Settings

Table of contents

Note

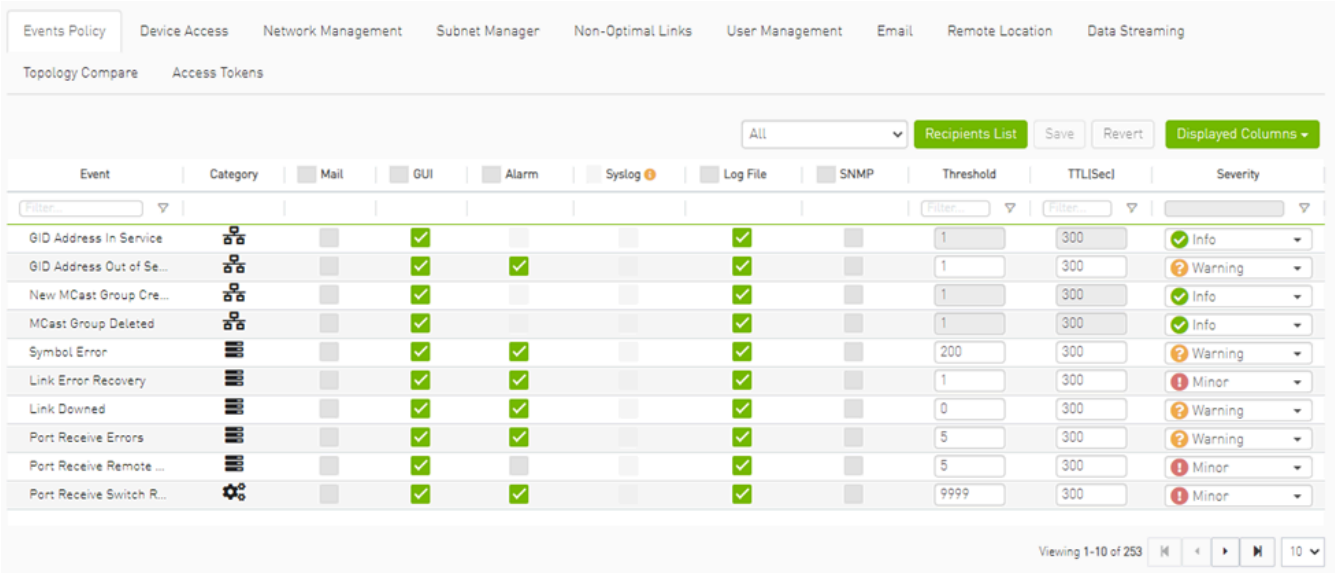
All information provided in a tabular format in UFM web UI can be exported into a CSV file.

This window enables configuring the following UFM server and fabric-related settings:

- Events Policy
- Device Access
- Network Management
- Subnet Manager Tab
- Non-Optimal Links
- User Management Tab
- Email
- Remote Location
- Data Streaming
- Topology Compare
- Token-based Authentication
- Plugin Management
- Rest Roles Access Control
- User Preferences

Events Policy

The Events Policy tab allows you to define how and when events are triggered for effective troubleshooting and fabric maintenance.



Events are reported by setting the following parameters:

Option	Description/Instructions
Event	Event description.
Category	Event category, such as Communication Error and Hardware represented by icons.
Mail	When selected, the corresponding events will be sent a list of recipients according to Configuring Email-on-Events.
Web UI	When selected, the corresponding events are displayed in the Events & Alarms window in the Web UI.
Alarm	Select the Alarm option to trigger an alarm for a specific event. When selected, the alarms will appear in the Events & Alarms window in the Web UI.
Syslog	When checked along with the Log file option, the selected events will be written to Syslog.

Option	Description/Instructions
Log File	Select the Log File option if you would like the selected event to be reported in a log file.
SNMP	The UFM Server will send events to third-party clients by means of SNMP traps. Select the event SNMP check box option to enable the system to send an SNMP trap for the specific event. The SNMP trap will be sent to the port defined in Configuration file located under: /opt/ufm/conf/gv.cfg. For further information, refer to SNMP Settings.
Threshold	An event will be triggered when the traffic/error rate exceeds the defined threshold. For example: when PortXmit Discards is set to 5 and the counter value grows by 5 units or more between two sequential reads, an event is generated.
TTL (Sec)	TTL (Alarm Time to Live) sets the time during which the alarm on the event is visible on UFM Web UI. TTL is defined in seconds. CAUTION: Setting the TTL to 0 makes the alarm permanent, meaning that the alarm does not disappear from the Web UI until cleared manually.
Action	The action that will be executed in case the event which has triggered the action can be none or isolated (make the port unhealthy or isolated). This attribute can be set only for ports event policy.
Severity	Select the severity level of the event and its alarm from the drop-down list: Info, Warning, Minor, and Critical.

Note

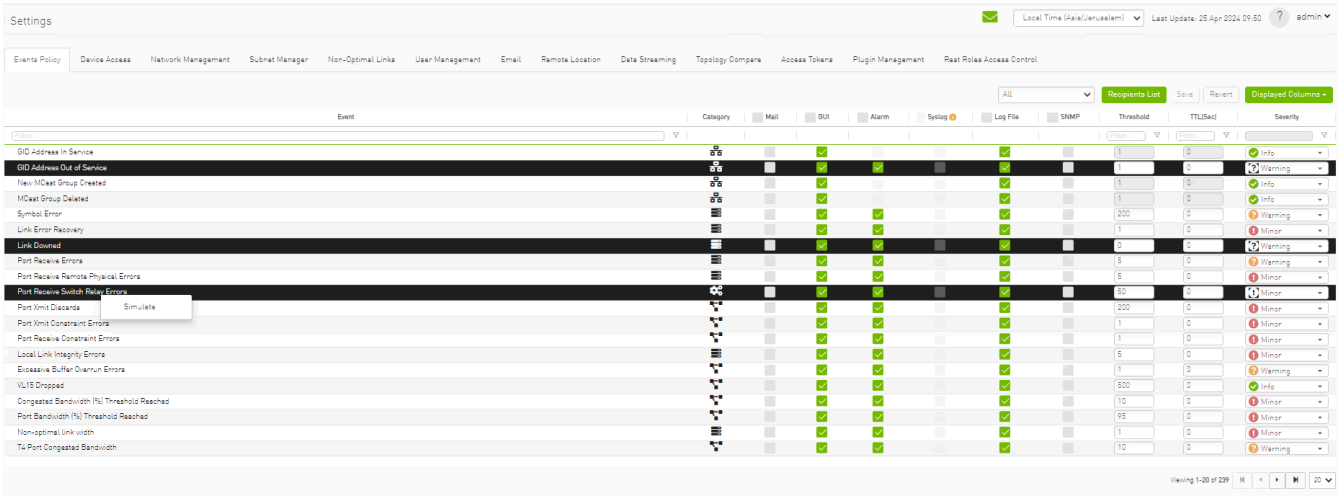
- Category column in the Events Policy table indicates to which category the event belongs. These categories are defined in the event configuration file and cannot be modified. Categories are: Hardware, Fabric Configuration, Communication Error, Fabric Notification, Maintenance, Logical Model, Fabric Topology, Gateway, Module Status, and UFM Server.
- Event logs can still be checked even if the events.log file checkbox was not checked during Syslog configuration.

- For a certain event to be sent to Syslog, both the Syslog and the Log File checkboxes must be checked. Otherwise, the selected events will not be sent to Syslog.

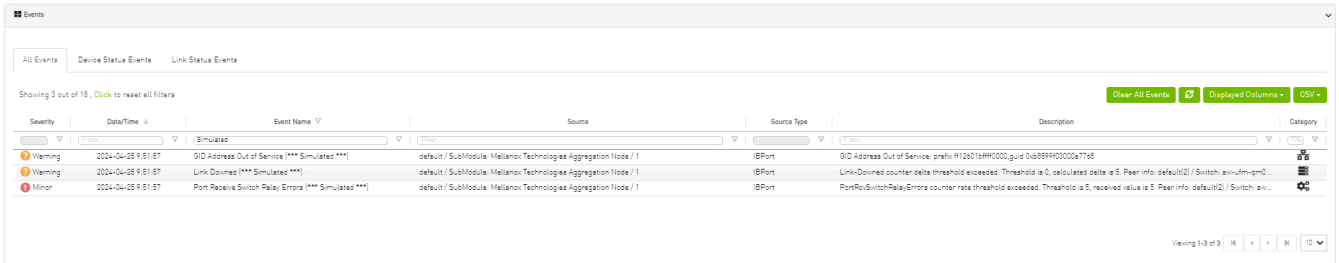
See Appendix - Supported Port Counters and Events for detailed information on port counters and events.

Events Policy Simulation

This feature enables you to simulate one or multiple event policies. To perform a simulation, choose one or multiple events from the events policy table, right-click, and then select the "Simulate" action from the context menu.



To view the simulated events policy, navigate to the Events & Alarms tab.



SNMP Settings

When UFM is running, the Web UI Policy Table shows the SNMP traps. You can then modify and save an SNMP Trap flag for each event. SNMP settings are enabled only after the installation of the UFM license.

UFM sends SNMP Trap using version SNMPV2 to the default port 162.

To set the SNMP properties:

1. Open the /opt/ufm/conf/gv.cfg configuration file.
2. Under the [Notifications] line (see the following example):
    1. Set the (snmp_listeners) IP addresses and ports
    2. Port is optional – the default port number is 162
    3. Use a comma to separate multiple listeners

    Format:

    ```
    snmp_listeners = <IP Address 1>[:<port 1>][,<IP Address 2>[:<port 2>]...]
    ```

    Example:

    ```
    [Notifications]
    snmp_listeners = host1, host2:166
    ```

Configuring Email-on-Events

UFM enables you to configure each event to be sent by email to a list of pre-defined recipients. Every 5 minutes (configurable) UFM will collect all “Mail” selected events and send them to the list of pre-defined recipients. By default, the maximum number of events which can be sent in a single email is 100 (configurable, should be in the range of 1–1000)

The order of events in the email body can be set as desired. The available options are: order by severity or order by time (by default: order by severity)

To change email-on-events setting, do the following:

1. Edit the /opt/ufm/conf/gv.cfg file.

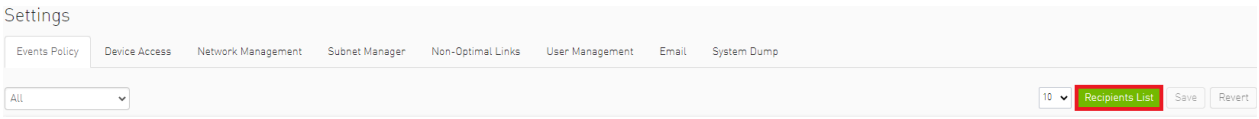
2. Go to section “[Events]” and set the relevant parameters:

    - sending_interval (default=5)—Time interval for keeping events (minimum 10 seconds, maximum 24 hours)
    - sending_interval_unit (default = minute)—Optional units: minute, second, hour
    - cyclic_buffer (default=false)—If the cyclic buffer is set to true, older events will be dropped, otherwise newer events will be dropped (if reaches max count)
    - max_events (default=100)—Maximum number of events to be sent in one mail (buffer size), should be in the range of 1–1000
    - group_by_severity (default=true)—Group events in mail by severity or by time

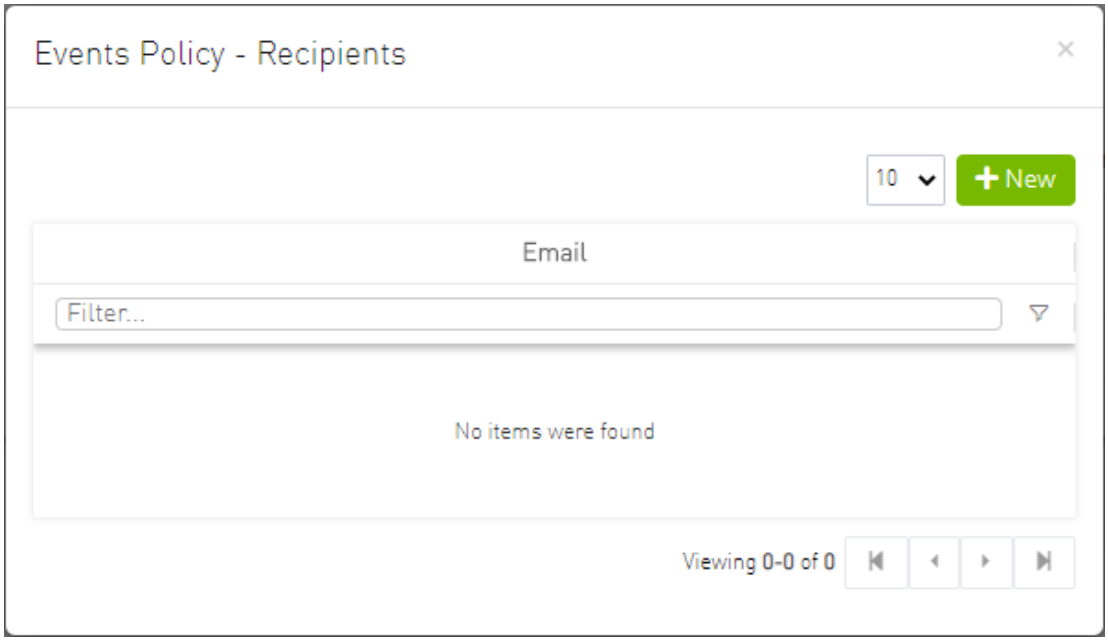
To receive the email-on-events, do the following:

> **Note**
>
> Configure SMTP settings under Settings window Email tab – see Email Tab.

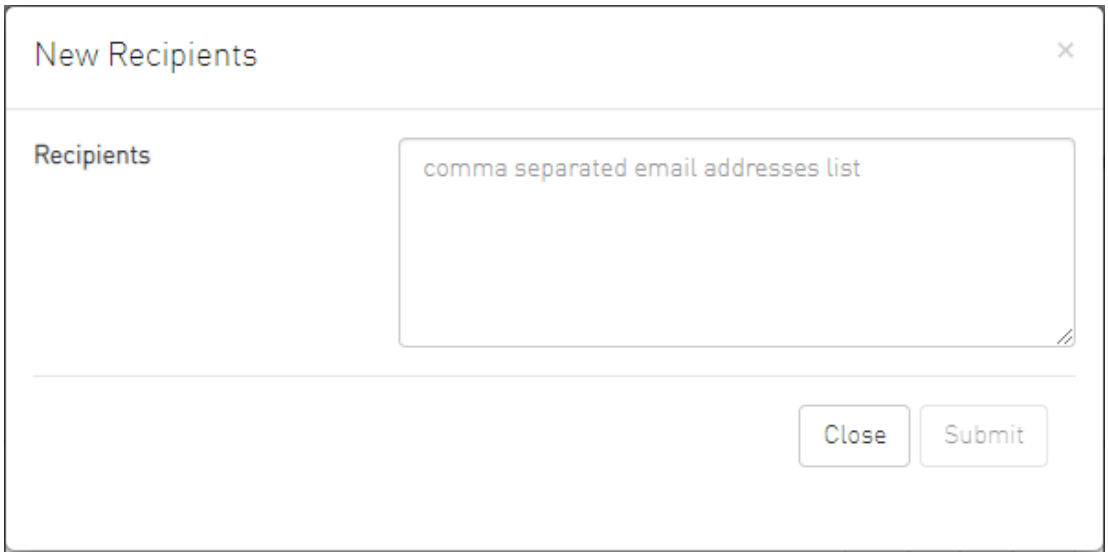
1. Configure the **Recipients List** under Settings Events Policy.



2. Click **New**.



3. In the Recipients List window, enter valid recipient email addresses, comma-separated, and click **Submit**.



The new recipients are then added to the Events Policy Recipients list.

These recipients automatically start receiving emails on the events for which the Mail checkbox is checked in the table under Events Policy.

Device Access

You can configure default access parameters for remote administration via the following protocols:

- **Switch SSH** – allows you to define the SSH parameters to open an SSH session on your switch
- **Server SSH -** allows you to define the SSH parameters to open an SSH session on your server
- **HTTP** – allows you to define the HTTP parameters to open an HTTP session on your device

  Default credentials are applicable to all switches and servers in the fabric.

> **Note**
>
> The default SSH (CLI) switch credentials match the Grid Director series switch. To change the credentials for IS5030/IS5035 edit the [SSH_Switch] section in the gv.cfg file.

Define access parameters for the remote user as described in the following table.

Site Access Credential Parameters

Parameter	Description
User	The name of the user allowed remote access.
Password	Enter the user password.
Confirmation	Re-enter the password.

Parameter	Description
Port	Each communication protocol has a default port for connection. You can modify the port number, if required.
Timeout	Each communication protocol has a default timeout, i.e. the maximum time, in seconds, to wait for a response from the peer. You can modify the timeout, if required.
Save the current password for fallback checkbox	This checkbox should be checked in case if you require the previous password to remain operational. This feature is beneficial during the period when the global switch password is changed for large-scale fabrics due to security considerations. It is only applicable for the MLNX_OS (HTTP) credentials type. By default, the value is set to false.

