RELEASE NOTES

LIGHTHOUSE

VERSION 25.04.2

INTRODUCTION

This is a recommended patch release for Lighthouse. Please check the Lighthouse User Guide for instructions on how to upgrade your Lighthouse.

DEFINITIONS

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

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

KNOWN ISSUES

- Due to a current limitation in Lighthouse, once a subscription is upgraded to either a Core or Enhance, the node filter will no longer return nodes with criteria that matches any NetOps module. It is recommended to push the disable NetOps module templates using the node filter before applying the new subscription. If the subscription has already been applied, it is recommended to push the disable NetOps module templates to all nodes by clearing the node filter and selecting all when pushing config templates. Users may also navigate to the Nodes page and use the “Template Run Status” column to determine which have had Netops templates pushed to them. [IM-17457]
- Ogconfig crashes when accessing the NTP server list. It is recommended to remove the NTP server in Lighthouse. [IM-18411]
- RADIUS login requests use 127.0.1.1 as the NAS-IP-Address, which can cause downstream RADIUS server policies to break and reject the authentication request. [IM-18552]

DEPRECATION NOTICE

- Support for DSA-signed SSH keys is being deprecated and will be removed in a future version of Lighthouse.
- Support for the following APIs are being deprecated.

Deprecated Endpoint	Replacement Endpoint
/interfaces GET	/system/network GET
/interfaces/:id GET	/system/network/:lighthouse_id GET
/interfaces/:id PUT	/system/network/:lighthouse_id PUT
/system/external_endpoints GET	/system/network GET
/system/external_endpoints POST	/system/network/:lighthouse_id PUT
/system/external_endpoints/:id GET	/system/network/:lighthouse_id GET
/system/external_endpoints/:id PUT	/system/network/:lighthouse_id PUT
/system/external_endpoints/:id DELETE	/system/network/:lighthouse_id PUT
/system/hostname GET	/system/network/:lighthouse_id GET
/system/hostname PUT	/system/network/:lighthouse_id PUT

25.04.2 (June, 2025)

This is a patch release.

Enhancements

- **Per-interface routing added to prevent asymmetric replies** [IM-18240]
  - Lighthouse now replies via the same interface a connection is made on, preventing asymmetric routing in multi-interface and OSPF/SMF environments.

Security Fixes

- **Added support for the Message-Authenticator header when using RADIUS** [IM-17884]
  - A new toggle to require or not require Message-Authenticator has been added to the remote authentication screen.
  - By default, enforcement of this header is disabled so as not to break compatibility with older servers. Enable it to avoid CVE-2024-3596 (BlastRADIUS).

Defect Fixes

- Fixed an issue where the users and groups config template can have a user with no groups or assign groups to users not from the group list. [IM-17580]
- Fixed an issue where the warning banner on disabling admin users was not shown for non-root administrators. [IM-16471]
- Changed pmshell/nmshell so that leaving a serial port returns to the port list rather than going to the node list. It is now possible to get from the port list to the node list. [IM-18081]
- Resolved an issue where the UTC time was displayed in the System Date & Time drop down instead of the user's selected timezone. [IM-18244]

25.04.1 (May, 2025)

This is a patch release.

Migration Guide

This patch release fixes an issue where upgrades to 25.04.0 were rolling back due to legacy node certificates having duplicate serial numbers [IM-18235].

Lighthouse will prevent upgrades to 25.04.1 if active certificates with duplicate serial numbers exist.

To check if Lighthouse is impacted, do the following before upgrading:

- As `root` or using `sudo`, run:

```
mysql lighthouse -e "SELECT common_name, revoke_time, serial FROM certificates WHERE serial IN
(SELECT serial FROM certificates GROUP BY serial HAVING COUNT(*) > 1) AND revoke_time IS NULL"
```

If the command returns no output, there are no duplicate serial numbers and upgrade can continue.

