



# Operations Manager

## User Guide

21.Q1 March 2021





## Contents

<b>Copyright ©</b> .....	<b>6</b>
<b>Safety &amp; FCC Statement</b> .....	<b>7</b>
<b>About This User Guide</b> .....	<b>9</b>
<b>Installation And Connection</b> .....	<b>10</b>
Power Connection .....	11
Dual AC Supply .....	13
Device Status LEDs .....	15
Connecting to the Network .....	17
Serial Connection .....	18
Cellular Connectivity .....	19
Reset and Erase .....	20
<b>Initial System Configuration</b> .....	<b>21</b>
Default Settings .....	22
Management Console Connection via CLI .....	24
Change the Root Password .....	25
Disable a Root User .....	27
<b>MONITOR Menu</b> .....	<b>31</b>
System Log .....	32
LLDP CDP Neighbors .....	33
Triggered Playbooks .....	34
<b>ACCESS Menu</b> .....	<b>35</b>
Local Terminal .....	36
Access Serial Ports .....	37



<b>CONFIGURE Menu</b> .....	<b>40</b>
Serial Ports .....	41
Local Management Consoles .....	45
Lighthouse Enrollment .....	47
Playbooks .....	49
PDUs .....	52
SNMP Alerts .....	54
SNMP Alerts System - Temperature, Authentication, Configuration ...	55
SNMP Alerts Power .....	58
SNMP Alerts Networking (Connection Status) .....	60
<b>Network Connections</b> .....	<b>62</b>
Network Interfaces .....	63
Dual SIM .....	64
Dual SIM Automatic Failover .....	70
Network Aggregates - Bonds and Bridges .....	76
Spanning Tree Protocol .....	82
IPsec Tunnels .....	85
<b>Network Resilience</b> .....	<b>89</b>
OOB Failover .....	90
IP Passthrough .....	91
<b>User Management</b> .....	<b>92</b>
Groups .....	93
Local Users .....	96
Remote Authentication .....	101
RemoteLocal for AAA Server .....	107
Local Password Policy .....	110
<b>Services</b> .....	<b>115</b>
HTTPS Certificate .....	116
Network Discovery Protocols .....	118



Routing .....	119
SSH .....	120
Unauthenticated SSH to Console Ports .....	122
Syslog .....	128
Remote Syslog .....	130
Session Settings .....	135
<b>Firewall .....</b>	<b>136</b>
Firewall Management .....	137
Interzone Polices .....	144
Services - Firewall .....	147
<b>Date &amp; Time .....</b>	<b>149</b>
Time Zone .....	150
Manual Settings .....	151
Automatic Settings .....	152
<b>System .....</b>	<b>153</b>
Administration .....	155
Factory Reset .....	156
Reboot .....	157
System Upgrade .....	158
<b>SNMP .....</b>	<b>159</b>
SNMP Service .....	160
SNMP Alert Managers .....	161
Multiple SNMP Alert Managers .....	163
<b>Advanced Options .....</b>	<b>166</b>
Communicating With The Cellular Modem .....	167
OGCLI Guide .....	169
Docker .....	184
Cron .....	185
Initial Provisioning via USB Key .....	187



EULA and GPL .....	189
<b>UI Button Definitions .....</b>	<b>190</b>



## Copyright ©

Opengear Inc. 2020. All Rights Reserved.

Information in this document is subject to change without notice and does not represent a commitment on the part of Opengear. Opengear provides this document “as is,” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of fitness or merchantability for a particular purpose.

Opengear may make improvements and/or changes in this manual or in the product (s) and/or the program(s) described in this manual at any time. This product could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes may be incorporated in new editions of the publication.



## Safety & FCC Statement

### Safety Statement


Please take care to follow the safety precautions below when installing and operating the OPERATIONS MANAGER:

- Do not remove the metal covers. There are no operator serviceable components inside. Opening or removing the cover may expose you to dangerous voltage which may cause fire or electric shock. Refer all service to Opengear qualified personnel.
- To avoid electric shock the power cord protective grounding conductor must be connected through to ground.
- Always pull on the plug, not the cable, when disconnecting the power cord from the socket.

Do not connect or disconnect the appliance during an electrical storm. Also use a surge suppressor or UPS to protect the equipment from transients.

### FCC Warning Statement

This device complies with Part 15 of the FCC rules. Operation of this device is subject to the following conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference that may cause undesired operation.

	Proper back-up systems and necessary safety devices should be utilized to protect against injury, death or property damage due to system failure. Such protection is the responsibility of the user.
---	--



This device is not approved for use as a life-support or medical system.

Any changes or modifications made to this device without the explicit approval or consent of Opengear will void Opengear of any liability or responsibility of injury or loss caused by any malfunction.

This equipment is for indoor use and all the communication wiring are limited to inside of the building.





## About This User Guide

This user guide covers the Opengear Operation Manager products, including the OM2200 family of rack-mountable appliances (available with combinations of up to 48 serial ports and 24 Ethernet ports) and the OM1200 family of small form-factor appliances (available with combinations up to 8 serial and 8 Ethernet ports).

This manual is up to date for the 20.Q4 November 2020 firmware release. When using a minor release there may or may not be a specific version of the user guide for that release. The current Operations Manager user guide can always be found [here](#).



## Installation And Connection

This section describes how to install the appliance hardware and connect it to controlled devices.

## Power Connection

OM2200 and some newer OM1200 have dual power inlets with auto failover built in. These power supplies each accept AC input voltage between 100 and 240 VAC with a frequency of 50 or 60 Hz. The OM2224-24E-10G-L draws a maximum of 48W, while non-24E are less than 30W.

Two IEC AC power sockets are located on the power side of the metal case, and these IEC power inlets use conventional IEC AC power cords.

**Note:** Country specific IEC power cords are not included with OM2200s. OM1200s are shipped with a 12VDC to universal AC (multi-country clips) wall adapter.

See also ["Dual AC Supply" on page 13](#) and ["SNMP Alerts Power" on page 58](#).

Operations Manager Platform (OM1200) Environmental And Power	
Power Draw	< 25 Watts
Operating conditions	Temperature 0~50C, Rel Humidity 5~90%
Cooling	Passive
Environmental Sensors	Smart Controller with multi-zone temperature sensors.
	Auto-shutdown/re-boot on severe thermal events
Power Draw Sensors	Active multi-zone power draw monitoring

Operations Manager Platform (OM2200) Environmental And Power	
Power Supply	Dual AC or dual DC
Power Draw	48 Watts for -24E, others <30W
Operating conditions	Temperature 0~50C, Rel Humidity 5~90%
Cooling	Passive
Environmental Sensors	Smart Controller with multi-zone temperature sensors
	Supervisory environmental controller with safety power down.
Power Draw Sensors	Active multi-zone power draw monitoring

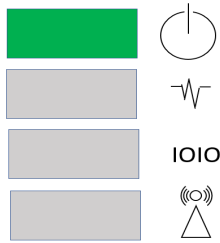
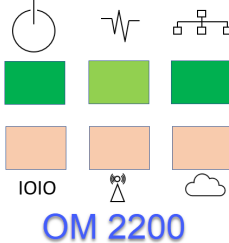
## Dual AC Supply

Dual AC Supply can provide power redundancy for devices, especially those that may operate in harsher environments. A secondary power supply provides redundancy for the device if one PSU is unplugged or in the event of a failure.


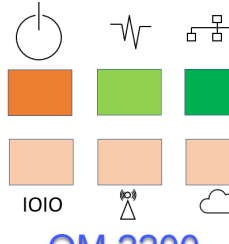
### LED Power Status Indicator

The power LED indicator requires no configuration and will display the dual power status on any Operations Manager device with a dual power supply.

On a device with a **single** PSU (power supply unit) *or*, a **dual** PSU device has power connected to *two* PSUs, the LED power status indicator should be green at all times.

 <p>OM 1200</p>	 <p>OM 2200</p>
---	--

If a **dual** PSU device has power connected to *one* PSU (power supply unit), the LED power status indicator is colored orange indicating that the unit has no redundancy in the event of a power failure.

 <p>OM 1200</p>	 <p>OM 2200</p>
--	---



## SNMP Alerts for Power-related Events




The System Voltage Range SNMP alert is triggered when there is a change in power status such as a system reboot or when the voltage on either power supply leaves or enters the configured range of the System Voltage alert.




## SNMP Alert Configuration

The System Voltage Range SNMP alert is configured in the Configure > SNMP Alerts page, see ["SNMP Alerts Power" on page 58](#).

## Device Status LEDs

The LED states shown below are determined through infod status and config-server data. The config server holds a configurable threshold value for the Cell LED Amber / Green light, and modem enabled / disabled information.

Status LEDs					
LED Condition					
	LED Off	Amber Flashing	Amber Solid	Green Flashing	Green Solid
Power 	Device is off.		On a dual power supply system: Only one PSU is connected.		On a single power supply system: power is connected. On a dual power supply system: Redundant power is connected.
Heartbeat 	Device has halted.	Device is booting.		Normal operation.	Device is halted.
Network 	No active network connection	Device is fail-over starting.	Device is in failover.	Normal network connection is stopping or normal network is up and failover is stopping.	Network is connected.

Status LEDs (continued).					
LED Condition					
	LED Off	Amber Flashing	Amber Solid	Green Flashing	Green Solid
Cellular Interface 	Cellular is not in use.	Cell is starting and signal is below threshold. The LED signal threshold config is set to 50%.	Cell is connected and signal is below threshold. The LED signal threshold config is set to 50%.	Cell is starting and signal is above, or equal to the threshold.	Cell is connected and signal is above, or equal to the threshold.
IOIO 				Any serial activity is received, on either console/usb console or device serial ports.	
Cloud / Internet 	Not implemented.				

**Note:** The amber LED signal threshold config is set to 50%.of normal signal strength.

For information on the setting of network and power alert thresholds, see:

["SNMP Alerts Networking \(Connection Status\)" on page 60](#)

["SNMP Alerts Power" on page 58](#)





## Connecting to the Network

All Operations Manager products have two network connections labeled NET1 and NET2. In the OM2200, there are options for copper wiring (on a standard RJ-45 connector) and fiber (through a standard SFP module).

The network connections on the OM2200 are located on the serial port side of the unit. Connect the provided shielded CAT5 cable to the NET1 to a computer or into your network for initial configuration. By default NET1 and NET2 are enabled.

You can use either 10/100/1000BaseT over Cat5 or fiber-optical transceiver (1Gbps) in the SFP slot for NET1 or NET2 on OM2200 (non-10G) and OM1208-8E.



## Serial Connection

The serial connections feature RS-232 with software selectable pin outs (Cisco straight –X2 or Cisco reversed –X1). Connect serial devices with the appropriate STP cables.

## Cellular Connectivity

The Operations Manager products offer an optional global cellular LTE interface (models with -L suffix). The cellular interface is certified for global deployments with most carriers and provides a CAT12 LTE interface supporting most frequencies in use. To activate the cellular interface, you should contact your local cellular carrier and activate a data plan associated to the SIM installed.

For -L models, attach the 4G cellular antennas to the unit's SMA antenna sockets on the power face (or to the extension RF cables) before powering on. Insert the 2FF SIM card on the power face with the contact facing up. Use the left SIM socket first.

### Installing A New SIM Card

Before installing a new SIM card, the OM device must first be powered down. This can be done by switching off the power supply and waiting until the device has shut-down. Install the new SIM card into its slot, then restart the device

**Note:** The device will not recognize the new SIM card unless a shut-down and restart is performed. The new SIM card will be read during start-up.

## Reset and Erase

[CONFIGURE > System > Reboot](#)

The OPERATIONS MANAGER reboots with all settings (e.g. the assigned network IP address) preserved.

To reboot the unit:

Select **CONFIGURE > System > Reboot**.

To erase the unit:

Push the Erase button on the port-side panel twice with a bent paper clip while the unit is powered on.

This resets the appliance to its factory default settings. Any modified configuration information is erased. You will be prompted to log in and must enter the default administration username and administration password (Username: root Password: default). You will be required to change this password during the first log in.

## Initial System Configuration

This section provides step-by-step instructions for the initial configuration of your OPERATIONS MANAGER.

By default, all interfaces are enabled. The unit can be managed via WebGUI or by command line interface (CLI).

- ["Default Settings" on the next page](#)
- ["Management Console Connection via CLI" on page 24](#)
- ["Change the Root Password" on page 25](#)
- ["Disable a Root User" on page 27](#)
- ["Change Network Settings" on page 27](#)
- [For Configure Serial Ports \(see "Serial Ports" on page 41\)](#)

## Default Settings

The OPERATIONS MANAGER comes configured with a default static IP Address of 192.168.0.1 Subnet Mask 255.255.255.0.

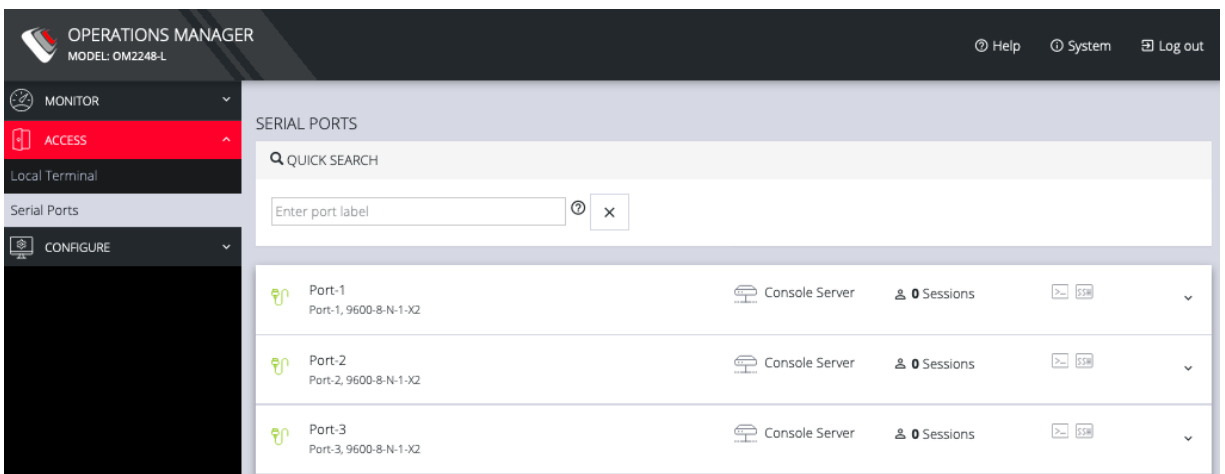
The OM offers a WebGUI via web browser that supports HTML5.

1. Type https://192.168.0.1 in the address bar. HTTPS is enabled by default.
2. Enter the default username and password

**Username:** root

**Password:** default

3. After the first successful log-in you will be required to change the root password.
4. After log-in, the WebGUI is available. Check system details
5. After log-in the WebGUI is available. Check system details in the top right-hand side of the WebGUI.
6. In the Navigation Bar on the left side, navigate to the **ACCESS > Serial Ports** page. The Serial Ports page displays a list of all the serial devices, including the links to a Web Terminal or SSH connection for each.



The screenshot shows the OPERATIONS MANAGER interface. The top navigation bar includes 'OPERATIONS MANAGER MODEL: OM2248-L', 'Help', 'System', and 'Log out'. The left sidebar has 'MONITOR', 'ACCESS' (highlighted), 'Local Terminal', 'Serial Ports', and 'CONFIGURE'. The main content area is titled 'SERIAL PORTS' and features a 'QUICK SEARCH' box with the placeholder 'Enter port label'. Below the search box is a table listing three serial ports:

Port Label	Device Type	Sessions	Actions
Port-1 Port-1, 9600-8-N-1-X2	Console Server	0 Sessions	[Web Terminal] [SSH] [Dropdown]
Port-2 Port-2, 9600-8-N-1-X2	Console Server	0 Sessions	[Web Terminal] [SSH] [Dropdown]
Port-3 Port-3, 9600-8-N-1-X2	Console Server	0 Sessions	[Web Terminal] [SSH] [Dropdown]

## Using the WebUI

The WebUI can be switched between **Light** or **Dark** mode by adjusting the toggle on the bottom left.

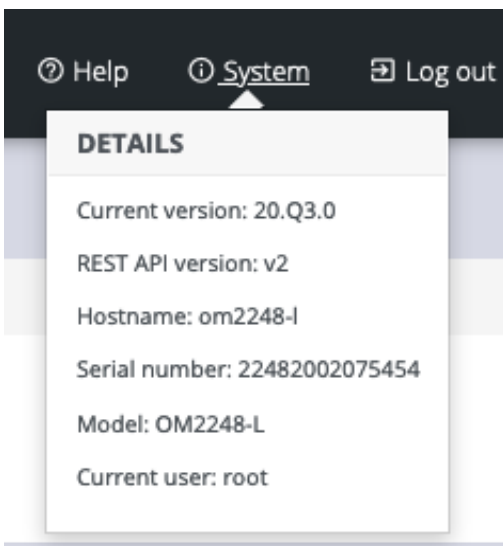


Light mode changes the user interface to display mostly light colors. This is the default UI setting. Dark mode changes the user interface to display mostly dark colors, reducing the light emitted by device screens.

The WebUI has three menu options on the upper right: **Help**, **System**, and **Log out**.

The **Help** menu contains a link to generate a **Technical Support Report** that can be used by Opengear Support for troubleshooting. It also contains a link to the latest Operations Manager User Manual.

The System menu presents the **Current version**, **REST API version**, **Hostname**, **Serial Number**, **Model**, and **Current user**.



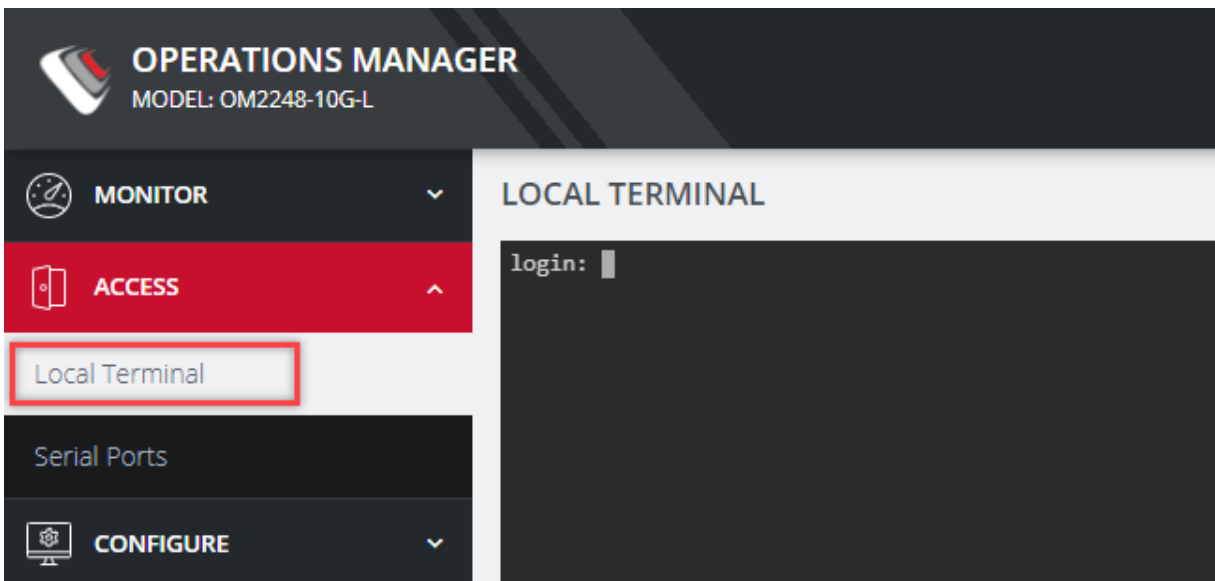
## Management Console Connection via CLI

The Command Line Interface (CLI) is accessible using your preferred application to establish an SSH session. Open a CLI terminal on your desktop, then:

1. Input the default IP Address of 192.168.0.1. SSH port 22 is enabled by default.
2. When prompted, enter the log in and password in the CLI.
3. After a successful log in, you'll see a command line prompt.

### Accessing the WebGUI CLI Terminal

An alternative CLI terminal is provided within the WebGUI. To access this terminal, in the left-hand side **Navigation Bar**, navigate to the **ACCESS > Local Terminal** page. You will be required to submit your log-in credentials.





## Change the Root Password

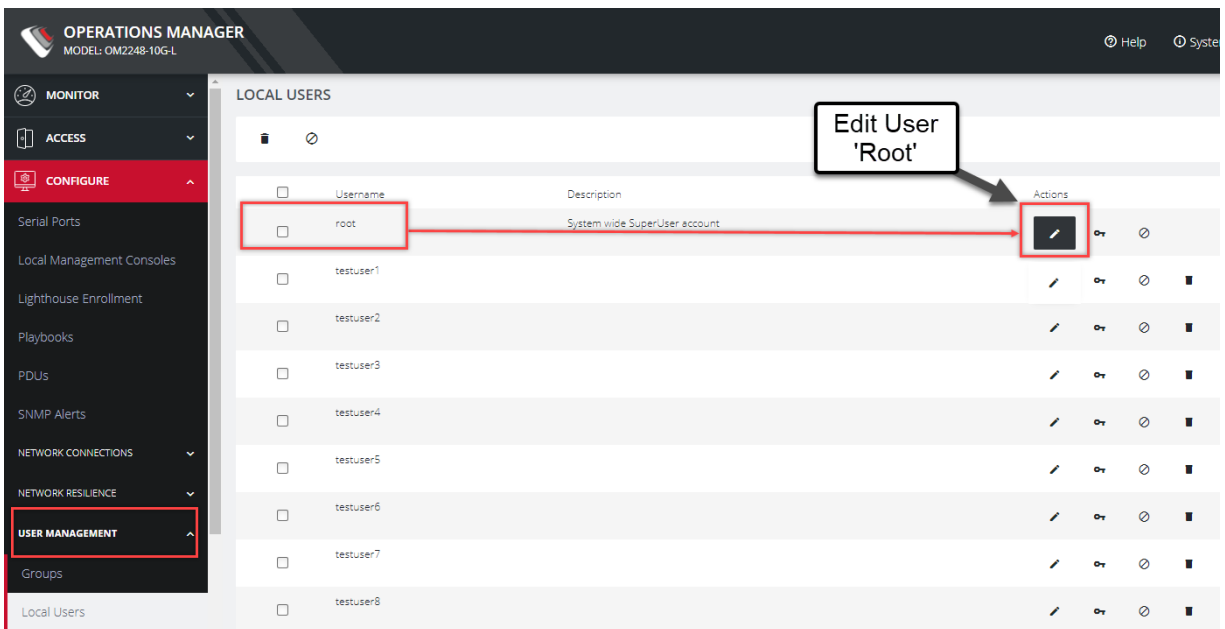
[CONFIGURE](#) > [User Management](#) > [Local Users](#) > [Edit User](#)

For security reasons, only the root user can initially log into the appliance. Upon initial log in the default password must be changed.

**Tip:** Other Users' passwords may be changed using the same procedure by selecting the User's account name under the **Username** heading.

To change the password at any time:

1. Navigate to **CONFIGURE** > **User Management** > **Local Users**
2. Click the Root user's **Edit User** icon below the **Actions** heading.



3. In the **Edit User** page, if required, enter an optional description in the **Description** field. Enter a new password in the **Password** field and re-enter the password in the **Confirm Password** field.

### EDIT USER

User Enabled

Username  
testuser1

Description

Password ⓘ

Confirm Password ⓘ

SSH Password Enabled ⓘ

4. Click **Save User**. A green banner confirms the password change has been saved.

## Disable a Root User

[CONFIGURE > User management > Local Users](#)

To disable a root user:

**Note:** Before proceeding, make sure that another user exists that has the Administrator role or is in a group with the Administrator role. For information on creating, editing, and deleting users, see "[Local Users](#)" on page 96

1. Navigate to **CONFIGURE > User management > Local Users**
2. Click the **Disable User** button in the **Actions** section next to the root user.
3. Click **Yes** in the **Confirmation** dialog.

To enable root user, log in with another user that has the Administrator role and click the **Enable User** button in the **Actions** section next to the root user.

## Change Network Settings

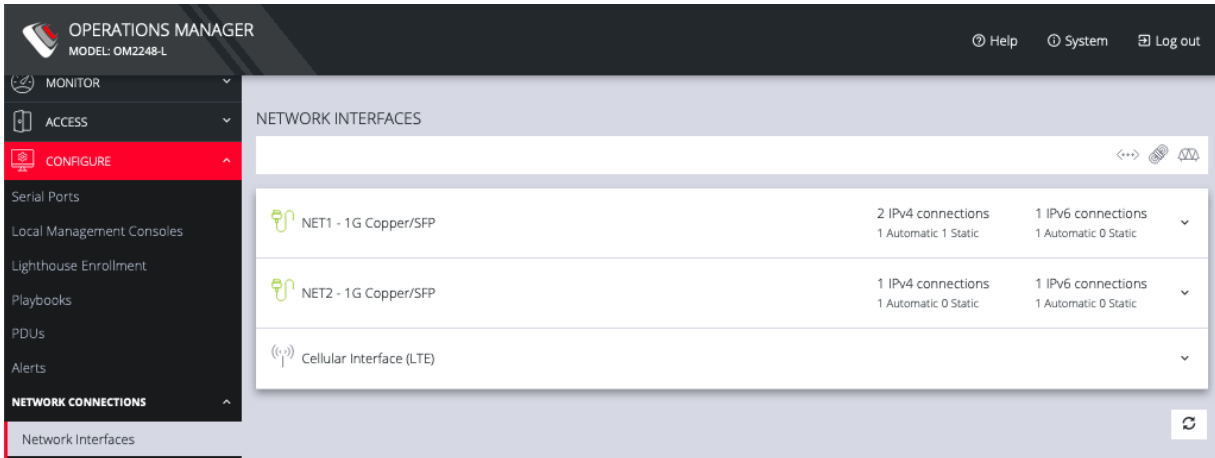
[CONFIGURE > Network Connections > Network Interfaces](#)

The interface supports both IPv4 and IPv6 networks. The IP address of the unit can be setup for Static or DHCP. The following settings can be configured for network ports:

- IPv4, IPv6
- Static and/or DHCP
- Enabling or disabling network interfaces
- Ethernet Media types

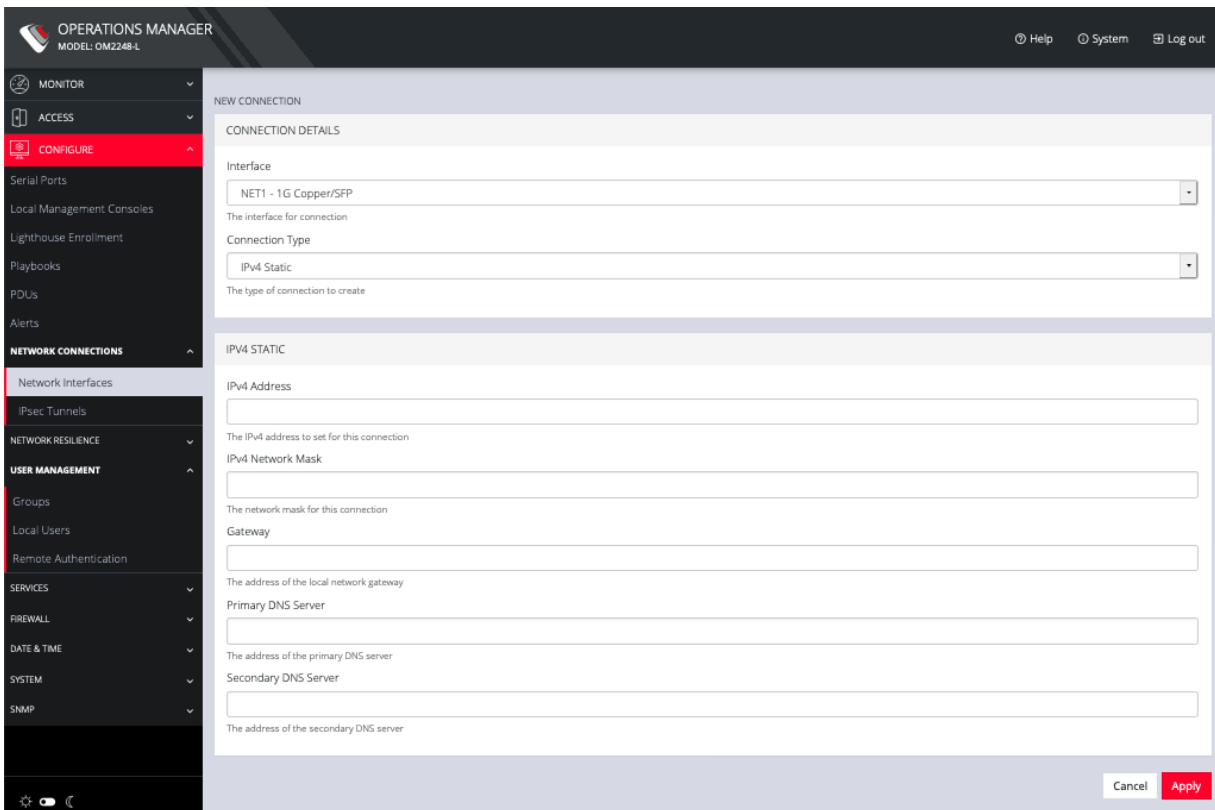
To add a new connection:

1. Click **CONFIGURE** > **Network Connections** > **Network Interfaces**



2. Click the **expand arrow** to the right of the desired interface to view its details.

3. Click the **plus icon** to open the **New Connection** page.



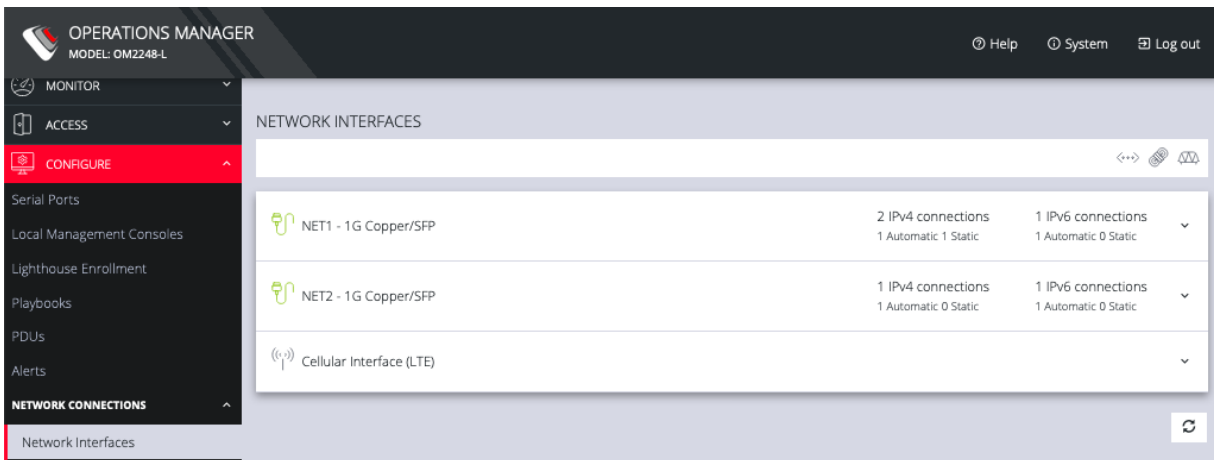
4. Select the **Interface** and **Connection Type** for your new connection.
5. The form on the bottom part of the page will change based on the **Connection Type** you choose. Enter the necessary information and click **Apply**.

To disable or delete interfaces, use the controls on the expanded section on the **CONFIGURE > Network Connections > Network Interfaces** page.

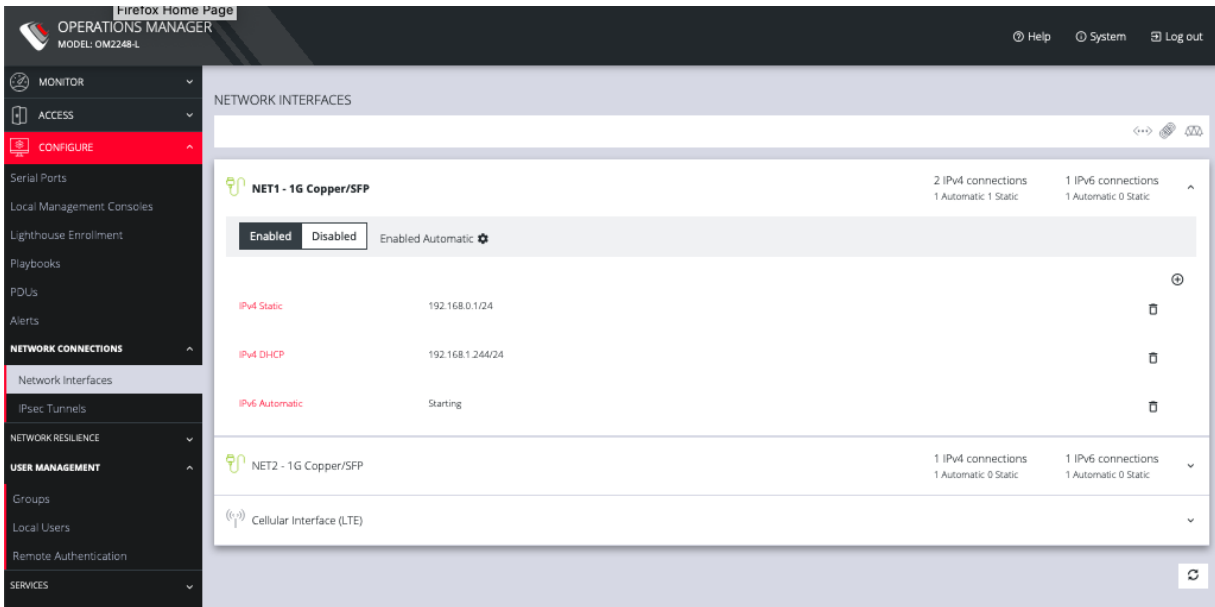
**Note:** If you experience packet loss or poor network performance with the default auto-negotiation setting, try changing the Ethernet Media settings on the OPERATIONS MANAGER and the device it is connected to. In most cases, select 100 megabits, full duplex. Make sure both sides are set identically.

