RELEASE NOTES

VERSION 23.10.4

INTRODUCTION

This is a production software release for all Operations Manager and Console Manager CM8100 products. Please check the Operations Manager User Guide or CM8100 User Guide for instructions on how to upgrade your device. Latest appliance software is available on the Opengear Support Software download portal.

SUPPORTED PRODUCTS

- OM1200
- OM2200
- CM8100

KNOWN ISSUES

- NG-6282 A valid user configured with no access rights can log into the REST API and get a session. The user is not immediately logged back out but can not access any resources either.
- NG-7848 The cellular modem sometimes fails to detect the SIM.
- NG-7886 The Wireguard listening port is not correctly configured by the POST request for the default case. A subsequent PUT request is needed to set the port.
- NG-8304 Default setting of POTS modem baud on relevant SKUs is too high

CHANGE LOG

Production release: A production release contains new features, enhancements, security fixes and defect fixes.

Patch release: A patch release contains only security fixes, high priority defect fixes and minor feature enhancements.

23.10.4 (February 2024)

This is a patch release.

Defect Fixes

- **Remote Password Only users (AAA)**
  - Improved implementation of a fixed issue that prevented upgrading to 23.10.0 or 23.10.1 when “Remote Password Only” local users exist on the device. Also prevents bootlooping if a “Remote Password Only” user is created after upgrading to 23.10.0 or 23.10.1. [NG-8338]

23.10.3 (February 2024)

This is a patch release.

Features

- **Configuration Diff**
  - A feature has been added to ogcli so that it will compare the running configuration with a provided template file. [NG-8850]

Defect Fixes

- **FIPS Provider Version**
  - The OpenSSL FIPS provider version is pinned at 3.0.8 which is certified as compliant with FIPS 140-2. [NG-8767]
- **Static Routes**
  - Fixed an issue where a static route with a gateway but no interface would be incorrectly identified as missing, causing it to be removed and added every 30 seconds. [NG-8957]

23.10.2 (November 2023)

This is a patch release.

Defect Fixes

- **Remote Password Only users (AAA)**
  - Fixed an issue that prevented upgrading to 23.10.0 or 23.10.1 when “Remote Password Only” local users exist on the device. Also prevents bootlooping if a “Remote Password Only” user is created after upgrading to 23.10.0 or 23.10.1. [NG-8338]

23.10.1 (November 2023)

This is a patch release.

Defect Fixes

- **Config Import**
  - Fixed an issue where ogcli import would fail if there was an SSH key in the export file. [NG-8258].

23.10.0 (October 2023)

Features

- **Support for OM models equipped with a PSTN Dial-Up modem** • A dial-in console is available on console servers with build in POTS modems (-M models). The modem is configurable via the CLI and Web UI.
- **Configurable single session restriction on serial ports** • When configured, sessions on serial ports are exclusive so that other users cannot access the serial port while it is in use.
- **Port configuration from pmshell** • While in a pmshell session, a user with the right access permissions can escape to the port menu and enter a configuration mode where settings such as the baud rate can be changed.
- **Prevent “default” being used as password beyond factory reset** • This security enhancement prevents the default password being reused.
- **Wireguard VPN** • Wireguard VPN is fast and easy to configure. It can be configured via the CLI and REST API.
- **Configuration support for OSPF Routing Protocol** • OSPF is a route discovery protocol which previously had limited support. Full configuration support via the CLI and REST API is now supported.

Enhancements

- NG-6132 Support Windows line endings in ZTP manifest files.
- NG-6159 Added logging for ZTP missing image or wrong type of image.
- NG-6223 Add traceroute6 to the image.

Security Fixes

- NG-5216 Updated the Web UI to allow services/https to use larger number of bits when generating a Certificate Signing Request (CSR).
- NG-6048 Change to use SHA-512 passwords by default (not SHA-256).
- NG-6169 Added a syslog message upon successful login through the Web UI (REST API).
- NG-6233 Web UI: clear the password field when the wrong password is entered.
- NG-6354 Patched CVE-2023-22745 tpm2-tss buffer overrun.
- NG-8059 Upgraded LLDP to version 1.0.17 to address CVE-2023-41910 and CVE-2021-43612

Defect Fixes

- NG-3113 Fixed an issue where pinout did not work as expected for local consoles on OM2200.
- NG-3246 `services/snmpd` now keeps persistent data between reboots. Prior to this change, runtime persistent data such as `snmpEngineBoots` would be cleared each time the device rebooted.
- NG-3651 Fixed an issue where creating and deleting a bridge left old entries in the perifrouted firewall table.