If the command outputs serial numbers, take the following steps to replace the node certificates:

- As `root` or using `sudo`, run:
  - `cert_manage renew --nodes`
  - `cert_manage run`
- Once the nodes have reconnected to Lighthouse, upgrade can proceed.
  - Node reconnection may take some time to complete.
  - The log file /var/log/cert_manager.log shows relevant details.
  - The `mysql` command above can be re-run to see if all the duplicate serials have been revoked.

  If any nodes cannot have their certificate replaced (for example, if the node is temporarily offline), it may be necessary to manually un-enroll the node, then re-enroll it later.

Enhancements

- Added support for Authenticated Network Time Protocol (NTP) [IM-18022]
  - Provide secure, reliable and verifiable time synchronisation for enterprise customers who require authentication mechanisms and intuitive UI controls/visuals for managing NTP configurations.
  - Allow secondary instances to have independent NTP settings, configurable separately from the primary instance.
- Added the ability to configure optional certificate subject attributes when configuring an external CA via CLI. [IM-17903]
- Added a session logout warning to the UI, allowing users to extend or end their session. [IM-17507]
- Improved accessibility of dropdown lists and Network Settings Page. [IM-18161]
- Added CLI to generate sanitized configuration backups. [IM-17356]
- Extended `GET /system/entitlements` API response to return the license expiry date in UTC, in the format `YYYY-MM-DD HH:MM:SS` under the property expiry_date_utc. [IM-17864]

Security Fixes

- Upgraded `docker-moby` to 26.1.4 to patch CVE-2024-29018. [IM-18210]

Defect Fixes

- Fixed an issue where incorrect data was being captured from the AWS metadata endpoint when spinning up IPv6 only Lighthouses. [IM-18015]
- Fixed an issue where serial sessions initiated from the Web Terminal button in the Ports page or Node Details page were incorrectly displayed as being initiated by the `root` user, regardless of the actual user. [IM-18097]
- Fixed an issue where the connected nodes tab shows negative numbers. [IM-18227]
- Fixed an issue where the redis would restart in a loop instead of recovering from a corrupted AOF file. [IM-18036]
- Fixed an issue where updating the SMF MTU through the LHVPN MTU setting did not update the WireGuard interface MTU's. [IM-18093]
- Fixed some conman `start` commands to be idempotent. [IM-17769]
- Fixed an issue where cron was unintentionally disabled during a weekly cron job, causing features that depend on cron to stop working. [IM-18079]
- Fixed OSPF routing issue between Lighthouse and nodes. [IM-17855]
- Fixed an issue where SAML users were unable to access serial ports from the web-ui under certain conditions. [IM-18232]

25.04.0 (April, 2025)

This is a production release.

Migration Guide

- Lighthouse 25.04.0 introduces support for configuring an external certificate authority (CA).
  - An external CA can only be configured on a deployment that does not have any Opengear devices or secondaries enrolled.
- This release introduces port session management functionalities enabling administrators with the ability to view/terminate active serial port connections from Lighthouse for all nodes, including third party devices, enrolled into Lighthouse. For this feature, a new role permission Port Management has been added under the Nodes and Configuration permission group with the following settings:
  - `FULL ACCESS`: The user can view and terminate serial sessions.
  - `READ-ONLY`: The user can only view the list of Lighthouse initiated serial sessions.
  - `DENY`: The user cannot see the active serial sessions, nor can they terminate any sessions.

  By default, the:
  - `Lighthouse Admin` role is set to `FULL ACCESS`
  - `Node Admin` role is set to `READ-ONLY`
  - `Node User` role is set to `DENY`
  - `Reporter` role is set to `READ-ONLY`

Features

- **External Certificate Authority support** [IM-17445] Lighthouse now supports integration with external certificate authorities for certificate issuance using the Simple Certificate Enrollment Protocol (SCEP) and revocation using the Online Certificate Status Protocol (OCSP). This enhancement addresses customer requirements for compliance, interoperability, and improved security by allowing organisations to manage certificates through their preferred CA.
  Supported external certificate authorities include:

  - Venafi Trust Protection Platform
  - Microsoft Active Directory Certificate Services

  The external CA integration does not currently support certificate renewals and rollover. It is recommended to set your certificate validity to greater than a year. This will be addressed in a following release.