Network Management

UFM achieves maximum performance with latency-critical tasks by implementing traffic isolation, which minimizes cross-application interference by prioritizing traffic to ensure critical applications get the optimal service levels.

UFM Routing Protocols

UFM web UI supports the following routing engines:

- MINHOP – based on the minimum hops to each node where the path length is optimized (i.e., shortest path available).
- UPDN – also based on the minimum hops to each node but it is constrained to ranking rules. Select this algorithm if the subnet is not a pure Fat Tree topology and deadlock may occur due to a credit loops in the subnet.
- DNUP – similar to UPDN, but allows routing in fabrics that have some channel adapter (CA) nodes attached closer to the roots than some switch nodes.
- File-Based (FILE) – The FILE routing engine loads the LFTs from the specified file, with no reaction to real topology changes.
- Fat Tree – an algorithm that optimizes routing for congestion-free "shift" communication pattern.

  Select Fat Tree algorithm if a subnet is a symmetrical or almost symmetrical fat-tree. The Fat Tree also optimizes K-ary-N-Trees by handling non-constant K in cases where leafs (CAs) are not fully staffed, and the algorithm also handles any Constant Bisectional Bandwidth (CBB) ratio. As with the UPDN routing algorithm, Fat Tree routing is constrained to ranking rules.

  - Quasi Fat Tree – PQFT routing engine is a closed formula algorithm for two flavors of fat trees
  - Quasi Fat Tree (QFT)

    - Parallel Ports Generalized Fat Tree (PGFT)

      PGFT topology may use parallel links between switches at adjacent levels, while QFT uses parallel links between adjacent switches in different sub-trees. The main motivation for that is the need for a topology that is not just optimized for a single large job but also for smaller concurrent jobs.

- Dimension Order Routing (DOR) – based on the Min Hop algorithm, but avoids port equalization, except for redundant links between the same two switches. The DOR algorithm provides deadlock-free routes for hypercubes, when the fabric is cabled as a hypercube and for meshes when cabled as a mesh.

- Torus-2QoS – designed for large-scale 2D/3D torus fabrics. In addition, you can configure Torus-2QoS routing to be *traffic aware*, and thus optimized for neighbor-based traffic.

- Routing Engine Chain (Chain) – an algorithm that allows configuring different routing engines on different parts of the IB fabric.

- Adaptive Routing (AR) – enables the switch to select the output port based on the port's load. This option is not available via UFM Web UI.

    - AR_UPDN

    - AR_FTREE

    - AR_TORUS

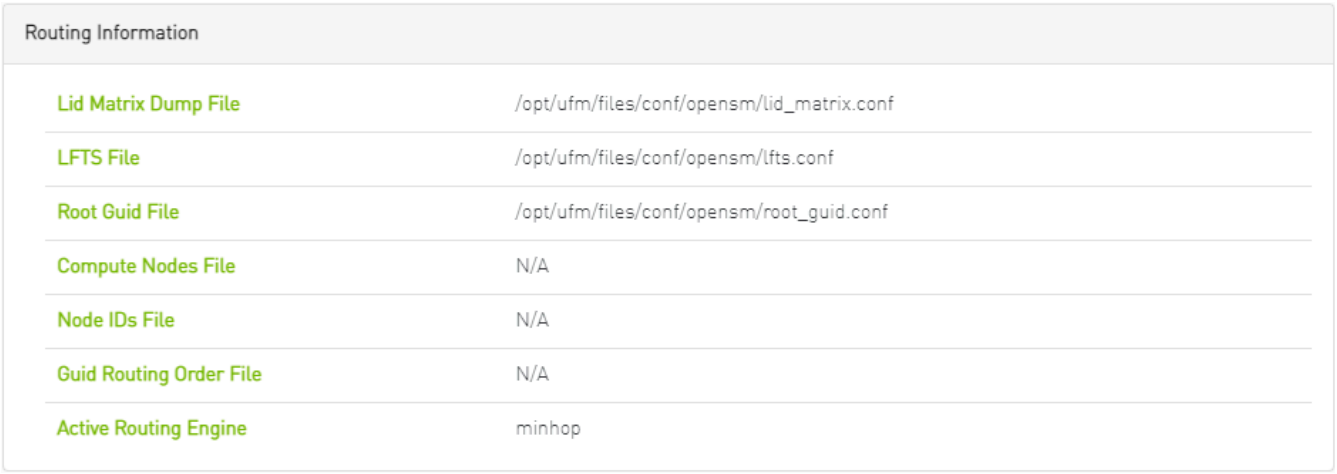
    - AR_DOR

- Dragonfly+ (DFP, DPF2)

Configuring Routing Protocol

Network Management tab enables setting the preferred routing protocol supported by the UFM software, as well as routing priority.

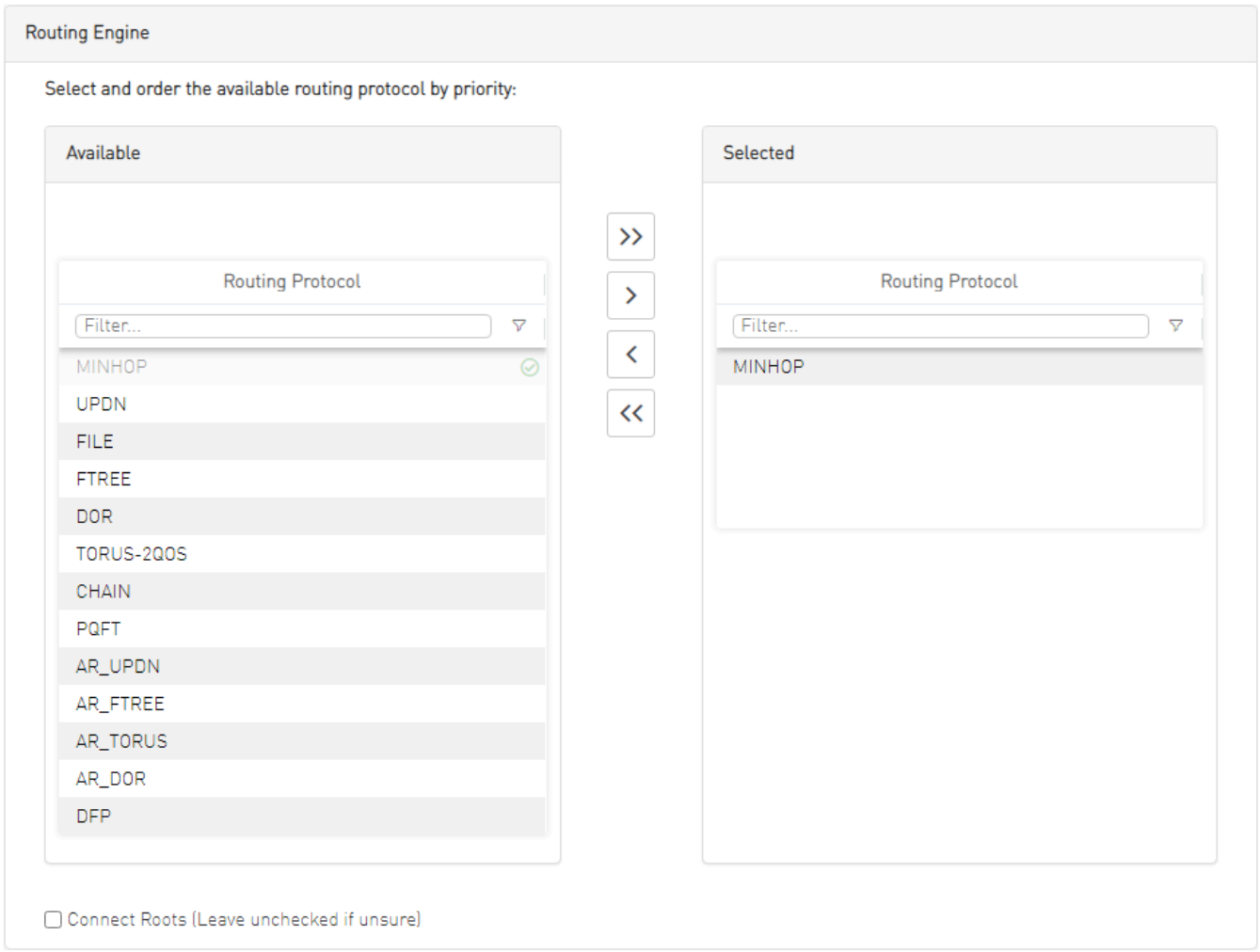
To set the desired routing protocol, move one routing protocol or more from the **Available** list to the **Selected** list, and click "Save" in the upper right corner.



The protocol at the top of the list has the highest priority and will be chosen as the **Active Routing Engine**. If the settings for this protocol are not successful, UFM takes the next available protocol.

Routing Information is listed on the top of the screen:

Field/Box	Description
LID Matrix Dump File	File holding the LID matrix dump configuration
LFTS File	File holding the LFT routing configuration
Root GUID File	File holding the root node GUIDS (for fat-tree or Up/Down)
Compute Nodes File	File holding GUIDs of compute nodes for fat-tree routing algorithm
GUID Routing Order File	File holding the routing order GUIDs (for MinHop and Up/Down)
Node IDs File	File holding the node IDs
Active Routing Engine	The current active routing algorithm used by the managing OpenSM


Routing Engine
Select and order the available routing protocol by priority:
Available
Routing Protocol
Filter...
MINHOP
UPDN
FILE
FTREE
DOR
TORUS-2QOS
CHAIN
PQFT
AR_UPDN
AR_FTREE
AR_TORUS
AR_DOR
DFP
Selected
Routing Protocol
Filter...
MINHOP
Connect Roots (Leave unchecked if unsure)

Subnet Manager Tab

UFM is a management platform using a user-space application for InfiniBand fabric management. This application is developed within the context of an open-source environment. This application serves as an InfiniBand Subnet Manager and a Subnet Administration tool.

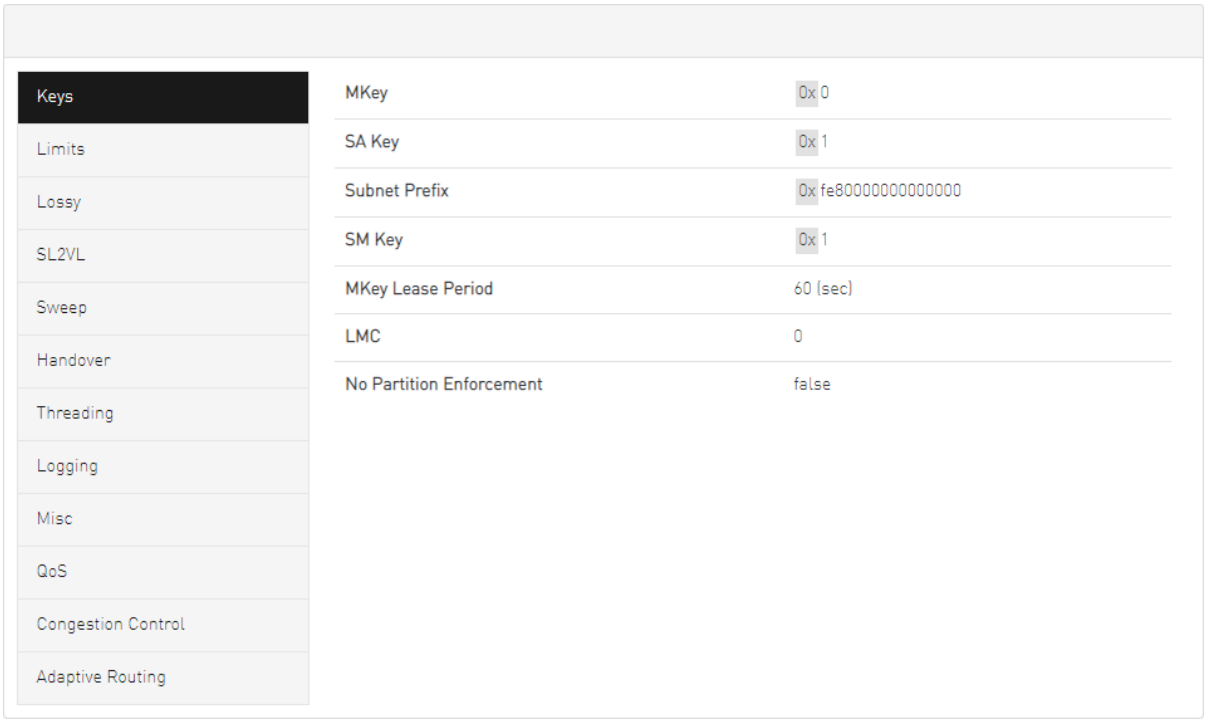
The UFM Subnet Manager (SM) is a centralized entity running on the server that discovers and configures all the InfiniBand fabric devices to enable traffic flow throughout the fabric.

To view and configure SM parameters in the ***Subnet Manager*** tab, select the relevant tab according to the required configuration.

For more information, please refer to Appendix – Enhanced Quality of Service.

SM Keys Configuration

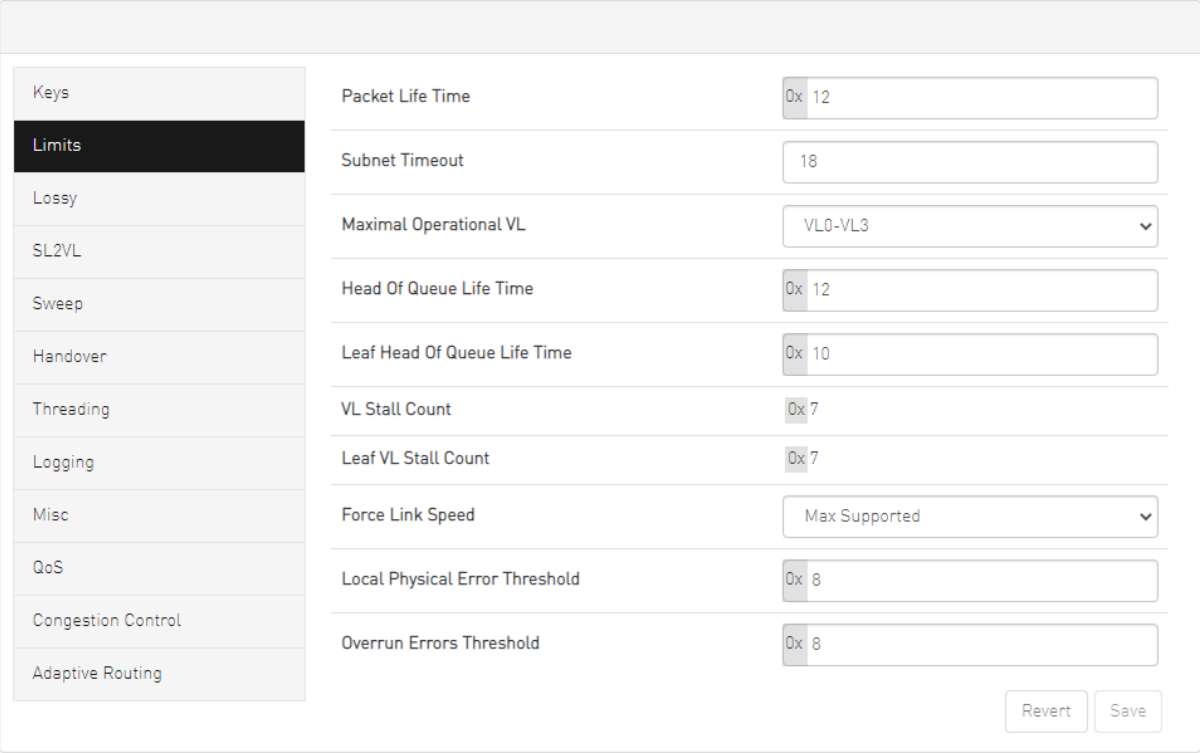
The SM Keys tab enables you to view the Subnet Manager Keys. You cannot change the configuration in this tab.



Field	Description	Default
MKey	A field that allows you to view or edit the M_Key value sent to all ports to qualify all the set (PortInfo). Authentication is performed by the management entity at the destination port and is achieved by comparing the key contained in the SMP with the key (the M_Key Management key) residing at the destination port.	0x0000000000000000
SA Key	Shows the SM_Key value to qualify the receive SA queries as 'trusted'.	0x0000000000000001
Subnet Prefix	An identifier of the subnet. The subnet prefix is used as the most significant 64 bit of the GID of each InfiniBand node in the subnet.	0xfe8000000000000
SM Key	Read-only field that displays the Key of the Subnet Manager (SM).	0x0000000000000001
MKey Lease Period	A field that allows you to view or edit the lease period used for the M_Key on this subnet in [sec].	0
LMC	Defines the LID Mask Control value for the SM. Possible values are 0 to 7. LID Mask Control (LMC) allows you to assign more than one LID per port. NOTE: Changes to the LMC parameter require a UFM restart.	0
No Partition Enforcement	Disables partition enforcement by switches.	Disabled

SM Limits Configuration

The SM Limits tab enables you to view and set the Subnet Manager Limits.



