



# Operations Manager

## User Guide

21.Q3 November 2021





<b>Contents</b> .....	<b>2</b>
<b>Copyright ©</b> .....	<b>9</b>
<b>Safety &amp; FCC Statement</b> .....	<b>10</b>
Safety Statement .....	10
FCC Warning Statement .....	10
<b>About This User Guide</b> .....	<b>12</b>
<b>Installation And Connection</b> .....	<b>13</b>
Power Connection .....	14
Dual AC Supply .....	16
SNMP Alerts for Power-related Events .....	17
SNMP Alert Configuration .....	17
Device Status LEDs .....	18
Connecting to the Network .....	20
Serial Connection .....	21
Cellular Connectivity .....	22
Installing A New SIM Card .....	22
Reset and Erase .....	23
<b>Initial Settings</b> .....	<b>24</b>
Default Settings .....	25
Using the Web GUI .....	26
Management Console Connection via CLI .....	28
Accessing the Web GUI CLI Terminal .....	28
Change the Root Password .....	29



Disable a Root User .....	31
Change Network Settings .....	32
<b>MONITOR Menu .....</b>	<b>36</b>
System Log .....	37
LLDP CDP Neighbors .....	38
Triggered Playbooks .....	39
<b>ACCESS Menu .....</b>	<b>40</b>
Local Terminal .....	41
Access Serial Ports .....	42
Quick Search .....	42
Access Using Web Terminal or SSH .....	43
Serial Port Logging .....	43
<b>CONFIGURE Menu .....</b>	<b>45</b>
Configure Serial Ports .....	46
Edit Serial Ports .....	47
Autodiscovery .....	49
Local Management Consoles .....	51
Lighthouse Enrollment .....	53
Manual Enrollment Using UI .....	54
Manual Enrollment Using the CLI .....	55
Playbooks .....	56
Create Or Edit a Playbook .....	56
PDUs .....	61
Add and Configure a PDU .....	61
PDU Operation .....	63
SNMP Alerts .....	64
SNMP Alerts System - Temperature, Authentication, Configuration .....	65

Temperature .....	65
Configure SNMP System Temperature Alerts .....	65
Authentication .....	67
Configuration .....	67
SNMP Alerts Power .....	68
Configure Power Alerts .....	68
SNMP Alerts Networking (Connection Status) .....	70
Configure Signal Strength Alerts .....	70
Network Connections .....	72
Network Interfaces .....	73
DNS Configuration .....	74
Configure DNS via the Web UI .....	74
Configure DNS via the Command Line .....	75
Dual SIM .....	77
Display SIM Status and Signal Strength .....	77
Installing A New SIM Card .....	79
Select The Active SIM (Manual Failover Mode) .....	80
Select The Primary SIM (Automatic Failover Mode) .....	81
Dual SIM Automatic Failover .....	83
Failover Modes .....	85
Activate or Configure Automatic Failover .....	86
Cellular Interface Policy Settings .....	87
Network Aggregates - Bonds and Bridges .....	89
Bridges .....	89
Bonds .....	92
Spanning Tree Protocol .....	96
Enable STP in a Bridge .....	97
Bridge With STP Enabled - UI .....	97
Bridge With STP Enabled - OGCLI .....	97
Bridge With STP Disabled - OGCLI .....	98
IPsec Tunnels .....	99

Create, Add or Edit IPsec Tunnels .....	99
Static Routes .....	104
Configure Static Routes .....	105
Managing Static Routes via Command Line .....	106
<b>Network Resilience .....</b>	<b>108</b>
Out Of Band Failover .....	109
Enable Out-of-Band Failover .....	109
Dormant DNS on Failover Interface .....	110
OOB Failover Types & Failover Behavior .....	111
IP Passthrough .....	113
<b>User Management .....</b>	<b>115</b>
Groups .....	116
Create a New Group .....	116
Edit an Existing Group .....	118
Local Users .....	120
Create a New User With Password .....	121
Create a New User With No Password (Remote Authentication) .....	122
Modify An Existing User Account With Password .....	122
Manage SSH Authorized Keys for a User Account .....	123
Delete a User's Account .....	124
Remote Authentication .....	125
Configure RADIUS Authentication .....	126
Configure TACACS+ Authentication .....	127
Configure LDAP Authentication .....	128
Local Password Policy .....	130
Set Password Complexity Requirements .....	131
Set Password Expiration Interval .....	132
Password Policy Implementation Rules .....	133
<b>Services .....</b>	<b>135</b>
Brute Force Protection .....	136



Configure Brute Force Protection .....	136
Viewing Current Bans .....	137
Managing Brute Force Protection via Command Line .....	137
HTTPS Certificate .....	139
Network Discovery Protocols .....	141
File Server .....	143
Enable TFTP Service .....	143
Update The TFTP Service Storage Location .....	144
Routing .....	146
Dynamic Routing .....	146
Static Routing (via the ogcli) .....	147
SSH .....	149
Unauthenticated SSH to Serial Ports .....	150
Enable Unauthenticated SSH .....	150
Enable SSH .....	151
Enable/Disable .....	151
Connecting Directly to Serial Ports .....	152
Feature Persist .....	153
Properties and Settings .....	153
Syslog .....	156
Add a New Syslog Server .....	156
Global Serial Port Settings .....	157
Edit or Delete an Existing Syslog Server .....	158
Session Settings .....	159
Firewall .....	160
Firewall Management .....	161
Firewall Zone Settings .....	162
Port Forwarding .....	162
Manage Custom Rules .....	163
Interzone Policies .....	164
Create an Interzone Policy .....	164



Edit or Delete an Interzone Policy .....	166
Customized Zone Rules .....	166
<b>Date &amp; Time .....</b>	<b>167</b>
Time Zone .....	168
Manual Settings .....	169
Automatic Settings .....	170
<b>System .....</b>	<b>171</b>
Check System Details .....	171
Administration .....	172
Factory Reset .....	173
Reboot .....	174
Export Configuration .....	175
Export Configuration via Web UI .....	175
Export Configuration via ogcli .....	176
Control The Export Of Sensitive Data .....	176
Lighthouse Node Backup .....	177
Import Configuration .....	178
Restore Configuration Via Web UI .....	178
Import Configuration via ogcli .....	180
System Upgrade .....	181
Upgrade Via Fetch From Server .....	182
Upgrade Via Upload .....	182
<b>SNMP .....</b>	<b>183</b>
SNMP Service .....	184
SNMP Alert Managers .....	185
Multiple SNMP Alert Managers .....	186
Create or Delete an SNMP Manager .....	186
New SNMP Alert Manager Page Definitions .....	187



<b>Advanced Options</b> .....	<b>189</b>
Communicating With The Cellular Modem .....	190
Opengear CLI Guide .....	192
Getting Started with ogcli .....	192
Basic Syntax .....	193
Common Configuration Examples .....	199
Docker .....	206
Cron .....	207
Options: .....	207
Initial Provisioning via USB Key .....	209
EULA and GPL .....	211
<b>UI Button Definitions</b> .....	<b>212</b>





## Copyright ©

Opengear Inc. 2021. 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 21.Q2 May 2021 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 16](#) and ["SNMP Alerts Power" on page 68](#).

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

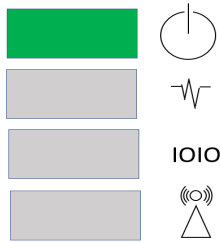
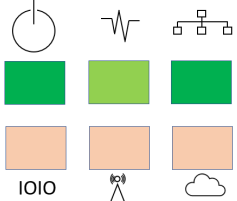
## Dual AC Supply

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.

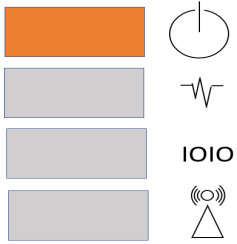
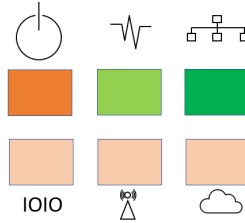
### LED Power Status Indicator

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 amber 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 68](#).

## 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 failover 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 70](#)

["SNMP Alerts Power" on page 68](#)



## 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 Settings

This section provides step-by-step instructions for the initial settings on your OPERATIONS MANAGER.

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

- ["Default Settings" on the next page](#)
- ["Management Console Connection via CLI" on page 28](#)
- ["Change the Root Password" on page 29](#)
- ["Disable a Root User" on page 31](#)
- ["Change Network Settings" on page 32](#)
- For Configure Serial Ports (see ["Configure Serial Ports" on page 46](#))

**Tip:** There is also a Quick Start Guide to assist with easy setup of the Operations Manager. The QSG is available at:  
<http://ftp.opengear.com/download/quickstart/om2200/OMQSG.pdf>



## Default Settings

**Tip:** See also the Quick Start Guide at:

<http://ftp.opengear.com/download/quickstart/om2200/OMQSG.pdf>

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

### Serial Port Settings

The default settings for the serial ports on a new device are:

“Console server” mode, 9600, 8N1, X2 (Cisco straight) pinout; the escape character is “~” .

### Browser Web GUI

The OM offers a Web GUI via web browser that supports HTML5.

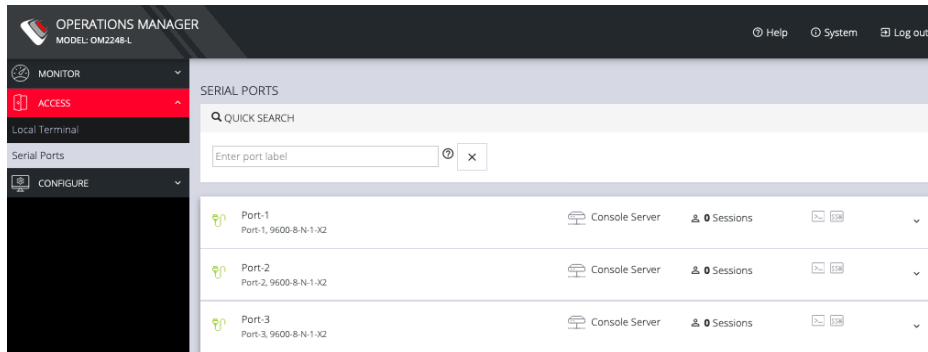
1. Type `https://192.168.0.1` in the address bar. HTTPS is enabled by default.
2. Enter the default username and password

**Username:** root

**Password:** default

3. After the first successful log-in you are required to change the root password.
4. After log-in the Web GUI is available. Check system details in the top right-hand side of the Web GUI.
5. 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.



## Using the Web GUI

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

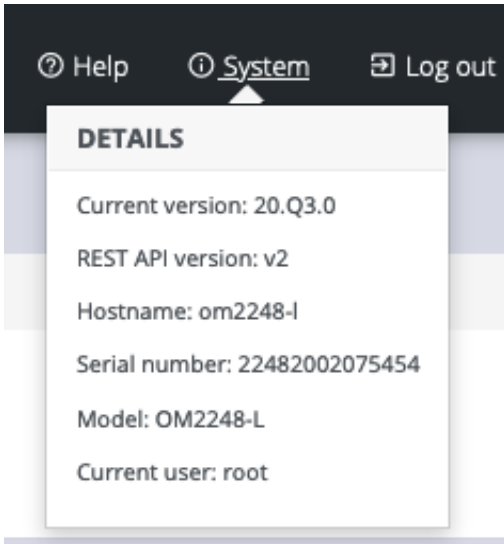


Light mode changes the user interface to display mostly light colors. This is the default UI setting. Dark mode changes the user interface to display mostly dark colors, reducing the light emitted by device screens.

The Web GUI 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**.



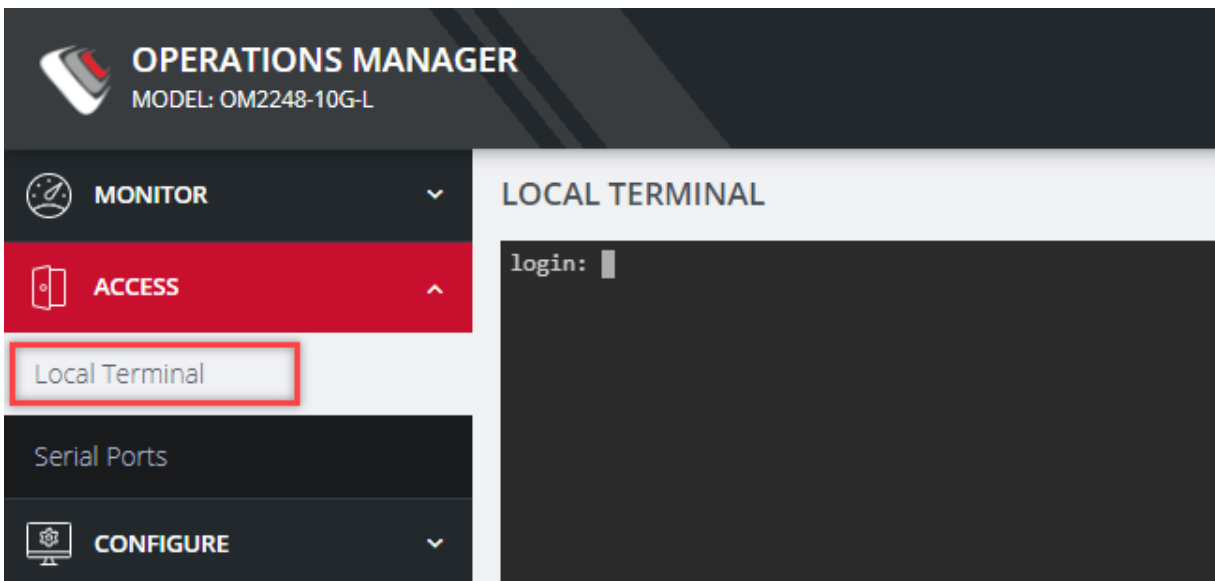
## Management Console Connection via CLI

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 prompt.

### Accessing the Web GUI CLI Terminal

An alternative CLI terminal is provided within the Web GUI. 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

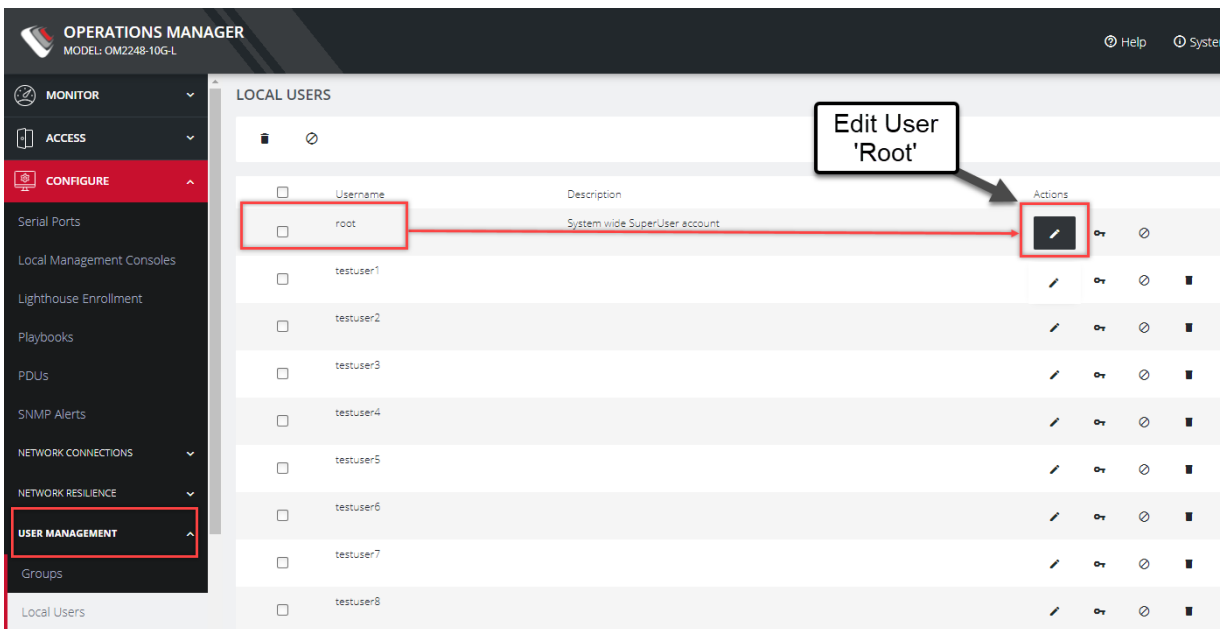
[CONFIGURE](#) > [User Management](#) > [Local Users](#) > [Edit User](#)

For security reasons, only the root user can initially log in to the appliance. Upon initial login 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 120

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

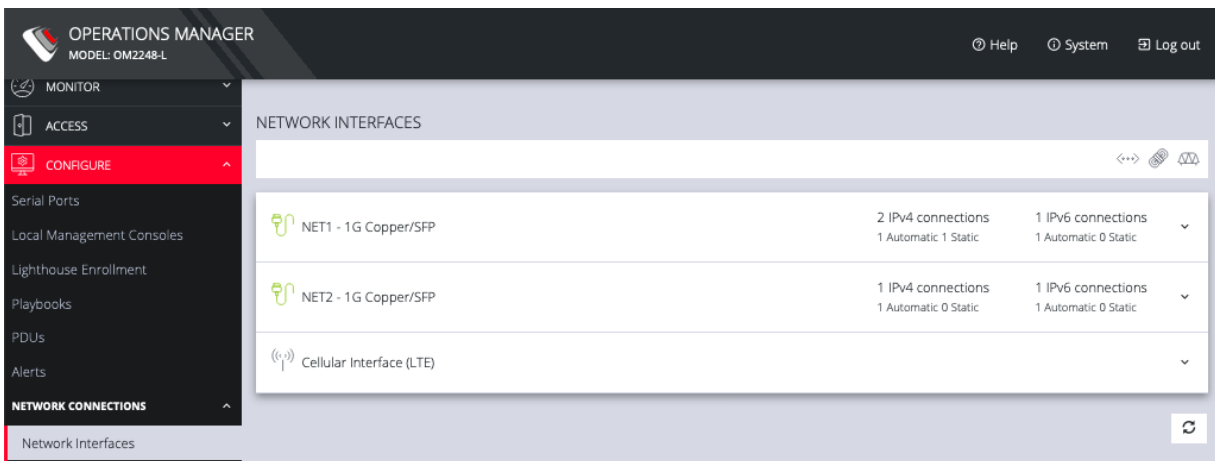
[CONFIGURE](#) > [Network Connections](#) > [Network Interfaces](#)

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

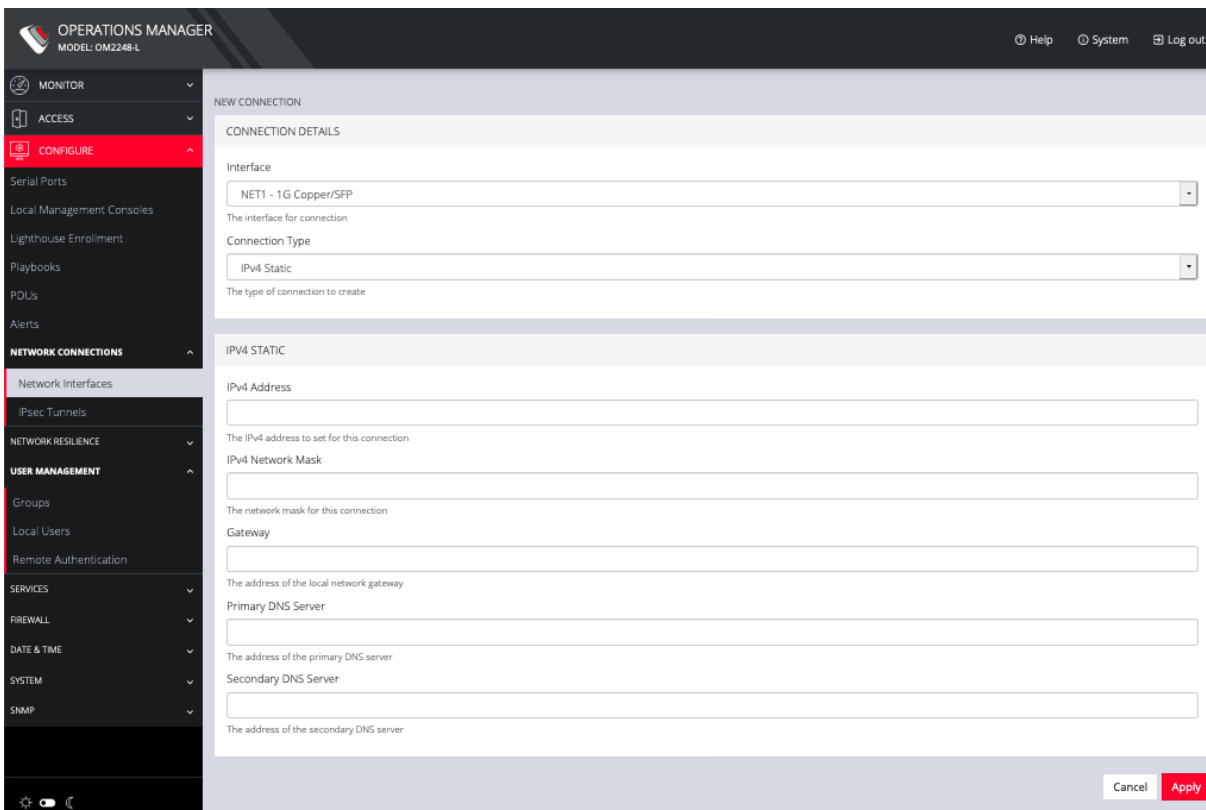
To add a new connection:

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.





