Operations Manager User Guide

Table of Contents

About this User Guide

This user guide covers the Opengear Operation Manager products, including the OM2200 family of rack-mountable appliances (available with combinations of up to 48 serial ports and 24 Ethernet ports) and the OM1200 family of small form-factor appliances (available with combinations up to 8 serial and 8 Ethernet ports). This manual is up to date for the 20.Q2.0 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.

GLOSSARY

Terms used in this guide to define elements and concepts are listed below.

Term	Definition
AAA	Authentication, Authorization, and Accounting is a framework for intelligently controlling access to computer resources, enforcing policies, and auditing usage.
Dark Mode	Changes the user interface to display mostly dark colors, reducing the light emitted by device screens.
Enrollment	Connecting a node to Lighthouse
Enrollment Bundle	Used to assign a number of tags to a set of nodes when they

	are enrolled. During enrollment, the bundle is specified using its name, and a bundle-specific enrollment token.
Enrolled Node	Node that has been connected to Lighthouse and is ready for use.
Enrollment Token	A password that authorizes the node with Lighthouse. Used when performing Node-based, or ZTP enrollment.
Light Mode	Changes the user interface to display mostly light colors. This is the default UI setting.
Lighthouse	System for accessing, managing and monitoring Opengear console servers.
Lighthouse Enterprise	Offers an elevated centralized management solution with additional functionality. It supports growing trends such as edge computing and SD-WAN with High Availability and Remote IP Access.
Lighthouse VPN	The OpenVPN based connections that the Lighthouse instance has with the nodes it is managing
LocalAuth (Radius/LDAP/AAA)	When this authentication option is selected, if local authentication fails, the unit tries to authenticate the user using a remote AAA server.
Node	A device that can be enrolled with Lighthouse, allowing it to be accessed, managed, and monitored. Currently, Opengear console servers are supported on a standard license, with support

	for other vendors Console Servers available as an add-on.
Pending Node	A node that has been connected to Lighthouse and has been configured with a VPN Tunnel, but which has not yet been approved for access, monitoring, or management. The approval operation can be automated by configuring Lighthouse to auto- approve nodes.
Role	A set of access rights for a particular group.
Smart Group	Dynamic filter used to search for particular nodes, or for defining the access rights of a group of users. Smart Groups use node properties, as well as tags defined by users.
Tag	User-defined attribute and value that is assigned to one or more nodes. Tags are used when creating Smart Groups for filtering views or access to nodes.

1. Installation

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

1.1 Power Connection

The rack mountable units (OM2200) may be equipped with built-in single- or dual- AC or DC power supplies. The small form-factor units (OM1200) use a single external 12V power adapter.

OM2200 have dual universal AC power supplies 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 (multicounty clips) wall adapter.

1.2 Network Connection

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.

1.3 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.

1.4 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.

1.5 Reset and Erase

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.

2. Initial System Configuration

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

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

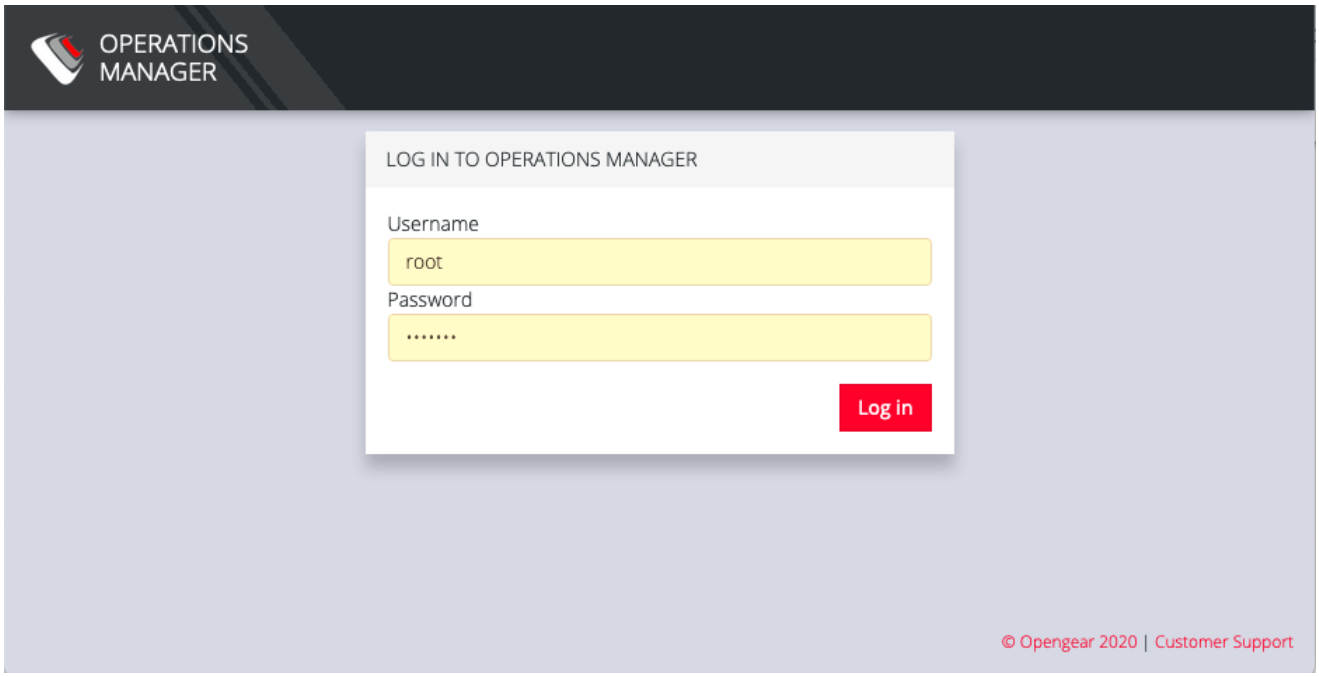
- Accessing the Management Console via Browser (WebGUI)
- Accessing the Management Console via CLI
- Changing the default Administrator password
- Changing network settings

2.1 Default Settings

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

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

1. Type https://192.168.0.1 in the address bar. HTTPS is enabled by default.

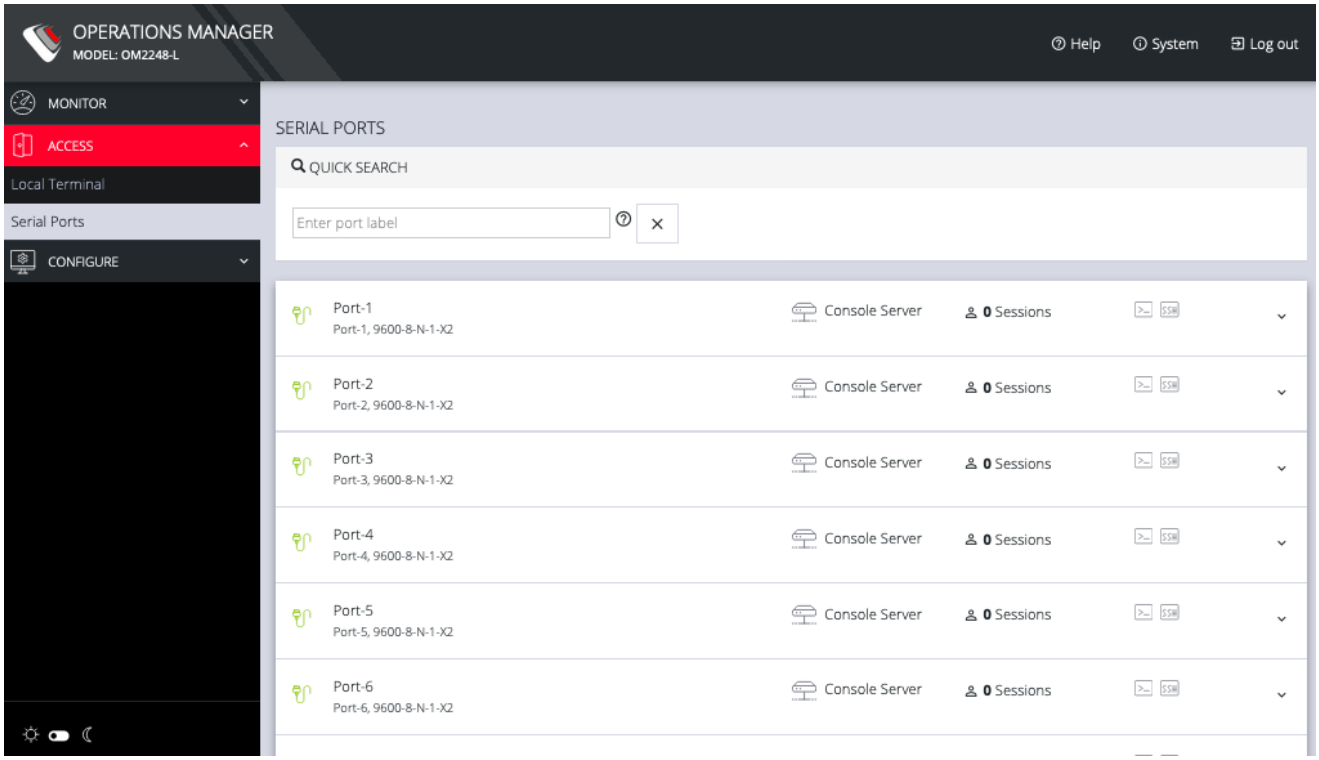


2. Enter the default username and password

   Username: root

   Password: default

3. After the first successful login you will be required to change the root password.
4. Next, you will be presented with the **ACCESS > Serial Ports** page that shows you a list of serial devices and links to a Web Terminal or SSH connection for each.



Using the WebUI

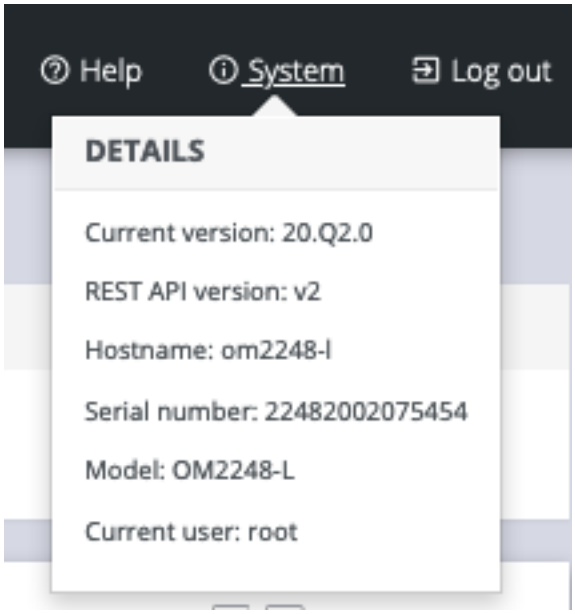
The WebUI can switched between **Light** or **Dark** mode by adjusting the toggle on the bottom left.

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

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

The **Help** menu contains a link to generate a **Technical Support Repor**t 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**.



2.2 Management Console Connection via CLI

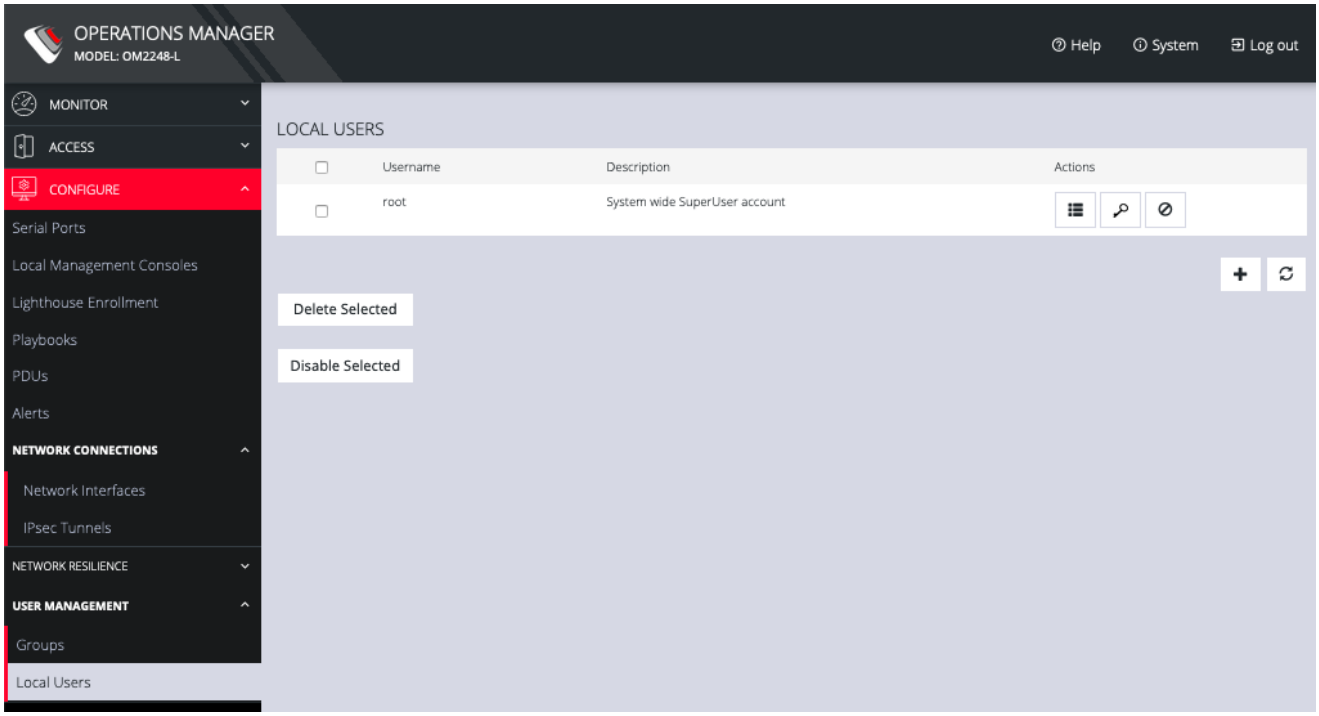
The Command Line Interface (CLI) is accessible using your preferred application to establish and SSH session.

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

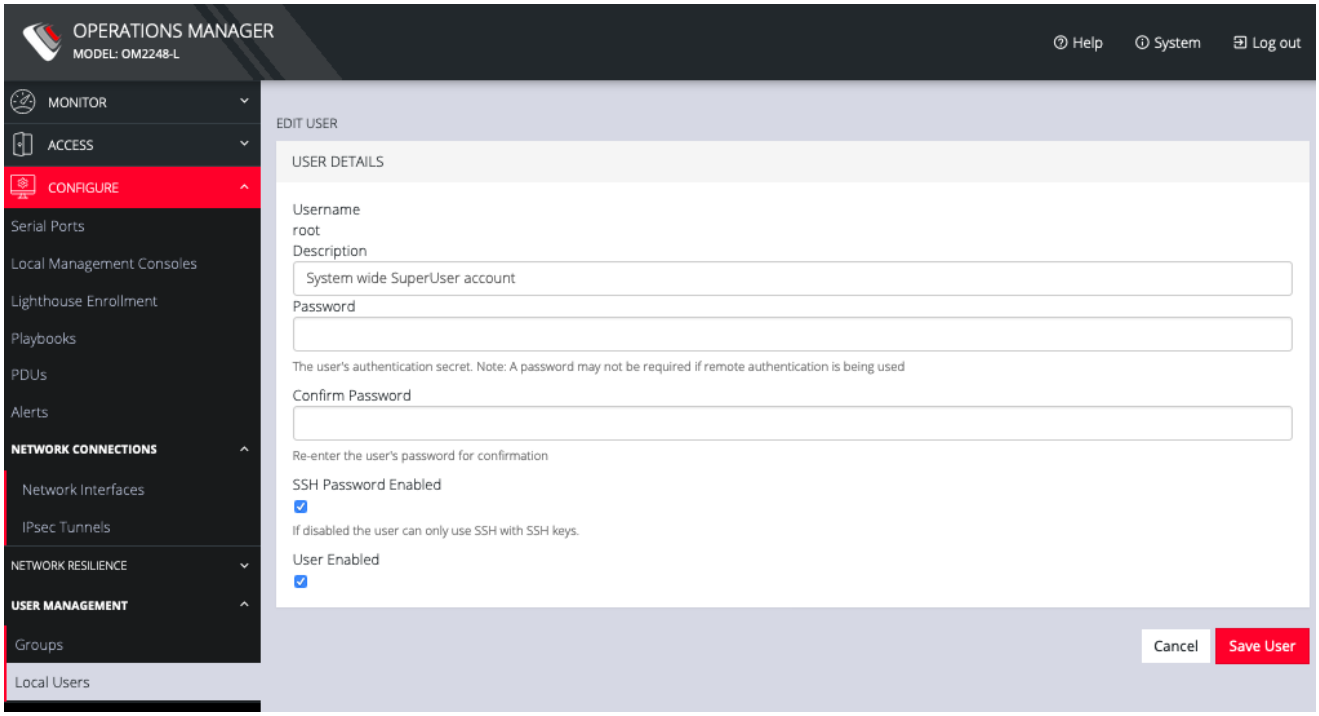
2.3 Changing the root password

For security reasons, only the root user can initially log into the appliance. Upon initial login the default password must be changed. To change the password at any time,

1. Click **CONFIGURE > User Management > Local Users**



2. Click the **Edit User** icon under **Actions**.



3. Enter a new password in the Password field and enter it again in the **Confirm Password** field.
4. Click **Save User**.

2.4 Disabling 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 Chapter 5.5.2 Local Users.

To disable a root user:

1. Click **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.

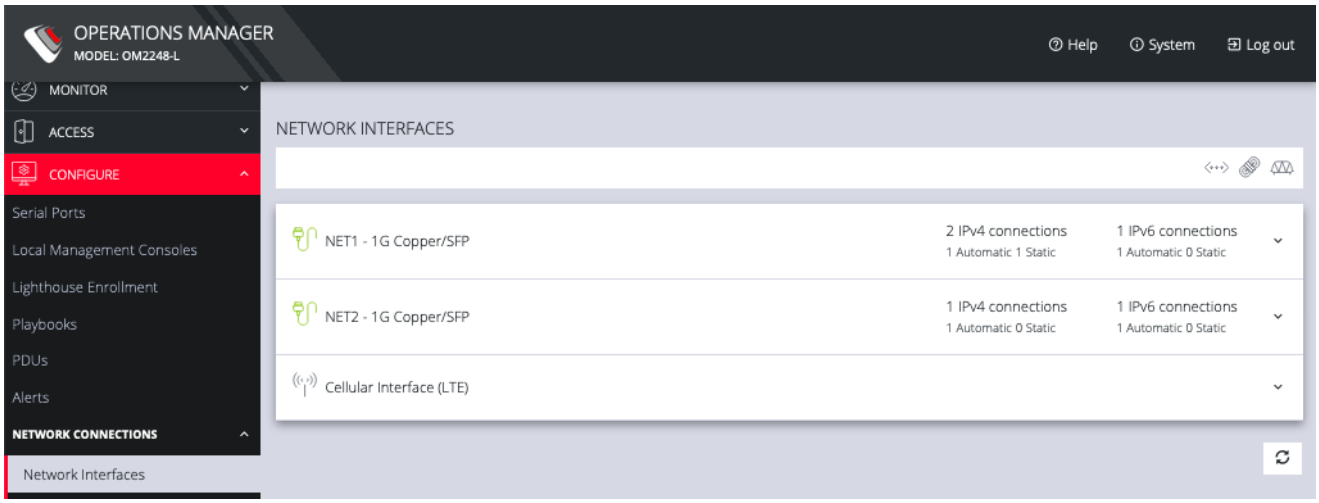
2.5 Changing Network Settings

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:

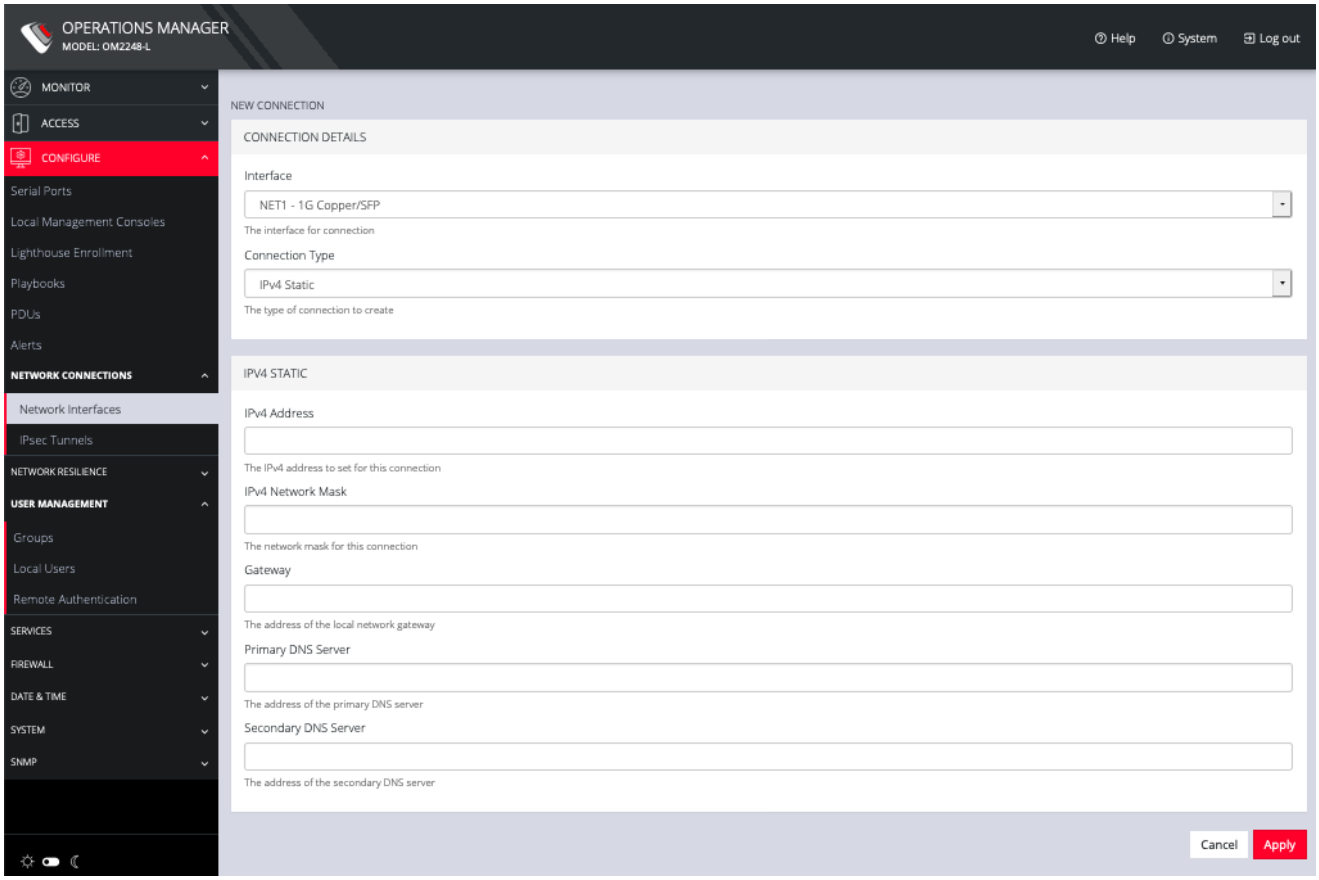
- IPv4, IPv6
- Static and/or DHCP
- Enabling or disabling network interfaces
- Ethernet Media types

To add a new connection:

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



2. Click the arrow to the right of the desired interface.
3. Click the plus icon to open the **New Connection** page.



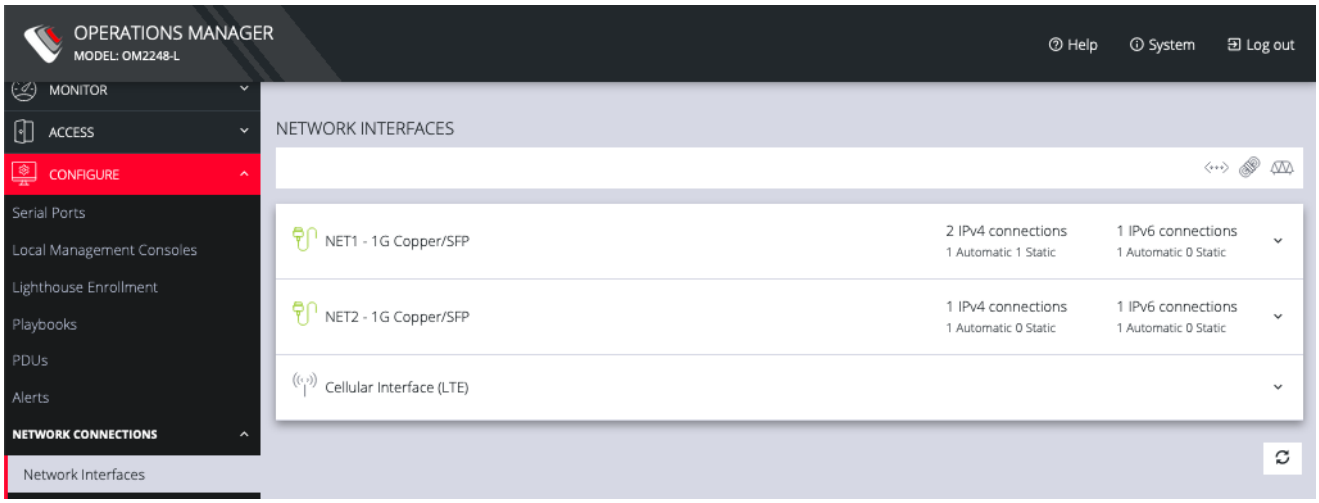
4. Select the Interface and Connection Type for your new connection.
5. The form on the bottom part of the page will change based on the **Connection Type** you choose. Enter the necessary information and click **Apply**.

