



Cisco License On-Prem Release Notes

Version 10 Release 202609

First Published: 5/29/2026

Last Modified: 9/09/2026

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

<http://www.cisco.com>

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2018-2026 Cisco Systems, Inc. All rights reserved.

General Information

SSM On-Prem is redesigned as Cisco License On-Prem. The application introduces a modern UI, improved navigation, and consistent interaction patterns. Terminology and workflows are aligned more closely with Cisco License Central to reduce learning effort for users managing hybrid environments

Cisco License On-Prem helps in managing the assets on-premises that work in conjunction with Cisco License Central (software.cisco.com).

It enables customers to administer products and licenses on their premises, instead of having to directly connect Smart License-Enabled devices to Cisco License Central hosted on Cisco.com.

Obtaining Product Artifacts

See the following sections for instructions on how to download Cisco License On-Prem installation files and documentation.

How to Obtain Product Information

The following documentation items are available for **Cisco License On-Prem**:

- *Cisco License On-Prem User Guide*
- *Cisco License On-Prem Console Guide*
- *Cisco License On-Prem Installation Guide*
- *Cisco License On-Prem Migration Guide*
- *Cisco License On-Prem API Guide*

These documents can be easily accessed when downloading *.iso* or *.zip* files of a particular release. If you hover over the green *.iso* or *.zip* image, a pop-up containing links to all the relevant documentation items will become available.

Important Considerations



NOTE:

- If you experience an issue after upgrading from SSM **On-Prem 9.x** to Cisco License On-Prem **10-202606 or above**, do not revert your snapshot to 9.x. Open a Cisco TAC case and TAC will assist with diagnosis and, if required, a supported recovery path.
- It is highly recommended that before performing an upgrade, you have a backup of your database (if you are using a VM). For more information, see the *Cisco License On-Prem User Guide (Chapter 5: Customize the setup-Backup and restoration settings)*.
- The synchronization architecture has been transitioned from the legacy multi-process approach to a single, consolidated mechanism. Due to these architectural changes, customers must update their firewall or network security policies to allow outbound traffic to id.cisco.com.
- When synchronizing a large volume of reports, the synchronization status may remain in an "In Progress" state for several hours. This is expected

behavior; the system will automatically transition to "Complete" once all data has been processed. No manual intervention is required.

- If you are migrating from 8.x to 10.x (CLP), please verify the hardware installation requirements detailed in *the Installation Guide under the System Requirements and Prerequisites section* to ensure your environment meets the necessary specifications.
- If using legacy products, such as Cisco Unity Connection and Cisco HCM-F, it is required that you enable **TLS 1.2 legacy ciphers** after upgrading. This enables communication between Cisco License On-Prem and the legacy devices. For more information, see the *Cisco License On-Prem User Guide (Chapter 5: Customize the setup - (Enable obsolete TLS versions))*.
- Starting with Cisco License On-Prem release **10-202606**, installation is supported on **AMD-based CPUs** in addition to Intel-based processors.
- After changing the hostname in the **Admin Workspace**, you must access the CLI and run `systemctl restart satellite`. Allow approximately 10 minutes for all Cisco License On-Prem services to restart and become available.

Direct Upgrade and Migration Paths

Target release	Direct upgrade supported from	Migration supported from
8-202404	Previous five releases	—
9-202406	—	8-202404
9-202407	9-202406	—
9-202410	9-202406, 9-202407	—
9-202412	9-202406, 9-202407, 9-202410	—
9-202501	9-202406, 9-202407, 9-202410, 9-202412	—
9-202502	9-202406, 9-202407, 9-202410, 9-202412, 9-202501	—
9-202504	9-202406, 9-202407, 9-202410, 9-202412, 9-202501, 9-202502	—
9-202507	9-202406, 9-202502, 9-202504	—
9-202510	9-202406, 9-202502, 9-202507	—
9-202601	9-202406, 9-202502, 9-202510	—
10-202606	9-202502, 9-202504, 9-202507, 9-202510, 9-202601	8-202404
10-202608	10-202606, 9-202601	—
10-202609	10-202608	—

How to read this table: Direct upgrade to 8-202404 is supported from the five releases immediately preceding it. However, 8-202404 → 9-202406 and 8-202404 → 10-202606, is a migration, not a direct

upgrade. Paths from the listed 9.x releases are direct upgrades. If the current release is not listed, do not proceed directly and open a TAC case.

