data activity, Solid: ready, Off: no link/cable disconnected/Ethernet fault·Right/Green - 1000BaseT link speed·Right/Orange - 100BaseT link speed·Right/Off - no link/cable disconnected/Ethernet fault
USB	2 x USB 2.0 Port 2 x USB 3.0 Port
ETH1	Network Interface(NET)·Left/Green - Blinking: data activity, Solid: ready, Off: no link/cable disconnected/Ethernet fault·Right/Green - 1000BaseT link speed·Right/Orange - 100BaseT link speed·Right/Off - no link/cable disconnected/Ethernet fault

Table 20: Nodegrid Bold SR Rear Interfaces

PORT	DESCRIPTION
ETH2	Network Interface(NET)·Left/Green - Blinking: data activity, Solid: ready, Off: no link/cable disconnected/Ethernet fault·Right/Green - 1000BaseT 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 - 1000BaseT 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 - 1000BaseT link speed·Right/Orange - 100BaseT link speed·Right/Off - no link/cable disconnected/Ethernet fault
Serial	Serial Interfaces 1-8·Right/Orange DCD/DTR - On: port open and/or cable connected, Off: not ready·Left/Green RX/TX - Blinking: data activity, Off: no activity

Nodegrid Link SR

The Nodegrid Link SR brings agility to the branch network, packing 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.



- Secure, fast and consistent deployments across your branches with the ZPE Cloud
- Combines Cellular gateway and Wi-Fi 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
- SSL 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

Table 21: Nodegrid Link SR Hardware Specifications

ITEM	DESCRIPTION
CPU	Intel Multi-core x86_64 CPU
Memory & Storage	4-8 GB of DDR3 DRAM, 32 GB SATADOM SSD (Upgradeable)

Table 21: Nodegrid Link SR Hardware Specifications

ITEM	DESCRIPTION
Interfaces	1 Gigabit (10/100/1000BT) Ethernet interfaces on RJ45 with PoE in1 SFP (1G) Ethernet1 RJ45 serial ports 1 Console port on RJ45 2 USB 2.0 Hosts on Type A2 GPIO 2 Digital Out Port1 Wi-Fi slot (client or server) optional1 Cellular Slot (4G/LTE) with Dual SIM - optional1 VGA port
Power	10V - 57VDC power inputAC Power adapter (add-on) 100-240V~ 50-60Hz, 1.5APoE power input Power consumption 15 W typical
Physical	DIM Rail and Wall Mountable Size (L x W x H): 170 x 130 x 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.

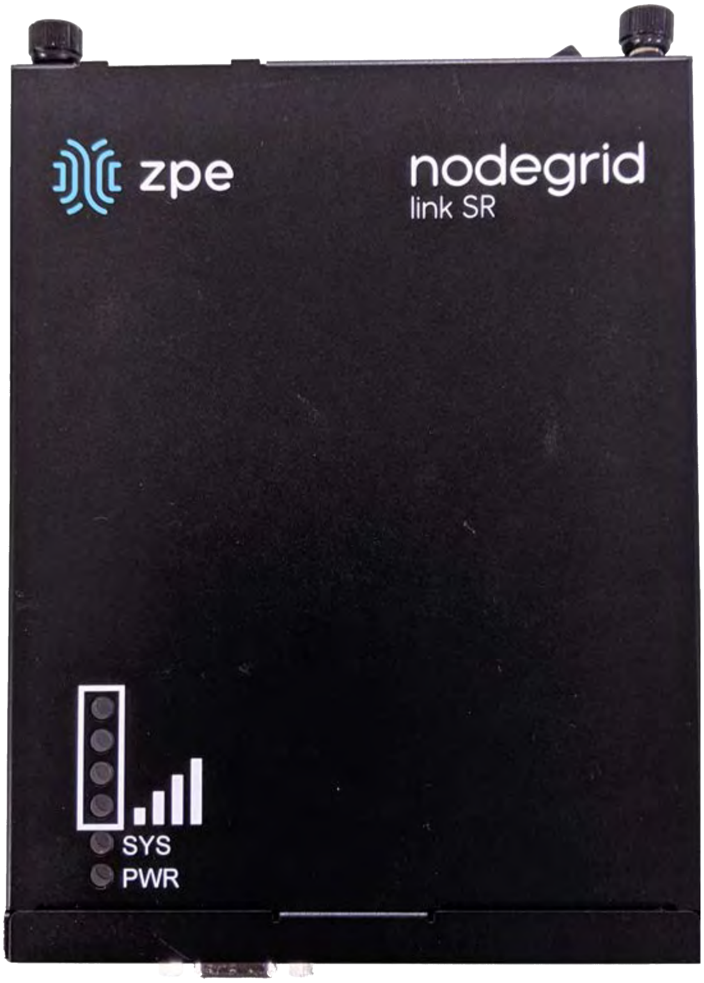


Table 22: Nodegrid Link SR Top

DESIGNATION	DESCRIPTION
BARS	Signal Strength indicator
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

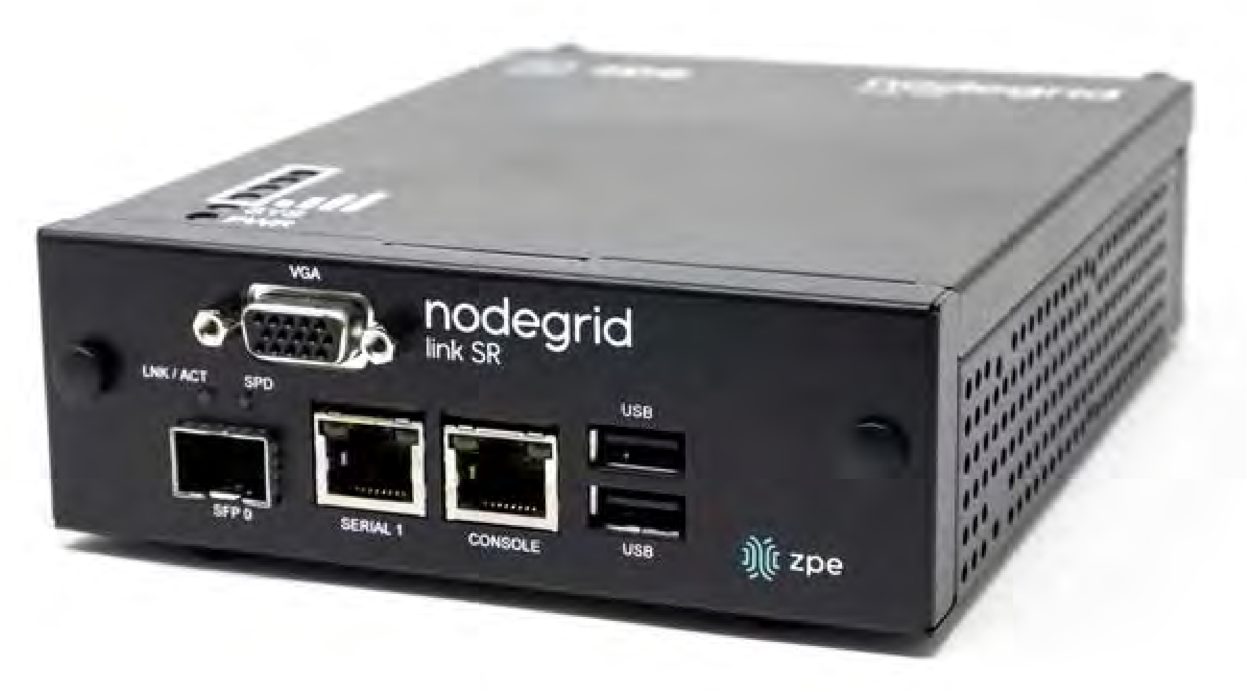


Table 23: Nodegrid Link SR Front Interfaces

DESIGNATION	DESCRIPTION
SFP 0	SFP Network Interface 0·Left/Yellow - Blinking: data activity, Solid: link up, Off: no link/cable disconnected ·Right/Green - Solid: 1000BaseT link speed, Off: no link/cable disconnected
Serial	Serial Interface 1·Right/Orange DCD/DTR - Solid: port open and/or cable connected, Off: not ready ·Left/Green RX/TX - Blinking: data activity, Off: no activity
Console	Console MGMT Interface
USB	2 x USB 2.0
VGA	Monitor Interface

Interfaces Back

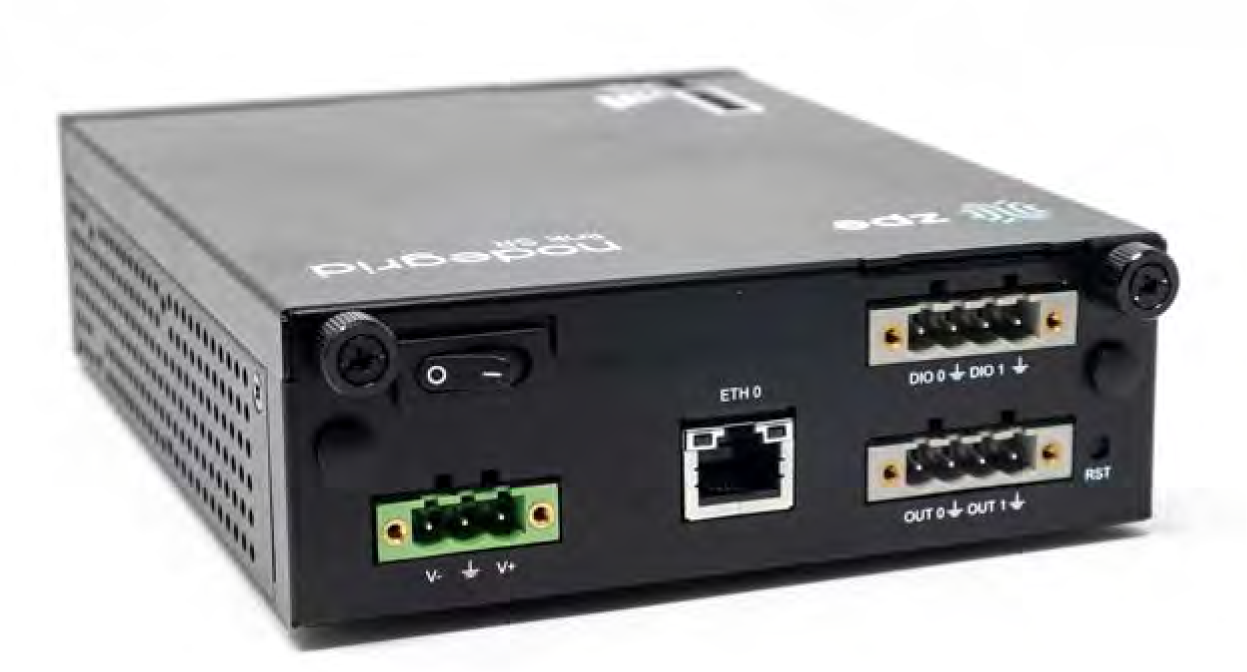


Table 24: Nodegrid Link SR Rear Interfaces

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: 1000BaseT link speed, Off: 10/100BaseT link speed
DIO0	Digital I/O TTL level 5.5V max @ 64mA
DIO1	Digital I/O TTL level 5.5V max @ 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 Manager

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

Table 25: Nodegrid Manager Hardware Specifications

ITEM	DESCRIPTION
CPU	min. 2 x Intel Multi-core x86_64 CPU
Memory & Storage	4 GB RAM, min 32 GB HDD
Interfaces	min 1 Gigabit Ethernet interface
Supported Hypervisors	VMWare ESX, Linux KVM, Oracle Virtualbox -- Linux OS

Installation

Hardware Installation

Please refer to the "Quick Install Guide" on page 304 provided along with the unit in the box for quick instructions on how to start your box.

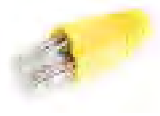
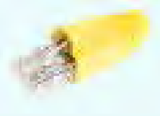
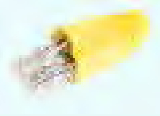
What is in the box

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

Table 26: Included 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

Table 26: Included Accessories

MODEL	MOUNTING BRACKETS	POWER CABLES	LOOP-BACK ADAPTER	CONSOLE ADAPTER	NETWORK CABLE	QUICK START GUIDE & SAFETY SHEET
Nodegrid Serial Console - S Series - TxxS	Yes	Yes	Legacy/ Cisco	Z000015Z 000036	Yes	Yes
Nodegrid 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

Installation of Modules for Nodegrid Services Router

The Nodegrid 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 Services Router is powered off
2. Turn off the power supplies on the Nodegrid 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 screw bolds
6. The Nodegrid 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.

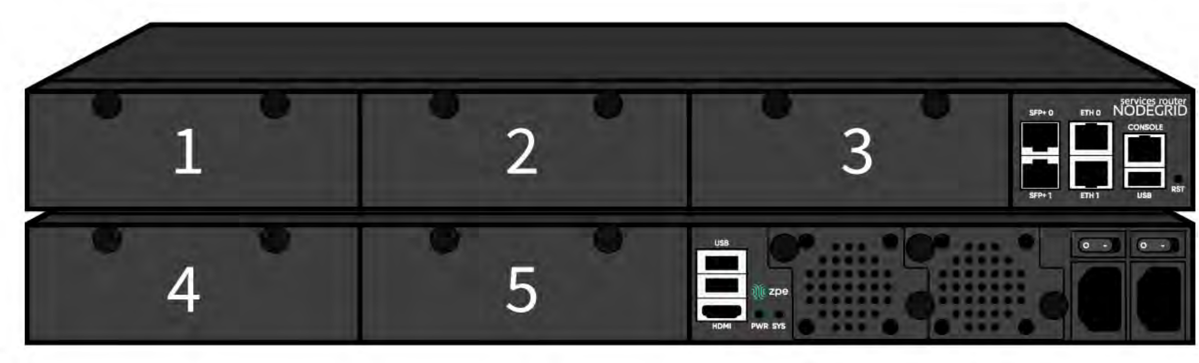


Table 27: Nodegrid Services Router Expansion Module Compatibility Chart

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 / Wi-Fi	✓	✓	✓	✓	✓
8-Port SFP+	✓	✓	✓	Secure Isolated Mode **	Secure Isolated Mode **
8-Port POE+	✓	✓	✓	–	–
Compute	✓	✓	✓	Secure Isolated Mode **	Secure Isolated Mode **
Storage *	–	–	–	✓	✓
M.2 SATA *	–	–	–	✓	✓

Note:

(*) The Nodegrid 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

Note: 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 car 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

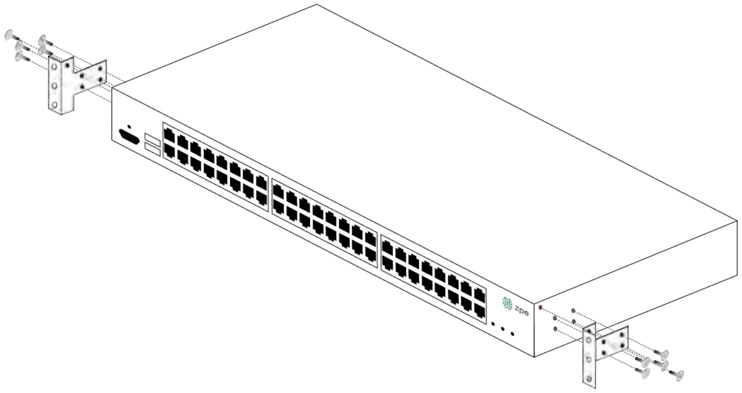
Rack Mounting

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".

To prepared the unit for rack mounting:

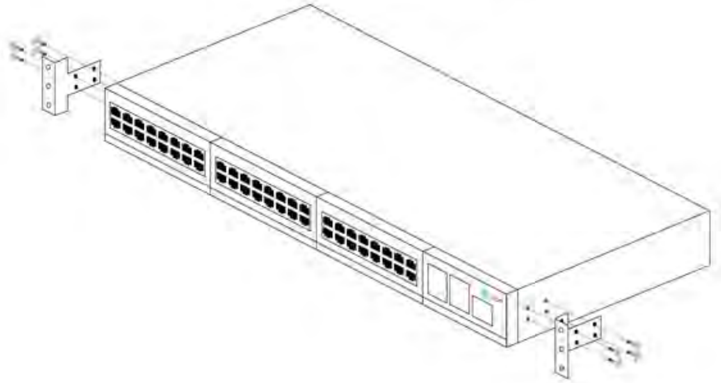
1. Install the rack mounting brackets with the provided screws as shown in the diagrams below

Nodegrid Serial Console - NSC-T96R



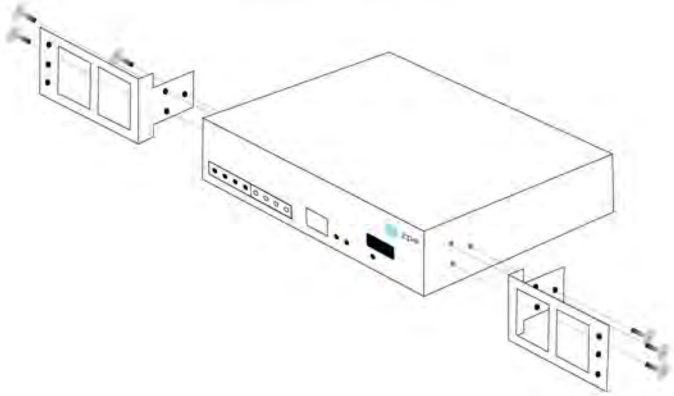
Nodegrid Services Router

Nodegrid Services Router



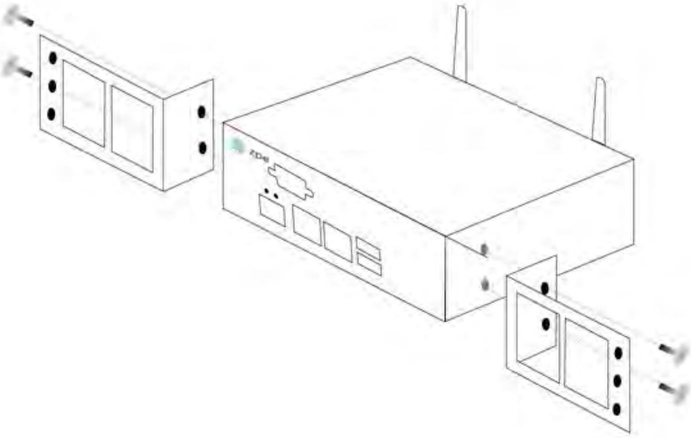
Nodegrid Bold SR

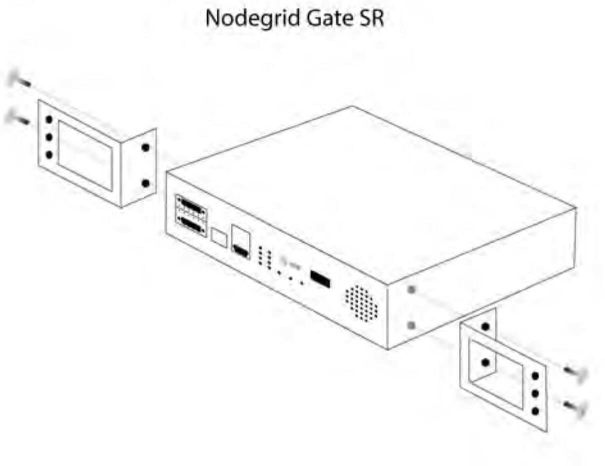
Nodegrid Bold SR



Nodegrid Link SR

Nodegrid Link SR





Note: 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. Please refer to the table below for more information on proper positioning.

Table 28: Rack Mounting

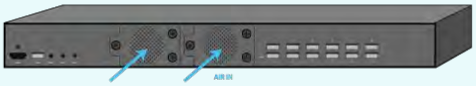
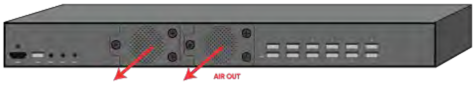
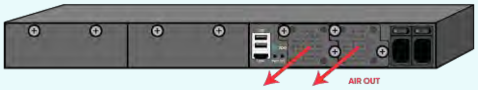
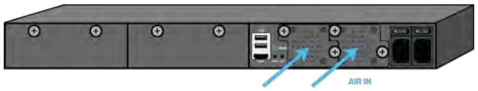
MODEL	PART NUMBER	COOLED	AIRFLOW	IMAGE
Nodegrid Serial Console - T Series	NSC-Txx-xxxx-xxx	Passive	N/A	N/A
Nodegrid Serial Console - R Series	NSC-TxxR-xxxx-xxx	Passive	N/A	N/A
Nodegrid Serial Console - S Series	NSC-TxxS-xxxx-xxx-F	Active	Front-Back (air in)	
Nodegrid Serial Console - S Series	NSC-TxxS-xxxx-xxx-B	Active	Back-Front (air out)	

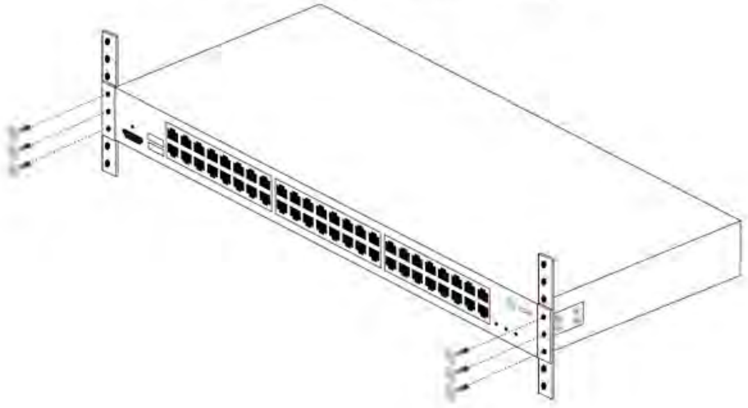
Table 28: Rack Mounting

MODEL	PART NUMBER	COOLED	AIRFLOW	IMAGE
Nodegrid Services Router	NSR-xxxx-xxx	Active	Front-Back (air out)	
Nodegrid Services Router	NSR-xxxx-xxx	Active	Back-Front (air in)	
Nodegrid Bold Services Router	BSR-xx-xxxx	Passive	N/A	N/A
Nodegrid Link Services Router	LSR-xx-xxxx	Passive	N/A	N/A
Nodegrid Gate Services Router	GSR-xx-BASE	Passive	N/A	N/A
Nodegrid Gate Services Router	GSR-xx-UPGx	Active	Front-Back (air out)	N/A

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:

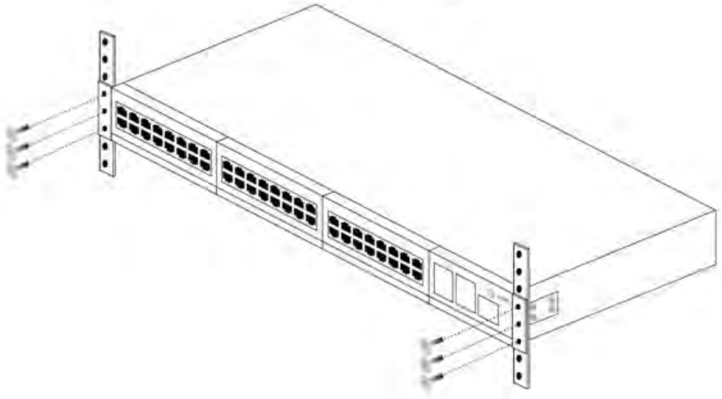
Nodegrid Serial Console

Nodegrid Serial Console - NSC-T96R

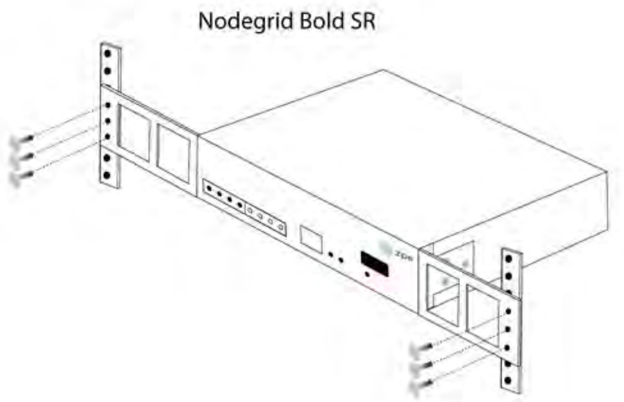


Nodegrid Services Router

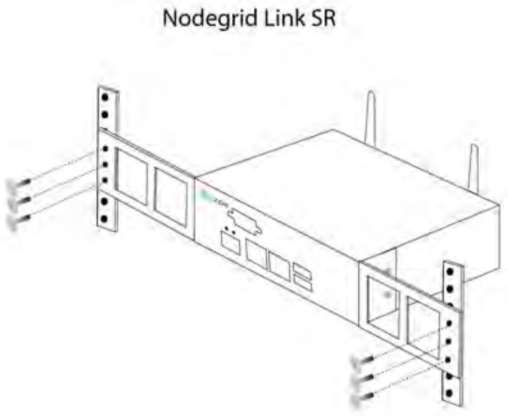
Nodegrid Services Router

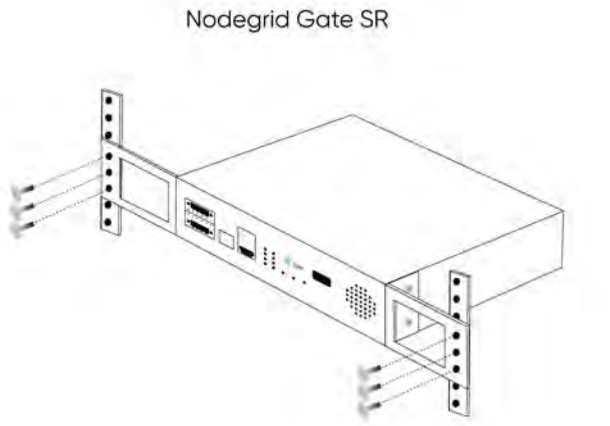


Nodegrid Bold SR



Nodegrid Link SR





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

Network Connection

Depending on the model and version the unit will either have a minimum of 2 copper Ethernet ports or 2 SFP+ ports. Connect the desired network cables (CAT5e, CAT6, CAT6A) from your network switch port to any of the available network ports of the unit. For models with SFP+ ports, install the SFP+ module before the unit is turned on and connect the appropriate cables.

Connecting power cord(s)

The Nodegrid unit includes one or multiple power supplies (AC or DC). Connect all the power supplies with appropriate cables to an available power source, like a Rack PDU. In case your unit is shipped with one power supply then no redundancy for power failure is available. Units with two power supplies provide redundancy against power failures. Both power supplies should be connected to two independent power sources.

> Note - Nodegrid Services Router with PoE: On the Nodegrid Services Router with PoE support, the 2nd power supply is used to provide power for the PoE feature and can not be used to provide redundancy for a power outage.

After all the power supplies are appropriately connected to a power source turn the power supplies on.
(See “DC Power” on page 298 for information on the DC power supply ports).

Connecting target devices

Connecting serial target devices

Note: To avoid EMC issues use good quality network cable for all port connections.

The cabling and adapters that you may need to use between the unit serial ports and the serial devices' console port will depend on their pin-outs.

Newer serial devices such as routers, switches, and servers will use either a DB9, RJ45 or USB port as their console ports. See the manufacturer's manual of your serial device for the port pin-out. In the case of an RJ45 console port, it will likely use the Cisco-like pin-out.
See the table below for cabling you will need to use depending on your unit's serial ports and Serial Devices' console port.

Table 29: Required Cabling

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
Nodegrid Services Router	RJ45	Cisco	-	CAT5e cable	CAT5e cable plus Z000015 crossover adapter	USB

Table 29: Required Cabling

MODEL	PORT TYPE	PIN-OUT	DEVICE PORT - RJ45 (LEGACY)	DEVICE PORT - RJ45 (CISCO)	DEVICE PORT - DB9	DEVICE PORT - 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 if you have any questions on connecting your serial device to the unit, please contact ZPE Systems Technical Support for assistance.

Connecting IP target devices

Note: To avoid EMC issues use good quality network cables for all port connections.

All IP based target devices can be either directly connected to a network interface on a Nodegrid unit, or through an existing network infrastructure. In case the target devices are directly connected, standard network cables (CAT 5, CAT6, CAT6e) can be used for Ethernet connections, or an appropriate fiber cables can be used.

Connecting to a Nodegrid

Connection through the Console port

Use the provided CAT5e and RJ45-DB9 Z000036 adapter/cable to communicate with the Nodegrid unit. Connect one end of the CAT5e cable to the Nodegrid console port. Connect the other end to the RJ45-DB9 adapter, and then plug it to your laptop or PC's DB9 COM port (if your laptop or PC does not have DB9 COM port, use a USB-DB9 adapter (not provided)).

Have a serial application (such as xterm, TeraTerm, Putty, SecureCRT) running on your laptop/PC to open a terminal session to the COM port (see system information to find the COM port to be used) with 115200bps, 8 bits, No parity, 1 stop bit, and no flow control settings.

Connecting through ETH0

The ETH0 interface is configured by default to listen for DHCP requests. In case no DHCP Server is available, the unit will use a default IP address of 192.168.160.10. The unit can be accessed using a browser on https://[DHCP ASSIGNED IP] or on https://192.168.160.10. Alternatively, the unit may be accessed with an ssh client.

Table 30: Connecting 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

Connection through WiFi

The Nodegrid device is pre-configured to act as a Wi-Fi hotspot to allow an appropriate Wi-Fi device to connect. This can either be a built-in Wi-Fi module or a USB Wi-Fi adapter.
The Nodegrid will automatically be presenting a Wi-Fi network with the SSID “Nodegrid”. The default WPA Shared key is “Nodegrid”. The Nodegrid device will not automatically provide an IP address to clients. The client must be configured to have a valid IP address in the 192.168.162.1/24 range. The unit can now be accessed using a browser via https://192.168.162.1 or through ssh.

Table 31: Connecting Through WiFi

SETTING	VALUE
SSID	Nodegrid
WPA Shared key	Nodegrid
Default Network	192.168.162.1/24
Default URL	https://192.168.162.1
Default ssh	`ssh admin@192.168.162.1`

Connection through KVM Port

The Nodegrid unit can be directly configured and managed through it's KVM interfaces.

1. Connect a Monitor with an HDMI cable to the units HDMI interface.

The Nodegrid Bold SR provides a VGA port instead of an HDMI interface.

> Note: HDMI to DVI-D adapters can be used and allow the connections of a DVI-D Monitor.

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

> Note: The keyboard and mouse need to support Linux. Windows only devices are not supported. This limitation mostly affects devices which use a USB wireless dongle.

3. The login prompt will be presented.

I/O Ports (GPIO)

The Nodegrid Gate SR supports two digital I/O ports (DIO0, DIO1), one digital output port (OUT0) and one relay port (1A@24V). The Nodegrid Link SR supports two digital I/O ports (DIO0, DIO1) and two digital output port (OUT0, OUT1).

Both 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) and ESD protection exceeding JESD 22. When the DIO port is configured as an input, it will sense:

- as high or digital ‘1’ when the contact is open;
- as low or digital ‘0’ when the contact is closed.

> Note: Configuring DIO0 and DIO1 ports as input are ideal for dry contact applications like door close, vibration, water, smoke sensors.

When the DIO port is configured as an output, it will output:

- as TTL high, when set to high;
- as TTL low, when set to low.

> Note: Configuring DIO0 and DIO1 ports as output can be used to 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 the OUT port is:

- set to high, it will be enabled/active and it will pull the output OUT to ground.
- set to low, it will be disabled/inactive and it will keep the output OUT open.

> Note: The OUT0 and OUT1 can be used to pull a power connected line to ground, like a relay circuit.

The RELAY port on Nodegrid Gate SR is normally a closed (NC) relay, with a rated max value of 24V @ 1A. However, per RELAY's specification, it supports a maximum switching power of 60W, 125VA; maximum switching voltage of 220VDC, 250VAC; maximum switching current of 2A, with restive load. The primary function of the RELAY is to work as a Power Source Control

Alarm. When the RELAY is close, it indicates that Nodegrid Gate SR is either being powered by a single power source or it does not have power at all. Therefore, if the Nodegrid Gate SR is being powered by both power input sources, when this RELAY is closed, it indicates a FAILURE on at least one of the power input sources. Optionally, the RELAY function can be changed to follow software control (Open / Close), in order to control an external device. The following are the possible relay states:

- open, it will open the relay contact.
- close, it will close the relay contact.

The I/O Port configuration is under `System :: I/O Ports`. The status of the I/O Ports, along with other hardware information is under `Tracking :: HW Monitor`.

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

Nodegrid Manager Installation

The Nodegrid Manager software is installed from an ISO file. The installation procedure is a three-step process:

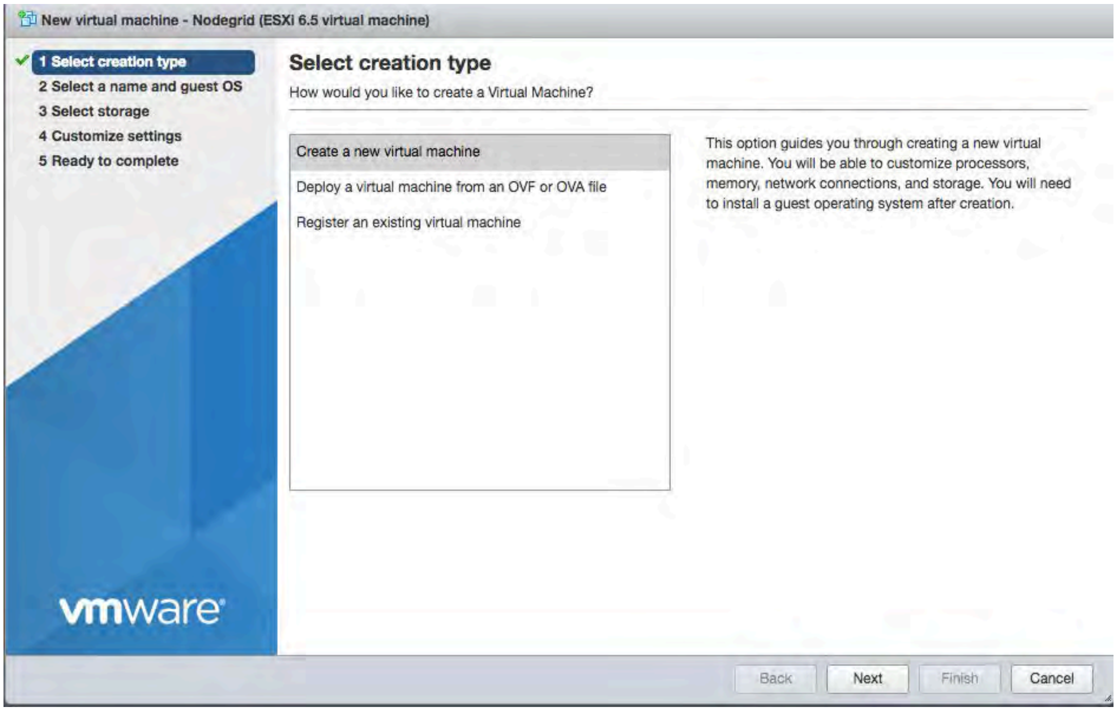
1. Creating a virtual machine
2. Booting from the ISO file/CD in order to install the software
3. Restarting and booting from the newly created virtual machine.

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)

Creating a Virtual Machine - VMWare

1. From the ESXi vSphere screen, click on the Create a new virtual machine link
2. For the virtual machine configuration, click on Create a new virtual machine and then click Next



New virtual machine - Nodegrid (ESXi 6.5 virtual machine)

1 Select creation type
2 Select a name and guest OS
3 Select storage
4 Customize settings
5 Ready to complete

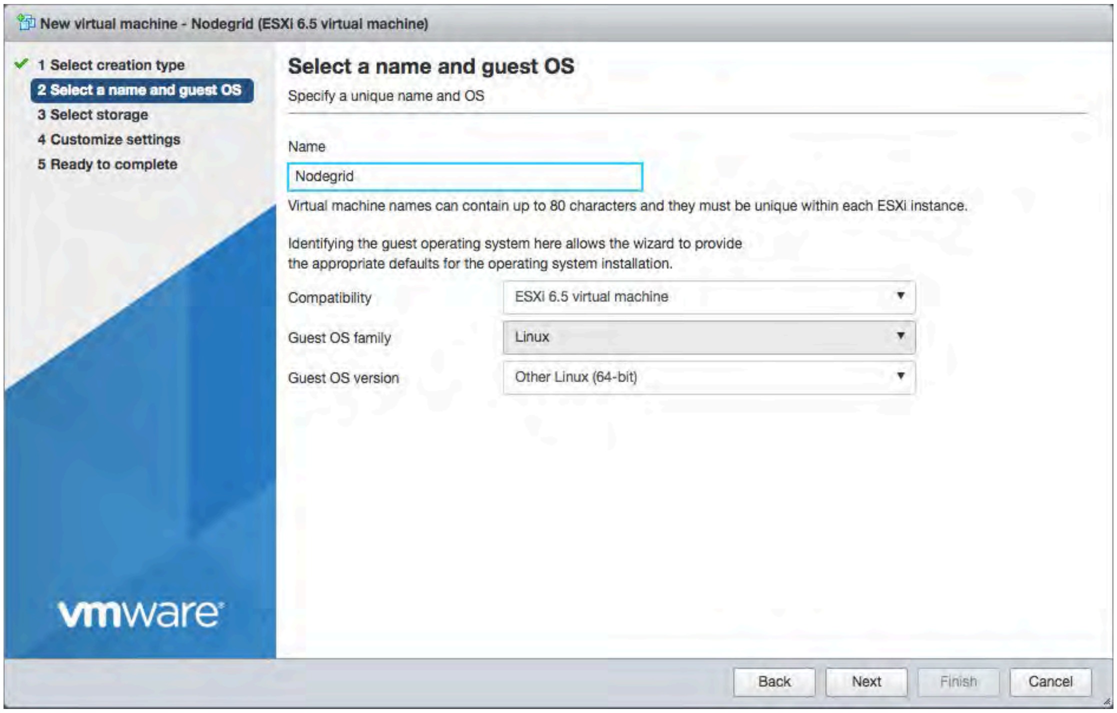
Select creation type

How would you like to create a Virtual Machine?

Create a new virtual machine
Deploy a virtual machine from an OVF or OVA file
Register an existing virtual machine

This option guides you through creating a new virtual machine. You will be able to customize processors, memory, network connections, and storage. You will need to install a guest operating system after creation.

3. Choose an appropriate "Name" for your Nodegrid Manager virtual machine and select Linux for "Guest OS family" and Other Linux (64-Bit) for "Guest OS version" then, click Next



New virtual machine - Nodegrid (ESXi 6.5 virtual machine)

1 Select creation type
2 Select a name and guest OS
3 Select storage
4 Customize settings
5 Ready to complete

Select a name and guest OS

Specify a unique name and OS

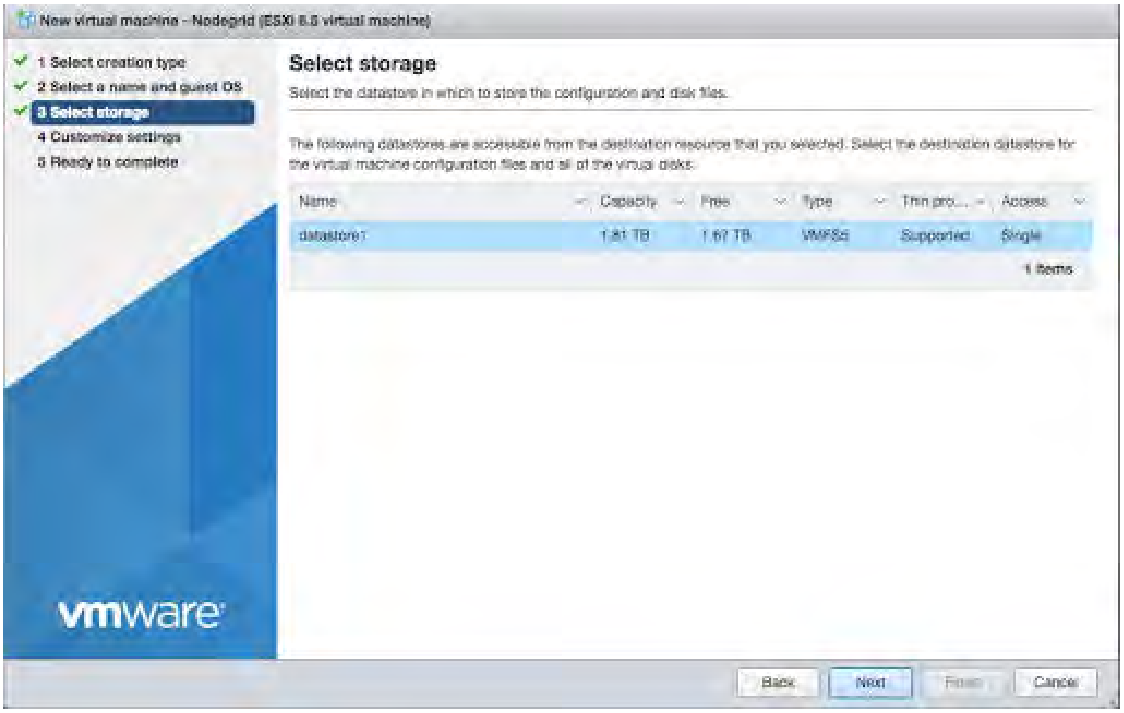
Name: Nodegrid

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Compatibility: ESXi 6.5 virtual machine
Guest OS family: Linux
Guest OS version: Other Linux (64-bit)

4. Select the data storage volume where you wish to create the new virtual machine, then click Next



New virtual machine - Nodegrid (ESXi 6.5 virtual machine)

Select storage

Select the datastore in which to store the configuration and disk files.

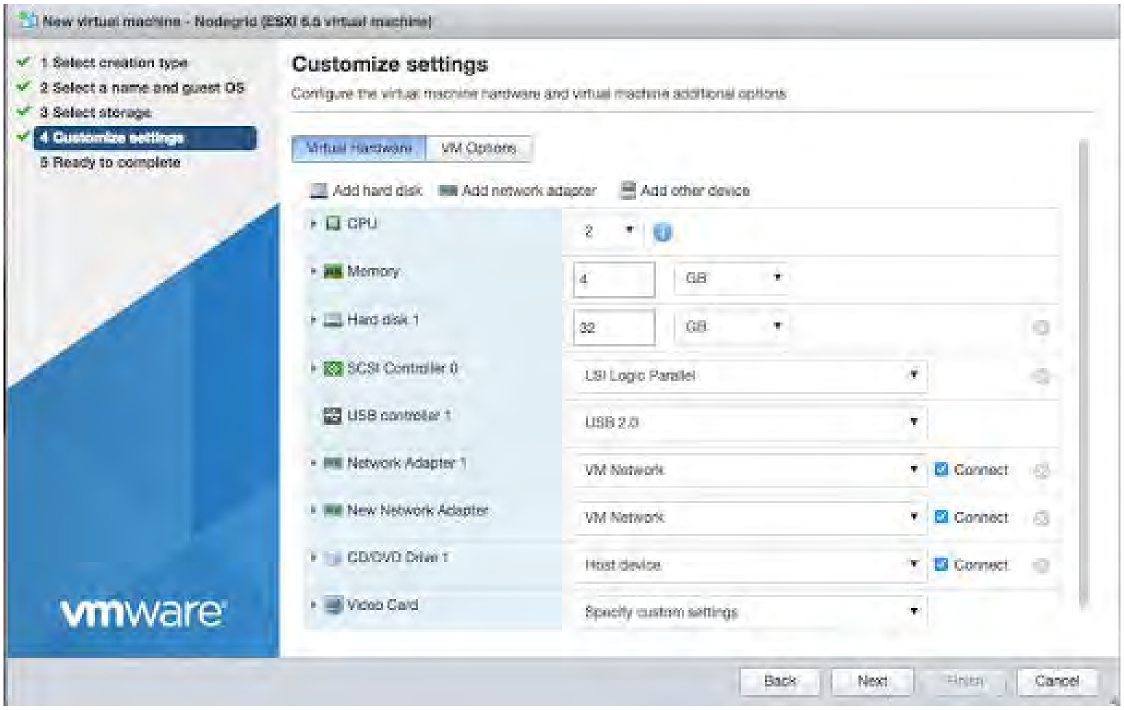
The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	1.81 TB	1.67 TB	VMFS6	Supported	Single

1 items

5. In the "Customize settings" screen, provide the following settings:CPU: 2Memory: 4GBhard disk: 32GBSCSI Controller:LSI Logic Parallelnetwork adapters: 2 of type E1000, then click Next

   Note: the values are minimum settings and should be adjusted as needed



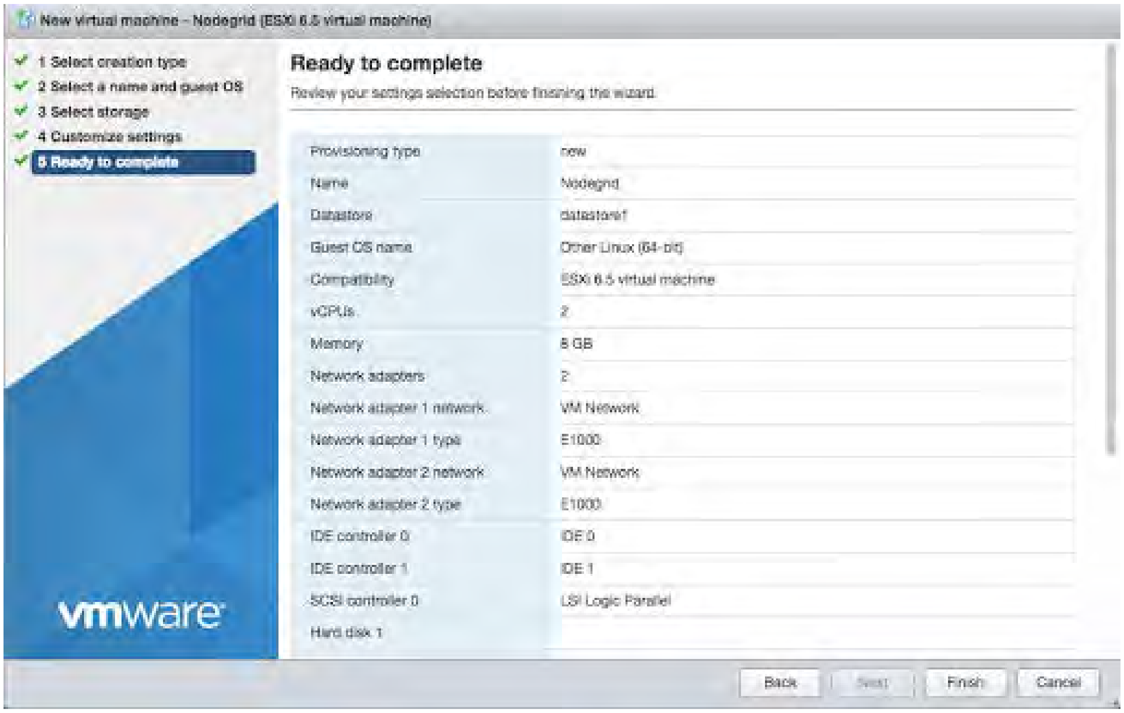
New virtual machine - Nodegrid (ESXi 6.5 virtual machine)

Customize settings

Configure the virtual machine hardware and virtual machine additional options

CPU	2
Memory	4 GB
Hard disk 1	32 GB
SCSI Controller 0	LSI Logic Parallel
USB controller 1	USB 2.0
Network Adapter 1	VM Network ☑ Connect
New Network Adapter	VM Network ☑ Connect
CD/DVD Drive 1	Host device ☑ Connect
Video Card	Specify custom settings

6. Click Finish to complete the configuration of the virtual machine on the ESXi server.



Ready to complete

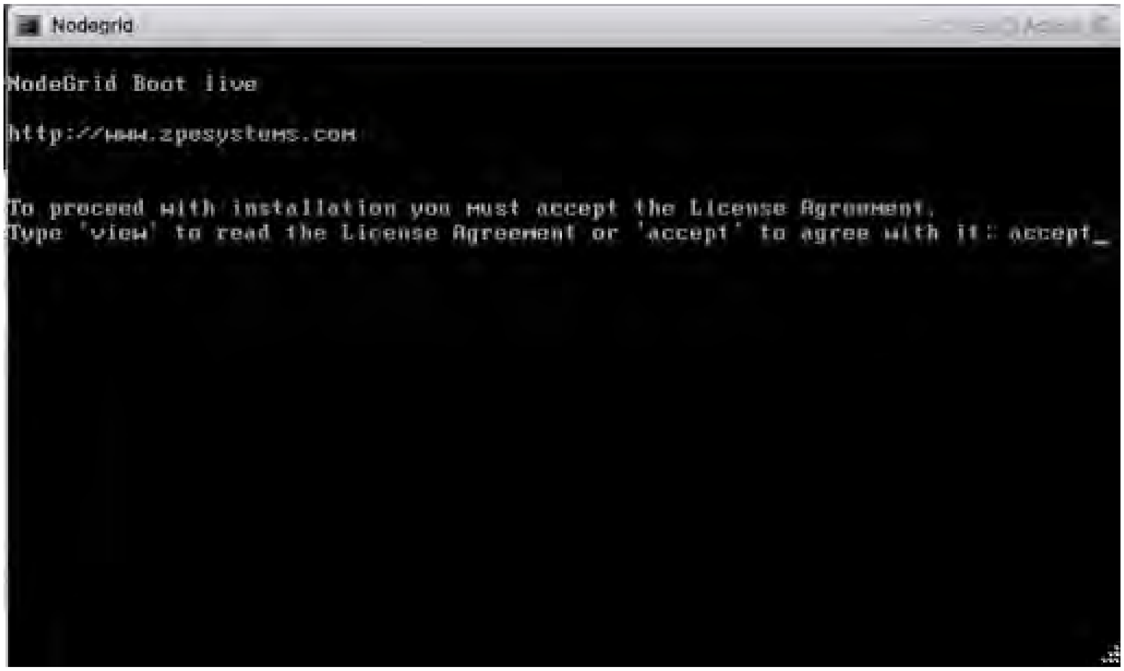
Review your settings selection before finishing the wizard.

Provisioning type	new
Name	Nodegrid
Datastore	datastore1
Guest OS name	Other Linux (64-bit)
Compatibility	ESXi 6.5 virtual machine
vCPUs	2
Memory	8 GB
Network adapters	2
Network adapter 1 network	VM Network
Network adapter 1 type	E1000
Network adapter 2 network	VM Network
Network adapter 2 type	E1000
IDE controller 0	IDE 0
IDE controller 1	IDE 1
SCSI controller 0	LSI Logic Parallel
Hard disk 1	

Installing Nodegrid Manager

To install your Nodegrid Manager software:

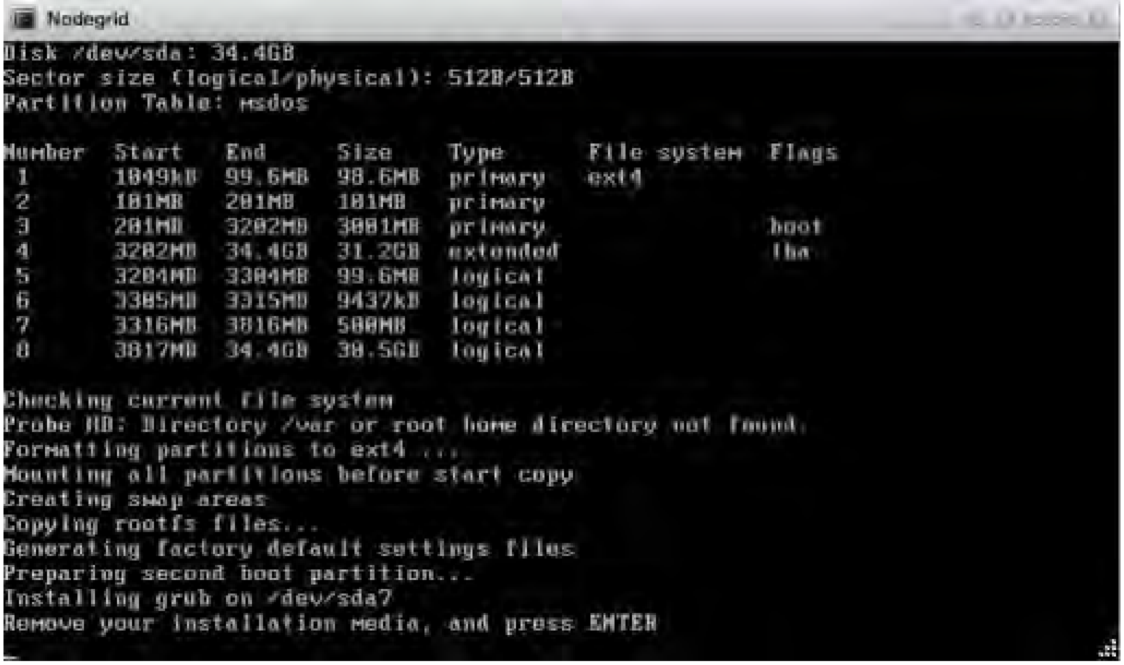
1. Click on the Console tab from the summary screen of the virtual machine
2. Turn on the power. The virtual machine will fail to boot since there is no operating system installed
3. Click on the CD/DVD icon and select the location of Nodegrid Manager ISO file in your system
4. Reboot the virtual machine by clicking on CTL-ALT-INSERT in the console area
5. The virtual machine console server software will start with a boot prompt. At the boot prompt, you can hit ENTER or wait. The image will be decompressed and then loaded
6. Once the image has booted, follow the instructions on the console. You must accept the EULA to proceed with the installation, type accept



Nodegrid

```
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_
```

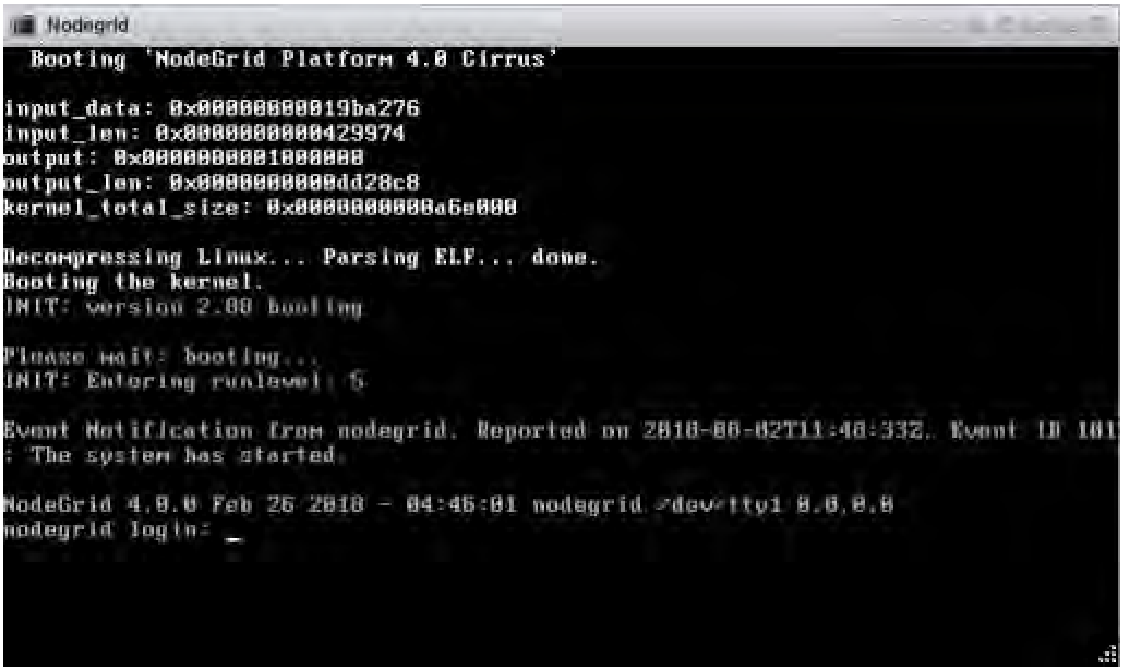
7. The installation process will copy the files into the virtual machine and automatically reboot the system in order to start Nodegrid Manager. Click ENTER to boot the image or wait for the image to boot automatically.



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
_
```

8. After booting the image, your new copy of Nodegrid Manager will be available and ready to be configured.



```
  Booting 'NodeGrid Platform 4.0 Cirrus'

input_data: 0x000000000019ba276
input_len: 0x0000000000429974
output: 0x0000000001000000
output_len: 0x000000000dd28c8
kernel_total_size: 0x00000000000a6e000

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

After the Nodegrid Platform is turned on, boot messages will be displayed, and the login prompt will be displayed.

The default administrator username is **admin** and the default password is **admin**. Admin users can access the Nodegrid Platform via a console port, through the web interface (HTTPS), or CLI (SSH). Other access methods can be enabled later.

The superuser is **root** and the default password is **root**. The root user has SHELL access to the Linux OS, but not to the Web Interface.

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

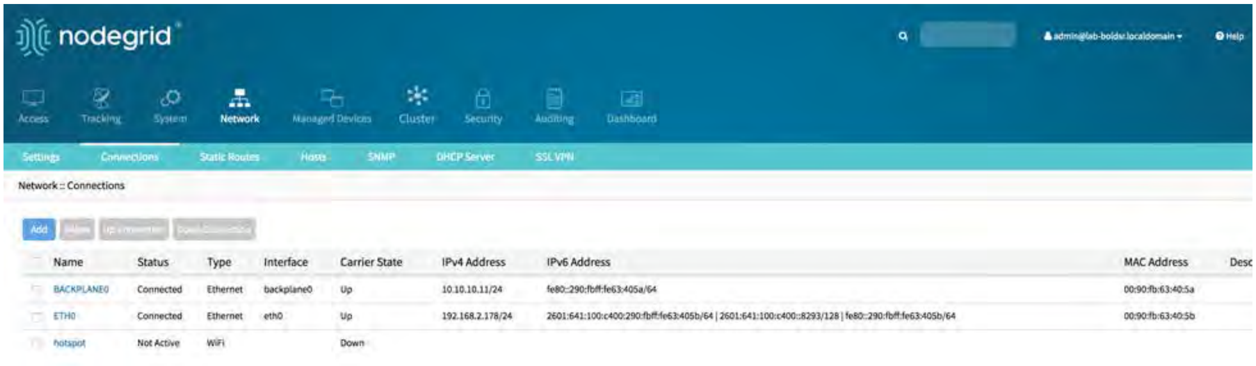
> Note: The Nodegrid Platform will respond on ETH0 at 192.168.160.10 if your DHCP server fails or is unavailable.

Identify the current IP address

To identify the currently assigned IP address/addreses login to the Nodegrid Platform as an **admin** user and navigate to the Network Connections screen.

Identify current IP address - WebUI

1. Login as **admin** user with the default password **admin**
2. Navigate to `Network :: Connections`



Network :: Connections

Name	Status	Type	Interface	Carrier State	IPv4 Address	IPv6 Address	MAC Address	Desc
BACKPLANE0	Connected	Ethernet	backplane0	Up	10.10.10.11/24	fe80::290:fbff:fe63:405a/64	00:90:fb:63:40:5a	
ETH0	Connected	Ethernet	eth0	Up	192.168.2.178/24	2601:641:100:c400:290:fbff:fe63:405b/64 | 2601:641:100:c400::8293/128 | fe80::290:fbff:fe63:405b/64	00:90:fb:63:40:5b	
hotspot	Not Active	WiFi		Down				

Identify current IP address - CLI

1. Login as admin user with the default password admin
2. Display the current settings with `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
```

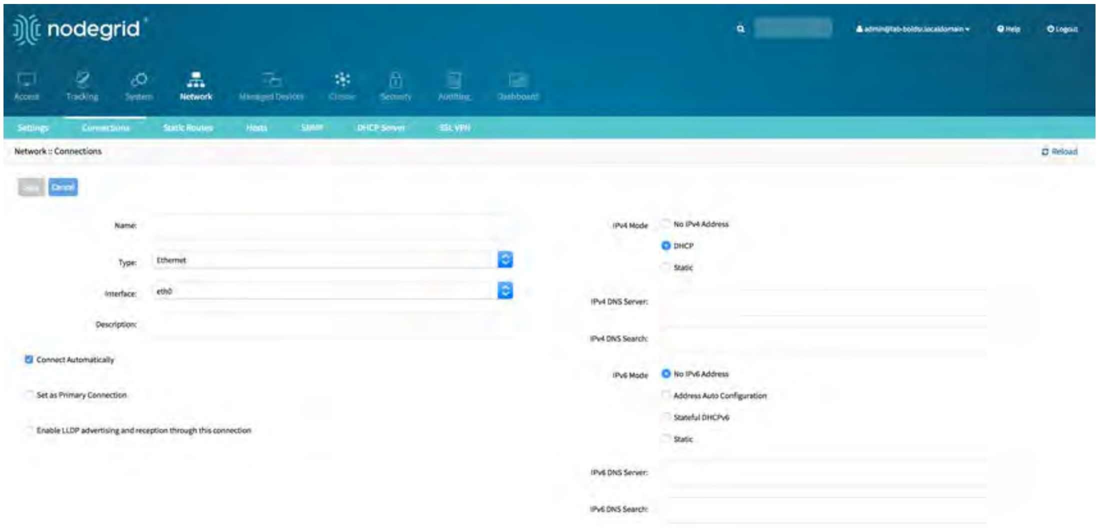
Define Static IP Address

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

> Note: The below examples use IPv4 for communication. IPv6 is fully supported on the Nodegrid Platform and appropriate settings are available in the same menus.

Define Static IP Address - Web UI

1. Navigate to `Network:: Connections`
2. Click on the Interface which should be configured
3. Provide the desired details



Network :: Connections

Name:

Type: Ethernet

Interface: eth0

Description:

☑ Connect Automatically

☐ Set as Primary Connection

☐ Enable LLDP advertising and reception through this connection

IPv4 Mode ○ No IPv4 Address ● DHCP ○ Static

IPv4 DNS Server:

IPv4 DNS Search:

IPv6 Mode ● No IPv6 Address ○ Address Auto Configuration ○ Stateful DHCPv6 ○ Static

IPv6 DNS Server:

IPv6 DNS Search:

4. Click on Save

Define Static IP Address - CLI

1. Navigate to the desired network Interface

```
[admin@Nodegrid /]# cd settings/network_connections/ETH0/
```

2. Configure the Network interface

```
[admin@Nodegrid ETH0]# set ipv4_mode=static
[admin@Nodegrid ETH0]# set ipv4_address=<IP_ADDRESS> ipv4_bitmask=<BITMASK>
ipv4_gateway=<GATEWAY>
[admin@Nodegrid ETH0]# 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 as required.

Interfaces

WebUI

The Nodegrid platform can be accessed via its build in WebUI. The interface allows for full access to all target devices and configuration and management of the platform.
The Web UI supports all modern browsers with HTML5 support including mobile browsers. Current supported browsers include Internet Explorer 11, Edge, Chrome and Firefox.

The WebUI provides the following general structure.:

Table 32: Web UI

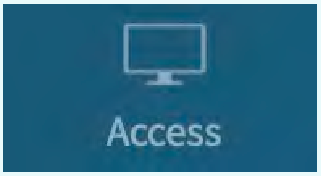
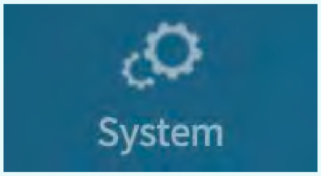
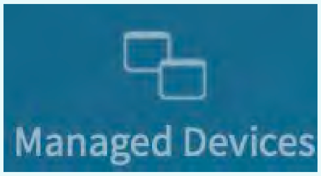
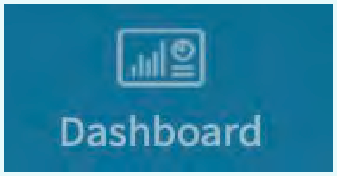
MENU	ITEM	DESCRIPTION
Access		The access menu provides easy access for all users to managed devices. It allows users with the appropriate permissions to start sessions, control power and review the device logging details
Tracking		The tracking menu provides an overview of general statistics and system information, like system utilization and serial port statistics besides others.
System		The system's menu allows administrators to perform general administrative tasks on the Nodegrid Platform, for example, Firmware updates, backups and restores and licenses
Network		The Network menu allows access and administration to all network interfaces and features
Managed Devices		Through this menu, administrators may add, configure, and remove devices which are managed through the Nodegrid platform
Cluster		The Cluster menu allows administrators to configure the Nodegrid Cluster feature
Security		The Security menu provides configuration options which control user access and general security of the Nodegrid platform

Table 32: Web UI

MENU	ITEM	DESCRIPTION
Auditing		The Auditing menu allows administrators to configure auditing levels and locations as well as some global logging settings.
Dashboard		The Dashboard allows users and administrators to create and view dashboards and reports.
Applications		The Applications menu is only visible if a valid Virtualization license is available. With a proper license, it allows administrators to manage and control NFV's and Docker applications.

CLI

The Nodegrid platform can be accessed through a CLI interface. The CLI is accessed by connecting to the platform using an ssh client or through its console port. The interface allows for access to all console target sessions and configuration and management of the platform.
The CLI structure follows mostly the structure of the WebUI.
The CLI provides the following general structure:

Table 33: CLI Folders

FOLDER	DESCRIPTION
/access	The access menu provides easy access for all users to managed devices. It allows users with the appropriate permissions to start sessions, control power and review the device logging details
/system	The system folder provides the combined functions of the Tracking and System menu from the web UI. The tracking features provide an overview of general statistics and system information, like system utilization and serial port statics beside others. The system's features allow administrators to perform general administrative tasks on the Nodegrid Platform, for example, Firmware updates, backups and restores and licenses
/settings	The settings folder provides access to the system, security, auditing, and managed devices settings and configuration options

While the CLI provides many commands and options, the general usage of the CLI can be broken down into a few basic commands.

Table 34: CLI Commands

CLI COMMAND	DESCRIPTION
`TAB TAB`	The key combination of a double TAB provides a list of all available commands, settings, or options which are currently availble
`ls`	The `ls` command list the current folder structure
`show`	The show command, when valid, will display the current settings in a tabular view
`set`	All changes and settings are initiated with the set command in the general form of `set option=value`. Multiple settings can be combined by providing additional `option=value` pairs, like `set option1=value1 option2=value2`
`commit`	Most changes are not directly saved and activated. Changes to the configuration can be reviewed with the `show` command before they get saved and activated with the `commit` command. Those changes are not active yet. Those that need to be saved are indicated in the CLI by a `+` sign in front of the command prompt, like `[+admin@nodegrid /]#`
`cancel` or `revert`	In case a setting should not be committed and saved, the `cancel` or `revert` command can be used to revert the changes.

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_de-
vice_state_detection=
CTS    DCD    None
[+admin@nodegrid /]# set settings/devices/ttyS2/access/ rs-232_signal_for_de-
vice_state_detection=DCD enable_hostname_detection=yes
[+admin@nodegrid /]# commit
[admin@nodegrid /]#
```

Shell

The Nodegrid platform provides direct access to the operating system's shell. By default access is only available to the **root** user (directly) and **admin** user (from CLI). Direct shell access can be granted to users of specific groups (See Groups section). This can be useful for users which are used for system automation processes and which require direct shell access. Nodegrid supports authorization for these uses through ssh key authorization. It is recommended to review the requirement for shell access and limit access as required. Shell access is provided for advanced use cases and should be used with caution. Changes made to the configuration of the Nodegrid platform through the Shell can have a negative impact on the general workings of the platform.

Device Access

The `Access` page provides an overview of all available target devices. It allows users to easily connect to managed devices as well as review their current device status and search for target devices. The displayed target devices will be determent by the user's permissions as well as by the current state of Nodegrid Cluster nodes.

Device Sessions

The first view available to a user after logging into the Web UI is the `Access` View. This view provides an overview of all available targets that the user has access to. Each target will indicate its current connection status as well as the available connection types.

Connection Status:

Table 35: Device Sessions

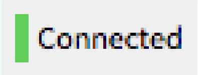
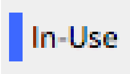
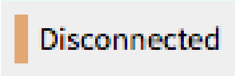
STATE	INDICATOR COLOR	ICON	DESCRIPTION
Connected	Green	 Connected	Nodegrid can successfully connect to the target device and it is available for sessions
In-Use	Blue	 In-Use	The Device is currently in use
Disconnected	Orange	 Disconnected	Nodegrid could not successfully connect to the target device and it is not available for sessions

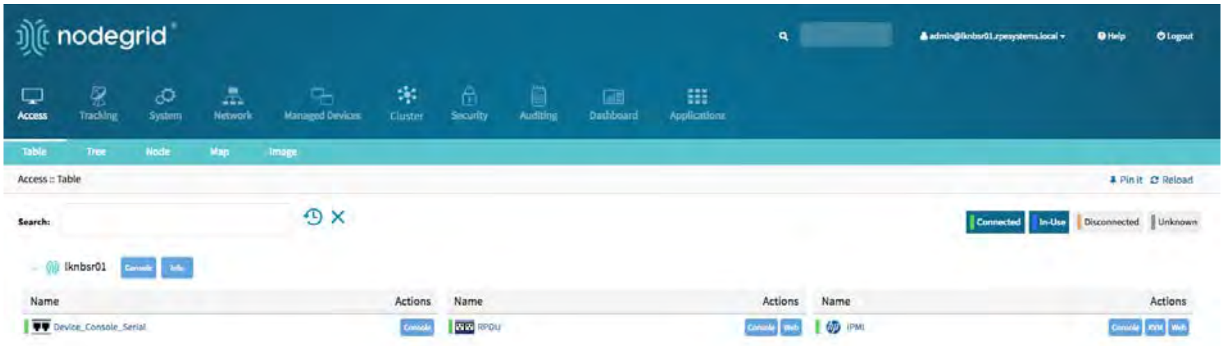
Table 35: Device Sessions

STATE	INDICATOR COLOR	ICON	DESCRIPTION
Unknown	Grey	▮ Unknown	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.

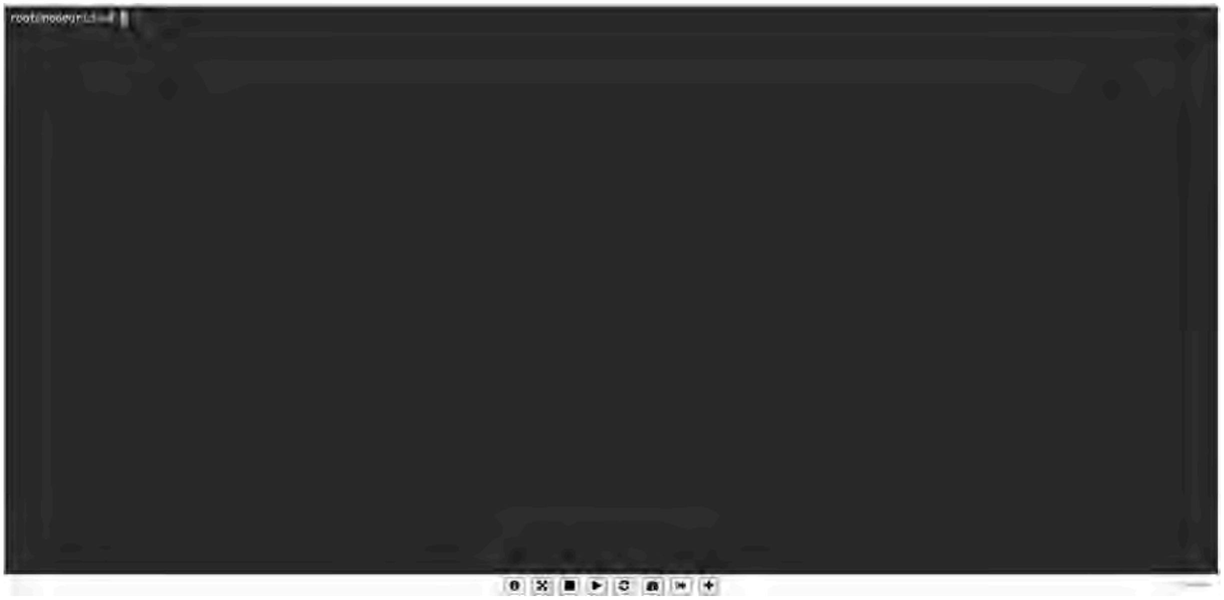
Device sessions can be directly be started from this location.

Device Sessions - Web UI

A user has multiple options to start a device session from the WebUI. In the `Access` screen, the user will directly see the available target sessions and can start a new session by clicking on the connection button.



This will start a new window in which the target session will be established.



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

At the bottom of the window, the user is presented with buttons which allow the user to further control the target session and target device. The options available will depend on the connection type and device configuration.

Table 36: Session Options

OPTIONS	DESCRIPTION
ⓘ Info	The Info option will display the current device details
⤧ Full Screen	The Full Screen option will expand the window to use the enite screen. The session window itself will not expand beyond its maximum size
■ Power Off	The Power Off option will perform a power off on the target device through a connected Rack PDU or IPMI device
▶ Power On	The Power On option will perform a power on for the target device through a connected Rack PDU or IPMI device
⟳ Reset	The Reset option will perform a power cycle on the target device through a connected Rack PDU or IPMI device
Power Status	The Power Status will display the current power status of a device as returned by a connected Rack PDU or IPMI device
⇥ Close Session	This option closes the active session

Table 36: Session Options

OPTIONS	DESCRIPTION
⊞	The plus sign expands or minimizes the command line options at the bottom of the screen

By closing the window, the session to the target device will be closed.

Copy & Paste

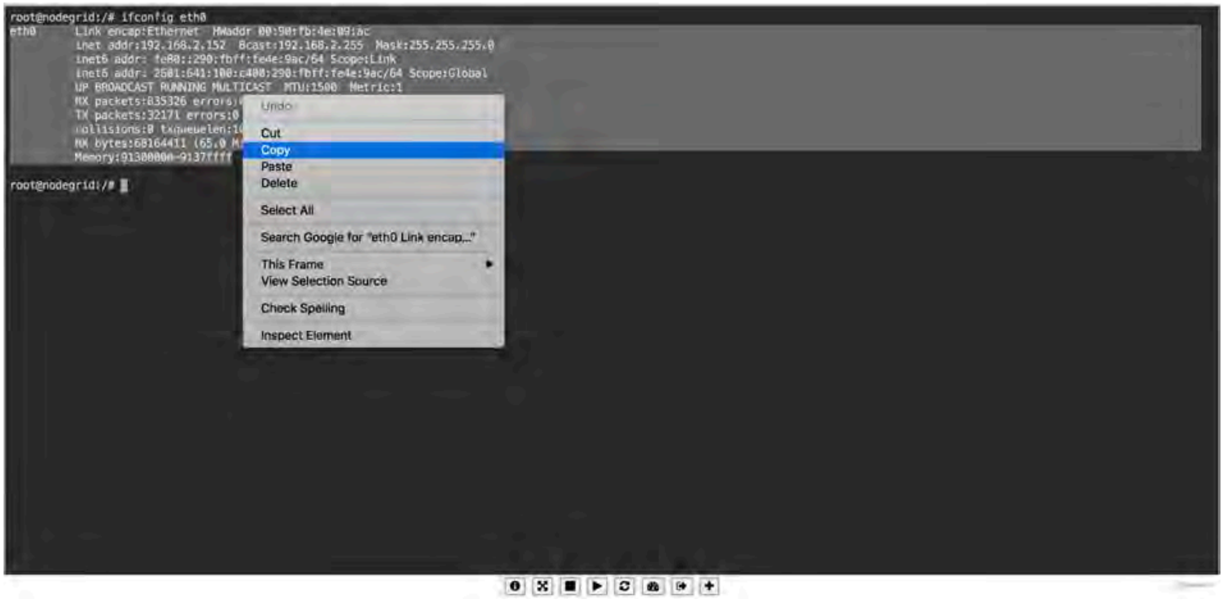
Nodegrid supports **Copying & Pasting** text between the HTML5 graphical device session window and the desktop environment, similar to any other application.
Notice, however, that due to peculiarities of Operating Systems, the copy and paste operations require a distinct combination of keys to activate the copy and paste functions, as shown below.

- In Windows and Linux, use `Ctrl+Ins` to copy and `Shift+Ins` to paste.

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

- In Mac, use `Cmd+C` to copy, and `Cmd+V` to paste.

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



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

root@nodegrid:/#
```

Device Sessions - CLI

The access view is available in the CLI through the `access` menu. A user can directly navigate to this menu with `cd /access`. To see the currently available targets the user can use the command `show`.