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

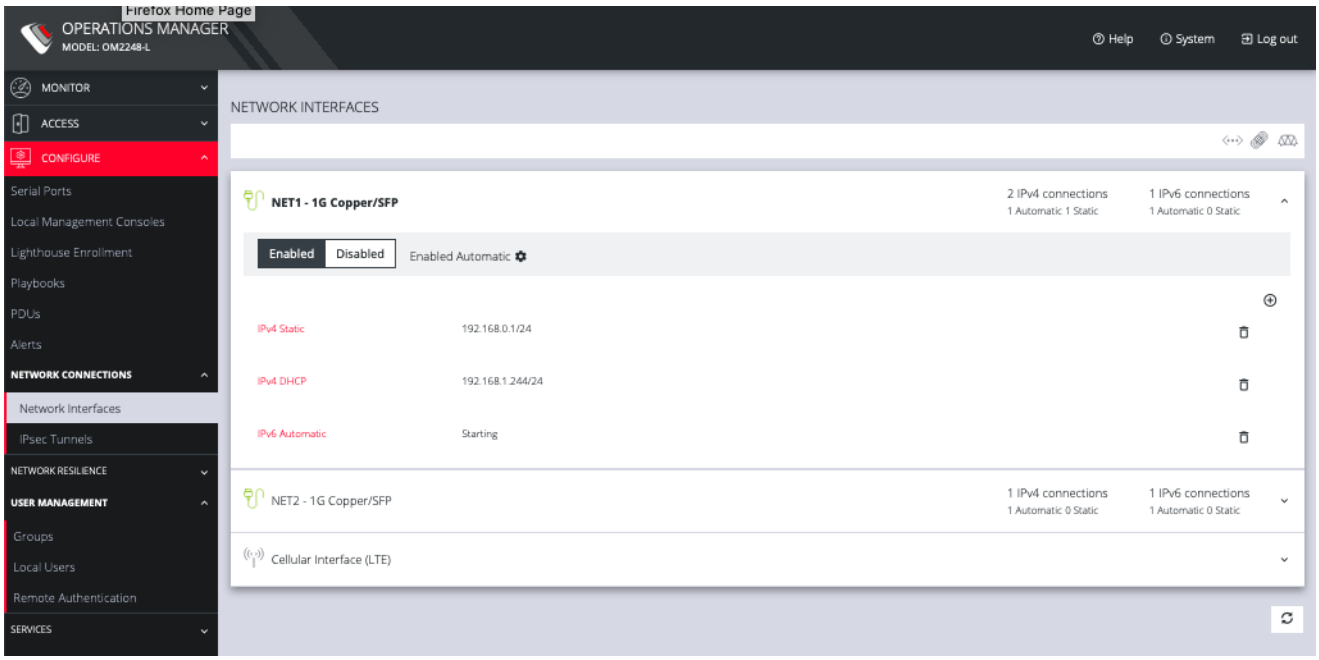
NOTE: If you experience packet loss or poor network performance with the default auto-negotiation setting, try changing the Ethernet Media settings on the OPERATIONS MANAGER and the device it is connected to. In most cases, select 100 megabits, full duplex. Make sure both sides are set identically.

To change the Ethernet Media Type:

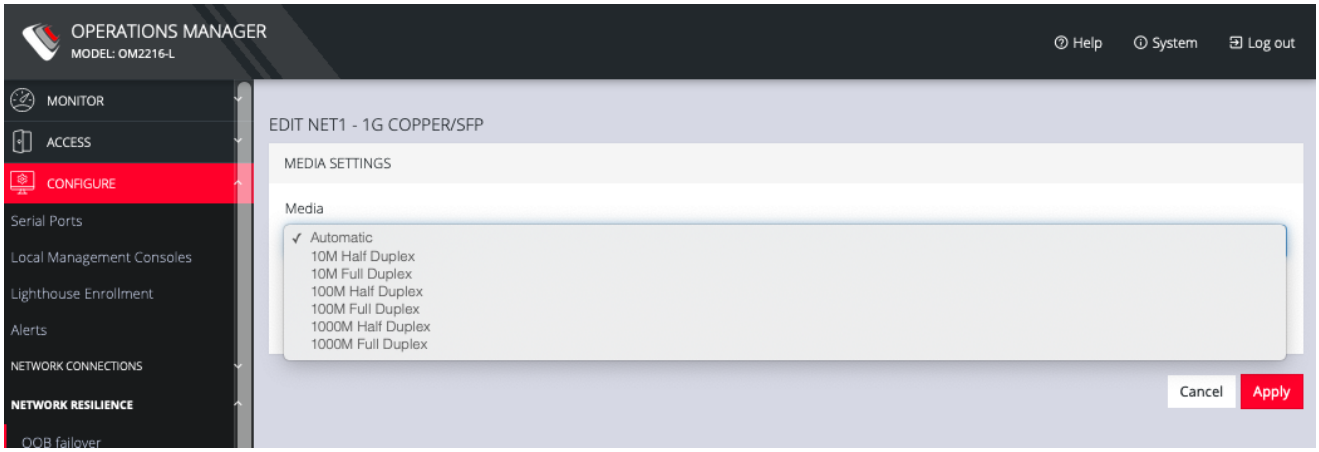
1. Click **CONFIGURE > Network Connections > Network Interfaces**



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



3. Click **Enabled Automatic**.



4. Change the Ethernet Media Type setting as needed and click **Apply**.

2.6 Configuring Serial Ports

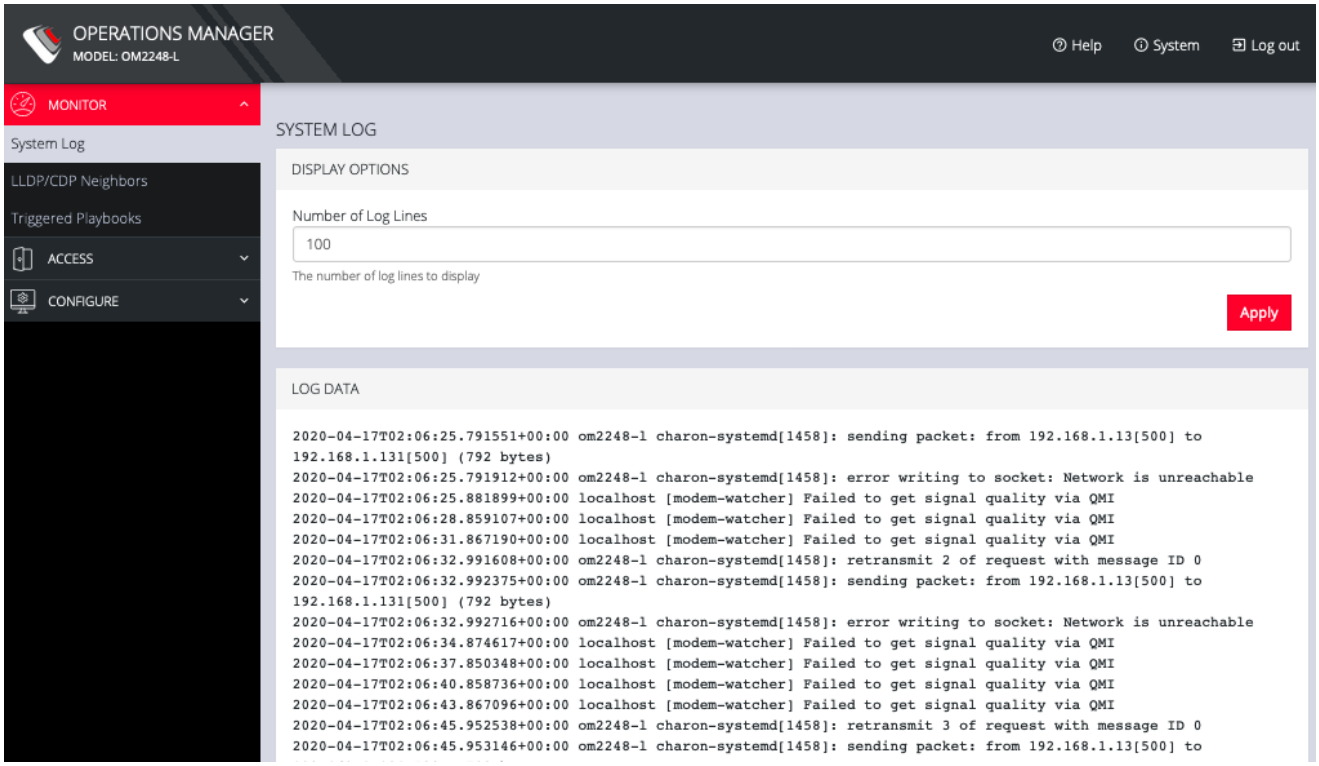
For information on configuring serial ports, see Chapter 5.1 Serial Ports.

3. MONITOR Menu

3.1 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.

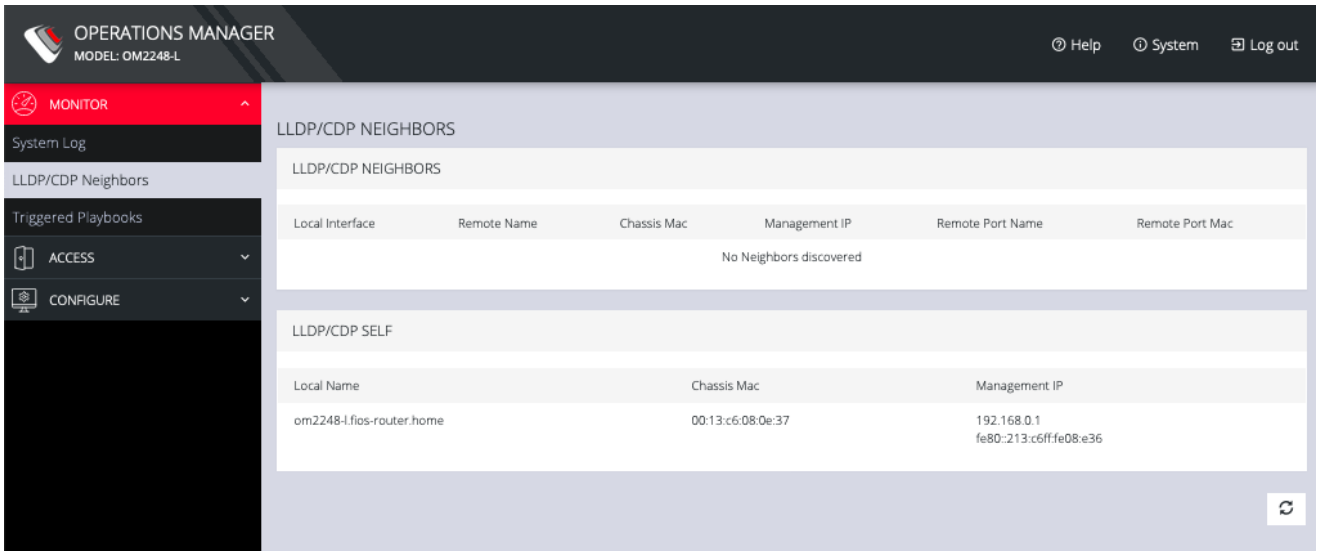
To view the System Log, click **MONITOR > System Log**.



The 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.

3.2 LLDP/CDP Neighbors

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



3.3 Triggered Playbooks

For information on creating **Playbooks**, see 5.5 Playbooks.

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

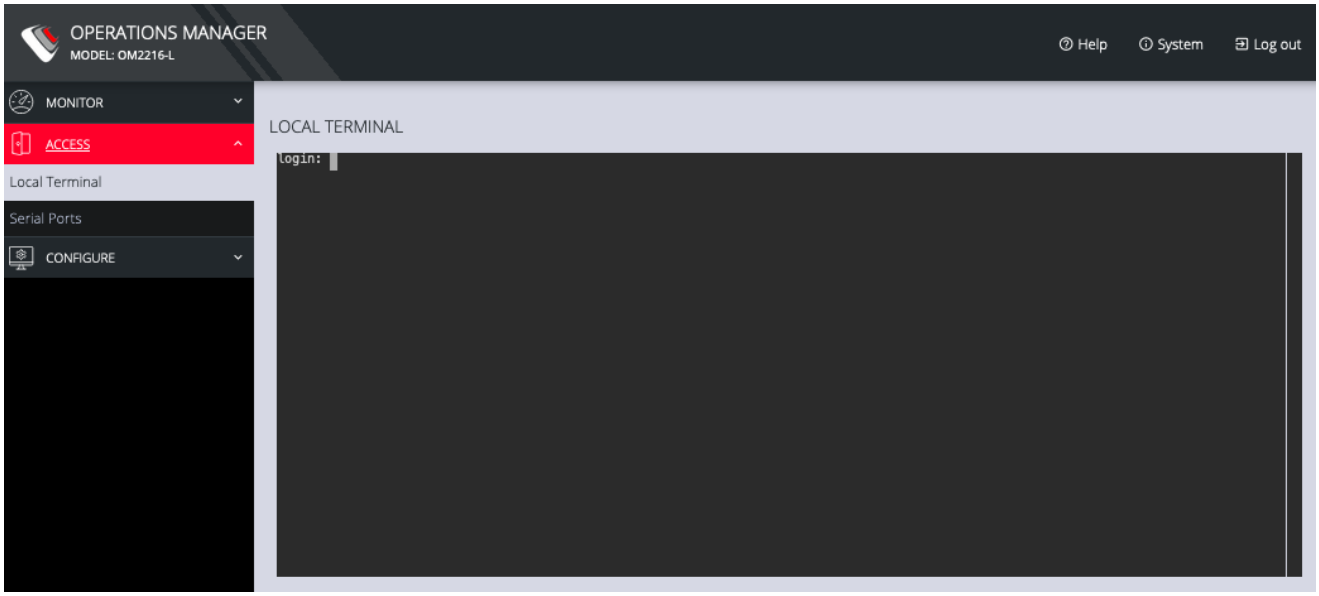
4. ACCESS Menu

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.

4.1 Using the Local Terminal

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

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



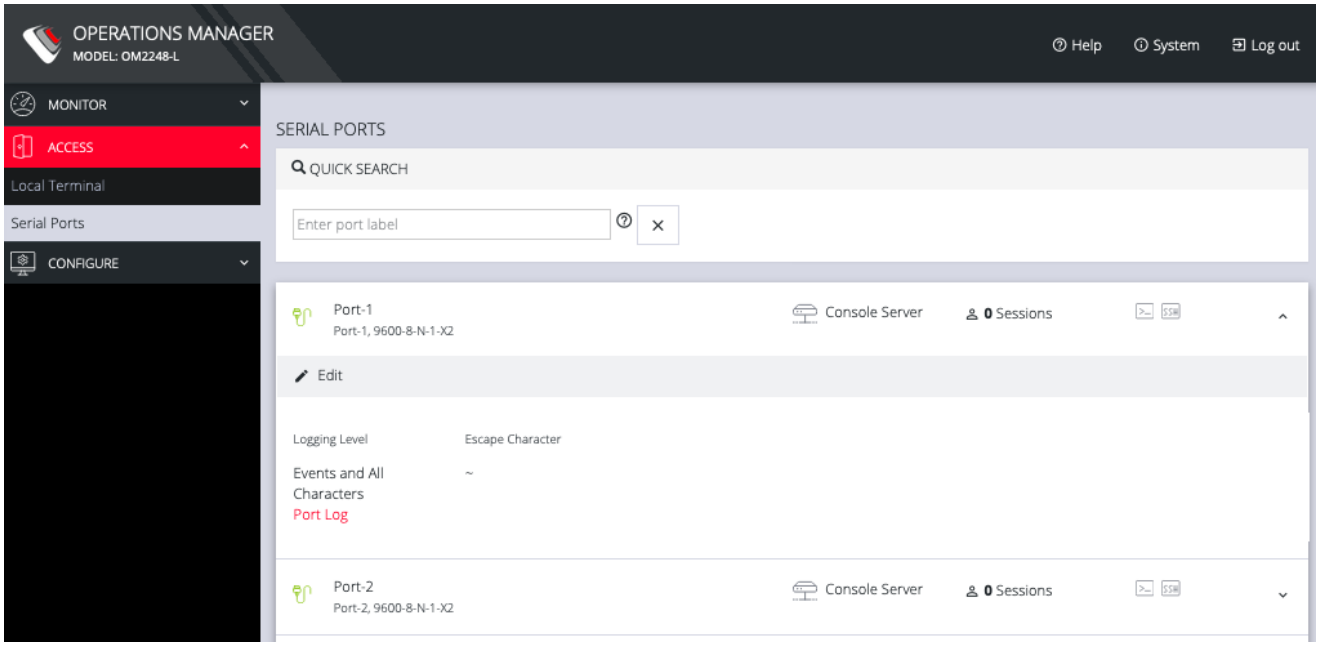
2. At the login prompt, enter a username and press Return.
3. At the password prompt, enter a password and press Return.
4. A bash shell prompt appears.

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

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

4.2 Accessing Serial Ports

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



4.2.1 Quick Search

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

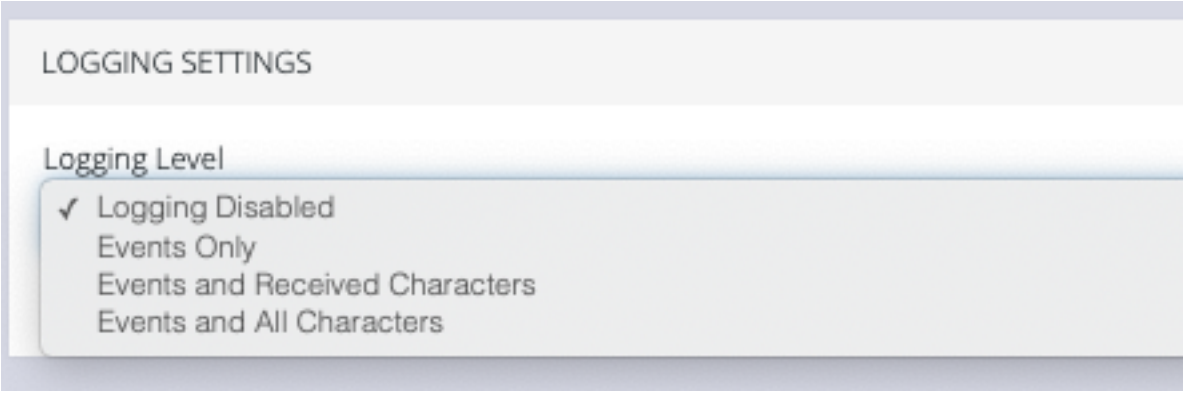
4.2.2 Accessing via Web Terminal or SSH

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

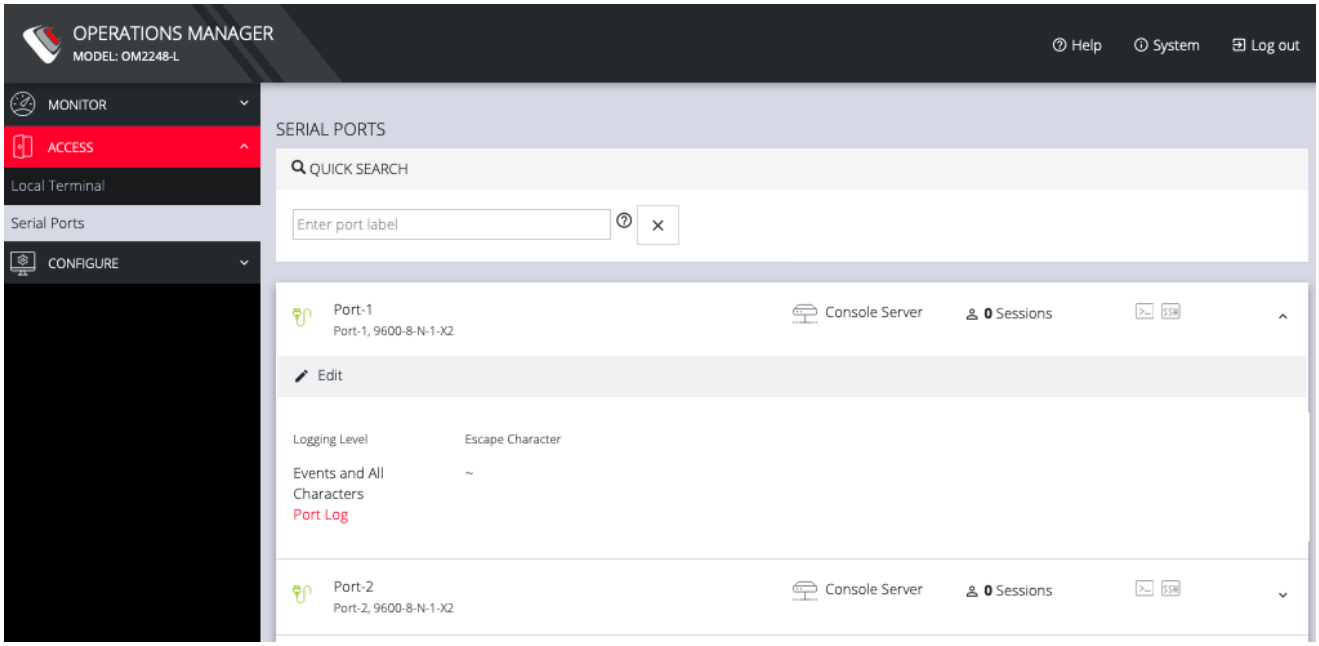
1. Locate the particular port on the **ACCESS > Serial Ports** page and click the expand arrow.
2. Click the **Web Terminal** or SSH link for the particular port.

- Choosing **Web Terminal** opens a new browser tab with the terminal.
- Choosing **SSH** opens an application you have previously associated with SSH connections from your browser.

NOTE: Serial port logging is disabled by default. You can control the level of logging for each serial port by changing Logging Settings on its **Configure > Serial Ports > Edit** page.



The log will then appear via the Port Log link for that port on the **ACCESS > Serial Ports** expanded page.


OPERATIONS MANAGER
MODEL: OM2248-L
Help
System
Log out
MONITOR
ACCESS
Local Terminal
Serial Ports
CONFIGURE
SERIAL PORTS
QUICK SEARCH
Enter port label
Port-1
Port-1, 9600-8-N-1-X2
Console Server
0 Sessions
Edit
Logging Level
Escape Character
Events and All Characters
Port Log
~
Port-2
Port-2, 9600-8-N-1-X2
Console Server
0 Sessions

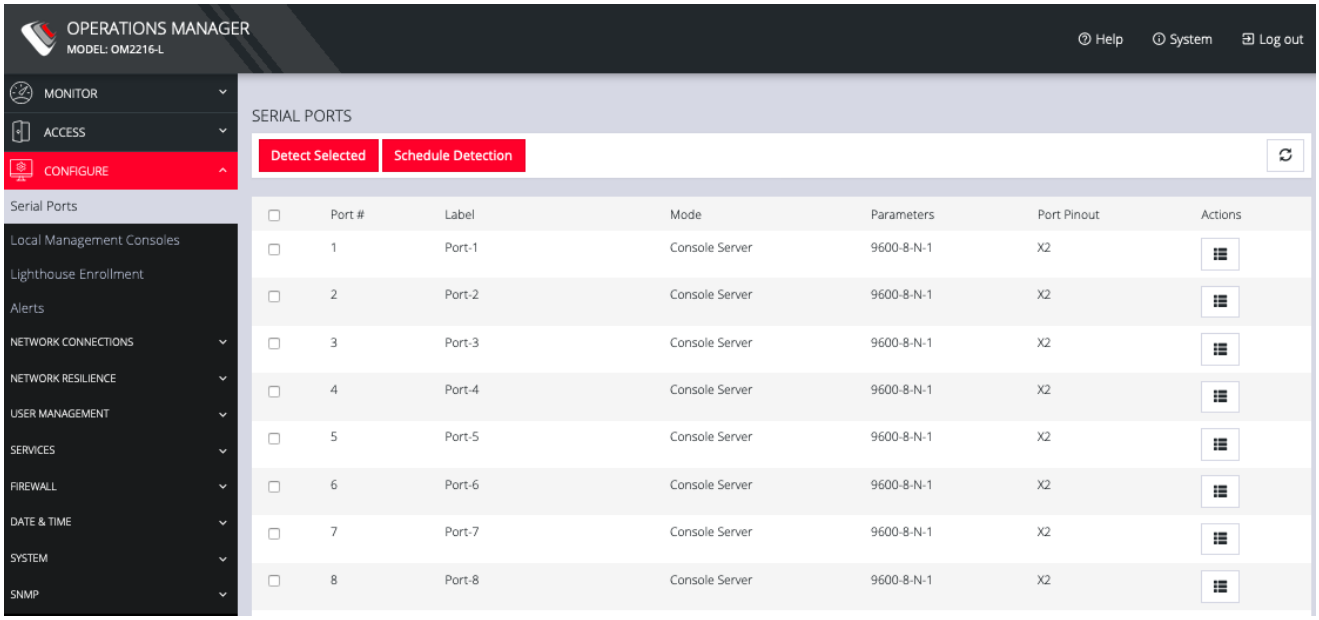
5. CONFIGURE Menu

This chapter provides step-by-step instructions for the menu items under the CONFIGURE menu. Configuration options include:

- Configuring serial ports
- Configuring the local management consoles
- Controlling interfaces and connections
- Enrolling the OPERATIONS MANAGER to Lighthouse
- Creating and managing Playbooks
- Monitoring Power Distribution Units (PDUs)
- Managing users, groups, and remote authentication
- Configuring network resilience
- Setting up services
- Managing firewall settings
- Setting date and time
- Managing system settings
- Configuring SNMP

