RELEASE NOTES

VERSION 25.11.9

INTRODUCTION

This release is for all Operations Manager and Console Manager products. Please check the Operations Manager User Guide or Console Manager 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
- OM1300
- OM2200
- CM8000
- CM8100

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.

25.11.9 (September 2026)

This is a patch release

Defect fixes

- Fixed ogtelem-snmp-agent parse failure log spam. [NG-13565]
- Fixed defunct processes being left behind by the REST API. [NG-14149]

KNOWN ISSUES

- “Failed to find module 'qmi-wwan'” is falsely reported in the syslog for CM8099-10G-C on boot. [NG-12194]
- The following high severity vulnerabilities affect the urllib2 package, and will be addressed in an upcoming release. [NG-13419]
  - CVE-2026-66418
    - For more information see CVE-2026-66418
  - CVE-2026-66471
    - For more information see CVE-2026-66471

25.11.8 (July 2026)

This is a patch release

Security fixes

- Upgraded OpenSSH to 10.4p1 to address CVEs: CVE-2026-59995, CVE-2026-59996, CVE-2026-59997, CVE-2026-59998, CVE-2026-59999, CVE-2026-60000, CVE-2026-60001, CVE-2026-60002. [NG-14433]
- Upgraded libssh2 from 1.10.0 to 1.11.1 with patches to address CVEs: CVE-2026-7598, CVE-2026-55199 and CVE-2026-55200. [NG-14288]

25.11.7 (June 2026)

This is a patch release

Security Enhancement

- Added support to restrict the webserver to the loopback interface [NG-14158]

  Restrict your Opengear appliance's web server and REST API to local-only access with a single configuration change. Ideal for hardened deployments in untrusted network environments.

  Note: This setting is intended for deployments where web/API exposure must be eliminated entirely. Most deployments should leave this at the default (true). Setting it to false from a remote browser/REST session will drop that session (nginx restarts and no longer accepts remote connections). Always change this setting from a console/SSH session, or be prepared to recover via SSH/console. Other services (e.g. SSH) are unaffected.

  Restricting the web server to the loopback interface will greatly restrict the available functions from Lighthouse for this appliance, such as the Node Web-Management Interface. This option is ***not*** *recommended* to be used with Lighthouse.

  See the Operations Manager User Guide or Console Manager User Guide for more information.

25.11.6 (June 2026)

This is a patch release

Security fixes

- Upgraded nginx from 1.26.3 to 1.30.2 to address CVE-2026-42945 and CVE-2026-49975. [NG-14032]

25.11.5 (May 2026)

This is a patch release

Enhancements

- Allowed local and remote users that have shell access to be able to read the syslogs. [NG-13625]
- Allowed users with the admin group role that have shell access to be able to read the journal. [NG-13625]

Defect fixes

- Fixed an issue where updating the hostname of a device would not update the value during an SNMP-Walk. [NG-13689]
- Fixed an issue where remote authentication groups with spaces were not being matched with local groups with underscores. [NG-13686]
- Raw TCP access will now run as the unauth user instead of root. This fixes an issue where rawTCP will stop working after a reboot until the root user logs in. [NG-13675]
- Reliably enumerate modem on CM81xx when booting. [NG-13770]

Security Fixes

- Disabled CONFIG_CRYPTO_USER_API_AEAD in the kernel config to mitigate “Copy Fail” CVE-2026-31431. [NG-13845]
- Upgraded OpenSSH to 10.3p1 to address CVE-2026-35385, CVE-2026-35386, CVE-2026-35387, CVE-2026-35388 and CVE-2026-35414. [NG-13832]

25.11.4 (March 2026)

This is a patch release

Enhancements

- Added a 5G NSA dormancy indicator to the Cellular status in the Web-UI indicating when that connection is being actively used. [NG-12168]
- Added the LLDP portid_subtype field to the config, allowing it to persist between upgrades. This field allows for either the MAC address or the interface name to be used as the port identifier in an LLDP packet. [NG-13022]
- Added the ability to automatically generate SNMPv3 localized keys from a password. This simplifies the process of generating localized keys and prevents passwords from being stored in a config file in plaintext. [NG-13232]
- Improved ease of device identification by adding the device hostname to the header banner [NG-13324]
- Improved ease of port identification by displaying the serial port number or USB designation in page title and panel heading. [NG-13324]
- UX improvements for SNMPv3 encryption and authentication settings. [NG-13409]
- Made Serial port web terminal session tabs more identifiable by including the hostname in the title. [NG-13184]
- Added the ability to disable perifrouted through ogcli and config shell. [NG-13352]

Defect fixes

- Fixed long port labels being truncated on the Access > Serial Ports page. Port labels should now automatically have line breaks added in response to changes in screen width or text length. [NG-12169]
- Fixed an issue where typing in the serial port web terminal would not prevent the UI from timing out, when multiple windows were open. [NG-13146]
    - Fixed a related issue where opening web terminals on multiple devices via LH UI proxy would not handle session timeout as expected.
- Removed modem-watcher’s redundant logging when SIMs are missing from the cellular modem. [NG-13154]
- Ogcli config diff will now prefer exact matches over diff from default. [NG-13206]
- Ensured OG-OMTELEM-MIB::ogOmCellularUimFailoverState is initialized to 1 (disabled) to prevent it from returning 0 (which isn’t valid for the MIB). [NG-13259]
- Fixed an issue where support-report would write unexpected messages when run from the CLI. In particular, “Did not detect modem installation” is no longer printed when run on a device without a modem. [NG-13260]
- Fixed an issue where the Node Interface IP address could overlap with Wireguard Tunnel Address subnets. [NG-13497]
- Fixed an issue that allowed RAs to be processed on the wrong interface, resulting in IPv6 addresses being unexpectedly assigned to the wrong interface. [NG-11620]
- Fixed an issue where the modem could not be edited without confirming the SIM password. [NG-12423]
- Fixed SIM password handling to allow independent SIM edits. [NG-12434]

- Fixed PDU SNMP credentials not working when special characters were found. [NG-13015]
- Increased the amount of time that PDU status will wait for (60 → 180 seconds). [NG-13101]
- Fixed an issue where NAS-IP for accounting packets was reported incorrectly. [NG-13122]
- Fixed an issue where the SNMP agent was sending invalid values for some MIBs when values were uninitialised. [NG-13305]
- Removed the –complete-bootloader option from puginstall. [NG-13379]

Security Fixes

- Prevented sensitive passwords and values from being logged when an SNMP subprocess fails and returns errors. [NG-13301]
- Upgraded runc to version 1.2.9 to address CVE-2025-31133, CVE-2025-52565 and CVE-2025-52881. [NG-13386]

25.11.3 (January 2026)

This is a patch release

Defect fixes

- Fixed an issue on OM1300 that prevented cellular firmware updates from being able to be performed. [NG-13517]

25.11.2 (January 2026)

This is a patch release

Enhancements

- **OM1300 and CM8000 Support**
  This is the first release supporting the OM1300 Operations Manager and the CM8000 Console Manager.