Upgrading High Availability (HA) Cluster

For detailed instructions for upgrading a High Availability (HA) cluster, please see:

Cisco License On-Prem Installation Guide (Chapter 4 Post-installation configuration of Cisco License On-Prem, Upgrading High Availability (HA) Cluster).



NOTE:

The Cisco License On-Prem provides access to two interfaces, namely, port 443 (the default HTTPS port) and port 8443.

Port 443, which facilitates communication between Cisco devices and Cisco License On-Prem, carries product certificates that are signed and issued by Cisco. Since it is intended only for Cisco devices, the certificate used for port 443 is often not recognized by standard web browsers.

Port 8443 is meant for the end user to access Cisco License On-Prem and adjust the settings. As a predefined setting, this port serves as a self-signed local certificate. However, users can choose to generate a CSR, have it signed by a certificate authority, and upload it. To generate a CSR and to upload a certificate, navigate to Admin Workspace > Security > Certificates Tab.

Release Specifications

The following sections provide information on specific release dates, new features, bug fixes, and resolved vulnerabilities.

Version 10 Release 202609

Release Date: 9/09/2026

This release includes security hardening and resilience improvements that strengthen the overall security posture of Cisco License On-Prem.

Version 10 Release 202608

Release Date: 10/08/2026

New Features

System Monitoring (Prometheus Integration)

Cisco License On-Prem introduces built-in system monitoring, allowing administrators to enable metrics collection for their deployment. Monitoring settings are available under **Admin Workspace > Settings > Monitoring**, where users can enable or disable the feature, choose an authentication method (Basic

Authentication or No Authentication), select a TLS method (CA Signed Certificate or Skip TLS Certificate Validation), and configure the scrape interval and timeout used for metrics collection.

Once enabled, a metrics endpoint URL is provided, so external monitoring tools (such as Grafana) can retrieve system metrics. The settings page also displays real-time scrape status, showing whether monitoring is active, inactive, or still establishing its first successful scrape.

Deployment limitation: System Monitoring is supported only in standalone deployments. Do not enable it in two-node or three-node High Availability deployments.

Recommendation:

The '**No authentication**' and '**Skip TLS certificate validation**' options are strictly intended for testing environments only. These options expose the monitoring endpoint and must not be used in production deployments under any circumstances.

For production use, Cisco requires selecting '**Basic authentication**' together with '**TLS authentication**' (CA Signed Certificate) to preserve the security posture of the appliance. Failure to do so leaves the monitoring endpoint and system APIs vulnerable to unauthorized access.

*(For detailed configuration steps, refer to the **Configure Monitoring Settings** section in the **Cisco License On-Prem User Guide**.)*

Monitoring TLS Certificate

Cisco License On-Prem now supports Monitoring TLS certificate for the system monitoring endpoint, allowing administrators to secure metrics collection with a trusted certificate. These settings are available under **Admin Workspace > Security > Certificates**, where user can generate a Certificate Signing Request (CSR) from the Certificates by providing certificate details such as Common Name, Organization, Organizational Unit, Country, State, Locality, key size, and Subject Alternative Names (SANs). The generated CSR can be downloaded and submitted to a Certificate Authority for signing.

Once signed, the certificate (along with an optional intermediate certificate) can be uploaded to activate secure, CA-validated metrics collection. If a certificate already exists, uploading a new one replaces it. Alternatively, user can choose Skip TLS Certificate Validation when certificate-based validation is not required—but this is not recommended.

*(For detailed configuration steps, refer to the **Monitoring TLS Certificate** section in the **Cisco License On-Prem User Guide**.)*

Multi Datacenter (Geo-Location) Three Node HA

Cisco License On-Prem (CLP) now supports three-node High Availability (HA) deployments across multiple datacenters (minimum of two, maximum of three) to ensure geospatial data redundancy and disaster recovery capabilities.

Prerequisites and Load Balancing Requirements

This feature requires an external, physical Global Server Load Balancer (GSLB)—such as F5 or A10—that can reach all networks hosting the multi-datacenter CLP HA nodes.

- **Mandatory Requirement:** The GSLB must be configured with Client IP Session Affinity.
- **Performance Recommendation:** It is highly recommended to use Round-Trip Time (RTT)-based load balancing instead of Round-Robin to ensure optimal performance.

