Managed Elements

Table of contents

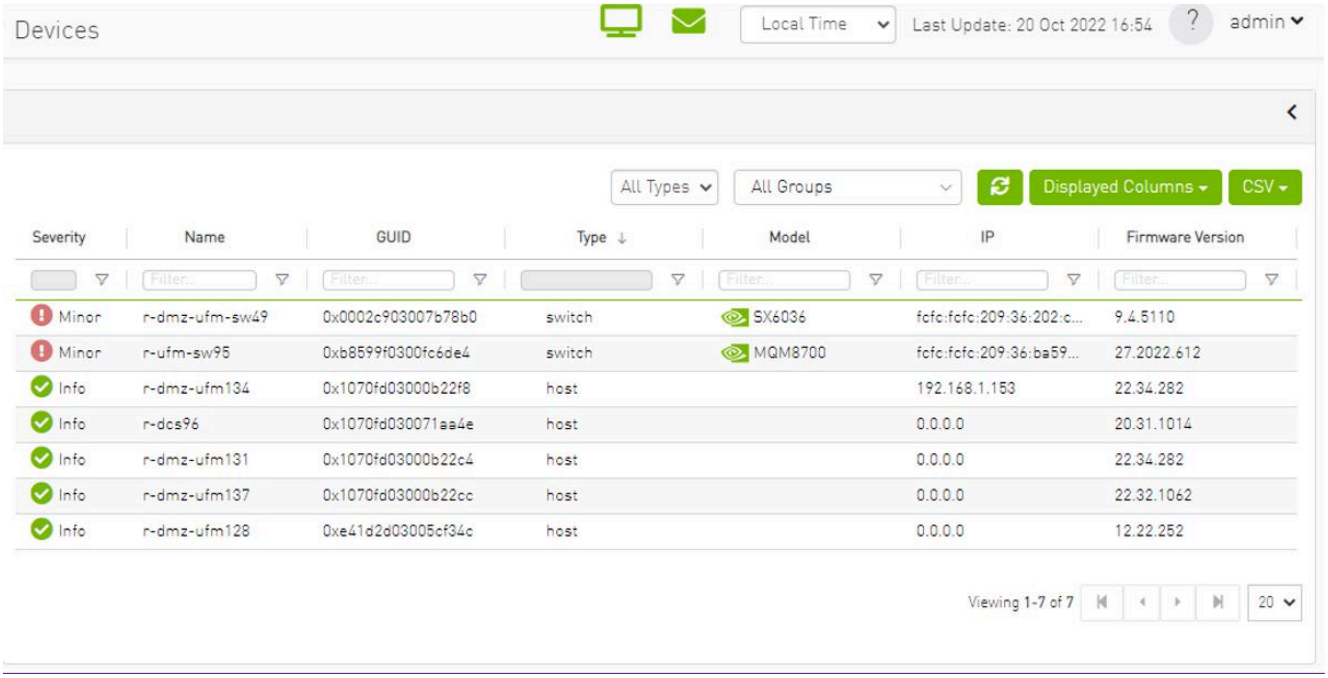
The UFM **Managed Elements** window allows you to obtain information on the fabric physical elements, such as devices, ports and cables.

> **Note**
>
> All information provided in a tabular format in UFM web UI can be exported into a CSV file.

- Devices Window
- Ports Window
- Virtual Ports Window
- Unhealthy Ports Window
- Cables Window
- Groups Window
- Inventory Window
- PKeys Window
- HCAs Window

Devices Window

The Devices window shows data pertaining to the physical devices in a tabular format.



Devices Window Data

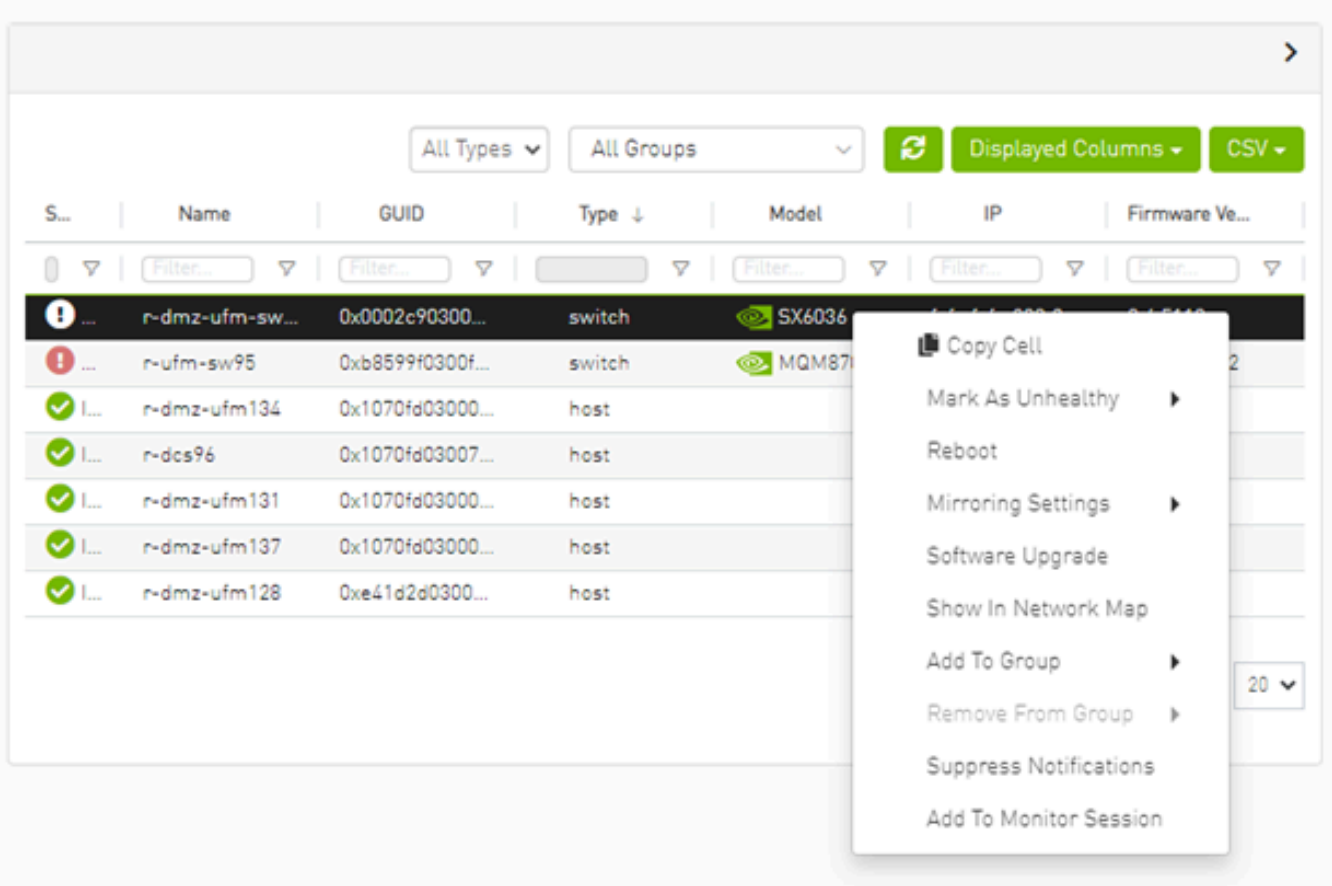
Data Type	Description
Health	Health of the device reflecting the highest alarm severity. Please refer to the Health States table.
Name	Name of the device **Note** If UFM Agent is running on a device, the following icon will appear next to the device name: images/download/thumbnails/2958633828/image2019-6-

Data Type	Description
	20_12-15-36-version-1-modificationdate-1719923428843-api-v2.png
GUID	System GUID of the device
Type	Type of the device: switch, node, IB router, and getaway
IP	IP address of the device
Vendor	The vendor of the device
Firmware Version	The firmware version installed on the device

Health States

Icon	Name	Description
	Normal	Information/notification displayed during normal operating state or a normal system event.
	Critical	Critical means that the operation of the system or a system component fails.
	Minor	Minor reflects a problem in the fabric with no failure.
	Warning	Warning reflects a low priority problem in the fabric with no failure. A warning is asserted when an event exceeds a predefined threshold.

A right-click on the device name displays a list of actions that can be performed on it.



Devices Actions

Action	Description
Firmware Upgrade	Perform a firmware upgrade on the selected device
Firmware Reset	Reboot the device. This action is only applicable to unmanaged hosts (servers).
Set Node Description	Configure a description to this node
Collect System Dump	Collect the system dump log for a specific device
Add to Group	Add the selected device to a devices group
Remove from Group	Remove the selected device from a devices group
Suppress Notifications	Suppress all event notifications for the device

Action	Description
Add to Monitor Session	Configure and activate host monitoring
Show in Network Map	Move to Zoom In tab in network map and add the selected device to filter list

Note

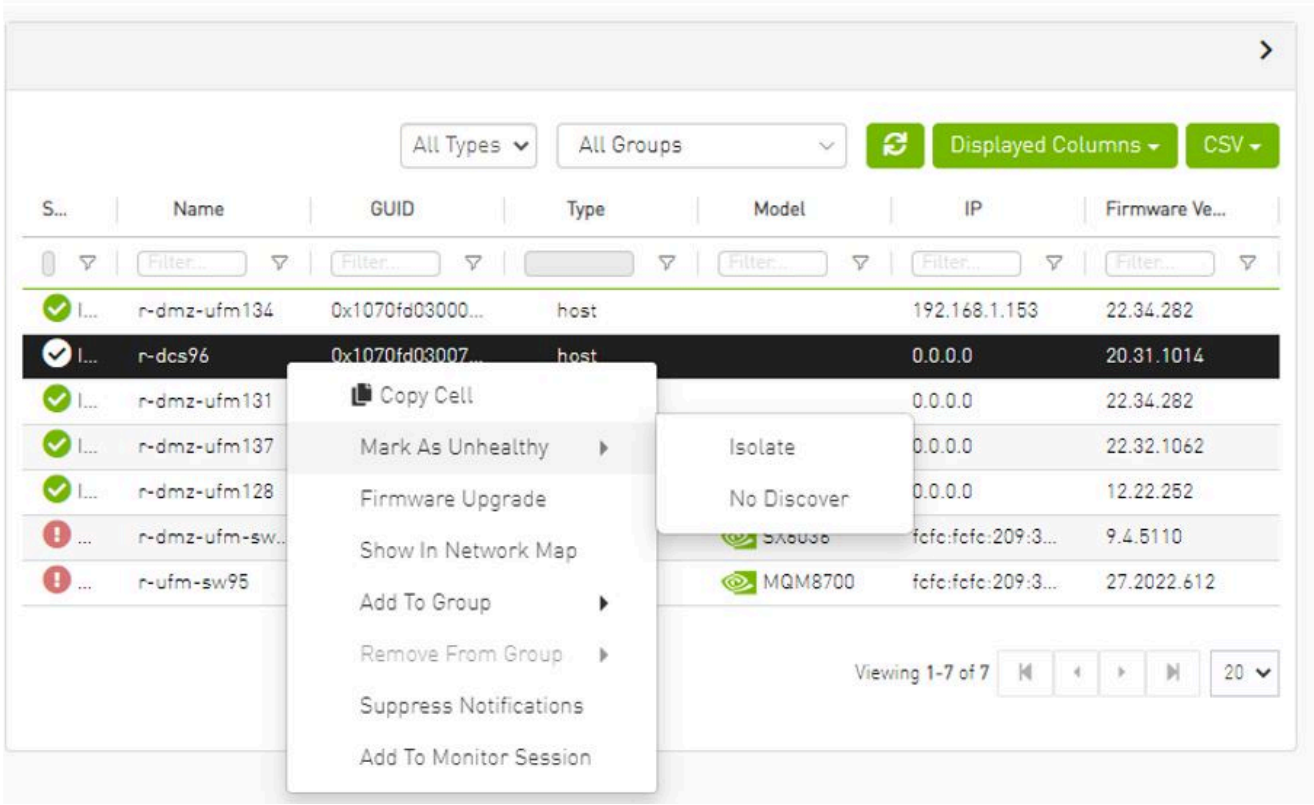
Collecting system dump for hosts, managed by UFM, is available only for hosts which are set with a valid IPv4 address and installed with MLNX_OFED.

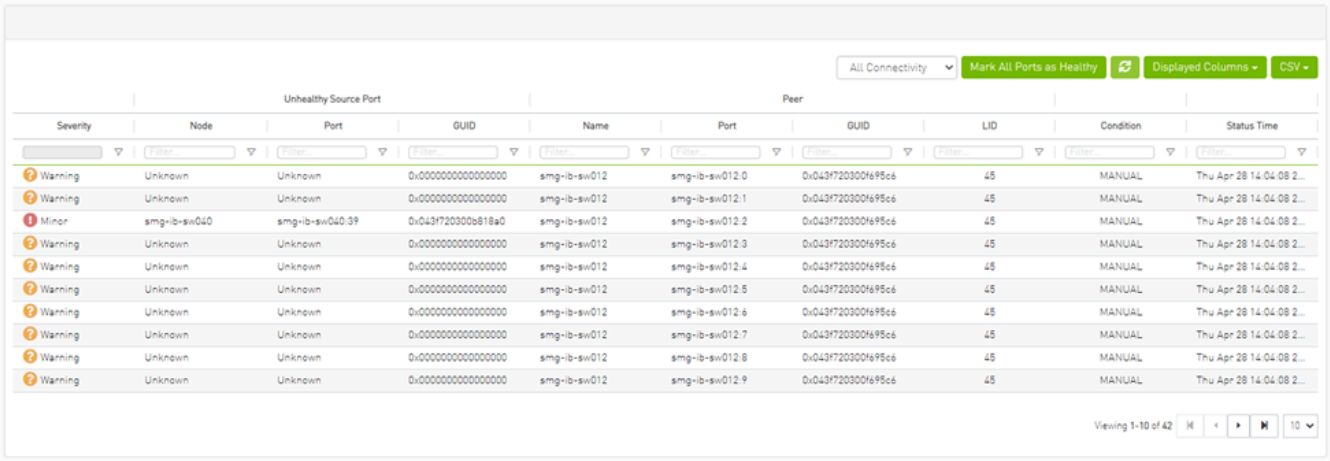
Mark Device as Unhealthy

From the Devices table, it is possible to mark devices as healthy or unhealthy using the context menu (right-click).

There are two options for marking a device as unhealthy:

- Isolate
- No Discover





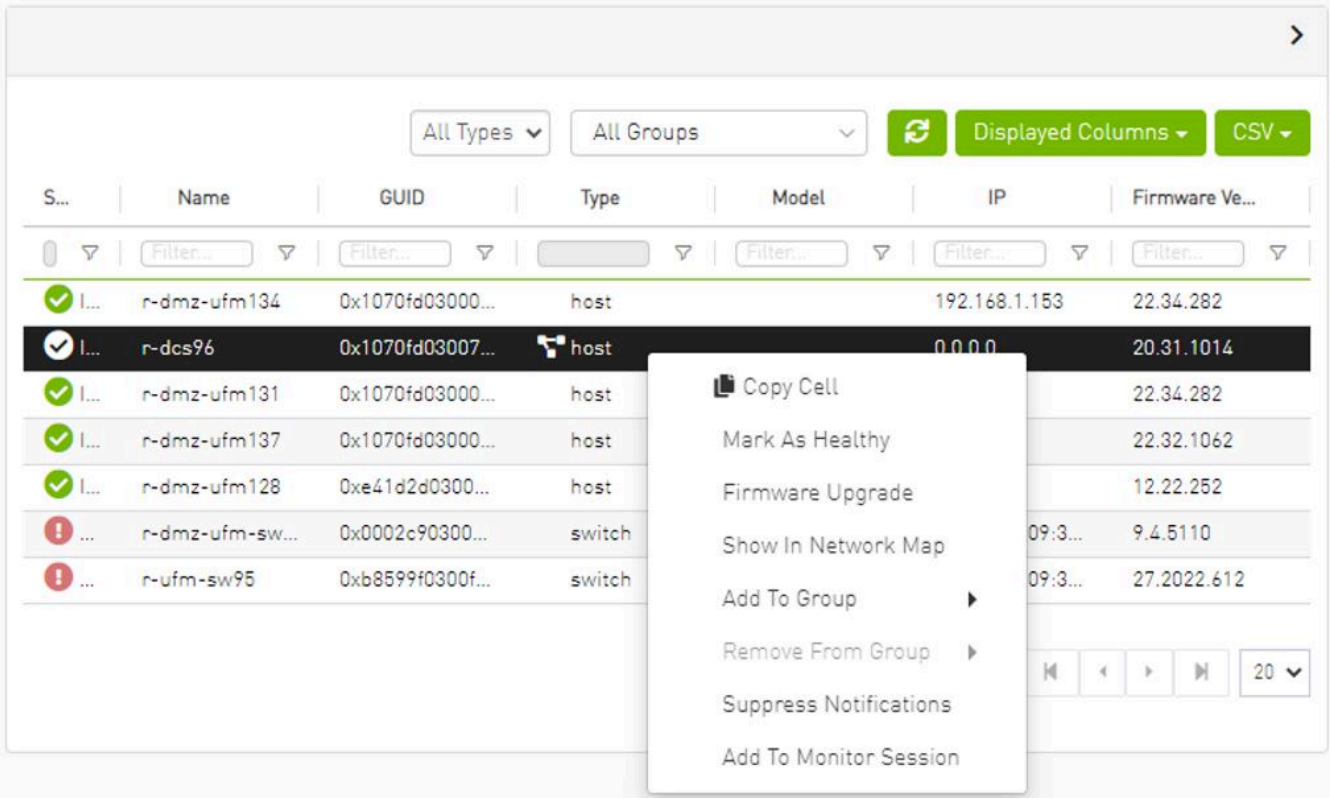
Server: conf/opensm/opensm-health-policy.conf content:

```
0xe41d2d030003e3b0 34 UNHEALTHY isolate
0xe41d2d030003e3b0 19 UNHEALTHY isolate
0xe41d2d030003e3b0 3 UNHEALTHY isolate
0xe41d2d030003e3b0 26 UNHEALTHY isolate
0xe41d2d030003e3b0 0 UNHEALTHY isolate
0xe41d2d030003e3b0 27 UNHEALTHY isolate
0xe41d2d030003e3b0 7 UNHEALTHY isolate
```

```
0xe41d2d030003e3b0 10 UNHEALTHY isolate
0xe41d2d030003e3b0 11 UNHEALTHY isolate
0xe41d2d030003e3b0 22 UNHEALTHY isolate
0xe41d2d030003e3b0 18 UNHEALTHY isolate
0xe41d2d030003e3b0 29 UNHEALTHY isolate
0xe41d2d030003e3b0 8 UNHEALTHY isolate
0xe41d2d030003e3b0 5 UNHEALTHY isolate
0xe41d2d030003e3b0 17 UNHEALTHY isolate
0xe41d2d030003e3b0 23 UNHEALTHY isolate
0xe41d2d030003e3b0 15 UNHEALTHY isolate
0xe41d2d030003e3b0 24 UNHEALTHY isolate
0xe41d2d030003e3b0 2 UNHEALTHY isolate
0xe41d2d030003e3b0 16 UNHEALTHY isolate
0xe41d2d030003e3b0 13 UNHEALTHY isolate
0xe41d2d030003e3b0 14 UNHEALTHY isolate
0xe41d2d030003e3b0 32 UNHEALTHY isolate
0xe41d2d030003e3b0 33 UNHEALTHY isolate
0xe41d2d030003e3b0 35 UNHEALTHY isolate
0xe41d2d030003e3b0 20 UNHEALTHY isolate
0xe41d2d030003e3b0 21 UNHEALTHY isolate
0xe41d2d030003e3b0 28 UNHEALTHY isolate
0xe41d2d030003e3b0 1 UNHEALTHY isolate
0xe41d2d030003e3b0 9 UNHEALTHY isolate
0xe41d2d030003e3b0 4 UNHEALTHY isolate
0xe41d2d030003e3b0 31 UNHEALTHY isolate
0xe41d2d030003e3b0 30 UNHEALTHY isolate
0xe41d2d030003e3b0 36 UNHEALTHY isolate
0xe41d2d030003e3b0 12 UNHEALTHY isolate
0xe41d2d030003e3b0 25 UNHEALTHY isolate
0xe41d2d030003e3b0 6 UNHEALTHY isolate
```

/opt/ufm/files/log/opensm-unhealthy-ports.dump content:

Mark Device as Healthy



Server /opt/ufm/files/conf/opensm/opensm-health-policy.conf content:

```
0xe41d2d030003e3b0 15 HEALTHY
0xe41d2d030003e3b0 25 HEALTHY
0xe41d2d030003e3b0 35 HEALTHY
0xe41d2d030003e3b0 0 HEALTHY
0xe41d2d030003e3b0 11 HEALTHY
0xe41d2d030003e3b0 21 HEALTHY
0xe41d2d030003e3b0 28 HEALTHY
0xe41d2d030003e3b0 7 HEALTHY
0xe41d2d030003e3b0 17 HEALTHY
0xe41d2d030003e3b0 14 HEALTHY
0xe41d2d030003e3b0 24 HEALTHY
0xe41d2d030003e3b0 34 HEALTHY
0xe41d2d030003e3b0 3 HEALTHY
0xe41d2d030003e3b0 10 HEALTHY
0xe41d2d030003e3b0 20 HEALTHY
0xe41d2d030003e3b0 31 HEALTHY
0xe41d2d030003e3b0 6 HEALTHY
0xe41d2d030003e3b0 16 HEALTHY
0xe41d2d030003e3b0 27 HEALTHY
0xe41d2d030003e3b0 2 HEALTHY
```

```
0xe41d2d030003e3b0 13 HEALTHY
0xe41d2d030003e3b0 23 HEALTHY
0xe41d2d030003e3b0 33 HEALTHY
0xe41d2d030003e3b0 30 HEALTHY
0xe41d2d030003e3b0 9 HEALTHY
0xe41d2d030003e3b0 19 HEALTHY
0xe41d2d030003e3b0 26 HEALTHY
0xe41d2d030003e3b0 36 HEALTHY
0xe41d2d030003e3b0 5 HEALTHY
0xe41d2d030003e3b0 12 HEALTHY
0xe41d2d030003e3b0 22 HEALTHY
0xe41d2d030003e3b0 32 HEALTHY
0xe41d2d030003e3b0 1 HEALTHY
0xe41d2d030003e3b0 8 HEALTHY
0xe41d2d030003e3b0 18 HEALTHY
0xe41d2d030003e3b0 29 HEALTHY
0xe41d2d030003e3b0 4 HEALTHY
```

/opt/ufm/files/log/opensm-unhealthy-ports.dump content:

```
# NodeGUID, PortNum, NodeDesc, PeerNodeGUID, PeerPortNum, PeerNodeDesc, {BadCond1, BadCond2, ...}, timestamp
```

Upgrading Software and Firmware for Hosts and Externally Managed Switches

Software/Firmware Upgrade via FTP

Software and firmware upgrade over FTP is enabled by the UFM Agent. UFM invokes the Software/Firmware Upgrade procedure locally on switches or on hosts. The procedure copies the new software/firmware file from the defined storage location and performs the operation on the device. UFM sends the set of attributes required for performing the software/firmware upgrade to the agent.