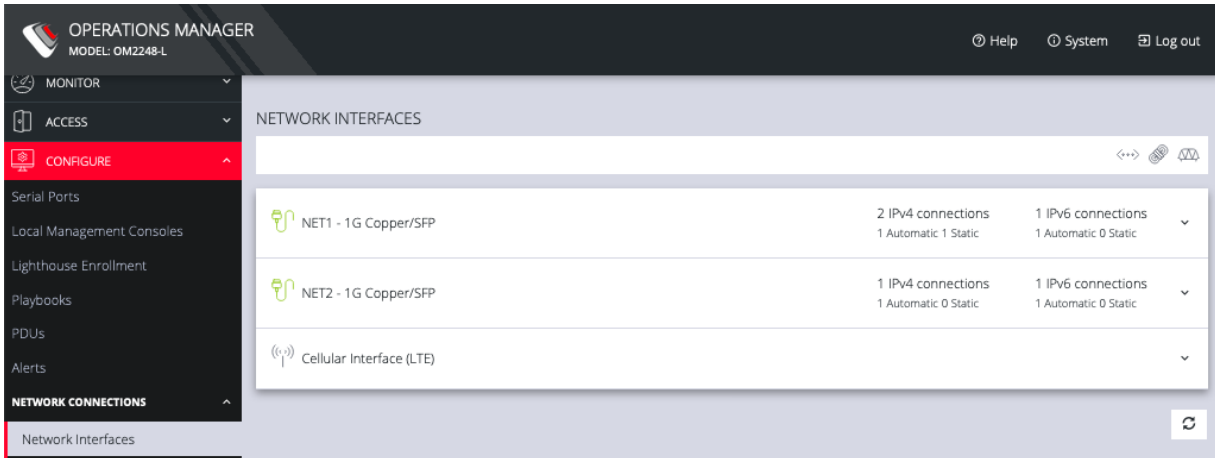
4. Select the **Interface** and **Connection Type** for your new connection.
5. The form on the bottom part of the page will change based on the **Connection Type** you choose. Enter the necessary information and click **Apply**.

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

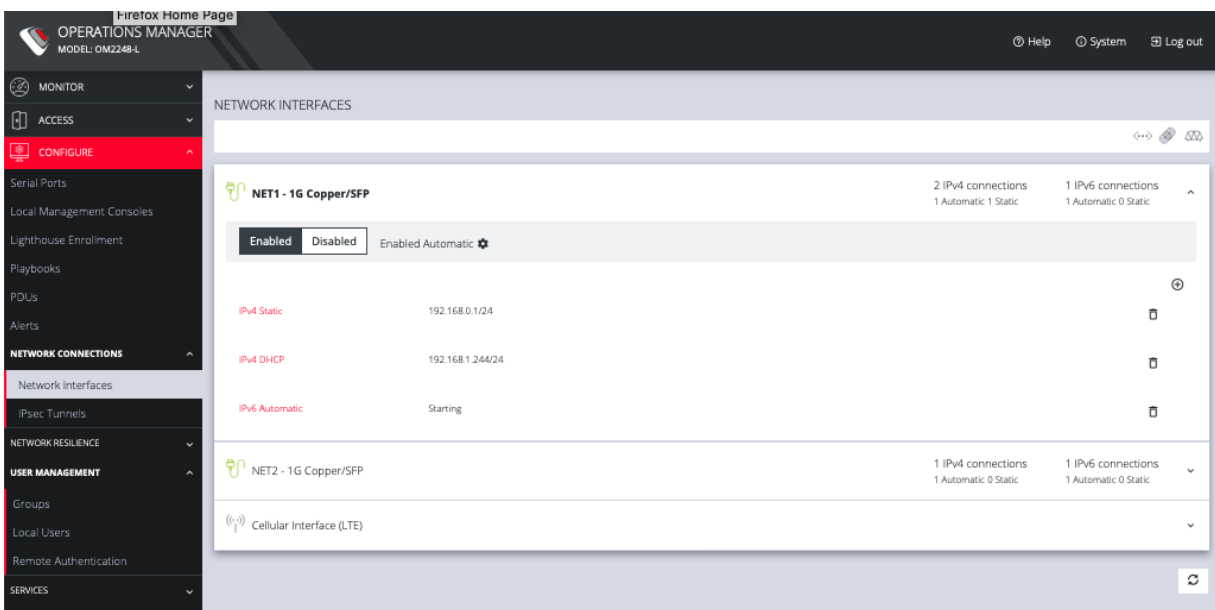
**Note:** If you experience packet loss or poor network performance with the default auto-negotiation setting, try changing the Ethernet Media settings on the OPERATIONS MANAGER and the device it is connected to. In most cases, select 100 megabits, full duplex. Make sure both sides are set identically.

To change the Ethernet Media Type:

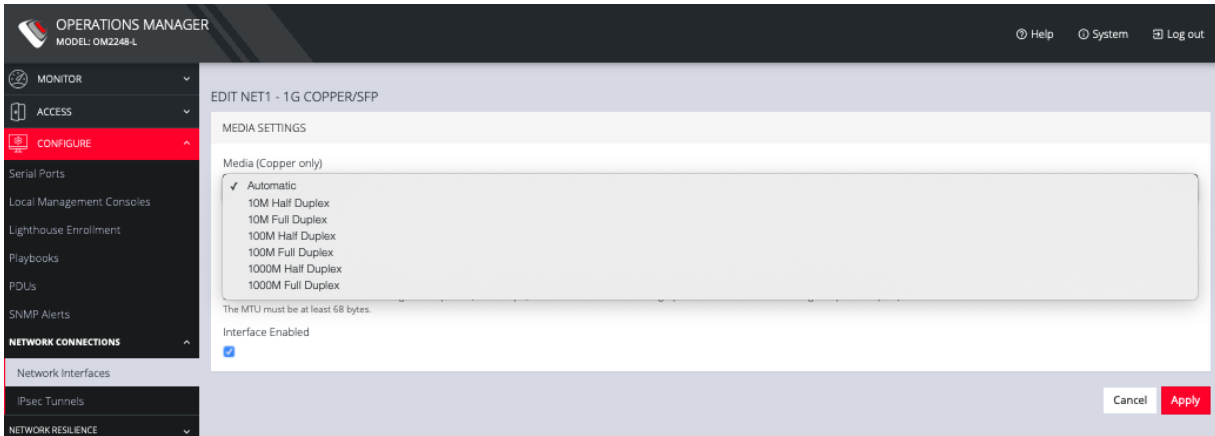
1. Click **CONFIGURE** > **Network Connections** > **Network Interfaces**



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.

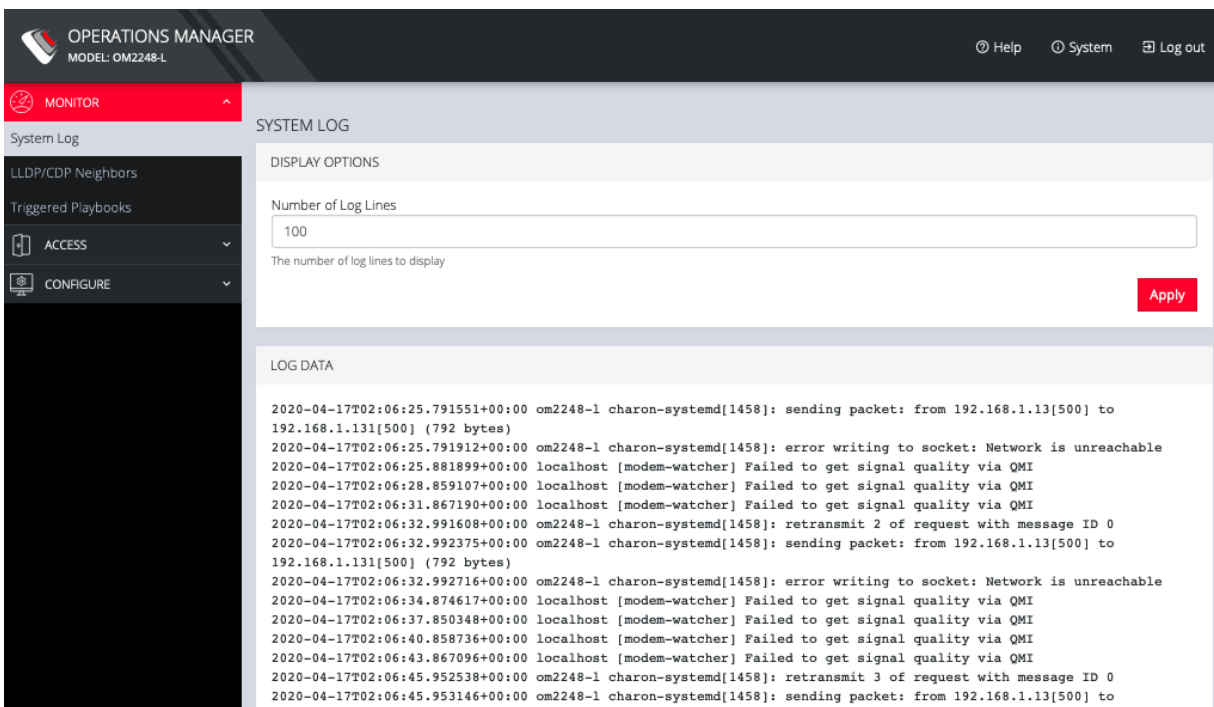
- System Log
  - Details of the system activity log, access and communications events with the server and with attached serial, network and power devices.
- LLDP/CDP Neighbors
  - Details of the LLDP/CDP Neighbors that are displayed when enabled for a connection.
- Triggered Playbooks
  - Monitoring 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 network packets and modem-related errors.

