opengear
A DIGI Company

CONSOLE MANAGER 25.11

USER GUIDE version 3

CONTENTS

CONTENTS 2
COPYRIGHT © 17
WHAT'S NEW 18
Release Versions 18
User Guide Version 2 Updates 19
User Guide Version 1 Updates 20
SAFETY & FCC STATEMENT 22
Safety Statement 22
FCC Warning Statement 22
ABOUT THIS USER GUIDE 24
INSTALLATION AND CONNECTION 25
Power Connection 27
Dual Power Supply 28
LED Power Status Indicator 29
SNMP Alerts for Power-related Events 30
Device Status LEDs 30
Connect to the Network 33
Serial Connection 33
Cellular Connectivity 34
Cellular Modem Antenna Gain Specifications 35
MPE Safe Distance Statement 35

CM8100-10G-C Antenna Gain and Collocated Radio Transmitter Specifications 35
Antenna Gain 35
Collocated Radio Transmitters 36
RF Band Support 36
Device Reboot 37
INITIAL SETTINGS 38
Default Settings 38
Serial Port Settings 38
Browser WebUI 38
UsE the WebUI 39
Management Console Connection via CLI 40
Access the WebUI CLI Terminal 40
Change the Root Password 41
Disable a Root User 43
Change Network Settings 43
Add a New Connection 44
Change the Ethernet Media Type 45
MONITOR MENU 47
System Log 47
LLDP CDP Neighbors 48
Triggered Playbooks 48
Cellular Modem 48

ACCESS MENU 51
Local Terminal 51
Serial Ports 52
Quick Search 53
Access Using Web Terminal or SSH 53
Serial Port Logging 54
Display Port Logs 54
CONFIGURE MENU 55
Serial Ports 55
Edit Serial Ports 55
Assigning Unique IP Addresses for Each Console Port 58
Configure Single Sessions for Ports 59
Single Session Enabled In the WebUI 60
In Config Shell 62
Single Session Behavior 64
Configure Raw TCP Access for Serial Ports 65
Service Implementation 65
WebUI Configuration 66
Config CLI Configuration 67
ogcli Configuration 69
Autodiscovery 69
Autodiscovery Enhancements 70
Cancel Autodiscovery 71

Schedule Autodiscovery 71
Retrieve Port Discovery Logs 72
Local Management Consoles 73
Lighthouse Enrollment 74
Manual Enrollment Using UI 75
Manual Enrollment Using the CLI 76
Automatic Enrollment By Lighthouse Service Portal (LSP) 76
LSP Service Initialization 77
LSP Commands 78
Restart The Service 78
LSP Errors and Exit Codes 78
Access Lighthouse Service Portal 80
Register an account / log in to Lighthouse Service Portal 80
Dashboard 81
Permissions 81
ENROLLMENT SETTINGS 82
ASSETS 83
USER MANAGEMENT 84
Playbooks 86
Create Or Edit a Playbook 87
Monitor a current Playbook 92
PDUs 92
Add and Configure a PDU 93

System Alerts 95
System Alerts - General 96
Authentication 96
Configuration Change 96
System Alerts - Power 97
Enable Power Supply Syslog Alerts 97
System Alerts - Networking (Connection Status) 98
Configure Signal Strength Alerts 99
Network Connections 99
Network Interfaces 100
Dual SIM 100
Cellular Modem Firmware Upgrade 111
Bonds and Bridges 125
Spanning Tree Protocol 131
Configure a VLAN 134
IPsec Tunnels 137
Create, Add or Edit IPsec Tunnels 138
Static Routes 141
Create a Static Route 143
Edit or Delete a Static Route 144
Manage Static Routes via Command Line 144
Network Resilience 146
Out-Of-Band Failover 146

Enable Out-Of-Band Failover 147
DNS Queries on a Dormant Failover Interface 149
OOB Failover Types & Failover Behavior 150
IP Passthrough 151
User Management 153
Groups 153
Permission Changes in the Web UI 154
Understand Access Rights 154
Understand Serial Port Access 158
Create a New Group 161
Edit an Existing Group 163
Local Users 163
Create a New User With Password 165
Create a New User With No Password (Remote Authentication) 165
Modify An Existing User Account With Password 166
Manage SSH Authorized Keys for a User Account 167
Delete a User Account 167
Remote Authentication 168
Configure RADIUS Authentication 169
Configure TACACS+ Authentication 170
Configure LDAP Authentication 172
Configure LDAP over SSL 173
LDAP and LDAPS Port Settings 174

Limitations for LDAPS Implementation 175
Local Password Policy 175
Set Password Complexity Requirements 176
Set Password Expiration Interval 177
Password Policy Implementation Rules 178
Services 179
FIPS Compliance 179
Considerations for Using the FIPS Feature 180
Enable FIPS mode at the CLI 182
Disable FIPS 183
Verify that FIPS is Enabled 183
Brute Force Protection 184
Configure Brute Force Protection 185
View Current Bans 186
Manage Brute Force Protection via Command Line 186
HTTPS Certificate 188
Network Discovery Protocols 191
Routing 193
Dynamic Routing 193
Static Routing (via the ogcli) 194
OSPF Configuration 195
Wireguard Configuration 203
SSH 211

Unauthenticated SSH to Serial Ports 211
Syslog 217
Add a New Syslog Server 217
Global Serial Port Settings 218
Edit or Delete an Existing Syslog Server 220
Session Settings 222
File Server 223
Enable TFTP Service 223
Modify Firewall Zones to Allow the TFTP Service to be Used 223
Update the TFTP Service Storage Location 224
SNMP Service 225
SNMP Alert Managers 226
Multiple SNMP Alert Managers 227
Firewall 230
Firewall Guide 230
Introduction 230
Firewall Rules 231
Firewall Policies 232
Example WebUI Configuration 232
Custom Rules (firewalld “rich-rules”) 234
Useful Templates for use in WebUI or CLI 235
Firewall Management 237
Firewall Zone Settings 238

Firewall Source Address Filtering 240
Firewall Source Address Bulk Services 242
Firewall Policies 242
Logging and Debugging Firewall Policies 249
Firewall Services 249
Add WireGuard Zones to a Firewall 250
System 250
Administration 251
Date and Time Setting 252
Set the time by NTP 252
Set the time Manually 254
Factory Reset 255
Reset FROM THE WEBUI 255
Reset at the External Erase Button 256
Reset from the CLI Terminal 257
Reboot 258
Export/Restore Configuration 258
Export Configuration 258
Restore Configuration 260
Automated Rollback To Working Configuration 262
Lighthouse Node Backup 264
System Upgrade 265
Perform a System Upgrade VIA WEBUI 265

Perform a System Upgrade via CLI 266
ADVANCED OPTIONS 267
Communicate With The Cellular Modem 267
5G Settings and behavior 269
Standalone versus non-standalone operation 269
Run Diagnostics with Modem-Test 271
Config CLI GUIDE 273
Navigation in Config CLI 274
Start a Session in Config CLI 274
Exit a Config CLI Session 274
Navigate the Config CLI 275
Understand Fields, Entities and Contexts 276
Global & Entity-Context Commands 278
Global Context Commands 278
Entity Context Commands 279
Config CLI Entities 279
Supported Entities 280
Config CLI Commands 286
Add 287
Apply 288
Changes 292
Delete 293
Diff 295

Discard 298
Edit 301
Exit 302
help (or ?) 303
Import/Export 305
Show 308
up / exit / .. 312
Config CLI Use Case Examples 313
Users 314
Ports 318
Create or Configure Loopback Interface 321
Configure NET1 Static IPV4 325
Configure NET2 Static IPV4 325
Configure NET3 Static IPV4 for OM2224-24e units 326
Configure WireGuard through Config Shell 326
Passwords 327
Edit System Information 328
Enable NETGRP Set to ConsoleUser 330
Change SSH Delimiiter to : default is + 330
Enable TACACS - Set Mode to remotelocal 331
Enable LLDP on NET1 & NET2 331
Enable TFTP 331
Enable Boot Messages 331

Enable SIMM 1 332
Enable Failover 334
Syslog Server 334
Set Port Logging Remote Syslog Settings 335
Enable System Monitor SNMP Traps 335
SNMP 336
Create a Static Route 337
Firewall 337
Edit LAN (Net2) Firewall Zone 337
Edit WAN (Net1) Firewall Zone 338
Custom_rule Example for Port and Protocol 338
Enrol into Lighthouse 339
How Changes Are Applied or Discarded 339
Apply or Discard Changes 340
Multi-Field Updates 341
Description 341
Example 341
Error Messages 343
Error Messages 345
String Values In Config Commands 346
Description 346
Example 346
Error Messages 347

Opengear CLI Guide 348
Get Started with ogcli 348
Access ogcli Help and Usage Information 348
Basic Syntax 349
ogcli Operations 350
Supply Data To ogcli 351
Here Document 351
Inline Arguments 352
Pipes and Standard Input 352
Quoting String Values 352
Tab Completion 353
Display Secrets in ogcli 353
Common Configuration Examples 354
Replace Message of the Day (MOTD) Displayed at login 354
Retrieve User Record 355
Update Item with Field Where Value is a String 355
Update Item with Field Where Value is Not a String 355
Export System Configuration 355
Import System Configuration 356
Restore System Configuration 356
Compare Current Configuration with a Proposed Configuration 356
Use the diff Tool 356
Enable Local Console Boot Messages 360

Create New User 361
Change Root Password 361
Create New Administrative User 361
Manually Set Date and Time 361
Enable NTP Service 362
Update System Hostname 362
Adjust Session Timeouts 362
Setup Remote Authentication with TACACS+ 362
Setup Remote Authentication with Radius 363
Create User Group with Limited Access to Serial Ports 363
View and Configure Network Connections 363
Configure a DNS 364
Configure a DNS via the Command Line 365
Configure Serial Ports 365
Enable Cellular Modem Interface 366
Disable Cellular Modem Interface 366
Advanced Portmanager PMShell Guide 367
Running pmshell 367
pmshell Commands 367
Custom Control Codes for Serial Ports 368
Configure Custom Control Codes 369
Configure Control Codes for a Specified Port (CLI Examples) 369
Configure a Control Code Value for All Ports 370

Control Codes for All Ports via CLI (Examples) 370
DNS Configuration 370
Configure DNS via the Web UI 371
Name Servers 371
DNS Search Domains 372
Configure DNS via the Command Line 372
Docker 373
Docker CM8100 Support 373
AMD64 Docker Container Usage 374
System Resource Utilization 374
Cron 374
Initial Provisioning via USB Key 376
Restrict Web Server Remote Access 377
EULA and GPL 378
UI BUTTON DEFINITIONS 379

COPYRIGHT ©

Opengear Inc. 2026. 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.

WHAT'S NEW

RELEASE VERSIONS

The following table describes release dates for the software and user guide for 25.11 releases. The link from the software to the user guide always points to the latest version of the user guide.

Release Date	Software Version	User Guide Version	Description Of Changes
June 2026	25.11.7	3	• For a full list of any features, improvements, or bug fixes for the Console Manager 25.11 software, see the Release Notes. • Update made to the Advanced Options section to include information around added support to restrict the webserver to the loopback interface only.
June 2026	25.11.6	2	For a full list of any features, improvements, or bug fixes for the Console Manager 25.11 software, see the Release Notes.
May 2026	25.11.5		
March 2026	25.11.4		
January 2026	25.11.3		
January 2026	25.11.2		

Release Date	Software Version	User Guide Version	Description Of Changes
January 2026	-	2	This is a documentation only update to align with a product release. For more information, see User Guide Version 2 Updates.
December 2025	25.11.1	1	For a full list of any features, improvements, or bug fixes for the Console Manager 25.11 software, see the Release Notes.
November 2025	25.11	1	• For a full list of any features, improvements, or bug fixes for the Console Manager 25.11 software, see the Release Notes. • For details of changes to the user guide, see User Guide Version 1 Updates.

USER GUIDE VERSION 2 UPDATES

Updates have been made to the following topics to include information around the new CM8000 variant where appropriate:

- Installation and Connection
- Dual Power Supply
- Device Status LEDs
- Connect to the Network
- Serial Connection

- Default Settings
- Serial Ports
- Local Management Consoles
- Lighthouse Enrollment
- System Alerts - Power
- System Alerts - Networking
- Enable System Monitor SNMP Traps

USER GUIDE VERSION 1 UPDATES

- Information to describe how Out-Of-Band Failover works has been added to the Out-of-Band-Failover topic.
- The HTTPS Certificate topic has been updated to:
  - add information for the **Subject Alternative Name** (SAN) field.
  - restructure the topic and provide more information about the available fields.
- A new modem test diagnostic tool has been added and is described on the following new topics:
  - CLI: Run Diagnostics with Modem-Test
  - Web UI: Cellular Modem
- The **Configure >** Serial Ports topic has been updated under Edit Serial Ports to include information for a new **DTR and RTS pins** field.
- Additional Message of the Day (MOTD) information and examples have been added. The following topics have been updated:
  - The Config CLI Use Cases > Edit System Information topic under Define MOTD.
  - The Advanced Options > OGCLI Guide topic under Replace MOTD Displayed at Login.
- The Cellular Modem Firmware Upgrade topic has been updated to add:
  - the See all cell firmware installed on the modem via ogcli section to include information about the ability to get all installed firmware on the modem via ogcli.

  - the Update Cell Firmware with a Cell Only Connection section to include steps for updating cell firmware with a cell only connection.
  - more information around the 'defer if failed over' feature under Cellular Availability During Upgrade.
- The Device Status LEDs topic has had a minor update to clarify differences between port types.

SAFETY & FCC STATEMENT

SAFETY STATEMENT

Please take care to follow the safety precautions below when installing and operating the Console 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

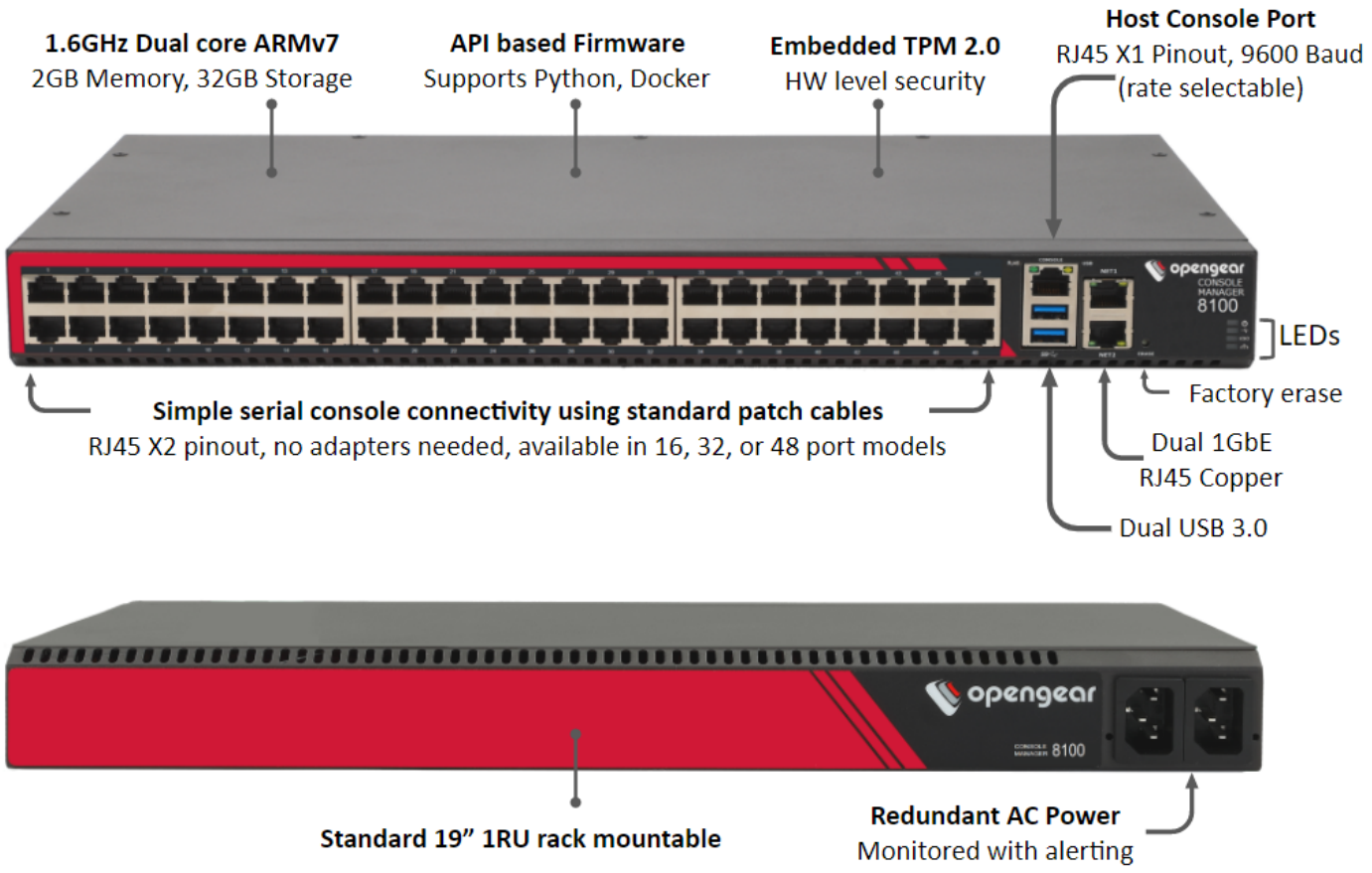
This user guide describes how to use Console Manager and is current as of June 25, 2026.

When using a minor release, there may or may not be a specific version of the user guide for that release. For information about specific software and user guide versions, see Release Versions.

INSTALLATION AND CONNECTION

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

CM8100 Features:



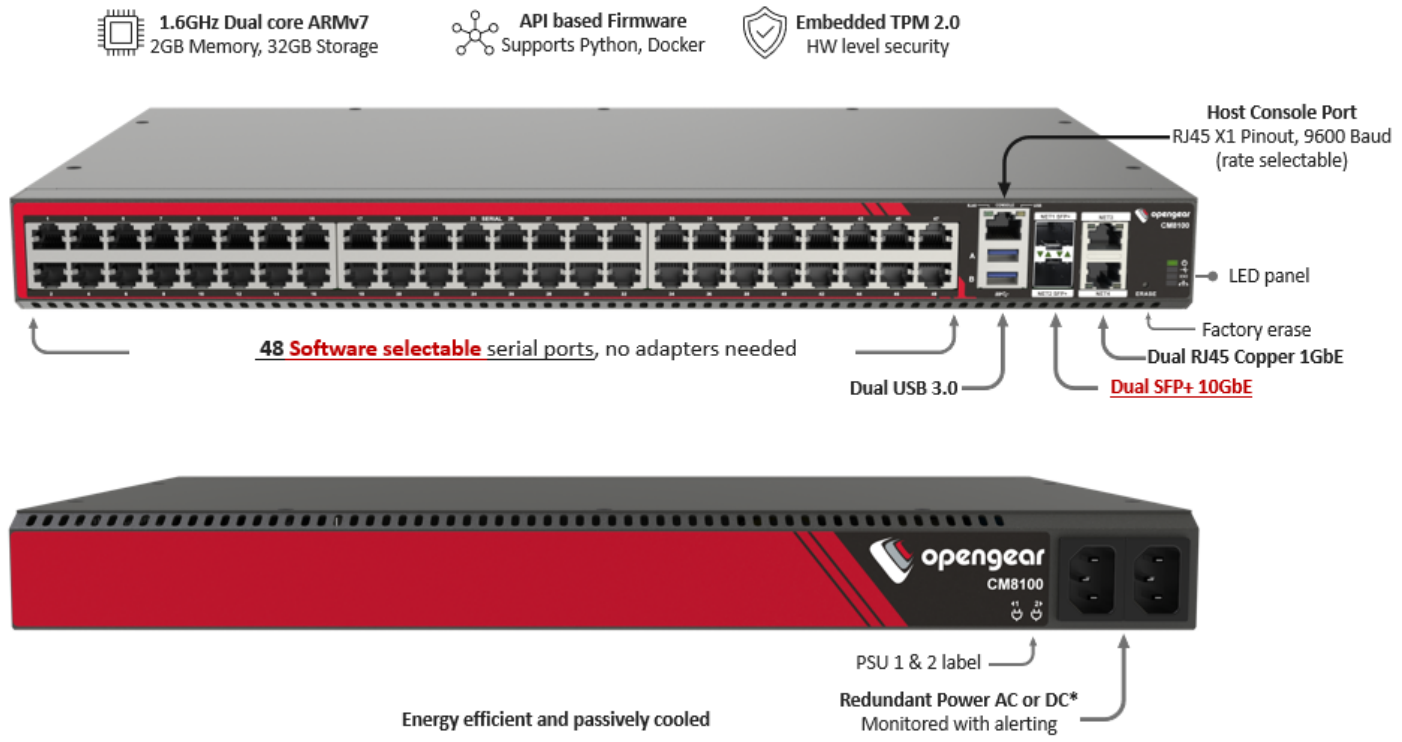
CM8100-10G Features

> **Note:** Serial USB Variant - The CM8100-10G model has a USB variant that comes with 8 x USB-C 2.0 for Serial Ports on the rear of the device.

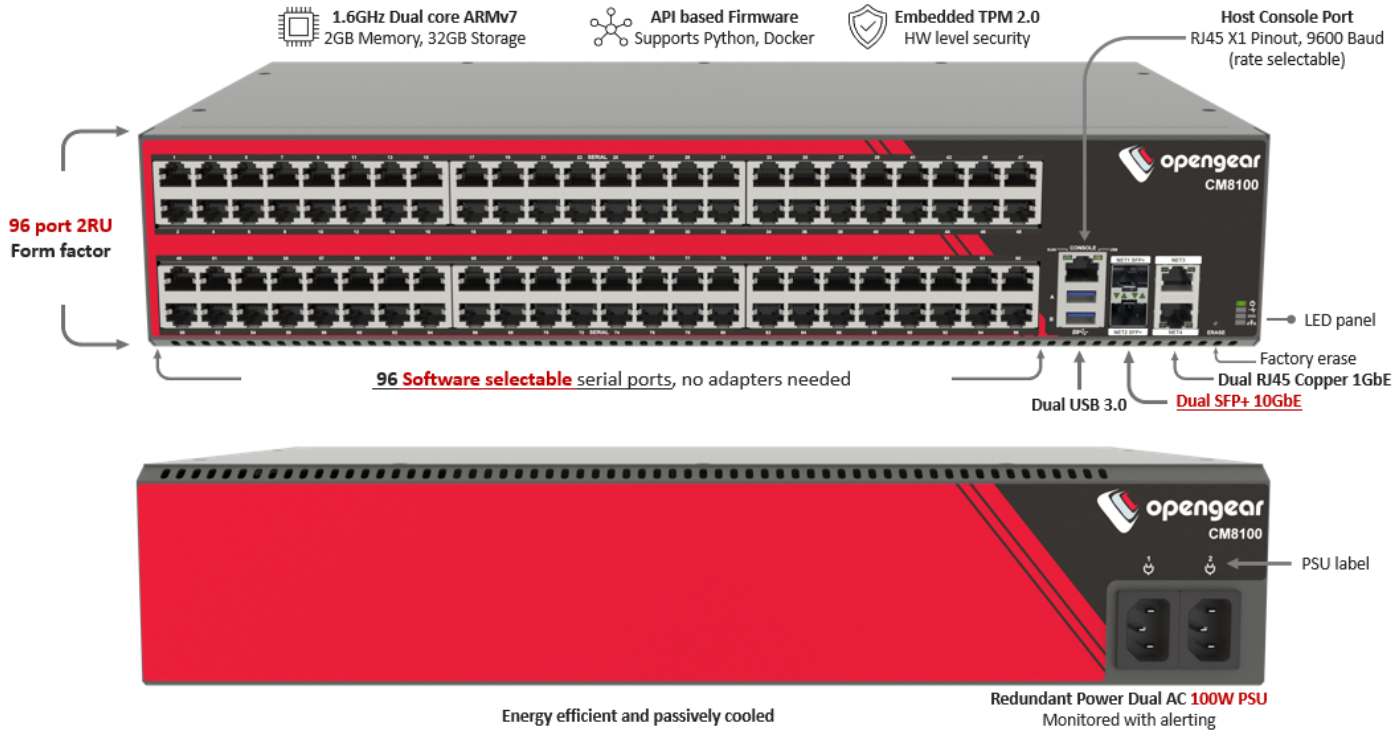
The following features apply to the CM8100-10G model:

- Static IP on Net 3.
- Pin out switching by software selectable pinout.
- Two additional 10G SFP+ fiber interfaces.

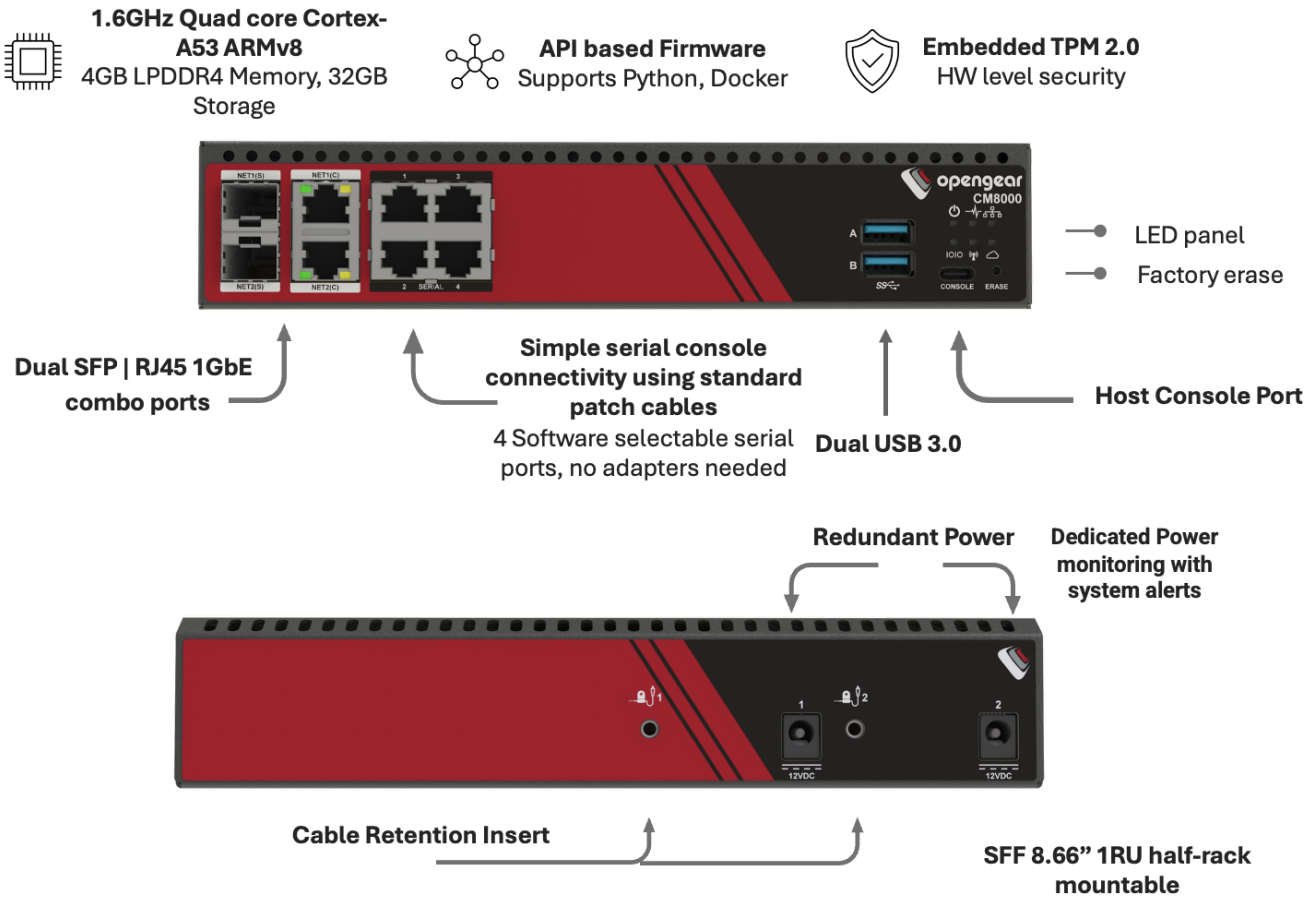
CM8148-10G



CM8196-10G



CM8000 Features



POWER CONNECTION

> **Note:** The power cord is useable only with the device. Do not use it for any other purpose.

The CM8100 models have dual power inlets with built-in auto failover. These power supplies accept AC input voltage between 100 and 240 VAC with a frequency of 50 or 60 Hz. See the following tables for typical power draw.

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

Notes:

- Dual DC Power Supply. DDC models have a dual DC power supply with screw-in DC terminals (supplied).
- Country specific IEC power cords are included with the CM8100.

For more information, see Dual Power Supply, and System Alerts - Power.

Console Manager Platform (CM8100) Environmental And Power	
Power Supply	Dual AC
Power Draw CM8100	Typically <15W
Power Draw CM8100-10G	CM8148-10G <25W Typical CM8196-10G <30W Typical
Operating conditions	Temperature 5~50C, Rel Humidity 5~90%
Cooling	Passive
Power Draw Sensors	Active multi-zone power draw monitoring of 12V power. No monitoring on 120V AC.

DUAL POWER SUPPLY

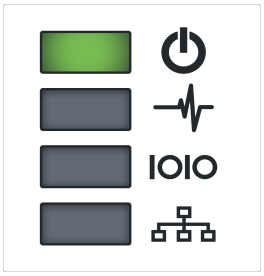
Dual Power Supply, including Dual DC (DDC) can provide power redundancy for devices, especially those that may operate in harsher environments. A secondary power supply provides redundancy for the device if one PSU is unplugged or in the event of a failure.

LED POWER STATUS INDICATOR

The power LED indicator requires no configuration and displays the dual power status on the Console Manager device.

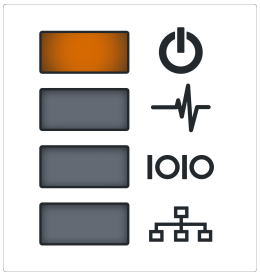
> **Note:** CM8000 devices have displays with six LEDs that include Lighthouse (Cloud) and Network Status. See Device Status LEDs for LED definitions.

On a **dual** PSU device that has power connected to *two* PSUs, the LED power status indicator should be green at all times.





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





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.
- configured in the Configure > SNMP Alerts page, see System Alerts - Power.

DEVICE STATUS LEDS

The LED states shown in the following table are determined through user-configurable threshold values for the Cell LED Amber / Green light, and modem enabled / disabled information.

	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: The 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.

LED Condition					
	LED Off	**Amber Flashing**	**Amber Solid**	**Green Flashing**	**Green Solid**
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.
CM8100 ONLY					
NET1	No active network connection	Network activity	Network link (any speed)	N/A	Network link 1G.
NET2	No active network connection	Network activity	Network link (any speed)	N/A	Network link 1G.
CM8100-10G ONLY					
NET1	No active network connection	Network activity	Network link	Network activity 10G	Network link 10G.
NET2	No active network connection	Network activity	Network link	Network activity 10G	Network link 10G.
NET3	No active network connection	Network activity	Network link (any speed)	N/A	Network link 1G.
NET4	No active network connection	Network activity	Network link (any speed)	N/A	Network link 1G.
CM8000 ONLY					

LED Condition					
	LED Off	**Amber Flashing**	**Amber Solid**	**Green Flashing**	**Green Solid**
NET1	No active network connection	Network activity	Network link (any speed)	N/A	Network link 1G.
NET2	No active network connection	Network activity	Network link (any speed)	N/A	Network link 1G.
Cloud / Internet 	LSP is disabled and there are no existing Lighthouse enrollments.	LSP is currently running on the device.	An error occurred while running LSP.	The device can reach the lighthouse instance and is attempting to enroll. If a lighthouse is unreachable the LED will not start.	The device is enrolled and connected to a lighthouse. There will be a short delay between the UI status reported and the LED changing to solid green.
IOIO 				Any serial activity is received, on either console/usb console or device serial ports (RJ45).	

Notes:

- The amber LED signal threshold configuration is set to 50%.of normal signal strength.
- CM8100 series devices do not have a cloud LED, therefore, no LED indication is available for LSP or Lighthouse.

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

- System Alerts - Networking (Connection Status)
- System Alerts - Power

CONNECT TO THE NETWORK

Generally, Console Manager products have two network connections labeled NET1 and NET2. In the CM8100 and CM8000 there are options for copper wiring (on a standard RJ-45 connector). The CM8100-10G also has a static IP port on NET3.

> **Note:** Installing an SFP module triggers a communication between the module and the device. Usually, this automatically limits the Ethernet interface to 1G. However, if a 10G interface is indicated, support the interface will be configured for 10G speeds.

The network connections on the CM8100 and CM8000 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.

SERIAL CONNECTION

> **Note:** X1 and X2 are Opengear specific labels, where X2 = Cisco straight and X1 = Cisco reversed.

CM8100

Serial Ports: The serial connections feature RS-232 with Cisco Straight X2 pinout, 50 to 230, 400bps. Connect serial devices with the appropriate STP cables.

> **Note:** The CM8100-10G also offers a software-selectable pin out (Port PinOut) on all serial ports.

Console Port: 1 x RJ45 RS-232 Console Port - Cisco rolled X1 pinout, baud rate 9600

CM8000

Serial Ports: The serial connections feature RJ45 RS-232 X2 Pinout 50 to 115,200bps. Connect serial devices with the appropriate STP cables.

Console Port: 1 x USB-C Console Port- X2 Pinout, baud rate 9600/8N1.

CELLULAR CONNECTIVITY

> **Note:** This section applies to cellular variants only. The CM8000 does not support cellular connectivity.

The cellular interface is certified for global deployments with most carriers and provides a 5G NR Sub-6 and LTE CAT20 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.

INSTALL A NEW SIM CARD

When you install a new SIM card into its slot while the appliance is active (hot swapping), it may take a minute or two for the system to react and stabilize after the SIM card change.

Two SIM card slots are located on the rear face of the device, insert each SIM card(s) into its respective slot (marked 1 and 2) until you feel the card click into place.



CELLULAR MODEM ANTENNA GAIN SPECIFICATIONS

> **Note:** This section applies to cellular variants only. The CM8000 does not support cellular connectivity.

MPE SAFE DISTANCE STATEMENT

Opengear cellular products are intended for use 28cm or more from the body. This meets limits for Maximum Permissive Exposure (MPE) and is the minimum safe distance.

CM8100-10G-C ANTENNA GAIN AND COLLOCATED RADIO TRANSMITTER SPECIFICATIONS

ANTENNA GAIN

Cellular Modem Frequency CM8100-10G-C						
Antenna Gain and Collocated Radio Transmitter Specifications						
Note: The radiated power of a collocated transmitter must not exceed the EIRP limits stipulated in this table.						
	Operating mode	Tx Freq Range (MHz)		Max Time-Avg Cond. Power (dBm)	Antenna Gain Limit (dBi)	
					Standalone	Collocated
EM9291	WCDMA Band 2	1850.0	1910.0	24.5	7.5	7.0
	WCDMA Band 4	1710.0	1755.0	24.5	4.5	4.5
	WCDMA Band 5	824.0	849.0	24.5	5.5	4.5
	LTE B2	1850.0	1910.0	24.5	7.5	7.0
	LTEB4	1710.0	1755.0	24.0	4.5	4.5
	LTEB5	824.0	849.0	24.0	5.5	4.5
	LTEB7	2500.0	2570.0	24.0	5.5	5.5
	LTEB12	699.0	716.0	24.0	5.0	4.0
	LTEB13	777.0	787.0	24.0	5.0	4.5
	LTEB14	788.0	798.0	24.0	5.0	4.5
	LTEB17	704.0	716.0	24.0	6.5	5.0
	LTEB25	1850.0	1915.0	24.0	7.5	7.0
	LTEB26	814.0	849.0	24.0	5.5	4.5
	LTEB41_PC3	2500.0	2690.0	24.0	5.5	5.5
	LTEB41_PC2	2500.0	2690.0	26.0	5.5	5.5
	LTEB42_PC3	3450.0	3600.0	24.0	4.0	4.0
	LTEB42_PC2	3450.0	3600.0	26.0	4.0	4.0
	LTEB43_PC3	3600.0	3800.0	24.0	4.0	4.0
	LTEB43_PC2	3600.0	3800.0	26.0	4.0	4.0
	LTEB48	3550.0	3700.0	24.0	4.5	4.5
	LTEB66	1710.0	1780.0	24.0	4.5	4.5
	LTEB71	663.0	698.0	24.0	4.5	4.0
	5GNRn2	1850.0	1910.0	25.5	7.5	7.0
	5GNRn5	824.0	849.0	25.5	5.5	4.0
	5GNRn7	2500.0	2570.0	25.5	5.5	5.5
	5GNRn12	699.0	716.0	25.5	5.0	4.0
	5GNRn13	777.0	787.0	25.5	5.0	4.5
	5GNRn14	788.0	798.0	25.5	5.0	4.5
	5GNRn25	1850.0	1915.0	25.5	7.5	7.0
	5GNRn26	814.0	849.0	25.5	5.5	4.5

COLLOCATED RADIO TRANSMITTERS

	Collocated Radio Transmitters					
	Note: The radiated power of a collocated transmitter must not exceed the EIRP limits stipulated in this table.					
	Operating mode	Tx Freq Range (MHz)		Max Time-Avg Cond. Power (dBm)	Max Antenna Gain (dBi)	Maximun EIRP (dBm)
Collocated Transmitters	5GNRn30	2305.0	2315.0	25.5	-1.5	-1.5
	5GNRn41_PC3	2500.0	2690.0	25.5	5.5	5.5
	5GNRn41_PC2	2500.0	2690.0	27.5	5.5	5.5
	5GNRn48	3550.0	3700.0	25.5	4.5	4.5
	5GNRn66	1710.0	1780.0	25.5	4.5	4.5
	5GNRn71	663.0	698.0	25.5	4.5	4.0
	5GNRn77_PC3	3450.0	3980.0	25.5	2.5	2.5
	5GNRn77_PC2	3450.0	3980.0	27.5	2.5	2.5
	5GNRn78_PC3	3450.0	3800.0	25.5	2.5	2.5
	5GNRn78_PC2	3450.0	3800.0	27.5	2.5	2.5
	WLAN2.4GHz	2400.0	2500.0	20.0	5.0	25.0
	WLAN5GHz	5150.0	5850.0	20.0	5.0	25.0
	WLAN6GHz	5925.0	7125.0	20.0	5.0	25.0
	Bluetooth	2400.0	2500.0	15.0	5.0	20.0

RF BAND SUPPORT

RF Band Support	a and d (see note)								
	1	2	3	4	5	7	8	12	14
5G NR Sub-6 GHz	F	F	F	-	F	F	F	F	F
4G LTE	F	F	F	F	F	F	F	F	F
3G (WCDMA)	-	Y	-	Y	Y	-	-	-	-
	17	18	19	20	25	26	28	29	30
5G NR Sub-6 GHz	-	F	-	F	F	F	F	S	F
4G LTE	F	F	F	F	F	F	F	S	F[b]
3G (WCDMA)	-	-	-	-	-	-	-	-	-
	32	34	38	39	40	41	42	43	46
5G NR Sub-6 GHz	-	-	T	-	T	T	-	-	-
4G LTE	S	T	T	T	T	T	T	T	T[c]
3G (WCDMA)	-	-	-	-	-	-	-	-	-
	48	66	70	71	75	76	77	78	79
5G NR Sub-6 GHz	T	F	F	F	S	S	T	T	T
4G LTE	T	F	-	F	-	-	-	-	-
3G (WCDMA)	-	-	-	-	-	-	-	-	-

DEVICE REBOOT

When the Console Manager reboots, the cellular IP address is not preserved.

To reboot the unit, select **CONFIGURE > System > Reboot**.

To conduct a full erase and factory reset, see Factory Reset.

> **Note:** Factory reset restores the appliance to its factory default settings. Any modified configuration information is erased.

INITIAL SETTINGS

This section provides step-by-step instructions for the initial settings on your Console Manager.

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

> **Tip:** There is also a Quick Start Guide to assist with easy setup of the Console Manager. The QSG is available at: https://opengear.com/support/documentation/

> **Note:** For Configure Serial Ports, see Serial Ports.

DEFAULT SETTINGS

> **Tip:** See also the Quick Start Guide available at the Opengear documentation web page: https://opengear.com/support/documentation/

The CM8100 and CM8000 are configured with a default static IP Address for NET1 of 192.168.0.1 Subnet Mask 255.255.255.0.

The CM8100-10G devices are configured with a default static IP Address for NET3 of 192.168.0.1 Subnet Mask 255.255.255.0.

SERIAL PORT SETTINGS

The default settings for the serial ports (1 up to 48) on a new device are:

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

BROWSER WEBUI

The Console Manager offers a WebUI via any web browser that supports HTML5.

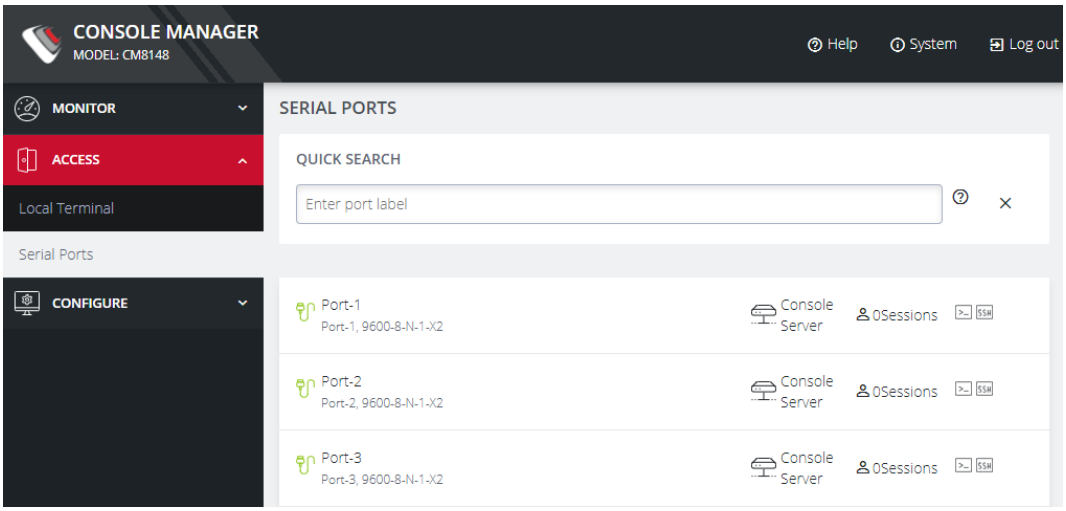
1. Type *https://192.168.0.1* in the address bar.
   HTTPS is enabled by default.

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 WebUI is available; check the system details in the top right-hand side of the WebUI.
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.



USE THE WEBUI

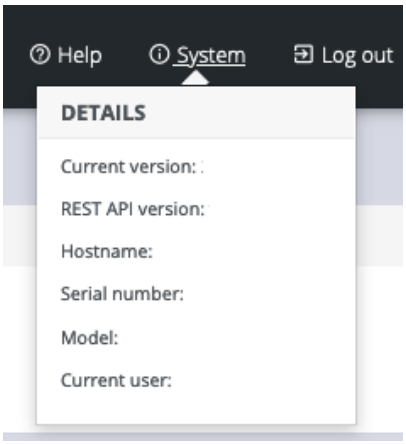
You can adjust the toggle on the bottom left to switch the WebUI between the following modes:

- **Light**: Changes the user interface to display mostly light colors. This is the default UI setting.
- **Dark**: 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**: 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 User Guide.
- **System**: The System menu presents the **Current version**, **REST API version**, **Hostname, Serial Number, Model**, and **Current user**.



- **Log out**

MANAGEMENT CONSOLE CONNECTION VIA CLI

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

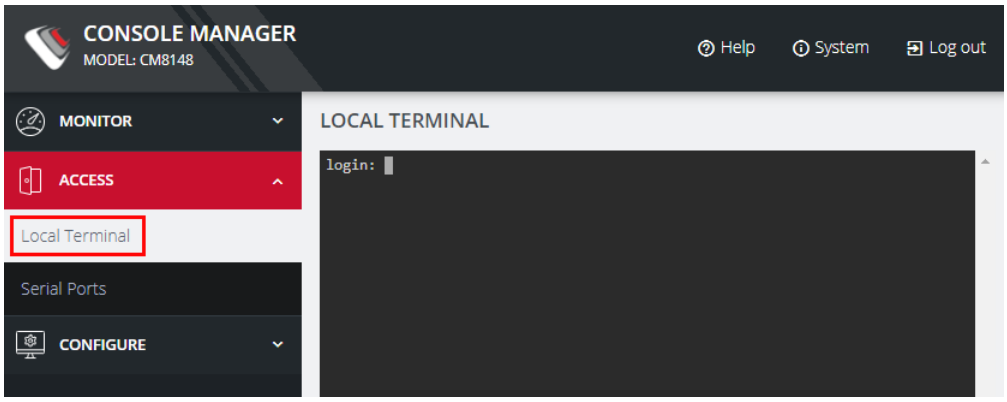
1. Open a CLI terminal on your desktop.
2. Input the default IP Address of *192.168.0.1*.
   SSH port 22 is enabled by default.
3. When prompted, enter the log in and password in the CLI.
   After a successful log in, you'll see a command prompt.

ACCESS THE WEBUI CLI TERMINAL

An alternative CLI terminal is provided within the WebUI.

To access this terminal, in the left-hand side **Navigation Bar**, navigate to the **ACCESS > Local Terminal** page.

You are required to submit your log in credentials.



CHANGE THE ROOT PASSWORD

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

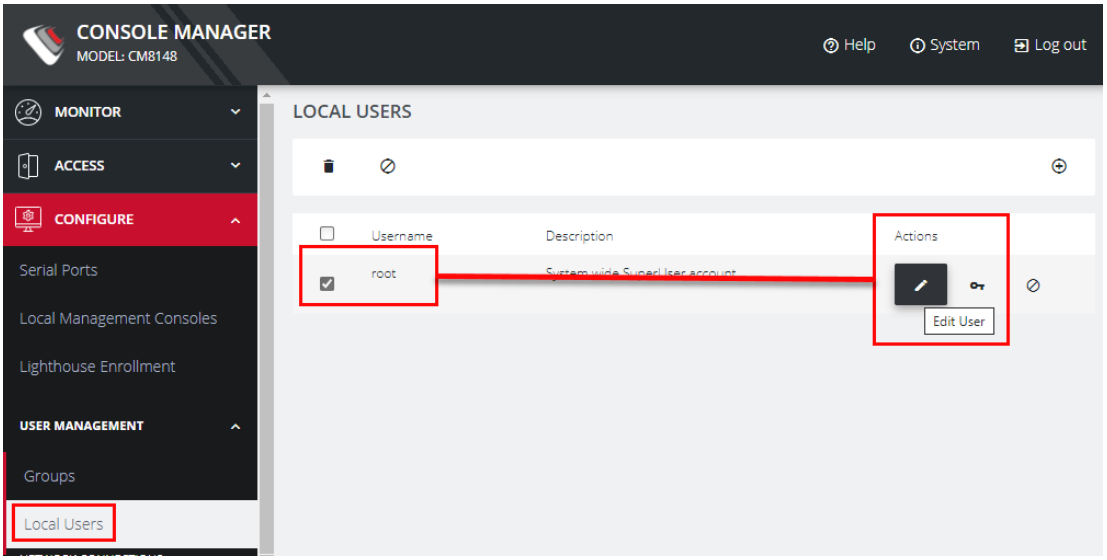
Passwords must comply with your company's password complexity policy, see Local Password Policy.

> **Note:** Users are prevented from reusing the word “default” as their password. The factory default password automatically expires after a factory reset and users must choose a new password. This policy is applied through the WebUI, Config Shell and CLI.

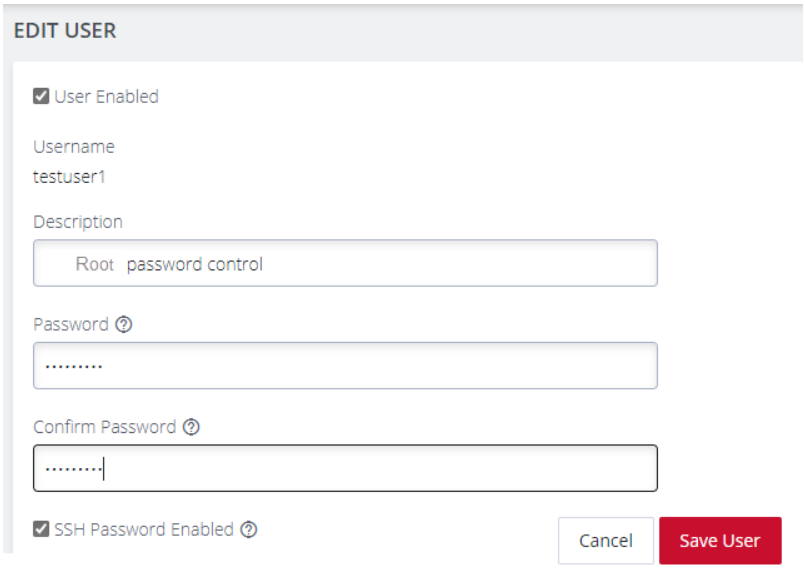
> **Tip:** Any other user's passwords may be changed using the same procedure by selecting the user's account name under the **Username** heading.

To change the password at any time:

1. Navigate to **CONFIGURE > User Management > Local Users**.
2. Under **Actions**, click the **Edit User** icon for the user.



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



4. Click **Save User**.

   A green banner confirms the password change is saved.

DISABLE A ROOT USER

Before you proceed, make sure that another user exists that has the Administrator role or is in a group with the Administrator role. For information on how to create, edit, and delete users, see Local Users.

To disable a root user:

1. Navigate to **CONFIGURE > User management > Local Users**.
2. Under **Actions**, click the **Disable User** button 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.

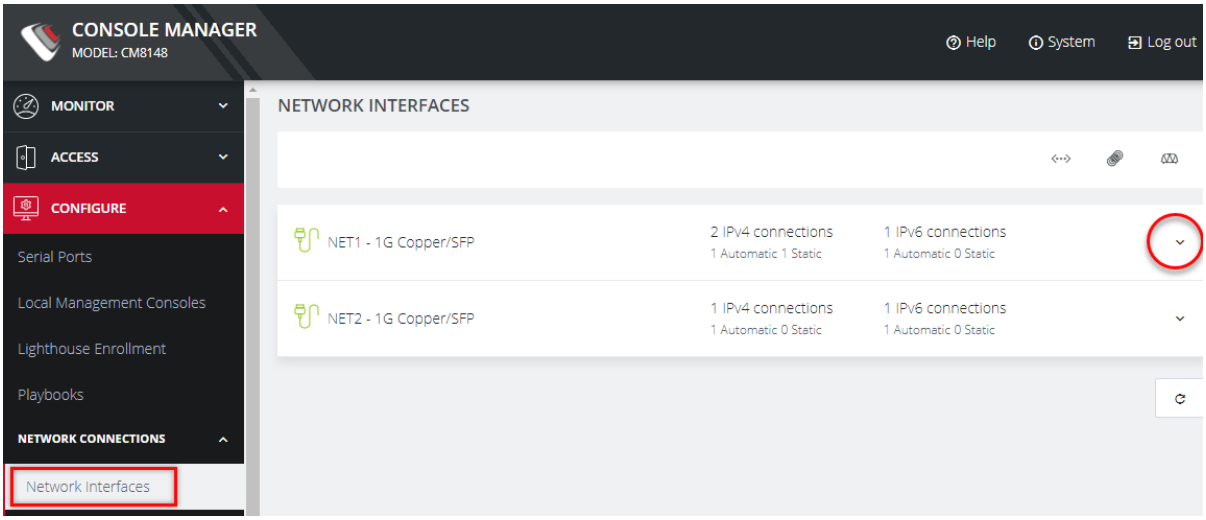
CHANGE NETWORK SETTINGS

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:

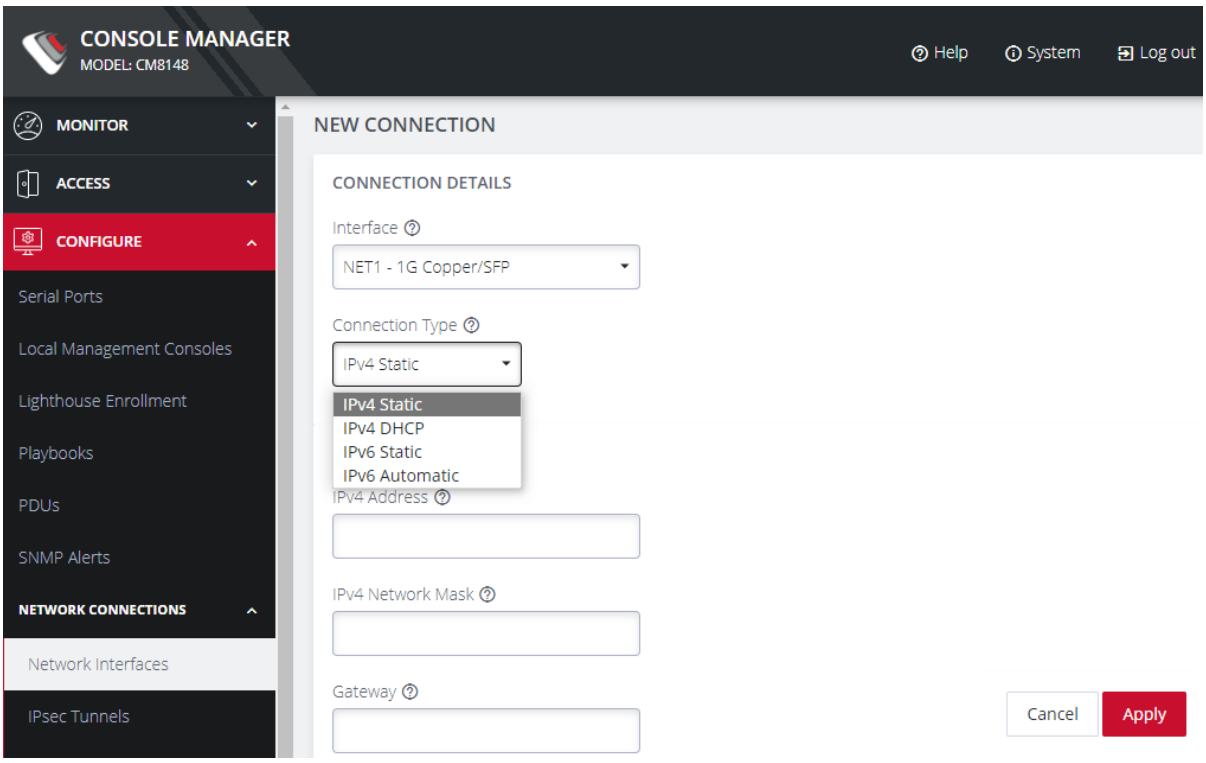
- IPv4, IPv6.
- Static and/or DHCP.
- Enabling or disabling network interfaces.
- Ethernet Media types.