The attributes are:

- File Transfer Protocol – default FTP

    - The Software/Firmware upgrade on InfiniScale III ASIC-based switches supports FTP protocol for transmitting files to the local machine.
    - The Software/Firmware upgrade on InfiniScale IV-based switches and hosts supports TFTP and protocols for transmitting files to the local machine.
- IP address of file-storage server
- Path to the software/firmware image location

  The software/firmware image files should be placed according to the required structure under the defined image storage location. Please refer to section Devices Window.
- File-storage server access credentials (User/Password)

In-Band Firmware Upgrade

You can perform in-band firmware upgrades for externally managed switches and HCAs. This upgrade procedure does not require the UFM Agent or IP connectivity, but it does require current PSID recognition. Please refer to section PSID and Firmware Version In-Band Discovery. This feature requires that the Mellanox Firmware Toolkit (MFT), which is included in the UFM package, is installed on the UFM server. UFM uses flint from the MFT for in-band firmware burning.

Before upgrading, you must create the firmware repository on the UFM server under the directory /opt/ufm/files/userdata/fw/. The subdirectory should be created for each PSID and one firmware image should be placed under it. For example:

```
/opt/ufm/files/userdata/fw/
    MT_0D80110009
        fw-ConnectX2-rel-2_9_1000-MHQH29B-XTR_A1.bin
    MT_0F90110002
        fw-IS4-rel-7_4_2040-MIS5023Q_A1-A5.bin
```

Directory Structure for Software or Firmware Upgrade Over FTP

Before performing a software or firmware upgrade, you must create the following directory structure for the upgrade image. The path to the <ftp user home>/<path>/ directory should be specified in the upgrade dialog box.

```
<ftp user home>/<path>/
      InfiniScale3 - For anafa based switches Software/Firmware upgrade images
            voltaire_fw_images.tar – firmware image file
            ibswmpr-<s/w version>.tar – software image file
      InfiniScale4 - For InfiniScale IV based switches Software/Firmware upgrade images
            firmware_2036_4036.tar – Firmware image file
            upgrade_2036_4036.tgz – Software image file
      OFED /* For host SW upgrade*/
            OFED-<OS label>.tar.bz2
      <PSID>* – For host FW upgrade
            fw_update.img
```

The <PSID> value is extracted from the mstflint command:

```
mstflint -d <device> q
```

The device is extracted from the lspci command. For example:

```
# lspci
06:00.0 InfiniBand: Mellanox Technologies MT25208 InfiniHost III Ex
# mstflint -d 06:00.0 q | grep PSID
PSID: VLT0040010001
```

PSID and Firmware Version In-Band Discovery

The device PSID and device firmware version are required for in-band firmware upgrade and for the correct functioning of Subnet Manager plugins, such as Congestion Control

Manager and Lossy Configuration Management. For most devices, UFM discovers this information and displays it in the Device Properties pane. The PSID and the firmware version are discovered by the Vendor-specific MAD.

By default, the gv.cfg file value for event_plugin_option is set to (null). This means that the plugin is disabled and opensm does not send MADs to discover devices' PSID and FW version. Therefore, values for devices' PSID and FW version are taken from ibdiagnet output (section NODES_INFO).

The below is an example of the default value:

```
event_plugin_options = (null)
```

To enable the vendor-specific discovery by opemsm, in the gv.cfg configuration file, change the value of event_plugin_option to (--vendinfo –m 1), as shown below:

```
event_plugin_options = --vendinfo –m 1
```

If the value is set to –vendinfo –m 1, the data should be supplied by opensm, and in this case the ibdiagnet output is ignored.

> **Note**
>
> In some firmware versions, the information above is currently not available.

Switch Management IP Address Discovery

From NVIDIA switch FM version 27.2010.3942 and up, NVIDIA switches support switch management IP address discovery using MADs. This information can be retrieved as part of ibdiagnet run (ibdiagnet output), and assigned to discover switches in UFM.

There is an option to choose the IP address of which IP protocol version that is assigned to the switch: IPv4 or IPv6.

The discovered_switch_ip_protocol key, located in the gv.cfg file in section [FabricAnalysys], is set to 4 by default. This means that the IP address of type IPv4 is assigned to the switch as its management IP address. In case this value is set to 6, the IP address of type IPv6 is assigned to the switch as its management IP address.

After changing the discover_switch_ip_protocol value in gv.cfg, the UFM Main Model needs to be restarted for the update to take effect. The discovered IP addresses for switches are not persistent in UFM – every UFM Main Model restarts the values of management IP address which is assigned from the ibdiagnet output.

Upgrading Server Software

The ability to update the server software is applicable only for hosts (servers) with the UFM Agent.

To upgrade the software:

1. Select a device.
2. From the right-click menu, select Software Update.
3. Enter the parameters listed in the following table.

Parameter	Description
Protocol	Update is performed via FTP protocol
IP	Enter the host IP
Path	Enter the parent directory of the FTP directory structure for the Upgrade image. The path should not be an absolute path and should not contain the first slash (/) or trailer slash.
User	Name of the host username

Parameter	Description
Password	Enter the host password

4. Click Submit to save your changes.

Upgrading Firmware

You can upgrade firmware over FTP for hosts and switches that are running the UFM Agent, or you can perform an in-band upgrade for externally managed switches and HCAs.

Before you begin the upgrade ensure that the new firmware version is in the correct location. For more information, please refer to section In-Band Firmware Upgrade.

To upgrade the firmware:

1. Select a host or server.
2. From the right-click menu, select Firmware Upgrade.
3. Select protocol In Band.
4. For upgrade over FTP, enter the parameters listed in the following table.

Parameter	Description
IP	Enter device IP
Path	Enter the parent directory of the FTP directory structure for the Upgrade image. The path should not be an absolute path and should not contain the first slash (/) or trailer slash.
Username	Name of the host username

Parameter	Description
Password	Enter the host password

5. Click submit to save your changes.

> **Note**
>
> The firmware upgrade takes effect only after the host or externally managed switch is restarted.

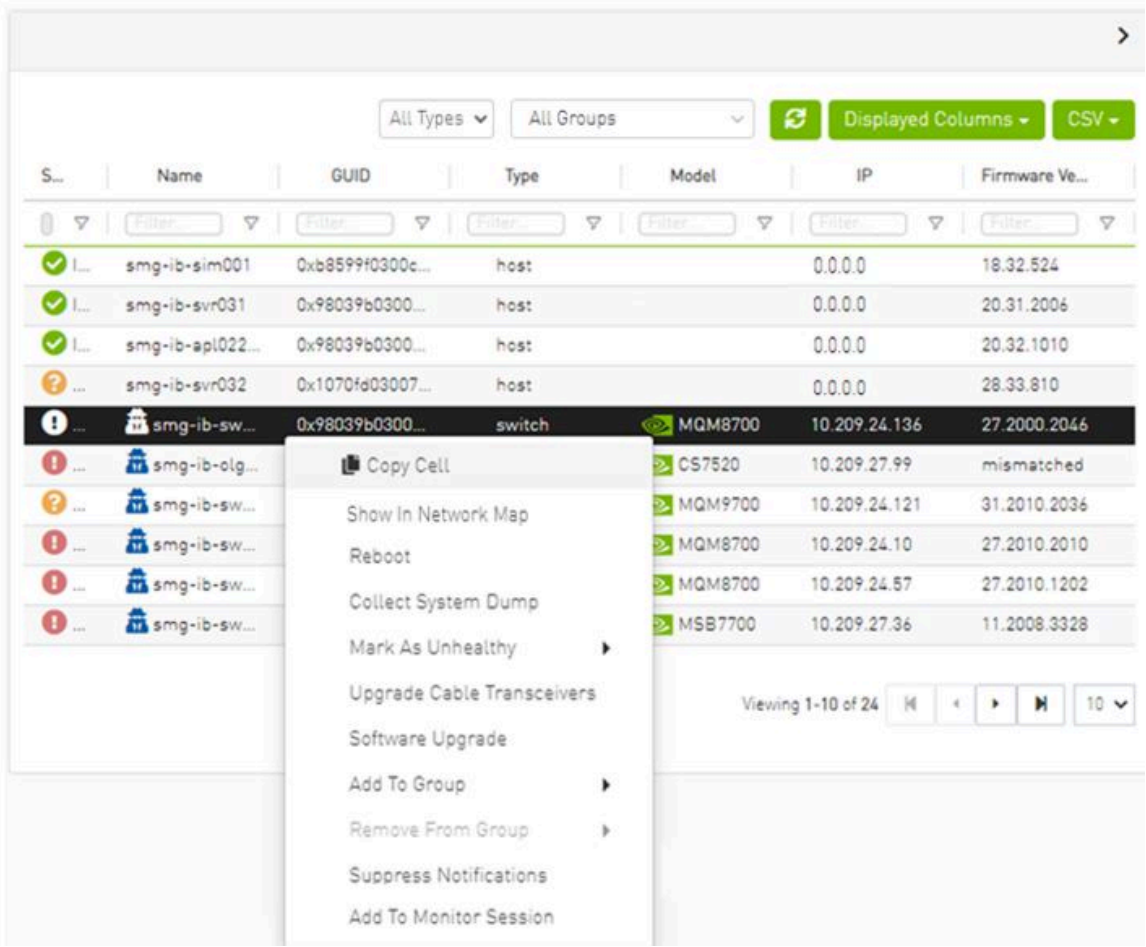
Upgrade Cables Transceivers Firmware Version

The main purpose of this feature is to add support for burning of multiple cables transceiver types on multiple devices using linkx tool which is part of flint. This needs to be done from both ends of the cable (switch and HCA/switch).

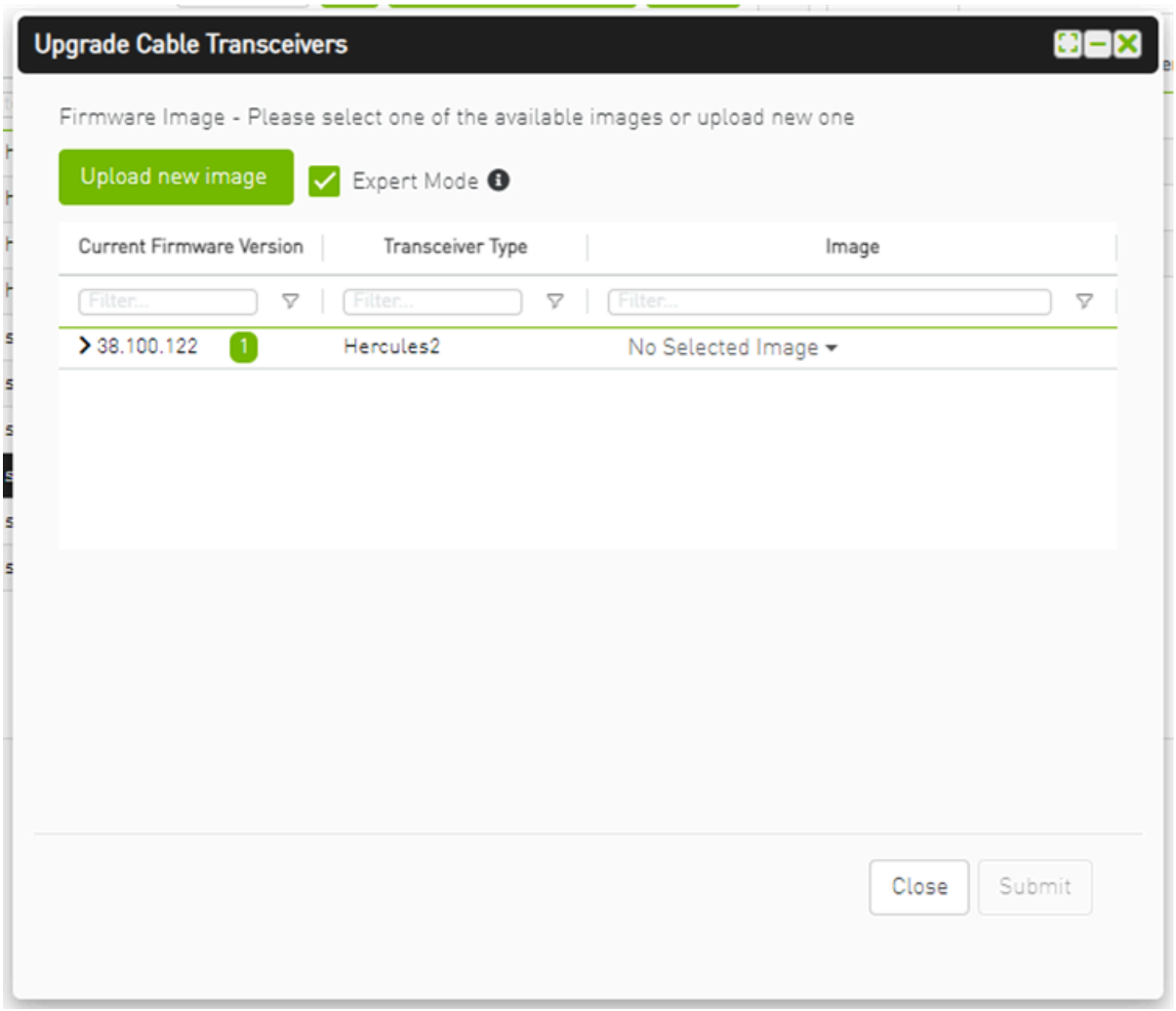
To upgrade cables transceivers FW version:

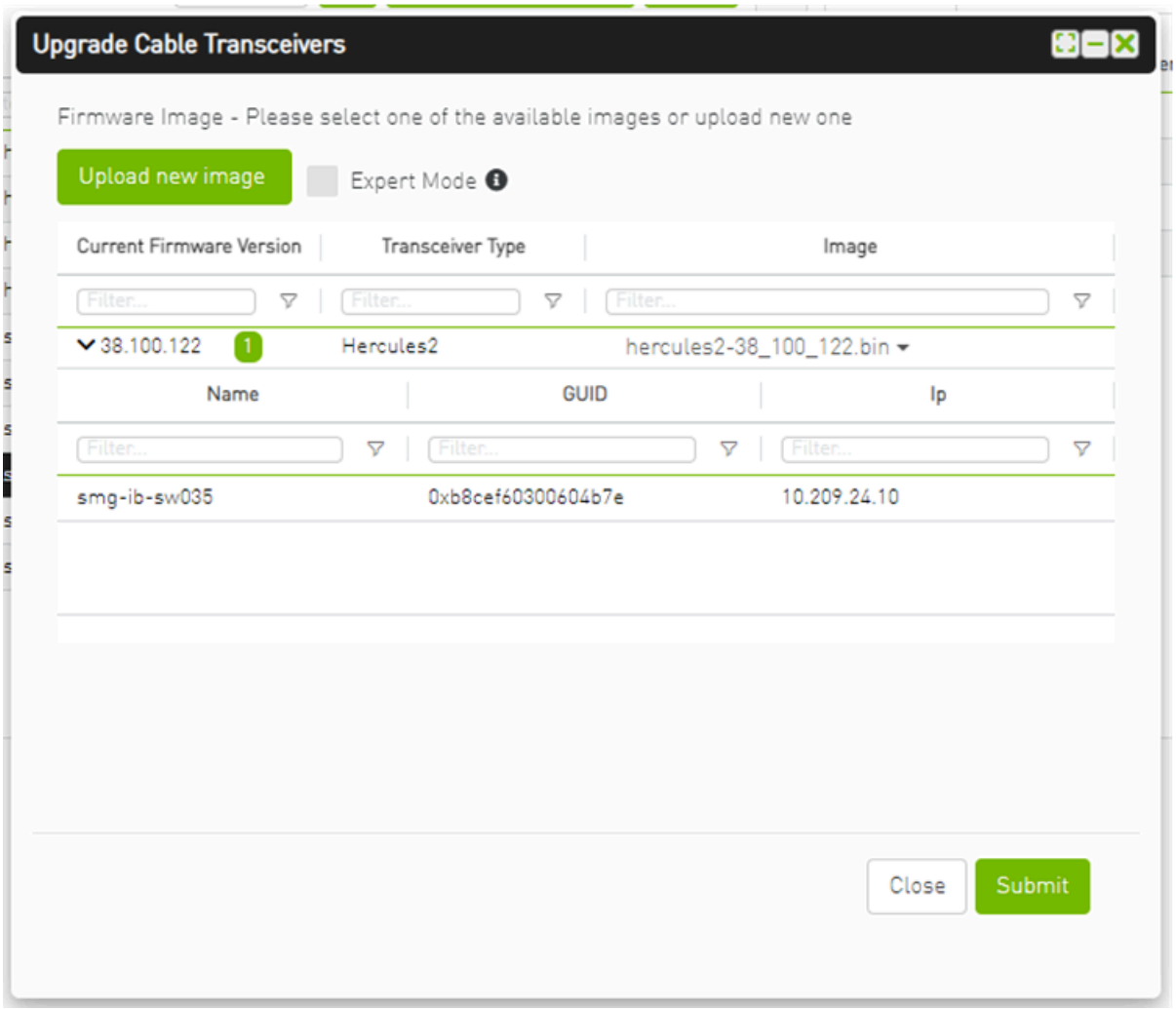
1. Navigate to managed elements page

2. select the target switches and click on Upgrade Cable Transceivers option

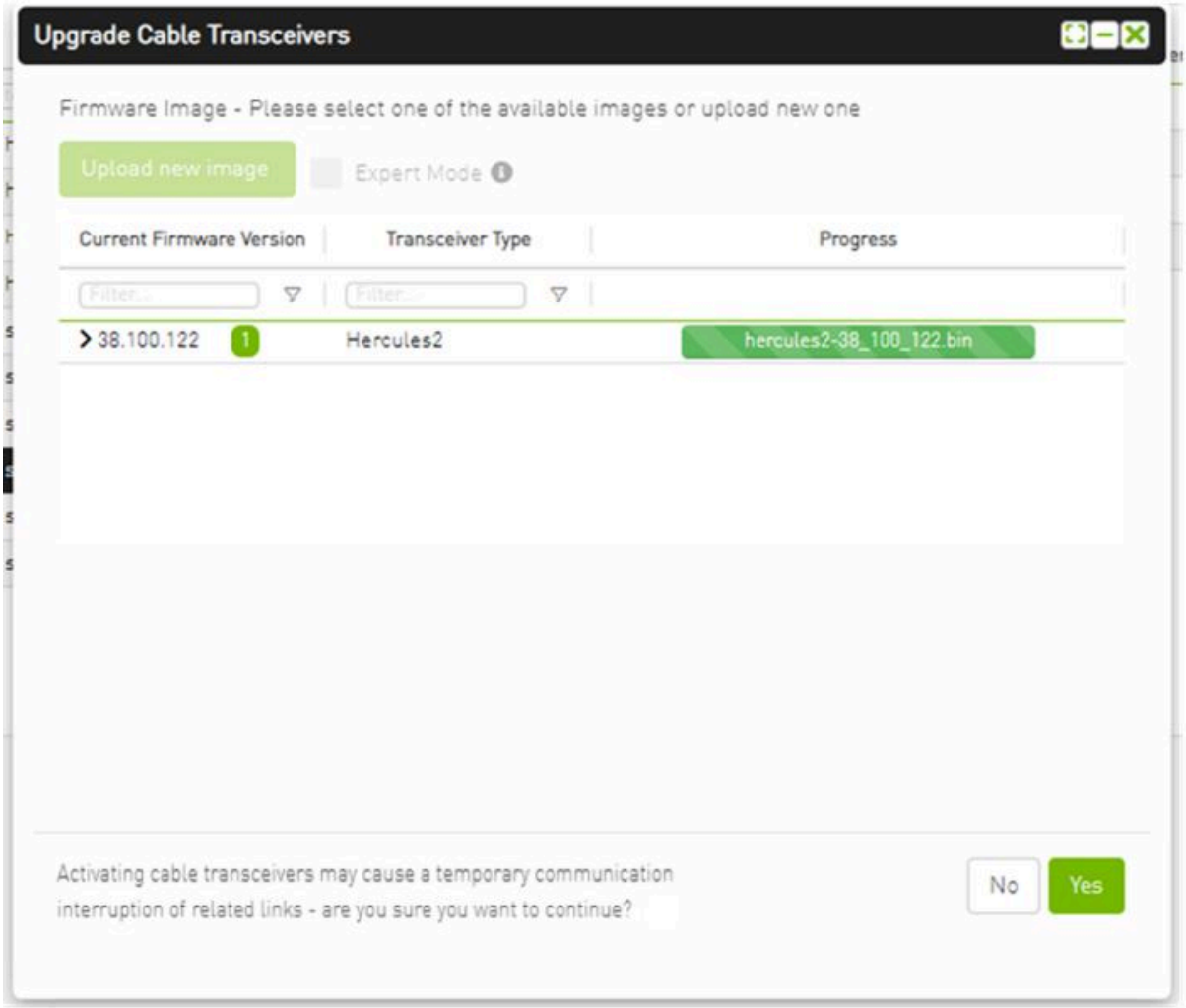


3. A model will be shown containing list of the active firmware versions for the cables of the selected switches, besides the version number, a badge will show the number of matched switches:


Upgrade Cable Transceivers
Firmware Image - Please select one of the available images or upload new one
Upload new image
Expert Mode
Current Firmware Version
Transceiver Type
Image
Filter...
Filter...
Filter...
38.100.122
1
Hercules2
No Selected Image
Close
Submit

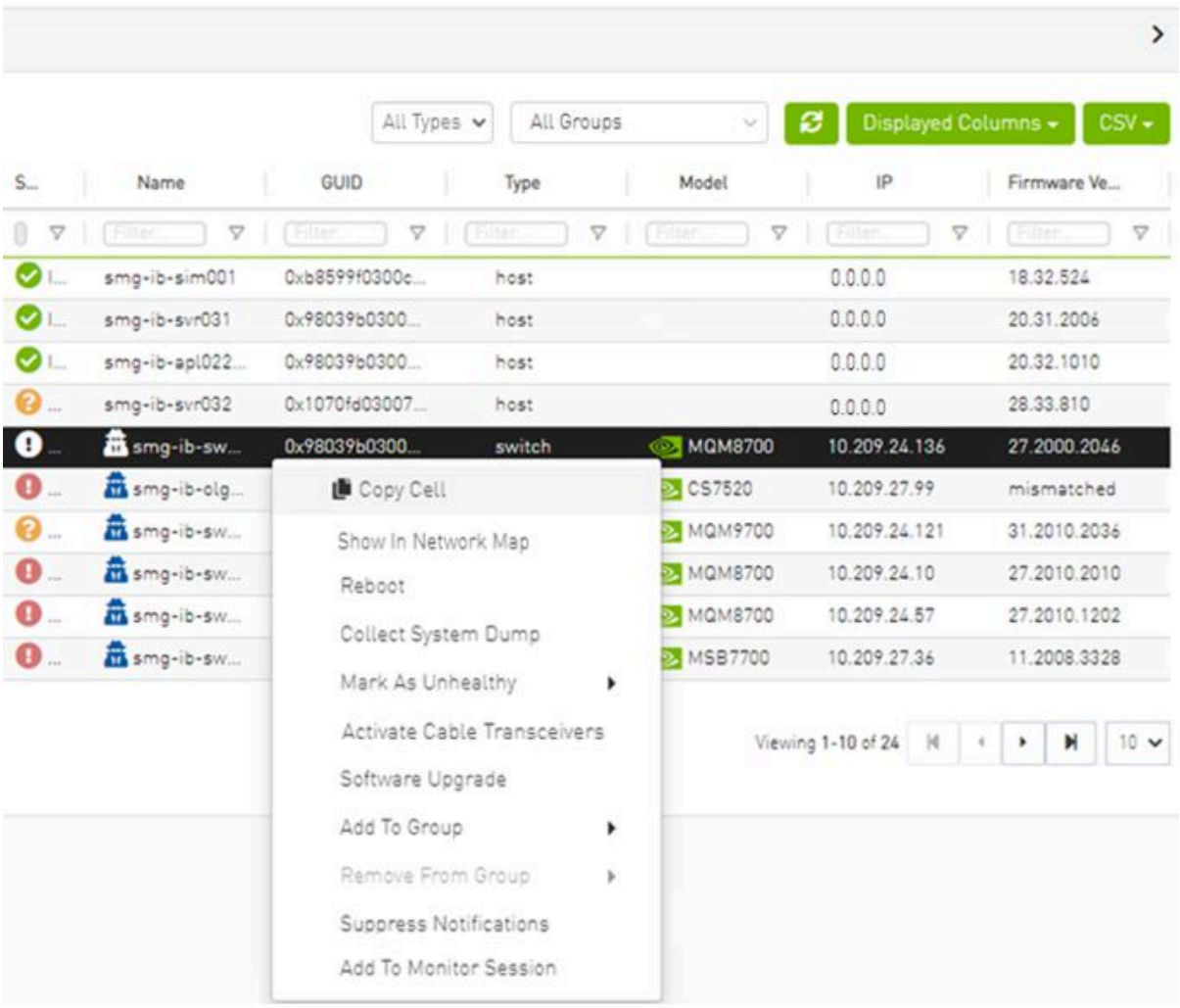


4. After the user clicks Submit, the GUI will start sending the selected binaries with the relevant switches sequentially, and a model with a progress bar will be shown (this model can be minimized):



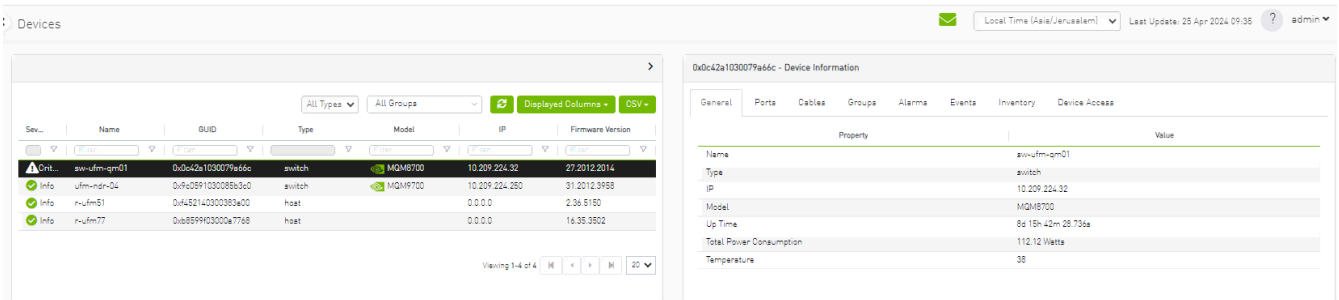
5. After the whole action is completed successfully, you will be able to see the following message at the model bottom The upgrade cable transceivers completed successfully, do you want to activate it? by clicking the yes button it will run a new action on all the burned devices to activate the new uploaded binary image.

6. Another option to activate burned cables transceivers you can go to the Groups page and right click on the predefined Group named **Devices Pending FW Transceivers Reset** or you can right click on the upgraded device from managed element page and select Activate cable Transceivers action.



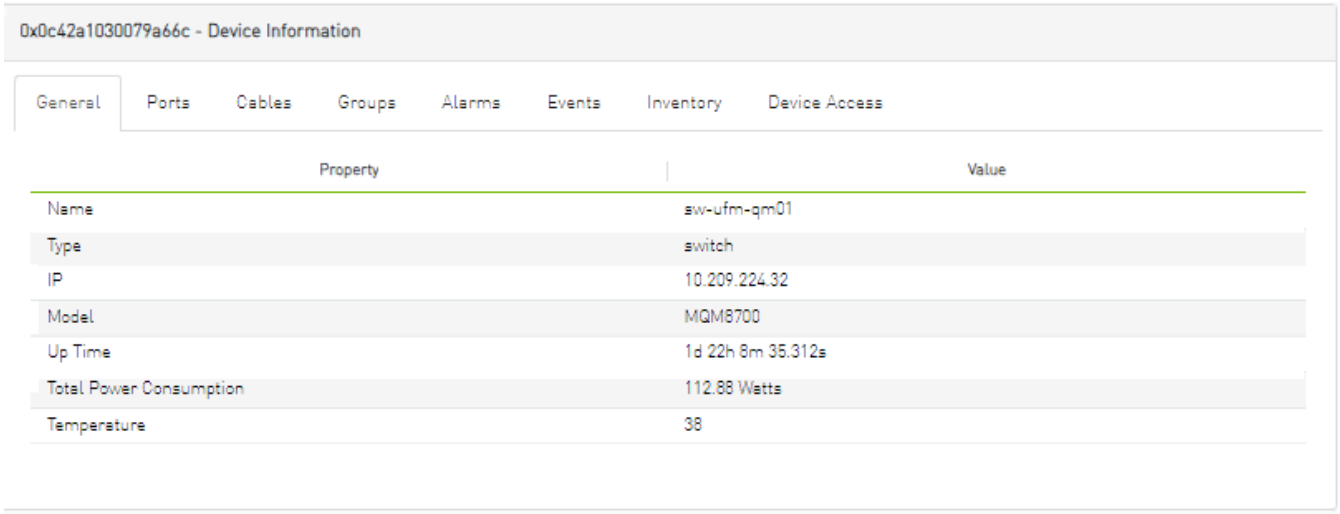
Device Information Tabs

Selecting a device from the Devices table reveals the **Device Information** table on the right side of the screen. This table provides information on the device's ports, cables, groups, events, alarms, , and device access.



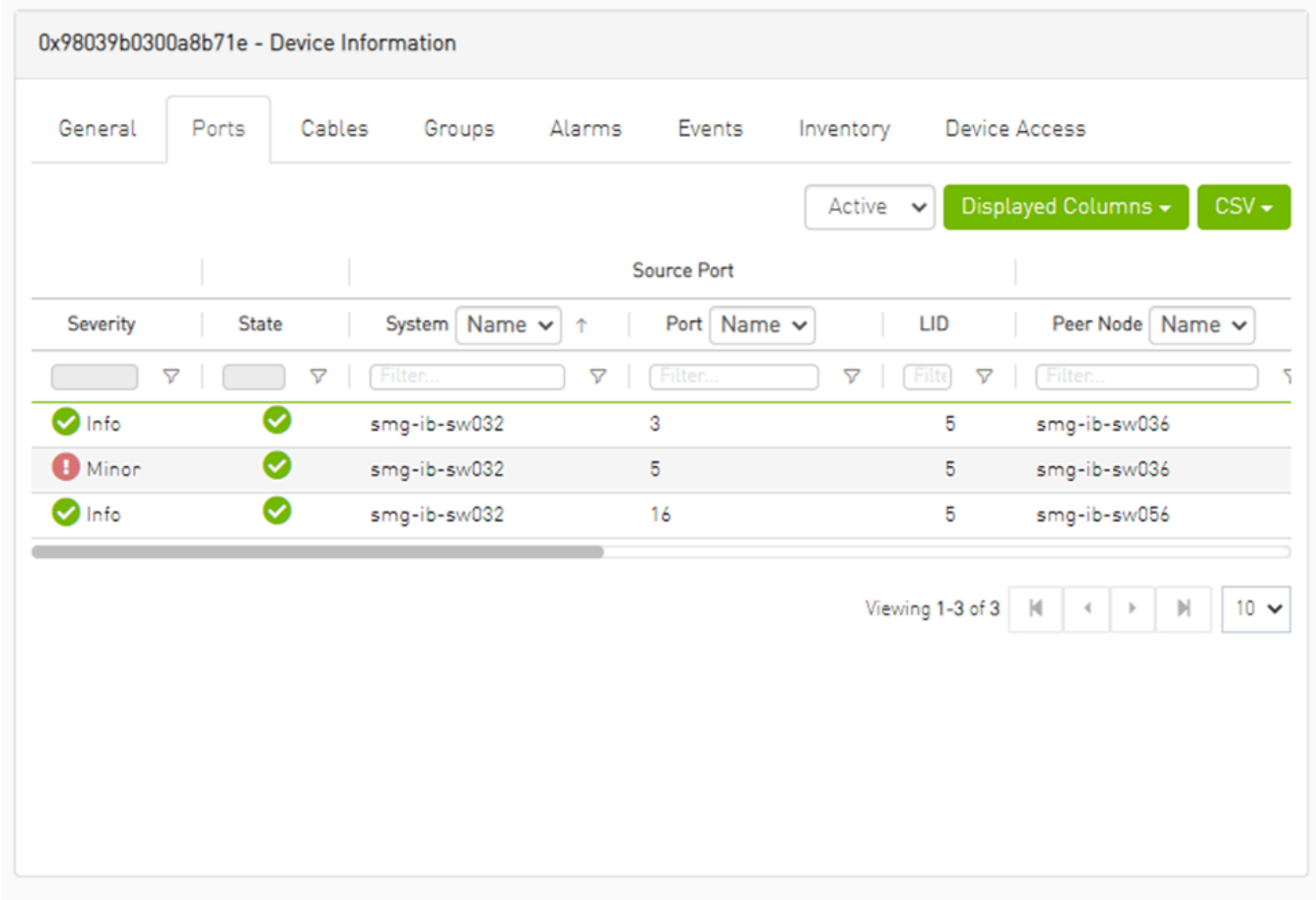
General Tab

Provides general information on the selected device.



Ports Tab

This tab provides a list of the ports connected to this device in a tabular format.



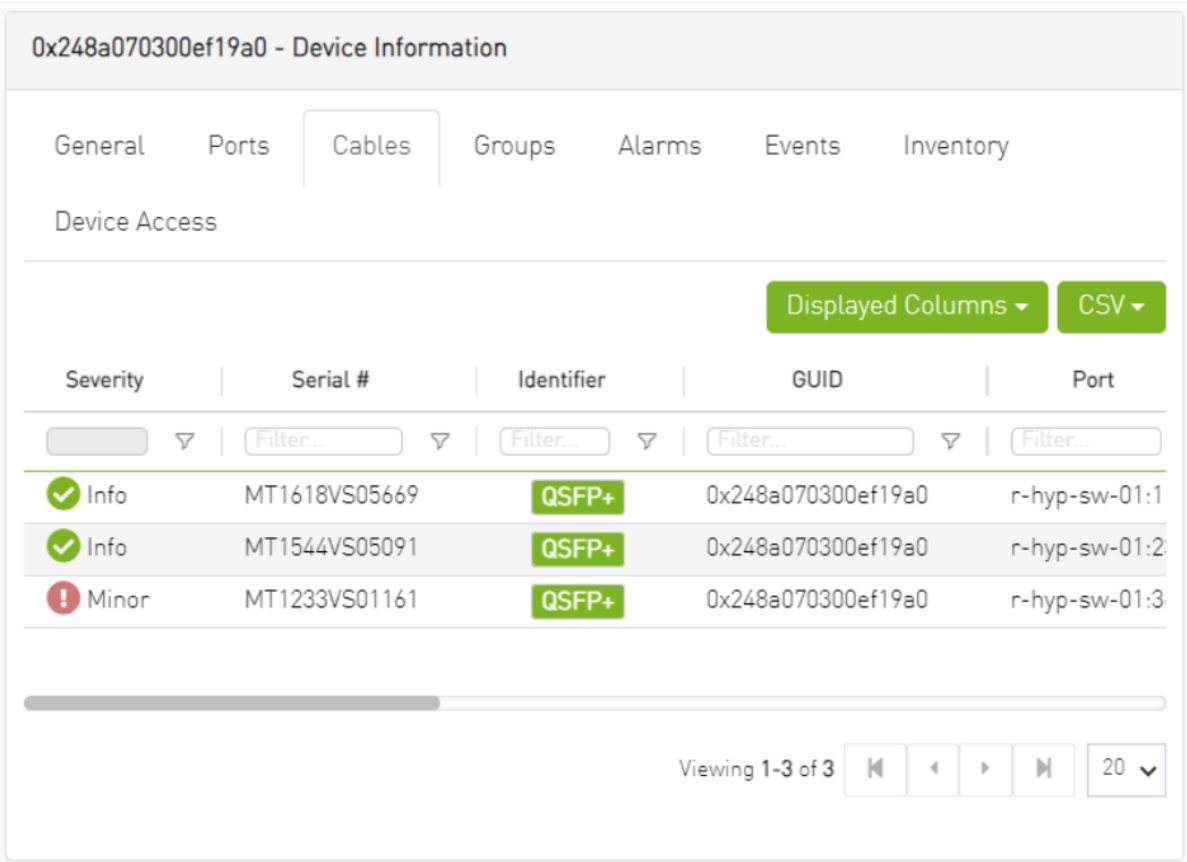
Ports Data

Data Type	Description
Port Number	The number of ports on device.
Node	The node name/GUID/IP that the port belongs to. Note that you can choose the node label (name/GUID/IP) using the drop-down menu available above the Ports data table.
Health	Health of the port reflecting the highest alarm severity. Please refer to the Health States table.
State	Indicates whether the port is connected (active or inactive).
LID	The local identifier (LID) of the port.
MTU	Maximum Transmission Unit of the port.
Speed QDR FDR EDR	Lists the highest value of active, enabled and supported speeds in icons indicating their status: • Dark green – active speed

Data Type	Description
	• Light green – enabled speed • Grey – supported yet disabled speed
Width 	Lists the highest value of active, enabled and supported widths in icons indicating their status: • Dark green – active width • Light green – enabled width • Grey – supported yet disabled width
Peer	The GUID of the device the port is connected to.
Peer Port	The name of the port that is connected to this port.

Cables Tab

This tab provides a list of the cables connected to this device in a tabular format.

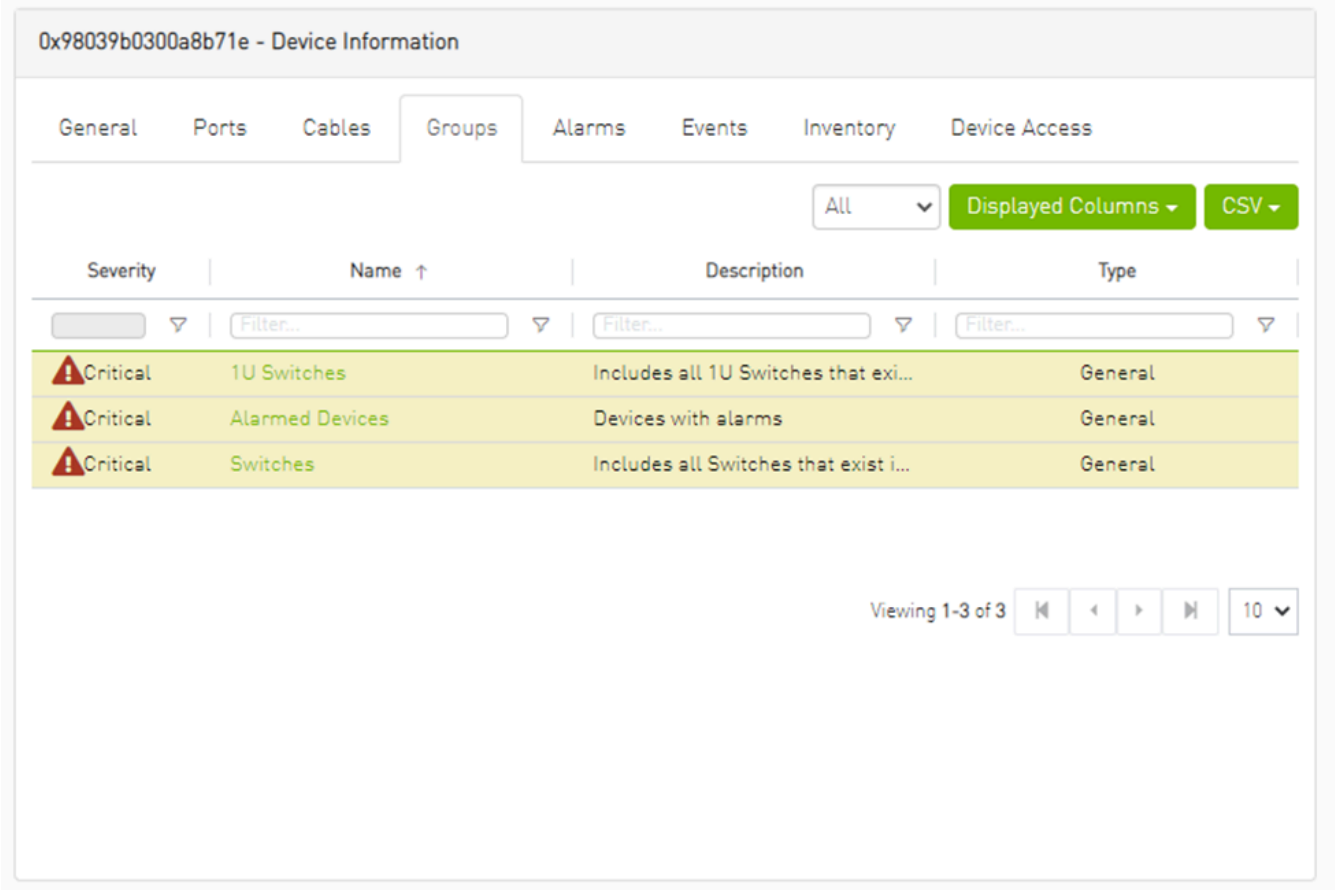


Cables Data

Data Type	Description
Basic Information	
Health	Health of the cable reflecting the highest alarm severity. Please refer to the Health States table.
Serial Number	Serial number of the cable.
Identifier	Identifier of the cable.
Source Port Information	
Source GUID	GUID of the source port the cable is connected to.
Source Port	The number of the source port the cable is connected to.
Destination Port Information	
Destination GUID	GUID of the destination port the cable is connected to.
Destination Port	The number of the destination port the cable is connected to.
Advanced Information	
Revision	Revision of the cable.
Link Width	The maximum link width of the cable.
Part Number	Part number of the cable.
Technology	The transmitting medium of the cable: copper/optical/etc.
Length	The cable length in meters.

