RELEASE NOTES

LIGHTHOUSE

VERSION 22.11.1

INTRODUCTION

This is a recommended production software release for Lighthouse. Please check the [Lighthouse User Guide](#) for instructions on how to upgrade your Lighthouse.

SUPPORTED PRODUCTS

- Lighthouse

KNOWN ISSUES

- User Interface on Firefox reverting to a previous version after upgrade:
  - When using Firefox, if the user interface reverts to a previous version after upgrading a lighthouse, users can resolve the issue by clearing their browser cache (settings > privacy & security > cookies and site data > clear data).

DEFINITIONS

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.

22.11.1 (November, 2022)

This is a patch release.

Defect Fixes

- Fixed issue where the User Interface was being cached and reverting to a previous state after Lighthouse upgrades on Firefox
- Fixed issue where node enrollments weren't being counted against Licenses correctly

22.11.0 (November, 2022)

This is a production release.

Features

- Added Mix n Match Subscription support:
  - Allowing up to 2 Subscriptions to co-exist on a Lighthouse to leverage feature sets on different nodes
  - Improved functionality and support for adding and viewing Subscriptions
  - Subscription Assignment system to allow nodes to leverage features from applied Subscriptions

Enhancements

- The Jobs page now has the ability to filter jobs by status (All, Success, Failed, Pending)
- Hardened Secondary Lighthouse upgrading process when encountering upgrade failures
- Improved node-info function to attain node connection states, reflecting what is present on the Lighthouse Dashboard - For further info use the command "node-info -h" in the CLI
- Cellular Health failover status reporting has been improved to be more consistent
- Improved reporting of SIM status when cellular interface is disabled
- Improved node VPN connection processes during Lighthouse start-up
- Improved handling of OGCS cell health response when the modem is rebooting (due to changing SIMs)
- Removed support for old, no-longer-recommended ssh encryption functions
  - Note that these changes do not get applied to upgrading systems
  - To manually apply this change, follow this [Opengear Zendesk article](#)

Defect Fixes

- Fixed issue where deleting smart groups and managed device filters would delete attached groups. Users now see an error message blocking the process until groups are detached
- Fixed issue where Lighthouse upgrades were failing when users that exist have smart_group_ref unset
- Fixed issue with node upgrade sometimes not displaying firmware filenames correctly
- Fixed issue where pmshell access was missing for users with a managed device filter but no smart group filter (ie. "All Nodes")
- Fixed issue where skip to main content accessible button did not work for NetOps pages
- Fixed IP address range validation for LHVPN range setting
- Fixed issue where editing group templates can duplicate groups
- Fixed issue where SNMP traps for secondary replication were misaligned with MIBs
- Fixed an issue where cellular IP addresses for NetOps Console Servers would persist after the cellular connection went down
- Fixed certain scenarios for when NetOps Console Servers did not show up on the cell health dashboard
- Fixed issue where non-admin user couldn't see support report option
- Fixed the permission for read only users to edit smartgroups
- Fixed issue with LDAP configuration validation where the LDAP Bind DN field could not be left blank
- Fixed issue where the Search field on the port logs page was missing
- Fixed issue where external end points for IPv6 were not being populated automatically on Azure Instances

- Fixed issue where you could not drag and drop multiple files onto the Node Firmware file manager
- Fixed issue where Node ID parameter was not part of the free text search

22.Q1.2 (September, 2022)

This is a patch release.

Enhancements

- Accessibility improvements to raise standards of keyboard and screen reader support
- Minor interface and input changes to improve user experience and flow when accessing parts of the UI

22.Q1.1 (August, 2022)

This is a patch release.

Enhancements

- Managed Device Filter parameters can now be combined using AND or OR in the Web UI

Defect Fixes

- Fixed intermittent multi-instance replication issue during upgrade
- Fixed a post-upgrade issue to 22.Q1.0 for remote authentication of groups with upper case characters
- Fixed logging into the Lighthouse UI using 2FA
- Fixed an issue affecting upgrades with a large number of nodes
- Fixed an issue which could result in user sessions being incorrectly logged out when the system is processing multiple requests for the same session

22.Q1.0 (June, 2022)

This is a production release.