Defect fixes

- Fixed an issue where bonds on some OM2200-24E switch ports would not pass traffic. [NG-13199]
- Fixed an issue where updating SIM-to-SIM failover settings while it is enabled caused the system to erroneously failover. [NG-13158]

Security Fixes

- Upgraded OpenSSH to version 10.2p1 to fix CVE-2025-61984 and CVE-2025-61985.

25.11.1 (December 2025)

This is a patch release

Defect Fixes

- Fixed an issue where the REST-API for cellular firmware update were failing intermittently. [IM-18887]

25.11.0 (November 2025)

This is a production release

Enhancements

- Added support for cellular firmware upgrades via the REST API via the cellfw endpoint. [IM-17751]
  - Support for upgrading cellular firmware for a single carrier via the cellfw/update endpoint.
  - Support for retrieving the status of that upgrade via the cellfw/upgrade_status endpoint.
  - Support for retrieving the currently installed cellular firmware via the cellfw/installed endpoint.
- Added support for wildcard characters in CSRs and added support for SANS to

CSR and https certificate parsing. [NG-12146], [NG-12905]
- Added indication of current Radio Access Technology (RAT) for active cellular connections (E.g. 4G, 5G-NSA, 5G-SA). [NG-12167]
- Added DTR Mode to serial ports giving the ability to control the DTR/RTS line behavior. [NG-12806]
- Added support for alternate base port feature to work with IPv6. [NG-13004]
- Portmanager now logs informational messages by default. [NG-4360]
- Improved port auto discovery logging. [NG-12895]
- PDU Enhancements:
  - Added SNMP support for Eaton G4 PDUs. [NG-12816]
  - Added improved logging for the ogpower system. [NG-12816]
  - Added SNMP support for APC PDUs. [NG-12811]
  - Added support for Vertiv Geist PDUs. [NG-12864]
  - Added support for PDUs using SNMPv3 algorithms: SHA-224, SHA-256, SHA-384, SHA-512, AES-192, and AES-256. [NG-12901]
  - Added local serial support for APC PDUs using AOS v3.2.0.x. [NG-13099]
  - Improved speed of the initial SNMPv1 probe of PDUs. [NG-4209]
- Added a Cellular Troubleshooting Tool. This is a CLI and Web-UI-based tool that provides a diagnostic summary of the cellular modem status on an Opengear device. It includes key test results, signal metrics, and troubleshooting guidance. [NG-11710]

Security Fixes

- Fixed an issue where some sensitive information was not redacted in the support report. [NG-12884]
- Upgraded Redis to v8.0.0 to fix CVEs CVE-2025-49844, CVE-2025-46817 CVE-2025-46818, CVE-2025-46819, CVE-2025-48367, CVE-2025-27151. [NG-13157], [NG-13221]
- Upgraded edge IQ binary to 4.1.15 to fix CVE CVE-2025-22871. [NG-13167]
- Upgraded containerd in Yocto packages to fix CVE-2024-40635. [NG-13183]
- Upgraded libexpat in Expat to 2.7.3 to fix CVE-2025-59375. [NG-13223]

Defect Fixes

- Applied the user-configured cellular MTU at the 3GPP and USB level as well as the Operating System. [NG-12426]
- Preserve existing gid when modifying pre-existing groups. [NG-12570]
- Auto Response SNMP Action now properly escapes MIB values allowing TRAP and INFORM packets containing spaces and other special characters to be properly sent once it triggers. [NG-12836]
- Fixed an issue where RADIUS auth requests included a Service-Type attribute set to Authenticate Only. This is no longer set. [NG-12885]
- Fixed an issue where RADIUS auth requests did not include a useful NAS-IP-Address attribute. This restores the behavior that existed before 24.11.4. [NG-12877]
- Fixed an issue where usernames did not allow non-leading period characters. [NG-13013]
- Fixed original SNMP support for Gen 1 APC PDUs. [NG-13035]
- Renamed the Raritan PX2 SNMP driver to better indicate its ability to be used with newer devices. [NG-13094]

- Fixed an issue where SNMP message type could be set to INFORM for unsupported version v1. [NG-13095]
- Fixed re-enabling the cellular modem via physif wwan0 after a cellular firmware upgrade is performed. [NG-13142]
- Fixed an issue that caused salt-sproxy processes to not exit, consuming resources until the device reboots. [NG-12916]
- Fixed some instances of NTP not enabling/disabling correctly. [NG-13155]
- Changes to the systems timezone now correctly update the timezone for rsyslog times and cron event triggers. [NG-13150]
- Fixed an issue where rear USB port on CM8100-10G-USB was not usable in console mode when using hub and dual-port device. [NG-13130]
- Fixed an issue for CM8100-10G-C to handle a rare occurrence of cellular modem not getting initialized on boot. [NG-13214]
- Fixed an issue where nmea-streamer would terminate unexpectedly upon launch. [NG-13170]

25.10.0 (October 2025)

This is a production release

Enhancements

- Added support for CM8100-10G-USB devices. [NG-13028]
- Disable USB Mass Storage (Previous 25.07 Release). [NG-12482]
  - Added support for the ability to remove the Linux kernel support for usb_storage, preventing the use of USB mass-storage devices.
  - This can be done at runtime using the following command in the Linux CLI:

    ```
    rmmod usb_storage
    ```

  - This can be configured to be removed by default on boot by updating the Linux kernel module configuration as follows:

    ```
    echo "blacklist usb-storage" > /etc/modprobe.d/blacklist.conf
    ```

  - The support can be re-enabled at runtime using the following command in the Linux CLI:

    ```
    modprobe usb_storage
    ```

  - Zero Touch Provisioning via USB is still supported when USB mass-storage is disabled.