Groups Tab

This tab provides a list of the groups to which the selected device belongs.

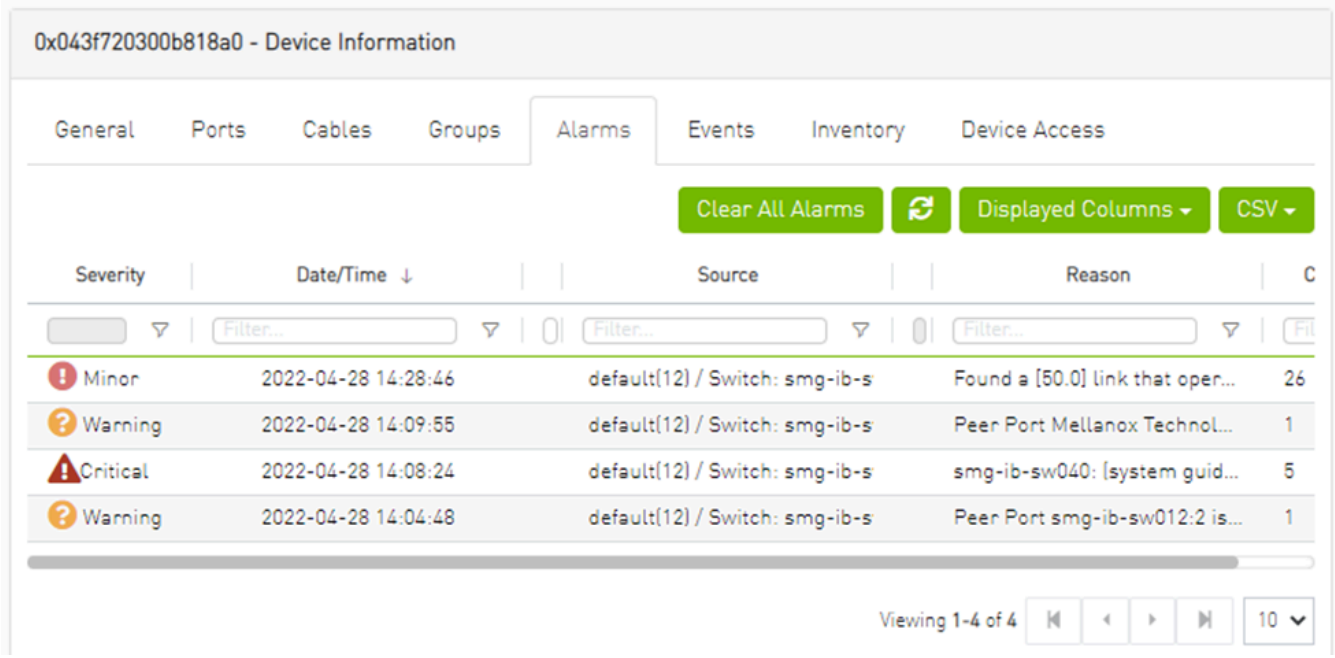


Groups Data

Data Type	Description
Severity	Aggregated severity level of the group (the highest severity level of all group members).
Name	Name of the group.
Description	Description of the group.
Type	Type of the group: General/Rack.

Alarms Tab

This tab provides a list of all UFM alarms related to the selected device.

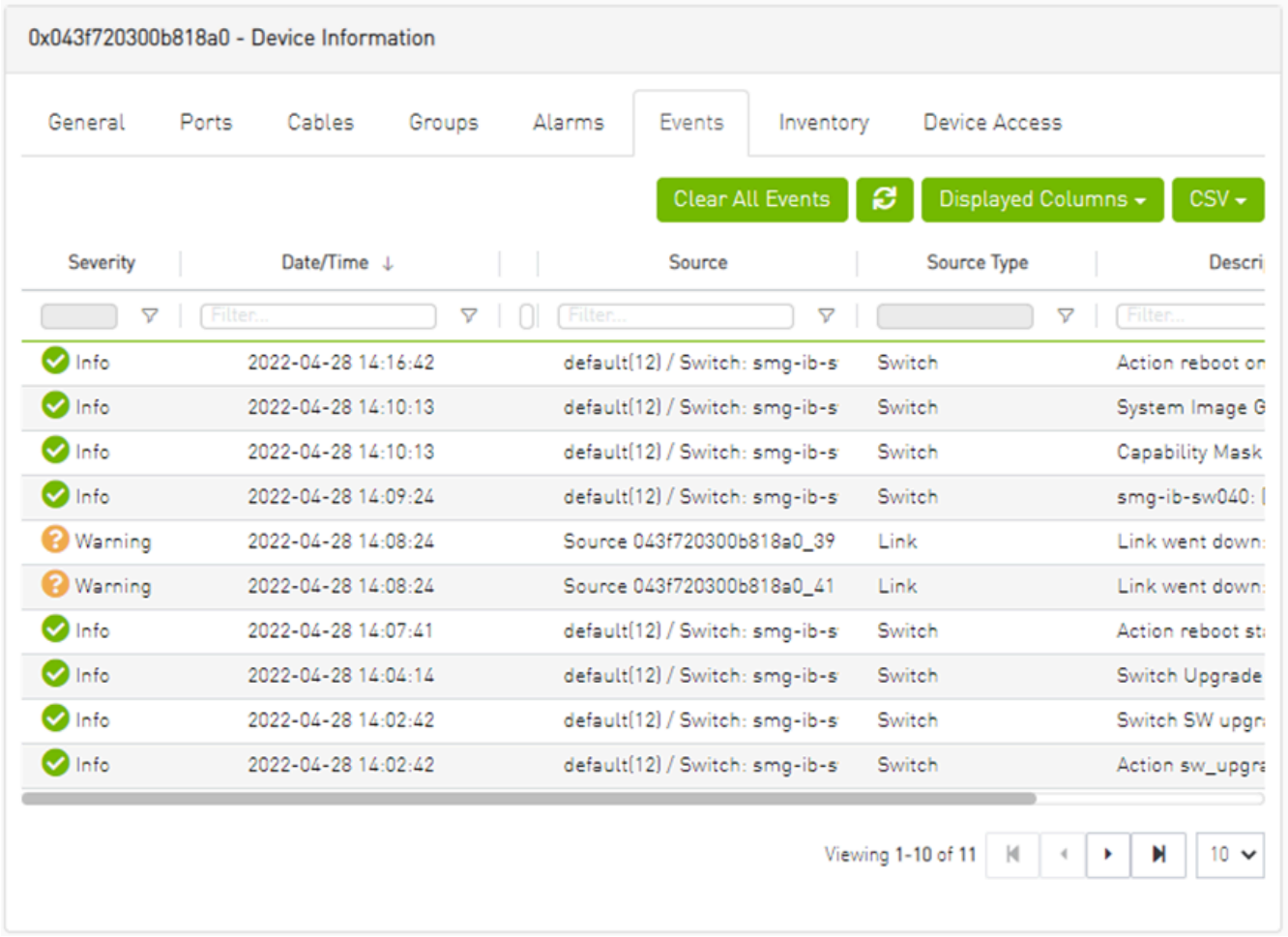


Alarms Data

Data Type	Description
Alarms ID	Alarm identifier.
Source	Source object (device/port) on which the alarm was triggered.
Severity	The severity of the alarm.
Description	Description of the alarm.
Date/Time	The time when the alarm was triggered.
Reason	Reason for the alarm.
Count	Number of instances that the alarm occurred on the related source object.

Events Tab

This tab provides a list of the UFM events that are related to the selected device.



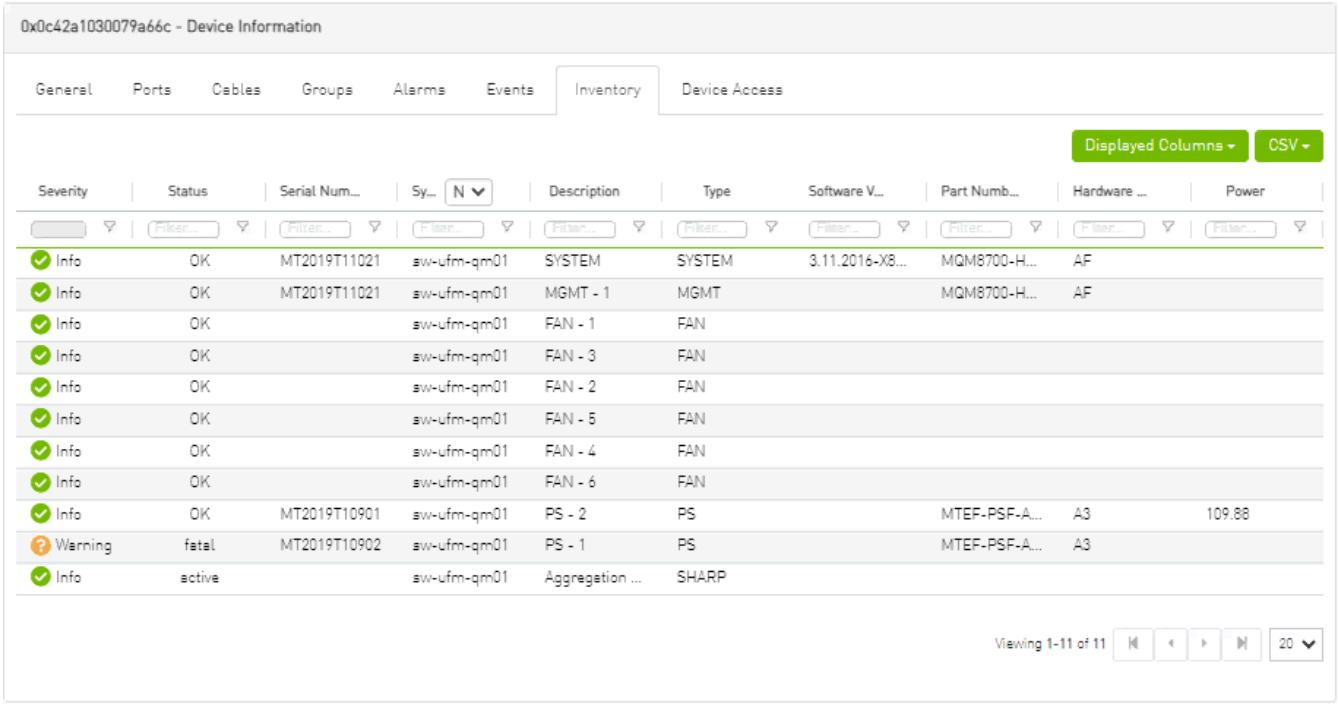
Events Data

Data Type	Description
Severity	Event severity – Info, Warning, Error, Critical or Minor.
Event Name	The name of the event.
Source	The source object (device/port) on which the event was triggered.
Date/Time	The time when the event was triggered.
Category	The category of the event indicated by icons. Hovering over the icon will display the category name.
Description	Description of the event. Full description can be displayed by hovering over the text.

Inventory Tab

This tab provides a list of the device's modules with information in a tabular format.

> **Note**
>
> This tab is available for switches only.



Inventory Data

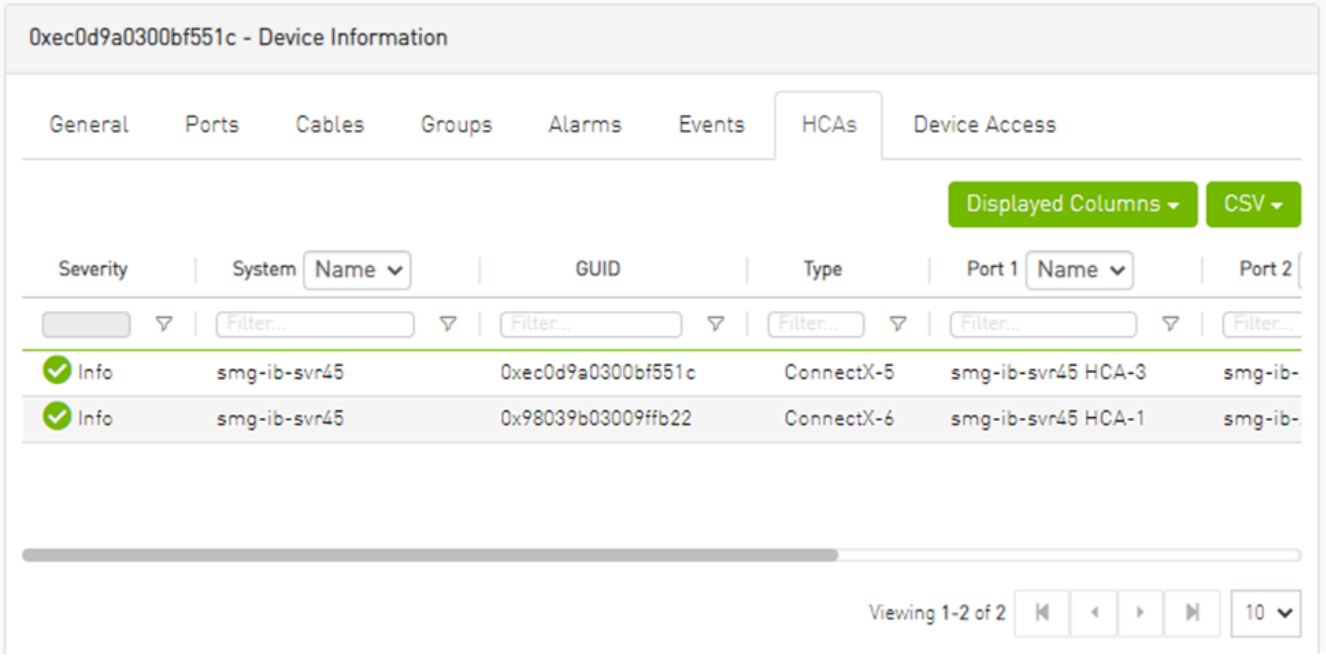
Data Type	Description
Severity/Health	Health of the module reflecting the highest alarm severity. Please refer to the Health States table.
Status	The module status.
Serial Number	Serial number of the module.
System	Name of the device.
Description	Description of the module.

Data Type	Description
Type	Type of the module: spine/line/etc.
Software Version	Firmware version installed on the module.
Part Number	Part number of the module.
Hardware Version	Hardware version of the module.
Power	Power supply of the PSU.

HCAs Tab

This tab provides a list of the device's HCAs with information in a tabular format.

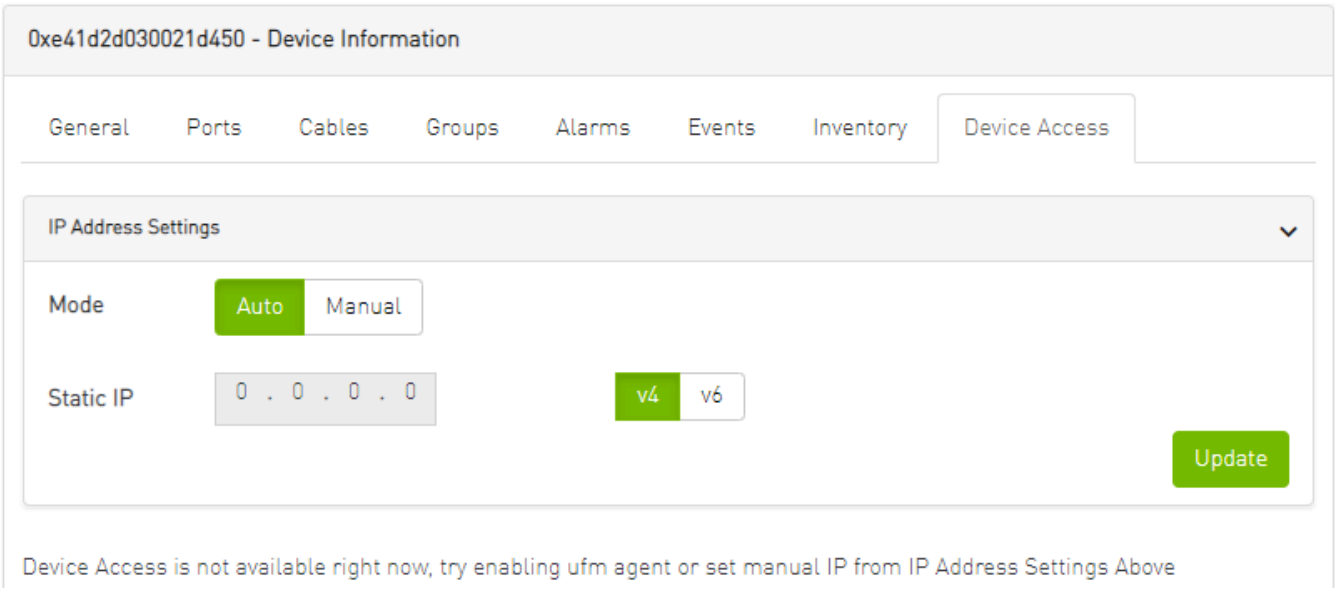
> **Note**
>
> This tab is available for hosts only.



Data Type	Description
Health	Health of the HCA reflecting the highest alarm severity. Please refer to the Health States table.
Name	HCA Index
GUID	HCA GUID
Type	HCA Type
Port GUID	HCA ports GUIDs
PSID	HCA PSID
FW Version	HCA firmware version

Device Access Tab

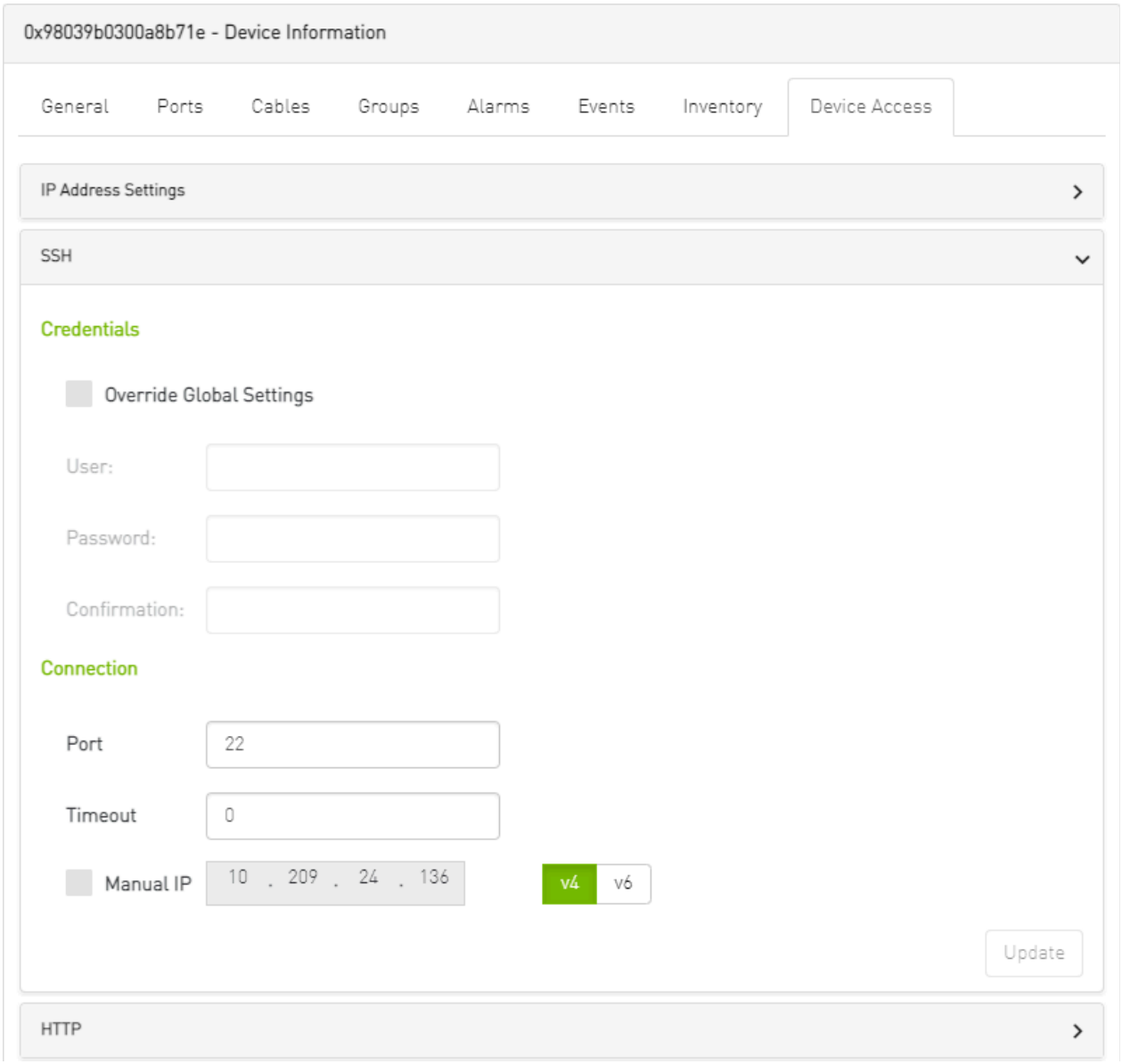
This tab allows for managing the access credentials of the selected device for remote accessibility. To be able to set access credentials for the device, a device IP must be set either by installing UFM Agent on the device, or by manually setting the IP under **IP Address Settings** (IP is now supported with v4 and v6).