To change the Ethernet Media Type:

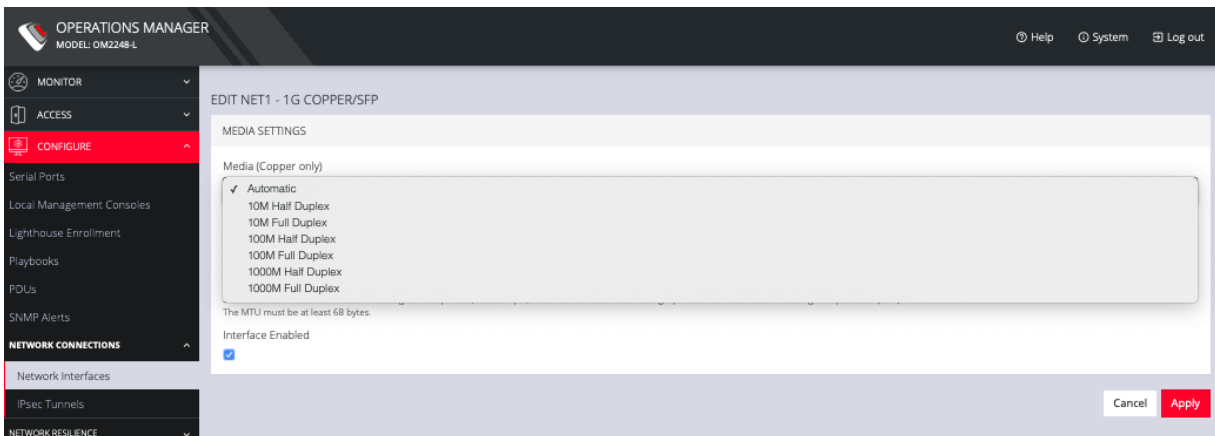
1. Click **CONFIGURE > Network Connections > Network Interfaces**



2. Click the expand arrow to the right of the interface you wish to modify.



### 3. Click **Enabled Automatic**.



### 4. Change the **Media Setting** as needed and click **Apply**.

## MONITOR Menu

The MONITOR Menu is a relatively short section comprising only three topics.

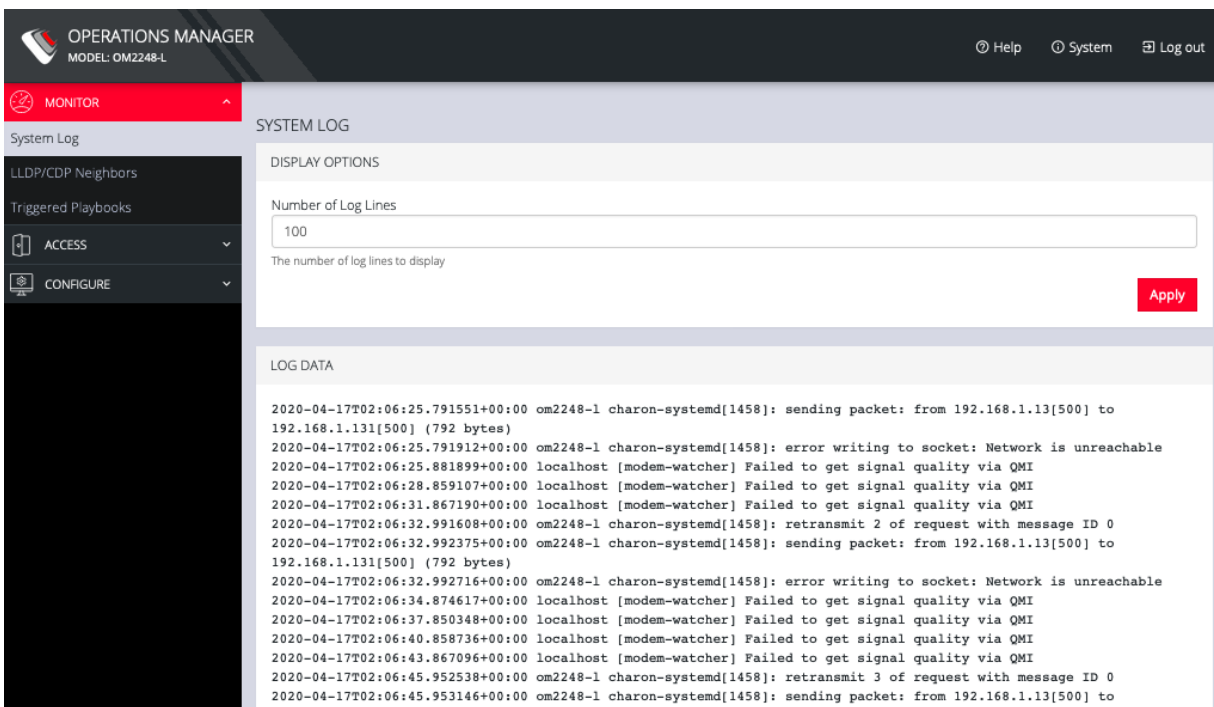
- System Log
  - Details of the system activity log, access and communications events with the server and with attached serial, network and power devices.
- LLDP/CDP Neighbors
  - Details of the LLDP/CDP Neighbors that are displayed when enabled for a connection.
- Triggered Playbooks
  - Monitoring current **Playbooks**, and applying filters to view any Playbooks that have been triggered.

# System Log

## MONITOR > System Log

The OPERATIONS MANAGER maintains a log of system activity, access and communications events with the server and with attached serial, network and power devices.

To view the System Log, click **MONITOR > System Log**.



The screenshot shows the OPERATIONS MANAGER interface for model OM2248-L. The 'MONITOR' menu is active, and the 'System Log' page is displayed. Under 'DISPLAY OPTIONS', the 'Number of Log Lines' is set to 100. Below this, the 'LOG DATA' section shows a list of system events, including packet transmissions and modem-related errors.

```
2020-04-17T02:06:25.791551+00:00 om2248-1 charon-systemd[1458]: sending packet: from 192.168.1.13[500] to 192.168.1.131[500] (792 bytes)
2020-04-17T02:06:25.791912+00:00 om2248-1 charon-systemd[1458]: error writing to socket: Network is unreachable
2020-04-17T02:06:25.881899+00:00 localhost [modem-watcher] Failed to get signal quality via QMI
2020-04-17T02:06:28.859107+00:00 localhost [modem-watcher] Failed to get signal quality via QMI
2020-04-17T02:06:31.867190+00:00 localhost [modem-watcher] Failed to get signal quality via QMI
2020-04-17T02:06:32.991608+00:00 om2248-1 charon-systemd[1458]: retransmit 2 of request with message ID 0
2020-04-17T02:06:32.992375+00:00 om2248-1 charon-systemd[1458]: sending packet: from 192.168.1.13[500] to 192.168.1.131[500] (792 bytes)
2020-04-17T02:06:32.992716+00:00 om2248-1 charon-systemd[1458]: error writing to socket: Network is unreachable
2020-04-17T02:06:34.874617+00:00 localhost [modem-watcher] Failed to get signal quality via QMI
2020-04-17T02:06:37.850348+00:00 localhost [modem-watcher] Failed to get signal quality via QMI
2020-04-17T02:06:40.858736+00:00 localhost [modem-watcher] Failed to get signal quality via QMI
2020-04-17T02:06:43.867096+00:00 localhost [modem-watcher] Failed to get signal quality via QMI
2020-04-17T02:06:45.952538+00:00 om2248-1 charon-systemd[1458]: retransmit 3 of request with message ID 0
2020-04-17T02:06:45.953146+00:00 om2248-1 charon-systemd[1458]: sending packet: from 192.168.1.13[500] to 192.168.1.131[500] (792 bytes)
```

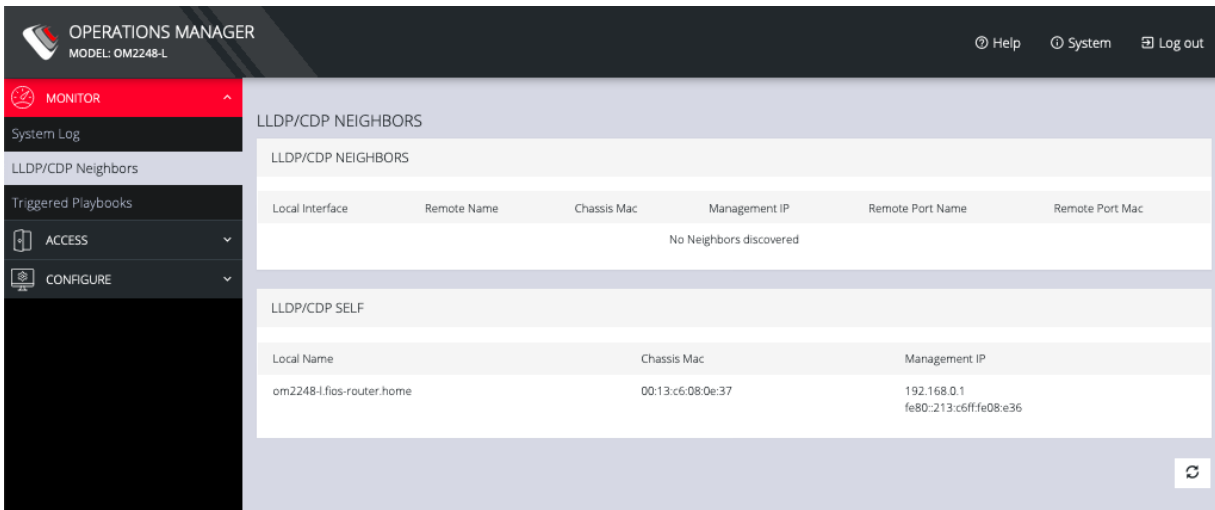
The System Log page lets you change the Number of Log Lines displayed on the screen. The newest items appear on the bottom of the list. Click the Refresh button on the bottom right to see the latest entries.



# LLDP CDP Neighbors

## MONITOR > LLDP/CDP Neighbors

The OPERATIONS MANAGER displays LLDP/CDP Neighbors when enabled for a connection. See **CONFIGURE > SERVICES > Network Discovery Protocols** to enable/disable.



OPERATIONS MANAGER  
MODEL: OM2248-L

Help System Log out

MONITOR

System Log

LLDP/CDP Neighbors

Triggered Playbooks

ACCESS

CONFIGURE

### LLDP/CDP NEIGHBORS

Local Interface	Remote Name	Chassis Mac	Management IP	Remote Port Name	Remote Port Mac
No Neighbors discovered					

### LLDP/CDP SELF

Local Name	Chassis Mac	Management IP
om2248-l.fios-router.home	00:13:c6:08:0e:37	192.168.0.1 fe80::213:c6ff:fe08:e36

Refresh

## Triggered Playbooks

[MONITOR > Triggered Playbooks](#)

For information on creating **Playbooks**, see [Playbooks](#).

To monitor current **Playbooks**, click on **Monitor > Playbooks**. Choose the time period if desired, and filter by **Name** of **Playlist** to view any that have been triggered.



## ACCESS Menu

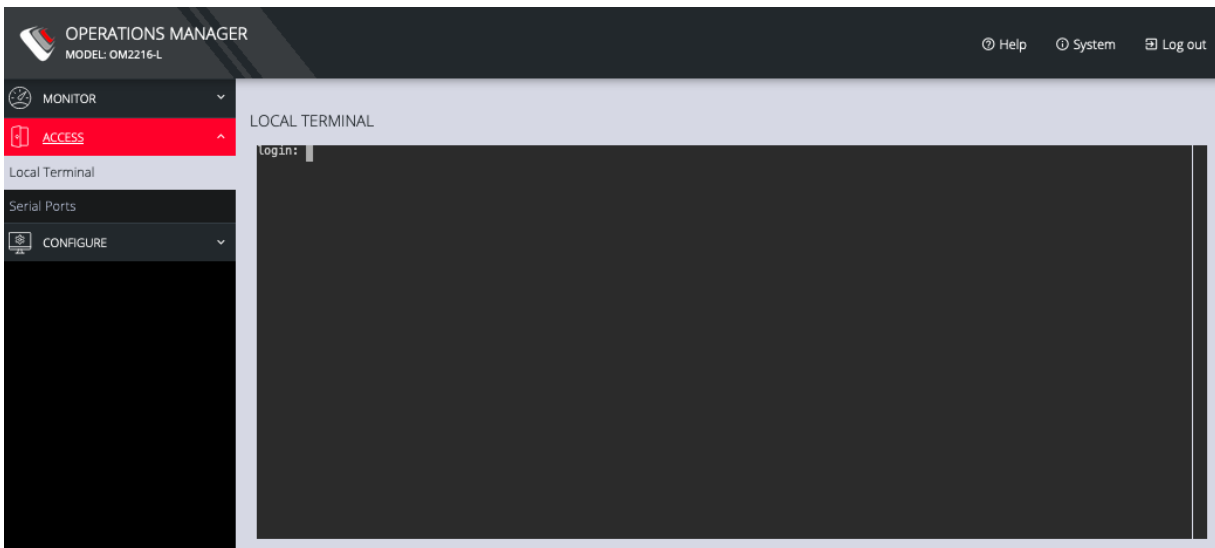
The ACCESS menu lets you access the OPERATIONS MANAGER via a built-in Web Terminal. It also provides SSH and Web Terminal access to specific ports.

## Local Terminal

### [ACCESS > Local Terminal](#)

The OPERATIONS MANAGER includes a web-based terminal. To access this bash shell instance:

1. Select **ACCESS > Local Terminal**.



2. At the log in prompt, enter a username and press Return.
3. At the password prompt, enter a password and press Return.
4. A bash shell prompt appears.

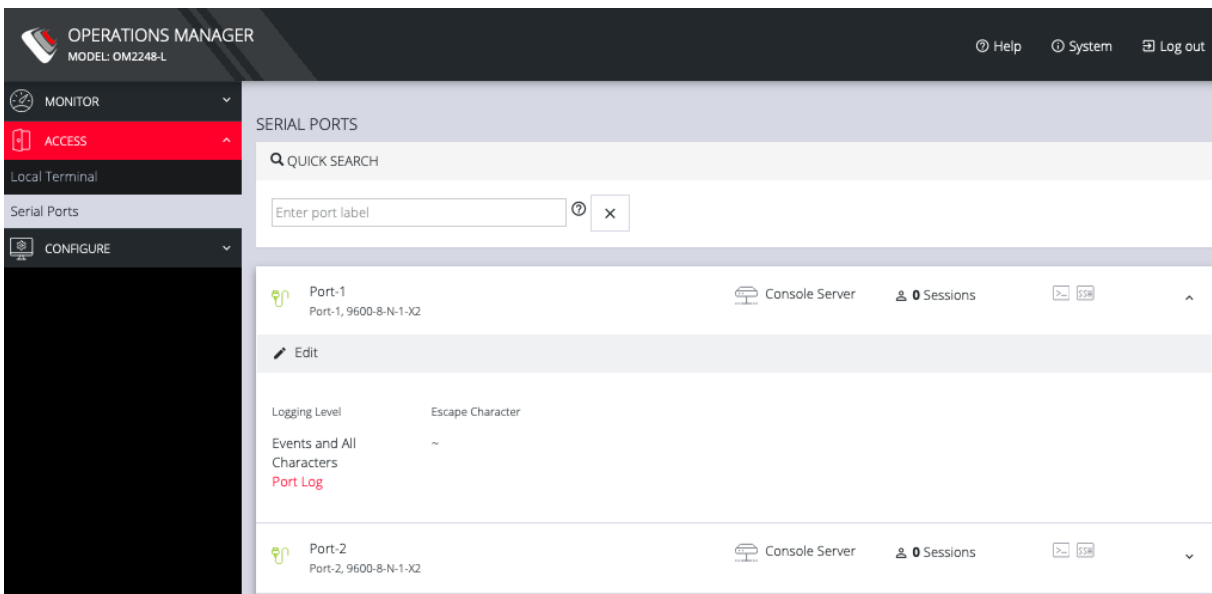
This shell supports most standard bash commands and also supports copy-and-paste to and from the terminal.

To close a terminal session, close the tab, or type exit in the Web Terminal window. The session will timeout after 60 seconds.

## Access Serial Ports

### [ACCESS > Serial Ports](#)

The **ACCESS > Serial Ports** page allows you to quickly locate and access specific ports via Web Terminal or SSH. Click the **expand arrow** to the right of the port to see these options.



### Quick Search

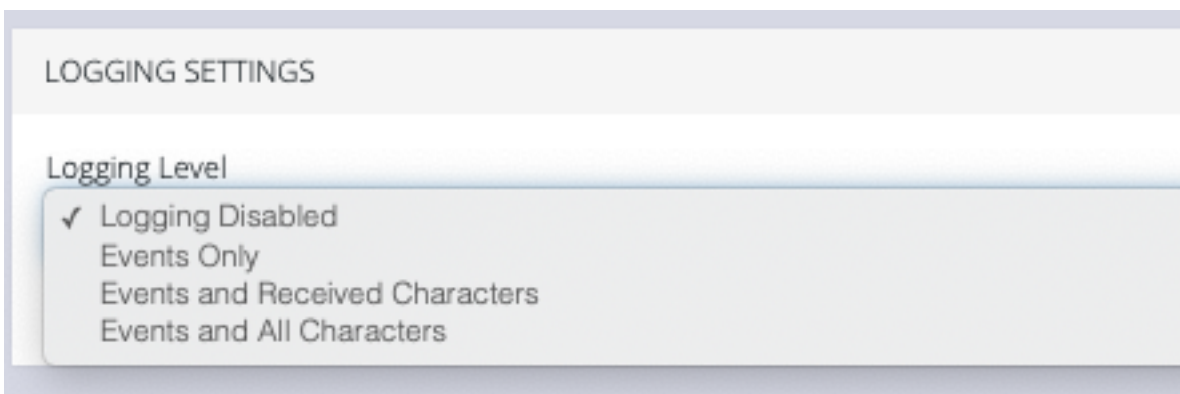
To find a specific port by its port label, use the **Quick Search** form on the top of the **ACCESS > Serial Ports** page. Ports are given default numbered labels. You can set the port label for a given serial port under **CONFIGURE > Serial Ports**. Click the edit button under Actions to open the **EDIT SERIAL PORT** page.

### Access Using Web Terminal or SSH

To access the console port via the Web Terminal or SSH:

1. Locate the particular port on the **ACCESS > Serial Ports** page and click the expand arrow.
2. Click the **Web Terminal** or SSH link for the particular port.
  - Choosing **Web Terminal** opens a new browser tab with the terminal.
  - Choosing **SSH** opens an application you have previously associated with SSH connections from your browser.

**Note:** Serial port logging is disabled by default. Control the logging level for each serial port by changing Logging Settings in **Configure > Serial Ports > Edit** page.



The log will appear via the Port Log link on the **Serial Ports** expanded page.

OPERATIONS MANAGER  
MODEL: OM2248-L

Help System Log out

MONITOR

ACCESS

Local Terminal

Serial Ports

CONFIGURE

### SERIAL PORTS

QUICK SEARCH

Enter port label

Port-1	Port-2
Port-1, 9600-8-N-1-X2	Port-2, 9600-8-N-1-X2
Console Server	Console Server
0 Sessions	0 Sessions
SSM	SSM
^	v

Edit

Logging Level	Escape Character
Events and All Characters	~
Port Log	



## CONFIGURE Menu

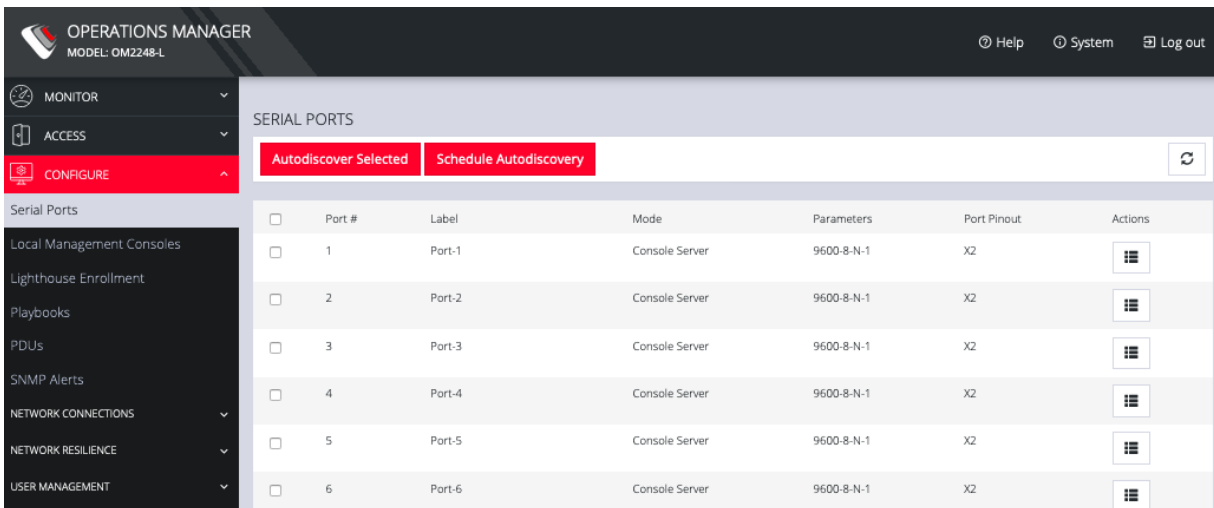
This section provides step-by-step instructions for the menu items under the CONFIGURE menu.









## Serial Ports

[CONFIGURE > Serial Ports](#)

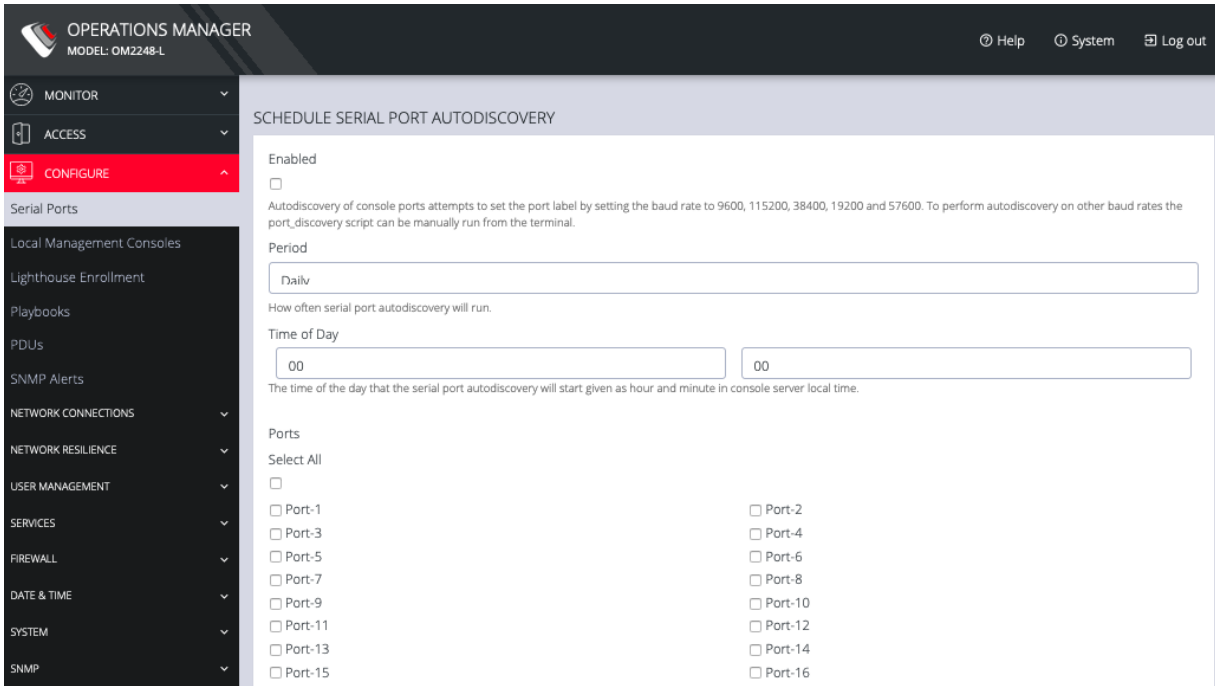
Click **CONFIGURE > Serial Ports**. A list of serial ports appears.



<input type="checkbox"/>	Port #	Label	Mode	Parameters	Port Pinout	Actions
<input type="checkbox"/>	1	Port-1	Console Server	9600-8-N-1	X2	
<input type="checkbox"/>	2	Port-2	Console Server	9600-8-N-1	X2	
<input type="checkbox"/>	3	Port-3	Console Server	9600-8-N-1	X2	
<input type="checkbox"/>	4	Port-4	Console Server	9600-8-N-1	X2	
<input type="checkbox"/>	5	Port-5	Console Server	9600-8-N-1	X2	
<input type="checkbox"/>	6	Port-6	Console Server	9600-8-N-1	X2	

This page lets you select serial ports and **Autodiscover Selected** ports.

You can **Schedule Autodiscover** by clicking the button. This opens a page that allows you to select the ports and specify a time and period for port detection to occur.



The screenshot shows the 'SCHEDULE SERIAL PORT AUTODISCOVERY' configuration page in the OpenGear Operations Manager. The page is titled 'SCHEDULE SERIAL PORT AUTODISCOVERY' and is located under the 'CONFIGURE' menu. The configuration options include:

- Enabled:** A checkbox that is currently unchecked.
- Autodiscovery of console ports:** A text box containing the text: "Autodiscovery of console ports attempts to set the port label by setting the baud rate to 9600, 115200, 38400, 19200 and 57600. To perform autodiscovery on other baud rates the port\_discovery script can be manually run from the terminal."
- Period:** A dropdown menu set to 'Daily'.
- Time of Day:** Two input fields, both containing '00'.
- Ports:** A list of 16 ports (Port-1 to Port-16) with checkboxes next to them. The 'Select All' checkbox is also present and unchecked.

From the **Configure > Serial Ports** page, click the **Edit Serial Port** button under **Actions** next to the Serial Port you wish to configure. The **Edit Serial Port** page opens.

EDIT SERIAL PORT

Label  
Port-1

The serial port unique identifier

Mode  
Console Server

The serial port mode

Port Pinout  
X2 (Cisco Straight)

The cabling pinout used for this port

Baud Rate  
9600

The serial port speed (bps)

Data Bits  
8

The number of data bits to use

Parity  
None

The serial port parity

Stop Bits  
1

The number of stop bits to use

Escape Character  
-

The character used for sending out-of-band shell commands

---

LOGGING SETTINGS

Logging Level  
Events and All Characters

Specify the detail of data to Log  
Warning: output logging will capture and store any user-entered passwords in plain text.

---

SERIAL PORT IP ALIASES

IP Address	Interface	Actions
No IP aliases have been set.		

+

Cancel Apply

The **Edit Serial Port** page lets you configure the serial port's:

- **Label:** This can be used to locate this port using the **Quick Search** form on the **ACCESS > Serial Ports** page.
- **Mode:** **Disabled** or **Console Server**
- **Pin out:** **X1 Cisco Rolled** or **X2 Cisco Straight**
- **Baud Rate:** 50 to 230,400 bps
- **Data Bits:** 5, 6, 7, 8
- **Parity:** None, Odd, Even, Mark, Space
- **Stop Bits:** 1, 1.5, 2



- **Logging Levels**
- **Serial Port Aliases**

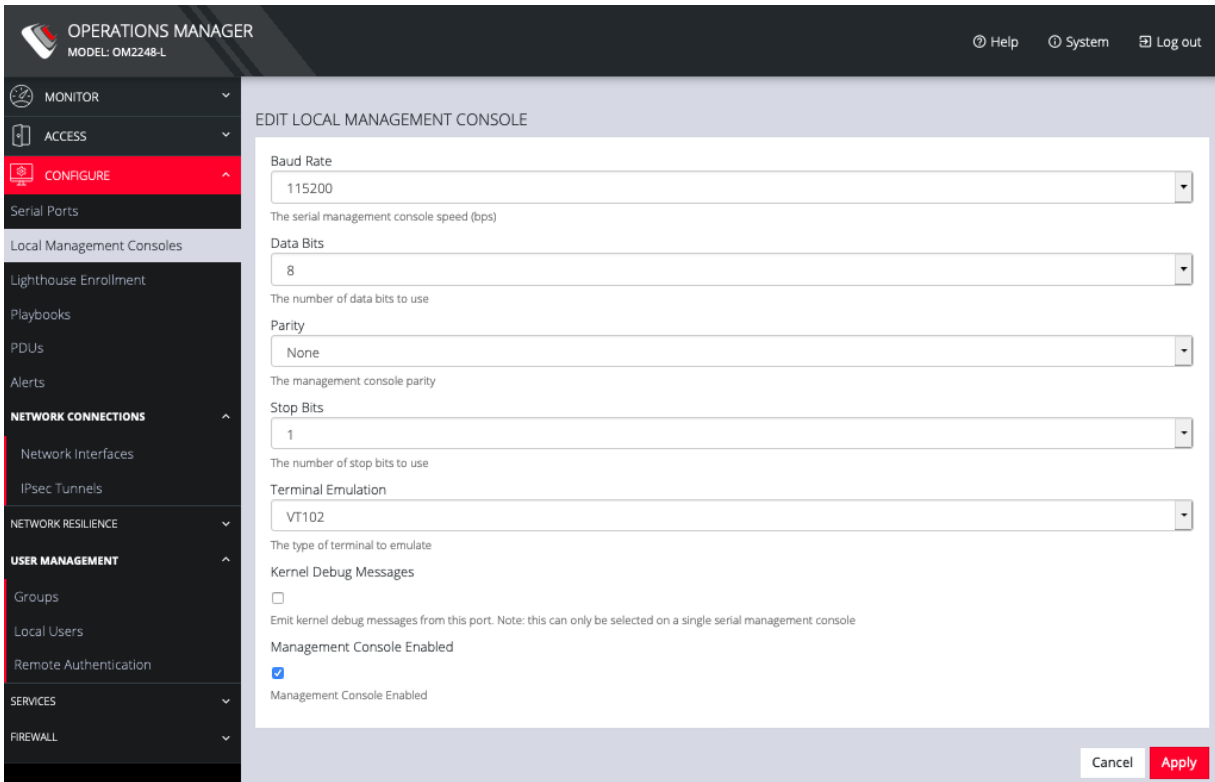
# Local Management Consoles

## CONFIGURE > Local Management Consoles

You can edit settings or disable the local RJ45 serial console (Cisco straight -X2 pinout) and the USB serial console (needs user supplied micro-USB to USB-A cable).

To edit the settings of a local management console:

1. Click **CONFIGURE > Local Management Consoles**.
2. Click on the **Edit Management Console Port** button under **Actions** next to the console you wish to disable.



3. The **Edit Local Management Console** page lets you control:

- **Baud Rate**
- **Data Bits**
- **Parity**
- **Stop Bits**
- **Terminal Emulation**
- Enable or disable **Kernel Debug Messages**
- Enable or disable the selected **Management Console**

**Note:** Enabling **Kernel Debug Messages** can only be applied to a single serial management console.

To disable a local management console, click **CONFIGURE > Local Management Consoles**. Click on the **Disable Management Console Port** button under **Actions** next to the console you wish to disable.

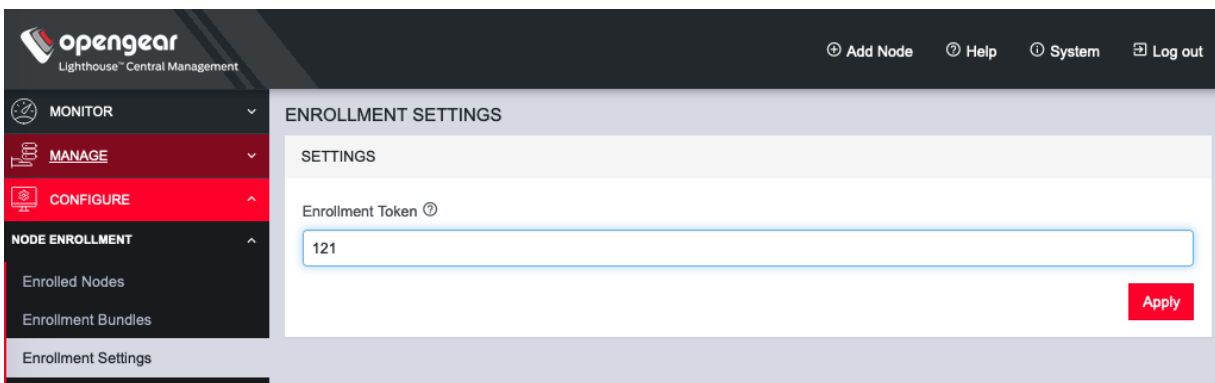
# Lighthouse Enrollment

[CONFIGURE > Lighthouse Enrollment](#)

Opengear appliances can be enrolled into a Lighthouse instance, providing centralized access to console ports, NetOps Automation, and central configuration of Opengear devices.

