RELEASE NOTES

VERSION 5.3.3

INTRODUCTION

Please check Upgrading firmware using the web UI for instructions on how to upgrade your device. Latest appliance software is available on the Opengear Support Software download portal.

While every effort is made to migrate your existing configuration when upgrading, we recommend that you follow the instructions on How to backup and restore the configuration BEFORE performing the upgrade.

SUPPORTED PRODUCTS

- IM7200
- CM7100
- CM7196
- ACM700x
- ACM7004-5

KNOWN ISSUES

- No known issues

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 or defect fixes for high priority issues.

5.3.3 (May 2026)

This is a patch release

NOTE

- FIPS Mode
  - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
  - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
  - Backup your configuration before attempting an upgrade to 5.x
  - After a successful upgrade, make sure to capture a new backup
  - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- 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 https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Added support for configuring MTU on the L2 switch interface, with the value automatically applied to all member switch ports. [OG-11571]

Fixes

- Use modern ip command to setup aggregation interfaces. [OG-11581]
- Fixed 'Trusted Network' configuration changes on a cascade primary not syncing to cascade secondaries. [OG-11630]

Security Fixes

- Upgraded BIND to 9.16.48 for CVE-2023-50868. [OG-11674]
- Upgraded GLib for CVE-2025-6052, CVE-2025-13601, and CVE-2025-14087. [OG-11677]
- Upgraded Kerberos for CVE-2019-14844, CVE-2020-28196, CVE-2021-36222, CVE-2022-

42898, CVE-2024-37370, and CVE-2024-37371. [OG-11678]
- Upgraded libpng to 1.6.58 for CVEs. [OG-11679]
- Upgraded OpenSSL to 3.1.8 for CVE-2026-31790. [OG-11684]
- Upgraded OpenSSH to 10.3p1 for CVE-2026-35385 and CVE-2026-35414. [OG-11668]
- Upgraded OpenVPN to 2.6.26 for CVE-2025-13086. [OG-11685]
- Patched Lua for CVE-2014-5461. [OG-11680]
- Patched musl for CVE-2025-26519 and CVE-2026-40200. [OG-11681]
- Patched Net-SNMP for CVE-2025-68615. [OG-11682]

5.3.2 (Mar 2026)

This is a patch release

NOTE

- FIPS Mode
  - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
  - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
  - Backup your configuration before attempting an upgrade to 5.x
  - After a successful upgrade, make sure to capture a new backup
  - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- 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 https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Improved pmshell escape handling during nested sessions. [OG-8830]
- Added /failover endpoint to support Lighthouse failover reporting. [OG-11585]
- Changed REST API session endpoints (GET/DELETE/PUT /sessions/{sid}) to return HTTP 404 for non-existent or invalid session IDs instead of HTTP 200 with “challenge-in-progress”. [OG-11595]
- Added a comprehensive list for missing carriers in India. This fixes excessive logging generated when the carrier used is not listed. [OG-11611]

Fixes

- Fixed SNMP EngineID to match exactly what is set by the user. [OG-11313]
- Fixed dd and busybox commands failing on CM7100 and CM8100 platforms with the OGCS

5.x musl toolchain. [OG-11458]
- Fixed cellular firmware upgrade failures for modems that do not support storing multiple firmware images (MC7304). [OG-11518]
- Fixed an issue where harmless ntp server artifacts were left in config after a modification. [OG-11542]
- Fixed a race condition in odhcp6c that could process an IPv6 Router Advertisement on the wrong interface when multiple instances start simultaneously. [OG-11555]
- Fixed a memory leak in portmanager. [OG-11579]
- Fixed config for custom and overridden serial RPC device files. [OG-11591]
- Fixed kernel earlyprintk messages from appearing at the login prompt after device reboot. [OG-11593]
- Fixed cell health test not running when the device is configured for OOB failover mode. [OG-11596]
- Fixed an issue where ModemManager would leak memory continuously until out of memory. [OG-11600]
- Fixed the '-b' option in the 'top' command to work as expected. [OG-11617]

Security Fixes

- Updated OpenVPN to have LZO Compression disabled by default for new tunnels. Mitigates the Voracle attack vector. [OG-9339]

5.3.1 (Dec 2025)

This is a patch release

NOTE

- FIPS Mode
  - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
  - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
  - Backup your configuration before attempting an upgrade to 5.x
  - After a successful upgrade, make sure to capture a new backup
  - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- 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 https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Added HTTPS as default when accessing the cellfw repository: `https://ftp.opengear.com/download/cellfw/`. [OG-11502]
- Added MTU setting to IPSec tunnel configuration. [OG-11522]
- Improved portscraper to reduce writes to storage. [OG-11489]

Fixes

- Fixed an issue where adding a network host would result in extra config being left behind. [OG-11455]
- Fixed v1.9 typo in v2 REST API RAML. [OG-11534]
- Fixed DNS relay with dnsmasq installed to `/bin`. [OG-11536]
- Fixed the RSA keys' type used by webui validator to ensure they can be uploaded. [OG-11545]
- Fixed issue blocking cellular firmware updates through the REST API. [OG-11543]

Security Fixes

- Upgraded OpenSSH to 10.2p1 to fix CVE-2025-61984. [OG-11492]

5.3.0 (Nov 2025)

This is a production release

NOTE

- FIPS Mode
  - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
  - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
  - Backup your configuration before attempting an upgrade to 5.x
  - After a successful upgrade, make sure to capture a new backup
  - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- 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 https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Features

- Added cell firmware update REST API for lighthouse [OG-11355]

Enhancements

- Added a DNS Server WebUI input field to lookup the Cellmodem's DDNS Hostname when it is unable to be resolved by the system DNS servers. [OG-11435]
- Added an input field to specify the Lighthouse Callhome MTU, which will be applied for the lhvpn1 interface of the primary enrollment. [OG-11468]
    - Note, if the primary Lighthouse server triggers a secondary enrollment to another Lighthouse server, the MTU on the lhvpn2 interface will be the default 1500.
    - The MTU of any existing enrolments can be adjusted with the following command, where "X" is 1 for the primary enrolment and 2 for the secondary one and "1200" is new MTU:
      `config -s config.lhvpn.tunnels.tunnelX.mtu=1200 -r lhvpn_tunnel`
- Improved wording around the option to save password across config erases. [OG-11446]
- Improved the handling of the Authentication REST API, allowing multiple authentication methods to have config applied in a single POST. [OG-9279]

Fixes

- Fixed Cherokee not cleaning up /var/tmp folders. [OG-11488]
- Fixed cellular modems sending and receiving SMS over the Verizon network (MC73xx). [OG-11408]
    - Users must specify `Capabilities = lte` and `Allowed Modes = 00` under:
      `Dial` -> `Internal Cellular Modem` -> `Cellmodem Capabilities and SELRAT - Advanced`
      Then re-enable the cellular modem or reboot the device.
- Fixed cellular modems dropping from the Verizon network and generating periodic ping requests over the data connection (MC73xx). [OG-11408]
    - Users can change the default settings in:
      `Dial` -> `Internal Cellular Modem` -> `Cellmodem Keepalive - Advanced`
- Fixed some incorrect hard-coded REST API versions in URLs returned by endpoints. [OG-11258]
- Fixed missing SID (session ID) field from /sessions REST API endpoint. [OG-11258]
- Fixed an issue where RADIUS requests did not include a useful NAS-IP-Address attribute. Restores the behaviour that existed before 5.2.2. [OG-11447]
- Fixed handling of unpartitioned internal USB drives on IM72xx and CM71xx devices to automatically partition, format and mount. [OG-11437]

Security Fixes

- Fixed CVEs: [OG-11495]
    - Patched OpenSSL to mitigate CVE-2024-6119.
    - Patched Busybox to mitigate CVE-2022-48174.
    - Upgraded net-snmp to 5.9.2 to mitigate CVE-2022-24805, CVE-2022-24810.
    - Upgraded OpenVPN to 2.6.14 to mitigate CVE-2024-4877, CVE-2024-5594, CVE-2025-2704.
    - Patched gLib to mitigate CVE-2024-52533.

5.2.4 (Jul 2025)

This is a patch release

NOTE

- FIPS Mode
    - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.

    - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
    - Backup your configuration before attempting an upgrade to 5.x
    - After a successful upgrade, make sure to capture a new backup
    - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- 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 https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Improved efficiency when removing `-up-restarted` conns. [OG-11417]

Fixes

- Fixed IPsec tunnel over cellular modems. [OG-11415]
- Fixed web terminal when all egress IPv6 traffic is blocked on any interface. [OG-11424]
- Fixed Fail2Ban while using AAA authentication method. [OG-11426]
- Fixed OpenSSL migrations to ensure its configuration files are correct after 4.x to 5.x upgrade. [OG-11429]

Security Fixes

- Upgrade sudo package to address CVE-2025-32462 and CVE-2025-32463. [OG-11428]

5.2.3 (Jun 2025)

This is a patch release

NOTE

- FIPS Mode
    - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
    - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
    - Backup your configuration before attempting an upgrade to 5.x
    - After a successful upgrade, make sure to capture a new backup
    - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- 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 https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Fixed the ability to correct Verizon APN settings during data connection for cellular modems. [OG-11343]
- Fixed cell-fw-update to recover from the low-power mode should it fail during cellmodem firmware update. [OG-11344]
    - Added a button on the dialin page to remove selected carriers.
- Fixed an issue where HTML special characters could not be used in CSR fields (Organization, Organization Unit). [OG-11346]
- Fixed cellmodem connection issues with the wwan1 interface and the cdc-wdm1 control device (MC74xx). [OG-11361]
- Fixed openvpn server not binding to a given address or DNS hostname. [OG-11376]
- Fixed Fail2Ban regex to capture ssh login failures from the syslog. [OG-11389]
- Fixed minor IPSec duplicate configuration issue. [OG-11390]
- Fixed full-tunnel ipsec default route metric. [OG-11377]
    - A new Right Metric option has been added to the IPsec configuration page for modifying the metric used for routes to the peer or peer subnet if specified. Defaults to 100.

Security Fixes

- Upgrade OpenSSH to version 10.0p1 to mitigate CVEs. [OG-11394]

5.2.2 (May 2025)

This is a patch release

NOTE

- FIPS Mode
    - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
    - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
    - Backup your configuration before attempting an upgrade to 5.x
    - After a successful upgrade, make sure to capture a new backup
    - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- 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 https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Added logging of failed conman start and stop commands. [OG-11319]

Fixes

- Fixed cellmodem responding to external ICMP requests after disconnection (EM7565 and MC74xx). [OG-11333]
- Fixed issue with IPSec host-to-host or subnet-to-host configurations. [OG-11296]
- Fixed VPN routes not being added when configured on the WebUI (with Interface == None). [OG-11367]
- Fixed missing dos2unix package (CM71xx and CM7196a). [OG-11370]
- Fixed an issue where deleting all IPSec tunnels did not flush route table 220. [OG-11371]
- Fixed the bond interface going down once any enslaved interface is dropped (a regression introduced in 5.2.1 by OG-11298). [OG-11368, OG-11369]

Security Fixes

- Upgrade pam_radius to version 3.0.0 to mitigate CVE. [OG-11336]
  - Fixed CVE-2024-3596 (BlastRADIUS attack).
  - A new “Require Message-Authenticator” option has been added to RADIUS settings to mitigate BlastRADIUS attacks. It must be enabled manually, as it’s off by default after a config erase.
  - Added BlastRADIUS mitigation endpoint to REST API. [OG-11352]
- Upgrade OpenSSH to version 9.9p2 to mitigate CVEs. [OG-11335]
  - Fixed CVE-2025-26465 (VerifyHostKeyDNS machine-in-the-middle attack).
  - Fixed CVE-2025-26466 (Denial of service attack).

5.2.1 (Feb 2025)

This is a patch release

NOTE

- FIPS Mode
  - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
  - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
  - Backup your configuration before attempting an upgrade to 5.x

    - After a successful upgrade, make sure to capture a new backup
    - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- 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 https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Added support for the external EMD32 Environmental Monitor (EMD). [OG-11182] [OG-11204]
    - EMD32 is interchangeable with EMD5000
    - EMDs connect to the RS232 serial port via the EMD adapter cable.

Fixes

- Fixed cellmodem connection failure on /dev/cdc-wdm1 by disabling RMNET usb endpoints (MC73xx). [OG-11173]
- Fixed an issue where RPC status indicators displayed incorrect status and colour after upgrading to 5.1.1. [OG-11287]
- Fixed the race condition to set WAN MTU while bonding is enabled.[OG-11298]
- Fixed ez-ipupdate being restarted too quickly due to wrong user configurations of dyndns. [OG-11308]
- Fixed USB provisioning (ZTP) (IM72xx). [OG-11311]
- Fixed handling of duplicate conns/groups in conman config. [OG-11315]
- Fixed default self signed openssl certificates not being automatically renewed. [OG-11329]
- Fixed dashboard configuration to sanity check the number of widgets. [OG-11330]
- Fixed the description of the first USB stick in the configuration. [OG-11331]
- Fixed ability to connect to some Aruba and Cisco USB consoles by adding cdc_acm driver back (CM71xx). [OG-11188]

Other

- CDMA bands will now be disabled on -LMV SKUs using MC7354 cell modem modules. [OG-11297]
    - To override this behavior and continue using legacy CDMA bands run:
      ```
      config -s config.cellmodem.enable_cdma=on
      /etc/scripts/cell-carrier
      ```
    - The second command will be automatically run in time, this sequence of commands will ensure the effect is immediate.

5.2.0 (Nov 2024)

This is a production release

NOTE

- FIPS Mode
  - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
  - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
  - Backup your configuration before attempting an upgrade to 5.x
  - After a successful upgrade, make sure to capture a new backup
  - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- 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 https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Feature

- IPSec IKEv2 Support. [OG-11195]
  - Add IKEv2 to allow for multiple subnets and is also more secure and recommended for Key Exchange.
  - Adds the “IKE Version” option to the UI with the available values: Auto, IKEv1, and IKEv2.
    - Connections marked with ‘Auto’ will use IKEv2 when initiating, but accept any protocol version when responding.
  - Add back the 4x ipsecX interface.
    - A virtual ‘ipsecX’ interface where ‘X’ is the tunnel IPsec number as it appears in config.
    - Uses VTI and user space.
    - Allows for interface based routing over policy based in the firewall.
    - Allow for the Forwarding and Masquerading UI page to forward between IPSec and other interfaces.
  - IPSec initiator will now restart on a responder ipsec restart command.
  - Correct phase 2 Perfect Forward Secrecy of keys (PFS) behavior.

- Added IPSec missing DH groups. [OG-10991]
  - NIST Elliptic Curve Groups.
    - `ecp192-ecp224-ecp256-ecp384-ecp521`
  - Available for phase 1 (Negotiable only) and phase 2.
    - For individual selection of both phase 1 or phase 2 ciphers, its recommend to use the Custom Tunnel Options and this can override any previous settings in the UI.
    - For example (Option name = Argument):
      For phase1:

`ike = <encryption_alg>-<integrity_alg>[-<prf>]-<dh_group>`

For phase2:

`esp = <encryption_alg>-<integrity_alg>-<dh_group>`

Or:

`ah = <integrity_alg>[-<dh_group>]`

- e.g. `ike = aes256gcm12-sha256-modp4096`

- To utilize the AEAD (Authenticated Encryption with Associated Data) algorithms that can't be combined with classic encryption ciphers in the same proposal, the Custom Tunnel Option is also recommended.

Enhancements

- Added handling for bearers inactive timeout threshold (IM72xx). [OG-10986]
  - Some carriers may have adopted bearer's inactive timeout threshold, and if the ipv6 connection stays idle (no application-driven traffic) the bearer connection may be dropped. Although the cellmodem could reconnect and obtain new ipv6 addresses, the link is not usable.
  - To avoid such situations, use the following two config variables to enable the pinging of cellmodem's gateway's ipv6 link-local address to keep the connection alive:

    ```
    config -s config.cellmodem.ipv6.keepalive.enabled=on
    config -s config.cellmodem.ipv6.keepalive.threshold=900
    ```

  - The first variable is not needed for the Verizon network (since this "keepalive" feature is automatically enabled for it).
  - The second variable, if unset, defaults to 3600 seconds, or 1 hour
- Fixed issues with DNS over IPv6 when another interface is configured as IPv4. [OG-11203]
  - DNS, Media, MTU and Serial Port Aliases also apply to IPV6 Settings and are now grouped together and located after the IPv4 and IPv6 settings.
- Add missing help info in the web UI for custom OpenVPN tunnels. [OG-11157]

Fixes

- Fixed an issue where having a USB ZTP image parameter prevented the script or lighthouse parameters from being used. [OG-11156]
- Fixed an issue where ACM devices would have high CPU utilization when /var/mnt/storage.nvlog was not mounted. [OG-11164]
  - If the behaviour is present on IM/CM products, the user will need to specify volume format in config for the storage media.
- Fix issue with link speed/duplex not being set on IM72xx OOBFO interface. [OG-11192]
- Fixed jumbo frame drops when the path MTU is larger than the TX checksum offload limit of the Ethernet controller (1600 bytes) (IM72xx). [OG-11213]
- Fixed static route behavior. [OG-11241]
- Fixed an issue where crontab stored files in volatile storage instead of /etc/config/crontab.'user' as 4.x does. [OG-11242]
- Fixed /etc/scripts/cellmodem-power not working as expected (MC7430). [OG-11244]
- Fixed IPv6 addresses accruing (MC7354). [OG-6488]
- Fixed IPv6 configuration disallowed error for the cellmodem when it is not supported by the carrier [OG-11250]
- Fixed redundant invocation of conman_status when checking if cellmodem is configured as the failover interface. [OG-11278]
- Fixed web terminal to serial ports 502 Bad gateway error [OG-11280]
- Fixed web terminal to serial ports intermittently hangs on user input [OG-11276]
- Fixed snmpd restarting unnecessarily when an interface's override ifDescr token is used. [OG-11289] [OG-11274]

Other

- Backup configuration files with a different major version than the current firmware version will no longer be applied. [OG-11257]

5.1.1 (Oct 2024)

This is a patch release

NOTE

- FIPS Mode
  - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
  - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- 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 https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Added XFRM state and policies, and IP tunnel info to the support report. [OG-11172]

Fixes

- Fixed client side SFTP support. [OG-11221]
- Fixed issues with IPsec by setting system routing rules at a fixed and known priority. [OG-11183]
- Fixed an issue where setting RADIUS to MSCHAPv2 would sometimes add PAP headers to the request. [OG-11152]
- Fixed an issue that prevented port sessions to disconnected USB ports from being cleaned up as expected. [0G-11044]
- Fixed an issue where SFP interfaces were not allowed to use 1000base Tx-FD when auto-negotiation fails. [OG-11161]
- Fixed an issue where the dashboard widget settings would be overwritten with defaults until the widget layout is saved. [OG-11163]
- Fixed an error when updating user passwords with the API when there are multiple local users. [OG-11191]
- Fixed infod high CPU usage while generating support report. [OG-11162][OG-11239]

Security Fixes

- Fixed CVE-2024-39894 in SSH (ObscureKeystrokeTiming logic error). [OG-11189]

- Fixed CVE-2024-45490, CVE-2024-45491, CVE-2024-45492 in libexpat. [OG-11219]

5.1.0 (Aug 2024)

This is a production release

NOTE

- FIPS Mode
  - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
  - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- 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 https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Features

- Added FIPS support.
  - The OpenSSL FIPS provider version is pinned at 3.0.9 which is certified as compliant with FIPS 140-2. [OG-11065]
- Added NAT64 support. [OG-10990]
- Added SNMP configuration to set interface descriptions. [OG-11113]
- Added Remote Authentication AAA connection timeout configuration. [OG-11142]

Enhancements

- Added support for Panduit G5 PDU for dynamic outlet detection. [OG-11079]
- Enabled IPSec updown to run a custom script on up/down and enable a custom script to be run when the cellular interface gets an IP address. [OG-11166]
  - Enabled the IPVTI kernel module.

Fixes

- Fixed a failure to enrol 5.x node with Lighthouse driven enrollment in IPv6 only setup. [OG-11132]
- Fixed issue preventing SMS sending (IM72xx-LMV). [OG-11015]
- Fixed IPv6 serial port aliases failing to apply when IPv4 is not configured. [OG-11159]
- Fixed inconsistent WAN routes metrics. [OG-11122]

5.0.5 (Jun 2024)

This is a patch release

NOTE

- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Fixes

- Fixed cellmodem bearers having issues disconnecting when using some carrier's APN (MC7430). [OG-11063]
- Fixed frequent SNMP `No such file or directory` messages in syslog. [OG-11070]
- Fixed default credentials not working after upgrade to 5.0.0+ (rev6 IM72xx). [OG-11101]
- Fixed cherokee and sshd warnings about missing SSL certificate after config erase. [OG-11102]
- Fixed setting up crontab.root after config erase. [OG-11103]
- Fixed cell and dormant failover static routes not installing until failover occurs. [OG-11105]

5.0.4 (May 2024)

This is a patch release.

NOTE

- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Fixes

- Fixed displaying the name of current active carrier on cellmodem (MC73xx). [OG-11057]
- Fixed cellmodem sim2sim failover. [OG-10258]
- Fixed a false-positive error message when groups are initialized at startup. [OG-11054]
- Fixed RADIUS + PAP appending garbage characters to passwords. [OG-11058]
- Fixed Statistics > Cellular page failing to display preferred firmware/carrier. [OG-11062]
- Fixed ipsec configurator segfault when cellular modem is enabled but has failed to obtain an IP address from the bearer. [OG-11064]

Other

- Removed WiFi support as of 5.0.0 (IM72xx).
- EOL notice for WiFi was given in April of 2019 and has now been discontinued.
- Remove support for FIPS 140-2 as of 5.0.0. If using FIPS mode, it is recommend to remain on a previous version of 4.x.x.