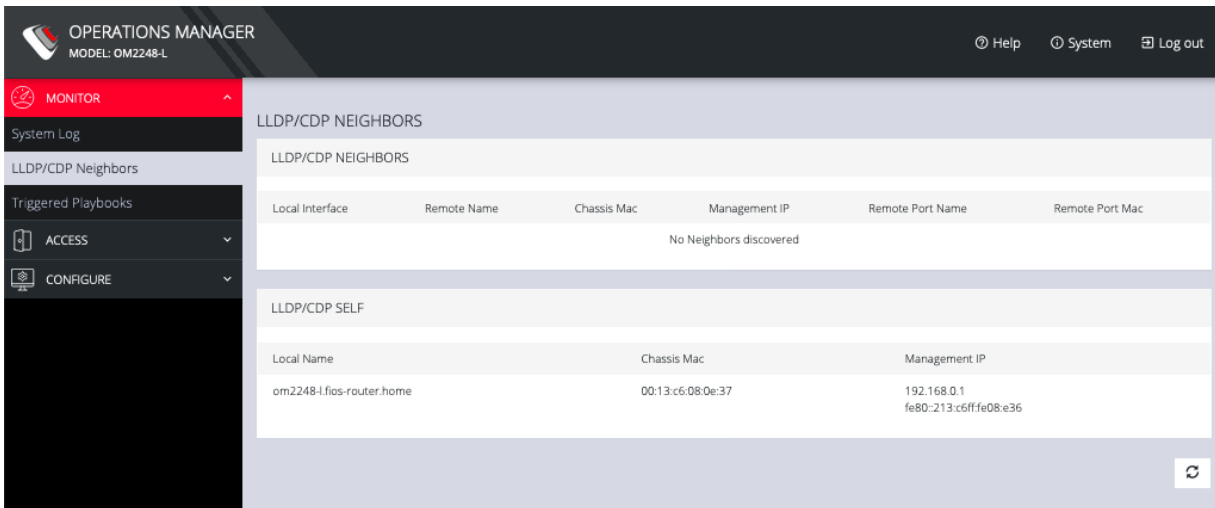
```
2020-04-17T02:06:25.791551+00:00 om2248-1 charon-systemd[1458]: sending packet: from 192.168.1.13[500] to 192.168.1.131[500] (792 bytes)
2020-04-17T02:06:25.791912+00:00 om2248-1 charon-systemd[1458]: error writing to socket: Network is unreachable
2020-04-17T02:06:25.881899+00:00 localhost [modem-watcher] 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.



The screenshot shows the OPERATIONS MANAGER interface for a device with model OM2248-L. The left sidebar contains a menu with 'MONITOR' selected, and sub-items for 'System Log', 'LLDP/CDP Neighbors', 'Triggered Playbooks', 'ACCESS', and 'CONFIGURE'. The main content area displays the 'LLDP/CDP NEIGHBORS' page. It features two tables: 'LLDP/CDP NEIGHBORS' which is currently empty with the message 'No Neighbors discovered', and 'LLDP/CDP SELF' which shows the local device's information.

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

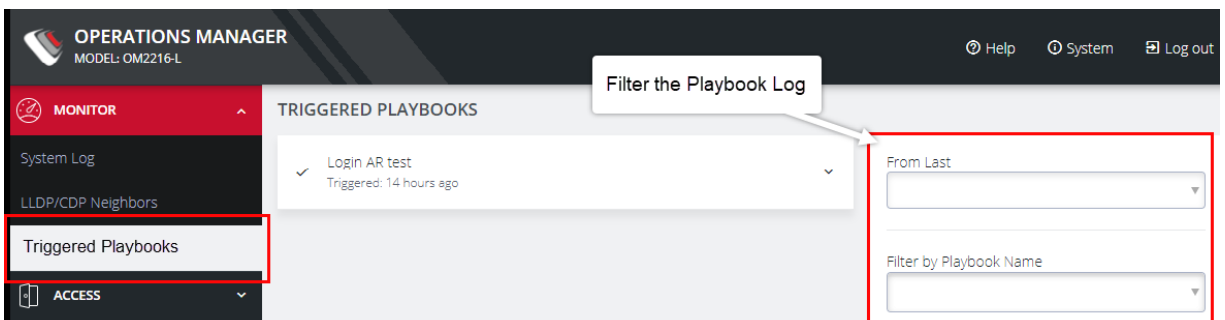
Local Name	Chassis Mac	Management IP
om2248-l.fios-router.home	00:13:c6:08:0e:37	192.168.0.1 fe80::213:c6ff:fe08:e36

## Triggered Playbooks

[MONITOR > Triggered Playbooks](#)

For information on creating **Playbooks**, see the [Playbooks](#) topic in this User Guide.

To monitor current **Playbooks**, click on **Monitor > Triggered 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.

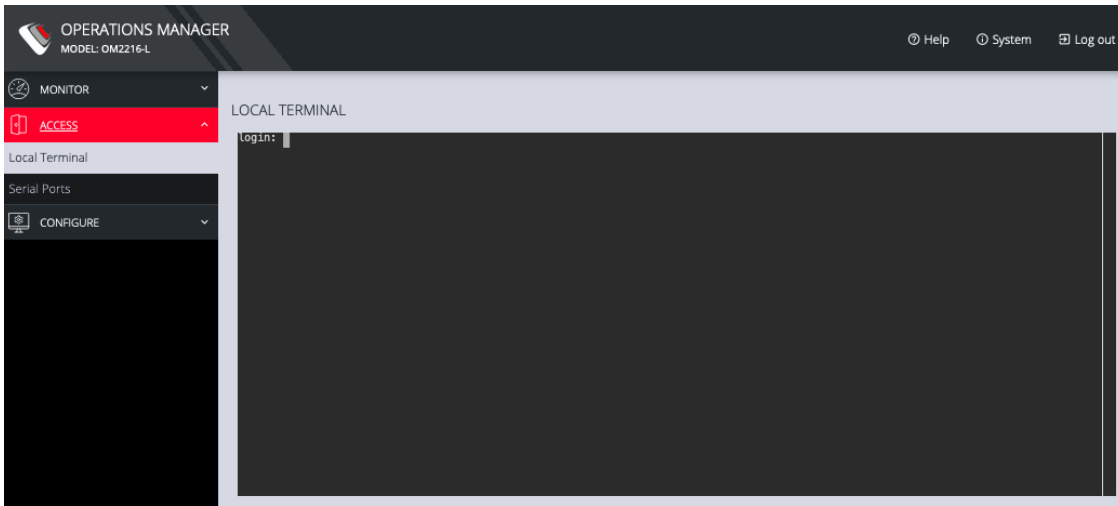


# Local Terminal

## 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 login prompt, enter a username and password.
3. 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.

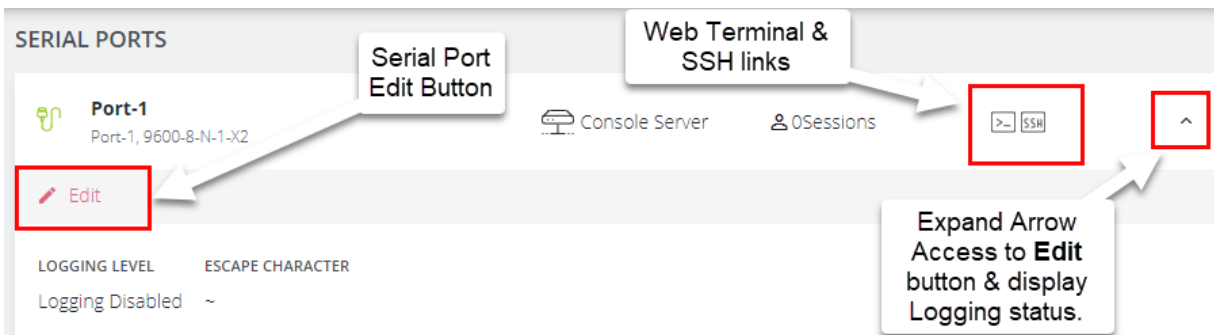
**Tip:** The default for the CLI session timeout is “never” (value of 0), however, the Web session timeout defaults to 20min. The web session time-out will kill the CLI session even though the CLI session itself is set to “never”.

## Access Serial Ports

[ACCESS > Serial Ports](#)

**Tip:** Ensure you are on the **ACCESS > Serial Ports** page and not the similar **CONFIGURE > Serial Ports** page.

The **ACCESS > Serial Ports** page allows you to quickly locate and access specific ports via Web Terminal or SSH link shown in the image below.



Click the **Expand arrow** to the right of the port to see the Port Logging status or access the port **Edit** button, which is a link to the **CONFIGURE > Serial Ports** page.

### Quick Search

To find a specific port by its port label, use the **Quick Search** form at the top-right of the **ACCESS > Serial Ports** page.

Ports have default numbered labels. You can edit the port label for a given serial port under **CONFIGURE > Serial Ports**. Click the **Edit** button to open the **EDIT SERIAL PORT** page.

## Access Using Web Terminal or SSH

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

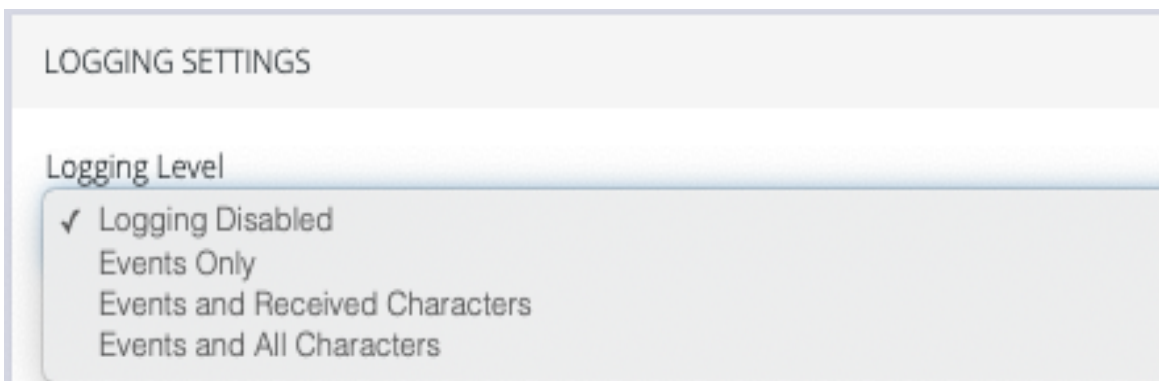
1. Locate the particular port on the **ACCESS > Serial Ports** page and click the expand arrow.
2. Click the **Web Terminal** or SSH link for the particular port.
  - Choosing **Web Terminal** opens a new browser tab with the terminal.
  - Choosing **SSH** opens an application you have previously associated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

## Serial Port Logging

The port logging facility and severity associated with the serial port logs is controlled and set at the **Configure > Services > Syslog > Global Serial Port Settings** page.

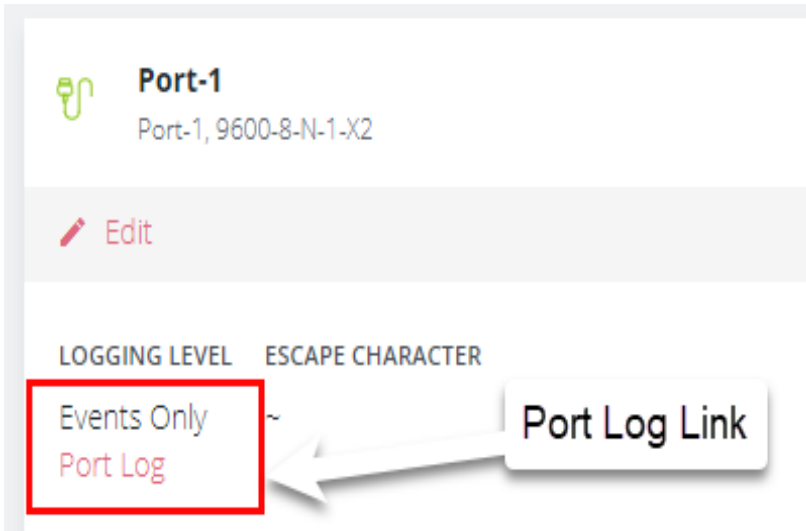
There is a separate setting to enable sending of serial port logs to remote side.

**Note:** Serial port logging is disabled by default. The logging level for each serial port is set at Logging Settings in **Configure > Serial Ports > Edit** .



## Display Port Logs

**Tip:** The log is accessed by clicking the **Port Log** link on the **ACCESS > Serial Ports** page. The link is only available when port logging is enabled.



**Port-1**  
Port-1, 9600-8-N-1-X2

Edit

LOGGING LEVEL	ESCAPE CHARACTER
Events Only	~
Port Log	

Port Log Link



## CONFIGURE Menu

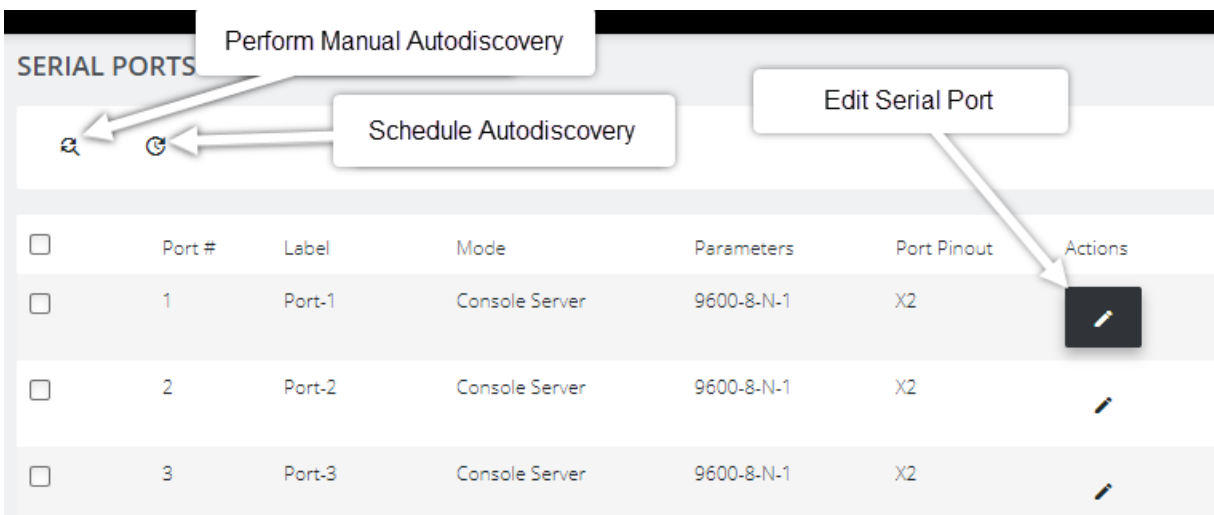
This section provides step-by-step instructions for the menu items under the CONFIGURE menu.




## Configure Serial Ports

[CONFIGURE > Serial Ports](#)

**Tip:** Ensure you are on the **CONFIGURE > Serial Ports** page and not the similar **ACCESS > Serial Ports** page.

Navigate to **CONFIGURE > Serial Ports**; a list of serial ports is displayed. On this page you can configure and edit specific ports. Click the **Edit** button (pencil icon) to the right of the port to display the port editing page.



<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	

## Edit Serial Ports

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 is displayed.

Edit Serial Port Properties		
Field	Options	Definition
Label	Default or Custom	The serial port unique identifier. This can be used to locate this port using the <b>Quick Search</b> form on the <b>ACCESS &gt; Serial Ports</b> page.
Mode	Disabled Console Server Local Console	<b>Console Server</b> mode allows access to a downstream device via its serial port. <b>Local Console</b> mode allows access to the NGCS device's console through a serial port.
Port Pinout	Cisco Rolled Cisco Straight	Select pin-out type depending on the type of device or host to be connected via the port.
Baud Rate	Baud rate	Select the Baud rate expected for this port. From 50 to 230,400 bps.
Data Bits	Integer	The data bit length for character.
Parity	None, Odd, Even, Mark, Space.	The parity type for character.
Stop Bits	1, 1.5, 2	The Stop bit length used in character.
Escape Character	~	The character used for sending OOB Shell commands.

LOGGING SETTINGS		
Logging Level	Disabled Events Only Events & Received Characters Events & All Characters	Specify the level of detail you require in the logs. Logs may also be sent to a Syslog server. Other settings to consider are:  GLOBAL SERIAL PORT SETTINGS” under Services > "Remote Syslog" on page 1  “Send Serial Port Logs” under Services > Syslog > Edit Syslog Server
PORT IP ALIASES		
IP Address	Alias IP Address and interface type.	Allocate an IP address for dedicated access to a specific serial port.

### Assigning unique IP addresses for each console port

**Note:** For further information about assigning unique IP addresses for each console port see the Zendesk article [Assigning Unique IP Addresses For Each Console Port](#) .



## Autodiscovery

The Autodiscovery feature attempts to discover the host name of connected devices, this uses the hostname to set it as the port label of each serial port. This can save the need to manually provide hostnames during device setup.

Autodiscovery has been enhanced to discover baud rate and pinout (X1 / X2). The UI has been updated to indicate if ports are scheduled for discovery.

The **Serial Ports** page also allows you perform an Autodiscovery on selected ports. Autodiscovery of console ports attempts to set the port label by setting the baud rate to various rates (in the following order): 9600, 115200, 38400, 19200, and 57600.

**Tip:** Autodiscovery on other Baud rates may be done by manually running the `port_discovery` script from the Web Terminal.

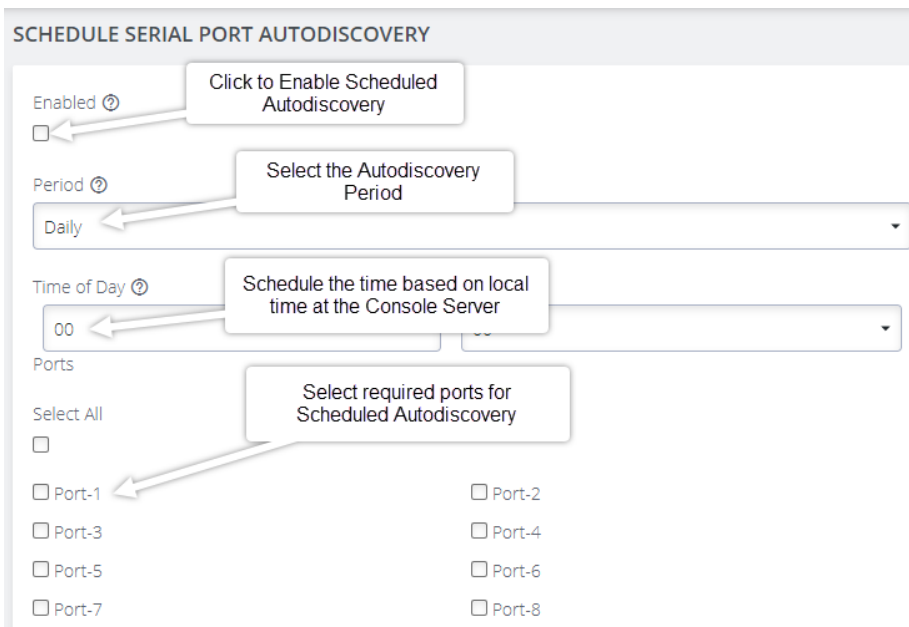
Autodiscovery may be done manually by clicking the **Perform Autodiscovery** button.

## Schedule Autodiscovery

Autodiscovery can be scheduled periodically as required by clicking the **Schedule Autodiscovery** button.

The **Schedule Autodiscovery** page allows you to select the ports and specify a time and period for port detection to run.

*The Serial Port Autodiscovery Page:*



The screenshot shows the 'SCHEDULE SERIAL PORT AUTODISCOVERY' configuration page. It includes the following elements:

- Enabled:** A checkbox that is currently unchecked. A callout box points to it with the text 'Click to Enable Scheduled Autodiscovery'.
- Period:** A dropdown menu currently set to 'Daily'. A callout box points to it with the text 'Select the Autodiscovery Period'.
- Time of Day:** A dropdown menu currently set to '00'. A callout box points to it with the text 'Schedule the time based on local time at the Console Server'.
- Ports:** A section titled 'Ports' containing a 'Select All' checkbox and eight individual checkboxes labeled 'Port-1' through 'Port-8'. A callout box points to this section with the text 'Select required ports for Scheduled Autodiscovery'.

## Local Management Consoles

**Note:** Applies to OM2200 Devices only. Not applicable to OM1200.

### [CONFIGURE > Local Management Consoles](#)

This feature allows administrators to log in and configure the OM via the RJ-45 or USB ports on the device. 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. Navigate to **CONFIGURE > Local Management Consoles**. Here you'll see a list of consoles.
2. Locate the console you want to manage, then, click on the **Edit Management Console Port** button (pencil icon) under **Actions**.
3. On the **Edit Local Management Console** page you can set the parameters for:
  - **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:

1. Click **CONFIGURE > Local Management Consoles**.
2. 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.

Lighthouse central management uses a persistent, public key authenticated SSH tunnels to maintain connectivity to managed console servers.

All network communications between Lighthouse and each console server (e.g. access to the web UI), and the console server's managed devices (e.g. the serial consoles of network equipment), is tunneled through this SSH management tunnel.

The below Zendesk articles and user guide contain further information about Lighthouse Enrollment:

[Manual enrollment using UI or CLI](#)

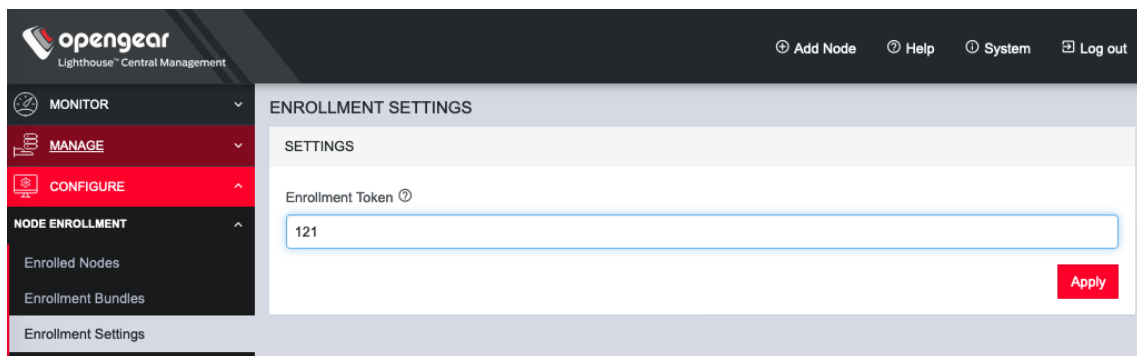
[How do I add Nodes to Lighthouse](#)

[Lighthouse User Guide](#)

## Manual Enrollment Using UI

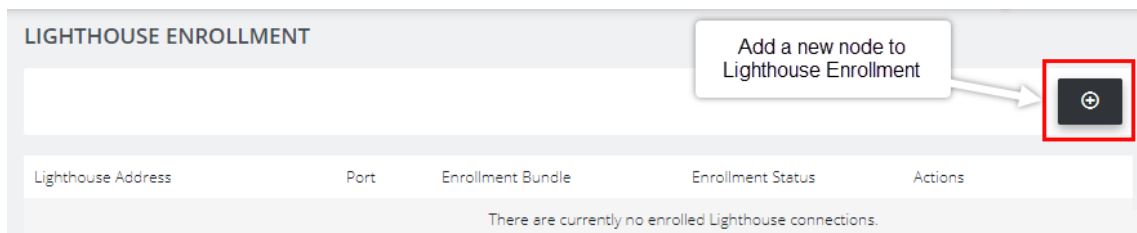
**Note:** To enroll your OPERATIONS MANAGER to a Lighthouse instance, you must have Lighthouse installed and have an enrollment token set in Lighthouse.

1. In Lighthouse. Set an OM enrollment token, click on **CONFIGURE > NODE ENROLLMENT > Enrollment Settings** page, and enter an **Enrollment Token**.

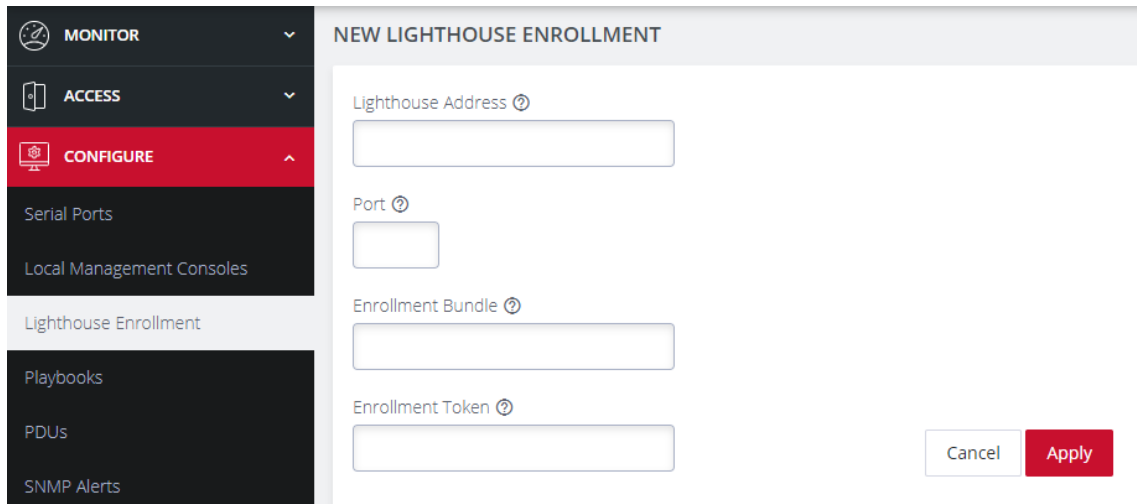


**Tip:** The same token will be entered in the NEW LIGHTHOUSE ENROLLMENT page of the OM.

2. Enroll your OPERATIONS MANAGER in this Lighthouse instance:  
Click **CONFIGURE > Lighthouse Enrollment**
2. Click on the **Add Lighthouse Enrollment** button on the top-right of the page.  
The **New Lighthouse Enrollment** page opens.



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 about Bundling).



The screenshot shows the 'NEW LIGHTHOUSE ENROLLMENT' form. On the left is a navigation menu with 'CONFIGURE' selected. The form fields are: 'Lighthouse Address' (text input), 'Port' (text input), 'Enrollment Bundle' (text input), and 'Enrollment Token' (text input). At the bottom right are 'Cancel' and 'Apply' buttons.

4. Click the **Apply** button. A flag will confirm the enrollement.

**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.

## Manual Enrollment Using the CLI

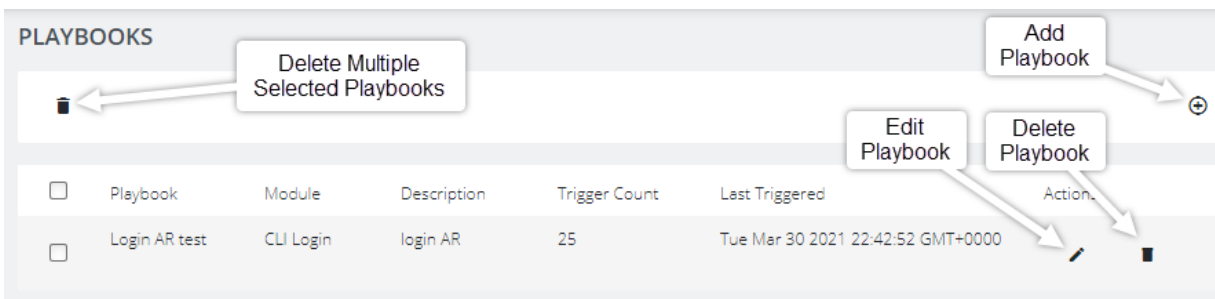
For complete instructions on Lighthouse Enrollment vias the CLI please refer to this link: [Manual enrollment using UI or CLI .](#)

## Playbooks

[CONFIGURE > Playbooks](#)

**Playbooks** are configurable systems that periodically check if a user-defined **Trigger** condition has been met. Playbooks can be configured to perform one or more specified **Reactions** when a specific trigger event occurs.

*The Playbook Landing Page:*



### Create Or Edit a Playbook

[CONFIGURE > Playbooks > Add Playbook](#)

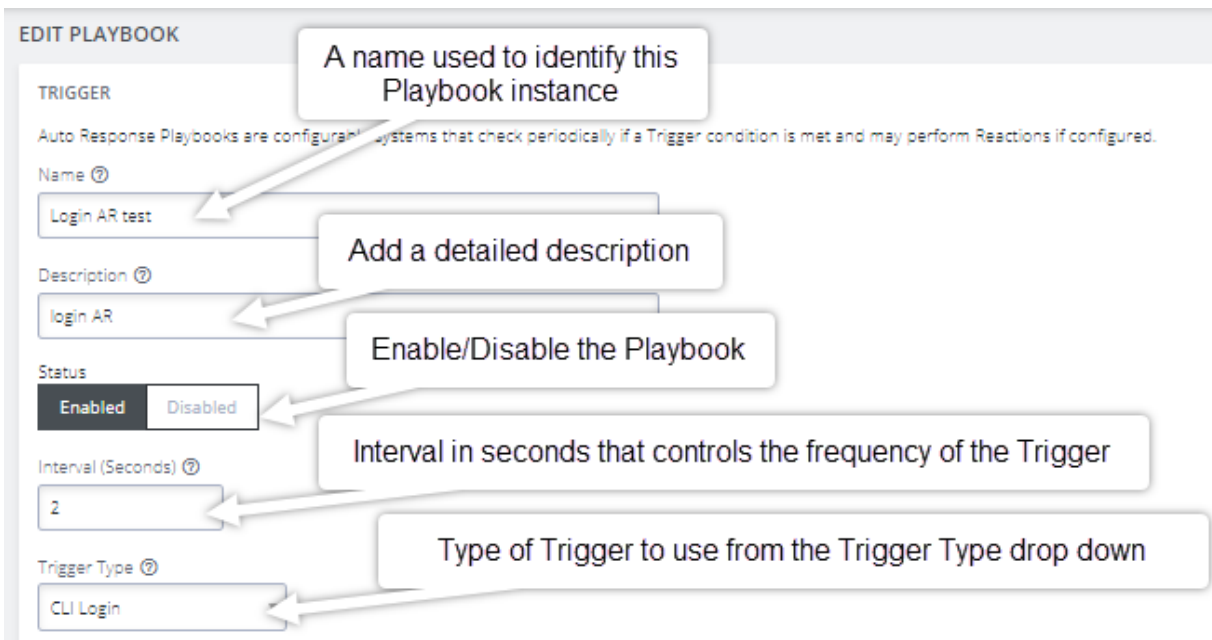
To create a new Playbook:

Navigate to the **Configure > Playbooks** page.

Click the **Add Playbook** button (top-right) to create a new **Playbook**. The **Edit Playbook** page is displayed. Complete the required Playbook setup information as detailed in the following procedures.



## TRIGGER Section:



**EDIT PLAYBOOK**

**TRIGGER**

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

Name ⓘ  
Login AR test

Description ⓘ  
login AR

Status  
 Enabled  Disabled

Interval (Seconds) ⓘ  
2

Trigger Type ⓘ  
CLI Login

A name used to identify this Playbook instance

Add a detailed description

Enable/Disable the Playbook

Interval in seconds that controls the frequency of the Trigger

Type of Trigger to use from the Trigger Type drop down

1. Enter a unique **Name** for the **Playbook** that reflects its purpose.
2. Add a detailed **Description** that will help others to understand what it does.
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.

**Tip:** See the Trigger Type table on the following page for additional trigger type information.

Trigger Types:

Trigger	Reaction Description
CLI Login	Triggers upon Login or Logout events. Select either or both.
CLI Login Failure	Monitor the terminal and trigger on failed user login attempts.
Cell Connection	Triggered whenever the cellular connection state changes. This Trigger type is only compatible with cellular units.
Cell Message	Triggered when an SMS message that matches the user-defined message pattern. Cellular units only.
Cell Signal Strength	Triggered if the cellular signal strength moves below a user-defined percentage.
Curl	Periodically attempts to perform a HTTP request using curl and triggers the Playbook reaction based on the results.
Custom Command	Periodically runs a custom Shell command and triggers the Playbook reaction upon failure.
Load	Monitors the system load average and triggers the Playbook if it breaches the user-defined acceptable range.
Memory Usage	Triggered if the system memory usage exceeds the user-defined percentage threshold.
Network Settings	Monitors network interfaces for specific attributes and triggers a user-defined reponse when they change.
Ping	Periodically pings an address and triggers a user-defined reponse upon failure.

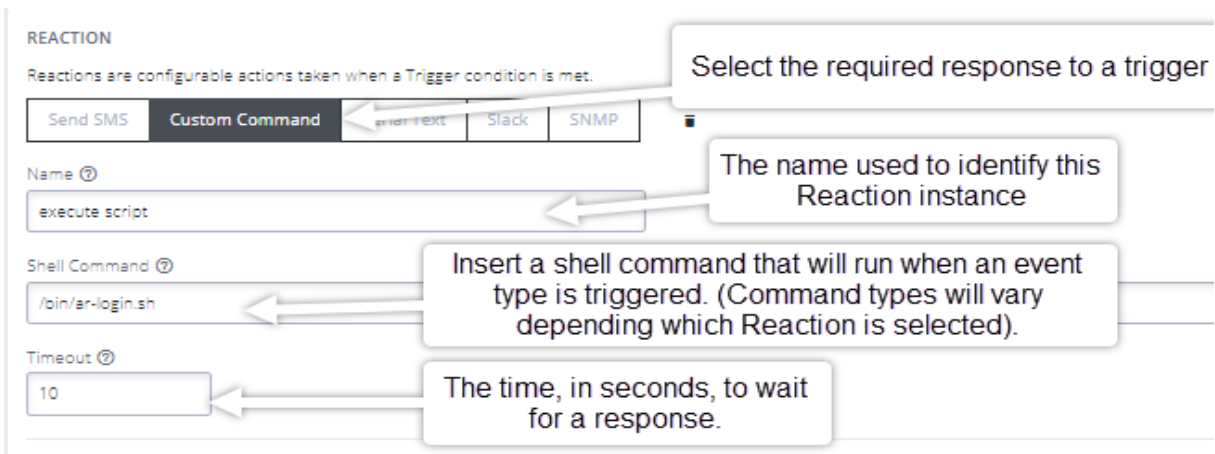
*Continued...*

Trigger	Description
Serial Login	Monitors selected serial ports and triggers a user-defined reaction upon user login and logout events.
Serial Pattern	Monitors serial ports and triggers a reaction when data matching a pattern is received on specific ports.
Serial Signal	Monitors selected serial ports and triggers when signals are changed.

### REACTION Section:

In this section you customise the response to the Trigger that you created.

1. Clicking on each **Reaction** opens a custom screen to provide necessary information.



**REACTION**  
Reactions are configurable actions taken when a Trigger condition is met.

Select the required response to a trigger

Send SMS Custom Command **Smart Text** Slack SNMP

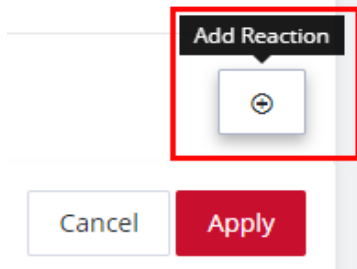
Name  The name used to identify this Reaction instance

Shell Command  Insert a shell command that will run when an event type is triggered. (Command types will vary depending which Reaction is selected).

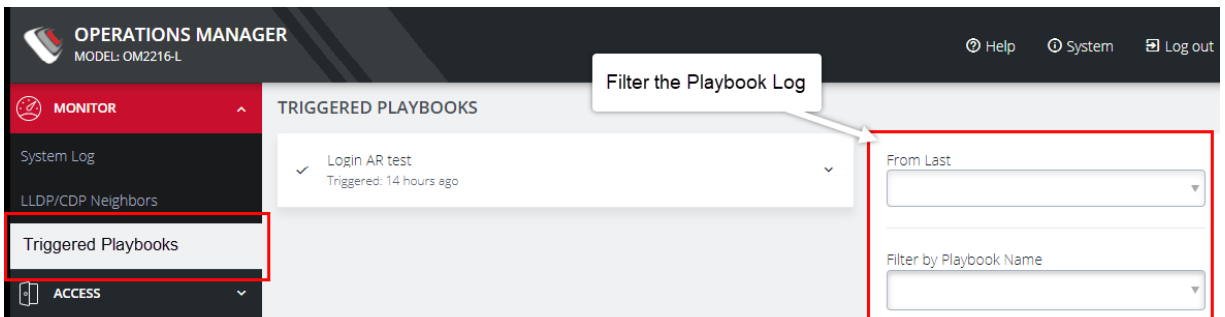
Timeout  The time, in seconds, to wait for a response.

*Continued...*

2. To create additional Reactions, click the **Add Reaction** button.



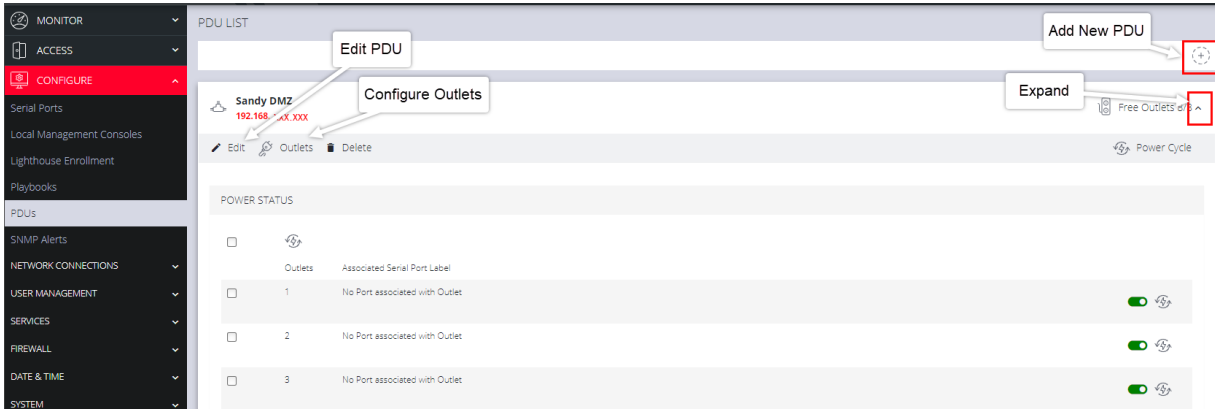
3. When you are finished, click **Apply**. A banner confirms that the Playbook settings are saved, if the Playbook is **Enabled** it is activated.
4. To monitor current **Playbooks**, click on the **Monitor > Triggered Playbooks** menu (shown below). Select the time period if desired and filter by **Name of Playlist** to view any that have been triggered.



# PDU's

## CONFIGURE > PDU's

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



## Add and Configure a PDU

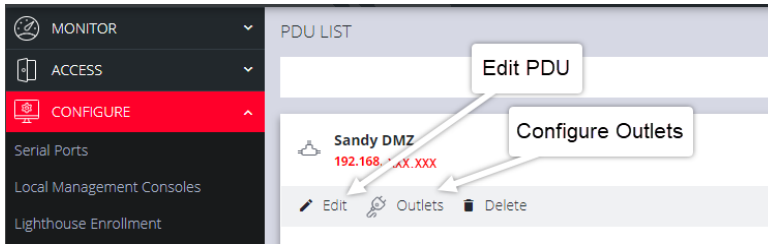
PDU configuration definitions are provided in the on the "[PDU Settings Table](#)" on the next page.

1. In the PDU List page, click the **Add New PDU** button. The **Edit** page opens.
2. Enter a meaningful **Label** that will easily identify this **PDU**.
3. Select the **Monitor** checkbox.
4. Select **Local** or **Remote**.

**Note:** Note that **Local** or **Remote** have different settings forms.

5. Complete the **Local** or **Remote** settings in accordance with the "[PDU Settings Table](#)" on the next page.

- Click on the **Configure Outlets** link, assign a port for each of the PDUs' ports and enter a meaningful name for each outlet.



- When you are finished, click **Apply**. A green banner confirms your settings.

## PDU Settings Table

PDU Settings	
Label	Enter a meaningful label that will easily identify the individual <b>PDU</b> .
Monitor	Click to check this box to monitor the outlet's status.
Mode	Note that ( <b>Local</b> or <b>Remote</b> have different settings forms).
Driver	Select the appropriate driver compatible with this PDU.
Local Mode Only	
Port	The serial port that the PDU is connected to.
Username	Enter the Username to use when connecting.
Password	User password to use when connecting to the device.

The table is continued on the following page...

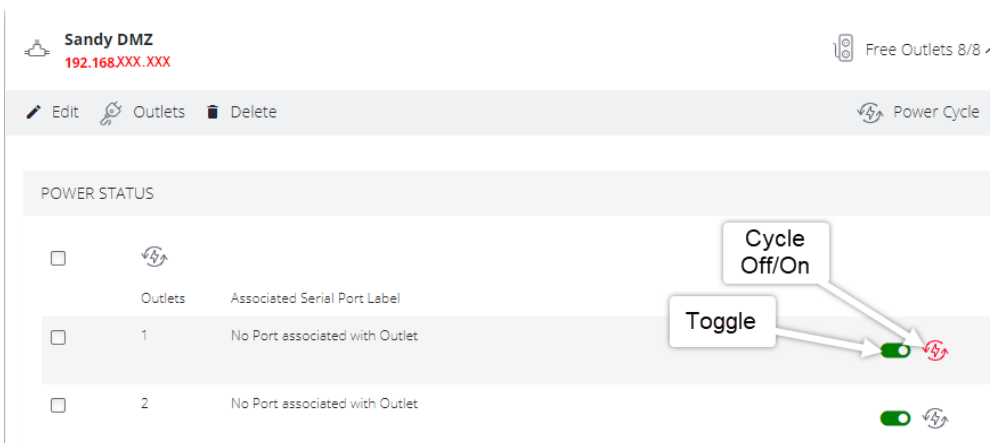
Continued...

Remote Mode Only	
Address	The remote address of the PDU.
SNMP Protocol	Click the drop-down arrow and select the correct transport protocol used to communicate with the PDU. The default value is UDP.
Version	The version of SNMP to use, V1, V2c and V3 are supported. The default value is V1.
Community	Enter a group name authorized to communicate with the device for SNMP versions 1 and 2c.

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

## PDU Operation

After the PDU has been created and configured, PDU operation is simple. For any PDU that has Monitoring set to **Enabled**, the **Toggle** on/off switch will power-on or power-off the PDU, and the **Cycle** button cycles the PDU through a power-down and power-up cycle.



The screenshot shows the configuration page for a PDU named "Sandy DMZ" with IP address "192.168.XXX.XXX". At the top right, it indicates "Free Outlets 8/8". Below the header, there are buttons for "Edit", "Outlets", "Delete", and "Power Cycle". The main section is titled "POWER STATUS" and contains a table with columns for "Outlets" and "Associated Serial Port Label".

Outlets	Associated Serial Port Label
1	No Port associated with Outlet
2	No Port associated with Outlet

At the bottom right of the interface, there are two control buttons: a "Toggle" button (a green switch) and a "Cycle Off/On" button (a circular arrow icon). Arrows from the labels point to these buttons.

## 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 GUI, 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 68 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.

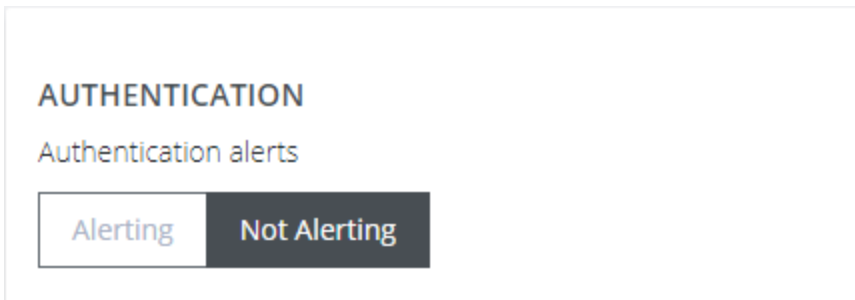
**Tip:** The temperature display is automatically converted to Fahrenheit.

## 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.

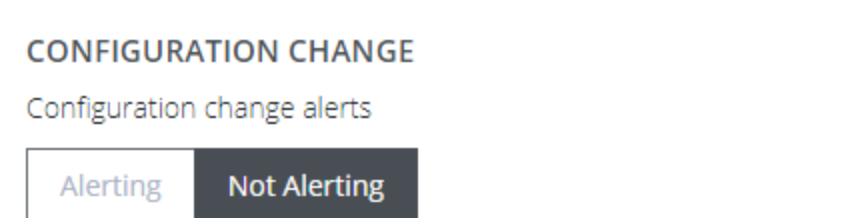


## Configuration

[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

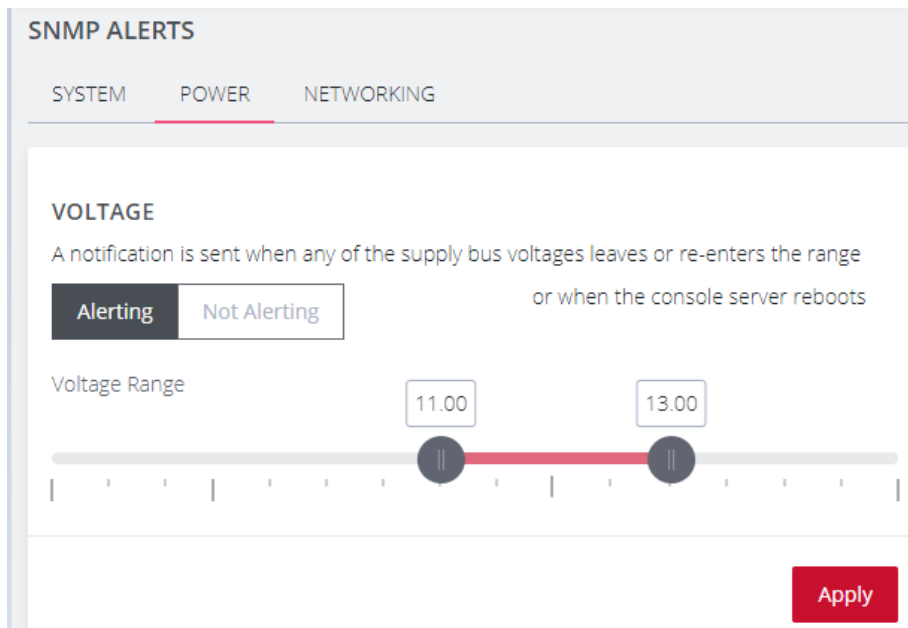
[Configure > SNMP Alerts > Power > Voltage](#)

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.



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

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

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.

## Network Connections

[CONFIGURE > NETWORK CONNECTIONS](#)

The **Network Connections** menu contains the **Network Interfaces**, **IPsec Tunnels** and **Static Routes** 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 32](#).

For information about VLAN interfaces, bridges and bonds, see ["Network Aggregates - Bonds and Bridges" on page 89](#)

## DNS Configuration

DNS settings such as Name Servers and Search Domains can be configured for each network interface, which will override the DHCP provided settings.

Name servers allow the system to resolve hostnames to IP addresses to communicate with remote systems. Search domains allow the system to resolve partially qualified domain names (PQDN) by appending entries from the listed search domains to form a fully qualified domain name (FQDN).

When adding an interface to a Bond or Bridge, it will use the DNS configuration of the aggregate interface.

**Note:** Interfaces must have at least one network connection to be able to perform DNS resolution.


### Configure DNS via the Web UI


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


On the Network Interfaces page, select the desired interface and click the Edit link.


#### Name Servers


1. Add one or more name servers to the list by clicking the **Add Name Server** button.
2. Name servers can be IPv4 or IPv6 addresses.
3. Name servers can be removed from the list by clicking the

Name Server 








 Add Name Server


**Delete** button next to each row.


4. Click **Apply** to save the changes.


## DNS Search Domains


1. Add one or more DNS search domains to the list by clicking the **Add Search Domain** button.
2. Search domains should be fully qualified domain names.
3. Search domains can be removed from the list by clicking the **Delete** button next to each row.
4. Click **Apply** to save the changes.

Search Domain 

office.example.com 

sales.example.com 

development.example.com 

 Add Search Domain

## Configure DNS via the Command Line

Description	Command
Display configured DNS settings for an interface	<pre>ogcli get physif "net1"</pre>
Update DNS settings for an interface	<pre>ogcli update physif "net1" &lt;&lt; END dns.nameservers[0]="1.1.1.1" dns.nameservers[1]="1.0.0.1" dns.search_domains[0]="example.net" dns.search_domains[1]="example.com" END</pre>

Description	Command
Check unbound service status	<pre>systemctl status unbound.service</pre>
List forward-zones in use	<pre>unbound-control list_forwards</pre>

## 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.

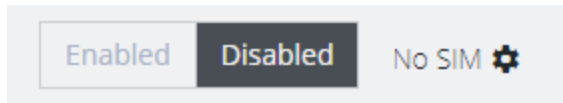
With the Dual SIM feature activated, in the event of a failure of OOB communications through the Active SIM, it is possible to manually de-select the failed SIM and activate the secondary SIM by making *it* the Active SIM. This changeover allows OOB communications to resume through the newly designated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

### Display SIM Status and Signal Strength

**Note:** For information about configuring the **Signal Strength Thresholds** see: ["SNMP Alerts" on page 64](#)

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

## Cellular Interface (LTE)

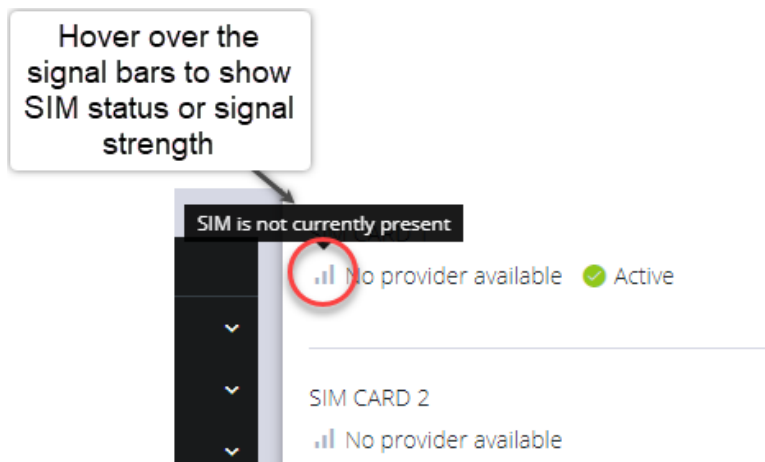


3.

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.
- **Amber** 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

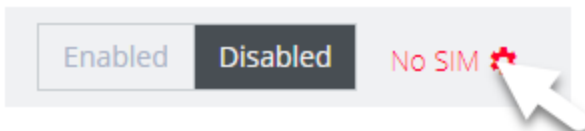
**Note:** The device will not recognize the new SIM card unless a shut-down and restart is performed. The new SIM card will be read during start-up.

## Select The Active SIM (Manual Failover Mode)

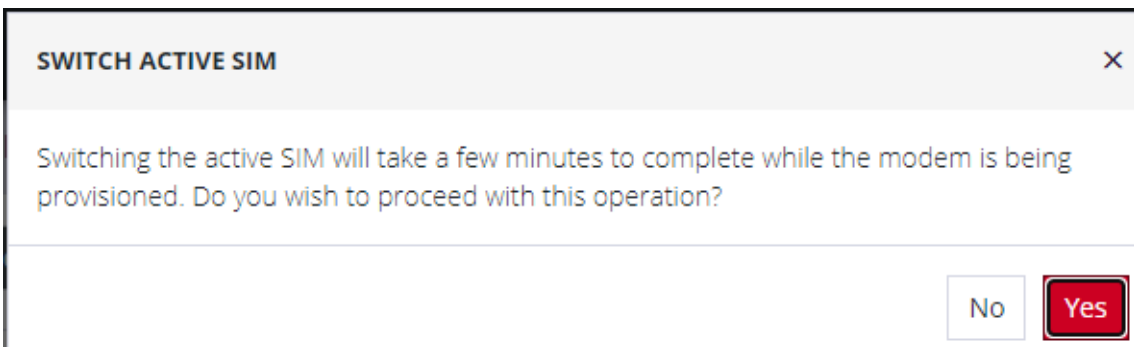
Switching the active SIM must be done manually. To switch the Active SIM:

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
```



