NVIDIA MELLANOX NEO DOCUMENTATION

Software version 2.7

Exported on Nov/14/2023 08:31 PM

Table of Contents

NVIDIA® Mellanox® NEO® is a powerful platform for managing scale-out computing networks. Mellanox NEO enables data center operators to efficiently provision, monitor and operate the modern data center fabric. Mellanox NEO serves as interface to the fabric, thus extending existing tools capabilities into monitoring and provisioning the data center network. Mellanox NEO uses an extensive set of REST APIs to allow access to fabric-related data and provisioning activities. Mellanox NEO eliminates the complexity of fabric management. It automates the configuration of devices, provides deep visibility into traffic and health, and provides early detection of errors and failures.

The documentation here relates to:

- Release Notes
- User Manual

Intended Audience

This manual is intended for cluster and data center administrators who are responsible for the deployment, configuration, and day-to-day maintenance of Mellanox devices.

Software Download

To download product software, please refer to the NEO Software Download product page.

Document Revision History

A list of the changes made to the user manual are provided in User Manual Revision History.

Typography

The following table describes typographical conventions in Mellanox documentation. All terms refer to isolated terms within body text or regular table text unless otherwise mentioned in the Notes column.

Term, Construct, Text Block	Example	Notes
File name, pathname	/opt/neo/controller/conf/controller.conf	-
Console session (code)	-> flashClear <CR>	Complete sample line or block. Comprises both input and output. The code can also be shaded.
Linux shell prompt	#	The "#"character stands for the Linux shell prompt.
String	< > or []	Strings in < > or [ ] are descriptions of what will actually be shown on the screen, for example, the contents of <your ip> could be 192.168.1.1

Related Documentation

For additional information, see the following documents and links:

- Mellanox NEO® REST API User Manual
- Mellanox NEO® SDK User Manual
- Telemetry Agent User Manual
- Free online training

Document Conventions

The following conventions might appear in this document.

Note: Identifies important information that contains helpful suggestions

Warning: Alerts you to the risk of personal injury, system damage, or loss of data.

Alert: Warns you that failure to take or avoid a specific action might result in personal injury or a malfunction of the hardware or software. Be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents before you work on any equipment.

Release Notes

These release notes pertain to the Mellanox NEO software.

System Requirements

Mellanox NEO Server Requirements

Platform	Type and Version (Up to 20 Nodes)	Type and Version (Above 20 Nodes)
OS	RedHat/CentOS 7.4, 7.5, 7.6, 7.7, 7.8	
CPU	8-core server and above	24-core server and above
RAM	16GB and above	32GB and above
Disk	10G* + 500MB per switch	

⚠ If NEO is managing more than 20 switches, you must use SSD disk for the machine running NEO.

⚠ For IP Discovery to load, DNS should be configured properly on installed machine or hostname should be defined at /etc/hosts file.

Supported Platforms and Operating Systems

Platform	Operating System
Bare metal server	RedHat/CentOS 7.x
Virtualized Environment	
Linux virtualization	RedHat/CentOS 7.x
Microsoft Hyper-V virtualization	Windows Server 2008 R2 Windows Server 2012 Windows Client 10 Windows Server 2016
VMware virtualization	VMware Workstation 15.1.0 ESXi 6.7.0
Oracle VirtualBox	6.08

Mellanox NEO GUI Client Requirements

Supported Browser	Browser Version
Microsoft Edge	80.0.361 and above
Chrome	62 and above

Supported Browser	Browser Version
Firefox	72.0.2 and above
Safari	11.0 and above

⚠ Deprecated Safari versions on Windows are not supported by NEO.

Recommended Screen Resolutions

Screen Type	Screen Size	Recommended Resolution
Desktop	23”	1920 X 1080
Laptop	15”	1366 X 786
Tablet	9.7”	1024 X 768

Supported Mellanox Internally Managed Systems

Platform	Device	Software Version
Mellanox SN2000 Series	SN2010 SN2100 SN2100B SN2410 SN2410B SN2700 SN2700B SN2740	Mellanox Onyx v3.9.1014 or above Cumulus Linux 3.6.2 or above
Mellanox SN3000 Series	SN3420	
Mellanox SN4000 Series	SN4600C	
HPE M-Series	SN2100M SN2410M SN2410bM SN2700M	Mellanox Onyx v3.9.1014 or above
Edgecore	AS4610	Cumulus Linux 3.2 or above

⚠
- The latest supported Mellanox Onyx version is: 3.9.1014
- The latest supported Cumulus version is: 3.7.9
- Support for Mellanox Onyx SwitchX family systems stopped starting from Mellanox NEO version v2.4

Key Features

Feature	Description
Telemetry	Enables the user to collect telemetry data from Spectrum based managed switches, and stream it to external data collectors.
Device Management	Enables chassis discovery, health monitoring and running operations (reboot, software-upgrade) on managed systems
Device Provisioning	Enables the user to run commands on selected systems
Port & Device Monitoring	Enables the user to collect all managed switches ports traffic and error counters via the SNMP protocol
Ethernet Discovery	Enables the user to discover the managed devices' connectivity via the LLDP protocol
Report Management	Enables the user to generate and save traffic counter graphs
Events	Enables the user to receive notifications on the managed systems and the Mellanox NEO application, and enables the use to define rules for events triggering
Task and Job Management	Enables the user to centralize task running on managed switches, and enables tracking running and completed jobs in the system
Task Sequence	Enables the user to create and manage sequences of tasks which can be executed at any time
Running and Tracking Configuration Info	Enables the user to view the current running configuration of every managed switch system, and notifies the user of network configuration changes, summarizing all systems configuration changes
Dashboard	Provides a summary of the managed site's traffic and events behavior
RoCE Dashboard	The RoCE Dashboard contains a snapshot of the RoCE related network state, including information on service state, traffic and events. RoCE services can also be added and managed from this dashboard.
What Just Happened (WJH)	A dashboard that contains information about packet drops in the fabric.
Network Mismatch Analysis	Notifying the user on a network configuration mismatch – for example: MTU mismatch, Mellanox Onyx mismatch
Topology Map	Enables the user to have a graphical view of managed network topology
Configuration Management	Enables the user to edit and apply running configuration files (Global Configuration), CLI files (Provisioning Templates) and to save/restore old running configurations (Network Snapshots).
Cable Information	Enables the user to present cable information of selected devices, ports and groups
NIC Capabilities	Enables the user to retrieve important information about managed Hosts Adapter Cards (HCAs)
Performance Monitoring	Enables the user to run performance checks between two hosts
Performance Health Check	Enables the user to run performance health tests between all managed hosts or for randomly selected hosts
Service View and Bring-up Wizard	Enables the user to apply selected network configurations and validate these configurations periodically
High Availability	Enables the user to use a cluster of nodes for high availability of network management
Cumulus Linux Support	Added support for Cumulus Linux network operating system operated over Mellanox switch systems

Changes and New Features

This section lists the new features and changes in this Mellanox NEO® version.

Feature	Description
Rev 2.7	
New system support	Added support for SN3420, SN3700, and SN4600C switch systems
What Just Happened®	WJH is now enabled on Mellanox NEO by default upon Telemetry Agent installation
	WJH now supports up to 5K WJH drops per second
	Added ability to enable/disable WJH events per severity
	Added the ability to filter out WJH events by category, severity or reason (Streaming Settings)
	Enhanced wording for WJH events
	Updated WJH dashboard
Connectivity check	Added ability to verify device connectivity across multiple communication protocols

Bug Fixes in This Release

Ref. #	Issue
2146982	**Description:** Reported aggregated traffic for the switch in the Network Map view is displayed incorrectly.
	Keywords: Switch, Network Map
	Discovered in version: 2.6
	Fixed in version: 2.7
2170410	**Description:** Upgrading from 2.3-2.6 with Event Policy configured causes NEO to fail to load.
	Keywords: Upgrade, fail, event policy
	Discovered in version: 2.6
	Fixed in version: 2.7

Known Issues

This section lists the known issues in this version of Mellanox NEO® with available workarounds.

Ref. #	Issue
2388786	**Description:** Network map periodically refreshes. When that happens, selected items become unselected.
	Workaround: N/A
	Keywords: Network Map

Ref. #	Issue
	Detected in version: 2.7
2412055	**Description:** The What Just Happened button "Export to CSV" is missing from UI.
	Workaround: N/A
	Keywords: WJH, WebUI
	Detected in version: 2.7
2187852	**Description:** Any change related to the "RoCE" sub-category under "Events Policy" on NEO 2.4 or below will be lost upon NEO upgrade. User is required to reconfigure it after the upgrade.
	Workaround: N/A
	Keywords: RoCE, upgrade
	Detected in version: 2.7
2107670	**Description:** When working with NEO, any switch configuration done directly on the switch (via switch CLI) might be conflicted with NEO configuration and interfere with NEO switch management and configuration.
	Workaround: N/A
	Keywords: NEO, CLI, configuration, conflict, overwrite
	Detected in version: 2.7
2225134	**Description:** In Streaming Settings, the events "TTL value is too small" and "Packet size is larger than MTU" (under Forwarding > L3) are always streamed even if configured otherwise.
	Workaround: N/A
	Keywords: Streaming, MTU, TTL
	Detected in version: 2.7
2147008	**Description:** RoCE service does not display MLAG port-channel traffic.
	Workaround: N/A
	Keywords: RoCE, MPo
	Detected in version: 2.7
2211606	**Description:** The NEO dashboard, the WJH dashboard specifically, may at times become slow to respond.
	Workaround: N/A
	Keywords: WJH, dashboard, slow
	Detected in version: 2.7
2248362	**Description:** Upgrading Mellanox NEO to software version 2.7 rebuilds the database and removes all Telemetry and WJH data.
	Workaround: N/A
	Keywords: WJH, database
	Detected in version: 2.7
2239514	**Description:** Any task with a snapshot created on top of it in NEO 2.4 version (or older) is displayed under "Telemetry" → "Snapshots", not under "Tasks".
	Workaround: N/A
	Keywords: Telemetry, task, snapshot
	Detected in version: 2.7
2239662	**Description:** Any collector added to a telemetry session in NEO version 2.4 (or older) is detached from the session after Mellanox NEO upgrade.
	Workaround: Reattach collector after software upgrade.

Ref. #	Issue
	Keywords: Collector, session, upgrade
	Detected in version: 2.7
2245329	**Description:** WJH buffer drop trap_probability is probability to extract the packet from stream of the packets that get exception. If the packet rate is low the extraction rate can deviate from configured value.
	Workaround: N/A
	Keywords: WJH
	Detected in version: 2.7
2098905	**Description:** NEO OpenStack integration is supported only over HTTPS protocol (HTTP is not supported).
	Workaround: N/A
	Keywords: HTTPS, OpenStack
	Detected in version: 2.6
2119441	**Description:** NEO supports up to to 10 MPOs in a single "apply MLAG" service.
	Workaround: If more MPOs are required, the service must be updated and re-applied.
	Keywords: MLAG, MPO
	Detected in version: 2.6
-	**Description:** When interoperating with switch systems installed with Onyx 3.9.0300, they may reach high CPU utilization.
	Workaround: Run the command "ssh server login record-period 1" in order to avoid this.
	Keywords: Onyx, high CPU utilization
	Detected in version: 2.6
2126093	**Description:** Mellanox Onyx® switches support up to 64 buffer histogram samplings.
	Workaround: N/A
	Keywords: Histogram, buffer events, telemetry
	Detected in version: 2.6
2118673	**Description:** The following 3rd party systems are not supported by Mellanox NEO®: Arista, Brocade, Cisco, Juniper and HP. It is not possible to add new systems from these vendors to NEO. However, if NEO is upgraded from an older version where these switch systems have been added, then they can be presented and managed without issue. NEO is still able to detect these 3rd party systems by IP range scanning or by LLDP.
	Workaround: N/A
	Keywords: 3rd party, switch systems
	Detected in version: 2.6
2107670	**Description:** Switch configuration performed directly on the switches (via switch CLI) may conflict with Mellanox NEO configuration and interfere with NEO switch management and configuration.
	Workaround: Only use NEO for managing configuration over the managed switches (avoid manual configuration on the managed switches).
	Keywords: Configuration, CLI
	Detected in version: 2.6
1918927	**Description:** In-band migration not supported.
	Workaround: N/A
	Keywords: VLAN provisioning
	Detected in version: 2.6

Ref. #	Issue
1912682	**Description:** Telemetry Agent does not provide telemetry information on split ports if they are configured while the agent is running.
	Workaround: Restart Telemetry Agent.
	Keywords: Telemetry Agent, split ports
	Detected in version: 2.6
1952279	**Description:** Every new device added to NEO must have a unique management IPv4 address, otherwise the displayed devices data might be corrupted.
	Workaround: N/A
	Keywords: Management Elements
	Detected in version: 2.6
2082427	**Description:** When configuring LLDP on the host interface, LLDP must be configured to publish the host management IPv4 address. Otherwise, the host is not presented correctly in Mellanox NEO.
	Workaround: N/A
	Keywords: LLDP
	Detected in version: 2.6
2061726	**Description:** When adding a Cumulus switch to Mellanox NEO, the initial discovery results in SNMP failure. Once SNMP is configured on the switch, it returns to normal status (i.e. "OK").
	Workaround: N/A
	Keywords: Cumulus, SNMP
	Detected in version: 2.6
-	**Description:** NEO v2.5.1 supports up to 50 managed switches. If Mellanox NEO is managing more than 20 switches, it is recommended to use SSD disk otherwise NEO performance issues are expected.
	Workaround: N/A
	Keywords: Managed switches, performance
	Detected in version: 2.5.1
-	**Description:** Running the Telemetry Agent configuration provisioning templates will attempt to restart the Agent, but it will fail to start it. Affected Telemetry Agent Provisioning Templates: • Agent-Active-Ports-Update • Agent-Interval-Factor-Change • Agent-Port-Channel-Discovery
	Workaround: Edit the template in NEO: 1. Click the “Edit” option. 2. Replace the command `docker exec neo-agent "/etc/init.d/telemetryd restart"` with the command `fae docker cmd "restart neo-agent"` 3. Click the “Apply” button to save the changes.
	Keywords: Telemetry Agent Provisioning Templates
	Detected in version: 2.5.1
-	**Description:** Running WJH on a Cumulus switch is not supported. (Up to the release of NEO v2.5, no Cumulus version that supports WJH existed.)
	Workaround: N/A
	Keywords: WHJ, Support, Cumulus
	Detected in version: 2.5
-	**Description:** Running WJH and Threshold Events telemetry sessions on Onyx switches is supported only for Onyx version 3.8.2004 or newer.

Ref. #	Issue
	Workaround: N/A
	Keywords: WJH, Threshold events, Onyx Version
	Detected in version: 2.5
1922607	**Description:** If a device (Linux host or switch) is removed from NEO while some Mellanox switches are running telemetry, then all the telemetry sessions running on these switches will be stopped.
	Workaround: Manually disable and enable telemetry sessions using NEO (Telemetry → Streaming) in order to reactivate the required telemetry sessions.
	Keywords: Telemetry, Device, Remove, Switch, Session, Stop
	Detected in version: 2.5
1917681	**Description:** NEO monitoring over SNMP is not supported for Cumulus switches (due to a known issue in Cumulus switch).
	Workaround: N/A
	Keywords: SNMP, Monitoring, Cumulus
	Detected in version: 2.5
1917323	**Description:** If a switch is unresponsive, NEO will not display a continuous graph of the monitoring data.
	Workaround: N/A
	Keywords: Unresponsive, Switch, Continuous, Monitoring
	Detected in version: 2.5
1920182	**Description:** General device information (Memory and CPU) might be displayed at a delay of 2-4 minutes after the device has been added to NEO.
	Workaround: N/A
	Keywords: General information, Memory, CPU, Delay
	Detected in version: 2.5
1920520	**Description:** In Cumulus switch, in case of “non-ascii” characters used in the switch configuration files, creating configuration backup and network snapshots or restoring from them might fail.
	Workaround: N/A
	Keywords: Cumulus, “non-ascii”, Characters, Configuration
	Detected in version: 2.5
1920601	**Description:** When editing MLAG port channels via MLAG wizard, configuration changes might fail in case telemetry was configured prior to the change (e.g., via the Bring-Up Wizard).
	Workaround: N/A
	Keywords: MLAG, Editing, Configuration, Telemetry
	Detected in version: 2.5
1887761	**Description:** Telemetry agent will not publish telemetry data for MLAG port channel in the following cases: • MLAG port channel of MLAG slave switch • MLAG port channel was disabled and enabled on MLAG master switch In these cases, telemetry data is published for the physical ports (the MLAG port channel members).
	Workaround: N/A
	Keywords: MLAG, Telemetry, MLAG port channel, disabled, enabled
	Detected in version: 2.5
-	**Description:** When upgrading NEO v2.4 to NEO v2.5, due to the transition from Graphite to InfluxDB, historical counters data kept on Graphite will not be transferred to the InfluxDB.

Ref. #	Issue
	Workaround: N/A
	Keywords: Upgrade, Graphite, InfluxDB, counters
	Detected in version: 2.5
1848870	**Description:** General information (CPU and Memory information) for Cumulus switches managed by NEO are not displayed in the NEO interface until it is exposed by the switch. For more information, please refer to Exposing CPU and Memory Information via SNMP.
	Workaround: N/A
	Keywords: CPU and Memory information, Cumulus switches
	Detected in version: 2.5
-	**Description:** RoCE Service configuration is not supported for Onyx versions prior to 3.6.5000.
	Workaround: Upgrade the switch to the latest Onyx version.
	Keywords: Services, RoCE, Onyx
	Detected in version: 2.5
-	**Description:** RoCE Service configuration cleanup is not supported for services upgraded from older NEO versions.
	Workaround: Remove the old service and recreate it with the latest NEO.
	Keywords: Services, Clean-up, RoCE, upgrade
	Detected in version: 2.5
-	**Description:** RoCE Service configuration cleanup is supported only for Onyx and Cumulus switches.
	Workaround: For other service types, remove the configuration manually using switch CLI.
	Keywords: Services, Clean-up, RoCE
	Detected in version: 2.5
-	**Description:** Service configuration clean-up is supported only for RoCE service.
	Workaround: For other service types, remove the configuration manually using switch CLI.
	Keywords: Services, Clean-up
	Detected in version: 2.5
1329530	**Description:** Manual HA takeover or failover might take up to 60 seconds (depending on the machine NEO is running on). During that time, triggering additional failover or takeover operations might result in the original action failure.
	Workaround: Wait for at least 60 seconds between HA operations - failover or takeover.
	Keywords: HA, failover, takeover
	Detected in version: 2.4
1600868	**Description:** Configuring RoCE on a host bond interface is currently not supported.
	Workaround: Configure RoCE on the bond slaves.
	Keywords: Bond, RoCE
	Detected in version: 2.3
1582800	**Description:** Running too many frequent live monitoring sessions for a specific switch may overload the switch's JSON API and result in timeouts.
	Workaround: Run fewer live monitoring sessions in parallel.
	Keywords: JSON, timeout, live monitoring
	Detected in version: 2.3
-	**Description:** When a WJH is enabled on the Telemetry Agent, WJH on the Onyx switch is disabled (the user is not able to view WJH details via Onyx switch CLI) and vice versa.

Ref. #	Issue
	Workaround: N/A
	Keywords: What Just Happened, WJH, Onyx, Telemetry Agent
	Detected in version: 2.3
2090123	**Description:** WJH is supported by NEO only for Onyx Spectrum switches using v3.7.1134, or newer.
	Workaround: N/A
	Keywords: What Just Happened, WJH, Dropped Packets
	Detected in version: 2.3
-	**Description:** NEO-Host installation is supported only for Linux hosts, using one of the following HCAs: ConnectX-4 / ConnectX-4 Lx / ConnectX-5.
	Workaround: N/A
	Keywords: NEO-Host
	Detected in Version: 2.3
1578231	**Description:** NEO telemetry agent can stream Routing Table information up to 20K records, and MAC table information up to 800 records.
	Workaround: N/A
	Keywords: Telemetry Agent, Routing Table, MAC Table
	Detected in Version: 2.3
1417273	**Description:** System icons are not shown for Edge and Safari systems.
	Workaround: N/A
	Keywords: Network Map, Edge, Safari
	Detected in Version: 2.2
1504128	**Description:** The network path calculation requires that all switches along the path will have the same SSH credentials. Otherwise, the calculation will fail.
	Workaround: N/A
	Keywords: Network Path, SSH, Credentials
1484291	**Description:** The telemetry agent cannot be stopped on switches running Onyx OS v3.6.8100.
	Workaround: Do not deploy the telemetry agent on Onyx OS v3.6.8100.
	Keywords: Telemetry Agent, Onyx
1421369	**Description:** The "In Packets rate" calculated counter shows an incorrect value for Cumulus switches only, due to an issue with the switch (the Unicast RX Packets counter always returns a value of zero).
	Workaround: N/A
	Keywords: In Packets Rate, Cumulus, Unicast RX Packets
1498434	**Description:** The network path calculation will display the links transmitted bandwidth utilization according to the maximal value of the aggregated links (in case of a multiple links connection).
	Workaround: N/A
	Keywords: Network Path, Bandwidth, Utilization
1332120	**Description:** Telemetry Agent does not support split ports.
	Workaround: N/A
	Keywords: Telemetry Agent, Split Port
1328501	**Description:** In the MLAG service, the bond is configured with the default gateway.
	Workaround: Configure a different static route to the relevant ports.
	Keywords: MLAG, Bond

Ref. #	Issue
1316429	**Description:** Port live monitoring only works from a certain Onyx version.
	Workaround: N/A
	Keywords: Telemetry, Live Monitoring
1327385	**Description:** Upgrade procedure (from an older version to 2.1.0) does not include Events Policy and RoCE Service.
	Workaround: N/A
	Keywords: Upgrade
1309655	**Description:** Telemetry session interval cannot be changed
	Workaround: N/A
	Keywords: Telemetry Agent
1298137	**Description:** When loading images with a similar name (differed only by tag) the 1st image name becomes empty due to an issue in Red Hat Docker.
	Workaround: N/A
	Keywords: Docker, Container
1272497	**Description:** There is no validation for the maximum ECN value in RoCE Service. The max allowed ECN value is dynamic and depends on switch type, current memory state , etc.
	Workaround: N/A
	Keywords: RoCE Service
1277047	**Description:** Configuring one of the IPL ports in MLAG service to 'switchport mode trunk' fails the service.
	Workaround: Reset switchport mode before adding the port to the IPL.
	Keywords: MLAG Service
1302777	**Description:** Switch reboot stops a telemetry agent session (if running).
	Workaround: After switch reboot, manually restart the telemetry session.
	Keywords: Telemetry
1071652	**Description:** For optimized UI functionalities, LastPass browser add-on should either be disabled or not installed.
	Workaround: N/A
	Keywords: UI, LastPass
-	**Description:** A NEO-Host package installation is required for successful provisioning of RoCE through the new RoCE service.
	Workaround: Install NEO-HOST either on Linux-without-Neo-Host-installed predefined group or on a specific host.
	Keywords: RoCE Service
1064979	**Description:** The MLAG service is supported in MLNX Onyx (MLNX_OS) starting from v3.6.4000.
	Workaround: Make sure to upgrade your Onyx version to v3.6.4000 or above.
	Keywords: MLAG Service
-	**Description:** When using SNMPv3 with sha authentication and priv=aes128 option, the switch will become unreachable due to timeout.
	Workaround: For Mellanox PPC switches, use md5 authentication with a priv=des option.
	Keywords: Authentication
-	**Description:** Mellanox NEO Client (browser) might fail to connect to the NEO server in case the iptables service is running.

Ref. #	Issue
	Workaround: Make sure to disable the iptables service before running NEO installation.
	Keywords: Installation
-	**Description:** VLANs and LAGs information may not be displayed as part of device information for non-Mellanox devices.
	Workaround: N/A
	Keywords: 3rd Party Systems Support
-	**Description:** Linux/Windows host provisioning via NEO is non-persistent.
	Workaround: N/A
	Keywords: Host Provisioning
-	**Description:** NEO start-up will fail in case the machines' local time zone is not configured.
	Workaround: Make sure the installed machines' local time zone is configured. (/etc/localtime file exists).
	Keywords: NEO Start-Up
-	**Description:** Apply Config operation is only available for switches with Onyx v3.6.2000 and above.
	Workaround: N/A
	Keywords: Configuration Management
-	**Description:** Cable information is only supported for Mellanox Onyx switch ports.
	Workaround: N/A
	Keywords: Cable Information
951789	**Description:** Performance tests are only supported for ConnectX-4 and ConnectX-5 family adapter cards.
	Workaround: N/A
	Keywords: Performance Check
-	**Description:** Performance check can be performed only on two Linux hosts, running MLNX_OFED_LINUX-3.3-1.0.4.0 version or higher.
	Workaround: N/A
	Keywords: Performance Check
-	**Description:** RoCE configuration on hosts is non-persistent.
	Workaround: N/A
	Keywords: RoCE Service

Introduction

Mellanox NEO® is a powerful platform for managing scale-out computing networks. Mellanox NEO enables data center operators to efficiently provision, monitor and operate the modern data center fabric.

Mellanox NEO serves as interface to the fabric, thereby extending existing tool capabilities into monitoring and provisioning the data center network. Mellanox NEO uses an extensive set of REST APIs to allow access to fabric-related data and provisioning activities.

Mellanox NEO eliminates the complexity of fabric management. It automates the configuration of devices, provides deep visibility into traffic and health, and provides early detection of errors and failures.

Mellanox NEO incorporates a monitoring mechanism that can be combined with Mellanox Care®, a support program that offers 24/7 fabric management services to monitor network health. This mechanism traps network events and issues regular notifications to Mellanox's Network Operations Center (Mellanox NOC). Special Mellanox personnel analyze the details of the reported events and take action according to the service level agreement (SLA).

Mellanox NEO presents the following benefits:

- Reduces complexity of fabric management
- Provides in-depth visibility into traffic and health information
- Network API supports integration, automation, and SDN programmable fabrics
- Historical health and performance graphs
- Generates preventive maintenance and "soft degradation" alerts
- Quickly troubleshoots topology and connectivity issues
- Integrates and streamlines fabric information for your IT systems
- Combined with Mellanox Care, produces regular event notifications to Mellanox NOC for 24/7 health monitoring

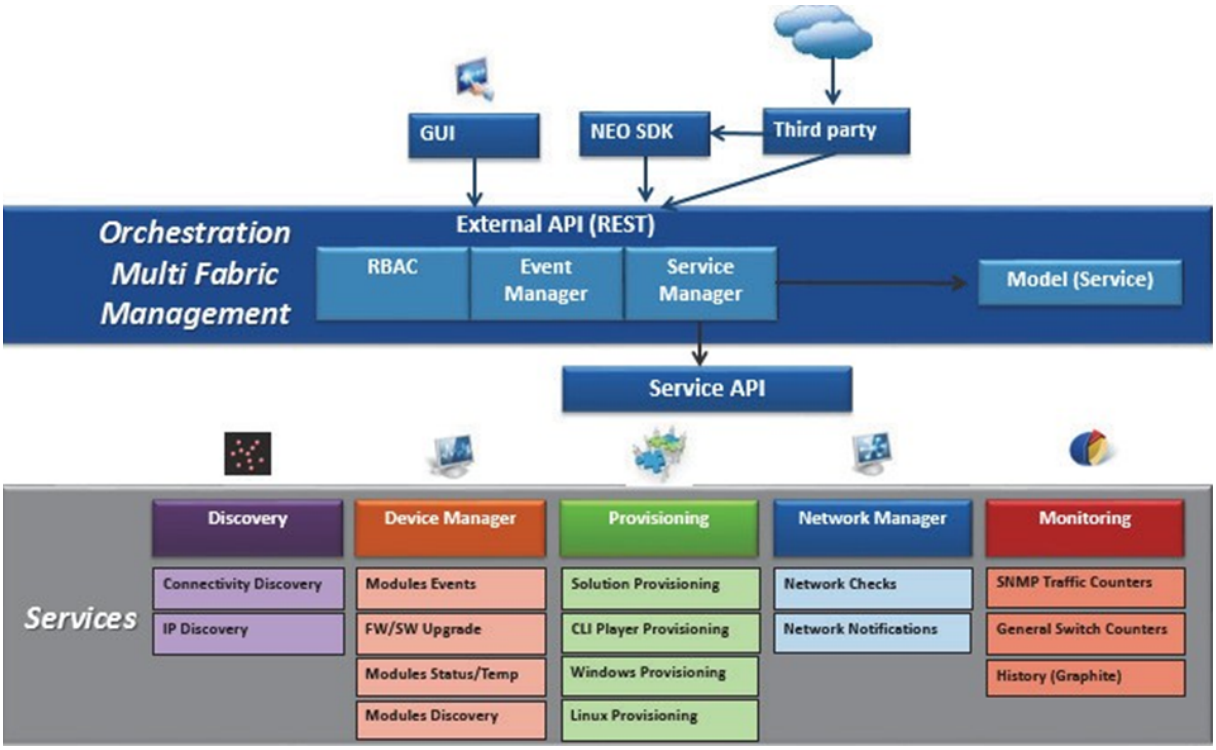
Central Management Console	Mellanox NEO provides network and device management functions via one central console. Its centralized dashboard can be used to monitor, troubleshoot, configure and optimize the system via a single interface.
In-Depth Visibility and Control	Mellanox NEO includes an advanced granular monitoring engine that provides real-time access to switches, enabling cluster-wide health and performance monitoring, real-time identification of problems and failures, and quick problem resolution via granular threshold-based alerts and its utilization dashboard.
Quick Resolution of Problems	Mellanox NEO provides comprehensive information from switches, showing errors and traffic issues such as congestion. The information is presented concisely over a unified dashboard and configurable monitoring sessions. The monitored data can be correlated per job and customer, and threshold-based alarms can be set.
Open Architecture	Mellanox NEO provides an advanced REST interface and SDK package integrated with external management tools. This combination enables data center administrators to consolidate management dashboards while flawlessly sharing information among the various management applications, synchronizing overall resource scheduling, and simplifying provisioning and administration.

Mellanox NEO as Network API	Mellanox NEO serves as an interface to the fabric, thereby extending existing tool capabilities into monitoring and provisioning the data center network. Mellanox NEO uses an extensive set of REST APIs to allow access to fabric-related data and provisioning activities. The interface can provide external tools with the fabric topology, device health and performance status, alerts, and device and fabric management actions. This allows taking advantage of existing tools and enhancing them, as well as building new DevOps oriented management frameworks. For further information on Mellanox NEO API documentation, please refer to the NEO SDK User Manual.

Mellanox NEO Software Architecture

Mellanox NEO architecture includes controller and service providers (Device Manager, Provisioning, Fabric Manager, Monitoring and Access Credentials Manager). The controller transfers information from the service providers to the user, as well as controls the service providers and verifies their status. It queries and fetches information from providers and performs operations such as:

- Storing a list of supported logs per each provider
- Pausing, resuming, resetting, and fetching a specific log
- Maintaining a connection with a provider



Mellanox NEO Graphical User Interface

The Mellanox NEO Web GUI is the front-end of the application. It communicates with the Mellanox NEO REST API in order to retrieve and display the relevant information.

Mellanox NEO Controller

The Mellanox NEO controller is the central component enabling data collection from all the service providers. The collected data is maintained in a central repository. The controller exposes a Restful API that allows retrieving any type of information and running any type of supported actions.

Mellanox NEO Providers

The Mellanox NEO providers listed below are the data sources for the controller. Each provider is an independent process (service) which communicates with the controller.

- Device Management Provider
- Provisioning Provider
- Monitoring Provider
- Access Credentials Provider
- IP Discovery Provider
- Telemetry Provider
- Ethernet Connectivity (LLDP) Discovery Provider
- IB Provider
- Solution Provider
- Virtualization Provider
- Host Manager Provider
- Performance Provider

Communication Protocols

Mellanox NEO utilizes the following communication protocols.

Protocol	Purpose
HTTPS	Collecting chassis data regarding Mellanox devices and Windows servers
SNMP	Collecting connectivity data, monitoring data and general data from switches
SSH	Switch/Linux provisioning

Installation and Initial Configuration

Installation Requirements

Prior to the installation process, make sure:

- A supported version of Linux is installed on your machine as listed below
- To have HTTPS/HTTP access from your client machine (on which a browser is running) to the machine that you intend to run NVIDIA® Mellanox® NEO® on

  > ⚠ The default access protocol is HTTPS.

- The ports listed below are not being used by another application running on the same machine/VM as Mellanox NEO

System Requirements

Mellanox NEO Server Requirements

Please refer to "Mellanox NEO Server Requirements" in the Release Notes page.

Ports Mellanox NEO Application Uses

Ports	Protocol	Description
Listening		
2022	TCP	SSH protocol (relevant for HA mode only)
2224	TCP	Pacemaker PCS service (relevant for HA mode only)
8086	TCP	InfluxDB (relevant for HA mode only)
8088	TCP	InfluxDB
8094	TCP	Telegraf
7658	TCP	Mellanox NEO GRPC collector used for collection of buffer threshold events
7654	TCP	Used to communicate between NEO telemetry agent and Mellanox NEO
162	UDP	SNMP traps receiver
Transmitting		
22	SSH	Access managed devices
443	HTTPS	Access managed devices
80	HTTP	Access managed devices
161	SNMP	Access managed devices

Mellanox NEO GUI Client Requirements

Please refer to "Mellanox NEO GUI Client Requirements" in the Release Notes page.

Recommended Screen Resolutions

Please refer to "Recommended Screen Resolutions" in the Release Notes page.

Supported Mellanox Internally Managed Systems

Please refer to "Supported Mellanox Internally Managed Systems" in the Release Notes page.

Supported Platforms and Operating Systems

Please refer to "Supported Platforms and Operating Systems" in the Release Notes page.

Managed Hosts Supported by Mellanox NEO

Please refer to "Managed Hosts Supported by Mellanox NEO" in the Release Notes page.

Downloading Mellanox NEO

Using MyMellanox Account

> ⚠ If you do not have an active support contract, skip these steps, and follow the next procedure instead.

To download Mellanox NEO software:

1. Log into MyMellanox.
2. Go to Software → Management Software → Mellanox NEO.
3. Click the “Downloads” tab and click the software image.
4. Click “Download”.

From the Mellanox Website

> ⚠ If you have a valid support contract, follow the previous procedure instead.

1. Go to the Mellanox NEO product page on the Mellanox website.
2. Click the "Download Software" button.

3. Fill the short form and click "Submit".
4. A direct link to the image download is sent to the email address you provided in the form.

Installing Mellanox NEO

The default Mellanox NEO installation directory is /opt/neo.

To install Mellanox NEO software:

1. Copy the Mellanox NEO installation package to a local temporary directory (e.g. /tmp).
2. Enter the temporary directory.

```
cd /tmp
```

3. Delete the previous installation folder (if any exist).

```
rm -rf /tmp/neo
```

4. Extract the Mellanox NEO installation package.

```
tar zxvf neo-2.7.0-5.el7.tar.gz
```

5. Enter the new created directory.

```
cd neo
```

6. Install Mellanox NEO.

```
./neo-installer.sh
```

7. If a previous Mellanox NEO installation is detected, you will be asked to confirm proceeding with the upgrade procedure. Type “y” to proceed. See Upgrading Mellanox NEO below for more information.

```
[root@neo tmp]# ./neo/neo-installer.sh
Mellanox NEO Software Installation
=====================================================
=====================================================
pip is already installed!

Mellanox NEO SYSTEM PREREQUISITE TESTS

Checking Server architecture ...                                    [  OK  ]
Checking Installed distribution ...                                 [  OK  ]
Checking OS Version ...                                             [  OK  ]
Checking Installer Dependencies ...                                 [  OK  ]
Checking Python version (2.7) ...                                   [  OK  ]
Checking Checking Localhost resolving ...                           [  OK  ]
Checking Hostname resolving ...                                     [  OK  ]
Checking SELinux disabled ...                                       [  OK  ]
Checking basic packages installation ...                            [  OK  ]
Checking Plugin ...                                                 [  OK  ]

NEO Access Credentials Provider 2.7.0-5.el7 PREREQUISITE TESTS
```

8. [Optional] In order to use more provisioning templates of Mellanox NEO supported system types (Linux hosts, Windows hosts, Arista switches and Cisco switches), you may download and install Mellanox NEO external RPMs. For further details on how to download and install Mellanox NEO external RPMs, please refer to the community post "HowTo Install NEO Plugins".

> ⚠ You can download and install the external RPMs also after Mellanox NEO is up and running.

9. [Optional] Run Mellanox NEO manually after the installation is complete.

```
/opt/neo/neoservice start
```

> ⚠ During the installation process, a warning message will display when NTP is not configured. To resolve that, please install NTP and run the ntpd process.

Installing NEO for High Availability

Mellanox NEO High Availability (HA) deployment is composed of a three-node cluster (based on CentOS 7.x) installed with Mellanox NEO software. The HA mechanism for NEO is based on two standard Linux mechanisms:

- Pacemaker cluster resource manager – responsible for detection and recovery of machine and application-level failures
- Rsync – responsible for synchronizing all file systems between the three cluster nodes

Prerequisites

- CentOS v7.x installed on your machine, where HA is exclusively supported
- Configure SSH trust between the three nodes. Run the following on each of the three nodes:

```
ssh-keygen
ssh-copy-id -i /root/.ssh/id_rsa user@server
```

- In order to install Mellanox NEO as a docker container, SSH trust can be established by using the script "create_ha_trust_on_docker.sh" with the IP addresses of all the nodes as parameters. For example:

```
/opt/neo/common/utils/create_ha_trust_on_docker.sh 10.212.220.7 10.212.220.13 10.212.220.6
```

  - The script opens port 2022 for SSH on all cluster nodes which is used for file synchronization
  - For the script to run successfully, the names of the containers must be identical on all nodes
- Configure /etc/hosts and add all 3 server IPs and hostnames for each of the three nodes. For example:

```
# cat /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
10.250.24.4 neo-server-1
10.250.24.3 neo-server-2
10.250.24.2 neo-server-3
```

Installing Mellanox NEO Cluster

Install NEO separately on each node. For further information, refer to Installing Mellanox NEO section above.

Configuring Mellanox NEO Cluster

> ⚠ The following steps are performed on one node only, but will automatically apply to the other two nodes once the cluster is started.

Choose one node and update the parameters in its yaml file, located at: /opt/neo/common/conf/ha.yaml:

1. [Optional] Hacluster_password – this parameter is set by default to use a pre-configured password. To change the password, please contact Mellanox Support.
2. [Optional] ha_file_sync – the periodic time for syncing the persistent data. Default value is 300 seconds. Minimum value is 100 seconds.
3. ha_nodes – the IP addresses of the three nodes on which NEO is installed, in addition to their priority:
    - local_ip – the IP of the node that is part of the HA cluster
    - priority – either 1, 2 or 3 according to their mode (active/stand-by). Node priority is only considered upon the first NEO startup.
4. virtualIP – the virtual IP address for the GUI. This IP is the gateway for all nodes.
5. rsync_user – the username used to authenticate all three nodes of the HA

The following is an example of an ha.yaml file:

```
Hacluster_password:
rsync_user: root
ha_file_sync:
ha_nodes:
- local_ip: 10.250.24.2
  priority: 1
- local_ip: 10.250.24.3
  priority: 2
- local_ip: 10.250.24.4
  priority: 3
virtual_ip: 10.250.24.10
ssh_port: 22
```

Once configuration is completed successfully, make sure to start NEO and check its status as described in the section below.

Operating Mellanox NEO Cluster

Mellanox NEO user can start, stop, or restart Mellanox NEO cluster, or check its status at any time.

- To start Mellanox NEO cluster, run:

```
/opt/neo/neocluster start
```

- To check Mellanox NEO cluster status, run:

```
/opt/neo/neocluster status
```

- To stop Mellanox NEO cluster, run:

```
/opt/neo/neocluster stop
```

- To restart Mellanox NEO cluster, run:

```
/opt/neo/neocluster restart
```

- To return to the standalone mode from the HA mode, stop neocluster and then starting neoservice.

Connecting NEO Web UI to Mellanox NEO Cluster

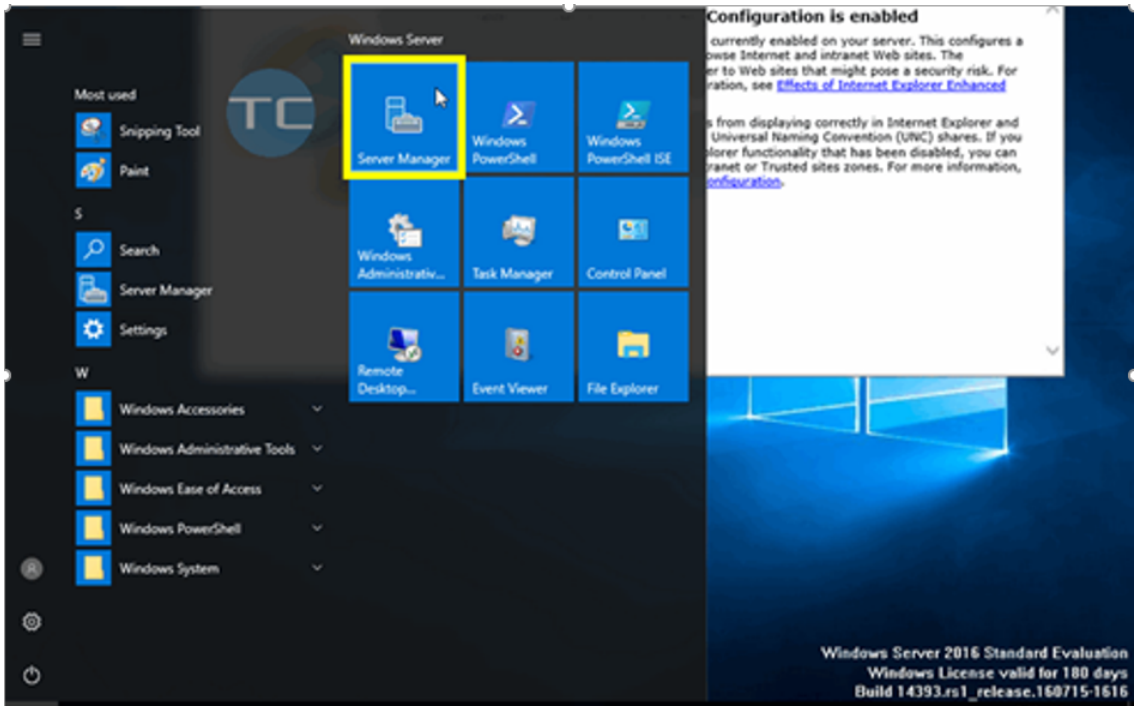
When connecting NEO Web UI to Mellanox NEO HA cluster, make sure to connect via the virtual IP address of the cluster.

Deploying NEO Virtual Appliances

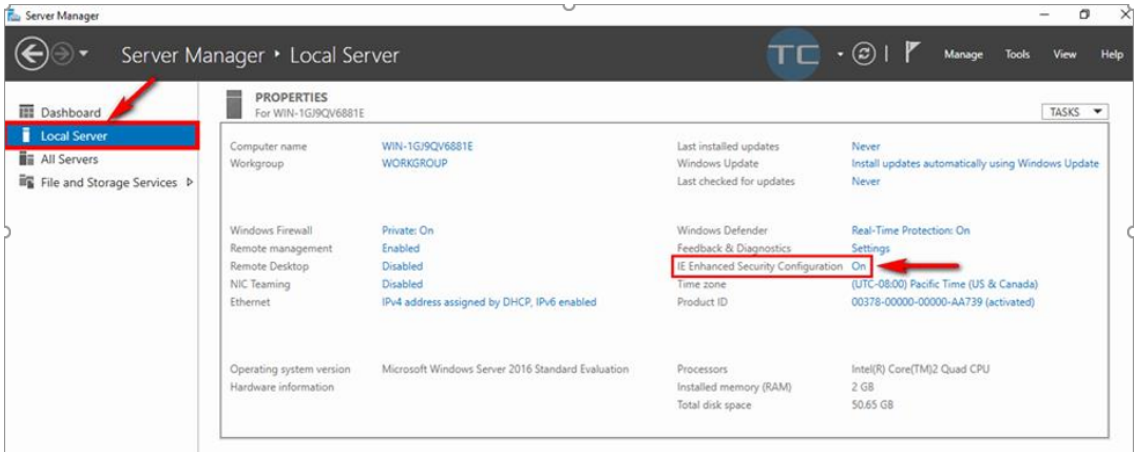
> When working with NEO over VM, the VM name will be "neo-server-NEO-<version>-${mac-suffix}".
>
> In order to override this name, comment, or remove, the line `hostnamectl set-hostname "neo-server-NEO-2.6.0-9-${mac-suffix}"` from the file /usr/sbin/ifup-local.

Mellanox NEO supports several virtual appliances for selected hypervisors for easier deployment. Before deploying the NEO virtual machine (VM) on Windows 2016, make sure to disable the following security settings so you can access the UI from the host machine:

1. Click the Start button and launch the "Server Manager":



2. Click "Local Server".
3. In the "Properties" window, make sure the "IE Enhanced Security Configuration" is set to “On”.



4. Turn off the "IE ESC for Administrators and/or for Users", and click OK:

5. Restart the browser, and attempt logging-in.

Deploying NEO Virtual Appliance on Linux KVM

1. Go to the VM host (hypervisor) storage directory:

```
cd /images
```

2. Copy your release image to the VM host:

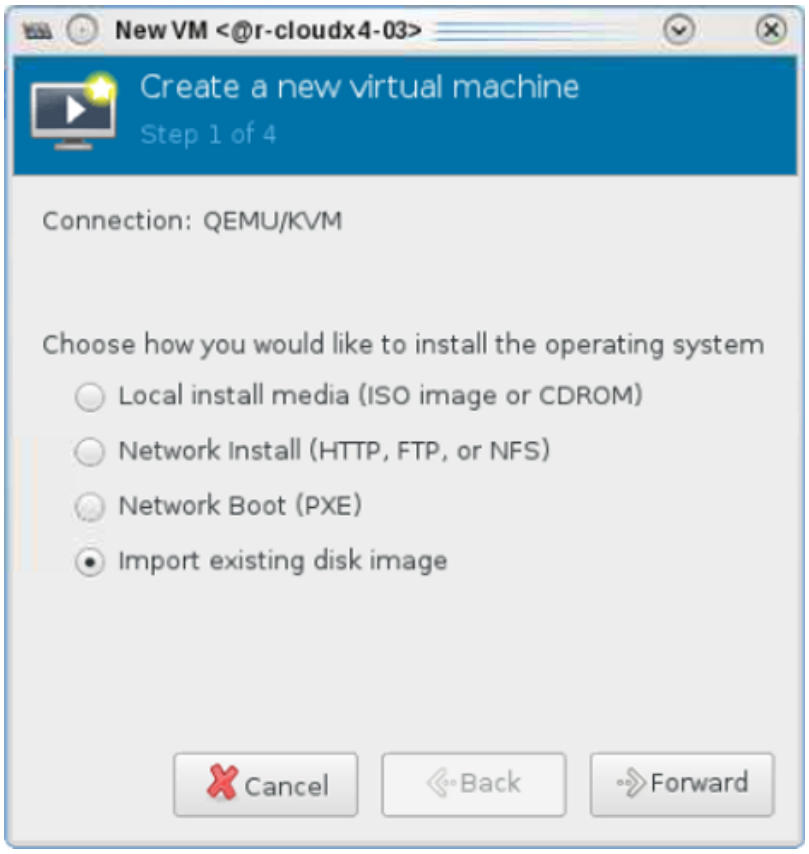
```
cp /release/vm/neo-1.4.9-10.qcow2
```

3. Run:

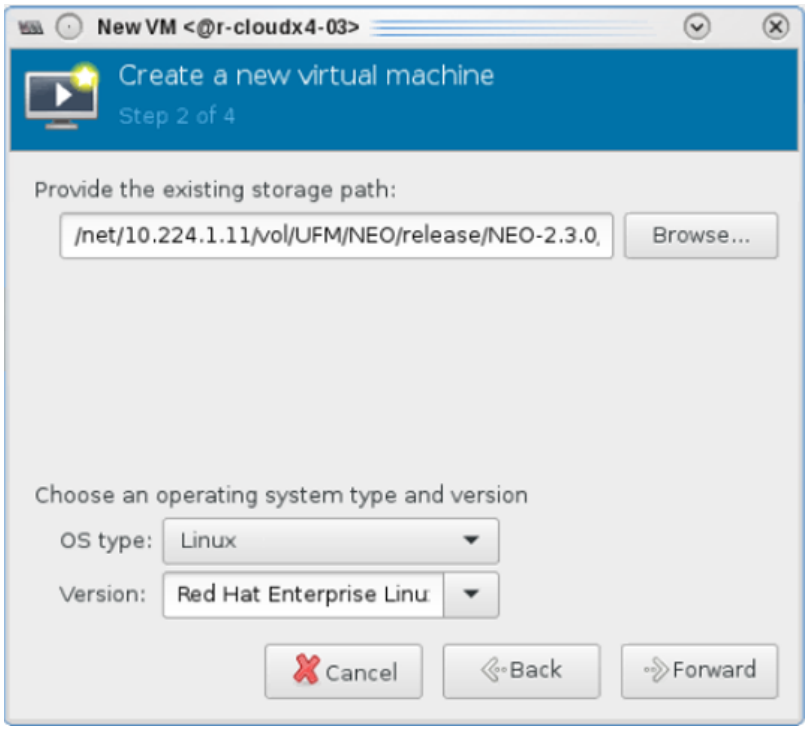
```
virt-manager &
```

4. Create a new VM:

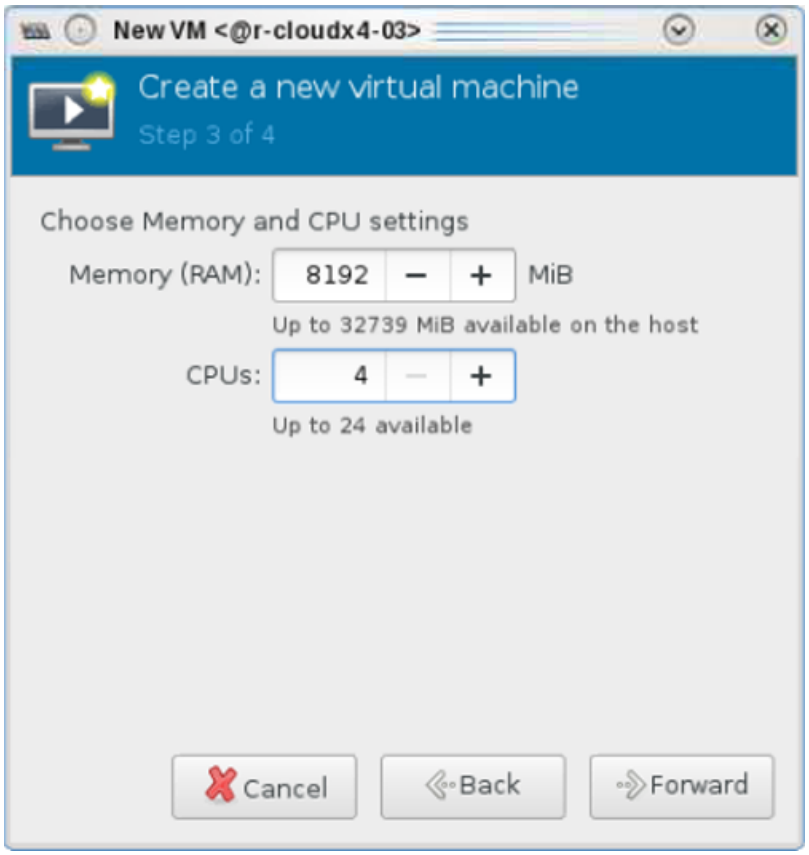
a. Choose to "Import existing disk image" for installing the OS:



b. Provide the storage path, and as OS select Linux Red Hat 7.3 or above:

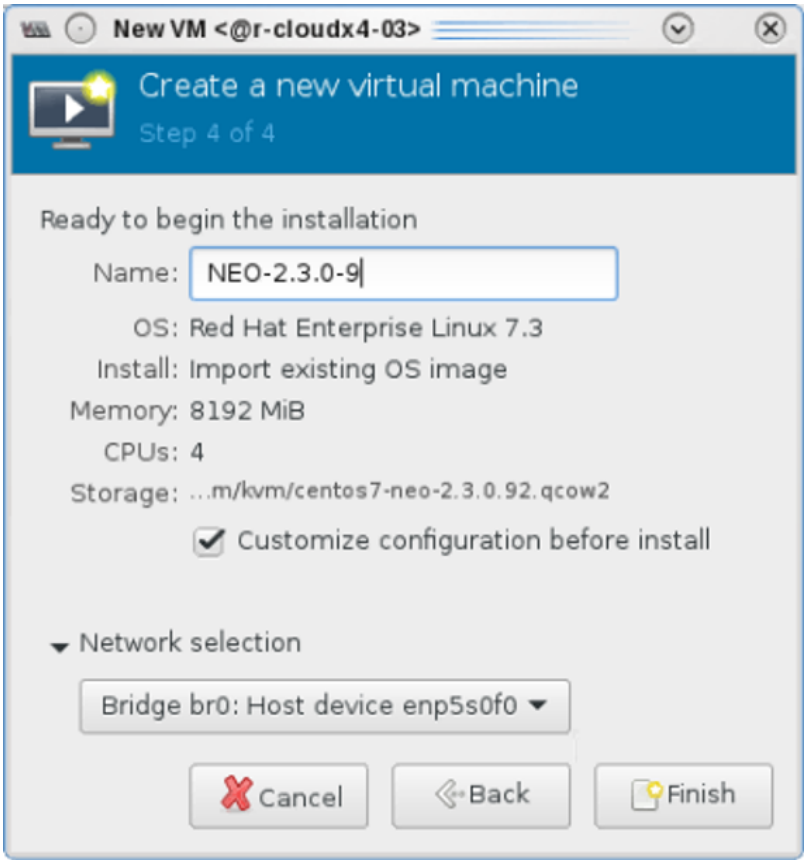


c. Specify the memory usage and the number of CPUs:

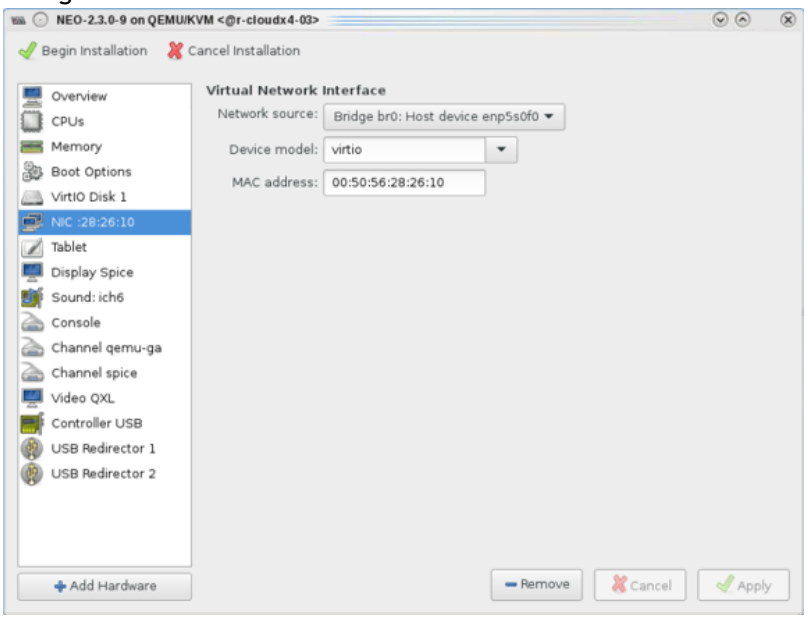


> ⚠ As the memory usage and the number of CPUs get higher, the performance improves. Memory usage should at least be 8192 MB.

d. Enter a name for the VM. If you wish to configure the NIC card, select "Customize configuration before install":



e. If you wish to set a fixed MAC address, do so in the NIC section of the VM configuration:



Once the new VM is successfully complete, the following screen with the hostname and

login username will appear:

5. Log into the VM and using the following credentials:
    - Username – root
    - Password – 123456
6. Stop the NEO service. Run:

```
cd /opt/neo
./neoservice stop
```

7. Verify the date and timezone are configured properly:

```
date
```

   If you need to update the timezone, follow the steps below:
    a. Delete the current “localtime” file under /etc/ directory.

```
cd /etc
```

    b. Remove the local time.

```
rm localtime
```

    c. Select a time zone.

```
ln -s /usr/share/zoneinfo/US/Pacific localtime
```

8. Check the hostname resolution. Run:

```
hostname -i
```

9. Make sure you received your local IP.
10. Start NEO. Run:

```
cd /opt/neo
./neoservice start
```

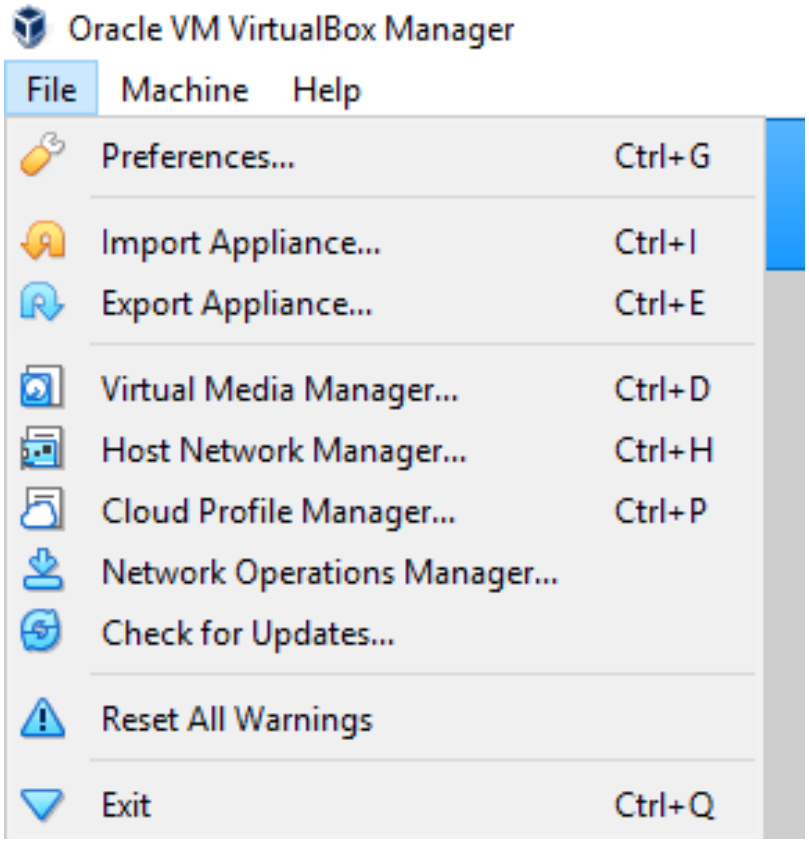
11. Make sure you can access the VM through your browser.

Deploying NEO Virtual Appliance on VirtualBox

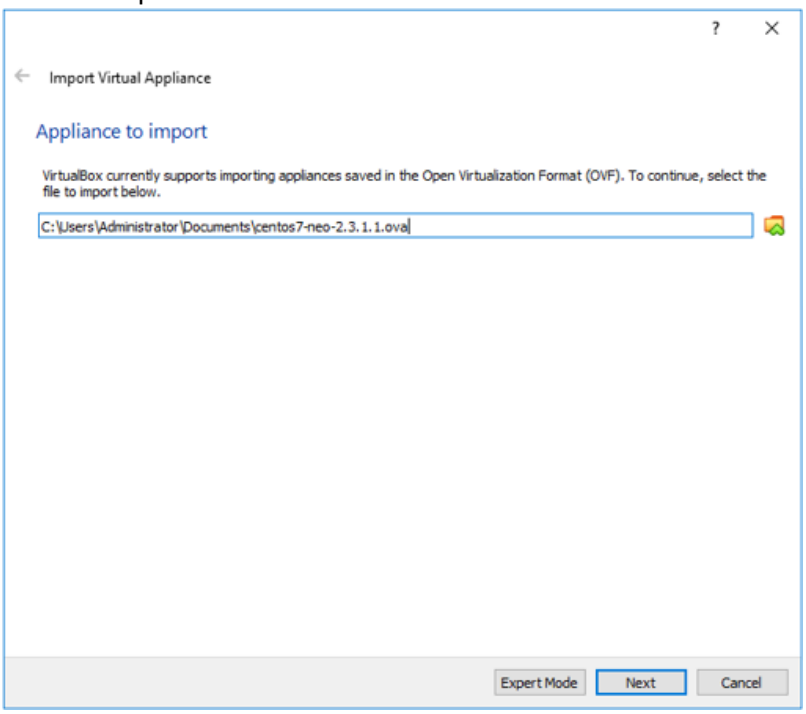
> ⚠ NEO VM uses 64-bit architecture. If you have a 32-bit OS, virtualization might not be enabled on your machine, and an error message of unavailable hardware acceleration will appear. In this case, make sure to enable virtualization through BIOS.

In order to enable virtualization through BIOS, follow the steps below:

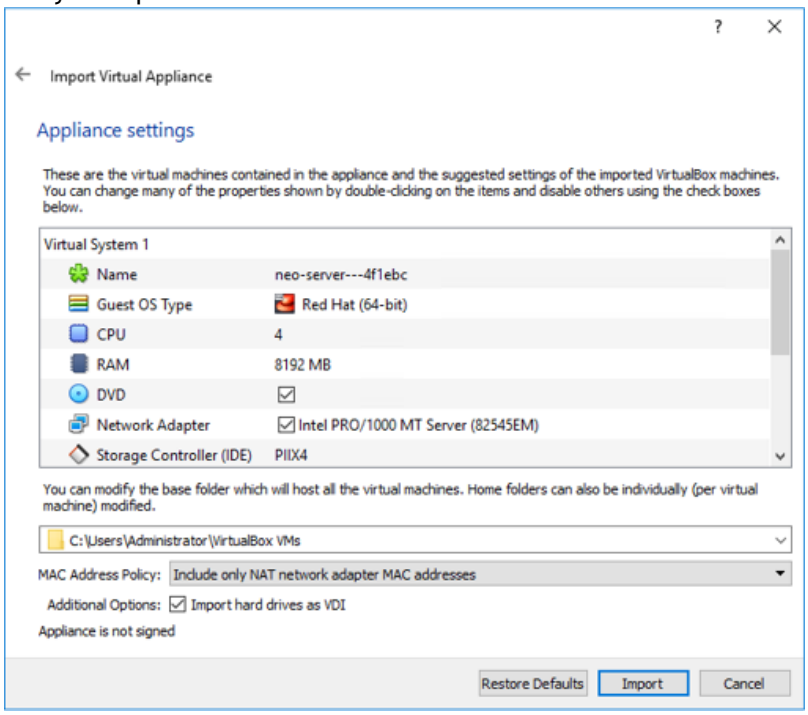
1. Click "File" and choose "Import Appliance".



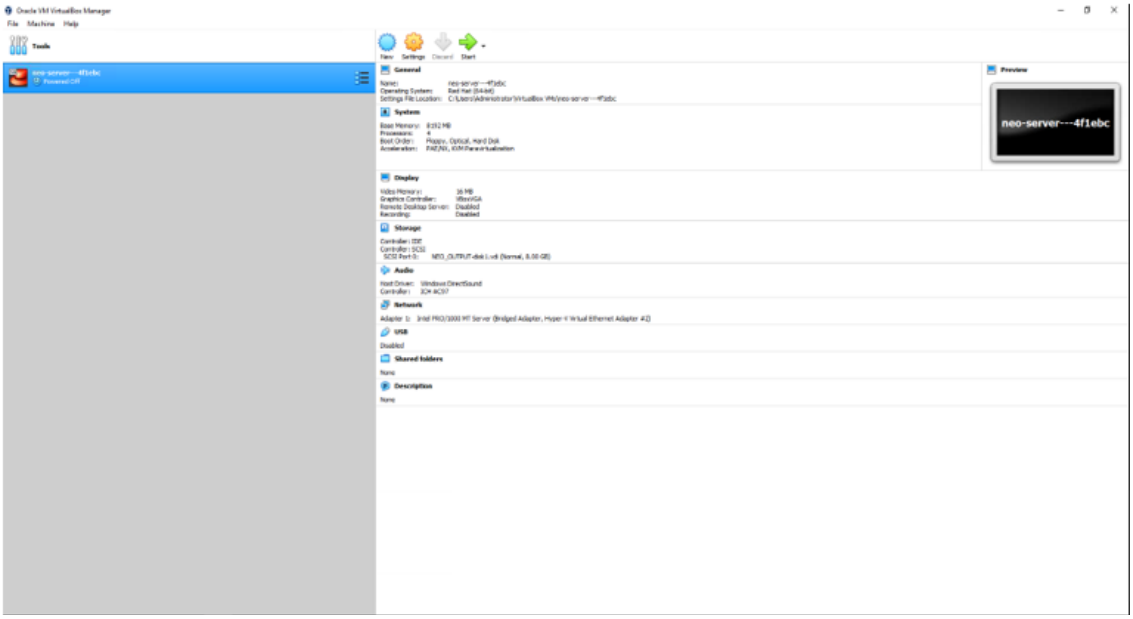
2. Choose the path for the ova file in the VM files and click Next.



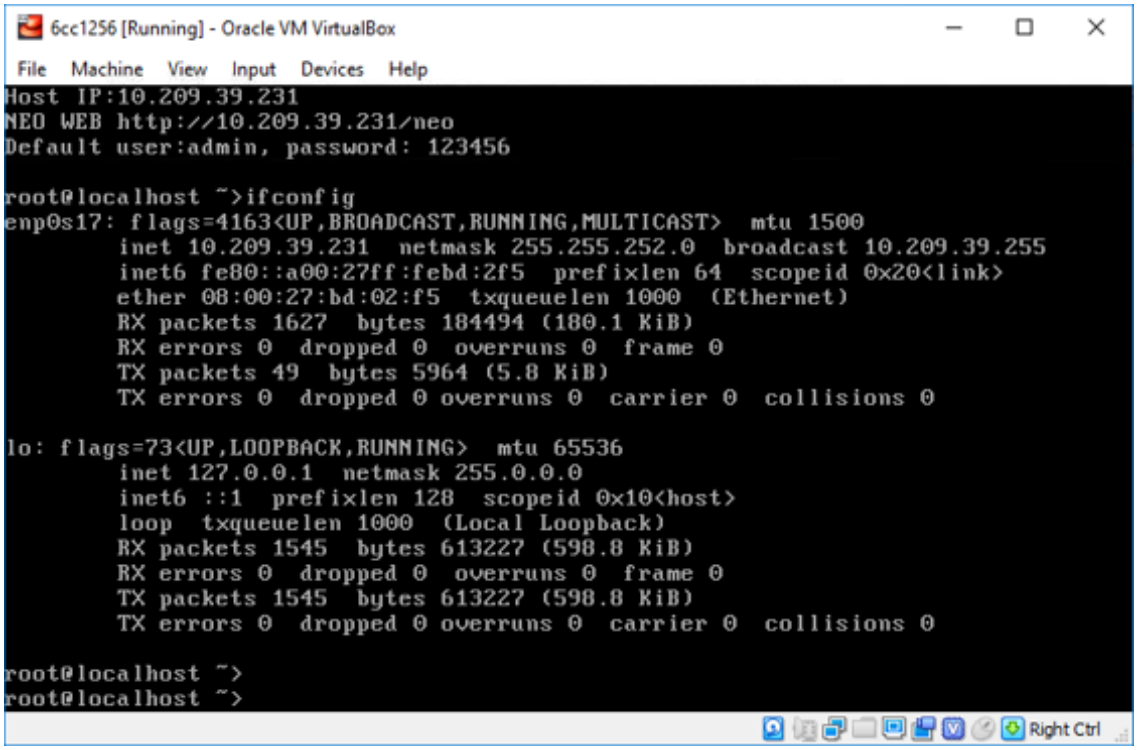
3. Click "Import" to import the VM into VirtualBox. After this step, the VM will be imported and ready to explore NEO on it.



4. Choose “vm” and click start to run it.



5. Once the VM starts, log in using the following credentials:
    - Username – root
    - Password – 123456
6. Run ifconfig to display the interfaces. As can be seen below, eth0 has already acquired an IP on the network:

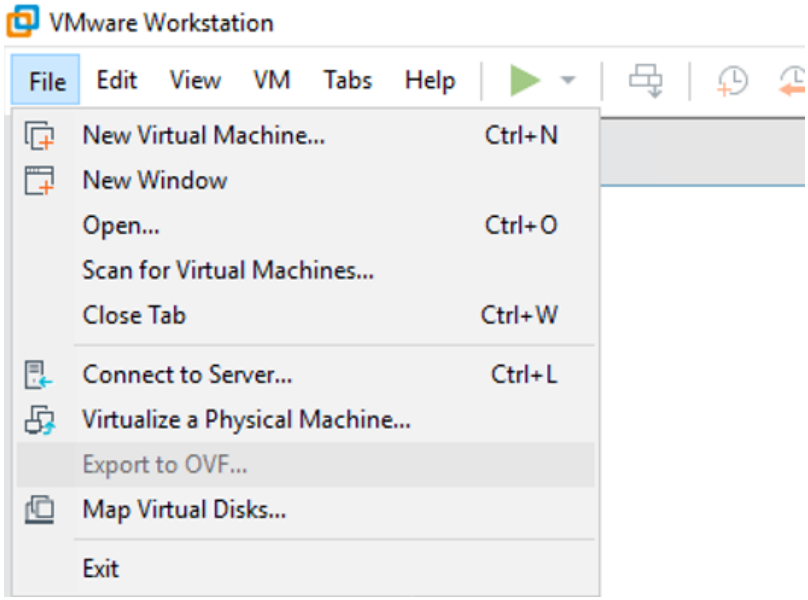


> ⚠ The MAC address assigned to the VM must be on DHCP records in order to get an IP address from the VM.

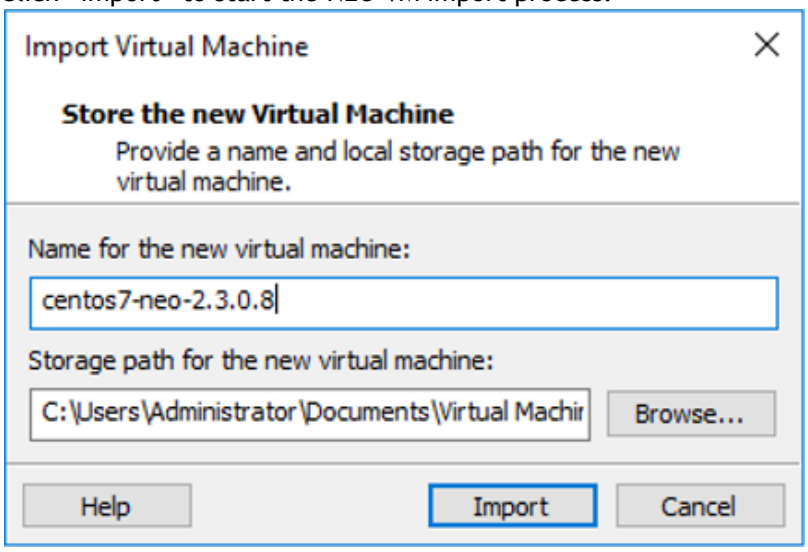
7. Log into NEO GUI using the IP found in the previous step (http://<NEO_server_IP>/neo) with the following credentials:
    - Username – admin
    - Password – 123456

Deploying NEO Virtual Appliance on VMware Workstation

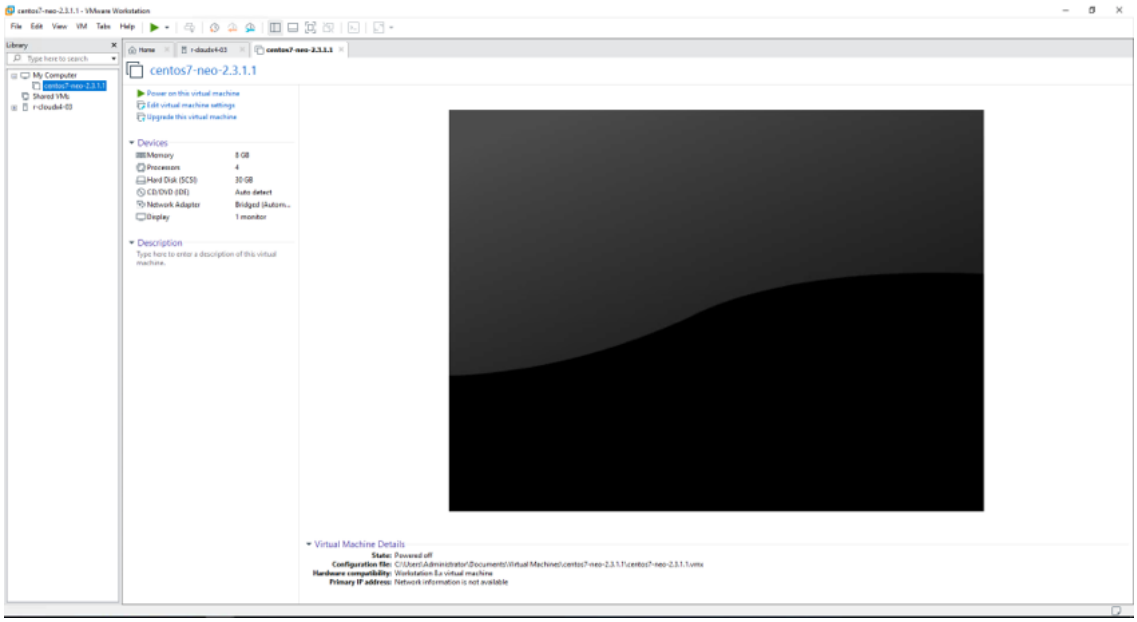
1. Click “File” → “Open” and open the ovf template.



2. Click “import” to start the NEO VM import process.



The VM can then be seen imported:



3. Click “Power on this virtual machine” to start the VM. Use the following credentials:
    - Username – root
    - Password – 123456
4. Run ifconfig to display the interfaces. As can be seen below – eth0 already acquired an IP.

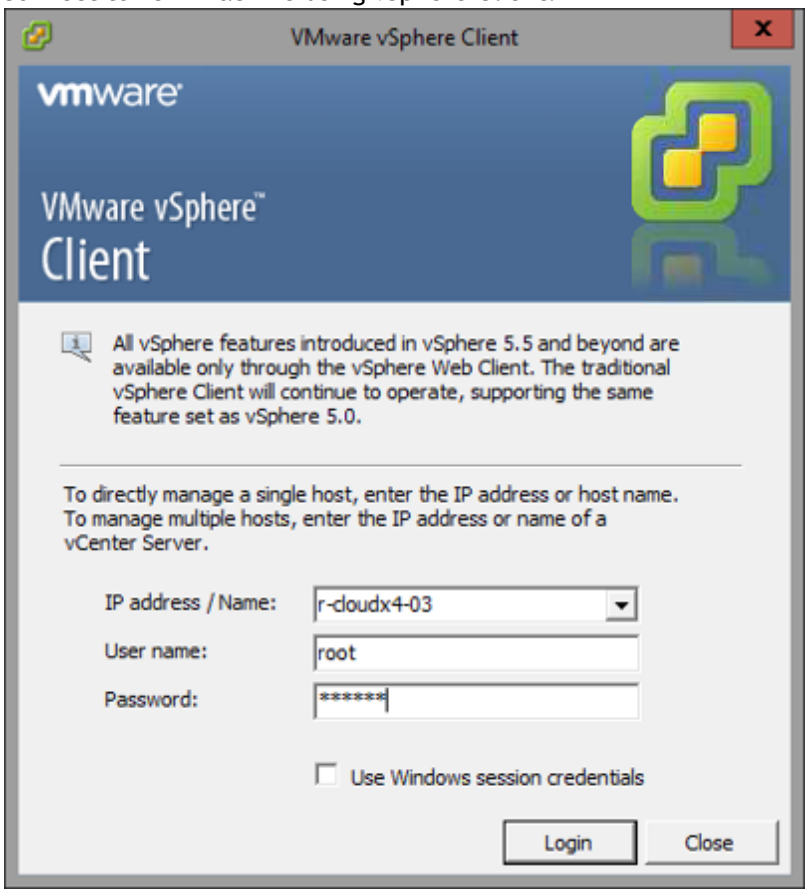
> ⚠ The MAC address that is assigned to VM must be on DHCP records in order to get an IP address from the VM.

5. Log into NEO GUI using the IP found in the previous step (http://<NEO_server_IP>/neo) with the following credentials:
    - Username – admin
    - Password – 123456

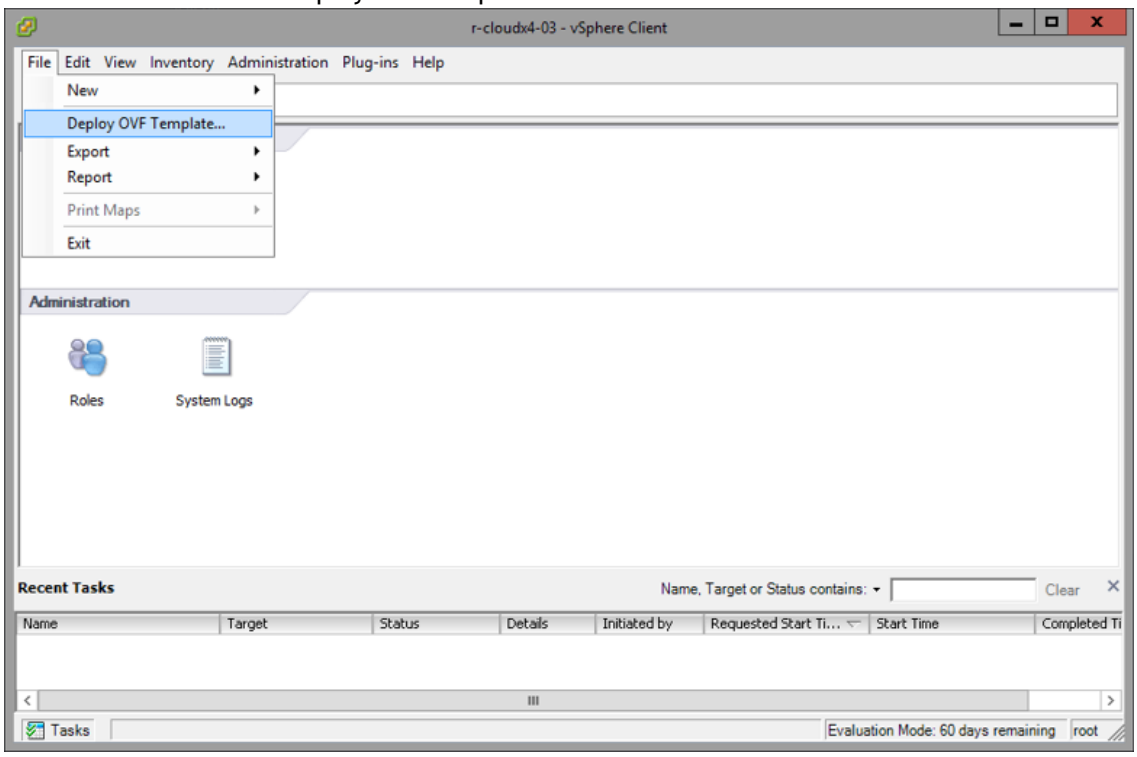
> ⚠ If the VM does not succeed at gaining an IP, check the "Automatic Settings" under "Edit" → "Virtual Network Editor". Make sure to untick the checkbox of VirtualBox which is installed on your machine, and then reboot the VM so it can acquire an IP.

Deploying NEO Virtual Appliance on VMware ESXi Server

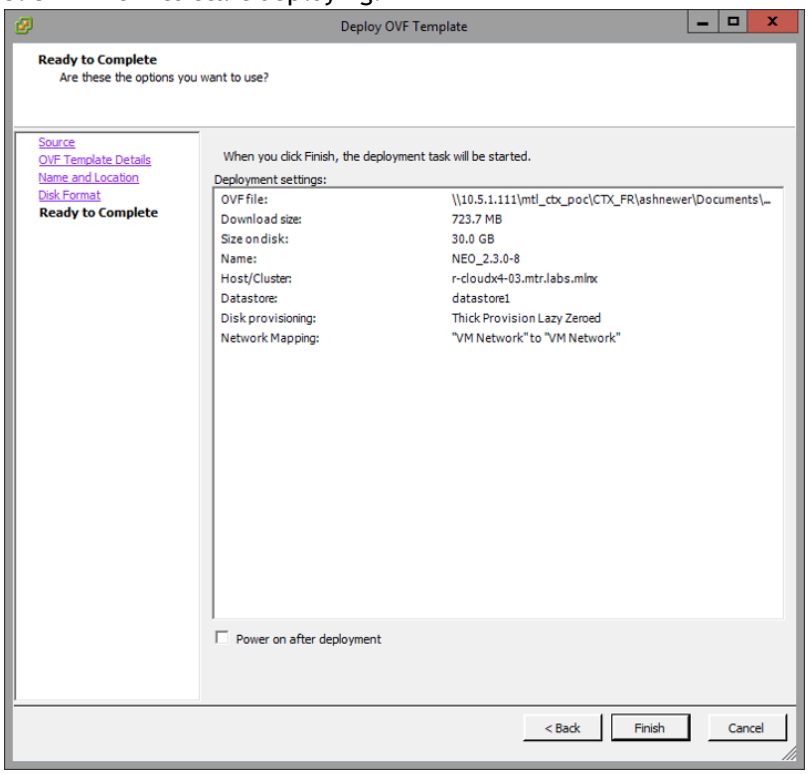
1. Connect to ESXi machine using vSphere Client.



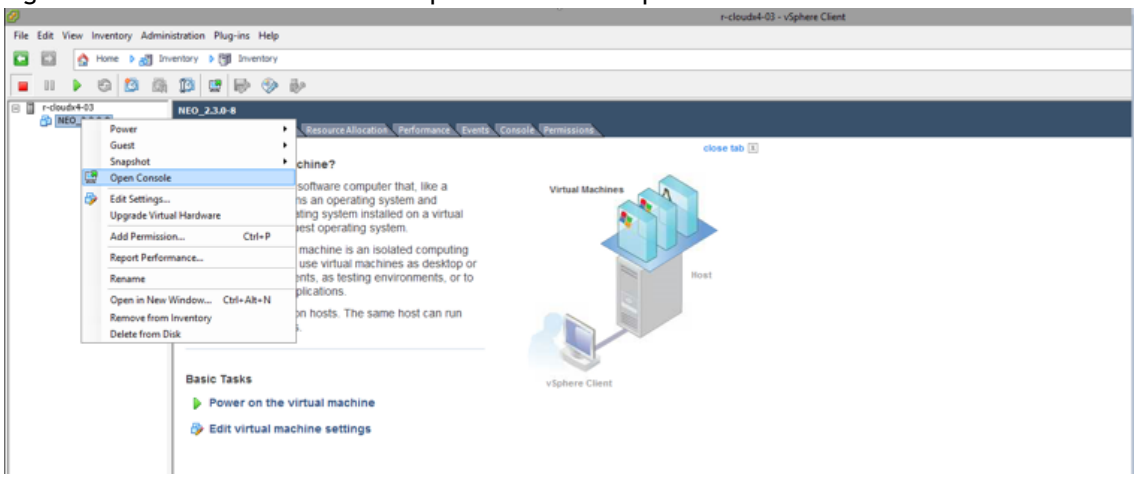
2. Click "File" and choose "Deploy OVF Template…".



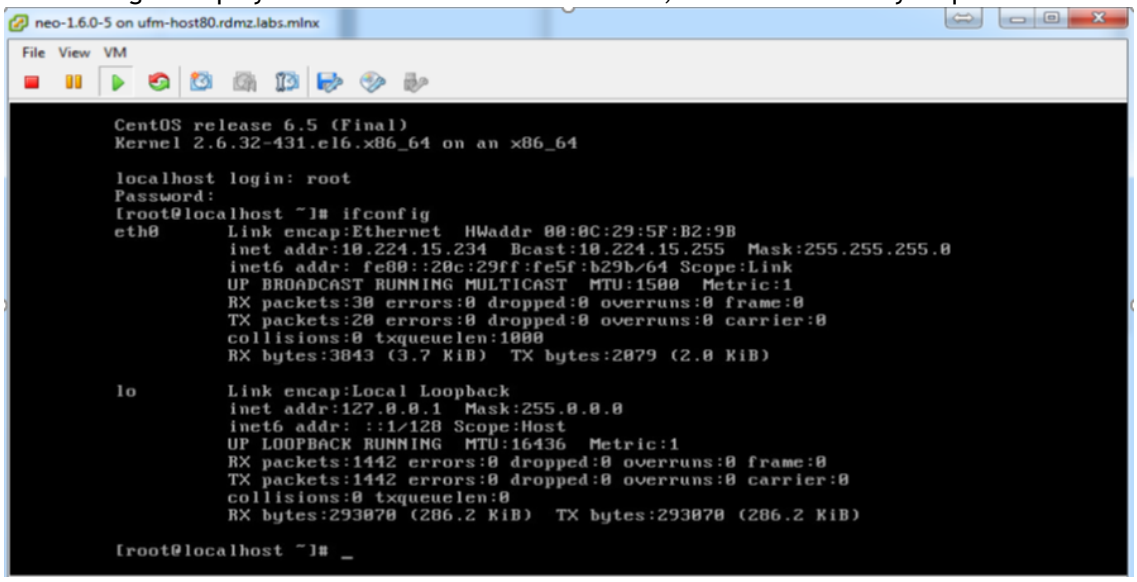
3. Choose the path for the OVF template and go through the pages by clicking "Next".
4. Click "Finish" to start deploying.



5. Right-click on the VM and choose "Open Console" and power on the machine.



6. Use the following credentials to log into the machine:
   - Username – root
   - Password – 123456
7. Run ifconfig to display interfaces. As can be seen below, the VM has already acquired an IP.



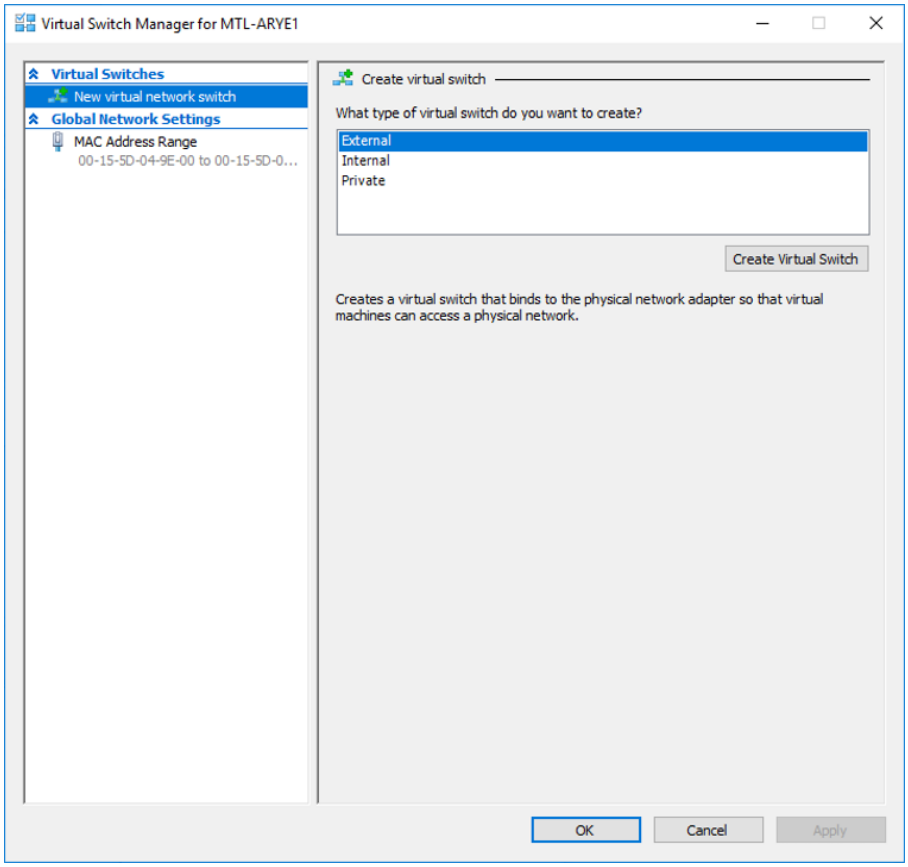
> ⚠ The MAC address assigned to the VM must be on DHCP records in order to get an IP address from the VM.

8. Log into NEO GUI using the IP found in the previous step (http://<NEO_server_IP>/neo) with the following credentials:
   - Username – admin
   - Password – 123456

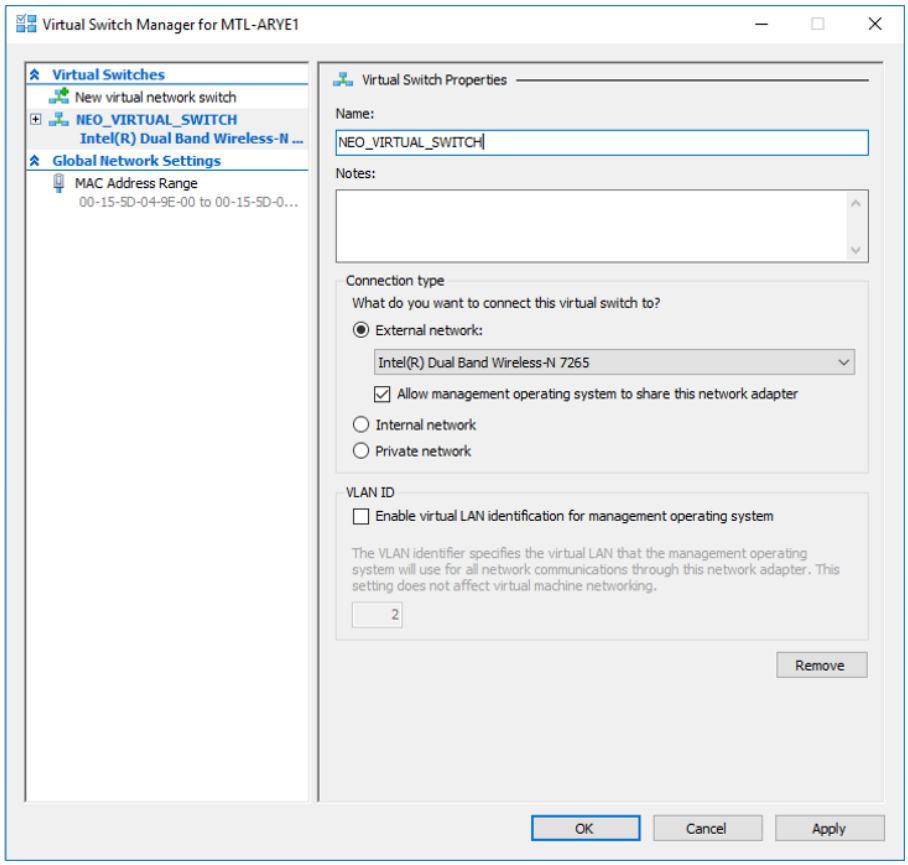
Installing NEO Virtual Appliance on Hyper-V

1. Launch the Hyper-V.
2. Click "Action" → "Virtual Switch Manager".

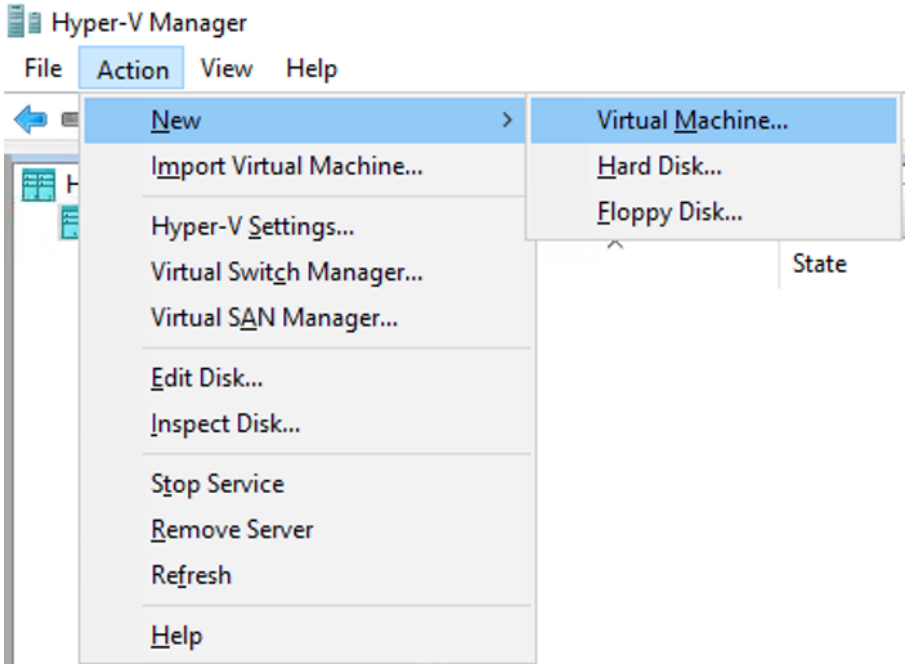
3. Create a new external virtual switch:



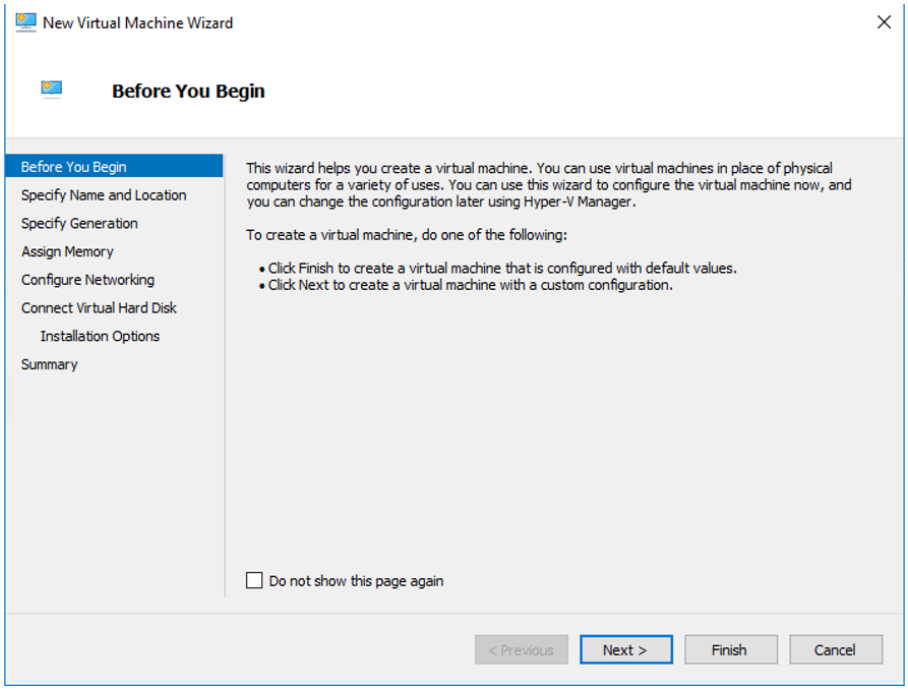
4. Provide a name and make sure you choose the right network adapter connected to the management network:



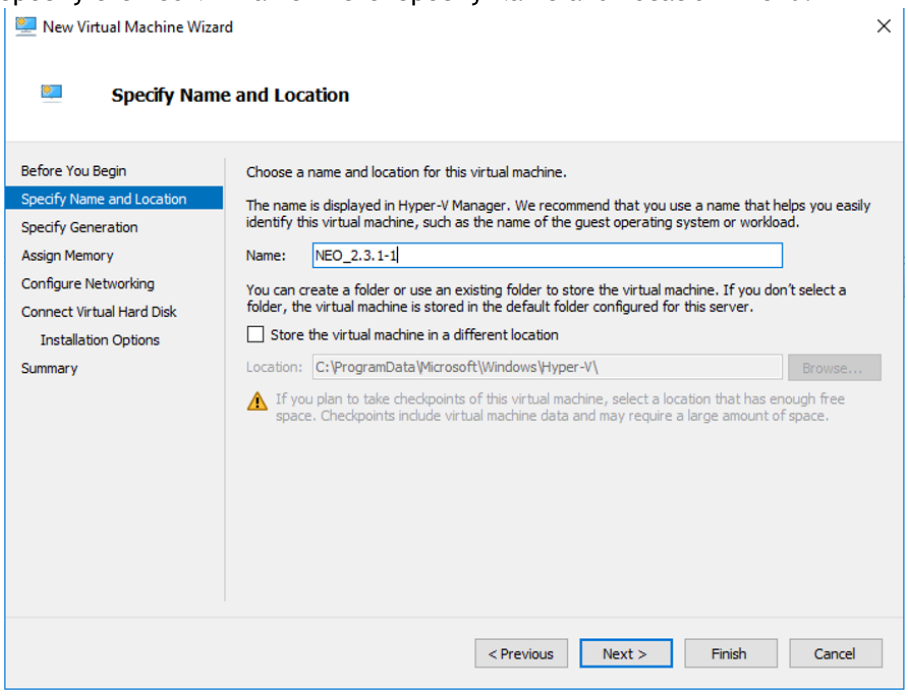
5. Click "Action" → "New" → "Virtual Machine".



6. Click "Next" in the New Virtual Machine Wizard window.

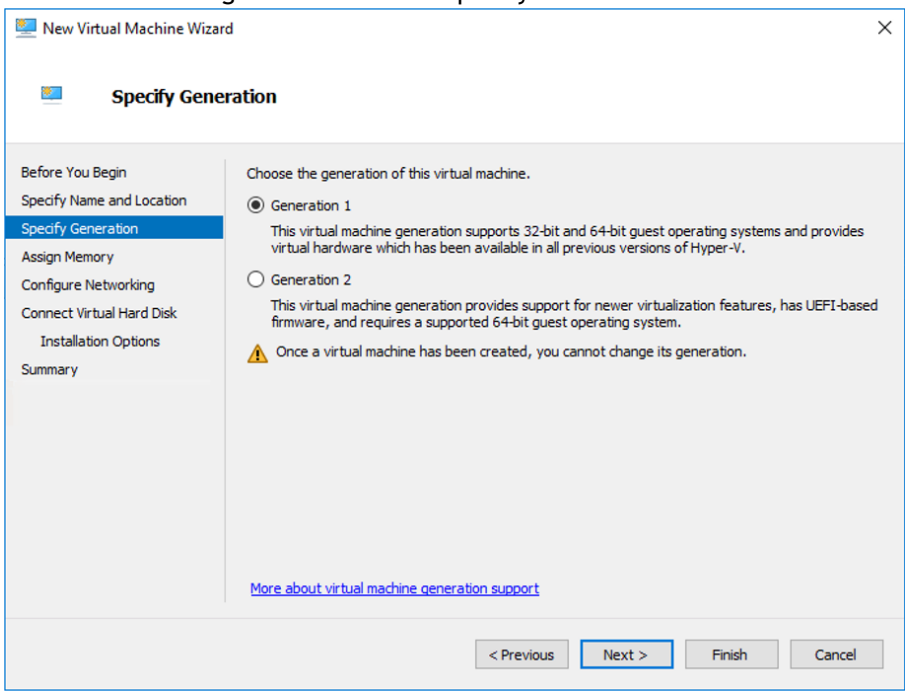


7. Specify the neo-vm name in the "Specify Name and Location" menu.

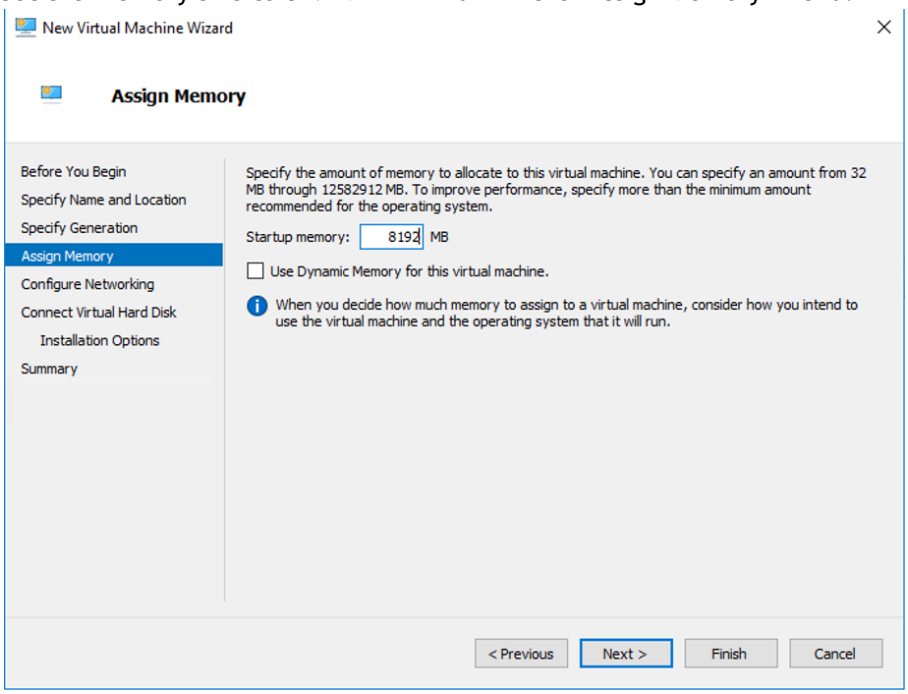


8. Click "Next".

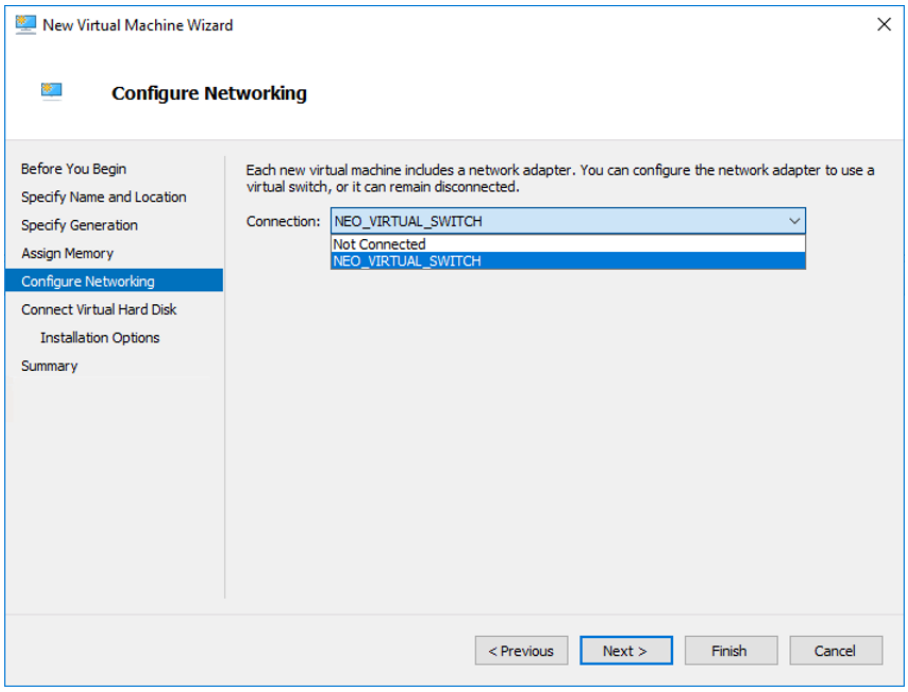
9. Chose the desired generation in the "Specify Generation".



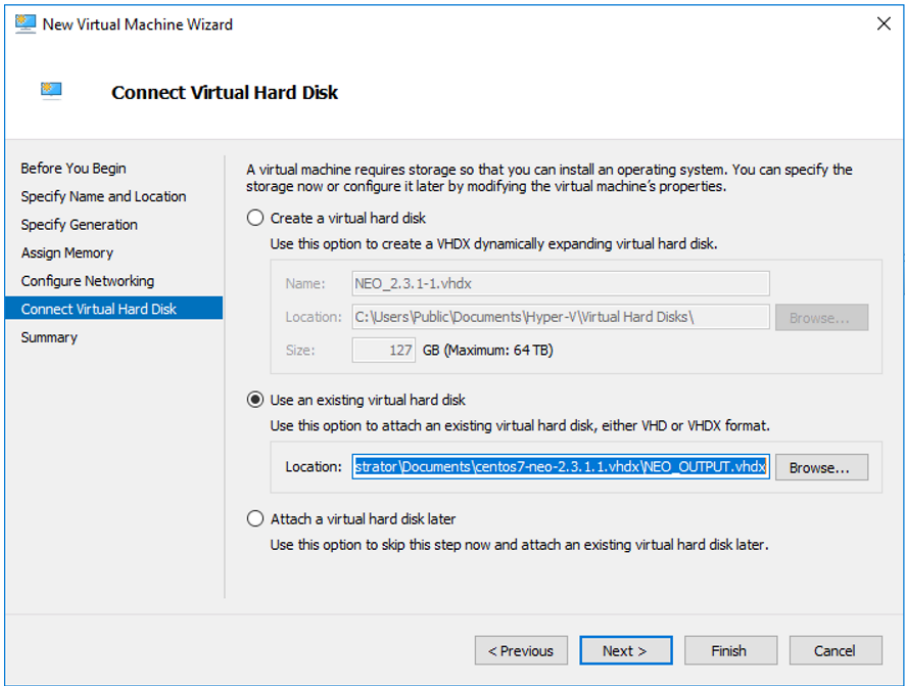
10. Click "Next".
11. Set the memory size to 8192MB minimum in the "Assign Memory" menu.

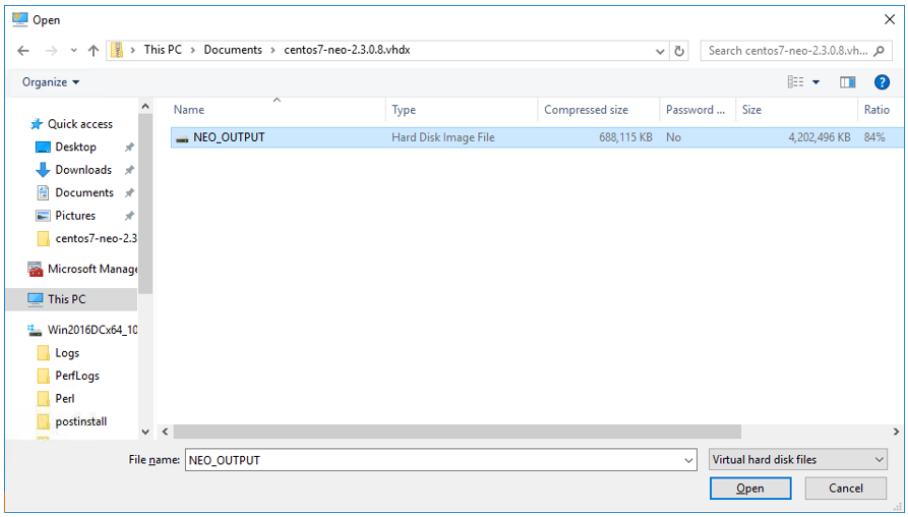


12. Click "Next".
13. Use the virtual switch that appears in the "Connection" drop down menu in the "Configure Network" menu.

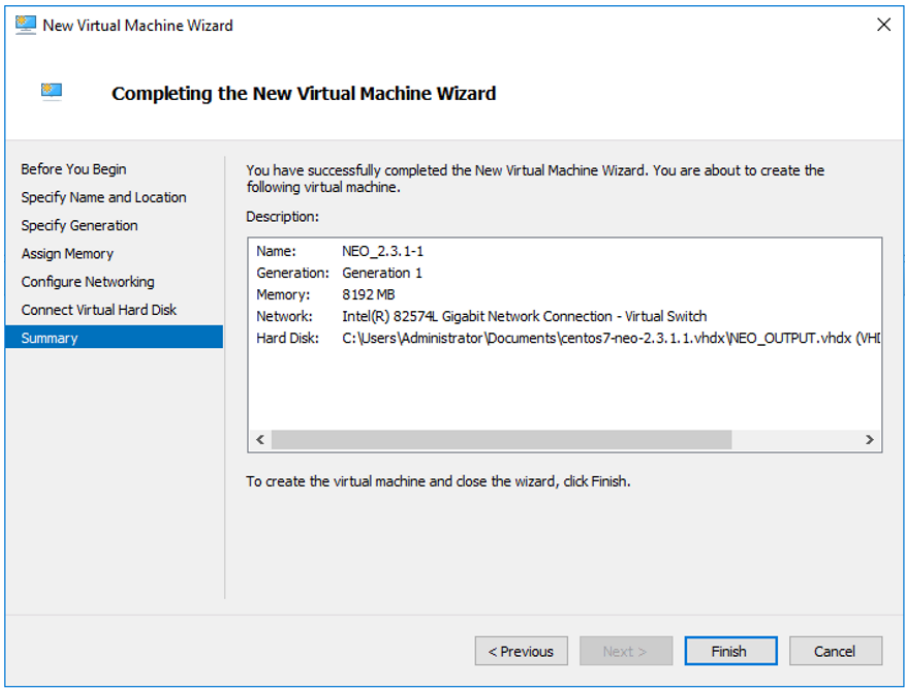


14. Click "Next".
15. Choose "Use an existing virtual hard disk" and browse to the neo-v vhd file in the "Connect Virtual Hard Disk" menu.

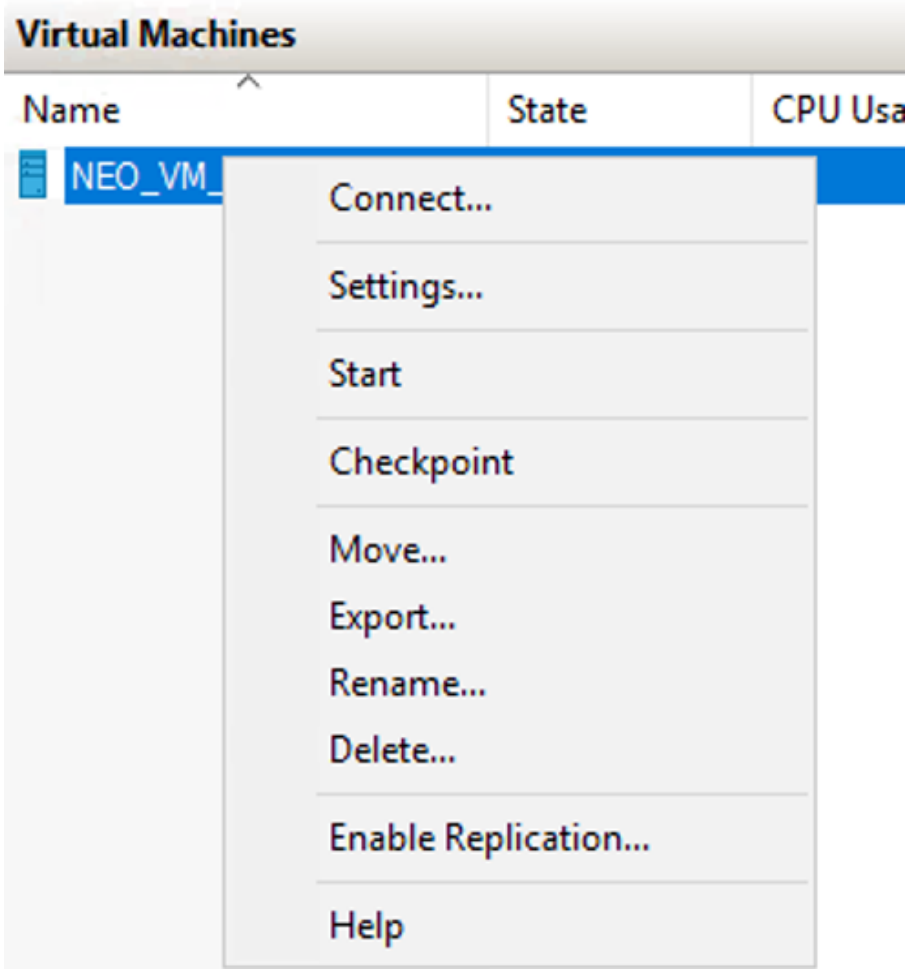




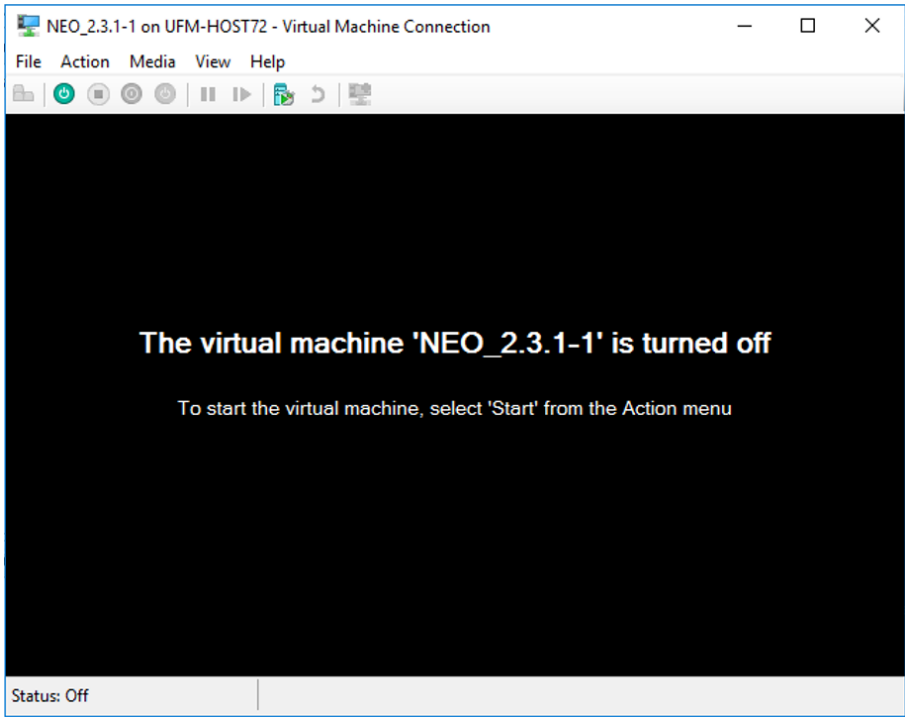
16. Click "Next".
17. Click "Finish" in the "Summary" menu when displayed.



18. Right click and choose Connect once you see the neo-vm on your Hyper-V



19. Select "Start" from the "Action" menu to start the VM.



20. Use the following credentials to log in to your VM:
    - Username – root
    - Password – 123456

Installing Mellanox NEO as Docker Container

1. Install Docker CE on CentOS 7.X:

```
yum install -y yum-utils device-mapper-persistent-data lvm2
yum-config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo
yum-config-manager --enable docker-ce-edge
yum-config-manager --enable docker-ce-testing
yum makecache fast
yum -y install --setopt=obsoletes=0 docker-ce-17.03.2.ce-1.el7.centos.x86_64 docker-ce-
selinux-17.03.2.ce-1.el7.centos.noarch
```

> ⚠ In order to upgrade Mellanox NEO docker, users must configure a location on the host to be shared with the docker. To do that please add the following to the docker run command:
>
> ```
> -v </path/to/shared/folder/on/host>:/neo-data
> ```

2. Run the container:

```
cp <image path> /tmp
Service docker start
gzip -d <image name.tar.gz>
docker load -i /tmp/<image name.tar>
docker images (To get image id)
docker run -dit --network host -v /dev/log:/dev/log --privileged <image id> /usr/sbin/init
```

Alternatively you may pull the image from the docker hub:

```
docker pull mellanox/neo
docker run -dit --name 'neo' --restart unless-stopped --network host -v /dev/log:/dev/log --privileged
mellanox/neo:latest /usr/sbin/init
```

3. The NEO web UI is reachable by default on port 3080 (SSL 3443) (e.g. https://<host_ip>:3443/neo/). To access the web UI without mentioning the port, you may do so by following the steps below.
    a. In the host (not inside the container) create the file etc/httpd/conf.d/neo.conf with the following content:

    ```
    <Location /neo>
    ProxyPass http://127.0.0.1:3080/neo
    ProxyPassReverse http://127.0.0.1:3080/neo
    </Location>
    ```

    b. Run:

    ```
    service httpd restart
    ```

4. Get/find the container ID by running in the host (not inside the container):

    ```
    docker ps
    ```

    ⚠ Make sure NEO is not running on the Linux host machine before starting the NEO on the container.