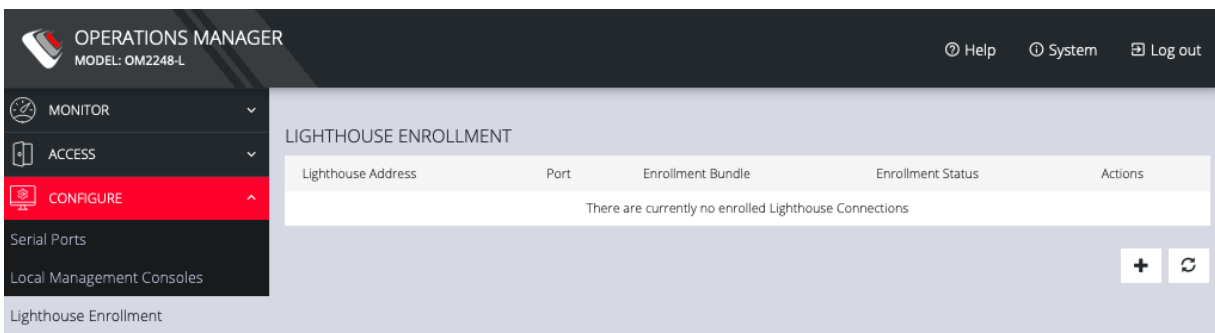
To enroll your OPERATIONS MANAGER to a Lighthouse instance, you must have Lighthouse installed and have an enrollment token set in Lighthouse.

To set an enrollment token in Lighthouse, click on **CONFIGURE > NODE ENROLLMENT > Enrollment Settings** page, and enter an **Enrollment Token**.

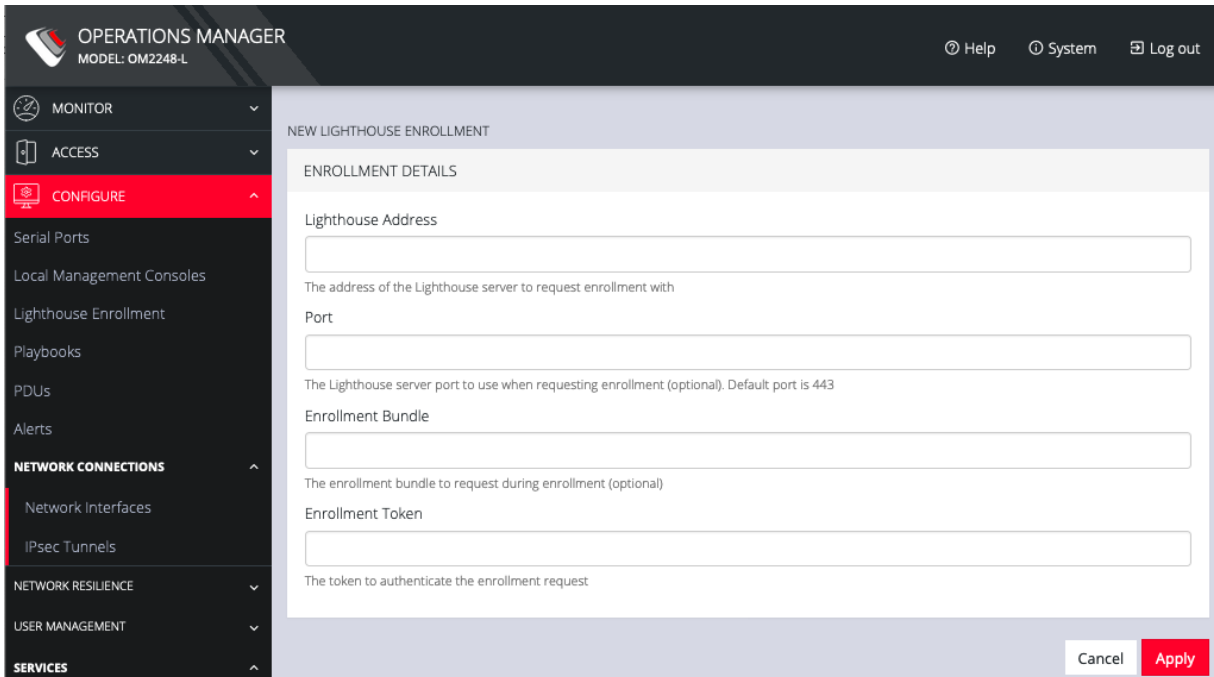


To enroll your OPERATIONS MANAGER in this Lighthouse instance:

1. Click **CONFIGURE > Lighthouse Enrollment**.



2. Click on the **Add Lighthouse Enrollment** button on the bottom right. The **New Lighthouse Enrollment** page opens.



The screenshot shows the 'OPERATIONS MANAGER' interface with the 'CONFIGURE' menu item selected. The main content area is titled 'NEW LIGHTHOUSE ENROLLMENT' and contains the following fields:

- ENROLLMENT DETAILS**
- Lighthouse Address**: A text input field with a description: 'The address of the Lighthouse server to request enrollment with'.
- Port**: A text input field with a description: 'The Lighthouse server port to use when requesting enrollment (optional). Default port is 443'.
- Enrollment Bundle**: A text input field with a description: 'The enrollment bundle to request during enrollment (optional)'.
- Enrollment Token**: A text input field with a description: 'The token to authenticate the enrollment request'.

At the bottom right of the form, there are two buttons: 'Cancel' and 'Apply'.

3. Enter the IP address or fully qualified domain name of the Lighthouse instance and the **Enrollment Token** you created in Lighthouse. Optionally enter a **Port** and an **Enrollment Bundle** (see the [Lighthouse User Guide](#) for more information).
4. Click **Apply**.

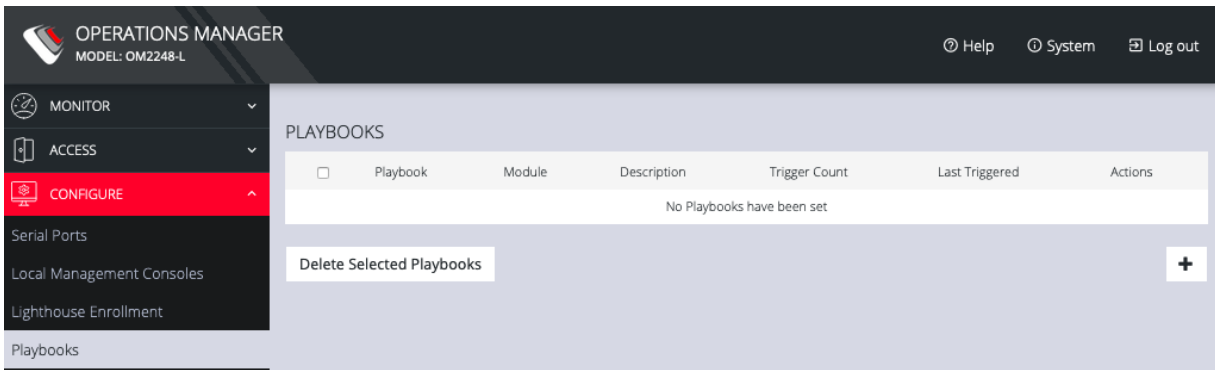
**Note:** Enrollment can also be done directly via Lighthouse using the Add Node function. See the Lighthouse User Guide for more instructions on enrolling Opengear devices into Lighthouse.



# Playbooks

[CONFIGURE > Playbooks](#)

**Playbooks** are configurable systems that periodically check if a **Trigger** condition has been met. They can be configured to perform a one or more specified **Reaction**. To create a new Playbook, select **Configure > Playbooks**.



Click the **Plus** button to create a new **Playbook**.

#### ADD PLAYBOOK

##### TRIGGER

Auto Response Playbooks are configurable systems that check periodically if a Trigger condition is met and may perform Reactions if configured.

Name

The name used to identify this Playbook.

Description

A detailed description of this Playbook.

Status

 Enabled  Disabled

Interval (Seconds)

The frequency in seconds at which the Trigger check should be performed.

Trigger Type

The type of Trigger to be used with this Playbook. When the Trigger condition is met, one or more configured Reactions will be executed.

##### REACTION

Reactions are configurable events that occur when a Trigger condition is met.

No Reactions have been configured.



Cancel Apply

1. Enter a **Name** for the **Playbook**.
2. Add a **Description**.
3. Select **Enabled** to activate the **Playbook** after you have created it.
4. Enter an **Interval** in seconds to control the frequency that the **Trigger** will be checked.
5. Choose the type of **Trigger** to use from the **Trigger Type** drop down.
6. In the **Reaction** section, click the **Plus** and click on specific **Reactions** for this **Playbook**.

REACTION

Reactions are configurable events that occur when a Trigger condition is met.

Cell Message	Custom Command	Serial Text	Slack	SNMP	x
--------------	----------------	-------------	-------	------	---

Name

The name used to identify this Reaction.

+

Clicking on each **Reaction** opens a custom screen to provide necessary information. When you are finished, click **Apply**.

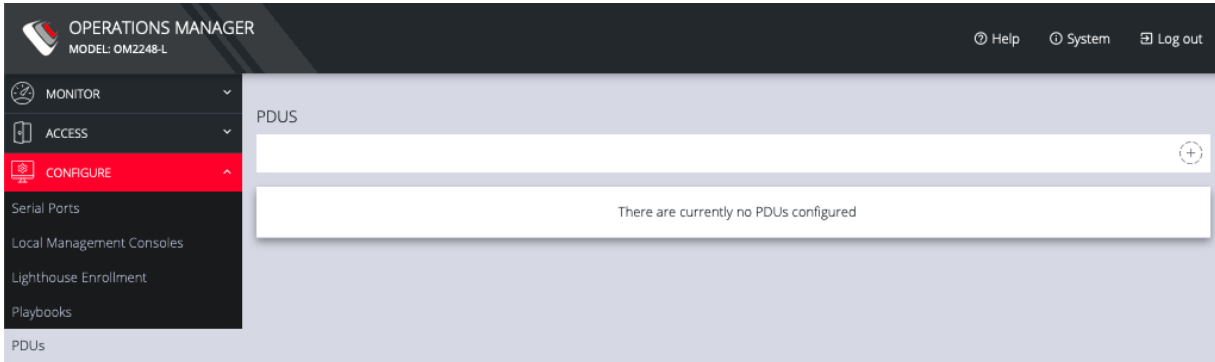
After you have created **Playbooks**, you can **Edit** or **Delete** them from the **Configure > Playbooks** page.

To monitor current **Playbooks**, click on **Monitor > Playbooks**. Choose the time period if desired and filter by **Name** of **Playlist** to view any that have been triggered.

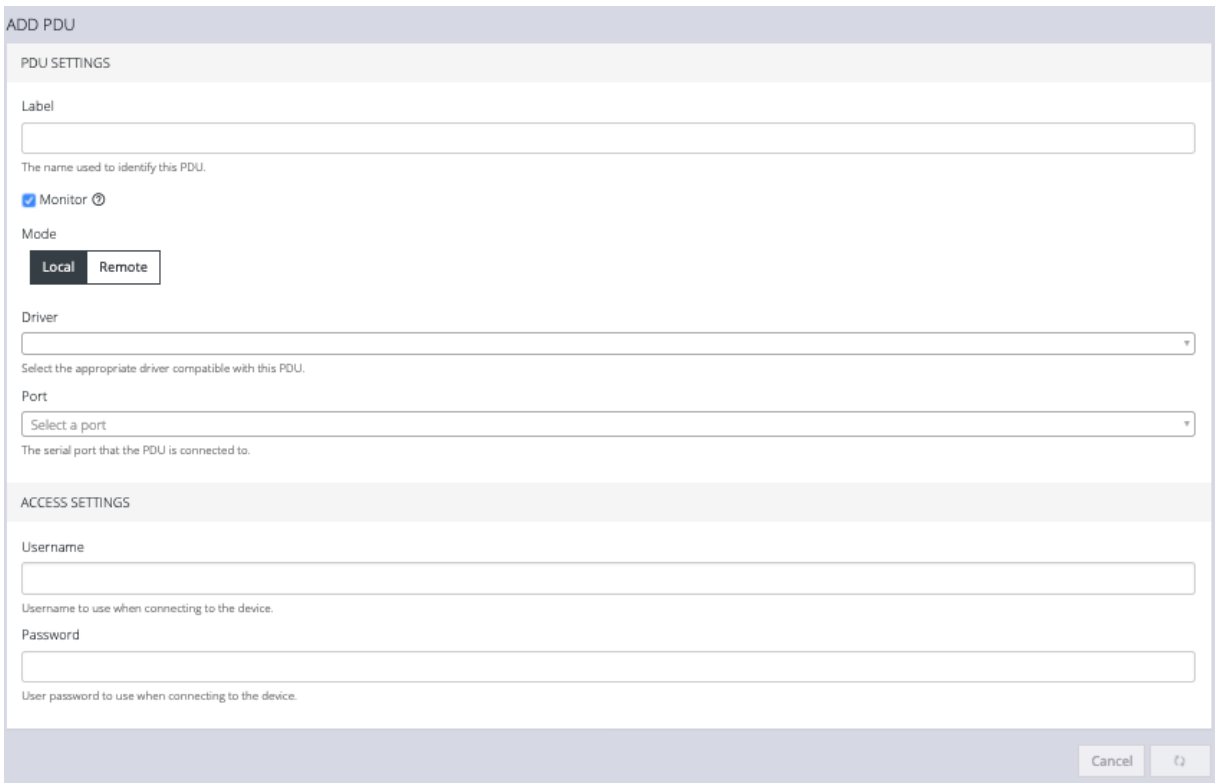
# PDU's

## CONFIGURE > PDUs

One or more Power Distribution Units (**PDUs**), both **Local** and **Remote** can be monitored. To add information for a **PDU**, select **Configure > PDUs**.



Click the **Plus** button to configure a new **PDU**.



**ADD PDU**

**PDU SETTINGS**

Label  
  
The name used to identify this PDU.

Monitor ⓘ

Mode

Driver  
  
Select the appropriate driver compatible with this PDU.

Port  
  
The serial port that the PDU is connected to.

**ACCESS SETTINGS**

Username  
  
Username to use when connecting to the device.

Password  
  
User password to use when connecting to the device.



1. Enter a **Label** for this **PDU**.
2. Select the **Monitor** checkbox.
3. Choose **Local** or **Remote**.
4. Select the appropriate **Driver** from the drop-down list.
5. Select the **Port**.
6. Add a **Description**.
7. Under **Access Settings**, enter a **Username** and **Password** to use when connecting to the device.
8. When you are finished, click **Apply**.

After you have created **PDU**s, you can **Edit** or **Delete** them from the **Configure > PDU**s page.

## SNMP Alerts

[CONFIGURE > SNMP Alerts > System/Power/Networking](#)

**Tip:** For more detailed information about configuring SNMP Alerts see the individual topic pages that follow.

On the **CONFIGURE > SNMP Alerts** page; SNMP Alert Managers can be added or deleted under **SNMP > SNMP Alert Managers**, for the following:

- **System:** Covers notification for the following causes.
  - **Authentication:** Notifies when a user attempts to log in via SSH, REST API, Web UI, or the device's serial ports. An alert is sent regardless of whether the log in has succeeded or failed.
  - **Configuration:** For changes that occur to the system configuration.
  - **System Temperature:** When temperature SNMP alerts are enabled, network operators are immediately notified should the system begin operating outside user-defined tolerances.
- **Power:** When voltage SNMP alerts are enabled, network operators are immediately notified should the PSU begin operating outside design tolerances. See "[SNMP Alerts Power](#)" on page 58 for further information.
- **Networking (Cell Signal Strength):** Be notified when cell signal strength leaves or re-enters the selected range, or when the network link state changes. A slider adjusts the upper and lower signal strength.

**Tip:** Manage the SNMP settings on the **CONFIGURE > SNMP > SNMP Alert Managers** page.

# SNMP Alerts System - Temperature, Authentication, Configuration

## Temperature

[CONFIGURE > SNMP Alerts > System > System Temperature](#)

It is essential to ensure that the system is operating within its design temperature as premature aging of the component can occur if the device is excessively hot during operation. This can lead to component failure and ultimately result in RMA.

When temperature SNMP alerts are enabled (Alerting), network operators are immediately notified (subject to network connectivity and latency) should the PSU begin operating outside user-defined temperature tolerances.

System generated SNMP Alerts send SNMP traps to a remote SNMP manager which alerts the user of temperature events.

**Tip:** The OM device can send network, power and system events to the remote SNMP manager.

## Configure SNMP System Temperature Alerts

[Configure > SNMP Alerts > System > System Temperature](#)

The System Temperature Range alert reports the system temperature (measured at **System Temperature 1** and **System Temperature 2** sensors) and sends an alert when the system temperature leaves or enters the user-configured temperature range.

1. Navigate to Configure > SNMP Alerts > System > System Temperature.
2. Click on the **Alerting** button to activate the function, this also activates the user-defined range sliders.

**Note:** The **Not Alerting** button de-activates the function and temperature alerts will be stopped until activated again.

3. Click+Drag the temperature range limiters to the required upper and lower limits.
4. Click **Apply**. The **Details Saved** banner confirms your settings.

#### SYSTEM TEMPERATURE

A temperature notification will be sent when any of the temperature sensors leaves or re-enters the specified range.

Alerting  Not Alerting

Temperature Range

-  Degrees Celsius

~ 122 - 210 Degrees Fahrenheit

In this image, if any temperature sensor reports the system temperature (measured at **System Temperature 1** and **System Temperature 2** sensors) to be less than 50 degrees C or greater than 99 degrees C, an SNMP alert will be triggered.

**Tip:** The temperature display is automatically converted to Fahrenheit.

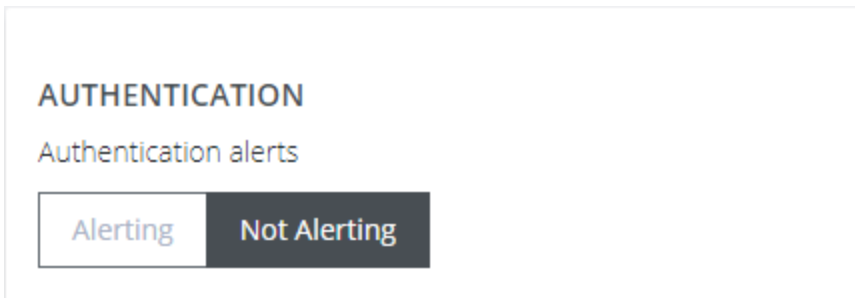


## Authentication

[CONFIGURE > SNMP Alerts > System > Authentication](#)

Notifies when a user attempts to log in via SSH, REST API, or the device's serial ports. An alert is sent regardless of whether the log in has succeeded or failed.

1. Navigate to [Configure > SNMP Alerts > System > Authentication](#).
2. Click on the **Alerting** button to activate the function.
3. Click **Apply**. The **Details Saved** banner confirms your settings.

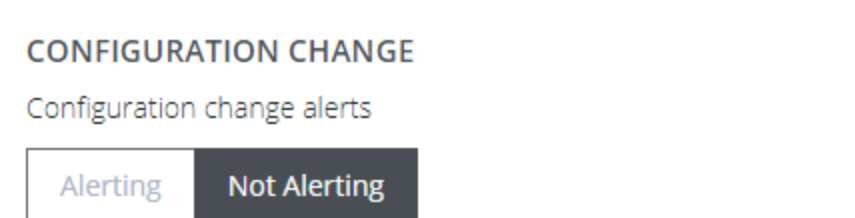


## Configuration

[CONFIGURE > SNMP Alerts > System > Configuration](#)

Notifies of changes that occur to the system configuration.

1. Navigate to [Configure > SNMP Alerts > System > Configuration](#).
2. Click on the **Alerting** button to activate the function.
3. Click **Apply**. The **Details Saved** banner confirms your settings.



## SNMP Alerts Power

[Configure > SNMP Alerts > Power > Voltage](#)

The PSU is one of the most critical part of the OM device so it is essential to ensure that the PSU is operating within its design tolerances.

When voltage SNMP alerts are enabled, network operators are immediately notified of PSU failures (subject to network connectivity and latency). Should the PSU begin operating outside design tolerances, PSU-related SNMP Alerts will trigger an alert for the following conditions:

- Output DC voltage of both PSUs

If the voltage drops too low, it risks the device going into brown-out state. If it gets too high, it can damage components.

System generated SNMP Alerts send SNMP traps to a remote SNMP manager which alerts the user of system events. The OM device can send network, power and system events to the remote SNMP manager.

**Tip:** The OM device can send network, power and system events to the remote SNMP manager.

## Configure Power Alerts

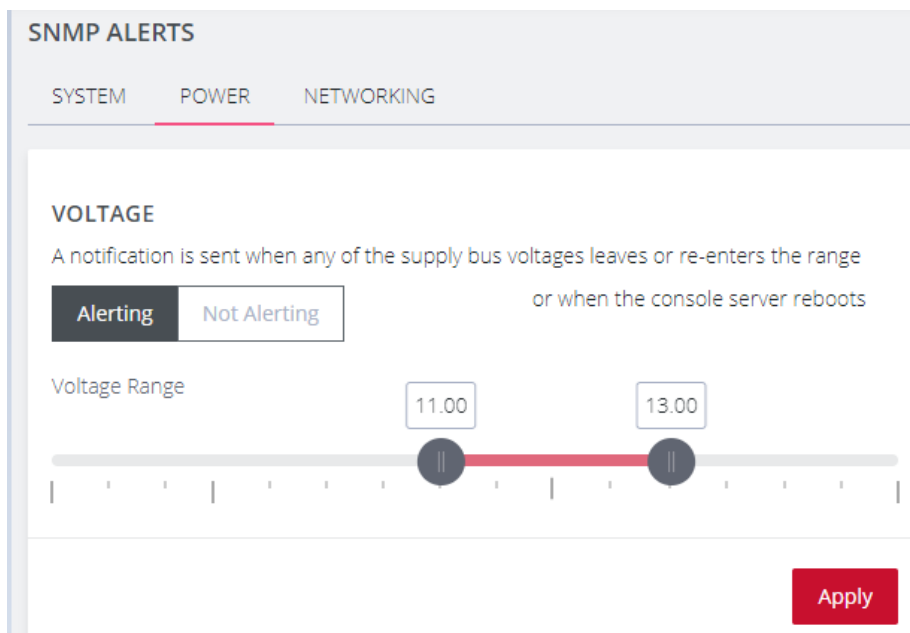
[Configure > SNMP Alerts > Power > Voltage](#)

The alert related to this functionality is the System Voltage Range alert which sends an alert when the system reboots or the voltage on either power supply leaves or enters the user-configured voltage range.

1. Navigate to Configure > SNMP Alerts > Power > Voltage.
2. Click on the **Alerting** button to activate the function, this also activates the user-defined range sliders.

**Note:** The **Not Alerting** button de-activates the function and power alerts will be stopped until activated again

3. Click+Drag the voltage range limiters to the required upper and lower limits.
4. Click **Apply**. The **Details Saved** banner confirms your settings.



SNMP ALERTS

SYSTEM POWER NETWORKING

**VOLTAGE**

A notification is sent when any of the supply bus voltages leaves or re-enters the range or when the console server reboots

Alerting Not Alerting

Voltage Range

11.00 13.00

Apply

In the above image, if any power supply fails, is disconnected or some other power anomaly occurs which causes the voltage to drop below 11V or above 13V, an SNMP alert will be triggered.

**Warning:** The recommended safety settings are 11.4 ~ 12.6 volts.

When an event occurs that causes the voltage range on any power supply to re-enter the configured voltage range, it will cause an SNMP alert to be triggered.

## SNMP Alerts Networking (Connection Status)

[Configure > SNMP Alerts > Networking > Network Connection Status](#)

The alert related to this functionality is the Network Connection Status which sends an alert when cell signal strength leaves or re-enters a user-defined range, or, when the network link state changes. A slider adjusts the upper and lower signal strength limits.

### Configure Signal Strength Alerts

[Configure > SNMP Alerts > Networking > Network Connection Status](#)

To set the Network Connection Status signal strength boundaries:

1. Navigate to [Configure > SNMP Alerts > Network Connection Status > Signal Strength](#) page.
2. Click on the **Alerting** button to activate the function, this also activates the user-defined range sliders.
3. Click+Drag the signal strength range limiters to the required upper and lower limits.

**Note:** The **Not Alerting** button de-activates the function and signal strength alerts will be stopped until activated again.

4. Click **Apply**. The **Details Saved** banner confirms your settings.

### NETWORK CONNECTION STATUS

Be notified when cell signal strength leaves or re-enters the range, or when the network link state changes.

**Alerting** Not Alerting

Signal Strength

33 66

0 25 50 75 100

Apply

In the above image, if any anomaly occurs that causes the signal strength to drop below 33 or above 66, an SNMP alert will be triggered.

When an event occurs that causes the signal strength to re-enter the user-defined range, an SNMP alert will be triggered.

## Network Connections

[CONFIGURE > NETWORK CONNECTIONS](#)

The **Network Connections** menu contains the **Network Interfaces** and **IPsec Tunnels** settings.

## Network Interfaces

[CONFIGURE > NETWORK CONNECTIONS > Network Interfaces](#)

The interface supports both IPv4 and IPv6 networks. The IP address of the unit can be setup for Static or DHCP. The following settings can be configured for network ports:

- IPv4, IPv6
- Static and/or DHCP
- Enabling or disabling network interfaces
- Ethernet Media types

For detailed information about Network Interface configuration and adding a new connection, see ["Change Network Settings" on page 27](#).

## Dual SIM

[CONFIGURE > NETWORK CONNECTIONS > Network Interfaces > Cellular Interface \(LTE\)](#)

Operations Manager has been available for some time with support for two SIM cards/slots, whereby, it is possible designate which SIM slot is the Active SIM that is normally used by the device for OOB communications (in Automatic failover mode this SIM is termed the Primary SIM). The secondary SIM is used as a failover SIM. This feature increases the reliability of the OOB solution by providing redundant Out-Of-Band access over a cellular connection.

**Note:** The terminology changes when SIM Failover policy is switched from **Manual** to **Automatic**. In Manual failover mode the active SIM is designated ACTIVE, whereas in Automatic failover mode the active SIM is designated PRIMARY.

With the Dual SIM feature activated, in the event of a failure of OOB communications through the Active SIM, it is possible to manually de-select the failed SIM and activate the secondary SIM by making *it* the Active SIM. This changeover allows OOB communications to resume through the newly designated Active SIM.

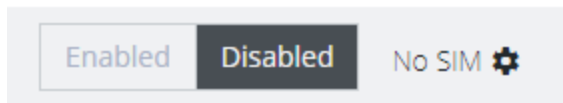
### Display SIM Status and Signal Strength

**Note:** For information about configuring the **Signal Strength Thresholds** see: ["SNMP Alerts" on page 54](#)

1. Navigate to Configure > Network Connections > Network Interfaces.
2. Click on the **Cellular Interface (LTE)** row.



## Cellular Interface (LTE)

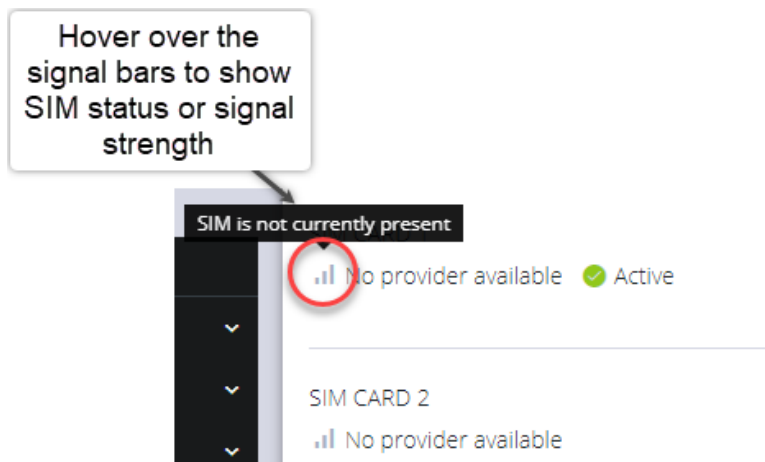


3.

The information bar expands, and the page shows the current status of the active and inactive SIM cards.

**Note:** If the unit does not have a cell modem (-L) then the cellular interface will not be visible.

4. The active SIM indicates the color of the signal strength based upon the selected thresholds in **Configure** → **SNMP Alerts** under the **Networking Signal Strength Alert**.



The signal bar color (not the number of bars) indicates signal strength:

- **Green** if signal is above the higher threshold.
- **Orange** if signal is between lower and higher threshold.
- **Red** if signal is below the lower threshold,
- **Grey** for 0 or not active,

5. Click the **Refresh** button to display the current signal strength of the active SIM.



**Note:** When the **Refresh** button is clicked the signal strength is only updated for the active SIM. If you would like to know what the other SIM Signal Strength is, you need to activate it, let the modem come back online, which may take 3 minutes or more.

## Installing A New SIM Card

Before installing a new SIM card, the OM device must first be powered down. This can be done by switching off the power supply and waiting until the device has shut-down. Install the new SIM card into its slot, then restart the device

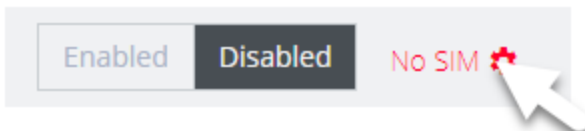
**Note:** The device will not recognize the new SIM card unless a shut-down and restart is performed. The new SIM card will be read during start-up.

## Select The Active SIM (Manual Failover Mode)

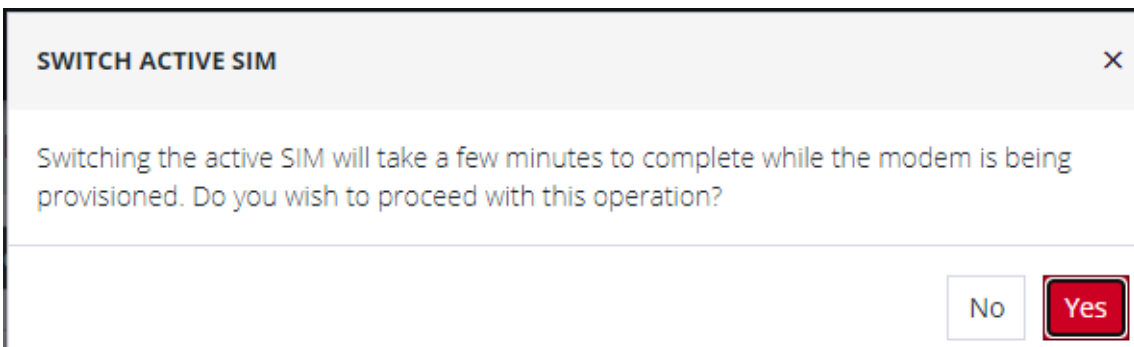
Switching the active SIM must be done manually. To switch the Active SIM:

1. Navigate to **CONFIGURE > NETWORK CONNECTIONS > Network Interfaces > Cellular Interface (LTE)**.
2. Click the **Settings cog** , this will display the **MANAGE CELLULAR INTERFACE (LTE)** page and the current status of both SIM slots, including the current carrier name.

 **Cellular Interface (LTE)**



3. On the right, select the **Make Active** button of the new, active SIM and apply the change by selecting **Confirm**.
4. A pop-up alert states that this operation will take a few minutes to complete. Click **Yes** to confirm the change.



**Note:** During the change-over the current IP address is hidden and then returned when the modem re-connects.

5. If you require, you can monitor the interface during the changeover via the CLI with the command:.

```
watch ip address show dev wwan0
```

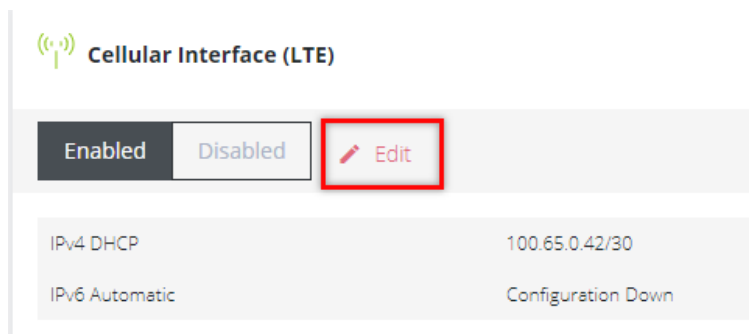
You can also set the SIM settings by expanding the menu for each SIM to set the APN.

If no SIM is inserted you can still select a SIM slot. If you insert a SIM it will not force it to become the active SIM.

## Select The Primary SIM (Automatic Failover Mode)

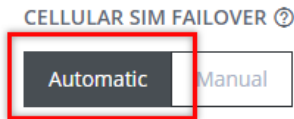
Switching the primary SIM must be done manually. To switch the Primary SIM:

1. Navigate to **CONFIGURE > NETWORK CONNECTIONS > Network Interfaces > Cellular Interface (LTE)**.
2. Click the **Edit** icon, this will display the **MANAGE CELLULAR INTERFACE (LTE)** page and the current status of both SIM slots.



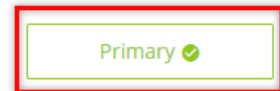
3. Ensure the cellular interface is enabled by clicking the **Enabled** button.

4. Under **Cellular SIM Failover** click the **Automatic** button, this will display the **Primary** selection buttons.

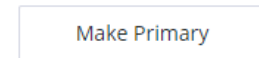


▲ Cellular SIM Failover may take a few minutes due to the need to switch firmware.

Primary - SIM CARD 1  
Verizon Wireless  
ICCID: 8914800005844013102  
SIM Settings ▾



Secondary - SIM CARD 2  
AT&T Wireless Inc.  
ICCID: 89010303300021797361  
SIM Settings ▾



5. Click the **Primary** button of the SIM selected to be the primary SIM.
6. Click the **Confirm** button at the bottom of the page. A green banner will appear to confirm that the new settings have been saved.

## Dual SIM Automatic Failover

[CONFIGURE > NETWORK CONNECTIONS > Network Interfaces > Cellular Interface \(LTE\)](#)

Devices that carry two SIM cards can be configured so that either SIM card slot may be activated. In Automatic failover mode, either of the two SIM cards may be designated as the Primary SIM. (see ["Dual SIM" on page 64](#)).

Dual SIM Automatic Failover works seamlessly with the existing failover solution to provide another layer of redundancy. This feature allows the software to detect a failure in OOB communications via the Primary SIM and will automatically failover to the Secondary SIM without the need for manual operator intervention.