ADD A NEW CONNECTION

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



2. Click the **expand arrow** to the right of the required 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.

   The form on the bottom part of the page changes based on the **Connection Type** you choose.

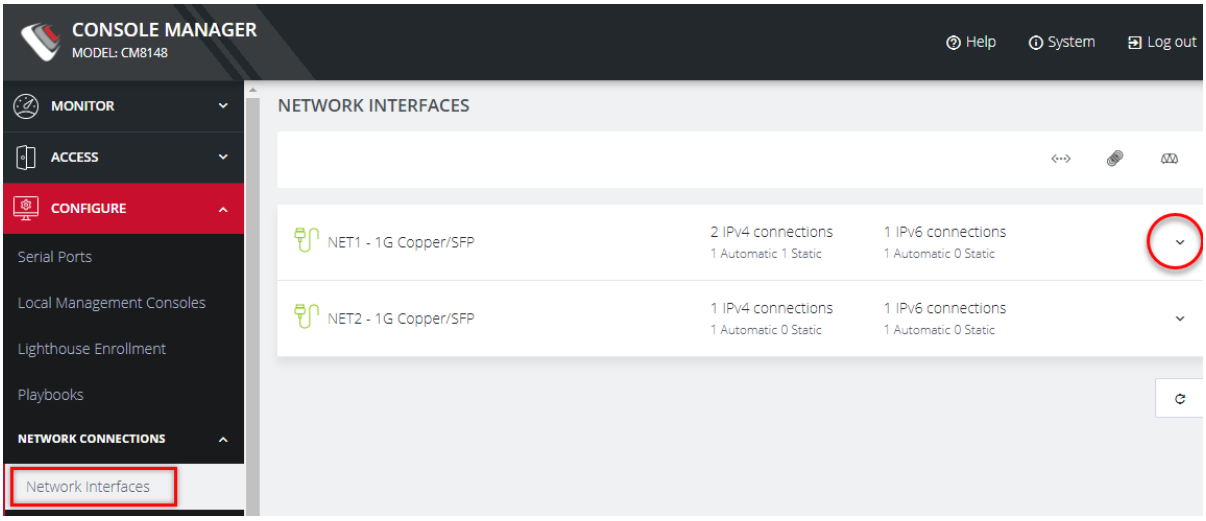
5. To disable or delete interfaces, use the controls on the expanded section on the **CONFIGURE > Network Connections > Network Interfaces** page.

6. Enter the necessary information and click **Apply**.

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

CHANGE THE ETHERNET MEDIA TYPE

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

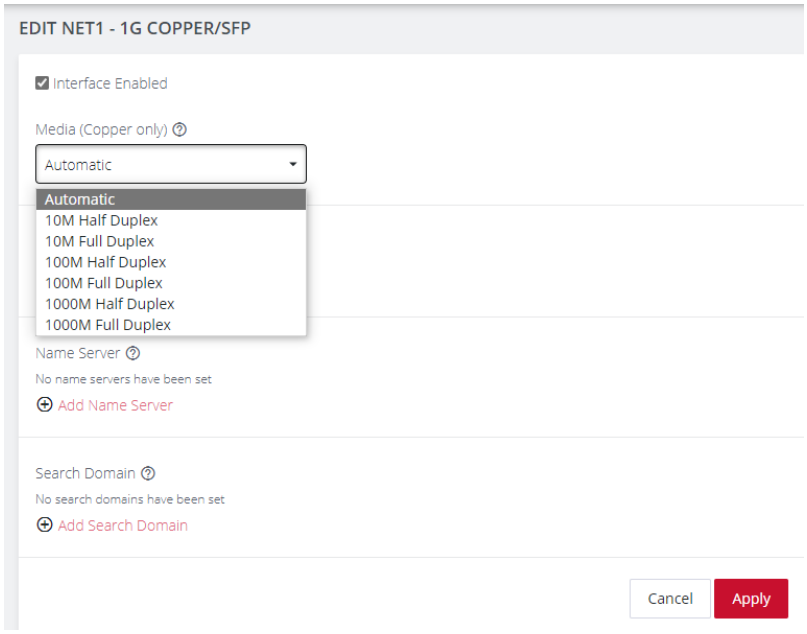


2. Click the **expand arrow** to the right of the interface you want to modify.

3. Click **Enabled** .

4. To change the interface media setting, click the **Edit** button and edit the media settings as

required, then click **Apply**.



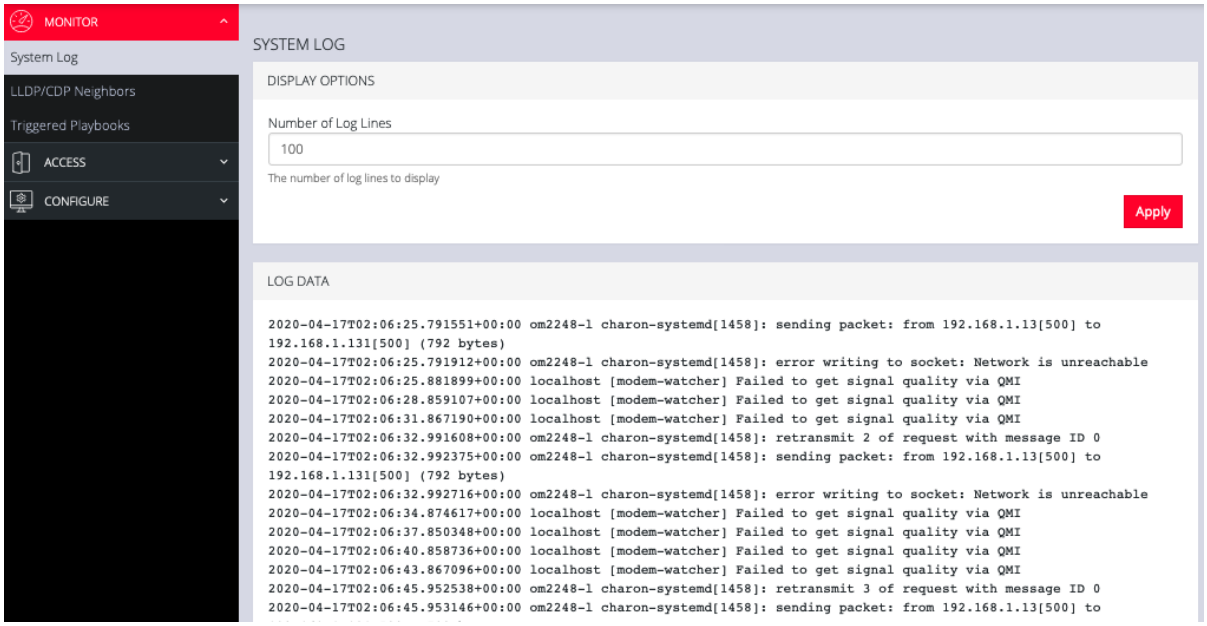
MONITOR MENU

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

SYSTEM LOG

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

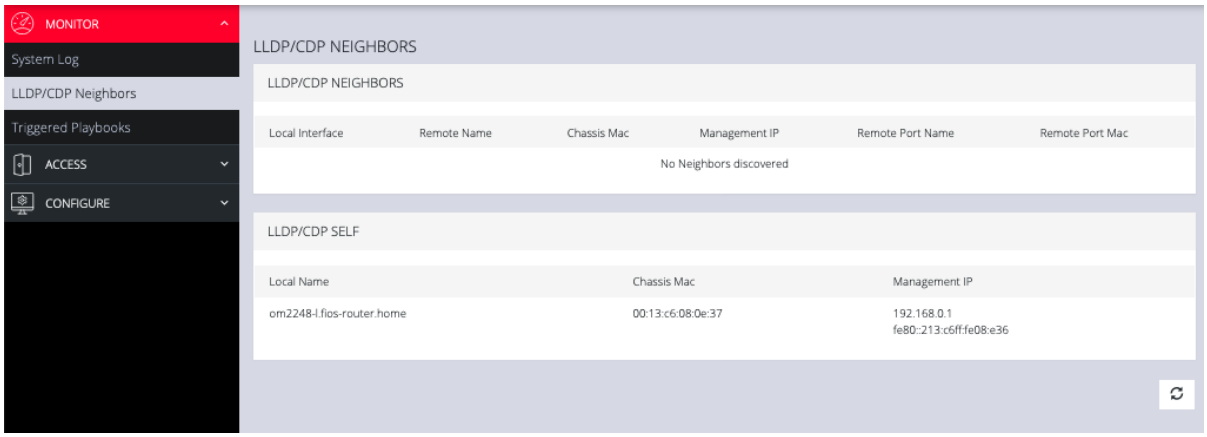
To view the System Log, click **MONITOR > System Log**.



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.

LLDP CDP NEIGHBORS

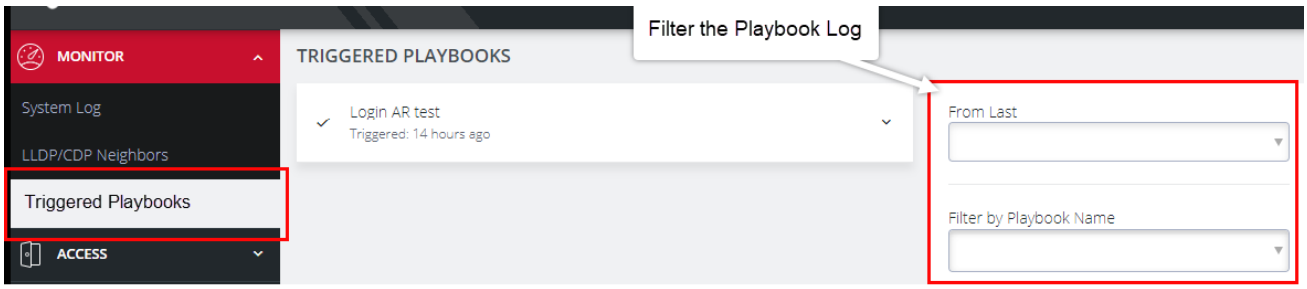
The Console Manager displays LLDP/CDP Neighbors when enabled for a connection. To enable or disable, see Network Discovery Protocols.



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 required, and filter by **Name** of **Playlist** to view any that have been triggered.



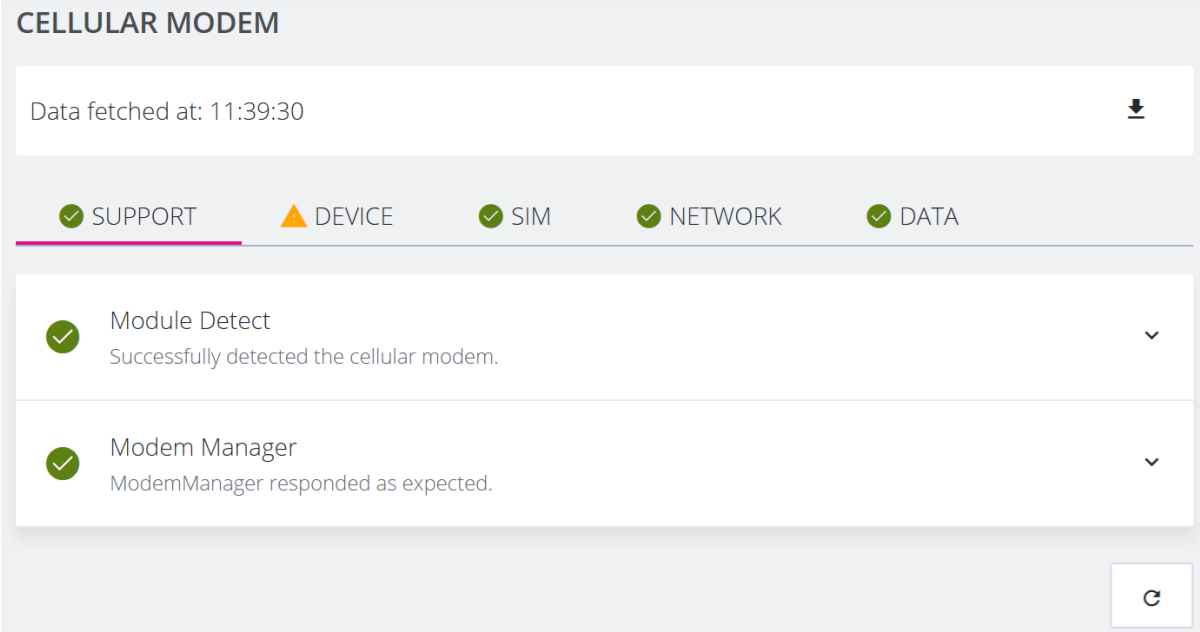
CELLULAR MODEM

> **Note:** This section applies to cellular variants only. The CM8000 does not support cellular connectivity.

The Cellular Modem page is a WebUI-based tool you can use to run and view a diagnostic summary of the cellular modem status for an Opengear device. The summary includes key test results, signal metrics, and troubleshooting guidance.

> **Note:** You can also use this tool in the CLI, see Run Diagnostics with Modem-Test.

To run or view the summary, click **MONITOR > Cellular Modem**.



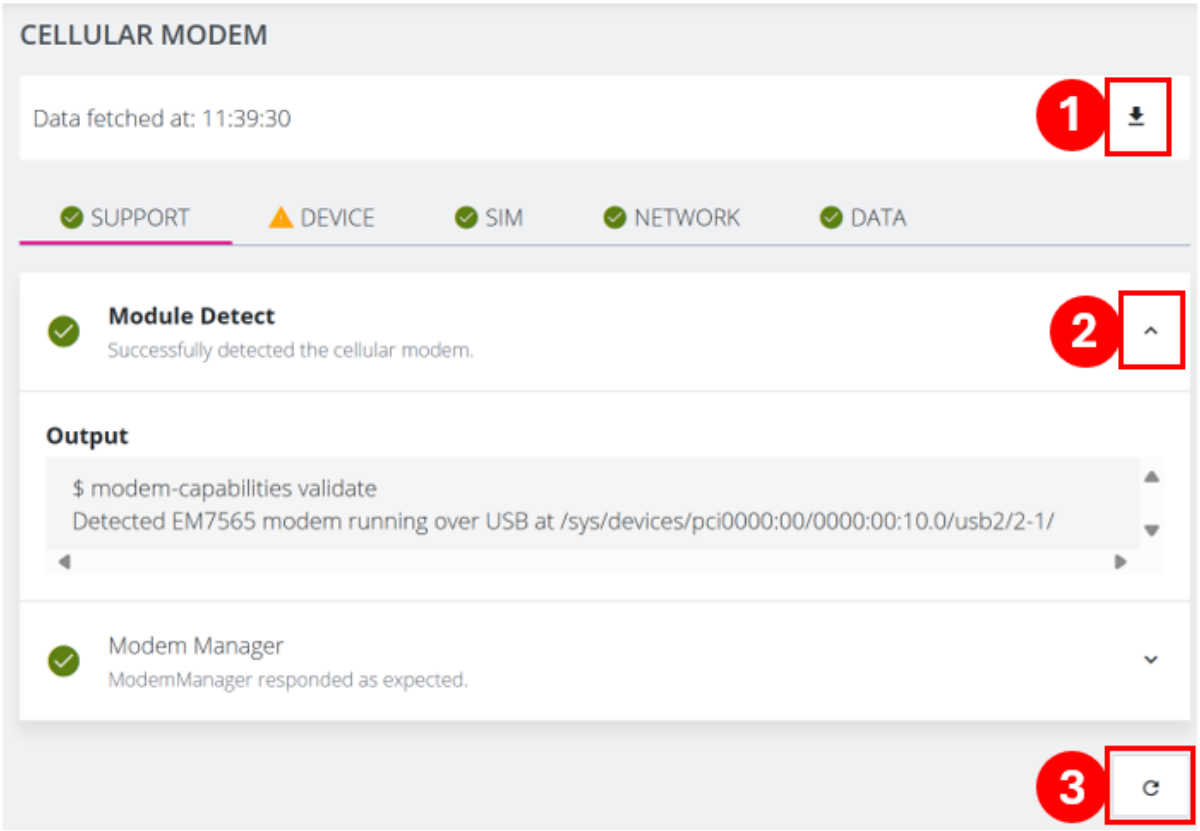
When the page opens, the:

- top of the page displays the last time the tests ran.
- following tabs display summaries for each group of test results:
  - **Support:** Test results for support, such as **Module Detect**, and **Modem Manager**.
  - **Device:** Test results for the device, such as **Device Information**, **Device Image Status**, **Device Module Info**, **Device Firmware Info**, and **Device Operating Mode**.
  - **SIM:** Test results for the SIM, such as **SIM Slot Status**.
  - **Network:** Test results for the network, such as **Signal Strength Status**, **Signal Info**, **Network Status**, **Access Technology Status**, and **Operator Network Status**.

- **Data:** Test results for data, such as **Packet Data Protocol Context** and **Data Connection Status**.

You can also click the:

1. **Download** button to download a text version of the results.
2. Chevron to expand the summary and view more detailed test result information.
3. Refresh button to re-run the tests for interactive troubleshooting.



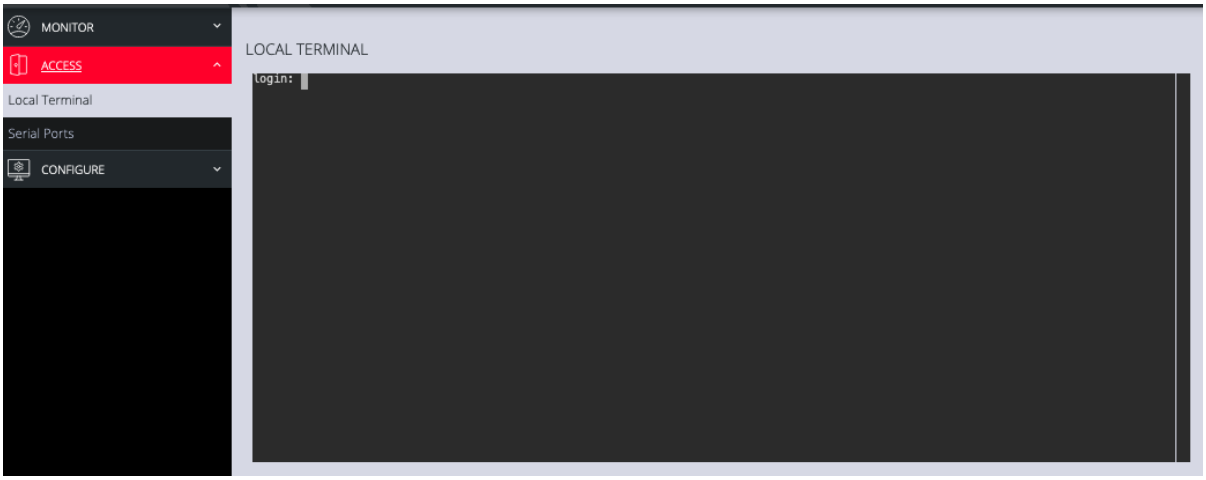
ACCESS MENU

The ACCESS menu provides access to Local Terminal of the Console Manager. It also provides SSH and Web Terminal access to specific ports.

LOCAL TERMINAL

The Console 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.

   A bash shell prompt displays.

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

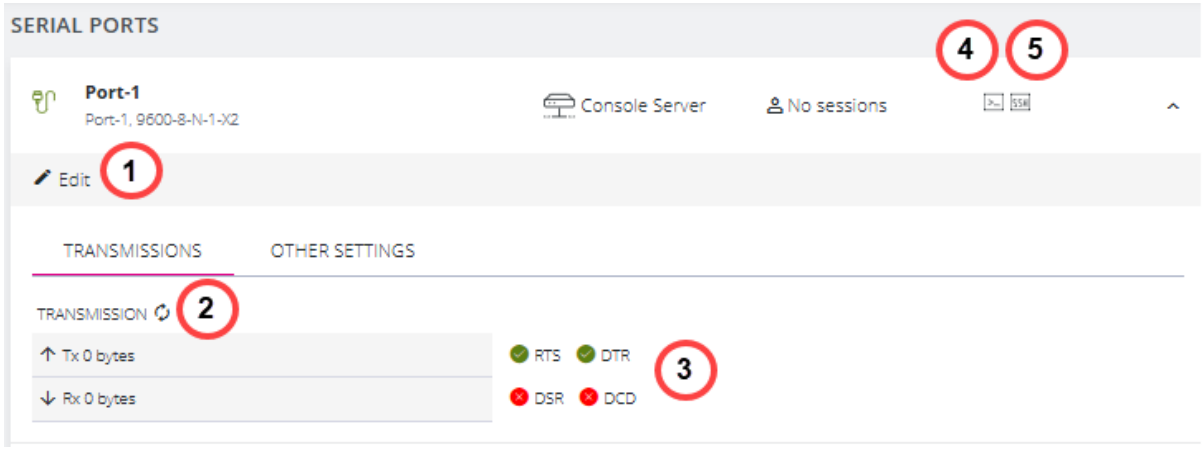
To close a terminal session, close the tab, or type exit in the Web Terminal window. The session times out after 60 seconds.

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

SERIAL PORTS

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

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



Callout #	Item Definition
1	Serial port edit button.
2	Counter reset.
3	Serial port Data, Rx & Tx counters. Signaling status (RTS, DTR, DSR, DCD), requires refresh.
4	Web terminal and SSH links.
5	Expand arrow to display logging status.

Click the **Expand arrow (5)** 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 (ogcli: `ogcli get ports/ports_status`).

The following information displays under **Access > Serial Ports** when the individual serial ports are expanded:

- Rx byte counter (counter reset requires 'Admin' or 'port config' rights)
- Tx byte counter (counter reset requires 'Admin' or 'port config' rights)
- Signaling information (DSR, DTR, CTS (see tip), RTS and DCD)

  > **Tip:** CTS information is not displayed in the UI but is available via the ogcli query `ogcli get ports/ports_status`.

- Logging information.

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.

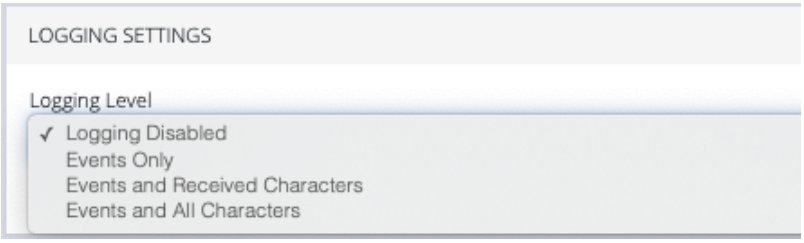
> **Note:** MS WIndows does not connect to puTTY by default. You may have to install the WinSCP program to launch puTTY from the Opengear WebUI SSH Serial Port button.

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.

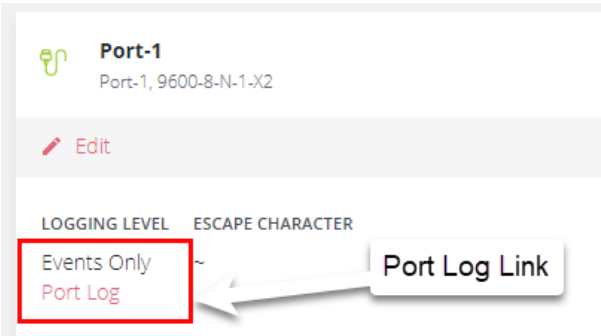
There is a separate setting to enable sending of serial port logs to remote side.

> **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.



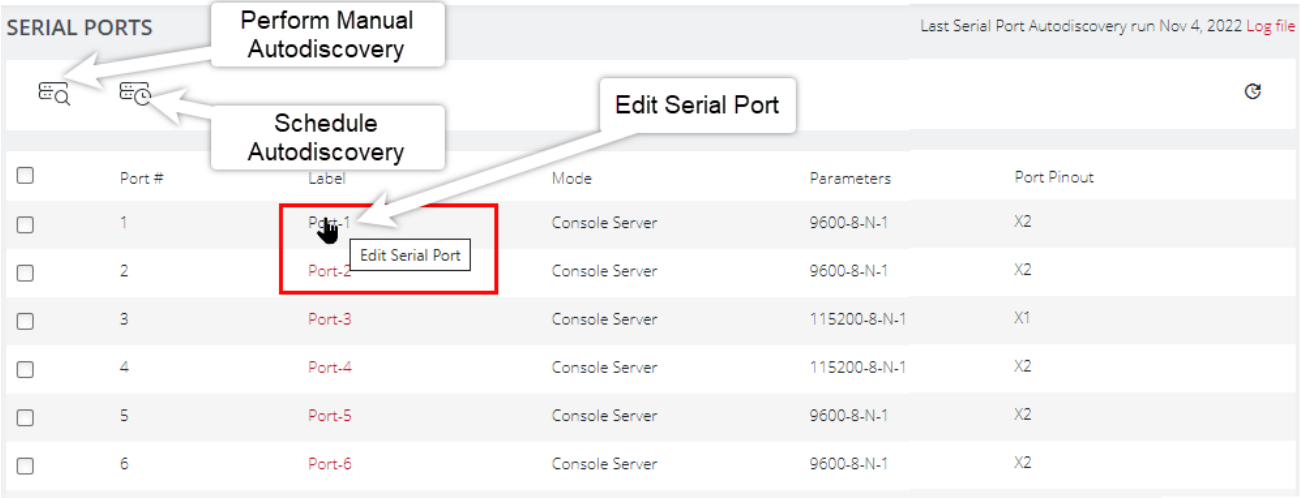
CONFIGURE MENU

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

SERIAL PORTS

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

On this page you can configure and edit specific ports.



EDIT SERIAL PORTS

1. Navigate to **CONFIGURE > Serial Ports**.
   A list of serial ports displays.
2. Click the **Port label** text in the **Label** column.
   The **Edit Serial Port** page displays.
3. Complete the following fields as appropriate:

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 **Quick Search** form on the **ACCESS > Serial Ports** page.
Mode	Disabled Console Server Local Console	**Console Server** mode allows access to a downstream device via its serial port. **Local Console** mode allows access to the OM device's console through a serial port.
Port Pinout	Fixed - X2 Cisco Straight	The pin-out type is fixed on the CM8100 and CM8000.
Port Pinout CM8100-10G	Selectable - X2 Cisco Straight	The pin-out type is software selectable on the CM8100-10G
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.

Edit Serial Port Properties		
Field	**Options**	**Definition**
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.
Raw TCP	Enabled, Disabled	Select whether raw TCP is enabled or disabled. For more information, see Configure Raw TCP Access for Serial Ports.
DTR and RTS pins	Always On, Always Off, On when connected	Use this setting to control the DTR and RTS pins. The default setting is **Always On**. You can also set them to **On when Connected** which means they are on only when there is an active user session/client connected to the port.
LOGGING SETTINGS		

Edit Serial Port Properties		
Field	**Options**	**Definition**
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 > Syslog. “Send Serial Port Logs” under Services > Syslog > Add 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 Knowledge Base article Configure IP alias for serial ports.

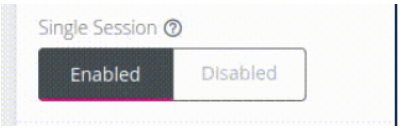
CONFIGURE SINGLE SESSIONS FOR PORTS

Single Session Port Config, or *Single Session* is a feature that can be enabled on a given port to prevent multiple users from connecting to that port or limit the port to a single concurrent connection. This feature is port-specific and is disabled by default. This feature must be enabled on a port-by-port basis. It can be enabled on all types of serial ports (including USB).

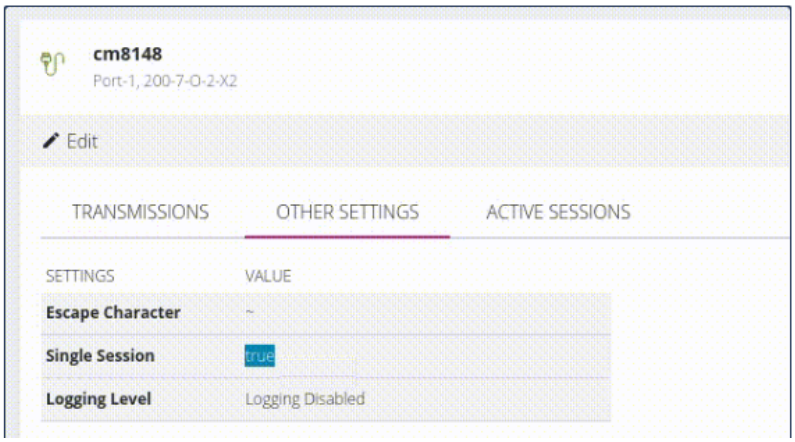
Similar to Config Shell, a single session must be enabled or disabled on a port-by-port basis, currently it cannot be enabled on all ports.

SINGLE SESSION ENABLED IN THE WEBUI

Single Session can be viewed and configured in the WebUI. It is enabled (or disabled) in the configure page for a given serial port. The buttons to connect to a serial port are automatically disabled when the feature is enabled and the session is in use.



You can also confirm the session in the **Access > Serial Ports** page to check if the feature is enabled.

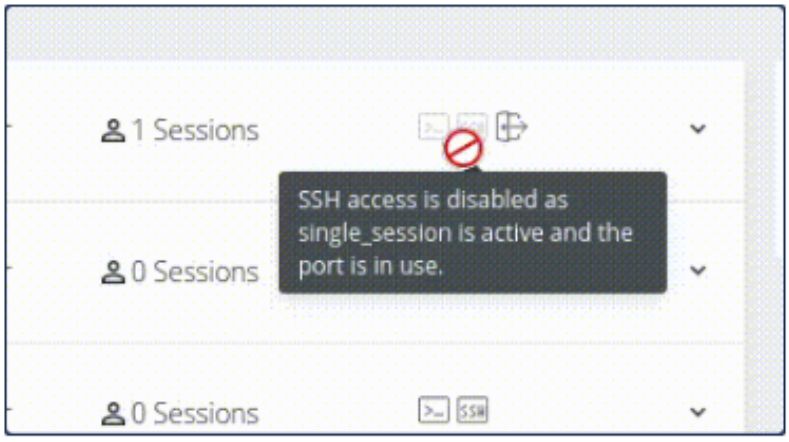


When the Single Session feature is enabled and the port is in use, if a subsequent user attempts to connect to the port, the connection is declined, and the second user receives the following message:

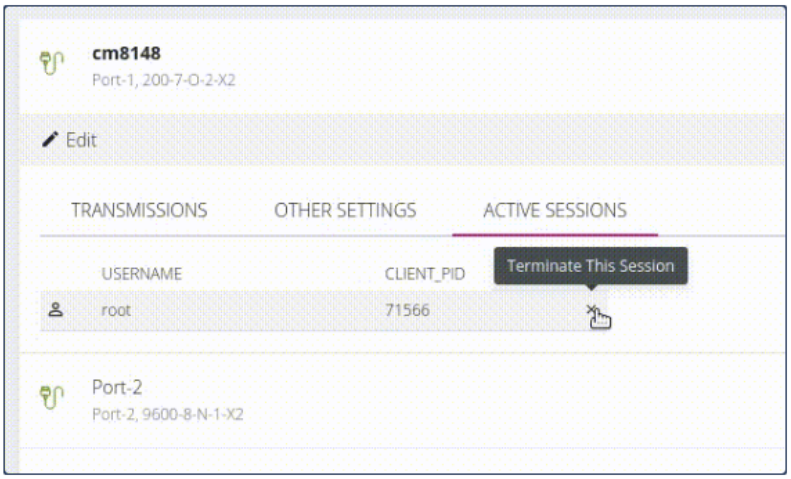
```
Unable to connect. Another session is currently active.
Please disconnect from the current session before attempting to connect again.
```

The pmshell exits, and the user who tried to connect does not see the first user's session. Everything they have done remains confidential.

The single session is indicated next to the user.



If necessary, a user's single session can be terminated with the **Terminate all sessions** button which is shown beside individual users. This re-enables the **Single Session** button and allows you to connect.



IN CONFIG SHELL

The Single Session feature can be enabled or disabled by editing the `single_session` field of a port. When a user port level Administrator access is logged in via pmshell, the port configuration menu can be accessed via any port by pressing the escape character (~ by default) followed by c (~c).

You can access a port with the following commands, the following example will access “Port 1”:

```
config: port
config(port): port01
```

The port configuration might look like the following example. You can see for this port, single_ session is set to false, so the feature is disabled:

```
config(port port01): show
Entity port item port01
   baudrate 9600
   databits 8
   escape_char ~
   label                    Port-1
   logging_level    disabled
   mode                  consoleServer
   parity                   none
   pinout                 X2
   portnum              1
   single_session   false
   stopbits              1
   control_code (object)
      break       ""
      chooser    ""
      pmhelp     ""
      portlog      ""
```

```
      power       ""
      quit            ""
   ip_alias (array)
```

The feature is enabled by typing `single_session true`, then apply the change.

```
config(port port01):      single_session true
config(port port01):      apply
Updating entity port      item port01.
config(port port01):      show
Entity port item              port01
    baudrate                     9600
...
single_session                true
...
ip_alias (array)
```

SINGLE SESSION BEHAVIOR

The following table describes single session feature behavior in various circumstances.

Q.	What occurs if users are connected to the port with the feature disabled, then the feature is enabled while users are still connected?
A.	Users who are already connected will continue to be able to use the port. If they leave, they will not be able to rejoin (unless there are no active sessions). Their current session will continue as normal, however, their session can be manually terminated from Config Shell (config(port_session):) or from the WebUI from the Access/Serial Ports page.
Q.	What if a user must be removed from a port?
A.	Administrators can remove the right for a given user to access a port. They can also manually remove them from the port in the Config Shell (config(port_session):) or the WebUI from the **Access > Serial Ports** page.
Q.	What if someone tries to join a port that is already in use?
A.	The user who tries to join is prevented from doing so and receive a notification. The person currently using the port is unaffected and not be aware of the attempt.
Q.	Is there a way to enable the feature for every port?
A.	Currently, the feature must be enabled or disabled on a port-by-port basis.
Q.	What if I enable this port on localConsole mode?
A.	The feature is ignored on local console mode and is only active for Console Server mode. It also remains ignored if the port mode is set to disabled.

CONFIGURE RAW TCP ACCESS FOR SERIAL PORTS

The Raw TCP Access feature is an option under the ports endpoint and provides a means of accessing serial ports directly through netcat (nc), or Telnet.

> **Note:** Raw TCP can only be enabled when the port is in **consoleServer** mode.

Raw TCP is enabled or disabled through the WebUI, Config Shell, or through ogcli. When enabled, Raw TCP will open a TCP socket on a TCP port in the range of 40XX, where XX corresponds to the serial port number on which Raw TCP access is enabled. Any TCP messages sent to this port are relayed to the corresponding serial port.

The Console Manager serial ports can be configured to operate in Raw TCP mode on a port-by-port basis.

Pre-defined firewall services allow Raw TCP connections through the firewall. These services correspond to each serial port on the device.

> **CAUTION:** Raw TCP access bypasses any authentication methods. When Raw TCP access is enabled on a serial port, anyone with network access is able to access that serial port, and any devices connected serially to it. **This feature should only be used on a secure network.**

> **Note:** Raw TCP access is disabled by default on Opengear devices. Users must enable Raw TCP access on a serial port through the WebUI, Config CLI or ogcli.

SERVICE IMPLEMENTATION

Raw TCP access allows you to access serial ports on a device directly by connecting to a TCP port in the range 40XX.

In order to achieve Raw TCP access, you must first allow TCP packets through port 4002 in the firewall:

1. Navigate to the **Firewall Management** page in the WebUI.
2. Add a `raw_tcp_serial02` service, which corresponds to serial port 2.
3. Add the service for the firewall zone the service will be connecting over; in the following example, it is the LAN zone. Check the service has been correctly added (as shown in the example).



When this service has been added to the correct firewall zone, you can create a Raw TCP connection to the target port.

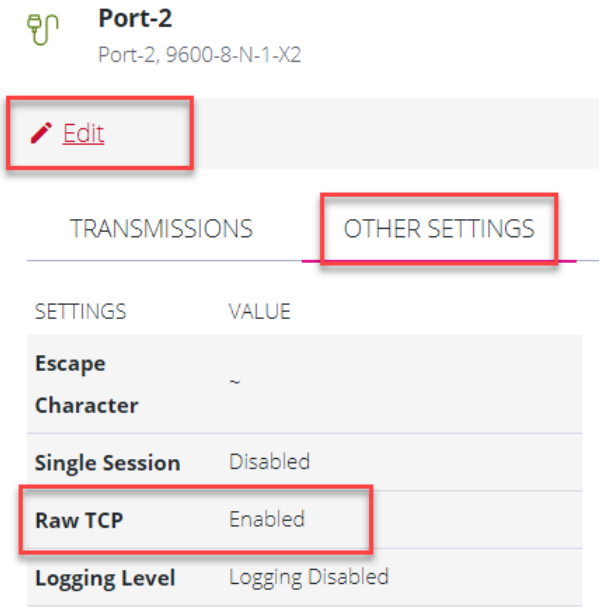
> **Note:** `tcp_serial` service must be manually added to relevant firewall zones after Raw TCP has been enabled on a port.

WEBUI CONFIGURATION

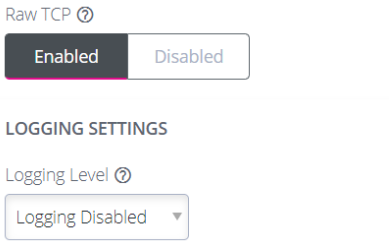
Raw TCP access can be enabled or disabled on a selected serial port through the WebUI. When looking at the serial port access page, the enabled/disabled status of Raw TCP access is visible under the **Other Settings** tab for each serial port.

1. In the WebUI, navigate to **Access > Serial Ports** and click the drop-down arrow to the right side of the target port. This displays the port settings, including the Raw TCP status.

2. Click the **Edit** text to open the **Edit Serial Port** page:



3. At the **Edit Serial Port** page, scroll down the page to see the Raw TCP settings:



4. To Enable Raw TCP, click the **Enabled** button then click **Apply** at the bottom of the page. A confirmation message is flagged when Raw TCP is successfully enabled.

CONFIG CLI CONFIGURATION

Raw TCP can be configured through the Config Shell. Navigate to the port endpoint and enter the context of the target serial port (for example, serial port 2 is used in the following procedure):

```
config: port port02
config(port port02): show
Entity port item   port02
  baudrate            9600
```

```
  databits             8
  escape_char     ~
  label                  Port-2
  logging_level   disabled
  mode                consoleServer
  parity                 none
  pinout                X2
  portnum           2
  raw_tcp             false
  single_session false
  stopbits             1
  control_code (object)
    break        ""
    chooser   ""
    pmhelp    ""
    portlog    ""
    power      ""
    quit          ""
  ip_alias      (array)
```

To enable Raw TCP access:

```
config(port port02): raw_tcp true
config(port port02): apply
Updating entity port item port02.
```

To disable Raw TCP access:

```
config(port port02): raw_tcp false
config(port port02): apply
Updating entity port item port02.
```

OGCLI CONFIGURATION

To enable Raw TCP access on a port through ogcli, users can use ogcli update to set `raw_tcp` to **true** on the target port (the device information in the following ogcli command is shown as an example):

```
root@om2216-1-tp1-p3:~# ogcli update port port02 raw_tcp=true
```

To disable Raw TCP, set `raw_tcp` to **false** on the target port:

```
root@om2216-1-tp1-p3:~# ogcli update port port02 raw_tcp=false
```

You can check that the socket is active by running:

```
systemctl status raw-tcp-serial-port02.socket
```

AUTODISCOVERY

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

The first discovery run uses currently configured port settings such as the current baud rate, etc. Thereafter, it will fetch or use a single set of pre-configured credentials to log in and discover the hostname from e.g. the OS prompt, for devices that do not display hostname pre-authentication.

Syslogging enhancement assists in the diagnosis of common issues (for example, no communications or, hostname failed validation). Autodiscovery does not collect a hostname when there is a communication issue between the console server and the target device. The logs are saved for the last-run instance of autodiscovery.

The UI displays error messages and logs with the reason for auto-discovery failure, for example:

- Authentication failed.
- Communication issue with the target device.
- Password to renew before being able to authenticate to the target device.
- Abnormal characters or strings detected.

Autodiscovery has been enhanced to discover baud rate and pinout. The WebUI now indicates 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 **Perform Autodiscovery**.

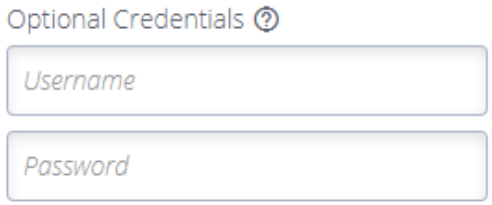
AUTODISCOVERY ENHANCEMENTS

From the 22.11 release, the following parameter enhancements have been added to the port_discovery script which can be configured via the REST API or CLI:

- `--username` and `--password`
- `--apply-config` and `--no-apply-config`
- `--auth-timeout`
- `--hostname-pattern`

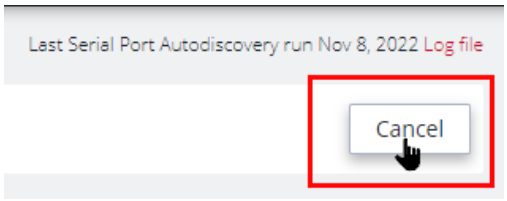
The `--username` and `--password` options can also be configured via the WebUI under *Optional Credentials*.
If the values are provided (optional), they are used to attempt login to obtain the hostname to a

downstream serial device. You can only specify a single username and/or password to try on all devices.



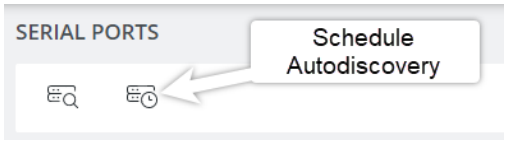
CANCEL AUTODISCOVERY

Port Autodiscovery may be canceled *while running* by clicking on the **Cancel** button at the top-right of the Serial Ports window of the WebUI.



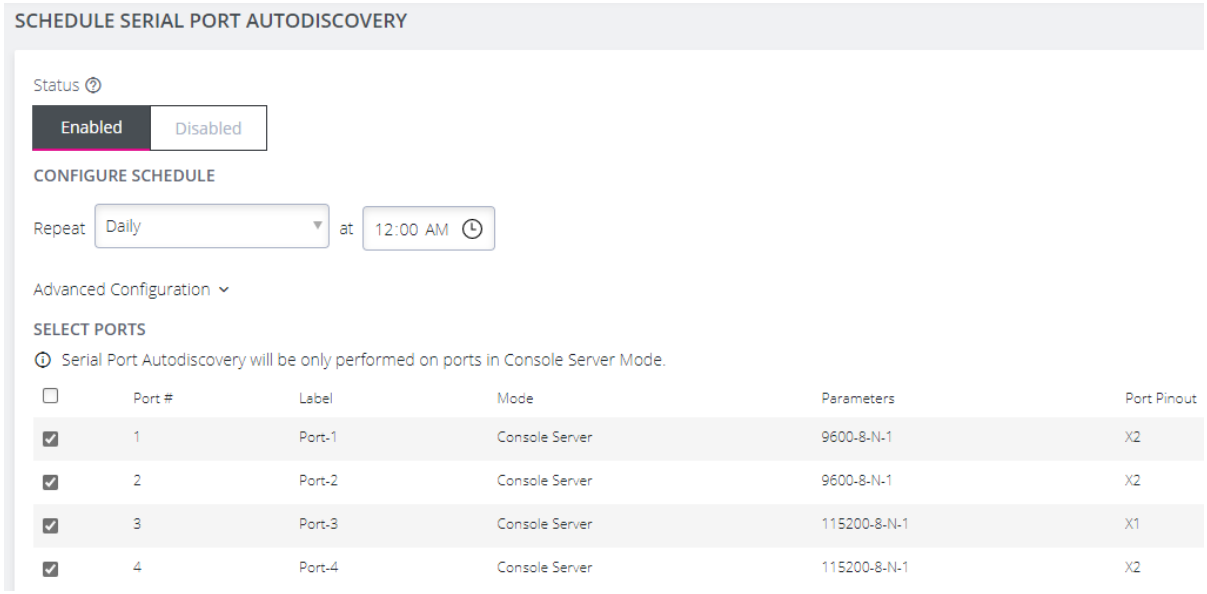
SCHEDULE AUTODISCOVERY

Autodiscovery can be scheduled periodically as required by clicking the **Schedule Autodiscovery** button in the **Serial Ports** window.



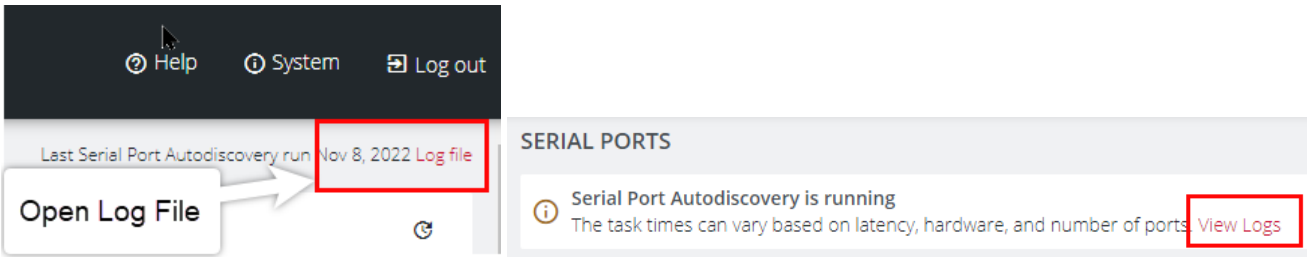
The **Schedule Autodiscovery** window allows you to select the ports and specify a time and period for port detection to run. Activate the schedule by clicking on the **Enabled** button.

The Serial Port Autodiscovery Page:

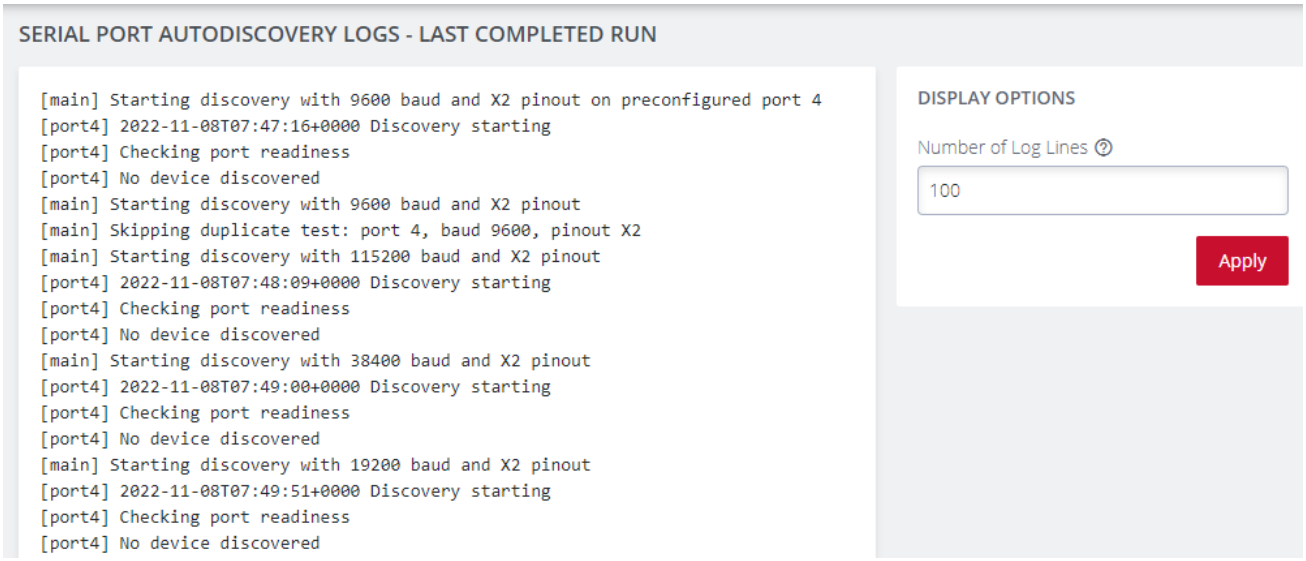


RETRIEVE PORT DISCOVERY LOGS

At the top-right of the UI window, click on the **Log File** red text to retrieve the port discovery logs or by clicking on the **View Logs** red text in the **autodiscovery running** banner.



Port Discovery Log File Example:



LOCAL MANAGEMENT CONSOLES

This feature allows Administrators to log in and configure the:

- CM8100 via the RJ-45 ports on the device. Not accessible by USB.
- CM8000 via the USB-C port on the device.

To edit the settings of a local management console:

1. Navigate to **CONFIGURE > Local Management Consoles**.
   A list of consoles displays.
2. Locate the console you want to manage, then under **Actions**, click on the **Edit Management Console Port** button (pencil icon).
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**

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

- Enable or disable the selected **Management Console**

To disable a local management console:

1. Click **CONFIGURE > Local Management Consoles**.
2. Locate the console you want to disable, then under **Actions**, click on the **Disable Management Console Port** button.

LIGHTHOUSE ENROLLMENT

Opengear appliances can be enrolled into a Lighthouse instance, providing centralized access to console ports, 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 following articles and Lighthouse 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 Console Manager to a Lighthouse instance, you must have Lighthouse installed and have an enrollment token set in Lighthouse.

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

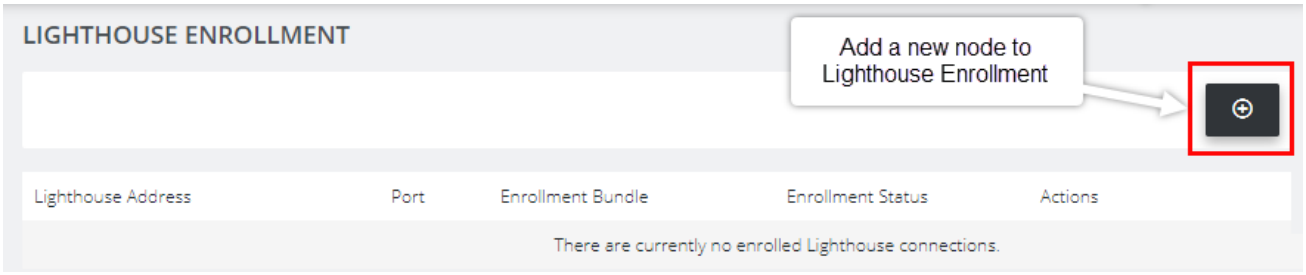
   > **Tip:** The same token is entered in the **NEW LIGHTHOUSE ENROLLMENT** page of the Console Manager.

2. Enroll your Console Manager in this Lighthouse instance:

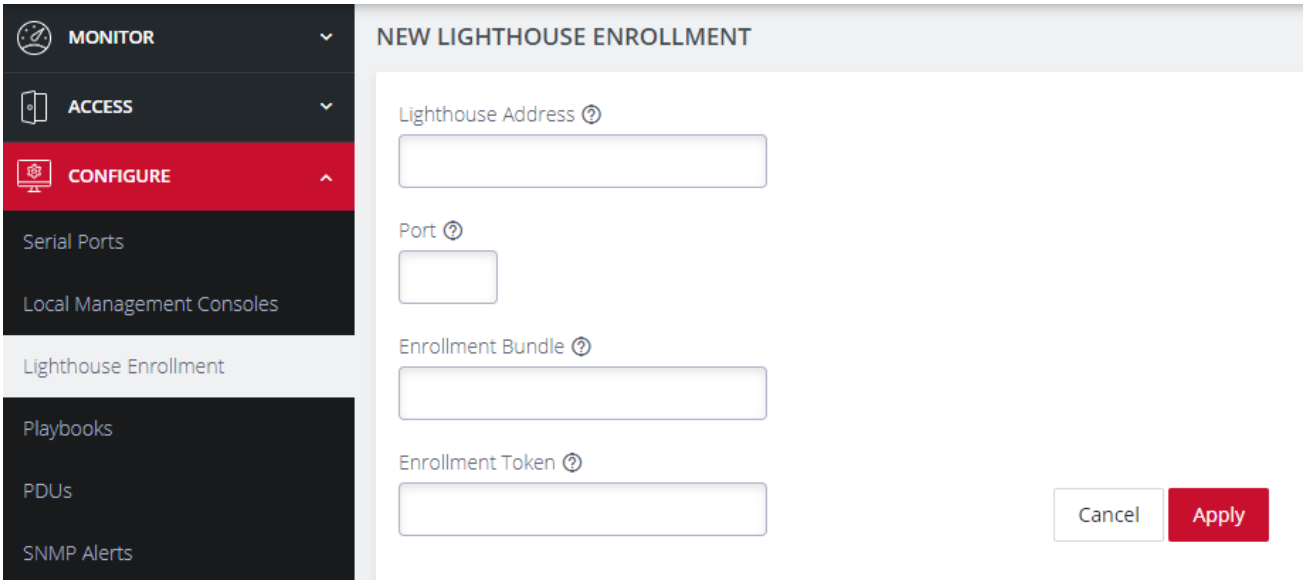
   Click **CONFIGURE > Lighthouse Enrollment**.

3. Click on the **Add Lighthouse Enrollment** button on the top-right of the page.

   The **New Lighthouse Enrollment** page opens.



4. 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).



5. Click the **Apply** button.
   A flag confirms the enrollment.

> **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 via the CLI please refer to this link: Manual enrollment using UI or CLI .

AUTOMATIC ENROLLMENT BY LIGHTHOUSE SERVICE PORTAL (LSP)

Lighthouse Service Portal (LSP) is an Opengear solution that enables Console Manager nodes to perform a zero touch call home and automatic enrollment into a customers Lighthouse instance of choice.

> **Note:** LSP is not configurable and cannot be added in-field.

No User setup is required for LSP. LSP should begin working on boot or factory reset.