5. Start NEO on the container:

    ```
    docker exec -it <container id>  /bin/bash
    cd /opt/neo
    ./neoservice start
    ```

    ⚠ If the device was rebooted, the running instance will disappear and a new instance should be run.

Upgrading Mellanox NEO

In order to upgrade the Mellanox NEO software:

1. Stop the Mellanox NEO services.

    ```
    /opt/neo/neoservice stop
    ```

2. Copy the Mellanox NEO installation package to a local temporary directory (for example: /tmp).
3. Enter the temporary directory.

    ```
    cd /tmp
    ```

4. Extract the Mellanox NEO installation package.

> ⚠ If a “neo” directory still exists in the current directory—left over from the previous version you had installed—please make sure to remove it before extracting the new NEO installation package.

```
tar zxvf neo-2.4.0-5.el6.tar.gz
```

5. Enter the new created directory.

```
cd neo
```

6. Install Mellanox NEO.

```
./neo-installer.sh
```

If a previous Mellanox NEO installation is detected, you will be asked to confirm proceeding with the upgrade. Type “y” to proceed.

```
[NEO Server]# ./neo-installer.sh
Mellanox NEO Software Installation
============================================================
============================================================
Previous NEO installation detected.
Are you sure you want to proceed with the upgrade ? [y/n]
```

If there is a conflict between the current installed RPMs and the new RPMs that NEO needs to install, you might be asked to confirm proceeding with the upgrade process twice:

```
Mellanox NEO Software Installation
============================================================
============================================================
Previous NEO installation detected.
Are you sure you want to proceed with the upgrade ? [y/n]
In order to proceed with the upgrade process, the following RPMs will be removed:
xmltodict-0.9.2-1.noarch
isodate-0.5.4-1.noarch
six-1.9.0-1.noarch
python-pywinrm-0.0.3-1.0.noarch
Are you sure you want to proceed with the upgrade ? [y/n]
```

> ⚠ This will only occur when upgrading from NEO v1.5. Before clicking 'y', make sure the RPMs do not have any dependencies that are not related to NEO.

7. [Optional] Run Mellanox NEO manually after the installation is complete.

```
/opt/neo/neoservice start
```

8. [Optional] In order to use more provisioning templates of Mellanox NEO supported system types (Linux hosts, Windows hosts, Arista switches and Cisco switches), you may download and install Mellanox NEO external RPMs. For further details on how to download and install external Mellanox NEO RPMs, please refer to the community post "HowTo Install NEO Plugins".

> ⚠ You can download and install the external RPMs also after Mellanox NEO is up and running.

Uninstalling Mellanox NEO

To uninstall the Mellanox NEO software, run:

```
/opt/neo/neo-uninstaller.sh
```

Uninstalling Mellanox NEO as Docker Container

To uninstall Mellanox NEO as a Docker Container, run:

```
docker stop <container-id>
docker rm <container-id>
```

For Mellanox NEO running in High Availability mode, run the following:

```
docker exec -it <container-id> /opt/neo/neocluster stop
docker stop <container-id>
docker rm <container-id>
```

Operating Mellanox NEO Services

NVIDIA® Mellanox® NEO® users may start, stop, or restart Mellanox NEO services, or check their status at any time.

To start Mellanox NEO services, run:

```
/opt/neo/neoservice start
```

In order to stop Mellanox NEO services, run:

```
/opt/neo/neoservice stop
```

In order to restart Mellanox NEO services, run:

```
/opt/neo/neoservice restart
```

In order to check Mellanox NEO services status, run:

```
/opt/neo/neoservice status
```

NEO Health Monitoring

NEO uses Monit to monitor the status of NEO and dependent services (influxdb, telegraf, kapacitor). If one of these services is down, Monit detects it and restarts the service after a few seconds.

To see the exact monitoring configuration, please refer to /etc/monit.d/neo.monitrc.

Mellanox Care

Mellanox NEO incorporates a monitoring mechanism that can be combined with Mellanox Care™, a support program that offers 24/7 fabric management services to monitor network health. This mechanism traps network events and issues regular notifications to Mellanox's Network Operations Center (Mellanox NOC). Special Mellanox personnel analyzes the details of the reported events and takes action according to the service level agreement (SLA).

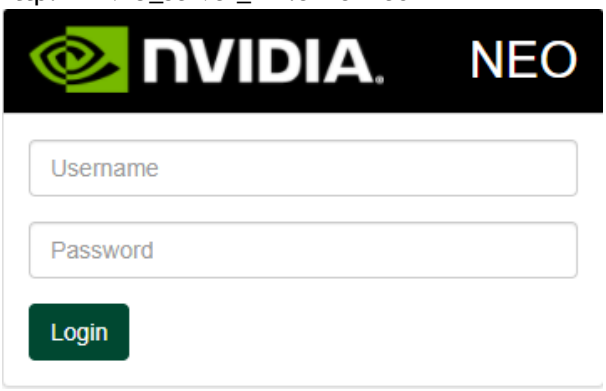
Mellanox Care identifies, alerts and addresses hardware failures, non-optimal configuration, service degradation issues, performance issues and more.

To obtain a Mellanox Care license, please contact your Mellanox Support.

Launching Mellanox NEO GUI

To launch a Mellanox NEO GUI session:

1. Start the Mellanox NEO server.
2. Launch the GUI by entering the following URL in your browser:
   http://<NEO_server_IP>:3443/neo



3. In the Login Window, enter your Username and your predefined user Password and click Submit.

User Authentication

Mellanox NEO user authentication is based on standard Apache user authentication. Each web service client application must authenticate against the Mellanox NEO server to gain access to the system. The Mellanox NEO software comes with one predefined user:

- Username: admin
- Password: 123456

> ⚠ It is recommended to change the default password to a new and personalized one in order to ensure that your NEO account is safe.

Mellanox NEO GUI

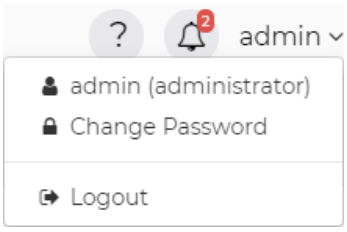
The Mellanox NEO software has several main GUI views. Before exploring the different options, it is recommended to perform the following steps:

> ⚠ The steps below can be performed by administrators only.

1. Click on the “Settings” tab:
   a. Select the “Users” view to add new Mellanox NEO users, and define users’ roles and credentials.
   b. Select the “Email” view to add recipient lists. Upon user’s definition, these lists could be used to distribute specific event alerts to a group of recipients.
   For further instructions, see “Settings”.
2. Click on the “Events” tab to activate and deactivate events, and define the severity, condition-value, description and notification parameters for each event. For further instructions, see “Events”.

Interface Frame

Profile Icons



When clicking the small profile icon on the top left corner of the left-hand menu, a drop down menu will appear, providing the user with the following:

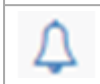
- Username – can either be a regular user or an admin
- The ability to change the account password

Main Tabs/Categories/Navigator Buttons

The following table describes the main Mellanox NEO® windows and categories:

Navigator Tabs

Tab Icon	Function	Description
	Dashboard	Provides single view highlighting information and network status

Tab Icon	Function	Description
	Managed Elements	Provides a list of devices, inventory, ports, groups, virtual machines, and virtual switches
	Network Map	Provides a visual view of the physical connectivity between managed devices
	Services	Provides automation tools for complex networking configurations
	Configurations	Available for administrators only. Provides the ability to create/edit configuration files and provisioning templates and manage network snapshots.
	Telemetry	Presents several reports of information collected by the management system, and allows to save and load them
	Tasks	Available for administrators only. Displays future scheduled Jobs.
	Jobs	Available for administrators only. Displays all the running and completed jobs in the system.
	Events	Provides notification events or critical device faults of the switch and server data events. The “Events Policy” view allows the user to activate and deactivate events, and define the severity, condition-value, description and notification parameters for each event.
	Notifications	Displays all network notifications
	System Health	Provides information on Mellanox NEO building blocks
	Settings	Available for administrators only. General system settings (default access credentials, user management).

Monitoring Window

The Mellanox NEO dashboard enables an efficient network view from a single screen and serves as a starting point for event or metric exploration.

There are 4 dashboard views:

- General dashboard
- RoCE dashboard
- What Just Happened dashboard
- Network Health dashboard

General Dashboard

The fabric dashboard provides single view that is highlighting information and network status in the following smaller dashboard windows:

- Events
- Network Health
- WJH Category Distribution
- Services
- Configuration Changes

For more information, please refer to page Mellanox NEO Fabric Interface Dashboard.

What Just Happened®

The What Just Happened dashboard provides a view of the fabric packet drops information and statistical data of the drop reasons. The information is retrieved from the Telemetry Agent by a dedicated “What Just Happened” session.

RoCE Dashboard

The RoCE dashboard provides a single view that is highlighting information and network status related to RoCE traffic. The information is displayed in the following smaller dashboard windows:

- Last 24 Hours RoCE Related Events
- RoCE Services
- Recent RoCE Related Activity

Network Health Dashboard

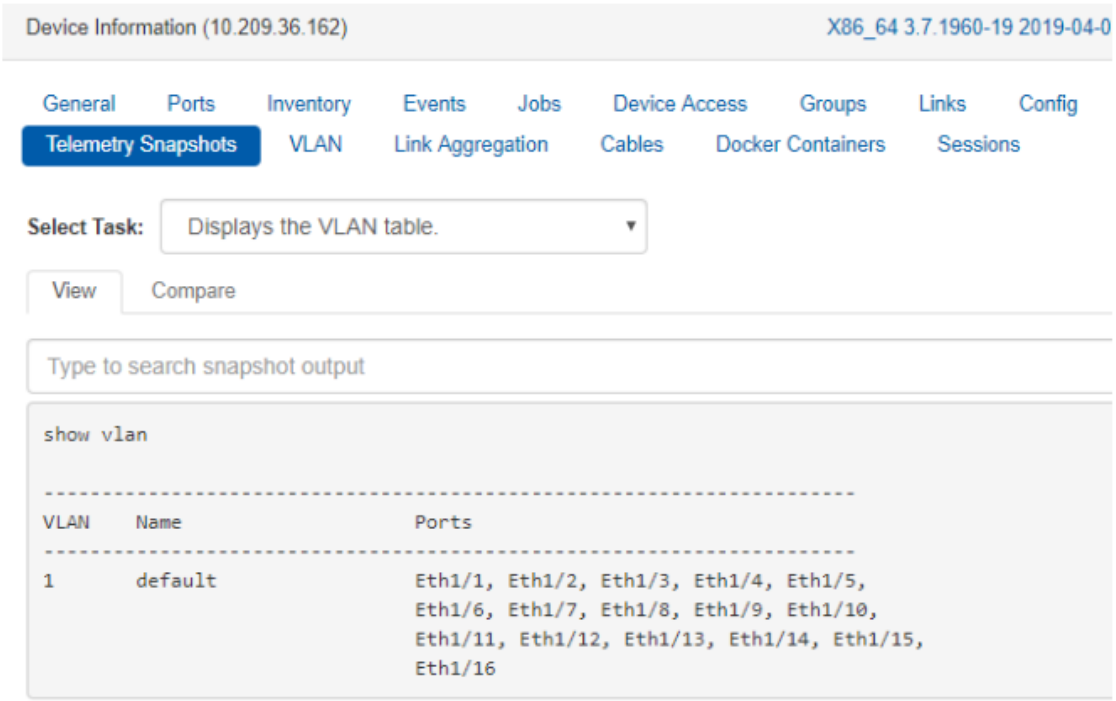
This dashboard provides a graphic display for each device in the system representing its status and the severity of events reported on it.

Managed Elements Windows

The Managed Elements panel provides a list of devices, inventory, ports, groups, virtual machines, virtual switches, cables and sites.

- The Devices window displays a list of all devices on the machine, with the following related to each device: its IP address, name, system type, status, and MAC address.
    - A click on any device will display in a right panel a list of “Device Information” that includes: Stats, Ports, Inventory, OS, Events, Jobs, Credentials, Groups, Links, Config, Telemetry Snapshots, VLAN, LAG, Cables and Docker Containers.
    - A right click on a device or on multiple devices will allow performing any of the following actions, provided that the selected devices are capable of these actions: Provisioning, Connectivity Check, Install, Reboot, Remove, Acknowledge, Go To Map, History Monitoring, Live Monitoring, Create MLAG with, Add to Group, Add to Site and Generate Dump.
      For more information on the Devices window, refer to "Devices"
- The Inventory window provides detailed information about each device part (such as CPU and FAN) - its serial number (S/N), part number (P/N), model, vendor, state and health. For more information on the Inventory window, refer to "Inventory".

- The Ports window provides information about all ports in the fabric – the device they are connected to, their name, protocol type, active speed, MTU, operational state and admin state. A click on one of the ports will display further information about that specific port: Counters, Errors, Cable, VLAN and LAG, when available. For more information on the Ports window, refer to "Ports".
- The Cables window provides the following information about the cables connected to the switches: the ports to which the cable is connected, its serial number, cable type, part number, revision, length and speed.
- The Groups window provides information about existing groups, their members and group credentials (if defined), and allows the user to create new groups. For more information on the Groups window, refer to "Groups".
- The Sites window allows you to define physical locations of devices with information about the site's members. For more information on the Sites window, refer to "Sites".
- The Virtual Machines window lists all the Virtual Machines (VMs) that run on all KVMs in the network. For more information on the Virtual Machines window, refer to "Virtual Machines".
- The Virtual Switches window lists all the Virtual Switches that run on all KVMs in the network. For more information on the Virtual Switches window, refer to "Virtual Switches".
- The Telemetry Snapshots window provides a view of the system telemetry snapshots:



Network Map Window

The Network Map window shows the fabric, its topology, elements and properties. NEO performs automatic fabric discovery and displays the fabric elements and the connectivity between the elements. In the Network Map window you can see how the fabric and its elements are organized (e.g. switches and servers).

For more information on the Network Map window, refer to "Network Map".

Configuration Management Window

> ⚠ This panel is visible to administrators only.

The Configuration Management panel allows creating and editing configuration files and provisioning templates, as well as managing network snapshots. This panel is composed of three tabs: Network Snapshots, Global Configuration and Provisioning Templates.

For more information on the Configuration Management window, refer to "Configuration Management".

Telemetry Window

The Telemetry panel is composed of three windows:

- Monitoring – allows creating live and history monitoring sessions
- Snapshots – allows creating monitoring snapshots
- Streaming – allows to view the current telemetry sessions (predefined and customized sessions), their status, and their members (switches)
  For more information on the Streaming window, refer to "Streaming".

Tasks Window

> ⚠ This panel is visible to administrators only.

The Tasks panel presents user's defined tasks (future scheduled Jobs). The following tasks are supported:

- Selecting a single or multiple devices and setting an action such as software upgrade or provisioning (CLI-command) and the action setting data
- Selecting a specific action on a device/a group of devices and creating a task from this action and its setting data
- Adding or deleting a task
- Dynamically selecting devices using filters (wildcards) tasks

For more information on the Tasks window, refer to "Tasks".

Jobs Window

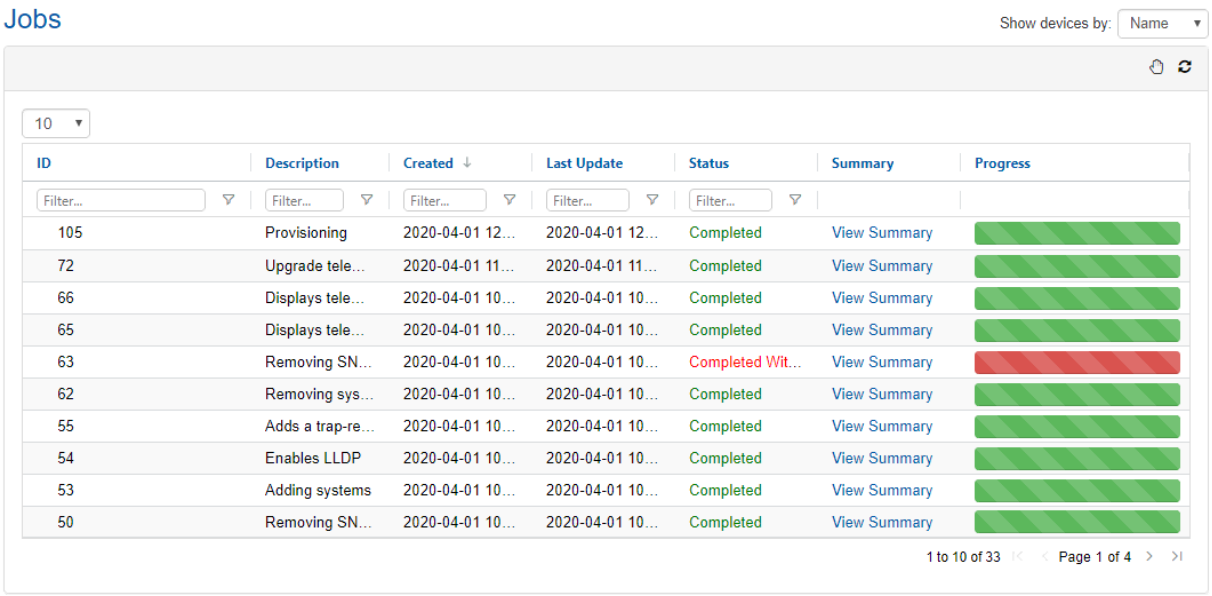
> ⚠ This panel is visible to administrators only.

The Jobs panel displays all of Mellanox NEO's running Jobs. A Job is a running task defined by a user and applied on one or more of the devices (provisioning, software upgraded, switch reboot etc.)

Mellanox NEO users can monitor the progress of a running job, as well as the time it was created, its last update description and its status. The status value can be "Running", during operation, "Pending", if another job is already running in the same device, "Completed with Errors" if an error has occurred, and "Completed". To cancel a pending job, right-click on the relevant job, and then choose "Abort".

Job States

Job State	Description
Created	Job was created and will shortly start running.
Pending	Job is pending by Mellanox NEO. This state appears in case another job that contains at least one common device is already running.
Running	The pending job was released and is now running.
Completed	All sub-jobs were completed successfully
Completed with Errors	All sub-jobs were completed, but on some of them, errors occurred.
Aborted	A pending job was canceled by the user.



Jobs can also be tasks scheduled by the system. In such cases, the users can monitor the progress of these jobs but cannot control them.

For further information on the Jobs window, refer to "Jobs".

Events Window

Mellanox NEO includes an advanced granular monitoring engine that provides real time access to switch and server data events. Network events can either be notification events or critical device faults. The events information includes severity, time.

For further information on the Events window, refer to "Events".

Notifications Window

The Notifications tab is Mellanox NEO's incoming messages box, providing the administrators network notifications.

For further information on the Notifications window, refer to "Notifications".

System Health Window

> "High Availability" panel is visible to administrators only.

The System Health panel is composed of three windows:

- Providers – the building blocks of Mellanox NEO
- High Availability – a mechanism meant to serve as a backup if the active node on which NEO is installed should fail
- Logs – presents detailed logs and alarms that are filtered and sorted by category, providing visibility into traffic and device events as well as into Mellanox NEO server activity history.

For further information on the System Health window, refer to "System Health".

Settings Window

> This panel is visible to administrators only.

For further information on the Settings window, refer to "Settings". The Settings panel allows administrators to edit users' profiles, define general system settings such as default access credentials, generate backups and restoration points and create and manage provisioning templates.

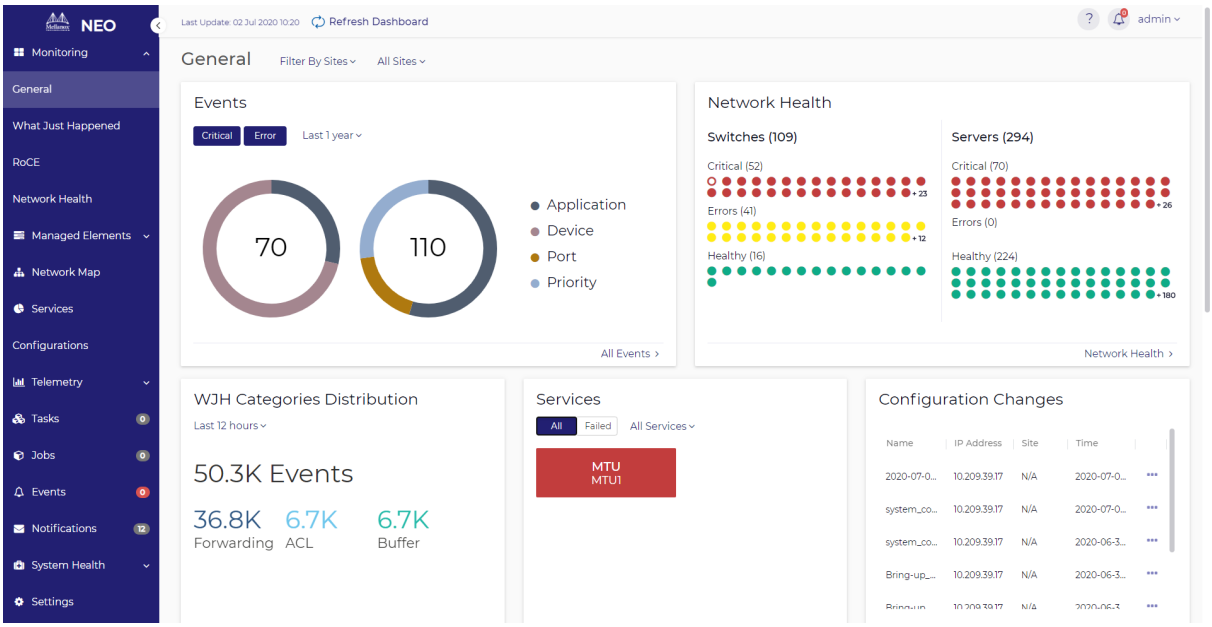
Mellanox NEO Monitoring

NEO's monitoring dashboards are central views enabling to oversee and analyze the network state. The available dashboards are:

- Fabric dashboard – for overall network status
- What Just Happened® – for information about packet drops in the fabric
- RoCE dashboard – for RoCE related network status
- Network Health – for a graphic display for each device in the system representing its status and the severity of events reported

General Dashboard

The general fabric dashboard displays several sub-panels, as shown in the following figure.



Events

The Events panel displays statistics pertaining to critical and error events that occurred over a specific period. A pie chart is available to visualize each event type. You may show critical and/or error events by clicking the Critical and/or Error buttons respectively. If only one severity is selected, you will see one big pie chart instead of two smaller ones.

The events are distributed over 4 categories: Application, Device, Port, and Priority.

Inside each one of the pie charts, you will have the total number of events. Hovering over a specific slice, shows the category and number of events belonging to that category.

You may utilize a time filter to view events for a specific time period. It has dropdown list with the following options:

- Last 5 minutes
- Last 1 hour
- Last 12 hours (default)
- Last 24 hours
- Last 1 week
- Last 1 month
- Last 6 months
- Last 1 year

The charts are updated according to the time filter settings and the settings of the general filters in the dashboard (Sites, Groups, Devices).

Clicking the "All Events" link at the bottom redirects to the events page.

Clicking on a specific category will open a preview model displaying the subcategory distribution for that category.

If both Critical and Error severities are selected, the area on the left displays "Critical" subcategories and the one on the right displays "Error" subcategories.

If more than 5 subcategories exist, the top 5 appear first, and the rest are collapsed under a bar called "Other" which can be expanded to reveal the statistics for the subcategories inside.

Clicking "Full Report" on the bottom right corner navigates to the Events page.

The pagination function allows us to navigate between categories—clicking the right arrow (>) to the right of the preview model takes you to the subcategory distribution of the next category.

Network Health

Network Health displays switches and servers as circular nodes in different colors according to the severity of their health state; it will show the switches in the left panel and the servers in the right panel.

The colors of circles will indicate the status of the device as follows:

- Green – OK
- Yellow – Error
- Red – Critical
- Empty red circle – Lost communication

For each device type (Servers, Switches) we will have the title (Switches or Servers) and next to it the number of devices under this type; and for each severity we will have the title (Critical, Errors, Healthy) and next to it we will have in brackets the number of devices under that severity.

Once a certain device is clicked, a preview model is displayed showing more information about the device (hostname, IP, site, system type, MAC address).

In the preview model, pagination is enabled and clicking on the "<" or ">" arrows navigates to other nodes of the same device type.

Clicking "Network Health" in the model or in the Network Health panel redirects to the "Network Health" dashboard.

If there are too many devices to show on the small panel, a + sign with a number appear indicating the number of remaining devices (e.g. +34). If clicked, a preview model appears showing all devices in same severity.

WJH Category Distribution

WJH Categories Distribution provides information regarding packet drops throughout the fabric and statistical data of the drop reasons. It consists of four main parts:

- A drop-down menu time filter to view statistics for a specific time period
- The total number of events in the selected time period
- Distribution of events per category displaying the number of drops per category and the name of that category under the number
- The "WJH Dashboard >" button which navigates to the What Just Happened dashboard

If more than three categories exist, then pagination is activated making it possible to navigate to the other categories.

Clicking any of the categories opens a preview model showing drop reasons that fall under that category.

Per drop reason distribution, you see:

- Reason name
- Number of drops associated with it
- Bar illustrating the proportion of drops belonging to it

If there are more than 5 reasons, the distribution for the top 5 is shown and a reason group called "Other" is displayed which combines all other reasons. If Other is expanded, distribution for all the remaining reasons is displayed.

Clicking < or > navigates to next/previous category. Clicking "WJH Dashboard" navigates to the What Just Happened dashboard.

Services

The Services panel provides a view of all services created in the system. In addition to global filters in the dashboard, this panel has two filters which affect what is displayed:

- All/Failed filter: "All" shows all the services created. Failed shows for showing the failed services only.
- Custom filter that displays specific services. by default, "All services" is selected.

Clicking on a specific service opens a service preview model displaying the following information for each member:

- Validation Status
- Configuration Status
- System Name
- IP
- Site

The validation and configuration status will be displays with a circle as follows:

- Red – completed with errors
- Green – completed
- Gray – unknown

The title of the model will contain the name of the service and the number of members in that service in parentheses.

Hovering over specific status indicators shows a tooltip of the status (e.g. Completed).

You're able to navigate to the status of other services by clicking the "<" and ">" arrows.

Clicking "All Services" redirects to the "Services" page.

Configuration Changes

The Configuration Changes panel provides the user with some information about the latest configuration changes applied to devices. This panel contains the following information:

- Device hostname
- Device IP address
- Site to which the device is assigned

- Time of last change on the device

If desired, the three dots can be clicked in order to download configuration for a specific device.

Clicking "All Configurations" redirects to the "Configurations" page.

What Just Happened® Dashboard

NEO gives the user an out-of-box, built-in WJH dashboard to view current and historical WJH data from managed Mellanox Spectrum® switches. In order to do so, NEO relies on InfluxDB and switch Telemetry Agents on the switches as part of the solution. Please see "NEO Telemetry Agent" for the Telemetry Agent installation procedure.

The telemetry data can be visualized and queried by using either NEO or any visualization software available. To get the telemetry data into the database of choice, a switch Telemetry Agent is used to pull, parse, and apply logic and stream out of the Mellanox Spectrum switch.

To enable WJH using NEO, the Telemetry Agent must be installed in a docker container on the switch.

WJH is only supported through CLI with Web UI or using NEO, but not in parallel.

Once installed and enabled, The WJH dashboard can be accessed to visualize WJH categories, events, and other details. For a list of possible packet drop reasons, please refer to What Just Happened® Reasons.

The upper main section of the page, contains the title, the number of dropped packets, and the filters button.

WJH Filtering

Under the title, users can find the WJH presets, where they are able to add/edit filters which affect the data presented in the WJH dashboard.

On the top-right of this area, users can save filters to the current preset, create a new preset, or reset the filters to the default preset. More about presets in the Manage Presets and History section.

Filter Editing Area

Users may access this area by clicking the filters icon on the top-right of the dashboard, or clicking the edit icon next to each item in the filters area, or clicking "+ Add Filters".

This screen allows users to modify currently selected filters, add new filters, or manage presets.

Time Filtering

In the Active Filters section, users are able to sort through WJH results by setting a time filter. Clicking the dropdown menu allows users to select from several preset time options. Alternatively, users may also select a custom time frame by clicking the Custom option.

This opens up a calendar from which users may select start and end time.

Severity Filtering

Users may select which severity (i.e. Error, Warning, Notice) they want to include (at least one should be selected) in their WJH results.

Add Filters

This area provides the ability to add new filters to your presets.

- The search box enables users to search for specific attributes and filter with them (e.g. search for specific drop reasons)
- The Metadata section provides the ability to filter for metadata (e.g. reason, switch, port, etc.)
- The Flow Details section features the following submenus for filters (L2, L3, L4, VXLAN) If expanded, users can filter attributes for these categories (e.g. filter specific MAC under L2, or filter for a specific L3 protocol).

  Every category has the option to either include or exclude.

Categories Distribution

This panel provides statistics about the reported drops per category. Per category, this section shows the reason distribution in pie chart format.

Above each pie chart, users can see the name of the category it represents, and in the middle of each pie chart, users can see the total number of drops belonging to this category. Each slice in the pie represents the portion for specific reason drops.

Filtering for Specific Drop Category

Hovering in the middle of one pie chart (on the number), opens a tooltip showing the name of the category and the option to add it to filter by clicking "+ Add to Filters".

After filtering on a specific category is applied, it will affect the entire dashboard. All results for drops would belong to that category only. The name of this area is also changed from "Categories Distribution" to "Reasons Distribution". The filter is then added to the filters area (e.g. category is Forwarding).

The reason distributions will appear beside the pie chart in bars graphs. The first two bars will show the proportion of drops with the highest rate of occurrence. The remainder of the drops are lumped under an expandable "Other" bar.

The filter may be removed by clicking the Edit button at the top of the dashboard and removing it in the Edit Filters module.

Filtering for Specific Drop Reason

Clicking on a specific slice under Categories Distribution shows a tooltip containing the name of the drop reason, the number of drops belongs to that reason, and the option to add that reason to your filters by clicking "+ Add to Filters".

Once the filter is added, both category and reason are added to the filters, and only drops for the filtered reason will appear now.

Reordering Categories

By default, the categories are presented in descending order according to the number of drops, but the pie charts can be rearranged by clicking and dragging the 4 dots below each category.

Once the order is changed, a button appears to reset the order to default (descending).

Events Distribution Per Switch

This view displays the distribution of events per switch and features two options. One is to show all switches, and another to show the Top 3. If Top 3 is selected, then only 3 pie charts (if any) are visible. If All is selected, then we can see more than 3 pie charts (3 per screen).

By default, the pie charts are shown in descending order according to the number of drops. It is possible to reorder them by dragging and dropping them using the 4 dots below each switch.

In the following screen All is enabled. This enables pagination so more than 3 switches are visible. The order of the switch is changed so the button that reorders them (Order by Descending) is enabled.

Event Distribution Per Port – Multiple Mode (One Switch Filtered)

Hovering in the middle of the pie chart reveals a tooltip that contains the name of the switch and the option to add the switch to the filters.

If the switch is added to the filters, then the whole dashboard is affected as all panels will return data for that switch only.

The name of this panel will change from "Events Distribution Per Switch" to "Events Distribution Per port" as now it presents the distribution of events per port for the selected switch.

Event Distribution Per Port – Single Mode (One Port Filtered)

Hovering in the middle of the ports pie chart reveals a tooltip that shows the name of the port and the option to add it to the filters.

If the port is added to the filters, then the whole dashboard is affected as only drops for this port are displayed.

Events Distribution Per Port – Filtering for Specific Category

Hovering on a slice of the pie chart reveals a tooltip presenting the category name and the option to add it to the filters.

Once added, only drops for that port and that category are displayed.

Time-based Categories

This panel displays the WJH events received during in a specified period. This panel is affected with the filters applied to the dashboard.

Hovering over any point on the graph reveals a tooltip containing the name of the category, the date and time, and the number of drops that had occurred. It also has the option to add that category to the filters.

Detailed Flow Distribution

This panel allows users to select multiple properties and aggregate the events to display the combined number of WJH events.

Hovering over a specific bar displays the names of the properties selected, their value, and the combined number of WJH events for the selected properties.

The "i" icon indicates that L1 drops are not included in this distribution.

Detailed WJH Events

This table presents detailed information about each drop.

There is a collapse button at the top of each column in the table. Clicking it opens a filter module allowing users to narrow down the results they see in the table by deselecting certain values and clicking the apply button.

There are three vertical dots at the end of each WJH event (row). Clicking them opens up a context menu showing the two options:

- Details & Recommended Actions
- Streaming Settings

Details & Recommended Actions

Clicking "Details & Recommended Actions" opens a module showing the name of the switch, time of the WJH event, reason, and recommended actions to be taken.

Streaming Settings

Clicking "Steaming Settings" opens a module showing the streaming settings of the WJH event.

This model provides the ability to define some filters on the agent-side level. For example, to prevent the agent from streaming buffer drops, then they can be disabled using this module.

RoCE Dashboard Overview

The RoCE Dashboard contains a snapshot of the RoCE related network state, including information on service state, traffic and events. RoCE services can also be added and managed from this dashboard.

The RoCE related counters and events can be taken from the Telemetry Agent or retrieved by JSON API requests. This can be configured by the controller.cfg configuration file, in the Telemetry section. When using a Telemetry Agent, you must enable the NEO Counter Events session in the Telemetry streaming definitions page in order to get traffic events (see "Enable/Disable Session").

This feature is only supported for Onyx Spectrum switches.

Last 24 Hours RoCE Events

Last 24 Hours Events displays the RoCE related events that occurred over the last 24 hours in a column graph, where each column accumulates events by severity, per hour. Clicking a column on the graph presents a detailed view of the events that compose it.

RoCE Services

The RoCE services section displays all the RoCE services and allows adding new ones and managing them.

Clicking the "+ Add" button opens the RoCE Service Creation wizard, which allows defining and configuring RoCE on the network devices. For more details, see "RoCE".
Clicking a RoCE service element will open a panel that shows details on this service.

List Tab

This tab displays all the devices managed by the service, their ports and their status. The Status column displays the device configuration and validation status, and the RoCE Telemetry column displays the RoCE traffic state for this device. High bandwidth, utilization, packet discard and other traffic related events are reflected in this column.

Clicking a device row opens another panel with the device ports' details.

Ports Sub-Tab

This sub-tab shows a list of ports with their utilization and congestion information. The definitions of utilization and congestion vary by the type of RoCE configuration defined by this service:

RoCE Configuration	Utilization Means	Congestion Means
ECN Only	Total Port Utilization (%)	Total Port Packet Drops (%)
ECN + QoS	RoCE Traffic Class Utilization (%)	RoCE Traffic Class Packet Drops (%)
ECN + QoS + PFC	RoCE Traffic Class Utilization (%)	RoCE Traffic Class Congested Bandwidth (%)

Clicking the graph icon () near the port name opens the Telemetry tab, that displays telemetry data for the selected port.

Clicking the bell icon ( ) near the port name opens the Event tab, that displays events for the selected port.

Telemetry Sub-Tab

This sub-tab displays a graph with the last hour values of port counters relevant to the RoCE configuration defined by this device. The displayed counters are controlled by the checkboxes below the graph. The port can be changed by the drop down list above the graph.

The counters are displayed according to the selected configuration:

Displayed Counters per RoCE Configuration

ECN	ECN + QOS	ECN +QOS+PFC
Normalized bandwidth Normalized ECN Packets Normalized Discarded Packets	Normalized bandwidth Normalized ECN Packets Normalized Discarded Packets TC<priority> Normalized Bandwidth TC<priority> Discarded Packets	Normalized bandwidth Normalized ECN Packets Normalized Discarded Packets TC<priority> Normalized Bandwidth TC<priority> Discarded Packets PFC<priority> Normalized Congested Bandwidth

The RoCE data is gathered by the Telemetry Agent if it is installed on the switch. Otherwise, NEO uses the switch JSON-API to retrieve the data.

You may change the number of allowed priorities in the SNMP Monitoring controller file, and then create a RoCE service that matches one of the selected priorities (via max_priorities=?).

Events Sub-Tab

This sub-tab displays all the RoCE related events for this device. This includes service lifecycle events (service configuration, validation etc.), and RoCE traffic events for ports and priorities on this device.

Map Tab

This tab displays a network map with all the devices managed by this service. The color of the elements is based on their RoCE traffic state.

Events Tab

This tab displays all the RoCE related events for this service. This includes service lifecycle events (service configuration, validation etc.), and RoCE traffic events for ports and priorities on devices managed by this service.

Recent RoCE Activity

The Recent Activity panel provides direct access to the most recent 20 RoCE related events, in a date descending order. Clicking an event shows its details in the events page.

Network Health Dashboard

This dashboard provides a graphic display for each device in the system representing its status and the severity of events reported on it.

Devices Heatmap

Devices Heatmap displays all the devices in different colors according to the severity of their health state. Once clicked on a certain device, you will be directed to the Devices tab under Managed Elements where you can access all information about that device.

The colors imply the following health states:

- Green – OK
- Yellow – error
- Red – critical
- Empty red circle – lost communication

Through the Devices Heatmap panel, you can apply filters by clicking the icon (see above). The following filter dialog will be displayed.

After customizing a certain filter for the devices, you can choose either the red or the green color to denote the devices that match your filter.

Example:

To filter for the devices whose CPU load is greater than 5, select the “CPU Load” as the Attribute, the “>” icon as the operator, and “5” as the threshold. To view the devices filtered in green, select the Matching Color to be green.

Once clicked on “Submit”, the customized filter will be added to the bottom of the Devices Heatmap panel in the Dashboard (see below). The filters will be stored in the browser’s local storage so on any user login or page reload, the heatmap panel will remain saved with all applied filters.

On the right side of the panel, there are:

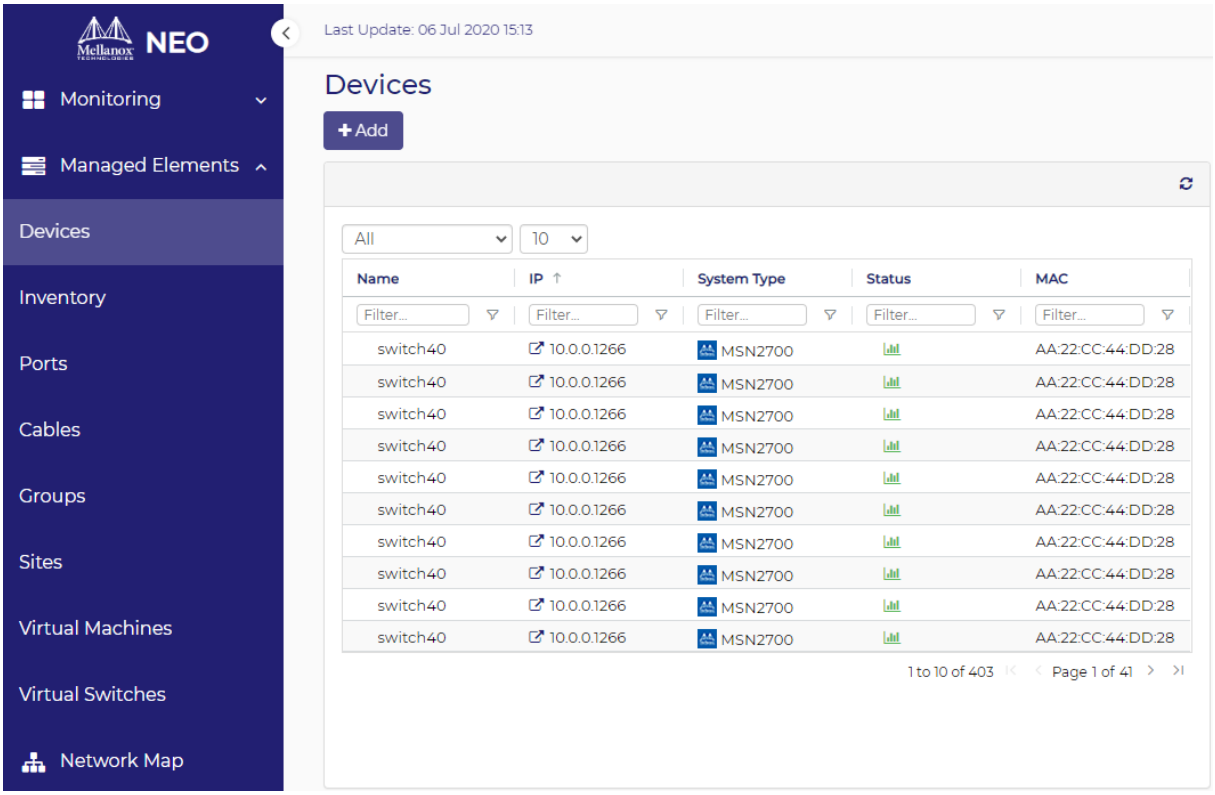
- A brief text that describes the filtered criterion, and a square icon colored with the Matching Color (in this example, CPU Load > 5, green). If you click on the description, you will be able to edit your current customized filter.
- A recycle bin icon () that enables you to delete the filtered heatmap
- A help icon (“?”) that displays your devices’ criteria according to the defined colors

Managed Elements

The Managed Elements tab provides a list of devices, inventory, ports, cables, groups, sites virtual machines and virtual switches.

Devices

Devices information includes the IP address of each device, the device's name, system type, status, health and MAC address.



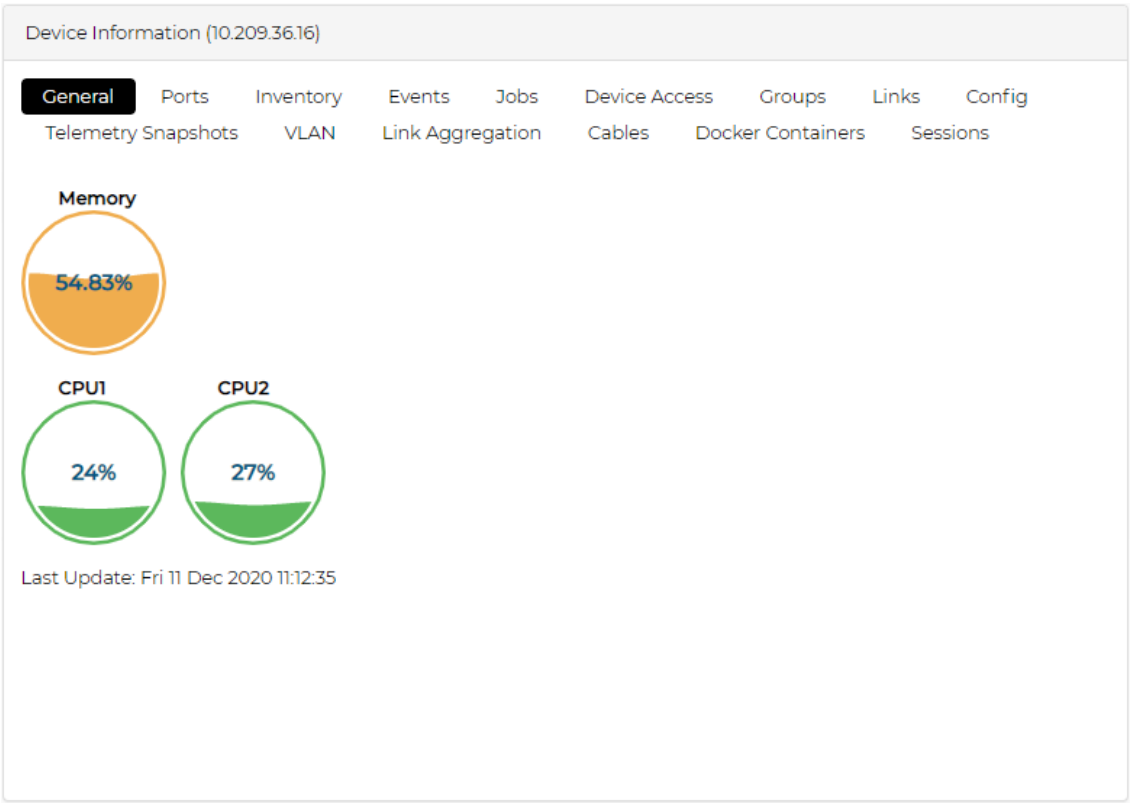
Device Information List

Device Information	Description
IP	The switch's IP address. **Note**: For Mellanox Switches, when clicking on the IP address, you will be redirected to the switch's web page, in which you will be able to configure the switch as desired.
Name	The switch's name.
System Type	Mellanox switch ( ) - displayed with its type. For example: MSN2100.
	Non-Mellanox switch ( ) - displayed with its name. For example: Arista/Cumulus Linux/Cisco/Juniper/Other Switches.
	Host ( ) - displayed with its type. For example: Windows/Linux/Nutanix/Other Hosts. The switch icon will also appear in case of a host with a bridge interface.

Device Information	Description
Status	The switch's status, which can be any of the following: • Unknown • Communication OK • Lost Communication • Rebooting • Pending Reboot
Health	The switch's health status, represented by the following icon colors: • Red - Major • Green - OK • Orange - Unknown
MAC Address	The switch's MAC address.

Additional Device Information

When clicking a single device, a list with the following information will appear on the right side of the screen:

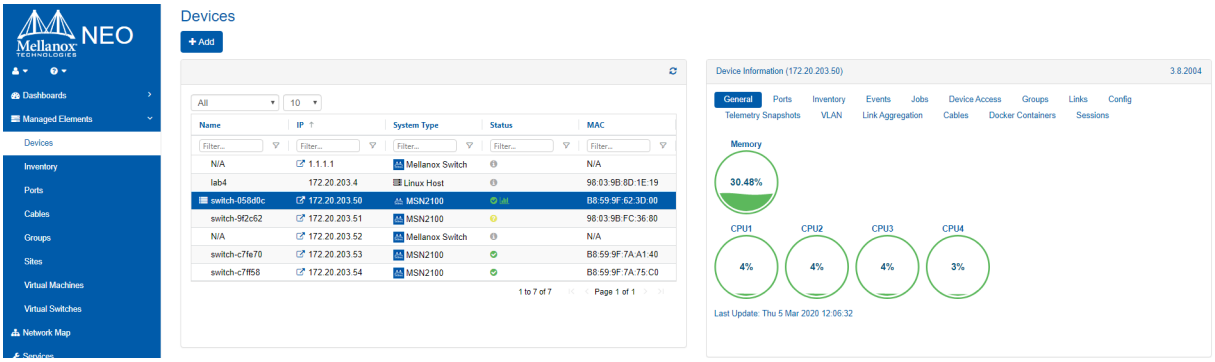


⚠ The "OS", "Events", "Jobs" and "Device Access" displays are not available for systems that are detected via the ETH Discovery provider.

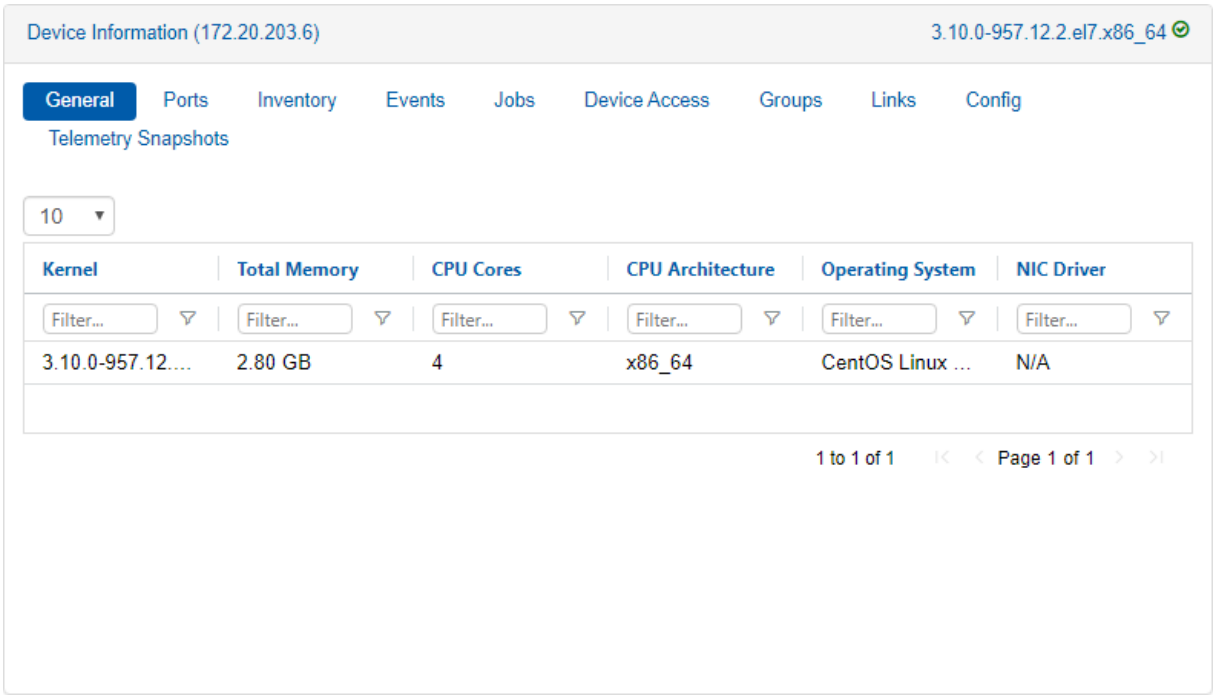
General Tab

Provides information about the device's CPU and memory usage in a gauge view. The colors are changed according to the utilization percentage as follows:

- 0-50%: Green
- [> 50]-70%: Orange
- [> 70]%: Red

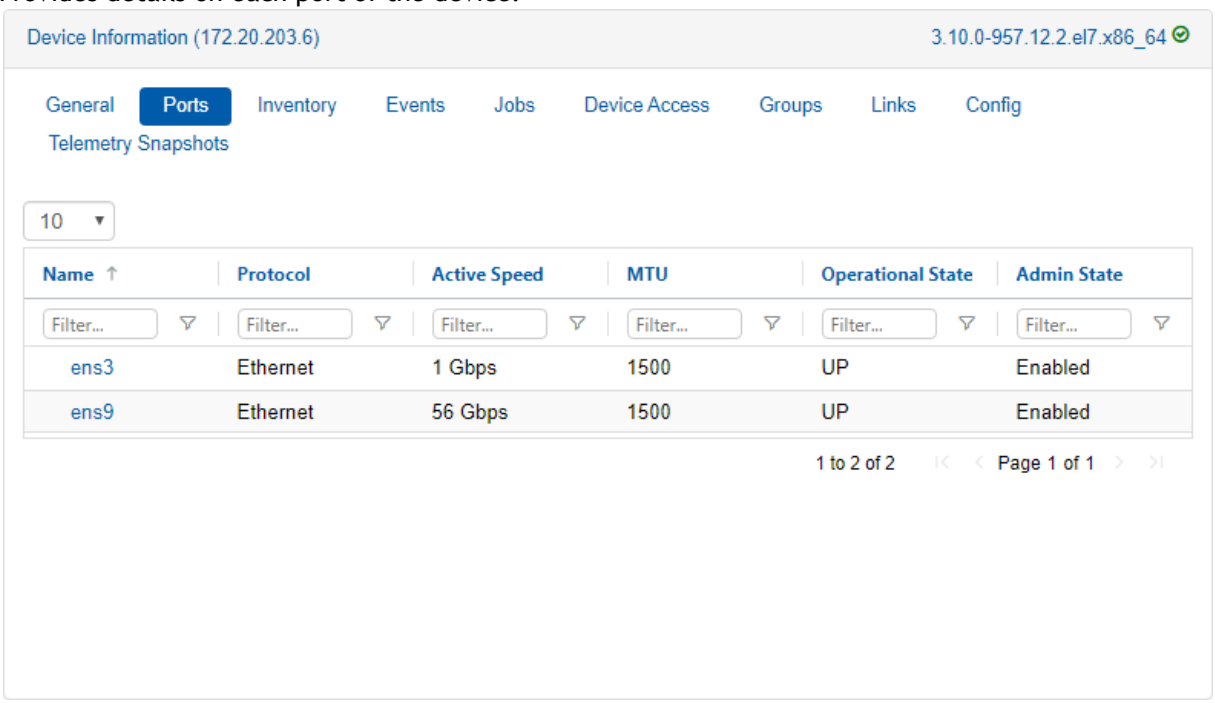


For hosts on which NEO-Host is installed, a table with information about the Linux server will be displayed:



Ports Tab

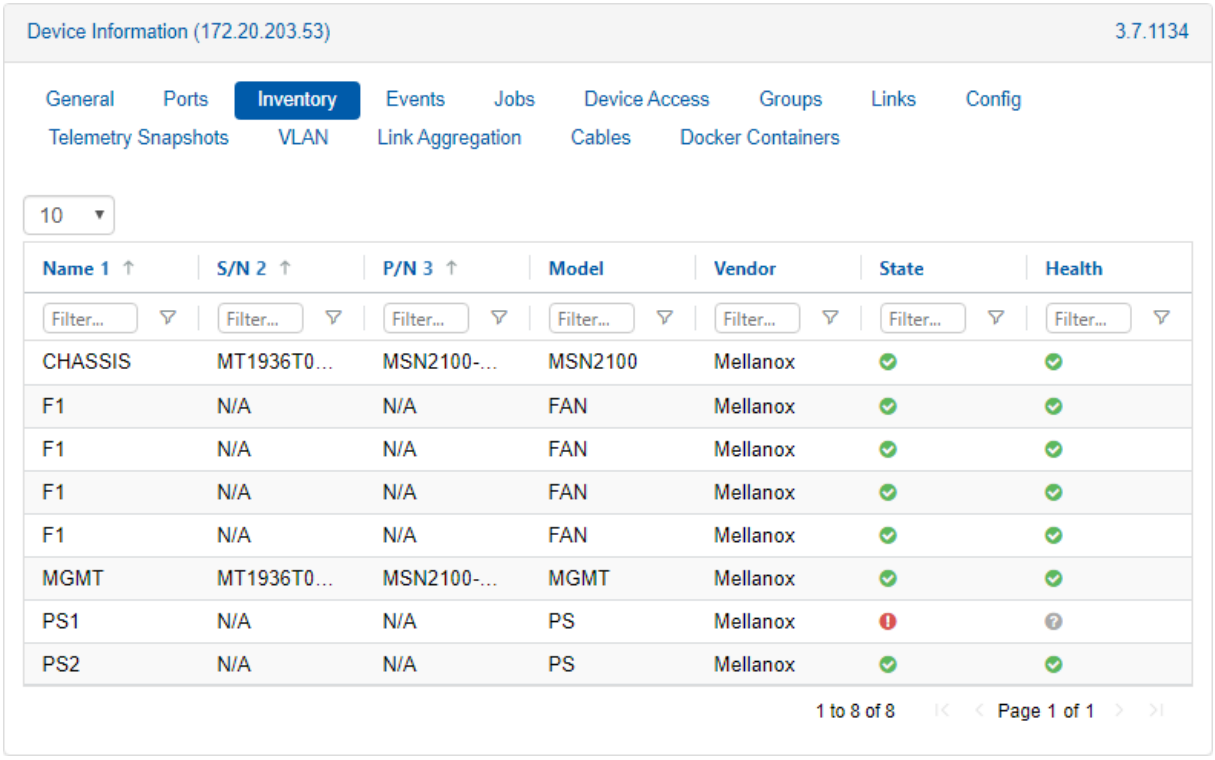
Provides details on each port of the device.



A right click on one port or more will enable performing live/history monitoring and provisioning on those ports. For information on these actions, refer to "Ports Actions".

Inventory Tab

Provides details on switch parts, such as FAN and CPU.

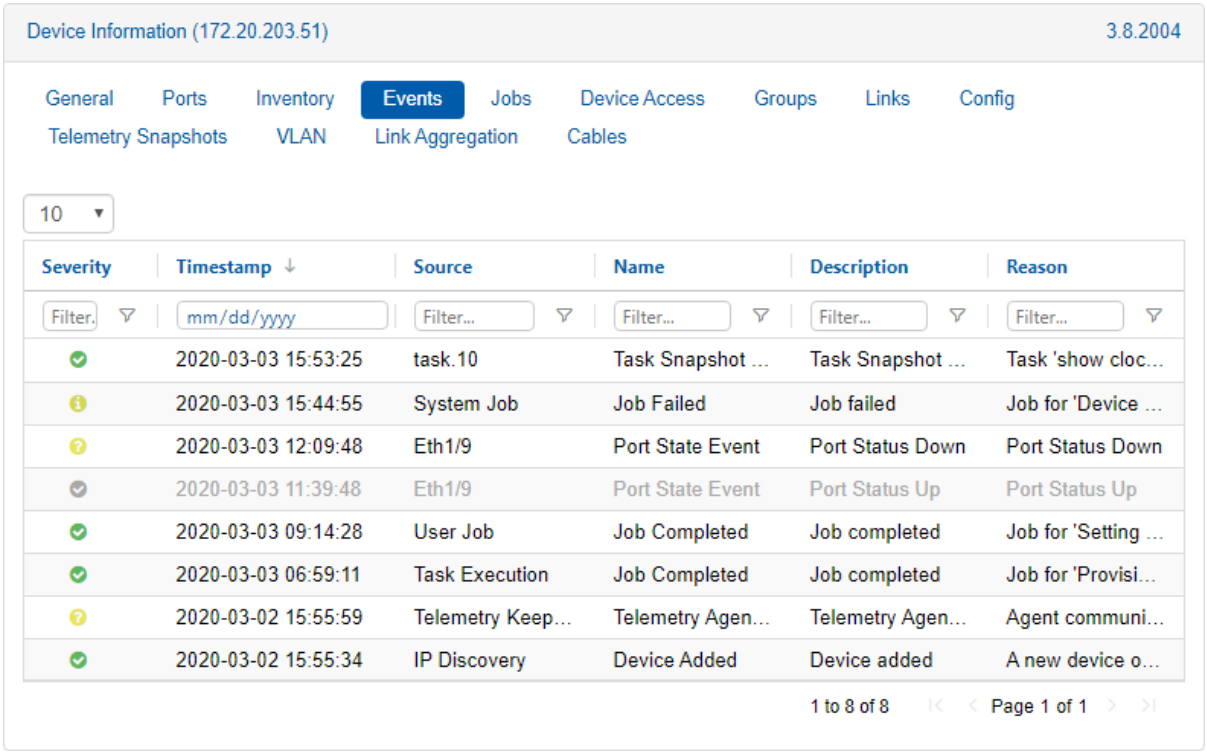


For Linux hosts on which NEO-Host is installed, a table with information about the Mellanox adapter cards will be displayed:

ID	Model	S/N	P/N	PSID	FW Version	Orig. Base MAC	State	Health
0000:82:00.0	ConnectX4	N/A	MCX456A-ECA_Ax	MT_2190110032		e4:1d:2d:5c:eb:68	OK	OK
0000:08:00.0	ConnectX5	N/A	MCX556A-EDA_Ax	MT_0000000009		24:8a:07:9c:13:8e	OK	OK

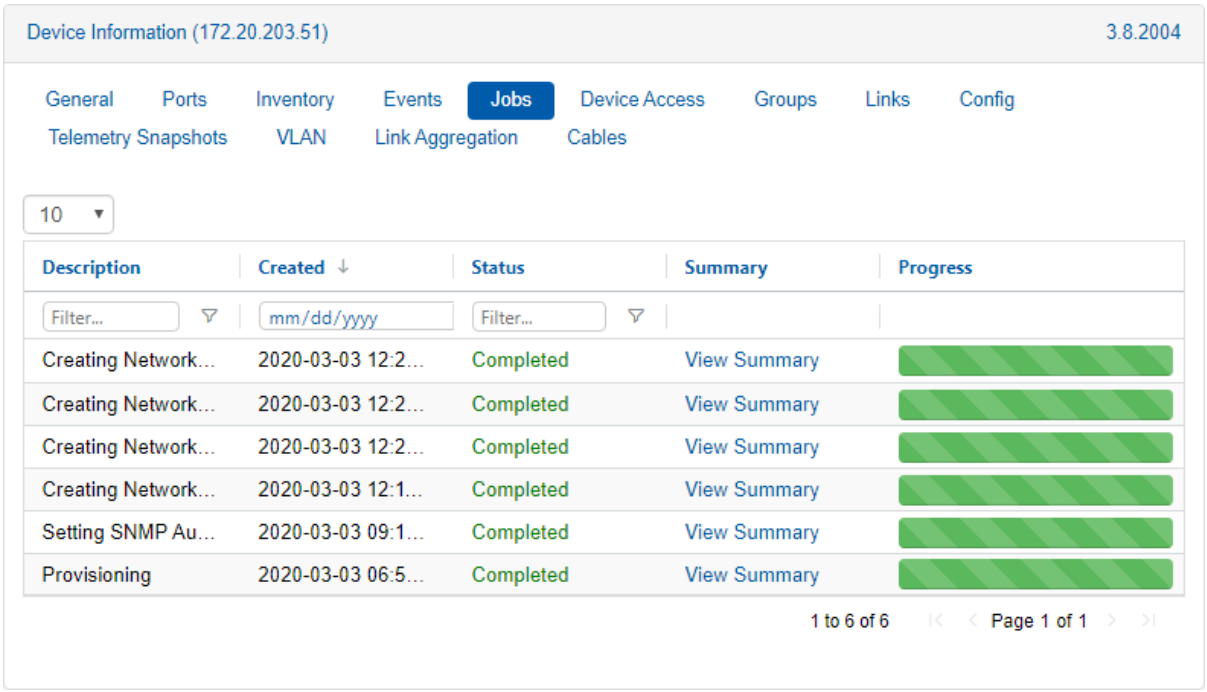
Events Tab

Lists specific switch related events.



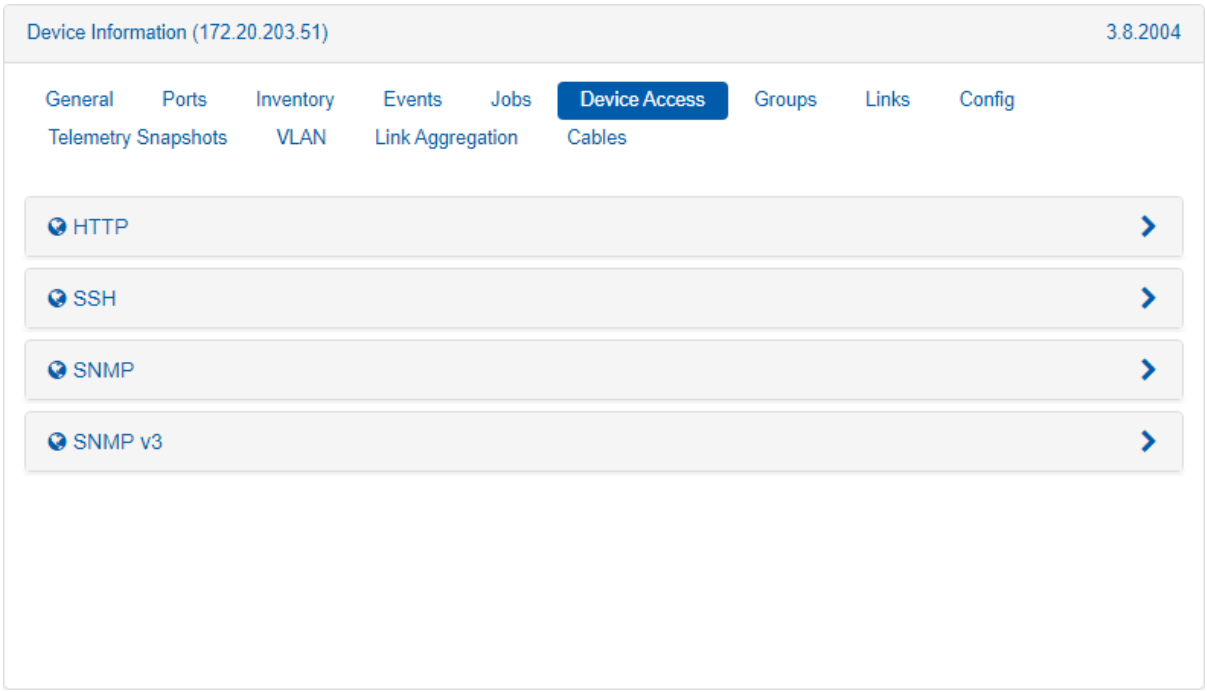
Jobs Tab

Lists switch jobs and their status.



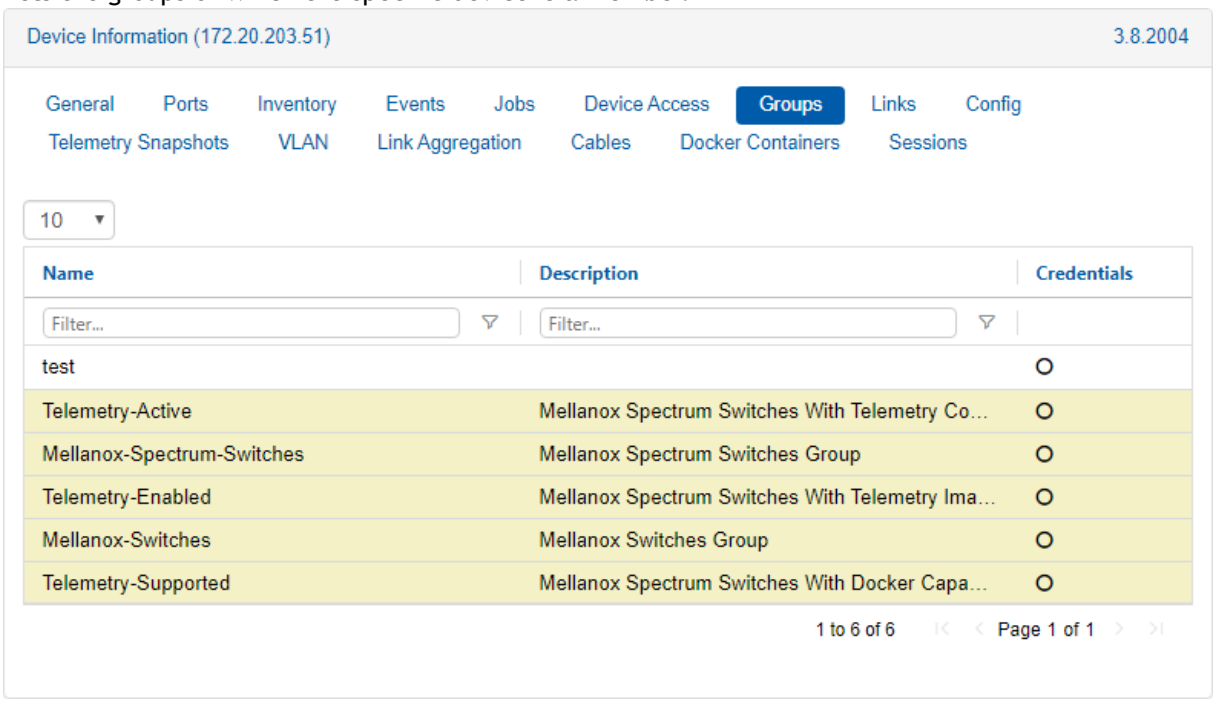
Device Access Tab

Displays access credentials for the specific device in the applicable protocols - HTTP, SSH, SNMP, SNMP v3.



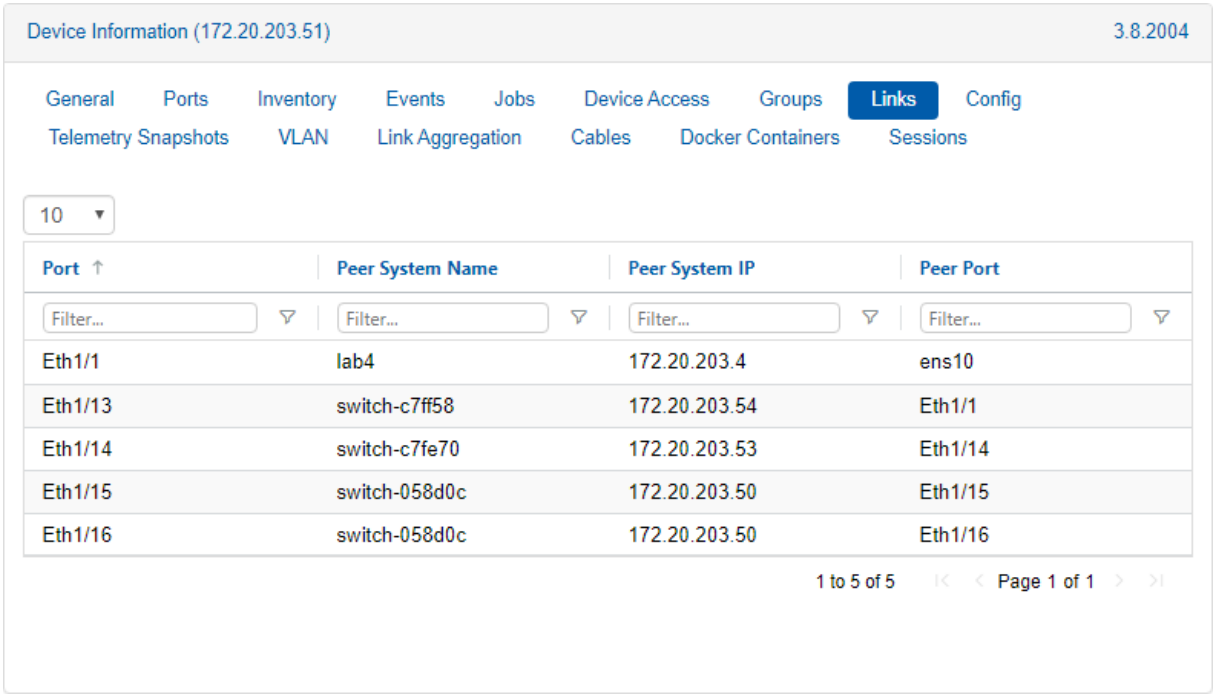
Groups Tab

Lists the groups of which the specific device is a member.



Links Tab

Details the active links of the specific device. The "Peer Name" and "Peer IP" columns specify the management peer and name, and the "Peer Port" column refers to the port to which the interface is connected. If the "Peer Port" is "Unknown", the interface is up, but no ETH discovery (LLDP) connection information is available.



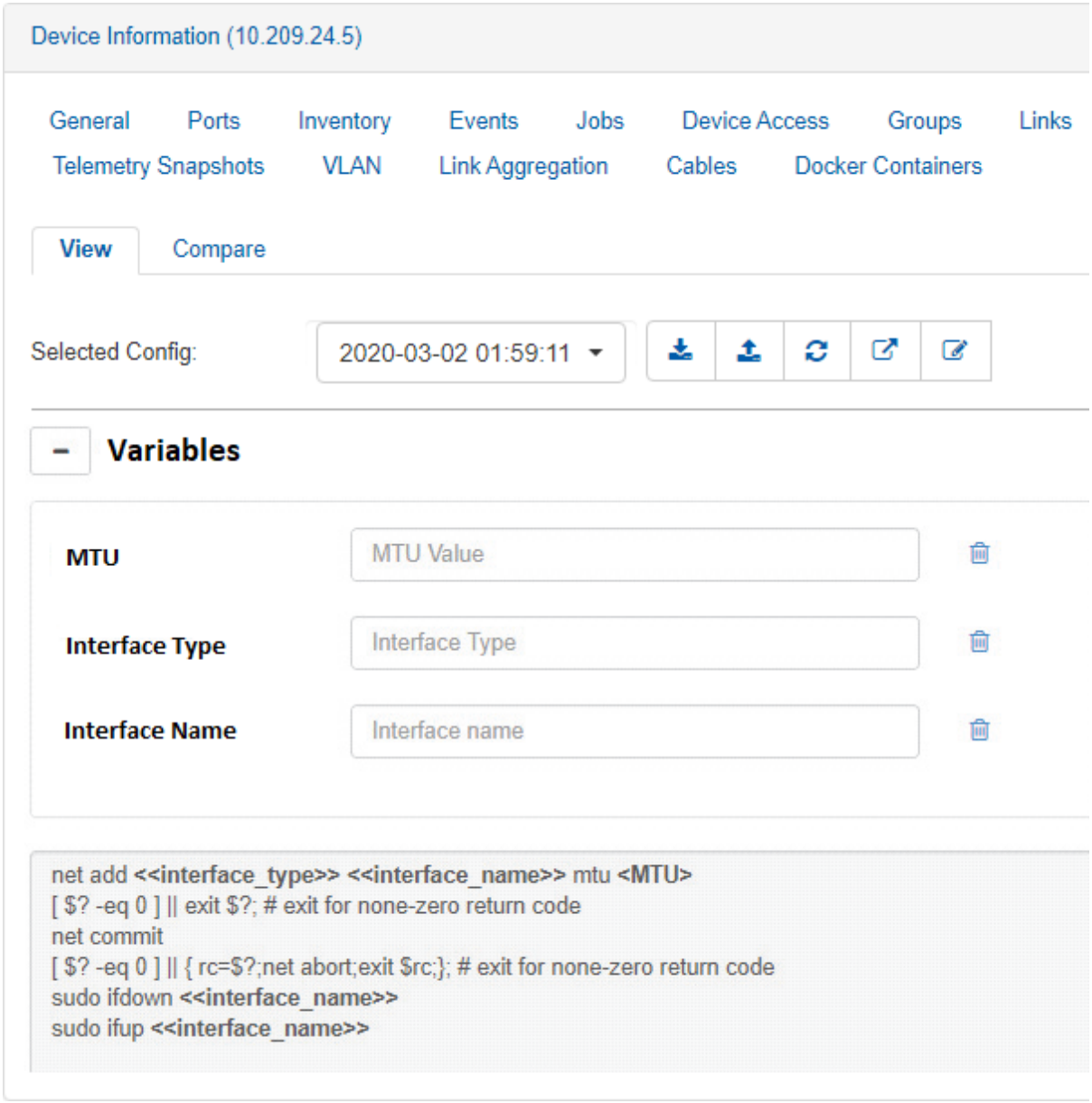
Config Tab

Enables users to perform the following:

- Take snapshots of running configuration files of a specific system in NEO. Configuration files provide general information about hosts.
- Manage existing snapshots and device specific configuration files.

Configuration Management can be accessed from two main windows in NEO; this Config tab, and the Configuration Management window from the left pane. For information on the latter window, please refer to “Configuration Management”.

In the Config tab under Devices, there are multiple buttons with different functionalities and purposes, explained in the tables below.

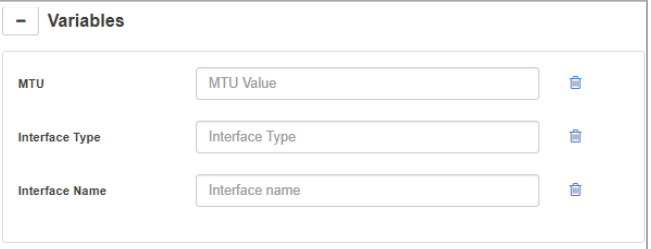


Config Tab Components

Icon	Name	Description
⇄	Compare Config Data	Allows comparing two configuration files or snapshots and tracks the changes between them (added information will be colored in green, and removed information will be colored in red and crossed out). See related Figure 4 below.
	Show Config Data	Displays configuration files content. See related Figures 3 and 4 below.
	Download	Downloads the chosen configuration file or snapshot to the user's computer.
	Upload	Uploads a device specific configuration file to NEO's repository. Note that snapshots cannot be uploaded.
▶	Fetch Config Data	Fetches information about the selected system's running configuration file. This icon is used for the first information retrieval request, and will be replaced with the next icon below.

Icon	Name	Description
	Refresh Config Data	Retrieves the content of the current running configuration on the system. If the content retrieved is different from the latest snapshot for that system, it will create a new snapshot. Otherwise, it will only update the "Last Verified" date to the time when the last snapshot was taken. These snapshots are also taken by NEO as it refreshes the configuration files of all devices every 24 hours. By default, NEO saves up to 7 snapshots for each device. **Note:** Hosts do not have running configuration files like switches. Therefore, "refreshing" a host will return general information about it.
	Apply Config	[Applicable to Mellanox and Cumulus Switches only] Applies the chosen configuration file or snapshot on the switch. The apply operation replaces the current running configuration. The operation might take a few minutes.
	Edit Config	Enables editing an existing configuration file of a specific system in NEO, and saving it for future use. The new configuration file can be saved as a new file using the "Save Config As" icon, or can overwrite the existing one, using the "Save Config" icon.
	Delete	Removes selected configuration files. This icon is only available for device specific configuration files (edited snapshots).

Related Figures:

Figure 1- Selected Config Drop Down Menu	Figure 2 - Configuration File Variables
 The Config drop down menu displays a log archive menu of all device specific configuration files ( ), snapshots ( ) of the chosen device, and global configuration files ( ).	 In order to apply the configuration file selected from the drop-down menu, values should be provided for the previously defined variables (if applicable).
Figure 3 - Configuration Content Example	**Figure 4 - Compare Config Data Output**

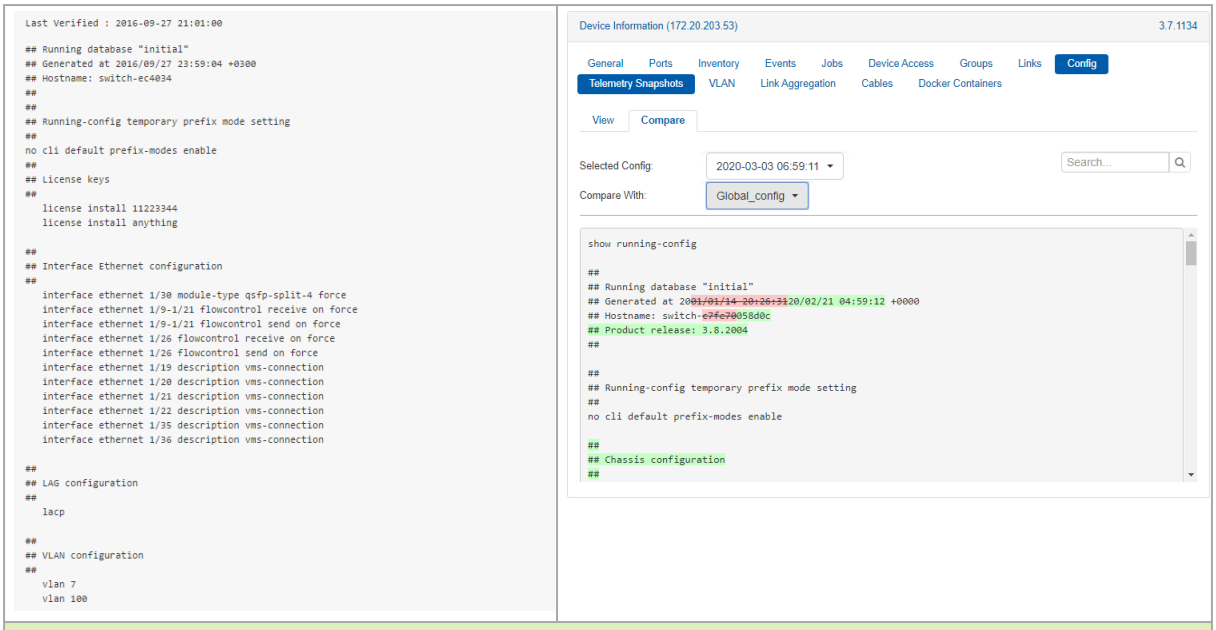


Figure 5 - Last Verified

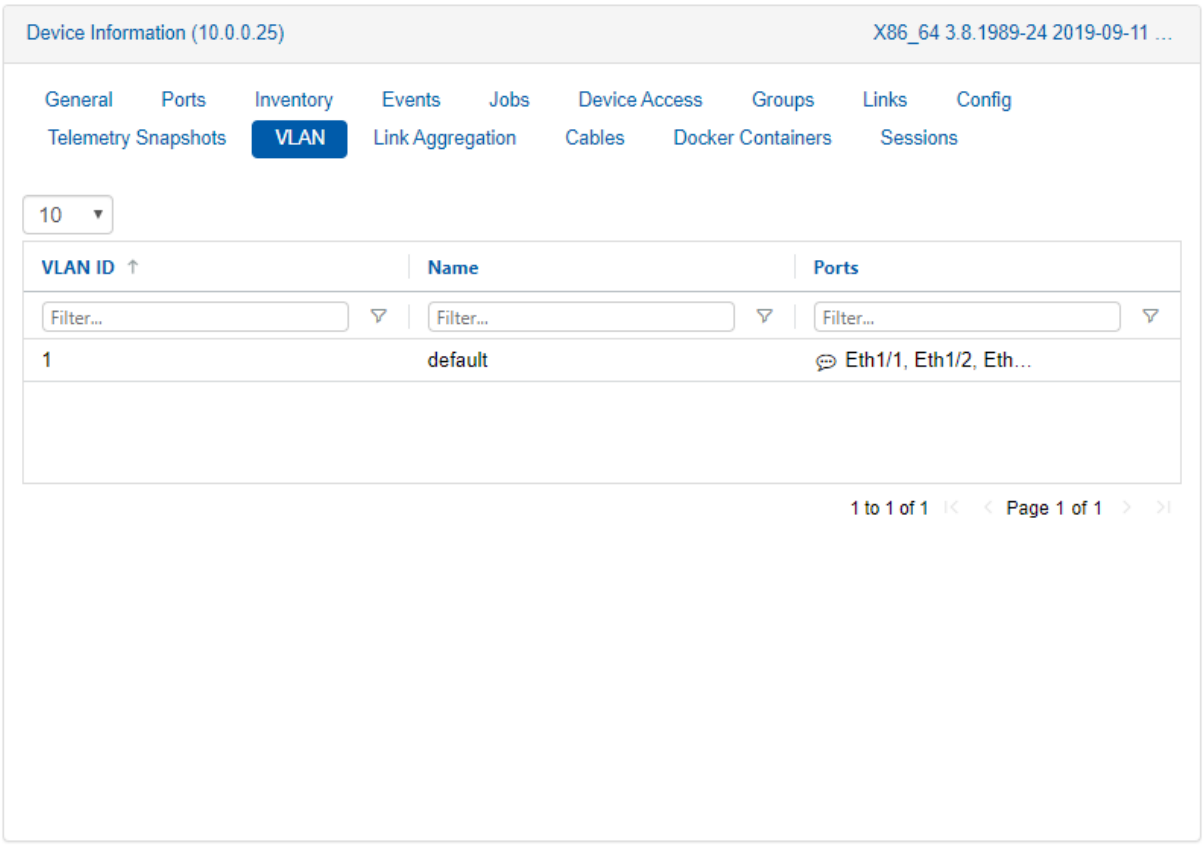
```
Last Verified : 2016-09-28 11:57:38
```

The “Last Verified” marks the last time the snapshot was known to be the current configuration on the device. The snapshot can be updated by clicking the "refresh" button, or when an auto-refresh takes place.

Snapshots cannot be deleted, but when removing a system, all its snapshots, including the edited snapshots (device specific configuration files) will be permanently removed as well.

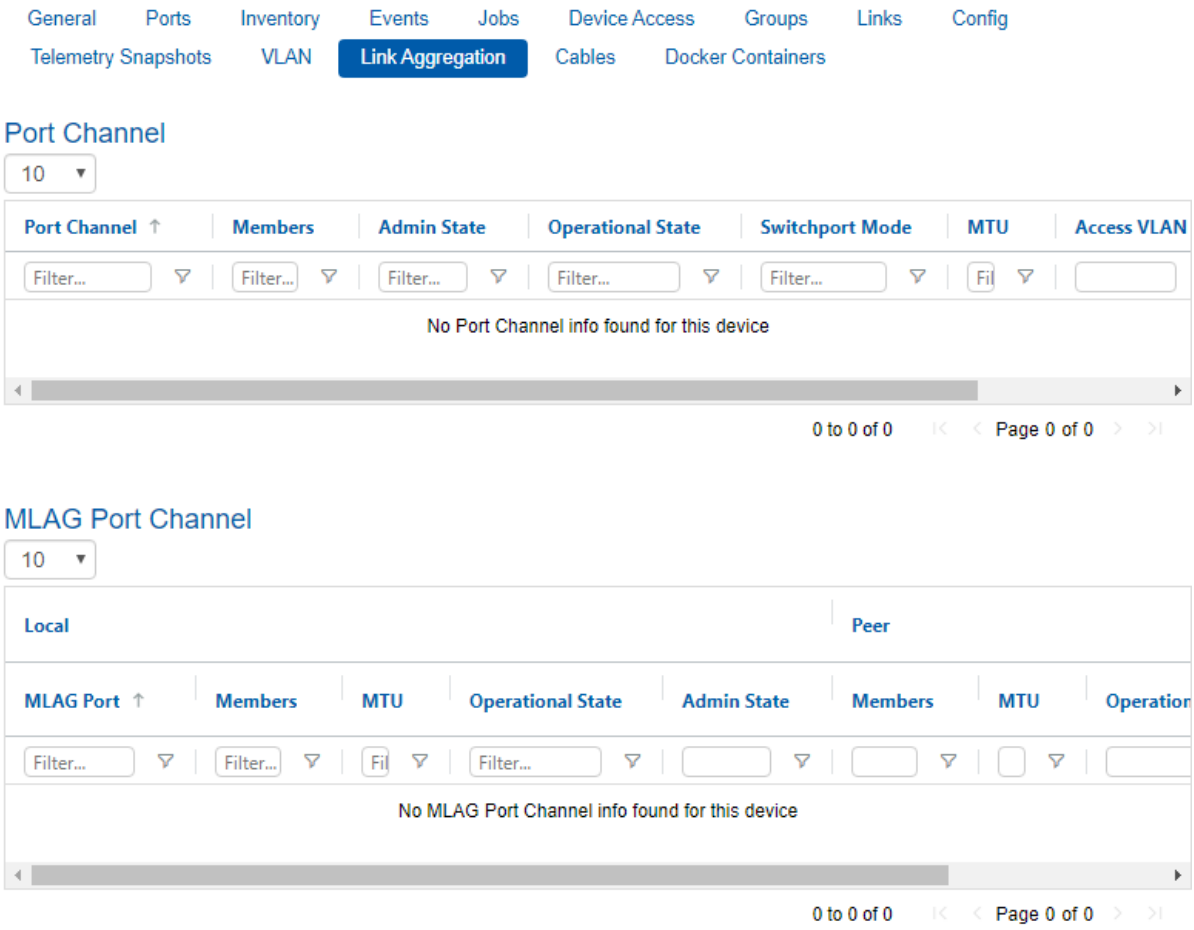
VLAN Tab

Lists all VLANs of which a certain device is a member.



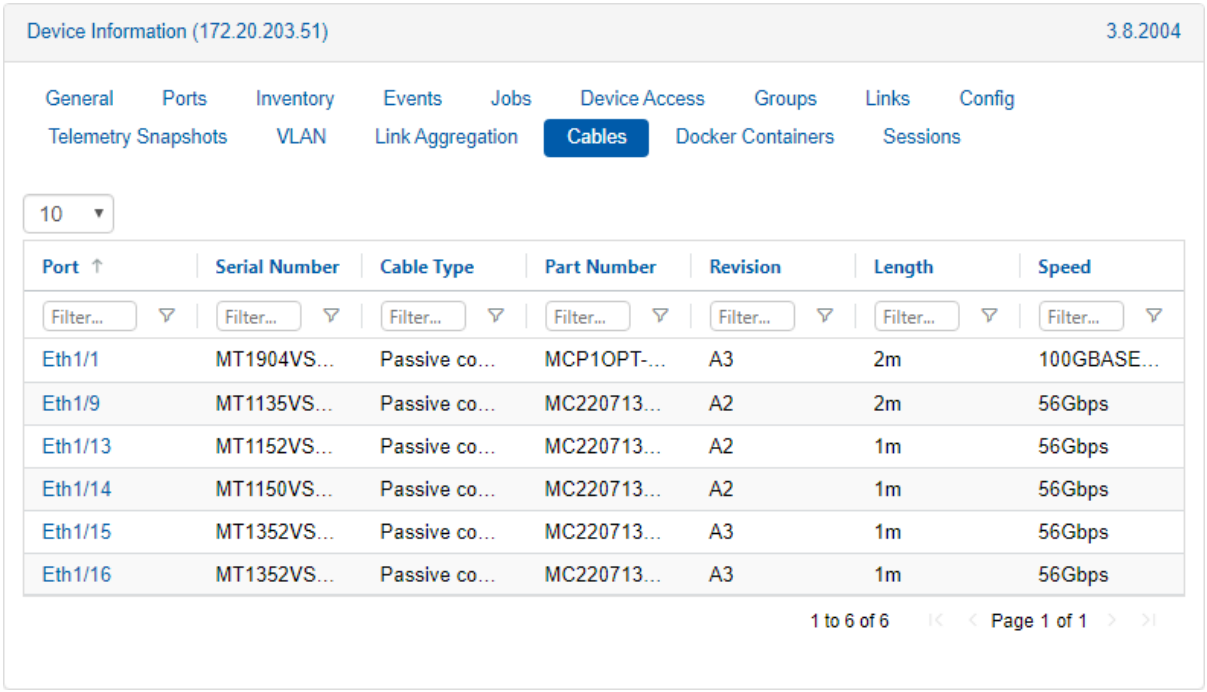
Link Aggregation Tab

The top table lists all LAG information of the selected device. The bottom table lists MLAG ports for the selected device and their corresponding ports in the peer device.



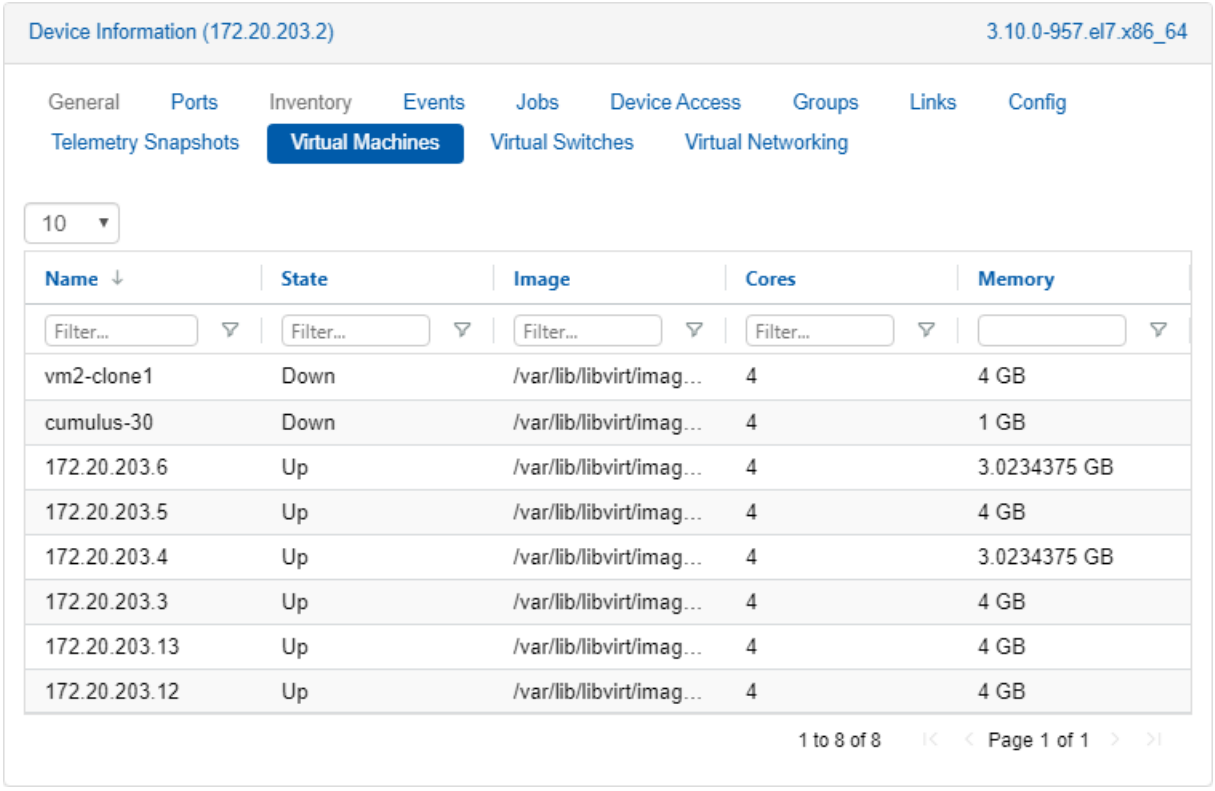
Cables Tab

Lists the cables connected to a Mellanox/Cumulus switch of communication status “OK”, and provides the following information about each cable: the port to which it is connected, its serial number, cable type, part number, revision, length, and speed.

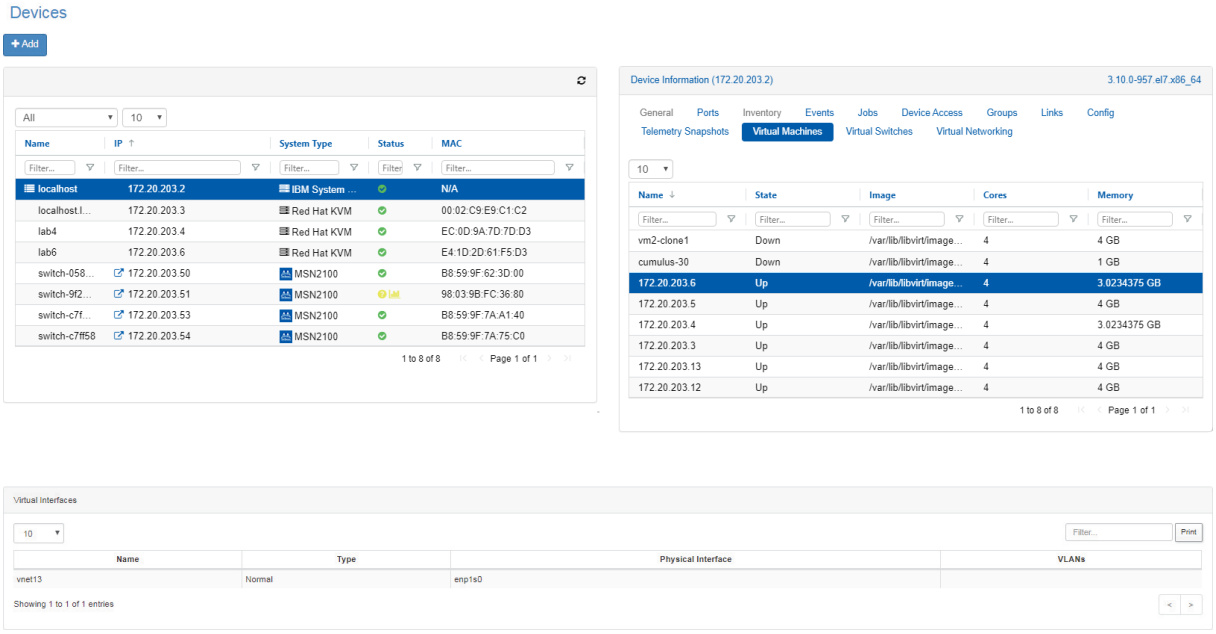


Virtual Machines Tab

This tab is available only for Linux KVM/Nutanix/ESXi hypervisors. When clicking a hypervisor machine, a list of all VMs that run on that machine will appear, and the following VM information will be provided: the VM name, its state, the image the VM runs, the number of cores the VM has, and the VM memory size.

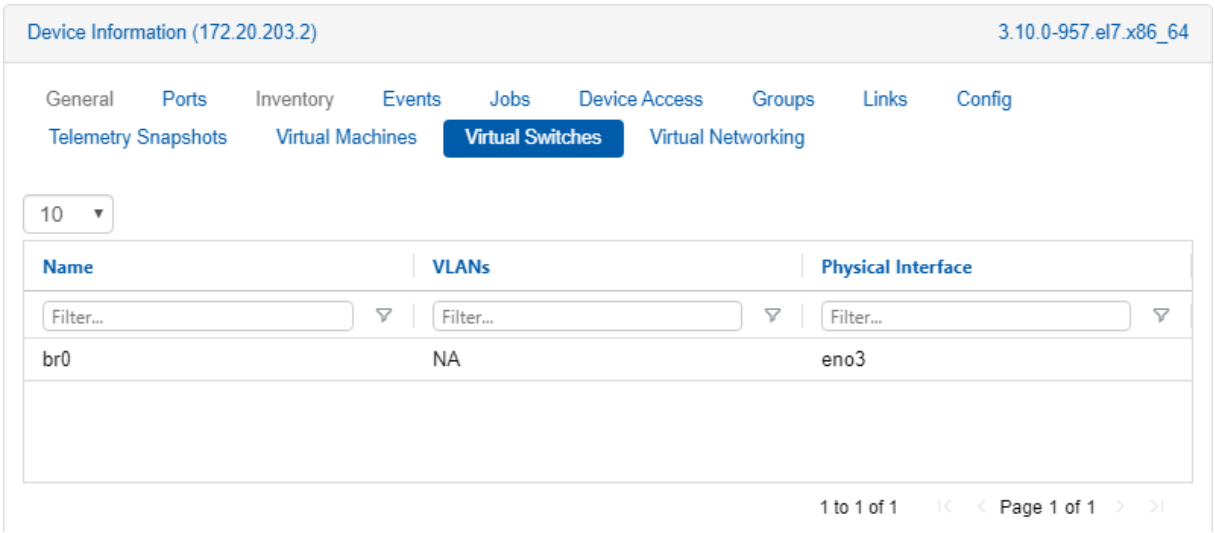


When clicking a VM, a list of its virtual interfaces will be displayed with information about its name, type (Normal/SR-IOV), physical ports and VLAN ID.



Virtual Switches Tab

This tab is available only for Linux KVM/ESXi hypervisors. When clicking on a hypervisor machine, a list of all Virtual Switches that run on that machine will appear, and the following Virtual Switches information will be provided: the virtual switch name, VLAN ID and physical interface.

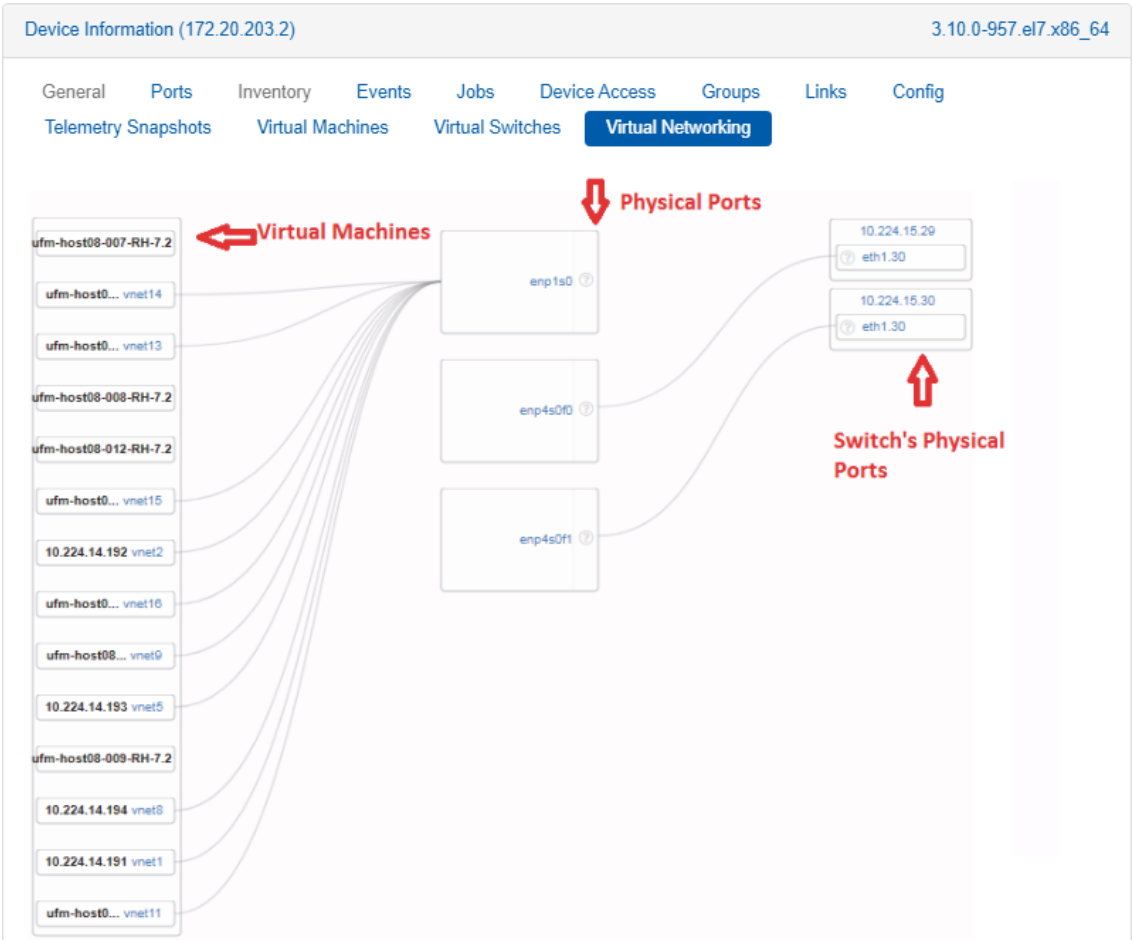


Virtual Networking Tab

This tab is available only for Linux KVM/Nutanix/ESXi hypervisors. When clicking on a hypervisor machine, a simplified host visualization network map will appear, and the following visualization information will be provided:

- The virtual machines in the selected hypervisor

- The physical ports that are connected to these VMs through virtual interfaces. These ports are blue colored, and when clicking them, you will be redirected to the Ports page, where port information will be provided in a table
- The switch ports that are connected to the physical ports - available only for Linux KVM hosts



Docker Containers Tab

Enables the user to manage, deploy, remove, start and stop the docker images and instances, and to discover current images and instances. This tab is available only for Spectrum Mellanox switch systems that possess docker capability, using Onyx OS or Cumulus OS (for the OS versions, please refer to the latest Release Notes document).

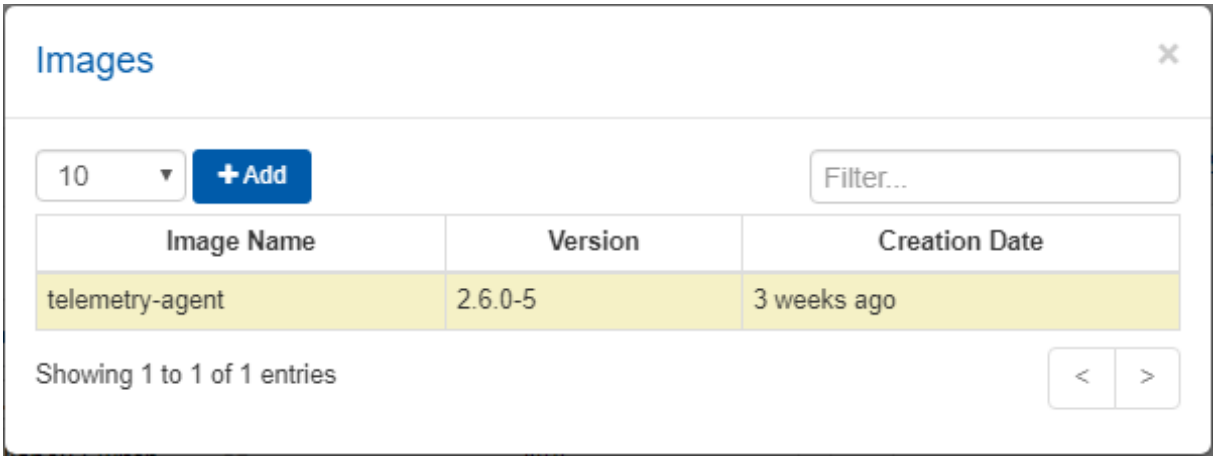
- When clicking on this tab, a table that contains the docker instances is displayed. The table includes the following attributes: Instance Name, Image Name, Version and Uptime, as well as multiple buttons for multiple functionalities, as described in the following table.

Docker Instances

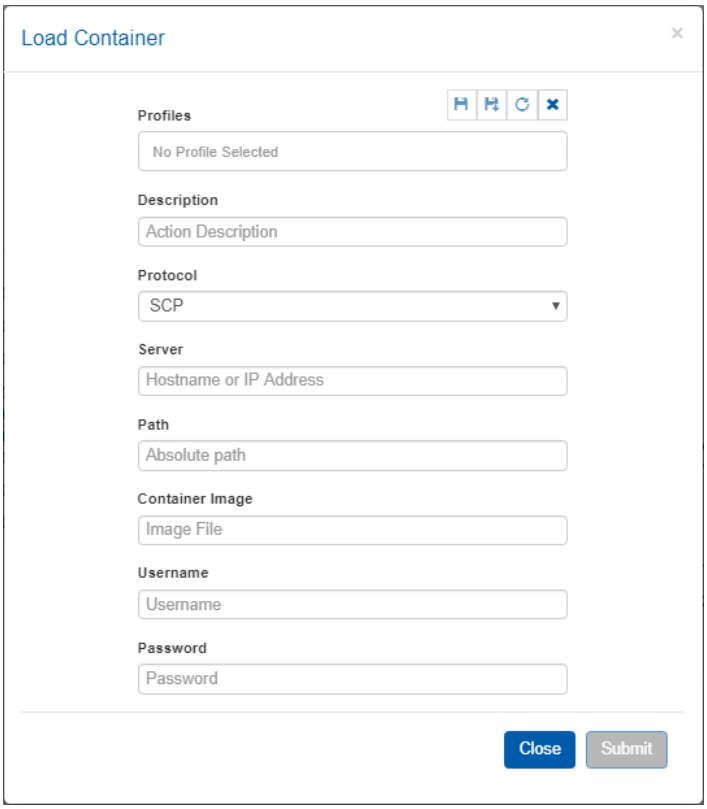
Icon	Name	Description
	Create Instance	Starts a new instance from a loaded docker image.

	Stop Instance	Stops a running instance from the switch.
Images	Images	• Shows a list of loaded images with the following attributes: Image Name, version, creation date • Adds a button that allows to load a new docker image. A right click on an image record offers the capability to remove the image.

When clicking on the "Image" button, a list of loaded images is displayed.

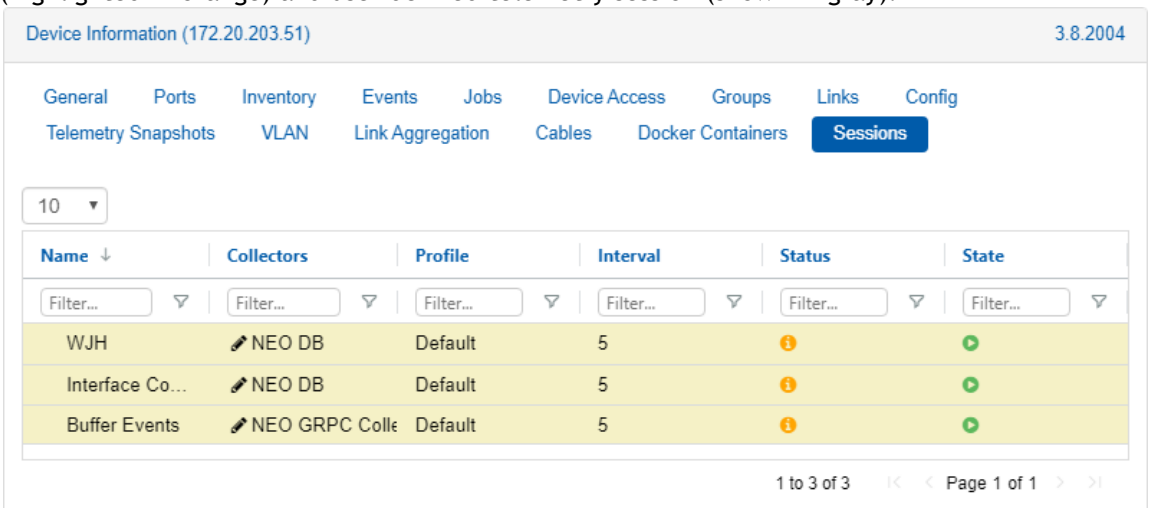


When clicking on the “Add” button, a new popup will allow to load a new docker image.



Sessions Tab

Lists all telemetry related sessions of the selected device, including default telemetry sessions (highlighted in orange) and user defined telemetry session (shown in gray).



Possible Device Actions

Right clicking on a device will show the actions that can be done on it, depending on the device type and capabilities:

Acknowledge

Acknowledges all events related to the selected device(s). This action will gray out the selected device events.

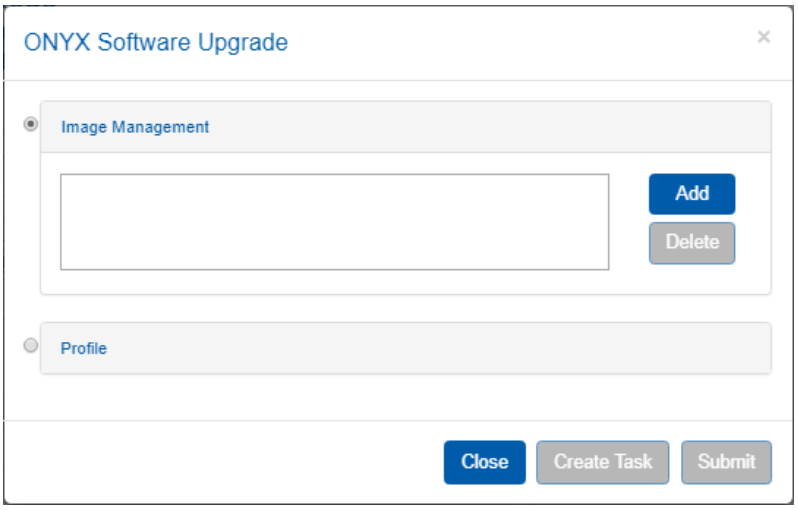
Reboot

Reboots the device. When choosing “Reboot”, a dialog box appears, requiring the users to confirm their choice or create a reboot task.

When reboot is started, the device’s status will turn into “Rebooting”, and an event named “Reboot Started” will be created. If the operation is completed successfully, a “Reboot Completed” event will be created. If the operation fails, a “Reboot Failed” event will be created.

Onyx Software Upgrade

Enables the user to upgrade the device's software. When choosing "Onyx Software Upgrade", a dialog box appears, requiring the users to fill in the relevant details in order to perform the upgrade.

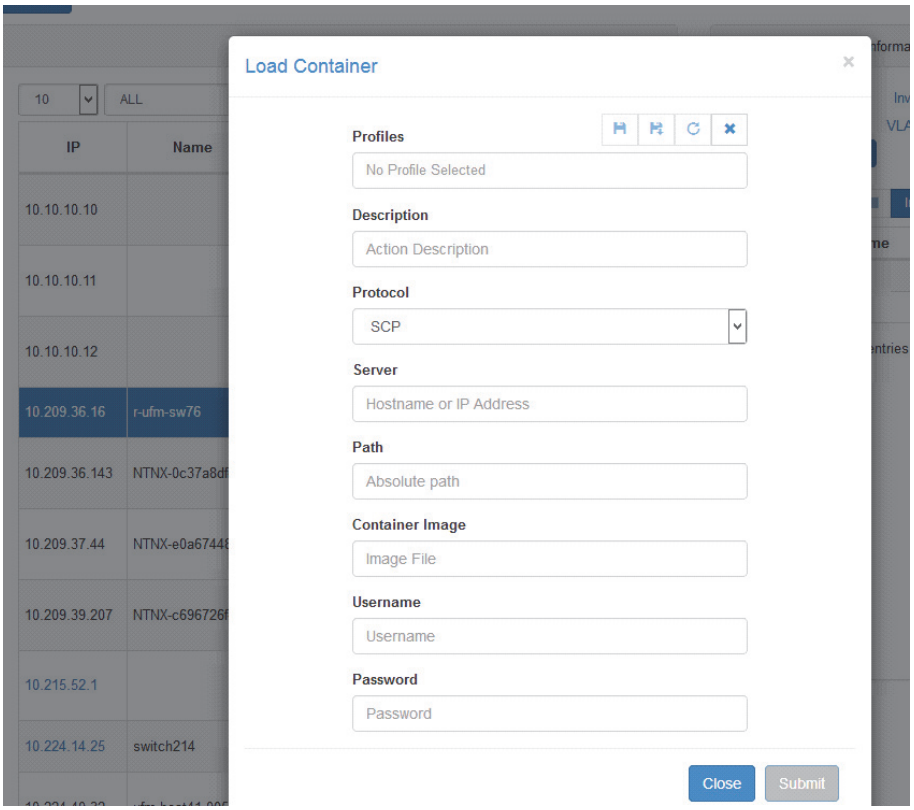


- "Create Task" directs the user to the Tasks page
- "Submit" directs the user to the Jobs page and starts the upgrade process immediately

After the Onyx Software Upgrade is completed successfully, the device's status will turn into "Pending Reboot", meaning that SW upgrade will only take place after rebooting the device.

Load Docker Image

Enables the user to load new docker image on the device's. When choosing "Docker Container", a dialog box appears, requiring the users to fill in the relevant details in order to load a docker image.



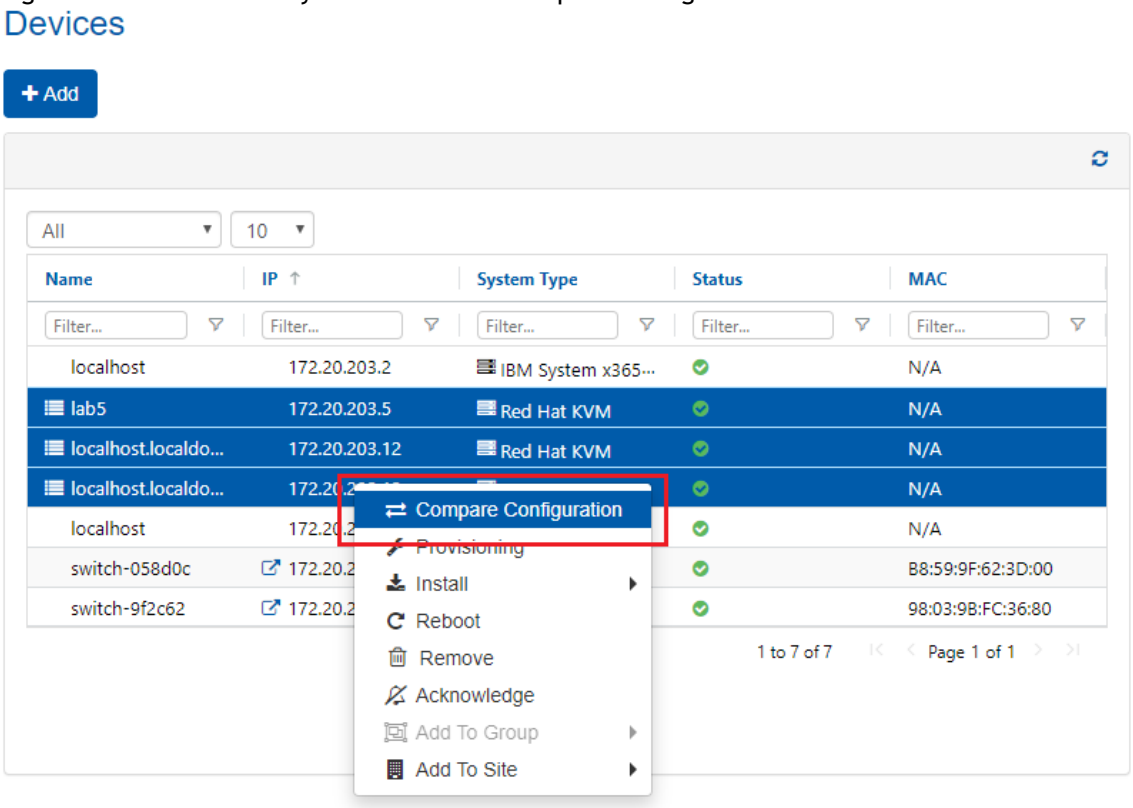
- “Submit” directs the user to the Jobs page, and starts the loading process immediately.