To configure SM Limits, set the fields as described in the table below, and click “Save."

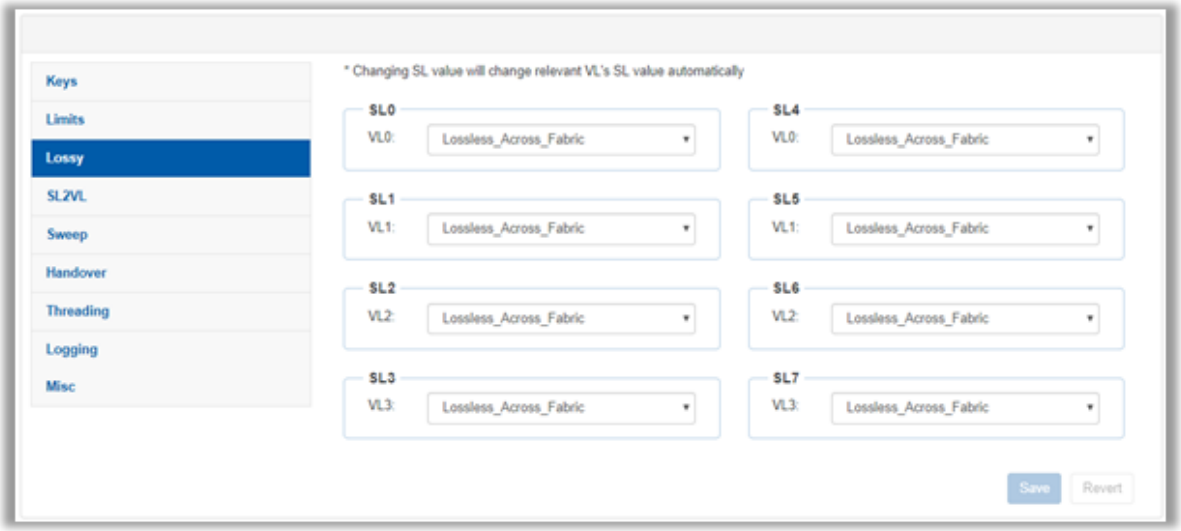
Field	Description	Default
Packet Life Time	A field that allows you to view and/or edit the code of maximum lifetime a packet in a switch. The actual time is 4.096 usec * 2^<packet_life_time>. The value 0x14 disables this mechanism	0x12
Subnet Timeout	A field that allows you to view and/or edit the subnet_timeout code that will be set for all the ports. The actual timeout is 4.096usec * 2^<subnet_timeout>	18
Maximal Operational VL	A field that allows you to view and/or edit the limit of the maximal operational VLs: • 0: NO_CHANGE • 1: VL0 1 • 2: VL0_VL1 • 3: VL0_VL3 • 4: VL0_VL7 • 5: VL0_VL14	3

Field	Description	Default
Head of Queue Life Time	A field that allows you to view and/or edit the code of maximal time a packet can wait at the head of transmission queue. The actual time is 4.096usec * 2^<head of queue lifetime> The value 0x14 disables this mechanism.	0x12
Leaf Head of Queue Life Time	A field that allows you to view and/or edit the maximum time a packet can wait at the head of queue on a switch port connected to a CA or gateway port.	0x10
VL Stall Count	A field that allows you to view the number of sequential packets dropped that cause the port to enter the VLStalled state. The result of setting this value to zero is undefined.	0x07
Leaf VL Stall Count	This field allows you to view the number of sequential packets dropped that cause the port to enter the VLStalled state. This value is for switch ports driving a CA or gateway port. The result of setting the parameter to zero is undefined.	0x07
Force Link Speed	A parameter that allows you to modify the PortInfo:LinkSpeedEnabled field on switch ports. If 0, do not modify. • Values are: • 1: 2.5 Gbps • 3: 2.5 or 5.0 Gbps • 5: 2.5 or 10.0 Gbps • 7: 2.5 or 5.0 or 10.0 Gbps • 2,4,6,8-14 Reserved • 15: set to PortInfo:LinkSpeedSupported	15 By default, UFM sets the enabled link speed equal to the supported link speed.
Local Physical Error Threshold	A field that allows you to view and/or edit the threshold of local phy errors for sending Trap 129.	0x08
Overrun Errors Threshold	A field that allows you to view and/or edit the threshold of credit overrun errors for sending Trap 130.	0x08

SM Lossy Manager Configuration

> **Note**
>
> This tab is available to users with an advanced license only.

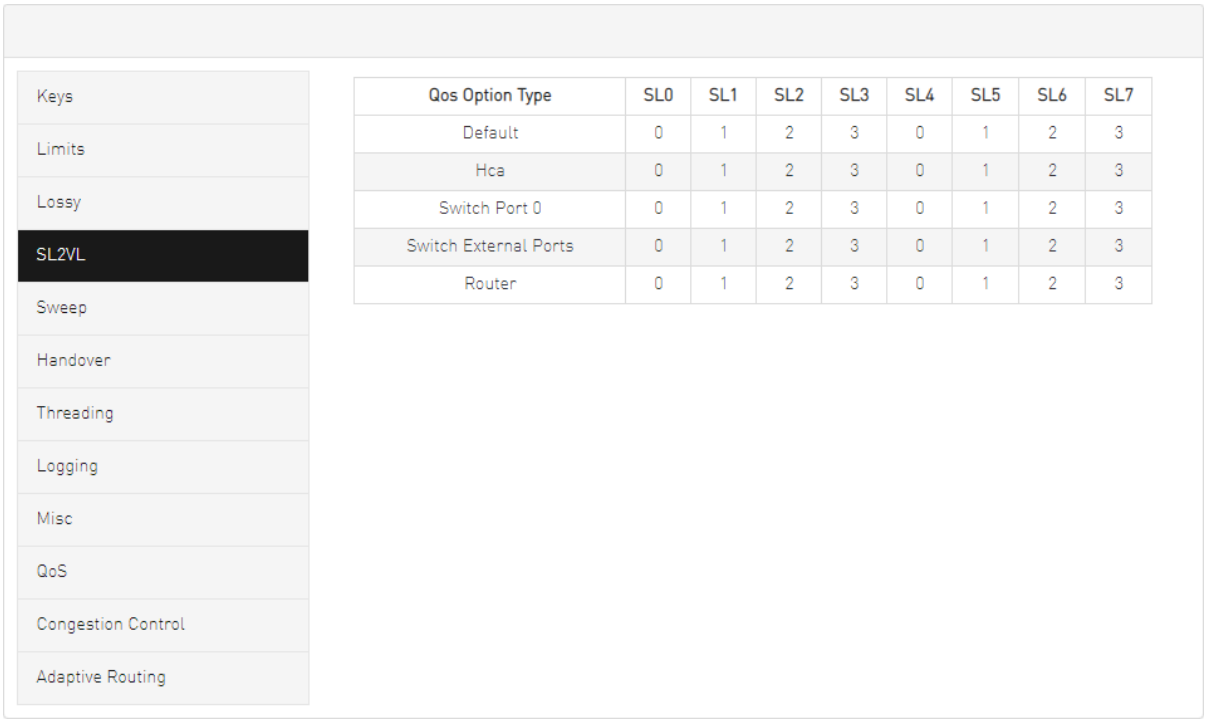
The SM Lossy tab enables you to view and set the Lossy Configuration Manager options after Lossy Configuration has been enabled.



SM SL2VL Mapping Configuration

The SM SL2VL tab enables you to view the SL (service level) to VL (virtual lane) mappings and the configured Lossy Management. You cannot change the configuration in this tab.

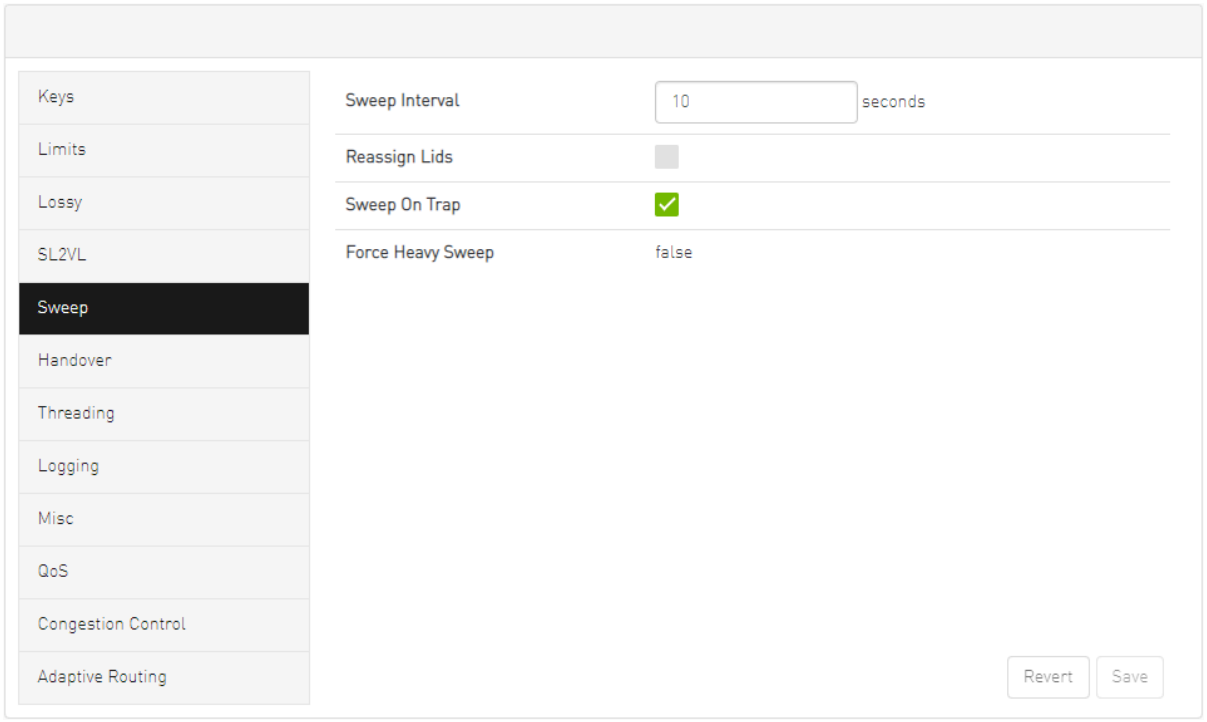
However, you can change it in the previous SM Lossy Manager Configuration (Advanced License only) tab.



Qos Option Type	SL0	SL1	SL2	SL3	SL4	SL5	SL6	SL7
Default	0	1	2	3	0	1	2	3
Hca	0	1	2	3	0	1	2	3
Switch Port 0	0	1	2	3	0	1	2	3
Switch External Ports	0	1	2	3	0	1	2	3
Router	0	1	2	3	0	1	2	3

SM Sweep Configuration

The Sweep tab enables you to view and/or set the Subnet Manager Sweep Configuration parameters.

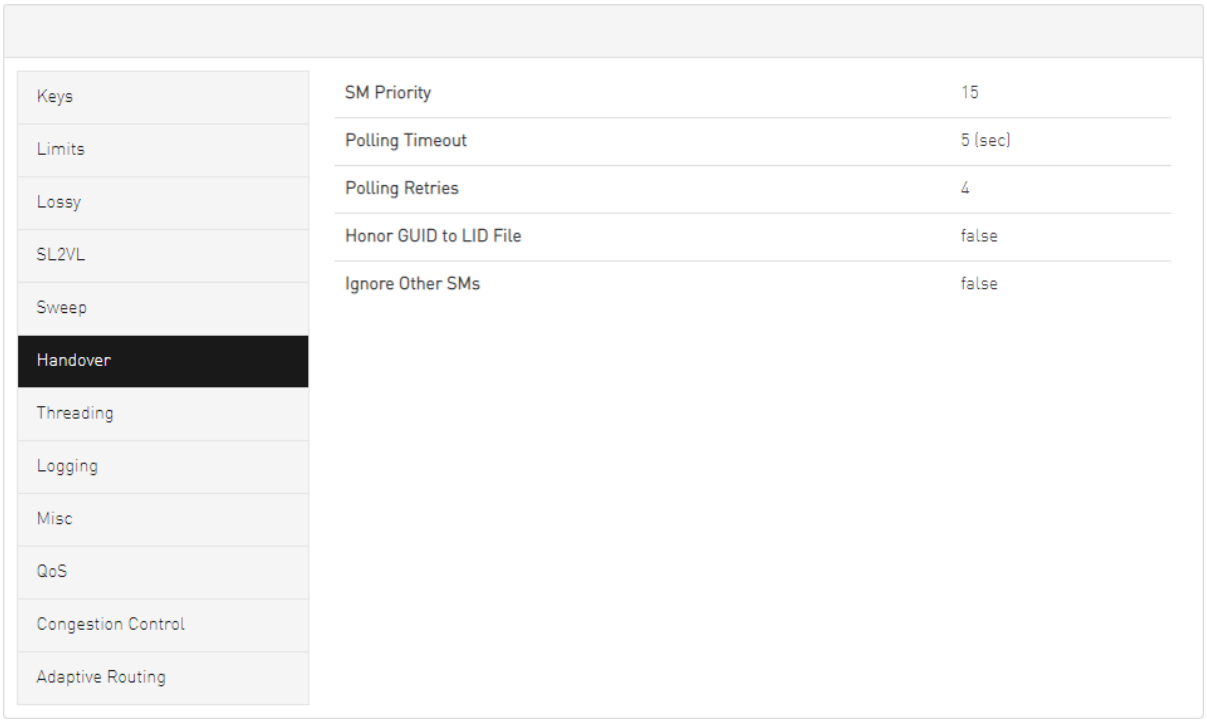


To configure SM Sweep, set the fields as described in the table below and click “Save."

Field/Box	Description	Default
Sweep Interval	A field that allows you to view and/or edit the number of seconds between light sweeps (0 disables it).	10
Reassign LIDs	If enabled, causes all LIDs to be reassigned.	Disabled
Sweep on Trap	If enabled, traps 128 and 144 will cause a heavy sweep.	Enabled
Force Heavy Sweep	If enabled, forces every sweep to be a heavy sweep.	Disabled

SM Handover Configuration

The SM Handover tab enables you to view the Subnet Manager Handover Configuration parameters. You cannot change the configuration in this tab.

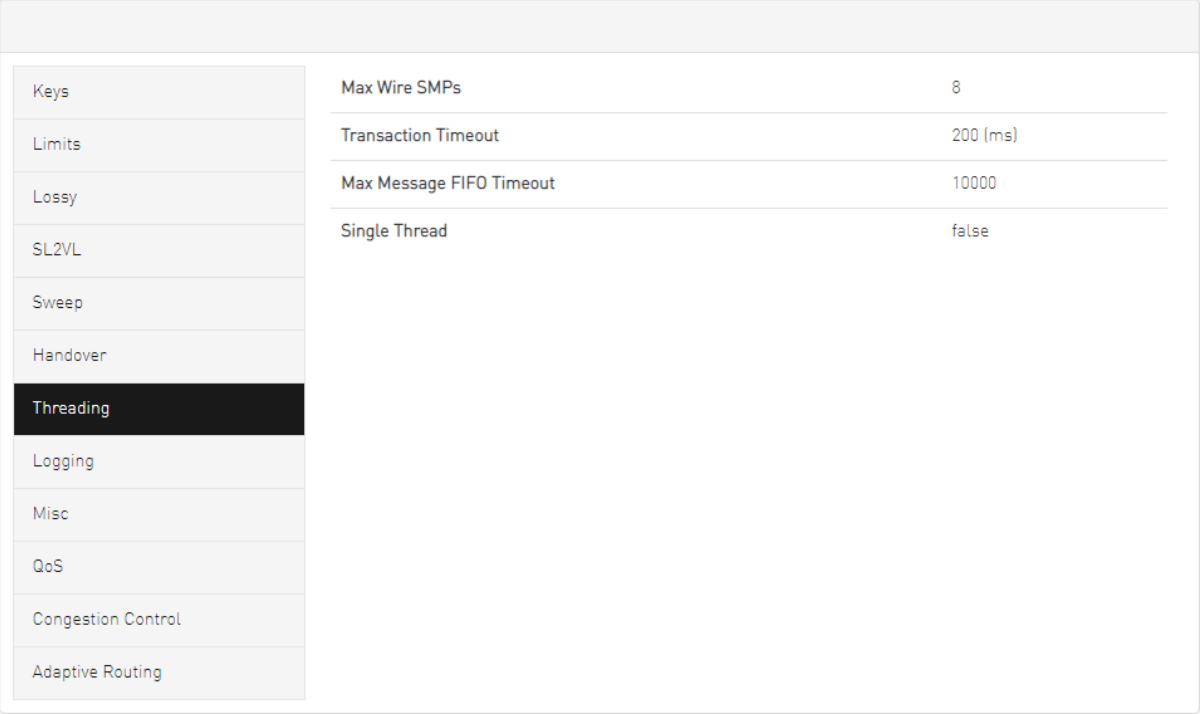


Field/Box	Description	Default
SM Priority	A field that shows the SM priority used for determining the master. Range is 0 (lowest priority) to 15 (highest). Note: Currently, these settings may not be changed.	15

Field/Box	Description	Default
Polling Timeout	A field that shows the timeout in [sec] between two polls of active master SM.	Range=10000
Polling Retries	Number of failing polls of remote SM that declares it "not operational."	4
Honor GUID to LID File	If enabled, honor the guid2lid file when coming out of standby state, if the file exists and is valid.	Disabled
Ignore other SMs	If enabled, other SMs on the subnet are ignored.	Disabled

SM Threading Configuration

The SM Threading tab enables you to view the Subnet Manager Timing and Threading Configuration parameters. You cannot change the configuration in this tab.