Features

- Support for UI driven node firmware upgrades
- Support for CM 8100 nodes

Enhancements

- Accessibility improvements:
    - Improved keyboard navigation
    - Styling changes for focus items
- Increased the timeout for secondary Lighthouse upgrades
- Enhanced performance with better task prioritization
- Improved config validation error messages
- Improved network error handling
- Improved node backup error handling
- Expanded managed device filters support from smart groups to all nodes
- User can be enabled or disabled using ogpasswd without needing to change their password

Defect Fixes

- Resolved issues with events service that could cause it to stop
- Fixed issue where the 'root' user could be removed from the 'admin' group

21.Q4.2 (March 2022)

This is a patch release.

Defect Fixes

- Fixed issue where NetOps deployments could lose access to node information if the root user was disabled on non-azure deployments
- Fixed issue where NetOps deployments could lose access to node information on the Azure platform due to the root user being disabled
- Fixed an issue which could result in user sessions being incorrectly logged out when the system is processing multiple requests for the same session
- Fixed an issue where a node in the Lighthouse database with an unknown firmware version caused an upgrade to fail and rollback
- Fixed an issue where any users with Unicode characters in their description field could cause users to be locked out of Lighthouse
- Fixed a problem where usernames containing a full-stop/period caused an upgrade to fail and rollback
- Fixed a problem where a misconfigured node serial port could cause an upgrade to fail and rollback
- Fixed issue with missing serial port mode when config retrieving OM devices, this could cause an upgrade to fail and rollback

21.Q4.1 (February 2022)

This is a patch release.

Enhancements

- Enhanced Authentication logging for Lighthouse users logged in with SAML
- Improved Support Report information including AWS Targets
- Improved Monitor Nodes page to now apply user group managed device filters
- Improved node cell health status logic for more clear communication
- Adjusted colour scheme for Node Dashboard
- Disabled SSH links for Lighthouse users logged in using SAML

Defect Fixes

- Fixed issue where node upgrade command did not allow multiple nodes to be selected
- Fixed issue where smart groups did not allow more than 18 entries of criteria
- Fixed issue in RADIUS setup stopping save changes after port field selection

21.Q4.0 (December, 2021)

This is a production release.

Features and Enhancements

- WebUI SAML support added for Single Sign-on Identity Providers: Azure AD, Okta, and OneLogin - Review the 21.Q4 manual for setup instructions.
- Connected ports now displayed on Quick Search page with sorting and free text search support.
- Performance improvement for pmshell load times when the Lighthouse has a large number of nodes/ports.
- Improved failover login behaviour when using high latency remote AAA authentication.
- Lighthouse now detects and prevents duplicate enrolment attempts during node enrolment.
- Added additional support for FQDN usernames when using remote AAA authentication.
- Additional help/error messages added for when the user's browser is using a stale cache of the Web UI.
- Improved the error messaging for issues with 2FA token challenges.
- Added additional integrity checking to the creation of tags for enrolled nodes from bundles.
- Updated the error checking/reporting around LDAP CA certificates.
- Removed a number of static key ciphers from use by the WebUI and node proxies.

Defect Fixes

- Fixed the missing use of the hostname in the syslog for certain system messages
- Fixed refresh issue when accessing node proxies via saved hyperlinks in the Web UI.

21.Q3.0 (September, 2021)

This is a production release.

Features and Enhancements

- Node-upgrade CLI utility improvements and support for Operation Manager series devices
- Improved display of information and upgrade results
- CLI arguments and options preserved for backwards compatibility
- Additional arguments/options:
    - —firmware-file for selecting a specific firmware image instead of specifying a directory to search through
    - —product for selecting nodes by product family
    - —verbose for displaying log information (but not as much as with –debug)
- Added password verification when performing user changes for local Lighthouse users
    - This is applicable for Lighthouses configured to only use local auth
- Usernames including "." characters can now be used in Lighthouse
- Content Security Policy header has been implemented
- Updated the WebUI display for third party/digi passport nodes to show the node address
- Added support for a configurable remote AAA timeout value via the ogconfig-cli tool
    - Once your AAA auth has been set, use "ogconfig-cli auth.timeout #" to set the timeout in the CLI
- Improvements to Cell Health handling and display of the Failover status for nodes
- Added script to support for bulk-unenrolling of nodes - please contact support if you wish to utilize this script
- Added additional system status information to the Lighthouse support report
- Enabled support for the Carrier Grade NAT IP range (RFC 6598, 100.64.0.0/10) for LHVPN tunnels to Nodes

Defect Fixes

- Fixed an issue in which the default static IPv4 address was left in External Network Address list when the associated network interface is disabled
- Fixed issues with the smart group node-id search that had previously resulted in incorrect results when using the abbreviated id form (i.e. 1 instead of nodes-1) or viewing the results on the Console Gateway page
- Fixed an issue in which the "read_write" SNMP community field could not be cleared once set
- Fixed an issue with generic third party nodes which resulted in the port labels being assigned to the incorrect ports

21.Q2.1 (July, 2021)

This is a patch release.