Compare Configuration

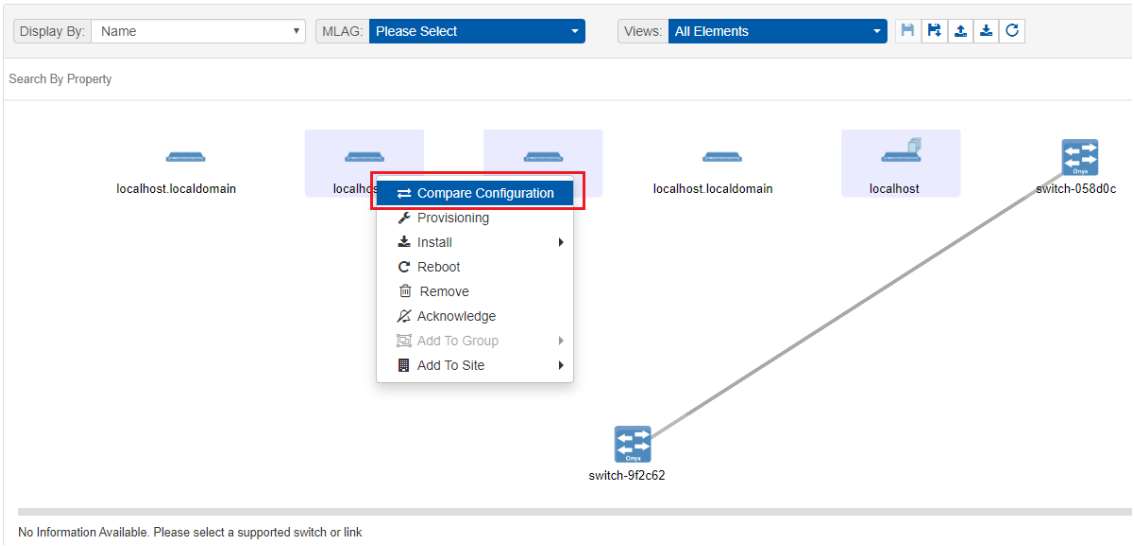
This enables users to compare the configuration of several switch systems through Mellanox NEO.

1. Mark at least two systems.

2. Right-click the selected systems and click Compare Configuration.

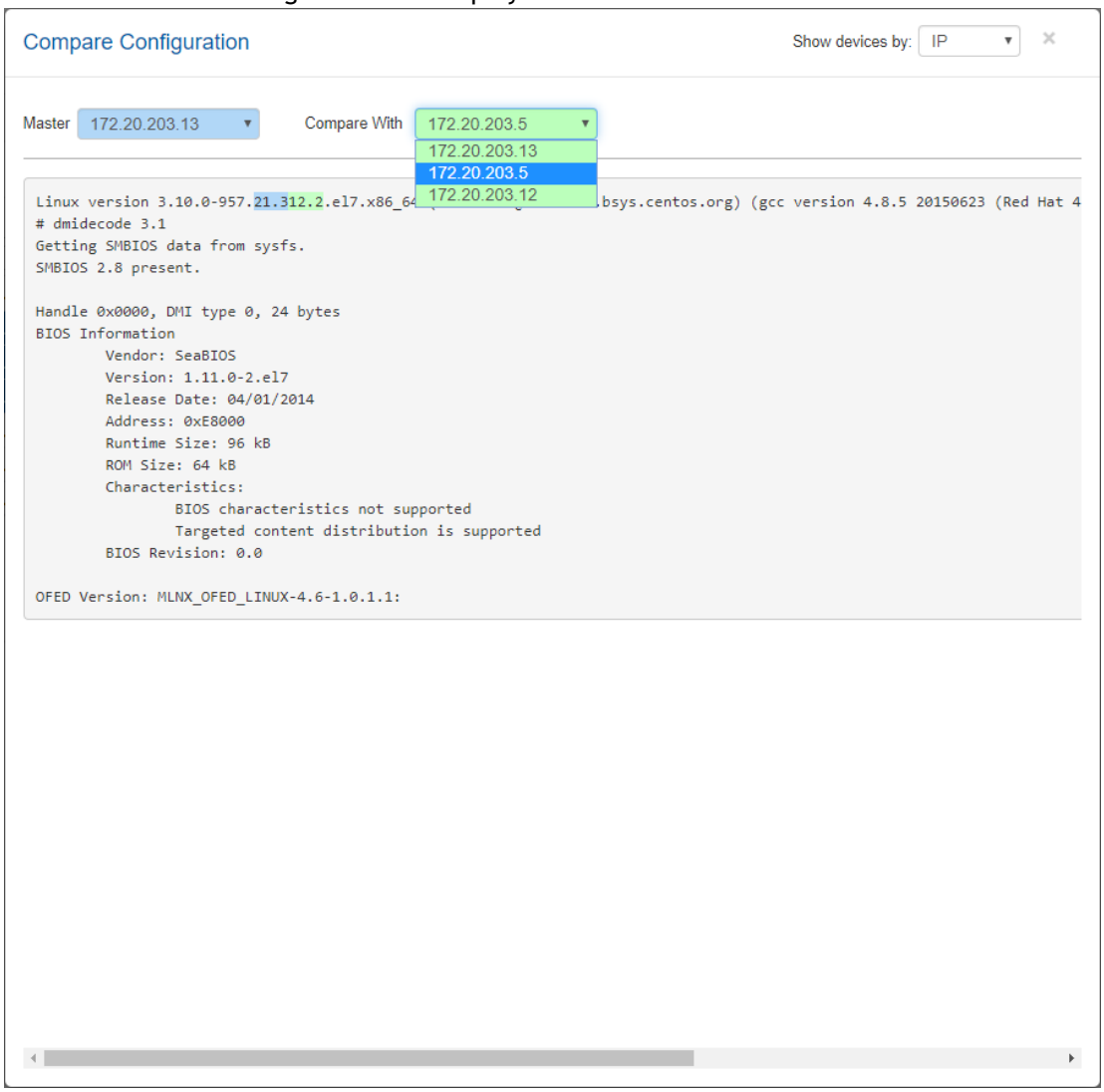


It is also possible to do this from the Network Map screen.



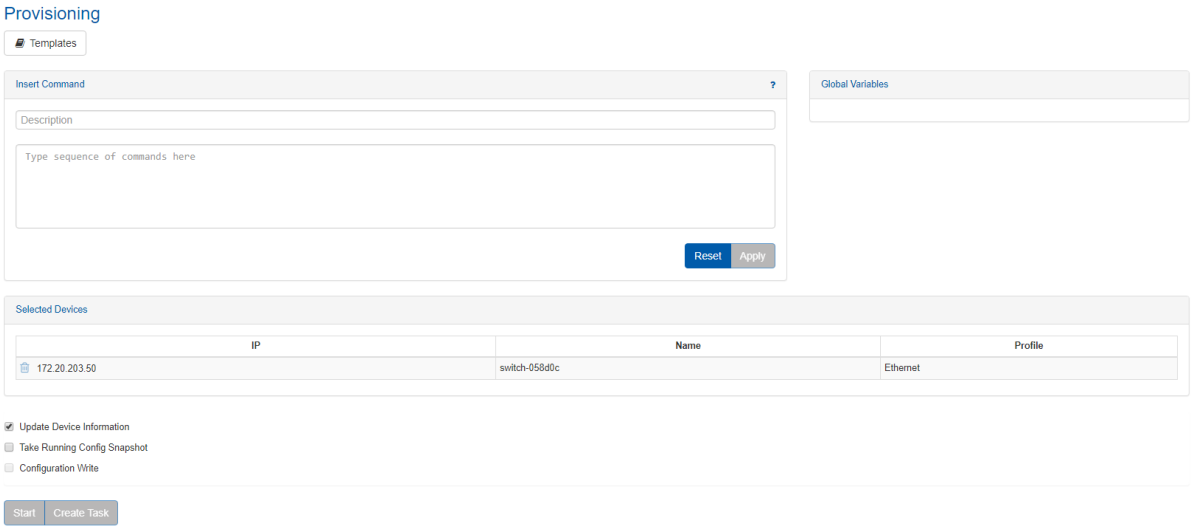
3. Select a master system.
4. Select a system to compare the master with.

5. The differences in configuration are displayed in color.



Provisioning

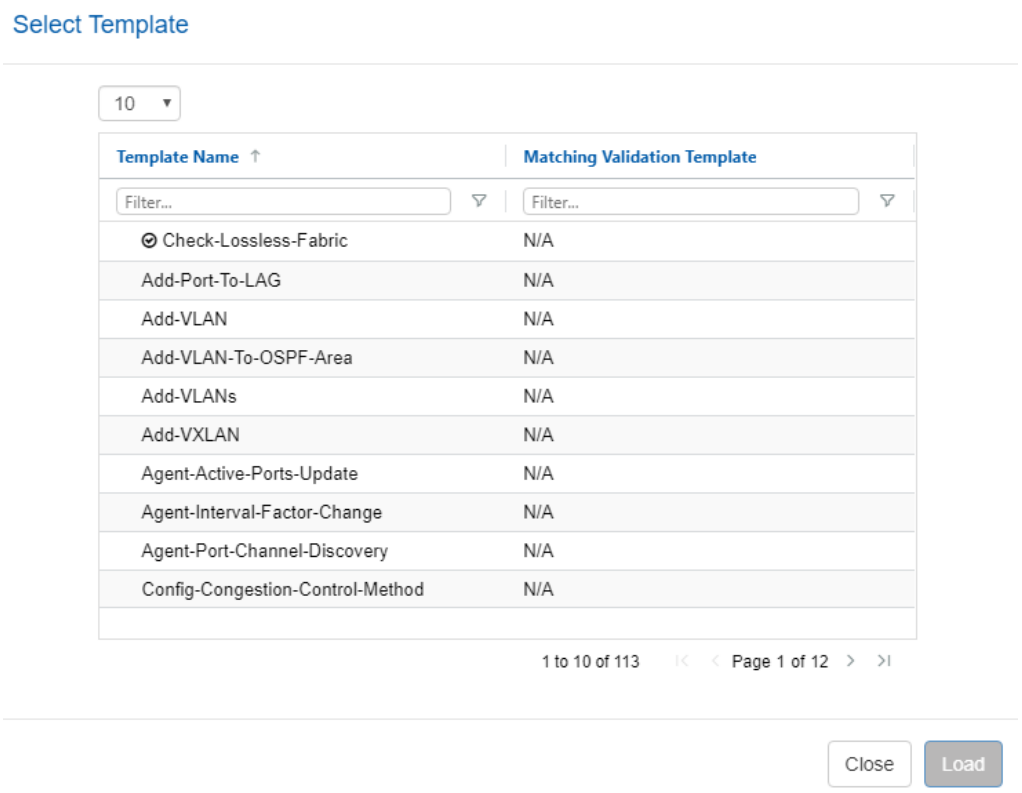
Provisioning enables the user to perform actions via the CLI player. The actions can be sent to one or more devices. Mellanox NEO provides provisioning templates with common CLI commands. Clicking on “Provisioning” opens a dialog box where the user is required to fill in the desired CLI commands and job description or select a predefined template.



- “Templates” will open a dialog with a list of the available provisioning templates.

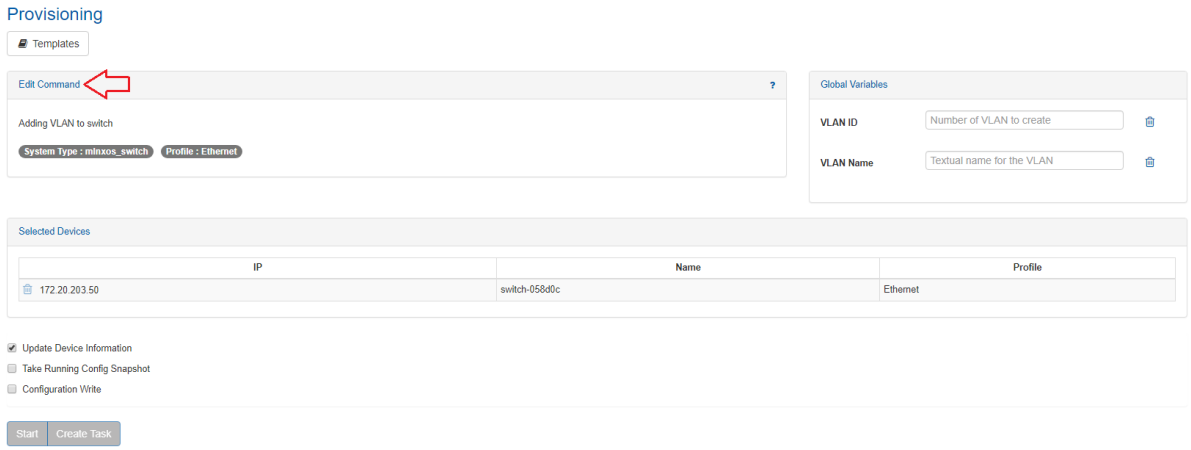
Typing string into the Filter box (at the top right corner) will filter the list.

The templates table contains two columns: the left column for a template name and the right column for a matching validation template.



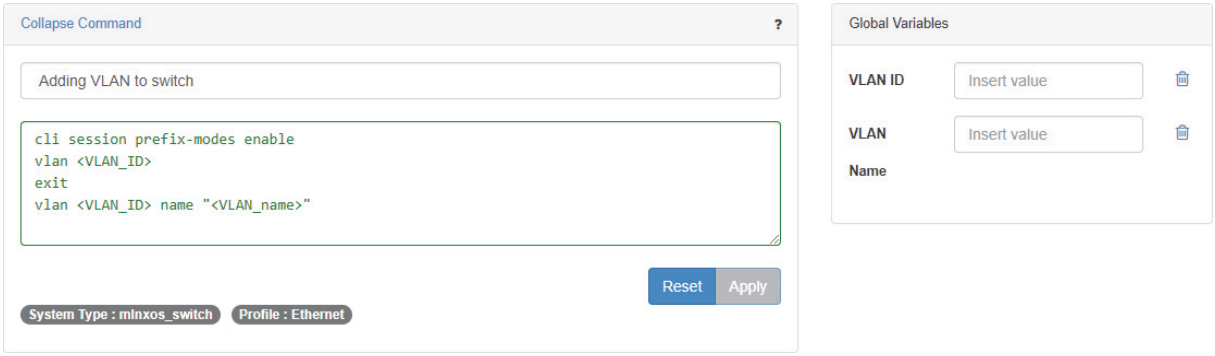
Template Type	Icon	Description
Provisioning	No Icon	Applies configuration or commands to the selected devices
Validation		Checks that a specific configuration still exists on the selected devices

If you wish to edit an existing template, click “Edit command” and edit it as desired.



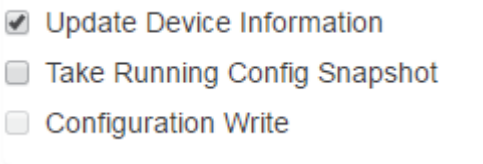
When adding invalid variables, a validation mechanism will notify you in case the variable’s value is invalid, and will instruct on the correct options in order to avoid the occurrence of a failed job (see image below). This mechanism also provides description of the variable used. For example:

- VLAN ID – number of VLANs to create
- VLAN Name – textual name of the VLAN



- “Create Task” directs the user to the Tasks page.
- “Start” directs the user to the Jobs page and starts the provisioning process immediately.

The three boxes on the bottom-left corner can be checked when loading a template that involves changes in the system configuration or when creating/editing a template.



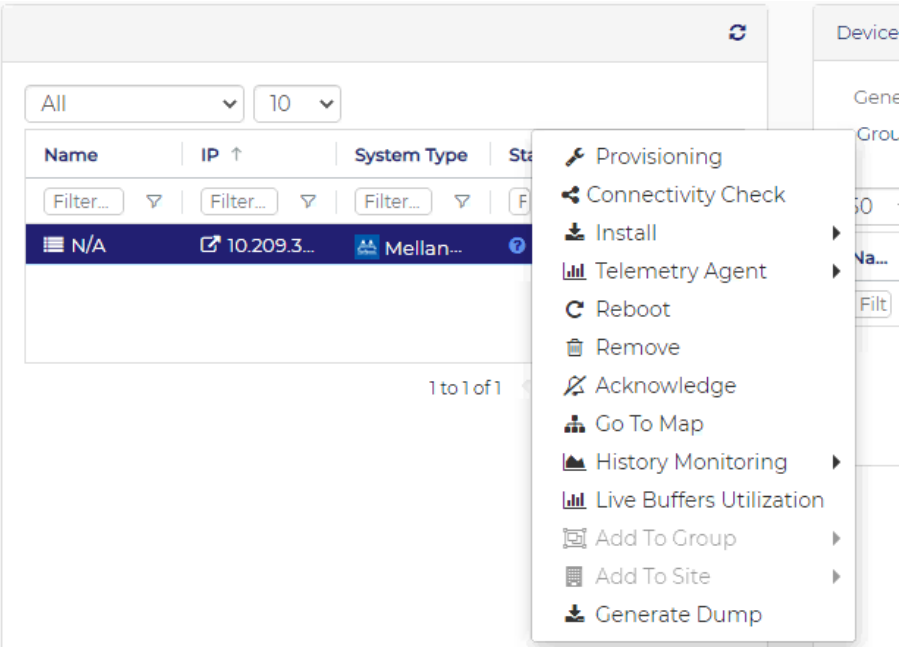
- Update Device Information – This box is checked by default. When checked, it refreshes NEO's device information after the provisioning execution. Otherwise, the devices are refreshed every 15 minutes by the Device Manager. The refresh operation might take up to one minute.
- Take Running Config Snapshot – When checked, a snapshot of each device's configuration will be taken before the provisioning execution.

- Configuration Write – This checkbox is enabled only when applying pre-defined templates. When checked, it sends the 'configuration write' command after the provisioning execution. This command makes all changes persistent, which means that they will still be valid after switch reboot.

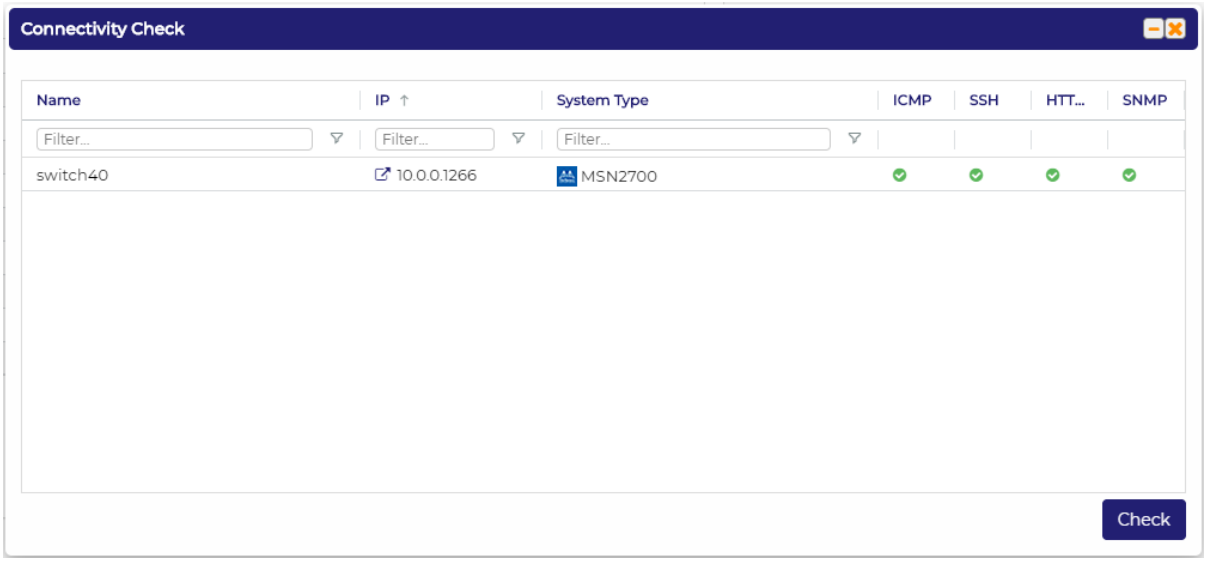
For further information on the provisioning of devices, please refer to "Providers".

Connectivity Check

Connectivity Check allows the user to verify their device's connectivity across multiple communication protocols (i.e. ICMP, SSH, HTTP, and SNMP).

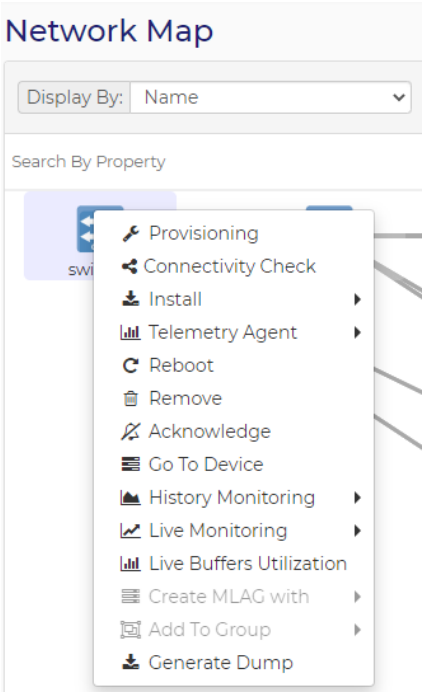


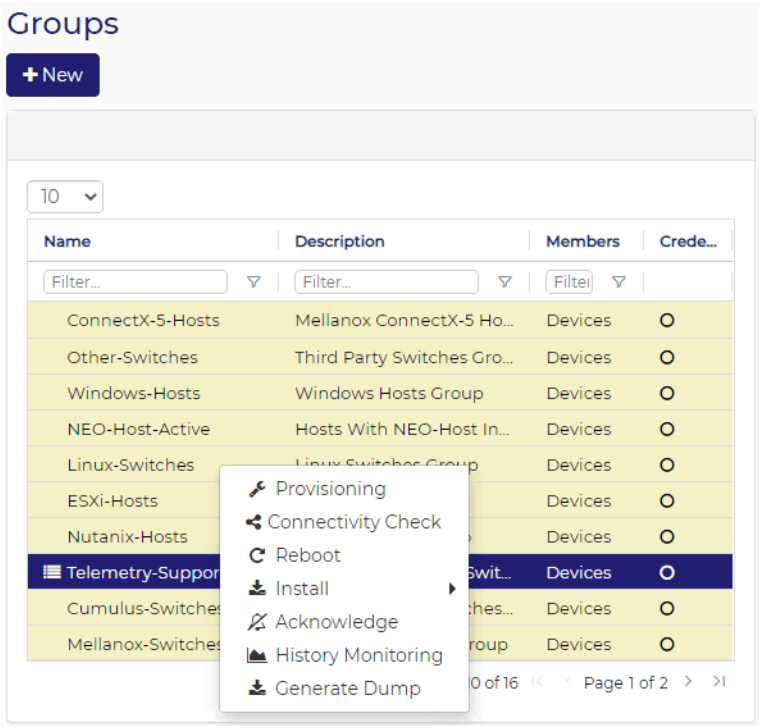
Clicking "Connectivity Check" opens up a window showing the connectivity status of your device over the supported protocols.



Hovering over the status icons provides a description of the status indicated by that icon.

This can also be done from the Network Map view and the Managed Elements > Groups window.



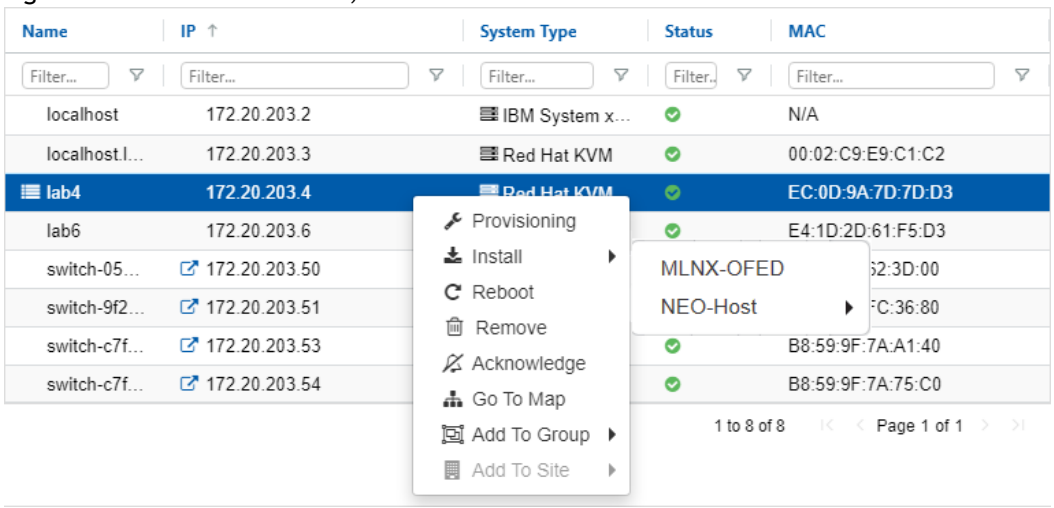


Install

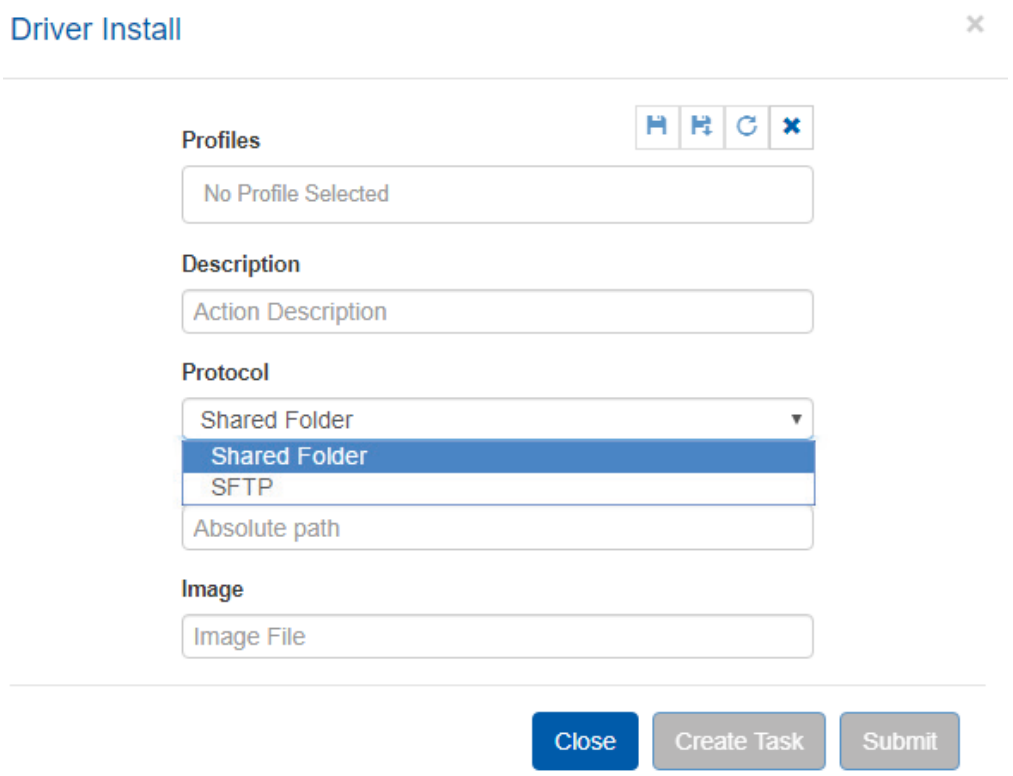
Mellanox Driver

Allows users to perform MLNX_OFED/MLNX_EN driver installation or upgrade on hosts. Follow the steps below to perform a driver install/upgrade.

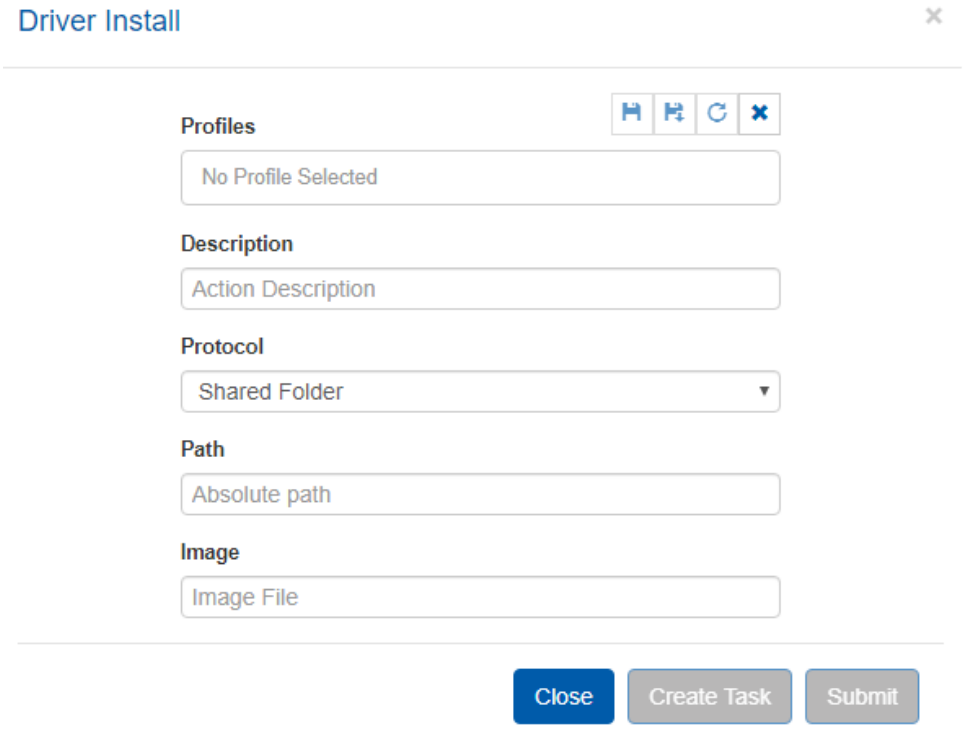
1. Right-click one or more hosts, and choose “Install” → ”MLNX-OFED”



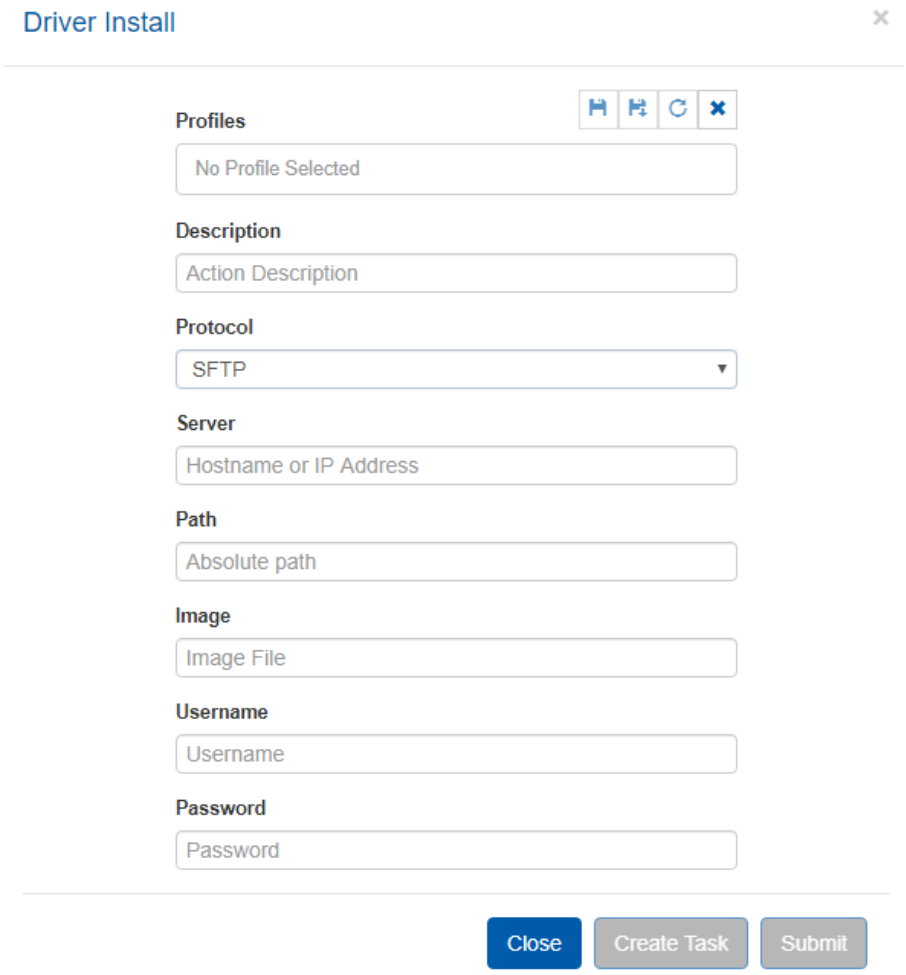
2. Fill out the required data. There are two ways to do so:
   a. Choose a pre-defined profile, in which case all data will automatically be filled out. If a profile is selected, it can be edited in the same dialog window. Choosing one of these icons  will enable saving the changes and overwriting the profile selected, saving and creating a new profile, or reloading and reverting to the initial data. For more information on the profiles, see “Image Profiles Settings”.
   b. Skip “Profiles” and manually fill in the required fields. If no profile is selected, provide description, then choose the desired protocol in the dialog window:



i. For the Shared Folder protocol – provide the path and image name. The image should be located in a shared folder that can be accessed by the hosts.

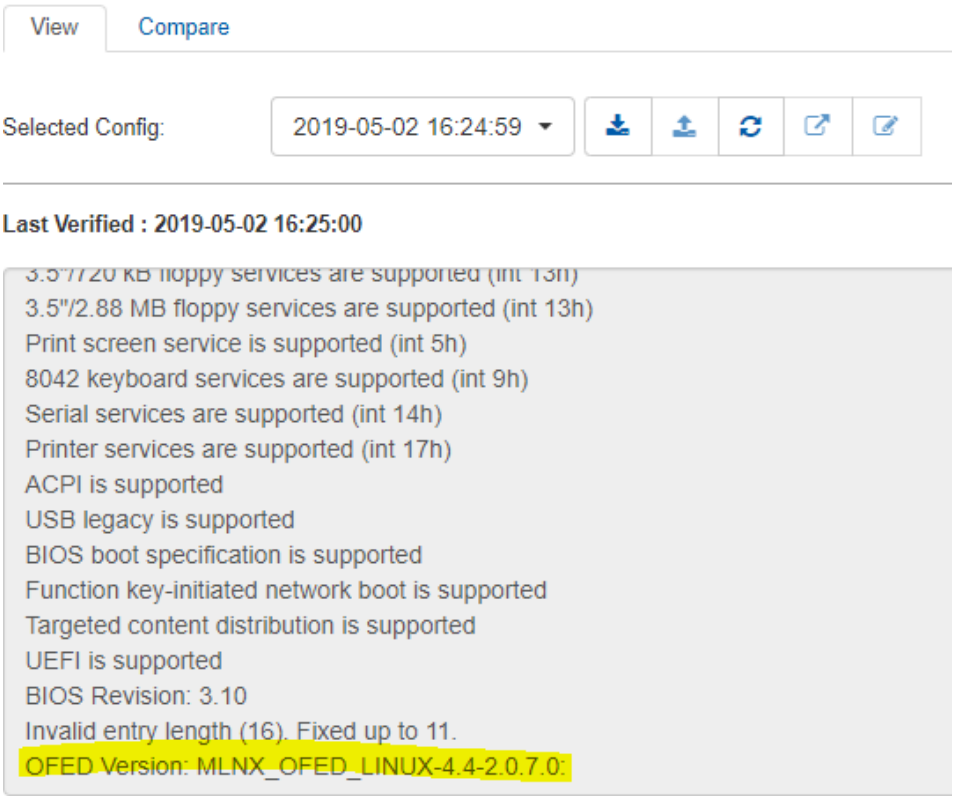


ii. For the SFTP server protocol - provide the credentials, path and image name. The image should be located in an SFTP server that can be accessed by the NEO machine.



iii. Clicking “Create Task” will generate a driver install task that can be executed at any time. Clicking “Submit” will perform an immediate driver installation. Note that the procedure might last for several minutes.

In order to view the current driver version of the hosts, choose the host or any of the hosts for which you installed the driver under “Devices”, and refresh the Config tab. You will be able to see the driver version as part of the configuration content.

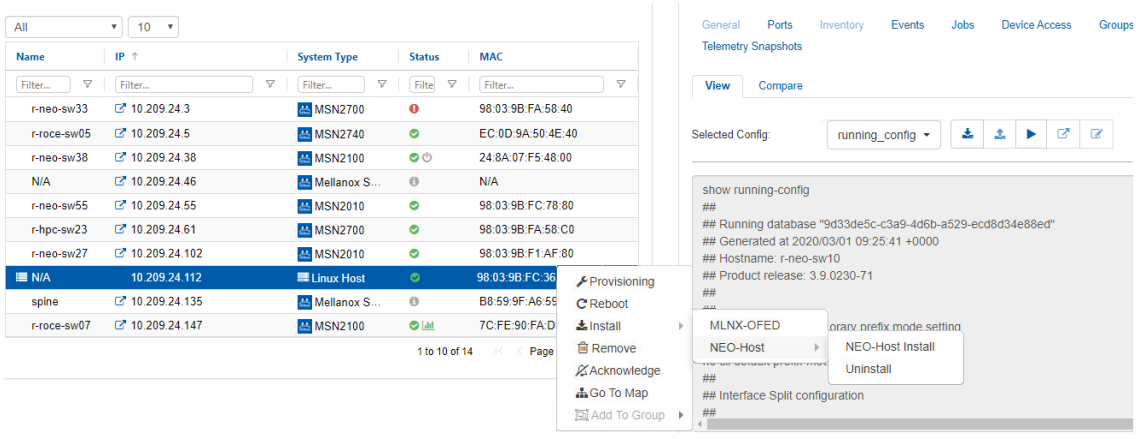


NEO Host

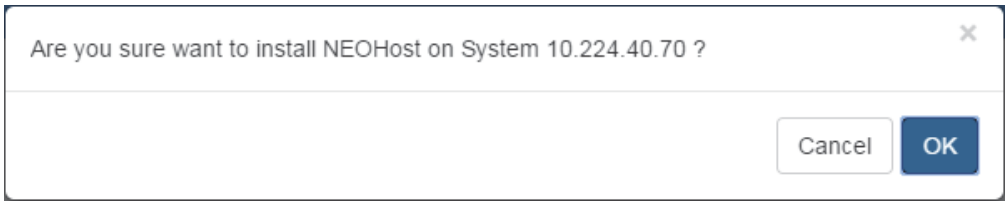
Allows users to install/uninstall NEO-Host on a Linux machine.

Follow the steps below to perform a NEO-Host install/uninstall/upgrade.

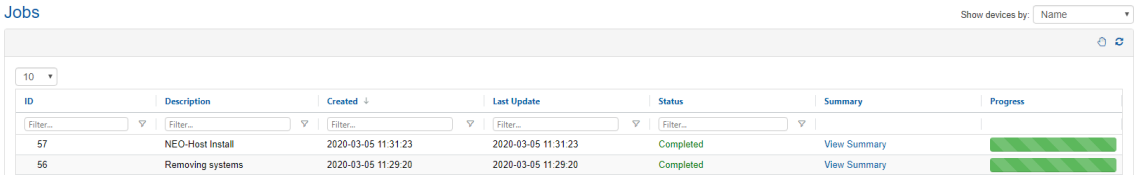
1. Right-click one or more hosts, and choose “Install--> NEO Host --> Install/Upgrade/Uninstall”.



2. Confirm the install/upgrade/uninstall by clicking “Ok”.



A job will be created:



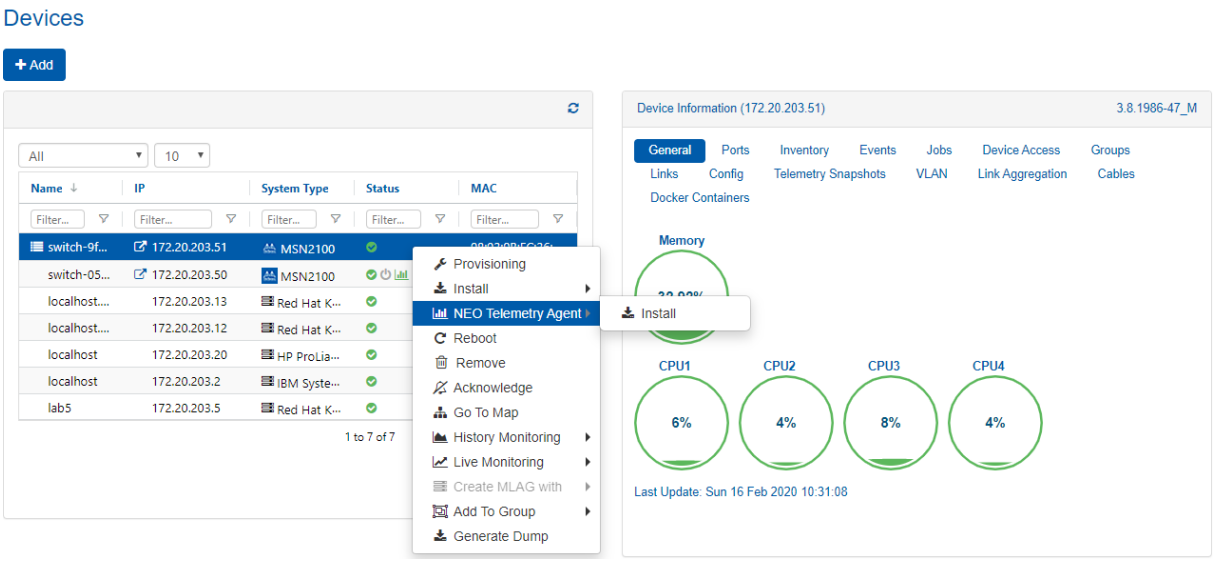
NEO Telemetry Agent

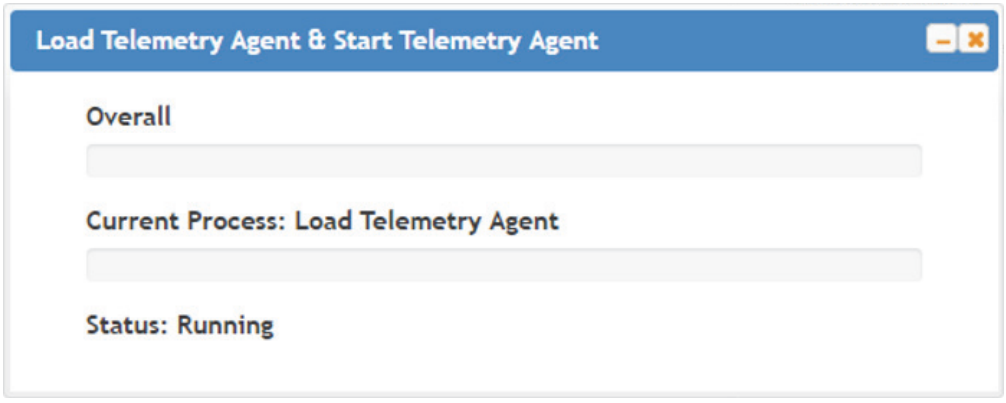
Allows users to install NEO Telemetry Agent on switches that supports Docker capability.

> ⚠ Before deploying the Telemetry Agent on a Cumulus switch, make sure to install docker on the switch and that it is running.

> ⚠ The switch's clock must be synchronized with NEO's clock. A lack of synchronization may prevent certain telemetry features from working properly.

To perform a NEO Telemetry Agent installation, right-click one or more switches and navigate to "NEO Telemetry Agent → Install".





The agent will be installed on the switch, and the session will be started.

For further information, please refer to "Activating Switch Telemetry Using the NEO Telemetry Agent".

History Monitoring

Provides a report of the device attributes values history. For further information on the history monitoring of devices, please refer to "Providers".

Live Monitoring

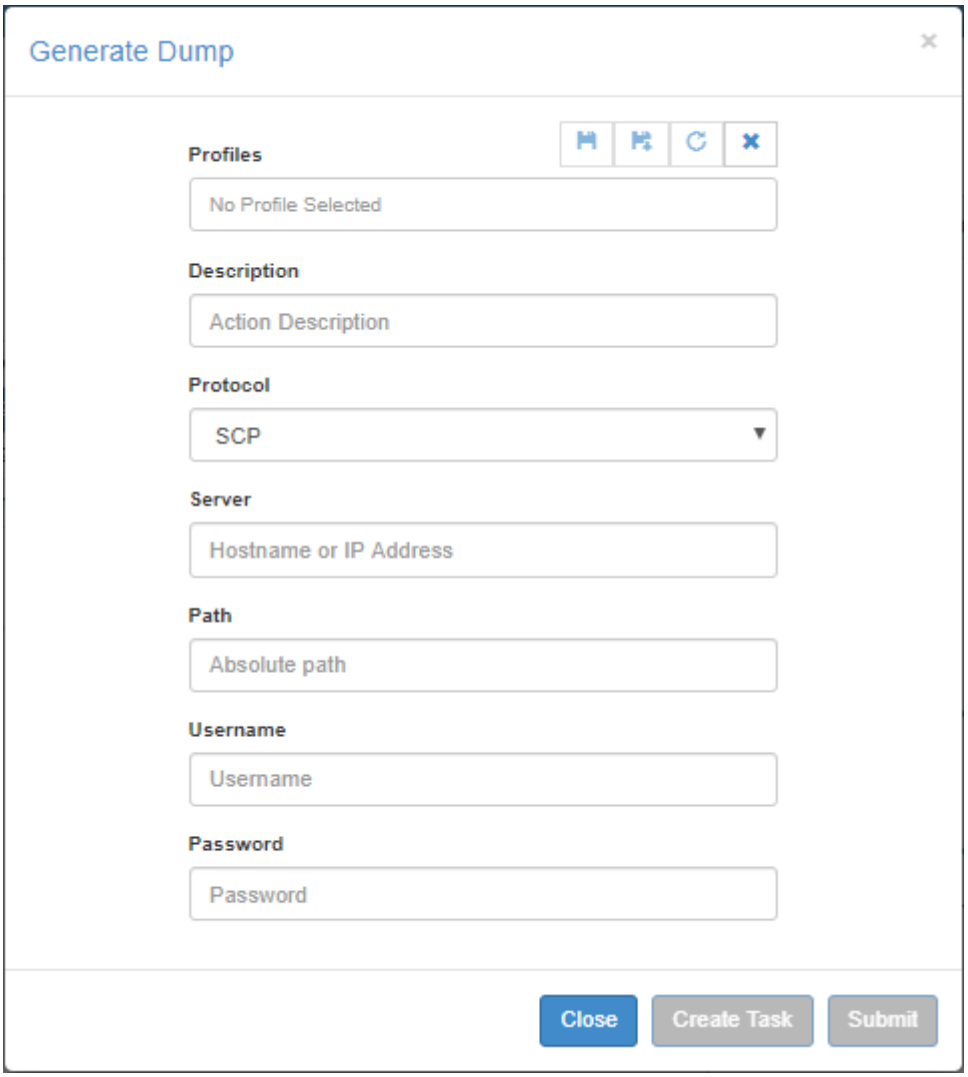
Provides a live report of the device attributes values.

Create MLAG

Allows users to configure an MLAG with devices that have at least two links to this device. This action is applicable for Mellanox Ethernet switches only.

Generate Dump

Allows the user to generate a debug dump file for the device and upload it to a remote folder. Available for Onyx switch systems. When choosing "Generate Dump", a dialog box appears, requiring the users to fill in the relevant details in order to perform the dump generation.



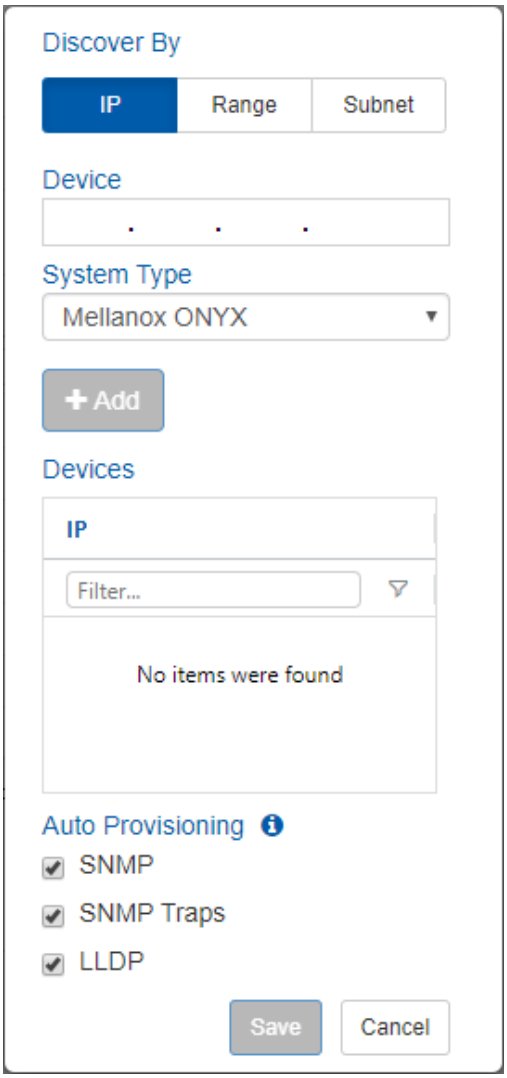
- “Create Task” directs the user to the Tasks page
- “Submit” directs the user to the Jobs page and starts the dump generation and upload process immediately.

Adding Devices

To add a device click the 

button above the Devices Information list. You can add a device either by manually typing its IP address, or by scanning a range or a subnet of IP addresses.

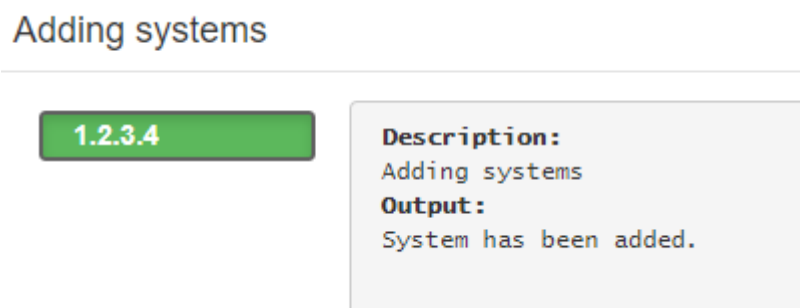
Discover by IP



1. Insert the Device IP address, select its type, and click the 

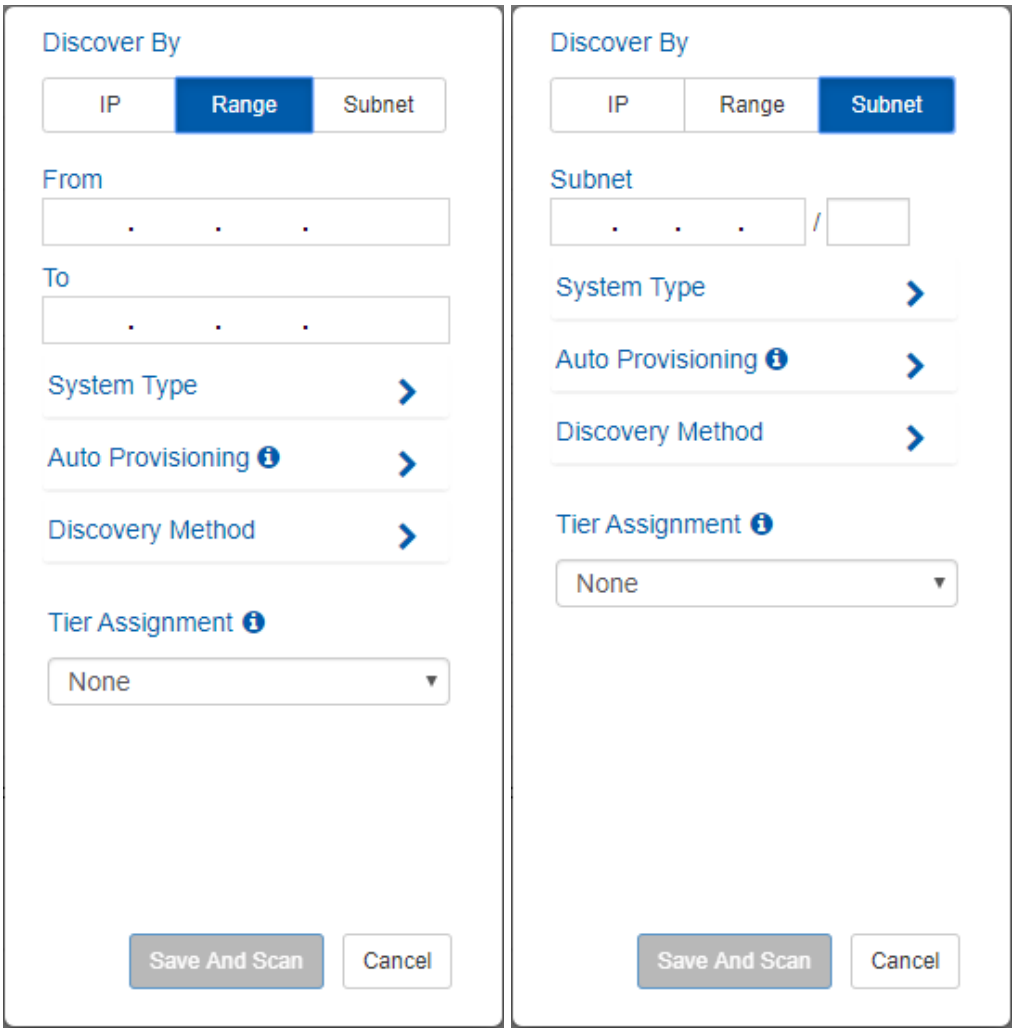
button to add the device. Repeat the action for all devices you wish to add.
2. Once all devices are added, click Submit.

A window with the devices that have been added will be displayed. Clicking one of the devices will show the system addition status.



Each newly added device under this window will automatically appear in the Allowed list under Settings → Discovery, in a grayed-out row.

Discover by Range/Subnet



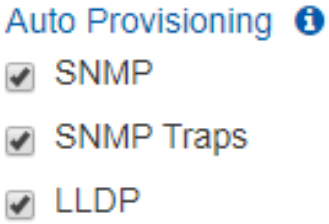
Insert the IP range or subnet to scan for devices, and select the device types to discover, and the discovery methods to use.

Discovery method options:

- LLDP – when checked, NEO discovers all devices found within the range specified and on which LLDP is enabled
- Multicast – when checked, NEO discovers all Mellanox Onyx switches found within the range specified using multicast

You can optionally specify a tier for the devices discovered by the scan. This tier is used to present the network map in a hierarchical structure.

Auto-Provisioning



Whether you added the devices by specifying IP or by scanning, the following provisioning actions are enabled by default on all added devices:

- SNMP – configure the device to listen and respond to SNMP requests (SNMP version 2c)

  > ⚠ Supported for Cumulus switches.

- SNMP Traps – configure device to send SNMP traps to NEO. The SNMP trap version (2c/3) is decided by the Onyx global SNMP credentials used.

  > ⚠ Supported for Onyx switches.

- LLDP – configure device to enable LLDP protocol

  > ⚠ Supported for Onyx and Cumulus switches.

Removing Devices

To remove a device, right-click it, and click “Remove”. A job will be created automatically.

> ⚠ In some cases the "Remove" operation is blocked because the device is used or is running Telemetry Agent. If so, remove the agent or any other usage of the device and retry removing the device.

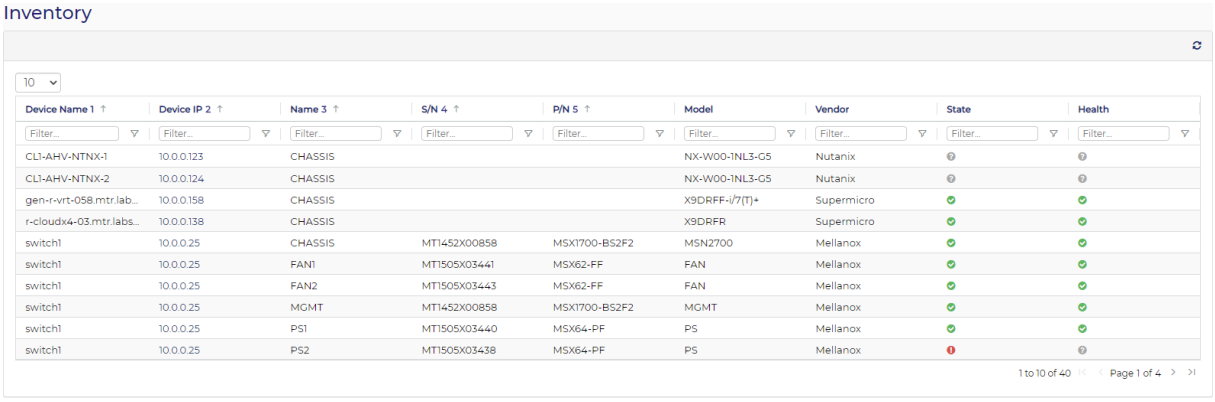
> ⚠ Each removed device is automatically dropped from the “Allowed” list under Settings → Discovery.

> ⚠ When removing a device from NEO, it is automatically moved to the blacklist in the Discovery settings. These devices are not added automatically to NEO when scanning for new devices.

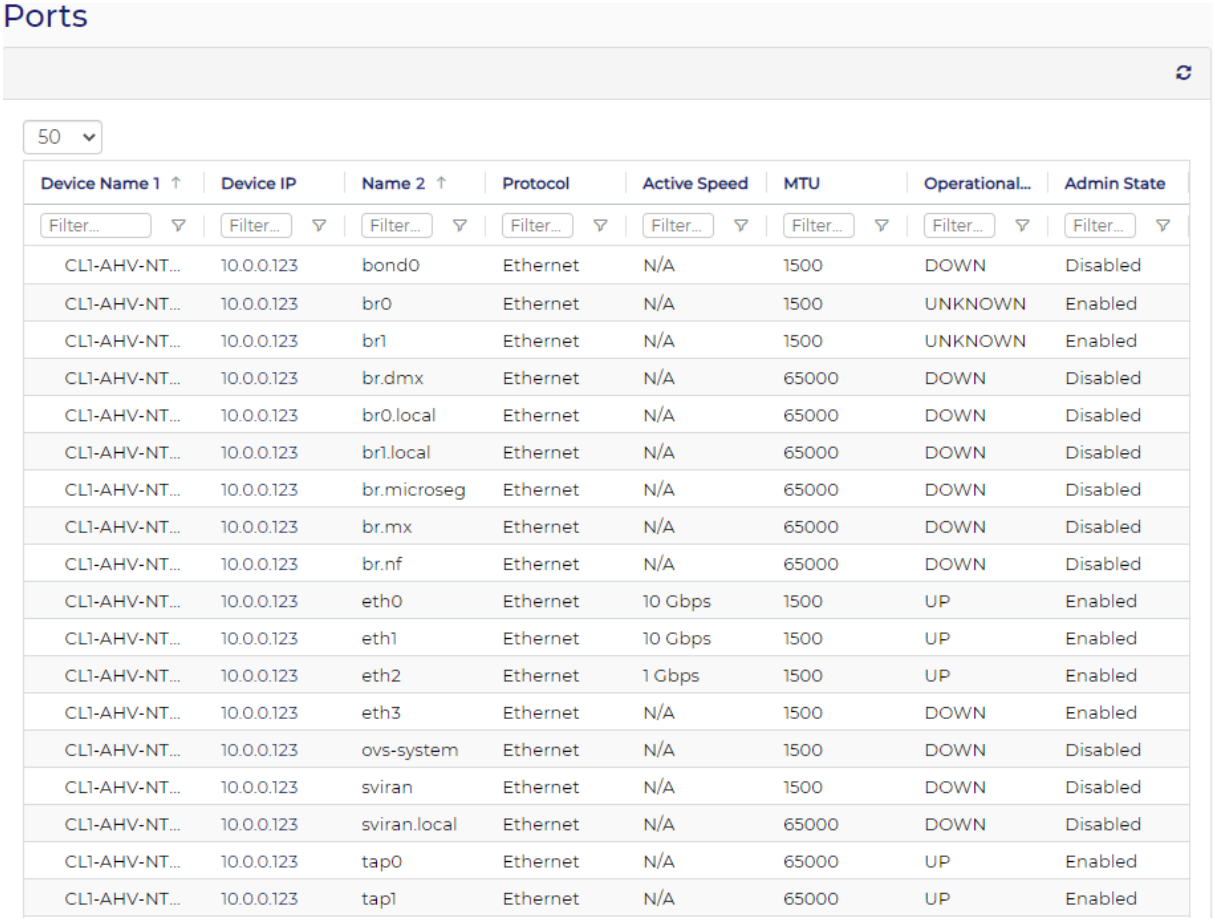
> ⚠ NEO removes itself as an SNMP trap listener from Onyx switches when they are removed.

Inventory

Mellanox Inventory page provides a detailed presentation of each device part (such as CPU and FAN), part number, SKU and serial number.



Ports



Ports Information

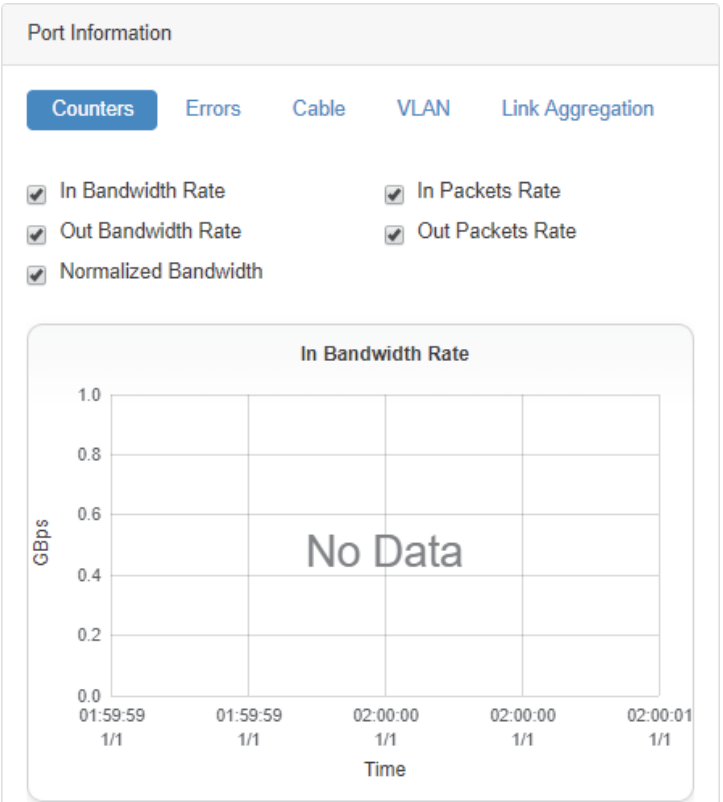
The Ports page provides the following details on each device port..

Device Port Details

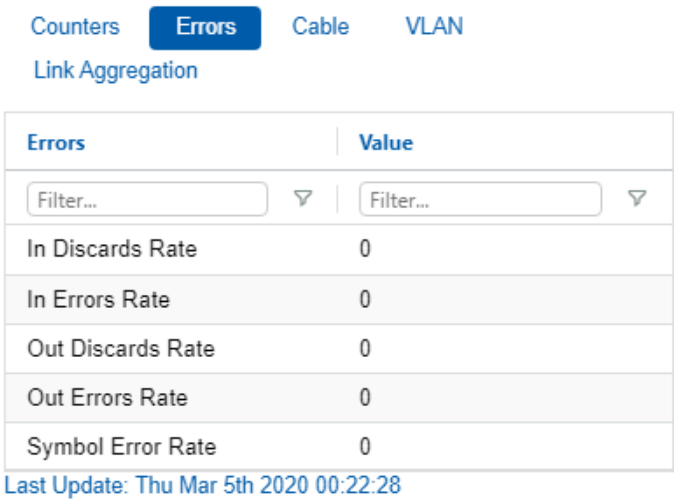
Details	Description
Device	The device name
Name	The port name
Protocol	Shows the port's used protocol. It can be either Ethernet or InfiniBand
Active speed (Mbps)	The actual speed in which the port operates
MTU (Maximum Trans- mission Unit)	The standard MTU is 576, however ISPs often suggest using 1500
Operational State	Up/Down
Admin State	Enabled/ Disabled

Once a port is selected, a window with the available Port Information will be displayed:

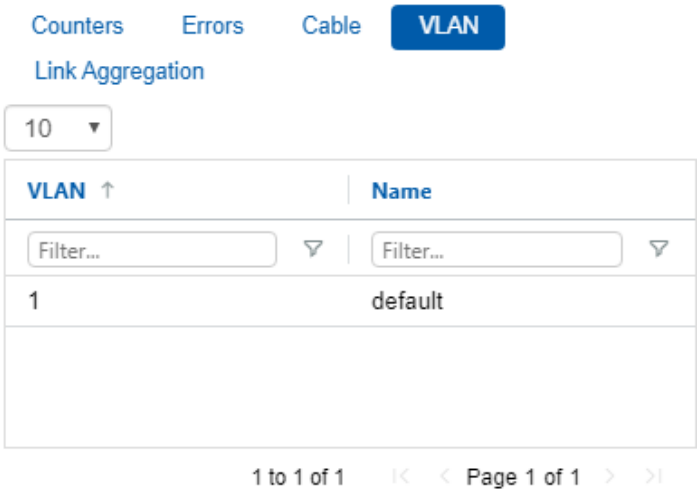
- Counters: The user can choose to view the following counters:
- In Octets Rate – Received Data Rate in MBps
- Out Octets Rate –Transmit Data Rate in MBps
- In Packet Rate
- Out Packet Rate
- Normalized Bandwidth – Percentage of Bandwidth utilization in %



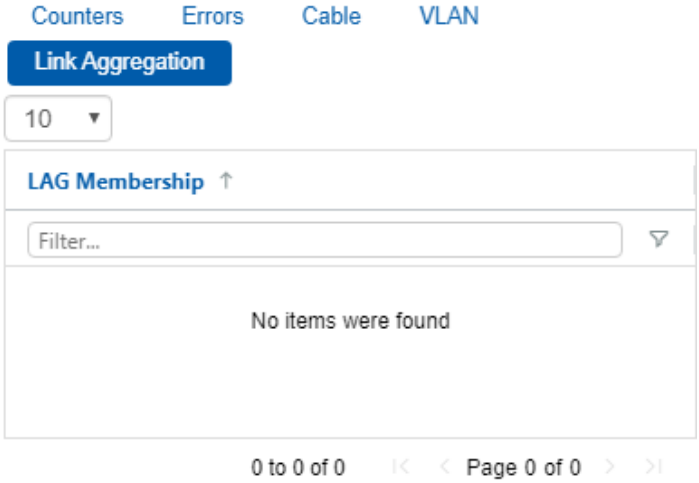
- Errors: The “Errors” tab includes the following counters:
- In Discards
- In Errors
- Out Discards
- Out Errors
- Symbol Errors



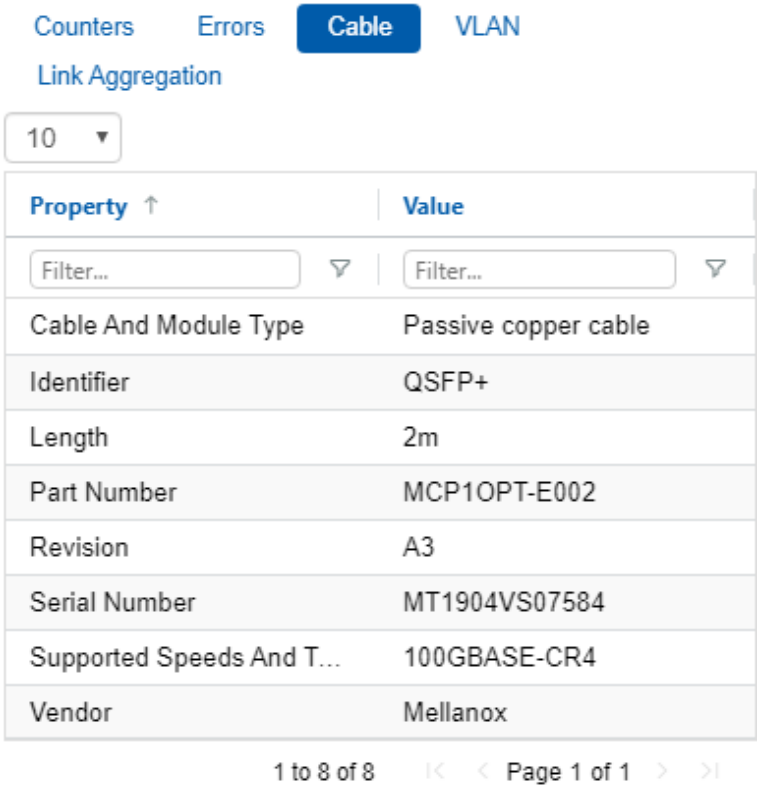
- VLAN: Provides VLAN information of the selected device, if available.



- LAG: Provides LAG information of the selected device, if available.



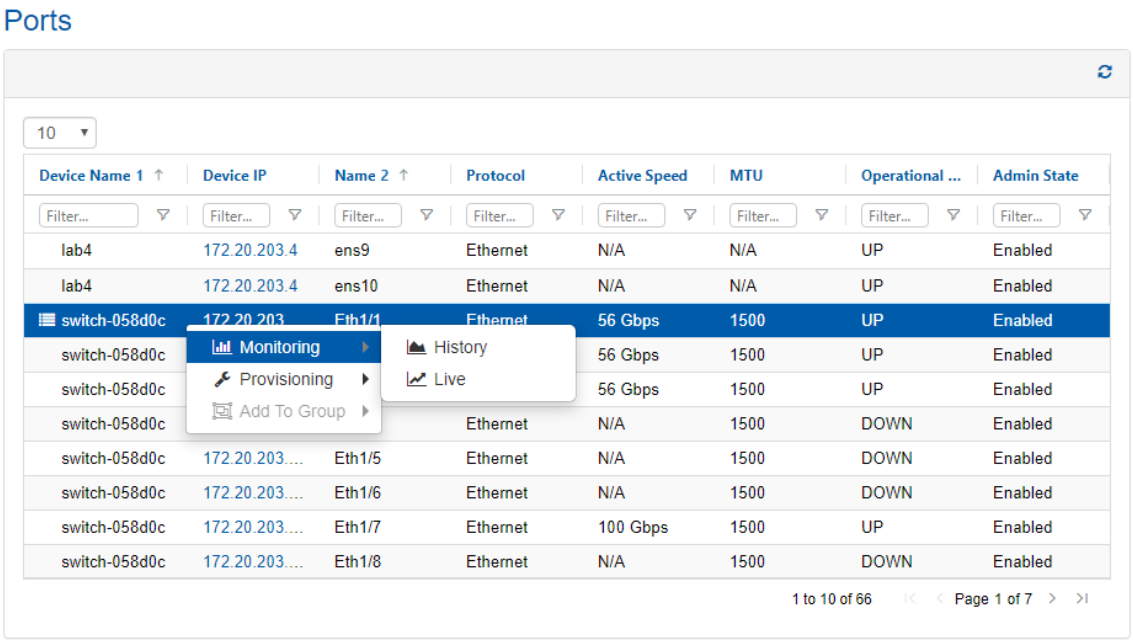
- Cable: Provides information about the cable connected to the selected port, if available.

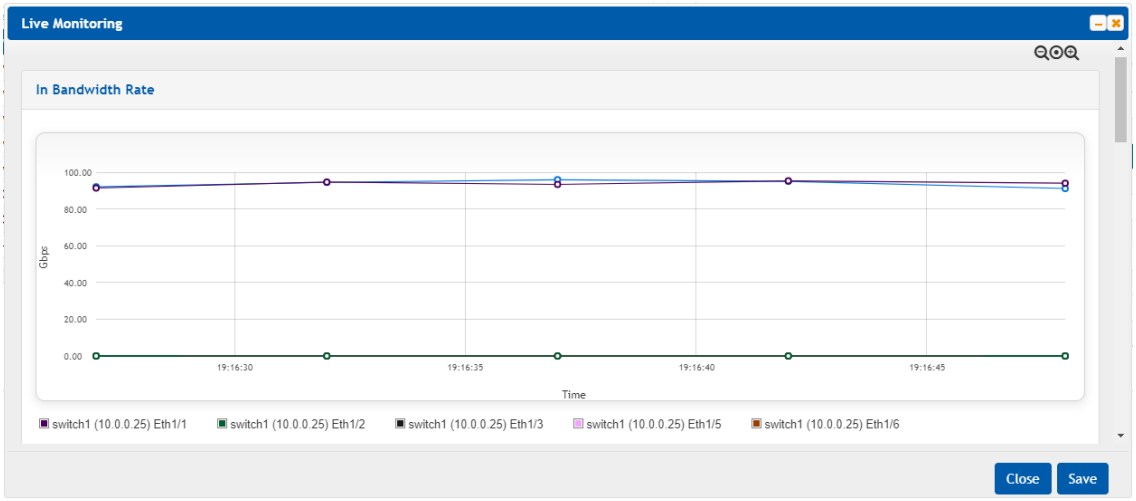


Ports Actions

A right-click on a port will enable performing the following actions:

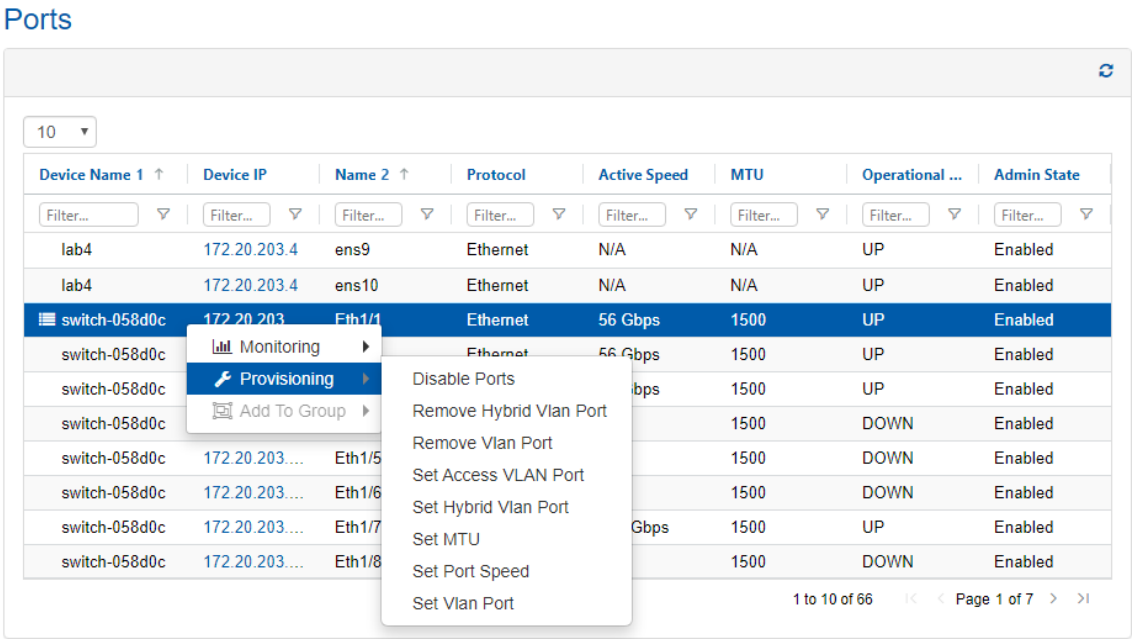
1. History/Live Monitoring:



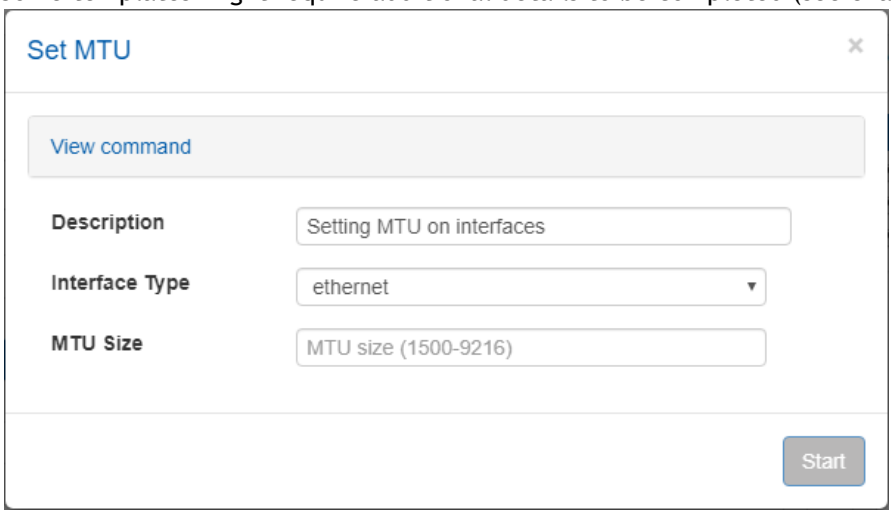


For information on Live/History Monitoring, refer to sections "History Monitoring" and "Live Monitoring".

2. Provisioning: NEO allows performing port provisioning on ports of Mellanox switches. This can be performed on one or more ports of the same Mellanox Switch.



Some templates might require additional details to be completed (see example below).

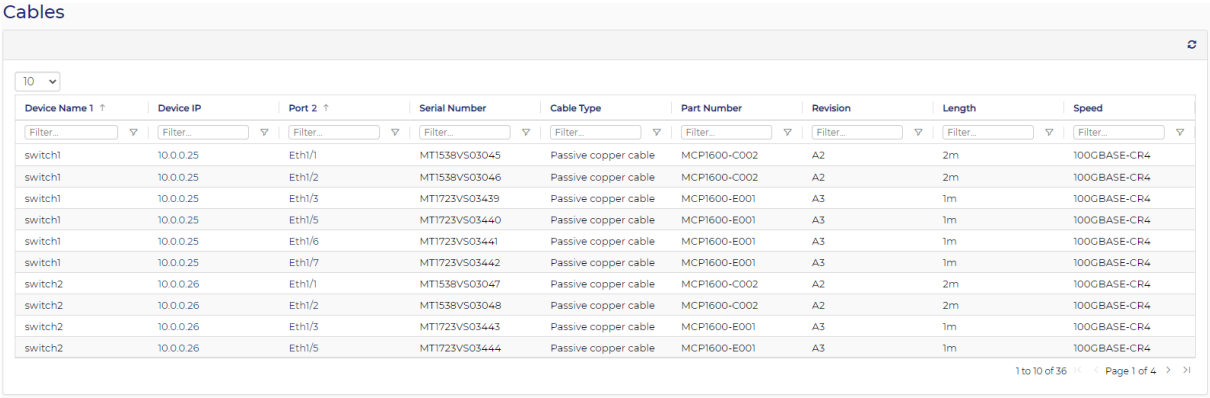


Clicking Start launches a port provisioning job.

> ⚠ After the port provisioning job is completed, it might take up to a minute for NEO tables to be updated with the new data.

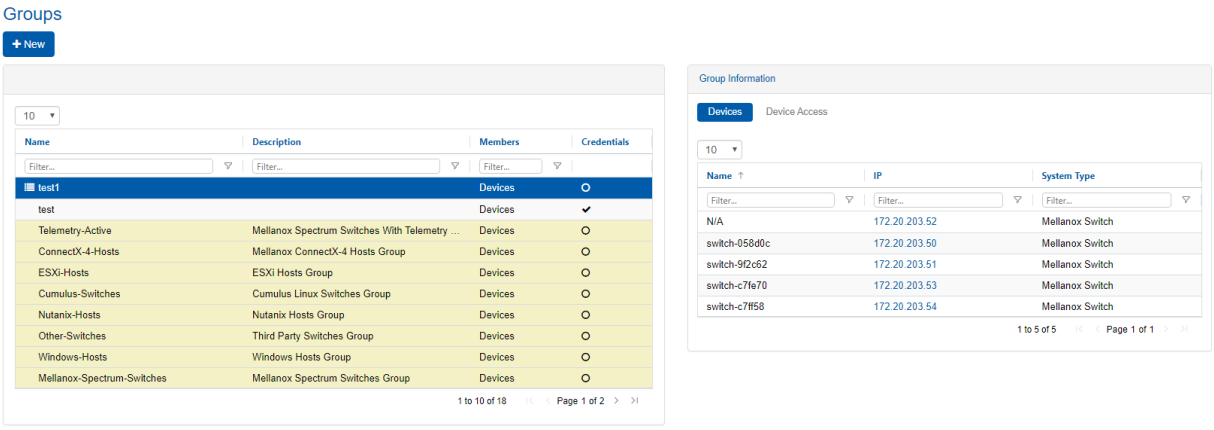
Cables

The Cables window provides information on the cables and modules connected to devices in the network.



Groups

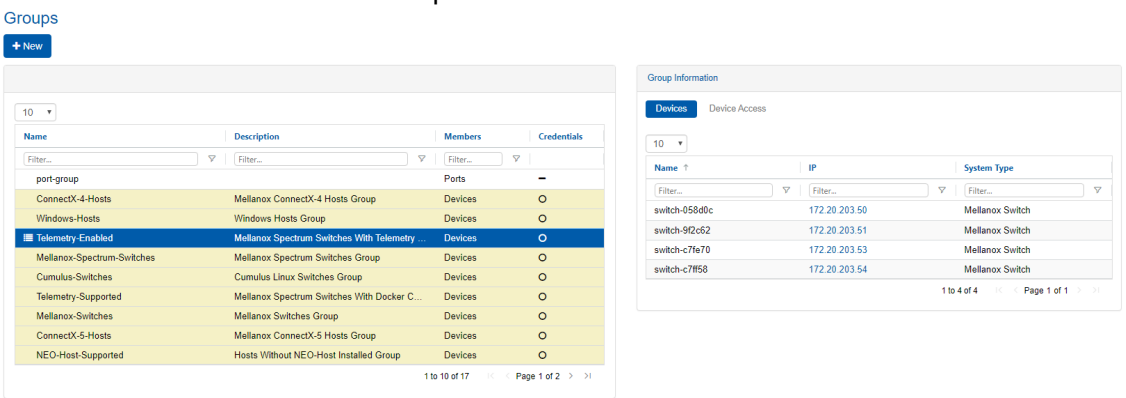
The Groups window includes 17 predefined groups for hosts/switches/ports with information about the groups members and credentials (if defined). The Members column indicates the group type: Device/Port.



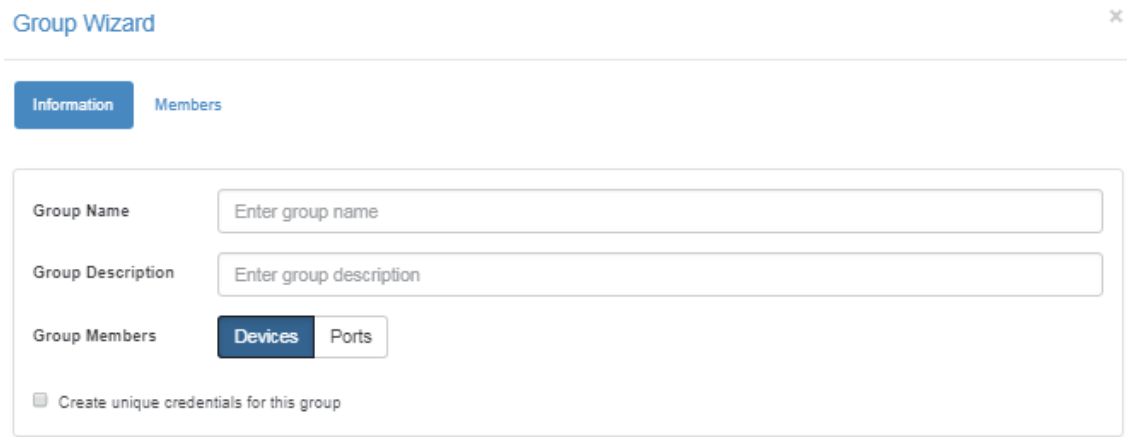
This window also allows creating new groups.

To create a group of a number of devices/ports:

1. Click the “New” button under “Groups”.



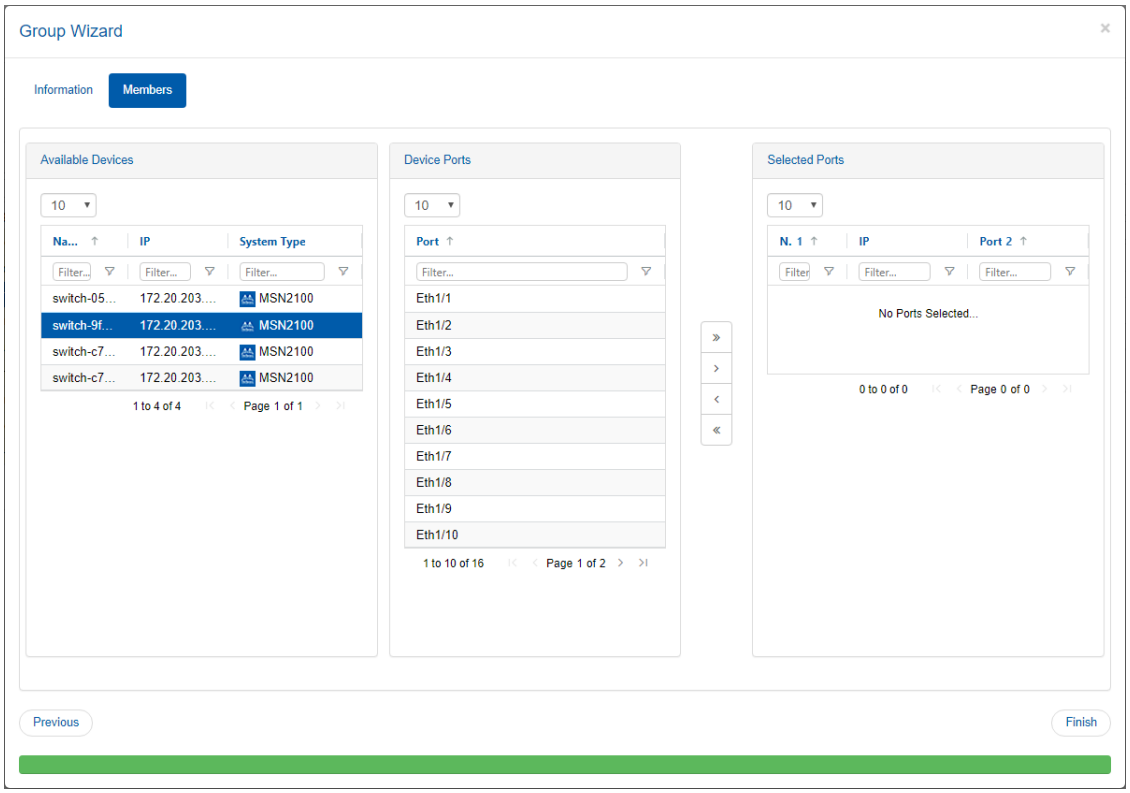
2. Select the Group Members (Devices/Ports), fill in the Group Name and Group Description in the Group wizard, then click “Next”.



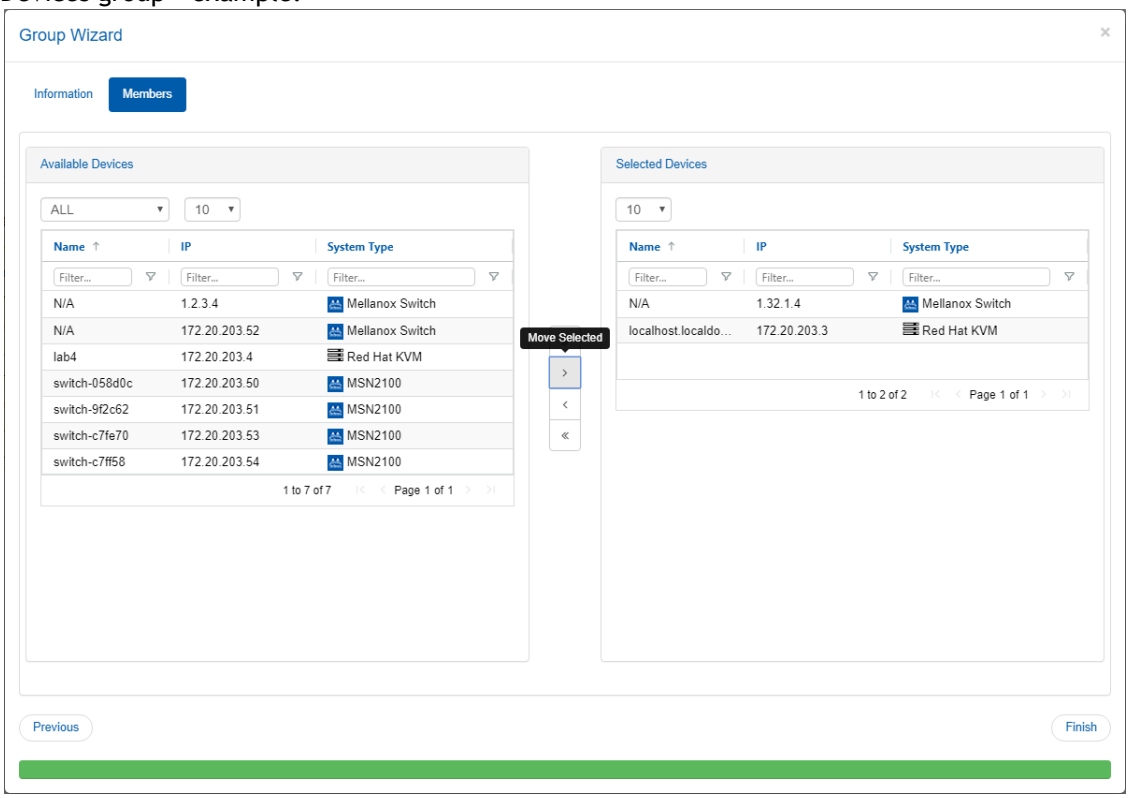
The "Create Unique Credentials For This Group" checkbox is only available for devices groups. If checked, you will be able to create new credentials for the group members which will overwrite the global default credentials (set under Settings > Device Access), and the device credentials (set under Devices > Device Access). Any of the three credential levels (global, group, and device) can overwrite each other.

3. Choose the members of the group under “Members” by moving the devices from Available Devices to Selected Devices/Ports, and click “Next”.
Ports group - example:

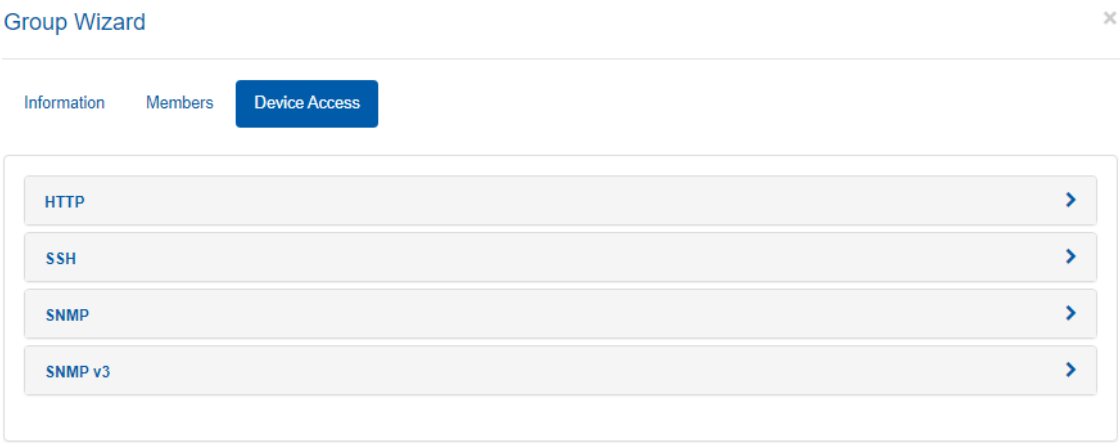
> ⚠ Grouping ports is supported for Mellanox/Cumulus ports. Note that when creating a port group, you can group the ports of one device or more, provided that the ports are of the same type (for example: Eth type). Select one device, then its ports, and move them under “Selected Ports”, then repeat the action for all devices you wish to add to the same group.



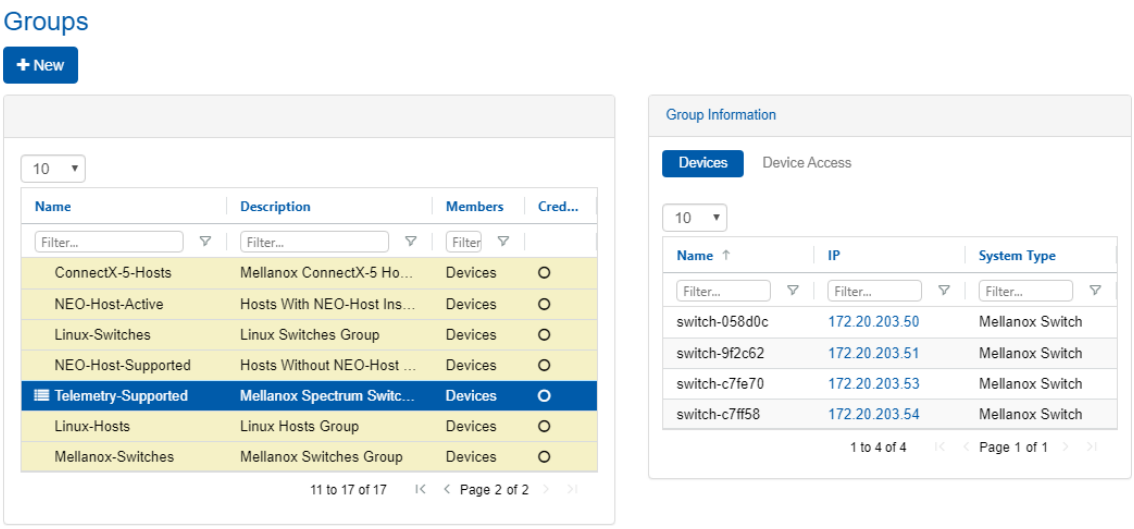
Devices group - example:



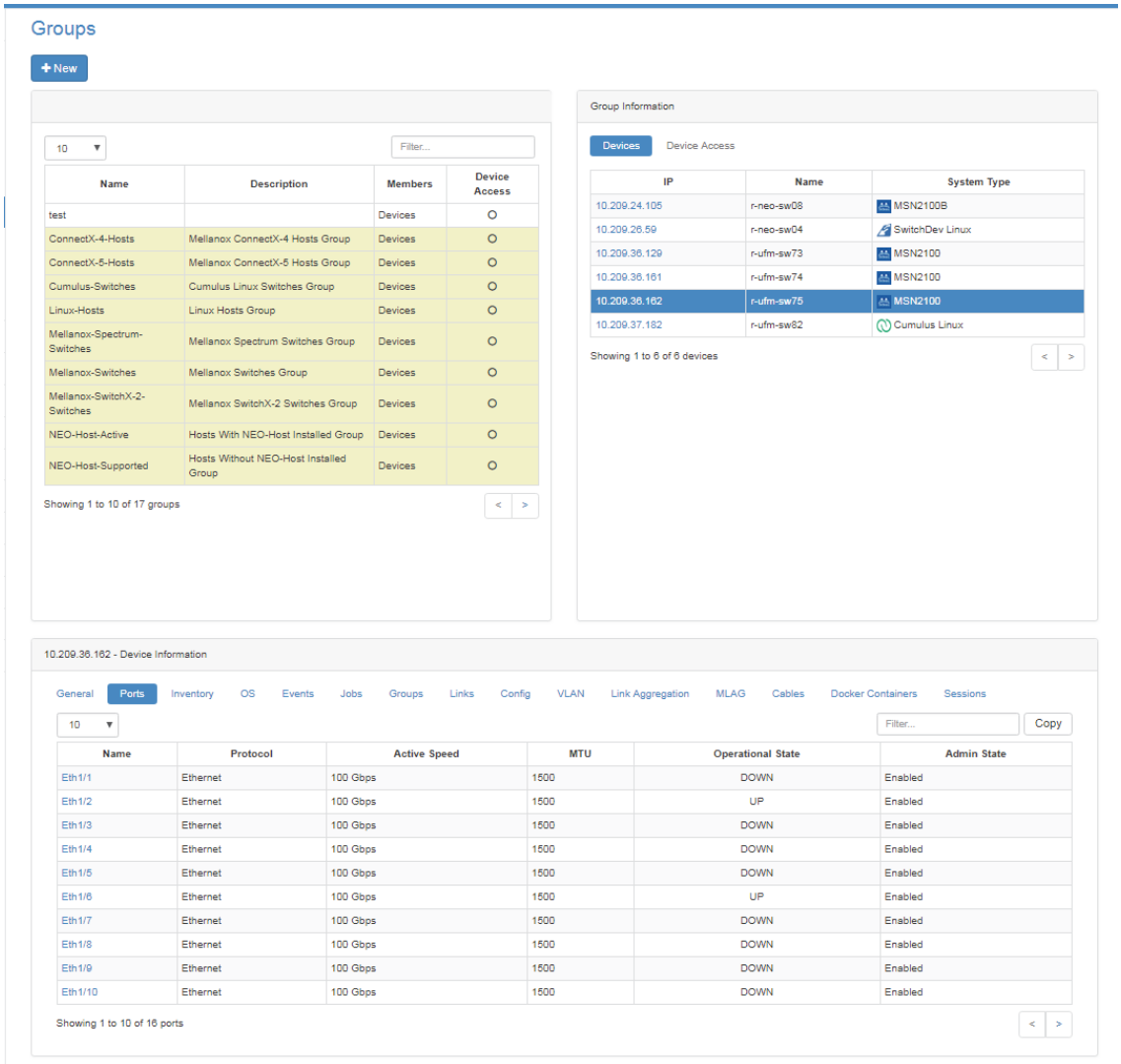
4. If you checked the Credentials button for the devices group, you will be asked to provide the new credentials as a final step.



5. Once you click "Finish", the group will be displayed on the left pane, and the Group Information will be displayed on the right pane.

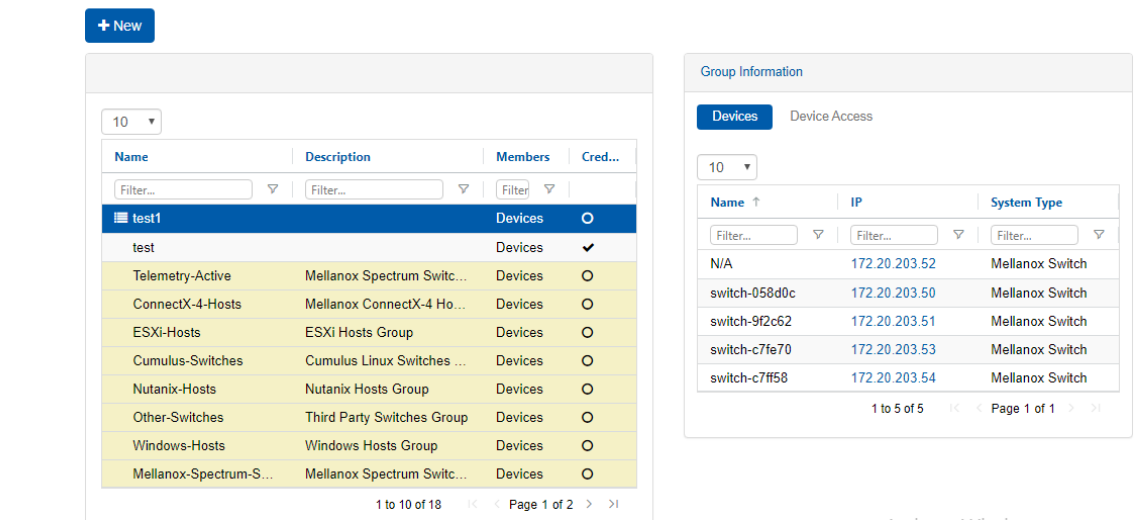


Note that you can view the device information of a device in a group by clicking the device under Group Information in the "Groups" window.



In addition, a right click on a specific group will offer the following selection of actions:

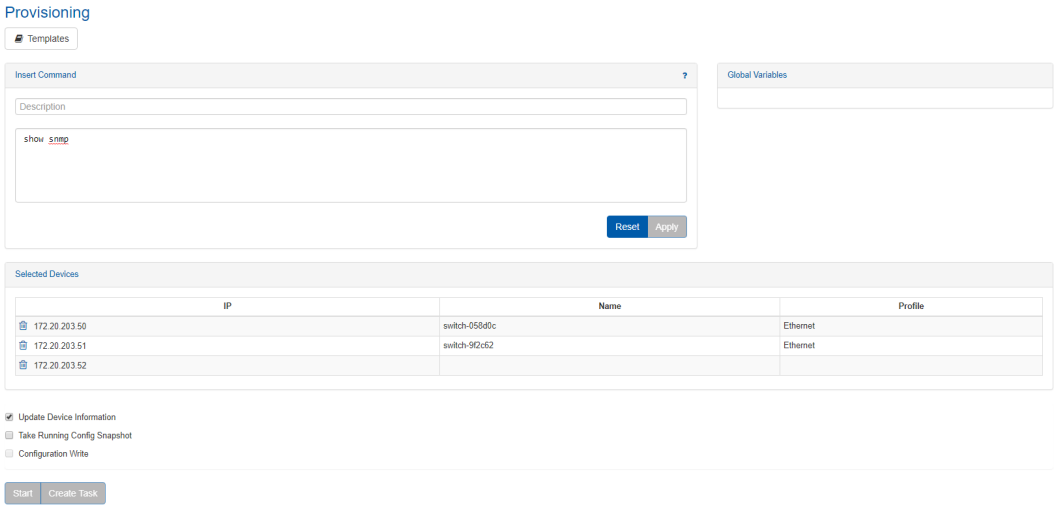
- Modify Members: Opens the Group Wizard in which members can be removed and added to the group.



- Delete: Clicking the OK button in the dialog box removes the group from NEO.
- Provisioning: allows applying a command or a sequence of commands on all group members at once, or on specific group members, per user selection. For further information on Provisioning, refer to "Provisioning".

  > ⚠ While the user may create a task for the entire group, the changes will apply to members included in the group at the time of the task's execution. Provisioning templates of specific arguments cannot be applied on groups.

  > ⚠ Provisioning templates of specific arguments cannot be applied on groups.



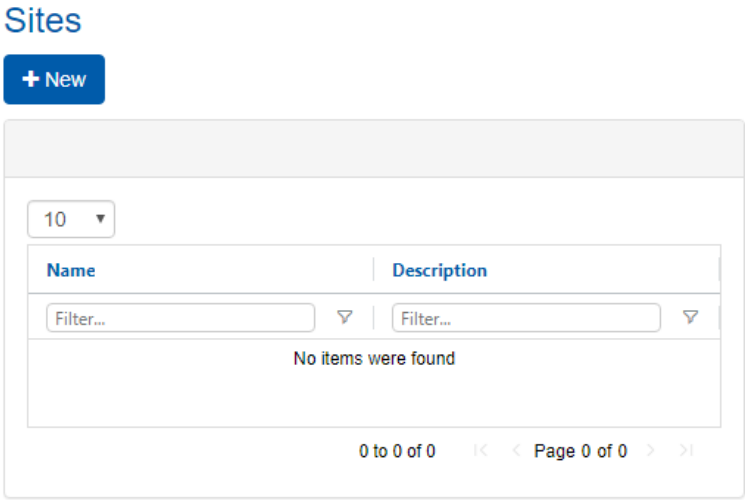
- Reboot: upon clicking on the "OK" button in the dialog box, all the devices in the group will be rebooted.
  Note: This action can be performed on groups that contain Mellanox switches.
- Onyx Software Upgrade: when selecting this option, a dialog box will appear, requiring the user to fill in the relevant details in order to perform the upgrade on all devices in the group. For further information on SW Upgrade, refer to "Onyx Software Upgrade".
  Note: This action can be performed on groups that contain only Mellanox switches.
- Generate Dump: When selecting this option, a dialog box will appear, requiring the user to fill in the relevant details in order to perform the dump generation for all devices in the group. For further information on Generate Dump, refer to Generate Dump.
  Note: This action can be performed on groups that contain only Mellanox switches.
- Driver Install: When selecting this option, a dialog box will appear, requiring the user to fill in the relevant details to perform the installation/upgrade on all hosts in the group.Note: This action can be performed on groups that contain only Linux hosts.
- Acknowledge: acknowledges all events related to the devices in the selected group.
- History Monitoring: Provides a report of the devices' attributes values history.
  Note: This action can be performed on groups that contain only Mellanox switches.

Sites

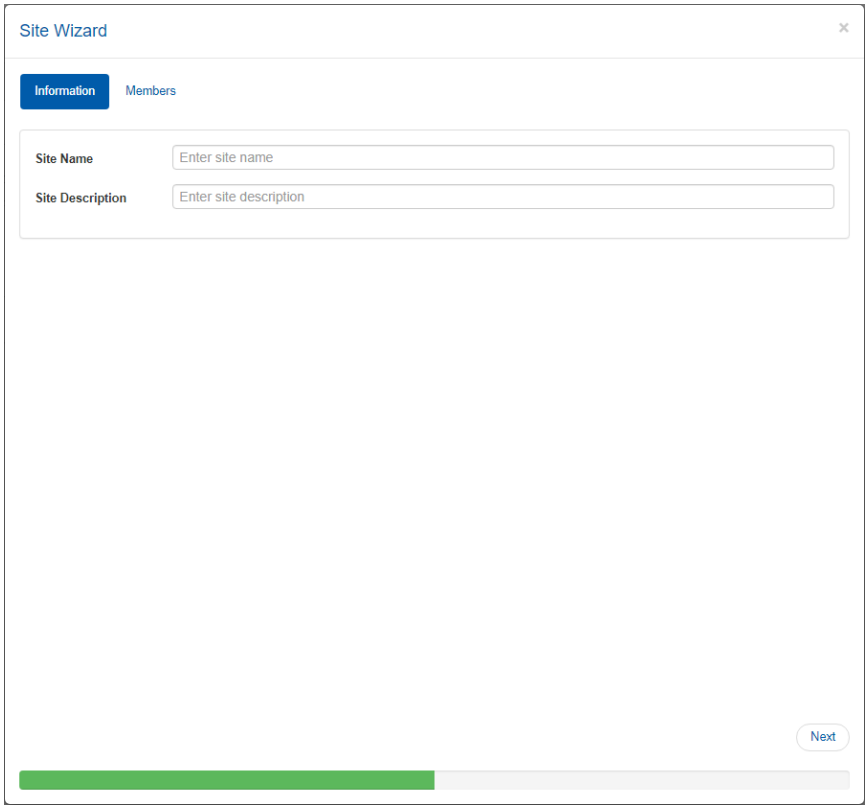
The Sites window allows you to define physical locations of devices with information about the site's members. This window also allows creating new sites.

To create a site of a number of devices:

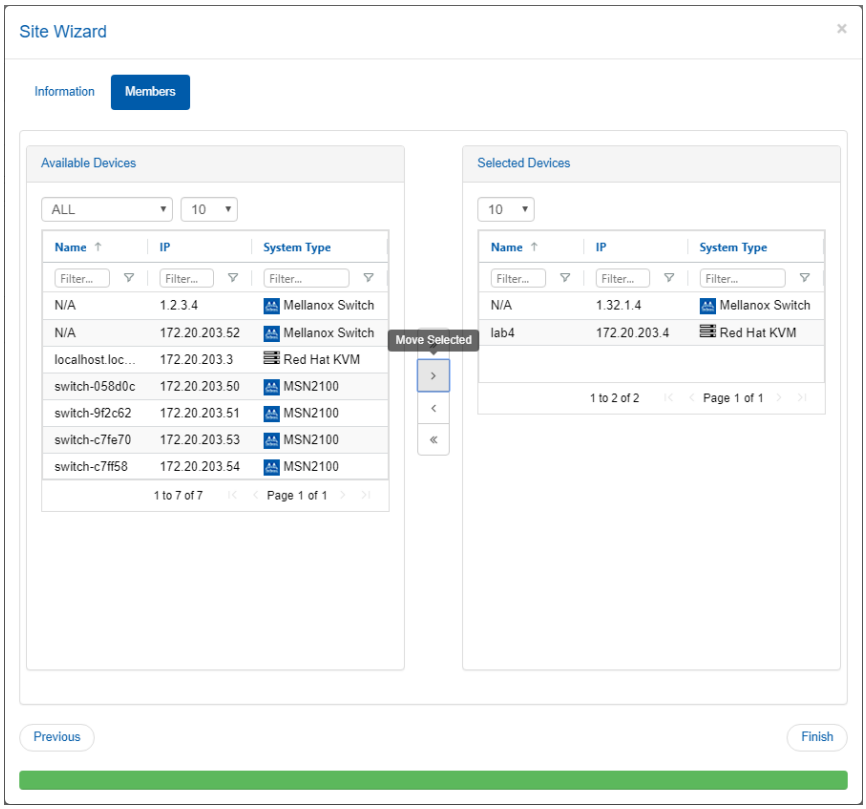
1. Click the “New” button under “Sites”.



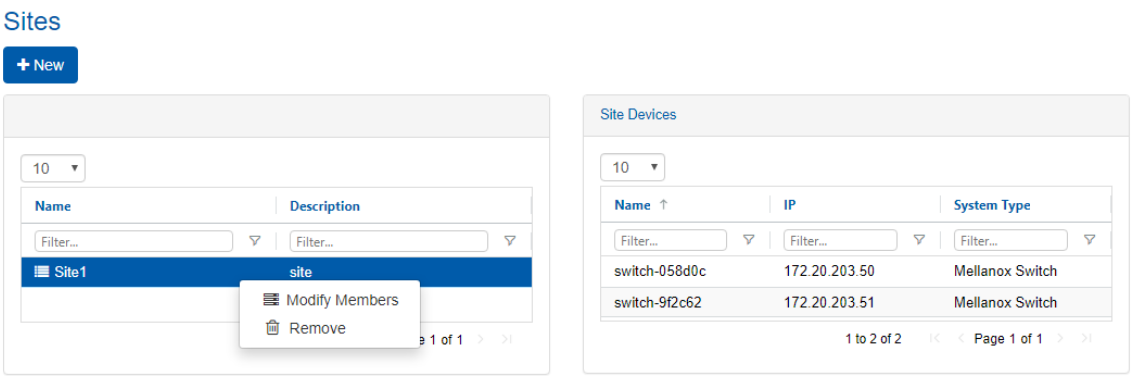
2. Select the Site Members. Fill in the Site Name and Site Description in the Site wizard, then click “Next”.



3. Choose the members of the site under “Members” by moving the devices from Available Devices to Selected Devices/Ports, and click “Next”.



4. Once you click Finish, the site will be displayed on the left pane, and the Site Information will be displayed on the right pane.



Note that you can view the Device Information of a device in the site by clicking the device under Site Information in the “Sites” window.

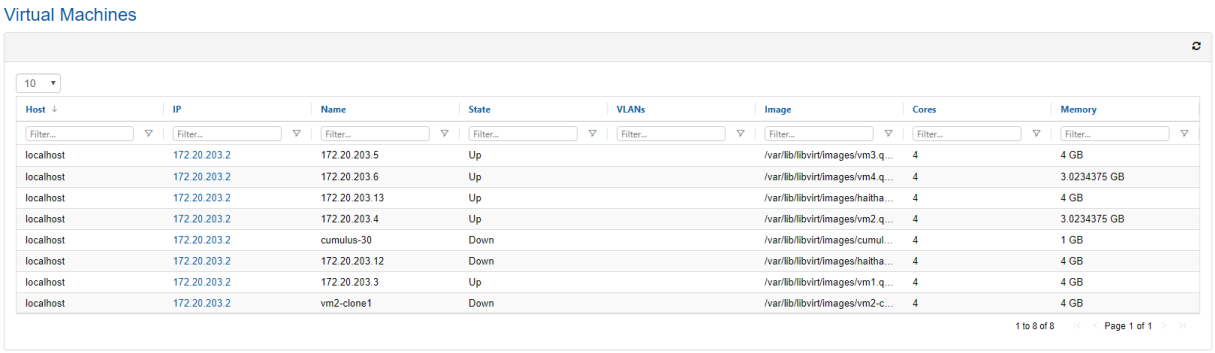
In addition, a right-click on a specific site will offer the following actions:

- Modify Members – opens the Site Wizard in which members can be removed and added to the site
- Remove – upon clicking on the “OK” button in the dialog box, the site will be removed from NEO

Virtual Machines

The Virtual Machines window lists all the Virtual Machines (VMs) that run on all KVMs in the network, and provides the following details of each VM.

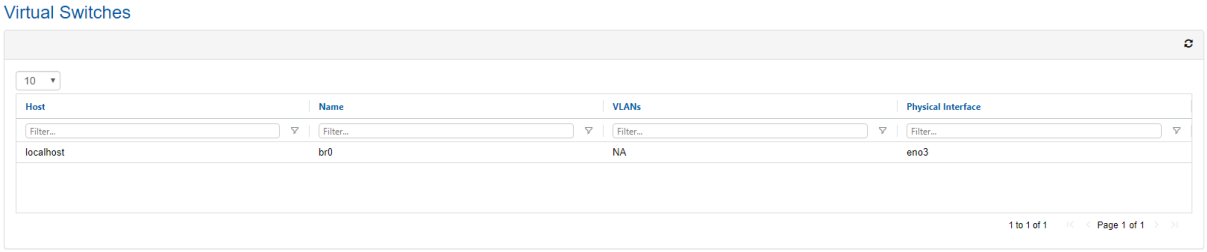
VM Info	Description
Host	Name of the KVM
Name	Name of the VM
State	State of the VM
VLANs	VLAN IDs
Image	The image run by the VM
Cores	VM number of cores
Memory	VM memory size



Virtual Switches

The Virtual Switches window lists all the Virtual Switches that run on all KVMs in the network, and provides the following details of each virtual switch:

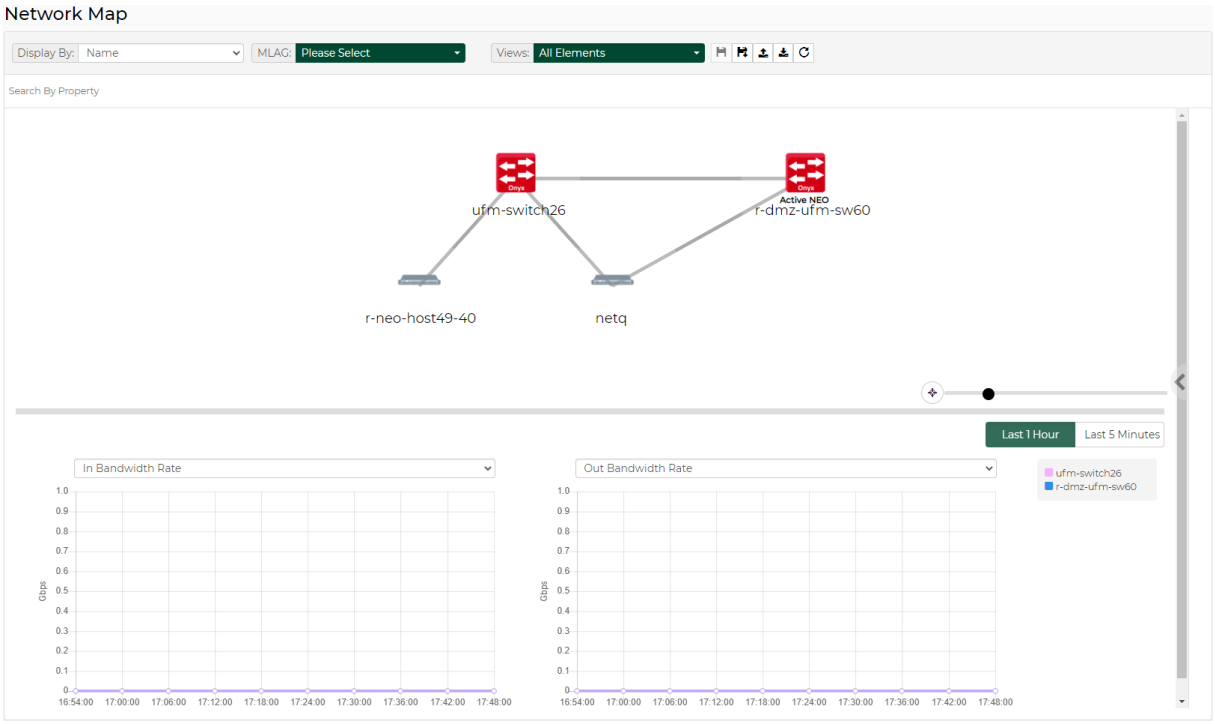
VM Info	Description
Host	Name of the KVM
Name	Name of the virtual switch
VLANs	VLAN ID
Physical Interface	Physical port



Network Map

The Network Map screen shows the fabric, its topology, elements and properties. NEO performs automatic fabric discovery and displays the fabric elements and the connectivity between the elements. In the Network Map screen, you can see how the fabric and its elements are organized (e.g., switches and servers). In addition, it helps to utilize resources and traffic by performing telemetry and monitoring actions on the fabric in a colorful, user-friendly interface.