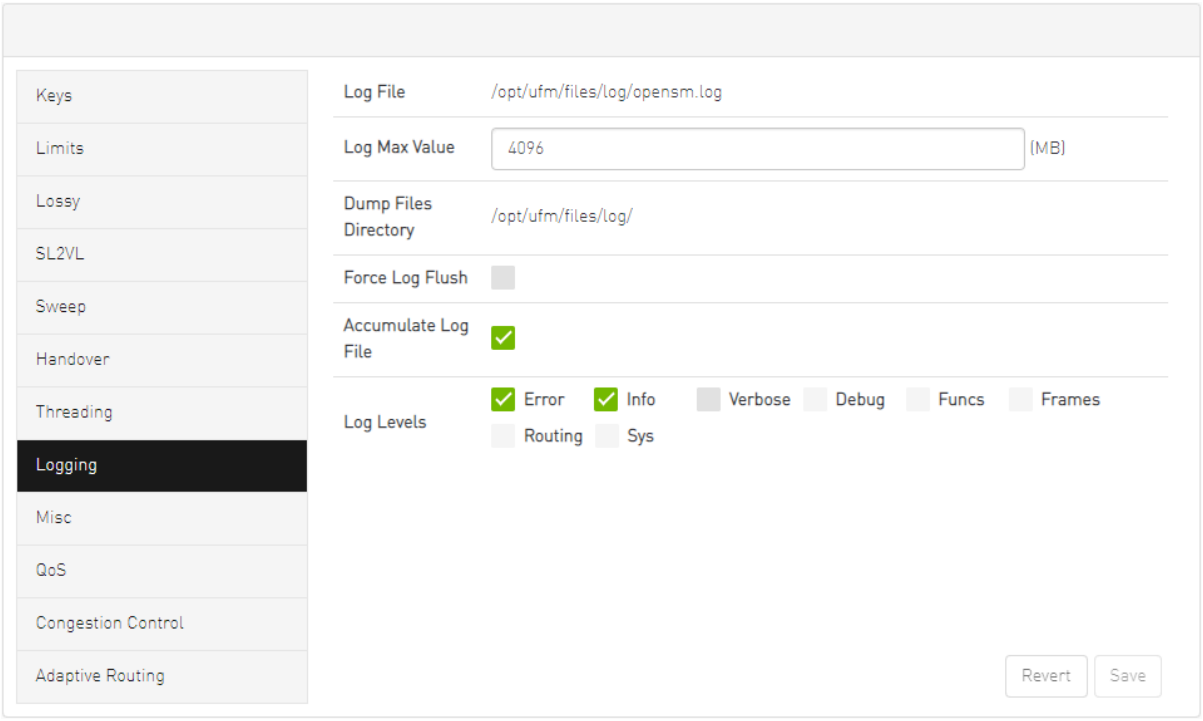


Field/Box	Description	Default
Max Wire SMPs	A field that shows the maximum number of SMPs sent in parallel.	4

Field/Box	Description	Default
Transaction Timeout	A field that shows the maximum time in [msec] allowed for a transaction to complete.	200
Max Message FIFO Timeout	A field that shows the maximum time in [msec] a message can stay in the incoming message queue.	10000
Single Thread	When enabled, a single thread is used for handling SA queries.	Disabled

SM Logging Configuration

The SM Logging tab enables you to view and/or set the **Subnet Manager Logging Configuration** parameters.



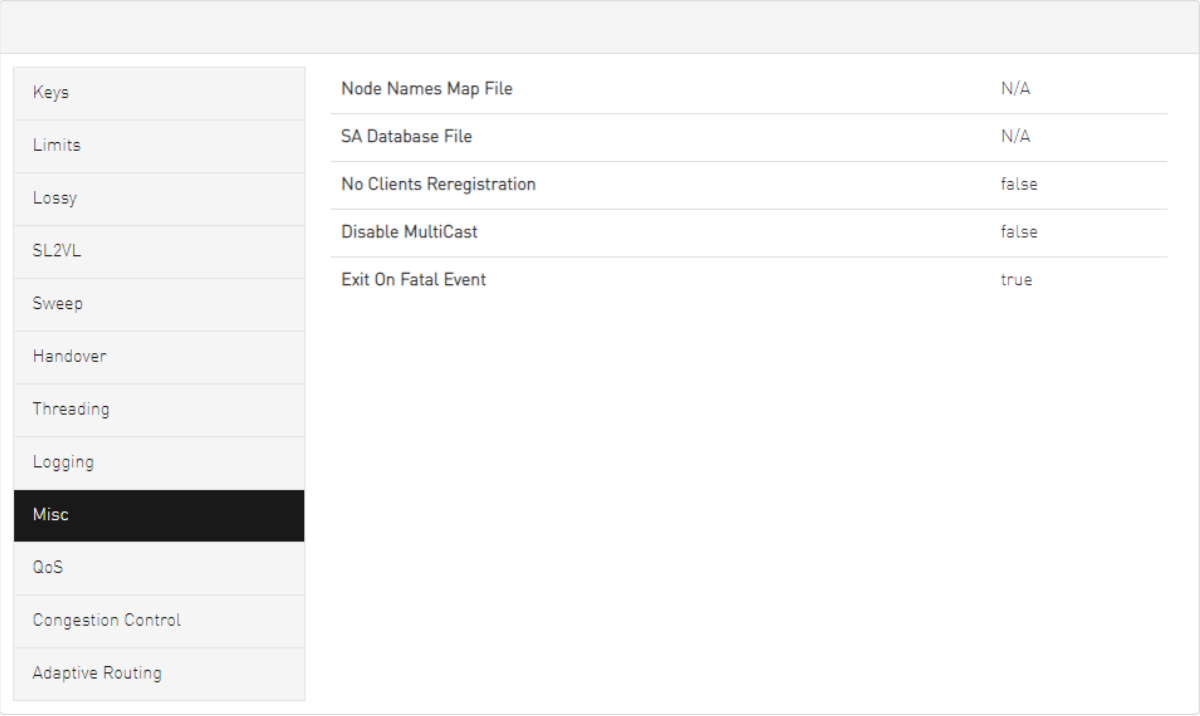
To configure SM Logging, set the fields as described in the table below and click “Save."

Field/Box	Description	Default
Log File	Path of the Log file to be used.	cond/opt/ufm/files/log/opensm.log
Log Max Size	A field that allows you to view and/or edit the size limit of the log file in MB. If overrun, the log is restarted.	4096

Field/Box	Description	Default
Dump Files Directory	The directory that holds the SM dump file.	/opt/ufm/files/log
Force Log Flush	Force flush to the log file for each log message.	Disabled
Accumulate Log File	If enabled, the log accumulates over multiple SM sessions.	Enabled
Log Levels	Available log levels: Error, Info, Verbose, Debug, Funcs, Frames, Routing, and Sys.	Error and Info

SM Miscellaneous Settings

The Misc tab enables you to view additional **Subnet Manager Configuration** parameters. You cannot change the configuration in this tab.

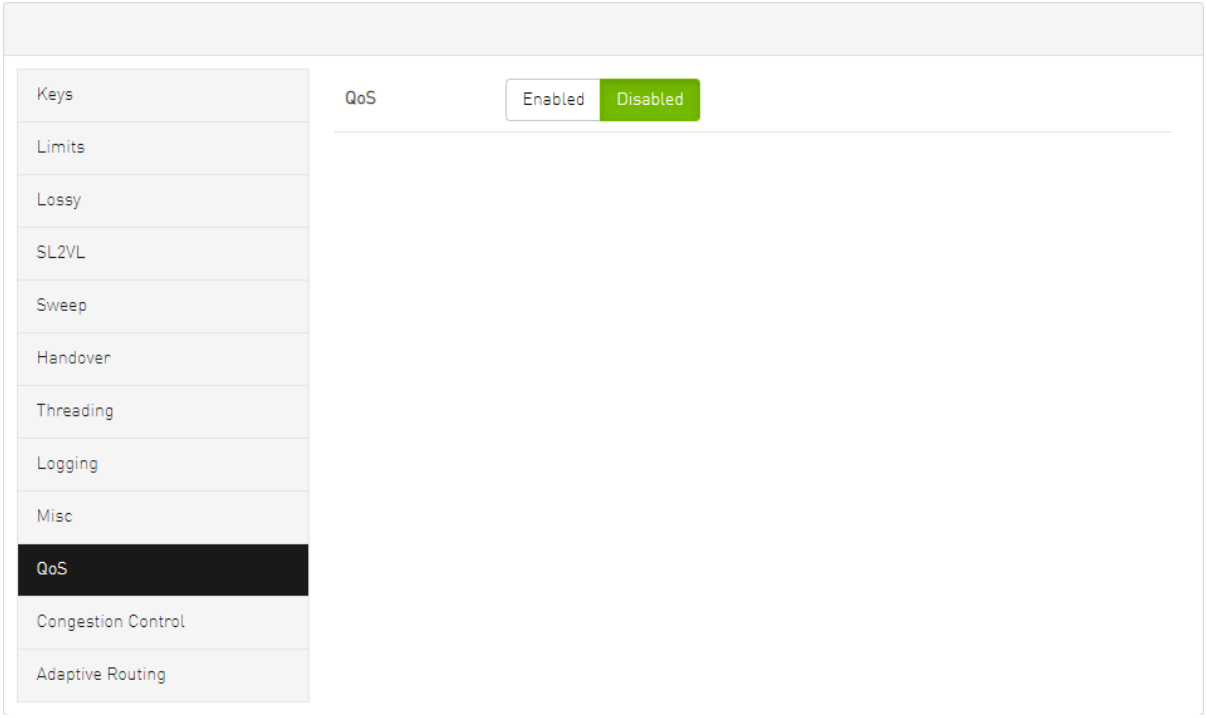


Field/Box	Description	Default
Node Names Map File	A field that allows you to view and/or set the node name map for mapping nodes to more descriptive node descriptions.	None

Field/Box	Description	Default
SA Database File	SA database file name	None
No Clients Reregistration	If enabled, disables client re-registration.	Disabled
Disable Multicast	If enabled, the SM disables multicast support and no multicast routing is performed.	Disabled
Exit on Fatal Event	If enabled, the SM exits on fatal initialization issues.	Enabled

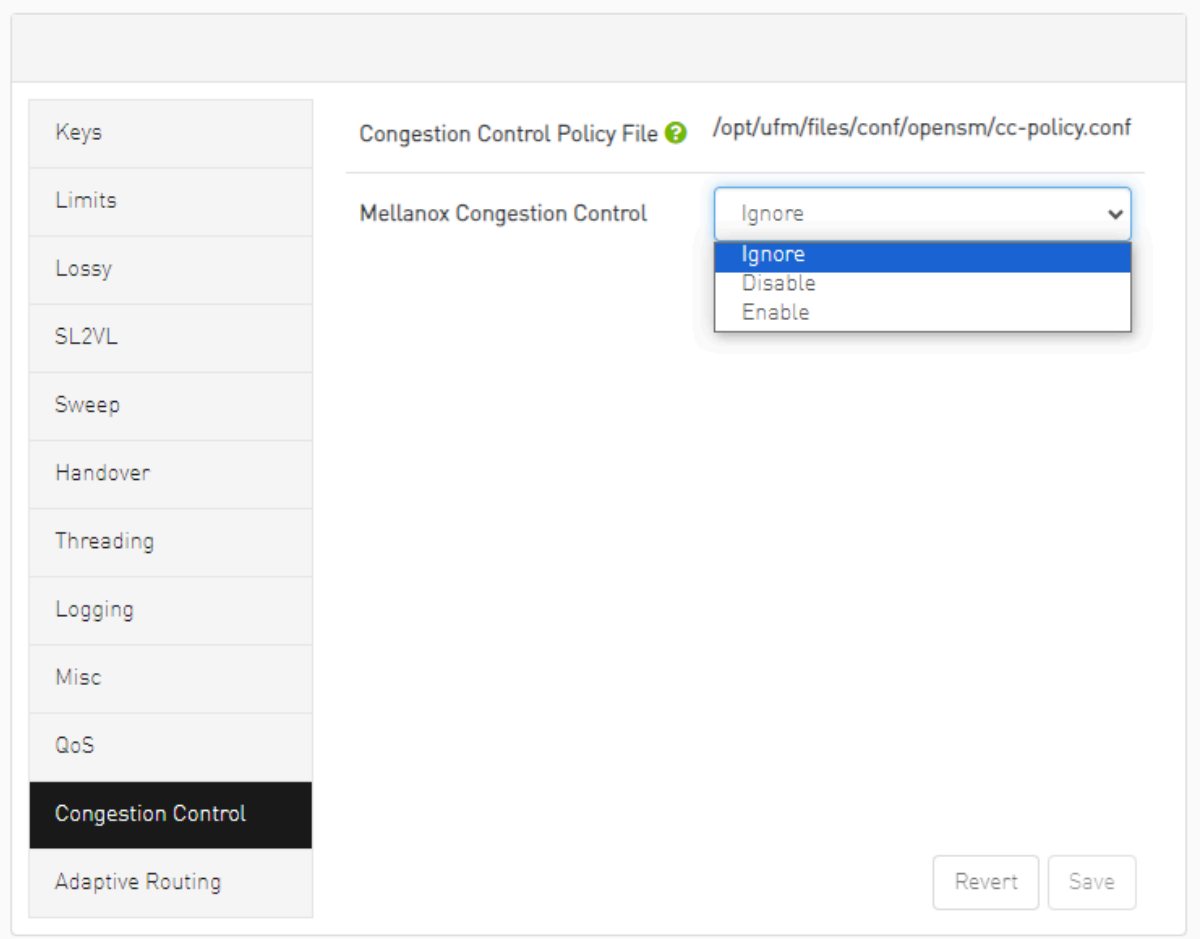
SM QoS Configuration

The QoS tab allows you to enable or disable QoS functionality. QoS is disabled by default.



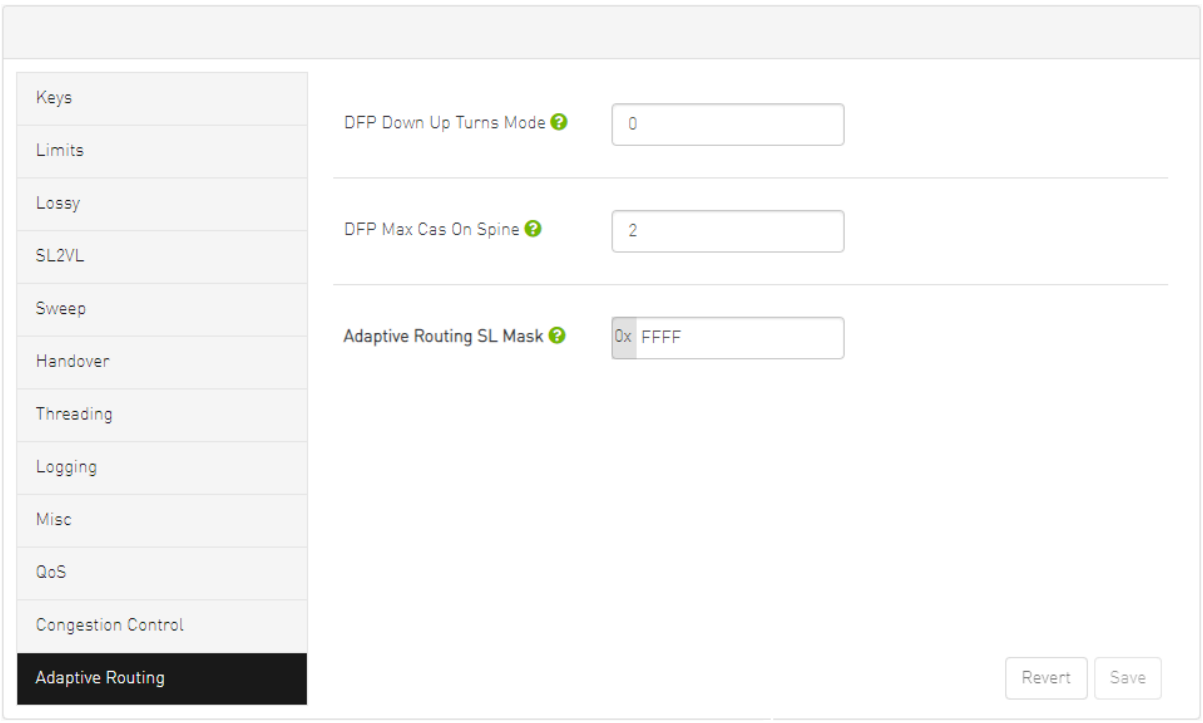
SM Congestion Control Configuration

The Congestion Control tab allows you to enable, disable, or ignore congestion control.