Example:

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

A device session can be directly started from here with the `connect` command. Use: `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.

After a connection is established you may use the escape sequence `^Ec` or `^O` to further control the session.

Note: the Escape sequences can be changed in the device settings.

The following options are available.:

Table 37: Session Options

OPTION	ESCAPE SEQUENCE	DESCRIPTION
.	`^Ec.`	disconnect the current session
g	`^Ecg`	displays the current user group information
l	`^Ecl`	sends the break signal as defined in the device settings
w	`^Ecw`	displays the currently connected users
<cr>	`^Ec<cr>`	sends an ignore/abort command signal
k	`^Eck`	serial port (speed data bits parity stop bits flow)
b	`^Ecb`	sends a broadcast message. A message can be typed after the escape sequence sent.
i	`^Eci`	displays the current serial port information
s	`^Ecs`	changes the current session to read-only mode
a	`^Eca`	changes the current session to read-write mode
f	`^Ecf`	forces the current session to read-write mode
z	`^Ecz`	disconnect a specific connected user session
?	`^Ec?`	print this message

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

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

Enter option:
```

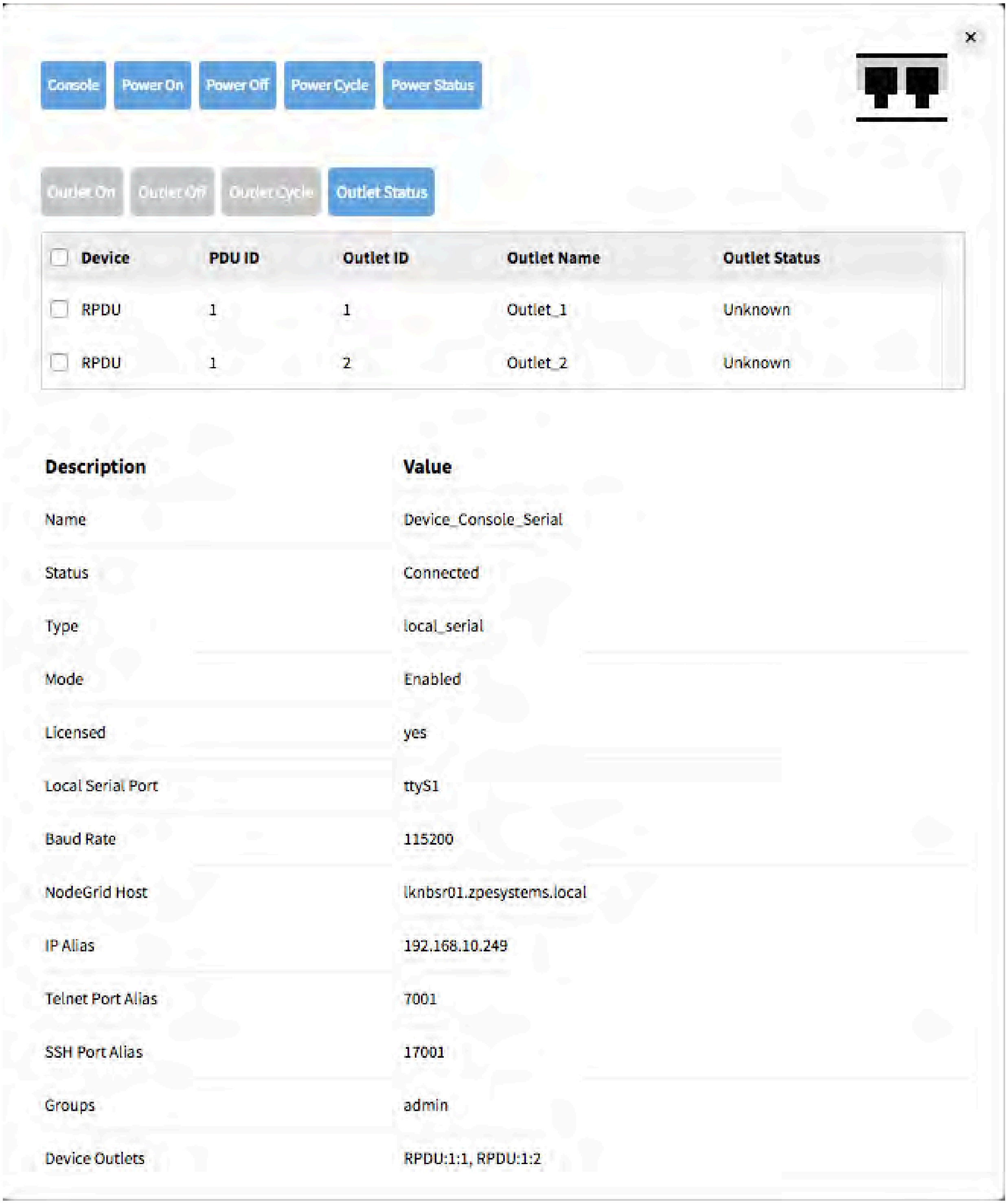
Device Information

Each device maintained by the Nodegrid platform has a multitude of device information stored in the system. This information is visible to users and fully searchable in the system. This is useful when you are trying to identify specific targets.
The stored information is a combination of automatically discovered values. These values were set during the device configuration. Additional information may have been associated with a device by an administrator.

The device information can be displayed in the Access view for a specific device by clicking on a target name in the WebUI, or by navigating to the device in the CLI.

Display Device Information - Web UI

1. Navigate to `Access:: Table`
2. Click on the Target Name to display Device Details



□ Device	PDU ID	Outlet ID	Outlet Name	Outlet Status
□ RPDU	1	1	Outlet_1	Unknown
□ RPDU	1	2	Outlet_2	Unknown

Description	Value
Name	Device_Console_Serial
Status	Connected
Type	local_serial
Mode	Enabled
Licensed	yes
Local Serial Port	ttyS1
Baud Rate	115200
NodeGrid Host	lknbsr01.zpesystems.local
IP Alias	192.168.10.249
Telnet Port Alias	7001
SSH Port Alias	17001
Groups	admin
Device Outlets	RPDU:1:1, RPDU:1:2

Display Device Information - CLI

1. Navigate to `cd /access/`

2. Use the `show` command to display the device details

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

Device Views

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

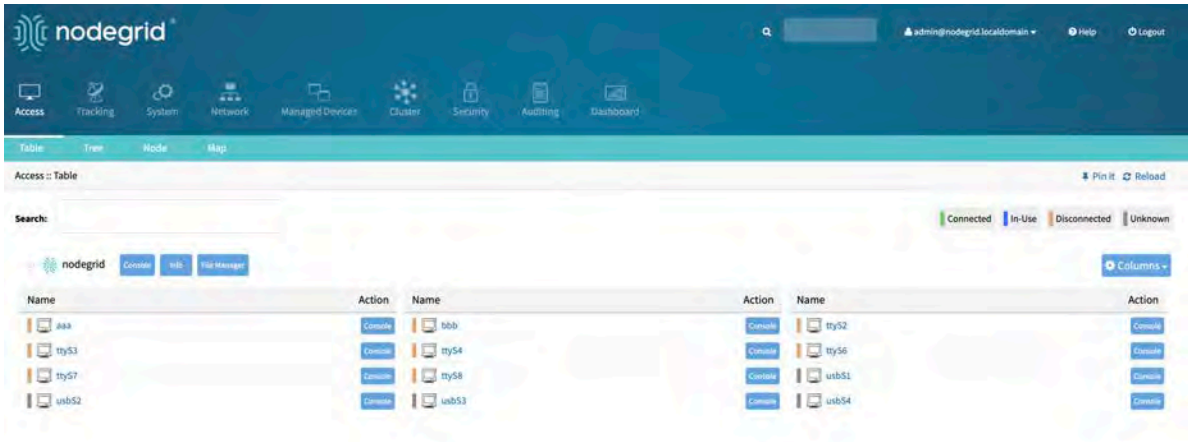
- Table View
- Tree View
- Node View
- Map View
- Image View

Each user can change the default view which will be displayed immediately after login. To change the default view, the user opens the preferred view and uses the `Pin It` button to set it to default.

Note: The Table view is the only view which is available on the CLI.

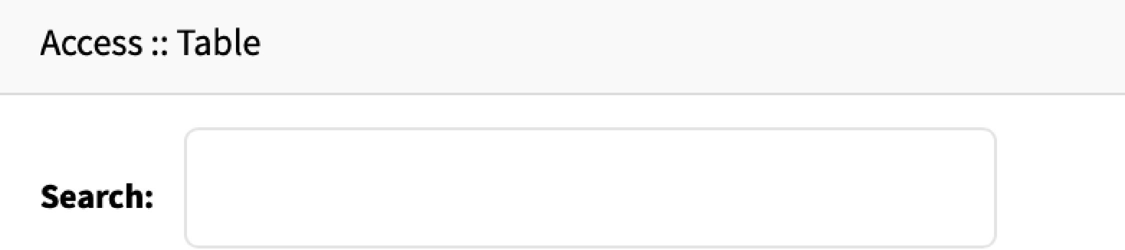
Table View

The table view allows for easy access to all target device and their device sessions. It provides a tabular view which outlines the current status for each device. The view will display all devices currently connected to the unit, as well as all other targets which are available through the Cluster feature. See “Cluster” on page 266 for more information.



Name	Action	Name	Action	Name	Action
aaa	Console	bbb	Console	ttyS2	Console
ttyS3	Console	ttyS4	Console	ttyS6	Console
ttyS7	Console	ttyS8	Console	usbS1	Console
usbS2	Console	usbS3	Console	usbS4	Console

The view supports filtering the current list by current device status and other search criteria. In order to filter by current device status, Click on the device status icons in the top right-hand corner. The following example filters the devices by Connection State (Connected and In-Use)

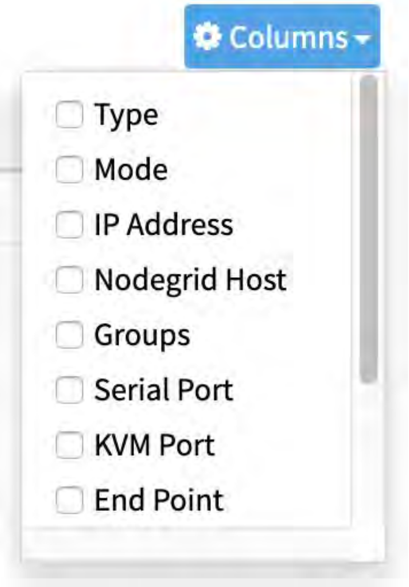


More advanced search options are available through the Search field. See [“Device Search” on page 71](#) for more details.

Access Table Tabular View

By default, the **Name** and **Actions** columns are shown for each device. You may choose to show additional columns by doing the following:

1. Navigate to `Access::Table`
2. Click on the Columns button to view the drop-down menu

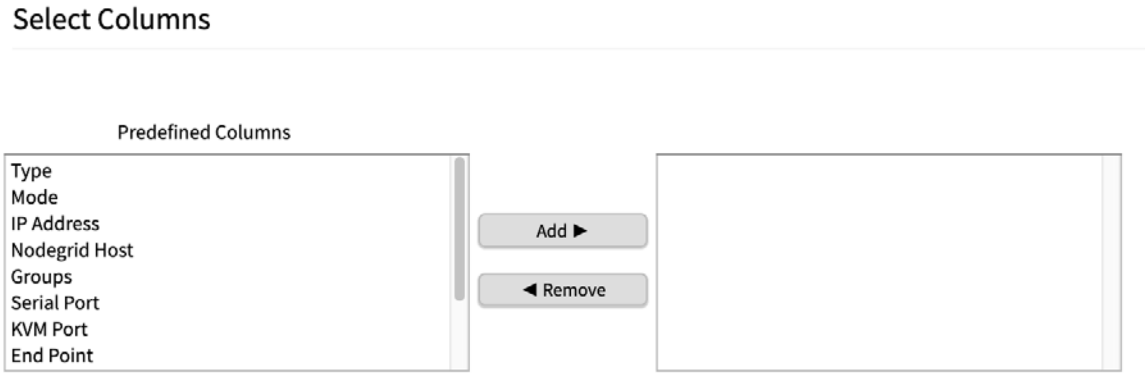


The following options are available by default:

- Type
- Mode
- IP Address
- Nodegrid Host
- Groups
- Serial Port
- KVM Port
- End Point
- Port Alias
- IP Alias
- Second IP Alias

3. The new columns will appear or disappear as they are selected or unselected from the menu

Columns can also be enabled or disabled within `Managed Devices::Preferences::Views` by using the Select Columns option.



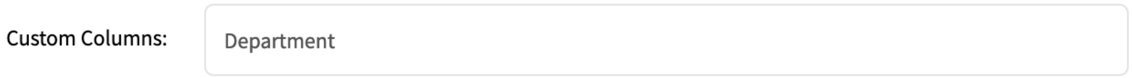
Columns may be re-ordered by dragging the name of the column to the desired position within the Columns drop-down menu.

> Note: Column selections and arrangements are stored locally on your computer and will not be available if you log in on another device. The **Name** and **Action** column positions are fixed and cannot be changed.

Creating Custom Columns

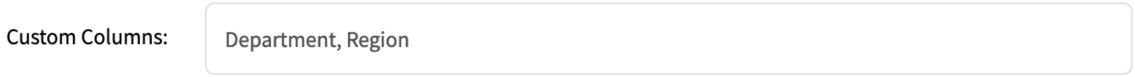
Custom columns can be created and enabled to further organize your connected devices. To create a custom column:

1. Navigate to `Managed Devices::Preferences::Views`
2. Enter the desired column name in the Custom Columns dialog box



Custom Columns: Department

- To add multiple columns you can separate them with a comma



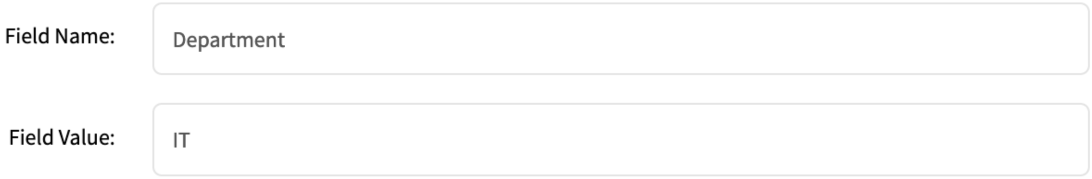
Custom Columns: Department, Region

3. Click Save

   Note: The new custom column(s) will not appear on the `Access:Devices` page until there is a device associated with them and the column has been enabled.

To associate a device to the new column:

1. Navigate to `Managed Devices::Devices`
2. Click on the name of the device you want to associate
3. Click on Custom Fields
4. Click Add
5. Enter a Field Name and a Field Value



Field Name: Department

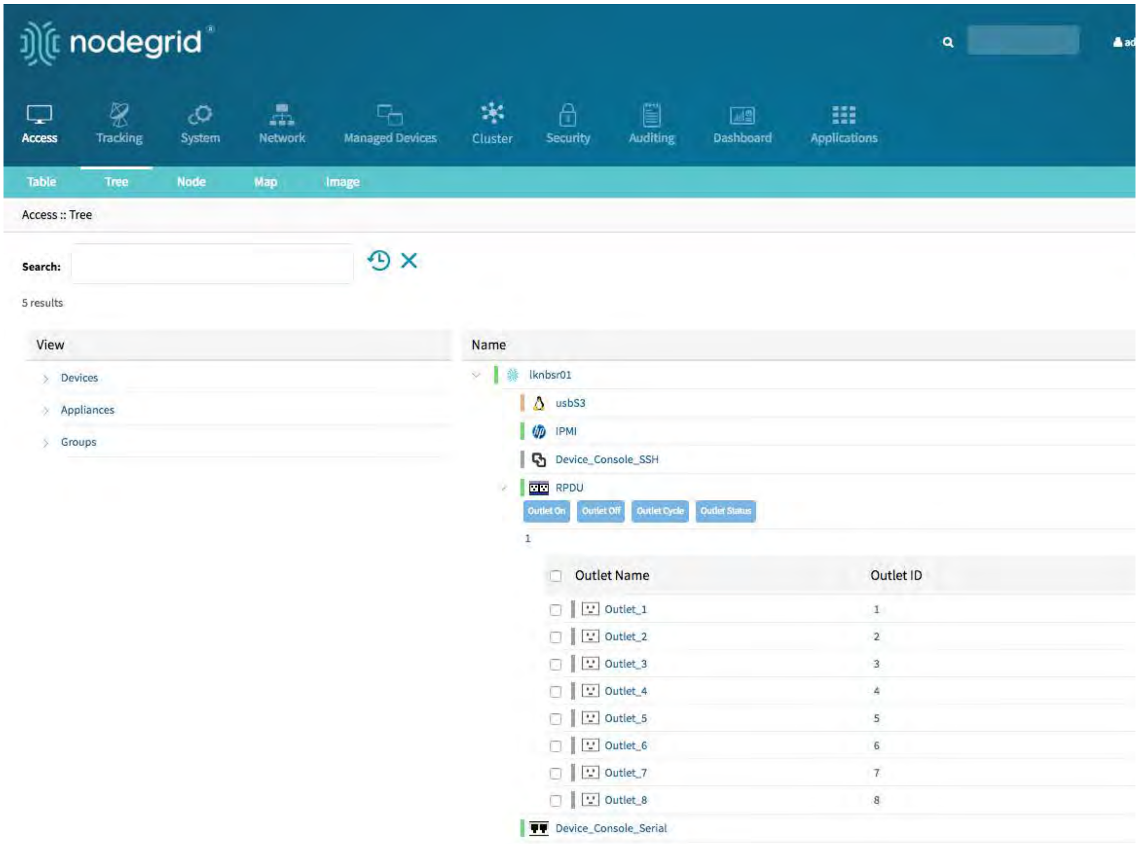
Field Value: IT

   Note: The Filed Name must exactly match the name you entered in the Custom Columns dialog box

6. Click Save

Tree View

The Tree view displays all targets based on the physical hierarchies of the Nodegrid setup and allows you to start connections for each target. It allows for easy access to target devices based on their location, like Nodegrid name, city name, data center name, row and rack, and others. The View section offers filters based on location and device types.



Access :: Tree

Search:

5 results

View
- Devices
- Appliances
- Groups

Name
- lknbsr01
  - usbS3
  - IPMI
  - Device_Console_SSH
  - RPDU
    1

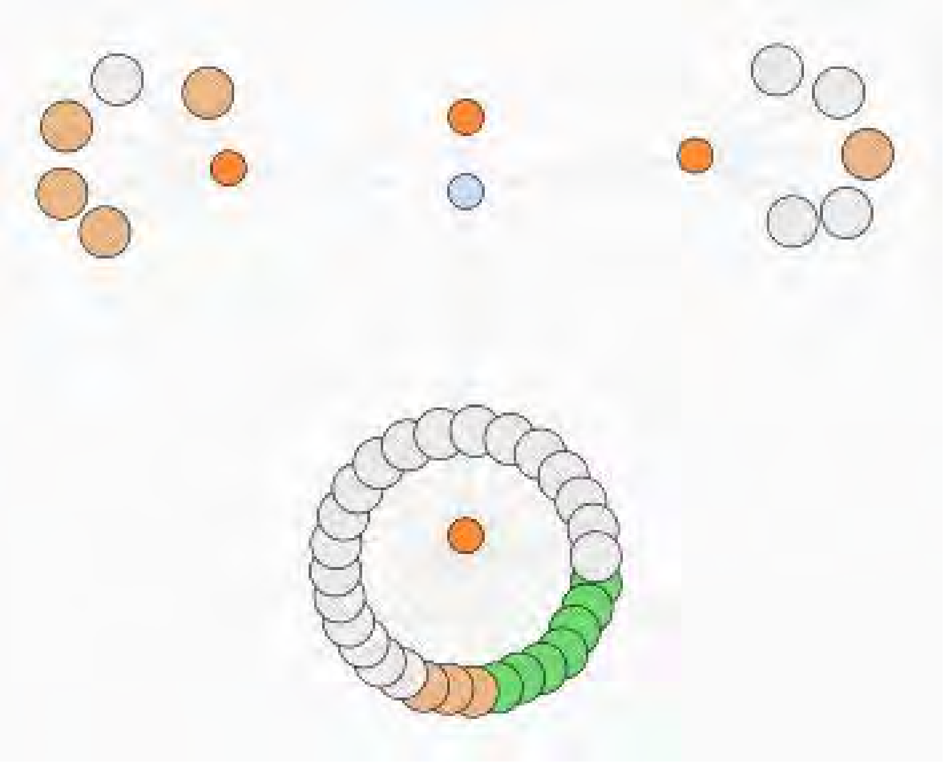
□ Outlet Name	Outlet ID
□ Outlet_1	1
□ Outlet_2	2
□ Outlet_3	3
□ Outlet_4	4
□ Outlet_5	5
□ Outlet_6	6
□ Outlet_7	7
□ Outlet_8	8

  - Device_Console_Serial

More advanced search options are available through the Search field. See “Device Search” on page 71 for more details.

Node View

The Node View arranges all target devices around their connected Nodegrid units and makes it easy to get a complete overview of all targets and Nodegrid units in a Cluster (see “Cluster” on page 266). This view allows access to target device information and connections by clicking on the target nodes.

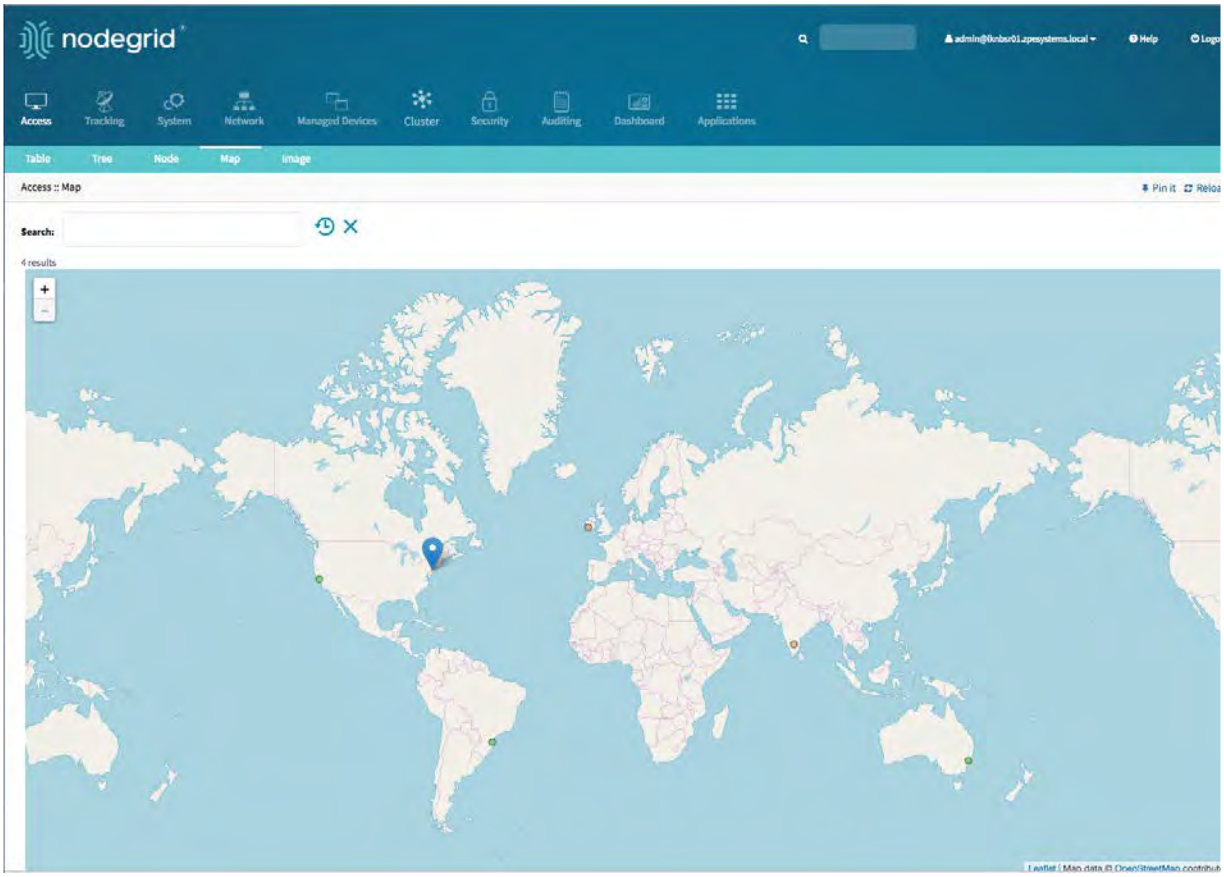


More advanced search options are available through the Search field. See “Device Search” on page 71 for more details.

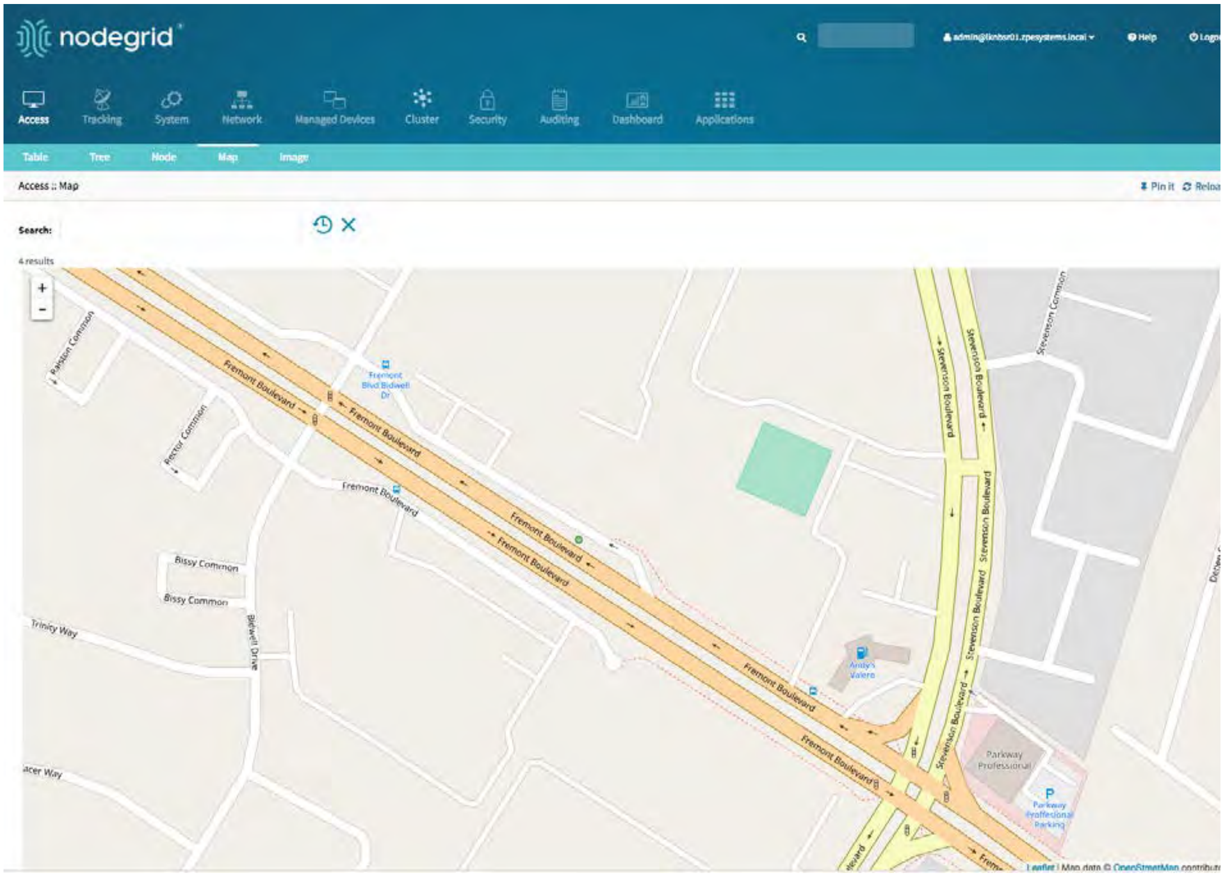
Map View

The Map View allows you to see the current status of your devices on a global map to get a complete overview of all targets and Nodegrid units in a Cluster (see “Cluster” on page 266). The Map View displays precise location details down to a building level. This view allows you to access target device information and connections by clicking on the target nodes.

Global View


nodegrid
admin@lknbsr01.zpesystems.local
Help
Logo
Access
Tracking
System
Network
Managed Devices
Cluster
Security
Auditing
Dashboard
Applications
Table
Tree
Node
Map
Image
Access :: Map
Pin it
Reloa
Search:
4 results
+
-
Leaflet | Map data © OpenStreetMap contribut

Street View



More advanced search options are available through the Search field. See “Device Search” on page 71 for more details.

Image View

The Image View allows customers to display a custom view of their Nodegrid units and target devices and associated information. This configuration requires Professional Services implementation. Please contact Customer Support at support@zpesystem.com for additional information.

Search

The Nodegrid Platform provides advanced search capabilities which allow users to easily search and access the information and target devices they require.

Device Search

The Device Search is available on all Device views and provides an easy method to search and filter the Target devices in each view.

The Device Search can be accessed in the WebUI through the search field in the top left-hand corner of each view, and on the CLI with the `search` command in the access menu. The NodeIQ™ Natural Language Search allows users to search for device property fields, including custom fields. This function works naturally with stand-alone units as well across all Nodegrid units in a Cluster configuration. The System automatically updates all the information about device changes and newly added devices and their properties in the background.

The Search filed supports the following keywords:

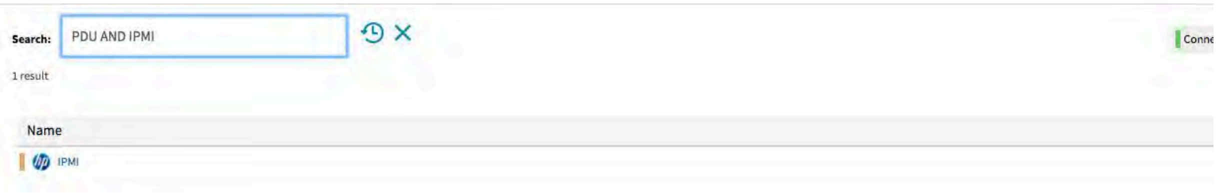
Table 38: Search Field

[Search String]	A search string which represents part of or a complete string to be searched for
AND	Combines multiple search strings with an AND
OR	Combines multiple search strings with an OR. Default search behavior for more than one search string
NOT	Any targets matching the search string will NOT be returned
[Field Name]	Allows limit of the Search String to a specific Field Name

Note: The keywords AND, OR and NOT are case-sensitive "and", "or", "not" will be identified as search strings.

To search for standard and custom field data (including groups, such as "admin" group), IP addresses or a specific device, follow the examples below:

Example with AND
"PDU AND IPMI"



Search: PDU AND IPMI

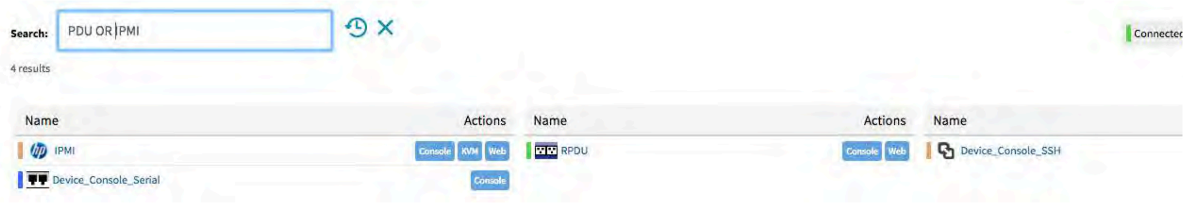
1 result

Name
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"



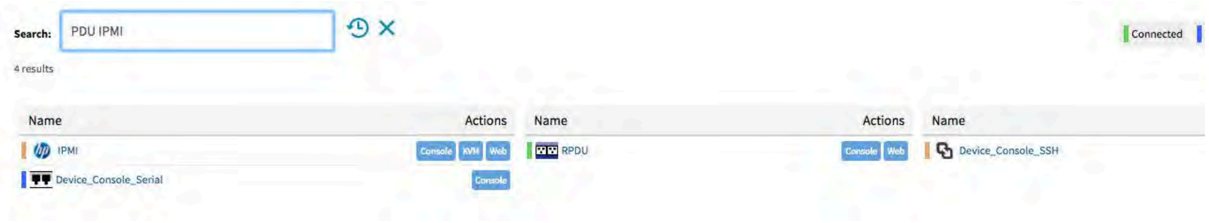
Search: PDU OR IPMI

4 results

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

```
[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  -
```

"PDU IPMI"



Search: PDU IPMI

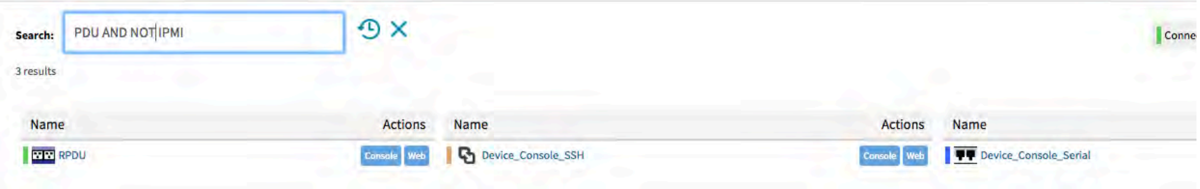
4 results

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

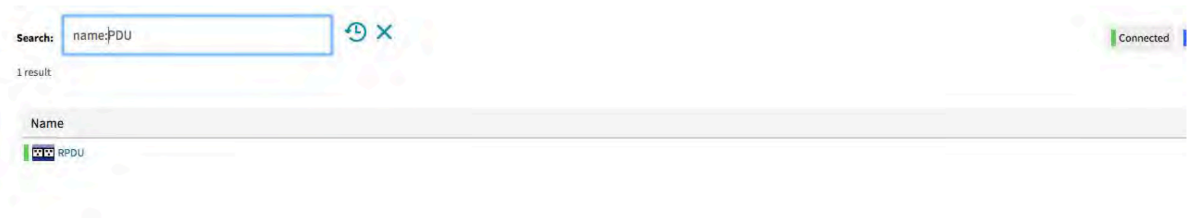
3 results

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"



Search: name:PDU

1 result

Name
RPDU

```
[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

A Global Search option is available in the WebUI. The Search field is located at the top of the screen beside the current user information and log out option. Global search works in the same way as Device Search and supports the same keywords. Search is available from all screens and allows easy access to all target devices and target sessions.

Device Management (Managed Devices)

The Managed Devices Section allows users to configure, create, and delete target devices. The Nodegrid Platform supports target devices which are connected through a serial, USB, or network connection. The following protocols are currently supported for network-based devices:

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

The user has multiple options to enable or create and new target devices. They can be manually enabled/created or can be discovered.

Each managed device added in the system uses one license from the pool. Each unit is shipped with enough perpetual licenses to cover the number of physical ports. Additional licenses can be added to a unit to allow it to manage additional devices. If licenses expire or are deleted from the system, the devices exceeding the total licenses will have their status changed to “unlicensed”. While their information will be retained in the system, the unlicensed devices will not show up in the access page preventing the user from connecting to them. Only licensed devices are listed on the access page and are available for access and management. The top right corner of the Managed Devices view shows the total licenses in the system, total in use and total available licenses. See “Licenses” on page 175 for more details.

The Nodegrid platform supports the following managed device types:

- Console connections utilizing RS232 protocol. Supported on Nodegrid Console Server and Nodegrid Services Router family.
- 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

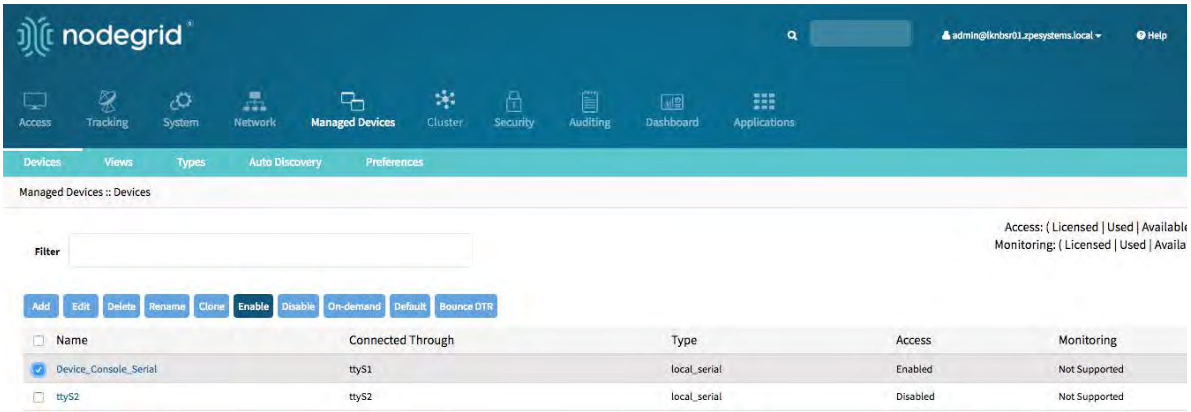
Configuration of Managed Devices

New devices can be added to the Devices menu. The menu offers the options to:

- `enable`, `disable`, `configure` and `reset` devices connected to physical ports
- `add`, `delete` and `configure` devices connected through a network connection
- `rename` existing devices/ports
- `clone` existing devices
- to quickly change the connection mode to `On-Demand`
- To `Bounce DTR` signal for serial ports

To perform any of these tasks, click on the button or select a device and then click the button in the WebUI, or use the command in the CLI.

WebUI Enable Port 1 example



Managed Devices :: Devices

Filter

Access: (Licensed | Used | Available
Monitoring: (Licensed | Used | Availa

	Name	Connected Through	Type	Access	Monitoring
☑	Device_Console_Serial	ttyS1	local_serial	Enabled	Not Supported
□	ttyS2	ttyS2	local_serial	Disabled	Not Supported

CLI rename port 2 example

```
[admin@nodegrid devices]# rename ttyS2
[admin@nodegrid {devices}]# set new_name=Port2
[admin@nodegrid {devices}]# commit
```

Serial Devices

The Nodegrid Platform supports RS-232 Serial connections thought the available Serial and USB interfaces. The ports are automatically detected and displayed in the Devices menu. Each port needs to be enabled and configured to provide access to the target device.

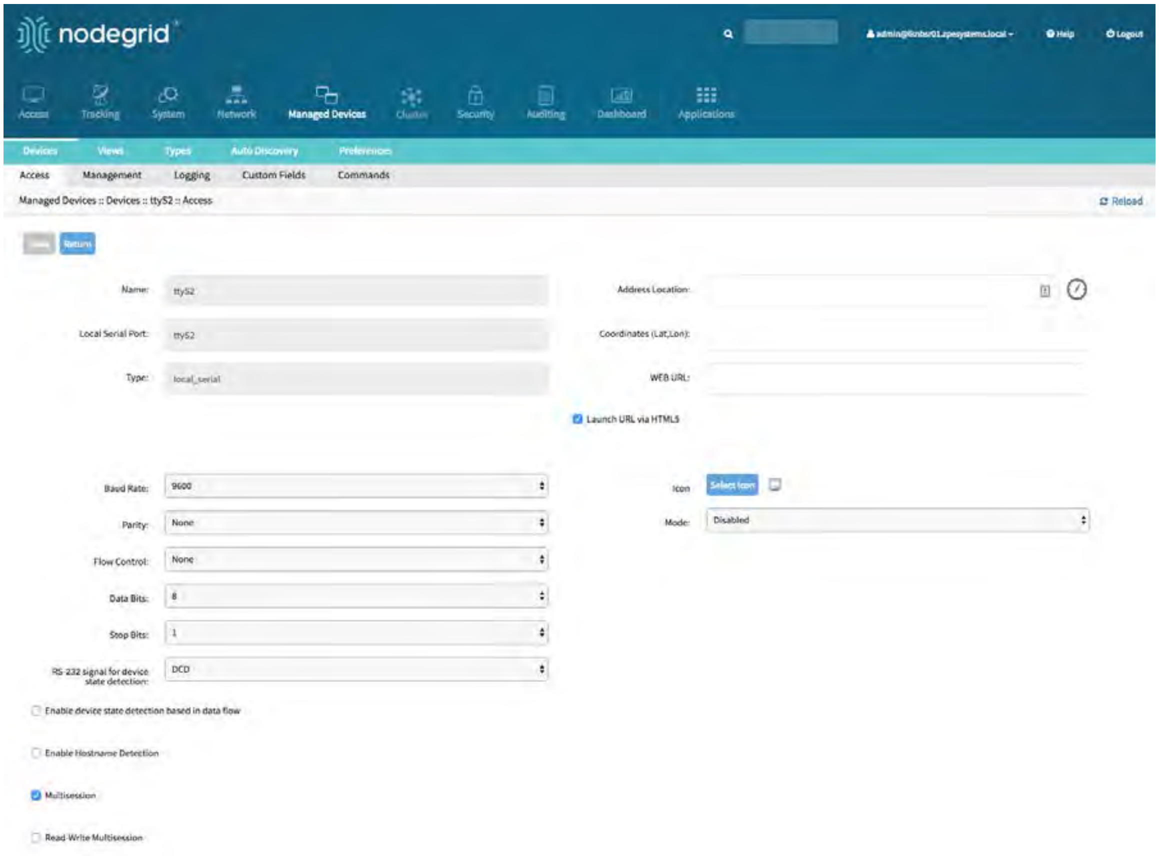
Before configuring the Nodegrid port, check the console port settings of the target device with the manufacturer. Most devices use the following settings which are default for the port: 9600,8,N,1

The Nodegrid Console Server S Series supports advanced auto-detection which simplifies the configuration process by automatically detecting the cable pinout (Legacy and Cisco) and connection speed.

Configure Serial Devices - WebUI

1. Navigate to `Managed Devices:: Devices`
2. Click on the port or select the port and click on `Edit`. Multiple Ports can be selected
3. Confirm the values for:
    - `Baud Rate` set it to the correct speed matching the target device settings or to `Auto`
    - `Parity` possible values are: None (default), Odd, or Even
    - `Flow Control` possible values are: None (default), Software, Hardware
    - `Data Bits` possible values are: 5,6,7,8 (default)
    - `Stop Bits` possible values are: 1
    - `RS-232 signal for device state detection` possible values are: DCD (default), None, CTS
    - `Mode` possible values are: Enabled, On-Demand, Disabled

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See "Device Settings" on page 132 for more details



Managed Devices :: Devices :: ttyS2 :: Access

Name: ttyS2

Local Serial Port: ttyS2

Type: local_serial

Address Location:

Coordinates (Lat,Lon):

WEB URL:

☑ 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

Icon

Mode: Disabled

☐ Enable device state detection based in data flow

☐ Enable Hostname Detection

☑ Multisession

☐ Read-Write Multisession

Configure Serial Devices - CLI

1. Navigate 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 the current values
4. use the `set` command adjust the values for:
   - `baud_rate` set it to the correct speed matching the target device settings or to `Auto`
   - `parity` possible values are: None (default), Odd, or Even
   - `flow_control` possible values are: None (default), Software, Hardware
   - `data_bits` possible values are: 5,6,7,8 (default)
   - `stop_bits` possible values are: 1
   - `rs-232_signal_for_device_state_detection` possible values are: DCD (default), None, CTS
   - `mode` possible values are: Enabled, On-Demand, Disabled

Optional: settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings” on page 132 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 = ^O
show_text_information = yes
enable_ip_alias = no
enable_second_ip_alias = no
allow_ssh_protocol = yes
ssh_port =
allow_telnet_protocol = yes
telnet_port = 7002
allow_binary_socket = no
data_logging = no
[admin@nodegrid {devices}]# set mode=enabled baud_rate=Auto
[admin@nodegrid {devices}]# commit
```

Service Processor Devices

The Nodegrid platform supports multiple IPMI based Service Processors like IPMI 1.5, IMPI 2.0, Hewlett Packard ILO's, Oracle/SUN iLOM's, IBM IMM's, Dell DRAC and iDRAC.

In order to manage these devices, Nodegrid requires a valid network connection to the target device. This can be through a dedicated network interface on the Nodegrid itself or through an existing network connection.

Nodegrid supports the following features for Service Processors.

Note: Some features might not be available depending on the Service Processor's capabilities.

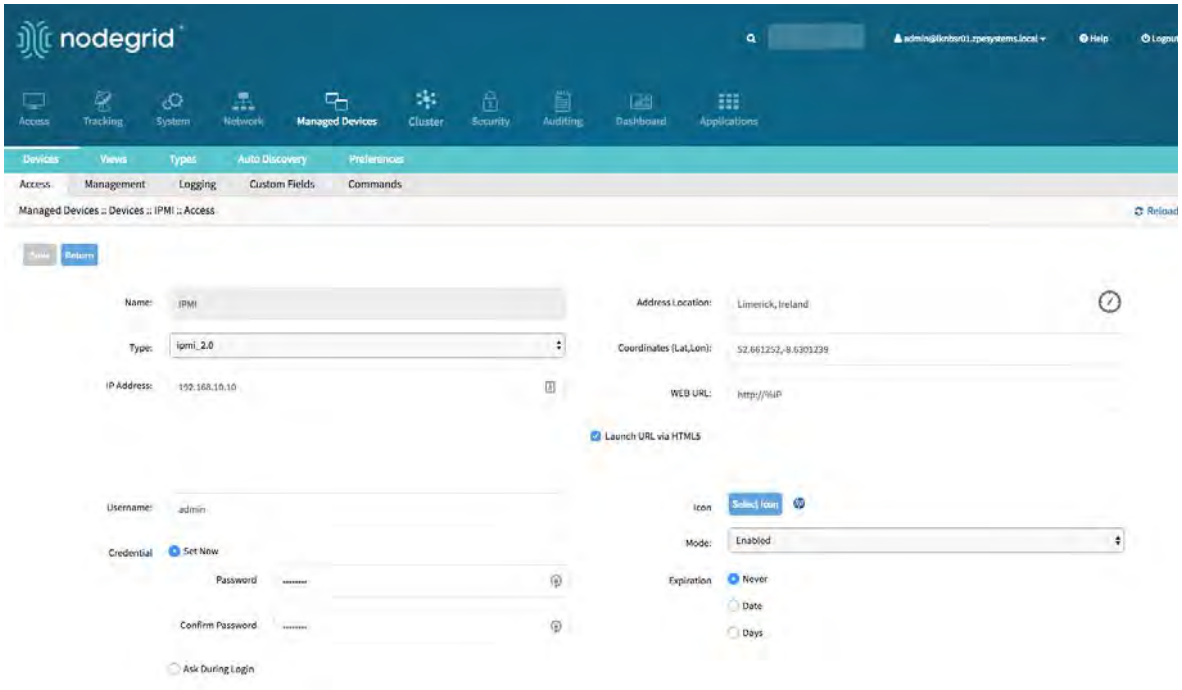
- Serial Over LAN (SOL)
- Web Interface
- KVM sessions
- support for Virtual Media
- Power Control
- Data Logging
- Event Logging
- Power Control through Rack PDU

For console access via SOL, you must also enable BIOS console redirect and OS console redirect (typically for Linux OS) on the server.

Add Service Processor Devices - WebUI

1. Navigate `Managed Devices:: Devices`,
2. Click the `Add` button to add a device to the system. For the purpose of this example, provide the following information:
3. Enter the name of the server you want to add.
4. Enter the IP address of the service processor. Make sure the IP address is reachable by the Nodegrid platform.
5. In the `Type` field, select a type that matches the service processor in use. Possible values are: ipmi1.5,ipmi2.0, ilo, ilom, imm, drac, idrac6
6. Enter the `username` and `password` of the service processor, or select `Ask During Login` option if you want to provide user credentials during the login time
7. Click the Save button.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See "Device Settings" on page 132



Managed Devices :: Devices :: IPMI :: Access

Name: IPMI

Type: ipmi_2.0

IP Address: 192.168.10.10

Address Location: Limerick, Ireland

Coordinates (Lat,Lon): 52.661252,-8.6301239

WEB URL: http://%IP

☑ Launch URL via HTML5

Username: admin

Credential ● Set Now

Password ········

Confirm Password ········

○ Ask During Login

Icon

Mode: Enabled

Expiration ● Never

○ Date

○ Days

Add Service Processor Devices - CLI

1. Navigate 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`, possible values are: ipmi1.5,ipmi2.0, ilo, ilom, imm, drac, idrac6
    - `ip_address`
    - `username` and `password` of the service processor, or select `Ask During Login` option if you want to provide user credentials during the login time
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” on page 132 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

The Nodegrid solution supports the use of remote shares like NFS or Windows shares to contain files which can be shared with Service Processor systems through an existing Virtual Media feature on the Service Processor. Before the files can be shared out through the Virtual media function, the remote share needs to be mounted to the Nodegrid.

1. connect to the Nodegrid shell as the root user
2. Navigate to /var/firefox/datastore/
3. Create a folder which will be used to mount the remote share
4. Use the mount command to mount the remote share to the folder

The mount command can be added to the `/etc/fstab` file to get the share mounted permanently.

NFS mount example to folder VirtualMedia

```
 mount -t nfs  192.168.1.1.:/NFS/NG /var/firefox/datastore/VirtualMedia
```

Devices with SSH

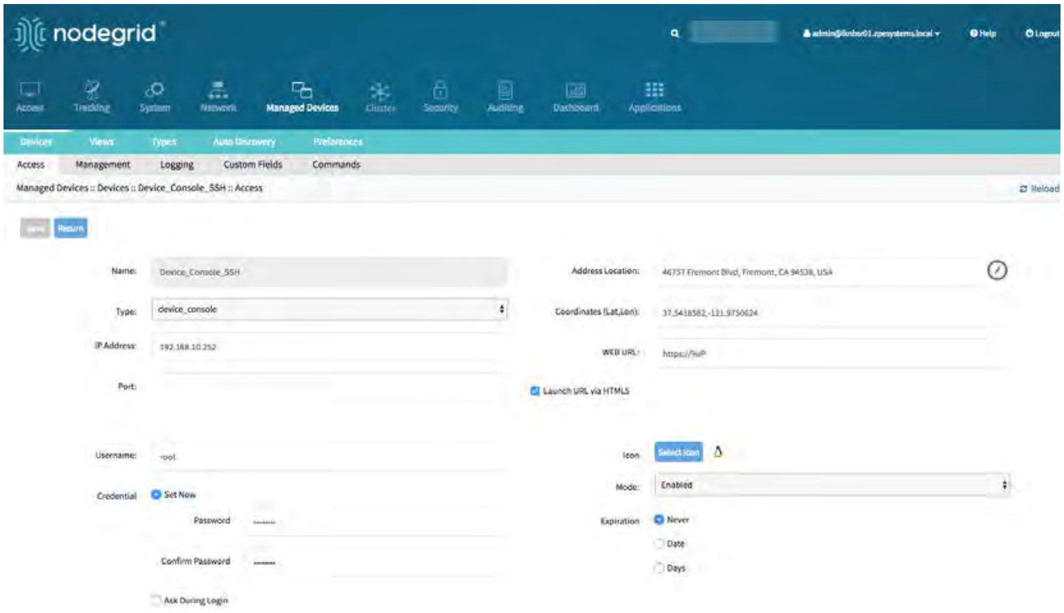
The Nodegrid solution supports the management of target devices through SSH. The following features are supported for these devices:

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

Add Devices with SSH - WebUI

1. Navigate `Managed Devices:: Devices`,
2. Click the `Add` button to add a device to the system.
3. Enter the name of the server you want to add.
4. Enter the IP address of the device. Make sure the IP address is reachable by the Nodegrid platform.
5. In the `Type` field, select a type that matches the ssh or telnet in use. Possible values are: device_console
6. Enter `username` and `password` of the ssh server, or select `Ask During Login` option if you want to provide user credentials during the login time
7. Click the Save button.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings” on page 132



Managed Devices :: Devices :: Device_Console_SSH :: Access

Name: Device_Console_SSH
Type: device_console
IP Address: 192.168.10.252
Port:
Username: root
Credential: ● Set Now
Password: ....
Confirm Password: ....
□ Ask During Login

Address Location: 46757 Fremont Blvd, Fremont, CA 94538, USA
Coordinates (Lat,Lon): 37.5418582,-121.9750624
WEB URL: https://%IP
☑ Launch URL via HTML5
Icon
Mode: Enabled
Expiration: ● Never ○ Date ○ Days

Add Devices with SSH - CLI

1. Navigate 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`, possible values are: device_console
   - `ip_address`
   - `username` and `password` of the device, or select `Ask During Login` option if you want to provide user credentials during the login time
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” on page 132 for more details.

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

Console Servers

Nodegrid supports multiple 3rd party Console Servers from different vendors, including console servers from Avocent and Servertech. These devices can be added to the Nodegrid Platform to allow the connected targets to be used as if they had been directly connected to a Nodegrid appliance. Adding 3rd party Console Servers is a two-step process, In the first step, the 3rd party appliance is added to the Nodegrid and in a 2nd step, all enabled ports will be added to the platform.
The Nodegrid supports the following features for these devices:

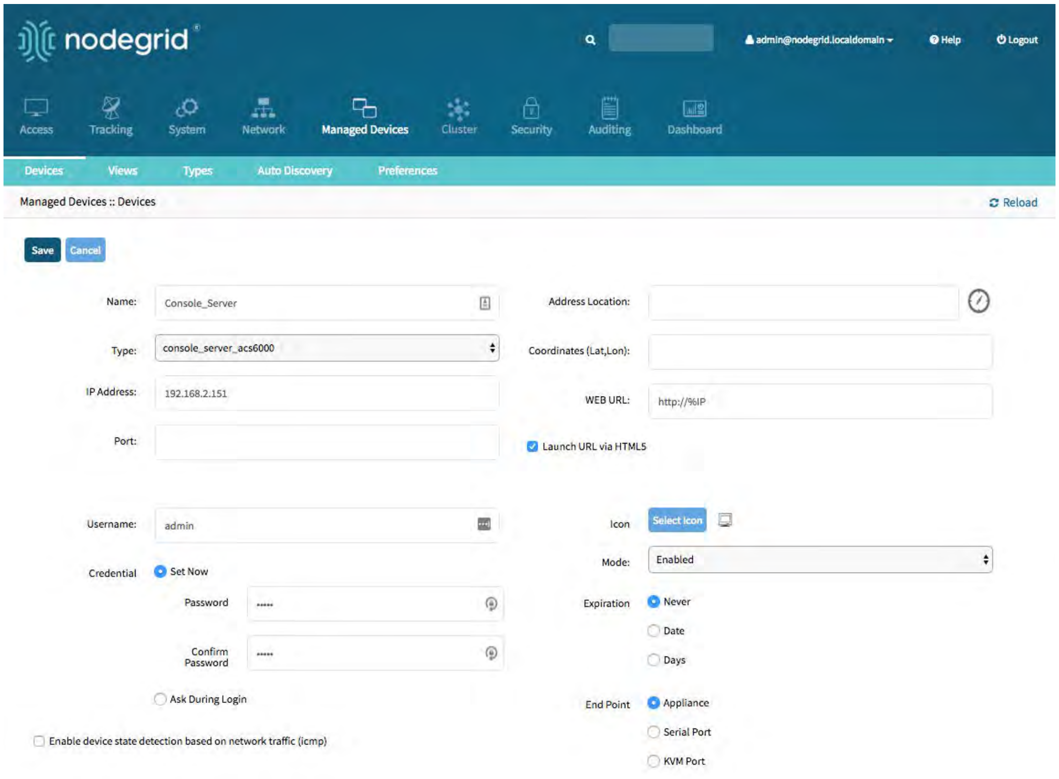
- Console Session
- Data Logging
- Custom Commands
- Web Sessions
- Power Control through Rack PDU

Add Console Servers - WebUI

1. Navigate `Managed Devices:: Devices`,
2. Click the `Add` button to add a device to the system.
3. Enter the name of the console server you want to add.
4. Enter the IP address of the console server. Make sure the IP address is reachable by the Nodegrid platform.

5. In the `Type` field, select a type that matches the console server. Possible values are: console_server_nodegrid,console_server_acs,console_server_acs6000,console_server_lantronix,console_server_opengear,console_server_digicp
6. Enter the `username` and `password` of the console server, or select the `Ask During Login` option if you want to provide user credentials during the login time
7. Click the Save button.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See "Device Settings" on page 132



Managed Devices :: Devices

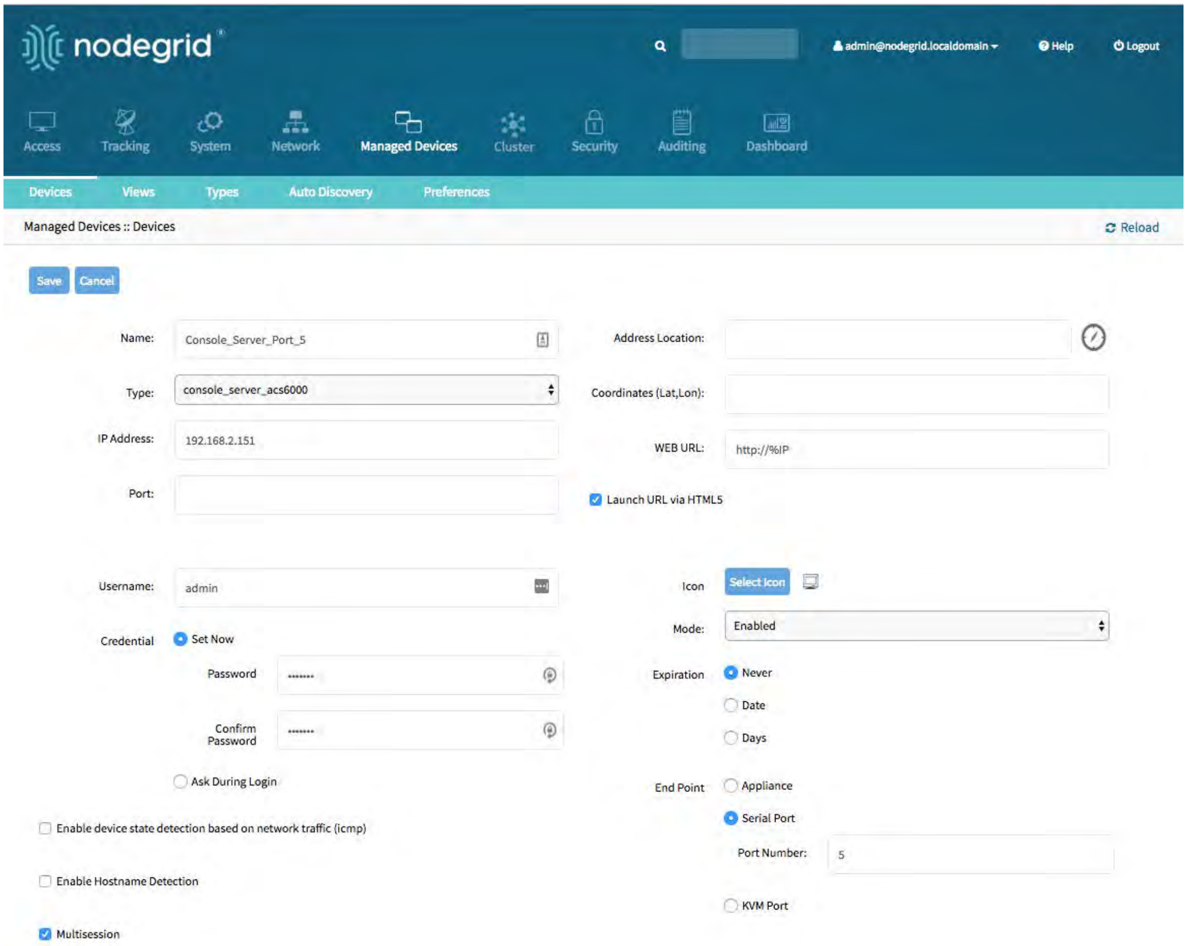
Name:	Console_Server	Address Location:	
Type:	console_server_acs6000	Coordinates (Lat,Lon):	
IP Address:	192.168.2.151	WEB URL:	http://%IP
Port:			☑ Launch URL via HTML5
Username:	admin	Icon	
Credential	● Set Now	Mode:	Enabled
Password	•••••	Expiration	● Never ○ Date ○ Days
Confirm Password	•••••		
	○ Ask During Login	End Point	● Appliance ○ Serial Port ○ KVM Port

□ Enable device state detection based on network traffic (icmp)

Add Console Server Ports - WebUI

1. Navigate `Managed Devices:: Devices`
2. Click the `Add` button to add a device to the system.
3. Enter the name of the console server port you want to add.
4. Enter the IP address of the console server. Make sure the IP address is reachable by the Nodegrid platform.
5. In the `Type` field, select a type that matches the console server. Possible values are: console_server_nodegrid_,console_server_acs,console_server_acs6000,console_server_lantronix,console_server_opengear,console_server_digicp
6. Enter `username` and `password` of the console server, or select `Ask During Login` option if you want to provide user credentials during the login time
7. Select as `End Point` Serial Port and enter the port number
8. Click the Save button.

Note: Ports can be automatically detected and added. See “Auto-Discovery” on page 112 for more details.



Name: Console_Server_Port_5

Type: console_server_acs6000

IP Address: 192.168.2.151

Port:

Username: admin

Credential ● Set Now

Password ••••••

Confirm Password ••••••

○ Ask During Login

☐ Enable device state detection based on network traffic (icmp)

☐ Enable Hostname Detection

☑ Multisession

Address Location:

Coordinates (Lat,Lon):

WEB URL: http://%IP

☑ Launch URL via HTML5

Icon Select Icon

Mode: Enabled

Expiration ● Never ○ Date ○ Days

End Point ○ Appliance ● Serial Port

Port Number: 5

○ KVM Port

Add Console Servers - CLI

1. Navigate 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`, possible values are: console_server_acs, console_server_acs6000,console_server_lantronix,console_server_opengear,console_server_digicp
   - `ip_address`
   - `username` and `password` of the device or select `Ask During Login` option if you want to provide user credentials during the login time
   - `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” on page 132

```
[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
```

Add Console Server Ports - CLI

1. Navigate 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`, possible values are: console_server_acs, console_server_acs6000,console_server_lantronix,console_server_opengear,console_server_digicp
    - `ip_address`
    - `username` and `password` of the device, or select `Ask During Login` option if you want to provide user credentials during the login time
    - `endpoint` should be defined as serial_port
    - `port_number` should be defined as the 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” on page 132

Note: Ports can be automatically detected and added. See Auto Discovery“Auto-Discovery” on page 112 Section 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

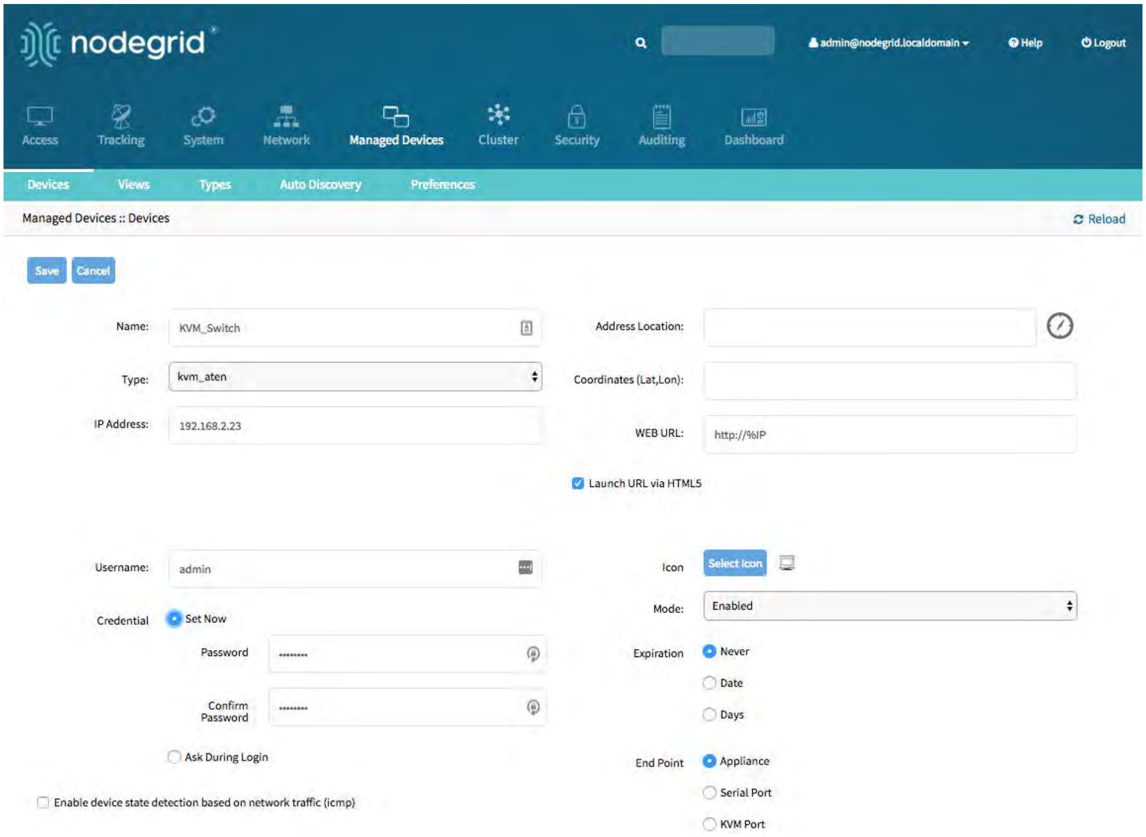
The Solution supports multiple 3rd party KVM Switches from different vendors, including products from Avocent and Raritan. These devices can be added to the Nodegrid Platform and the system to allow the connected targets to be used as if they had been directly connected to a Nodegrid appliance. Adding 3rd party KVM Switches is a two-step process, in the first step the 3rd party appliance is added to the Nodegrid and in a 2nd step, all enabled ports will be added to the platform.
The Nodegrid supports the following features for these devices:

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

Add KVM Switches - WebUI

1. Navigate `Managed Devices:: Devices`,
2. Click the `Add` button to add a device to the system.
3. Enter the name of the KVM switch you want to add.
4. Enter the IP address of the KVM switch. Make sure the IP address is reachable by the Nodegrid platform.
5. In the `Type` field, select a type that matches the KVM switch. Possible values are: kvm_dsr, kvm_mpu,kvm_aten,kvm_raritan
6. Enter `username` and `password` of the KVM switch, or select `Ask During Login` option if you want to provide user credentials during the login time
7. Click the Save button.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings” on page 132



Managed Devices :: Devices

Name: KVM_Switch

Type: kvm_aten

IP Address: 192.168.2.23

Address Location:

Coordinates (Lat,Lon):

WEB URL: http://%IP

☑ Launch URL via HTML5

Username: admin

Credential ● Set Now

Password ••••••••

Confirm Password ••••••••

○ Ask During Login

□ Enable device state detection based on network traffic (icmp)

Icon

Mode: Enabled

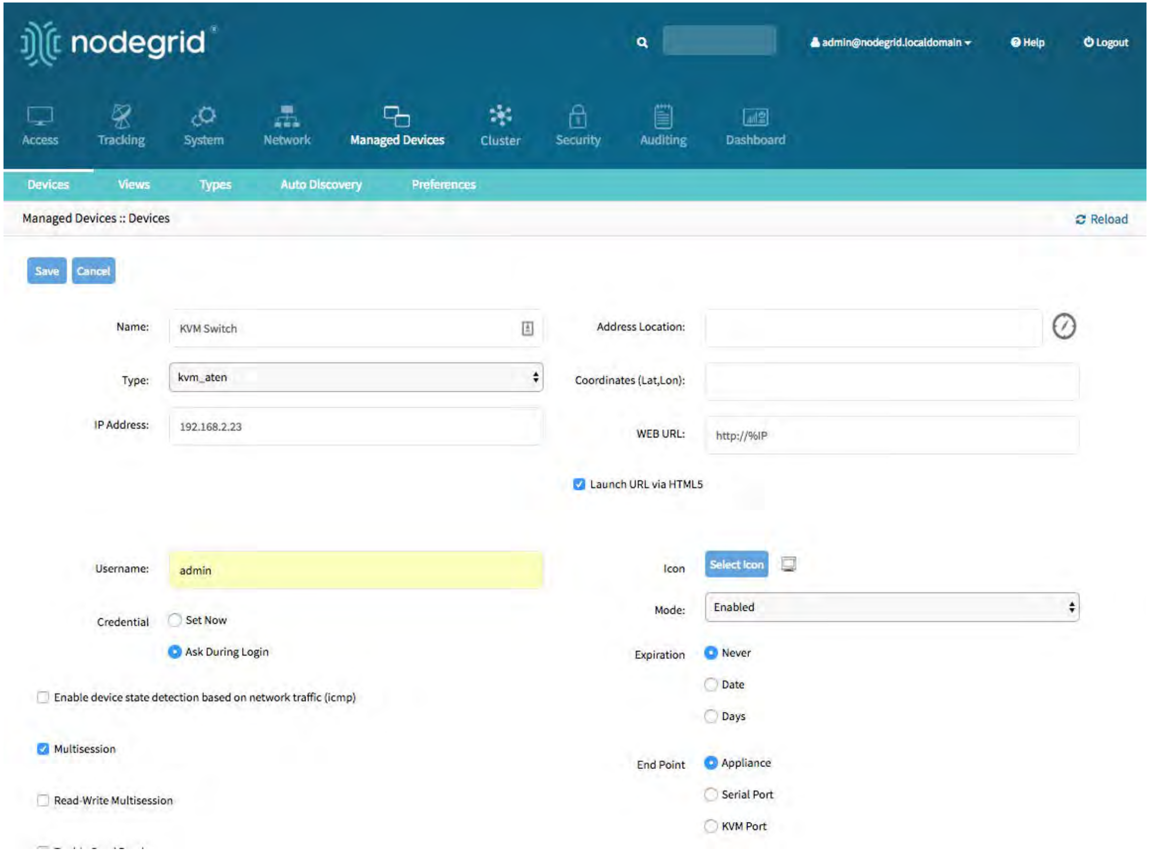
Expiration ● Never ○ Date ○ Days

End Point ● Appliance ○ Serial Port ○ KVM Port

Add KVM Switch Ports - WebUI

1. Navigate `Managed Devices:: Devices`,
2. Click the `Add` button to add a device to the system.
3. Enter the name of the KVM switch port you want to add.
4. Enter the IP address of the KVM switch. Make sure the IP address is reachable by the Nodegrid platform.
5. In the `Type` field, select a type that matches the KVM switch. Possible values are: kvm_dsr, kvm_mpu,kvm_aten,kvm_raritan
6. Enter `username` and `password` of the KVM switch, or select `Ask During Login` option if you want to provide user credentials during the login time
7. Select as `End Point` KVM Port and enter the port number
8. Click the Save button.

Note: Ports can be automatically detected and added see Auto Discovery“Auto-Discovery” on page 112 Section for details



Managed Devices :: Devices

Name: KVM Switch

Type: kvm_aten

IP Address: 192.168.2.23

Address Location:

Coordinates (Lat,Lon):

WEB URL: http://%IP

☑ Launch URL via HTML5

Username: admin

Credential ○ Set Now ● Ask During Login

Icon

Mode: Enabled

Expiration ● Never ○ Date ○ Days

□ Enable device state detection based on network traffic (icmp)

☑ Multisession

End Point ● Appliance ○ Serial Port ○ KVM Port

□ Read-Write Multisession

Add KVM Switches - CLI

1. Navigate 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`, possible values are: kvm_dsr, kvm_mpu,kvm_aten,kvm_raritan
   - `ip_address`
   - `username` and `password` of the device, or select `Ask During Login` option if you want to provide user credentials during the login time
   - `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” on page 132