> **Note**
>
> After manually setting the IP address of NVIDIA® Mellanox® InfiniScale IV® and SwitchX® based switches, UFM will first validate the new IP before setting it.

To edit your device access credentials

1. Select the preferred protocol tab:
    - **SSH** – allows you to define the SSH parameters to open an SSH session on your device (available for **nodes** and **switches**)
    - **IPMI** – allows you to set the IPMI parameters to open an IPMI session on your device for remote power control (available for **nodes only**)
    - **HTTP** – allows you to define the HTTP parameters to open an HTTP session on your device (available for **switches only**)
2. Click **Update** to save your changes.



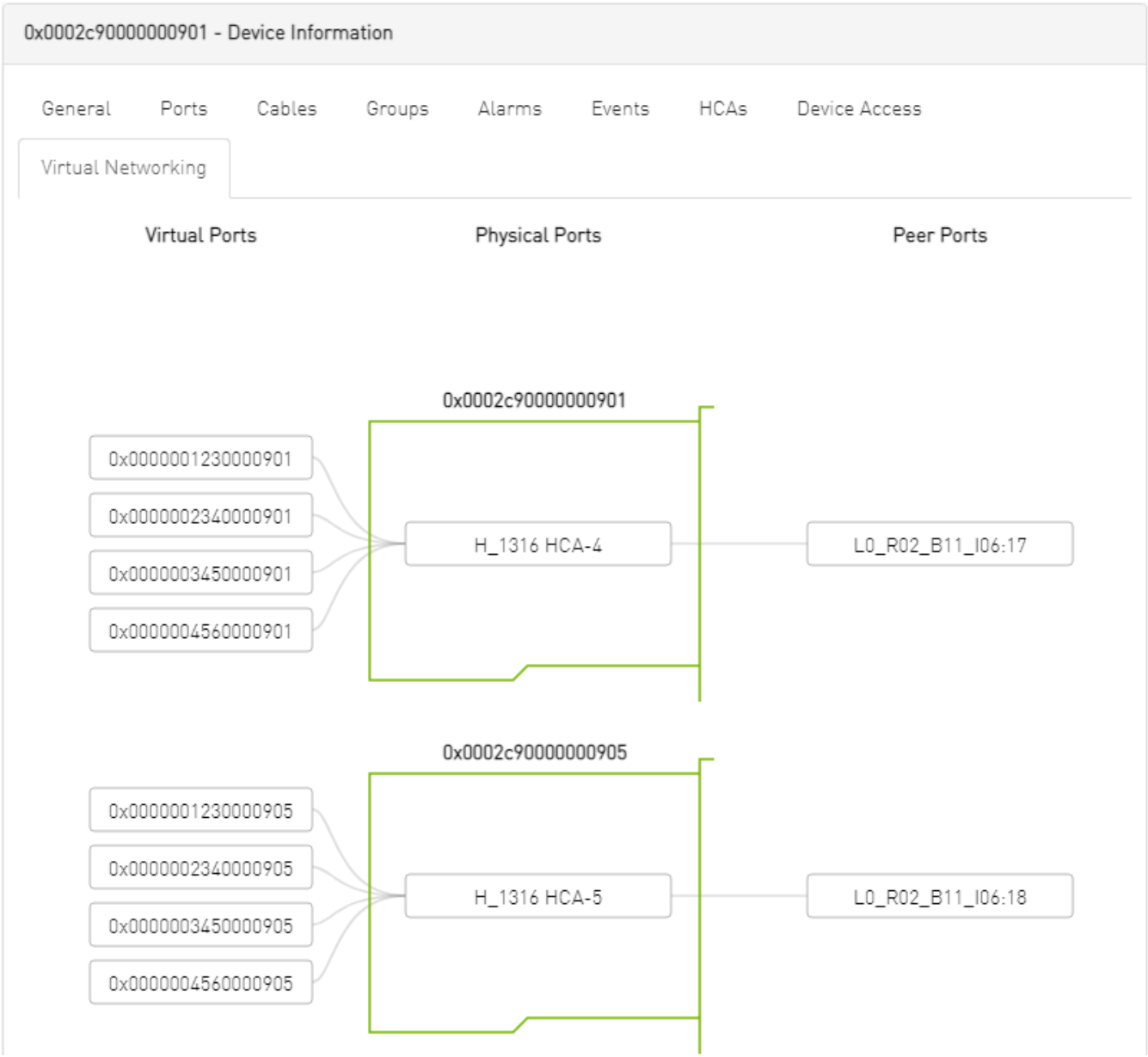
Device Access Credentials Parameters

Field	Description
User	Fill in or edit the computer user name.
Password	Enter the device password.
Confirmation	Enter the device password a second time to confirm.
Manual IP	Enter the device IP address (could be IPv4/IPv6).
Port	Enter the port number.
Timeout	Enter the connection timeout (in seconds) for the device specific

Field	Description
	protocol (SSH/HTTP/IPMI).

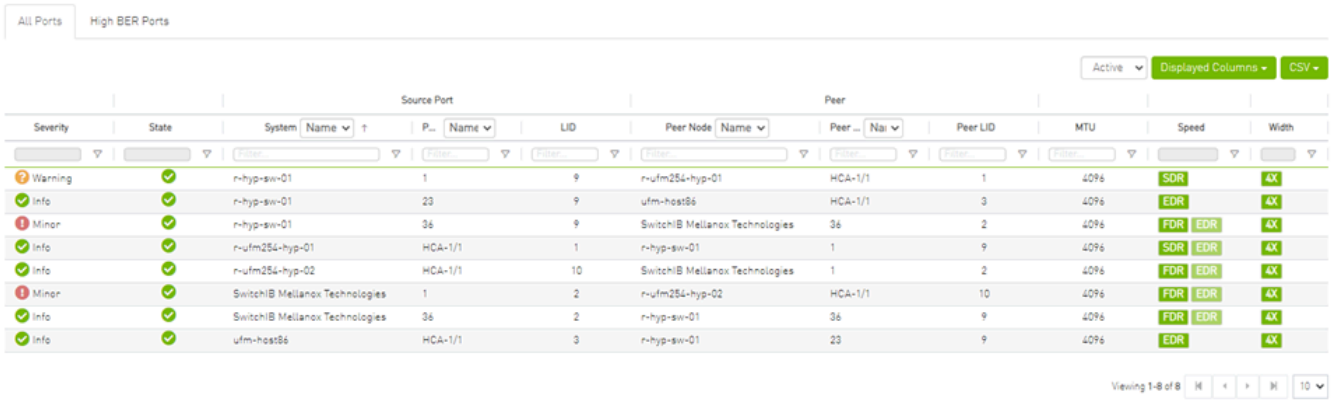
Virtual Networking Tab

This tab displays a map containing the HCAs for the selected device, and the ports and virtual ports it is connected to.



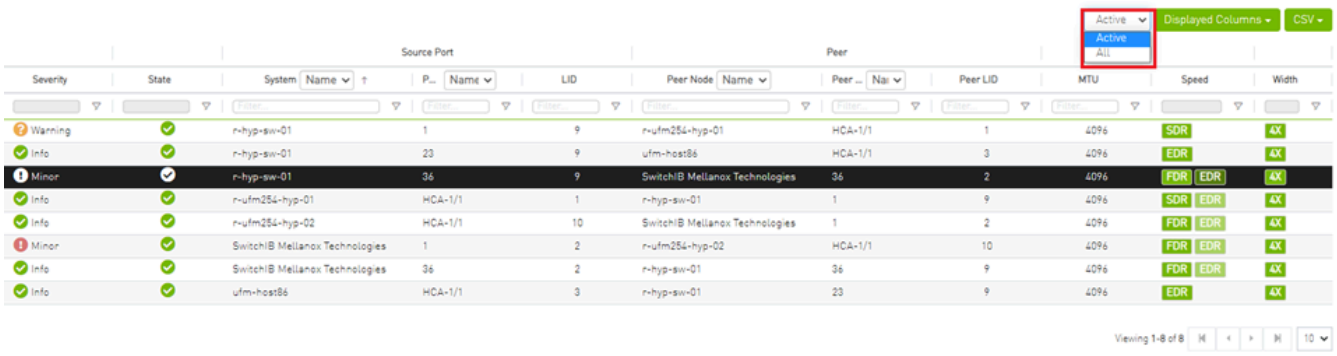
Ports Window

Provides a list of all ports in UFM.

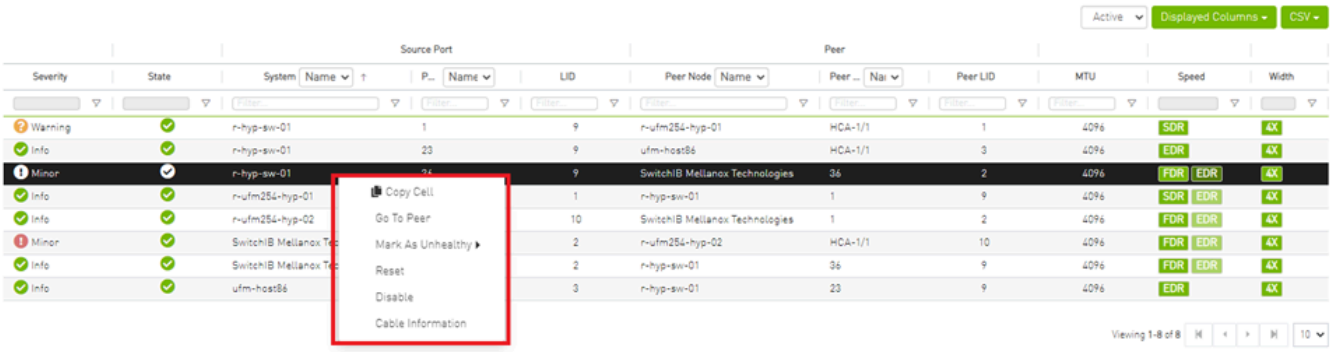


The table can be filtered by port state. The filter contains two options:

- Active – only active ports
- All – all ports



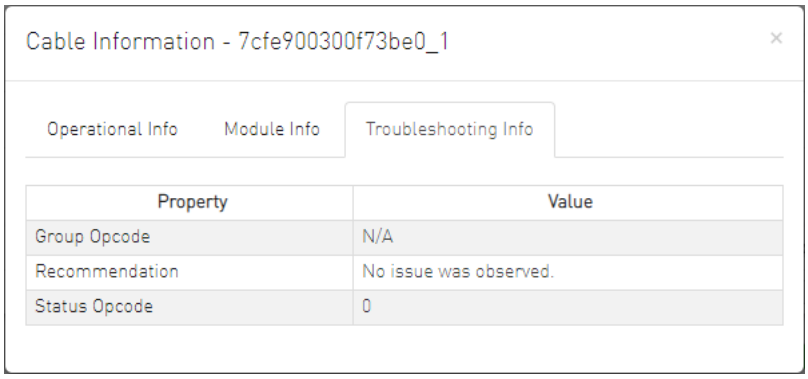
When right-clicking one of the available ports, the following actions appear:

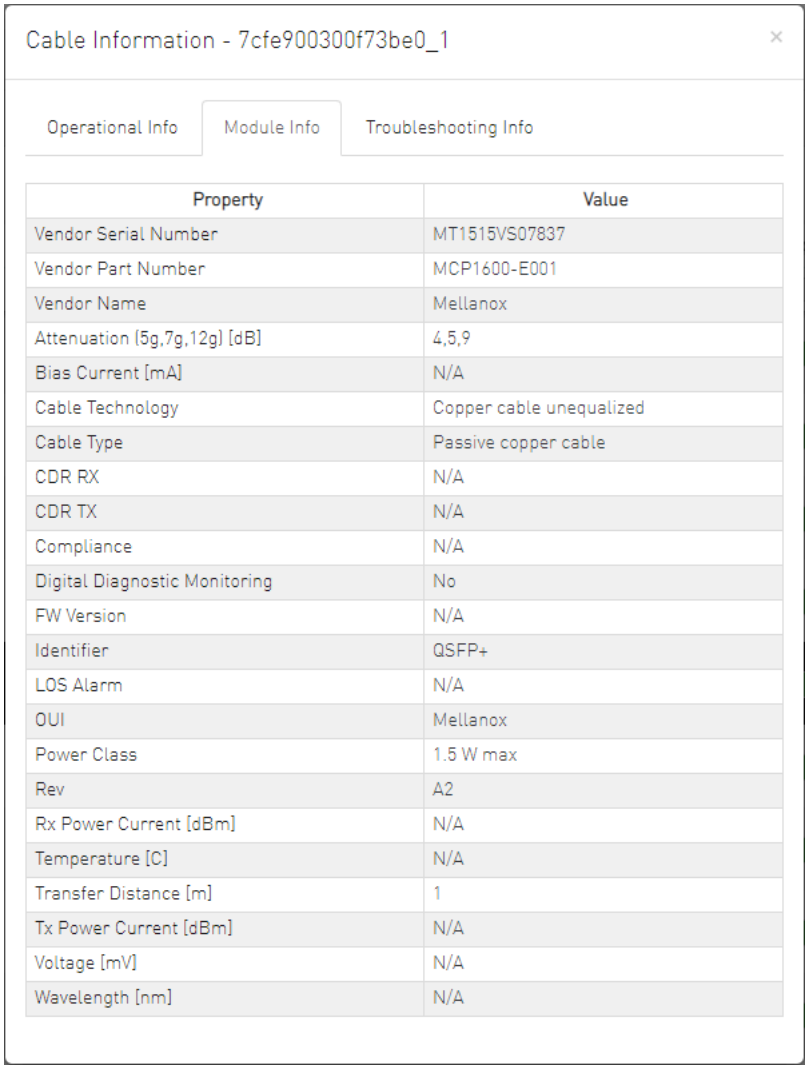


Note

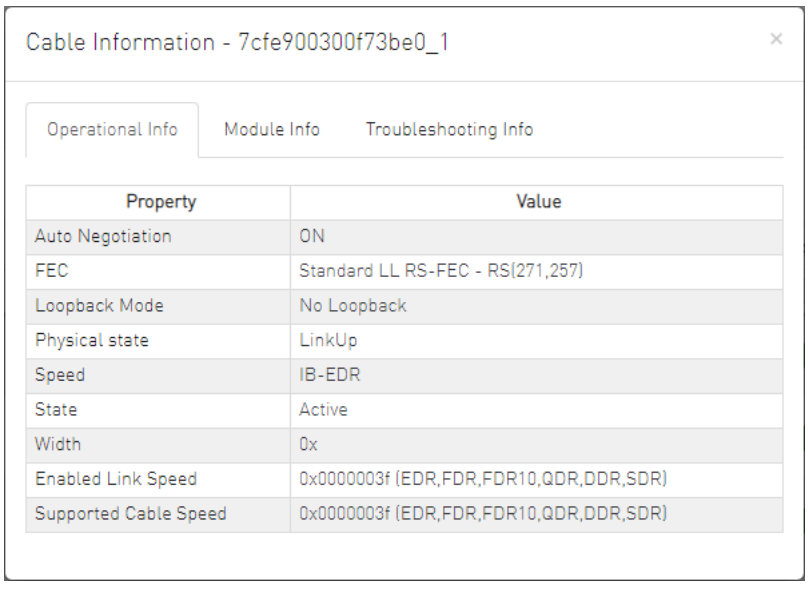
All enable/disable actions on managed switches' ports are persistent. Thus, if a managed switch port is disabled, the port remains disabled even when rebooting the switch.

Clicking "Cable Information" opens up a window which provides data on operational, module, and troubleshooting information as shown in the following:





Property	Value
Vendor Serial Number	MT1515VS07837
Vendor Part Number	MCP1600-E001
Vendor Name	Mellanox
Attenuation (5g,7g,12g) [dB]	4,5,9
Bias Current [mA]	N/A
Cable Technology	Copper cable unequalized
Cable Type	Passive copper cable
CDR RX	N/A
CDR TX	N/A
Compliance	N/A
Digital Diagnostic Monitoring	No
FW Version	N/A
Identifier	QSFP+
LOS Alarm	N/A
OUI	Mellanox
Power Class	1.5 W max
Rev	A2
Rx Power Current [dBm]	N/A
Temperature [C]	N/A
Transfer Distance [m]	1
Tx Power Current [dBm]	N/A
Voltage [mV]	N/A
Wavelength [nm]	N/A



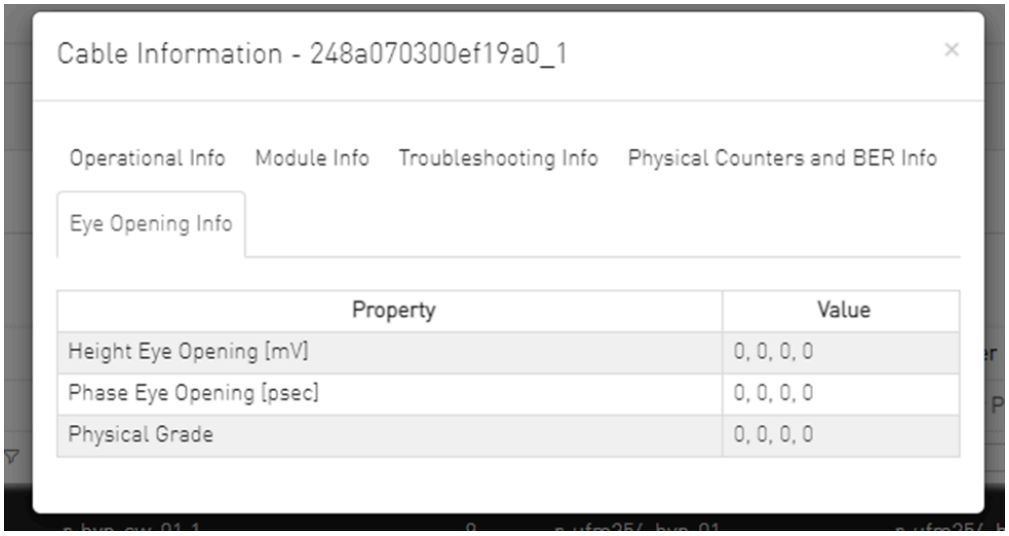
Property	Value
Auto Negotiation	ON
FEC	Standard LL RS-FEC - RS(271,257)
Loopback Mode	No Loopback
Physical state	LinkUp
Speed	IB-EDR
State	Active
Width	0x
Enabled Link Speed	0x0000003f (EDR,FDR,FDR10,QDR,DDR,SDR)
Supported Cable Speed	0x0000003f (EDR,FDR,FDR10,QDR,DDR,SDR)

Physical Grade and Eye Opening Information

Eye opening information contains the following data:

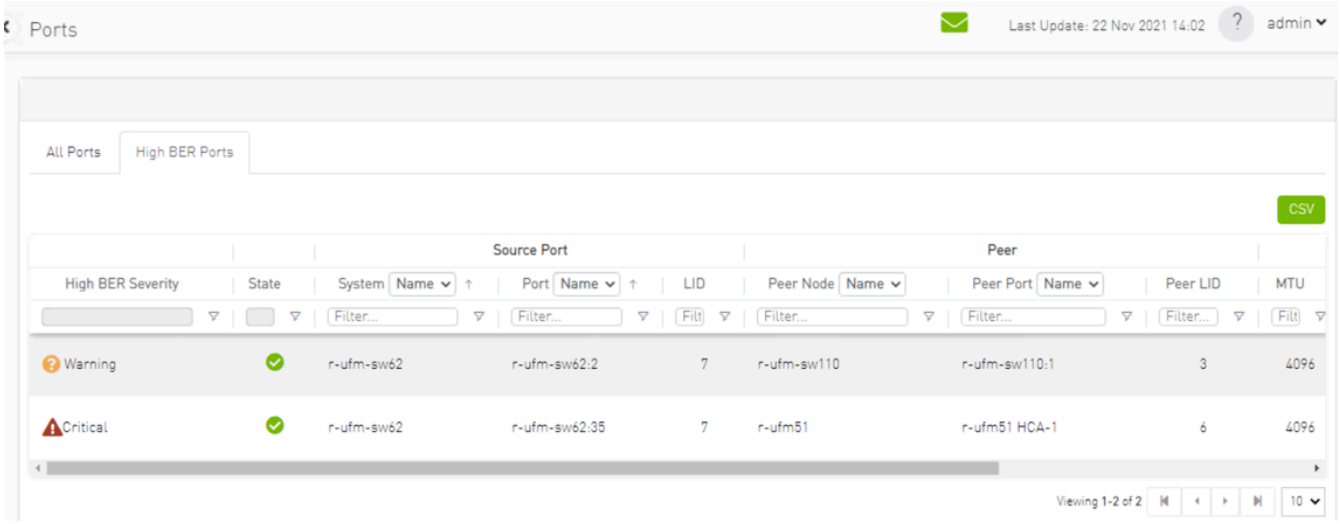
- Physical Grade: [Grade0, Grade1, Grade2, Grade3]
- Height Eye Opening [mV]: [Height0, Height1, Height2, Height3]
- Phase Eye Opening [psec]: [Phase0, Phase1, Phase2, Phase3]

A new tab called Eye Information was added under cable information modal in ports table.