Security Fixes

- Patched SQLite to address security vulnerability CVE-2025-6965. [NG-13113]
- Patched Python setuptools to address security vulnerability CVE-2025-47273. [NG-13115]
- Updated iperf3 to version 3.19.1 to address security vulnerability CVE-2025-54351. [NG-13114]

Defect Fixes

- Fixed issue where physically ejecting a SIM sometimes did not trigger sim-to-sim failover. [NG-12709]

25.07.2 (September 2025)

This is a patch release

Defect Fixes

- Fixed issue where version string incorrectly reporting as 25.07.0. [NG-13084]

25.07.1 (September 2025)

This is a patch release

Defect Fixes

- Fixed issue where some migrations would not occur on upgrade. [NG-13016]

25.07.0 (August 2025)

This is a production release

Enhancements

- Kernel version upgraded to 6.6. [NG-10262]
- Display the default APN stored in the cellular modem when the user has not provided a new APN to overwrite this value. [NG-3831]
- The cellular LED now blinks orange when changing the active SIM, if the modem is disabled. [NG-11811]
- Added the ability for auto response to trigger in response to texts received from any phone number by supplying an empty list of phone numbers when creating an auto response beacon or playbook. [NG-12607]
- Lighthouse Service Portal (LSP) CM8100 Support. [NG-12583]
  - Lighthouse Service Portal now also supports CM8100 nodes to perform a zero touch call home and automatic enrollment into a customer's Lighthouse instance of choice.
  - Lighthouse Service Portal device port has been changed from 8883 to 443.
- Docker container emulation for the linux/amd64 platform is supported for the CM8100. [NG-12583]

Security Fixes

- Sudo package updated to 1.9.17p1 to address security issues for CVE-2025-32462 and CVE-2025-32463. [NG-12685]
- Upgraded OpenSSH to 10.0p2 to address security issues for CVE-2025-32728, CVE-2025-26465, CVE-2025-26466. [NG-12237]
  - This version also explicitly declares that CVE-2023-51767 does not affect OpenSSH.
- Upgraded OpenVPN to 2.6.14 to address security issues for CVE-2025-2704 and CVE-2024-5594. [NG-12807]
- Upgraded Docker to 25.0.6 to address security issue CVE-2024-41110. [NG-

12808]
- Upgraded JQ to fix CVE-2024-23337, CVE-2025-48060, CVE-2024-53427. [NG-12719]
- NG-12287 CyberCX Pen Test Fixes:
  - Password complexity is enabled by default with below criteria. [NG-12489]
    - Minimum password length - 8 characters
    - One capital letter
    - One number
    - Disable username in password
    - **NOTE** Customers with an updated password policy will have their settings migrated during the upgrade process. Due to a limitation, customers that have not made any changes to the defaults prior to the upgrade will get the new password policy defaults when upgrading.
- Upgraded OpenSSL to 3.0.16 to address security issue CVE-2024-4741. [NG-12869]

Defect Fixes

- Fixed an issue where the config tool would present different interfaces when creating or editing an aggregate (bridge or bond), compared to the web UI. [NG-2712]
- Ensured all CLI login Playbooks work correctly. [NG-3349]
- Fixed an issue where the Auto-Response Trigger count would max out at 25 triggers. [NG-3385]
- Fixed an issue where AAA config could not be restored to a new device. [NG-3420]
- IPSec UI: the IPSec tunnel page now requires Phase 1 algorithms to be specified when users set the Algorithm Proposal to Specific. In prior releases, when users set to Specific but didn't actually set any specific proposals, upon save it would fall back to Negotiable. [NG-3551]
- Fixed an issue where console server could not report failover as active if the cellular modem was not enabled. [NG-4880]
- Ensured all custom command reactions execute as part of a playbook. [NG-9361]
- Fixed DHCPv6 Option Code 16 - Vendor Class Option that was malformed prior to this change. [NG-10026]
- Edit buttons in the web UI are temporarily disabled while firewall changes are processing. [NG-10297]
- Fixed an issue where port logs were being written to the journal. Port logs are only written to /var/log/portxx.log. Port logs are sent to remote syslog servers if requested. [NG-10303]
- Fixed an issue where SNMP interface names (IF-MIB::ifName) and descriptions (IF-MIB::ifDescr) were not kept in sync if an interface's ifIndex changed. [NG-10472]
- Fixed an issue that caused support report generation to timeout. [NG-10515]
- Fixed an issue where /var/log/messages may not be rotated if the system reboots regularly. Fixed an issue where upgrades would fail when /mnt/nvram is full. [NG-11451]
- Fixed an issue where the hostname configurator would run unexpectedly. [NG-11452]
- Clock is updated correctly when timezone changes. [NG-11528]

- Fixed an issue with the display of multi-line strings in the config tool. [NG-11666]
- Fixed an issue with pasting multi-line strings into the config tool. [NG-11668]
- Fixed an issue where the SIM connection status would be erroneously reported as “None (Roaming via None)”. [NG-11798]
- Improved config shell help text for reading values through the `show` command. [NG-11851]
- Removed invalid PRF algorithms from integrity algorithms for IPsec. [NG-11898]
- Improved robustness of network management process. [NG-11907]
- Removed error related to configurator_cloud_connector on initial boot. [NG-12014]
- Fixed an issue where syslog referred to PSU0 and PSU1, instead of PSU1 and PSU2. [NG-12015]
- Avoid writing an APN to the incorrect profile when the cell modem is busy. [NG-12016]
- Fixed an issue causing snmpd to log “unexpected header length”. [NG-12075]
- Fixed an issue where the Logging Level control was too narrow for its contents. [NG-12076]
- Fixed an issue where SNMP would not report any power supply names. [NG-12094]
- Cellular username and passwords can now contain special characters reliably for authentication types such as PAP and CHAP. [NG-12108]
- Fixed missing translation for U.S Cellular firmware. [NG-12142]
- Fixed startup issues with the defaults config server. [NG-12166]
    - The server no longer re-initialises on every boot. It only re-initialises on upgrade.
    - This server is required, so if it fails, upgrades will no longer succeed. This should only be visible in rare cases where hardware has failed.
- The PDU name cache is now (re)built on boot. When adding new, custom PDU definitions, the new `refresh-pdu-name-cache` command can be used to update the PDU name cache without rebooting. [NG-12416]
- Fixed an issue where carrier names that are not ASCII would cause modemwatcher to crash. [NG-12419]
- Port Auto Discovery: fixed an issue in `port_discovery` that caused it to crash when a USB port was connected to a serial console during discovery. [NG-12562]
- Fixed an issue where the sysDescr SNMP field shows the old version after upgrading. Fixed an issue where the vendor class in DHCP requests uses the old version after upgrading. [NG-12574]
- Fixed USB ZTP for CM8100. [NG-12580]
- Fixed an issue where lighthouse could not connect to a node’s serial ports when using RADIUS or LDAP. [NG-12589]
- Fixed an issue affecting EM7565 modems on OM2200 devices by running the cellular USB port at high-speed, instead of super-speed. [NG-12718]
- Fixed an issue where static routes to ::/0 incorrectly failed to install. [NG-12737]