Defect Fixes

- Fixed issue where Lighthouse couldn't receive firewall zone data from OM series devices on 21.Q1
- Fixed issue where Lighthouse could use incompatible upgrade files
- Fixed issue where multiple instance enrollment via alternate port still sends traffic to port 443

21.Q2.0 (June, 2021)

This is a production release.

Features and Enhancements

- Upgraded Yocto version to Dunfell
- Deprecated Python 2 in favor of Python 3 on Lighthouse
- Improved monitoring and error notifications for Multiple Instance Lighthouses
- Improved upgrade process and flow for Multiple Instance Lighthouses
- Improved enrollment and unenrollment process of nodes on Lighthouse
- Improved performance of cellular health reporting on Lighthouse
- IMEI, IMSI and ICCID reported for cellular health on UI and through REST API
- Added node ID and port ID to Lighthouse system logs
- Added sorting support through REST API for smartgroups endpoint
- Added sorting support through REST API for jobs endpoint
- Added sorting support through REST API for nodes endpoint
- Improved REST API backward compatibility
- Added MI diagnostics to support report
- Added versions support for Hyper-V powershell install script

Defect Fixes

- Fixed Lighthouse CVE issues
- Fixed issue with free text search not working for IP Addresses on node pages
- Fixed SSL problems with self-signed certs in web UI on Big Sur chrome
- Fixed issue where in 20.Q4.0 third party (Avocent) nodes can't connect with pmshell
- Fixed issue with multiple instance Lighthouse enrollments when the replication_user already exists
- Fixed cross site scripting vulnerability for script templates
- Fixed issue where rest_api_log process was logging with incorrect hostname
- Fixed issue with Lighthouse memory usage info in SNMP (slab memory)
- Fixed issue with enrollment bundle template ordering not being saved
- Fixed issue with LDAP configuration changes not getting saved
- Fixed issue with 7008 configuration not getting updated on Lighthouse
- Fixed issue where LDAP does not fall back to local authentication on failure
- Fixed issue where node-related redis keys are not deleted when node is unenrolled
- Fixed issue where Lighthouse console_gateway API doesn't always return address used for SSH links
- Fixed issue with RADIUS sending incorrect Service-Type
- Fixed issue where changing the node VPN on the Primary instance in a MI cluster does not check for vpn conflicts
- Fixed issue where Lighthouse generates invalid engine ID for SNMPv3
- Fixed issue with cell health when communicating with an OM device that has no modem
- Fixed issue where a user cannot deploy Azure Lighthouse without Public IP Address
- Fixed issue where hitting a node proxy URL when not logged in gives a 401 screen
- Fixed issue where Enrollment Token cannot contain special characters
- Fixed issue where port label with '%' breaks web terminal page
- Resolved Enrollment bundle UI issue for adding Netops modules
- Fixed issue where lh-client-connect script is too slow
- Fixed issue where Lighthouse on AWS becomes unresponsive after upgrading and then factory resetting

20.Q4.2 (May, 2021)

This is a patch release.

Defect Fixes

- Added storage of Azure configuration parameters to allow persistence after factory reset
- Fixed issue where Node Backup may be disabled after upgrading to 20.Q4.0, if it was configured on 20.Q3.0
- Fixed issue where replication on secondaries may be interrupted after promoting a secondary to primary
- Fixed issue where debugging log messages were being logged after enabling remote syslog
- Fixed issues with MI and node enrollment in various firewall configurations (combinations of NAT, external endpoints, alternate ports, etc.)
- Improved log handling of node config retrieval to not log spurious data
- Improved memory footprint by disabling some services if not enabled (eg. Zapier event notification)
- Improved memory usage by cleaning up database entries for old configuration updates
- Improved upgrade process in hosting configurations with non-standard device names (eg. /dev/vda, /dev/xvda)

20.Q4.1 (April, 2021)

This is a patch release.

Defect Fixes

- Fixed issue where remote syslog may debug log user credentials
- Improved framework logging handling of errors
- Added sanitization of framework logging stack traces
- Improved reliability of rollback process on failed upgrade
- Fixed handling and validation of custom HTTPS certificates
- Fixed issue with REST API endpoints fail when trailing slash specified
- Improved sanitization of REST API logging when non-standard content-type specified

20.Q4.0 (January, 2021)

This is a production release.