Configuration Process

Once the GSLB is provisioned with the appropriate DNS name and the CLP nodes are deployed, you can enable this feature during the three-node HA configuration wizard inside the onprem-console. Simply respond **yes** to the following prompt:

2. Enter if Multi Datacenter setup is required (yes/no): yes

Post-Deployment Monitoring

After the deployment completes, an updated user interface will be available under **Admin Workspace > High Availability**. This dashboard provides:

- Node and datacenter health status.
- Real-time RTT metrics measure connectivity between each cluster node to help verify network reliability.

(For detailed configuration steps, refer to the **Multi Datacentre (Geolocation) Three-Node HA Cluster Deployment Section** in the **Cisco License On-Prem Installation Guide**.)

Enhancements

Proxy support available for Oauth ADFS and SSO Authentication

Cisco License On-Prem now allows Oauth ADFS and SSO authentication providers to be routed through the configured HTTP/HTTPS proxy server.

A new per-provider "Route through proxy server" checkbox is now available on both authentication provider configuration screen. When enabled, all server-to-identity-provider traffic for that provider is routed through the proxy. When disabled, or when the global proxy is off, that provider's traffic continues to connect directly, exactly as before.

(For detailed configuration steps, refer to the **Set Up Proxy Server Support** section in the **Cisco License On-Prem User Guide**.)

Known Issues

Bug ID	Description
CSCwv98421	Cisco License On-Prem account removal may not be reflected in Cisco License Central When removing a Cisco License On-Prem account, the operation may display "Error deleting On-Prem Account." The account may no longer appear in Cisco License On-Prem but can remain visible in Cisco License Central. If you encounter this issue, contact Cisco TAC for assistance.

Fixes

This release introduces the following fixes.

Bug ID	Description
CSCwv66337	License synchronization could fail for accounts with large transaction volumes

	Previously, online or offline license synchronization could fail with an internal error when processing an account containing a large number of license transactions. This could leave the account's license data out of date. This issue has been resolved so large transaction sets can be processed successfully.
CSCwv92750	Removing an HSEC PUSH device could leave stale license entries Deleting an HSEC PUSH device could leave related license entries visible with zero available, in-use, and balance quantities. Device removal now clears the associated stale license information from the interface.
CSCwv49224	License synchronization could display an incorrect failure status During some network synchronizations, Cisco License On-Prem could display a timeout or failure status even though synchronization completed successfully in the background. Timeout handling has been improved so that longer-running synchronizations complete without displaying a misleading failure status.
CSCwv92757	Non-reporting access points could not be removed Access points that were no longer reporting could remain in the device inventory without a supported removal action. Non-reporting access points can now be deleted, and their associated licenses are released.
CSCwu88090	First post-upgrade synchronization could reactivate inactive devices The first network synchronization after an upgrade could reactivate previously removed device records, producing duplicate entries and an inflated device count. Synchronization now preserves the inactive state of removed records.
CSCwv92764	Email notification settings restricted addresses to the cisco.com domain Previously, the Email Notification Settings page accepted only email addresses in the cisco.com domain. This restriction has been removed, and users can now save properly formatted email addresses from any valid domain. Existing cisco.com addresses continue to be supported.
CSCwu86383	Post-upgrade synchronization could rename accounts and interrupt SLP communication When the local On-Prem account name differed from its Virtual Account name, the first post-upgrade synchronization could overwrite the local name and device tenant identifier. The original values are now preserved so existing SLP devices continue communicating with the appliance.
CSCwv92774	Cisco License Central could display an incorrect controller version The Device Managers view in Cisco License Central could show an outdated hardcoded version for the Cisco License On-Prem controller. Registration, renewal, and synchronization now report the installed release version correctly.
CSCwv92782	Online synchronization could deactivate transactions beyond the first 500 Accounts containing more than 500 license transactions could have additional transactions incorrectly deactivated during a full online synchronization, resulting in inaccurate license balances. Synchronization now retrieves all transaction pages before updating local records.
CSCwv92783	TACACS+ and LDAP authentication could fail over IPv6 Connections to TACACS+ and LDAP authentication servers could fail when the appliance used IPv6. External authentication now connects correctly in IPv6 deployments.
CSCwu75108	Time-zone labels could show incorrect daylight-saving offsets The Time Settings page could display a static UTC offset for locations that observe daylight saving time, causing the label to differ from the current local offset. Geographic time-zone labels now account for daylight-saving changes.
CSCwu69567	TACACS+ users could receive authorization errors during account and synchronization operations