24.11.7 (July 2025)

This is a patch release

Defect Fixes

- Fixed issue where SNMP trap server would reject the request when contexts

EngineID did not match the authoritative EngineID on SNMPv3. [NG-12713]

24.11.6 (July 2025)

This is a patch release

Enhancements

- Updated ogcli diff to compare cleartext values of obfuscated secrets for a more accurate diff. Removed `--ignore-secrets-mismatch` flag because diff can now compare a cleartext value against the cleartext value of an obfuscated secret. [NG-12608]

Defect Fixes

- Fixed an issue where the modem was not initialised correctly after a firmware swap. [NG-9777]
- The snmpd engineID setting will be configured exactly as what was set from now on instead of it being auto generated by snmpd from the given setting. [NG-11882]

24.11.5 (June 2025)

This is a patch release

Enhancements

- Enables 5G for 8100 family when available. [NG-12273]

Defect Fixes

- Fixed an issue where admin group users could not run import and restore without inputting their password. [NG-12561]
- Fixed an issue where netgrp users GID changed after running import/restore. [NG-12566]
- Fixed an issue where config restore did not work if there were wireguard configs in the backup. [NG-12348]
- Fixed an issue where UI logins were reported as coming from ::ffff:<IP> for IPv4 clients, which caused problems with some AAA setups. [NG-12236]
- Cleaned up warnings in connectivty-test tool output. [NG-12083]
- Fixed an issue where configuring a static address for a vlan where the master is in a bridge causes issues. [NG-11887]

24.11.4 (May 2025)

This is a patch release

Enhancements

- Added the ability to specify an alternate base port for ssh access to ports. This works in addition to the default base port of 3000. Please note that connections to the alternate port number are always allowed, and cannot be blocked by firewall rules. [NG-11663]
- Added speedtest-cli to the image. Note for end users: speedtest-cli does not seem to have a way to force the use of a specific interface, the default outgoing

route will be used. Use `--source` to specify the IPv4 address of the cellular interface (wwan0). [NG-11942]
- Added support for disabling radius accounting. [NG-11958]

Security Fixes

- Added support for the Message-Authenticator header when using RADIUS. [NG-12035] By default, enforcement of this header is disabled so as not to break compatibility with older servers. Enable it to avoid CVE-2024-3596 (BlastRADIUS).
- Removed the “Server:” header from http responses. [NG-12198]
- Upgraded nginx to 1.26.3 to address minor CVEs. [NG-12205]
- Upgraded docker-moby to 25.0.5 for CVE-2024-29018. [NG-12220]
- Patched libxml2 for CVE-2025-27113. [NG-12221]
- Patched libxml2 for CVE-2025-32414. [NG-12221]
- Patched libxml2 for CVE-2025-32415. [NG-12221]

Defect Fixes

- Fixed an issue where users were not required to update their expired password when logging in with LDAP and RADIUS authentication. [NG-10226]
- Disabled support for ssh-dss (DSA) public key algorithm in OpenSSH. [NG-10712]
- Fixed an issue where beanstalkd binlog files are not deleted, which fills up /etc. [NG-11835]
- Fixed an issue where running cell-power off could lead to a bootloop. [NG-11843]
- Fixed an issue where -M devices had a non-functioning console port on first boot. [NG-11994]
- Fixed an issue where port control codes (part of a CLI-only feature) were cleared when editing the port via the web UI. [NG-11997]
- Fixed an issue where special characters could not be used for modem connection fields. [NG-12032]
- Fixed an issue where connecting a USB peripheral caused the modem to be unable to be probed successfully. [NG-12139]

24.11.3 (March 2025)

This is a patch release.

Enhancements

- Added the ability to explicitly set the carrier firmware running on the cellular modem, rather than relying on the firmware automatically being selected by the modem. [NG-9041]
- Locally connected, more specific subnets will be preferred over IPsec tunnel subnets. [NG-11429]
- Added support for additional privacy protocols for SNMP. [NG-11626]
- Added support for LDAP over SSL. [NG-11638]
- Allow port discovery to set undiscovered port labels to their default value rather than leaving them unchanged. Note that this is only implemented as an opt-in command-line (bash) flag. The API/UI cannot use this. Append the `--restore-default-labels` flag to the `port_discovery` command to use this option. [NG-11661]

- Allowed capital letters in local usernames. [NG-11777]
- Added tooling to enable non-standard modem configurations to support solutions for customer issues (including SIM detection, and modem module crashes). Please contact Opengear Technical support for assistance. [NG-11618]

Defect Fixes

- Fixed an issue where switch ports were incorrectly activated, before being de-activated. This caused external systems to see the port become active, even though it was disabled in config. [NG-11231]
- Fixed the ability to login to Cisco IOS devices to get the hostname. It is strongly recommended that existing users of port_discovery test this release carefully due to the changes that were made. [NG-11308]
- Fixed an issue with IPSec where multiple subnets could not be used with IKEv2. [NG-11430]
- Fixed an issue where the incorrect cellular profile was modified when using a Verizon SIM. [NG-11559]
- Resolved an issue where the modem would generate excessive log entries when low signal quality was detected. [NG-11598]
- Fixed an issue where some scripts were logging directly to /var/log/messages, bypassing the journal. [NG-11635]
- Fixed an issue where connectivity test would fail to bring the modem interface down. [NG-11636]
- Added the ability to specify the authentication protocol to be used when creating a cellular connection. [NG-11679]

24.11.2 (December 2024)

This is a patch release.

Enhancements

- Added support for MS-CHAPv2 authentication to the RADIUS server. [NG-11418]
- Add a configurable timeout for remote authentication. [NG-11433]
- Added support for additional authentication protocols for SNMP. [NG-11443]

Defect Fixes

- Fixes an issue where some cellular Carrier Networks were being misidentified. [NG-11612]
- Fixes an issue where rollback did not occur if the import was interrupted while configurators were running. [NG-11650]

24.11.1 (December 2024)

This is a patch release.