- **Serial Port Connection Status** [IM-17496] This release introduces centralized visibility and control over active serial port sessions across all nodes (Opengear and third-party) enrolled in Lighthouse. It enables administrators and network engineers to monitor, filter, and terminate serial port connections via Lighthouse across multiple nodes.

- **Cell Failover and Health Observability Enhancements** [IM-17822] [IM-17863] Enhanced visibility of nodes in cellular failover mode from the Lighthouse dashboard and across multiple pages. These improvements ensure that failover status is communicated through visual indicators and filtering options available to help users detect failover conditions at scale and take action, if necessary.

Enhancements

- Updated the `cert_manage` CLI command to only run as root or using sudo. [IM-16675]

- Updated the `cert_manage` CLI command to output the number of certificates either scheduled or processed for renewal. [IM-16510]
- Added progress bar to `cert_manage` CLI. [IM-16458]
- Limited the user password to less than 512 characters. [IM-16791]
- Improved the documentation for POST and PUT endpoints for smart groups. [IM-17897]
- Improved the error message to explain node enrollment failure when the user's group contains node or port filters. [IM-14641]
- Added the script `/usr/bin/pre-upgrade_checks.sh` to help assess Lighthouse readiness for upgrade. [IM-15808]
- Improved the Lighthouse upgrade checks to ensure the dependent has enough space for a database dump. [IM-17352]
- Improved robustness of back-end worker processes. [IM-17897]
- Updated the configuration authentication templates to allow LDAP over SSL configuration for NGCS devices. [IM-17502]
- Updated node backup and firmware upgrade cron jobs to use UTC timestamps, ensuring consistent scheduling regardless of local timezone settings. [IM-17832]
- Improved logging of failed conman start/stop commands. [IM-17768]
- Improved the accessibility of the stepper component on the Template and Firmware Upgrade pages. [IM-17506]
- Improved the focus indicator contrast when the light color theme is active. [IM-17509]

Security Fixes

- Updated OpenSSH to 9.9p2 to fix CVE-2025-26465 and CVE-2025-26466 [IM-17835]

Defect Fixes

- Fixed handling of duplicate entries in conman configurations. [IM-17723]
- Fixed the support script `generate-graphs.sh` for generating status history charts. [IM-17774]
- Fixed a tooltip issue that prevented users from moving the mouse pointer onto the text. [IM-17510]
- Fixed a layout issue where long node names caused a horizontal scroll bar to appear on the node details page. [IM-17508]
- Fixed an issue where node firmware upgrade jobs were scheduled incorrectly if local timezone was set to anything other than UTC. [IM-17144]
    - Note: Jobs on affected Lighthouses prior to this update must be cancelled and rescheduled to ensure accurate scheduled times.
- Fixed an issue where netops modules do not show in the UI when using a legacy license. [IM-17797]
- Fixed an issue where the Console Gateway SSH Address could not be updated with a hostname value. [IM-17227]
- Fixed an unexpected 429 error when bulk approving nodes. [IM-14996]
- Fixed an issue where MTU could not be set for network interfaces via ogconfig-cli. [IM-18032]
- Fixed an issue where Lighthouse would show incorrect user name "???" in the logs when ogconfig-cli was used to enable logging. [IM-17858]
- Resolved an issue where users assigned the same node filter, but different port filters can only see ports that overlap. [IM-10930]
- Resolved an issue where the Smart Management Fabric navigation bar item was not highlighted on the Lighthouse OSPF settings page. [IM-17814]
- Resolved an issue where users were able to delete node and port filters that were linked to user groups. A warning message now shows. [IM-13663]
- Resolved an issue where the "SSH Port" for external link specified under network settings was incorrectly treated as an internal SSH port. [IM-17929]

24.12.3 (May, 2025)

This is a patch release.