NOTE: This release includes major changes that can break NetOps functionality on Lighthouse. As such, it is highly recommended to upgrade NetOps modules to the latest version. (If the version of NetOps modules on Lighthouse does not match the required criteria, a banner is displayed on UI prompting the user to update the modules.)

Features and Enhancements

- Added ability to combine multiple smart group search conditions using logical 'OR'
- Updated default TLS version on Lighthouse to 1.2 and made it configurable using ogconfig-cli
- Improved Lighthouse security
- Improved Lighthouse user experience and usability
- Upgraded EmberJS to 3.16 LTS release
- Added static code analysis for security vulnerabilities
- Added granular group roles and permissions
- Upgraded Yocto version to Zeus
- Added capability to store and display console serial port logs
- Removed non inclusive language from Lighthouse code
- Added version checking for config restore
- Added node name to node backup file names
- Added support for ordering node tables by connection status
- Added capability to cleanup logs when disk is filling up
- Added warning banner to be displayed if NetOps modules are not compatible with this release of Lighthouse

Defect Fixes

- Fixed issue where cellular connectivity test does not work with alternate API port
- Fixed issue where node upgrade commands fail with LUA error
- Fixed issue where secondary Lighthouse nodes receive varying IP addresses on boot
- Fixed issue where Lighthouse sets default switch type to private on HyperV
- Fixed issue with multiple license handling on Lighthouse
- Fixed Lighthouse Zapier integration to add tags to events. If users are running Lighthouse Zapier app privately, please update with the latest packages
- Fixed issue where Azure Lighthouse could not be deployed without assigning public IP address

20.Q3.0 (August, 2020)

This is a production release.

NOTE: To support the improvements required for disk management, this version of Lighthouse requires a new 20.Q3 virtual machine to be deployed and a configuration backup and restore from at least 20.Q2.0 onto the new virtual machine. From this release onwards, the supported upgrade path will be from the last major release (or patch release of that major release) only. This will generally be from the previous quarter.

Features and Enhancements

- Add improved UI for viewing consolidated Node and Port information
- Add support for system notifications, with Zapier as the initial integration. More information can be found in this FAQ article; https://opengear.zendesk.com/hc/en-us/articles/360048367371
- Add support for more effective and extendable disk management in Lighthouse, utilising LVM
- Add UI for viewing results of system tasks, currently supported are registrations, enrollments, and configuration retrieval
- Add support for enrolling Digi Passport devices
- Improved REST API performance and stability

20.Q2.1 (July, 2020)

This is a patch release.

Defect Fixes

- Fixed Web Terminal problems (sometimes not loading properly or restarting)
- Fixed issue with spurious SNMP server restarts on secondary Lighthouses
- Fixed issue with SNMP not reporting node information accurately after restarting some system services
- Fixed issue with some Cell Health SNMP traps being sent, regardless of status change
- Fixed issue with log file partitions filling up due to excessively large log files
- Fixed issue with slow Web UI responsiveness if the private VPN range is changed from the default
- Fixed issue with incorrect response codes to console servers during enrollment with many parallel enrollments
- Fixed issue with many parallel enrollments becoming bottlenecked and timing out
- Fixed issue with config retrieval job failures on nodes with poor connectivity

20.Q2.0 (May, 2020)

This is a production release.

Features and Enhancements

- Add support for implementing password policies for users
- Add logging capability for CLI and REST API
- Improved UI look and feel
- Improved performance for node registration and enrollment process
- Improved REST API performance and stability
- Improved formatting for remote syslog messages
- Improved reporting of cellular health for nodes
- Improved reporting of issues during node communication for enrollment and config retrieval

Defect Fixes

- Fixed session creation when system is under high load
- Fixed some memory leak issues when system is under high load
- Fixed enrollment for some ACS Classic configurations

20.Q1.0 (February, 2020)

This is a production release.

NOTE: The minimum required RAM for Lighthouse is now 8GB from this release.

Features and Enhancements

- Add support for IPv6
- Add support for different remote authentication methods (eg. RadiusLocal, RadiusDownLocal, LocalRadius, etc.)
- Improved security - limit web server information exposure, and add cross-site scripting protection
- Improved UI look and feel (including Ember 3.12 upgrade)
- Improved REST API performance and scalability
- Updated base operating system distribution (new versions of many opensource packages, security fixes, etc.)