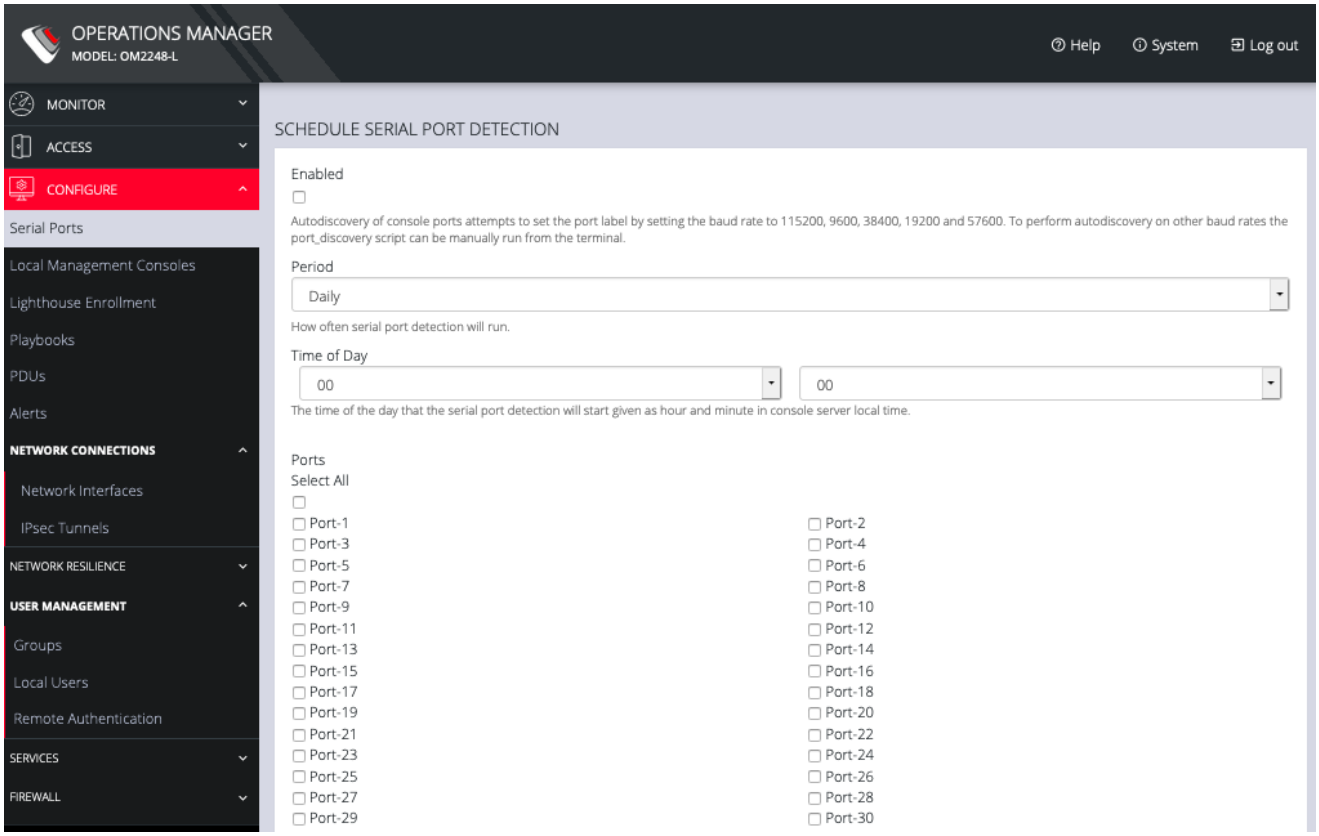
5.1 Serial Ports

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

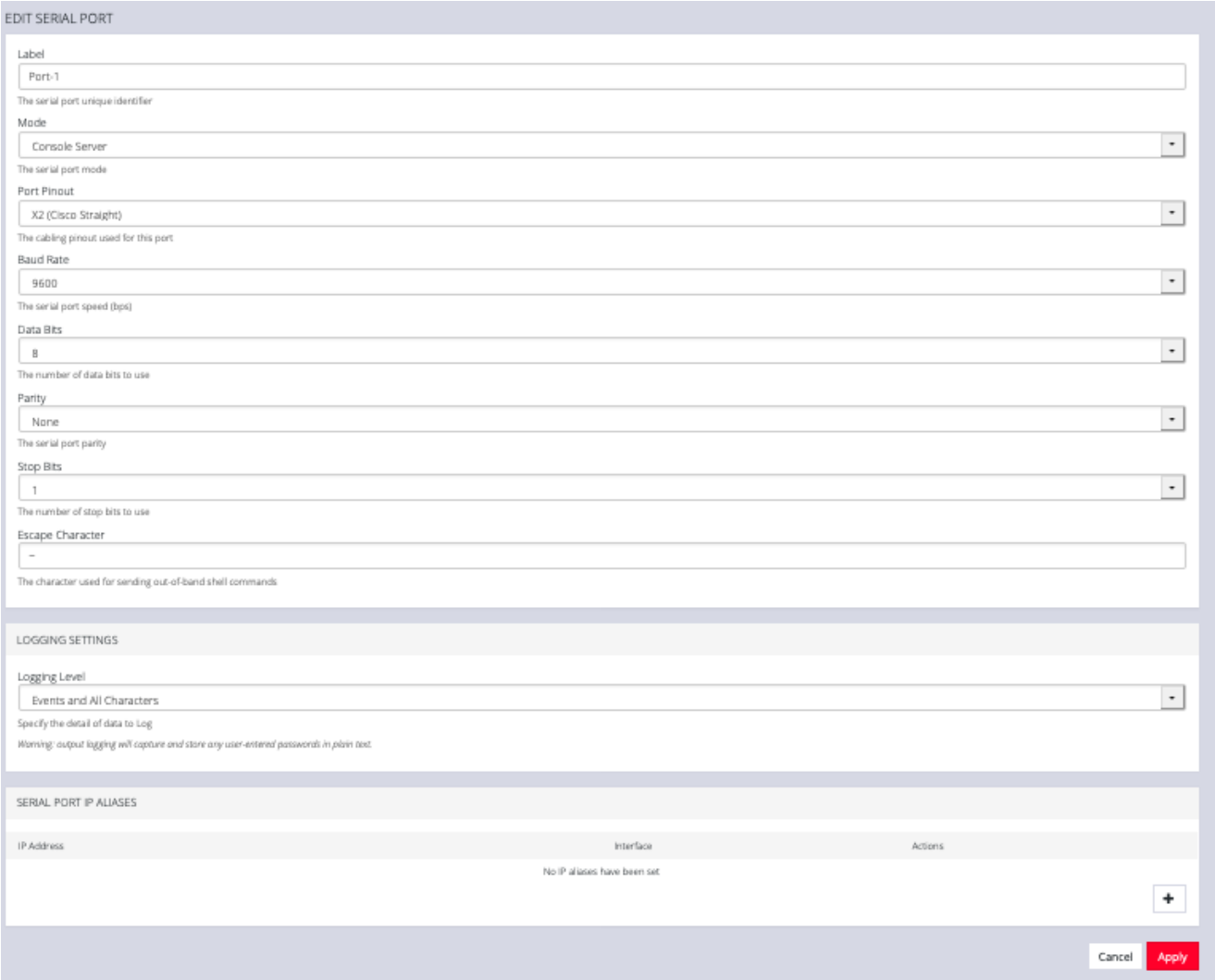


This page lets you select serial ports and **Detect Selected** ports.

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



Click the **Edit Serial Port** button under **Actions** next to the Serial Port you wish to configure. The **Edit Serial Port** page opens.



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

- Label: this can be used to locate this port using the **Quick Search** form on the **ACCESS > Serial Ports** page.
- **Mode**: **Disabled** or **Console Serve**r
- **Pin out**: **X1 Cisco Rolled** or **X2 Cisco Straight**
- **Baud Rate**: 50 to 230,400 bps
- **Data Bits**: 5, 6, 7, 8

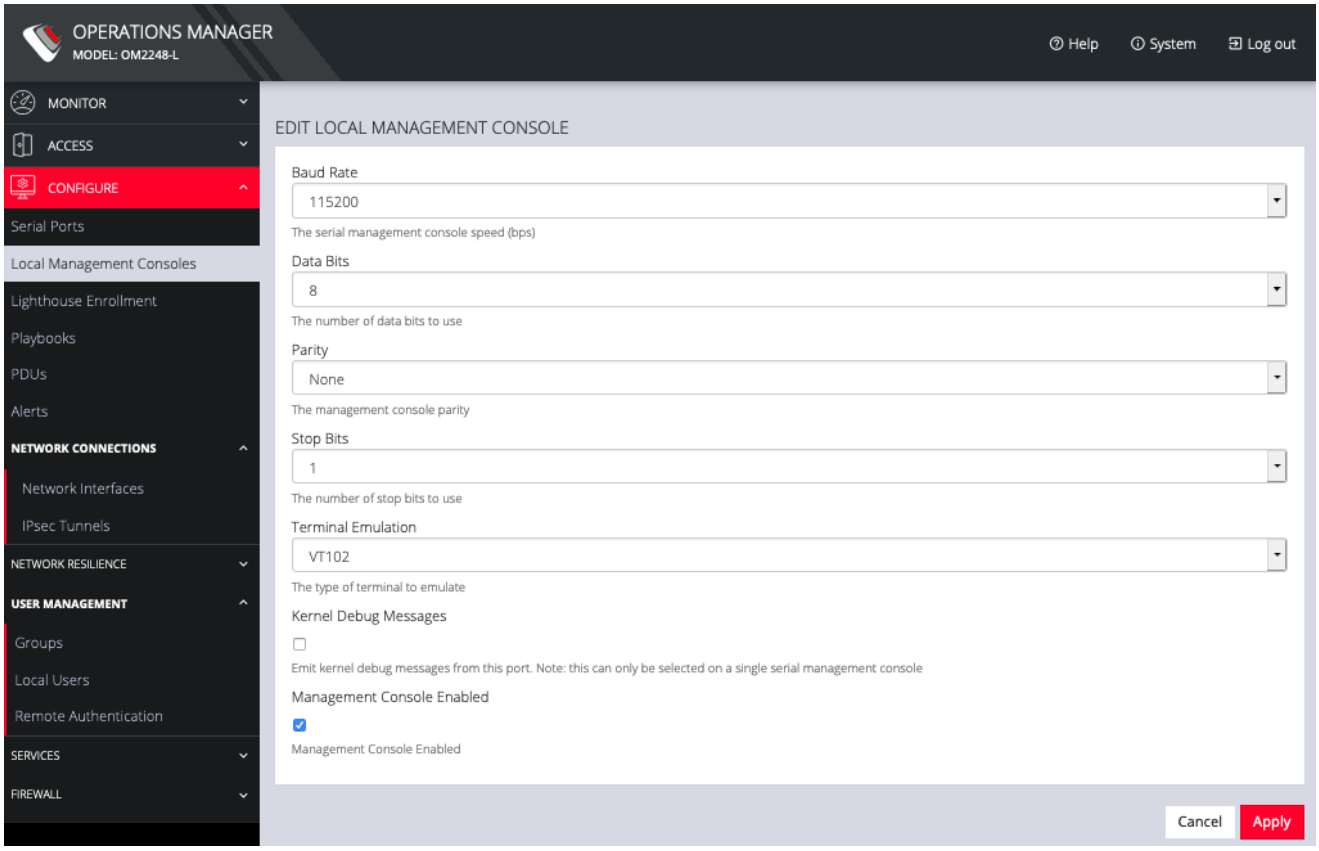
- **Parity**: **None, Odd, Even, Mark, Space**
- **Stop Bits:** 1, 1.5, 2
- **Logging Levels**
- **Serial Port Aliases**

5.2 Local Management Consoles

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

To edit the settings of a local management console:

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



3. The **Edit Local Management Console** page lets you control:
    - **Baud Rate**
    - **Data Bits**
    - **Parity**
    - **Stop Bits**
    - **Terminal Emulation**
    - Enable or disable **Kernel Debug Messages**
    - Enable or disable the selected **Management Console**

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

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

5.3 Interfaces and Connections

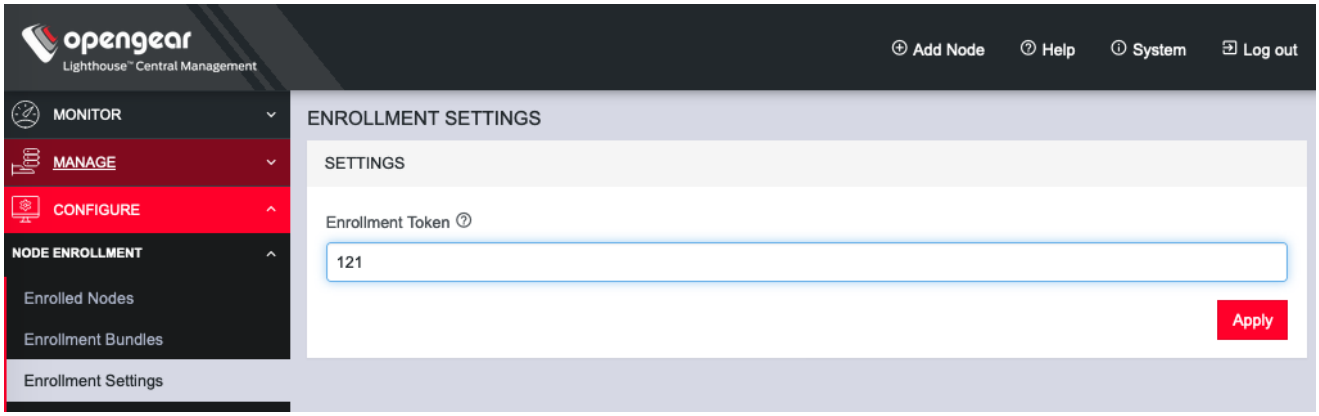
For instructions on adding, editing, or deleting network connections, see *2.8 Changing the IP Address of the Primary LAN Port*.

5.4 Lighthouse Enrollment

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

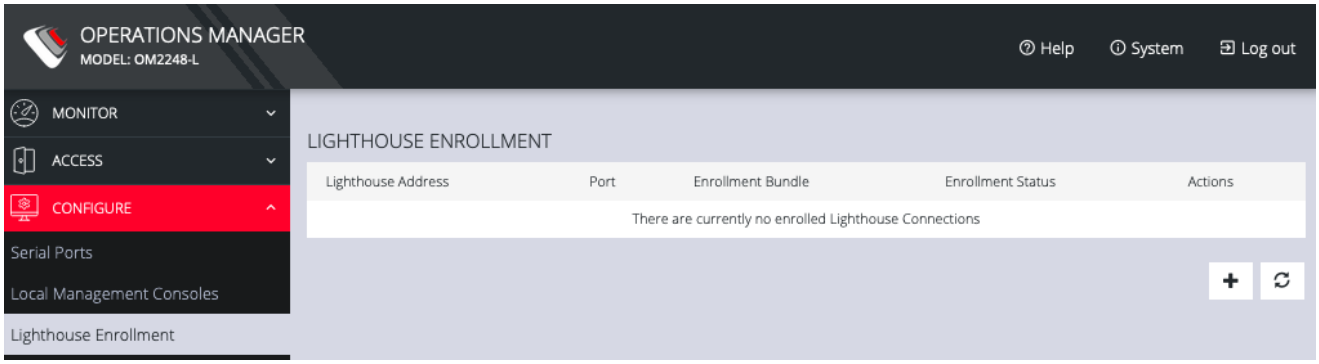
To enroll your OPERATIONS MANAGER to a Lighthouse instance, you must have Lighthouse installed and have an enrollment token set in Lighthouse.

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

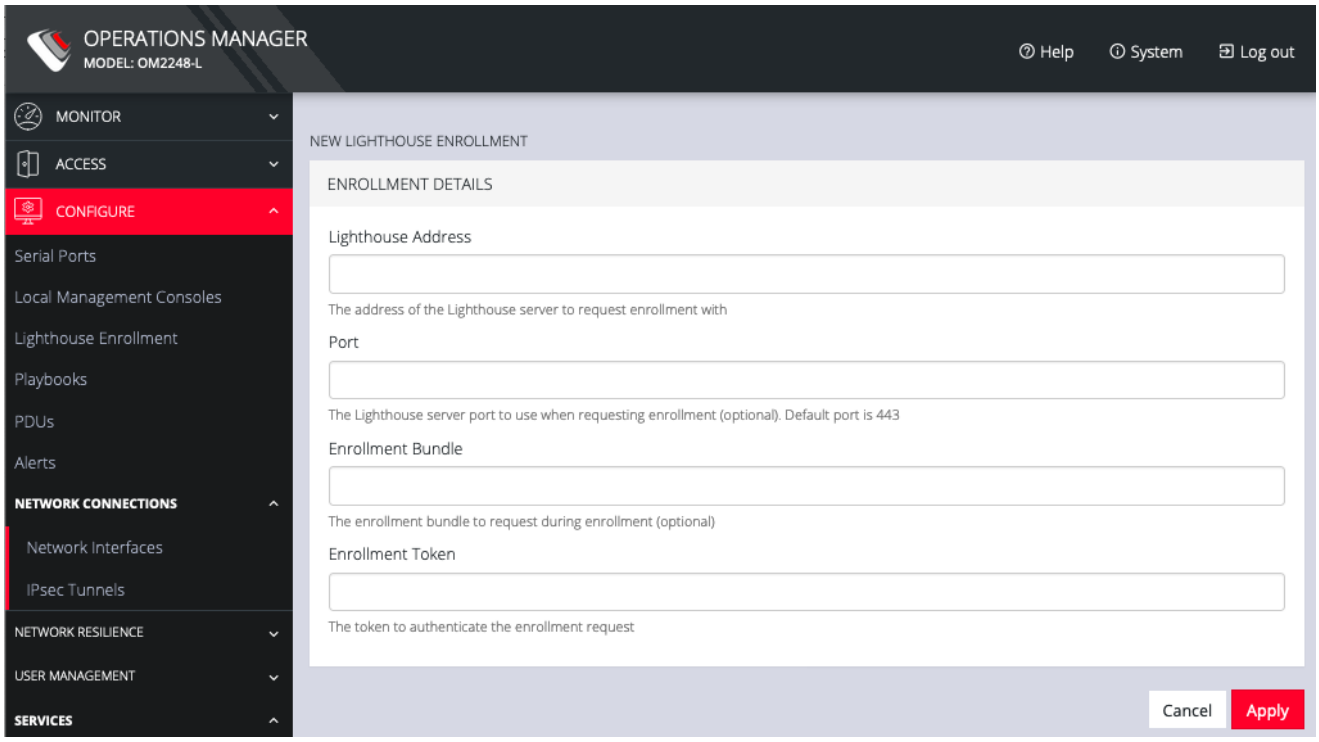


To enroll your OPERATIONS MANAGER in this Lighthouse instance:

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



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

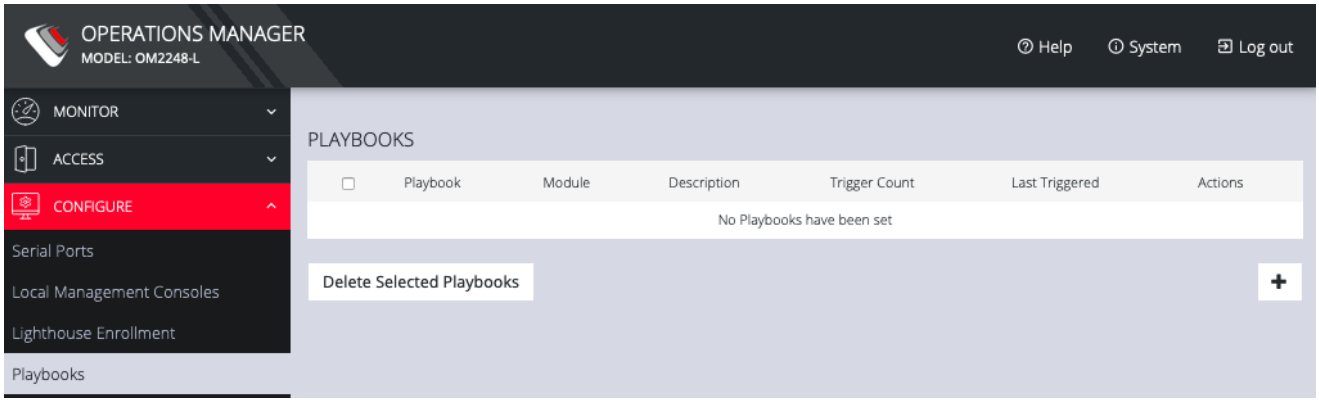


3. Enter the IP address or fully qualified domain name of the Lighthouse instance and the Enrollment Token you created in Lighthouse. Optionally enter a Port and an Enrollment Bundle (see the Lighthouse User Guide for more information).
4. Click **Apply**.

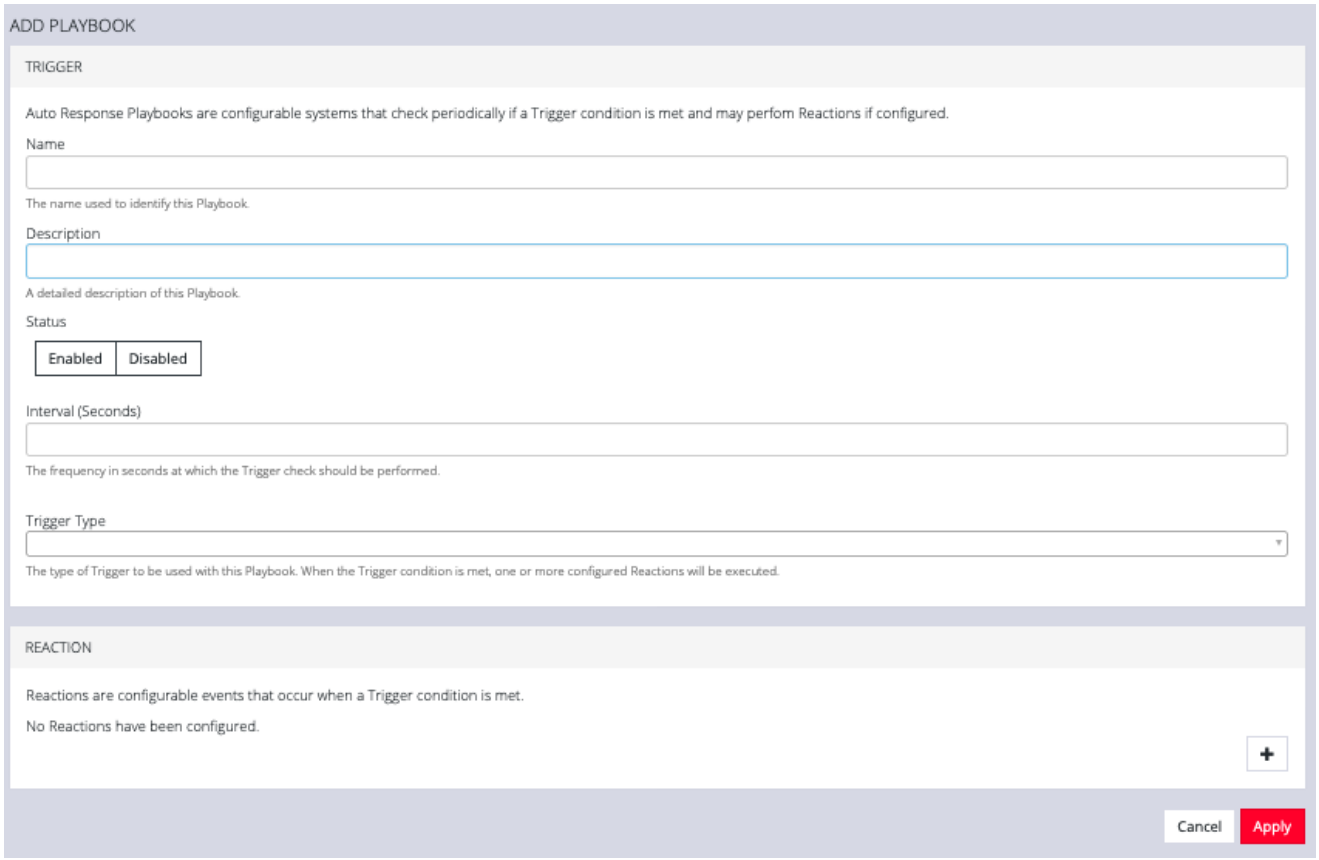
NOTE: Enrollment can also be done directly via Lighthouse using the Add Node function. See the Lighthouse User Guide for more instructions on enrolling Opengear devices into Lighthouse.

5.5 Playbooks

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

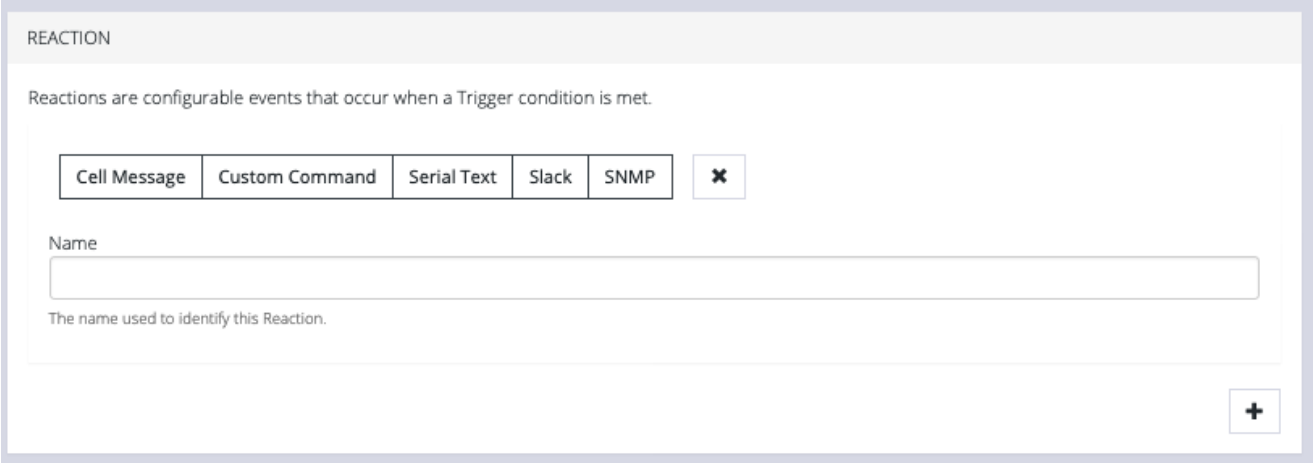


Click the **Plus** button to create a new **Playbook**.



1. Enter a **Name** for the **Playbook**.
2. Add a **Description**.

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



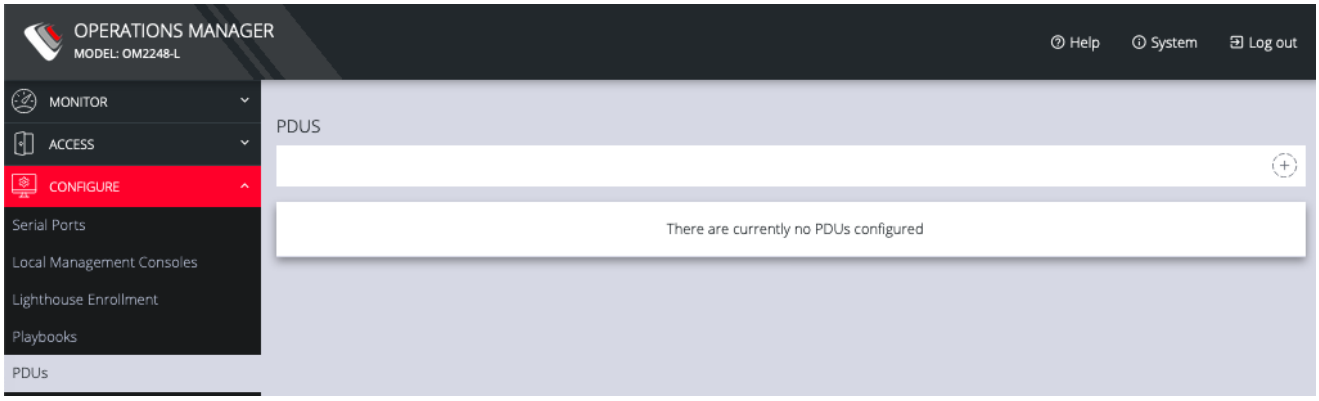
Clicking on each **Reaction** opens a custom screen to provide necessary information. When you are finished, click **Apply**.