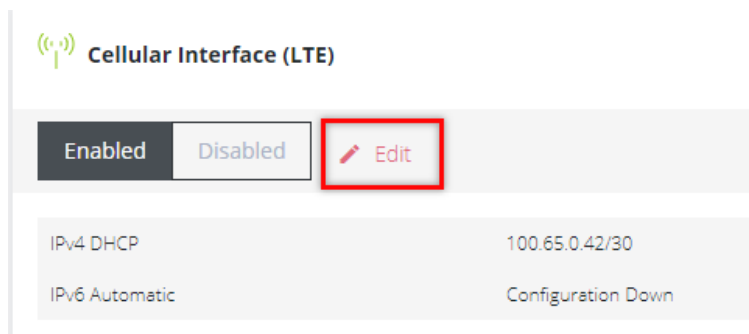
You can also set the SIM settings by expanding the menu for each SIM to set the APN.

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)

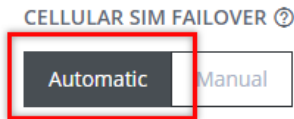
Switching the primary SIM must be done manually. To switch the Primary SIM:

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.



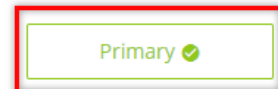
3. Ensure the cellular interface is enabled by clicking the **Enabled** button.

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

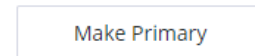


▲ Cellular SIM Failover may take a few minutes due to the need to switch firmware.

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 77](#)).

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 87](#).

**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

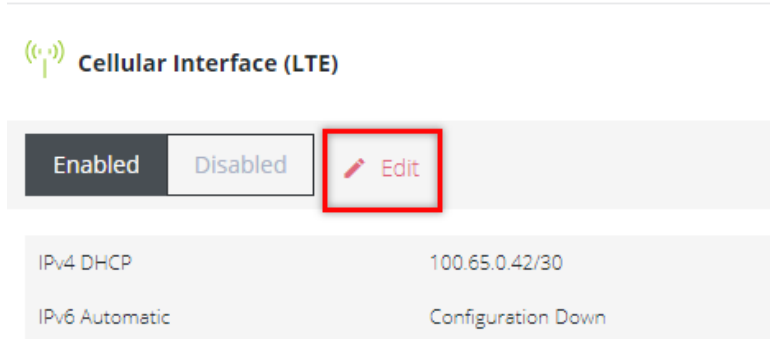
Features of Automatic Failover include:

- 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 87](#) 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 77).
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](#)

### Bridges

Network bridges allow connecting of multiple network segments together so that they may communicate as a single network.


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.

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

### Create A New Bridge

To create a new bridge:

1. Navigate to the **Configure > Network Connections > Network Interfaces** page on the Web GUI.
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.

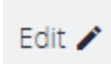
## Edit an Existing Bridge

To edit an existing bridge:

1. Navigate to the **Configure > Network Connections > Network Interfaces** page on the Web GUI.
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.

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

## 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	<p>Enable or disable Spanning Tree Protocol.</p> <p>See "Spanning Tree Protocol" on page 96.</p>
Network Interface Selection	<p>Click the checkbox of each network interface you want to include in the bridge.</p> <p>Available interfaces include Ethernet and VLAN interfaces that are not part of another bond or bridge.</p> <p>Bond interfaces can be included in a bridge by using the <b>ogcli</b> tool. See <a href="#">Support for Bonds in Bridges</a> on Zendesk.</p>
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.

## Bonds

Network bonds allow combining two or more network interfaces together into a single logical "bonded" interface for load balancing, redundancy or improved performance depending on the bond mode used.

Definitions of the bond details as in the **Bond Form Definitions** table below.

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

### Create A New Bond

To create a new bond:

1. Navigate to the **Configure > Network Connections > Network Interfaces** page on the Web GUI.
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

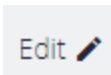
To edit an existing bond:

1. Navigate to the **Configure > Network Connections > Network Interfaces** page on the Web GUI.
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.

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

## Edit Bond - Form Definitions

New Bond Field	Definition
Description	<p>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.</p>
Mode	<p>The mode determines the way in which traffic sent out via the bonded interface is dispersed over the real interfaces. Available modes are:</p> <p><b>Round Robin Balancing</b> - Packets are sequentially transmitted/received through each interfaces one by one.</p> <p><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.</p> <p><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.</p> <p><b>Broadcast</b> - All network transmissions are sent on all secondary interfaces. This mode provides fault tolerance.</p> <p><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> <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	<p>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.</p>
Network Interface Selection	<p>Click the checkbox of each network interface you want to include in the bridge.</p> <p>Available interfaces include Ethernet and VLAN interfaces that are not part of another bond or bridge.</p>
Primary Interface	<p>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.</p>
Active Connections	<p>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.</p>
	<p>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.</p>

## Spanning Tree Protocol

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

Spanning Tree Protocol (STP) allows Operations 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))



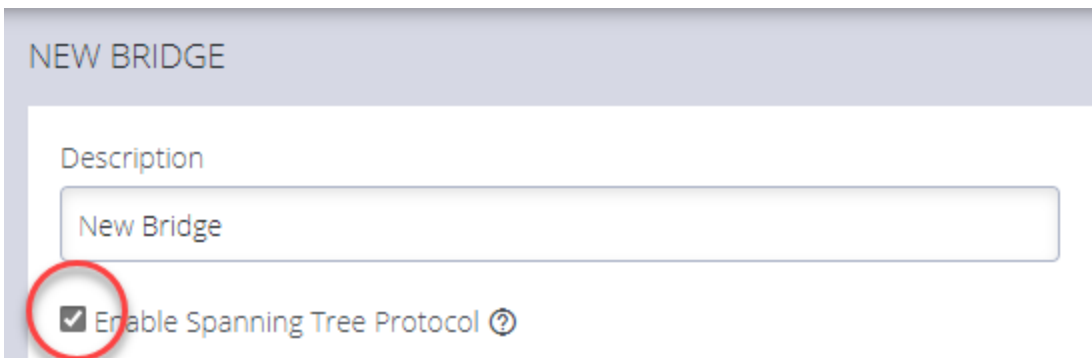
## Enable STP in a Bridge

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](#)

The Opengear OM can use IPsec to securely connect and route between two or more LANs (sometimes referred to as site to site, LAN-to-LAN, L2L VPN), or as a single client endpoint connecting to a central LAN or endpoint (sometimes referred to as host to site, or host to host).