Options within the configuration also allow you to configure the failback settings from Secondary SIM, back to the previous Primary SIM when OOB communications have been restored. See ["Cellular Interface Policy Settings" on page 74](#).

**Note:** The terminology changes when SIM Failover policy is switched from **Manual** to **Automatic**. In Manual mode the active SIM is designated ACTIVE, whereas in Automatic failover mode the active SIM is designated PRIMARY.

See the image on the following page for a depiction of Primary and Secondary SIM card slots.

Either of the SIM card slots can be designated as the Primary SIM. In the following image, SIM card 1 has been designated as the Primary SIM and is currently the active SIM, while SIM card 2 is designated as the Secondary SIM which, (in the scenario below), is only activated in the event of an automatic failover such as occurs during an OOB communications failure on the Primary SIM.

**CELLULAR SIM FAILOVER** ⓘ

Automatic  Manual

⚠ Cellular SIM Failover may take a few minutes due to the need to switch firmware.

---

Primary - SIM CARD 1  
📶 Verizon Wireless  
ICCID: 8914800005844013102  
SIM Settings ▾

Primary ✓

---

Secondary - SIM CARD 2  
📶 AT&T Wireless Inc.  
ICCID: 89010303300021797361  
SIM Settings ▾

Make Primary

## Failover Modes

Features of Automatic Failover include:

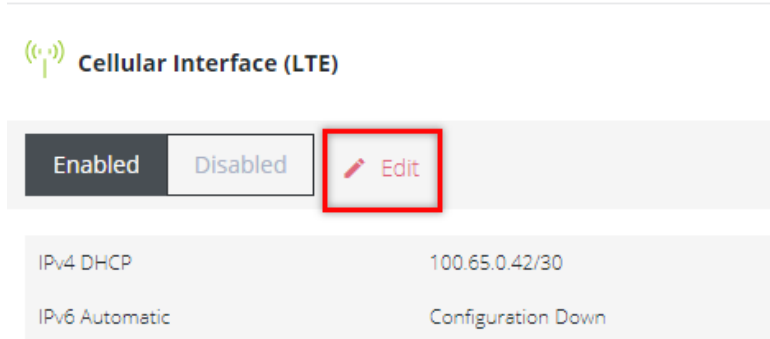
- Select either **Manual** or **Automatic** SIM failover.
- Specify SIM failback policy (applicable when the Ethernet connection and primary SIM are both down):
  - **Upon disconnect** - See the table "[Cellular Interface Policy Settings](#)" on [page 74](#) for an explanation of the policy.
  - **After a Delay** (specified in minutes) - The device switches back to primary after a pre-defined time has elapsed.
  - **Never** - The device never switches back to the Primary.
- SIM failover settings allow you to configure the parameters that affect cellular data usage, for example, quicker failover (consumes more data) vs less frequent tests (consumes less data). The configuration preferences include
  - Ping test for failover from Primary to Secondary and failback from Secondary to Primary.
  - Failover settings are per SIM slot and consist of a failover and failback ping test.
- Automatic Failover functions in both dormant and non-dormant mode.



## Activate or Configure Automatic Failover

[CONFIGURE > NETWORK CONNECTIONS > Network Interfaces > Cellular Interface \(LTE\) > Manage Cellular Interface \(LTE\)](#)

1. Navigate to the Cellular Interface page at: [CONFIGURE > NETWORK CONNECTIONS > Network Interfaces > Cellular Interface \(LTE\)](#).
2. Click the **Edit** link next to the Cellular Interface Enabled/Disabled switch.



3. In the Manage Cellular Interface page, select the **Automatic** failover option.
4. Ensure the correct SIM card is selected as the Primary SIM (see 'Set Primary SIM' in ["Dual SIM" on page 64](#)).
5. Complete the Cellular Interface options in accordance with the table below.
6. Click **Confirm** to activate the failover policy settings, a green banner will confirm the settings are enabled.

## Cellular Interface Policy Settings

MANAGE CELLULAR INTERFACE (LTE) Properties	
Field	Definition
CELLULAR SIM FAILOVER - <b>Manual/Automatic.</b>	Automatically switch between the Primary SIM Card and the secondary SIM Card on dis-connection.
<b>Primary SIM Failover</b>	
Failover Probe Address.	Network address to probe in order to determine if connection is active. <b>Note:</b> The probe address accepts IPv4, IPv6 addresses and hostnames.
Test interval (seconds).	The number of seconds between connectivity probe tests.
Pings per test.	The maximum number of times a single ping packet is sent per probe before considering the probe failed.
Consecutive test failures before failover.	The number of times a probe must fail before the connection is considered failed.
<b>Failback Policy</b>	
Never / Delayed / On Dis-connect.	Select the policy to be used to determine Failback recovery from the Secondary SIM Card back to the Primary SIM Card.
Never	No Failback recovery is attempted.
Delayed	Attempted failback after $n$ minutes. The number of minutes after failover to the secondary SIM Card that the connection should failback to the Primary SIM Card.

On Disconnect	Secondary SIM Failback
	<b>Failback Probe Address</b> ie. The Network address to probe in order to determine if the connection is active.
	<b>Test Interval</b> The number of seconds between connectivity probe tests (this not the same thing as Attempted Failback).
	<b>Pings per Test</b> The maximum number of times a single ping packet is sent per probe before considering the probe failed.
	<b>Consecutive Test Failures (before failover)</b> The number of times a probe must fail before the connection is considered failed.

## Network Aggregates - Bonds and Bridges

[CONFIGURE > NETWORK CONNECTIONS > Network Interfaces > Select the target interface](#)

The Network Aggregates feature allows you to create or edit bridges that contain any type of interface or other config options which are included in a bridge or bond after it is created, without having to delete the bridge or bond and start over. Such changes can be made remotely without organizing a site visit.. The supported configuration options for bonds and bridges are discussed in the Bridge and Bond Definitions tables later in this topic.

This also includes other settings on bonds, such as the mode or poll interval.

**Note:** Editing the primary interface will not update its connections.

Operations Manager models with an integrated switch (OM1204-4E, OM1208-8E and OM2224-24E) have a bridge configured by default that includes all of the switch ports, which can be edited or deleted as required.

Definitions of the bridge details as in the **Bridge Form Definitions** table below.

### Create A New Bridge

**Note:** Whether creating a new bridge or editing an existing bridge the page is very similar.

To create a new bridge:

1. Navigate to the **Configure > Network Connections > Network Interfaces** page on the Web UI.
2. Click on the **New Bridge** button that is located at the top-right of the window.

3. Select which interface will serve as the primary interface for the new bridge.

**Note:** When the primary interface is selected, its MAC address is displayed in the MAC address field. This MAC address is inherited by the new bridge interface.

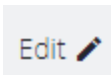
4. Complete the new bridge details form as in the **Bridge Form Definitions** definitions table below.
5. Click the **Create** button to finalize the creation of the new bridge.

## Edit an Existing Bridge

To edit an existing bridge:

1. Navigate to the **Configure > Network Connections > Network Interfaces** page on the Web UI.
2. Click on the bridge that you would like to edit, the bridge details are expanded.
3. Click on the bridge **Edit** button that is located next to the Enable / Disable toggle buttons.
4. Select which interface will serve as the primary interface for the new bridge.
5. Change the bridge details as required in accordance with the **Bridge Form Definitions** table below.
6. Click the **Update** button to finalize the edit process. Updating the bridge will temporarily interrupt network activity on this interface.

## Edit Bridge Form Definitions

New Bridge Field	Definition
Description	The editable <b>Description</b> field allows you to add a description of the interface. If the description field is not completed the field will default to a computed value to describe the interface.
Enable Spanning Tree Protocol?	Spanning Tree Protocol allows Operation Manager devices to: <ul style="list-style-type: none"> <li>• Discover and eliminate any unexpected networks loops so that there is no broadcast radiation and the network stays healthy and reliable</li> <li>• Be able to function with redundant links (intentional network loops) to increase the networks reliability and fault tolerance</li> </ul>
Network Interface Selection	Click the check box of each network interface you want to include in the bridge.
Primary Interface	Select the interface that is to be used for selecting the MAC address of the aggregate. The new bond inherits the MAC address of the primary interface. On creation, any Network Connections which exist on the Primary Interface will be attached to the Bond/Bridge after it is initially created. When a Bond/Bridge is deleted, any Network Connections which exist on the aggregate interface are handed over to the Primary Interface.
Inherited Connections	When the Primary Interface is selected, the connections inherited by the new bridge are listed here.
	Click to edit the details of an existing interface.

## Create A New Bond

**Note:** Whether creating a new bond or editing an existing bond the page is very similar.

To create a new bond:

1. Navigate to the **Configure > Network Connections > Network Interfaces** page on the Web UI.
2. Click on the **New Bond** button that is located at the top-right of the window.
3. Select which interface will serve as the primary interface for the new bond.

**Note:** When the primary interface is selected, its MAC address is displayed in the MAC address field. This MAC address is inherited by the new bond interface.

4. Complete the new bond details form as in the **Bond Form Definitions** definitions table below.
5. Click the **Create** button to finalize the creation of the new bond. Network connections from non-primary interfaces will be deleted when the new bond is created.

## Edit an Existing Bond

To edit an existing bond:

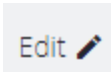
1. Navigate to the **Configure > Network Connections > Network Interfaces** page on the Web UI.
2. Click on the bond that you would like to edit, the bond details are expanded.
3. Click on the bond **Edit** button that is located next to the Enable / Disable toggle buttons.

4. Change the bond details as required in accordance with the **Edit Bond Form Definitions** table below.
5. Click the **Update** button to finalize the edit process. Updating the bond will temporarily interrupt network activity on this interface.

## Edit Bond Form Definitions

New Bond Field	Definition
Description	The editable <b>Description</b> field allows you to add a description of the interface. If the description field is not completed the field will default to a computed value to describe the interface.
Mode	The mode determines the way in which traffic sent out via the bonded interface is dispersed over the real interfaces. Available modes are:
	<b>Round Robin Balancing</b> - Packets are sequentially transmitted/received through each interfaces one by one.
	<b>Active Backup</b> - If the active secondary interface is changed during a failover, the bond interface's MAC address is then changed to match the new active secondary's MAC address.
	<b>XOR Balancing</b> - Balances traffic by splitting up outgoing packets between the Ethernet interfaces, using the same one for each specific destination when possible.
	<b>Broadcast</b> - All network transmissions are sent on all secondary interfaces. This mode provides fault tolerance.
	<b>802.3ad (Dynamic Link Aggregation)</b> - Aggregated NICs act as one NIC, but also provides failover in the case that a NIC fails. Dynamic Link Aggregation requires a switch that supports IEEE 802.3ad.



	<p><b>Transmit Load Balancing</b> - Outgoing traffic is distributed depending on the current load on each secondary interface. Incoming traffic is received by the current secondary interface. If the receiving secondary fails, another secondary takes over the MAC address of the failed secondary.</p> <p><b>Adaptive Load Balancing</b> - Includes transmit load balancing (tlb) and receive load balancing (rlb) for IPv4 traffic and does not require any special switch support.</p>
Poll Interval	The poll interval specifies the MII link monitoring frequency in milliseconds. This determines how often the link state of each secondary is inspected for link failures. A value of zero disables MII link monitoring.
Network Interface Selection	Click the check box of each network interface you want to include in the bridge.
Primary Interface	Select the interface that is to be used for selecting the MAC address of the aggregate. The new bond inherits the MAC address of the primary interface. On creation, any Network Connections which exist on the Primary Interface will be attached to the Bond/Bridge after it is initially created. When a Bond/Bridge is deleted, any Network Connections which exist on the aggregate interface are handed over to the Primary Interface.
Active Connections	When the Primary Interface is created, the connections inherited by the new bond are listed here. When edited, Active Connections on the aggregate will not be updated if the primary interface is changed.
	Click to edit the details of an existing interface. Updating a bridge will temporarily interrupt network activity on the interface when you click the <b>Update</b> button.

## Spanning Tree Protocol

[CONFIGURE > NETWORK CONNECTIONS > Network Interfaces > Select the target interface](#)

Spanning Tree Protocol (STP) allows Operation Manager devices to discover and eliminate loops in network bridge links, preventing broadcast radiation and allowing redundancy.

When STP is implemented on switches to monitor the network topology, every link between switches, and in particular redundant links, are cataloged. The spanning-tree algorithm blocks forwarding on redundant links by setting up one preferred link between switches in the LAN. This preferred link is used for all Ethernet frames unless it fails, in which case a non-preferred redundant link is enabled.

### **Note: STP Limitations**

If multiple bridges are created on the same switch they should not be used on the same network segment as they have the same MAC addresses, therefore STP will likely not work correctly as they will have the same bridge id.

Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP) and other proprietary protocols are not supported.

The bridge settings relating to STP cannot be changed from the default values shown below:

group\_address

forward\_delay (default is 15)

hello\_time (default is 2)

max\_age (default is 20)

priority (default is 32768 (0x8000))

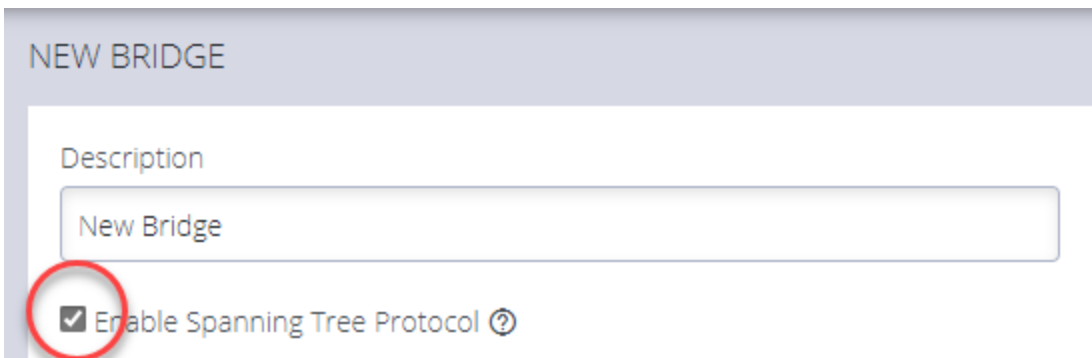
## Enable STP in a Bridge

To enable STP you can use the UI or CLI. The procedures are:

### Bridge With STP Enabled - UI

CONFIGURE > NETWORK CONNECTIONS > Network Interfaces > Select the target interface > New Bridge page

1. In the **Network Interfaces** page, click the **Create New Bridge** button.
2. Click to select the **Enable Spanning Tree Protocol** option.



NEW BRIDGE

Description

New Bridge

Enable Spanning Tree Protocol ?

### Bridge With STP Enabled - OGCLI

```
admin@om2248:~# ogcli get physif system_net_physifs-5
  bridge_setting.id="system_net_physifs-5"
  bridge_setting.stp_enabled=true
description="Bridge"
  device="br0"
enabled=true
id="system_net_physifs-5"
  media="bridge"
name="init_br0"
  slaves[0]="net2.3"
```

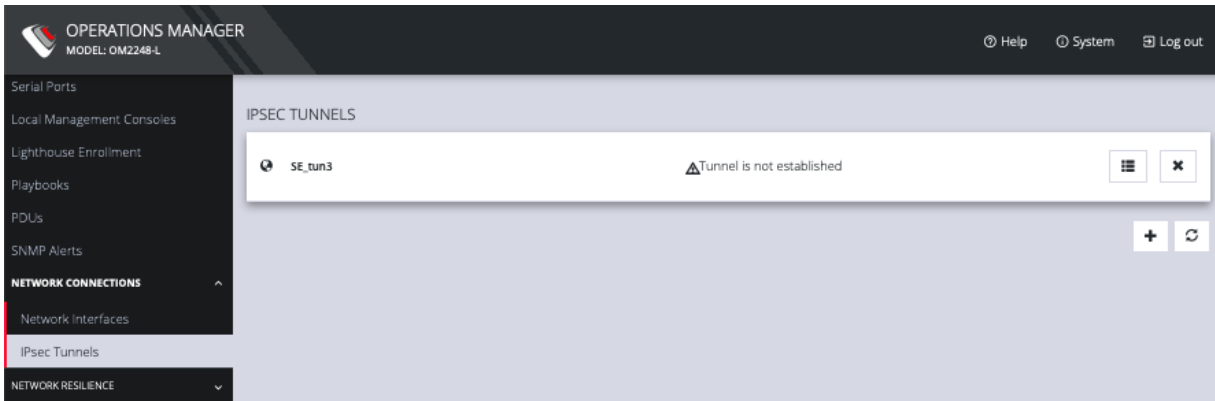
## Bridge With STP Disabled - OGCLI

```
admin@om2248:~# ogcli update physif system_net_physifs-5
bridge_setting.stp_enabled=false
bridge_setting.id="system_net_physifs-5"
bridge_setting.stp_enabled=false
description="Bridge"
device="br0"
enabled=true
id="system_net_physifs-5"
media="bridge"
name="init_br0"
slaves[0]="net2.3"
```

# IPsec Tunnels

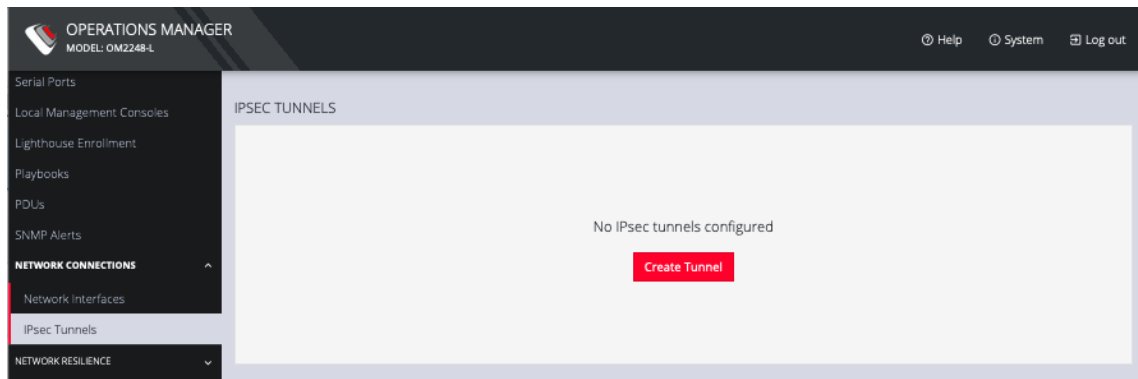
[CONFIGURE > NETWORK CONNECTIONS > IPsec Tunnels](#)

On the IPsec Tunnels page, you can create, edit, and delete IPsec tunnels.



To create an IPsec tunnel:

1. Click **CONFIGURE > NETWORK CONNECTIONS > IPsec Tunnels**.



2. Click **CREATE TUNNEL**. This opens the **EDIT IPSEC TUNNEL** page.

EDIT IPSEC TUNNEL SE\_TUN3

TUNNEL CONFIGURATION

Enabled

Name

Each IPsec tunnel must have a unique symbolic name. The name can contain letters, digits, and hyphens. It will appear in log messages when the tunnel is being established. Use this to distinguish between multiple tunnels on the device.

IKE Protocol Version  
 IKEv2  
 IKEv1 Main Mode  
 IKEv1 Aggressive Mode

Select the IKE protocol version to be used for exchanging keys. IKEv1 provides two modes: Main and Aggressive. When using IKEv1, Main Mode is recommended. Aggressive Mode is considered less secure because the hash of the pre-shared key is exchanged unprotected.

Cipher Suite Proposal  
 Negotiable  
 Negotiable with PFS

A set of algorithms used for negotiation when attempting to establish the IPsec tunnel. By default, the device will attempt to negotiate the tunnel using a list of common algorithms which are considered safe. Alternatively, a set of default proposals that guarantee Perfect Forward Secrecy (PFS) can be selected.

Initiate

When **Initiate** is selected, the device will actively initiate the tunnel by sending IKE negotiation packets to the remote end.

Outer Local Address

Enter a local IP address to be used as the source address of the tunnel.

Outer Remote Address

Enter the IP address or hostname of the remote end of the tunnel.  
When **Initiate** is selected, IKE negotiation packets will be sent to this address. Otherwise incoming IKE negotiation packets must originate from this address.

3. In the top section of the page, **TUNNEL CONFIGURATION**, click the **Enabled** check box and give your new tunnel a name.
4. Select an **IKE Protocol Version** to use for exchanging keys. IKEv1 provides two modes: **Main** and **Aggressive**. When using IKEv1, Main Mode is recommended. Aggressive Mode is considered less secure because the hash of the pre-shared key is exchanged unprotected.
5. Select a **Cipher Suite Proposal**. This is a set of algorithms used for negotiation when attempting to establish the IPsec tunnel. By default, the device will attempt to negotiate the tunnel using a list of common algorithms which are considered safe. Alternatively, a set of default proposals that guarantee Perfect Forward Secrecy (PFS) can be selected.
6. Click the **Initiate** checkbox to actively initiate the tunnel by sending IKE negotiation packets to the remote end.

7. Enter an **Outer Local Address**, a local IP address to use as the source address of the tunnel
8. Enter an **Outer Remote Address**, the IP address or hostname of the remote end of the tunnel.
9. Scroll down to the **Traffic Selectors** section of the page.

TRAFFIC SELECTORS

The traffic selectors specify which IP traffic will be sent through this tunnel. Each traffic selector is a comma-separated list of subnets in CIDR notation or IP addresses. For example: **192.168.0.1** matches a single IP address, or **10.1.0.0/16,10.2.0.0/16** matches two subnets.

Typically the remote traffic selector configured on this device must match the local traffic selector configured on the other end of the tunnel, and vice versa.

Local Subnet

Specify local traffic to be tunneled.  
When no subnets are specified, only traffic originating from this device will be tunneled.

Remote Subnet

Specify addresses or subnets which are behind the remote end of this tunnel.  
When no subnets are specified, only traffic originating from the outer remote address will be accepted.

10. Enter a **Local Subnet** and **Remote Subnet**.
11. Scroll down to the third section, **AUTHENTICATION**.

AUTHENTICATION

PSK Shared Secret

For the pre-shared key authentication mode, both ends of the tunnel must use the same key.

Local ID

Specify the identity of this end of the tunnel, to be presented during IKE negotiation. Fill this in if the remote end requires it for authentication.  
To construct ID\_USER\_FQDN type identities, use `user@example.com`.  
To construct ID\_FQDN type identities, use `@host.example.com`.  
If this is left blank, the outer local IP address of the tunnel is used as the identity.

Remote ID

Specify the expected identity of the remote end of the tunnel. The tunnel will only be established if the remote end's identity matches this value. This field accepts the same syntax as the **Local ID**.  
If this is left blank, any remote identity will be accepted.

Cancel Save

12. Enter a **PSK Shared Secret**.
13. Enter a **Local ID** and **Remote ID**.
14. Click **Save**. The new tunnel is now listed on the **CONFIGURE > NETWORK CONNECTIONS > IPsec Tunnels** page.





## Network Resilience

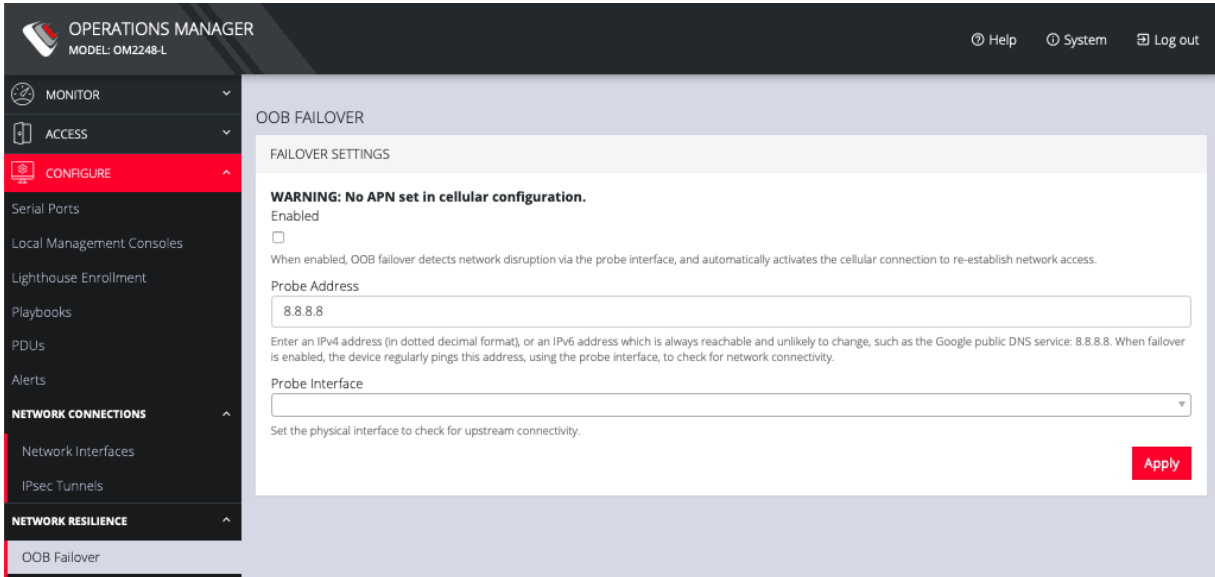
[CONFIGURE > NETWORK RESILIENCE >](#)

Under the NETWORK RESILIENCE menu, you can manage Out-of-Band (OOB) and IP Passthrough settings.

# OOB Failover

[CONFIGURE](#) > [NETWORK RESILIENCE](#) > [OOB Failover](#)

To manage Out-of-Band failover, click **CONFIGURE**  
> **NETWORK RESILIENCE** > **OOB Failover**:



The screenshot shows the 'OPERATIONS MANAGER' interface for model 'OM2248-L'. The left sidebar contains navigation options: MONITOR, ACCESS, CONFIGURE (highlighted), Serial Ports, Local Management Consoles, Lighthouse Enrollment, Playbooks, PDUs, Alerts, NETWORK CONNECTIONS (with sub-items Network Interfaces and IPsec Tunnels), and NETWORK RESILIENCE (with sub-item OOB Failover). The main content area is titled 'OOB FAILOVER' and contains 'FAILOVER SETTINGS'. A warning message states: 'WARNING: No APN set in cellular configuration.' Below this, there is an 'Enabled' checkbox which is currently unchecked. A descriptive text explains that when enabled, OOB failover detects network disruption via the probe interface and automatically activates the cellular connection. The 'Probe Address' field contains '8.8.8.8'. A note below the field states: 'Enter an IPv4 address (in dotted decimal format), or an IPv6 address which is always reachable and unlikely to change, such as the Google public DNS service: 8.8.8.8. When failover is enabled, the device regularly pings this address, using the probe interface, to check for network connectivity.' The 'Probe Interface' is shown as a dropdown menu. A final instruction reads: 'Set the physical interface to check for upstream connectivity.' An 'Apply' button is located at the bottom right of the settings area.

# IP Passthrough

[CONFIGURE > NETWORK RESILIENCE > IP Passthrough](#)

To manage **IP Passthrough** settings click **CONFIGURE > NETWORK RESILIENCE > OOB Failover:**

### IP PASSTHROUGH

#### SETTINGS

Enable ⓘ

Interface

NET1 - 1G Copper/SFP

NET2 - 1G Copper/SFP

The device will offer a DHCP lease for the cellular IP address on this interface.

Downstream MAC Address

The DHCP lease will only be offered to this MAC address. DHCP requests from other MAC addresses will be ignored. Enter the MAC address of the downstream device.

#### SERVICE INTERCEPTS


When IP Passthrough is enabled above, access to this device directly via the cellular interface will no longer work. You can configure specific ports below which will be redirected to this device instead of the downstream device.

HTTPS Intercept Port

Enter a port to be redirected to this device's HTTPS service. You can use this port to access the Operations Manager web interface. If you leave this field blank, the HTTPS service intercept will be disabled.

SSH Intercept Port

Enter a port to be redirected to this device's SSH service. You can use this port to access the Operations Manager command line interface. If you leave this field blank, the SSH service intercept will be disabled.

 **Apply**

## User Management

### [CONFIGURE > USER MANAGEMENT](#)

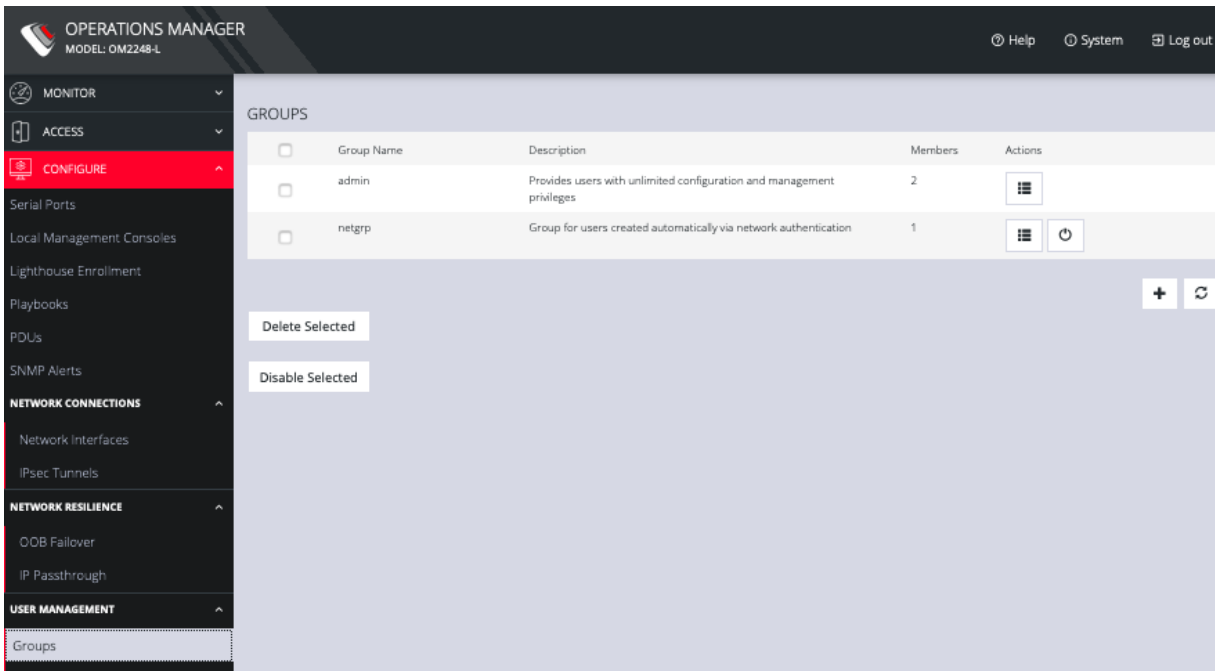
Under the User Management menu, you can create, edit, and delete groups and users, as well as assign users to groups. You can also set up remote user authentication.

# Groups

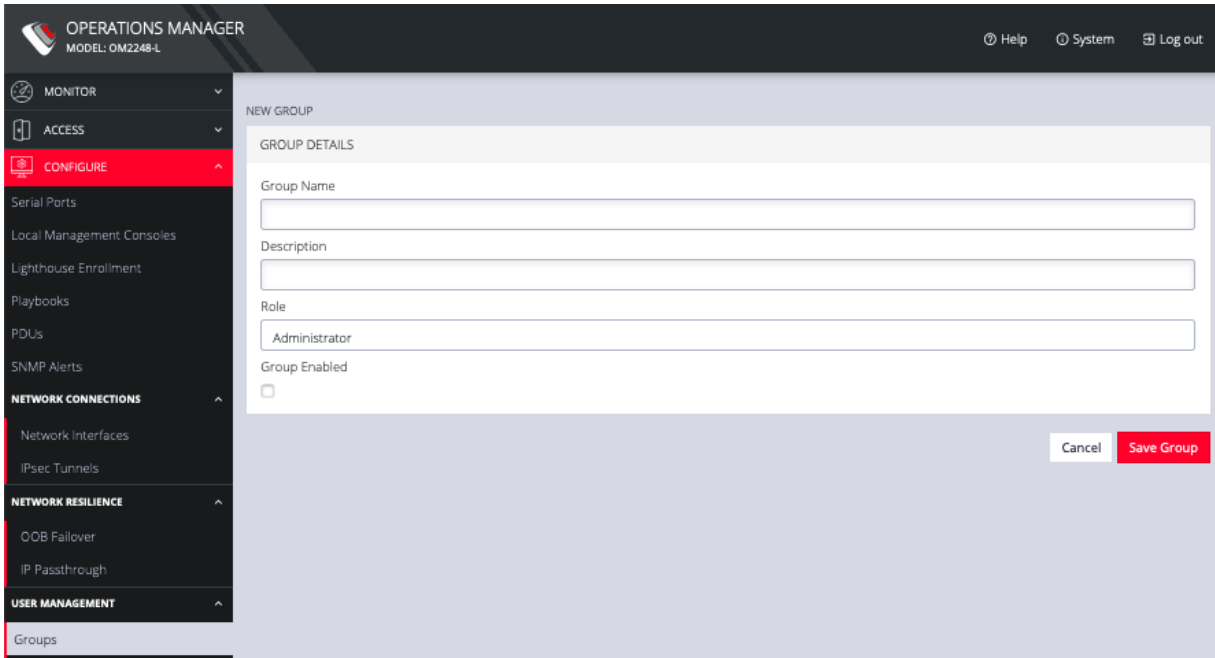
[CONFIGURE](#) > [USER MANAGEMENT](#) > [Groups](#)

To create a new group:

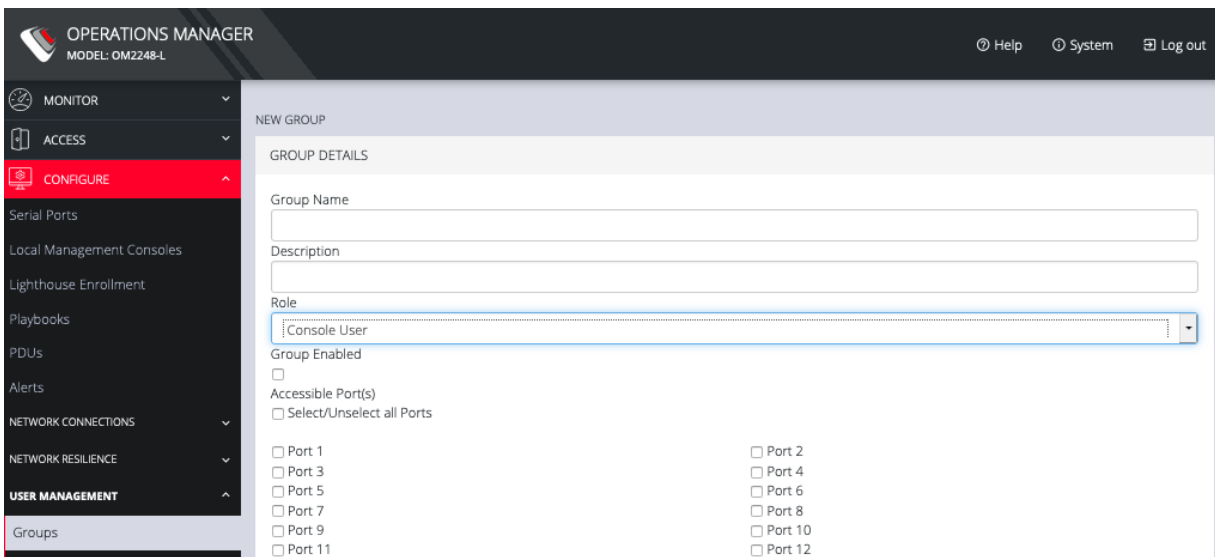
1. Select **CONFIGURE** > **USER MANAGEMENT** > **Groups**.