Enhancements

- Improved robustness of back-end worker processes. [IM-17924]

Defect Fixes

- Fixed the SNMP service using too many TCP connections. [IM-18158]
- Fixed an issue where netops modules do not show in the UI when using a legacy license. [IM-17797]
- Fixed the support script ‘generate-graphs.sh’ for generating status history charts. [IM-17774]

24.12.2 (April, 2025)

This is a patch release.

Enhancements

- Added SSH key authentication as an alternative to password authentication when enrolling third party nodes. [IM-17908]
- Improved data handling from a node during config retrieval. [IM-17886]
- Added the ability to set the default metric for each interface connected to Lighthouse. [IM-17717]

Defect Fixes

- Fixed an issue where NGINX was reloading constantly in the background due to unused enabled IPv6 automatic connections on Lighthouse. [IM-17819]
- Fixed an issue that could cause an upgrade to fail and roll back. [IM-17798]
- Fixed an issue where remote port logs from nodes can cause rsyslogd to crash. [IM-17752]
- Resolved an issue where error messages for the node filter fields were not being read out with screen reader software. [IM-17511]

24.12.1 (February, 2025)

This is a patch release.

Defect Fixes

- Fixed an issue with Cell Health Connectivity Check not working correctly with IPv6 addresses. [IM-17658]
- Fixed an issue on the Network Settings page not displaying Secondary Lighthouse's run time status data correctly. [IM-17574]
- Resolved a display issue on the Lighthouse OSPF Settings page when a description is not set for Secondary Lighthouses. [IM-17672]
- Fixed an issue with Node Backup frequency converting weeks to days incorrectly. [IM-17544]
- Fixed an issue that allowed roles to be deleted while assigned to groups and groups to be deleted while assigned to local users. [IM-16564]
- Fixed an issue to prevent the users and groups configuration templates from being created with duplicate groups. [IM-16342]
- Resolved an issue with the dynamic setting for the number of concurrent API connections on upgrade boot. Any other boot was not affected. [IM-17642]
- Fixed an issue where unexpected Cellular Health data would result in unwanted errors in the Lighthouse logs. [IM-17631]
- Ensured Lighthouse upgrades are rolled back when invalid nginx configuration is found. [IM-17472]

24.12.0 (December, 2024)

This is a production release.

Migration Guide

- This release comes with added functionality to support multiple network interface connections. It is strongly recommended to follow the migration guidelines on our support portal if your deployment is already running additional network interfaces. Skipping the migration steps when upgrading with a second network interface connection may result in exposing Lighthouse on undesired networks or loss of access to Lighthouse. It is important that these steps are done before upgrading.

- The Network Interfaces and Network Settings pages have been consolidated into a single page called Network Settings. This change impacts Role-Based Access Control permissions as follows:

    - Obsolete Permissions:
        - "Network Interfaces" permission previously controlled access to the Network Interfaces page.
        - "Admin and Subscriptions" permission previously controlled access to the Network Settings page.
    - New Permissions:
        - Access to the consolidated **Network Settings** page is governed by a newly introduced permission called "Network Settings", with the following default settings for built-in roles:
          `Lighthouse Admin: Full-Access, Reporter: Read-Only, Node Admin/Node User: Deny`.
          All custom-created roles will be set to `Deny`.
        - While upgrading to 24.12.0 please note that built-in roles will automatically inherit the new "Network Settings" permission as specified above. All custom-created roles will not receive the new permission by default. These roles must be manually updated to ensure proper access control for the Network Settings page.