> ⚠ The network map and its inner components are automatically refreshed every 30 seconds.

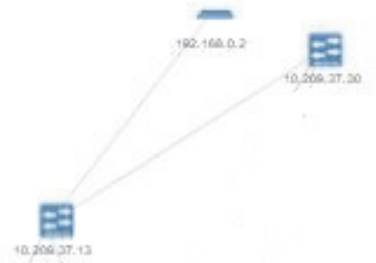


The zoom slider enables zooming in and out on the map, while the compass icon serves as a reset button.

"Search By Property" allows users to search for keywords using free text.

Map Components

Component	Description
Mellanox Onyx Switches* 	Represents Mellanox-OS switches discovered/ managed by Mellanox NEO.

Component	Description
Non-Mellanox OS Switches* 	Represents third party switches discovered/ managed by Mellanox NEO.
Servers 	Represents the computer (host) connected to the discovered/ managed switches.
Links 	In the Network Map view, you may also see the connections (represented by a line) between each of the devices and between switches and servers.
Network icon 	Represents a group of unknown discovered devices.
Unknown connection 	Represents an unknown physical connection (while one of the peers is unknown).

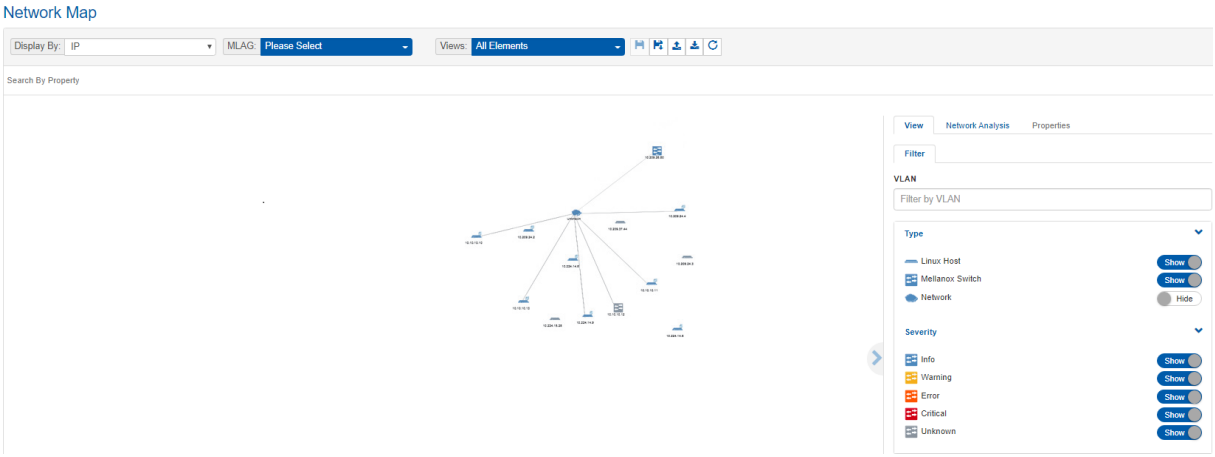
The color of the device varies according to its severity level. For further information, refer to Devices' Severity Levels.

Map Info and Settings

The Network Map window includes physical hierarchies of the fabric. Hovering over one element in the map will highlight its connections and blur the other elements.

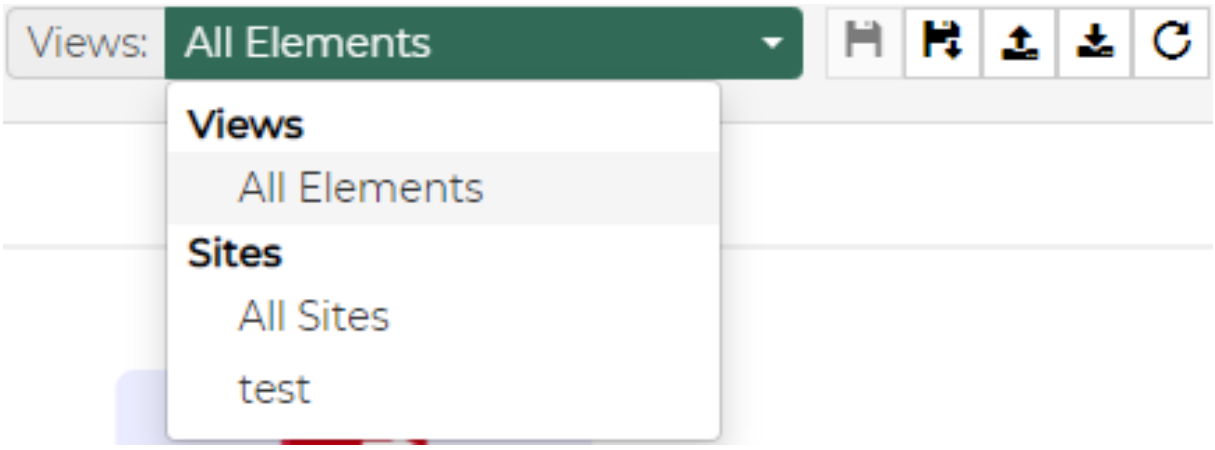
The View tab in the right pane enables filtering for certain elements to be viewed in the Network Map (see below).

The views created are saved per user, thus cannot be accessed using a different username.



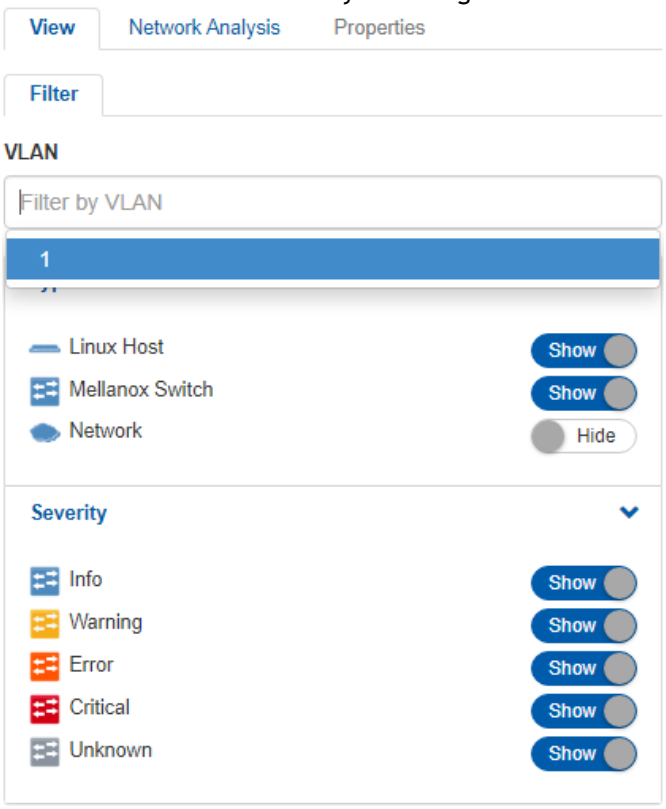
In the example above, only Mellanox Switches that have three levels of severity will be viewed in the map; those in Warning level, Error level, and Critical level. This customized filter can be saved by clicking the "Save As" button above ( ).

After clicking “Save”, the view will be saved and can be accessed from the drop down menu next to “Views:”. It can be deleted by clicking the “x” icon.



Note that the view can be edited by selecting it, modifying the filters, and saving it using the Save button ( ). The refresh button ( ) is used for reset. Network map layouts can be exported and saved to text files by clicking on the Export icon ( ). In addition, they can be imported from text files by clicking on the Import icon ( ). This allows the sharing of a layouts between different users.

You can also filter for the devices allocated to one or more VLANs by selecting the VLAN number/

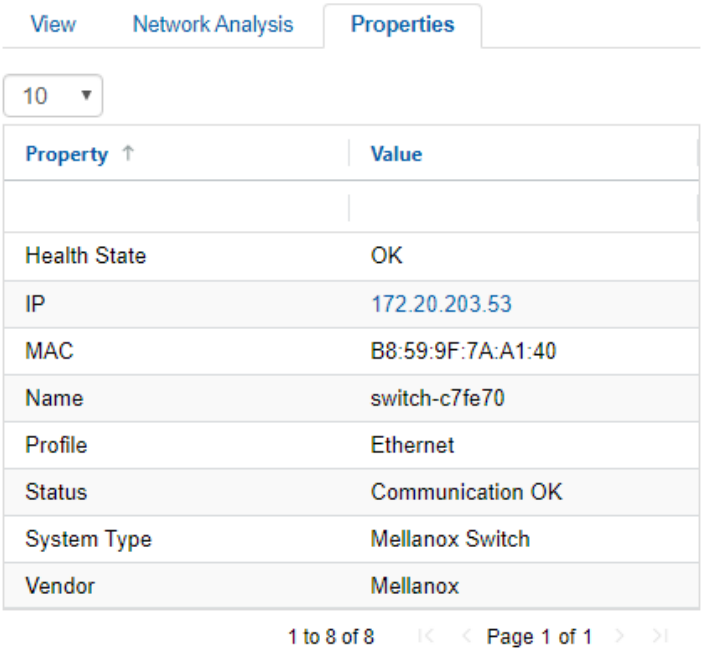


numbers in the right pane (see below). Note that when filtering for the members that belong to a certain VLAN number, the option to hover over any device in the map will be disabled.

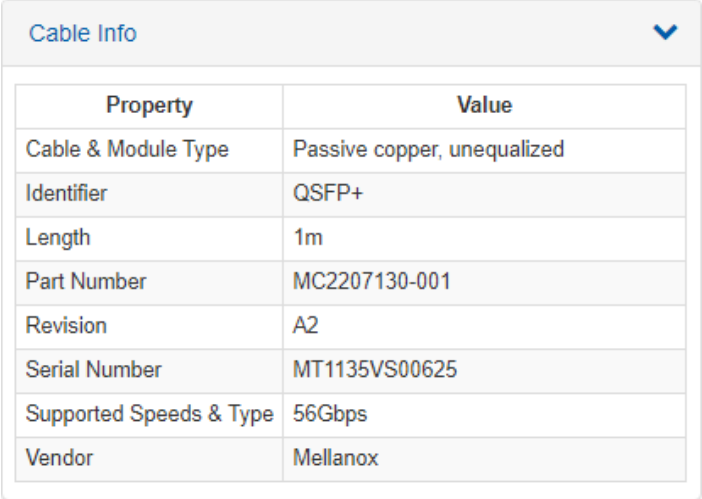
Properties Tab

- The Properties tab in the same pane provides the following:
  - When selecting an element in the network map, its name, vendor, profile, status, IP, system type, and health information will be displayed.
  - When selecting a link connecting between two devices, various types of information will be displayed in the following order:

a. A list of all ports' links.

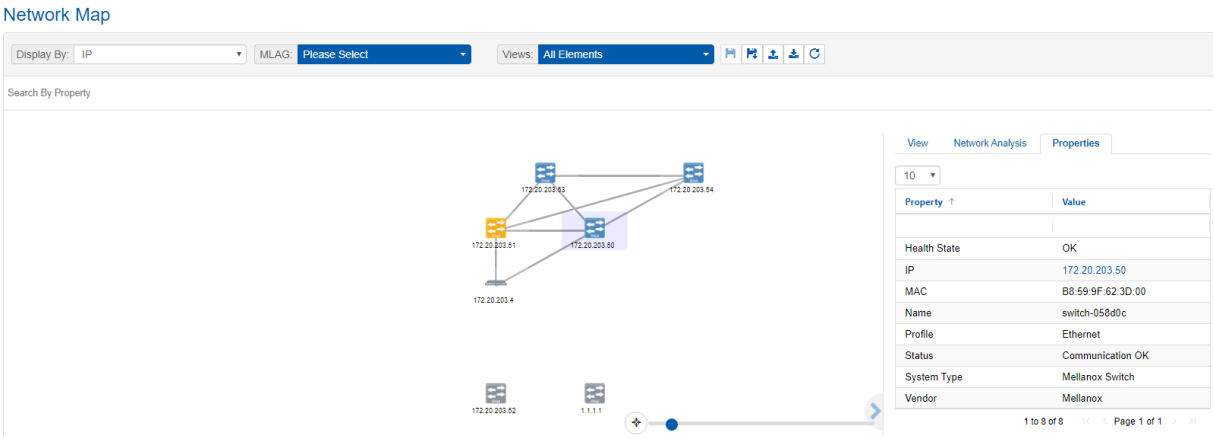


b. Port cable information is available when at least one of the devices connected in the link is a Mellanox switch of communication status “OK”. Cable info can be exposed by clicking “+”. When this information is called for the first time, it will take a few minutes for the server to request and upload it.



Device Info

When selecting a system in the network map, its name, vendor, profile, status, IP, system type, and health information will be displayed in a table under the properties tab.



Links Info

When selecting a link on the map connecting two devices, the following information will be displayed:

1. A list of links between the two devices, recognized by the corresponding ports of each device.
2. A table of basic port information.

Cable Info

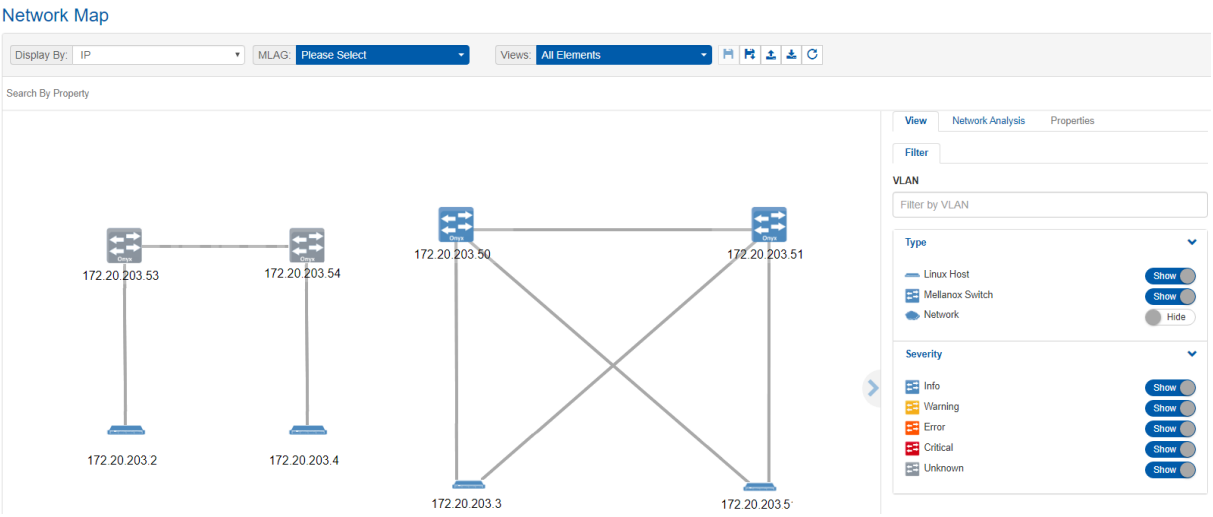
The cable info can be viewed by clicking the [+] icon. It may be available when at least one of the devices of the link edges is a Mellanox switch of communication status "OK".

Cable Info

Property	Value
Cable & Module Type	Passive copper, unequalized
Identifier	QSFP+
Length	1m
Part Number	MC2207130-001
Revision	A2
Serial Number	MT1135VS00625
Supported Speeds & Type	56Gbps
Vendor	Mellanox

View Tab

The View tab in the right pane enables filtering for certain elements to be viewed in the Network Map, and allows performing monitoring and telemetry actions for network analysis (see below).



Type and Severity Filters

In the example above, there are three available system types; Mellanox Switch, Linux Host and Cumulus Linux, listed under the Type section. It is possible to filter the displayed systems in the map by toggling the buttons next to each system type. It is also possible to filter according to the severity of the system status - Info, Warning, Error, Critical or Unknown.

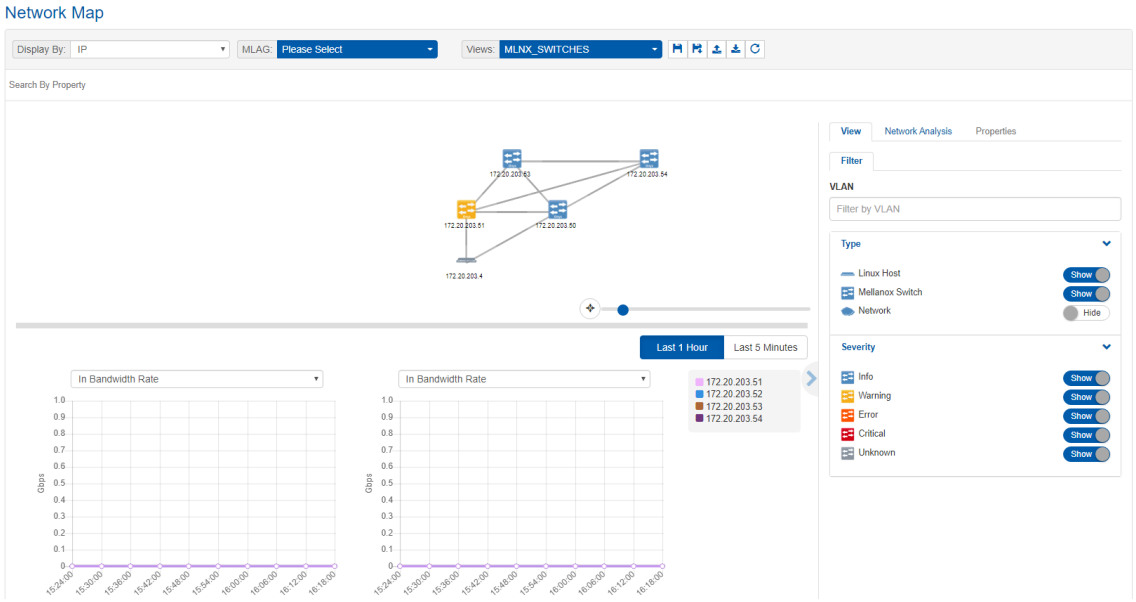
Network Analysis

The Network Analysis pane provides several network monitoring and analysis options. One option may be enabled at a given time.

1. Link Analysis: Performs monitoring on the links based on specific counters and conditions.
2. RoCE Congestion: Performs monitoring on the links based on the ECN Normalized Packets counter.
3. Network Path: Finds a path composed of links between a switch & an In-Band IP and performs monitoring on these links based on Out Bandwidth Rate counter.
4. Buffers Utilization: Indicates the status of the buffers utilization for the switches, if a threshold event occurs. In addition, provides an option to view the switch buffers histograms in a bar chart.

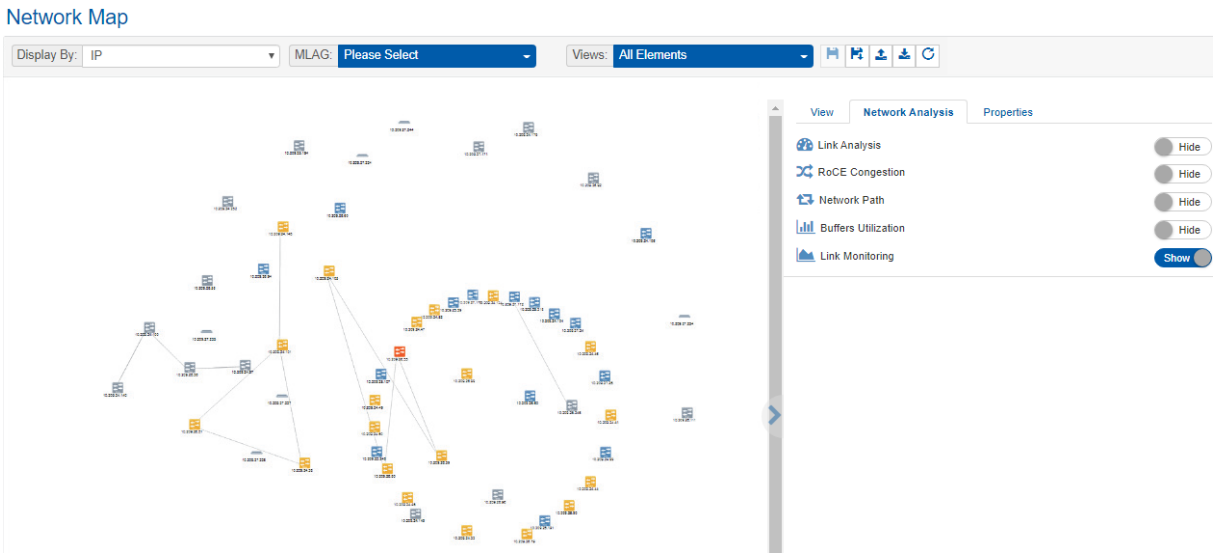
> ⚠ To enable histograms, run the following template: NEO GUI → Managed Elements → SwitchXXX → Provisioning → template → enable histogram

5. Link Monitoring: Retrieves telemetry data on switches and ports and presents it in line or bar charts.

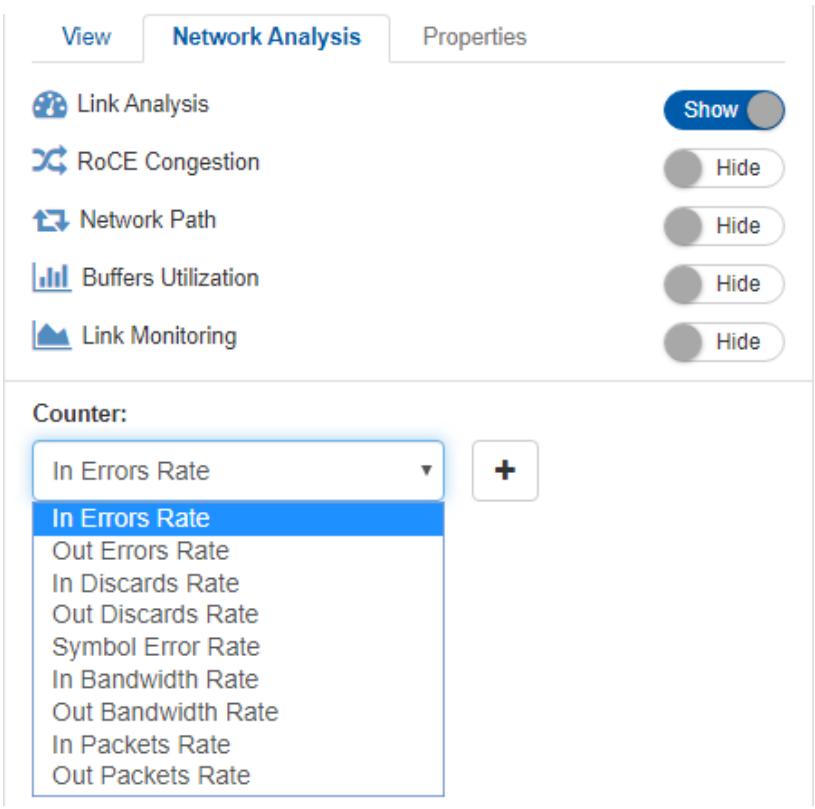


Link Analysis

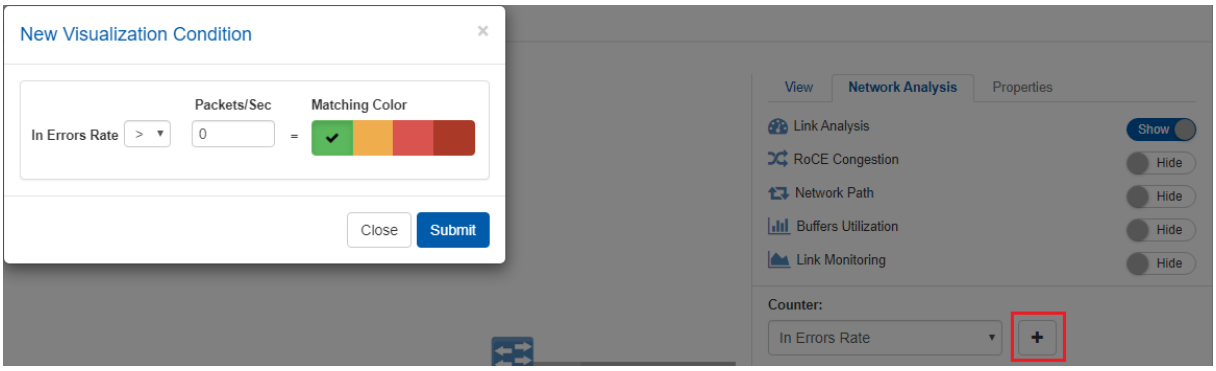
Link analysis allows you to display the link analytics according to a selected static counter, and define the conditions on which the analysis is based. The links will be colored according to the specified conditions. You may define up to five conditions.



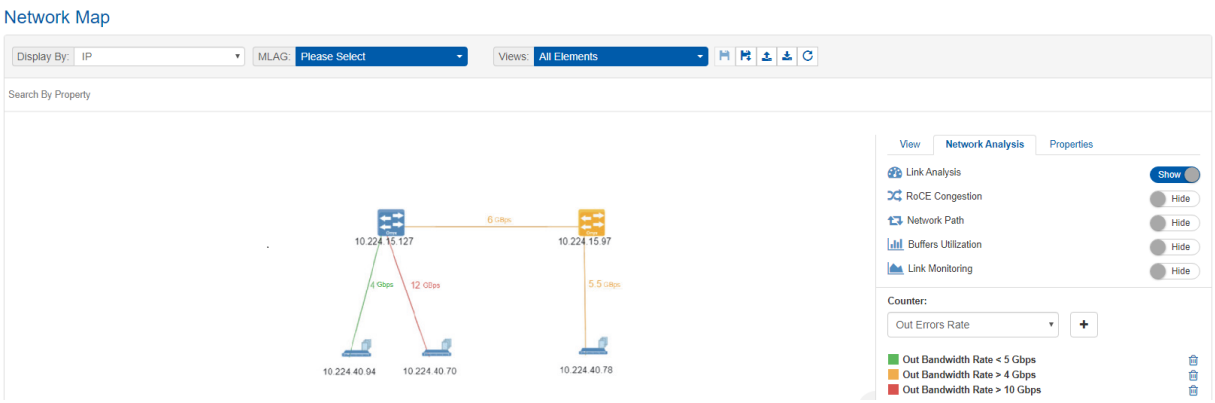
To define a condition, select the desired counter, and click on the [+] button.



A form will pop up. Choose the appropriate operator, and define the desired threshold and color. This color will be applied on the link, if the link monitoring value matches the respective condition.



The added conditions are listed in the Network Analysis section, if Link Analysis is enabled. The links are colored and labeled accordingly.



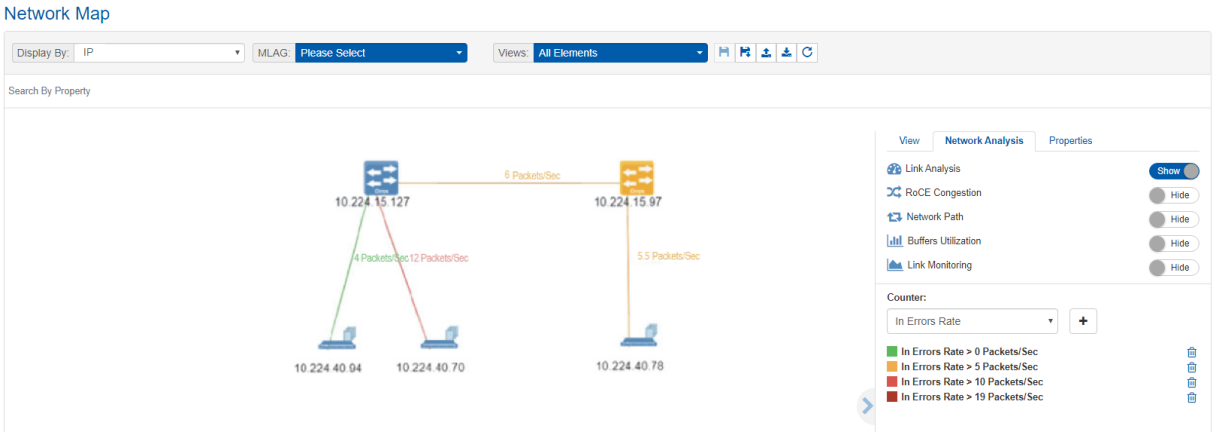
Instead of aggregating all values, the displayed value represents the worst-case scenario:

- If: (Condition) > X, the highest value will be shown
- If: (Condition) < X, the lowest value will be shown

The data samples are retrieved using the Telemetry Agent, if it is installed on the switch. Otherwise, NEO uses the SNMP requests to retrieve the data. Sampling using the Telemetry Agent is done in higher resolution.

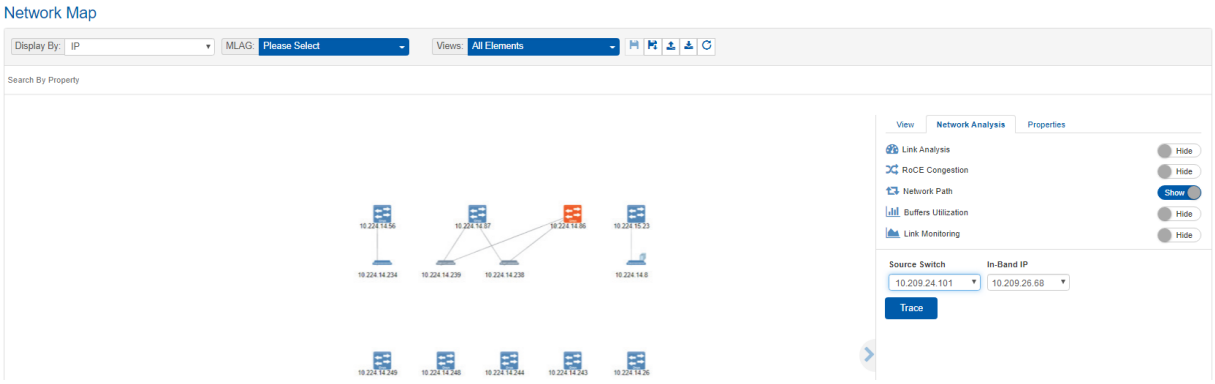
RoCE Congestion

The RoCE Congestion sub-pane provides monitoring based on ECN Normalized packets, given that there are 4 predefined conditions.



Network Path

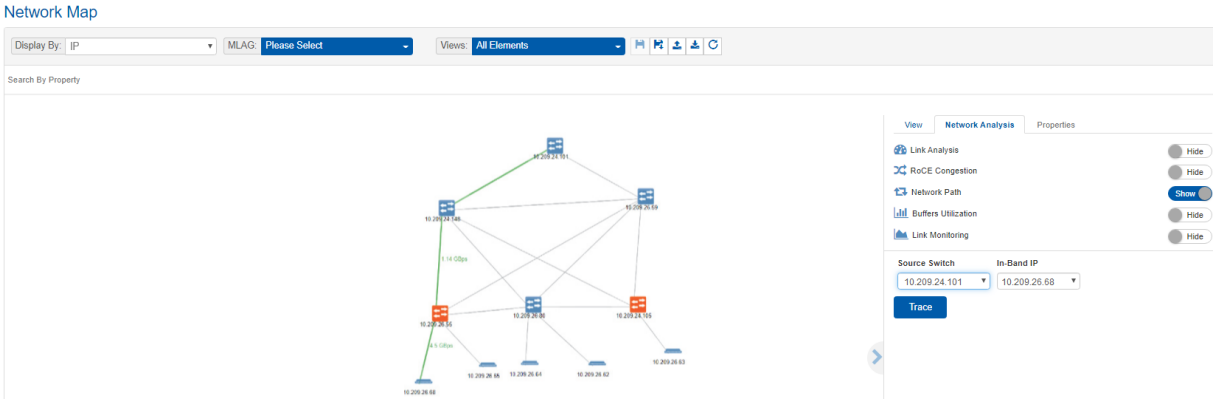
The Network Path sub-pane allows you to display the paths between a selected source switch and a specific target host (In-Band IP). The display includes the Out-Bandwidth Rate values on top of these paths.



The Network Path capability is supported by both Onyx and Cumulus operating systems. For the OS versions, please refer to the latest Release Notes document.

The displayed out bandwidth rate value is the highest value of the interfaces. Thus, if two switch systems are connected by several links, only the highest value will be displayed. You may click on the link on the map for a table with all the values.

To do so, select the source switch from the drop-down menu, type the In-Band IP in the IP Field, and click the Trace button. The optional detected paths (can be more than one path) will be colored, and the Out-Bandwidth Rate value will be displayed on the map.



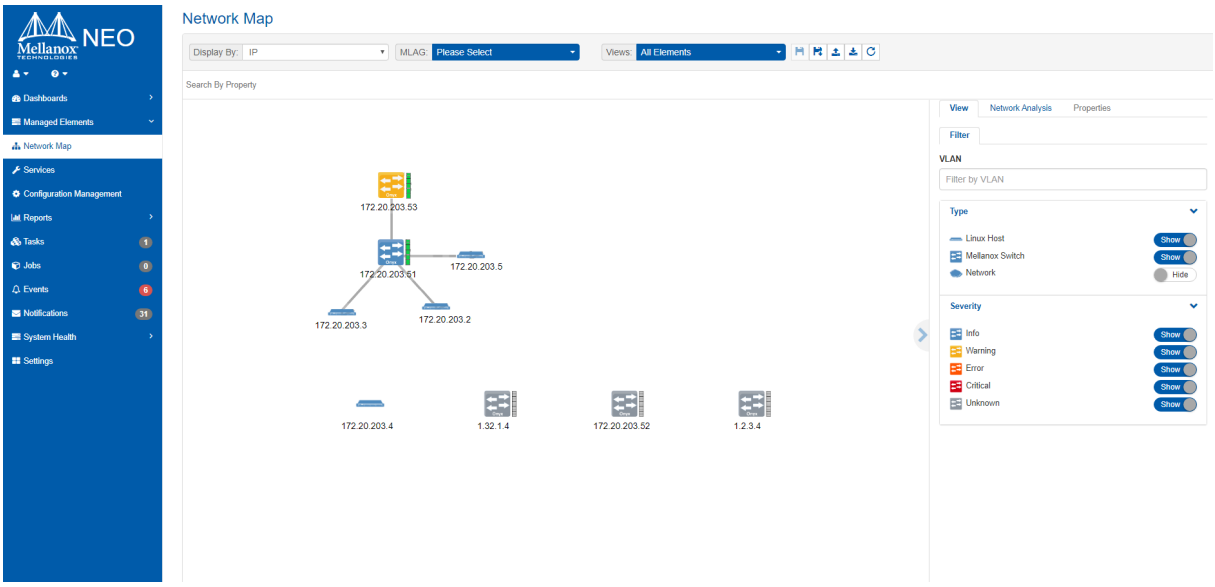
When entering a Loopback interface as the destination in NEO, one path is displayed.

Buffers Utilization

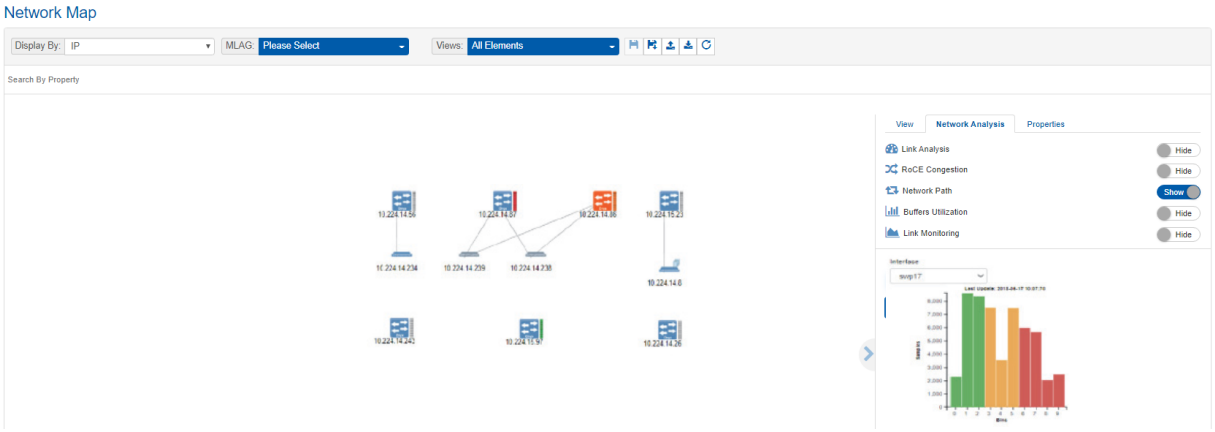
The Buffers Utilization feature samples and summarizes the capacity of admitted packets stored and queued in the buffer. This sub-pane allows a view on the switches' buffers utilization status, and provides an option to view the buffers histograms for each switch in a bar chart per interface.

The buffer icon beside each switch indicates the Buffer Utilization status. Each color corresponds to a specific status:

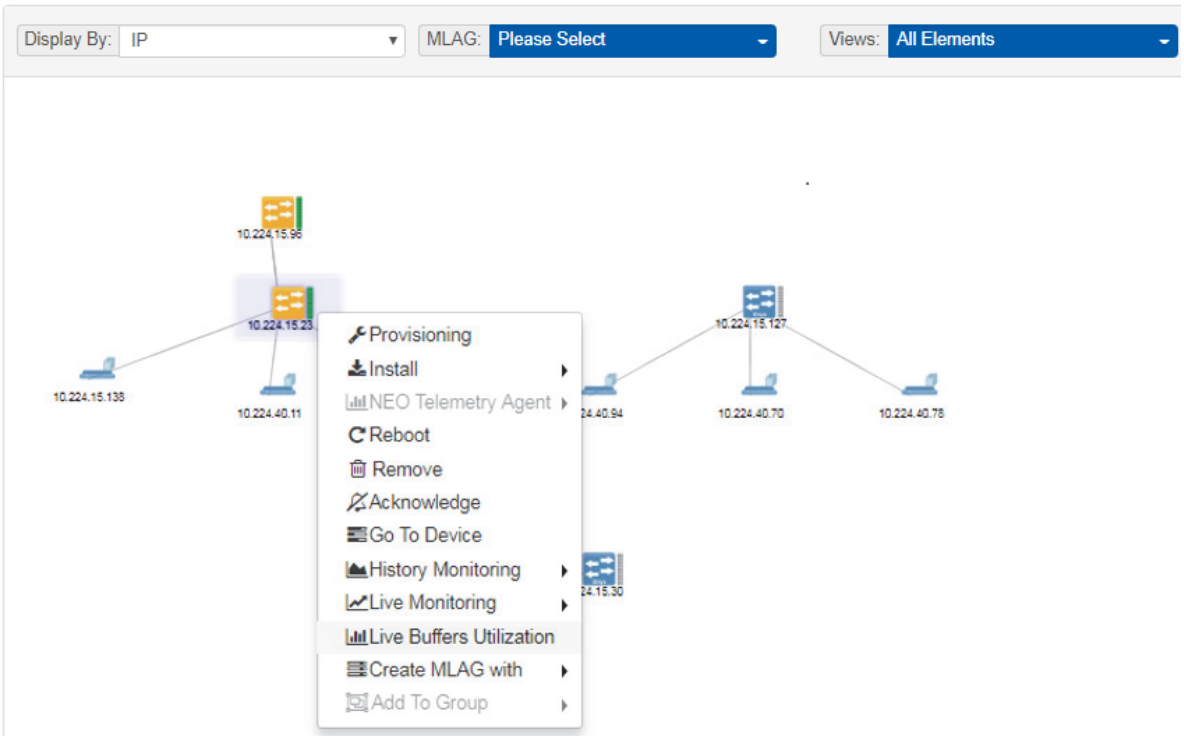
1. Grey: Unknown
2. Green: OK
3. Orange: Degraded
4. Red: Major or Critical

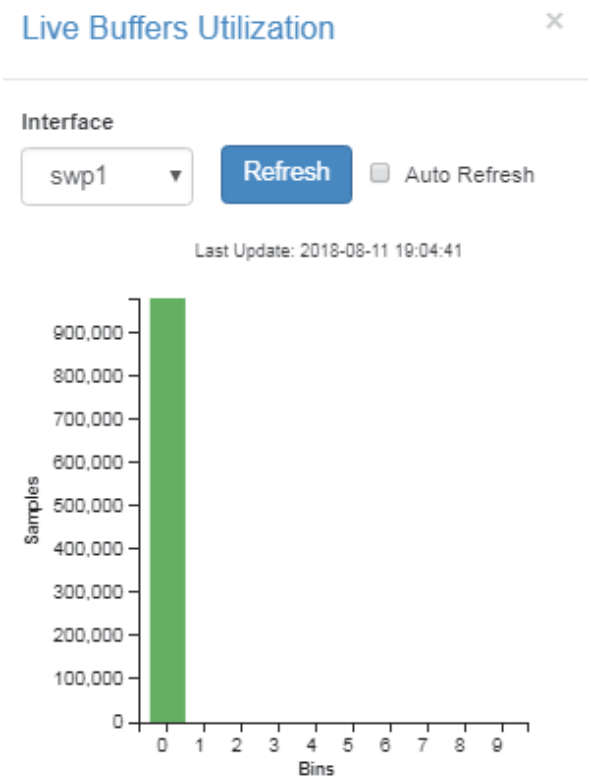


To view the histograms data for a switch if a threshold event occurs, select a switch in the map, and the interface for which you wish to see the histograms. The histograms are viewed in a bar chart. The X-axis represents the bin number, and the Y-axis represents the buffer size distribution.



For a live view of the current buffer utilization histogram, right-click on a device, and select “Live Buffers Utilization”:



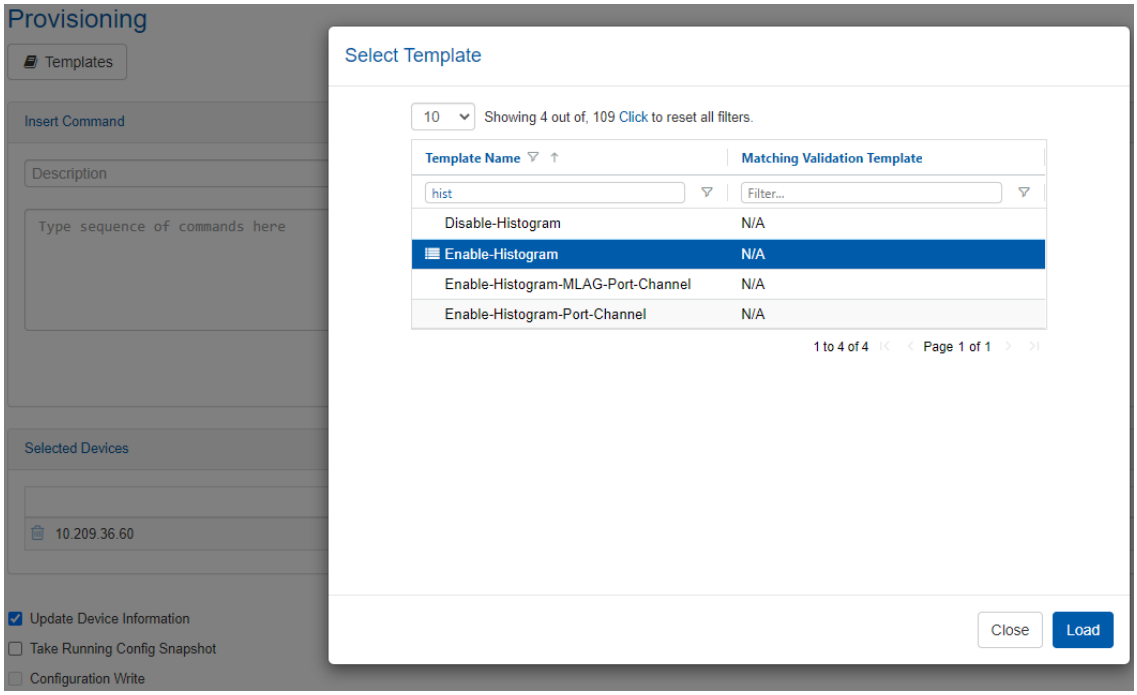


In order to configure Live Buffer Utilization follow this procedure:

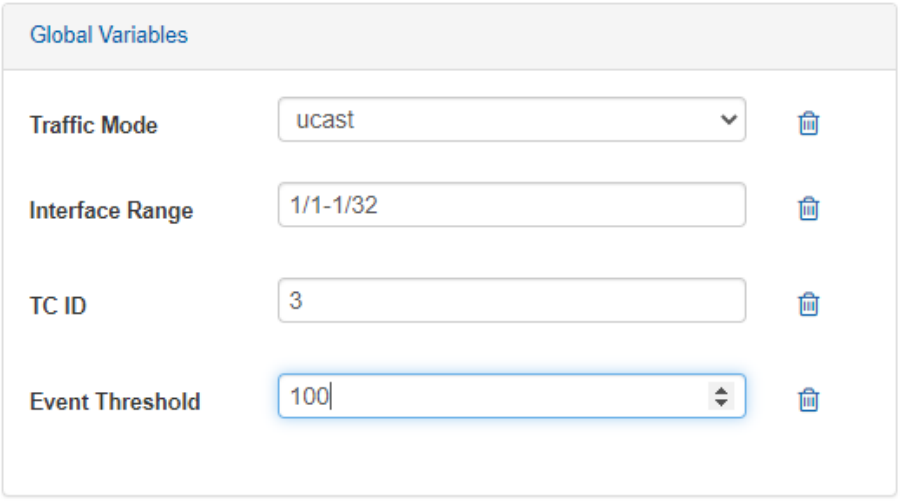
1. Right-click the desired switch under Managed Elements → Devices and install/run telemetry on it.

2. Right-click the switch under Devices and click on Provisioning and choose the“Enable Histogram” template.

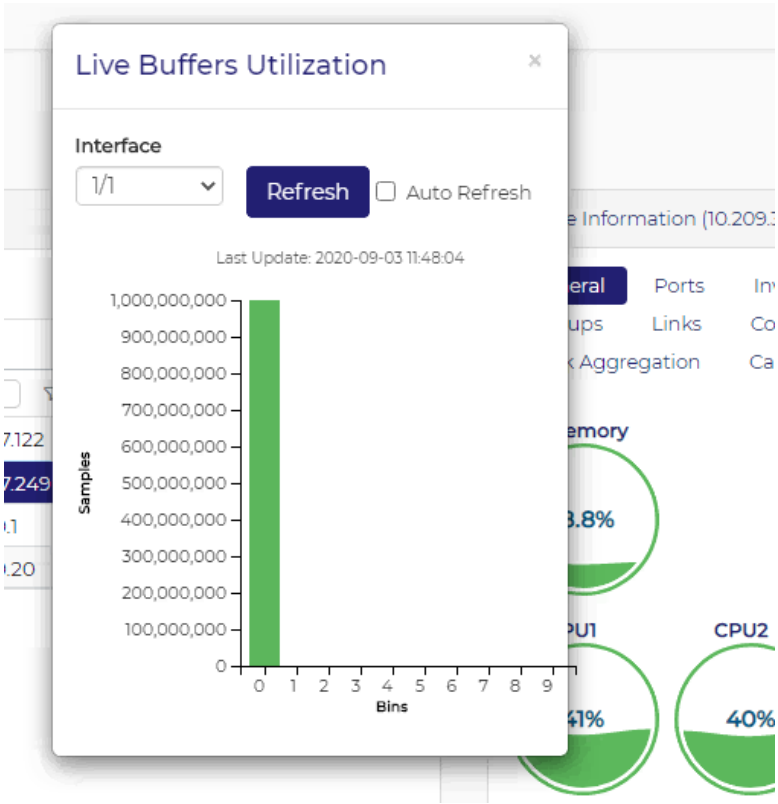
> ⚠ By default, the priority configured with NEO is 3 (i.e. TC=3 on the switch side). The priority can be changed under controller.cfg if desired.



3. Fill out the following global variables for this template.



4. Click on Live Buffer Utilization to show histogram samples based on switch histogram configuration.



Link Monitoring

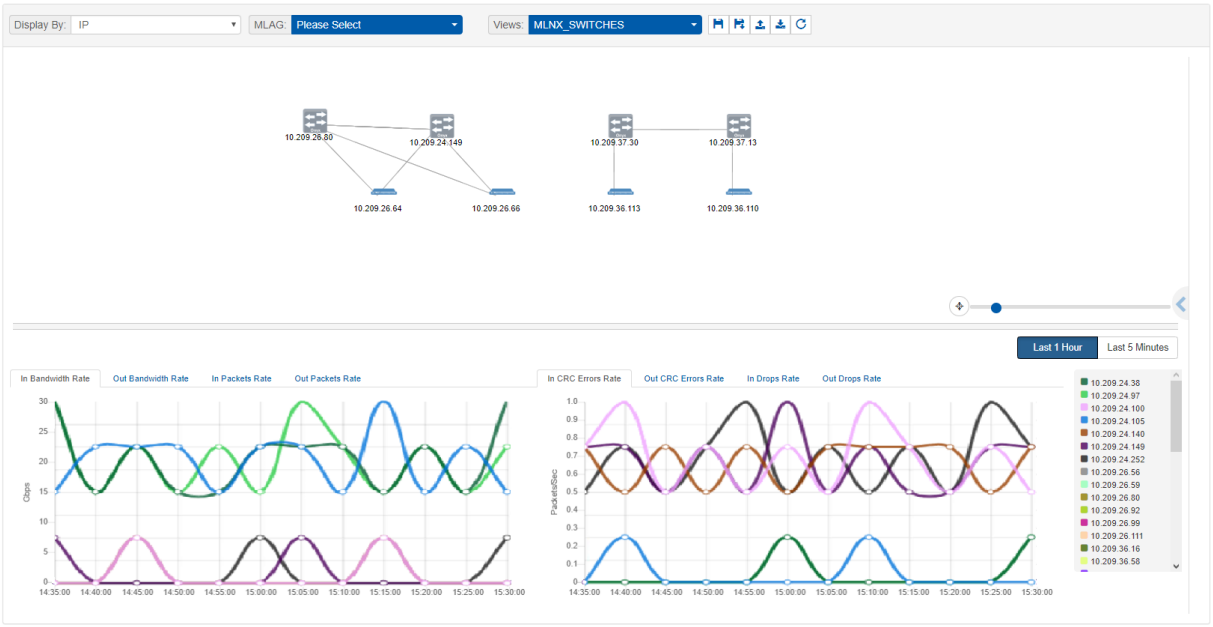
Link Monitoring displays telemetry data in the form of line charts and bar charts. There are 3 cases of monitoring:

1. No selection: All the switches that support monitoring are monitored.
2. A switch is selected: The ports of the selected switch are monitored.
3. A link is selected: The ports of the two devices making that link are monitored.

Monitoring All Switches

If nothing is selected, we perform telemetry of all the supported switches.

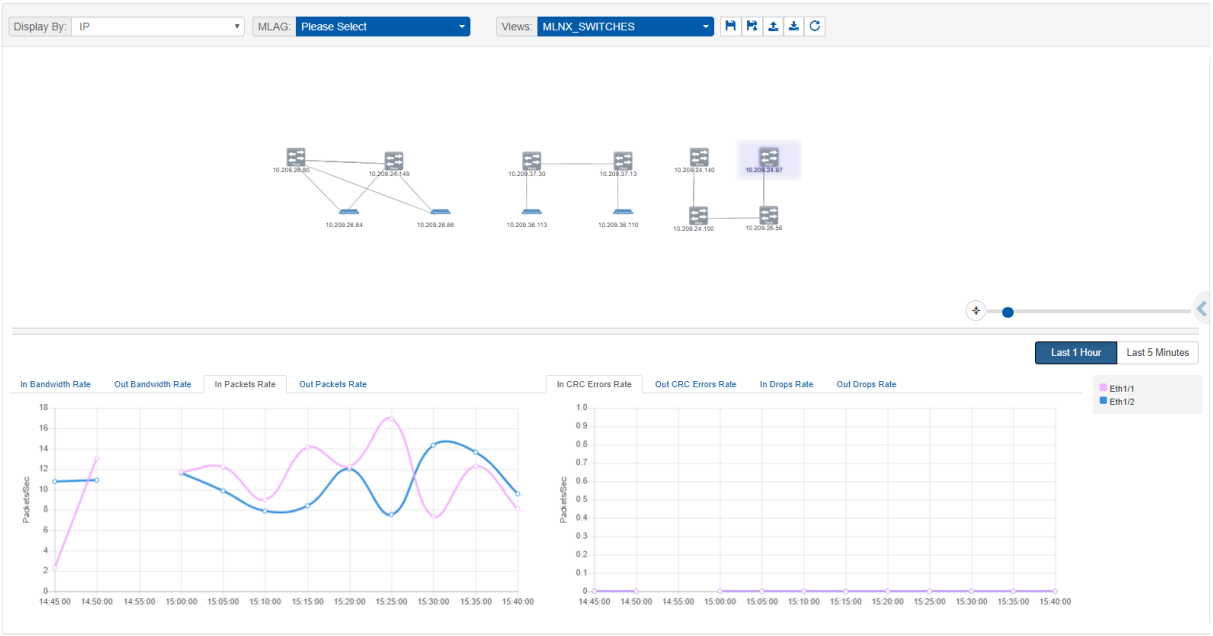
Network Map



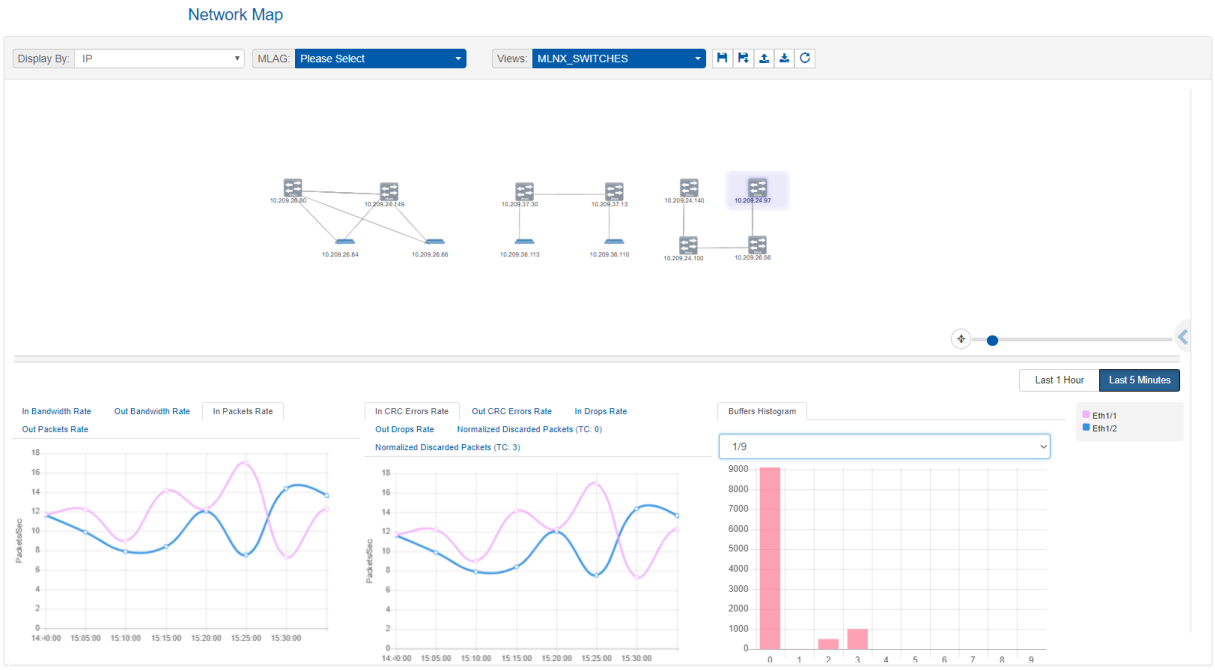
Switch Monitoring

When a switch is selected, all its running ports are monitored.

Network Map

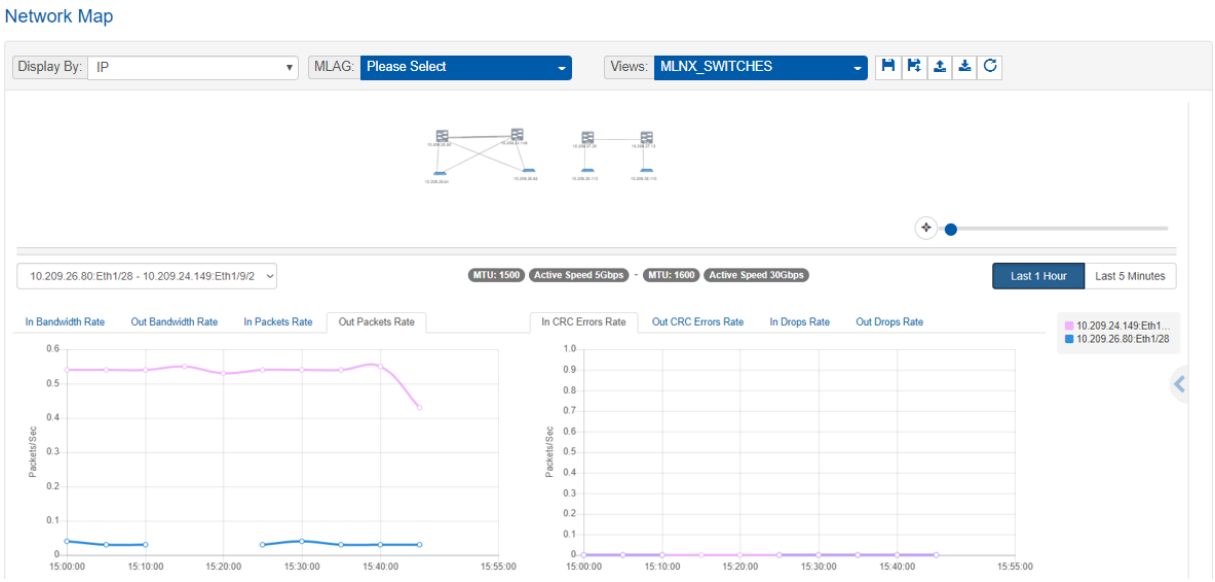


If you select the Last 5 Minutes mode, telemetry is streamed from the Telemetry Agent, and more counters are available.



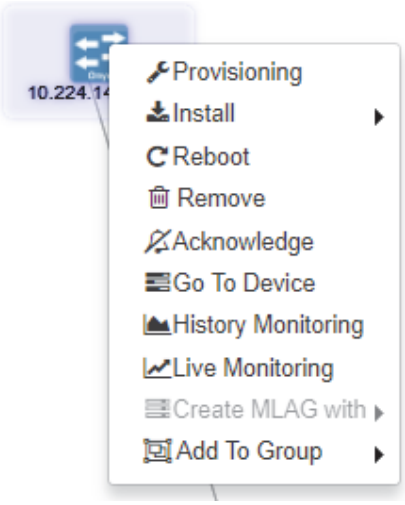
Link Monitoring

If a link selected, the ports of the two devices taking part in this link are monitored.



Running Operations

To run operations on more than one element in the map, hold the ctrl key down and select the elements, right-click on one of them and choose the action.



The level of severity of the devices' health state varies from OK to Critical, and is indicated by the device's icon color.

Devices' Severity Levels

Icon	Heath State
	Info/OK
	Error/Major
	Warning/Unknown/Degraded
	Critical

Views

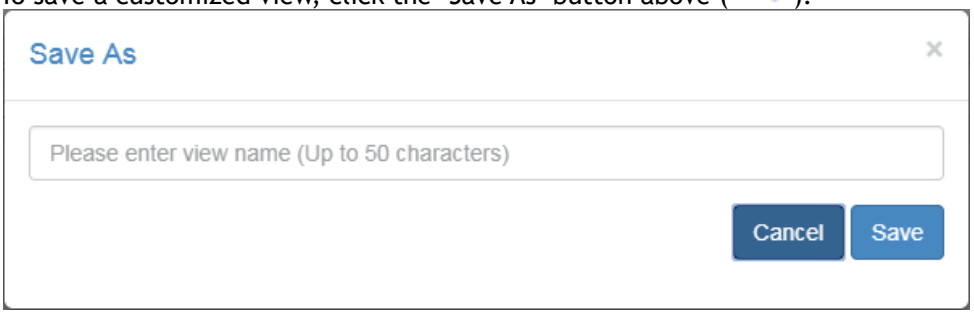
A view is a combination of a topology of nodes with (x, y) positions, filters state and Network Analysis state. By default, NEO offers a view (called "All Elements") which provides a multi-layer topology, based on either Spine-Leaf topology or user-defined tiers.

It is possible to save custom views with their own topology. The following parameters can be customized, saved in a view, and accessed later, on another machine or browser:

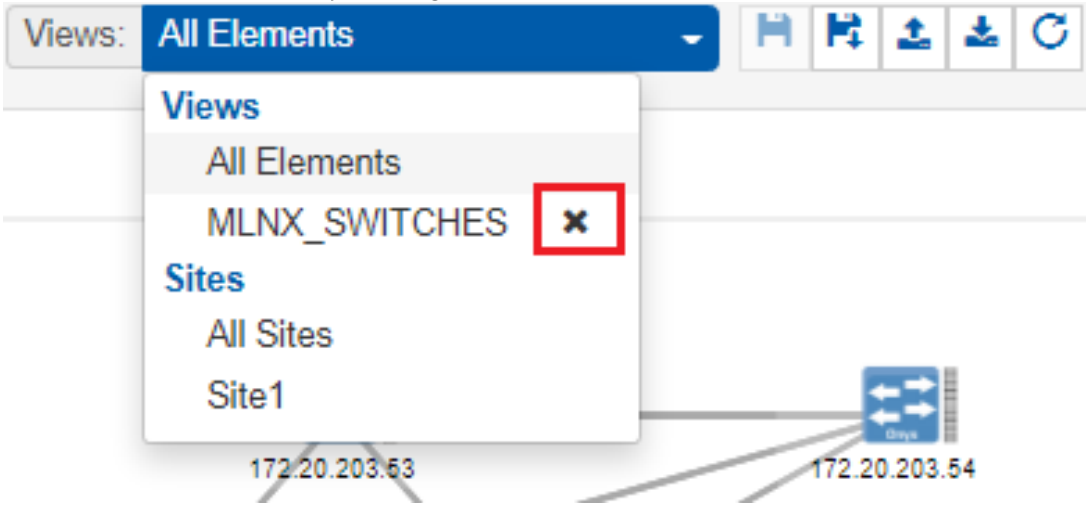
1. Systems positions in the map
2. VLANs filter selection
3. Type filters state
4. Severity filters state
5. Network Analysis state

Saving Customized Views

To save a customized view, click the "Save As" button above ( ).



After clicking “Save”, the view will be saved and can be accessed from the drop-down menu next to "Views". It can be deleted by clicking the “x” icon.



Note that the view can be edited by selecting it, modifying the filters, and saving it using the “Save” button ( ). The refresh button ( ) is used for reset.

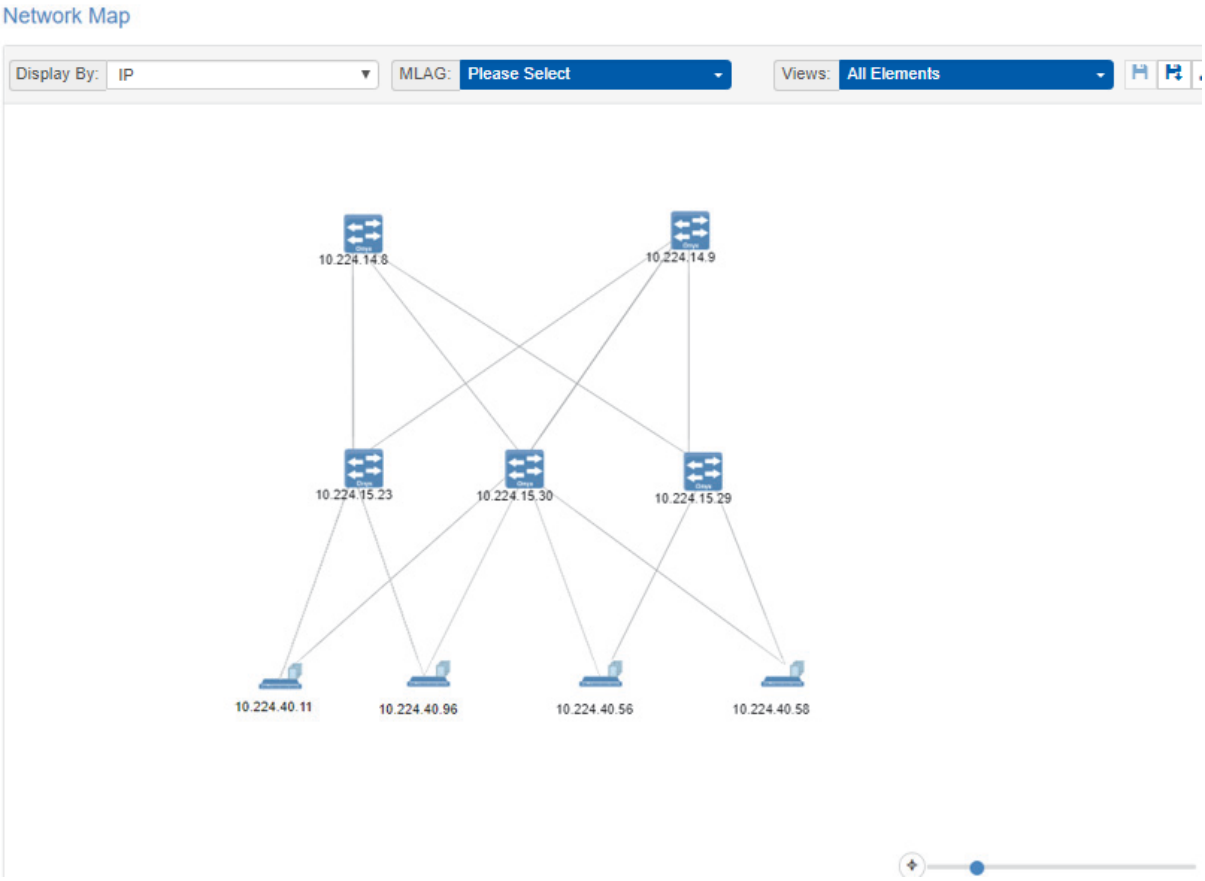
Network map layouts can be exported and saved to text files by clicking on the Export icon ( ). In addition, they can be exported from text files by clicking on the Import icon ( ). This allows the sharing of a layouts between different users.

All Elements View

In the All Elements View display type, the devices are shown in layers (tiers), for better understanding of the network. To select the All Elements view, click on the “Views” drop-down menu, and select “All Elements”.

Default All Elements View

This view follows the concept of Spine-Leaf topology, where the hosts are in the bottom line of a topology, the leaves are switches directly connected to those hosts, and the spines are switches connected to the leaves.



Sites View

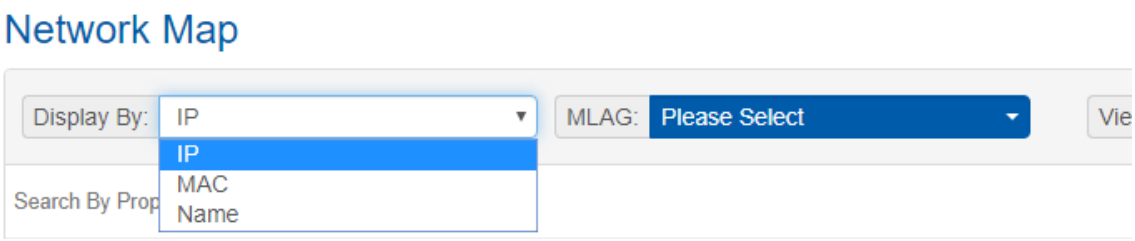
Sites, once configured under Managed Elements, can be viewed from the Network Map screen.

The color for each site indicates the worst status for a device in that site.

Map Options

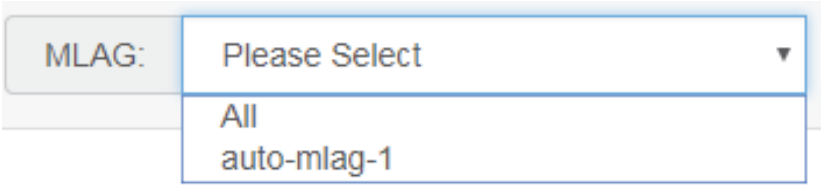
At the top of the Network Map panel, there are several View options:

- You can choose to display a device by its name or its IP address and search for it accordingly.

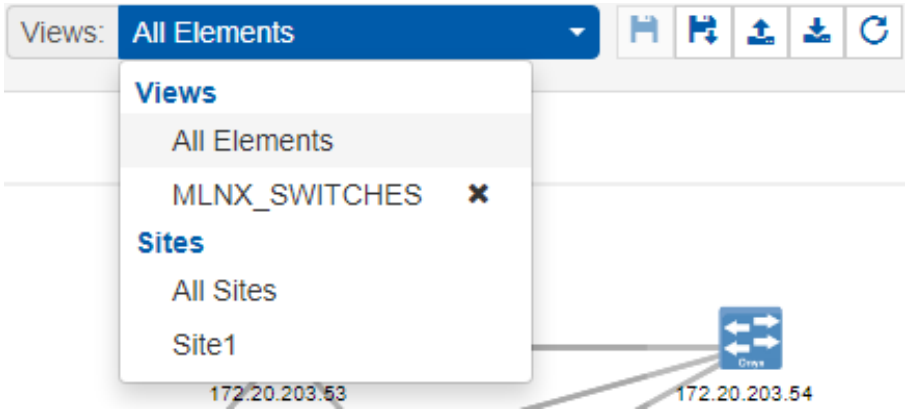


The device will be highlighted in the network map.

- MLAG visualization drop down menu: will only appear if there is one/more instances of MLAG service in NEO. MLAG members of the instance selected will be highlighted in the Network Map.



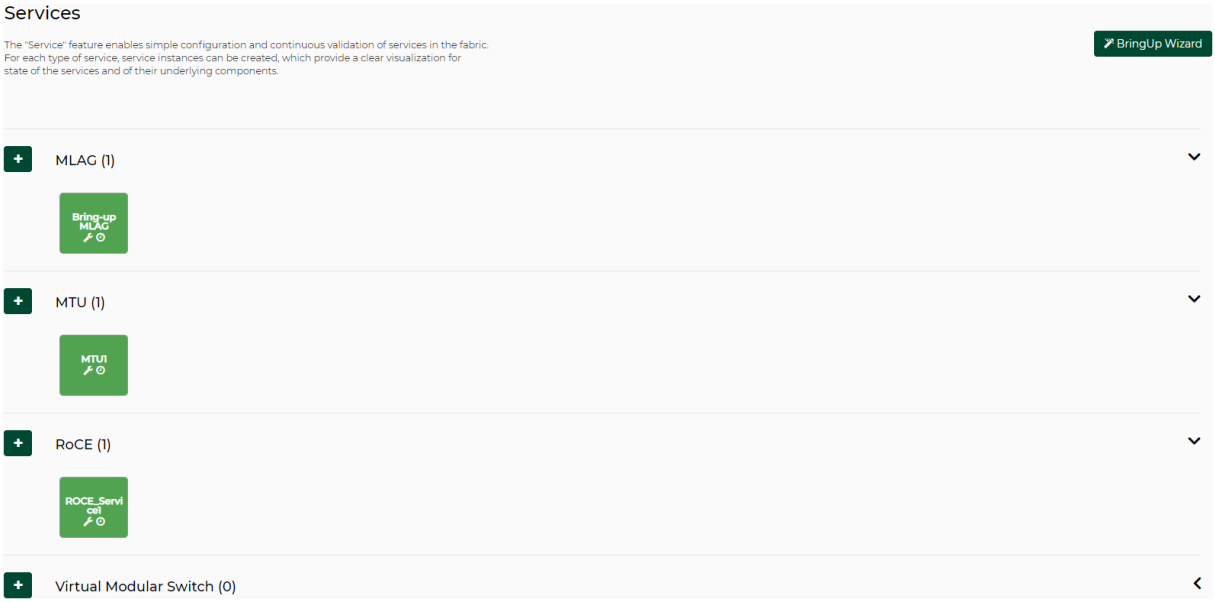
- Any change in the devices view using the filtering options can be saved using the “Save As” icon.



These new views can be saved and later accessed from the Views drop down menu.

Services

The Services window enables simple configuration and continuous validation of services in the fabric. For each type of service, service instances can be created providing a clear visualization for the state of the services and their underlying components. A bring-up wizard can further simplify the configuration of the network by allowing the user to provide in a few minimal steps all the input required for bringing up the network from scratch.



The five available service types are:

- Bring Up
- Virtual Modular Switch
    - VMS
    - L3 Network Provisioning
- MLAG

- MTU
- RoCE

The service types and configurations are divided in the Service view as seen in the figure above, and an Add button, as well as a help button, are available for each one of them.

> ⚠ The configuration and cleanup commands generated for the services assume that the switches have no prior configuration. Prior configuration may cause some of the commands to fail and lead to inconsistent configuration on the switches.

Bring-up Wizard

NEO enables a quick network bring-up that includes all the required configurations in one easy process. The user should only provide minimal input for the type of configurations needed in the bring-up wizard. All configuration steps are optional. Clicking “BringUp Wizard” will open the wizard for user input.

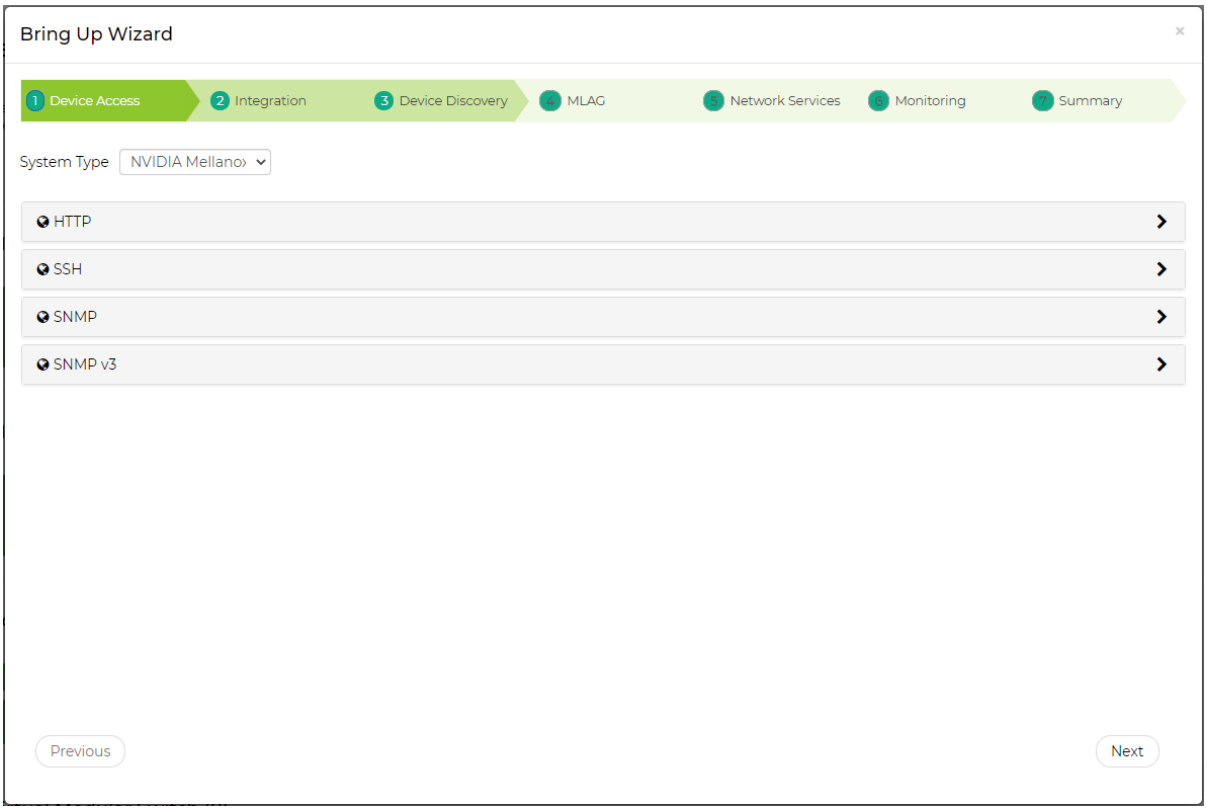
> ⚠ The wizard works on Onyx switch systems.

> ⚠ A configuration snapshot is taken for the devices participating in the bring-up before any configuration is done. This snapshot can be used to revert all the bring-up configuration changes.

Device Access

In this tab, the user can fill out the Device Access information for the device types participating in the bring-up.

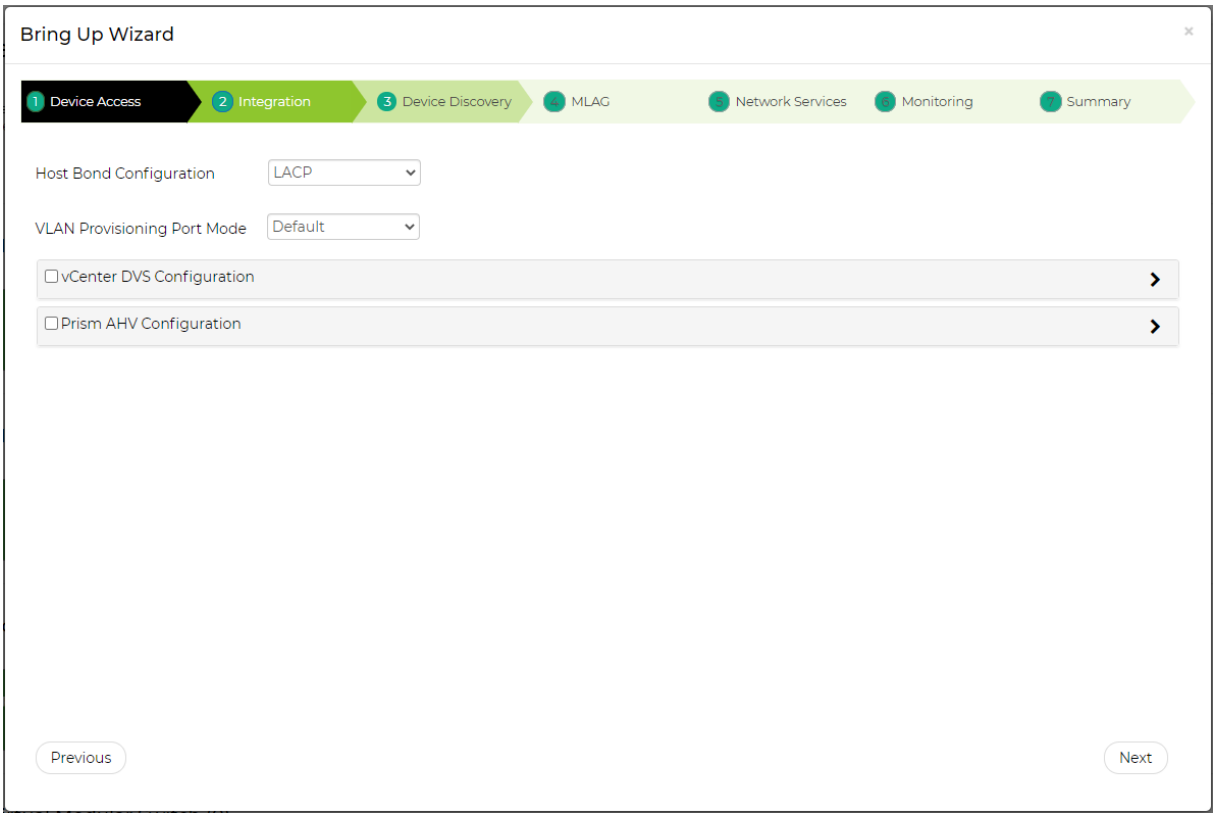
> ⚠ This updates the global credentials for the selected system type.



Integration

In this tab, the user can define integration with various hypervisors. This new capability helps NEO acquire information about the VMs running on them and handle VM lifecycle events to properly configure VLAN on the switches.

- Host Bond Configuration – the user can select the type of bonds that are being used on the hosts. If LACP bond configuration is used, NEO will suggest to create MPOs (see MLAG Port Channels) according to the links it detected on the switches.
- VLAN Provisioning Port Mode – the user can select which port mode to assign to the switch ports or MPOs (according what the user selected in the Host Bond Configuration section mentioned above). The options are hybrid, trunk, or default (which is to let NEO use the current switch port mode configuration). This is used when using NEO to handle VM lifecycle events and change switch VLAN configuration accordingly.



VMware vCenter DVS Configuration

In this section the user can define VMware vCenter connectivity information. NEO uses it to get information from the vCenter regarding VM information and lifecycle events.

The VLAN Provisioning drop down contains the following options:

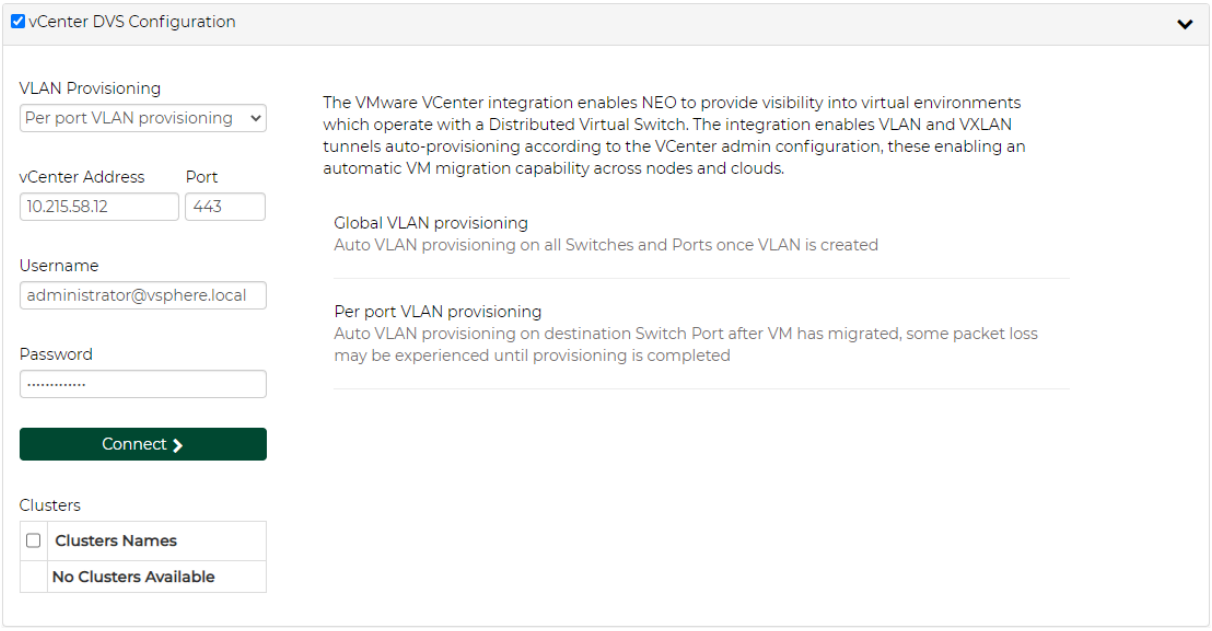
- Disabled – VM lifecycle events will not be handled. NEO will only retrieve VM information from vCenter.
- Global VLAN provisioning – NEO will listen to network events. In case of a network change event (e.g. adding or removing a network), NEO will add or remove VLANs to/from all switch ports. VLANs will be removed from the ports but will not be removed from the switch.

  > ⚠ This is the recommended VLAN provisioning mode when working with Live Migration. In this mode, the VLANs' auto-provisioning is performed upon network creation (before the VM migration event) therefore, it prevents traffic lose.

- Per port VLAN provisioning – NEO will listen to VM lifecycle events. In case of a VM change (e.g. VM added, removed or migrated) which required changes in VLANs, NEO will add or remove the VLAN accordingly from the relevant switch ports.

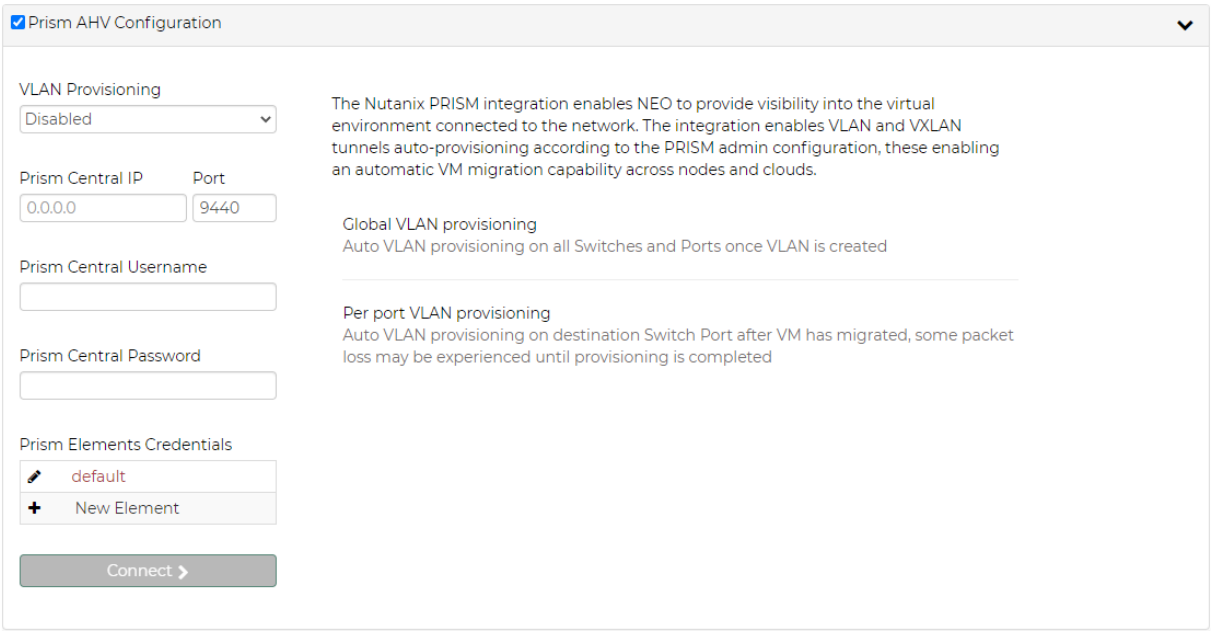
Upon filling the vCenter IP address, port, username and password, the user should click the Connect button to make sure the details are correct and NEO can connect the vCenter. If the connection is successful, a list of clusters managed by the vCenter will be shown in the Clusters table. The user should check the clusters he/she wants NEO to manage.

The Connect button should be clicked after every change so the new information will be processed by NEO.



Nutanix Prism AHV Configuration

In this section the user can define the Nutanix Prism Central and the Prism Element connectivity information. NEO uses it to get information from Prism regarding devices, VM information and lifecycle events. For further information, refer to Mellanox NEO/Nutanix Prism Plug-in.



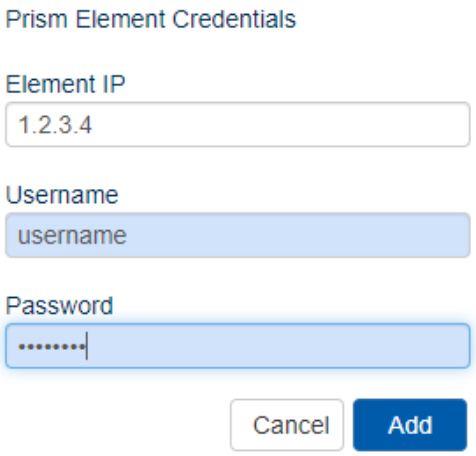
- The VLAN Provisioning drop down contains the following options:

- Disabled – VM lifecycle events will not be handled. NEO will only retrieve VM information from vCenter.
- Global VLAN provisioning – NEO will listen to network events. In case of a network change event (e.g. adding or removing a network), NEO will add or remove VLANs to/ from all switch ports. VLANs will be removed from the ports but will not be removed from the switch.

  > ⚠ This is the recommended VLAN provisioning mode when working with Live Migration.
  > In this mode, the VLANs' auto-provisioning is performed upon network creation (before the VM migration event) therefore, it prevents traffic lose.

- Per port VLAN provisioning – NEO will listen to VM lifecycle events. In case of a VM change (e.g. VM added, removed or migrated) which required changes in VLANs, NEO will add or remove the VLAN accordingly from the relevant switch ports.

- Prism Central - IP, port, username and password are used to connect to the Prism Central. In case of working without Prism Central, put the Prism Element details instead.

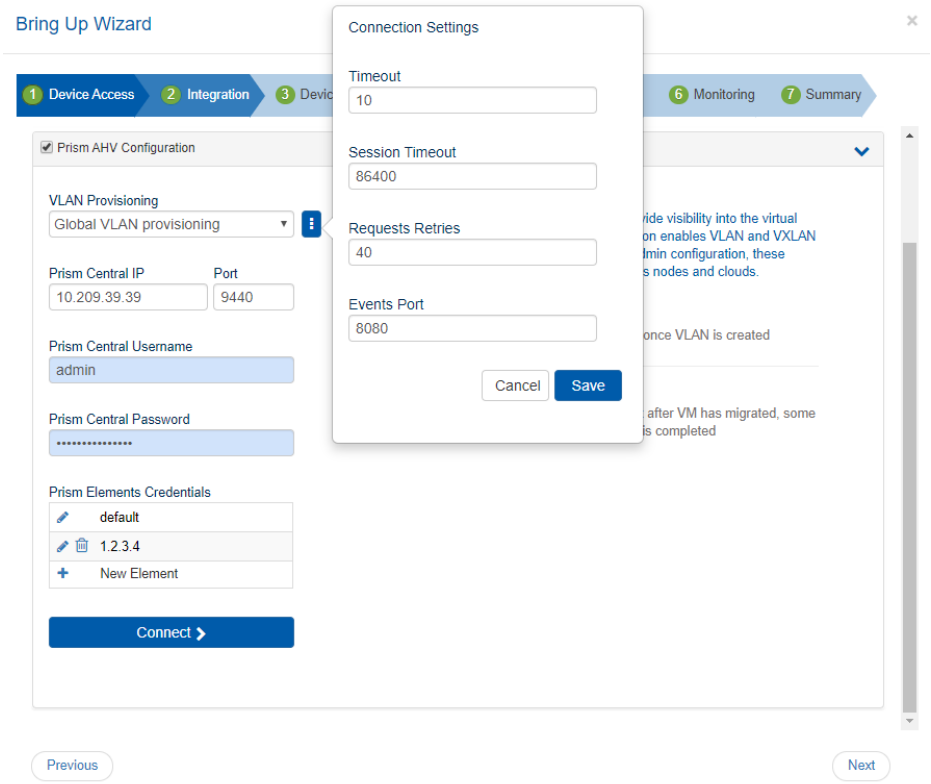


- Prism Elements Credentials – in this table the user should fill the username and passwords of each Prism Element in the network. Use “default” to fill the same credentials to all Prism Elements or specify credentials per Prism Element IP.

Upon filling the Prism Central IP address, port, username and password, and the Prism Element credentials, the user should click the Connect button to make sure the details are correct and NEO can connect the Prism. If the connection is successful, the switches and Nutanix hosts known to Prism will be added to NEO. This might take a couple of minutes.

> ⚠ The Connect button should be clicked after every change so the new information will be processed by NEO.

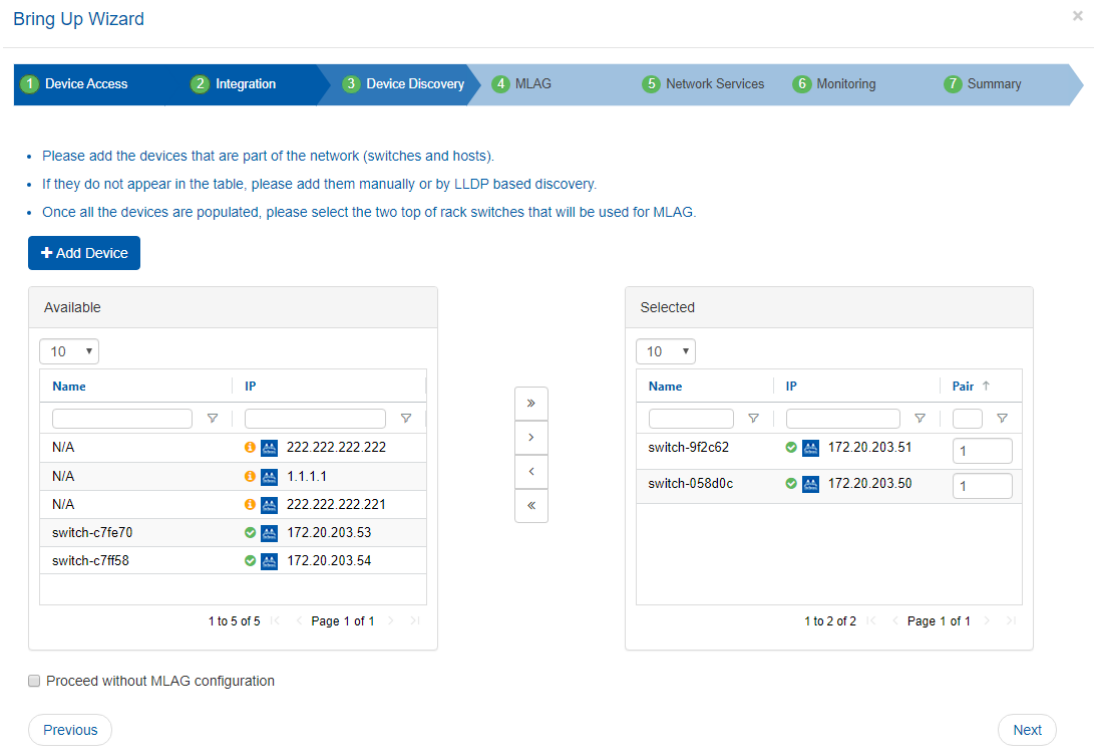
When enabling VLAN provisioning, the user can also set some advanced properties that affect the communication with Prism:



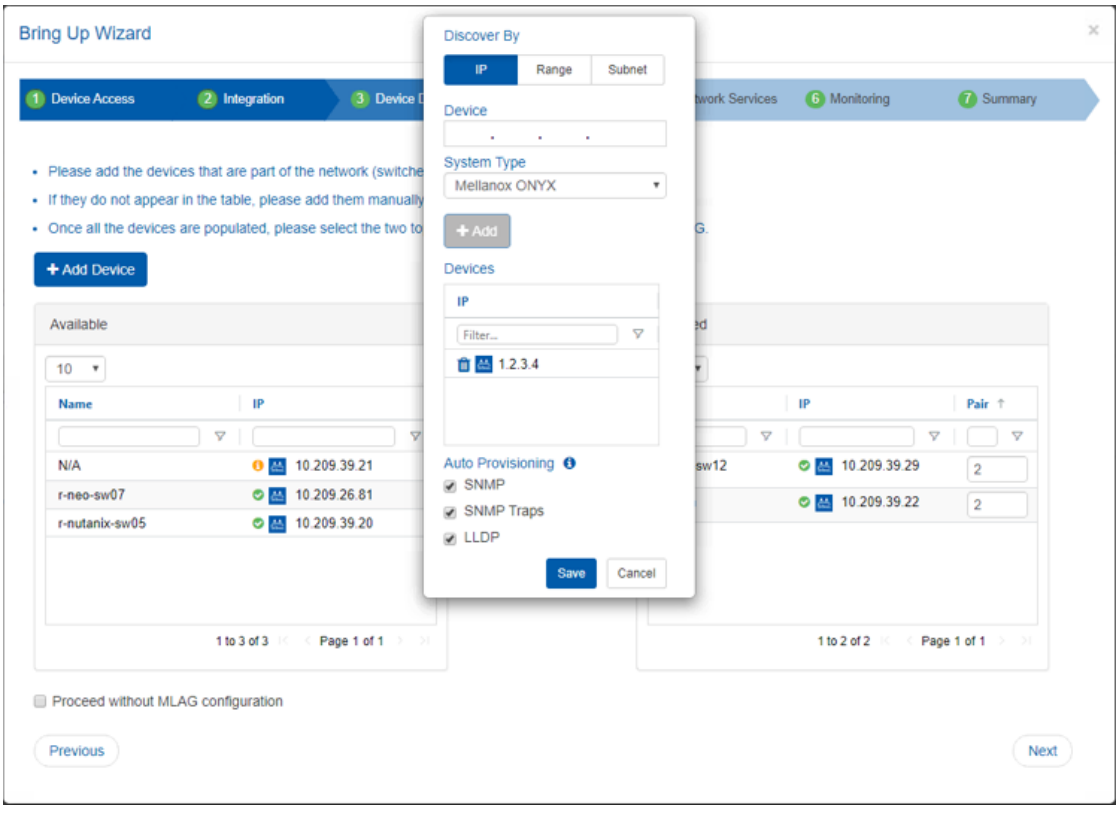
Device Discovery

In this tab, the user can fill out the switches needed to be configured. The switches are organized in pairs, so MLAG can be created from each pair. Mellanox NEO® can automatically detect MLAG switch pairs that fulfill the connectivity prerequisites and move them to the “Selected” table.

> ⚠ MLAG configuration may be skipped by using the "Proceed without MLAG configuration" checkbox, and selected devices can be configured with MTU and ROCE in the Network Services step.

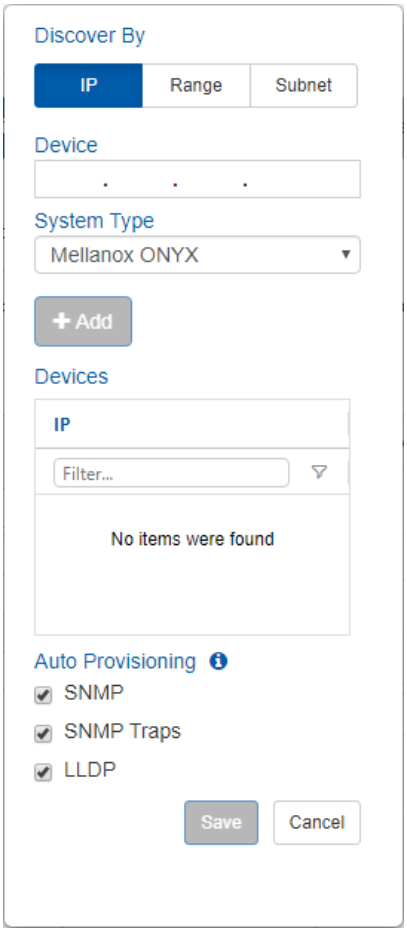


If the switches are not listed, the user can click “Add Device” and add them.

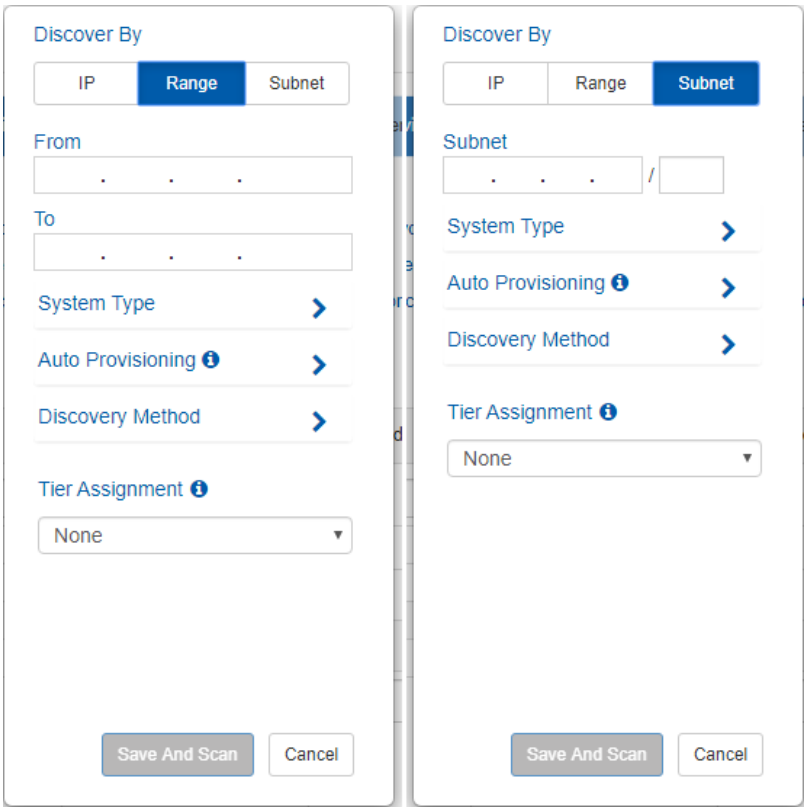


Devices can be added by their management IP address (click the  button to add them to the list). When done, click the “Add Devices” button. In case only one switch is known by NEO, NEO will try to discover switches linked to this switch using LLDP. If you want to use this ability, please make

sure that LLDP protocol is enabled on your switches. once LLDP results are retrieved, relevant switch IP will be automatically populated.



Alternatively, the user can specify a range of IPs or subnet IP to scan (see also Discovery Settings) and click the "Save and Scan" button to start scanning.

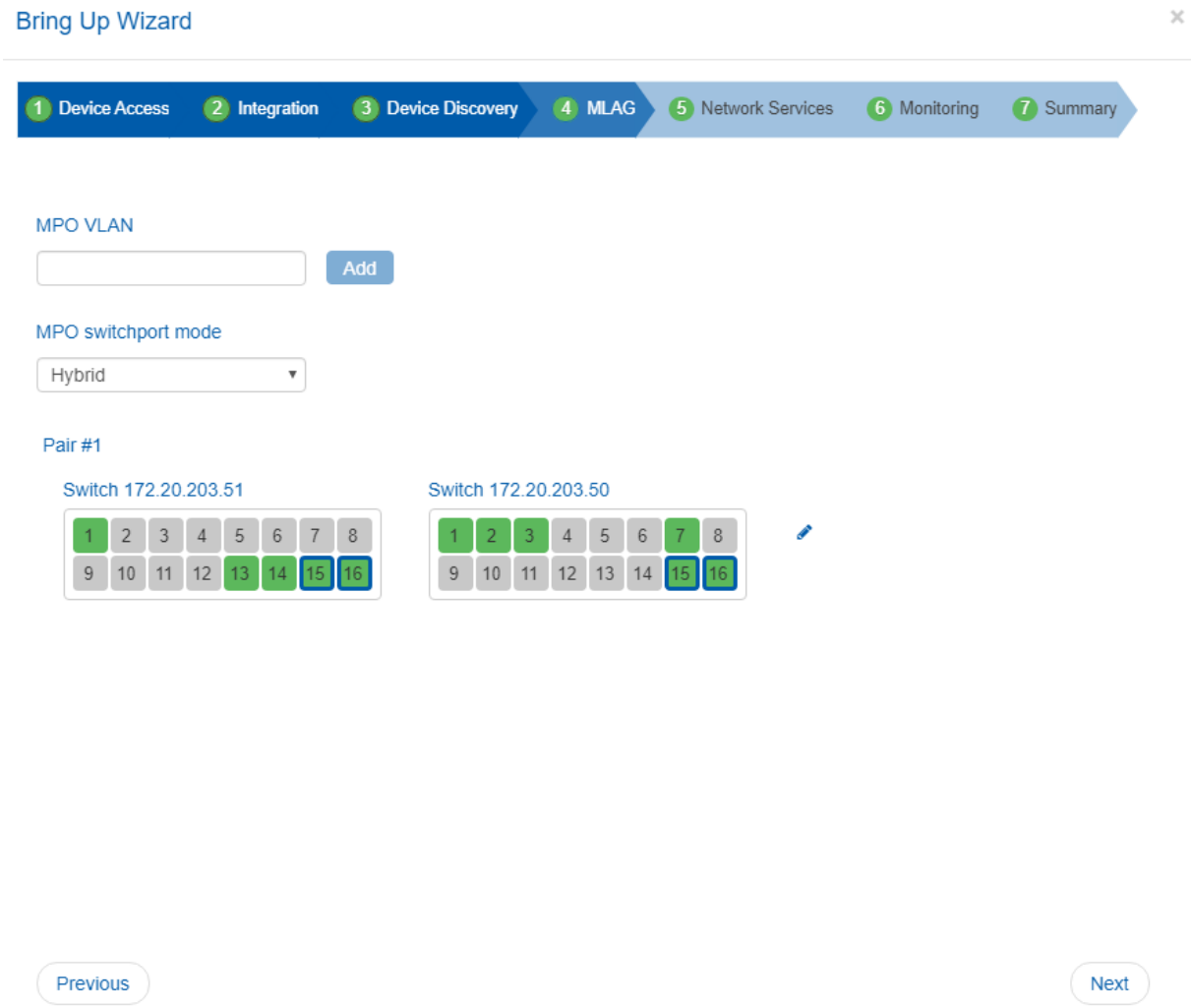


After adding the devices in any of the above methods, they will undergo a short discovery cycle to get the required data and then will be available for the bring-up.

MLAG

The MLAG tab defines the necessary information for MLAG configuration in the selected switch pair.

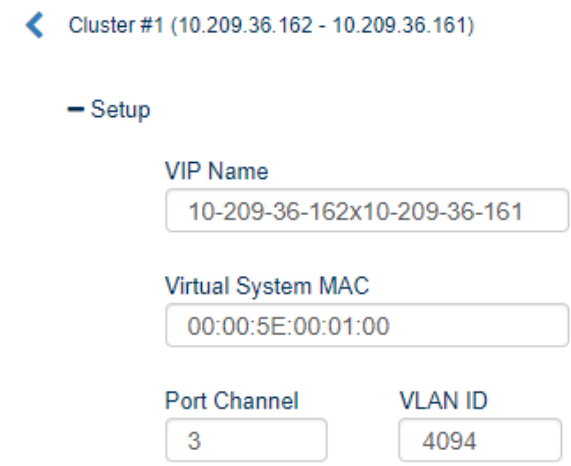
- The MPO VLAN field allows the user to add VLANs (networks) to all switch pairs in one click.
- The MPO switchport mode field sets the default switchport mode that will be used for MPOs defined in each MLAG pair. The user can change specific MPOs to other values if necessary.



For each pair, the user can select the ports that will be part of the MLAG IPL. The ports that NEO identified as linking the two switches are automatically selected. Clicking the button will allow the user to set other MLAG related attributes.

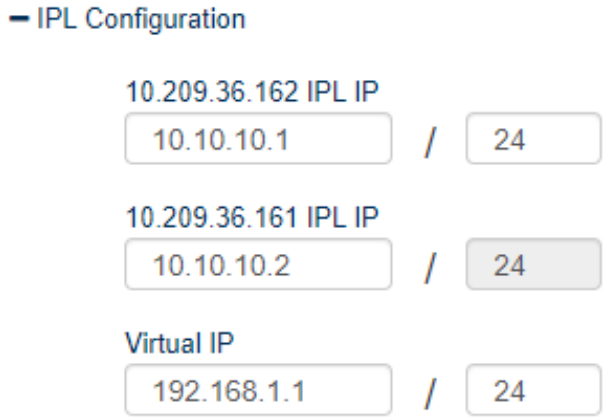
Setup

This section defines MLAG attributes:



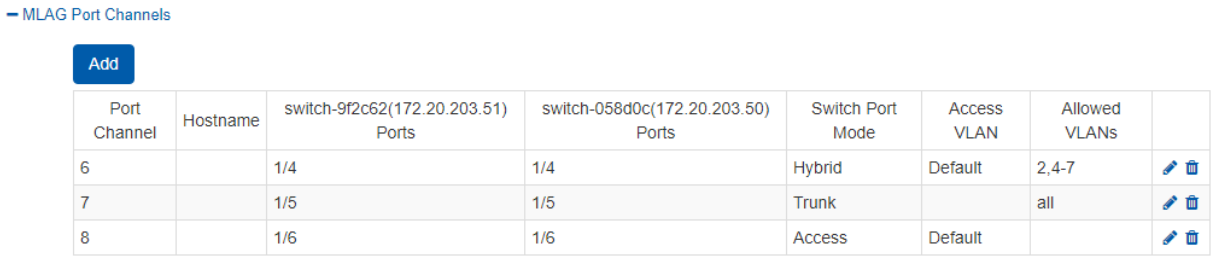
IPL Configuration

This section defines MLAG IPL attributes:



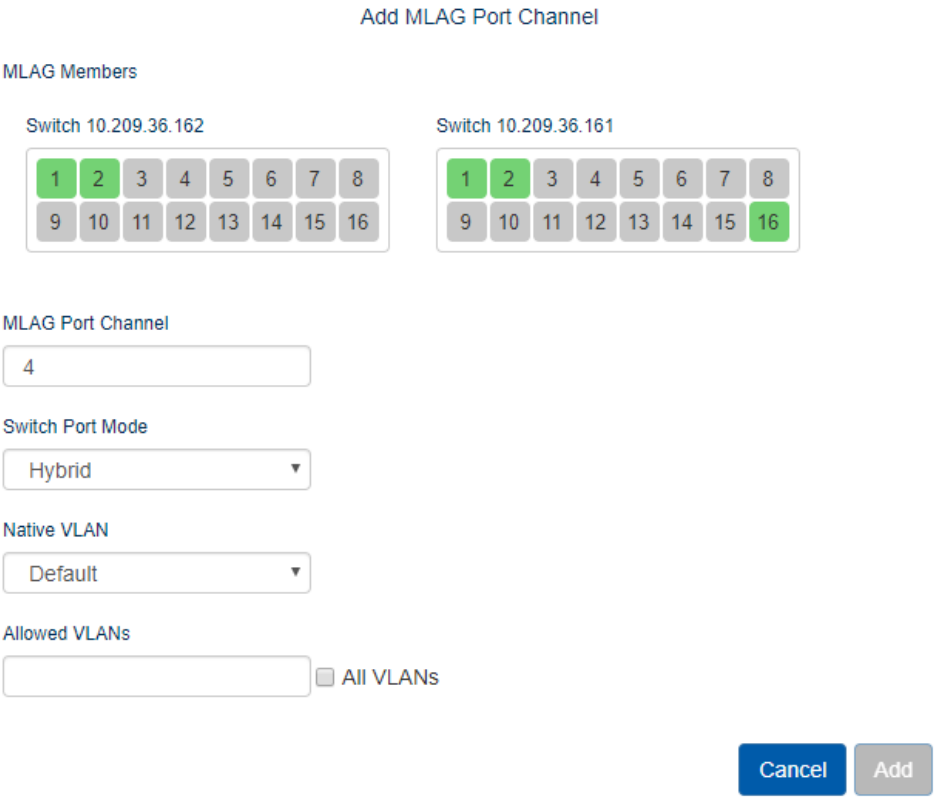
MLAG Port Channels

This section defines MPOs to configure on the switch. If you are using LACP bond mode configuration, Mellanox NEO will auto-populate the table with any host linked to both switches in the pair.



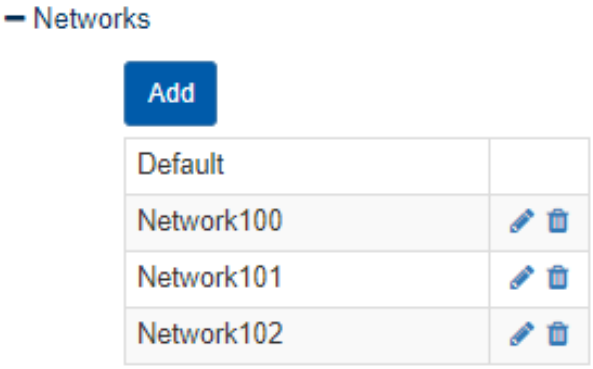
Port Channel	Hostname	switch-9f2c62(172.20.203.51) Ports	switch-058d0c(172.20.203.50) Ports	Switch Port Mode	Access VLAN	Allowed VLANs	
6		1/4	1/4	Hybrid	Default	2,4-7	
7		1/5	1/5	Trunk		all	
8		1/6	1/6	Access	Default		

The user can add or change MPOs according to the required network configuration.

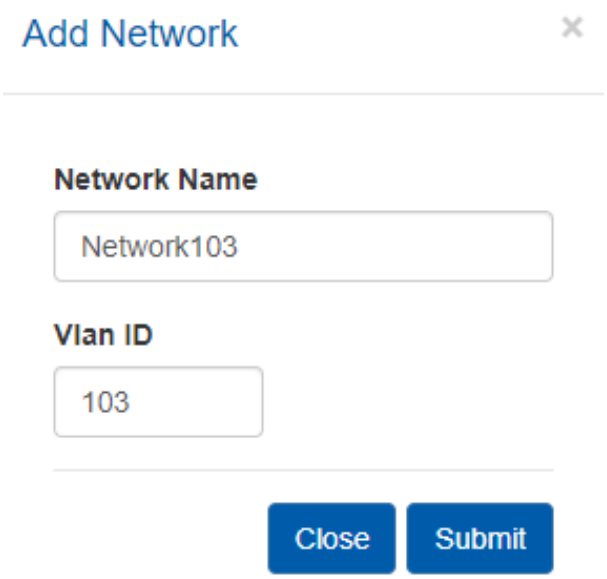


Networks

This section defines layer 2 networks (VLANs) to configure on the switch. A default network with VLAN 1 is automatically added and is the default for MLAG port channel native VLAN definition.