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

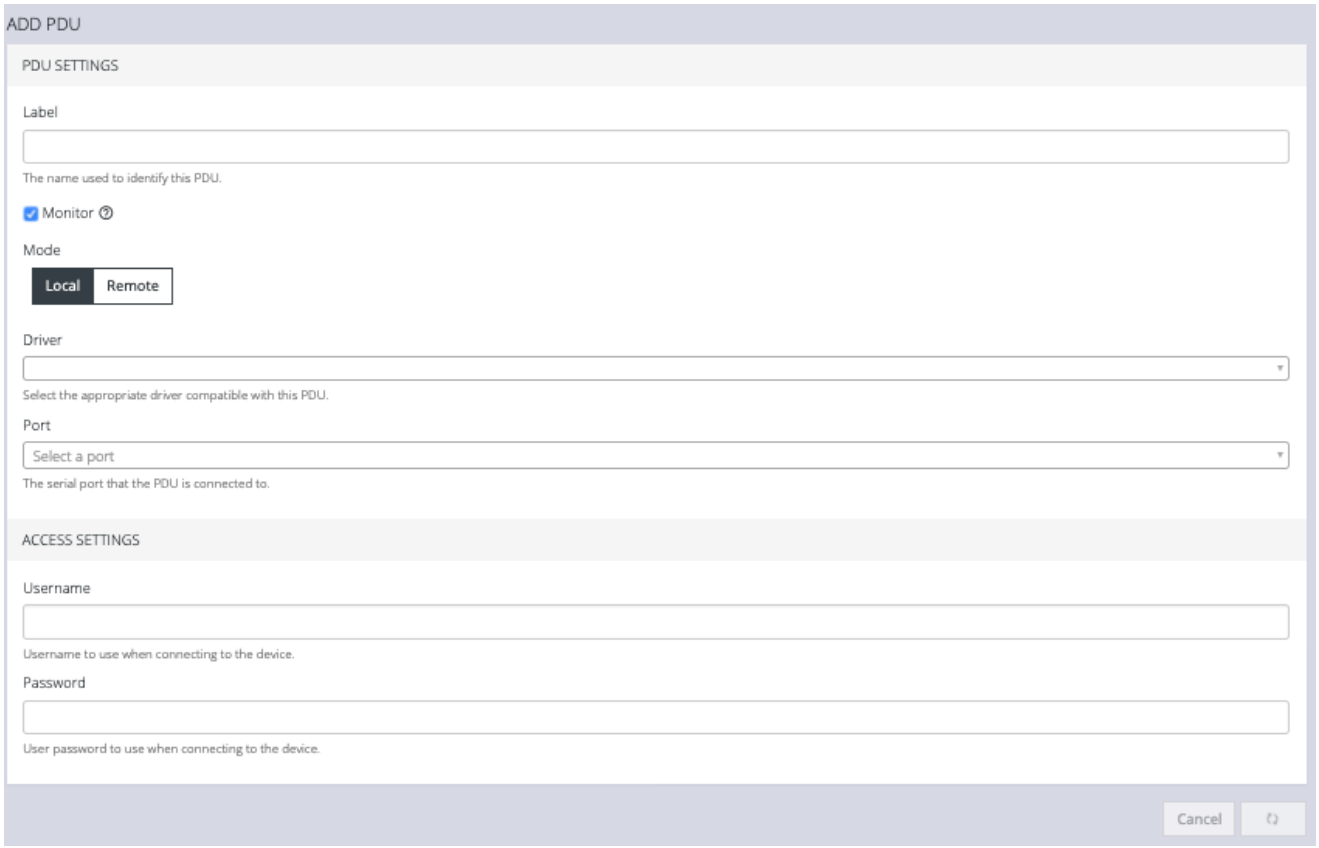
To monitor current **Playbooks**, click on **Monitor > Playbooks**. Choose the time period if desired,and filter by **Name** of **Playlist** to view any that have been triggered.

5.6 PDUs

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



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



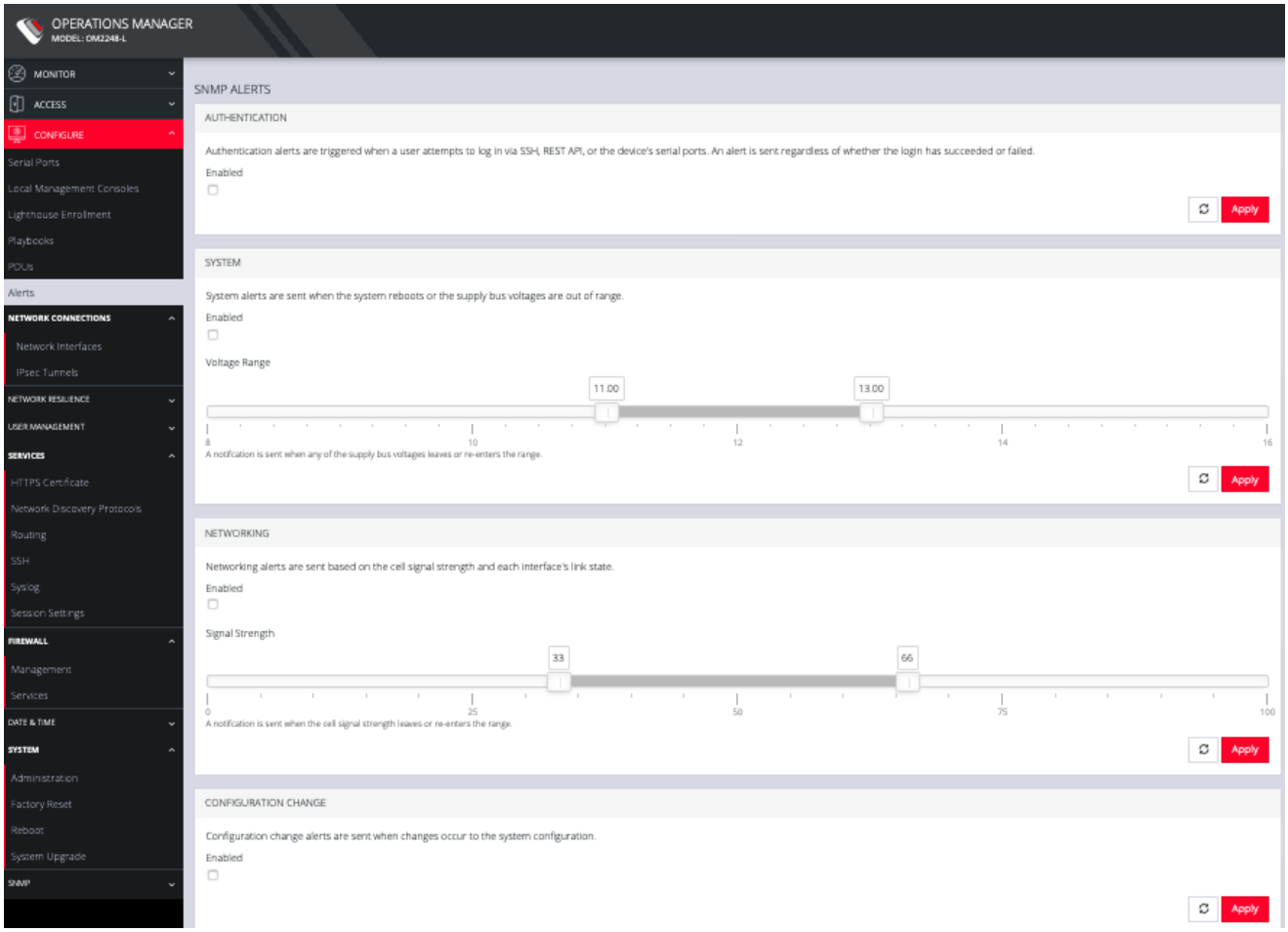
1. Enter a **Label** for this **PDU**.
2. Select the **Monitor** checkbox.
3. Choose **Local** or **Remote**.

4. Select the appropriate **Driver** from the drop-down list.
5. Select the **Port**.
6. Add a **Description**.
7. Under **Access Settings**, enter a **Username** and **Password** to use when connecting to the device.
8. When you are finished, click **Apply**.

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

5.7 Alerts

On the **Configure > Alerts** page, you can add and delete SNMP alerts.



You can set triggers to send SNMP alerts for the following:

- **Authentication**: 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 login has succeeded or failed.
- **System**: when the system reboots or the supply bus voltages are out of range. Use the slider to adjust the upper and lower voltage range.
- **Networking**: based on the cell signal strength and each interface's link state.Use the slider to adjust the upper and lower signal strength.
- **Configuration**: when changes occur to the system configuration.

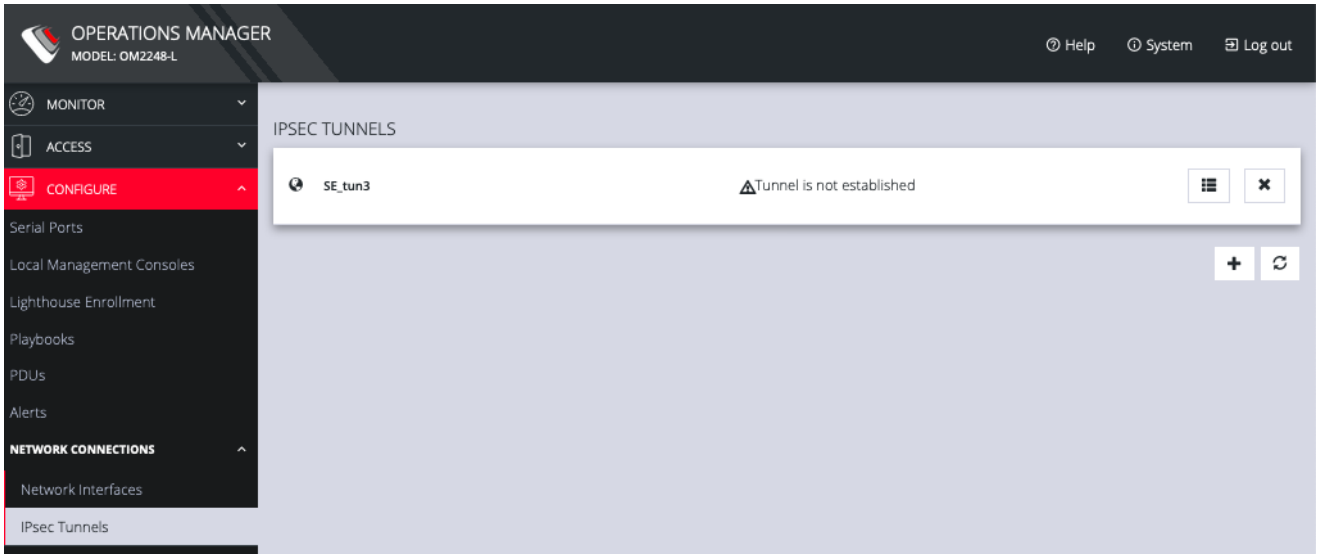
NOTE: Manage the SNMP settings for these alerts on the **CONFIGURE > SNMP > SNMP Alerts Protocol Configuration** page.

5.8 Network Connections

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

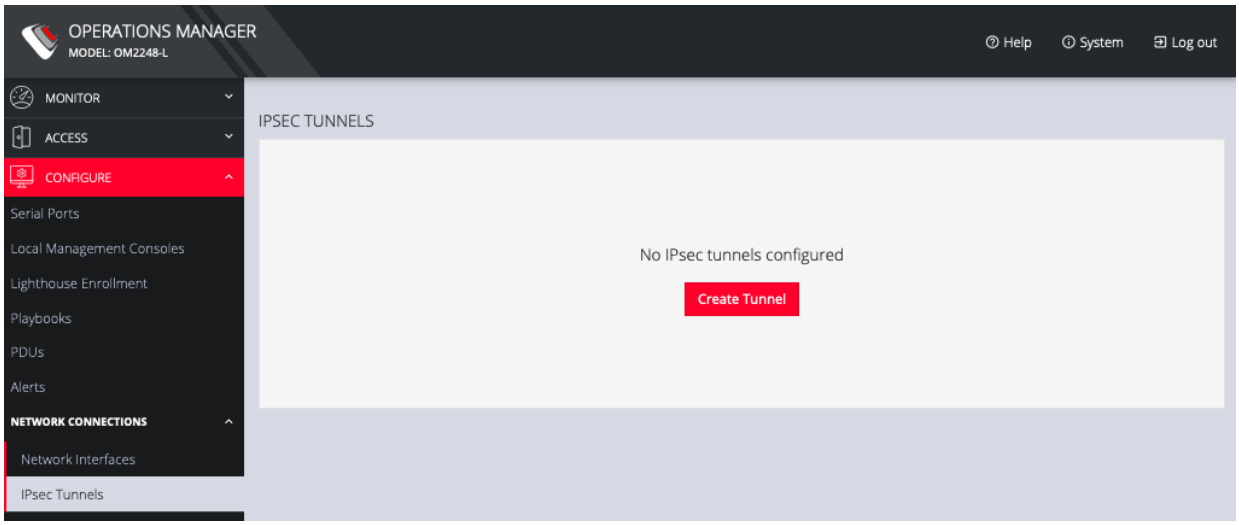
For Network Interface configuration, see Chapter 2.5 for details.

On the **CONFIGURE > NETWORK CONNECTIONS > IPsec Tunnels** page, you can create, edit, and delete IPsec tunnels.

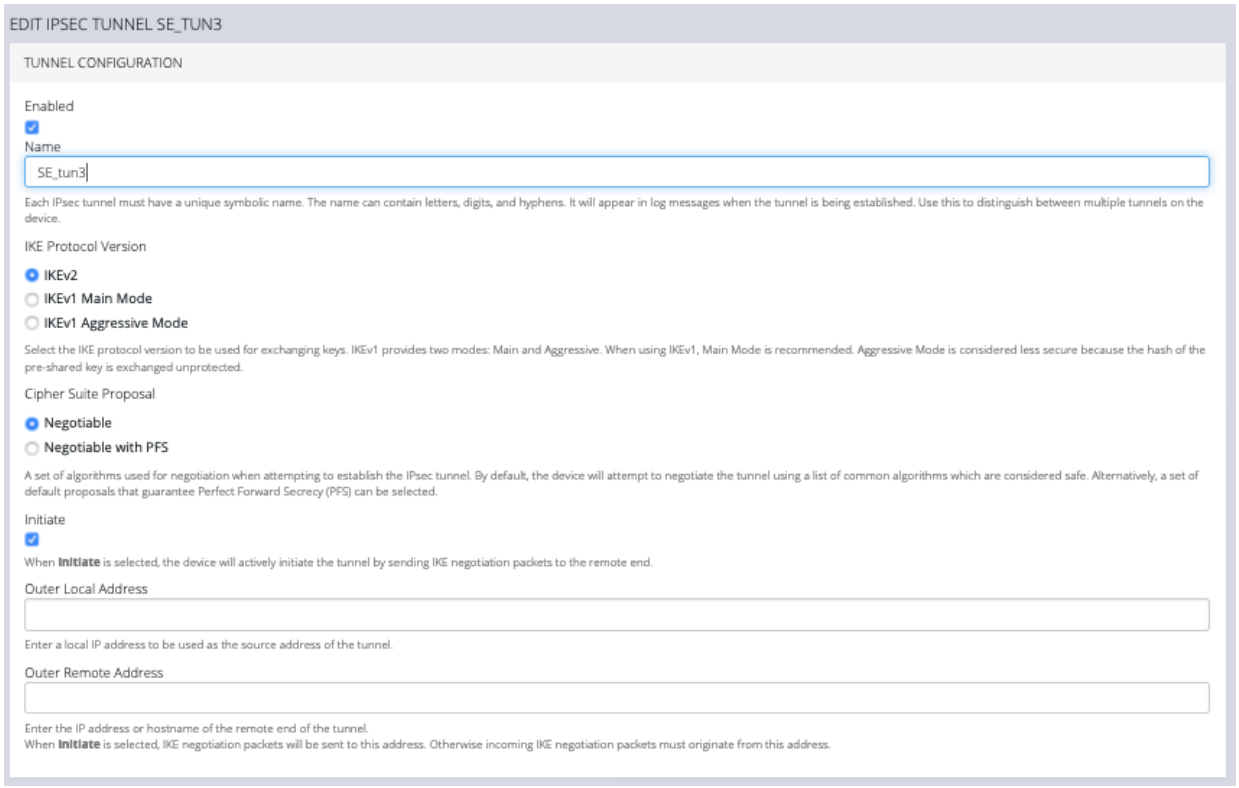


To create an IPsec tunnel:

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



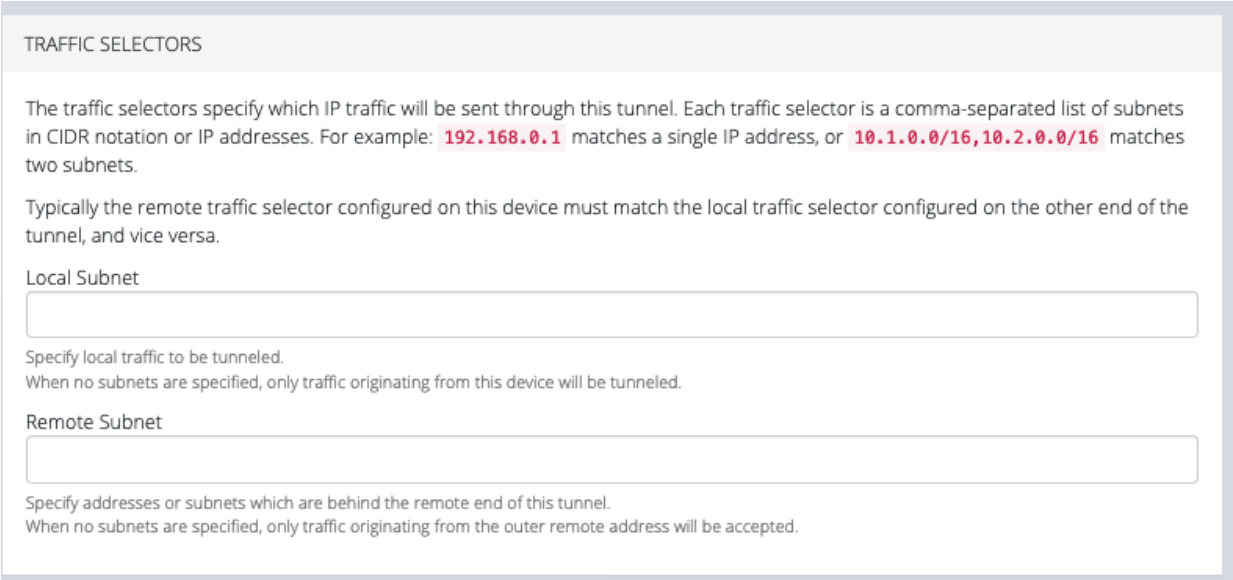
2. Click **CREATE TUNNEL**. This opens the **EDIT IPSEC TUNNEL** page.



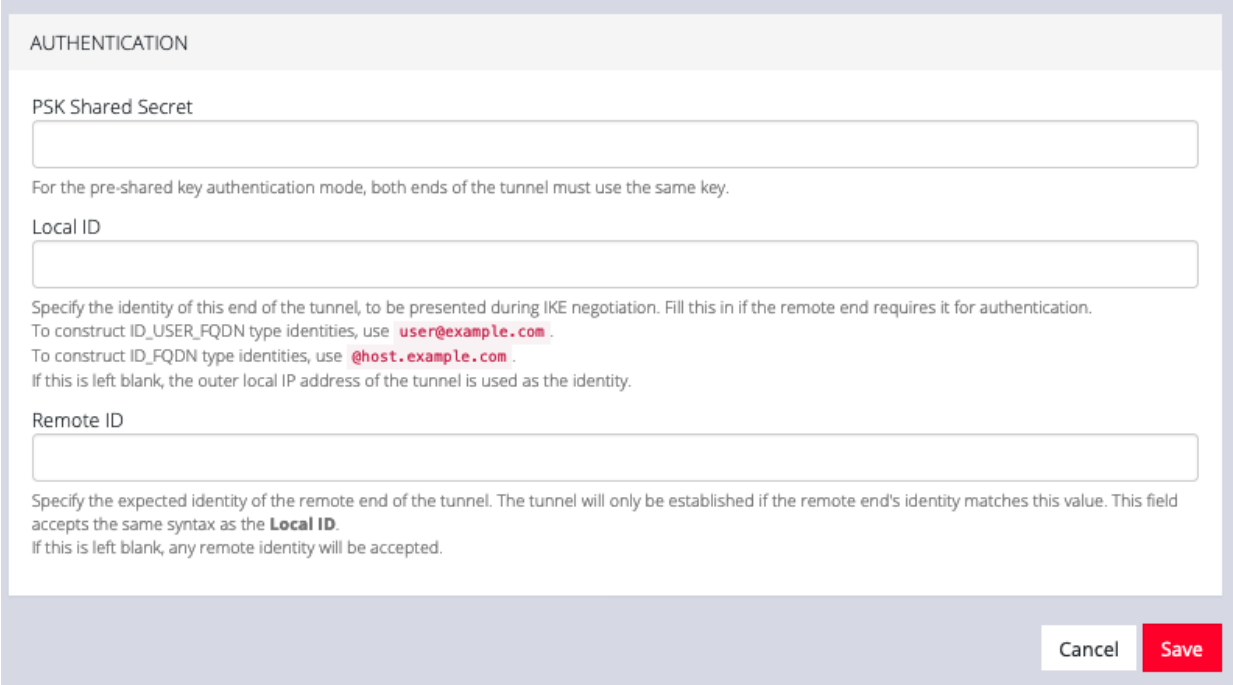
3. In the top section of the page, **TUNNEL CONFIGURATION**, click the **Enabled** check

box and give your new tunnel a name.

4. Select an **IKE Protocol Version** to use for exchanging keys. IKEv1 provides two modes: **Main** and **Aggressive**. When using IKEv1, Main Mode is recommended. Aggressive Mode is considered less secure because the hash of the pre-shared key is exchanged unprotected.
5. Select a **Cipher Suite Proposal**. This is a set of algorithms used for negotiation when attempting to establish the IPsec tunnel. By default, the device will attempt to negotiate the tunnel using a list of common algorithms which are considered safe. Alternatively, a set of default proposals that guarantee Perfect Forward Secrecy (PFS) can be selected.
6. Click the **Initiate** checkbox to actively initiate the tunnel by sending IKE negotiation packets to the remote end.
7. Enter an **Outer Local Address**, a local IP address to use as the source address of the tunnel
8. Enter an **Outer Remote Address**, the IP address or hostname of the remote end of the tunnel.
9. Scroll down to the **Traffic Selectors** section of the page.



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



12. Enter a **PSK Shared Secret**.

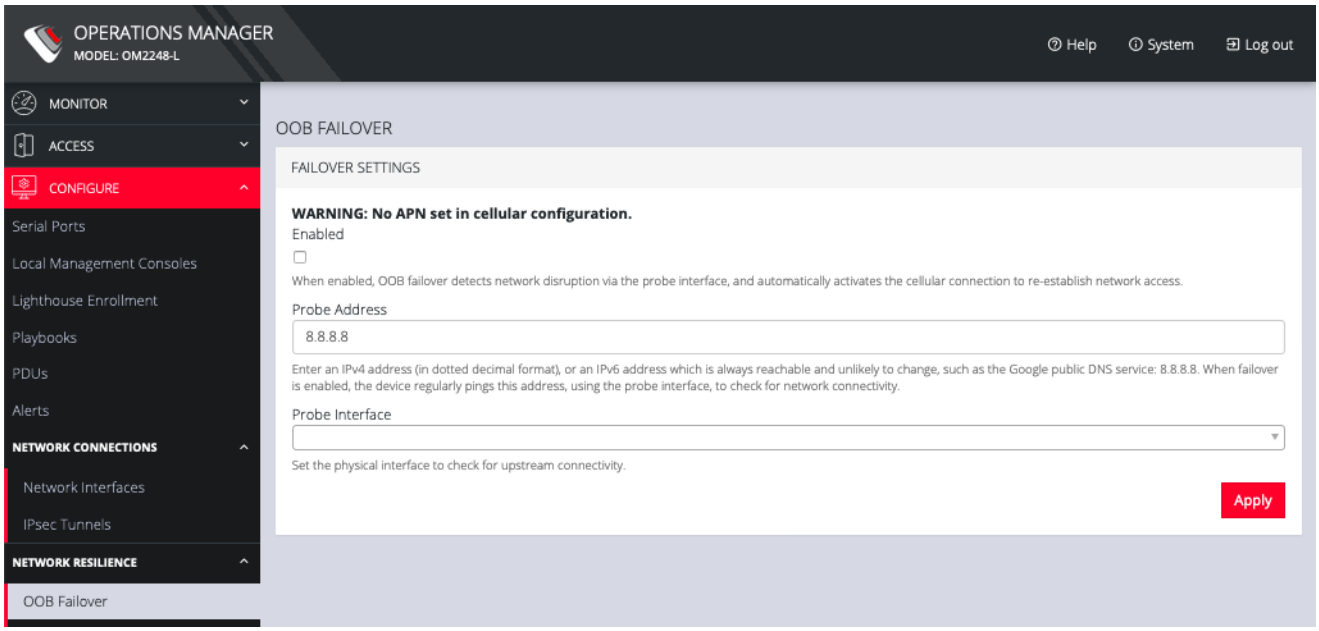
13. Enter a **Local ID** and **Remote ID**.
14. Click **Save**. The new tunnel is now listed on the **CONFIGURE > NETWORK CONNECTIONS > IPsec Tunnels** page.

5.9 Network Resilience

Under the NETWORK RESILIENCE menu, you can manage OOB failover and IP Passthrough settings.