2. Click the **Plus** button. The **NEW GROUP** page opens.



3. Enter a **Group Name**, **Description**, and select a **Role** for the group.
4. Choosing the **Console User** role allows you to select specific ports this group will be able to access.



5. Click the **Group Enabled** checkbox to enable the group. After creation, groups can also be enabled or disabled from the **CONFIGURE > USER MANAGEMENT > Groups** page.
6. Click **Save Group**.

**Note:** **Group Name** is case sensitive. It can contain numbers and some alpha-numeric characters. When using remote authentication, characters from a user's remote groups that are not allowed are converted to underscores during authentication. Local groups can be created that take that into account, allowing the authentication to continue.

If the **Role** selected is **Administrator**, members of the group have full access to and control of all managed devices, full system configuration privileges, and full access to the command line shell.

To modify an existing group:

1. Select **CONFIGURE > USER MANAGEMENT > Groups**.
2. Click **Edit** in the **Actions** section of the group to be modified and make desired changes.
3. Click **Save Group**.

The **CONFIGURE > User Management > Groups** page also allows administrators to delete a group. Users who were members of the deleted group lose any access and administrative rights inherited from the group.

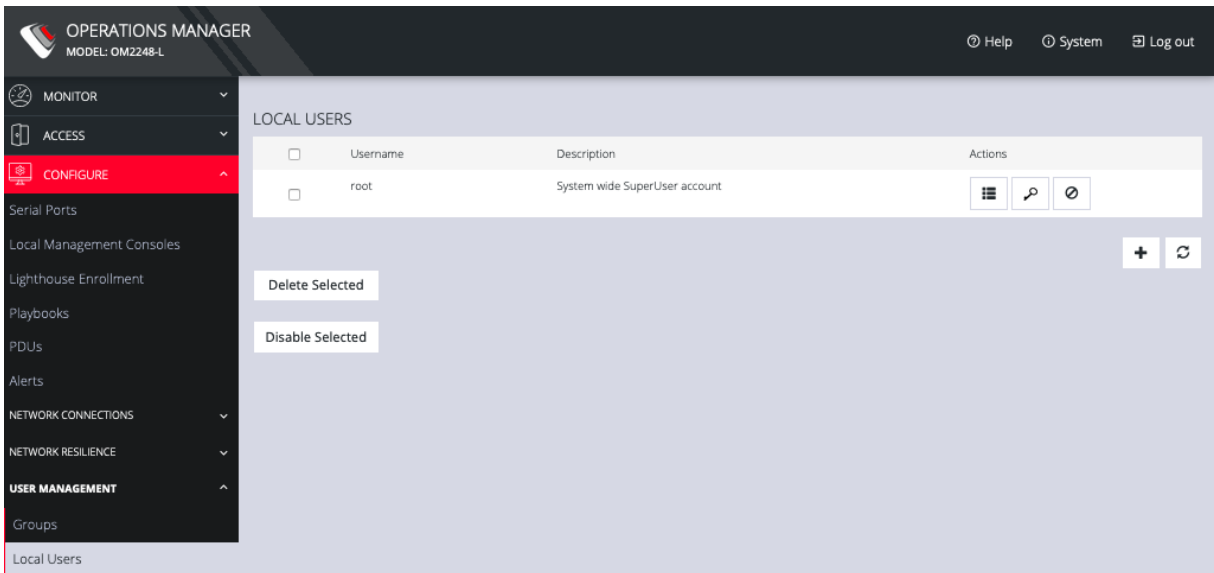
**Note:** The netgrp group is inherited as the primary group for all remote AAA users who are not defined locally. By default, netgrp has the Administrator role and is disabled. It must be enabled to take effect for remote AAA users.

## Local Users

[CONFIGURE](#) > [USER MANAGEMENT](#) > [Local Users](#)

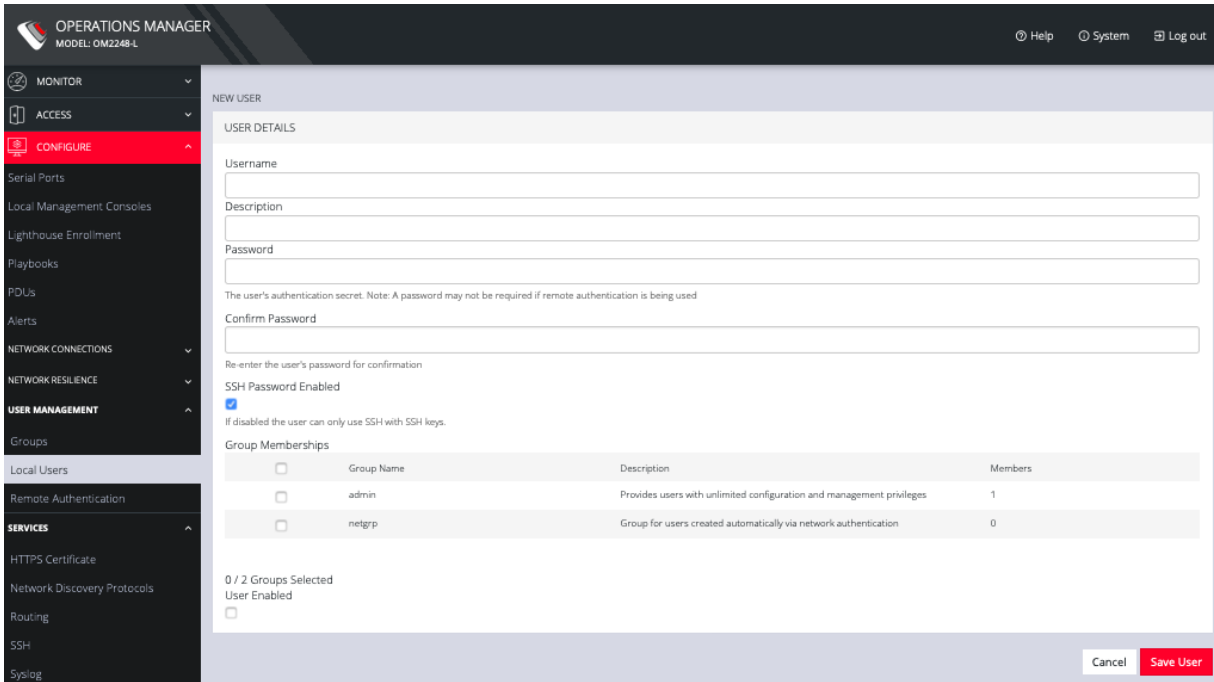
To create a new user:

1. Navigate to the **CONFIGURE > USER MANAGEMENT > Local Users** tab.



2. Click the **+** button. The **New User** dialog appears.





OPERATIONS MANAGER  
MODEL: OM2248-L

Help System Log out

MONITOR  
ACCESS  
**CONFIGURE**

Serial Ports  
Local Management: Consoles  
Lighthouse Enrollment  
Playbooks  
PDUs  
Alerts

NETWORK CONNECTIONS  
NETWORK RESILIENCE  
**USER MANAGEMENT**

Groups  
Local Users  
Remote Authentication

SERVICES  
HTTPS Certificate  
Network Discovery Protocols  
Routing  
SSH  
Syslog

NEW USER

USER DETAILS

Username  
Description  
Password  
Confirm Password

The user's authentication secret. Note: A password may not be required if remote authentication is being used

Re-enter the user's password for confirmation

SSH Password Enabled

If disabled the user can only use SSH with SSH keys.

Group Memberships

Group Name	Description	Members
admin	Provides users with unlimited configuration and management privileges	1
netgrp	Group for users created automatically via network authentication	0

0 / 2 Groups Selected  
User Enabled

Cancel Save User

3. Enter a **Username**, **Description**, and **Password**.
4. Re-enter the **Password** in the **Confirm Password** field.
5. Select the **Enabled** checkbox.
6. Click **Apply**.

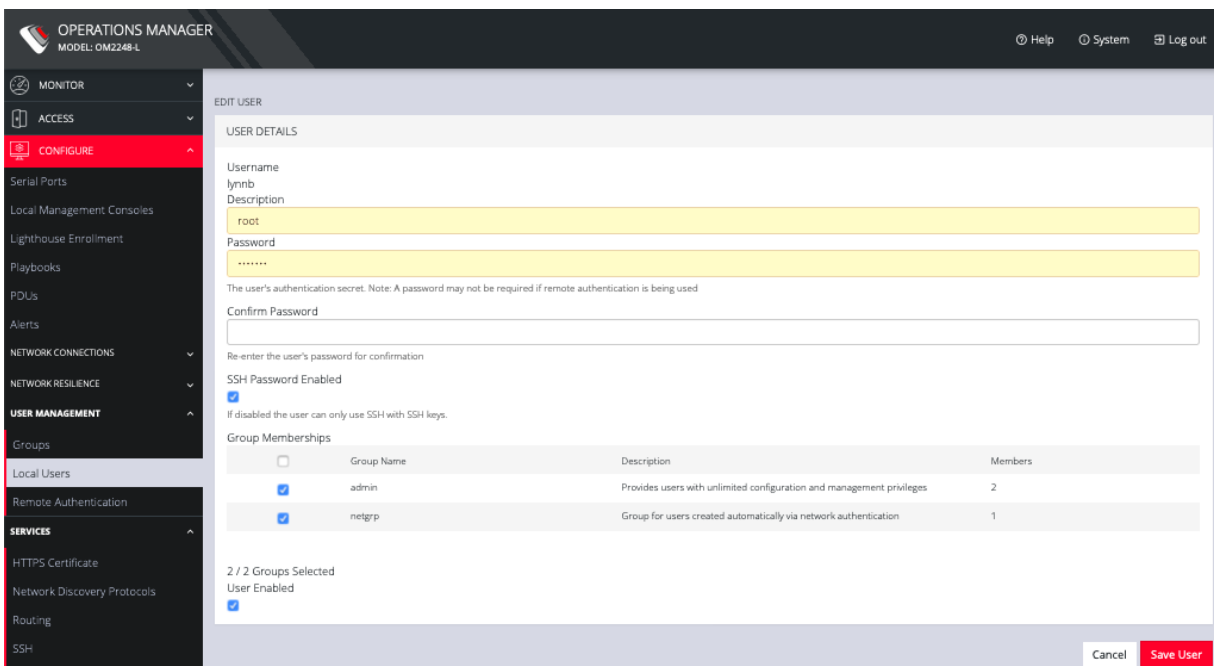
To create a new user without password which causes them to fall back to remote authentication:

1. Select **CONFIGURE > User Management > Remote Authentication**
2. Select a Scheme.
3. Enter Settings and click **Apply**.
4. Select **CONFIGURE > USER MANAGEMENT > Local Users**
5. Click the **+** button. The **New User** dialog loads.
6. Enter a **Username**, **Description**.
7. Select the **Remote PasswordOnly** checkbox.

8. Select the **Enabled** checkbox.
9. Click **Apply**.

To modify an existing user:

1. Select **CONFIGURE > USER MANAGEMENT > Local Users**
2. Click the **Edit User** button in the **Actions** section next to the user to be modified and make desired changes.
3. Click **Save User**.



OPERATIONS MANAGER  
MODEL: OM2248-L

Help System Log out

MONITOR

ACCESS

CONFIGURE

Serial Ports

Local Management Consoles

Lighthouse Enrollment

Playbooks

POUs

Alerts

NETWORK CONNECTIONS

NETWORK RESILIENCE

USER MANAGEMENT

Groups

Local Users

Remote Authentication

SERVICES

HTTPS Certificate

Network Discovery Protocols

Routing

SSH

EDIT USER

USER DETAILS

Username  
lynrb

Description  
root

Password  
.....

The user's authentication secret. Note: A password may not be required if remote authentication is being used

Confirm Password

Re-enter the user's password for confirmation

SSH Password Enabled

If disabled the user can only use SSH with SSH keys.

Group Memberships

<input type="checkbox"/>	Group Name	Description	Members
<input checked="" type="checkbox"/>	admin	Provides users with unlimited configuration and management privileges	2
<input checked="" type="checkbox"/>	netgrp	Group for users created automatically via network authentication	1

2 / 2 Groups Selected

User Enabled

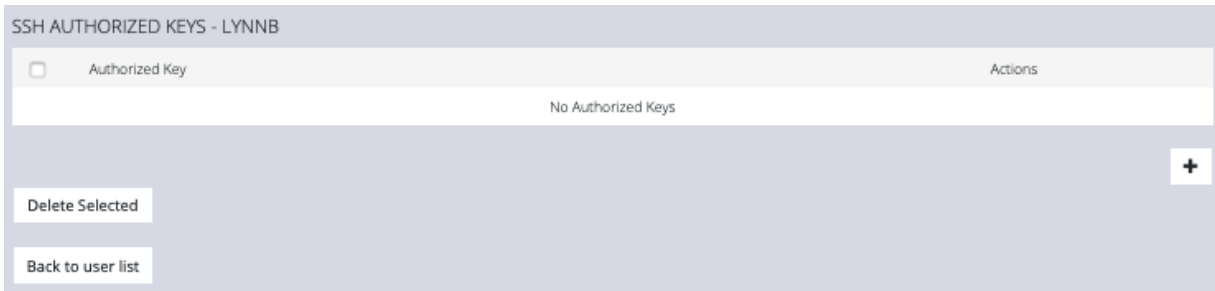
Cancel Save User

The **Edit Users** dialog allows the user's **Description** to be changed, **Group Memberships** modified, and the user's **Password** to be reset. The username cannot be changed. To disable a user, uncheck the **Enabled** checkbox.

Disabled users cannot log in to the OPERATIONS MANAGER using either the Web-based interface or via shell-based logins.

To manage SSH authorized keys for a user:

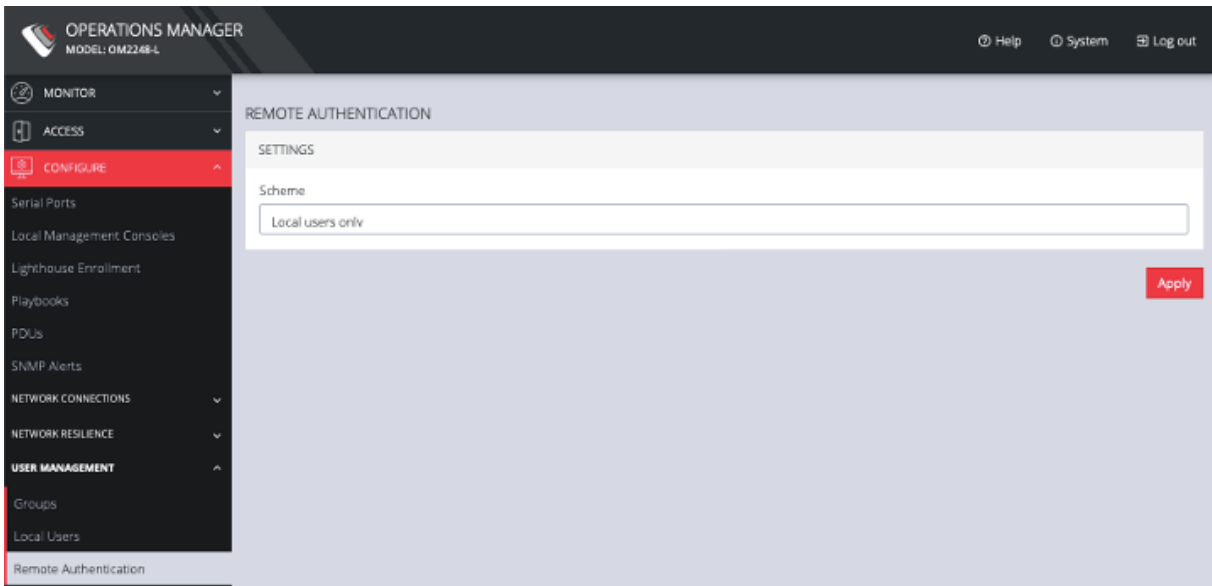
1. Select **CONFIGURE > USER MANAGEMENT > Local Users**
2. Click the **Manage SSH Authorized Keys** button in the **Actions** section next to the user.



3. Click the **Plus** button to add a new key. This opens the **NEW AUTHORIZED KEY** page for this user.



4. Enter the key and click **Apply**. You can also click on **Add Authorized Key** and disable password for SSH for this user from this page.
5. To delete a key, click **CONFIGURE > USER MANAGEMENT > Local Users** and click the **Authorized Key** button for the user.



6. Click the **Delete** button next to the key you wish to remove.

To delete a user:

1. Select **CONFIGURE > USER MANAGEMENT > Local Users**
2. Click the **Delete User** button in the **Actions** section next to the user to be deleted.
3. Click **Yes** in the **Confirmation** dialog.

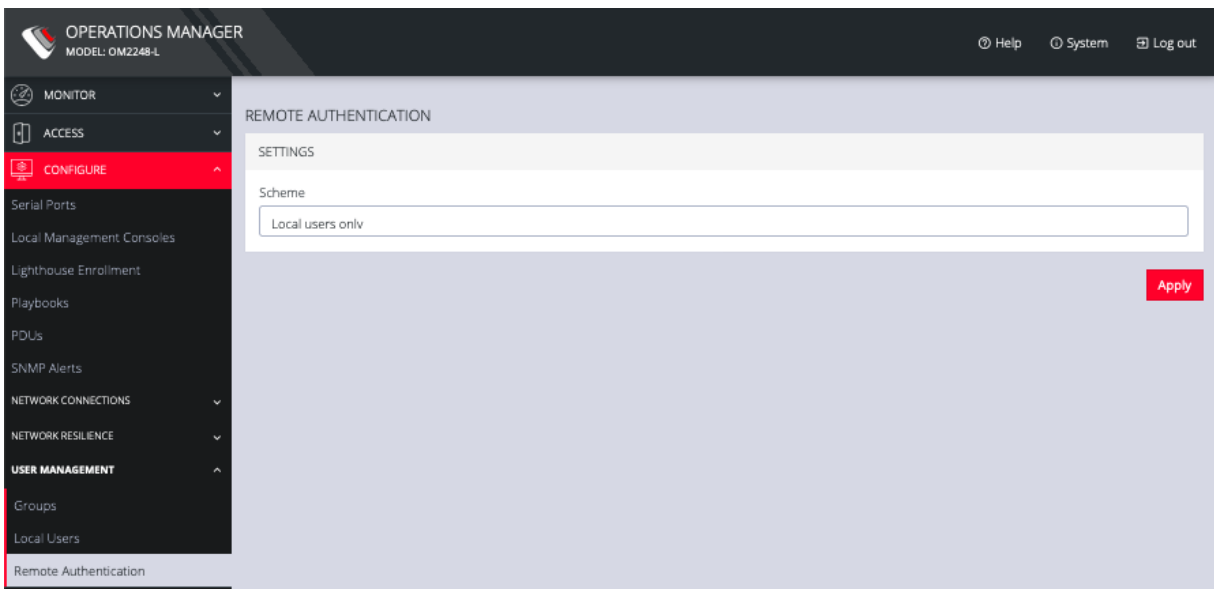
## Remote Authentication

[CONFIGURE](#) > [USER MANAGEMENT](#) > [Remote Authentication](#)

The OPERATIONS MANAGER supports three AAA systems:

- LDAP (Active Directory and OpenLDAP)
- RADIUS
- TACACS+

To begin, select **CONFIGURE > USER MANAGEMENT > Remote Authentication**.



To configure LDAP authentication (for example):

1. Under **CONFIGURE > User Management > Remote Authentication**, select **LDAP** from the **Mode** drop-down menu.

REMOTE AUTHENTICATION

SETTINGS

Scheme  
LDAP

Remote authentication servers

Address	Port (default is 389)
<input type="text"/>	<input type="text"/> - <input type="text"/>

LDAP base DN  
  
The distinguished name of the search base. For example: dc=my-company,dc=com

LDAP bind DN  
root  
The distinguished name to bind to the server with. The default is to bind anonymously.

Bind DN password  
.....  
Confirm password

LDAP username attribute  
  
The LDAP attribute that corresponds to the login name of the user (commonly "sAMAccountName" for Active Directory, and "uid" for OpenLDAP).

LDAP group membership attribute  
  
The LDAP attribute that indicates group membership in a user record (commonly "memberOf" for Active Directory, and unused for OpenLDAP).

Ignore referrals  
  
Disregard LDAP referrals to other servers

Apply

2. Add the **Address** and optionally the **Port** of the LDAP server to query.
3. Add the **Base DN** that corresponds to the LDAP system being queried.  

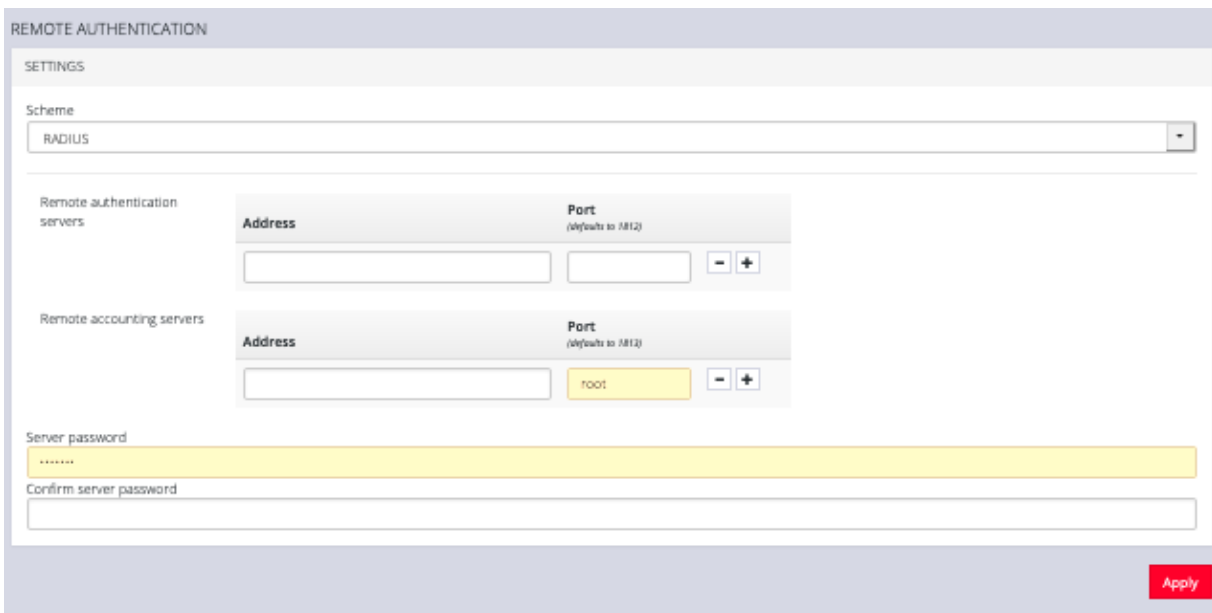
For example, if a user's distinguished name is cn=John Doe,dc=Users,dc=ACME,dc=com, the *Base DN* is dc=ACME,dc=com
4. Add the **Bind DN**. This is the distinguished name of a user with privileges on the LDAP system to perform the lookups required for retrieving the username of the users, and a list of the groups they are members of.
5. Add the password for the binding user.

6. Add the **Username Attribute**. This depends on the underlying LDAP system. Use sAMAccountName for Active Directory systems, and uid for OpenLDAP based systems.
7. Add the **Group Membership Attribute**. This is only needed for Active Directory and is generally memberOf.
8. If desired, check Ignore referrals option. When checked, LDAP will not follow referrals to other remote authentication servers when logging users in. If multiple remote authentication servers exist on the network, checking this option may improve log in times.

**Note:** Multiple servers can be added. The LDAP subsystem queries them in a round-robin fashion.

To configure RADIUS:

1. Under **CONFIGURE > User Management > Remote Authentication**, select **RADIUS** from the **Scheme** drop-down menu.



The screenshot shows the 'REMOTE AUTHENTICATION' configuration page. Under the 'SETTINGS' section, the 'Scheme' dropdown menu is set to 'RADIUS'. Below this, there are sections for 'Remote authentication servers' and 'Remote accounting servers'. Each section has an 'Address' field and a 'Port' field. The 'Remote accounting servers' port is set to 'root'. At the bottom, there are fields for 'Server password' and 'Confirm server password'. An 'Apply' button is located in the bottom right corner.

2. Add the **Address** and optionally the **Port** of the RADIUS authentication server to query.
3. Add the **Address** and optionally the **Port** of the RADIUS accounting server to send accounting information to.
4. Add and confirm the **Server password**, also known as the RADIUS Secret.

**Note:** Multiple servers can be added. The RADIUS subsystem queries them in a round-robin fashion.

To provide group membership, RADIUS needs to be configured to provide a list of group names via the Framed-Filter-Id attribute. The following configuration snippet shows how this can be configured for FreeRADIUS:

```
operator1 Auth-Type := System
```

```
Framed-Filter-ID = ":group_name=west_coast_admin,east_coast_user:"
```

**Note:** The Framed-Filter-ID attribute must be delimited by the colon character.

To configure TACACS+:

1. Under **CONFIGURE > USER MANAGEMENT > Remote Authentication**, select TACACS+ from the *Scheme* drop-down menu.



REMOTE AUTHENTICATION

SETTINGS

Scheme  
TACACS+

Remote authentication servers

Address	Port (default is 49)
<input type="text"/>	49 <input type="button" value="-"/> <input type="button" value="+"/>

TACACS+ login method  
PAP

The method used to authenticate to the server. Defaults to PAP. To use DES encrypted passwords, select Login

Server password  
.....

Confirm server password

TACACS+ service

The service to authenticate with. This determines which set of attributes are returned by the server. Defaults to "raccess"

2. Add the **Address** and optionally the **Port** of the TACACS+ authentication server to query.
3. Select the **Login Method**. **PAP** is the default method. However, if the server uses DES-encrypted passwords, select **Login**.
4. Add and confirm the **Server password**, also known as the TACACS+ Secret.
5. Add the **Service**. This determines the set of attributes sent back by the TACACS+ server

**Note:** Multiple servers can be added. The TACACS+ subsystem queries them in a round-robin fashion.

```
user = operator1 {  
    service = raccess {  
        groupname = west_coast_admin,east_cost_user  
    }  
}
```



To do this with Cisco ACS, see [Setting up permissions with Cisco ACS 5 and TACACS+](#) on the Opengear Help Desk.

## RemoteLocal for AAA Server


[CONFIGURE > USER MANAGEMENT > Remote Authentication](#)

[CONFIGURE > USER MANAGEMENT > Local Users](#)

RemoteLocal authentication allows users to be authenticated locally if they don't exist on the AAA server so that users can still access any consoles that are required to be accessed.

A RemoteLocal alert banner ensures all users are made aware that if the RemoteLocal policy is selected their local users will not be accessible.

If a RemoteDownLocal policy is selected and the AAA server is contactable, then local authentication won't be used.

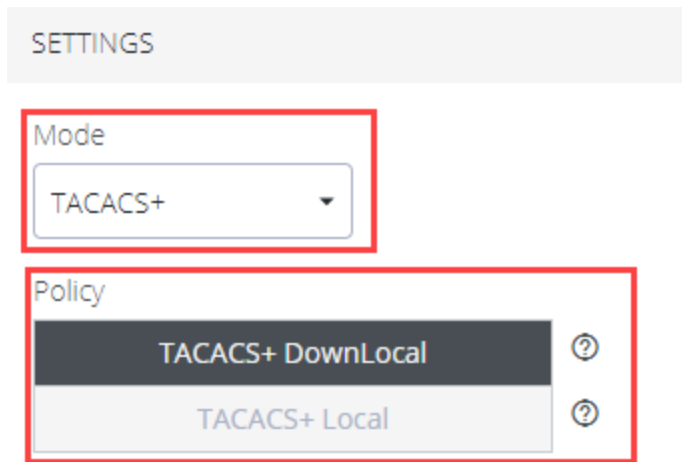
 You are using a remote authentication server with a RemoteDownLocal policy. Ensure that users also exist on that server in order to sign in.

**Note:** This feature is backwards compatible with previous versions of software (the rest api version is unchanged).

## Change Authentication Policy

Changing the Authentication policy is simple.

1. Navigate to **CONFIGURE > USER MANAGEMENT > Remote Authentication**.
2. Ensure the required protocol mode is selected (TACACS+, RADIUS, LDAP).



SETTINGS

Mode

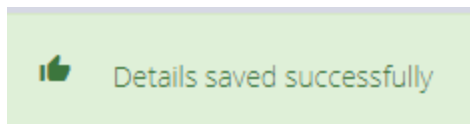
TACACS+

Policy

TACACS+ DownLocal

TACACS+ Local

3. Select the authentication policy you require (DownLocal or Local).
4. Click **Apply**. The policy change is confirmed by a green confirmation banner.



## Authentication Scenarios

The following example shows RADIUS protocol mode, but the behavior is the same for other protocols such as TACACS+ or LDAP.

- User does not exist:
  - When using RemoteLocal authentication for all types of remote servers, if remote authentication fails because the user does not exist on the remote AAA server, the OM device will attempt to authenticate the user using a local account as per a regular local log in.

- Remote Server Down / Unreachable:
  - If the remote AAA server is unreachable or down, the OM device tries to authenticate the user using a local account as per a regular local log in.
- Remote server is up, but incorrect credentials:
  - The user is denied access. Warnings indicate that RemoteLocal is enabled.

## Local Password Policy

[CONFIGURE > USER MANAGEMENT > Local Password Policy](#)

A Password Complexity policy allows network administrators to implement and enforce a password policy that meets the customers' security standards for local users (including root). This functionality enables administrators to mandate the setting of complex passwords thus making it difficult for malicious agents to succeed in password attacks.

Enabling this feature will:

- Enforce the use of complex passwords so as to improve security.
- Schedule expiry of passwords to enforce regular password updates.

**Note:** Password policy such as complexity and expiry can only be configured by an administrator. Password requirements are applied to all accounts.

**Tip:** Password policy may be enabled and configured via the web-ui, rest-api and ogcli. The password policy also applies to underlying CLI tools.

## Set Password Complexity Requirements

[CONFIGURE > USER MANAGEMENT > Local Password Policy](#)

**Note:** Some password complexity rules are required, other rules are optional. Optional rules can be selected by clicking on the relevant check box.

See also "[Password Policy Implementation Rules](#)" on page 113

To set the password complexity requirements:

1. Navigate to [CONFIGURE > USER MANAGEMENT > Local Password Policy](#).
2. Click the **Enforced** button to implement the password complexity policy (the policy is not activated until the **Apply** button is clicked).
3. Enter the information required to form the password complexity rules to comply with your company policy:
  - Password cannot be a palindrome (required)
  - Minimum length (required)
  - Must contain an upper case letter (optional)
  - Must contain a numeric character (optional)
  - Must contain a special character (non-alphanumeric eg. e.g. #,\$,%)
  - Disallow user names in passwords (optional)

See "[Password Policy Implementation Rules](#)" on page 113

4. Click the **Apply** button to activate the password complexity policy.

## Set Password Expiration Interval

[CONFIGURE > USER MANAGEMENT > Local Password Policy](#)

See also "[Password Policy Implementation Rules](#)" on the next page

Password Expiration schedules the expiry of passwords to enforce regular password updates. When this feature is applied and a password becomes expired, an expired password prompt is displayed at log-in.

**Note:** The Password Expiration policy affects local passwords only and does not apply to remote authentication modes.

To set the password expiration interval:

1. Navigate to [CONFIGURE > USER MANAGEMENT > Local Password Policy](#).
2. Click the **Enabled** button to implement the password expiration policy (the policy is not activated until the **Apply** button is clicked).
3. Input a number to represent the desired number of days between mandatory password updates. The default time is 90 days and the minimum is 1 day.
4. Click the **Apply** button to activate the password interval policy.