- Remove SDT Connector as of 5.0.0. [OG-9717]

5.0.3 (Apr 2024)

This is a patch release.

NOTE

- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Fixes

- Fixed the `sfp_info` command causing issues with the GPIO line when enabling the SFP module on ACM7004-5. Also sometimes triggered by generation of the support report. [OG-11001]
  - Workaround is to reboot the device
  - Or run `gpioset 4 22=0`
- Fixed CLI session timeout not working. [OG-11047]
- Fixed TFTP not working. [OG-11048]
  - Workaround is to remove the following line
    `69 stream udp nowait root /bin/tftpd /var/mnt/storage.nvlog/tftpboot`
    from `/etc/config/inetd.conf` and restart `inetd`
  - Or run `sed -i '/^69 stream/d' /etc/config/inetd.conf; killall inetd`
- Fixed early failure when attempting to resolve an unreachable Lighthouse external IP address. Allowed additional external IPs to be attempted. [OG-11012]
- Fixed cellctld segfault while accessing bearer's ipv6 configuration. [OG-11055]
- Fixed ModemManager regex initialisation error. [OG-10967]

Other

- Removed WiFi support as of 5.0.0 (IM72xx).
  - EOL notice for WiFi was given in April of 2019 and has now been discontinued.
- Remove support for FIPS 140-2 as of 5.0.0. If using FIPS mode, it is recommend to remain on a previous version of 4.x.x.
- Remove SDT Connector as of 5.0.0. [OG-9717]

5.0.2 (Mar 2024)

This is a patch release.

NOTE

- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with

your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Improved wording around Modem Watchdog threshold function. [OG-6855]
- Improved cell-modem interface determinism. [OG-8110]
- Improved clarity of disabled interfaces in ogNetInterfaceTable. [OG-11004]
- Restored lsusb behaviour from OGCS 4. [OG-10987]

Fixes

- Fixed a potential bootloop issue when upgrading from version 4.x.x to 5.x.x. (ACM700x) [OG-10994]
- Fixed inconsistent system state with wrong PID in conman.pid. [OG-3551]
- Fixed auto-response starting multiple network event triggers. [OG-8529]
- Fixed ICMPv4 echo-requests to a cellmodem address still receiving responses once the connection has been disconnected. [OG-10258]
- Fixed a bug where the correct SIM slot is not confirmed to be active before modifying profiles. [OG-10522]
- Fixed console output not mapping newlines. [OG-10955]
- Fixed power supply values not being updated in SNMP OIDs. [OG-10968]
- Fixed SNMP displaying duplicate PSU sensors. [OG-10972]
- Fix the Delay Config Commits feature preventing the re-generation of configuration files after upgrade. [OG-11007]
- Fixed a bug in snmpstatusd to ensure the ogEmdTable OID may be fetched correctly. [OG-10989]
- Fixed the modeSettings documentation in the RAML. [OG-10985]
- Fixed bug preventing access to cascaded device ports. [OG-11014]

Other

- Added missing radvd package. [OG-10988]
- Removed “Cellmodem MTU” field from “Enable Dial-Out” page. [OG-9281]
- Removed WiFi support as of 5.0.0 (IM72xx).
    - EOL notice for WiFi was given in April of 2019 and has now been discontinued.
- Remove support for FIPS 140-2 as of 5.0.0. If using FIPS mode, it is recommend to remain on a previous version of 4.x.x.
- Remove SDT Connector as of 5.0.0. [OG-9717]

5.0.1 (Feb 2024)

This is a patch release.

NOTE

- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx).

Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Sierra Wireless RRC logging now occurs via QCDM. [OG-10920]
- SSH keys may be removed using a new delete API. [OG-10822]
- Updated Statistics Failover & Out-of-Band page to show IP address. [OG-8543]

Fixes

- Fixed USB serial ports not appearing (CM71xx). [OG-10960]
- Fixed Custom WAN MTU causing eth0 routes to disappear. [OG-10930]
- Fixed cell-fw-update attempting to update already up-to-date firmware. [OG-10929]
- Fixed sysObjectID OID showing ogIM72xx (CM71xx). [OG-10928]
- Fixed corrupted support reports (CM71xx). [OG-10927]
- Fixed connection refused error for SSH to port 30xx. [OG-10922]
- Fixed modem-watchdog failing to find cellmodem interface. [OG-10903]
- Fixed StrongSwan IPSec phase2 not occuring. [OG-10902]
- Fixed missing password parameter from /auth endpoint for TACACS. [OG-10859]
- Fixed inconsistent GET users/{$id} results. [OG-10821]
- Fixed https redirect with HSTS enabled. [OG-10815]
- Fixed overly strict cellular username field disallowing certain characters. [OG-10734]
- Fixed restricting access to PDU outlets via group permissions breaking access to subsequent PDU outlets. [OG-10703]
- Fixed iptable entry not being created when forwarding between the same interface. [OG-10634]
- Fixed monitored/remote UPS connection not being removed. [OG-10613]
- Fixed RPC Status page Outlet tabs changing inconsistently. [OG-10531]
- Fixed IPv6 DNS servers on cellmodem populating wwanX.dhcp rather than wwanX.dhcp6. [OG-10179]
- Fixed erroneous errors during the transfer of the main RSA public key to the cascaded nodes using SCP. [OG-9798]
- Fixed multiple DHCP servers on various interfaces resulting in conflicts within the dhcpd.conf file. [OG-9236]
- Fixed GPS Fix Frequency Web UI notation and functionality. [OG-8183]
- Fixed DHCP server logs polluting syslog before LAN interface is up. [OG-7503]
- Fixed overly permissive file permissions for /etc/config/hosts. [OG-10824]
- Fixed issue where script templates could not be applied from Lighthouse. [OG-10934]
- Fixed CVE-2016-20014 in PAM TACPLUS (Non zeroed arep structure). [OG-10943]
- Fixed CVE-2020-13881 in PAM TACPLUS (TACACS+ secret leaks to journald). [OG-10943]
- Fixed CVE-2020-27743 in PAM TACPLUS (No check for OpenSSL RAND_[pseudo_]bytes). [OG-10943]
- Fixed CVE-2023-41913 in StrongSwan (Buffer overflow and unauthenticated remote code execution). [OG-10945]
- Fixed CVE-2023-5363 in OpenSSL (Process key length and iv length early if present). [OG-10938]
- Fixed CVE-2022-1586 in PCRE2 (Incorrect value reading in JIT). [OG-10939]
- Fixed CVE-2022-1587 in PCRE2 (Duplicated data transfers affecting recursions in JIT). [OG-10939]
- Fixed CVE-2022-41409 in PCRE2 (Negative repeat value in pcre2test subject line). [OG-10939]
- Fixed CVE-2023-46849 in OpenVPN (–fragment option divides by zero). [OG-10941]

- Fixed CVE-2023-46850 in OpenVPN (Use after free memory issue). [OG-10941]
- Fixed CVE-2023-42465 in Sudo (Vulnerability to ROWHAMMER attacks). [OG-10946]
- Fixed CVE-2020-10595 in PAM KRB5 (Buffer overflow). [OG-10942]
- Fixed CVE-2008-5730 in Netcat (CRLF injection vulnerabilities). [OG-10940]
- Fixed CVE-2023-48795 in OpenSSH (Susceptibility to terrapin attack). [OG-10944]

Other

- Removed WiFi support as of 5.0.0 (IM72xx).
    - EOL notice for WiFi was given in April of 2019 and has now been discontinued.
- Remove support for FIPS 140-2 as of 5.0.0. If using FIPS mode, it is recommend to remain on a previous version of 4.x.x.
- Remove SDT Connector as of 5.0.0. [OG-9717]

5.0.0 (Nov 2023)

This is a production release that includes a Linux kernel update. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.

NOTE

- Added minimum required versions before upgrade to 5.0.0 (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0

Features

- Upgraded the Linux kernel, move to modern security standards and utilize a well supported standard C library.
    - Upgraded Linux Kernel from 3.10.0 to 5.17.0.
    - Upgraded OpenSSL from 1.0.1u to 3.1.2 (Enables TLSv1.3 and disables 1.0 and 1.1).
    - Upgraded OpenSSH from 7.7 to 9.5p1 (adds host-key algorithms: rsa-sha2-512 (2048-bit), rsa-sha2-256 (2048-bit)).
    - Upgraded OpenVPN from 2.4.6 to 2.6.2 (supports OpenSSL 3.0, TLS v1.3 and enforces stricter TLS, cipher selection, and modern security standards).
    - Changed Openswan U2.6.37/K to Strongswan 5.9.11 (Added authentication algorithm options for IKE and ESP/AH cipher suites sha256 and sha512).

Enhancements

- Update output of ifconfig and Statistics UI page due to updated kernel.
- Upgrade IPsec, implementation changed to Strongswan from Openswan. [OG-9444]
    - Aggressive mode now defaults to off for security reasons.
    - Strongswan does not present the “ipsec0” interface in ifconfig output. This has no effect on functionality, however IPsec tunnels may still be queried through CLI with “ipsec status”.
    - When overriding the default ciphers, perfect forward secrecy is now activated by providing Diffie-Hellman groups in the Phase 2 ESP/AH ciphers.
    - Added authentication algorithm options for IKE and ESP/AH cipher suites sha256 and sha512.
    - Renamed dh22, dh23, and dh24 Diffie-Hellman groups to modp1024s160,

modp2048s224, modp2048s256.
    - The keywords “leftsubnets” and “rightsubnets” are now “leftsubnet” and “rightsubnet” and limited to a single subnet.
    - The “leftsourceip” and “rightsourceip” options were cleared and are now derived from the leftsubnet and rightsubnet fields and are no longer required for LAN or Cellular tunnels
- Change DNS Resolver IPv4/IPv6 preference configuration. [OG-10316]
    - This has moved to /etc/config/resolvpref.conf from /etc/gai.conf.
- Update micro SD card to normalized path. [OG-10313]
    - config.storage.sd.device has been normalized to /dev/mmcblk0p1. This path will be update automatically during the upgrade.
- Update REST API version to v1.8
    - SDT configuration was removed from the REST API, so the latest API version has been incremented.
- Add syslog warning message for cases where the system clock is out of a pre-set range which likely indicates a bad Real Time Clock (RTC) battery. [OG-10876]
- Reduce PHY emissions. [OG-10798]
- Enhancement to allow applying a config backup between IM7200-24E and non- IM7200-24E devices. [OG-10895]

Fixes

- Fix protocol identifiers in inetd.conf, tcp6 and udp6 changed to tcp46 and udp46. [OG-9291]
- Fix some classes of error messages being un-logged.
- Error messages will now appear on the console when “config.console.debug=on”.
- Fix ethernet routes not being removed when aggregation is enabled.
- Fix an issue where the MC7455 modem would load Verizon firmware instead of AT&T, even when configured for AUTO-SIM with an AT&T SIM card inserted. [OG- 10607]
- Fix an error when checking for cellular firmware updates. [OG-10651]
- Fix issues of internal services restarting when logging facilities are used. [OG- 10738]
- Upgrade IEEE 802.1x (EAPOL) to use PEAP-MD5 instead of PEAP-MSCHAPv2 which utilises a weak cipher. [OG-10466]
- Fix REST API PATCH request method for serialPorts endpoint. [OG-10693]
- Fixed an issue where autoresponse could not match regular expressions in multi- line SMSes by replacing ” with ’ ’ in incoming SMS messages before applying regular expressions. [OG-10778]

Other

- Remove WiFi support (IM72xx).
    - EOL notice for WiFi was given in April of 2019 and has now been discontinued.
- Due to kernel changes, the output of ifconfig is slightly different. This results in changes to the Statistics UI page and may break existing scripts that make use of the device IP.
- Remove support for FIPS 140-2. If using FIPS mode, it is recommend to remain on a previous version of 4.x.x.
- Remove FAT32 mount option “-o sync”, consider replacing with “-o flush”. [OG- 9844]
- Remove all options from lsusb.
    - Output may be filtered using grep.
- Remove SDT Connector. [OG-9717]
- Remove Network Host Permitted Services and Host Logging.
- Router Throughput Performance Using Iperf3 With 128KB Buffers:
    - Bandwidth Results With Bridging Enabled ACM7000, CM7100: 550 Mbps IM7200: 700

Mbps
    - Bandwidth Results With IP Forwarding Enabled ACM7000, CM7100: 430 Mbps IM7200: 600 Mbps

4.13.6 (Sep 2023)

This is a patch release.

Features

- Add Web-UI support for selecting Internal Cellular Modem SIM authentication protocols. [OG-10687]

Fixes

- Fix cellular authentication protocol selection and support for non-alphanumeric password characters. [OG-10687]

4.13.5 (Jun 2023)

This is a patch release.

Enhancements

- Allow for username to have capitalized first letter. [OG-10610]

Fixes

- Fix enrolment to Lighthouse with modified HTTPS port. [OG-10532]
- Fix cascading ports links on the main menu. [OG-10505]
- Fix generation of complete support report. [OG-10500]
- Correct source IP address for pmloggerd for remote serial logging. Independent of global routes changes. [OG-10342]

Known Issues

- Cellular username field has overly restrictive character requirements. [OG-10734]

4.13.4 (Apr 2023)

This is a patch release.

Fixes

- Fix SSH and secondary Lighthouse enrolment in FIPS mode by including the weak SSH ciphers removed in 4.13.0 for FIPS mode only. [OG-10456]

Known Issues

Applying group permissions to restrict access to PDU outlets results in a loss of access to the subsequent outlets. [OG-10703]

4.13.3 (Mar 2023)

This is a patch release.

Enhancements

- Add enlarged image partition size to enable upgrading to future releases. (PLEASE NOTE: A UI 'Error 24' or a netflash 'image too large for FLASH device' error will be displayed if upgrading from a prior release and the loaded image is too large). (IM72xx) (CM71xx) [OG-10283]
- Add missing security headers to the web interface. [OG-9856]
- Update web UI DH key size to 2048. [OG-10411]
- Update web server to allow use of more secure ECDHE key exchange ciphers. [OG-10202]

Fixes

- Fix RAML stating that execution_id for script template must be an integer when it's a string. [OG-9865]
- Fix PortShare password being cleared when editing a serial port via the web UI. [OG-9944]
- Fix incorrect OpenVPN port information on UI when using custom configuration. [OG-9251]
- Fix an issue causing new devices to ignore USB-serial adaptors due to hardware change. (CM71xx) [OG-10168]
- Fix a process that adds a user to allow a hyphen in the username. [OG-10244]
- Fix an issue where sysUpTimeInstance was set to 0 for some SNMP traps. [OG-10388]
- Fix a benign error message when saving a config backup to a USB stick. [OG-10297]
- Fix high verbosity of some portmanager logging. [10341]

4.13.2 (Feb 2023)

This is a patch release.

Enhancements

- Add an upgrade safety check for usage of the JFFS2 image#2 partition to prevent potential data loss. If required, apply the "-O" option to bypass this check and allow overwriting (IM72xx) [OG-10346]
- Add information on how to disable WDS autoconnect in the wwan-custom script. [OG-10102]
- Add a warning that RFC 2217 cannot be used with other access methods for a serial port in Console Server mode. [OG-9927]
- Update minimum web management session timeout from 10 minutes to 5 minutes. [OG-10343]

Fixes

- Fix an issue where rpcd did not fetch status when requested. [OG-9504]
- Fix an issue where OpenVPN tunnels not cleaning up configuration files when removed. [OG-9776]
- Fix unclear pmshell -l usage text. [OG-9790]
- Fix serial port UI missing Raw TCP '+Auth+Crypt' PortShare info. [OG-9945]

- Fix wrong baud rate shown on the statistics page and pmstats for local console mode port. [OG-9995]
- Fix IPv4 /31 netmasks breaking connectivity. [OG-10080]
- Fix an issue where /etc/config/groups would become unreadable by pmshell. [OG-10108]
- Fix wwan-conn can try to use /dev/cdc-wdm0 for QMI which does not work in all cases. [OG-10203]
- Fix Portmanager FD limit not configurable. [OG-10205]
- Fix all values associated with SNMP Trap not sent. [OG-10290]
- Fix a benign error message when saving a config backup to a USB stick. [OG-10297]
- Fix verbose logging from portmanager. [OG-10341]
- Fix cellmodem connection taking too long to reconnect if DHCP client fails. [OG-10365]
- Fix an issue where the device would sometimes not reboot during failure when upgrading via the web UI. [OG-10366]

Other

- Remove CDK Support. [OG-10358]

4.13.1 (Nov 2022)

This is a patch release.

Enhancements

- Improve cellular connection disconnect detection. [OG-10201]

4.13.0 (Nov 2022)

This is a production release.

Features

- Add support for encrypted backups. [OG-9998]

Enhancements

- Add missing security headers to the web interface. [OG-9856]
- Improve cell firmware update script. [OG-10134]
- Improve MC7455 cellular modem handling (IM72xx-LR). [OG-10110]
- Improve language used in Kerberos authentication page. [OG-10072]
- Upgrade vsftpd to 3.0.5. [OG-9857]

Fixes

- Fix issue when trying to run lhvpn-callhome as non-root user. [OG-10032]
- Fix weak SSH ciphers as recommended by ssh-audit. Note: may change the known fingerprint of a device - users may need to clear the host entry from their known_hosts file. [OG-9855]
- Fix issue with APN not displaying on cellctl command. [OG-9878]
- Fix cell-fw-update for MC7455 modems (IM72xx-LR). [OG-9902]
- Fix missing cellmodem info in support report. [OG-9964]
- Fix spelling in dialin web page. [OG-10029]

Known Issues

Opengear are aware of the following product-specific issues with this release:

- SSL/TLS Weak key exchange (DH 1024): Recommended ECDHE (Curve 25519 DHE 253) key exchange ciphers are not supported by the web server.

4.12.4 (Aug 2022)

This is a patch release.

Enhancements

- Add a script /etc/config/scripts/wwan-custom, which allows custom commands to be sent to the modem in response to specific events. [OG-9853]
- Add more cellular information to the support-report. [OG-9964]
- Add alternative PHY support for CM7100 boot-loaders. [OG-10067]

Fixes

- Fix the Web-UI dashboard to not display an IPv4 address when IP Passthrough is enabled. [OG-8108]
- Fix Cascaded Port configuration node naming. [OG-9248]
- Fix support for querying currently mounted file-systems via SNMP. [OG-9595]
- Fix DNS Server details propagating correctly when IP Passthrough is enabled. [OG-9601]
- Fix the LDAP group membership attribute field to allow special XML text. [OG-9774]
- Fix the firewall packet filter and translation rules for IP Passthrough. [OG-9775]
- Fix the REST-API response to bad credentials. [OG-9779]
- Fix the firewall to drop invalid ICMP replies when IP Passthrough is enabled. [OG-9781]
- Fix cellular GPS NMEA streaming persistance when rebooting. [OG-9834]
- Fix the Web-UI and cellctl command to display the current cellular APN correctly. [OG-9878]
- Fix the Cascaded Port configuration from being partially removed during firmware upgrade. [OG-9903]
- Fix some successful login attempts being reported as failures in logs. [OG-9950]

Other

- Remove SNMP Multiplex (SMUX) support (TCP port 199) for the SNMP Service. [OG-9684]
- Remove the forced detachment from the cellular packet service when disconnecting a data session. [OG-9867]

4.12.3 (May 2022)

This is a patch release.

Enhancements

- Add interfaces v1.7 API with IMSI and ICCID
- Improve brute force detection logic
- Improve performance when adding and removing users
- Improve reliability of IM7248-2-DAC-LR modem

- Improve reliability of long-running cellular connections
- Improve allow pmshell -l xx, in addition to the existing portxx and /dev/portxx
- Improve tighten permissions of infod.pid
- Improve run scripts in /etc/config/resolvconf/uclinux.d when resolv.conf changes

Fixes

- Fix issue where auto-response settings were reset to default when entries are removed
- Fix editing of multiple ports on CM7196 only showing ports the user can edit
- Fix issue where users can only see Network Hosts they have access to
- Fix issue with RPC Status (logging and graphs)
- Fix warnings about /etc/config/openssl.cnf
- Fix non-wan, dormant failover interfaces can be used for DNS requests
- Fix the peer for a dial-in/out modem is used as the default gateway for that interface
- Fix issue with login for 'root' user when LDAP server are uncontactable
- Fix validation of the CSR common name to allow wildcards
- Fix a number of cell modem interface endpoints in the RAML documentation
- Fix an issue with generating support reports on some devices
- Fix for portmanager no longer intermittnetly hanging when 'single connection' is in use
- Fix an issue with SMS autoresponse using EM7565 modem and Verizon
- Fix cell firmware update
- Fix CVE-2022-0778 in OpenSSL (Infinite loop in BN_mod_sqrt())
- Fix issue with upload using tftp
- Fix a potential crash in pmshell

4.12.2 (Dec 2021)

This is a patch release.

Fixes

- Fix cellmodem issue with network registration after disconnection

4.12.1 (Nov 2021)

This is a patch release.