	After successfully signing in with TACACS+, users could receive an unauthorized error when performing account-management or license-synchronization operations, including registering accounts and transferring offline synchronization files. TACACS+ session handling has been corrected so these operations now complete successfully.
CSCwv92786	Deleted Local Virtual Accounts could reappear after account reactivation Local Virtual Accounts that had been deleted could reappear after the parent On-Prem account was deactivated and activated again. Deleted Local Virtual Accounts now remain removed throughout the account lifecycle.
CSCwv92791	CA certificate changes could fail to replicate in IPv6 three-node HA Adding or deleting a CA certificate in an IPv6 three-node High Availability cluster could update only one node, leaving certificate data inconsistent across the cluster. Certificate changes now replicate to all nodes.
CSCwv92796	UNIX device manager removal could report success without removing the controller Removing a UNIX device manager after an upgrade could display both success and account-not-found messages while leaving the controller in the inventory. The controller and its managed-device associations are now removed correctly.
CSCwv49205	NTP and time settings could be lost after an upgrade Previously configured NTP server, port, synchronization, and authentication settings could be cleared during an upgrade. Time configuration is now preserved across supported upgrade paths.
CSCwv92799	Call Home workflows could fail over IPv6 Call Home communication configured with IPv6 could fail, affecting registration, renewal, deregistration, and account synchronization. These workflows now complete successfully over IPv6.
CSCwv92801	Scheduled database backups could fail to transfer to an IPv6 server In an IPv6 deployment, a scheduled database backup could be created locally but fail to copy to the configured remote IPv6 server. Backup transfers to IPv6 destinations now complete successfully.
CSCwv92804	SLP device alerts could show incorrect synchronization messages After an upgrade, SLP device alerts could display a generic sync-request message instead of the current usage-report and acknowledgment status. Device alerts now reflect the correct synchronization stage.
CSCwv92805	Resource Monitor could report incorrect disk usage The disk usage percentage shown in Resource Monitor could differ significantly from the actual usage of the appliance's /var partition. The displayed value now reflects the intended partition usage.
CSCwv92807	V1 API license transfer could leave device compliance status outdated When a V1 API license transfer corrected a shortage, pool quantities could update while affected devices remained marked out of compliance. Device-level compliance is now recalculated after the transfer completes.
CSCwv92809	Virtual Account transaction history could show account-wide activity The transaction history for a license in a Local Virtual Account could display transactions from the entire On-Prem account. The history now shows only transactions associated with the selected Virtual Account and license pool.
CSCwv92810	Claimed licenses could be transferred between Virtual Accounts Licenses already claimed by a license-management controller could be included in the quantity available for transfer. Claimed quantities are now excluded so only licenses available for reassignment can be moved.
CSCwt59124	Device hostname could remain visible after privacy was re-enabled

	For Cisco IOS XR devices, a hostname learned while privacy was disabled could remain visible after privacy was enabled again and the device synchronized. Re-synchronization now removes the hostname when device privacy settings require it.
CSCwu43761	STIG mode now prevents inbound SCP and SFTP access Cisco License On-Prem now blocks incoming SCP and SFTP connections when STIG mode is enabled. This prevents users from transferring files to the server or browsing its files through SCP or SFTP.