Auto-isolation of High-BER Ports

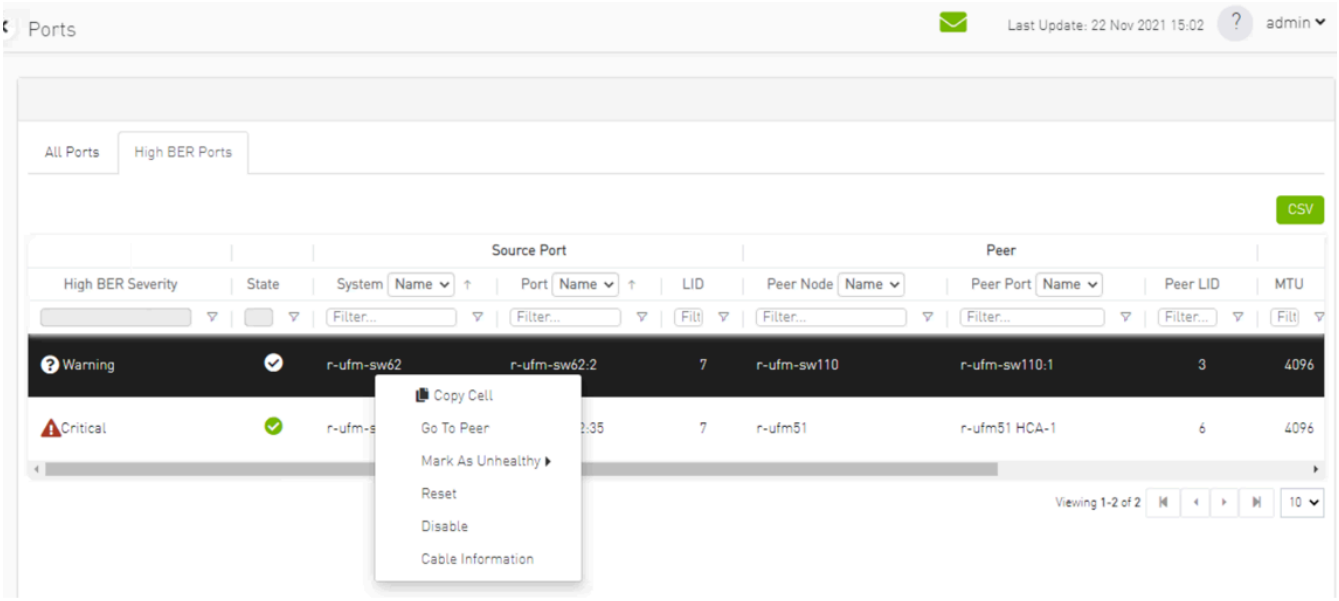
The High BER Ports tab lists all high-BER ports in the fabric.



The flags high_ber_ports_auto_isolation must be configured in the gv.cfg file to enable this feature.

For each port discovered as a high-BER port, a new event is triggered in the Events table.

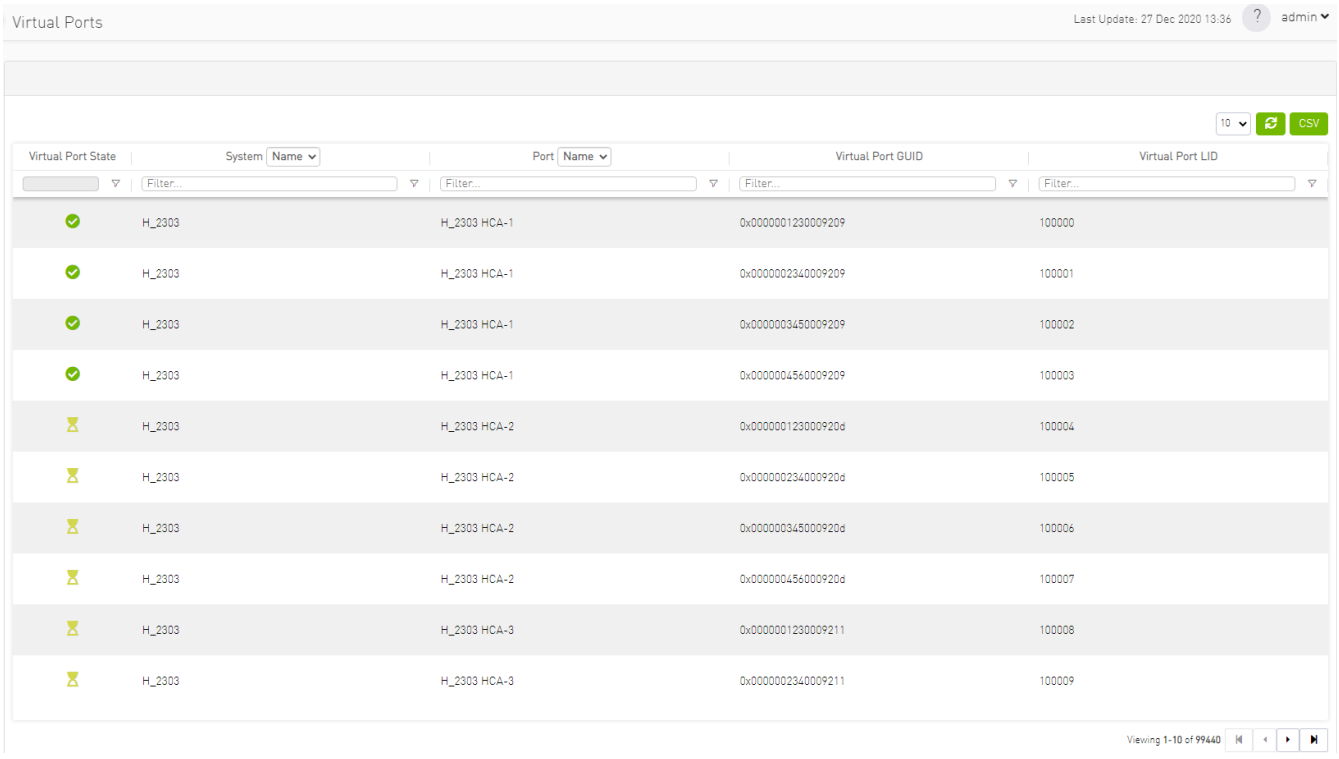
Marking the high-BER port as unhealthy suppresses all events and notifications related to the auto-isolated port.



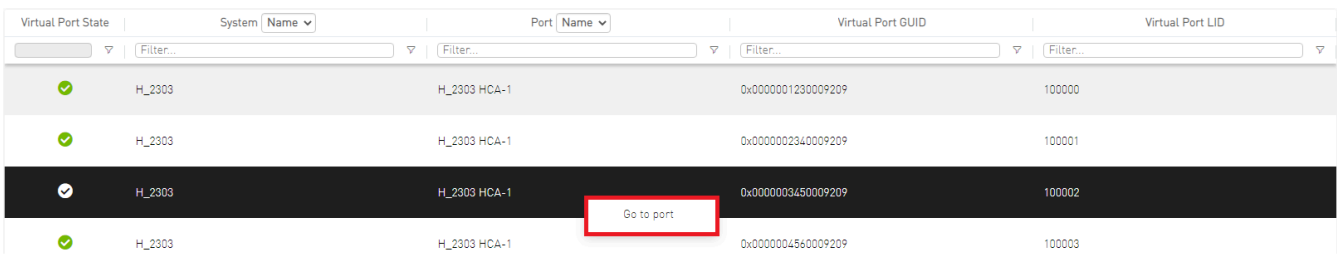
Virtual Ports Window

> **Note**
>
> This page is only available if Virtualization is enabled in gv.cfg.

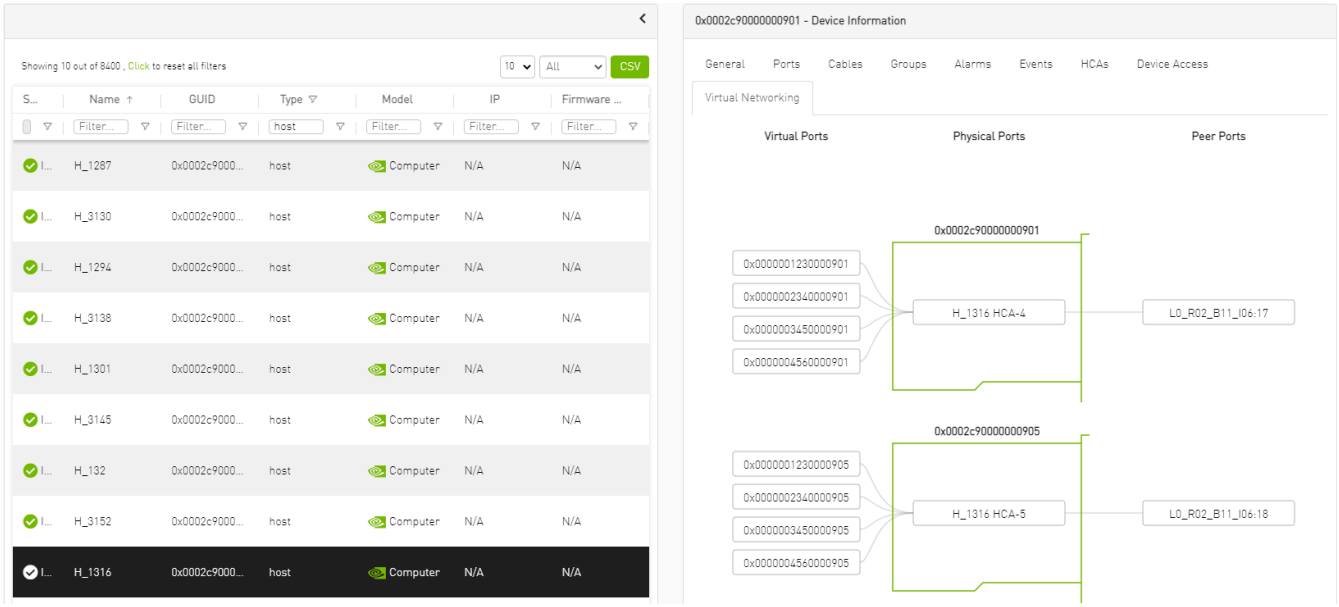
Provides a list of all virtual ports in UFM.



Right-clicking a virtual port allows navigation to the physical port mapped it is mapped to.



Clicking "Go to port" navigates to the Virtual Networking tab of the Device Information screen.

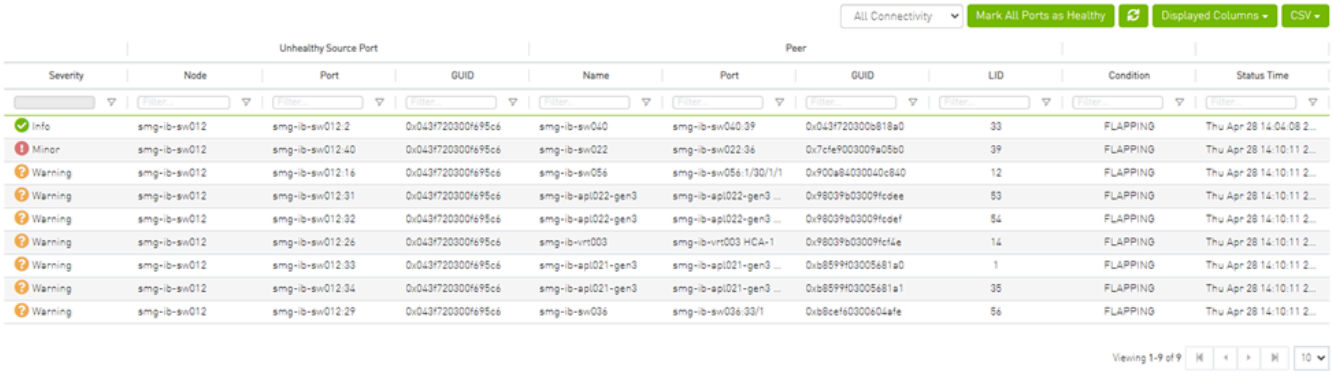


Unhealthy Ports Window

The Unhealthy Ports view shows all the unhealthy nodes in the fabric and the OpenSM health policy of the healthy/unhealthy nodes.

After the Subnet Manager examines the behavior of subnet nodes (switches and hosts) and discovers that a node is “unhealthy” according to the conditions specified below, the node is displayed in the Unhealthy Ports window. Once a node is declared as “unhealthy”, Subnet Manager can either ignore, report, isolate or disable the node. The user is provided with the ability to control the actions performed and the phenomena that declares a node “unhealthy." Moreover, the user can “clear” nodes that were previously marked as “unhealthy."

The information is displayed in a tabular form and includes the unhealthy port’s state, source node, source port, source port GUID, peer node, peer port, peer GUID, peer LID, condition, and status time.



Note

The feature requires OpenSM parameter hm_unhealthy_ports_checks to be set to TRUE (default).

Note

This feature is not available in the "Monitoring Only Mode."

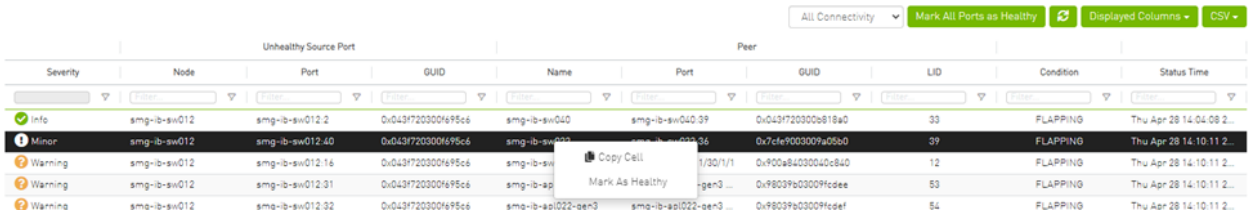
The following are the conditions that would declare a node as “unhealthy”:

- Reboot - If a node was rebooted more than 10 times during last 900 seconds
- Flapping - If several links of the node found in Initializing state in 5 out of 10 previous sweeps
- Unresponsive - A port that does not respond to one of the SMPs and the MAD status is TIMEOUT in 5 out of 7 previous SM sweeps
- Noisy Node - If a node sends traps 129, 130 or 131 more than 250 traps with interval of less than 60 seconds between each two traps
- Seterr - If a node respond with bad status upon SET SMPs (PortInfo, SwitchInfo, VLArb, SL2VL or Pkeys)
- Illegal - If illegal MAD fields are discovered after a check for MADs/fields during receive_process
- Manual - Upon user request mark the node as unhealthy/healthy
- Link Level Retransmission (LLR) – Activated when retransmission-per-second counter exceeds its threshold

All conditions except LLR generate Unhealthy port event, LLR generates a High Data retransmission event.

To clear a node from the Unhealthy Ports Tab, do the following:

1. Go to the Unhealthy Ports window under Managed Elements.
2. From the Unhealthy Ports table, right click the desired port it and mark it as healthy.



➤ ***To mark a node as permanently healthy, do the following:***

1. Open the /opt/ufm/files/conf/health-policy.conf.user_ext file.
2. Enter the node and the port information and set it as "Healthy."
3. Run the /opt/ufm/scripts/sync_hm_port_health_policy_conf.sh script.

> ⓘ **Note**
>
> To control Partial Switch ASIC Failure event:
>
> Trigger Partial Switch ASIC Failure whenever number of unhealthy ports exceed the defined percent of the total number of the switch ports.
>
> The switch_asic_fault_threshold flag (under the UnhealthyPorts section in gv.cfg file) default value is 20.

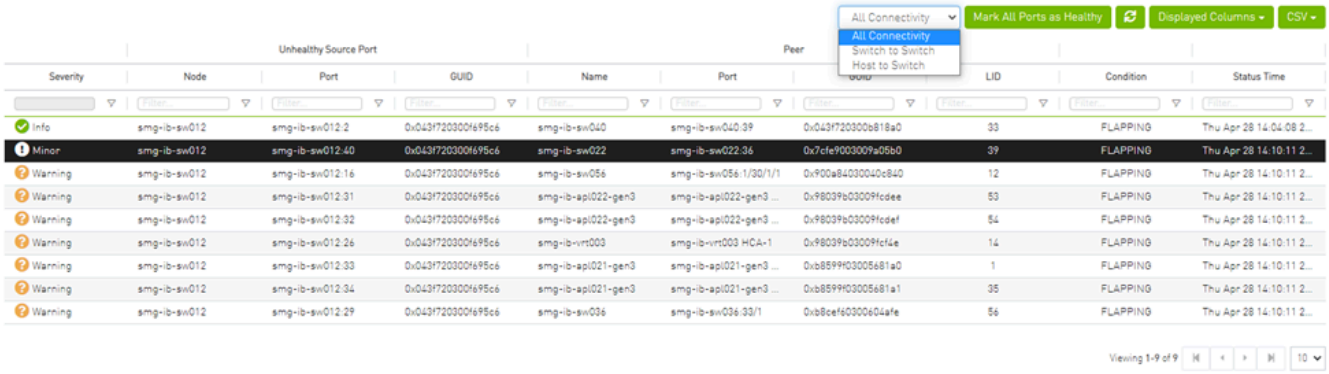
Unhealthy Port Connectivity Filter

It is possible to to filter the Unhealthy Ports table by connectivity (all, host-to-switch, or switch-to-host).

Filtering the Unhealthy Ports table is possible from the dropdown options at the top of the table which includes

- All Connectivity
- Switch to Switch

- Host to Switch

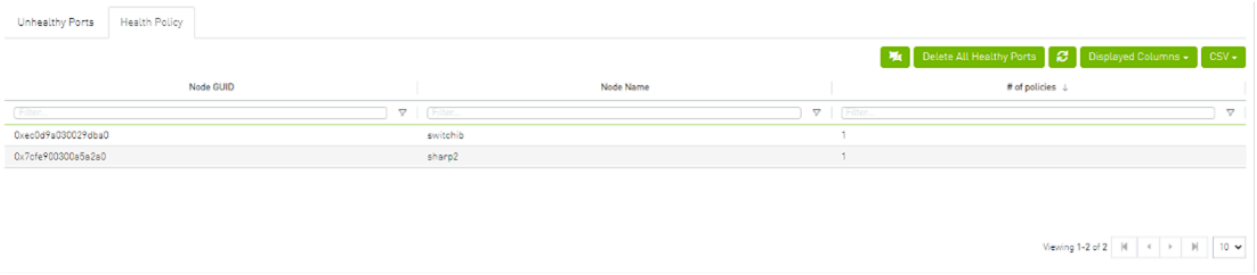


Health Policy Management

This view manages the OpenSM health policy for the healthy/unhealthy nodes and ports. The OpenSM health policy is stored in the /opt/ufm/files/conf/opensm/opensm-health-policy.conf file.

The information is displayed in a tabular form, with an option to group it either by devices or ports, and includes the health nodes/ports details (GUID, Name, policy [healthy/unhealthy])

1. Health Policy by devices:



2. Health Policy by ports:

To switch between the above views, simply click on the control button located at the top right corner of the table. By default, the devices view will be shown.

The health policy supports the following capabilities. When you select a policy and right-click, you can perform the following actions:

1. Delete the Policy

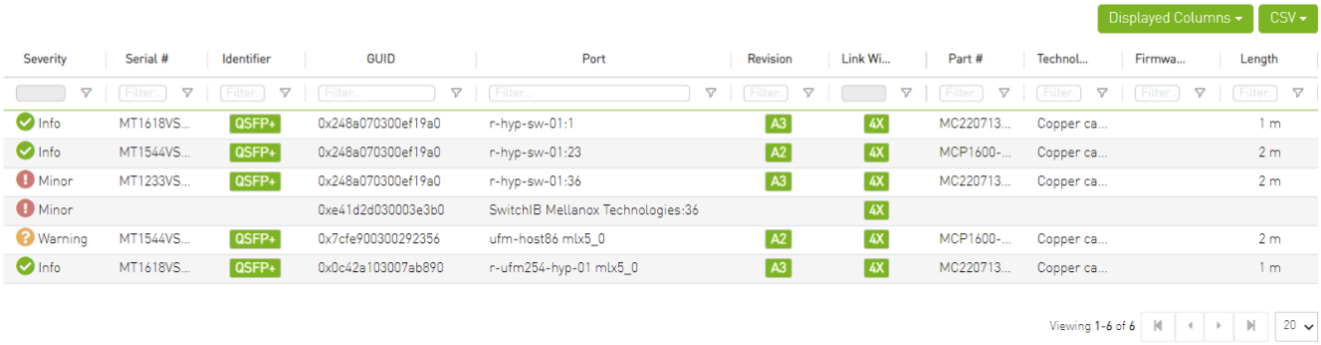
2. Mark the selected healthy policies as unhealthy (Isolate/No discover)

3. Mark the selected unhealthy policies as healthy

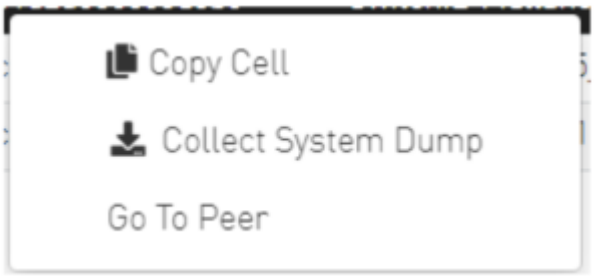
If you wish to delete all the healthy ports from the health policy, click on the 'Delete All Healthy Ports' option situated at the top right corner of the policy table.