Enhancements

- Improve the relevance of OpenVPN syslog messages

Fixes

- Fix process listing in the support report
- Fix missing SNMP OID value for sysObjectID
- Fix TACACS login failover if the remote authentication server behaves incorrectly
- Fix the validation of DHCP hostnames to forbid the use of spaces
- Fix an issue with the port flow control settings not being correctly saved

4.12.0 (Oct 2021)

This is a production release.

Enhancements

- Add support for Digi RPM 8, 10
- Add support for MS-CHAPv2 RADIUS user authentication
- Improve behaviour with duplicate Lighthouse enrolment
- Improve config -e error robustness
- Improve loopback test tool reliability
- Improve nameserver configuration as a comma-separated list
- Improve session POST input sanitisation
- Improve webui by removing inaccessible navigation elements
- Upgrade to net-snmp 5.9.1
- Upgrade to procps-ng 3.3.17
- Upgrade to rsyslog 8.2106.0

Fixes

- Fix cellmodem responds to ping when interface disabled
- Fix dynamic DNS not working with cellular interfaces
- Fix dynamic DNS server config ignored except for gnudip
- Fix infod_listener reporting strange ipv4address change
- Fix ipsetd removal
- Fix IPv6 formatting in Lighthouse manifest files
- Fix Lua crash in REST API (VACM)
- Fix misreported cell info while in IP passthrough mode
- Fix nameserver query order during failover
- Fix nameserver search domains
- Fix OGTRAP MIBs not compiling with OpenNMS and HP IMC
- Fix OpenVPN defaults for CVE-2016-2183 CVE-2016-6329
- Fix pmshell and web terminal crash when using LocalTACACS
- Fix portmanager resource leak when using TACACS
- Fix RPCs connected above serial port 64 (CM7196)
- Fix SMS failures with MC7354 modems
- Fix USB serial port hotplug tracking
- Fix webui firewall rule order arrows
- Fix webui radio buttons not selecting default

4.11.0 (May 2021)

This is a production release.

NOTE

- pmslave was removed, use ‘sudo pmshell -s -l ’ instead.
- Some equipment may no longer connect using the revised default ciphers. Refer to the Opengear knowledge base
- SDT Connector is no longer supported

Enhancements

- Add cellmodem firmware download and auto-upgrade support for EM7565 and MC74xx
- Add cellmodem multi-carrier installation support for EM7565 and MC74xx

- Add cellmodem per-SIM carrier configuration support for EM7565 and MC74xx
- Add cellmodem support for MC7455 in IM72xx-LR
- Add cellular IMSI and ICCID status to REST API
- Add password-less support for some SSH users
- Add retry-backoff behaviour for Lighthouse integration
- Add self-signed web server cert regeneration on expiry
- Improve inclusive language in user interface
- Improve migration of modem watchdog configuration
- Improve OpenSSH default cipher strength
- Improve OpenVPN default cipher strength, disable TLS 1.1
- Improve the timing to bring up IPsec tunnel via cellmodem interfaces
- Improve web server security against CSRF
- Upgrade dnsmasq 2.84, fixing various CVEs

Fixes

- Fix an IPv6 address representation issue in REST API
- Fix blank buttons in SNMP manager page
- Fix Cherokee CVE-2019-20799 (memory corruption errors)
- Fix deprecated IPv6 addresses on cellmodem interfaces
- Fix dhcp-relay over ipsec tunnels via cellmodem interfaces without MAC addresses
- Fix disconnected USB ports display issues
- Fix Cherokee CVE-2020-12845 (DoS issue in web server)
- Fix excessive cellmodem QMI operation messages in syslog
- Fix false-positive notifications of IPv6 address changes for Lighthouse
- Fix handling of multiple Lighthouse enrolments
- Fix issue when processing large TACACS+ authorization packets
- Fix LDAPDownLocal behaviour with bad server key
- Fix OpenSSL CVE-2020-1971 (EDIPARTYNAME NULL pointer de-reference)
- Fix SNMP engineBoots counter
- Fix the number of power supplies shown on some models (IM72xx)
- Fix webserver TLS 1.2 support when in FIPS mode

Other

- Removed ipsetd support (address learning through ARP)

Known Issues

Opengear are aware of the following product-specific issues with this release:

- Some carriers have been observed to take longer than usual to connect.
- Automatic carrier selection (AUTO-SIM) on models that support it is unreliable for some carriers and will require changing the ‘Preferred Carrier’ setting from the default AUTO-SIM.

4.10.0 (Dec 2020)

This is a production release.

NOTE

- **Backwards compatibility alert:**

This version supports SHA-512 password hashing which is not supported in previous versions. After installing this version there are some cases where reverting to a previous version could result in loss of access to user accounts including the root account. Please refer to this Knowledge Base Article for details:

Enhancements

- Add netfilter DSCP QoS support
- Add model information to SysDescr SNMP OID
- Add support for SHA-512 crypt in password file
- Add SysName to SNMP traps
- Add failover status SNMP OID
- Add /var ramdisk usage listing to support report
- Add support for Tripp-Lite PDUMH20HVATNET (auto transfer switch)
- Add sudo password for users in admin group

Fixes

- Fix wireless network forwarding
- Fix cascade configuration with FIPS enabled
- Fix a network connection problem (ACM7004-2-LV)
- Fix slow authentication in LocalRADIUS mode
- Fix drivers for Cyberpower and Eaton UPS
- Fix serial port log level OID in SNMP
- Fix RADIUS sending incorrect service type
- Fix GPS NMEA logging (ACM700x-L)
- Fix NTP over cellular connection
- Fix SNMP iftable duplicating ipsec and vpn interfaces
- Fix USB to serial interface reconnection handling
- Fix duplicate VPN processes
- Fix options being lost on UPS page
- Fix CVE-2019-20800 web server request header vulnerability
- Fix edinittab editing bug
- Fix remote logging on port numbers higher than 64
- Fix log level of Modem Manager info messages
- Fix DHCP Relay over cellular on models with EM7565 modems
- Fix power supply failure log messages priority (now uses “error”)

4.9.0u1 (Aug 2020)

This is a production release.

Enhancements

- Add 802.1X (EAPoL) support
- Add Operations Manager product OID to products MIB
- Add REST support for serial port logging
- Add support for SNMP pre-hashed keys
- Add support for Tripp Lite PDUMH20HVATNET over SNMP
- Improve boot diagnostics, show board ID (IM72xx)
- Improve dashboard display active connection detail
- Improve dashboard display for IPv6-only interfaces
- Improve DHCP server pool address range validation to avoid silent service failure
- Upgrade to netkit-tftp-0.17 fixes timeout, segfault

Fixes

- Fix corrupted config when setting up IPsec tunnel
- Fix corrupted config when setting up OpenVPN tunnel
- Fix delayed config changes being applied during read-only operations
- Fix ethernet switch initialisation timeout under load (IM7216-24E)
- Fix global routes not being applied when IP passthrough in effect
- Fix memory leak when querying power supply table over SNMP
- Fix NTP client failing to use IPv4 secondary when IPv6 primary is unreachable
- Fix REST enrollment issue by deduplicating tunnels
- Fix rsyslog generic config filenames
- Fix silent character escaping in user password field
- Fix /var/log exhaustion when refreshing sessions
- Fix web UI issue with default syslog level selection
- Fix web UI validator rejecting valid email addresses

4.8.0 (Apr 2020)

This is a production release.

Enhancements

- Add cellfw update and carrier select to MC7304 models (ACM700x-LMR, IM72xx-LR)
- Add password masks to support-reports and RPC logs
- Add interface address lists to REST API
- Add port control-code control to REST API

Fixes

- Fix pmloggerd log spam when chowning files
- Fix DDNS using wrong cellmodem interface
- Fix Subject Alternate Name missing from CSRs
- Fix web UI bug when deleting multiple syslog server entries
- Fix option consistency (ls -h) (CM71xx)
- Fix incorrect IPv6 enable checkbox initial state
- Fix DHCP Relay to support ipsec0 as upper interface
- Fix ipsec cleaning up routes it didn't create
- Fix lost power monitoring log messages

Known Issues

Opengear are aware of the following product-specific issues with this release:

- Cellular modem may be disabled when selecting 'generic' carrier (IM7200-LR, ACM700x-LMR)

4.7.0u3 (Feb 2020)

This is a patch release.

Fixes

- Fix issue where PIN-locked SIMs would appear to be missing
- Fix SIM switching issue with empty slot (ACM7000-L)
- Fix unactivated SIM slot with autoresponse-controlled cellmodem

4.7.0u1 (Feb 2020)

This is a patch release.

Fixes

- Fix autoresponse ICMP ping test to use active interface
- Fix issue when clock changes during firewall update
- Fix misconfigured IM7216-24E switch MDIO bus

4.7.0 (Jan 2020)

This is a production release.

Enhancements

- Add DHCPv4 relay agent support
- Add initial root password change to comply with Californian laws
- Add IPv6 support to FTP client and FTP server
- Add support for configuring firewall log rate limiting
- Add support for Panduit G5 series PDU
- Add support for reporting CPU temperature (IM72xx)
- Add support for SNMP lm-sensors MIB: CPU and PCB temperatures
- Add support for static IPv6 routes
- Improve firewall reconfiguration performance
- Improve flash memory access performance during boot
- Improve global IPv6 UI control
- Improve image size by removing unnecessary development files
- Upgrade DHCP server to ISC-DHCP 4.1

Fixes

- Fix access to unauthorized serial ports via pmshell escape
- Fix a SIM select issue (ACM700x-L)
- Fix carrier auto-select (ACM700x-L)
- Fix CLI tool support for large files (>4GB)
- Fix IPv6 TAHI compliance issues
- Fix IRQ boot loop issue (IM72xx)
- Fix lost option for management LAN as failover interface
- Fix misleading error bootargs message (IM72xx)
- Fix missing usb group boot warnings
- Fix OpenSSH CVE-2018-15473 CVE-2018-20685 CVE-2019-6109 CVE-2019-6110 CVE-2019-6111
- Fix port log file size inconsistency
- Fix switch port reset/initialisation (IM7216-24E)
- Fix switch ports not attempting lower link speeds (ACM7004-5)
- Fix unnecessary RADIUS warning messages when accounting is disabled
- Fix XSS vulnerability in API error handler

4.6.0 (Aug 2019)

This is a production release.

Enhancements

- Add power supply state change messages to syslog
- Add support for config backup via REST API for Lighthouse
- Add support for ACM700x-L
- Add support for password obfuscation in serial logs
- Add RFC3339 syslog format option
- Add support for Verizon autoprovisioned APNs
- Improve netflash reliability when using manifest.og on USB

Fixes

- Fix NTP server not working on eth1
- Fix message encoding errors in REST API
- Fix presentation of RFC2217 option for some system ports
- Fix a stability issue when auth misconfigured
- Fix Log Out button issue when not logged in
- Fix issue with AT command channels on some cellmodems

4.5.0u2 (Jun 2019)

This is a patch release.

Enhancements

- Add current APN to cellmodem dashboard

Fixes

- Fix cellmodem connection limit to 12 connect attempts per hour
- Fix lost IMSI and ICCID information (ACM700x-L)
- Fix missing AT command channel (ACM700x-L)

4.5.0 (May 2019)

This is a production release.

Enhancements

- Add cellular connectivity test support for Lighthouse
- Add configuration support for sshd MaxStartups
- Add SAN (Subject Alternative Name) support to CSR form, and update our algorithms
- Add support for Raritan PX3 PDUs
- Add support for rev6 power monitoring changes (IM7200)
- Add Tcl expect utility
- Add user disconnect support to pmshell
- Add vendor-specific attribute support to RADIUS groups
- Add RFC2217 control for built-in modems
- Improve UI styling
- Upgrade bash to 5.0

Fixes

- Fix an XSS vulnerability when viewing port logs
- Fix cannot enter '#' in username at login prompt
- Fix cellular modem not detected after upgrade with custom OpenVPN config
- Fix cellular modem not using CHAP authentication
- Fix cellular modem static routes not added to main routing table

- Fix crash in dashboard screen with custom widgets
- Fix ethernet port LEDs have inverted sense (ACM700x)
- Fix issue with IP Passthrough intercepted services config
- Fix missing network management tab (CM7196)
- Fix Net 2 lights constantly on (ACM700x-2)
- Fix service intercepts taking too long to stabilise during IP Passthrough
- Fix Verizon connections dropping with IP passthrough due to bad source IP address

Known Issues

Opengear are aware of the following product-specific issues with this release:

- Enabling forwarding between identical interfaces fails to create necessary iptables entries. [OG-10634]
- RFC2217 modem channel corruption (ACM700x-M)
- Fibre/SFP auto-media issues with bonded interfaces (IM72xx, ACM700x)

4.4.1 (January 2019)

This is a patch release.

Enhancements

- Add detection of invalid chars in user descriptions
- Add fw version to ZTP vendorclass and more client options
- Add support for disabling cellular modem
- Add support for Lighthouse v1.2 registration API

Fixes

- Fix cellular modem reference leak
- Fix ethernet switch issue after bond state change
- Fix IP-passthrough service issue when ethernet link is lost
- Fix mis-displayed error message in formlet
- Fix OpenVPN connection retry backoff delay
- Fix routing issue with static link-triggered failover
- Fix RPC log polling rate control
- Fix Wi-Fi activation after bridging/bonding enabled

4.4.0 (December 2018)

This is a production release.

Enhancements

- Add support for HTTP Strict Transport Security (HSTS)
- Add support for IPv6 to various CLI tools
- Add support for IPv6 for reverse DNS lookup
- Add support for switch port bonding (IM7216-24E)
- Add extended Diffie-Hellman group configuration to IPSec
- Add support for Cisco IRB829 router USB console
- Add support for Tripp Lite PowerAlert 15.04, 15.05 PDUs
- Add support for Servertech Sentry Switched V8.0 CDUs
- Add support for APC PDU AP8953 AP8959
- Add support for firewall “recent” matching

- Add support for DSCP QoS support (ACM700x, ACM7004-5)
- Add support for preferred DNS search domain on static IP interfaces
- Add support for modifying port configuration via REST API
- Add /system/version endpoint to REST API
- Add support for overriding shell selection when users have both admin and pmshell roles
- Add support for /etc/scripts/user-add and user-mod –password option
- Add “ogSpecific” SNMP field to OG-SMI-MIB
- Improve OpenVPN tunnel creation UI
- Improve SSH key generation at first boot
- Improve route handling with dormant failover interfaces
- Improve stability when switching MTU (CM71xx, CM7196)
- Improve ZTP logging of missing enrolment tokens
- Improve portmanager resource limits related to cascading
- Upgrade OpenSSH to 7.7p1
- Upgrade OpenVPN to 2.4.6

Fixes

- Fix initial HTTPS certificate generation
- Fix certificate key file permissions
- Fix “FragmentSmack” DoS vulnerability CVE-2018-5391
- Fix sshd host key selection at first boot
- Fix SSH logins not inheriting TERM variable
- Fix ping6 ignoring interface specifier
- Fix IPv6 failover test ping address issue
- Fix ethernet rx counters not incrementing (ACM7xxx, IM7xxx, CM71xx)
- Fix carrier lookup error with MC7710 modem (IM72xx-LR)
- Fix cellular interface metric not updated when disabling failover
- Fix undersized cellular MTU connectivity issue
- Fix MC7430 modem showing incorrect values for MDN and MSID (IM72xx-LMP, ACM700x-LMP)
- Fix an issue with modem detection after changing primary SIM
- Fix stale cellular address update issue with Lighthouse
- Fix firmware upload issue when enrolled with Lighthouse
- Fix memory leak when sending many SMSes
- Fix GPS serial port appearing on unsupported hardware
- Fix NTP client not updating time over cellular
- Fix USB stalls for some Cisco USB consoles
- Fix CTS flapping when unplugging another USB port
- Fix pmchat sometimes fails on USB ports above an unoccupied slot
- Fix duplicated Lighthouse tunnel issue
- Fix Lighthouse visibility of user enabled state
- Fix ZTP issue with user configuation in scripts
- Fix admin user can’t download port logs

Known Issues

Opengear are aware of the following product-specific issues with this release:

- Cellular interface name may alternate between wwan0/wwan1 affecting custom scripts

4.3.1 (September 2018)

This is a patch release.

Enhancements

- Add support for session disconnect by users with the Port Level Administrator Role

Fixes

- Fix pmshell label refresh after changes made via pmshell port configuration menu
- Fix SNMP Traps for network interface up and down events

4.3.0 (June 2018)

This is a production release.

Enhancements

- Add cellular MTU support
- Add syslog multiple endpoint support
- Add NTP password obfuscation
- Add port-level administrator support
- Add support for Lighthouse 5 user and group templates
- Add cellular firmware upgrade support for LMP products
- Improve serial port performance
- Improve OpenVPN routing when interface availability changes

Fixes

- Fix TACACS user authentication issue with some SSH clients
- Fix REST API reporting addresses for disabled interfaces
- Fix Wi-Fi using incorrect regulatory domain
- Fix SMS unavailability when cellular state controlled by Auto-Response
- Fix web terminal operation when IPv6 is disabled
- Fix cellular dashboard status display updates

4.2.0 (April 2018)

This is a production release.

Enhancements

- Add IPv6 syslog client support
- Add device country code for Wi-Fi regulatory band selection
- Add IPv6 support for cellular networks
- Add support for LMP cellular products
- Add support for IPv6 cellular per-interface default routes
- Add support for special chars in SNMP contact field
- Improve performance with many cascaded ports, UPS
- Improve status code uniformity in cellctl API
- Improve ZTP interaction with manual configuration

Fixes

- Fix cellular RAT wrongly reporting as unavailable via SNMP
- Fix detection of CP210x-based USB consoles
- Fix DTR “Always On” mode to follow pmshell signals
- Fix Huawei module cellular dashboard status display
- Fix IPv6 firewall dropping packets instead of sending reject

- Fix IPv6 route metric persistence
- Fix lost static routes during failover
- Fix memory leaks in cellular subsystem
- Fix SMS UTF-8 translation bug
- Fix UI duplicate address detection
- Fix issue with session ID

4.1.1u2 (May 2018) (IM42xx, ACM550x, ACM500x)

This is a production release.

Fixes

- Fix issue with session ID

3.16.6u5 (May 2018) (CM41xx)

This is a production release.

Fixes

- Fix issue with session ID

4.1.1u1 (February 2018)

This is a patch release.

Enhancements

- Improve system startup time (ACM500x)
- Improve UI to only allow valid failover configurations
- Improve flash memory error correction and recovery (ACM700x, CM7196)
- Improve SIM-to-SIM failover

Fixes

- Fix IP alias routing issue
- Fix APN persistence on some cellular modems (ACM550x, IM72xx)
- Fix APN settings change not always applied with auto SIM
- Fix DHCP address flapping when device under heavy load
- Fix LPK certificate check disable
- Fix rare IP Passthrough issue where outbound connections were blocked
- Fix dashboard widget showing unknown interface address
- Fix ethernet-ethernet failover restore issue

4.1.1 (December 2017)

This is a patch release.

NOTE

- This release does not include the IPv6 cellular changes from 4.0.1b0

Enhancements

- Add support for anonymous binds for LDAP public key SSH retrieval
- Add SIM slot auto-detection on dual-sim devices

- Add MTU settings for ethernet devices
- Add support for per-interface IPv6 default routes
- Add support hostname information to REST API
- Add support for APC AP8959 PDU new firmware
- Add support for APC 7900 PDU new firmware
- Add ZTP diagnostics
- Add support for Lighthouse 5.1.1 script templates
- Improve OpenVPN protocols used with Lighthouse 5, reduce sync traffic
- Improve per-interface route management
- Improve error message from power control utilities
- Upgrade dnsmasq to 2.78

Fixes

- Fix Wi-Fi KRACK vulnerability
- Fix bond and bridge link-down handling
- Fix management LAN configuration (ACM5504-5)
- Fix LDAP trusted certificate use
- Fix nrpe user permissions for environmental data
- Fix spurious 'no swap space' SNMP trap
- Fix ports permission issue for 'users' group
- Fix port forwarding routing issue
- Fix session timeout changes not being applied
- Fix firewall block breaking console login
- Fix argument limit with node-command
- Fix primary port used for SSH and telnet for serial port aliases

Known Issues

Opengear are aware of the following product-specific issues with this release:

- ACM500x/ACM550x-3G models: SIM auto-detect not reliable with some carriers
- MTU control not available on bonded interfaces
- Disabled accounts can login with LDAP public keys

4.1.0u3 (October 2017)

This is a patch release.

Fixes

- Fix Radio Access Technology selection update on 3G/GSM modems (ACM5xxx, IM42xx)

4.1.0u2 (September 2017)

This is a patch release.

Fixes

- Fix web terminal access to serial ports

4.1.0u1 (September 2017) (ACM550x)

This is a patch release.

Product

- Release for the ACM550x product family

4.1.0 (August 2017)

This is a production release.