LSP SERVICE INITIALIZATION

When the node is initially powered-up or rebooted, ZTP begins to run and sees that device is LSP enabled and ZTP exits before applying any configuration. `Systemd` triggers the LSP.

The node connects to internet and adds an NTP server to ensure crypto is working. It then pulls an updated docker container which it runs, and waits while the docker container writes out the appropriate lighthouse bundle associated with the serial number, then exits.

Identity is verified by a TPM attestation key with the serial number encoded and signed by the attestation key and a CA running in AWS. An accompanying certificate is stored the secure Trusted Platform Module (TPM).

If there are no connectivity issues the LSP status LED (cloud on CM8000) state changes progressively from amber flashing (LSP is running), green flashing (Lighthouse is connecting) and green solid (Lighthouse connected successfully). See Device Status LEDs.

> Note: The cloud LED applies to the CM8000 only.

	LED Off	Amber Flashing	Amber Solid	Green Flashing	Green Solid
Cloud / Internet 	LSP is disabled and there are no existing Lighthouse enrollments.	LSP is currently running on the device.	An error occurred while running LSP.	The device can reach the lighthouse instance and is attempting to enroll. If a lighthouse is unreachable the LED will not start.	The device is enrolled and connected to a lighthouse. There will be a short delay between the UI status reported and the LED changing to solid green.

LSP COMMANDS

LSP is run by a `systemd` service and can be controlled by `systemctl` commands which are self-explanatory:

```
systemctl start lsp
systemctl stop lsp
systemctl enable lsp
systemctl disable lsp
```

The `systemd` service also checks for the absence of a file /var/lib/lsp/.lsp-disabled before it will actually run the service.

RESTART THE SERVICE

If LSP has been disabled due to an error or a successful completion; to re-enable the service, remove the file `/var/lib/lsp/.lsp-disabled`, after which, LSP can be controlled via standard `systemctl` commands.

LSP ERRORS AND EXIT CODES

LSP initiation can sometimes encounter errors, for example, failure to communicate with the REST-API. In these situations, LSP attempts recovery by running from the start again after waiting for a short period.

LSP LOGGING & ERRORS

LSP logs from the `systemd` service and docker container are all stored in the system journal. The LSP service logs can be accessed with `journalctl -u lsp`, and the container logs can be viewed with `journalctl -b CONTAINER_NAME=LSP_AGENT`.

When the docker container runs, it will display the docker registry and digest hash of the running container.

Log Message/Error Code	Event/Definition
`Device is LSP enabled.`	The device supports LSP.
`No logs, the LSP service should disabled without performing any operations. Disabling the LSP systemd service.`	The device does not support LSP. No logs, the LSP service should disabled without performing any operations.
`Key detected in the TPM without a certificate. Due to the missing certificate this device is unable to perform LSP. Opengear Support Required!`	The device contains a key but no certificate. This should not happen in the field, and the device will require that the customer contact Opengear Support. It may require an RMA.
`No existing Lighthouse enrollment found, proceeding with LSP.`	No existing Lighthouse is configured, LSP is able to proceed.
`Running LSP Docker container.`	The docker container has started.
`LSP Docker container has finished executing.`	The docker container has finished.
`Configuring Lighthouse enrollment.`	Lighthouse enrollment configuration has started.
`Lighthouse enrollment configuration applied successfully.`	Lighthouse enrollment configuration has completed.
`No Internet connectivity.`	The device has no Internet connectivity and does not have a cellular modem, LSP will retry in 60s.
`Could not confirm Internet connectivity. Enabling failover.`	The device could not reach the Internet with the ethernet interfaces, failover will be enabled on the cellular interface.

EXIT CODES

The LSP process returns an exit code depending on the status of the process:

Code	Name	Definition
0	EXIT_SUCCESS	LSP completed successfully without error. Lighthouse is now enrolling, or Lighthouse is already configured and LSP doesn't have to run, or The device is not an LSP node.
151	EXIT_RETRY	LSP failed, but will retry.
152	EXIT_UNRECOVERABLE_ERROR	LSP failed but will not succeed, support is required.
153	EXIT_STOP	LSP has stopped during execution. It can be started manually.

ACCESS LIGHTHOUSE SERVICE PORTAL

REGISTER AN ACCOUNT / LOG IN TO LIGHTHOUSE SERVICE PORTAL

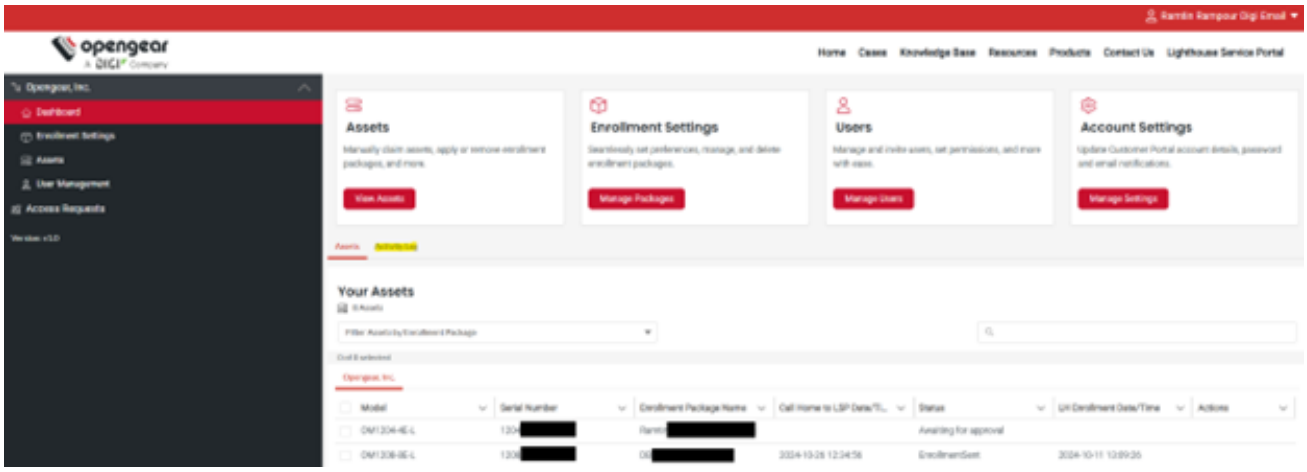
Visit portal.opengear.com.

If not already registered, click the user icon and select Register to initiate the process.

Log in to the portal with your credentials.

DASHBOARD

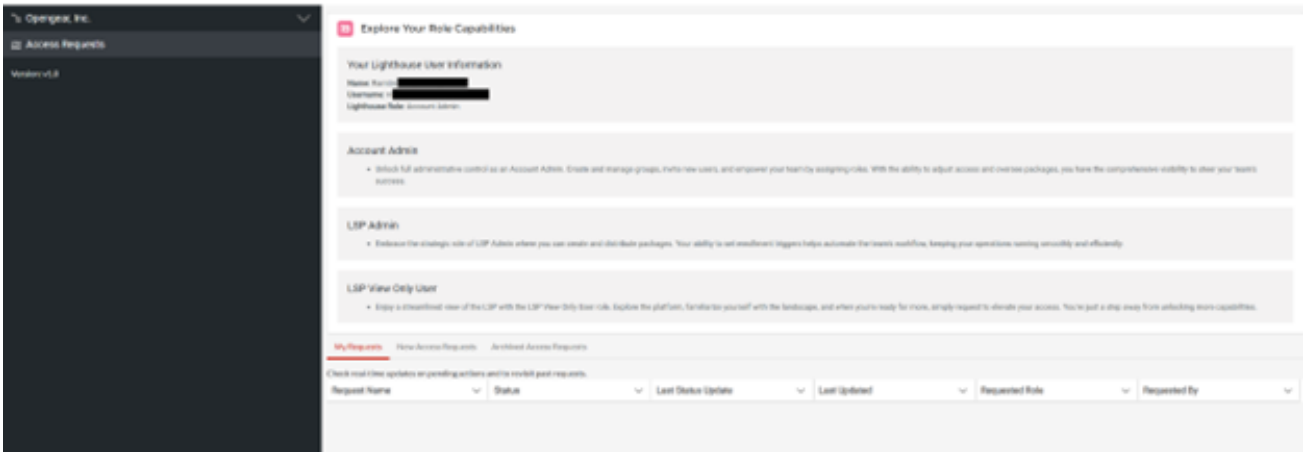
The LSP Dashboard shows any assets with recent activities such as enrollment, call homes, enrollment package assignments, and more.



PERMISSIONS

Only the user who originally received the Lighthouse License Key initially has access to the full LSP menu. Other users can be promoted in two ways:

1. Navigate to the Access Request page and send a request to an LSP admin inside your organization.



2. Open a Support Case or reach out to your Sales Rep directly to request access.

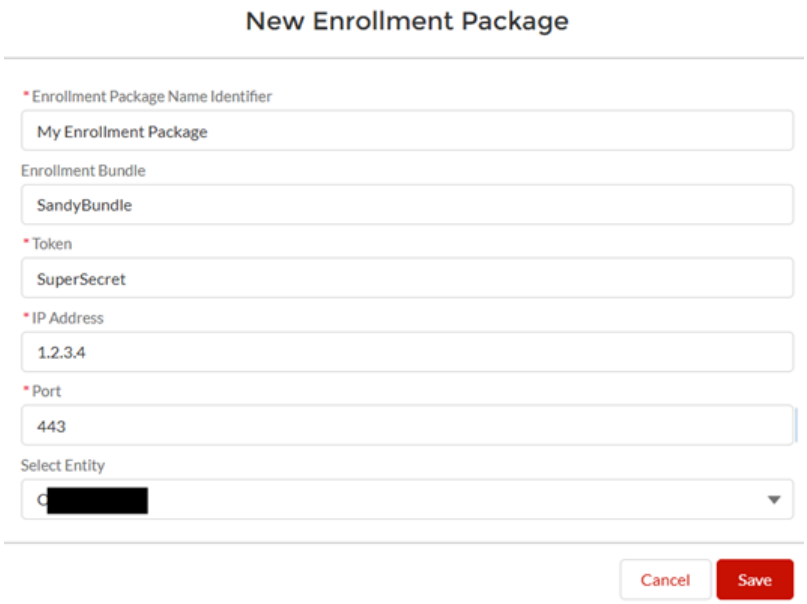
There are three different roles inside LSP:

1. **Account Admin**
   Account Admins have full administrative control. They can create and manage groups, invite new users, and assign roles. With the ability to adjust access and oversee packages, they have comprehensive visibility to steer team success.
2. **LSP Admin**
   LSP Admins can create and distribute packages. The ability to set enrollment triggers helps automate workflows, keeping operations running smoothly and efficiently.
3. **LSP View Only User**
   LSP View Only Users have a streamlined view of LSP. They can explore the platform, familiarize themselves with the landscape, and request elevated access when needed.

ENROLLMENT SETTINGS

This is where you create a new Enrollment Package and configure Enrollment preferences.

First, an admin should create at least one Enrollment Package. This package will include Lighthouse IP, Bundle/Token, and API Port to ensure your node can digest this info and enroll to the desired Lighthouse Instance.

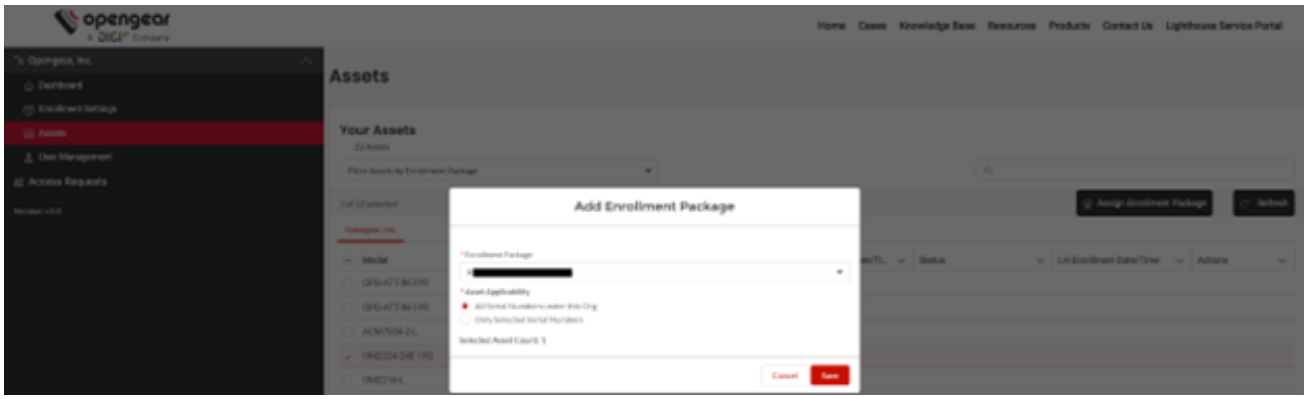


There are the four possible enrollment preference scenarios:

1. **Both Automatic Enrollment Triggering and Default Enrollment Packages are Disabled**
   Nodes must be manually assigned enrollment packages and approved before the system sends the enrollment package. Approval is only possible after nodes have performed a "call home" action.
2. **Both Automatic Enrollment Triggering and Default Enrollment Package are Enabled**
   Nodes automatically receive a default enrollment package immediately upon calling home; no manual intervention is required.
3. **Automatic Enrollment Triggering is Enabled and the Default Enrollment Package is Disabled**
   Nodes must have an enrollment package manually assigned after calling home, but do not require manual approval.
4. **Automatic Enrollment Triggering is Disabled and Default Enrollment Package is Enabled**
   Nodes automatically inherit the default package upon calling home but require manual approval before the package details are sent.

ASSETS

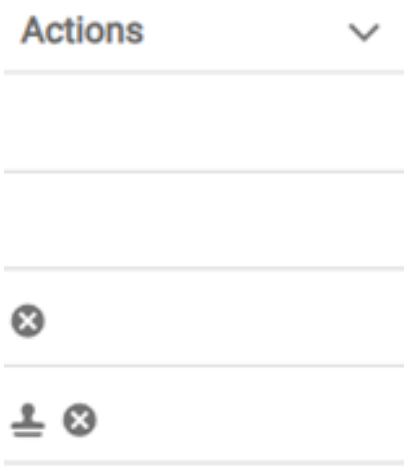
The assets tab shows all available assets (LSP enabled or not). You can assign enrollment packages to specific assets.



Possible Actions for each asset:

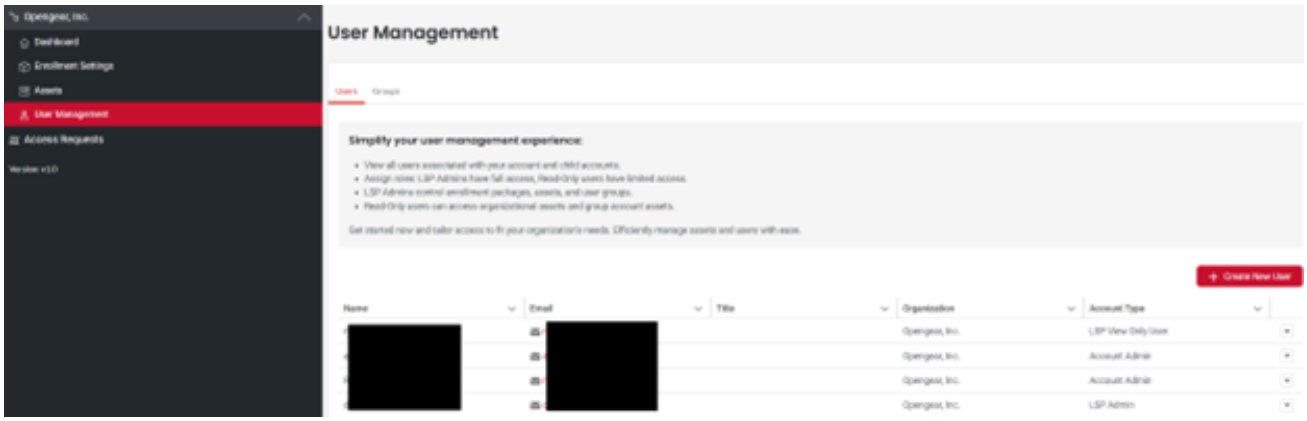
1. **Approve**: You can approve a call home action (if using manual enrollment).

2. **Clear**: You can clear a node of previous enrollment package information.



USER MANAGEMENT

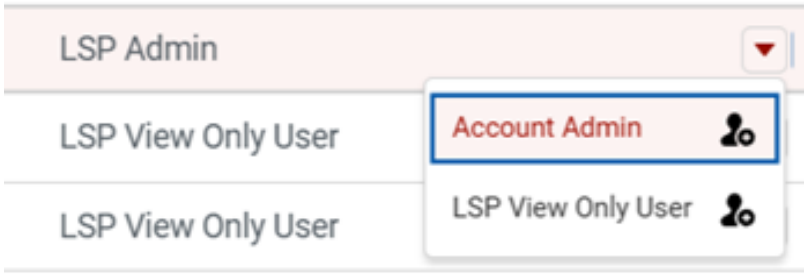
The User Management tab allows you to invite new users to the Opengear Customer Portal, Create new custom groups for permissions, and more.



Understanding the Roles inside LSP

Role	Account Admin	LSP Admin	LSP View Only User
Permission	• Create Groups • Invite/Create Users • Promote Users • Revoke Account/LSP Admin • Set Enrollment Triggering • Create Package • Assign Packages • Set Enrollment Triggering preferences	• Create Package • Assign Packages • Set Enrollment Triggering preferences	• View Only of LSP • Request Account/LSP Admin permission
Visibility	• See Current Account and Child • Note: When Creating a Group, Can see the Entire Account Structure Including Parent/Child/Sibling	See Current Account and Child	See Current Account and Child
Creation	License Key Owner	• Promoted by Account Admin • Promoted by Opengear Support or Sales team	All Portal Users

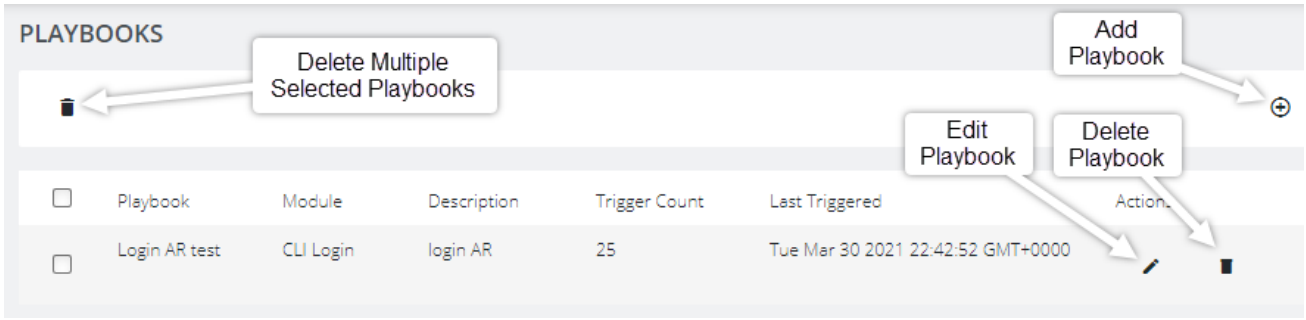
LSP Admins can promote or demote users inside your organization.



PLAYBOOKS

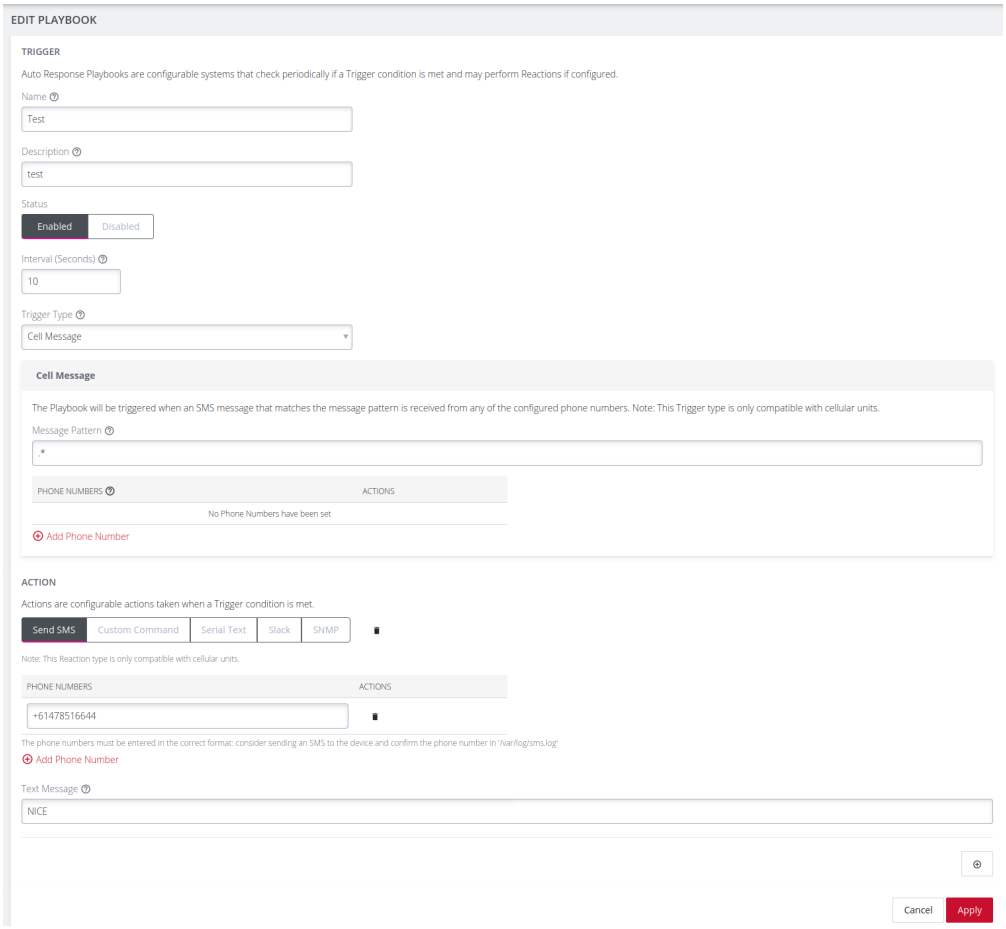
Playbooks are configurable systems that periodically check if a user-defined **Trigger** condition has been met. Playbooks can be configured to perform one or more specified **Reactions** when a specific trigger event occurs.

The Playbook Landing Page:



CREATE OR EDIT A PLAYBOOK

1. Navigate to the **Configure > Playbooks** page.
2. Click the **Add Playbook** button (top-right) to create a new **Playbook**.
   The **Edit Playbook** page displays.



3. In the **Trigger** section, complete the following fields as appropriate:

Field	Required Information
Name	Enter a meaningful name that will help other users understand the purpose of this playbook instance.

Field	Required Information
Description	Enter a detailed description of the playbook to help others understand what it does.
Status	Enable or Disable this playbook instance. Select enabled to activate the playbook after you have created it.
Interval (Seconds)	Enter the interval, in seconds, of the frequency that this playbook is repeated.

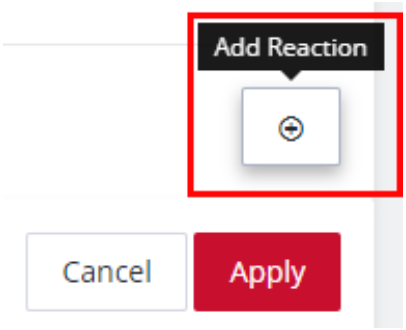
Field	Required Information
Trigger Type	From the drop-down, select the trigger type for this playbook instance: • **CLI Login**: Triggers upon Login or Logout events. Select either or both. • **CLI Log in Failure**: Monitor the terminal and trigger on failed user log in attempts. • **Cell Connection**: 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.

Field	Required Information
Trigger Type	• **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 response when they change. • **Ping**: Periodically pings an address and triggers a user-defined response upon failure. • **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. Additional fields may display depending on the selected **Trigger Type**.
CLI Login	This is displayed when the **Trigger Type** selected is **CLI Login**. Select the check boxes to monitor the terminal and trigger on user **Login** and/or **Logout** events.

Field	Required Information
Cell Message	This is displayed when the **Trigger Type** selected is **Cell Message**. You can: • Enter a **Message Pattern** to match against. • **Add Phone Number** to filter by phone number. If no phone number is specified, then this filter matches against all phone numbers.

4. In the **Action** section, customize the follow up action when a playbook is triggered:
   a. Select the **Action** to take when a trigger condition is met. You can select from:
      - **Send SMS**
      - **Custom Command**
      - **Serial Text**
      - **Slack**
      - **SNMP**

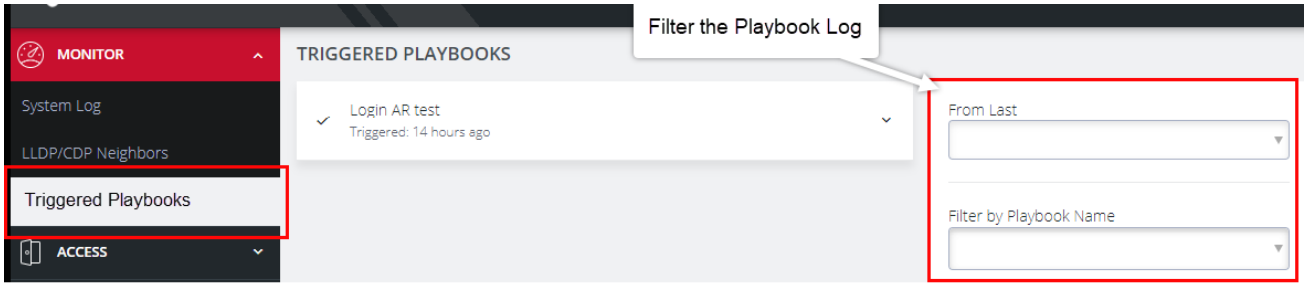
      Additional fields display depending on the **Action** selected.
   b. Complete any additional fields as appropriate.
   c. To create additional **Actions** for the same trigger, click the **Add Reaction** button.



5. When you are finished, click **Apply**.
   A banner confirms that the Playbook settings are saved, if the Playbook is **Enabled** it is activated.

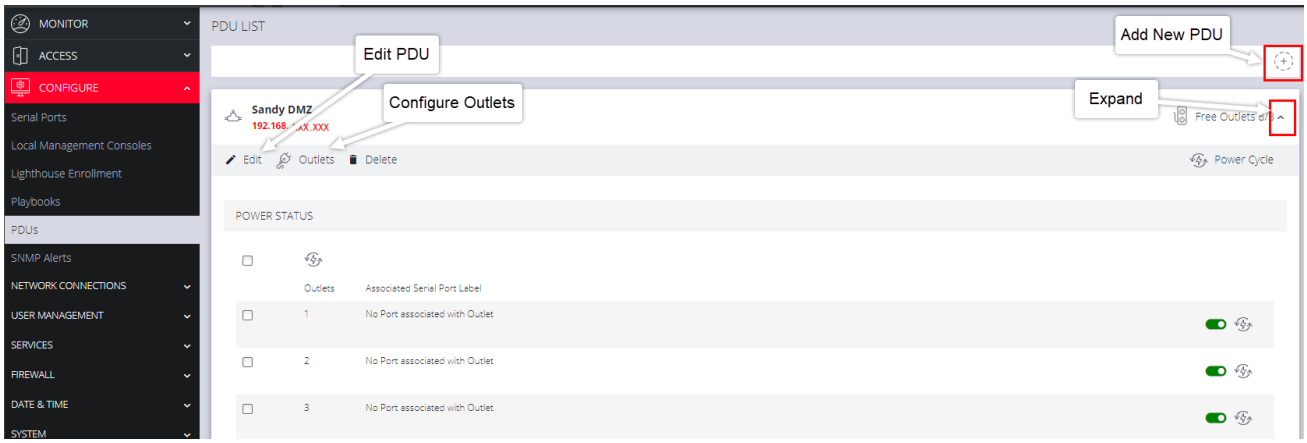
MONITOR A CURRENT PLAYBOOK

1. Click on the **Monitor > Triggered Playbooks** menu (shown in the following image).
2. Select the time period if required.
3. Filter by **Name** of **Playlist** to view any that have been triggered.



PDUS

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



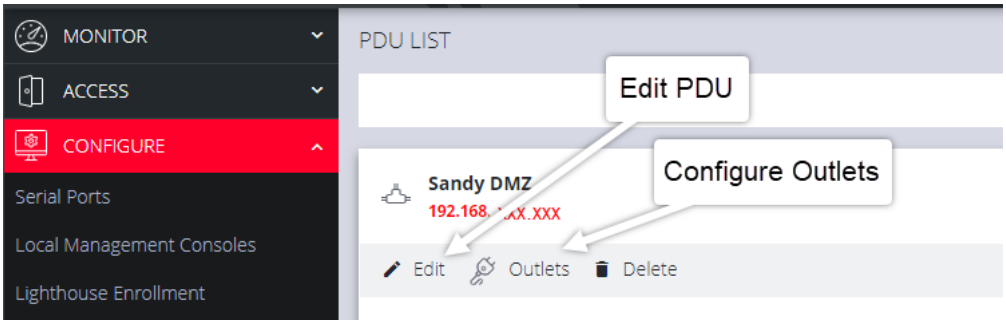
ADD AND CONFIGURE A PDU

1. In the **PDU List** page, click the **Add New PDU** button.
   The **Edit** page displays.
2. Complete the fields as appropriate:

Field	Description
Label	Enter a meaningful label to easily identify the individual PDU.
Monitor	Select this check box to monitor the outlet's status.
Mode	Select the mode from **Local** or **Remote**. Different fields display depending on the selection.
Driver	Select the appropriate driver compatible with this PDU.
Port	The serial port to which the PDU is connected. This field is available only when **Mode** is set to **Local**.
Username	Enter the Username to use when connecting. This field is available only when **Mode** is set to **Local**.
Password	User password to use when connecting to the device. This field is available only when **Mode** is set to **Local**.

Field	Description
Address	The remote address of the PDU. This field is available only when **Mode** is set to **Remote**.
SNMP Protocol	Click the drop-down arrow and select the correct transport protocol used to communicate with the PDU. The default value is UDP. This field is available only when **Mode** is set to **Remote**.
Version	The version of SNMP to use, V1, V2c and V3 are supported. The default value is V1. This field is available only when **Mode** is set to **Remote**.
Community	Enter a group name authorized to communicate with the device for SNMP versions 1 and 2c. This field is available only when **Mode** is set to **Remote**.
Authentication Protocol	Click the drop-down arrow and select the authentication protocol used for authenticated SNMP v3 messages. Only available when the **Version** is set to **v3**. This field is available only when **Mode** is set to **Remote**.

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

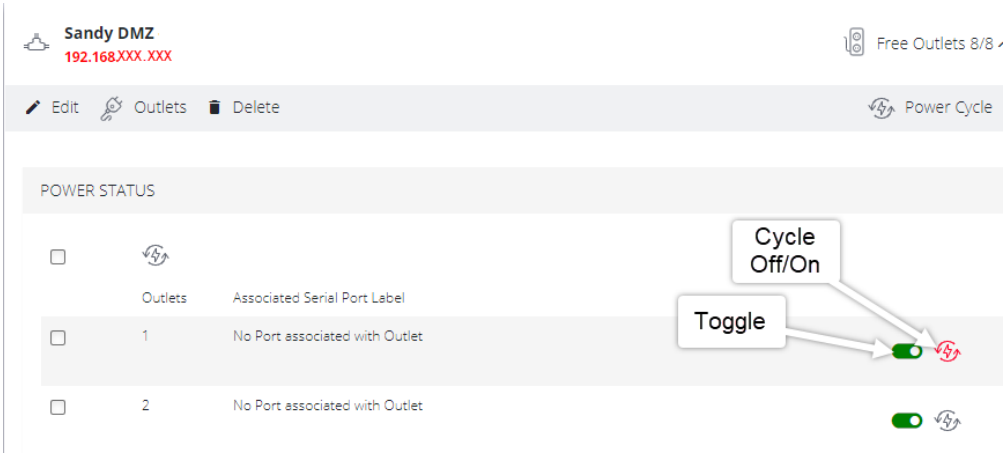


4. When you are finished, click **Apply**.

   A green banner confirms your settings.

After you have created (and configured) **PDUs**:

- you can **Edit** or **Delete** them from the **Configure > PDUs** page.
- operation is simple. For any PDU that has Monitoring set to **Enabled**, the **Toggle** on/off switch powers-on or powers-off the PDU, and the **Cycle** button cycles the PDU through a power-down and power-up cycle.



SYSTEM ALERTS

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

You can add or delete System Alert Managers under **Configure > System Alerts** for the following:

- System Alerts - General: Covers notification for the following:
  - **Configuration Change**: For changes that occur to the system configuration.
- System Alerts - Power: When voltage SNMP alerts are enabled, network operators are immediately notified should the PSU begin operating outside design tolerances.
- System Alerts - Temperature: When system temperature alerts are enabled, network operators are immediately notified should the system begin operating outside user-defined tolerances.
- System Alerts - Networking (Connection Status) **(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.

SYSTEM ALERTS - GENERAL

AUTHENTICATION

Provides notification 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 > System Alerts > General > Authentication**.
2. Click on the **Enabled** button to activate the function.
3. Click **Apply**.
   The **Details Saved** banner confirms your settings.

CONFIGURATION CHANGE

Notifies of changes that occur to the system configuration.

1. Navigate to **Configure > System Alerts > General > Configuration Change**.
2. Click on the **Enabled** button to activate the function.
3. Click **Apply**.
   The **Details Saved** banner confirms your settings.

SYSTEM ALERTS - POWER

The PSU is one of the most critical parts of the Console Manager, 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 Console Manager going into brown-out state. If it gets too high, it can damage components.

For the CM8000, where the PSU manages any overvoltage with protection circuitry, the PSU indicates presence when power is available.

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

ENABLE POWER SUPPLY SYSLOG ALERTS

The System Voltage Range alert sends an alert when the system reboots or the voltage on either power supply leaves or re-enters the fixed voltage range between 11.4V to 12.6V (SNMP) (or 11V to 13V Syslog).

> **Note:** For the CM8000, the PSU alert sends an alert when the PSU voltage presence becomes active or inactive.

1. Navigate to **Configure > System Alerts > Power**.
2. Click on the **Enabled** button to activate the function.

   > **Note:** The **Disabled** button de-activates the power syslog function and power alerts are stopped until activated again

3. Configure the Syslog Alert Severity:
   a. For **Power Lost** alert, click the drop-down list and select the severity level required (default level is **3 - ERROR**) when power level is outside the pre-set range.
   b. For **Power Restored** alert, click the drop-down list and select the severity level required (default is **6 - INFO**) after an error condition has been fixed.
4. Click **Apply**.
   The **Details Saved** banner confirms your settings.

When an event occurs that causes the voltage range on any power supply to leave or re-enter the configured voltage range, it causes an SNMP alert to be triggered. The alert reports the event type and identity and status of the PSU, as in the following example.

```
Nov 03 06:09:35 om2232 system-alerts[850]: Redundant Supply Active (PSU0 online, PSU1 online)
Nov 03 07:05:02 om2232 system-alerts[850]: Redundant Supply Inactive (PSU0 offline, PSU1 online)
Nov 03 07:05:05 om2232 system-alerts[850]: Redundant Supply Active (PSU0 online, PSU1 online)
```

To view log severity messages locally, use the journal tool command: `journalctl -f -u alert-logger -o verbose` where: f = follow. Check the alert-logger using the `systemctl status alert-logger` command.

> **Note:** For the CM8000, the PSU alert sends an alert when the PSU voltage presence becomes active or inactive.

SYSTEM ALERTS - NETWORKING (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.

> **Notes:**
> - Cell signal strength applies to cellular enabled devices only.
> - Network link state applies to all devices.

CONFIGURE SIGNAL STRENGTH ALERTS

Configure > SNMP Alerts > Networking > Network Connection Status

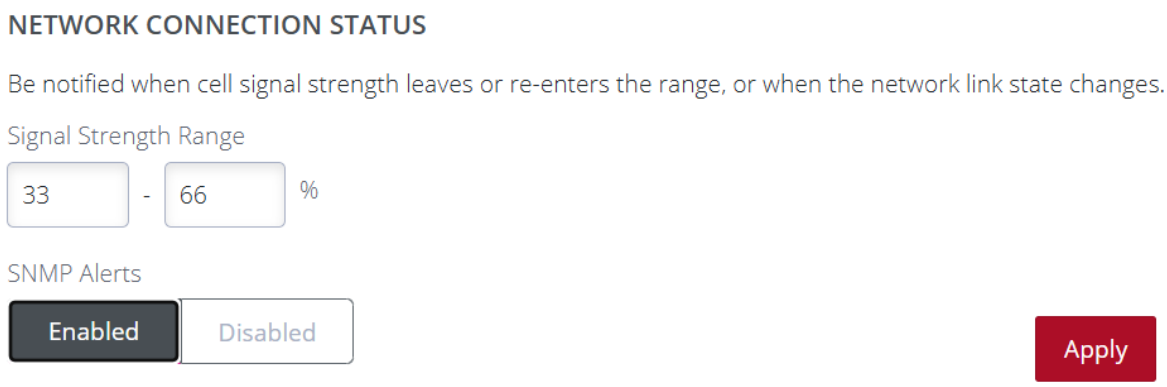
To set the Network Connection Status signal strength boundaries:

1. Navigate to the **Configure > System Alerts > Networking** page.
2. Click on the **Enabled** button to activate the function.
3. In the **Signal Strength Range** fields, set limiters to the required upper and lower limits.

   > **Note:** The **Disabled** button de-activates the function and signal strength alerts are stopped until activated again.

4. Click **Apply**.

   The **Details Saved** banner confirms your settings.



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

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

NETWORK CONNECTIONS

The **Network Connections** menu provides:

Network Interfaces,

IPsec Tunnels

Static Routes

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.

For information about VLAN interfaces, bridges, and bonds, see Bonds and Bridges.

For information about creating or configuring Loopback Interfaces see Create or Configure a Loopback Interface in the Config CLI Use Case Examples section.

DUAL SIM

> **Note:** This section applies to cellular variants only. The CM8000 does not support cellular connectivity.

CONFIGURE > NETWORK CONNECTIONS> Network Interfaces > WWAN0 - Cellular Interface

Console 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 CM

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.

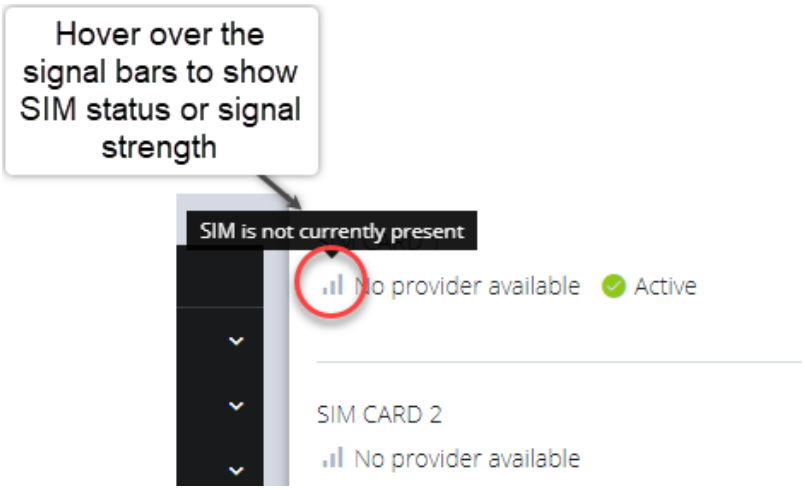
DISPLAY SIM STATUS AND SIGNAL STRENGTH

> **Note:** For information about configuring the **Signal Strength Thresholds**, see System Alerts.

1. Navigate to **Configure > Network Connections > Network Interfaces**.
2. Click on the **WWAN0 - Cellular Interface** row.
   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 - then the cellular interface is not visible.

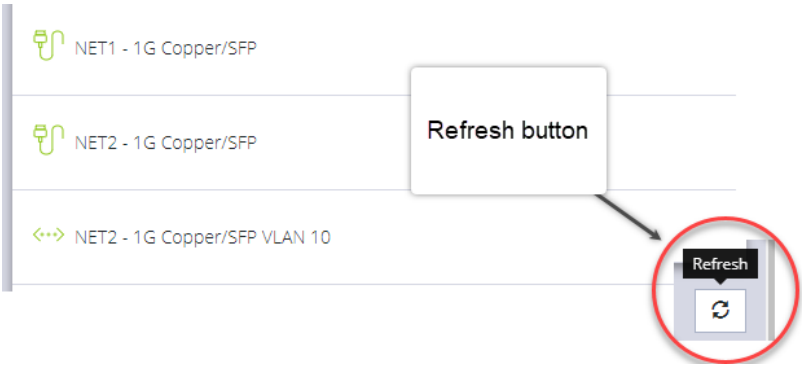
3. The active SIM indicates the color of the signal strength based on the selected thresholds in **Configure → SNMP Alerts** under the **Networking Signal Strength Alert**.



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,

4. 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 want to know what the other SIM Signal Strength is, you must activate it, let the modem come back online, which may take three minutes or more.

INSTALL A NEW SIM CARD

When you install a new SIM card into its slot while the appliance is active (hot swapping), it may take a minute or two for the system to react and stabilize after the SIM card change.

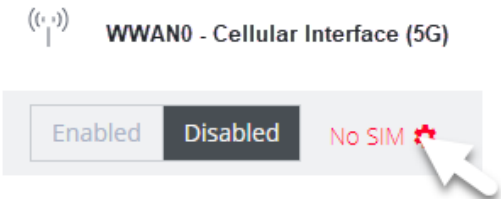
Two SIM card slots are located on the rear face of the device, insert each SIM card(s) into its respective slot (marked 1 and 2) until you feel the card click into place.



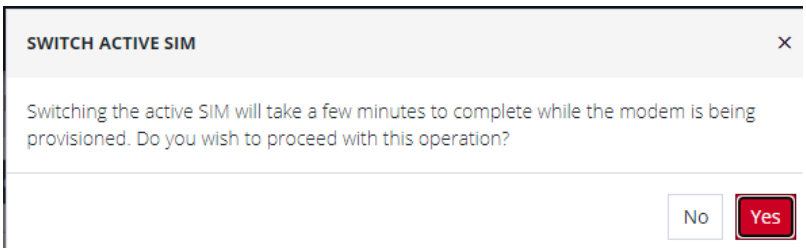
SELECT THE ACTIVE SIM (MANUAL FAILOVER MODE)

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

1. Navigate to **CONFIGURE > NETWORK CONNECTIONS > Network Interfaces > WWAN0 - Cellular Interface** .
2. Click the **Settings cog** .
   This displays the **MANAGE WWAN0 - Cellular Interface** page and the current status of both SIM slots, including the current carrier name.



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
```

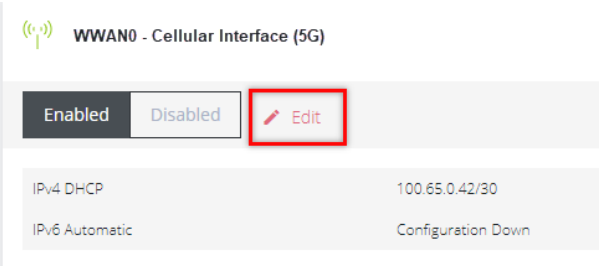
You can also set the SIM settings by expanding the menu for each SIM to set the APN.

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.

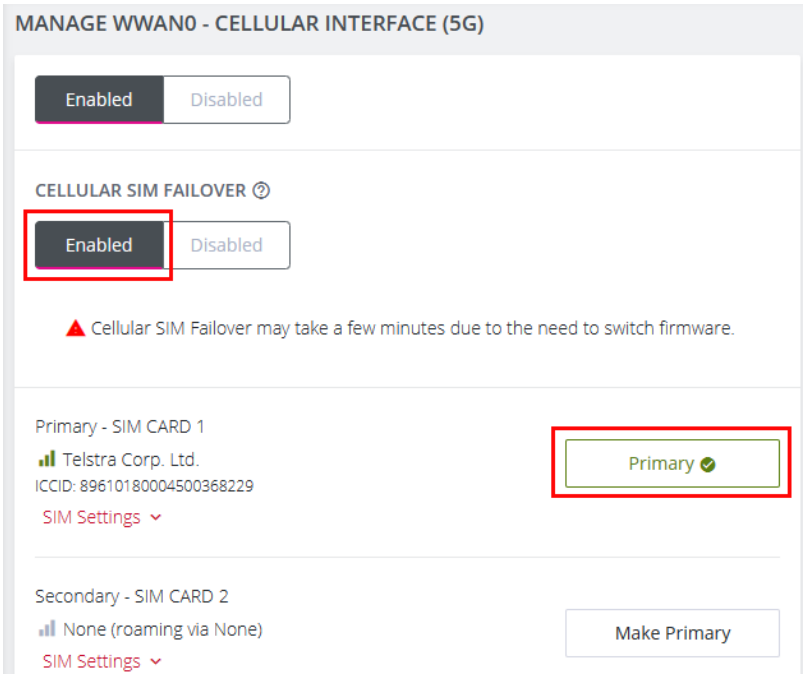
SELECT THE PRIMARY SIM (AUTOMATIC FAILOVER MODE)

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

1. Navigate to **CONFIGURE > NETWORK CONNECTIONS > Network Interfaces > WWAN0 - Cellular Interface**.
2. Click the **Edit** icon.
   This displays the **MANAGE WWAN0 - Cellular Interface** page and the current status of both SIM slots.

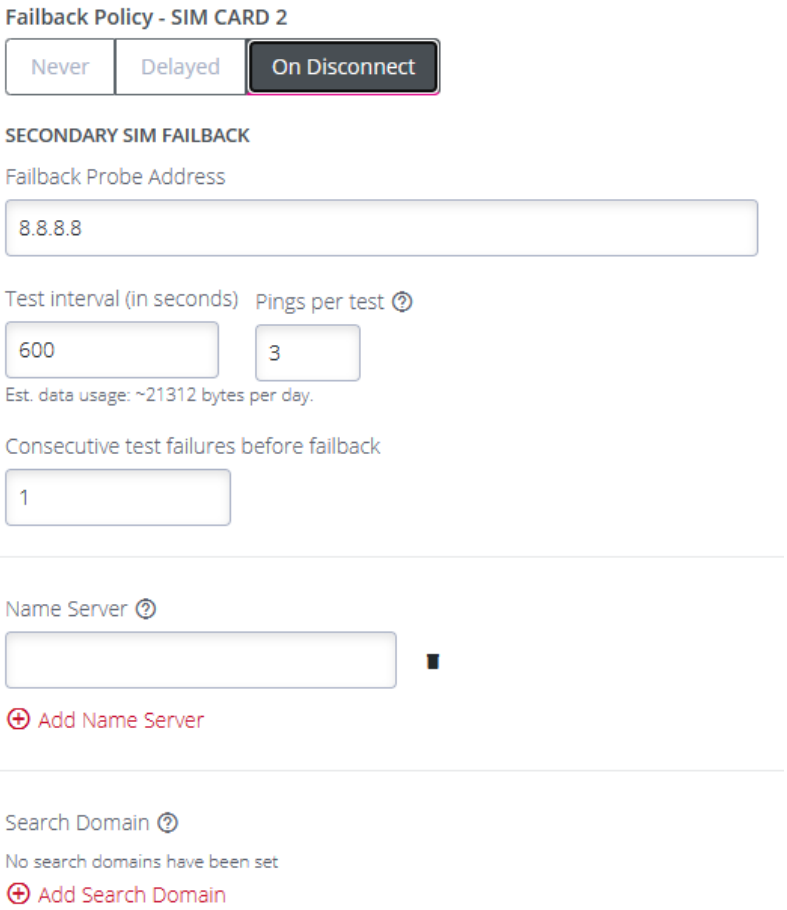


3. Ensure the cellular interface is enabled by clicking the **Enabled** button.



4. Click the **Primary** button of the SIM selected to be the primary SIM.

5. Select the required **Failback Policy** for the failback SIM and complete the failback policy details.



6. Click the **Confirm** button at the bottom of the page.
   A green banner displays to confirm that the new settings are saved.

DUAL SIM FAILOVER

> **Note:** This section applies to cellular variants only. The CM8000 does not support cellular connectivity.

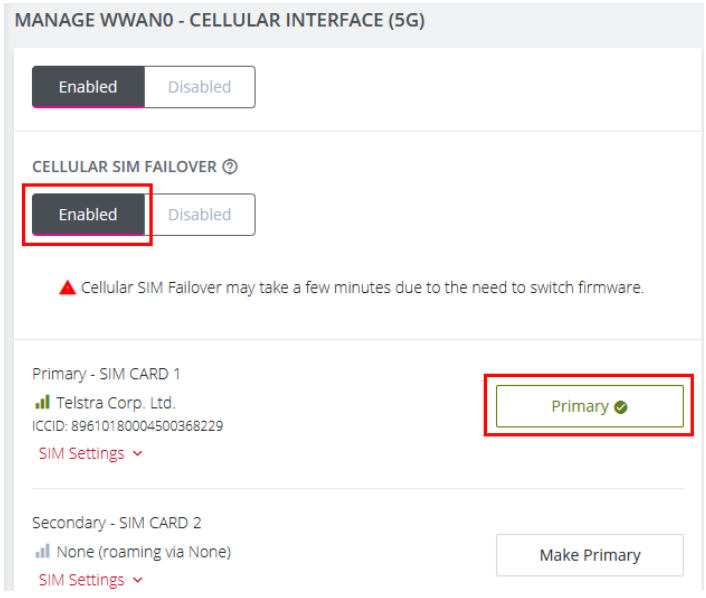
CONFIGURE > NETWORK CONNECTIONS> Network Interfaces > WWAN0 - Cellular Interface > Edit

Console Managers that carry two SIM cards can be configured so that either SIM card slot may be activated. In failover mode, either of the two SIM cards may be designated as the Primary SIM. (see Dual SIM).

Dual SIM 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 failover to the Secondary SIM without the requirement 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.

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 following scenario), is activated in the event of a failover such as occurs during an OOB communications failure on the Primary SIM.



FAILOVER MODES

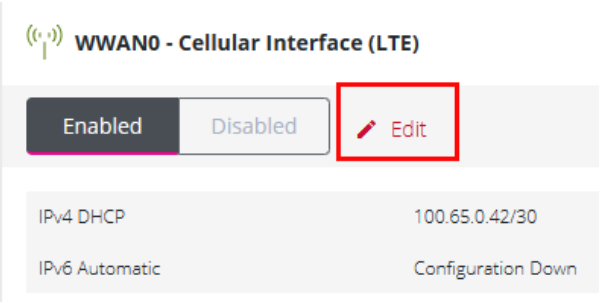
Features of Failover include:

- Select **Enabled** SIM failover.
- Specify SIM failback policy (applicable when the Ethernet connection and primary SIM are both down):
  - **Never** - The node never switches back to the Primary.
  - **Delayed** (specified in minutes) - The node switches back to primary after a pre-defined time has elapsed.
  - **On Disconnect** - See Cellular Interface Policy Settings for an explanation of the policy.
- 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.

ACTIVATE OR CONFIGURE FAILOVER

CONFIGURE > NETWORK CONNECTIONS> Network Interfaces > WWAN0 - Cellular Interface > Edit

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. Select the **Enabled** failover option.

4. Ensure the correct SIM card is selected as the Primary SIM (see 'Set Primary SIM' on Dual SIM).
5. Complete the Cellular Interface options in accordance with the following table:

MANAGE WWAN0 CELLULAR INTERFACE Properties	
Field	**Definition**
CELLULAR SIM FAILOVER - **Enabled.**	Switch between the Primary SIM Card and the secondary SIM Card on disconnection.
Primary SIM Failover	
Failover Probe Address.	Network address to probe in order to determine if connection is active. 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.
Failback Policy	

MANAGE WWAN0 CELLULAR INTERFACE Properties	
Field	**Definition**
Never / Delayed / On Disconnect.	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 fail-back to the Primary SIM Card.
On Disconnect	Secondary SIM Failback.
	Failback Probe Address - The Network address to probe in order to determine if the connection is active.
	Test Interval - The number of seconds between connectivity probe tests (this not the same thing as Attempted Failback).
	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.

6. Click **Confirm** to activate the failover policy settings.
   A green banner confirms the settings are enabled.

CELLULAR MODEM FIRMWARE UPGRADE

> **Note:** This section applies to cellular variants only. The CM8000 does not support cellular connectivity.

This Cellular Modem Firmware Upgrade procedure provides an automatic download and upgrade process for carriers, and, a secondary manual upgrade process for users who must use a firmware set that has not been tested by Opengear or use a carrier that is not supported by the standard cellular modem firmware.

Opengear devices use a standard modem, however, due to the variety of carriers that exist, there is a wide variety of firmware packages which are offered by Sierra Wireless (Opengear's modem provider) in order to accommodate these different carriers. When Opengear devices are supplied, they are provided with the most common set of modem firmware pre-installed; this minimizes difficulty when setting up cellular services on devices. The manual cellular upgrade procedure supports users deploying cellular capable devices to regions that use a carrier that is not supported by the standard cellular modem firmware.

> **Note:** The Cellular Firmware Upgrade procedure is only available through terminal or shell access. The use of automated tools such as cron jobs is not supported and is therefore discouraged.

MODEM FIRMWARE UPGRADE PROCEDURES

CELLULAR AVAILABILITY DURING UPGRADE

The `cell-fw-update` command disables the cellular modem during the upgrade process. This causes a loss of availability of the Out-of-Band (OOB) link which can only be restored when the cellular modem has returned to a working state. If in failover, the modem upgrade is deferred until the device is not in failover. To override this feature, set the `--ignore-defer` flag.

CELL-FW-UPDATE HELP

```
root@om2248-1-tp1-p14:~# cell-fw-update --help
Usage: /usr/bin/cell-fw-update [options] <actions>
Actions:
              -m <file> [-m <file>]..     Flash modem with firmware <file>(s)
              -c <carrier>                                          Flash modem
with firmware suitable for <carrier>




              -l




List carrier IDs suitable for use with -c
              -f                                      Write current fingerprint and
timestamp to stdout
              -u                                      Update file lists from remote
server
              -d                                     Download/synchronize fw files
from remote server









              -h
```

```
Show this usage

Options:

              -a                                        Report automated upgrade

messages

              -b <url>                                Specify base URL to remote

              -v                                         Verbose messages




              -C




Continue/resume partial downloads

              --unsafe                               Ignore all checksums/signatures and

allow downgrades.