Cables Window

Provides a list of all cables in UFM. For more information, see Device's Cables Tab.



Right-clicking a cable from the list allows users to Collect System Dump for the endpoints of the link and navigate to peer port.



Groups Window

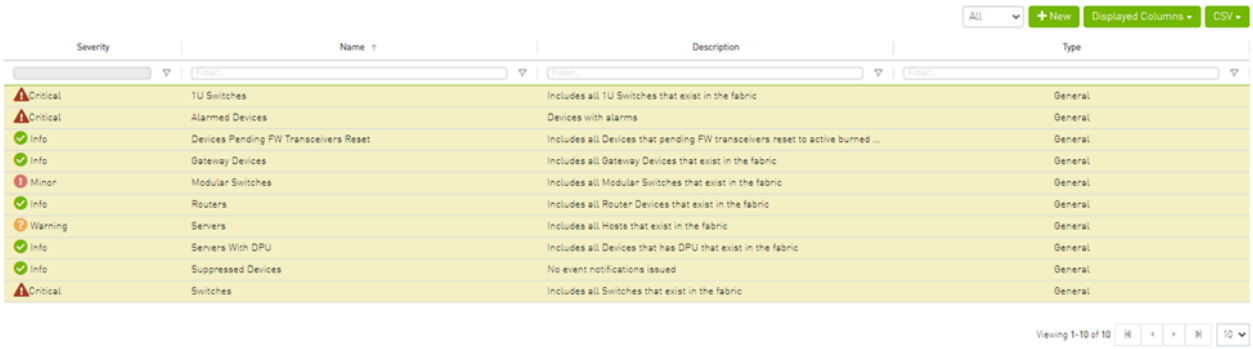
The Groups window allows users to create new groups of devices and provides information about existing groups.

> **Note**
>
> All predefined groups have Read permissions only, except Suppressed_Devices to/from which the user is also able to add/remove members or devices.

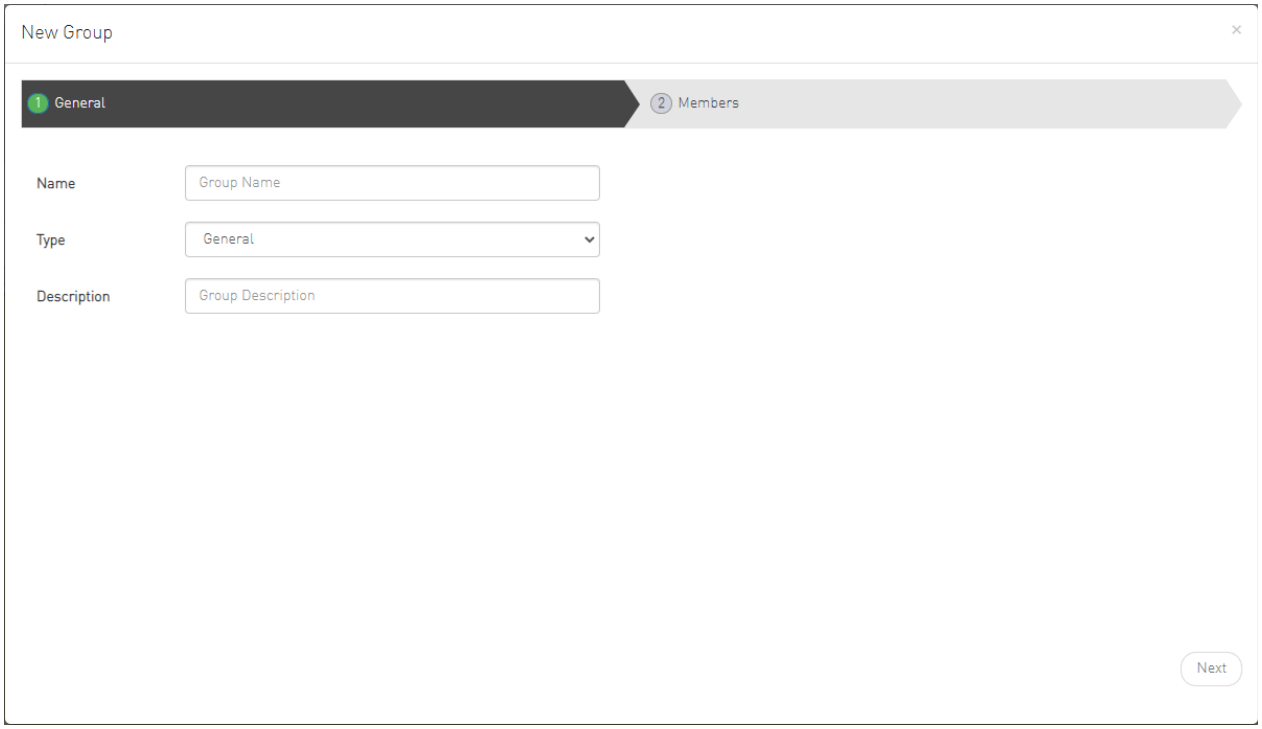
> **Note**
>
> The following predefined groups auto-populate upon UFM startup: Switches, 1U_Switches, Modular_Switches, Gateway_Devices, and Hosts.

To create a group of devices, do the following:

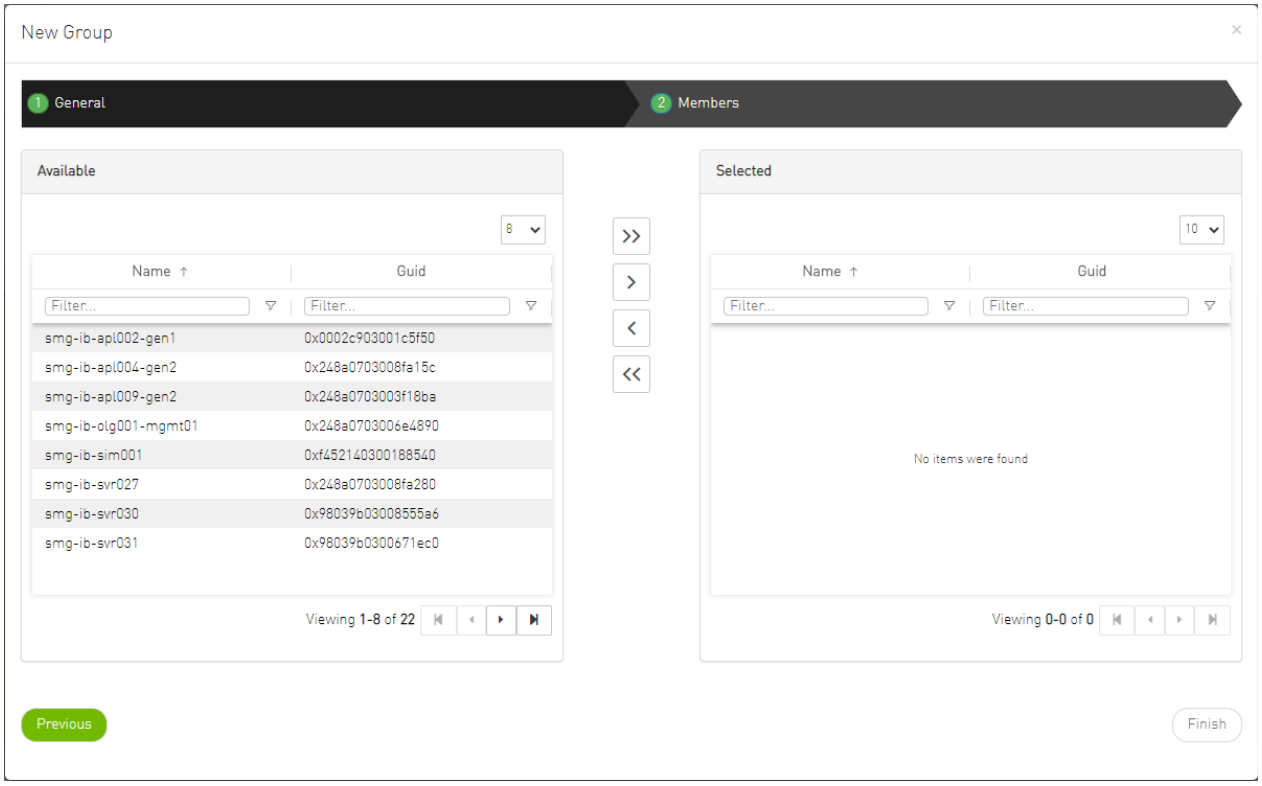
1. Click “New” under “Groups.”



2. In the New Group wizard, fill in the required information under the General tab: Name (must be between 4-20 characters), Type (General/Rack/Port), and Description (optional), and click **Next**.

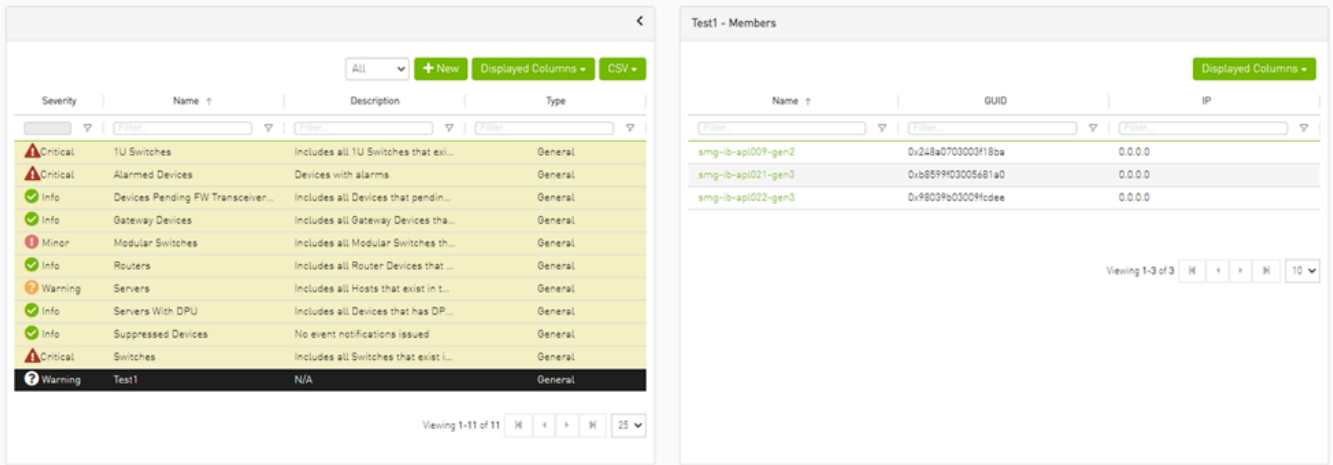


3. Under Members tab, move the members of the new group from the **Available** list to the **Selected** list.



4. Click “Finish” and the new group will appear under the Groups window.

Group members details – port’s hostname, port’s GUID, and device’s IP address – can be viewed when selecting the group from the list of all groups available.



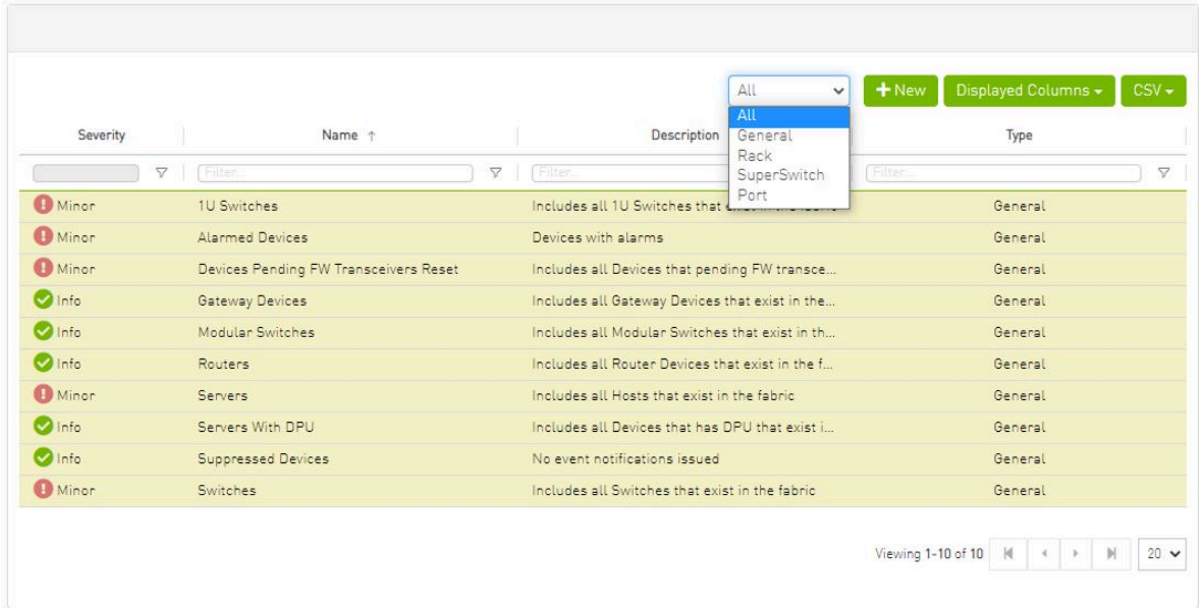
Group Actions

Right-clicking a group enables performing the following actions:

- **Edit** – groups can be modified either by editing the group description under **General** tab, or substituting group members under **Members** tab

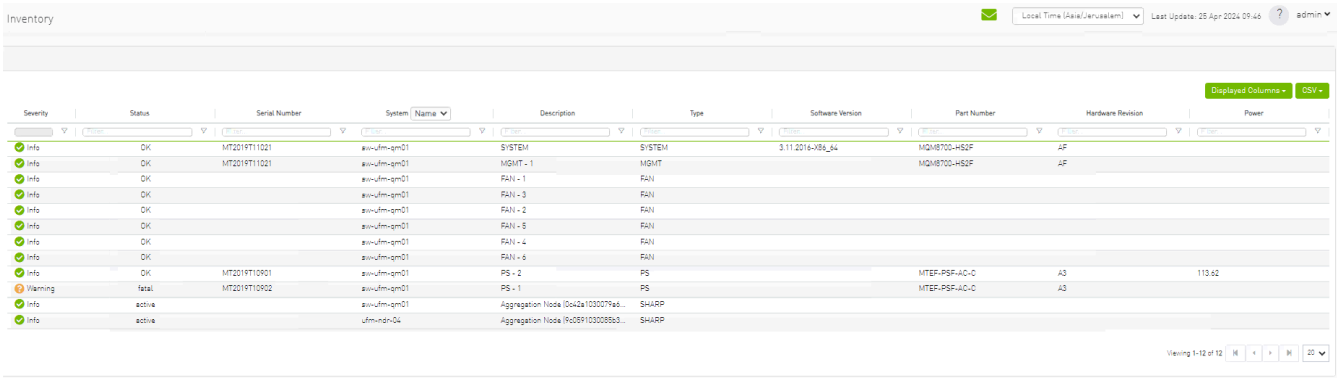
- **Delete** – existing groups can be deleted from the list
- **Remove All Members** – all members of an existing group can be removed at once
- **Collect System Dump** – sysdump may be generated for all members of an existing group

  The user can filter group by type (General, Rack, Super Switch and Port)



Inventory Window

Provides a list of all modules in UFM. For more information, see Device's Inventory Tab.



PKeys Window

The PKeys window allows users to create new groups of ports and provides information about existing PKeys.

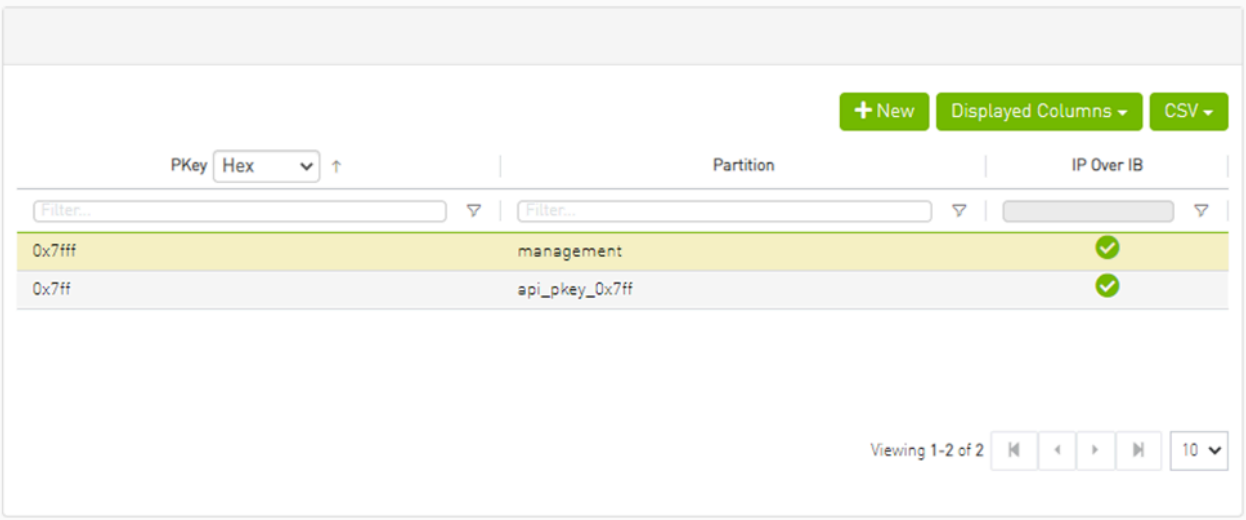
> **Note**
>
> This window offers one predefined PKey (highlighted in the list of PKeys): Management key 0x7fff with Read permissions only.

For further information about InfiniBand partitioning (Pkeys management), please refer to the Partitioning Appendix.

Creating New PKey

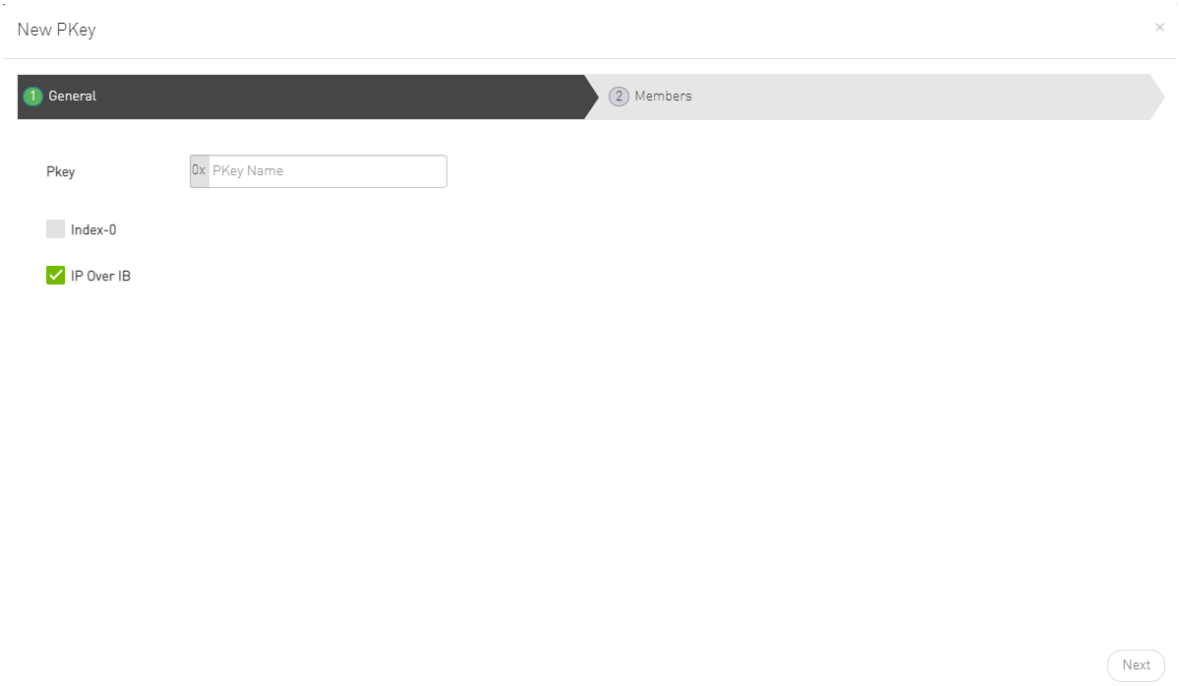
1. Click the “New” button under “PKeys".

   Please note that the yellow highlighted PKeys are predefined ones.