Enhancements

- Add support for IPv6 address configuration from DHCPv6
- Add support for ZTP (Zero Touch Provisioning) over DHCPv6
- Add support for configurable cellular interface network masks
- Add CDK documentation
- Add support for SNMP ipSystemStatsOutFragOKs properties
- Add support for opt-in automated cellular modem firmware updates
- Add support for IPv6 aliases of serial port services
- Improve web terminal security
- Add support for accessing by Lighthouse with multiple addresses
- Add support for Lighthouse AAA templates
- Add support for Lighthouse Node Group templates
- Improve Lighthouse disconnection handling
- Improve Lighthouse CLI tools
- Modify Lighthouse VPN tunnel configuration

Fixes

- Fix NTP service after upgrade from factory settings
- Fix failing firmware upgrades when initiated over SSH without a tty
- Fix framed UI usage under Lighthouse
- Fix support for authorized access to logs on non-FAT storage
- Fix diagnostic interface issues with cellular modem control tool
- Fix issue with LTE cellular modem drivers in CDK builds
- Fix gateway discovery with some cellular networks
- Fix unresponsive UI after running template wizard
- Fix power supply sensor access (psmon) in IM72xx-DDC models
- Fix quietened console diagnostic output during firmware upgrade
- Fix Lighthouse enrollment issue with cascaded ports
- Fix issue with Lighthouse authorized keys API
- Fix config saves blocking when a Lighthouse tunnel is down
- Fix Lighthouse bundle identifier being lost after enrollment completes

Other

- Remove unused rssh tool

4.0.0u1 (July 2017)

This is a patch release.

Enhancements

- Add support for USB port power control from CLI
- Improvements to CP210x USB serial driver

Fixes

- Fix Cisco USB console speed change issue

- Fix network interface reset issue during reconfiguration
- Fix IP passthrough padding issue with older Cisco devices
- Fix multi-homed routing issue when NAT forwarding is in use

4.0.1b0 (July 2017)

This is a patch release.

Enhancements

- Add support for IPv6 cellular connections
- Add support for automated cellular modem firmware updates
- Add support for USB port power control from CLI
- Add support for Cisco ASR USB consoles
- Improve cellular and system stability after cellular firmware upgrade

Fixes

- Fix SNMP routing issue
- Fix Cisco USB console speed change issue
- Fix network interface reset issue during reconfiguration
- Fix NTP service after upgrade from factory settings
- Fix session checking during use of web terminal service
- Fix CDK documentation

Other

- Remove unused rssh tool

4.0.0 (April 2017)

This is a production release.

Enhancements

- Add REST API for managing configuration from Lighthouse 5.0
- Add Lighthouse 5.0 support for ZTP and USB enrollment
- Add SNMP events and autoresponse support for CLI session logins
- Add support for APC AP7998 24-port PDU
- Add USB console information to customer support report
- Add support for USB consoles that look like modems
- Add support for Microchip-based USB consoles
- Add support for longer DHCP options
- Add sudo access to users with admin role
- Add more information shown for Sierra CDMA modems
- Add USB information displayed by pmstats tool
- Add netflash error reporting
- Add web UI text for DHCP configuration
- Add logging of malformed DHCP messages with ZTP

Fixes

- Fix hardware clock drift issues (ACM700x, CM71xx)
- Fix cases where the hardware clock wasn’t always being initialized
- Fix SMS reliability issues
- Fix OpenVPN network configuration issue with static keys

- Fix OpenVPN deadlock issue with filesystem driver
- Fix autonegotiation on ethernet interfaces (IM72xx)
- Fix asymmetric UDP SNMP replies
- Fix sending unnecessary SNMP traps
- Fix sshd concurrent connection limit to 100
- Fix rare bug where Apply button would have no effect
- Fix backslash handling in callhome passwords
- Fix LED/GPIO issues during boot (ACM7xxx)

3.16.6u4 (March 2017)

This is a patch release.

Enhancements

- Add extra HTTP header to help defend against clickjacking
- Add connection state matching options to firewall rules (new vs. established/related)
- (ACM700x, ACM7004-5, CM71xx, IM72xx, CM7196A only) Add support for CDP alongside LLDP
- Add support for semi-colon characters in SNMP 'Location' field
- Add 'diff' command to CM7196 devices, to fix display issue with RPC Connections page
- Add extra configuration options for Brute Force Protection (ban lifetime, login attempts before trigger)
- Update timezone data to most recent, to fix Turkey timezone

Fixes

- Fix potential buffer overflow in SSH
- Fix corner cases of utmp filling up tmp and preventing web login
- Fix issue with RTC not setting time properly on boot for some devices
- Fix issue with incorrect detection of internal v92 modems on some ACM700x devices
- Fix issue with detection of cellular MCC and MNC information
- Fix issue with ports above 49 not being accessible via some network protocols on CM7196 devices
- Fix issues with SNMP v3 traps using automatically generated engine IDs
- Fix issue using serial cascading with remote authentication
- Fix issue with roaming cellular data connections reconnecting automatically after a reboot
- Fix issue with ethernet connection link speed when not using autonegotiation
- Fix potential netflash failure when running netflash without a console (eg. ZTP)
- Fix local config backup to work with ACM700x devices

3.16.6u3 (January 2017) (ACM700x, CM71xx, IM72xx)

This is a patch release.

Enhancements

- We no longer bring up the 192.168.0.1 default static address if it's already in use elsewhere on the network

3.16.6u2 (December 2016) (ACM700x)

This is a patch release.

Features

- ACM700x: Add support for SFP interfaces
- ACM700x: Add support for internal v92 modems
- ACM700x: Add support for internal temperature sensors

3.16.6u1 (November 2016) (Console Servers)

This is a patch release.

Fixes

- Fix CVE-2016-5195 (dirtyc0w)
- Fix issue where root user was unable to log into UI
- Fix config restore process breaking existing AAA users
- Fix issue where CM41xx was not keeping date and time across reboots
- Fix Huawei modem control software memory leak

3.16.6 (October 2016) (Console Servers)

This is a patch release.

Enhancements

- Add ability to set more fine-grained permissions for remote users
- Add support for monitoring power supply status via SNMP
- Display dormant interface status in Dashboard connection summary
- Add device firmware upgrade via ZTP
- Update timezone information
- Reduced memory usage for ACM500x
- Allow disabling of accounting in RADIUS and TACACS+ configuration
- Add support for obfuscation of AAA authentication passwords in device configuration file
- Add support for ACM700x with internal modem
- Add support for CM7196A console server
- Modified mount options for USB drives to improve I/O performance
- Support asserting DTR on serially-connected device during pmshell session
- (ACM700x, ACM7004-5, CM71xx, IM72xx, CM7196A only) Report interface name as LLDP port ID
- Add user programmable carrier support for IM72xx devices
- Update OpenSSL to version 1.0.1u
- Handle empty/missing SNMP values in ogPowerSupplyTable

Fixes

- Fix pmshell group not taking precendence over admin group for shell choice
- Fix USB port labels on ACM7004-5
- Fix custom firewall scripts not run on reboot
- Fix Huawei modem disconnecting session
- Fix single SMS being received twice on Huawei modems
- Fix microSD cards not being mounted automatically (IM72xx)
- Fix SNMP for PM3000 single-bank PDU
- Fix inaccessible webshell ports on cascaded devices
- Fix config erase button on IM72xx
- Fix USB storage occasionally not mounted on IM72xx
- Fix internal modem not displayed in UI for ACM5003-M
- Fix memory leaks in cellctl
- Fix cellctl not cleaning up socket files properly on exit

- Fix remote AAA users being unable to run ssh

3.16.5u1 (July 2016) (IM42xx, CM41xx, ACM550x, ACM500x)

This is a patch release.

Fixes

- Fix intermittent boot issues with high port count devices

3.16.5 (July 12 2016) (Console Servers)

This is a patch release.

NOTE

- As of console server firmware 3.16.5 for acm700x, acm7004-5, cm71xx and im72xx, each USB console port is allocated a fixed port number following the RS-232 serial ports. This replaces the previous behaviour of dynamically allocating port numbers to USB consoles, as they were attached. This may affect existing cascading, NMEA and USB console configurations, which may need to be reconfigured after upgrading to use the new port numbering scheme.

Enhancements

- Add USB console support
- (ACM700x, ACM7004-5, CM71xx, IM72xx, CM7196A only) Add support for LLDP
- Add IE11/Edge support for WebShell
- Add warning to UI about port logging capturing passwords
- Add ability to set APN on Verizon cellular devices
- Add support for Liebert Network Attached PDUs
- Improve cellular stability

Fixes

- Fix validation of user-supplied SSL certificates
- Fix interface for editing multiple serial ports
- Fix garbage characters when editing XML config
- Fix erroneous temperature readings on internal temperature sensor (ACM550x)
- Fix problem with IP Passthrough service intercepts with default gateway configured
- Fix portmanager errors to be more descriptive
- Fix rare firmware upgrade failure happening under certain conditions
- Fix resubmit dialog loop on Microsoft Edge
- Fix environmental status information in SNMP when no values available
- Fix issue with losing dial connection settings after carrier change
- Fix issue with cellular APNs that require username and password
- Fix modem watchdog interaction with dual sim failover and autoresponse
- Fix possible race condition during SIM select
- Fix UI ethernet media selection to add gigabit option
- Fix cellular firmware update sometimes deleting firmware files
- Fix issue with connection manager not terminating some ‘start’ commands properly
- Fix SIM unlocking in UI
- Fixed issue where inaccessible ports were visible to unprivileged users on Port Logs page
- Fix setting cellular authentication method
- Fix SNMPv3 username not allowing hyphen or underscore characters

- Fix spurious SNMP syslog message
- Fix issue persisting Radio Access Technology setting from UI
- Fix issue with changing carrier to currently selected carrier
- Fix issue polling CDMA modem stats while modem is resetting
- Fix error when connecting on 2G cellular network
- Fix issue with ethernet speed negotiation on CM71xx
- Fix issue starting NTP with DHCP network interface and NTP server by IP
- Fix issue using unauth SSH direct to serial port 30
- Fix issue with external USB v92 modems not appearing in UI
- Fix issue with network dashboard widget information for bridged/bonded connections
- Fix issue with ethernet link when forced to 10Mbps (CM71xx)
- Fix issue with on-device ssh client remote host key verification for non-root users
- Fix output of command line 'pmstats' command
- Fix issue running 'setfset' and 'showserial' commands as non-root admin user
- Fix issue with traffic counter accuracy on outgoing traffic for cell modems
- Fix issue with reliability of cell modem enumeration after modem reset
- Fix issue where changing SNMP community string would not automatically restart SNMP service
- Fix spurious error when running support report generator on devices without modem

3.16.4u6 (May 2016) (IM72xx, IM42xx, ACM500x, ACM550x, ACM700x, ACM7004-5)

This is a patch release.

Enhancements

- Improve cellular stability
- Add support for ZTP via custom bash script

3.16.4u5 (May 2016) (ACM700x, ACM7004-5, IM72xx)

This is a patch release.

Enhancements

- Improve cellular stability

3.16.4u4 (April 2016) (IM72xx)

This is a production release.

Enhancements

- Improve cellular stability

4.5.6 (March 2016) (Lighthouse)

This is a production release.

Enhancements

- Upgrade OpenSSL to version 1.0.1p
- Update default TLS cipher list to Mozilla Intermediate Compatibility recommended settings

Fixes

- Fix SDTConnector to support newer SSH clients and SSL requirements
- Fix DDNS not working
- Fix selective sync via UI and via node-sync always contacting all nodes
- Fix node enrollment when networking is in a factory default state
- Disable monitor managed devices by default when enrolling nodes
- Fix various issues in the support report

3.16.4u2 (March 2016) (Console Servers)

This is a patch release.

Enhancements

- Add support for the ACM7004-5
- Add MD5 ssh key fingerprints to support reports

Fixes

- ACM700x: Fix signal status intermittently showing incorrect values
- ACM700x: Fix temperature sensor display in the UI
- ACM700x: Fix incorrect IO port order in the UI
- CM71xx: Fix missing product definition in SNMP MIB
- Fix dual-sim failover not always working on dual-sim cellular models
- Fix NFS unmounting of remote shares not working
- Fix SNMPv3 usernames incorrectly not allowing numbers
- Fix ssh direct to serial ports failing on high number serial ports
- Fix duplicate fields on CDMA settings page
- Fix cellular PAP settings not persisting
- Other security fixes

3.16.4u1 (February 2016) (IM72xx)

This is a patch release.

Fixes

- Fix issue with XHCI Controller Detection

3.16.4 (January 2016) (Console Servers)

This is a patch release.

Enhancements

- Upgrade OpenSSH to version 7.1p2
- Upgrade OpenSSL to version 1.0.1p
- Update default TLS cipher list to Mozilla Intermediate Compatibility recommended settings
- Add support for new Servertech PRO UPS MIB
- Add support for retrieving SSH public keys over LDAP (SSH LPK)
- Add TCP SYN traceroute support (via the -T option)
- Add unauthenticated SSH and telnet services for serial port IP aliases

Fixes

- ACM700x: Fix “No buffer space available” error messages
- ACM5508: Fix serial flow control not working on top four ports
- CM71xx: Fix internal SD storage not being used for TFTP and FTP services
- Fix incorrect version string appearing in CDK builds
- Fix Some SNMPv3 username lengths causing authentication to fail
- Fix IP Pass Through mode not overlooking existing DHCP setup
- Fix SNMP EMD DIO values not updating
- Fix incorrect date being presented on modem firmware update page
- Fix adding extra white space in text fields could break firewall
- Fix ALLMULTI not being disabled when turning off IPv6
- Fix cases where a 4G cellmodem would sometimes fail to get an IP address
- Fix cases where cellular signal strength LEDs wouldn’t be updated
- Fix misreporting of cellular roaming when not roaming
- Fix broken HTML on -GV model Internal Cellular Modem page
- Fix spurious “SIM Not Present” error
- Fix IMSI/ICCID retrieval not working on some gobi modems
- Fix missing cellular carrier information field under Cellular Statistics UI
- Fix issues where cellular modem wouldn’t be detected
- Fix spurious AT$DEBUG commands being sent to cellmodems and appearing in logs
- Fix cell-fw-update using incorrect field for firmware version
- Fix cases where /var would reach 100% used
- Fix pmpower pmchat scripts not working for admin users
- Fix switching between primary and secondary SNMP manager tabs in UI not working
- Fix enabling bridge mode does not bring up the br0 interface
- Fix spelling errors in UI

3.16.2u1 (22 December 2015) (Console Servers)

This is a patch release.

Enhancements

- Add support for the ACM700x-2-LMC
- Add warning on firmware upgrade to remind users to check release notes

Fixes

- Fix regression of cellular robustness on LTE modems
- Fix issue with /var filling up on some product families
- Fix device firmware version checking on cell firmware update
- Fix intermittent issue with some internal POTS modems not answering calls in time

3.16.2 (9 November 2015) (Console Servers)

This is a production release.

Enhancements

- Add support for the ACM700x-LMx
- Add support for the ACM7008
- Add multi-carrier cellular module support
- Add support for upgrading cellular module firmware where possible
- Add ServerTech multibank and multitower PDU outlet support
- Add unauthenticated SSH as an optional service
- Add SFTP support

- Improve cellular modem robustness on ACM700x products

Fixes

- Fix version information on CDK builds
- Fix spurious SNMP restart traps (NOTE: this may cause some restart traps to be missed)
- Fix inconsistencies with authentication when using KerberosDownLocal or LDAPDownLocal
- Fix IP Passthrough link instability when upstream DHCP lease renews
- Fix SMS reception on ACM7004-LV
- Fix ZTP not working when the DHCP server is also distributing NTP server information
- Fix OpenVPN tun-mode server with static keys not starting correctly
- Fix configured RADIUS accounting port number not being used correctly
- Fix spurious log messages when using ServerTech serial PDUs
- Fix IPMI power status reporting
- Fix accumulation period causing pmshell to not work
- Fix who and w commands not returning any information (also removed 'last' command)
- Fix Failover & Out-of-Band page not reporting cellular connection status correctly
- Fix internal modem not working on IM42xx products (broken in 3.16.1b0)
- Fix tftpboot directory on usb storage sometimes receiving incorrect permissions
- Fix incorrect error message when importing configuration files fail

4.5.5u1 (3 September 2015) (Lighthouse)

This is a production release.

Enhancements

- Add support for new Lighthouse Enterprise HW Appliance (Dell R430)

Fixes

- Fix CVE-2015-5600 (openSSH brute force using keyboard-interactive)
- Fix permissions/access issues found via the web interface

3.16.1b0 (27 August 2015) (Console Servers)

This is a production release.

Enhancements

- Add bgpd to IM7200 images
- Add info for custom OpenVPN tunnels with additional commands required

Fixes

- Fix CVE-2015-5600 (openSSH brute force using keyboard-interactive)
- Fix config corruption issues with concurrent config CLI commands
- Fix dialback on IM7200
- Fix permissions/access issues found via the web interface
- Fix web interface session ID length
- Fix per-serial port IP aliases in network bonding mode
- Fix FTP firewall issues in PASV mode
- Fix multiple hotplug processes causing memory problems
- Fix missing or renumbered ttyUSB devices
- Fix ACM700x hostname not being set correctly on first boot

- Fix modem crash when signal strength reported as “NOSERVICE”
- Fix OpenVPN not starting correctly in specific scenarios

3.15.3 (7 August 2015) (ACM500x)

This is a patch release.

Enhancements

- Add LTE modem support for ACM500x products
- Add watchdog for CDMA modems

Fixes

- Fix devlog crash when sending hangup signal
- Fix URB handling in GobiNet driver

3.15.2u1 (31 July 2015) (ACM550x)

This is a patch release.

Fixes

- Fix reliability issues on ACM550x

3.16.0 (21 July 2015) (ACM700x)

This is a production release.

Enhancements

- Add support for the ACM700x products
- Add IPv6 support to the LDAP client
- Add IPv6 support to the RADIUS client
- Add additional support for editing APN where allowed
- Add support to ftpd to no longer need /bin/ls inside the server directory

Fixes

- Fix bug where local backups with the same name as an existing backup silently failed
- Fix issue with IP aliases not reliably starting
- Fix utmp filling up tmp and preventing web login
- Fix LTE not connecting when APN is correctly left empty
- Fix issues with sending large SMS messages
- Fix spurious log messages when sending SMS messages
- Fix CDMA SMS sending sometimes causing cellmodem error log messages
- Fix spurious log message “invalid conn”ippassthrough””
- Fix pmshell crash when changing between ports with RPC connections
- Fix issue with repeated pings failing with “No buffer space available”
- Fix rare network related crash on CM71xx and ACM700x products
- Fix spurious cellctl error log messages when cell modem is disabled
- Fix repeated “syslogd: started” messages on boot when using remote syslog

3.15.2 (4 May 2015) (Console Servers)

This is a production release.

Enhancements

- Add IPv6 support in firewall rules
- Add IPv6 support to the TACACS client
- Add IPv6 information to the support report generation
- Add informational message to warn about cell data usage charges
- Add informational message to warn about adding “block all” firewall rules
- Add ability to force netmask value when using cellular IP Passthrough
- Update OpenSSL to 0.9.8zf to mitigate CVEs.

Fixes

- Fix weak ciphers used in OpenVPN (FREAK vulnerability)
- Fix issue with dialout default route not being added when IP is renewed
- Fix issue with IO ports page being displayed on models without IO ports
- Fix issue with dialpool dialin connections not succeeding when local LAN disconnected
- Fix issue when malformed username login attempts would not be logged correctly
- Fix display issue with CDMA modem option checkboxes on initial page load
- Fix issue with OpenVPN event Autoresponses not reliably triggering
- Fix issue with RPC monitoring not reliabliy polling load information
- Fix issue with retrieving RPC status for dual APC7900 devices
- Fix issue with DDNS updates being run before being able to route to the services
- Fix log messages with CDMA SMS usage to help diagnosis and troubleshooting
- Fix issue where non-dormant ethernet interfaces would always behave dormant
- Fix issue with some SNMP UPS updates intermittently not working
- Fix issue where MC5728V modules may error if receiving SMSs larger than 160 characters

4.5.5 (4 May 2015) (Lighthouse)

This is a production release.

Enhancements

- Update OpenSSL to 0.9.8zf to mitigate CVEs.

Fixes

- Fix weak ciphers used in OpenVPN (FREAK vulnerability)
- Fix issue with node-upgrade command with newer firmware version strings
- Fix issue with dialpool connections not succeeding when remote LAN disconnected

3.11.4 (March 11 2015) (CMS61xx, VCMS)

This is a production release.

Fixes

- Fix glibc GHOST vulnerability: CVE-2015-0235

3.9.4 (March 11 2015) (KCS61xx)

This is a patch release.

Fixes

- Fix glibc GHOST vulnerability: CVE-2015-0235

3.15.1 (February 24 2015) (Console Servers)

This is a production release.

Enhancements

- Add ability to automatically provision unconfigured devices using DHCP (ZTP)
- Add support to TACACS+ authentication to provide the remote address of authentication attempts

Fixes

- Fix OpenSSH timing leak vulnerability: CVE-2006-5229
- Fix readability issue with cellctl error codes: errors now have human-readable descriptions
- Fix issue where configuration changes after RPC probing would not be detected
- Fix issue where some SNMP UPS devices would heavily utilize CPU unnecessarily
- Fix issue where status information for external EMD devices would not be provided via SNMP
- Fix issue where SNMP daemon config file may not be generated correctly when SNMP configuration changes
- Fix issue with NUT scanner utility crashing
- Fix error message being produced by cellular watchdog script
- Fix issue where NRPE on console servers would not allow command line arguments
- Fix issue where probing remote UPS/RPC devices on managed devices would not be indexed correctly
- Fix issue where SIM failover on LTE devices with dual SIM capability was not reliable
- Fix issue where custom routes over dial/cellular interfaces would not be added correctly
- Fix issue where removing specific custom routes from the interface would not always work correctly
- Fix issue where the internal temperature monitor on some ACM devices would not read correctly
- Fix issue where LTE cell data usage monitoring may sometimes report inaccurate values
- Fix issue where a bonded ethernet device would not use a consistent MAC address
- Fix issue where ethernet link detection would produce spurious log messages on ACM550x devices
- Fix issue using the power menu on a serial port when accessing a console server via Lighthouse

4.5.4 (February 24 2015) (Lighthouse)

This is a patch release.