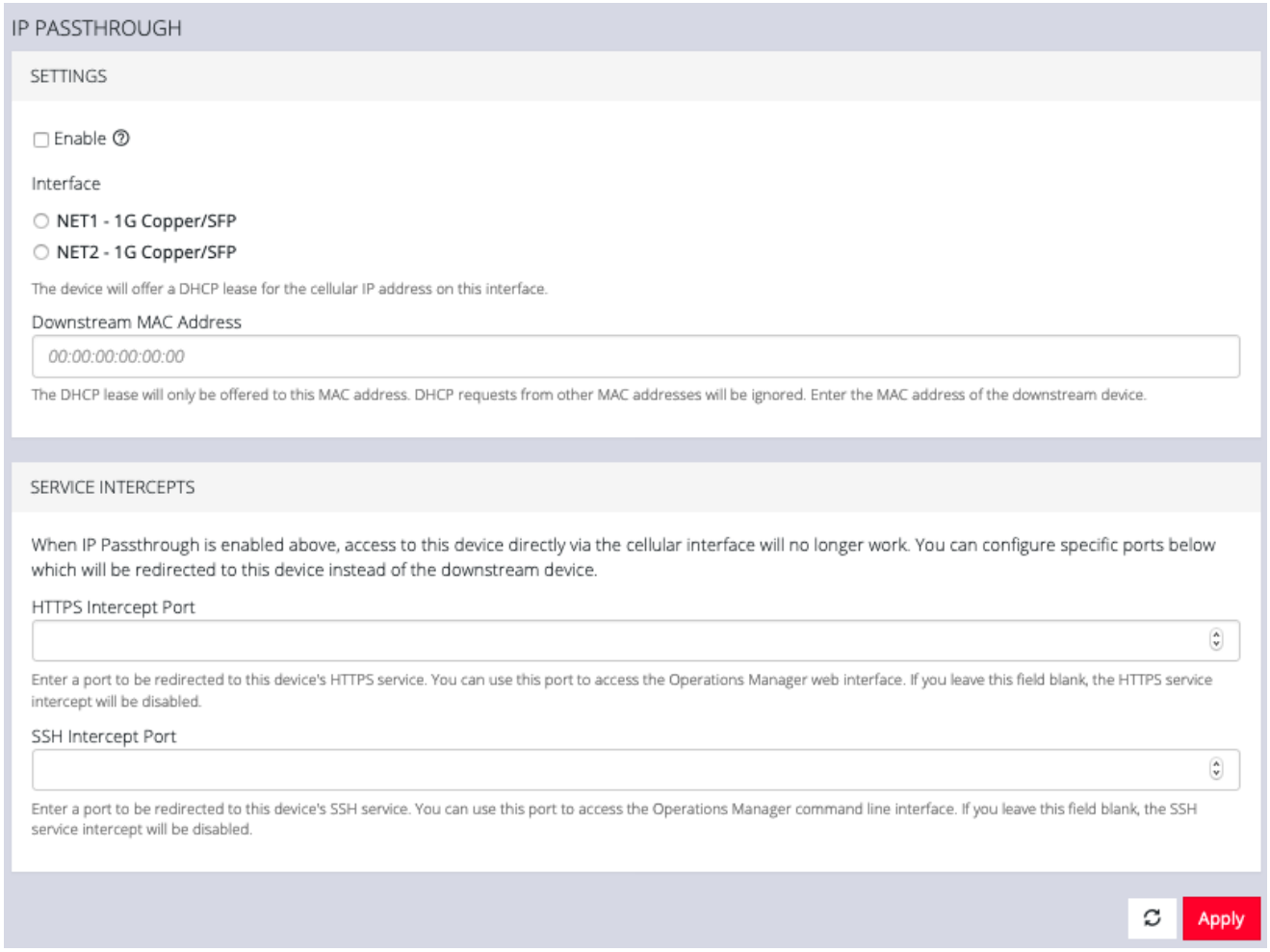
5.9.1 OOB failover

To manage Out of Band failover:



5.9.2 IP Passthrough

To manage **IP Passthrough** settings:



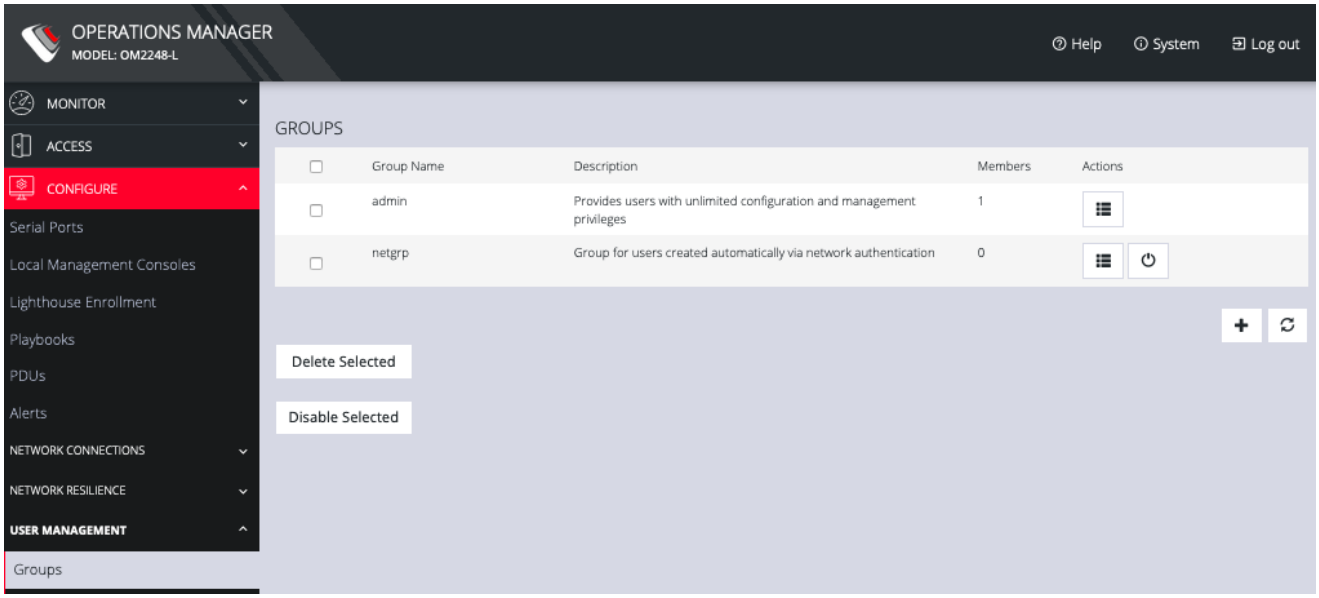
5.10 User Management

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.

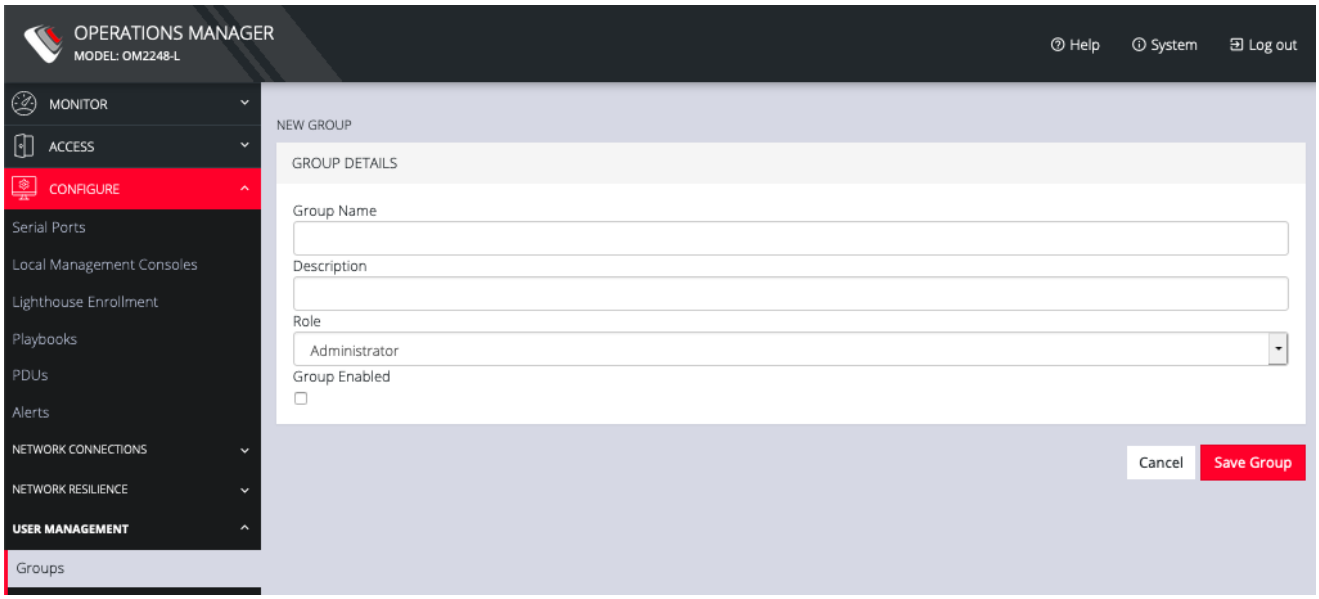
5.10.1 Groups

To create a new group:

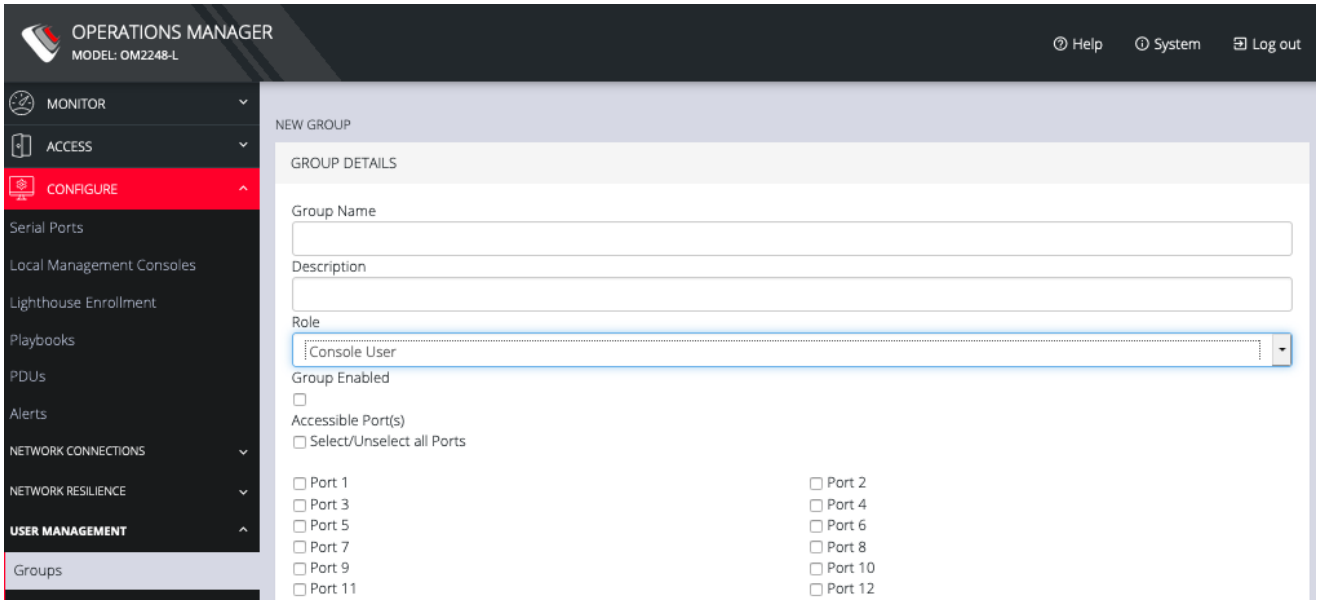
1. Select **CONFIGURE > User Management > Groups.**



2. Click the **Plus** button. The New Group page opens.



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



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

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

If the **Role** selected is **Administrator**, members of the group have access to all nodes.

To modify an existing group:

1. Select **CONFIGURE > User Management > Groups**.
2. Click **Edit** in the **Actions** section of the group to be modified and make desired

changes.

3. Click **Save Group**.

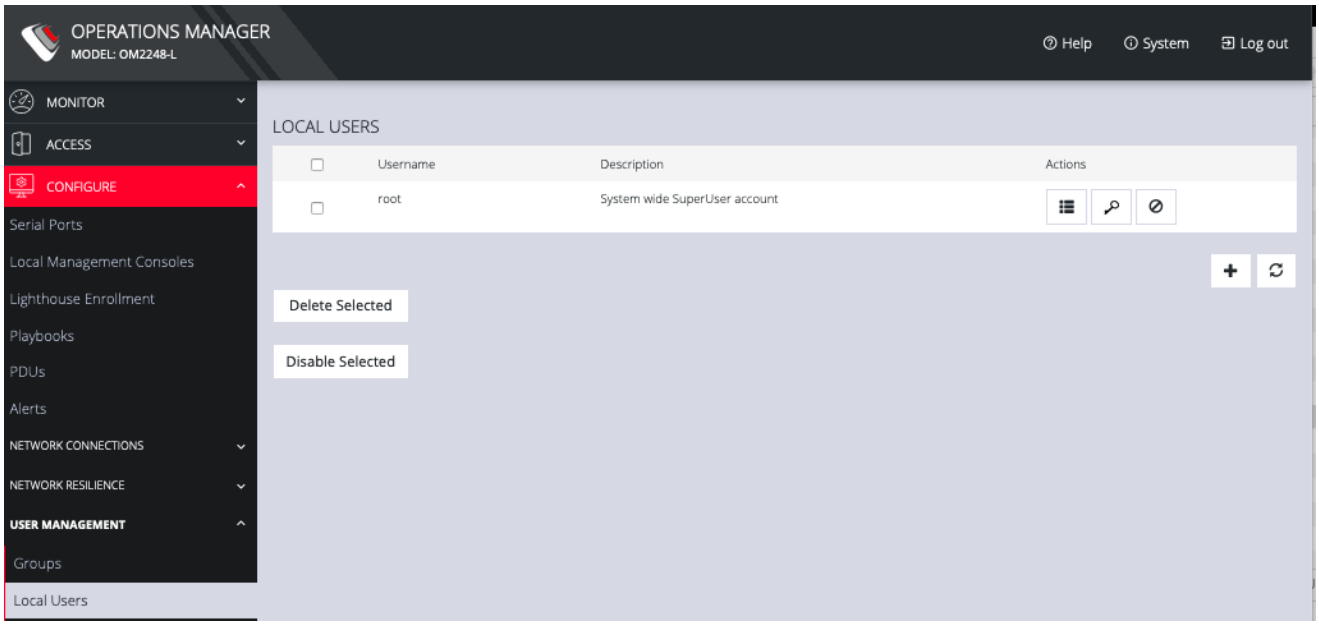
The **CONFIGURE > User Management > Groups** page also allows administrators to delete a group. Users who were members of the deleted group lose any access and administrative rights inherited from the group.

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

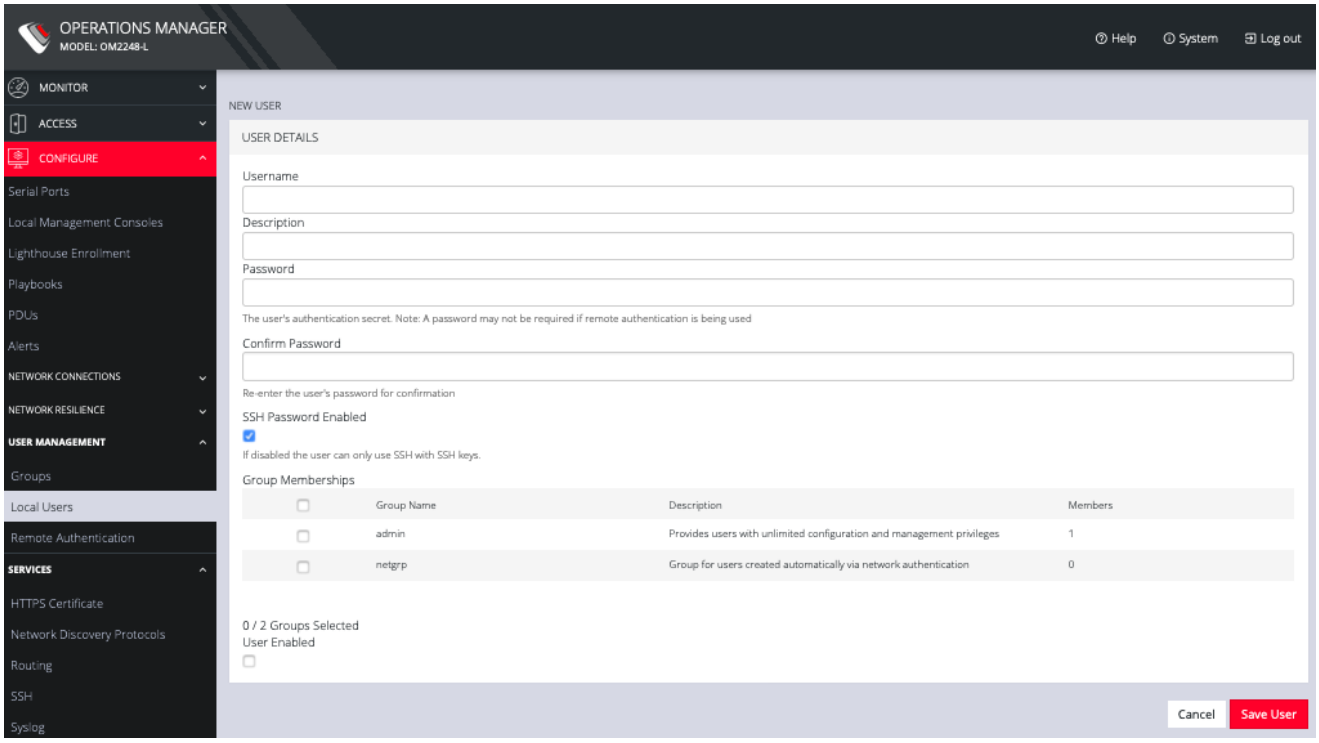
5.10.2 Local Users

To create a new user:

1. **CONFIGURE > User Management > Local Users**.



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



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

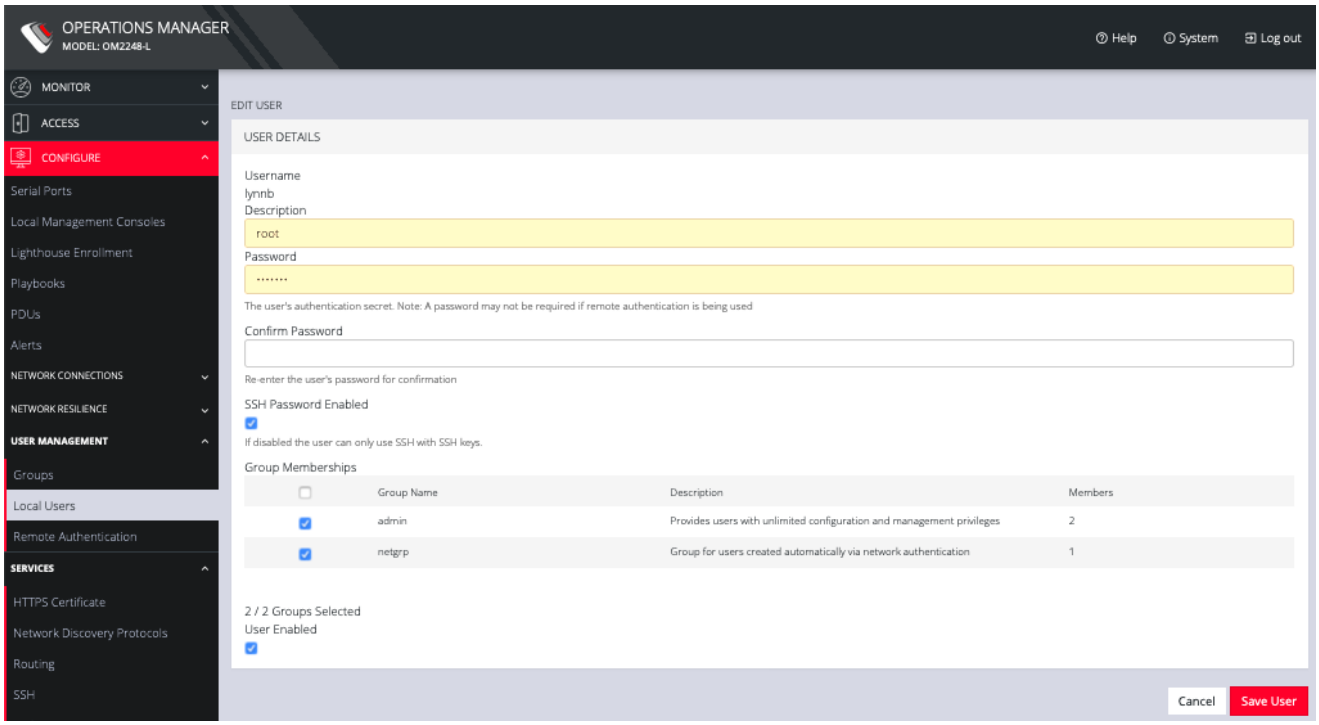
To create a new user without password which causes them to fall back to remote authentication:

1. Select **CONFIGURE > User Management > Remote Authentication**
2. Select a Scheme.
3. Enter Settings and click **Apply**.
4. Select **CONFIGURE > User management > Local Users**
5. Click the **+** button. The **New User** dialog loads.

6. Enter a **Username**, **Description**.
7. Select the **Remote Password Only** checkbox.
8. Select the **Enabled** checkbox.
9. Click **Apply**.

To modify an existing user:

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

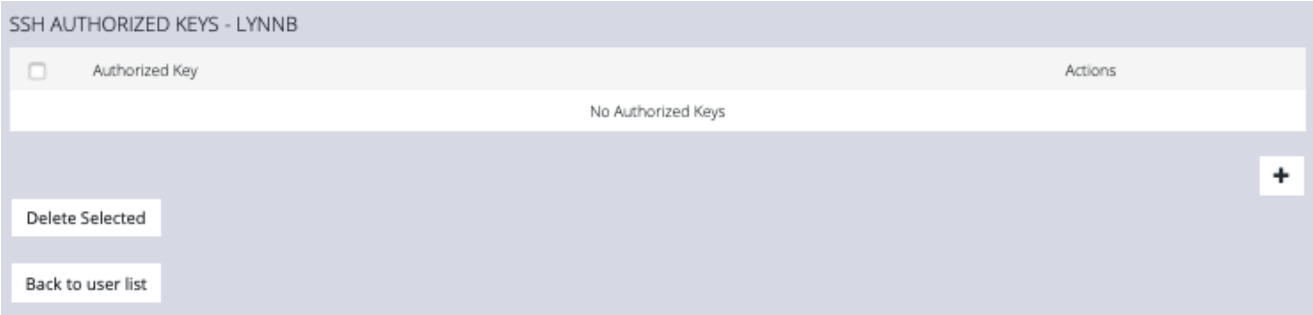


The **Edit Users** dialog allows the user's **Description** to be changed, **Group Memberships** modified, and the user's **Password** to be reset. The username cannot be changed. To disable a user, uncheck the **Enabled** checkbox.

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

To manage SSH authorized keys for a user:

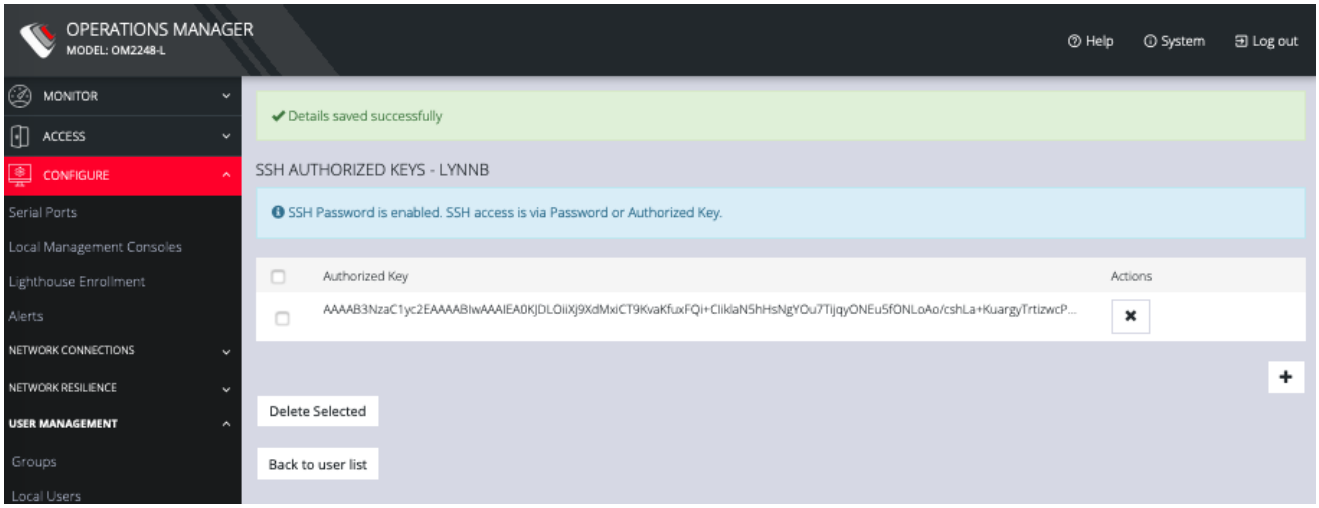
1. Select **CONFIGURE > User management > Local Users**
2. Click the **Manage SSH Authorized Keys** button in the **Actions** section next to the user.



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

4. Enter the key and click **Apply**. You can also click on **Add Authorized Key** and disable password for SSH for this user from this page.

5. To delete a key, click **CONFIGURE > USER MANAGEMENT > Local Users** and click the **Authorized Key** button for the user.