Resolved Vulnerabilities

CVE-2024-34459, CVE-2025-4877, CVE-2025-4878, CVE-2025-5278, CVE-2025-5351, CVE-2025-8114, CVE-2025-8277, CVE-2025-8677, CVE-2025-9615, CVE-2025-10263, CVE-2025-10911, CVE-2025-13151, CVE-2025-14087, CVE-2025-14512, CVE-2025-22105, CVE-2025-37980, CVE-2025-38015, CVE-2025-38097, CVE-2025-38166, CVE-2025-38279, CVE-2025-38400, CVE-2025-38405, CVE-2025-38441, CVE-2025-38470, CVE-2025-38653, CVE-2025-39866, CVE-2025-40134, CVE-2025-68183, CVE-2025-68366, CVE-2025-68724, CVE-2025-71066, CVE-2025-71089, CVE-2025-71116, CVE-2026-0964, CVE-2026-0965, CVE-2026-0966, CVE-2026-0967, CVE-2026-0968, CVE-2026-1933, CVE-2026-2100, CVE-2026-2340, CVE-2026-3012, CVE-2026-3039, CVE-2026-3832, CVE-2026-3833, CVE-2026-4046, CVE-2026-4408, CVE-2026-4437, CVE-2026-4438, CVE-2026-4480, CVE-2026-5260, CVE-2026-5419, CVE-2026-5450, CVE-2026-5946, CVE-2026-7383, CVE-2026-9076, CVE-2026-22984, CVE-2026-22990, CVE-2026-23040, CVE-2026-23060, CVE-2026-23216, CVE-2026-23243, CVE-2026-23392, CVE-2026-23401, CVE-2026-23455, CVE-2026-23479, CVE-2026-23631, CVE-2026-25679, CVE-2026-28390, CVE-2026-31408, CVE-2026-31411, CVE-2026-31419, CVE-2026-31474, CVE-2026-31488, CVE-2026-31508, CVE-2026-31532, CVE-2026-31581, CVE-2026-31607, CVE-2026-31613, CVE-2026-31669, CVE-2026-31677, CVE-2026-31684, CVE-2026-31685, CVE-2026-31709, CVE-2026-31772, CVE-2026-31786, CVE-2026-31787, CVE-2026-31790, CVE-2026-33416, CVE-2026-33636, CVE-2026-33845, CVE-2026-33846, CVE-2026-34180, CVE-2026-34181, CVE-2026-34182, CVE-2026-34183, CVE-2026-35091, CVE-2026-35092, CVE-2026-35177, CVE-2026-39979, CVE-2026-40164, CVE-2026-40170, CVE-2026-40355, CVE-2026-40356, CVE-2026-41316, CVE-2026-41411, CVE-2026-42009, CVE-2026-42010, CVE-2026-42011, CVE-2026-42012, CVE-2026-42013, CVE-2026-42014, CVE-2026-42015, CVE-2026-42245, CVE-2026-42246, CVE-2026-42258, CVE-2026-42496, CVE-2026-42764, CVE-2026-42766, CVE-2026-42767, CVE-2026-42768, CVE-2026-42769, CVE-2026-42770, CVE-2026-43020, CVE-2026-43023, CVE-2026-43027, CVE-2026-43037, CVE-2026-43038, CVE-2026-43051, CVE-2026-43056, CVE-2026-43074, CVE-2026-43110, CVE-2026-43112, CVE-2026-43116, CVE-2026-43125, CVE-2026-43128, CVE-2026-43158, CVE-2026-43163, CVE-2026-43190, CVE-2026-43198, CVE-2026-43260, CVE-2026-43276, CVE-2026-43279, CVE-2026-43303, CVE-2026-43329, CVE-2026-43414, CVE-2026-43501, CVE-2026-44431, CVE-2026-44432, CVE-2026-45186, CVE-2026-45445, CVE-2026-45446, CVE-2026-45447, CVE-2026-45852, CVE-2026-45898, CVE-2026-45984, CVE-2026-46054, CVE-2026-46056, CVE-2026-46090, CVE-2026-46113, CVE-2026-46116, CVE-2026-46117, CVE-2026-46125, CVE-2026-46135, CVE-2026-46145, CVE-2026-46152, CVE-2026-46155, CVE-2026-46166, CVE-2026-46173, CVE-2026-46176, CVE-2026-46181, CVE-2026-46189, CVE-2026-46209, CVE-2026-46227, CVE-2026-46242, CVE-2026-46243, CVE-2026-46244, CVE-2026-46259, CVE-2026-46316, CVE-2026-46323, CVE-2026-46331, CVE-2026-48962, CVE-2026-53266, CVE-2026-53359, CVE-2026-6893, CVE-2026-32280, CVE-2026-32281, CVE-2026-32282

Version 10 Release 202606

Release Date: 31/05/2026

New Features

Reimagined Landing Page

Cisco License On-Prem introduces a new default landing page named On-Prem Accounts Overview. This page appears when a user logs in to the application. It displays a consolidated list of available On-Prem accounts. The page shows account status, synchronization state, license usage summary, device count, and overconsumption indicators. Users can request a new On-Prem account or request access to an existing account from this page.

Consolidated Account-Level View

Cisco License On-Prem provides a consolidated account-level view available from the Licensing workspace. From this view, users can see devices and licenses across all Virtual Accounts (VAs) within an On-Prem account, along with account status and usage information.