## Password Policy Implementation Rules

Rule	Policy
Expiry Rules	The expiry time is measured in number of whole days. When the expiry period is reached users are required to update their password on their next login. The default expiry period is 90 days and the minimum is one (1) day.
	If there are existing user passwords when the expiry is enabled, the expiry time will be applied from when the password was initially set by the user. If a password falls outside the new expiry period the user will be immediately prompted to change the password.
	Local Password policy is only applied to local passwords and does not apply to remote authentication modes.
	When local password policy is enabled it will remain in force until the feature is turned off.
	If the minimum password length is modified and then the password complexity feature is disabled, the minimum length requirement is not updated.
Complexity Rules	The password cannot be a palindrome (this requirement cannot be disabled except by disabling password complexity entirely).  (A palindrome is a word or other sequence of characters that reads the same backward as forward, such as <i>madam</i> or <i>racecar</i> ).
	The minimum length (enforced) must be at least 8 characters (this requirement cannot be disabled except by disabling password complexity entirely).
	The password should contain at least one upper case alphabetic character (enabled or disabled separately).

	<p>The password must contain at least one numeric character (enabled/disabled separately).</p>
	<p>The password should contain at least one special character (e.g. #,\$,%) (enabled/disabled separately).</p>
	<p>The password cannot contain your user-name.</p>
	<p>Complexity requirements will apply when a user next tries to update their password.</p>
	<p>An administrator can force the expiry of a users password by running the ogCLI command: <code>passwd --expire {username}</code> to force a user to change their password.</p>
	<p>The operations <code>ogadduser</code>, <code>ogpasswd</code> and <code>ogsshaddsshkey</code> have been removed. You should instead use ogCLI for these operations.</p>



## Services

[CONFIGURE > SERVICES](#)

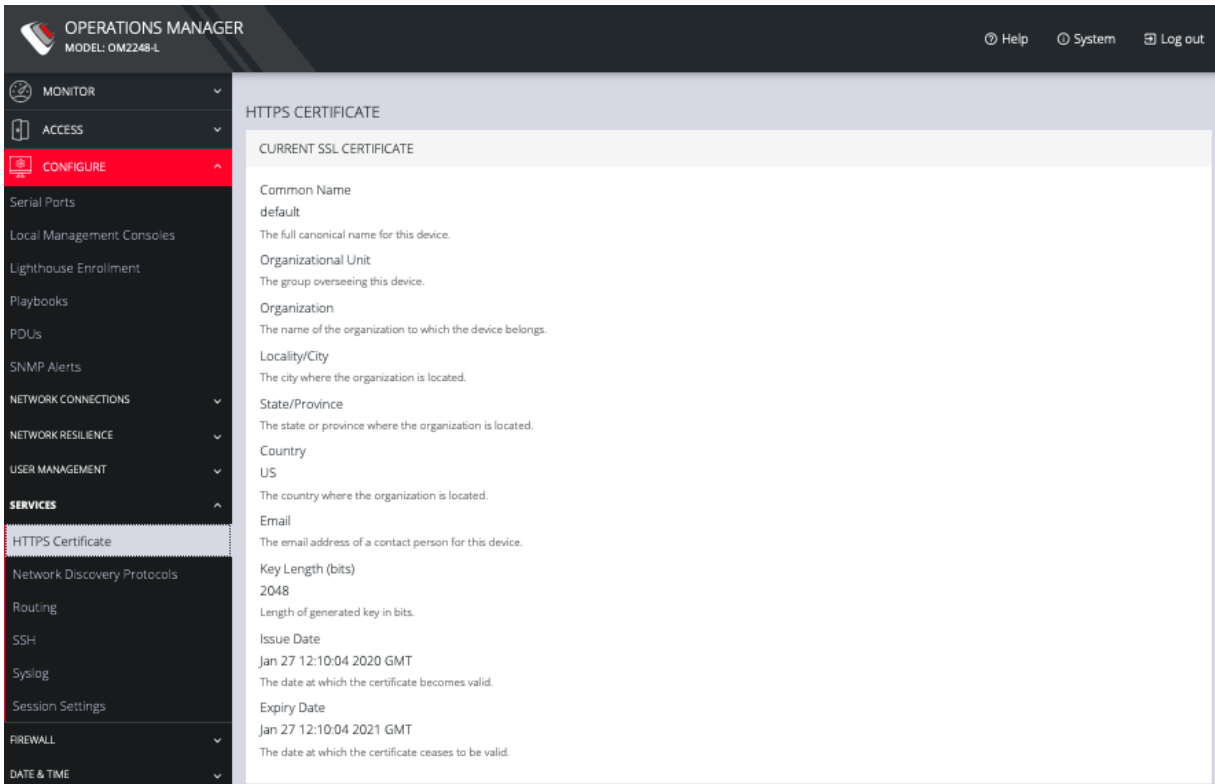
The **CONFIGURE > SERVICES** menu lets you manage services that work with the OPERATIONS MANAGER.

# HTTPS Certificate

[CONFIGURE](#) > [SERVICES](#) > [HTTPS Certificate](#)

The OPERATIONS MANAGER ships with a private SSL Certificate that encrypts communications between it and the browser.

To examine this certificate or generate a new Certificate Signing Request, select **CONFIGURE > SERVICES > HTTPS Certificate**. The details of the **Current SSL Certificate** appear.



Below this listing is a **Certificate Signing Request** form, which can be used to generate a new SSL certificate.

CERTIFICATE SIGNING REQUEST

Common Name

The full canonical name for this device

Organizational Unit

The group overseeing this device

Organization

The name of the organization to which the device belongs

Locality/City

The city where the organization is located

State/Province

The state or province where the organization is located

Country

The country where the organization is located

Email

The email address of a contact person for this device

Key Length (bits)

Length of generated key in bits

Challenge Password

An optional (dependent on CA) password

Confirm Password

Confirmation of the challenge password

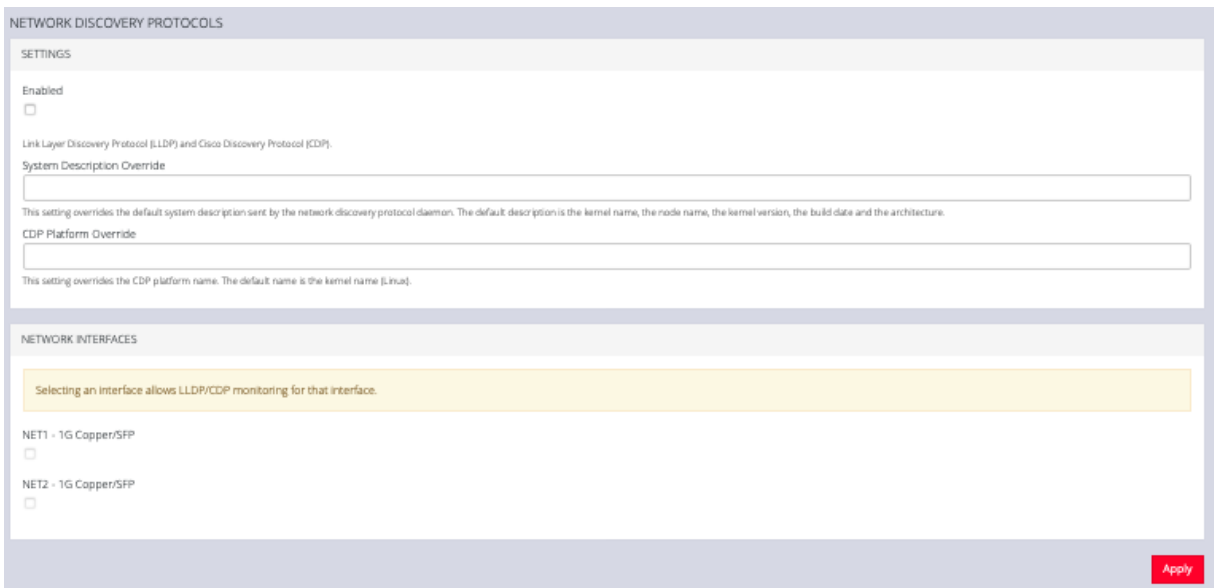
Private Key File

A private key to use when generating the CSR (optional)

## Network Discovery Protocols

[CONFIGURE](#) > [SERVICES](#) > [Network Discovery Protocols](#)

The OPERATIONS MANAGER displays LLDP/CDP Neighbors when enabled for a connection. See **CONFIGURE > SERVICES > Network Discovery Protocols** to enable/disable.



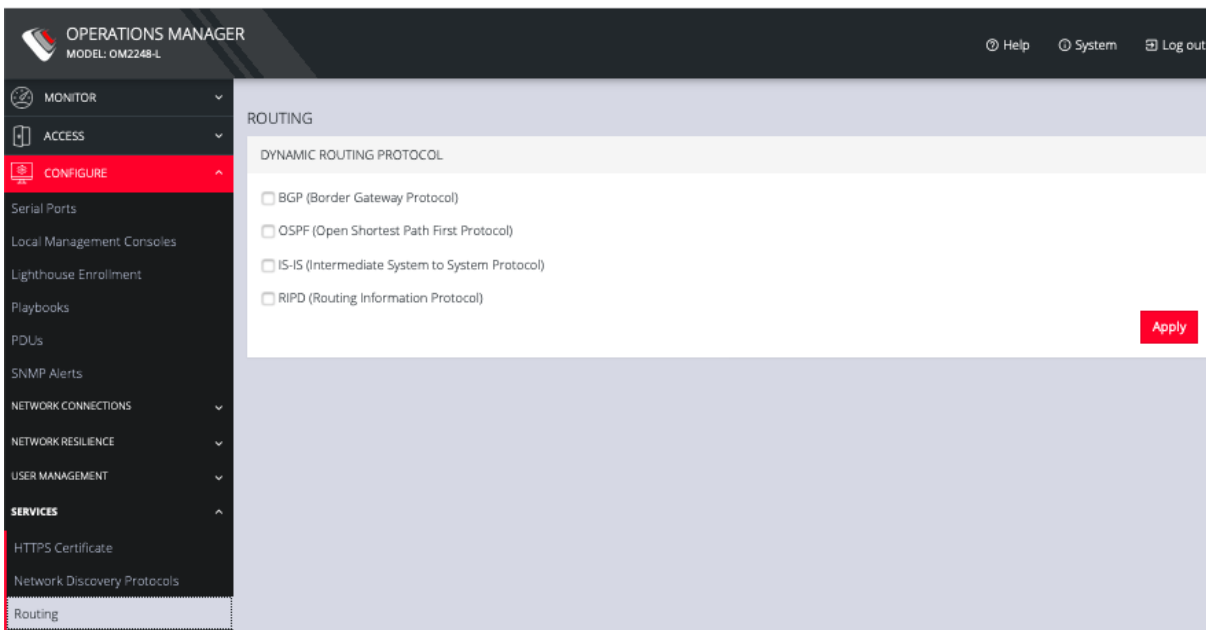
The screenshot shows the configuration page for Network Discovery Protocols. It is divided into two main sections: SETTINGS and NETWORK INTERFACES. In the SETTINGS section, there is an 'Enabled' checkbox which is currently unchecked. Below it, there are two text input fields: 'System Description Override' and 'CDP Platform Override'. The 'System Description Override' field has a small text box below it explaining that the default description is the kernel name, node name, kernel version, build date, and architecture. The 'CDP Platform Override' field has a small text box below it explaining that the default name is the kernel name (Linux). The NETWORK INTERFACES section contains a yellow warning box stating 'Selecting an interface allows LLDP/CDP monitoring for that interface.' Below this, there are two interface entries: 'NET1 - 1G Copper/SFP' and 'NET2 - 1G Copper/SFP', each with an unchecked checkbox. At the bottom right of the page, there is a red 'Apply' button.

The **CONFIGURE > SERVICES > Network Discovery Protocols > LLDP/CDP NEIGHBORS** page allows you to enable this service by clicking the Enable checkbox. You can set a System Description that overrides the default system description sent by the network discovery protocol daemon. The default description is the kernel name, the node name, the kernel version, the build date and the architecture. You can also enter a value in the CDP Platform Override to override the CDP platform name. The default name is the kernel name (Linux). Select one or more checkboxes in the **NETWORK INTERFACES** section of the page and click Apply.

## Routing

[CONFIGURE](#) > [SERVICES](#) > [Routing](#)

You can enable routing protocols on this page. Select **CONFIGURE** > **SERVICES** > **Routing** page.



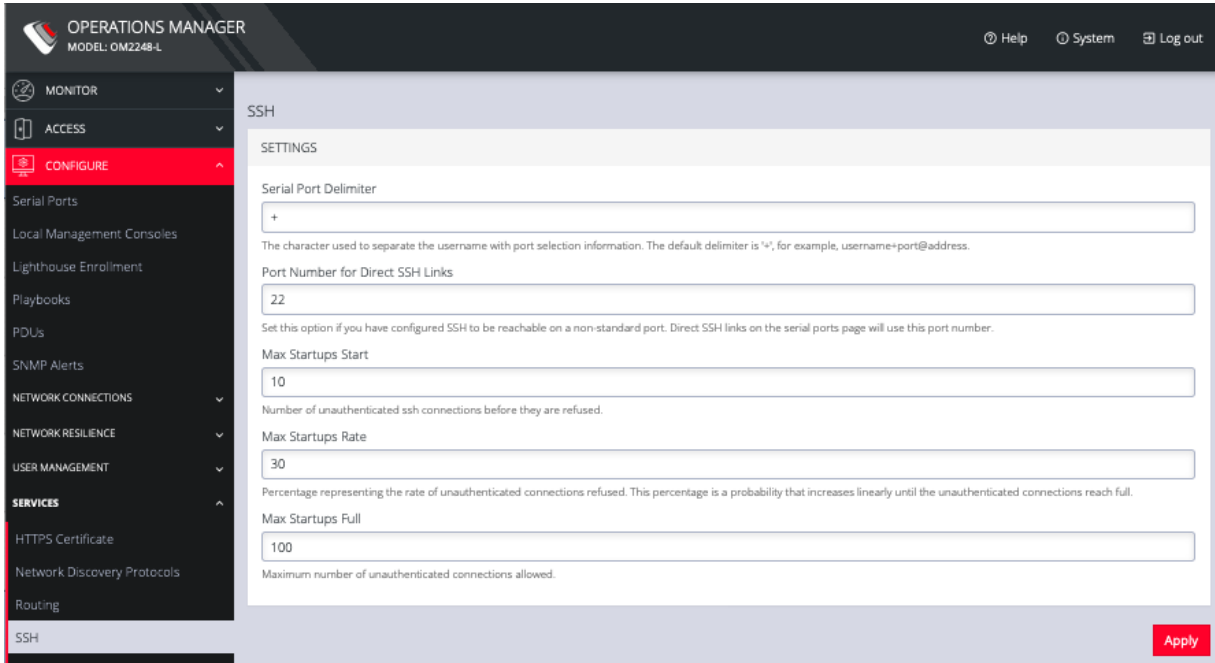
Select any of the following and click the Apply button:

- **BGP** (Border Gateway Protocol)
- **OSPF** (Open Shortest Path First Protocol)
- **IS-IS** (Intermediate System to System Protocol)
- **RIPD** (Routing Information Protocol)

# SSH

[CONFIGURE](#) > [SERVICES](#) > [SSH](#)

To modify the port used for connecting to serial consoles via SSH, click **CONFIGURE > SERVICES > SSH**.



This page also lets you set the delimiting character used to separate the username with port selection information. The default delimiter is a plus sign (+). For example, `username+port@address`.

You can change more values on this page.

- **Max Startups Start**, the number of unauthenticated connections before they are refused.
- **Max Startups Rate** is a percentage that represents the rate of unauthenticated connections refused. This percentage is a probability that



increases linearly until the unauthenticated connections reach full.

- **Max Startups Full** is the number of unauthenticated connections allowed.

## Unauthenticated SSH to Console Ports

[Configure](#) > [Services](#) > [SSH](#)

The Unauthenticated SSH Access feature provides the option to access console ports (using TCP high ports) by establishing per-port SSH connection between a console and serial ports at a remote device. This allows a single step log-in and avoids the necessity for two log-ins to reach a remote end device within secure, closed networks.

Usually, you would need to authenticate on the Opengear appliance, followed by any log in to a device you are connecting to via the serial port.

When unauthenticated access is enabled SSH is available to all serial ports on the device without requiring a password.

**Note:** Unauthenticated access can be used with or without IP aliases for serial ports.

**Caution:** For security, **Unauthenticated SSH** should only be used when operating within a trusted, closed network, for example within a lab. There is a security risk in allowing any kind of unauthenticated access to serial ports and any terminals connected to them.

### Enable Unauthenticated SSH

Authenticated or Unauthenticated access is determined via a global configuration option. Unauthenticated access to individual ports is achieved by command such as `ssh -p 300X user@<IP>`.

## Enable SSH

**Note:** This feature may be enabled using the default settings without the need for configuration.

1. Open the SSH form, **Configure > Services > SSH > SSH (form)**.
2. Complete the SSH form (if this is the first time Unauthenticated SSH has been used), a description of the input data is provided at [Properties and Settings](#) in this topic.
3. When required, enable the Unauthenticated SSH feature by clicking the **Enabled** button.

**Note:** Unauthenticated access to all serial ports will be available through SSH on TCP port 3000+ or Serial Port IP aliases.

## Enable/Disable

Enabling or disabling this feature is done in the user interface.

To **enable** the feature click on the **Enabled** button then click the **Apply** button. The feature is enabled immediately and a pop-up will confirm that the feature is enabled.

**Note:** Clicking the **Apply** button saves any changes you have made to the SSH form. A Details Saved banner confirms that the changes have been saved.

To **disable** the feature click on the **Disabled** button then click the **Apply** button. There is no confirmation pop-up when the feature is disabled.

## Connecting Directly to Serial Ports

For ports that have been configured with the SSH access service, you can connect directly to a port and start a session, bypassing the chooser, by using one of the four conventions described in the following:

Convention	Example
Use a network client to connect to the service network Base Port + serial port number.	<pre># SSH to serial port 1 by TCP port ssh -p 3001 -l operator 70.33.235.190</pre> <p>In this example, the SSH base port is TCP port 3000, so SSH to TCP port 3001 directly connects you to serial port 1</p>
SSH to the Opengear device, log in adding :portXX to your username (e.g. root:port01 or operator:port01)	<pre># SSH to serial port labelled Router ssh -l operator:Router 70.33.235.190</pre>
SSH to the Opengear device, log in adding the :port-label to your username (e.g. root:Router or operator:Router)	<pre># SSH to serial port 1 by port name ssh -l operator:port01 70.33.235.190</pre>
Configure per-port IP aliases	

**Note:** For additional reading on connecting to serial ports see:

<https://opengear.zendesk.com/hc/en-us/articles/216373543-Communicating-with-serial-port-connected-devices>

**Note:** Serial ports in the Local Console and Disabled ports modes are not available for SSH connection.

## Feature Persist

If the device has an active console session after closing pmsHELL, connecting to the device again will resume the session and you are not prompted for the device password.

## Properties and Settings

Property	Definition/Range
Serial Port Delimiter	<p>A character that separates the User name and port selection information. The default value is the + character.</p> <p><i>Default is '+', maximum length is 1.</i></p> <p><i>The prohibited characters are '\', ' ", ' ` ', ' ' ', ' = ' and '#'.</i></p> <p><b>Source: schema</b></p> <p>required ssh_delimiter: string (default = "+"; minimum = 1; maximum = 1; validator = ("ssh_url_</p>

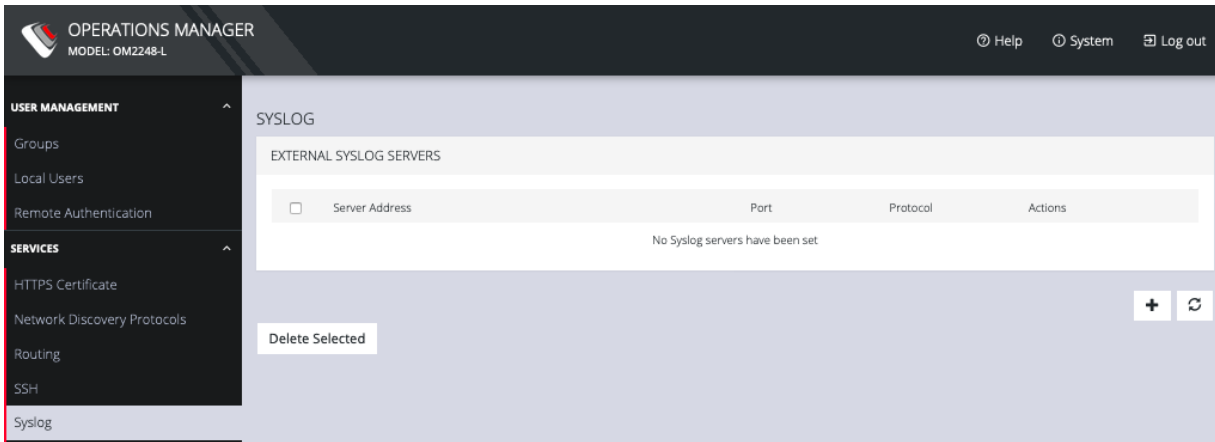
	<pre> delimiter")), <b>Source: validator</b> if (strlen(v) != 1) valid = 0; else if (v[0] == '\\') valid = 0; else if (v[0] == '"') valid = 0; else if (v[0] == '`') valid = 0; else if (v[0] == ' ') valid = 0; // breaks sshd_config else if (v[0] == '=') valid = 0; // breaks sshd_config else if (v[0] == '#') valid = 0; // breaks sshd_config else if (!isprint(v[0])) valid = 0; else { valid = 1; } </pre>
<p>Port Number for Direct SSH Links</p>	<p>This port number will be used for direct SSH links on the serial ports page. Set this option if you have configured SSH to be reachable on a non-standard port.</p>
<p>Max Startups Start</p>	<p>The number of connections pending authentication before new connections <i>begin</i> to be refused.</p> <p><i>Required start: int (minimum = 1; default = 10)</i></p>

<p>Max Startups Full</p>	<p>The number of connections pending authentication before <i>all</i> new connections are refused.</p> <p><i>Required full: int (minimum = 1; default = 100)</i></p>
<p>Max Startups Rate</p>	<p>This is the percentage rate at which new connections are refused once the Max Startups value is reached. The rate is increased to 100% at Max Startup Full.</p> <p><i>Required rate: int (minimum = 1; maximum = 100; default = 30),</i></p> <p><i>The rate at which connections are refused randomly begins at max startup rate and increases linearly until the number of connections pending authentication reach max startups full, in which case 100% of new connections are refused.</i></p>
<p>Unauthenticated Access to Serial Ports</p>	<p>This is the feature Enable/Disable button.</p>

# Syslog

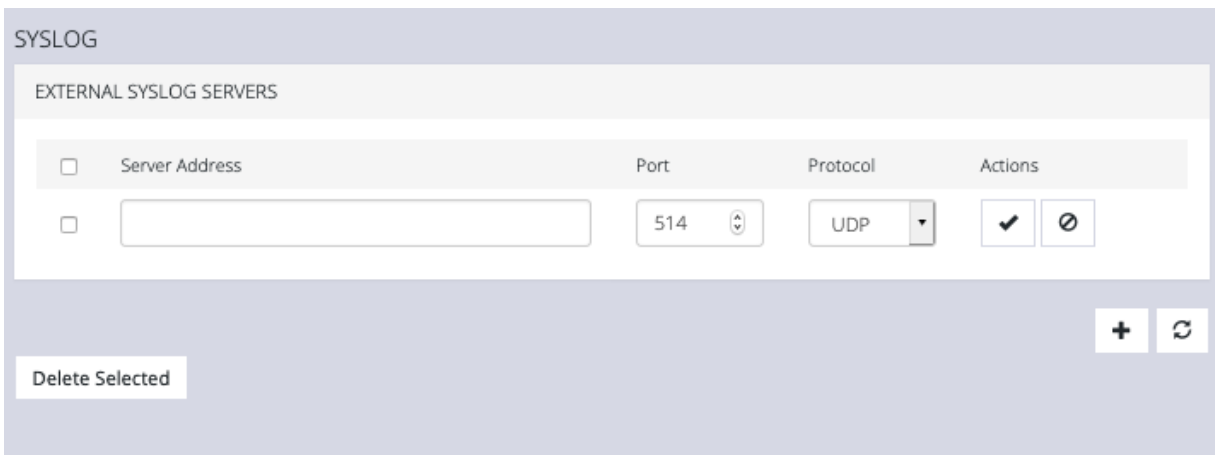
[CONFIGURE](#) > [SERVICES](#) > Syslog

Administrative users can specify multiple external servers to export the syslog to via TCP or UDP.



This page lists any previously added external syslog servers. To add a new one,

1. Navigate to **CONFIGURE > SERVICES > Syslog**.
2. Click the **Plus** button. The **External Syslog Servers** form appears.







2. Enter the **Server Address**.
3. Enter the Protocol, either **UDP** or **TCP**.
4. Enter the correct **Port**. If no port is entered, UDP defaults to port 514 and TCP defaults to 601.
5. Click **Apply**.

To edit an existing syslog server, click the **Edit** button under **Actions**. Delete a server by clicking the Delete button or the checkbox next to multiple servers and the Delete Selected button.

## Remote Syslog

[Configure > Services > Syslog](#)

[Configure > Services > Syslog > Create Syslog Server](#)

[Configure > Services > Syslog > Edit Syslog Server](#)

[Configure > Services > Syslog > Global Serial Port Settings](#)

[Configure > Serial Ports > Edit Serial Port](#)

The Remote Syslog facility provides the flexibility to specify a Remote Syslog server so that you can redirect console serial port logs to the Remote Syslog server so as to provide a central (and regional) repository where you can view the port-related activity. When remote logs are being received, local logs continue to be recorded.

Devices in a network can produce thousands of log entries; due to the number of logs occurring each hour, users demand the ability to configure the facility and severity for console port logs. The Remote Syslog collector can be configured so as to categorize and prioritize the logs appropriately thus allowing you to easily identify issues as they arise.

The Remote Syslog server provides the flexibility to:

- Analyze logs centrally.
- Monitor for suspicious activities.
- Collect and view analytics (for example, Splunk).

## Requirements

IP address of syslog server

Syslog server port number

## Set Logging Levels For Remote Syslog Server

Local Log Level limits the Syslog information being logged. Any log entry with a value equal or greater than the level specified in the config is sent to the remote server.

## Ensure Port Logging is Set to the Required Level

1. Navigate to the **Serial Ports** page and enable port logs through the serial port (**Configure > Serial Ports**)
2. For the serial port number you have selected, click the **Edit Serial Ports** button in the **Actions** column.
3. Navigate to **Logging Settings** and select the required logging level.
4. Click the **Apply** button. The change will be applied within a few seconds.

## Set Global Serial Port Settings

Navigate to: **Configure > Services > Syslog > Global Serial Port Settings**

1. In the **Global Serial Ports** tab
  - i. Select the required Facility.
  - ii. Select the required Severity.

**Note:** See the tables below for definitions of **Facility** and **Severity** .

2. Click the **Update** button and wait for the update confirmation banner:

The Syslog will log only those entries of the nominated event type.

## Edit or Delete an Existing Syslog Server

**Configure > Services > Syslog > Edit Syslog Server**

1. In the Configure > Services > Syslog tab click on the **IP address** of the target server. The **Edit Syslog Server** tab is opened for editing.
2. You can delete a server by clicking the **Delete** button at the top right of the Edit tab page.

## Syslog Terminology

Syslog logging terminology used in setting Facility and Severity of the Syslog.

## Create Syslog Server Tab - Field Definitions

Page location: Configure > Services > Syslog > Create Syslog Server

Field	Definition
Description	Unique, familiar text description or name given to this syslog server that users will recognize.
Server Address	The IP address of the remote syslog server you are using for logging.
Protocol	Click to select the required protocol for data transmission to the syslog server.
Port	The Remote Syslog Server IP address.
Minimum Log Severity Level	Log entries with a value equal or greater than the level specified are sent to the remote server.
Send Serial Port Logs	Click to enable serial port logging.
Create Button	Click to initiate the remote syslog, wait for confirmation banner.

## Syslog Facility Definitions

Facility	Definition
Kern	Kernel messages
User	User-level messages
Mail	Mail system
Daemon	System daemons
Auth	Security/authentication messages
Syslog	Messages generated internally by syslogd
lpr	Line printer subsystem
News	Network news subsystem
uucp	UUCP subsystem
Cron	Clock daemon
Authpriv	Security/authentication messages
ftp	FTP daemon
Local	Locally used facilities

## Syslog Severity Definitions

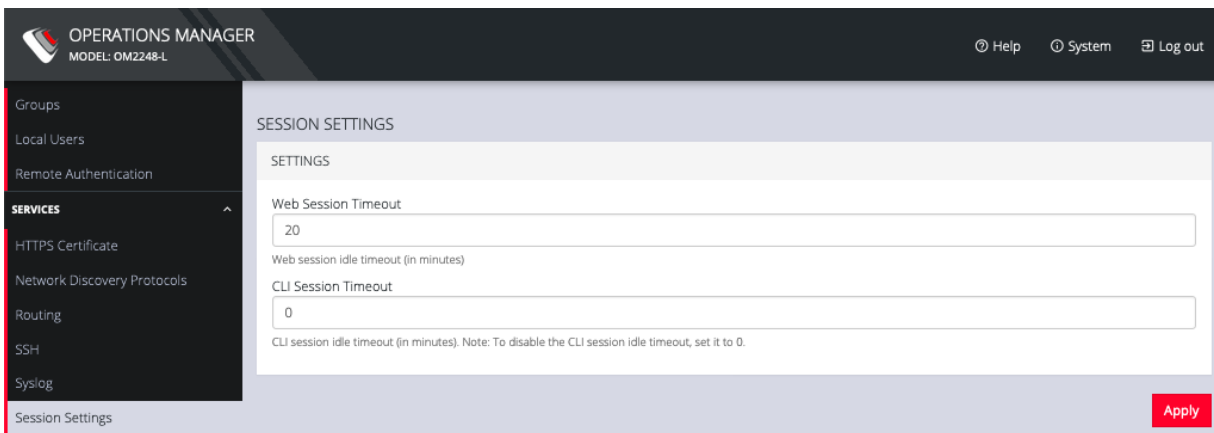
Severity	Definition
0- Emergency	System is unusable.
1 - Alert	Action must be taken immediately.
2 - Critical	Critical conditions.
3 - Error	Error conditions.
4 - Warning	Warning conditions.
5 - Notice	Normal but significant conditions.
6 - Info	Informational messages
7- Debug	Debug-level messages

## Session Settings

[SETTINGS](#) > [SERVICES](#) > [Session Settings](#)

To modify Web and CLI session settings navigate to the **SETTINGS > Services > Session Settings** page.

- **Web Session Timeout:** This value can be set from 1 to 1440 minutes.
- **CLI Session Timeout:** This value can be set from 1 to 1440 minutes or set it to 0 to disable the timeout. Changes take effect the next time a user logs in via the CLI.



The screenshot shows the 'SESSION SETTINGS' page in the OpenGear Operations Manager. The page has a dark header with the 'OPERATIONS MANAGER' logo and 'MODEL: OM2248-L' on the left, and 'Help', 'System', and 'Log out' links on the right. A left sidebar menu lists 'Groups', 'Local Users', 'Remote Authentication', and 'SERVICES' (expanded to show 'HTTPS Certificate', 'Network Discovery Protocols', 'Routing', 'SSH', 'Syslog', and 'Session Settings'). The main content area is titled 'SESSION SETTINGS' and contains a 'SETTINGS' section with two input fields: 'Web Session Timeout' (set to 20) and 'CLI Session Timeout' (set to 0). Below the CLI field is a note: 'CLI session idle timeout (in minutes). Note: To disable the CLI session idle timeout, set it to 0.' An 'Apply' button is located at the bottom right of the settings area.

## Firewall

### [CONFIGURE > FIREWALL](#)

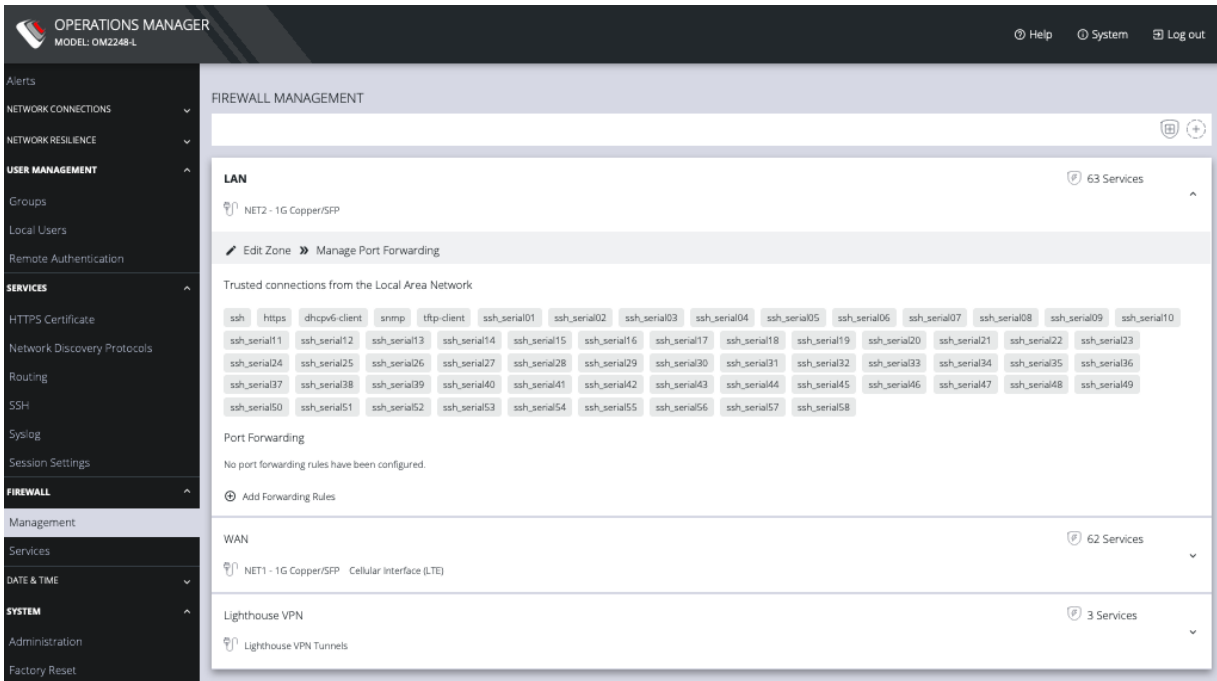
The **CONFIGURE > FIREWALL** menu lets you configure **Firewall Management**, **Interzone Policies**, and **Services**.