                                                           This enables existing

firmware to be re-flashed when using the qmi-firmware-update back-end

              --defer                                  deprecated!      Do not permit

firmware upgrade if system is currently failed-over.

                                                           This is now default

behaviour. Use the flag --ignore-defer to bypass this.

              --libqmi                                                          Force use

of libqmi tool qmi-firmware-update. Cannot use with --mbpl

              --mbpl                                                              Force

use of Sierra Wireless MBPL fwdwl-lite. Cannot use with --libqmi

              --ignore-defer                                Bypass the 'failover

defer' check to force a modem firmware upgrade
```

```
root@om2248-l-tp1-p14:~# cell-fw-update --help
Usage: /usr/bin/cell-fw-update [options] <actions>

Actions:
    -m <file> [-m <file>].. Flash modem with firmware <file>(s)
    -c <carrier>        Flash modem with firmware suitable for <carrier>
    -l              List carrier IDs suitable for use with -c
    -f              Write current fingerprint and timestamp to stdout
    -u              Update file lists from remote server
    -d              Download/synchronize fw files from remote server
    -h              Show this usage
Options:
    -a              Report automated upgrade messages
    -b <url>            Specify base URL to remote
    -v              Verbose messages
    -C              Continue/resume partial downloads
    --unsafe            Ignore all checksums/signatures and allow downgrades.
                    This enables existing firmware to be re-flashed when using the qmi-firmware-
update back-end
    --defer             deprecated! Do not permit firmware upgrade if system is currently failed-over.
                    This is now default behaviour. Use the flag --ignore-defer to bypass this.
    --libqmi            Force use of libqmi tool qmi-firmware-update. Cannot use with --mbpl
    --mbpl              Force use of Sierra Wireless MBPL fwdwl-lite. Cannot use with --libqmi
    --ignore-defer      Bypass the 'failover defer' check to force a modem firmware upgrade
```

UPDATE LOCAL FILE LIST AND DOWNLOAD LATEST FIRMWARE FILES

This procedure updates the local file list and downloads the latest firmware files.

Note: `cell-fw-update` can be run directly from a CLI shell as root and requires no configuration. You can combine this update action with the following download operation by providing both -u and -d simultaneously.

```
root@om8148-10g-tp2-p35:~# cell-fw-update -ud
Waiting for clients to stop using the modem...
The modem is now locked


=== INFO ===
The modem is locked by client cellfw
No clients want to use the modem
UIM failover status is disabled
Active UIM slot is 1 (ICCID: 89610180003137049629)
Operator is telstra corp. ltd.
0157863e6fe95988415b264e35ac0b4f687ffbf9 2024-01-18
download e4c83bb1ae1e5be73c3a254fca7e13e38b33e39a SWIX65C_02.13.08.00.cwe
download 31dca80c90d37100b17ac8e49998ce35724c6b90 SWIX65C_02.13.08.00_GENERIC_
030.047_001.nvu
download 5ed78eb2d69d651d73e177c855eaecb02c6df0b0 SWIX65C_02.13.08.00_PTCRB_
030.045_001.nvu
download 91b8c518ddfad508ffe22c0f099465abb8b31d88 carrier-canon.txt
download b8d3a9cb4faabcf6f5e1fa5acb0f4e41ed72f506 carriers.txt
copy a6ddf97fb6b6f8dd0d011d54dcdfe34db64b25ee cell-firmware.txt
copy - localfiles.txt
copy - localdb.txt
copy - SHA1SUMS
```

Note: The `cell-fw-update -u` and `cell-fw-update -d` commands may be run separately.

LIST SUPPORTED CARRIERS

The resulting carriers shown are for example only (local results may vary).

```
root@om2216-1:~# /etc/scripts/cell-fw-update -l
att AT&T
docomo DoCoMo
generic Generic
kddi KDDI
kt Korea Telecom
rogers Rogers
softbank SoftBank
sprint Sprint
telstra Telstra
telus Telus
tmo T-Mobile
uscellular U.S. Cellular
verizon Verizon Wireless
```

AUTOMATIC FIRMWARE UPDATE FOR CURRENT CARRIER

This procedure detects the currently connected carrier and updates the firmware set for that specific carrier. A firmware set consists of the modem's firmware image (.cwe) and a carrier specific PRI firmware image (.nvu). This set is required for modem operation.

```
cell-fw-update -a
```

FIRMWARE UPDATE FOR SPECIFIC CARRIER

Specify the carrier for which you want to update the firmware.

```
cell-fw-update -c <carrier>
```

> **Note:** Use the `cell-fw-update -l` command to list supported carriers.

MANUAL FIRMWARE UPDATE

Specify a firmware set to download to the modem. This allows you to update the modem with a specific firmware set instead of one provided by Opengear FTP. The path to the firmware set specified must be relative from the directory /mnt/nvram/cellfw/.

> **WARNING:** This operation must be used with great caution as can result in the modem becoming *permanently* unavailable or damaged. Use at your own risk.

```
root@om8148-10g-tp2-p35:~# cell-fw-update --unsafe -m SWIX65C_02.13.08.00.cwe -m
SWIX65C_02.13.08.00_GENERIC_030.047_001.nvu
Waiting for clients to stop using the modem...
The modem is now locked
=== INFO ===
The modem is locked by client cellfw
No clients want to use the modem
UIM failover status is disabled
Active UIM slot is 1 (ICCID: 89610180003137049629)
Operator is telstra corp. ltd.
Application version: 1.0.2307.1
Target image Info:
Carrier :GENERIC
FW Version :02.13.08.00
Model ID :SWIX65C
Package ID :001
PRI Version:030.047
SKU :9999999
Switching device into download mode ...
Modem Needs FW
Modem Needs PRI
```

```
Downloading: /tmp/cell-fw-update.4045/SWIX65C_02.13.08.00.cwe
Downloading: /tmp/cell-fw-update.4045/SWIX65C_02.13.08.00_GENERIC_030.047_001.nvu
All image data was downloaded successfully.
Device is about to reset ...
Waiting for modem to come up in ONLINE mode ...
Modem is now in ONLINE mode ...
FW update status: Successful
FW info from modem:
Model ID : EM7565
FW Version : SWIX65C_02.13.08.00
Carrier Name : GENERIC
Carrier PRI Revision: 030.047_001
Firmware download process completed successfully.
INFO: QDL Port: /dev/wwan0qdl0
INFO: Device Path: /dev/wwan0qmi0
INFO: FW Path: /tmp/cell-fw-update.4045
Waiting for modem to disconnect from the host ...
Modem disconnected from host.
Waiting for modem to come up in BOOT and HOLD mode ...
BOOT and HOLD Mode. Downloading firmware ...
[/dev/wwan0qmi0] Device list of stored images retrieved:
[/dev/wwan0qmi0] Device list of stored images retrieved:
<14>Jan 22 06:05:25 cell-fw-update: The firmware was successfully stored on the
modem
[/dev/wwan0qmi0] Device list of stored images retrieved:
```

SEE ALL CELL FIRMWARE INSTALLED ON THE MODEM VIA OGCLI

Use the following to return all cell firmware installed on the modem:

```
# ogcli get cellfw/installed
```

The following shows an example result:

```
# ogcli get cellfw/installed
ogcli get cellfw/installed
firmware[0].active=true
firmware[0].carriers[0].active=false
firmware[0].carriers[0].full_firmware_version="02.17.08.00_CARRIER_030.094_001"
firmware[0].carriers[0].name="CARRIER"
firmware[0].carriers[0].unique_id="030.094_001"
firmware[0].carriers[1].active=false
firmware[0].carriers[1].full_firmware_version="02.17.08.00_CARR2_030.018_001"
firmware[0].carriers[1].name="CARR2"
firmware[0].carriers[1].unique_id="030.018_001"
firmware[0].carriers[2].active=false
firmware[0].carriers[2].full_firmware_version="02.17.08.00_GENERIC_030.081_001"
firmware[0].carriers[2].name="GENERIC"
firmware[0].carriers[2].unique_id="030.081_001"
firmware[0].failures=0
firmware[0].firmware_version="02.17.08.00"
firmware[0].slot=1
modem.model="TEST123"
modem.sku_id="1122334"
modem.slots=3
```

UPDATE CELL FIRMWARE WITH A CELL ONLY CONNECTION

> **CAUTION:** When the cellular firmware update is initiated, the connection to the device is lost. It is recommended to have console access to the device BEFORE the cellular firmware update is initiated.

View Installed Cell Firmware

Knowing the cellular modem model and the corresponding cellular firmware that can be installed for this device helps with the manual installation of cellular firmware.

Use the following to return all cell firmware installed on the modem:

```
ogcli get cellfw/installed
```

The following shows an example result, which includes the cellular modem model installed on the device:

```
# ogcli get cellfw/installed
ogcli get cellfw/installed
firmware[0].active=true
firmware[0].carriers[0].active=false
firmware[0].carriers[0].full_firmware_version="02.17.08.00_CARRIER_030.094_001"
firmware[0].carriers[0].name="CARRIER"
firmware[0].carriers[0].unique_id="030.094_001"
firmware[0].carriers[1].active=false
firmware[0].carriers[1].full_firmware_version="02.17.08.00_CARR2_030.018_001"
firmware[0].carriers[1].name="CARR2"
firmware[0].carriers[1].unique_id="030.018_001"
firmware[0].carriers[2].active=false
firmware[0].carriers[2].full_firmware_version="02.17.08.00_GENERIC_030.081_001"
firmware[0].carriers[2].name="GENERIC"
firmware[0].carriers[2].unique_id="030.081_001"
firmware[0].failures=0
firmware[0].firmware_version="02.17.08.00"
firmware[0].slot=1
modem.model="TEST123"
modem.sku_id="1122334"
modem.slots=3
```

Download Cell Firmware

You can either:

- Complete the download on a factory reset device:
  1. Create the cellfw directory into which the firmware files will download.

     ```
     cd /mnt/nvram/
     sudo mkdir cellfw
     cd cellfw
     ```

  2. Download a zip file of all the cellular firmware files.

     ```
     sudo wget https://ftp.opengear.com/download/cellfw/cellfw-bundle-20250520.zip
     ```

  3. Extract the cellular firmware bundle.

     ```
     sudo unzip -j cellfw-bundle-20250520.zip
     ```

- Complete a targeted download:

  > **Note:** A targeted download is useful if the device has had a previous cellular firmware download and only requires specific files from the ftp. The user should know which cellular firmware files are required.

  1. Change directory to the local cellfw directory where firmware files are stored.

     ```
     cd /mnt/nvram/cellfw/
     ```

  2. Backup any local files that will be overwritten.

     ```
     sudo cp cell-firmware.txt cell-firmware.txt.bak
     sudo cp SHASUMS SHASUMS.bak
     ```

  3. At a minimum, download the cell-firmware.txt, SHASUMS, and the pre-requisite cellular firmware (*.cwe) and carrier PRI (*.nvu).

```
sudo wget https://ftp.opengear.com/download/cellfw/cell-firmware.txt -O cell-firmware.txt
sudo wget https://ftp.opengear.com/download/cellfw/SHA1SUMS -O SHA1SUMS
sudo wget https://ftp.opengear.com/download/cellfw/SWI9X50C_01.14.24.00.cwe -O SWI9X50C_01.14.24.00.cwe
sudo wget https://ftp.opengear.com/download/cellfw/SWI9X50C_01.14.24.00_VERIZON_002.064_000.nvu -O SWI9X50C_01.14.24.00_VERIZON_002.064_000.nvu
```

Identify Compatible Cellular Firmware Files

After you download the cell-firmware.txt file, you can use the file to identify cellular modem firmware files that are compatible with your cellular modem based on the model of your device.

```
cat /mnt/nvram/cellfw/cell-firmware.txt | grep $(ogdeviceinfo --no-cache system-sku-number | tr '[:upper:]' '[:lower:]' )
```

To further refine the list, only use the firmware files for the cellular modem model. This can be found from the previous instruction that showed how to view the currently installed firmware.

```
ogcli get cellfw/installed | grep modem.model
```

Update Cellular Firmware

> **Note:** The manual mode checks the SHA1SUM of the specified firmware files to ensure integrity and checks the versions to ensure that they are valid for this cellular modem model.

Use the manual mode to install the cellular firmware ensuring both required files are included for the supported cellular modem the device supports, cellular firmware (*.cwe), and carrier PRI (*.nvu).

```
sudo cell-fw-update -m SWI9X50C_01.14.05.00.cwe -m SWI9X50C_01.14.05.00_KT_002.016_004.nvu
```

MODEM UPDATE TROUBLESHOOTING GUIDE

The following procedure can be used to determine if the cellular modem is ready and available and may provide recovery if necessary if the upgrade or modem repeatedly fails.

DETERMINE IF MODEM IS READY & AVAILABLE

The service `ModemManager` is an essential dependency for all cellular modem operations. Please ensure it is running.

```
root@om8196-10g:~# systemctl start ModemManager
```

If the modem is running correctly, it should be able to be detected by ModemManager within 60 seconds of the service starting.

```
root@om8196-10g:~# mmcli -L
```

If the modem was not detected or is still problematic, the modem must be recovered.

RECOVER FROM BOOT & HOLD [EM9291 ONLY]

First, check if the modem is stuck in Boot & Hold mode. This can happen on a cellular firmware upgrade failure. If this is the case, then the device file /dev/wwan0qdl0 will be exposed, run:

```
root@om8196-10g:~# ls /dev/wwan0qdl0
```

If the device file was found, you can reset the modem with the following command:

```
root@om8196-10g:~# /usr/libexec/sierra/mbpl/fwdwl-lite --qdl /dev/wwan0qdl0 -reset
```

You should also reset the cellular modem's Device Management Service with the following command:

```
root@om8148-10g~# qmicli -p -d /dev/wwan0qmi0 --device-open-qmi --dms-reset
```

You can now run "Determine if Modem is Ready & Available" above.

POWER CYCLE [EM9291 ONLY]

If the modem cannot be recovered manually as per the previous steps, it may be recoverable through a power cycle. If the product is installed in the field and a full power cycle is not possible, the cellular modem can be individually rebooted with a script.

This should only be performed by support staff and it is not advised to inform customers about this unsupported feature. The script can be executed with the following command:

```
root@om8148-10g-tp2-p34:~# /usr/unsupported/bin/cell-reboot
```

You can now run "Determine if Modem is Ready & Available" on the previous page.

DETERMINE IF THE MODEM IS CURRENTLY BEING UPGRADED

The simplest way to determine if the modem is currently being upgraded is to check the currently running processes an look for `cell-fw-update`. This is done through the following check:

```
ps aux | grep cell-fw
```

The following example shows that an upgrade is running:

```
root@om2216-1:~# ps aux | grep cell
root 122965 0.2 0.0 4780 3992 pts/0 S+ 23:42 0:00 /bin/bash /usr/bin/cell-fw-
update -aud
root 125966 0.0 0.0 3332 1756 pts/1 S+ 23:47 0:00 grep cell
```

The following example shows that there is no upgrade running:

```
root@om2216-1:~# ps aux | grep cell-fw
root 126417 0.0 0.0 3332 1776 pts/1 S+ 23:48 0:00 grep cell-fw
```

BONDS AND BRIDGES

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.

For more information, see Create a bond and Edit a bond.

Bridges

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

For more information, see Create a bridge and Edit a bridge.

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

CREATE A BOND

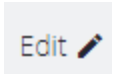
1. Navigate to the **Configure > Network Connections > Network Interfaces** page on the WebUI.
2. Click on the **New Bond** button that is located at the top-right of the window.
3. Select which interface will serve as the primary interface for the new bond.

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

4. Complete the new bond details form as appropriate:

New Bond Field	Definition
Description	The editable **Description** field allows you to add a description of the interface. If the description field is not completed the field defaults to a computed value to describe the interface.

New Bond Field	Definition
Mode	The mode determines the way in which traffic sent out via the bonded interface is dispersed over the real interfaces. Available modes are: • **Round Robin Balancing** - Packets are sequentially transmitted/received through each interface, one by one. • **Active Backup** - 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. • **XOR Balancing** - Balances traffic by splitting up outgoing packets between the Ethernet interfaces, using the same one for each specific destination when possible. • **Broadcast** - All network transmissions are sent on all secondary interfaces. This mode provides fault tolerance. • **802.3ad (Dynamic Link Aggregation)** - 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. • **Transmit Load Balancing** - 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. • **Adaptive Load Balancing** - Includes transmit load balancing (tlb) and receive load balancing (rlb) for IPv4 traffic and does not require any special switch support.

New Bond Field	Definition
Poll Interval	The poll interval specifies the MII link monitoring frequency in milliseconds. This determines how often the link state of each secondary is inspected for link failures. A value of zero will disable MII link monitoring.
Network Interface Selection	Click the checkbox of each network interface you want to include in the bridge. Available interfaces include Ethernet and VLAN interfaces that are not part of another bond or bridge.
Primary Interface	Select the interface to use for selecting the MAC address of the aggregate. The new bond inherits the MAC address of the primary interface. On creation, any Network Connections which exist on the Primary Interface will be attached to the Bond/Bridge after it is initially created. When a Bond/Bridge is deleted, any Network Connections which exist on the aggregate interface are handed over to the Primary Interface.
Active Connections	When the Primary Interface is created, the connections inherited by the new bond are listed here. When edited, Active Connections on the aggregate will not be updated if the primary interface is changed.
	Click to edit the details of an existing interface. Updating a bridge will temporarily interrupt network activity on the interface when you click the **Update** button.

5. Click the **Create** button to finalize the creation of the new bond.
   Network connections from non-primary interfaces are deleted when the new bond is created.

EDIT A BOND

1. Navigate to the **Configure > Network Connections > Network Interfaces** page on the WebUI.
2. Click on the bond that you want 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.

   For more information about the available fields, see Create a bond.
5. Click the **Update** button to finalize the edit process.

   Updating the bond temporarily interrupts network activity on this interface.

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

CREATE A BRIDGE

1. Navigate to the **Configure > Network Connections > Network Interfaces** page on the WebUI.
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 displays in the MAC address field. This MAC address is inherited by the new bridge interface.

4. Complete the new bridge details form as appropriate:

New Bridge Field	Definition
Description	The editable **Description** 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	Enable or disable Spanning Tree Protocol. For more information, see Spanning Tree Protocol.
Network Interface Selection	Click the checkbox of each network interface you want to include in the bridge. Available interfaces include Ethernet and VLAN interfaces that are not part of another bond or bridge. Bond interfaces can be included in a bridge by using the **ogcli** tool. See Support for Bonds in Bridges in the Knowledge Base.
Primary Interface	Select the interface to use 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.
Edit	Click to edit the details of an existing interface.

5. Click the **Create** button to finalize the creation of the new bridge.

EDIT A BRIDGE

1. Navigate to the **Configure > Network Connections > Network Interfaces** page on the WebUI.
2. Click on the bridge that you want 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.
   For more information about the available fields, see Create a bridge.
6. Click the **Update** button to finalize the edit process.
   Updating the bridge temporarily interrupt network activity on this interface.

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

SPANNING TREE PROTOCOL

Spanning Tree Protocol (STP) allows an Console Manager 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))

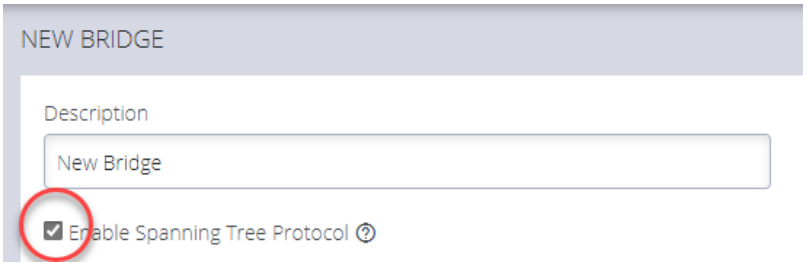
ENABLE STP IN A BRIDGE

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.



BRIDGE WITH STP ENABLED - OGCLI

```
admin@cm8148:~# 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"
```

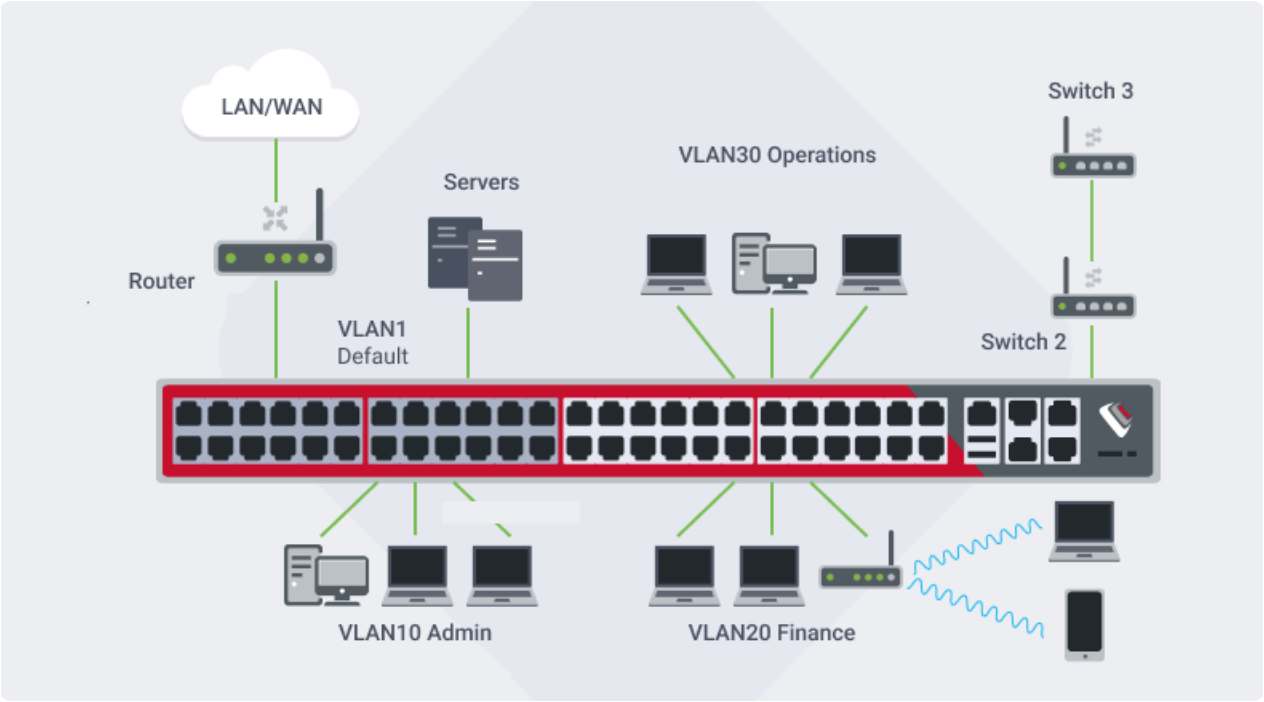
BRIDGE WITH STP DISABLED - OGCLI

```
admin@cm8148:~# 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"
```

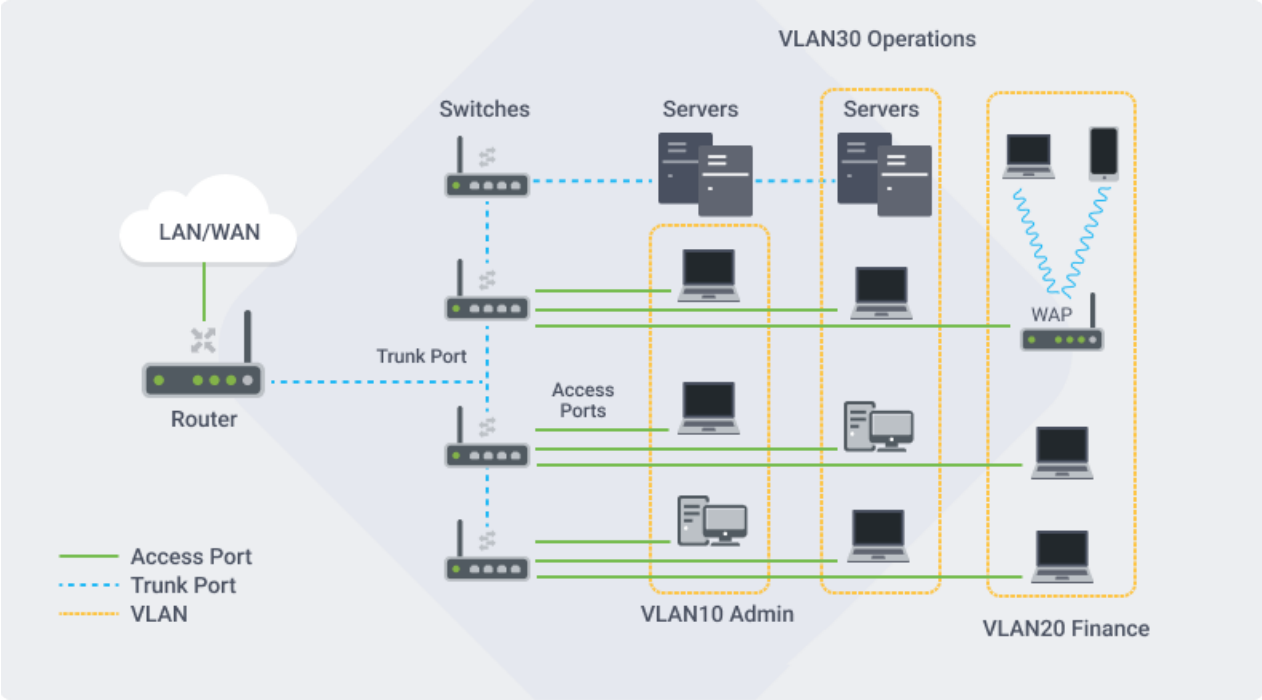
CONFIGURE A VLAN

The CM Series has flexible Ethernet capabilities, including support for VLANs. More specifically, it supports 802.1Q VLAN tagging to allow a trunked connection into an external switch or other device. It also supports the Linux logical "bridge group" feature which is the ability to group physical and virtual interfaces together. This can be used to group switch ports together, and to map physical switch ports into VLANs to create what are commonly referred to as "access ports" for those VLANs.

Picture a VLAN as a network that is usually segmented by function or application. VLANs behave much like physical LANs, but you can group hosts even if they are not physically co-located. A switch port can belong to a VLAN.



VLANs allow you to make separate broadcast domains on a switch. The broadcast domains can associate with one another with the help of a Layer 3 device such as a router. A VLAN is mainly used to form groups among the hosts regardless of where the hosts are physically located. In a bigger network, the configured VLANs with interfaces assigned as access and trunk ports on switches could look like this:



Switch Ports

For models with built-in switch ports, by default these are configured in a single bridge group called "Switch", which effectively puts all the switch ports into one virtual LAN or layer 2 broadcast domain. This default "Switch" bridge group can be deleted, and each of the switch ports is capable of being configured as a separate layer 3 interface with its own IP address. Alternatively, a number of switch ports can be grouped together using a bridge, to make a virtual LAN of any size. A bridge group can also include an 802.1Q VLAN interface (configured on a trunk port), effectively mapping the physical ports into that VLAN as "access ports".

IP Addressing

In order to communicate with an Ethernet interface, VLAN or bridge group, the CM must have a configured IP address on what is called a connection or "conn". This is similar in concept to a layer 3 subinterface or virtual interface on other networking equipment. The connection can be assigned to the bridge itself, or any of the members, including any physical (access) port or the 802.1Q VLAN, which makes the configuration quite flexible. For example, you can have a VLAN trunk with multiple 802.1Q VLANs, and each can be configured with a connection (IP Address information) so the CM appliance can communicate with other hosts on those VLANs. You can

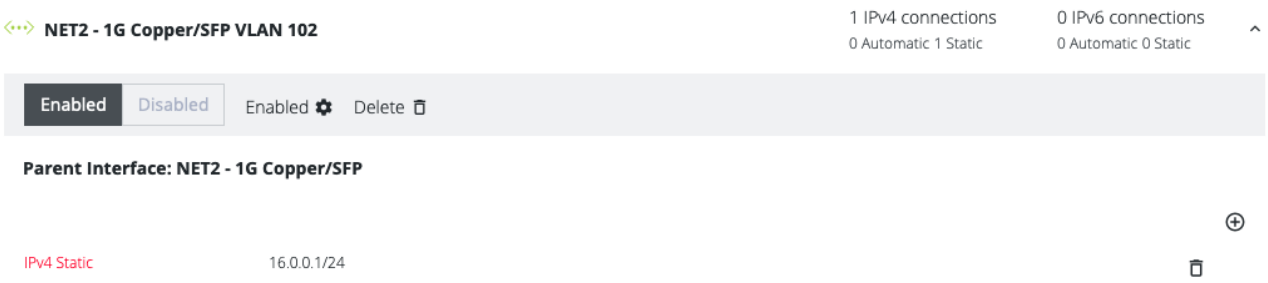
configure switch ports to operate individually, or in bridge groups (to make virtual LANs), and assign these IP addresses using a connection. You can combine these two by creating a bridge group that has an 802.1Q VLAN member and one or more switch ports, which become "access ports" to that VLAN.

Local VLANs

If the requirement is to just to group CM switch ports together into a "local" virtual LAN, but there is no requirement for a trunk, then this does not require a VLAN to be configured on the CM, you just require a bridge group, which behaves like a L2 virtual LAN. Create a new bridge group, assign the CM switch ports, and optionally create a new connection to add an IP address.

Navigate to Configure > Network Connections > Network Interfaces, then click on the New Bridge icon to create a new bridge group. Give this a name, then select the Switch Port(s) that you want to connect into this bridge group (local VLAN). Hit Create and the bridge group is created.

The following example shows VLAN 102 on the NET2 trunk port, with 16.0.0.1 address assigned:



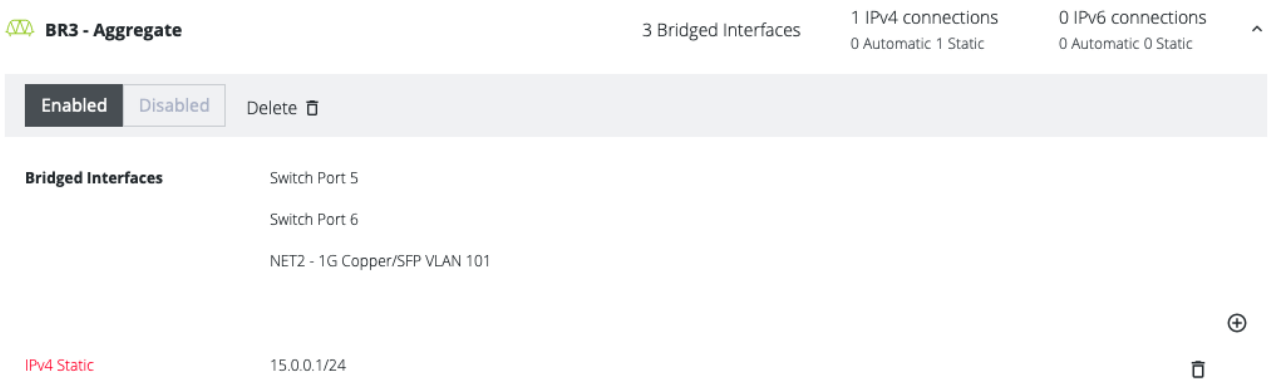
Configure CM Switch Ports as VLAN access ports (untagged ports)

To map the CM switch ports as "Access Ports" into a trunked VLAN, the CM uses a Bridge Group to join the switch port(s) to the same Layer 2 bridge domain as the VLAN subinterface, effectively bridging them together.

If the CM switch ports are still in the default "Switch" bridge group, you can delete or leave in place the "Switch" bridge group. Then you can assign some of the switch ports into new bridge group(s).

Go to Configure > Network Connections > Network Interfaces ... then click on the New Bridge icon to create a new bridge group. Give this a name, then select the Switch Port(s) that you want to connect into this bridge group (VLAN), and finally select the VLAN subinterface that you created on the Trunk port, e.g. NET2 - VLAN 22. Hit Create and the bridge group is created.

The following example shows bridge group BR3 with switch ports 5 and 6 bridged into VLAN 101 on the NET2 trunk. Switch ports 5 and 6 are now effectively untagged VLAN ports since the VLAN 101 trunk port NET2 is now in the same bridge group BR3. The subinterface NET2/VLAN101 is a 802.1Q tagged port. Note that the CM has a static IP address of 15.0.0.1 on this bridge group (VLAN).



IPSEC TUNNELS

The Opengear Console Manager (CM) 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 CM can both initiate tunnels (as the "initiator") and have other devices initiate tunnels to it (as a "responder").

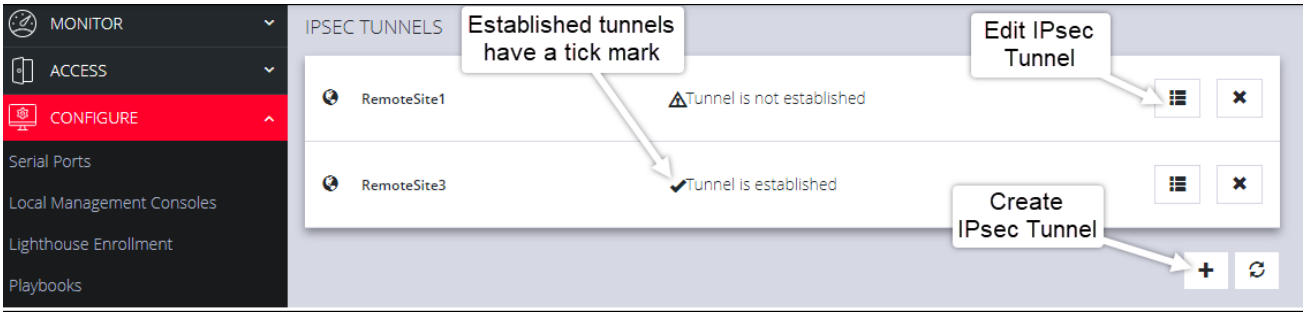
CREATE, ADD OR EDIT IPSEC TUNNELS

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 displays:*

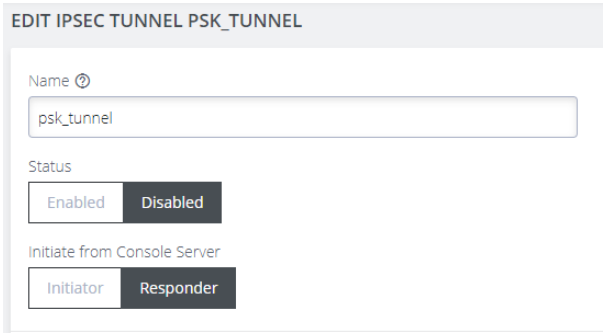


2. Click **CREATE TUNNEL**.

   This **EDIT IPSEC TUNNEL** page displays.

3. Configure the **Name** and **Status** settings:

   a. In the **Name** section of the page, give your new tunnel a unique name and set the **Status** to **Enabled**.

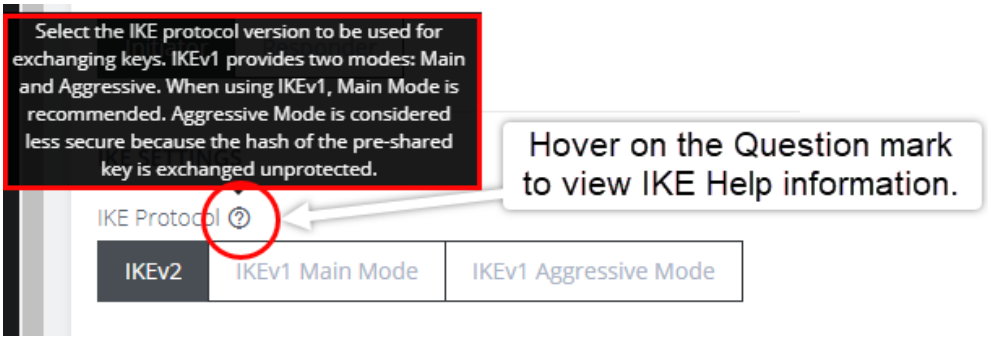


b. Set the Console Server to be the **Initiator** or **Responder**.

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

4. Configure the **IKE Settings**:

a. 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.



b. Select the **Algorithm Proposal**. This is a set of algorithms used for negotiation when attempting to establish the IPsec tunnel. By default, the node 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.

c. Select **Initiate** to actively initiate the tunnel by sending IKE negotiation packets to the remote end.

d. Set up the **Phase 1** and **Phase 2** time interval between the key material refresh of the IKE and Child.

5. Configure the **Authentication**:
CM Authentication can use PSK or PKI.

a. **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.

b. 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.

c. **For Public Key Infrastructure (PKI) authentication**, upload the certification bundle file or drag and drop the file into the Certificate Bundle field.

6. Configure the **Tunnel Settings**:

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

7. Configure the **Addressing**:

a. Enter the **Local Address** to be used as the source address of the tunnel.
If left blank, IPsec automatically uses a default.

b. Enter a **Local Subnet**.
Specify local traffic to be tunneled. When no subnets are specified, only traffic originating from this device is tunneled.

c. Enter the **Remote Address** or hostname for the remote end of the tunnel.
If left blank, IPsec accepts initiation packets from any address.

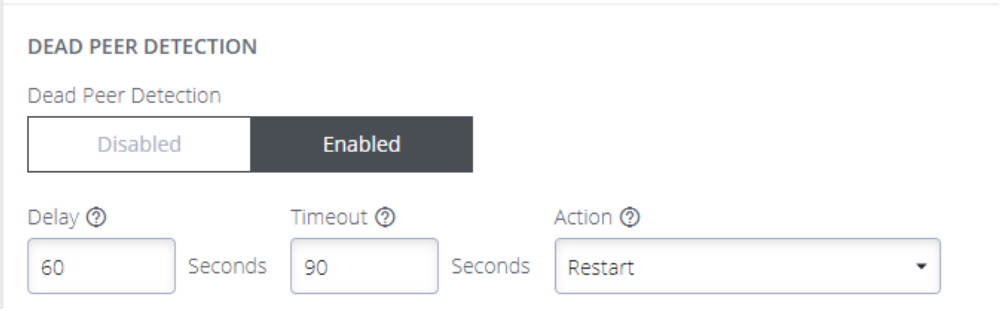
d. Enter the **Remote Subnet**.
Specify addresses or subnets that are behind the remote end of this tunnel. If no subnet is specified, only traffic originating from the outer remote address is accepted.

8. Configure **Dead Peer Detection**:

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

Dead Peer Detection (DPD) is a method used by nodes to verify the current existence and availability of IPsec peers. A node 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.

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



- **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** immediately attempts to renegotiate the tunnel.
  - **Clear** closes the CHILD_SA.
  - **Trap** catches matching traffic.

9. 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

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 displays 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.

For more information, see:

- Create a static route
- Edit or delete a static route
- Manage static routes via Command Line

CREATE A STATIC ROUTE

On the **Static Routes** page, you can add 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.

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

Destination Address	Default Metric
IPv4	0
IPv6	1024

6. Click the **Apply** button to save the changes.
7. 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 displays.
   - If the route installed successfully, a green success banner displays.

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

EDIT OR DELETE A STATIC ROUTE

On the **Static Routes** page, you can 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.

EDIT A STATIC ROUTE

1. Navigate to **CONFIGURE > NETWORK CONNECTIONS > Static Routes**.
2. Click the description of the required static route in the list to access the **Edit** page.
3. Update the details of the static route.
4. Click **Apply** to save the changes.

DELETE A STATIC ROUTE

1. Navigate to **CONFIGURE > NETWORK CONNECTIONS > Static Routes**.
2. Click the description of the required static route in the list to access the **Edit** page.
3. Click the **Delete** button at the top-right of the page.
4. Click **Yes** to confirm the action.
   If the route was removed from the routing table as expected, a green success banner displays.

MANAGE STATIC ROUTES VIA COMMAND LINE

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

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

Description	Command
Display IPv4 installed routes	ip route
Display IPv6 installed routes	ip -6 route
Display all route information	ip route show table all
Show status of configured routes via ogcli	ogcli get monitor/static_routes/status
Get static route configuration via ogcli	ogcli get static_routes
Create static route via ogcli	ogcli create static_route << END destination_address="1.1.1.1" destination_netmask=32 gateway_address="1.1.1.1" interface="net1" metric=0 END

Description	Command
Update static route via ogcli	ogcli update static_route "1.1.1.1" << END interface="net2" metric=100 END
Delete static route via ogcli	ogcli delete static_route "1.1.1.1"

NETWORK RESILIENCE

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

OUT-OF-BAND FAILOVER

Out-Of-Band (OOB) Failover detects network disruption via the probe interface, and automatically activates a cellular or ethernet interface 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 node regularly pings this address, using the probe interface, to check for network connectivity.

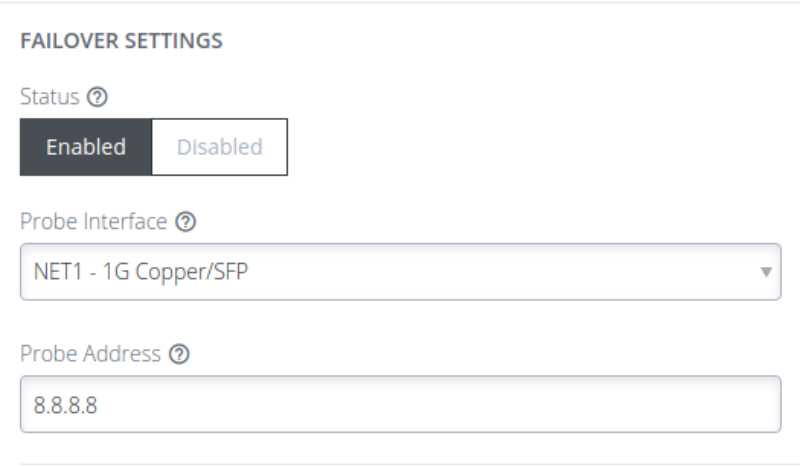
If you enable OOB failover:

- The system pings the probe address via the probe interface.
  If you have added a second probe address, only one of the two addresses needs to be reachable.

- When the probe interface comes up, the probe address is pinged every 30 seconds and sends three ping packets.
  If the first probe address fails, the second address is attempted, when means six ping packets are sent per 30 seconds.
- After four consecutive ping failures, OOB failover is triggered. This means a connection failure is detected after approximately two minutes.
- When failover is triggered, the pinging continues. If a ping succeeds, the system discontinues OOB failover. To help prevent interface flapping, the system does not do this until 60 seconds after OOB failover is triggered.
- If the prob interface does not come up, the ping test never runs and OOB failover is triggered after five minutes.

ENABLE OUT-OF-BAND FAILOVER

1. To manage out-of-band failover, navigate to the **CONFIGURE > NETWORK RESILIENCE > OOB Failover** page.



Probe Interface: this is the interface that is used to test if ping can reach the configured address.

Probe Address: the ipv4 or ipv6 or domain name of the address that is “pinged”.

2. In the **Failover Interface** section, select the failover interface from the drop-down list.

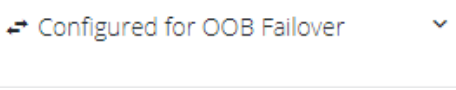


   Configurable probe (failover from) and failover (failover to) interfaces are shown:

   - **NET1** - the default probe interface.
   - **Cellular** - the default failover interface for cellular-capable models.
   - **NET2** - the default failover interface for non-cellular models.

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

4. On the **Network Interfaces** page, the Failover Interface displays "Configured for OOB Failover" beside the interface name.



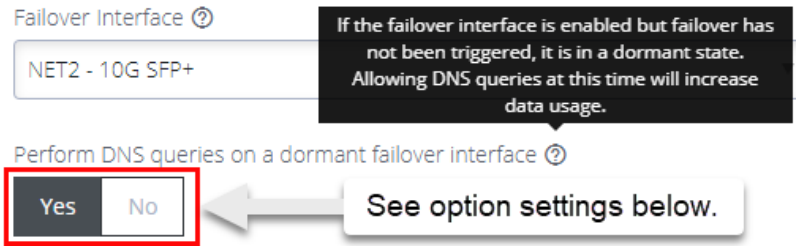
5. When failover is triggered, the interface is marked with the warning: **OOB Failover Active** to an Admin user when logged in.



> **Note:**
>
> - It may take up to five minutes for a failover to actually occur after the probe stops connecting to the probe address.
> - The shortcut button **Enabled/Disabled** is disabled or removed when an interface is in active failover.

DNS QUERIES ON A DORMANT FAILOVER INTERFACE

The Dormant DNS option allows DNS queries on the failover interface to be disabled in normal operation so that DNS queries can be paused.



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

- If set to **Yes**, the DNS name servers and search domains configured for the failover interface will always be available to the system for DNS name resolution. Allowing DNS queries while failover has not been triggered make it more likely that DNS requests are made over the cellular interface which increases data usage.
- If set to **No**, the DNS name servers and search domains are 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 370.

OOB FAILOVER TYPES & FAILOVER BEHAVIOR

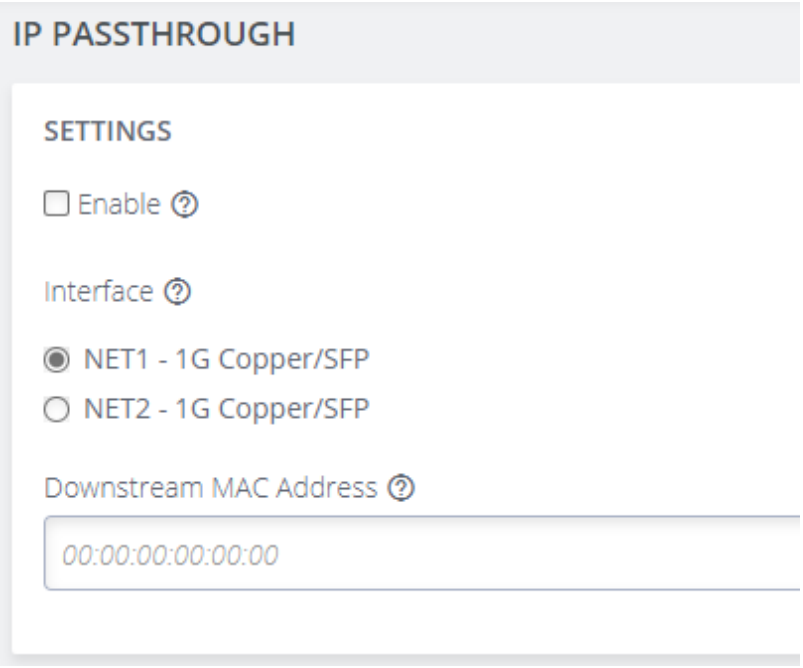
OOB Setting	Failover Interface	Mode	Description
Disabled	Enabled	Always up OOB	When OOB Failover is disabled, the default outgoing interface cannot be specified, the default route is selected automatically. Outbound network connections (e.g. VPN client tunnels, SNMP alerts) are established according to the main static routing table, regardless of network state.
Enabled	Disabled	Failover mode	Failover detection is enabled on the selected “probe” interface. The network or cellular interface remains in a down state with no network configuration. When failover is initiated, the network or cellular interface is started and configured. If a default route is installed on the 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 over network or cellular connection during failover. 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.

OOB Setting	Failover Interface	Mode	Description
Enabled	Enabled	Dormant failover	Failover detection is enabled. Only inbound connections on the network or cellular interface are routed back out the network or 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. When failover is initiated, the default route of the network or cellular interface takes precedence over the failed “probe” interface. Outbound network traffic (e.g. VPN client tunnels, SNMP alerts) are established or re-established over the network or cellular connection during failover. The advantage of this mode is the network or cellular connection is available for inbound out-of-band access during normal operation.

IP PASSTHROUGH

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

1. To manage **IP Passthrough**, navigate to the **CONFIGURE > NETWORK RESILIENCE > IP Passthrough** page.
2. Configure the IP Passthrough Settings:



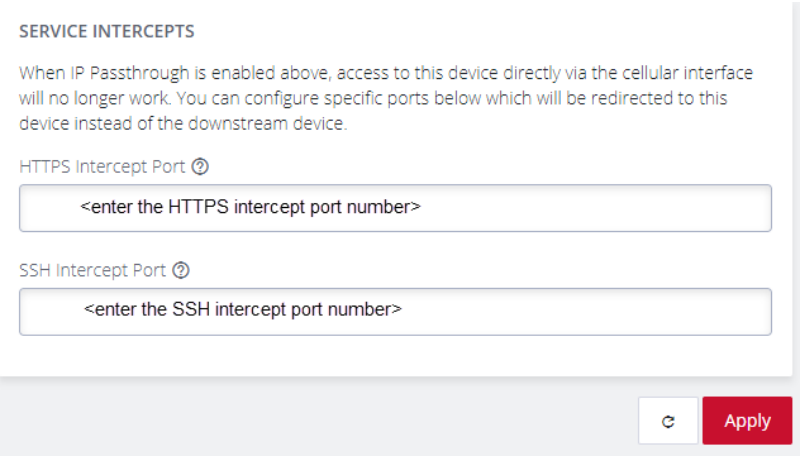
a. Click the IP Passthrough status checkbox to set the status to **Enabled**

b. From the dropdown selector, select the interface type that is used.

c. Enter the MAC address of the downstream device that will make the DHCP requests. The MAC address of the device is offered a DHCP lease. DHCP requests from other MAC addresses are ignored.

3. Configure the IP Passthrough Service Intercepts:

> **Tip:** When IP Passthrough is enabled, access to this node directly via the cellular interface no longer works. You can configure specific ports below which will be redirected to this node instead of the downstream device.



a. Enter the port number that is to be used for HTTPS Intercepts.

b. Enter a port to be redirected to this node's SSH service.

> **Tip:** You can use this port to access the Console Manager command line interface. If you leave this field blank, the SSH service intercept is disabled.

c. Under **Access Control**, enter the blocked and allowed addresses.

4. 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

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

Groups are used to grant privileges to users. When a user is a member of a group, defined privileges may be granted to the group by an Administrator. When editing a group, the (authorized) user selects from a list of devices, all of which are under the heading SERIALLY CONNECTED DEVICES.

PERMISSION CHANGES IN THE WEB UI

A new feature change called Access Rights was introduced in release 22.11 to replace the previous concept of a user *Role* and instead uses a set of configurable *Access Rights* for each group. Each access right governs access to a particular feature (or set of highly related features), with a user only having access to features for which they have an assigned access right.

> **Tip:** To support the new permissions model several rest API endpoints have been updated for the new functionality. Wherever possible, these changes are backwards compatible. See the release notes for details.

UNDERSTAND ACCESS RIGHTS

An access right is a permit authorizing access to a feature or collection of related features. Holders of the permit (i.e., the access right) are given access to the feature.

A user gains access rights by the following:

- Access Rights are assigned to Groups.
- Users are members of zero or more Groups.
- A User inherits all Access Rights from all the Groups they are a member of.

Some features may require the user to hold multiple access rights to access the feature through a specific interface. For example, a user requires the “right to use the web UI” and the “right to configure serial ports” to make configuration changes to a serial port through the web UI.

DEFINED ACCESS RIGHTS

There are four *defined* rights (admin, web_ui, pmshell, and port_config) as summarized in the following table.

Access Rights	Description
admin	The admin access right grants a holder access to everything; every feature and every user interface.
web_ui	Permits access for an authenticated user to basic status information via the web interface and rest API. Users can: • Make requests to the subset of endpoints that provide this same information. In both cases the user must be authenticated. • See information about their own user and groups. • See serial port status information for the specific ports to which the user is granted access.
pmshell Restricted CLI	Permits access to devices connected to serial ports. Does not give permission to configure all serial ports, only to those that are added to the same group containing the pmshell rights.
Port Config	Permits access to configure serial ports. This access right gives the holder the ability to configure serial ports. This right does not give the holder the ability to access the serial port.

Tip: A right may be combined with another right for a feature to be accessible by a user. For example, `web_ui` to log in and port_config to configure a serial port. The `port_config` right by itself is not useful.

ADMIN ACCESS RIGHTS (`ADMIN`)

Any user who was previously an `Administrator` role now inherits the `admin` access right, giving that user the same “can do everything” permission.

Tip: The **Admin Access** toggle switch in the Web UI hides other rights selections as Admin Access overrides all other rights.

WEBUI ACCESS RIGHTS (`WEB_UI`)

Any user who was previously a Console User role now inherits the `web_ui` and `pmshell` access rights and there are no functional changes for this user.

> **Tip:** From release 22.11 in the Web UI, the **Rights** checkbox replaces the **Roles** drop-down selection.

The `web_ui` access right grants the user the ability to

- log into the WebUI.
- see a listing of serial ports (The “Access → Serial Ports” menu item).
- edit a restricted set of user configuration such as changing their own password.

PORTMANAGER SHELL ACCESS RIGHTS (`PMSHELL`)

Any user who was previously a Console User role now inherits the `pmshell` access rights and there are no functional changes for this user.

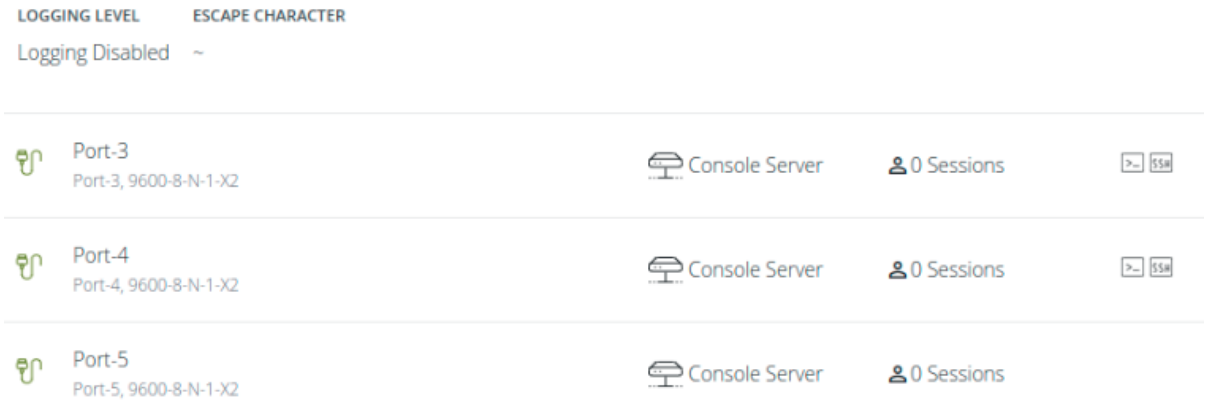
The `pmshell` access right grants the user access to the serial port web terminals and the ability to use `pmshell` over SSH. These rights are applied only to the access ports to which they have been granted rights.

PORT CONFIGURATION ACCESS RIGHTS

The `port_config` access right grants the holder of this right the ability to make configuration changes to the serial ports they have been assigned. Note that a user without the `web_ui` right cannot log in to the WebUI to configure serial ports, so a user must inherit the `web_ui` from at least one group.

ACCESS > SERIAL PORTS VIEW

Users with the `port_config` access right to some serial ports are able to see the **Edit** link on the **Access > Serial Ports** page for those ports only. Non-Admin users with the `port_config` role are able to see any active sessions on a port but are not able to terminate the session.



CONFIGURE > SERIAL PORTS VIEW

The Configure Serial Ports page is accessible to users with the `port_config` and `web_ui` access rights appear in the navigation sidebar menu. This page lists ports that the user has both `port_config` and `web_ui` access rights.

> **Tip:** It is possible to edit all details on these ports, however, changing the “mode” of a port disconnects any sessions.

NON-ADMIN USERS

Non-admin users with `port_config` access right are able to perform Serial Port Autodiscovery on the ports that they are able to configure. If autodiscovery is already running, they can see the banner but cannot view the autodiscovery logs or cancel the running job. Non-admin users are not able to configure the Serial Port Autodiscovery Schedule and the icon is hidden, but are able to see which ports are configured of the ports to which they have access.

PROTECTED GROUPS AND USERS

Certain types of groups and users have protected status, meaning that they cannot be changed or deleted. Protected groups comprise the following:

- `root` - The root user is hard-coded member of the Admin group. As such, the root user cannot be deleted.
- `admin` - The Admin group cannot be disabled or changed to a non-admin group.
- `netgrp` - The special ‘netgrp’ also cannot be deleted. This group is assigned to users from AAA auth that don’t have a group assigned from the authentication server.

> **Tip:** For these protected groups no 'Delete' button displays beside them in the Web UI.

UNDERSTAND SERIAL PORT ACCESS

Serial ports are assigned to a group in the same way as access rights are assigned to a group, however, it is the access rights that are assigned to the same group that determine what a user can actually do with those serial ports. The access rights assigned to one group will only apply to the serial ports assigned to that same group, they do not apply to the serial ports of another group.

For example, a user in a group with `port_config` and `port-01` can configure that port but not access the device (as that requires `pmshell` access rights).

Consider the following two groups, *Accounts Admin* and *Port #03 User*:

Group Name	Accounts Admin	Port #03 User
Access Rights	`port_config` `web_ui`	`pmshell` `web_ui`
Serial Ports	`port-01` `port-02`	`port-03`

The effective rights for a user in one or both of those groups is shown in the following table. It shows how access rights assigned to one group will only apply to the serial ports assigned to that same group:

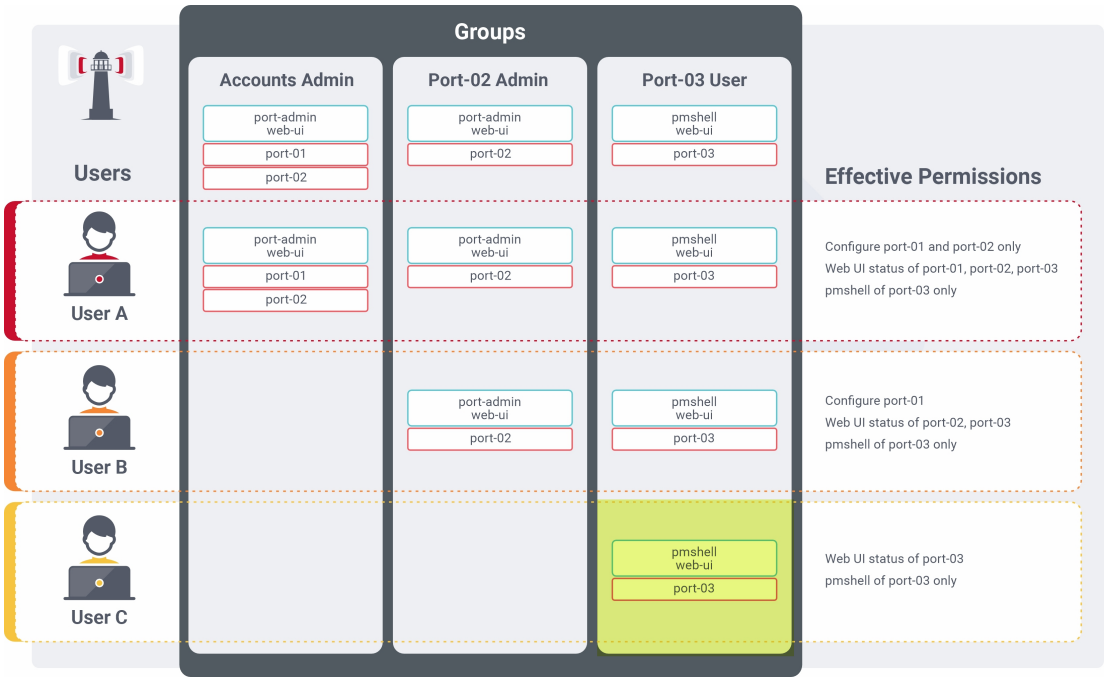
The following table shows the effective rights for a user in one or both of those groups, *Accounts Admin* and *Port #03 User*:

Action	*Group Membership*		
	Accounts Admin	*Port #03 User*	*Accounts Admin & Port #03 User*
Configure `port-01`	✓	✗	✓
Configure `port-02`	✓	✗	✓
Configure `port-03`	✗	✗	✗
Access `port-01`	✗	✗	✗

Action	*Group Membership*		
	Accounts Admin	*Port #03 User*	*Accounts Admin & Port #03 User*
Access `port-02`	✗	✗	✗
Access `port-03`	✗	✓	✓

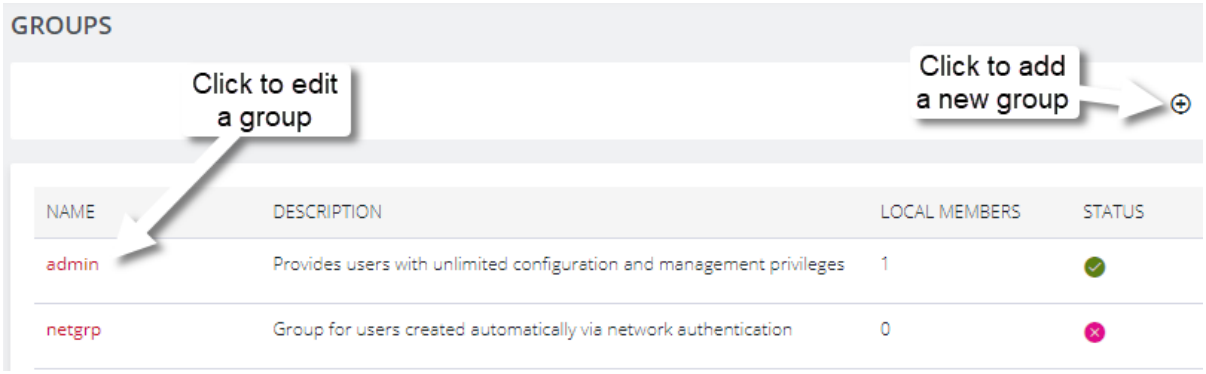
Note: Note the highlighted cell; a user with `pmshell` access to `port-03` (from the *Port #03* user group) does not also get `port_config` for that port, even though that access right is inherited from the *Accounts Admin* group. The access rights of a group *only apply to the serial ports in that same group*. This principle is illustrated in the following figure:

The following image shows how access rights assigned to one group only apply to the serial ports assigned to that same group.



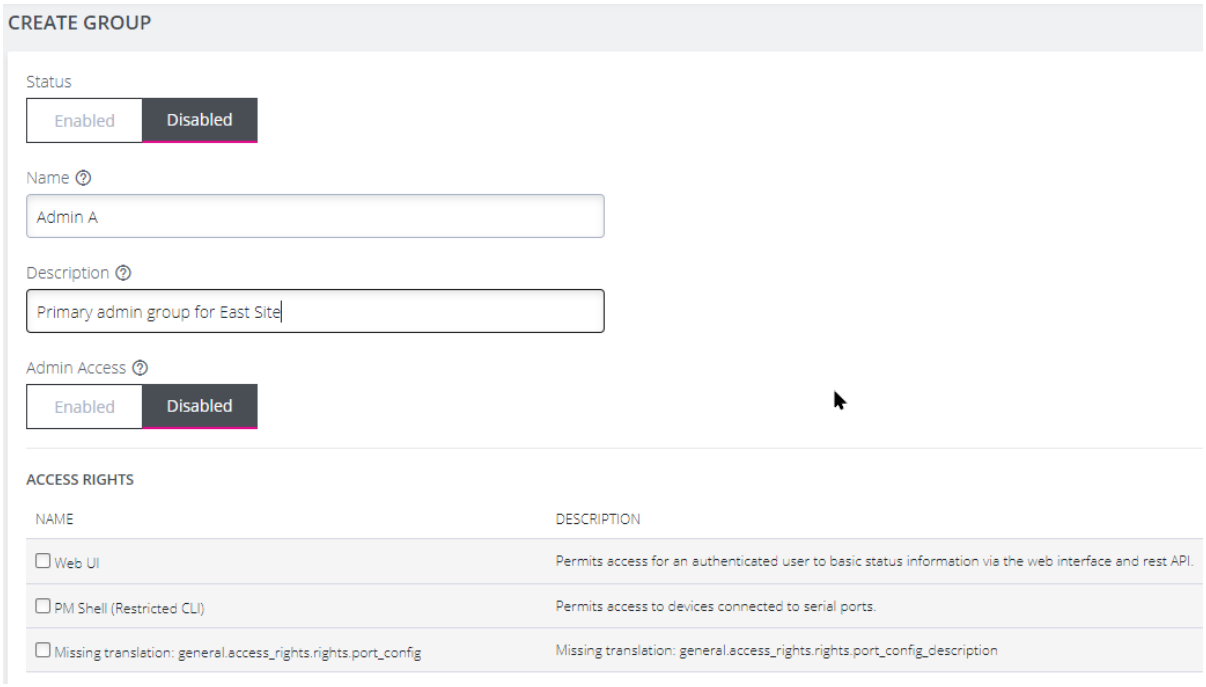
CREATE A NEW GROUP

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



⊕	Add a new group.
admin	Click on the group name to edit an existing group.
Status Enabled Disabled	In the EDIT GROUP window - Enable/Disable an existing group.
Admin Access ⓘ Enabled Disabled	Grant administrative access rights and full control of this console, and all attached devices, to all users of this group.
🗑	Delete a group (or delete selected groups).

2. Click the **Add New Group** button.
   The **CREATE GROUP** page displays.



3. Enter a **Group Name**, **Description**, and set **Admin Access** to **Enabled** or **Disabled**. Specific access rights can be selected in the ACCESS RIGHTS area.

   Notes:

   - **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.
   - If **Admin Acess** is Enabled, members of the group will have full access to and control of selected managed devices, and the rights that are selected under **ACCESS RIGHTS** for that group.

4. Select the applicable **Access Rights** for the group.
5. If the new group is to be activated immediately, set the group Status to **Enabled**.
6. Click the **Submit** button to save the group.
   After creation, group **Status** and **Admin Access** may be enabled or disabled from the **CONFIGURE > USER MANAGEMENT > Groups > EDIT GROUP** page.

EDIT AN EXISTING GROUP

1. Select **CONFIGURE > USER MANAGEMENT > Groups**.
2. Click on the name of the group to modify and make the required changes.
3. Click **Submit** to save the changes

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.

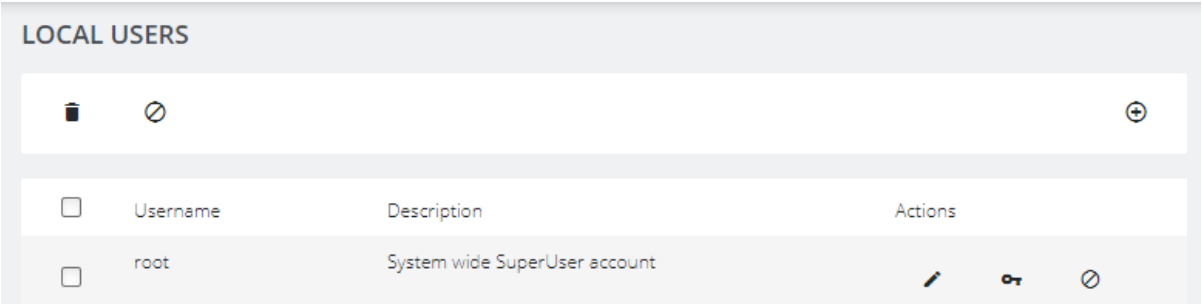
> **Notes:**
>
> - The netgrp group is inherited as the primary group for all remote AAA users who are not defined locally. By default, netgrp has the Administrator role and is disabled. It must be enabled to take effect for remote AAA users.
> - For users that don't have any group, they are still part 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 Administrator already, so setting "console user" in netgrp does not matter.

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 console user).
- Accessible ports.



The button action definitions are described in the following table:

	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 selected users.

CREATE A NEW USER WITH PASSWORD

Notes:

- Users are prevented from using the word “default” as their password. The factory default password automatically expires after a factory reset and users must choose a new password. This password policy applies to the WebUI, Config Shell and CLI. users configured on the system using software versions prior to 23.10 with password “default” are forced to change the user password to something other than “default” after upgrading to 23.10. This password feature update applies to configured boxes with existing users, not just factory defaulted software.
- Passwords must comply with your company's password complexity policy, see Local Password Policy.

1. Navigate to the **CONFIGURE > USER MANAGEMENT > Local Users** page.
2. Click the **Add User** ⊕ button.

   The **New User** dialog displays.
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 confirms that the data is saved.

CREATE A NEW USER WITH NO PASSWORD (REMOTE AUTHENTICATION)

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 **Mode**.
3. Enter the settings and click **Apply**.

4. Select **CONFIGURE > USER MANAGEMENT > Local Users**.
5. Click the **Add User** button.
   The **New User** dialog displays.
6. Enter a **Username**, **Description**.
7. Select the **Remote Password Only** checkbox.
8. Select the **Enabled** checkbox.
9. Click **Apply**.
   A banner confirms that the data is 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 confirms the changes are saved.

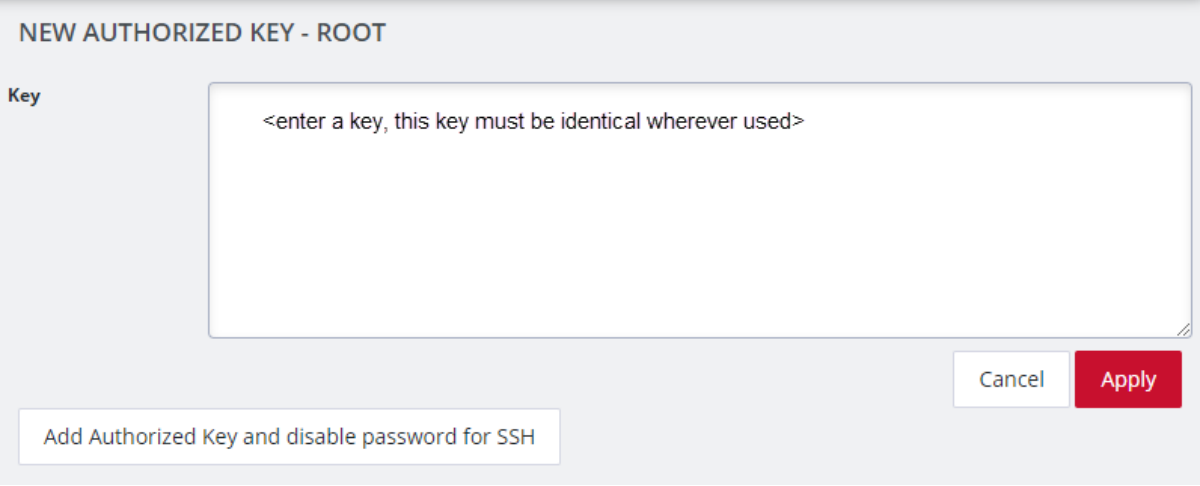
The **Edit Users** dialog allows the user's **Description** to be changed, **Group Memberships** modified, and the user's **Password** to be reset. The username cannot be changed. To disable a user, uncheck the **Enabled** checkbox.

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

MANAGE SSH AUTHORIZED KEYS FOR A USER ACCOUNT

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 want to remove.

DELETE A USER ACCOUNT

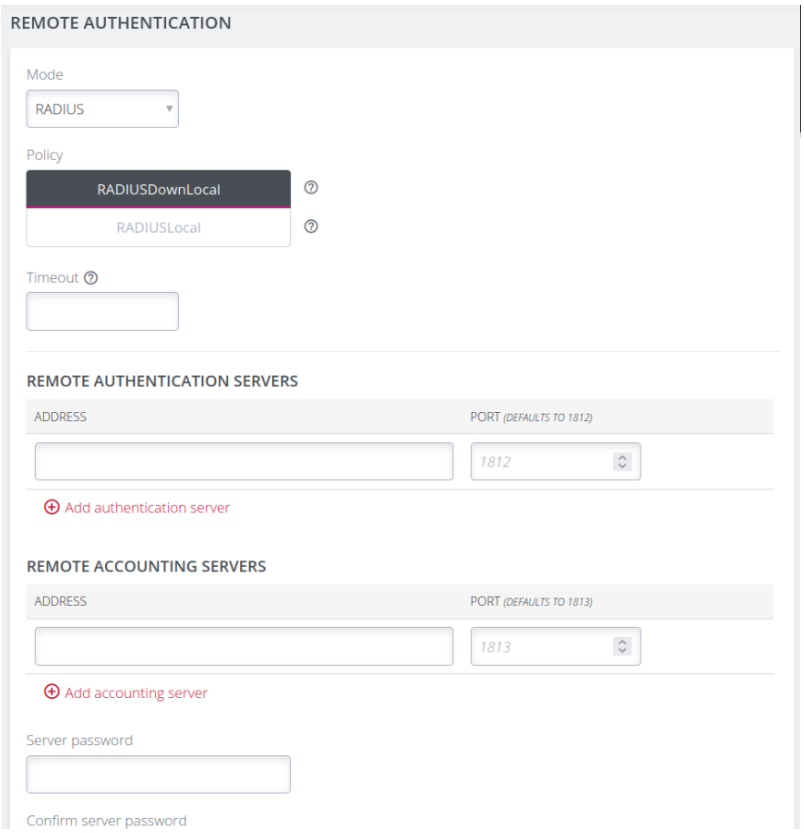
1. Select **CONFIGURE > USER MANAGEMENT > Local Users**
2. Click the **Delete User** button in the **Actions** section next to the user you want to delete.
3. Click **Yes** in the **Confirmation** dialog.

REMOTE AUTHENTICATION

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

- Configure RADIUS Authentication
- Configure TACACS+ Authentication
- Configure LDAP Authentication

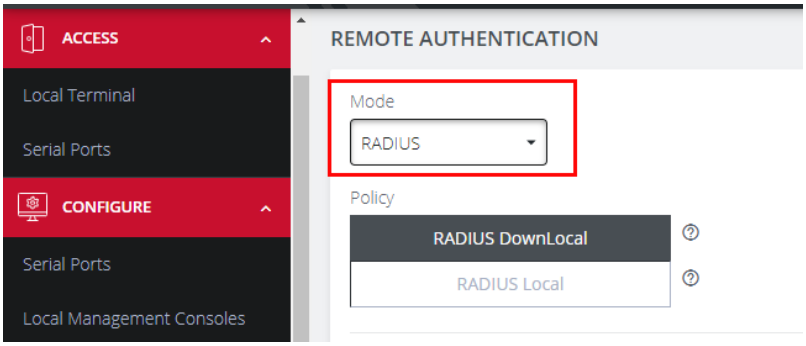
Navigate to **CONFIGURE > USER MANAGEMENT > Remote Authentication**. The Remote Authentication Home page displays.



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**: Users are authenticated through their local account only if the remote AAA server is unreachable or down. If the credentials provided at log in are incorrect or if the account does not exist on the remote server, the user is denied access.
   - **Radius Local**: If remote authentication fails because the user account does not exist on the remote AAA server, the CM attempts to authenticate the user using a local account as per a regular local log in.
3. Enter the authentication **Timeout** value to apply.
   The timeout value specifies the number of seconds to wait for a response from the server before trying the next server.

   > **Note:** The timeout value is global and applied to all authentication methods when you set the value on one authentication method.

4. Add the **Address** and optionally the **Port** of the authentication server.
5. Add the **Address** and optionally the **Port** of the RADIUS accounting server.
6. Select whether **Message-Authenticator** is required for server responses.
   The default setting is **Do not require Message-Authenticator**. If the default setting is left, RADIUS responses may be subject to BlastRADIUS attack.

7. Add and confirm the **Server password,** also known as the RADIUS Secret.
8. Select the preferred **Radius Server Authentication** method to apply.

> **Note:** The method defaults to PAP if not configured. Ensure that the selected method is supported by the remote server.

9. Click **Apply**.

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

To provide group membership, RADIUS must 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 **Mode** drop-down menu.
2. Select the preferred TACACS+ Remote Authentication policy to be applied:
   - **TACACS+ DownLocal**: Users are authenticated through their local account only if the remote AAA server is unreachable or down. If the credentials provided at log in are incorrect or if the account does not exist on the remote server, the user is denied access.
   - **TACACS+ Local**: If remote authentication fails because the user account does not exist on the remote AAA server, the CM attempts to authenticate the user using a local account as per a regular local log in.

3. Enter the authentication **Timeout** value to apply.
   The timeout value specifies the number of seconds to wait for a response from the server before trying the next server.

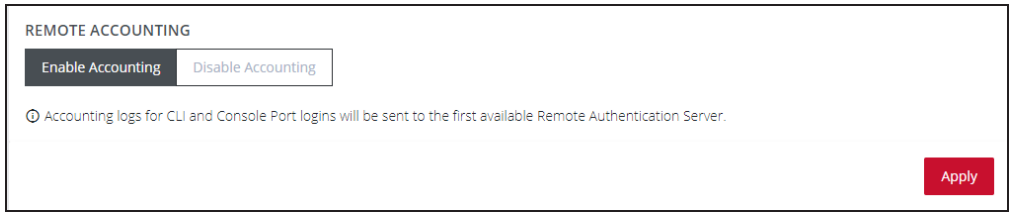
   > **Note:** The timeout value is global and applied to all authentication methods when you set the value on one authentication method.

4. Add the **Address** and optionally the **Port** of the TACACS+ authentication server to query.
5. Select the **Log in Method**. **PAP** is the default method. However, if the server uses DES-encrypted passwords, select **Login**.
6. Add and confirm the **Server password**, also known as the TACACS+ Secret.
7. 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
       }
   }
   ```