```
[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
```

Add KVM Switch Ports - CLI

1. Navigate 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`, possible values are: kvm_dsr, kvm_mpu,kvm_aten,kvm_raritan
   - `ip_address`
   - `username` and `password` of the device, or select `Ask During Login` option if you want to provide user credentials during the login time
   - `endpoint` should be defined as serial_port
4. `port_number` should be defined as the port number
5. 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” on page 132

> Note: Ports can be automatically detected and added. See Auto Discovery“Auto-Discovery” on page 112 Section 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 PDU's

The Solution supports multiple 3rd party Rack PDUs from different vendors, including products from APC, Avocent, Baytech,CPI, Cyberpower, Eaton, Enconnex, Geist, Liebert, Raritan, Rittal, and Servertech. These devices can be added to the Nodegrid Platform and the system will allow users to connect to the Rack PDU and control the power outlets (only if this function is supported by the Rack PDU). Outlets can then be associated to specific target devices, which allows users to directly control the specific power outlets for this target device.

The Nodegrid supports the following features for these devices:

- Console Sessions
- Data Logging
- Custom Commands
- Web Sessions
- Power Control of outlets

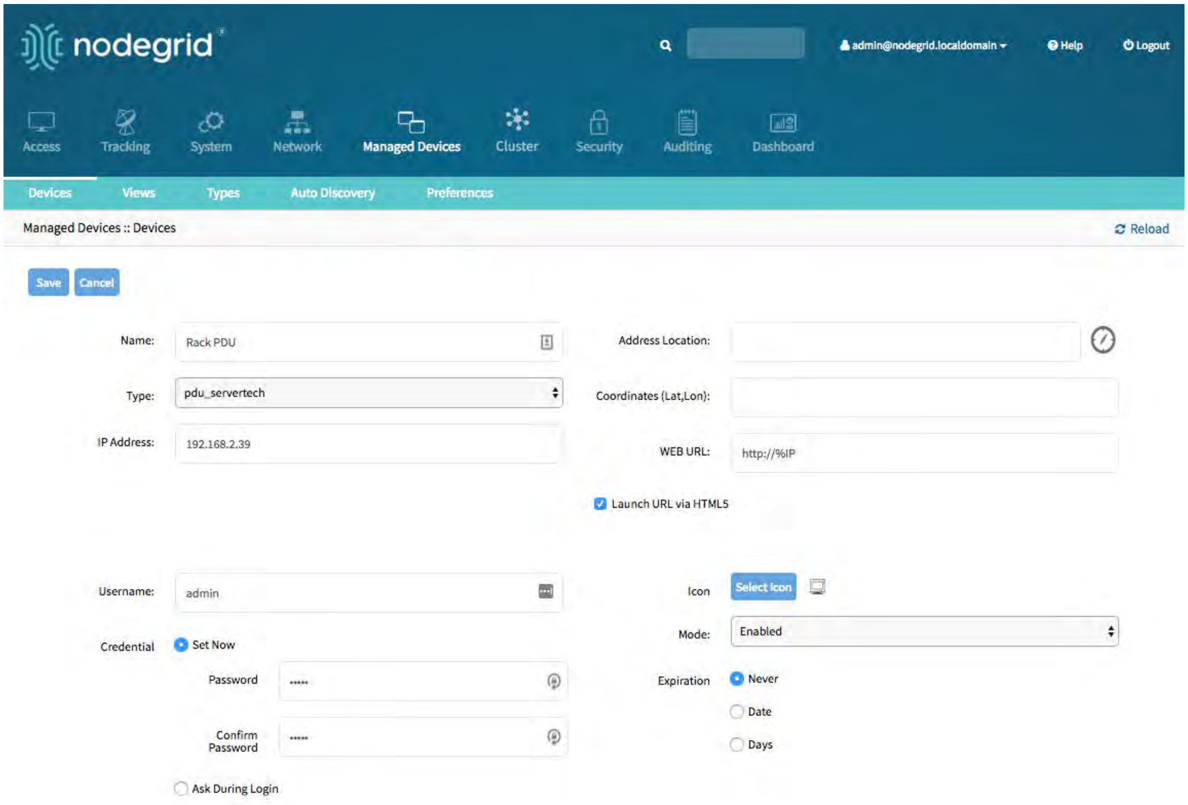
  Note: The Power Control feature needs to be supported by the Rack PDU. Check the manual of the Rack PDU if the feature is available on a specific model.

Rack PDUs - WebUI

1. Navigate `Managed Devices:: Devices`
2. Click the `Add` button to add a device to the system.
3. Enter the name of the Rack PDU you want to add.

4. Enter the IP address of the Rack PDU. Make sure the IP address is reachable by the Nodegrid platform.
5. In the `Type` field, select a type that matches the Rack PDU. Possible values are: pdu_apc, pdu_baytech,pdu_eaton,pdu_mph2,pdu_pm3000,pdu_cpi,pdu_raritan,pdu_geist,pdu_-servertech,pdu_enconnex,pdu_cyberpower,pdu_rittal
6. Enter `username` and `password` of the Rack PDU, or select `Ask During Login` option if you want to provide user credentials during the login time
7. Click the Save button.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See "Device Settings" on page 132



Managed Devices :: Devices

Name: Rack PDU

Type: pdu_servertech

IP Address: 192.168.2.39

Address Location:

Coordinates (Lat,Lon):

WEB URL: http://%IP

☑ Launch URL via HTML5

Username: admin

Credential ● Set Now

Password •••••

Confirm Password •••••

○ Ask During Login

Icon

Mode: Enabled

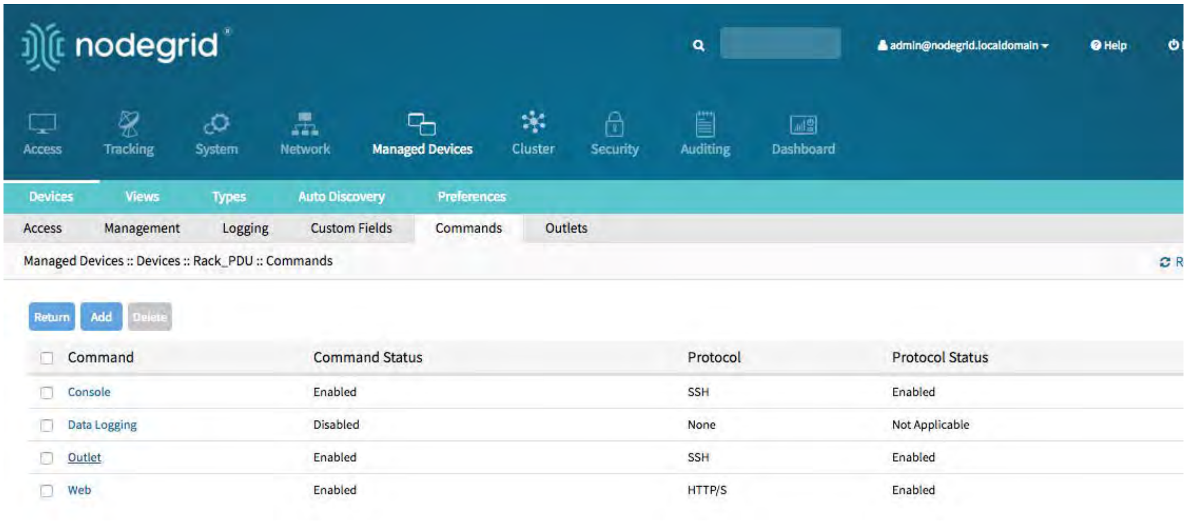
Expiration ● Never

○ Date

○ Days

Note: By default will Nodegrid communicate with the Rack PDU using ssh/telnet. The reaction time of Rack PDUs using these interface is typically very slow. It is therefore recommended to use SNMP for the communication with the Rack PDU if possible.

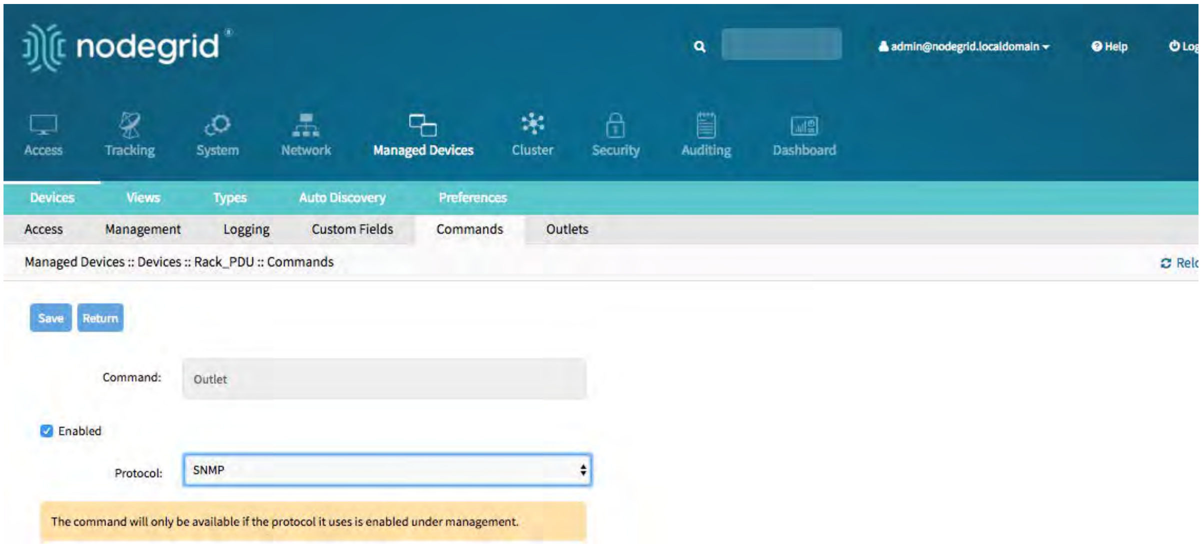
1. Navigate `Managed Devices:: Devices`
2. Click on the `Name` of the newly added Rack PDU
3. Navigate to the `Commands` menu and click on Outlets



Managed Devices :: Devices :: Rack_PDU :: Commands

Command	Command Status	Protocol	Protocol Status
Console	Enabled	SSH	Enabled
Data Logging	Disabled	None	Not Applicable
Outlet	Enabled	SSH	Enabled
Web	Enabled	HTTP/S	Enabled

4. Change the `Protocol` to SNMP and click on Save



Managed Devices :: Devices :: Rack_PDU :: Commands

Command: Outlet

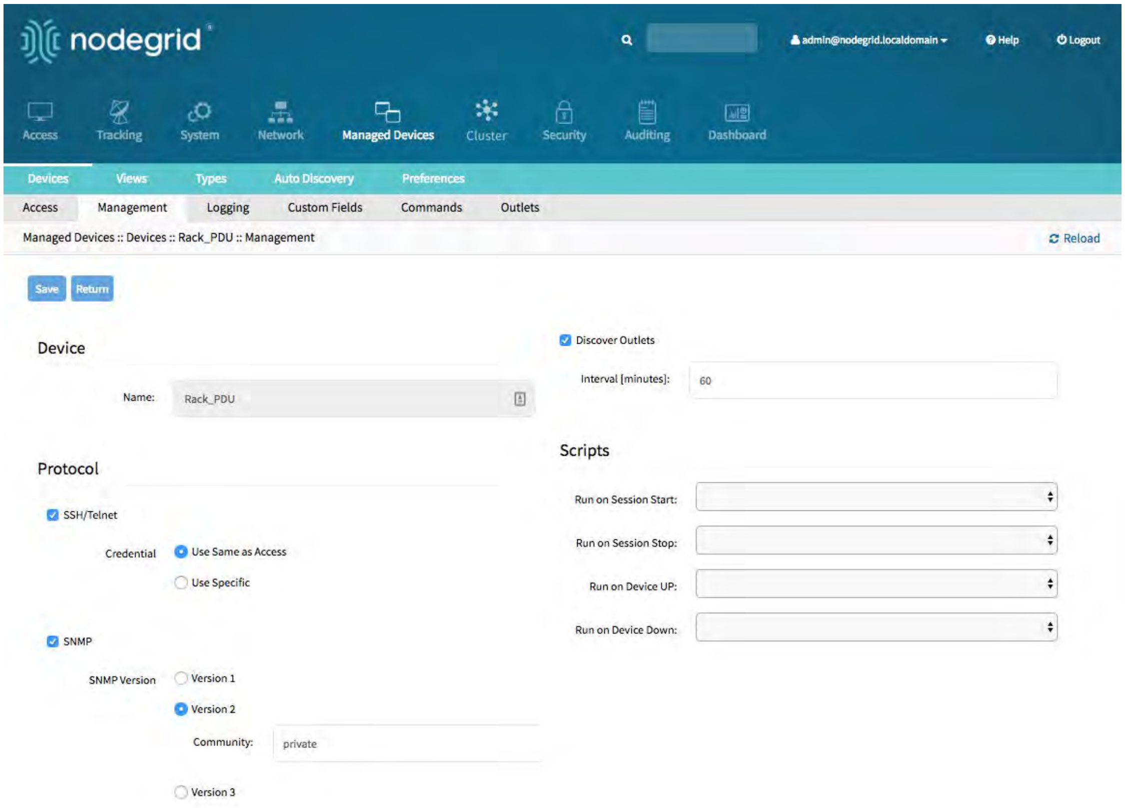
☑ Enabled

Protocol: SNMP

The command will only be available if the protocol it uses is enabled under management.

5. Navigate to the `Management` menu and update the SNMP values to match the settings on the Rack PDU, click on `Save`

   Note: Use SNMP details which provide read and write access. With Read-Only credentials, the Nodegrid Platform may not control the power outlets.



Device

Name: Rack_PDU

Protocol

☑ SSH/Telnet

Credential ● Use Same as Access

○ Use Specific

☑ SNMP

SNMP Version ○ Version 1

● Version 2

Community: private

○ Version 3

☑ Discover Outlets

Interval [minutes]: 60

Scripts

Run on Session Start:

Run on Session Stop:

Run on Device UP:

Run on Device Down:

6. The Rack PDU Outlets will be automatically discovered. This process may take a few minutes depending on the Rack PDU.

Add Rack PDU - CLI

1. Navigate 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`, possible values are: 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 select `Ask During Login` option if you want to provide user credentials during the login time
   - `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” on page 132

Note: By default will Nodegrid communicate with the Rack PDU using ssh/telnet. The reaction time of Rack PDUs using these interface is typically very slow. It is therefore recommended to use SNMP for the communication with the Rack PDU if possible.

1. Navigate to `/settings/devices/<device name>/commands/outlet`
2. Change the protocol to SNMP
3. Navigate 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 details which provide read and write access. With Read-Only credentials, the Nodegrid Platform may not control the power outlets.

6. The Rack PDU Outlets will be automatically discovered. This process may take 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_commmunity = private
[+admin@nodegrid management]# commit
```

Cisco UCS

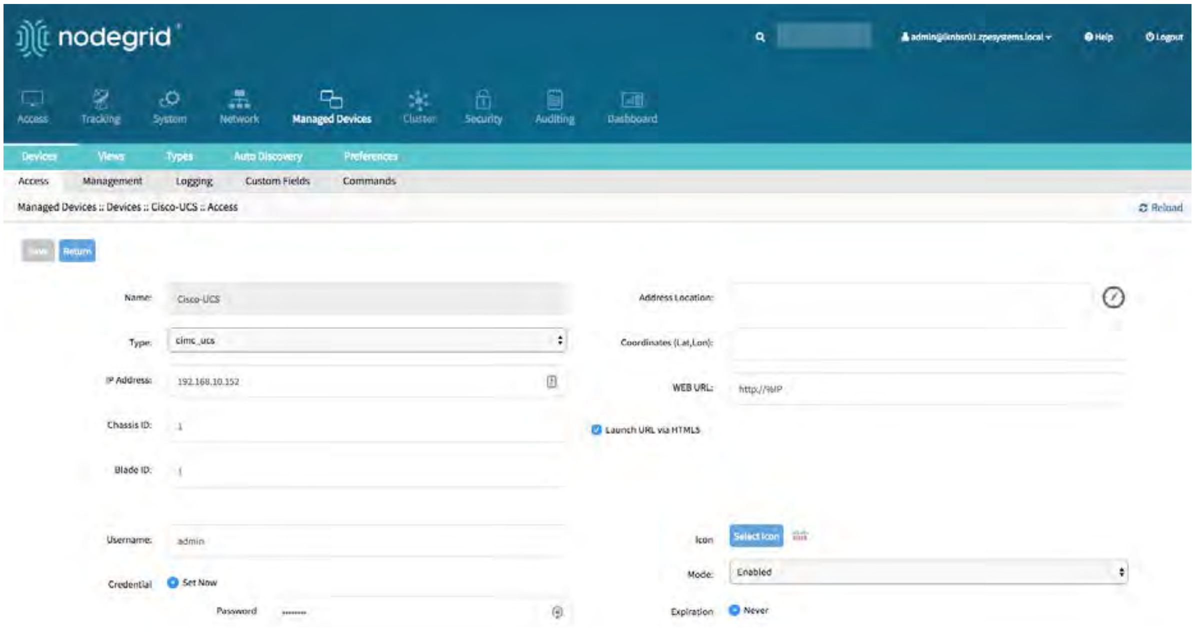
The Solution supports the management of Cisco UCS through there Console Ports as well as there management interfaces. The Nodegrid supports the following features for these devices:

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

Add Cisco UCS - WebUI

1. Navigate `Managed Devices:: Devices`,
2. Click the `Add` button to add a device to the system.
3. Enter the name of the Cisco UCS Blade to be added.
4. Enter the IP address of the Blade Chassis. Make sure the IP address is reachable by the Nodegrid platform.
5. In the `Type` field, select a type that matches the appliance. Possible values are: cimc_ucs
6. Enter the `Chassis ID` and the `Blade ID` which represent the blade
7. Enter `username` and `password` of the Blade Chassis, or select `Ask During Login` option if you want to provide user credentials during the login time
8. Click the Save button.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings” on page 132



Managed Devices :: Devices :: Cisco-UCS :: Access

Name:	Cisco-UCS	Address Location:	
Type:	cimc_ucs	Coordinates (Lat,Lon):	
IP Address:	192.168.10.152	WEB URL:	http://%IP
Chassis ID:	1	☑ Launch URL via HTML5	
Blade ID:	1		
Username:	admin	Icon	
Credential	● Set Now	Mode:	Enabled
Password	••••••••	Expiration	● Never

Add Cisco UCS - CLI

1. Navigate 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 to be added
   - `type`, possible values are: cimc_ucs
   - `ip_address` of the blade chassis
   - `chassis_id` of the blade chassis
   - `blade_id` of the blade server
   - `username` and `password` of the blade chassis, or select `Ask During Login` option if you want to provide user credentials during the login time
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” on page 132

```
[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

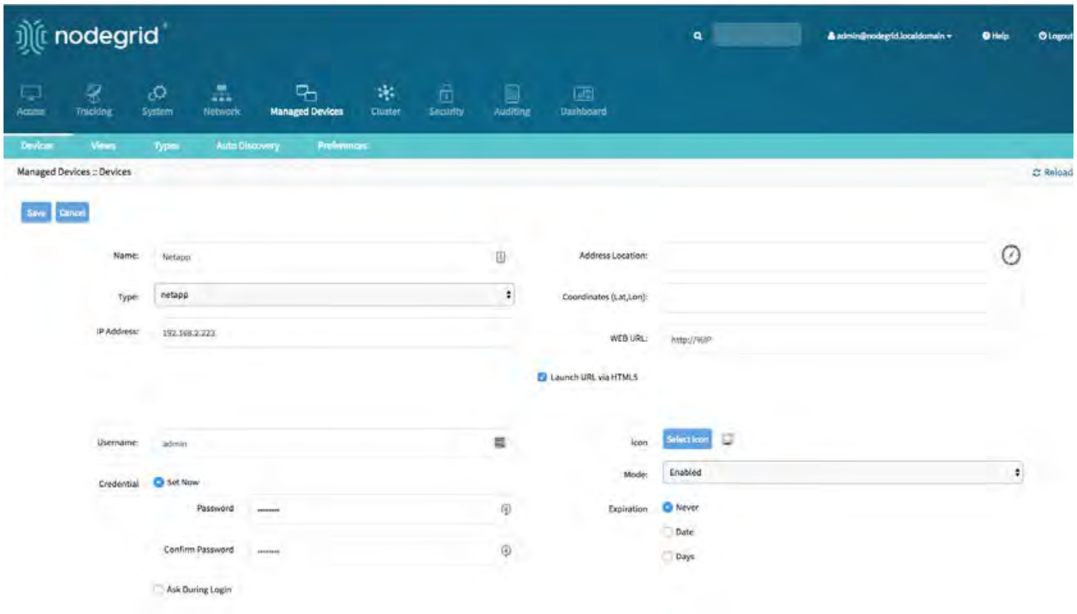
The Nodegrid solution supports the management of Netapp appliances through their management interfaces. The Nodegrid supports the following features for these devices:

- Console Session
- Data Logging
- Event Logging
- Power Control through Netapp appliance
- Web Session
- Custom Commands
- Power Control through Rack PDU

Add Netapp - WebUI

1. Navigate `Managed Devices:: Devices`,
2. Click the `Add` button to add a device to the system.
3. Enter the name of the appliance you want to add.
4. Enter the IP address of the device. Make sure the IP address is reachable by the Nodegrid platform.
5. In the `Type` field, select a type that matches the NetApp appliance. Possible values are: netapp
6. Enter `username` and `password`, or select `Ask During Login` option if you want to provide user credentials during the login time
7. Click the Save button.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings” on page 132



Managed Devices :: Devices

Name: Netapp

Type: netapp

IP Address: 192.168.2.223

Address Location:

Coordinates (Lat,Lon):

WEB URL: http://%IP

☑ Launch URL via HTML5

Username: admin

Credential ● Set Now

Password ········

Confirm Password ········

☐ Ask During Login

Icon

Mode: Enabled

Expiration ● Never ○ Date ○ Days

Add Netapp - CLI

1. Navigate 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`, possible values are: netapp
    - `ip_address`
    - `username` and `password` of the device, or select `Ask During Login` option if you want to provide user credentials during the login time
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” on page 132

```
[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

The Solution supports the Smart Access Control for Rack's solution appliances (Infrabox) from InfraSolution.

Nodegrid supports the following features for these devices:

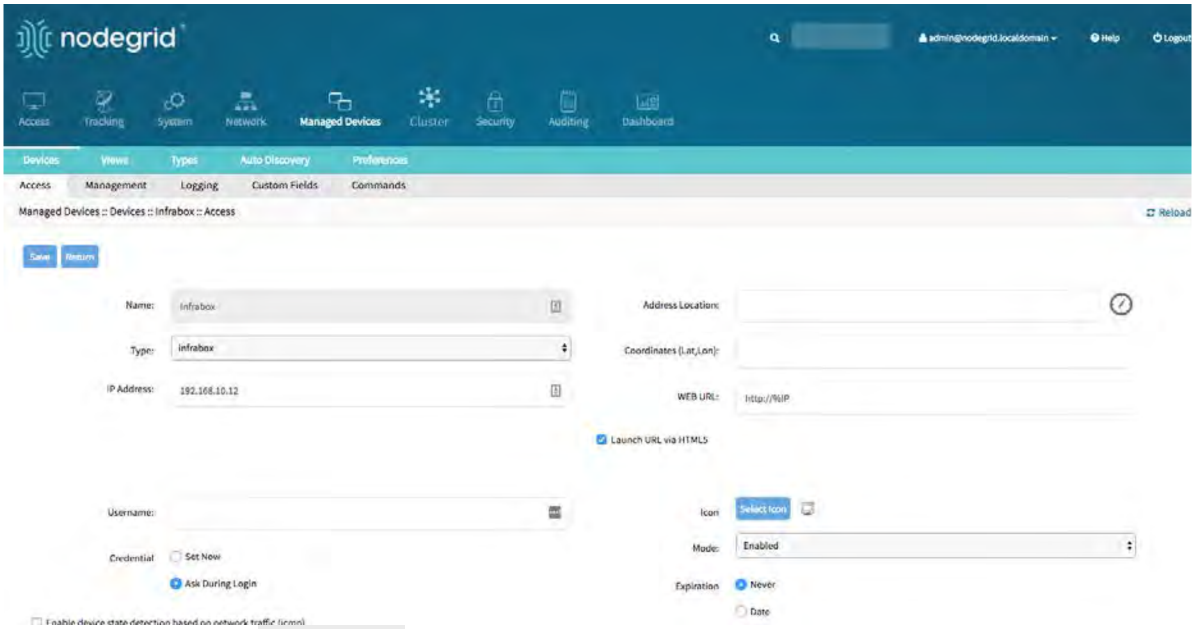
- Door Control
- Web Session
- Power Control through Rack PDU

Note: Communication to the appliances requires SNMP to be configured on the appliances

Add Infrabox - WebUI

1. Navigate `Managed Devices:: Devices`,
2. Click the `Add` button to add a device to the system.
3. Enter the name of the appliance you want to add.
4. Enter the IP address of the device. Make sure the IP address is reachable by the Nodegrid platform.
5. In the `Type` field, select a type that matches the Infrabox appliance. Possible values are: infrabox
6. Select `Ask During Login` and do not provide user credentials
7. Click the Save button.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings” on page 132

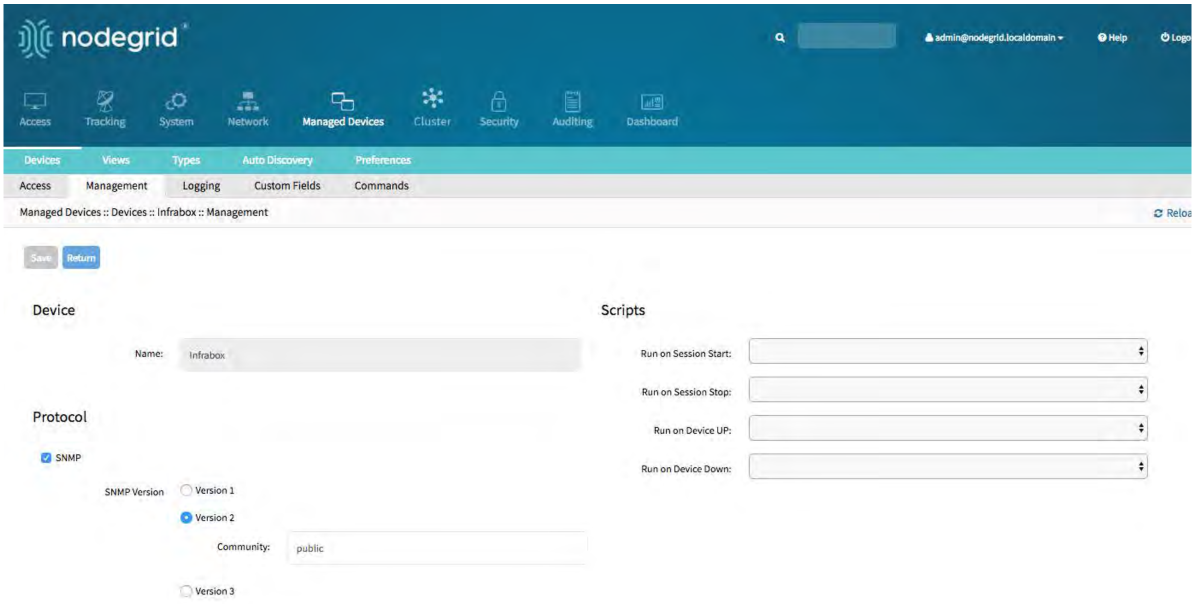


Managed Devices :: Devices :: Infrabox :: Access

Name: Infrabox
Type: infrabox
IP Address: 192.168.10.12
Username:
Credential ○ Set Now
● Ask During Login
□ Enable device state detection based on network traffic (icmp)

Address Location:
Coordinates (Lat,Lon):
WEB URL: http://%IP
☑ Launch URL via HTML5
Icon: Select Icon
Mode: Enabled
Expiration ● Never
○ Date

8. Navigate to the `Management` menu and update the SNMP values to match the settings on the appliance
9. Click on `Save`



Managed Devices :: Devices :: Infrabox :: Management

Device

Name: Infrabox

Protocol

☑ SNMP

SNMP Version ○ Version 1
● Version 2
Community: public
○ Version 3

Scripts

Run on Session Start:
Run on Session Stop:
Run on Device UP:
Run on Device Down:

Add Infrabox - CLI

1. Navigate 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`, possible values are: infrabox
    - `ip_address`
    - `username` and `password` of the device, or select `Ask During Login` option if you want to provide user credentials during the login time
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” on page 132

5. Navigate to `/settings/devices/<Device>/management/`
6. Use the `set` command to define the SNMP values
7. `snmp_version`
8. `snmp_community`
9. Save the changes with `commit`

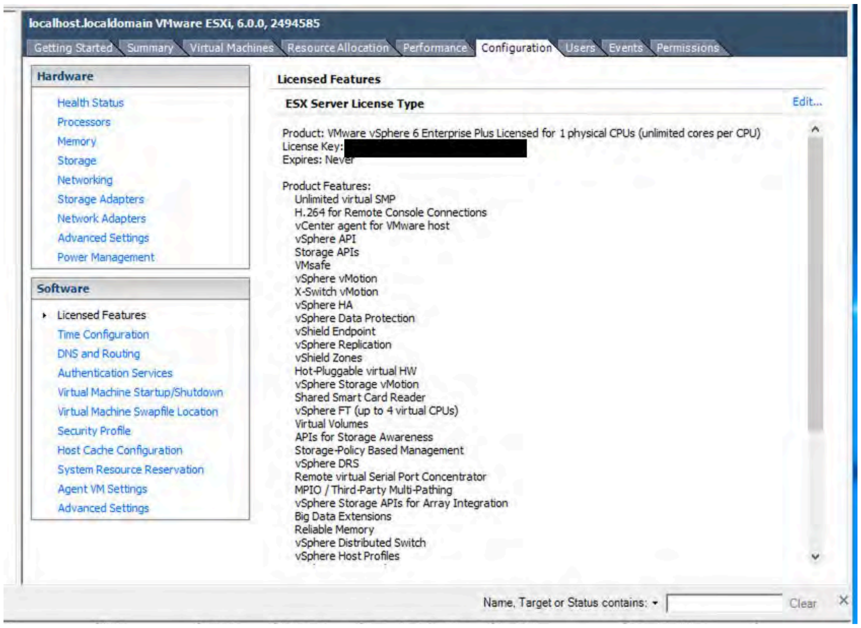
```
[admin@nodegrid /]# cd /settings/devices
[admin@nodegrid devices]# add
[admin@nodegrid {devices}]# set name=Infrabox
[admin@nodegrid {devices}]# set type=infrabox
[admin@nodegrid {devices}]# set ip_address=192.168.10.250
[admin@nodegrid {devices}]# set credential=ask_during_login

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_commmunity=private
[+admin@nodegrid management]# commit
```

Virtual Machines

Nodegrid supports the management of VMWare virtual machines as well a KVM Virtual Machines. The following features for these devices are supported:

- 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

Nodegrid supports direct connections to ESX or VSphere servers. When a connection is made directly, the ESX server has to support the "vCenter agent for VMware Host" feature, which can be enabled through an ESX server license. To check if the ESX server supports this feature, login to the ESX host and navigate to the License Feature section. Here are the available licenses and features listed which are supported by the host:



Licensed Features

ESX Server License Type

Product: VMware vSphere 6 Enterprise Plus Licensed for 1 physical CPUs (unlimited cores per CPU)
License Key: [redacted]
Expires: Never

Product Features:
Unlimited virtual SMP
H.264 for Remote Console Connections
vCenter agent for VMware host
vSphere API
Storage APIs
VMsafe
vSphere vMotion
X-Switch vMotion
vSphere HA
vSphere Data Protection
vShield Endpoint
vSphere Replication
vShield Zones
Hot-Pluggable virtual HW
vSphere Storage vMotion
Shared Smart Card Reader
vSphere FT (up to 4 virtual CPUs)
Virtual Volumes
APIs for Storage Awareness
Storage-Policy Based Management
vSphere DRS
Remote virtual Serial Port Concentrator
MPIO / Third-Party Multi-Pathing
vSphere Storage APIs for Array Integration
Big Data Extensions
Reliable Memory
vSphere Distributed Switch
vSphere Host Profiles

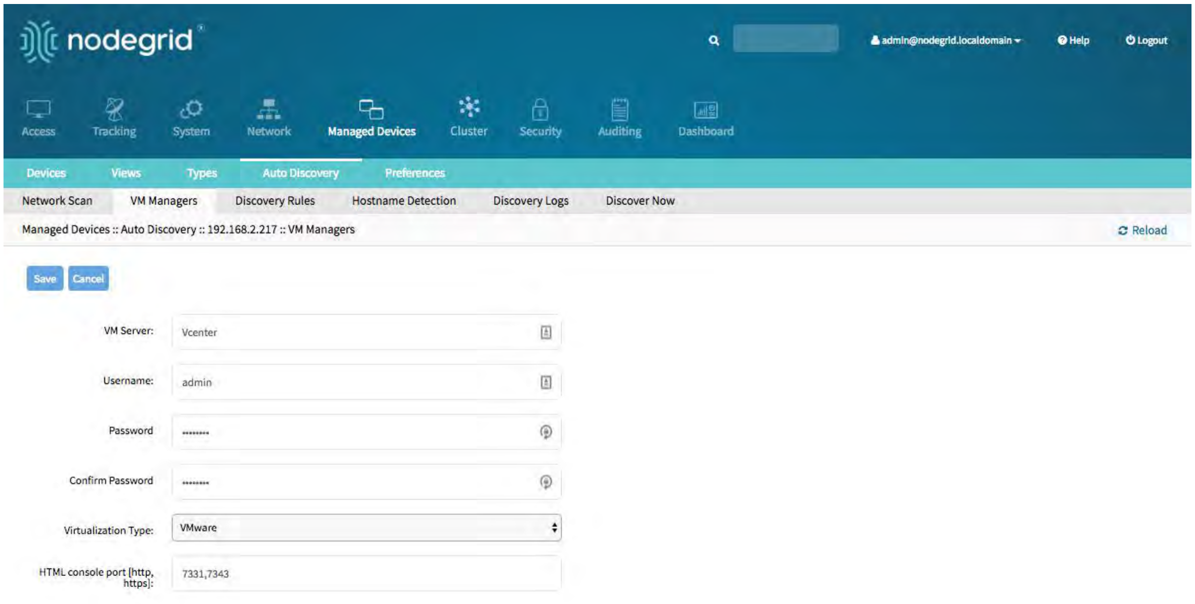
> Note : In order to utilize the vSPC option with VMWare virtual machines the port needs to be configured on the Virtual Machine. See “Configuring Virtual Serial Port (vSPC) on VM Servers” on page 296

Add VMWare Virtual Machines - WebUI

To define a VM Manager:

1. Navigate to `Managed Devices :: Auto Discovery :: VM Managers`
2. Click on `Add` to define a new VM Manager

3. Provide the vCenter/ESXi IP or FQDN in `VM Server` field
4. Define the `Username` and `Password` for the server
5. Adjust the `HTML console port` if needed
6. Click on `Save`



Managed Devices :: Auto Discovery :: 192.168.2.217 :: VM Managers

VM Server: Vcenter

Username: admin

Password ••••••••

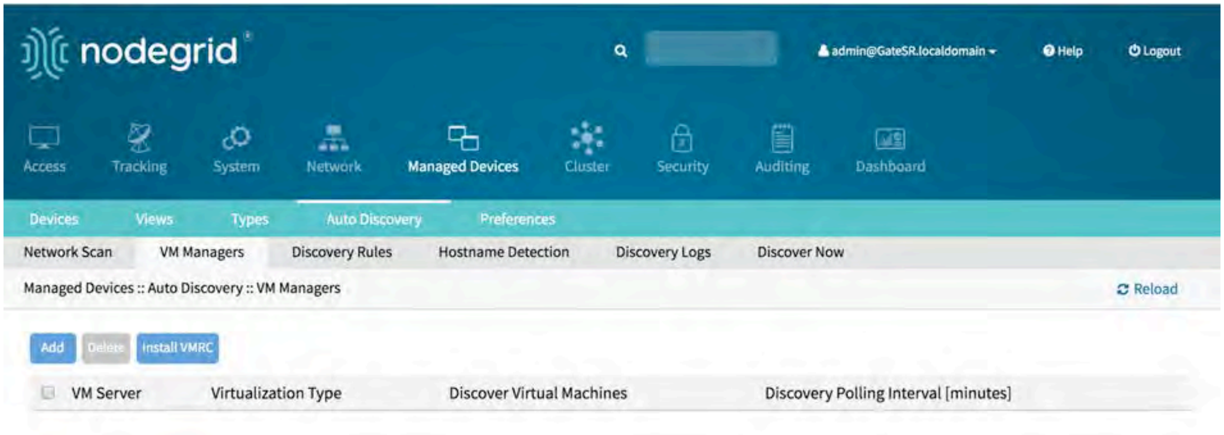
Confirm Password ••••••••

Virtualization Type: VMware

HTML console port [http, https]: 7331,7343

Install VMRC - WebUI

Click on "Install VMRC" (VMware Remote Console) under `Managed Devices::Auto Discovery::VM Managers` to provide properly working graphical device connections and console access to virtual machines.



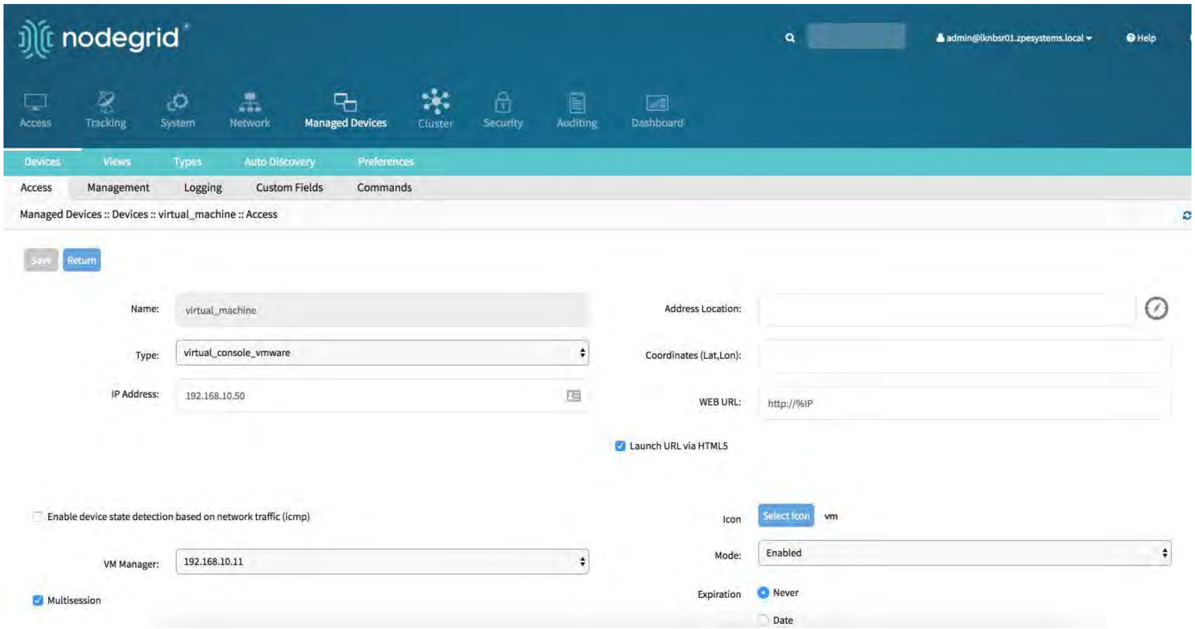
Managed Devices :: Auto Discovery :: VM Managers

☐	VM Server	Virtualization Type	Discover Virtual Machines	Discovery Polling Interval [minutes]

To create a device:

1. Navigate to `Managed Devices:: Devices`

2. Click the `Add` button to add a device to the system.
3. Enter the name of the Virtual Machine to be managed. The name has to match the name on the hypervisor
4. Optional: enter the IP address of the Virtual Machine
5. In the `Type` field, select a type that matches the Virtual Machine type. Possible values are: virtual_console_vmware
6. In `VM Manager` field select the correct hypervisor o which the machine runs
7. Click the Save button.



Managed Devices :: Devices :: virtual_machine :: Access

Name: virtual_machine

Type: virtual_console_vmware

IP Address: 192.168.10.50

Address Location:

Coordinates (Lat,Lon):

WEB URL: http://%IP

☑ Launch URL via HTML5

□ Enable device state detection based on network traffic (icmp)

VM Manager: 192.168.10.11

☑ Multisession

Icon vm

Mode: Enabled

Expiration ● Never ○ Date

Add VMWare Virtual Machines - CLI

To define a VM Manager:

1. Navigate 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` : Provide the 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
```

To create a Device:

1. Navigate 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`, possible values are: virtual_console_vmware
    - optional, `ip_address` as of the target device
    - `vm_manager`, set to a existing VM Manager
4. Save the changes with `commit`

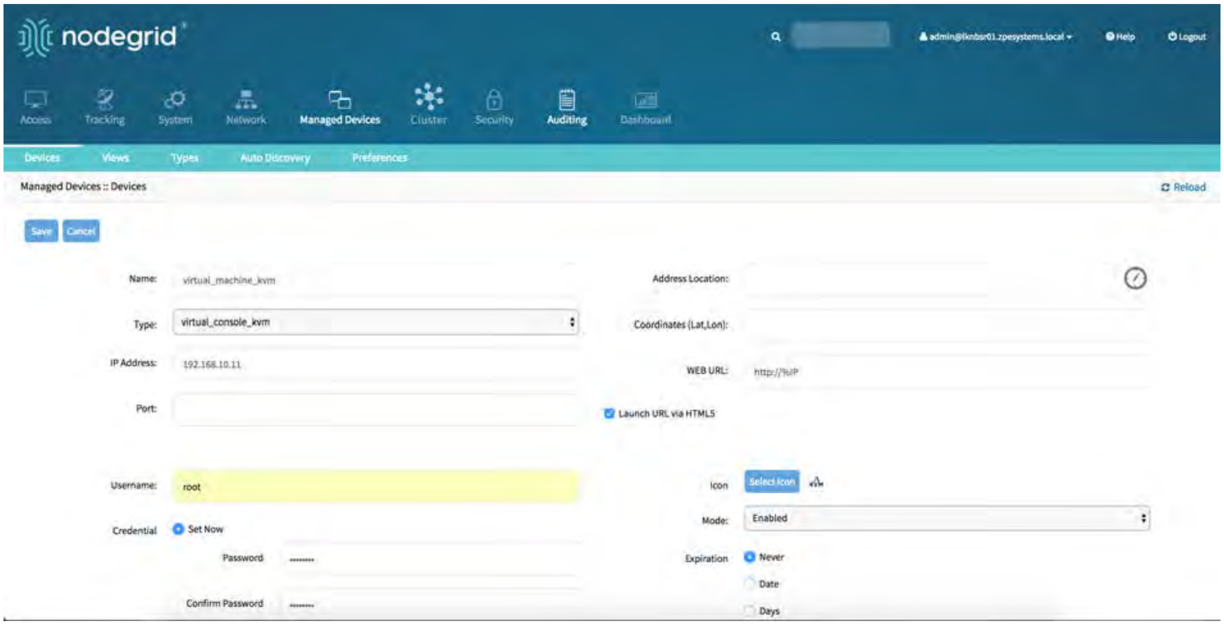
Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings” on page 132

```
[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 Machines - WebUI

To create a Device:

1. Navigate to `Managed Devices:: Devices`
2. Click the `Add` button to add a device to the system.
3. Enter the name of the Virtual Machine to be managed. The name has to match the name on the hypervisor
4. Enter the IP address of the KVM hypervisor
5. Provide the username and password for the KVM hypervisor
6. In the `Type` field, select a type that matches the Virtual Machine type. Possible values are:
    - virtual_console_kvm
7. Click the Save button



Managed Devices :: Devices

Name: virtual_machine_kvm

Type: virtual_console_kvm

IP Address: 192.168.10.11

Port:

Username: root

Credential ● Set Now

Password ········

Confirm Password ········

Address Location:

Coordinates (Lat,Lon):

WEB URL: http://%IP

☑ Launch URL via HTML5

Icon

Mode: Enabled

Expiration ● Never ○ Date ○ Days

Add KVM Virtual Machines - CLI

To create a Device:

1. Navigate to `/settings/devices`
2. Use the `add` command to create a new device
3. Use the `set` command to define the following settings
   - `name` or the virtual machine, this has to match the name of the machine on the hypervisor
   - `type`, possible values are: virtual_console_kvm
   - `ip_address` of the KVM hypervisor
   - provide `username` and `password` for the 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” on page 132

```
[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
```

Nodegrid Devices

USB Sensors

Nodegrid USB Temperature and Humidity Sensors are automatically discovered by the Nodegrid system. The system will automatically Adjust the device type to `usb_sensor`. After the device is detected it needs to be enabled. The device is now ready and can be used for monitoring and alarm management.

KVM Dongle

The USB KVM dongle allows customers to establish a KVM session to a legacy server through VGA and USB connection. The Dongle is automatically detected by the system as soon as it is connected. The device then needs to be enabled.

Bluetooth

The Nodegrid Platform supports Bluetooth devices, primarily 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, so it needs to be manually enabled before it can be used.

The service can be enabled via the shell by an admin user by running the following 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/blue-
tooth/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 and then used for monitoring or exposed to an IoT application.

The `bluetoothctl` command can be used to pair a device:

```
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
```

Auto-Discovery

The Nodegrid Platform is able to automatically discover and add network devices, enabled ports on console servers, KVM switches and Virtual Serial Ports (VMWare) and Virtual Machines (VMWare).

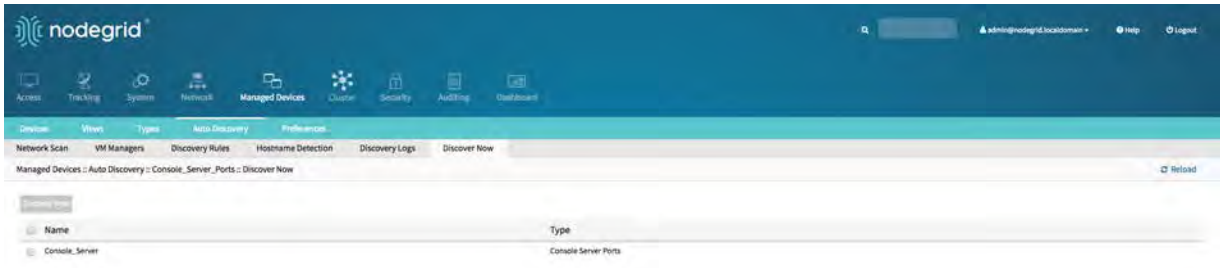
This feature clones discovered devices from existing devices matching their profile and build dynamic access groups. For best results, make sure the device to be used as a reference in the cloning process is correctly configured.

- Verify that username, password and IP address are correct by accessing the device.
- Verify that the data logging and event logging settings are correct by auditing the log files. Verify that events are being detected based on data logging and event logging by simulating events and checking if any notification was created.
- Verify that the device is in the desirable authorization group with correct access rights.

The Auto Discovery follows the general process below:

1. Create a template device. This device will be used to clone all the settings, with the exception of the connection details to the discovered devices. It is beneficial to configure all settings as they should appear on the end devices.

   Note: For each target device type a template device needs to 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 step will link the template device with the discovery rules, which makes the decision which action will be taken with every discovered device
5. Start the discovery process. This step is automatic depending on the added device types. The Discovery Process is automatically started when an appliance is added to the platform and can manually be started at any point from `Managed Devices:: Auto Discovery:: Discover Now` in the WebUI or `/settings/auto_discovery/discover_now/` from CLI



Managed Devices :: Auto Discovery :: Console_Server_Ports :: Discover Now

Name	Type
Console_Server	Console Server Ports

Auto Discovery of Console Server and KVM Switch Ports

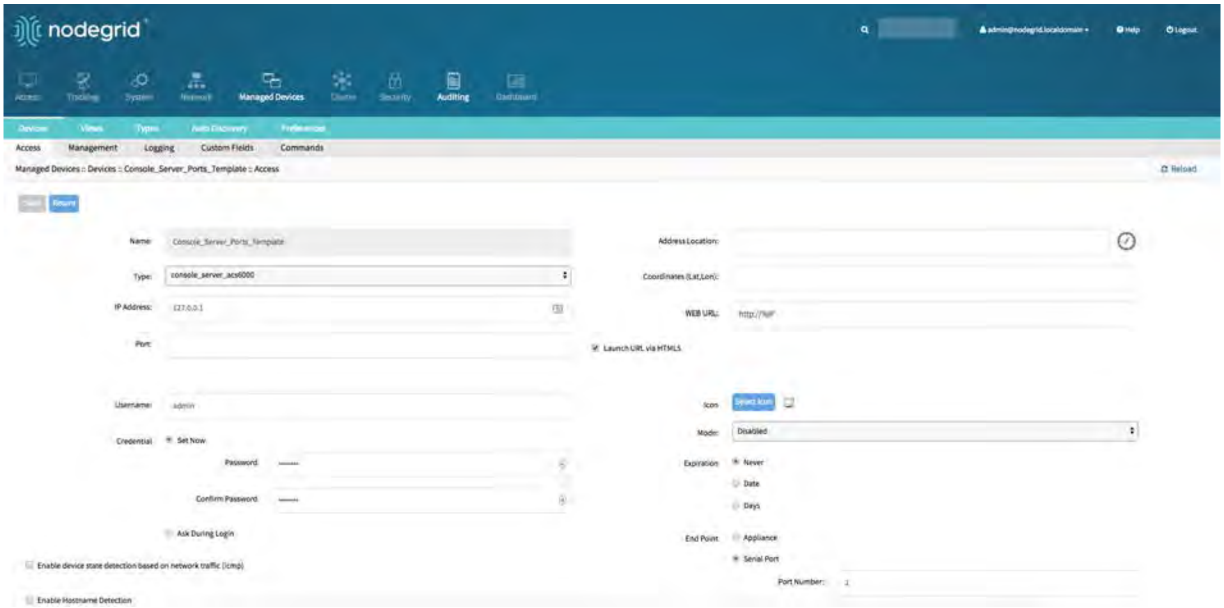
The Auto Discovery process can be used to automatically add and configure managed devices for 3rd party console server ports and KVM Switch ports. The process will discover all enabled ports on a managed appliance. The Console Server appliance and KVM Switches can be discovered using the Network Devices process. See “Auto Discovery of Network Devices” on page 117.

Auto Discovery of Console Server and KVM Switch ports - WebUI

To create a Template Device:

1. Navigate to `Managed Devices:: Devices`
2. Click the `Add` button to add a device to the system.
3. Enter a name of the template you want to add
4. Enter 127.0.0.1 for the IP address
5. In the `Type` field, select a type that matches the console server. Possible values are: console_server_acs, console_server_acs6000,console_server_lantronix,console_-server_opengear,console_server_digicp
6. Select `Ask During Login`
7. Select as `End Point` as either Serial Port or KVM Port and enter the port number
8. Select as `Mode` Disabled, this will ensure that the device is not displayed in the access page
9. Click the Save button.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings” on page 132



Managed Devices :: Devices :: Console_Server_Ports_Template :: Access

Name: Console_Server_Ports_Template

Type: console_server_acs6000

IP Address: 127.0.0.1

Port:

Username: admin

Credential: ● Set Now

Password: ••••••••

Confirm Password: ••••••••

○ Ask During Login

☐ Enable device state detection based on network traffic (icmp)

☐ Enable Hostname Detection

Address Location:

Coordinates (Lat,Lon):

WEB URL: http://%IP

☑ Launch URL via HTML5

Icon:

Mode: Disabled

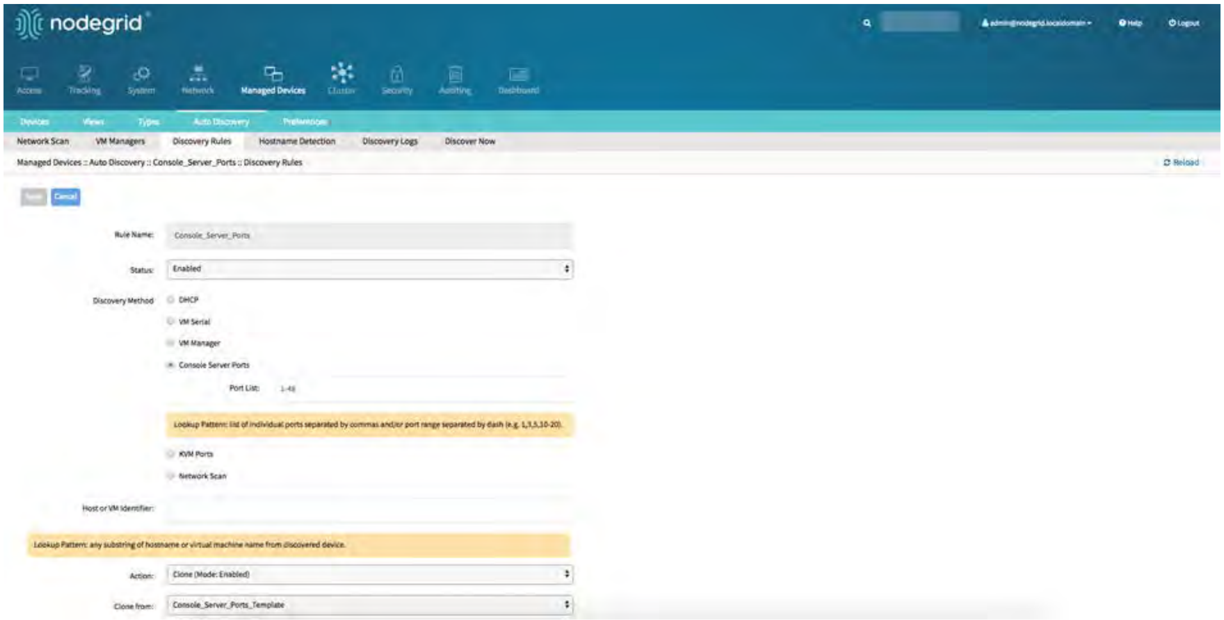
Expiration: ● Never ○ Date ○ Days

End Point: ○ Appliance ● Serial Port

Port Number: 1

To create a Discovery Rule:

1. Navigate to `Managed Devices:: Auto Discovery:: Discovery Rules`
2. Click on `Add` to add a new Discovery Rule
3. Enter a `Name` for the Discovery Rule
4. Select a `Status` for the discovered rule. Possible values are: Enabled, Disabled
5. As `Discovery Method` select either Console Server Ports or KVM Ports
6. For `Port List` provide a list of ports which should be scanned, examples are 1,3,5,10-20
7. The `Host or VM 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
8. For `Action` select an action which should be performed when a new device is discovered, possible values are: Clone (Mode:Enabled),Clone (Mode:On-Demand),Clone (Mode:Discovered),Discard discovered Devices
9. In the `Clone from field` select the template device which was created earlier
10. Click on `Save` to create the rule



Managed Devices :: Auto Discovery :: Console_Server_Ports :: Discovery Rules

Rule Name: Console_Server_Ports

Status: Enabled

Discovery Method
○ DHCP
○ VM Serial
○ VM Manager
● Console Server Ports

Port List: 1-48

Lookup Pattern: list of individual ports separated by commas and/or port range separated by dash (e.g. 1,3,5,10-20).

○ KVM Ports
○ Network Scan

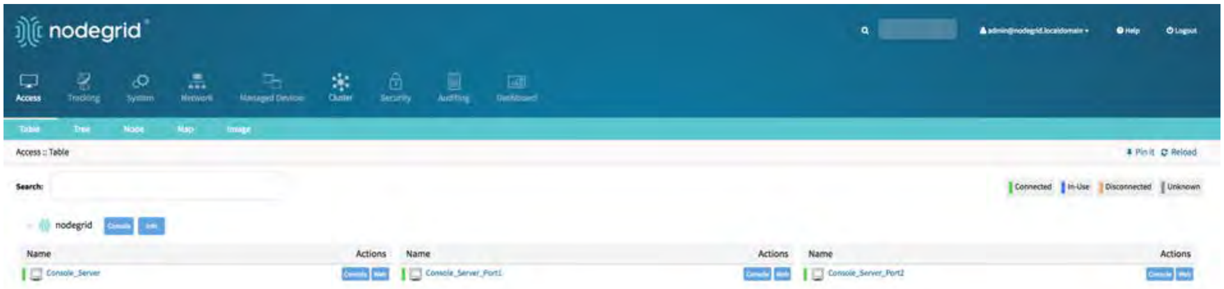
Host or VM Identifier:

Lookup Pattern: any substring of hostname or virtual machine name from discovered device.

Action: Clone (Mode: Enabled)

Clone from: Console_Server_Ports_Template

11. Create a Console Server or KVM Switch appliance (See “Add Console Servers - WebUI” on page 86)
12. After the appliance is created, the Nodegrid Platform will automatically start discovering attached devices based on the created `Discovery Rules`. This process will take a few minutes to complete.



Access :: Table

Search:

nodegrid

Name	Actions	Name	Actions	Name	Actions
Console_Server	Console Web	Console_Server_Port1	Console Web	Console_Server_Port2	Console Web

Auto Discovery of Console Server and KVM Switch ports - CLI

To create a Template Device:

1. Navigate 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`, possible values are: console_server_acs, console_server_acs6000,console_server_lantronix,console_server_opengear,console_server_digicp
    - `ip_address` as 127.0.0.1
    - Set user authentication to `Ask During Login`
    - `endpoint` should be defined as serial_port or kvm_port
    - `port_number` should be defined as the port number
    - 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" on page 132

```
[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
```

To create a Discovery Rule:

1. Navigate 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, possible values are: enabled, disabled
    - `method` set to either console_server_ports or kvm_ports
    - `port_list` provide a list of ports which should be scanned, examples are 1,3,5,10-20
    - `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
4. For `action` select an action which should be performed when a new device is discovered, possible values are: clone_mode_enabled,clone_mode_on-demand,clone_mode_discovered,discard_device
5. `clone_from` set to the template device which was 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 - WebUI” on page 86)
8. After the appliance was created the Nodegrid Platform will automatically start discovering attached devices based on the created `Discovery Rules`. This process will take a few minutes to complete.

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 besides others.

Appliances can be discovered through 3 separate method's, which can be combined or used independently:

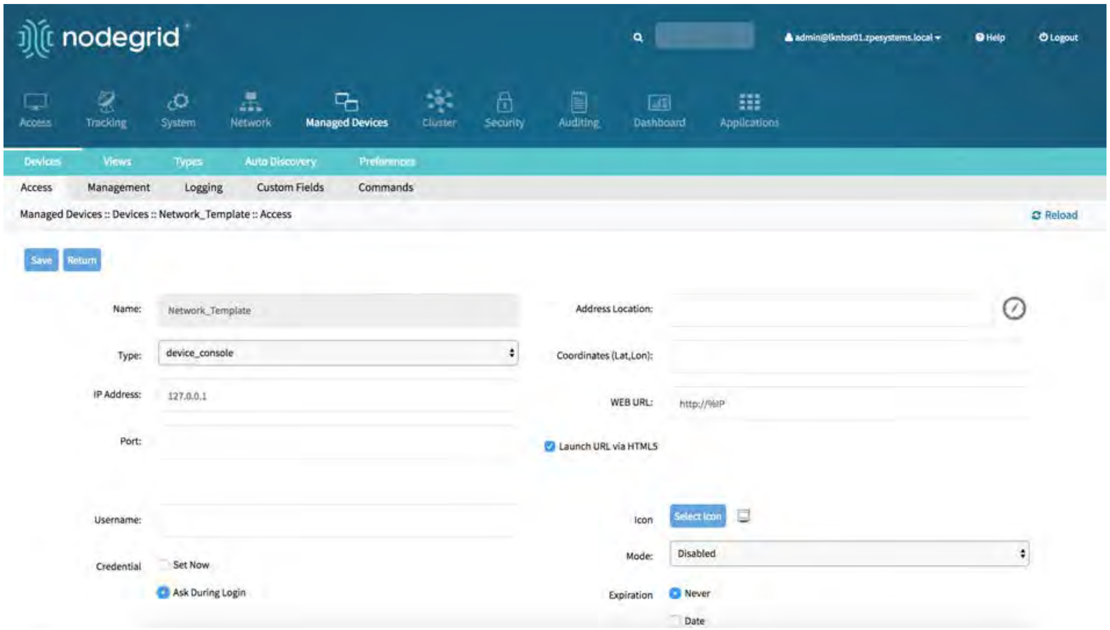
- Similar Devices (select one of the devices from the drop-down menu),
- Port Scan and enter a list of ports in the Port List field,
- Ping

Auto Discovery of Network Devices - WebUI

To create a Template Device:

1. Navigate to `Managed Devices:: Devices`
2. Click the `Add` button to add a device to the system.
3. Enter a name of the template you want to add
4. Enter 127.0.0.1 for the IP address
5. In the `Type` field, select a type that matches the console server. Possible values are: device_console, ilo,imm,drac,idrac6,ipmi1.5,impi2.0,ilom,cimc_ucs,netapp,infrabox,pdu*
6. Enter `username` and `password`, or select `Ask During Login` option if you want to provide user credentials during the login time
7. Select as `Mode` Disabled, this will ensure that the device is not displayed in the access page
8. Click the Save button.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings” on page 132

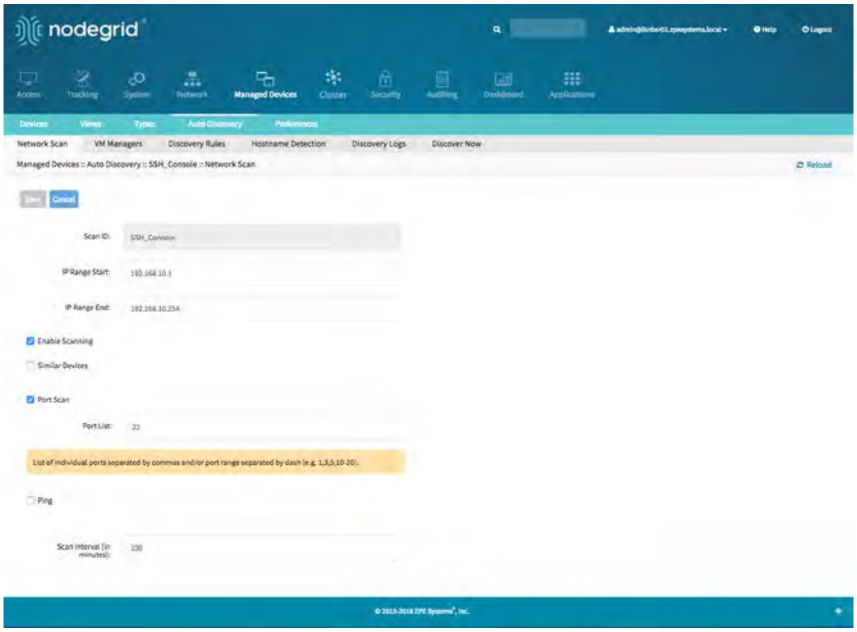


Managed Devices :: Devices :: Network_Template :: Access

Name:	Network_Template
Type:	device_console
IP Address:	127.0.0.1
Port:	
Username:	
Credential	○ Set Now ● Ask During Login
Address Location:	
Coordinates (Lat,Lon):	
WEB URL:	http://%IP
☑ Launch URL via HTML5	
Icon	
Mode:	Disabled
Expiration	● Never ○ Date

To create a Network Scan:

1. Navigate to `Managed Devices:: Auto Discovery:: Network_Scan`
2. Click on `Add` to create a new Network Scan
3. Enter a name for `Scan ID`
4. Define an IP Range to be scanned with `IP Range Start` and `IP Range End`
5. Select and define one or more of the three scan methods:
    - for `Similar Devices` select an existing template which will be used to identify devices
    - for `Port Scan` define a list of ports which should be reachable on the device
    - for `ping` no further settings are required
6. `Enable Scanning` to enable the rule and define a `Scan Interval` which can range in minutes



Managed Devices :: Auto Discovery :: SSH_Console :: Network Scan

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).

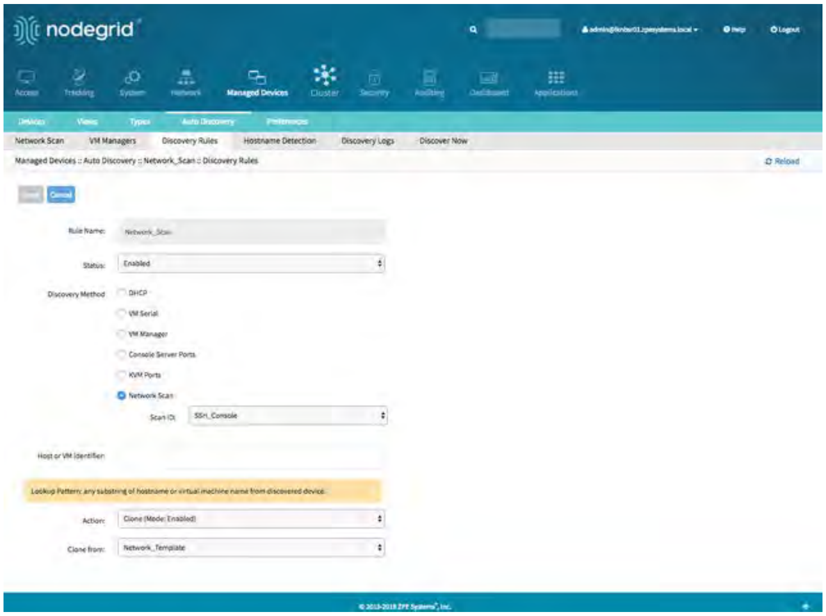
□ Ping

Scan Interval (in minutes): 100

© 2013-2018 ZPE Systems®, Inc.

To create Discovery Rule:

1. Navigate to `Managed Devices:: Auto Discovery:: Discovery Rules`
2. Click on `Add` to add a new Discovery Rule
3. Enter a `Name` for the Discovery Rule
4. Select a `Status` for the discovered rule, possible values are: Enabled, Disabled
5. As `Discovery Method` select Network Scan
6. For `Scan ID` select the Network Scan ID which was created
7. The `Host or VM 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
8. For `Action` select an action which should be performed when a new device is discovered, possible values are: Clone (Mode:Enabled),Clone (Mode:On-Demand),Clone (Mode:Discovered),Discard discovered Devices
9. In the `Clone from field` select the template device which was created earlier
10. Click on `Save` to create the rule



Managed Devices :: Auto Discovery :: Network_Scan :: Discovery Rules

Rule Name: Network_Scan

Status: Enabled

Discovery Method: ○ DHCP ○ VM Serial ○ VM Manager ○ Console Server Ports ○ KVM Ports ● Network Scan

Scan ID: SSH_Console

Host or VM Identifier:

Lookup Pattern: any substring of hostname or virtual machine name from discovered device.

Action: Clone (Mode: Enabled)

Clone from: Network_Template

11. The Nodegrid Platform will automatically start discovering devices based on the created `Discovery Rules`. This process will take a few minutes to complete.