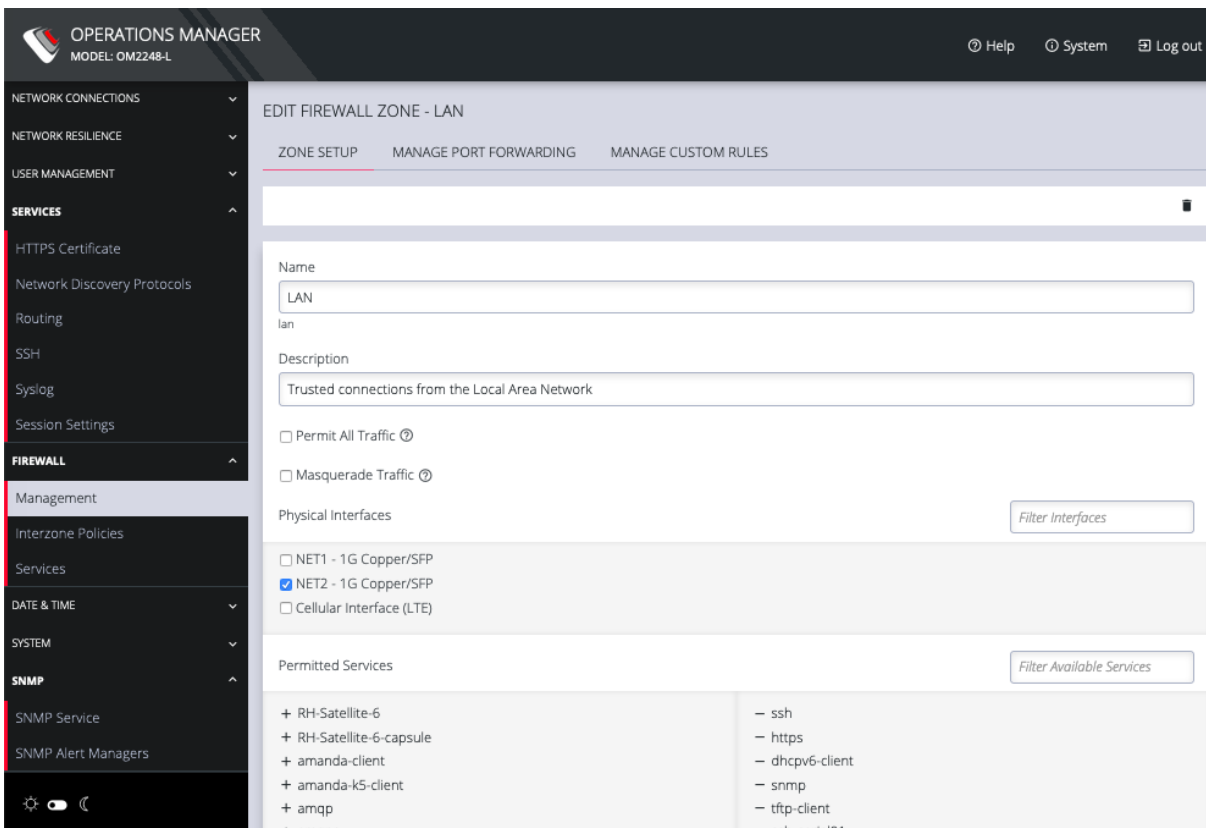
# Firewall Management

[CONFIGURE > FIREWALL > Management](#)

To change firewall management settings navigate to **CONFIGURE > FIREWALL > Management**.



You can expand each zone by clicking the Expand arrow on the right. Once expanded, you can click Edit Zone to change settings for a particular zone.

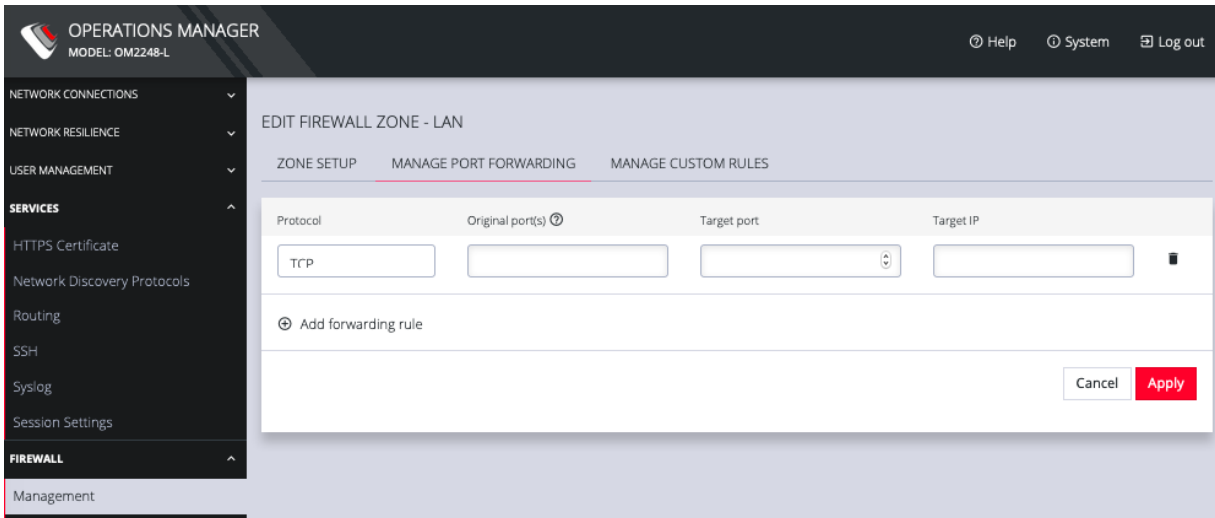


The **Edit Zone** page has three tabs. The **ZONE SETUP** page allows you to:

- Modify the Name of the zone
- Add a Description for this zone
- Permit all Traffic
- Masquerade Traffic
- Select Physical Interfaces
- Manage Permitted Services by clicking on Plus or Minus next to each

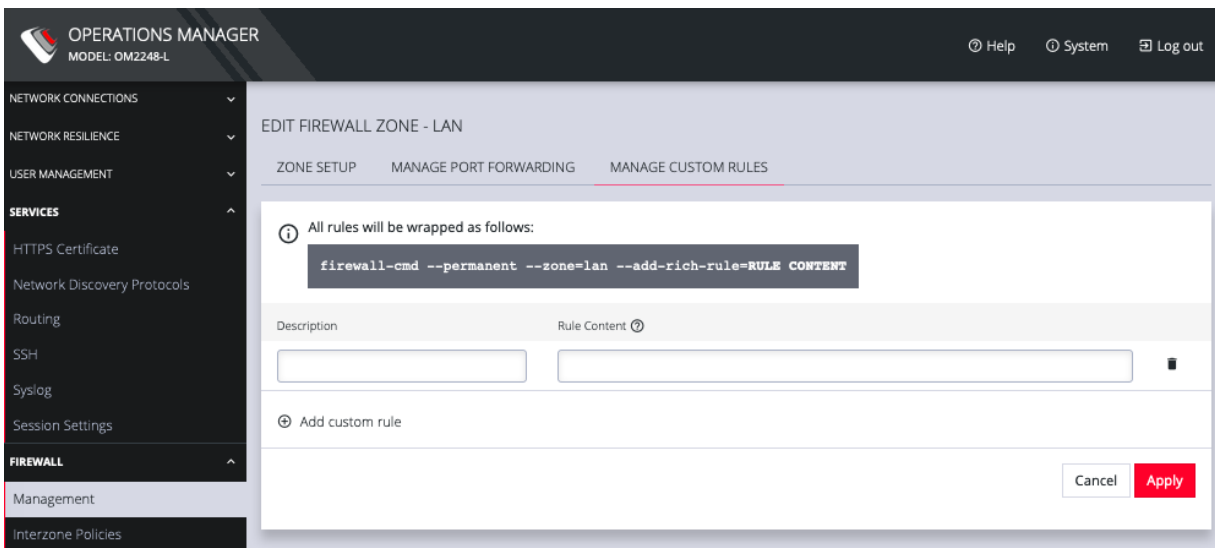
**Note:** You can use the Filter Interfaces and Filter Available Services text boxes to navigate through the lists.

The **MANAGE PORT FORWARDING** tab allows you to add, edit, and delete forwarding rules for the particular zone you are editing.



The third tab, **MANAGE CUSTOM RULES**, allows you to add, edit, and delete custom firewall rules for the zone you are editing. These custom rules continue to exist after reboots, upgrades, and power cycles.

These rules are prioritized by the order they are added.



To add a new custom rule:

CONFIGURE MENU	139
----------------	-----

1. Click Add custom rule.
2. Enter a Description for this rule.
3. Enter Rule Content, custom rule content formatted with firewall-cmd syntax.
4. Click Apply.

All rules will be wrapped as follows:

```
firewall-cmd --permanent --zone=lan --add-rich-rule=RULE CONTENT
```

Additional menu options under **CONFIGURE > FIREWALL** are **Rules, Services, and Zones**.

The main **FIREWALL MANAGEMENT** page also contains quick links to **Add Firewall Service** (shield icon on upper right), **Add Firewall Zone** (plus icon on upper right), and **Edit Zones** pages (pencil icon in expanded view) for the currently selected zone.

### Manage Firewall Rules

Click **CONFIGURE > FIREWALL > Services**. This opens the **SERVICES** page with a list of all firewall rules.

OPERATIONS MANAGER  
MODEL: OM2248-L

Help System Log out

Alerts

NETWORK CONNECTIONS

NETWORK RESILIENCE

USER MANAGEMENT

Groups

Local Users

Remote Authentication

SERVICES

HTTPS Certificate

Network Discovery Protocols

Routing

SSH

Syslog

Session Settings

FIREWALL

Management

Services

DATE & TIME

SYSTEM

Administration

Factory Reset

Reboot

System Upgrade

SERVICES

Name Label Ports Actions

No Firewall Services have been set

Delete Selected + ↺

PREDEFINED FIREWALL SERVICES

Name	Label	Ports
RH Satellite-6	Red Hat Satellite 6	68/udp 5000/tcp 5646-5647/tcp 5671/tcp 8000/tcp 8080/tcp 8140/tcp 9090/tcp
amanda-client	Amanda Backup Client	10080/udp 10080/tcp
amanda-k5-client	Amanda Backup Client (kerberized)	10082/tcp
amqp	amqp	5672/tcp
amqps	amqps	5671/tcp
apcupsd	apcupsd	3551/tcp
audit	Audit	60/tcp
bacula	Bacula	9101/tcp 9102/tcp 9103/tcp
bacula-client	Bacula Client	9102/tcp
bb	Big Brother	1984/tcp 1984/udp
bgp	BGP service listen	179/tcp

Services can be added, deleted, or edited from this page. Scroll to the bottom of the page to access the Plus button to add a new service.

ADD FIREWALL SERVICE

Name

Label

Port # Protocol

+ Add another port

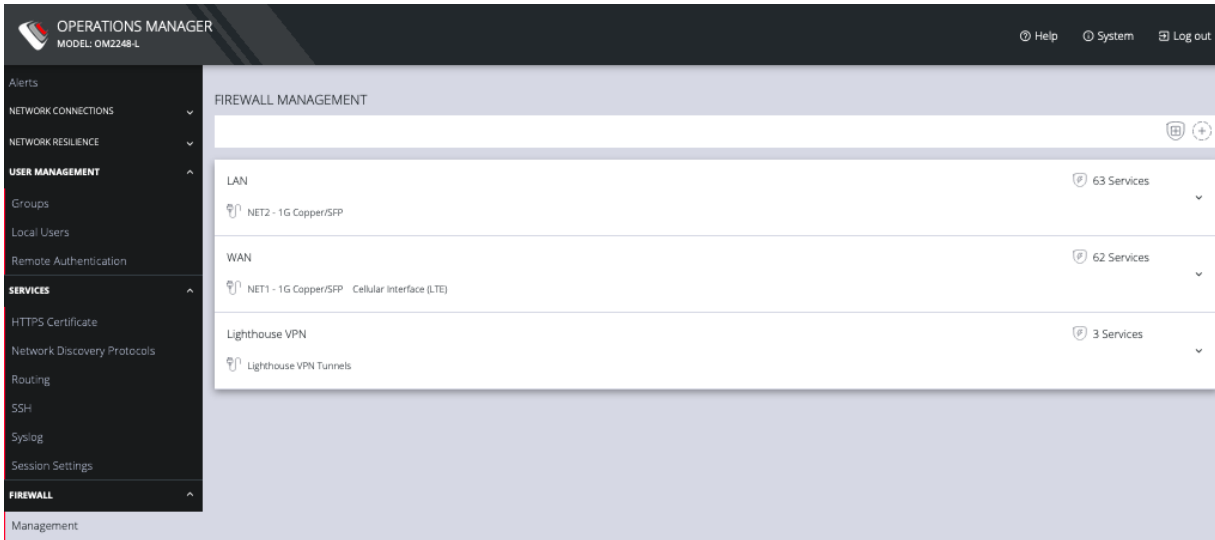
Cancel Apply

Enter a Service description and a Zone for the new rule.

## Manage Firewall Zones

Click **CONFIGURE > FIREWALL > MANAGEMENT**.

This opens the **ZONES** page with a list of all firewall zones.



Zone Name	Services
LAN NET2 - 1G Copper/SFP	63 Services
WAN NET1 - 1G Copper/SFP Cellular Interface (LTE)	62 Services
Lighthouse VPN Lighthouse VPN Tunnels	3 Services

Zones can be added, deleted, or edited from this page. Click the **PLUS** symbol on the top right of the page to add a new zone.

### ADD FIREWALL ZONE

Name

Label

Description

Permit All Traffic  
  
When this option is enabled, all traffic is permitted in this zone. Any rules configured for this zone will have no effect.

Masquerade Traffic  
  
When this option is enabled, traffic through this zone is masqueraded. If you wish to enable masquerading, it should be enabled on the zone bound to the external interface.

Adding an interface to this zone will remove that interface from the zone it is currently in. This may prevent access to the console server until appropriate rules are made for this zone.

Physical Interfaces  
 NET1 - 1G Copper/SFP  
 NET2 - 1G Copper/SFP  
 Cellular Interface (LTE)  
Traffic entering on the selected interfaces is in this zone

The **NEW FIREWALL ZONE** page allows you to:

- Name the zone
- Add a Description for this zone
- Permit all Traffic
- Masquerade Traffic
- Select Physical Interfaces

## Interzone Policies

[CONFIGURE > FIREWALL > Interzone Policies > Create Interzone Policy](#)

In the Operations Manager, Interzone firewall policy is implemented through FirewallD; this is a zone-based firewall which allows you to define zones and create rules to manage the traffic between the zones.

The firewallD feature provides a dynamically managed firewall with support for network/firewall “zones” to assign a level of trust to a network and its associated connections, interfaces or sources.


The feature allows you to define policies to configure forwarding between zones and can be configured to allow directional forwarding from one or more ingress zones to one or more egress zones.

Rules and filtering may be applied at the zone level. When you add a zone, you select which services are part of that zone. Interzone policy allows these rules and filtering to be applied so as to control the type of traffic allowed to be forwarded.

The default policy, ie. when no zones are added, is that no traffic is forwarded.

### Create an Interzone Policy

[CONFIGURE > FIREWALL > Interzone Policies > New Interzone Policy](#)

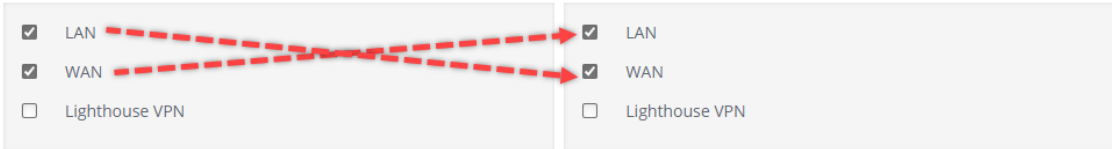
1. Navigate to the **Interzone Policies** page: [CONFIGURE > FIREWALL > Interzone Policies](#).
2. Click the **Add Firewall Policy** button  , the **New Interzone Policy** page opens for editing.
3. In the **Name** field, enter a name that clearly identifies this policy instance to other users.



4. In the **Description** field provide a detailed description of this interzone policy (optional).
5. Click to check the boxes for each Ingress and Egress zone that is to be included in this policy. You can configure traffic in both directions by selecting both zones in the Ingress and Egress as indicated by the red arrows in the image below:

#### *Two Directional Traffic Interzone Policy:*

INGRESS ZONES	EGRESS ZONES
<small>Traffic originating from the ingress zones will be allowed to forward to the egress zones.</small>	<small>The egress zones specify the list of zones that traffic will be forwarded to in this policy.</small>
<input type="checkbox"/> Select All Zones	<input type="checkbox"/> Select All Zones
<input checked="" type="checkbox"/> LAN	<input checked="" type="checkbox"/> LAN
<input checked="" type="checkbox"/> WAN	<input checked="" type="checkbox"/> WAN
<input type="checkbox"/> Lighthouse VPN	<input type="checkbox"/> Lighthouse VPN



**Note:** Additional zones may be added to the zones list at: [CONFIGURE > FIREWALL > Management > New Firewall Zone](#).  
Zone customized rules may be edited at [CONFIGURE > FIREWALL > Management > Firewall Management](#).

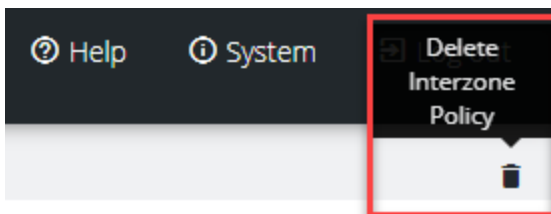
6. Click the **Apply** button to implement the policy, a green banner will inform you that the policy details are saved successfully. The interzone policy is now in force.

## Edit or Delete an Interzone Policy

[CONFIGURE > FIREWALL > Interzone Policies > Edit Interzone Policy](#)

1. Navigate to the **Interzone Policies** page: [CONFIGURE > FIREWALL > Interzone Policies](#).

2. Click the name of the policy you wish to edit (editable policies are identified by **red text**). The **Edit Interzone Policy** page opens for editing.
3. Edit the policy details to be changed.
4. If necessary, change the the **Description** field to provide a detailed description of the edited interzone policy.
5. To **delete** a policy, click on the **Bin** widget in the top-right corner of the **Edit** page.



- 6.
7. Click the **Apply** button to implement the edited policy, a green banner will inform you that the policy details are saved successfully. The edited interzone policy is now in force.

## Customized Zone Rules

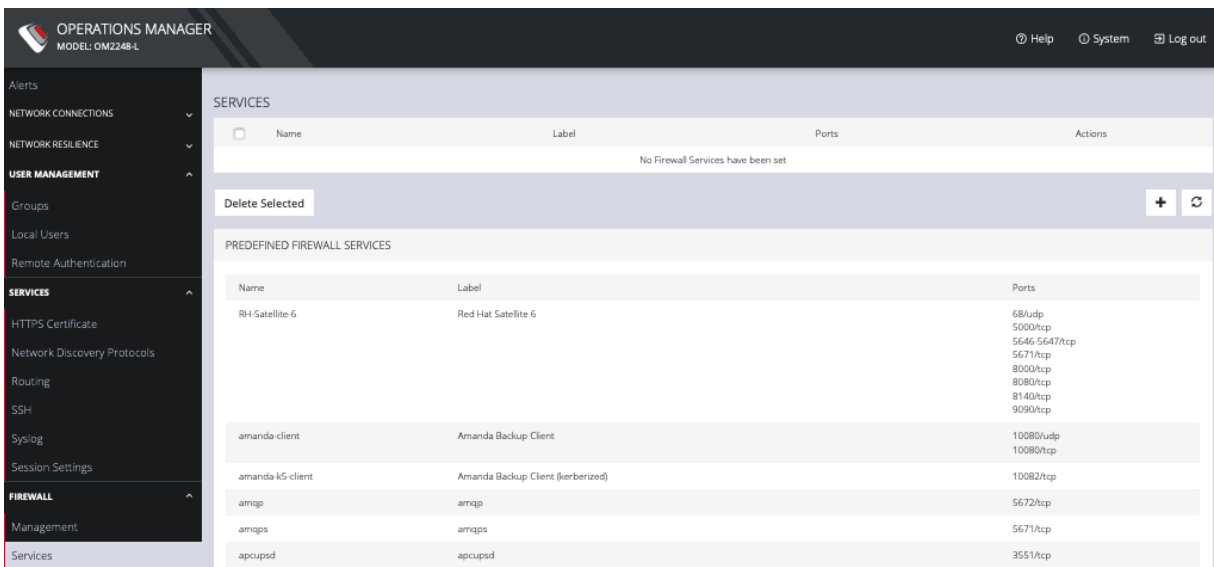
Customized zone rules may be applied to any zone at [CONFIGURE > FIREWALL > Management > Firewall Management: "Firewall Management"](#) on page 137.

## Services - Firewall

[CONFIGURE](#) > [FIREWALL](#) > [Services](#)

Managing Firewall Services

Click **CONFIGURE** > **FIREWALL** > **Services**. This opens the **SERVICES** page with a long list of predefined firewall services.



OPERATIONS MANAGER  
MODEL: OM2248-L

Help System Log out

Alerts

NETWORK CONNECTIONS

NETWORK RESILIENCE

USER MANAGEMENT

Groups

Local Users

Remote Authentication

**SERVICES**

HTTPS Certificate

Network Discovery Protocols

Routing

SSH

Syslog

Session Settings

**FIREWALL**

Management

Services

SERVICES

Name Label Ports Actions

No Firewall Services have been set

Delete Selected + ↺

PREDEFINED FIREWALL SERVICES

Name	Label	Ports
RH-Satellite-6	Red Hat Satellite 6	68Audp 5000/tcp 5646-5647/tcp 5671/tcp 8000/tcp 8080/tcp 8140/tcp 9090/tcp
amanda-client	Amanda Backup Client	10080/udp 10080/tcp
amanda-k5-client	Amanda Backup Client (kerberized)	10082/tcp
amqp	amqp	5672/tcp
amqps	amqps	5671/tcp
apcupsd	apcupsd	3551/tcp

Services can be added, deleted, or edited from this page.

**Note:** Predefined services cannot be edited.

Click the **Plus** button to add a new service.

#### ADD FIREWALL SERVICE

Name

Label

Port #

Protocol

+ Add another port

Cancel

Apply

Enter a **Name**, **Label**, **Port #**, and **Protocol**. Select a **Protocol** (TCP or UDP) from the **Plus** button menu. Add more **Ports** and **Protocols** as desired and click **Apply**.

## Date & Time

### [CONFIGURE > DATE & TIME](#)

The Date & Time section of the navigation bar provides a means to

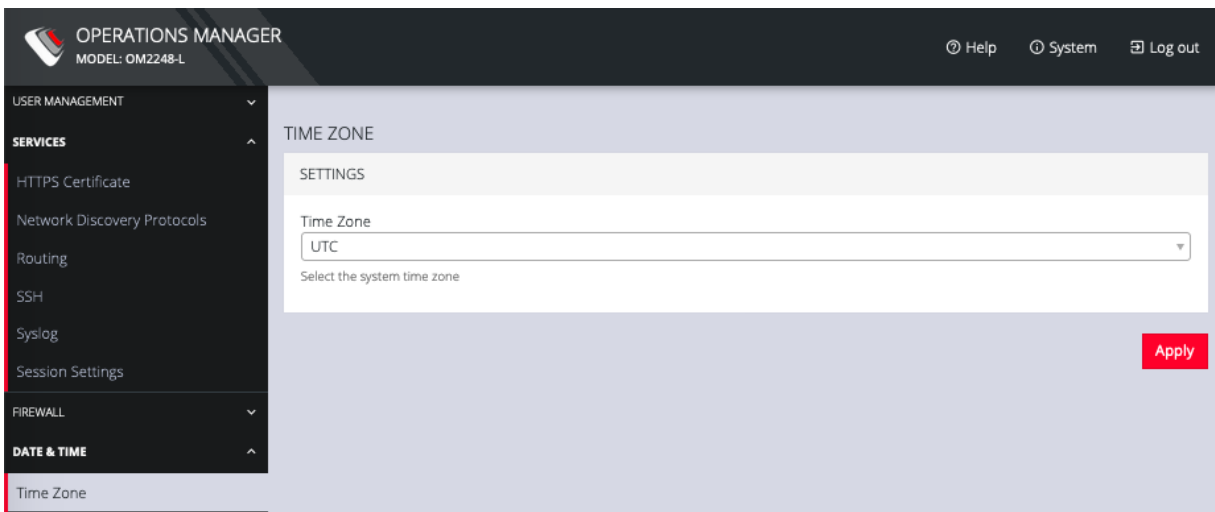
- Set the time zone
- Manually set the correct time and date
- Automatically set the date and time

## Time Zone

[CONFIGURE](#) > [DATE & TIME](#) > [Time Zone](#)

To set the time zone:

1. Click **CONFIGURE** > **DATE & TIME** > **Time Zone**.
2. Select the OPERATIONS MANAGER's time-zone from the **Time Zone** drop-down list.
3. Click **Apply**.

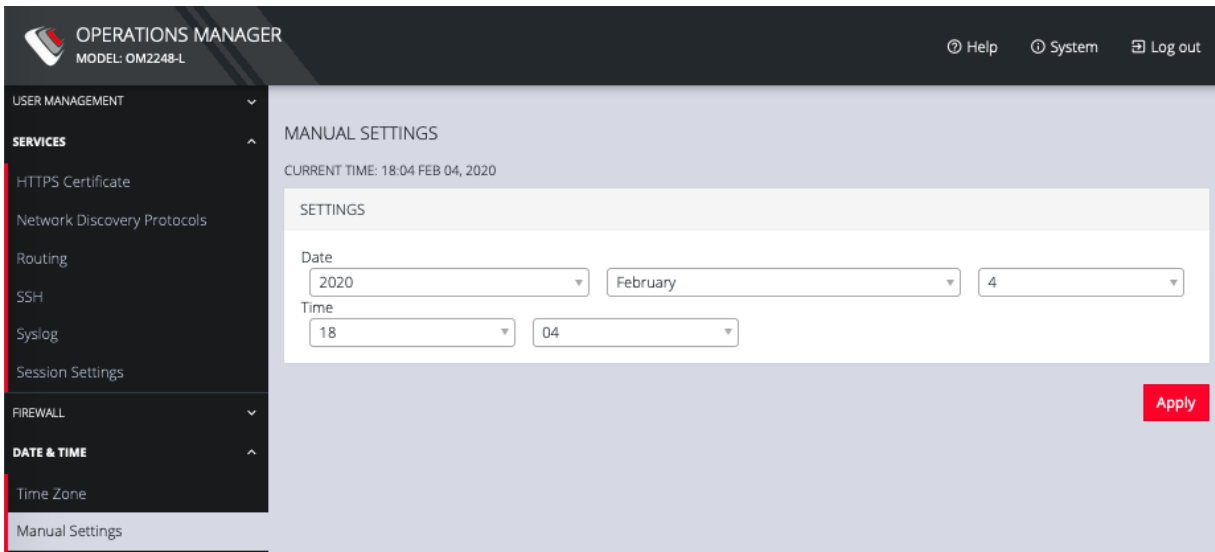


## Manual Settings

[CONFIGURE](#) > [DATE & TIME](#) > [Manual Settings](#)

To manually set the correct time and date:

1. Click **CONFIGURE** > **DATE & TIME** > **Manual Settings**.
2. Enter the current **Date** and **Time**.
3. Click **Apply**.



OPERATIONS MANAGER  
MODEL: OM2248-L

Help System Log out

USER MANAGEMENT

SERVICES

HTTPS Certificate

Network Discovery Protocols

Routing

SSH

Syslog

Session Settings

FIREWALL

DATE & TIME

Time Zone

Manual Settings

MANUAL SETTINGS

CURRENT TIME: 18:04 FEB 04, 2020

SETTINGS

Date

2020 February 4

Time

18 04

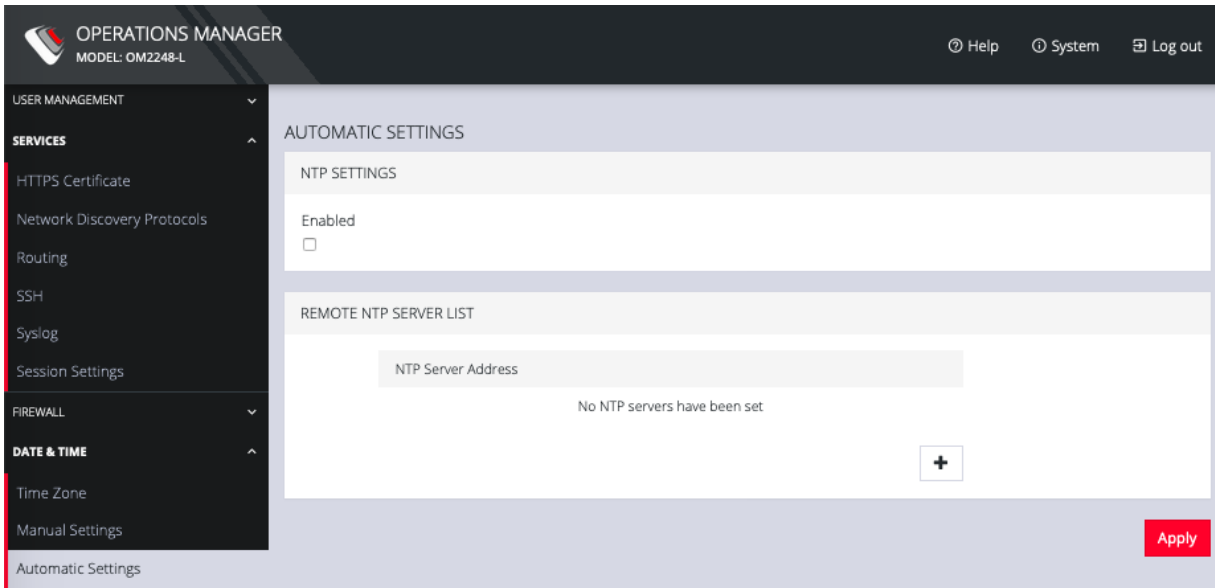
Apply

## Automatic Settings

[CONFIGURE](#) > [DATE & TIME](#) > [Automatic Settings](#)

Automatic Setting of the date and time:

1. Click **CONFIGURE > DATE & TIME > Automatic Settings**.
2. Click the *Enabled* checkbox.
3. Enter a working NTP Server address in the **NTP Server Address** field.
4. Click **Apply**.



The screenshot shows the OpenGear Operations Manager web interface. The top navigation bar includes the logo, 'OPERATIONS MANAGER MODEL: OM2248-L', and links for 'Help', 'System', and 'Log out'. A left sidebar menu is expanded to 'DATE & TIME', with 'Automatic Settings' selected. The main content area is titled 'AUTOMATIC SETTINGS' and contains two sections: 'NTP SETTINGS' with an 'Enabled' checkbox, and 'REMOTE NTP SERVER LIST' with a text input field labeled 'NTP Server Address' and a '+', followed by the text 'No NTP servers have been set'. A red 'Apply' button is located at the bottom right of the settings area.



# System

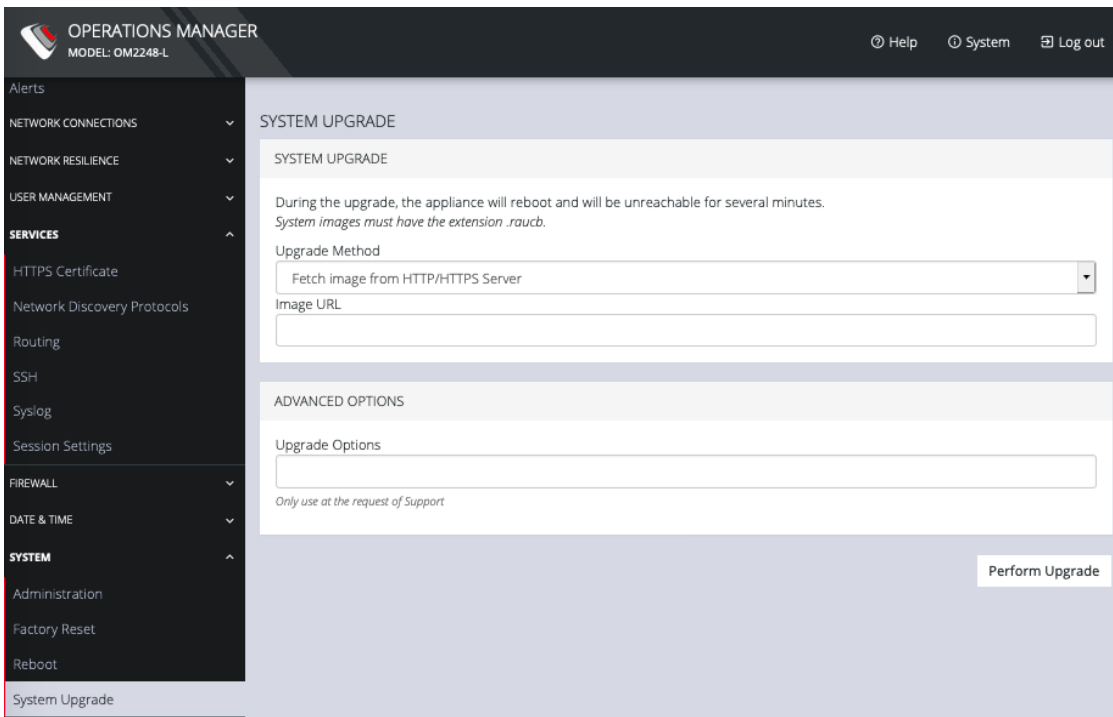
## CONFIGURE > SYSTEM

The **CONFIGURE > SYSTEM** menu lets you change the OPERATIONS MANAGER hostname, perform system upgrades, and reset the system.