Fixes

- Fix glibc GHOST vulnerability: CVE-2015-0235
- Fix issue where connection status LEDs may not show the correct status for call-home console servers

4.5.3 (January 14 2015) (Lighthouse)

This is a production release.

Enhancements

- Add display into “Access Managed Devices” page to show useful information at a glance

(connection status & dial status)

Fixes

- Fix issue where a 'retrieve managed hosts' operation would not fail completely if any individual host was not contactable
- Fixed XSS sanitization in JSON data for device attributes page
- Fix dialpool timeout when the remote console server has network connection disconnected.

3.15.0 (January 13 2015) (Console Servers)

This is a patch release.

Enhancements

- Add post-configurator hook for custom firewall rules

Fixes

- Fix NTP vulnerabilities: CVE-2014-(9293,9294,9295,9296), CVE-2009-0021
- Fix issue with dashboard display width on small monitors/browsers
- Fix issue where SMS messages could stop sending on dual-SIM devices after failover
- Fix support report display of per-interface route tables to be more readable
- Fix support report display of netstat information (network connections)
- Fix support report display of infod dump information
- Fix support report display of USB bus information
- Fix issue where cell modem RSSI could sometimes be reported incorrectly as -1
- Fix the display of data on the ICMP statistics page
- Fix minor display consistency issues on the SNMP configuration page
- Fix spurious warning message when rebooting from the command line
- Fix issue when restoring a local config backup after erase
- Fix issue where wireless configuration may not be applied in some cases until rebooted
- Fix issue with firewall rules or per-interface routing tracking PPTP connections
- Fix issue where firewall log messages would contain spurious text
- Fix issue with spurious log messages about the "route" configurator
- Fix issue with IPsec not consistently/reliably starting on boot
- Fix issue with IPsec routing interoperation with per-interface default routes

3.15.0b0 (December 18 2014) (Console Servers)

This is a production release.

Enhancements

- Add cellular IP Passthrough feature, to 'half-bridge' between a cell modem and downstream router/device
- Add the system name to the title bar of web pages in the UI

Fixes

- Fix issue where cell data usage autoresponse would not trigger on -LA devices
- Fix issue when using RPCs on X1 serial pinout mode
- Fix issue where CDMA cell modems may be reported up even without a service
- Fix issue where some UI web pages may not display correctly after reconfiguring 'Services'
- Fix issue where some log messages may not expand variables correctly

- Fix issue where an MC5728V cell modem may not be detected correctly on boot
- Fix issue where LDAP authentication could not be configured with an empty password (for anonymous bind)
- Fix issue with CDMA modems not setting some per-interface routes correctly
- Fix issue where per-interface default routes may not be added for aliases on different networks
- Fix issue where a cell modem watchdog would not trigger when in non-dormant failover mode
- Fix issue where POTS modems may not get caller ID details if answered too quickly
- Fix issue with failover probe addresses: if multiple addresses are used, an interface would fail over if any address is down, rather than all addresses
- Fix issue with querying SNMP EMD details on ACM devices without humidity sensors

3.14.2 (December 8 2014) (CM71xx)

3.12.3 (December 8 2014) (Console Servers)

This is a patch release.

Fixes

- Fix issue with per-interface routing tables: network routes were not always added; some networks could become uncontactable if the network gateway was not contactable

3.14.1 (November 24 2014) (CM71xx)

This is a production release.

Enhancements

- Add support for default routes on multiple interfaces
- Add option to download the support report

Fixes

- Fix UI issue where it was possible to specify a port number on non-TCP/UDP firewall rules
- Fix missing data from command line generated support reports
- Fix issue with phone numbers containing non alphanumeric characters
- Fix issue where custom OpenVPN configuration files could be deleted if stored with internal files
- Fix CVE-2014-7186 and CVE-2014-7187 vulnerabilities in bash
- Fix issue with refreshing the managed devices page (no longer resends any previous commands)
- Fix issued where missing internal sensor data no longer prevents creation of new auto-responses
- Fix issue where failed IPsec connections would not come back up
- Fix issue where custom serial port escapes weren't being saved
- Fix display bug for SNMP devices in power menu
- Fix issue where incomplete auth configuration could prevent logins
- Fix issues with deleting VPN tunnels
- Fix MOTD display in System configuration page
- Fix Web Session Timeout
- Fix timing issue with connection failover
- Fix issue where route information could be lost on upgrade
- Fix issue where syslogd wouldn't restart after failure

- Fix issue with syslog not using updated hostnames
- Fix issue where backups from incompatible firmware could be restored
- Fix issue where multiple ping autoresponse checks could cause excessive cpu usage
- Fix where ogHostPingNotification SNMP traps not always being sent

3.12.2 (November 24 2014) (Console Servers)

This is a patch release.

Enhancements

- Add support for default routes on multiple interfaces (Note: this may interfere with custom scripted routing setups)
- Add option to download the support report
- Add mkdosfs utility to IM4200 firmware

Fixes

- Fix issue with custom APN on -LA models
- Fix UI issue where it was possible to specify a port number on non-TCP/UDP firewall rules
- Fix missing data from command line generated support reports
- Fix issue with phone numbers containing non alphanumeric characters
- Fix issue where custom OpenVPN configuration files could be deleted if stored with internal files
- Fix issue where devices with GPS would misreport their model number
- Fix CVE-2014-7186 and CVE-2014-7187 vulnerabilities in bash
- Fix issue with refreshing the managed devices page (no longer resends any previous commands)
- Fix issued where missing internal sensor data no longer prevents creation of new auto-responses
- Fix issue where failed IPsec connections would not come back up
- Fix issue where custom serial port escapes weren't being saved
- Fix flow control problems with the top four ports of ACM5508
- Fix ACM550x instability issues when cell antenna is unplugged
- Fix issue with multiple APC7900 RPCs
- Fix cleanup of outgoing SMS queue
- Fix display bug for SNMP devices in power menu
- Fix issue where incomplete auth configuration could prevent logins
- Fix issues with deleting VPN tunnels
- Fix MOTD display in System configuration page
- Fix Web Session Timeout
- Fix timing issue with connection failover
- Fix issue where route information could be lost on upgrade
- Fix issue with editing Send SMS trigger actions
- Fix issue where syslogd wouldn't restart after failure
- Fix issue with syslog not using updated hostnames
- Fix issue where outgoing cellmodem dialup connections were not using the provided username/password
- Fix issue where backups from incompatible firmware could be restored
- Fix issue where multiple ping autoresponse checks could cause excessive cpu usage
- Fix where ogHostPingNotification SNMP traps not always being sent

3.12.1 (September 26 2014) (Console Servers)

This is a production release.

Fixes

- Fix CVE-2014-6271 and CVE-2014-7168 vulnerabilities in bash
- Fix issue with display of Managed Devices with non admin users

4.5.2 (September 26 2014) (Lighthouse)

This is a production release.

Fixes

- Fix CVE-2014-6271 and CVE-2014-7168 vulnerabilities in bash

3.11.3 (September 26 2014) (VCMS/CMS)

This is a production release.

Fixes

- Fix CVE-2014-6271 and CVE-2014-7168 vulnerabilities in bash

3.9.3 (September 26 2014) (SD4002/SD4001,IM4004-5, KCS61xx)

This is a production release.

Fixes

- Fix CVE-2014-6271 and CVE-2014-7168 vulnerabilities in bash

3.8.3 (September 26 2014) (CM4001/CM4008, SD4008)

This is a patch release.

Fixes

- Fix CVE-2014-6271 and CVE-2014-7168 vulnerabilities in bash

3.12.0 (September 25 2014) (Console Servers)

This is a production release.

Enhancements

- Added Serial pinout display to Serial page on IM72xx devices
- Added Cellular Modem details to SNMP
- Added Connection Manager and Cellular Dashboard widgets to the Dashboard
- Added Brute force protection (Fail2Ban) for WebUI and SSH
- Major redesign of the Manage page
- Improved the Serial Config UI pagination
- Added per serial port IP alias support
- Added the ability to download port logs as files
- Added better RPC status on the RPC and manage pages
- Added Raritan PX SNMP support
- Added support for disabling serial ports
- Added shortcut icons for the Dashboard and Manage pages

Fixes

- Fixed SMS sending by admin users using the CLI
- Fixed issue with some powerman devices not reporting temperature
- Fixed consistency issues with UI labels and display names
- Fixed CDK issue with LTE drivers not being included
- Fixed IM72xx slow boot issues
- Fixed ACM5508-2M internal modem reset issue
- Fixed incorrect TCP and UDP stats on the statistics page
- Fixed Memory leak in portmanager
- Fixed OpenVPN secret file permissions
- Fixed sendsms issue with multiple invocations
- Fixed OpenVPN custom port UI display issue
- Fixed SNMPv3 username validation
- Fixed address corruption in SNMP traps for IPv6 WebUI logins
- Fixed issue with WebUI not handling some characters in form variables
- Fixed issue with CLI config command crashing when printing errors

4.5.1 (July 24 2014) (Lighthouse)

This is a production release.

Fixes

- Fixed issue with ‘node-upgrade’ printing an incorrect error message if the node is unreachable
- Fixed issue where ‘node-upgrade’ commands can cause console servers without internal storage to fill up /var
- Fixed issue where bulk node commands were not correctly checking permissions in all cases
- Fixed issue where host routes would not be reported as ‘installed’ in the GUI when they are

3.11.1 (July 16 2014) (Console Servers)

This is a production release.

Enhancements

- Added ability to add network routes through a specific interface.

Fixes

- Fixed issue with ACM5004-GV: reliability of detecting USB cell modem on boot.
- Fixed stability issue with IM42xx devices when a cellmodem is in use and ethernet interfaces are flapping.
- Fixed issue with IM72xx devices using fibre WAN connections potentially not getting a DHCP address.
- Fixed issue with dos2unix binary setting file mode permission bits to 600.
- Fixed issue with provisioning wizard script not allowing some special characters in initial password.
- Fixed issue with call-home passwords that contain spaces.
- Fixed issue when using bulk node-update command to upgrade IM42xx devices.

3.9.2 (July 16 2014) (IM4004, SD4002, KCS61xx)

This is a production release.

Enhancements

- Updated OpenSSL to 0.9.8za to mitigate CVE-2014-0224.

3.8.2 (July 16 2014) (CM4001, CM4008, SD4008)

This is a production release.

Enhancements

- Updated OpenSSL to 0.9.8za to mitigate CVE-2014-0224.

4.5.0 (June 25 2014) (Lighthouse)

This is a production release.

Features

- Lighthouse now has support to broadcast commands to managed devices (from the CLI) and report the results.
- Lighthouse now has support to add, remove and modify user accounts on managed devices in bulk (from the CLI).
- Lighthouse now has support to update firmware on managed devices in bulk (from the CLI).
- Lighthouse bulk commands support selection of managed devices by attribute.
- Lighthouse now has support for dual NICs.

3.11.0 (June 25 2014) (Console Servers & (V)CMS)

This is a production release.

Enhancements

- Major overhaul of SNMP status reporting; addition of new MIB (OG-STATUSv2-MIB) with extra details.
- Major overhaul of SNMP traps; addition of new MIB (OGTRAPv2-MIB), with extra traps.
- Added support for authentication against OpenLDAP servers (ie. using POSIX account schemas).
- Improved LDAP over SSL support (better certificate handling, protocol selection, ignoring signing errors).
- Added support for SMS triggered autoresponses from multiple phone numbers.
- Added ability to disconnect serial sessions from the web interface or CLI per port, per user, or a combination of both.
- Added RPC support for WTI VMR-HD4D32.
- Added RPC support for APC 7900 v3.7.3 AOS v3.7.3.
- Added RPC support for APC 8959 v5.1.6 AOS v5.1.9.
- Added RPC support for Raritan PX via SNMP.
- Added RPC support for TrippLite PDUs with PowerAlert v12.06.0061.
- Added ability to specify facility and severity of outgoing remote syslog (via CLI config only).
- Added support for custom CTRL keystrokes for pmshell commands (via CLI config only).
- Added ability for users on ‘unauthenticated telnet’ serial ports to use the power menu.
- Added ability to turn off LDAP referrals when using LDAP authentication.
- Added ability to ignore privilege levels of TACACS authenticated users.
- Added serial number information the support report if available.

- Improved local backup description/filename field to allow spaces.
- Updated OpenSSL to 0.9.8za to mitigate CVE-2014-0224.

Fixes

- Fixed memory leaks in the SNMP daemon.
- Fixed issue with IM72xx probing servertech outlets (via NUT).
- Fixed issue with IM72xx spurious interrupt kernel warning on boot.
- Fixed issue where the environmental page may unnecessarily restart the SNMP service.
- Fixed issue with serial pattern matching where slow input data would not trigger a match.
- Fixed issue where adding a port forward would add extra spaces and newlines to the config file.
- Fixed issue where some wireless configuration changes (eg. password) would not restart the connection.
- Fixed issue where aliases on network interfaces would not have correct IDs or stop correctly.
- Fixed issue where DIO autoresponse checks would not trigger correctly if configured as “trigger on change”.
- Fixed issue where serial signal autoresponse checks would not trigger correctly if configured as “trigger on change”.
- Fixed issue where the IM72xx would not work with an EMD in X1 or X2 serial pinout configuration.
- Fixed issue where OpenVPN tunnel netmask configurations were not being applied correctly.
- Fixed issue where an RPC managed with powerman would not have status info interpreted correctly.
- Fixed issue where the web server would not listen on the alternate HTTP port if specified.
- Fixed issue where IP aliases field in web interface was not long enough to enter a large number of IPs.
- Fixed issue where RADIUS accounting messages may be sent to the wrong server if multiple are configured.
- Fixed issue where deconfiguring a network bridge could cause interfaces to stop responding.
- Fixed issue with RPC daemon stability.
- Fixed issue where autoresponse daemon could start in a bad state on system boot.
- Fixed issue where cell data autoresponse event was not running actions and/or restarting daemon.
- Fixed issue where CM devices could sometimes reset to default IP addresses.
- Fixed issue where Nagios NRPE configuration could break IPv6 firewall rules.
- Fixed issue where ethernet failover targets would not get tests applied correctly or be in failover groups.
- Fixed issue where RPC daemon would not restart/re-read configuration after multiple devices are added.

4.4.2 (April 22 2014) (Lighthouse)

This is a production release.

Fixes

- Fix issue with ssh:// and tcp:// URLs generated in the management console

3.10.1 (April 7 2014) (Console Servers & (V)CMS)

This is a patch release.

NOTE

- As of console server firmware 3.10.0, we have replaced the majority of the onboard networking scripts with a single, dependency-based connection management daemon called ‘conman’. If you have set up custom networking scripts, they are highly likely to be INCOMPATIBLE and NOT WORK in firmware versions 3.10.0 and higher. It is recommended that upgrades be performed in a test environment before being rolled out to production sites.

Fixes

- Fix Wi-fi WEP passwords being unintentionally changed by the UI
- Fix smsd restarting too much when failing over between SIM cards
- Fix smsd not being able to be disabled
- Fix CDMA modem failover
- Fix IP Addresses not being masqueraded correctly on Verizon LTE connections
- Fix RPCD locking issue
- Fix Pantech UML290 repeatedly receiving the latest SMS
- Fix Servertech PDU Multibank UI Issues
- Fix dialout modem Interface Actions
- Fix Raritan PX2 definition error
- Fix LTE connection stability issues
- Fix Interface Event Ethernet support
- Fix Auto-Response ping check interface selection
- Fix dormant failover settings for non-conman devices
- Fix RPCD CPU Utilisation

3.10.0 (February 24 2014) (Console Servers)

This is a production release.

NOTE

- As of console server firmware 3.10.0, we have replaced the majority of the onboard networking scripts with a single, dependency-based connection management daemon called ‘conman’. If you have set up custom networking scripts, they are highly likely to be INCOMPATIBLE and NOT WORK in firmware versions 3.10.0 and higher. It is recommended that upgrades be performed in a test environment before being rolled out to production sites.

Enhancements

- In unconfigured IP settings, eth0:0 is now the static 192.168.0.1 interface and eth0 is the DHCP client interface
- Migrate networking code to new dependency based daemon, conman
- Improve the speed of an initial bootup after factory erase
- Add support for triggering VPNs from auto-responses
- Add RPC support for Raritan PX2 PDUs
- Add a bash .profile for root user
- Add more conman and network interface information to support reports
- Add cli8895 tool to interrogate internal switch on ACM5504-5 products

Fixes

- Fix RPC status page
- Fix issue with migration to Cherokee webserver
- Fix Servertech Single Bank support
- Fix serial signal auto-responses not triggering
- Fix Servertech “No such power device” error
- Fix RPC support crashing if /etc/config/powerstrips.xml is present
- Fix RPC support sometimes not unlocking serial ports
- Fix adding firewall rules adding extra spaces and unclosed tags to config file
- Fix SNMP notification for SMS checks
- Fix soft-reboot not repowering internal switch on ACM5504-5
- Fix internal powersupply monitoring support
- Fix failover on CDMA cell modems
- Fix override DNS settings not working on CDMA modems
- Fix callback not working after moving dial to conman infrastructure
- Fix pantect uml290 modems repeatedly receiving latest sms
- Fix unauthenticated telnet access to serial ports
- Fix file descriptor leak in snmpstatusd
- Fix rpcd showing high CPU utilization
- Fix NTP support on mixed IPv4 and IPv6 networks
- Fix setting SNMPv3 Engine ID
- Fix UPS autoresponses not triggering
- Fix Digipower SNMP RPC not showing status in Power menu
- Fix ping auto responses getting stuck in triggered state
- Fix bad error message for invalid SMS gateway field when configuring autoresponses
- Fix incorrect validation errors for hidden autoresponse actions
- Fix UPS graphing
- Fix modem watchdog interoperation with cellmodem failover
- Fix being unable to disable SNMPv1 and SNMPv2 to run in SNMPv3 mode only
- Fix portmanager hanging in some circumstances when port logging to remote CIFS servers
- Fix inconsistent options between snmpd and snmptrap configuration
- Fix enabling debug serial console on ACM550x, ACM550x and IM72xx
- Fix rare hang on IM72xx reboots
- Fix WEP configuration file and key selection
- Fix setting up RPCs where the have parentheses in the RPC type
- Fix management lan tab not reappearing after disabling bridged mode on IM4216-34
- Fix LTE modems sometimes not connecting, even when modem appears to be fine
- Fix serial pattern match autoresponses all being triggered whenever one occurs
- Fix CIFS mounted port logging not reliably working on boot
- Fix cases where cellular SMS sending and receiving would stop working after dual SIM failover

Other

- Remove NTP monitor support to remove chance of NTP amplification attacks
- Remove irrelevant system log messages from rpcd

4.4.0 (January 14 2013) (Lighthouse)

This is a production release.

Enhancements

- Add Console Gateway feature to Lighthouse

Fixes

- Fix bulk provisioning issues
- Fix infod entry removal
- Fix portmanager log message spam
- Fix Cherokee so that it doesn't leave tmp files around
- Fix VCMS netflash issue with long filenames
- Fix Config backup/restore issue through Lighthouse proxy
- Fix netstat display of IPv6 and IPv4v6 addresses
- Fix issue with IPv6 Firewalling

3.9.1 (December 17 2013) (Console Servers)

This is a patch release.

Enhancements

- Add support for the serial port concentrator in LightHouse 4.4.0
- Add bulk provisioning scripts for rolling out large numbers of devices
- Add support for persisting 'log' options in conman.conf
- Add support for Raritan PX2 PDUs

Fixes

- Fix sending sms messages when cell modem is a failover interface
- Fix Servertech single bank script
- Fix cherokee leaving old temporary directories in /tmp
- Fix configuration back up through LightHouse web proxy
- Fix memory leak in conman

3.9.0u2 (November 21 2013) (Console Servers)

This is a patch release.

Enhancements

- Improve WebUI authentication logging and Auto-Response integration
- Add DC power supply support for IM72xx-DDC devices

Fixes

- Fix XHCI errors on IM72xx products
- Fix LTE dialout route metric
- Fix IM72xx Dial menu labelling issue
- Fix TACACS issue with incorrectly padding attributes
- Fix migration issues when delayed config commit is enabled
- Fix issue with Verizon LTE cellular statistics
- Fix issue with adding Serial RPC devices
- Fix isse with comma separated email addresses and cellular phone numbers in Auto-Response actions

3.9.0u1 (October 23 2013) (Console Servers, (V)CMS)

4.3.0u1 (October 23 2013) (Lighthouse)

This is a production release.

Fixes

- Fix migration issue for webserver configuration

3.9.0 (October 21 2013) (Console Servers, (V)CMS)

This is a production release. ## 4.3.0 (October 21 2013) (Lighthouse)

This is a production release.