Features

- **Subscription Changes** [IM-16965]

  Enterprise Edition and Automation Edition subscription including NetOps modules will reach their End-of-Life, making way for Opengear's new commercial model with two new subscription types. Learn more about the changes. This Lighthouse release introduces support for the two new subscription types:

    - Lighthouse Core as a replacement for the Enterprise Edition subscription.
    - Lighthouse Enhance as a replacement for the Automation Edition subscription.
    - Evaluation mode now offers Lighthouse Enhance as the trial subscription.
    - The duration of evaluation mode has been increased from 30 days to 90 days.
    - Node filters now come with an option to filter nodes running NetOps modules.
    - Three new **Disable NetOps** templates provided to cleanup NetOps infrastructure running on OM1200, OM2200 and CM8100.

- **Smart Management Fabric (SMF) Enhancements** [IM-16657]

  Introduced advanced SMF capabilities, resolving routing limitations and improving multi-instance network management for enterprise deployments.

    - Extended **OSPF functionality for networks connected to Lighthouse**, to enable

devices on the management subnet to connect directly to Lighthouse and access devices on networks connected to Opengear Nodes through routed IP.
    - Added support for **multiple network interface connections**, allowing you to specify connections as “reserved” for Lighthouse OSPF configuration.

- **Centralized Network Settings Management for Primary and Secondary Instances** [IM-16657]

  Enhanced user experience to streamline network settings management for multi-instance administration. The new **Network Settings** page allows you to centrally manage hostnames, multiple interface connections, direct access port configurations, and external network addresses for all instances, including secondaries.

- **Custom Login Message** [IM-16099]

  This release introduces support for administrators to configure and display a custom login message on the Login page and login via CLI. The message can include hyperlinks within the text.

Enhancements

- Added the ability to show/hide unmasked password. [CDM-1251]
- Enhanced the search functionality on the Ports page to support searching by node name.[IM-14917]
- Enhanced local syslog storage to be more robust. [IM-16024]
- Added the ability to tag a single resource on the Resource page. [IM-14931]
- Enhanced the View Group Details page to show the filters associated with the user group. [IM-15191]
- Disabled NetOps related services when not in use. [IM-17075]
- Updated the background image on the Login and Password Reset pages. [IM-16919]
- Improved cleanup of SSH authorized keys added by or for remote-only users.[IM-16150]
- Added the ability to tag multiple resources on the Resource page. [IM-15704]
- Improved error message when tagging a non-existent resource. [IM-15568]
- Displayed number of user groups associated to a filter on the: [IM-15197]
    - Resource Filter page and Delete Resource Filter modal.
    - Port Filter page and Delete Port Filter modal.
- Database transfers for secondary upgrades and replication between primary and secondary lighthouses are now compressed. [IM-17351]

Security Fixes

- Upgraded Docker to 25.0.3 for CVE-2024-24557 and Go to 1.22.6 for CVE-2024-24790. [IM-17147]
- Fixed CVE-2015-9542. [IM-16121]
- Upgrade waitress to 3.0.1 to fix CVE-2024-49769. [IM-17337]

Defect Fixes

- Fixed an issue where nodes would never enroll if they were approved too quickly. [IM-17187]
- Fixed a bug where the CRG proxy buttons were incorrectly enabled when SMF was disabled. [IM-17186]
- Fixed an issue that caused OGCS nodes without modems to log SignalStrength errors in the logs when cellular health checks are enabled. [IM-17045]
- Fixed an issue where node-command logs were attached to support reports, leading to errors due to dangling symlinks. [IM-17044]
- Resolved an issue with including log files in the configuration backup. [IM-17042]