Defect Fixes

- Fixed two-factor authentication with SSH
- Fixed issue booting on ESXi (older hardware without DRNG random number entropy support)
- Fixed support for node cell health status and IP address display
- Fixed serial console gateway using delimiters and SSH pubkey together
- Fixed issue where promoted secondary Lighthouse instances can't enroll future secondary Lighthouses
- Fixed permissions issue when administrators try to delete syslog server configuration from Lighthouse
- Fixed various UI bugs (display, input field validation, etc.)
- Fixed issue with web terminal session remaining when UI logs out
- Fixed intermittent config server sync error when using many secondary lighthouses (causing failed web logins)
- Fixed issue with node backups not being visible between different version installs

19.Q3.3 (October, 2019)

This is a patch release.

Defect Fixes

- Fixed Netops Web UI support on upgrade
- Improved Multi-Instance processes to allow for slower networks/systems
- Improved configuration validation routines

19.Q3.2 (September, 2019)

This is a patch release.

Defect Fixes

- Fixed handling of large queues of system configuration updates

19.Q3.1 (September, 2019)

This is a patch release.

Defect Fixes

- Fixed issue with web terminal sessions persisting over reboots
- Fixed problems preventing secondary Lighthouse enrollment over alternative HTTPS ports
- Fixed problems with 3rd party nodes getting removed during secondary lighthouse promotion
- Fixed issue where many rapid node config updates could fill the disk
- Fixed issue where a high number of database updates used more disk than necessary
- Fixed issue with secondary Lighthouses in AWS not upgrading cleanly

19.Q3.0 (July, 2019)

This is a production release.

Features and Enhancements

- Add support for multiple secondary Lighthouse instances
- Added numerous improvements to multi instance upgrades
- Added numerous improvements to multi instance node enrolments
- Add support for deploying Lighthouse on AWS
- Add support for backing up and restoring Lighthouse configuration
- Add support for backing up managed node configuration (requires Console Server v4.6+)
- Add support for remote authentication using LDAPS
- Add node-id in the node list display in Lighthouse UI
- Add support for SSH links to nodes via node-id
- Add support for displaying third party nodes in node-info on CLI
- Improved Licence expiry banner display
- Improved node status dashboard widget links to more useful filtered list of nodes
- Improved SNMP traps sent for node connection/disconnection

Defect Fixes

- Fixed an issue where Lighthouse was reporting negative time in "Last Changed" field
- Fixed an issue with memory management of ogconfig-srv
- Improved processes around node connection while adding dependant secondary Lighthouse instances
- Fixed Lighthouse not listening correctly on alternative enrollment port

19.Q2.2 (June, 2019)

This is a patch release.

Defect Fixes

- Fix issue with many (> ~500) 3rd party console servers where some would not start up correctly
- Fix potential upgrade issue from versions pre-5.3.0 under certain circumstances

19.Q2.1 (June, 2019)

This is a patch release.

Defect Fixes

- Fix issue with multiple overlapping config retrieval operations occasionally crashing
- Improve speed of configuration for large numbers of 3rd party nodes

19.Q2.0 (May, 2019)

This is a production release.

Features and Enhancements

- Add support for Azure deployment
- Add ability to upgrade multi-instance Lighthouse deployments using a provided script
- Add license expiry warnings. Expired licenses will put Lighthouse into a read only operational mode
- Licenses are now uploaded as a file
- Lighthouse now supports retrieval and reporting on cellular health status for enrolled nodes
- Updated base operating system, new versions of many opensource packages
- Fixed potential vulnerability in web terminal
- Add ability to filter nodes by connection status
- Add script to set static IP (for support assistance)

Defect Fixes

- Scalability improvements for third party enrollment
- Fix issues where sudoing as root may not grant the expected permissions
- Fix issue where it was not possible to search by internal VPN address
- Fix issue where secondary lighthouses could lose their network configuration upon enrollment

5.3.0 (February, 2019)

This is a production release.

Features and Enhancements

- Add support for adding a secondary Lighthouse for the purpose of redundancy and failover
- Add support for changing the IP range to use for the internal Lighthouse VPN
- Add support for applying authentication templates to OM22xx devices
- Add support for applying user and group templates to OM22xx devices
- Third party node authentication settings can now be modified using the REST API
- Improved network validation
- Updated base operating system, new versions of many opensource packages

Defect Fixes

- Fix display error in ogconfig-cli where references displayed the wrong target path
- Fix authorization error for users with short usernames

5.2.2u1 (December, 2018)

This is a patch release.