- NG-3678 Better handling of duplicate IP addresses in config.
- NG-4080 Fixed an issue where management port settings other than baud were ignored.
- NG-4289 Fixed issue with DHCP leases repeatedly triggering lighthouse config resyncs.
- NG-4355 Fixed an issue where a getty would run when the management port was disabled (by only allowing kernel debug on an enabled management port).
- NG-4779 Fixed an issue where the Remote Authentication page would reject changes with a cryptic error (when the optional accounting server was blank).
- NG-5344 Fixed an issue where invalid baud rates were offered for management ports.
- NG-5421 Added a check to the groups endpoints to prevent them from overwriting system groups.
- NG-5499 Fixed an issue where invalid baud rates were offered for serial ports.
- NG-5648 Fail-over banner behavior fixed when failover is disabled.
- NG-5968 RAML documentation fix *(execution_id for script template)*.
- NG-6001 Fixed an issue where misleading static defaults were being used for LLDP. Now LLDP's own defaults are used.
- NG-6062 Fixed an issue where an IPSec tunnel set to initiate did not attempt to re-connect after the peer closes the link.
- NG-6079 Raritan PX2 PDU driver update to work with newest Raritan firmware.
- NG-6087 Allow adding USB ports to port autodiscovery.
- NG-6147 Fix an issue where sfp_info would appear to work (but fail) on OM2200-10G.
- NG-6147 The support report is now more explicit about the support (or lack thereof) for SFP on each Ethernet interface.
- NG-6192 Fixed an issue where port_discovery –no-apply-config could not discover ports.
- NG-6223 Switch traceroute from busybox to the standalone verison.
- NG-6249 Fixed an issue where stopping salt-master would cause a stack trace in the log.
- NG-6300 Fixed issue where ogcli restore command could remove cellular config.
- NG-6301 Disabled redis dababase snapshotting.
- NG-6305 Fixed an issue where port logging options were presented for local consoles.
- NG-6370 Fixed an issue where DHCP option 43 (ZTP) decoding could fail and prevent the interface from being displayed as up.
- NG-6373 Fixed an issue where invalid serial settings (data bits, parity, stop bits) were offered on serial ports and management ports.
- NG-6423 Loopback tool waits for port manager to exit before starting.
- NG-6444 Fixed an issue that allowed VLAN's to be created on the wrong interface.
- NG-6806 SSH access to the device allowed even if /run partition is full.
- NG-6814 Fixed an issue where unnecessary data was included in config exports.
- NG-6827 Fixed an issue where messages were cut off before the login prompt is printed. This was most noticeable when running the console at 9600 baud (default speed for CM8100).
- NG-6865 NG-6910 NG-6914 NG-6928 NG-6933 NG-6958 NG-6096 NG-6103 NG-6105 NG-6108 NG-6127 NG-6153 Fixed many small config shell parsing and data consistency problems.
- NG-6953 Loading pmshell history with ~h option fixed.
- NG-7010 Fix for ssh access rejection when /run partition full.
- NG-7087 Fixed issue with SNMP Service page not loading sometimes.

- NG-7326 Fix rich rules missing service problem.
- NG-7327 Fix routes metrics when fail-over is complete.
- NG-7455 NG-7530 Fixed bridging issue on 24E switch models.
- NG-7491 Default configuration for OSPF daemon fixed to avoid crash.
- NG-7528 Fixed an issue where CM8100 devices could not connect to Cisco USB consoles.
- NG-7534 Fixed an issue causing high CPU at boot by disabling an unnecessary component in rngd.
- NG-7585 Fix Editing Bonds/Bridges to show user errors on web UI.

23.03.3 (May 2023)

This is a patch release.

Enhancements

- **Support Report**
  - Added cell modem info to the support report.
  - Added more logs such as web server, migration and serial port autodiscovery.
  - Restructured the zipped report to include subfolders.
  - Performance improvements for displaying the syslog.

Defect Fixes

- **Serial Port Autodiscovery**
  - Fixed an issue where serial breaks (received as NULL) would prevent port_discovery from working as expected. Now, all non-printable characters are stripped from the detected port label [NG-5751].
  - Fixed an issue where port discovery could not detect Cisco stacked switches [NG-5231].
- Kernel debug on serial ports [NG-6681]
  - Avoid various issues with kernel debug on serial ports by disabling it in all cases except for serial port 1 on OM1200.
  - This does not affect management ports on OM2200 and CM8100, as they are handled separately to serial ports.
- Improved error handling for firewall configurator [NG-6611]

23.03.2 (April 2023)

This is a production release.

Important Note

- Any customers who previously upgraded to version 23.03.1 should immediately upgrade to the latest release to avoid an issue related to custom firewall rules, as well as serial ports configured for X1 pinout. Relevant defect fixes:
  - Custom firewall rules can disappear on reboot after upgrade [NG-6447].
  - Serial ports in X1 mode can stop working after reboot [NG-6448].

Features

Configuration Shell: New Functionality

Single line Multi-field Configuration

• Prior to to these changes, configuration could only be updated one field at a time using multiple navigation commands. Configuration for several fields has been consolidated into a single command which will also improve ability for users to transfer config between devices.

Support for Configuration Import and Export

• This feature allows for users to import and export their devices' configurations through the Configuration Shell. Configuration Shell importing is compatible with configurations exported using `ogcli`. However, exports done with the Configuration Shell will not be compatible with `ogcli import`.

Other Enhancements

• Added `?` command to provide context-dependent help for individual commands or properties. For example, `user root groups ?` will provide documentation for `groups`.
• Added the `show-config` command to easily display a device's entire configuration.
• Added new `system/version` endpoint to view multiple system version details in one location.

Trusted Source Networks • This feature extends existing permitted services functionality to enable users to permit access to specific network services for a specified IP address or address range. Previously, users could only permit services for all IP addresses without fine-grain control for specific address or address ranges.

Upon upgrade from prior releases, existing permitted services will be updated to use this new format without altering functionality. Existing permitted services on previous software releases will be enabled by default for all IPv4 and IPv6 addresses.

Second Ping Failover Test • This feature enables users to configure an additional probe address for failover tests. Previously, users could specify a single address that, when unreachable, would trigger failover to cellular. If two probe addresses have been provided, failover will only activate when both addresses are unreachable.

CM8100-10G Support • This release contains support for CM8100-10G products.

Security Fixes

- Fixed obfuscated passwords exposed with page source modification [NG-5116]
- OpenSSL CVE-2023-0286 Type confusion vulnerability for X.509 GeneralNames containing X.400 addresses
- OpenSSL CVE-2023-0215 Use-after-free when streaming ASN.1 data via BIO
- OpenSSL CVE-2022-4450 Double-free vulnerability when reading invalid PEM in certain scenarios
- Several other CVEs and security fixes were brought in with the Yocto upgrade from Hardknott (3.3.6) to Kirkstone (4.0.7)
- Fixed obfuscated passwords exposed with page source modification [NG-5116]

Defect Fixes

- Bond in bridge using switch ports not working [NG-3767].
- Error when editing default NET1 DHCP connection [NG-4206].
- `ogpower` command not working for admin users [NG-4535].
- OM22xx devices sending SNMP traffic with incorrect source address [NG-4545].