Auto Discovery of Network Devices - CLI

To create a Template Device:

1. Navigate 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`, possible values are: device_console, ilo,imm,drac,idrac6,ipmi1.5,impi2.0,ilom,cimc_ucs,netapp,infrabox,pdu*
   - `ip_address` as 127.0.0.1
   - Set `username` and `password`, or select `Ask During Login` option if you want to provide user credentials during the login time
   - 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” on page 132

```
[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
```

To create a Network Scan:

1. Navigate 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` enter a name for the Network Scan
    - define a Network range which should be scanned with `ip_range_start` and `ip_range_end`
    - Set `enable_scanning` to yes to enable the scan
    - Define one or more of the three scan methods:
        - To use `similar_devices` set `device` to match one of the existing devices or templates
        - To use `port_scan` set `port_list` to a list of ports which should be reachable on the device
        - To use `ping` no further settings are required
4. Set `scan_interval` which can range in minutes

```
[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
```

To create a Discovery Rule:

1. Navigate 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, possible values are: enabled, disabled
    - `method` set to network_scan
    - `scan_id` select a Network Scan ID which was created earlier
    - `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
4. For `action` select an action which should be performed when a new device is discovered, possible values are: clone_mode_enabled,clone_mode_on-demand,clone_mode_discovered,discard_device
5. `clone_from` set to the template device which was 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
```

7. The Nodegrid Platform will automatically start discovering devices based on the created `Discovery Rules`. This process will take 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" on page 296

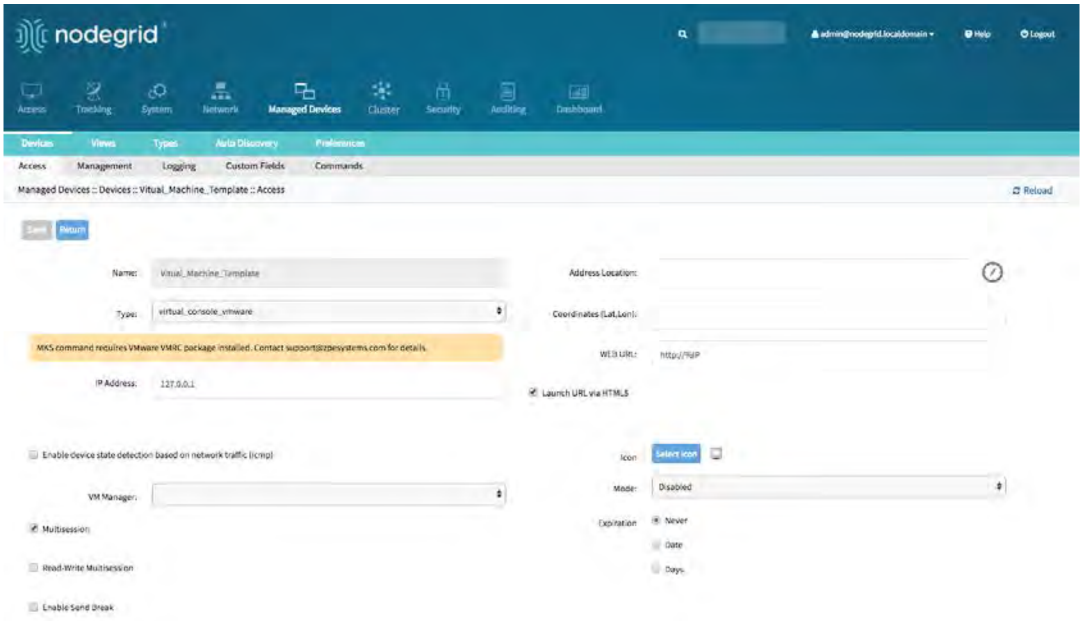
Note: The free version of ESXi is not supported.

Auto Discovery of Virtual Machines - WebUI

To create a Template Device:

1. Navigate to `Managed Devices:: Devices`
2. Click the `Add` button to add a device to the system.
3. Enter a name of the template you want to add
4. Enter 127.0.0.1 for the IP address
5. In the `Type` field, select a type that matches the Virtual Machine type. Possible values are: virtual_console_vmware
6. Enter `username` and `password`, or select `Ask During Login` option if you want to provide user credentials during the login time
7. Select as `Mode` Disabled, this will ensure that the device is not displayed in the access page
8. Click the Save button.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See "Device Settings" on page 132



Managed Devices :: Devices :: Vitual_Machine_Template :: Access

Name: Virtual_Machine_Template

Type: virtual_console_vmware

MKS command requires VMware VMRC package installed. Contact support@zpesystems.com for details.

IP Address: 127.0.0.1

Address Location:

Coordinates (Lat,Lon):

WEB URL: http://%IP

☑ Launch URL via HTML5

□ Enable device state detection based on network traffic (icmp)

VM Manager:

☑ Multisession

□ Read-Write Multisession

□ Enable Send Break

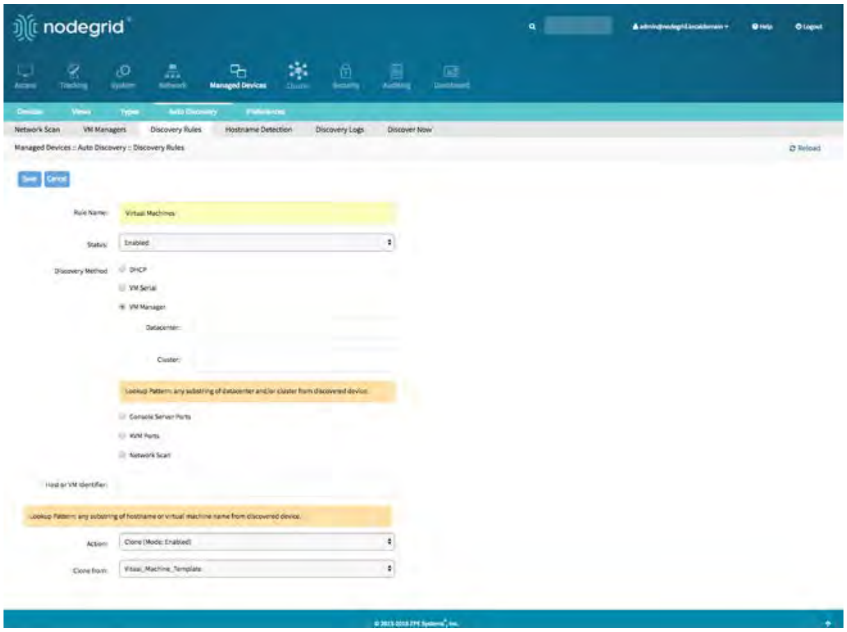
Icon

Mode: Disabled

Expiration ● Never ○ Date ○ Days

To create a Discovery Rule:

1. Navigate to `Managed Devices:: Auto Discovery:: Discovery Rules`
2. Click on `Add` to add a new Discovery Rule
3. Enter a `Name` for the Discovery Rule
4. Select a `Status` for the discovered rule, possible values are: Enabled, Disabled
5. As `Discovery Method` select VM Manager
6. Optional use the fields `Datacenter` and `Cluster` to filter the scan to these specific entries
7. The `Host or VM 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
8. For `Action` select an action which should be performed when a new device is discovered, possible values are: Clone (Mode:Enabled),Clone (Mode:On-Demand),Clone (Mode:Discovered),Discard discovered Devices
9. In the `Clone from field` select the template device which was created earlier
10. Click on `Save` to create the rule



Managed Devices :: Auto Discovery :: Discovery Rules

Rule Name: Virtual Machines

Status: Enabled

Discovery Method: ○ DHCP ○ VM Serial ● VM Manager

Datacenter:

Cluster:

Lookup Pattern: any substring of datacenter and/or cluster from discovered device.

○ Console Server Ports
○ KVM Ports
○ Network Scan

Host or VM Identifier:

Lookup Pattern: any substring of hostname or virtual machine name from discovered device.

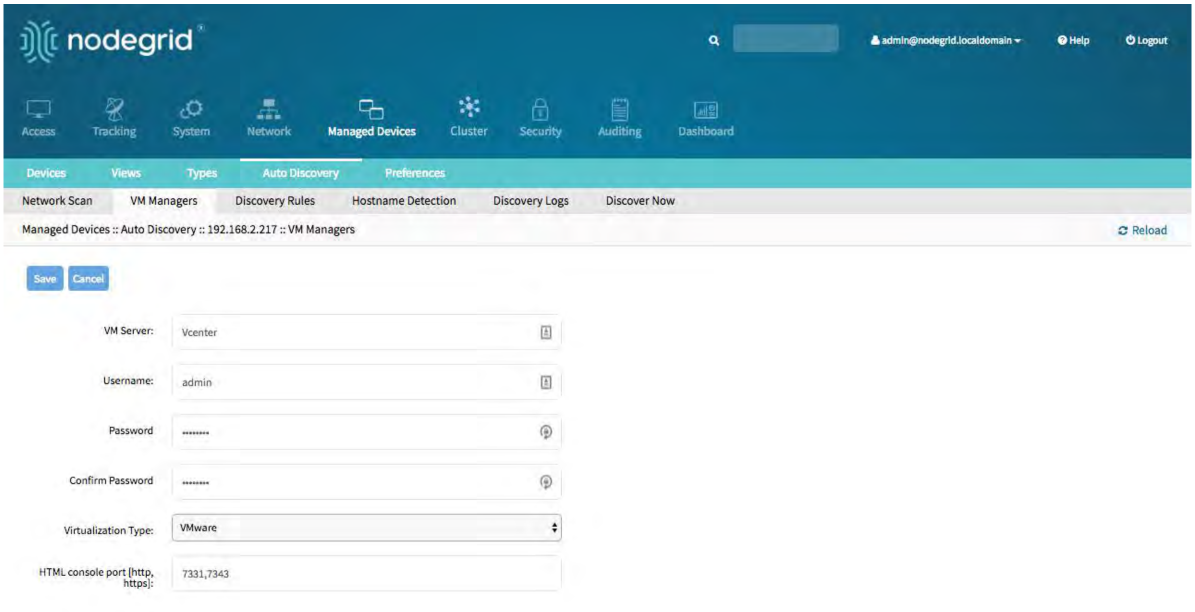
Action: Clone (Mode: Enabled)

Clone from: Vitual_Machine_Template

© 2013-2018 ZPE Systems®, Inc.

To define a VM Manager:

1. Navigate to `Managed Devices :: Auto Discovery :: VM Managers`
2. Click on `Add` to define a new VM Manager
3. Provide the vCenter/ESXi IP or FQDN in `VM Server` field
4. Define the `Username` and `Password` for the server
5. Adjust the `HTML console port` if needed
6. Click on `Save`

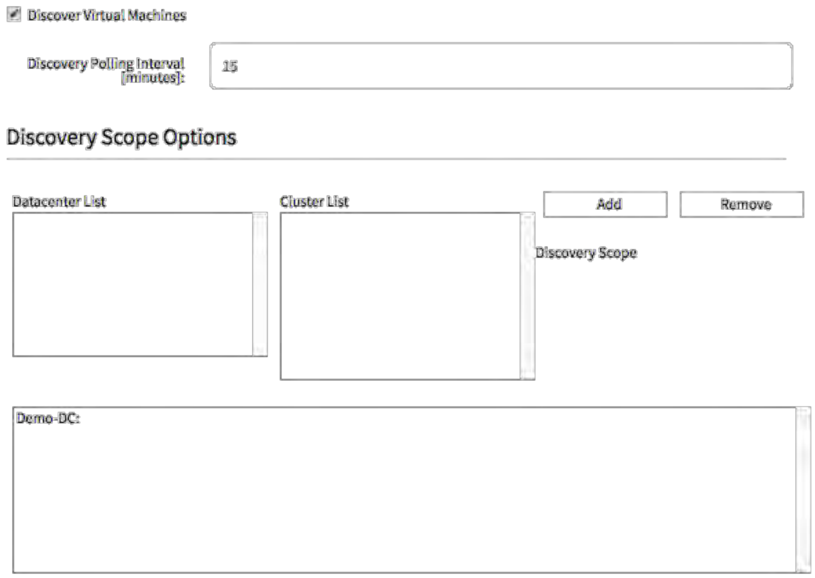


Managed Devices :: Auto Discovery :: 192.168.2.217 :: VM Managers

VM Server:	Vcenter
Username:	admin
Password	••••••••
Confirm Password	••••••••
Virtualization Type:	VMware
HTML console port [http, https]:	7331,7343

To enable Discover Virtual Machines:

1. Nodegrid platform will connect now to the vCenter or ESXi system, this can take a few minutes
2. Click on the newly created and connected `VM Manager`
3. Enable `Discover Virtual Machines` option to configure the Virtual Machine discovery option, define as a minimum a `Data Center` and `Discovery Polling Interval`.
4. Click on `Save`



☑ Discover Virtual Machines

Discovery Polling Interval [minutes]: 15

Discovery Scope Options

Auto Discovery of Virtual Machines - CLI

To create Template Device:

1. Navigate 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`, possible values are: 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” on page 132

```
[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
```

To create a Discovery Rule:

1. Navigate 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, possible values are: enabled, disabled
    - `method` set to vm_manager
    - Use `datacenter` and `cluster` to define filters based on Data Center and or Cluster
    - `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
4. For `action` select an action which should be performed when a new device is discovered, possible values are: clone_mode_enabled,clone_mode_on-demand,clone_mode_discovered,discard_device
5. `clone_from` set to the template device which was 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=Vitual_Machine_Template
[admin@nodegrid {discovery_rules}]# commit
```

To define a VM Manager:

1. Navigate 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` : Provide the 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
```

To enable Discover Virtual Machines:

1. Nodegrid platform will connect now to the vCenter or ESXi system, this can take a few minutes
2. Click on the newly created `VM Manager`
3. Enable `Discover Virtual Machines` option to configure the Virtual Machine discovery option, define as a minimum a `Data Center` and `Discovery Polling Interval`.
4. Click on `Save`

```
[admin@nodegrid 192.168.2.217]# show
vm server: 192.168.2.217
username = Administrator@zpesystems.com
password = ********
type = VMware
html_console_port = 7331,7343
discover_virtual_machines = yes
interval_in_minutes = 15
discovery_scope =  Demo-DC!
```

Auto Discovery of DHCP Clients

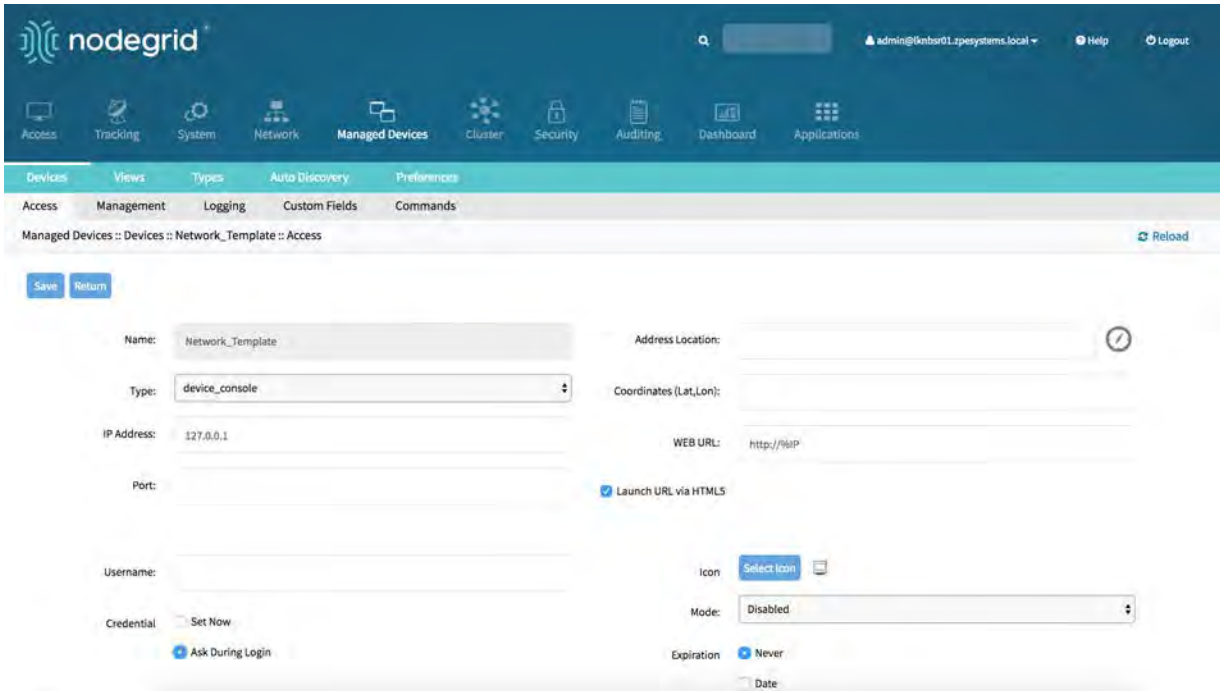
The Nodegrid Platform can be used as a DHCP Server for Clients within the management network. These devices can be automatically discovered and added to the Nodegrid platform. This feature only supports DHCP Clients which receive their DHCP lease from the local Nodegrid platform. See “DHCP Server” on page 210 for details on how to setup the DHCP Server feature.

Auto Discovery of DHCP Clients - Web UI

To create a Template Device:

1. Navigate to `Managed Devices:: Devices`
2. Click the `Add` button to add a device to the system.
3. Enter a name of the template you want to add
4. Enter 127.0.0.1 for the IP address
5. In the `Type` field, select a type that matches desired device type.
6. Enter `username` and `password`, or select `Ask During Login` option if you want to provide user credentials during the login time
7. Select as `Mode` Disabled, this will ensure that the device is not displayed in the access page
8. Click the Save button.

Optional: Settings which control the display and behavior of the device can be adjusted at this time. See “Device Settings” on page 132



Managed Devices :: Devices :: Network_Template :: Access

Name: Network_Template

Type: device_console

IP Address: 127.0.0.1

Port:

Username:

Credential ○ Set Now ● Ask During Login

Address Location:

Coordinates (Lat,Lon):

WEB URL: http://%IP

☑ Launch URL via HTML5

Icon

Mode: Disabled

Expiration ● Never ○ Date

To create a Discovery Rule:

1. Navigate to `Managed Devices:: Auto Discovery:: Discovery Rules`
2. Click on `Add` to add a new Discovery Rule
3. Enter a `Name` for the Discovery Rule
4. Select a `Status` for the discovered rule, possible values are: Enabled, Disabled
5. As `Discovery Method` select DHCP
6. Optional use the field `MAC Address` to filter to these specific entries
7. The `Host or VM 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
8. For `Action` select an action which should be performed when a new device is discovered, possible values are: Clone (Mode:Enabled),Clone (Mode:On-Demand),Clone (Mode:Discovered),Discard discovered Devices
9. In the `Clone from field` select the template device which was created earlier
10. Click on `Save` to create the rule

After the rule is created the device be automatically added to the system as soon as it receives a DHCP address or renews its DHCP address lease. The default value for the address lease renewal is every 10min.

Auto Discovery of DHCP Clients - CLI

To create a Template Device:

1. Navigate 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`, possible values are: device_console, ilo,imm,drac,idrac6,ipmi1.5,impi2.0,ilom,cimc_ucs,netapp,infrabox,pdu*
   - `ip_address` as 127.0.0.1
   - Set `username` and `password`, or select `Ask During Login` option if you want to provide user credentials during the login time
   - 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” on page 132

```
[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
```

To create a Discovery Rule:

1. Navigate 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, possible values are: 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
4. For `action` select an action which should be performed when a new device is discovered, possible values are: clone_mode_enabled,clone_mode_on-demand,clone_mode_discovered,discard_device
5. `clone_from` set to the template device which was 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=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
```

Device Settings

Most devices support additional configuration options and settings. This section will explain these settings and how they can be configured.

Hostname Detection

This feature allows the automatic discovery of a target devices hostnames (network or serial), based on its login prompt, prompt, or banner.

By default, Nodegrid already has some probes and matches for most of the following devices types: PDUs, NetApp, Console Servers, Device Consoles, and Service Processors.

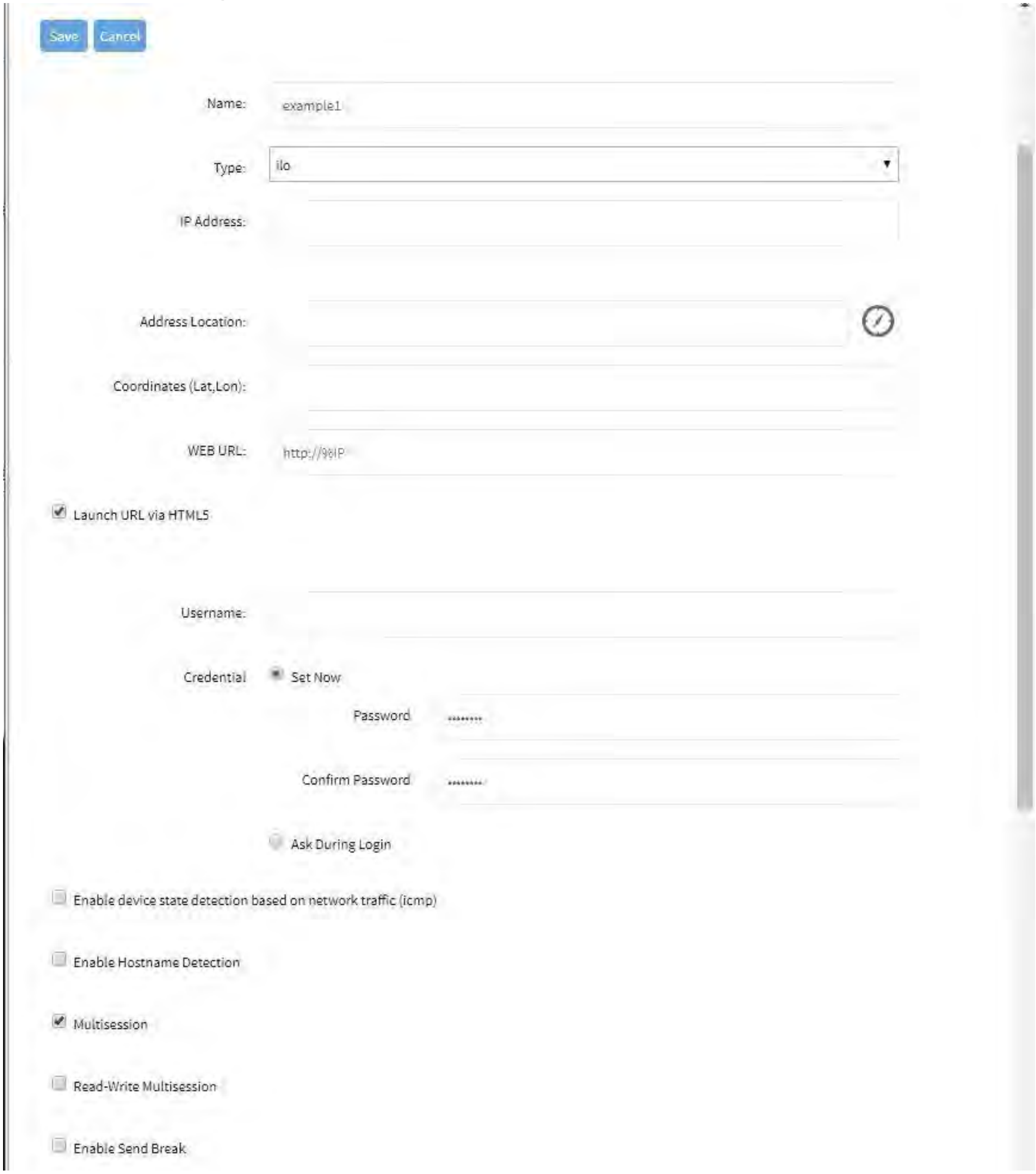
Nodegrid will send the first probe and wait for a match. If there is no match, it will send the second probe, and so on. Once there is a match, the probing stops for that device.

Configure Hostname Detection

In most cases the only configuration required is to enable the feature on the target device. For this, navigate to the desired device in the `Managed Devices` (WebUI) or `settings/devices/` (CLI) section to enable the feature.

WebUI

1. Navigate to `Managed Devices:: Devices`
2. Click on the Target Device to access its settings
3. Tick the box beside `Enable Hostname Detection`
4. Save the settings



Name: example1

Type: ilo

IP Address:

Address Location:

Coordinates (Lat,Lon):

WEB URL: http://%IP

☑ 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

CLI

1. Navigate to `/settings/devices/<Device Name>/access`
2. Set `enable_hostname_detection` to yes
3. Commit the changes

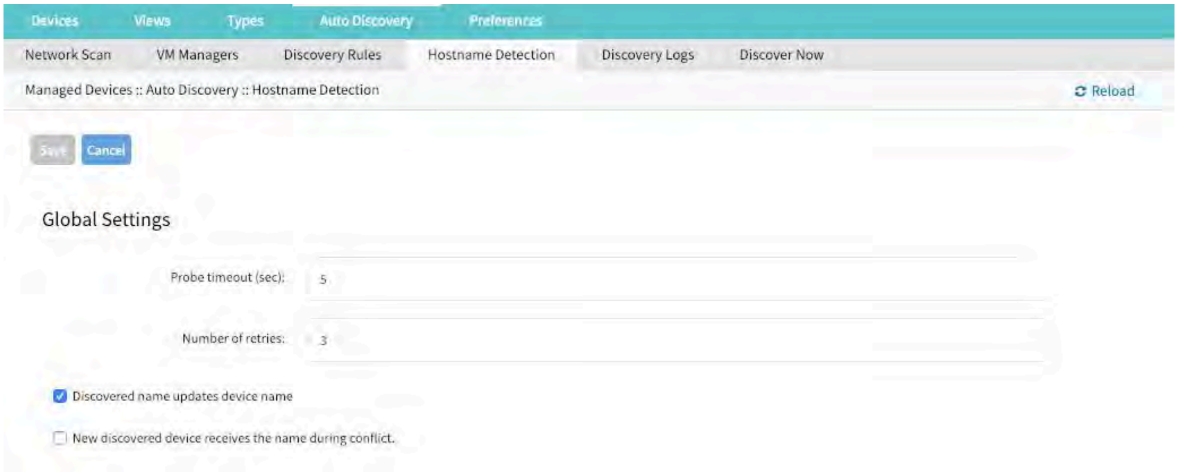
```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/access/
[admin@nodegrid /]# set enable_hostname_detection=yes
[+admin@nodegrid /]# commit
```

Global Settings for Hostname Detection

To enable the feature for each target device the following settings can be adjusted under `Managed Devices:Auto Discovery:Hostname Detection` (WebUI) or `/settings/auto_discovery/hostname_detection` (CLI)

- **Probe timeout**: Timeout in seconds which the Nodegrid will wait for output after the probe was sent
- **Number of retries**: The number of times the probes will be resent to the device if no output was available
- **Discovered name updates device name**: This setting is enabled by default, by disabling it no devices names will be updated even if a match was found.
- **New discovered device receives the name during conflict**: This option can be enabled. In case multiple devices have the same name then the latest device discovered with this name will receive the name.
- **Probe**: String (Text) combinations of characters send to the device. The output is then matched against the existing Match Strings. Existing probes can be adjusted or new probes created.
- **Match**: RegEx expressions, which are matched against the probe's output. In case a match is found the hostname will be extracted and the device name updated. Existing matches can be adjusted and new matches created.

General Settings



Global Settings

Probe timeout (sec): 5

Number of retries: 3

☑ Discovered name updates device name

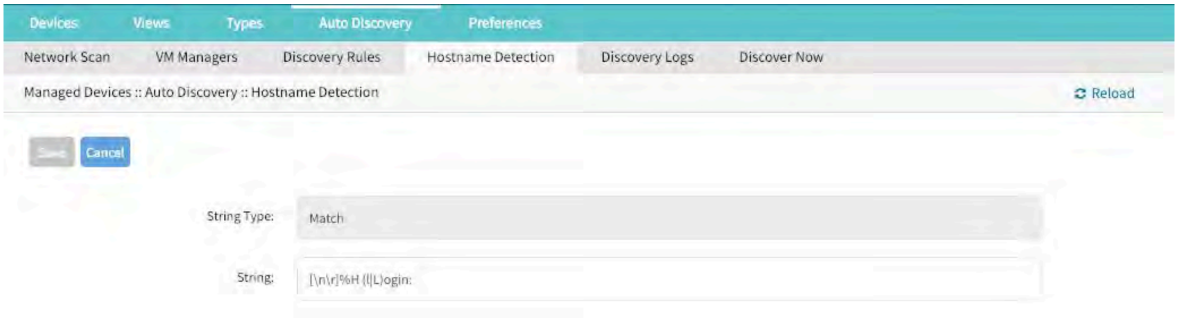
☐ New discovered device receives the name during conflict.

Create a Probe or Match

WebUI

1. Navigate to `Managed Devices:Auto Discovery:Hostname Detection`
2. Click on Add
3. Select a value from `String Type`
4. Provide a String which will be the Match or Probe.

   Note: For Matches RegEx expressions are allowed. Use the variable `%H` to indicate the location of the hostname



String Type: Match

String: [\n\r]%H (l|L)ogin:

CLI

1. Navigate to `/settings/auto_discovery/hostname_detection/string_settings`
2. Type `add`
3. Use the `set` command to define `string_type` as either match or probe
4. Use the `set` command to define a probe or match string
5. Active and save the change with`commit`

   Note: For Matches RegEx expressions are allowed. Use the variable `%H` to indicate the location of the hostname

Multi Sessions

`Multisessions` allow multiple users to access the same device at the same time. All users will be able to see the same output. By default, the first user has read-write access and all other users only have read access to the session. By enabling the option `Read-Write Multisession`, this behavior be changed so that all connected users have read-write access to the session. In this case, only one user at a time has write access so the system automatically switches to the first user who is trying to enter keystrokes.

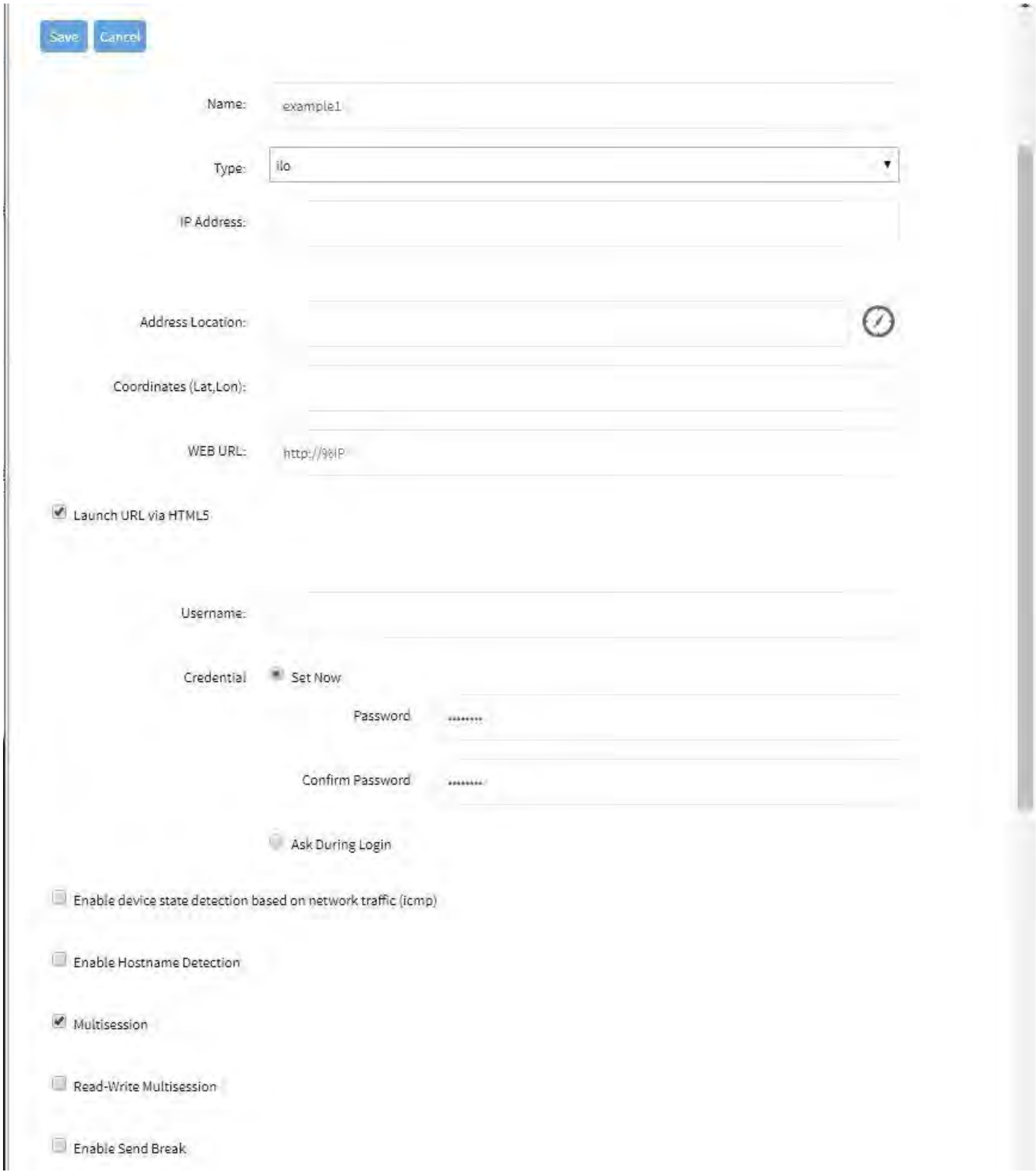
It is possible to see all connected users during a session via the console session menu (see “Break Signal” on page 138). This feature is available for device console sessions.

WebUI

1. Navigate to `Managed Devices:: Devices`
2. Click on the Target Device to access its settings
3. Tick the box beside `Multisessions`

Optional: Tick the box beside `Read-Write Multisession`

4. Save the settings



Name: example1

Type: ilo

IP Address:

Address Location:

Coordinates (Lat,Lon):

WEB URL: http://%IP

☑ 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

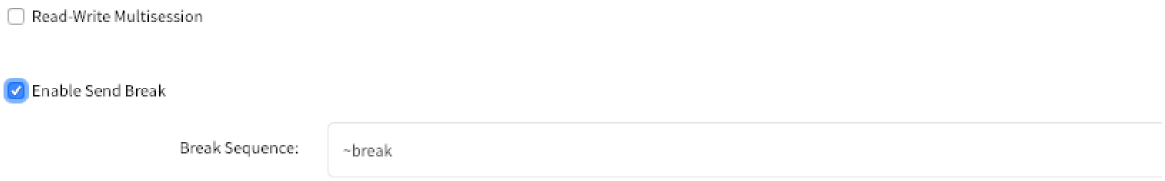
CLI

1. Navigate to `/settings/devices/<Device Name>/access`
2. Set `multisession` to yes
3. Optional: set `write_multisession` to yes
4. `commit` the changes

```
[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

This option allows users to send a break signal via the ssh console session. The function can be enabled on a per-device basis. The break sequence can also be configured.



□ Read-Write Multisession

☑ Enable Send Break

Break Sequence: ~break

WebUI

1. Navigate to `Managed Devices:: Devices`
2. Click on the Target Device to access its settings
3. Tick the box beside `Enable Send Break`
4. Adjust the `Break Sequence` as needed

CLI

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

```
[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 escape from the current session and bring up a menu, or to directly perform specific tasks like bring up the power menu.

The Nodegrid supports two escape sequences. One for the normal session menu and a second for the power menu which allows for direct power control of a target device. See "Power Menu Preferences" on page 163

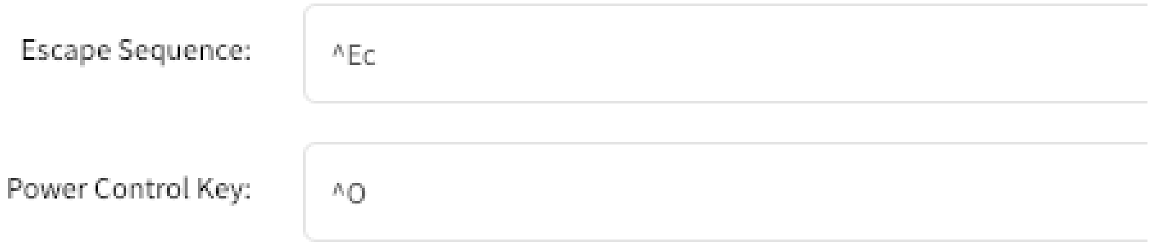
Both escape sequences are preset with a default value which can be changed if needed.

Table 39: Escape Sequences

ITEM	DEFAULT SEQUENCE	KEY COMBINATION
Escape Sequence	^Ec	CTRL+SHIFT+E c
Power Control Key	^O	CTRL+SHIFT+O

WebUI

1. Navigate to `Managed Devices:: Devices`
2. Click on the Target Device to access its settings
3. Adjust the `Escape Sequence` or `Power Control Key` as needed



Escape Sequence: ^Ec

Power Control Key: ^O

CLI

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

```
[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, when accessing a target device, the user has to authenticate first against the Nodegrid unit and is then connected through to the device. If this is not required then this features allows you to disable Nodegrid authentication for specific devices.

Note: This will disable any Nodegrid authentication method for this device. Ensure that appropriate authentication mechanism are setup on the target device.

WebUI

1. Navigate to `Managed Devices:: Devices`
2. Click on the Target Device to access its settings
3. Tick the box beside `Skip authentication to access device (NONE authentication)`
4. CLI
5. Navigate to `/settings/devices/<Device Name>/access`
6. Set the `skip_authentication_to_access_device` to yes to disable authentication
7. `commit` the changes

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

SSH / Telnet Port

These features allow administrators to define a specific ssh or telnet port for target devices.

By default, each target device has a unique telnet port assign which uses port 7000 as a base port plus the port number. For ssh connections, the default port will be used for all connections.

SSH and Telnet ports can be adjusted as needed.

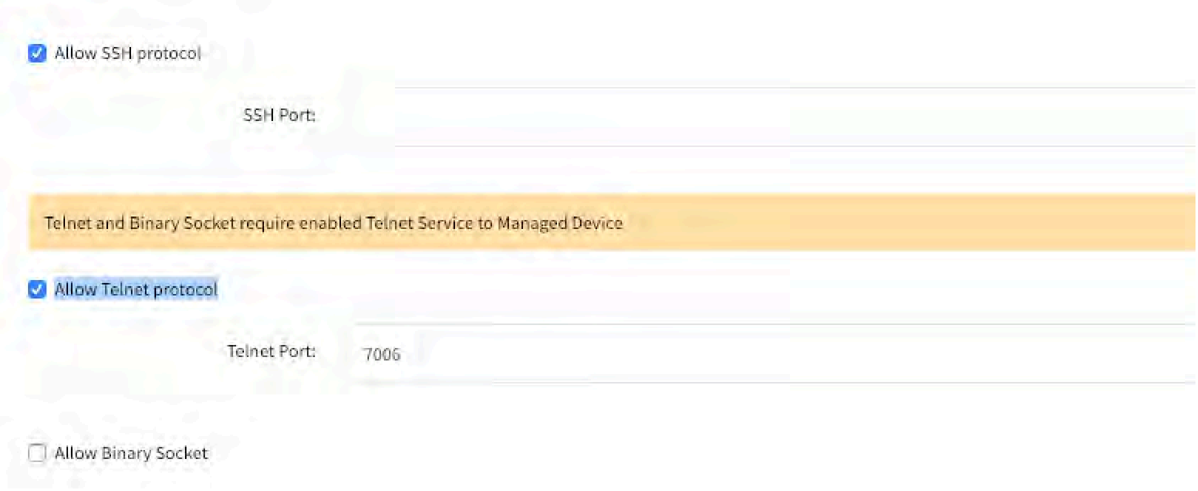
Note: SSHv1 is deprecated. We only support SSHv2 now.

WebUI

1. Navigate to `Managed Devices:: Devices`
2. Click on the Target Device to access its settings
3. Tick the box beside `Allow SSH protocol` or `Allow Telnet protocol`.

   Note: Both options are enabled by default.

4. Provide or adjust the port number as needed



☑ Allow SSH protocol

SSH Port:

Telnet and Binary Socket require enabled Telnet Service to Managed Device

☑ Allow Telnet protocol

Telnet Port: 7006

□ Allow Binary Socket

CLI - SSH

1. Navigate 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. `commit` the changes

CLI - Telnet

1. Navigate 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. `commit` the changes

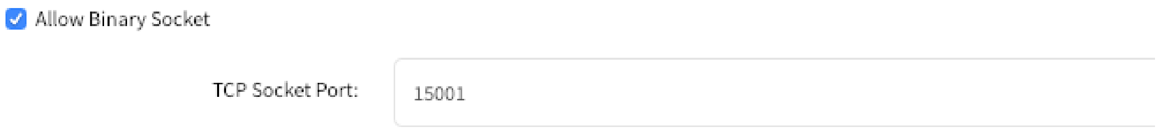
```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/access/
[admin@nodegrid /]# set allow_ssh_protocol=yes
[+admin@nodegrid access]#set ssh_port=17001
[+admin@nodegrid access]#set allow_telnet_protocol=yes
[+admin@nodegrid access]#set telnet_port=7001
[+admin@nodegrid access]#commit
```

Binary Socket

The Binary Socket Feature allows 3rd party systems to directly access the device as if it would be physically connected. Signals will be transmitted directly and will not be encapsulated in the telnet or ssh protocol. A specific port needs to be assigned.

WebUI

1. Navigate to `Managed Devices:: Devices`
2. Click on the Target Device to access its settings
3. Tick the box beside `Allow Binary Socket`
4. Provide or adjust the port number as needed



☑ Allow Binary Socket

TCP Socket Port: 15001

CLI

1. Navigate 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. `commit` the changes

```
[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 or directly through a ssh/telnet client. In case an ssh client is used, the default method to access a specific target device is to pass the target device name through as a parameter.

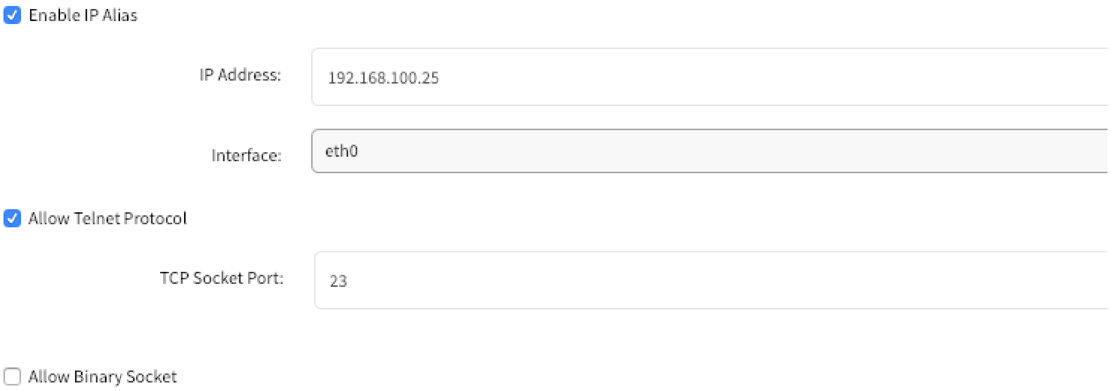
Port Aliases allow users to connect to a target device by using an IP Addresses. Each IP Alias supports the definition of a telnet and binary port as desired.

The Nodegrid solution supports the allocation of up to 2 IP address alias for each target device. The feature supports IPv4 as well as IPv6 Addresses.

WebUI

1. Navigate to `Managed Devices:: Devices`
2. Click on the Target Device to access its settings

3. Tick the box beside `Enable IP Alias`
    - Provide a valid IP address
    - Select a valid network interface through which the IP address will be accessible.
    - `Allow the Telnet` protocol for the interface if desired
        - Adjust the port if desired
    - `Allow Binary Socket` for direct access if desired
    - Adjust the port if desired
4. Repeat these steps for `Enable Second IP Alias`



☑ Enable IP Alias

IP Address: 192.168.100.25

Interface: eth0

☑ Allow Telnet Protocol

TCP Socket Port: 23

□ Allow Binary Socket

CLI

1. Navigate 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 as required
    - ip_alias - IP address
    - Interface - Network interface to be 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. `commit` the changes

```
[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
```

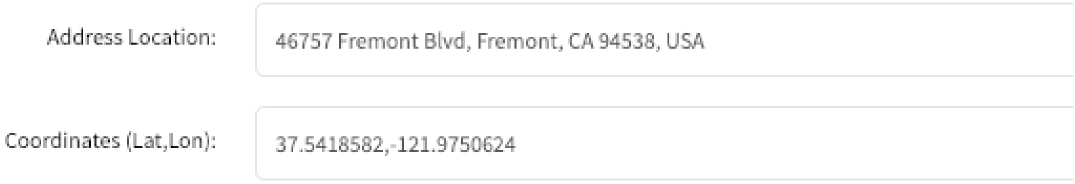
Location

Each Device can be associated with a location. The location details are used to display the device and its status on the map view.

The location can be defined through address details or directly through Longitude and Latitude values. In case the location values are provided through an address, the unit does require a Internet connection for the translation into longitude and latitude.

WebUI

1. Navigate to `Managed Devices:: Devices`
2. Click on the Target Device to access its settings
3. Provide a address in the `Address Location` field and press the locater icon to the right to identify the latitude and longitude coordinates.
4. Alternatively directly provide valid latitude and longitude coordinates



Address Location: 46757 Fremont Blvd, Fremont, CA 94538, USA

Coordinates (Lat,Lon): 37.5418582,-121.9750624

CLI

1. Navigate to `/settings/devices/<Device Name>/access`
2. Use the `set` command to provide valid latitude and longitude coordinates
3. Alternatively, provide an address

```
[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 function to look up a address and convert it to valid latitude and longitude coordinates.

Web URL

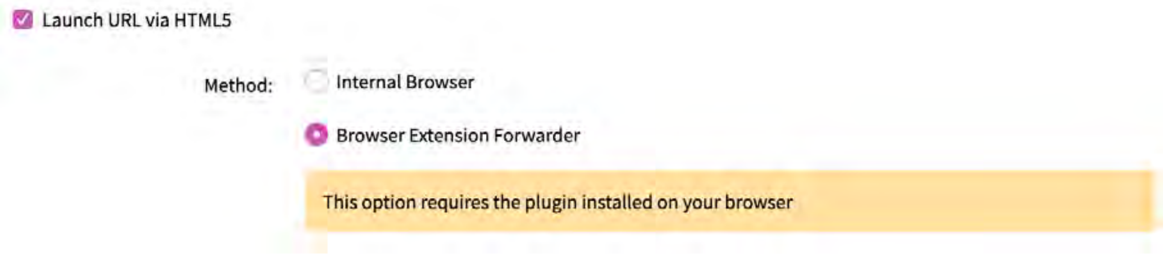
A Web URL can be defined for each device. The URL will be used for the `Web` command which is available for each device by default.

The default URL defined for all IP based sessions is `http://%IP` where `%IP` will be replaced by the IP Address values defined for each device. By default, the URL will be opened inside an HTML5 frame which is forwarded to the client. This allows passing through unsecured device web interfaces without exposing the devices to the network.

This can be controlled by disabling the feature `Launch URL via HTML5`

Another option would be to launch the URL via Forwarder. This option reduces resource usage by redirecting to a web server and offers the same behavior as the HTML5 frame. This option also allows you to view the device's interface in full-screen mode as apposed to a windowed frame.

This can be enabled by checking the Launch URL via Forwarder check box.



☑ Launch URL via HTML5

Method: ○ Internal Browser

● Browser Extension Forwarder

This option requires the plugin installed on your browser

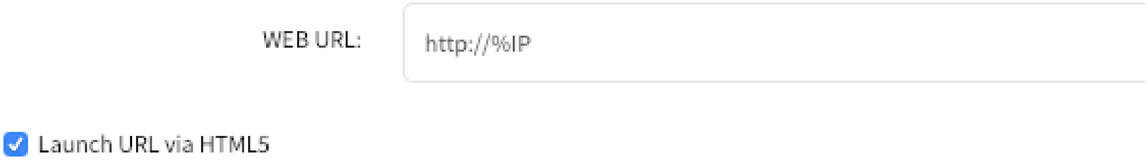
Note: The required extension must be installed on the client's browser for the Forwarder option to work.

To install the extension for Google Chrome:

1. Open Google Chrome and go to https://chrome.google.com/webstore/detail/nodegrid-web-access-exten/cmcpkbfnablakhllgdmbhkedpoengpik
2. Click on “Add to Chrome”
3. The extension is now installed and ready to use

WebUI

1. Navigate to `Managed Devices:: Devices`
2. Click on the Target Device to access its settings
3. Adjust the `WEB URL` value as needed
4. Enable or Disable the launch of the URL in HTML5 window as needed by setting `Launch URL via HTML5`



WEB URL: http://%IP

☑ Launch URL via HTML5

CLI

1. Navigate 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 HTM5 window by setting `launch_url_via_html5`

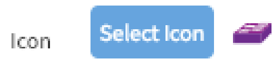
```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/access/
[admin@nodegrid /]#set web_url="https://%IP"
[+admin@nodegrid access]#set launch_url_via_html5=yes
[+admin@nodegrid access]#commit
```

Icon

For each device an icon can be defined to represent its device type.

WebUI

1. Navigate to `Managed Devices:: Devices`
2. Click on the Target Device to access its settings
3. Adjust the device icon by click on `Select Icon` and selecting the desired icon



CLI

1. Navigate 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. `Commit` the changes

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

Mode

The device `Mode` defines how the device is managed by the Nodegrid platform and how the device status is confirmed. The system supports 4 different modes.

Table 40: Modes

MODE	DESCRIPTION
Disabled	In this mode is a device disabled. No sessions can be opened to it and Nodegrid does not check if the device is reachable.

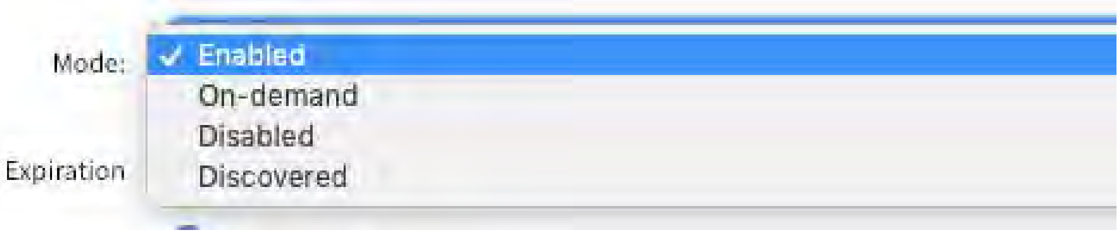
Table 40: Modes

MODE	DESCRIPTION
Enabled	In this mode is a device enabled and sessions can be started. Nodegrid actively checks if a device is reachable.
On-Demand	In this mode is a device enabled and a session can be started. Nodegrid does not check if a device is reachable
Discovered	In this mode is a device disabled. No sessions can be opened to it and Nodegrid does not check if the device is reachable. This mode indicates that the device was added to the system through a discovery process.

WebUI

1. Navigate to `Managed Devices:: Devices`
2. Click on the Target Device to access its settings
3. Set the device mode by selecting a valid mode from the drop-down list

   Note: Discovered can not be selected as this is a system status only



CLI

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

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

Expiration

For each device an expiration date or days can be defined. Once expired, the device will automatically become unavailable. The default value is `Never` in which case the device and its data will stay in the system until admin user removes it.

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.

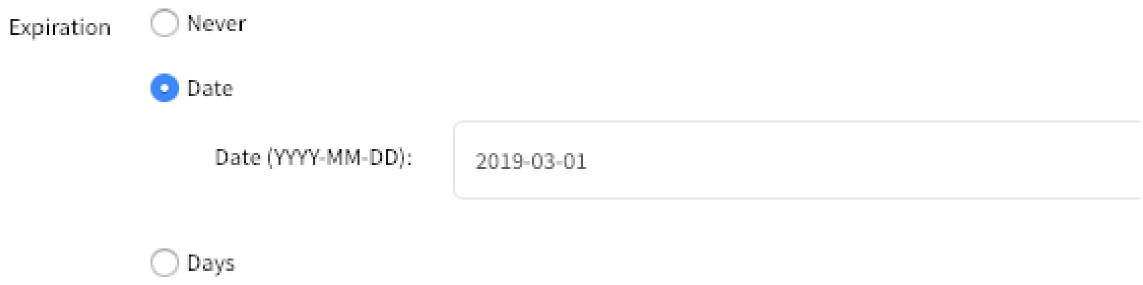
Days – This is similar to timeout. If there is no update on the device's configuration after the specified days, the device and its data will be removed from the system. This is independent of the use of the device.

Both **Date** and **Days** will be applied to VM devices in order to sync 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

1. Navigate to `Managed Devices:: Devices`
2. Click on the Target Device to access its settings
3. Select either `Never`, `Expiration Date` or `Expiration Days` and provide an appropriate value.
   - Date: Dates need to be provided in the format of YEAR-MONTH-DAY (YYYY-MM-DD)
   - Days: value has to be between 1 and 9999999999



Expiration ○ Never

● Date

Date (YYYY-MM-DD): 2019-03-01

○ Days

CLI

1. Navigate to `/settings/devices/<Device Name>/access`
2. Use the `set` command to adjust the `expiration` to either
    - `never`
    - `date`
        - use the `set` command to provide a valid expiration date in `expiration_date`
    - `days`
        - use the `set` command to provide a valid number of days between 0 and 9999999999 in `expiration_days`
3. `commit` the changes

```
[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

Nodegrid supports all devices which are set to **enabled mode**. 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. In case these signals do not exist for a specific device, the device state detection can be changed to use data flow instead. For data flow, the state will be determent based on actual data be transmitted by the device.

To use this feature, the function `Enable device state detection based in data flow` needs to be enabled.

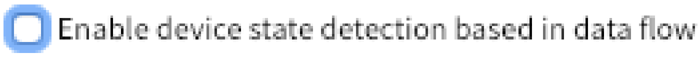
IP Devices

The default mechanism for IP based devices is to establish and monitor an active ssh session to a device. Additionally, an ICMP (ping) check may be enabled to check if the device is active.

To use this feature ,the function `Enable device state detection based on network traffic (icmp)` needs to be enabled.

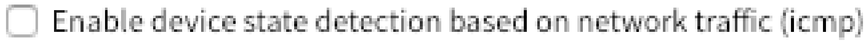
WebUI

1. Navigate to `Managed Devices:: Devices`
2. Click on the Target Device to access its settings
3. Enable device state detection by ticking the box
   - For serial: `Enable device state detection based in data flow`



□ Enable device state detection based in data flow

   - For other devices: `Enable device state detection based on network traffic (icmp)`



□ Enable device state detection based on network traffic (icmp)

CLI

1. Navigate 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. `commit` the changes

```
[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_traf-
fic=yes

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

Run Custom Scripts on Device Status Change

This feature allows users to assign custom scripts to specific device status changes. This is normally used in specific cases where actions need to be performed on status changes which go beyond event notifications.

The following status changes can be used:

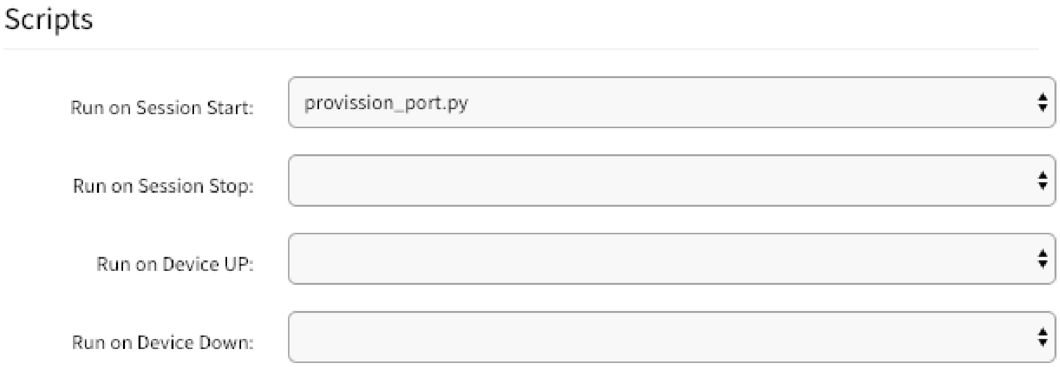
- Session Start
- Session Stop
- Device Up
- Device Down

The scripts need to be written and provided by the customer or through a Professional Services engagement.

Scripts need to be copied to Nodegrid before they can be assigned to a device status. Scripts need to be placed in the `/etc/scripts/access` folder. Each script needs to be executable with user privileges.

WebUI

1. Navigate to `Managed Devices:: Devices`
2. Click on the Target Device to access its settings and Navigate to `Management`
3. In the `Scripts` section assign available scripts to a device status
    - `Run on Session Start`
    - `Run on Session Stop`
    - `Run on Device UP`
    - `Run on Device Down`



Scripts

Run on Session Start: provission_port.py

Run on Session Stop:

Run on Device UP:

Run on Device Down:

CLI

1. Navigate 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. `commit` the changes

```
[admin@nodegrid /]# /settings/devices/Device_Console_Serial/management/
[admin@nodegrid /]#set on_session_start=sessionstart.sh
[+admin@nodegrid management]#commit
```

Data Logging

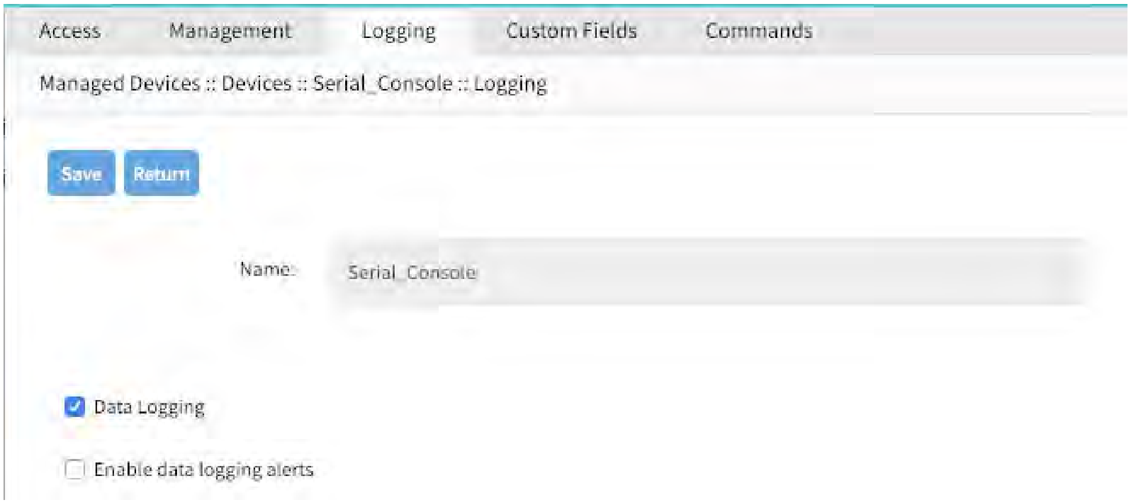
Note: This feature is available to all text-based sessions, like serial sessions or ssh based sessions.

Enabling the `Data Log` feature will allow the system to collect data logs from a device. Data logs will capture all information sent and received from a device. If a device is in enabled mode, the logs will collect data even if no user is currently connected to the device. This enables logging of system messages which are pushed to console sessions.

The collected data logs will be stored locally to the Nodegrid or remotely depending on the `Auditing` settings.

WebUI

1. Navigate to `Managed Devices:: Devices`
2. Click on the Target Device to access its settings and Navigate to `Logging`
3. Enable the option `Data Logging`



Managed Devices :: Devices :: Serial_Console :: Logging

Name: Serial_Console

☑ Data Logging

□ Enable data logging alerts

CLI

1. Navigate to `/settings/devices/<Device Name>/logging`
2. Use the `set` command to change the `data_logging` value to `yes` or `no`
3. `commit` the changes

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

Event Logging

Note: This feature is available to Service Processor and IPMI sessions.

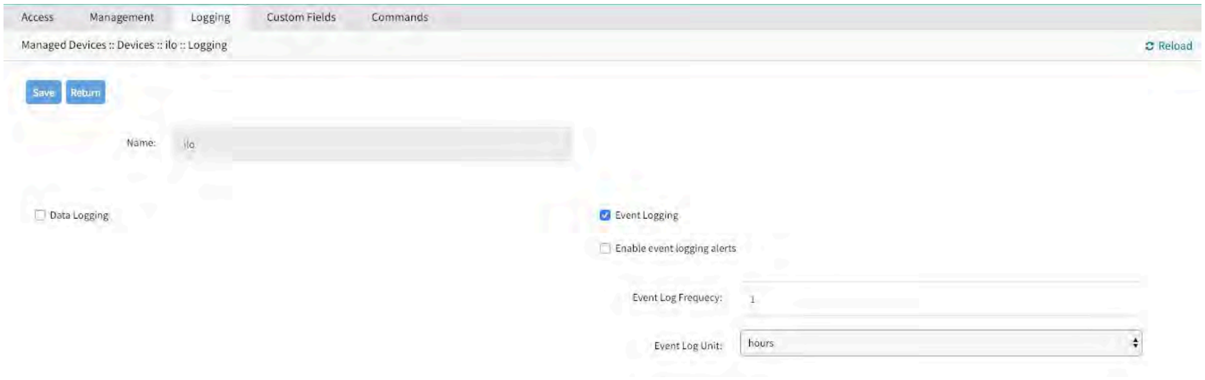
By enabling this feature, the system will be configured to collect Service Processor Event Log data. The type of data collected will depend on the abilities and configuration of the Service Process.

The settings of `Log Frequency` and `Log unit` can control how often the information will be collected. Collection intervals range from 1 min to 9999 hours.

The collected data logs will be stored locally to the Nodegrid or remotely depending on the `Auditing` settings.

WebUI

1. Navigate to `Managed Devices:: Devices`
2. Click on the Target Device to access its settings and Navigate to `Logging`
3. Enable the option `Event Logging`
4. Adjust the values for `Event Log Frequency` or `Event Log Unit` as needed



Managed Devices :: Devices :: ilo :: Logging

Name: ilo

☐ Data Logging

☑ Event Logging

☐ Enable event logging alerts

Event Log Frequecy: 1

Event Log Unit: hours

CLI

1. Navigate 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 `event_log_frequency` and `event_log_unit` as needed
   - `event_log_frequency` range from 1 - 9999
   - `event_log_unit` options `hours` or `minutes`
4. `commit` the changes

```
[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
```

Alert Strings and Custom Scripts

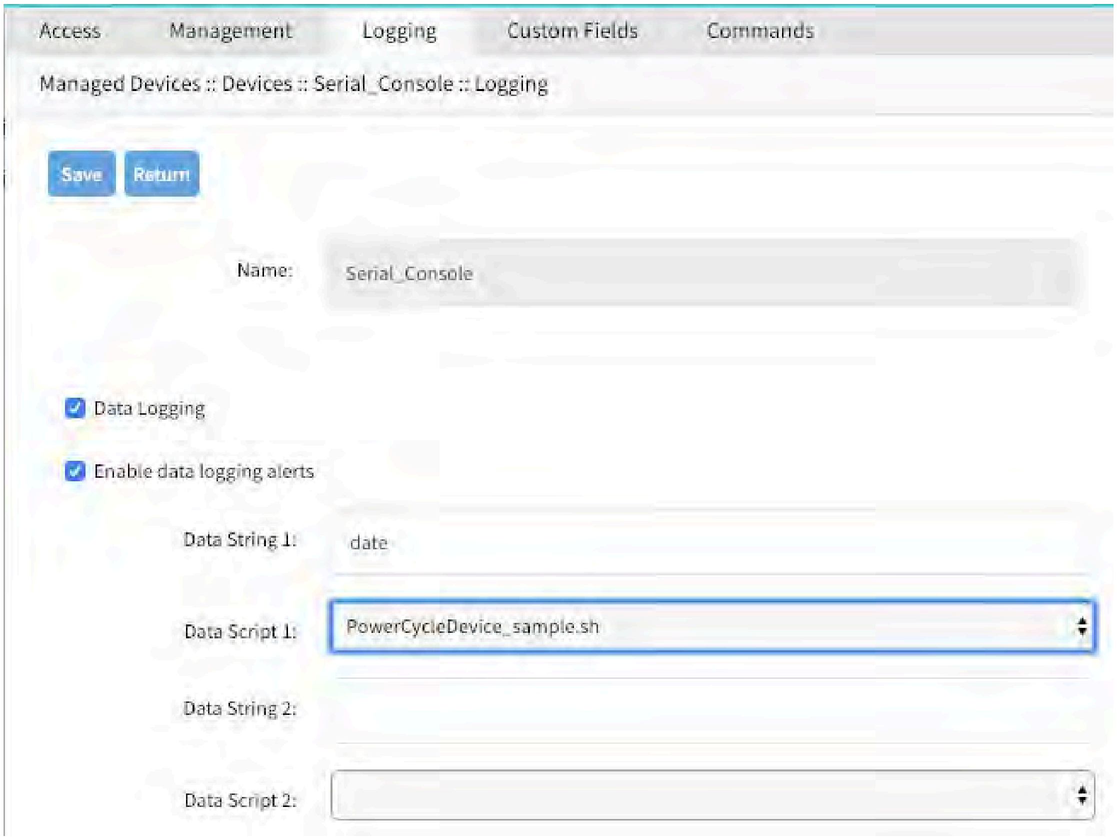
The Data and Event Logging features can also be configured to collect information and create event notifications based on the events executed by custom scripts. This is archived by defining alert strings. Alert strings can be a simple text match or a regular expression pattern string that is evaluated against the data source stream as the data is collected. Events are generated for each match.

The scripts need to be written and provided by the customer or through a Professional Services engagement.

The scripts need to be copied to Nodegrid before they can be assigned to a device status. Scripts need to be placed in the `/etc/scripts/datalog` folder for data log events or `/etc/scripts/events` folder for event logs. Each script needs to be executable with user privileges.

WebUI - Data Logging Alerts

1. Navigate to `Managed Devices:: Devices`
2. Click on the Target Device to access its settings and Navigate to `Logging`
3. Enable the option `Data Logging`
4. Enable the option `Enable data logging alerts`
5. Define a min of one `Data String` which will be matched against the data stream
6. Select an available script for the defined `Data Script` in case a custom script should be executed



Managed Devices :: Devices :: Serial_Console :: Logging

Name: Serial_Console

☑ Data Logging

☑ Enable data logging alerts

Data String 1: date

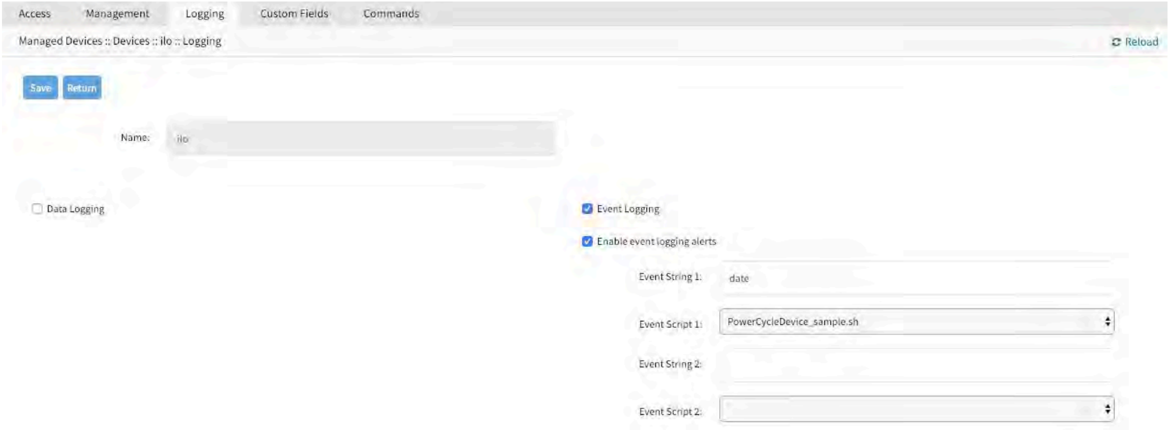
Data Script 1: PowerCycleDevice_sample.sh

Data String 2:

Data Script 2:

WebUI - Event Logging Alerts

1. Navigate to `Managed Devices:: Devices`
2. Click on the Target Device to access its settings and Navigate to `Logging`
3. Enable the option `Event Logging`
4. Enable the option `Enable event logging alerts`
5. Define a min of one `Event String` which will be matched against the data stream
6. Select an available script for the defined `Event Script` in case a custom script should be executed



Name: ilo

□ Data Logging

☑ Event Logging

☑ Enable event logging alerts

Event String 1: date

Event Script 1: PowerCycleDevice_sample.sh

Event String 2:

Event Script 2:

CLI - Data Logging Alerts

1. Navigate 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. `commit` the changes

```
[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
```

CLI - Event Logging Alerts

1. Navigate 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. Define for `event_string_1` string or regular expression which will be matched against the data stream
6. Define for `event_script_1` an available script in case a custom script should be executed
7. `commit` the changes

```
[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

Custom Fields allow users to assign additional information to devices. This information will be visible for each device in the device overview page and are fully searchable.
Custom information is stored as a key/value pair.

WebUI

1. Navigate to `Managed Devices:: Devices`
2. Click on the Target Device to access its settings and Navigate to `Custom Fields`
3. Click on `Add` to create a new Custom Field
    - Provide a Field Name
    - Provide a Filed Value

CLI

1. Navigate 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. `commit` the changes

```
[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 offers a collection of commands which allow users to access and interact with a device. The default configuration is sufficient for most users and is, therefore, the recommended option. If the default configuration is not sufficient, admin users may disable or change existing commands, add existing commands which are not enabled by default, or assign custom commands to a device. Changes made in the Command feature affect all users and should be taken with care. If an admin user wishes to not have specific commands available to certain users or groups, this can be accomplished via user and group authorization.

The available commands for a device will depend on the device type. For example, the `KVM` command (which enable Service Processor KVM session support) is only available to Service Processor devices while the Outlet command is available to all device types.

Custom Commands are available to all device types and are provided through custom scripts. Custom commands can provide support for a wide range of different functions, from additional session options to specific custom tasks which should be performed on a device.

The scripts need to be written and provided by the customer or through a Professional Services engagement.

> Note: While Custom Commands can be executed through the WebUI and CLI, Custom Commands currently only provide feedback and output to the CLI, not the WebUI

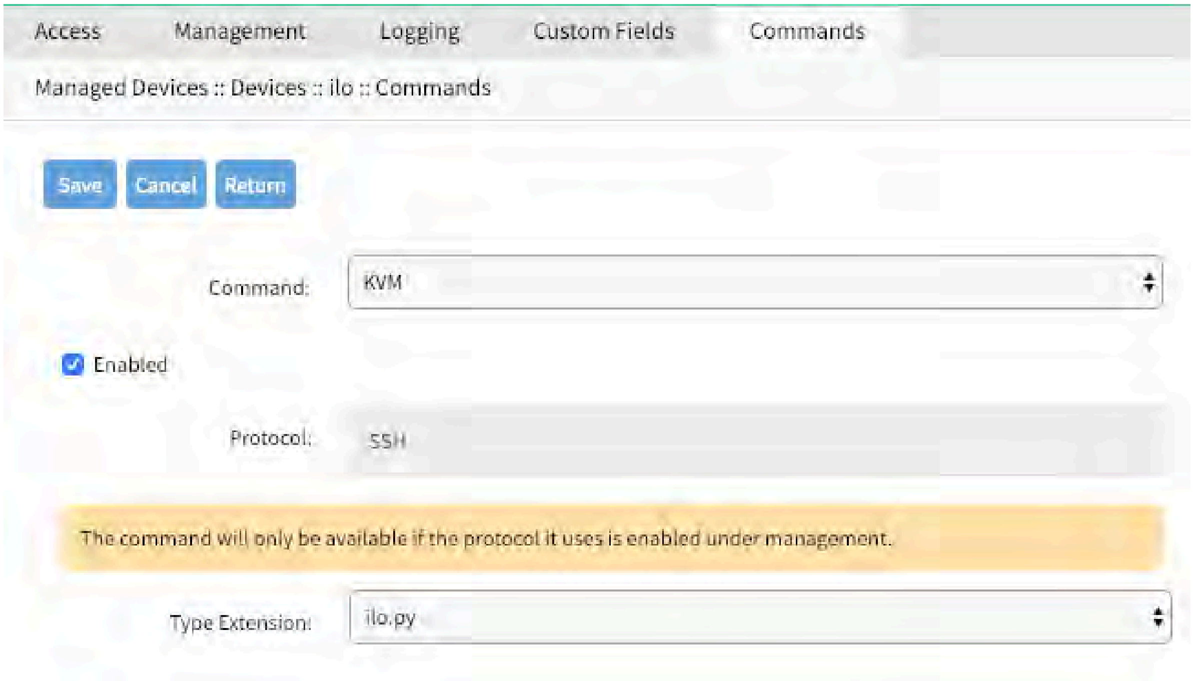
Certain requirements must be met for custom scrips:

- All custom scripts must be written in Python
- The “Command label” must match a function within the script
- The custom scrip must be placed in /etc/scripts/custom_commands

WebUI - Generic

1. Place the custom script inside /etc/scripts/custom_commands
2. Navigate to `Managed Devices:: Devices`

3. Click on the Target Device to access its settings and Navigate to `Commands`
4. Click on `Add` to and select the Command to associate it to a device
5. Click on an existing Command to change, or disable commands



Managed Devices :: Devices :: ilo :: Commands

Command: KVM

☑ Enabled

Protocol: SSH

The command will only be available if the protocol it uses is enabled under management.

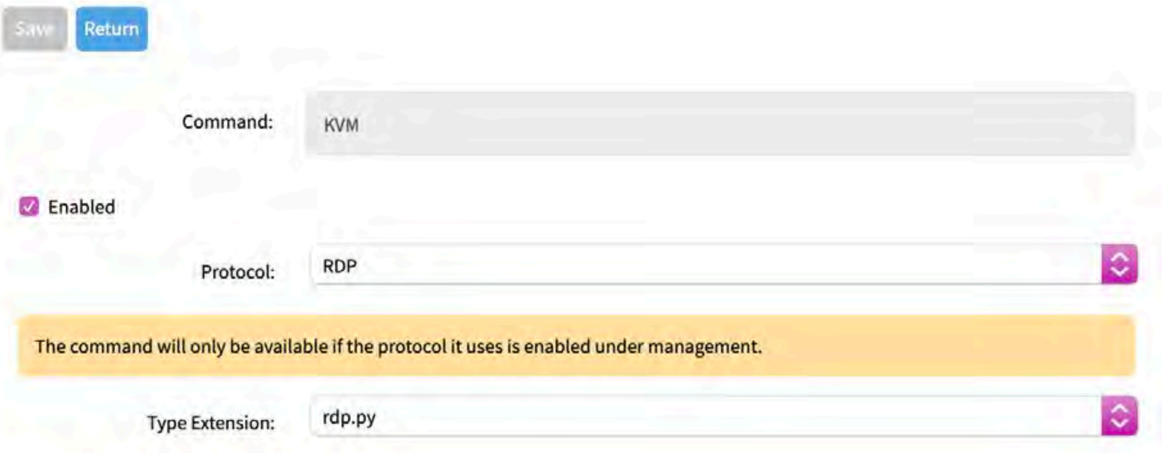
Type Extension: ilo.py

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)
```

WebUI - Device Access via RDP

1. Navigate to Managed `Devices:Devices`
2. Click on the target device to access its settings
3. Navigate to Commands
4. Click on Add and select KVM
5. Click the check box for Enabled
6. Select the following from the drop-down menus:
    - Protocol
    - Type Extension



Command: KVM

☑ Enabled

Protocol: RDP

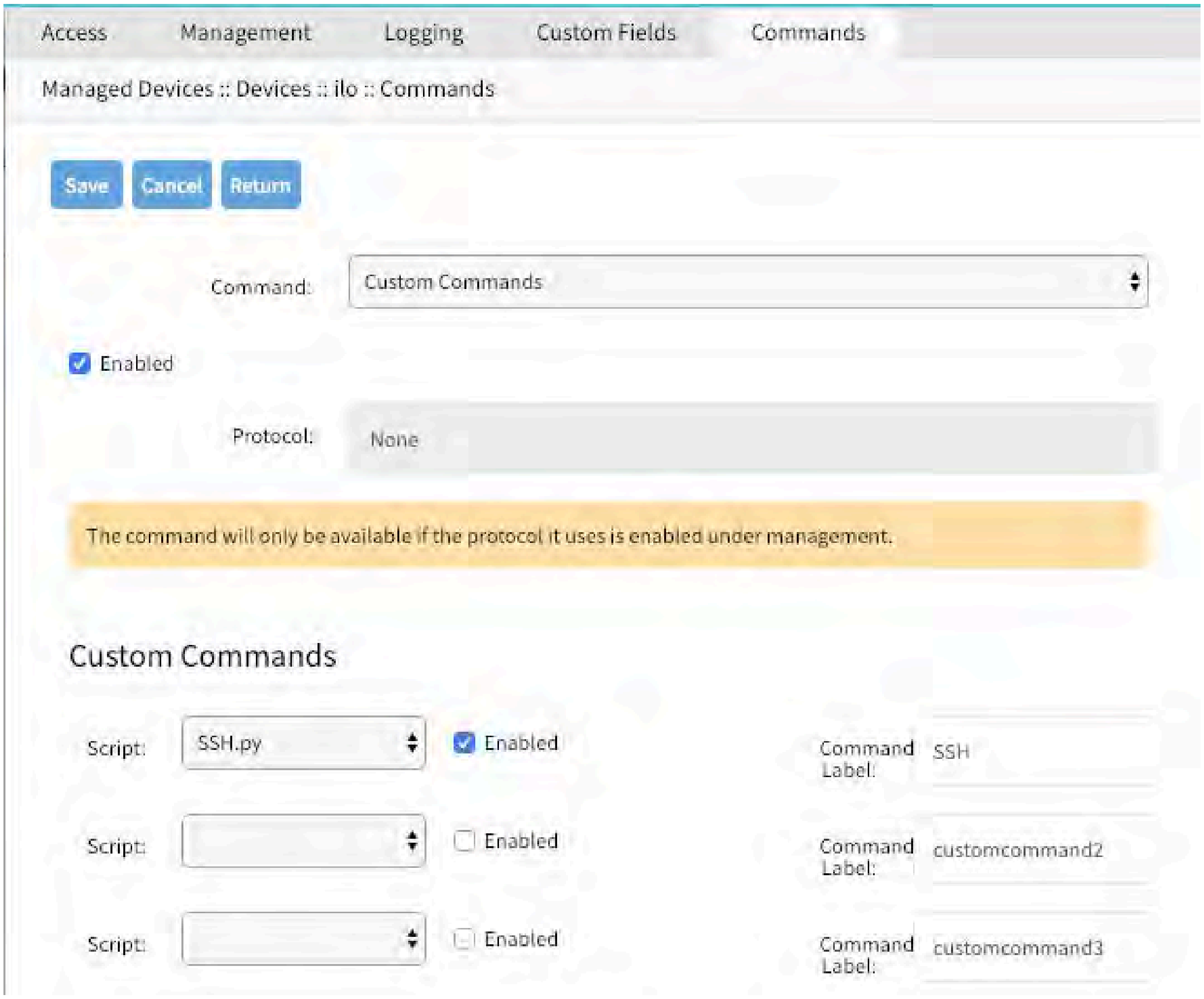
The command will only be available if the protocol it uses is enabled under management.

Type Extension: rdp.py

7. Click save

WebUI - Custom Commands

1. Navigate to `Managed Devices:: Devices`
2. Click on the Target Device to access its settings and Navigate to `Commands`
3. Click on `Add` to and Select `Custom Commands`
    - Select a `Script` from a list of available scripts
    - Click on Enable to enable the specific command
    - Adjust the Command Label to match the command option in the script



Managed Devices :: Devices :: ilo :: Commands

Command: Custom Commands

☑ Enabled

Protocol: None

The command will only be available if the protocol it uses is enabled under management.