Defect Fixes

- Improved performance for script template push to OpenGear console server
- Improved reliability of authentication

5.2.2 (September, 2018)

This is a production release.

Features and Enhancements

- Upgrade OpenSSH to 7.7p1
- Add OM22xx Operations Manager enrollment support and basic management
- Add support for running NetOps Automation Modules
- Add Secure Provisioning module for NetOps Automation
- Add expect to the Lighthouse CLI for custom scripting
- Add MOTD banner post-login that displays IP address information
- New deployments include a secondary drive for NetOps Modules. Upgrades of existing deployments will need to manually add this disk.
- Update the Web UI to use Ember 2.16
- Add support for running Docker containers on Lighthouse

Defect Fixes

- Improve handling of node's cellular addresses (requires console servers to be version 4.4 or above)
- Fix an rare incorrect authentication failure in the REST API
- Fix incorrect error when on script template PUT REST API endpoint
- Fix spurious log messages when connecting via SSH as an Admin user
- Fix incorrect error when invalid address entered into Authentication template UI
- Fix /system REST API endpoints being visible by Node Admin users
- Fix incorrect error when invalid arguments passed to node-copy cli
- Fix syslogd not restarting if the process exits
- Fix references in ogconfig-cli displaying with off-by-one indices

Security Fixes

- CVE-2017-17080
- CVE-2017-16830
- CVE-2017-16831
- CVE-2017-16832
- CVE-2017-17123
- CVE-2017-16828
- CVE-2017-17125
- CVE-2017-17122
- CVE-2017-17124
- CVE-2017-17121
- CVE-2017-16829
- CVE-2017-16827
- CVE-2017-16826
- CVE-2018-5390
- CVE-2018-5391
- CVE-2018-6323

5.2.1u1 (July, 2018)

This is a patch release.

Defect Fixes

- Fixed snmpwalk not listing all nodes.
- Fixed upgrade to 5.2.1 failing when LDAP auth is configured.

5.2.1 (June, 2018)

This is a production release.

Features and Enhancements

- The following endpoint namespaces have been modified in v3 of the REST API, so v1, v1.1, and v2 have been deprecated and will no longer be updated. As the endpoint's functionality has changed, there may be changes required to user programs utilising the REST API. Refer to the REST API documentation for v3 for example request/response bodies. Deprecated endpoints since 5.2.0u1:
- /v2/auth
- /v2/templates In general, prefer the latest version of the REST API (v3) in your own programs as this ensures the latest functionality is available.
- Add SNMP MIBs for Lighthouse 5.
- Add support for SNMP TRAP/INFORM messages on node connection status changes.
- Improve password handling in ogconfig server.
- Add support for Google Compute Engine deployment.
- Extend functionality for User and Group templates.
- Allow node users to have rights limited to specific ports on nodes.
- Add support for Console Gateway SSH links to use specified external address.
- Add support for exporting syslog to remote server.
- Add support for LDAP ignore_referrals.
- Default LHVPN timeout reduced to 60 seconds, and added config option to allow custom value.
- Changed sidebar ordering for sub-elements.
- Add support for configuring number of nodes/ports per page.
- Web UI pop-ups can now be closed by hitting escape and submitted by pressing enter.

Defect Fixes

- Fixed warning bar not showing when licence limit is exceeded.
- Fixed third party nodes causing a config sync error.
- Fixed UI allowing duplicate external endpoints.
- Fixed deleted template appearing on UI.
- Fixed DOM error on Remote Authentication page.
- Fixed success message not showing on bundles page.
- Fixed race condition with script templates.
- Fixed error when disabling enrolment only REST API port.
- Fixed Cisco 2900 failing if MOTD set.
- Fixed error on REST API Port endpoint.
- Fixed memory leaks in REST API.
- Fixed pmshell crashing if columns set to 1.
- Fixed third party node config sync error.
- Fixed rare segfault when deleting users.
- Fixed core daemons from having multiple instances.
- Made delete icon in web-ui consistent.
- Fixed error when editing Authentication templates.

5.2.0u1 (April, 2018)

This is a patch release.

Defect Fixes

- Fix issue with session IDs

5.2.0 (March, 2018)

This is a production release.