- Fixed an issue where node-info, node-command, node-copy did not process repeated switches correctly. [IM-17040]
- Fixed an issue where SNMP values were reported incorrectly due to service startup order. [IM-17031]
- Resolved an issue where pending nodes were not being listed following an upgrade. [IM-16774]
- Fixed an issue where not all permitted CSR key lengths were supported. [IM-16604]
- Resolved a bug where on support report download, the success message was being shown before the download was complete. [IM-16487]
- Fixed an issue where customers could not upgrade Lighthouses when two tags with the name “Bundle” where specified for an enrollment bundle. [IM-15948]
- Fixed an issue where dependent Lighthouses would attempt to enroll nodes via API. [IM-15580]
- Fixed input length validation on several API. [IM-15419]
- Fixed ‘Console Shell’ access permissions to assign the correct permissions. [IM-14601]
- Resolved an issue where the SHA1 signed cert was being overwritten on upgrade. [IM-17009]
- Resolved a race condition that caused issues with upgrading Secondary Lighthouses from version 24.06.1 to 24.06.2 [IM-17523]
- Fixed an issue to ensure the subscription bar graph uses the Lighthouse system time not the user’s local time [IM-17422]

24.06.2 (September, 2024)

This is a patch release.

Enhancements

- Third-party nodes can now be added as resources for HTTP, HTTPS, and SSH access after they are enrolled in Lighthouse with Smart Management Fabric (SMF) enabled.
- Added additional screen reader navigation landmark.
- Improved link differentiation.
- Added form field labels to aid form comprehension.
- Improved password validation feedback for remote authentication.
- Removed large decorative icons from empty tables.

Security Fixes

- Patched python to fix CVE-2024-7592.
- Patched expat to fix CVE-2024-45490, CVE-2024-45491 and CVE-2024-45492.

Defect Fixes

- Resolved accessibility limitations regarding keyboard and screen reader support.
    - Fixed screen reader navigation, icon, status, warnings, table header and tool tip announcements.
    - Fixed job filter announcements.
    - Fixed focus order for tables and modals.
    - Fixed role definition for tool tips, no longer buttons.
    - Corrected link navigation announcements.
- Disabled 3rd party node Web UI access links from dashboard and nodes pages.
- Allowed scrollbar buttons to be accessed on the local terminal page.
- Fixed refreshing template status updates.
- Allowed mixed case ‘yes’ confirmation for Backup and Restore and Factory reset pages.

24.06.1 (August, 2024)

This is a patch release that supersedes the 24.06.0 release. Please refer to the 24.06.0 release notes section below for the full list of features and fixes.

Security Fixes

- Updated Libarchive to 3.7.4 to fix CVE-2024-37407
- Patched Wget to fix CVE-2024-38428

Defect Fixes

- Fixed an issue where Filters (Smart Groups) were not being migrated correctly when upgrading to 24.06.0.
- Fixed an issue where Lighthouse Web Service failed to start when a DNS server was not configured.
- Resolved an issue on the Resources page where the SSH Access button in the SSH connection modal did not prompt users for their preferred client when using Firefox.
- Updated the RAML documentation to remove unused fields from the Connected Resource Gateway API examples.
- Fixed an issue where the Lighthouse menu pane was overlapping with the main page content.

24.06.0 (July, 2024)

This is a production release.

The Lighthouse User Interface (UI) has been re-architected for an enhanced user experience. This release replaces the Ember UI fully with React. It brings a new color and design scheme, better organization of functionality to improve workflow, clearer indication of form errors, and other improvements. Additionally, it adds auto-refresh capabilities to the UI, presenting real-time data display to the user.

Please refer to the Lighthouse User Guide for more information on the changes in this release.

Features

- **Connected Resource Gateway**

  Connected Resource Gateway (CRG) is a feature that allows users to build and manage a catalog of resources in Lighthouse, that are within the Smart Management Fabric (SMF) discovered networks. CRG allows clientless network access to these resources (via SSH, HTTP, HTTPS proxy), leveraging the IP connectivity enabled by our SMF infrastructure.

  CRG, like SMF, is available as part of the Lighthouse Enterprise Automation Edition subscription and requires Opengear appliances running firmware version 23.10.4 or higher.