Enhancements

- LH: Add SNMP sysObjectId for Lighthouse
- LH/CMS/VCMS: Fix user permissions when using remote groups
- Add SNMP sysObjectId for IM72xx products
- Add Connection Manager daemon (conman), to manage cellular and dial connections
- Add support for failover between dual modem sim cards on appropriate models
- Add SNMP table describing status of digital I/O ports
- Add default sysservices option to SNMP
- Switch to the Cherokee web server
- Add secure cookie attribute
- Add human-readable descriptions of LTE information preferences
- Add more diagnostic information to support report for 3G/USB problems

Fixes

- Fix more problems with webserver causing intermittent “500 internal server error”
- Fix lower case Kerberos realms being forced to upper case
- Fix deleting custom IPSec tunnel attributes causing config errors
- Fix nagios checks being incorrectly HTML escaped
- Fix TACACSLocal and TACACSDownLocal users being locked out when server is down
- Fix sidebar layout changing dimensions while page is loading
- Fix inconsistent naming of digital I/O ports
- Fix inforrect display of UML290 IMEI
- Fix supurious ‘unauthorized access attempted’ log messages
- Fix SNMP configuration page incorrectly complaining about no community string
- Fix activation of CDMA cellular modems
- Fix SNMP MIBs failing syntax checks
- Fix HTTPS login attempts being logged as ‘::1 (localhost)’
- Fix HTTPS loging auto-responses seeing source IPs as ‘::1 (localhost)’

3.8.1u2

This is a patch release.

NOTE

- Downgrading from Lighthouse 4.2.0 or console server 3.8.0 (or later) to earlier versions will cause HTTP and HTTPS to stop functioning. To remedy this after the downgrade, you will need SSH access to the device. Connect, and run

```
rm /etc/config/lighttpd.d/https.conf
```

then

```
config -r services
```

3.8.1u1 (September 2013) (Console Servers, (V)CMS and Lighthouse)

This is a patch release.

Enhancements

- Add FTDI drivers to USB enabled products
- Improve the authentication test page group listings

Fixes

- Fix CDMA modem issue on ACM5504-5-GV and GS
- Fix IM42xx default config from USB issue
- Fix Auto-Response Pattern match not disconnecting users
- Fix Serial port labels getting reset
- Fix NSCA check to newer NSCA daemon issue
- Fix LDAP DN field validation
- Fix user changes removing SSH keys
- Fix FIPS mode issue
- LH: Fix spurious error in syslog from dialpool heath check

3.8.0u2 (September 2013) (Console Servers)

This is a patch release.

(See note above about downgrading from this version)

Fixes

- Fix Kerberos realm being forced to uppercase
- Fix network host nagios checks being mangled and escaped
- Fix problems with webserver causing intermittent “500 internal server error”

Known Issues

Opengear are aware of the following product-specific issues with this release:

- Secure cookie attribute is no longer being set
- HTTPS login attempts are logged as coming from ‘::1 (localhost)’
- HTTPS login auto-responses will see source IPs as ‘::1 (localhost)’

3.8.0u1 (August 2013) (Console Servers)

This is a patch release. (See note above about downgrading from this version)

Enhancements

- Add NTLM support to curl

Fixes

- Fix IPSec over LTE cellular connections restarting needlessly
- Fix serial port labels being HTML escaped in config

- Fix DOS vulnerability in lighttpd (CVE-2012-5533)
- Fix generation of wildcard SSL certificates
- Fix not allowing whitespace in autoresponse names
- Fix setting serial break characters
- Fix running a DHCP server on bridged and bonded interfaces
- Fix creating portforwards and port rules with bot TCP&UDP selected
- Fix IPv6 HTTPS access to the web configuration UI.

3.8.0 (July 2013) (Console Servers)

This is a production release. (See note above about downgrading from this version)

Enhancements

- Add error messages when running invalid configurators from command line config tool
- Add secure cookie attribute when using HTTPS
- Add more cellular status information and settings

Fixes

- Fix failover with bridged and bonded interfaces on the IM4216-34
- Fix IMPI RPC status command
- Fix problems with retrieving stats from Pantech UML290 cellular modem
- Fix modem watchdog for LTE modems
- Fix cascading issues with port 1 on ACM slaves
- Fix link monitoring on ACM500x and ACM550x models
- Fix serial port logs not taking timestamp size into account when rotating
- Fix CDMA modems misreporting provisioning status
- Fix 5th argument not being passed to custom auto-response actions
- Fix TACACSDownLocal authorization interaction with local groups
- Fix unclear definition of TX/RX for logging levels
- Fix deletion of configured NTP servers
- Fix TACACSDownLocal authorization interaction with local groups
- Fix migration to add root user to config.xml
- Fix problems with side bar in web configuration cgi being too narrow
- Fix problems with invalid characters in group names
- Fix minor page formatting error on SNMP page
- Fix Nagios event auto-response to use nagios configured host name.
- Fix security vulnerability CVE-2012-2944 in NUT
- Fix cases where we had potential XSS vulnerabilities
- Other security fixes

4.2.0 (July 24 2013) (Lighthouse)

This is a production release. (See note above about downgrading from this version)

Enhancements

- Add periodic health testing of dialpool connections and modems
- Add Auto-response capabilites to Lighthouse
- Add improved dialpool support, including auto-modem selection
- Add different web banner for Lighthouse product to easily distinguish it from Console Servers
- Add error messages when running invalid configurators from command line config tool
- Add secure cookie attribute when using HTTPS

- Add source IP logging for web configuration cgi login

Fixes

- Fix modify user console server command - user lock/unlock works again
- Fix deletion of configured NTP servers
- Fix TACACSDownLocal authorization interaction with local groups
- Fix migration to add root user to config.xml
- Fix problems with side bar in web configuration cgi being too narrow
- Fix problems with invalid characters in group names
- Fix minor page formatting error on SNMP page
- Fix Nagios event auto-response to use nagios configured host name.
- Fix security vulnerability CVE-2012-2944 in NUT
- Fix cases where we had potential XSS vulnerabilities
- Other security fixes

3.7.0u3 (June 3 2013) (Console Servers)

This is a patch release.

Enhancements

- Add sudo support for admin users on IM/ACM devices
- Add SMS support for Verizon LTE on ACM5504-5-LV

Fixes

- Fix serial port syslog format changes
- Fix multicast issue with IM42xx and CM41xx ethernet drivers
- Fix bridging issue on IM4216-34
- Fix NUT detection of Slave DC Servertech PDUs

3.7.0u1 (April 19 2013) (Console Servers)

This is a production release.

Enhancements

- Switch to ethtool for monitoring link status on the IM42xx and CM41xx

Fixes

- Fix mangle rules for OOB LTE modems
- Fix failed web login exposing version information
- Fix FTP transfer of large files sometimes dropping connection
- Fix CIFS port log mounting not working
- Fix USB port logging
- Fix no data appearing after changing from local console to console server mode
- Fix CM41xx switch support

4.1.0u2 (April 18 2013) (Lighthouse)

This is a patch release.

Fixes

- Lighthouse: Fix missing dialpool support

4.1.0u1 (April 16 2013) (Lighthouse)

This is a production release.

Fixes

- Lighthouse: Fix KVM support for US-based ElasticHosts provider
- Fix failed web login exposing version information

3.7.0 (April 12 2013) (Console Servers)

This is a production release. ## 4.1.0 (April 12 2013) (Lighthouse)

This is a production release.

Enhancements

- Lighthouse: Add support for Lighthouse Standard and Lighthouse Enterprise
- Lighthouse: Add support for OpenVPN and IPSec
- Lighthouse: Add user configurable firewall support
- Lighthouse: Improve speed of upgrades on KVM virtual machines
- Lighthouse: Build a USB install key for Lighthouse Standard and Enterprise
- Improve speed of serial port logging
- Added support for admin users reading syslog via CLI
- Add improvements to web ui security, including longer session keys
- Added support for LTE modems
- Added script to setup an IP address per serial port

Fixes

- Fix ServerTech outlet status reporting
- Fix vulnerabilites reported in OpenSSL and libPNG packages
- Fix support for PDUs with many outlets requiring multiple probes
- Fix NUT support for SNMP Servertech multi-tower PDUs
- Fix network interface not being correctly configured after config erase
- Fix broken modem support on IM42xx platforms
- Fix UPS battery voltage auto-responses not resolving
- Fix debug messages appearing in syslog with remote user authentication
- Fix specifying /32 peers in IPSec config page
- Fix ECIO reporting for the MC5728V modem

3.6.1u1 (March 14 2013) (Console Servers & (V)CMS)

4.0.0u3 (March 14 2013) (Lighthouse)

This is a production release.

Enhancements

- Add NUT scanner support
- Add cycle command for serial Servertech CDUs

Fixes

- Fixed Serial PDU outlet probing
- Fixed wording for Pattern Match Auto-Response triggers

- (CMS/Lighthouse) Fixed managed Console Server setup with DNS names
- Fixed Graph display using Safari on OS X
- Fixed Auto-Response Remote UPS triggers
- Fixed Auto-Response Environmental trigger issue
- Fixed GRE support on ACM/IM devices
- Fixed TFTP/FTP support on IM4004

3.6.1 (Feb 19 2013) (Release for Console Servers)

This is a production release.

Enhancements

- Add variable outlet probing for Serial RPCs

Fixes

- Fixed flow control issues on serial ports
- Fixed Servertech serial RPC issues on 2 and 8 outlet models
- Fixed Auto-Response configuration issues
- Fixed Port Cascading
- Fixed Cellmodem region changin
- Fixed outlet status for Cyclades PM10 RPCs

4.0.0u2 (Feb 15 2013) (Release for Lighthouse VM only)

This is a production release. ## 3.6.1 (Feb 15 2013) (Release for VCMS and CMS only)

This is a production release.

Enhancements

- CMS: Added features from 4.0.0u1 for CMS and VCMS

4.0.0u1 (Feb 1 2013) (Release for Lighthouse VM)

This is a production release.

Enhancements

- VCMS: Added groups and searching capabilities for console servers and managed devices
- VCMS: Added new VCMS dialout support via RFC2217 modems to contact remote console servers
- VCMS: Added single sign-on pass-through authentication from VCMS to console servers
- VCMS: Added proxied webshell connections from VCMS to console servers and serial ports
- VCMS: Added improved security for public cloud deployment

Fixes

- VCMS: Fixed incorrect NTP server installation
- VCMS: Fixed run_check fails on post-redundancy console servers
- VCMS: Fixed freshness checking still not working

3.5.3u5 (November 8 2012)

This is a patch release.

NOTE

- The stable firmware for all console servers is now at least 3.6.1 - If the console servers are being managed via a (V)CMS or Lighthouse appliance, must be first upgraded to 3.6.1 (for (V)CMS) or 4.0.0 (for Lighthouse) at a minimum.
- CMS: With 3.5.3, please upgrade your Opengear CMS install to 3.5.3 FIRST, before upgrading devices under managment to 3.5.3 or later. Failure to do so has the potential to lock users out of the CMS installation.

Fixes

- Fixed issue with 8 bit character corruption with even/odd parity
- Fixed issue with web logins that was causing occasional failed logins
- Fixed issue with FTP server doing reverse DNS lookups for logging
- Fixed issue with command line config backups reporting errors
- Fixed issue when deleting users
- Fixed issue when setting permissions for network hosts and RPCs
- Fixed duplicated log line issue with port and autoresponse logging
- Fixed crash in pmshell when FIPS mode is enabled

3.6.0 (October 15 2012)

This is a production release.

Enhancements

- Added support for CDMA SMS on cellular devices
- Added support for wireless AP country and hardware mode selection
- Added ACM550x recovery image with other recovery images

Fixes

- Fixed issue when CGI netflash fails (device now reboots)
- Fixed issue with the format of SDT host ports stored in config
- Fixed issue with occasional authentication failure logging into the web UI
- Fixed issues found with the 3.6.0b0 beta firmware:
  - Wireless AP bridging/bonding configuration problems
  - Wireless AP large data transfer occasionally causes instability
  - hwclock not working on some devices
  - user/group permissions for network hosts/RPC ports not persisting
  - USB modem device links missing on some devices

3.5.3u4 (October 2 2012)

This is a patch release.

Enhancements

- Added Authenticated NTP support for upstream servers

Fixes

- Fixed issue with network host permitted services
- Fixed issue with configuration mutual exclusion with large configurations

3.6.0b0 (September 13 2012)

This is a production release.

Enhancements

- Added default IP NAT and forwarding for cellular ACMs
- Added Wifi AP support for ACM 5504-5 products with wireless cards
- Upgraded NUT version to 2.6.2

3.5.3u3 (September 05 2012)

This is a patch release.

Fixes

- Fixed issue with multiple LDAP server addresses
- Fixed issue with TFTP client
- Fixed issue with services configurator
- Fixed issue with pmshell only users and SSH direct to ports
- Fixed issue restoring config backups
- Fixed issue with logging port logs to remote syslog after failover
- Fixed bad memory allocation in infod
- Fixed crontab -e command
- Fixed UPS compatibility hyperlink
- Fixed override DNS servers so that server addresses can be left empty
- Fixed Port access page not showing correct permissions with unauthenticated telnet

3.5.3u1 (July 27 2012)

This is a patch release.

Enhancements

- Added an new unpowered signal line mode for serial ports, to handle out-of-specification devices drawing excess power

Fixes

- Fixed the command line user-del script
- Fixed link from index cgi page to new location to set root password
- Fixed issue with cgi authentication session files not being checked correctly
- Fixed miscellaneous typographical errors in the configuration cgi

3.5.3 (July 19 2012)

This is a patch release.

Enhancements

- Added support for a default group for TACACS users
- Added put '/proc/loadavg' and 'df' in the support report

Fixes

- Fixed enabling FIPS with delayed config commit causing immediate reboot
- Fixed serial statistics all showing as zero

- Fixed many ssh logins/logins causing wtmp file to fill /tmp

3.5.3b1 (June 27 2012)

This is a patch release.

Enhancements

- Added support for ServerTech RPC load banks
- Added support for USB Consoles (i.e. newer Cisco units)
- Added HOST-RESOURCES MIB to SNMP, allows for system uptime reporting
- Added support for service names other than raccess for TACACS+
- Added support for running custom cgi web apps on board

Fixes

- Fixed local (i.e. USB) configuration backup and load-on-erase
- Fixed remote backup downloads sometimes being truncated
- Fixed cron not restarting if it terminated early
- Fixed link on index page for setting root password
- CMS: Fixed root being described as an unauthorized user
- CMS: Fix Nagios Auto-Response checks

3.5.3b0 (June 06 2012)

This is a patch release.

Enhancements

- CMS: Added for multiple redundant CMS servers
- Added new Services page to ease configuration of network services (e.g. FTP, HTTP, Telnet, SSH)
- Improved management of root user, now appears in user list in web management console
- Added support for custom root password on configuration reset (ACM500x and ACM550x family devices only)
- Added support for configuring public key authentication of SSH
- Added support for PEAP-MSCHAPv2 WiFi
- Improve web management console on mobile devices (e.g. iPhone/iPad, Android)
- Improve webshell terminal on mobile devices (e.g. iPhone/iPad, Android)
- CMS: Reduce data traffic for remote devices, now more suitable for 3G

Fixes

- CMS: Fixed scheduled commands not working
- Fixed display of default gateway routes when added via web management console
- Fixed multiple TACACS+ servers, they now work correctly if first is down
- Fixed several instances of harmless noise messages appearing in syslog
- Fixed instances where new auto-responses were unable to be saved
- Fixed display of managed devices outlet numbering

3.5.2u16 (May 4 2012)

This is a patch release.

Enhancements

- Added SMS command enhancements for Auto Response
- Added region setting for 3G GSM modems
- Added current 3G tech to Cellular Statistics
- Added power-cycle support for IP Power 9258
- Support for SD4001 Rev 01

Fixes

- Fixed sendsms command on IM42xx with cellular modem
- Fixed CGI displaying OpenGear on CM/SD4001/2/8
- Fixed DHCP configurator warning message
- Fixed pmshell power menu issue
- Fixed failover on single port ethernet units
- Fixed webterminal issue
- Fixed serial port log facility/priority override

3.5.2u14 (April 19 2012)

This is a patch release.

Fixes

- Fixed cases where some enabled services weren't started until after a reboot
- Fixed NTP not being actually being disabled when asked to do so via configuration
- Fixed remote ups logging

3.5.2u13 (April 16 2012)

This is a production release.

Enhancements

- Added modem watchdog that can optionally reboot the unit if sufficient pings fail to a remote host
- Added bootloader version string to support report
- Added more detail about cell modem and USB subsystems to support report

Fixes

- Fixed CMS: combinations of 3.4.x and 3.5.x managed devices with remote authentication now work correctly
- Fixed upgrades from before 3.0.4 causing user's passwords to break
- Fixed RFC2217 RS485 mode
- Fixed serial signal autoresponse SNMP traps not working
- Fixed https in FIPS mode
- Fixed remote syslog for port logs breaking emd logging and graphing
- Fixed managed device RPC outlets
- Fixed harmless configurator error messages after factory erase
- Fixed cascading issues with low serial port count slaves (e.g. ACM5004)
- Fixed enabling IPSec sometimes braking SNMP
- Fixed ability to modify saved auto-response trigger actions
- Fixed dyns.cx dynamic dns configuration on the dialin/dialout page
- Fixed infrequent and usually harmless SQUASHFS errors during netflash
- Fixed CDK builds not being about to be accessed by ssh
- Fixed pmshell ~m escape not working with cascaded slaves

- Fixed pmshell help not working with cascaded slaves
- Fixed pmshell history hot working with cascaded slaves
- Fixed ability to add custom udhcpc scripts with /etc/config/udhcpc.script
- Fixed debug information appearing in syslog while cascading
- Fixed RS485 issues with the top four ports on the ACM5508
- Fixed cases where passwords were being crypted twice or incorrectly removed from /etc/shadow

3.4.1u2 (Mar 30 2012) (Release for ACM5002, ACM5003, ACM5004 and ACM5004-2 only)

This is a patch release.

Enhancements

- Updated release of pre-autoresponse firmware to add support for the hardware watchdog on ACM500x models

3.5.2u12 (Mar 23 2012) (Internal release - not available publicly)

This is a patch release.

Enhancements

- Added support for longer serial numbers

Fixes

- Fixed default baud rate to be 38400
- Fixed USB LED so that it now triggers on USB data transfers

3.5.2u11 (Mar 15 2012)

This is a patch release.

Enhancements

- Improved speed and performance of serial port logging and auto-responses

Fixes

- Fixed SSL vulnerablity CVE-2011-3389
- Fixed config migration issues concering dialin user accounts
- Fixed inablity to specify gateway on management lan ports on some devices
- Fixed support for IPSec 'leftsourceip' custom option
- Fixed dyns.cx dynamic DNS support
- Fixed rare cases that could cause firmware upgrades to safely hang
- Fixed CMS 'admin' users on managed devices causing them to unregister

3.5.2u10 (Mar 2 2012) (Release for ACM5504-2, ACM5504-5, ACM5508-2 only)

This is a patch release.

Fixes

- Fixed management lan not appearing in the web management console.

3.5.2u9 (Feb 28 2012)

This is a patch release.

Enhancements

- Added ACM550x-M device support

Fixes

- Fixed remote-only (e.g. RADIUS) pmshell group-based authorization
- Fixed logging intervals being incorrect for recording periodic information (e.g. environmental statistics)
- Fixed CDK builds not having an sshd user in /etc/config/passwd

3.5.2u8 (Feb 22 2012) (Released for CMS6100 and VCMS only)

This is a patch release.

Enhancements

- Added protection against config cmdline utility corrupting config.xml
- Added support for MD5 crypted system passwords
- Added idle LED display on ACM500x units
- Added CMS log rotation to Nagios log files
- Added CMS option to turn off Nagios monitoring for managed devices

Fixes

- Fixed rare circumstance that could corrupt config.xml on upgrade
- Fixed SSH keys being recreated if device reboots before all keys initially generated
- Fixed TACACS remote group retrieval inconsistencies
- Fixed Incorrect daylight savings setting on default timezone
- Fixed port logs for port numbers greater than 10 being sent to the wrong file
- Fixed CMS failing service checks being interpreted as host checks
- Fixed CMS access to managed console servers for non-root users
- Fixed CMS call home forwards not working after introduction of restricted shells
- Fixed CMS certain configurations not being written out when webserver restarted

3.5.2u7 (Feb 13 2012)

This is a patch release.

Enhancements

- Added ACM550x device support
- Added support for DES encrypted TACACS passwords
- Added support for setting log level filters for syslog
- Added support for setting IPv6 static gateways
- Added ethernet statistics to the support report
- Added different log size rotation thresholds for different devices
- Added AR_DEV_REF macro for custom auto-response scripts

Fixes

- Fixed AR_CHECK_DEV macro custom auto-response scripts

- Fixed inablity to disable DHCP server via command line
- Fixed editing RPC outlet labels removing SNMP community
- Fixed memory leak in web terminal
- Fixed TACACS prompting twice for password
- Fixed log messages from sierra-gsm-watchdog filling syslog
- Fixed migration of dialin config not removing old chap/pap-secrets entries
- Fixed spurious malformed line syslog errors when powering off RPC outlets

3.5.2u6 (Jan 25 2012) (Released for ACM5002, ACM5003, ACM5004 and ACM5004-2 only)

This is a patch release.

Enhancements

- Further improve 3G reliability

Fixes

- Fix cases where reboots wouldn't complete successfully

3.5.2u5 (Jan 17 2012)

This is a patch release.

Enhancements

- Improved 3G reliablity w.r.t SMS failures
- Added SMTP client authentication overrides (allow LOGIN type authentication)

Fixes

- Fixed user configurator excessive logging
- Fixed large file incompatibility with tftp32/64 clients uploading
- Fixed remote group membership issues when users only have one remote group
- Fixed local authentication with TACACSLocal
- Fixed NTP vulnerability CVS-20093563
- Fixed RS485 timing issue
- Fixed migration of serial alerts
- Fixed ACM500x network RX stall under heavy traffic
- Fixed CHAP/PAP secrets issues when using delayed config commits
- Fixed exposed services and hosts for SDTConnector
- Fixed bonding and bridging support on IM4004-5

3.5.2u4 (Dec 13 2011) (Released for IM4216-34 only)

This is a patch release.