Features and Enhancements

- The following endpoint namespaces have been modified in v2 of the REST API, so v1, and v1.1 have been deprecated and will no longer be updated. As the endpoint's functionality has changed, there may be changes required to user programs utilising the REST API. Refer to the REST API documentation for v1.1 for example request/response bodies. Deprecated endpoints since 5.1.1u1:
- /v1.1/auth
- /v1.1/search
- /v1.1/nodes/smartgroups
- /v1.1/ports
- /v1.1/support_report
- /v1.1/services/console_gateway In general, prefer the latest version of the REST API (v2) in your own programs as this ensures the latest functionality is available.
- Large performance improvements across the board, allowing for larger numbers of nodes to be used on a single Lighthouse instance
- Updated base operating system, new versions of many opensource packages
- Add support for Hyper-V deployment
- Add support for configuring an enrollment-only HTTPS REST API endpoint
- Add managed device filters to UI and REST API
- Add search support in ogconfig-cli
- Make Console Gateway SSH links use the configured External Network Address
- Add a syslog entry when a new local user is created
- Add support for mounting additional filesystems for bulk file storage
- Add link to download the user manual
- License body is now hidden from UI
- Add human readable format for uptime in support report
- Add SNMP service and reporting
- Add log rotation to /var/log/wtmp

Defect Fixes

- Manually installed SSH keys are no longer breaking shell access
- Fix multiple issues caused by nodes with duplicate names
- Disable TCP timestamps
- Use SHA512 instead SHA1 in certificate generation
- Deleting a CSR now removes it from the SQL database
- Fix a failure with Avocent 3rd-party enrollments when using non-default serial port settings
- Fix issues with AAA logins and add more error reporting
- Fix crash in ogadduser when referencing a non-existent group
- Fix Administration/System button not responding in IE11
- Fix uncommon error message in syslog when unenrolling 3rd party nodes
- Fix upgrade issues that could occur from 5.1 to 5.1.1u1
- Fix lhadmin users not being able to run node-command
- Fix last successful config push losing status
- Fix lack of copy/paste in the Web Terminal

5.1.1u1 (December, 2017)

This is a patch release.

Defect Fixes

- Fix for a critical issue that prevented nodes being enrolled or coming back online after a system reboot in some circumstances.

5.1.1 (December, 2017)

This is a patch release.

Features and Enhancements

- The following endpoint namespaces have been modified in v1.1 of the REST API, so v1 has been deprecated and will no longer be updated. As the endpoint's functionality has changed, there may be changes required to user programs utilising the REST API. Refer to the REST API documentation for v1.1 for example request/response bodies.
- Deprecated endpoints:
- /v1/nodes
- /v1/system
- /v1/auth
- /v1/bundles
- /v1/users
- /v1/groups
- /v1/templates In general, prefer the latest version of the REST API (v1.1) in your own programs as this ensures the latest functionality is available.
- (Breaking change) AAA groups are now case-sensitive when mapping to local group authorization. This will only effect AAA groups that use capital letters.
- Change node names to be automatically synchronized to console server's hostname (needs CS firmware 4.1.1)
- Add support for pushing templated bash scripts to nodes (needs CS firmware 4.1.1)
- Add support for configuring a CLI session expiry
- Add Smart Group support to node-command and associated tools
- Improve performance of our REST API
- Improve usability of our Console Port Access page
- Add more examples to our REST API documentation
- Add ability for AAA-users to be defined locally without password
- Allow local user group names to contain more special characters
- Add netgrp user group that will contain all AAA users, allows for default permissions for AAA users
- Default netgrp permissions to Lighthouse Admin
- Add support for templates to be associated with bundles for automatic configuration application on enrollment
- Add information about current user to top bar in UI
- Add vmxnet3 driver for better VMWare virtualization support
- Add reporting about configuration template push status to node details
- Change default Lighthouse VPN MTU to be 1400
- Add ability to change the MTU for the Lighthouse VPN
- Add REST API endpoint to expose current firmware and API versions
- Add better node status reporting in the UI
- Update our HTTPS ciphers and protocols to comply with Mozilla Server Side TLS Recommended guidelines
- Add command line support for scheduling cron jobs

Defect Fixes

- Fix assorted authorization issues
- Fix issues caused when date is set to the past
- Fix failing configuration synchronizations causing enrollment to fail
- Fix inconsistencies in node terminology in the UI