Custom Commands

Script: SSH.py ☑ Enabled Command Label: SSH

Script: ☐ Enabled Command Label: customcommand2

Script: ☐ Enabled Command Label: customcommand3

CLI - Custom Commands

1. Navigate 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. `commit` the changes

```
[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
```

Tree View Settings

In `Managed Devices :: Views` an admin may adjust and create a tree structure to which devices can be associated. This feature is used to reflect specific organizational or physical structures which help users to find and access their devices.

Groups may also be used to aggregate monitoring values like a rack or room level.

Device Types

Device Type settings allow administrators to adjust or create customized versions of existing device types. This is beneficial in cases where the default value for a device type does not match a customer's current default values.

By either Cloning, Editing or Deleting existing device types, these values can, be adjusted as needed. These setting will take effect automatically for all devices which currently utilize the specific device type.

Preferences

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 Preferences

The power menu preferences options allow administrators to define the order and labeling of the power menu as it appears in a console session.

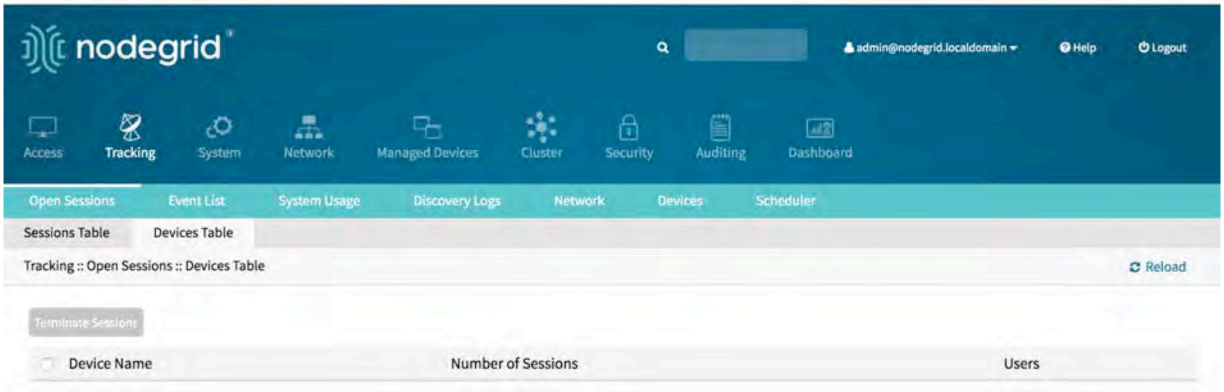
Session Preferences

The session preference section allows users to define a session `Disconnect HotKey` for console sessions. This feature is beneficial when users start console sessions from within console sessions, as well as cascaded console sessions. In this case, it can be difficult to exit a specific console session without closing all sessions in the chain. The hotkey will provide a user the option to specifically disconnect from a specific amount of the console session within the chain. Starting from the current session working its way back up the chain.

The value is by default undefined.

Tracking

The *Tracking* features provide information about the system and connected devices like Open Sessions, Event List, Routing Table, System Usage, Discovery Logs, LLDP and Serial Statistics.



Open Sessions

The `Open Sessions` page provides an overview of connected users and devices sessions.

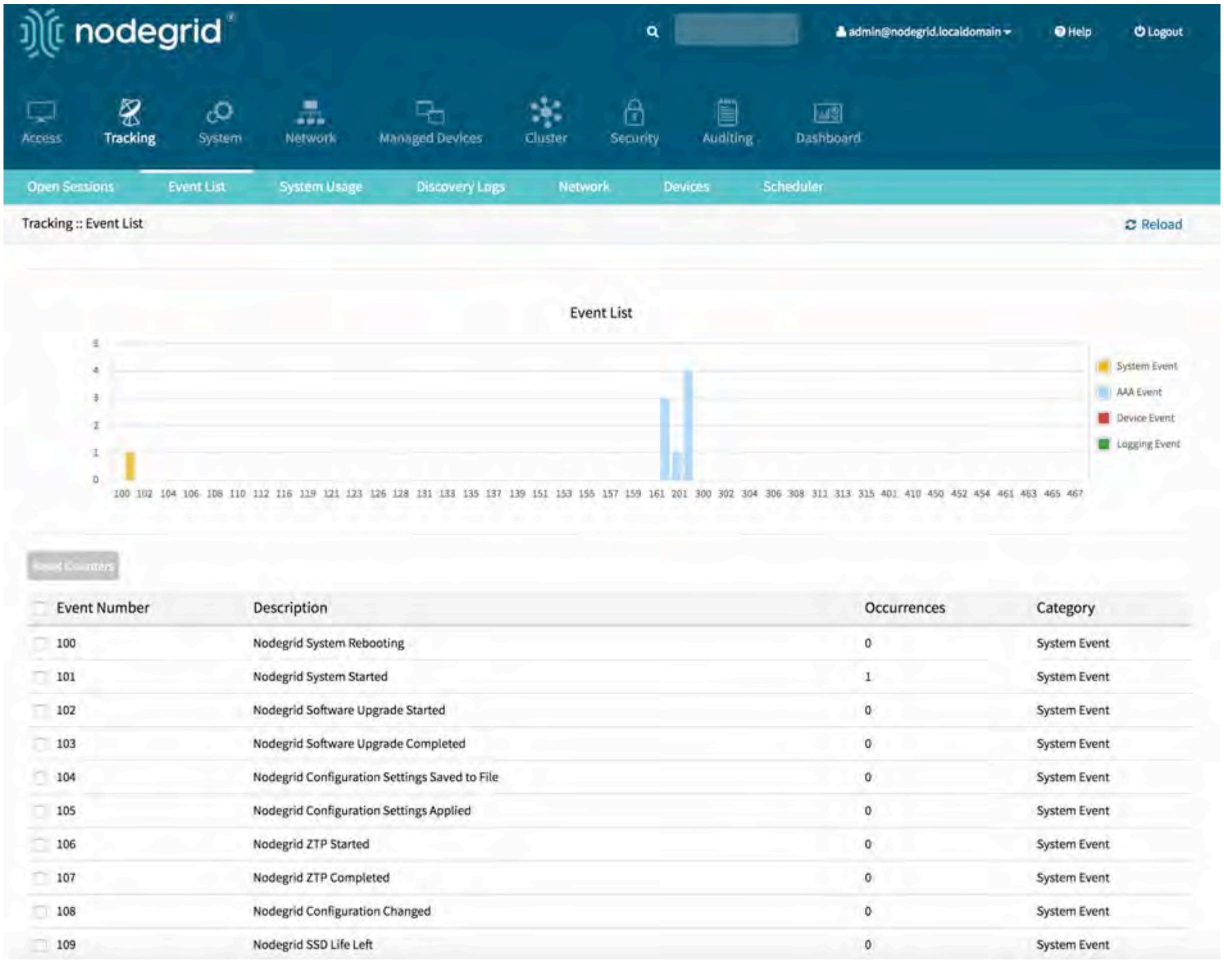
The `Sessions Table` menu shows all users actively connected to the system, from where they are connecting from, and for how long.

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

If a user has permission based on an authorization group, he/she can terminate sessions.

Event List

The `Event List` menu provides statistical information on the system events occurrences. Events can be selected and the current counters reset.



□ Event Number	Description	Occurrences	Category
□ 100	Nodegrid System Rebooting	0	System Event
□ 101	Nodegrid System Started	1	System Event
□ 102	Nodegrid Software Upgrade Started	0	System Event
□ 103	Nodegrid Software Upgrade Completed	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

The complete list for registered events in the Nodegrid system follows. New events may be added as needed.

Table 41: Registered Events

EVENT NUMBER	DESCRIPTION	OCCURRENCES	CATAGORY
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

Table 41: Registered Events

EVENT NUMBER	DESCRIPTION	OCCURRENCES	CATAGORY
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
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

Table 41: Registered Events

EVENT NUMBER	DESCRIPTION	OCCURRENCES	CATAGORY
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
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

Table 41: Registered Events

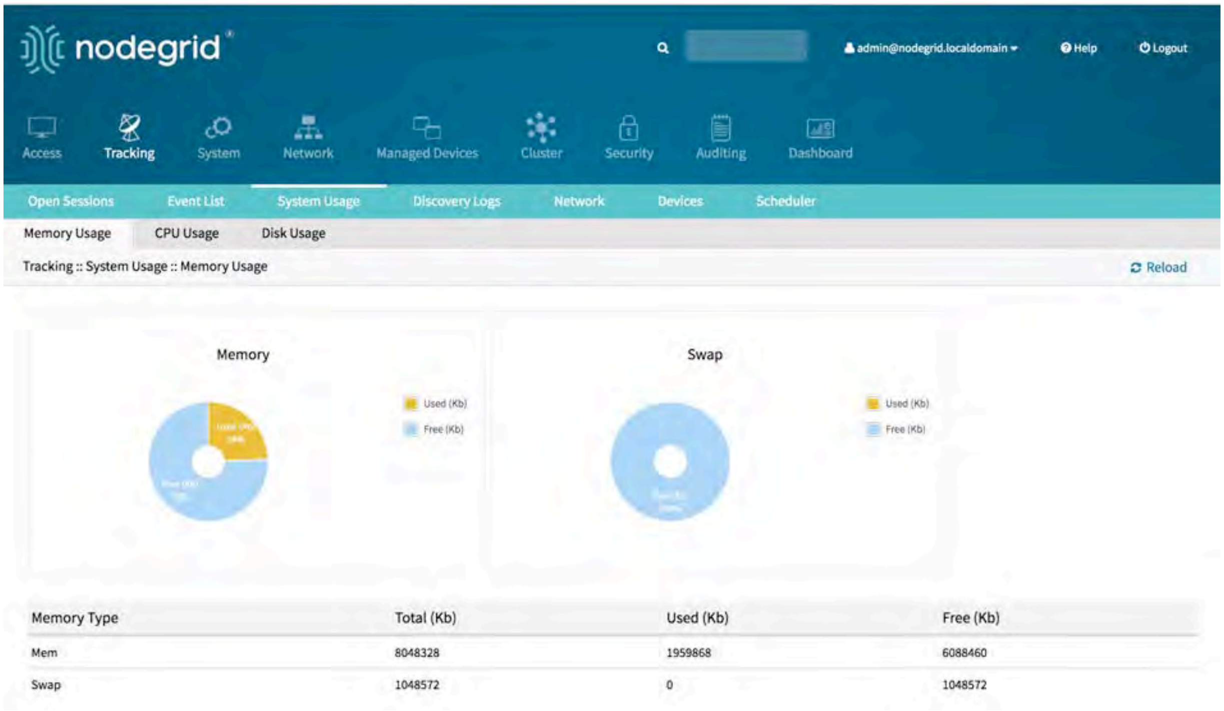
EVENT NUMBER	DESCRIPTION	OCCURRENCES	CATAGORY
158	Nodegrid Cluster Coordinator Created	0	System Event
159	Nodegrid Cluster Peer Configured	0	System Event
160	Nodegrid Search Unavailable	0	System Event
161	Nodegrid Search Restored	0	System Event
200	Nodegrid User Logged In	3	AAA Event
201	Nodegrid User 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
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

Table 41: Registered Events

EVENT NUMBER	DESCRIPTION	OCCURRENCES	CATAGORY
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
467	Nodegrid PoE Power Fault	0	Logging Event
468	Nodegrid PoE Power Budget Exceeded	0	Logging Event

System Usage

The `System Usage` page presents information about `Memory Usage`, `CPU Usage`, and `Disk usage` for the current system.

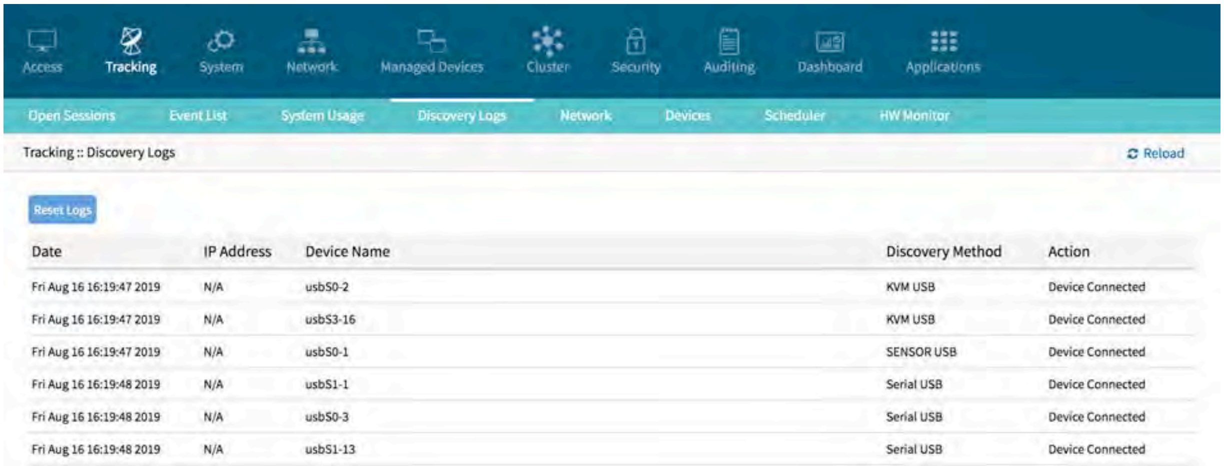


Tracking :: System Usage :: Memory Usage

Memory Type	Total (Kb)	Used (Kb)	Free (Kb)
Mem	8048328	1959868	6088460
Swap	1048572	0	1048572

Discovery Logs

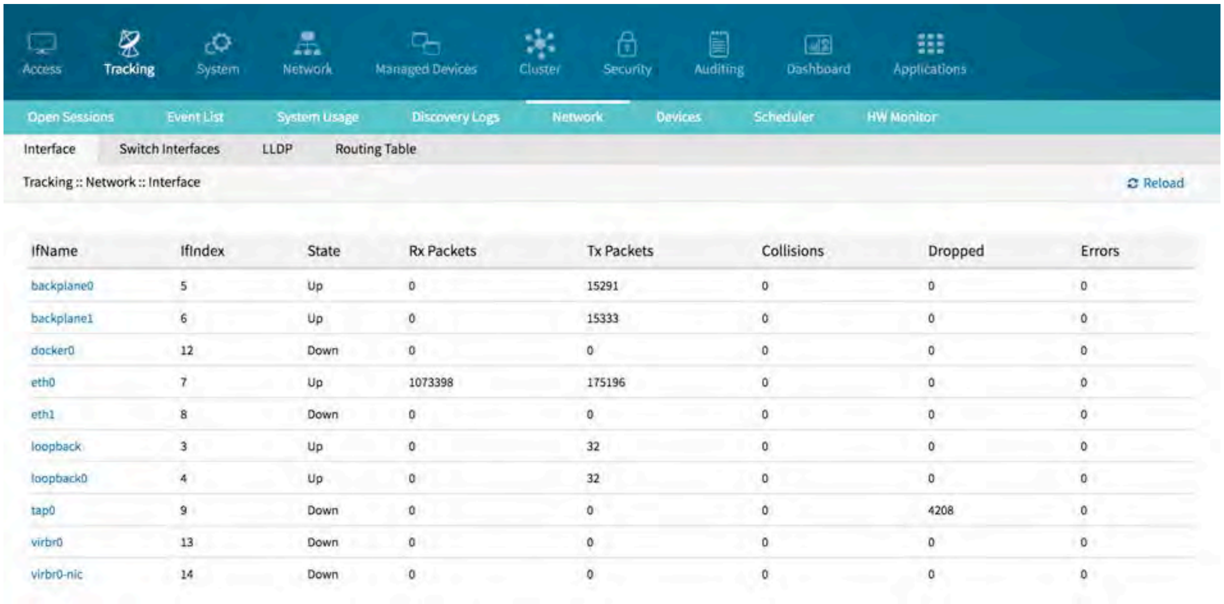
The `Discovery Logs` page shows the logs of the discovery processes set on the Managed Devices' setting for auto discovery.



Tracking :: Discovery Logs

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

Network Statistics



Tracking :: Network :: Interface

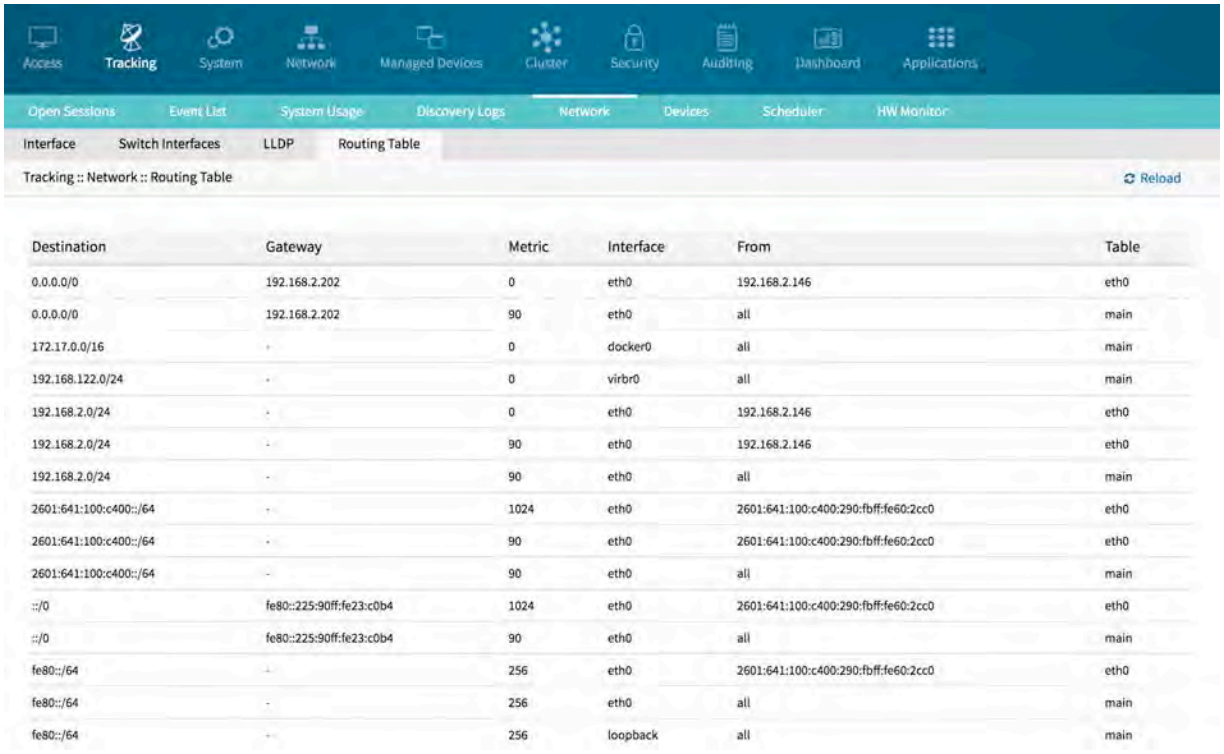
IfName	IfIndex	State	Rx Packets	Tx Packets	Collisions	Dropped	Errors
backplane0	5	Up	0	15291	0	0	0
backplane1	6	Up	0	15333	0	0	0
docker0	12	Down	0	0	0	0	0
eth0	7	Up	1073398	175196	0	0	0
eth1	8	Down	0	0	0	0	0
loopback	3	Up	0	32	0	0	0
loopback0	4	Up	0	32	0	0	0
tap0	9	Down	0	0	0	4208	0
virbr0	13	Down	0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

The `Network` statistics page displays network `Interface` information, `LLDP` and the `Routing Table` details.

The `Interface` page displays the network interface statistics, like state, package counters, collisions, dropped and errors.

The `LLDP` page shows the devices that are advertising their identity and capabilities on the LAN. You may want to enable `LLDP advertising and reception through this connection` in your Nodegrid by setting it up in network connections.

The `Routing Table` page shows the routing rules that Nodegrid follows for network communications. It also included any static network routes which were added.



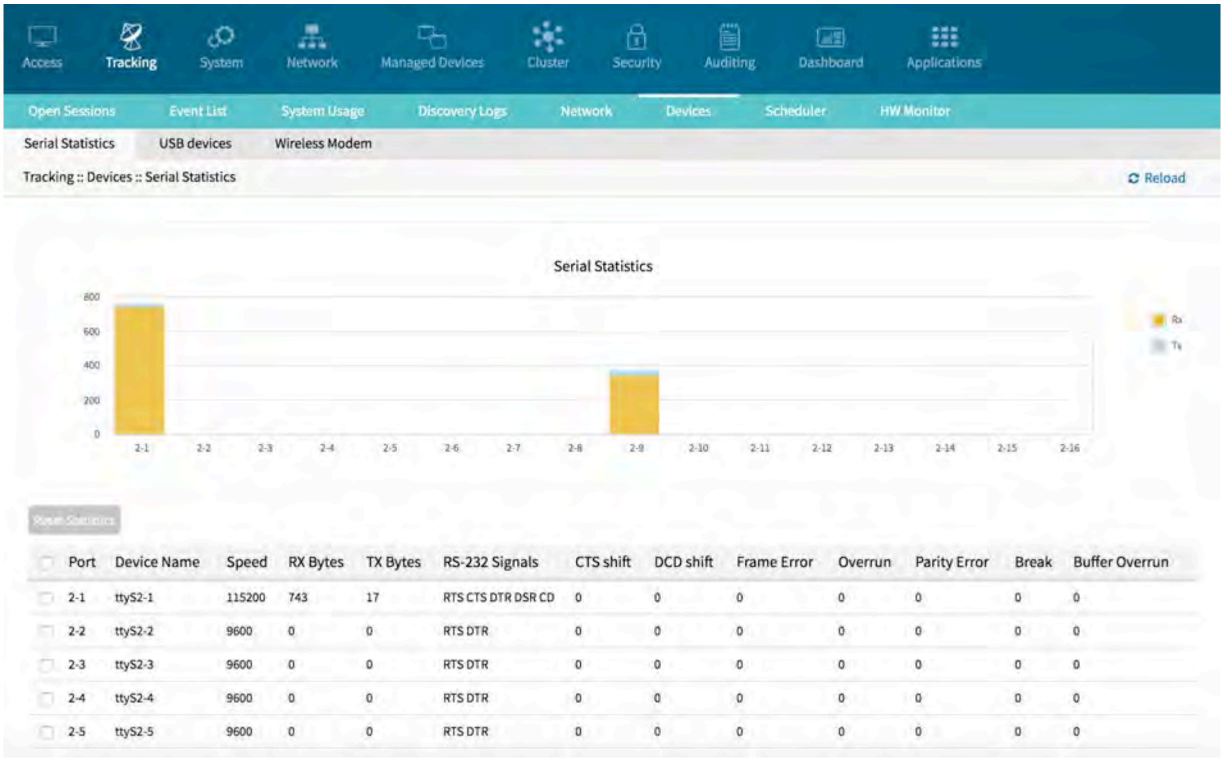
Tracking :: Network :: Routing Table

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

Device Statistics

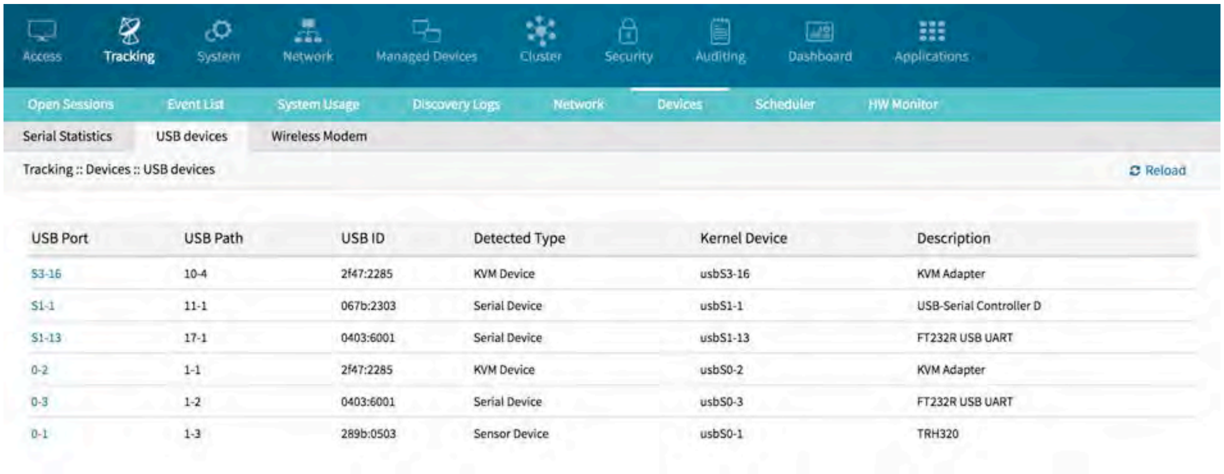
The `Devices` page shows connection statistics for physically connected devices, like serial and USB devices, and wireless modems. The available options will depend on the specific Nodegrid unit.

The `Serial Statistics` page provides statistical information on the serial ports connectivity such as transmitted and received data, RS232 signals, errors.



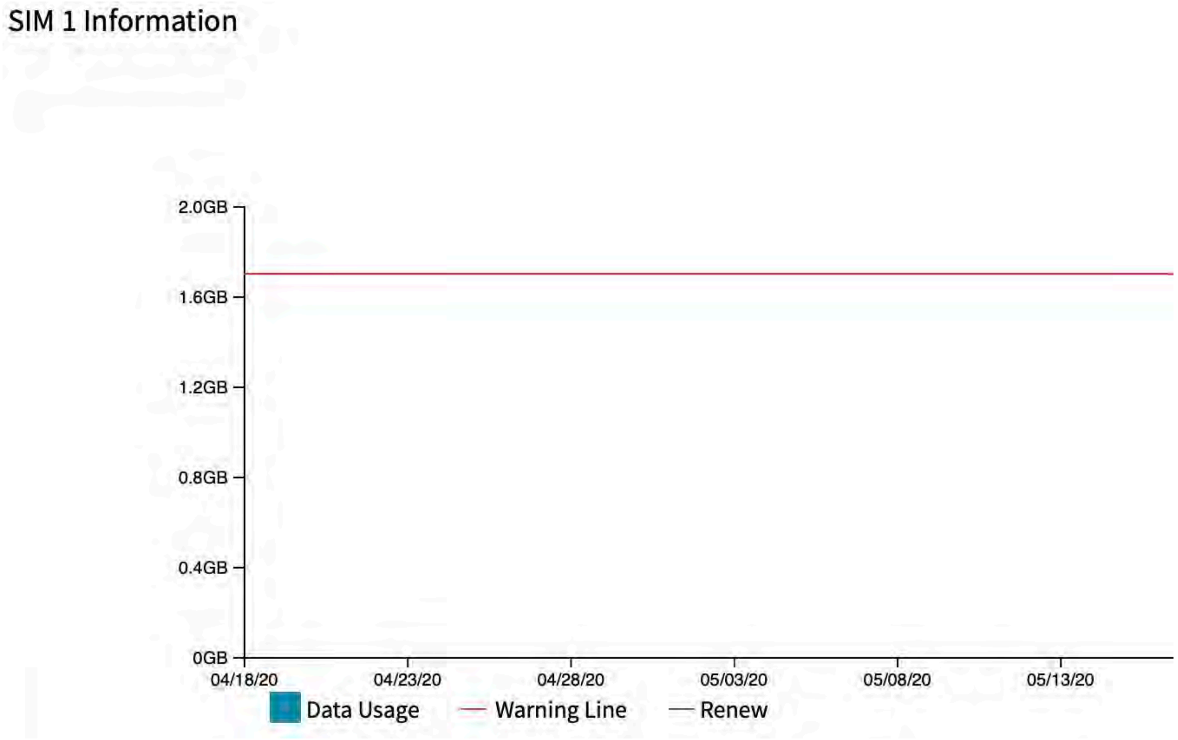
	Port	Device Name	Speed	RX Bytes	TX Bytes	RS-232 Signals	CTS shift	DCD shift	Frame Error	Overrun	Parity Error	Break	Buffer Overrun
□	2-1	ttyS2-1	115200	743	17	RTS CTS DTR DSR CD	0	0	0	0	0	0	0
□	2-2	ttyS2-2	9600	0	0	RTS DTR	0	0	0	0	0	0	0
□	2-3	ttyS2-3	9600	0	0	RTS DTR	0	0	0	0	0	0	0
□	2-4	ttyS2-4	9600	0	0	RTS DTR	0	0	0	0	0	0	0
□	2-5	ttyS2-5	9600	0	0	RTS DTR	0	0	0	0	0	0	0

The `USB devices` page provides details about connected USB devices and initialized drivers. The `Wireless Modem` page displays information about slot, SIM status, and signal strength.



USB Port	USB Path	USB ID	Detected Type	Kernel Device	Description
S3-16	10-4	2f47:2285	KVM Device	usbS3-16	KVM Adapter
S1-1	11-1	067b:2303	Serial Device	usbS1-1	USB-Serial Controller D
S1-13	17-1	0403:6001	Serial Device	usbS1-13	FT232R USB UART
0-2	1-1	2f47:2285	KVM Device	usbS0-2	KVM Adapter
0-3	1-2	0403:6001	Serial Device	usbS0-3	FT232R USB UART
0-1	1-3	289b:0503	Sensor Device	usbS0-1	TRH320

If Data Usage Monitoring is enabled, you may view the mobile data usage statistics for each SIM via graphs on the Wireless Modem page



Usage statistics can be manually reset at any time by clicking on the Reset button.

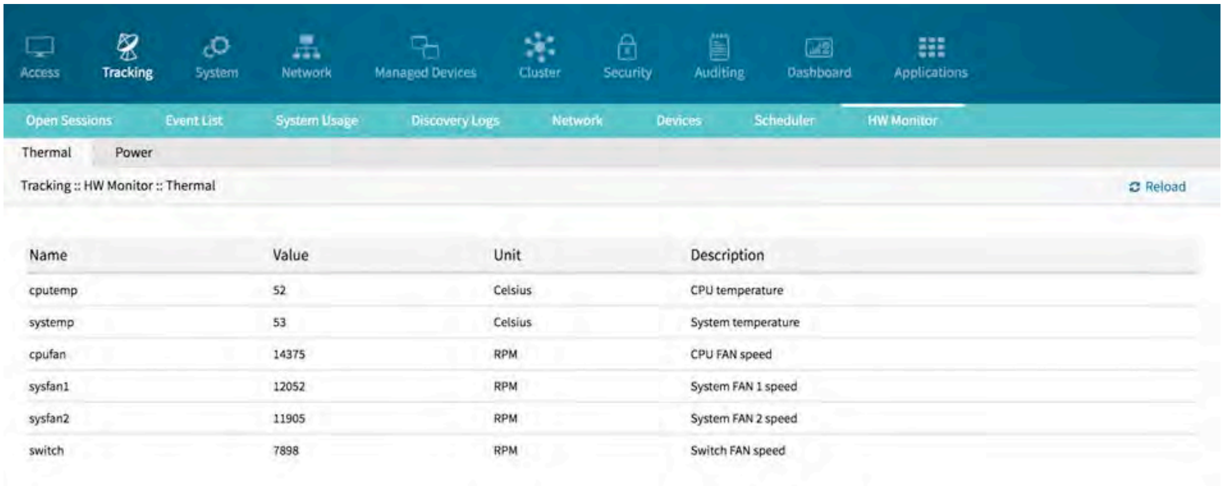
Scheduler

The `Scheduler` page provides information about scheduled tasks when they ran, by whom and any events or errors are displayed.

HW Monitor

The `HW Monitor` page displays Nodegrid system information. `Thermal` displays the current CPU temperature, System temperature as well as FAN speeds if available. `Power` section displays information about the current Power sources like current state and power consumption. The section `I/O Ports` 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.

(example NSR is shown)

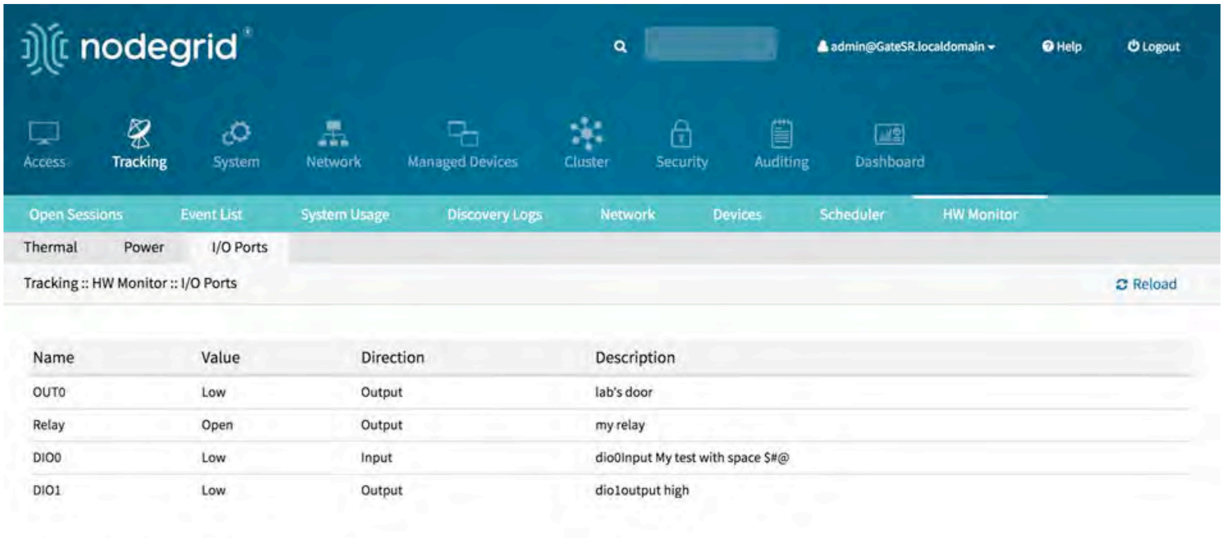


Name	Value	Unit	Description
cputemp	52	Celsius	CPU temperature
systemp	53	Celsius	System temperature
cpufan	14375	RPM	CPU FAN speed
sysfan1	12052	RPM	System FAN 1 speed
sysfan2	11905	RPM	System FAN 2 speed
switch	7898	RPM	Switch FAN speed

I/O Ports (GPIO)

This page shows the status of GPIO ports. It is only available on models with GPIO ports, like Nodegrid Gate SR and Nodegrid Link SR.

(example Nodegrid Gate SR shown)



Name	Value	Direction	Description
OUT0	Low	Output	lab's door
Relay	Open	Output	my relay
DIO0	Low	Input	dio0input My test with space $#@
DIO1	Low	Output	dio1output high

System

The system settings allow the configuration of system-specific settings like license keys, general system settings, firmware updates, backup and restore and others.

Licenses

Clicking on `System` brings you straight to the `Licenses` tab. This tab displays all licenses enrolled in this Nodegrid, along with other relevant information, a license key, expiration date, application, etc. The upper right corner shows the number of licenses, used and available. Licenses can be added or deleted in this page. If licenses expire or are deleted, the devices exceeding the total licenses will change the status to "unlicensed", but their information will be retained in the system. However, unlicensed devices will not show up in the access page.

A license is required for each managed device for Nodegrid access and control. The required license for each serial port of the Nodegrid is included with the product.

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

System Preferences

Main system preferences are configured in this tab.

- Address Location and coordinates
- Online help URL
- Session idle timeout
- Revision Tag and Latest Profile Applied
- Login logo image and banner message
- The Utilization rate of serial ports and licenses
- Nodegrid serial console speed, bauds
- Display of dual power supplies
- Network boot parameters and ISO image URL

Nodegrid Location

Enter a valid address location for this Nodegrid, and click on the small compass icon/button on the right of this field to populate the "Coordinates" field below with Latitude and Longitude of that address.

The "Help Location" field is an alternate URL location for the user manual. The administrator can download the user manual and post to a specific location reachable by Nodegrid. When the small "Help" icon/button on the top right of the Nodegrid WebUI is clicked, a new web page opens with the file referenced by this URL.

Session Idle Timeout

This is the number of seconds for open sessions to time out due to inactivity. You may enter a zero value for new sessions to never expire. Configuration changes on this field will be effective for new sessions only. Existing sessions will continue following their timeout value specified at session start. This setting applies to all telnet, SSH, HTTP, HTTPS, and console sessions.

Nodegrid Configuration

The `Revision Tag` field allows to define a free format string which will be used as a configuration reference tag. This field can be manually updated by user or through an automated change management process.

The `Latest Profile Applied` informs which profile was last applied through a ZTP process or the ZPE Cloud.

Login logo image

Use this feature to change the logo image to be used on Nodegrid's WebUI login page. The new image file has to be a .png or .jpg and can be uploaded from your local desktop or a remote server (FTP, TFTP, SFTP, SCP, HTTP, and HTTPS). Enter the respective URL format, username and password may be required. `<PROTOCOL>://<ServerAddress>/<Remote File>`.

After uploading, refresh the browser cache to show the new image.

Login Banner

Nodegrid can be configured to show a login banner on Telnet, SSHv2, HTTP, HTTPS and Console login, to display the user a message before logging into the system. The default banner (below) can be edited and customized by the admin.

Default login banner:

```
WARNING: This private system is provided for authorized use only and it may be mon-
itored for all lawful purposes to ensure its use. All information including per-
sonal 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.
```

Utilization Rate

Click and check respective boxes and enter the desired usage percentage to enable monitoring the utilization rate of licenses and local serial ports. An event will be generated when the percentage is reached. The default value is 90%.

Console Port

Set the baud rate of the local console port. The default value is set to 115,200 bps.

Power Supplies

Displays the state of dual power supplies (ON/OFF) and to enable alarm sound (check the appropriate box) when one power supply go down.

To acknowledge the alarm state, click on `Acknowledge Alarm State` on the top left of this page `System::Preferences`.

Network Boot

Nodegrid can be set to boot from an ISO image from the network. Enter the unit's IPv4 address and netmask, the ethernet interface to be used (eth0 or eth1), and the URL where the ISO image is `http://ServerIPAddress/PATH/FILENAME.ISO`

PXE Boot

The Nodegrid supports PXE boot (Pre-Boot Execution Environment). PXE forms part of the UEFI (Unified Extensible Firmware Interface) to boot an appropriate software image retrieved at boot time from a network server. It is one of the most preferred methods in data centers for OS booting, installation, and deployment.

PXE boot is enabled by default in Nodegrid, but it can be disabled via Web page under `Security::Services` or via CLI within `/settings/services` scope. The example below shows how to configure the DHCP/PXE server in Linux (Ubuntu) with installed Apache web server, tftpd-hpa service and Nodegrid 4.1.x. The PXE, DHCP and TFTP servers must have been 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 and unzip the tar file which will create 2 directories (nodegrid 4.1.xx and boot) or create the directory and put tar file in that directory and then unzip the tarball file (ie. cd /var/lib/tftpboot/PXE directory)

```
Example:
root@ubuntu-srv1:~# cd /var/lib/tftpboot/
root@ubuntu-srv1:/var/lib/tftpboot# ls -l
drwxrwxr-x 2 root  root       4096 Apr 24 03:20 nodegrid-4.1.xx
root@ubuntu-srv1:/var/lib/tftpboot# ls -l nodegrid-4.1.xx
total 558468
-rw-r--r-- 1 root root  22270823 Apr 24 03:19 initrd
-rw-rw-r-- 1 root root 544343672 Apr 24 03:19 rootfs.img.gz
-rw-rw-r-- 1 root root         7 Apr 24 03:19 version
-rw-r--r-- 1 root root   5242832 Apr 24 03:19 vmlinuz
      root@ubuntu-srv1:/var/lib/tftpboot#
```

3. Edit dhcpd.conf file and add these lines in the host definition section. The `hardware ethernet` value has to match the MAC address of the Nodegrid unit, and the `fixed-address` is the IP of the Nodegrid unit.

```
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-4.1.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;
}
```

4. On Web server (e.g. Apache), cd /var/www and create a soft link to the file where you want it to do network boot: ln -s and filename you want to link to the directory.

```
  Example:
root@ubuntu-srv1:/var/www# pwd
root@ubuntu-srv1:/var/www#
root@ubuntu-srv1:/var/www# ln -sf /var/lib/tftpboot/PXE/nodegrid-4.1.xx/ nodegrid-
4.1.xx
```

5. Restart the DHCP server

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

6. Restart tftpd-hpa process
7. Start the Nodegrid. This will install the Nodegrid netboot image on to the specific Nodegrid.

Date and Time

Set the Network Time Protocol (NTP) server for automatic retrieval of accurate time, or manually set the date and time. NTP is the default configuration and it will try to retrieve the date and time from any server in the NTP pool. In manual configuration mode, Nodegrid will use its own clock to provide date and time information. Refresh the page to see the current system time.

Nodegrid supports `NTP Authentication` and `Cellular Tower Synchronization`.

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.

Date and time synchronization from cell tower also provides an additional convenience for obtaining exact time directly from the carrier network.

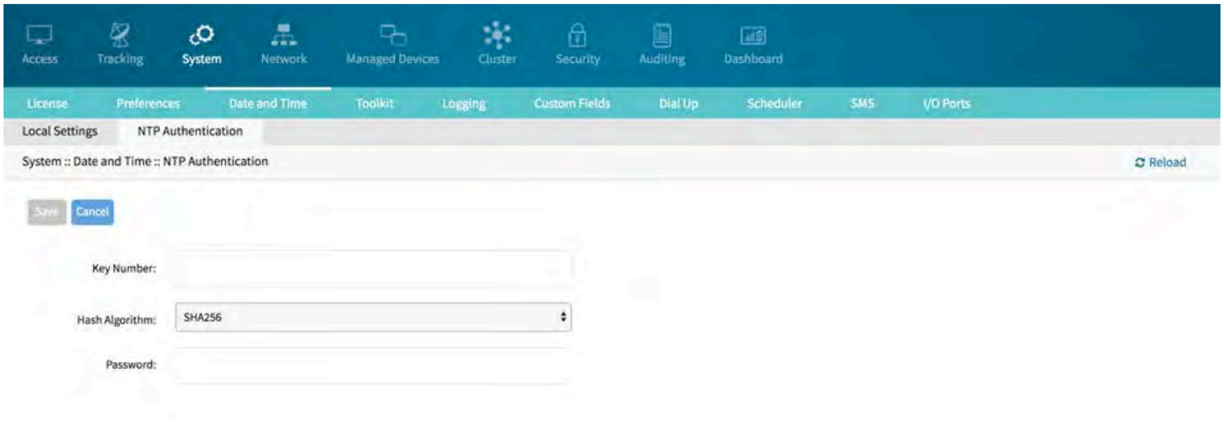
The local time zone can also be set from the drop-down menu, the default is UTC.

Note: All timestamps in Event Logs are in UTC.

NTP Authentication

NTP provides a number of measures to reduce security risks associated with time synchronization. Authentication is one such measure. It allows a client to be sure that a response has been generated from an expected source, rather than being maliciously generated or intercepted. Authentication is based on a list of agreed keys, or passwords, between a server and a client. Any communication between server and client has an encrypted version of one of the agreed keys appended to the messages. The server or client can then un-encrypt the key appended to any received communication to ensure it matches one of the agreed keys before taking appropriate action.

1. In the webUI as admin, navigate to `System :: Date and Time :: NTP Authentication` to provide the following information:
   - Key Number or Key ID: a number that identifies the key/password
   - Hash Algorithm or Type: the cryptographic hash function to be used
   - Password or Key value: The password is used with the hash algorithm to generate and verify a message authentication code (MAC) in NTP packets.



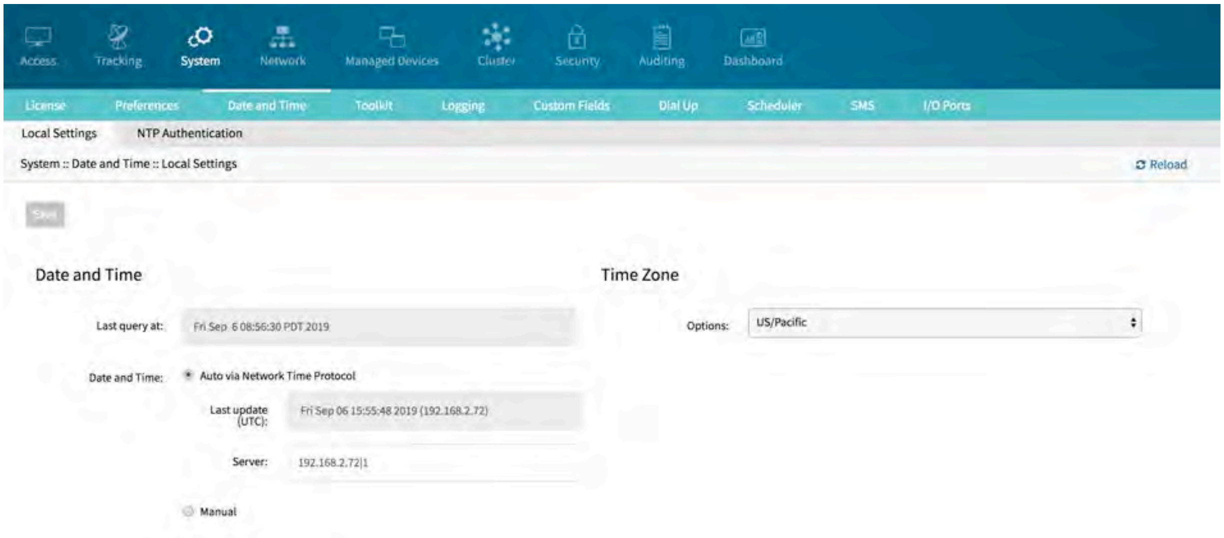
Key Number:

Hash Algorithm: SHA256

Password:

2. Add each key number under System > Date and Time > NTP Authentication
   - Key Number: any unsigned integer in the range 1 through 2^32-1
   - Hash Algorithm: 'MD5','RMD160','SHA1','SHA256','SHA384','SHA512', 'SHA3-224','SHA3-256','SHA3-384','SHA3-512'
   - Password: The password can be specified as a string of characters not containing white space, or as a hexadecimal number with the 'HEX:' prefix.

3. Link the NTP server and its key number Link is provided in `System :: Date and Time :: Local Settings` or under System > Date and Time > Local Settings. Use separator '|' (pipe) between server address and its key number.



System :: Date and Time :: Local Settings

Date and Time

Last query at: Fri Sep 6 08:56:30 PDT 2019

Date and Time: ● Auto via Network Time Protocol

Last update (UTC): Fri Sep 06 15:55:48 2019 (192.168.2.72)

Server: 192.168.2.72|1

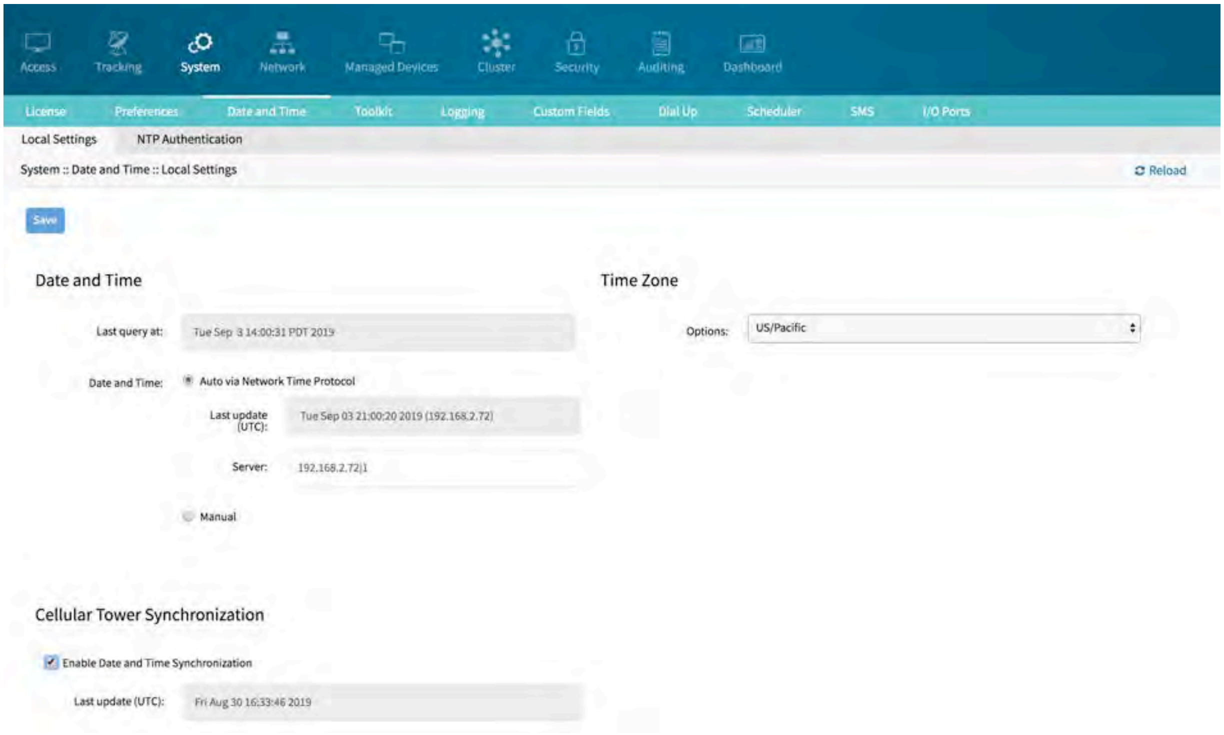
○ Manual

Time Zone

Options: US/Pacific

Cellular Tower Synchronization

This functionality is supported by units that have a Wireless Modem card installed with valid SIM card. It will allow Nodegrid to get date and time from the cellular tower when the SIM card is registered to the carrier network. Check the appropriate box to enable this functionality.



System :: Date and Time :: Local Settings

Date and Time

Last query at: Tue Sep 3 14:00:31 PDT 2019

Date and Time: ● Auto via Network Time Protocol

Last update (UTC): Tue Sep 03 21:00:20 2019 (192.168.2.72)

Server: 192.168.2.72|1

○ Manual

Time Zone

Options: US/Pacific

Cellular Tower Synchronization

☑ Enable Date and Time Synchronization

Last update (UTC): Fri Aug 30 16:33:46 2019

It is possible to have both NTP and Cellular Tower Synchronization enabled. The last date and time received from either source will be applied. This approach allows to receive date/time information in connection failover configuration as well.

Logging

The System Logging feature enables data logging of all CLI session to the Nodegrid to be logged for later inspection and auditing.

The collected data logs will be stored locally to the Nodegrid or remotely depending on the `Auditing` settings.

The Data Logging features can create event notifications in addition to collect information. This is archived by defining alert strings. Alert strings can be a simple text match or a regular expression pattern string that is evaluated against the data source stream as the data is collected. Events are generated for each match.

Custom Fields

This section adds searchable custom fields to the unit.

Use this feature to add pieces of information that are not available by default. The Nodegrid system allows the creation of custom fields so that they become part of information of the device.

Dial-Up

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.

Scheduler

The Scheduler allows administrators to execute tasks and scripts on a scheduled basis. This can be used for maintenance tasks or automation tasks including end devices.

The tasks which should be executed need to be part of a `cli` file or script file located on the Nodegrid. The file needs to be accessible and executable by the user.

Table 42: Scheduler

SETTING	VALUE	DESCRIPTION
Task Name	String	A Task Name
Task Description	String	A task description will be displayed on the overview
User	String	Must be a valid local user who has access to the script file. Default: daemon

Table 42: Scheduler

SETTING	VALUE	DESCRIPTION
Command to Execute	String	Shell command which will be executed. To execute a cli file the following setting can be used`cli -f <path><cli file name>`
Minute	Integer	Minute (0-59) when the task should be executed. Default: * (any)
Hour	Integer	Hour (0-23) when a task should be executed. Default: * (any)
Day of Month	Integer	Day of the Month (1-31) when a task should be executed. Default: * (any)
Month	Integer	Month (1-12) when a task should be executed. Default: * (any)
Day of Week	Integer	Day of the Week (0-6 Sunday to Saturday) when a task should be executed. Default: * (any)

Note: a cli file is a text file which only contains Nodegrid cli commands.

Scheduler Date and Time examples:

Table 43: Run a task every day at 00:01

Minute	1
Hour	0
Day of Month	*
Month	*
Day of Week	*

Table 44: Run a task at 23:45 Every Saturday

Minute	45
Hour	23
Day of Month	*
Month	*
Day of Week	6

Table 45: Run every hour on the hour

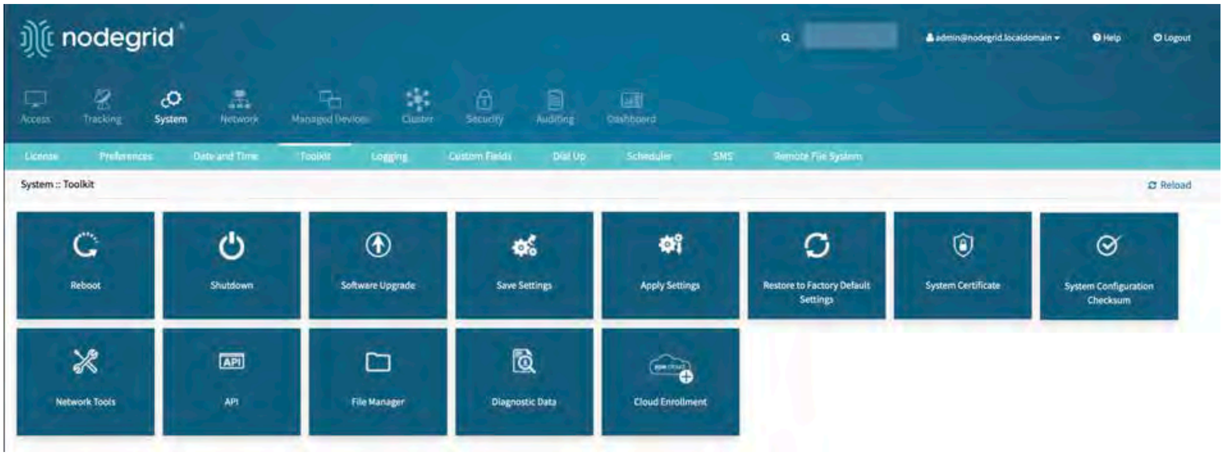
Minute	0
Hour	*
Day of Month	*
Month	*
Day of Week	*

System Maintenance

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
- Diagnostic Data
- Cloud Enrollment



Reboot & Shutdown

Reboot and Shutdown commands allow the graceful shutdown and reboot of Nodegrid. The system will show a warning message that all active sessions will be dropped.

During a reboot of the unit, the operating system will be automatically restarted. 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, by either turning off the power supplies or removing the power cords from the unit. To turn the unit back on, the power supply will need to be stopped and then restarted.

Software Upgrade

There are three methods for upgrading software:

- From the device itself
- From the computer connected to the device
- From a remote server

The ISO image of the new software must be previously loaded on those specific places.

- To upgrade from the Nodegrid device itself, place the new software ISO file in `/var/sw`.
- To upgrade from your local computer connected to the Nodegrid, click on the `Local Computer` radio button and select the file to be used for upgrading.
- To upgrade from a remote server, click on `Remote Server` radio button and enter the URL of the server, as well as username and password as required. FTP, TFTP, SFTP, SCP, HTTP, and HTTPS protocols are supported. The Server address can be the IP address or hostname/FQDN. If using IPv6, use brackets [ ].

For example:

```
ftp://192.168.22.21/downloads/Nodegrid_v4.1.0_20191225.iso
```

If downgrading, you can choose to apply factory default configuration or to restore a saved configuration.

Save Settings

The current configuration can be saved in the Nodegrid itself, to the local computer connected to the device, or to a remote server. Give any (meaningful) name to the configuration, it will be saved to the "/backup" directory.

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

Apply Settings

Saved configurations can be loaded from the Nodegrid itself, from the local computer connected to the device, or from a remote server and applied on Nodegrid which becomes the new configuration of the unit. The server address can be the IP address or hostname/FQDN. If using IPv6, use brackets [...].

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

Restore to Factory Default Settings

The Nodegrid solution offers multiple options to reset the unit back to factory default settings. This option is used to restore all configuration to factory default, by resetting all configuration files back to factory default. The user can choose to clear all log files or not.
The system can also be reset to factory defaults by pressing down the `RST` button on the chassis for at least 10 seconds. In this case, all configuration files are reset to there default state and the log files are cleared.

> ** Note:** Reset to factory default through the `RST` button requires a minimum ET version of 80814T00. See `About` information for the current version.

The system can also be reset by reformatting the whole system partition. This will wipe all existing files and reset the system back to a state in which it was shipped in. See “Software Upgrade” on page 185

System Configuration Checksum

Use this feature to create a checksum baseline of a specific current configuration. This provides administrators a quick tool to verify periodically if the configuration has changed. Click to compare running configuration to the saved baseline; the main result will be "Passed" if all configuration matches (all "OK"), and will fail if there is a change detected, pinpointing the altered place.

MD5 and SHA256 are currently supported.

System Certificate

A certificate can be loaded from the local computer connected to Nodegrid or from a remote server. If loading from the local computer, select the file or enter the URL of the remote server as well as the username and password.

WARNING: When the certificate is applied, the web server will be restarted and may disconnect active sessions.

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

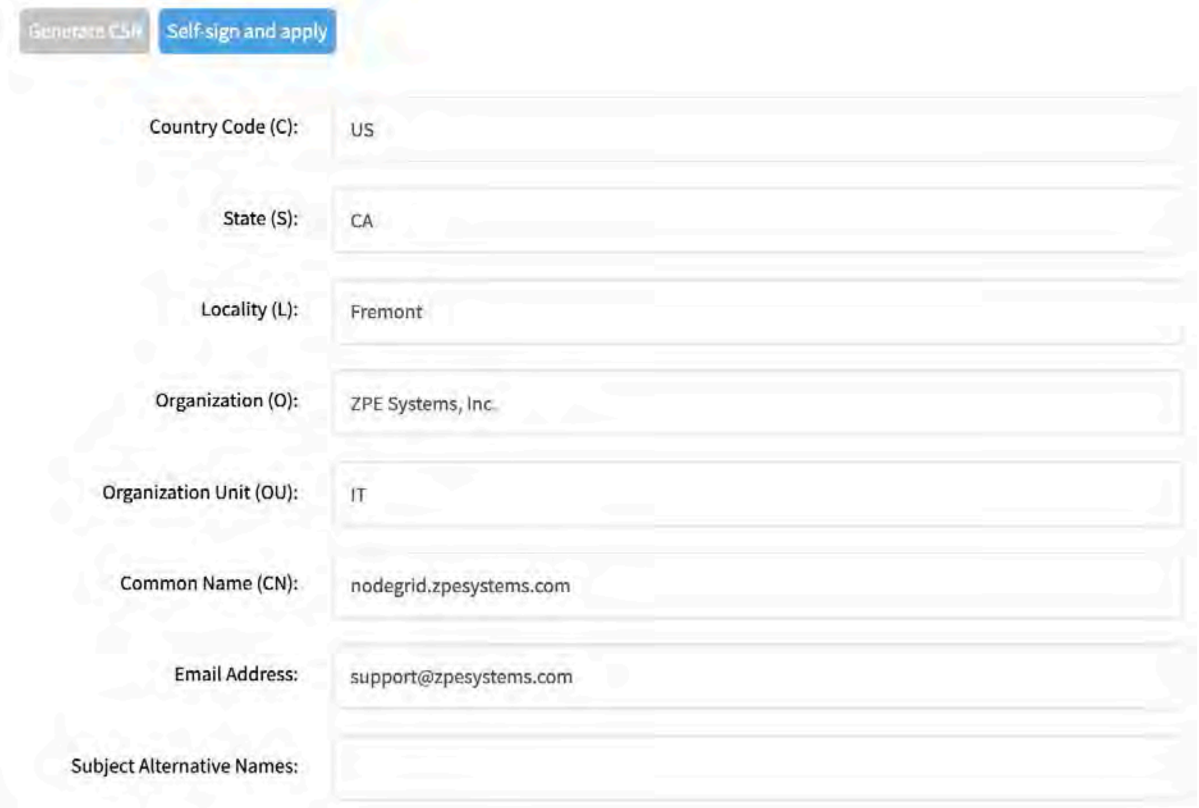
Creating a Self-Sign Certificate

A self-sign certificate can be created and applied directly in the Nodegrid. To create a self-sign certificate:

1. Navigate to `System::Toolkit::Create CSR`
2. Fill in the following information:
    - Country Code (C)
    - State (S)
    - Locality (L)
    - Organization (O)
    - Organization Unit (OU)
    - Common Name (CN)
    - Email Address

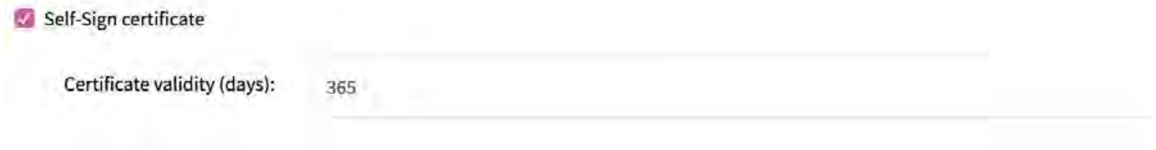
Optional

- Subject Alternative Names



Country Code (C):	US
State (S):	CA
Locality (L):	Fremont
Organization (O):	ZPE Systems, Inc.
Organization Unit (OU):	IT
Common Name (CN):	nodegrid.zpesystems.com
Email Address:	support@zpesystems.com
Subject Alternative Names:	

3. Check the Self-Sign certificate check box
4. Enter the desired time frame into the Certificate validity (days) dialog box



☑ Self-Sign certificate

Certificate validity (days): 365

5. Click the Self-sign and apply button
6. The page will reload after 10 seconds and the certificate will be applied

Network Tools

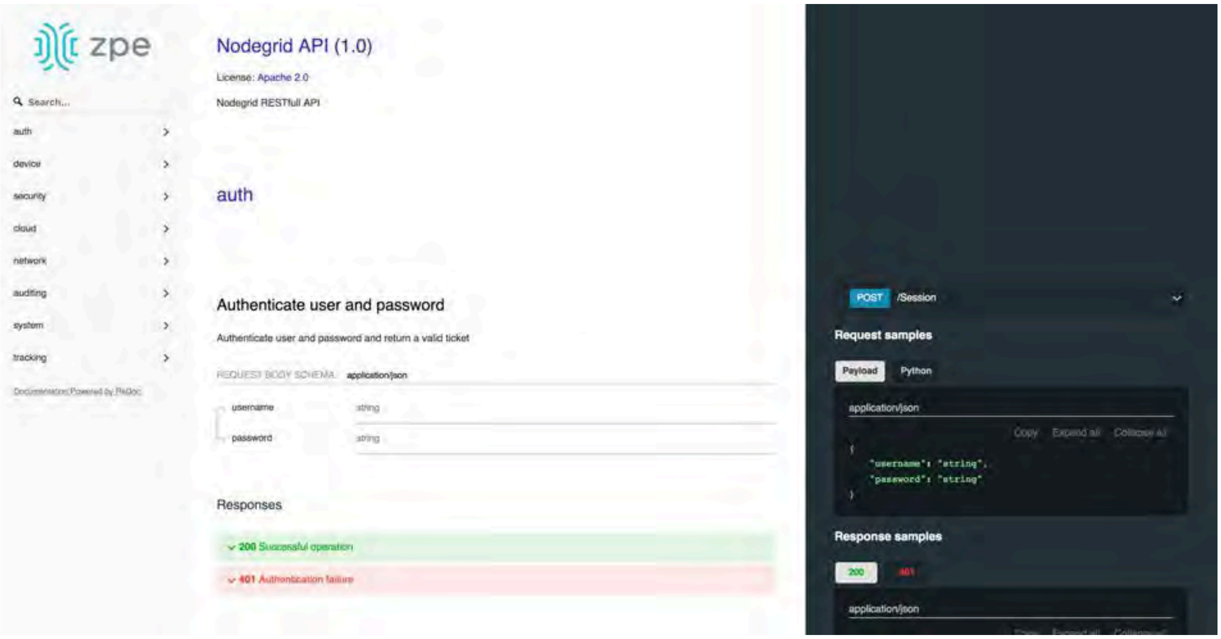
This page provides essential network tools such as "ping", "traceroute" and "DNS lookup", similar to using the command line. Command output is displayed in the lower part of the page.

API

RESTful API

The Nodegrid platform provides a RESTful API, which can be used to read and change and Nodegrid configuration. The API documentation is embedded on Nodegrid and it is available

under `System::Toolkit ::API` or from the pull-down USER menu in the top right corner of the main WEB page (pull-down and click on "API Documentation").
Scroll down to reveal several examples of API requests and responses.



Nodegrid API (1.0)

License: Apache 2.0

Nodegrid RESTfull API

auth

Authenticate user and password

Authenticate user and password and return a valid ticket

REQUEST BODY SCHEMA: application/json

username	string
password	string

Responses

200 Successful operation

401 Authentication failure

POST /Session

Request samples

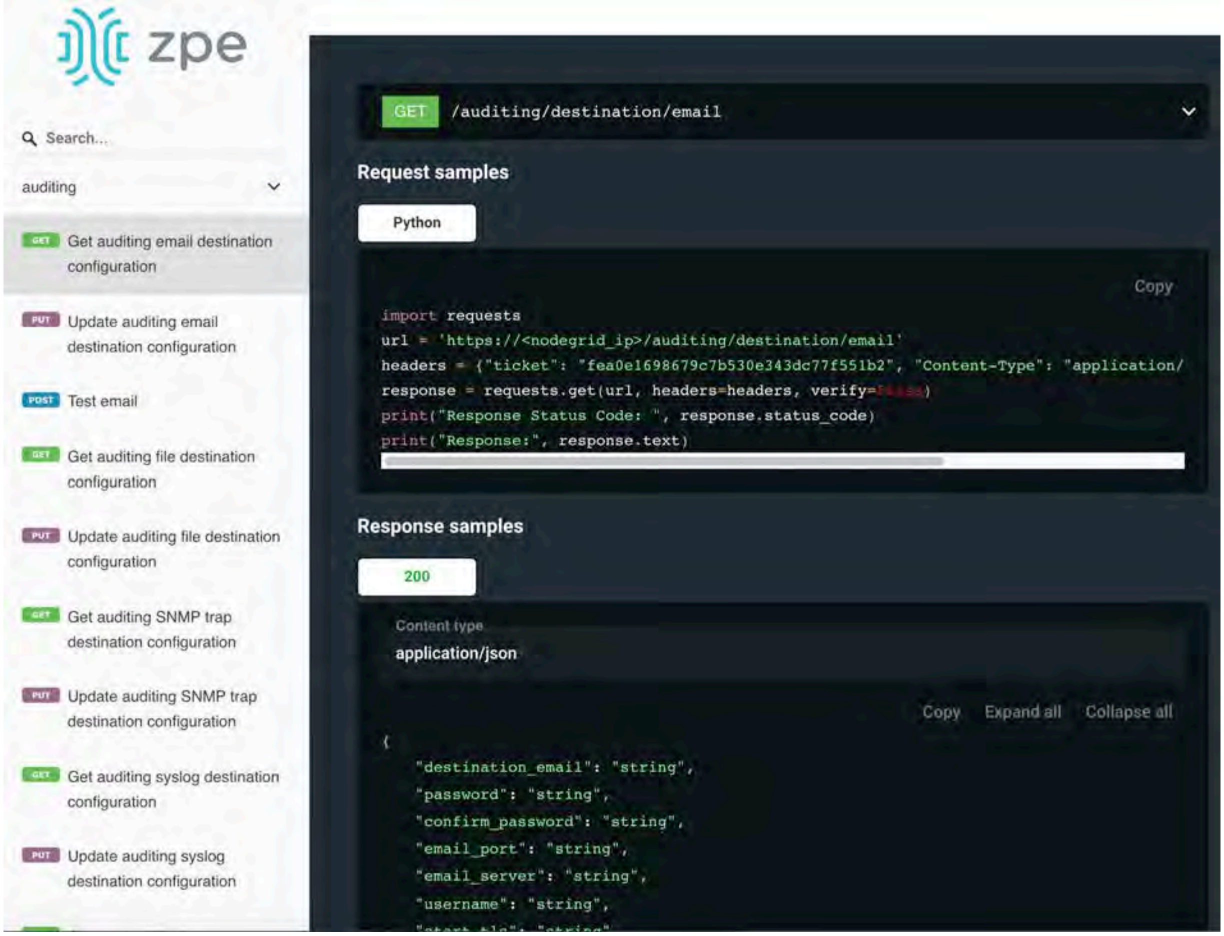
application/json

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

Response samples

application/json

Example "get auditing email destination configuration"



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

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

Content type
application/json

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

Note: The API documentation can be found on each Nodegrid platform under `https://<Nodegrid IP>/api_doc.html`

gRPC

The Nodegrid Platform supports the gRPC framework. The service is disabled by default. To enable the gRPC support see “Active Services” on page 262

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

The Nodegrid implements 4 service definitions:

- get_request (APIRequest) - Allows reading data, returns (APIReply)
- post_request (APIRequest) - Allows executing commands or add an entry, returns (APIReply)
- put_request (APIRequest) - Allows executing commands that need an entry selected or update an entry, returns (APIReply)
- delete_request (APIRequest) - Allows to delete existing data sets or to destroy a session, returns (APIReply)

All APIRequest expect 3 arguments:

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

All 3 arguments follow the same structure as the existing REST API's, see `https://<Nodegrid IP>/api_doc.html` for more details

All APIReply return 2 arguments:

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

Basic Examples:
post_request - Authentication - Returns a session ticket

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

get_request to get network connection details

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

post_request to add a phone number to the sms whitelist

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

put_request to update an existing value on the sms whitelist

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

delete_request to delete an existing value on the sms whitelist

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

SMS Triggered Actions

Users can run actions remotely on Nodegrid via an SMS incoming message. The SMS message authentication must be valid and only allowed actions are executed. This feature requires a cellular connection capable of SMS messaging and it is available on units with the cellular module installed in.

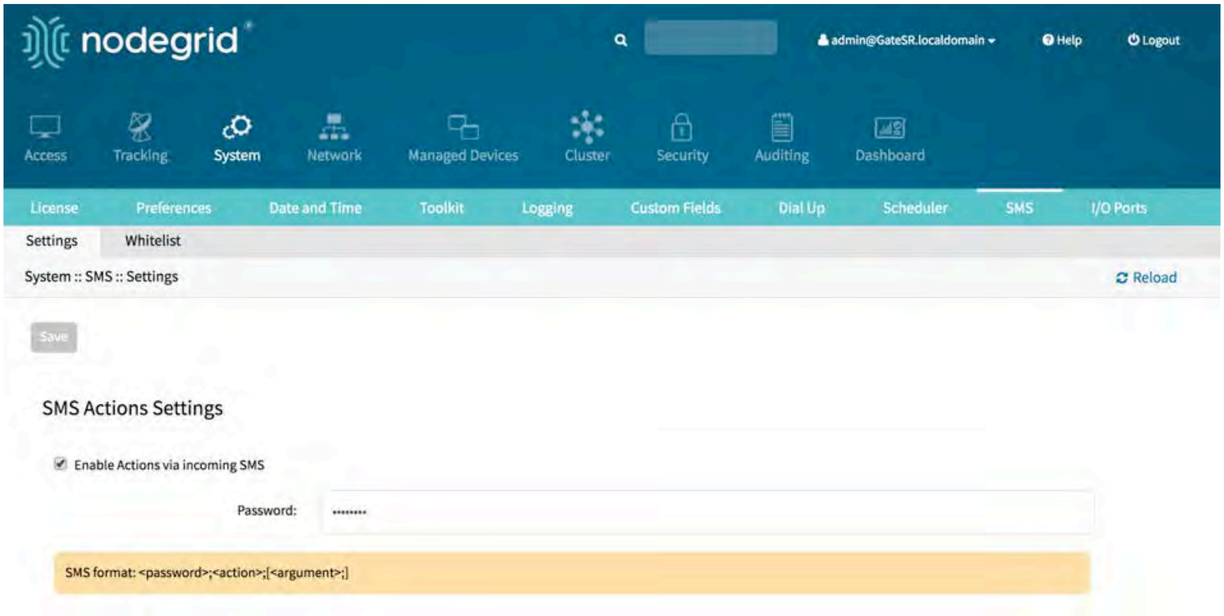
This feature is supported on SMS capable models such as Nodegrid Services Router, Bold SR, Gate SR and Link SR loaded with M2-Card EM7565 M2/wireless modem. By default, the `Enable Actions via incoming SMS` is `Disabled`. When this is enabled in the default state (no password), Nodegrid will accept SMS triggered Actions from all phone numbers, and uses the MAC address of ETH0 as the default password.

> Note: The SMS option requires that the SIM card and plan is 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 if this is required.