SM Adaptive Routing Configuration

The Adaptive Routing tab allows you to configure adaptive routing parameters.


Keys
Limits
Lossy
SL2VL
Sweep
Handover
Threading
Logging
Misc
QoS
Congestion Control
Adaptive Routing
DFP Down Up Turns Mode
0
DFP Max Cas On Spine
2
Adaptive Routing SL Mask
0x FFFF
Revert
Save

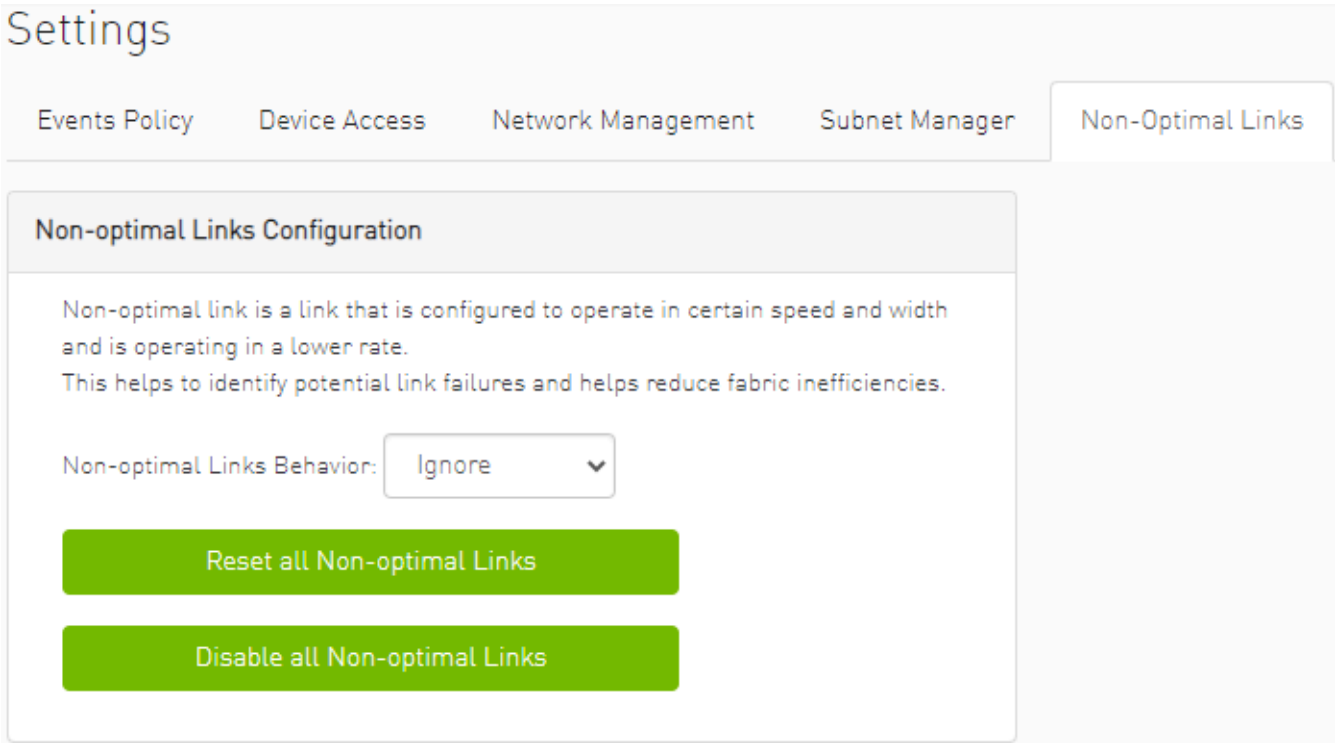
Non-Optimal Links

A non-optimal link is a link between two ports that is configured to operate at a certain speed and width and is operating at a lower rate. The Non-optimal links feature helps you identify potential link failures and reduce fabric inefficiencies.

Non-optimal links can be any of the following:

- NDR links that operate in HDR, EDR, FDR, QDR, DDR or SDR mode
- HDR links that operate in EDR, FDR, QDR, DDR or SDR mode
- EDR links that operate in FDR, QDR, DDR or SDR mode
- FDR links that operate in QDR, DDR or SDR mode
- QDR links that operate in DDR or SDR mode
- 4X links that operate in 1X mode

The Non-Optimal Links window allows you to set the preferred action for non-optimal links.



To set the non-optimal links policy:

From the drop-down menu, select the action for Non-optimal Links behavior.

The drop-down menu defines the default behavior. Options are: **Ignore** (default), **Disable**, and **Reset**.

Option	Description
Ignore	Ignore the non-optimal links
Reset	Reset all non-optimal links ports
Disable	Disable all non-optimal links ports

Reset all Non-Optimal Links allows users to reset all current non-optimal links ports on-demand.

Disable all Non-Optimal Links allows users to disable all current non-optimal links ports on-demand.

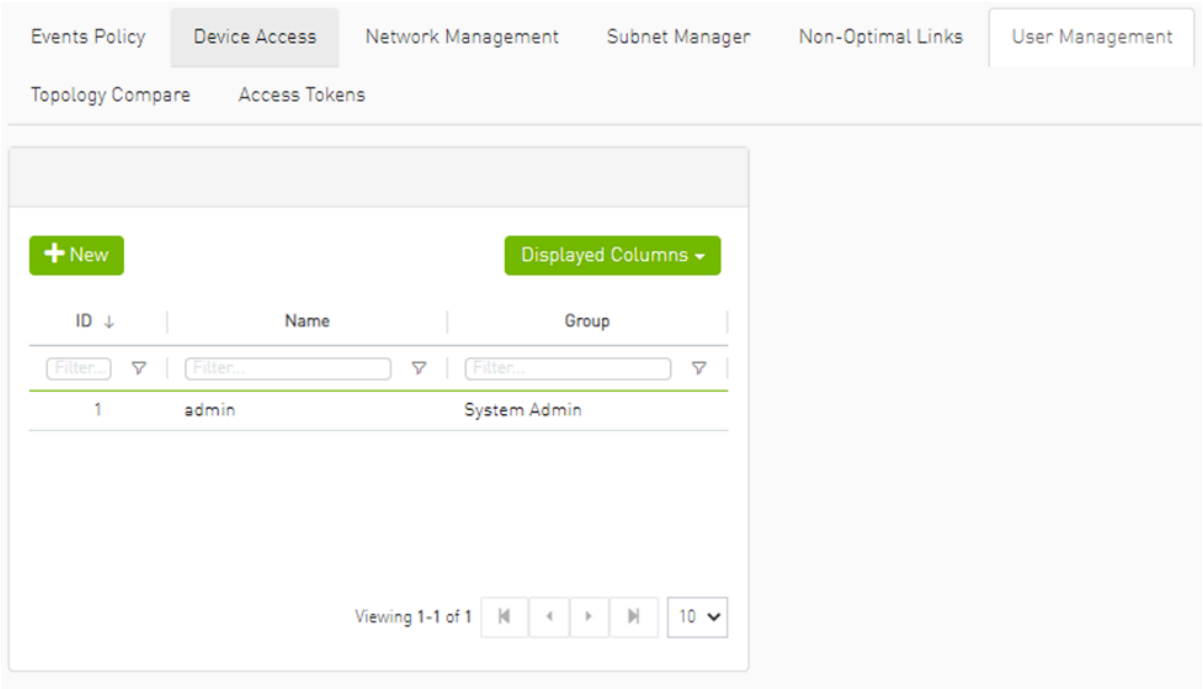
User Management Tab

UFM User Authentication is based on standard Apache User Authentication. Each Web Service client application must authenticate against the UFM Server to gain access to the system. UFM implements any kind of third-party authentication supported by the Apache Web Server.

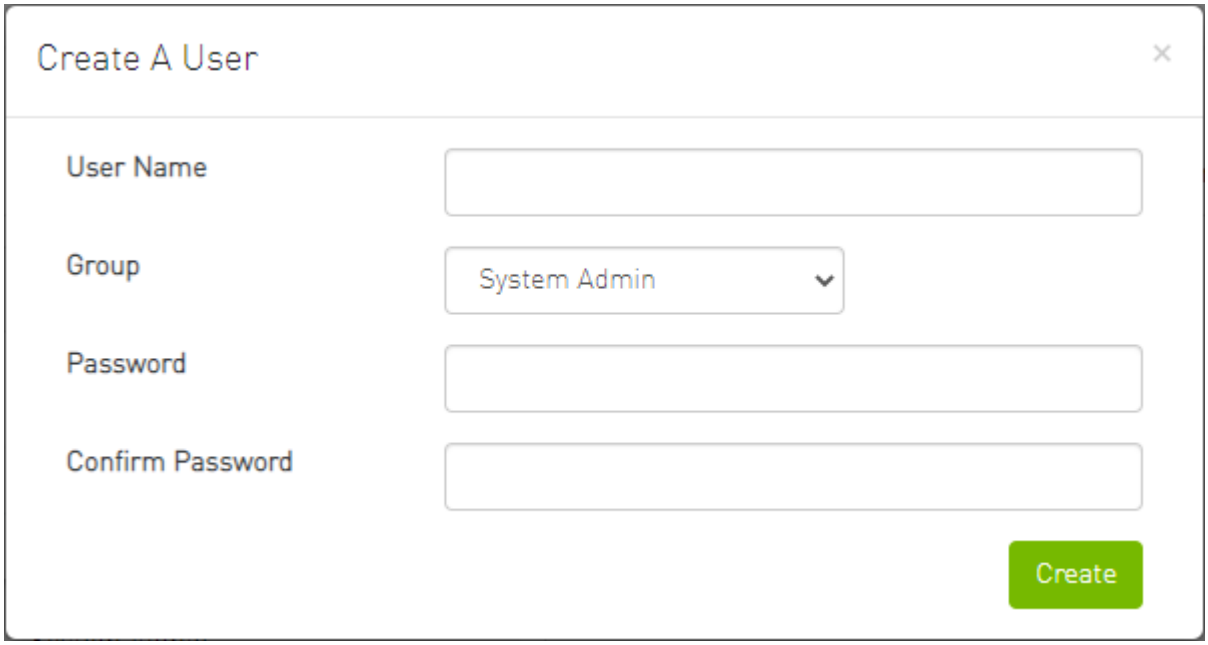
The default user (admin) has System Administration rights. A user with system Administration rights can manage other users' accounts, including creation, deletion, and modification of accounts. The system's default user is the **admin** user.

To add a new user account, do the following:

1. Click the "New" button.



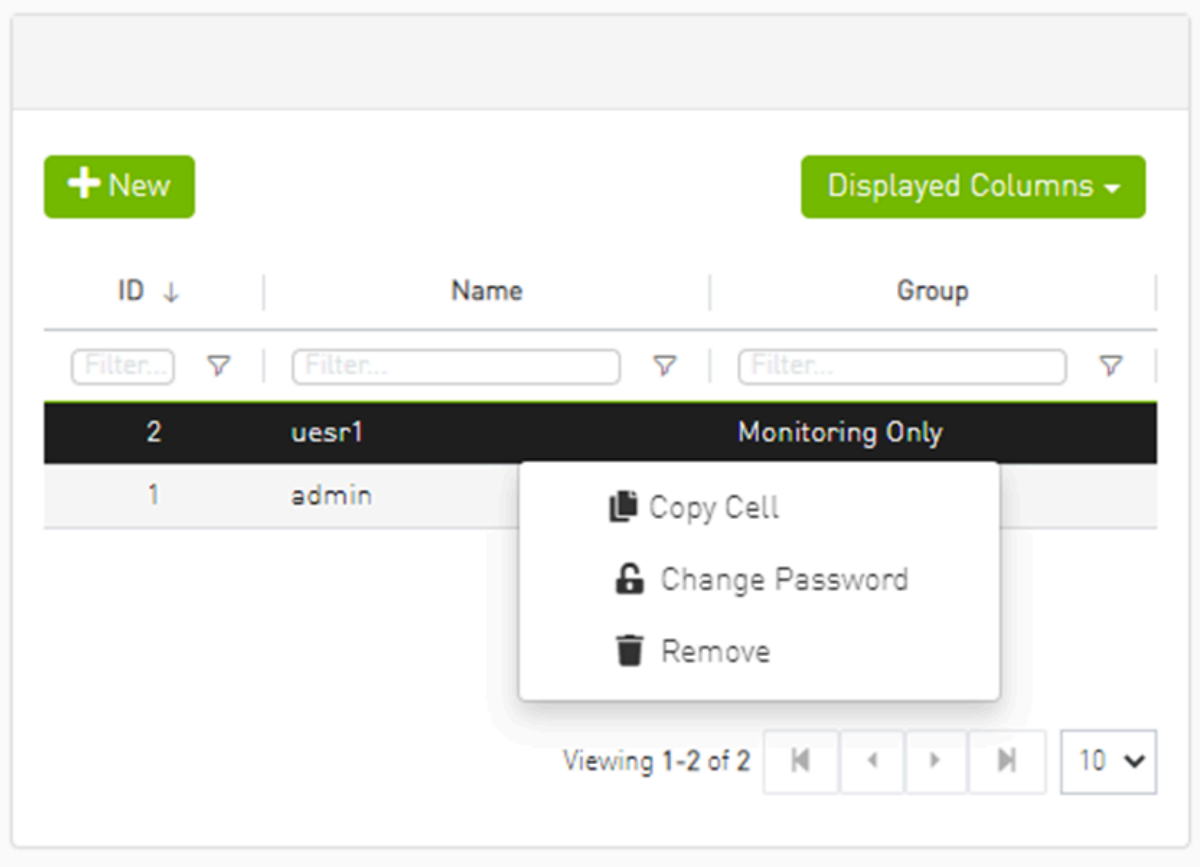
2. Fill in the required fields in the dialog box.



Each user can be assigned to one of the following Group (role) options:

- **System Admin** – users can perform all operations including managing other users accounts.
- **Fabric Admin** – users can perform fabric administrator actions such as update SM configuration, update global credentials, manage reports, managing unhealthy ports, and manage PKeys, etc.
- **Fabric Operator** – users can perform fabric operator actions such as device management actions (enable/disable port, add/remove devices to/from groups, reboot device, upgrade software, etc.)
- **Monitoring Only** – users can perform monitoring actions such as view the fabric configuration, open monitoring sessions, define monitoring templates, and export monitoring data to CSV files, etc.

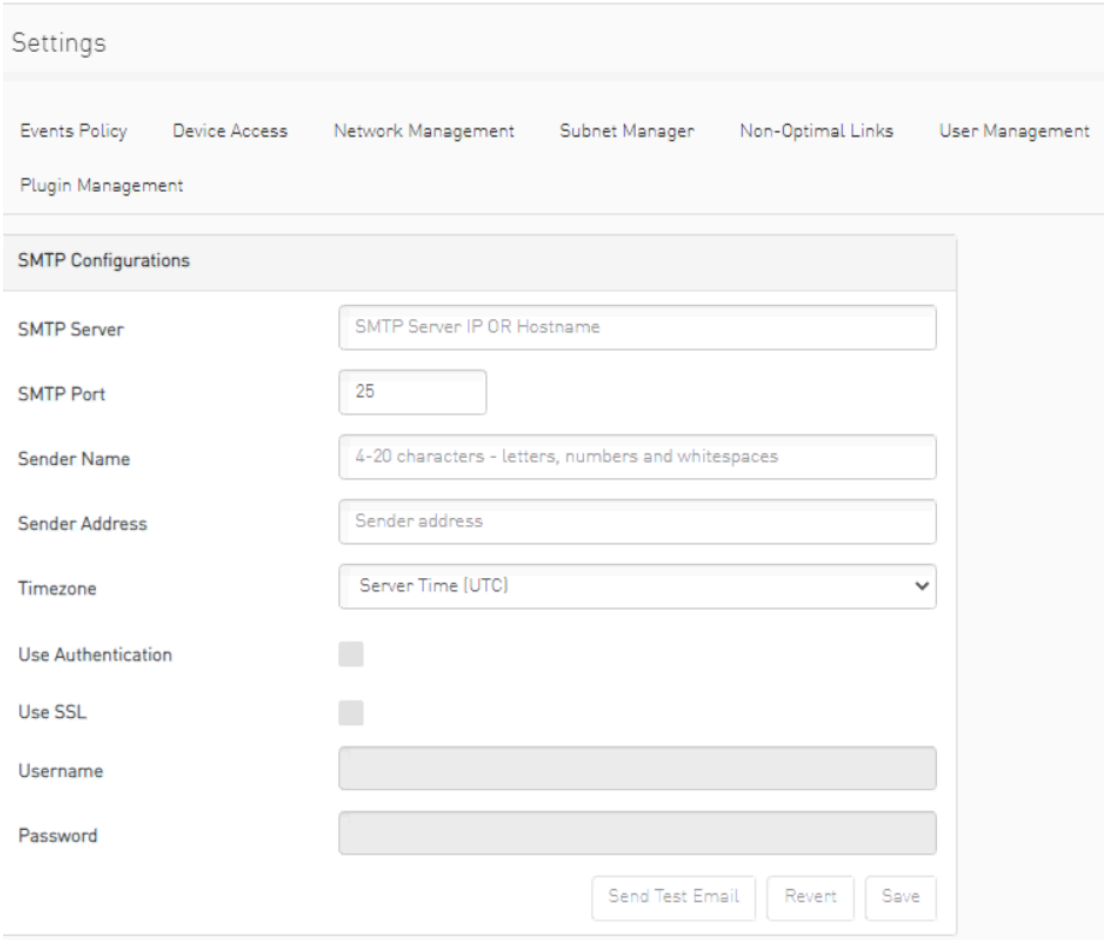
To edit existing users accounts, right-click the account from the list of user accounts and perform the desired action (Change Password/Remove).