IPsec does not make a formal distinction between initiator and responder, however the Opengear OM can both initiate tunnels (as the "initiator") and have other devices initiate tunnels to it (as a "responder").

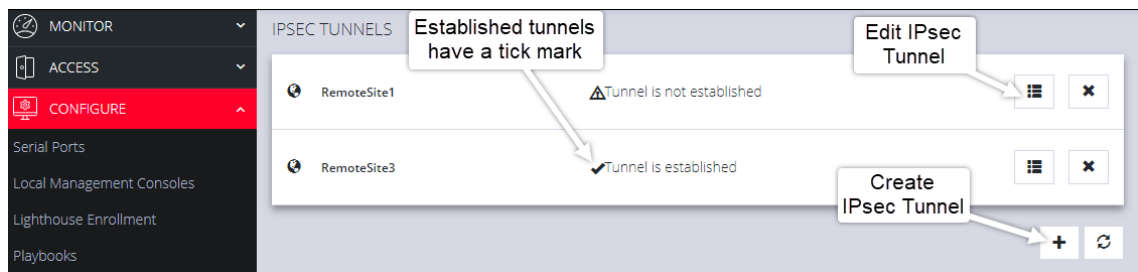
### Create, Add or Edit IPsec Tunnels

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

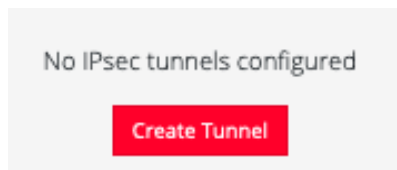
To create an IPsec tunnel:

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

*The IPsec Tunnels page with two tunnels previously created.*



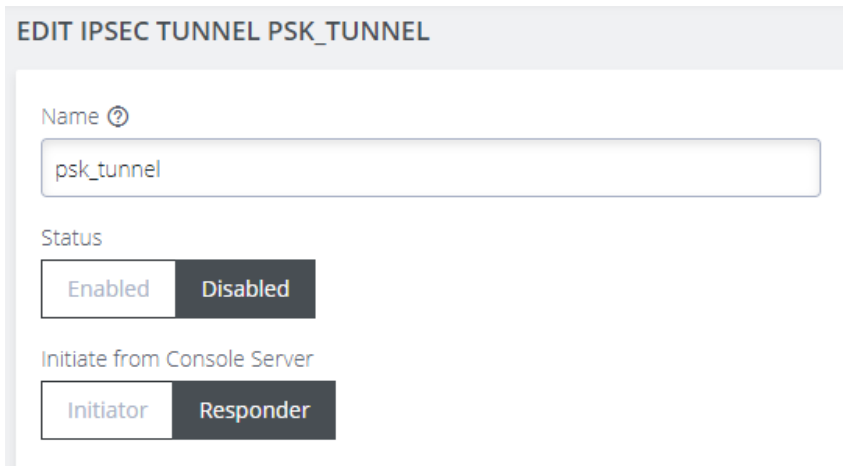
*If there are no existing tunnels, this **Create Tunnel** button is displayed:*



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

## NAME and STATUS

3. In the **Name** section of the page, give your new tunnel a unique name and click the **Enabled** button.



EDIT IPSEC TUNNEL PSK\_TUNNEL

Name ⓘ

psk\_tunnel

Status

Enabled Disabled

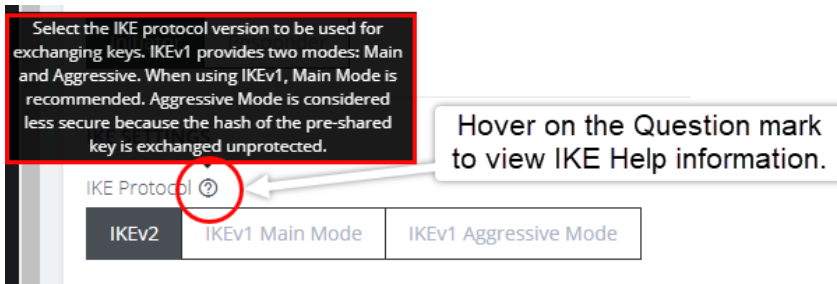
Initiate from Console Server

Initiator Responder

4. Set the Console Server to be the **Initiator** or **Responder**.

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

## IKE SETTINGS



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.

Hover on the Question mark to view IKE Help information.

IKE Protocol ⓘ

IKEv2 IKEv1 Main Mode IKEv1 Aggressive Mode

Continued...

5. 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.
6. Select the **Algorithm 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.
7. Select **Initiate** to actively initiate the tunnel by sending IKE negotiation packets to the remote end.
8. Set up the **Phase 1** and **Phase 2** time interval between the key material refresh of the IKE and Child.

## AUTHENTICATION

OM Authentication can use PSK or PKI.

9. **For pre-shared key (PSK) authentication**, enter a pre-shared secret key; both ends of the tunnel must use the same key.

### Tip:

To construct ID\_USER\_FQDN identities, use `user@example.com`

To construct ID\_FQDN type identities, use `@host.example.com`

If left blank, the outer local IP address of the tunnel is used as the identity.

10. Enter a **Local ID** Identity or IP address for the local end of the tunnel. If left blank, the outer-local IP address is used as the source address of the tunnel.
11. **For Public Key Infrastructure (PKI) authentication**, upload the certification bundle file or, drag and drop the file into the Certificate Bundle field.

## TUNNEL SETTINGS

12. Select **Enabled** if enforced UDP encapsulation is required. When enabled, the IKE daemon can simulate the NAT detection payload.

## ADDRESSING

13. Enter the **Local Address** to be used as the source address of the tunnel. If left blank, IPsec will automatically use a default.
14. Enter a **Local Subnet**. Specify local traffic to be tunneled. When no subnets are specified, only traffic originating from this device will be tunneled.
15. Enter the **Remote Address** or hostname for the remote end of the tunnel. If left blank, IPsec will accept initiation packets from any address.
16. Enter the **Remote Subnet**. Specify addresses or subnets that are behind the remote end of this tunnel. If no subnet is specified, only traffic originating from the outer remote address will be accepted.

## DEAD PEER DETECTION

**Tip:** Dead Peer Detection may be used to support long-lived tunnels.

Dead Peer Detection (DPD) is a method used by devices to verify the current existence and availability of IPsec peers. A device performs this verification by sending encrypted IKE Phase 1 notification payloads (R-U-THERE messages) to a peer and waiting for DPD acknowledgments (R-U-THERE-ACK messages) from the peer.

Continued...

You can enable DPD and configure the various options to fine-tune the functionality:

### DEAD PEER DETECTION

Dead Peer Detection

Delay <sup>?</sup>  Seconds    Timeout <sup>?</sup>  Seconds    Action <sup>?</sup>

- **Delay** - the time interval between polling the peer (default is 60 seconds).
- **Timeout** - the waiting time before deciding that a peer connection is not live (default is 90 seconds).
- **Action** - the action to be performed when a connection is timed-out. (default is Restart).
  - **Restart** will immediately attempt to renegotiate the tunnel.
  - **Clear** will close the CHILD\_SA.
  - **Trap** will catch matching traffic.

ENABLE the IPsec TUNNEL

17. When you have completed the IPsec Tunnel set-up process, ensure the IPsec tunnel status is set to **Enabled**, then, click **Save**.

The new tunnel is now listed on the **CONFIGURE > NETWORK CONNECTIONS > IPsec Tunnels** page.

## Static Routes

[CONFIGURE > NETWORK CONNECTIONS > Static Routes](#)

Static routes are predefined paths that traffic can be configured to take through the network for purposes such as security, cost or to override the default route.

The list of configured static routes are displayed in a table with their current status indicated by the status column.

Status	Meaning
Installed	The route is installed in the routing table.
Not Installed	The route may not be currently installed, but should update in a moment.
Error	The route failed to be installed.
Failed to fetch status	There is an error with the system and status failed to be obtained. This is a temporary error and should update in a moment.
The network interface is disabled	The static route is bound to an interface which is not enabled.
The network interface is disconnected	The static route is bound to an interface which is not connected.
The network interface has no active connections	The route cannot be installed as there are no active connections on this interface.



## Configure Static Routes

On the Static Routes page you can add, edit or delete static routes.

**Note:** Only basic validation is performed when static routes are saved. Check the status column to ensure your route is installed and working correctly.

### Create a static route

1. Click the **Add** button to navigate to the creation page.
2. Enter a valid IPv4 or IPv6 destination address or network, followed by the netmask in CIDR notation. The destination address/network must be unique.
3. Enter the gateway or select an interface for the static route to use.
4. Optionally, provide a metric for the route. Routes with a lower metric value are higher priority.

Destination Address	Default Metric
IPv4	0
IPv6	1024

5. Click the **Apply** button to save the changes.
6. If the changes are saved successfully you are returned to the Static Routes list page.
  - If there is an error with the configuration and the route fails to install, a red banner is displayed.
  - If the route installed successfully, a green success banner is displayed.

7. The current status of the configured route is displayed in the table, which may change depending on the status of the network configuration.

### Edit a static route

1. Click the description of the desired static route in the list to access the **Edit** page.
2. Update the details of the static route.
3. Click apply to save the changes.

### Delete a static route

1. Click the description of the desired static route in the list to access the **Edit** page.
2. Click the **Delete** button at the top-right of the page.
3. Click **Yes** to confirm the action.
4. If the route was removed from the routing table as expected, a green success banner is displayed.

## Managing Static Routes via Command Line

Administrative users can also view the status and perform configuration of static routes via the command line interface.

After creating or modifying a route via the command line, you should take note of the route id and confirm that it has been installed successfully in the routing table.

Description	Command
Display IPv4 installed routes	<pre>ip route</pre>

Description	Command
Display IPv6 installed routes	<pre>ip -6 route</pre>
Display all route information	<pre>ip route show table all</pre>
Show status of configured routes via ogcli	<pre>ogcli get monitor/static_routes/status</pre>
Get static route configuration via ogcli	<pre>ogcli get static_routes</pre>
Create static route via ogcli	<pre>ogcli create static_route &lt;&lt; END destination_address="1.1.1.1" destination_netmask=32 gateway_address="1.1.1.1" interface="net1" metric=0 END</pre>
Update static route via ogcli	<pre>ogcli update static_route "1.1.1.1" &lt;&lt; END interface="net2" metric=100 END</pre>
Delete static route via ogcli	<pre>ogcli delete static_route "1.1.1.1"</pre>

## Network Resilience

[CONFIGURE > NETWORK RESILIENCE >](#)

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

## Out Of Band Failover

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

Out-of-Band (OOB) Failover detects network disruption via the probe interface, and automatically activates the cellular connection to re-establish network access.

OOB failover requires an IPv4 address (in dotted decimal format), or an IPv6 address, or a domain name, which is always reachable and unlikely to change. When OOB failover is enabled, the device regularly pings this address, using the probe interface, to check for network connectivity.

### Enable Out-of-Band Failover

1. To manage Out-of-Band Failover, navigate to the **CONFIGURE** > **NETWORK RESILIENCE** > **OOB Failover** page

#### FAILOVER SETTINGS

Status ?

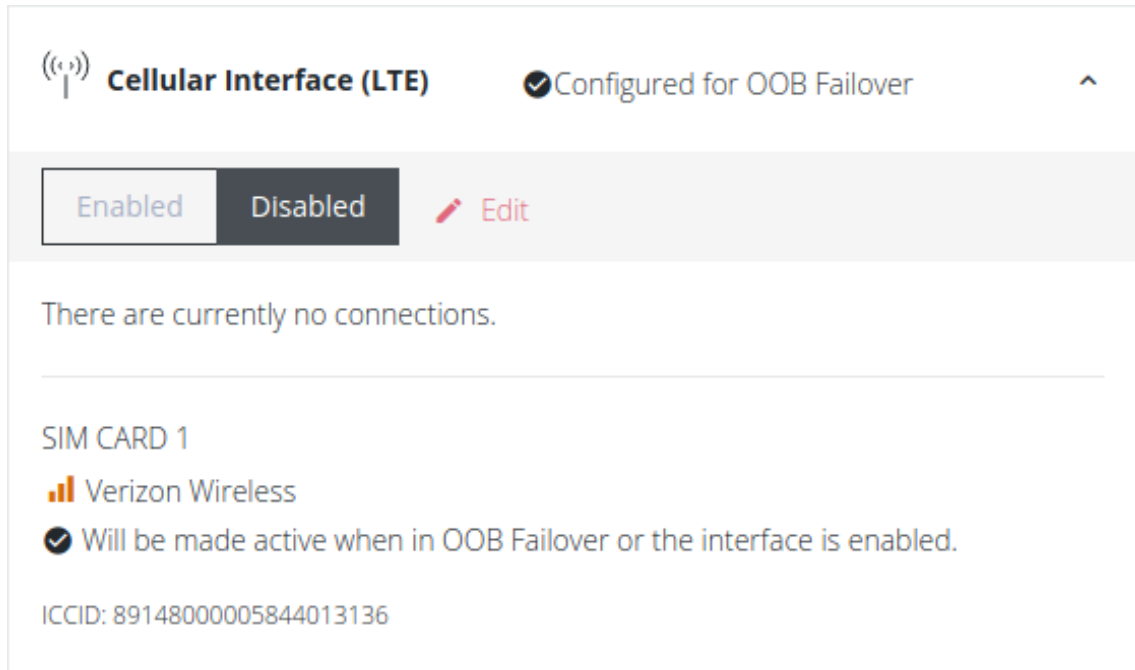
 Enabled  Disabled

Probe Interface ?

Probe Address ?

2. When you have completed the OOB Failover set-up, ensure the OOB Failover status is set to **Enabled**, then, click **Apply**.

3. On the **Network Interfaces** page, the cellular interface will display "Configured for OOB Failover".



4. When failover is triggered, the interface will be marked with "OOB Failover Active".

## Dormant DNS on Failover Interface

This option configures how the DNS name servers and search domains configured for the failover interface are used by the system.

DNS Dormant on Failover Interface 

Never

Until Failover

- If set to **Never**, the DNS name servers and search domains configured for the failover interface will always be available to the system for DNS name resolution.
- If set to **Until Failover**, the DNS name servers and search domains will be made available to the system only when the failover state is active.

To configure the DNS name servers and search domains, see ["DNS Configuration" on page 74](#).

## OOB Failover Types & Failover Behavior

OOB Setting	Cellular Interface	Mode	Description
Disabled	Enabled	Always up OOB	Failover detection is disabled. Only inbound connections on the cellular interface are routed back out the cellular interface, to enable OOB access from remote networks (e.g. incoming SSH). Otherwise outbound network connections (e.g. VPN client tunnels, SNMP alerts) are established according to the main static routing table, regardless of network state.
Enabled	Disabled	Failover mode	<p>Failover detection is enabled on the selected "probe" interface. The cellular interface remains in a down state with no network configuration.</p> <p>When failover is initiated, the cellular network interface is started and configured. If a default route is installed on the cellular interface, it takes precedence over the default route on the failed "probe" interface. Outbound network traffic (e.g. VPN client tunnels, SNMP alerts) are established or re-established out cellular connection during failover.</p> <p>The advantage of this mode is the secondary connection is completely inactive during normal operation which may be advantageous where the goal is to keep the interface off the Internet as much as possible, e.g. a cellular plan with expensive data rates and no carrier-grade NAT.</p>

Enabled	Enabled	Dormant failover	<p>Failover detection is enabled. Only inbound connections on the cellular interface are routed back out the cellular interface, to enable OOB access from remote networks (e.g. incoming SSH). Otherwise outbound network connections (e.g. VPN client tunnels, SNMP alerts) are established according to the main static routing table, regardless of network state.</p> <p>When failover is initiated, the default route of the cellular interface takes precedence over the failed “probe” interface. Outbound network traffic (e.g. VPN client tunnels, SNMP alerts) are established or re-established out the cellular connection during failover.</p> <p>The advantage of this mode is the cellular connection is available for inbound out-of-band access during normal operation.</p>
---------	---------	------------------	--



## IP Passthrough

Devices with dialout support and an Ethernet port can enable a special DHCP service called IP Passthrough. When IP Passthrough is enabled, other devices (eg. the "passthrough target" or "downstream host") that are plugged into the Ethernet port will operate as if they are directly connected to the dialout network.

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

1. To manage **IP Passthrough** navigate to the **CONFIGURE > NETWORK RESILIENCE > IP Passthrough** page.

### SETTINGS

2. Click the IP Passthrough status checkbox to set the status to **Enabled**.
3. Click the radio button next to the interface type that is used.
4. Enter the MAC address of the downstream device that will make the DHCP requests. The MAC address of the device will be offered a DHCP lease. DHCP requests from other MAC addresses will be ignored.

#### IP PASSTHROUGH

**SETTINGS**

Enable ?

Interface ?

NET1 - 1G Copper/SFP  
 NET2 - 1G Copper/SFP

Downstream MAC Address ?

## SERVICE INTERCEPTS

**Tip:** When IP Passthrough is enabled, 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.

### 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 

SSH Intercept Port 



Apply

5. Enter the port number that is to be used for HTTPS Intercepts.
6. Enter a port to be redirected to this device's SSH service.

**Tip:** 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.

7. When you have completed the IP Passthrough Settings and Service Intercept form, ensure the IP Passthrough status is set to **Enabled**, then, click **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.

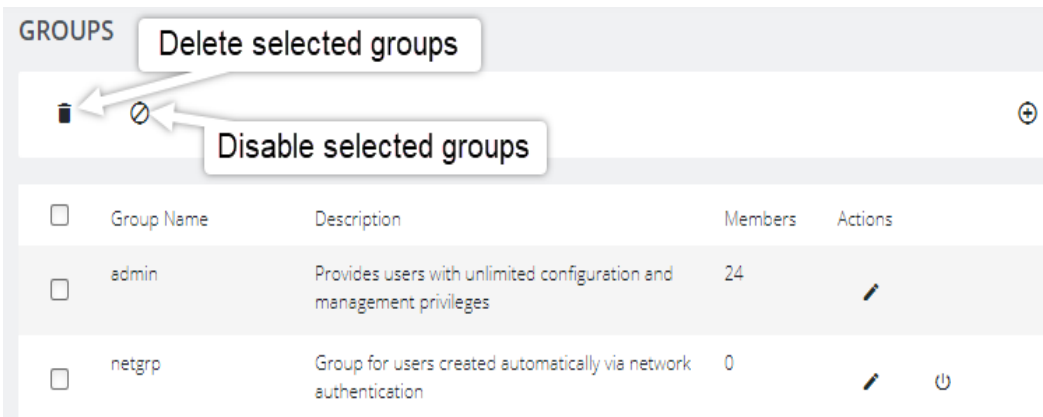
## Groups

[CONFIGURE > USER MANAGEMENT > Groups](#)

Groups are used to grant privileges to users. When a user is a member of a group, they select the serial ports and serial PDUs, for example, from within the groups. Privileges include lists of accessible serial/USB console ports, these can be defined per-group.

### Create a New Group

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



	Add a new group.
	Edit an existing group.
	Enable an existing group.
	Disable an existing group (or disable selected groups).
	Delete a group (or delete selected groups).

2. Click the **Add New Group** button. The **NEW GROUP** page opens.

### NEW GROUP

Group Enabled

Group Name

Description

Role

3. Enter a **Group Name**, **Description**, and select a **Role** for the group.

**Note:** **Group Name** is case sensitive. It can contain numbers and some alphanumeric 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.

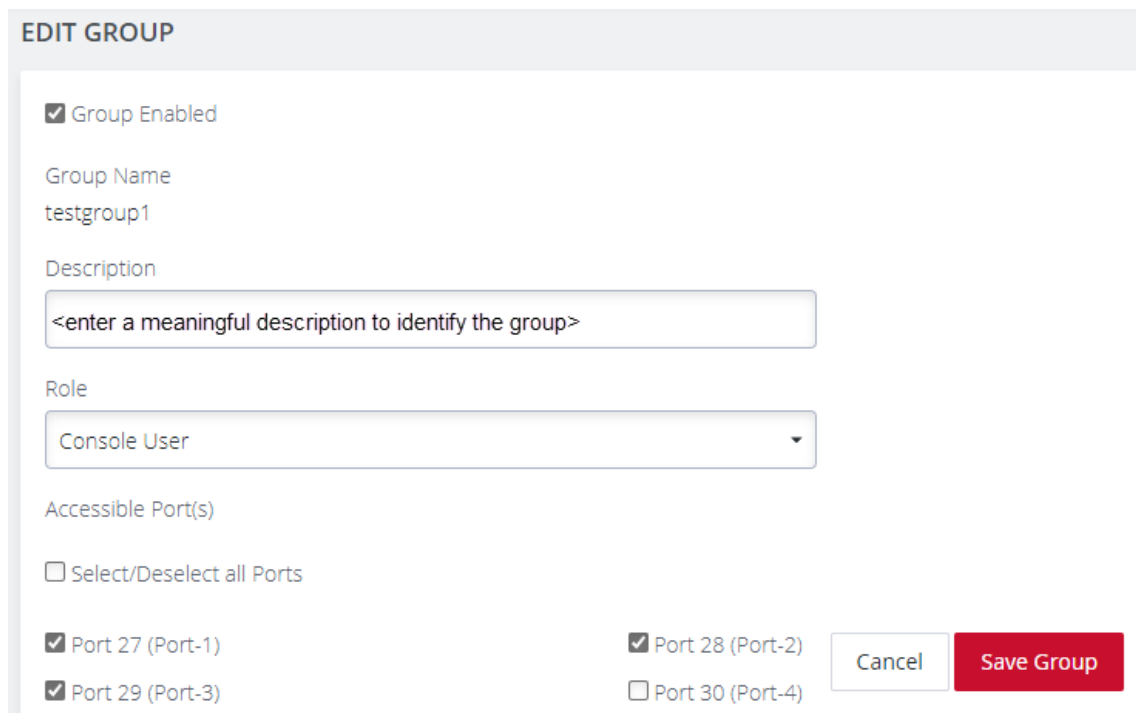
**Note:** If the **Role** selected is **Administrator**, members of the group have full access to and control of all managed devices, full system configuration privileges, and full access to the command line shell.

**Tip:** Choosing the **Console User** role allows you to select specific ports this group will be able to access.

4. 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.
5. Click **Save Group**.