SMS Settings

Table 46: SMS Settings

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	allows to 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	current modem status is returned
reset - reset wireless modem	True/False	triggers a reset of a modem
info - request information about Nodegrid	True/False	about information are returned
factorydefault - factory default Nodegrid	True/False	a factory default of the Nodegrid appliance is triggered
reboot - reboot Nodegrid	True/False	a reboot of the Nodegrid is triggered



System :: SMS :: Settings

SMS Actions Settings

☑ Enable Actions via incoming SMS

Password: ••••••••

SMS format: <password>;<action>;[<argument>;]

SMS Actions and Messages Examples

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

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

```
1. connect: try to power on data connection:
< password >;connect;
Connect action started;
```

```
2. disconnect: drop current data connection
< password >;disconnect;
Disconnect action started;
```

```
3. reset: reset wireless modem
< password >;reset;
Modem Reset will start soon;
```

```
4. apn: configure temporary APN
< password >;apn;<new apn>;
```

```
5. 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 >
```

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

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

```
8. reboot: reboot Nodegrid
< password >;reboot;
Nodegrid will reboot soon;
```

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

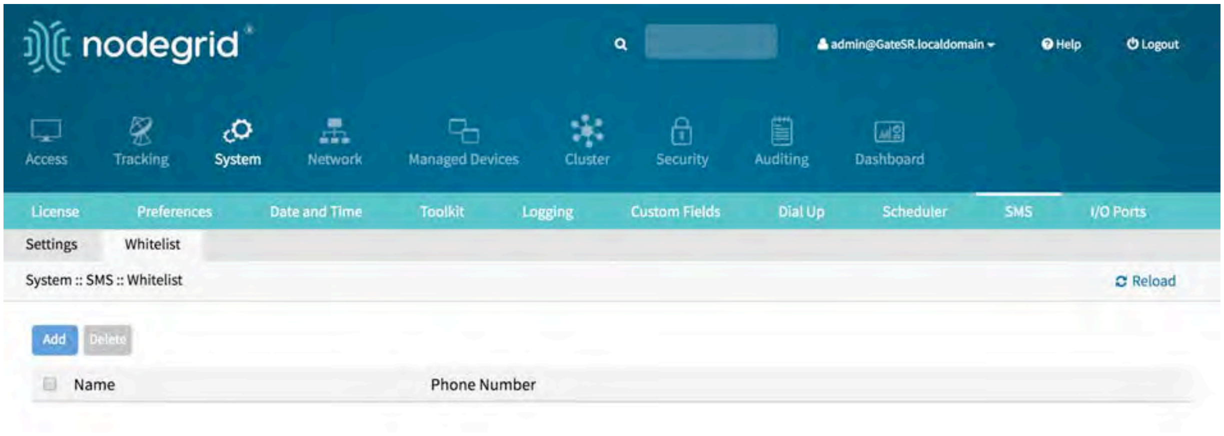
SMS Whitelist

The SMS Whitelist table allows administrators to add, delete, or change phone numbers which are allowed to send SMS action triggers. Requests from all other phone numbers will be ignored. To add an entry to the whitelist click on `Add` and enter items to be whitelisted.

Table 47:

SETTING	VALUE	DESCRIPTION
Name	String	Name
Phone Number	Phone Number	Allowed Phone Number

Note: If the whitelist table is empty then requests from all phone numbers will be accepted.

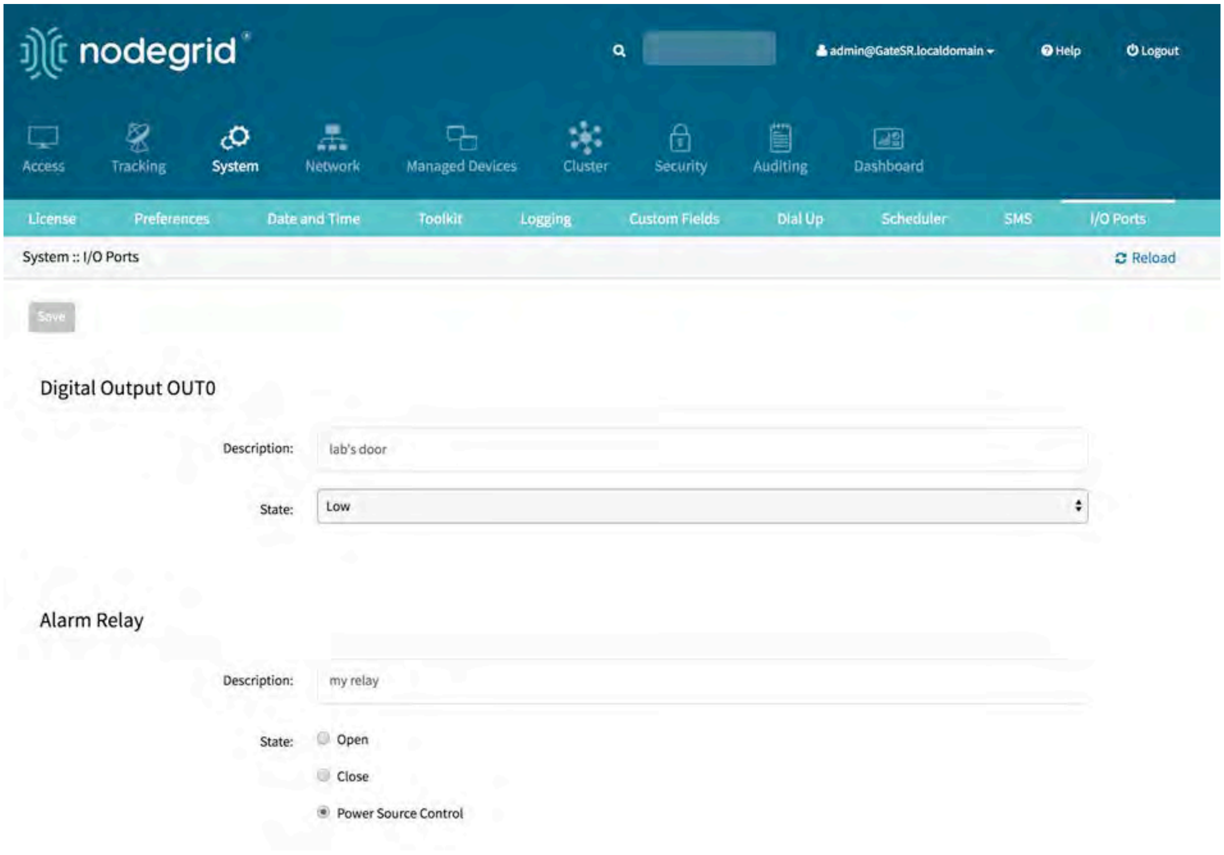


System :: SMS :: Whitelist

Name	Phone Number

Digital I/O

In Nodegrid models equipped with GPIO (Digital I/O ports), there will be an `I/O Ports` tab in `System :: I/O Ports`. This page allows setting the state of digital outputs, as well as the configuration of DIO0 and DIO1 as input or output. When DIO0/DIO1 is configured as output, the state can be set to **Low** or **High**



System :: I/O Ports

Digital Output OUT0

Description: lab's door

State: Low

Alarm Relay

Description: my relay

State: ○ Open ○ Close ● Power Source Control

Network

The Network menu allows administrators to configure and adjust all network-related settings, like configuring the network, LTE, WIFI interfaces or configuring bounding or VLAN details.

Settings

The Network Settings menu allows administrators to define the units host and domain name, configure Network Failover between multiple interfaces, enable IP Forwarding and to configure a loopback address.

Hostname and Domain Name

The units hostname and domain name can be 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.

For each failover setting can an administrator define the following settings:

Table 48: Failover Settings

SETTING	OPTIONS	DESCRIPTION
Primary Connection	Interfaces	List of all available network interfaces. One needs to be selected
Secondary Connection/ Tertiary Connection	Interfaces	List of all available network interfaces. One needs to be selected
Trigger	• Unreachable Primary Connection IPv4 • Default GatewayUnreachable IP address	Based on the setting the system will either check the availability of the default gateway or of an address which can be specified
Number of failed retries to failover	Number	Amount of failed tries to reach the trigger address. This value will be used to trigger a failover.

Table 48: Failover Settings

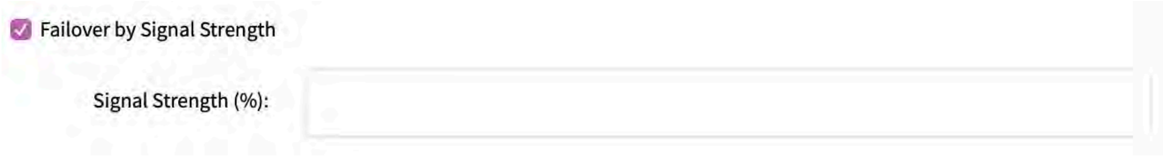
SETTING	OPTIONS	DESCRIPTION
Number of successful retries to recover	Number	Number of successful tries to reach the trigger address. This value will be used to trigger a fallback.
Interval between retries (seconds)	Number	Amount of time which will be waited between tries

The Nnodegrid system supports the configuration of a Dynamic DNS for failover interfaces.

Network Failover for Wireless Connections

Additional failover options are available for wireless connections. These include the following:

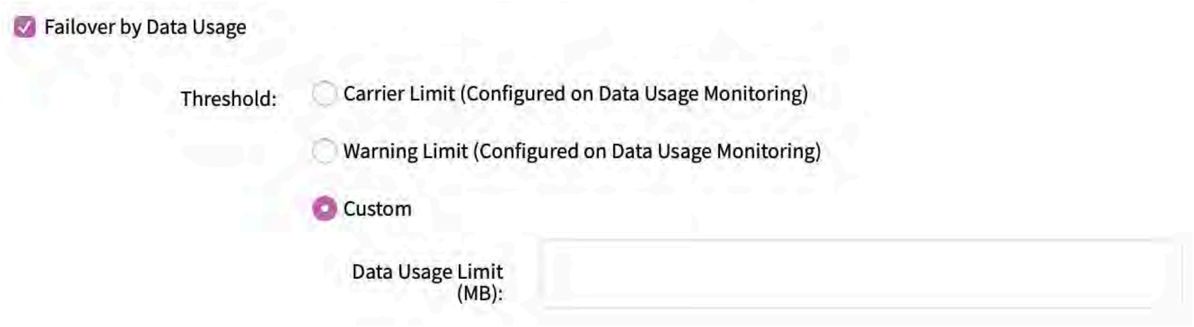
- **Failover by Signal Strength** - Triggered when the signal strength drops below a user definable percentage



☑ Failover by Signal Strength

Signal Strength (%):

- **Failover by Data Usage** - Triggered when one of the following limits are met:
  - Carrier Limit
  - Warning Limit
  - Custom (Data Usage Limit (MB))



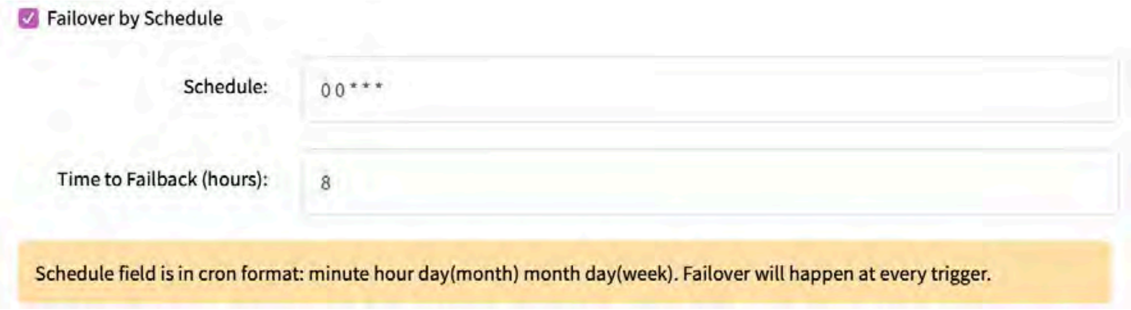
☑ Failover by Data Usage

Threshold: ○ Carrier Limit (Configured on Data Usage Monitoring)
○ Warning Limit (Configured on Data Usage Monitoring)
● Custom

Data Usage Limit (MB):

Note: See “Note: An APN (provided by your 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" on page 205 for details on how to configure Carrier and Warning limits.

- **Failover by Schedule** - Triggered based on a set schedule



☑ Failover by Schedule

Schedule: 0 0 * * *

Time to Failback (hours): 8

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:" on page 184 for schedule format examples.

IPv4 and IPv6 Profile

IP Forwarding

IP Forwarding can be used to route network traffic between network interfaces. The behavior of the routing traffic can be further adjusted using firewall settings.

IP Forwarding can be enabled independently for IPv4 and IPv6.

Loopback Address

The Nodegrid system allows you to configure a Loopback address for IPv4 and IPv6 if required. The address configured is assigned with a bitmask of /32 (IPv4) or /128 (IPv6).

Reverse Path Filtering

The `Reverse Path Filtering` settings allows admins to configure the Reverse Path Filtering behavior of the Nodegrid device. By default, Nodegrid sets it to the Strict Mode which is recommended for most environments as it provides protection against some forms of DDoS attacks.

It might be necessary to change this value in case dynamic routing protocols or in other specific network setup scenarios. The following options are available:

Table 49: Reverse Path Filtering Options

VALUE	DESCRIPTION
Disabled	No source address validation is performed.

Table 49: Reverse Path Filtering Options

VALUE	DESCRIPTION
Strict Mode	Each incoming packet to the Nodegrid is tested against the routing table and if the interface represents the best return path. In case the packet can not be routed or is not the best return path it gets dropped.
Loose Mode	Each incoming packet is tested against the route table only. In case the packet can not be routed it gets dropped. This allows for asymmetric routing scenarios.

Multiple Routing Tables

Nodegrid supports multiple routing tables which allows for assigning specific routing details to specific network interfaces or IP clients. This feature is enabled by default. Administrators have the option to disable the feature if required.

Network Connection Configuration

The network connection configuration allows administrators to edit, to add, and delete existing network configurations. The Nodegrid solution will automatically add all existing physical interfaces. The following physical interfaces exist, depending on the model.

Table 50: Physical Interfaces

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

For each interface the administrator may define the following settings

Table 51: Physical Interface Settings

SETTINGS	DESCRIPTION
Description	Interface Description
Set as Primary Connection	Defines the interface as the primary connection for the unit, 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 to be used for the interface, available areNo (IPv4/IPv6) AddressDHCP (IPv4)Address Auto Configuration (IPv6)Stateful DHCPv6Static (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	Defines a static IP gateway, if the mode is set to static (Optional)
(IPv4/IPv6) DNS Server	Defines a DNS Server to be used for this connection Defines a static IP gateway, if the mode is set to static (Optional)
(IPv4/IPv6) DNS Search	Defines a domain name which will be used for DNS lookups

Additional interfaces can be defined to the existing physical interfaces which allow for more advanced configuration options. The following interface types are supported.

Table 52: Supported Interface Types

INTERFACE	DESCRIPTION
Bonding	Allows the Bonding of multiple interfaces for Failover purposes
Ethernet	Allows the configuration of additional physical interfaces
Mobile Broadband GSM	Allows the configuration of available LTE modem connections
VLAN	This option allows the configuration of VLAN interfaces, which are bound to physical interfaces
WiFi	This option allows the configuration of WIFI interfaces as WIFI client or hotspot. By default, a WiFi interface already exists with the name `hotspot`

Table 52: Supported Interface Types

INTERFACE	DESCRIPTION
Bridge	Allows the creation of a Bridge interface of one or multiple physical interfaces

Bonding Interfaces

Bonding interfaces allow the system to bond two physical network interfaces to one interface. All physical interfaces in the bond will then act as one interface. This allows for an active failover between the two interfaces in case a physical connection to an interface is interrupted. The built-in feature Network Failover can be used for the same purpose. The main difference is that the built-in feature Network Failover works on the IP layer and allows for more functionality. A bonding interface works on the link layer.

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

For each bonding interface, the administrator may define normal network settings like IP address, bitmask and the following specific settings.

Table 53: Bonding Interface Options

SETTING	DESCRIPTION
Primary Interface	Primary network interface
Secondary Interface	Secondary network interface

Table 53: Bonding Interface Options

SETTING	DESCRIPTION
Bonding Mode	Allows to set the Bond mode to be used. Valid options are: • **Round Robin** (0) - Transmit packets in sequential order from the first available slave through the last. • **Active Backup** (1) - Only one slave in the bond is active. A different slave becomes active if, and only if, the active slave fails. • **Balance XOR** (2) - Transmit based on the selected transmit hash policy. • **Broadcast** (3) - Transmits everything on all slave interfaces. This mode provides fault tolerances. • **802.3ad/LACP** (4) - 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. • **Balance TLB** (5) - Adaptive transmit load balancing: channel bonding that does not require any special switch support. The 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. • **Balance ALB** (6) - Adaptive load balancing. Includes balance-tlb plus receive load balancing (rlb) for IPV4 traffic, and does not require any special switch support. The receive load balancing is achieved by ARP negotiation.
Link Monitoring	Allows the Link monitoring mode to be specified, valid options areMIIARP
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. Value needs to be defined for ARP mode.

Table 53: Bonding Interface Options

SETTING	DESCRIPTION
ARP validate	Allows defining which interfaces to use for the ARP validation, options areNoneActiveBackupAll
Bond Fail-over-MAC policy	Allows to define the MAC address failover policy, possible values arePrimary InterfaceCurrent Active InterfaceFollow Active Interface
Primary Interface	Primary network interface

Ethernet Interfaces

Additional Ethernet interfaces can be added and configured after additional physical interface are added to the system. This might be the case 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 unit. The Nodegrid SR family (NSR, GSR, BSR, and LSR) support built-in modems which are 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 which is most commonly used for failover options. Users and remote systems can directly access the device through a mobile connection if this is supported by the ISP.

Note: The build-in modems support Active-Passive SIM failover. The settings for SIM-2 are only supported for the built-in modems.

Table 54: 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	This option allows a 2nd SIM card to be configured.
Active SIM card	Allows the definition of the primary SIM card, which will be used
SIM-2 User name	User name to unlock the SIM

Table 54: Mobile Broadband GSM Interface Options

SETTING	DESCRIPTION
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

Note: An APN (provided by your 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**

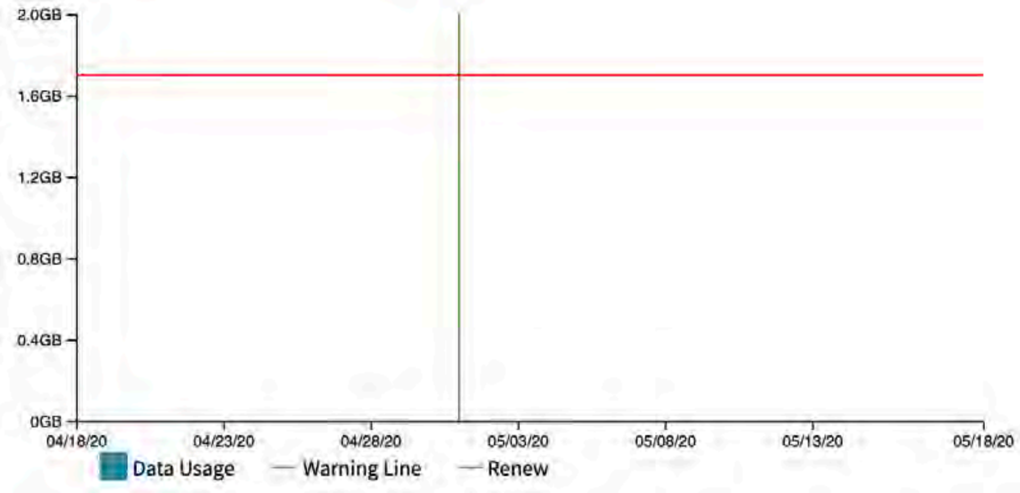
Enable Data Usage Monitoring

You may enable Data Usage Monitoring to trigger an alarm once your mobile data usage has reached a set percentage of your monthly allowance.

To enable Data Usage Monitoring:

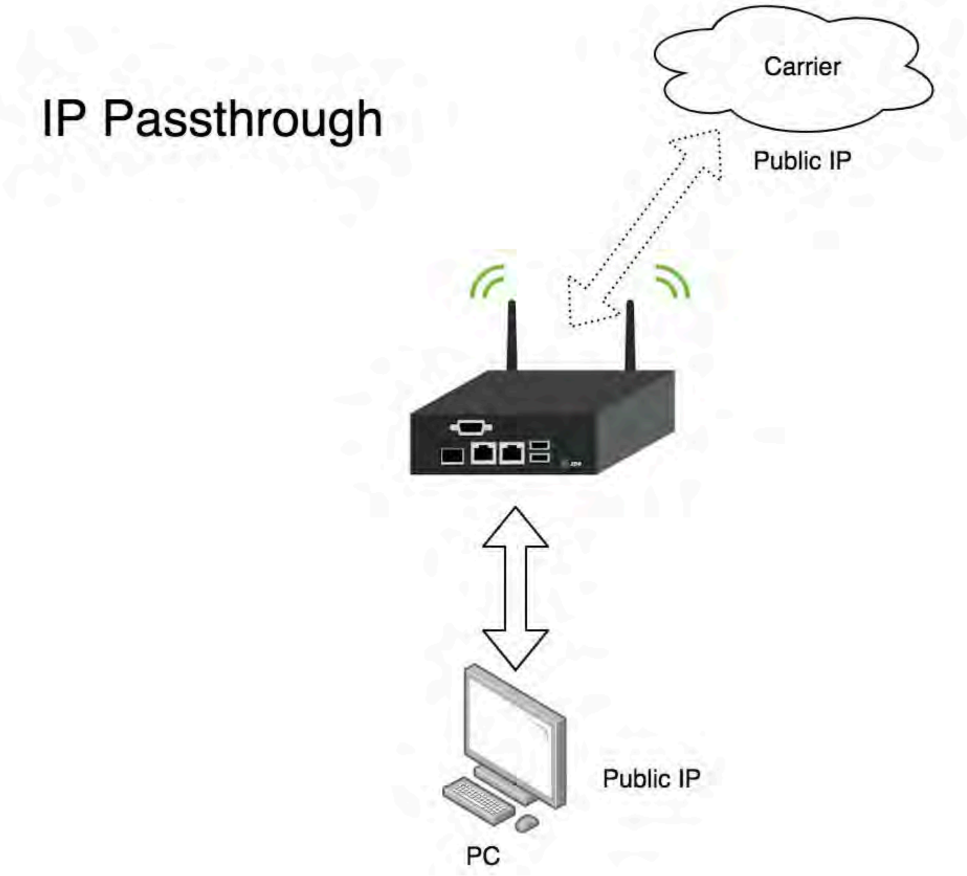
1. Navigate to `Network::Connections`
2. Click on the Mobile Broadband GSM connection where you wish to enable Data Usage Monitoring
3. Check the Enable Data Usage Monitoring check box
4. Fill in the following:
    - **SIM-1 Data Limit Value (GB)** - This is the monthly data limit
    - **SIM-1 Data Warning (%)** - This is the percentage at which you want to trigger an alarm
    - **SIM-1 Renew Day** - This is the day you want the accumulated data to reset
5. Click Save

A graph will be shown with lines set based on the parameters entered



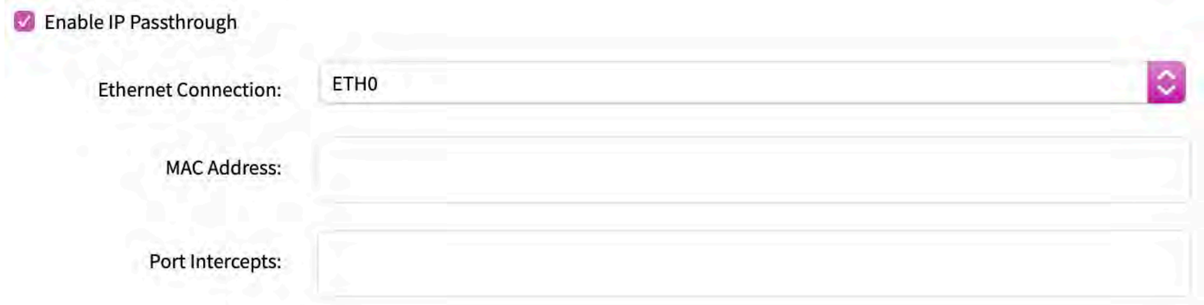
Enable IP Passthrough

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



To enable IP Passthrough:

1. Navigate to `Network::Connections`
2. Click on the Mobile Broadband GSM connection where you wish to enable IP Passthrough
3. Check the Enable IP Passthrough check box
4. Select the desired Ethernet Connection from the drop-down menu



☑ Enable IP Passthrough

Ethernet Connection:	ETH0
MAC Address:	
Port Intercepts:	

The following options are available:

Table 55: IP Passthrough Options

ITEM	DESCRIPTION
MAC Address	Enter the MAC address of the target device. If left empty, the system will use DHCP to get the target device.
Port Intercepts	Enter any ports that should **NOT** pass through the Nodegrid.

5. Click save

VLAN Interface

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

WIFI Interface

The Nodegrid solution supports the use of a Nodegrid as a WiFi client or access point. For this, a compatible WiFi module needs to be installed.

WIFI Access Point

By default, a `hotspot` interface is defined which will configure the Nodegrid solution as an access point if a WiFi module is present.

To use the Nodegrid as an Access Point, change the existing values to the desired new values

WIFI Client

To use the Nodegrid a WiFi client, you must first disable the existing `hotspot` connection by navigating to its settings and disabling the `Connect Automatically` option. Ensure that the `hotspot` interface is down at this point.

A new WiFi interface can now be created which will allow the Nodegrid to act as a client.

WIFI Settings

The Wifi configuration currently supports `No Security` or `WPA2 Personal` security configuration options.

The following WiFi specific settings are available.

Table 56: 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 the security to be set up to either No SecurityWPA2 Personal
WPA shared key	If WPA2 Personal is defined as security, then a shared key can be defined

Bridge Interface

Bridge Interfaces allow the system to create a virtual switch which crosses one or more interfaces. The switch is completely transparent to the network interfaces and does not require any additional setup. The most common use for a bridge network is to provide easy network access for any NFV running on the Nodegrid solution, with the outside as well as with the Nodegrid system itself.

Bridge network interfaces allow the same network configuration options as all Ethernet interfaces. The following options may be defined.

Table 57: Bridge Network Options

SETTING	DESCRIPTION
Bridge Interfaces	a comma-separated list of physical interfaces
Enable Spanning Tree Protocol	allows to enable the Spanning Tree Protocol for the interface
Hello Time (sec)	The number of seconds a HELLO packet is sent. The setting is used when Spanning Tree is enabled.
Forward Delay (sec)	Allows defining a packet forward delay. The setting is used when Spanning Tree is enabled.
Max Age (sec)	Allows defining maximum age for packages. The setting is used when Spanning Tree is enabled.

Analog Modem Interface

The analog modem interface allows administrators to configure an existing analog modem and the required PPP connection details. To configure this option successfully, a supported analog modem needs to be connected to the Nodegrid system.

The following settings can be configured:

Table 58: Analog Modem Options

SETTING	DESCRIPTION
Status	the status defines the connection status, options are Enabled or Disabled
Device Name	name of the detected modem, example `ttyUSB0`
Speed	The serial connection speed to the modem
PPP Dial-Out Phone Number	
Init Chat	This option allows defining a specific AT init string if this is required
PPP Idle Timeout (sec)	The settings define the connection idle timeout after which the connection gets automatically disconnected. 0 sec indicates that the connection does not get automatically disconnected.
PPP IPv4/ IPv6Address	This setting allows the definition of IPv4 addresses for the PPP connection the following options are availableNo AddressLocal Configuration - allows the configuration of a local and remote IP addressAccept Configuration from Remote Peer
PPP Authentication	This setting allows the definition of PPP authentication options. Possible options areNoneBy 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

The static routes feature allows the definition and management of static routes. Routes can be created for IPv4 and IPv6 and are assigned to specific network interfaces. The following options exist.

Table 59: Static Route Options

SETTING	DESCRIPTION
Connection	Allows the selection of the network connection to which the route will be associated with
Type	Allows the definition of the IP type. Options areIPv4IPv6
Destination IP	Allows the definition of the destination IP or network
Destination BitMask	Allows the definition of the associated bitmask in the form of xxx.xxx.xxx.xxx or xx Example: 255.255.255.0 24
Gateway IP	Allows the definition of the gateway address

Table 59: Static Route Options

SETTING	DESCRIPTION
Metric	Allows the definition of the routing metric value. Normal routes have a default value of 100

Manual Hostnames

The hostname feature allows the configuration and management of manual hostname definitions, which is equivalent to entries in the host's file.

Table 60: Manual Hostname Options

SETTING	DESCRIPTION
IP Address	allows the definition of the target hosts IP address. IPv4 and IPv6 formats are supported
Hostname	allows the definition of the hostname of the target
Alias	allows the definition of additional hostname aliases

DHCP Server

The DHCP function allows the configuration and management of a DHCP server for target devices. The DHCP server is not configured or active by defualt. After a DHCP scope is defined, the system will start serving IP addresses to all target devices which are connected to the interface and which match the general DHCP scope.

The configuration of the DHCP server is a two-step process. First, the general DHCP scope and configuration is configured and created. Next, IP address ranges (`Network Range`) are defined which will be used to server IP addresses as well as IP address reservations (`Hosts`) for specific hosts.

Table 61: DHCP Server Options

SETTING	DESCRIPTION
SubNet	IP address subnet network which will be used. This has to match the configuration of a configured interface.
Netmask	The network mask for the defined subnet in the format xxx.xxx.xxx.xxx
Domain	allows defining the domain name for the scope
Domain Name Servers (DNS)	allows the definition of DNS servers for the scope
Router IP	allows the definition of a default gateway for the scope

Table 61: DHCP Server Options

SETTING	DESCRIPTION
Network Range - IP Address Start	allows the definition of the first IP address which will be severed
Network Range - IP Address End	allows the definition of the last IP address which will be served
Hosts - Hostname	allows the definition of a hostname for IP address reservation
Hosts - HW Address	allows the definition of a MAC address to which an IP address reservation applies
Hosts - IP Address	allows the definition of an IP address which will be assigned to specific host matching the defined MAC address

Network Switch Configuration

The Nodegrid Server Router appliance enables users to configure the built-in network switch. Advanced network configuration for each network enable card and port are availble. Currently supported functions include the enabling and disabling of individual ports, and 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. The interfaces Backplane0/1 and SFP0/1 are active by default and can be used to provide or consume ZTP, PXE and DHCP requests by default. All other network interfaces are disabled by default.

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

Switch Interfaces

The switch interfaces provide an overview of all switch ports, their current status, and allow enabling, disabling, show the current VLAN associations (Tagged and Untagged), and to configure Port VLAN IDs.

The Port VLAN ID will be assigned to all incoming untagged packets. The Port VLAN ID will then be used to forward the packets to other ports which match that VLAN ID.

The switch port interface will clearly identify the VLAN interfaces to which a port belongs. For most scenarios, a port is either an untagged port, which is the equivalent to an access port, or a tagged port, which is the equivalent to a trunk port.

VLAN Configuration

The VLAN options allow administrators to create, delete, and manage VLAN's and assign ports to them as needed. By default, VLAN 1 and VLAN 2 exist. All ports belong by default to VLAN 1 except BACKPLANE1 and SFP1 which belong by default to VLAN2.

Untagged/Access Ports

To assign a port to a specific VLAN as an untagged or access port, you may enable the port and then changing the PORT VLAN ID to the desired VLAN. By doing this, the port will automatically be assigned to VLAN and untagged port.

Note: the VLAN needs to exist before the port can be assigned to it

Tagged/Trunk Ports

Tagged ports allow incoming packets to carry VLAN tags. Tagged ports will accept any packet which belongs to an assigned VLAN. They are mostly used to create a trunk connection between multiple switches. To assign a port as a tagged port, a minimum of 1 VLAN needs to be added to a port as tagged VLAN. This can be done through the VLAN configuration. The Port VLAN ID for a tagged port should match one of the assigned VLANs or should be blank. In this case, no untagged traffic will be accepted by the port.

Note: the VLAN needs to exist before the port can be assigned to it

Backplane Ports

The backplane settings control the switch interfaces which are exposed to the Nodegrid platform directly. For the Nodegrid to communicate with any of the existing switch ports or VLANs, at least one of the backplane interfaces has to be part of the specific VLAN. The backplane settings display the current VLAN associations and allow to set the Port VLAN ID's for the backplane interfaces.

VPN

The Nodegrid solution supports multiple VPN options, which allow the system to act as VPN servers or Clients in a variety of different scenarios. The system currently supports SSL VPN Client and Server options as well as IPSec configuration options for a host to host, site to site and others. Support for IPsec with asymmetric PSL auth support for IKEv2 tunnel is also available.

SSL VPN

Nodegrid supports a wide variety of SSL configuration options, and the system can act as either an SSL Client or SSL Server depending on the customer configuration and security needs.

SSL VPN CLIENT

The SSL VPN client configuration option is mostly used for failover scenarios, whereby a main secure connection fails over to a less secure connection type. The VPN tunnel is then used to secure the traffic between the sides. When the Nodegrid is configured as an SSL VPN client, the configuration gets bound to a network interface (optional) and the VPN tunnel will automatically be established as soon as the bounded interface is starting. Multiple Client configurations can be added supporting different connection and interface details.

> Note: Depending on the configuration multiple files are required, which have to be present before the configuration can be completed. All files need to be placed in /etc/openvpn/CA

Table 62: SSL VPN Client Options

SETTING	DESCRIPTION
Name	connection name
Network Connection	allows selecting the network interface to which the tunnel will be bound.
Gateway IP Address	IP address or FQDN of the SSL VPN server
Gateway TCP Port	TCP port which will be used for the connection, the default value is 1194
Connection Protocol	supported connection protocols areUTPTCP
Tunnel MTU	MTU size for the tunnel interface
HMAC/Message Digest Alg	allows selecting the HMAC connection algorithm from a list
Cipher Alg	allows selecting the connection cipher algorithm from a list
Use LZO data compress Algorithm	Can be enabled to support data compression
Authentication Method	allows to define the user authentication method, options are TLSStatic KeyPasswordPassword plus TLS
TLS - CA Certificate	CA Certificate used by the SSL Server
TLS - Client Certificate	The certificate which is recognized by the SSL Server
TLS - Client Private Key	Client Certificates Private key
Static Key - Secret	The secret to be used

Table 62: SSL VPN Client Options

SETTING	DESCRIPTION
Static Key - Local Endpoint (Local IP)	Local IP address for the VPN connection
Static Key - Remote Endpoint (Remote IP)	The 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 which is recognized by the SSL Server
Password plus TLS - Client Private Key	Client Certificates Private key

SSL VPN SERVER

Nodegrid can be configured to act as an SSL VPN server. By default, the server is disabled. After the server is configured and started, it provides the SSL Server Status page and overview of the general server status and connected clients.

Note: Depending on the configuration multiple files are required, which have to be present before the configuration can be completed. All files need to be placed in /etc/openvpn/CA

Table 63: SSL VPN Server Options

SETTING	DESCRIPTION
Status	Default value is `Disabled` this setting needs to be set to `Enabled` to start the server after it is fully configured
Listen IP address	This setting allows to the definition of a listening IP address if defined the server will only respond to client requests coming in on this interface.
Listen Port number	this setting defines the listening port for incoming connections. The default value is `1194`
Protocol	this value defines the protocol to be used options available areUDPTCP
Tunnel MTU	allows defining the MTU used for the tunnel. The default value is `1500`
Number of Concurrent Tunnels	allows defining the total amount of concurrent SSL client sessions. The default value is `256`
IP Address	This section allows the definition of the IP address settings for the tunnel options available areNetworkPoint to PointPoint To Point IPv6
IP Address - Network - IPv4 Tunnel(NetAddr Netmask)	Allows the definition of an IPv4 network address and network mask which will be used for the tunnel
IP Address - Network - IPv6 Tunnel(NetAddr/ Bitmask):	Allows the definition of an IPv4 network address and network mask which will be used for the tunnel
IP Address - Point-to-Point - Local Endpoint (Local IP)	Allows the definition of a local IPv4 IP address for a Point to Point connection
IP Address - Point-to-Point - Remote Endpoint (Remote IP)	Allows the definition of a remote IPv4 IP address for a Point to Point connection

Table 63: SSL VPN Server Options

SETTING	DESCRIPTION
IP Address - Point-to-Point IPv6 - Local Endpoint (Local IP)	Allows the definition of a local IPv6 IP address for a Point to Point connection
IP Address - Point-to-Point IPv6 - Remote Endpoint (Remote IP)	Allows the definition of a remote IPv6 IP address for a Point to Point connection
Authentication Method	This allows selecting the desired authentication method, available options areTLSStatic KeyPasswordPassword plus TLS
TLS - CA Certificate	allows selecting the CA certificate to be used
TLS - Server Certificate	allows selecting the server certificate to be used
TLS - Server Key	allows selecting the private key belonging to the server certificate
TLS - Diffie Hellman	allows selecting the Diffie Hellman key
Static Key - Secret	allows selecting the secret to be used
Static Key - Diffie Hellman	allows selecting the Diffie Hellman key
Password - CA Certificate	allows selecting the CA certificate to be used
Password - Server Certificate	allows selecting the server certificate to be used
Password - Server Key	allows selecting the private key belonging to the server certificate
Password - Diffie Hellman	allows selecting the Diffie Hellman key
Password plus TLS - CA Certificate	allows selecting the CA certificate to be used

Table 63: SSL VPN Server Options

SETTING	DESCRIPTION
Password plus TLS- Server Certificate	allows selecting the server certificate to be used
Password plus TLS- Server Key	allows selecting the private key belonging to the server certificate
Password plus TLS- Diffie Hellman	allows selecting the Diffie Hellman key
HMAC/Message Digest	allows selecting the HMAC connection algorithm from a list
Cipher	allows selecting the connection cipher algorithm from a list
Min TLS version	The expected connection TLS minimum version. Supported values areNoneTLS 1.0TLS 1.1TLS 1.2TLS 1.3
Use LZO data compress Algorithm	When enabled all tunnel traffic with be compressed
Redirect Gateway (Force all client generated traffic through the tunnel)	When enabled all traffic emanating from a client will be forced through the tunnel.

IPSEC VPN

The Nodegrid solution supports the configuration of IPSec tunnels. The system supports a variety of configuration options for a host to host, host to site, site to site and road warrior configurations.

Note: As the Nodegrid node will be directly be exposed to the Internet. Is it strongly recommended securing the appliance. Built-in features can be used for this like:

- Configuring Firewall
- Enabling Fail-2-Ban
- Changing all default passwords with strong passwords
- Disabling services which are not required

Authentication Methods

Multiple Authentication methods are available together with IPSec and the Nodegrid solution. Some of these are very easy to implement, like Pre-Shared keys and RSA keys, but offer limited flexibility in larger setups. Other certificates required more initial configuration and setup, but offer the flexibility and consistency to easily manage and maintain larger setups.

Pre-shared Keys

Pre-shared Keys is the simplest and least secure method to secure an IPSec connection. Pre-shared keys are a combination of characters which represent a secret. Both nodes need to share the same secret. Nodegrid supports pre-shared keys with a minimum length of 32 characters. The maximum length is much higher, but due to compatibility reasons with other vendors, we will use a length of 64 bit for the examples below. In general, 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 manually configured to have each other's RSA keys as part of the configuration.

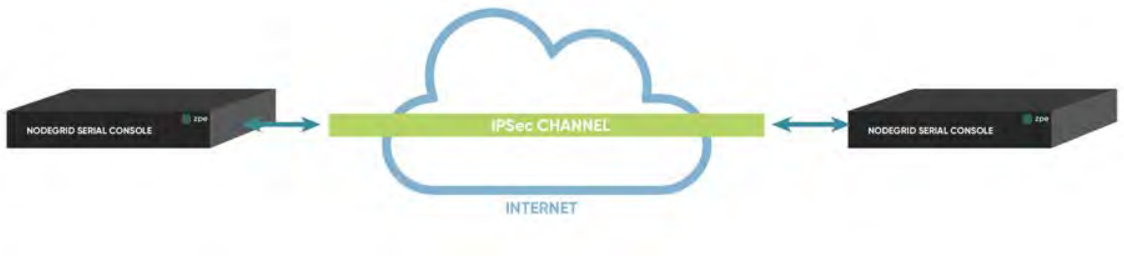
X.509 Certificates

X.509 Certificate authentications are typically 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 is used to maintain the trust relationship between the nodes including revocation of trust for specific nodes. The Nodegrid solution supports both public and private CA's. The Nodegrid Solution may also be used to host and manage its own Certificate Authority for an IPSec communication.

Connection Scenarios

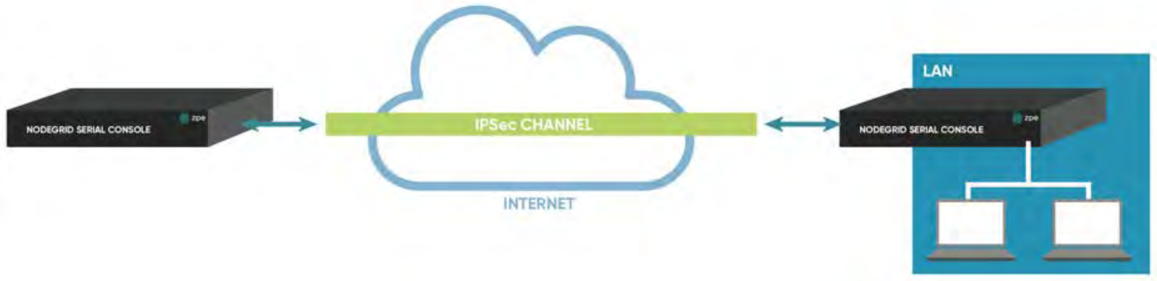
IPSec supports many connection scenarios, starting from communication just between 2 nodes to communication of one node to multiple nodes. Communication may be limited to just the nodes involved, or expanded beyond the directly involved nodes to the networks access table behind the nodes. Examples are provided for some of the most common scenarios.

Host to Host



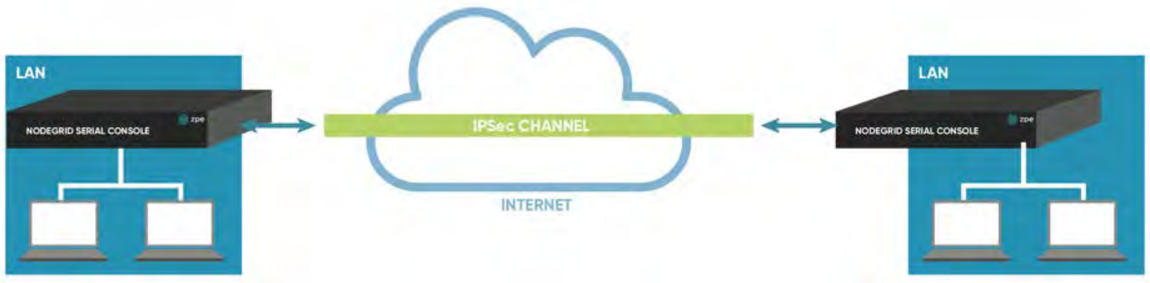
Host to Host communication means that 2 nodes have a VPN tunnel open which connects them directly. The communication which is exchanged through the tunnel is limited to direct communication between them. None of the packages will be routed or forwarded. This is essentially a point-to-point communication between 2 nodes.

Host to Site



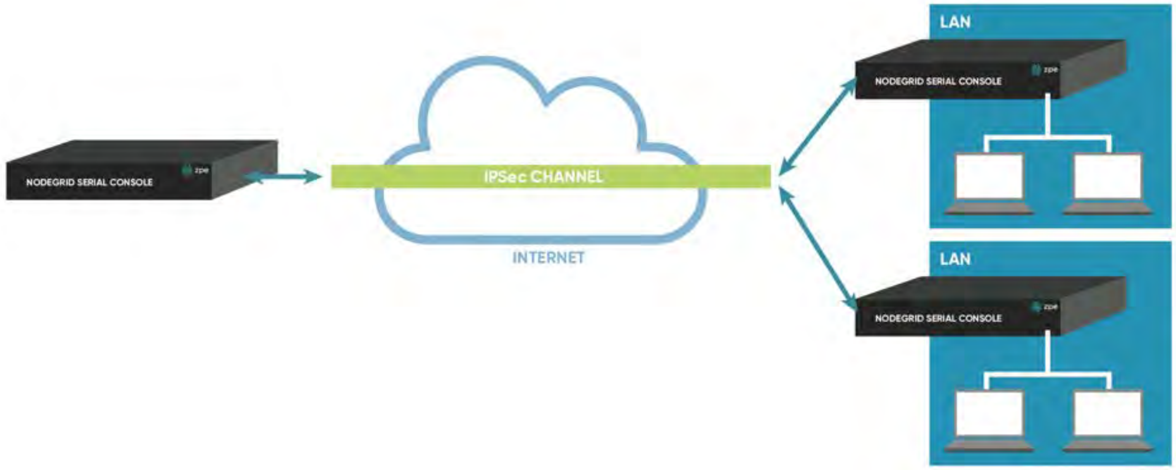
In a Host to Site communication scenario one node establishes a VPN tunnel to a 2nd node. Communication is limited on one site to the specific node and on the other side to all devices in a range of subnet which is accessible by the 2nd node.

Site to Site



In a Site to Site communication, the tunnel is as before established between 2 nodes, communication is allowed to specify the subnet on both sides, allowing for communication between devices on either side of the connection.

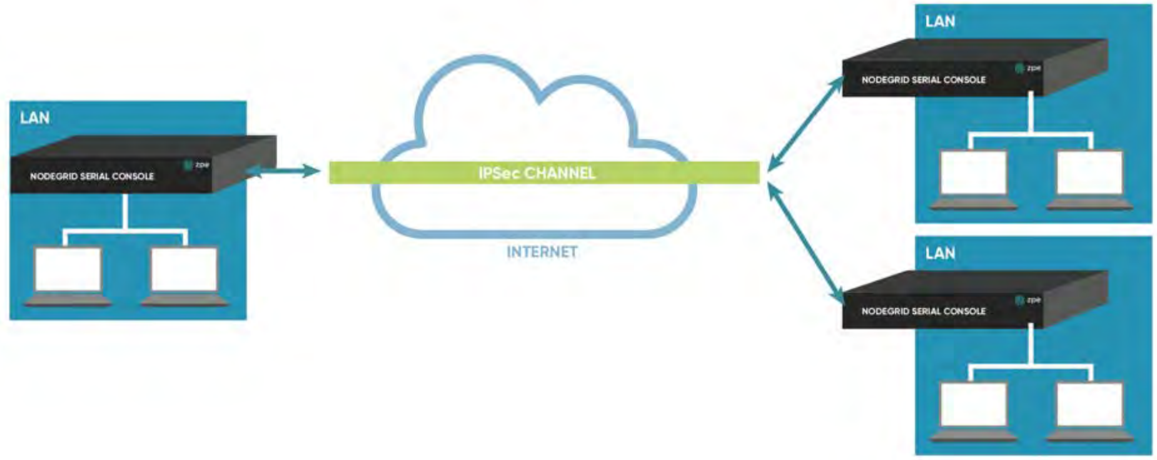
Host to Multi-Site



Multi-Site communication scenarios can be created by either creating individual VPN connections between hosts or by specific multi-site configurations. The later greatly improve scalability and manageability of the connection setup.

Host to multi-site communication allows multiple nodes to connect to the same node. A typical scenario for this would be that remote offices have a VPN connection to the main office. In this specific scenario would the communication be limited to the one node and devices on specified subnets in the remote locations.

Site to Multi-Site



This scenario is normally the most common form for enterprise VPN setups. It is similar to the Host to multi-site option, but communication is allowed to the specific subnet on either side, whereby the West node would have access to all specified subnet on any of the sites but the remote sites have only access to subnet exposed by the West node.

Table 64: 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

Configuration of IPSec

This section outlines the general configuration steps which can be used to configure the desired connection.

- To prepare the Nodegrid see: How to Prepare a Nodegrid Node for IPSec
- 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. Pre-Shared Keys are easy to set up and are a good starting point for test environments.

- 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
- Distribute and exchange configuration files and Keys as required to all nodes
- Test the connection

For more detailed instruction on how t use IPSec with the Nodegrid solution, visit our Knowledge Base.

Advanced Network Features

VRRP (Virtual Router Redundancy Protocol) Support

The Nodegrid platform supports embedded Virtual Router Redundancy Protocol (VRRP). This protocol allows the Nodegrid to become part of a virtual router interface, which allows for redundancy of a router. This is mostly used to provide automatic failover support for default gateways. By default, the protocol is not configured and the service is not running. To enable support, the service must first be configured. This can be done by an administrator using the shell.

> Note: VRRP can only be used with network interfaces which are directly exposed to the Nodegrid OS. Individual switch ports on a Nodegrid Service Router card for example can not be used.

VRRP support is implemented through keepalived services. The official documentation for the service can be found here.

The configuration files for the service are located in `/etc/keepalived/`. At a minimum, the `keepalived.conf` needs to have a valid configuration. The service can then be started using the following command.

```
/etc/init.d/keepalived start
```

To automatically start keepalived on the next system start run the following command

```
update-rc.d -s keepalived defaults 90
```

Authentication

Authentication is the process of validating who you are or who you claim to be, which is usually done using credentials. Credentials most often take the form of a username and password.

Authorization is an essential security feature that complements authentication. Once you are authenticated using your credentials, authorization determines what you have access to, e.g. certain directories, power or serial devices, etc.

Nodegrid has a built-in admin user account named 'admin' with full access and rights to set all configurable aspects of the unit, network, security, authentication, authorization, devices to be managed, including other users. This special user account, 'admin' cannot be deleted and it has the default password 'admin'.

> Note: For security reasons, administrators are strongly advised to change the default password during the first login by using the Change Password option on the pull-down menu under your username in the top right corner of the WebUI.

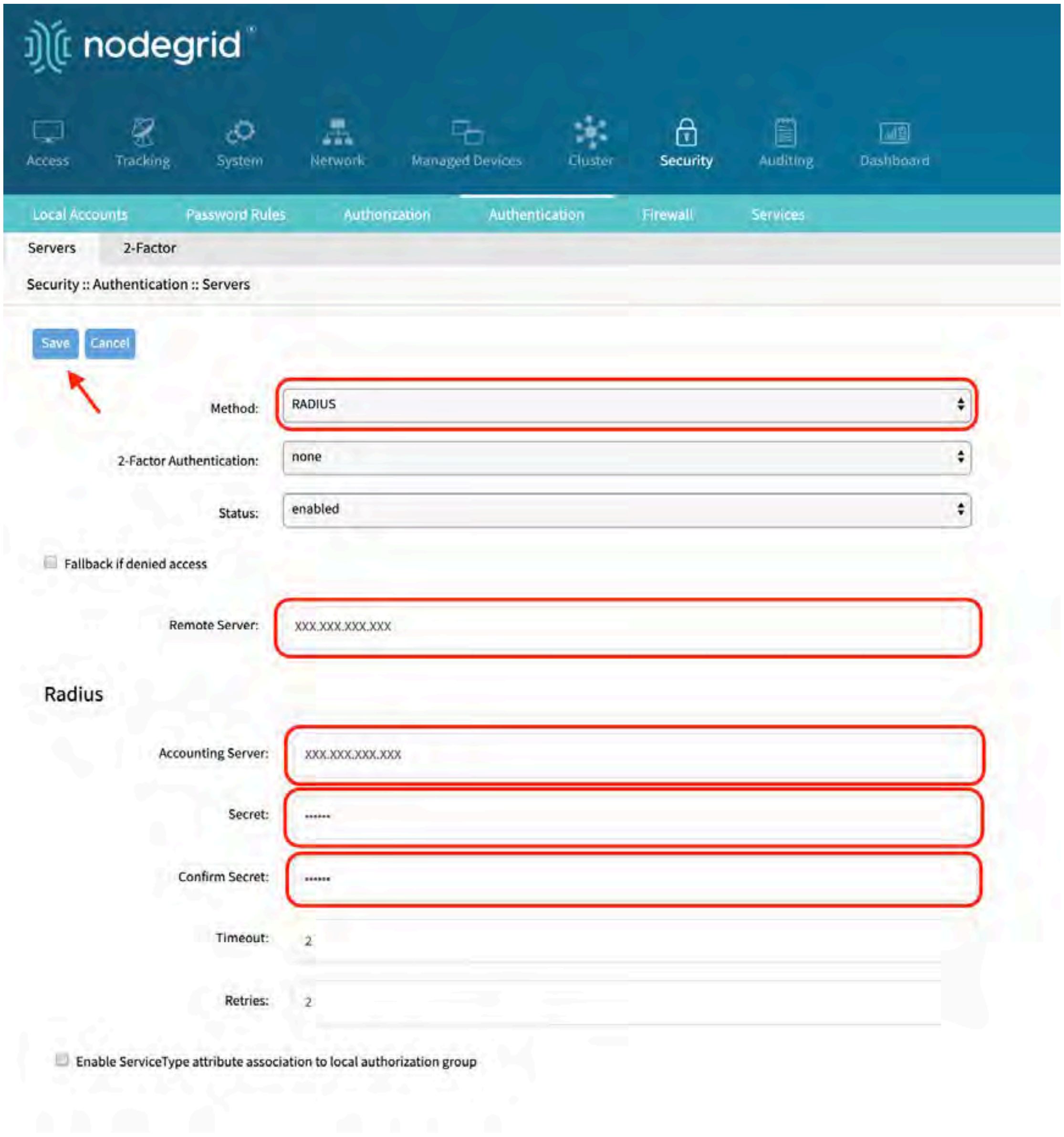
The Nodegrid platform fully the supports Authentication of local users and groups, as well as external users and groups. External authentication of users and groups can be done through LDAP/AD, Tacacs+, Radius and Kerberos.

All users have access to all enabled managed devices by default. Fine Grain Authorization can be enabled by selecting the option `Device access enforced via user group authorization` under `Services`.

Based on the groups they are assigned to, these users have limited access to Nodegrid Web portal management attributes. Privileges of users can be modified by setting profile and access rights in an authorization group. A user who belongs to the Admin group will have the same administrative privileges as the admin user. Each user must have a specific user account on Nodegrid, or on an external authentication server. A user can be assigned to one or more authorization groups.

Add a server

Go to `Security :: Authentication :: Servers` and add some authentication server to associate any server's user to a group.



Security :: Authentication :: Servers

Method: RADIUS

2-Factor Authentication: none

Status: enabled

□ Fallback if denied access

Remote Server: XXX.XXX.XXX.XXX

Radius

Accounting Server: XXX.XXX.XXX.XXX

Secret: ••••••

Confirm Secret: ••••••

Timeout: 2

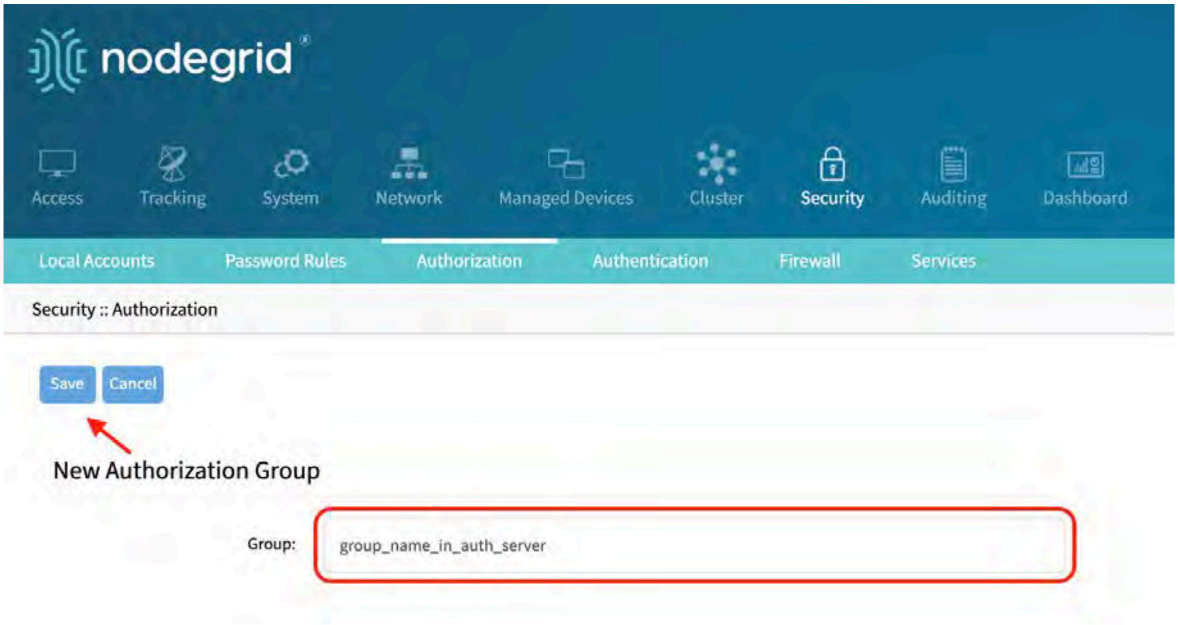
Retries: 2

□ Enable ServiceType attribute association to local authorization group

Add a group

Go to `Security :: Authorization` and click on `Add` button to add a valid group. Remember to add some group that already has users associated with it. Set the following field and save to add a group:

- Group: `group_name_in_auth_server`



Group: group_name_in_auth_server

SSO (Single Sign-On)

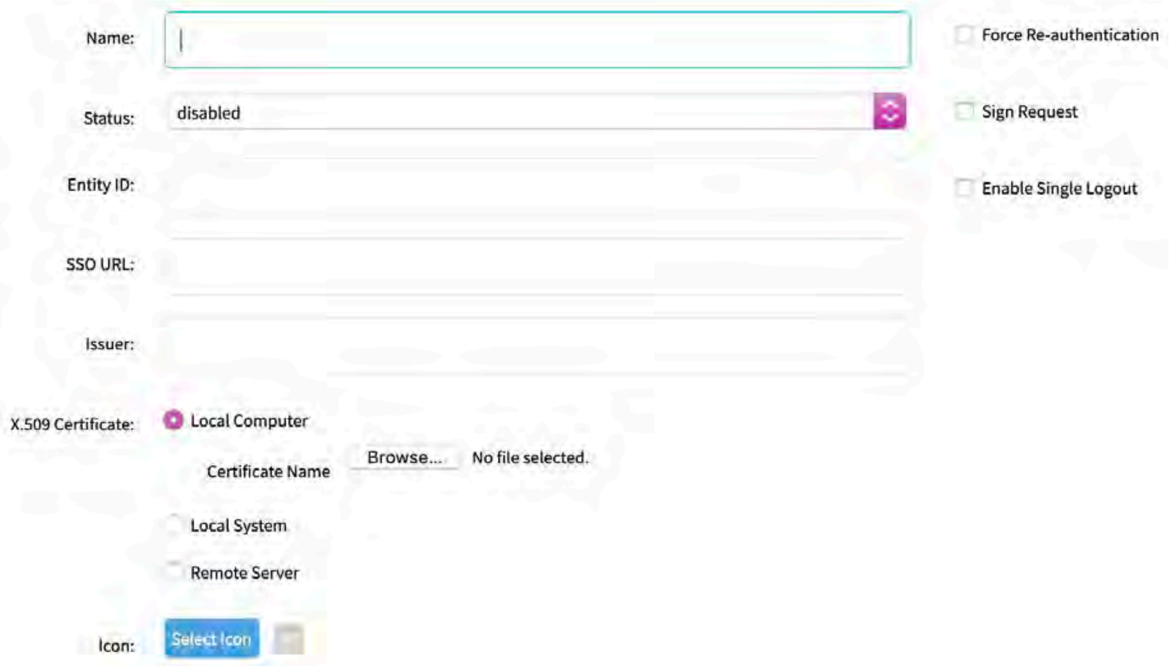
Single Sign-On (SSO) allows users to authenticate once and gain access to multiple secured systems without resubmitting their credentials. Nodegrid currently supports the following Service Providers:

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

To configure SSO:

1. Navigate to `Security::Authentication::SSO`
2. Click Add

3. Fill in the following fields:
    - Name
    - Status
    - Identity Provider
    - SSO URL
    - Entity ID
    - Certificate



Name:

Status: disabled

Entity ID:

SSO URL:

Issuer:

X.509 Certificate: ● Local Computer

Certificate Name Browse... No file selected.

○ Local System

○ Remote Server

Icon: Select Icon

□ Force Re-authentication

□ Sign Request

□ Enable Single Logout

4. Click save

The following fields are required to configure a successful SAML flow for each Identity Provider:

Table 65: SAML Requirments

IDENTITY PROVIDER (IDP)	FIELDS TO COPY FROM NODEGRID TO IDP	FIELDS TO PASTE TO NODEGRID FROM IDP
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

Table 65: SAML Requirments

IDENTITY PROVIDER (IDP)	FIELDS TO COPY FROM NODEGRID TO IDP	FIELDS TO PASTE TO NODEGRID FROM IDP
G Suite	ACS URL Entity ID	SSO URL Entity ID Certificate

Fields to be configured in the IdP

- **Entity ID**: A globally unique name for the SP (URL)
- **Assertion Consumer Service (ACS)**: URL in which the Identity Provider will redirect the user and send the SAML assertion after it is done with 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 is SHA-256.

Fields to be configured in the SP

- **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. Will be used for <ip>/direct/<device>/console.

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

Local Accounts

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 the user accounts. Regardless of activation options, users can change their passwords at any time. This feature lists all users and their respective information.

- User name and password
- Hash format password (optional)
- Account expiration (optional)
- Groups, the user is part of

Manage Local Users

The Management of Local users can be archived under `Security :: Local Accounts`. The following options are available.

- `Add` - New users can be added
- `Edit` - Existing user settings can be changed
- `Delete` - Existing users can be removed
- `Lock` - Existing users can be locked, this will prevent users from login in, without removing the account
- `Unlock` - Existing locked users accounts can be unlocked

Add Local Users

1. Navigate to `Security :: Local Accounts`, all local users are displayed
2. Click on `Add` to display the Local User Information screen
3. Enter a new user name and password
    - If the password is in a hash format tick the `Hash Format Password` checkbox, see Hash Format Password below

Optional:

- Enter Account Expiration Date
- Check the Require password change at login time checkbox

- To add the user to an available user group, choose the group name from the box on the left and then click `Add`.
- To remove a user group from the box, select it and click `Remove`

4. Click save.

Hash Format Password

If you are an admin and prefer to not use a plain password and instead use a hash format password, you can do so by using this feature. This may be of special interest in using scripts, to avoids scripts containing or displaying actual passwords of the users.

Notice hat this requires the hash password to be generated separately beforehand, using a hash password generator of your preference. Examples of popular hash generators in Linux are OpenSSL, chpasswd, mkpasswd, using MD5, SHA256, SHA512, etc..

The Nodegrid can also be used for this purpose, its own OpenSSL implementation. Example using Nodegrid's OpenSSL version.

```
root@nodegrid:~# openssl passwd -1 -salt mysall
Password:
$1$mysall$YBFr9On0wjde5be32mC1g1
```

Password Rules

All local user accounts are subject to password rules. These can be adjusted under `Security::Password Rules`. The administrator can set values for password complexity as well as password expiration, as a set of minimum days, maximum days and warning days.

The following settings can be adjusted:

Table 66: Password Rules Options

SETTING	VALUE	DESCRIPTION
Check Password Complexity	TrueFalse	Enables or Disables, Password complexity rules. The default value is disabled
Password Complexity - Minimum Number of Digits	Number	The minimum amount of digits which need to be included in the password. Default value: 0
Password Complexity - Minimum Number of Upper Case Characters	Number	The minimum amount of upper cases which need to be included in the password. Default value: 0
Password Complexity - Minimum Number of Special Characters	Number	The minimum amount of special characters which need to be included in the password. Default value: 0
Password Complexity - Minimum Size	Number	The minimum amount of characters included in the password. Default value: 8
Password Complexity - Number of Passwords to Store in History	Number	Amount of password stored in the password history. Preventing the reuse of passwords for this amount. Default value: 1
Password Expiration - Min Days	Number	Amount of days the password has to be valid for before it can be changed. Default value: 0
Password Expiration - Max Days	Number	The maximum amount of days a password can be valid for before it has to be changed. Default value: 99999
Password Expiration - Warning Days	Number	Amount of days, users will be notified before their password expires. Default value: 7

Groups

Nodegrid uses user groups to combine multiple local and remote users into a single local group, which is then used to assign system-wide administrative roles/permissions like user permission and administrative permissions. Groups are used to grant access permissions to specific target devices. User Groups which are authenticated against an external authentication provider are mapped to local groups. This will assign the remote groups the permissions of the assigned local group.

Should a user be a member of multiple groups then the combined access rights will take effect.

Administrators can add and delete groups, as well as change their permissions. When you log in to the Nodegrid for the first time, you will see two groups in the default configuration, Admin and Users, which can not be deleted.

Manage Groups

The Nodegrid platform contains two default groups with default permissions. The `admin` grants the admin user full system and target access. The `user` group grants all members full access to all targets if Fine Grain Authorization is disabled (default). In case Fine Grain Authorization is enabled, the `user` group members have no access to any target device by default.

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

Create a User Group

1. Go to `Security::Authorization` to display all groups
2. Click `Add` to enter the new group name and then `Save`

The group has been created. To change its properties and permissions, click on the group name.

Add local users to a group

1. Go to `Security::Authorization` to display all groups
2. Click on the name of the group you want to add members to
3. Click on `Members`. This shows a list of members already in the group.
4. Click on `Add` to show a list of local users that can be added in the left box.
5. Select the user and click on `Add` to move the selected user to this group, in the right box.

Click on `Remove` to remove a selected user in this group and place it back to the local user's box.

Assign system permissions and settings to a group

1. Go to `Security :: Authorization` to display all groups
2. Click on the name of the group you want to add members to
3. Click on `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.

The following system permissions can be assigned:

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

Table 67: System Permissions

PERMISSION	DESCRIPTION
Track System Information	Grants access to tracking information. See section `Tracking`
Terminate Sessions	Grants the permission to terminal user and device sessions
Software Upgrade and Reboot System	Grants Permission to perform system upgrades and reboots
Configure System	Grants administrative 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

The following settings can be configured:

Table 68: System Permission Settings

SETTING	VALUE	DESCRIPTION
Permissions	Track System InformationTerminate SessionsSoftware Upgrade and Reboot SystemConfigure SystemConfigure User AccountApply & Save SettingsShell Access	System Permissions
Restrict Configure System Permission to Read Only	TrueFalse	The granted system settings are visible but cannot be changed
Menu-driven access to devices	TrueFalse	The members of the group will be presented with a target menu when ssh connection directly to the Nodegrid is established.

Table 68: System Permission Settings

SETTING	VALUE	DESCRIPTION
Sudo permission	TrueFalse	Allows users to execute 'sudo commands'
Custom Session Timeout	TrueFalse	Enable a custom session time
Timeout [seconds]	Number	Session timeout in seconds
Startup application	CLIShell	Allows an administrator to set the default start application when a user of this group 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

Assign external groups

External groups need to be assigned to a local group. This will ensure that the remote group gets the correct permissions assigned. To assign an external group, follow the below steps

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

1. Go to `Security::Authorization` to display all groups
2. Click on the name of the group you want to add members to
3. Click on `Remote Groups`
4. List the external group names separated by a comma, which are to be assigned to the local group
5. Click save

Assign device permissions

In case Fine Grain Authorization is enabled, the permissions to access specific devices need to be assigned to groups. This is done by adding specific devices to a group and to set the appropriate access rights to the target. Multiple devices can be added at the same time and the access permissions can be set together.

> Note: access permissions to control power outlets are granted through the `Outlets` permissions and not through `Devices`

1. Access permissions can be added, deleted and edited for each group as necessary
2. Go to `Security::Authorization` to display all groups
3. Click on the name of the group you want to add members to
4. Click on `Devices`

5. Click on `Add`
    - To move managed devices from the available device list on the left to the list of authorized devices on the right, double-click on the name or select the device and then click Add.
    - Devices can be removed from the box on the right, by double-clicking on the device or by clicking on the delete button after selecting the device to be removed
6. Select desired device permissions
7. Click save

The following access permissions can be assigned:

Table 69: Access Permissions

PERMISSION	VALUE	DESCRIPTION
Session	Read-WriteRead-OnlyNo-Access	Permission to access serial or ssh sessions (Console)
Power	Power ControlPower StatusNo Access	Power Control permissions through IPMI
Door	Door ControlDoor StatusNo Access	Door Control permissions
MKS	TrueFalse	Access to MKS sessions
Reset Device	TrueFalse	Permission to reset a device session
KVM	TrueFalse	Access to KVM sessions
SP Console	TrueFalse	Access to IPMI console sessions (Serial over Lan)
Virtual Media	TrueFalse	Access to establish a Virtual Media session to an IPMI device
Access Log Audit	TrueFalse	Access to read the access log of an IPMI device
Access Log Clear	TrueFalse	Permission to clear the access log of an IPMI device
Event Log Audit	TrueFalse	Permission to read the device-specific event log
Event Log Clear	TrueFalse	Permission to clear the device-specific Event Log
Monitoring	TrueFalse	Permission to access monitoring features

Table 69: Access Permissions

PERMISSION	VALUE	DESCRIPTION
Sensors Data	TrueFalse	Permission to read sensor data
Custom Commands	TrueFalse	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` to display all groups
2. Click on the name of the group you want to add members to
3. Click on `Outlets`
4. Click on `Add`
   - To move managed devices from the available device list on the left to the list of authorized devices on the right, double-click on the name or select the device and then click Add.
   - Devices can be removed from the box on the right by double-clicking on the device or by clicking on the delete button after selecting the device to be removed
5. 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
6. Click `Save`

External Authentication Provider

Nodegrid provides an easy and simple way to enable external authentication on the platform. It can be set up to 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)

In order to allow external users access to the Nodegrid platform the, following steps need to be performed independently of the specific authentication provider:

- An Internal group needs to be created
- Permission needs to be assigned to the group
- External Authentication Provider needs to be added, see below
- External groups need to be mapped to an internal group

Authentication providers can be added, deleted, modified in the `Security::Authentication` section. The section will display all currently configured authentication providers and allows the creation, deletion, modification, and order of the authentication providers. The order of the authentication providers determent which one will be used first to authenticate the user. Should the authentication fail, the user access might be rejected or the next authentication provider might be tried. The authentication provider setting `Fallback if denied access` controls this. If the feature is enabled then the next provider will be used. If disabled, user access will be granted or denied based on the result.

> Note: Should a provider not be available to authenticate users at any given time then the provider will be skipped and the next provider will be used.

All users accessing the Nodegrid need to be a member of a group. If a user can not be identified as being a group member then a default group will be used. By default, this is the `user` group. The group which will be used can be adjusted using the `Default Group` option.

The following section outlines how the different external authentication providers are added and configured.

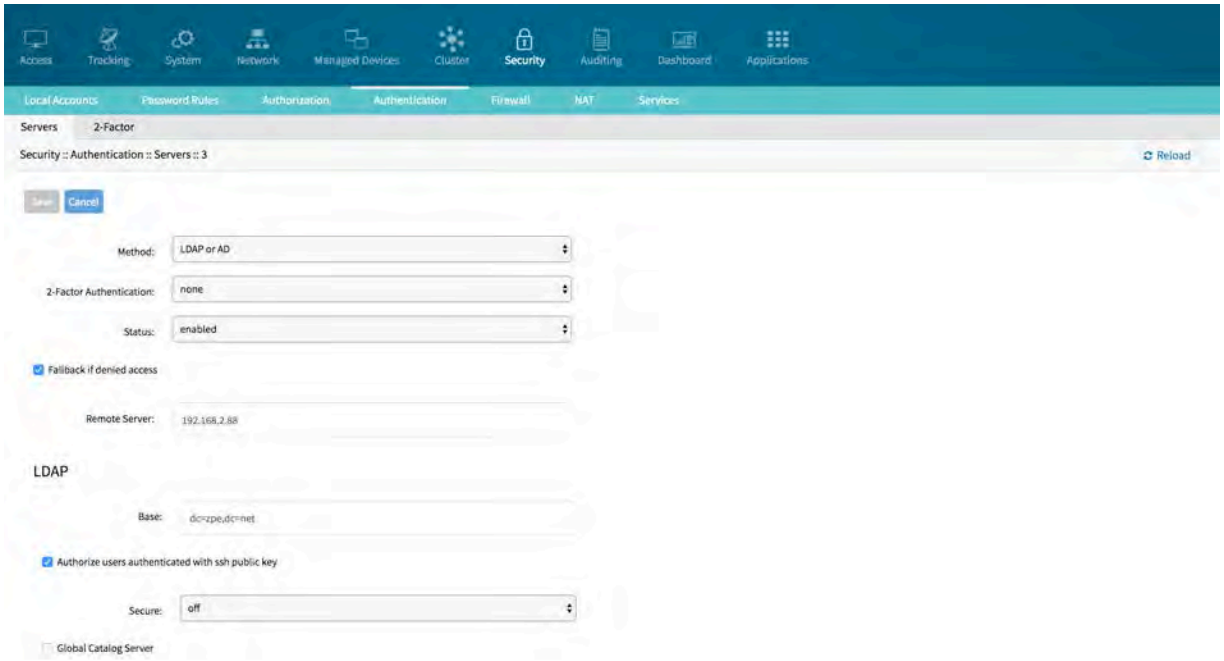
LDAP and Active Directory

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. It allows the implementation of very complex authentication provider structure reflecting the internal organization of companies.

Provide the following information to set up an LDAP or Active Directory authentication server.

Note: This page allows enabling features such as `Fallback if denied access`, `Authorize users authenticated with ssh public key` and `Search Nested Groups (AD only)`.