- MTU for cellular connections not being configurable [NG-4886].
- OM1208-E-L not able to send SNMP traps over IPv6 [NG-4963].
- OpenVPN for former Primary Lighthouse instance not being removed when secondary Lighthouse instance is promoted [NG-5414].
- Admin users not having write access to attached USB storage [NG-5417].
- Inconsistent naming for Operations Manager interfaces [NG-5477].
- Set the SNMP product code to the family of the device rather than a single, fixed value. The SNMP MIB has been updated with the new family codes. [NG-5500].
- `curl` not supporting use with a proxy on Operation Manager devices [NG-5774].
- `pmshell` to port not working when the escape character is set to '&' [NG-6130].

22.11.0 (November 2022)

This is a production release.

Features

Operational Permissions • This feature provides a new framework and new UI to support operational permissions. When creating a new group, the user is presented with more permissions options so that they can fine-tune the role to suit their needs. The groups configuration now allows selecting more permissions to allow fine-grained control over which operations will be permitted to access the selected devices. It allows the administrator to create groups that have full access (administrator rights) or some operational permissions by choosing a combination of devices and their access rights.

In previous versions of product (22.06.x and older) each group was assigned a single Role, either Administrator or Console User. The permissions assigned to each role were hard-coded by the product with no customization available for the end user, administrator or otherwise.

This "operational permissions" feature changes the model used for assigning permissions to groups by replacing the concept of a Role with a configurable set of Access Rights. 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.

The assignment of a user into specific groups has not changed; a user can be a member of any number of groups and inherits all of the access rights from all of the groups they are a member of.

This release introduces the following access rights:

- admin - Permits access to everything, including shell.
- web_ui - Permits access for an authenticated user to basic status information via the web interface and rest API.
- pmshell - Permits access to devices connected to serial ports. Does not give permission to configure serial ports.
- port_config - Permits access to configure serial ports. Does not give permission to access the device attached to each serial port.

When upgrading from a previous release, the group's role is upgraded to a set of access rights as follows:

- Role (Before Upgrade) - Administrator / Access Rights (After Upgrade) - admin
- Role (Before Upgrade) - Console User / Access Rights (After Upgrade) - web_ui,

pmshell

The following is a summary of the changes:

The Configure / Groups page has been redesigned to allow assignment of access rights to the group (for holders of the admin access right only).

Users with the port_config access right now have the ability to configure serial ports, including port autodiscovery.

Existing Administrator users should see no other functional changes in either the web UI, bash shell, or pmshell. Existing Console Users should see no functional changes.

NTP Key Support • This feature provides the ability for the definition of one or more NTP servers and the definition and enforcement of NTP key authentication. A user can now supply NTP Authentication Key and NTP Authentication Key identifier. The user has an option of whether or not they want to utilize NTP Authentication Keys. NTP keys have the same obfuscation behaviour as passwords. If NTP Authentication keys are in use, the NTP server is verified using the Authentication Key and Authentication Key Index before synchronizing time with the server.

Power Monitor Syslog Alerts • This feature provides the ability to receive an appropriately severe log alert when unacceptable voltage levels are present so that the user can ensure they are aware of any power anomalies that occur on devices within their control.

Display Serial Signals • This feature provides the ability to view serial port statistics in the UI. The following information is displayed under Access > Serial Ports when the individual serial ports are expanded:

- Rx byte counter
- Tx byte counter
- Signalling information (DSR, DTR, RTS and DCD)

Enhancements

Serial Port Autodiscovery • Several enhancements have been made to the Serial Port Autodiscovery feature to provide a better overall user experience. The enhancements include the following items.

- Attempt first discovery run using currently configured port settings (current baud rate, etc.)
- Fetch or use pre-configured credentials to login and discover the hostname from e.g. the OS prompt, for devices that don’t display hostname pre-authentication.
- Syslogging enhancement to help users diagnose common issues (e.g. no comms whatsoever, hostname failed validation).
- UI display of error messages and logs with the reason for auto-discovery failure, e.g 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, etc.
- The logs for the last-run instance of autodiscovery are saved.
- Users can configure Serial Port Autodiscovery to run on a determined schedule or trigger a single instance.

Configuration Shell •The new interactive CLI tool gives the user a more guided

experience when configuring a device from the command line interface. It is launched by typing `config` from the shell prompt. The existing `ogcli` tool continues to be available and is particularly suited for scripting. The Phase 2 enhancement includes access to all endpoints available in ogcli with extensive help throughout the configuration steps. There is also simple navigation commands throughout the configuration steps. All user config can be configured using the Interactive CLI.

New functionality

- `config --help` This command will display base level help output.
- `top` This command navigates to the top of the configuration hierarchy. Previously, when a user was several contexts deep, they had to issue the 'up' command a number of times to return to the top context. Now the user can issue the 'top' command just once to achieve the same effect.
- `show [entity name]` The show command now accepts an argument to display the value of a field or entity. `show description` displays the value of the description field and `show user` displays the values of the user entity. For a field example, `show description` is equivalent to description. For an entity example, `show user` is equivalent to user, show, up. This includes autocompletion support and updated help text for `config --help`.