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

To delete a user:

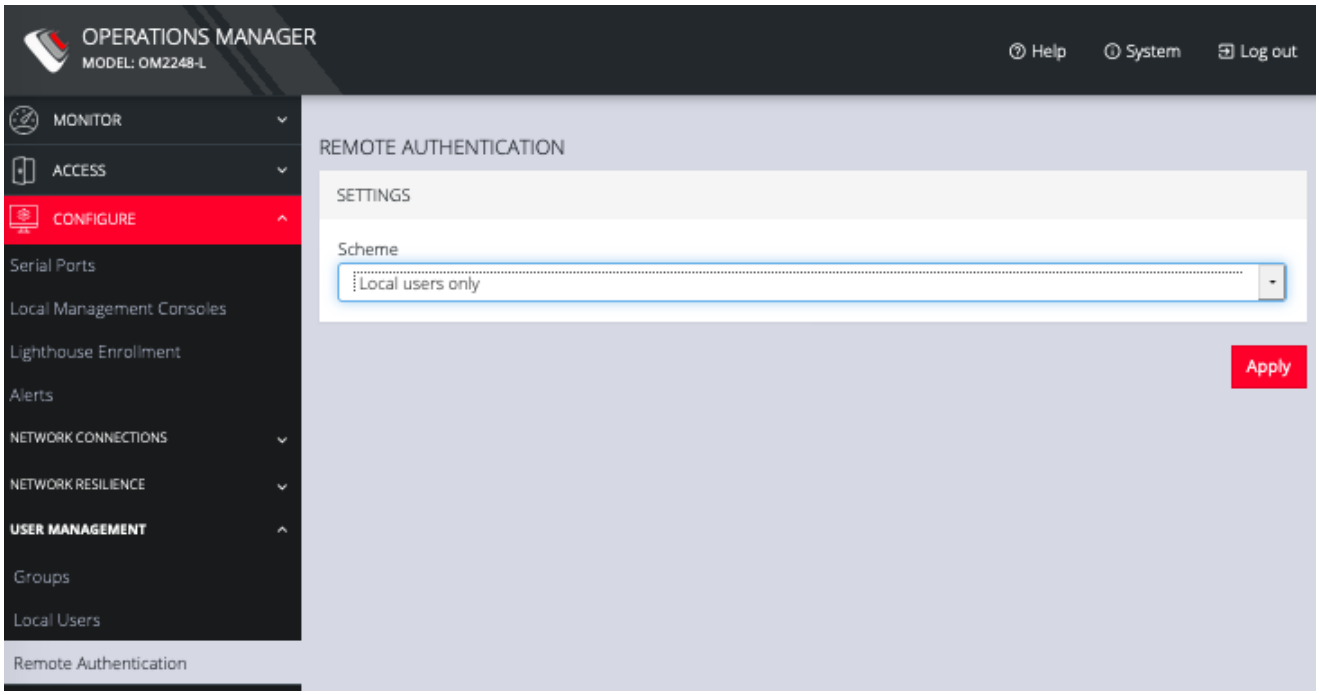
1. Select **CONFIGURE > User management > Local Users**
2. Click the **Delete User** button in the **Actions** section next to the user to be deleted.
3. Click **Yes** in the **Confirmation** dialog.

5.10.3 Remote Authentication

The OPERATIONS MANAGER supports three AAA systems:

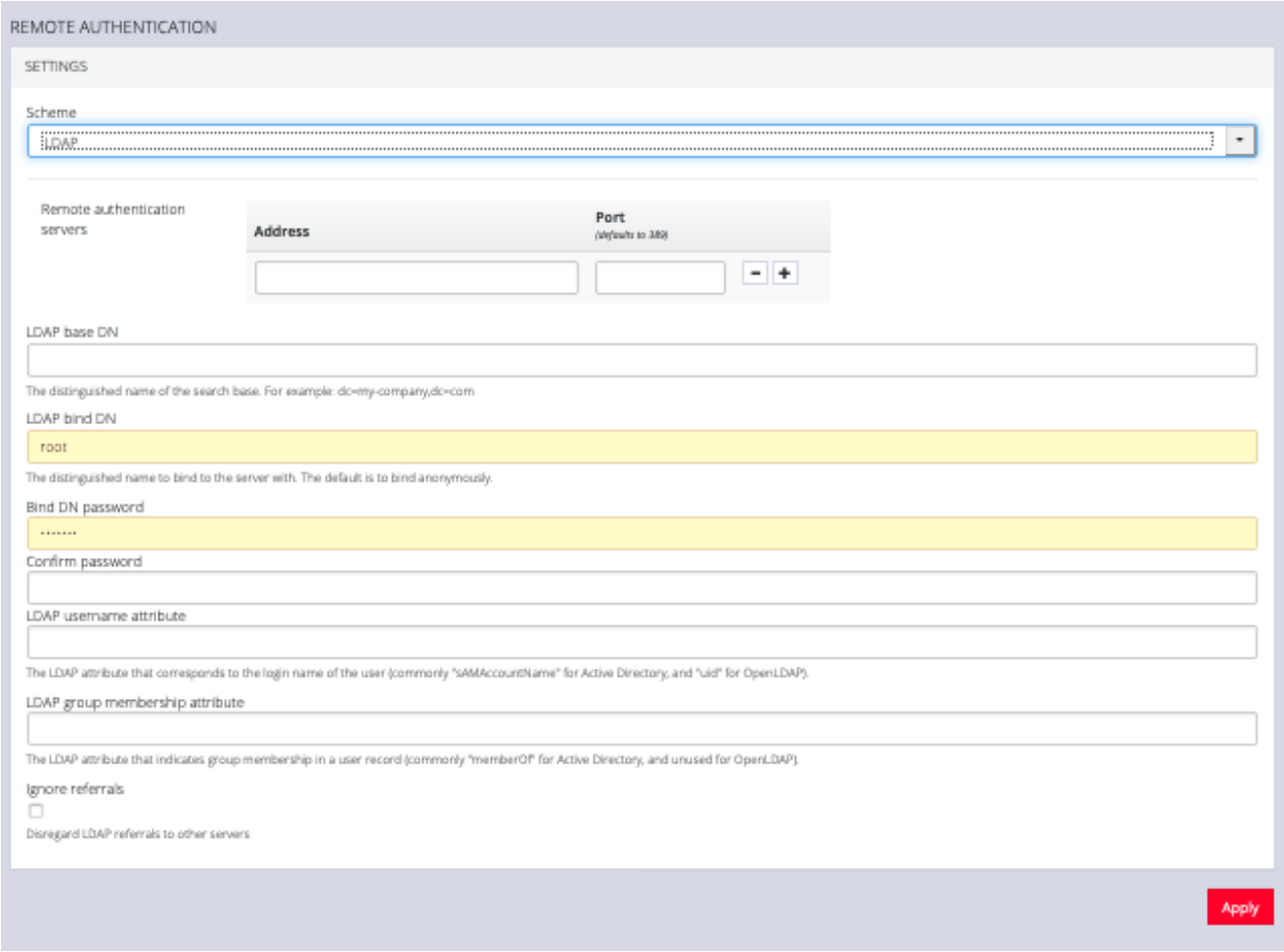
- LDAP (Active Directory and OpenLDAP)
- RADIUS
- TACACS+

To begin, select **CONFIGURE > User Management > Remote Authentication**.



To configure LDAP authentication:

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



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

   For example, if a user's distinguished name is cn=John Doe,d-c=Users,dc=ACME,dc=com, the *Base DN* is dc=ACME,dc=com

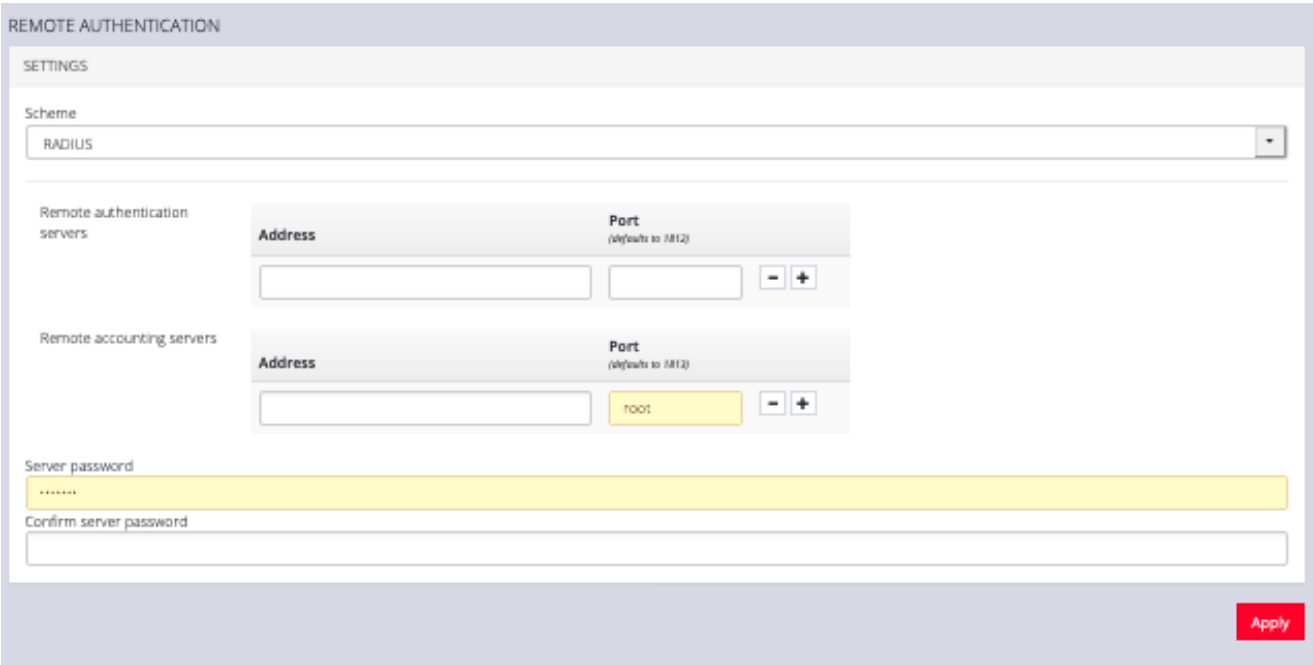
4. Add the **Bind DN**. This is the distinguished name of a user with privileges on the LDAP system to perform the lookups required for retrieving the username of the users, and a list of the groups they are members of.
5. Add the password for the binding user.

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

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

To configure RADIUS:

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



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

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

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

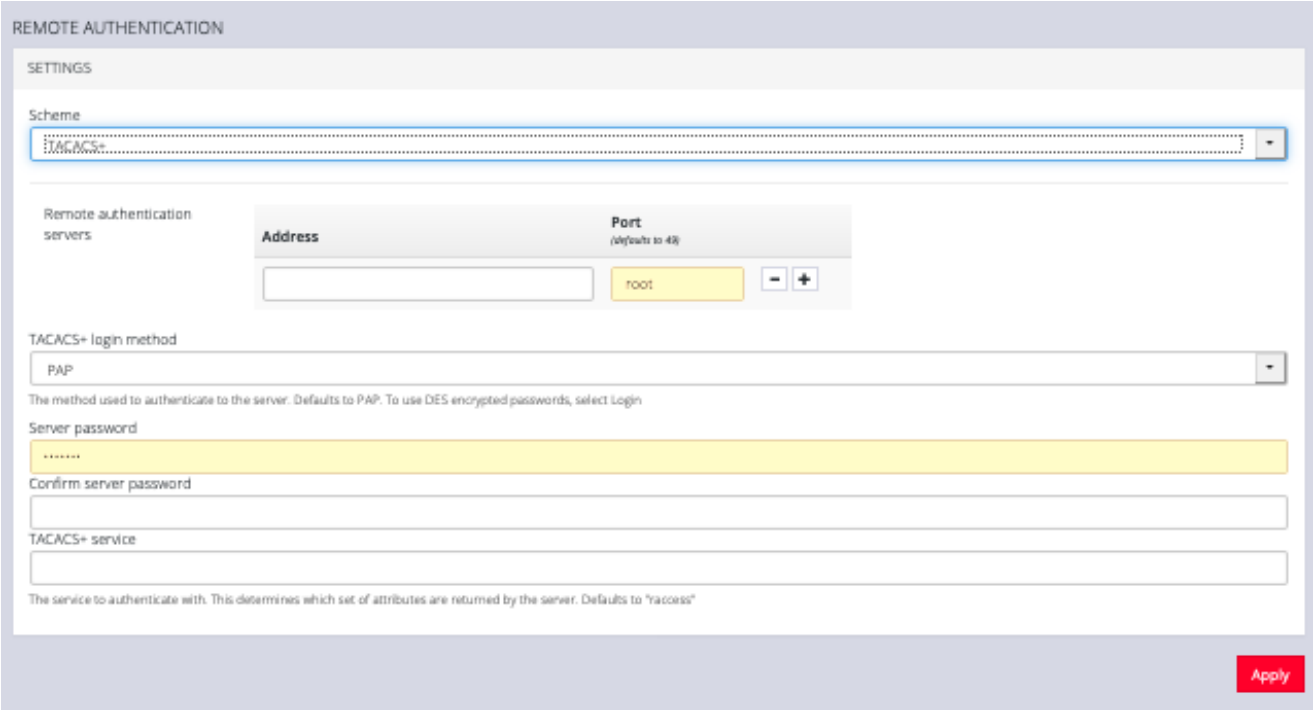
operator1 Auth-Type := System

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

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

To configure TACACS+:

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



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

To provide group membership, TACACS+ needs to be configured to provide a list of group names This following configuration snippet shows how this can be configured for a tac_plus server:

user = operator1 {

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

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

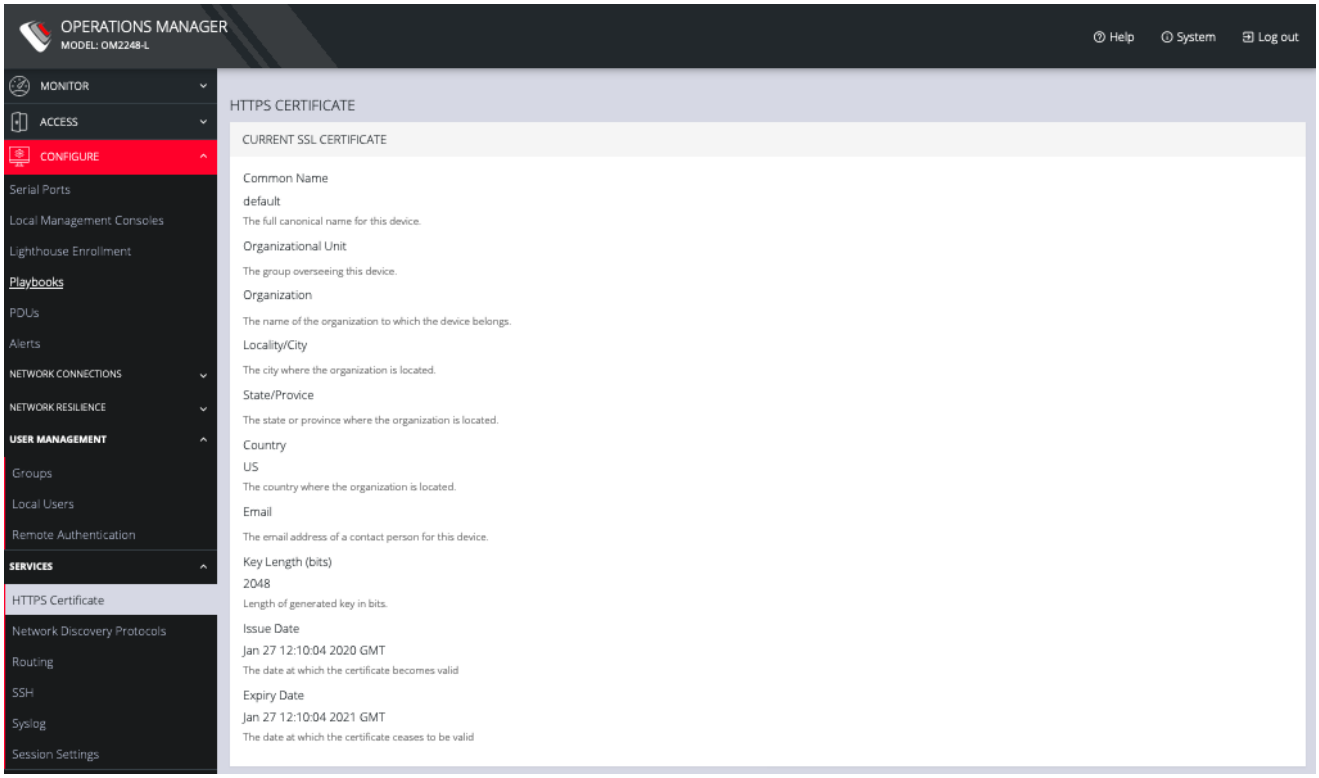
5.11 Services

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

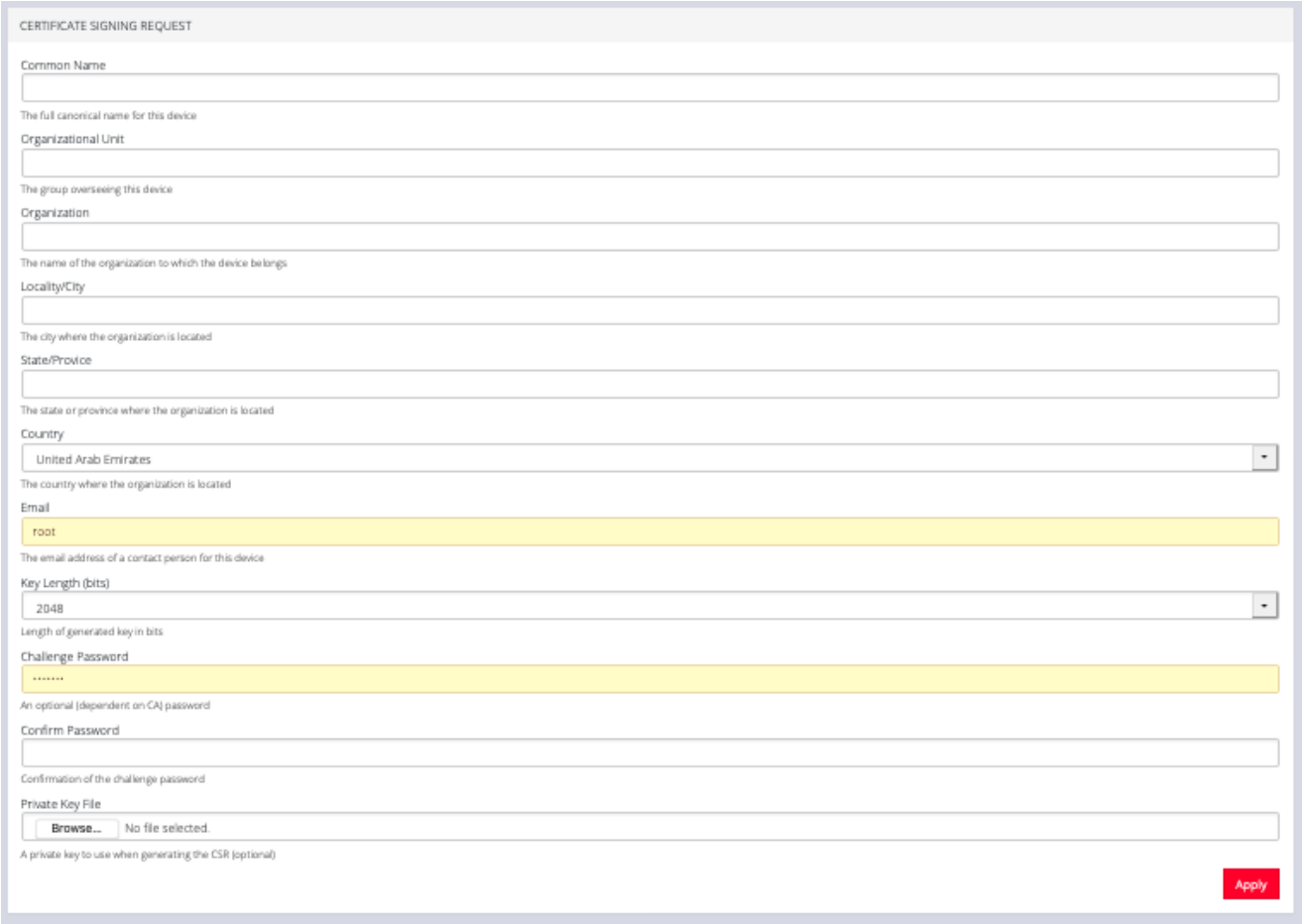
5.11.1 HTTPS Certificate

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

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

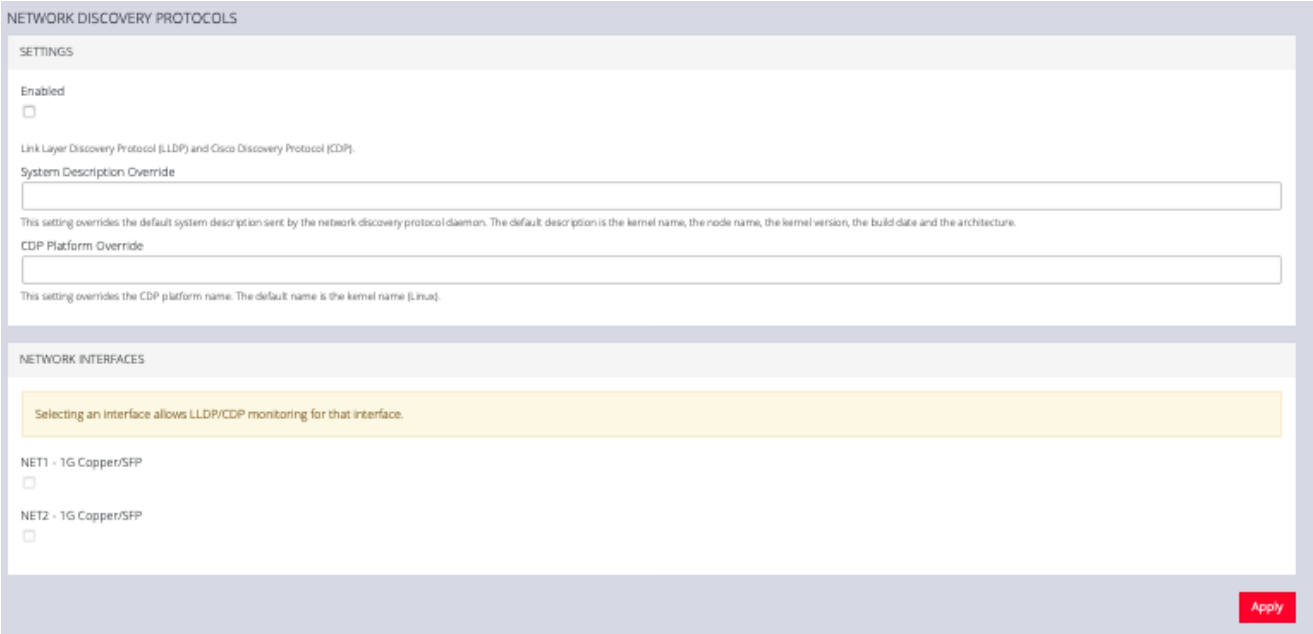


Below this listing is a **Certificate Signing Request** form, which can be used to generate a new SSL certificate.



5.11.2 Network Discovery Protocols

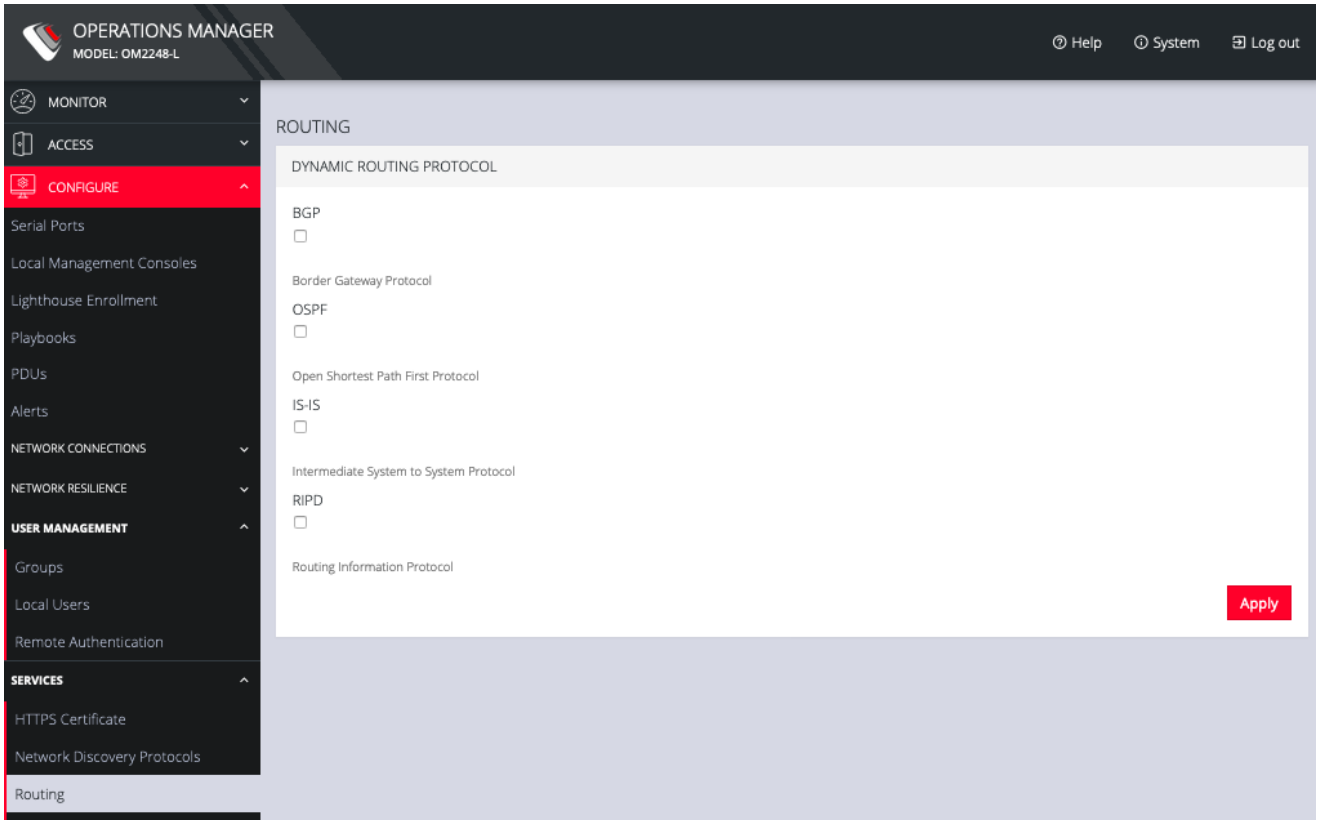
The OPERATIONS MANAGER displays LLDP/CDP Neighbors when enabled for a connection. See **CONFIGURE > SERVICES > Network Discovery Protocols** to enable/disable.



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

5.11.3 Routing

You can enable routing protocols on this page. Select CONFIGURE > SERVICES > Network Discovery Protocols > Routing.