Security :: Authentication :: Servers :: 3

Method: LDAP or AD

2-Factor Authentication: none

Status: enabled

☑ Fallback if denied access

Remote Server: 192.168.2.88

LDAP

Base: dc=zpe,dc=net

☑ Authorize users authenticated with ssh public key

Secure: off

□ Global Catalog Server

Table 70: LDAP / Active Directory Options

FIELD	VALUES	DESCRIPTION
Status	TrueFalse	Default value is Enabled. This means the provider will be used to authenticate users
Fallback if denied access	Enabled or Disabled	Default is Disabled. It is recommended to Enable this feature in case the provider is not available.
Remote Server	FQDN or IP of LDAP server or domain	Nodegrid supports resolution of Active Directory Servers through DNS requests. This means that either specific Active Directory Servers can be specified or a valid Active Directory Domain. In case of the later, the system will contact the closest Server based on the DNS results.
Base	Base DN	This field can contain the Root DN or a sublevel DN. This DN marks the highest point which will be used to search for users or groups
Authorize users authenticated with ssh public key	Enabled or Disabled	Disabled by Default

Table 70: LDAP / Active Directory Options

FIELD	VALUES	DESCRIPTION
Secure	On, Off or Start_TLS	Default is off, all traffic between the Nodegrid and the LDAP server will be sent unencrypted. On is recommended. (This feature needs to be supported by the Server)
Global Catalog Server	TrueFalse	When enabled that the provider will use an Active Directory Global Catalog Server
Database Username	Search User Name	Full Qualified username, which can be used to search through the directory. Only required if the LDAP server requires authentication for browsing of the directory
Database Password and Confirm Password	Password for the search user	Only required if the LDAP server requires authentication for browsing of the directory
Login Attribute	Field identifies the username	attribute field which contains the username. For Active Directory this is `sAMAccountName` by default.
Group Attribute	Field identifies the group names	Attribute filed which contains the group identifier. For Active Directory this is `memberOf` by default
Search Filter	Search Filter following the LDAP implementation	
Search Nested Groups (AD only)	Enabled or Disabled	Disabled by Default

Example configuration for OpenLDAP server

Table 71: OpenLDAP Example Configuration

FIELD	VALUE
Status	True
Fallback if denied access	True
Remote Server	192.168.1.1
Base	dc=zpe,dc=net

Table 71: OpenLDAP Example Configuration

FIELD	VALUE
Secure	Off
Global Catalog Server	False
Database Username	cn=admin,dc=zpe,dc=net
Login Attribute	cn
Group Attribute	memberUID

Example configuration for Active Directory server

Table 72: Active Directory Example Configuration

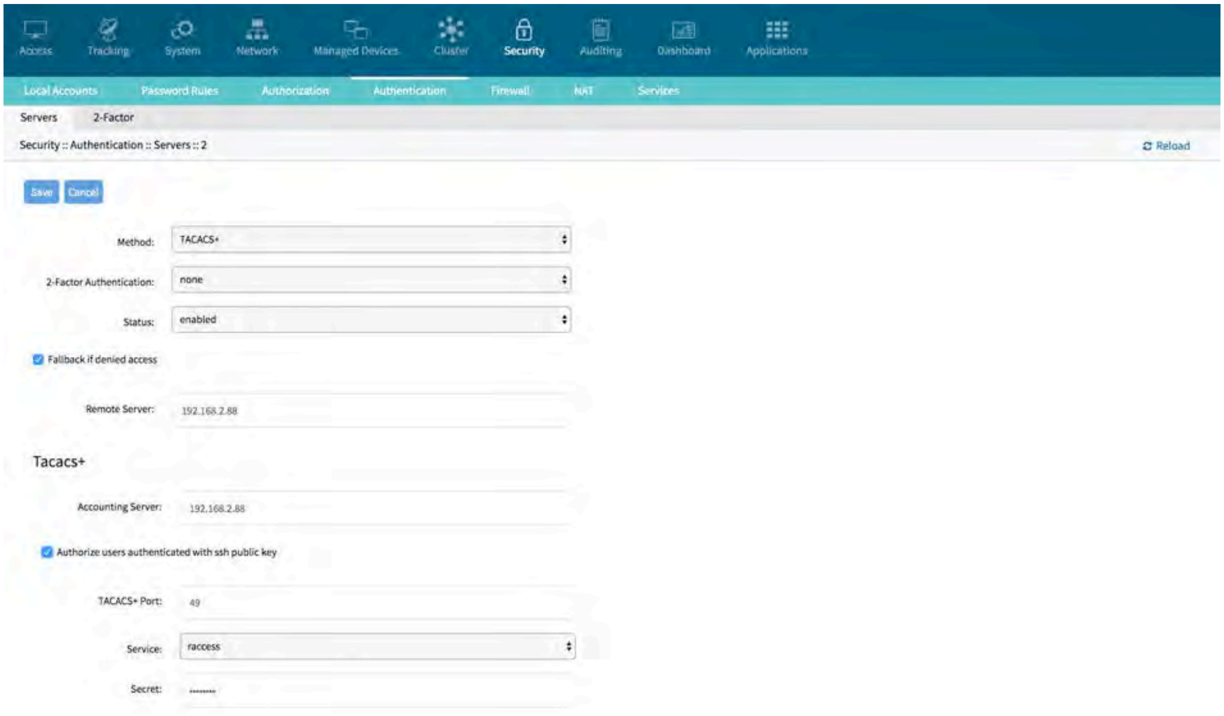
FIELD	VALUE
Status	True
Fallback if denied access	True
Remote Server	192.168.1.1
Base	dc=zpesystems,dc=com
Secure	Start TLS
Global Catalog Server	True
Database Username	cn=Administrator,cn=Users,dc=zpesystems,dc=com
Login Attribute	sAMAccountName
Group Attribute	memberOf

More information on how to setup LDAP and Active Directory can be found in How to Configure Active Directory or LDAP Authentication Provider

TACACS +

Terminal Access Controller Access-Control System Plus (TACACS+) 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 allows to 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`.



Security :: Authentication :: Servers :: 2

Method: TACACS+

2-Factor Authentication: none

Status: enabled

☑ Fallback if denied access

Remote Server: 192.168.2.88

Tacacs+

Accounting Server: 192.168.2.88

☑ Authorize users authenticated with ssh public key

TACACS+ Port: 49

Service: raccess

Secret: ••••••••

Table 73: TACACS+ Options

FIELD	VALUES	DESCRIPTION
Status	EnabledDisabled	Default value is Enabled. This means the provider will be used to authenticate users
Fallback if denied access	Enabled or Disabled	Default is Disabled. It is recommended to Enable this feature in case the provider is not available.
Remote Server	IP address	
Accounting Server	IP address	
Authorize users authenticated with ssh public key	Enabled or Disabled	Disabled by Default
TACACS+ Port	TCP Port	Default port 49

Table 73: TACACS+ Options

FIELD	VALUES	DESCRIPTION
Service	pppshellraccess	Authentication service used by TACACS. The default value is `raccess`
Secret/Confirm Secret	Secret	
Timeout	Number	Communication timeout in seconds. Default value: 2
Retries	Number	Amount of retries before connection fails
TACACS+ Version	V0V1V0_V1V1_V0	TACACS version to be used. The default value is `V1`
Enable User-Level attribute of Shell and raccess services association to local authorization group	TrueFalse	
User Level 1 - 10	Nodegrid group name	

RADIUS

RADIUS is a client/server protocol that runs in the application layer and can use either 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. The following options exist:

- 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>];”`
- Besides `Framed-Filter-ID`, Nodegrid supports Vendor-Specific Attributes (VSA) as well, which can be used for authorization purposes. The following 2 properties need to be defined on the Radius server -- VENDOR ZPE 42518 -- ATTRIBUTE ZPE-User-Groups 1 string

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

Configuration Example for FreeRadius server:

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", adding a line with dictionary.zpe as below. The location is just a suggestion.

```
$INCLUDE dictionary.zpe
$INCLUDE dictionary.jradius
```

3. Configure users in /etc/freeradius/users assigning user's groups. It can be done defining attribute "Framed-Filter-ID" (as before) or defining new attribute "ZPE-User-Groups".

   NOTE: If both attributes are defined, "ZPE-User-Groups" will take 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
```

Table 74: Radius Options

FIELD	VALUES	DESCRIPTION
Status	TrueFalse	The default value is Enabled. This means the provider will be used to authenticate users
Fallback if denied access	Enabled or Disabled	Default is Disabled. It is recommended to Enable this feature in case the provider is not available.
Remote Server	IP address	
Accounting Server	IP Address	
Secret / Confirm Secret	Secret	
Timeout	Number	Communication timeout in seconds. The default value: 2
Retries	Number	Amount of retries before connection fails

Table 74: Radius Options

FIELD	VALUES	DESCRIPTION
Enable ServiceType attribute association to local authorization group	TrueFalse	Allows the 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	
Service Type Administrative	Nodegrid group name	

Kerberos

Kerberos is a computer network authentication protocol that uses tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Designed primarily as a client–server model, it provides mutual authentication. Both the user and the server verify each other's identity. It builds on symmetric key cryptography and requires a trusted third party, and optionally may use public-key cryptography. It uses UDP port 88 by default.

Table 75: Kerbos Options

FIELD	VALUES	DESCRIPTION
Status	TrueFalse	Default Value is Enabled. This means the provider will be used to authenticate users
Fallback if denied access	Enabled or Disabled	Default is Disabled. It is recommended to Enable this feature in case the provider is not available.
Remote Server	IP address	
Realm Domain Name	Kerberos realm name	

Table 75: Kerbos Options

FIELD	VALUES	DESCRIPTION
Domain Name	domain name	

RSA SecurID 2-factor authentication

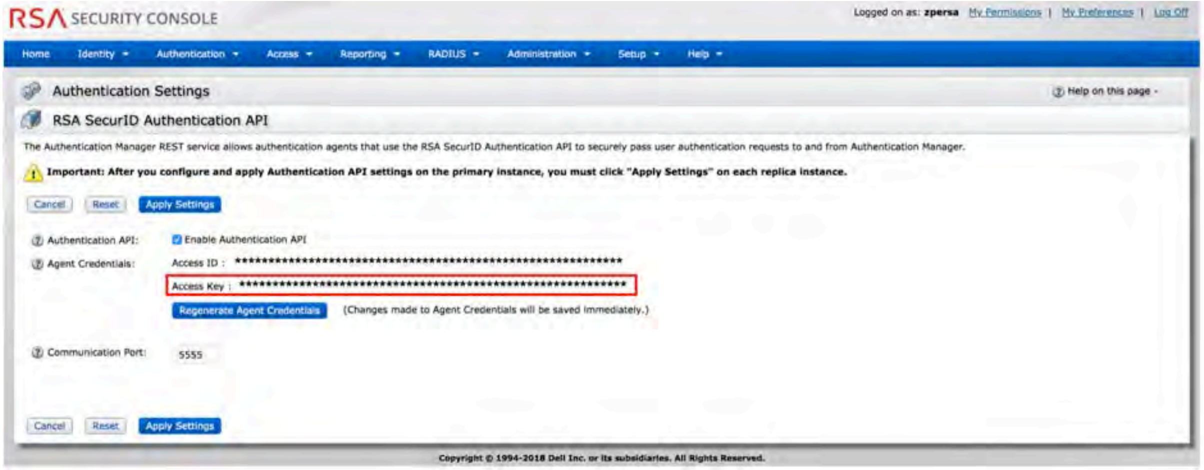
This section covers 2-factor authentication configuration required in Nodegrid as well as RSA Security Console.

Nodegrid Setup: Web Interface

Add SecurID Server

1. Login as admin in the Nodegrid Web Interface
2. Click on the 'Security' icon, then 'Authentication' tab
3. Click on '2-Factor' tab and then the 'Add' button

4. Fill in all fields following the examples below
   - Name: This name will identify your SecurID system, e.g. SecurID
   - Rest URL: URL to access the SecurID Authentication API. It should follow the format https://:5555/mfa/v1_1/authn
   - Enable Replicas: Rest Service URL to failover to the server. There can be up to 15 replicas. One per line. e.g. 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 available at RSA SecurID Authentication API (under System Settings)



Authentication Settings

RSA SecurID Authentication API

The Authentication Manager REST service allows authentication agents that use the RSA SecurID Authentication API to securely pass user authentication requests to and from Authentication Manager.

Important: After you configure and apply Authentication API settings on the primary instance, you must click "Apply Settings" on each replica instance.

Authentication API: ☑ Enable Authentication API

Agent Credentials: Access ID : **

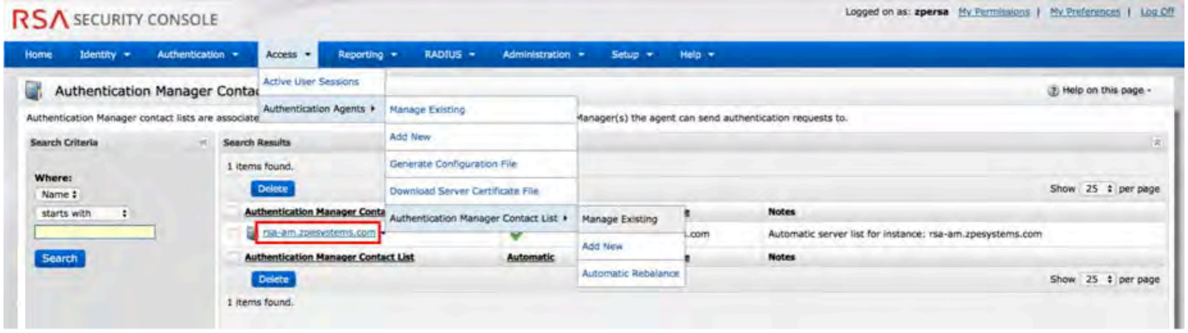
Access Key : **

(Changes made to Agent Credentials will be saved immediately.)

Communication Port: 5555

Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

   - Client ID: Retrieve the Server Node name from the Authentication Manager Contact List.



Authentication Manager Contac

Authentication Manager contact lists are associate ... Manager(s) the agent can send authentication requests to.

Search Criteria

Where: Name, starts with

Search Results

1 items found.

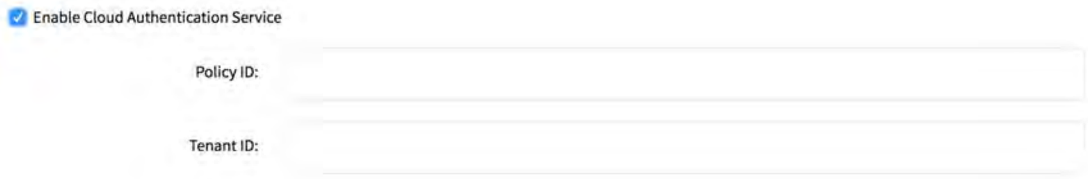
Show 25 per page

Authentication Manager Conta	Automatic		Notes
rsa-am.zpesystems.com	✓	.com	Automatic server list for instance: rsa-am.zpesystems.com
Authentication Manager Contact List	Automatic		Notes

Show 25 per page

1 items found.

5. Enable Cloud Authentication Service: If enabled, two fields will appear. These two fields are required for the service to work properly.

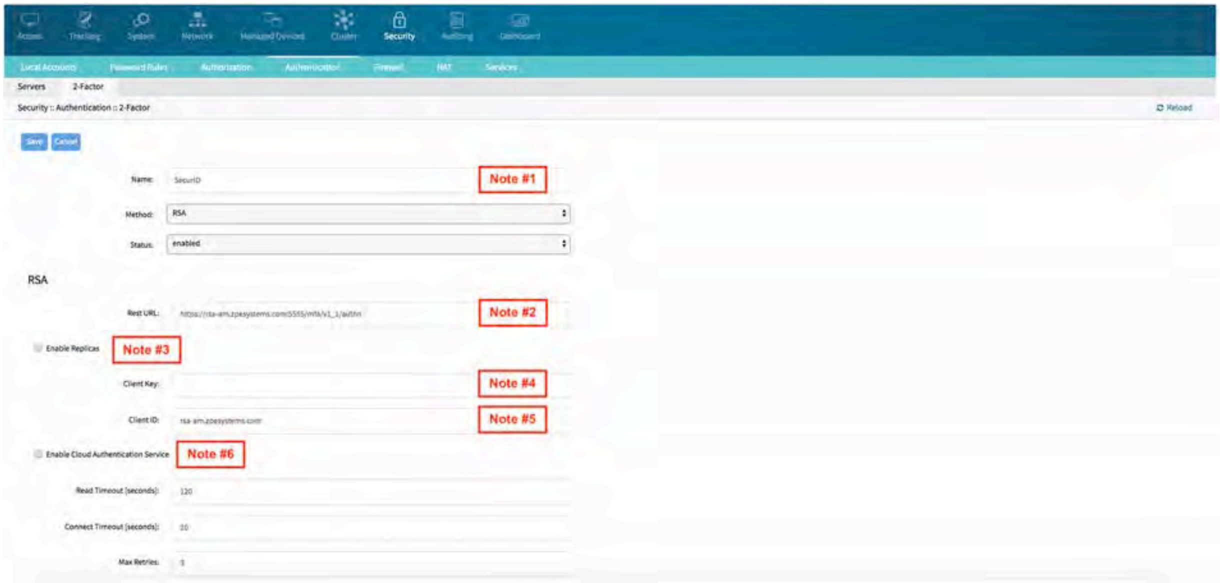


☑ Enable Cloud Authentication Service

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.



Security :: Authentication :: 2-Factor

Name: SecurID

Method: RSA

Status: enabled

RSA

Rest URL: https://rsa-am.zpesystems.com:5555/mfa/v1_1/authn

□ Enable Replicas

Client Key:

Client ID: rsa-am.zpesystems.com

□ Enable Cloud Authentication Service

Read Timeout [seconds]: 120

Connect Timeout [seconds]: 20

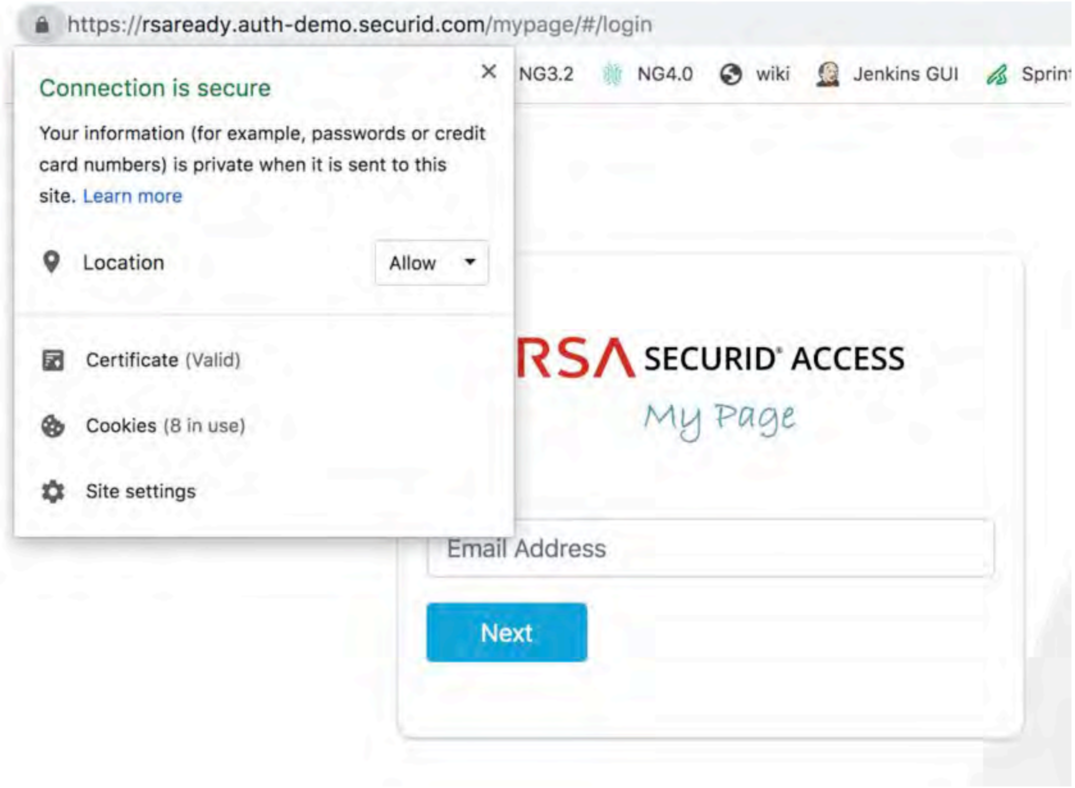
Max Retries: 3

6. Click Save

Set Certificate to access SecurID Server

1. If RSA server is through Cloud Authentication
   - Go to RSA SecurID Access, and click on the lock icon next to URL
   - Click on the `Certificate`. This popup will appear. Click on the first/top certificate, and drag it to your desktop to copy it. The copied certificate will be available in your

workstation and can be directly uploaded to Nodegrid. Nodegrid will convert it automatically to the expected certificate format.



https://rsaready.auth-demo.securid.com/mypage/#/login

Connection is secure

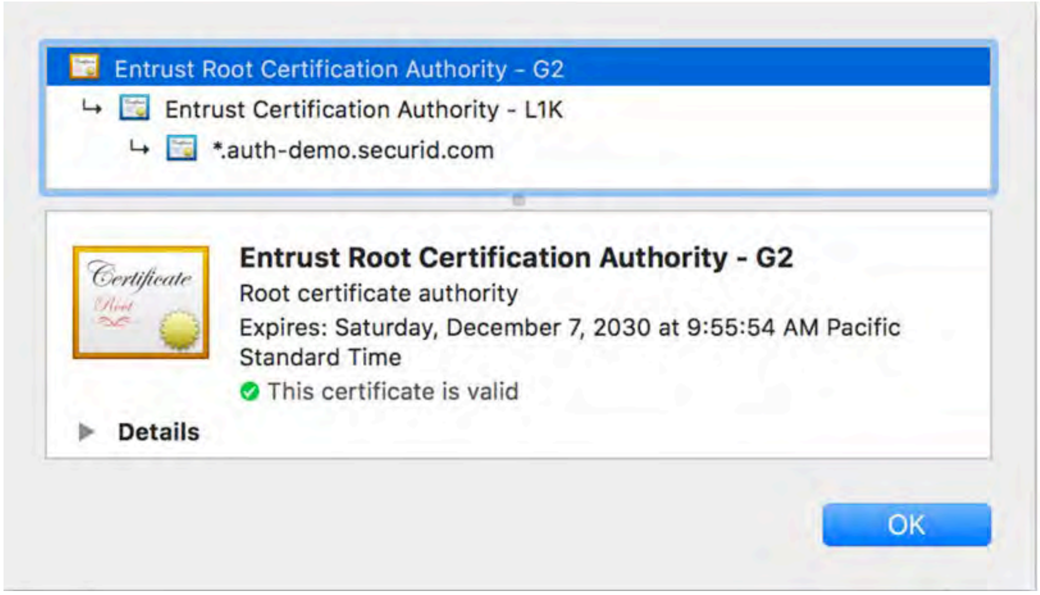
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Location: Allow

Certificate (Valid)

Cookies (8 in use)

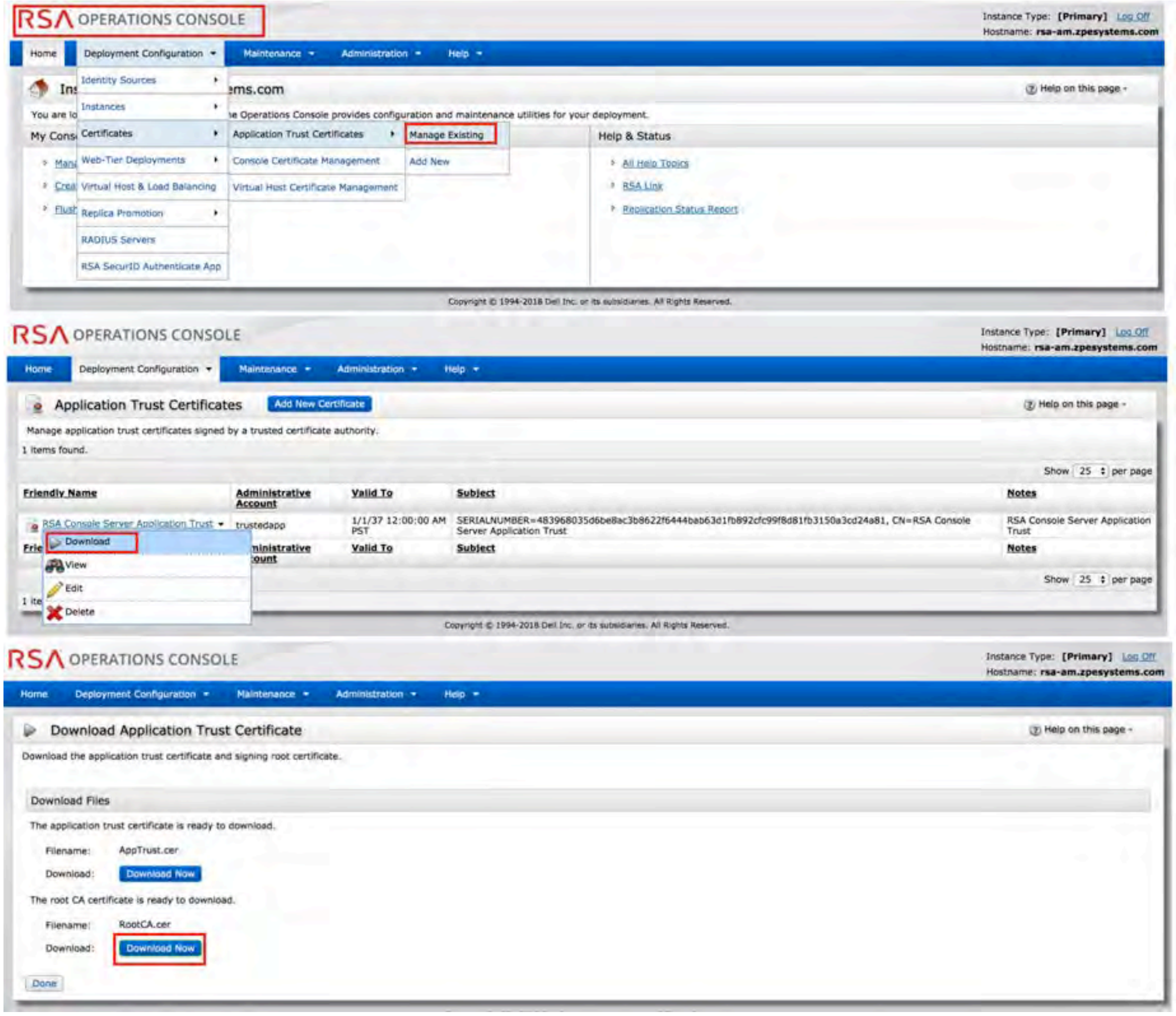
Site settings



Entrust Root Certification Authority - G2
↳ Entrust Certification Authority - L1K
↳ *.auth-demo.securid.com

Entrust Root Certification Authority - G2
Root certificate authority
Expires: Saturday, December 7, 2030 at 9:55:54 AM Pacific Standard Time
✓ This certificate is valid

2. If not via Cloud, download the Signing Root Certificate from RSA Operations Console.



Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Application Trust Certificates

Manage application trust certificates signed by a trusted certificate authority.

1 items found.

Show 25 per page

Friendly Name	Administrative Account	Valid To	Subject	Notes
RSA Console Server Application Trust	trustedapp	1/1/37 12:00:00 AM PST	SERIALNUMBER=483968035d6be8ac3b8622f6444bab63d1fb892cfc99f8d81fb3150a3cd24a81, CN=RSA Console Server Application Trust	RSA Console Server Application Trust

Download Application Trust Certificate

Download the application trust certificate and signing root certificate.

Download Files

The application trust certificate is ready to download.

Filename: AppTrust.cer

Download: Download Now

The root CA certificate is ready to download.

Filename: RootCA.cer

Download: Download Now

The downloaded certificate file (RootCA.cer) will be available in your workstation and can be directly uploaded to Nodegrid. Nodegrid will convert it automatically to the expected certificate format.

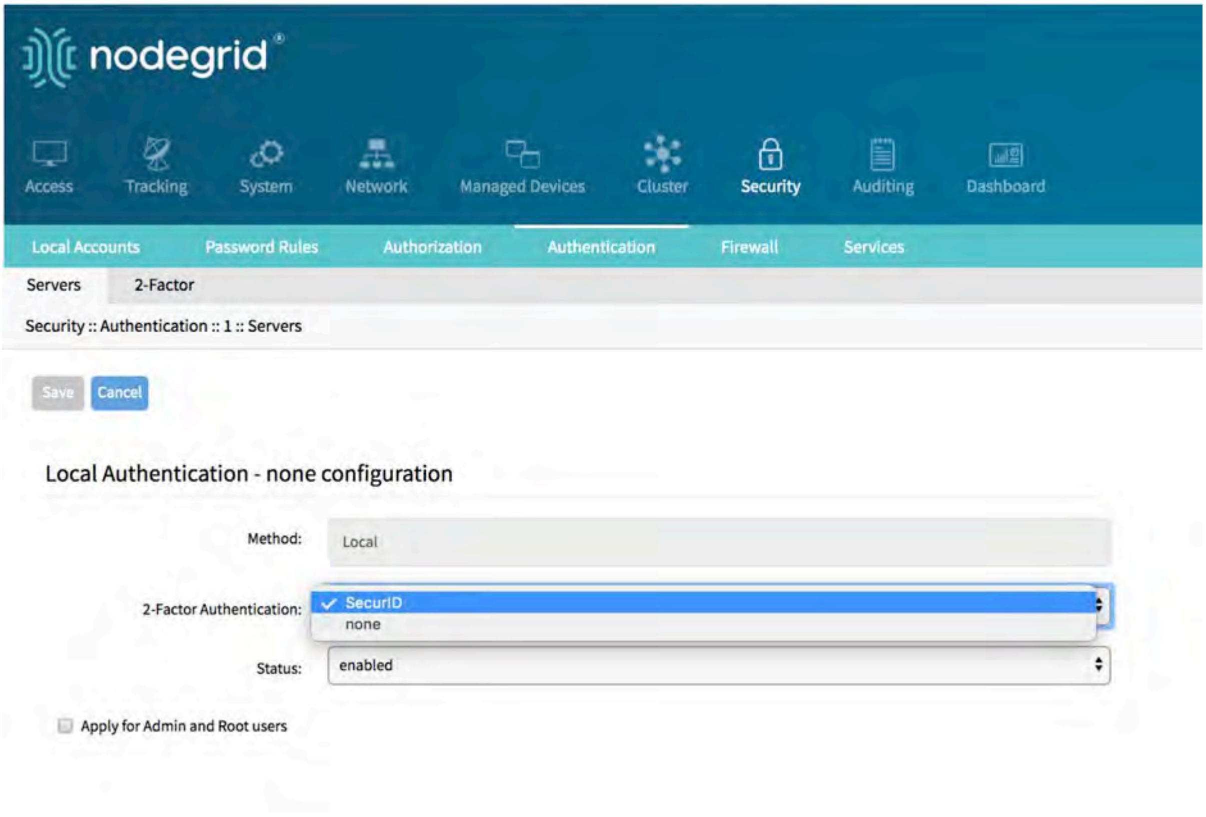
1. Login again as admin in the Nodegrid Web Interface if needed
2. Click on the 'Security' icon, then 'Authentication' tab
3. Click on '2-Factor' tab and then the link representing the SecurID server added in step above.
4. Click on the ‘Certificate’ button, select ‘Local Computer’ option and click ‘Choose File’
5. Browse your workstation file system to locate the certificate file downloaded (i.e. RootCA.cer file). To import it, click ‘Apply’

Assign the 2-factor authentication to an Authentication method

RSA SecurID 2-factor authentication can be added to any of the supported authentication methods in Nodegrid: Local, LDAP/AD, Radius, Tacacs or Kerberos.

Nodegrid will authenticate the users following the authentication servers' order as configured. Once a method succeeds, i.e. the user is authenticated, Nodegrid will start the 2-factor authentication if such method has such configuration.

The user will then receive a request straight from RSA SecurID to provide the token code and PIN as it was set in the RSA Security Console for such user. This process applies to users logging in via Web Browser, SSH, Telnet or Console port.



Security :: Authentication :: 1 :: Servers

Local Authentication - none configuration

Method: Local

2-Factor Authentication: ✓ SecurID
none

Status: enabled

□ Apply for Admin and Root users

Note: For Local authentication method it is possible to enforce or skip the 2-factor authentication. This allows local Nodegrid administrators to login without having to configure the counterpart users in the RSA Security Console.

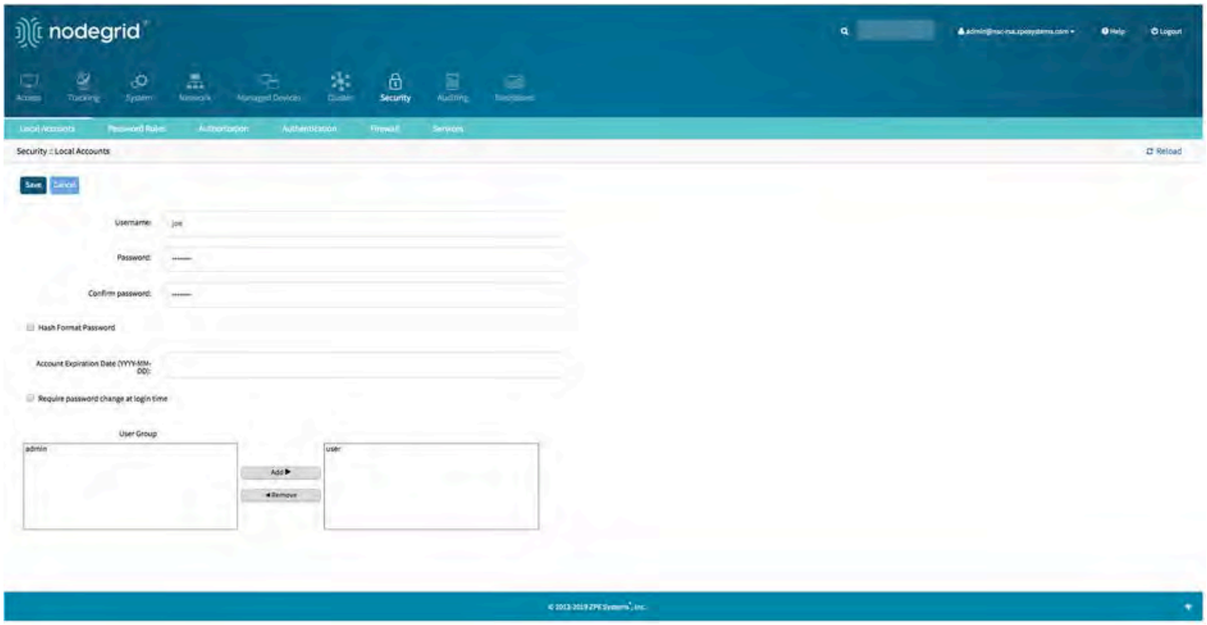
Users

Once 2-factor authentication is enabled, the user will need to provide credentials as well as pass code in order to be granted access. This means the users allowed to login must be configured also in RSA Security Console.

To configure a user in Nodegrid's local accounts:

1. Login again as admin in the Nodegrid Web Interface.
2. Click on the 'Security' icon, then 'Local Accounts' tab and click 'Add'.

3. Enter the user's name and password, then click 'Save'



Security :: Local Accounts

Username: joe

Password: ••••••••

Confirm password: ••••••••

☐ Hash Format Password

Account Expiration Date (YYYY-MM-DD):

☐ Require password change at login time

User Group

admin

user

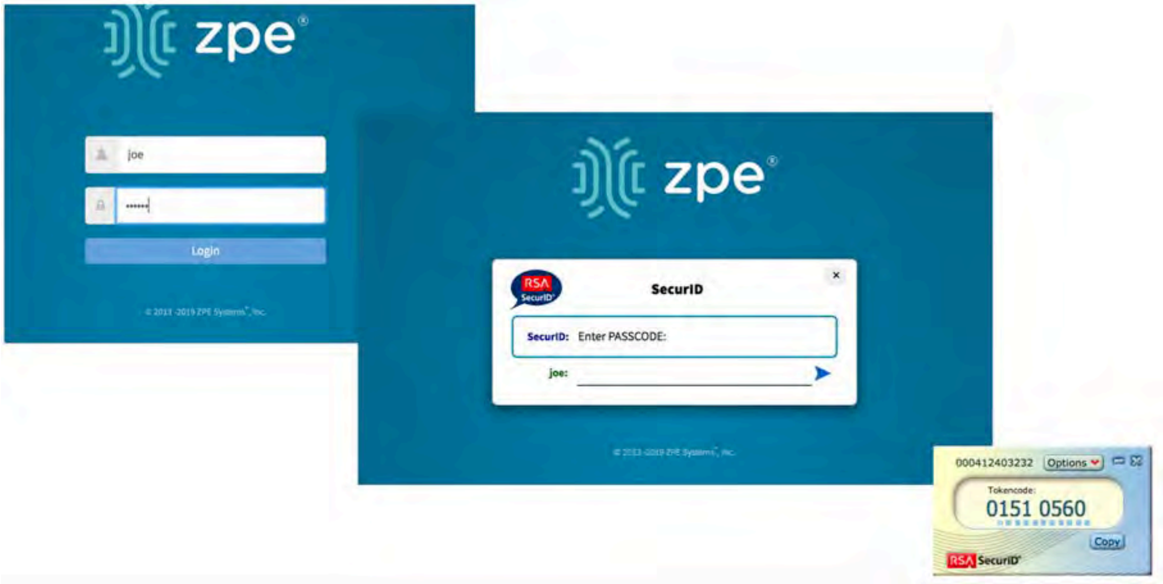
Note: The exact same users must be configured in RSA SecurID and have a token assigned.

Authenticate App (for Cloud Authentication Services only)

4. Download the app: RSA SecurID Authenticate
5. On the workstation, go to RSA SecurID Access, and login. Then follow the steps to register the device.

Login

To login in Nodegrid, provide the user's credentials. Whenever 2-factor authentication is required, the login process will prompt for the information as directly requested by SecurID.



joe

SecurID

SecurID: Enter PASSCODE:

joe:

000412403232

Tokencode: 0151 0560

SSHKey Authentication

The Nodegrid platform allows users to use ssh keys for authorization. The feature is primarily designed to allow automation systems to provide secure access to the unit without the need to provide a password, hence it is designed to work with direct Shell access and each user which wants to use ssh keys needs to have 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.

To setup ssh key authorization for a user:

1. Navigate to `Security::Authorization`
2. Create a group or use an existing Group
3. Navigate to the Groups `Profile` option.
4. Set the `Startup application` value to Shell, all users which are part of this group will get by default shell access and not CLI access on connection via SSH
5. Navigate to `Security::Local Accounts`
6. Create a local user and add the user to the newly created group
7. The user can now use the default ssh tools to copy his ssh key to the Nodegrid, for example `ssh-copy-id`
8. After this point, the user may use the ssh key for authentication

Optional:

- If the user needs by default CLI access and not Shell access, then the user can be at this point be removed from the newly created Group.
- If the user should be authorized by an external authentication provider like LDAP, AD or TACACS+, then the Local user account can be locked.
  - Navigate to `Security :: Local Accounts`
  - Highlight the user and click on `Lock` The user can then still use the sskhey for authentication but his permissions will be enforced based on his group permissions using the external authentication provider.

Security

Firewall

Nodegrid acts as a Firewall when configured to do so by an administrator. There are 6 built-in default chains, 3 for IPv4 and 3 for IPv6. These accept Output, Input, and Forward packets. Additional User chains can be created and deleted if required. For each chain, the default policy can be set. The default policy is set to `Accept` packages. 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. For more details please review the iptables documentation.

Table 76: Firewall Settings

SETTING	VALUES	DESCRIPTION
Target	ACCEPTDROPREJECTLOGRETURN	
Source IP/Mask	IP address and mask	
Reverse match for source IP/mask	TRUEFALSE	
Destination IP/Mask	IP address and mask	
Reverse match for destination IP/mask	TRUEFALSE	
Input Interface	AnyAvailable interfaces	one value of the list can be selected
Reverse match for input interface	TRUEFALSE	

Table 76: Firewall Settings

SETTING	VALUES	DESCRIPTION
Output Interface	AnyAvailable interfaces	one value of the list can be selected
Reverse match for output interface	TRUEFALSE	
Enable State Match	NEWESTABLISHEDRELATEDINVALID	one or multiple States can be selected
Reverse state match	TRUEFALSE	
Fragments	All packets and fragmentsUnfragmented packets and 1st packets2nd and further packets	one value of the list can be selected
Reject With	Network UnreachableHost UnreachablePort Unreachable Protocol UnreachableNetwork ProhibitedHost ProhibitedAdministratively ProhibitedTCP Reset	
Protocol	NumericTCPUDPICMP	
Protocol - Numeric - Protocol Number	Protocol Number	
Protocol - TCP - Source Port	Port Number	
Protocol - TCP - Destination Port	Port Number	
Protocol - TCP - TCP Flag SYN	AnySetUnset	
Protocol - TCP - TCP Flag ACK	AnySetUnset	
Protocol - TCP - TCP Flag FIN	AnySetUnset	
Protocol - TCP - TCP Flag RST	AnySetUnset	

Table 76: Firewall Settings

SETTING	VALUES	DESCRIPTION
Protocol - TCP - TCP Flag URG	AnySetUnset	
Protocol - TCP - TCP Flag PSH	AnySetUnset	
Protocol - TCP - Reverse match for TCP flags	TRUEFALSE	
Protocol - UDP - Source Port	Port Number	
Protocol - UDP - Destination Port	Port Number	

Table 76: Firewall Settings

SETTING	VALUES	DESCRIPTION
Protocol - ICMP - ICMP Type	AnyEcho ReplyDestination UnreachableNetwork UnreachableHost UnreachableProtocol UnreachablePort UnreachableFragmentation NeededSource Route FailedNetwork UnknownHost UnknownNetwork ProhibitedTOS Network UnreachableTOS Host UnreachableCommunication ProhibitedHost Precedence ViolationPrecedence CutoffSource QuenchRedirectNetwork RedirectHost RedirectTOS Network RedirectTOS Host RedirectEcho RequestRouter Advertisement Router SolicitationTime ExceededTTL Zero During TransitTTL Zero During ReassemblyParameter ProblemBad IP HeaderRequired Option MissingTimestamp RequestTimestamp ReplyAddress Mask RequestAddress Mask Reply	
Protocol - ICMP - Reverse match for ICMP type	TRUEFALSE	
Reverse match for protocol	TRUEFALSE	
Reverse match for source port	TRUEFALSE	

Table 76: Firewall Settings

SETTING	VALUES	DESCRIPTION
Reverse match for destination port	TRUEFALSE	
Log Level	DebugInfoNoticeWarningErrorCriticalAlertEmergency	
Log Prefix	Log Prefix String	
Log TCP Sequence Numbers	TRUEFALSE	
Log Options From The TCP Packet Header	TRUEFALSE	
Log Options From The IP Packet Header	TRUEFALSE	

NAT

Nodegrid acts as a Firewall when configured to do so by an administrator. The NAT section allows defining rules for the NAT table and can be used to define Network Address Translation rules (NAT). There are 8 built-in default chains, 4 for IPv4 and 4 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. For more details please review the iptables documentation.

Table 77: NAT Settings

SETTINGS	VALUES	DESCRIPTION
Target	ACCEPTDROPREJECTLOG RETURN	
Source IP/Mask	IP address and mask	
Reverse match for source IP/mask	TRUEFALSE	
Destination IP/Mask	IP address and mask	
Reverse match for destination IP/mask	TRUEFALSE	
Input Interface	AnyAvailable interfaces	one value of the list can be selected

Table 77: NAT Settings

SETTINGS	VALUES	DESCRIPTION
Reverse match for input interface	TRUEFALSE	
Output Interface	AnyAvailable interfaces	one value of the list can be selected
Reverse match for output interface	TRUEFALSE	
Enable State Match	NEWESTABLISHEDRELATEDINVALID	one or multiple States can be selected
Reverse state match	TRUEFALSE	
Fragments	All packets and fragmentsUnfragmented packets and 1st packets2nd and further packets	one value of the list can be selected
Reject With	Network UnreachableHost UnreachablePort Unreachable Protocol UnreachableNetwork ProhibitedHost ProhibitedAdministratively ProhibitedTCP Reset	
Protocol	NumericTCPUDPICMP	
Protocol - Numeric - Protocol Number	Protocol Number	
Protocol - TCP - Source Port	Port Number	
Protocol - TCP - Destination Port	Port Number	
Protocol - TCP - TCP Flag SYN	AnySetUnset	
Protocol - TCP - TCP Flag ACK	AnySetUnset	
Protocol - TCP - TCP Flag FIN	AnySetUnset	

Table 77: NAT Settings

SETTINGS	VALUES	DESCRIPTION
Protocol - TCP - TCP Flag RST	AnySetUnset	
Protocol - TCP - TCP Flag URG	AnySetUnset	
Protocol - TCP - TCP Flag PSH	AnySetUnset	
Protocol - TCP - Reverse match for TCP flags	TRUEFALSE	
Protocol - UDP - Source Port	Port Number	
Protocol - UDP - Destination Port	Port Number	

Table 77: NAT Settings

SETTINGS	VALUES	DESCRIPTION
Protocol - ICMP - ICMP Type	AnyEcho ReplyDestination UnreachableNetwork UnreachableHost UnreachableProtocol UnreachablePort UnreachableFragmentation NeededSource Route FailedNetwork UnknownHost UnknownNetwork ProhibitedTOS Network UnreachableTOS Host UnreachableCommunication ProhibitedHost Precedence ViolationPrecedence CutoffSource QuenchRedirectNetwork RedirectHost RedirectTOS Network RedirectTOS Host RedirectEcho RequestRouter Advertisement Router SolicitationTime ExceededTTL Zero During TransitTTL Zero During ReassemblyParameter ProblemBad IP HeaderRequired Option MissingTimestamp RequestTimestamp ReplyAddress Mask RequestAddress Mask Reply	
Protocol - ICMP - Reverse match for ICMP type	TRUEFALSE	
Reverse match for protocol	TRUEFALSE	
Reverse match for source port	TRUEFALSE	

Table 77: NAT Settings

SETTINGS	VALUES	DESCRIPTION
Reverse match for destination port	TRUEFALSE	
Log Level	DebugInfoNoticeWarning ErrorCriticalAlertEmergency	
Log Prefix	Log Prefix String	
Log TCP Sequence Numbers	TRUEFALSE	
Log Options From The TCP Packet Header	TRUEFALSE	
Log Options From The IP Packet Header	TRUEFALSE	

Services

The Services page allows you to defining the `Active Services` running on the system, as well as general service settings for `ZPE Cloud`, `Managed Devices`, `Intrusion Prevention`, `SSH` settings to the systems itself, `Web Service` settings and `Cryptographic Protocols` for the Web Service.

This allows configuration of the security level of the system. For instance, unsecured protocols like Telnet or HTTP may be disabled, or the SSH version which is allowed to access the system can be selected.

ZPE Cloud

ZPE Cloud is a cloud based management platform for Nodegrid products. No need for shipping pre-configured devices to the branch. ZPE Cloud makes the initial deployment, configuration, and ongoing management simple and provides with a 360 visibility of the entire deployment along with rich analytics that are easy to understand and operate.

ZPE Cloud coupled with Nodegrid devices allows for shipping IT devices without having to stage or pre-configure them. This allows you to configure the IT devices once they are safely at the branch. Deploy consistent, automated provisioning via the ZPE Cloud from the safety of your NOC.

ZPE Cloud brings together all Nodegrid products on a cloud platform. Use “Reset” button available on all Nodegrid products to reconnect back your Nodegrid to the ZPE Cloud.
The `ZPE Cloud` section allows configuring the cloud services on the unit.

The following settings are available:

Table 78: ZPE Cloud Settings

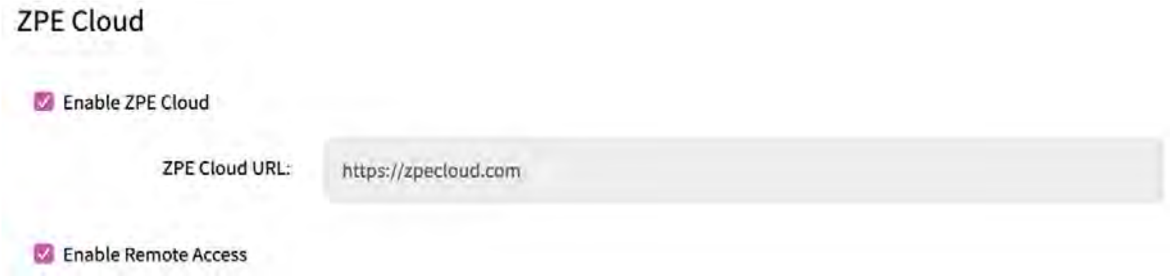
SETTING	VALUE	DESCRIPTION
Enable ZPE Cloud	TRUEFALSE	Enabled by Default for the Nodegrid SR family (NSR, GSR, BSR & LSR) Note: Nodegrid Serial Console default value is disabled.
Enable File Protection	TRUEFALSE	Disabled by Default.When enabled, any file transfer will require an authentication hash based on this password to validate the integrity and origin of the file.
Enable File Encryption	TRUEFALSE	Disabled by Default.When enabled, file must be encrypted via ZIP by the owner using the password defined under file protection.

> Note: For Nodegrid units shipped prior to Nodegrid v4.1, the following command must be executed by `root` in order to enroll the unit to the ZPE Cloud.

Enable ZPE Cloud on Nodegrid Serial Console

To enable ZPE Cloud on the Nodegrid Serial Console:

1. Navigate to `Security::Services`
2. Check the Enable ZPE Cloud and Enable Remote Access check boxes
3. Enter the ZPE Cloud URL



ZPE Cloud

☑ Enable ZPE Cloud

ZPE Cloud URL: https://zpecloud.com

☑ Enable Remote Access

4. Click Save

Next, you will need to complete the enrollment process by doing the following:

1. Navigate to `Access:Table`
2. Click on the Console button
3. Execute the following commands:

```
shell sudo su -
zpe_cloud_enroll
```

4. Enter your customer code
5. Enter your enrollment key

Note: Your customer code and enrollment key can be found by logging in to your ZPE Cloud account under Settings::Enrollment. The Enable Device Enrollment check box must be enabled for the enrollment to process to proceed.

6. You will receive a confirmation that the enrollment was successful.

Usage of zpe_cloud_enroll

The script can be called with 3 combinations of arguments as shown below:

```
root@ZPECloudNSR2:~# zpe_cloud_enroll -h
Usage: zpe_cloud_enroll [options]
ZPE Cloud Enrollment

Options:
  -v, --version        Displays version information.
  -h, --help           Displays this help.
  -c <customer-code>   ZPE Cloud customer code to enroll device.
  -k <enrollment-key>  ZPE Cloud customer enrollment key.
  -r                   Read customer enrollment key from barcode.
```

No arguments

If no arguments are provided, the device will request that the `customer code` and the `enrollment key` to be entered:

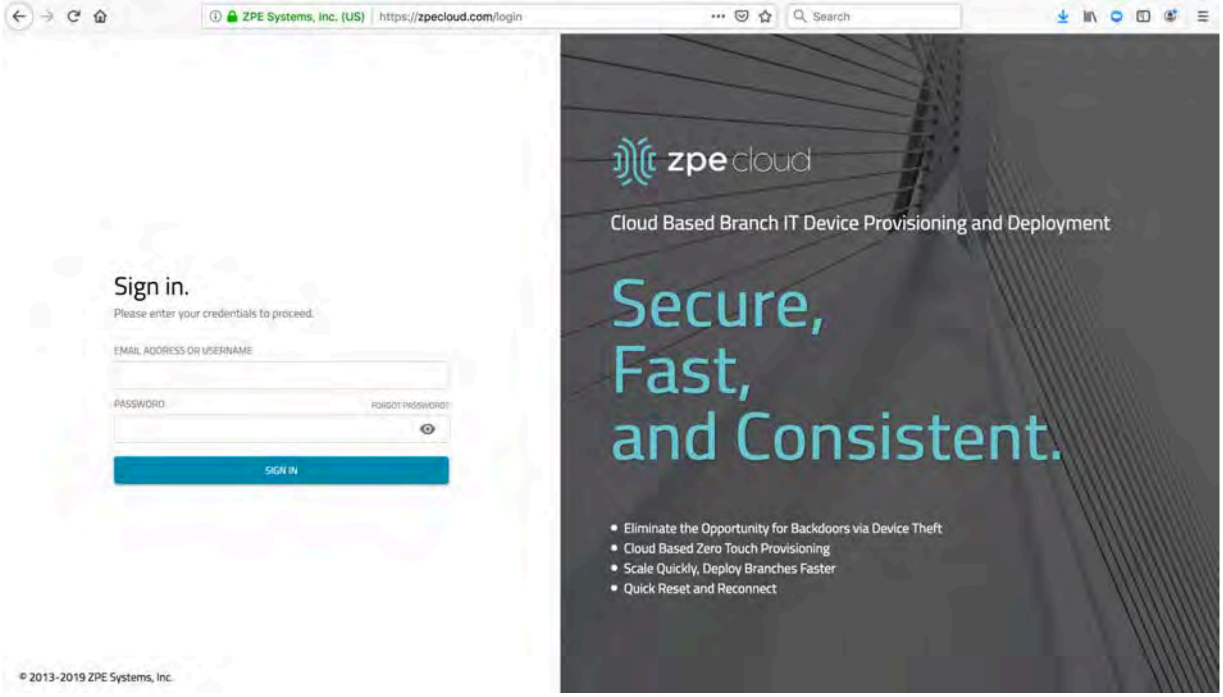
```
root@ZPECloudNSR2:~# zpe_cloud_enroll
Enter your customer code: 2
Customer Code:  "2"
Enter your enrollment key: example_key
```

Arguments (Customer Code and Enrollment Key)

For this case, customer code (-c) and enrollment key (-k) are provided as the script arguments:

```
zpe_cloud_enroll -c 2 -k example_key
```

Once the ZPE Cloud is enabled on the unit, access www.zpecloud.com to manage all enrolled devices. The cloud management portal requires a Company registration and an admin user account.



Sign in.

Please enter your credentials to proceed.

© 2013-2019 ZPE Systems, Inc.

Cloud Based Branch IT Device Provisioning and Deployment

Secure,
Fast,
and Consistent.

- Eliminate the Opportunity for Backdoors via Device Theft
- Cloud Based Zero Touch Provisioning
- Scale Quickly, Deploy Branches Faster
- Quick Reset and Reconnect

Active Services

The `Active Services` page allows you to control which Services should be enabled in the system and which network ports they should be using.

The following settings are available:

Table 79: Active Services Settings

SETTING	VALUE	DESCRIPTION
Enable detection of USB devices	TRUEFALSE	Enabled by Default
Enable RPC	TRUEFALSE	Required for NFS share access
Enable gRPC	TRUEFALSE	Support for gRPC protocol. Disabled by Default
Enable FTP Service	TRUEFALSE	
Enable SNMP Service	TRUEFALSE	Enabled by Default
Enable Telnet Service to Nodegrid	TRUEFALSE	

Table 79: Active Services Settings

SETTING	VALUE	DESCRIPTION
Telnet TCP Port	Port number	Default value: 23
Enable Telnet Service to Managed Devices	TRUEFALSE	
Enable ICMP echo reply	TRUEFALSE	Enabled by Default
Enable USB over IP	TRUEFALSE	
Enable Virtualization Services	TRUEFALSE	Needs to be Enabled in order to run NFV's or Docker apps. Both features require licenses
Cluster TCP Port	Port Number	Default value: 9966
Enable Automatic Cluster Enrollment	TRUEFALSE	
Search Engine TCP Port	Port Number	Default Value: 9300
Enable Search Engine High Level Cipher Suite	TRUEFALSE	
Enable VM Serial access	TRUEFALSE	Enabled by Default
VM Serial Port	Port Number	Default Value: 9977
vMotion timeout [seconds]	Number in seconds	Default Value: 300
Enable Zero Touch Provisioning	TRUEFALSE	Enabled by Default
Enable PXE (Preboot eXecution Environment)	TRUEFALSE	Enabled by Default

Managed Devices

The `Managed Devices` section allows controlling of general aspects and services controlling managed devices.

The following settings are available:

Table 80: Managed Devices Settings

SETTING	VALUE	DESCRIPTION
Device access enforced via user group authorization	TRUEFALSE	When this feature is enabled, users will only have access to devices listed under the authorization groups that the user belongs. If this feature is not enabled, all enrolled devices in the Nodegrid will be available to the user and the user will be able to access them without restriction.
Enable Autodiscovery	TRUEFALSE	This feature allows the Auto Discovery of managed devices on the network.
DHCP lease controlled by autodiscovery rules	TRUEFALSE	If this feature is enabled then the DHCP server will only server leases to devices which have been discovered through the Auto Discovery process. This feature is only available when `Enable AutoDiscovery` is enabled.

Intrusion Prevention

The `Intrusion Prevention` section allows the configuration of mechanisms which can prevent unauthorized access to a system, like `Fail 2 Ban` and `Rescue Mode`.

The following settings are available:

Table 81: Intrusion Prevention Settings

SETTING	VALUE	DESCRIPTION
Block host with multiple authentications fails	TRUEFALSE	
Period Host will stay blocked (min)	Number in min	Amount of time the system will not be reachable on the network. Default value:10
Timeframe to monitor authentication fails (min)	Number in min	Amount of time during which failed authentication attempts are counted and before the counter gets reset. Default value:10

Table 81: Intrusion Prevention Settings

SETTING	VALUE	DESCRIPTION
Number of authentication fails to block host	Number	Amount of failed authentication attempts during `Number of authentication fails to block host` before the host will be blocked. Default value:5
Rescue Mode requires authentication	TRUEFALSE	After this feature is enabled, the Rescue Mode will require authentication through a local user account, like root.
Password protected boot	TRUEFALSE	After this feature is enabled, editing BIOS and Grub will require authentication based on password defined here.

Note : Password Protected Boot is a patent-pending feature that allows Nodegrid OS to communicate with BIOS in order to enable the BIOS password to prevent unauthorised changes on it. The same password will also protect Grub from unauthorized changes.

Note: The `Password Protected Boot` feature requires minimum Bios version of 81122T00. See `About` information for the current version.

SSH

The `SSH` section allows configuration of the SSH service controlling access to the Nodegrid system.

Note: Explicit specification of SSHv1 is eliminated. We only support SSHv2 now.

The following settings are available:

Table 82: SSH Settings

SETTING	VALUE	DESCRIPTION
SSH allow root access	TRUEFALSE	Allows root access through SSH, Enabled by default.
SSH TCP Port	Port Number	Default value: 22
SSH Ciphers	allowed list of ciphers	Default value: blank, which allows all ciphers which are supported by Nodegrid
SSH MACs	allowed list of MAC addresses	Default value: blank, which allows all systems to access the Nodegrid via ssh
SSH KexAlgorithms	an allowed list of key exchange algorithms	Default value: blank

Web Service

The `Web Service` section allows the configuration of the web server.

The following settings are available:

Table 83: Web Service Settings

SETTING	VALUE	DESCRIPTION
Enable HTTP access	TRUEFALSE	Default value: Enabled
HTTP Port	Port Number	Default value: 80
Enable HTTPS access	TRUEFALSE	Default value: Enabled
HTTPS Port	Port Number	Default value: 443
Redirect HTTP to HTTPS	TRUEFALSE	Default value: Enabled

Cryptographic Protocols

The `Cryptographic Protocols` allow configuration of which ciphers are supported to access the web server.

The following settings are available:

Table 84: Cryptographic Protocol Settings

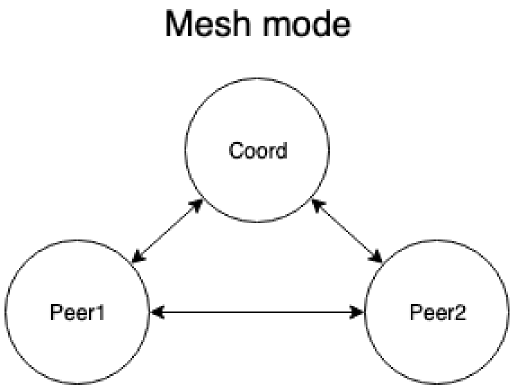
SETTING	VALUE	DESCRIPTION
TLSv1.3	TRUEFALSE	Default value: Enabled
TLSv1.2	TRUEFALSE	Default value: Enabled
TLSv1.1	TRUEFALSE	Default value: Enabled
TLSv1	TRUEFALSE	Default value: Disabled
Cipher Suite Level	HighMediumLowCustom	Default value: Medium

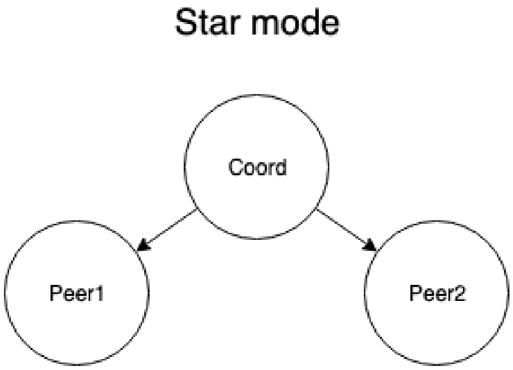
Cluster

Cluster is a Nodegrid feature that establishes a secure and resilient connection among other Nodegrid platforms, so that when Clustering is enabled, multiple Nodegrid systems can easily manage and access all managed devices from other nodes. Nodegrid makes cluster access management even easier with cluster asset search. By logging into any Nodegrid, users can search the entire Nodegrid-managed enterprise network and cluster 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 will act as the coordinator and central node. All the other peers will connect to the coordinator in a star formation. Only the coordinator will have the list of all peers and attached devices on the configuration. This option allows for centralized access and visibility from the Nodegrid unit acting as coordinator while keeping a light system resource demand on the Nodegrid units acting as peers.
- MESH - In mesh configuration, one Nodegrid unit will act as the coordinator and all Nodegrid units (coordinator and peers) will be able to see each other and all the attached devices in the cluster. This option allows for distributed access and therefore it requires that every unit keep a list of all peers and attached devices, demanding equal system resources of all units on the clustering. This configuration is recommended when clustering with less than 50 units.





Peers Overview

The `Peers` page lists all Nodegrid units that are enrolled in the cluster.

The table shows the name of each Nodegrid, their IP Addresses, type, and status of communication with other peers.

Peers can be removed by selecting entries and then clicking on the `Remove` button. If the Nodegrid is the coordinator, it cannot be removed from the table.

Cluster Settings

In this section, the Cluster feature and the additional services `Peer Management` and `License Pool` can be enabled and configured.

> Note: The Cluster feature requires a software license for each node in the cluster.

Enable Cluster

The Cluster feature can be enabled by checking the `Enable Cluster` check box. Each Cluster requires to have one `Coordinator` which coordinates and controls the enrollment of peer systems.

The first unit the cluster needs to be set as type `Coordinator`. All other units can then be set to type `Peer`. The role of the `Coordinator` can later be changed to another system by selecting the Type of Coordinator on a peer. The change will then automatically propagated through the system.

If the Nodegrid is the coordinator, make sure the `Allow Enrollment` check box is checked, and provide a `Cluster Name` and `Pre-Shared Key` so that peers can be enrolled to the Cluster. Select `Cluster Mode` as Star or Mesh, to configure the type of clustering desired.

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

If the Nodegrid is the Peer, then enter the Coordinator's `Cluster Name`, `Coordinators's Address`, and the `Pre-Shared Key`.

Check the `Enable Clustering` check box for allowing 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

The `Automatic Enrollment` features allow administrators to automatically add new Nodegrid systems which become available to an existing cluster. The feature is enabled by default for `Peers`. The `Pre-Shared Key` setting needs to be the same on the Coordinator as well as on the Peers. It is set by default to nodegrid-key. The value `Interval [seconds]` only applies to coordinators 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 where other Nodegrid systems are on the network. To add network ranges for the discovery process, add them to the `Automatic Enrollment Range` page under Cluster Settings.

> Note: It is recommended to only add IP's to the Automatic Enrollment Range which are potentially Nodegrid units, as the system will send continually invitations to all IP's until a Nodegrid unit was found on a specific IP and it was added to the Cluster.

The Coordinator will communicate with any Nodegrid system on those ranges and add them to the Cluster, thus eliminating the need to go to each of the Nodegrid nodes and set them as peers.

License Pool

The `License Pool` feature allows for central management of all software licenses within a cluster. For this at least one unit needs (in STAR, it should be the coordinator) to be set up as a `License Pool Server`, all other units are set up as `License Pool Clients`, which is the default setting.

License Pool Clients will automatically request required licenses from the `License Pool Server`. Licenses Pool Server will check the availability of licenses and assign the requested licenses if they are available. The Client will renew the licenses depending on the server's `Renew Time [days]`. In case a client becomes unavailable for an extended period of time and exceed the servers `Lease Time [days]`, the licenses will become invalid on the client and return to the pool. The `Lease Time [days]` option accepts values from 7-30 days.

The currently leased licenses can be viewed on the License Pool Server in the `System::Licenses` section.

> Note: Each Nodegrid unit is shipped with 5 additional test target licenses. The test license will be licensed automatically when a target license is added to the system. This applies as well if a target license is applied through the license pool server. This means the first time a system request target licenses it will request 5 additional licenses to cover the currently used test licenses.

Peer Management

The `Peer Management` feature enables a function to centrally upgrade the firmware of Nodegrid units in the cluster. To enable the feature select `Enable Peer Management`.

The cluster `Management` page allows then to start the software upgrade process for remote Nodegrid units from a central location. The firmware which will be applied to the units needs to be hosted on a central location which is 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 page lists all Nodegrid systems in the Cluster. Select desired nodes that have the Management Status as Idle. If the status shows disabled, it means that the Nodegrid has `Peer Management` feature disabled. Once the selection is done, click on the Software Upgrade button. Select `Remote Server` and enter `URL`, `Username`, and `Password`. The option `Format partitions before upgrade` will format the Nodegrid units hard drive before performing the firmware upgrade.

If downgrading the software, you have the option to `Restore configuration saved on version upgrade` or `Apply factory default configuration`.

Auditing Settings

The auditing feature allows events which have been created to be sent to four different destinations: Email, File, SNMP Trap, and Syslog. It also allows data logging and events logging to be stored locally, remotely via NFS or sent to a syslog server.

Data Logging

The Data logging feature allows capturing the data stream going to and coming from target devices as well as from the Nodegrid system. General settings for the data logging feature are available under `Auditing::Settings`. The following settings are available.

Table 85: Data Logging Settings

SETTING	VALUES	DESCRIPTION
Enable File Destination	TRUEFALSE	When the feature is enabled all Data Logs are stored to the defined File location under `Auditing Destinations`. Default Value: Enabled
Enable Syslog Destination	TRUEFALSE	When the feature is enabled all Data Logs are sent to the defined Syslog location under `Auditing Destinations`.Default Value: Disabled
Add Timestamp on every line logged	TRUEFALSE	When this feature is enabled, a timestamp will be added to each data log line
Timestamp Format	UTCLocal Time	Defines the timestamp timezone, which will be used. Default value: UTC

Events

The Nodegrid system automatically creates events based on its and device settings. All events get stored to the local file system by default. This behavior can be adjusted under `Auditing::Events`. The administrator can configure to which destination events get logged and which event categories get logged.

The system supports 4 event categories which can be individually controlled:

- Systems Events
- AAA Events
- Device Events
- Logging Events

Note: Under `Tracking::Event List` are all events listed and the category they belong to.

Each of these event categories can be configured to send the events to any of the 4 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

Data logs are written by default to files which are maintained locally. The file destination and archive settings can be set under `Auditing::Destinations::File`

Note: NFS requires RPC service to be enabled in Security :: Services

The following options are available:

Table 86: 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 unit should have its own root directory.
File Size [Kbytes]	File size in Kbytes	File size at which the file will be rotated. Valid values are between 0 (disabled) and 2048 Kb. Default value: 1024.
Number of Archives	Number	Number of archive files which should be kept before they will be discarded. Default value: 10 max value: 99
(NFS) Archive by Time [HH:MM]	Time in format HH:MM	Time at which the file archive will be rotated. Default value: blank

Syslog

The Syslog destination can be used to store data logs and event notifications. The system supports a local Syslog destination or a remote IPv4 and IPv6 destination.

The following options are available:

Table 87: Syslog Options

SETTING	VALUE	DESCRIPTION
System Console	TRUEFALSE	Syslog events will be displayed on the Nodegrid system console port sessions. By default, this option is enabled
Admin Session	TRUEFALSE	Syslog events will be displayed and any admin session which is open to the Nodegrid system. By default this option is disabled.
IPv4 Remote Server	IP address	One or multiple IP addresses can be provided. Addresses need to be separated by a comma.
IPv4 Address or Hostname	TRUEFALSE	By default is disabled
IPv6 Remote Server	IP address	One or multiple IP addresses can be provided. Addresses need to be separated by a comma.
IPv6 Address or Hostname	TRUEFALSE	By default is disabled
Event Facility	Log Local 0Log Local 1Log Local 2Log Local 3Log Local 4Log Local 5	Defines the Syslog logging facility for Events
Data Logging Facility	Log Local 0Log Local 1Log Local 2Log Local 3Log Local 4Log Local 5	Defines the Syslog logging facility for data logs

SNMP Trap

Any triggered event can be sent via an SNMP trap to an existing NMS system. The Nodegrid system supports SNMP v2 and 3 for traps. The MIB files for the Nodegrid system 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.

The following options are available:

Table 88: SNMP Trap Settings

SETTING	VALUE	DESCRIPTION
SNMP Engine ID	none	Displays the systems Engine ID
Server	IPv4 or IPv6 IP address	
Transport Protocol	UDP-IPv4TCP-IPv4UDP-IPv6TCP-IPv6	protocol used to send the traps. Default is UDP-IPv4.
Port	TCP port	default value is 161
Trap Version	Version 2cVersion 3	SNMP version to be used
Version 2c - Community	community name	
Version 3 - User Name	user name	
Version 3 -Security Level	noAuthNoPrivauthNoPrivauthPriv	
Version 3 -Authentication Algorithm	MD5SHA	
Version 3 -Authentication Password	Password	
Version 3 -Privacy Algorithm	DESAES	
Version 3 -Privacy Passphrase	Passphrase	

Email Notification

Events can be sent via Email to an email address.

The following options are available:

Table 89: Email Notification Settings

SETTING	VALUE	DESCRIPTION
Server	SMTP server address	
Port	TCP port to be used	Default port is 25
Username	Username	
Password	Password	
Confirm Password	Password	
Destination Email	email address	target email address to which the events will be sent to
Start TLS	TRUEFALSE	Should TLS be used for the communication

Monitoring

The Monitoring feature allows Nodegrid to monitor and collect sensor data from Managed Devices which are connected to a Nodegrid sensor or support SNMP or IPMI as a protocol.

The collected data are defined and controlled through `Monitoring Templates` which will be assigned to a monitored device during its configuration.

Customizing a Monitoring Template

There are a number of preexisting monitoring templates which typically fulfill the user's requirements. Should the need arise then these templates can be customized.

All templates are text files located in sub directories of the`/etc/collectd.templates` directory according to the protocol used to collect the monitoring data, either SNMP or IPMI.

- `/etc/collectd.templates/snmp`
- `/etc/collectd.templates/ipmi`

Any new file in these directories will automatically appear in the user interface.

SNMP Template

To create a new SNMP template, login as root to the shell. Create a copy of one existing template as a starting point for the new template.

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, defines SNMP parameters, the collecting interval, and which data points are to be collected.

The template file should only include data points which are of interest, all other data points can be removed from the file.

The following table explains the settings and the possible values for a data entry:

Table 90: Settings and Values for Data Entry

SETTING	VALUE	DESCRIPTION
Data	Internal name of the Data point as it will be collected by the Nodegrid system. The Name should be unique.	the name should not have any spaces. ExampleData "pdu_in_cur"Data "pdu_in_vol"
Type	temperaturefanspeedhumiditycounterpercenttimeleftvoltagecurrentpowerapparent_powerpower_factorfrequency	data type
Table	truefalse	reflects if the OID is part of a table or not
Instance	truefalse	If **Table** is true: A SNMP OID prefix that will be walked to retrieve a list of names that will be associated with the corresponding values. For example, in a PDU this could be the outlet name. If **Table** is false: The name [of the instance] that will be associated with the value, as a string.
Instance Prefix	String	*Optional.* A string to the prepend to the Instance, enclosed in double quotes.
Values	truefalse	If **Table** is true: The SNMP OID prefix that will be walked to retrieve a list of values. If **Table** is false: The SNMP OID used to retrieve a single value.
Scale	Decimal value	*Optional.* A 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 does only require an adjustment in the `Collect` setting. The values list should contain a list of all data entries which should be collected. All listed data entries require a corresponding data entry definition.

IPMI Discovery Template

The ‘discover’ template for IPMI will automatically discover all the sensors available on an IPMI device.

The template will have only one subsection, Host, and the options of interest are:

Table 91: IPMI Options

SETTING	VALUE	DESCRIPTION
AuthType	nonemd2md5straight	The authentication type for the IPMI protocol. The default is to negotiate the strongest one.
Privilege	callbackuseroperatoradmin	The privilege level for the IPMI protocol. The default is `admin`.
Sensor	Name of the Sensor to be collected	Selects sensors to collect or to ignore, depending on **IgnoreSelected**. May be defined multiple times, each one selecting one sensor.
IgnoreSelected	truefalse	If true, will not collect that for the sensors selected by **Sensor**. If false will only collect the sensors selected by **Sensor**.
Scale	“”	*Optional.* A decimal value to be multiplied to the value retrieved before persisting it.

Enabling Monitoring

Monitoring is enabled on a per-device basis. The settings are part of the Managed Device settings. To enable Monitoring are the following steps required:

- Navigate to the device in the `Managed Device` section.
- Navigate on the specific device to the `Management` section
- Enable and configure the required monitoring protocol like SNMP or IPMI
- Enable Monitoring and assign the template and assign the collection interval.

Dashboard

Nodegrid provides the dashboard tool to visually see Event Details, Managed Device details, and monitoring data from the system and the Managed Devices. It gives the flexibility to create several dashboards for different purposes and monitor managed devices data points such as Power Consumption, Voltage (V), Current (A), Temperature, Fan speed, and many more. It provides options to show data from a different period of times such as the last 15 minutes, the last hour, the last day, this week, this month, the last 5 years.

The Dashboard guide will provide a starting point on how to create simple and useful Dashboards which can be expanded if needed and allow users to create the relevant dashboards.

> Note: The Dashboard feature is only available through the WebUI

Exploring Data Points

This section is not required, but it will describe how to verify that the collected data are stored and to learn more about the data being collected. The raw data points which are collected can be viewed by performing the steps below.

1. Click on `Dashboard`
2. Click on `Discover`
3. Select the desired Index Pattern
   - `logstash-*` contains monitored data
   - `*_date_*` contains event notifications
4. By default, all data are displayed which were collected in the defined time frame.
   - Adjust the time frame as needed
   - Use the `Search` field to search for a specific device or data point
5. Verify that data points where collected and inspect the available fields.

> Note: As collected data is buffered before being stored, it can take a couple of collection cycles before the data can be visualized.

The following fields can be used in search expressions.

Data Point fields (`logstash-*` Index)

Table 92: Data Point Fields

FIELD	VALUE	DESCRIPTION
host	Device Name	The name of the device being monitored.
plugin	snmpipminominalaggregation	Name of the collection plugin
plugin_instance	sumaverage	Theinstance of the plugin collecting the data, if the plugin requires it. Present in the aggregation plugin
collectd_type	temperaturefanspeedhumiditycounterpercenttimeleftvoltagecurrentpowerapparent_powerpower_factorfrequency	Type of measurement
type_instance	Data Point Name	The name of the element associated with the measurement

Device fields (`logstash-*` Index)

Table 93: Device Fields

FIELD	VALUES	DESCRIPTION
name	Device Name	The name of the device being monitored.
mode	enabledondemanddisabled	operational mode of the device
type	device type	Device type as assigned to the device under `Managed Devices`
family	ilodracipmi_1.5ilmi_2.0cimc_ucsdevice_consolepdu	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	

Table 93: Device Fields

FIELD	VALUES	DESCRIPTION
groups	list of groups	The authorization groups which have granted access to the device
licensed	yesno	device license state
status	connecteddisconnectedin-useunknown	The current status of the device
nodegrid	Nodegrid hostname	The hostname of the Nodegrid that controls the device
custom fields		Any custom field configured for the device

Event fields (`*_date_*` Index)

Table 94: Event Fields

FIELD	VALUE	DESCRIPTION
event_id	Number	Event ID number
event_msg	Text	Event Message
host	Nodegrid hostname	hostname of the Nodegrid where the Event occurred.
message	Text	Full message text

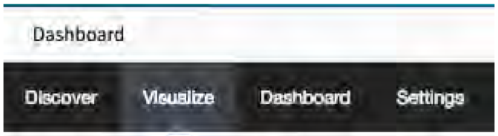
Creating a Visualization

Visualizations allow the gathered data to be displayed on a Dashboard. Visualization includes a wide variety of different options to display and aggregate data. The following sections cover a small subset of the options available and aim to be a starting point in the creation process of custom visualizations.

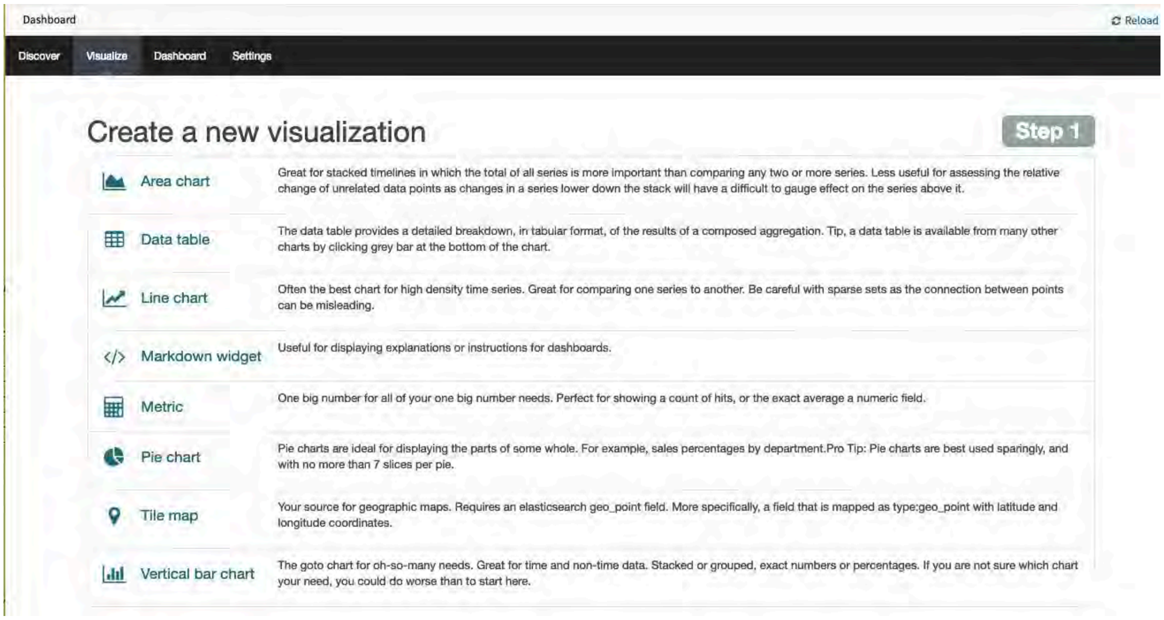
Line Charts

Line Charts allow the visualization of data points along the line graph.
The following process outlines the general steps to create a line chart:

1. Click on `Visualize`



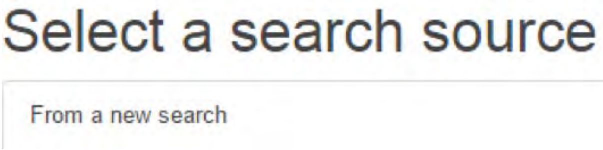
2. Select a Visualization Style to be used. In this example, a `Line Chart` will be created



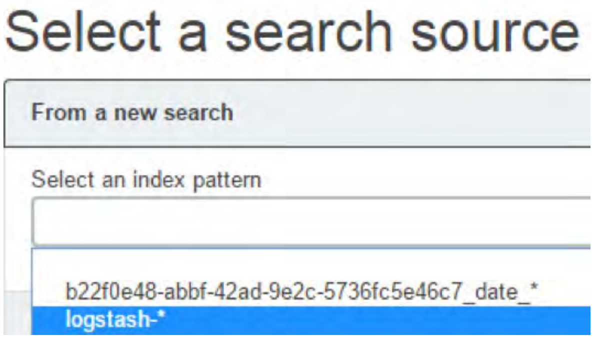
Create a new visualization

Area chart	Great for stacked timelines in which the total of all series is more important than comparing any two or more series. Less useful for assessing the relative change of unrelated data points as changes in a series lower down the stack will have a difficult to gauge effect on the series above it.
Data table	The data table provides a detailed breakdown, in tabular format, of the results of a composed aggregation. Tip, a data table is available from many other charts by clicking grey bar at the bottom of the chart.
Line chart	Often the best chart for high density time series. Great for comparing one series to another. Be careful with sparse sets as the connection between points can be misleading.
Markdown widget	Useful for displaying explanations or instructions for dashboards.
Metric	One big number for all of your one big number needs. Perfect for showing a count of hits, or the exact average a numeric field.
Pie chart	Pie charts are ideal for displaying the parts of some whole. For example, sales percentages by department.Pro Tip: Pie charts are best used sparingly, and with no more than 7 slices per pie.
Tile map	Your source for geographic maps. Requires an elasticsearch geo_point field. More specifically, a field that is mapped as type:geo_point with latitude and longitude coordinates.
Vertical bar chart	The goto chart for oh-so-many needs. Great for time and non-time data. Stacked or grouped, exact numbers or percentages. If you are not sure which chart your need, you could do worse than to start here.

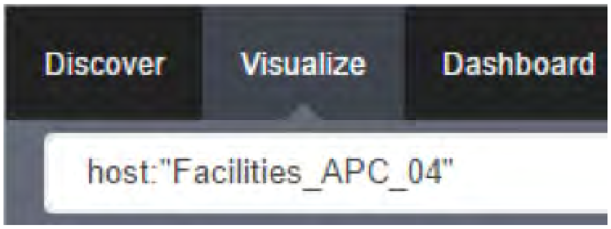
3. `Select a search source` by clicking on **From a new search**.



4. Select **logstash-*** as `index pattern`

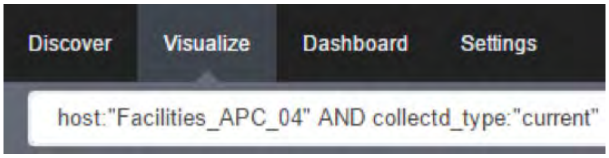


5. Select the data points you want to visualize by entering a search expression such as `host:”<device name>”` in the search field.



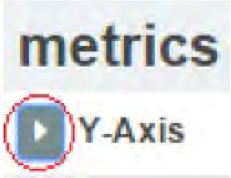
host:"Facilities_APC_04"

6. The search expression can be extended to be more selective.

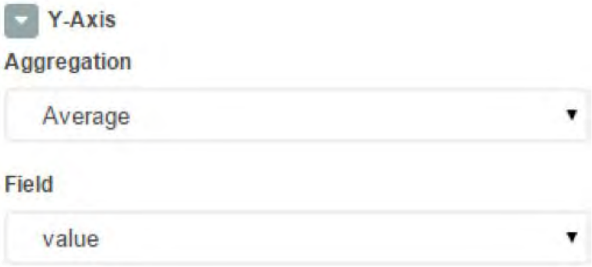


host:"Facilities_APC_04" AND collectd_type:"current"

7. Click on the `Arrow` to the left of Y-Axis to expand it.



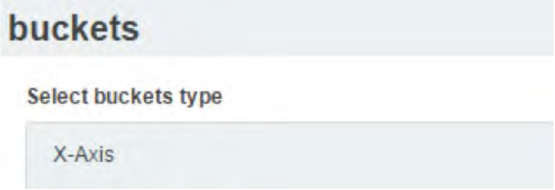
8. Select **Average** for `Aggregation` and **value** for Field.



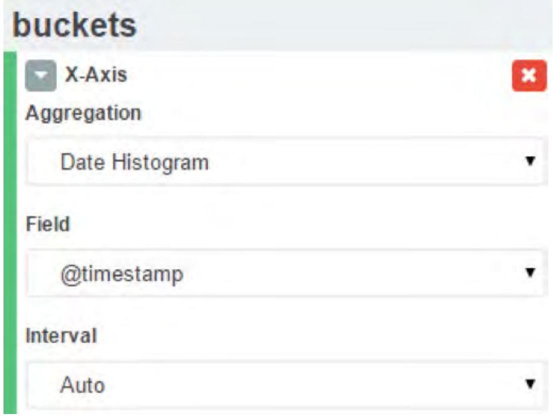
Aggregation: Average

Field: value

9. Click on X-Axis.



10. Select **Date Histogram** as `Aggregation`. Leave `Field` and `Interval` as default. If you just want your visualization to be a single-line graph, skip the next sub-steps, as the next steps will split the data point set into a multi-line graph.



buckets

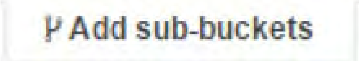
X-Axis

Aggregation: Date Histogram

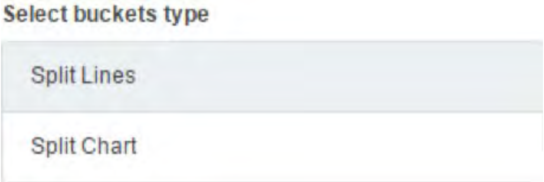
Field: @timestamp

Interval: Auto

11. Click on `Add sub-buckets` to add multiple data points.



12. Click on `Split Lines`.

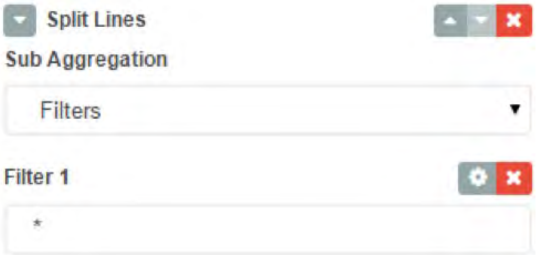


Select buckets type

Split Lines

Split Chart

13. Select **Filters** as `Sub Aggregation`.

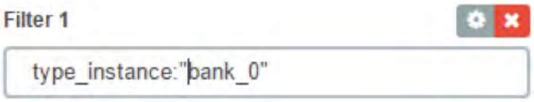


Split Lines

Sub Aggregation: Filters

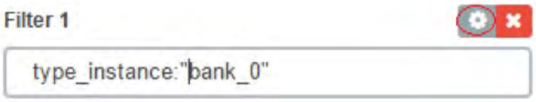
Filter 1: *

14. Enter a search expression to select the element you want to visualize.



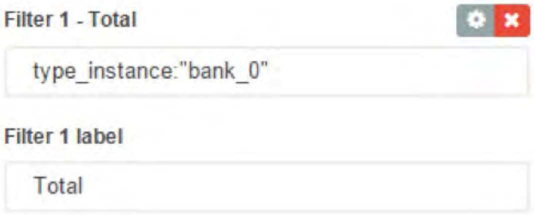
Filter 1: type_instance:"bank_0"

15. Optionally, associate a label by clicking on the `settings icon`



Filter 1: type_instance:"bank_0"

16. provide a **label**



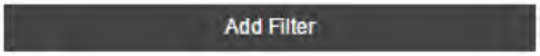
Filter 1 - Total

type_instance:"bank_0"

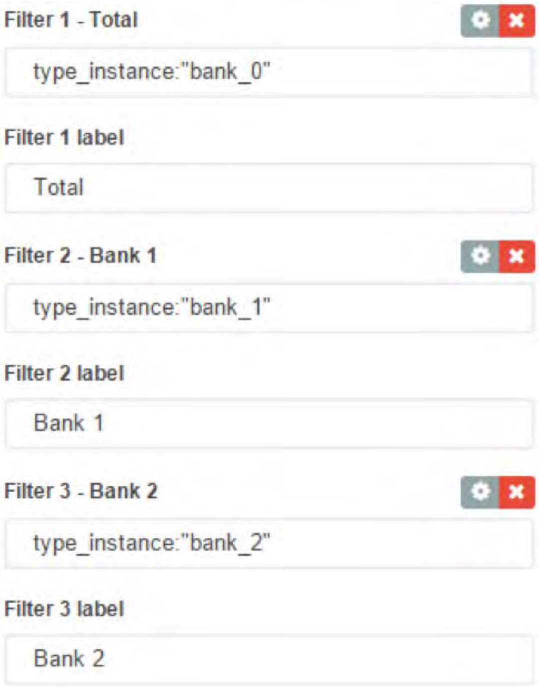
Filter 1 label

Total

17. Click on `Add Filter` to add another element to the visualization



18. Repeat these steps to add all desirable elements



Filter 1 - Total

type_instance:"bank_0"

Filter 1 label

Total

Filter 2 - Bank 1

type_instance:"bank_1"

Filter 2 label

Bank 1

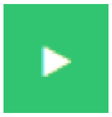
Filter 3 - Bank 2

type_instance:"bank_2"

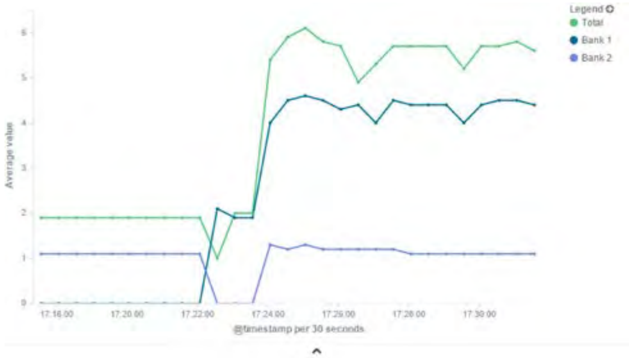
Filter 3 label

Bank 2

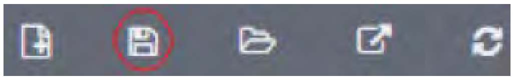
19. Click on the green arrow to refresh the graph based on the configuration provided.



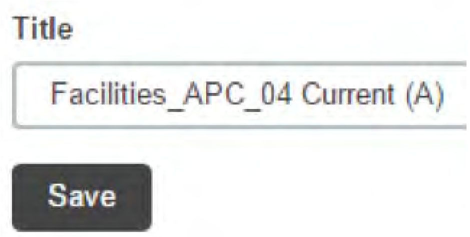
20. The graph will reflect the configuration provided.



21. Click on the `Save` icon to save the visualization.



22. Provide a **Title** for the visualization and click on `Save`.



Title

Facilities_APC_04 Current (A)

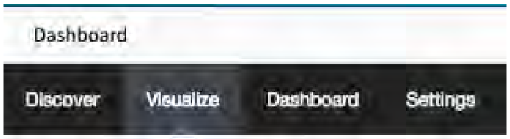
Save

Area Charts

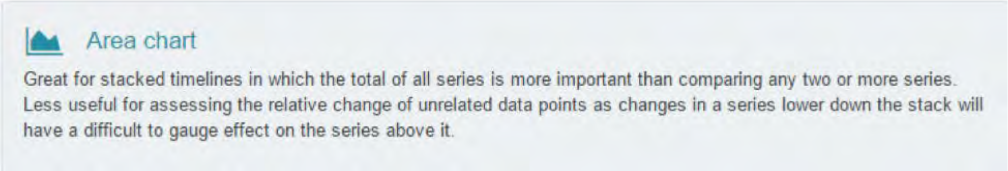
The area chart is useful for stacking measurements for different although related entities, such as the outlets of a PDU.

Note: Review the `Line Chart` section before continuing with the `Area Chart`

1. Click on `Visualize`



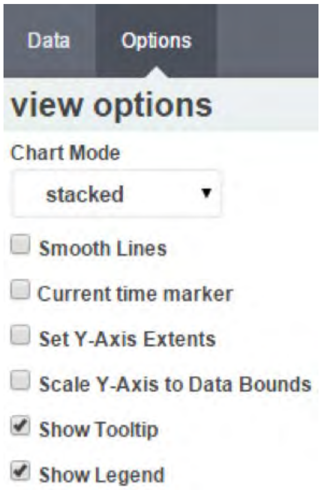
2. Select a Visualization Style to be used. In this example, a `Area Chart` will be created



Area chart

Great for stacked timelines in which the total of all series is more important than comparing any two or more series. Less useful for assessing the relative change of unrelated data points as changes in a series lower down the stack will have a difficult to gauge effect on the series above it.

3. Configure the visualization options to have `Chart Mode` as **stacked**.



view options

Chart Mode

stacked ▾

☐ Smooth Lines

☐ Current time marker

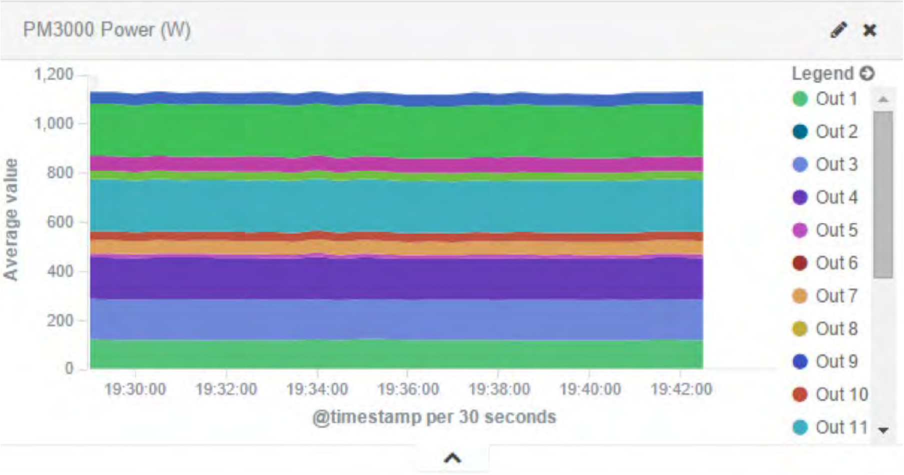
☐ Set Y-Axis Extents

☐ Scale Y-Axis to Data Bounds

☑ Show Tooltip

☑ Show Legend

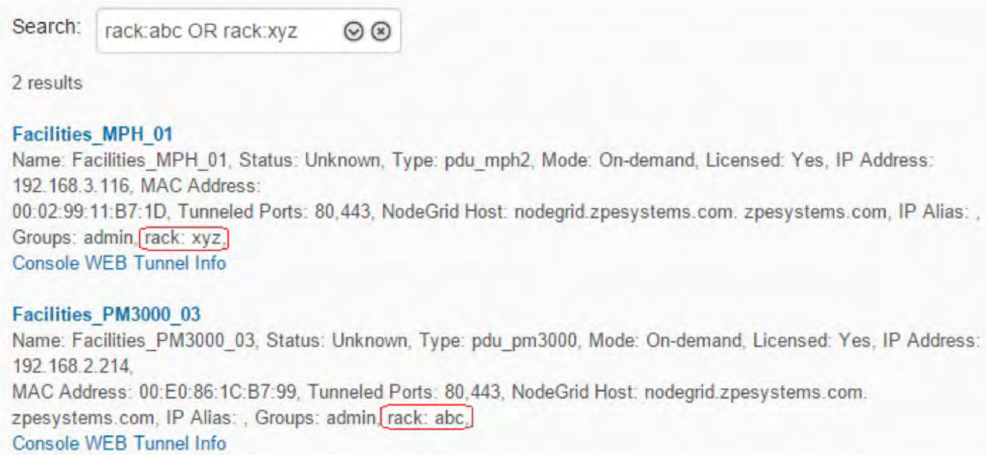
This is the appearance of such a visualization



All search expressions are used to select, or limit the data points that will be used to compose 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.

These search expressions are not restricted to the data points' fields, but they can also refer to fields associated with the device in Nodegrid, such as type, IP address, authorization groups, custom fields, and more

For example, to collect the current provided by each outlet in a selection of Rack PDUs, one with the custom field “rack:abc” and another with “rack:xyz”.



Search: rack:abc OR rack:xyz

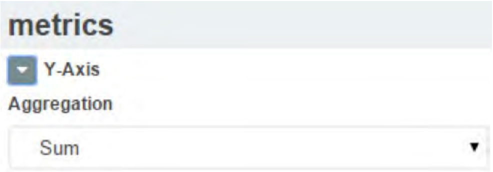
2 results

Facilities_MPH_01
Name: Facilities_MPH_01, Status: Unknown, Type: pdu_mph2, Mode: On-demand, Licensed: Yes, IP Address: 192.168.3.116, MAC Address: 00:02:99:11:B7:1D, Tunneled Ports: 80,443, NodeGrid Host: nodegrid.zpesystems.com. zpesystems.com, IP Alias: , Groups: admin, rack: xyz,
Console WEB Tunnel Info

Facilities_PM3000_03
Name: Facilities_PM3000_03, Status: Unknown, Type: pdu_pm3000, Mode: On-demand, Licensed: Yes, IP Address: 192.168.2.214, MAC Address: 00:E0:86:1C:B7:99, Tunneled Ports: 80,443, NodeGrid Host: nodegrid.zpesystems.com. zpesystems.com, IP Alias: , Groups: admin, rack: abc,
Console WEB Tunnel Info

To show the total sum of the current provided by outlets of each Rack PDU the following settings can be used:

- Visualization `Aggregation` as **Sum**

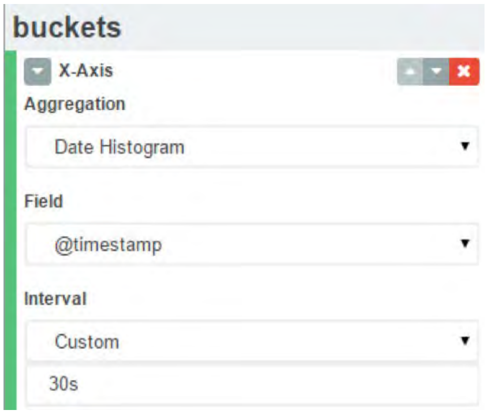


metrics

Y-Axis

Aggregation: Sum

- The `buckets` interval to match the collecting period



buckets

X-Axis

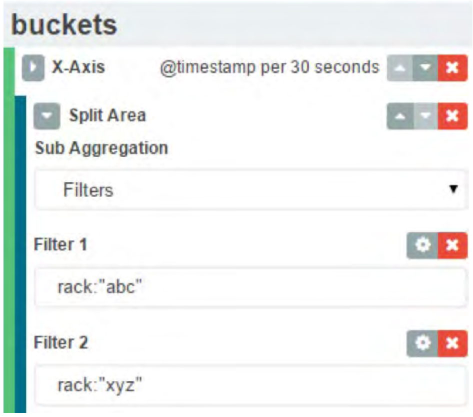
Aggregation: Date Histogram

Field: @timestamp

Interval: Custom

30s

- `Sub-Aggregation` filters are set to custom fields



buckets

X-Axis @timestamp per 30 seconds

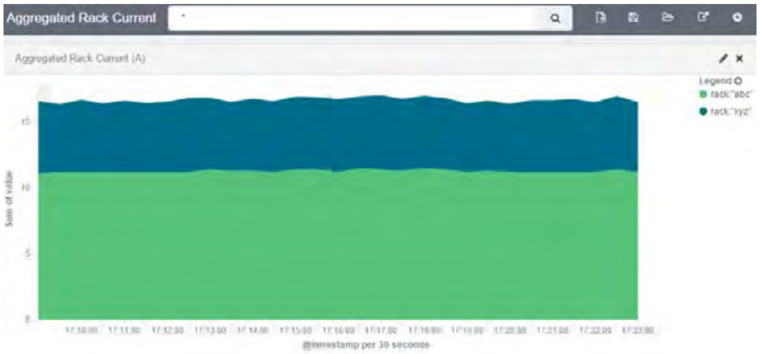
Split Area

Sub Aggregation: Filters

Filter 1: rack:"abc"

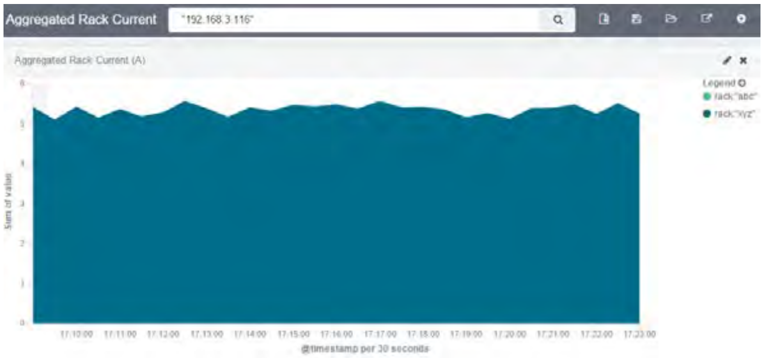
Filter 2: rack:"xyz"

The resulting visualization would look like this:



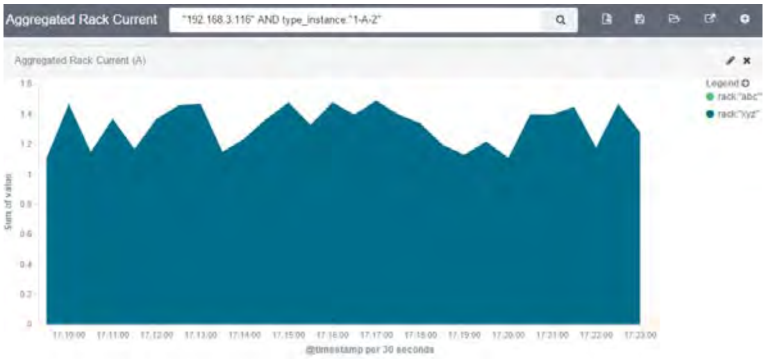
*

- Filters can be added to display the values of only one Rack PDU by using the IP address



"192.168.3.116"

- Additional filters can be used as needed, all from the same visualization.



"192.168.3.116" AND type_instance:"1-A-2"

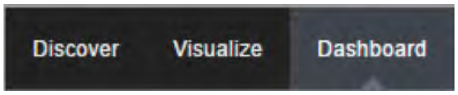
Note: When using area charts too careful to not account for the same measurement twice, by mixing power consumers and power producers, or a Rack PDU's input and output power.

Creating a Dashboard

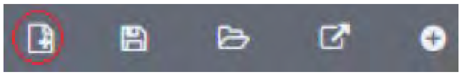
Dashboards are a collection of one or more visualizations. They can be changed or new Dashboards can be created.

The following steps outline how a new Dashboard can be created:

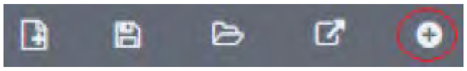
1. Click on Dashboard.



2. Click on the new dashboard icon.

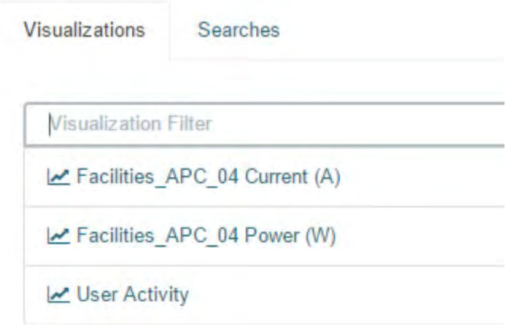


3. Click on the add visualization icon.

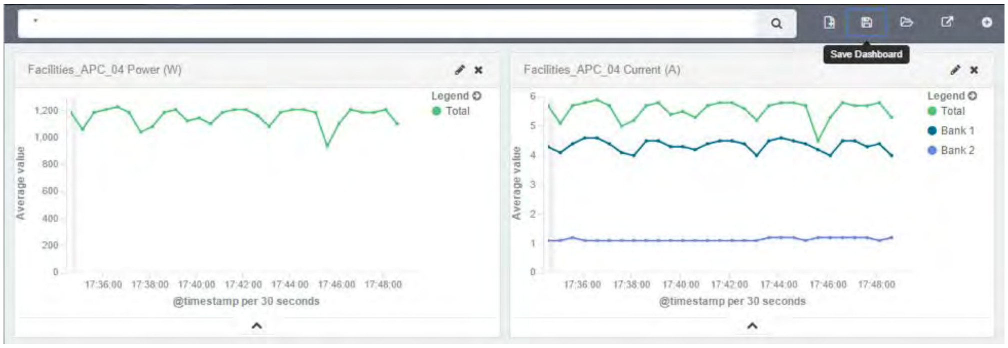


This will show the previously saved visualizations.

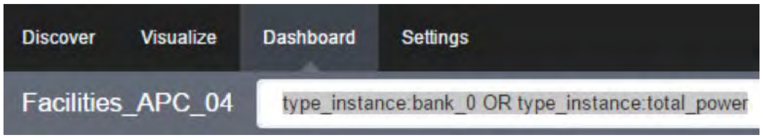
4. Click on the visualization you want to add to the dashboard.
5. Repeat the previous steps until all the desired visualizations are added.



6. Resize and reposition the graphs as needed.

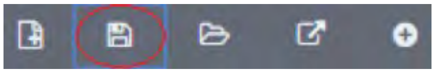


If applicable, filters can be added to the dashboard.

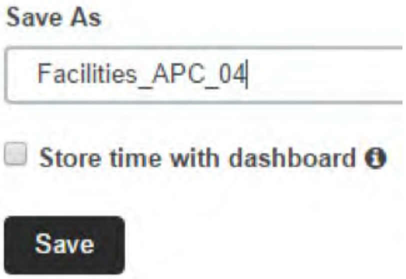


type_instance:bank_0 OR type_instance:total_power

7. Click on the save icon.



8. Provide the dashboard name and then click on save.



Save As

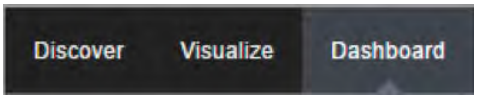
Facilities_APC_04

□ Store time with dashboard

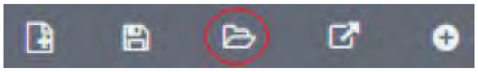
Inspecting a Dashboard

From this point on the dashboard can be opened and viewed by following these steps:

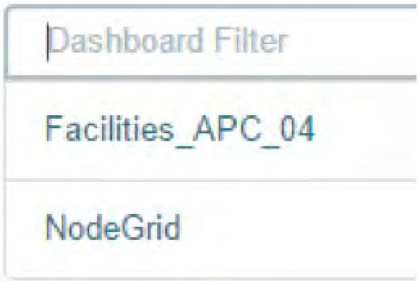
1. Click on Dashboard.



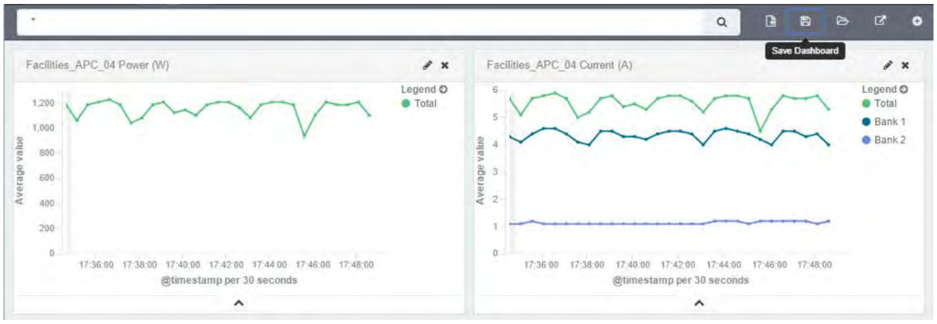
2. Click on the folder icon.



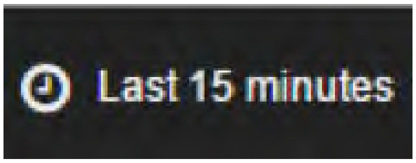
3. Click on the dashboard name. It is possible to search for a dashboard by entering a search expression in the dashboard filter.



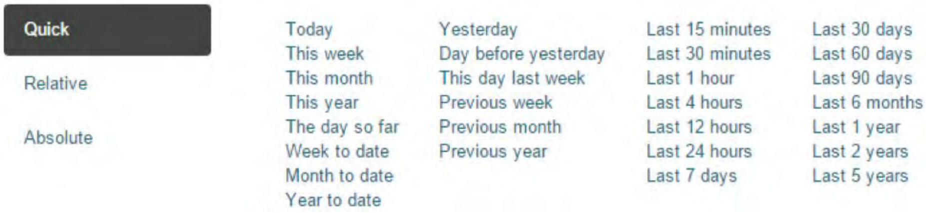
4. The selected dashboard will show up.



- The display time frame can be adjusted by clicking on the clock icon.



5. Select a new time frame.



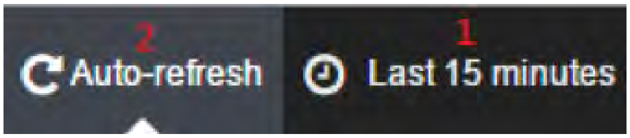
Today
This week
This month
This year
The day so far
Week to date
Month to date
Year to date

Yesterday
Day before yesterday
This day last week
Previous week
Previous month
Previous year

Last 15 minutes
Last 30 minutes
Last 1 hour
Last 4 hours
Last 12 hours
Last 24 hours
Last 7 days

Last 30 days
Last 60 days
Last 90 days
Last 6 months
Last 1 year
Last 2 years
Last 5 years

- It is possible to automatically refresh the Dashboard by clicking on the auto-refresh icon and select the refresh frequency



Applications

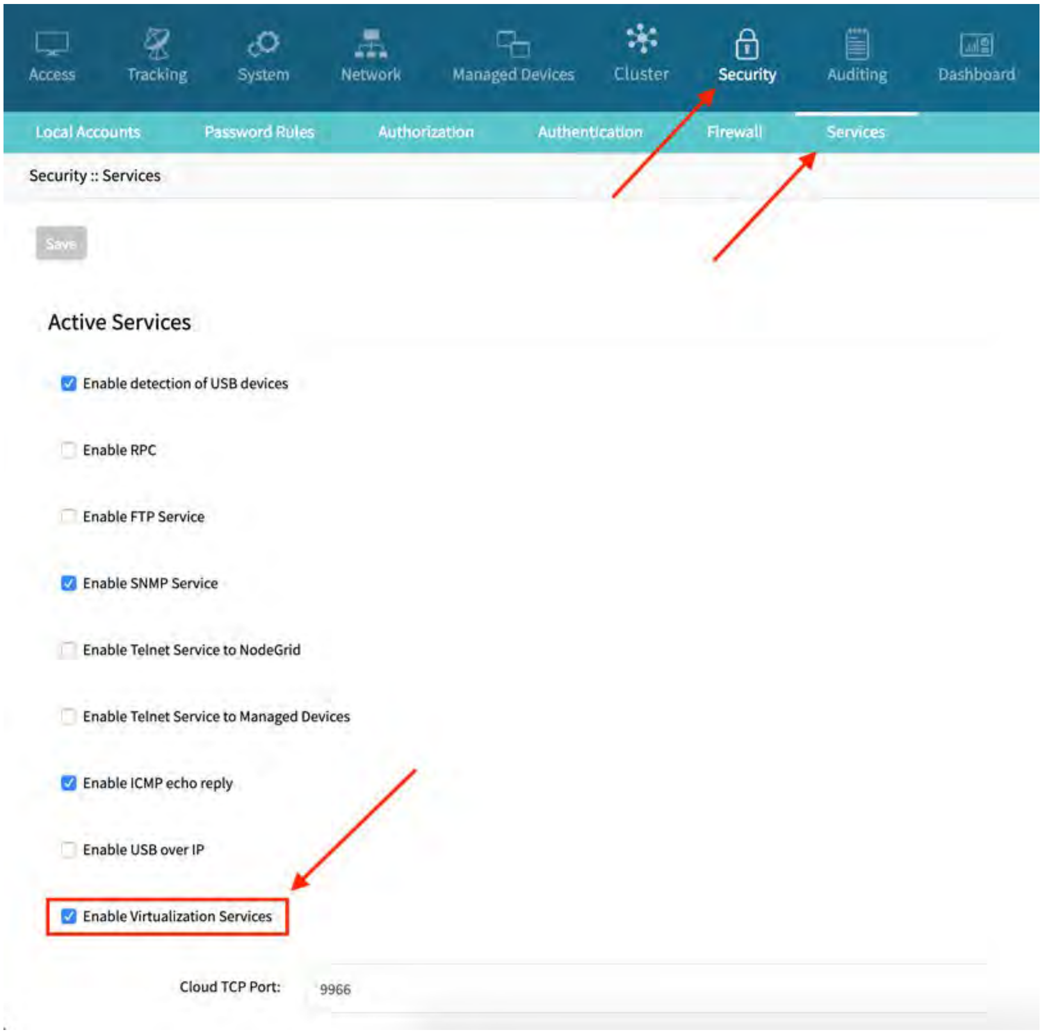
The Nodegrid platform allows you to run additional applications directly on it. This is mostly used to expand software capabilities, like running specific applications close to the end devices. The most common use cases are in the areas of monitoring and SD-WAN. While all Nodegrid units support this feature, the Services Router Family is specifically designed to run applications and provides a wide variety of connectivity options.

> Note: The applications feature requires additional licenses to be installed. The Virtualization service is by default disabled and needs to be enabled under `Services`

Docker Applications

Docker is an open platform for building, shipping and running distributed applications. The Nodegrid platform allows administrators to run Docker applications. The platform allows pulling of Docker applications from **Docker Hub**, starting and stopping of the Docker Containers.

Note: "Enable Virtualization Services" must be enabled in Security :: Services in order to run NFV's or Docker apps. Both features require licenses (System :: License).



Security :: Services

Active Services

☑ Enable detection of USB devices

□ Enable RPC

□ Enable FTP Service

☑ Enable SNMP Service

□ Enable Telnet Service to NodeGrid

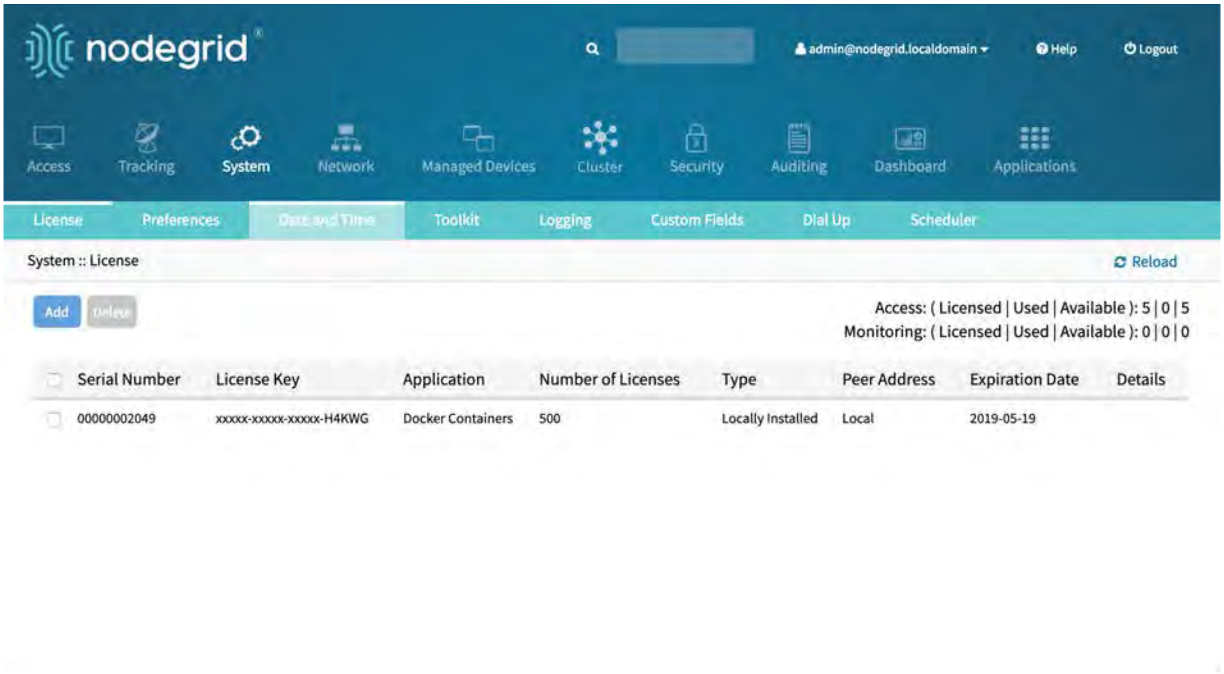
□ Enable Telnet Service to Managed Devices

☑ Enable ICMP echo reply

□ Enable USB over IP

☑ Enable Virtualization Services

Cloud TCP Port: 9966



System :: License

Access: (Licensed | Used | Available): 5 | 0 | 5
Monitoring: (Licensed | Used | Available): 0 | 0 | 0

Serial Number	License Key	Application	Number of Licenses	Type	Peer Address	Expiration Date	Details
00000002049	xxxxx-xxxxx-xxxxx-H4KWG	Docker Containers	500	Locally Installed	Local	2019-05-19	

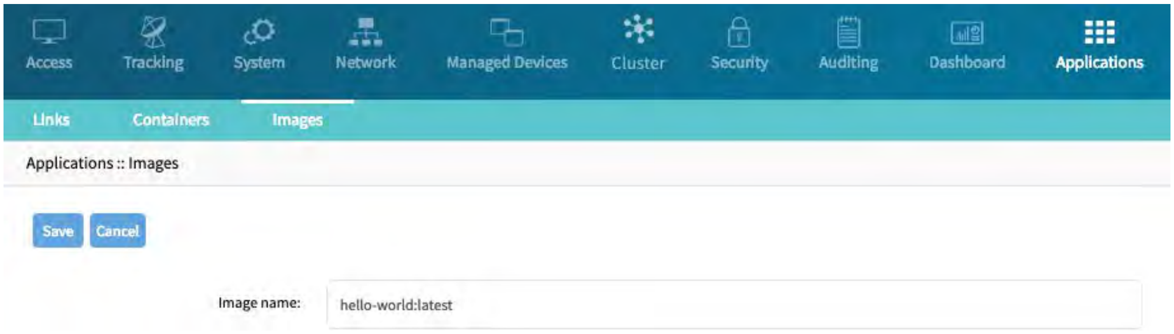
Note: The management of Docker Applications is currently only available through the WebUI. The WebUI provides a basic interface to manage Docker Containers. For more advanced features can administrators use the docker command line tools.

Docker Images

The `Applications::Images` section allows administrators to download and to delete specific Docker containers images. They can be directly downloaded from **Docker Hub**. For this, Nodegrid requires direct network access to Docker Hub.

New Images can be download following the below steps:

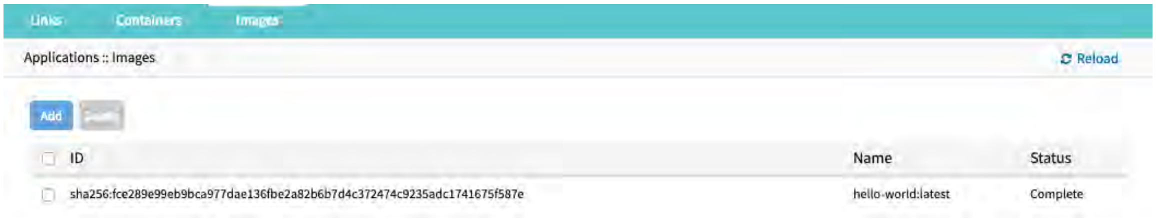
1. Navigate to `Applications::Images`
2. Click on `Add`
3. Provide the image which should be downloaded, specific versions can be downloaded by using the `:` sign



Applications :: Images

Image name: hello-world:latest

4. Click on `Save`, the image will now be downloaded



☐	ID	Name	Status
☐	sha256:fce289e99eb9bca977dae136fbe2a82b6b7d4c372474c9235adc1741675f587e	hello-world:latest	Complete

Docker Containers

The `Applications::Containers` section allows administrators to add a container based on an existing image to the Nodegrid system. The container can be started, stopped and deleted if required.

For additional detail see the official Docker create documentation.

> Note: After the container was created it will not be started automatically.

To add a container follow the following steps:

1. Navigate to `Applications::Containers`
2. Click on Add
3. Provide the following information

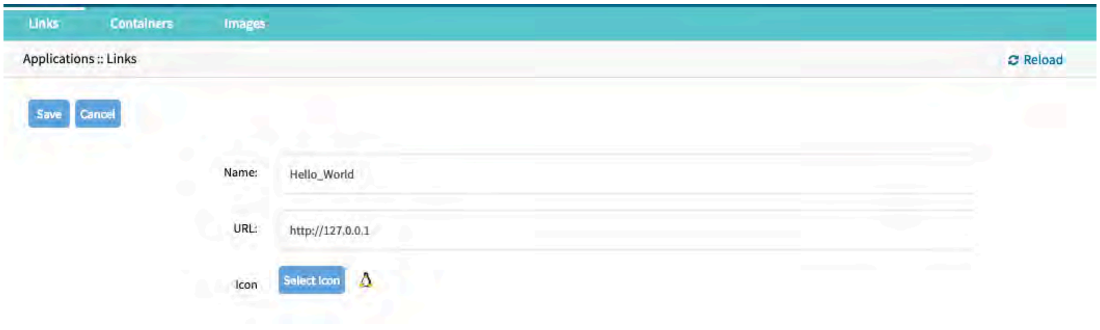
Table 95: Container Information

SETTING	VALUE	DESCRIPTION
Image name	name of a Docker Image	List of valid image names can be found under `Applications :: Images`
Command	Command	Optional, command which will be run within the container
Hostname	hostname	Hostname which will be assigned to the container
Domain	domain name	Domain name which will be assigned to the container
Container Name	Name	Name of the Docker container
CPUs	NUMBER	Amount of CPU's which will be assigned to the container
Memory(MB)	NUMBER	Amount of RAM assigned to the container
Arguments	Arguments	Optional, Options which will be used when the container is created

Application Links

Application Links allow administrators to create simple web links to running containers and other applications.

1. Navigate to `Applications::Links`
2. Click on `Add`
3. Provide a `Name` for the link
4. Provide a valid URL in the `URL` field
5. Select an Icon as desired by clicking on `Select Icon`

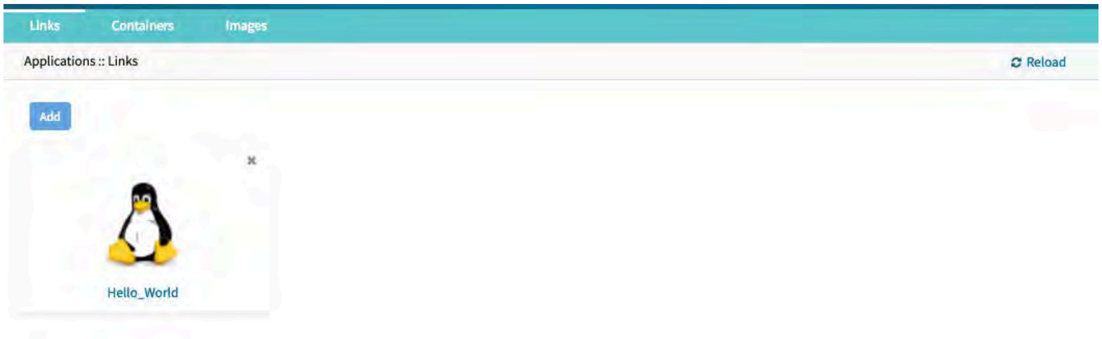


Name: Hello_World

URL: http://127.0.0.1

Icon

6. The link will now be available



Note: Depending on the Application might it be advantages to create a target device for the created Application.

Network Function Virtualization

The Nodegrid platform allows administrators to run additional NFV's or other Virtual Machines. A large variety of configuration options is available through the command line interface.

Please contact Technical Support for more information.

Appendix

Technical Support

Our Technical Support staff are standing by to provide assistance in case you have any operational or installation issues regarding your licensed Nodegrid product. In order to be assisted in the fastest way possible, please follow the steps below:

- Reference the relevant section of this manual to see if the problem can be solved by following the recommended procedure
- Check our Online help documentation at www.zpesystems.com/support
- Visit our Help Center Website for our Knowledge Base and other useful links

Submit a Support Ticket

To submit an online ticket request for support follow the following steps:

1. Click on `Submit a request` link in the top right corner of the page.
2. Enter the required information on the request form. Provide as much detailed information as possible on the description of the problem or question.
3. If there is an attachment, add a file or drop the file in the drop area.
4. Check the `I'm not a robot` check box.
5. Click on `Submit`

You will receive an Email from ZPE Systems confirming that your request has been received. The Email will as well contain your ticket number. Please note the ticket number as you may need to refer to it later.

Updates and Patches

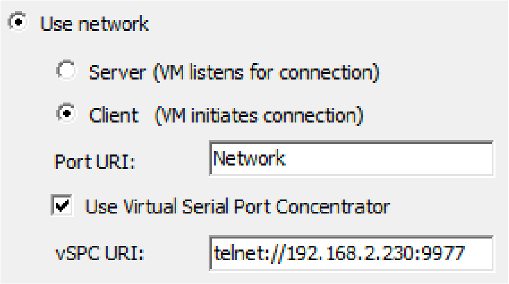
To automatically receive information about important security patch announcements, future firmware updates, and other technical information, sign up to **The Loop** at www.zpesystems.com/loop/

Configuring Virtual Serial Port (vSPC) on VM Servers

In order to redirect the VMware virtual machine vSPC data to the Nodegrid Platform, the virtual machine serial port needs to be configured as described below:

1. Go to ESXi configuration (vSphereTM). Select the virtual machine you want to connect and click the Edit Virtual Machine Settings link;
2. Click Add. The virtual machine must be turned off;
3. Click Serial Manager Device, then click on Next in the pop-up window;
4. Click Connect Via Network, then click Next;
5. Select Client (VM initiates the connection) – this is the default
6. For Port URI, type <group_id> where group_id is an identifier that can be used during the auto-discovery to relate servers of the same group. This field is optional.
7. On vSPC URI, type telnet://<IP or Nodegrid Manager hostname>:9977

8. Click Finish.



● Use network

○ Server (VM listens for connection)

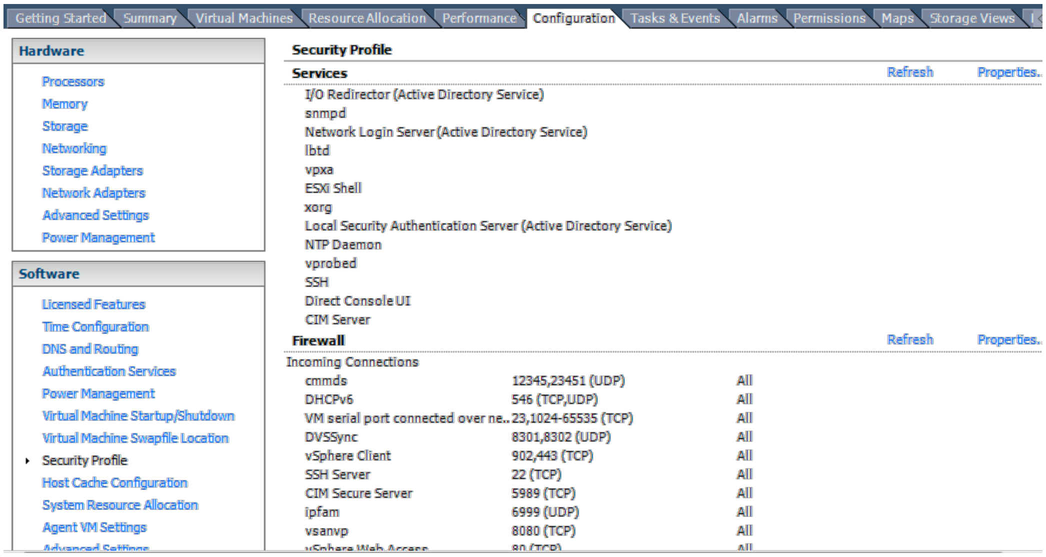
● Client (VM initiates connection)

Port URI: Network

☑ Use Virtual Serial Port Concentrator

vSPC URI: telnet://192.168.2.230:9977

9. Finally, make sure that vSPC port is enabled on the ESXi firewall. In order to check that, go to ESXi Configuration, select Security Profile and click on Properties.



Security Profile

Services

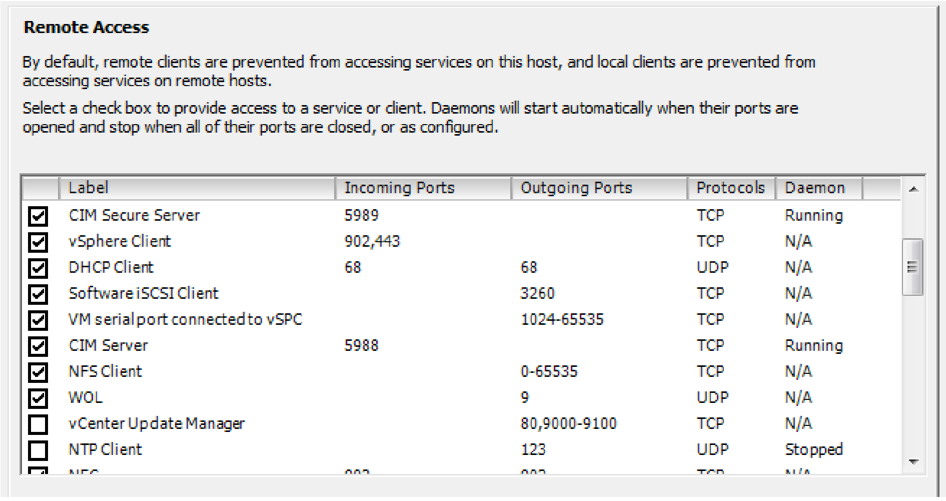
I/O Redirector (Active Directory Service)
snmpd
Network Login Server (Active Directory Service)
lbtd
vpxa
ESXi Shell
xorg
Local Security Authentication Server (Active Directory Service)
NTP Daemon
vprobed
SSH
Direct Console UI
CIM Server

Firewall

Incoming Connections

cmmds	12345,23451 (UDP)	All
DHCPv6	546 (TCP,UDP)	All
VM serial port connected over ne...	23,1024-65535 (TCP)	All
DVSSync	8301,8302 (UDP)	All
vSphere Client	902,443 (TCP)	All
SSH Server	22 (TCP)	All
CIM Secure Server	5989 (TCP)	All
ipfam	6999 (UDP)	All
vsanvp	8080 (TCP)	All
vSphere Web Access	80 (TCP)	All

On the Remote Access page, check the box related to VM serial port connected to vSPC. The Outgoing Ports should have a TCP port range starting from 1024 or higher and the port range must include the TCP port used on the vSPC URI field (default 9977).



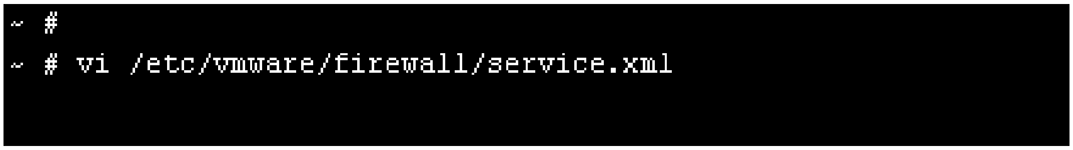
Remote Access

By default, remote clients are prevented from accessing services on this host, and local clients are prevented from accessing services on remote hosts.

Select a check box to provide access to a service or client. Daemons will start automatically when their ports are opened and stop when all of their ports are closed, or as configured.

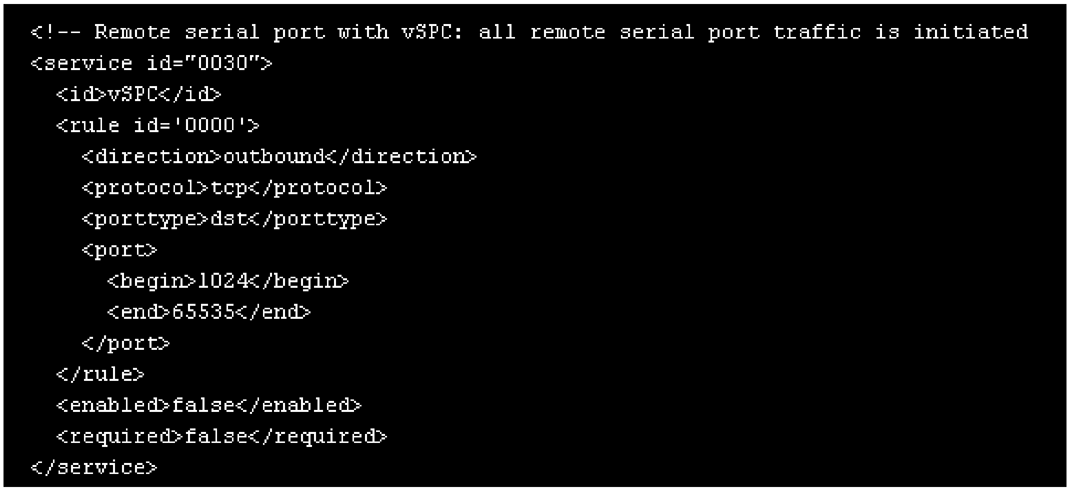
	Label	Incoming Ports	Outgoing Ports	Protocols	Daemon
☑	CIM Secure Server	5989		TCP	Running
☑	vSphere Client	902,443		TCP	N/A
☑	DHCP Client	68	68	UDP	N/A
☑	Software iSCSI Client		3260	TCP	N/A
☑	VM serial port connected to vSPC		1024-65535	TCP	N/A
☑	CIM Server	5988		TCP	Running
☑	NFS Client		0-65535	TCP	N/A
☑	WOL		9	UDP	N/A
□	vCenter Update Manager		80,9000-9100	TCP	N/A
□	NTP Client		123	UDP	Stopped
☑	NFC	902	902	TCP	N/A

To modify the outgoing port range, connect to the ESXi command line and execute the following commands:



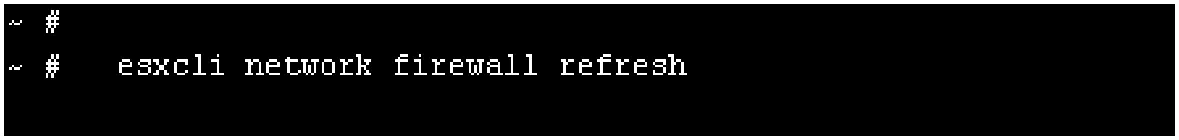
```
~ #
~ # vi /etc/vmware/firewall/service.xml
```

Edit the port section:



```
<!-- Remote serial port with vSPC: all remote serial port traffic is initiated
<service id="0030">
  <id>vSPC</id>
  <rule id='0000'>
    <direction>outbound</direction>
    <protocol>tcp</protocol>
    <porttype>dst</porttype>
    <port>
      <begin>1024</begin>
      <end>65535</end>
    </port>
  </rule>
  <enabled>false</enabled>
  <required>false</required>
</service>
```

Save the changes and then restart the firewall service:



```
~ #
~ #   esxcli network firewall refresh
```

For further information on VMware firewall, please refer to the VMware Knowledge Base.

DC Power

DC power is connected to DC-powered equipment using 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 your power source is the correct type and that your 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.

Fundamentals

Dual DC Power Connection Terminal Block

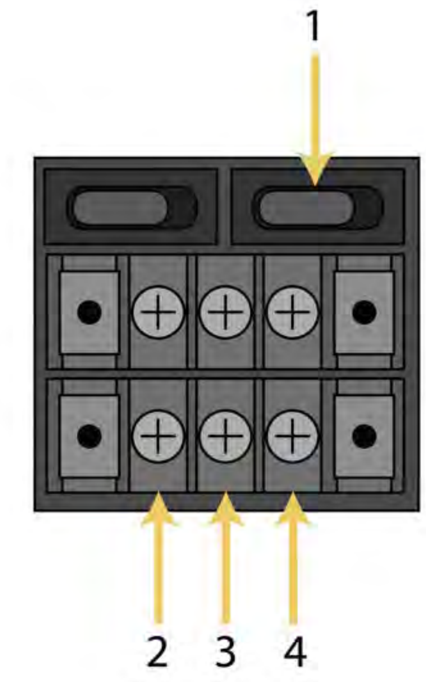
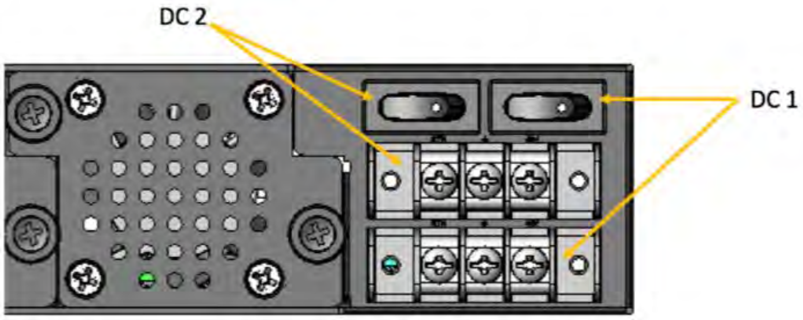


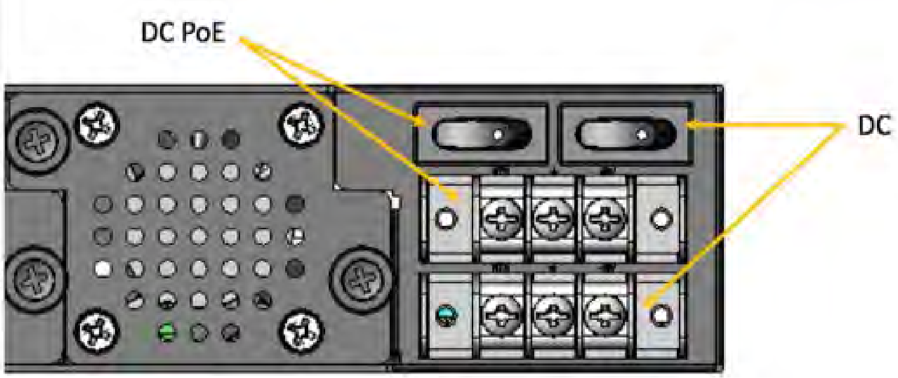
Table 96: DC Power Block Terminals

NUMBER	DESCRIPTION
1	Power Switch
2	RTN (Return)
3	Ground
4	48 VDC

DC association - terminal power source and switch



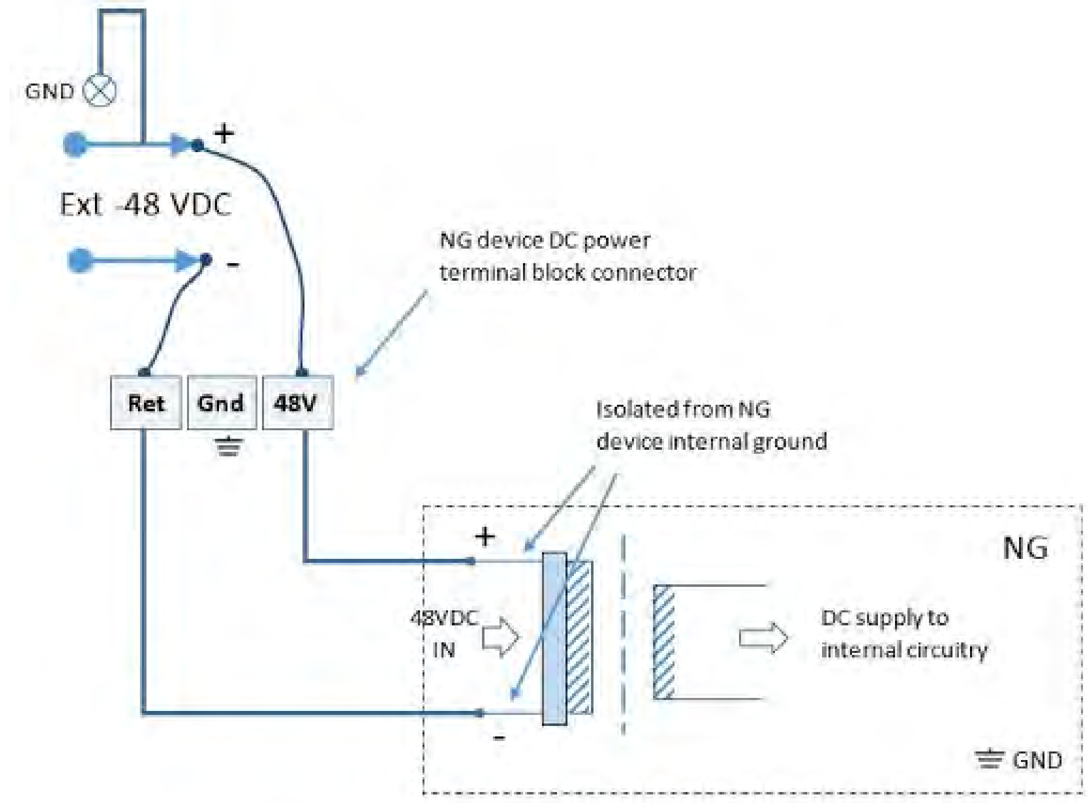
NSR Single DC + PoE Power Connection Terminal Block



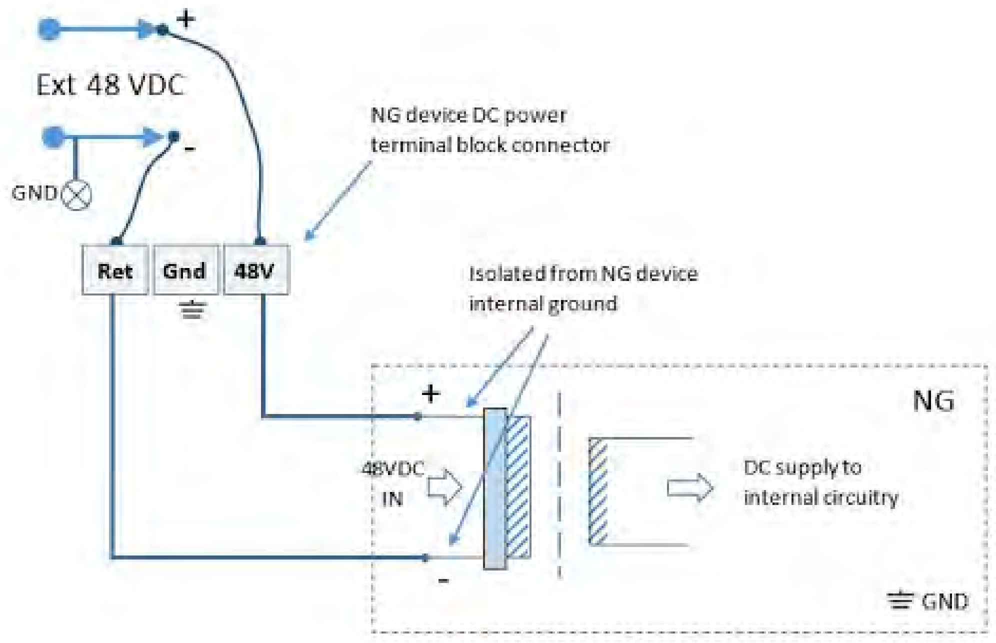
To power on a Nodegrid unit using DC power:

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

Case of -48VDC supply

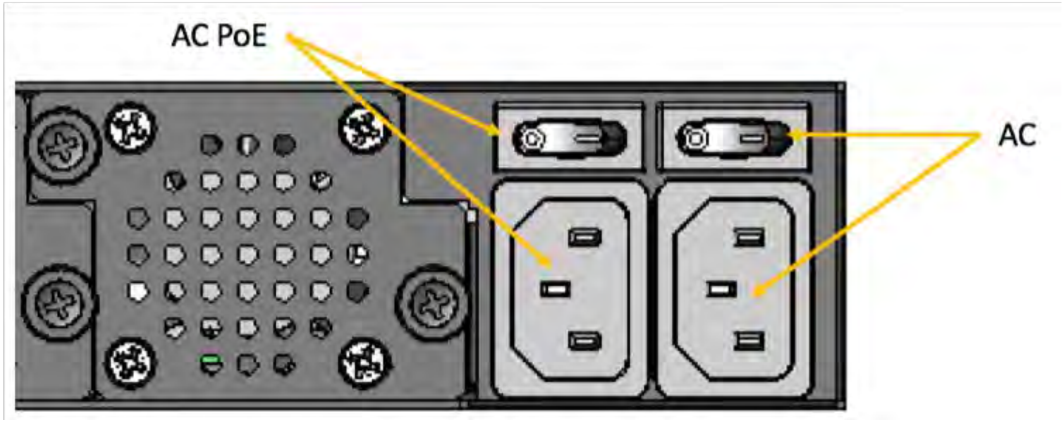

GND
+
Ext -48 VDC
-
NG device DC power terminal block connector
Ret
Gnd
48V
Isolated from NG device internal ground
+
NG
48VDC IN
DC supply to internal circuitry
-
GND

Case of +48VDC supply


+
Ext 48 VDC
-
GND
NG device DC power terminal block connector
Ret
Gnd
48V
Isolated from NG device internal ground
+
NG
48VDC IN
DC supply to internal circuitry
-
GND

AC Power

AC diagram for the NSR models with PoE+ support



Serial Port Pinout

The tables below display serial port pinout information.

Table 97: 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

Table 98: 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, user data resulting from keystrokes, managed devices output, and device monitoring data passing through our product may be stored in nonvolatile device memory when data logging or monitoring is enabled in the configuration settings.

The Nodegrid devices contain the following 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

There are two ways to remove user data from the nonvolatile memory of Nodegrid unit:

- **Soft Removal**: removes files and installs factory default configuration on flash disk.
- **Hard Removal**: completely erases the flash disk. This procedure will destroy ALL data on flash disk and render it unrecoverable even by data recovery services. After that, the Nodegrid software must be reinstalled via network.

Soft Removal

Erase the nonvolatile memory of Nodegrid using the following procedure:

1. Shutdown Nodegrid unit and power it off
2. Remove Nodegrid unit from the network (disconnect Ethernet cables of the unit)
3. Disconnect any USB storage device and USB network device connected to Nodegrid unit
4. Access Nodegrid unit with one of the following options:
    - Nodegrid console port using an RJ-45 console adapter and a straight-through network cable connected to a terminal or workstation.
    - HDMI port and USB port connected to an HDMI monitor and USB keyboard.
5. Power on Nodegrid unit and select 'Nodegrid - Rescue Mode' in the following menu:

```
*****************************************************************************
*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.`
```

6. At the prompt ("bash-4.3#"), run this command to erase all files and load factory configuration, without quotation marks (‘’): 'apply_settings --factory-and-cleanlogs -f -h'
7. Wait for the following message:

```
Apply factory settings completed.  INIT:
Switching [ ... ] reboot: System halted
```

8. Power off the unit.

Hard Removal - Secure Erase

Erase the nonvolatile memory of Nodegrid unit using the following procedure:

1. Shutdown Nodegrid unit and power it off
2. Remove Nodegrid unit from the network (disconnect Ethernet cables of the unit)
3. Disconnect any USB storage device and USB network device connected to Nodegrid unit
4. Access Nodegrid unit with one of the following options:
    - Nodegrid console port using an RJ-45 console adapter and a straight-through network cable connected to a terminal or workstation.
    - HDMI port and USB port connected to an HDMI monitor and USB keyboard.
5. Power on the unit
6. Press the 'Esc' key after the BIOS setup page appears on your screen
7. Select 'Nodegrid Platform - Secure Erase' in the Grub Menu:

```
                             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 to be power cycled (powered off and powered on) prior to executing the erase command. Otherwise, the following message will show and the system will halt to allow the user to perform a power cycle as required:

```
Operation not supported. Unit must be power cycled prior to erase com-
mand. Wait for system halt and power cycle the unit.  [ 4.614365]
reboot: System halted
```

9. Confirming

```
Secure erase cannot be canceled once confirmed.  Type 'yes' to confirm
secure erase:
```

10. Wait for the message 'System halted'.

```
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:  Issu-
ing 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

Credits

Contact us
Sales: sales@zpesystems.com
Support: support@zpesystems.com
ZPE Systems, Inc. 46757 Fremont Blvd. Fremont, CA 94538 USA
www.zpesystems.com