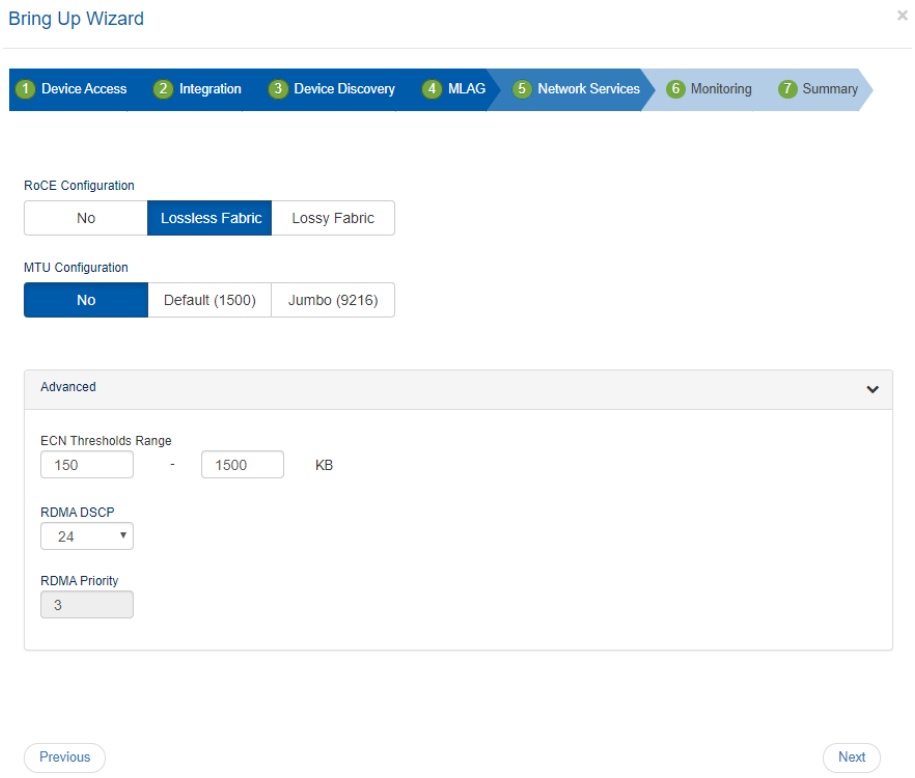


Add a network by clicking the “Add” button and setting its name and VLAN ID:



Network Services

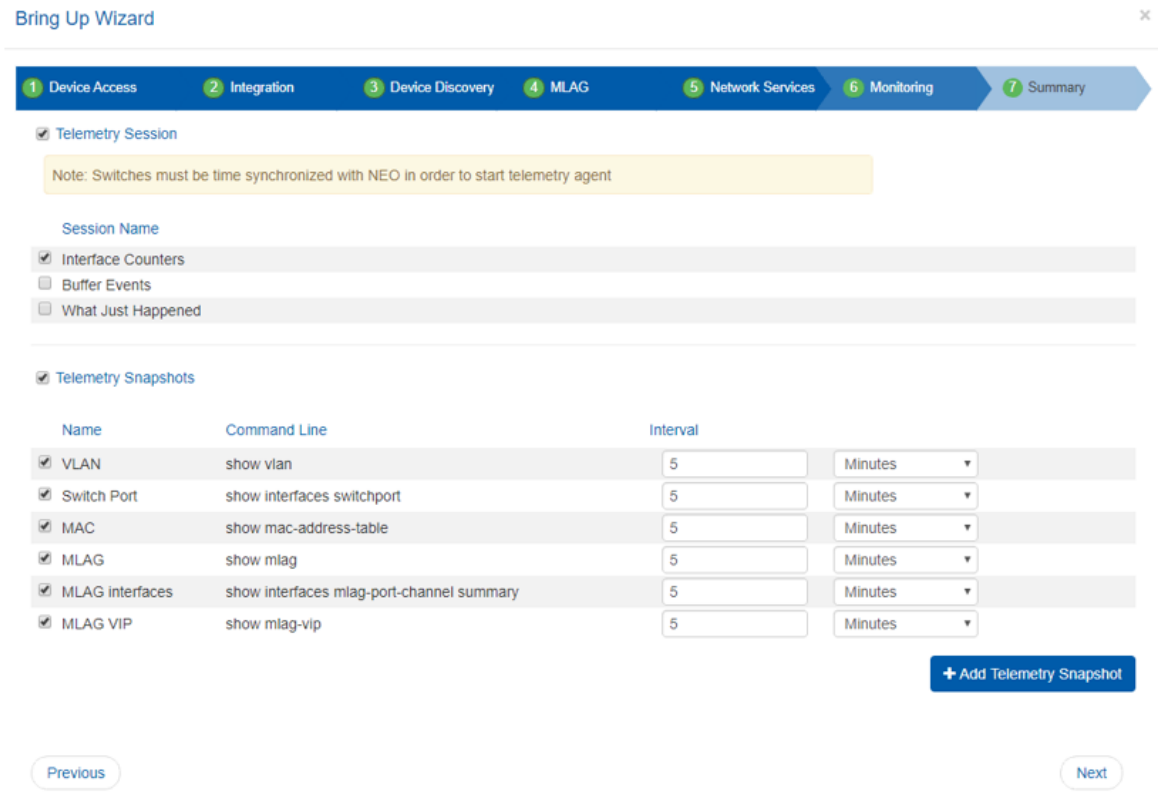
In this tab, the user can specify RoCE and MTU definitions. If RoCE is required, the user can define in the advanced section ECN thresholds and the priority to use for RoCE traffic.



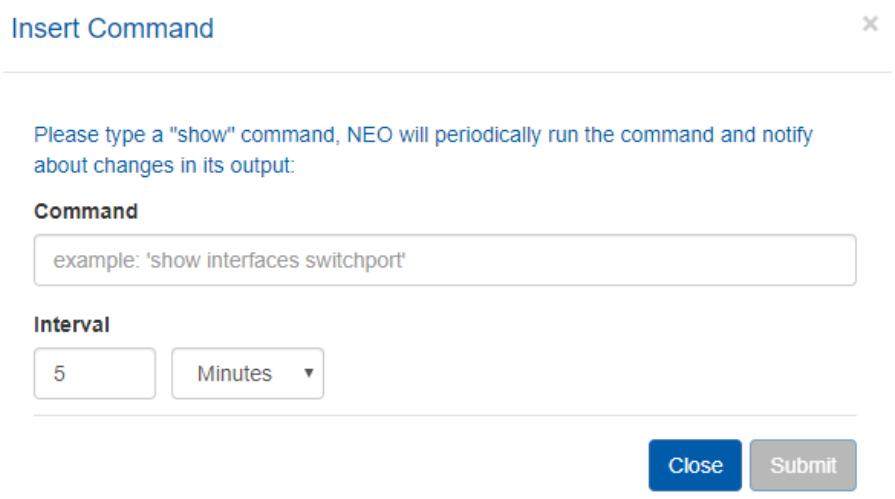
Monitoring

In this tab, the user can define the telemetry means for monitoring the network configuration and traffic behavior. In the top section, the user can decide whether or not to deploy the telemetry agent on the switches (top checkbox), and if so, which telemetry sessions to use.

For more information on Telemetry Agent and Sessions see Telemetry Streaming.

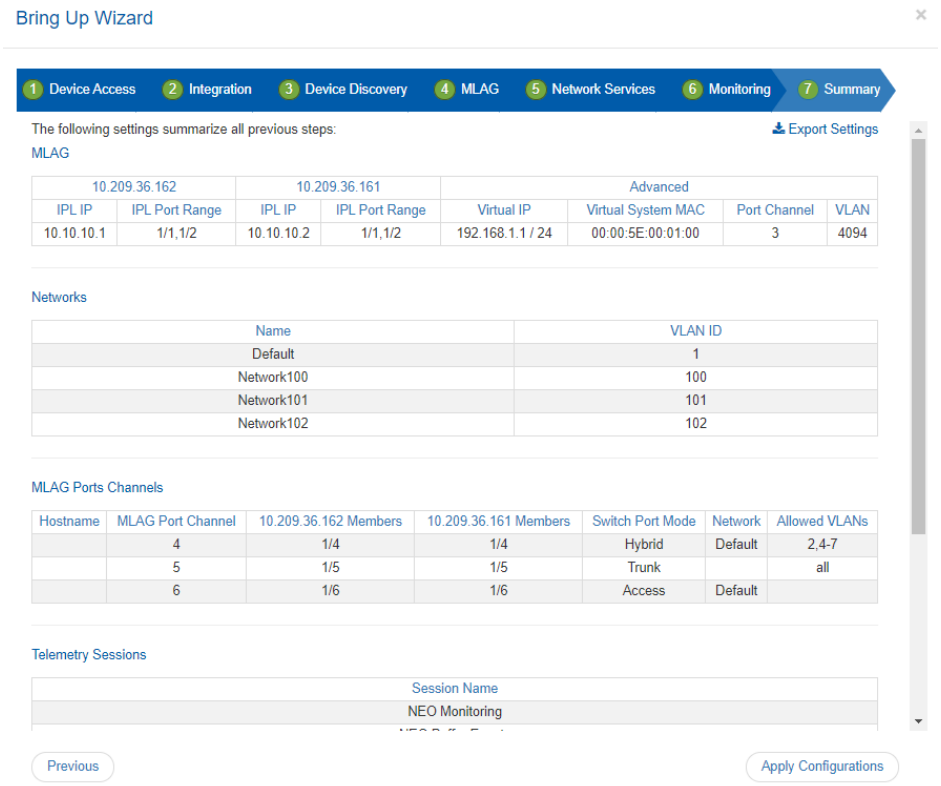


In the bottom section, the user can select which telemetry snapshots to enable. These will run a show command periodically and the user will be notified when the output will change. Clicking “Add Telemetry Snapshot” allows the user to add his own show command:



Summary

In this tab, the user can see a summary of all the definitions that are going to be configured on each switch pair.



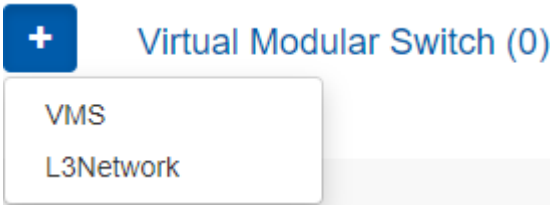
Clicking “Apply configuration” will start the configuration process, which can take a couple of minutes. You can track the progress in the bring-up progress dialog and in the jobs page. For MLAG, RoCE and MTU configurations, service objects will be created and used to apply the required configuration on the switch pairs (see section Service Elements for more information). Telemetry actions (agent deployment and session configuration) will be done after the services are configured.

In case the MLAG configuration failed, the bring-up will not continue to the next phases. After failures in other phases NEO will try to continue with the bring-up process.

Service Types

Virtual Modular Switch

A drop-down menu will appear, allowing the user to select two types of services when clicking the "+" button:



VMS

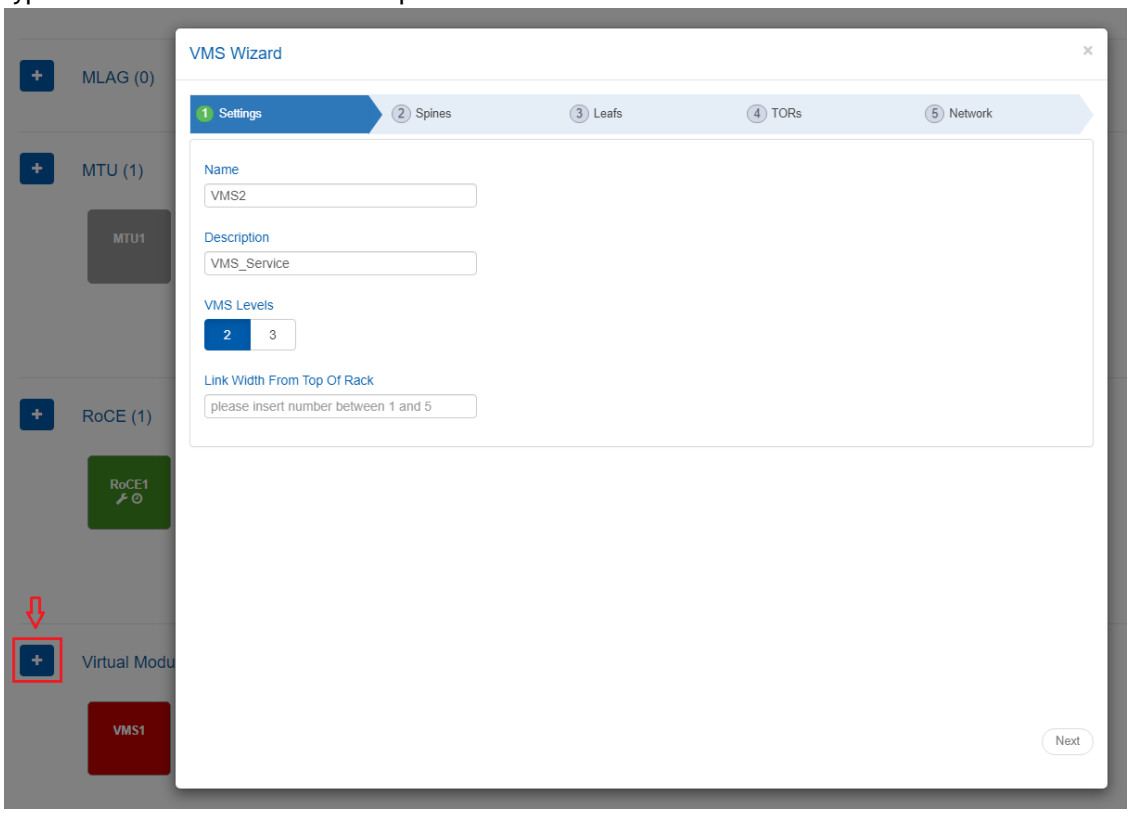
> Before setting up VMS using the NEO VMS service, it is highly recommend to review the information and prerequisites found in Mellanox Virtual Modular Switch™ Reference Guide.

Mellanox Virtual Modular Switch® (VMS) solution, comprised of Mellanox 10GbE, 40GbE, and 56GbE fixed switches, provides an ideal and optimized approach for a fixed switch aggregation. VMS is energy efficient and scales up to 28.8Tb/s of non-blocking bandwidth and up to 720 nodes of 40GbE and operates at ultra-low latencies. The VMS can be set up in Layer 3 mode (L3-VMS) based on OSPF. VMS configuration and bring-up can be fully automated, from the early planning stages until it is operational, by leveraging the VMS Wizard. The VMS Wizard provides an automation environment to provision the fabric with a centralized application, an application that learns the way the switches interconnect and how they ought to operate in the data center. Once the fabric size is defined and the types of switches in the fabric are selected, the VMS Wizard specifies how to configure the switches. After installation, the wizard verifies the connectivity and applies the configuration to the switches.

In order to configure the VMS solution:

1. Click the “Add” button on the right side of the VMS row.

2. Type the service name and description under “General”.



Select the number of tiers (VMS Levels – 2 or 3).

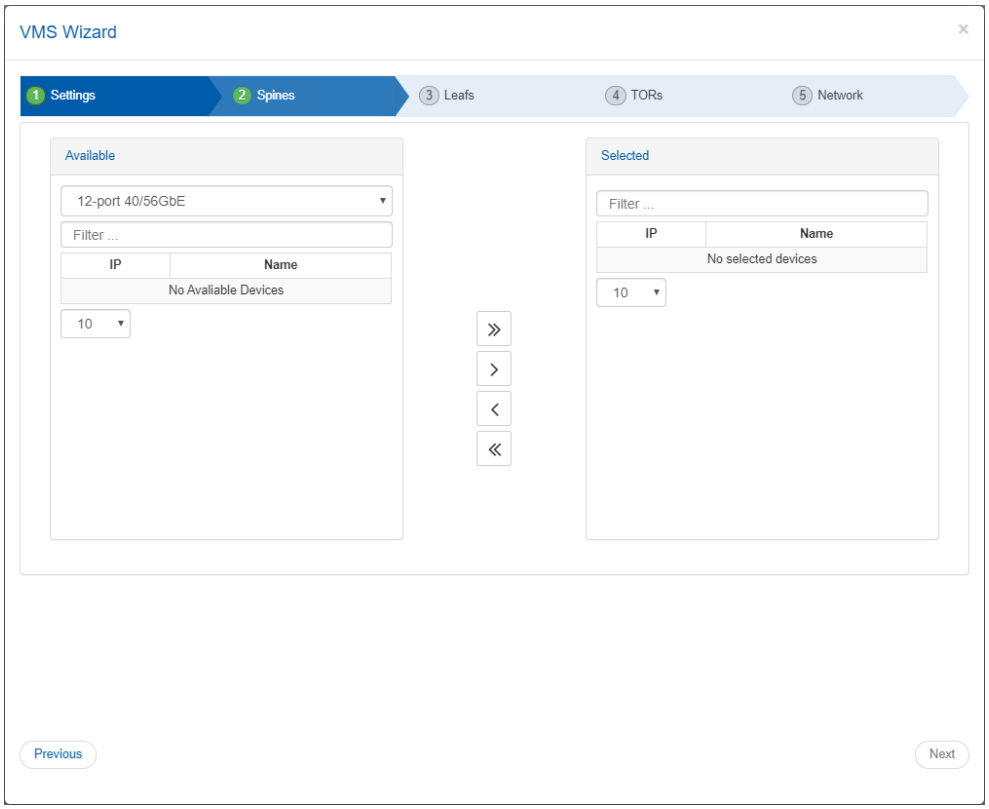
> ⚠ For 2 levels only (Spines and TORs), select 2. For 3 levels (TORs, Leafs and Spines), select 3.

Unlike the 2 levels choice, if you select 3 levels, you will be given more options, as can be seen in the figure below. You will also be requested to fill out the Leafs tab.

a. Link width from top of rack – The number of cables from each TOR to Leaf
b. Uplink from top of rack – The number of Leafs connected to each TOR
c. Link width from Leafs – The number of cables from each Leaf to Spine

> ⚠ For further information on the VMS topology, you may refer to the VMS Reference Guide at www.mellanox.com, under Products -> Ethernet Switch Systems -> VMS.

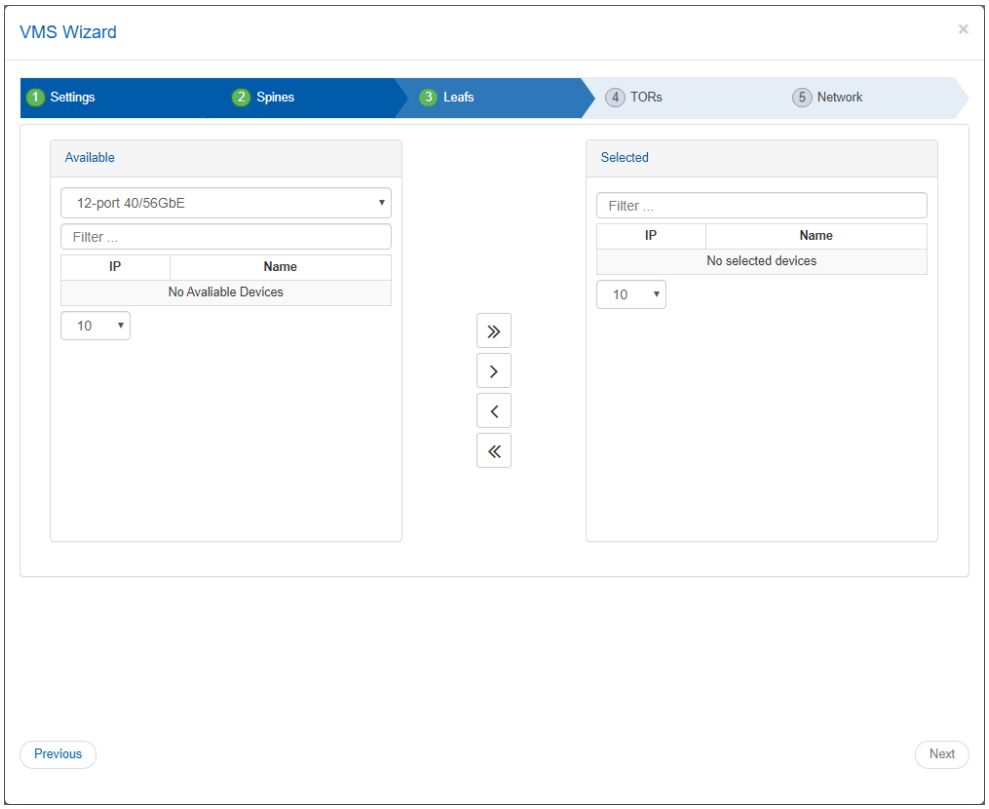
3. Select the switch members of Spines after choosing the number of ports. The available options for this tier are 12 and 36 ports. For further information on these options, please refer to "Supported Switches per Tier".



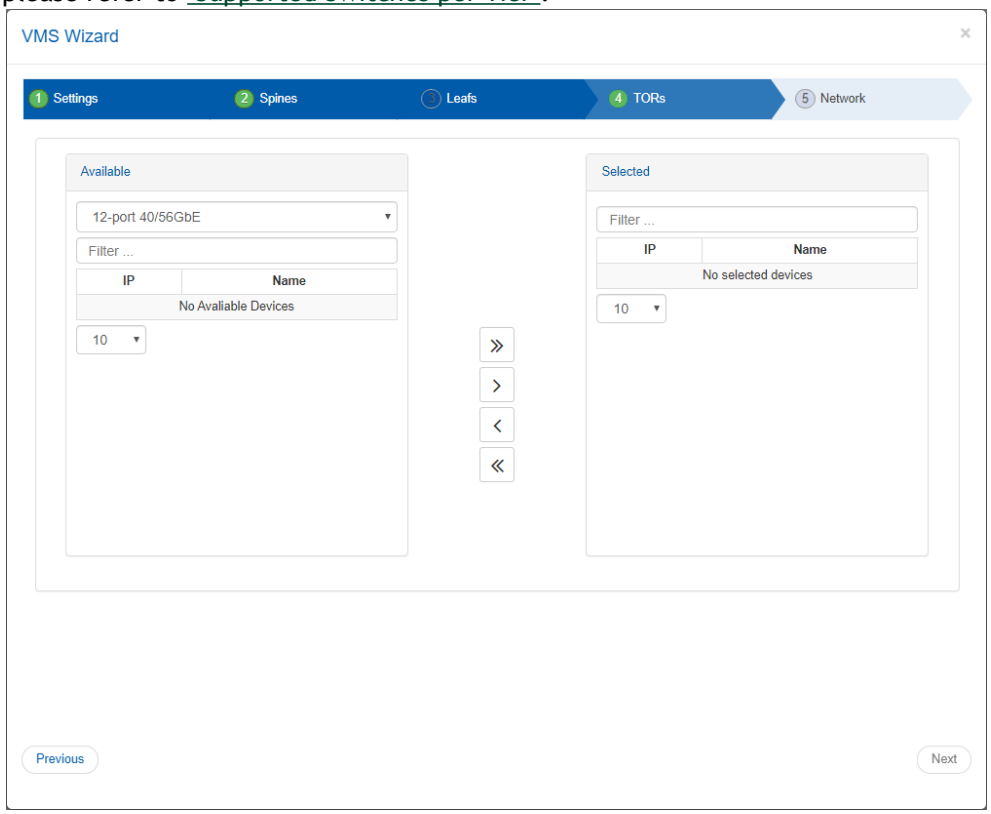
Supported Switches per Tier

Number of Ports	Switch Family	Supported Tier/s
12 ports	MSN2100	TOR/Leaf/Spine
32 ports	MSN2700, MSN3700	TOR/Leaf/Spine
48+8 ports	MSN2410	TOR

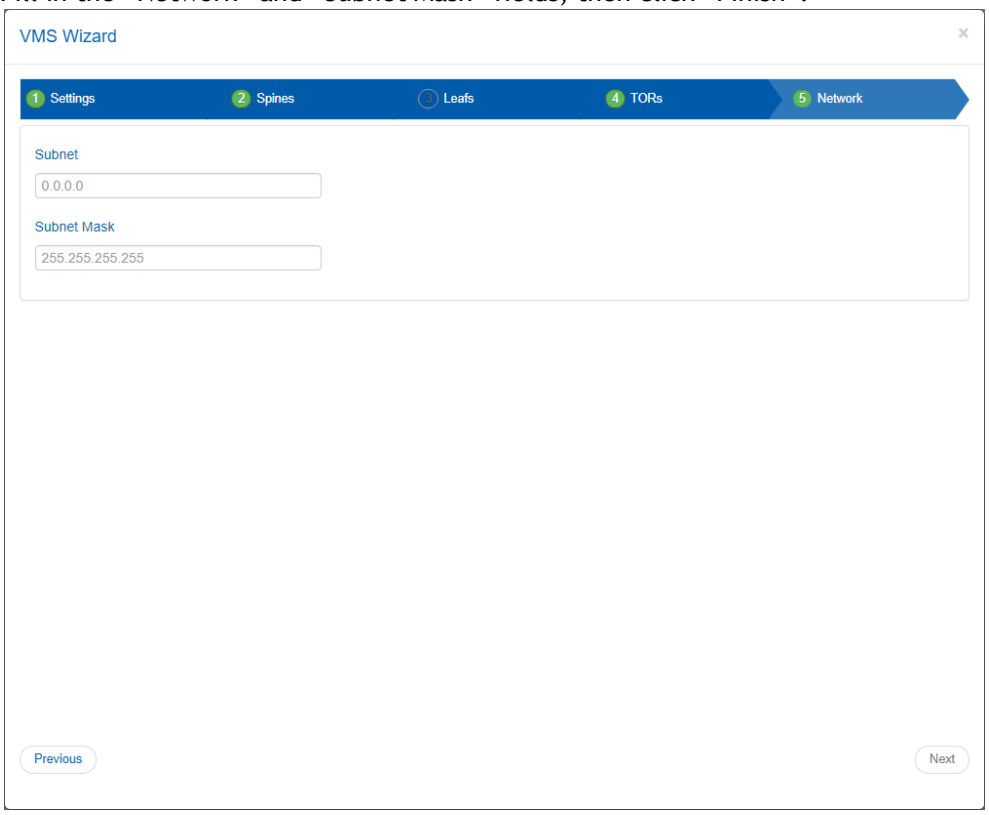
4. Select the switch members of Leafs after choosing the number of ports. The available options for this tier are 12 and 32 ports. For further information on these options, please refer to Supported Switches per Tier.



5. Select the switch members for TORs after choosing the number of ports. The available options for this tier are 12, 32, and 48+12 ports. For further information on these options, please refer to "Supported Switches per Tier".

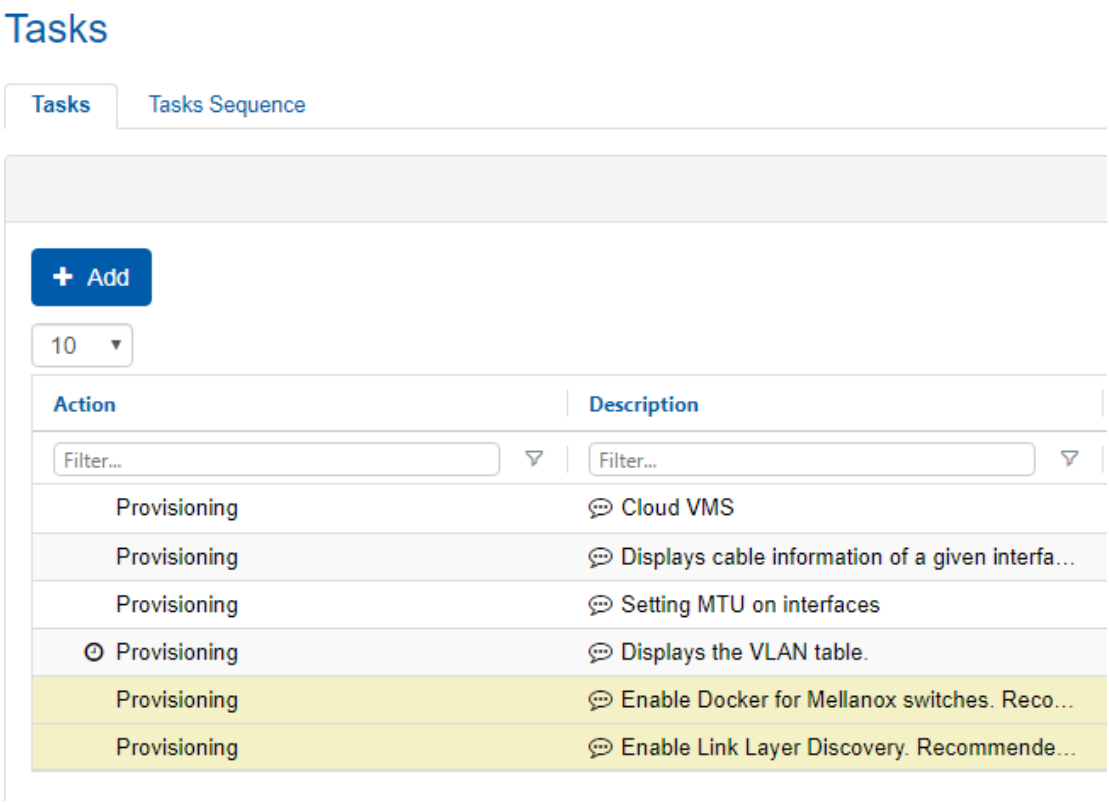


6. Fill in the “Network” and “Subnet Mask” fields, then click “Finish”.



Once clicked “Finish”, a service instance will be created and a service element will appear on the Services main page. A right click on a service element will enable performing different operations. For information on the operations and the service instances in general, please refer to “Service Elements”. A task for the VMS configuration will also be created when clicking “Finish”, as described in the step below.

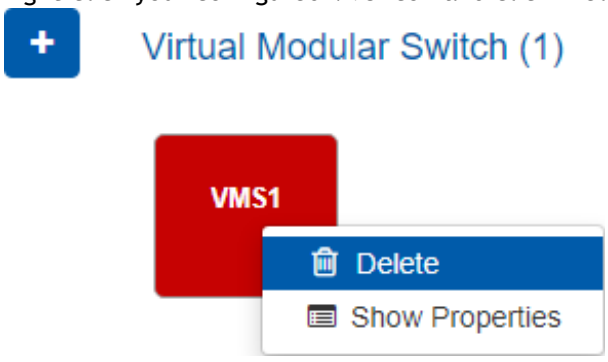
7. A task that contains all the VMS configurations to all switches will be created. Right-click the task and select “Run” to configure all the switches that are part of the VMS.



⚠ If the selected switches are not connected as a fat tree, Mellanox NEO will not create the task and will send an error message.

In order to delete a configured VMS service:

1. Right-click your configured VMS icon and click "Delete".



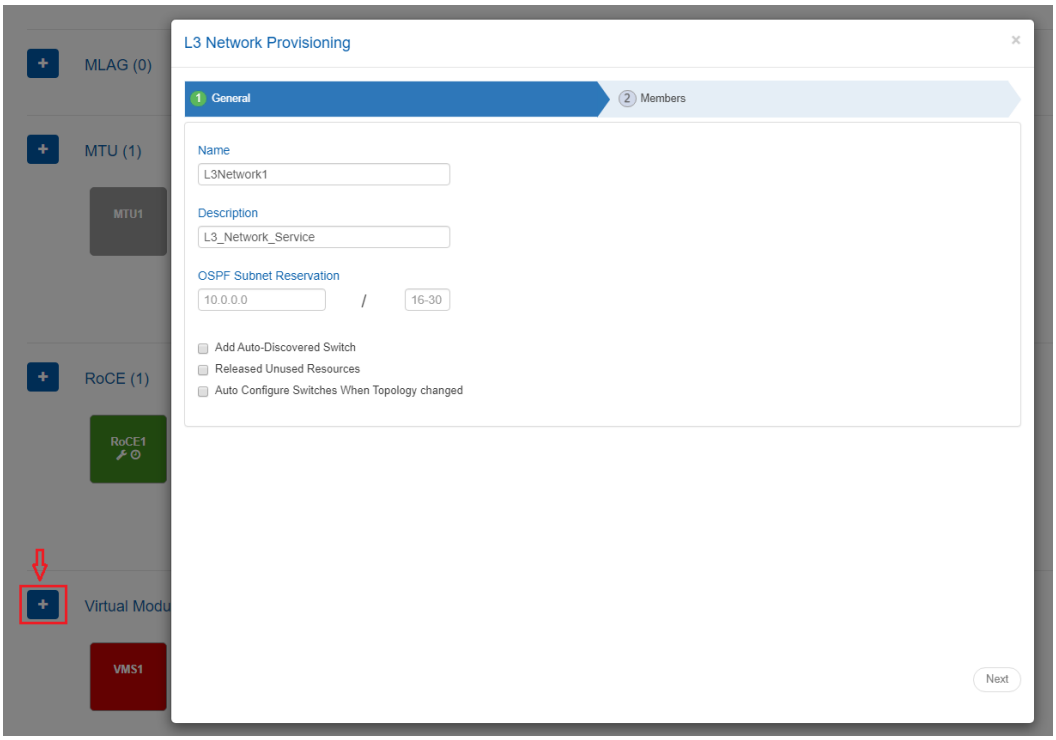
2. Click OK when prompted by the following message.

L3 Network Provisioning

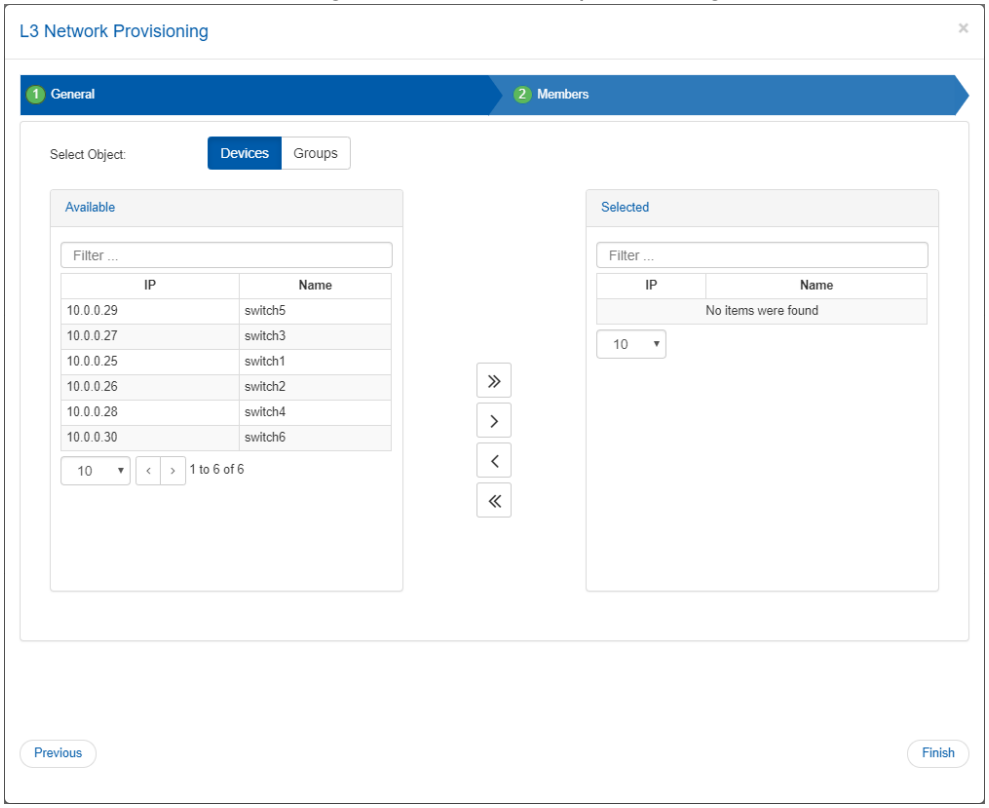
The L3 network provisioning service provides a simple provisioning capability for configuring the layer 3 network connectivity. This can be done by selecting the Mellanox switches and defining their IP subnet for inter-switch connectivity. The service will then discover all links between these switches and will allocate a subnet of the length of 30 for each link pair from the subnet provided by the user.

In order to configure the L3 network provisioning service, follow the steps below:

1. Click the “Add” button on the right side of the Virtual Modular Switch row.
2. Fill in the required information and check the desired checkboxes under the General dialog box:
    a. Provide a name and description of the service.
    b. Then in the OSPF Subnet Reservation field, type the subnet used for allocating IP addresses to OSPF areas.
    c. [Optional] When the “Add Auto-Discovered Switches” checkbox is checked, a notification will be generated, notifying the user of a topology change in the newly created topology/service. For further information, refer to “Notifications”.
    d. [Optional] Check the “Release Unused Resources” checkbox for unused links to be deallocated within the timeout interval chosen in minutes (the minimum is 15 minutes).
    e. [Optional] Check the “Auto Configure Switches When Topology Changed” checkbox for auto configuration of devices upon topology changes. When this checkbox is checked, no notification will be generated. Rather, an event will appear under “Events”.



3. Choose the devices to configure the L3 network provisioning service for, and click “Finish”.



Once clicked “Finish”, a service instance will be created and a service element will appear on the Services main page. A right click on a service element will enable performing different

operations. For information on the operations and the service instances in general, please refer to “Service Elements”.

MLAG

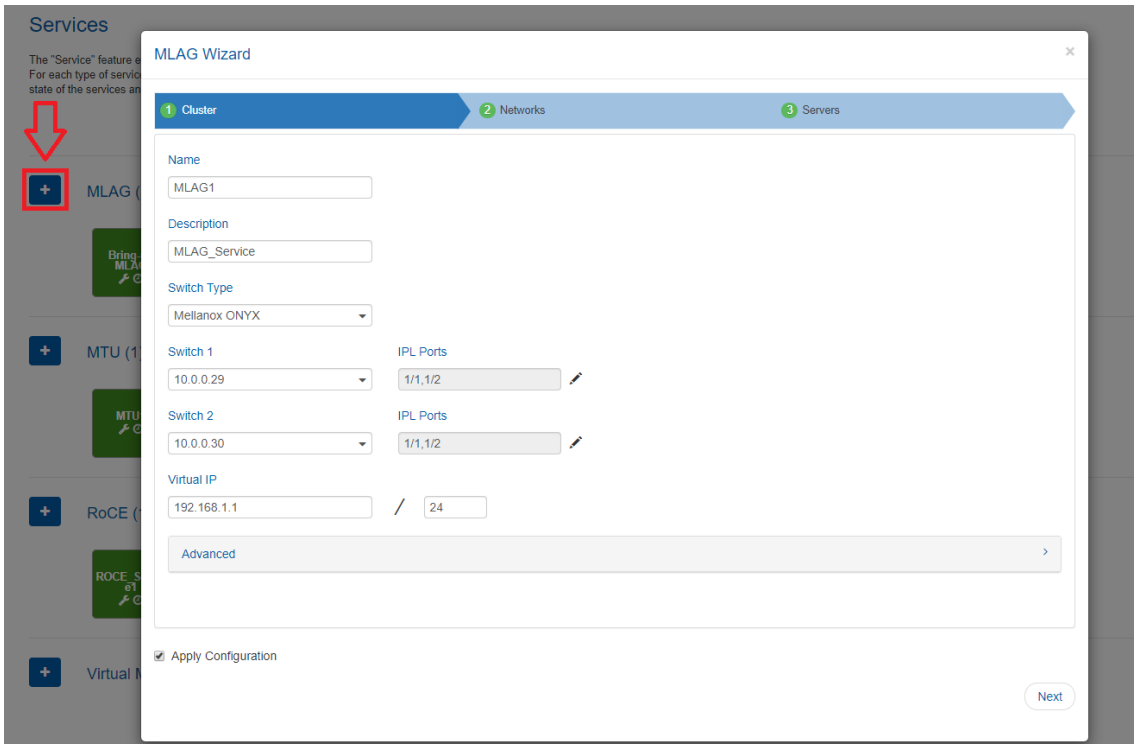
The MLAG service allows configuring a pair of Mellanox Onyx or Cumulus switches with the following to support multi-chassis LAGs and periodically validates their configuration:

1. Switch cluster
2. MAGP router and network
3. MLAG port channel
4. Host bond

In order to configure the MLAG service:

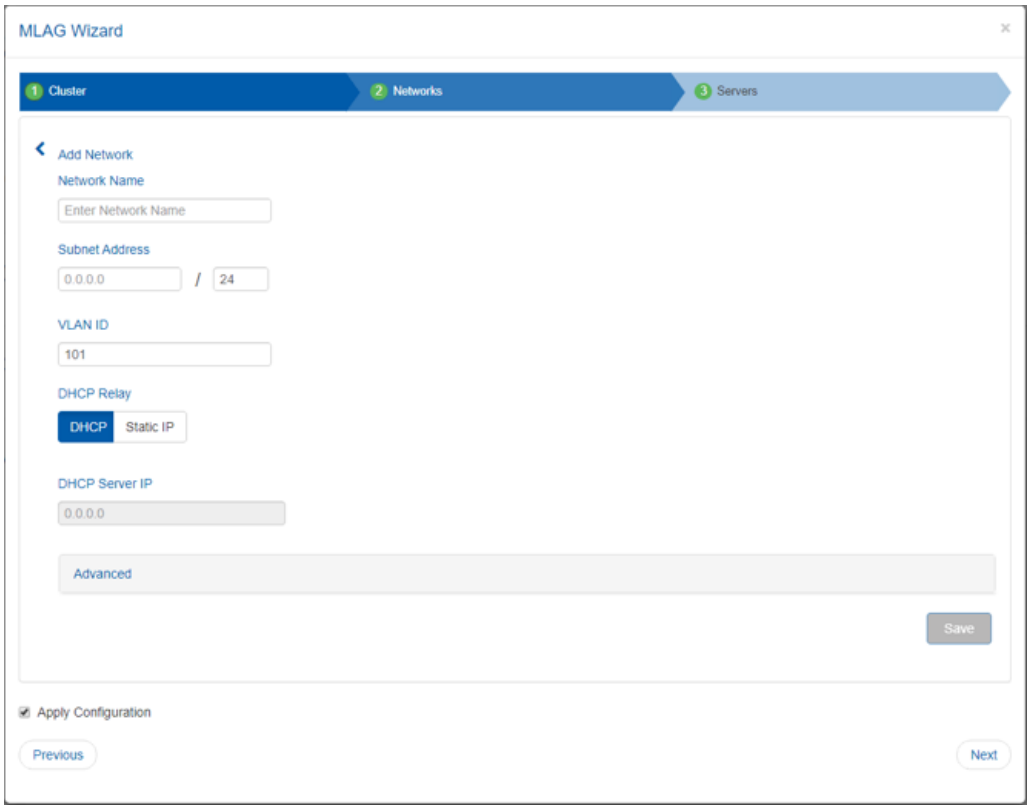
1. Click the “Add” button on the right side of the MLAG row.
2. In the Cluster tab, select the switch type and IP of the first switch in the cluster. The rest of the fields (including the collapsible Advanced section) will be filled out automatically, with the option to be edited. Note that some fields might not be filled in case there is no appropriate peer switch.

> ⚠ The information in the Cluster tab is mandatory for the creation of the MLAG service, and cannot be changed once the service is created.



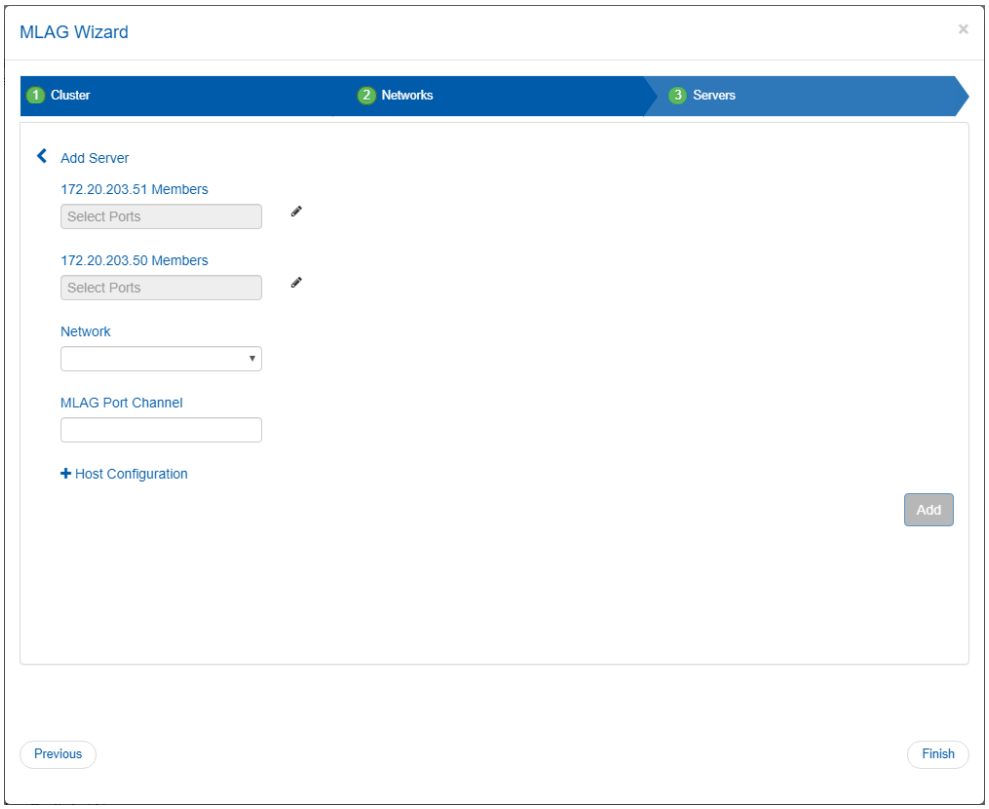
3. Under Networks tab, you can manage MAGP networks on the MLAG cluster. Click “Add” to add a new network and fill in the required information, or edit/delete a network using the icons in the rightmost column of the network row.

⚠ Networks are not mandatory for the MLAG service creation. They can be added, edited or removed after the service has been created.



4. Under Servers tab, you can manage the connectivity between the MLAG switches and the Linux hosts the MLAG switches are connected to. This includes both switch side configuration and (optionally) the host side bond creation. When first accessing this tab, it will be initialized with connected servers that NEO has already identified. Click “Add” to add a new server and fill in the required information, or edit/delete a server using the icons in the rightmost column of the server row.

⚠ Servers are not mandatory for the MLAG service creation. They can be added, edited or removed after the service has been created. However, if you define a server, you also need to define the network it belongs to in the Networks tab.



Once clicked “Finish”, a service instance will be created and a service element will appear on the Services main page. A right click on a service element will enable performing different operations. For information on the operations and the service instances in general, please refer to “Service Elements”.

> When NEO discovers an MLAG configured on the switches, it will automatically create a service for it.

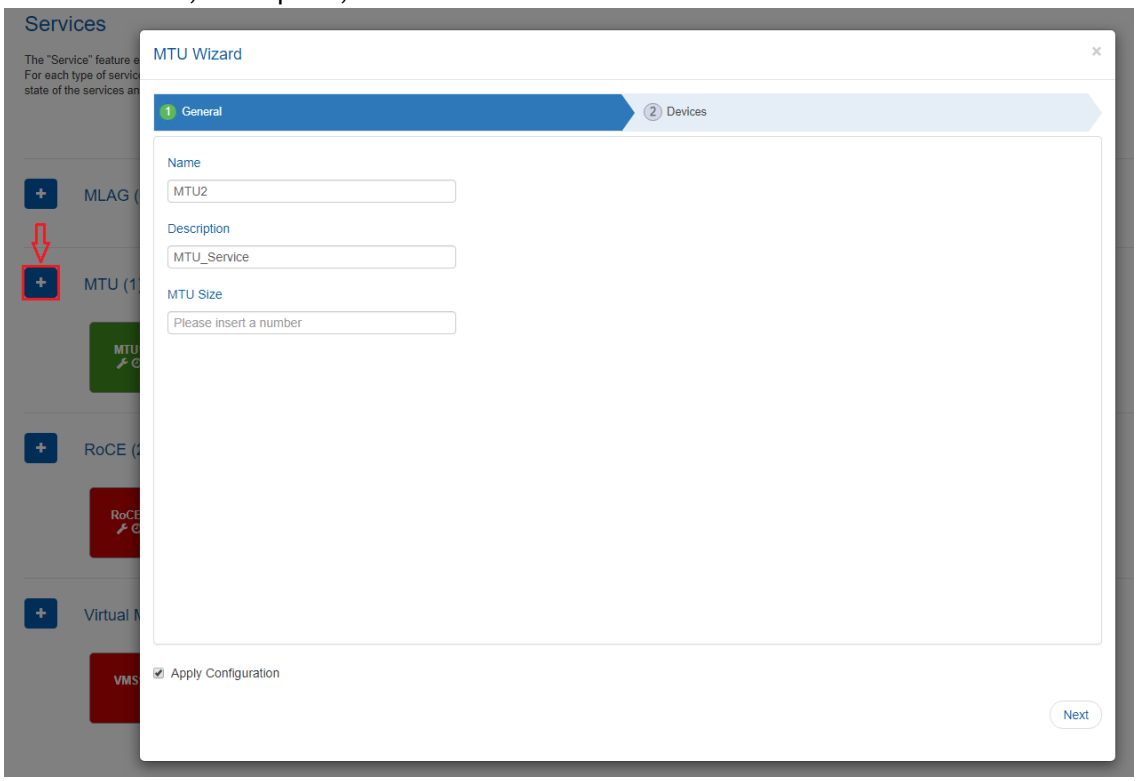
MTU

The MTU service allows configuring an interface MTU on specified Mellanox Onyx switches to a desirable value and periodically validates their configuration.

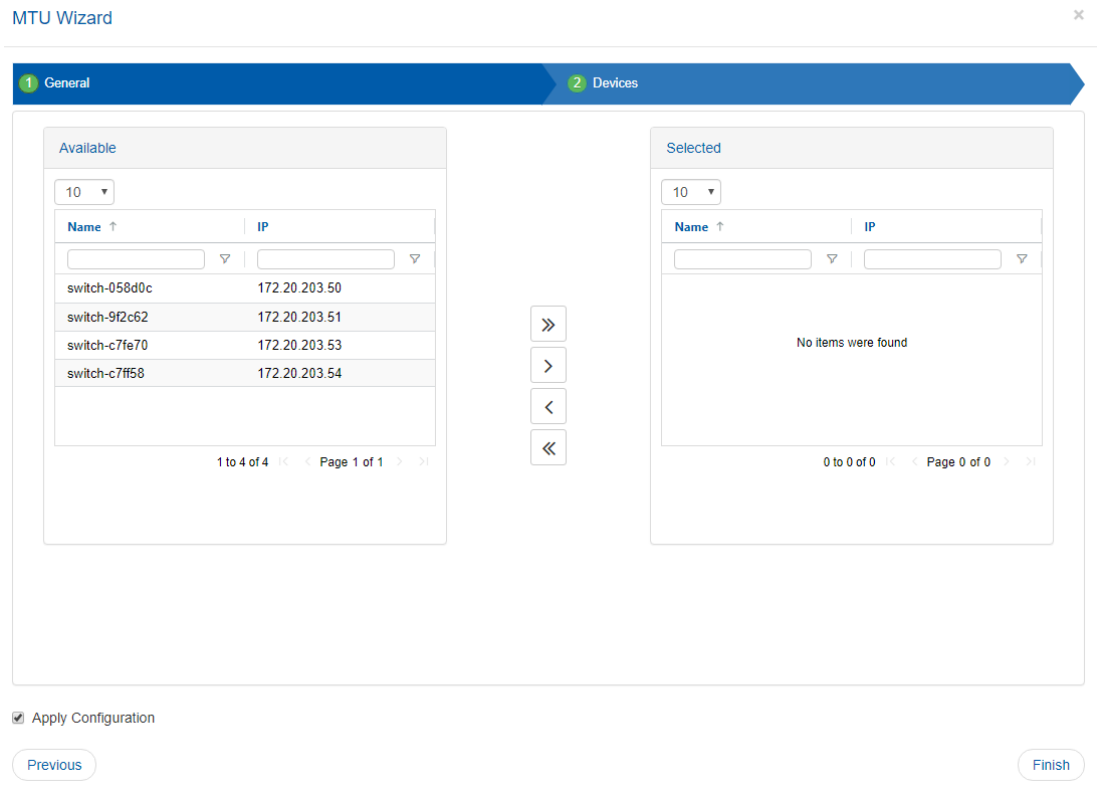
In order to configure the MLAG service:

1. Click the “Add” button on the right side of the MTU row.

2. Fill in the name, description, and MTU fields.



3. Choose the device to configure the MTU service for, and click “Finish”.



Once clicked “Finish”, a service instance will be created and a service element will appear on the Services main page. A right click on a service element will enable performing different

operations. For information on the operations and the service instances in general, please refer to “Service Elements”.

RoCE

RDMA over Converged Ethernet (RoCE) is a network protocol that allows remote direct memory access (RDMA) over an Ethernet network. It is mainly useful for network-intensive applications like networked storage or cluster computing, which require a network infrastructure with high bandwidth and low latency.

RoCE can be configured in the following configuration types: ECN only, ECN with QoS, and ECN with QoS and PFC.

To allow the network to use RoCE, both switches and hosts should be configured appropriately. The service allows one of the following modes to specify the devices to configure:

1. All host ports - configures all network starting from the hosts’ ports, through their directly linked switch ports, and including ports interconnecting switches.
2. All switch ports - configures all ports and LAGs on all network switches applicable for RoCE. Does not include host ports.
3. Custom selection - allows the user to specifically define which devices will be configured. If this option is selected, the wizard will include another step to define the devices. Each device can be defined as:
    a. Host - In this mode you select the specific host interfaces that you wish to configure. These interfaces must be linked to a supported switch. The switch interfaces that are directly connected to the host interfaces will also be configured.
    b. Switch - In this mode you select the specific switch interfaces that you wish to configure. These can also be LAGs or MLAGs.

    In both modes you can select the "Configure inter-switch links" option to configure all the switch interfaces that are connected to the selected devices. For example, if you specify the leaf switches and select this option, the interfaces that connect the leaf switches to the spine switches or between different spine switches will also be configured.

For Windows hosts, the interface connectivity is not automatically detected. Therefore, the switch interfaces that are directly connected to the host interfaces will not be implicitly configured, and the "Configure inter-switch links" option is not relevant. You must explicitly create another RoCE service for the switch ports you wish to configure. This is relevant in case you select the "all host ports" option, or define hosts in the "Custom selection" option.

Editing RoCE Service

In case you have specified the configured devices explicitly, using the "Custom selection" option, you can edit the RoCE service to add or remove devices and interfaces to/from your configuration. However, you will not be able to change the network configuration type, the configuration parameter values or the device type to be configured (host/switch).

⚠ Removing a switch interface does not remove the RoCE configuration that is already assigned to it until the user applies the changes.

Requirements

Before configuring RoCE using NEO, make sure your network fulfills the following requirements:

- Host
  - The host should have a ConnectX-4 or ConnectX-5 NIC installed.
  - The host should have NEO-Host v1.3 and above installed.
  - Linux host should have a MLNX_OFED version compatible with NEOHost installed.
  - For Linux host, the configuration will only run on ports that NEO identifies as links to an applicable switch.
  - Linux host should have Link Layer Discovery Protocol Agent Daemon (LLDPAD) package installed.
  - Windows host should have a Windows Server 2016 operating system and WinOF2 v2.0 and above installed.
- Switch
  - The switch should be either a Mellanox Spectrum, a Cumulus or a 3232C/3231Q Cisco switch.
  - Mellanox switch should have Mellanox Onyx OS of v3.6.5000 and above installed.
  - Cumulus switch should have operating system v3.5 and above installed.
  - The cables should support 100G rate.
  - The ports speed should be configured to 100G.

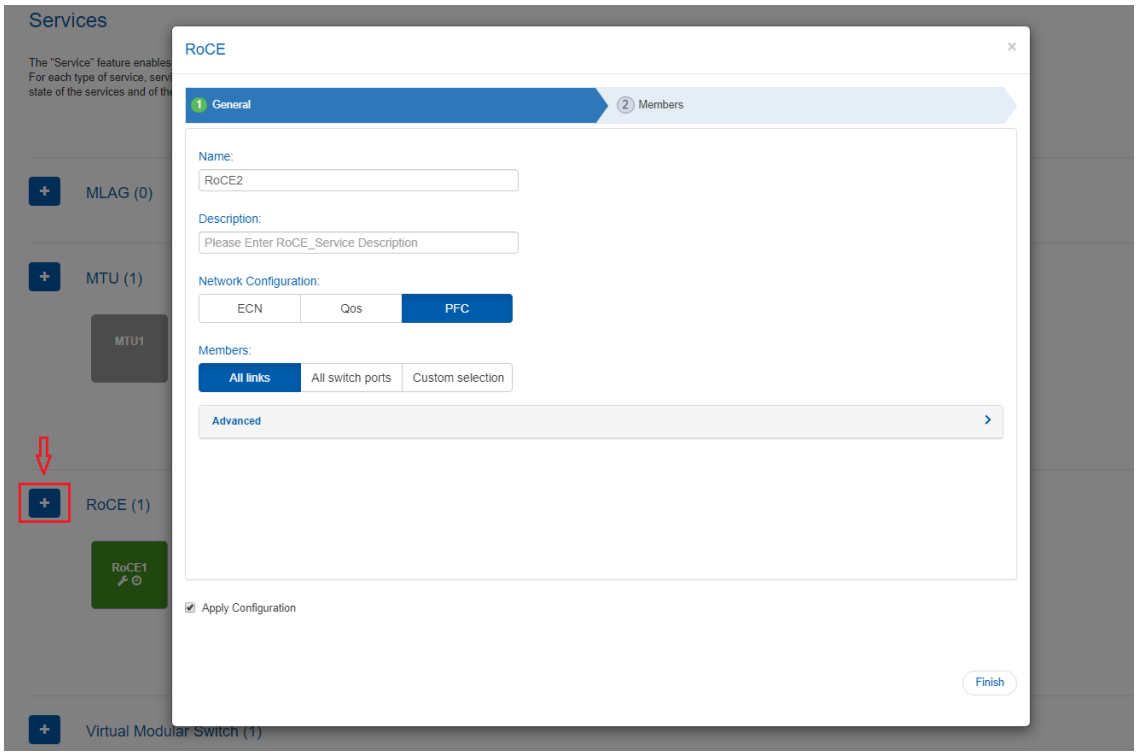
Limitations

- Host: The configuration is non-persistent. Rebooting a host requires reconfiguring it.

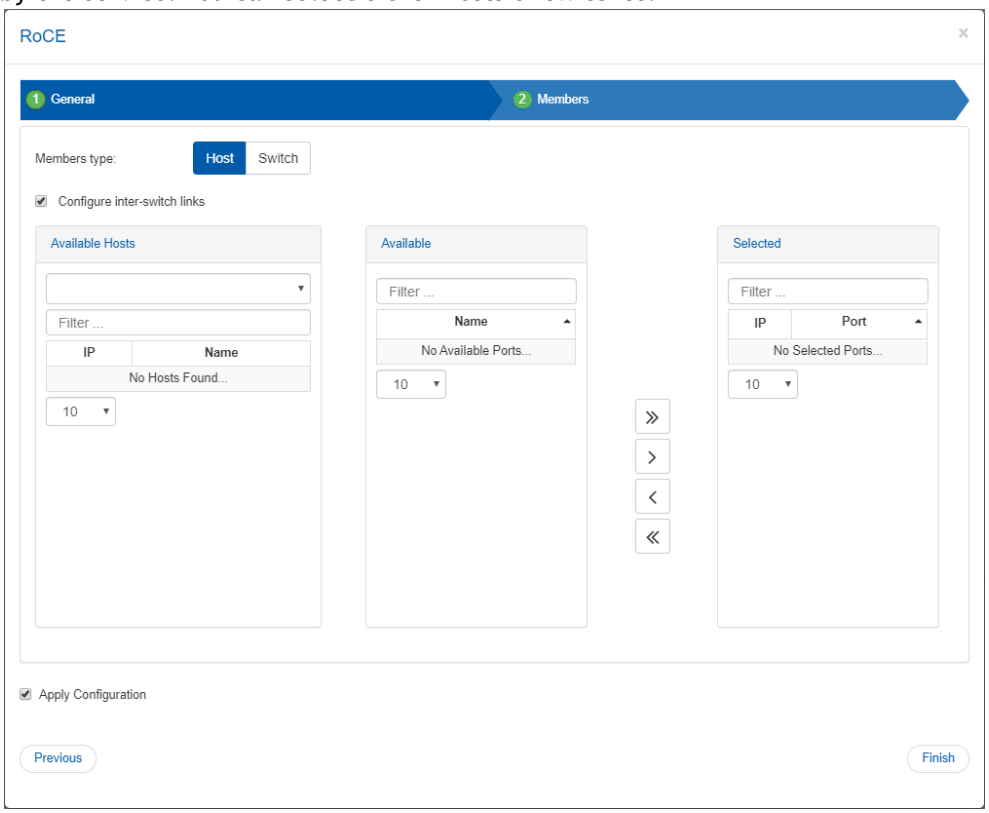
RoCE Configuration

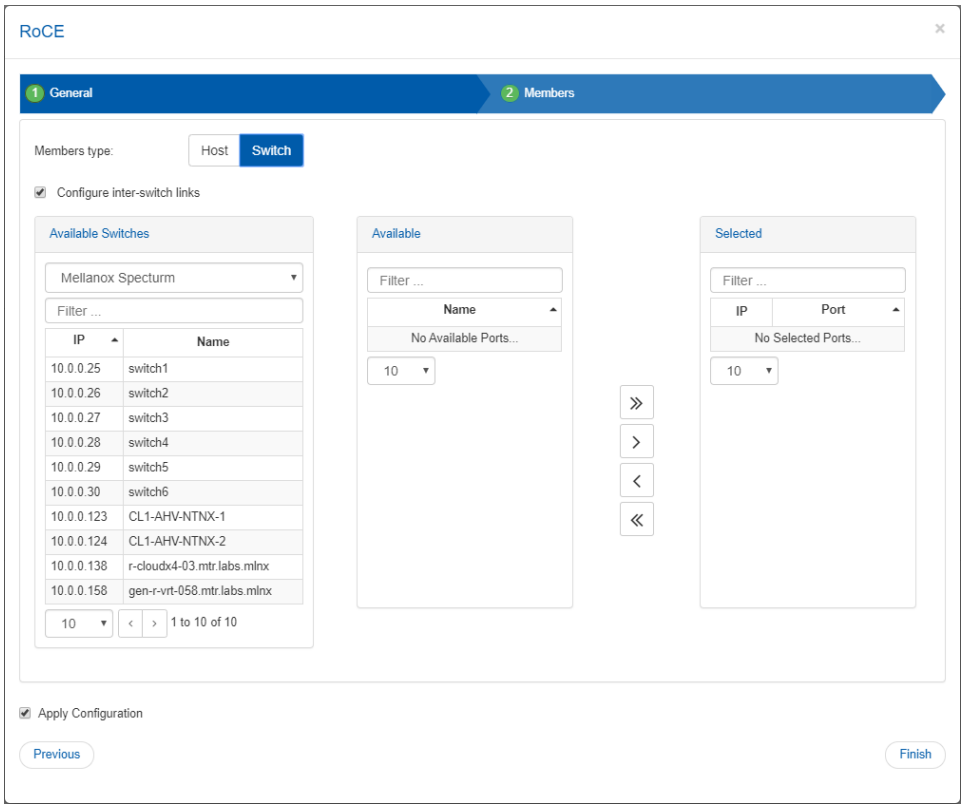
In order to configure RoCE,:

1. Click the “Add” button on the right side of the RoCE row.
2. Name your service and check/uncheck the QoS and PFC checkboxes, as desired. Select which devices will be configured by this service. In the Advanced section you can also alter the configured value for certain parameters, depending on the RoCE configuration you choose. The "Apply Configuration" checkbox defines whether configuring the devices will start immediately upon clicking the “Finish” button.



3. If you choose to explicitly define the devices to be configured with the "Custom selection" option, use the Members tab to define the devices and the interfaces that will be configured by the service. You can select either hosts or switches.

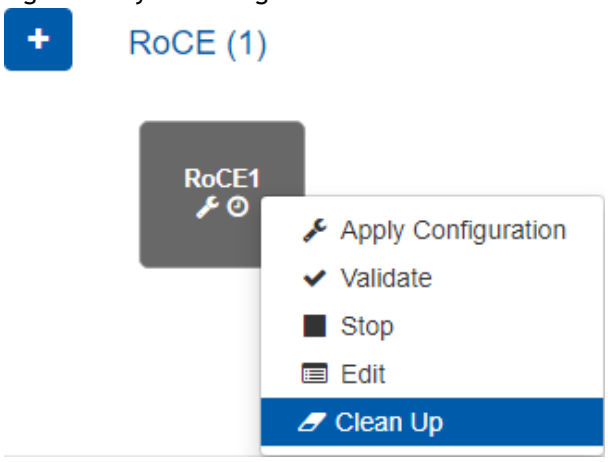




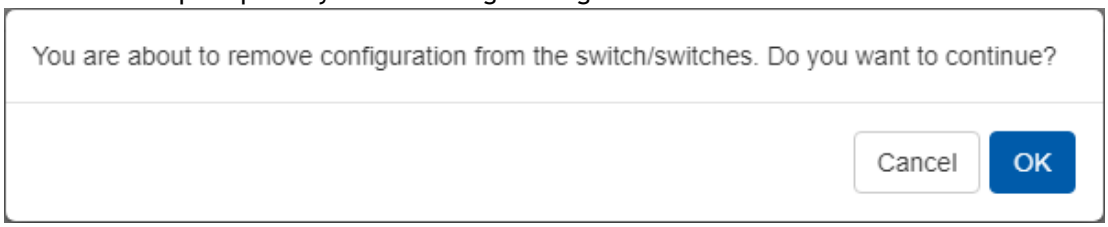
Once clicked “Submit”, a service instance will be created and a service element will appear on the Services main page. A right click on a service element will enable performing different operations. For information on the operations and the service instances in general, please refer to “Service Elements”.

In order to delete a configured RoCE service:

1. Right-click your configured RoCE icon and click "Clea-n Up".

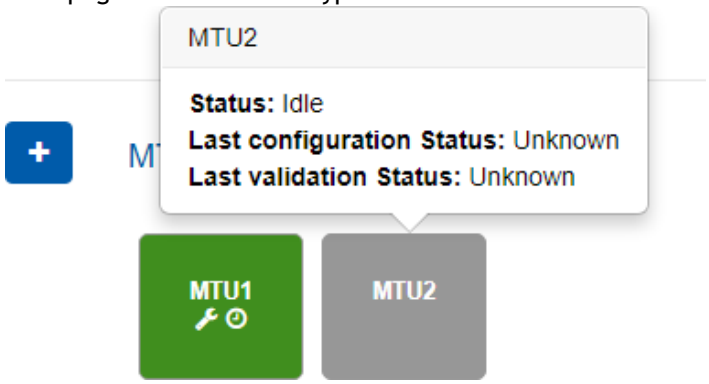


2. Click OK when prompted by the following message.



Service Elements

The service elements are colored squares that stand for service instances and appear in the Services main page once a service type is created.



1. Elements Colors: The color of a service element varies mainly according to the service instance's last configuration status. However, when the service's status is "Monitoring", the color will be determined according to the service instance's last validation status.

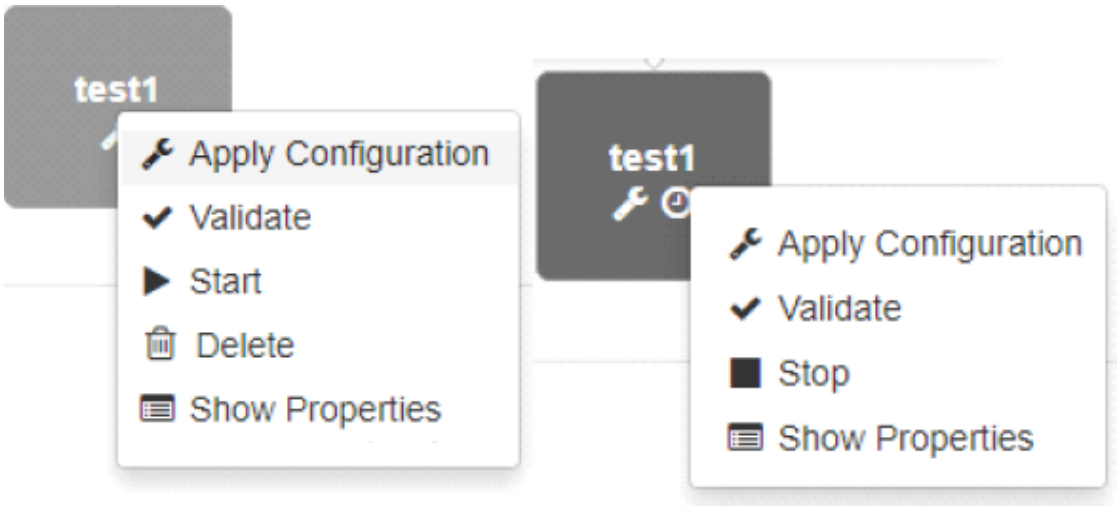
lastConfigurationStatus	Color
Initializing	Blue
Idle	Grey
InitializingFailure	Red

Colors According to the Last Validation Status

lastConfigurationStatus	lastValidationStatus	Color
Monitoring	Unknown	Grey
	Completed	Green
	Completed With Errors	Red

2. Colors According to the Last Configuration Status

- Element Operations: A right-click on a service element will enable configuring the service by selecting "Apply Configuration". Other operations may also be available for a service element depending on its status, see details in the table below.



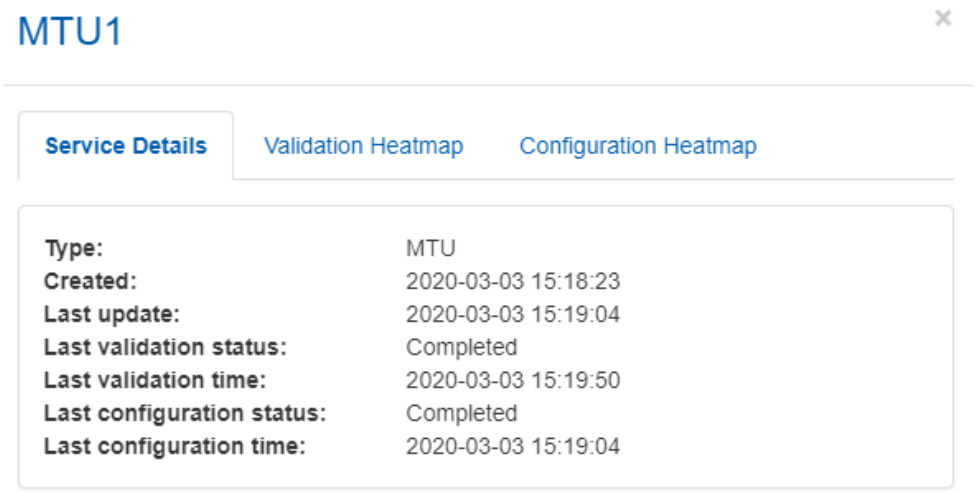
Available Service Element Operations

Status	Operations Available	Operations Description
Initializing	None	N/A
Idle	Apply Configuration	Configures the service. Once the configuration is applied, the service status will automatically change to "Monitoring", and start periodic validation. Only once the configuration is applied, the "Validate" and operation will become available.
	Apply Changes	Available if the service has been edited since applying the configuration. Applies only the configuration changes.
	Clean-up	Cleans-up the configuration done by the service. Once the configuration is cleaned, the service status will automatically change to "Idle", and stop periodic validation. Previous configuration and validation status will be reset. ⚠ Clean-up is currently supported for RoCE and MLAG service types on Onyx and Cumulus switches. ⚠ MLAG clean-up is only supported for MLAG services created in NEO 2.6 and above. ⚠ After MLAG clean-up is performed, MPO VLAN, IP routing, IP DHCP relay instance, LACP, and protocol MAGP configuration will remain on Mellanox Onyx switches. For Cumulus switches, only the MPO's VLAN configuration remains.
	Validate	Validates the configuration of the service.
	Start	Starts a periodic validation of the service (default interval is 30 minutes). This will change the status to “Monitoring”.
	Delete	Deletes the service.
	Show Properties/ Edit Service	Shows the information filled when the service was created. Some service types can be edited.

Status	Operations Available	Operations Description
Initializing Failure	Delete	Deletes the service.
	Show Properties	Shows the information filled when the service was created.
Monitoring	Stop	Stops a periodic validation of the services. This will change the status to “Idle”.
	Show Properties/ Edit Service	Shows the information filled when the service was created. Some service types can be edited.

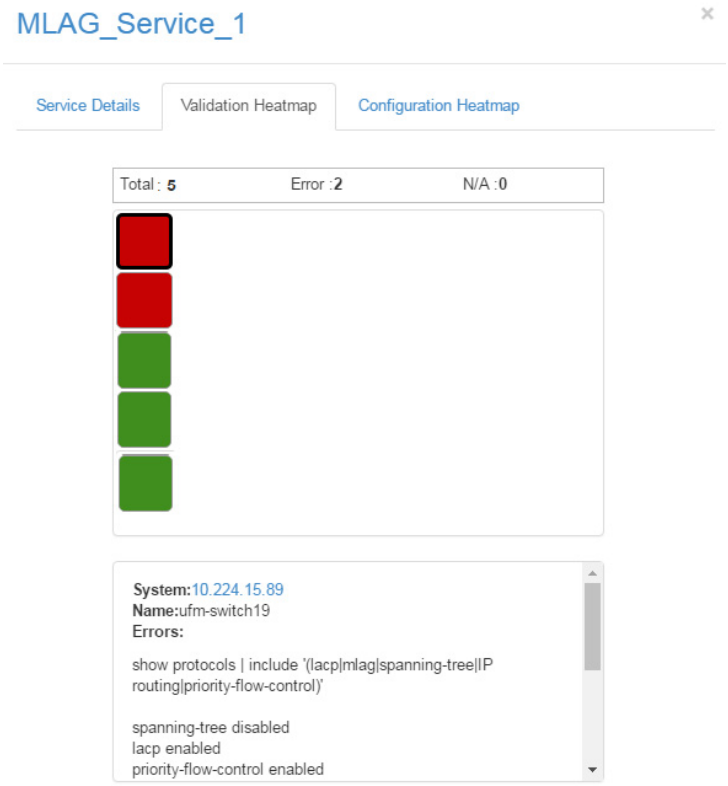
- Device configuration backup: Before configuration changing operations (Apply Configuration, Apply Changes, Clean-up: see table above), a network snapshot will be created for all the devices that are about to be configured. This snapshot can be used to revert to the original device state if the configuration fails, or if it has unwanted implications. If the snapshot creation fails the operation will not run.
- Element Icons: Each service element contains the following (example: 

):
  - The name of the service
  - The wrench icon – if the last configuration status of the service was “Unknown”
  - The clock icon – if the service state is Monitoring
  - The spinner icon – if the service is going under a validation or configuration process at the moment
- Element Information: When hovering over an element, the following information will be displayed:
  - The service’s “state”
  - The service’s “last configuration status”
  - The service’s “last validation status”
- Service Details Modal: When clicking a service element, a modal with more details about the service will appear. The modal consists of three tabs:
  - “Service Details” tab – lists the service type, the time it was created, the time it was last updated, the last validation status and time, and the last configuration status and time.



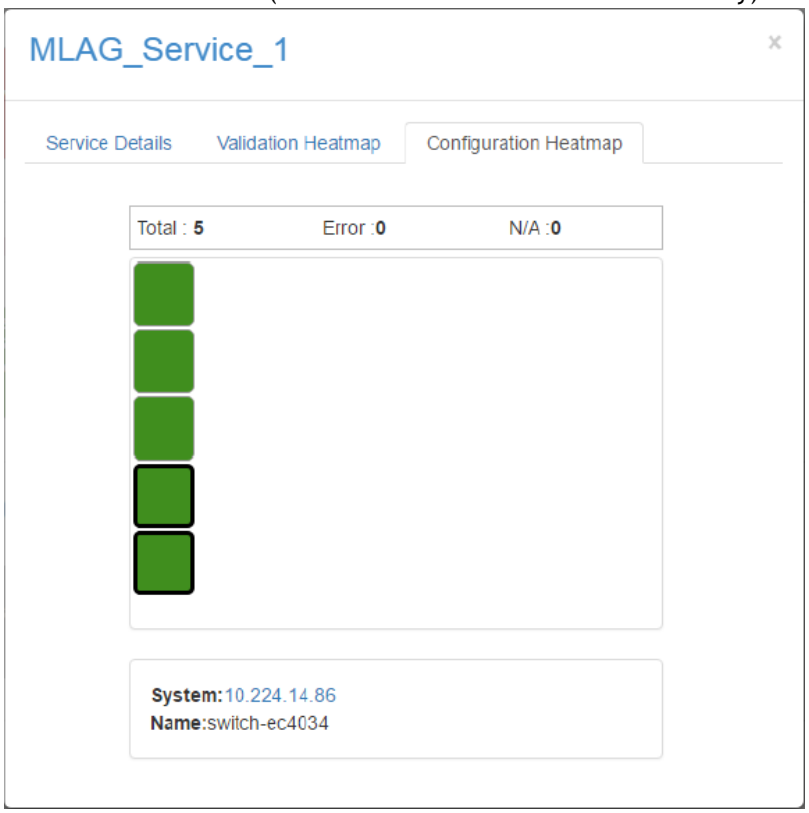
If the service initialization fails, an error message will be added to the bottom of Service Details list.

- “Validation Heatmap” tab – provides a validation heatmap of the service devices, colored according to their validation job status (Completed – Green, Completed with Errors – Red, Unknown – Grey). When clicked on a device, more details about its IP and name (and the relevant errors if there are any) will be displayed.



- “Configuration Heatmap” tab – provides a configuration heatmap of the service devices, colored according to their configuration job status (Completed – Green, Completed with Errors – Red, Unknown – Grey). When clicked on a device, more details

about its IP and name (and the relevant errors if there are any) will be displayed.



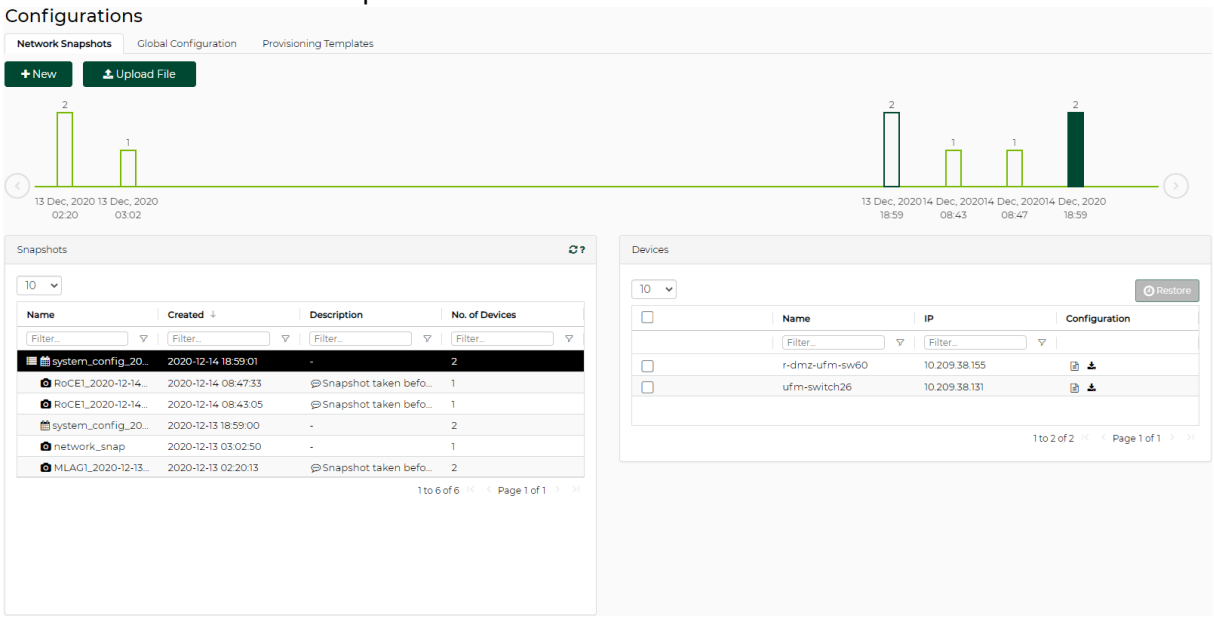
Configuration Management

Configuration Management manages network configurations and provisioning templates.

Network Snapshots

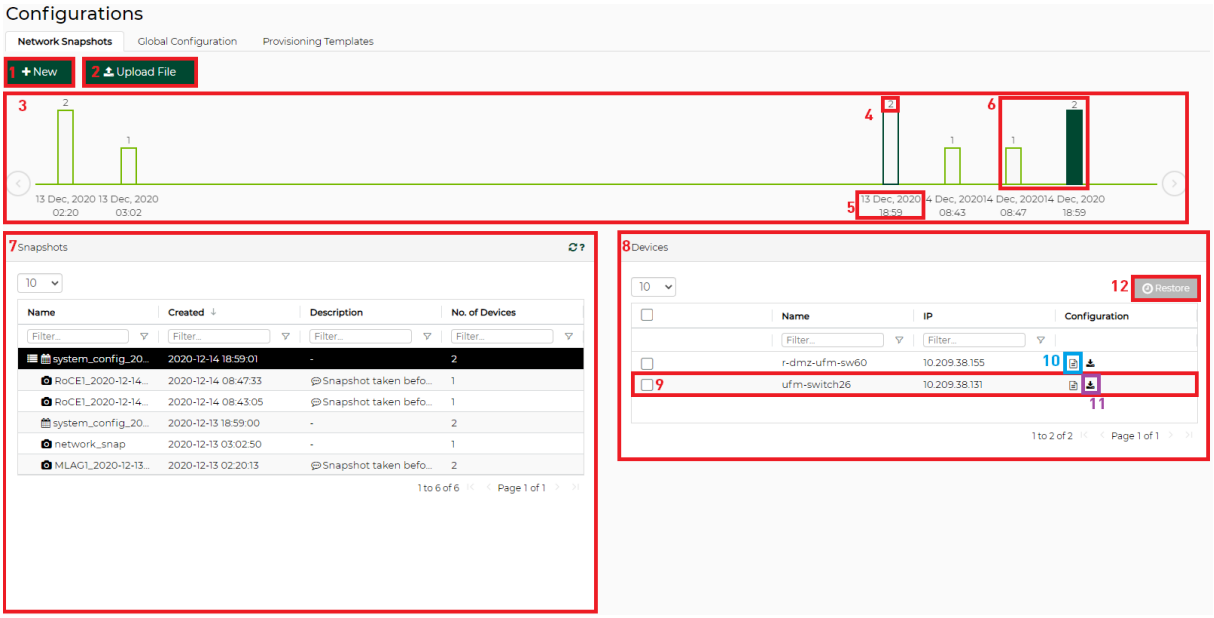
Network Snapshots manages configuration snapshots of the switches, by creating and restoring snapshots when needed. NEO takes an automatic snapshot once a day (system snapshots), and maintains the last seven snapshots (taken over the last seven days). Users can also create snapshots (user snapshots), and manage them by performing a number of actions detailed below.

Network snapshots are saved configuration files captured at a certain point of time. These snapshots can be later used to restore a previous state of the network.



Tab Components

Using this tab, users can manage network snapshots by viewing, editing, creating, importing, deleting, copying, and restoring them.



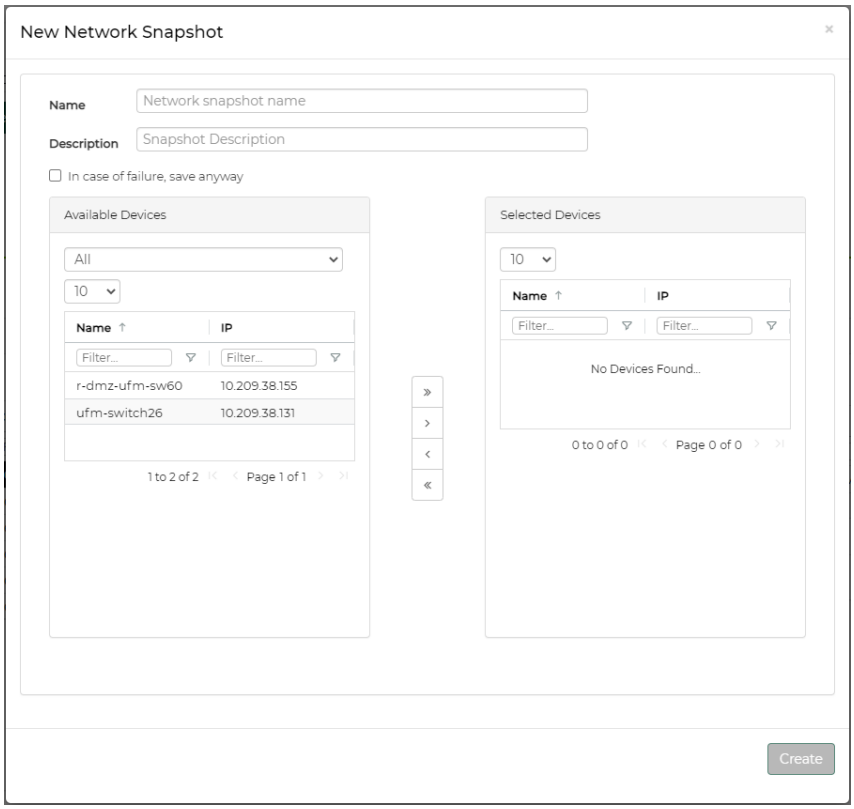
Network Snapshots Tab Components

#	Name	Description
1	New Button	Enables users to create new user snapshots.
2	Upload File Button	Enables users to upload local tar (compressed) snapshot files.

#	Name	Description
3	Snapshots Timeline	Displays snapshots in a chronological order in the form of a bar chart. This timeline is linked to the snapshots table, as when a snapshot is selected from the table, it will be highlighted in the timeline, and vice versa.
4	Devices Count	The number of devices that are included within a snapshot. It is also used to represent the height of the bar.
5	Snapshot Date	The date on which the snapshot was taken. Appears below the snapshot.
6	Snapshots Colors	System snapshots are green-colored, while user snapshots are blue-colored.
7	Snapshots Table	Lists all system () and user () snapshots. The format of a system snapshot is: “system_config_yyyy-mm-dd_hh-mm-ss”.
8	Devices Table	Lists all devices of which configurations have been saved in the selected snapshot from the Snapshots table.
9	Disabled Row	A switch that was once part of the system and was included in the snapshot, but no longer exists. This switch’s configuration cannot be restored, but users can view or download its saved configurations.
10	View Icon	Displays configuration output of the corresponding switch.
11	Download Icon	Downloads the saved configuration of the switch to the user's computer.
12	Restore Button	Enables restoring the configurations of the selected switches.

To take a new snapshot of specific systems:

1. Click the “New” button.
2. Provide a name and description of the snapshot, and move the systems you want to be part of the snapshot to the rightmost table:



Note the following:

- The snapshot name must be a unique non-whitespace name
- Snapshot description is optional
- When the failure checkbox is checked, snapshots will be created even if not all of the switch's configurations were taken successfully. When it is unchecked, the snapshot will only be created if all of the switches' configurations were taken successfully.

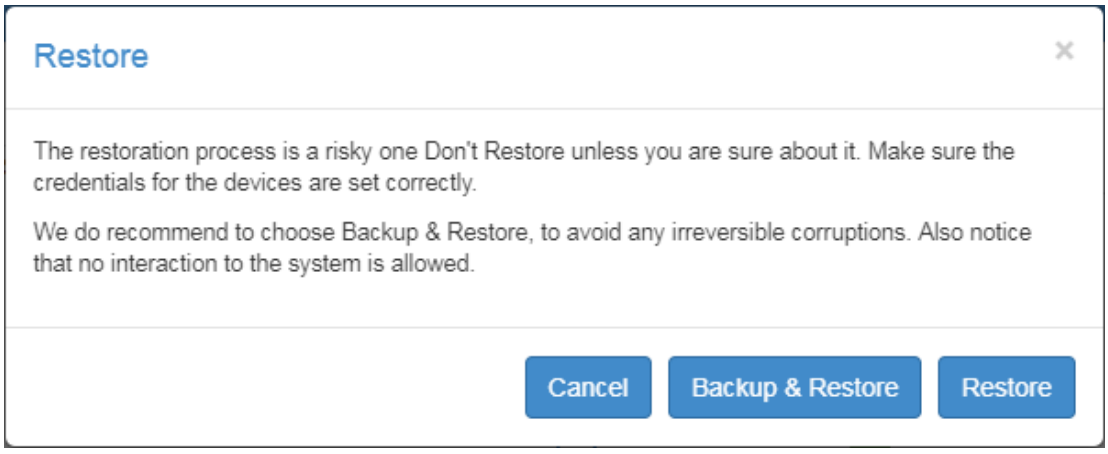
3. Click “Create”. A new bar will be added to the right side of the timeline.

Restoring Snapshots

The main goal of taking network snapshots is to help retrieve certain switches’ configurations in case errors/misconfigurations take place. Previously saved snapshots of switches’ running configurations can be restored and applied on these switches.

To restore a snapshot:

1. Select the desired snapshot from the Snapshots table.
2. Select the switches that you would like to store their configurations from the Devices table.
3. Click “Restore”. A pop-up will bring to attention the seriousness of the restoration process, and will prompt choosing either to backup and restore, or to restore only:



4. Backup snapshots are taken right before restoration and capture the currently running configurations. The name format of these backup snapshots is: system_config_yyyy-mm-dd_hh-mm- ss_Auto_Snapshot. The backup snapshot will immediately be added to the Snapshots table. Once the backup process is successfully completed, the restoration process will take place.
5. Click “Backup & Restore” or “Restore”. The restoration process will start.

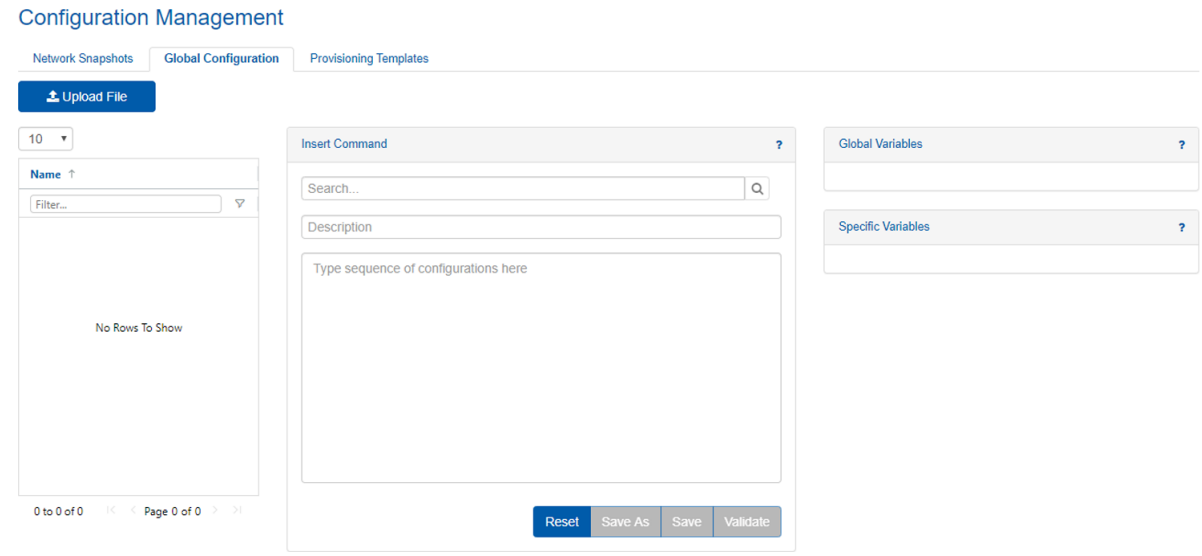
Snapshots Actions

A right-click on a snapshot from the Snapshots table will enable performing the following actions:

- Remove : Deletes the selected snapshot. Only user snapshots can be deleted by users. System snapshots are deleted automatically seven days after their creation.
- Download : Downloads the selected snapshot to the user's computer as a tar/compressed file.
- Save Copy : Copies the selected snapshot and prompts the user to add a new different name:

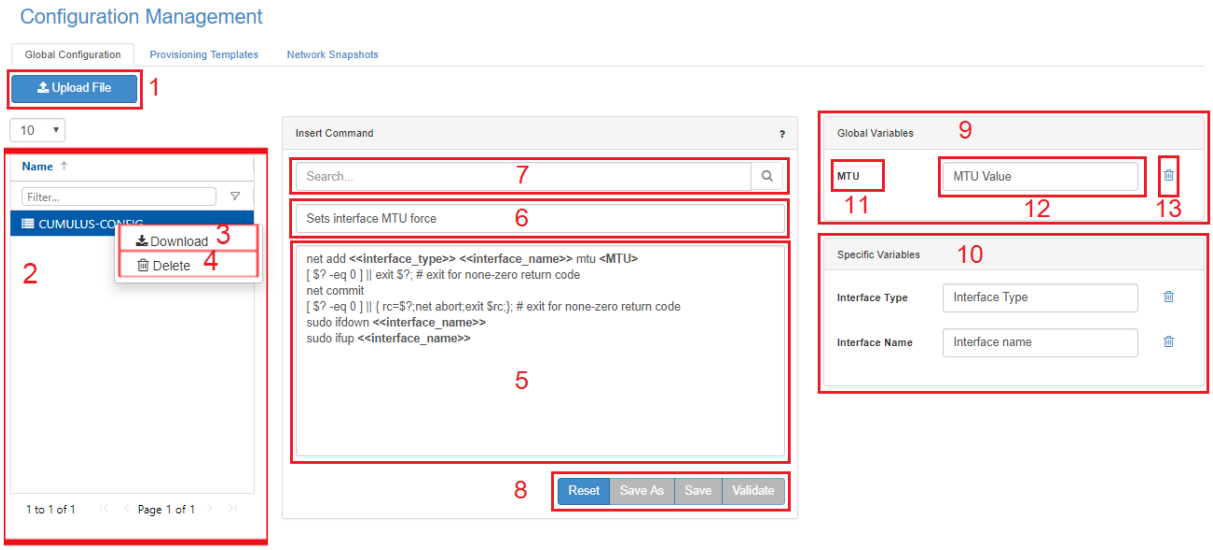
Global Configuration

Global Configuration manages global configuration files. These global files are not necessarily associated with a specific system in NEO, and are editable text files to which variables can be added, and contain a list of configurations that can later be applied on specific systems.



Tab Components

Using this tab, users can manage configuration files by viewing, editing, creating, validating, and deleting them and their variables (if applicable).



Global Configurations Tab Components

#	Name	Description
1	Upload File Button	Enables users to upload local .txt configuration files.
2	Configuration Files Menu	Displays all available global configuration files (files can be filtered for using the **Filter** field).
3	Download Icon	Enables users to download configuration files to the File System in .txt format.
4	Delete Template Icon	Enables users to delete configuration files from NEO.
5	Configuration Text Box	An editor that enables users to type in a list of configurations in separate lines and add global/specific variables.

#	Name	Description
6	Description Field	An editable field that describes the configuration file.
7	Search Field	Enables users to search for specific data that will be highlighted in the configuration text box below if any match is found.
8	Editor Buttons	**Reset**: Clears the text box, description and variables forms.
		Save As: Enables saving a newly created configuration file.
		Save: Keeps the edits on the currently selected file.
		Validate: Inserting any changes to the text box, description field or variables forms needs to be validated before continuing.
9	Global Variables Menu	A global variable is a single value given to all switches in the system. This field is comprised of all global variables defined in the configuration file. These variables appear in the configuration text box in **bold**, and are enclosed between angle brackets (for example: <variable1>).
10	Specific Variables Menu	A specific variable is a single value given to a single switch in the system. This field is comprised of all specific variables defined in the configuration file. These variables appear in the configuration text box in **bold**, and are enclosed between two angle brackets (for example: <<variable1>>).
11	Variable Name Field	A label before the field denoting the name of the variable.
12	Variable Description Field	An editable field that describes the variable.
13	Delete Variable Icon	Removes the variable from the configuration file.

To edit an existing configuration file:

1. Choose the configuration file from the list available on the left pane. It will be loaded into the middle pane, and variables, if found, will be loaded into the right pane.
2. Make the necessary edits.
3. Click “Validate”.
4. Click “Save”/“Save As”.

To create a new configuration file:

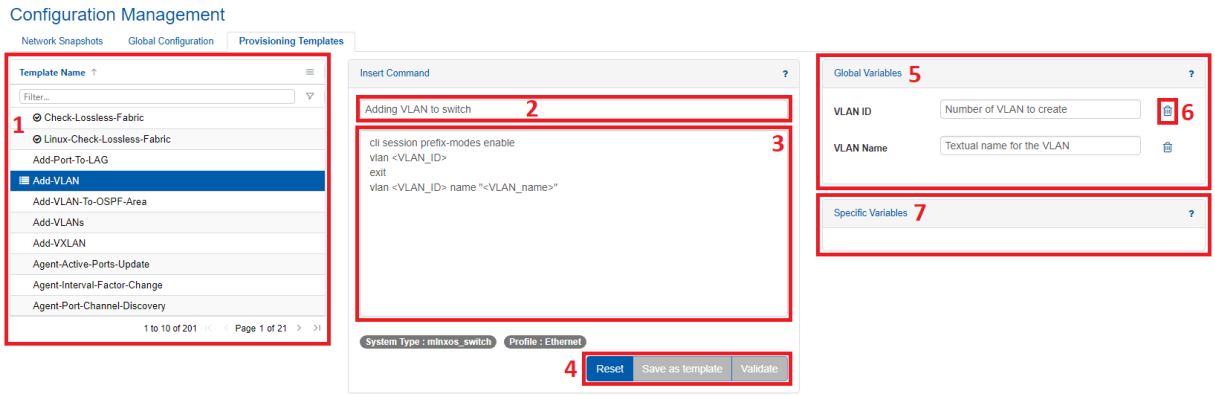
1. Make sure the editor is cleared by clicking “Reset”.
2. Start typing a list of configurations in separate lines, and provide a description to the new file.
3. Click “Validate”.
4. [Optional] Add a description to the variables (if applicable), then validate the changes again.
5. Click “Save As”. You will be prompted to add a name and choose a system type. If the system type is “Mellanox”, you may choose a system profile as well.

Provisioning Templates

The “Provisioning Templates” view enables you to edit existing commands or create new ones.

Tab Components

Using this tab, users can manage provisioning templates by viewing, editing, and creating them.



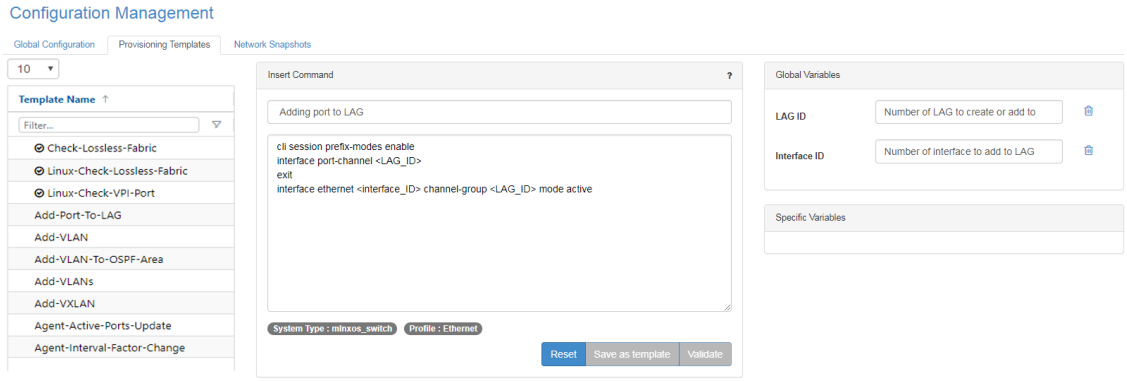
Provisioning Templates Tab Components

#	Name	Description
1	Provisioning Templates Menu	Displays all available provisioning templates (templates can be filtered for using the **Filter** field).
2	Description Field	An editable field that describes the provisioning template.
3	Templates Text Box	An editor that enables users to type in a sequence of commands and add global/specific variables.
4	Editor Buttons	**Reset**: Clears the text box, description and variables forms.
		Save as template: Enables saving a newly created provisioning template.
		Validate: Inserting any changes to the text box, description field or variables forms needs to be validated before continuing.
5	Global Variables Menu	A global variable is a single value given to all switches in the system. This field is comprised of all global variables defined in the provisioning template. These variables are enclosed between angle brackets (for example: <variable1>).
6	Delete Variable Icon	Removes the variable from the template.

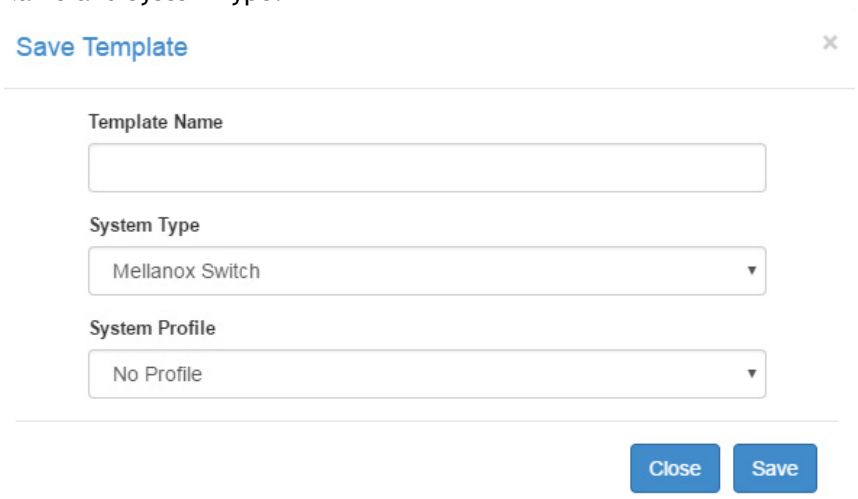
#	Name	Description
7	Specific Variables Menu	A specific variable is a single value given to a single switch in the system. This field is comprised of all specific variables defined in the provisioning template. These variables are enclosed between two angle brackets (for example: <<variable1>>).

In order to edit existing templates:

1. Choose the Template Name you wish to edit from the list on the left pane of the window, and edit it in the middle pane.



2. Click “Validate”, then “Save as template”. You will then be requested to insert a Template Name and System Type.

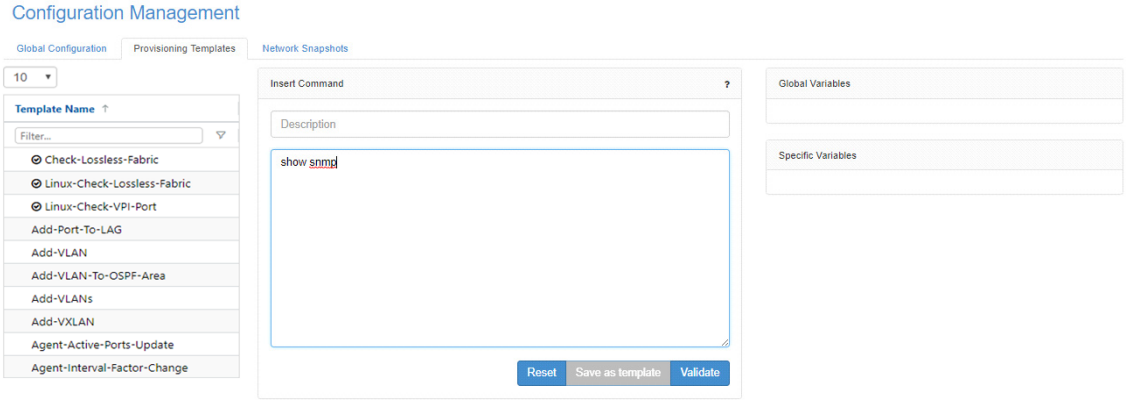


If your system type is “Mellanox Switch”, you will be asked to select the “System Profile”.

To add a new template:

1. Make sure the editor is cleared by clicking “Reset”.

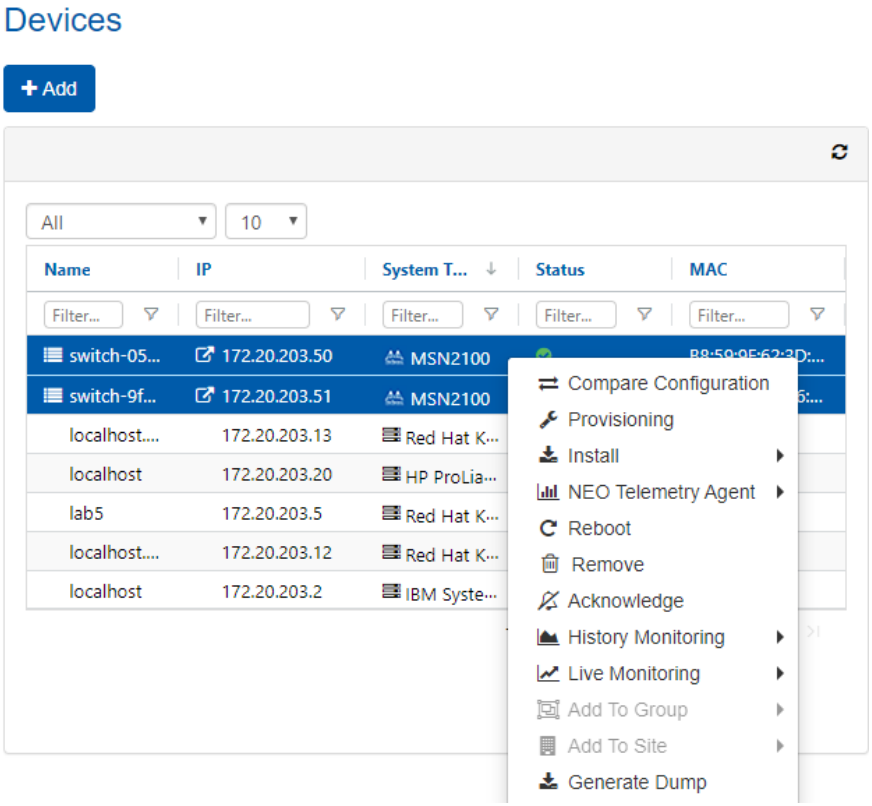
2. Insert a new command and its description:



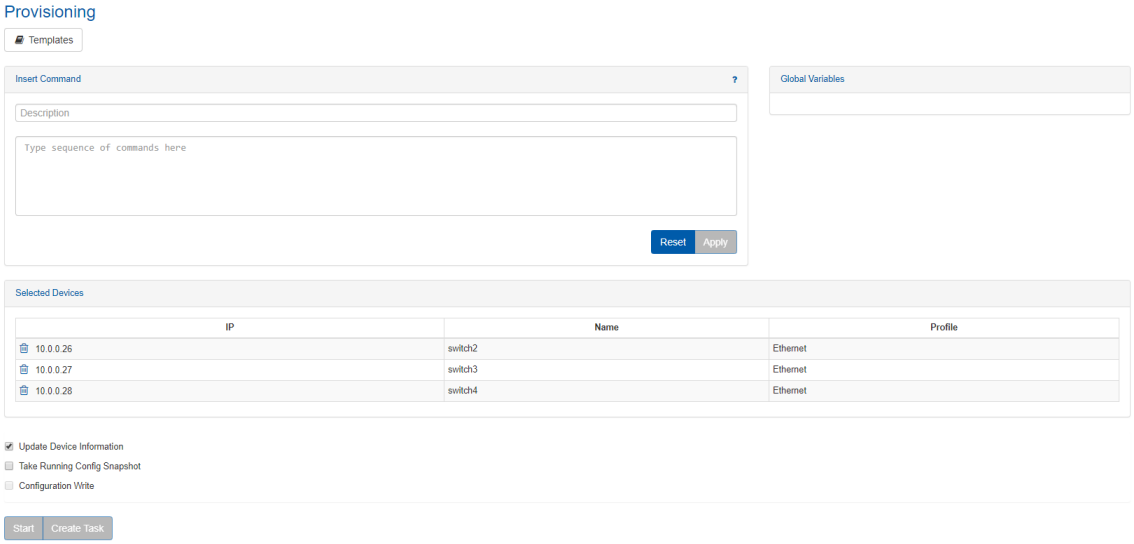
3. Click “Validate”, then “Save as template”.

To run a set of commands with certain values on multiple devices in parallel, and/or with different values per device:

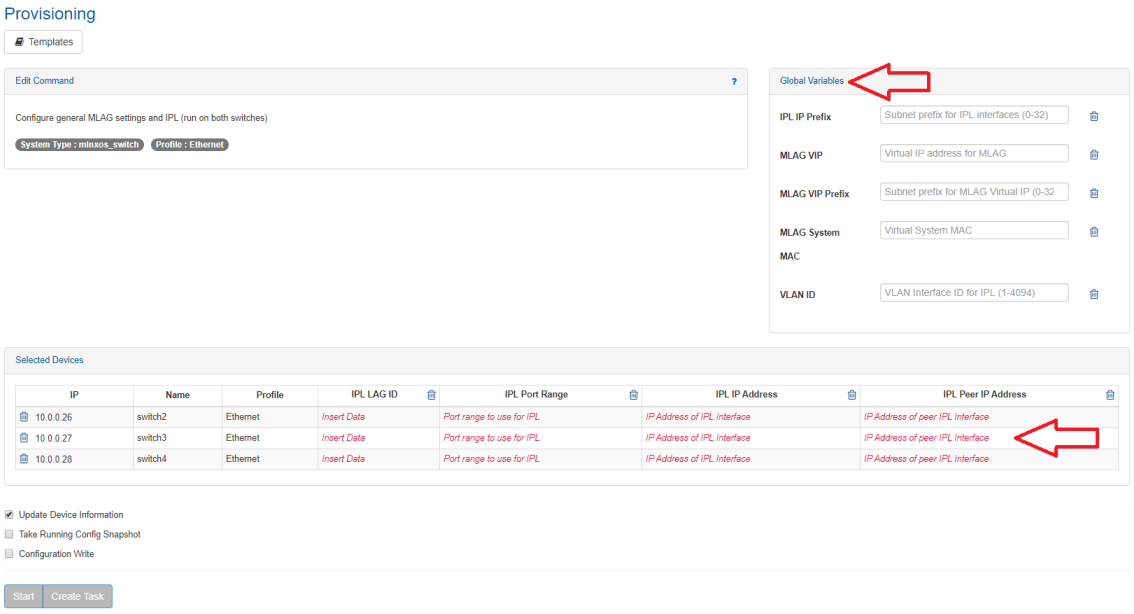
1. Choose the devices you wish to run these commands on from “Devices” under “Managed Elements”, right-click on them and click “Provisioning”.



2. Choose your template:



3. Set the global and local variables, then click “Start” or “Create Task”:

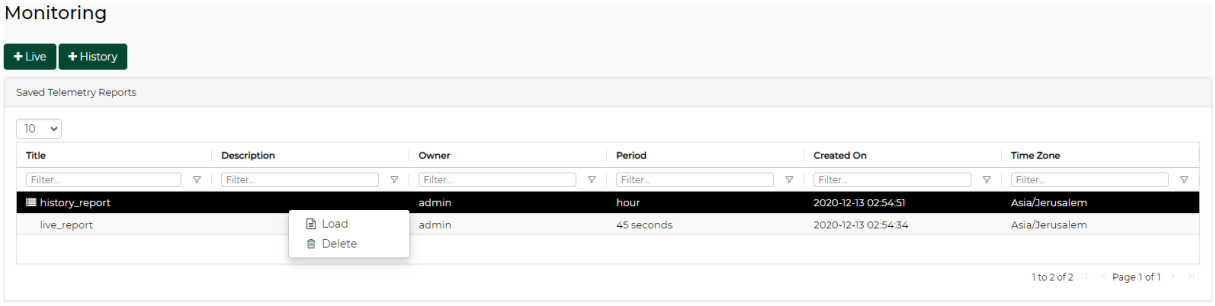


Telemetry

Monitoring

Telemetry may be used to monitor the success and faults of the network and its operations. The initial view lists the saved reports. Administrators can view all saved reports, while standard users can only view the reports they create. A right-click on a specific report opens a menu with the options to load the report or delete it from the list. Multiple reports can be selected and deleted at

once.



There are four types of reports that users can generate:

- History Monitoring
- Live Monitoring
- Performance
- Snapshot

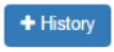
The monitoring actions can be performed from multiple windows:

- Managed Elements --> Devices --> Right-click on one or more devices
- Managed Elements --> Ports --> Right-click on one or more ports
- Managed Elements --> Groups --> Right-click on a group (available only for History Monitoring)
- Telemetry streaming – refer to History Monitoring and Live Monitoring sections below.

History Monitoring

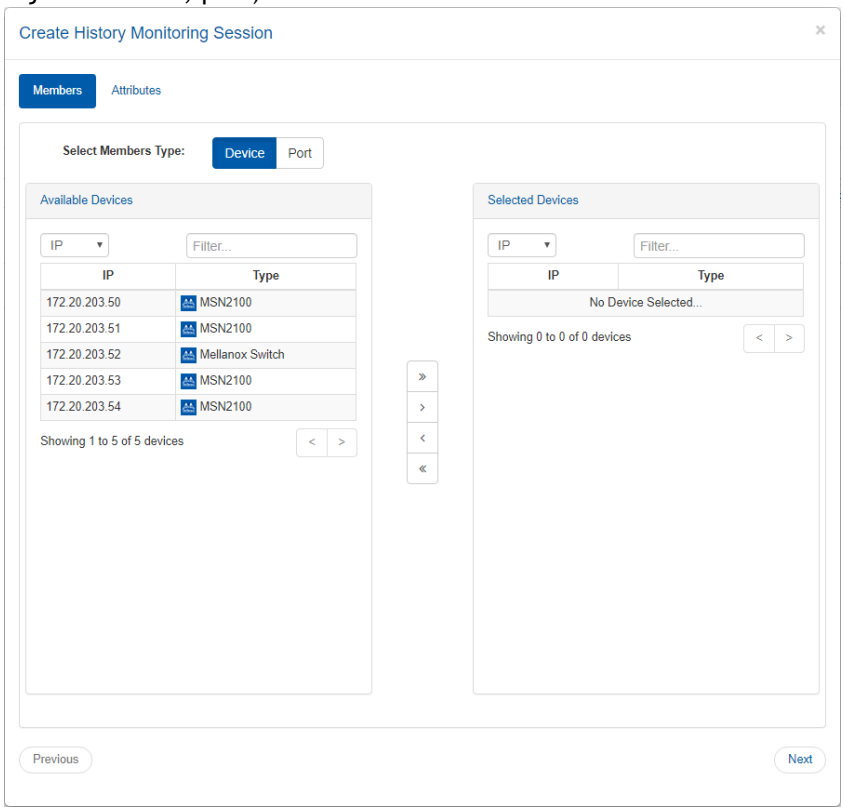
Provides a report of the device attributes values history.

To create a history monitoring report:

1. Click the 

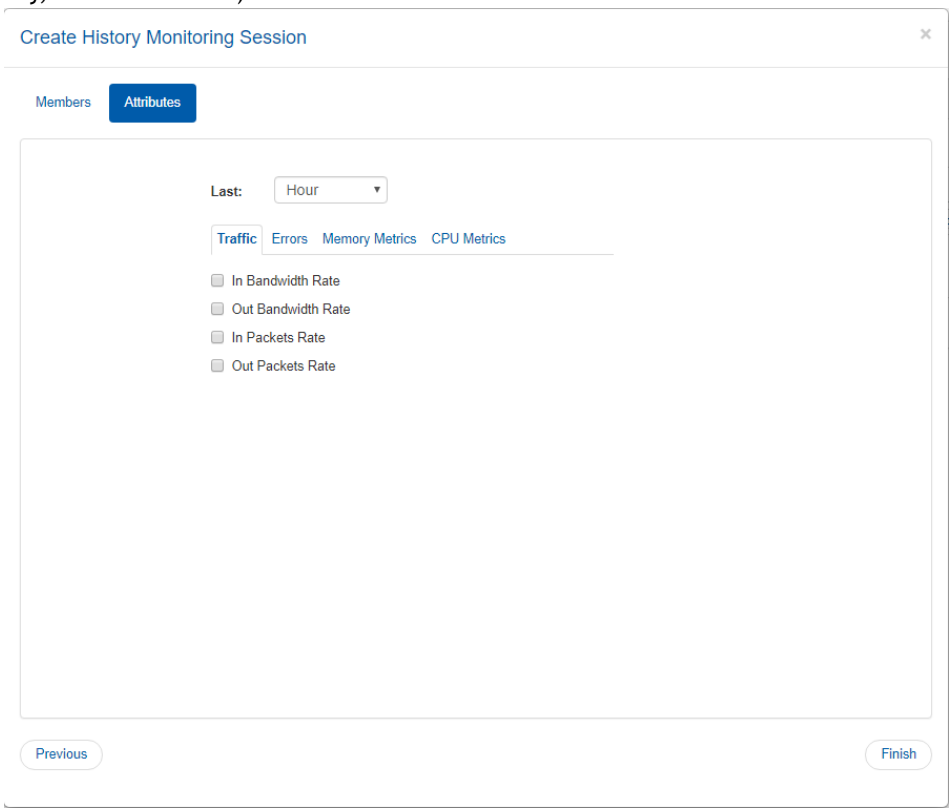
button.