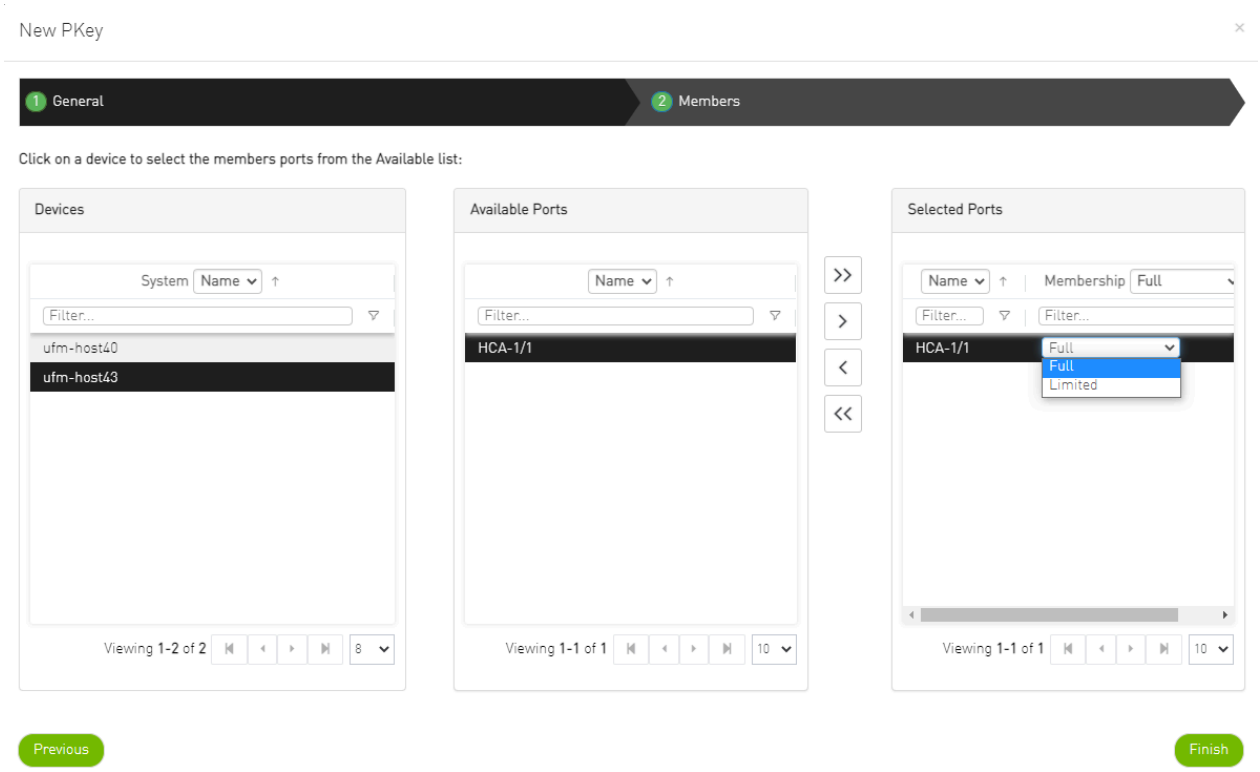


2. In the New PKey wizard, fill in the required information under the General tab:

- Name—must be between 0x1 and 0x7fff, inclusive
- Index-0 attribute—True/False
- IP Over IB attribute—True/False



3. Click "Next."
4. Under Members tab, select the device of which ports you would like to group in one PKey, and move the members (ports) from the **Available** list to the **Selected** list. For each member (port) you may specify a membership type (Full/limited).

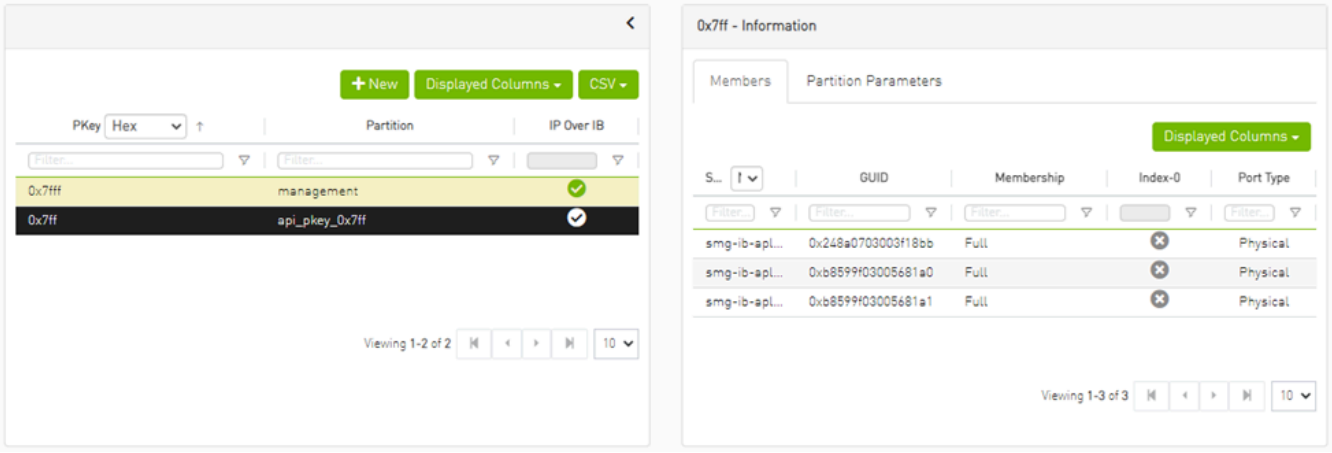


5. Click “Finish”. The new PKey will become available under the PKey window.

When selecting a PKey from the PKeys table, **PKey Information** table will appear on the right side of the screen. This table provides information on the PKey's members and QoS settings.

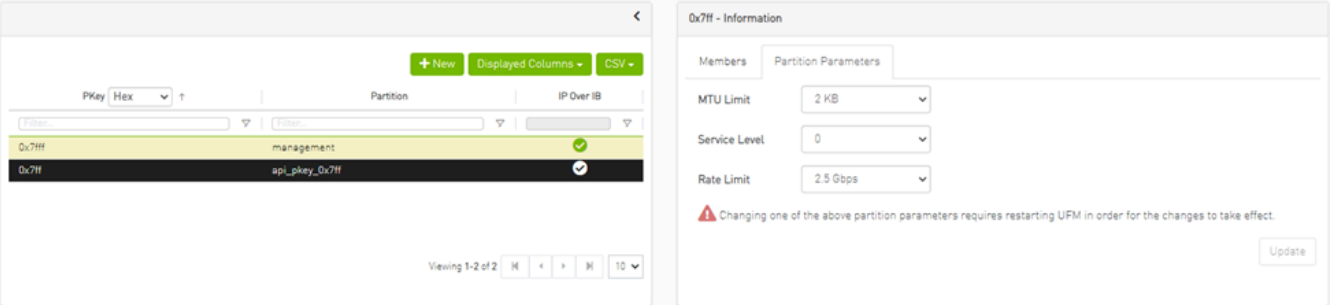
PKey Members Tab

Provides details on the PKey members: port’s hostname (node), device's IP address, port GUID, port number, membership and index-0 attributes values.



PKey QoS Tab

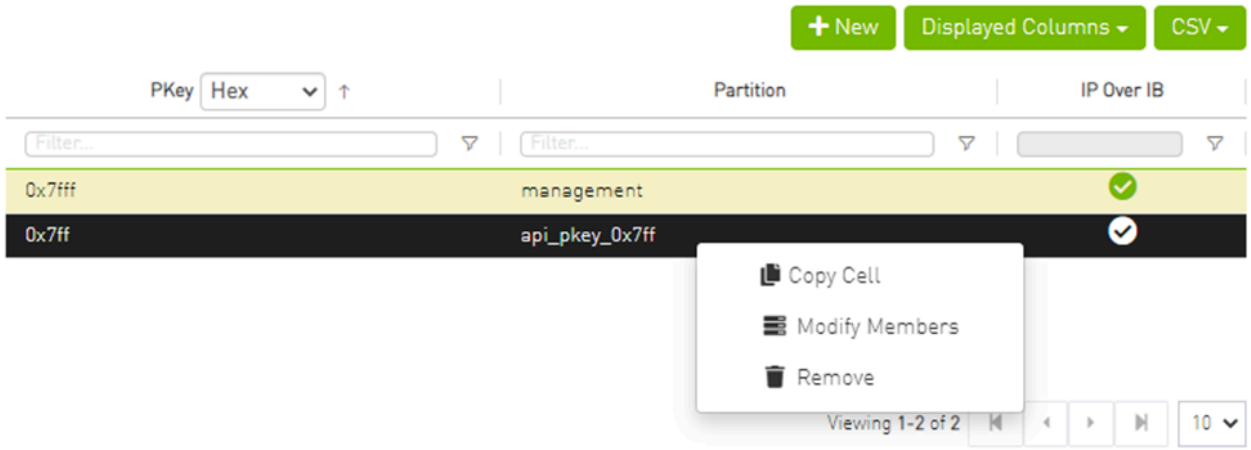
Displays the current partitioning parameter settings of the selected PKey: MTU Limit, Service Level and Rate limit. These settings can be modified by the user.



PKey Actions

Right-clicking one PKey from the list enables performing the following actions:

- **Modify Members** – PKeys can be modified either by editing the attributes under **General** tab, or updating the members under **Members** tab. Including updating ports memberships.
- **Remove** – existing PKeys can be deleted from the list.



Note

For information on partitioning, refer to Appendix – Partitioning.

Note

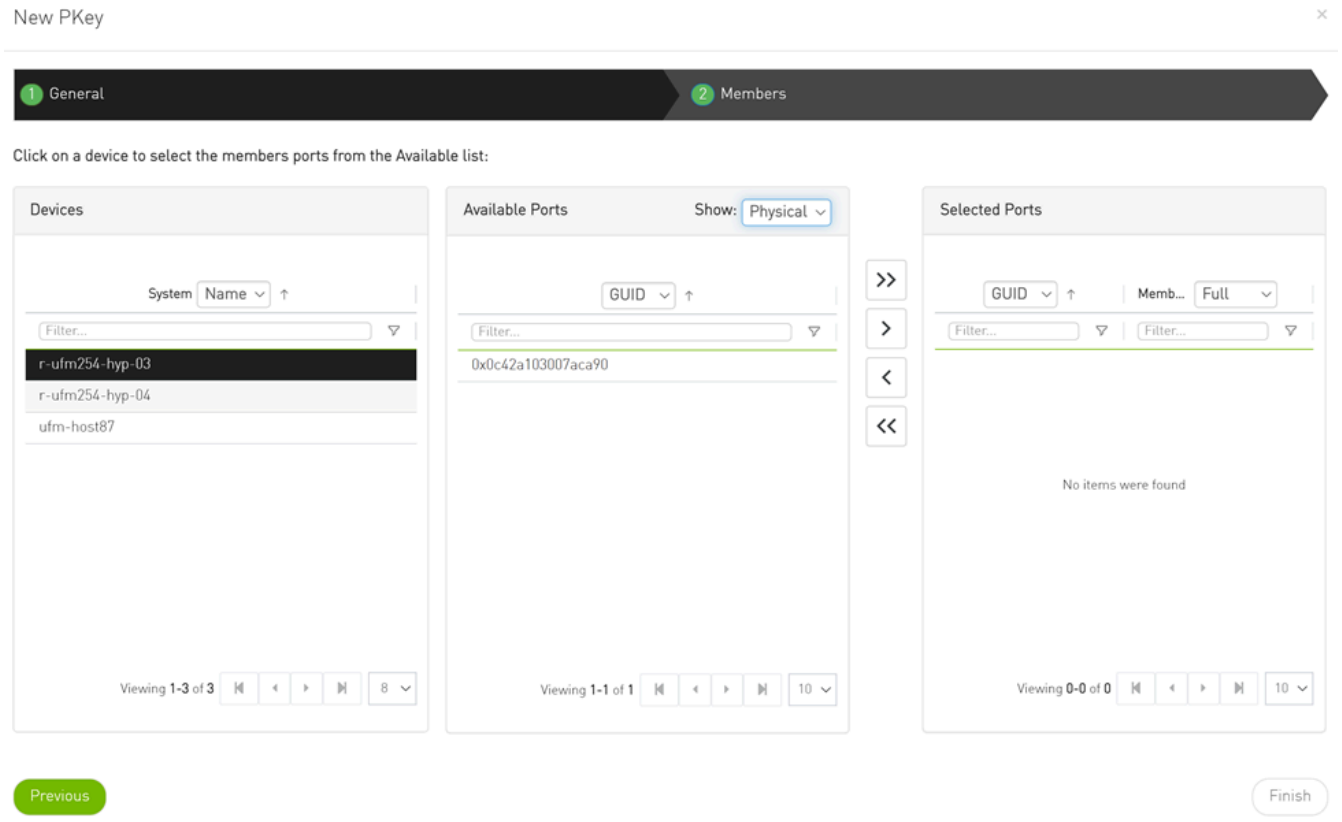
Note that restarting OpenSM is required for the QoS parameters change to take effect.

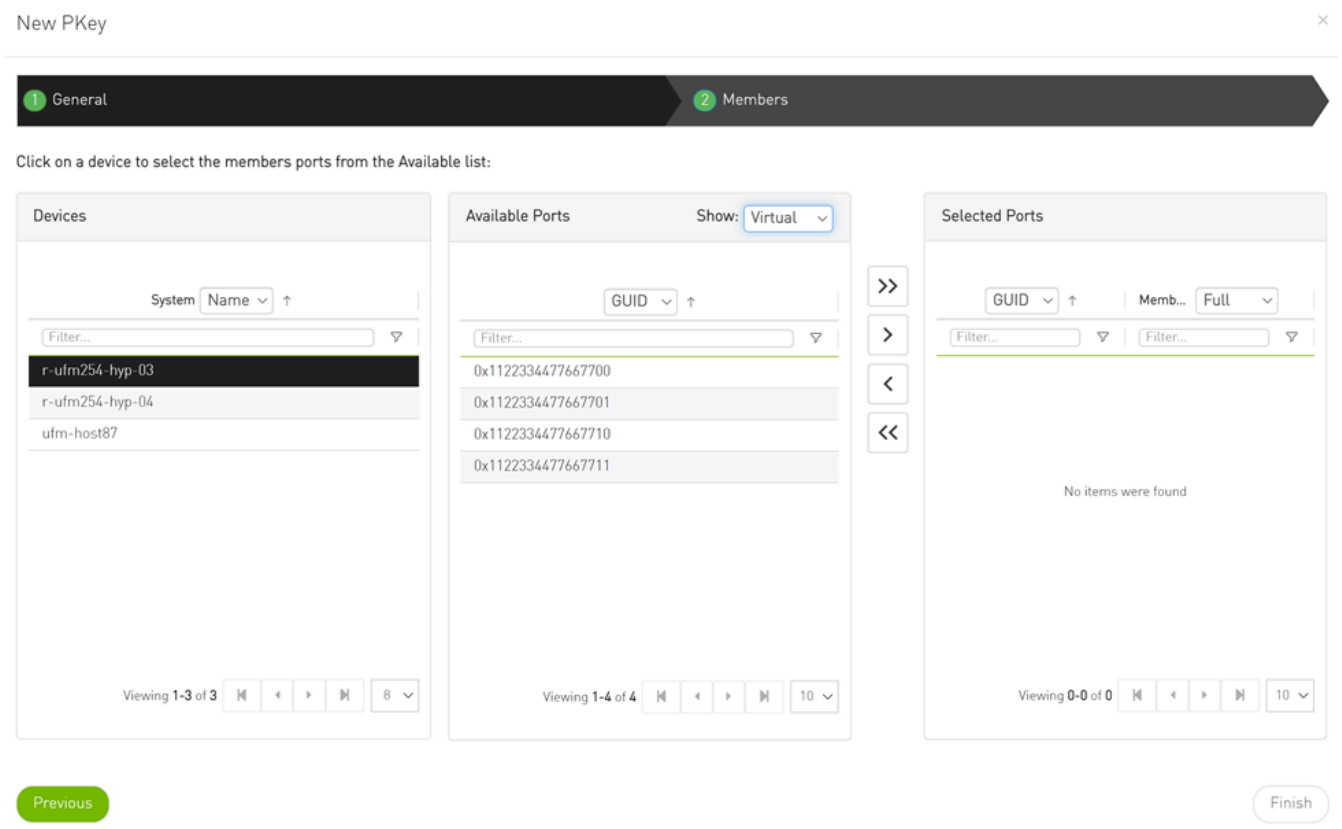
Support Pkey with Virtual Ports

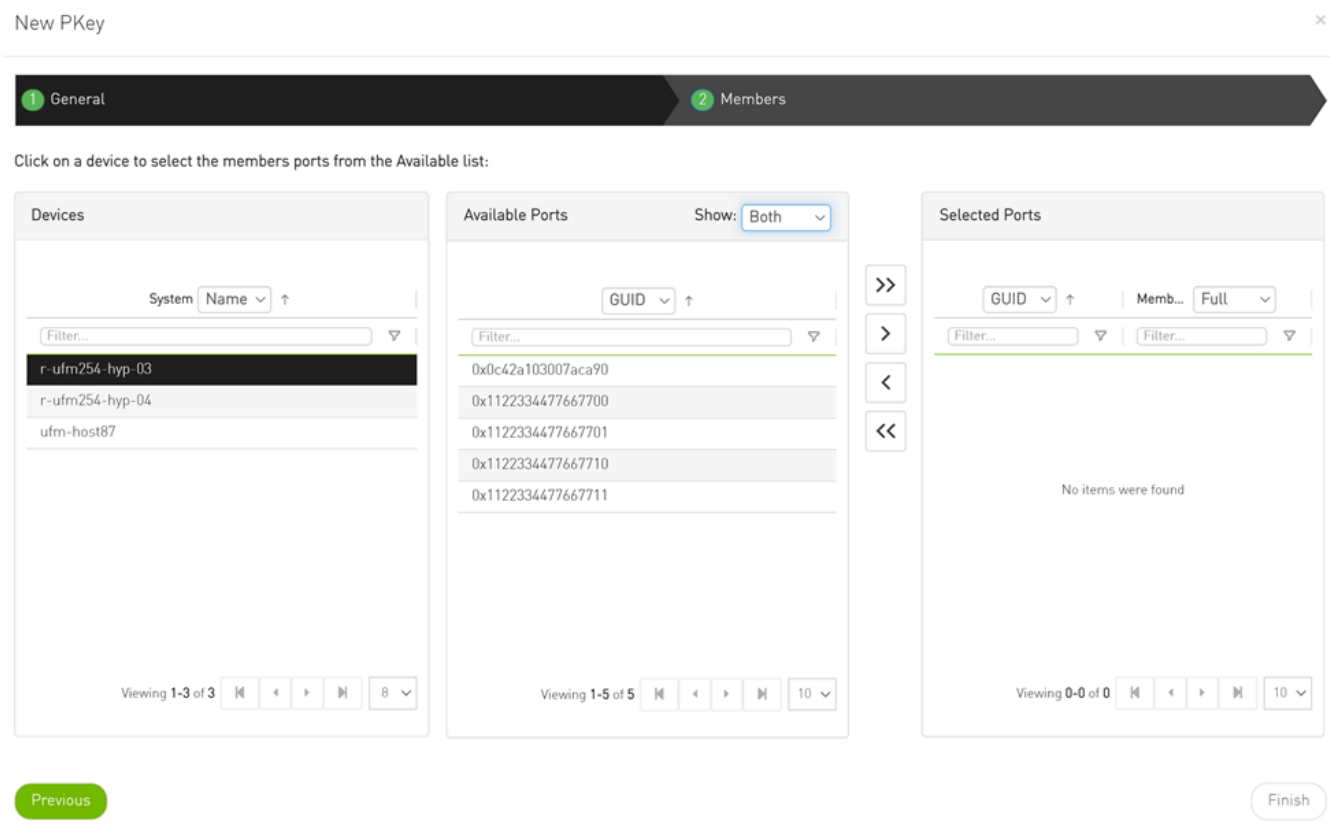
Creating a pkey with virtual ports is supported, so pkey can contain the following types of port:

- Physical
- Virtual
- Both physical and virtual

The create new pkey wizard dropdown includes port types.


New PKey
1 General
2 Members
Click on a device to select the members ports from the Available list:
Devices
System Name
Filter...
r-ufm254-hyp-03
r-ufm254-hyp-04
ufm-host87
Viewing 1-3 of 3
8
Available Ports
Show: Physical
GUID
Filter...
0x0c42a103007aca90
Viewing 1-1 of 1
10
Selected Ports
GUID
Memb... Full
Filter...
No items were found
Viewing 0-0 of 0
10
Previous
Finish


New PKey
1 General
2 Members
Click on a device to select the members ports from the Available list:
Devices
System Name
Filter...
r-ufm254-hyp-03
r-ufm254-hyp-04
ufm-host87
Viewing 1-3 of 3
8
Available Ports
Show: Virtual
GUID
Filter...
0x1122334477667700
0x1122334477667701
0x1122334477667710
0x1122334477667711
Viewing 1-4 of 4
10
Selected Ports
GUID
Memb... Full
Filter...
No items were found
Viewing 0-0 of 0
10
Previous
Finish


New PKey
1 General
2 Members
Click on a device to select the members ports from the Available list:
Devices
System Name
Filter...
r-ufm254-hyp-03
r-ufm254-hyp-04
ufm-host87
Viewing 1-3 of 3
8
Available Ports
Show: Both
GUID
Filter...
0x0c42a103007aca90
0x1122334477667700
0x1122334477667701
0x1122334477667710
0x1122334477667711
Viewing 1-5 of 5
10
Selected Ports
GUID
Memb... Full
Filter...
Filter...
No items were found
Viewing 0-0 of 0
10
Previous
Finish

HCAs Window

Provides a list of all the HCAs of the hosts in UFM. For more information, see section "HCAs Tab".