Improved SLP Device Synchronization Accessibility

Cisco License On-Prem introduces a dedicated SLP Device Synchronization menu item in the Licensing workspace for devices configured to use Smart Licensing Using Policy (SLP) in pull mode.

This menu item provides a centralized location to collect usage data from SLP pull devices to Cisco License On-Prem. Usage collection can be initiated directly by the user or scheduled to run automatically on a daily, weekly, or monthly basis.

The interface also improves visibility by displaying the usage collection status at both the device and controller levels. Status values include current, pending and overdue, allowing users to easily track completion.

Unified Synchronization with Cisco License Central

Cisco License On-Prem provides a unified, one-click synchronization with Cisco License Central from Licensing Workspace.

Users can initiate synchronization for both SL and SLP devices from a single location, with clear status visibility. This interface reduces navigation effort and improves overall usability. Users can view real time sync progress.

Theme Selector

Cisco License On-Prem includes a theme selector in the global header. Users can choose between Light, Dark, or System theme modes. The System option follows the operating system preference by default. The selected theme applies across all workspaces and pages. Theme changes do not affect functionality or user permissions.

AI Assistant

Cisco License On-Prem includes AI Assistant in the global header. This AI assistant provides contextual, documentation-based assistance to help you manage Cisco License On-Prem deployments and device licensing. The AI Assistant supports documentation search and product-specific licensing queries and is available only for connected customers.

Device Managers and Controllers

Cisco License On-Prem introduces support for Device Managers (controllers). Controllers represent systems that manage multiple devices. Controllers appear in the Device Manager view with associated metadata. Information includes managed device count, synchronization status, and trust state. To access Device Managers, Navigate to **Licensing Workspace > Devices > Device Managers**.

Okta Verification Support

Support is added for Okta as an external identity provider. Okta is used for user authentication and verification for Cisco License On-Prem (CLP) login. Validation through Okta is performed for user sign-in and verification workflows. This also extends to specific authenticated requests within the application, such as approving accounts, accessing the approving new On-Prem account requests or initiating network synchronization. Okta configuration is performed as part of external authentication setup.

Device-Led Conversion (DLC) Settings Management

This release introduces enhanced capabilities for managing Device-Led Conversion (DLC) settings within your Cisco License On-Prem environment. Users can now precisely control how traditional licenses are automatically converted to Smart licenses.

Key Capabilities:

- **Centralized Management:** Navigate to DLC settings directly from the Account Management sub-menu.
- **Flexible Conversion Control:**
 - Enable or disable device-led conversion for your organization.
 - Apply conversion settings to all local Virtual Accounts or selectively choose specific Virtual Accounts.
- **Improved User Experience:** A clear interface for managing conversion preferences, including immediate feedback and error handling for Virtual Account selection.

Product Image Security Scanning

To ensure the security and integrity of the Cisco License On-Prem license server, the product is routinely scanned for out-of-date packages as well as any known critical or high CVEs (Common Vulnerabilities and Exposures). Based on evaluating reports from various tools, several key packages have been updated.

For full list of all CVEs fixed please refer to resolved vulnerabilities section

Accessibility Compliance

Cisco License On-Prem interface aligns with **WCAG 2.1 Level AA standards** reinforcing our commitment to providing a more inclusive, accessible, usable experience for all users.

This release focuses on enhanced keyboard navigation, clearer error notifications, improved information structure, and optimized component design.

Enhancements

Easier and More Streamlined Interface

The user interface is updated to use a React-based Magnetic UI framework. Layout behavior is standardized across pages and workspaces. Drawers, tables, and navigation elements follow consistent interaction patterns. The update improves responsiveness and alignment across views.

Standardized Success Confirmations

To enhance consistency and user experience, success confirmations throughout the application have been standardized. Instead of various page-level banners, successful operations (like managing access, editing user details, updating network settings, or modifying security settings) now display as brief, clear, temporary messages. This ensures immediate, consistent feedback, confirming actions without interrupting the workflow.

License and Device Alerts

License and device alert visibility is enhanced across inventory views. Alert indicators appear alongside devices and licenses. Alerts identify conditions such as overconsumption, pending synchronization, and compliance issues.

Device Inventory Enhancements

The Device Inventory view includes additional contextual information. Devices display controller association and High availability where applicable. Visual indicators differentiate between SL and SLP devices. Managed devices appear conditionally when associated with a controller. Filtering and sorting options reflect these attributes.