- **Resource Tagging**

  Resource Tags is a feature that allows unique identification of serial ports and resources using tags. It improves the ability to separate and tie batches of ports or resources to relevant user groups.

  NOTE: The 'Port Tags' feature has been renamed to 'Resource Tags' in the UI and API, expanding its functionality to cover both Serial Ports and Resources.

Enhancements

- Added support for Certificate Management.
  Certificate Manager enables automatic renewal of Node and other VPN certificates used to authenticate Lighthouse. The `cert_manage` CLI command may be used for additional configuration.
- Added support for AWS Lighthouse to allow login on IPv6-only subnets, enabling access for instances without public IPv4 addresses or any IPv4 addresses. For IPv6-only deployments, ensure the following instance-specific settings are configured:
  - Metadata access: enabled
  - Metadata transport: enabled
  - Metadata version: V1 and V2 (token optional)
- By default the root account is disabled on an AWS image, for new installs. A new account lhadmin has been provided for initial configuration.
- By default, root login is disabled over SSH on an AWS image, for new installs. Existing AWS installs are unaffected, but could leverage the security enhancement.
  For scripts that need to be run by a root user, a Lighthouse admin may `sudo` to assume root permission.
- By default, password authentication is disabled over SSH on an AWS image, for new installs. Existing AWS installs are unaffected, but could leverage this.
- Enhanced error handling for duplicate users created on the Users page.
- Enhanced debugging capability by adding additional logs for upgrades.
- Enhanced the robustness of Multiple Instance Primary/Secondary replication resync scripts.

- Historical system stats are now included in support reports, providing a comprehensive view of system performance over time, and aiding support capabilities.
- Implemented a new script that runs daily and attempts to re-enroll nodes that have previously failed on a secondary Lighthouse. The `retry_secondary_node_enrollments` script can also be manually executed at any time.
- Improved input validation in the Configuration Backup feature to address a vulnerability.
- Improved input validation in the Configuration Restore feature to prevent a potential server error.

Security Fixes

- A number of critical and high Javascript related CVEs have been resolved with the UI upgrade to React. The addressed CVEs include: CVE-2022-2421, CVE-2023-26136, CVE-2023-37466, CVE-2023-37903, CVE-2023-45133, CVE-2021-23424, CVE-2023-45133, CVE-2023-46234, CVE-2022-21222, CVE-2022-38900, CVE-2021-23337, CVE-2022-21213, CVE-2020-7792, CVE-2021-3803, CVE-2022-25883, CVE-2023-32695, CVE-2023-26115.
- Enhanced security by using File Key Encryption to encrypt the database at rest.
- Hardened API security by limiting cookie authentication.
- OpenSSL patched to include fix for CVE-2023-6129.
- Updated glibc to include fix for CVE-2023-0687.
- Updated gnutls to include fixes for CVE-2024-0553 and CVE-2024-0567.
- Updated libuv to include fix for CVE-2024-24806.
- Updated libxml2 to include fix for CVE-2024-25062.
- Updated MariaDB from version 10.7.8 to 10.11.6.
- Updated nginx to include fix for CVE-2023-44487
- Updated OpenSSH from version 8.9p1 to 9.8p1 to include fix for CVE-2024-6387.
- Updated perl to include fix for CVE-2023-47100
- Updated python3-cryptography from version 41.0.6 to 42.0.5 to include fix for CVE-2023-50782.
- Updated redis from version 7.0.13 to 7.0.15 to include fix for CVE-2023-41056.
- Updated runc from version 1.1.4 to 1.1.12 to include fix for CVE-2024-21626, CVE-2023-28642, CVE-2023-27561.
- Updated sqlite3 to include fix for CVE-2023-7104.