You can perform a system upgrade when new firmware is released. After specifying the location of the firmware and beginning the process, the system will unavailable for several minutes and then reboot. Unlike a factory reset, users, and other configuration data is maintained.

To perform a system upgrade:

1. Navigate to **CONFIGURE > System > System Upgrade**.
2. Select the **Upgrade Method**, either **Fetch image from HTTP/HTTPS Server** or **Upload Image**.



If upgrading via **Fetch image from HTTP/HTTPS Server**:

1. Enter the URL for the system image in the **Image URL** text-entry field.
2. Click **Perform Upgrade**.

Or if upgrading via **Upload Image**:

1. Click the **Choose file** button.
2. Navigate to the directory containing the file.
3. Select the file and press **Return**.
4. Click **Perform Upgrade**.

**Note:** The **Advanced Options** section should only be used if a system upgrade is being performed as part of an OpenGear Support call.

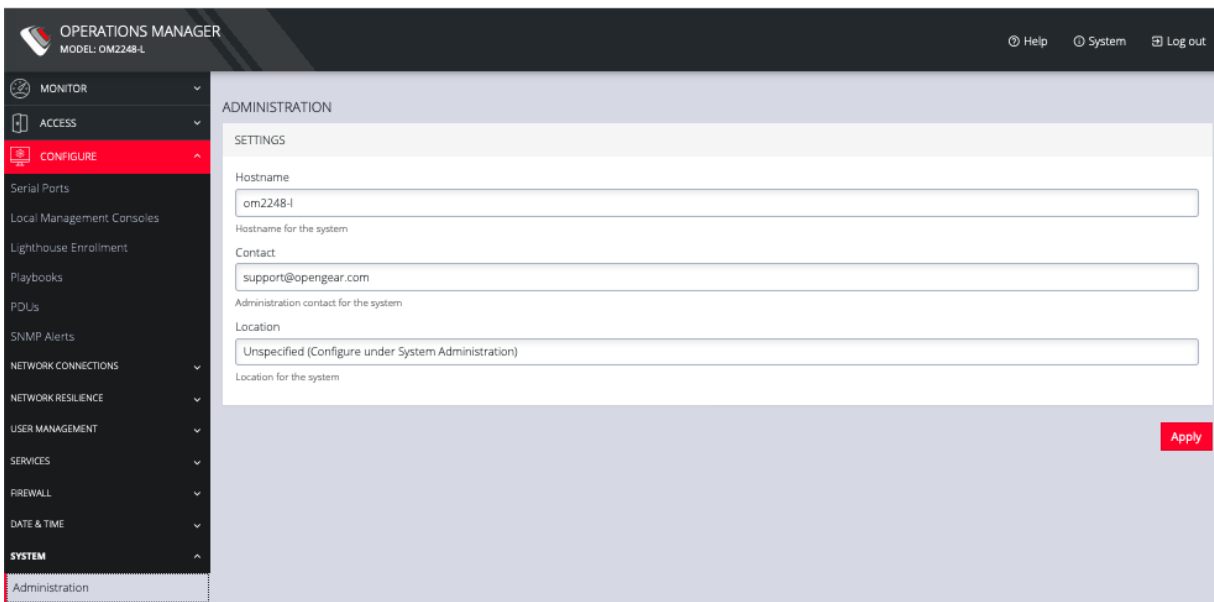
Once the upgrade has started, the System Upgrade page displays feedback as to the state of the process.

## Administration

[CONFIGURE](#) > [SYSTEM](#) > Administration

To set the hostname, add a contact email, or set a location for the OPERATIONS MANAGER:

1. Click **CONFIGURE** > **SYSTEM** > **Administration**.
2. Edit the **Hostname** field.



OPERATIONS MANAGER  
MODEL: OM2248-L

Help System Log out

MONITOR  
ACCESS  
CONFIGURE  
Serial Ports  
Local Management Consoles  
Lighthouse Enrollment  
Playbooks  
PDUs  
SNMP Alerts  
NETWORK CONNECTIONS  
NETWORK RESILIENCE  
USER MANAGEMENT  
SERVICES  
FIREWALL  
DATE & TIME  
SYSTEM  
Administration

ADMINISTRATION

SETTINGS

Hostname  
om2248-l  
Hostname for the system

Contact  
support@opengear.com  
Administration contact for the system

Location  
Unspecified (Configure under System Administration)  
Location for the system

Apply

3. Click **Apply**.

## Factory Reset

[CONFIGURE > SYSTEM > Factory Reset](#)

You can perform a factory reset, where logs and docker containers are preserved and everything else is reset to the factory default.

To return the OPERATIONS MANAGER to its factory settings:

1. Select **CONFIGURE > SYSTEM > Factory Reset**.
2. Read the Factory Reset warning notice.

**Warning:** This will delete all configuration data from the system and reset all options to the factory defaults. Any custom data or scripts on the device will be lost. Please check the box below to confirm you wish to proceed.

3. If you still wish to proceed with the reset, Select the **Proceed with the factory reset** checkbox.
2. Click **Reset**.

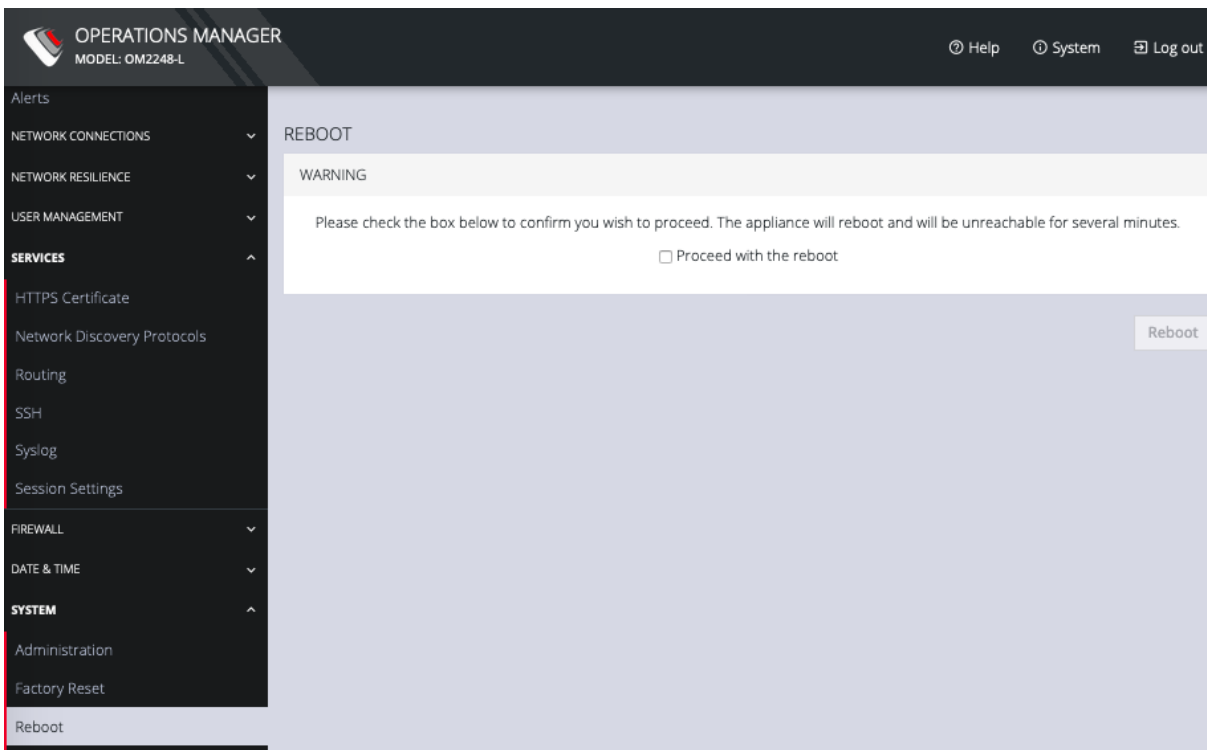
**Warning:** This operation performs the same operation as the hard factory erase button. This resets the appliance to its factory default settings. Any modified configuration information is erased. You will be prompted to log in and must enter the default administration username and administration password (Username: root Password: default). You will be required to change this password during the first log in.

## Reboot

[CONFIGURE](#) > [SYSTEM](#) > [Reboot](#)

To reboot the OPERATIONS MANAGER:

Select **CONFIGURE** > **SYSTEM** > **Reboot**.



Select **Proceed with the reboot** and click **Reboot**.

## System Upgrade

[CONFIGURE > SYSTEM > System Upgrade](#)

You can perform a system upgrade when new firmware is released. After specifying the location of the firmware and beginning the process, the system will be unavailable for several minutes and then reboot. Unlike a factory reset, users, and other configuration data is maintained.

To perform a system upgrade:

1. Navigate to the **CONFIGURE > System > System Upgrade** page.
2. Select the **Upgrade Method**, either **Fetch image from HTTP/HTTPS Server** or **Upload Image**.

## SNMP

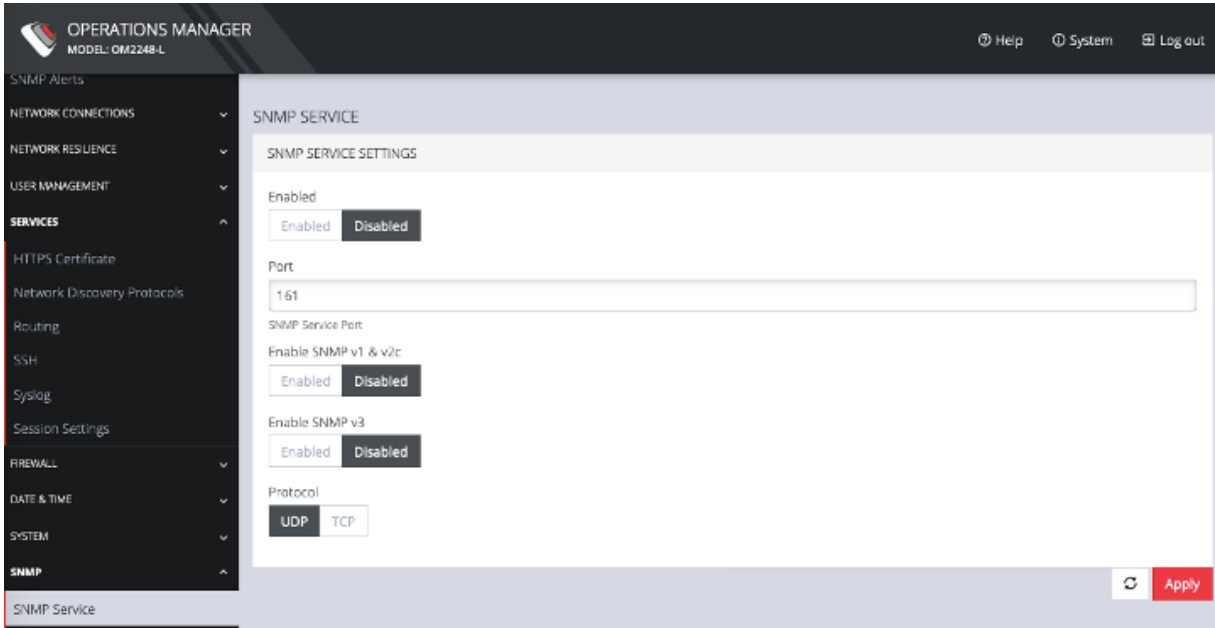
[CONFIGURE > SNMP](#)

The **CONFIGURE > SNMP** menu has two options, **SNMP Service** and **SNMP Alert Managers**.

## SNMP Service

[CONFIGURE](#) > [SNMP](#) > [SNMP Service](#)

Navigate to the **CONFIGURE > SNMP > SNMP Service** to open the **SNMP Service** page.



This page allows you to specify which SNMP services to enable. When you click on **ENABLED** for **SNMP V1 & V2** or **SNMP V3**, a detail form appears where you can add service specific settings.

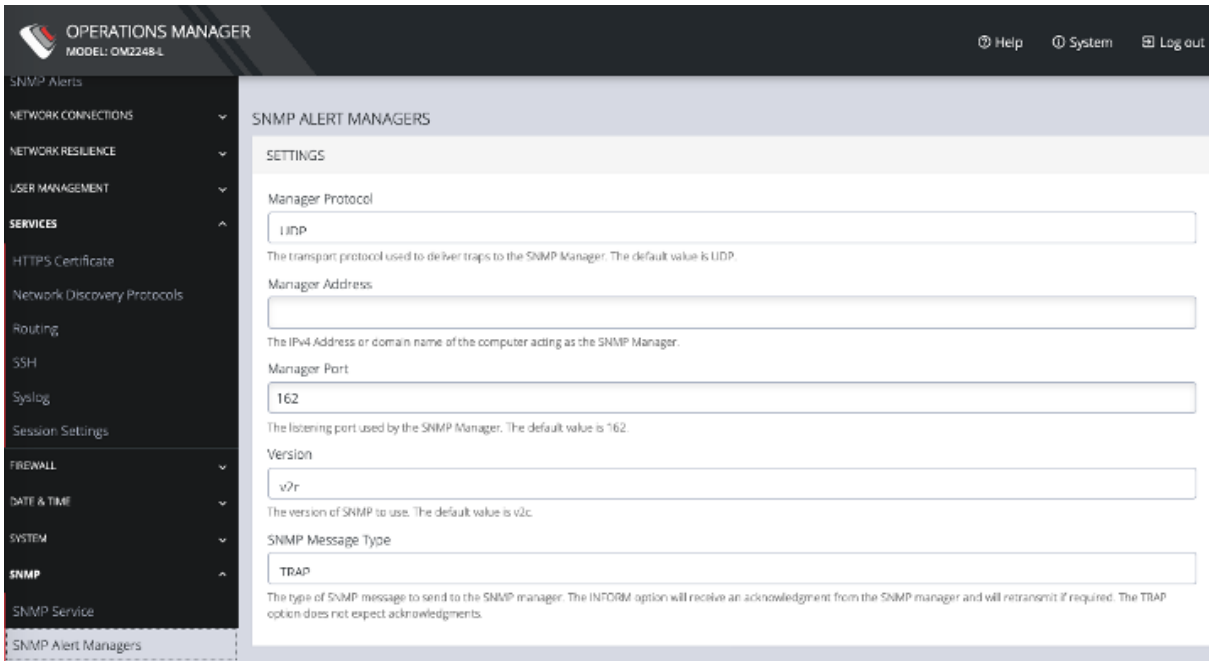
You can also specify the **SNMP Service Port** and choose between **UDP** or **TCP** for the **Protocol**.



# SNMP Alert Managers

[CONFIGURE](#) > [SNMP](#) > [SNMP Alert Managers](#)

Navigate to **CONFIGURE > SNMP > SNMP Alert Managers** to open the **SNMP Alert Managers** page.



On this page, you can set the following:

- **Manager Protocol:** The transport protocol used to deliver traps to the SNMP Manager. The default value is UDP.
- **Manager Address:** The IPv4 Address or domain name of the computer acting as the SNMP Manager.
- **Manager Port:** The listening port used by the SNMP Manager. The default value is 162.
- **Version:** The version of SNMP to use. The default is v2c.



· **SNMP Message Type:** The type of SNMP message to send to the SNMP manager. The INFORM option will receive an acknowledgment from the SNMP manager and will retransmit if required. The TRAP option does not expect acknowledgments.

For SNMP V1 & V2C, you can specify a **Community**. This is a group name authorized to send traps by the SNMP manager configuration for SNMP versions 1 and 2c. This must match the information that is setup in the SNMP Manager. Examples of commonly used values are log, execute, net and public.

## Multiple SNMP Alert Managers

[CONFIGURE > SNMP > SNMP Alert Managers > Add New SNMP Alert Manager](#)

The Multiple SNMP Alert Managers feature provides the option to configure more than one SNMP manager. Multiple SNMP Alert Managers can receive trap and inform events that can be used to trigger remedial action; events can be sent to multiple SNMP Alert Managers. The AR functionality sends traps to all configured SNMP Alert Managers for a reaction of type SNMP. Whether you input an IPv6 address or a domain name, the correct protocol needs to be selected.

### Create or Delete a New SNMP Manager

To create a new SNMP manager:

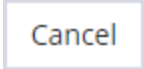


1. Navigate to **Configure > SNMP > SNMP Alert Managers**.
2. Click the **Add New SNMP Manager** button (a plus character in the top-right of the window)
3. Complete the new **SNMP Alert Manager Form** as per the **Definitions** table below.
4. Click the **Submit** button. A banner appears confirming that the new SNMP Manager has been successfully created.
5. The new manager appears in the list of SNMP Alert Managers.
6. To delete an SNMP manager, click on the IP address of the item to open the **Edit SNMP Manager** page for that SNMP Manager.
7. Click on the **Delete SNMP Manager** widget in the top-right of the page.

**Note:** If you would like to use an IPv6 Address, then you need to select either UDP6 or TCP6 from the list of protocols. Whether you input an IPv6 address or a domain name, the correct protocol needs to be selected.

**Note:** For SNMP V3 TRAPS, an Engine ID will be provided by default if none is specified. This is generated by the snmpd service and can be found in the SNMPD RUNTIME CONF `/var/lib/net-snmp/snmpd.conf`. Traps will be sent for Alerts added in **Configure > SNMP Alerts**. Traps will also be sent to all the configured SNMP Alert Managers for a Playbook SNMP Reaction.

## New SNMP Alert Manager Page Definitions

New SNMP Alert Manager Field	Definition
Description	The editable Description field allows you to add a description of the SNMP Alert Manager.
Server Address	The IPv4/IPv6 address or domain name of the computer acting as the SNMP Alert Manager.
Port	The listening port used by the SNMP Alert Manager. The default value is 162.
Protocol	<p>The transport protocol used to deliver traps or informs (for SNMP v3).</p> <p>UDP - Speeds up transmissions by enabling the transfer of data before an agreement is provided by the receiving party.</p> <p>TCP - A commonly used protocol used to transmit data from other higher-level protocols that require all transmitted data to arrive.</p> <p>UDP6 - Similar to UDP but uses IPv6.</p> <p>TCP6 - Similar to TCP but uses IPv6.</p>

Version	<p>The version of SNMP protocol to use. The default value is v2c. For further reading on SNMP versions we suggest:</p> <p><a href="https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol#Protocol_versions">https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol#Protocol_versions</a></p>
SNMP V1 & V2C Community	<p>A group name authorized to send traps by the SNMP alert manager configuration for SNMP versions 1 and 2c. This will need to match what is setup in the SNMP alert manager. Examples of commonly used values are log, execute, net and public.</p>
 	<p>Click the <b>Submit</b> button to finalize the New SNMP Manger process.</p>
	<p>Click the bin widget to <b>Delete</b> an SNMP Manager (in the Edit SNMP Manager page).</p>

## Advanced Options

The OPERATIONS MANAGER supports a number of command line interface (CLI) options and REST API.

# address : Primary Lighthouse address to enroll with

# api\_port : Optional port to use for the primary address when requesting enrollment

# external\_endpoints : List of additional "address:port" endpoints to fall back to when enrolling

# password : LH global or bundle enrollment password

# bundle : Name of LH enrollment bundle

## Communicating With The Cellular Modem

Interfacing with the cellular modem is currently only available via CLI.

Usage:

`mmcli [OPTION?] - Control and monitor the ModemManager`

Options:

<code>-h, --help</code>	Show help options
<code>--help-all</code>	Show all help options
<code>--help-manager</code>	Show manager options
<code>--help-common</code>	Show common options
<code>--help-modem</code>	Show modem options
<code>--help-3gpp</code>	Show 3GPP related options
<code>--help-cdma</code>	Show CDMA related options
<code>--help-simple</code>	Show Simple options
<code>--help-location</code>	Show Location options
<code>--help-messaging</code>	Show Messaging options
<code>--help-voice</code>	Show Voice options

<code>--help-time</code>	Show Time options
<code>--help-firmware</code>	Show Firmware options
<code>--help-signal</code>	Show Signal options
<code>--help-oma</code>	Show OMA options
<code>--help-sim</code>	Show SIM options
<code>--help-bearer</code>	Show bearer options
<code>--help-sms</code>	Show SMS options
<code>--help-call</code>	Show call options

#### Application Options:

- `-v, --verbose` Run action with verbose logs
- `-V, --version` Print version
- `-a, --async` Use asynchronous methods
- `--timeout=[SECONDS]` Timeout for the operation



## OGCLI Guide

The Operations Manager employs an API-first approach, so all configuration tasks are brokered via its RESTful API. The web UI and ogcli tool are convenient clients of this API. The ogcli allows you to inspect and modify the configuration tree from the command line.

### Commands For Exploring ogcli Usage

**Note:** Double-quotes around strings should be protected from the shell. For single quotes use the dedicated quotes key, do not use the shared Tilde key, for example:

```
'password="mypass"' and NOT `password="mypass"``
```

The ogcli features tab completion to assist when typing commands. Additionally, extensive help is available by running commands that you can try out, for example:

```
##### ogcli #####
ogcli --help = show this help message then exit
ogcli --usage = show usage examples then exit
ogcli --notation = show the simple notation reference
then exit
ogcli --list-endpoints = list all the endpoints
ogcli help <endpoint> = show help information for this
endpoint
-d = increase debugging (up to 2 times)
```

```
##### ogcli (continued) #####-j = use JSON instead
of simple notation (for coloured, structured print out-
put).
-u USERNAME, --username USERNAME = authenticate as a dif-
ferent user
-p PASSWORD, --password PASSWORD = authenticate with the
supplied password
```

## ogcli Sub Commands

```
##### sub-command operations #####
get (g) fetch a list or item
replace (r) replace a list or item
update (u) update an item
merge (m) merge a provided list with existing config
create (c) create an item
delete (d) delete a list or item
help (h) help for an endpoint
export (e) export the existing configuration
import (i) import the existing configuration
```

## Commonly Used ogcli Commands

```
##### Replace MOTD displayed at log in #####
ogcli replace banner 'banner="DESIRED MESSAGE HERE" '
```

```
##### Retrieve items #####
ogcli get user <username> > record
```

**##### Replace items #####**

*Modify items:*

```
ogcli update user <username> < partial_record
```

*For fields where the value is a string:*

```
ogcli update user <username> 'field="value"'
```

*For fields where the value is not a string, e.g. to enable/disable a user:*

```
ogcli update user <username> field=value
```

**##### Create items #####**

```
Ogcli create user <username>
```

**##### Delete items #####**

```
ogcli delete user <username>
```

**##### Merge items in a list #####**

```
ogcli merge syslog_servers < list of records
```

**##### Export all config #####**

```
ogcli export [/path/to/file]
```

```
##### Import config #####
ogcli import [/path/to/file]
ogcli import < [/path/to/file]
```

*ogcli takes records from stdin so a variety of options are available when passing records.*

```
##### Create user #####
ogcli create user << 'END'
  description="superuser"
  enabled=true
  groups[0]="admin"
  no_password=true
  username="root"
END

echo 'username="root"
description="superuser"
no_password=false
password="mysecretpass"' | ogcli
create user
```

*ogcli takes records from stdin so a variety of options are available. ogcli also takes records from any additional command line arguments.*

## Configuration Task Examples in ogcli

These examples contain a variety of notations and usage patterns to help illustrate the flexibility of ogcli. The examples can be copied and pasted into the CLI.

### ##### Change root password #####

```
sudo ogcli update user root 'password="oursecret"'
```

### ##### Create admin user #####

```
sudo ogcli create user <<'END'  
  username="adal"  
  description="Ada Lovelace"  
  enabled=true  
  no_password=false  
  groups[0]="groups-1"  
  password="oursecret"  
END
```

### ##### Manually set date and time #####

```
sudo ogcli update system/timezone 'timezone=  
e="America/New_York" '  
sudo ogcli update system/time 'time="15:30 Mar 27,  
2020" '
```

### ##### Enable NTP #####

```
sudo ogcli update services/ntp <<'END'  
  enabled=true  
  servers[0].value="0.au.pool.ntp.org"  
END
```

**##### Set system hostname #####**

```
sudo ogcli update hostname 'hostname="oob01"'
```

**##### Adjust session timeouts #####**

```
sudo ogcli update system/cli_session_timeout 'timeout-  
t=180'
```

```
sudo ogcli update system/webui_session_timeout 'timeout-  
t=180'
```

**##### Setup TACACS remote AAA #####**

```
sudo ogcli update auth <<'END'  
  mode="tacacs"  
  tacacsAuthenticationServers[0].host name=  
e="192.168.250.21"  
  tacacsMethod="pap"  
  tacacsPassword="tackey"  
END
```

**##### Setup RADIUS remote AAA #####**

```
sudo ogcli update auth <<'END'  
  mode="radius"  
  radiusAuthenticationServers[0].host-  
name="192.168.250.21"  
  radiusAccountingServers[0].hostname="192.168.250.21"  
  radiusPassword="radkey"  
END
```

```
##### Create user group with limited access to  
console ports #####
```

```
sudo ogcli create group <<'END'  
  description="Console Operators"  
  groupname="operators"  
  role="ConsoleUser"  
  mode="scoped"  
  ports[0]="ports-10"  
  ports[1]="ports-11"  
  ports[2]="ports-12"  
END
```

```
##### View and configure network settings #####
```

```
sudo ogcli get conns  
sudo ogcli get conn system_net_conns-1  
  
sudo ogcli update conn system_net_conns-1 'ipv4_static_  
settings.address="192.168.0.3" '  
  
sudo ogcli create conn <<'END'  
  description="2nd IPv4 Static Address Example"  
  mode="static"  
  ipv4_static_settings.address="192.168.33.33"  
  ipv4_static_settings.netmask="255.255.255.0"  
  ipv4_static_settings.gateway="192.168.33.254"  
  physif="net1"  
END
```

```
##### Set up serial console ports #####
sudo ogcli get ports
sudo ogcli get ports | grep label
sudo ogcli get port ports-1

sudo ogcli update port "serial/by-opengear-id/port05"
<<'END'
  mode="consoleServer"
  label="Router"
  pinout="X2"
  baudrate="9600"
  databits="8"
  parity="none"
  stopbits="1"
  escape_char="~"
  ip_alias[0].ipaddress="192.168.33.35/24"
  ip_alias[0].interface="net1"
  logging_level="eventsOnly"
END
```

```
##### Enable cellular modem #####
sudo ogcli get physifs

sudo ogcli update physif wwan0 <<'END'
  enabled=true
  physif.cellular_setting.apn="broadband"
  physif.cellular_setting.ipctype="IPv4v6"
END
```



```
##### Disable cellular modem #####  
sudo ogcli update physif physif wwan0 'enabled=false'
```

```
##### Enable remote syslog #####  
sudo ogcli create services/syslog_server 'address-  
s="192.168.34.112" '  
  
sudo ogcli create services/syslog_server <<'END'  
address="192.168.34.113"  
protocol="UDP"  
port=514  
END
```

```
##### Enable local console boot messages #####  
sudo ogcli get managementports  
  
sudo ogcli update managementport mgmtPorts-1 'ker-  
neldebug=true'
```

## Available Endpoints

Here is the full list of available endpoints that can be used with the ogcli sub-commands:

ENDPOINT	OPERATIONS	ARGS
alerts/authentication	get/replace	
alerts/config_change	get/replace	
alerts/networking	get/replace	
alerts/system	get/replace	
auth	get/replace	
auto_response/beacons	get/merge/delete	
auto_response/beacon	create/get/replace/delete	id
auto_response/reactions	get/merge/delete	
auto_response/reaction	create/get/replace/delete	id
auto_response/status	get	
auto_response/status/beacon-modules	get	

auto_response/status/beacons	get	id
cellfw/info	get	
conns	get/merge	
conn	create/get/replace/delete	id
export	get	
failover/settings	get/replace	
failover/status	get	
firewall/policies	get/merge	
firewall/policy	create/get/replace/delete	id
firewall/predefined_services	get	
firewall/rules	get/merge/delete	
firewall/rule	create/get/replace/delete	id
firewall/services	get/merge	
firewall/service	create/get/replace/delete	id
firewall/zones	get/merge	

firewall/zone	create/get/replace/delete	id
groups	get/merge/replace	
group	create/get/replace/delete	id
ip_passthrough	get/replace	
ip_passthrough/status	get	
ipsec_tunnels	get/merge	
ipsec_tunnel	create/get/replace/delete	id
lighthouse_enrollments	get	
lighthouse_enrollment	create/get/delete	id
logs/portlog	get	id
managementports	get/merge	
managementport	get/replace	id
monitor/ldp/chassis	get	
monitor/ldp/neighbor	get	
pdus	get/merge	

pdu	create/get/replace/delete	id
physifs	get/merge	
physif	create/get/replace/delete	id
ports	get/merge	
port	get/replace	id
port_power	replace	id
port_sessions	get/delete	
port_session	get/delete	idpid
ports/auto_discover/schedule	get/replace	
ports/fields	get	
search/ports	get	
services/https	get/replace	
services/lldp	get/replace	
services/ntp	get/replace	
services/routing	get/replace	

services/snmp_manager	get/replace	
services/snmpd	get/replace	
services/ssh	get/replace	
services/syslog_servers	get/merge	
services/syslog_server	create/get/replace/delete	syslog_server_id
ssh/authorized_keys	get/merge	
ssh/authorized_key	create/delete	user-idkey-id
static_routes	get/merge/replace/delete	
static_route	create/get/replace/delete	id
system/admin_info	get/replace	
system/banner	get/replace	
system/cell_reliability_test	get/replace	
system/cli_session_timeout	get/replace	
system/firmware_upgrade_status	get	

system/hostname	get/replace	
system/model_name	get	
system/serial_number	get	
system/ssh_port	get/replace	
system/system_authorized_keys	get/merge	
system/system_authorized_key	create/delete	key-id
system/time	get/replace	
system/timezone	get/replace	
system/version	get	
system/webui_session_timeout	get/replace	
users	get/merge/replace	
user	create/get/replace/delete	user-id

## Docker

Docker is a tool designed to make it easier to create, deploy, and run applications by distributing them in containers. Developers can use containers to package up an application with all of the parts it needs, like libraries and dependencies, and then ship it out as one package. Docker is running by default on the OPERATIONS MANAGER. You can access commands by typing `docker` in the Local Terminal or SSH.

For more information on Docker, enter `docker --help`.



## Cron

Cron service can be used for scheduled cron jobs runs. Daemon can be managed via the `/etc/init.d/crond` interface, and cron tables managed via `crontab`. `Crontab` supports:

Usage:

```
crontab [options] file
```

```
crontab [options]
```

```
crontab -n [hostname]
```

### Options:

`-u <user>` define user

`-e` edit user's crontab

`-l` list user's crontab

`-r` delete user's crontab

`-i` prompt before deleting

`-n <host>` set host in cluster to run users' crontabs

`-c` get host in cluster to run users' crontabs

`-x <mask>` enable debugging

To perform start/stop/restart on `crond` service:

```
/etc/init.d/crond start
```

Cron doesn't need to be restarted when crontab file is modified, it examines the modification time on all crontabs and reload those which have changed.

To verify the current crond status:

```
/etc/init.d/crond status
```

To check current cron jobs running with the following command to list all crontabs:

```
crontab -l
```

To edit or create a custom crontab file:

```
crontab -e
```

This opens a personal cron configuration file. Each line can be defined as one command to run. The following format is used:

```
minute hour day-of-month month day-of-week command
```

For example, append the following entry to run a script every day at 3 am:

```
0 3 * * * /etc/config/backup.sh
```

Save and close the file.

## Initial Provisioning via USB Key

Also known as “ZTP over USB”, this feature allows provisioning an unconfigured (factory erased) unit from a USB storage device like a thumb drive.

The USB device must contain a filesystem recognized by the OM (currently FAT32 or ext4) with a file named manifest.og in the root directory. This file specifies which provisioning steps will be done. An article with a partial description of the file format is here:

<https://opengear.zendesk.com/hc/en-us/articles/115002786366-Automated-enrollment-using-USB>

The USB device can be inserted any time (before or after power is applied to the unit) and as long as the unit is unconfigured, the ZTP over USB process will be triggered. Here “unconfigured” has the same meaning as for ZTP: no changes made to the ogconfig data store.

**Note:** Setting the root password on first log in counts as a config change.

The following manifest.og keys are implemented. This provides image installation, Lighthouse enrollment, and arbitrary script execution:

- # manifest.og contains <key>=<value> pairs. Recognized keys are:
- # image : Firmware image file name on the USB device's filesystem that will be flashed after boot once the image is validated
- # script : Configuration script to run
- # address : Primary Lighthouse address to enroll with
- # api\_port : Optional port to use for the primary address when requesting enrollment



# external\_endpoints : List of additional "address:port" endpoints to fall back to when enrolling

# password : LH global or bundle enrollment password

# bundle : Name of LH enrollment bundle
















## EULA and GPL

The current Opengear End-User License Agreement and the GPL can be found at <http://opengear.com/eula>.

## UI Button Definitions

The table below provides a definition of the button icons used in the UI.

Button Icon	Definition
	Edit button
	Add item (eg. SNMP Manager)
 	VLAN interface or create VLAN interface.
 	Bonded interfaces or create new bond
 	Bridged interfaces or create new bridge
	Standard network interface
	Cellular interface
	Interface with bridge
	Interface with bond
	Bin widget. <b>Delete</b> selected object.

---

UI BUTTON DEFINITIONS	191
-----------------------	-----