Defect Fixes

- Add auto-focus to login username in Web UI. [NG-11114]
- Add tab complete for ogcli diff command. [NG-11370]
- Prevent stack trace when ogconfig server is down during import/restore. [NG-11448]
- Fix ogcli import incorrectly updating “enabled” in groups. [NG-11453]
- Don’t use shadow file to populate default db. [NG-11524]
- Complete current command before rollback during import/restore. [NG-11526]
- Handle minor formatting changes of ogcli commands. [NG-11527]
- Fix error adding playbook after changing trigger type. [NG-11532]
- Remove the –check-before-replace argument from the export file. [NG-11533]
- Explain diff from defaults in help text. [NG-11534]
- Fix ogcli import/restore help exceeds column width. [NG-11538]
- Web UI REST API polling resume after config server disconnect during import/restore. [NG-11539]
- Stop ogcli crashing when closing ssh session with bad config during import/restore. [NG-11542]
- Make the Web UI upgrade/reboot polling stop after timeout. [NG-11543]
- This fixes an issue with the nmea-streamer tool which is currently not outputting NMEA data. [NG-11544]
- Report when SIM failback has completed. [NG-11550]
- Stop system upgrade banner popping up after failure. [NG-11557]
- Don’t probe PDU outlets if provided during import/restore. [NG-11558]
- Fixed an issue where ssh links did not show up with Lighthouse 24.06 and later. [NG-11564]
- ogcli help operations exceeds column length. [NG-11577]
- Add rollback messages on restore page. [NG-11581]
- Make ogcli import/restore run in root. [NG-11593]
- Fix added character on login page. [NG-11602]
- Remove duplicated field groupNames from user export. [NG-11609]
- Improve secrets handling code during import/restore. [NG-11613]
- Improve handling of badly formatted heredoc during import/restore. [NG-11625]
- Ignore white-space for import variable declarations and in heredoc during import/restore. [NG-11634]
- Fix configurators not running at end of ogcli import. [NG-11647]

24.11.0 (November 2024)

This is a production release.

Enhancements

- **Configuration Diff** • The ogcli and config applications now support an upgraded diff mode that is order-aware and can report configuration options that have changed from defaults.

- **Configuration Rollback** • If a problem occurs when restoring configuration, then the system will automatically rollback the configuration to the state the device was in before the restore started. This ensures restore commands do not leave the console server in an invalid state.

Security Fixes

- Upgraded Docker to 25.0.3 for CVE-2024-24557. [NG-10173]
- Instead of SHA1, make SHA256 the default signature algorithm when generating CSRs via the web UI. [NG-10951]
- Patched curl for CVE-2024-7264
- Patched python3-certifi for CVE-2024-39689

Defect Fixes

- Fixed an issue where adding the current interface to a bridge or bond would result in poor user experience. [NG-2569]
- Fixed an issue where the “last triggered” display on playbook configuration page was comparing the triggered date in the wrong timezone. [NG-3327]
- Fixed an issue where incorrect link speeds were shown. [NG-3536]
- conman: ensure that vlans wait for ethernet to be connected before downstream devices can use the interface. [NG-3762]
- Fixed an issue where devices that appear as a UART behind a USB hub did not work. Note that this does not remove the restriction of a single UART for each USB port. Where multiple UARTS are visible, the hide-usb-port script must be used. This also fixes an issue where dual-UART USB devices did not work in every USB port for every device. [NG-8610]
- Fixed an issue where typing into a pmshell session for a disconnected USB port would cause that session to become stuck and fail to clean up properly. [NG-9357]
- Fixed an issue where resolve actions would not trigger after a trigger action had fired. Also fixed a strange UI bug where auto response actions would be flipped on edit. [NG-9834]
- Port logs are now stored in /var/log rather than in /run. Port logs are no longer lost when rebooting. Port logs are rotated when over 64k with 1 old log kept (rotation happens when logrotate runs - approx once per hour). It is no longer possible for port logs to blow up and prevent access to a device (e.g. poorly configured device sending a massive stream of data that is being logged). [NG-10259]
- Fixed an issue with IP Passthrough where the downstream interface going down and up would break communications. Fixed an issue with IP Passthrough where a loss of the downstream client was not noticed by the system. [NG-10386]

- Fixed an issue that prevented the token being handled correctly when accessing via Lighthouse UI proxy. This fix allows 2 devices to be opened via 2 tabs at the same time. [NG-10716]
- Fixed an issue where replacing all firewall zones and using an interface in multiple zones would result in invalid configuration. [NG-10506]
- Fixed an issue where omitting the optional description when updating an interface would clear the stored description. [NG-10671]
- Fixed various issues related to auto-response by aligning the API to the web UI. Because of this change, the previous APIs (auto_response/beacons and auto_response/actions) have been deprecated, with the new auto_response/playbooks API replacing them. [NG-10682]
- Fixed Cyclades PM10 PDU device specification not found. [NG-10724]
- Fixed per-interface start-up issue that would sometimes result in the console server becoming inaccessible on some interfaces. [NG-10729]
- Fixed an issue that can prevent web terminal and support report download from nodes accessed via Lighthouse UI proxy. [NG-10746]
- We no longer volatile mount /var/lib onto /etc/lib since most application state files don't need to be preserved across reboots. logrotate: the state file is now stored in /etc/lib/logrotate.status instead of /var/lib/logrotate.status. This allows state data for logrotate to be persisted across reboots. Upgrading from 23.10 or earlier will reset the engine boots counter. [NG-10755]
- Fixed issue where upgrading firmware from 23.10.4 (or earlier) with cellular logging enabled broke cellular modem functionality. [NG-10756]
- Fixed an issue where a bad Authorization header would be ignored if a valid cookie was present. Now, the cookie can only be used if the header is absent. [NG-10870]
- Fixed an issue where loopback interfaces were omitted from configuration exports. [NG-10933]
- Fixed an issue where deleting a firewall zone or service could result in an orphaned firewall policy. [NG-10964]
- Added the capability for a user to specify a put list for the auto_response/playbooks endpoint. [NG-11048]
- Fixed an issue where configuration erroneously advertised 'get' as a sub-command. [NG-11123]
- Fixed missing MCC/MNC 454/35 in cell modem carriers table. [NG-11134]
- Fixed issue sending SMS when signal strength is low. [NG-11155]
- Fixed an issue where ssh-rsa2 algorithms were removed unnecessarily. The 24.07.0 release removes ssh-rsa2 algorithms which are not listed as supported. However, these algorithms still work and may be needed to access older hosts. If these algorithms are needed, they can be manually re-added. Skipping over the 24.07.0 release, or clean installing 24.07.1 or later will avoid removing the ssh-rsa2 algorithms. [NG-11179]
- Fixed an issue where SMSes could not be sent or received on Verizon's network if autoconnect was enabled. [NG-11187]
- Fixed an issue where some Cisco devices were not detected using port discovery. [NG-11239]

24.07.1 (October 2024)

This is a patch release.