Enhancements

- Added support for the IM4216-34

Fixes

- Fixed restricted shell interoperability with CMS

3.5.2u3 (Dec 6 2011)

This is a patch release.

Enhancements

- Added support for USB Keyboard/Mice on KCS
- Added Kerberos authentication support on IM/ACM/KCS
- Added an Authentication Test Page
- Added support for specifying authentication type for 3G connections
- Added logic to disable serial ports during error conditions (floating serial lines)

Fixes

- Fixed extraneous SNMP log messages
- Fixed migration issues coming from early firmware
- Fixed TFTPD consistency issues
- Fixed USB stick mounting issues on KCS
- Fixed SNMP poll differences with EMD and serial signals
- Fixed FIPS mode banner issues
- Fixed powersupply configurator warning messages
- Fixed Auto-Response Repeat Trigger Delay not saving
- Fixed Email Body field in Auto-Response Email Action size restrictions
- Fixed unauthenticated telnet issues with cascaded ports
- Fixed IPSec PFS issues
- Fixed speed issues with hosts and users configurator on complex configurations

Other

- Disabled SSLv2 due to protocol level security issues

3.5.2u1 (Nov 8 2011)

This is a patch release.

Fixes

- Fixed migration of users to restriced shells

3.5.2 (Nov 3 2011)

This is a patch release.

NOTE

- Under 3.5.2 or later, users that are not members of any groups will not get shell access to the device. To give shell access, add the user to the “user” or “admin” groups. If a user just requires pmshell access, add them to the “pmshell” group.

Enhancements

- Added support for having pmshell as default shell
- Added pmshell chooser escape command
- Added pmshell idle timeout
- Added configurable port spacing on pmshell menu
- Added multiple dialin and callback user support
- Added syslog and more firewall information to support report
- Added client side config generation to OpenVPN

- Added ethernet bonding support on dual interface devices
- Added remote auth support to FTP server
- Added MOTD support for Serial/Web Console/FTP
- Added Alias IP address support
- Added RS485 with echo mode on console servers with RS485
- Added PPTP VPN server support
- Added more supported protocols to Firewall rules
- Added destination IP matching for DNAT rules
- Restricted user shell for users not in the “users” or “admin” groups

Fixes

- Fixed OpenVPN configuration issues
- Fixed Portmanager serial signal noise in syslog
- Fixed editing users without respecifying passwords
- Fixed SNMP alarm traps not including alarm name
- Fixed Auto-Response configuration via CMS Proxy
- Fixed bash command completion in vi mode
- Fixed Cellular technology 2G/3G preferences not changeable from UI
- Fixed Auto-response digital IO actions not working
- Fixed SIM PIN unlocking not persisting over modem restart

3.5.1u2 (Oct 13 2011)

This is a patch release.

Enhancements

- Added FTP server on IM/ACM/KCS devices
- Added repeat delay setting to Auto-Response

Fixes

- Fixed a number of SNMP memory leaks
- Fixed an issue with SDT Connector connections for Remote users from CMS Beta
- Fixed a ping issue with the modem watchdog script

3.5.1 (Oct 3 2011)

This is a patch release.

Enhancements

- Added support for Blackbox Elite Managed PDU
- Added integration support for Auto-Response into CMS
- Added support for Sierra Wireless MC5728V module
- Added command line IP tunnelling (GRE) support to ACM/IM/KCS devices
- Added Migration of existing Alerts to Auto-Response subsystem
- Added multiple outlet control for IP-PDU 9108 RPC
- Added PDU Export PDU Support
- Added Eaton 9140 USB UPS support
- Added ServerTech 24 Port PDU support
- Added a command line configurable cellular connection watchdog

Fixes

- Fixed Dialout subsystem migration from 3.4.x series firmware
- Fixed Dialout reconfiguration of active connections
- Fixed built-in VNC client on KCS devices
- Fixed default alarm name generation for EMDs
- Fixed RS485 TX enable issue on ACM-I devices

3.5.1b0 (Aug 26 2011)

This is a production release.

Enhancements

- Added support for Sierra Wireless 308 USB 3G modem
- Added support for Sierra Wireless 312U 3G modem
- Added extra IPSec configuration options for improved interoperability
- Added command line utilities for OSPF failover on dual ethernet devices
- Added Auto-response framework as a replacement for alerting

Fixes

- Fixed incorrect automatic IPSec route
- Fixed unauthenticated telnet cascading issue
- Fixed excessive logging when using PortShare encryption or authentication
- Fixed connection restart issues on PortShare encryption or authentication change

3.4.1u1 (Jul 27 2011)

This is a patch release.

Enhancements

- Added Wifi Dongle support for IMX series IM42xx devices
- Added SMSTools on IMX series IM42xx devices
- Added hostname identifier to SMS and Email alert message bodies

Fixes

- Fixed a memory leak in the SNMP daemon
- Fixed a race condition with multiple concurrent RADIUS/TACACS+/LDAP users
- Fixed an issue with SMS alerting

3.5.0u1 (Jul 7 2011)

This is a production release.

Enhancements

- Added CMS support for remote authentication
- Added TACACS remote group support
- Added Windows LDAP “users” group mapping support
- Added customizable RPC outlet names
- Added drag and drop support to web terminal

Fixes

- Fixed OpenVPN failing to connect to legacy server
- Fixed SMS alerts not triggering without email configured

- Fixed login form password autocompletion being enabled
- Fixed web terminal to cascaded ports
- Fixed dialin configurator requiring local and remote IP
- Fixed DHCP server configuration issue on IP address change
- Fixed serial port “mode” displayed deleted RPC name

3.4.1 (Jun 15, 2011)

This is a patch release.

Enhancements

- Added external cellular support to IM4004-5
- Added WebUI configuration and alerting support for direct SMS transmission on devices with cellular modems
- Added x/y/zmodem support on IM4004/IM42xx/KCS61xx/ACM500x devices

Fixes

- Fixed confusing log messages relating to ‘monitor’
- Fixed utmp issue causing incorrect log messages

3.5.0 (Jun 9, 2011)

This is a production release.

NOTE

- Any existing pre-3.5.x alerts will be migrated to the Auto-Response subsystem, but there is not a 1-1 correlation between the systems, and it is recommended in that upgrades be performed in a test environment first. The logging subsystem has also been rewritten, and logging formats (particularly for Environmental and UPS data) have changed. If these logs are currently being backed-up or machine-parsed, it is recommended that the upgrade be tested before deployment into production.
- When upgrading VCMS for VMware from an earlier release, use the following procedure to resolve the licence key issue:
    - Shut down VCMS using System Administration -> Shut Down
    - Force power off the virtual machine
    - Edit CMS61xx-vcms-vmware.vmdk on the host system, under “Extent description” change 7791525 to 7807590

Enhancements

- Added CMS RFC2217/PortShare proxy support
- Added CMS node fingerprint inspection support

Fixes

- Fixed CMS uncontactable node causes retrieve Managed Devices to fail
- Fixed CMS Nagios service visibility for users in multiple groups
- Fixed CMS spurious scrollbars in Nagios
- Fixed CMS uncontactable node reports status unknown
- Fixed CMS basic TACACS+ support
- Fixed VCMS licence key not being accepted under VMware
- Fixed VCMS OVF packaging to work around WinZip bug

3.4.0u3 (May 20, 2011)

This is a patch release.

Enhancements

- Added watchdog to IM42xx, CM41xx and IM4004
- Added the ability to send CTRL-H instead of CTRL-? on consoles
- Added a default TERM variable to user environment set to dumb

Fixes

- Fixed Forwarding and Masquerade page for IMG4216-25
- Fixed IPv6 on IM4216-25
- Fixed dashboard for non-admin users on devices with internal EMD's
- Fixed default Wireless settings
- Fixed handling of multiple RFC2217 connections
- Fixed issue of changing baud rates on ports with existing RFC2217 connections
- Fixed port forwarding

3.4.0u2 (March 18, 2011)

This is a patch release.

Enhancements

- Added MAC address matching in Firewall rules
- Added DNS information to statistics and support report pages
- Added Calling-Station-ID RADIUS attribute support with Telnet
- Added support for NFS mounts over TCP
- Added IPv6 support for SNMP

Fixes

- Fixed issue with TACACSDownLocal and WebUI access
- Fixed issue where refresh links do not work
- Fixed error logging issues with Cellular data alerts
- Fixed issue with failover when per-serial-port IP script is used
- Fixed AZERTY keyboard issue with webshell
- Fixed firewalling issue for Call-Home
- Fixed SIM unlocking/CDMA provisioning issue
- Fixed KCS built-in Firefox config ui
- Fixed KCS configuration corruption on unexpected shutdown
- Fixed NTPD time update issue
- Fixed Baytech RPC support
- Fixed Command line config changes by admin users
- Fixed DHCP lease pool editing
- Fixed log file formatting errors with certain UPSs

3.4.0u1 (February 15, 2011)

This is a patch release.

Enhancements

- Added SNMP traps/notifications for data usage alerts

Fixes

- Fixed CDK kernel build issues
- Fixed data usage alert script ALERT_SECONDS value
- Fixed issue creating TCP based OpenVPN tunnels
- Fixed data logging log settings so that alerts can have a time period of 30 days
- Fixed Nagios serial port hyperlinks to point at the new webshell

3.4.0 (February 4, 2011)

This is a production release.

Enhancements

- Added Basic Throughput logging and alerting for cellular modems
- Added always Up Dialout support on all products
- Added cellmodem CSD dialin support
- Added firewall rule improvements and ordering support
- Added port forward improvements
- Added static routing support
- Added DNS masquerading support

Fixes

- Fixed interaction between Trusted Networks and Web Terminal
- Fixed 3G Dongle support issues
- Fixed external CDMA dongle authentication issues
- Fixed dialout routing and IPSec interaction issues
- Fixed modem setup with non-PPP dialin robustness issues
- Fixed Web Terminal through CMS proxy issues
- Fixed graphing issues with Internet Explorer 7 & 8

3.3.2u2 (January 13, 2011)

This is a patch release.

Enhancements

- Prevent config corruption with incorrectly encoded characters
- Improve DCD signal handling on ACM500x devices
- Add a warning if no static leases or pools exist when DHCP server is enabled

Fixes

- Fix firewall handling of PortForwards with no destination IP
- Fix firewall being disabled in some conditions
- Fix Port Forward and Port Rule editing issues

- Fix IPSec over 3G issue
- Fix support for GNUdip DDNS servers
- Fix intermittent auth failure for External CDMA dongles
- Fix deletion of static leases and pools on multi-interface devices
- Fix TACACS+ permissions issue using Cisco ACS
- Fix Portshare Encryption issue
- Fix ACM5003-W Adhoc Wifi issues

3.3.2 (December 14, 2010)

This is a patch release.

Enhancements

- Improved IO-Port Configuration on ACM
- Restricted serial protocol configuration to supported devices
- Increased Cellular interface stability during configuration changes
- Support for Sierra Wireless 598U CDMA Modem
- Support for Sierra Wireless C885 GSM Modem
- Changed NTP servers to support NTP time serving
- Added OpenVPN support to KCS

Fixes

- Fixed TACACS+ support on KCS
- Fixed SSL Certificate Downloads by root user
- Fixed Fail forward using analog modem
- Fixed VNCS firewall rules on KCS
- Fixed DHCP configuration issues on ACM5003-W
- Fixed Management LAN configuration issues on IM4216-25
- Fixed IPSec Firewall issues
- Fixed OpenVPN Firewall issues
- Fixed KCS Firewall issues
- Fixed KCS Configuration modification issues
- Fixed Hexadecimal WPA PSK Support
- Fixed EMD issues with negative temperatures on CM4001/8 and SD4001/2/8
- Fixed spurious text output on Local Config Restore

3.3.1 (November 19, 2010)

This is a patch release.

Enhancements

- Added GPS position support

Fixes

- Fixed encryption configuration issues with SNMPv3
- Fixed CMS proxy compatibility
- Fixed TFTP server USB mounting
- Fixed issues switching between encrypted and plain RFC2217/raw TCP
- Fixed spurious port forward rule created by successive saves
- Fixed firewall configuration page spuriously applying configuration

3.3.0 (November 5, 2010)

This is a production release.

Enhancements

- Added advanced firewall and port forwarding configuration
- Added masquerading and network forwarding configuration
- Added AJAX serial console and system terminal via web UI
- Added PortShare encryption and authentication server support
- Added SNMP GUI configuration support

Fixes

- Fixed serial port SDT password spuriously autocompleted
- Fixed IPv6 firewall rules not not setup after enabling IPv6
- Fixed RSSI units inconsistent between ACM UMTS and CDMA models
- Fixed SNMP v3 support
- Fixed OG-STATUS-MIB minor type mismatches

3.2.2u2 (November 5, 2010)

This is a patch release.

Fixes

- Fixed dial-in become Default Route option
- Fixed serial DB9 port dial for IM42xx products
- Fixed serial port alerts not included in auto-generated Nagios config
- Fixed GUI can erroneously report CDMA module not activated

3.2.2u1 (October 27, 2010)

This is a patch release.

Fixes

- Fixed some MySQL database tables not being flushed on VCMS
- Fixed IPv6 support on SD400x and CM400x
- Fixed EMD Fahrenheit temperature conversion

3.2.2 (October 23, 2010)

This is a patch release.

Enhancements

- Added support for Tripp Lite SU600RT4U

Fixes

- Fixed IM42xx internal modem at higher baud rates
- Fixed IM4216-25 switch cross talk in bridged mode
- Fixed Australia/Tasmania time zone
- Fixed DHCP default gateway in bridged mode
- Fixed UPS monitor issues with repeated on-line/on-battery events
- Fixed input, output and load polling for Tripp Lite USB UPSes

3.2.1u2 (September 28, 2010)

This is a patch release.

Enhancements

- Added Intel PC-Card modem support
- Added serial break reset support for SD4001

Fixes

- Fixed user group migration issue in delayed config commit mode

3.2.1u1 (September 17, 2010)

This is a patch release.

Enhancements

- Added support for CDMA cellular modem on IMX42xx

Fixes

- Fixes related to CDMA activation

3.2.1 (September 15, 2010)

This is a patch release.

Enhancements

- Added support for CDMA cellular modem
- Added support for UMTS cellular modem on IMX42xx
- Added support for 48V DC power supply monitoring on IMX42xx
- Added support for VCMS licence key

Fixes

- Fixed support for pmchat serial RPCes
- Fixed ACM500x-G spurious emissions from unused DDR clocks
- Fixed invalid user group created at first boot
- Fixed DHCP client behaviour when failed over
- Fixed UMTS cellular modem slow reconnection after soft reboot
- Fixed ACM500x-W wireless site survey
- Fixed ACM500x-W wireless LED
- Fixed remote syslog support on KCS61xx
- Fixed switching from serial port console mode -> RFC2217 server mode
- Fixed CMS not importing internal EMD status
- Fixed dynamic DNS maximum interval field units
- Fixed network interface bridging on ACM500x-2
- Fixed CM network down during multicast and broadcast storm

3.2.0u1 (August 17, 2010)

This is a patch release.

Fixes

- Fixed CMS alert import and triggering

3.2.0 (August 5, 2010)

This is a production release.

Enhancements

- Added OpenVPN support
- Added Zenoss support via ZenPack and SNMP
- Added Solarwinds Orion NPM integration via SNMP
- Added specifying UID adding user from command line
- Added UTC as a timezone
- Added group support for improved remote authentication access control
- Added option to configure dynamic DNS retries
- Added two-factor RSA SecureID support
- Added graphing improvements
- Added delay configuration commit mode
- Added hardware watchdog support on ACM products
- Added new UPS support via NUT upgrade
- Added “call home”, SSH port forwarding GUI
- Added CMS support for managing firewalled nodes
- Added CMS web proxy for firewalled nodes
- Added CMS support for alternate node SSH port

Fixes

- Fixed IM42xx USB support improvements
- Fixed “change your password” error after editing password
- Fixed large values reported by UPS alerts
- Fixed NTPD not making initial time setting with large delta
- Fixed ‘users’ configurator failing if $HOME/.ssh exists
- Fixed APC PDU outlet probing
- Fixed validation of duplicate permitted services on a Network Host
- Fixed config applied twice for some pages
- Fixed spurious “possible flash corruption” message on ACM products
- Fixed serial power hotkey menu to work with remote authentication
- Fixed RADIUS and TACACS admin user environmental graph visibility
- Fixed system slow down when monitoring a lot of UPSes and SNMP RPCs
- Fixed serial port edits not being applied to running user configuration
- Fixed login session timeout
- Fixed IM and IMG products not utilizing all available RAM
- Fixed CMS not reporting disconnected or broken EMD
- Fixed CMS admin user host visibility
- Fixed CMS Nagios logging and log rotation
- Fixed CMS node NSCA cron job not removed
- Fixed CMS sanitization of Description/Notes and Host Name fields
- Fixed CMS invalidating password of final user after Retrieve Hosts
- Fixed CMS email alerts
- Fixed CMS icons
- Fixed CMS environmental service check link
- Fixed CMS node name validation too restrictive
- Fixed CMS menu formatting issue when deleting node
- Fixed CMS detected console server drop down to work with all browsers

- Fixed CMS undefined checks returning bogus output
- Fixed CMS EMD service check formatting

3.1.0u3 (June 25, 2010)

This is a patch release.

Fixes

- Fixed zero-indexed SNMP table rows issue with Zenoss
- Fixed broadband failover to static IP firewall issue
- Fixed ACM dual Ethernet management LAN connectivity issue
- Fixed ACM dialin user removed after config change

3.1.0u2 (June 10, 2010)

This is a patch release.

Fixes

- Fixed SNMP v2/3 Environmental Traps
- Fixed Local Backup Tab not appearing on IM/IMG/KCS
- Fixed KCS Dashboard display
- Fixed KCS serial port issues - ports 9 - 16
- Fixed KCS Bootsplash
- Fixed TFTP permissions
- Fixed Management Lan issue on ACM

3.1.0u1 (June 3, 2010)

This is a patch release.

Enhancements

- Added DNS override fields for dialout connections
- Added automatic failover recovery when primary network is restored
- Added failover and out-of-band statistics page
- Added TFTP server support for serving files > 32MB

Fixes

- Fixed TTY break length to be 500 msec as per Cisco specification
- Fixed custom config-post-configurator scripts not running
- Fixed web UI access using IPv6 address
- Fixed wireless network interface connecting in WPA2 mode
- Fixed possible failure detecting internal cellular modem
- Fixed possible failure unlocking SIM while connection is enabled
- Fixed dialout connections not accepting MSDNS servers
- Fixed DNS server handling across multiple connections
- Fixed CM41xx missing backup icon
- Fixed SNMP sysObjectId to use Opengear enterprise OID
- Fixed Nagios NSCA check reporting handling of check timeouts
- Fixed KCS configuration migration upgrading from 2.8.x
- Fixed KCS serial port cascading automatic key propagation

3.1.0 (May 10, 2010)

This is a patch release.

Enhancements

- Added dynamic DNS support for broadband OOB/FO port

Fixes

- Fixed access to web UI using IPv6 address
- Fixed IMG4004-5 switch not detecting link
- Fixed cascading slave configuration not applied
- Fixed network access to cascaded serial ports by port number
- Fixed setting IPsec left subnet
- Fixed SSH serial port access via OOB interface
- Fixed changing Local Console -> Console Server port requiring reboot
- Fixed upgrade migration can cause web server to fail to bind ports
- Fixed IPsec network to network traffic forwarding rules
- Fixed IM42xx-2 system/model name setting
- Fixed cellular modem SIM PIN entry
- Fixed KCS61xx configuration migration
- Fixed SNMP MIBs redefining OIDs when used together
- Fixed redefined OIDs when status and trap SNMP MIBs used together

3.1.0b1 (April 7, 2010)

This is a patch release.

Enhancements

- Added support for SD4008

Fixes

- Fixed SD4001 model naming
- Fixed image size: use busybox ftp(get/put), tftp, traceroute and remove mail in favour of msmtp on 8MB flash products

3.1.0b0 (April 2, 2010)

This is a production release.

Enhancements

- Added SNMP alert status and device status agents
- Added external EMD support to ACM products
- Added environmental temperature reporting in Farenheit
- Added IMX42xx support
- Added ACM5004-I RS4xx, digital I/O support

Fixes

- Fixed unable to set real time clock to year 2010
- Fixed RadiusDownLocal blocks local user when RADIUS server is down
- Fixed various LDAP authentication issues
- Fixed dial-in callback with USB modem
- Fixed USB storage on ACM products

- Fixed disabled ACM internal sensor displaying on environmental alert
- Fixed various UI form field validation issues
- Fixed logout button giving false positive under Chrome and Safari
- Fixed 'Stop Bits' serial setting
- Fixed shared local console/console server port UI layout
- Fixed TFTP Server option displayed on products where it is unavailable
- Fixed CIFS remote logging not reconnecting after server autodisconnect
- Fixed CIFS remote logging on KCS
- Fixed CIFS remote logging without username and password
- Fixed SNMP MIB lint compliance
- Fixed browser fav icon for Firefox and Chrome
- Fixed wireless WEP support
- Fixed applying wireless settings when editing existing connection
- Fixed services being restarted when DHCP lease renewed
- Fixed firewall rules being re-applied affecting configurator speed
- Fixed LDAP user access to serial ports using LocalLDAP authentication
- Fixed failed ping hangs custom portmanager init script
- Fixed invalid character validation
- Fixed standard SNMP MIBs not available
- Fixed naming, syntax and file organization clean ups in SNMP MIBs

3.0.4u1 (March 23, 2010)

This is a patch release.