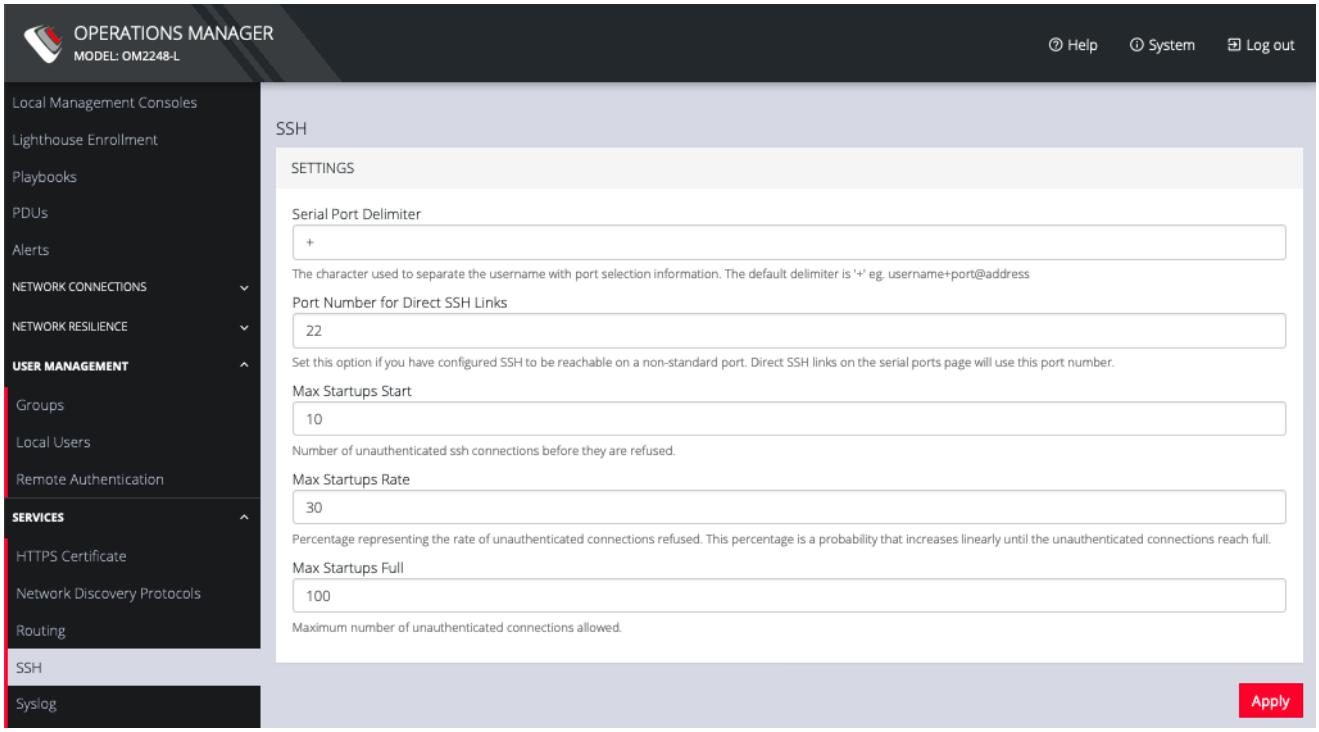


Select any of the following and click the Apply button:

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

5.11.4 SSH

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



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

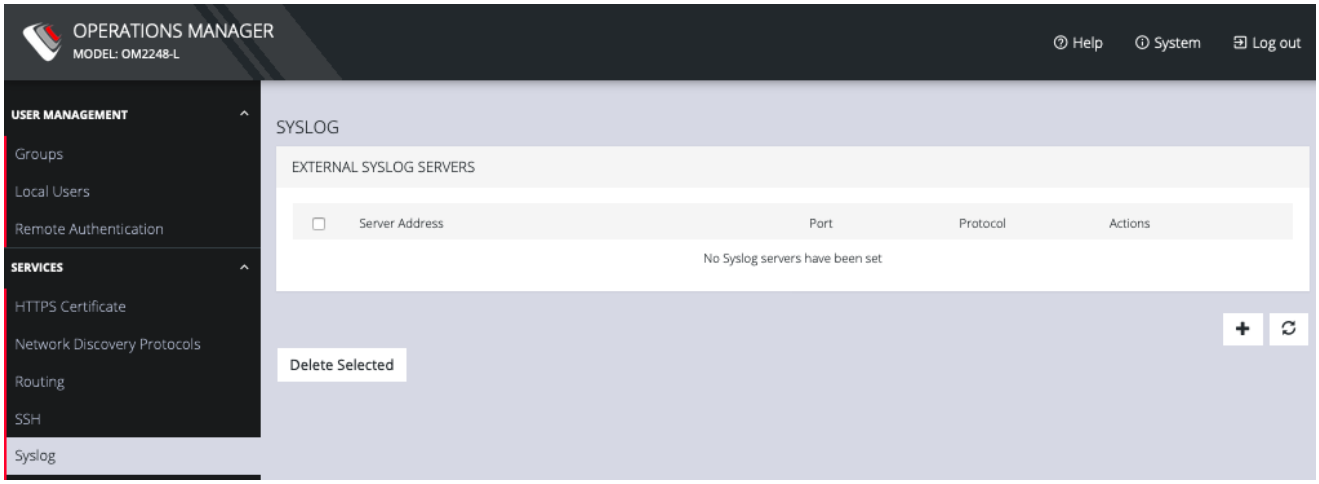
You can change more values on this page.

- **Max Startups Start**, the number of unauthenticated connections before they are refused.
- **Max Startups Rate** is a percentage that represents the rate of unauthenticated connections refused. This percentage is a probability that increases linearly until the unauthenticated connections reach full.
- **Max Startups Full** is the number of unauthenticated connections allowed.

5.11.5 Syslog

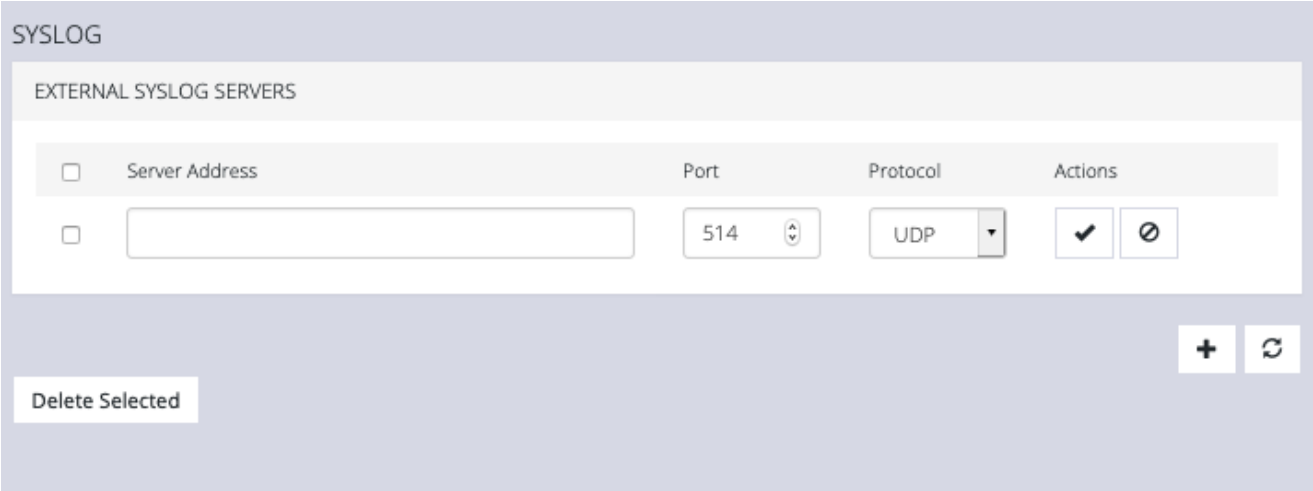
Administrative users can specify multiple external servers to export the syslog to via TCP or UDP.

Select **CONFIGURE > Services > Syslog**.



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

1. Click the **Plus** button. The **External Syslog Servers** form appears.



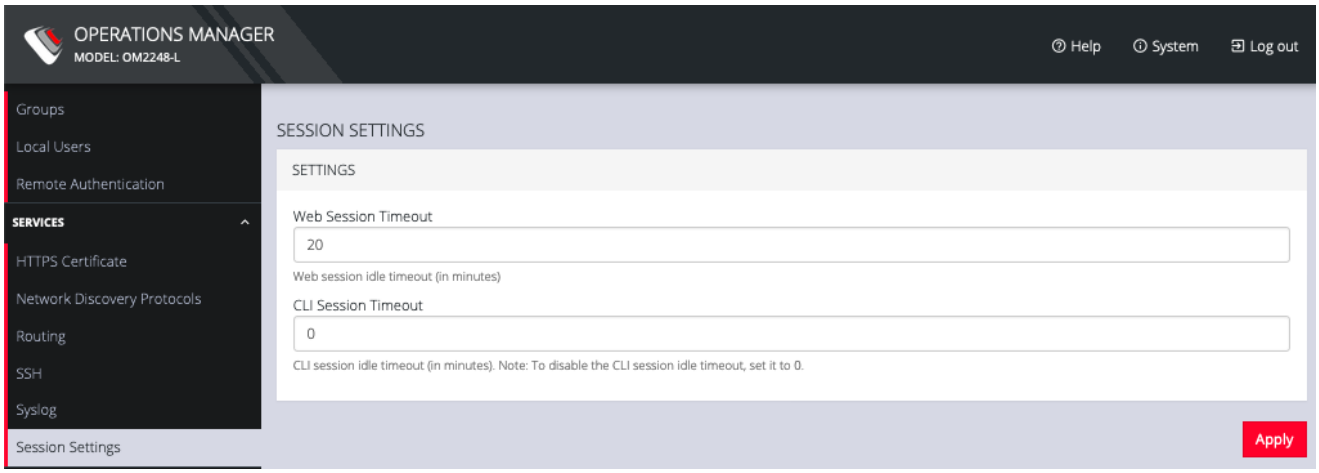
2. Enter the **Server Address**.
3. Enter the Protocol, either **UDP** or **TCP**.
4. Enter the correct **Port**. If no port is entered, UDP defaults to port 514 and TCP defaults to 601.
5. Click **Apply**.

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

5.11.6 Session Settings

To modify Web and CLI session settings select **SETTINGS > Services > Session Settings**.

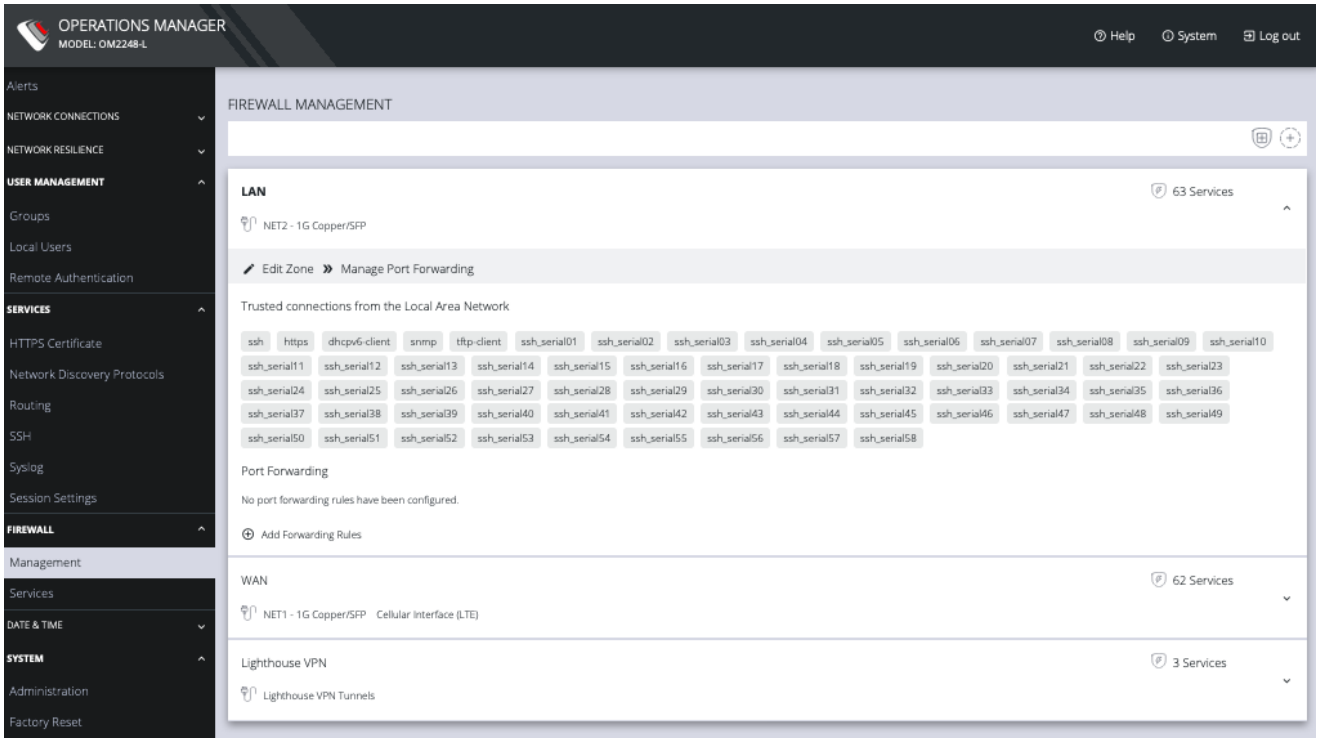
- **Web Session Timeout**: This value can be set from 1 to 1440 minutes.
- **CLI Session Timeout:** This value can be set from 1 to 1440 minutes or set it to 0 to disable the timeout. Changes take effect the next time a user logs in via the CLI.



5.12 Firewall

The CONFIGURE > FIREWALL menu lets you change firewall management, rules, zones, and services.

To change firewall management settings click **CONFIGURE > FIREWALL > Management**.



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

The **EDIT FIREWALL SETTINGS** page allows you to:

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

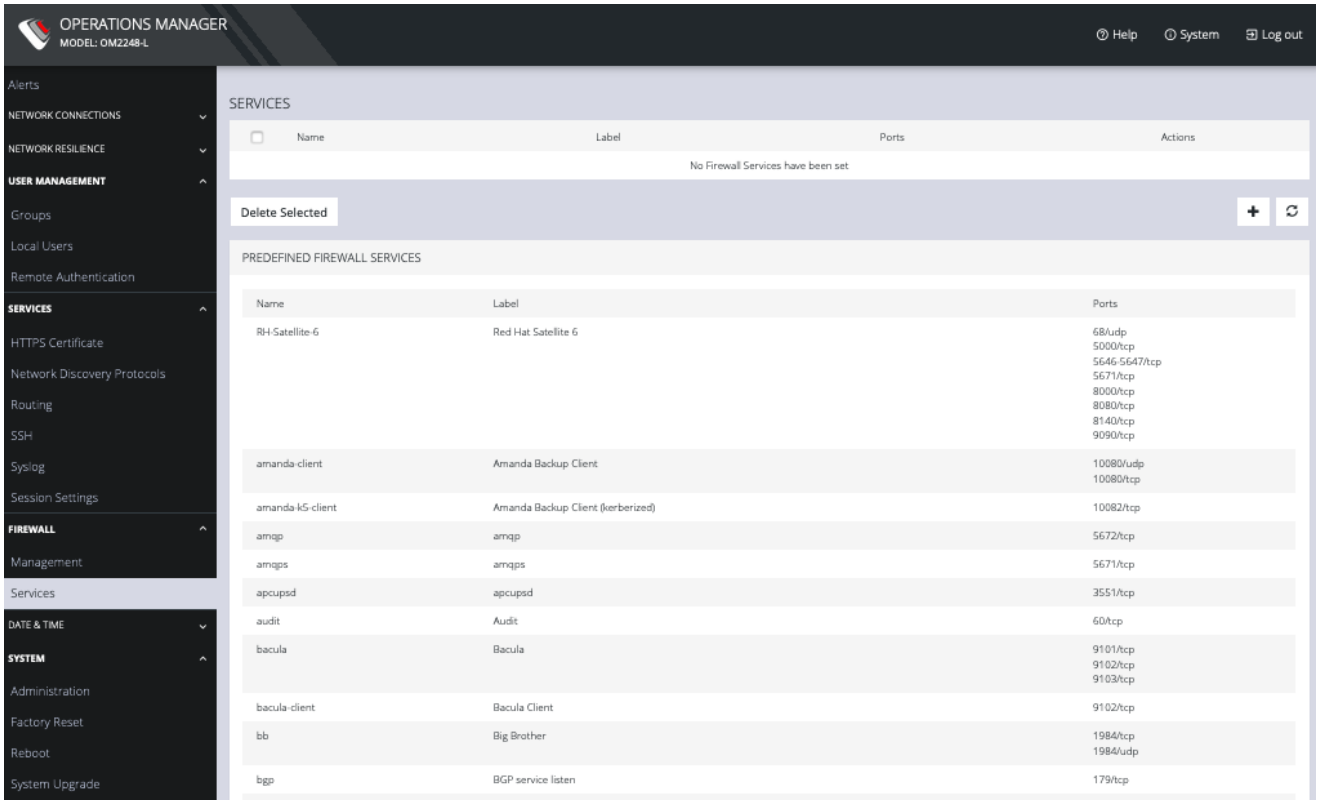
NOTE: You can use the Filter Interfaces and Filter Available Services text boxes to navigate through the lists.

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

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

Manage Firewall Rules

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



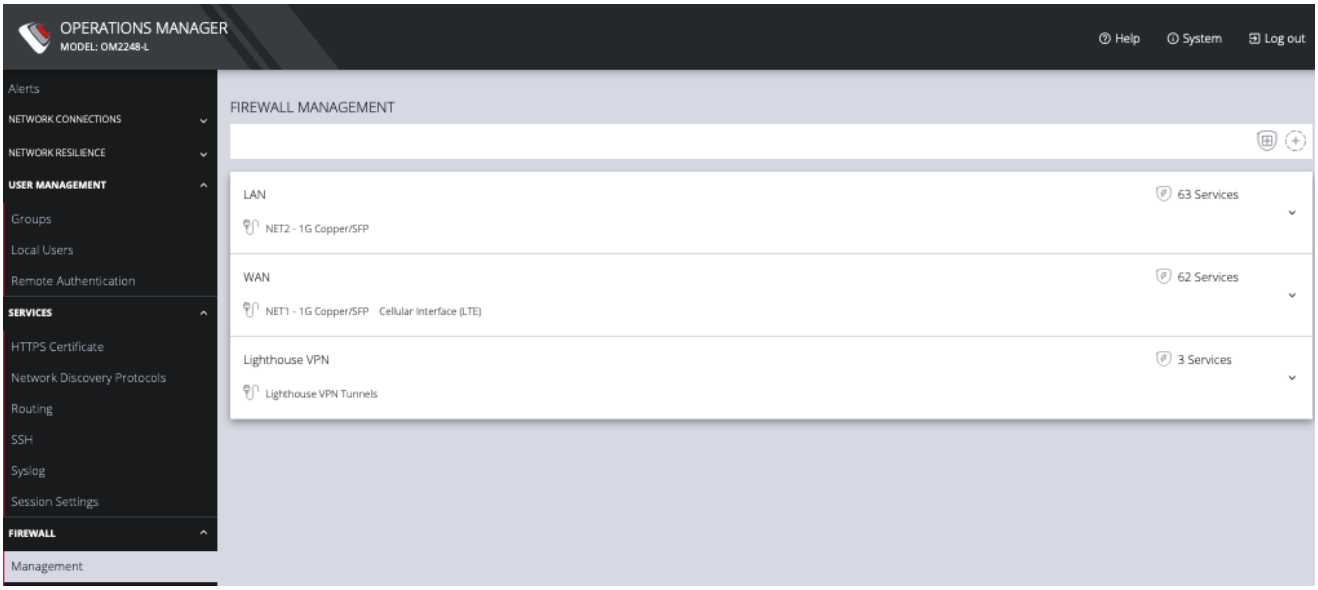
Services can be added, deleted, or edited from this page. Scroll to the bottom of the page to access the Plus button to add a new service.

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

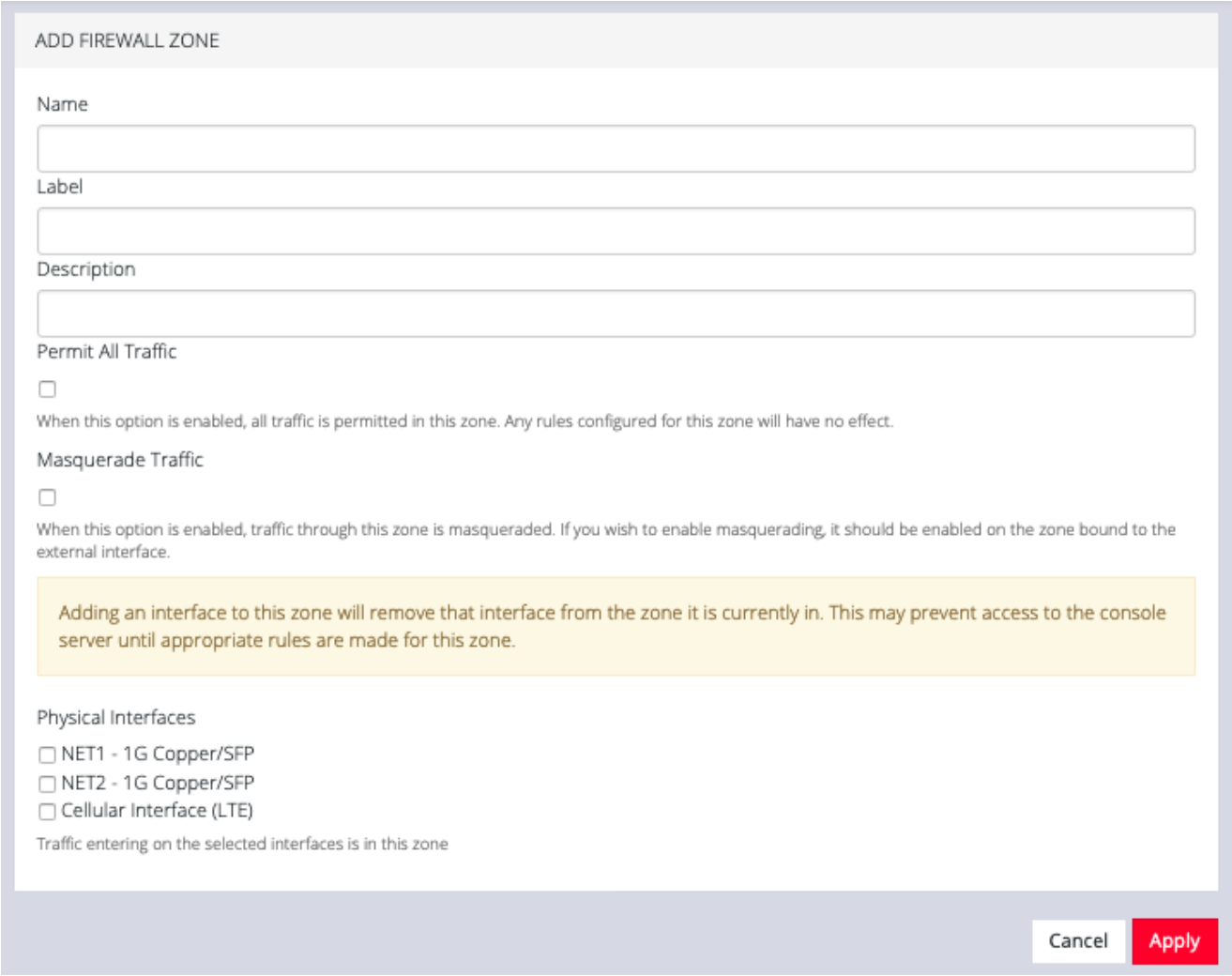
Manage Firewall Zones

Click **CONFIGURE > FIREWALL > MANAGEMENT.**

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



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

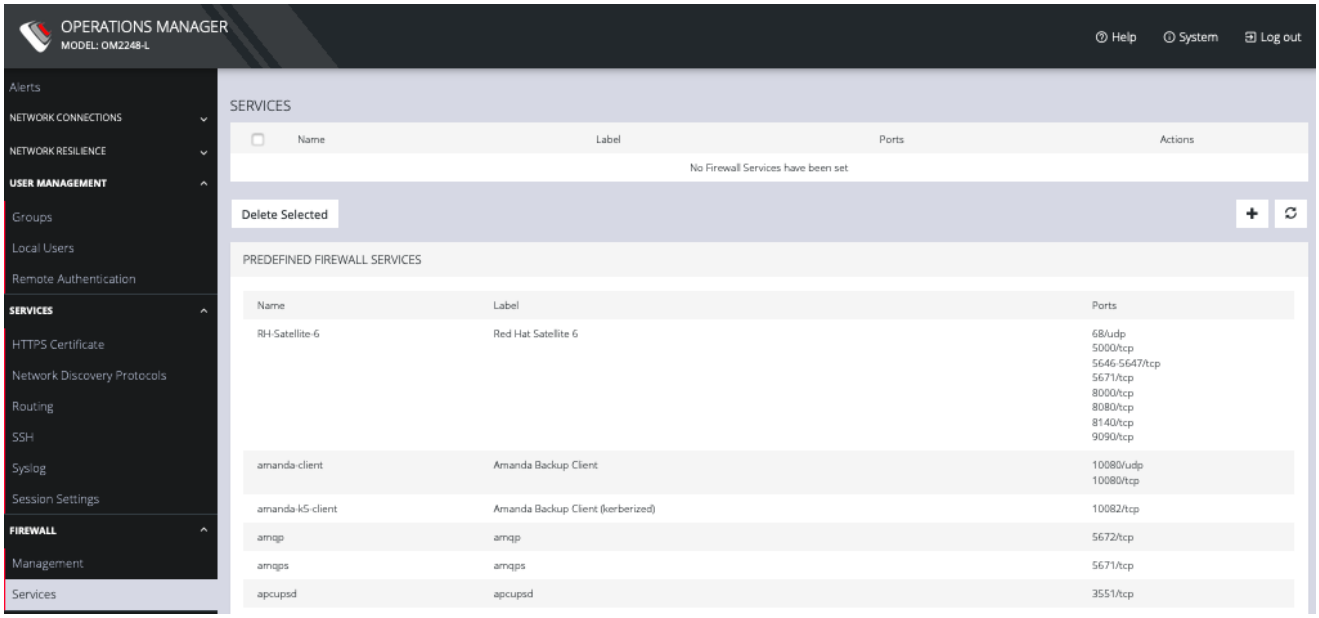


The **ADD FIREWALL ZONE** page allows you to:

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

Manage Firewall Services

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



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

NOTE: Predefined services cannot be edited.