Security Fixes

- Patched expat 2.5.0 for CVE-2024-45490, CVE-2024-45491, and CVE-2024-45492. [NG-11228]
- Patched python3 for CVE-2024-7592. [NG-11140]
- Patched wget for 1.24.5 for CVE-2024-38428. [NG-11052]

Defect Fixes

- Fixed an issue where ssh-rsa2 algorithms were removed unnecessarily in the 24.07.0 release. If these algorithms are needed, they can be manually re-added. [NG-11179]
    - Skipping over the 24.07.0 release, or clean installing 24.07.1 or later will avoid removing the ssh-rsa2 algorithms.
- Fixed an issue where the modem would crash with failure_reason=“unknown capabilities” when using SMS. This fix prevents ModemManager from crashing, which allows the modem to function properly. [NG-11155]
- Fixed an issue with IP Passthrough where a loss of the downstream client was not noticed by the system. [NG-10386]
- Fixed an issue where SHA1 instead of SHA256 was selected as the default signature algorithm when generating CSRs. [NG-10951]
- Fixed an issue that prevented the token being handled correctly when accessing devices via the LH UI proxy. This fix allows two devices to be opened via two tabs at the same time. [NG-10716]
- Fixed an issue that prevented web terminal and support report download from nodes accessed via the LH UI proxy. [NG-10746]
- Fixed an issue where loopback interfaces were omitted from config exports. [NG-10933]
- Fixed an issue where some Cisco devices were not detected using port discovery. [NG-11239]
- Fixed an issue where ‘Webbing’ network was missing from the SIM MCC/MNC table. [NG-11134]
- Fixed a possible issue where SMF scenarios under a low MTU network could prevent SMF discovery. [NG-11307]

24.07.0 (July 2024)

This is a production release.

Features

- **Lighthouse Service Portal (LSP)** • This is an Opengear solution that enables nodes to perform a zero touch call home and automatic enrollment into a customer’s Lighthouse instance of choice.
- **Raw TCP Support** • This feature enables relay of TCP messages to corresponding serial ports and includes pre-defined firewall services for secure connections. Users can now create raw TCP sockets on specific ports and connect to them using tools like nc or telnet.
- **OM1300 and CM8000 Support** • This is the first release supporting the OM1300 Operations Manager and the CM8000 Console Manager.

Enhancements

- Front end WebUI framework EmberJS has been upgraded to version 4.12. [NG-5251]
- Login time is now reduced when unresponsive LDAP servers are being used. [NG-3159]
- Removed an unused file. [NG-8837]
- No longer log irrelevant DHCPv6 client events when IPv6 is not being used. [NG-8920]
- Allowed users to enable a previously disabled serial port from the `/access/serialports` page. [NG-9355]
- libogobject: Increased the buffer size for interface name to accommodate longer interface alias names such as vlans above 999. [NG-9393]
- Added success and error toasts to IPsec page. [NG-9454]
- Allow DNS settings to carry over when an aggregate is created or deleted. [NG-9489]
- Allow removing the last RADIUS accounting server by clearing the hostname. [NG-9506]
- Removed unused code. [NG-9573]
- Removed constant log messages when using a device without a SIM card. [NG-9625]
- Removed trivial fan alarm SNMP alerts for operation manager SKUs as fans are not present. [NG-9701]
- Remove numbers from the syslog server page so that the severity label and tooltip are not confusing. [NG-9774]
- Not user visible. [NG-9787]
- Improved ModemManager status gathering for the Support Report. [NG-10509]

Security Fixes

- **NOTE:** This release includes security changes that impact a case where a Lighthouse VPN server certificate can be SHA-1 signed and will prevent the Console Server device enrolling into Lighthouse.
  - Please refer to Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- PDUs configured using the SNMPv3 authPriv security level will now work as intended. [NG-9587]
- Fixed an issue preventing the use of passwords with BGP. [NG-9761] *Note that BGP passwords may not be FIPS-compliant, as they use MD5.*
- Custom usernames and passwords will now be respected for powerman-type PDUs. [NG-9872]
- Fixes CVE-2015-9542. [NG-9943]
- Libraries upgraded to mitigate the following CVEs: CVE-2023-41056, CVE-2023-45145, CVE-2023-25809, CVE-2023-27561, CVE-2023-28642, CVE-2024-21626, CVE-2023-44487, CVE-2023-50387. [NG-9944]
- Added validation to IPSec Addressing Fields. [NG-10192]
- Fixed an issue where root cannot SSH to the device with an authorized key when the password is expired and AAA is configured. [NG-10417]
- Fixed CVE-2024-6387 by upgrading OpenSSH to 9.8p1. [NG-10578]
  Note that this automatically removes support for a number of old, insecure host key algorithms:
  - sk-ecdsa-sha2-nistp256-cert-v01@openssh.com
  - sk-ssh-ed25519-cert-v01@openssh.com
  - rsa-sha2-512-cert-v01@openssh.com
  - rsa-sha2-256-cert-v01@openssh.com
  - sk-ecdsa-sha2-nistp256@openssh.com
  - sk-ssh-ed25519@openssh.com
  - rsa-sha2-512
  - rsa-sha2-256