Defect Fixes

- Addressed a security vulnerability by isolating sensitive authentication processes, strengthening Brute Force Protection mechanisms, and reducing the risk of unauthorized access to Lighthouse.
- Fixed an issue where a user who was previously locked out still appears as locked out after the lockout timer expires.
- Fixed an issue where an AWS Lighthouse instance would not start when using AWS metadata v2 (IMDSv2) only.
- Fixed an issue where certain configuration files in /etc/ were not replaced correctly during system upgrades and migrations.
- Fixed an issue where invalid port filters could be created.
- Fixed an issue where node configuration changes, such as serial port label updates, were not reflected on a secondary Lighthouse promoted to primary.
- Fixed an issue where running outdated configurators potentially leads to incorrect configurations.
- Fixed an issue where Smart Group (Node filter) or Port Filter queries that are exactly 255 characters long prevent Lighthouse from being upgraded.
- Fixed an issue with failed script templates triggering unexpected behavior for subsequent script runs.
- Fixed an issue with upgrades failing due to usernames with backslashes (such as domain) in

the passwd or shadow files.

- Resolved a bug with access control filters so they are fully enforced.
- Resolved an issue where users without SSH permissions could still reach nodes through SSH jump.
- Resolved an issue where all serial port sessions initiated from Lighthouse were incorrectly reported as “root” on the console server. Sessions now display the correct Lighthouse user who initiated them.
- Resolved an issue where large support reports were not being generated.
- Resolved errors being generated by race conditions during node enrollment. Additionally, this also fixes an issue related to AWS Lighthouse failing to upgrade from version 23.10.2 to 24.02.0.
- Restricted permissions on config files used in Azure deployments.
- Updated RAML documentation for the Bundles endpoint to include ‘tier’ as a required item in the example.

24.02.1 (May, 2024)

This is a patch release.

Defect Fixes

- Resolved an issue where all serial port sessions initiated from Lighthouse were incorrectly reported as “root” on the console server. Sessions now display the correct Lighthouse user who initiated them.
- Fixed an issue where upgrading from LH 23.10.2 to 24.2.0 would fail with an error related to subnet size in certain deployment scenarios.
- Fixed an issue where certain configuration files in /etc/ were not being replaced correctly during system upgrades and migrations.
- Updated RAML documentation for the Bundles endpoint to include ‘tier’ as a required item in the example.
- Fixed an issue with upgrades failing due to usernames with backslashes (such as domain) in the passwd or shadow files.
- Number of config push workers are now dynamically allocated based on system resources to improve performance in larger deployments.
- Fixed an issue with failed script templates triggering unexpected behavior for subsequent script runs.
- Enhanced the robustness of Multiple Instance Primary/Secondary replication resync scripts.
- Fixed an issue causing some upgrades on AWS deployed Lighthouses to rollback.
- Added support for AWS Lighthouse to allow login on IPv6-only subnets, enabling access for instances without public IPv4 addresses or any IPv4 addresses. Additionally, this also fixes an issue related to AWS Lighthouse failing to upgrade from version 23.10.2 to 24.02.0. For IPv6-only deployments, ensure the following instance-specific settings are configured:
    - Metadata access: enabled
    - Metadata transport: enabled
    - Metadata version: V1 and V2 (token optional)
- Addressed a security vulnerability by isolating sensitive authentication processes, strengthening Brute Force Protection mechanisms and reducing the risk of unauthorized access to Lighthouse.
- The upgrade process now includes a check to detect if a CA certificate with a SHA-1 signature is in use, and if so, halt the upgrade. In case the upgrade is essential despite the SHA-1 certificate warning, a mechanism has been provided to override this check. However, overriding is not recommended.
- Fixed an issue where a cron script could run outdated configurators, potentially leading to incorrect configurations in certain cases.
- REST API connection limit is now dynamically increased at boot based on system resources, enhancing performance and availability.
- Fixed an issue where node configuration changes, such as serial port label updates, were not reflected on a secondary Lighthouse promoted to primary.
- Historical system stats can now be included in support reports, providing a comprehensive view of system performance over time, and aiding support capabilities.