Search, search filter and filter controls

Cisco License On-Prem introduces consistent search, search filter and filter controls across tables. Users can refine searches by selecting specific attributes before entering search text. Search filters affect only the search behavior and do not change the underlying table data set.

The Filter control is separate from the search filter. Filters allow users to refine the table based on the status or the conditions. Filter options are specific to each table and reflect operational or compliance status. For example, users can filter the licenses from the license table based on license overconsumption or expiration date etc.

Centralized Event Logs

Event logs are centralized across the Admin and Licensing Workspaces. System, configuration, synchronization, and access events are recorded in one location. Events include timestamps and categories. Users can view events based on workspace context and permissions.

Known Issues

Bug ID	Description
N/A	Required post-upgrade NTP configuration Following an upgrade, previously configured Network Time Protocol (NTP) settings may not persist. After the upgrade process is complete, please navigate to the settings and re-configure your NTP server details to ensure time synchronization is restored.
N/A	Verify source node before Three-node HA upgrade In a three-node High Availability (HA) deployment, nodes can occasionally contain minor replication differences due to events such as node maintenance, temporary network interruptions, or service restarts. If these differences exist before an upgrade, they can be carried into the upgraded cluster. Before upgrading a three-node HA deployment, perform a validation check after cluster teardown to identify the node that contains the most current and complete data. Use this node as the source of truth when rebuilding the upgraded cluster. This best-practice step helps ensure data consistency and provides a known-good baseline for the upgraded deployment.
N/A	HTTP product registration is not supported on the product-only interface When the second NIC is configured as a "Product-Only" interface, HTTP product registration is not supported as port 80 is disabled. Please use an HTTPS registration URL (port 443) to complete the product registration process successfully.
N/A	Disk usage displayed in the resource monitor may differ from CLI values The disk usage value displayed in Admin Workspace > System Health > Resource Monitor may not match the disk usage reported for the "/var" partition by CLI commands such as "df -h".
N/A	Login page may not load after automatic logout in Firefox After a session time out and the user is automatically logged out in Firefox, the login page may remain on a loading screen and fail to load. Refresh the browser page to load the login screen and sign in again.
N/A	System information values may differ from node metrics in a Three-Node HA deployment In a three-node HA deployment, the CPU and memory values displayed in the High Availability widget may differ from the actual resource utilization reported on

	individual nodes. As a result, the values shown in the UI may not accurately reflect the current CPU and memory usage of a node.
N/A	API Toolkit does not support assigning roles to multiple local virtual accounts When creating a Client Credentials Grant in the Admin Workspace > API Toolkit , users can assign a role to only one Local Virtual Account for a given On-Prem Account. Additional role assignments for other Local Virtual Accounts under the same On-Prem Account are not supported.
N/A	System log search may not return matching log entries In Admin Workspace > Support Center > System Logs, the search function may fail to return matching log entries. As a result, the table may appear empty.
N/A	Exported Authorization request CSV file may fail validation in Cisco License Central The Authorization Request CSV file exported from the Device Inventory may fail validation when uploaded to Cisco License Central because the exported file format does not match the required CLC template. Download the CSV template directly from Cisco License Central and use it instead of the exported file from Cisco License On-Prem.
N/A	License expiration alerts may not be displayed after upgrade After upgrading from Cisco Smart Software Manager On-Prem 9-202510 to Cisco License On-Prem, license expiration alerts may not be displayed in the License Inventory or On-Prem Accounts Overview pages. As a result, users may not be notified of licenses that are approaching expiration.
N/A	Device transfer performance may be slower than expected after upgrade After upgrading to Cisco License On-Prem, transferring multiple devices between Local Virtual Accounts using Edit Local Virtual Account Assignment may take longer than expected to complete. The transfer operation completes successfully, but the completion time may exceed expected performance benchmarks.

Resolved Vulnerabilities

CVE-2026-43284, CVE-2026-35385, CVE-2026-35386, CVE-2026-35387, CVE-2026-35388, CVE-2026-35414, CVE-2026-31431, CVE-2026-22695, CVE-2026-22801, CVE-2026-25646, CVE-2025-61662, CVE-2026-4519, CVE-2026-1519, CVE-2026-28417, CVE-2026-28421, CVE-2026-33412, CVE-2026-25679, CVE-2025-39766, CVE-2025-68741, CVE-2026-20160