Defect Fixes

- External endpoints are not supported by our USB ZTP function, and all references to them have been removed. [NG-8244]
- Fixed an issue where the static route 0.0.0.0/0 appeared to fail even though it succeeded. [NG-8449]
- Fixed an issue where IP addresses may not be removed when bringing down the cellular interface. [NG-8614]
- Fixed an issue that caused root logins to trigger AAA accounting. [NG-8829]
- Fixes an issue that could lead to running an old web UI after upgrading a device. [NG-8893]
- No visible change, just some details behind the REST API. [NG-8944]
- Fixed an issue where the refresh button (on several pages) would not remove items as expected. [NG-9114]
- Fixed an issue where countries were not displaying correctly on the HTTPS page. [NG-9213]
- Fixed an issue that caused ports to display out of order when editing groups. [NG-9336]
- Fixed an issue that prevented OG-OMTELEM-MIB::ogOmSerialUserStartTime from being reported correctly on CM8100. [NG-9337]
- Tooltips vertically aligned with their arrows and more padding on the right. [NG-9344]
- Fixed an issue with adding local console serial ports to a group. [NG-9354]
- Fixed an issue with character requirements in the RAML. [NG-9356]
- Fixed an error in the logs by removing a bad file (renew_self_signed_certs.cron) and fixed a problem where a new install would generate one HTTPS certificate, only to replace it later from a migration script. [NG-9363]
- Fixed an issue with the localConsole Computed options. [NG-9371]
- Fixed an issue with Config shell tab complete options. [NG-9379]
- Fixed an ogcli parser edge case that failed to show the expected error message. [NG-9381]
- Fixed an issue that prevented OG-OMTELEM-MIB::ogOmSerialUserStartTime from being populated. [NG-9384]
- Fixed an issue where a device cannot be turned off from the serial ports page. [NG-9409]
- Fixed an issue with the IPsec-tunnels page when deleting tab content. [NG-9453]
- Fixed a problem that stopped error messages from displaying on firewall services pages. [NG-9583]
- Fixed an issue that prevented serial port sessions from being removed from SNMP reports. [NG-9624]
- Ensured keystroke triggered form submission functions as intended. [NG-9752]
- Fixed an issue with the firewall management page’s confirmation modal. [NG-9790]
- Ensured that modem-watcher stores RSSI values as integers and not floats. This allows ogtelem to report SNMP OG-OMTELEM-MIB::ogOmCellUimRssi without parsing errors. [NG-9886]
- Fixed an issue that prevented IPSec-encapsulated subnet traffic from leaving via the modem. [NG-9908]
- Powerman drivers differ from what ogpower expects. [NG-9909]
- Fixed issue with subnet mask on modem connection being set or calculated

incorrectly in some edge cases. [NG-10029]
- Fixed support report generation to avoid writing the journal to `/tmp` (which could fail due to insufficient space). [NG-10164]
- Fix issue with static route errors being shown repeatedly in the web UI. [NG-10193]
- Fixed an issue with the tooltip for banned IP. [NG-10236]
- Fixed an issue with the GET ports/ports_status endpoint that when the user didn’t have port permissions, it would return an empty object causing the UI to error out since it was expecting an array. Updated the endpoint to always return an array. [NG-10270]
- Fixed an issue where the cellular MTU was set to ‘None’. [NG-10399]

24.03.0 (March 2024)

This is a production release.

Features

- **Cellular Modem Firmware Upgrade** • A new command line tool (cell-fw-update) has been added to allow users to upgrade the carrier firmware for their devices cellular modems.
- **Loopback Interface Support** • Users can now create virtual loopback interfaces. These interfaces support ipv4 and ipv6 addresses. Loopbacks cannot be configured through the Web UI.
- **Firewall Egress Traffic Filtering Support** • Device firewalls can now be configured to have egress filtering rules. These rules allow users to create firewall policies to permit or deny traffic leaving the device.
- **Quagga to FRR Upgrade** • The Quagga software suite, which provides implementations of dynamic routing protocols (OSPF, IS-IS, BGP, etc) has been replaced with FRR (Free Range Routing) version 8.2.2
  - **Migration Notes** • Depending on circumstance users might have to perform some manual migrations.

Routing Protocol Used	FRR Upgrade Changes
No routing protocols	Not affected
Configured OSPF through a supported interface. E.g. Config CLI, REST API or Web UI	Not affected
Manually configured routing protocols (Any protocol that was manually configured including OSPF)	Perform a manual migration.

In most cases users can simply copy the relevant configuration file (ospf.conf, bgp.conf, etc) from /etc/quagga to /etc/frr and enable that routing protocol in the /etc/frr/daemons file. Consult the Free Range Routing documentation if required.

Enhancements

- Improve display of network interfaces to remove ambiguity by always including the device and the description. For example network interfaces in the Web UI will be displayed as “<device> - <description>”. [NG-7244]

Security Fixes

- Ipsec PSK’s are no longer written to tunnel config files in plain text. [NG-3542]
- Password complexity rules for short usernames being contained in passwords are now clearer. [NG-7874]
- Fixed CVE-2023-48795 OpenSSh allows remote attackers to bypass integrity checks (Terrapin)

Defect Fixes

- Fixed an issue where the web terminal would prevent session timeout when accessing a node via LH UI proxy. [NG-2867]
- Fixed an issue where static routes attached to an interface would get stuck down after removing a network connection from a network interface. [NG-3750]
- Removed race condition between ogtelem_redis.service and ogtelem-snmp-agent.service. [NG-3864]
- Fixed an issue that could cause network connections to get stuck in the “Reloading” state. [NG-4346]
- ztp: wait for migrations to finish before running ztp provided scripts in order to prevent conflicts with migration scripts. [NG-6170]
- User without web-ui rights will not create session files. [NG-6282]
- port_discovery script is now more resilient to errors when port settings change from another source. [NG-6330]
- Make Rsyslog listen on ipv6 localhost which fixes Secure Provisioning NetOps module, which runs rsyslogd inside of the remote-dop container. [NG-6667]
- Restored functionality of physical Switch on 24E devices. [NG-7455]
- Fixed an issue that prevented certain endpoints from working with ogcli. [NG-7482]
- Prevent the ogtelem-snmp-agent from crashing when bad data is published on redis. [NG-7521]
- puginstall: when this script is killed, ensure that the current slot is marked as good and bootable. [NG-7564]
- Fixed an issue where infod2redis would consume lots of CPU when switch ports were enabled but not connected. [NG-7567]
- Fixed an issue that allowed traffic to leave the modem with the incorrect source IP. [NG-7650]
- Fix ogcli merge crash and spam of the log. [NG-7657]
- Fixed a case that caused the cellular modem to sometimes fail to detect the SIM. [NG-7848]
- Fixed an issue causing file descriptor leaks in the REST API (potentially leading to an inability to login). [NG-7888]
- The Wireguard listening port is not correctly configured by the POST. [NG-7886] request for the default case. A subsequent PUT request is needed to set the port.
- Fixed a visual bug that caused bonds to not appear as an option when creating bridges. [NG-8109]
- Fix of configurator_local_network crash at first boot after upgrade. [NG-8014]
- DM stream now correctly closes after dm-logger closes. [NG-8134]
- Fixed an issue where new DHCP conns did not use the correct vendor_class(until reboot). [NG-8164]
- Fixed an issue where config could not load the monitor/lldp/neighbor endpoint when more than 1 neighbor is present. [NG-8201]