2. Choose the devices or ports you wish to generate a report for under “Members” (available objects: device, port).



3. Check the checkboxes of the attributes you wish to monitor their values (available attributes are listed in the table below), and define the time frame of the report (over the last hour,

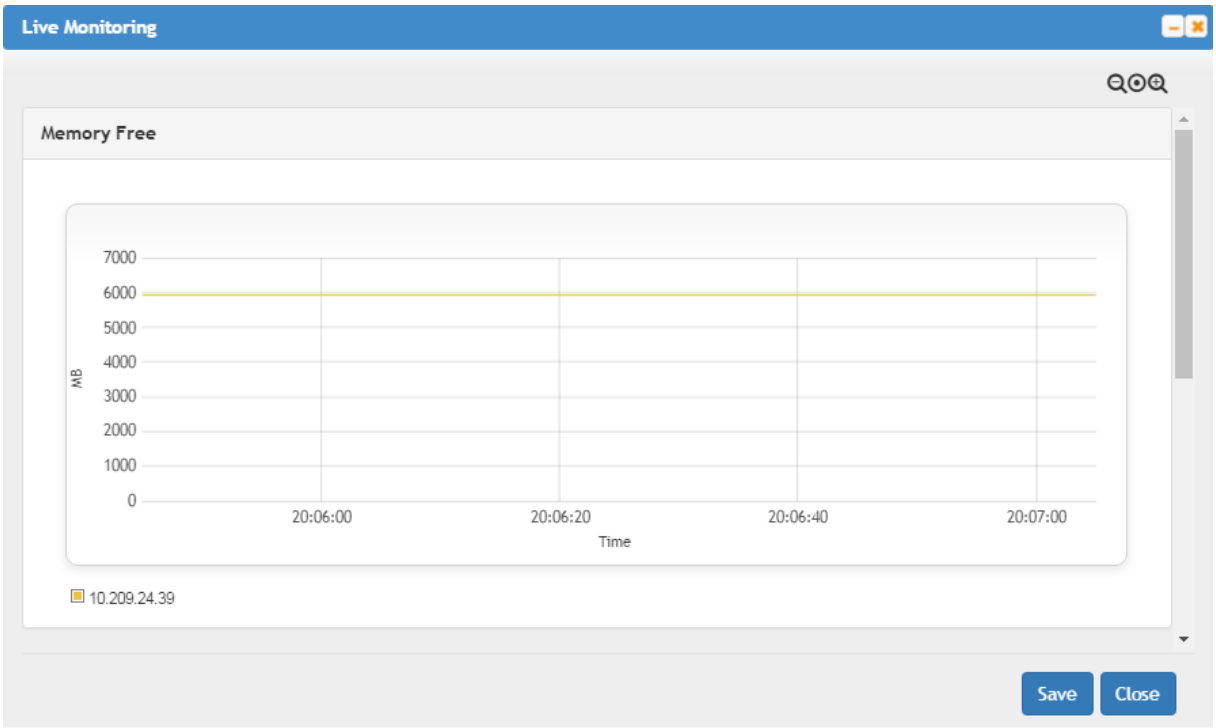
day, week or month).



History Monitoring Available Attributes

Available Objects	Available Attributes
Devices	Counters
	Errors
	Memory Metrics
	CPU Metrics
Ports	Counters
	Errors

4. Once clicked “Finish”, the report will be generated.

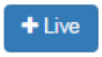


For saving the generated reports, see “Saving Reports”.

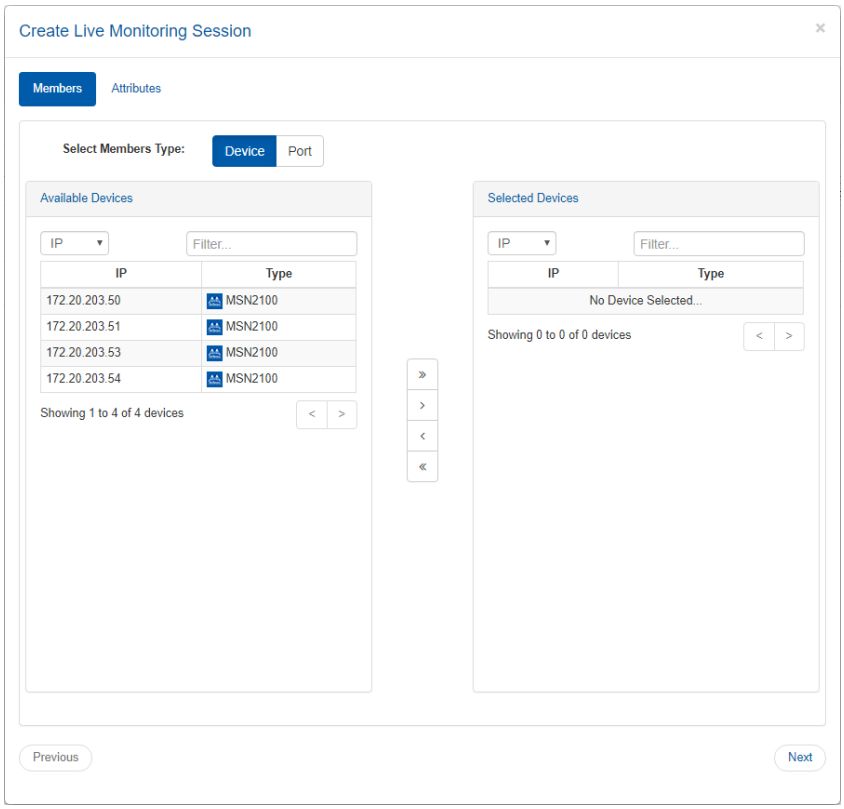
Live Monitoring

Provides a live report of the device attributes values.

To create a live monitoring session:

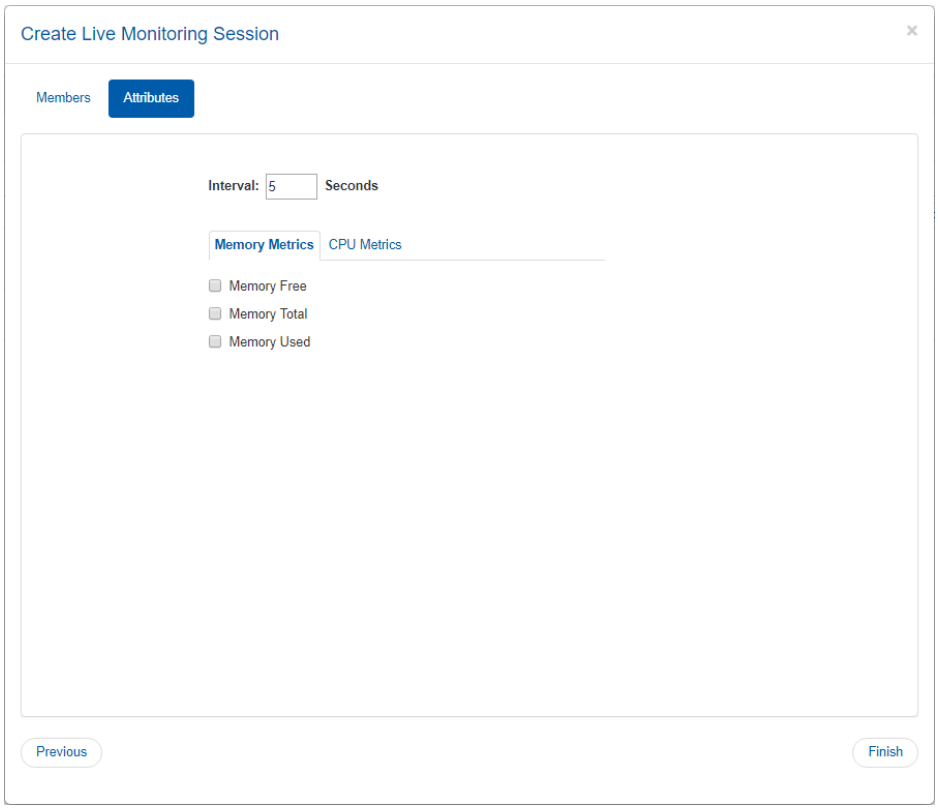
1. Click the 

button.
2. Choose the devices or ports you wish to generate a report for under “Members” (available objects: device, port).



3. Check the checkboxes of the attributes you wish to monitor their values (available attributes are listed in the table below), and define the interval of the monitoring (the minimal monitoring interval can be as low as 2 seconds).

> ⚠ The minimal interval of 2 seconds applies to Spectrum and SwitchX switches, while for other devices, the minimal interval is 20 seconds for ports, and 5 seconds for devices.



Live Monitoring Available Attributes

Available Objects	Available Attributes
Devices	Memory Metrics
	CPU Metrics
Ports	Counters
	Errors

4. Clicking Finish starts the monitoring session.

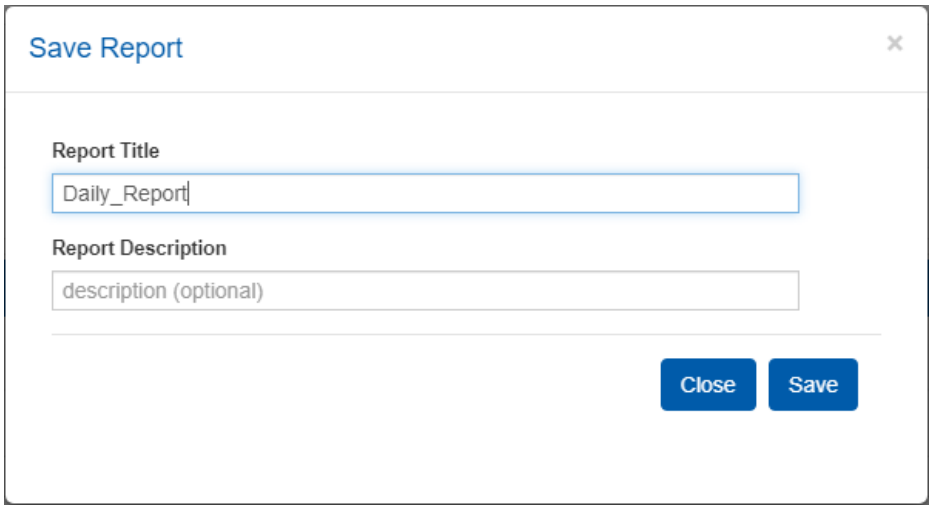
For saving the monitoring session, see "Saving Reports" section.

> ⚠ Live Monitoring is not supported for third party switches (non-Mellanox switches), but is supported for the ports of those switches.

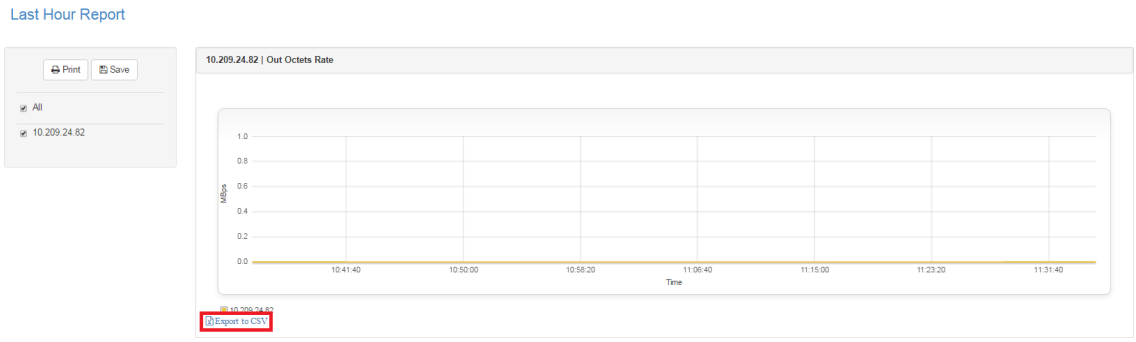
Saving Reports

The generated reports can be saved or printed by clicking on the designated buttons.

- A Report Title can be composed of 4-20 alphanumeric characters, as well as "_" (underscore) and "-" (dash). See "Appendix – Mellanox NEO GUI Fields Validations".
- The Report Description field is optional, and can contain an unlimited number of characters.



- Users can save a report within 30 minutes from its creation time.
- Once a report is generated, it can be exported to a CSV file.
    - If the report was generated for multiple devices – the CSV file can only be created if each graph contains a single device ("Group by Counter" checkbox on the left side of the graph is unchecked).
    - If the report was generated for a single device – the option of creating a CSV file will automatically become available.



- Removing temporary reports is done by a garbage collector mechanism that is activated every 5 minutes.
- By default, the maximum number of reports that can be saved is 200, while each user can save up to 20 reports (the administrator can keep saving reports even after reaching the 20 report limit, but once the system's 200 report limit is met, no additional reports could be saved, unless reconfiguration is performed).

To configure the maximum number of reports to save:

1. Open the /opt/neo/controller/conf /controller.cfg file.
2. Find the Report section.
3. Set the maximum allowed number of saved reports in the system by changing the `max_reports_per_system` value (the default is 200).
4. Set the maximum allowed number of saved reports per user by changing the `max_reports_per_user` value (the default is 20).
5. Restart Mellanox NEO-controller.

To configure the report's garbage collector cycle interval:

1. Open the /opt/neo/controller/conf /controller.cfg file.
2. Find the Report section.
3. Set the `garbage_collector_interval` value to the desired number (the default is 5 minutes).
4. Restart Mellanox NEO-controller.

Streaming

Streaming is supported on Spectrum systems with either Onyx or Cumulus operating systems.

Predefined Sessions

For every Telemetry Agent controlled by Mellanox NEO, the sessions below are defined by default:

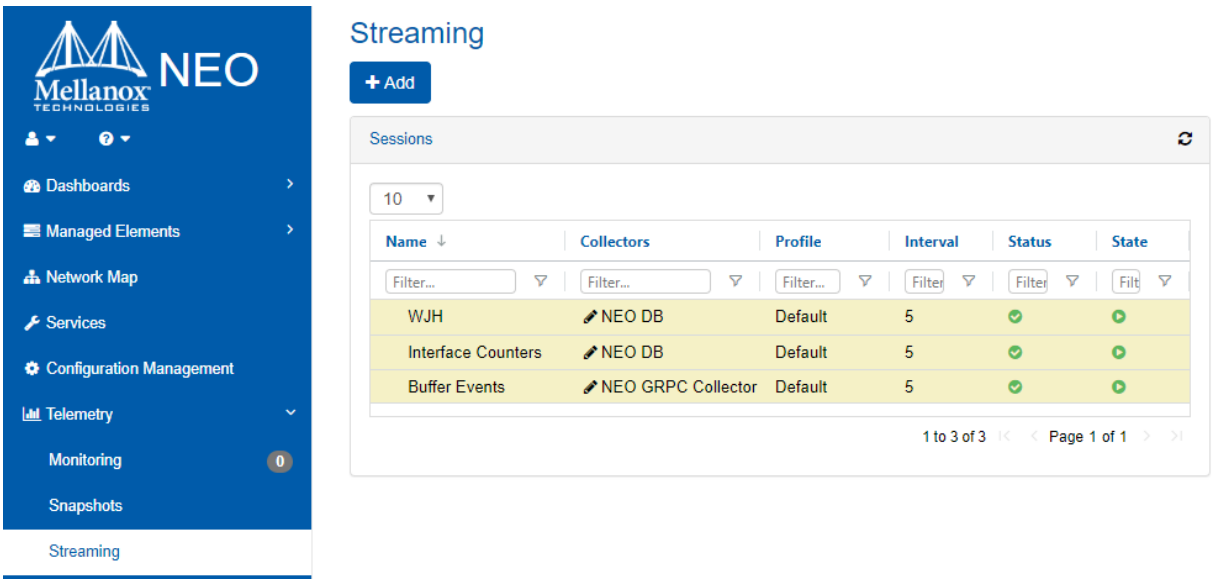
- WJH
- Interface Counters
- Buffer Events

By default (when Telemetry Agent is started on the switch) only “Interface Counters" session is enabled (activated).

These sessions retrieve information for various NEO views. They cannot be edited or deleted, and devices will be automatically added to/removed from them according to their telemetry capability. Some of them can be enabled or disabled by need.

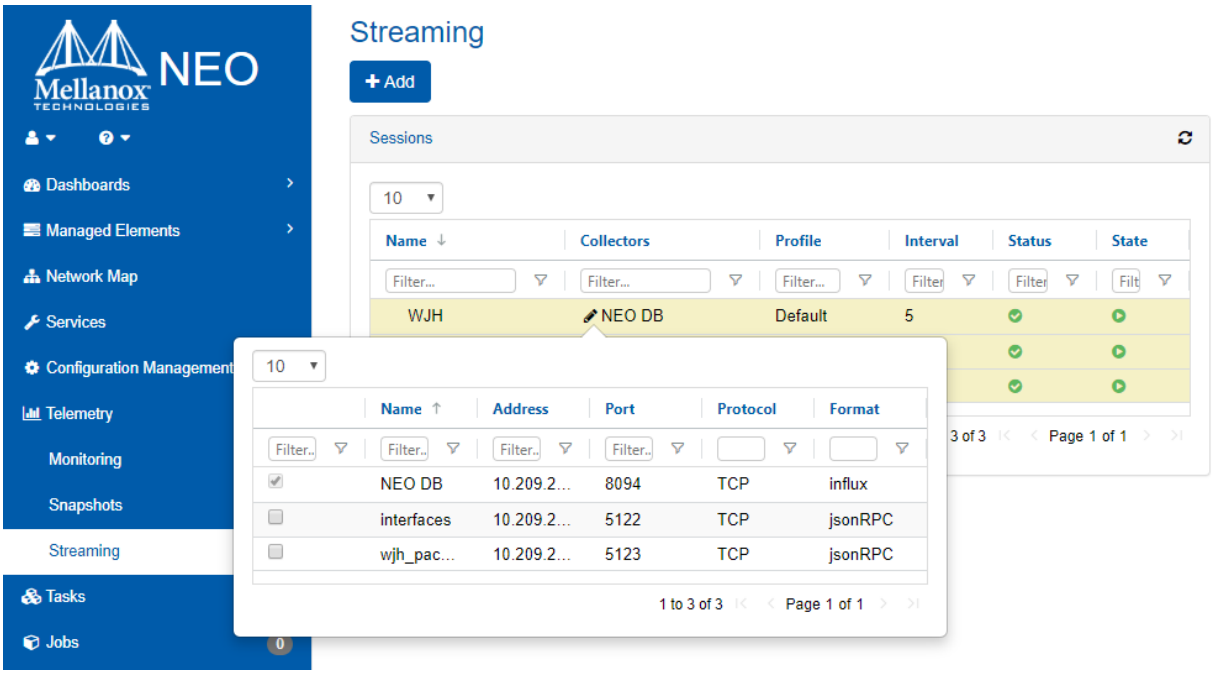
To perform an action on an added session, right-click on it, and select "Disable/Enable", "Modify Members" or "Delete".

The default streaming sessions are:



- WJH – samples the dropped packets buffer, and streams the data to Mellanox NEO.
- Interface Counters – samples interface counters. Please refer to the "Supported Telemetry Data Streaming" page of the Telemetry Agent User Manual for more information on the supported profiles and the available counters per profile.
- Buffer Events – samples the buffer histogram and creates an event every time the defined threshold is crossed. To view the buffer histogram when an event is created, go to Network Map, and click on "Buffers Utilization" under Network Analysis. For more information, see “Network Analysis”.

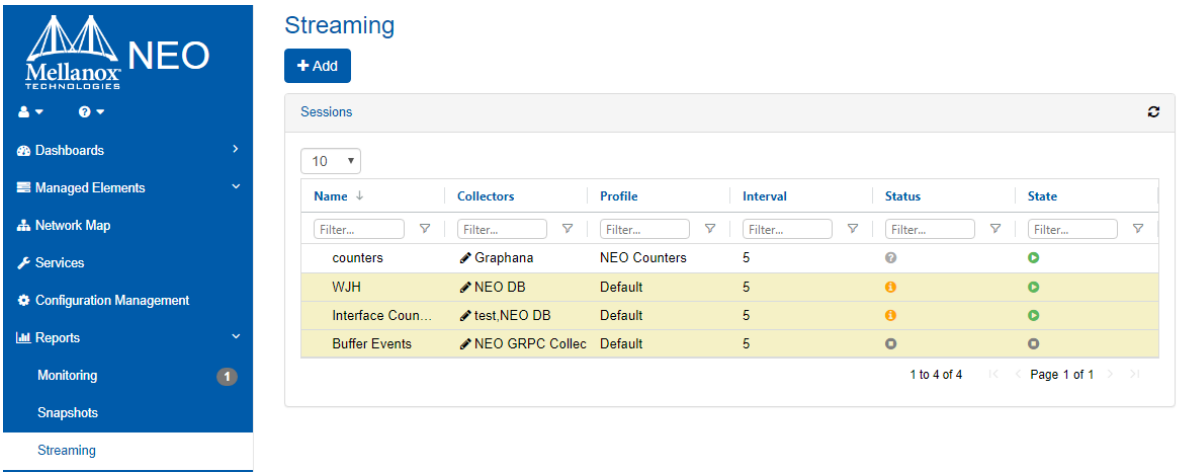
To perform a change of collectors to an existing session, go over the pencil mark under Collectors and mark the relevant collectors to add.



Sessions Management

View Session

In order to view all available sessions, go to “Telemetry”→”Streaming”. A table will appear with a list of all sessions, including the predefined sessions marked in yellow.



Create a New Session

To add a new streaming session, click on the “New” button, insert the new session’s name, and fill-in the required parameters:

- Profile: Select one of the profiles -
  - NEO Counters
  - Traffic Counters

    - Priority Counters
    - Buffer Histograms
    - FDB Table
    - Routing Table
- Interval: The time interval for the data collection
- Data Collectors: The collectors to which the data will be sent. For more information on defining the collectors, you can use the pencil icon, or refer to “Data Collector”.

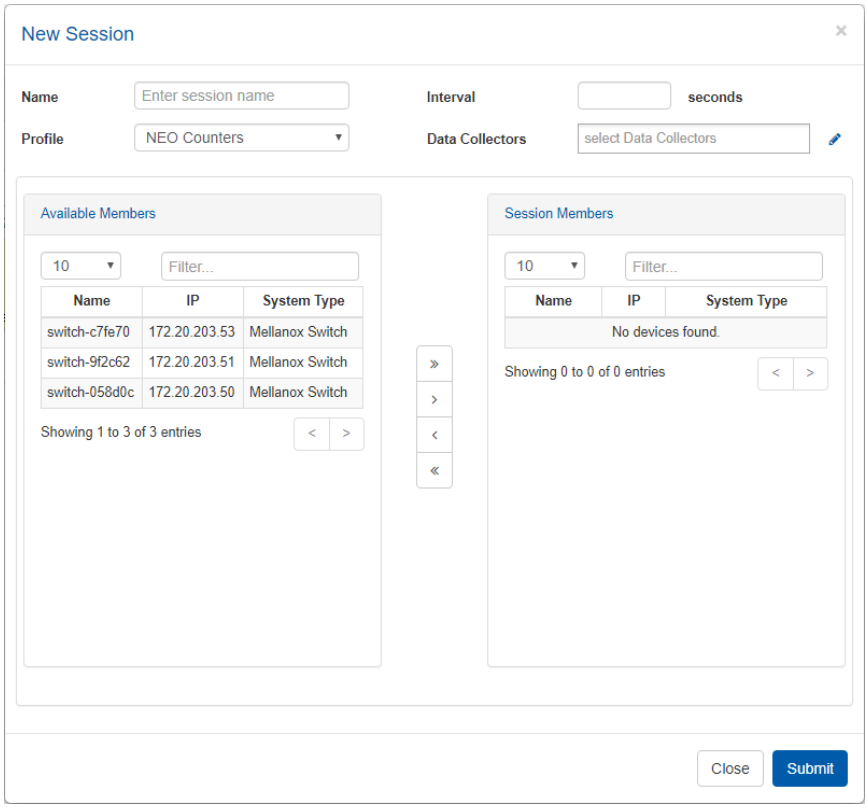
> ⚠ It is possible to define up to five sessions per system, and one per type.

> ⚠ It is impossible to create more than one session on the same profile for a specific device.

> ⚠ Before starting a buffer histogram session, make sure to configure the relevant traffic class on the switch using the “Enable Histogram” template.

> ⚠ Use the “Enable Histogram” template to configure default session “buffer events”.

> ⚠ Before running the routing profile, make sure it is enabled on the switch (run "ip routing").



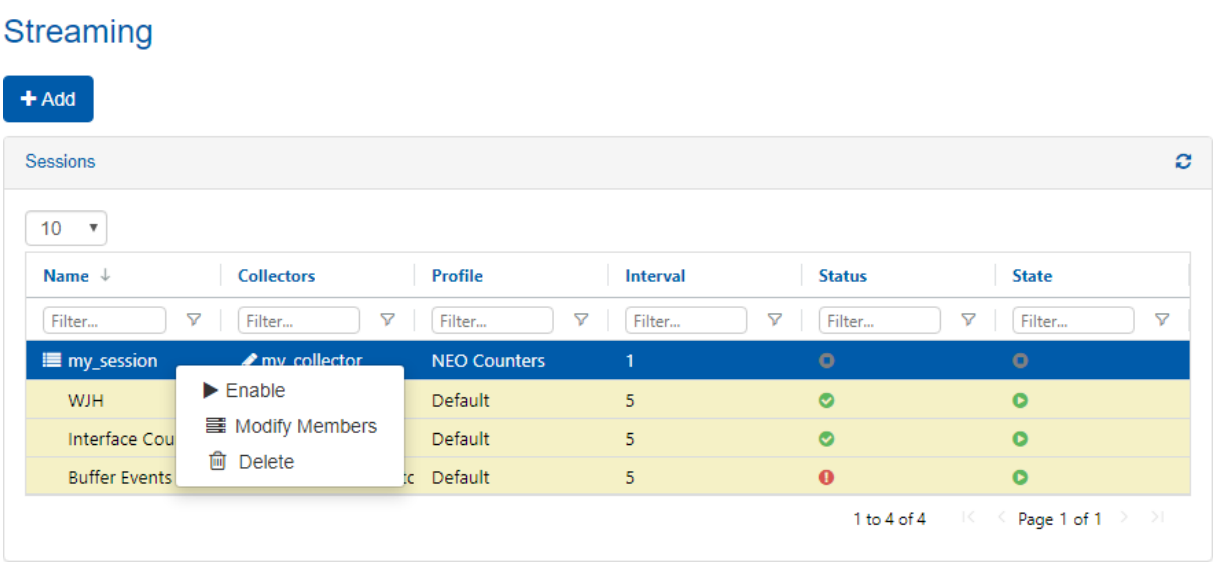
Telemetry Agent Supported Counters Per Profile

Please visit the Telemetry Agent User Manual under Appendixes>Supported Telemetry Data Streaming>Supported Counters Per Profile for more information.

Enable/Disable Session

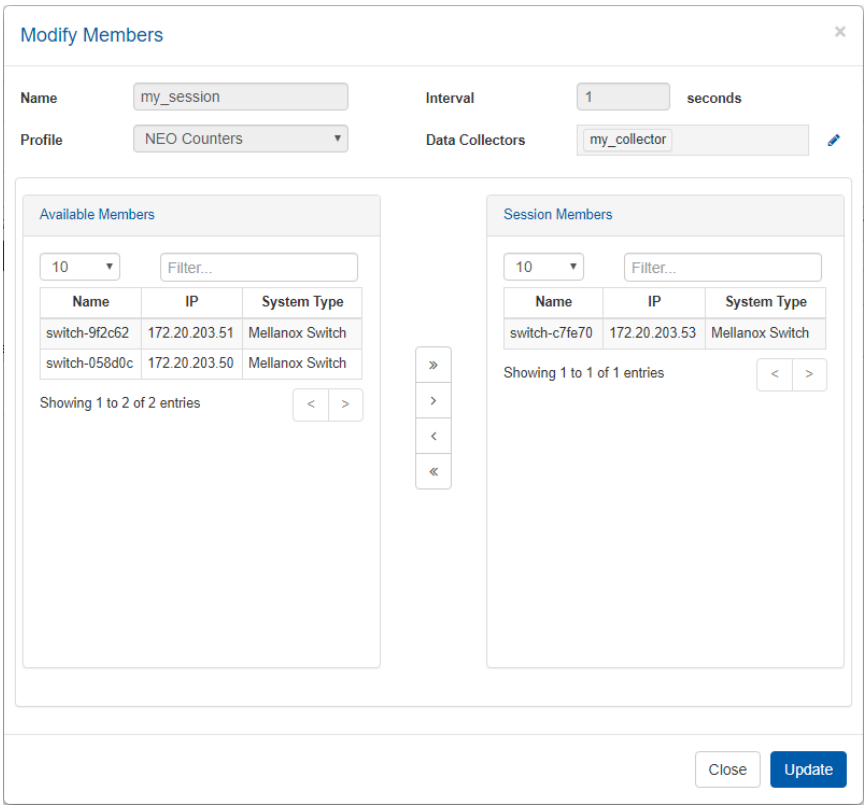
To enable or disable a session, right-click on it, and select the desired action: Enable/Disable.

> Warning: Running multiple sessions in high frequency may lead to high switch CPU conception.



Edit Sessions Members

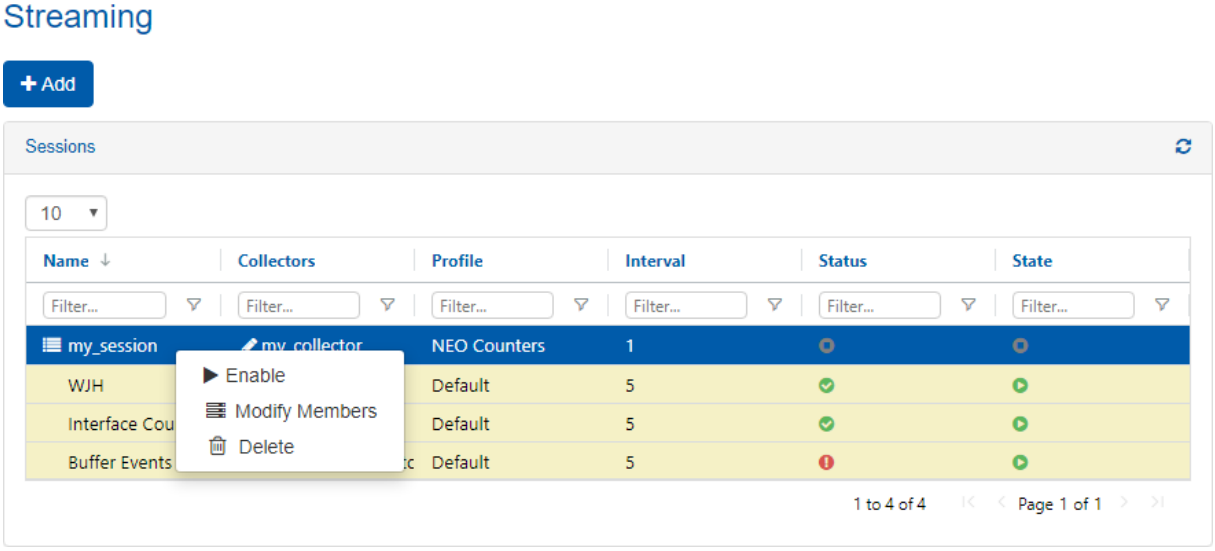
To modify the session members, right click on a session, and select “Modify Members”. The session member's view will open. You can use the arrows to add and remove members from a session. You can run only one session per profile and no more than 5 sessions (in total) per switch. Each session can be sent to several collectors.



You can run up to one session per profile, and each session can be sent to up to 3 different collectors (destinations).

Delete Session

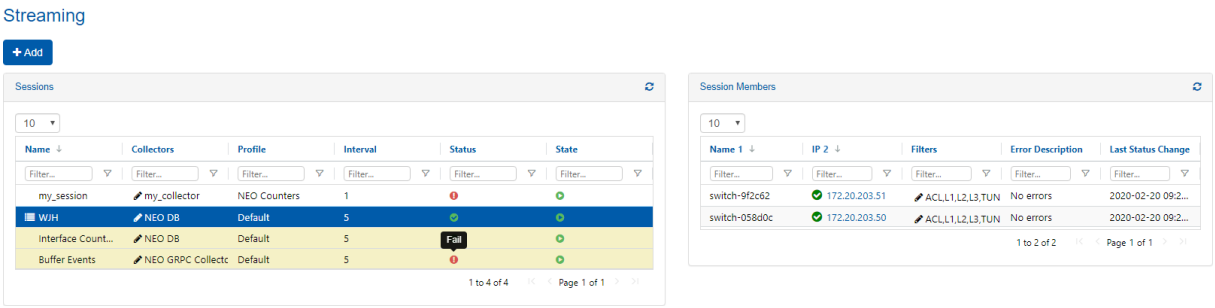
To delete a session, right-click on it, and select "Delete". When deleting a session from the sessions table, the specified session will be stopped on all session members (switches) that are currently running it.



Session Members Status

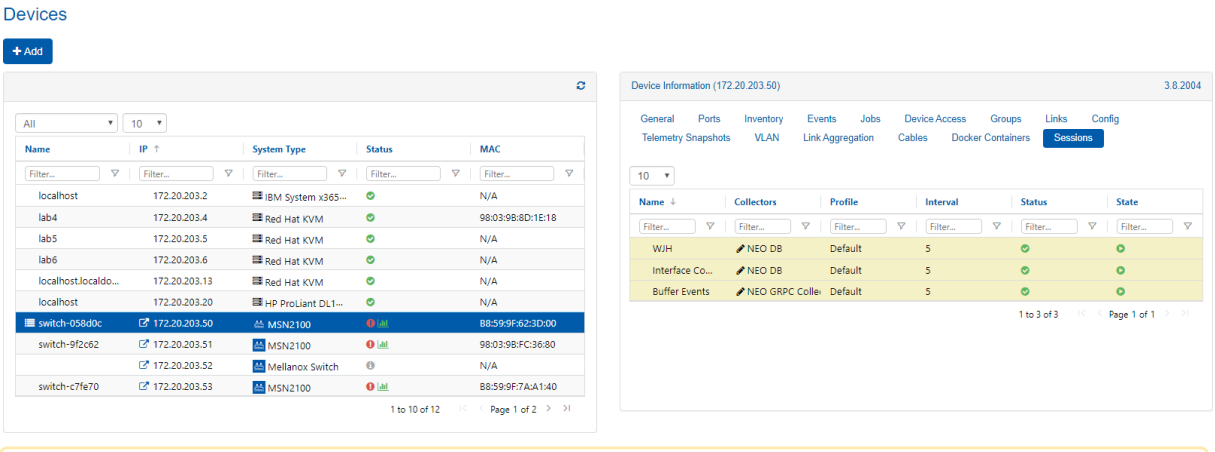
To view the status of session members, click on the session, and a table with the following parameters will appear on the right side of the screen:

- IP: System IP
- Status: OK, Fail/Warning or Stop (green, yellow or gray icon, respectively)
- Error Description: Will be displayed only in case there is a general telemetry error
- Last Status Change: Specifies the exact time in which the last status change occurred.



Device Sessions Information

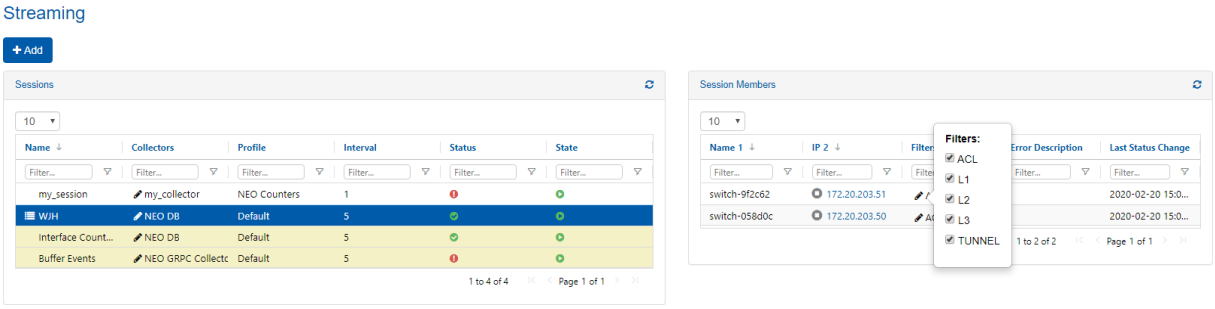
You may view the running sessions and the sessions status of each device, by selecting “Managed Elements”-->”Devices”, and clicking on the relevant device. The “Sessions” tab will appear in the “Device Information” panel on the right, as shown below. In case of a problem with the session, the problem type will be reflected in the session status.



> Running multiple sessions in high frequency may lead to high switch CPU conception.

What Just Happened Filtering

For WJH session, it is possible to get drops of specific categories only and silence alerts about other categories. Unselected categories will not be streamed, thus it is recommended to select all the wanted categories.

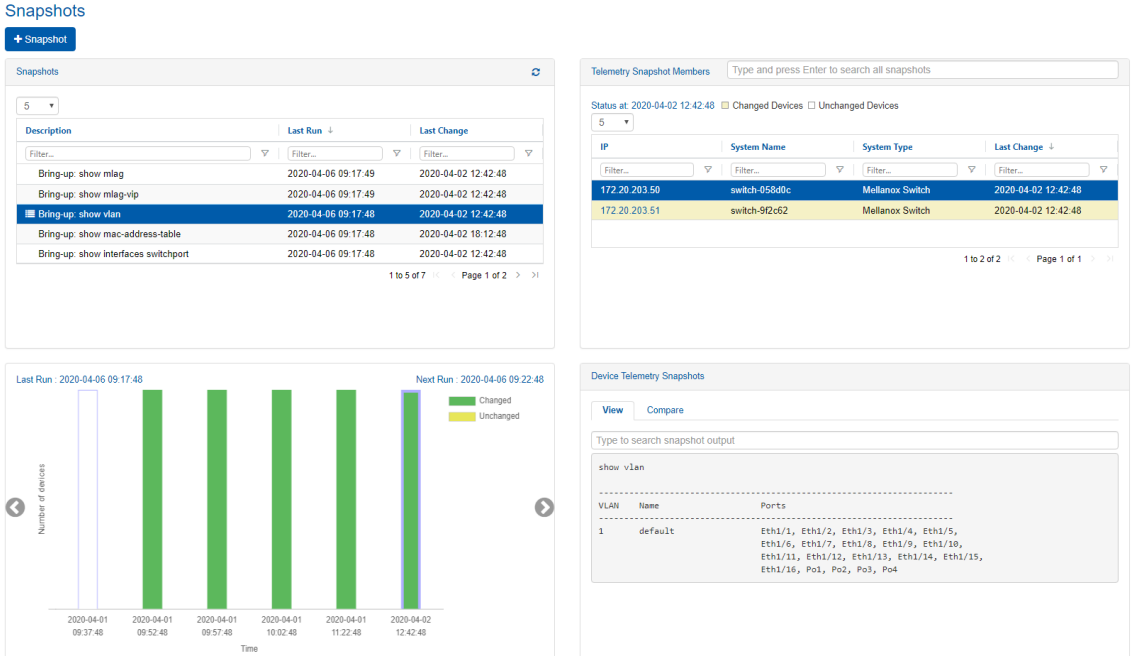


Snapshots

Telemetry snapshots allow the user to store snapshots of commands running periodically if the output was changed, and allow the user to search, view and compare these snapshots.

To create a telemetry snapshot:

1. Click the + Snapshot button:



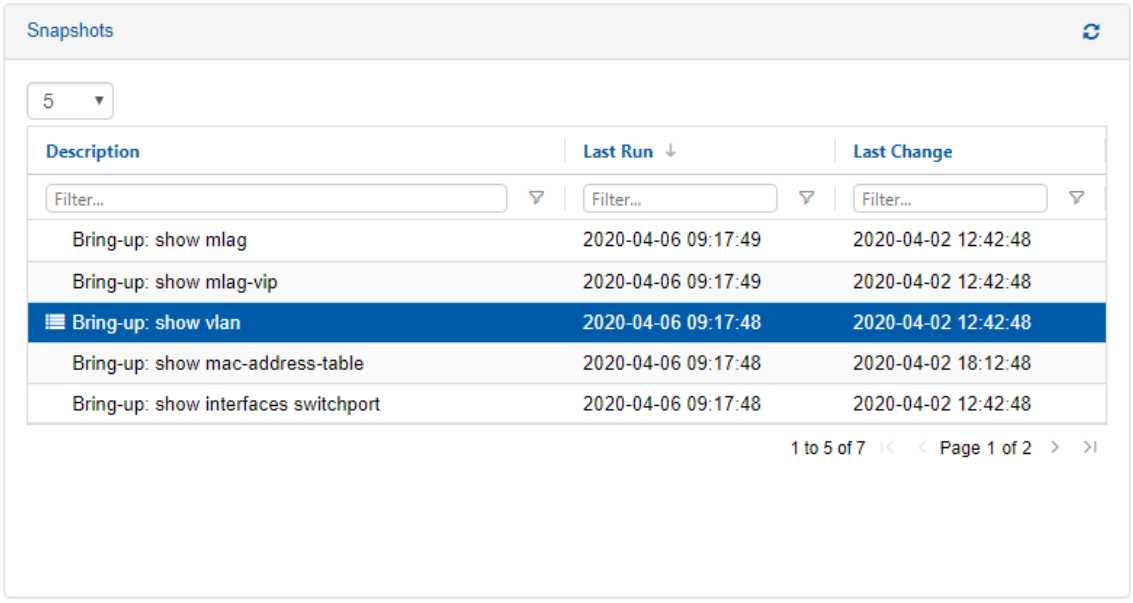
2. Select devices or group of devices.
3. Select a template or a command.
4. Select snapshot interval.
5. Click Finish.

> Right clicking an existing snapshot allows the user to run it immediately, edit, or delete it.

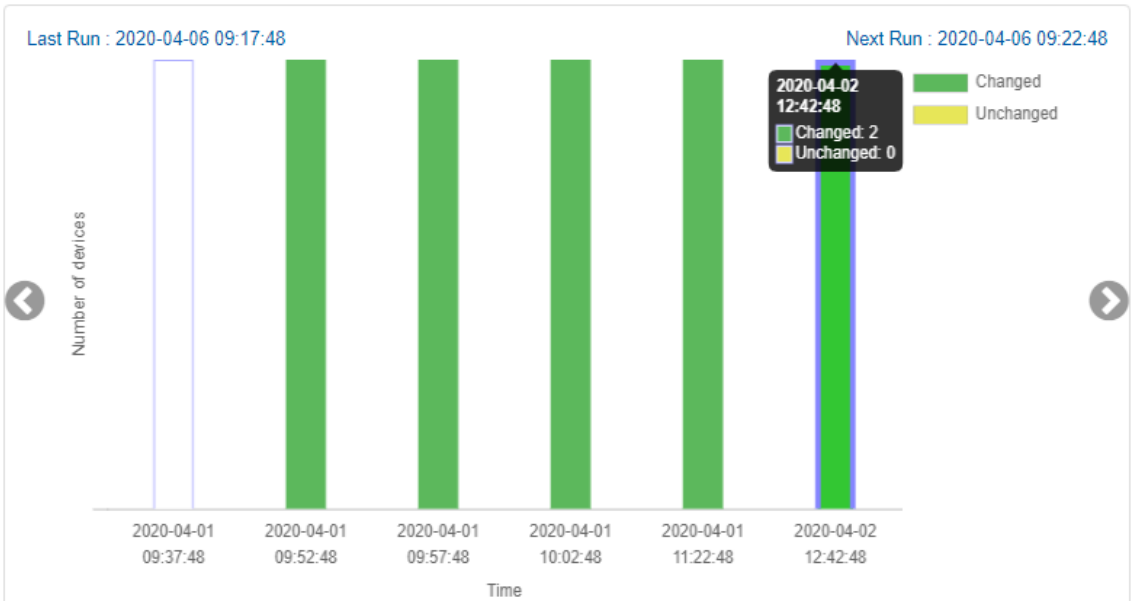
Snapshots Tab

The Snapshots tab displays information about all the snapshots that were taken, and it is divided to four sections:

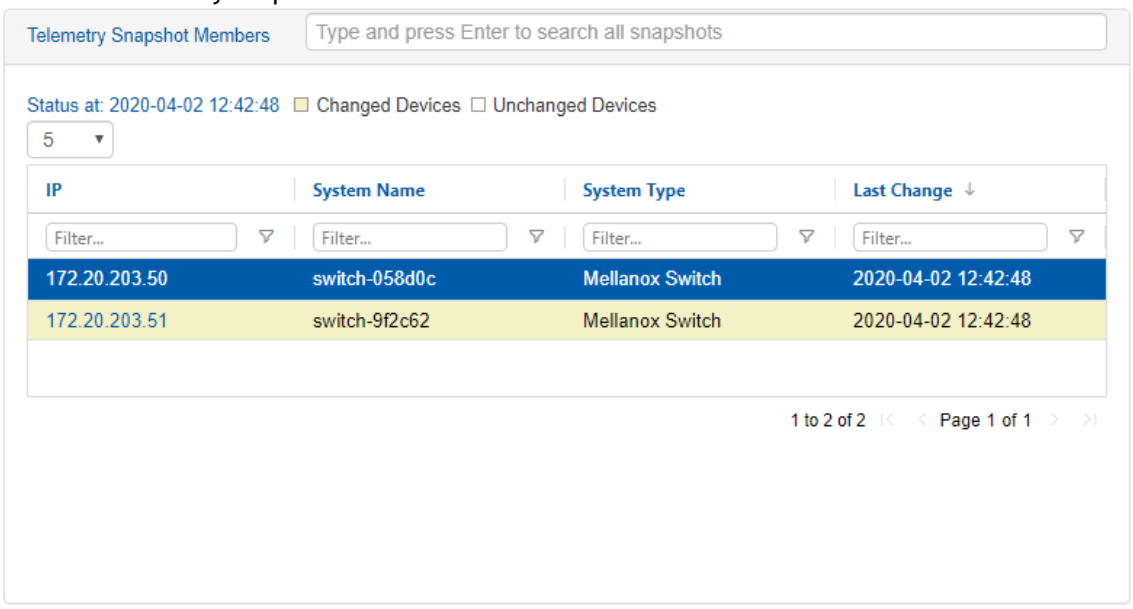
- The snapshots section displays all the telemetry snapshots configured by the user.



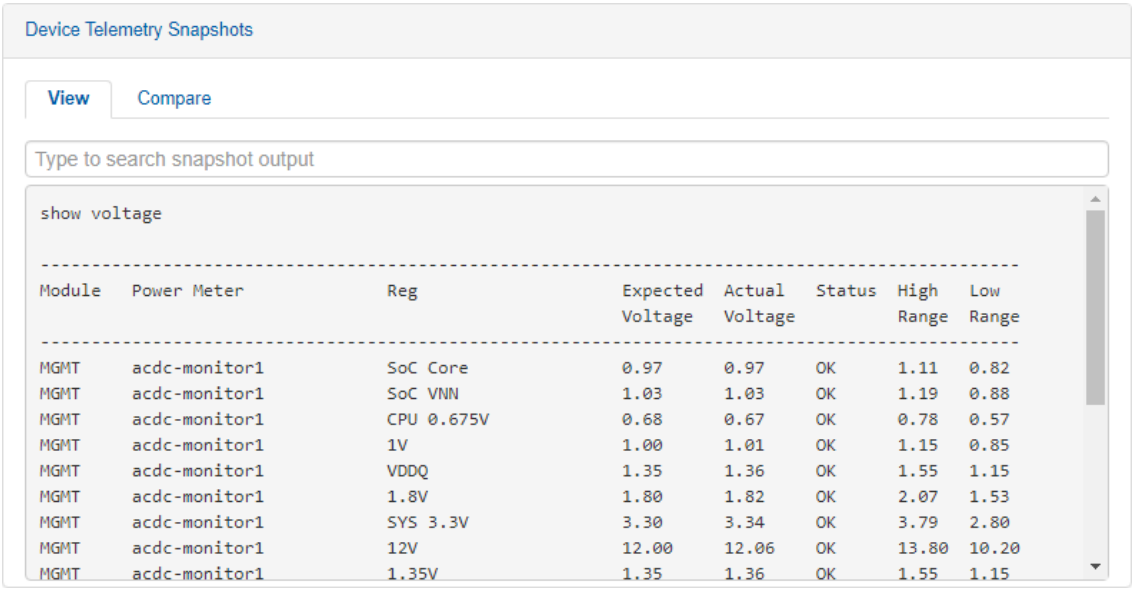
- The selected snapshot timeline displays the times of latest changes detected.



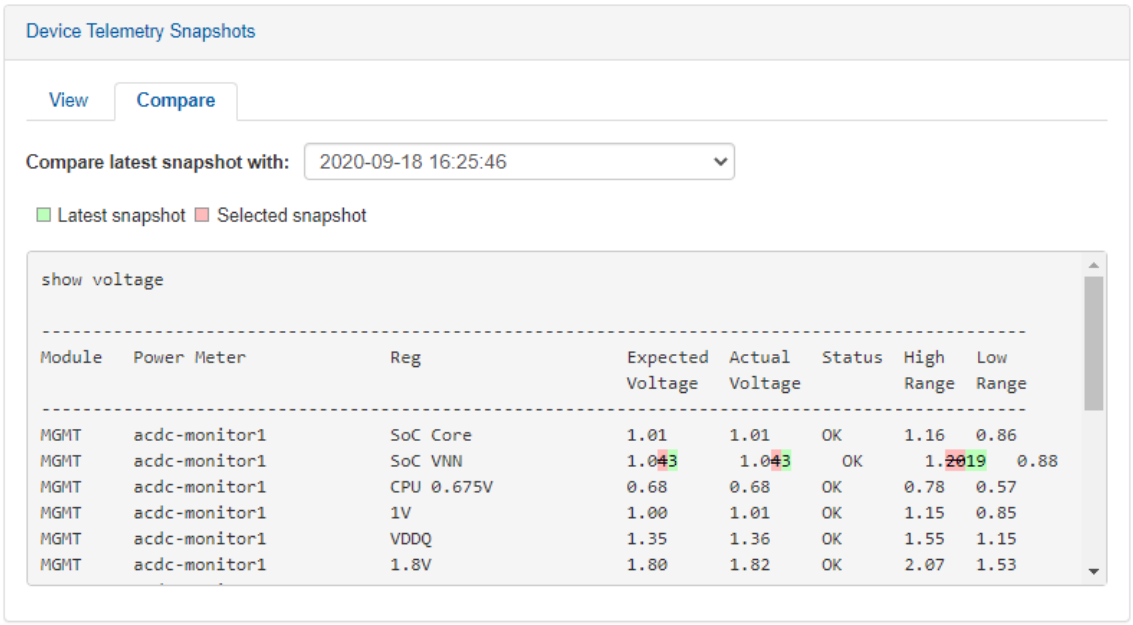
- Telemetry Snapshots Members displays a list of the devices which are members in the selected telemetry snapshots.



- Device Telemetry Snapshots displays the content of the selected device snapshot.



- The Compare tab displays the differences between the selected snapshot and any other snapshots.



Tasks

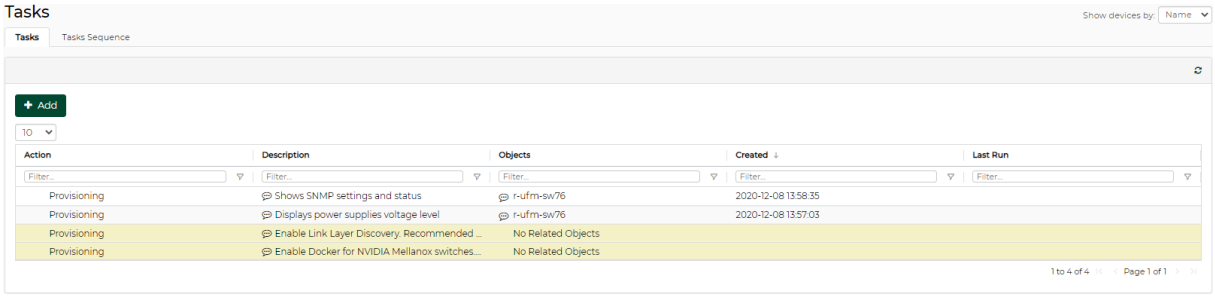
The Tasks window displays the full Mellanox NEO® tasks list.

A task is an action defined by a user to apply on one or more devices, ports, or groups. Users can create a task or a task sequence, using the respective tabs under this window.

All of these tasks can be saved with no execution date, set to run immediately (in which case, it will turn into a job), or scheduled to occur once or repeatedly in a predefined time.

Tasks Tab

This tab enables you to create, run, remove and edit tasks.



Built-in Tasks

NEO comes with the following built-in tasks for common switch configuration. These tasks can run on all applicable switches (*Run On All* option) or on a user selected list of switches (*Run* option):

- Enable Docker for Mellanox switches – activates docker capabilities on the switch

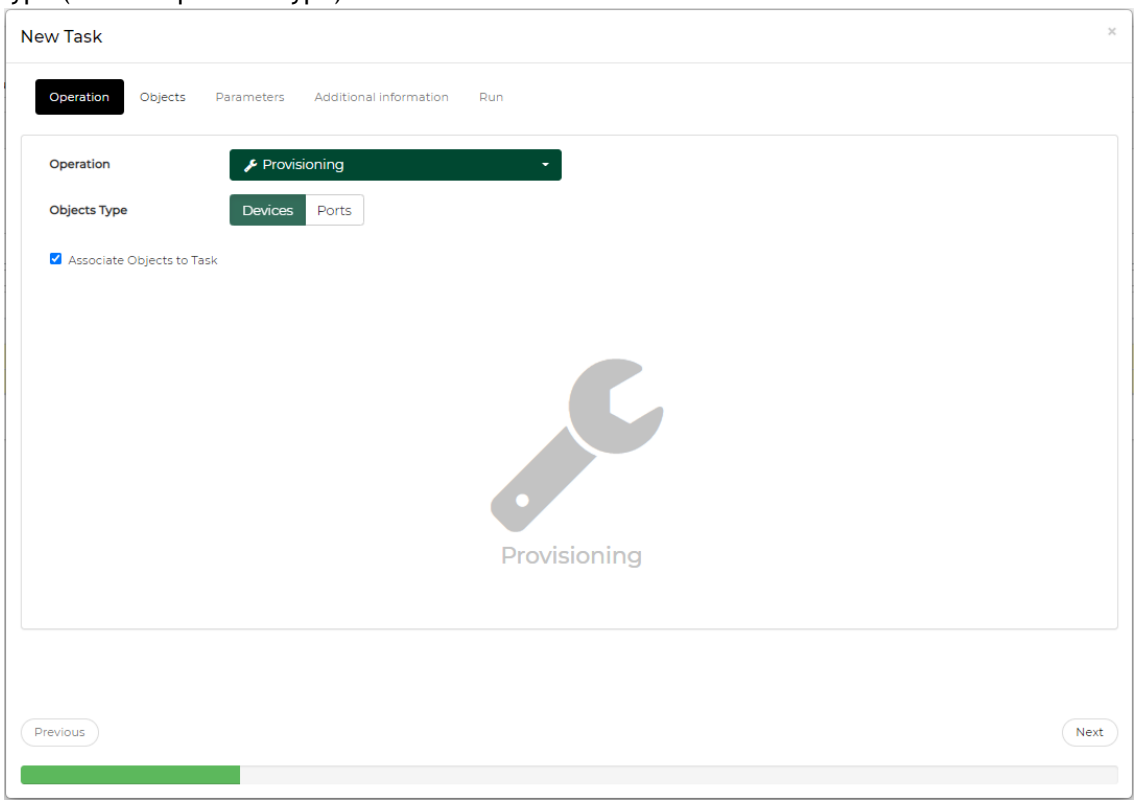
- Enable Link Layer Discovery – activates LLDP capabilities on the switch. Enabling this is recommended for network topology discovery.

> These tasks are applicable to switches running Mellanox Onyx only.

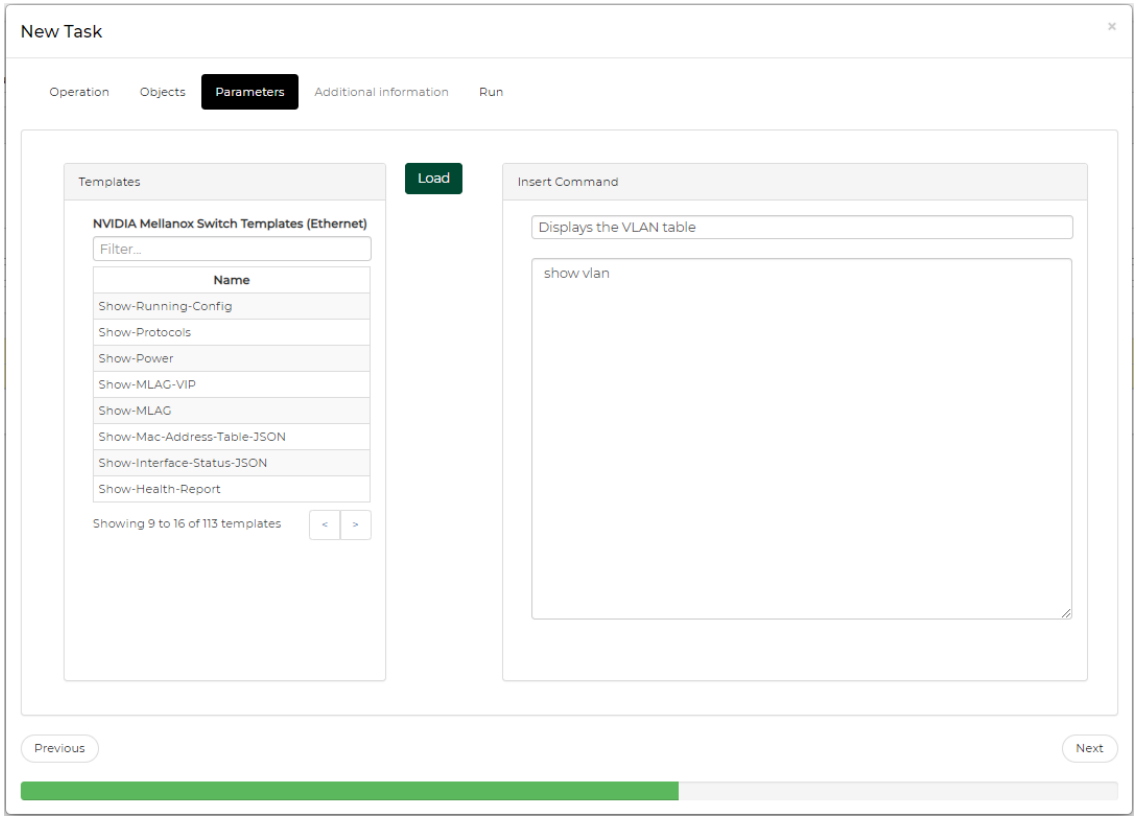
Creating a New Task

To create a new task:

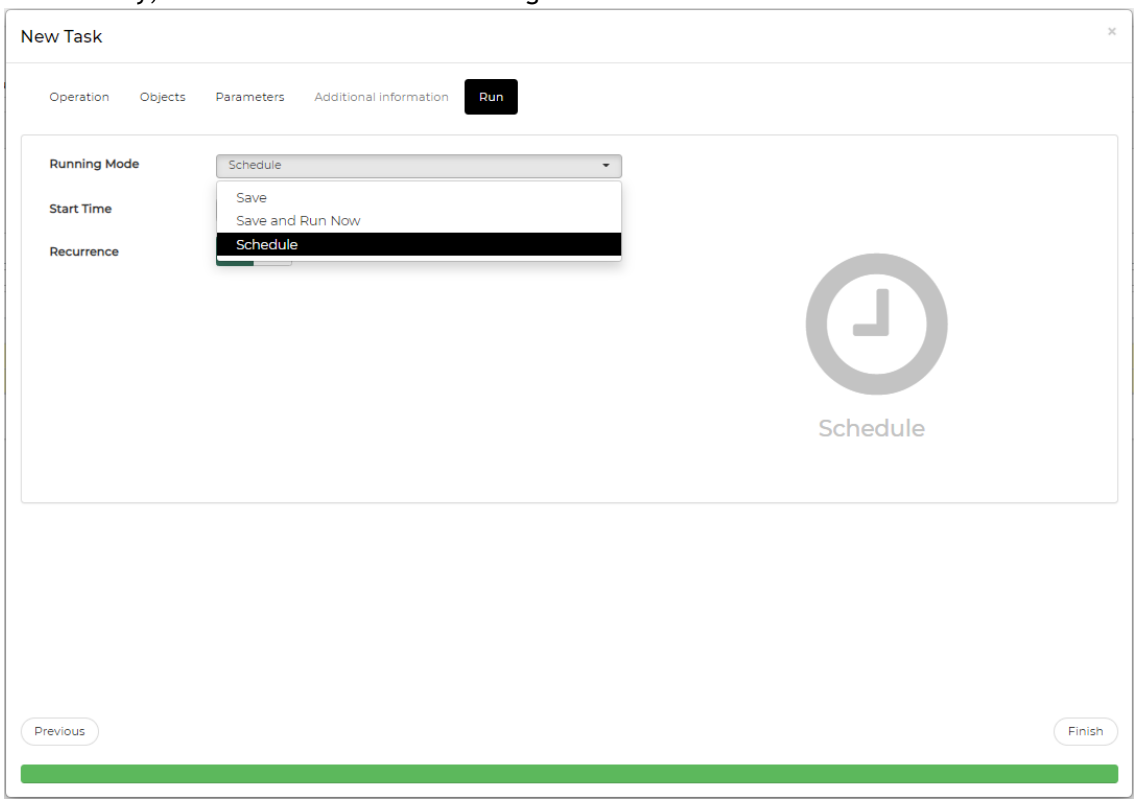
1. Under the Tasks tab in the "Tasks" panel, click "New". The Tasks wizard will open and allow you to select the desired operation: Provisioning, Onyx Software Upgrade, Driver Install, Apply Config, Generate Dump or Reboot.
2. You may associate the task to specific devices, ports, or groups by checking the "Associate Objects to Task" checkbox. If the checkbox is left unchecked, a template will be generated, and you will be required to select objects only when running the task.
   Note: When creating a task for a number of ports, these ports have to belong to the same type (for example: Eth type).



3. Click the "Next" button. In some cases, you will be requested to fill in several necessary parameters and provide additional information before the task can be executed.



4. The "Run" tab allows you to save the generated task as a template, save and run it immediately, or schedule a different running time.



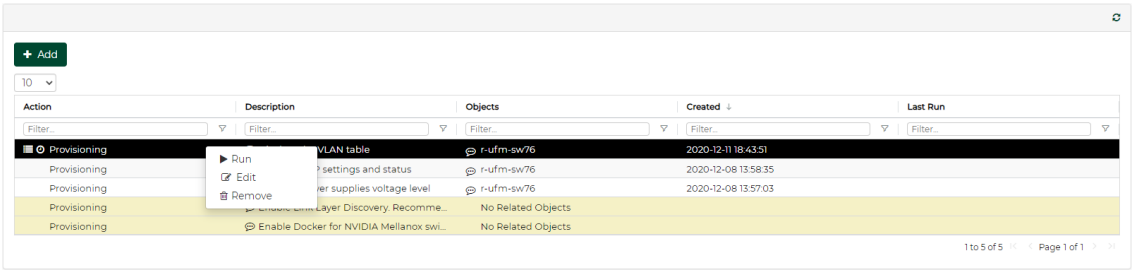
If you wish to generate a recurring task, select "Schedule" as the Running Mode, and check

the "Recurrence" checkbox. Insert the desired start time, interval units, interval value and end time. Click the "Finish" button to complete the process.

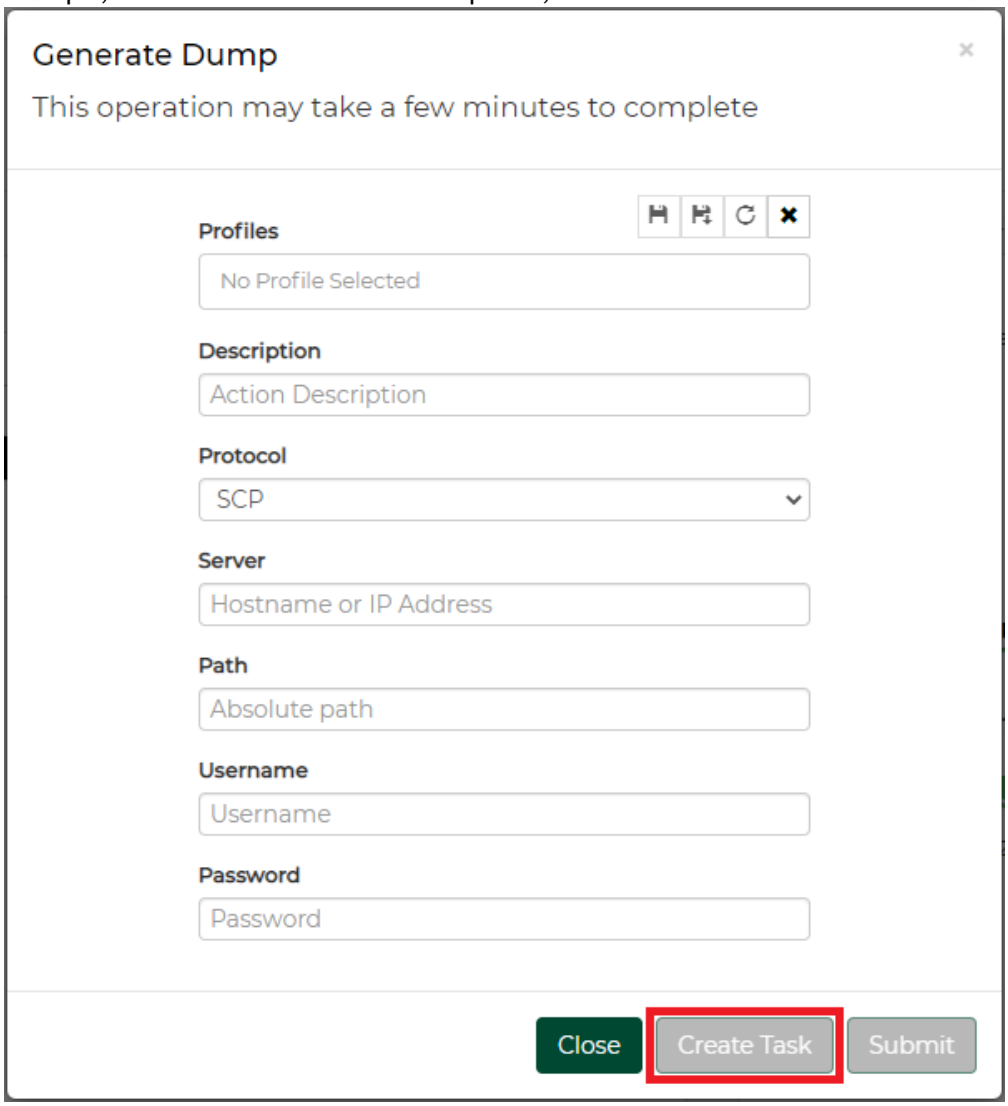
- If the task's execution has been scheduled for a later time, a small clock icon ( ) will appear next to its listing.

Task Actions

- To view the task's properties, click the small speech balloon icon ( ) in the description column.
- To run a task on all devices in the network, right click on it, and select "Run on all". Note that the "Run on all" option is only supported in tasks that are not associated with specific objects ("No objects" in the Objects column).
- To edit a task, right click on it and select "Edit".
- To remove a task, right click on it, and select "Remove".



- A new task can be generated through the Managed Elements panel as well. Go to "Devices" or "Groups", choose one of the available options, and click the "Create Task" button:

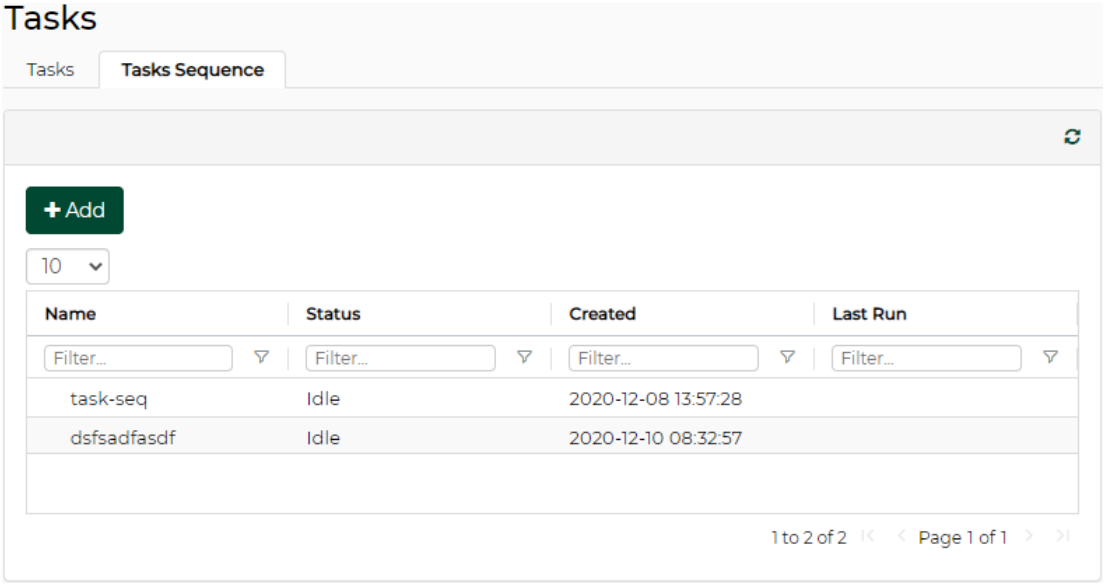


Task Sequence Tab

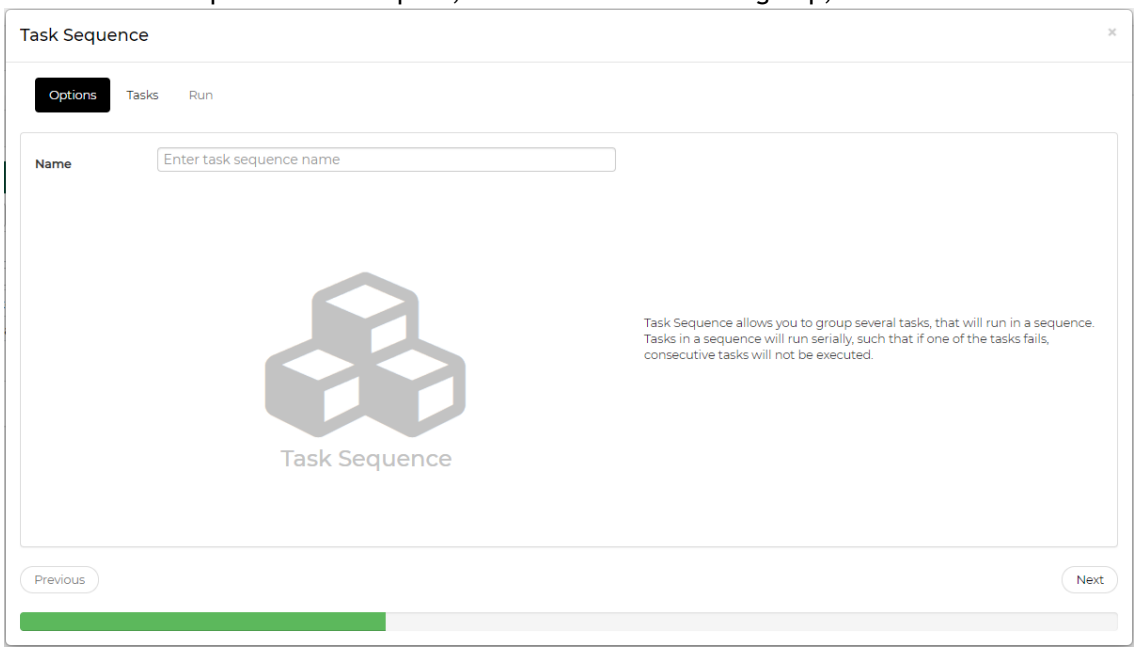
A group of tasks can be set through this tab to run successively. Users can determine the order of tasks within the task sequence.

To create a new task sequence:

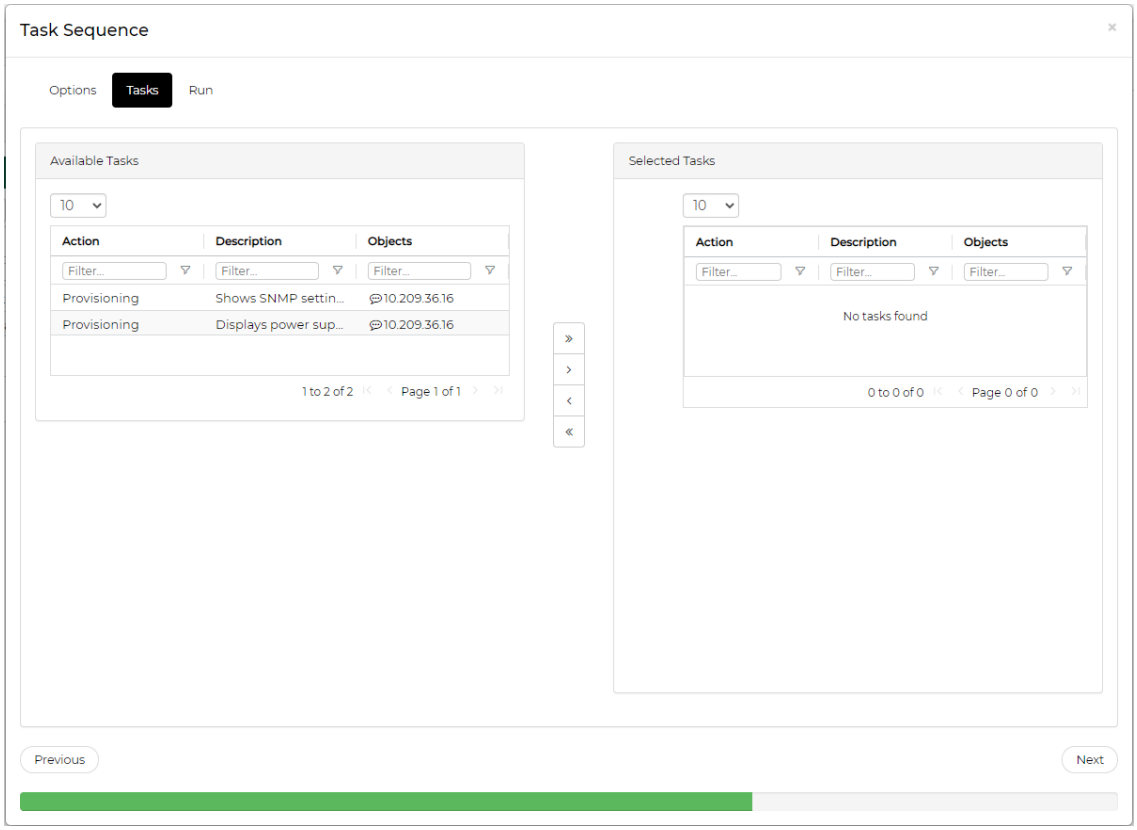
1. Click the "Add" button under Task Sequence.



2. Once the Task Sequence wizard opens, set a name for the task group, and click "Next".

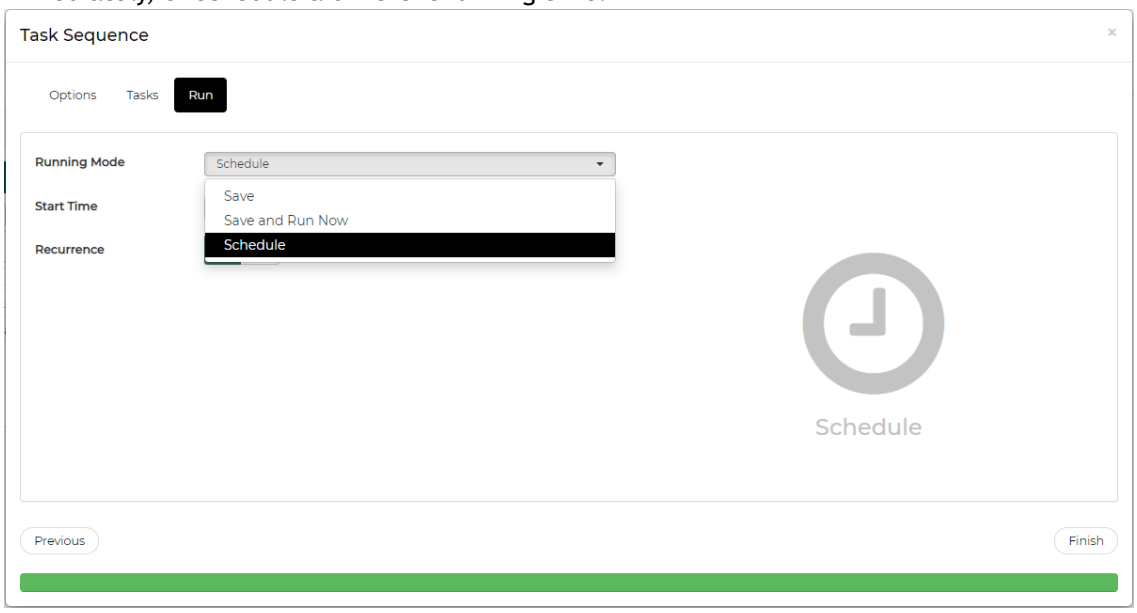


3. Choose the tasks from the list of Available Tasks and click "Next".



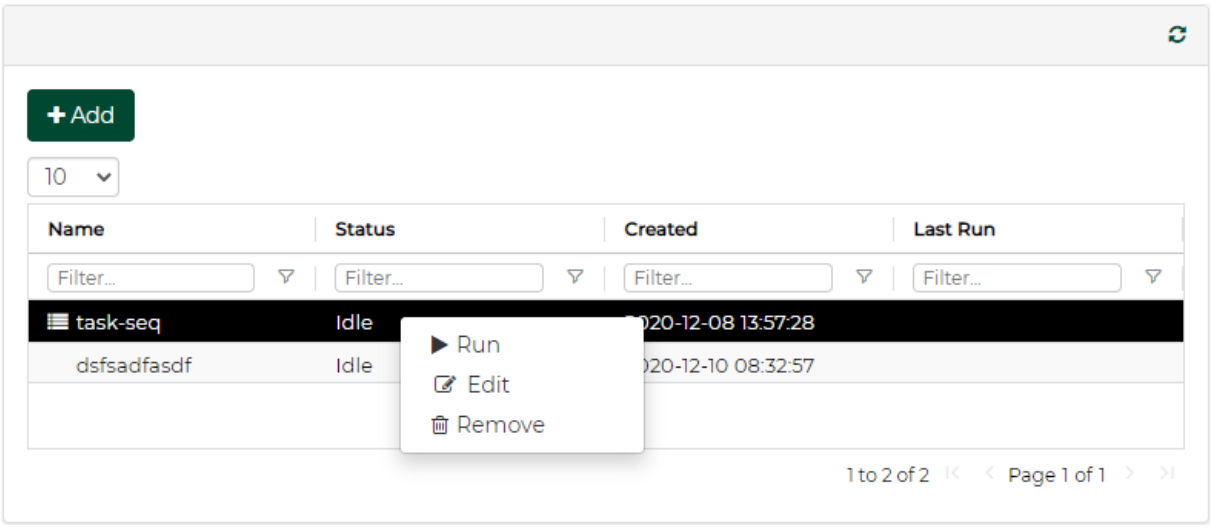
> You can re-order the sequence of tasks by clicking one of the tasks in the right pane and moving it up or down.

4. The "Run" tab allows you to save the generated task sequence as a template, save and run it immediately, or schedule a different running time.



5. Click "Finish" to complete the process.

A right-click on the newly created task sequence will enable running (in case no scheduling was set), editing, and removing it.



Notes:

- If a task is already scheduled to be run at a certain time, it will not appear in the list of available tasks. In order for it to appear, its scheduling should be removed, or alternatively, it could be recreated.
- If one task fails in the chain, the rest of the tasks that follow will be skipped and the process will not be completed successfully.
- If a device is part of a task sequence, users will not be able to remove it from the devices list.
- If a task is part of a task sequence, users will not be able to remove the task unless it is removed from the task sequence first.

Jobs

The Jobs window displays all Mellanox NEO® running tasks which were defined by a user and applied on one or more switches.

Mellanox NEO supports the following jobs:

- Software upgrade
- Reboot
- Provisioning
- Adding Systems
- Updating Access Credentials

Mellanox NEO users can monitor the progress of a running job, as well as the time it was created, its last update description and status.

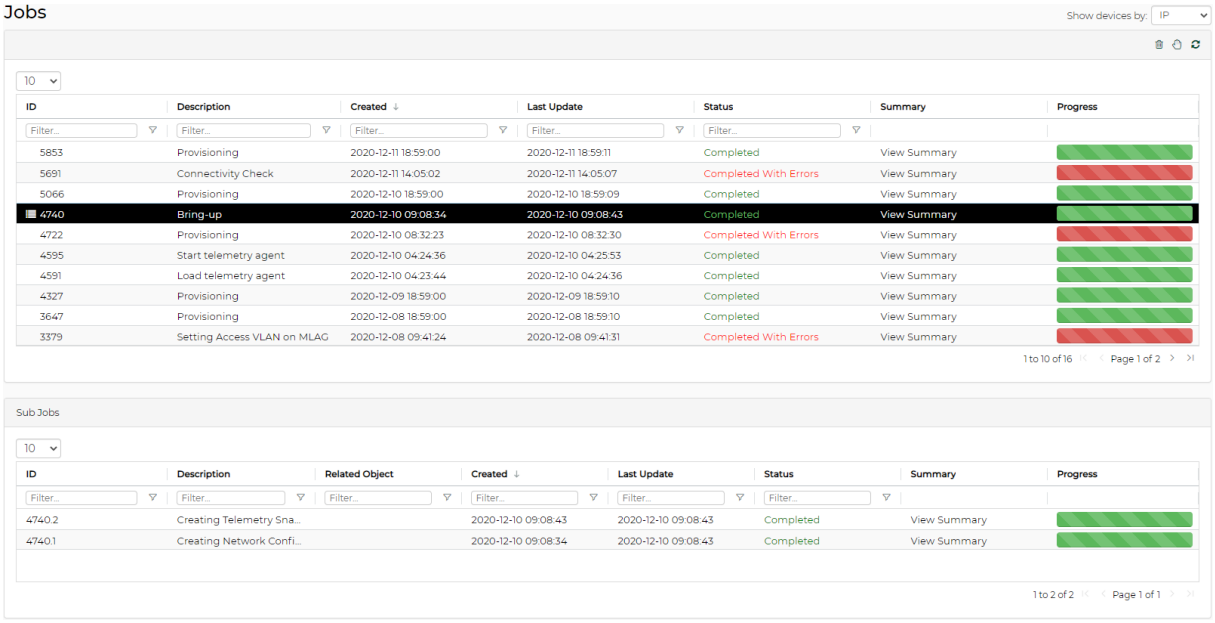
When an action (software upgrade, reboot or provisioning) is started by the user, a new job is created. The initial state of every job is “Running”. When the action is completed, the job state value can be either ‘Completed’, to indicate a successful job, or ‘Completed With Error’, if an error has occurred. In this case, the fault status will appear in red.

If during a switch action the related service (provider) goes down, all service (provider) related jobs will be aborted and the related jobs state will change to “Aborted”.

A Job can also be a task that was scheduled by the system. Mellanox NEO users can monitor the progress of these jobs as well, but cannot control them.

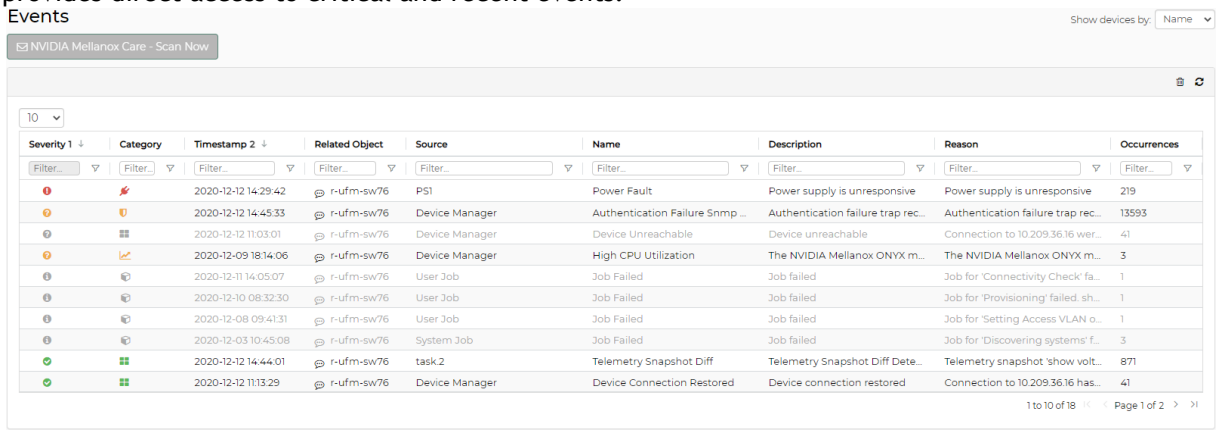
Choosing ‘View Summary’ for a certain device will display the status of running sub jobs on all IP addresses. The jobs that were completed with errors can also be filtered for by checking the “Completed with Errors” checkbox (see below). Clicking on a device IP address, will display the output of the sub-job related to it.

A detailed list with a Summary Information field is also available when choosing one device.



Events

Events information is accessible through the dashboard or through the main menu. This view provides direct access to critical and recent events.



The events infrastructure allows filtering for events by criteria and defining them based on various triggers (for example, traps and threshold crossing), upon configurable ranges and severities. A user may acknowledge one or more events by right-clicking on them. The acknowledged events will be

grayed-out. Identical events are grouped as “occurrences” when the same event takes place more than once (see last column to the right). Events can also be derived from SNMP traps sent by the switch.

Through the Events menu, the user can induce an event scanning operation by clicking the 

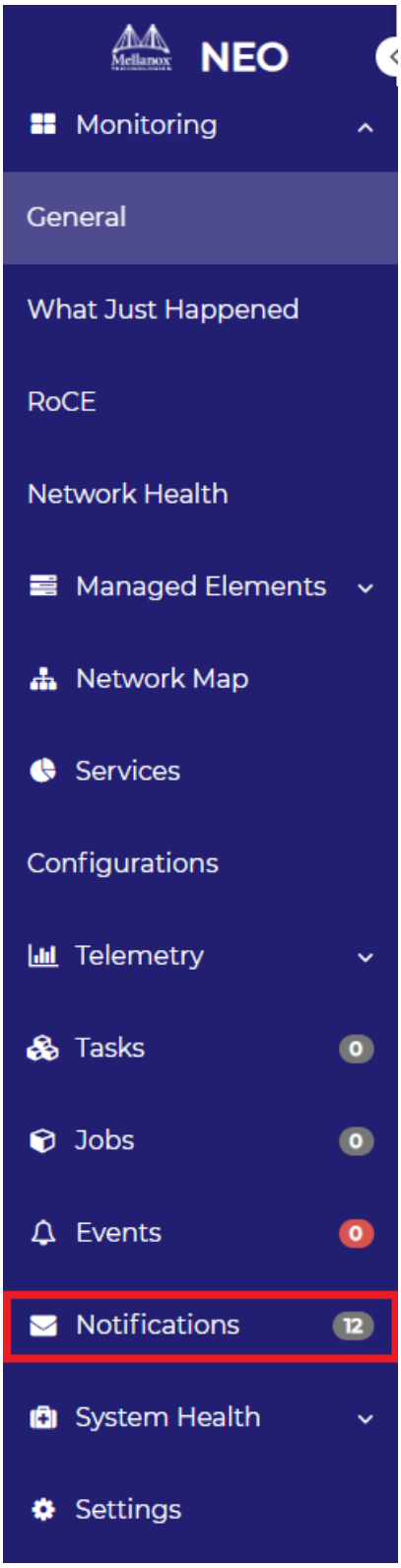
button. Consequently, Mellanox NEO sends an email with details of events to Mellanox NOC. For details on Mellanox Care, see Mellanox Care; for details on the generated email, see Events Policy Settings.

Notifications

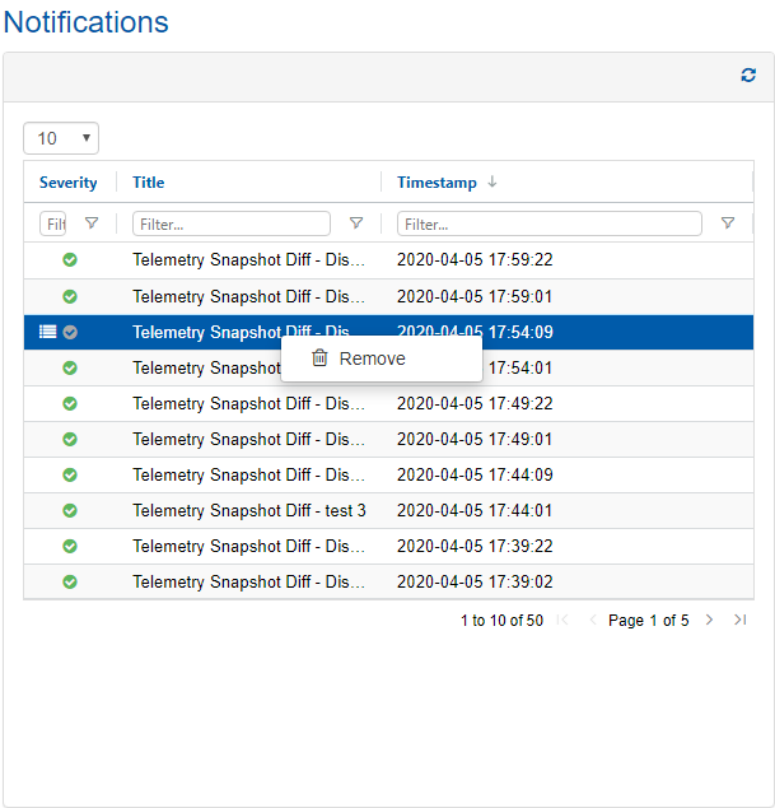
The Notifications window is Mellanox NEO’s incoming messages box, providing the administrators network notifications of several types.

By clicking a specific notification, a table with further information will appear on the right side of the screen. For each of the notifications, the table can be saved, copied or printed by the user.

Mellanox NEO scans the network for mismatches and changes once every 24 hours. The user can view the number of unread notifications at any time, as it is constantly displayed next to the small envelope icon on the top right corner of the interface’s frame.



Unread notifications will appear in a bold font until they are read for the first time. To remove notifications, right-click on the relevant notification and select “Remove”.

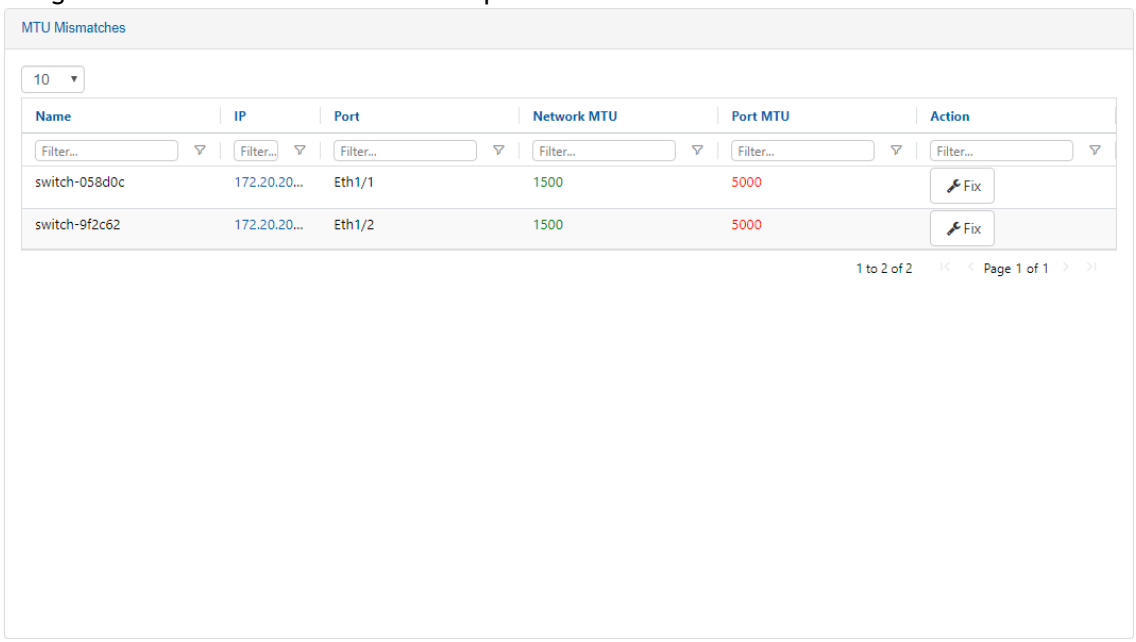


Incoming notifications appear in blue pop-up windows in the bottom right corner of the screen.

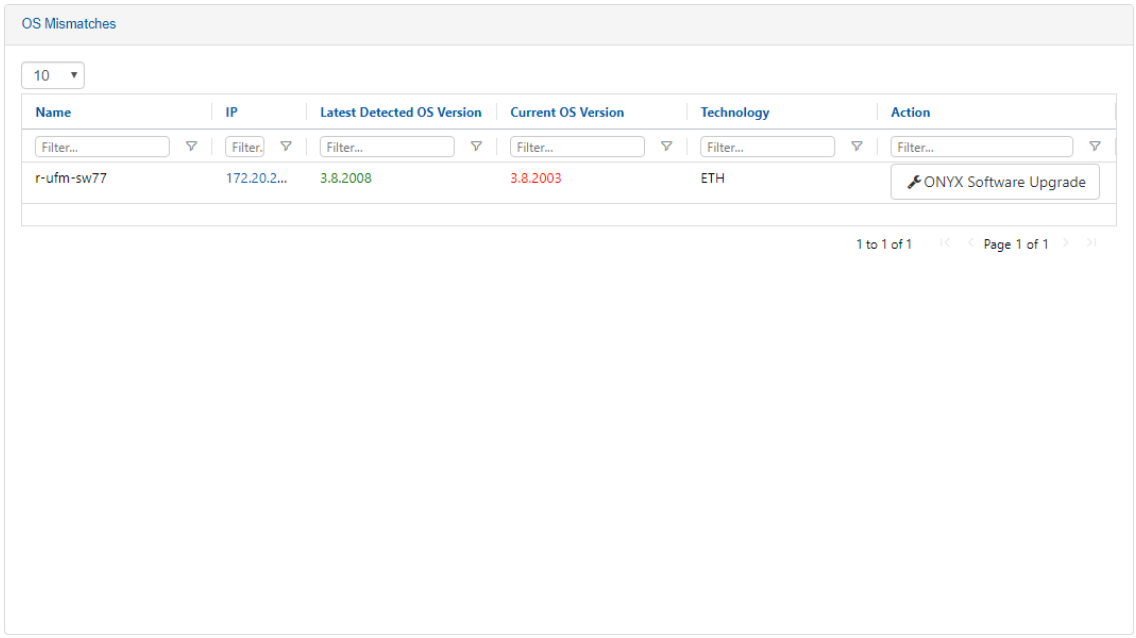
Notification Types:

- MTU Mismatches – Mellanox NEO checks the common Maximum Transmission Unit (MTU) configured in the network. The common MTU is calculated according to the MTU of the majority of the active ports that were discovered in the network. Once the common MTU is calculated, NEO will check for the ports that have different MTU than the common MTU, and

will generate a notification about these ports.

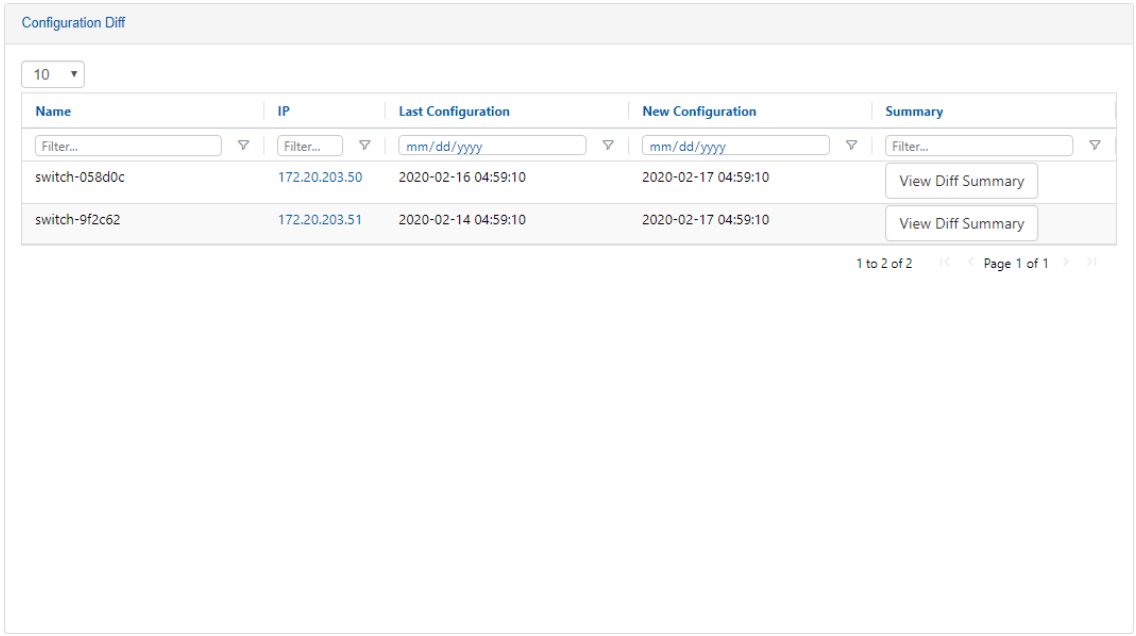


- OS Mismatches – Mellanox NEO verifies that the latest operation system (OS) version is installed on all devices in the network. A notification is generated in case a device with an older version is found.

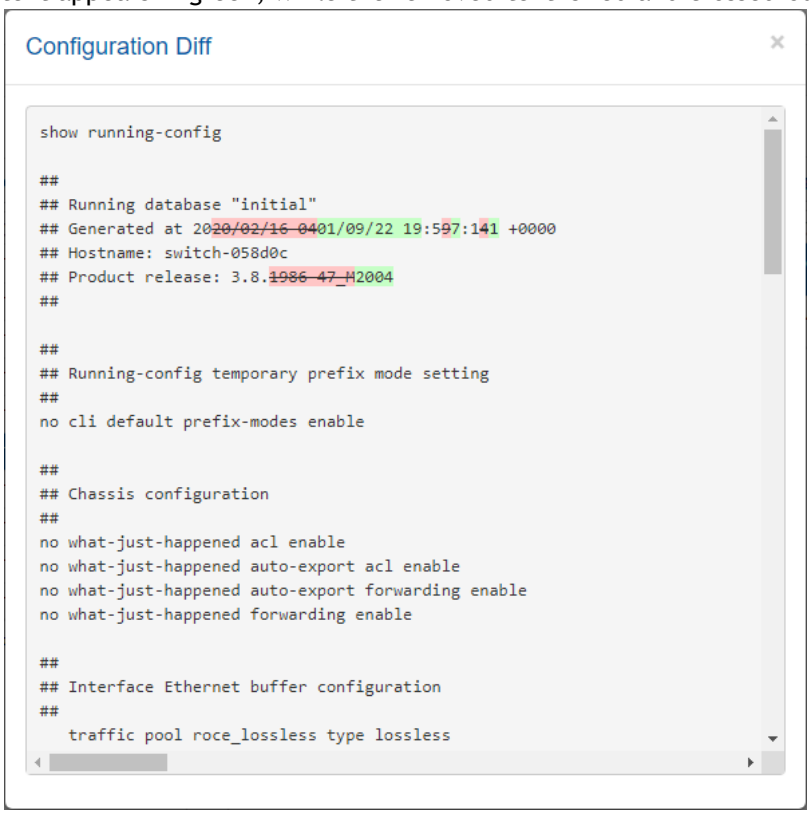


> ⚠ There are three OS types (IB, VPI and Ethernet), and therefore, three different latest versions.

- Configuration Diff – in case a configuration change has been performed on one of the switches, Mellanox NEO will generate a notification of this type.

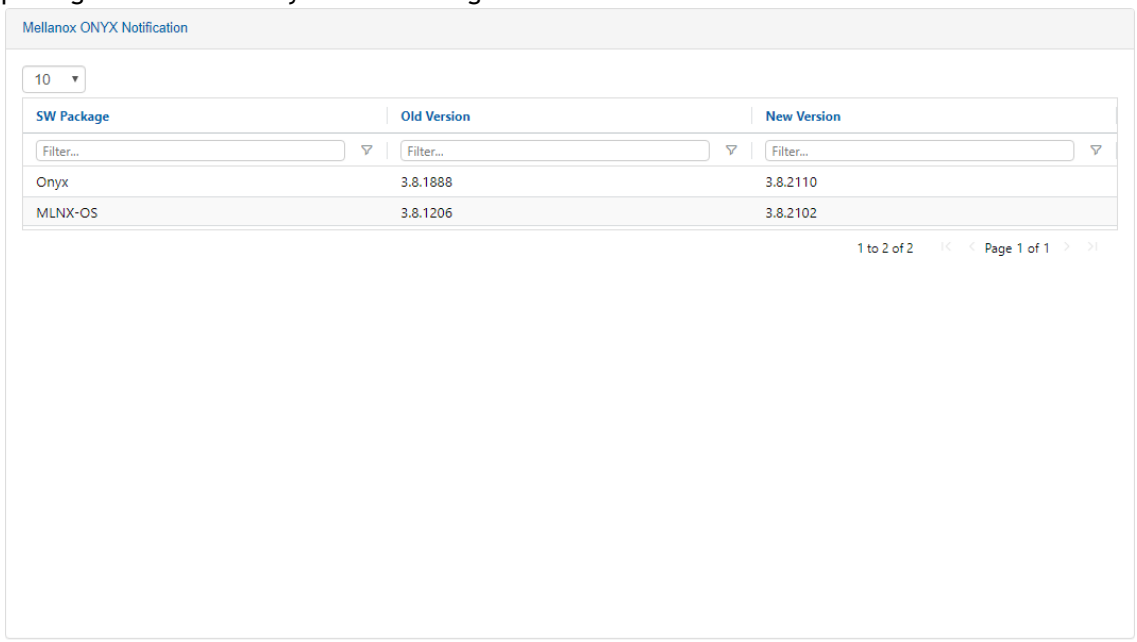


The user may also view the changed content by clicking “View Diff Summary”. The added text appears in green, while the removed text is red and crossed-out.



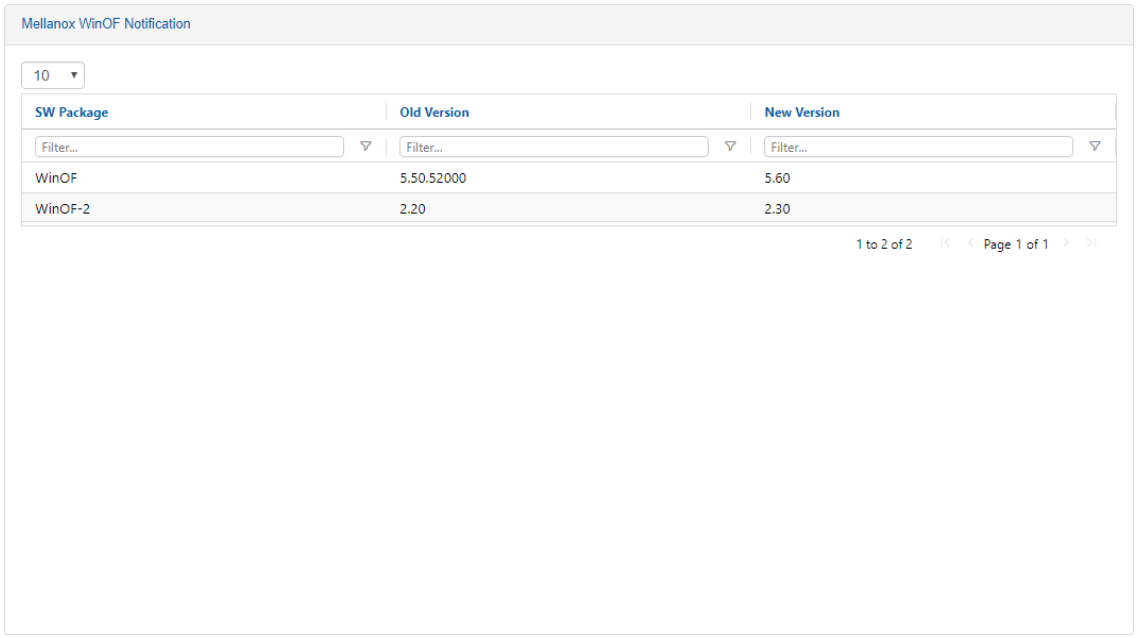
- Telemetry Snapshot Diff – If a running snapshot change has been performed on one of the switches, Mellanox NEO will generate a notification of this type:

- Mellanox Onyx Notification – Mellanox NEO checks for a new available version of any of the following MLNX Onyx packages: SX_Eth, SX_VPI, SX_IB, SIB, and Spectrum, and if it finds any, it will generate a notification. Note that you can define which MLNX Onyx package or packages to be traced by NEO in the cfg. file.

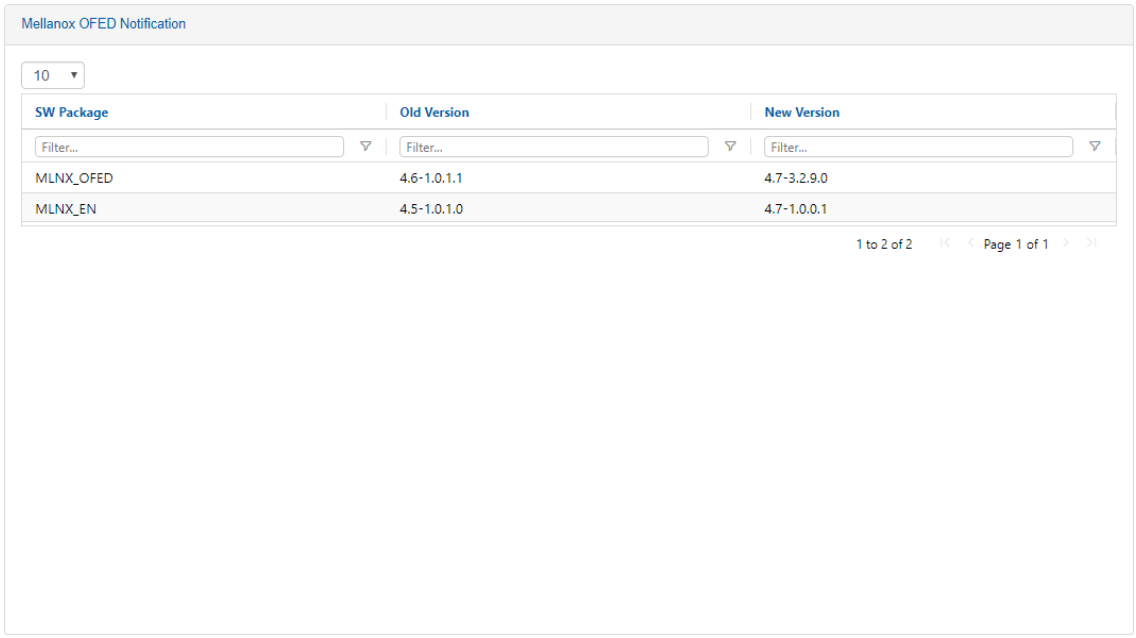


- Mellanox WinOF Notification – Mellanox NEO checks for a new available version of either of the following WinOF packages: WinOF and WinOF-2, and if it finds any, it will generate a notification. Note that you can define which WinOF package to be traced by NEO in the cfg.

file.

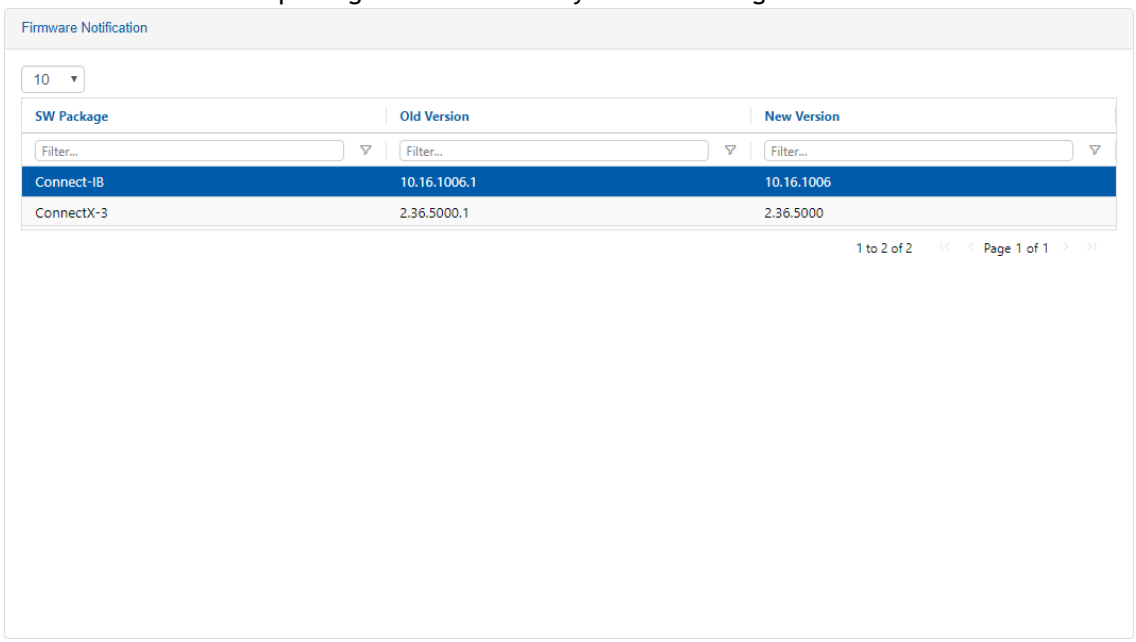


- Mellanox OFED Notification – Mellanox NEO checks for a new available version of either of the following OFED packages: MLNX_OFED and MLNX_EN, and if it finds any, it will generate a notification. Note that you can define which OFED package to be traced by NEO in the cfg. file.

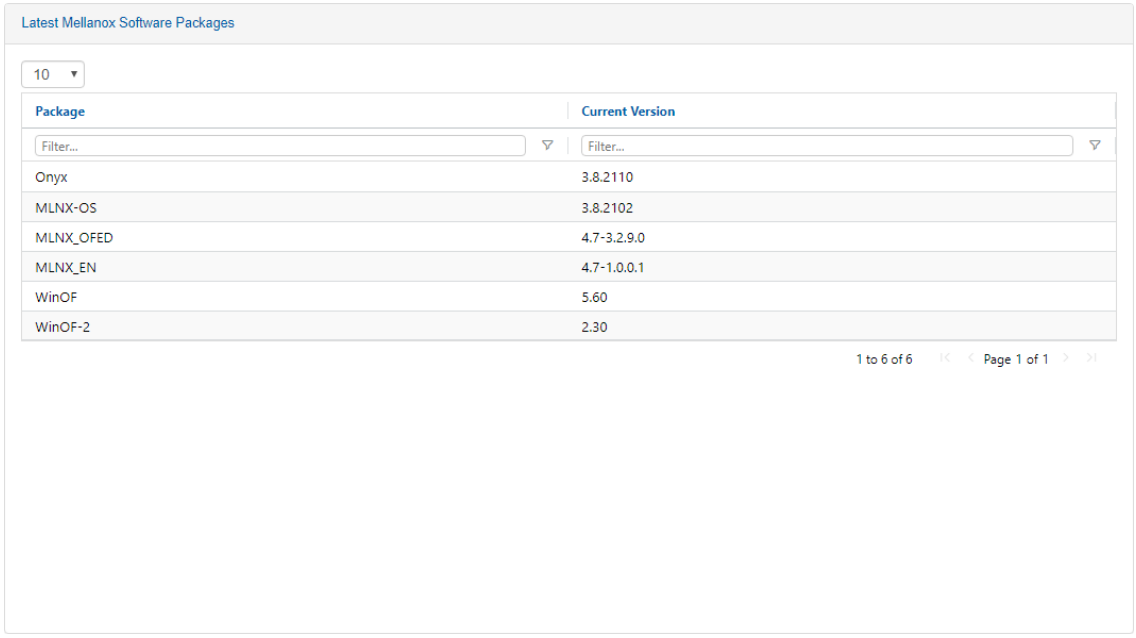


- Firmware Notification – Mellanox NEO checks for a new available version of either of the following firmware packages: ConnectX-3, ConnectX-3 Pro, ConnectX-4, Connectx-4 Lx, ConnectX-5 and Connect-IB, and if it finds any, it generates a notification. Note that you can

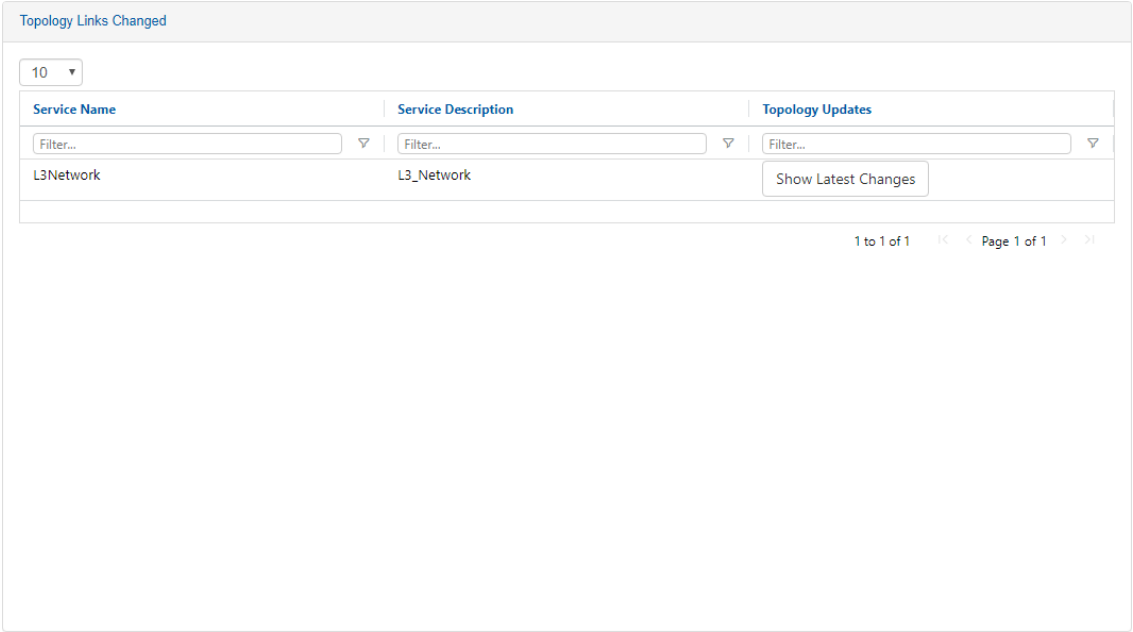
define which firmware package will be traced by NEO in the cfg. file.