Security Fixes

- 22.11 security audit improvements [NG-5279]
  - Add X-XSS-Protection header
  - Add X-Content-Type-Options header
  - Add X-Frame-Options header
  - Add Cross-Origin-Resource-Policy header

Defect Fixes

- Added support for dual-console Cisco devices. [NG-3846]
- Fixed memory leaks affecting the REST API. [NG-4105]
- Fixed issue with special characters in port labels and descriptions breaking access. [NG-4438]
- Fixed an issue where infod2redis could partially crash and then use up all memory on the device. [NG-4510]
- Fixes an issue upgrading to 22.06.0 with 2 or more lanX physifs. [NG-4628]
- Fix a number of bugs causing memory leaks when port logging is enabled and fixed the erroneous writing of port logs to /var/log. [NG-4706]
- Removed log noise about lh_resync (Lighthouse resync) when not enrolled to Lighthouse. [NG-4815]
- Updated documentation for the services/https endpoint so make its functions and requirements clearer. [NG-4885]
- Fixed modem-watcher to correctly explain that active SIM is absent. [NG-4930]
- Set the mode of a port to something other than consoleServer disconnects any active sessions. [NG-4979]
- Fixed an issue where factory_reset incorrectly enabled "rollback" for the current slot. [NG-4599]
- Implement the new IP Passthrough specification. [NG-4440]
- Cleaned up modem-watcher errors in logs. [NG-3654]
- Cleaned up log spam from info2redis. [NG-3674]
- Removed 'script called with parameter ra-updated' logspam. [NG-3675]

- Fixed the portmanager so it no longer locks up under rare cases (or when using the undocumented ‘single connection’ feature). [NG-4195]
- Fixed salt-sproxy to avoid leaks and OOM. [NG-4227]
- Fixed the pmshell so -l works. [NG-4229]
- Resolved the AT+COPS commands that had a disruptive side-effect on cellular connections [NG-4292]
- Fixed the cellmodem status endpoint to show IPv4 or IPv6 addresses [NG-4389]
- Local traffic cannot leave the modem with the wrong source address. [NG-4417]
- Lighthouse is now notified when the cellular modem comes up and down. [NG-4461]
- All configuratorsare run on upgrade, to ensure data migration and consistency. [NG-4469]
- Support reports now include “failed upgrade logs” if applicable. [NG-4738]
- Fixed a bootloop caused by removing all firewall services. [NG-4851]
- Fixed an issue breaking access to a device via ethernet while failed over. [NG-4882]
- Fixed uploading of a certificate for a pending CSR from the web UI. [NG-5217]

22.06.0 (June 2022)

This is a production release.

Features

CM8100 Support • This is the first release supporting the upcoming CM8100 Console Manager.

Configuration Shell • A new interactive CLI tool gives the user a more guided experience when configuring the device from the command line interface. It is launched by typing `config` from the shell prompt. The existing `ogcli` tool continues to be available and is particularly suited for scripting.

Enhancements

pmshell Control Codes • Control codes can be assigned to any of the existing pmshell commands. For example, the following command assigns `ctrl-p` to the *choose ports* command, `ctrl-h` to the *show help* command, and `ctrl-c` to quit pmshell, applicable only when connected to *port01*. Control codes are configured *per-port*.

```
ogcli update port "port01" << END
  control_code.chooser="p"
  control_code.pmhelp="h"
  control_code.quit="c"
END
```

The `set-serial-control-codes` script is a convenient way of assigning the same control code to all ports. For example, `set-serial-control-codes chooser p` to assign `ctrl-p` to the *choose ports* command for *all* ports.

pmshell Console Session Timeout • A console session is terminated if it has been idle for longer than the configurable timeout period. The timeout period is configured on the *Session Settings* page of the web UI, or using the `system/session_timeout` endpoint. The timeout is specified in minutes, where 0 is “never timeout” and 1440 is the largest allowable value. The following example sets the timeout to five minutes.

- `ogcli update system/session_timeout serial_port_timeout=5`

pmshell Reload Configuration • Changes made to pmshell configuration are now immediately applied to any active sessions.

TACACS+ Accounting • It is now possible to enable or disable sending of accounting logs to a TACACS+ authentication server. When enabled (true by default), logs are sent to the first available remote authentication server. It is not possible to configure an accounting server that is distinct from the authentication server. Accounting is configured via the web UI, or using the `auth` endpoint. The following example disables accounting.

- `ogcli update auth tacacsAccountingEnabled=false`

Configurable Net-Net Failover Interface • The failover interface can now be configured on the *OOB Failover* page. Previously the failover interface was implicitly always the cell modem interface. Since this feature no longer requires a cell modem, the *OOB Failover* page is now available on all devices, even those without a cell modem. The language for the DNS queries configuration item has also been clarified.

Security Fixes

Fix CVE-2022-1015 • Pertains to an out-of-bounds access due to insufficient validation of input arguments, and can lead to arbitrary code execution and local privilege escalation by extension. [NG-4101]

Fix CVE-2022-1016 • Pertains to related insufficient stack variable initialization, which can be used to leak a large variety of kernel data to userspace. [NG-4101]

Defect Fixes

Web UI

- With the *Add New SNMP Alert Manager* page there is now default placeholder text for server address (127.0.01) and port (162). [NG-3563]
- With the *Remote Authentication* page there is now a prompt to set the remote authentication server address. Previously a user had to submit an empty value before being notified of missing data. [NG-3636]
- With the *System Upgrade* page improve reporting for software installation errors. [NG-3773, NG-4102]
- With the sidebar, multiple top-level page groupings can be open at once (e.g. *Monitor*, *Access*, and *Configure*). [NG-4075]
- Fix the web UI being logged out when invalid values are entered for *Web Session Timeout* on the *Session Settings* page. [NG-3912]
- Fix rendering glitch with the *System* or *Help* popover menus when viewing in narrow windows. [NG-2868]
- Fix accessing `https://<ip>/terminal` results in a quick error loop. [NG-3328]
- Fix closing and opening the browser may allow access to the device without allowing access to the web terminal. [NG-3329]
- Fix cannot create a SNMP v3 PDU. [NG-3445]