New
Displayed Columns
ID
Name
Group
Filter...
Filter...
Filter...
2
uesr1
Monitoring Only
1
admin
Copy Cell
Change Password
Remove
Viewing 1-2 of 2
10

Email

SMTP configuration is required to set both the Daily Reports Tab and the Email-on-Events features.

1. In the SMTP Configuration dialogue window, enter the following information:

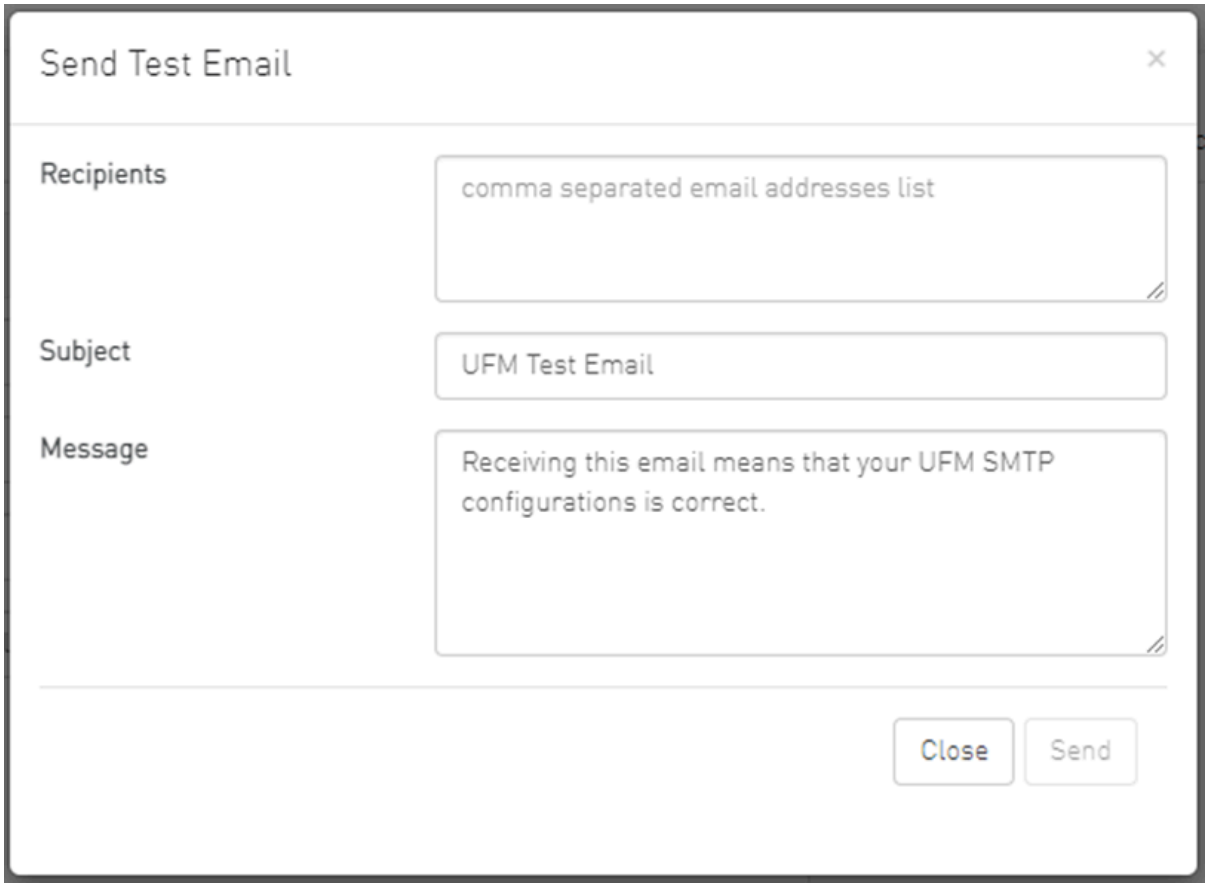


Attribute	Description
SMTP Server	The IP or host name of the SMTP server. **Examples**: ○ If mail service is installed, localhost is a valid value for this field, but usually it cannot send mails outside the local domain. ○ smtp.gmail.com

Attribute	Description
SMTP Port	Default value – 25
Sender Name	The name that will be displayed in the email header
Sender Address	A valid email address that will be displayed in the email header
Time Zone	The default time zone for receiving sent emails is the server time zone. Users have the option to specify a different preferable time zone
Use Authentication	By default, this field is unchecked. If checked, you must supply a username and password in the respective fields
Use SSL	Default value is false – not using SSL
Username	SMTP account username
Password	SMTP account password

2. Click “Save." All configuration of the SMTP server will be saved in the UFM Database.

   Click “Send Test Email” to test the configuration and the following model will appear:

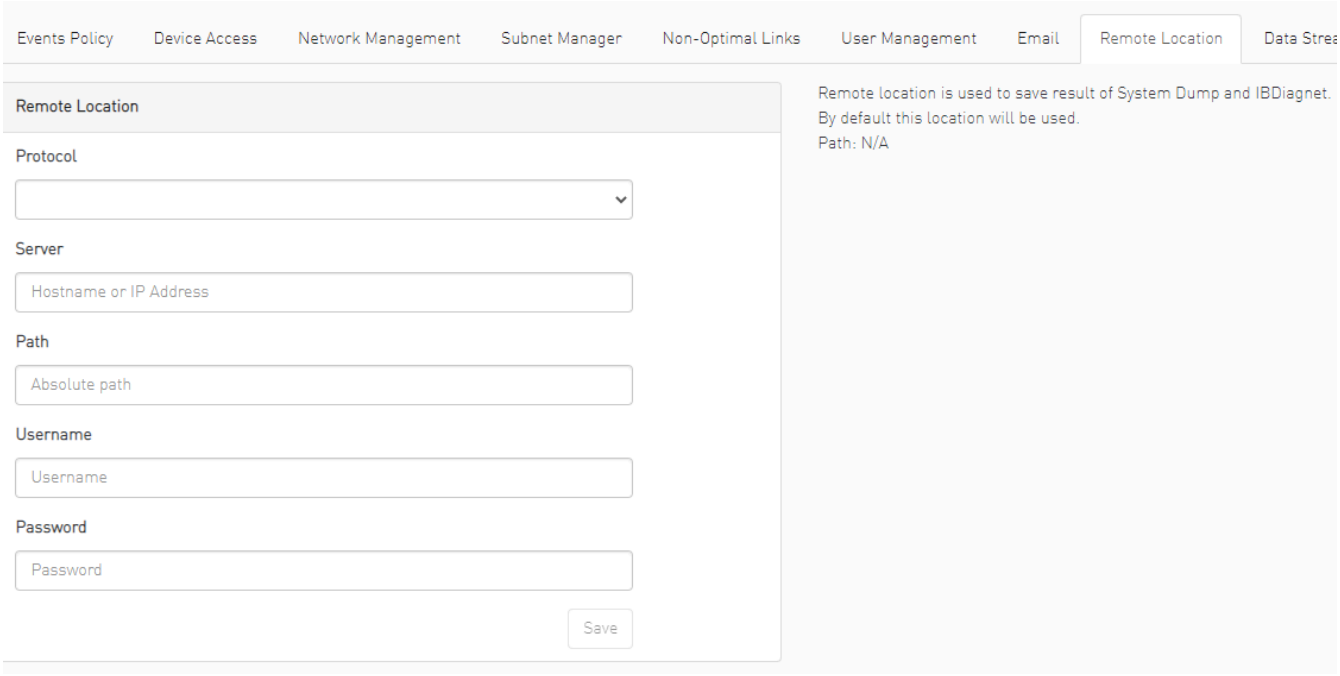


Attribute	Description
Recipients	User can choose email from event policy and daily report recipients or enter any email
Subject	Email subject
Message	Email message

The System Health window enables running and viewing reports and logs for monitoring and analyzing UFM server and fabric health through the following tabs: UFM Health, UFM Logs, UFM Snapshot, Fabric Health, Daily Reports and Topology Compare.

Remote Location

Remote location tab is used to set a predefined remote location for the results of System Dump action on switches and hosts and for IBDiagnet executions.

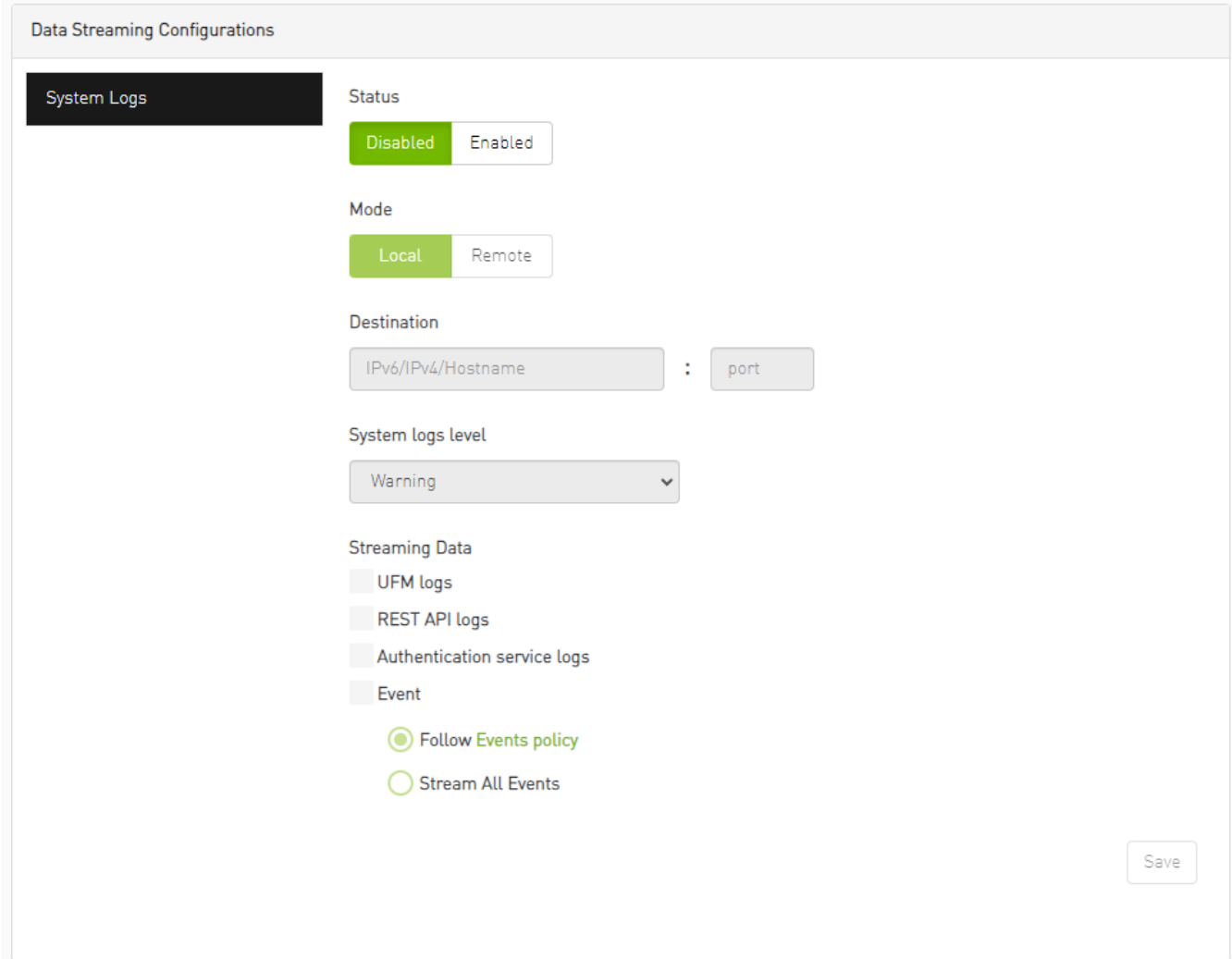


Field	**Description**
Protocol	The protocol to use to move the dump file to the external storage (scp/sftp)
Server	Hostname or IP address of the server
Path	The path where dump files are saved
Username	Username for the server
Password	Respective password

After configuring these parameters, it would be possible for users to collect sysdumps for specific devices, groups, or links (through Network Map/Cables Window) by right-clicking the item and selecting System Dump.

Data Streaming

This section allows users to configure System Logs (syslog) streaming settings via web UI.

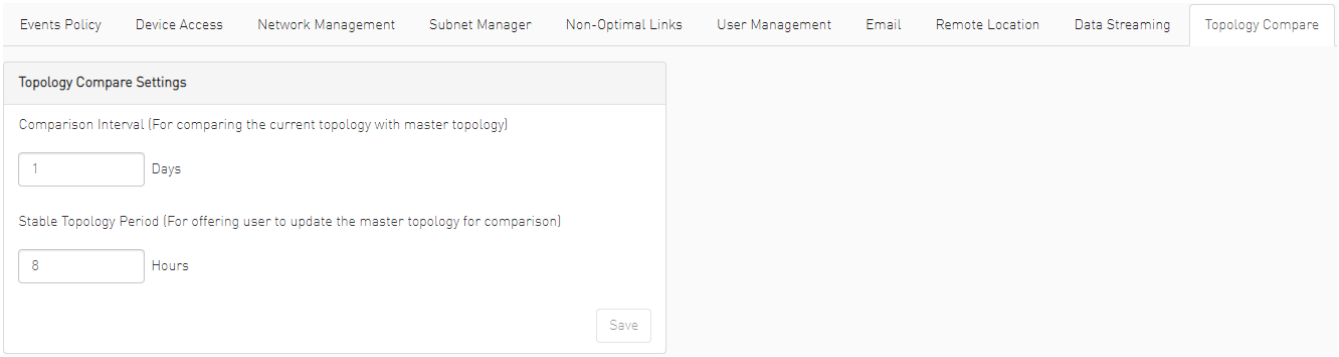


Field	Description
Status	Enable/disable exporting UFM logs to syslog
Mode	Export logs to local or remote syslog
Destination	Remote server IP/hostname and port in case of the remote mode

Field	Description
System Logs Level	Sets global syslog messages logging level. The syslog level is common for all the UFM components. The syslog level that is sent to syslog is the highest among the syslog level and component log level as defined in the config file.
Streaming Data	Logs to export to system logs. **Note** Events logs are selected one by one from Events Policy settings when the system logs feature is enabled. **Note** Authentication service logs will be only available in case the Authentication Service is enabled

Topology Compare

This tab controls the settings for the Periodic Topology Comparison feature.



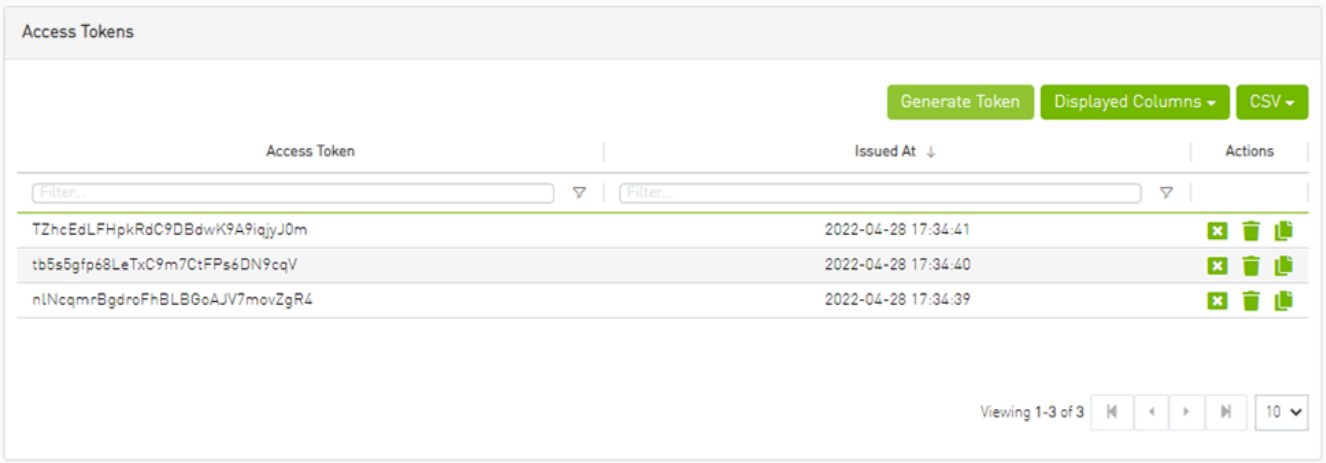
- Comparison Interval – determines how often the current topology is compared against the master topology
- Stable Topology Period – determines how long a topology must be stable before it is designated the new master topology

Token-based Authentication

Token-based authentication is a protocol which allows users to verify their identity, and in return receive a unique access token. During the life of the token, users then access the UFM APIs that the token has been issued for, rather than having to re-enter credentials each time they need to use any UFM API.