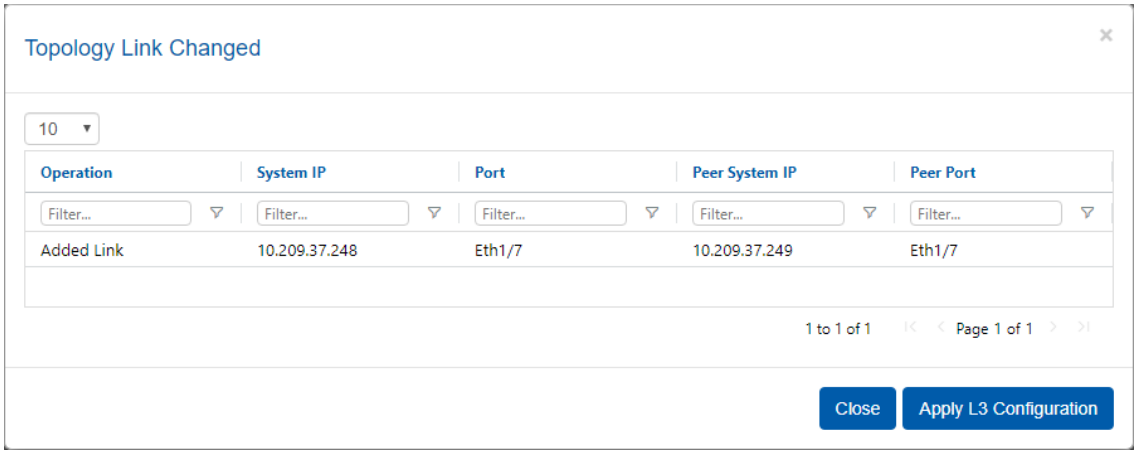
- Latest Mellanox Software Package – Once NEO is started, it checks for all of the latest packages available on [www.mellanox.com.](http://www.mellanox.com)



- Topology Links Changed – When a new device is discovered after the creation of a Layer 3 provisioning service, and if the “Add Auto-Discovered Switches” checkbox is checked and the “Auto Configure Switches When Topology Changed” checkbox is unchecked, a notification of the new discovered device will be generated.



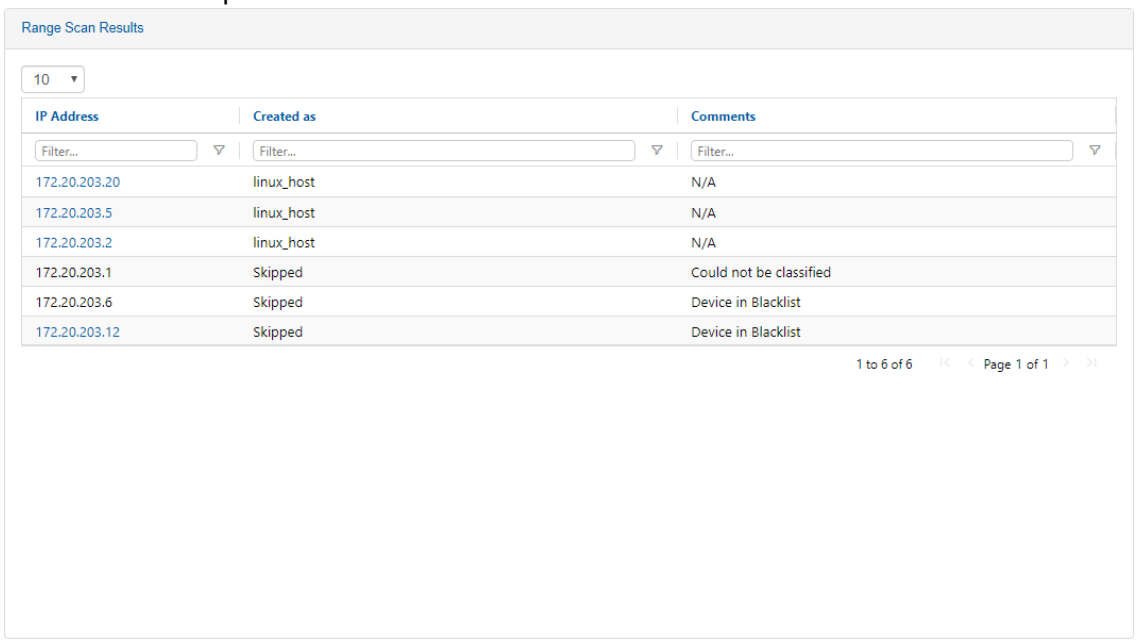
Clicking “Show Details” will display further information about the new device and the other devices it is connected to.



Since the “Auto Configure Switches When Topology Changed” checkbox was unchecked before, the configuration of the new device will not be automatic. Click the “Apply L3 Configuration” button for the new device to be added to the service and a job will be created.

- Range Scan Results – when running an IP scan through the Discovery window under Settings, NEO will list all devices it has discovered during that scan, including their type. When NEO does not succeed in identifying the device type, the type column will read “Skipped”, and

the reason will be provided under “Comments”.

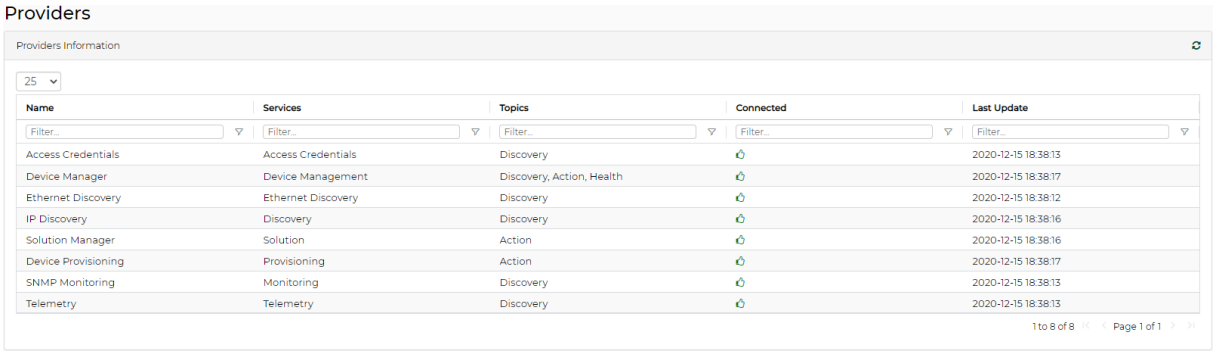


- "NEO-Host not installed” – Mellanox NEO checks if there is any host on which NEO-Host is not installed. If such hosts are found, NEO generates a "NEO-Host not installed" notification.
- More notification types:
    - lldp scan result
    - range scan result
    - multicast scan result
    - prism added devices
    - vcenter added devices

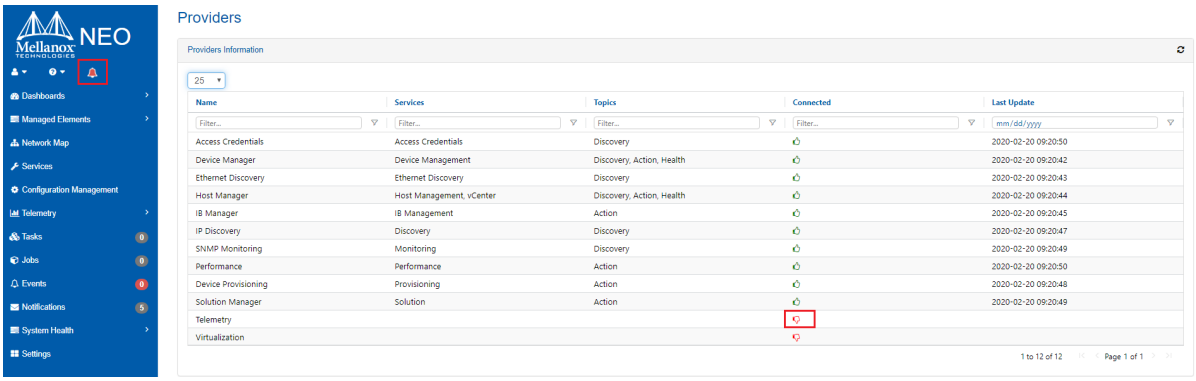
System Health

Providers

Providers are the building blocks of Mellanox NEO. Each provider runs a specific service such as Managing Device Access, Device Provisioning, and IP Discovery. Providers are controlled by a controller.



If a provider is disconnected, a small bell icon appears at the top right corner of the screen. To identify the disconnected provider, click on the “Providers” tab, and in the “Connected” column of the “Providers Information” table, look for the red “thumbs down” icon.



Device Manager

Mellanox NEO® will collect Chassis Discovery and information on Mellanox switches, such as modules, traps, temperature, ports, OS, etc. For the device manager to receive SNMP traps for all managed switches, all systems must be configured accordingly.

Device Access Manager

The Credentials Provider is responsible for managing the access credentials of all managed systems and groups (defaults).

Devices access credential can be managed via Mellanox NEO™ at three levels:

1. Global level (global groups) – relevant for all devices that use a specific protocol (http, ssh or snmp).
2. Group level – relevant for all devices which belong to a specific user-defined group.
3. Device level – relevant for a specific device for which credentials were set (once unique device access credentials are set, they overwrite global or group credentials definitions.)

The credentials provider is agnostic to the stored attributes, in order to allow support for any protocol in the future.

For more information about access credentials configuration, see “Configuring Access Credentials within Mellanox NEO™”.

Monitor Manager

- Forwards samples of all switch port counters to an internal 3rd party software: InfluxDB
- The controller will sample the counters of all the switches in the fabric at a configurable interval (default=5 minutes). The results will be displayed by InfluxDB.
- For more information, please refer to "Configuring SNMP on Mellanox Onyx Switch (for Port Counters Monitoring)"

ETH Discovery

The role of the ETH Discovery Provider is to discover the Ethernet topology type according to the LLDP protocol. In this phase, the LLDP information is collected using SNMP protocol. The controller initiates the periodic discovery process by providing a list of start-points and connection information. The provider sends the discovered data periodically, when it is containing the CIM objects and relations. The controller aggregator integrates the CIM objects and relations into the existing model and adds new devices as necessary.

For ETH discovery to work properly, the user must configure LLDP for all managed devices. For more information, see "Configuring Mellanox Onyx Switch for LLDP Discovery" and "Configuring Host for LLDP Discovery".

> For LLDP Discovery to work properly on Mellanox Onyx systems, Mellanox Onyx version 3.4.1802 is a minimum requirement.

IP Discovery

IP Discovery provider can operate in 2 optional modes:

1. Auto-Discovery – automatic discovery of devices found within a specified range of IP addresses using Mellanox UFM-Agent. In this mode, Mellanox NEO controller discovers all Mellanox Onyx switches by sending multicast messages. Every Mellanox Onyx switch responds to the controller with its IP address. This information is stored in the controller repository.

   > Mellanox NEO auto-discovery requires multicast traffic to be enabled on the managed switches.

2. Manual IP scan – manual discovery of devices of one or more types found within a specified range of IP addresses, run according to the following algorithm:

   - Checks for connectivity with a ping
   - If alive, NEO scans all devices and classifies them according to their type, using the following protocols in order:
     i. SNMP classification (SNMP v2, SNMP v3 using global credentials)
     ii. SSH connectivity with Linux credentials
     iii. WinRM with Windows classification

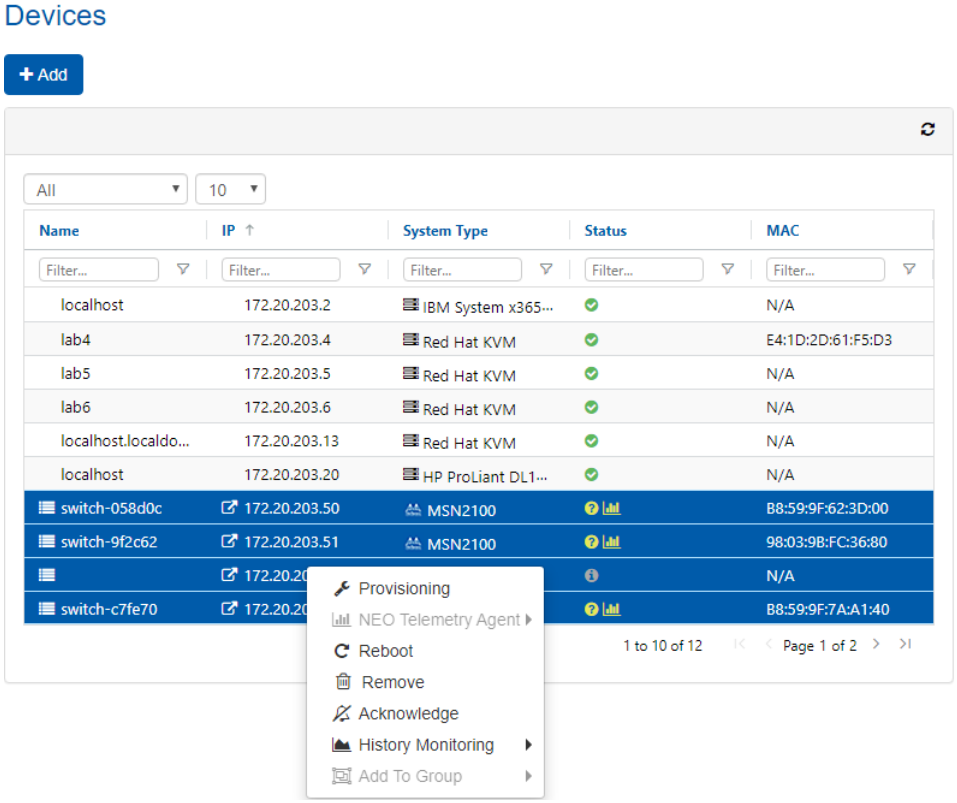
> When IP Discovery is loading, it reports the list of configured IP addresses to the controller. The controller stores this information in its repository.

Device Provisioning

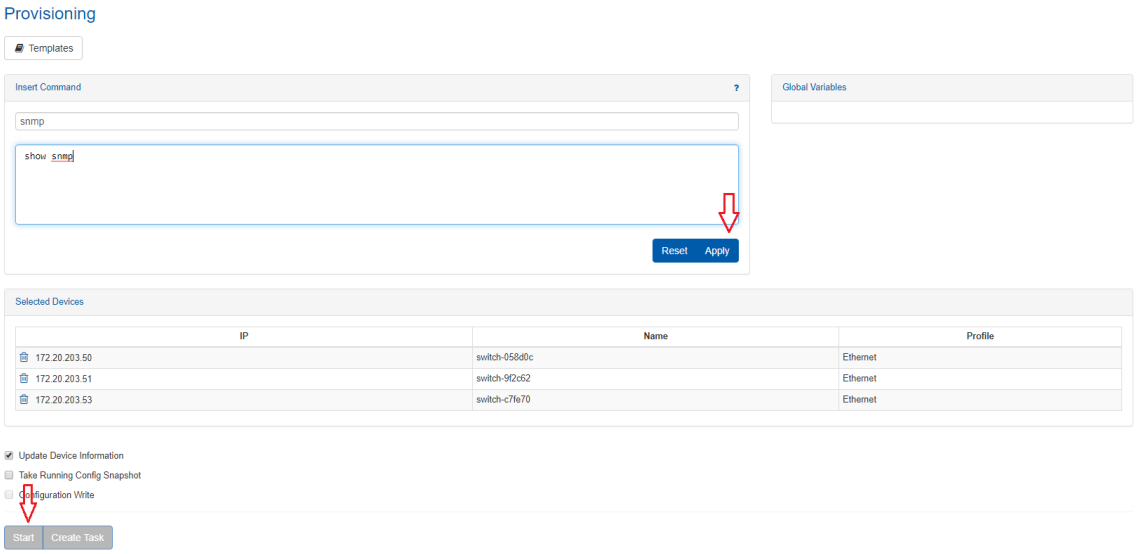
The Device Provisioning function allows the users to play a list of switch CLI commands on a list of Mellanox switches.

To run a command or a series of commands on one device or more:

1. Right-click on the desired devices, and select “Provisioning".



2. In the dialog window, type the switch CLI commands that you wish to run on the selected devices, click the “Apply” button, and then “Start”.



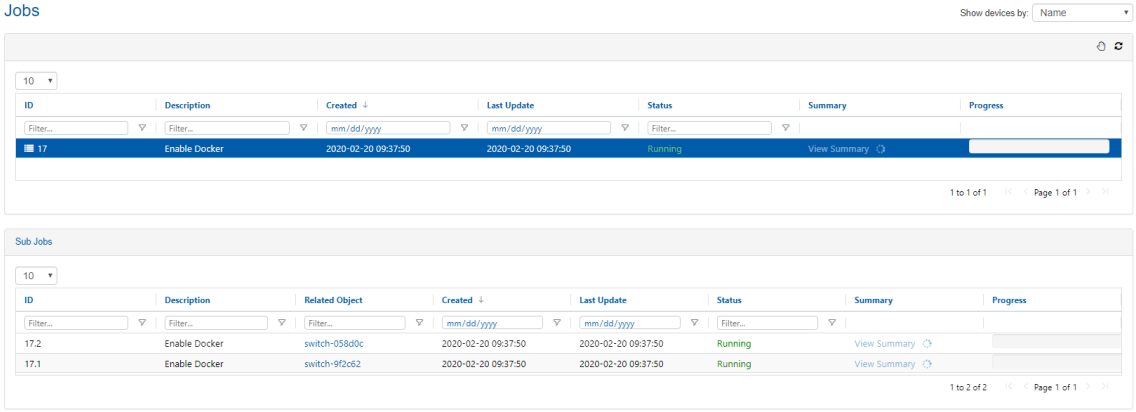
Notes:

- Your category selection will determine the template’s availability according to the chosen device protocol type: a template categorized as “General” will be available for all managed devices, a template categorized as “InfiniBand” will be available for

Infiniband devices only, and a template categorized as “Ethernet” will be available for Ether- net devices only.

- New CLI templates can also be uploaded manually to the Mellanox NEO™ templates folder (/opt/neo/controller/templates).
- Built-in Linux Cumulus templates are also available
- To edit the command or create a new one, refer to "Events Policy Settings".

3. Once the commands are initiated, Jobs and Sub-Jobs will be opened accordingly. To view the commands’ outputs, click on the “View Summary” button.



Configuring Access Credentials within Mellanox NEO

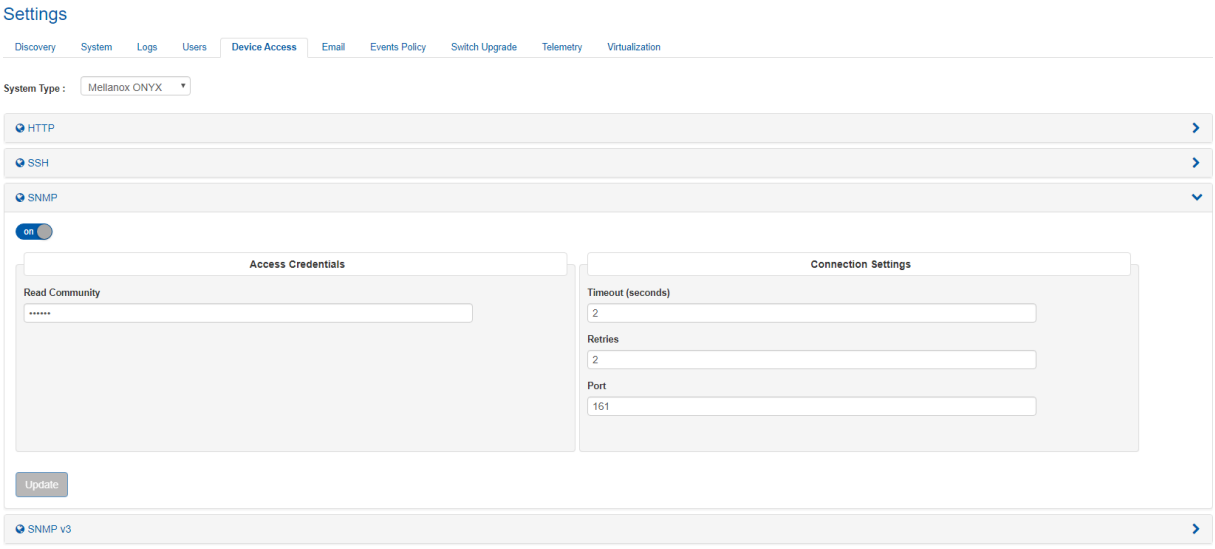
Using Mellanox NEO GUI

The default global access credentials are detailed in the following table. They can be changed through the “Settings” tab by selecting the “Device Access” view and filling-in the desired credentials for the relevant protocol.

Access Credentials

HTTP	SSH	SNMP	SNMP V2	SNMP V3	SNMP TRAP
Username: admin Password: Admin Secured (HTTPS): true Timeout: 60s Port: 443	Username: admin Password: Admin Timeout: 60s Port: 22	Read Communit y: pub- lic	Port: 161 Timeout: 2 [s] Retries: 2		Port: 162 Interface: eth0 Protocol: v2 Community: public
			---	Private authentication protocol password: adminauth123 Privacy protocol password: adminpriv123	

By default NEO will scan systems via snmpV2c protocol. In order to override specific device protocol setting definitions (for example, changing specific protocol type/protocol port/ timeout/number of retries for a specific system), contact Mellanox Support.



Under HTTP settings, you can select between HTTP and HTTPS, by checking/unchecking the "SSL Secured Connection (HTTPS)" toggle button.

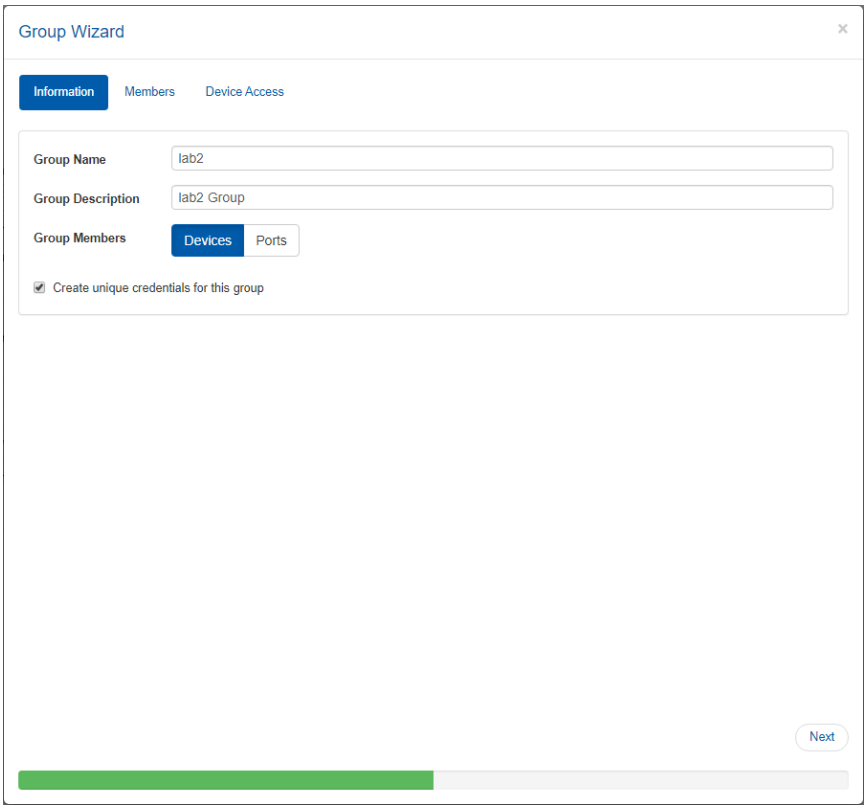
The Protocols section is only shown when the protocols are relevant to the system type. This applies to Global Settings and Unique Device Access.

It is possible to overwrite the defined credentials for a specific group or a specific system in the fabric:

Unique Group Access Credentials

This option can be enabled when creating a new group by checking the “Create Unique Credentials for this Group” checkbox. Once the group is created, its access credentials changeability mode cannot be altered. In case the checkbox is checked, devices for which unique access credentials are defined, will not appear as available for association with this group.

A device cannot be associated with more than one group that allows creating unique access credentials.

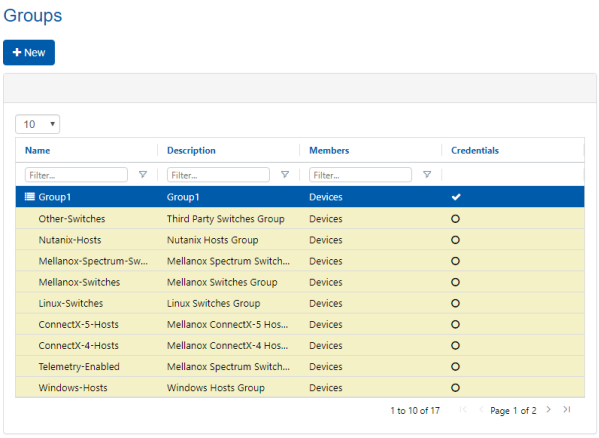


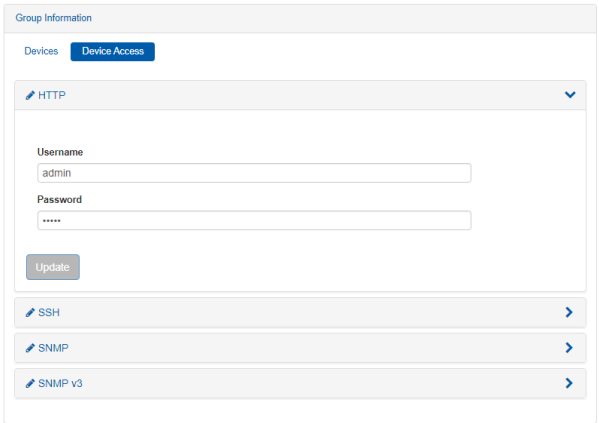
In order to change the access credentials for a specific group, select the desired group, click the “Device Access” tab and edit the credentials for the relevant protocol.

Unique Device Access Credentials

In order to change the access credentials for a specific device, click on the “Devices” sub-menu, select the “Credentials” tab and edit the credentials for the relevant protocol.

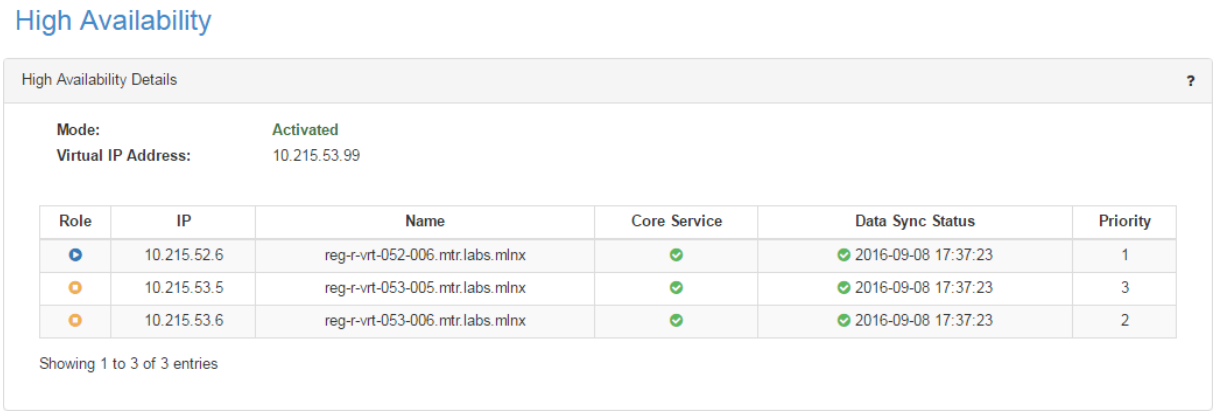
> ⚠ In case the selected device is associated with a group for which unique group access credentials are defined, the unique credentials defined for the group will be overwritten by the unique device credentials, for the specific device.





High Availability

This window is meant to grant more stability to the system. NEO can be installed on three nodes so that if the main node (known as the “active” node) fails, another node which has all NEO persistence data saved will take over, and the system will remain functioning properly. The three nodes form a cluster and will constantly be synchronized. While the main node is the active node, the other two will be in a “standby” mode, set in an order from 2-3, according to priority. The standby node can take over the active node in case of a failover due to an error.



The virtual IP address that appears on top of the table in the figure above is the gateway for the NEO UI in all nodes/physical IP addresses listed in the table.

- Each node is identified by its IP address and name.
- “Priority” column enumerates the nodes according to their priority:
  1- the active node
  2- the first node to take over the active node in case of a fail-over
  3- the second node to take over the active node in case of a fail-over
- The colored icons under the “Role” column indicate the node status:
  Blue - active
  Orange - stand-by
- “Core Service” column indicates the health status of the nodes:
  Green - OK
  Red - Failure
- “Data Sync Status” column indicates the time at which the nodes were last updated/ synchronized. This status is configured to update every several minutes.
- A right-click on the active node will enable performing a manual fail-over on it. After confirming the action, it might take up to a minute for the stand-by to automatically take over. You might also have to restart the GUI.
- A right-click on any of the stand-by nodes will enable performing a manual take-over.

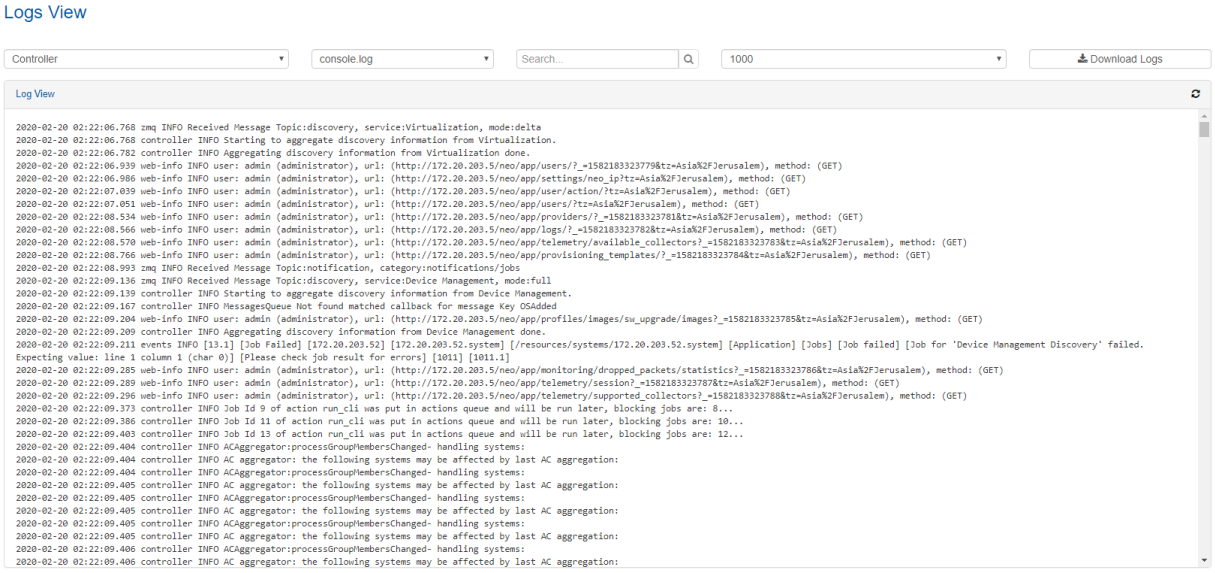
After confirming the action, it might take up to a minute for the active node to be disabled and the stand-by node to take over.

For HA installation and configuration, please refer to section "Installing NEO for High Availability".

Logs

Logs View

The Logs window provides a summary of all activities performed by Mellanox NEO in a list that can be filtered for NEO providers, log types and the number of the last lines.



By clicking “Download Logs”, all logs for all NEO providers and log types will be saved in one tar.gz file that can be downloaded.

Log Types

- console.log – contains the union of related component (controller or provider) logs
- controller.log – contains logging information for Mellanox NEO’s central controller component
- events.log – contains logging information regarding events of a related component
- jobs.log – contains logging information regarding related component jobs (currently running actions)
- repository.log - contains logging information on related component repository changes
- zmq.log – contains logging information on related component ZMQ communication
- rest.log - contains logging information on rest calls for a related component
- web-info.log – contains logging information on web access of a controller
- monitors.log – contains logging information on InfluxDB accessing via controller monitoring API

  > ⚠ InfluxDB is a Scalable Realtime Graphing open source tool (http://InfluxDB.wikidot.com/start) licensed by Creative Commons Attribution-ShareAlike 3.0 License.

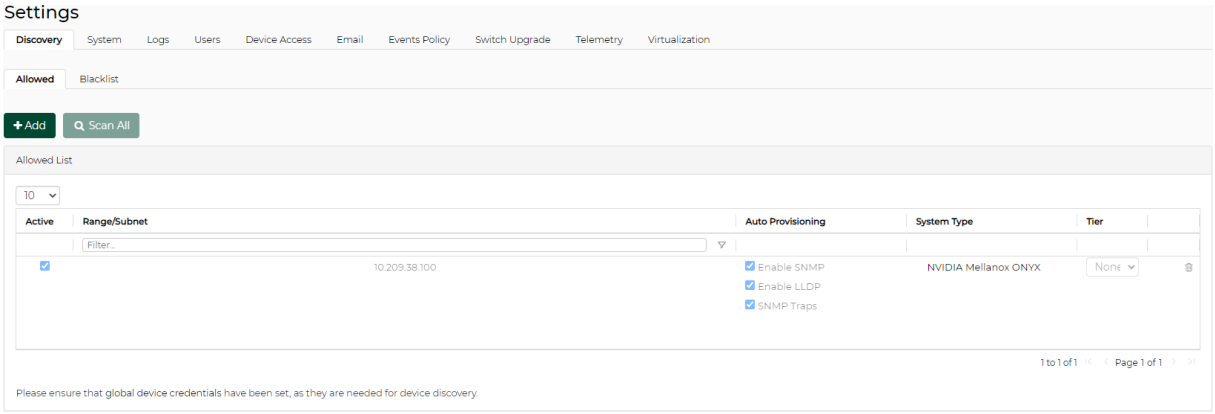
- web-access.log – contains logging information on web access of a specific internal service

Log files are located in the file system, according to the specific component (Controller or Provider):

- Controller logs are located at: /opt/neo/controller/log
- Access Credentials Provider logs are located at: /opt/neo/providers/ac/log
- IP Discovery Provider logs located at: /opt/neo/providers/discovery/log
- Device Manager Provider logs located at: /opt/neo/providers/dm/log
- Monitoring Provider logs located at: /opt/neo/providers/monitor/log
- Provisioning Provider logs located at: /opt/neo/providers/provisioning/log
- ETH Discovery Provider logs located at: eth discovery log /opt/neo/providers/ethdisc/ log/
- Solution Manager logs located at: /opt/neo/providers/solution/log/
- IB Manager logs located at: /opt/neo/providers/ib/log/

Settings

This section describes the different Settings tabs.



Discovery

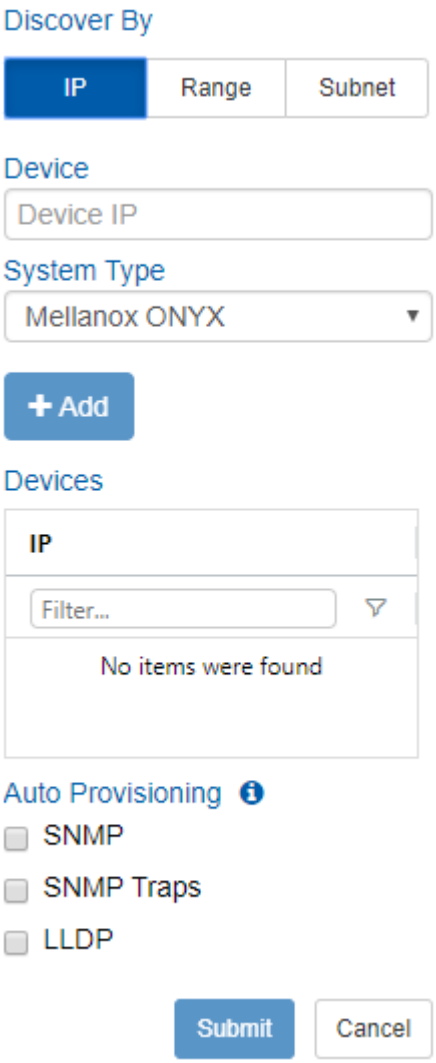
NEO supports two methods of device discovery:

- Auto-Discovery – periodic automatic discovery of devices
- IP Scan – manual discovery of devices

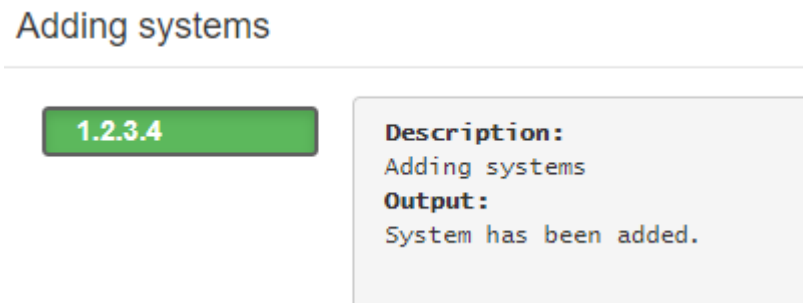
When running NEO for the first time, devices are not automatically discovered, unless the following discovery buttons are used:

- Agent Discovery button – when turned on, NEO enables automatic discovery of Mellanox Onyx switches. For further information, refer to “Auto-Discovery” method under “IP Discovery” in Providers.
- LLDP Discovery button – when turned on, NEO enables automatic discovery of switches and hosts on which LLDP is enabled. For further information, refer to “ETH Discovery” under Providers.
- 

button – using this option, users are able to add a device either by manually typing its IP address, or by scanning a range or a subnet of IP addresses:

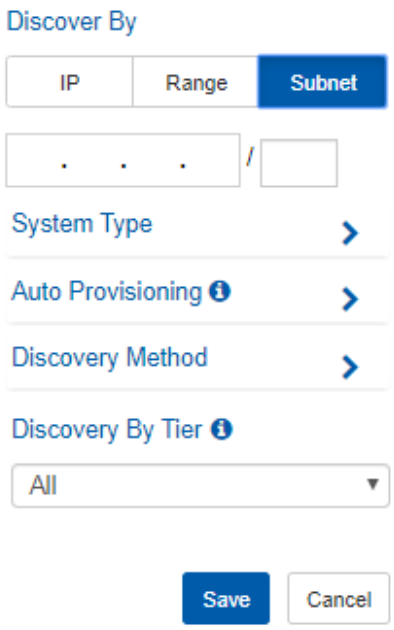


- Discover by IP: Insert the Device IP address, select its type, and click the "+Add" button to add the device. Repeat the action for all devices you wish to add. Once all devices are added, click "Submit".
  A window with the devices that have been added will be displayed. Clicking one of the devices will show the system status.

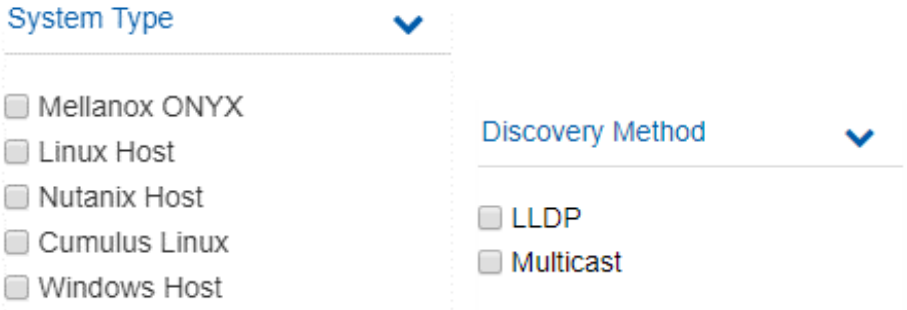


> ⚠ Each newly added device under this window will automatically appear in the "Allowed" list under Settings → Discovery, in a grayed-out row.

- Discover by Range/Subnet:



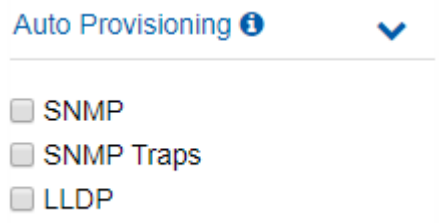
Insert the IP range or subnet address to scan for devices, and select the device types to discover, and the discovery methods to use:



- LLDP – when checked, NEO discovers all devices found within the range specified and on which LLDP is enabled
- Multicast – when checked, NEO discovers all Mellanox Onyx switches found within the range specified using multicast

You can optionally specify a tier for the devices discovered by the scan. The tier is used to present the network map in a hierarchical structure.

- Auto-provisioning – users may define some provisioning actions that run automatically on all the added devices:

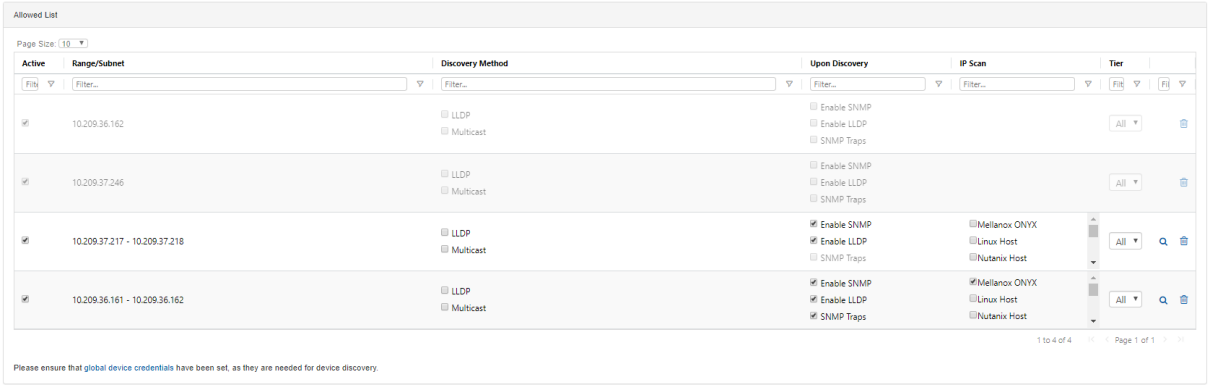


- SNMP – configure the device to listen and respond to SNMP requests (SNMP version 2c). Supported for Cumulus switches.

- SNMP Traps – configure device to send SNMP traps to NEO. The SNMP trap version (2c/3) is decided by the Onyx global SNMP credentials used. Supported for Onyx switches.
- LLDP – configure device to enable LLDP protocol. Supported for Onyx and Cumulus switches.

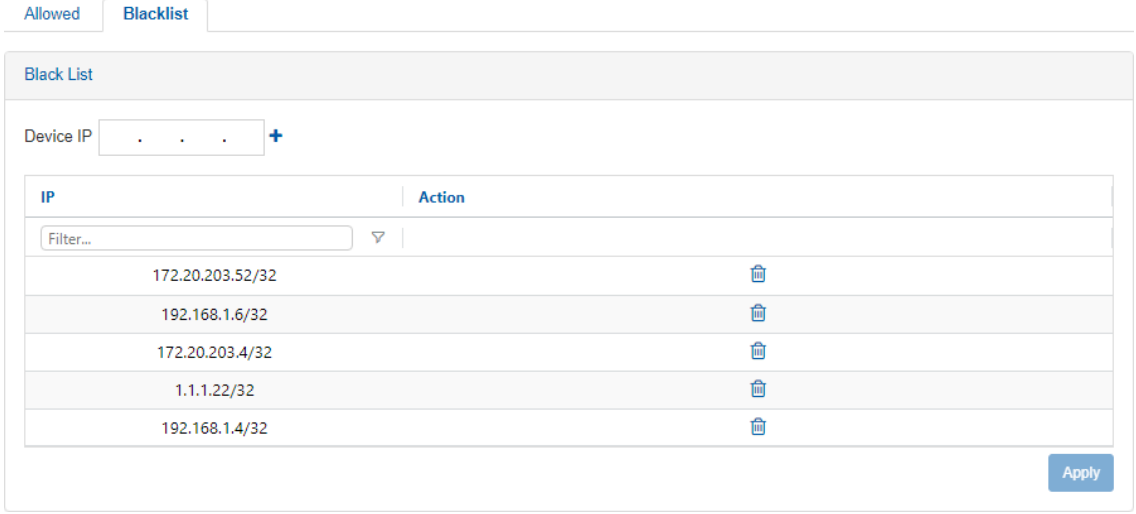
> ⚠ If a device is not applicable for a certain auto-provisioning task, NEO will skip this device.

Once a discovery operation is created, it will be added to the “Allowed” list, where all checkboxes/ fields can be edited:



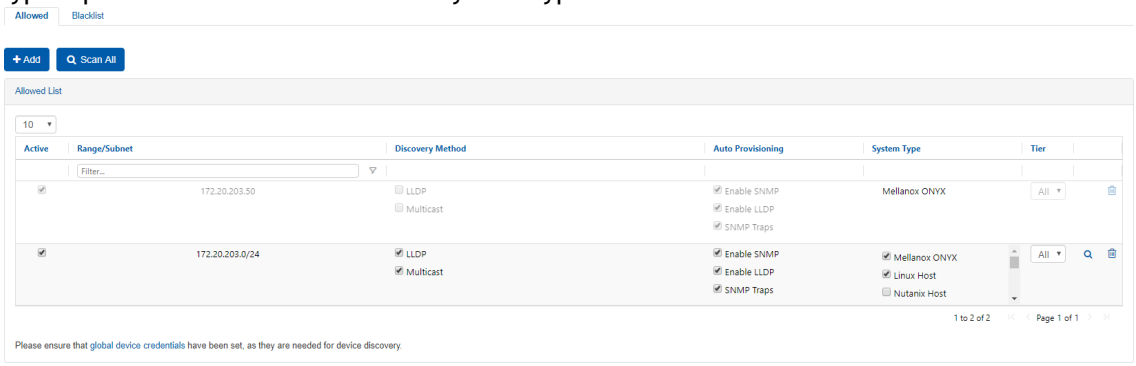
Notes:

- When removing a row using the icon, devices that were discovered in the range specified in that row will be removed from NEO
- When adding a device through the Devices window under Managed Elements, it will be added to the same list, without the option to edit the relevant row. When removing the device from NEO, the row will be removed from the list.
- When removing a device from NEO, it will automatically be blacklisted under the Blacklist tab. These devices can be removed from it by clicking the icon.



Devices can be added to the blacklist manually by inserting the device’s IP under the Blacklist tab.

“Scan All” option can be used when wishing to discover devices that belong to all device types specified in the in the “Select System Type” field.



System

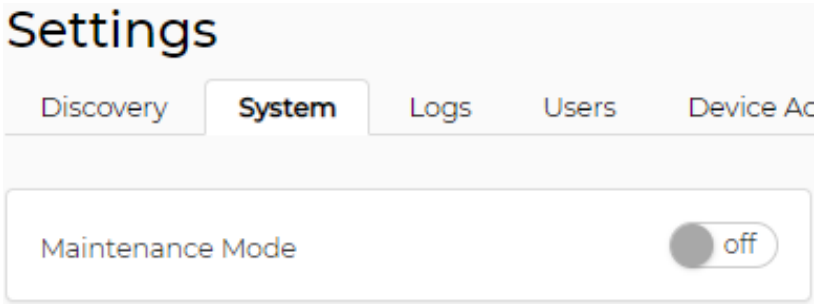
Maintenance Mode

When turned on, this mode prevents the system from creating events.

Modifying Management IP Address

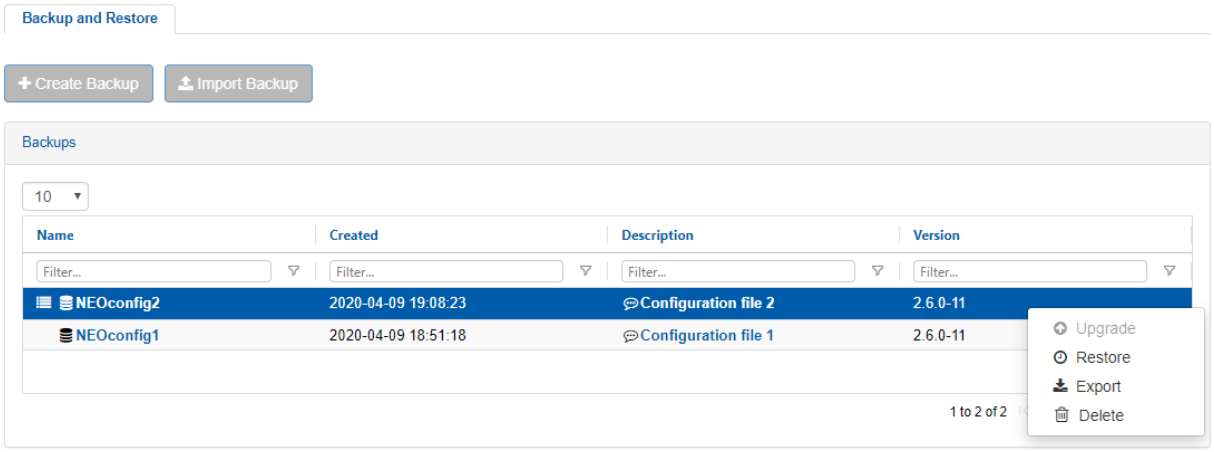
It is possible to edit the management IP of Mellanox NEO. The management IP address is used for the purposes of the telemetry agent, configuring SNMP traps, and multicast discovery.

> ⚠ The management IP configuration is updated dynamically if not configured by the user and if the user has one management IP address or DNS resolve available.



Backup and Restore

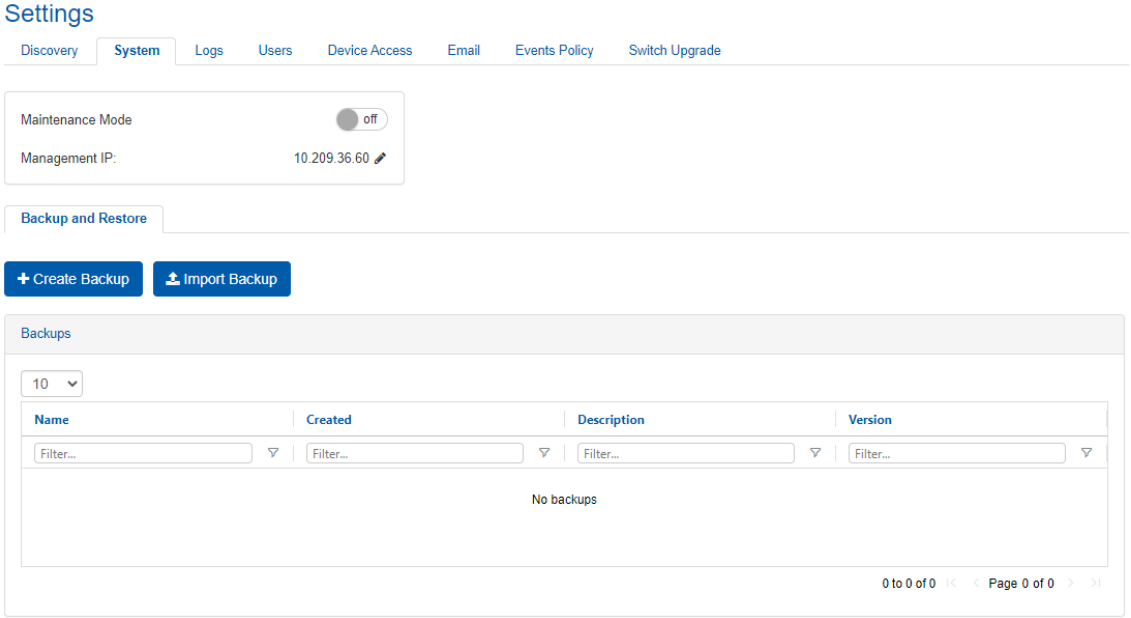
The user can create backups of NEO and restore them:



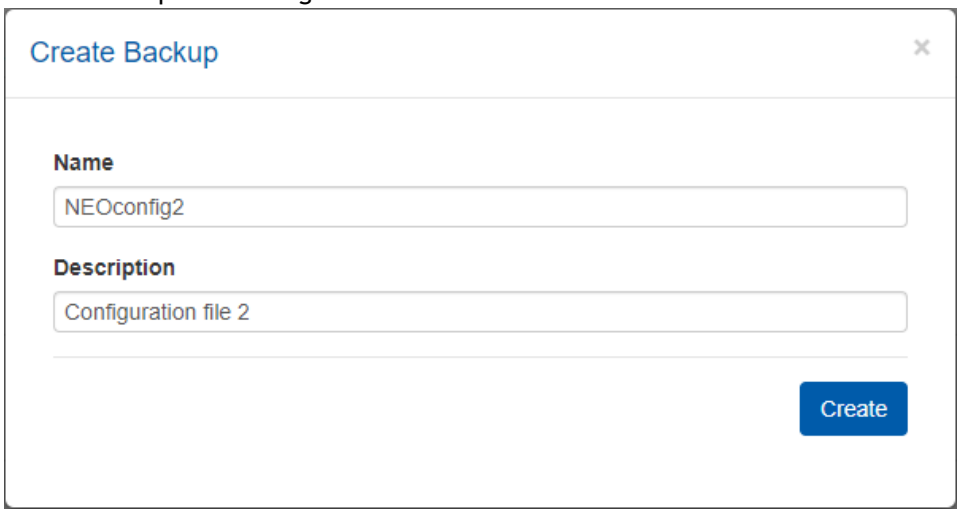
- Under Backup and Restore, the following actions can be performed:
  - Create a new NEO backup. This will create a backup of NEO's settings and discovery data.
  - Import Backup. The user can import a backup that already exists.
  - Backups table context menu:
  - Upgrade: upgrades an old backup file to work with the current NEO.
  - Restore: restores and applies the selected backup to NEO.
  - Export: exports selected backup as a tar file.
  - Delete: deletes the selected file.
- Change a backup name or description after creating it.

How to create NEO backups and restore them:

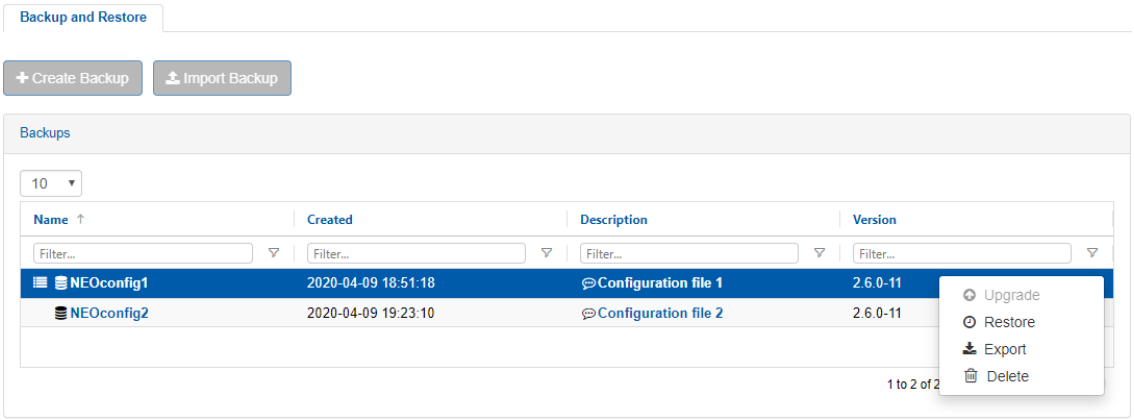
1. In NEO GUI go to the Settings tab → System tab → Backup and Restore.



2. Create backup "NEOconfig2".



3. In order to move the backup to another machine/NEO in the fabric, you need to export the backup file to a Windows folder.

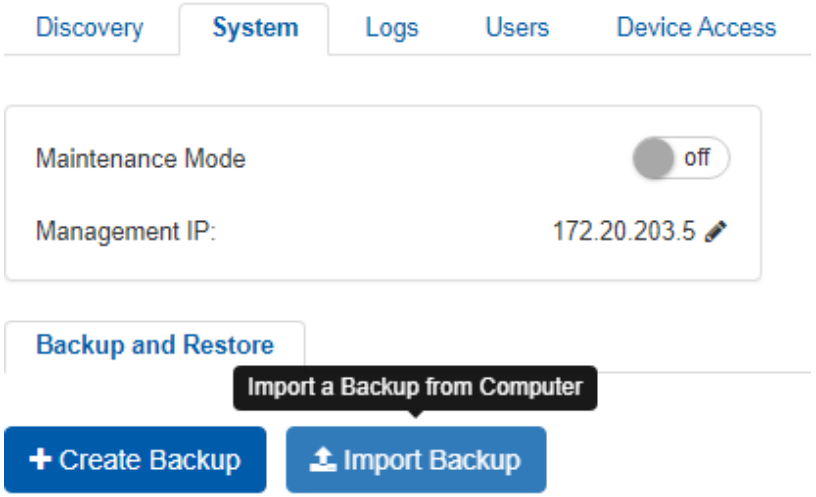


> ⚠ When 2 backup images are created, the "Create Backup" and "Import Backup" buttons are grayed out.

This creates the tgz file "NEOconfig1.tar.gz".

> ⚠ When using export, NEO saves the file on the NEO client (not on the server).

4. In order to restore the NEO backup, import the tgz file using the GUI.



> ⚠ When using import NEO searches for the file on the NEO client (not on the server).

> ⚠ Restoring a switch configured with NEO Agent to a snapshot without the agent, results with a switch with the Agent installed.

Saving Files on Remote Storage

NEO is able to save data files in a remote shared location. The following directories will be redirect to the shared location:

- Data (for backup, built-in tasks configuration tool, groups notifications, reports, smtp, telemetry)
- Logs
- Templates

Activate:

To activate this feature, perform the following steps:

1. Stop NEO.
2. Mount a local drive to a remote shared location.
3. Edit:

```
/opt/neo/controller/conf/controller.cfg
```

From:

```
[Controller]
share_location=LOCAL
```

to:

```
share_location=/new_location
```

4. Restart NEO.

Result:

If the shared location is empty, an initial copy of the shared location data will be saved to /new_location/neo.

All links to data, logs and templates will point to the relevant shared location. In case of HA file replication, stopping and activating the node will update the shared location.

Upgrade:

In case of upgrade, NEO will update the shared location data, so you will be able to continue working with it.

Disable:

To disable this feature, perform the following:

1. Stop Mellanox NEO.
2. Edit:

   ```
   /opt/neo/controller/conf/controller.cfg
   ```

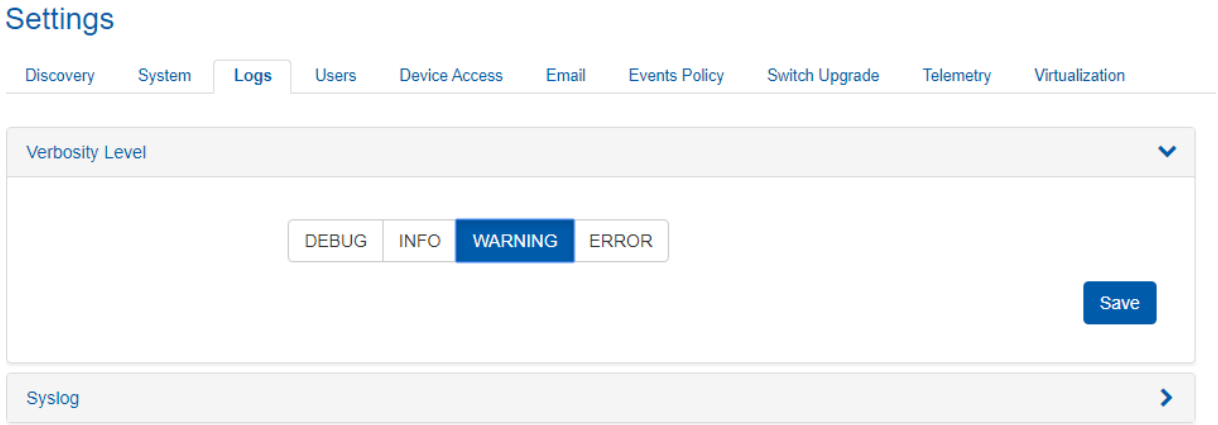
   to:

   ```
   [Controller]
   share_location=LOCAL
   ```
3. Restart NEO.

Logs

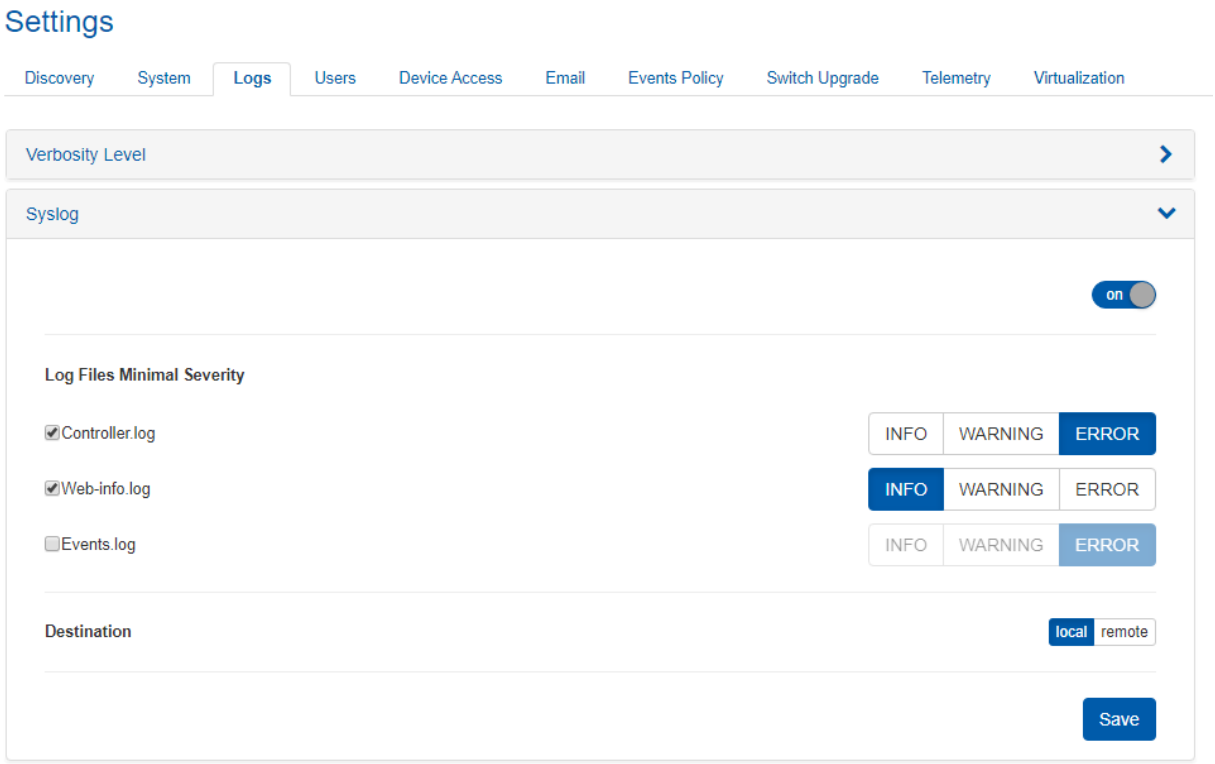
In order to configure the type of logs saved in the logging server, go to “Verbosity Level”, and select the required type: DEBUG/INFO/WARNING/ERROR.

> The verbosity level set in this menu applies only to the controller console log.



To send the log files to the local machine, check the desired log files (controller/web/events.log) with their severity from the radio buttons (INFO/WARNING/ERROR), and click “Save”.

Local Mode

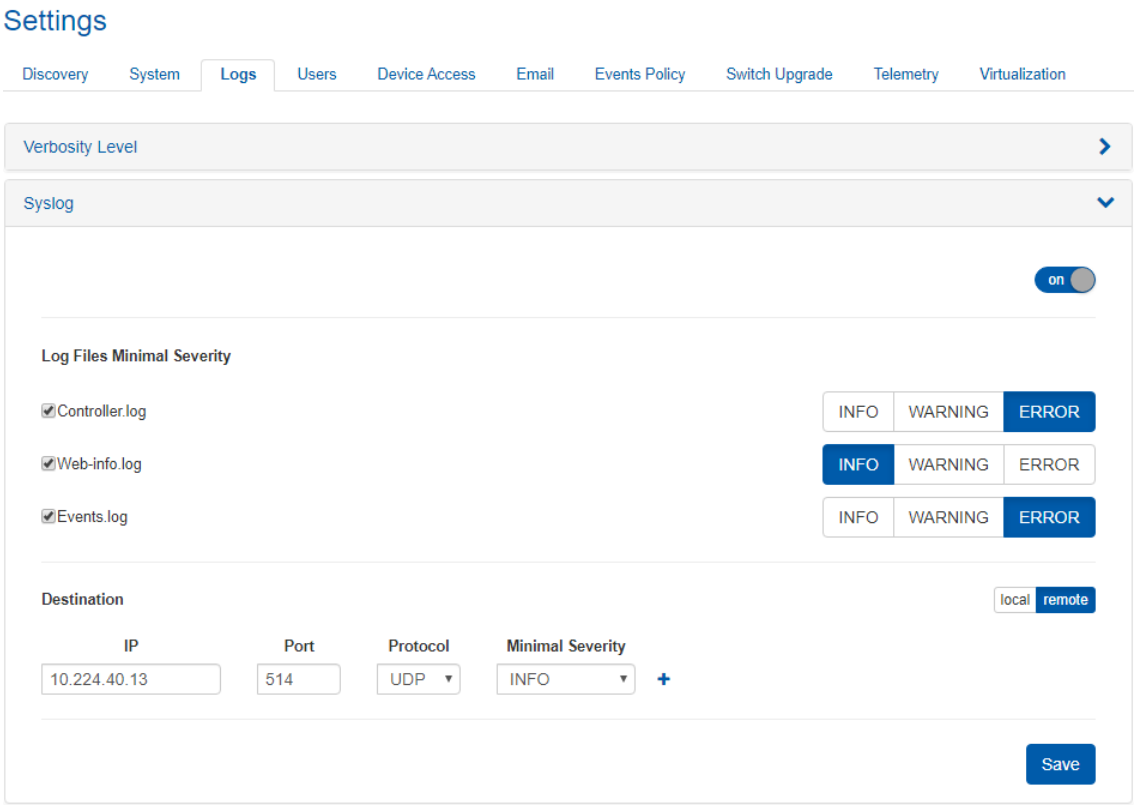


To send the log files to one or more remote machines (you may add as many as 5 destination machines using the icon), provide the destination/s IP address, port number, minimal severity and protocol (UDP/TCP), check the desired log files (controller/web/events.log) with their severity from the radio buttons (INFO/WARNING/ERROR), and click “Save”.

⚠ Please note that the only log files that can be send to the syslog are the following NEO controller files:

- Controller.log
- Web-info.log
- Events.log

Remote Mode



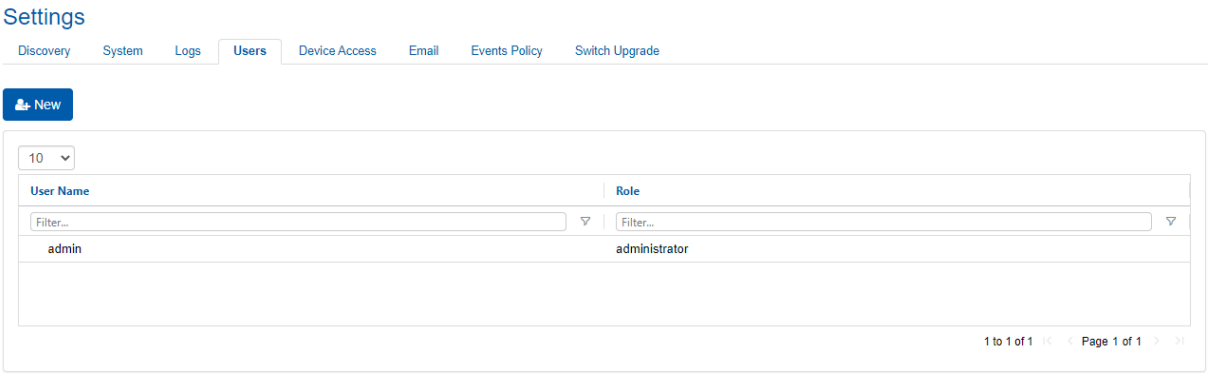
Users

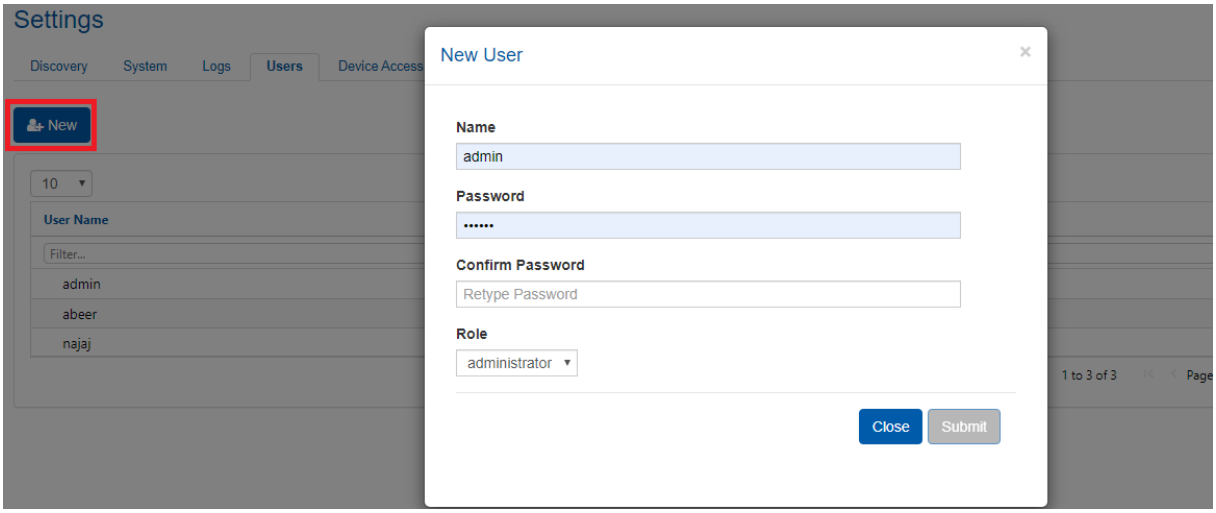
The “Users” view lists the system’s users and their roles, and allows adding new users. Administrators can also remove users from the list, upgrade users’ level to administrators and downgrade administrators’ level to users. The “admin” administrator is the only user that cannot be removed or downgraded.

Unlike administrators, standard users cannot:

- Change credentials
- Access the “Notifications” tab
- Access the “Logs” tab
- Access the “Providers” tab
- Access the “Tools” tab

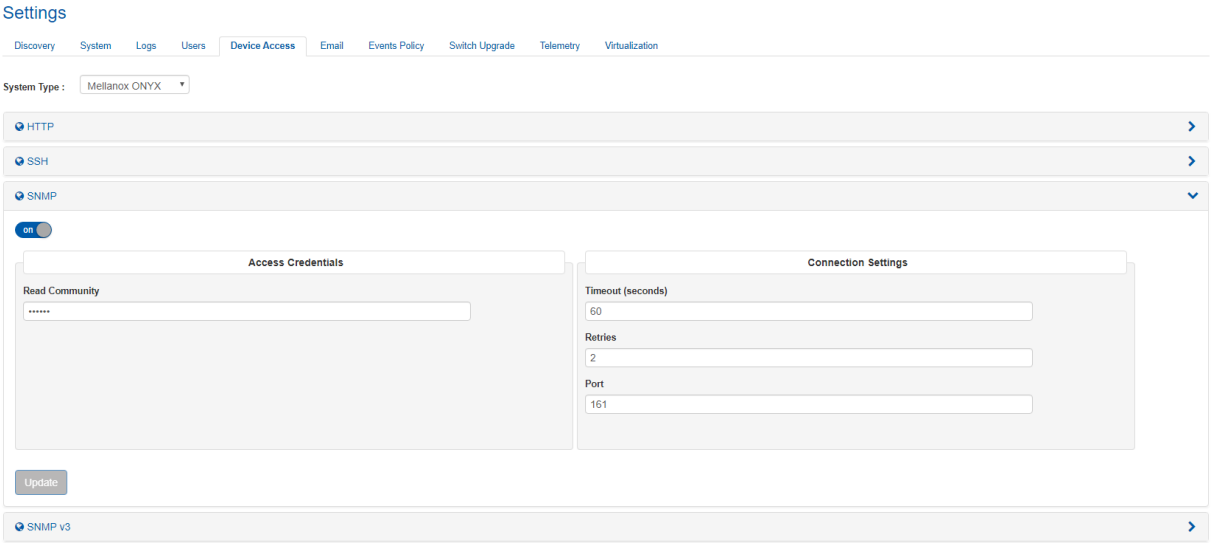
To add a new user, click “New” and fill in the required credentials (see Mellanox NEO GUI Fields Validations).





Device Access

The “Device Access” view allows administrators to change the default global access credentials for each protocol (HTTP, SSH, SNMP and SNMPv3), and change the connection settings for SNMP and SNMPv3 protocols. Such changes will only apply to devices for which no unique access credentials are defined (either exclusively or in association to a group).



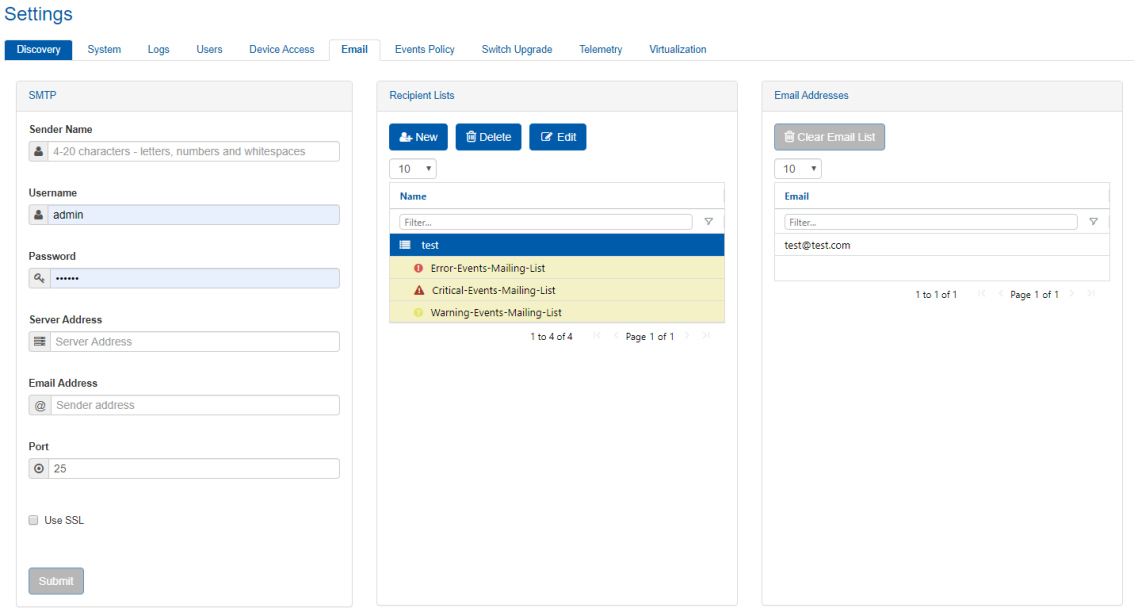
Note that only one of the SNMP protocols can be activated at the same time. These protocols can be activated/deactivated using the on/off button.

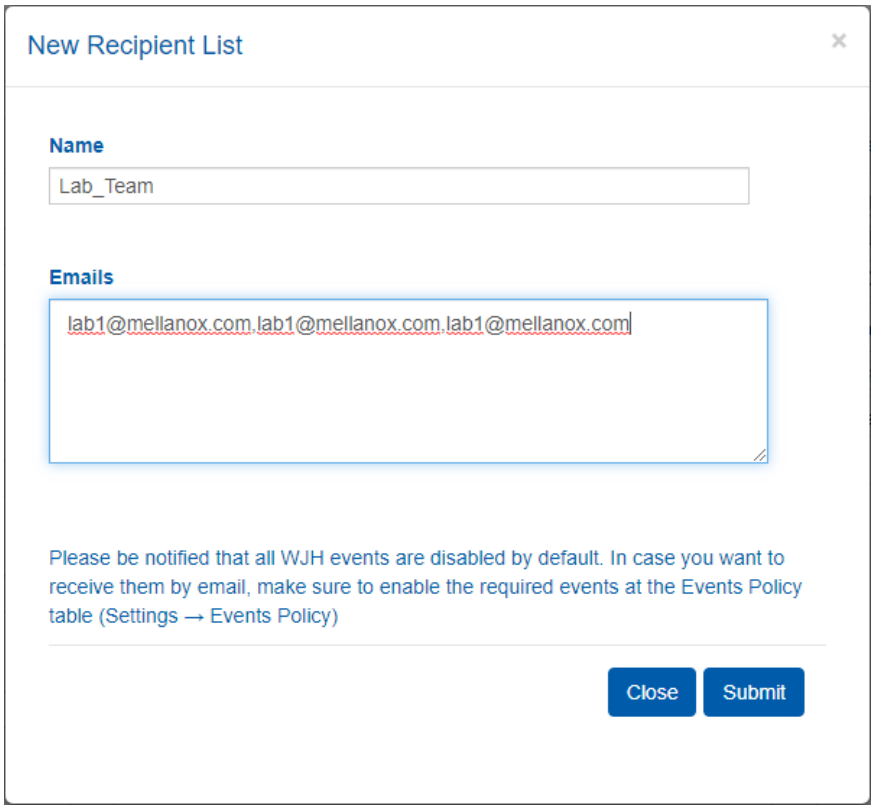
The active Onyx SNMP protocol version also affects the SNMP protocol version that NEO uses to listen to SNMP traps. This SNMP version is also used to configure switches when checking the "SNMP Traps" auto-provisioning option.

Email

The Email view is divided to two sections:

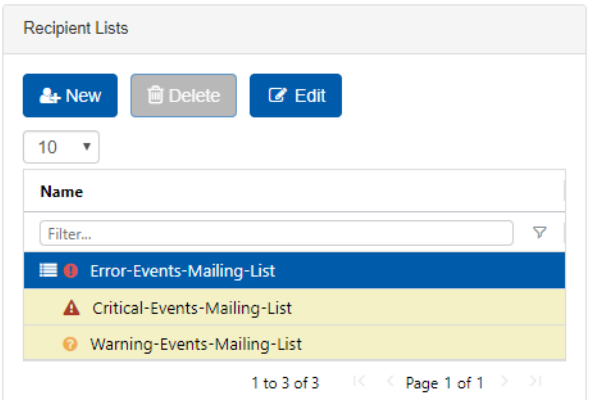
- The SMTP section allows administrators to configure a default email client to be used by Mellanox NEO for event notifications. Once the requested SMTP parameters are filled, the user can select the type of events for which email notifications are generated. For more information, see Events section.
- The Recipient Lists section allows the user to add email addresses lists to be used to distribute specific event alerts. To add a new list, click on the “New” button, insert a list name and a list of the desired email addresses, separated by commas (with no spaces).

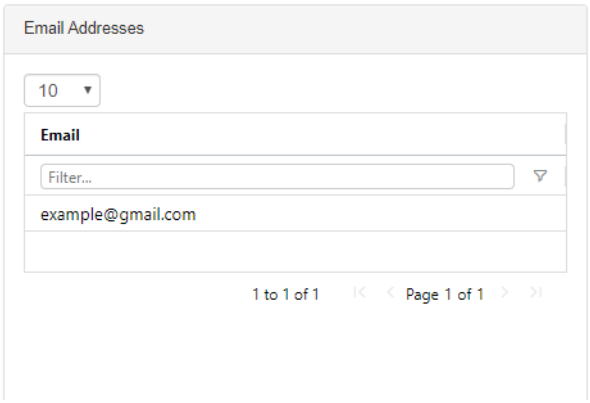




Configuring Email Notifications According to Event Severity

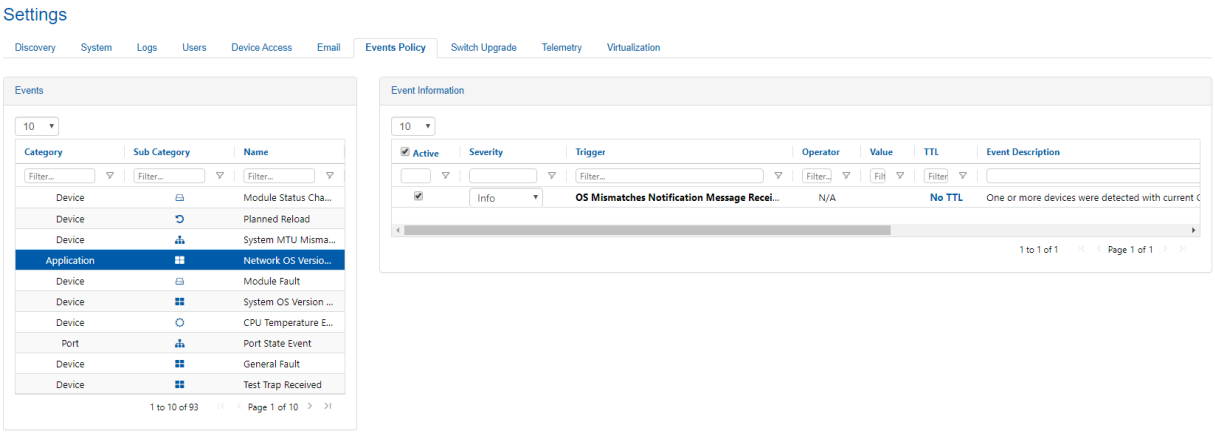
User are able to add an email to predefined mailing lists for events with different severities (i.e. Critical/Error/Warning). Once emails are added to a certain recipient list, NEO will send email notification for all events with that particular severity destined to the addresses defined within the recipient list.





Events Policy

The “Events Policy” view allows the user to activate and deactivate events, and to define the severity, condition-value and description of each event. Clicking an event name displays its relevant Event Information table.



The Event Information table displays the following columns:

- “Active” – check or uncheck boxes to activate or deactivate events as desired.
- “Severity” – there are 5 severity types: Info, Notice, Warning, Error and Critical. You may match each of the events to the appropriate severity type, as you see fit.
- “Trigger”, “Operator” and “Value” – these 3 parameters are used to define the circumstances which lead to the event’s generation. The “Value” is configurable, and may be a single number, or a range of values, depending on the event type.
- “TTL” – “Time To Live” (TTL) is used for setting a time frame within which an event that is taking place will become auto-acknowledged.
    - “No TTL” is set as default for most device evens and indicates that no TTL has been set for a specific event. To set a TTL, click the “No TTL” description and set the time frame in seconds, minutes, or hours, and click the  icon.
    - “24h” is set as default for most application events and indicates an auto-acknowledgment within 24 hours. This time frame can be edited by clicking the “24h” description and setting any other number of seconds/minutes/hours and then clicking  .

- “Event Description” – a brief definition of the event. You may edit the event description by clicking it.
- “Task” – associate an existing task to the selected condition. If a task is not assigned to objects, it will run on the objects on which the event took place.
- “Filter” – select a specific group for which the conditional event will apply. If no filter is set, the event will apply on all devices/ports in the network and will appear under the “Events” window. If a filter is set for a certain group, the event will only apply on the devices/ports in that group.

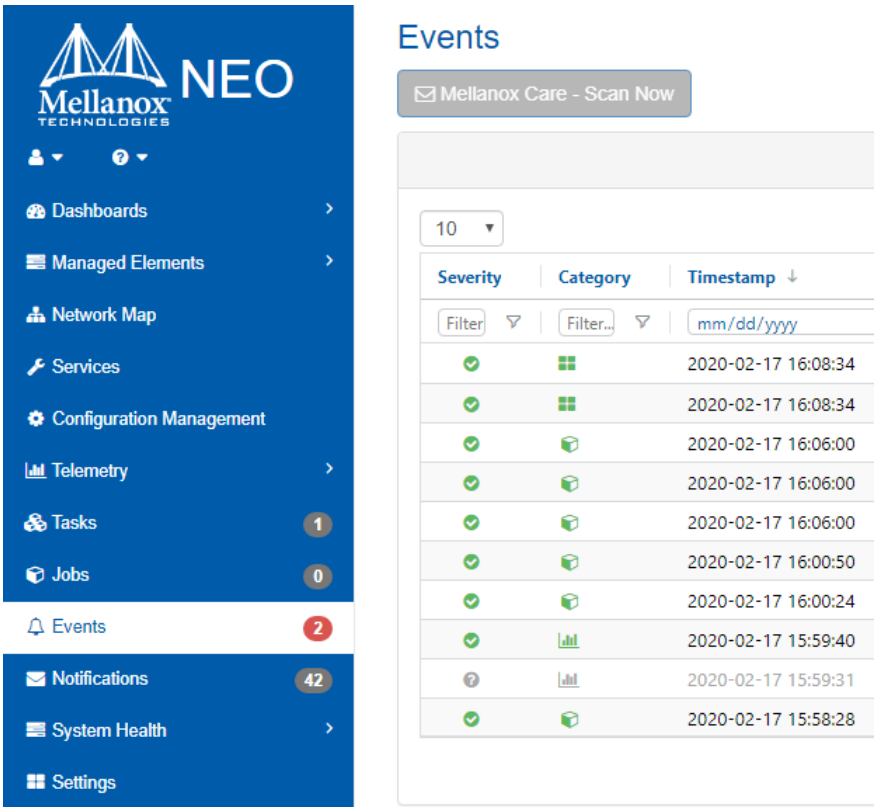
To create a new filtered condition, either click the “+” icon, or right click the event you wish to clone. Choose “Create a new filtered condition”, and select the groups you wish to apply the new conditional event on.

- “Email Notification” ( ) – set recipient lists to which alert emails will be sent when the event occurs, by clicking on the plus sign adjacent to the relevant event.
- “Mellanox Care” – this column is enabled for setting only after operating the Mellanox Care feature.

> Mellanox Care is a special service requiring a license. To obtain a license, please contact Mellanox Support.

For all the events with a checked Mellanox Care box, NEO generates and sends a regular email to Mellanox NOC with details of these events. (Note that the boxes of some events are checked by default.)

The Mellanox Care email is sent at the frequency defined in the Mellanox Care configuration (“sending_interval” parameter), and contains an aggregate of event occurrences during the last “scanning” interval. The details of the events are kept in a NEO database that is cleared each time an email is sent. Note that if no events occur during a scanning interval, no email will be sent for this interval. Mellanox NEO enables the user to “induce” a Mellanox Care email and not wait for the entire scanning interval to expire. To do so, go to the Events menu (left pane) and click the Mellanox Care - Scan Now button (see below). This generates and sends an email to Mellanox NOC with the aggregated events since the last sent email. The events database will be cleared after this email too.



Further information on events can be found in Application Events and Device Events.

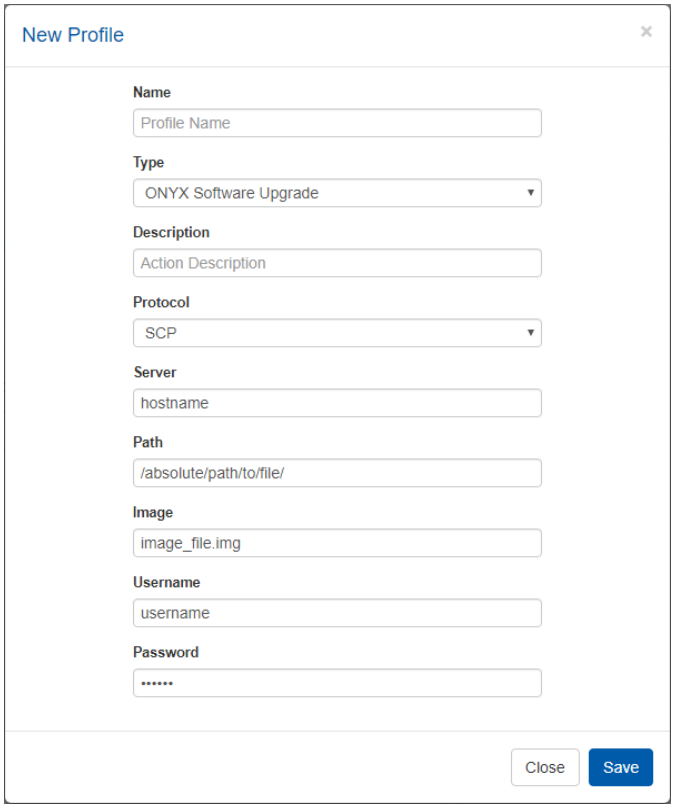
Image Profile

Through the Image Profiles view, users can define profiles with parameters required for NEO to execute switch software (Onyx) upgrade, driver install, Docker image load or generate switch dump file.

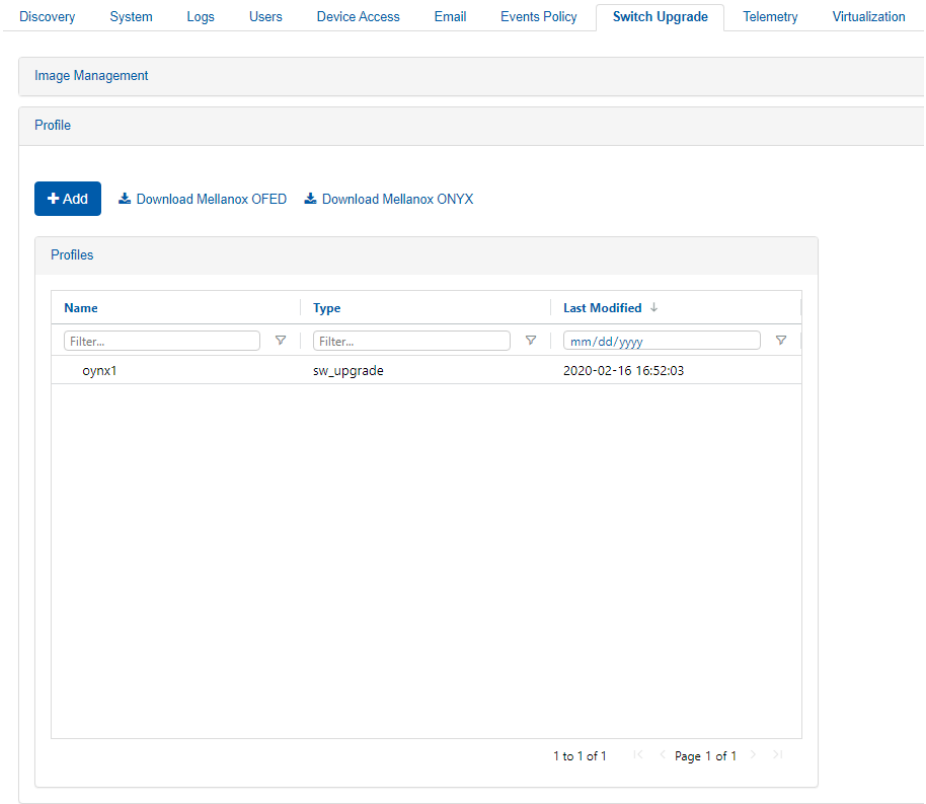
These profiles will become available under Managed Elements → Devices (right-click a host/ device) → Onyx Software Upgrade/Driver Install/Load Docker/Remote Folder → (dialog window) Profiles drop down menu.

To create a profile:

1. Click the “Add” button.
2. Fill in the data, including the type of profile (Onyx Software Upgrade/Driver Install/Docker Container/Remote Folder), and click “Save”.



A new profile with user-defined parameters will be created.



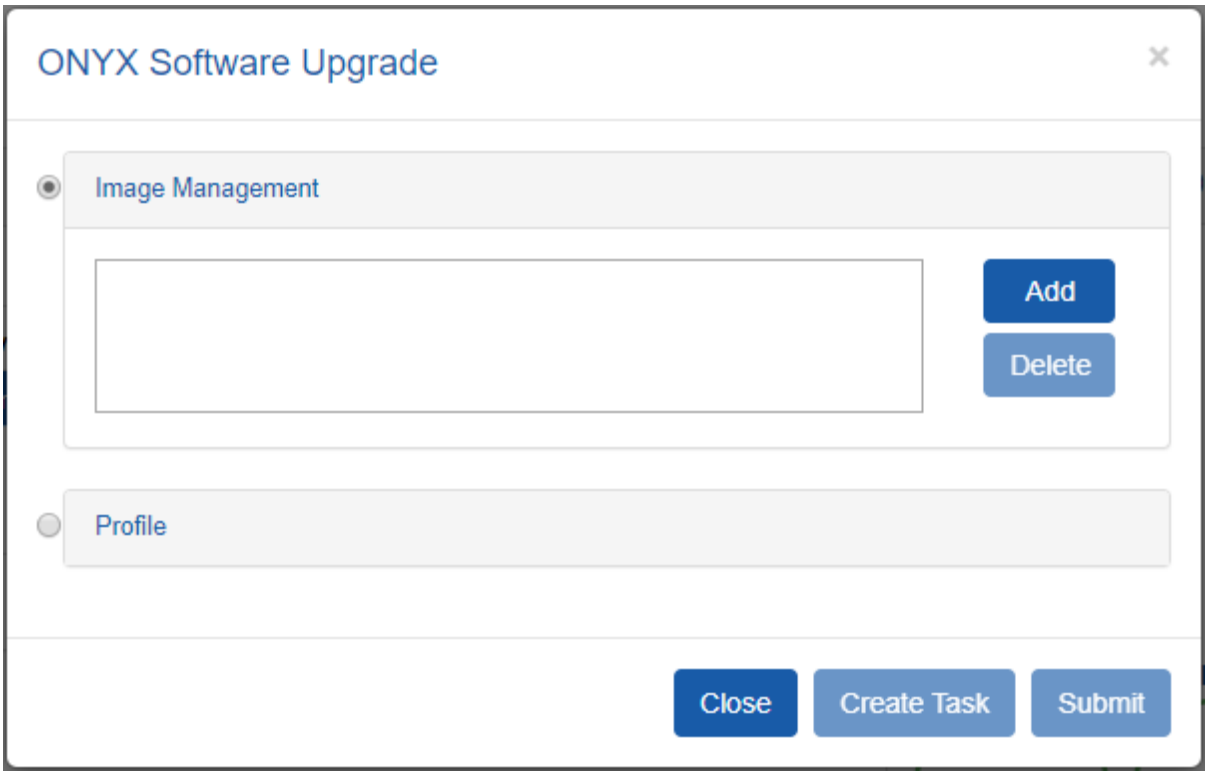
- To edit an existing profile, click it, modify the parameters on the right pane, and either click “Save” to overwrite it, or click “Save As” to create a new profile
- To remove a profile, right-click it and select “Remove”

These profiles will become available under Managed Elements → Devices (right-click a host/ device) → Onyx Software Upgrade/Driver Install/Load Docker → (dialog window) Profiles drop down menu.

> ⚠ Users can create up to 200 SW Upgrade/Docker Container/Driver Install profiles.

Image Management

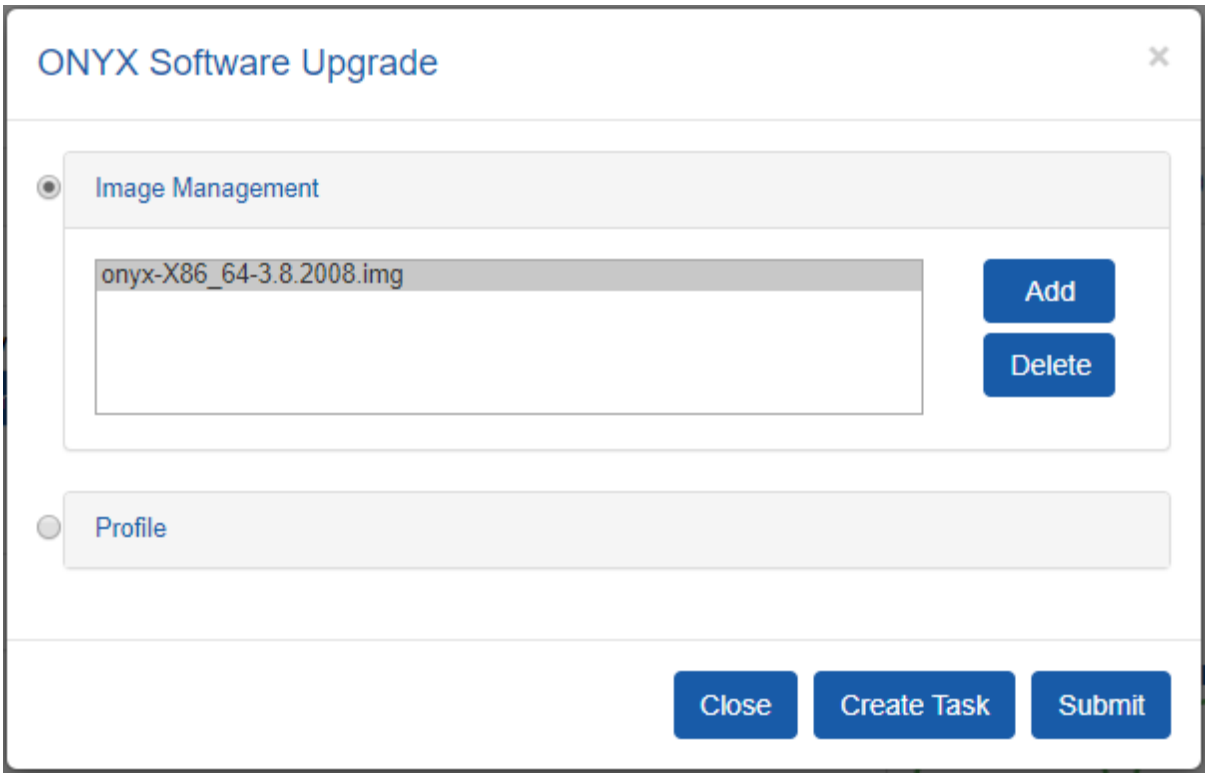
An alternative option to Image Profile, image management allows users to upload an NOS image directly from their local machine to the NEO management system.



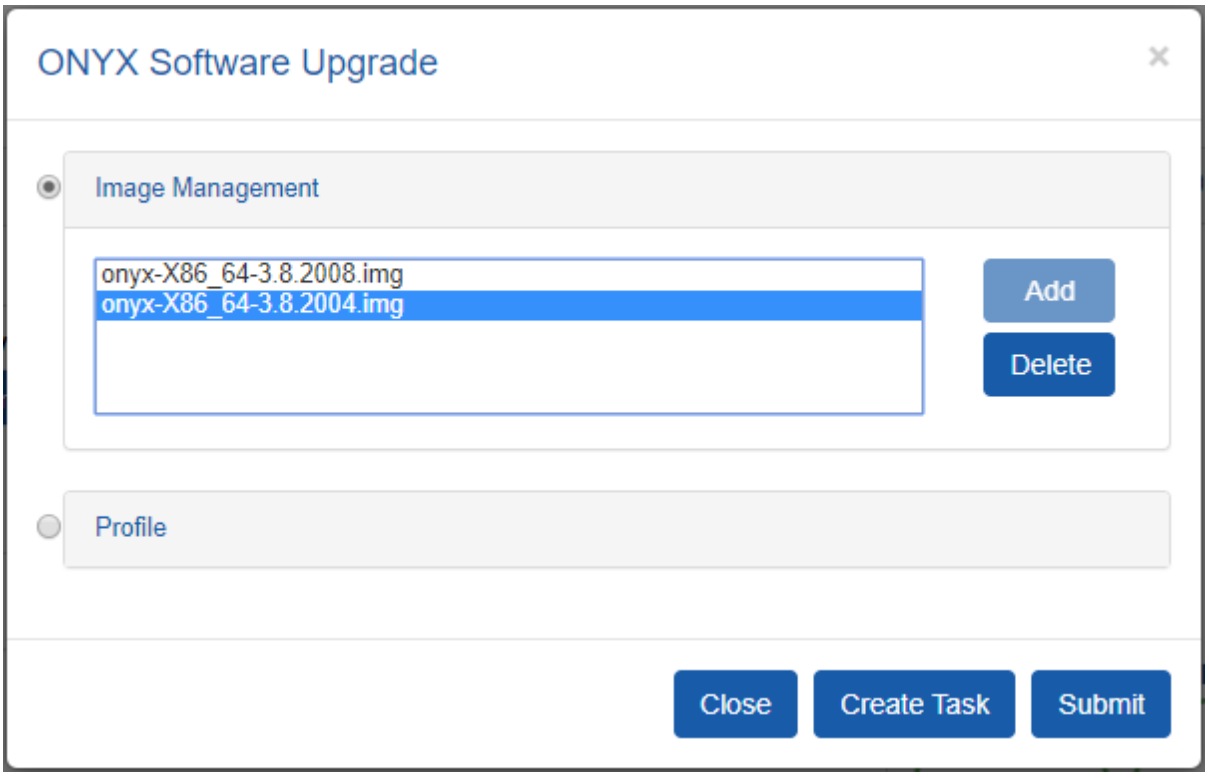
Users may reach the Image Management screen by following any of the following procedures:

- Managed Elements → Devices → Right-clicking one of the listed devices → Install → Onyx Software Upgrade
- Tasks → +Add → Operation tab → Onyx Software Upgrade operation → Objects tab → Adding devices to be upgraded → Parameters tab
- Settings → Switch Upgrade tab

By clicking the Add button, users are able to browse their local machine's directories and select the NOS image they would like to load.



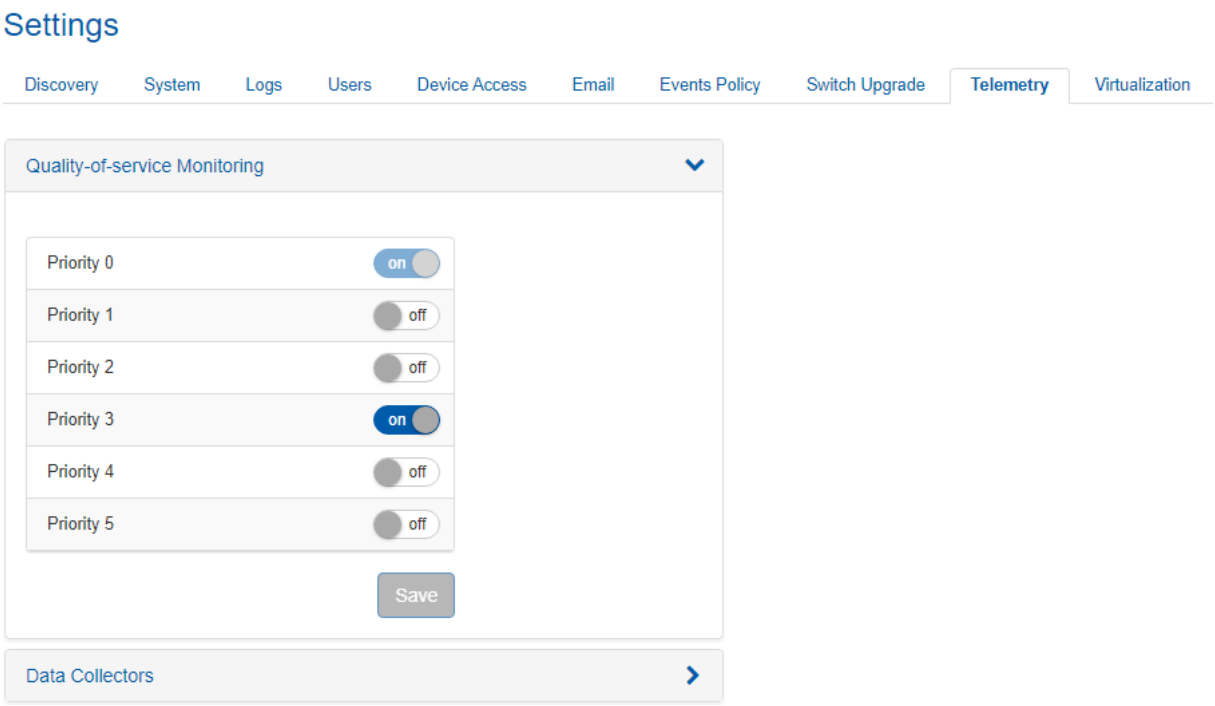
Users are able to upload up to 2 images to have on hand by clicking Add again and selecting a new image file.



Telemetry

Priority Counters

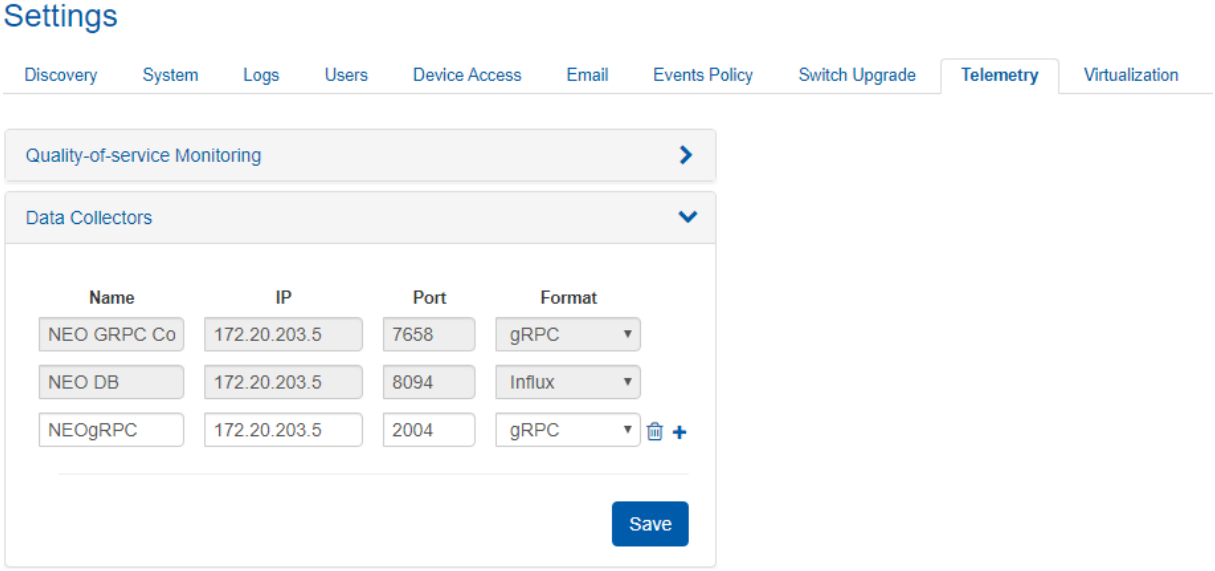
This section shows the priorities available for monitoring and usage in RoCE configuration. Each priority level has an on/off switch next to it, to enable or disable its usage. Priority 0 is always available and only one additional priority can be selected at a time. These priorities are used in the Telemetry wizard if Spectrum switches are monitored. If a priority level is enabled, it can be selected for the Telemetry operation.



Displays access credentials for the specific Mellanox device in four protocols – HTTP, SSH, SNMP, SNMP v3.

Data Collector

The Data Collector is the IP and port of the server that will collect the telemetry raw data.



NEO is configured to a number of default collectors, which cannot be removed.

> ⚠ Collectors that are related to sessions cannot be removed.

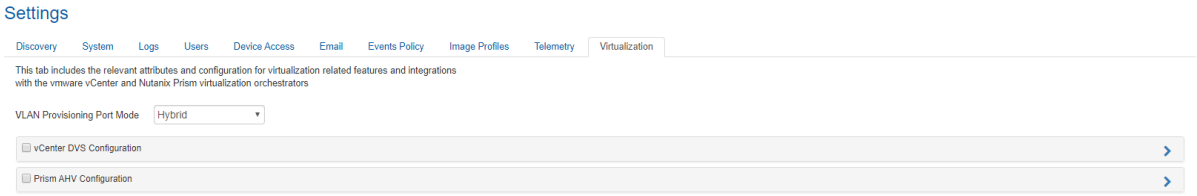
> ⚠ Make sure to add a collector before creating a session.

Virtualization

In this page, the user can define integration with various hypervisors. This can help NEO acquire information about the VMs running on them and handle VM lifecycle events to proper VLAN configuration on the switches.

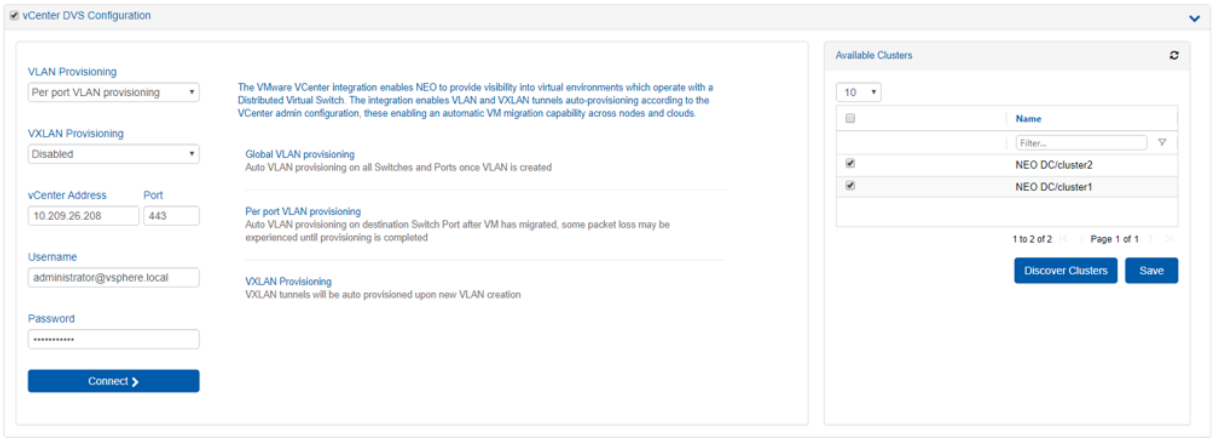
VLAN provisioning operations can be viewed under jobs (Jobs with the description Create/Delete VLAN, Create/Delete Network and Create/Delete Cluster are VLAN Provisioning jobs).

VLAN Provisioning Port Mode – the user can select what mode the switch ports are working with (Hybrid/Trunk). This will be used when using NEO to handle VM lifecycle events and change switch VLAN configuration accordingly.



VMware vCenter DVS Configuration

vCenter Server is the centralized management utility for VMware, and is used to manage virtual machines, multiple ESXi hosts, and all dependent components from a single centralized location. In this section, the user can define VMware vCenter connectivity information, which allows managing ESXi hosts.



The VLAN Provisioning drop down contains the following options:

- Disabled – VM lifecycle events will not be handled. NEO will only retrieve VM information from vCenter.
- Global VLAN provisioning – NEO will listen to network events. In case of a network change event (e.g. adding or removing a network), NEO will add or remove VLANs to/from all switch ports. VLANs will be removed from the ports but will not be removed from the switch.
  This is the recommended VLAN provisioning mode when working with Live Migration.
  In this mode, the VLANs' auto-provisioning is performed upon network creation (before the VM migration event) therefore, it prevents traffic lose.
- Per port VLAN provisioning – NEO will listen to VM lifecycle events. In case of a VM change (e.g. VM added, removed or migrated) which required changes in VLANs, NEO will add or remove the VLAN accordingly from the relevant switch ports.
  Some packet loss may be experienced until provisioning is completed.

The VXLAN Provisioning drop down contains the following options:

- Disabled –VXLAN tunnels will not be configured on VM lifecycle events.
- L2 – VXLAN tunnels will be configured on VM lifecycle events, and NEO will treat them as layer 2, without gateway configuration.

Upon filling the vCenter IP address, port, username and password, the user should click the Connect button to make sure the details are correct and NEO can connect the vCenter.

The Connect button should be clicked after every change so the new information will be processed by NEO.

Limitations:

- Regular Virtual Switches are not supported (this capability supports only Distributed Virtual Switches)

- Old events are not supported
- Removing network adapters while VM is ON is not supported
- Network configuration changes (DVS changes) are not supported
- NEO allows adding a list of ESXi manually or by choosing a cluster. For each cluster that will be chosen, a group will be created for the dedicated cluster.

To add a ESXi device manually:

See Adding/Removing Devices.

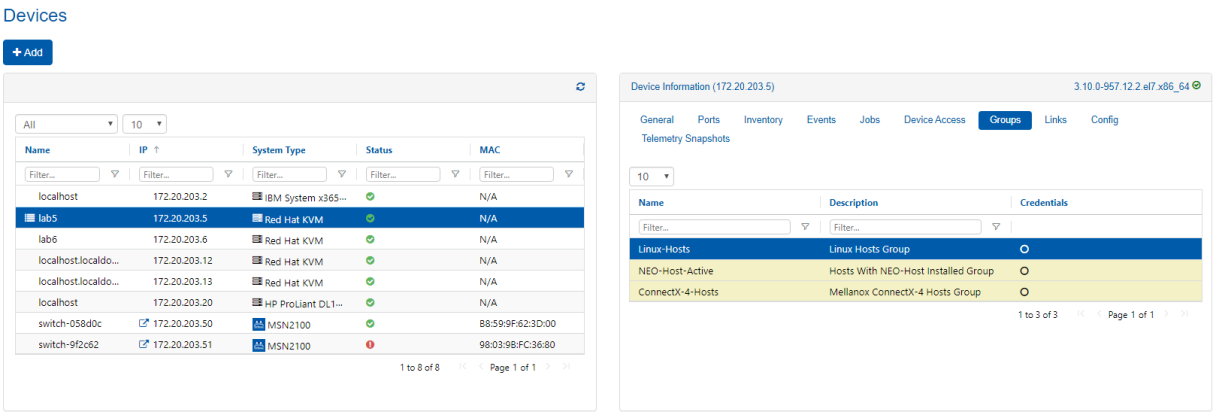
To add a cluster:

If the connection to vCenter is successful, a list of clusters managed by vCenter will be shown in the Clusters table.

Under Available Clusters a list of available clusters will be shown, mark the ones that you want to discover.

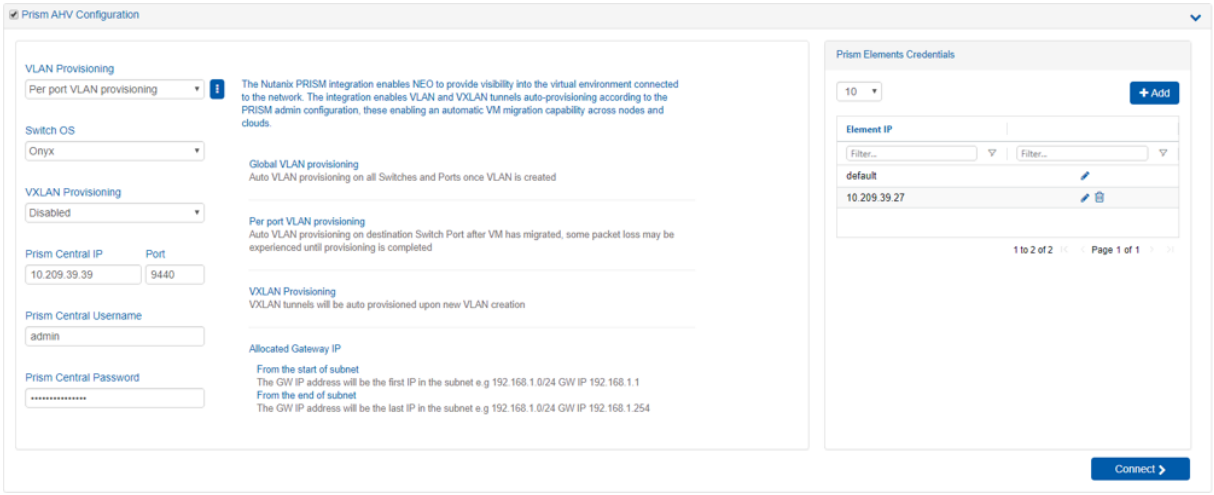
To refresh the list, click Discover Clusters.