- Fix network interfaces are not displayed in the right order on multiple pages. [NG-3749]
- Fix no loading transition screen between services pages. Switching between slower loading service pages now provides a visual cue that something is happening. [NG-3776]
- Fix unexpected UI changes when creating a user with the name ‘root’ on the *New User* page. [NG-3841]
- Fix being able to press “apply” while sending the request on the *New VLAN Interface*, *Session Settings*, and *Administration* pages. [NG-3884, NG-3929, NG-4058]
- Fix bad data sent when applying configuration on the *SNMP Service* page. [NG-3931]
- Fix web session timeout does not apply to console user. [NG-4070]
- Fix `Docker Runtime Information` in the support report which previously showed nothing meaningful. [NG-4160]
- Fix IPSec prints errors in support report when disabled. [NG-4161]

ogcli and Rest API

- Fix static route rest API validation doesn’t allow valid static routes. [NG-3039]
- Fix to improve error reporting in the rest API when a password is not provided for the root user. [NG-3241]
- Fix to allow interface of static routes to be referenced by both id or device. [NG-3039]
- Fix to improve ogcli help text for the “ogcli replace groups” example, to more clearly differentiate between *update* and *replace* operations, and to simplify the basic `ogcli --help` text. [NG-3893]
- Fix ogcli merge users command failing when remote-only users are present. [NG-3896]

Other

- Fix pmshell incorrectly listing port01 as available on a OM1200 when it is not. [NG-3632]
- Fix duplicate Lighthouse enrolment attempts succeeding when only one should succeed. [NG-3633]
- Fix RTC clock is not being updated with NTP sync (OM1200 and OM2200). [NG-3801]
- Fix Fail2Ban counts multiple attempts on login for disabled user. [NG-3828]
- Fix port logs forwarded to a remote syslog server no longer include port label. [NG-2232]
- Fix SNMP networking alerts do not work for cell interface link state. [NG-3164]

- Fix can’t select all ports using `ports=null` for ports auto-discovery. [NG-3390]
- Fix excessive logspam from “ogconfig-srv”. [NG-3676]
- Fix unable to discover PDU outlets over USB dongle. [NG-3902]
- Fix fail upgrade when /etc/hosts is “empty”. [NG-3941]
- Fix disabling root account on OM means Lighthouse can’t pmshell to ports. [NG-3942]
- Fix Spanning Tree Protocol not working on -8E and -24E devices. [NG-3858]
- Fix OM22xx-24E switch ports (9-24) in a bond do not receive LACP packets. [NG-3821]
- Fix switch ports not initialised on first boot when upgrading a -24E device. [NG-3854]
- Fix time-synchronization issue preventing enrollment with Lighthouse 22.Q1.0. [NG-4422]

21.Q3.1 (April 2022)

This is a patch release.

Security Fixes

- Fixed CVE-2022-0847 (The Dirty Pipe Vulnerability)
- Fixed CVE-2022-0778

Defect Fixes

- Exporting config when cellular is enabled no longer produces invalid config.
- Removed some noisy logs about signal strength when cellular is disabled.
- Changed SNMPv3 Engine ID to display in GUI.
- Changed SNMPv3 Engine ID to be generated based on the MAC address of net1.
- Improved validation of state route configuration (made more permissive).
- Increased groupname limit to 60 characters.
- Fixed cellular modems still responding to ping and holding an IP address even after disabling cellular.
- Fixed an issue with the parsing of wildcards in the rules for interzone forwarding.

21.Q3.0 (November 2021)

This is a production release.

Features

- Allow DNS Search Domains to be set
- Support bonds in bridges via ogcli
- Static Routes UI
- Brute Force Protection
- TFTP server
- Configuration overwrite
- Configuration backup and restore via Web UI

Enhancements

- Improve ogcli built-in help
- Improve ogcli port naming syntax
- Display hostnames that include . fully
- More than three DNS nameservers can be configured
- Prioritize DNS on failover interface during out-of-band failover

Security Fixes

- Upgraded Yocto from Gatesgarth to Hardknott
- SNMP RO community strings appear in cleartext
- Password for serial PDU is visible when typing it in
- Download links leak the session token

Defect Fixes

- Fixed a race condition that could cause issues bringing up the cell modem on fresh/factory reset devices.
- Fixed an issue with serial port IP aliases incorrectly overwriting the network interface configuration on update.
- Fixed an issue with remote AAA authentication negotiation when using IP aliasing.
- Fixed an issue with installing new firmware images from a USB device.
- Improved the resource usage of the ogpsmon service.
- Improved the information display/layout for PDUs.
- Improved the stability and usability of ogcli via the addition of a number of crash fixes and endpoint specific help/error messages.
- Fixed an issue preventing the bridging of NET1 and switch ports for OM1200 devices.
- Reduced the amount of spurious log noise resulting from SNMP updates.
- Allowed manual setting of https certificate which bypasses CSR generation.
- Added support for the SNMP Controlled TrippLite LX and ATS LX Platform SNMP drivers.

21.Q2.1 (July 2021)

This is a patch release.

Defect Fixes

- Fixed issue where nginx service would fail on bootup after a system upgrade

21.Q2.0 (June 2021)

This is a production release.