> **Note**
>
> Under the Settings section there is a tab titled called “Access Tokens”.

The functionality of the added tab is to give the user the ability to create new tokens & manage the existing ones (list, copy, revoke, delete):



Actions:

Name	Icon	Description
Revoke		Revoke a specific token.

Name	Icon	Description
		**Note** The revoked token will no longer be valid.
Delete		Delete a specific token.
Copy		Copy specific token into the clipboard.

Note

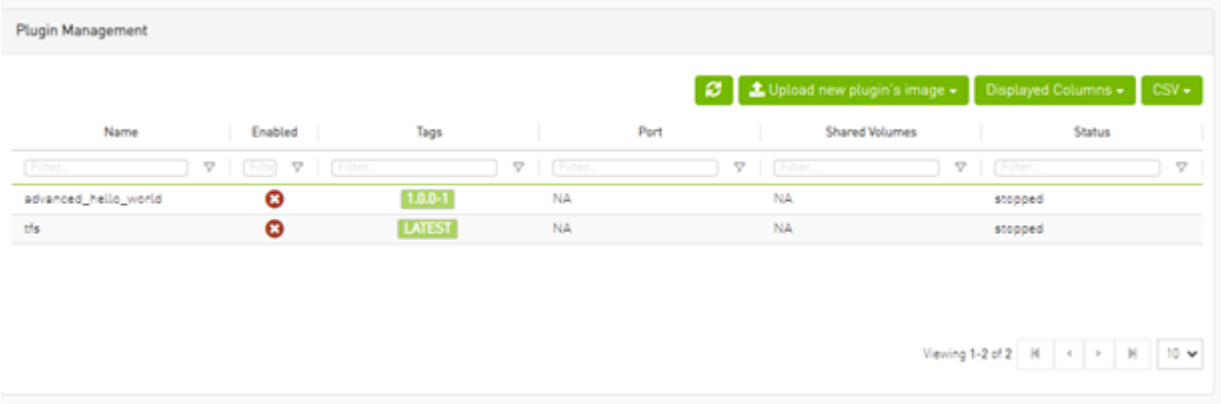
Each user is able to list and manage only the tokens that have been created by themselves. Only the users with system_admin role will be able to create tokens.

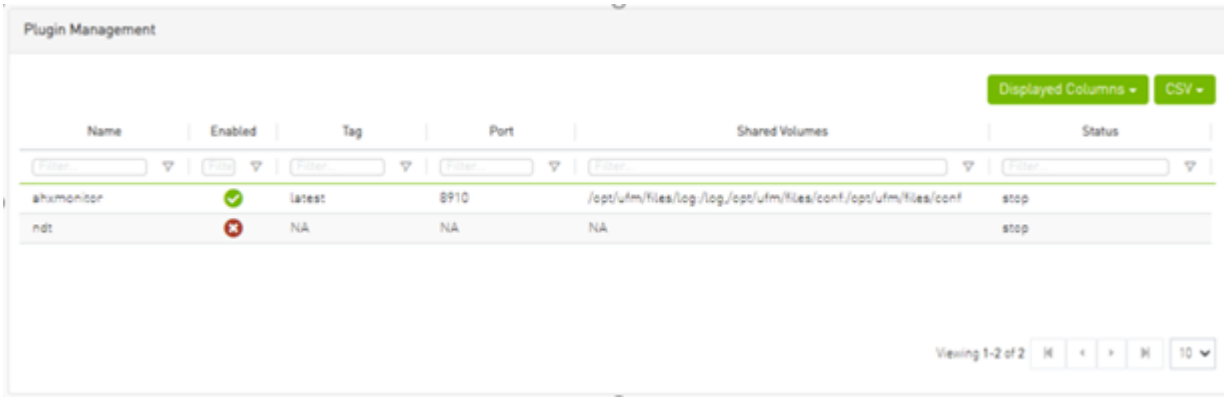
Plugin Management

Plugin management allows users to manage UFM plugins without using CLI commands. Under "Settings", there is a tab titled “Plugin Management”.

The functionality of the "Plugin Management" tab is to give the user the ability to add, remove, disable and enable plugins.

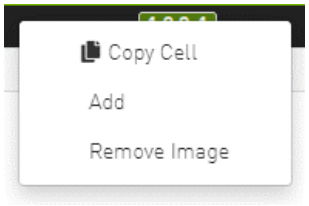
Furthermore, the plugin management feature allows loading a plugin's image in two ways: either by remotely pulling it from a Docker Hub repository or by directly uploading the image file from the user's local machine.



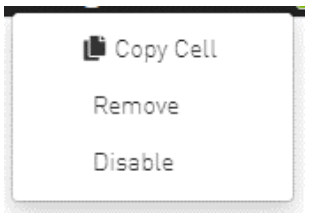


Actions:

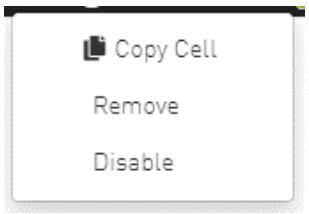
- Add – Used to add a selected plugin, opens a model to select the needed tag.



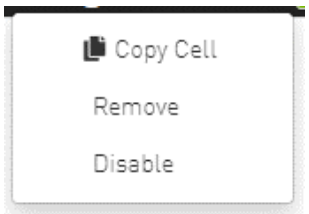
- Remove – Used to remove a selected plugin.



- Disable – Used to disable a selected plugin, so the plugin is disabled once the UFM is disabled.

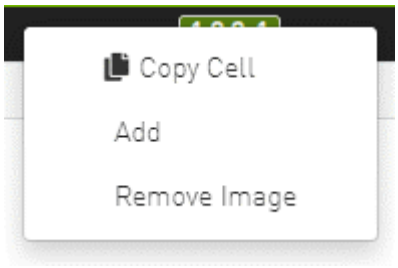


- Enable – Used to enable a selected plugin, so the plugin is enabled once the UFM is enabled.

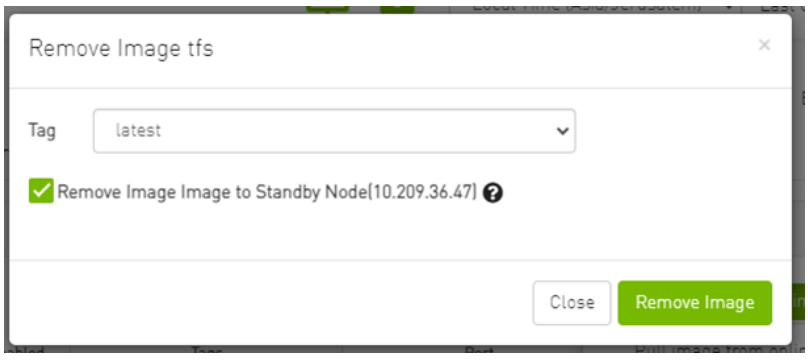


- Add ahxmonitor – Used to add a selected plugin; the action opens a modal to select the requested tag.

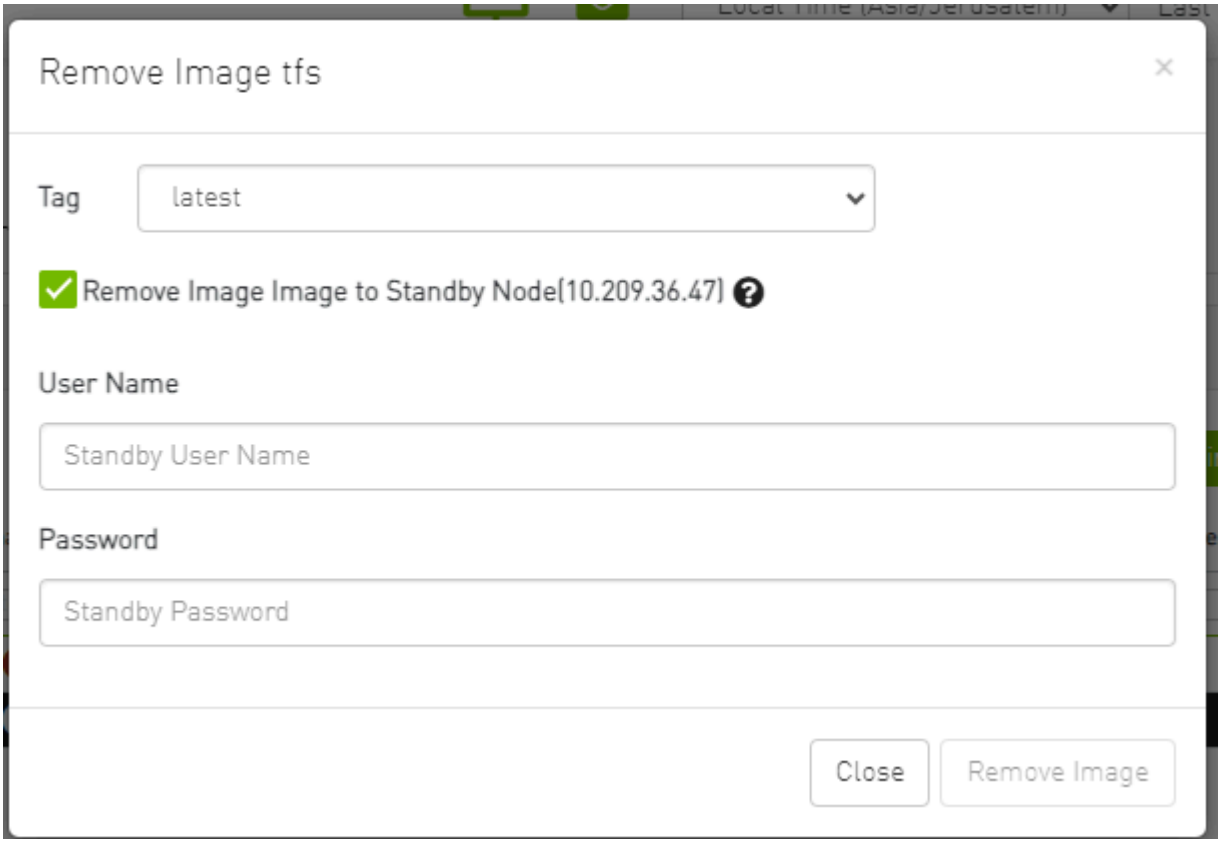
- Remove plugin Image – Used to remove plugin image



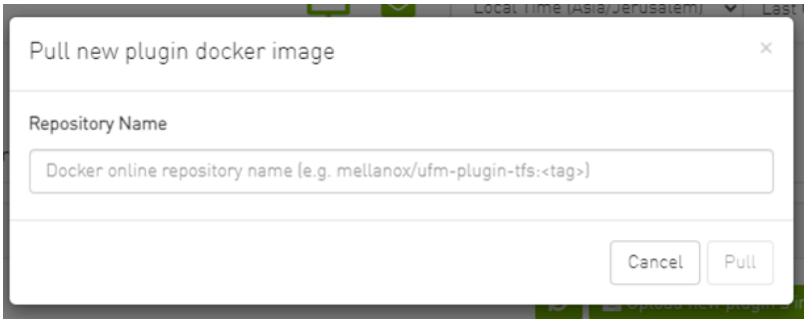
If the high availability (HA) mode is enabled, the user will see the option to remove the image from the standby node as well.



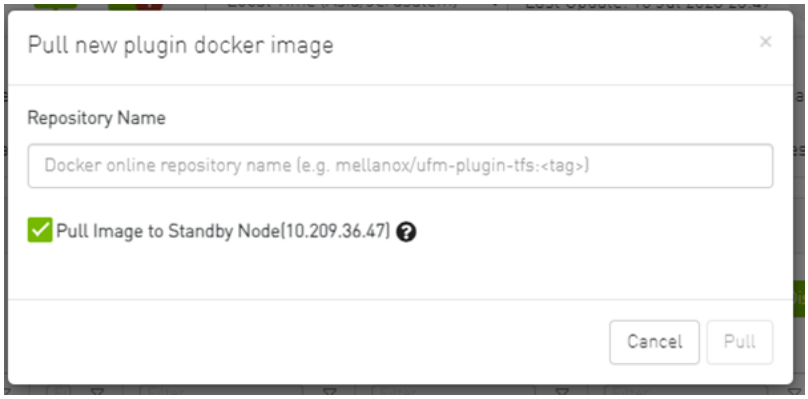
In cases where there is no established trust communication between the master and standby nodes, the user will be required to provide a username and password to establish an SSH connection between them.



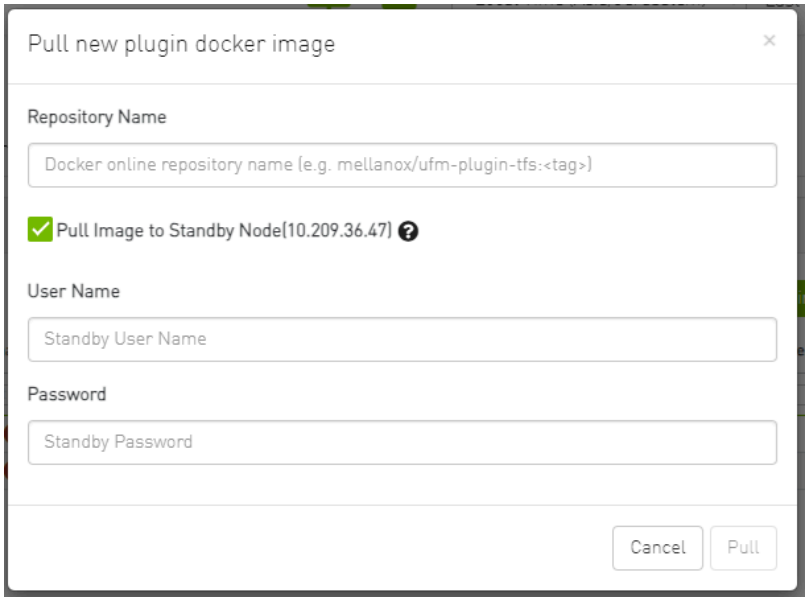
- Pull plugin Image – Used to pull plugin image remotely (e.g. from a Docker Hub repository) or by loading it from user local machine by uploading the image file itself.



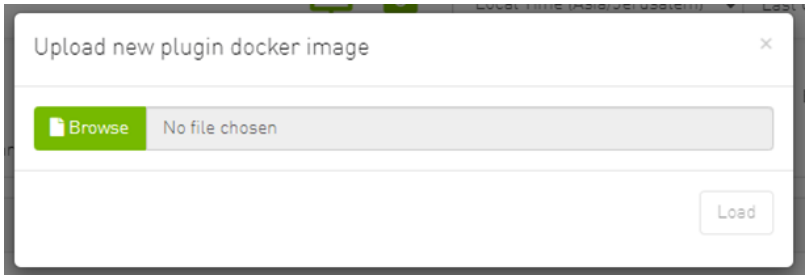
If the high availability (HA) mode is active, the user will be presented with the choice to pull the image to the standby node as well.



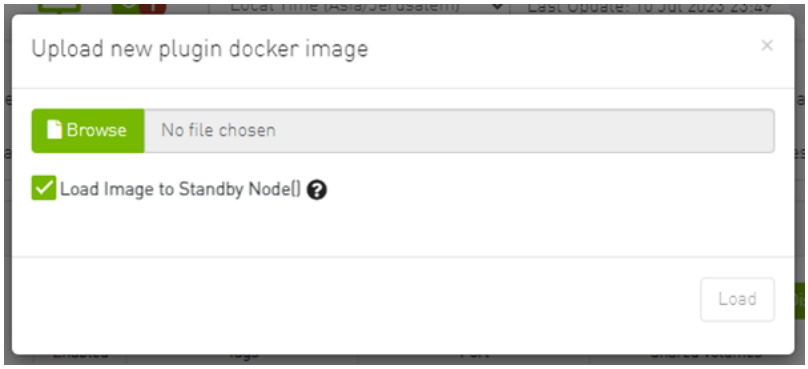
Once again, in the absence of trusted communication between the master and standby nodes, the user will need to input a username and password to create an SSH connection between the nodes.