To save and discover the Clusters, click Save and new ESXi hosts will be discovered under Managed Elements:



Prism AHV Configuration

In this section the user can define Nutanix Prism Central and Prism Element connectivity information. NEO uses it to get information from Prism regarding devices, VM information and lifecycle events. For further information, refer to Mellanox NEO/Nutanix Prism Plug-in.

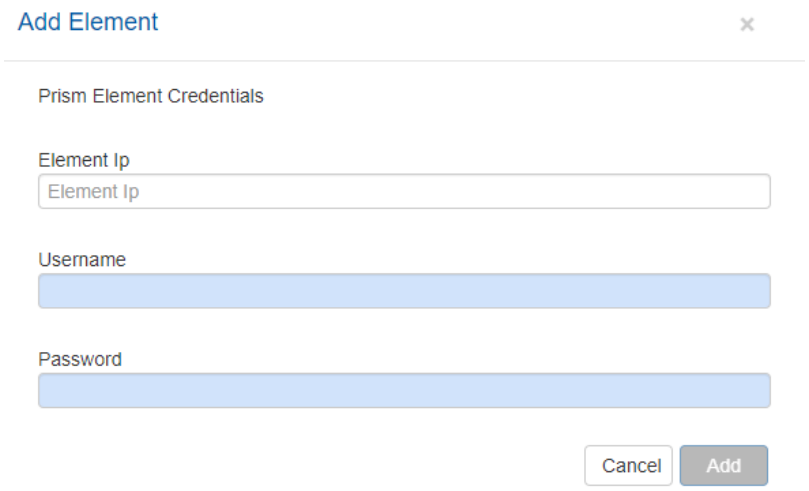


The VLAN Provisioning drop down contains the following options:

- Disabled – VM lifecycle events will not be handled. NEO will only retrieve VM information from vCenter.
- Global VLAN provisioning – NEO will listen to network events. In case of a network change event (e.g. adding or removing a network), NEO will add or remove VLANs to/from all switch ports. VLANs will be removed from the ports but will not be removed from the switch.
  This is the recommended VLAN provisioning mode when working with Live Migration.
  In this mode, the VLANs' auto-provisioning is performed upon network creation (before the VM migration event) therefore, it prevents traffic lose.
- Per port VLAN provisioning – NEO will listen to VM lifecycle events. In case of a VM change (e.g. VM added, removed or migrated) which required changes in VLANs, NEO will add or remove the VLAN accordingly from the relevant switch ports.

The VXLAN Provisioning drop down contains the following options:

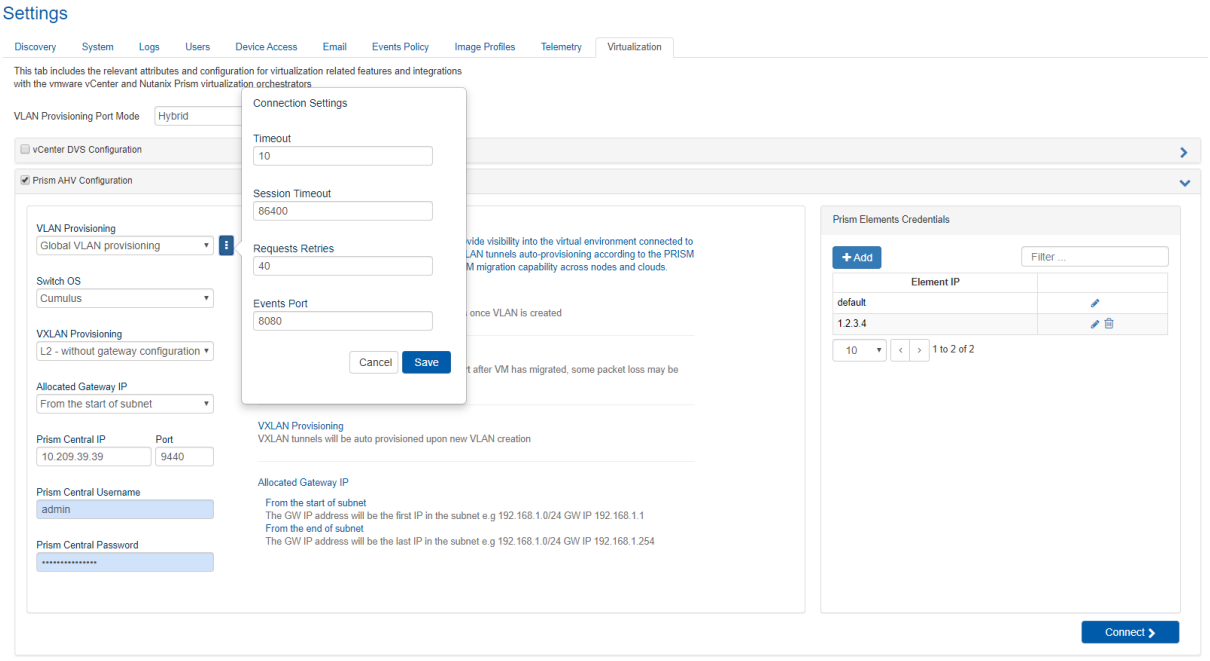
- Disabled –VXLAN tunnels will not be configured on VM lifecycle events.
- L2 – VXLAN tunnels will be configured on VM lifecycle events, and NEO will treat them as layer 2, without gateway configuration.
- L3 - VXLAN tunnels will be configured on VM lifecycle events, and NEO will treat them as layer 3, with gateway configuration. (supported only for Cumulus OS)
- Allocated Gateway IP – chooses whether the allocated gateway IP will be in the beginning of the subnet or in the end
- Prism Central IP - IP, port, username and password are used to connect to the Prism Central. In case of working without Prism Central, put the Prism Element details instead.
- Prism Elements Credentials – in this table the user should fill the username and passwords of each Prism Element in the network. Use “default” to fill the same credentials to all Prism Elements or specify credentials per Prism Element IP.



Upon filling the Prism Central IP address, port, username and password, and the Prism Element credentials, the user should click the Connect button to make sure the details are correct and NEO can connect the Prism. If the connection is successful, the switches and Nutanix hosts known to Prism will be added to NEO. This might take a couple of minutes.

The Connect button should be clicked after every change so the new information will be processed by NEO.

When enabling VLAN provisioning, the user can also set some advanced properties that affect the communication with Prism:



Add a device either by manually typing its IP address, or by scanning a range or a subnet of IP addresses.

Start the Restore task by right click on the image.

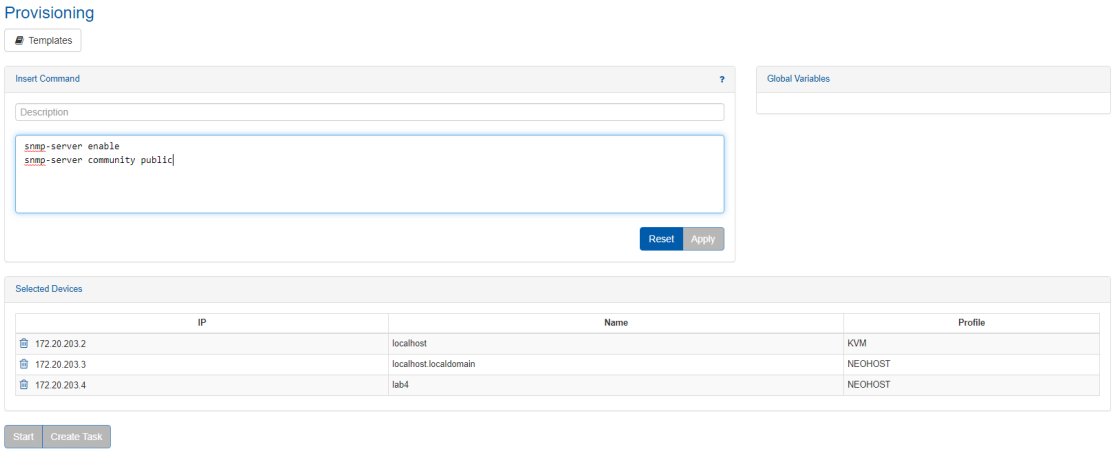
Configuring Managed Network Components

In order for Mellanox NEO® to retrieve information from Mellanox Onyx® managed switches and hosts, additional configuration on switches and hosts is required.

Configuring SNMP on Mellanox Onyx Switch (for Port Counters Monitoring)

To configure all Mellanox Onyx managed switches via Mellanox NEO GUI, perform the following:

1. Go to the “Managed Devices” table (Managed Elements → Devices).
2. Select the desired Mellanox Onyx switches to configure SNMP on (you can select multiple switches).
3. Right click on the selected switches and click on “Provisioning”
4. In the “Provisioning” view, click on the “Templates” button and load the “Enable-SNMP” template.
5. Click on the “Apply” button.
6. To send the configuration to the selected switches, click on the “Start” button. This will redirect you to the “Jobs” table.
7. Make sure that all sub-jobs (all switches) are completed successfully.



> To configure the SNMP-V3 protocol, refer to the Mellanox Onyx User Manual.

> For the SNMP monitoring to work properly, the credentials on the switch must match the Mellanox NEO switch settings.

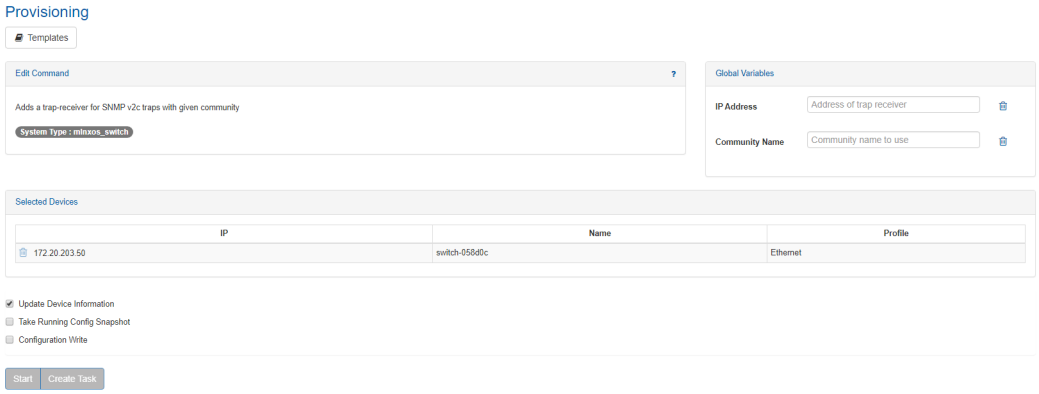
Configuring Mellanox Onyx Switch for Sending Traps to Mellanox NEO

NEO can listen to SNMP traps and generate events upon receiving them. NEO supports both SNMP v3 and v2c traps.

By default, NEO listens to SNMP v2c traps. If you want to use SNMP v3, refer to Setting NEO SNMP Trap Protocol Registration in order to configure NEO to listen to it.

You can configure the switches to send SNMP traps to NEO using one of these two methods:

- *Using auto-provisioning:* When adding the device, check the SNMP Traps auto-provisioning option. The protocol version configured (2c/3) depends on the SNMP protocol version active in the Onyx global credentials.
- *Using provisioning templates:*
    a. Go to the "Managed Devices" table (Managed Elements → Devices).
    b. Select one or more of the desired Mellanox Onyx switches to configure SNMP on (you can select multiple switches).
    c. Right-click the selected switches and click "Provisioning".
    d. In the "Provisioning" view, click the "Templates" button and load template relevant for the SNMP protocol you use ("Set-SNMP-V2c-Traps" or "Set-SNMP-V3-Traps"). For example:



    e. Click the "Apply" button.
    f. Set the "ip_address" field in the "Global Variables" panel to be your Mellanox NEO IP address.
    g. Click the "Start" button. This will redirect you to the "Jobs" table.
    h. Make sure that all sub-jobs (all switches) are completed successfully.

⚠ NEO removes itself as an SNMP trap listener from Onyx switches when they are removed.

Setting NEO SNMP Trap Protocol Registration

NEO listens by default to SNMP v2c traps. If the user changes the active SNMP protocol in the Onyx global credentials, the trap listening is also changed accordingly.

To configure NEO side SNMP v3 or v2c trap listening properties, edit the file `/opt/neo/providers/dm/conf/netservice.cfg`.

- When working with SNMP v2c, configure the following attributes in the [Snmp] section:

```
[Snmp]
#valid protocol: snmpV2c, snmpV3
protocol=snmpV2c
#valid for snmpV2c
community=public
```

- When working with SNMP v3, configure the following attributes in the [Snmp] section:

```
[Snmp]
#valid protocol: snmpV2c, snmpV3
protocol=snmpV3
#valid for snmpV3
#valid auth protocol: MD5, SHA
auth_protocol=MD5
#valid priv protocol: DES, AES-128
priv_protocol=DES
auth_password=adminauth123
priv_password=adminpriv123
```

For the configuration changes to take effect, restart NEO by running:

```
/opt/neo/neoservice restart
```

Configuring Mellanox Onyx Switch for LLDP Discovery

To configure all managed Mellanox Onyx switches via the Mellanox NEO GUI, perform the following:

1. Go to the “Managed Devices” table (Managed Elements → Devices).
2. Select the desired Mellanox Onyx switches to configure SNMP on (you can select multiple switches).
3. Right click on the selected switches and click on “Provisioning”.
4. In the “Provisioning” view, click on the “Templates” button and load the “Enable-LLDP” template.
5. Click on the “Apply” button.
6. Click on the “Start” button to send the configuration to the selected switches.
7. Click on the “Start” button. This will redirect you to the “Jobs” table.
8. Make sure all sub-jobs (all switches) are completed successfully.

Configuring Host for LLDP Discovery

In order to allow the LLDP to discover hosts, you must configure it accordingly. For instructions, refer to the following community page: HowTo Enable LLDP on Linux Servers for Link Discovery.

When configuring LLDP on the host, please make sure to configure the LLDP to publish the management IPv4 address of the host (i.e. the IP that Mellanox NEO must recognize and manage). Not doing so might result in non-deterministic behavior.

Configuring Windows Host for Basic Authentication

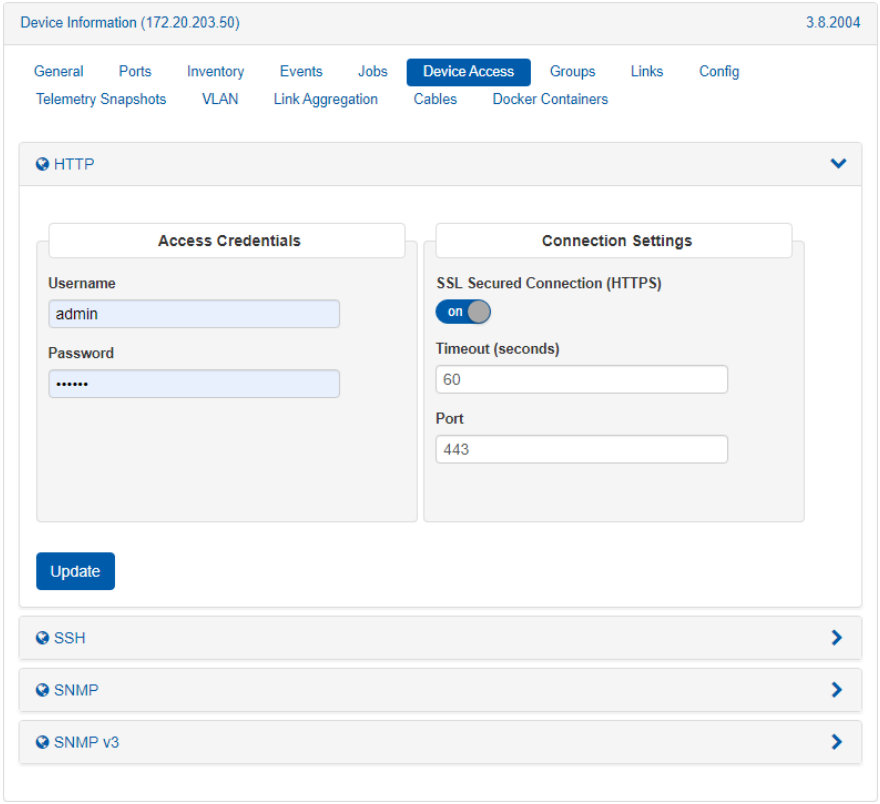
Basic authentication works across firewalls and proxy servers. Basic authentication requires valid user name and password to access content.

By default, Windows host authentication type is Kerberos. In order to connect to NEO, make sure basic authentication is enabled as well.

Allow basic and unencrypted message passing over WinRM on each of the Windows managed machines. Run the following command over PowerShell:

```
winrm set winrm/config/service @{AllowUnencrypted="true"}
winrm set winrm/config/service/auth @{Basic="true"}
```

Set the device credentials in the UI. Username attribute format must include the domain (username@domain), for example: administrator@mellanox.com.



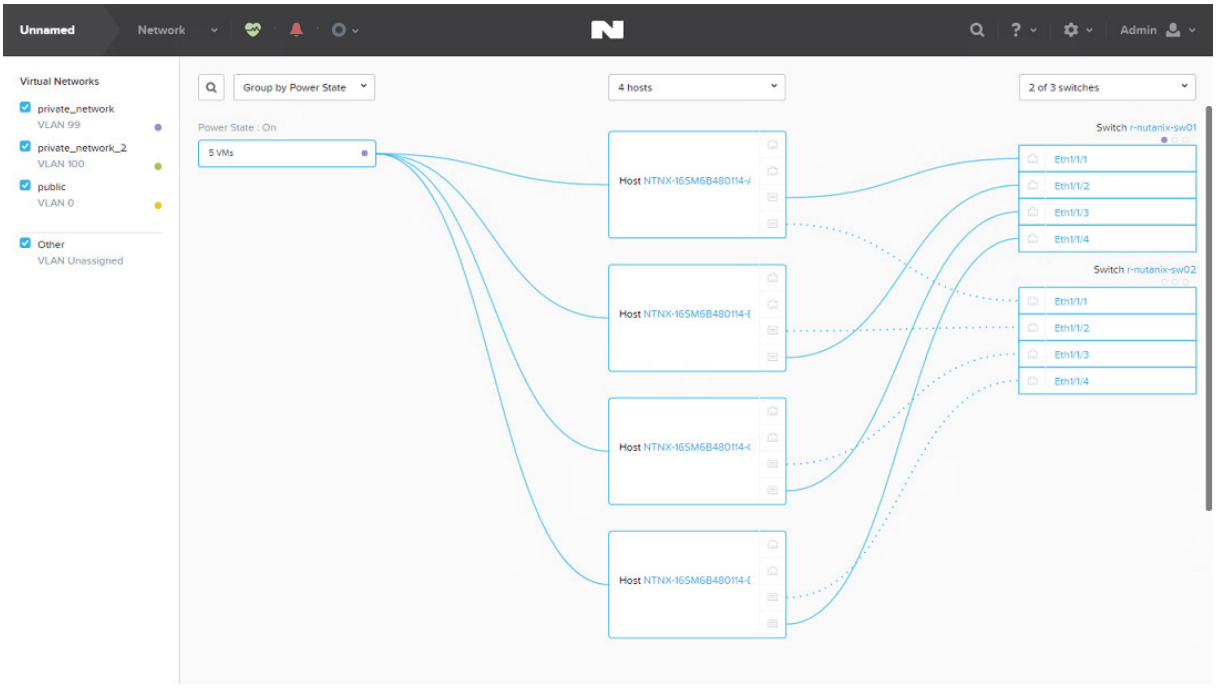
Appendix – Mellanox NEO/Nutanix Prism Plug-in

The Mellanox NEO/Nutanix Prism plug-in is a software add-on that offers enhanced functionality to Mellanox and Nutanix customers. As of NEO v2.5, the plug-in is bundled with NEO and will be automatically activated when enabling Prism integration in the bring-up wizard or the virtualization settings.

Nutanix Prism offers enhanced network capabilities, including a set of APIs to use Prism's accumulated VM data. Mellanox uses these new APIs to develop an integrated solution between Nutanix Prism and Mellanox NEO, which adds network automation for Nutanix Virtual Machine life-cycle management.

This integration addresses the most common use-cases of the Nutanix hyperconverged cloud: VLAN auto-provisioning on Mellanox switches for Nutanix VM creation, migration and deletion.

Mellanox NEO/Nutanix Prism plug-in purpose is to synchronize between a Nutanix cluster deployed with Mellanox switches, using the Mellanox NEO platform. By using this plug-in, users can start a service to listen to Nutanix cluster's events and have the infrastructure VLANs provisioned transparently. The plug-in can be installed and run on any RHEL/CentOS server (v6 or above) that has connectivity to both Nutanix Prism and the NEO API (including the NEO server itself).



Definitions, Acronyms and Abbreviations

Name	Description
Nutanix AOS	Nutanix Acropolis Operating System
Nutanix Node	A hypervisor server with Nutanix AOS installed
Nutanix Cluster	A group of nodes with Nutanix AOS installed
CVM	Controller Virtual Machine. Each cluster node has a CVM. Commands can be executed in CVM to take effect on the node

Name	Description
Prism	The web interface of Nutanix Cluster for network configuration, that creates VMs, etc. It can be accessed using any CVM IP address: https://<CVM_IP>:9440/console

Key Features

The plug-in enables the following functionalities:

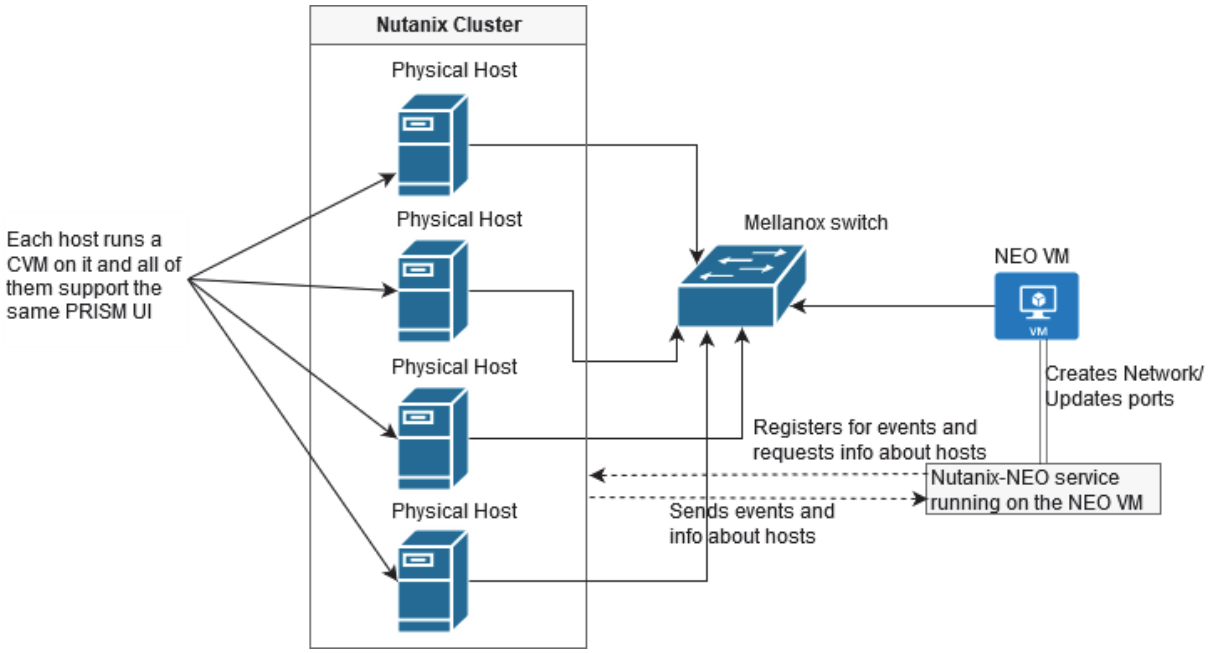
- Registering and listening to Nutanix Prism events
- Supporting auto-sync and switch auto-provisioning in the following events:
  - VM Creation
  - VM Deletion
  - VM (live/non-live) migration
  - Periodically
  - Upon service start
  - Subnet Creation
  - Subnet Deletion
- Supporting the following switch port modes:
  - LAG port channel
  - MLAG port channel
  - Port splitters
- Supporting the following Mellanox switch systems:
  - Mellanox SN2000 series of Ethernet switch systems
  - Mellanox SX1000 series of Ethernet switch systems
  - Supporting Cumulus switches

General Prerequisites

Make sure the following requirements are fulfilled in order for the Nutanix Prism plug-in to work properly:

- Nutanix Appliance v5.0.0.2 or above installed over cluster nodes with aspects documented in Nutanix website
- NEO v2.1 or above installed in the network
- SNMP and LLDP enabled on Mellanox switches
- Mellanox NEO/Nutanix Prism plug-in installed, configured and running
- All Nutanix nodes connected to the Mellanox switch
- IP connectivity between Prism and the NEO VM where the plug-in is installed

Typical Configuration



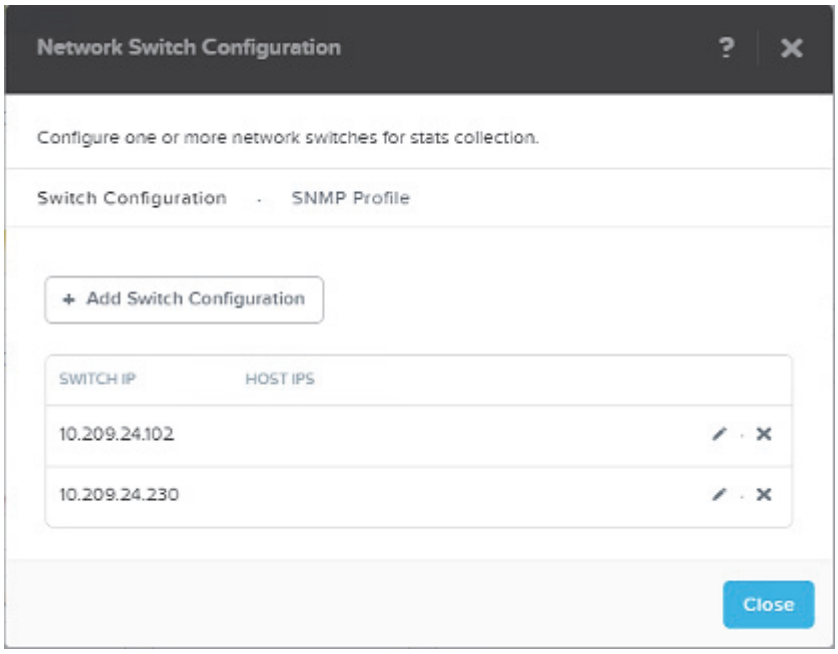
Setup Prerequisites

Cluster Nodes Configuration

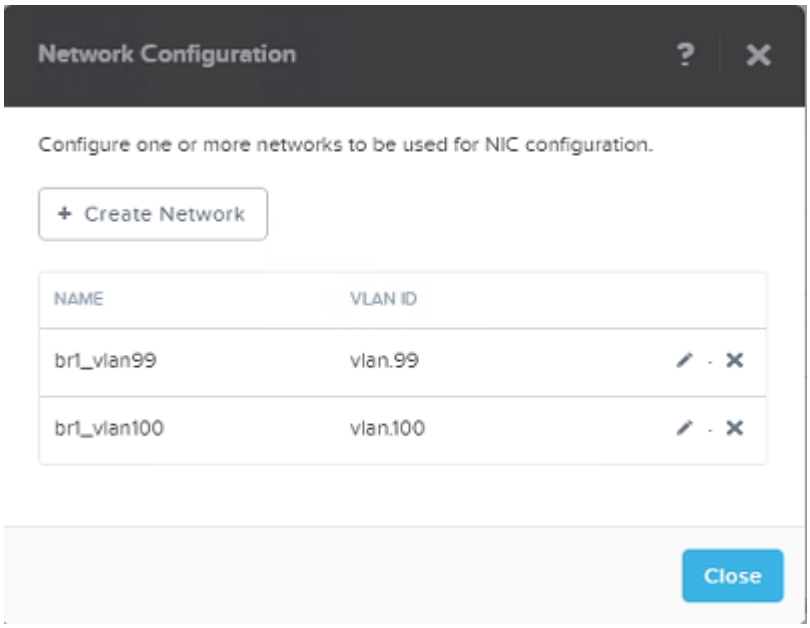
1. Enable LLDP on the switches of the environment:

```
# conf t
# lldp
```

2. Add the switches to the Nutanix Prism web UI. Click the wrench symbol on the right -> Network switch.



3. Create the Nutanix cluster network using Prism. Click the wrench symbol on the right -> Network Configuration. Make sure to edit the new network and identify the IP ranges if needed.



4. Assign a virtual IP to the Nutanix cluster. Click the wrench symbol on the right -> Cluster Details -> CLUSTER VIRTUAL IP ADDRESS.

> ⚠ For further information about Nutanix cluster network configuration, please refer to Nutanix Connect Blog.

Note:

- When there is more than one connection to the same switch, configure the LAG as follows:
  a. Configure Link Aggregation Control Protocol (LACP) on the switch.
  b. Add the LACP configuration as follows:
- For LACP bond type:

```
# ovs-vsctl set port br0-up lacp=active
```

- For normal bond type:

```
# ovs-vsctl set port br0-up lacp=off
```

NEO Virtual Machine Configuration

Add the Nutanix cluster connected switches to the NEO devices using NEO UI.

Installing Nutanix Prism Plug-in

By default, the plug-in is installed with NEO on the same machine, and is managed by NEO. In case you want to install the plug-in independently on another machine, download the plug-in from the MyMellanox portal, and install the Mellanox NEO/Nutanix Prism plug-in rpm. Run:

```
# yum install nutanix-neo-<version>.x86_64.rpm
```

For example:

```
# yum install nutanix-neo-2.5.0-3.x86_64.rpm
```

Nutanix Prism Plug-in Usage

When working with the plug-in that is bundled with NEO, all the configuration can be done from the web UI (see Prism AHV Configuration). This configuration will be saved in /opt/neo/controller/conf/nutanix-neo-plugin.cfg file. In case you work with an independent plug-in, follow the steps below:

1. Fill in the required details in the plug-in configuration file: /opt/nutanix-neo/config/nutanix-neo-plugin.cfg:

```
# Section: NEO server info
# username:                 (required) NEO username
# ip:                       (required) NEO server IP or NEO virtual IP in case
#                           of NEO HA
# password:                 (required) NEO password
#                           The password should be encrypted by the util/encrypt_config tool
# session_timeout:          (required) timeout of user session (default 86400)
# timeout:                  (required) timeout of connection (default 10)
# auto_discovery:           (required) auto add switches that are discovered in
#                           Nutanix cluster to NEO. Should be boolean
# add_host_credentials:     (optional) set Nutanix host's username and password
#                           in NEO
# host_ssh_username:        (optional) SSH login username for Nutanix hosts,
#                           required if add_host_credentials is True
# host_ssh_password:        (optional) SSH login password for Nutanix hosts,
```

```
#                           required if add_host_credentials is True
#                           The password should be encrypted by the util/encrypt_config tool
# vlan_ip_order:            (optional) The order in which reserved IPs
#                           should be taken from the subnet start/end
# vxlan_mtu:                (optional) MTU to be used for vxlan interface
#
# fast_migration:           (optional) True will make a fast migration

[NEO]
ip =1.2.3.4
#Protocol for communicating with NEO. Valid values are http/https.
#This property is optional, default is https.
protocol=https
# Port for communicating with NEO.
# This property is optional, default for https is 443 and for http is 80.
port =443
username = NEO-Nutanix-User
password = FB4M3HWCS6DGSC5TVCACFA2VDSZEPLVZ5FBYX3C42IWEL7TQ2MCQ====
session_timeout = 86400
timeout = 10
auto_discovery = True
add_host_credentials = False
host_ssh_username = root
host_ssh_password = SV5Y2RNPX3VIMIHT3UPWQUX7SFNHZIU5TRYSMQX7NCB5DUQ2SXYQ====
switch_ssh_username =
# The password should be encrypted by the util/encrypt_config tool
switch_ssh_password =
vlan_ip_order = end
vxlan_mtu = 9216
fast_migration = true
# When VLAN provisioning is disabled, the plugin will only add the
# cluster devices to NEO.
# When VLAN provisioning is enabled, in addition to device adding, the plugin
# will notify NEO on any change in VM that requires VLAN re-configuration.
# Valid values: true/false. Default is true.
vlan_provisioning = true
# When DCI is enabled, switch IPs are sent to NEO on network creation
# for VXLAN configuration on the switches.
# Valid values: true/false
dci_enable = False
dci_mode= L2


# Section: Nutanix PRISM Central and cluster info
# username:                 (required) Nutanix prism central username
# ip:                       (required) CVM IP or Virtual IP
#                                      of Nutanix prism central
# password:                 (required) Nutanix prism central user password
#                           The password should be encrypted by the util/encrypt_config tool
# requests_retries:         (required) maximum API requests retries
# cluster_default_username: (required) Nutanix cluster default username
# cluster_default_password: (required) Nutanix cluster default password
#                           The password should be encrypted by the util/encrypt_config tool
# cluster_<ip>_username:    (optional) Specific Nutanix cluster username
#                                      (overrides cluster_default_username
#                                       for the given IP)
# cluster_<ip>_password:    (optional) Specific Nutanix cluster password
#                                      (overrides cluster_default_username
#                                       for the given IP)
#                           The password should be encrypted by the util/encrypt_config tool
[PRISM]
username = admin
ip =4.3.2.1
password =OXBLXJO4U36CE5CVMRTBFII53I45N4RGPZQCCFGTW6ORS7AZPIRQ====
requests_retries = 40
cluster_default_username = username
cluster_default_password = BSCKG3ETU2Q3N7WZH4LIK2M2U3C2UXGVTKXBCMQOMHEPUVDTJLVQ====


# Section: Server where plugin installed
# ip:   (optional) IP of the server from the same subnet as the Nutanix Cluster.
#       if the ip left empty, then the plugin will obtain the server's interface
#       ip that is connected to same network as Nutanix cluster.
# port: (required) TCP port on server should be unused to receive events from
#       from Nutanix cluster.
#       if the port is used, then the plugin will kill the process that uses
#       the port and reclaim it.
[SERVER]
ip =
port = 8080
```

> ⚠ The passwords in the output above are encrypted. To update/change them, use the following encryption command:
> `/opt/nutanix-neo/utils/encrypt_config.py --section <configuration file section> --option <configuration option name> --value <clear text value>`
> For example: `/opt/nutanix-neo/utils/encrypt_config.py --section PRISM --option password --value my_password`

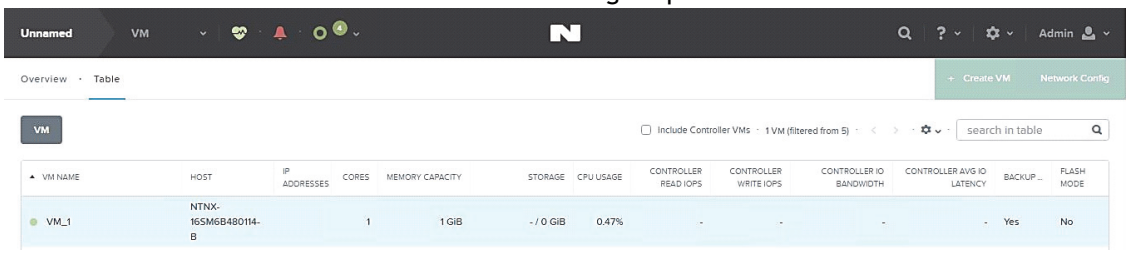
2. Start the service after installing the plug-in:

```
# service nutanix-neo start
```

3. The service will now apply the required changes in VLANs with interfaces assigned to them through NEO APIs. If two VMs are created over the same network, PING must work between the two VMs despite the Nutanix node hosting it in the cluster. In case of VM migration, the plug-in will apply the changes required on the switch to maintain connectivity.

Examples:

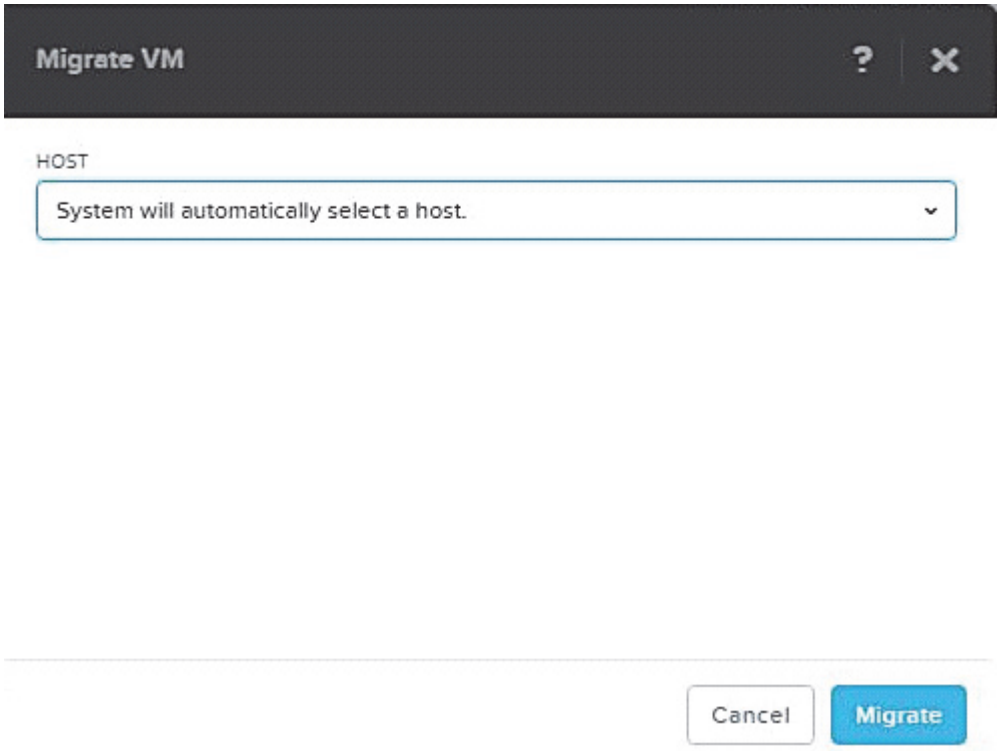
- VM Creation:
  The user creates a VM on the Nutanix cluster over a new VLAN ID 99 that did not exist on the switch before. Prism web UI will show the following output:



  The Nutanix-NEO service sends APIs to NEO to implement a job that will update the switch side about adding VLAN ID 99 to the switch with relevant Nutanix host ports, as follows:

- VM Migration:
  VM will be migrated to an automatically chosen host through Nutanix Prism web UI, as

follows:



The Nutanix-NEO service will send APIs to NEO to trigger jobs that will update the switch side with the new changes (adding VLAN ID for new host details/removing VLAN ID from old host details) as follows:

⚠ Note: Nutanix-NEO service only detects running VMs.

Nutanix-NEO Debug Files

- /var/log/nutanix-neo/console.log
- /var/log/nutanix-neo/nutanix_neo_server.log

VXLAN Support

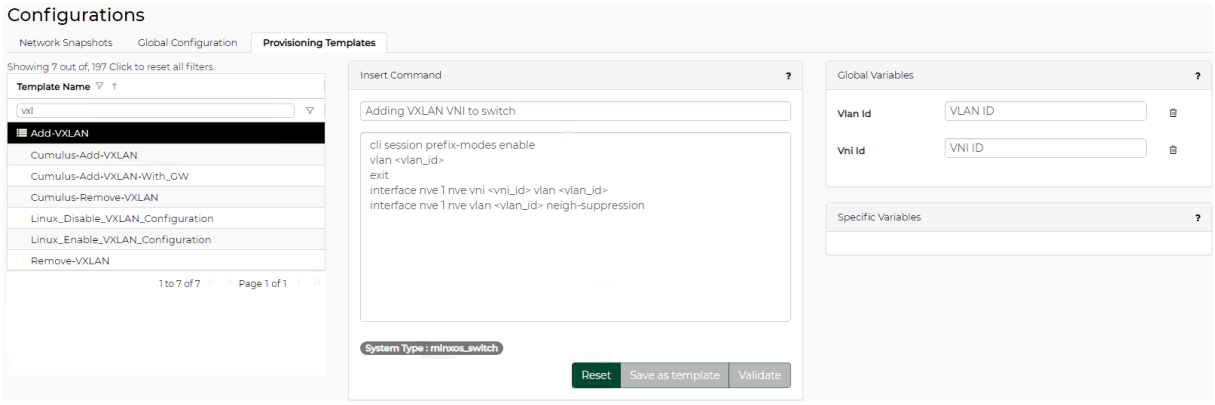
For the VXLAN support to operate, the plug-in must be running when you create the VXLAN on Nutanix. In addition, the VTEPs must be configured on the switches, and ping all VTEPs from all switches.

⚠ Vlan ID 0 is not allowed, since it is the native network.

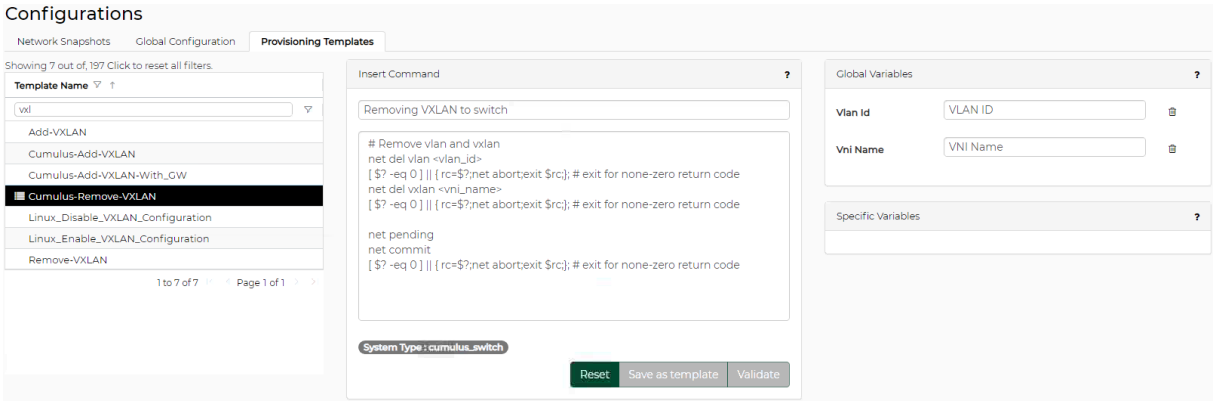
NEO VXLAN Templates

NEO has templates for creating and removing VXLAN from a Cumulus or ONYX switches. When you create a network on the Nutanix tool, it will run a provisioning job for NEO to add a VXLAN, using a designated template.

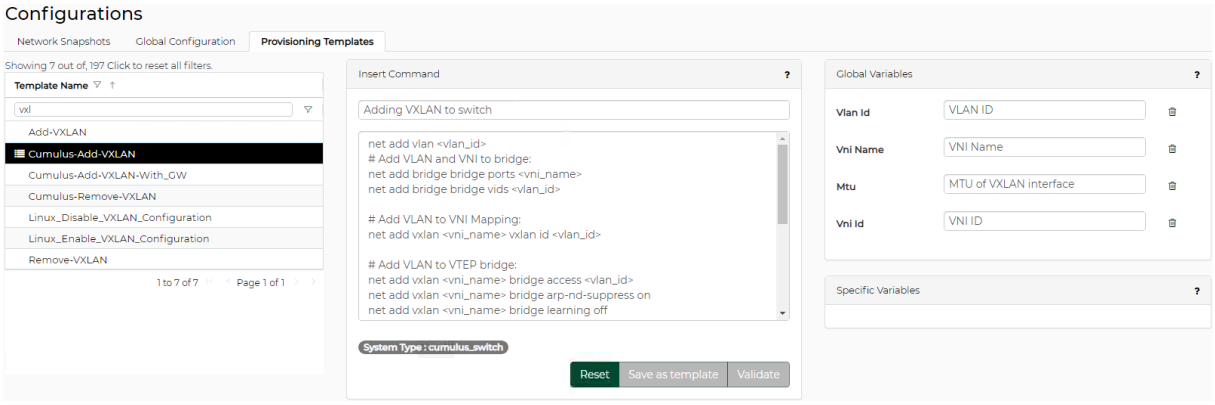
“Cumulus-Add-VXLAN” template:



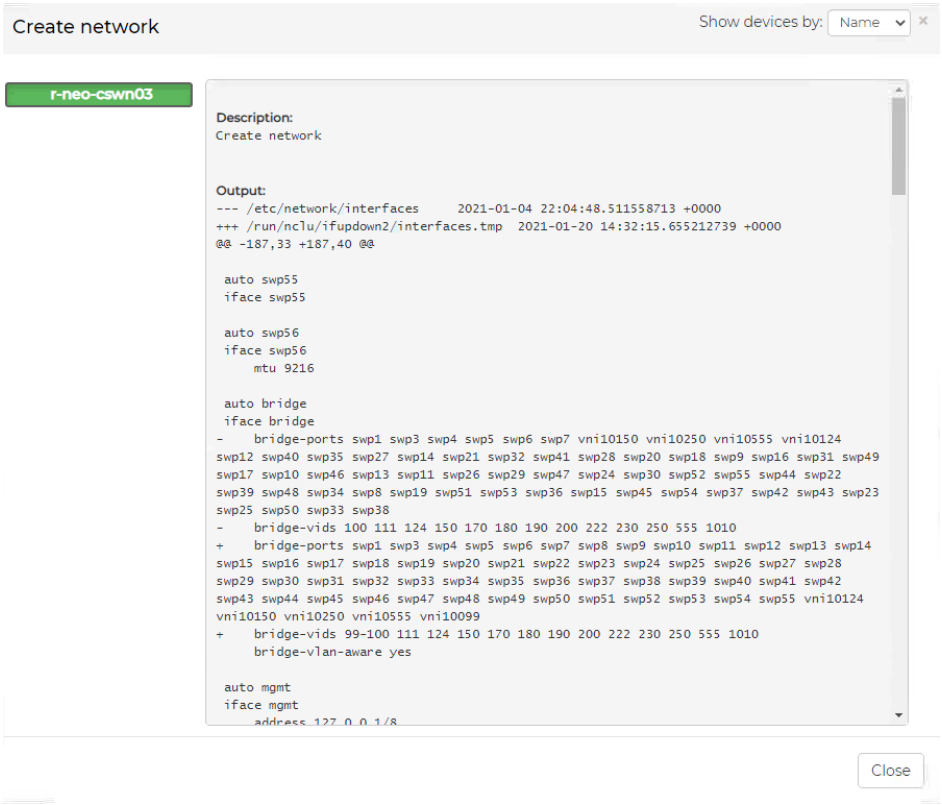
"**Cumulus**-Remove VXLAN" template:



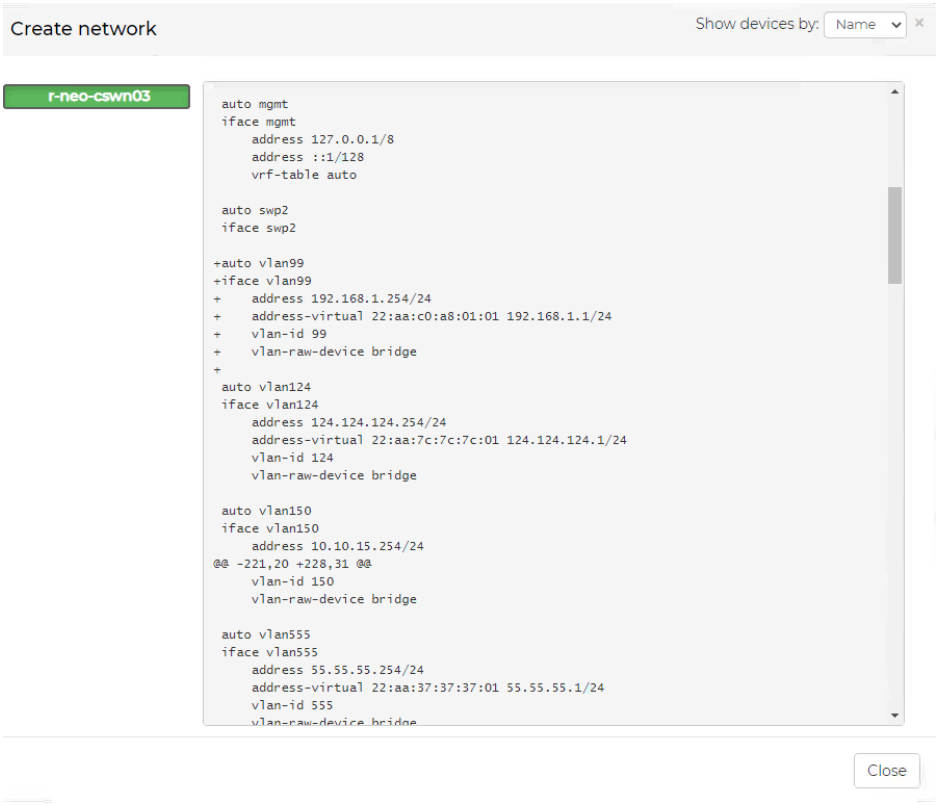
"Onyx-Add-VXLAN" template:

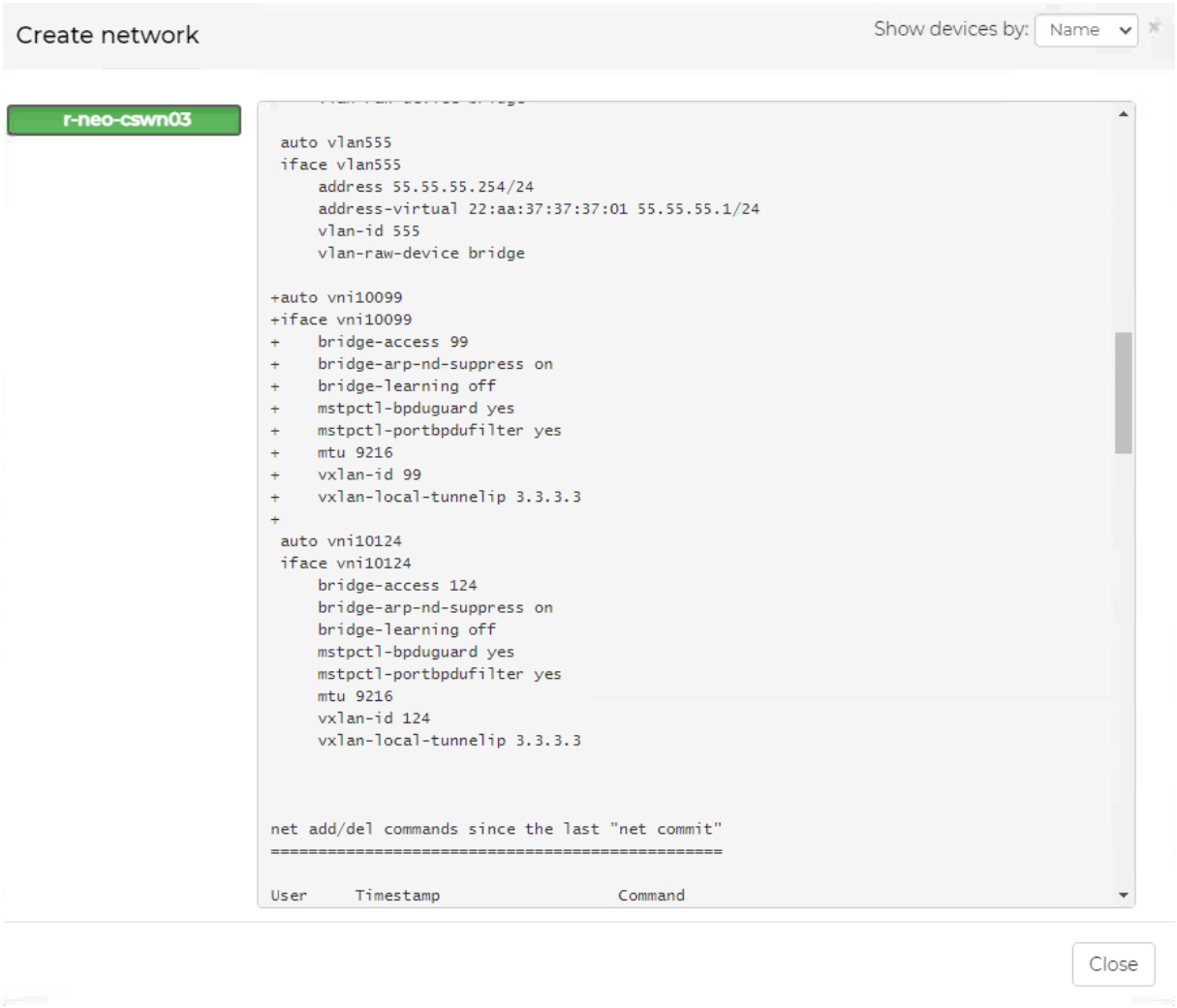


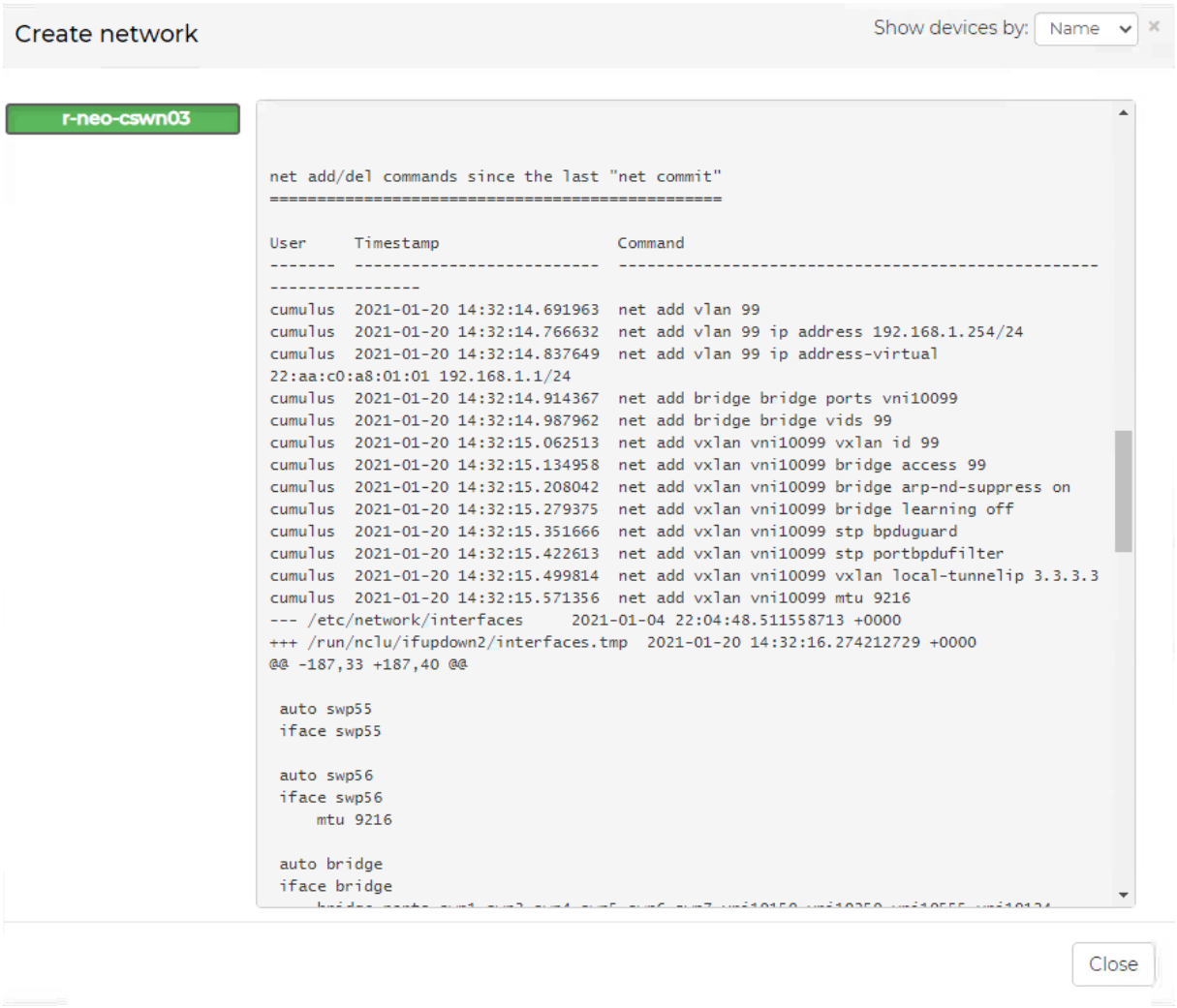
"Onyx-Remove-VXLAN" template:



VXLAN” template running results:




Create network
Show devices by:
Name
r-neo-cswn03
auto vlan555
iface vlan555
address 55.55.55.254/24
address-virtual 22:aa:37:37:37:01 55.55.55.1/24
vlan-id 555
vlan-raw-device bridge
+auto vni10099
+iface vni10099
+ bridge-access 99
+ bridge-arp-nd-suppress on
+ bridge-learning off
+ mstpctl-bpduguard yes
+ mstpctl-portbpdufilter yes
+ mtu 9216
+ vxlan-id 99
+ vxlan-local-tunnelip 3.3.3.3
+
auto vni10124
iface vni10124
bridge-access 124
bridge-arp-nd-suppress on
bridge-learning off
mstpctl-bpduguard yes
mstpctl-portbpdufilter yes
mtu 9216
vxlan-id 124
vxlan-local-tunnelip 3.3.3.3
net add/del commands since the last "net commit"
User Timestamp Command
Close


Create network
Show devices by: Name
r-neo-cswn03
net add/del commands since the last "net commit"
==========
User Timestamp Command
cumulus 2021-01-20 14:32:14.691963 net add vlan 99
cumulus 2021-01-20 14:32:14.766632 net add vlan 99 ip address 192.168.1.254/24
cumulus 2021-01-20 14:32:14.837649 net add vlan 99 ip address-virtual
22:aa:c0:a8:01:01 192.168.1.1/24
cumulus 2021-01-20 14:32:14.914367 net add bridge bridge ports vni10099
cumulus 2021-01-20 14:32:14.987962 net add bridge bridge vids 99
cumulus 2021-01-20 14:32:15.062513 net add vxlan vni10099 vxlan id 99
cumulus 2021-01-20 14:32:15.134958 net add vxlan vni10099 bridge access 99
cumulus 2021-01-20 14:32:15.208042 net add vxlan vni10099 bridge arp-nd-suppress on
cumulus 2021-01-20 14:32:15.279375 net add vxlan vni10099 bridge learning off
cumulus 2021-01-20 14:32:15.351666 net add vxlan vni10099 stp bpduguard
cumulus 2021-01-20 14:32:15.422613 net add vxlan vni10099 stp portbpdufilter
cumulus 2021-01-20 14:32:15.499814 net add vxlan vni10099 vxlan local-tunnelip 3.3.3.3
cumulus 2021-01-20 14:32:15.571356 net add vxlan vni10099 mtu 9216
--- /etc/network/interfaces 2021-01-04 22:04:48.511558713 +0000
+++ /run/nclu/ifupdown2/interfaces.tmp 2021-01-20 14:32:16.274212729 +0000
@@ -187,33 +187,40 @@
auto swp55
iface swp55
auto swp56
iface swp56
mtu 9216
auto bridge
iface bridge
Close

Create network

Show devices by: Name

r-neo-cswn03

```
 auto swp56
 iface swp56
     mtu 9216

 auto bridge
 iface bridge
-    bridge-ports swp1 swp3 swp4 swp5 swp6 swp7 vni10150 vni10250 vni10555 vni10124
swp12 swp40 swp35 swp27 swp14 swp21 swp32 swp41 swp28 swp20 swp18 swp9 swp16 swp31 swp49
swp17 swp10 swp46 swp13 swp11 swp26 swp29 swp47 swp24 swp30 swp52 swp55 swp44 swp22
swp39 swp48 swp34 swp8 swp19 swp51 swp53 swp36 swp15 swp45 swp54 swp37 swp42 swp43 swp23
swp25 swp50 swp33 swp38
-    bridge-vids 100 111 124 150 170 180 190 200 222 230 250 555 1010
+    bridge-ports swp1 swp3 swp4 swp5 swp6 swp7 swp8 swp9 swp10 swp11 swp12 swp13 swp14
swp15 swp16 swp17 swp18 swp19 swp20 swp21 swp22 swp23 swp24 swp25 swp26 swp27 swp28
swp29 swp30 swp31 swp32 swp33 swp34 swp35 swp36 swp37 swp38 swp39 swp40 swp41 swp42
swp43 swp44 swp45 swp46 swp47 swp48 swp49 swp50 swp51 swp52 swp53 swp54 swp55 vni10124
vni10150 vni10250 vni10555 vni10099
+    bridge-vids 99-100 111 124 150 170 180 190 200 222 230 250 555 1010
     bridge-vlan-aware yes

 auto mgmt
 iface mgmt
     address 127.0.0.1/8
     address ::1/128
     vrf-table auto

 auto swp2
 iface swp2

+auto vlan99
+iface vlan99
+    address 192.168.1.254/24
+    address-virtual 22:aa:c0:a8:01:01 192.168.1.1/24
+    vlan-id 99
+    vlan-raw-device bridge
+
```

Close

Create network

Show devices by: Name

r-neo-cswn03

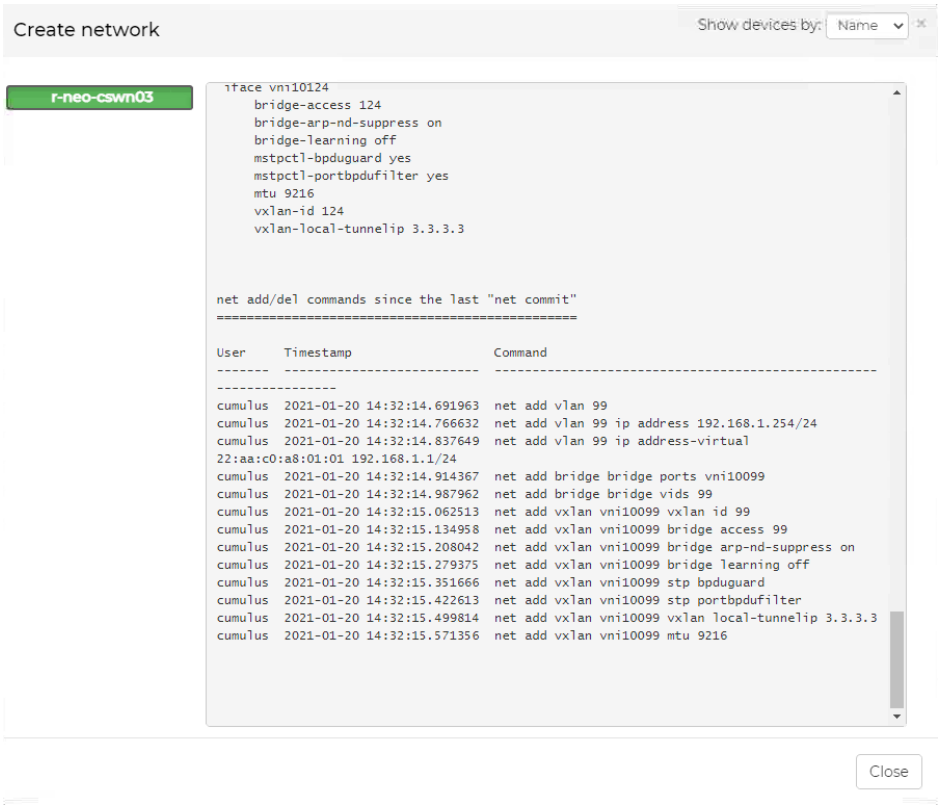
```
+auto vlan99
+iface vlan99
+    address 192.168.1.254/24
+    address-virtual 22:aa:c0:a8:01:01 192.168.1.1/24
+    vlan-id 99
+    vlan-raw-device bridge
+
 auto vlan124
 iface vlan124
     address 124.124.124.254/24
     address-virtual 22:aa:7c:7c:7c:01 124.124.124.1/24
     vlan-id 124
     vlan-raw-device bridge

 auto vlan150
 iface vlan150
     address 10.10.15.254/24
@@ -221,20 +228,31 @@
     vlan-id 150
     vlan-raw-device bridge

 auto vlan555
 iface vlan555
     address 55.55.55.254/24
     address-virtual 22:aa:37:37:37:01 55.55.55.1/24
     vlan-id 555
     vlan-raw-device bridge

+auto vni10099
+iface vni10099
+    bridge-access 99
+    bridge-arp-nd-suppress on
+    bridge-learning off
+    mstpctl-bpduguard yes
+    mstpctl-portbpdufilter yes
+    mtu 9216
```

Close



The network must be created on both Nutanix clusters with the same VLAN ID, subnet and gateway.

Examining the Connection

Once the networks on the Nutanix tool and the VMS are created, and a NIC is connecting between the network to the VMs, the VM on Cluster 1 must be able to ping the VM on Cluster 2:

```
root@localhost ~>ping 10.209.221.10
PING 10.209.221.10 (10.209.221.10) 56(84) bytes of data.
64 bytes from 10.209.221.10: icmp_seq=1 ttl=64 time=0.796 ms
64 bytes from 10.209.221.10: icmp_seq=2 ttl=64 time=0.218 ms
64 bytes from 10.209.221.10: icmp_seq=3 ttl=64 time=0.200 ms
64 bytes from 10.209.221.10: icmp_seq=4 ttl=64 time=0.260 ms
64 bytes from 10.209.221.10: icmp_seq=5 ttl=64 time=0.232 ms
64 bytes from 10.209.221.10: icmp_seq=6 ttl=64 time=0.338 ms
64 bytes from 10.209.221.10: icmp_seq=7 ttl=64 time=0.238 ms
```

Appendix – Events

Application Events

Event	Triggers	Permission Level	Default Severity	Category	Sub Category	Supported
Job completed with errors	All sub jobs were completed, but some of them failed	user	error	Application	Jobs	Yes
Job com-completed	All sub jobs were completed successfully	user	info	Application	Jobs	Yes
Device removed	Device removed	admin	Info	Application	General	Yes

Device Events

Event	Triggers	Permission Level	Default Severity	Category	Sub Category	Comments
ACL Dropped Packet	Access Control List	admin	Notice	Port	WJH	-
Layer 2 Dropped Packet	• Destination MAC is reserved (DMAC=01-80-C2-00-00-0x) • Ingress spanning tree filter • Ingress VLAN filtering • MLAG port isolation • Multicast egress port list is empty • Port loopback filter • Source MAC equals destination MAC • Source MAC is multicast • Unicast FDB action discard • VLAN tagging mismatch	admin	Notice	Port	WJH	-

Event	Triggers	Permission Level	Default Severity	Category	Sub Category	Comments
Layer 3 Dropped Packet	• Blackhole ARP/neighbor • Blackhole route • Checksum or IPver or IPv4 IHL too short • Destination IP is loopback address • Egress Router interface is disabled • Ingress Router interface is disabled • IPv4 destination IP is link local • IPv4 destination IP is local network (destination=0.0.0.0/8) • IPv4 LPM unicast miss • IPv4 source IP is limited broadcast • IPv6 destination in multicast scope FFx0:/16 • IPv6 destination in multicast scope FFx1:/16 • IPv6 LPM unicast miss • Multicast MAC mismatch • Non IP packet • Non-routable packet • Packet bigger than MTU • Router interface loopback • Source IP equals destination IP • Source IP is in class E • Source IP is loopback address Source IP is multicast • Source IP is unspecified • TTL is too small • Unicast destination IP but non-unicast destination MAC • Unresolved next-hop	admin	Notice	Part	WJH	-
Tunnel Dropped Packet	• Decapsulation error • Overlay switch:SMAC equals DMAC • Overlay switch:SMAC is multicast	admin	Notice	Port	WJH	-
General Fault	• Internal Bus Error trap Process Crash trap Process • Unexpected Exit trap • Unexpected Shutdown trap • Chip Down trap Module is unresponsive trap	admin	Warning	Device	General	triggers discovery refresh - modules
General Fault recovery	Module has been restored to its normal state trap	admin	Info	Device	General	triggers discovery refresh modules

Event	Triggers	Permission Level	Default Severity	Category	Sub Category	Comments
Power fault	• Insufficient Power trap Power Redundancy Mismatch trap • Low Power trap Power supply is unresponsive trap • Unit voltage is out of range trap	admin	Warning	Device	Power	triggers discovery refresh modules, power supplies
Power fault recovery	• Low Power Recover trap • Unit voltage is in range trap • Power supply has been restored to its normal state trap	admin	Info	Device	Power	triggers discovery refresh - power supplies
Fans fault	• Insufficient Fans trap Fan speed is below minimal range trap Fan is unresponsive trap • Fan is not present trap Insufficient number of working fans in the system trap	admin	Warning	Device	Fans	triggers discovery refresh modules, fans
Fans fault recovery	• Insufficient Fans Recover trap • Fan has been restored to its normal state trap The system currently has sufficient number of working fans trap	admin	Info	Device	Fans	triggers discovery refresh modules, fans
Temperature Fault	• Power supply temperature is too hot trap Chip Over Temperature Reset trap • Chip Over Temperature trap • Chip temperature is too hot trap • Temperature Sensor over threshold trap	admin	Warning	Device	Temperature	triggers discovery refresh temperature sensors
Temperature Fault recovery	• Power supply temperature is back to normal trap • Chip temperature is back to normal trap	admin	Info	Device	Temperature	triggers discovery refresh temperature sensors
High CPU Utilization	CPU Utilization High trap	admin	Warning	Device	CPU	-
Low Disk Space	Disk Space Low trap	admin	Warning	Device	Resources	-
IB SM state changed	IB SM up trap IB SM down trap IB SM restart trap	admin	Info	Device	Net-working	-
Link up	Link Up trap	admin	Info	Device	Net-working	triggers topology refresh
Link down	Link Down trap	admin	Warning	Device	Net-working	triggers topology refresh
Authentication Failure	Authentication Failure trap	admin	Warning	Device	Security	-
Test trap received	Test trap	admin	Info	Device	General	-

Event	Triggers	Permission Level	Default Severity	Category	Sub Category	Comments
Planned reload	Device has resumed after a planned reload operation	admin	Notice	Device	Reboot	-

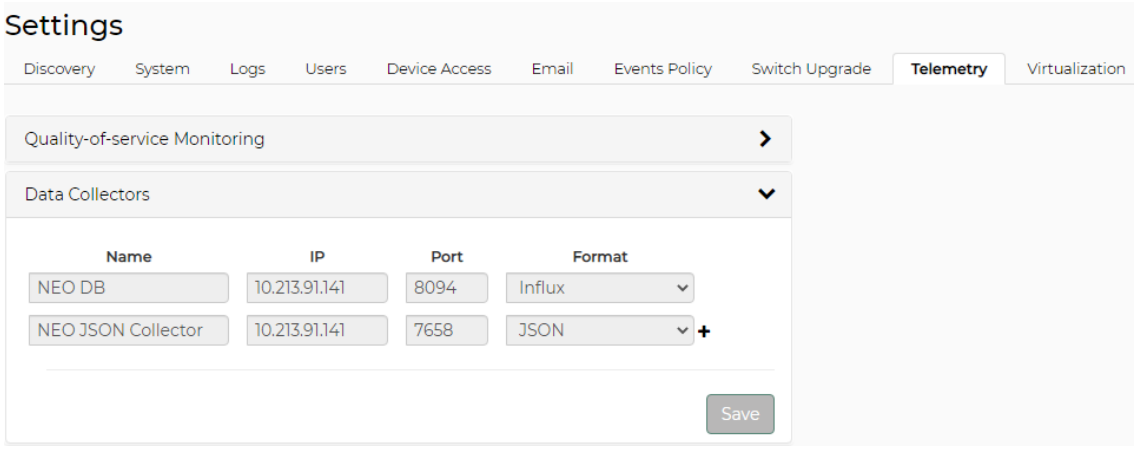
Appendix – Mellanox NEO GUI Fields Validations

Page	Field	Validation
Reports	Title	Alphanumeric + “_”, “-“ (4-20)
Users	UserName	Alphanumeric + “_”, “-“, “.” (4-20)
	Password	All characters except space (4-20)
Groups	Name	Alphanumeric + “_”, “-“ (4-20)
Credentials (HTTP)	UserName	Alphanumeric + “_”, “-“, “.” (1-20)
	Password	All characters except space (1-20) The password field can be left blank.
Credentials (SSH)	UserName	Alphanumeric + “_”, “-“, “.” (1-20)
	Password	All characters except space (1-20) The password field can be left blank.
Credentials (SNMP)	Read Community	All characters except space (1-20)
Credentials (SNMPV3)	UserName	All characters (1-20)
SMTP	Sender Name	Alphanumeric + “_”, space allowed (4-20)
	UserName	Alphanumeric + “_”, “.” (4-20)
	Password	All characters except space (4-20) The password field can be left blank.
	Email	A valid email address (exactly one “@” sign, and at least one “.” in the section following the “@”)
	Recipients	Valid Emails, comma separated
	Server	Valid Server Name - Valid Server IP
	Port	int 1-65535
Event Policy	Value	int 0-65535
	Description	All characters (1-1024)
SW Upgrade	Protocol	‘scp’ or ‘ftp’
	Server	Valid Server Name Regex Valid Server IP Regex
	Path	All characters (1-1024) must start with “/”
	Image	All characters (1-1024)
	UserName	Alphanumeric + “_”, “-“, “.” (1-20)
	Password	All characters except space (1-20)

Appendix – Activating Switch Telemetry Using Telemetry Agent

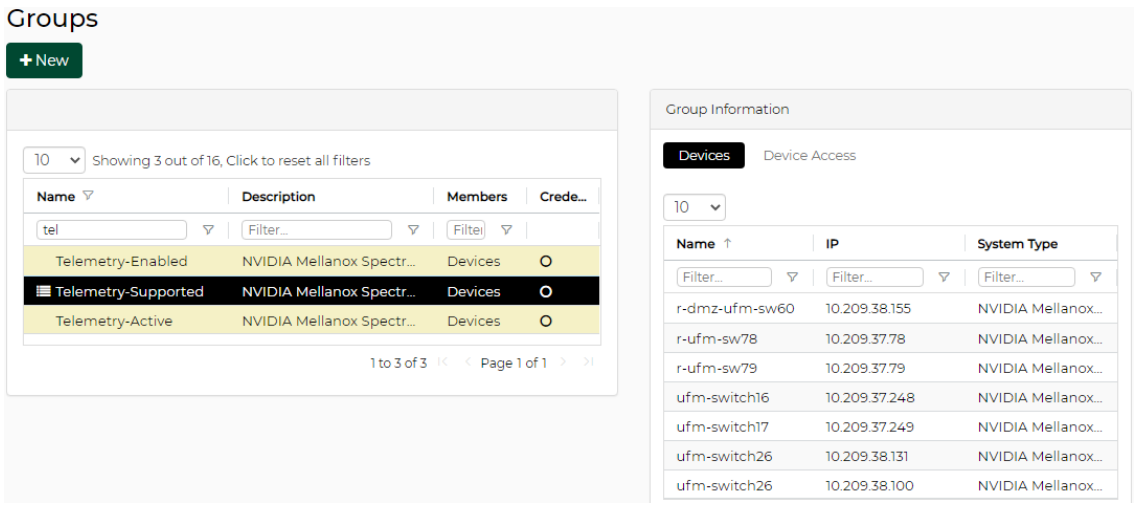
To use NVIDIA® Mellanox® NEO® as a controller for the telemetry agent, perform the following steps:

1. Go to Settings → Telemetry, and configure the Data Collector. The Data Collector is the server to which the telemetry agents send their data.

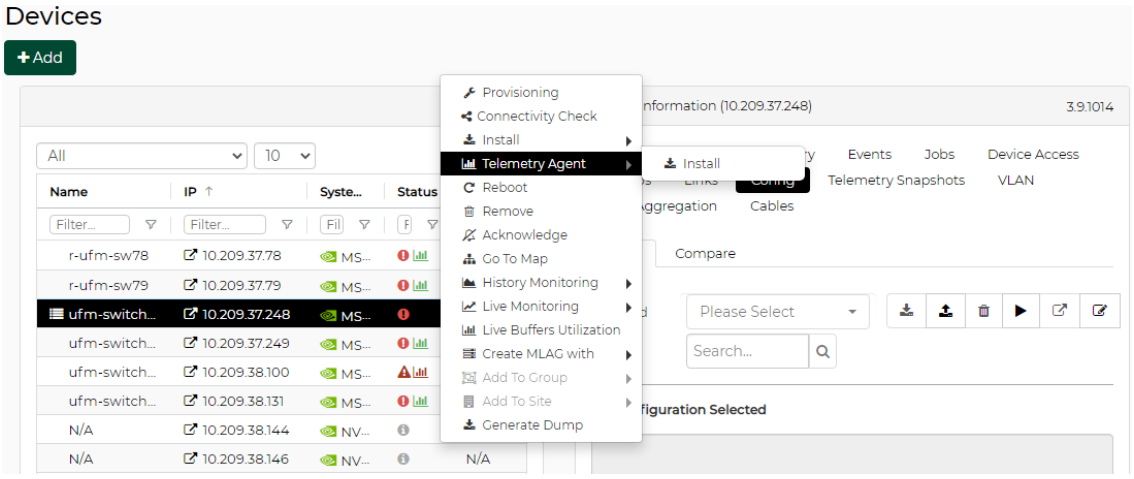


2. Go to the NEO Devices table, and select the switch on which you want to activate the telemetry agent.
   You can check the devices in a Telemetry-supported group, to see if the switch has Docker capability.

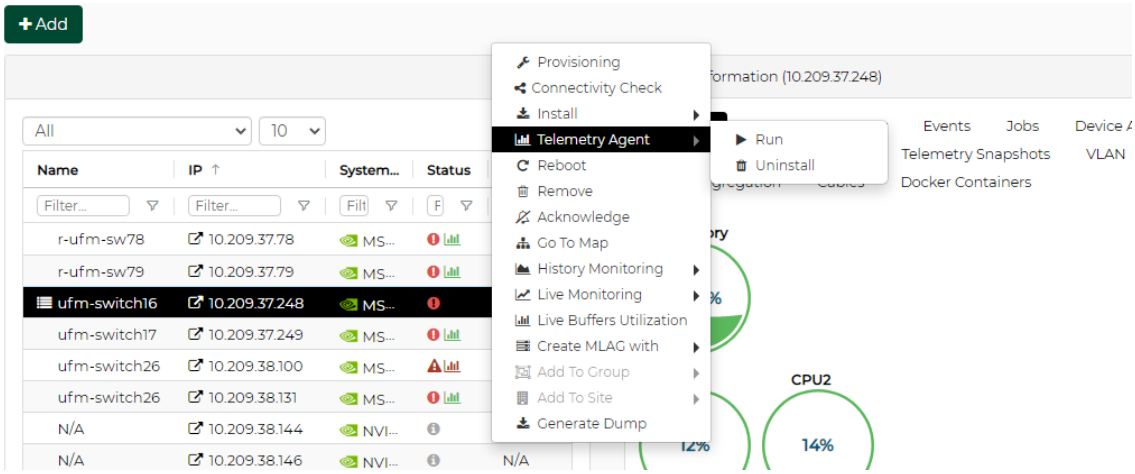
> ⚠ The selected switch must have Docker capabilities. You might need to update the OS version for Docker support.

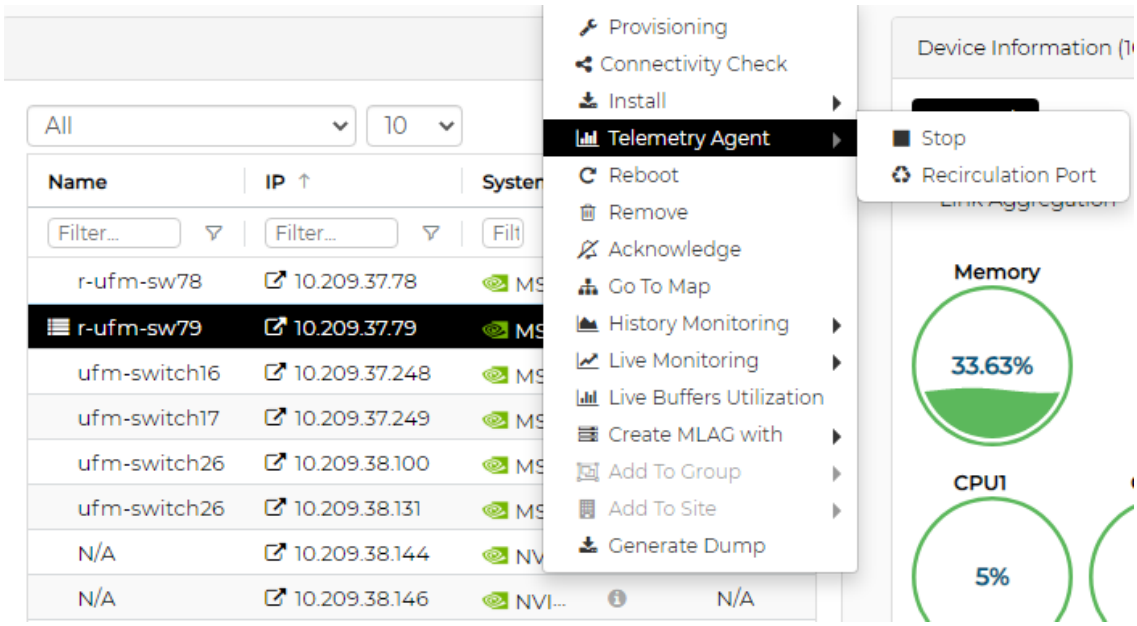


3. Right-click on the relevant device, and install the NEO telemetry agent.



4. Following a successful installation, the right-click menu for the device presents the new options set of "NEO Telemetry Agent", where you can stop/run the telemetry container, uninstall the telemetry agent or upgrade the telemetry agent if available.





Appendix – What Just Happened® Reasons

Category	Name	Description	Severity
Ethernet	Ingress Packet Reserved DMAC	Destination MAC is Reserved (DMAC=01-80-C2-00-00-0x)	Notice
Ethernet	Ingress Switch Vtag Allow	VLAN tagging mismatch	Notice
Ethernet	Ingress Switch VLAN	VLAN filtering	Notice
Ethernet	Ingress Switch STP	Ingress spanning tree filter	Notice
Ethernet	Lookup Switch UC	Unicast FDB discard	Notice
Ethernet	Lookup Switch MC Null	Multicast list is empty	Notice
Ethernet	Lookup Switch LB	Port loopback filter	Notice
Ethernet	Ingress Packet SMAC is MC	Source MAC is multicast	Notice
Ethernet	Ingress Packet SMAC Equals DMAC	Source MAC equals destination MAC	Notice
IP	Ingress Router No HDR	Non IP packet	Notice
IP	Ingress Router UC DIP MC DMAC	Unicast destination IP but non-unicast destination MAC	Notice
IP	Ingress Router DIP LB	Destination IP is loopback address	Notice
IP	Ingress Router SIP MC	Source IP is multicast	Notice
IP	Ingress Router SIP Class E	Source IP is in class E	Notice
IP	Ingress Router SIP LB	Source IP is loopback	Notice
IP	Ingress Router SIP Unspecified	Source IP is not specified	Notice
IP	Ingress Router IP HDR	Checksum or IPver or IPv4 IHL too short	Notice
IP	Ingress Router MC DMAC	Multicast MAC mismatch	Notice
IP	Ingress Router SIP Equals DIP	Source IP equals to destination IP	Notice
IP	Ingress Router SIP BC	IPv4 source IP is limited broadcast	Notice
IP	Ingress Router DIP Local Network	IPv4 destination IP is local network	Notice
IP	Ingress Router DIP Link Local	IPv4 destination IP is link local	Notice
IP	Router IRIF Disabled	Ingress IP interface is disabled	Notice
IP	Router ERIF Disabled	Egress IP interface is disabled	Notice
IP	Router LPM4	IPv4 LPM unicast miss	Notice
IP	Router LPM6	IPv6 LPM unicast miss	Notice
IP	MC Scope IPv6 0	IPv6 destination in multicast scope FFx0:/16	Notice
IP	MC Scope IPv6 1	IPv6 destination in multicast scope FFx1:/16	Notice
Tunnel	Decapsulation Packet	Remained packet is too short	Notice
Tunnel	Decapsulation Error	Decapsulation error	Notice
Tunnel	Overlay Switch SMAC Multicast	Overlay: source MAC is multicast	Notice
Tunnel	Overlay Switch SMAC Equals DMAC	Overlay: source MAC equals destination MAC	Notice

Document Revision History

Release	Date	Description
2.7	August 06, 2020	Added: • Section "Events" • Section "WJH Category Distribution" • Section "Services" • Section "Configuration Changes" • Section "WJH Filtering" • Section "Categories Distribution" • Section "Events Distribution Per Switch" • Section "Connectivity Check" • Section "Cables" Updated: • Section "Navigator Tabs" • Section "Monitoring Window" • Section "General Dashboard" • Section "Network Health"
2.6	May 26, 2020	Added: • Section "NEO Health Monitoring" • Section "Time-based WJH Events" • Section "Compare Configuration" • Section "Auto-Provisioning" • Section "Telemetry Agent Supported Counters Per Profile" Updated: • Section "Installation Prerequisites" • Section "Ports Used by Mellanox NEO Application" • Section "Installing NEO for High Availability" • Section "Installing Mellanox NEO as Docker Container" • Section "Sites" with Network Map view • Section "Uninstalling Mellanox NEO as Docker Container" • Note under Available Service Element Operations → Idle → Clean-up • Section "Adding Devices" • Section "Removing Devices" • Section "Tasks Tab" • Section "Built-in Tasks" • Section "Discovery" • Section "Backup and Restore" • Section "Modifying Management IP Address" • Section "Configuring Email Notifications According to Event Severity" • Section "Configuring Mellanox Onyx Switch for Sending Traps to Mellanox NEO" • Section “Configuring Host for LLDP Discovery” • Section "Setting NEO SNMP Trap Protocol Registration"

2.5	November 17, 2019	• Added the following sections:
		  • Built-in Tasks
		  • Setting NEO SNMP Trap Protocol Registration
		• Updated the following sections:
		  • Configuring Mellanox Onyx Switch for Sending Traps to Mellanox NEO
		  • Logs
		  • Local Mode

Release	Date	Description

	October 2, 2019	• Added two items to Known Issues section of Release Notes:
		  • Running WJH on a Cumulus switch is not supported. (Up to the release of NEO v2.5, no Cumulus version that supports WJH existed.)
		  • If a device (Linux host or switch) is removed from NEO while some Mellanox switches are running telemetry, then all the telemetry sessions running on these switches will be stopped.

	September 26, 2019	• Incorporated the Quick Start Guide document into the User Manual. • Added a new Element Operation (Clean-up) to table Available Service Elements' Operations • Added What-Just-Happened (WJH) Device Events. See Device Events • Added Prism AHV Configuration • Updated Virtualization Settings • Added What Just Happened Filtering • Added Uninstalling NEO as a Docker Container • Updated the Bring Up wizard screenshots due to a new look-and-feel interface. See Bring Up Wizard • Updated the Create a New Session section, updated the profiles list • Updated Mellanox NEO/Nutanix Prism Plug-in • Updated What Just Happened? • Updated NEO VXLAN Templates • Removed the switch limitation from section Limitations. • Removed section DCI Support from Mellanox NEO/Nutanix Prism Plug-in
2.4	April 30, 2019	Added the following sections: • Telemetry Snapshots • Virtualization Settings • Generate Dump • Bring-up Wizard and its subsections Updated the following sections: • “Main Tabs/Categories/Navigator Buttons” and its subsections • “Services” and its subsections • “Managed Elements” and its subsections • "Monitoring” • "Configuring Windows Host for Basic Authentication" • What Just Happened Overview • Network Map and its subsections • Updated the Network Notifications Icon screenshot: no eco mode
2.3.1	March 3, 2019	Updated the following section: • “Configuring Host for LLDP Discovery”
	January 31, 2019	No changes have been performed in this release

Release Notes Revision History

Release Notes Changes and Features History

This section lists the changes and new features of the previous versions of Mellanox NEO®.

Feature	Description
Rev 2.6	
Infrastructure	• Transition to Python 3 • Changing all UI tables to Grid Tables
Health monitoring	Added support for monitoring NEO processes and restarting them if they fail
Dashboard inventory	Display all managed devices inventory at NEO dashboard
Services	• Added clean-up option for MLAG service • Aligned all services to have the same look and feel like bringup wizard
Network map	Added support for viewing sites in Network Map screen
Auto-provisioning	• Automatically register for SNMP traps for every newly added Onyx switch • Automatically configure SNMP and LLDP for every newly added Cumulus switch
User management	Added support for limited view for NEO read only user
UI enhancements	• Added alternative to right click operations • Display switch names whenever switches are displayed • Aligned devices status and health for all managed devices • Aligned the format of all error handling messages
NEO container HA	Add support for NEO docker container to run in high availability mode
VLAN auto-provisioning	• Updating switch information (VLANs) once VLAN auto-provisioning is done • Added support for auto-VLAN provisioning according to the switchport mode detected • Configuring the VLAN name as part of the auto VLAN provisioning
Switch configuration comparison	Added option to compare configurations between two or more switches
Telemetry enhancements	• Added protection for users to not use localhost (127.0.0.1) if they are deploying telemetry agent • Added option to configure telemetry collectors via the telemetry streaming page
NEO container upgrade	Added support for upgrading NEO container using docker volumes
NEO discovery	Added pop-up indication and notification summary for every device being discovered (by scanning)
Events policy enhancement	Added 3 predefined recipient lists per severity for users who want to send all NEO events for specific severity to a specified list of recipients
Rev 2.5.1	
Telemetry Agent	Upgraded the Telemetry Agent to version 2.5.1-5
Telemetry Agent	Added provisioning templates to configure the Telemetry Agent via NEO

Telemetry Agent	Telemetry Agent LAG and MLAG discovery mechanism is now configurable and is disabled by default
NEO Discovery	Improved NEO switch interfaces discovery mechanism to be more efficient
WJH	The legend in WJH timeline graph is now displayed by reason category
Rev 2.5	
WJH Enhancements	Added support for collecting and viewing ACL dropped packets.
	Added support for collecting and viewing L1 dropped packets.
	Added support for filtering the WJH reasons categories when querying WJH from the switch.
Bring up wizard enhancements	Added support for multiple MLAGs configuration within the Bring Up wizard
	Added support for VMWare vCenter and Nutanix Prism integrations setting via the Bring Up wizard.
Auto VLAN Provisioning	Added support for automatic VLAN provisioning (on both Onyx and Cumulus switches) in case of networking or VM event, triggered by the vCenter.
	Added support for automatic VLAN provisioning over remote clusters (VXLAN) using Onyx switches connected to Nutanix AHV hypervisors.
	Added support for extending the amount of hypervisors in the Nutanix setup when working in “Global VLAN Provisioning” mode.
Transition to InfluxDB	Enabled collecting and inserting telemetry and monitoring data into InfluxDB (instead of Graphite).
RoCE Cleanup	Added support for removing RoCE configuration from switches which are part of NEO RoCE service.
NEO on Switch	Integrated the InfluxDB as part of NEO on Switch (NEO docker container) capability.
Enhanced Data collection	NEO was optimized to collect data from either Monitoring or Telemetry. Once Telemetry is enabled, Monitoring is disabled and vise versa.
Telemetry Agent	Performance improvements and more efficient way to collect telemetry data and stream it to external collector.
	Added support for upgrading the telemetry agent version via NEO Web UI.
	Added a mechanism which prevents the telemetry agent deployment in case the switch and NEO clocks are not synchronized.
	Added support for retrieving telemetry data for logical switch ports like LAG and MLAG.
	Added support for streaming telemetry data to Kafka Consumer.
	Added RAM limitation of 300M for the docker container running the telemetry agent.
	Added a new notification which lists the current switches that are using old telemetry agent version (which require upgrade).
Rev 2.4	
Snapshot Differences and Notifications/Events	Allows the user to create a telemetry snapshots of periodic CLI command output. These snapshots can be used to alert the user when a difference is found in the output.
gRPC Streaming Enhancements	Streams the Telemetry data to NEO using a unified collector with gRPC protocol.
Optimize NEO Refresh Rate	Shortens the refresh time of the device's Docker data.

Bring-up wizard for 2-switch MLAG for ESF	Allows the user to bring-up a network from scratch in a few quick steps.
VMware vCenter Virtualization Support (DVS)	Allows the user to manage ESXi hosts in NEO.
Generate System Dump	Allows the user to generate debug dumps for Onyx switches and upload them to a remote folder.
Support L2 in the ToR use-case	Nutanix integration for L2 networks.
Nutanix Calm BP update	Updated NEO Blueprint on Nutanix Calm.
Nutanix Plugin API Change to Webhook v3	Updated NEO Nutanix plugin to use Nutanix v3 REST APIs.
Package InfluxDB as an External Container with NEO	Provides a Docker container with InfluxDB and Grafana to be used as a Telemetry data collector.
Grafana Visualization Pack (on top of InfluxDB)	
What-Just-Happened (WJH) Debug	Provides the user more information on WJH failures.
Link Monitoring	Provides the user better visibility on the device and the ports' traffic, and the network behavior.
WJH integration with SDK	Integrated the Telemetry Agent with SDK for WJH data.
Onyx EVPN Templates	Added templates for EVPN configuration on Onyx.
WJH Enhancements	Enhanced the WJH dashboard user interface.
Telemetry	Added support for modifying the collectors to an existing session.
Power Management	Removed support for the eco mode as this capability is not supported in Spectrum based switches.
Rev 2.3.1	
Telemetry Agent	Telemetry sessions performance improvements
NEO Telemetry Management	Telemetry status reflection improvement
Discovery	Add option for disabling VLAN discovery
Task Management	Added an option to attach additional NEO data model attributes to the collected switch information
NEO VM Deployment	Improved the NEO OVA image for easier VM deployments
Rev 2.3	
RoCE Dashboard	The RoCE Dashboard contains a snapshot of the RoCE related network state, including information on service state, traffic and events. RoCE services can also be added and managed from this dashboard.
Nutanix Virtualization Improvements	Allows discovering the virtualization information (VM name) using prism central API.
Cisco Model 2960 Switches Support	Cisco switches model 2960 can be managed by NEO, apart from provisioning related operations.
What Just Happened	A dashboard that contains information about packet drops in the fabric.
MAC Address table for Onyx	Allows the Telemetry Agent to retrieve MAC Tables data.
Switch Agent (Onyx): Routing Tables	Allows the Telemetry Agent to retrieve Routing Tables data.
Telemetry Agent for SwitchDev (interface and port counters)	Allows running the telemetry agent as a docker container on SwitchDev switches. The data is collected using ethtool.
Telemetry Agent for Linux Host	Allows running the telemetry agent as a docker container on Linux hosts. The data is collected using ethtool.

LLDP Discovery APIAutomatic SNMP v3 Registration	Enables the user to attach the 'Register for SNMP v3 traps for Mellanox switch' built-in task to the ‘Device Added’ event so it will run every time a new device has been added.
Port Unsilenced Admin State	Added support for ‘Unlicensed’ port admin state.
Planned-Reload Event	Added a new event policy - ‘Planned Reload’.
MAC Address Table Scheduled Task	Allows the user to set a scheduled task to obtain the MAC address table for each Onyx device.
Rev 2.2	
Telemetry Agent Enhancements	• Added calculated counters (rate and normalized counters) • Added error handling and telemetry sessions status • Added support for multiple sessions and multiple destinations • Added a mechanism for triggering threshold crossing events
Telemetry Agent on Cumulus Linux	Added support for deploying and running telemetry agent on Cumulus Linux.
Telemetry Integration with ELK	Added support for switch telemetry data integration with ELK.
One Click RoCE	Added support for deploying RoCE on Windows and Cumulus Linux systems.
Network Map Enhancements	• Added support for link utilization (showing bandwidth utilization per link) • Added a new hierarchical view of managed devices
Log Debug level via Web UI	Added support for NEO controller log debug level.
Multi-site Support	Added support for grouping and managing devices per site
Network Path	Added a view of the optional network paths between a selected switch and a target host.
Nutanix Integration	Added support for NEO integration with Nutanix Prism Central and Multi-Cloud environment.
Rev 2.1	
One-click RoCE	• Updated the RoCE recipes for: 1. ECN only 2. ECN + QoS 3. ECN + QoS + PFC. • Added the ability to select specific switches, hosts and ports to RoCE provision. • Added the ability to easily grow the RoCE fabric after the initial provisioning with additional switches, hosts and ports.
Telemetry Agent (Early Availability)	The NEO telemetry agent is a software module designed to run inside a Docker container operated on a Mellanox Spectrum switch system. The agent collects data on the switch, and streams it out to an external data collector for processing, analysis and presentation. The telemetry agent can be centrally deployed and managed from the NEO application or from a 3rd party controller.
Mellanox Spectrum Containers Management	Added the ability to orchestrate Docker containers on Mellanox Spectrum switch systems operated with Mellanox Onyx software.
Cable Inventory	Added the ability to view and manage an inventory of cables across the fabric through one pane of glass.
NEO Docker Appliance	The NEO Docker appliance is a pre-packaged Docker container image operating on CentOS and installed with the NEO 2.1 software.
Backup & Restore	Added the ability to backup and restore a NEO instance for data protection and recovery purposes.

Event Management	• The condition ID was changed to be numeric instead of textual data • The event description contains the condition message instead of the reason • The reason field is generated by NEO, and contains Reason information per event ID. The user cannot modify the Reason information • The 'RelatedObjectID', 'RelatedObjectName' and 'RelatedObjectType' new attributes were added to each event • The 'Parent' attribute was changed to 'RelatedSystem'. Only one related system is supplied • The 'ConditionID' attribute was added • Additional log data entries were added - 'ConditionID', Event sequence ID and related object data • The corrective description is generated by NEO, and contains corrective information per condition ID
Remote Storage	Added the ability to change the default path where NEO stores all configuration files from the local host to a remote storage.
NEO-Host Notification	Added new notification listing hosts that are not installed with NEO-Host, as well as the ability to install the latest NEO-Host software.
Device Access	Added the ability to set http/https device access for every Mellanox Onyx operated device.
Export/Import Network Map Views	Added the ability to export Network Map views as files and import them to other NEO user environments.
QoS Monitoring	Added the ability to set traffic priority for monitoring, with priority 3 being the default for RoCE traffic.
Network Services	Added an option to automatically create a network snapshot before applying a service configuration to allow a restoration point in case of a failure.
Provisioning	Added several new provisioning templates.
Rev 2.0.5	
RoCE Profiles Support	Added the ability to use MLNX_OS 3.6.5000 traffic pool APIs for RoCE service configuration.
HTTPS Communication	Added the option to replace HTTP access to the switches with HTTPS access.
Configuration Management Module	Added a new module to consolidate all related configuration management functions, such as network provisioning templates, global configuration templates, etc. in a single pane of glass.
Running-Config Variables	Added the ability to use variables in running-config templates such that a single running-config can be provisioned on multiple switches in a single operation.
Network Snapshots	Added support for creating network-wide snapshot of switch running-configurations to use as restoration points. By default, a network snapshot is created automatically by the system every 24 hours.
One-click MLAG	Expanded the existing MLAG service to provision and validate IP networks and servers on the switch and host.
Nutanix AHV Support	Added support for auto-discovery and visibility of Nutanix Acropolis (AHV) virtual machines across the network fabric.
Linux Virtual Networking	Added modeling and visibility into a Linux host virtual networking and virtual functions bridging to physical adapters.
NEO Virtual Appliance for PowerKVM	Added support for new NEO Virtual Appliance compatible with PowerKVM based systems.

Device MAC	Added a new identifier for switch systems.
Device Access	Added SNMP-based connection settings per switch and changed “Device Credentials” to “Device Access”.
Syslog Server	Added configuration options to set up to five servers to export syslog messages to, each has its own service/port settings.
Live Monitoring Interval Improvement	Reduced the minimal counters monitoring interval of Spectrum and SwitchX devices from 20 to 2 seconds.
NMOS API	Added support for Networked Media Open Specifications (NMOS) API. For further information on NMOS, visit the following links: https://www.nmos.tv/about_NMI.html
Rev 1.9	
Enhanced Server/NIC Support	Added Mellanox adapter and port information through integration with NEO-Host software operated on the host.
Enhanced Device Discovery	Disabled the default automated device discovery mechanism, and enabled the user to create and manage a discovery policy of allowed IP subnets and/or ranges.
	Added a new discovery solution of IP subnet/range scan.
Configuration Management	Added the option to schedule a configuration swap/rollback on a Mellanox switch or a group of switches using an **Apply Config** task operation.
	Added the option to edit switch configuration through a built-in config editor.
One-Click RoCE Service	Added built-in automation for the provisioning and validation of RDMA over Converged Ethernet (RoCE). This feature is designed for Mellanox Spectrum switch systems operated with Mellanox Onyx, and Linux servers operated with Mellanox ConnectX-4 or ConnectX-5.
RoCE Monitoring	Added sampling of additional counters on Mellanox switches, used for RoCE traffic. This feature is designed for Mellanox Spectrum switch systems operated with Mellanox Onyx.
NEO Software Upgrade	Added an enhanced solution for NEO software upgrade from NEO v1.9 and up.
Enhanced Device State	Added the following new device states: • Pending Reboot – indicates that a device is pending reboot (as a result of a software upgrade or apply configuration) • Reboot Status – indicates the status of a device upon reboot operation
Enhanced LAG/MLAG Support	Added an enhanced support for LAG/MLAG port-channels on Mellanox Onyx powered switch systems with: • One-click provisioning – configuring LAG/MLAG ports configuration based on physical connectivity • LAG/MLAG information – added information on LAG/MLAG port members/peers, state, MTU, etc. • One-click validation – monitoring existing LAG/MLAG ports through network services
Rev 1.8	
Network Health Enhancements	Added new network health tests for: • IP connectivity between all nodes to all nodes, or random selection of one node per switch/rack. Multicast latency and bandwidth tests between all nodes to all nodes, or random selection of one node per switch/rack.

Network Health Report	Allows the user to execute data traffic tests across the network, to ensure utmost network performance
Task Sequence	Allows the user to select multiple tasks that will run in a sequence, to achieve end-to-end network automation in a single run-time
End to End RoCE Automation	Added a new wizard that configures Lossless RoCE/Resilient RoCE on an entire fabric comprised of Mellanox switches, Linux and Windows hosts
Ports Group	Enablse the user to create a group of ports, to achieve port-level network automation and create monitoring policies
Software Upgrade Profiles	Allows the user to manage software upgrade profiles for a more intuitive way to upgrade Mellanox software on switches and servers
VLAN Auto-Provisioning for Nutanix Acropolis Virtualization	Added network automation for configuring VLAN networks on Mellanox switches, for Nutanix Acropolis VM life-cycle, VM creation, VM migration and deletion. This is provided as a software add-on/plug-in.
Rev 1.7	
High Availability	Added the option to install and run NEO on a cluster of nodes that are synchronized and can take over each other in cases of failovers
Cable Information	Added the option to view cable information of selected devices, ports and groups
Performance Monitoring	Added the ability to run performance checks between two hosts
New Supported Virtual Appliances	Added new VM images of NEO for the following hypervisors: • VMWare Workstation • ESXI Server • Virtual-BOX • Hyper-V
Port Level Provision	Added the ability to run provisioning actions for Mellanox Onyx switch ports
L3 Network Provisioning	Added the option to define a dynamic layer 3 network configuration which can be automatically applied for new discovered systems
Syslog Configuration	Added the option to change NEO syslog configuration settings and filter for events to be written to Syslog
Support for 3rd Party Switches	Added support for managing HP and Brocade switches via monitoring and provisioning
Saving Topology Layouts	Added the option to save a user-defined layout of the discovered topology
Skin Personalization	Added the option to personalize the UI view of NEO in terms of colors and theme
Rev 1.6.1	
NEO Installation and Start-up Enhancements	Made various enhancements to the NEO installation process to make the installation experience easier for the user. These enhancements include: • An error message that appears once Python packages conflict with NEO packages during installation. • An error message that appears once RPM conflict with NEO packages during installation. • An error message that appears when trying to access NEO GUI while SELinux is enabled. This message asks for disabling SELinux to be able to access the GUI.
Mellanox Virtual Modular Switch (VMS)	Added support for configuring SN2410 and SN2700 switch systems as members in VMS.
Rev 1.6.0	

Enhanced Network Awareness	Presents VLAN and LAG configuration data per Mellanox switch on the fabric.
Virtualization Support	Enables NEO to automatically identify and extract data from Linux KVM hypervisos regarding virtual machines' properties and virtual switches. This data is presented to the user per device and on a fabric level.
Services View	Services View is a single pane of glass for initial network provisioning and monitoring. NEO services are used to provision complex configurations on multiple devices, and upon completion, constantly monitors these configurations. It includes an Out-of-the-box support for Virtual Modular Switch (VMS), Lossless Fabric, MLAG, and MTU services.
Live Monitoring	Enables the user to create graph reports on device and traffic counters with intensive polling rates, whenever real-time monitoring capabilities are needed.
Configuration Management	Enhanced configuration management with the following capabilities: • Provision new switches by pushing full device config • Rollback switch config to a last known good configuration • New global config repository to manage global device configurations
MLNX_OFED Software Upgrade	Added the option to upgrade MLNX_OFED software on Linux servers.
Maintenance Mode	Enables the user to set NEO to maintenance mode where all NEO events will be disabled.
Dashboard Enhancements	Added the option to create custom device heatmap views based on various types of attributes (CPU, memory, traffic, etc.), and user-defined thresholds.
Network Map Enhancements	Enhanced network map with the following capabilities: • Added filtering capabilities based on device type (switch, host, etc.), severity (warning, error, etc.) and VLAN number. • Enhanced search capabilities to use standard strings.
Mellanox Care Support	Enables Mellanox NEO customers to subscribe to Mellanox Care support service, where all configured events/alerts will be relayed to the Mellanox Care support team constantly.
Logs	Added the option to download log files.
Kerberos Authentication	Added support for Kerberos authentication for Windows hosts management.
Rev 1.5	
Topology Map	Added a visual view of the physical connectivity between managed devices.
VMS Configuration	Added a wizard for Virtual Modular Switch™ (VMS) configuration.
Provisioning of 3rd Party Switches	Added the option to provision configurations to 3rd party switches using templates.
Traffic Monitoring of 3rd Party Switches	Added the option to monitor traffic counters for 3rd party switches using SNMP protocol.
NEO SDK Enhancement	Added support for additional SDK scripts for NEO integrations.
Task Management Enhancement	Enhanced performance of task management and task editing.
RH7.0 Support	Added the option to install NEO on an RH7.0 system.
VM Deployment	Added a pre-configured Virtual Machine (VM) image with NEO for deploying it on a Linux KVM hypervisor system.

Bug Fixes History

Below are the fixes that were made in previous releases.

Ref. #	Issue
2170410	**Description:** Configuration restore after upgrade failed, causing the upgrade procedure not to work properly.
	Keywords: Upgrade procedure
	Discovered in version: 2.5.1
	Fixed in version: 2.6
2022521	**Description:** RoCE errors appear when RoCE is disabled in the switch.
	Keywords: RoCE; errors
	Discovered in version: 2.5.1
	Fixed in version: 2.6
1971770	**Description:** It is not possible to access NEO due to high CPU utilization.
	Keywords: CPU
	Discovered in version: 2.5
	Fixed in version: 2.6
2037732	**Description:** Port MTU is presented with the wrong value (-1).
	Keywords: MTU
	Discovered in version: 2.5.1
	Fixed in version: 2.6
2037729	**Description:** Interface utilization appears as 104% but packet drops occur in interface.
	Keywords: Utilization, packet drop
	Discovered in version: 2.5.1
	Fixed in version: 2.6
1992679	**Description:** In NEO virtualization, the user field for VCenter is character-limited.
	Keywords: Virtualization
	Discovered in version: 2.5.1
	Fixed in version: 2.6
1922607	**Description:** Fixed the issue that resulted in all running telemetry sessions on the switches to be removed when removed a system (which was not running telemetry) from NEO.
	Keywords: Telemetry Agent
	Discovered in Release: 2.5
	Fixed in Release: 2.5.1
1960703	**Description:** Fixed the NEO WJH purging mechanism (cleanup of old WJH events).
	Keywords: WJH
	Discovered in Release: 2.5
	Fixed in Release: 2.5.1

Ref. #	Issue
1973761	**Description:** Fixed the generation of several WJH reasons and enabled their exposure via the NEO WJH dashboard.
	Keywords: WJH
	Discovered in Release: 2.5
	Fixed in Release: 2.5.1
1958795	**Description:** Fixed an issue in the Telemetry Agent that caused the Agent to crash when splitting ports.
	Keywords: Telemetry Agent
	Discovered in Release: 2.5
	Fixed in Release: 2.5.1
1957584	**Description:** Fixed the log rotate mechanism for the Nutanix Plugin.
	Keywords: Log Rotate Mechanism
	Discovered in Release: 2.5
	Fixed in Release: 2.5.1
1959451	**Description:** Fixed issue in "NEO on Switch" that caused NEO providers status to appear offline.
	Keywords: NEO providers
	Discovered in Release: 2.5
	Fixed in Release: 2.5.1
1731941	**Description:** Moved UFM REST requests to use secure transport protocol (from HTTP to HTTPS). ⚠ To use the HTTP protocol, set supplier_protocol = http in the IB provider configuration file.
	Keywords: UFM, CloudX, HTTP, HTTPS
	Discovered in Release: 2.3.1
	Fixed in Release: 2.4
-	**Description:** Fixed a memory leak on NEO telemetry agent which occurred during telemetry sessions (WJH and Counters sessions).
	Keywords: Memory Leak, Telemetry Agent
	Discovered in Release: 2.3.0
	Fixed in Release: 2.3.1
1640823	**Description:** Fixed an issue where NEO CloudX API failed to connect UFM during a stress test.
	Keywords: CloudX, Stress Test
	Discovered in Release: 2.1.0-5
	Fixed in Release: 2.3.1
1593466	**Description:** Fixed an issue where NEO discovery failed to operate when the Fan Status was 'NOT PRESENT'
	Keywords: Fan Status
	Discovered in Release: 2.3.0
	Fixed in Release: 2.3.1

Ref. #	Issue
1370061	**Description:** Fixed an issue in VLAN mode, where NEO reported a switch port as an access port instead of a hybrid port in case of a hybrid port with “only one VLAN”.
	Keywords: VLAN Mode
	Discovered in Release: 2.1
	Fixed in Release: 2.2
1281752	**Description**: Fixed "*GraphiteSupplier: Failed to get response*" error (a workaround for versions prior to 2.1.0 can be found here).
	Keywords: GraphiteSupplier
	Discovered in Release: 2.0.5
	Fixed in Release: 2.1.0
1296798	**Description**: Fixed an issue where the Static IP was lost following a reboot of NEO OVA image.
	Keywords: Static IP, OVA
	Discovered in Release: 2.0.5
	Fixed in Release: 2.1.0
1321485	**Description**: Fixed an issue where Live Monitoring failed on split ports.
	Keywords: Split ports
	Discovered in Release: 2.0.5
1281714	**Description**: Fixed an issue where following switch upgrade, the new version was not displayed in the UI.
	Keywords: Switch upgrade
	Discovered in Release: 2.0.5
	Fixed in Release: 2.1.0
1321708	**Description**: Fixed an issue where the REST API sent a 'dummy' cookie as part of the response.
	Keywords: Cookies
	Discovered in Release: 2.0.5
	Fixed in Release: 2.1.0
777783	**Description**: Fixed an issue where the installation would exit with a vague error message. This issue occurred when NEO was installed using an installation package which was not compatible with the OS version.
	Keywords: Installation, OS version validation
	Discovered in Release: 1.6
	Fixed in Release: 1.6.1
777713	**Description**: Fixed the issue where a missing RPM (pyOpenSSL) in RedHat 7 used to cause NEO to crash during initialization.
	Keywords: RPM, initialization, RedHat 7
	Discovered in Release: 1.6
	Fixed in Release: 1.6.1

Notice

This document is provided for information purposes only and shall not be regarded as a warranty of a certain functionality, condition, or quality of a product. Neither NVIDIA Corporation nor any of its direct or indirect subsidiaries and affiliates (collectively: “NVIDIA”) make any representations or warranties, expressed or implied, as to the accuracy or completeness of the information contained in this document and assumes no responsibility for any errors contained herein. NVIDIA shall have no liability for the consequences or use of such information or for any infringement of patents or other rights of third parties that may result from its use. This document is not a commitment to develop, release, or deliver any Material (defined below), code, or functionality.

NVIDIA reserves the right to make corrections, modifications, enhancements, improvements, and any other changes to this document, at any time without notice. Customer should obtain the latest relevant information before placing orders and should verify that such information is current and complete.

NVIDIA products are sold subject to the NVIDIA standard terms and conditions of sale supplied at the time of order acknowledgement, unless otherwise agreed in an individual sales agreement signed by authorized representatives of NVIDIA and customer (“Terms of Sale”). NVIDIA hereby expressly objects to applying any customer general terms and conditions with regards to the purchase of the NVIDIA product referenced in this document. No contractual obligations are formed either directly or indirectly by this document.

NVIDIA products are not designed, authorized, or warranted to be suitable for use in medical, military, aircraft, space, or life support equipment, nor in applications where failure or malfunction of the NVIDIA product can reasonably be expected to result in personal injury, death, or property or environmental damage. NVIDIA accepts no liability for inclusion and/or use of NVIDIA products in such equipment or applications and therefore such inclusion and/or use is at customer’s own risk.

NVIDIA makes no representation or warranty that products based on this document will be suitable for any specified use. Testing of all parameters of each product is not necessarily performed by NVIDIA. It is customer’s sole responsibility to evaluate and determine the applicability of any information contained in this document, ensure the product is suitable and fit for the application planned by customer, and perform the necessary testing for the application in order to avoid a default of the application or the product. Weaknesses in customer’s product designs may affect the quality and reliability of the NVIDIA product and may result in additional or different conditions and/or requirements beyond those contained in this document. NVIDIA accepts no liability related to any default, damage, costs, or problem which may be based on or attributable to: (i) the use of the NVIDIA product in any manner that is contrary to this document or (ii) customer product designs.

No license, either expressed or implied, is granted under any NVIDIA patent right, copyright, or other NVIDIA intellectual property right under this document. Information published by NVIDIA regarding third-party products or services does not constitute a license from NVIDIA to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property rights of the third party, or a license from NVIDIA under the patents or other intellectual property rights of NVIDIA.

Reproduction of information in this document is permissible only if approved in advance by NVIDIA in writing, reproduced without alteration and in full compliance with all applicable export laws and regulations, and accompanied by all associated conditions, limitations, and notices.

THIS DOCUMENT AND ALL NVIDIA DESIGN SPECIFICATIONS, REFERENCE BOARDS, FILES, DRAWINGS, DIAGNOSTICS, LISTS, AND OTHER DOCUMENTS (TOGETHER AND SEPARATELY, “MATERIALS”) ARE BEING PROVIDED “AS IS.” NVIDIA MAKES NO WARRANTIES, EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE MATERIALS, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL NVIDIA BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF NVIDIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Notwithstanding any damages that customer might incur for any reason whatsoever, NVIDIA’s aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms of Sale for the product.

Trademarks

NVIDIA, the NVIDIA logo, and Mellanox are trademarks and/or registered trademarks of NVIDIA Corporation and/or Mellanox Technologies Ltd. in the U.S. and in other countries. Other company and product names may be trademarks of the respective companies with which they are associated.