Features

- Support for IPsec configuration
  - x509 certificate authentication
  - Dead Peer Detection (DPD)
  - Enhanced IPsec configuration options
- Improved support for automatic failover
  - Includes a SIM activated timestamp to show when failover takes place
  - Improved support for Verizon and AT&T

- Added SNMP Traps for PSUs
- ZTP Enhancements
- Added default password obfuscation and masking to ogcli

Defect Fixes

- Cell connection with a SIM card that requires a password will not connect
- URLs are not correctly validated
- Using ogcli commands in ZTP over USB script fails
- ogcli import [TAB] does not auto-complete existing files
- ttyd segfaults on exit
- systemd crashes in software boot when USB stick is inserted
- ogcli update fails when 2 items are added to a list
- Help text on Cellular SIM Failover does not change when selecting active SIM
- rsyslog collects debug logs showing passwords in clear text
- Web-UI “Cycle All Outlets” button/link fails when no outlets are selected
- v1 RAML is not compatible with raml2html
- Triggered auto-response playbooks dropdown menus fail after selecting an option
- SNMP temperature alert trap may not trigger in time
- Connecting a Cisco console does not reload portmanager as it should
- Ember proxy doesn’t work because of a cookie problem
- RTC self-test randomly fails
- USB-serial port incorrectly allows setting localConsole mode
- LDAPDownLocal with bad server key doesn’t fall back to local accounts
- TACACS+ errors when server returns large packet of Authorizations
- Local PDU breaks on port import
- puginstall downloads to /tmp (ie. tmpfs)
- Power select seems to be defaulting to allow search and does not work much of the time
- OM12XX has an empty Local Management Consoles page
- Entering an invalid URL for firmware upgrade results in a very long wait
- Uploaded images that fail to install are not removed until reboot
- ModemWatcher doesnt update sim, cellUim, or slotState for telemetry and SNMP
- Interzone forwarding to/from LHVPN zone is broken
- Removed weak ciphers from default SSH and SSL configuration options
    - Upgraded devices from older firmware versions will still have weak ciphers enabled

21.Q1.1 (May 2021)

This is a patch release.

Defect Fixes

- Remote syslog can log SNMPv3 PDU credentials in debug mode
- Connecting to a Cisco console via USB did not work
- Booting while connected to a Cisco 2960-X USB console would prevent it from working
- USB drive may not be mounted on boot, causing ZTP to fail
- ogcli update could not append multiple items to a list

21.Q1.0 (March 2021)

This is a production release.

Features

- Support for OM120xx SKUs with dual AC power supply
- Support for OM2224-24E SKUs
- Improved list access in ogcli
- Remove Non-Inclusive Language References from WebUI
- SNMP Traps for PSU and system temperature
- Automatic failover support - AT&T and Verizon
- Password Complexity Enforcement
- New bridge inherits MAC address of the primary interface

Defect Fixes

- ModemManager can probe the local console
- Description field on create bond/bridge is not cleared after submit
- 10G IPv6 crashes
- “ogcli update” is broken for all non-cellular interfaces
- Deleting an aggregate underneath a VLAN gives a confusing error message
- Cell Modems may come out of Auto-SIM mode
- “Internal Error.” is not a useful REST API error message
- Changing sim during failover causes device to come out of failover mode
- Allow uploading of firmware images over 400M
- “Port Number for Direct SSH Links” not working
- Console user can see the edit button on Access > Serial Ports page
- Aggregate creation errors not shown in web UI when f2c/failover is updated
- SNMP agent sometimes reports ports out of order
- Port Discovery requires multiple runs to complete
- Inform user of failure to add IP Alias to serial port configured as a local console
- Auto-Response Salt Master and Minion may not always sync keys
- REST failure messages not correctly reported in WebUI on Network Interfaces page
- Firewall Interzone Policy dropdowns show duplicate values when adding multiple entries
    - Redesigned UI to improve user experience
- odhcp6c script removes all IPv6 addresses and routes every time an RA event occurs
- search parameters in ‘/ports’ isn’t working
- Cannot use special characters in cell APN or username
- Portmanager does not re-open USB device after it is connected in some cases
- Access via Lighthouse proxy not working from behind NAT
- Configuration allowed multiple SNMP managers with the same destination and different message-types and protocol.
    - This resulted in multiple messages being received via SNMP.
    - Now it is invalid to have multiple SNMP managers with the same destination; each entry must have a unique combination of host, port and protocol.
    - Note: During upgrade to 21.Q1.0, if multiple entries with the same host, port and protocol are found, only the first entry will be kept.
- Mask client passwords in Support Report output
- Modem not present during initial boot, fails on subsequent boots
- Session tokens visible in URLs
- Session APIs are updated to not contain any session tokens
- Compatibility note for CURL users: POSTing to sessions and following the redirect (-L) without allowing cookies (-c /dev/null) will result in an error

20.Q4.0 (October 2020)

This is a production release.

Features

- Remote syslog support for port logs
- Support for Multiple SNMP managers
- Dual SIM Support
- Support for additional OM12XX SKUs
- Added the ability to use unauthenticated SSH to console ports
- Configurable RemoteDownLocal/RemoteLocal policies for AAA
- Editing interfaces in existing aggregates
- The ability to enable spanning tree protocol on bridges
- Upgraded Yocto from Zeus to Dunfell

Defect Fixes

- When deleting bond interfaces, the web UI can identify the primary interface incorrectly
- Auto response reactions can not always be removed in UI
- IP Passthrough status can display incorrectly if interface is changed
- SNMP Manager V3 password is not set correctly and does not appear in export
- Firewall services with spaces should be invalid
- SNMP Service does not support IPv6
- Ogcli -j import fails when any property contains an apostrophe
- Ogtelem snmp agent using 6% cpu
- Firmware upgrade via WebUI using file upload doesn’t work on OM1204/1208
- ssh to a bad port/label does not return expected error
- SNMP Alert Managers do not support IPv6 transport protocols
- Port forward does not work with perifrouted
- IPv6 cellular addresses are not reported in the UI
- Port forwarding does not work as expected on connections other than net1
- Port forwarding does not behave as expected for IPV6

20.Q3.0 (Jul 2020)

This is a production release.