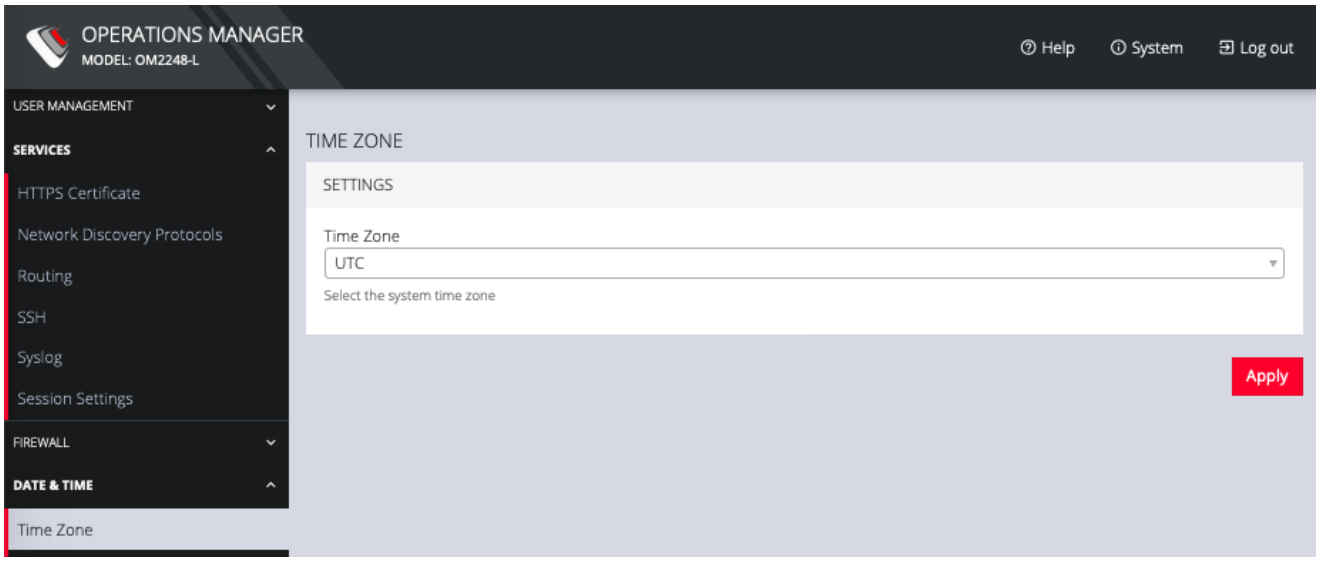
Click the **Plus** button to add a new service.

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

5.13 Date & Time

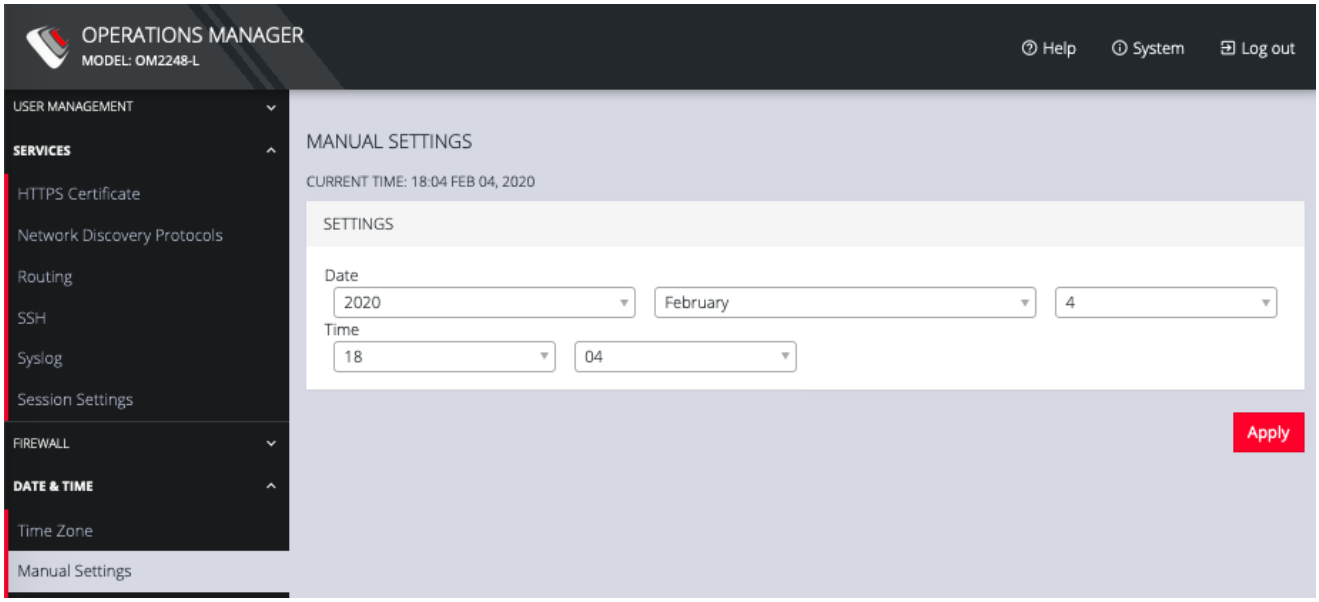
To set the time zone:

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



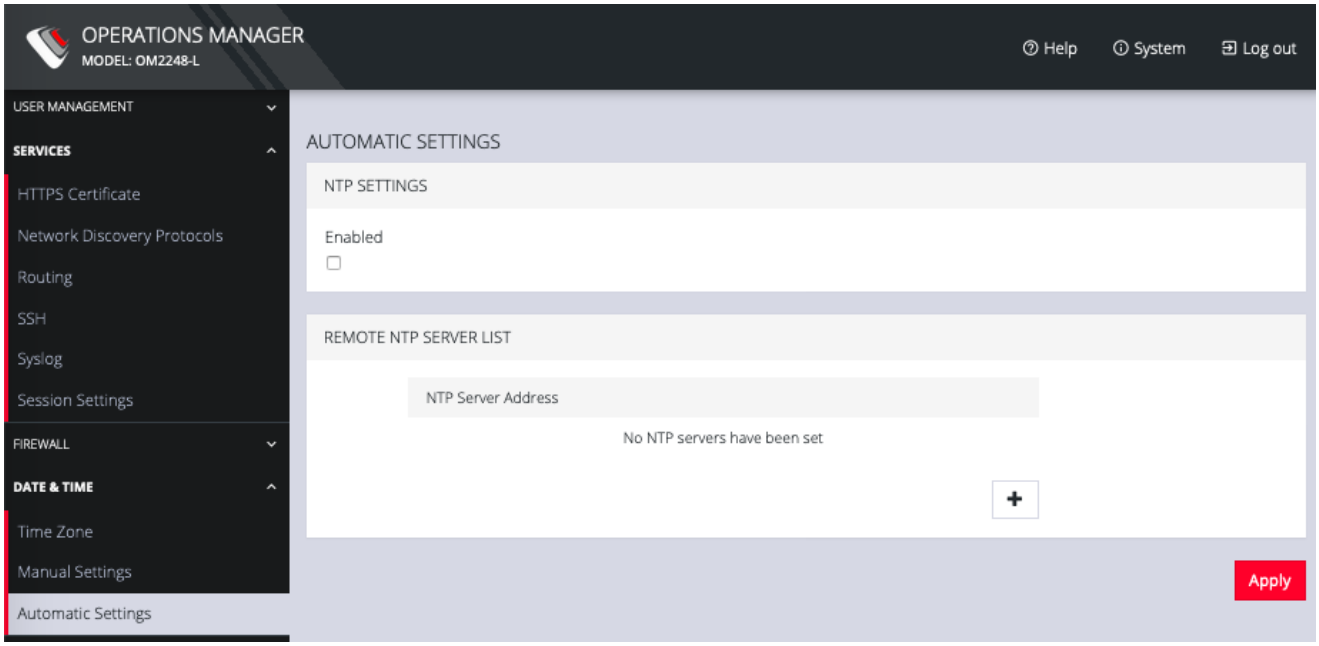
To set the correct time and date, either

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



or

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**.

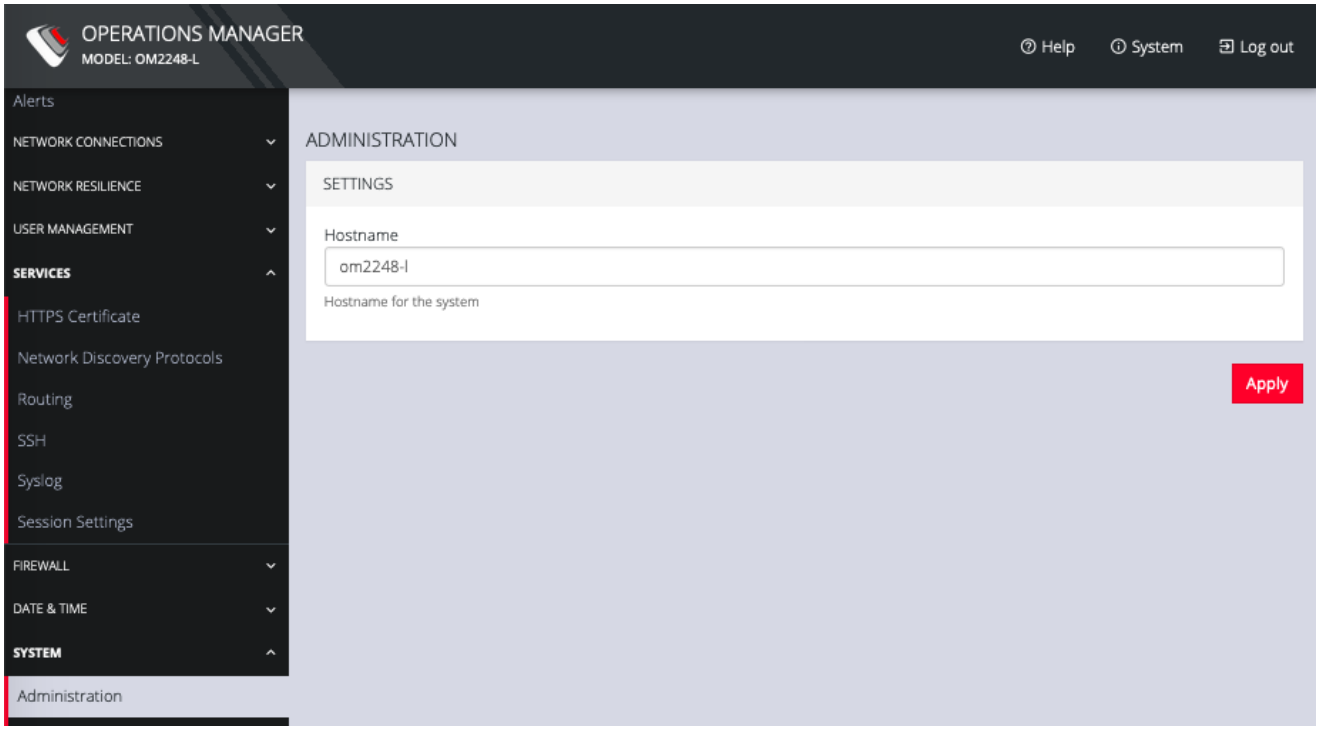


5.14 System

The **CONFIGURE > System** menu lets you change the OPERATIONS MANAGER's host-name, perform system upgrades, and reset the system.

To set the hostname for the OPERATIONS MANAGER:

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

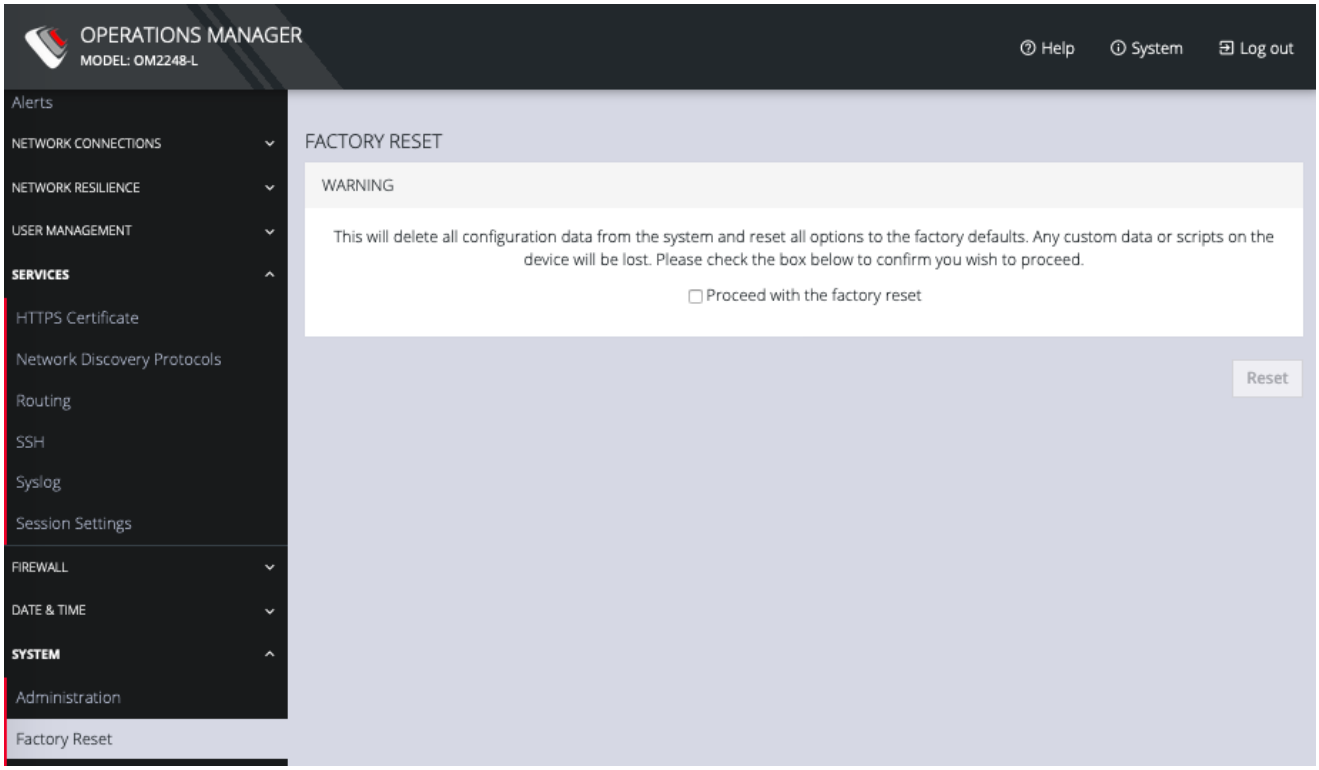


3. Click **Apply**.

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**.

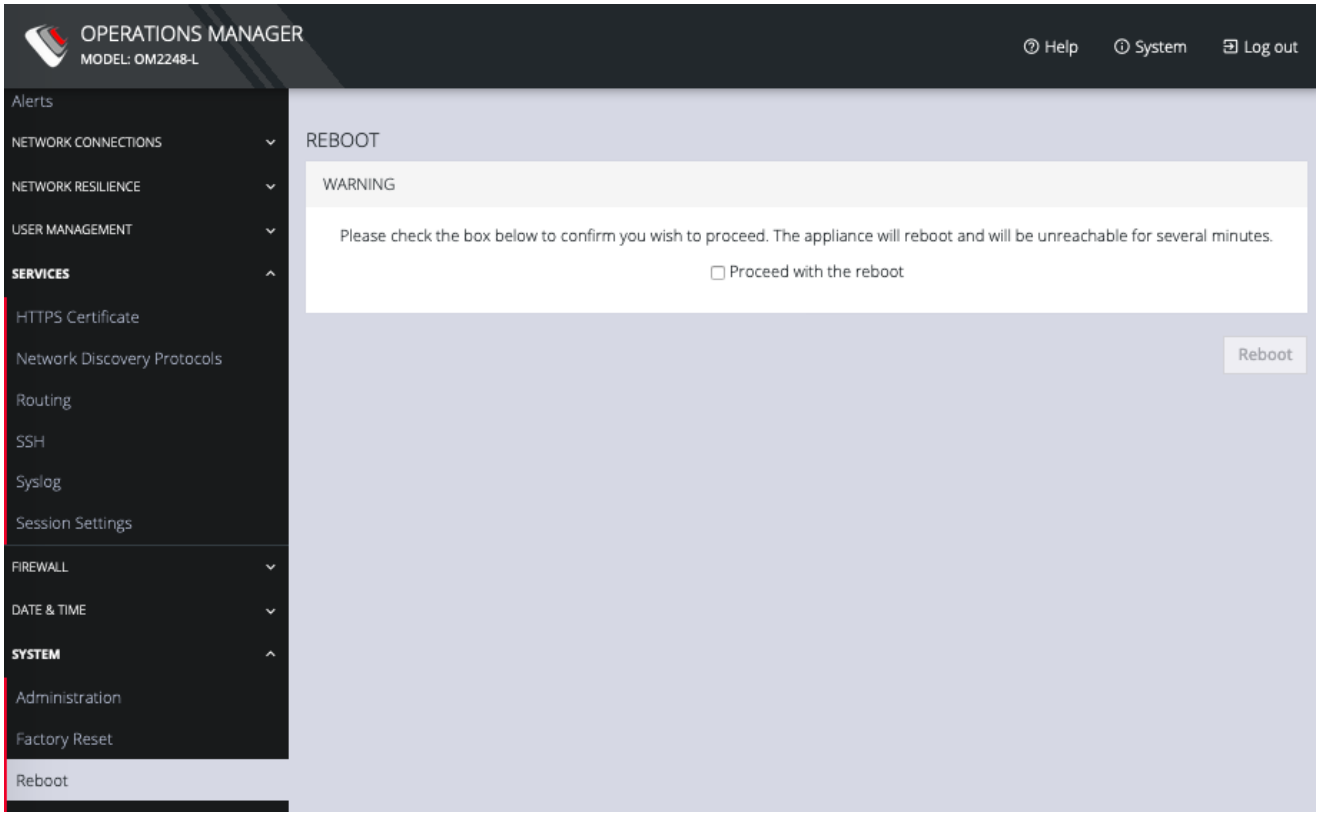


2. Select the **Proceed with the factory reset** checkbox.
3. Click **Reset**.

NOTE: This performs the same operation as the hard factory erase button covered section 1.7. 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.

To reboot the OPERATIONS MANAGER:

Select **CONFIGURE > System > Reboot**.

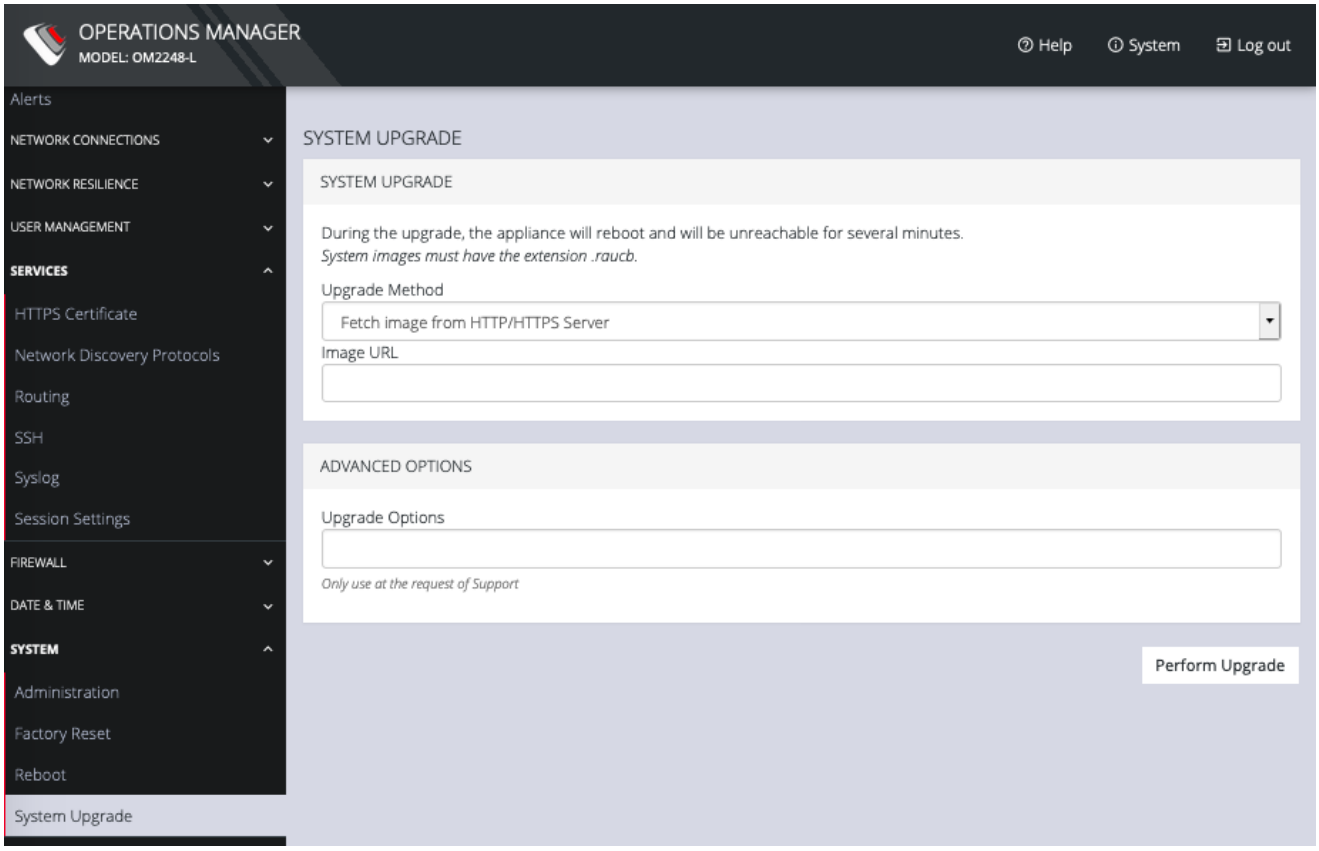


Select**Proceed with the reboot** and click **Reboot**.

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

To perform a system upgrade:

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



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

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

Or if upgrading via **Upload Image**:

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

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

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

6. Advanced Options

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

6.1 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:

-h, --help	Show help options
--help-all	Show all help options
--help-manager	Show manager options
--help-common	Show common options
--help-modem	Show modem options
--help-3gpp	Show 3GPP related options
--help-cdma	Show CDMA related options
--help-simple	Show Simple options
--help-location	Show Location options
--help-messaging	Show Messaging options
--help-voice	Show Voice options
--help-time	Show Time options
--help-firmware	Show Firmware options

--help-signal	Show Signal options
--help-oma	Show OMA options
--help-sim	Show SIM options
--help-bearer	Show bearer options
--help-sms	Show SMS options
--help-call	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

6.2 ogcli

ogcli allows users to inspect and modify the configuration tree from the command line.

6.2.1 Commands to try from within the ogcli tool

- `-h, --help` show this help message and exit
- `--notation` show the simple notation reference and exit
- `--list, --list-endpoints`
  - list endpoints
- `--usage` show usage examples and exit
- `-d` increase debugging (up to 2 times)

- `-j` use JSON instead of simple notation (pass twice to pretty-print output)
- `-u USERNAME, --username USERNAME`
  - authenticate as a different user
- `-p PASSWORD, --password PASSWORD`
  - authenticate with the supplied password
- `-n NEW_PASSWORD, --new-password NEW_PASSWORD`
  - authenticate with the supplied new password
- sub-commands:
  - operation
  - get (g) fetch a list or item
  - set (s) replace a list or item
  - update (u) update an item
  - create (c) create an item
  - delete (d) delete a list or item
  - list list endpoints

Run `ogcli operation -h` for help on that operation

6.2.2 Available endpoints

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

- `alerts/authentication` `get/set`
- `alerts/config_change` `get/set`
- `alerts/networking` `get/set`

- alerts/system get/set
- auth get/set
- auto_response/beacon(s) create/get/set/delete (get) id
- auto_response/reaction(s) create/get/set/delete (get) id
- auto_response/status get
- cellfw/info get
- cellmodem get
- conn(s) create/get/set/delete (get) id
- failover/settings get/set
- failover/status get
- firewall/predefined_services get
- firewall/rule(s) create/get/set/delete (get/delete) id
- firewall/service(s) create/get/set/delete (get) id
- firewall/zone(s) create/get/set/delete (get) id
- group(s) create/get/set/delete

(get/set) id

- ip_passthrough get/set
- ip_passthrough/status get
- ipsec_tunnel(s) create/get/set/delete (get) id
- lighthouse_enrollment(s) create/get/delete (get) id
- logs/portlog get id
- managementport(s) get/set (get) id
- monitor/lldp/chassis get
- monitor/lldp/neighbor get
- physif(s) create/get/set/delete (get) id
- port(s) get/set (get) id
- port_session(s) get/delete (get/delete) id pid
- ports/auto_discover/schedule get/set
- ports/fields get
- search/ports get

- services/https get/set
- services/lldp get/set
- services/ntp get/set
- services/routing get/set
- services/snmp_manager get/set
- services/ssh get/set
- services/syslog_server(s) create/get/set/delete (get)
  syslog_server_id
- ssh/authorized_key(s) create/delete (get)
  user-id key-id
- system/cell_reliability_test get/set
- system/cli_session_timeout get/set
- system/firmware_upgrade_status get
- system/global_enrollment_token get/set
- system/hostname get/set
- system/model_name get
- system/serial_number get
- system/ssh_port get/set
- system/time get/set
- system/timezone get/set

- system/version get
- system/webui_session_timeout get/set
- user(s) create/get/set/delete
  (get/set) user-id

6.2.3 Using ogcli

ogcli example usage

Retrieve items:

```
ogcli get users > record_list

ogcli get user users-1 > record
```

Replace items:

```
ogcli set users < record_list

ogcli set user users-1 < record
```

Modify items:

```
ogcli update user users-1 < partial_record

ogcli update user users-1 'field="value"'
```

Create items:

```
  ogcli create user < record
```

Delete items:

```
  ogcli delete user users-1
```

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

ogcli create user < record

```
ogcli create user <<END
  username="root"
  description="superuser"
END
```

```
echo 'username="root" description="superuser"' | ogcli create user
```

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

ogcli also takes records from any extra command line arguments.

Note Double-quotes around strings should be protected from the shell.

```
ogcli create user 'username="root"' 'description="superuser"'
```

6.3 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.

To find out more, enter `docker –help`.

6.4 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 3am:

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

Save and close the file.

7. EULA and GPL

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