8. Enable or Disable **Remote Accounting**.
   TACACS Accounting is enabled by default, the Remote Auth Server is used as the Accounting server. However, one or more Accounting Servers can be specified.
   a. To disable Remote Accounting, select **Disable**
   b. To enable Remote Accounting, select **Enable**.



9. Click **Apply.**

> **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**: Users are authenticated through their local account only if the remote AAA server is unreachable or down. If the credentials provided at log in are incorrect or if the account does not exist on the remote server, the user is denied access.
   - **LDAP Local**: If remote authentication fails because the user account does not exist on the remote AAA server, the CM will attempt to authenticate the user using a local account as per a regular local log in.
2. Enter the authentication **Timeout** value to apply.
   The timeout value specifies the number of seconds to wait for a response from the server before trying the next server.

   > **Note:** The timeout value is global and applied to all authentication methods when you set the value on one authentication method.
3. Add the **Address** and optionally the **Port** of the LDAP server to query. See the LDAP and LDAPS Port Settings topic.
4. 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
   ```

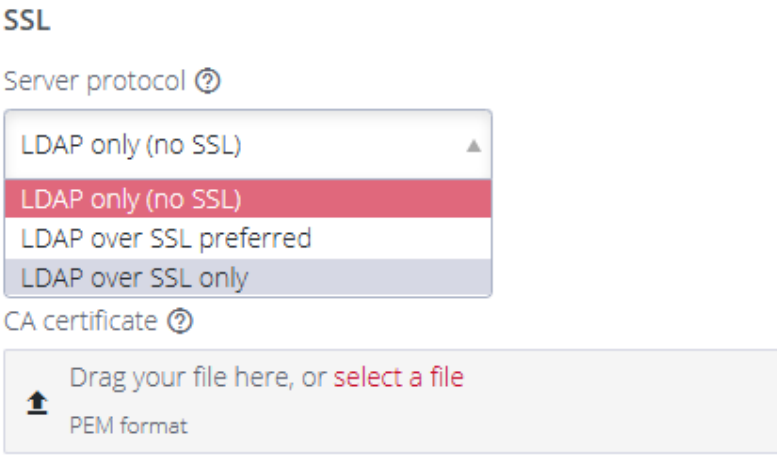
4. Add the **LDAP Bind DN**. This is the distinguished name of a user with privileges on the LDAP system to perform the lookups required for retrieving the username of the users, and a list of the groups they are members of.

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 required for Active Directory and is generally memberOf.
8. If required, 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.

CONFIGURE LDAP OVER SSL

1. Complete the LDAP Authentication configuration as per Configure LDAP Authentication.
2. At the SSL section of the LDAP page select the required server protocol:



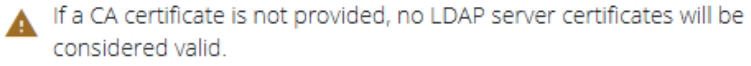
> **Note:** The default setting is LDAP only.
> Selecting 'LDAP over SSL uses the ldaps://server.
> Selecting 'LDAP over SSL preferred' uses both ldaps://server and ldap://server.

3. Provide a CA Certificate by dragging the CA Cert file into the CA certificate drop box.
   By default the LDAP server's CA certificate is verified.

4. If a CA certificate is not provided, certificate verification can be disabled by selecting the **Ignore SSL certificate errors** checkbox.

   > **Note:** Ignore SSL Certificate Errors also prevents some other SSL-related certificate errors.

   A warning displays if no CA Certificate is present and the **Ignore SSL certificate errors** checkbox is not selected. In this case no LDAP server certificates are considered valid:

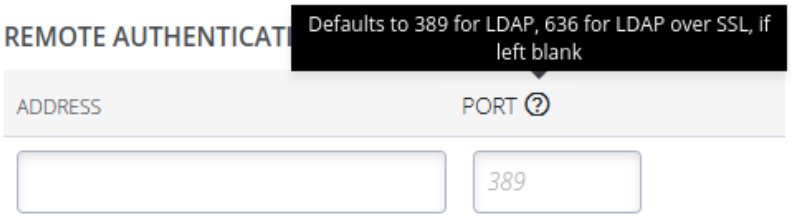
   

   > **Note:** The CA Certificate filename is correct when the certificate is initially uploaded. The filename is not maintained or stored, if the page is later revisited the filename is always shown as “cacert.pem”.

5. Click **Apply** to load and apply your settings.

LDAP AND LDAPS PORT SETTINGS

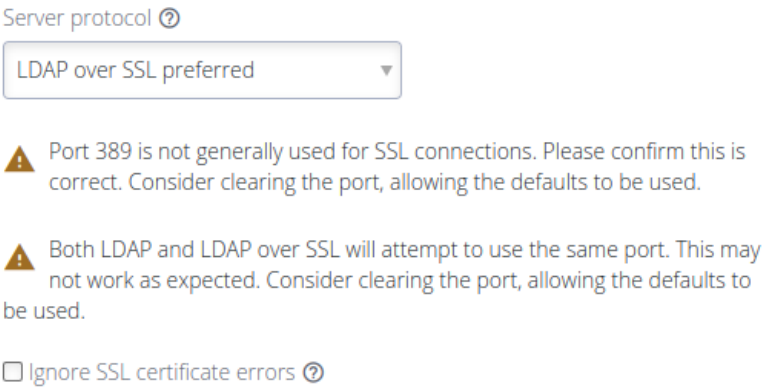
The default ports for LDAP and LDAPS are:
LDAP: Port 389
LDAPS: Port 636



Port selection warning messages:

- If port 389 has been set and LDAP over SSL is enabled, a warning is shown.
- If any port has been set and LDAP over SSL is preferred, a warning is shown.
- Setting LDAP over SSL preferred and port 389 results in both warnings being shown.

See the warning messages below:



LIMITATIONS FOR LDAPS IMPLEMENTATION

Previously, the port for LDAP servers had a default value. When upgrading, this port is not cleared. When enabling LDAP over SSL, it may be necessary to clear the port so that the LDAP over SSL default port can be used.

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:

- Enforces the use of complex passwords to improve security, see Set Password Complexity Requirements.
- Schedules expiry of passwords to enforce regular password updates, see Set Password Expiration Interval.

By default, the following settings are applied to passwords:

- Minimum length of eight characters.
- Must contain one uppercase letter.

- Must contain one number.
- Cannot contain usernames.

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 WebUI, REST API, and ogcli. The password policy also applies to underlying CLI tools.

SET PASSWORD COMPLEXITY REQUIREMENTS

Notes:

- Some password complexity rules are required, other rules are optional. Optional rules can be selected by clicking on the relevant checkbox.
- Users are prevented from using the word “default” as their password. The factory default password automatically expires after a factory reset and users must choose a new password. This password policy applies to the WebUI, Config Shell and CLI. users configured on the system using software versions prior to 23.10 with password “default” are forced to change the user password to something other than “default” after upgrading to 23.10. This password feature update applies to configured boxes with existing users, not just factory defaulted software.
- See also Password Policy Implementation Rules.

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). By default, this is set to a minimum password length of 8 characters.
- Must contain an upper case letter (optional). This is selected by default.
- Must contain a numeric character (optional). This is selected by default.
- Must contain a special character (non-alphanumeric e.g. #,$,%).
- Disallow usernames in passwords (optional). This is selected by default.

See Password Policy Implementation Rules.

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

SET PASSWORD EXPIRATION INTERVAL

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 displays at login.

See also Password Policy Implementation Rules.

> **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. Enter a number to represent the required 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 is applied from when the password was initially set by the user. If a password falls outside the new expiry period, the user is 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 *madam* or *racecar*).
	The minimum length (enforced) must be at least 8 characters (this requirement cannot be disabled except by disabling password complexity entirely). This setting is enabled by default.
	The password should contain at least one upper case alphabetic character (enabled or disabled separately). This setting is enabled by default.

Rule	Policy
	The password must contain at least one numeric character (enabled/disabled separately). This setting is enabled by default.
	The password should contain at least one special character (e.g. #,$,%) (enabled/disabled separately).
	The password cannot contain your username. This setting is enabled by default.
	Complexity requirements will apply when a user next tries to update their password.
	An Administrator can force the expiry of a user's password by running the ogcli command: `passwd --expire {username}` to force a user to change their password.
	The operations `ogadduser`, `ogpasswd` and `ogsshaddsshkey` have been removed. You should instead use ogcli for these operations.

SERVICES

The **CONFIGURE > SERVICES** menu lets you manage services that work with the Console Manager.

FIPS COMPLIANCE

The Federal Information Processing Standard Publication 140-2 (FIPS 140-2) is a U.S. government computer security standard that is used to approve cryptographic modules. Opengear appliances operating in FIPS mode provide FIPS 140-2 level one compliance by utilizing FIPS validated OpenSSL 3.0.8 cryptographic library while in FIPS mode.

> **Note:** The default provider is 3.0.10, however, the FIPS provider remains on 3.0.8 in release 23.10.4. See the example of list providers in Verify that FIPS is enabled.

For more information, see:

- Considerations for using the FIPS feature
- Enable FIPS at the CLI
- Disable FIPS
- Verify that FIPS is enabled

CONSIDERATIONS FOR USING THE FIPS FEATURE

In organizations where FIPS is required, the following points should be noted:

- OpenSSL 3.0.8 FIPS provider limits the available cryptography ciphers/algorithms only those that have been validated by laboratory to be FIPS compliant.

- Configuration backup should be taken before enabling or disabling FIPS.
- FIPS has the potential to break any service with secure connectivity, including services listed in the following table:

Feature	Affected Process/Service	Impact
Lighthouse enrollment	OpenVPN	OpenVPN is not compliant with FIPS standards; this issue is a recognized problem specifically when OpenSSL 3.x is being used. When OpenVPN addresses this issue, it will also meet FIPS compliance standards. However, for compatibility with Lighthouse enrollment, this feature remains enabled although it is non-compliant.
IPsec	Strongswan	Must be operated in FIPS mode to be FIPS compliant. The other end of the tunnel does not have to be operating FIPS mode to connect.
Remote authentication	freeradius, tacacs, ldap	These are not FIPS compliant.

Feature	Affected Process/Service	Impact
NTP	chrony	Authenticated NTP servers with MD5 will not connect. Use an algorithm that is FIPS compliant.
SNMP	ogtrapd, snmpd, snmptrapd	Authentication and Encryption should be used as the security policy as V1 and V2 have no encryption. SNMPv3 with MD5 encryption will fail. Use an algorithm that is FIPS compliant. It is recommended that authPriv security policy is used when in FIPS mode for SNMPv3.
LDAP	OpenSSL	LDAP has no encryption, therefore it does not use OpenSSL. For FIPS compliance it is recommended that it is not used.
OpenSSL	OpenSSL MD5	When OpenSSL MD5 is not available, pam_tacplus uses its own implementation of MD5. When FIPS is enabled it does not use OpenSSL (but will continue to work). Therefore, it is recommended that it is not used in FIPS mode.
SMF	SMF	Use of the SMF feature will render the device non-compliant for FIPS.
SSH connections	SSH	For SSH connections, a FIPS compliant algorithm must specified as part of the command to connect. See the note below:
NetOps Modules	gre (Secure Provisioning) nom-ipaccess-lhvpn (IP access) nom-ag-lhvpn (Access Gateway)	Opengear NetOps Modules are not functional when FIPS mode is enabled.
Note: SSH requires the cipher to be manually specified when FIPS is enabled. e.g. ssh root@10.0.0.1 -c aes256-gcm@openssh.com		

Feature	Affected Process/Service	Impact
WireGuard		WireGuard is not FIPS compliant and should not be used in FIPS mode.
Routing protocols		Routing protocols (eg. BGP), should not select an MD5 cipher.

ENABLE FIPS MODE AT THE CLI

ENABLE FIPS VIA CONFIG SHELL

```
root@<device name>:~# config
Welcome to the Opengear interactive config shell. Type ? or help for help.
config: system/fips
config(system/fips): enabled true
config(system/fips): apply
Updating entity system/fips.
```

ENABLE FIPS VIA OGCLI

```
ogcli update system/fips enabled=true
```

DISABLE FIPS

DISABLE FIPS VIA CONFIG SHELL

```
root@<device name>:~# config
Welcome to the Opengear interactive config shell. Type ? or help for help.
config: system/fips
config(system/fips): enabled false
config(system/fips): apply
Updating entity system/fips.
```

DISABLE FIPS VIA OGCLI

```
ogcli update system/fips enabled=false
```

VERIFY THAT FIPS IS ENABLED

1. Check the OpenSSL FIPS providers.

```
root@<device name>:~# openssl list -providers
Providers:
 default
  name: OpenSSL Default Provider
  version: 3.0.10
  status: active
 fips
  name: OpenSSL FIPS Provider
  version: 3.0.8
  status: active
```

2. Check that the digest algorithms provided by OpenSSL is limited to FIPS compliant ciphers/algorithms.

```
root@<device name>:~# openssl list -digest-algorithms
...
Provided:
  { 2.16.840.1.101.3.4.2.1, SHA-256, SHA2-256, SHA256 } @ default
  { 2.16.840.1.101.3.4.2.10, SHA3-512 } @ default
  { 2.16.840.1.101.3.4.2.8, SHA3-256 } @ default
  { 2.16.840.1.101.3.4.2.7, SHA3-224 } @ default
  { 2.16.840.1.101.3.4.2.2, SHA-384, SHA2-384, SHA384 } @ default
  { 2.16.840.1.101.3.4.2.3, SHA-512, SHA2-512, SHA512 } @ default
  { 2.16.840.1.101.3.4.2.5, SHA-512/224, SHA2-512/224, SHA512-224 } @ default
  { 2.16.840.1.101.3.4.2.12, SHAKE-256, SHAKE256 } @ default
  { 1.3.14.3.2.26, SHA-1, SHA1, SSL3-SHA1 } @ default
  { 2.16.840.1.101.3.4.2.9, SHA3-384 } @ default
  { 2.16.840.1.101.3.4.2.11, SHAKE-128, SHAKE128 } @ default
  { 2.16.840.1.101.3.4.2.4, SHA-224, SHA2-224, SHA224 } @ default
  { 2.16.840.1.101.3.4.2.6, SHA-512/256, SHA2-512/256, SHA512-256 } @ default
  { KECCAK-KMAC-128, KECCAK-KMAC128 } @ default
  { KECCAK-KMAC-256, KECCAK-KMAC256 } @ default
  { 2.16.840.1.101.3.4.2.1, SHA-256, SHA2-256, SHA256 } @ fips
  { 2.16.840.1.101.3.4.2.10, SHA3-512 } @ fips
  { 2.16.840.1.101.3.4.2.8, SHA3-256 } @ fips
  { 2.16.840.1.101.3.4.2.7, SHA3-224 } @ fips
```

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 access from offending source IP addresses.

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

For more information, see:

- Configure brute force protection
- View current bans
- Manage brute force protection via the Command Line

CONFIGURE BRUTE FORCE PROTECTION

> **Note:** Brute Force Protection is enabled by default for SSH and WebUI.

1. Navigate to **CONFIGURE > SERVICES > Brute Force Protection**.
2. Choose the required settings:

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

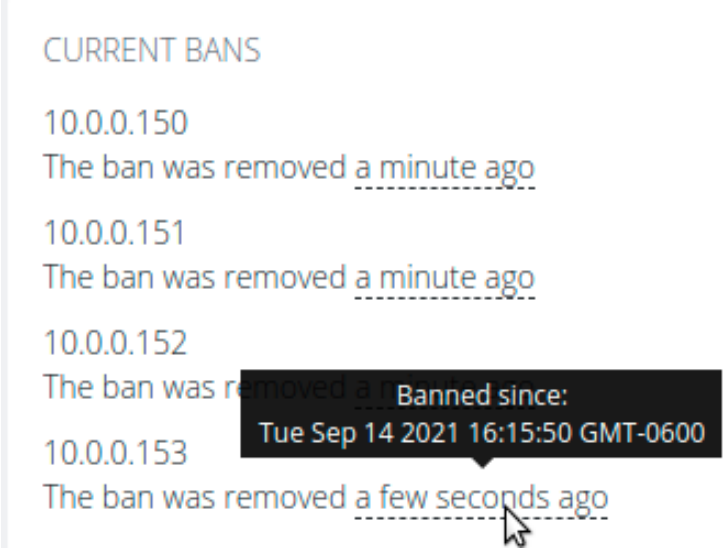
Field	Values	Description
Lockout period	60 (minimum)	The number of seconds that an IP address is banned after violating the Brute Force Protection policies.

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

VIEW CURRENT BANS

IP addresses that are currently blocked appear in the CURRENT BANS section of the WebUI, 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.



MANAGE 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.

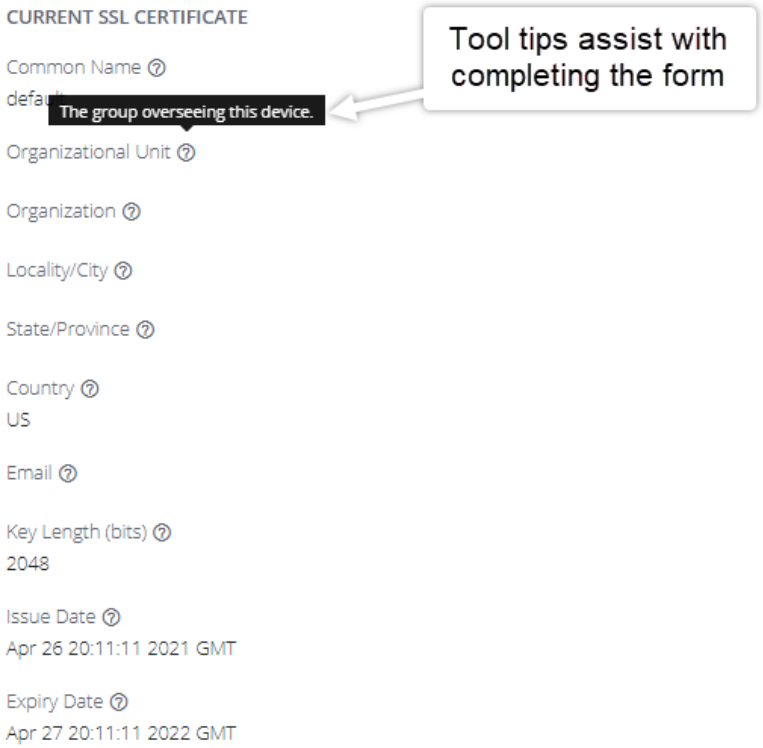
Description	Command	Notes
Display Brute Force Protection configuration	ogcli get services/brute_force_protection	
Update Brute Force Protection configuration	ogcli replace services/brute_force_ protection << END ban_time=180 find_time=1 https_enabled=false max_retry=4 ssh_enabled=true END	Ban time in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

Description	Command	Notes
List all bans with ogcli	ogcli get monitor/brute_force_protection/bans	

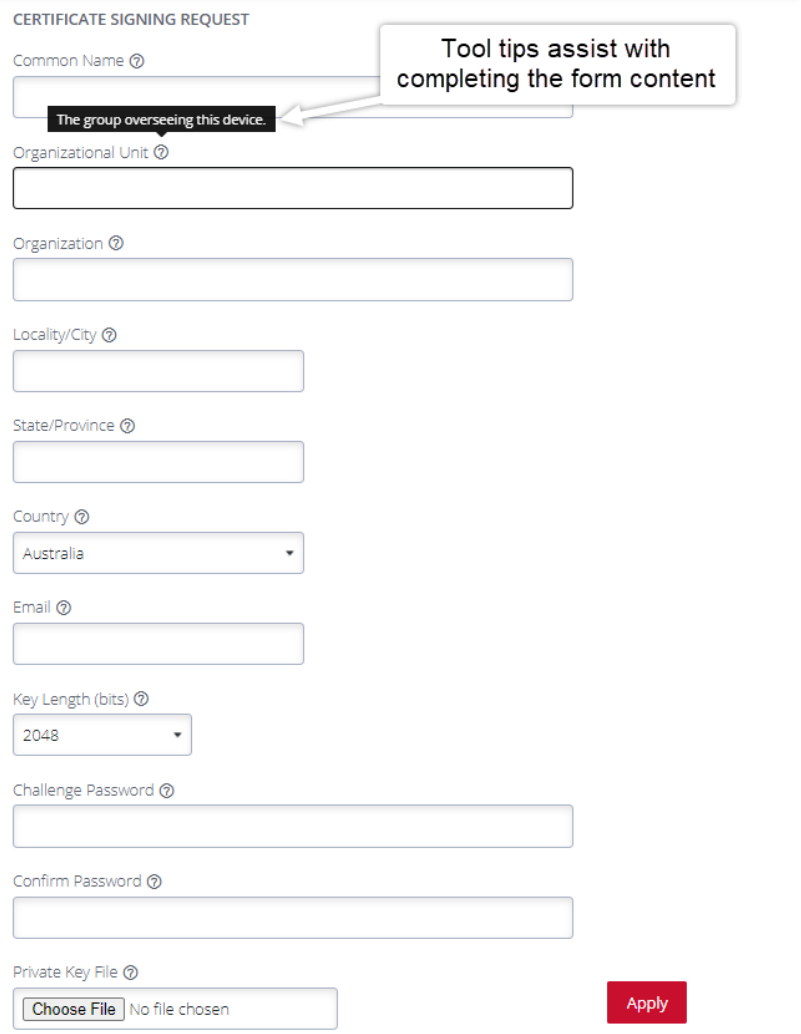
HTTPS CERTIFICATE

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

1. 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.



2. To generate a new SSL certificate, scroll down to the Certificate Signing Request form and complete the appropriate fields:



Field	Description
Common Name	The specific domain to which the certificate is issued. This is automatically added as a Subject Alternative Name (SAN).

Field	Description
Subject Alternative Names	Enter any alternative names for which the certificate is valid. A domain name can be an IP address or a domain. Click **Add SAN** to add additional subject alternative names.
Organizational Unit	Enter the organizational unit to which the certificate belongs.
Organization	Enter the organization to which the certificate belongs.
Locality/City	Enter the locality or city where the organization is located.
State/Province	Enter the state or province where the organization is located.
Country	Enter the country where the organization is located.
Email	Enter the email address for the organization contact, for example the certificate administrator or IT department.
Challenge Password	Enter the shared secret to authentication the certificate owner.
Confirm Password	Re-enter the **Challenge Password**.

Field	Description
Generate Private Key	Select whether to **Enable** or **Disable** the generation of a new private key for the CSR. If set to **Disable**, and no **Private Key File** is provided, the existing private key is used.
Key Length (bits)	Enter the number of bits in the certificate's key. Higher numbers mean stronger security. This field is available only if **Generate Private Key** is set to **True**.
Private Key File	Click **Browse** to navigate to and upload a private key file. This field is available only if **Generate Private Key** is set to **False**.

3. Click **Apply**.
4. To download a certificate, click **Download**.
5. To upload a signed certificate, under **Upload Certificate**, click **Browse** in the **Certificate** field then navigate to the certificate you want to upload.
6. Click **Apply**.

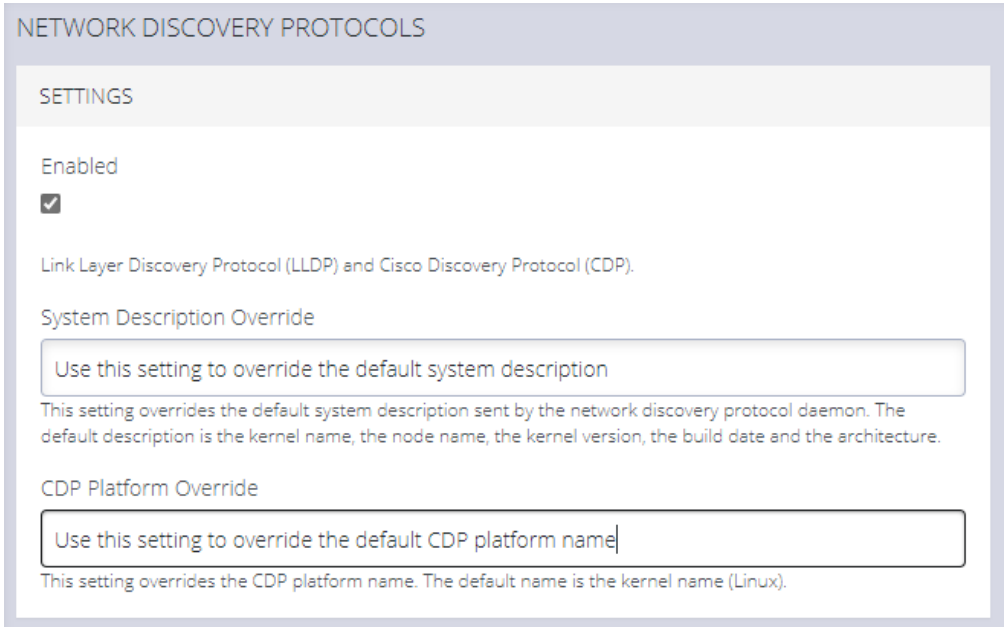
NETWORK DISCOVERY PROTOCOLS

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

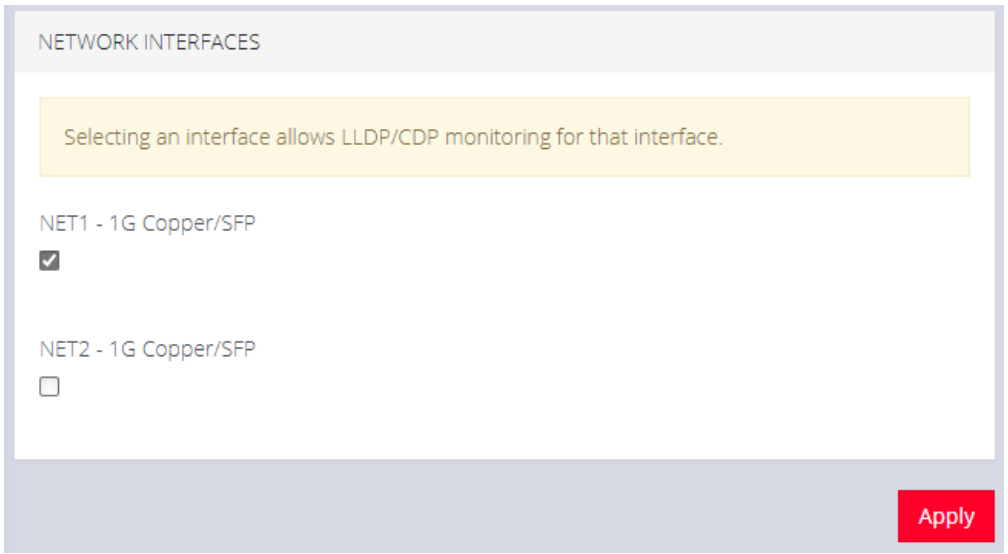
The **CONFIGURE > SERVICES > Network Discovery Protocols > LLDP/CDP NEIGHBORS** page allows you to enable this service by clicking the **Enabled** checkbox.

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).



Select one or more checkboxes in the **NETWORK INTERFACES** section of the page and click **Apply**.



ROUTING

The Console Manager supports Static Routing and Dynamic Routing. Static Routing and OSPF are currently configured via the ogcli interface, however, CLI configuration will not persist after a device reboot. Dynamic Routing can be enabled via the WebUI and configured using standard Free Range Routing interfaces (e.g., vtysh).

> **Note:** Configuration set via vtysh (or other FRR interfaces) must be manually backed up in addition to a standard Opengear configuration export.

DYNAMIC ROUTING

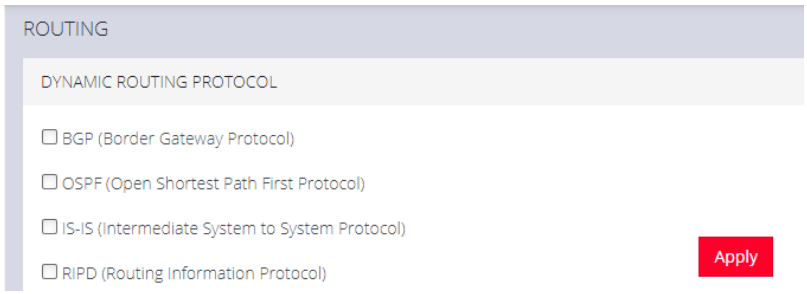
To enable Dynamic Routing on the CM, navigate to the **CONFIGURE > SERVICES > Routing** page.

Dynamic Routing supports four routing protocols, these are:

- **BGP**: Border Gateway Protocol.
- **OSPF**: Open Shortest Path First Protocol. For more information, see OSPF Configuration.
- **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 CM.



STATIC ROUTING (VIA THE OGCLI)

To enable Static Routing on the CM, 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

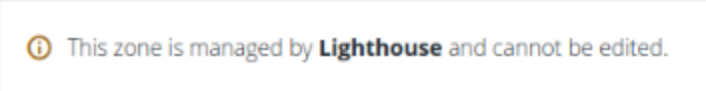
Argument	Description
`get`	Get a list of static routes.
`create`	Add a static route.
`replace`	Similar to the "Create Static Route" example given on the previous page. Creates a single static route by specifying its UUID; or a list of static routes. Overwrites existing routes.

Argument	Description
`delete`	Delete all static routes.
`merge`	Merge the existing configuration list with a new list.

OSPF CONFIGURATION

Open Shortest Path First (OSPF) is a link-state routing protocol used to discover routes on a network. It is used to dynamically adjust routes on the Console Server so that subnets connected to different interfaces can reach each other by routing through the Console Server.

Support for OSPF configuration and WireGuard was added to the REST API and Config Shell at release 23.02.

> **CAUTION:** Users are discouraged from editing OSPF configuration when it has been marked as managed by a Lighthouse. A warning message displays when an attempt is made to edit any configuration pushed down from Lighthouse through Config Shell. After being warned of the risk users may continue to edit configuration with a **managed_by** field set through Config Shell.
>
> 
>

MANAGED CONFIGURATION ITEMS

Certain items in the configuration can contain an optional **managed_by** field. Configuration items that have the managed_by field set are considered to be "managed". The managed_by field is set by a managing entity such as lighthouse, when the network plan is being managed by a remote node.

The following features can have managed configuration:

- Firewall Zones
- Firewall Policies
- Routing OSPF
- WireGuard Tunnels

If a firewall zone, policy or WireGuard tunnel is managed, this does not affect sister contexts, for example, if the WireGuard tunnel is managed, any other WireGuard tunnels configured separately by the user are not managed. However, there is only one OSPF configuration file and users must bypass the **managed_by** field in Config Shell in order to edit the configuration.

NEW FIELDS IN REST API & CONFIG SHELL

REST API

The OSPF sub-object now has a number of new fields:

```
"services": {
  "routing": {
    "bgpd": {
      "enabled": true
    },
    "isisd": {
      "enabled": false
    },
    "ripd": {
      "enabled": true
    },
    "ospfd": {
      "enabled": false,
      "router_id": "",
      "redistribute_connected": false,
      "redistribute_static": false,
      "redistribute_kernel": false,
```

```
      "interfaces": [],
      "neighbors": [],
      "networks": []
    }
  }
}
```

CONFIG SHELL

The services/routing OSPF context has new fields similar to the REST API:

```
config(services/routing ospfd): show
Entity services/routing field ospfd
  enabled                          false
  redistribute_connected  false
  redistribute_static         false
  router_id                        ""
  interfaces (array)
  neighbors (array)
  networks (array)
```

Field	Condition	Definition
enabled	(true / false)	When set to true, the OSPF service is started.
redistribute_connected	(true / false)	If this option is enabled, any directly connected network routes are broadcast to OSPF neighbours.
redistribute_static	(true / false)	Network routes can be statically defined (in OSPF, not the Linux Kernel) by editing the ospfd.conf file or through `vtysh`. If this option is enabled, redistribute_routes broadcasts any static routes that are managed by OSPF.

Field	Condition	Definition
redistribute_kernel	(true / false)	If this option is enabled, network routes that are configured in the Linux kernel via DHCP or static definition are shared with OSPF neighbors.
router_id		The router id (RID) is a 32-bit number which must be expressed as a dotted quad (i.e. in the format A.B.C.D). The RID is used to identify the router. It must be unique within the OSPF network. The highest RID in the network is used to determine which OSPF node is the designated router.

INTERFACES, NEIGHBORS AND NETWORKS.

There are a number of sub-objects under the ospfd context: interfaces, neighbors and networks.

INTERFACES CONTEXT

The services/routing OSPF interfaces context is an array in which each element holds the specific individual interface related parameters for OSPF. Each interface has the following fields:

```
Entity services/routing field ospfd interfaces 0
  auth_method    ""   (required)
  cost                    ""
  priority               ""
  name                  ""    (required)
  non_broadcast  ""    (required)
  passive                              ""    (required)
```

Definitions of interface related parameters for OSPF:

Parameter	Definition
auth_method	The authentication method to use for communications on this interface. Should be one of 'no_auth', 'cleartext' or 'md5'. If authentication is enabled (i.e. not no_auth), one or multiple authentication keys can be configured depending on your authentication method chosen. • Cleartext authentication only requires one authentication key. • Md5 authentication can use multiple authentication keys, each of which requires a unique id.
cost	The link cost of the interface used in OSPF route calculations. It is normally auto-calculated, but can be specified manually in the range of 1 to 65535.
priority	The priority of a router on an OSPF interface mainly is used to determine the designated router/backup designated router (DR/BDR) for a network. OSPF forwards all messages to the designated router, reducing the amount of repetitive routing traffic on the network. The priority is in the range of 0 to 255. The default priority for each router is 1 unless specified. Selecting a priority of 0 makes the router unable to become a DR/BDR. The higher the priority, the higher chance a OSPF router has of winning the DR/BDR election.
name	The name of the interface these settings apply to. This should match the name of an interface on the device.
non_broadcast	May be true or false. If true, the interface is marked as non broadcast for OSPF purposes. This would mean OSPF would not use multicast on this interface, and static neighbours would have to be defined.
passive	May be true or false. If true, the interface should be marked as passive for OSPF purposes. This would mean LSAs are not traded on this link.

NEIGHBORS CONTEXT

The services/routing OSPF neighbors context is an array where each element holds details about adjacent static neighbor devices. Neighbors must be specified for non-broadcast networks.