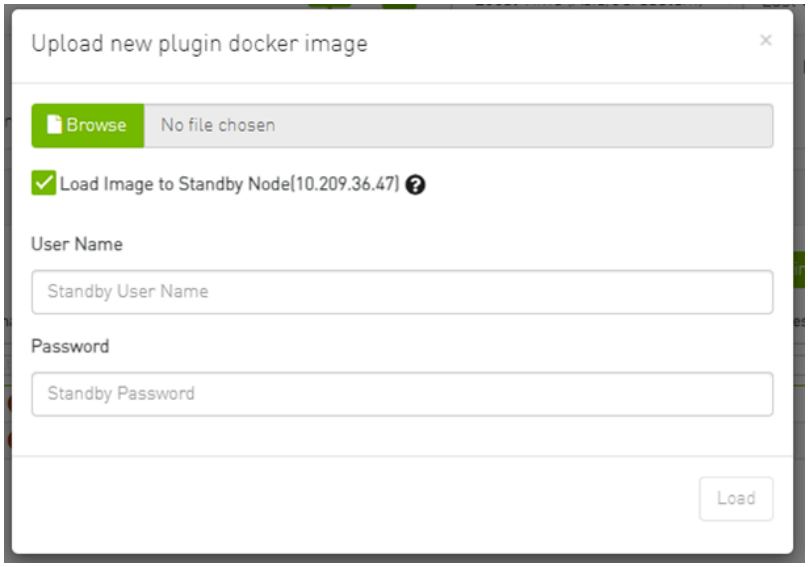
- Load plugin Image: this feature allows the user to upload the image file from their local machine directly.



Similarly, if the high availability (HA) mode is enabled, the user will have the option to load the image to the standby node too.



And, as mentioned earlier, if there is no trusted communication between the master and standby node, the user will need to provide a username and password to establish an SSH connection between the nodes.



Rest Roles Access Control

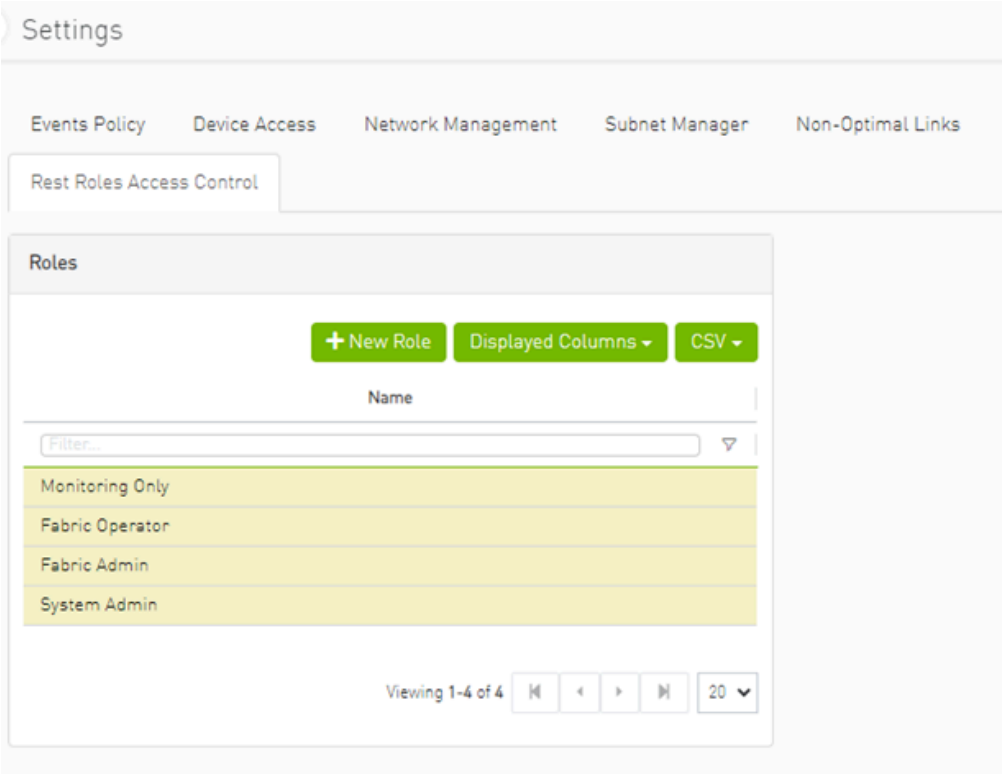
In UFM, there are four predefined roles with the following corresponding values:

1. System Admin (Role value: 5)
2. Fabric Admin (Role value: 4)
3. Fabric Operator (Role value: 3)
4. Monitoring Only (Role value: 2)

For more information, refer to the User Management Tab.

The "Rest Roles Access Control" tab empowers Admin users to design their custom roles alongside the existing predefined roles. Admins can set permissions and access levels for these custom roles, defining which APIs the roles can access.

Roles are presented in a table format, with the predefined roles highlighted in yellow.

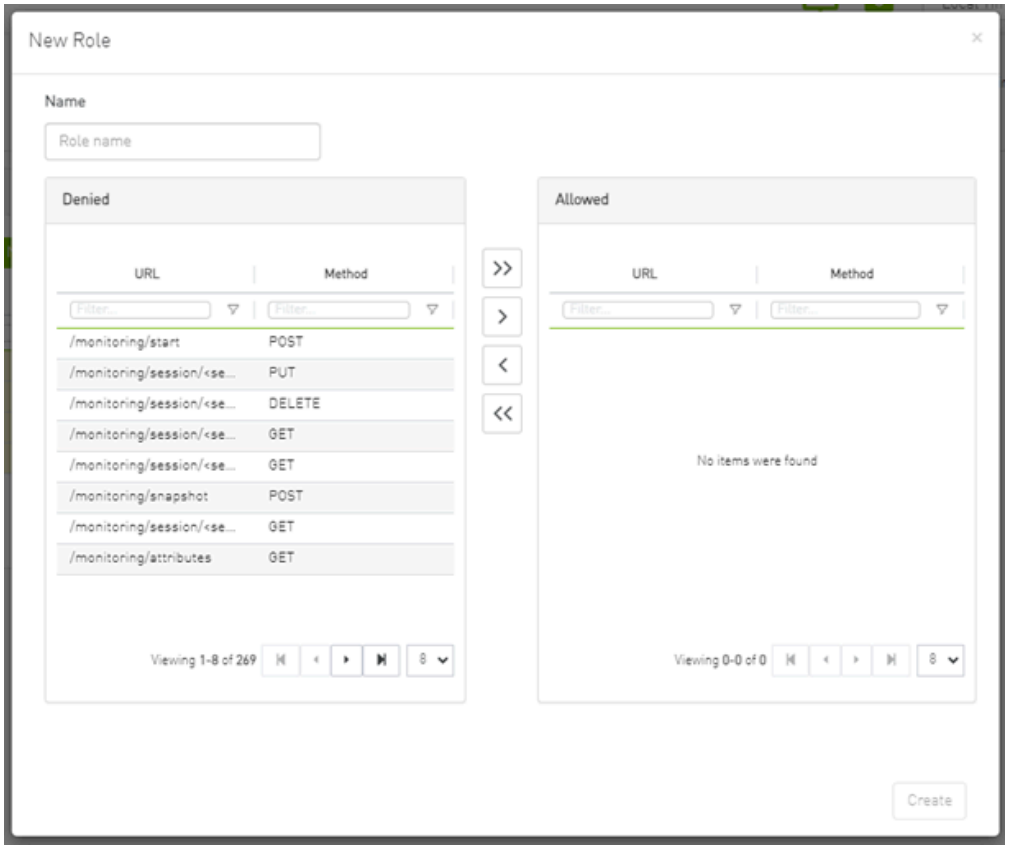


This tab is exclusively available to System_Admin users and can be enabled or disabled through the gv.cfg file. By default, it is enabled.

Adding a New Role

1. Click the + New Role button.

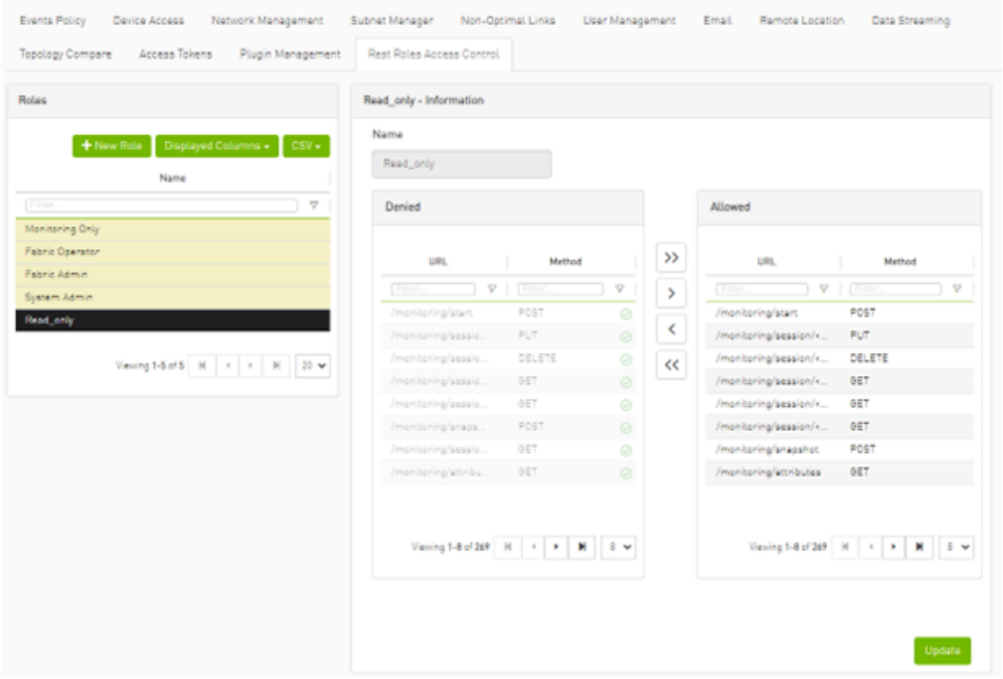
2. Fill in the necessary details in the dialog box.



   By default, all URLs are denied. To allow specific URLs for this role, move them to the "allowed" category.

Updating Custom Roles

1. Select the role that requires updating.

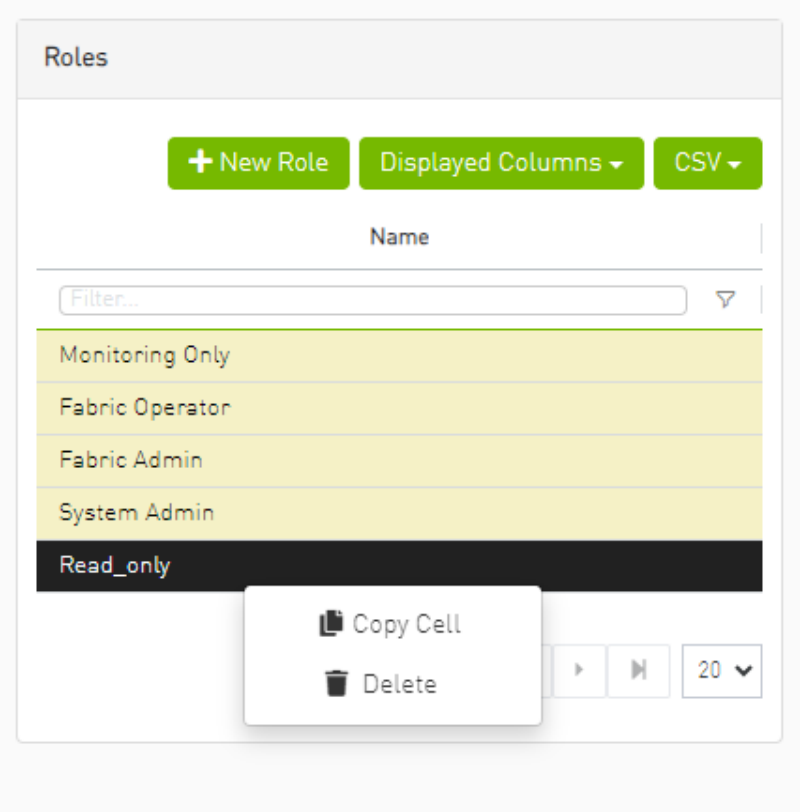


2. Modify the allowed list from the role information section.

Deleting Custom Roles

1. Right-click on the role that needs deletion.

2. Choose the "Delete" option from the context menu.

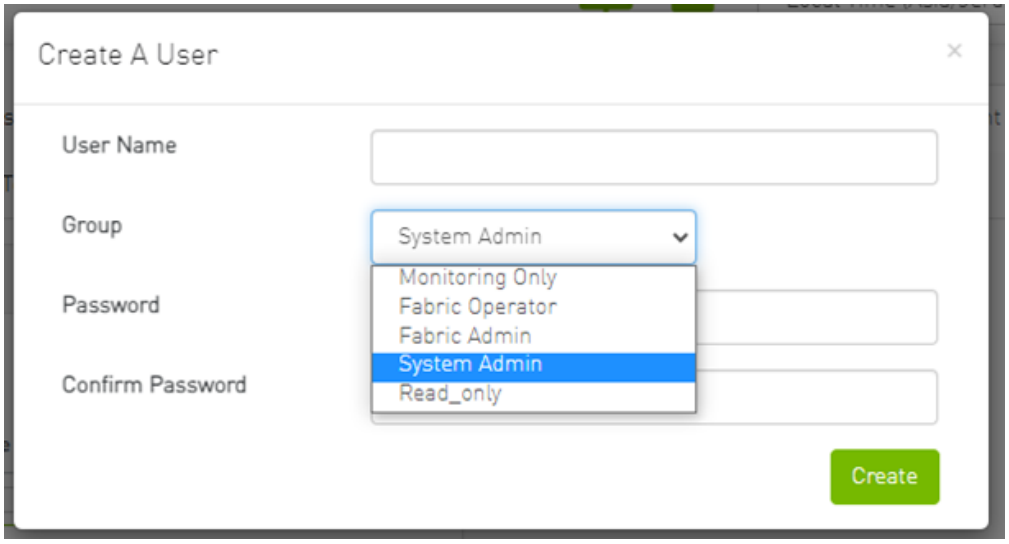


Note

Deleting and updating predefined roles is not permitted.

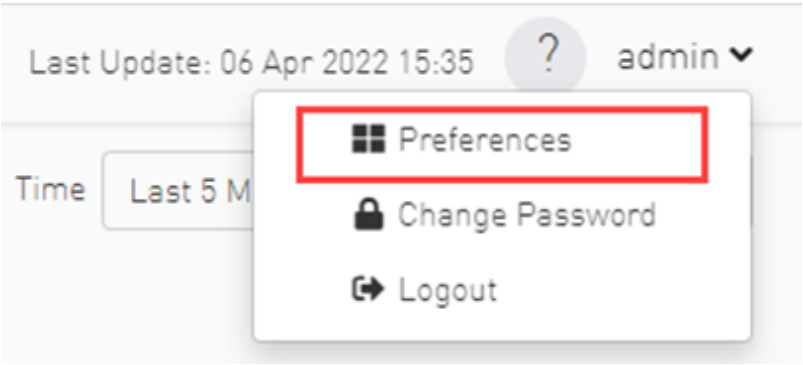
Creating a User with a Custom Role

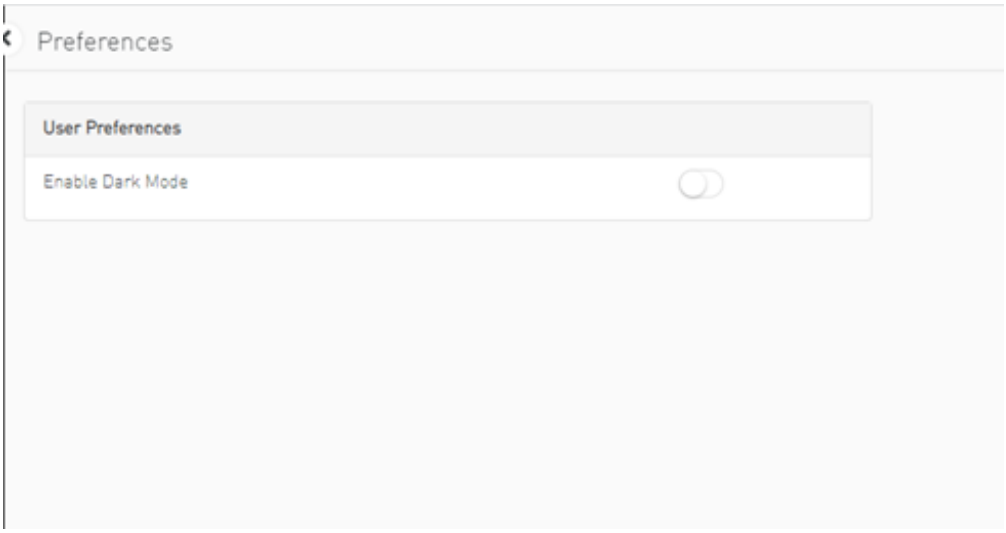
1. Navigate to the Users Management tab.
2. Create a new user, and you will find all roles (both custom and predefined) listed under the group list.


Create A User
User Name
Group
System Admin
Monitoring Only
Fabric Operator
Fabric Admin
System Admin
Read_only
Password
Confirm Password
Create

User Preferences

This page allows user to change UI preferences in general.





When user enables dark mode, the UFM is presented in dark theme.