Features

- Support for a configurable Login Banner for SSH and Web-UI
- Discover 9600 baud serial devices before other speeds
- Speed up Auto-Response Triggered Playbooks Web-UI page loading time
- Miscellaneous Web-UI wording changes
- Software support for new SKUs, OM2248-10G and OM2248-10G-L
- SNMP Service support for telemetry state
- Allow device configuration import and export
- Support to provision via USB key
- Support for IPv4/v6 Firewall Interzone Policies
- Support for Firewall zone custom/rich rules
- Improved ogcli error reporting
- Upgraded Yocto from Warrior to Zeus
- Upgraded Ember JS from 2.18 to 3.0.4

Defect Fixes

- When unenrolling from a primary Lighthouse instance ensure the device is also unenrolled from secondary Lighthouse instances
- Switch uplink interface is unable to send/receive frames

20.Q2.0 (Apr 2020)

This is a production release.

Features

- Software support for 10G SKU
- Software support for Ethernet Switch SKU
- Auto-Response Network Automation Solution
- 802.1Q VLAN Interfaces support
- Firewall Masquerading (SNAT)
- Firewall Port Forwarding
- PDU Control support
- Opengear Command Line Interface tool (ogcli)
- Static Route Support
- Console Autodiscovery Enhancements
- OOB Failover Enhancements

Defect Fixes

- Salt version on the Operations Manager has been upgraded from version 3000 to 3000.2
- Unable to change pinout mode on certain ports.
- LH proxy breaks Web UI static resources.
- Cannot connect to a remote TFTP server.
- Refreshing the Web UI causes the sidebar navigation to lose place on some pages.
- Deleting Multiple (3+) External Syslog Servers in a single operation causes Web UI errors.
- Serial port mode cannot be changed to ‘Console Server’ mode after configuring to ‘Local Console’ mode.
- Local Users ‘Disable/Delete Selected’ actions fail but claim to succeed on the Web UI.
- Adding a gateway using a static connection sets that gateway’s route metric to 0.
- OM12xx firmware sends several lines to front serial port 1 on boot.
- Web UI fails to update USB serial port configuration.
- Auto Response reactions/beacons REST endpoints with missing module specific table return errors.
- Web UI dark mode dialog box background and text too light.
- Auto Response REST API has various bugs in JSON/RAML.
- Port 1 default mode should be “local console” on OM12xx.
- OM12xx USB-A port mapped incorrectly.
- IPv6 network interfaces are not truly deleted when deleted from the Web UI.
- Remote authentication should support IPv6 servers.
- USB serial port Autodiscovery: devices show disconnected after populating hostname.
- REST API allows deletion of uuids under unrelated endpoints.
- Pre-release REST API endpoints have been consolidated or removed as necessary.
- REST API /api/v2/physifs POST fails with a 500 on “Not Found” error.

- REST API /support_report endpoint is not functional for API v1.
- Web UI session does not end session correctly when left on the web terminal.
- Remote AAA users are not granted expected access to device serial ports.
- Serial ports with lengthy label names do not display nicely in the Web UI.
- Support Report sfp_info tool does not work for 1G network ports.
- Using a switch port as the probe address for failover doesn’t work.
- Slow memory leak in ogconfig-srv causes OM22xx to eventually restart after ~125 days.
- Remote AAA user not granted port access via SSH/CLI pmshell.
- Slot switching should only ever be possible in the boot immediately after upgrade.
- Serial port label on access serial ports page can extend into next column.
- Web UI fixes on the Routing Protocol page.
- DELETE /config REST API documentation is incorrect.

20.Q1.0 (Feb 2020)

This is a production release.

Features

- Bonding Support
- Bridging Support
- Console autodiscovery for labeling ports with the hostname of connected devices
- Force password reset on first use / factory reset
- Add support for Lighthouse cell health reports
- Serial port login / out SNMP alerts
- General improvements to user interface and user experience
- Added support for IPSec tunnels
- Improved CLI configuration tool (ogcli)
- Added IPv4 Passthrough support
- Add support for periodic cell connectivity tests
- Support for OM12XX device family
- Lighthouse OM UI Remote Proxy Support

Defect Fixes

- System Upgrade: “Error contacting server.” appears after device begins an upgrade
- Fix issue with removing the last interface from a firewall zone using the web UI
- Improved firewall configuration change response time
- Firewall rules are not updated when a zone is deleted until the page is refreshed
- Ember error shows on network interface web UI page
- Web-UI fails to update USB serial port configuration
- Improved rest api documentation
- Unsaved hostname in Web UI leaks into heading and navigation components
- After importing config backup, web terminal and SSH links on Access Serial Ports do not work
- Log rotation improvements
- Improved exception handling
- IPv6 DNS support for cell modem unreliable
- Kernel using wrong realtime clock
- Interrupting an upgrade prevents further upgrades
- Lighthouse synchronisation improvements
- ZTP fixes and improvements

19.Q4.0 (Nov 2019)

This is a production release.

Features

- Added new CLI configuration tool, ogcli.
- Support for the Network and Cellular LED.
- Support for cellular connections on the Verizon network.
- SNMP v1, v2c, and v3 Trap support for system, networking, serial, authentication, and config changes.
- Cellular modem can now autodetect carrier from SIM card.
- Device now constructs FQDN from hostname and DNS search domain.
- Maximum number of concurrent SSH connections is now user configurable (SSH MaxStartups).
- Added LLDP/CDP support.
- Added support for the following routing protocols:
  - BGP
  - OSPF
  - IS-IS
  - RIP
- Add support for rebooting the device in UI.