```
config(services/routing ospfd neighbors): add
config(services/routing ospfd neighbors 0): show
Entity services/routing field ospfd neighbors 0
address "" (required)
```

Where `address` is an IPv4 host address of the static neighbor.

NETWORKS CONTEXT

The services/routing OSPF networks context is an array where each element holds IP network configurations to enable the system OSPF service for:

```
config(services/routing ospfd networks): add
config(services/routing ospfd networks 0): show
Entity services/routing field ospfd networks 0
address_with_mask "" (required)
area "" (required)
```

Network Configuration	Definition
address_with_mask	An IPv4 network address with CIDR subnet mask to enable OSPF for (e.g. A.B.C.D/E). No host bits should be set.
area	An OSPF network can be divided into sub-domains or groupings called areas which limit the scope of route information distribution. We specify the area number/id we want the interface to be in. This can be an integer between 0.0.0.0 and 255.255.255.255 or can take a form similar to an IP address A.B.C.D. All routers inside an area must be a part of the same OSPF network and have the same area number/id to become OSPF neighbours.

INTERACTION WITH CONFIGURATION FILES

The first line of /etc/quagga/ospfd.conf controls whether the console server configuration system will overwrite the file with new content or keep custom user configuration. This supports customers who want to upload a custom configuration file for OSPF. If the first line contains only the text `! autogen`, the configuration system will overwrite the file, otherwise, the configuration system will have no effect.

To verify the OSPF configuration, the configuration file generated can be found in /etc/quagga/ospfd.conf:

```
! autogen
! This configuration file has been autogenerated. Any changes made within
! will be overwritten. To stop this and allow for manual editing, remove
! or change the first line of this file to something other than '! autogen'.
! The behaviour can be reenabled by restoring the first line to this or by
! completely removing this contents of this file.
!
interface wg-smf-1
ip ospf network non-broadcast
!
interface net1
!
router ospf
ospf router-id 0.0.0.1
log-adjacency-changes
redistribute connected
redistribute static
network 10.0.0.0/24 area 0.0.0.0
network 192.168.41.0/24 area 0.0.0.0
neighbor 10.0.0.1
```

```
!
line vty
!
```

CONFIRM OSPF NEIGHBOURS

Use the `vtysh` command line tool to see if OSPF neighbours have been discovered:

```
root@<device name>-q:~# vtysh -c 'show ip ospf neighbor'
Neighbor ID       Pri State

Dead Time Address                           Interface

RXmtL     RqstL         DBsmL
```

```
-                               0 Attempt/DROther           33.007s 10.0.0.1

wg-smf-1:10.0.0.2                   0                                       0

0
```

(Where `wg-smf-1` is a user-named interface).

WIREGUARD CONFIGURATION

WireGuard is an open source encrypted VPN solution; WireGuard configuration support was added to the REST API and Config Shell at release 23.8. WireGuard facilitates communication between two peer devices; in order to communicate with a peer, both devices must have a virtual WireGuard interface configured over the physical or virtual interface they are connected over.

> **Note:** Users who have pre-existing configuration files for WireGuard will not have their configurations overwritten as the configurator only modifies those files if they are initially missing or are prefixed with a disclaimer that manual edits are overwritten.

VIEW A WIREGUARD CONFIGURATION

WireGuard installs the **wg** tool which can be used to control, configure and monitor WireGuard . Refer to the WireGuard online tools index page: index : wireguard-tools

> **Note:** Opengear does not own or operate the WireGuard tools web page and is not responsible for its content or maintenance. The link is provided only for the reader's convenience.

CONFIGURE WIREGUARD THROUGH CONFIG SHELL OR REST API

WireGuard is configured through Config Shell or REST API. The minimum configuration of WireGuard is shown in the following:

1. Provide a name for the interface (wg0 in the following example).
2. Set enabled.
3. Set the private_key of your WireGuard interface.
4. Add an address (at least one) for your WireGuard interface (10.0.0.1/24 in this case).
5. Add a peer with the following parameters: endpoint_address, endpoint_port, public_key.
6. Add at least one allowed IP for your peer with allowed_ips. This is the WireGuard address(es) (it can also accept an address range) of the other interface to which you are connected.

For example:

```
config: wireguard
config(wireguard): add wg0
config(wireguard wg0): private_key AGiZvFHY+r/dD0rHSKU5ZCrHNdLM0W/h29VxobxWgFo=
config(wireguard wg0): enabled true
config(wireguard wg0): addresses
config(wireguard wg0 addresses): add 10.0.0.1/24
config(wireguard wg0 addresses): up
config(wireguard wg0): peers
```

```
config(wireguard wg0 peers): add
config(wireguard wg0 peers 0): public_key
o+quB4sbUAG2hEGSPpMNTnO0YSaQTP7dD+Q4IVjiCW8=
config(wireguard wg0 peers 0): allowed_ips
config(wireguard wg0 peers 0 allowed_ips): add 10.0.0.2/32
config(wireguard wg0 peers 0 allowed_ips): up
config(wireguard wg0 peers 0): endpoint_address 192.168.1.2
config(wireguard wg0 peers 0): endpoint_port 51820
config(wireguard wg0 peers 0): up
config(wireguard wg0 peers): top
```

CONFIG SHELL WIREGUARD CONFIGURATION

The following shows a typical WireGuard configuration in Config Shell:

```
config: show wireguard wg0
Entity wireguard item wg0
  description ""
  enabled true
  mtu 1420
  name wg0
  port 51820
  private_key AGiZvFHY+r/dD0rHSKU5ZCrHNdLM0W/h29VxobxWgFo=
  public_key ""
  table ""
  addresses (array)
    0 10.0.0.1/24
  peers (array)
    0 (object)
      endpoint_address     192.168.1.2
      endpoint_port            51820
```

```
      keep_alive                    ""
      public_key                     o+quB4sbUAG2hEGSPpMNTnO0YSaQTP7dD+Q4IVjiCW8=
      allowed_ips (array)
          0 10.0.0.2/32
  post_down_hooks (array)
  post_up_hooks (array)
  pre_down_hooks (array)
  pre_up_hooks (array)
```

REST API WIREGUARD CONFIGURATION

The following shows a typical WireGuard configuration in Config Shell:

```
{
    "wireguards": [
        {
          "enabled": true,
          "post_down_hooks": [],
          "id": "wireguard_tunnels-1",
          "pre_up_hooks": [],
          "post_up_hooks": [],
          "private_key": "AGiZvFHY+r/dD0rHSKU5ZCrHNdLM0W/h29VxobxWgFo=",
          "name": "wg0",
          "pre_down_hooks": [],
          "addresses": [
              "10.0.0.1/24"
          ],
          "peers": [
              {
                    "allowed_ips": [
                          "10.0.0.2/32"
```

```
                        ],
                        "public_key":
"o+quB4sbUAG2hEGSPpMNTnO0YSaQTP7dD+Q4IVjiCW8=",
                        "endpoint_address": "192.168.1.2",
                        "endpoint_port": 51820
                }
            ]
        }
    ]
}
```

CONFIGURABLE WIREGUARD FIELDS

The WireGuard <interface-name> context holds the configuration for a WireGuard connection. The following fields can be configured:

WireGuard Field	Description
description	This can be any user text to describe the WireGuard interface.
enabled	Values may be **true** or **false**. When enabled, WireGuard is started for this configuration.
mtu	Allows customization of the maximum transmission unit (MTU) for the local WireGuard interface. The range is 1280 - 1472 and if not set, WireGuard will use the internal default of 1420.
name	The name of the WireGuard interface used in the Linux kernel. Names must be unique, max 15 characters and only contain letters, numbers, hyphens or underscores.

WireGuard Field	Description
port	The port the local instance of WireGuard will listen on. The range is 1 to 65535 and defaults to 51820.
private_key	The private key to use to authenticate the local WireGuard interface. This is obtained by running the wg genkey command.
public_key	The public key that corresponds your private key, which WireGuard peers will authenticate with. This is obtained by running the wg pubkey command.
table	The routing table for the WireGuard routes. Can be a table number, 'off' or 'auto'.

WIREGUARD CONTEXT SUB-OBJECTS

There are a number of sub-objects under the WireGuard context: addresses, peers and hooks.

ADDRESSES

The wireguard <interface-name> addresses context is a list that holds the IPv4 CIDR addresses of the local WireGuard interface. These are statically assigned when the WireGuard interface is brought up.

```
config: wireguard
config(wireguard): add wg0
config(wireguard wg0): addresses
config(wireguard wg0 addresses): add 10.0.0.1/24
```

PEERS

The following list defines the WireGuard settings for WireGuard-capable remote peers. Each peer has the following fields:

```
config(wireguard wg0 peers 0): show
Entity wireguard item wg0 field peers 0
    endpoint_address ""
    endpoint_port ""
    keep_alive ""
    public_key "" (required)
    allowed_ips (array) (required)
```

Peer Field	Description
endpoint_address	A reachable IP address or fully-qualified domain name for the remote peer with a WireGuard interface.
endpoint_port	The port number for which the WireGuard instance is listening on the remote peer.
keep_alive	Equivalent to PersistentKeepalive in the WireGuard config, this specifies how often the WireGuard interface must send a keep alive packet. This helps keep the routing entry alive for scenarios where the peer is behind a NAT.
public_key	The public key that is accepted by the local WireGuard service if offered by a peer for the purpose of mutual authentication during a five step key exchange process.
allowed_ips -	A list which specifies the IP ranges for which a peer routes traffic. For multiple WireGuard interfaces on the same device, the addresses must not overlap. The IP addresses specified here are the addresses of the peer's WireGuard interface(s) - this is where the peer "routes traffic". These are specified as IPv4 addresses in a.b.c.d/<cidr_mask> format.

HOOKS

WireGuard allows for commands to be executed before/after the interface is brought up/down. These can be specified in the following array fields:

> **Note:** Each field is an array of strings that correspond to commands to be executed.

Hook	Description
pre_up_hooks	Run a command before the interface is brought up (optional).
post_up_hooks	Run a command after the interface is brought up (optional).
pre_down_hooks	Run a command before the interface is brought down (optional).
post_down_hooks	Run a command after the interface is brought down (optional).

ADD A WIREGUARD INTERFACE TO A FIREWALL ZONE

The WireGuard interface can be added to a firewall zone as in the following example:

```
Entity firewall/zone item zone
description "" (required)
label "" (required)
masquerade "" (required)
name zone
permit_all_traffic "" (required)
address_filters (array)
custom_rules (array)
physifs (array)
port_forwarding_rules (array)
wireguards (array)
```

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	This is the feature Enable/Disable button. For information about Unauthenticated Access to Serial Ports, see Unauthenticated SSH to Serial Ports.
Alternate Base for direct serial port access	Specify an alternate base port for ssh access to ports. The alternate base is in addition to the default base port of 3000.

UNAUTHENTICATED SSH TO SERIAL PORTS

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 have 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 requirement 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 described in the following table.

Property	Definition/Range

Serial Port Delimiter	A character that separates the username and port selection information. The default value is the + character.
	Default is '+', maximum length is 1.
	The prohibited characters are '\', ' " ', ' ` ', ' ', '=' and '#'.
	Source: schema
	required ssh_delimiter: string (default = "+"; minimum = 1; maximum = 1; validator = ("ssh_url_delimiter")),
	Source: validator
	if (strlen(v) != 1) valid = 0;v 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;
	}

Port Number for Direct SSH Links	This port number is 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.
Max Startups Start	The number of connections pending authentication before new connections *begin* to be refused. *Required start: int (minimum = 1; default = 10)*

Property	Definition/Range
Max Startups Full	The number of connections pending authentication before *all* new connections are refused. *Required full: int (minimum = 1; default = 100)*
Max Startups Rate	This is the percentage rate at which new connections are refused after the Max Startups value is reached. The rate is increased to 100% at Max Startup Full. *Required rate: int (minimum = 1; maximum = 100; default = 30),* *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.*
Unauthenticated Access to Serial Ports	This is the feature Enable/Disable button.
Alternate Base for direct serial port access	The alternate base port for ssh access to ports in addition to the default base port of 3000. You can set this value to allow access to x + port in addition to 3000 + port. For example, if you set the alternate base to 2000, you can access port 2 with both of the following: *ssh -p2002 root@vom # using alternate base* *ssh -p3002 root@vom # using default base*

3. When required, enable the Unauthenticated SSH feature by clicking the **Enabled** button.

> **Note:** Unauthenticated access to all serial ports is 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.

CONNECT 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 conventions described in the following:

Convention	Example

Use a network client to connect to the service network Base Port + serial port number.	`# SSH to serial port 1 by TCP port`
	`ssh -p 3001 -l operator 70.33.235.190`
	
	In this example, the SSH base port is TCP port 3000, so SSH to TCP port 3001 directly connects you to serial port 1

SSH to the Opengear node, log in adding +portXX to your username (e.g. root+port01 or operator+port01).	`# SSH to serial port 1 by port name` `ssh -l operator+port01 70.33.235.190`
SSH to the Opengear node, log in adding the +port-label to your username (e.g. root+Router or operator+Router).	`# SSH to serial port labelled Router` `ssh -l operator+Router 70.33.235.190`

Notes:

- For additional reading on connecting to serial ports see: Communicating with serial port connected devices.
- Serial ports in the Local Console and Disabled ports modes are not available for SSH connection.

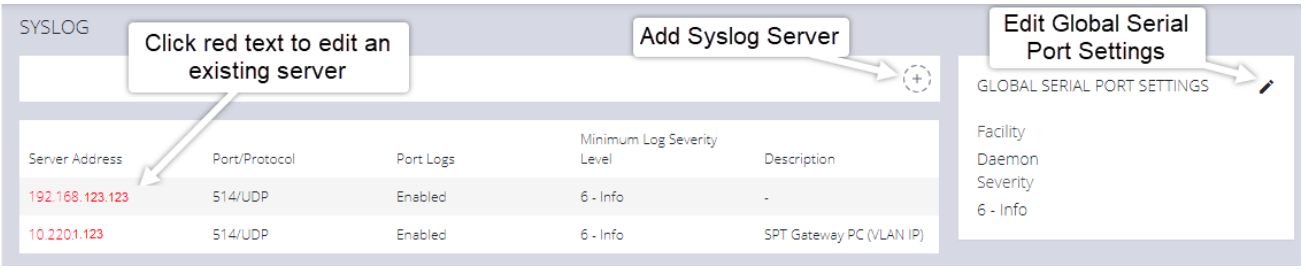
FEATURE PERSIST

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

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.



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 to help 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.
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.

GLOBAL SERIAL PORT SETTINGS TAB - FIELD DEFINITIONS

Configure > Services > Syslog > Global Serial Port Settings

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

Field	Definition
Add Button	Click to initiate the syslog, wait for confirmation banner.

SYSLOG FACILITY DEFINITIONS

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

Facility	Definition
ftp	FTP daemon
Local	Locally used facilities

SYSLOG SEVERITY DEFINITIONS

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

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 above). Make the required changes, then click the **Submit** button.

To delete a server, click the **Delete** icon on the top-right of the **Edit Syslog Server** page.

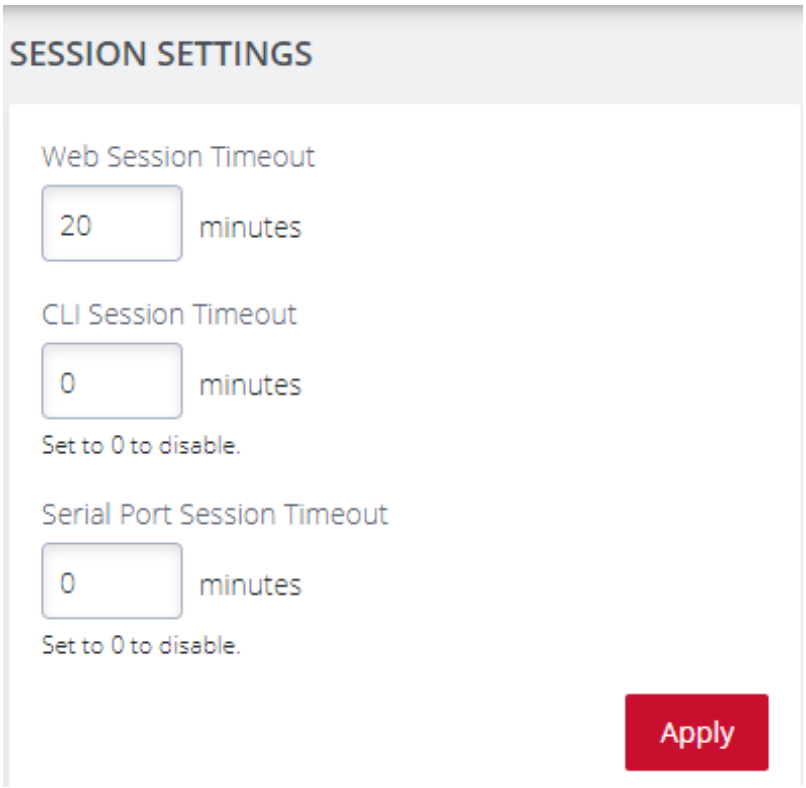


SESSION SETTINGS

Use **Session Settings** to set timeouts for console sessions where the users have been idle for a specified time. At timeout, the user's Web, CLI or Serial Port sessions are terminated, thus excluding authorized users with physical access to the node that has been left connected.

To set the timeouts for Web, CLI or Serial Port sessions settings:

1. Navigate to the **SETTINGS > Services > Session Settings** page.



2. Set the fields as appropriate:
   - **Web Session Timeout**: From 1 to 1440 minutes.
   - **CLI Session Timeout:** 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.
   - **Serial Port Session Timeout:** From 1 to 1440 minutes or set it to 0 to disable the timeout.
3. Click the **Apply** button to save the settings.
   The new session timeout takes immediate effect on all pmshell sessions, including ones in use.

FILE SERVER

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

TFTP can be used by nodes 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:

1. Click the **TFTP Enabled** button.



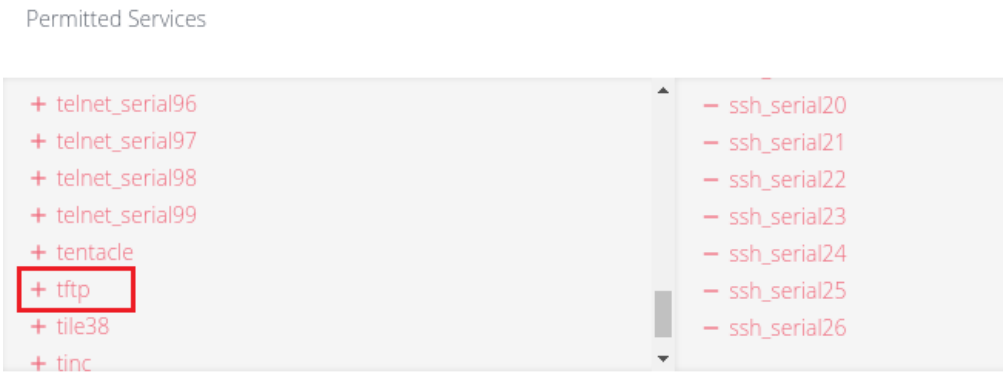
2. Click **Apply** to save the changes.
   The TFTP service is now running with a default location of **/mnt/nvram/srv**.
   This location is where all files uploaded to the TFTP server is stored.

> **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.

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



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

   On the **File Server** page, the zones with TFTP enabled are now displayed.



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.

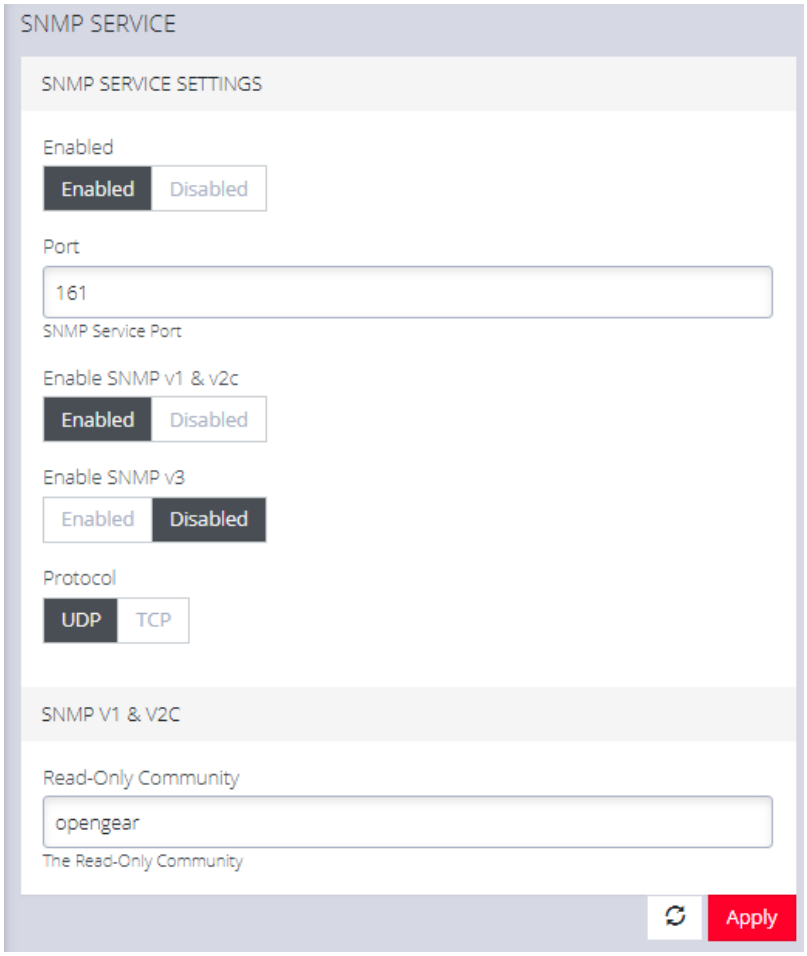
> **CAUTION:** Using a storage volume other than **/mnt/nvram** is not recommended. Data may be lost after reboot, or be inaccessible when switching boot slots.

As an administrative user, run:

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

SNMP SERVICE

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



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 displays where you can add service specific settings.

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

For **SNMP v3**, you can also set the **Authentication Protocol** to **MD5**, **SHA**, **SHA-224**, **SHA-256**, **SHA-384**, or **SHA-512**.

SNMP ALERT MANAGERS

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

See the Multiple SNMP Alert Managers feature for information about configuring more than one SNMP manager.

To create or configure SNMP Alert Manager, click the **Add New SNMP Alert Manager** button at the top-right of the page.

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.
- **Authentication Protocol**: The authentication protocol used for authenticated SNMP v3 messages. Only available when the **Version** is set to **v3**.

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

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 must be selected.

CREATE AN SNMP MANAGER

1. Navigate to **Configure > SNMP > SNMP Alert Managers**.
2. Click the **Add New SNMP Manager** button.
   The new **SNMP Alert Manager Form** displays.
3. Complete the fields as appropriate:

Field	Definition
Description	Add a description of the SNMP Alert Manager.
Server Address	Enter the IPv4/IPv6 address or domain name of the computer acting as the SNMP Alert Manager. If you want to use an IPv6 Address, then you must select either **UDP6** or **TCP6** from the list of **Protocols**. Whether you input an IPv6 address or a domain name, the correct protocol must be selected.
Port	Enter the listening port used by the SNMP Alert Manager. The default value is 162.

Field	Definition
Protocol	Select the transport protocol used to deliver traps or informs (for SNMP v3): • UDP - Speeds up transmissions by enabling the transfer of data before an agreement is provided by the receiving party. • TCP - A commonly used protocol used to transmit data from other higher-level protocols that require all transmitted data to arrive. • UDP6 - Similar to UDP but uses IPv6. • TCP6 - Similar to TCP but uses IPv6. If you want to use an IPv6 Address in **Server Address**, then you must select either **UDP6** or **TCP6**.
Version	The version of SNMP protocol to use. The default value is v2c. For further reading on SNMP versions we suggest: https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol#Protocol_versions
SNMP V1 & V2C Community	A group name authorized to send traps by the SNMP alert manager configuration for SNMP versions 1 and 2c. This must match what is setup in the SNMP alert manager. Examples of commonly used values are log, execute, net and public.
	Click the **Submit** button to finalize the New SNMP Manger process.

Field	Definition
	Click the bin widget to **Delete** an SNMP Manager (in the Edit SNMP Manager page).

4. Click the **Submit** button.

   A banner displays confirming that the new SNMP Manager is successfully created and the new manager displays in the list of SNMP Alert Managers.

> **Note:** For SNMP V3 TRAPS, an Engine ID is 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 are sent for Alerts added in **Configure > SNMP Alerts.** Traps are also sent to all the configured SNMP Alert Managers for a Playbook SNMP Reaction.

DELETE AN SNMP MANAGER

1. Click on the IP address of the item to open the **Edit SNMP Manager** page for that SNMP Manager.
2. Click on the **Delete SNMP Manager** widget in the top-right of the page.

FIREWALL

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

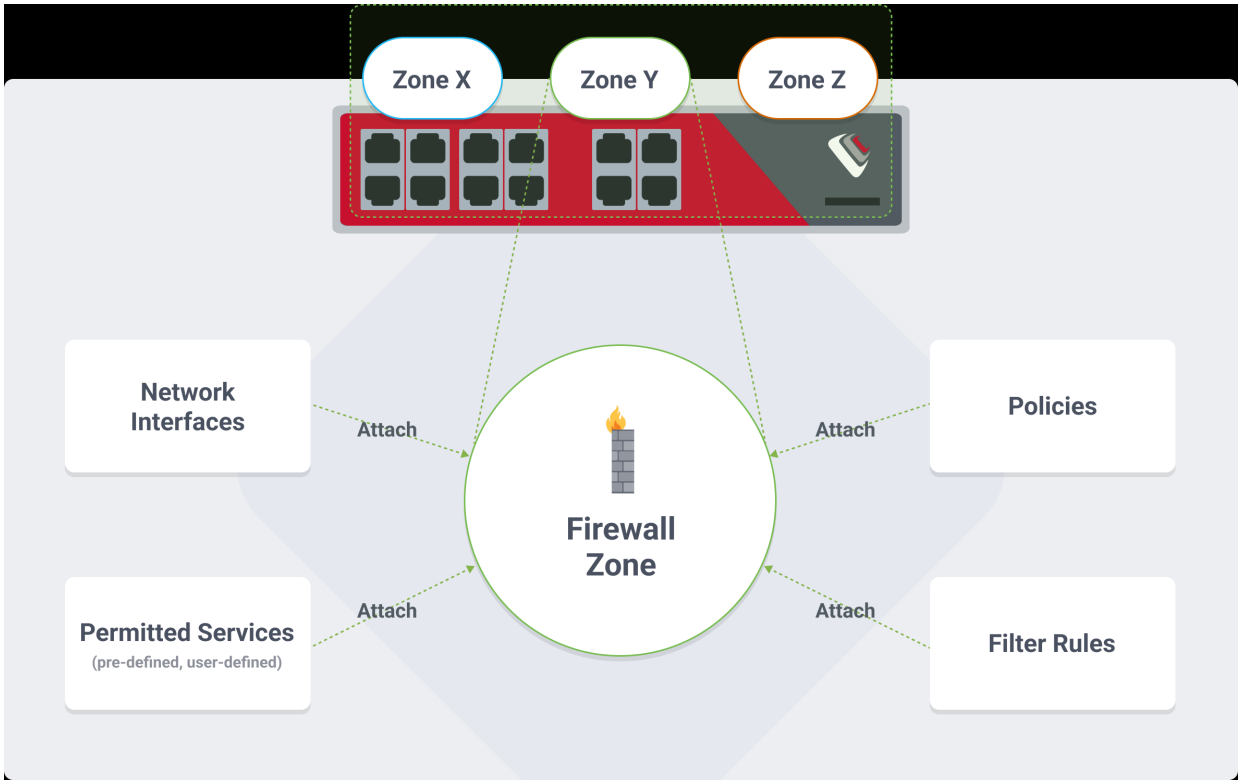
- Firewall Guide
- Firewall Management
- Firewall Policies
- Firewall Services
- Adding WireGuard Zones to a Firewall

FIREWALL GUIDE

INTRODUCTION

Opengear firmware is equipped with a powerful firewall stack based on leading open source firewalld and nftables tools. The default firewall rule set is configured with a default-deny policy.

The firewall is based on the concept of configurable Zones. Zones enable operators to create multiple “firewall segments” per node and attach network interface(s), services, filtering policies and filtering rules to the zones.



Note: To access services on the device, a user must have both access through the firewall and the appropriate authorization, e.g., via a local user account or remote AAA.

There are several kinds of rules and policies that may be applied to Zones.

FIREWALL RULES

- Permitted Services Rules allow access to Services for requests arriving on interfaces in the Zone - Services are configurable collections of TCP/UDP port or ports (e.g., TCP port 443 is the device's HTTPS service for WebUI and REST API access). There are pre-defined services, devices also support user-defined services.
- Custom Rules allow the full flexibility of the firewalld rich rule syntax for fine-grained access control and advanced applications.

FIREWALL POLICIES

- Interzone Policies control how Zones may forward traffic between each other – by default Zones may not forward between each other (note that interfaces in the same Zone may always forward between themselves).
- Port Forwarding Rules use destination NAT (DNAT) requests arriving on interfaces in the Zone to an external Target IP/Port, e.g., a web server running on another host
- Additionally, you can apply source NAT (SNAT) to traffic going out of a Zone by checking the Masquerade Traffic option.

EXAMPLE WEBUI CONFIGURATION

The following examples use Permitted Services Rules and Custom Rules features

> **Note:** Some aspects of the WebUI may change in future releases.

EXAMPLE 1: DISALLOW WAN ZONE ACCESS TO HTTPS

The default configuration is to allow HTTPS (i.e. the WebUI & API) on the WAN Zone. To disallow this:

> **Note:** Ensure you are accessing the device via an interface outside the WAN Zone (e.g., NET2 which is the LAN Zone by default) otherwise you may be locked out.

1. Log in to the WebUI as an Administrator user.
2. Select **CONFIGURE > FIREWALL > Management**.
3. Click **WAN** then **Edit Zone**.
4. Scroll down to **Permitted Services**.
5. In the right-hand column, click – to remove **https** service.

6. Any service in the right-hand column allows everyone access to this service from this zone.
7. Click **Apply**.

EXAMPLE 2: PERMIT ACCESS TO WAN ZONE HTTPS FROM A TRUSTED SOURCE NETWORK ONLY

When a service is permitted using a Permitted Services Rule, connections to the service in that Zone are permitted regardless of the originating network the connection is coming from. To disallow connections from all but a trusted source network, use Custom Rules (following examples) instead.

In this example, HTTPS connections from the 10.12.34.0/24 network to the Operation Manager's WAN Zone are permitted, other HTTPS connections on the WAN Zone are disallowed.

> **Note:** Ensure you are accessing the device via an interface outside the WAN Zone (e.g., NET2 which is the LAN Zone by default) or from the trusted source network, otherwise you will lock yourself out.

1. Log in to the WebUI as an Administrator user.
2. Select **CONFIGURE > FIREWALL > Management**.
3. Click **WAN** then **Manage Custom Rules**.
4. Click **Add Custom Rule**.
5. In **Description** enter: *Trusted HTTPS*.
6. In **Rule Content** enter:
   rule family=ipv4 source address=10.12.34.0/24 service name=https accept

   > **Note:** This is supported via firewalld ‘rich-rules’ option.
7. Click **Apply**.
8. Follow the steps in Example 1 above to remove the HTTPS Permitted Service.

> **Note:** It is not recommended to mix firewall configurations between the UI (WebUI/CLI) and firewalld commands (firewall-cmd) from Linux shell. Commands may be overwritten. Recommended to use either WebUI or CLI for all supported functionality instead of firewall-cmd

CUSTOM RULES (FIREWALLD “RICH-RULES”)

This feature enables users to define fine-grained control of services inside a zone. Users can apply custom filter rules to traffic in a firewall zone based on Layer2 Ethernet MAC, L3 IP fields, layer 4 ports, pre-defined services. Actions to permit, deny, drop the defined packets can be included in the rule. Logging facility is also provided via custom rules.

The following sections provide examples and many sample templates that users can directly use in WebUI or CLI in the rich-rules field/section

CUSTOM RULES EXAMPLES:

Example 1: Filter (drop) specific IPv4 source address

```
rule family="ipv4" source address="34.34.36.36" drop
```

Example 2: Permit specific source subnet and list of address

```
rule family="ipv4" source address="34.34.36.0/24" accept
```

Example 3: Permit Specific Service (HTTPS) from a specific source subnet:

```
rule family="ipv4" source address="10.0.0.0/16" service name="https" accept
```

Example 4: Drop Specific Service (HTTP)

```
rule family="ipv4" service name="http" drop
```

Example 5: Permit specific source subnet and log connection attempts

```
rule family="ipv4" source address="10.0.0.0/16" accept log
```

Example 6: Permit IPv6 packets with source address, TCP port number 4000. Log the packets

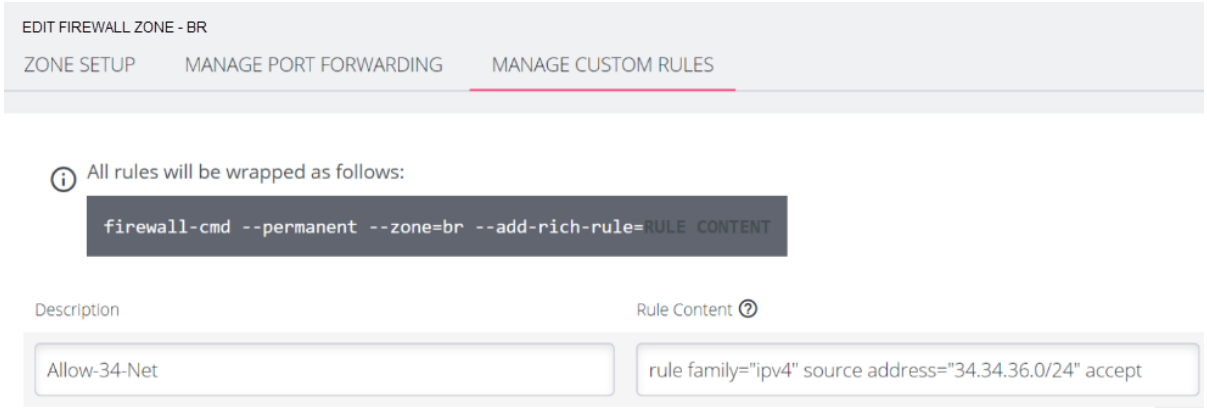
```
rule family="ipv6" source address="1:2:3:4:6::" port port=4000 protocol=tcp accept
log
```

Example 7: Permit IPv6 packets with source address, only TCP protocol, from all TCP ports. Log the packets

```
rule family="ipv6" source address="1:2:3:4:6::" protocol value="tcp" accept log
```

USEFUL TEMPLATES FOR USE IN WEBUI OR CLI

In WebUI:



In ogcli:

```
ogcli replace firewall/zones << 'END'
firewall_zones[0].custom_rules[0].description="allow rule"
firewall_zones[0].custom_rules[0].rule_content="rule family='ipv4' source
address='192.168.67.101/32' service name='telnet' accept"
…
END
```

SAMPLE RICH RULES TEMPLATES

```
1. rule family="ipv4" source address="<user-to-fill>" accept|drop|reject
```

```
2. rule family="ipv4" destination address="<user-to-fill>" accept|drop|reject
```

```
3. rule family="ipv4" destination address="<user-to-fill>" accept|drop|reject
```

```
4. rule family="ipv4" source address="<user-to-fill>" accept|drop|reject
```

```
5. rule family="ipv4" source address="<user-to-fill>" destination address="<user-to-fill>"
accept|reject|drop log
```

```
6. rule family="ipv4" source address="<user-to-fill>" service name="<user-to-fill>""
accept|reject|drop
```

```
7. rule family="ipv4" source address="<user-to-fill>" destination address="<user-to-fill>"
accept|reject|drop log
```

```
8. rule family="ipv4" source address="<user-to-fill>" destination address="<user-to-fill>"
accept|reject|drop log
```

```
9. rule family="ipv4" source address="<user-to-fill>" port port=<usr-to-fill>
protocol=tcp|udp accept|reject|drop
```

```
10. rule family="ipv4" source address="<user-to-fill>" protocol value="tcp|udp"
accept|reject|drop
```

Note: Ordering of rules is important. See this public article: Firewalld Rich Rules Explained.

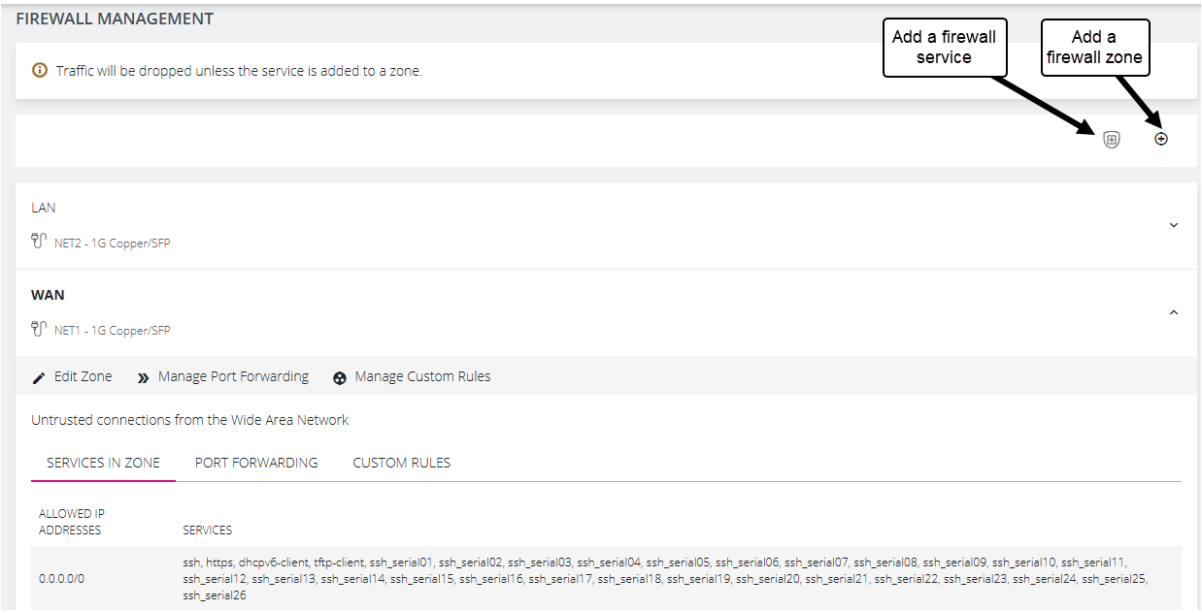
In the Template:

- Choose one of the actions accept|reject|drop [Drop action does not send any response back to source, reject does].
- For protocol value, tcp and udp examples are given in template, but many other choices are available.
- For values, source address as example, replace <user-to-fill> with the address. Address can be with or without subnet.

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.



Firewall Management main page.

FIREWALL ZONE SETTINGS

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

> **Note:** The application of any custom rules will result in **Permit All Traffic** being enabled in a zone.

ZONE SETUP

You can inspect details of any zone by clicking the **Expand** icon to the right of the zone. When 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:

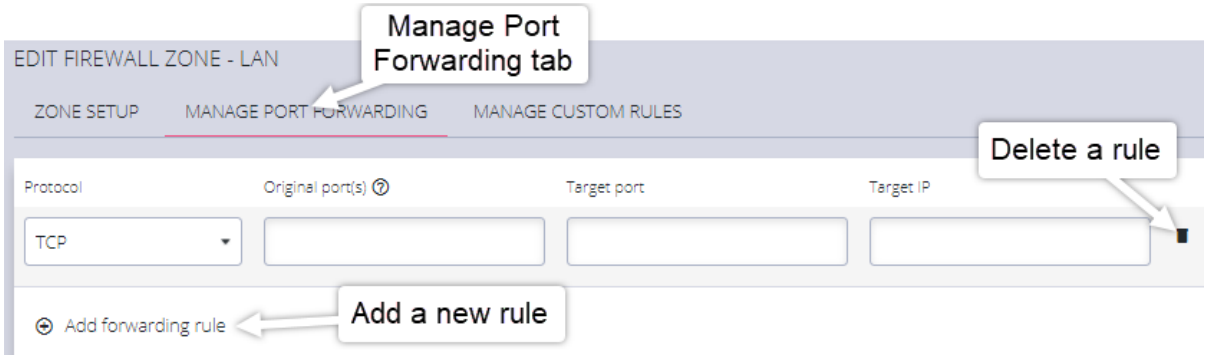
- Modify the Name of the zone.
- Add a Description for this zone.
- Permit all Traffic.
- Masquerade Traffic.

- 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 displays.

MANAGE PORT FORWARDING

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

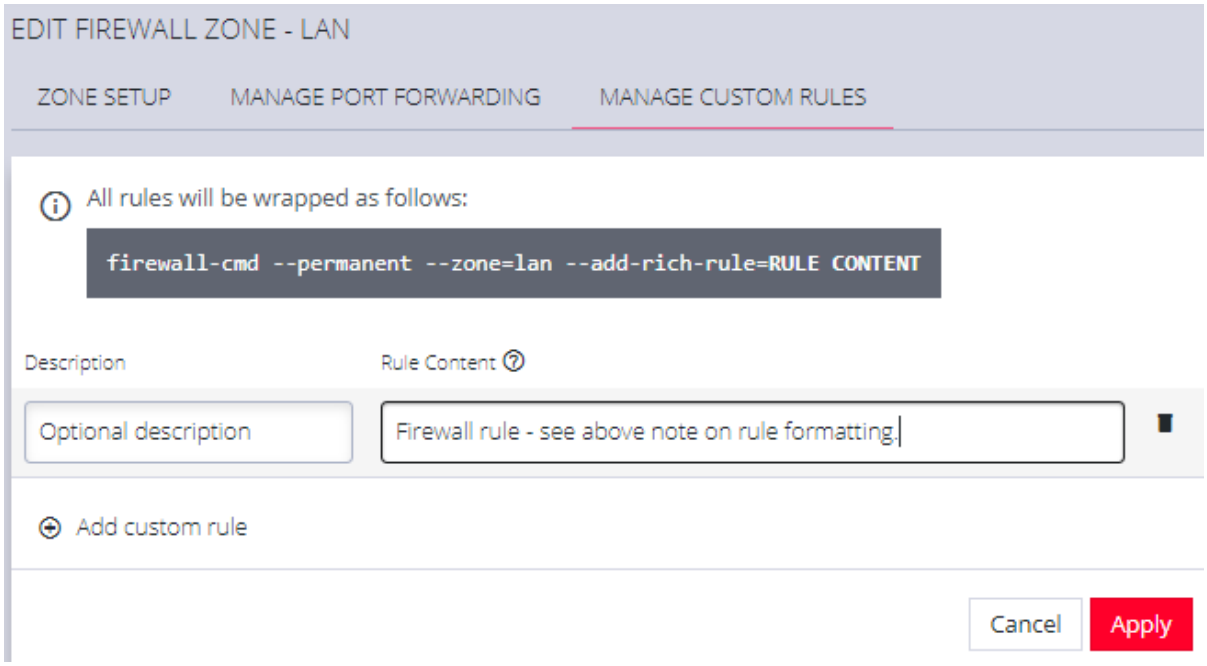


MANAGE CUSTOM RULES

> **Note:** The application of any custom rules will result in **Permit All Traffic** being enabled in a zone.

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

These rules are prioritized by the order they are added.



To add a new custom rule:

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**.

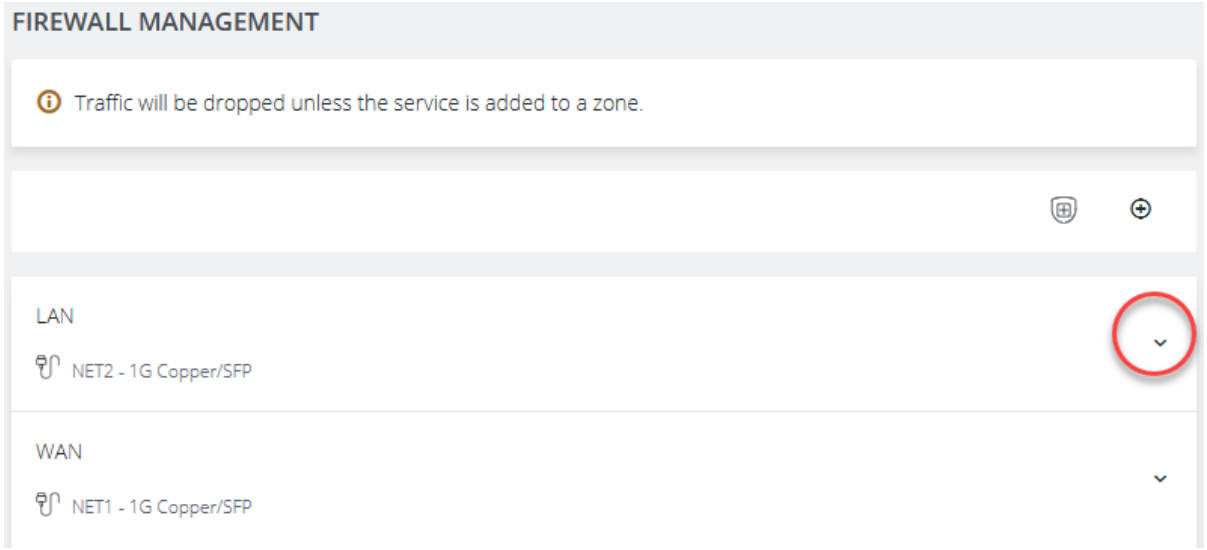
> **Note:** All rules are wrapped as follows:
> firewall-cmd --permanent --zone=lan --add-rich-rule=RULE CONTENT

FIREWALL SOURCE ADDRESS FILTERING

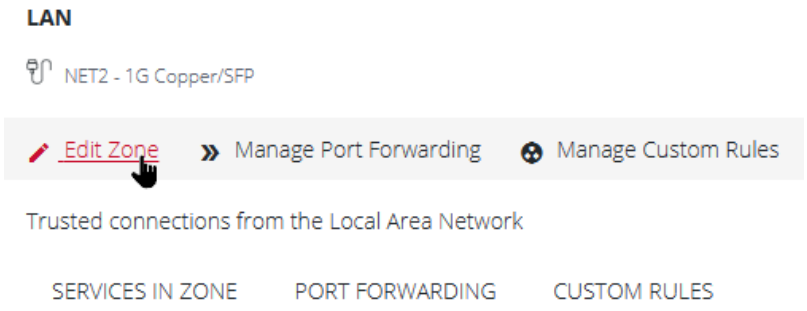
Source address filtering provides an interface by which users can permit access to services (for example, SSH, HTTPS, SNMP) on a device from specific source addresses.

This feature removes generic or global permitted services within firewall zones, and instead allows users to permit a service on a specified source address (or address range) within the firewall zone. Source address filters configured in a zone apply to all the interfaces within that zone.

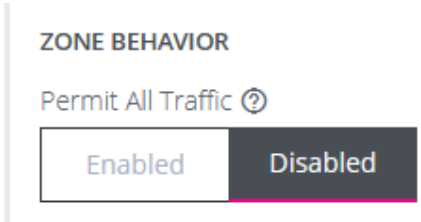
To access the feature, navigate to the **Configure > Firewall > Management** page through the WebUI then select the current source address filter configuration under the **services in zone** tab for each zone.



To add a source address filter for a zone, select the **edit zone** option under the required zone, which opens the **edit zone page** where source address filters can be configured.



You can choose to enable permit all traffic, which will permit all traffic in the zone (unless there is a custom rule configured overwriting this behavior).



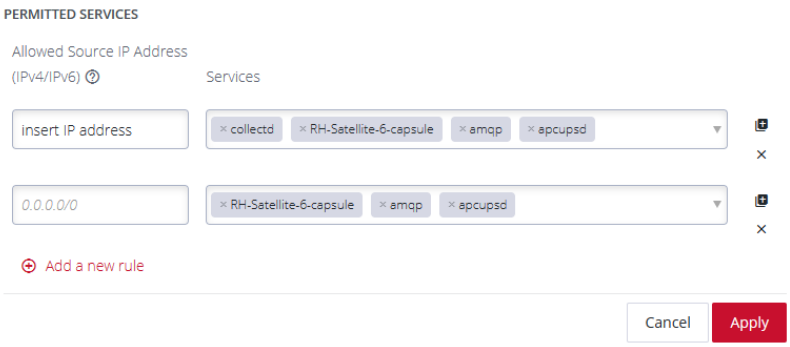
If the permit all traffic option is disabled, you will have the option to configure permitted services for any allowed source address. Permitted services can be added or removed from each source address filter under the "Services" field.

Source address filters can be added, duplicated or deleted by using the buttons below and to the right of the filter. Any new changes to the source address filters can be seen under the **services in zone** tab for each zone on the main firewall management page.

FIREWALL SOURCE ADDRESS BULK SERVICES

PERMITTED SERVICES

The firewall source ip field allows you to assign permitted services to specified source ip addresses in bulk rather than requiring individual rich rules to add each specific service. This change allows you to easily target specific IP Addresses with permitted services. Enter the target IP address, select services from the drop-down list and click **Apply**.



FIREWALL POLICIES

Firewall egress filtering may be used to allow or deny traffic leaving a device. This feature allows you to create firewall egress rules, which govern outgoing traffic leaving the device.

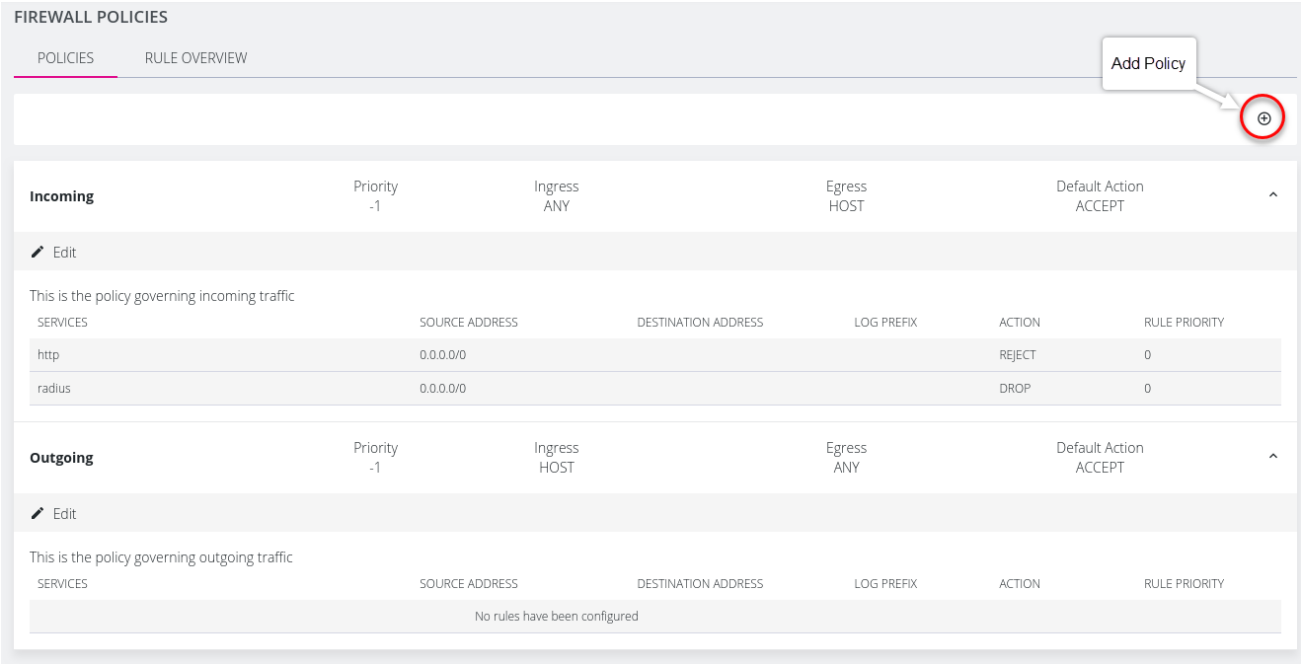
Firewall egress filtering extends the firewall/policies endpoint, allowing customization over both incoming (ingress) and outgoing (egress) traffic, thus allowing greater control of the device's security.

The feature allows you to:

- Change the default behavior of a firewall policy so it can accept or deny traffic moving between zones.
- Create, edit and delete firewall policy rules which allow or block specific service traffic based on IP addresses.
- Configure firewall policy rules through ogcli, Config Shell or the WebUI.
- Display and inspect rules in a single location in the WebUI.
- Create symbolic zones HOST and ANY which allow the creation of catch-all firewall policies affecting traffic incoming and outgoing all zones.

CREATING EGRESS POLICIES IN THE WEBUI

New policies or edits of existing policies are done from the Firewall Policies page. Navigate to **Configure > Firewall > Policies**, there is now an overview for firewall policies created on the device, as well as an overview page showing firewall policy rules created. To view firewall policy rules, click the drop-down arrow to the right of any policy row.



EGRESS POLICY DETAILS

New policies are created by first clicking on the **Add Policy** button at the top-right of the **Firewall Policies** page of the WebUI. New policies can have a user-defined default action, either ACCEPT, CONTINUE, DROP, or REJECT, which describes how traffic moving through the ingress and egress zones is treated. The ingress and egress zones may be configured as custom zones on the device through the firewall/zone endpoint, or can be symbolic (ANY/HOST) which represent traffic on all interfaces and the host device itself respectively. These default actions are described in the following table.

Default Action	Outcome
ACCEPT	All packets flowing between ingress and egress zones are accepted by default.
REJECT	Rejects every packet (a message warns that the connection was rejected and that packets will not be allowed through): `ssh: connect to host 10.236.3.7 port 22: Connection refused`

Default Action	Outcome
DROP	Drops every packet (users do not get a message, the connection hangs).
CONTINUE	Ongoing packets are subject to rules in following policies and zones.

CREATE A NEW FIREWALL POLICY

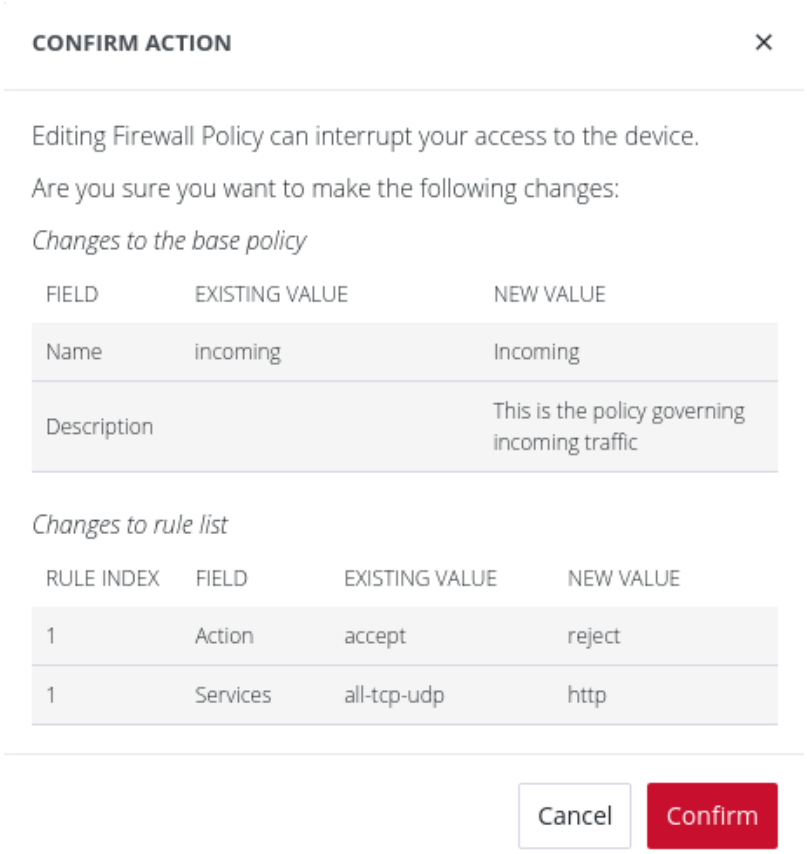
1. Click on the **Add Policy** button at the top-right of the **Firewall Policies** page of the WebUI.
2. Complete the **Name**, **Description**, **Default Action** and **Policy Priority** inputs of the New Policy.

> **Note: Policy Priority** - Policies with negative values are applied before any filtering rules in zones. Policies with positive values are applied after filtering rules in zones. A priority of 0 (zero) cannot be applied.

3. Select the required Ingress and or Egress zones.
4. Click on the **Add New Rule** button and complete the information; Source and Destination address, also Log Prefix are optional.
5. Click **Apply**. The new rule is instated.

EDITING POLICIES OR RULES

Rules associated with a policy can be edited. When saving their changes after editing, you are prompted to double check their changes using the **Confirm Action** window, which presents an overview of the policy changes.



Note: Editing a firewall policy or rule may interrupt access to the device.

CONFIGURE EGRESS POLICIES IN THE CONFIG SHELL

Firewall policies may be created through Config Shell as shown in the following example:

```
config: firewall/policy
config(firewall/policy): add incoming
config(firewall/policy incoming): default_action accept
config(firewall/policy incoming): egress_zones
config(firewall/policy incoming egress_zones): add host
config(firewall/policy incoming egress_zones): up
config(firewall/policy incoming): ingress_zones
config(firewall/policy incoming ingress_zones): add any
config(firewall/policy incoming ingress_zones): up
```

```
config(firewall/policy incoming): show
Entity firewall/policy item incoming
   default_action accept    *
   description                         ""
   name                                    incoming
   priority                                    -1
   egress_zones (array)
      0 host *
   ingress_zones (array)
      0 any *
   rules (array)
```

Policy Configurable Fields

default_action	The default action that is applied to packets that don't match any rule.
priority	The priority of the policy dictates when it is applied compared to other policies and zones. Policies with negative priorities are applied before rules in zones; policies with positive priorities are applied after. A priority of 0 is reserved for Rules and is not used for policies. The default value is -1.
egress_zones	Traffic directed to the egress zones is subject to this policy. This was pre-existing but has been expanded to include options for ANY/HOST.
ingress_zones	Traffic originating from the ingress zones is subject to this policy. This was pre-existing but has been expanded to include options for ANY/HOST.
rules	A list of rules that specify what happens to specific packets as they pass through the firewall policy.

CREATE RULES UNDER A POLICY - CONFIG SHELL

The rules that apply to a firewall policy may be created through Config Shell; as shown in the following example:

```
config(firewall/policy incoming): rules
config(firewall/policy incoming rules): add
config(firewall/policy incoming rules 0): show
Entity firewall/policy item incoming field rules 0
   action                          "" (required)
   destination_address ""
   log_prefix                     ""
   priority                           0
   source_address           ""
   services (array)
```

Rule Configurable Fields	
action	The action to apply to matching packets.
destination_address	The destination address to which this rule applies.
log_prefix	This sets the prefix of the info level log that is sent when this rule is hit. If it is empty, no logs are sent.
priority	The priority given to the selected rule. Rules with negative priorities are applied first. The default value is 0.
source_address	The source address to which this rule will apply. For multiple source addresses, a separate rule must be created for each address.

LOGGING AND DEBUGGING FIREWALL POLICIES

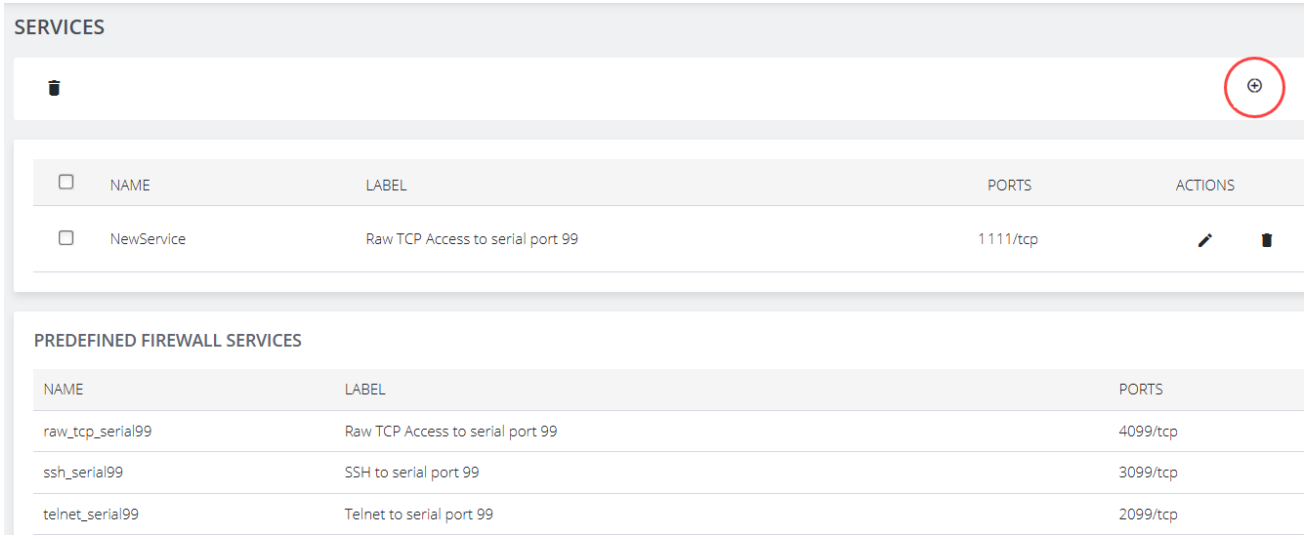
Some logging and debugging tools are provided for resolving firewall policy issues:

- List all firewall policies configured on the device: `firewall-cmd --list-all-policies`.
- Check the xml files which contain the firewall policy configuration information, under the /etc/firewalld/policies/ directory.
- Check the journal for firewall related messages: `journalctl -xeu firewalld`

> **Note:** `firewalld` is used to create firewall rules, `firewalld` is discussed in "Firewall Guide" on page 230.

FIREWALL SERVICES

The Firewall Services page of the WebUI provides a list of existing, predefined Firewall services and provides a means of creating, defining and editing services.



ADD WIREGUARD ZONES TO A FIREWALL

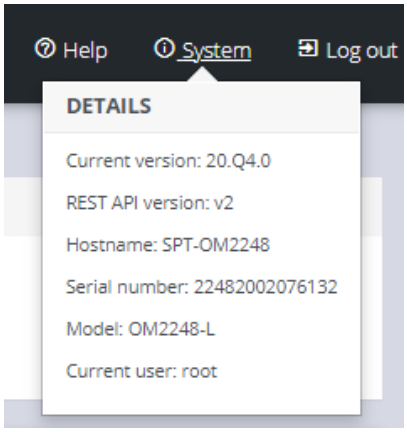
The WireGuard interface can be added to a firewall zone as in the following example:

```
Entity firewall/zone item zone
description "" (required)
label "" (required)
masquerade "" (required)
name zone
permit_all_traffic "" (required)
address_filters (array)
custom_rules (array)
physifs (array)
port_forwarding_rules (array)
wireguards (array)
```

SYSTEM

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

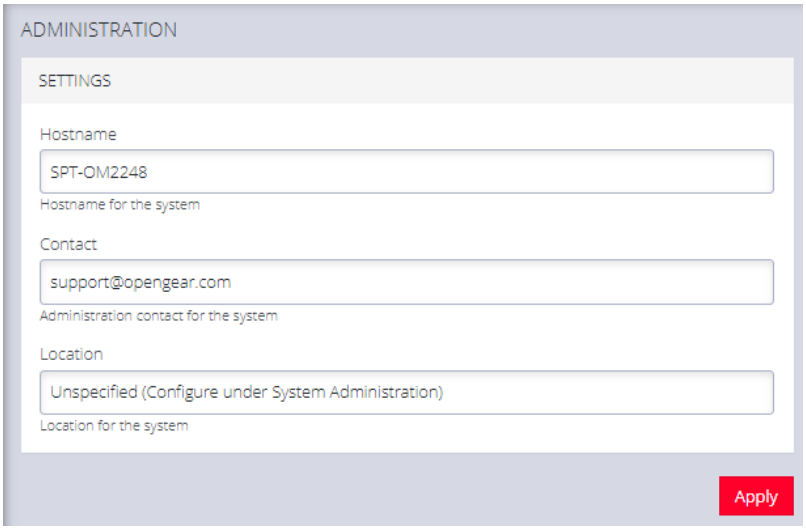
Click on the **System** link at the top-right of the CM window to check current system details.



ADMINISTRATION

To set the hostname, add a contact email, or set a location for the Console Manager:

1. Click **CONFIGURE > SYSTEM > Administration**.
   The **ADMINISTRATION** page displays.



2. Edit the settings as required:

Field	Description
Hostname	Enter a host name for the system.
Contact	Enter an administration contact email for the system.
Location	Enter a location for the system.

3. Click **Apply**.
   The new settings are saved.

DATE AND TIME SETTING

It is important to set the local Date and Time in your Opengear device as soon as it is configured. Features such as Syslog and NFS logging use the system time for time-stamping log entries, while certificate generation depends on a correct Timestamp to check the validity period of the certificate.

Your Opengear device can synchronize its system time with a remote Network Time Protocol (NTP) server. NTP uses Coordinated Universal Time (UTC) for all time synchronizations so it is not affected by different time zones.

You must specify your local time zone so the system clock shows correct local time. The Date & Time section of the navigation bar provides a means to:

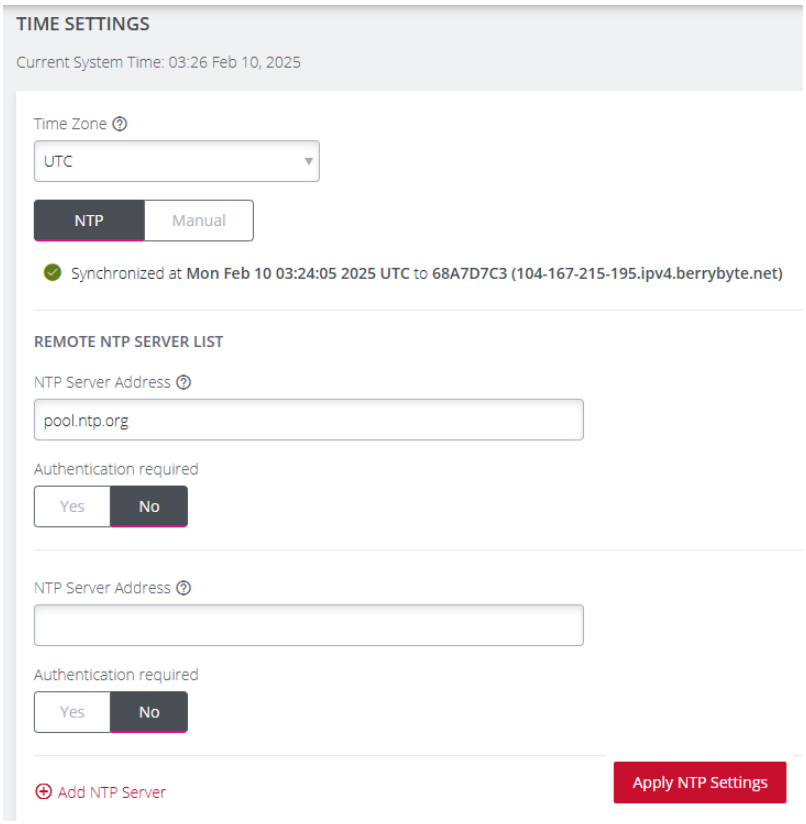
- Set the time zone.
- Manually set the correct time and date.
- Set the date and time by NTP Server.

SET THE TIME BY NTP

Configuring an NTP server ensures the Opengear device clock is kept accurate (when Internet connection has been established).

When defining an NTP server you can choose to supply an Authentication Key and Authentication Key Identifier or not to use Authentication. If NTP Authentication keys are in use, the NTP server must be verified using the Authentication Key and Authentication Key Index before synchronizing time with the server.

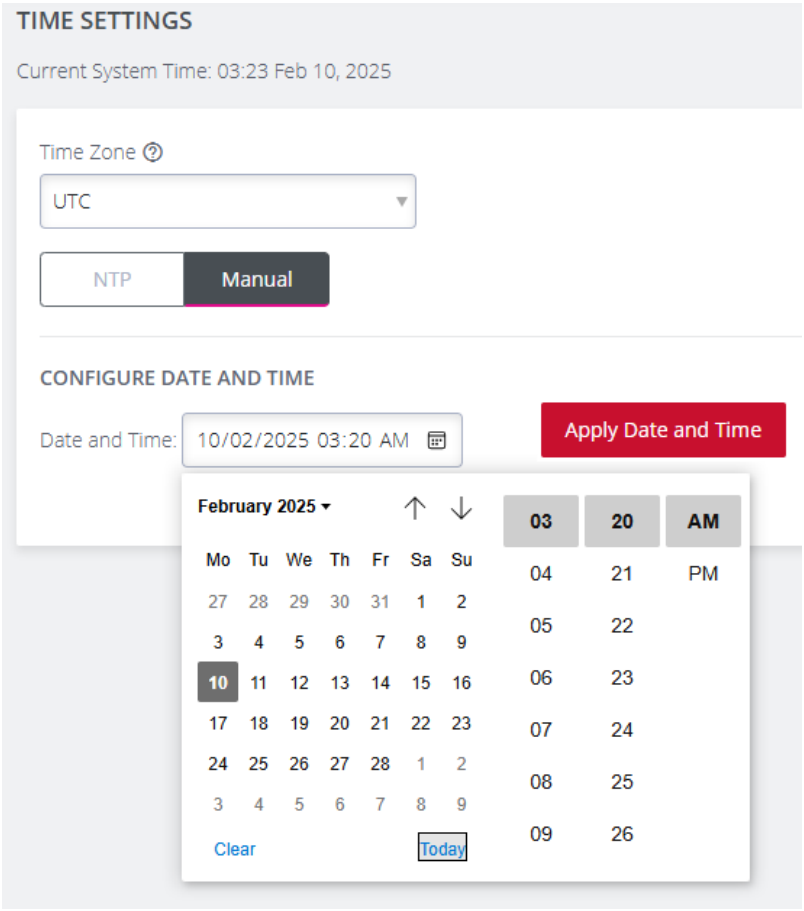
1. Navigate to the **CONFIGURE > DATE & TIME > Time Settings** page.



2. Select the Console Manager's time zone from the **Time Zone** drop-down list.
   A filter is provided to make selection easier.
3. Select the **NTP** option.
4. Enter the **NTP Server Address** and select whether Authentication is required.
5. Click on **Add NTP Server** if another NTP server is required and complete the address for the second NTP server.
6. Click **Apply NTP Settings**.

SET THE TIME MANUALLY

1. Navigate to the **CONFIGURE > DATE & TIME > Time Settings** page.



2. Select the Console Manager's time zone from the **Time Zone** drop-down list.
   A filter is provided to make selection easier.
3. Select the **Manual** option.
4. Under **Configure Date and Time**, click on the calendar icon to open the Date and Time Picker.
5. Either select the date and time manually or simply click **Today** to set the current date/time.
6. Click **Apply Date and Time**.

FACTORY RESET

You can perform a factory reset at the UI by pressing the **Factory Reset** button (CONFIGURE > SYSTEM > Factory Reset) or at the external **Erase** button, or from the **CLI**. All three methods are covered in this topic. During a factory reset the device is reset to the factory default.

> **Note:** During the reset process, the software driven LEDs on the front of the device (Power, Heartbeat, Network Activity, Serial Activity, Cellular) may take several seconds to appear ON. The LEDs are as described in the LED Status table. Note that the Power LED may appear to be OFF during part of the reboot process; this is a normal stage of the reboot process.

See Device Status LEDs for notes about device LED status.

RESET FROM THE WEBUI

To return the Console Manager to its factory settings:

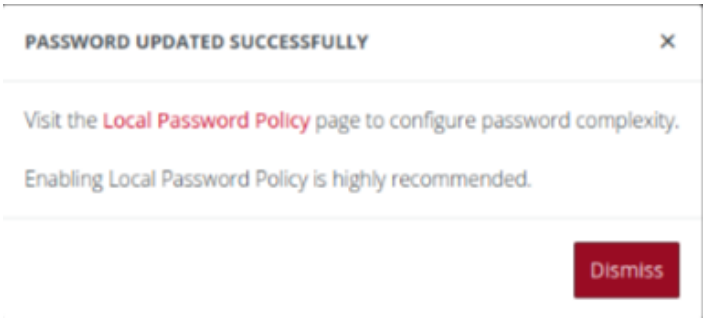
1. Log in to the Web UI as a user with Admin privileges.
2. Navigate to **CONFIGURE > SYSTEM > Factory Reset**.
3. Read the Factory Reset warning notice.

   > **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 node are lost. Please check the box below to confirm you want to proceed.

4. If you still want to proceed with the reset, select the **Proceed with the factory reset** checkbox.
5. 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 are prompted to log in and must enter the default administration username and administration password (Username: root Password: default). You are required to change this password during the first log in.

6. CONFIRM the message "Factory reset initiated. System will reboot in ten seconds." displays.
7. CONFIRM the appliance is undergoing a system reboot.
8. The 'Power' and 'Heartbeat' LEDs display orange briefly, then go off after approximately five seconds.
9. Wait for LEDs to indicate the device has rebooted normally (see LED Status below).
10. Log in to WebUI or CLI. Use the default password for initial login, then, change password in accordance with the local password policy.



RESET AT THE EXTERNAL ERASE BUTTON

1. Press the external physical **Erase** button on the device once.

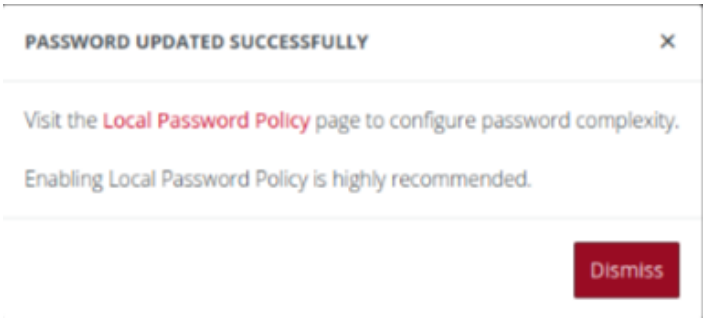
   > **Note:** On most devices the button is at the front panel, near the LEDs. On the OM1200 the button is on the rear, near the power inlet).

2. CONFIRM all LEDs come on.
3. Press the physical **Erase** button on the device a second time within five seconds.

   > **Note:** If the **ERASE** button is not depressed within five seconds of the LEDs turning on, the appliance resumes normal operation.

4. The 'Power' and 'Heartbeat' LEDs display orange briefly, then go off after approximately five seconds.
5. Wait for LEDs to indicate the device has rebooted normally (intermittently flashing heartbeat changes to green, see LED Status below).

6. Log in to WebUI or CLI. Use the default password for initial login, then, change password in accordance with the local password policy.



RESET FROM THE CLI TERMINAL

1. Log in at the CLI terminal, then enter:

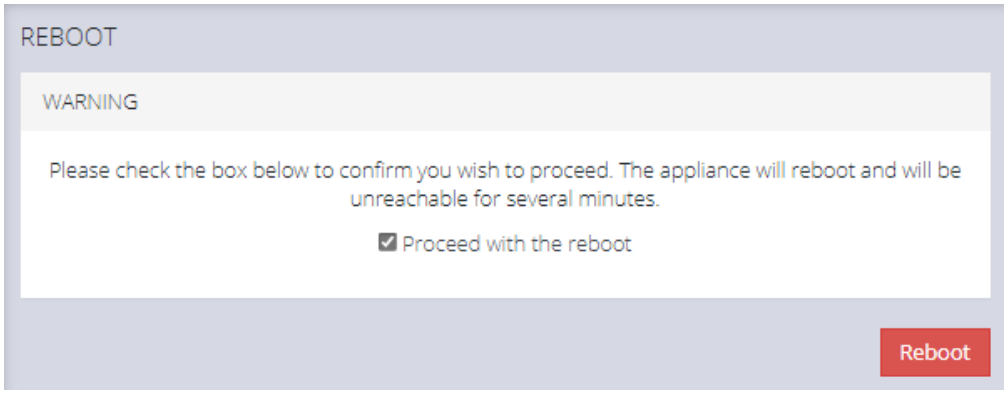
```
root@om2248-1-tp1-p14:~# factory_reset
```

2. Confirm: Factory reset system? [yes/no]:
3. Follow the procedure from step 2 in the 'Erase button' procedure above.

REBOOT

To reboot the Console Manager:

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



For detailed information about device behavior that may occur during a factory reset procedure, see Factory Reset.

EXPORT/RESTORE CONFIGURATION

EXPORT CONFIGURATION

The current system configuration can be downloaded as a plain text file. It contains all configuration performed via the WebUI and the ogcli tool. It does not contain log files, user scripts, docker containers, service configuration or other files stored via other means.

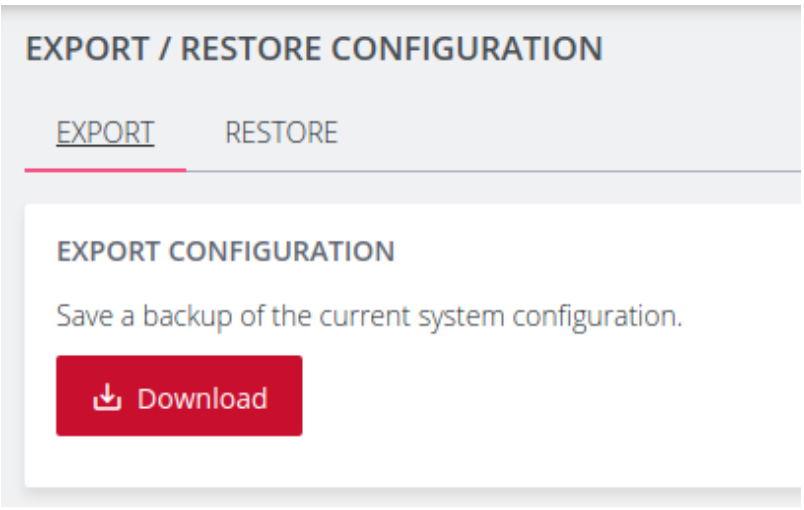
The exported configuration may be useful for:

- Disaster recovery.
  - issues with system upgrades.
  - unexpected configuration changes.

- Replacing devices after RMA.
- Configuration templating.

EXPORT CONFIGURATION VIA WEBUI

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 are obfuscated in the configuration export.

> **Note:** The default filename includes the system hostname and a timestamp. For example, **cm8148_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.

RESTORE CONFIGURATION

An exported system configuration can be imported to the node using the WebUI or ogcli tool.

> **Notes:**
>
> - If the configuration was exported using **--secrets=mask**, it cannot be used for configuration import.
> - It may take up to ten minutes to import a config file with a large amount of configuration.

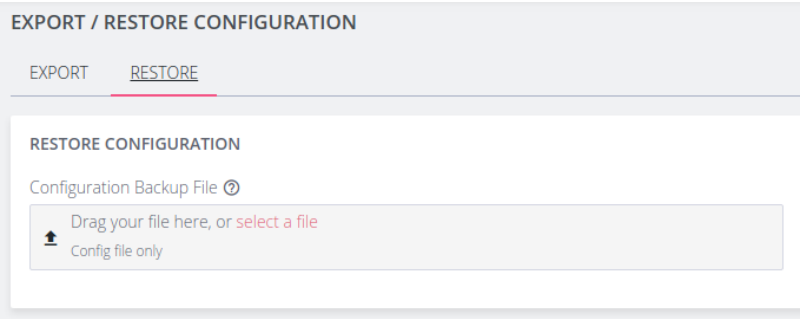
RESTORE CONFIGURATION VIA WEBUI

Importing configuration using the WebUI will use the restore strategy. Restoring configuration will override all settings on the node.

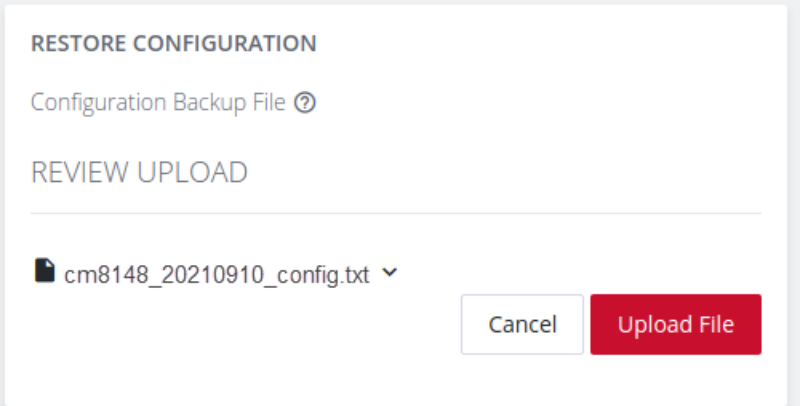
Only configuration from the same version and model can be restored.

To restore the system configuration:

1. Click the **Restore** tab



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



4. Click the **Upload File** button to start the import process.
   A green banner displays 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 is 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.

> **Note:** Restoring a configuration file may take up to three minutes for large files.

As an administrative user, run the following command:

```
ogcli restore <file_path>
```

AUTOMATED ROLLBACK TO WORKING CONFIGURATION

'Config Rollback' provides an automated rollback mechanism that ensures a device will automatically revert to its last known working configuration in case of a failed restore. Automated Rollback is the default configuration of this feature and cannot be overridden or configured for manual operation.

Rollback maintains operational stability, ensuring the system does not become partially upgraded due to some error during upgrade. The ability to roll back to a previously safe configuration minimizes downtime and service disruption, making it a vital addition to the system's resilience.

Rollback behavior in the event of a detected restore failure:

The system automatically detects a configuration update failure. On detection of a failure, the system automatically initiates a rollback to the last known working configuration without user intervention until a known working configuration is successfully installed.

```
root@om2248:~# ogcli restore restore.txt
⋮    restoring data

restore failed with the following error(s):
Error(s) detected during REPLACE operation on services/snmp_alert_managers
Adding record 1 from the list of supplied records has failed
Error: 'bad_address' is not a valid network address
Error: Push command failed

⋮    rolling back config
rollback successful
```

UPDATING THE IMPORT/RESTORE FILE

The import/restore file must follow a very specific format; deviation from format should be avoided. Comments and blank lines are allowed but any commands not starting with either ogcli or config must be in proper heredoc format, see the following example (note the <<'END' format, this is the only heredoc marker allowed).

> **Note:** Inline comments will not work.

```
config replace system/session_timeout <<'END'
  cli_timeout=0
  serial_port_timeout=0
  webui_timeout=20
END
```

ROLLBACK CAPABILITIES

- When the system initiates a rollback, it logs to syslog, prints a message in the CLI, and displays a pop up “toast” notification in the WebUI.
- This system is resilient to network issues; when Rollback is started it continues without the user being connected to the network.
- If a user sends a ctrl-c signal during restore/import the system also begins a rollback.
- If a user sends a ctrl-c signal during the rollback it is ignored. This is to ensure that the system does not enter a bad state.
- Users cannot start another restore/rollback if there is already one running on the system, a warning is issued.

ROLLBACK LIMITATIONS

- Config diff and Rollback can be used by any user with Administrator permission and access to the shell. It is initiated via the WebUI or command line.
- Only one import/restore and rollback is permitted on the box at any time.
- Rollback cannot be initiated without a failing import/restore.
- Rollback cannot be initiated to a specific version.
- Rollback does not support manual intervention and when rollback is initiated it cannot be stopped.
- Rollback cannot be initiated after import/restore is complete.

LIGHTHOUSE NODE BACKUP

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

For more information, see the latest Lighthouse User Guide.

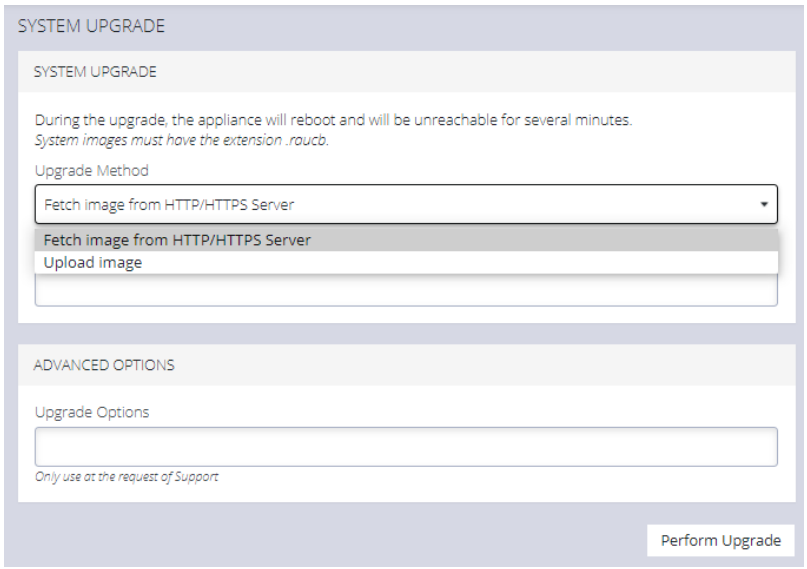
SYSTEM UPGRADE

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 is unavailable for several minutes and then reboots. Unlike a factory reset, users, and other configuration data is maintained after the upgrade.

PERFORM A SYSTEM UPGRADE VIA WEBUI

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

> **Note:** See https://opengear.com/support/device-updates/ for firmware updates.



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.

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

PERFORM A SYSTEM UPGRADE VIA CLI

1. Log in to the CLI as an administrator or root user.
2. Use one of the following methods to perform the upgrade:
   - Load an raucb file from a remote URL:

     ```
     sudo puginstall --reboot-after https://ftp.opengear.com/download/opengear_appliances/OM/current/operations_manager-YY.Qn-public.raucb
     ```

   - Copy the raucb file to the Operation Manager's /tmp directory using scp, WinScp or similar, then load the local file:

     ```
     sudo puginstall --reboot-after /tmp/operations_manager-YY.Qn-public.raucb
     ```

   The Console Manager writes the upgrade to its storage and reboots. This may take a few minutes.

> **Note:** To check the version before or after the upgrade, run `cat /etc/version`.

ADVANCED OPTIONS

The Console 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

password : LH global or bundle enrollment password

bundle : Name of LH enrollment bundle

COMMUNICATE WITH THE CELLULAR MODEM

> **Note:** This section applies to cellular variants only. The CM8000 does not support cellular connectivity.

Interfacing with the cellular modem is only available via CLI.

Usage	
`mmcli [OPTION?]`	Control and monitor the ModemManager.

Option	Description
`-h, --help`	Show help options
`--help-all`	Show all help options
`--help-manager`	Show manager options
`--help-common`	Show common options

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

5G SETTINGS AND BEHAVIOR

STANDALONE VERSUS NON-STANDALONE OPERATION

The 10G-C modules can connect in either standalone (SA) or non-standalone (NSA) mode.

5G-NSA employs a simultaneous 5GNR and LTE core connection. Data transfer occurs over 5G, while control aspects of the network use 4G technology. Depending on the carrier, the 5G connection may go dormant when inactive, activating either when data transfer begins or after a certain data transfer threshold.

To show which network the module is connected to, use the AT!COPS? command, which returns the following:

```
+COPS: [selection mode],[operator format],[operator],[access technology]
```

Example:

```
root@cm8196-10g-c-tp2-p29:~# mmcli -m a --command='AT+COPS?'
response: '+COPS: 0,0,"Telstra",13'
```

This example shows access technology 13 (5G-NSA), which corresponds to the following table.

2 (UTRAN)	3G
7 (E-UTRAN)	4G
11 (NR connected to a 5GCN)	5G SA
13 (E-UTRA-NR dual connectivity)	5G NSA

DETERMINE 5G STATUS

Determining the 5G status requires two commands:

- AT+COPS? : First, use this command to see if there is a 5G-NSA connection (see above).
- AT!GSTATUS? : Then, run this command and check if system_mode is LTE (to indicate that 5G is dormant) or ENDC (to indicate that 5G is active).

FORCING A 5G OR LTE CONNECTION

To force a 5G or LTE connection, use the “nas-set-system-selection-preference” and “AT!RATCONFIG” commands:

Action	Command Example
Force 5G-SA	`qmicli -p -d /dev/wwan0qmi0 --nas-set-system-selection-preference="5gnr",automatic`
Disable 5G-NSA	`AT!RATCONFIG="NR",2` `qmicli -p -d /dev/wwan0qmi0 --nas-set-system-selection-preference="lte|5gnr",automatic`

Action	Command Example
Force 5G-NSA	`AT!RATCONFIG="NR",1` `qmicli -p -d /dev/wwan0qmi0 --nas-set-system-selection-preference="lte|5gnr",automatic`
Force LTE	`qmicli -p -d /dev/wwan0qmi0 --nas-set-system-selection-preference="lte",automatic`

RUN DIAGNOSTICS WITH MODEM-TEST

Command	Description
`modem-test`	The `modem-test` command runs diagnostic and state tests on the cellular modem.

Options	
`-h, --help`	Show this help message and exit.
`-o {Output.TEXT,Output.JSON,Output.SUPPORT,Output.ZIP}, --output`	The test output format. If a format is not provided, the default output is text.
`-p, --privileged`	Run privileged tests, the modem will be rebooted.
`-n, --no-color`	Display terminal text in mono-chrome.
`-i MATCH_TEST_IDS, --match-test-ids MATCH_TEST_IDS`	Wildcard pattern matching test IDs to run.

Options

`-t {Type.AT,Type.QMICLI},--match-test-type {Type.AT,Type.QMICLI}`	Only run the matching test type.
`--input-file INPUT_FILE`	Read test results from the given JSON file.
`--output-file OUTPUT_FILE`	Output test results to the given file.
`-v, --verbose`	Display extra debug information.

Syntax

```
modem-test [-h] [-o {Output.TEXT,Output.JSON,Output.SUPPORT,Output.ZIP}] [-p] [-n]
[-i MATCH_TEST_IDS] [-t {Type.AT,Type.QMICLI}] [--input-file INPUT_FILE] [--output-
file OUTPUT_FILE] [-v]
```

Examples

Run all non-provileged tests and output in text format without color:

```
$ modem-test --no-color
```

Run all tests including privilieged and output in support-report format:

```
$ modem-test --privileged --out=support
```

Only run all 'network' and 'data' category tests and output as JSON:

```
$ modem-test -i network/* -i data/* --out=json
```

Run all 'device' category tests using AT commands and output in zipped support-report format:

```
$ modem-test -i device/* -t at --out=zip
```

Run all tests using QMI and output in text format:

```
$ modem-test -t qmi --out=text
```

Only run the support/module-detect test and output in the default text format:

```
$ modem-test --match-test-ids=support/module-detect
```

CONFIG CLI GUIDE

The Config Command Line Interface(CLI) provides users with an interactive and familiar environment similar to other networking devices that users may be familiar with. The result is a user-experience that feels like an Interactive CLI .

Advantages of the Config CLI are:

- Interactive CLI makes everyday operations such as configuration changes and troubleshooting activities easier for users.
- Items can be created or updated without being applied immediately.
- Items that are not applied are indicated by an asterisk (*) beside them when viewing information..
- Tab complete is supported for many commands.
- Built-in context sensitive help.
- Has a structured, tabular view when displaying lists of data.

NAVIGATION IN CONFIG CLI

START A SESSION IN CONFIG CLI

Start the Config Shell by typing `config` at a bash prompt. The bash prompt is presented to root and Administrator users when they log in via SSH or on the management or local console.

EXIT A CONFIG CLI SESSION

You can exit the Interactive CLI by in any of the following ways:

- Type `exit` to end the session.
- Send an EOF (Control+D).
- Send an INT (Control+C).

> **Note:** The session is prevented from exiting if there are un-committed changes, this condition is indicated by a message. However, you can force an exit by immediately executing an exit command again, any un-committed changes are discarded.

NAVIGATE THE CONFIG CLI

The Config CLI operates using a hierarchy . Due to the variety of endpoints, there are several ways to get to a place where you may want to make changes.

- Starting at the root, enter endpoint names to descend down to lower endpoints.
- Similarly, type 'up' to ascend towards the root or type 'top' to reset to the root context.

> **Note:** Every endpoint name is an operation that descends into that endpoint.

When using the config CLI, it is possible to navigate ‘downwards’ through multiple contexts with a single command line.

HIERARCHICAL IDENTIFIERS

This section outlines the identifiers required to navigate the CLI.

Identifier	Description
Singleton endpoints	These require only the endpoint name to be uniquely identified.
List/item endpoints	The first level is the endpoint name, the second level is the item identifier (the identifier is the same identifier used by ogcli).
Multiple identifiers	A single endpoint (ssh/authorized_keys) requires an extra identifier. In this case, the hierarchy is: ssh/authorized_keys > userid > [key_id]
Nested fields	The interactive CLI treats nested fields as additional hierarchy levels. This applies both to arrays and maps. For arrays of complex values, each value shall also be a hierarchy level.

UNDERSTAND FIELDS, ENTITIES AND CONTEXTS

The Config CLI allows you to configure the device settings through a number of required fields, which provide the settings for the device.

These fields are grouped in *entities* that describe a small set of functionality, for example, there is a ‘user’ entity which is used to access user settings. Entities can contain sub-entities as well as simple fields.

HOW CONTEXT OPERATES IN THE CONFIG CLI

Description

The *context* is the current entity that is the focus of the Config Shell. When the shell is first started, the context is a special parent context from which sub-entities can be seen. Within the Config Shell, a number of commands are available, depending on the current context.

When Config Shell is started the context is at the “top context” which lists all the entities when the show command is used. If the name of an entity is typed, then the context moves 'down' into that entity. When simple commands such as `show`, `help` or `apply` are used, they will act on the current context. The context can be moved down further by typing the name of an item.

Entities can contain sub-entities as well as simple fields. For example, there is a ‘user’ entity which is used to access user settings. Fields are grouped within entities that describe a small set of functionality.

Navigating Using Context

You select a context by typing the name of the target entity and pressing Enter/Return; the new context is shown in the prompt between brackets. In the following example, the ‘`user`’ context is accessed and then the ‘`john`’ sub-entity is accessed causing the context to become ‘user john’.

The ‘`show`’ command is used to list the entities and fields that descend from the current context.

```
config: user
config(user): show
Item names for entity user
  john matt myuser netgrp root
config(user): john
config(user john):
Entity user item john
  description
  enabled        true
  no_password                false
  password
  ssh_password_enabled true
  groups (array)
config(user john):
```

The following example will navigate the context to the root user object without first having to navigate to the user context:

```
config: user root
config(user root):
```

Sub-objects are supported. In the following example, power_supply_voltage_alert and syslog are nested sub-objects of the onitoring/alerts/power entity:

```
config: monitoring/alerts/power power_supply_voltage_alert syslog
config(monitoring/alerts/power power_supply_voltage_alert syslog):
```

GLOBAL & ENTITY-CONTEXT COMMANDS

GLOBAL CONTEXT COMMANDS

The following table lists commands available on any context:

Global Command	Description
`help (or '?')`	Show help which is context sensitive. It will list some special details about the current context, the list of sub entities (or fields) and a list of available commands.
`help <entity>`	Displays short-form help for the specific entity.
`show`	Lists the available entities and fields.
`<entity>`	Inputing the name of an entity changes the context to focus on the named entity.
`exit`	Exit the command shell.

ENTITY CONTEXT COMMANDS

In addition to the global context commands, when an entity context is selected then further, entity context, commands become available.

Entity Command	Description
`<field>`	Show the value of a field.
`help <entity>`	Displays short-form help for the specific entity.
`<field> <value>`	Set the value of a field.
`delete`	Deletes the current enitity. This is available when the context entity is an item in a list.
`add`	Append a sub-entity or field to the current entity. This is only available when the context entity is a list.

CONFIG CLI ENTITIES

The Config Shell allows the user to configure a number of fields which are the settings for the device. These fields are grouped in entities that describe a small set of functionality. For example, there is a ‘user’ entity which is used to access user settings. Entities can contain sub-entities as well as simple fields.

When in the shell, a number of commands are available depending on the current context. The context is the current entity that is the focus of the Config Shell. When the shell is first started, the context is a special parent context from which sub-entities can be seen.

When a context is selected by typing the name of the entity, it is shown in the prompt between brackets. e.g. In the following snippet, the ‘user’ context is accessed and then the ‘john’ sub-entity is accessed causing the context to become ‘user john’. The ‘show’ command is used to list the entities and fields that descend from the current context.

SUPPORTED ENTITIES

Entity	Definition
access_right	An access right is a permit that grants the holder access to a feature or collection of related features.
auth	Configure remote authentication, authorization, accounting (AAA) servers.
auto_response/playbook	Read and manipulate Auto-Response beacons and reactions for playbooks.
auto_response/status	Read the AutoResponse Status on the NetOps Console Server appliance.
auto_response/status/beacon-module	Read the AutoResponse Status of Beacon Modules on the NetOps Console Server appliance.
cellfw/info	Retrieve cellular modem version and related information.
cellmodem	Retrieve information about the cell modem.
cellmodem/sim	Cell modem SIM status.
conn	Read and manipulate the network connections on the NetOps Console Server appliance.

Entity	Definition
diff	config diff performs a comparison of the active configuration and an input configuration file, which is the product of the ogcli export <template-file> operation. Config diff shows additions, removals and changes clearly in the a streamlined format with only functional differences between the input and running configurations. See also ogcli diff.
failover/settings	failover/settings endpoint is to check and update failover settings. When failover is enabled, this device will consume from 1MB to 1.6 MB of bandwidth per day on the probe_physif connection. If the probe addresses are unreachable, this device will take from 108 to 156 seconds to enter the failover state.
failover/status	failover/status endpoint is to check current failover status.
firewall/policy	A collection of policies defined for the NetOps Console Server appliance's firewall. A policy specifies which zones traffic is allowed to route between.
firewall/predefined_service	A collection of predefined services for the NetOps Console Server appliance's firewall. A service is a named grouping of one or more TCP or UDP ports for a particular networking protocol. For example, the 'https' service refers to TCP port 443. This collection contains predefined services for common protocols and doesn't include the services added by the Administrator.
firewall/service	A collection of custom services defined for the NetOps Console Server appliance's firewall. A service is a named grouping of one or more TCP or UDP ports for a particular networking protocol. For example, the 'https' service refers to TCP port 443. The appliance includes many predefined services for common protocols (see /firewall/predefined_services). This collection contains only custom services which have been defined by the Administrator.
firewall/zone	Collection of zones defined for the NetOps Console Server appliance's firewall. A zone includes 1 or more interfaces.
group	Retrieve or update user group information.
ip_passthrough	IP Passthrough endpoints are for retrieving / changing IP Passthrough settings.

Entity	Definition
ip_passthrough/status	The IP Passthrough status endpoint provides information about what part of the IP Passthrough connection process the device is currently at and information about the connected downstream device.
ipsec_tunnel	Read and manipulate the IPsec tunnels on the NetOps Console Server appliance.
lighthouse_enrollment	View and control enrollment to a lighthouse.
local_password_policy	Configure the password policy for local users. This includes expiry and complexity settings.
logs/portlog	None
logs/portlog_settings	Check and update port log settings.
managementport	Used for working with local management console information.
monitor/brute_force_protection/ban	Used for monitoring addresses banned by Brute Force Protection.
monitor/lldp/chassis	Get the current status of the network discovery (LLDP/CDP) protocols on this device.
monitor/lldp/neighbor	Get the list of neighboring devices (peers) that have been discovered by the LLDP protocol.
monitor/static_routes/ status	Used for monitoring the status of static routes. Only IPv4 static routes are supported.
monitoring/ alerts/networking	Retrieve and configure Networking Alert Group settings.

Entity	Definition
monitoring/alerts/power	Retrieve and configure Power Alert Group settings.
monitoring/alerts/system	Retrieve and configure System Alert Group settings.
pdu	Configure, monitor and control PDUs connected to the device.
pdus/drivers	Read the PDU driver list.
physif	Read and manipulate the network physical interfaces on the NetOps Console Server appliance.
port	Configuring and viewing ports information.
port_session	None.
ports/ auto_discover/schedule	Manage Port Auto-Discovery Scheduling.
ports/status_port	Provides information about the serial pin status and Tx & Rx counters for each of this device's serial ports.
system/admin_info	Retrieve or change the appliance system's information (hostname, contact and location).
services/ brute_force_protection	Provides access to the Brute Force Protection configuration on the system. When this service is enabled, the system watches for multiple failed login attempts and temporarily bans the offending IP Address for the configured amount of time.
services/lldp	Provides access to the Network Discovery Protocols (LLDP/CDP) configuration.

Entity	Definition
services/ntp	Provides access to the NTP client configuration on the system.
services/routing	Retrieve and configure routing services on the NetOps Console Server appliance.
services/snmp_alert_manager	SNMP Alert Managers are used to receive and log SNMP TRAP and INFORM messages sent by the NetOps Console Server. To receive SNMP alerts generated by the system at least one SNMP Alert Manager must be configured.
services/snmpd	Simple Network Management Protocol (SNMP) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behaviour. This entity allows configuration of the SNMP service.
services/ssh	Configure the Secure Shell Protocol (SSH) service.
services/syslog_server	Provides access to the remote syslog server configuration.
services/tftp	Trivial File Transfer Protocol (TFTP) is a service that allows files to be transferred to or from the NetOps Console Server appliance. This entity provides access to the TFTP server configuration on the system.
single_session	Can be enabled on a given port to prevent multiple users from connecting to that port or limit the port to a single concurrent connection.
ssh/authorized_key	Configure the SSH authorized keys for a specific user.
static_route	Configuring and viewing static routes.
system/admin_info	Retrieve or change the NetOps Console Server appliance system's information (hostname, contact and location).

Entity	Definition
system/banner	Retrieve or change the appliance system's banner text.
system/cell_reliability_test	None.
system/cellular_logging	Cellular logging provides the ability to capture the RRC connection messages from the EM7565 cellular module. This entity allows configuration of cellular logging and is only to be used during compliance testing.
system/cloud_connect	Retrieve or change the appliance system's cloud connect configuration.
system/diskspace	Retrieve the system's Disk Space usage.
system/info	Retrieve basic system information.
system/model_name	Retrieve the appliance's Model Name.
system/serial_number	Retrieve the appliance's Serial Number.
system/session_timeout	Retrieve or change the appliance session timeouts.
system/ssh_port	The SSH port used in Direct SSH links.
system/ system_authorized_key	Configure the SSH authorized keys for all users.
system/time	Retrieve and update the NetOps Console Server's time.
system/timezone	Retrieve and update the system's timezone.
system/version	Retrieve the appliance's most recent firmware and REST API version.
user	Retrieve and update user information.

CONFIG CLI COMMANDS

Command	Definition
add	Add a new item for an entity.
apply	Apply changes on just the current entity.
changes	View a list of config areas with unapplied changes.
delete	Delete an item for an entity.
diff	Show additions, removals, changes and functional differences between the input and running configurations. See also `ogcli diff`.
discard	Discard changes on just the current entity.
edit	Making changes to configuration options without navigating through the hierarchy.
exit	Leave config mode without applying changes.
help / ?	Display the available options for the configuration section. Can be used in combination with a command or configuration option to access help documentation.
import/export	Copy a config file from a specific network location to the console server and run the file. The import/export commands operate in bash, ie. outside of config CLI. You must exit config to operate the import/export features.
modem-test	Run diagnostic and state tests on the cellular modem.
show	Display information relevant to the configuration section, highlighting changes.
up/exit/ ..	Allows users to traverse the configuration hierarchy.

ADD

The `add` command adds a new item for an entity. The add command requires a unique value to identify the record. This is used for the entity's label field.

You can use the **add** command:

- anywhere within the command structure to begin the process of progressively adding an element.
- as part of a single line command where an element is added and simple fields are set.

Parameters

`entity`	The entity to which the new item is added.
`label`	A unique value to identify the record.
`field`	Optional field to set for the item.
`value`	Optional value corresponding to the field.

Syntax

```
add <entity> <optional-entity> <label> <optional-field> <optional-value>
```

Example

```
add user aconsoleuser description "I am a console user"
```

APPLY

The `apply` command allows you to stage configuration changes by allowing proposed changes to be held in memory, separate from active configuration until they are applied.

This may be considered from a user perspective like this:

"When I am adding users and realize that groups are missing, I can take a pause and add the groups without having to discard my work so far."

or

"When I am in the process of creating a new firewall zone but there is required service missing, I can go off and add the service and come back without losing changes."

You can choose to apply changes in the following manner:

- Isolated changes that are specific to sections of configuration.
- Across all configurations.

Parameters

When no parameters are provided, the command applies the changes in the current item context. For example, if the current context is `user consoleuser`, any changes to the `consoleuser`user are saved. If the `apply` command is used outside of an item context, this results in an error.
`apply all` - When the '`all`' parameter is added, the command applies all changes to all items that have been changed in this session.

Syntax

`apply` [`all`]

Example

Apply changes to a single item

These commands change a user. Then the apply command is used while still in the “user myuser” item context so only changes to this user are applied:

```
config: user myuser
config(user myuser): password secret123 description "This is my user"
config(user myuser): apply
```

Example

Apply all Changes

These commands add a new group and then change a port setting. At the end, the apply all command saves both the group and port items.

```
config: add group mygroup
config: group mygroup
config(group mygroup): access_rights
config(group mygroup access_rights): add pmshell
config(group mygroup access_rights): up
config(group mygroup): ports
config(group mygroup ports): add port01
config(group mygroup ports): top
config: port port01
config(port port01): label "Port for my group"
config(port port01): top
config: apply all
```

Apply Changes to Specific Sections of Configuration

From within a specific section of hierarchy the following example applies any changes made specifically within the user's configuration section.