Fixes

- Fixed SDT Connector not connecting with password authentication
- Fixed PPP using wrong IP address using IPCP negotiation
- Fixed sendsms tool

3.0.4 (March 15, 2010)

This is a patch release.

Enhancements

- Added secure services available via OOB/FO connections by default
- Added Opengear IP PDU power support
- Added pmshell double authentication
- Added shadow password support
- Added SMS gateway support

Fixes

- Fixed radio enabled when no connection is running
- Fixed Environmental Status/dashboard for EMDs containing # characters
- Fixed LDAP "can't resolve symbol" error message
- Fixed TACACS authentication when client prefers PasswordAuthentication
- Fixed timeout configuring NTP
- Fixed remote log storage remount after reboot
- Fixed wifi statistics site survey on ACM
- Fixed internal EMD available as an option when disabled
- Fixed noisy web UI logging in syslog
- Fixed "Alarm sensor label (null)" in alert email

- Fixed DNS servers unavailable when failed over to modem
- Fixed “unable to retrieve fingerprint” as a cascading slave
- Fixed unknown status for EMD dry contacts
- Fixed LDAP group authorization
- Fixed remotely authenticated user access to web UI
- Fixed USB logging on partionless USB flash drives
- Fixed reboot command unavailable

3.0.2u1 (March 10, 2009)

This is a patch release.

Fixes

- Fixed changing baud rate when no console is enabled

3.0.2 (February 9, 2010)

This is a patch release.

Enhancements

- Added cellular modem module support
- Added dynamic DNS support

Fixes

- Fixed alerts page not displaying properly
- Fixed kernel messages displayed in console server mode
- Fixed remote system logging not logging
- Fixed remote system logging not starting after enable
- Fixed error editing or deleting groups
- Fixed SSL mode connecting to legacy SMTP server
- Fixed UI formatting for internal sensors
- Fixed USB modem configuration path
- Fixed USB flash drive Port Log storage
- Fixed recovery booting images > 8MB

3.0.1 (January 8, 2010)

This is a patch release.

Enhancements

- Added support for FIPS mode for ACM family
- Updated default SSL certificate

Fixes

- Fixed RADIUSDownLocal authentication allowing local auth
- Fixed HTTPS allowing weak ciphers
- Fixed Tripp Lite SNMP RPC not probing outlets
- Fixed Management Console occasionally not completing to load

3.0.0 (December 22, 2009)

This is a production release.

NOTE

- Before upgrading from 2.x series firmware to 3.x series firmware, it is critical that you back up any existing configuration. Downgrading 3.x series firmware to 2.x series firmware requires a FACTORY ERASE before the unit will permit you to login.

Enhancements

- Added support for the ACM500x family

2.8.2u1 (January 21, 2010)

This is a patch release.

Enhancements

- Added SD4001 support
- Updated default SSL certificate

Fixes

- Fixed UPS support on serial port 1 for SD4002

2.8.2 (January 6, 2010)

This is a patch release.

Enhancements

- Added IPSec VPN support
- Added support for Opengear Monitor
- Added support for FIPS mode for IM and IMG family
- Added ability to log serial TX or RX only
- Added support for multiple NTP servers

Fixes

- Fixed ntpd occasionally not starting up
- Fixed Server Technology Sentry Switched CDU 'on' command
- Fixed DHCP server running when bridging is enabled
- Fixed aborted power menu session causing pmshell to hang
- Fixed Telnet source IP logging
- Fixed ambiguous "respawning too fast" message
- Fixed network down during multicast storm
- Fixed remote logging not using millisecond timestamps
- Fixed DHCP default gateway occasionally not set after erase
- Fixed RADIUSDownLocal authentication allowing local auth
- Fixed pmshell menu for remotely authenticated users
- Fixed HTTPS allowing weak ciphers
- Fixed Tripp Lite SNMP RPC not probing outlets

2.8.1 (October 5, 2009)

This is a patch release.

Enhancements

- Added USB modem support on IMG4004-5
- Added scripts to add/modify/delete users from CLI

Fixes

- Fixed backup icon missing from CM41xx
- Fixed multiple graphs locking up dashboard

2.8.0u2 (August 21, 2009)

This is a patch release.

Enhancements

- Added the ability to upload new SSL certificates
- Added a Dashboard for Admin and Root users
- Added PC card modem support
- Added support for APC RPCs over SNMP

Fixes

- Fixed UPS queries/actions can be very slow
- Fixed connection alerts not working for Network Hosts
- Fixed chat scrips failing when connecting to Linux
- Fixed tftp server requires reboot after configuration
- Fixed tftp uploads to USB

2.8.0u1 (July 8, 2009)

This is a patch release.

Fixes

- Fixed group visibility of outlets and host through UI
- Fixed user visibility of managed devices through UI
- Fixed EMD Summary display on the KCS
- Fixed failing over to the Management LAN makes box uncontactable
- Fixed DHCP server on the IM4216-2
- Fixed KCS6104 default local console
- Fixed IM4216-2 failover not opening firewall
- Fixed level 1 host logging
- Fixed EMD dropdowns with blank serial port labels
- Fixed NTP client with IPv6 NTP servers
- Fixed “alias” missing from auto-generated Nagios server config
- Fixed EMD and RPC off box logging
- Fixed EMD and RPC log using non human-readable/Unix timestamp
- Fixed already set up UPSes still showing in add UPS dropdown
- Fixed SNMP community field displayed for serial RPCs
- Fixed deleted UPS, RPC, EMD & Host connections stay in Managed Devices
- Fixed KCS61xx deleting and re-adding UPS requiring reboot
- Fixed enviromon can only be run by root
- Fixed KCS61xx IPMI custom config not saving in graphical control panel
- Fixed ‘Backup’ button displaying for unprivileged users
- Fixed alarm Sensor SNMP alert requiring reboot to reset
- Fixed UPS shut down behaviour on low battery

- Fixed CM4001 network RPC and UPS sensor graph
- Fixed network RPC -> Log Connections not being set
- Fixed RPC driver not stopping when RPC Connection is deleted
- Fixed KCS61xx embedded VNC client doesn't show the taskbar
- Fixed NTP running after reboot when NTP is disabled
- Fixed KCS61xx default system name
- Fixed NUT extra driver zip and tar files distribution
- Fixed connecting to serial by port number after upgrading

2.8.0 (June 11, 2009)

This is a production release.

Enhancements

- Added wireless network support
- Added ability to run a custom script after any configurator runs
- Added remote and local USB configuration backup and restore
- Added ability to set alternate user defined default configuration
- Added network bridging capability
- Added management, logging and alerting of UPSes connected via remote hosts
- Added support for multiple email recipients per single alert

Fixes

- Fixed performance issues up when triggering many simultaneous alerts
- Fixed excessive environmental logging when system time changes
- Fixed HTML formatting of tabs and blank cells
- Fixed erroneous appending and truncation of log files
- Fixed Citrix ICA not launching on the KCS
- Fixed Statistics -> Routes formatting
- Fixed sensor graph not displaying for UPSes with spaces in their names
- Fixed UPS power status email and SNMP alerts
- Fixed nagios-plugins check_ups incompatibility with NUT

2.7.1u1 (May 15, 2009)

This is a patch release.

Enhancements

- Added environmental monitor support for the KCS61xx family

Fixes

- Fixed environmental SNMP alerts
- Fixed changing system name not setting hostname

2.7.0 (April 8, 2009)

This is a production release.

Enhancements

- Added per-user RPC outlet permissions
- Added hot key power menu

- Added RPC outlet alerts
- Added support for SNMP RPCs
- Added support to associate host, serial and power using Managed Devices

Fixes

- Fixed editing a networked RPC causes it to be removed
- Fixed editing network hosts deletes all networked RPCs
- Fixed environmental monitor scheduling
- Fixed host visibility through web UI
- Fixed sensors stalling when a EMD/RPC/UPS doesn't respond
- Fixed RPC/UPS logs page taking too long to display
- Fixed port labels not displayed on the users page
- Fixed newly added Powerman-controlled RPC startup
- Fixed uncontactable sensor logs variable as 0
- Fixed incorrect SMTP settings causes email alerts to retry forever
- Fixed web UI default SSL certificate needs updating
- Fixed Nagios configurator always re-runs firewall rules
- Fixed firmware upgrading CGI doesn't display footer properly
- Fixed Manage -> Power buttons are displayed twice
- Fixed tabs needed for Network, Serial, Power under Manage -> Devices
- Fixed firmware upgrade page shows "Unknown" in page heading

2.6.1u2 (February 27, 2009)

This is a patch release.

Fixes

- Fixed short host logs not being displayed
- Fixed UPS log multiple status formatting
- Fixed Powerman-controlled RPC outlet offset
- Fixed switch monitor and VLAN tool file permissions

2.6.1u1 (February 12, 2009)

This is a patch release.

Fixes

- Fixed environmental page adding unnecessary dry contact alarm config
- Fixed environmental alerts require logging to trigger
- Fixed no environmental status until logs first written
- Fixed environmental alert counter not counting alarms
- Fixed EMD names with spaces being allowed
- Fixed multiple NTP daemons running at once
- Fixed name of ifup script to reflect multiple network interfaces
- Fixed link to DHCP server not displayed on IM4216-2
- Fixed timezone incorrect after reboot
- Fixed bogus error message after upgrading and clicking logo
- Fixed several UI wording fix ups

2.6.1 (January 20, 2009)

This is a patch release.

Enhancements

- Added unauthenticated telnet access for serial ports
- Added port logs with 1/100th second timestamp

Fixes

- Fixed network switching problem on large networks
- Fixed interface failover alerts (manual config only)
- Fixed firewall rules run multiple time when failed over

2.6.0u1 (December 19, 2008)

This is a patch release.

Fixes

- Fixed environmental status alert formatting
- Fixed editing users when no hosts are enabled
- Fixed emails addresses with dashes being rejected as invalid

2.6.0 (December 14, 2008)

This is a production release.

Enhancements

- Added support for Baytech IPDUs
- Added support for SNMP/XML network UPSes
- Added remote UPS log storage
- Added RPC Connections GUI
- Added SMS via email gateway alert method
- Added environmental monitor support
- Added environmental, UPS and RPC log graphing
- Added simplified cascading setup

Fixes

- Fixed maximum SSH sessions dropping below 48
- Fixed pmshell slow start up time
- Fixed upgrading from 2.2.3 reverting to DHCP client mode
- Fixed UPS services not restarting when DHCP address changes
- Fixed UPS Connections under System menu instead of Serial & Network
- Fixed GUI becomes slow with many users and ports
- Fixed group accessible hosts not retrievable by SDT Connector

2.5.1 (January 30, 2009)

This is a patch release.

Enhancements

- Added unauthenticated telnet access for serial ports
- Added environmental monitor support
- Added port logs with 1/100th second timestamp

Fixes

- Fixed timezone incorrect after reboot

2.5.0u3 (September 24, 2008)

This is a patch release.

Fixes

- Unable to add more than 4 users via remote authentication
- Unable to access more than 10 cascaded serial ports per slave simultaneously

2.5.0u2 (September 4, 2008)

This is a patch release.

Enhancements

- Added support for the KCS61xx family

2.5.0u1 (August 15, 2008)

This is a patch release.

Fixes

- Fixed menu issue with group permissions
- Fixed RAW mode issue with IPv6
- Fixed memory leak in portmanager
- Fixed trusted Networks issue with IPv6
- Fixed frame in a frame bug triggered by cascading

2.5.0 (July 25, 2008)

This is a production release.

Enhancements

- Added IPv6 support
- Updated Management Console GUI look and feel
- Improved network status page
- Automatically insert equals between UPS driver option and argument
- Updated network page nomenclature

Fixes

- Fixes for adding and removing users from groups
- Fix network settings migration from 2.3.x
- Fix for enabling monitored UPS

2.4.2u1 (June 25, 2008)

This is a patch release.

Enhancements

- Brought LDAP in line with RADIUS and TACACS off-box authentication

Fixes

- Fixed UPS alerts page wording
- Fixed USB options being available on CM41xx GUI

2.4.2 (June 23, 2008)

This is a patch release.

Enhancements

- Added off-box authentication using RADIUS and TACACS
- Added UPS management and monitoring network services
- Added UPS integration into SDT for Nagios
- Added graphical UPS status monitoring
- Added UPS status logging
- Added UPS alert mode
- Added option to restrict serial access to one user at a time

Fixes

- Fixes unnecessary USB debug messages being displayed
- Fixes cascade connections to remote ports droped on reconfigure
- Fixes IMG4004-5 low-speed USB device detection

2.4.1 (May 7, 2008)

This is a production release.

Enhancements

- Added serial port clustering/cascading support
- Added SDT for Nagios support
- Added Nagios alert method
- Added Nagios host alive checks
- Added alerts support for multiple SNMP servers
- Added SDT Connector option to Manage: Terminal

Fixes

- Fixes Java terminal issues with Java 6
- Fixes not being able to add user and group with same names
- Fixes Wireshark host log compability
- Fixes issue adding many users
- Fixes issue adding many network hosts on CM400x
- Fixes overly restrictive PPP firewalling
- Fixes Nagios host checks overwriting other hosts' checks
- Fixes dial-in default route option not being set
- Fixes DHCP server on IMG4004-5
- Fixes issue with Nagios names that are long or containing spaces
- Fixes slow configuration loading speed issue
- Fixes incorrect default Nagios address on IMG4004-5
- Fixes "Unknown" failover interface being listed on IMG4004-5
- Fixes user added alert scripts not being run
- Fixes SDT SSH connection alerts not being triggered

- Fixes Management LAN not including OOBFO port on IMG4216-25
- Fixes additional Nagios host checks not being applied
- Fixes failover to internal modem
- Fixes alerts on serial port numbers > 32 not being triggered on CM4148

2.3.1u3 (October 20, 2007)

This is a patch release.

Fixes

- Fixes Network Host logging format problem.
- Fixes firewall incorrectly blocking traffic over modem and other PPP links.
- Fixes CDK build problems.

2.3.1u2 (October 16, 2007)

This is a patch release.

Enhancements

- Added SSH & HTTPS capability into Cayee firmware

2.3.1u1 (October 13, 2007) release.

This is a patch release.

Fixes

- Fixes DHCP client configuration migration issue.

2.3.1 (October 1, 2007)

This is a production release.

Enhancements

- Added Nagios support enhancements.
- Added Management LAN / OOB / Failover support for IM4216-25 switch
- Added DHCP Server for Management LAN on IM42xx models
- Added meaningful status reports for IP Power 9258
- Added APC PDU support to power system
- Added Server Technology CDU support to power system
- Added the ability to propagate Host descriptions to SDTConnector

Fixes

- Fixes adding multiple groups with the same name
- Fixes IP Management Console page timing out
- Fixes root not being permitted to SDT everywhere
- Fixes admin members SDT privileges
- Fixes Japanese Time Zone
- Fixes Java SSH Terminal applet not correctly displaying the last line of text
- Fixes non-root user connecting to Local Services via SDTConnector
- Fixes Traceroute
- Fixes broadcast address not being configured properly on interfaces
- Fixes a bug where all serial ports were configured for SDTConnector

2.2.3 (April 12, 2007)

This is a patch release.

Enhancements

- Added Nagios support.
- Added a serial console selection menu when connecting to portmanager.

Fixes

- Fixes 8 maximum connections to any particular TCP port.
- Fixes USA daylight savings changes.
- Fixes some malformed HTML in Management Console pages.
- Fixes non-root access to portmanager.
- Fixes group authorization privileges.
- Fixes the portmanager login script for non-root users.
- Fixes RFC-2217 server accepting subsequent connections.
- Fixes configuration corruption when changing the system password.
- Fixes SDT access for non-root users.
- Fixes corruption of Group configuration when editing SDT hosts.
- Fixes TACACS+ not being selectable from the Management Console.
- Fixes cron updates needing a reboot to become active.
- Fixes ping for non-root users.
- Fixes IPMI for devices not requiring a username and/or password.
- Fixes default escape character for portmanager sessions.
- Fixes Management Console allowing blank passwords for non-local authorization
- Fixes SNMP server not starting when enabled.
- Fixes TFTP server not starting when enabled.

2.2.2 (February 8, 2007)

This is a patch release.

Enhancements

- Added SSH key upload capability to the Management Console
- Added SSH support to RFC-2217 & Raw TCP serial tunnel clients.

Fixes

- Fixes a problem where innitab entries were being truncated.
- Fixes having to reboot before portmanager picks up new accumulation periods.
- Fixes spurious data being transmitted over Raw TCP tunnel on reconnect.

2.2.1 (November 20, 2006)

This is a production release.

Enhancements

- Added Network Host session connection and traffic logging.
- Added Network Host connection alerts.
- Added UDP services to SDT Network Hosts
- Added customizable TCP/UDP services to SDT hosts.

- Added group based authentication for consoles.
- Added support for IPMI capable network devices.
- Added non-root access to local system shell.
- Added Terminal Server support via the Management Console (getty configuration)
- Added Management Console support for LDAP BINDDN and BINDDN password.
- Added Rose UltraPower board support.
- Added a command line tool to perform power cycling with.
- Added an RFC-2217 client.
- Added scriptable console login banner.
- Added RS422 option in the Management Console (as well as RS485)
- Added IP Failover for the IM42xx.
- Added USB Flash Drive logging for the IM42xx.
- Added Internal Modem configuration for the IM42xx.
- Added TFTP Server for the use with the USB Flash drive on the IM42xx.
- Added more system details per Management Console page.
- Turn off insecure services such as HTTP & Telnet by default.

Fixes

- Fixes a problem with TACACS+ support.
- Fixes a problem with LDAPS support.
- Fixes a problem where mgetty log was filling up temporary file system.

2.1.0u7 (November 1, 2006)

This is a patch release.

Enhancements

- Added preconfigured support for IP Power 9258 power strips.

2.1.0u1 (May 9, 2006)

This is a patch release.

Fixes

- Fixes a problem where 2.1.0 was unable to set 2-Wire (half-duplex) RS485 signalling correctly.

2.1.0 (March 23, 2006)

This is a production release.

Enhancements

- Added the ability to send SNMP & SMTP alerts/traps based on login/logout, serial signal changes & text pattern match events.
- Added tailoring of facility / level for syslog on each console.
- Added the ability to add access to all ports for a user with one click.
- Added an SSH terminal applet for connecting to a console via the UI.
- Added the ability to customize escape character for pmshell.
- Added the ability to override default inetd settings.
- Added support for RFC-2217 to use the local port settings.

2.0.9 (December 12, 2005)

This is a patch release.

Enhancements

- Added media-independent interface configuration for networking.
- Added access to portmanager via TCP port 22 using the following methods:
  - SSH to `username:port02@opengear.address`
  - SSH to `username:serial@opengear.address` for a port selection option.
- Added the ability to change the TCP port base for serial port access.
- Added support for CM4002 local console mode toggling.

2.0.8 (November 18, 2005)

This is a patch release.

Enhancements

- Added Secure Desktop Tunnelling for remote VNC / RDP / Citrix access.
- Added a mechanism for editing multiple serial ports characteristics simultaneously.
- Added the ability to view serial port history via pmshell commands.
- Added a “System Location” field to the Management Console.
- Added slow baud rate support to the Serial Port Manager.
- Email alerts no longer need a configured DNS environment to send mails.

2.0.6 (August 2, 2005)

This is a patch release.

Enhancements

- Added the ability to set IP via ARP
- Added place for users to hook in startup items
- Turned off the “Connected to portXX” message
- Changed dialin support to use mgetty
- Updated console driver to support TIOCMBIC
- Increased available memory footprint in CM41xx (was only reporting having 32M RAM) and this was limiting 4148 to 30 concurrent ssh connections
- Updated passwords protection so they are not stored in plain text in the XML configuration
- Changed UI in: “Serial Port->Users” to provide a summary view of User configuration “Alerts & Logging->Serial Port Log” where system log page referred to “NFS Server” “Administration->Date & Time” to reposition timezone form and fix system time display “Network->Dial-In” to allow user-specified init script for modems

Fixes

- Fixed problem with UI syslog output not escaping HTML characters
- Fixed a modem answering but not connecting problem

2.0.4u1 (July 7, 2005)

This is a patch release.

Fixes

- Fixed remote logging via CIFS (windows file sharing) which now formats data in an MS

Windows compatible format.

2.0.4 (July 2, 2005)

This is a patch release.

Enhancements

- Added user labelling for serial ports.
- Added a serial port log buffer display to the Management Console.
- Changed the default flow control for external ports from hardware to none.
- Changed the Management Console “Statistics” sub-menu to “Status”.

Fixes

- Fixed a permissions problem with non-root users performing SSH public key authentication.
- Fixed a defect with serial port diagnostic software interacting with the Port Manager service.
- Fixed dial-in user-interface so secret file could never contain a blank secret.
- Fixed dial-in user-interface configuration of the PPP daemon for software flow control.
- Fixed a defect in the Port Manager service which was incorrectly denying access to serial ports 33 - 48 on the CM4148.
- Fixed serial port log buffering to only store TX log for serial ports it is configured to.