Defect Fixes

- Swapped default firewall zone assignment for net1 and net2.
- Removed default static IPv4 address on net2.
- Perl now reinstalled on the system.
- Improved reliability of cellular modems.
- Fixed some issues with IPv6 connectivity.
- Manual date and time setting now persist across reboot.
- Statically assigned cellular IP connections were not correctly appearing in UI.
- Modem was not being enabled correctly if ModemManager was in a disabled state.
- Fixed cell signal strength not being checked again if a previous check failed.
- SIM status was not always being correctly reported in the UI.
- Allow USB ports to be used in pmshell and display them correctly.
- ISO-8859-1 text messages were not being correctly handled.
- Correctly start chronyd for NTP.
- Fixed device stability issue from long-term REST API usage.
- IPv6 NTP servers could not be added in the UI.
- Fixed bug where an in-use IPv6 address could be added as a serial port address.
- Fix return code in REST API for port IP alias.
- Fixed rare issues with cellular failover and scheduled cellular firmware updates.
- Cellular connection was not being correctly brought down when performing cellular firmware upgrades.
- Administrator users were not being given correct rights when using pmshell.
- UI was not accepting valid URLs for system upgrade files.
- REST API was not indicating an error when an invalid date was sent.
- No new port logs appeared after rsyslogd was restarted.
- Changing assignment of interfaces to firewall zones had no effect on the firewall.
- Cellular interface did not come up when iptype was deleted from config.
- In the UI using enter on the keyboard now publishes the change instead of clearing it.

- Web server will now listen on IPv6 addresses.
- Cellular statistics were not updated if the modem was not connected.
- Running systemctl restart firewalld now works correctly.
- RAML documentation for PUT /groups/:id request was incorrect.
- Both network interfaces responded to ARP requests when connected to the same subnet (ARP flux).

19.Q3.0 (July 2019)

This is a production release.

Features

- Cellular failover and out-of-band access.
- Carrier firmware update ability for cellular modem.
- Administrators can force SSH logins via public-key authentication only, on a per-user basis.
- Users can now store their public-keys for SSH authentication in the configuration system.
- Ability to see users connected via pmshell to each serial port.
- User pmshell sessions can be terminated via the web-UI and from inside pmshell.
- Logs are now more efficient with their use of disk space.
- Users are now warned about high levels of disk use.
- Support report displays list of files that have been modified in each config overlay.
- Configuration backups can now be made and imported via ogconfig-cli.

Defect Fixes

- UI now navigates to the login screen as soon as session expires.
- Fixed ogconfig-cli pathof command returning incorrect paths for list items.
- Disabled ability for root user’s group to be changed in the UI.
- Model and serial number were not appearing in web-UI system dropdown.
- Refresh button was not functioning correctly on network interfaces page.
- Ethernet link speed changes were not being applied.
- Conman was bringing down network link unnecessarily on address changes.
- Conman took too long after a reload to notice the Ethernet links were up.
- Fixed missing text on syslog web-UI page.
- Some cell carriers with special characters in there name were not being handled correctly.
- SSL certificate upload via the web-UI was broken.
- Serial port IP Alias changes were being applied without clicking the apply button.
- Web UI terminal pages weren’t updating their page title.
- Serial port direct SSH did not accept public-key authentication.

19.Q2.0 (April 2019)

This is a production release.

Features

- USB console support for front and rear USB ports.
- LH5 enrolment support to ZTP.
- Cellular configuration support to UI and REST API with automatic SIM detection.
- Ruby scripting support for use with Puppet Agent.
- Model now displayed in System Details UI.

- Power LED enabled on front panel. Amber when only one PSU is powered, green if both are.
- Comment character support to ogconfig-cli. Character is '#'
- Upgraded underlying base system packages for security and stability enhancements.
- Support for configuring pmshell escape character.
- Basic support for OM2224-24E models gigabit switch.
- Enabled per-interface default routing.
- User configurable IPv4/v6 Firewall.
- Cellular modem firmware upgrade mechanism for CLI.

Defect Fixes

- Issue with small delay to CLI after login.
- REST API and UI not showing all IPv6 addresses on an interface.
- Incorrect description for Cellular Interface in config.
- Management Console connection wasn't re-establishing after baud rate changes.

18.Q4.0 (December 2018)

This is a production release.

Features

- System upgrade capability

Defect Fixes

- Fix issue in pmshell which produced brief high CPU usage periods
- Removed excessive udhcpc messages
- Updated schema for UART hardware settings

18.Q3.0 (September 2018)

First release for the Opengear OM2200 Operations Manager.

Features

- Built-in cellular modem for use as an Out Of Band connection.
- Dual SFP network ports for Gigabit Ethernet and fiber.
- Secure hardware enclave for storing secrets for encrypting configuration and logs.
- Support for running standalone Docker containers natively on the OM2200.
- Modern HTML5 and JavaScript based Web UI.
- Modern tab-completing configuration shell, ogconfig-cli.
- Consistently validated configuration backend.
- Configurable IPv4 and IPv6 networking stacks.
- Comprehensive REST API for external configuration and control of the OM2200.
- Streamlined user and group configuration and authentication mechanisms, including Radius, TACACS+, and LDAP.
- The ability to enroll and manage the OM2200 with Lighthouse 5.2.2.
- NTP client for accurate time and date settings.
- Support for provisioning the OM2200 via DHCP ZTP.
- Initial support for monitoring the OM2200 via SNMP.
- The ability to manage serial consoles via SSH, Telnet, and WebTerminal.
- Support for running Opengear NetOps Modules.

- Support for the Secure Provisioning NetOps Module which provides a platform to distribute resources and configuration (ZTP) to devices managed by the Lighthouse 5 platform and connected to the OM2200 appliance.