```
config users johnsmith
apply
```

Example

Apply changes from a different section in the hierarchy

For example, if changes have been made in

```
config users johnsmith
```

but the user has moved elsewhere in the hierarchy, the command:

```
apply users johnsmith
```

applies any changes made specifically within the user's configuration section.

Alternatively, a user might choose to apply all changes in the user list using the following command:

```
apply users
```

Using `apply` across all configurations

```
apply
```

```
apply all
```

CHANGES

The `changes` command allows you to view a list of config areas with unapplied changes.

This displays as a list, ordered alphabetically. You should be able to copy and paste items from the list and use it in conjunction with the show command to view details.

Parameters

None

Syntax

changes

Example

The following example shows changes made to multiple users and a port:

```
config: edit user root description "New description"
config: add user newuser description "New User"
config: edit port port01 baudrate 115200
config: changes
Entity user item root (edit)
 description New description
Entity user item newuser (add)
 description New User
Entity port item port01 (edit)
 baudrate 115200
```

DELETE

The `delete` command is used to delete an item or entity or remove a config section or sub-section. The command requires a unique value to identify the record. This is used for the entity's label field.

Similar to the `add` command, `delete` makes the change in a temporary state and affects configuration only when applied.

You can use the `delete` command on:

- Existing configuration
- Unapplied changes

When used on unapplied changes, this behaves in the same way as the `discard` command.

Parameters	
`entity`	The entity from which to delete the item.
`Item-label`	The label that identifies the item to delete.

Syntax

```
delete <entity> <optional-entity> <item-label>
```

Example

```
delete user aconsoleuser
config:
```

Removing an element

From the users context:

```
delete "username"
```

Single line command

```
delete user "username"
apply
```

Either of the above examples result in exiting the context of an item being deleted.

Refer to the `apply` command for how this behaves.

DIFF

The `config diff` feature provides the ability to compare the current running configuration of a device with a previously exported configuration template generated with `ogcli export`.

The `config diff` tool functions by performing an export of the current configuration of the system, and comparing it with a previous exported file, showing only the changes in a streamlined diff output containing the functional changes only.

> **Note:** The `config diff` tool performs the diff functionality in the same way as `ogcli diff`, and can be used interchangeably using export files in either format. See **config diff** in the "Opengear CLI Guide" on page 348.

Diff tool behavior

- Diff shows additions, removals and changes clearly in the a streamlined format with only functional differences between the input and running configurations.
- If any section, list item or sub-property is out of order between the input configuration and the running configuration, it is not shown in the diff unless the values have actually changed.
- If the input configuration file is missing properties or sections of configuration, it shows the differences between running configuration and the default values for those properties.
- If any property or configuration section is missing from input configuration, and the running configuration is identical to the system defaults, it is omitted from the diff output.
- If diff function detects no differences between the current configuration and configuration template files match, a return code of 0 and no output is shown.

Syntax

```
diff <proposed_configuration_file>
```

Usage Examples

1. Active configuration matches input file:

No differences between input file and active configuration.

```
root@om2224-24e-10g:~# ogcli diff ogcli1.txt
root@om2224-24e-10g:~#
```

2. Configuration differs from template:

Differences displayed between input file and active configuration.

```
root@om2224-24e-10g:~# ogcli diff hostname.txt
ogcli --secrets=obfuscate --check-before-replace replace system/admin_info <<'END'
-   hostname="hostname-a"
+   hostname="hostname-b"
END
```

3. Configuration differs from template with defaults:

Differences between active configuration and default configuration because the input file was empty.

```
root@om2224-24e-10g:~# ogcli diff empty.txt
ogcli --secrets=obfuscate --check-before-replace replace system/admin_info <<'END'
-   hostname="hostname-a"
END
root@om2224-24e-10g:~#
```

4. Configuration matches template with defaults:

No differences between active configuration and default configuration with empty input file.

```
root@om2224-24e-10g:~# ogcli diff empty.txt
root@om2224-24e-10g:~#
```

Positional Arguments

<input_file> Diff active configuration against <input_file>.

Options	
`-h, --help`	Show this help message and exit. If more detailed help is required, use `config diff --help`.
`--secrets`	The --secrets flag can be used to control how sensitive fields are displayed in the diff output. By default, sensitive fields are obfuscated. If the proposed config file was exported with `--secrets=cleartext` or `--secrets=mask` then the same value must be used when running `ogcli diff`, for example, `ogcli --secrets=cleartext diff <input file>` If the input file contains a different `--secrets` parameter than that provided, an error is returned.

DISCARD

The discard command is used to remove unapplied changes.

This can be used to discard specific or configuration wide changes including:

- Updates to configuration items.
- Additions not applied.
- Items designated for deletion.

Parameters	
`discard`	When used on its own discard the current item when in an item context, otherwise it is an error.
`discard all`	When used with the 'all' command, then any changes staged in the current session are dropped.

Syntax
`discard [all]`

Example

The following commands create a user and then discard the user (it is never saved).

> **Note:** The context changes to exit the 'myuser' item since it no longer exists.

```
config: add user myuser
```

```
config: user myuser
```

```
config(user myuser): discard
```

Discard changes

config(user):

The following commands discard changes to an existing item. The item isn't removed in this case since it has been applied previously. The description field will revert back to whatever it was before.

```
config: user root
config(user root): description "Root user"
config(user root): discard
```

The following commands discard changes to multiple entities, the group and port entities. Both are reverted:

```
config: edit group admin description "New group description"
config: edit port port01 label "New label"
config: discard all
```

Example

Discard all changes

```
discard *
```

This results in a confirmation being displayed.

Discard Groups of Changes

```
discard auth user "username"
```

- If “username” is an addition that has not been applied, it will result in the added user being discarded. In this case the user is prompted to confirm before the command is implemented.
- If “username” is an existing user with unapplied configuration changes, this results in any changes there being discarded. A confirmation is required.
- If “username” is an existing user but with no changes, the user is informed that there are no configuration changes to discard.

Discard Specific Changes

```
port port01
discard
```

- If the entity has unapplied changes it is discarded.
- If there are no unapplied changes an information message displays.

Confirmation

Discarding changes at a section, or configuration wide level gives a warning that multiple changes will be discarded.

EDIT

The edit command is used when making changes to configuration options without navigating through the hierarchy.

Parameters	
`entity`	The entity to be edited.
`item-label`	Unique value that identifies the item.
`record field`	The field to set for the item.
`value`	The value corresponding to the field.

Syntax

```
edit <entity> <optional-entity> <item-label> <field>
<value>
```

Example

Consider the following change to a port label:

```
config
port
port_01
label "Office-switch"
```

Alternatively, consider making the change from the root of configuration mode.

```
config
edit port port_01 label "Office-switch"
```

EXIT

The `exit` command can be run at any level in the configuration structure and will allow you to leave config mode. If there are unapplied changes, you are informed and asked to confirm it you want to proceed.

Parameters

There are no parameters applicable to the exit command.

Syntax

```
exit
```

Example

```
exit
```

HELP (OR ?)

> **Note:** Config mode will accept either `help` or a question mark `?` input.

Can be used in the following ways:

- A standalone command to view available options for the configuration section.
- In combination with a command to access help documentation.
- In combination with a configuration option to access help documentation and examples.

Parameters

The `help` command shows help for the current context.

`command`	Shows help for the command.
`field`	Shows help for the field.

Syntax

```
help <command or field>
<command or field> ?
```

Example

The following will print help for the “port port01” context:

```
config(port port01): help
```

or

```
config(port port01): ?
```

The following will print help for the baudrate field when in the “port port01” context:

```
config(port port01): help baudrate
```

or

```
config(port port01): baudrate ?
```

Help Command Used Standalone

When used by itself, `help` or `?` returns a list of available commands or configuration options.

Help Used in Conjunction with a Command

```
apply ?
```

When used in conjunction with a command, `help` displays available sub-options.

For example, when running the `apply` command from the root config level, the `help` command notifies you that changes will traverse the configuration structure, however, when running the `help` command from within a configuration section, changes will apply to configuration options contained within.

```
add user ?
```

Displays help content including syntax and config items (mandatory and optional).

Example

Help Used with a Configuration Option

In the context of this example, the user is running the command from within the port configuration section and is wanting to get information on the available options.

```
pinout ?
```

This displays a list of available options.

```
label ?
```

This displays the expected format and a sample.

IMPORT/EXPORT

> **Note:** The import / export and associated commands operate in bash, ie. outside of config CLI. You must exit config to operate the import/export features.

The Import / Export feature allows you to export the current configuration to a file and import or restore the configuration from that file. An import will add configuration to the current configuration and restore will replace the current configuration with the contents of the configuration file.

Import

Running the import command (within bash, not in config:) will allow you to import a configuration script from an external source file. You should point the console server to a config file on specific network location. The file is copied to the console server and run. Depending on how it has been set up, the changes can be automatically applied after the config file is run.

Export

Running the export command (within bash, not in config:) will allow you to generate a configuration script based on the existing configuration on the console server.

This command can be run at any level in the hierarchy and used to export either:

- The configuration across the node
- Configuration specific to the users's location in the hierarchy.

```
export all current config
```

This displays all config on the console server before it has been applied for copying.

```
export all saved config
```

This displays all saved config on the console server for copying.

```
export current config
```

This displays the config from the users's current position in the navigation hierarchy.

Parameters

Import and export are run from outside of the Config Shell. The `config` command is invoked from bash with different parameters to cause it to import or export the configuration without entering the Config Shell.
filename - The name of the file to import from or export to. If omitted then `stdin` or `stdout` is used.

Syntax

```
config export <optional filename>
config import <optional filename>
```

Example

```
config export /tmp/console_server.config
config import /tmp/console_server.config
```

Positional Arguments	Description
`export`	Export the current configuration.
`import`	Import config from a file.
`restore`	Restore config from a file.
`merge`	Merge a provided list with existing config.
`replace`	Replace a list or item.
`get`	Display an entity's associated values.

Options

`-h, --help`	Show this help message and exit.
`--show-config`	Display the entire configuration and exit.
`-d`	Increase debugging (up to 3 times).
`-j`	Export in json format.
`--entities`	Display entities and exit.

Exporting To A File

The import/export and associated commands operate in bash, ie. outside of config CLI. You must exit config to operate the import/export features.

SHOW

The `show` command displays information relevant to the configuration section, including the highlighting of changes. The context in which the command is run determines what displays.

At `config root`, the `show` command displays system information.

Within a config section, for example from **config > auth > user**, this displays a flat list of available users.

Parameters

`show`	Used on its own, this displays the fields of the current context. When used in the top context, it shows the list of all entities. When used in an entity context, it shows the list of items in that entity. When used in an item context, it shows the fields and values of the current item.
`entity`	The entity to display, or to show details of.
`item`	The item to display or show details of.
`field`	The field to show the value of.

Syntax

```
show <optional entity> <optional item> <optional field>
```

Config

You can view the content of all configuration in JSON format.

You can also view the config of a specific section of the hierarchy you are in.

```
show-config
```

Directed Usage

You will also be able to look into a config sections using the show command. For example:

```
show auth user
```

This displays a flat list of users.

```
show auth user “username”
```

This displays the configuration for the user specified.

Examples Using Context

The following examples show how the output of the show command changes in accordance with context as it may be used at the config, physif, net1 contexts:

show - at the config context:

```
config: show

Entities
========
access_right                        pdus/drivers
auth                                physif
auto_response/beacon                port
auto_response/reaction              port_session
auto_response/status                ports/auto_discover/schedule
auto_response/status/beacon-module  ports/status_port
cellfw/info                         services/brute_force_protection
cellmodem                           services/lldp
cellmodem/sim                       services/ntp
conn                                services/routing
failover/settings                   services/snmp_alert_manager
failover/status                     services/snmpd
firewall/policy                     services/ssh
firewall/predefined_service         services/syslog_server
firewall/service                    services/tftp
firewall/zone                       ssh/authorized_key
group                               static_route
ip_passthrough                      system/admin_info
ip_passthrough/status               system/banner
ipsec_tunnel                        system/cell_reliability_test
lighthouse_enrollment               system/cellular_logging
local_password_policy               system/cloud_connect
logs/portlog                        system/diskspace
logs/portlog_settings               system/info
managementport                      system/model_name
monitor/brute_force_protection/ban  system/serial_number
monitor/lldp/chassis                system/session_timeout
monitor/lldp/neighbor               system/ssh_port
monitor/static_routes/status        system/system_authorized_key
monitoring/alerts/networking        system/time
monitoring/alerts/power             system/timezone
monitoring/alerts/system            system/version
pdu                                 user

config:
```

Examples Using Context

show - at the physif context:

```
config: physif
config(physif): show
Item names for entity physif
  net1
  net2

config(physif):
```

show - at the net1 context:

```
config(physif): net1
config(physif net1): show
Entity physif item net1
  description NET1 - 1G Copper/SFP
  enabled     true
  mtu         1500
  dns (object)
    nameservers (array)
    search_domains (array)
  ethernet_setting (object)
    link_speed auto

config(physif net1):
```

Examples Using Parameters

The following examples show the output of the show command when used with different parameters:

```
config: show physif
Item names for entity physif
  net1
  net2

config: show physif net1
Entity physif item net1
  description NET1 - 1G Copper/SFP
  enabled     true
  mtu         1500
  dns (object)
    nameservers (array)
    search_domains (array)
  ethernet_setting (object)
    link_speed auto

config:


config: show physif net1 description
NET1 - 1G Copper/SFP
config:
```

UP / EXIT / ..

These commands allow users to traverse the configuration hierarchy.

```
up
```

The position will move one level up in the hierarchy.

If used at the root configuration level, it should point trigger the exit command.

Parameters

No parameters.

Syntax

```
up
exit
```

Example

If, as in this example, the context is a specific port, then the ports entity can be accessed by using the `up` command then moving into another port:

```
config: port port01
config(port port01): up
config(port): port02
config(port02):
```

CONFIG CLI USE CASE EXAMPLES

Use case examples are available for the following:

- Users
- Ports
- Create or Configure a Loopback Interface
- Configure NET1 Static IPV4
- Configure NET2 Static IPV4

- Configure NET3 Static IPV4 for OM2224-24e units
- Configure WireGuard through Config Shell
- Passwords
- System Information
- Enable NETGRP - Set to ConsoleUser
- Change SSH Delimiiter to : default is +
- Enable TACACS - Set Mode to remotelocal
- Enable LLDP on NET1 & NET2
- Enable TFTP
- Enable Boot Messages
- Enable SIMM 1
- Enable Failover
- Syslog Server
- Set Port Logging Remote Syslog Settings
- Enable System Monitor SNMP Traps
- SNMP
- Create a Static Route
- Firewall
- Enroll Into Lighthouse

USERS

ADD A USER

The following is a fully worked example showing the adding of a new user.

Note: In the following examples, some commentary has been added, the commentary is denoted with a '//' prefix. Where sessions continue onto the next page, this is shown with the comment "// session continues here:"

```
# config
Welcome to the Opengear interactive config shell. Type ? or help for help.
// Move to the user entity

config: user
config(user): help add
Add a new item for entity user.

The add command requires a unique value to identify the record.
This will be used for the username field.

Description for the item:
  Retrieve and update information for a specific user.

// Create the new user

config(user): add matt
config(user matt): show
Entity user item matt
  description

// Session continues here:
  enabled              true
  no_password         false
password                          (required)
ssh_password_enabled true
username               matt
```

```
groups (array)


// Fill out some fields


config(user matt): password topsecretpassword
config(user matt): description scrum master
config(user matt): show
Entity user item matt
  description          scrum master *
  enabled              true
password               topsecretpassword *
ssh_password_enabled  true
username               matt
groups (array)


// Edit the groups


config(user matt): groups
config(user matt groups): show
Entity user item matt field groups
config(user matt groups): add // Tab completion to show available values
admin myuser netgrp
config(user matt groups): add admin
config(user matt groups): up // Exit the groups list
// Session continues here:
// Show and apply


config(user matt): show
Entity user item matt
  description          scrum master *
  enabled              true
```

```
  password             topsecretpassword *
  ssh_password_enabled true
  username                                                matt
  groups  (array)
    0 admin *
config(user matt): apply
Creating entity user item matt.
config(user matt):
```

CREATE ADMIN USER

```
add user admin
  description "admin"
  enabled true
  no_password false
  password "password"
  user admin groups
  add "admin"
top
```

CREATE BREAKGLASS USER (BELONGS TO NETGRP)

```
add user breakglass
  description "breakglass" enabled true
  no_password false
  password "password"
  user breakglass groups
  add "netgrp"
top
```

PORTS

CONFIGURE A PORT

```
config: port

config(port): help

You are here: entity port


Description for the entity:

   Configuring and viewing ports information


Names (type <name> or help <name>)

==================================

USB-A USB-E USB-front-lower port03 port07 port11 port15 port19 port23

USB-B USB-F USB-front-upper port04 port08 port12 port16 port20 port24

USB-C USB-G port01               port05 port09 port13 port17 port21

USB-D USB-H port02 port06        port10 port14 port18 port22


Commands (type help <command>)

==============================

exit help show up


config(port): port01

config(port port01): baudrate // tab completion

110 1200 150 19200 230400 300 4800 57600 75

115200 134 1800 200 2400 38400 50 600 9600

config(port port01): baudrate 57600

config(port port01): label Router

config(port port01): control_code

config(port port01 control_code): break a

config(port port01 control_code): up

config(port port01): show

// Session continues here:
```

```
Entity port item port01
  baudrate        57600 *
  databits        8
  escape_char     ~
  label Router        *
  logging_level   disabled
  mode            consoleServer
  parity          none
  pinout          X2
  stopbits        1
  control_code (object)
    break a *
    chooser
    pmhelp
    portlog
    power
    quit
  ip_alias (array)
config(port port01): apply
Updating entity port item port01.
config(port port01):
```

CONFIGURE SINGLE SESSION ON PORT

The feature is enabled by typing `single_session true`, then apply the change.

```
config(port port01):      single_session true
config(port port01):      apply
Updating entity port      item port01.
config(port port01):      show
Entity port item              port01
```

```
    baudrate                    9600
...
single_session              true
...
ip_alias (array)
```

CHANGE PORT LABELS

```
edit port port01 label "cisco1"
edit port port02 label "cisco2"
edit port port03 label "cisco3"
edit port port04 label "cisco4"
```

CREATE OR CONFIGURE LOOPBACK INTERFACE

Loopbacks are not physical interfaces and as such cannot be attached to a firewall zone; firewall zone or policy rules must be created for whatever interface you are connecting over. Service translations can be created through the `firewall/service_translation` endpoint to change the source address of outbound packets to the loopback address.

To create a loopback, navigate to the `physifs` endpoint and set the media to `loopback`:

CREATE A LOOPBACK IN CONFIG SHELL

```
config: physif
config(physif): add loop
config(physif loop): media loopback
config(physif loop): enabled true
config(physif loop): apply
Creating entity physif item loop.
```

CREATE A LOOPBACK IN OGCLI

```
ogcli create physif << 'END'
device="loop"
enabled=true
media="loopback"
END
```

ADD AN ADDRESS TO A LOOPBACK INTERFACE

To add an address to a loopback interface, navigate to the `conns` endpoint and attach an ipv4 or ipv6 static address to the loopback (dhcp and ipv6_automatic are invalid for loopbacks):

ADD AN ADDRESS IN CONFIG SHELL

```
config: conn
config(conn): add new
config(conn new): mode static
config(conn new): physif loop
config(conn new): ipv4_static_settings
config(conn new ipv4_static_settings): address 10.0.0.1
config(conn new ipv4_static_settings): netmask 255.255.255.0
config(conn new ipv4_static_settings): apply
Creating entity conn item new.
```

ADD AN ADDRESS IN OGCLI

```
ogcli create conn << 'END'
mode="static"
physif="loop"
ipv4_static_settings.address="10.0.0.1"
ipv4_static_settings.netmask="255.255.255.255"
END
```

In the above example the `physif` is set to `loop`. Do not set the `broadcast_address` and `gateway_address` for loopback interfaces.

CREATE SOURCE NAT RULES

> **Note:** When referring to service translation rules, we refer to translating the source ip of traffic to a required source ip address. To change the source address of outbound packets for a particular service, a `service_translation` rule must be added, see the following example:

The following rule contains a list of outbound services along with the changed source address for the service packets. Navigating to the `firewall/service_translation` endpoint, you can add a new translation rule by using the `add` command. **Note:** Only services which use tcp or udp protocols are valid.

```
config(firewall/service_translation 10.0.0.1): show
Entity firewall/service_translation item 10.0.0.1
  address 10.0.0.1
  services (array)
     0 ssh
     1 https
```

If a service translation rule contains an address that does not exist on the box, a warning message is shown when creating the rule; however, it will not prevent these rules being created. See the following:

```
config(firewall/service_translation): add 10.0.0.2
  WARNING: The IP entered does not exist as a known IPv4 or IPv6 address.
  If this is expected, you can safely ignore this message.
```

If required, source NAT may be used for all tcp and udp traffic leaving the box by adding the service `all-tcp-udp` to the service list:

```
config(firewall/service_translation 10.0.0.1): show
Entity firewall/service_translation item 10.0.0.1
address 10.0.0.1
services (array)
0 all-tcp-udp
```

Notes:

- There **must** be either a static or dynamic route to the loopback address from which you are connecting to the device.
- Source NAT is not used for packets on the cell interface wwan0. A VPN can be set up over the cell interface if the loopback address is used over cell; dynamic routing must be configured over the VPN to share the route to the loopback address.

REST API

The `firewall/service_translation` endpoint is used to create nftables rules which configure source NATs for outgoing service traffic. This replaces the outgoing IP address of a service packet with the address given in the `service_translation`. This is done for all services within the service translation rule.

```
"service_translation" : {
   "address": "A.B.C.D"
   "services": []
}
```

The address can be ipv4 or ipv6 (no netmask required), and does not have to exist on the box (a warning is presented if the address does not exist).

The list of services is a list of strings of service names. The outbound services must already be defined on the box, either as a predefined `firewalld` service or as a custom user service.

LOGGING AND DEBUGGING

You can ping the loopback address like any other interface. You must have a static or dynamic route to the loopback in order to reach it.

- Use the command `ip a` to display logging information.
- Conman logs information about creating or deleting loopback interfaces, and connections attached to loopback interfaces, in `/var/log/message`.
- When creating loopback interfaces, the generated files should be directed to `/etc/config/conman.conf`.
- Use the command `tcpdump` on interfaces connected to the device to see source NAT traffic.
- Source NAT rules can be found under `/etc/nftables/og-service-snat/og-service-snat.conf`, or use the command `nft list ruleset` to check for rules under the service SNAT tables.

CONFIGURE NET1 STATIC IPV4

```
conn default-conn-1 ipv4_static_settings
  address 192.168.2.54
  gateway 192.168.2.1
top
```

CONFIGURE NET2 STATIC IPV4

```
add conn net2-static-1 mode static physif net2
conn net2-static-1 ipv4_static_settings
  address 192.168.3.58
  gateway 192.168.3.1
  netmask 255.255.255.0
top
```

CONFIGURE NET3 STATIC IPV4 FOR OM2224-24E UNITS

```
add conn net3-static-1 mode static physif net3
conn net3-static-1 ipv4_static_settings
  address 192.168.4.58
  gateway 192.168.4.1
  netmask 255.255.255.0
top
```

CONFIGURE WIREGUARD THROUGH CONFIG SHELL

WireGuard is configured through Config Shell (or REST API). The minimum configuration of WireGuard is shown in the following:

1. Provide a name for the interface (wg0 in the following example).
2. Set enabled.
3. Set the private_key of your WireGuard interface.
4. Add an address (at least one) for your WireGuard interface (10.0.0.1/24 in this case).
5. Add a peer with the following parameters: endpoint_address, endpoint_port, public_key.
6. Add an allowed_ip for your peer. At least one - this is the WireGuard address(es) (as it can also accept an address range) of the other interface to which you are connected.

For example:

```
config: wireguard
config(wireguard): add wg0
config(wireguard wg0): private_key AGiZvFHY+r/dD0rHSKU5ZCrHNdLM0W/h29VxobxWgFo=
config(wireguard wg0): enabled true
config(wireguard wg0): addresses
config(wireguard wg0 addresses): add 10.0.0.1/24
config(wireguard wg0 addresses): up
```

```
config(wireguard wg0): peers
config(wireguard wg0 peers): add
config(wireguard wg0 peers 0): public_key
o+quB4sbUAG2hEGSPpMNTnO0YSaQTP7dD+Q4IVjiCW8=
config(wireguard wg0 peers 0): allowed_ips
config(wireguard wg0 peers 0 allowed_ips): add 10.0.0.2/32
config(wireguard wg0 peers 0 allowed_ips): up
config(wireguard wg0 peers 0): endpoint_address 192.168.1.2
config(wireguard wg0 peers 0): endpoint_port 51820
config(wireguard wg0 peers 0): up
config(wireguard wg0 peers): top
```

PASSWORDS

ROOT USER PASSWORD - CLEARTEXT

```
edit user root password newpassword
```

ROOT USER PASSWORD = PASSWORD VIA SHA256

openssl passwd -5 password

> **Note:** This operation is not available in Config Shell.

DEFINE PASSWORD COMPLEXITY RULES

```
edit local_password_policy
  password_complexity_enabled true
  password_expiry_interval_enabled true
  edit local_password_policy
  password_disallow_username true
  password_must_contain_number true
  password_must_contain_special true
  password_must_contain_upper_case true
```

EDIT SYSTEM INFORMATION

HOSTNAME

```
edit system/admin_info hostname "OM2216-1-lab"
```

CONTACT INFO

```
edit system/admin_info
  contact "fred.bloggs@opengear.com"
  hostname "om2216-1.lab"
  location "Happy Valley Lab"
```

TIME ZONE AND NTP

```
edit system/timezone timezone "America/New_York"


edit services/ntp enabled true
services/ntp servers
  add
  value "74.207.242.234"
top
```

DEFINE MOTD

You can use the message of the day (MOTD) to display custom messaged on log in. When configured, the message displays in a banner on the WebUI and is printed on SSH login.

Enter banner text within triple quotations. The triple quotations enable any text entered between the quotations to be treated as one piece of text. This allows the MOTD to display on more than one line if required.

```
edit system/banner banner """
```

The following shows an example:

```
edit system/banner banner """
IMPORTANT
You must have the appropriate permissions to access this device.
Contact the IT Department.
"""
```

DEFINE SESSION TIMEOUTS

```
edit system/session_timeout cli_timeout 100 serial_port_timeout 100 webui_timeout 100
```

> **Note:** The inactivity timer starts only after you exit Config Shell, ie. it begins the count when you have left config and are at the bash command prompt.

ENABLE NETGRP SET TO CONSOLEUSER

```
edit group netgrp enabled true
group netgrp ports
  add port01
  add port02
  add port03
  add port04
top
group netgrp access_rights
  add web_ui
  add pmshell
  delete admin
top
```

CHANGE SSH DELIMIITER TO : DEFAULT IS +

```
edit services/ssh ssh_url_delimiter ":"
```

ENABLE TACACS - SET MODE TO REMOTELOCAL

```
edit auth mode "tacacs"
edit auth tacacsMethod "pap" tacacs
Password "tac_tests"
policy "remotelocal"
tacacsService "raccess"
auth tacacsAuthenticationServers
  add
  hostname "192.168.2.220"
  port 49
top
```

ENABLE LLDP ON NET1 & NET2

```
edit services/lldp enabled true
services/lldp physifs
  add "net1"
  add "net2"
top
```

ENABLE TFTP

```
edit services/tftp enabled true
```

ENABLE BOOT MESSAGES

Displays on local console port.

```
edit managementport ttyS0 kerneldebug true
```

ENABLE SIMM 1

ENABLE SIMM 1 ENABLE AND ADD APN

```
edit physif wwan0 enabled true
physif wwan0 cellular_setting
  apn hologram
top
```

ENABLE SIMM 1 COMPLETE END POINTS

```
edit physif wwan0 enabled true
physif wwan0 cellular_setting
  active_sim 1
  apn hologram
  iptype IPv4v6
  sim_failback_disconnect_mode ping
  sim_failback_policy never
  sim_failover_disconnect_mode ping
  sim_failover_policy never
top
physif wwan0 cellular_setting sims 0
  fail_probe_address 8.8.8.8
  fail_probe_count 3
  fail_probe_interval 600
  fail_probe_threshold 1
  failback_delay 60
  iptype "IPv4v6"
  slot 1
top
physif wwan0 cellular_setting sims 1
  fail_probe_address 8.8.8.8
  fail_probe_count 3
  fail_probe_interval 600
  fail_probe_threshold 1
  failback_delay 60
  iptype IPv4v6
  slot 2
top
```

ENABLE FAILOVER

```
edit failover/settings enabled true probe_address 192.168.2.1 probe_physif net1
```

SYSLOG SERVER

ADD A SYSLOG SERVER

```
services/syslog_server
  add server1
  address 192.168.34.113
  protocol TCP
  port 610
  description "my syslog server"
top
```

ADD FIVE SYSLOG SERVERS

> **Note:** Due to page width limitations, in the following example, some command lines break over two lines.

```
add services/syslog_server server0 address 192.168.34.112 min_severity notice port 514
port_logging_enabled true protocol UDP
add services/syslog_server server1 address 192.168.34.113 min_severity notice port 514
port_logging_enabled true protocol UDP
add services/syslog_server server2 address 192.168.34.114 min_severity notice port 514
port_logging_enabled true protocol UDP
add services/syslog_server server3 address 192.168.34.116 min_severity info port 514 port_
```

```
logging_enabled true protocol UDP
add services/syslog_server server4 address 192.168.128.1 description "lighthouse-remote-
syslog" min_severity info port 514 port_logging_enabled true protocol UDP
```

SET PORT LOGGING REMOTE SYSLOG SETTINGS

```
edit logs/portlog_settings facility daemon severity info Enable system monitor
snmp traps
```

ENABLE SYSTEM MONITOR SNMP TRAPS

Notes: In the following use case:

- The `threshold_upper`, `threshold_lower`, and `cell_signal_strength_alert` items are applicable only to cellular devices.
- The `millivolt_lower` and `millivolt_upper` items are not present for the CM8000.

```
monitoring/alerts/power power_supply_voltage_alert
  millivolt_lower 11000
  millivolt_upper 13000
  snmp
    enabled true
  up
top
monitoring/alerts/networking cell_signal_strength_alert
  enabled true
  threshold_lower 33
  threshold_upper 66
top
monitoring/alerts/system
  authentication_alert
```

```
    enabled true
  up
  config_change_alert
    enabled true
  up
  temperature_alert
    enabled true
    threshold_lower 35
    threshold_upper 67
  up
top
```

SNMP

ENABLE SNMP V2 SERVICE FOR POLLING

```
edit services/snmpd enable_legacy_versions true
enable_secure_snmp false enabled true port 161 protocol UDP
edit services/snmpd rocommunity "TkcxJAAAABBfDsigaxdDf7whb3sxKQKnjtCuuy/0COC6rE3lUu9ghg=="
```

ENABLE 2 SNMP TRAPS AND TRAP SERVERS

> **Note:** Due to page width limitations, in the following example, some command lines break over two lines.

```
add services/snmp_alert_manager "snmp trap server 1" address 10.1.1.199 port
162 protocol UDP version v2c
services/snmp_alert_manager "snmp trap server 1"
  community "TkcxJAAAABBfDsigaxdDf7whb3sxKQKnjtCuuy/0COC6rE3lUu9ghg==" msg_type TRAP
  top
```

```
apply all


services/snmp_alert_manager 10.1.1.199:162/UDP
  name "snmp trap server 1" privacy_password secret auth_password secret
  top
apply all
```

CREATE A STATIC ROUTE

> **Note:** Due to page width limitations, in the following example, some command lines break over two lines.

```
add static_route "static route test" destination_address 10.0.0.0 destination_netmask 8
interface net2
```

FIREWALL

EDIT LAN (NET2) FIREWALL ZONE

(allow only source address traffic)

```
firewall/zone lan custom_rules
  add
    description "source_net4-1"
    rule_content "rule family=ipv4 source address=192.168.3.0/24 accept"
  up
  add
    description "source_net4-2"
```

```
    rule_content "rule family=ipv4 source address=10.202.198.0/27 accept"
  up
top
```

EDIT WAN (NET1) FIREWALL ZONE

(allow only source address traffic)

```
  firewall/zone wan custom_rules
    add
      description "source_net4-1"
      rule_content "rule family=ipv4 source address=192.168.2.0/24 accept"
    up
    add
      description "source_net4-2"
      rule_content "rule family=ipv4 source address=192.168.4.0/24 accept"
    up
  top
```

CUSTOM_RULE EXAMPLE FOR PORT AND PROTOCOL

```
  add firewall/service myports label "My Serial Ports"
  firewall/service myports
    add
      port 3001
      protocol tcp
    up
    apply
  top
  firewall/zone wan address_filters
```

```
  add
    source_address 10.10.2.0/19
    services
      add myports
    up
  up
top
```

ENROL INTO LIGHTHOUSE

```
add lighthouse_enrollment lh1 address 2.21.99.188 bundle om2216-1 token password
```

HOW CHANGES ARE APPLIED OR DISCARDED

When fields and entities are changed, the changes are not immediately applied to the system configuration but remain in a staged status. Items that are staged are indicated by an '*' (asterisk) when the 'show' command is used. In addition, the 'changes' command can be used to show what fields have been changed.

In the following example, the user 'john' has been changed to alter the description. The 'show ' command indicates the changed field with an '*'. The changes command lists the changed field.

```
config(user john): description "Admin"
config(user john): show
Entity user item john
 description Admin * enabled true
 no_password false password false
 password
 ssh_password_enabled true
 groups (array)
```

APPLY OR DISCARD CHANGES

When fields and entities have been changed, they are not yet applied to the system configuration but are kept staged. Items that are staged are indicated with an '*' when the 'show' command is used. In addition, the 'changes' command can be used to show what fields have been changed.

When any changes have been made to a single or multiple entities, the following commands become available. These commands are described in detail in the Config CLI Commands section:

Command	Description
changes	Show staged changes on all entities.
apply	Apply changes only on the current entity.
discard	Discard changes only on the current entity.
apply all	Apply changes on all entities.
discard all	Discard changes on all entities.

Example

In the following example, the user 'john' has been changed to alter the description. The 'show' command indicates the changed field with an asterisk '*'. The changes command lists the changed field.

```
config(user john): description "Scrum Master"
config(user john): show
Entity user item john
description Scrum Master *
enabled true
no_password false
```

```
password
ssh_password_enabled true
groups (array)
config(user john): changes
Entity user item john (edit)
description Scrum Master
config(user john):
```

MULTI-FIELD UPDATES

DESCRIPTION

Within Config Shell, it is possible to update multiple fields with one command line. This is restricted to ‘flat’ fields within the current context ie arrays and sub-objects cannot currently be updated all in one command line.

For example, the following port fields can all be changed in a single command: `baudrate, databits, escape_char, label, logging_level, mode, parity, pinout` and `stopbits`. Other complex fields such as `control_code` and `ip_alias` cannot be modified from the port item context in one commands (multiple commands are required).

EXAMPLE

The following command sets the `baudrate, escape_char` and `label` fields.

```
config(port port01): baudrate 115200 escape_char ! label "My Router"
```

The changes are staged in Config Shell. Use the `apply` command to save the changes to config.

To further update the `control_codes` and `ip_aliases`, multiple commands are required as follows:

```
config(port port01): control_code
config(port port01 control_code): break b chooser c
config(port port01 control_code): up
config(port port01): ip_alias
config(port port01 ip_alias): add
config(port port01 ip_alias 1): interface net1 ipaddress 10.83.0.6/24
config(port port01 ip_alias 1): up
config(port port01 ip_alias): up
config(port port01): changes
Entity port item port01 (edit)
  control_code (object)
    break b
    chooser c
  ip_alias (array)
    1 (object)
      interface net1
      ipaddress 10.83.0.6/24
config(port port01):
```

If certain fields are hidden and only visible by first configuring other fields, these hidden fields must be set in another line. For example, the `kernel_debug` field is only revealed by setting the field `mode` of a port to `localConsole`, so this is configured on the next line:

```
config: port port03
config(port port03): mode localConsole baudrate 115200 databits 7 label aaa
logging_level eventsOnly parity even
config(port port03): kernel_debug true
```

ERROR MESSAGES

If there is an error while processing a multiple-fields command, the staged values in configuration will not be changed. If there were no staged changes on the item, then no staged changes will appear. If there were already staged changes, then those staged changes will not be affected.

In the following example, the user description was previously changed to “my user”

```
config(user consoleuser): show
Entity user item consoleuser
  description         my user *
  enabled             true
  no_password          false
  password            ""
  ssh_password_enabled true
  groups (array)
    0 consoleuser
```

If a bad field name or value is supplied on the command line, then the existing staged value is retained. The bad field name is highlighted using a ^ marker.

```
config(user consoleuser): description "My console user" invalid true
                                                        ^
Invalid input detected at '^' marker.
config(user consoleuser):
```

If the field is missing a value, a different error message displays:

```
config(user consoleuser): description "My console user" enabled
Incomplete command.
config(user consoleuser): show
Entity user item consoleuser
  description         my user *
```

```
  enabled               true
  no_password           false
  password             ""
  ssh_password_enabled true
  groups (array)
    0 consoleuser
```

The bad value for the field is indicated by an error message hinting the expected type of the value:

```
config(user consoleuser): description "My console user" enabled bad
Value bad for field enabled cannot be parsed as a boolean.
config(user consoleuser): show
Entity user item consoleuser
  description                          my user *
  enabled              true
  no_password                  false
  password             ""
  ssh_password_enabled true
  groups (array)
    0 consoleuser
```

Changes to previous functionality:

With the new `show` command, some previous syntax has changed. Just typing a field name is now an error condition. Previously this would be equivalent to the show command.

```
config: user root
config(user root): description
Incomplete command.
config(user root):
```

ERROR MESSAGES

When an error is made in the command line an error message which identifies the error is returned. For example, if the first token of the command is mistyped, the unknown command message displays.

```
config: usear root
There is no command usear root.
Type 'help' to see the available commands.
config:
config: aaaaa
There is no command aaaaa.
Type 'help' to see the available commands.
config:
```

If only the first few tokens of the command can be parsed, an error message with a ^ marker displays showing which part of the command cannot be parsed. If a context navigation is mistyped on the command line, then the context remains unchanged. It does not partially navigate through multiple contexts. In the following example, the context remains at the top context because `roopt` is not a valid item context in the user entity context.

```
config: user roopt
             ^
invalid input detected at '^' marker.
config:
```

STRING VALUES IN CONFIG COMMANDS

DESCRIPTION

The syntax for the use of string values has changed. It was previously possible to enter values containing spaces without using quotes. Multiple fields can now be assigned in one command line, quotes are required to keep field values together.

EXAMPLE

The following example shows setting multiple fields where the field value for the description has spaces. The first attempt doesn't work because the second part of the description is interpreted as a field name. The second attempt is the correct syntax:

> **Note:** In the example the syntax error in the first line in highlighted in **bold** for clarity; lhe correct syntax is highlighted in bold in line four.

```
config(user consoleuser): description My console user enabled true
There is no command description My console user enabled true.
Type 'help' to see the available commands.
config(user consoleuser): description "My console user" enabled true
config(user consoleuser): changes
Entity user item consoleuser (edit)
  description My console user
  enabled true
config(user consoleuser):
```

If the value itself must contain quotes, there is a triple quote form for entering string values:

```
config(user consoleuser): description """My "console" user""" enabled true
config(user consoleuser): changes
Entity user item consoleuser (edit)
  description My "console" user
  enabled true
```

The triple quoted string is used for entering multi-line strings:

```
config(system/banner): banner """
This is a banner that has
multiple lines.
"""
config(system/banner):
```

ERROR MESSAGES

If the multi-line command string cannot be tokenised, an error message displays in the following form:

```
config(system/banner): banner """
aaa
"""""
Invalid input. Tokens must be separated by whitespace.
Check your input and try again.
config(system/banner):
```

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.

GET STARTED WITH OGCLI

The best way to get started with ogcli is to use the help command. Refer to the following table 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.

Help Command	Displays...
ogcli help entities	The full list of entities and a brief description of each.
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
create	Create an item.
export	Export the system configuration.
diff	Show additions, removals, changes and functional differences between the input and running configurations. See also `config diff`.
get	Retrieve a list or single item.
help	Display ogcli help.
import	Import system configuration, merging with current system configuration.
merge	Merge a provided list with existing config.
replace	Replace a list or single item.
restore	Import system configuration, replacing the current system configuration.
update	Update an item, supports partial edits.

SUPPLY 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 have to be escaped.

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

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

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

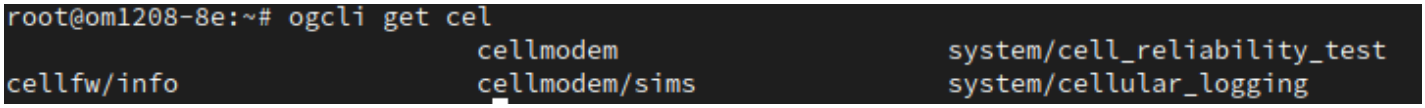
3. Double quotes not within single quotes have to be escaped.

```
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 are displayed for your reference.



DISPLAY 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 Console Manager.

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 behavior 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

You can use the message of the day (MOTD) to display custom messages on log in. When configured, the message displays in a banner on the WebUI and is printed on SSH login.

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

Detailed example:

```
ogcli replace banner banner=\"
  IMPORTANT
  You must have the appropriate permissions to access this device.
  Contact the IT Department.
\"
```

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>
```

COMPARE CURRENT CONFIGURATION WITH A PROPOSED CONFIGURATION

The updated `ogcli diff` tool enables Opengear users to compare a proposed configuration with an existing configuration so that they may understand any prospective changes to the config.

The diff function performs a comparison of active configuration and an input configuration file, which must be in the format an export file produced by either a `config export <template-file>` or an `ogcli export <template-file>` operation. Any manual changes to this export file must include config or ogcli commands in a multi-line format using the 'END' heredoc marker as produced by an export. One line config or ogcli commands will not be accepted.

USE THE DIFF TOOL

The diff tool can be used by any user with Administrator permission via the command line.

```
ogcli diff <input file>
```

or using config:

```
config diff <input file>
```

> **Note:** `config diff` and `ogcli diff`, and can be used interchangeably using export files in either format.

If there are no differences between the active configuration and the input configuration file, the diff tool will not print any output, and the operation will have an exit code of 0.

```
root@om2248:~# ogcli export config_file
root@om2248:~# ogcli diff config_file
root@om2248:~# echo $?
0
```

The diff function will show any additions, removals and changes clearly in a streamlined format with only functional differences between the input and running configurations. Any additions that are made to the active configuration are marked with a (+). For example, the `new_user` user does not exist in the active configuration, but is present in the input file supplied. If the input file was imported, this user would be added.

```
ogcli --secrets=obfuscate merge users <<'END'
+ users[1].enabled=true
+ users[1].groups[0]="admin"
+ users[1].no_password=false
+ users[1].ssh_password_enabled=true
+ users[1].username="new_user"
END
```

If the `new_user` user exists in the active configuration, but does not exist in the input file, this user is removed if the input file was imported or restored. Removals are marked with a (-) symbol.

```
ogcli --secrets=obfuscate merge users <<'END'
- users[1].enabled=true
- users[1].groups[0]="admin"
- users[1].no_password=false
- users[1].ssh_password_enabled=true
- users[1].username="new_user"
END
```

Changes in configuration between an item which exists in both the active configuration and the input file will also be displayed. The existing configuration is marked with a (-) and the incoming change as a (+). In the following example, the `new_user` user belongs to the netgrp group on the device. However, if the input file is imported, it belongs only to the Admin group.

```
ogcli --secrets=obfuscate merge users <<'END'
- users[1].groups[0]="netgrp"
- users[1].groups[1]="admin"
+ users[1].groups[0]="admin"
END
```

If any differences are found, the operation will have an exit code of 1. If there are any errors, the diff tool will have an exit code of 2.

Comparison to Default Values

If the input configuration file is missing properties or sections of configuration, the diff function will instead consider the differences between active configuration and the default values for those properties. Missing sections or properties from the input file will only be displayed in the diff tool output if the active configuration is different from the default system values. If any property or configuration section is missing from input configuration, and the running configuration is identical to the system defaults, it is omitted from the diff output.

How Secrets are Handled

The `--secrets` flag can be used to control how sensitive fields are displayed in the diff output. By default, sensitive fields are obfuscated.

- Secrets are output in the same format with which they are input:

If...	Then...
`--secrets=cleartext` is passed to the diff command	The running config secrets is output as cleartext in the diff output.
`--secrets=obfuscated` is passed to the diff command	The running config secrets is output as obfuscated in the diff output.
`--secrets=mask` is passed to the diff command	The running config secrets is output as masked in the diff output.
`--secrets=cleartext` is included in the command in the proposed config file	The proposed config secrets is output as cleartext in the diff output.
`--secrets=obfuscated` is included in the command in the proposed config file	The proposed config secrets is output as obfuscated in the diff output.
`--secrets=mask` is included in the command in the proposed config file	The proposed config secrets is output as masked in the diff output.

- Obfuscated values are decoded and the underlying cleartext is compared. A reported difference in obfuscated values indicates a difference in underlying value.

- Diff can be run with different secrets to the proposed config file and is able to compare obfuscated and cleartext secrets.
- Diff makes a best effort to compare masked passwords, but results may not be completely accurate

Diff Tool Help

Basic help for `ogcli diff` can be accessed with `ogcli diff -h`. Similarly, help for `config diff` can be accessed with `config diff -h`. Detailed help for both diff tools can be accessed by `ogcli help diff`.

Limitations
JSON template files are no longer supported with config diff.
`ogcli diff` only supports input configurations generated by the same product SKU and software version.
Comments can be included between ogcli or config commands in the export file, but not within the commands or an error is thrown. Comments must start with #. These are ignored by the diff tool.

Also see the CLI config command diff.

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"
 password=”test123"
 username="superuser123"
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 SERIAL PORTS

```
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 A DNS

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 A DNS VIA THE COMMAND LINE

Description	Command
Display configured DNS settings for an interface	ogcli get physif "net1"
Update DNS settings for an interface	ogcli update physif "net1" << 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
Check unbound service status	systemctl status unbound.service
List forward-zones in use	unbound-control list_forwards

CONFIGURE SERIAL PORTS

```
ogcli get ports
```

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

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

```
ogcli update port "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.iptype="IPv4v6"
END
```

DISABLE CELLULAR MODEM INTERFACE

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

ADVANCED PORTMANAGER PMSHELL GUIDE

The Portmanager program allows you to access any serial port on the console server using `pmshell` commands.

- Routes network connection to serial ports.
- Checks permissions.
- Monitors and logs all the data flowing to/from the ports.
- Allows you to run power commands if the serial port is associated with a PDU outlet.

RUNNING `PMSHELL`

`pmshell` provides an environment that allows you to access and interact with serial ports via a number of command sequences. It lets you navigate between ports using the chooser command (`~m`). For example, you can use pmshell to connect to port 8 via the portmanager via the following command line sequence.

```
# pmshell -l port08
```

`PMSHELL` COMMANDS

When running `pmshell` there are a number of command sequences that you can use that begin with the ~ key.

> **Note:** If you are connected to `pmshell` via SSH, you must add an additional ~ escape sequence.

Options	Name	Result
~c		The Single Session feature can be enabled or disabled by editing the single_session field in a given port. When a user port level administration access is logged in via pmshell, the port configuration menu can be accessed via any port by pressing the escape character (~ by default) followed by c (~c).
~b	break	Generates a BREAK on the serial port (if you're doing this over ssh, type "~~b").
~h	portlog	Generates a history on the serial port. Displays the traffic logs for the port - must have port logging enabled.
~.	quit	Quits pmshell.
~p	power	Opens the power menu for the port. The port must be configured for a PDU.
~u		Opens the list of user sessions, select by number to disconnect.
~m	chooser	Connects to the port menu - go back to the serial port selection menu.
~?	pmhelp	Displays help message.

CUSTOM CONTROL CODES FOR SERIAL PORTS

Custom control codes can be defined for ease of use per port or can be applied to all ports. For example, users could define a different Power Menu control code for every port, while having a single control code for View History that applies to all ports.

Custom control codes can be used by any user with access to the serial port. In order to run the shortcuts, the user presses the CTRL key + the keycode.

> **Note:** Only Admin users can specify short-cut control codes.

CONFIGURE CUSTOM CONTROL CODES

Admin users can configure control codes for any of the `pmshell` commands through the REST API, ogcli and the new interactive Config Shell.

Control code limitations are as follows:

- Cannot set multiple control codes for a port to use the same keycode
- The available key codes are a-z, excluding ‘i’ and ‘m’ as these can be triggered by commonly used keys TAB and BACKSPACE.

To disable a certain control code for an individual port, set the port’s control code to an empty string.

CONFIGURE CONTROL CODES FOR A SPECIFIED PORT (CLI EXAMPLES)

Control Codes Action	CLI Examples

Set control codes for a given port. In this example, the user sets multiple control codes for port 2	**Note:** `ogcli update port port02 << 'END'`
	`control_code.break="b"`
	`control_code.chooser="c"`
	`control_code.pmhelp="h"`
	`control_code.portlog="l"`
	`control_code.power="p"`
	`control_code.quit="q"`
	`END`

Clear all control codes for a given port, in this example, port 2	**Note:** `ogcli update port port02 << 'END'`
	`control_code.break=""`
	`control_code.chooser=""`
	`control_code.pmhelp=""`
	`control_code.portlog=""`
	`control_code.power=""`
	`control_code.quit=""`
	`END`

CONFIGURE A CONTROL CODE VALUE FOR ALL PORTS

To set a particular control code to one value across all serial ports, Admin users can use the script `set-serial-control-codes` from the CLI as follows:

```
set-serial-control-codes CONTROL_CODE KEY
```

where:

- CONTROL_CODE - Must be one of the following values: `break, chooser, pmhelp, portlog, power` or `quit`.
- KEY - Must be a single lower case letter a-z excluding ‘i' and ‘m’ or an empty string designated by '' which is used to clear the control code.

CONTROL CODES FOR ALL PORTS VIA CLI (EXAMPLES)

Control Codes Action	CLI Examples
Set chooser control code to CTRL-a on all ports	**Note:** `set-serial-control-codes chooser a`
Clear chooser control code on all ports	**Note:** `set-serial-control-codes chooser ''`

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.

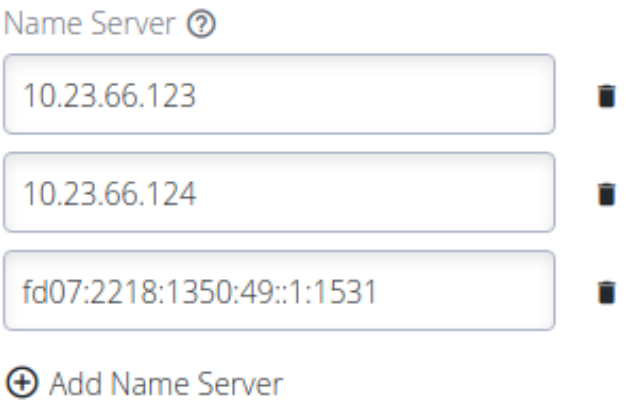
Note: Interfaces must have at least one network connection to be able to perform DNS resolution.

CONFIGURE DNS VIA THE WEB UI

CONFIGURE > NETWORK CONNECTIONS > Network Interfaces

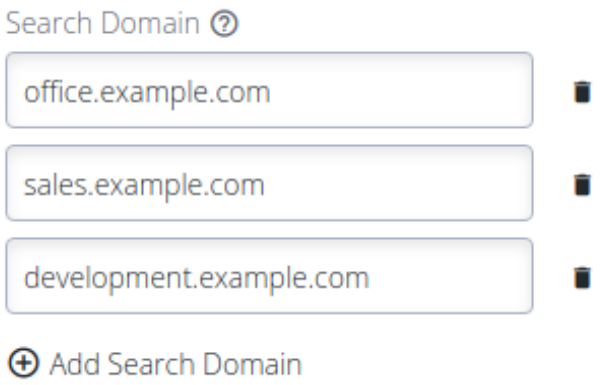
On the Network Interfaces page, select the required interface and click the Edit link.

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 **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.

CONFIGURE DNS VIA THE COMMAND LINE

Description	Command
Display configured DNS settings for an interface	`ogcli get physif "net1"`

Description	Command
Update DNS settings for an interface	ogcli update physif "net1" << 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
Check unbound service status	systemctl status unbound.service
List forward-zones in use	unbound-control list_forwards

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 requires, like libraries and dependencies, and then ship it out as one package. Docker is running by default on the Console Manager. You can access commands by typing docker in the Local Terminal or SSH.

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

DOCKER CM8100 SUPPORT

The CM8100 provides:

- native docker support for the linux/arm/v7 platform.
- additional support for docker container emulation for the linux/amd64 platform.

AMD64 DOCKER CONTAINER USAGE

No additional arguments are required to run an amd64 docker container, however when you run the container the following warning displays:

WARNING: The requested image's platform (linux/amd64) does not match the detected host platform (linux/arm/v7) and no specific platform was requested.

To explicitly specify the linux/amd64 platform when you pull a docker image or run the container, you can provide a `--platform` option .

SYSTEM RESOURCE UTILIZATION

The CM8100 has an ARM v7 CPU with two cores and 2GB of RAM. Supportable docker containers must operate within the CM8100 platform's resources. The commands `docker stats` and Linux `top` are helpful to determine available CPU/Memory consumption versus capacity.

To define the resources that the docker container can consume, you can also provide the `--memory` or `--cpus` and other related options when running the docker container.

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`

Usage
`crontab [options]`
`crontab -n [hostname]`

Option	Description
`-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 have 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 CM (currently FAT32 or ext4) with a file named `manifest.og` in the root directory. This file specifies which provisioning steps are done. An article with a partial description of the file format is available here: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 is 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 login 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 is flashed after boot when 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

password : LH global or bundle enrollment password

bundle : Name of LH enrollment bundle

RESTRICT WEB SERVER REMOTE ACCESS

This setting is intended for deployments where web/API exposure must be eliminated entirely. Most deployments should leave this as the default (true).

By default the appliance's web server (HTTP/HTTPS) is reachable from the network. You can harden the appliance by restricting the web UI/ RESTAPI so it only accepts connections from the appliance itself (via the loopback interface).

> **Note:** This option is NOT recommended for use with Lighthouse. Lighthouse does not support disabling remote access for the web server as it restricts available functions from Lighthouse for the appliance.

This is controlled by a single configuration setting via ogcli, the config shell, or the REST API.

In ogcli

View the current value:

```
ogcli get services/web
```

Disable remote web access (loopback only):

> **Note:** If you disable web access, you can only access the WebUI from the appliance itself.

```
ogcli update services/web <<'END'
allow_remote_access=false
END
```

Re-enable remote web access (all interfaces):

> **Note:** This is the default setting.

```
ogcli update services/web <<'END'
allow_remote_access=true
END
```

In the config shell

```
# config
config: services/web
config(services web): show                                          #
display current value
config(services web): allow_remote_access false      # set the field (true|false)
config(services web): apply                                         # save
and apply the change
config(services web): exit
```

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 following table 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

Button Icon	Definition
	Interface with bond
	Bin widget. **Delete** selected object.