## Edit an Existing Group

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



The screenshot shows the 'EDIT GROUP' form with the following fields and options:

- Group Enabled
- Group Name: testgroup1
- Description: <enter a meaningful description to identify the group>
- Role: Console User
- Accessible Port(s):
  - Select/Deselect all Ports
  - Port 27 (Port-1)
  - Port 28 (Port-2)
  - Port 29 (Port-3)
  - Port 30 (Port-4)

Buttons: Cancel, Save Group

2. Click **Edit** in the **Actions** section of the group to be modified and make desired changes.
3. Click **Save Group**.

Continued...

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.

**Note:** For users that don't have any group, they are still part of netgrp, even if the netgrp membership is not explicitly enabled for the user.

The permissions for the netgrp members is a union of the permissions that have been given in the netgrp AND the permission for the user in AAA (TACACS+, RADIUS, etc).







If your netgrp "role" says "Console User" and you have priv-lvl 13 in TACACS+ (level 15 being the highest), then the union of that is like an admin already, so setting "console user" in netgrp does not matter.

## Local Users

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

The Local Users feature allows a single point for the creation or management of local user accounts. The Local Users feature can use SSH authorized keys to control user access by using their local password; it is a point of control for:







- Authentication and authorization.
- Creating and editing user descriptions.
- Local passwords.
- User roles (admin or co sole user).
- Accessible ports.

LOCAL USERS			
			
<input type="checkbox"/>	Username	Description	Actions
<input type="checkbox"/>	root	System wide SuperUser account	  


See the Button Action Definitions table on the following page:



*Button Action Definitions:*

	Add a new local user.
	Edit an existing user.
	Enable an existing user.
	Manage SSH Authorized Keys.
	Disable an existing user (or disable selected users).
	Delete a user (or delete selected users).

## Create a New User With Password

1. Navigate to the **CONFIGURE > USER MANAGEMENT > Local Users** page.
2. Click the **Add User**  button. The **New User** dialog appears.
3. Enter a Username, Description, and Password that the new user will use.
4. Re-enter the **Password** in the **Confirm Password** field.
5. Select the **Enabled** checkbox.
6. Click **Apply**. A banner will confirm that the data has been saved.

## Create a New User With No Password (Remote Authentication)

To create a new user with no password.

**Note:** If a new user is created with no password, this will cause the user to fall-back use 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 **Add User** 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**. A banner will confirm that the data has been saved.

## Modify An Existing User Account With Password



1. Select **CONFIGURE > USER MANAGEMENT > Local Users**
2. Click the **Edit User** button and make the required changes.
3. Click **Save User**. A banner will confirm the changes have been saved.

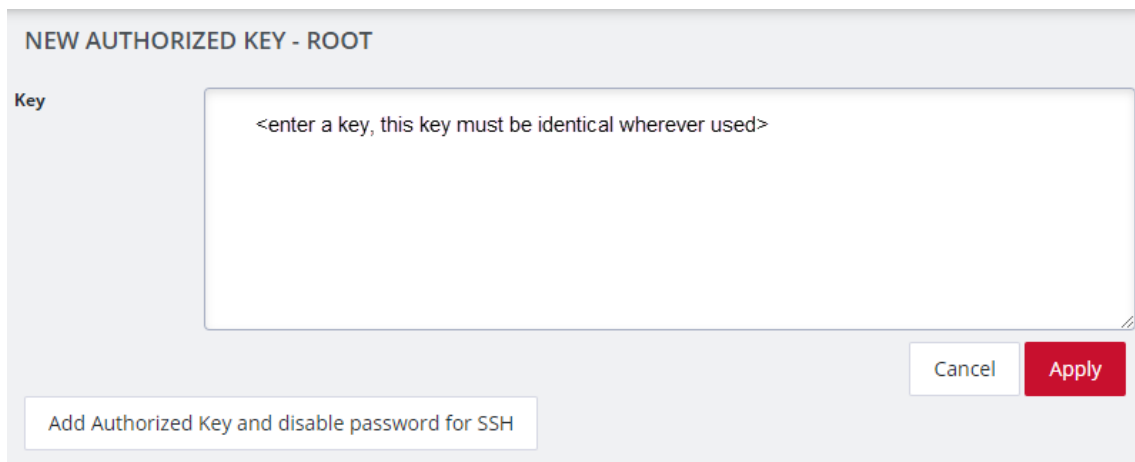
The **Edit Users** dialog allows the user's **Description** to be changed, **Group Memberships** modified, and the user's **Password** to be reset. The username cannot be changed. To disable a user, uncheck the **Enabled** checkbox.

**Note:** Users of disabled accounts cannot log in to the OPERATIONS MANAGER using either the Web-based interface or via shell-based logins.

## Manage SSH Authorized Keys for a User Account

To manage SSH authorized keys for a user:

1. Select **CONFIGURE > USER MANAGEMENT > Local Users**
2. Click the **Manage SSH Authorized Keys**  button for that user.
3. Click the **Add Authorized Key**  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 **Manage SSH Authorized Key** button for the user.
6. Click the **Delete** button next to the key you wish to remove.

## Delete a User's Account

To delete a user's account:

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.

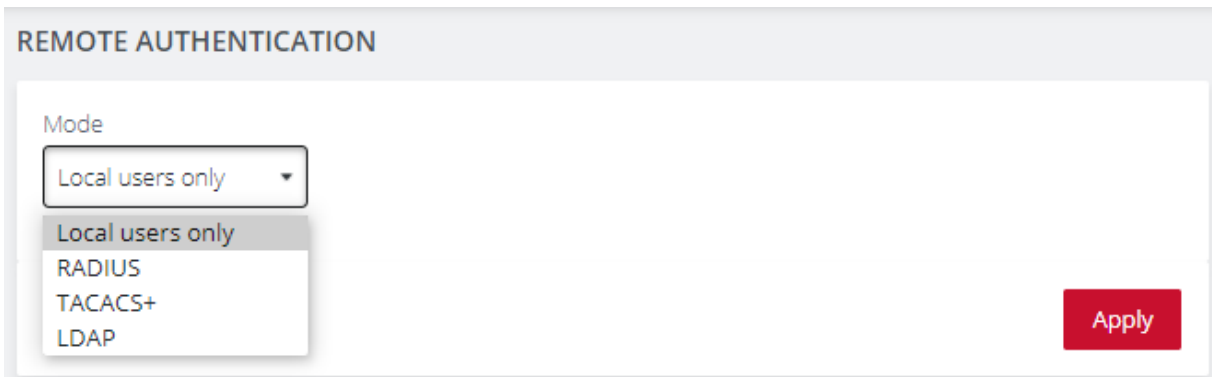
## Remote Authentication

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

The OPERATIONS MANAGER supports three AAA systems. Select the remote authentication mode to be applied (DownLocal, or Local apply for all modes):

- RADIUS
- TACACS+
- LDAP

Navigate to **CONFIGURE > USER MANAGEMENT > Remote Authentication**, the Remote Authentication Home page is displayed.



**Tip:** All fields in the Remote Authentication form have tooltips that provide additional information to assist with completing the form fields.

## Configure RADIUS Authentication

1. Under **CONFIGURE > User Management > Remote Authentication**, select **RADIUS** from the **Mode** drop-down menu.
2. Select the preferred Radius Remote Authentication policy to be applied: **Radius DownLocal**, or **Radius Local** (see the tips below).

**Tip: RADIUS DownLocal:** Users are authenticated using a local account as per a regular local login only if the remote AAA server is unreachable or down. If credentials are incorrect or if the user account does not exist, the user is denied access.

**Tip: RADIUS Local:** If remote authentication fails because the user account does not exist on the remote AAA server, the OM device attempts to authenticate the user using a local account as per a regular local login

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

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

*Continued...*

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.

## Configure TACACS+ Authentication

1. Under **CONFIGURE > USER MANAGEMENT > Remote Authentication**, select TACACS+ from the *Scheme* drop-down menu.
2. Select the preferred TACACS+ Remote Authentication policy to be applied: **TACACS+ DownLocal**, or **TACACS+ Local** (see the tips below).

**Tip: TACACS+ DownLocal:** Users are authenticated using a local account as per a regular local login only if the remote AAA server is unreachable or down. If credentials are incorrect or if the user account does not exist, the user is denied access.

**Tip: TACACS+ Local:** If remote authentication fails because the user account does not exist on the remote AAA server, the OM device attempts to authenticate the user using a local account as per a regular local login.

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

6. 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  
    }  
}
```

**Note:** For Cisco ACS, see [Setting up permissions with Cisco ACS 5 and TACACS+](#) on the Opengear Help Desk.

## Configure LDAP Authentication

1. Under **CONFIGURE > User Management > Remote Authentication**, select **LDAP** from the **Mode** drop-down menu.
2. Select the preferred LDAP Remote Authentication policy to be applied: **LDAP DownLocal**, or **LDAP Local** (see the tips below for explanation).

**Tip: LDAP DownLocal:** Users are authenticated using a local account as per a regular local login only if the remote AAA server is unreachable or down. If credentials are incorrect or if the user account does not exist, the user is denied access.



**Tip: LDAP Local:** If remote authentication fails because the user account 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 login.

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

For example:

```
CN=example-user,CN=Users,DC=example-domain,DC=com
```

4. Add the **LDAP 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. Input the password for the **LDAP Bind DN** user and confirm the password.
6. Add the **LDAP Username Attribute**. This depends on the underlying LDAP system. Use sAMAccountName for Active Directory systems, and uid for OpenLDAP based systems.
7. Add the **LDAP 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.

## 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 GUI, 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 checkbox.

See also "[Password Policy Implementation Rules](#)" on page 133

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 133

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).
	The password must contain at least one numeric character (enabled/disabled separately).

	<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.

## Brute Force Protection

[CONFIGURE > SERVICES > Brute Force Protection](#)

A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until the one correct combination that works.

Brute Force Protection offers an essential defense mechanism by automatically blocking device access from offending source IP addresses.

**Caution:** Brute Force Protection may prevent access to the system during an emergency.

### Configure Brute Force Protection

**Note:** Brute Force Protection is enabled by default for SSH and Web UI.

To configure Brute Force Protection:

1. Navigate to **CONFIGURE > SERVICES > Brute Force Protection**.
2. Choose the desired settings as described below.
3. Click **Apply** to save the changes.

Field	Values	Description
SSH Protection	Enabled / Disabled	Enable Brute Force Protection for SSH login attempts.
HTTPS Protection	Enabled / Disabled	Enable Brute Force Protection for Web UI login attempts.

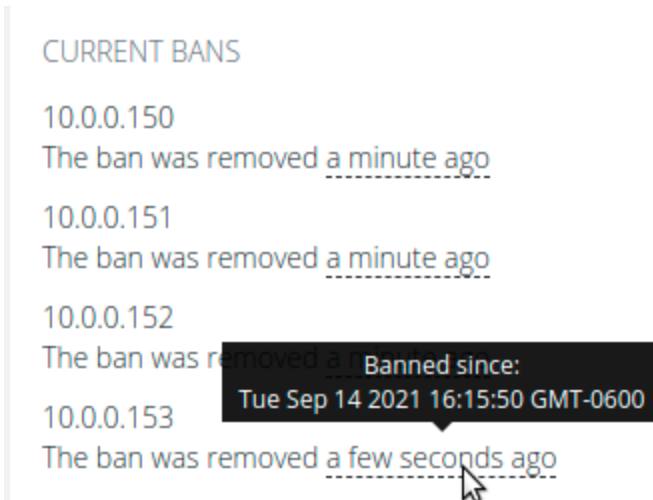


Field	Values	Description
Maximum failed attempts	Attempts: 3 (minimum) Time period in minutes: 1 (minimum)	The number of failed access attempts permitted within the given time period before preventing access.
Lockout period	60 (minimum)	The number of seconds that an IP address will be banned after violating the Brute Force Protection policies.

## Viewing Current Bans

IP addresses that are currently blocked appear in the CURRENT BANS section of the Web UI, displaying the address and remaining duration of the ban or how long ago the ban was lifted.

Hover over the ban time for more detailed information.



CURRENT BANS

10.0.0.150  
The ban was removed [a minute ago](#)

10.0.0.151  
The ban was removed [a minute ago](#)

10.0.0.152  
The ban was removed [a few seconds ago](#)

10.0.0.153  
The ban was removed [a few seconds ago](#)

Banned since:  
Tue Sep 14 2021 16:15:50 GMT-0600

## Managing Brute Force Protection via Command Line

For more control over Brute Force Protection, administrative users can use the command line to configure the service and remove bans manually.

Description	Command	Notes
Display Brute Force Protection configuration	<pre>ogcli get services/brute_force_protection</pre>	
Update Brute Force Protection configuration	<pre>ogcli replace services/brute_force_protection &lt;&lt; END ban_time=180 find_time=1 https_enabled=false max_retry=4 ssh_enabled=true END</pre>	Ban time in seconds. Find time in minutes.
Un-ban an IP address	<pre>fail2ban-client unban &lt;ipaddress&gt;</pre>	
Un-ban all current bans	<pre>fail2ban-client unban --all</pre>	
List SSH bans	<pre>fail2ban-client status sshd</pre>	SSH protection must be enabled
List HTTPs bans	<pre>fail2ban-client status https</pre>	HTTPs protection must be enabled
List all bans with ogcli	<pre>ogcli get monitor/brute_force_protection/bans</pre>	

## 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** are shown on the landing page.

### CURRENT SSL CERTIFICATE

Common Name ⓘ

default

The group overseeing this device.

Tool tips assist with completing the form

Organizational Unit ⓘ

Organization ⓘ

Locality/City ⓘ

State/Province ⓘ

Country ⓘ

US

Email ⓘ

Key Length (bits) ⓘ

2048

Issue Date ⓘ


Apr 26 20:11:11 2021 GMT

Expiry Date ⓘ

Apr 27 20:11:11 2022 GMT


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

### CERTIFICATE SIGNING REQUEST

Common Name 

The group overseeing this device.


Tool tips assist with completing the form content

Organizational Unit 


Organization 


Locality/City 


State/Province 


Country 

Email 

Key Length (bits) 

Challenge Password 

Confirm Password 

Private Key File 

Apply

## Network Discovery Protocols

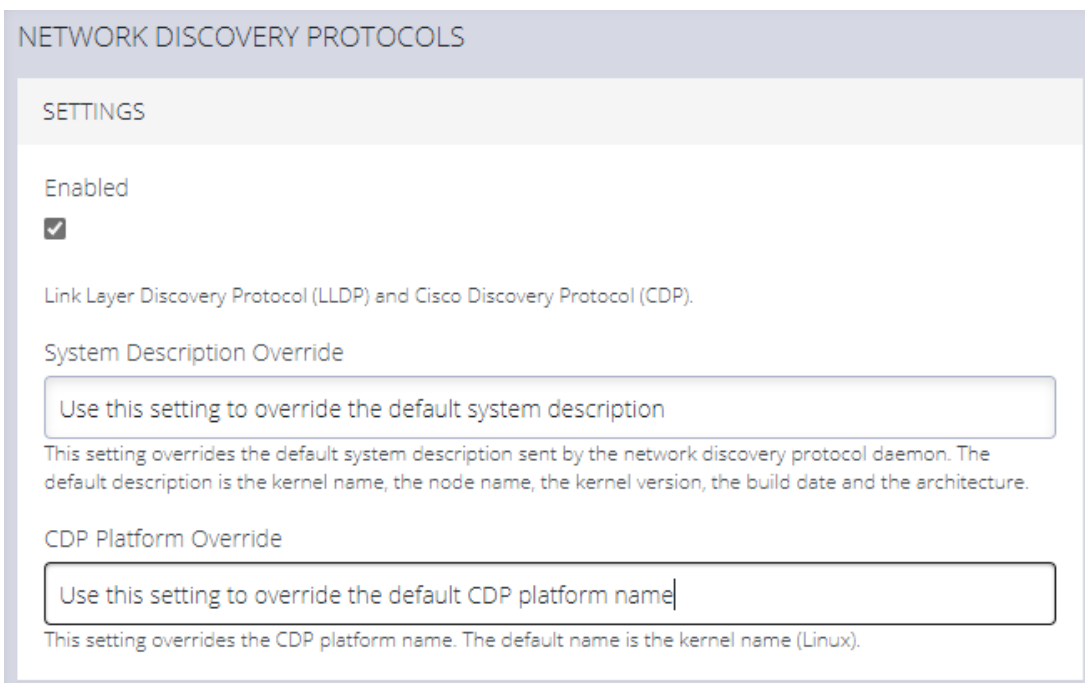
[CONFIGURE > SERVICES > Network Discovery Protocols](#)

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

The **CONFIGURE > SERVICES > Network Discovery Protocols > LLDP/CDP NEIGHBORS** page allows you to enable this service by clicking the **Enabled** 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.

A value can be entered in the CDP Platform Override to override the CDP platform name. The default name is the kernel name (Linux).



NETWORK DISCOVERY PROTOCOLS

SETTINGS

Enabled

Link Layer Discovery Protocol (LLDP) and Cisco Discovery Protocol (CDP).

System Description Override

Use this setting to override the default system description

This setting 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.

CDP Platform Override

Use this setting to override the default CDP platform name

This setting overrides 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**.

NETWORK INTERFACES

Selecting an interface allows LLDP/CDP monitoring for that interface.

NET1 - 1G Copper/SFP

NET2 - 1G Copper/SFP

**Apply**

## File Server

[CONFIGURE](#) > [SERVICES](#) > [File Server](#)

The Operations Manager can be configured to serve files to clients via Trivial File Transfer Protocol (TFTP).

TFTP can be used by devices on the network to perform a network boot, or to allow backup and restore of configuration files.

### Note: Limitations

- The user is responsible for disk space management.
- User permissions cannot be set on files at this time.

## Enable TFTP Service

**Note:** The TFTP service is disabled by default.

To enable the TFTP service:

- Click the **TFTP Enabled** button.



- Click **Apply** to save the changes.
- The TFTP service is now running with a default location of `/mnt/nvram/srv`.

This location is where all files uploaded to the TFTP server will be stored.

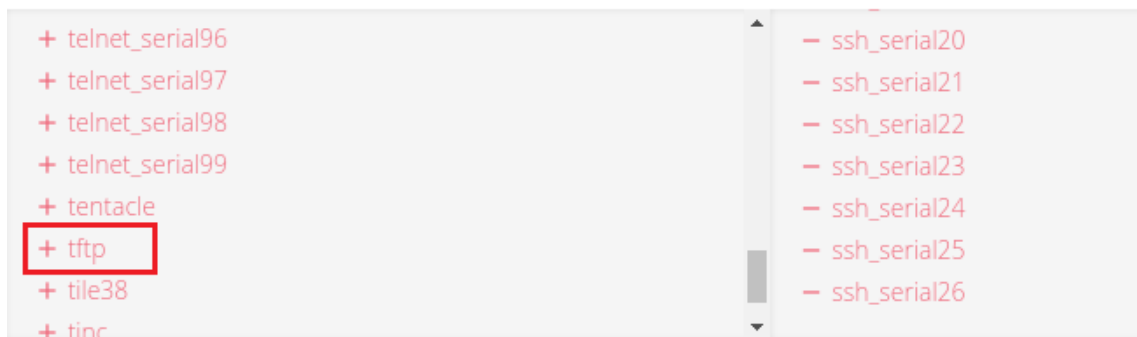
**Note:** The disk space usage information displayed on the page indicates the usage of the whole storage volume.

## Modify Firewall Zones To Allow The TFTP Service To Be Used

The TFTP service must be allowed through a firewall zone so that clients may upload and retrieve files.

- Navigate to the Firewall Management page via **CONFIGURE > FIREWALL > Management**.
- Expand the desired firewall zone and click the **Edit Zone** button.
- Allow the "tftp" service from the list of Permitted Services.

Permitted Services



- Click **Apply** to save the changes.
- On the File Server page, the zones with TFTP enabled are now displayed.

ZONES WITH TFTP ENABLED

LAN , WAN

## Update The TFTP Service Storage Location

The location used by the TFTP service can be updated using the **ogcli** tool.

**Note:** The storage location must be an existing directory before running **ogcli** update.



**Caution:** Using a storage volume other than **/mnt/nvram** is not recommended. Data may be lost after reboot, or be inaccessible when switching boot slots.

- As an administrative user, run:

```
ogcli update services/tftp path=\"<new path>\"
```

## Routing

[CONFIGURE > SERVICES > Routing](#)

The Operations Manager supports Static Routing and Dynamic Routing. Static Routing is currently configured via the ogcli interface, while Dynamic Routing is configured via the UI.

### Dynamic Routing

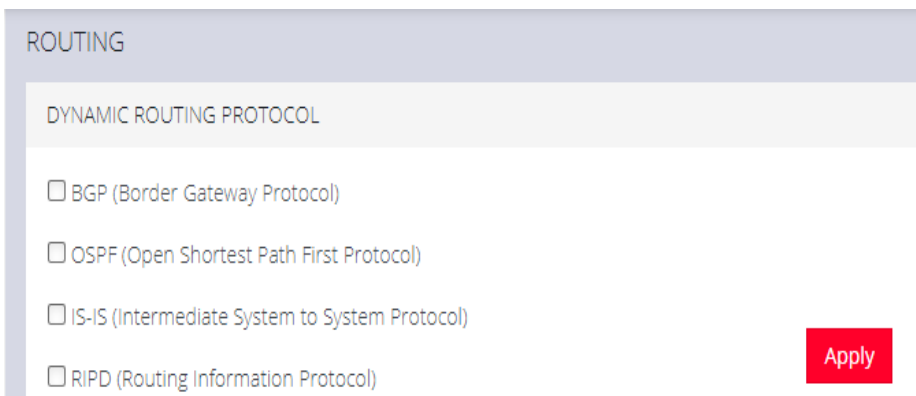
To enable Dynamic Routing on the OM, navigate to the **CONFIGURE > SERVICES > Routing** page.

Dynamic Routing supports four routing protocols, these are:

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

Select the preferred routing protocol then click **Apply**.

**Note:** If no protocol is selected, no route sharing services are run on the OM.



## Static Routing (via the ogcli)

To enable Static Routing on the OM, open an ogcli terminal by navigating to **ACCESS > Local Terminal**.

### Static Routing ogcli Help

For Help on implementing a Static Route protocol via ogcli, enter the command:

```
ogcli help static_routes
```

### Create Static Route - Example:

```
ogcli create static_route << 'END'  
destination_address="10.1.45.0"  
destination_netmask=24  
gateway_address="192.168.1.1"  
interface="system_net_physifs-1"  
metric=100  
  