- Fix crashes in ogconfig-cli
- Fix excess incorrect failure messages in syslog during successful enrollment
- Fix syslog error messages during unenrollment of 3rd party console servers
- Fix rare issue where the preflight check would list no nodes
- Fix browser window title incorrectly persisting after leaving console gateway page
- Fix ability to disable the root user
- Fix incorrect pmshell error message when no nodes selected
- Fix system details popover incorrectly sticking on screen
- Fix TACACS authentication hang when duplicate remote groups were discovered
- Fix ability for console servers with _ in hostnames to be enrolled
- Fix TTY parsing for Cisco 2900 3rd party console servers
- Fix incorrect usage information for node-upgrade
- Fix issue where long-lived LH5 instances would stop responding to REST API requests
- Fix TACACS Login authentication
- Fix Web Terminal copy and paste issues
- Fix rare configuration retrieval failing on node descriptions
- Fix configuration template pushes that raise errors never being marked as complete
- Fix remote AAA Lighthouse Admin users being unable to delete templates
- Fix Web UI Proxy when LH5 is being an external DNAT rule
- Fix user UID conflicts after switching from remote to local authentication schemes
- Fix memory leaks in configuration backend
- Fix memory leaks in our REST API
- Fix the disable multiple button not working on the Users page
- Fix left side bar inconsistencies
- Fix missing error messages when trying to add 3rd party nodes with more than 400 serial ports
- Fix enrollment breaking when secure HTTPS ciphers are configured on the console server
- Fix enrollment failures if remote node has portshare password set
- Remove autorefresh on Preflight and Template push pages

5.1.0 (August, 2017):

This is a production release.

Features and Enhancements

- (Breaking change) The Lighthouse OpenVPN connection now runs on UDP. This means Lighthouse 5.1.0 is only compatible with Opengear Console Servers version 4.1.0+.
- Add functionality for pushing configuration templates to groups of Opengear devices. Currently supported are Group and AAA templates.
- Add node-upgrade command line utility.
- Add system upgrade to the web UI. Users are able to upload a new system image or provide a URL where the file is hosted.
- Add license restrictions to the Lighthouse. Without a license, the Lighthouse is in evaluation mode with a limit of 5 enrolled nodes. Users can purchase licenses that increase that limit and give access to enroll third party devices.
- Add automated migration for configuration when upgrading to new Lighthouse versions.
- Add support for specifying multiple endpoints to access a Lighthouse device (from an Opengear Console Server) and custom ports on the Lighthouse that will listen for incoming requests.
- Add device support for non-Opengear devices (known as third party devices) with native configuration support for: – Avocent ACS 6000 & 8000 – Avocent Classic – Cisco ISR2921
- Add Console Gateway page with responsive searches over devices' serial ports
- Improved pmshell command line utility.
- Improved the config cli for manipulating Lighthouse configuration (ogconfig-cli).
- Improved the speed and stability of the configuration server and REST API.
- Improved the Web UI for usability.
- Improved configuration validation and feedback to client.
- Improved RAML documentation for the REST API.

Defect Fixes

- Users are redirected correctly after logging in.
- Fixed some stty issues around remote CLI sessions.
- Improved feedback when user attempts to access commands without suitable permissions.
- Free text search with multiple terms
- SSH custom delimiter parsing
- Disabling an interface could cause other interfaces to go down
- Group names can now contain a dash
- Console Gateway conventions are now adhered to for specifying username and port labels
- Improved shutdown & restart times
- Fixed enrollment of Console Servers with ports in Serial Bridging and Terminal Server mode
- Hostname and system time will now change in syslog when the system is updated
- A user's home directory will now be deleted when the user is deleted
- REST requests proxied via the Lighthouse to the Console Server will now be forwarded correctly by the Lighthouse
- Fixed an enrolment failing to complete if a node was approved too early in the registration stage. A node can now be approved at any point without breaking the enrollment.

5.0.0 (April, 2017):

This is a production release.

NOTE: This is a ground up rewrite of Lighthouse.

Features and Enhancements

- Add modern HTML5 Web UI
- Add streamlined user and groups mechanisms
- Add secure OpenVPN connections to remote nodes
- Add REST API for external integration and control of LH5
- Add HTML5 local web terminal
- Add HTML5 Console Gateway terminals
- Add 'Smart Groups', a way to group managed nodes through saved searches over their configuration and associated searchable tags
- Add support for searchable tags to be added to managed nodes
- Add a quick search bar at the top of every UI page that lists managed nodes
- Add initial and on-going synchronization of node serial port configuration, avoiding the need to 'Retrieve Managed Devices'
- Add streamlined enrollment methods via DHCP ZTP, USB, or Web UI
- Add consistently validated configuration backend
- Add tab-completable config cli