- Fixed an issue where ogcli get monitor/lldp/neighbor foo would return the last neighbor instead of an error. [NG-8201]
- Fixed a bug that caused dm-logger to stop logging even though it was still running. [NG-8240]
- Made /var/lib be mounted onto /etc/lib to ensure application data is persisted when the device reboots. [NG-8271]
- Fixed an issue where the LLDP page and endpoint allowed selecting invalid interfaces. Only physical interfaces make sense to be selectable. When no interfaces are selected, lldpd will use all physical interfaces. [NG-8276]
    - Note that when upgrading, invalid interfaces are simply removed. That will either leave some valid interfaces selected, or no interfaces. Customers should check their LLDP config after upgrading to be sure it matches what they are expecting.
- Fixed an issue where the POTS modem wasn't using flow control, which resulted in dropped characters when flooding the connection with data. [NG-8304]
- Fixed an issue where upgrading from 20.Q3 (or earlier) to 23.03 (or later) would break the SNMP Alert Managers configuration. [NG-8757]
- Scripts endpoint now exports the PATH prior to running the provided script. [NG-8802]
- Performing a PUT on /pots_modems endpoint will preserve the previous modem id instead of discarding it. [NG-8803]
- Fixed a Config CLI issue where deleting a list item wouldn't cause it to immediately disappear in some cases. [NG-8947]
- Fixed prompt not updating in some cases when items are renamed. [NG-8979]
- Fixed styling on certain Web UI buttons. A few instances of the last segmented button would show with square corners rather than the expected rounded corners. [NG-9029]
- Fix tooltip placement for remote auth policy buttons in the Web UI. [NG-9031]
- Fixed a regression in the tooltips styling Web UI. [NG-9035]
- Fix config shell crash caused by renaming a new item in a previously empty simple array. [NG-9040]
- Fixed a config cli crash caused by renaming a new item in a previously empty simple array. [NG-9055]
- Fixed PDU driver for Raritan PX2/PX3/PXC/PXO (these all use the same driver), including corrected baud rate of 115200 (the default for all of these models). [NG-9157]
- Various fixes when discarding items in Config CLI. [NG-8978]. [NG-8977]
- NG-5371 NG-7863 NG-8280 NG-8626 NG-8910 NG-9142 NG-9156 Improved various error messages. [NG-5369]

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

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

Security Fixes

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

Defect Fixes

- Fixed an issue where pinout did not work as expected for local consoles on OM2200. [NG-3113]
- 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-3246]
- Fixed an issue where creating and deleting a bridge left old entries in the perifrouted firewall table. [NG-3651]
- Better handling of duplicate IP addresses in config. [NG-3678]
- Fixed an issue where management port settings other than baud were ignored. [NG-4080]
- Fixed issue with DHCP leases repeatedly triggering lighthouse config resyncs. [NG-4289]
- 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-4355]
- Fixed an issue where the Remote Authentication page would reject changes with a cryptic error (when the optional accounting server was blank). [NG-4779]
- Fixed an issue where invalid baud rates were offered for management ports. [NG-5344]
- Added a check to the groups endpoints to prevent them from overwriting system groups. [NG-5421]
- Fixed an issue where invalid baud rates were offered for serial ports. [NG-5499]

- Fail-over banner behavior fixed when failover is disabled. [NG-5648]
- RAML documentation fix *(execution_id for script template)*. [NG-5968]
- Fixed an issue where misleading static defaults were being used for LLDP. Now LLDP's own defaults are used. [NG-6001]
- Fixed an issue where an IPSec tunnel set to initiate did not attempt to re-connect after the peer closes the link. [NG-6062]
- Raritan PX2 PDU driver update to work with newest Raritan firmware. [NG-6079]
- Allow adding USB ports to port autodiscovery. [NG-6087]
- 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-6147]
- Fixed an issue where port_discovery –no-apply-config could not discover ports. [NG-6192]
- Switch traceroute from busybox to the standalone verison. [NG-6223]
- Fixed an issue where stopping salt-master would cause a stack trace in the log. [NG-6249]
- Fixed issue where ogcli restore command could remove cellular config. [NG-6300]
- Disabled redis dababase snapshotting. [NG-6301]
- Fixed an issue where port logging options were presented for local consoles. [NG-6305]
- Fixed an issue where DHCP option 43 (ZTP) decoding could fail and prevent the interface from being displayed as up. [NG-6370]
- Fixed an issue where invalid serial settings (data bits, parity, stop bits) were offered on serial ports and management ports. [NG-6373]
- Loopback tool waits for port manager to exit before starting. [NG-6423]
- Fixed an issue that allowed VLAN's to be created on the wrong interface. [NG-6444]
- SSH access to the device allowed even if /run partition is full. [NG-6806]
- Fixed an issue where unnecessary data was included in config exports. [NG-6814]
- 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-6827]
- NG-6914 NG-6928 NG-6933 NG-6958 NG-6096 NG-6103 NG-6105 NG-6108 NG-6127 NG-6153 Fixed many small Config CLI parsing and data consistency problems. [NG-6865]. [NG-6910]
- Loading pmshell history with ~h option fixed. [NG-6953]
- Fix for ssh access rejection when /run partition full. [NG-7010]
- Fixed issue with SNMP Service page not loading sometimes. [NG-7087]
- Fix rich rules missing service problem. [NG-7326]
- Fix routes metrics when fail-over is complete. [NG-7327]
- Fixed bridging issue on 24E switch models. [NG-7455]. [NG-7530]
- Default configuration for OSPF daemon fixed to avoid crash. [NG-7491]
- Fixed an issue where CM8100 devices could not connect to Cisco USB consoles. [NG-7528]
- Fixed an issue causing high CPU at boot by disabling an unnecessary component in rngd. [NG-7534]
- Fix Editing Bonds/Bridges to show user errors on web UI. [NG-7585]

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.