END
```

## Static Routing Arguments

Argument	Description
<code>get</code>	Get a list of static routes.
<code>create</code>	Add a static route.
<code>replace</code>	Similar to the "Create Static Route" example given on the previous page. Creates a single static route by specifying its UUID; or a list of static routes. Overwrites existing routes.
<code>delete</code>	Delete all static routes.
<code>merge</code>	Merge the existing configuration list with a new list.

## SSH

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

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

The following table gives the definitions of the configurable SSH properties.

Parameter	Definition
Serial Port Delimiter	The delimiting character used to separate the username with port selection information. The default delimiter is a plus sign (+). For example, username+port@address.
Port Number for Direct SSH Links	If SSH is configured to be reachable on a non-standard port, the Direct SSH links on the serial ports page will use this port number.
Max Startups Start	The number of unauthenticated connections before they are refused.
Max Startups Rate	This is the percentage of unauthenticated connections refused. This percentage is a probability that increases linearly until the unauthenticated connections reach full.
Max Startups Full	The number of unauthenticated connections allowed.

### Unauthenticated Access to Serial Ports

For information about Unauthenticated Access to Serial Ports, see

["Unauthenticated SSH to Serial Ports" on the next page.](#)

## Unauthenticated SSH to Serial 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 data-bbox="704 604 1377 716"># SSH to serial port 1 by TCP port ssh -p 3001 -l operator 70.33.235.190</pre> <p data-bbox="704 730 1365 835">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 data-bbox="704 886 1377 997"># 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 data-bbox="704 1167 1377 1278"># 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>

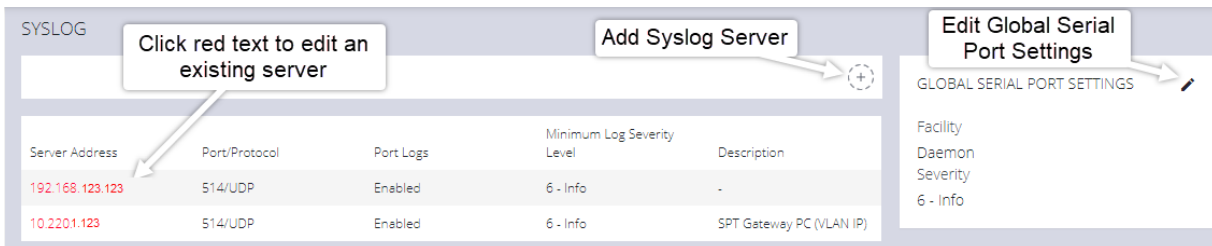
<p>Max Startups Full</p>	<p>The number of connections pending authentication before <i>all</i> new connections are refused.</p> <p><i>Required full: int (minimum = 1; default = 100)</i></p>
<p>Max Startups Rate</p>	<p>This is the percentage rate at which new connections are refused once the Max Startups 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 which the Syslog can be exported via TCP or UDP. There is a drop-down on each serial port to enable the logging and to define the “scope” of logging.

The Syslog page lists any previously added external syslog servers. See also "Remote Syslog" on page 1.



Server Address	Port/Protocol	Port Logs	Minimum Log Severity Level	Description
192.168.123.123	514/UDP	Enabled	6 - Info	-
10.2201.123	514/UDP	Enabled	6 - Info	SPT Gateway PC (VLAN IP)

## Add a New Syslog Server

**Note:** The combination of server address, protocol and port should be unique. There can be no duplicates. However, the same server could be used if the other entry is an IPv6 address to the same Syslog server.

Use the following procedure to add a new Syslog Server.

1. Navigate to **CONFIGURE > SERVICES > Syslog**.
2. Click the **Add Syslog Server** button. The **Add Syslog Server** form opens.
3. In the **Description** field, add a suitable description that will help to identify the new server.
4. Enter the **Server Address**.
5. Click the **Protocol** switch to select either **UDP** or **TCP**.

6. Enter the correct **Port**. If no port is entered, UDP defaults to port 514 and TCP defaults to 601.
7. From the drop-down list, select the required severity level to be logged, eight levels of log severity are supported.

**Note:** This configuration acts as a filter, such that any log equivalent or higher will be sent to the remote Syslog server.

8. Click **Add** to complete the process.

## Global Serial Port Settings

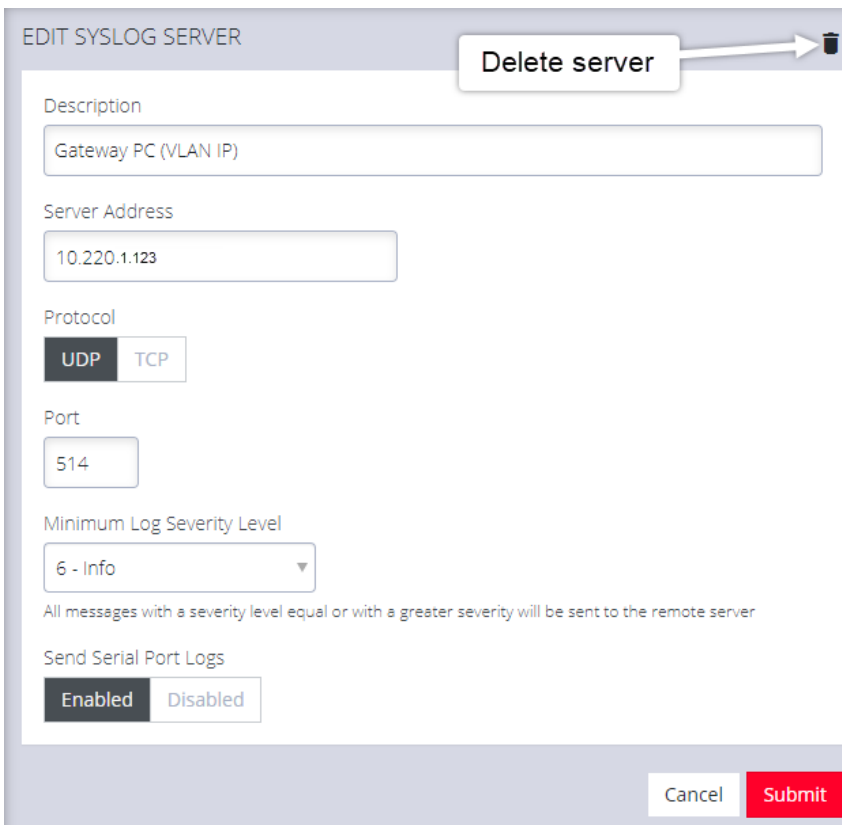
Global Serial Port Settings will define the Facility used and the Severity of all Syslog serial port activity sent from this node. There are two setting functions, Facility, and Severity. From the drop-down menus, select the preferred Facility and Severity as required.

For definitions of Facility and Severity, see "Syslog Facility Definitions" on page 1 and "Syslog Severity Definitions" on page 1.

## Edit or Delete an Existing Syslog Server

To edit an existing syslog server, click the hyperlinked **Red Text** server name in the server list (see the Syslog page image on the previous page). Make the required changes, then click the **Submit** button.

Delete a server by clicking the Delete icon at the top-right of the **Edit Syslog Server** page.



EDIT SYSLOG SERVER

Delete server

Description  
Gateway PC (VLAN IP)

Server Address  
10.220.1.123

Protocol  
UDP TCP

Port  
514

Minimum Log Severity Level  
6 - Info

All messages with a severity level equal or with a greater severity will be sent to the remote server

Send Serial Port Logs  
Enabled Disabled

Cancel Submit

## Session Settings

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

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

- **Web GUI 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 at the next login via the CLI.

When completed, click the **Apply** button to save the settings.

### SESSION SETTINGS

#### SETTINGS

Web Session Timeout

Web session idle timeout (in minutes)

CLI Session Timeout

CLI session idle timeout (in minutes). Note: To disable the CLI session idle timeout, set it to 0.

**Apply**

## Firewall

[CONFIGURE > FIREWALL](#)

In the **CONFIGURE > FIREWALL** menu you can configure:

- **Firewall Management**
- **Interzone Policies**
- **Services**

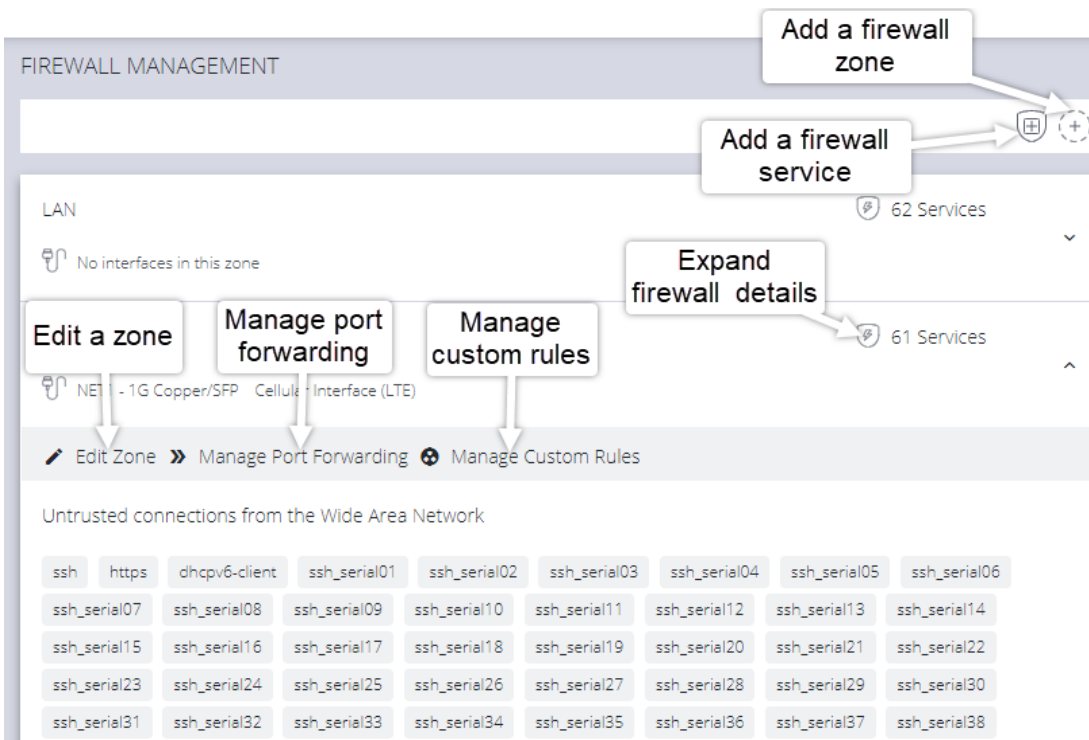


# Firewall Management

[CONFIGURE > FIREWALL > Management](#)

Navigate to the Firewall Management page, **CONFIGURE > FIREWALL > Management**, from here you can:

- Add a new firewall zone.
- Add a firewall service.
- Edit a firewall zone - manage the zone setup.
- Manage port forwarding.
- Manage custom rules for firewalls.



**Figure:** Firewall Management main page

## Firewall Zone Settings

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

You can inspect details of any zone by clicking the **Expand** icon to the right of the zone. Once expanded, you can click **Edit Zone** to change settings for a particular zone.

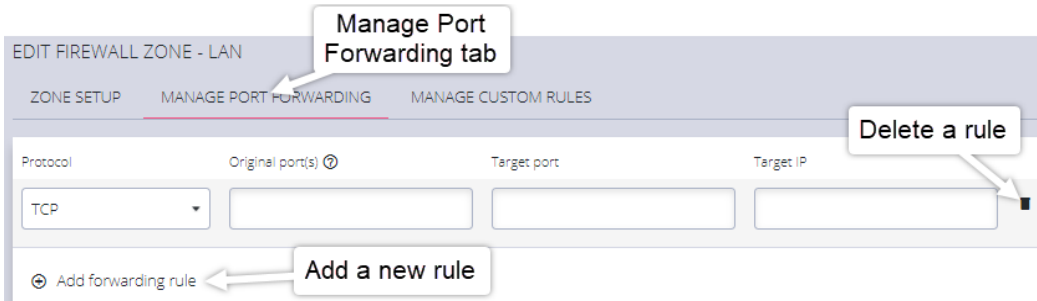
The **Edit Zone** page has three tabs. The **ZONE SETUP** page allows you to:

- 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.

**Tip:** You can use the **Filter Interfaces** and **Filter Available Services** text boxes to limit the list content that is displayed.

## Port Forwarding

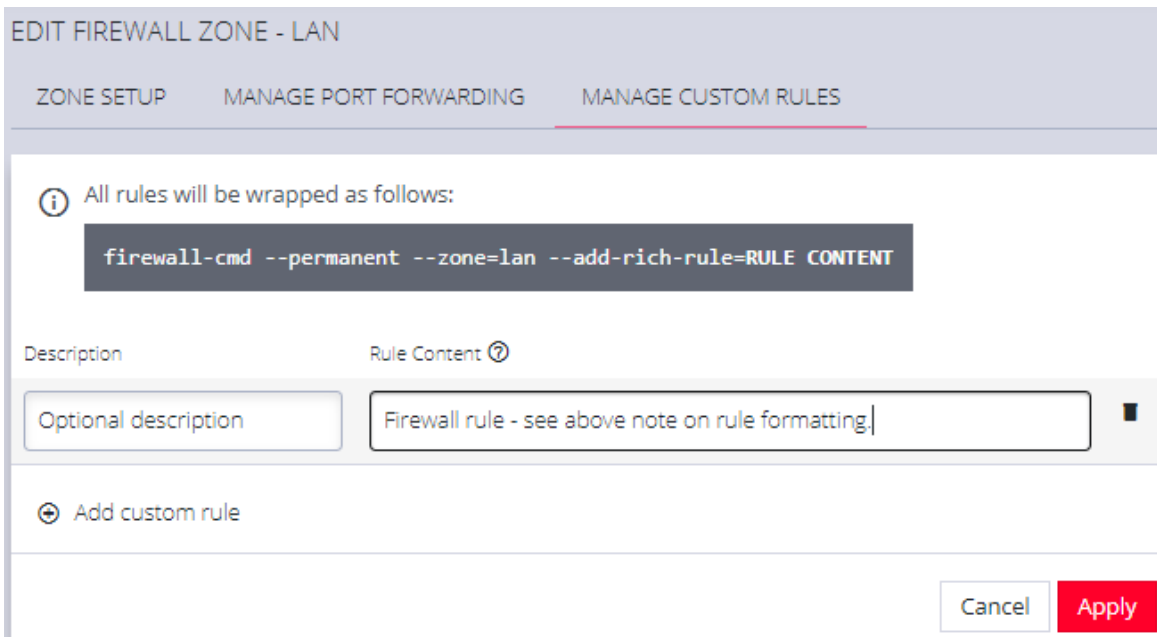
The **MANAGE PORT FORWARDING** tab allows you to add, edit, and delete forwarding rules for the particular zone you are editing.



## Manage Custom Rules

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.



EDIT FIREWALL ZONE - LAN

ZONE SETUP    MANAGE PORT FORWARDING    **MANAGE CUSTOM RULES**

*i* All rules will be wrapped as follows:

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

Description                      Rule Content *?*

Optional description              Firewall rule - see above note on rule formatting

+ Add custom rule

Cancel    **Apply**

To add a new custom rule:

1. Click **Add custom rule**.
2. Enter an optional description for this rule.
3. Enter the rule content, custom rule content formatted with firewall-cmd syntax.
4. Click **Apply**.

**Note:** All rules will be wrapped as follows:

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

## 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

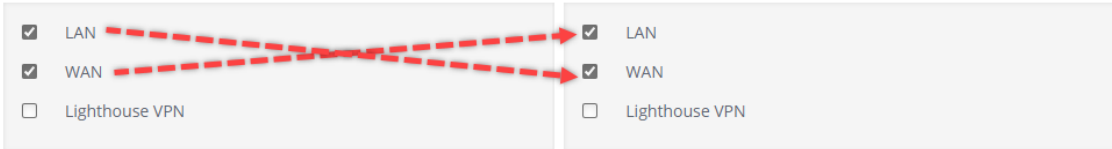
[CONFIGURE > FIREWALL > Interzone Policies > New Interzone Policy](#)

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.

- In the **Description** field provide a detailed description of this interzone policy (optional).
- 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 in 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



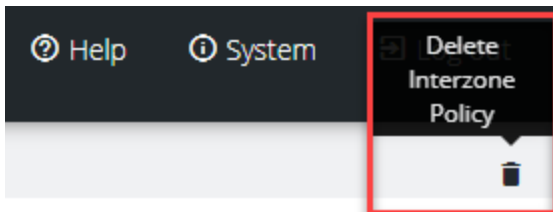
**Note:** Additional zones may be added to the zones list at: [CONFIGURE > FIREWALL > Management > New Firewall Zone](#).  
Zone customized rules may be edited at [CONFIGURE > FIREWALL > Management > Firewall Management](#).

- 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 161.

## Date & Time

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

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

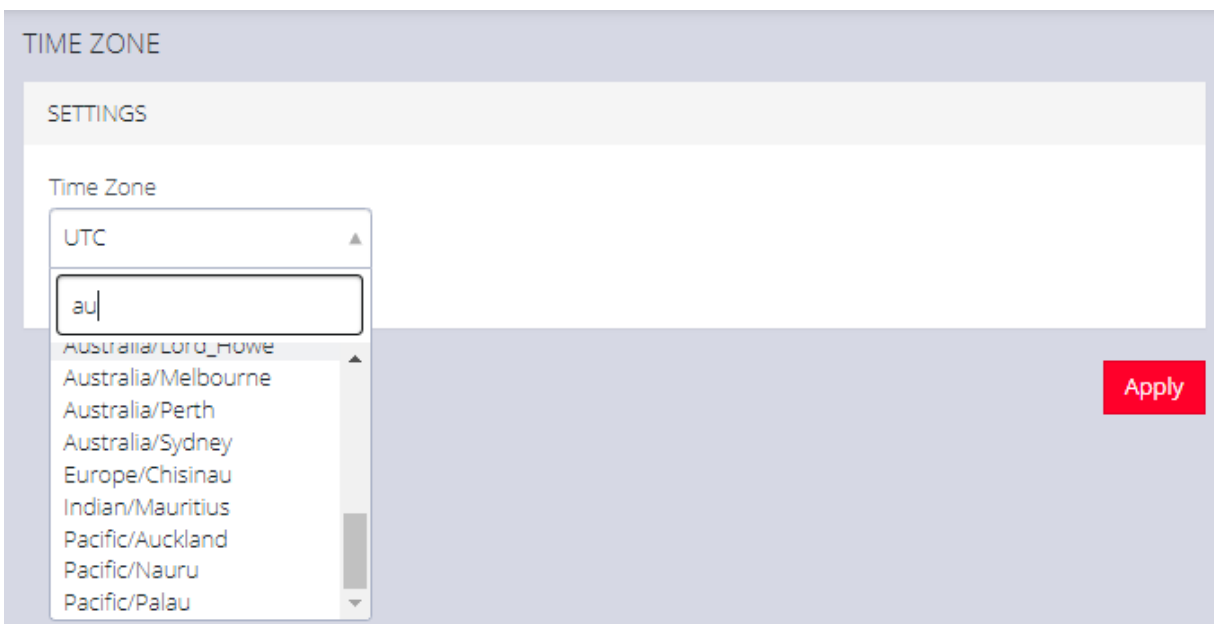
- Set the time zone
- Manually set the correct time and date
- Automatically set the date and time

## Time Zone

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

To set the time zone:

1. Navigate to the **CONFIGURE > DATE & TIME > Time Zone** page.
2. Select the Operations Manager's time-zone from the **Time Zone** drop-down list. A filter is provided to make selection easier.
3. Click **Apply**.



TIME ZONE

SETTINGS

Time Zone

UTC

au

Australia/Lord\_Howe

Australia/Melbourne

Australia/Perth

Australia/Sydney

Europe/Chisinau

Indian/Mauritius

Pacific/Auckland

Pacific/Nauru

Pacific/Palau

Apply

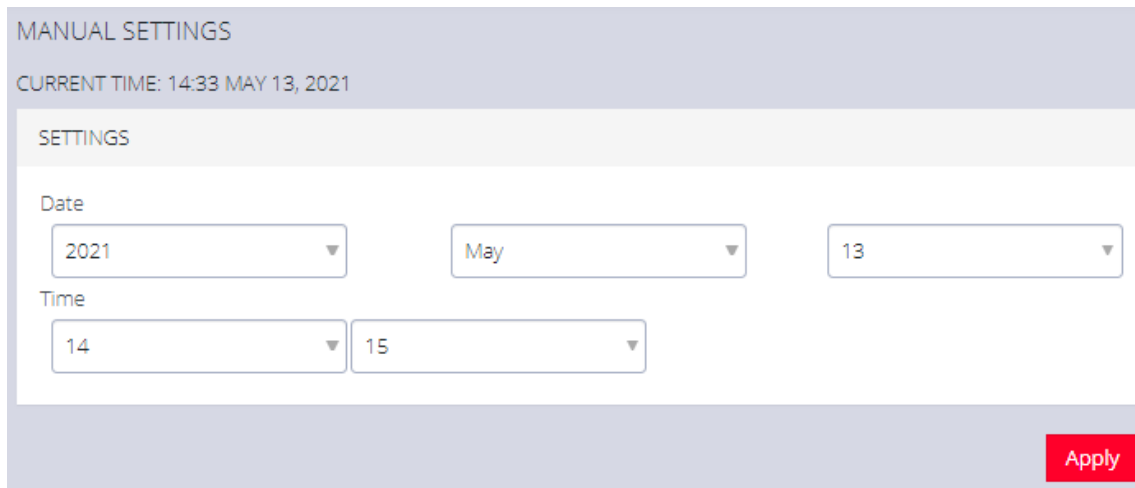


## Manual Settings

[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**.



MANUAL SETTINGS

CURRENT TIME: 14:33 MAY 13, 2021

SETTINGS

Date

2021 May 13

Time

14 15

Apply

The screenshot shows a web interface for manual settings. At the top, it says 'MANUAL SETTINGS' and 'CURRENT TIME: 14:33 MAY 13, 2021'. Below this is a 'SETTINGS' section. Under 'Date', there are three dropdown menus: the first is set to '2021', the second to 'May', and the third to '13'. Under 'Time', there are two dropdown menus: the first is set to '14' and the second to '15'. A red 'Apply' button is located at the bottom right of the settings area.

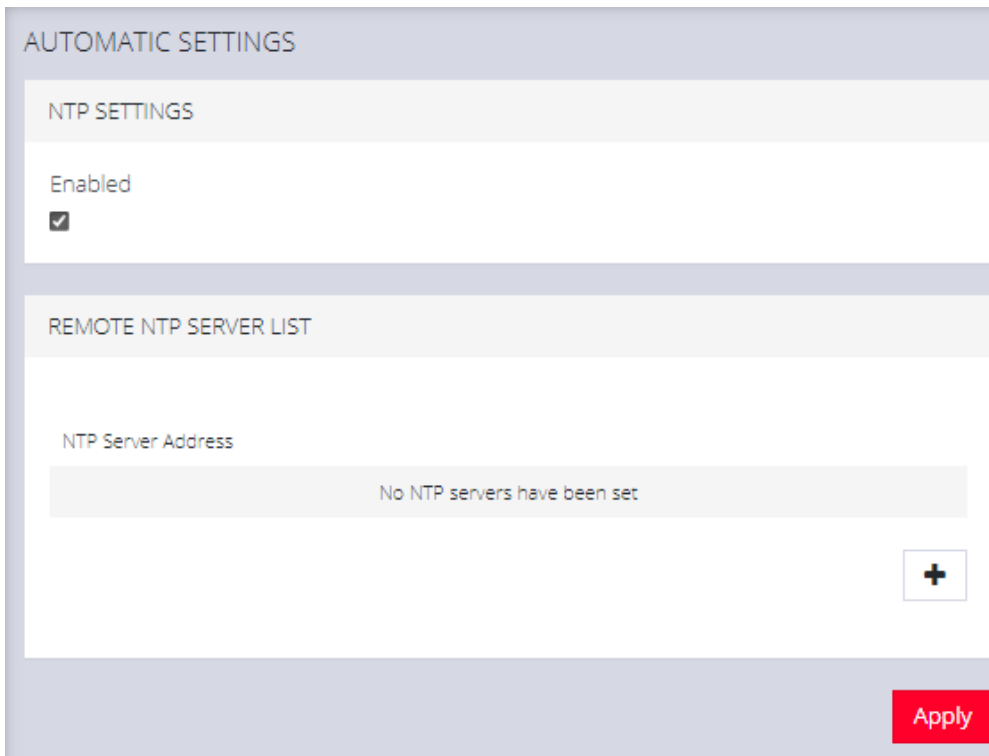
**Note:** When Automatic time setting is enabled, the manual settings are ignored and only automatic settings are applied. Devices enrolled in Lighthouse must be on the same time zone.

## 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**.



AUTOMATIC SETTINGS

NTP SETTINGS

Enabled

REMOTE NTP SERVER LIST

NTP Server Address

No NTP servers have been set

+

Apply

**Note:** When Automatic time setting is enabled, the manual settings are ignored and only automatic settings are applied. Devices enrolled in Lighthouse must be on the same time zone.

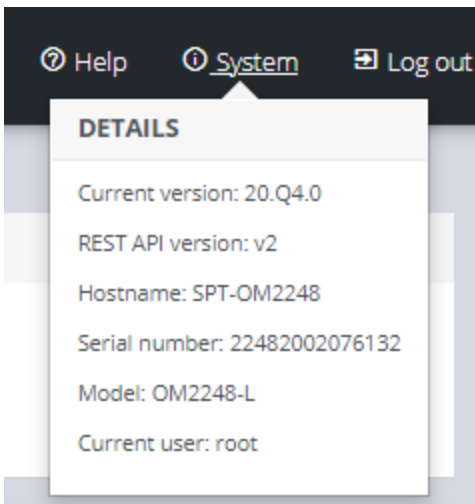
## System

### CONFIGURE > SYSTEM

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

### Check System Details

To ascertain current system details click on the System link at the top-right of the OM window.



## 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.



The screenshot shows the 'ADMINISTRATION' settings page. It features a 'SETTINGS' section with three input fields: 'Hostname' (containing 'SPT-OM2248'), 'Contact' (containing 'support@opengear.com'), and 'Location' (containing 'Unspecified (Configure under System Administration)'). Each field has a descriptive label below it. A red 'Apply' button is located at the bottom right of the settings area.

3. Click **Apply**, the new settings are saved.

## 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:

1. Navigate to **CONFIGURE > SYSTEM > Reboot**.
2. Select **Proceed with the reboot**,
3. Click **Reboot**.

REBOOT

WARNING

Please check the box below to confirm you wish to proceed. The appliance will reboot and will be unreachable for several minutes.

Proceed with the reboot

Reboot

## Export Configuration

The current system configuration can be downloaded as a plain text file. It contains all configuration performed via the Web UI and the ogcli tool.

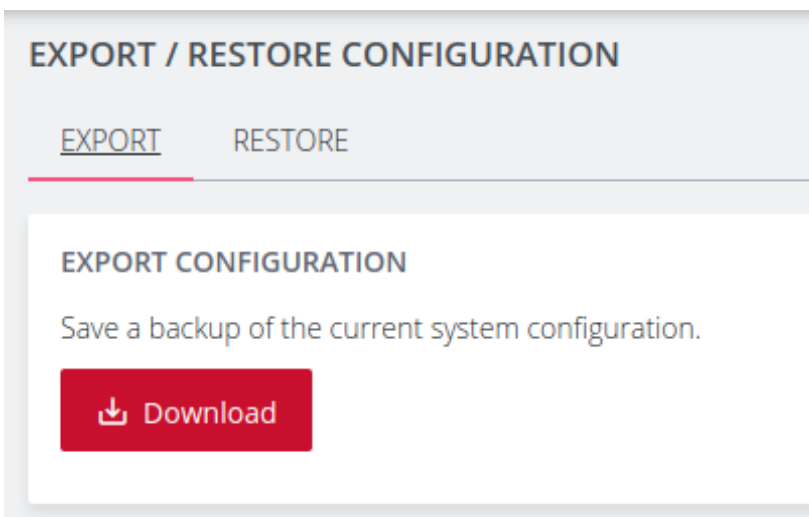
It does not contain log files, user scripts, docker containers, service configuration or other files stored via other means.

The exported configuration may be useful for:

- disaster recovery
  - issues with system upgrades
  - unexpected configuration changes
- replacing devices after RMA
- configuration templating

### Export Configuration via Web UI

[CONFIGURE](#) > [SYSTEM](#) > [Export / Restore Configuration](#)



To export the system configuration, click the **Download** button and save this file.

Sensitive data such as passwords and tokens will be obfuscated in the configuration export.

**Note:** The default filename includes the system hostname and a timestamp.  
For example, **om2248\_20210910\_config.txt**

## Export Configuration via ogcli

The system configuration can also be exported using the ogcli tool.

As an administrative user, run the following command:

```
ogcli export <file_path>
```

## Control The Export Of Sensitive Data

The display of sensitive data during export via ogcli can be controlled by modifying the ogcli command:

- To display secrets in cleartext, run:

```
ogcli --secrets=cleartext export <file_path>
```

- To display obfuscated secrets, run:

```
ogcli --secrets=obfuscate export <file_path>
```

- To display secrets masked with **\*\*\*\*\***, run:

```
ogcli --secrets=mask export <file_path>
```

**Caution:** Configuration exported with **--secrets=mask** cannot be used to import configuration.





## Lighthouse Node Backup

Configuration export can be scheduled to be performed periodically using the Lighthouse Node Backup feature.

For more details, consult the Lighthouse User Guide:

<https://opengear.com/support/documentation/>

## Import Configuration

Exported system configuration can be imported to the device using the Web UI or ogcli tool.

**Note:** If the configuration was exported using `--secrets=mask`, it cannot be used for configuration import.

**Note:** It may take up to ten minutes to import a config file with a large amount of configuration.

## Restore Configuration Via Web UI

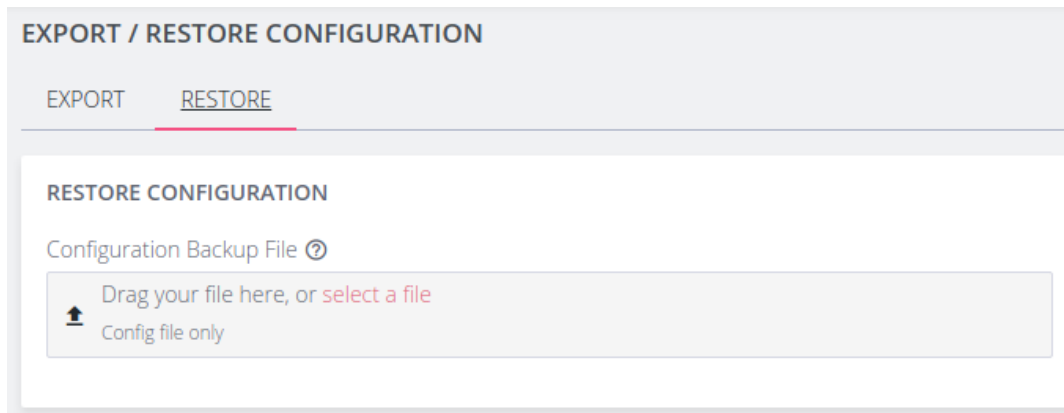
[CONFIGURE > SYSTEM > Export / Restore Configuration](#)

Importing configuration using the Web UI will use the restore strategy. Restoring configuration will override all settings on the device.

Only configuration from the same version and device model can be restored.

To restore the system configuration:

1. Click the **Restore** tab



**EXPORT / RESTORE CONFIGURATION**

EXPORT RESTORE

**RESTORE CONFIGURATION**

Configuration Backup File ⓘ

⬆ Drag your file here, or [select a file](#)

Config file only


2. Select the configuration file to import.
3. Review the configuration by clicking the arrow to display the file content.

**RESTORE CONFIGURATION**

Configuration Backup File ⓘ

**REVIEW UPLOAD**

---

 om2216\_20211117\_config.txt ▼

4. Click the **Upload File** button to start the import process.
5. A green banner will display when the configuration import is successful.

## Import Configuration via ogcli

The system configuration can also be imported using the ogcli tool. Either the import or restore strategies can be used.

### Import Configuration

Configuration that is imported using the `ogcli import` command will be merged with the current system configuration, preserving the current values and adding missing entries from the exported configuration where required.

As an administrative user, run the following command:

```
ogcli import <file_path>
```

### Restore Configuration

Configuration that is imported using the `ogcli restore` command will replace the current system configuration. The resulting system configuration will reflect what is in the exported configuration.

As an administrative user, run the following command:

```
ogcli restore <file_path>
```

## 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 upgrade process, the system will be unavailable for several minutes and then reboot. Unlike a factory reset, users, and other configuration data is maintained after the upgrade.

SYSTEM UPGRADE

SYSTEM UPGRADE

During the upgrade, the appliance will reboot and will be unreachable for several minutes.  
*System images must have the extension .roucb.*

Upgrade Method

Fetch image from HTTP/HTTPS Server

Fetch image from HTTP/HTTPS Server

Upload image

ADVANCED OPTIONS

Upgrade Options

*Only use at the request of Support*

Perform Upgrade

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**.

*Continued...*

## Upgrade Via Fetch From Server

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**.

## Upgrade Via Upload

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.

## SNMP

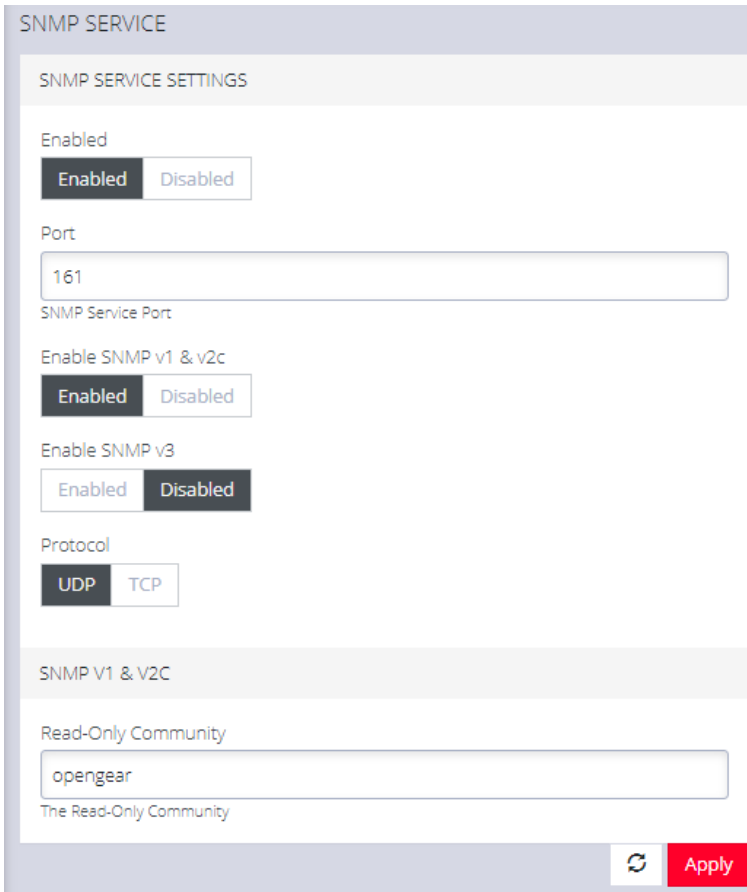
### [CONFIGURE > SNMP](#)

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.



The screenshot shows the 'SNMP SERVICE' configuration page. It is divided into two main sections: 'SNMP SERVICE SETTINGS' and 'SNMP V1 & V2C'. In the 'SNMP SERVICE SETTINGS' section, there are several controls: 'Enabled' (radio buttons for 'Enabled' and 'Disabled', with 'Enabled' selected), 'Port' (a text input field containing '161'), 'Enable SNMP v1 & v2c' (radio buttons for 'Enabled' and 'Disabled', with 'Enabled' selected), 'Enable SNMP v3' (radio buttons for 'Enabled' and 'Disabled', with 'Disabled' selected), and 'Protocol' (radio buttons for 'UDP' and 'TCP', with 'UDP' selected). The 'SNMP V1 & V2C' section contains a 'Read-Only Community' text input field with the value 'opengear'. At the bottom right of the form, there is a refresh icon and a red 'Apply' button.

SNMP Service 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.

See the "[Multiple SNMP Alert Managers](#)" on the next page feature for information about configuring more than one SNMP manager.

On this page, you can set the following:

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

To create a new SNMP manager:

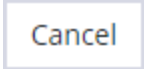


1. Navigate to **Configure > SNMP > SNMP Alert Managers**.
2. Click the **Add New SNMP Manager** button (a plus character in the top-right of the window)
3. Complete the new **SNMP Alert Manager Form** as per the **Definitions** table below.
4. Click the **Submit** button. A banner appears confirming 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

## Opengear CLI Guide

The **ogcli** command line tool is used for getting and setting configuration, and for retrieving device state and information. The purpose of ogcli is perform a single operation and exit. Operations are performed on a single entity, a list of entities, or all entities. Entities in ogcli are collections of related information items that represent device state, information or configuration.

For a list of operations supported by ogcli, see the "[ogcli Operations](#)" section.

**Note:** ogcli is not an interactive shell, it runs a single command and exits.

### Getting Started with ogcli

The best way to get started with ogcli is to use the help command. Refer to the table below to access help topics within ogcli.

For detailed information about ogcli and how it works, view the ogcli help topic by running this command:

```
ogcli help ogcli
```

### Access ogcli Help and Usage Information

Help Command	Displays...
ogcli help	Basic ogcli help and usage information
ogcli help help	Detailed information about the help command
ogcli help operations	The full list of operations and a brief description of each
ogcli help entities	The full list of entities and a brief description of each



Help Command	Displays...
ogcli help syntax	How to get information into and out of ogcli
ogcli help ogcli	More detailed information about the ogcli tool
ogcli help usage	Common ogcli usage examples
ogcli help secrets	Detailed information about controlling the display of secrets in ogcli.
ogcli help <operation>	A description and example usage of a specific ogcli operation
ogcli help <entity>	A description of a specific entity and the operations it supports
ogcli help <entity> <operation>	An example of how to perform a specific operation on a specific entity

## Basic Syntax

The ogcli tool is always called with an operation, with most operations also taking one or more arguments specifying an entity for the operation to act on.

```
ogcli <operation> [argument] [argument]
```

## ogcli Operations

Operation	Description
get	Retrieve a list or single item
replace	Replace a list or single item

Operation	Description
update	Update an item, supports partial edits
merge	Merge a provided list with existing config
create	Create an item
help	Display ogcli help
export	Export the system configuration
import	Import system configuration, merging with current system configuration
restore	Import system configuration, replacing the current system configuration

## Supplying Data To ogcli

For operations that modify an entity (e.g. 'update') the new information can be passed as inline positional arguments, but this quickly becomes cumbersome when setting a large number of fields. Information can instead be supplied through stdin by piping the contents of a file, or with Here Document (heredoc) style. The heredoc style is the most flexible format and is used extensively in ogcli examples.

### Here Document

A here document (heredoc) is a form of input redirection that allows entering multiple lines of input to a command. The syntax of writing heredoc takes the following form:

```
ogcli [command] << 'DELIMITER'  
  
HEREDOC  
  
DELIMITER
```

- The first line starts with the `ogcli` command, followed by the special redirection operator `<<` and a delimiting identifier. Any word can be used as the delimiter, commonly 'EOF' or 'END'.
- The `HEREDOC` block can contain multiple lines of strings, variables, commands or any other type of input. Each line can specify one field to update.
- The last line ends with the delimiting identifier used above, indicating the end of input.

```
ogcli update user <username> << 'END'  
  description="operator"  
  enabled=false  
END
```

### Inline Arguments

Field data can be entered inline with the `ogcli` command as arguments, with each field separated by a space.

```
ogcli update user <username> enabled=false description=\"operator\"
```

### Pipes and Standard Input

The data can also be entered via `stdin` by piping the data to the `ogcli` command.

```
echo 'enabled=true description="operator"' | ogcli update user  
<username>
```

Alternatively, you can provide a file via input redirection with `<`.

```
echo 'enabled=true description="operator"' > partial_record
```

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

## Quoting String Values

All string fields require the argument to be specified with double quotes ". The shell can consume double quotes, so care must be taken when specifying strings to ensure the quotes are passed to ogcli as input.

1. Double quotes in heredoc do not need to be escaped.

```
ogcli update physif <device-identifier> << 'END'
description="test network"
END
```

2. Double quotes within single quotes do not need to be escaped.

```
ogcli update physif user <username> 'description="test user"'
```

3. Double quotes not within single quotes need to be escaped.

```
ogcli update physif user <username> description=\"test user\"
```

## Tab Completion

ogcli includes tab completion to assist with typing commands. When entering the start of a command, press the **<tab>** key to complete the phrase to the nearest match.

If there are multiple matches, all options will be displayed for your reference.

```
root@oml208-8e:~# ogcli get cel
cellmodem          system/cell_reliability_test
cellfw/info        cellmodem/sims      system/cellular_logging
```

## Displaying Secrets in ogcli

Fields containing sensitive information are called **secrets**, which are handled specially by **ogcli** to obfuscate their values when they are displayed or exported.

Passwords and private keys are examples of secret fields.

The obfuscation process provides protection against "casual observation" only and offers no cryptographic security. The **obfusc** tool can be used to obtain the clear text version of any obfuscated secret generated by any Operations Manager device.

For more information, view the secrets help topic by running:

```
ogcli help secrets
```

The default behavior is for secrets to be passed to ogcli in clear text, and exported or displayed in obfuscated form.

For example, setting the password:

```
ogcli update services/snmpd auth_password=\"my secret\"
```

Retrieving the password (note, the output is abridged):

```
# ogcli get services/snmpd  
auth_  
password="TkcxJAAAABBSB3xoFWhPA6B7sDrzq3HwaTOAO/jsURqFa0qa7hc3TA=="
```

This behaviour can be overridden to display sensitive fields in clear text, obfuscated form, or masked form using the **--secrets** option. The clear text and obfuscated forms are also accepted when supplying a sensitive field.

```
# ogcli --secrets=cleartext get snmpd  
auth_password="my_secret"
```

```
# ogcli --secrets=obfuscate get snmpd  
auth_password="my secret"
```

```
# ogcli --secrets=mask get snmpd  
auth_password="*****"
```

If an export is performed with the **--secrets=mask** option it is impossible to subsequently import the configuration, because the secrets have been removed.

## Common Configuration Examples

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.

Replace message of the day (MOTD) displayed at login

```
ogcli replace banner banner=\"updated message\"
```

Retrieve user record

```
ogcli get user <username>
```

Update item with field where value is a string

```
ogcli update user <username> description=\"operator\"
```

Update item with field where value is not a string

For example, a numeric or boolean value

```
ogcli update user <username> enabled=true
```

Export system configuration

```
ogcli export <file_path>
```

Import system configuration

```
ogcli import <file_path>
```

## Restore system configuration

```
ogcli restore <file_path>
```

## Enable local console boot messages

```
ogcli get managementports
```

```
ogcli update managementport mgmtPorts-1 kerneldebug=true
```

## Create new user

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

## Change root password

```
ogcli update user root password=\"oursecret\"
```



## Create new administrative user

```
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

```
ogcli update system/timezone timezone=\"America/New_York\"
```

```
ogcli update system/time time=\"15:30 Mar 27, 2020\"
```

## Enable NTP service

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

## Update system hostname

```
ogcli update hostname hostname=\"system-hostname\"
```

## Adjust session timeouts

```
ogcli update system/cli_session_timeout timeout=180
```

```
ogcli update system/webui_session_timeout timeout=180
```

## Setup remote authentication with TACACS+

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

## Setup remote authentication with Radius

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

## Create user group with limited access to serialports

```
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 connections

```
ogcli get conns
```

```
ogcli get conn system_net_conns-1
```

```
ogcli update conn system_net_conns-1 ipv4_static_
settings.address="192.168.0.3"
```

```
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
```

## Configure serial ports

```
ogcli get ports
```

```
ogcli get ports | grep label
```

```
ogcli get port ports-1
```

```
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 interface

```
ogcli get physifs
```

```
ogcli update physif wwan0 << 'END'  
enabled=true  
physif.cellular_setting.apn="broadband"  
physif.cellular_setting.ipv4v6="IPv4v6"  
END
```

## Disable cellular modem interface

```
ogcli update physif physif wwan0 enabled=false
```

## Enable remote syslog service

```
ogcli create services/syslog_server address="192.168.34.112"
```

```
ogcli create services/syslog_server << 'END'  
address="192.168.34.113"  
protocol="UDP"  
port=514  
END
```

## 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 buttons
	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	213
-----------------------	-----