Cisco Smart Software Manager On-Prem Release Notes

General Information

Smart Software Manager On-Prem helps in managing the assets on-premises that works in conjunction with Cisco Smart Software Manager (software.cisco.com).

It enables customers to administer products and licenses on their premises, instead of having to directly connect Smart Licensed enabled product instances to Cisco Smart Software Manager hosted on cisco.com.

NOTE:

- Deployment of SSM On-Prem is now supported on AWS. However, deployment on other cloud platforms (such as GCP and so on) and physical servers (such as Cisco UCS M2, M3, and so on) is still not supported.
- Beginning with version 9-202406, SSM On-Prem can be installed on ESxi 8.0 update 3.
- Beginning with version 9-202504, SSM On-Prem supports installation on Microsoft Hyper-V and Nutanix.
- **Do not install third-party tools or applications on SSM On-Prem machine (CLI).** The SSM On-Prem system is designed and configured to operate within a controlled environment, where all installed components are validated and optimized to ensure stability, performance, and security. Unapproved software may interfere with core system functionality and prevent recovery in case of failure.

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

Obtaining Product Artifacts

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

How to Obtain Product Software

Follow the instructions below to download the installation files for the desired version of the SSM On-Prem:

1. Go to https://software.cisco.com/download/home
2. Type "Smart Software Manager" in the browser.
3. Select **Smart Software Manager** (from the Cloud and Systems Management category).
4. Select **Smart Software Manager On-Prem** in from the Software Type list.
5. Use the dropdown menu on the left to navigate between different releases. Select the release number you want. Use the **Download** button on the right to start downloading the installation files.

How to Obtain Product Information

The following documentation items are available for Smart Software Manager On-Prem:

- *Cisco Smart Software Manager On-Prem User Guide*
- *Cisco Smart Software Manager On-Prem Console Guide*
- *Cisco Smart Software Manager On-Prem Installation Guide*
- *Cisco Smart Software Manager On-Prem Migration 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.

Upgrade Procedure

NOTE:

- 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 Smart Software Manager On-Prem User Guide (Appendix 1: Manually Backing Up and Restoring SSM On-Prem).***
- **Upgrading to 9-202507 is only supported from SSM On-Prem versions 9-202406, 9-202502, and 9-202504.**
  From version **8-202404** follow the **SSM On-Prem Migration Guide (***Migrating Cisco SSM On-Prem 8 (CentOS) to SSM On-Prem 9 (Alma Linux)***).**
- 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 SSM On-Prem and the legacy devices. For more information, see the ***Cisco Smart Software Manager On-Prem User Guide (Enabling TLS 1.2 Legacy Ciphers).***

See the following sections for more information on the SSM On-Prem system upgrade.

Upgrading a System Prior to Version 9

If you are upgrading SSM OnPrem from a version prior to 9, please see:

Cisco Smart Software Manager On-Prem Migration Guide (Migrating Cisco SSM On-Prem 8 (CentOS) to SSM On-Prem 9 (Alma Linux)).

Upgrading a High Availability (HA) Cluster

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

Cisco Smart Software Manager On-Prem Installation Guide (Appendix 4 Upgrading a High Availability Cluster).

Getting Support with Technical Assistance Center (TAC)

Cisco provides around-the-clock, award-winning technical support services, online and over the phone to all customers, partners, resellers, and distributors who hold valid Cisco service contracts. To best meet customers' needs, TAC offers a wide variety of support options.

Opening a Case about a Product and Service

Follow these steps to open a support ticket for registering products or issues with SSM On-Prem.

NOTE: Please have your Cisco.com User ID, Contract and Serial number(s) ready when you contact Cisco Support to prevent any delays with your support request.

Step	Action
Step 1	Go to: https://mycase.cloudapps.cisco.com/case.
Step 2	Once in the Support Case Manager webpage, keep all the default settings and scroll down the left side of the page and click **Open New Case**. The Service Options pop-up opens on the left side of the screen.
Step 3	Select **Products and Services**.
Step 4	On the right section of the tab screen, click **Open Case**.
Step 5	Make sure the Request Type is set to **Diagnose and Fix and** then scroll down the screen to the **Bypass Entitlement** field.
Step 6	In the Bypass Entitlement field, select **Software Licensing Issue** from the drop-down list.
Step 7	Click **Next**.

Step 8	In the Describe Problem screen, select the **Ask a Question** for the Severity level.
Step 9	Enter the **Title** and **Description** and all **pertinent information**.
Step 10	Review the information you entered and click **Submit Case**. Your query has been submitted.

Opening a Case about a Software Licensing Issue

To open a case for CSSM licensing (software.cisco.com), follow these steps:

NOTE: Please have your Cisco.com User ID, Contract and Serial number(s) ready when you contact Cisco Support to prevent any delays with your support request.

Step	Action
Step 1	Go to: https://mycase.cloudapps.cisco.com/case
Step 2	Once in the Support Case Manager webpage, keep all the default settings and scroll down the left side of the page and click **Open New Case**. The Service Options pop-up opens on the left side of the screen.
Step 3	Select **Software Licensing**.
Step 4	Scroll down and select the **Category** that fits your needs.
Step 5	Click **Open Case**.
Step 7	Enter the **Title** and **Description** and all **pertinent information** in the optional fields. **NOTE**: You can also begin a **chat** using the chat screen on the right side of the screen.
Step 8	Review the information you entered, and then click **Submit Case**. Your license query has been submitted.

Smart Software Licensing (software.cisco.com)

Go to Smart Software Manager to track and manage your Smart Licenses.

Under **Convert to Smart Licensing**, you can convert PAK-based licenses to Smart Licenses (if applicable).

Smart Accounts

Go to the **Administration** section of Cisco Software Central to manage existing Smart Accounts or to request a new account from the choices.

- Go to Request Access to an Existing Smart Account to access your company's account.
- For training and documentation click here.

Enterprise License Agreements (ELA)

Go to the ELA Workspace to manage licenses from ELA.

Other self-serve licensing functions are available. Please go to our Help page for how-to videos and other resources.

For urgent requests, please contact us by phone.

To update your case, either send attachments or updates to attach@cisco.com and include the **case number** in the Subject line of your email. Please **do not** include licensing@cisco.com in your email with the engineer.

NOTE: The SSM 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 SSM On-Prem, carries browser 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 SSM 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 Widget > Certificates Tab.

Release Specifications

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

Version 9 Release 202507

Release Date: 25/07/2025

New Features

Version 9 Release 202507 introduces the following new features:

Three-Node High Availability (HA) Cluster Support for IPv6

With this release, the three-node High Availability (HA) architecture is now supported by IPv6 SSM On-Prem deployments.

It ensures enhanced performance, robust failover capabilities, continuous service availability, and reliability compared to the current two-node IPV6 HA setup. A three-node (Active-Active)

HA cluster consists of three nodes that are all simultaneously active and participate in handling workloads. All three nodes work in parallel to distribute the load, increase throughput, and ensure high availability.

Once High Availability (HA) is successfully established, the system requires some time to synchronize the database across all three nodes. This synchronization process ensures that all nodes have the latest configuration and data.

As a result, there may be a brief delay before the data (such as browser certificates and product certificates) is fully propagated to all three nodes from the source of truth (SoT) and is reflected on the Virtual IP (VIP) as well. During this period, certificate changes may not be immediately visible on every node or through the VIP until the synchronization is complete. This delay is expected, and it is resolved once the database is synced across the HA cluster.

This behavior of delayed propagation of the certificates is observed in IPv4 three node cluster as well.

NOTE: The Three-node High Availability (HA) for IPv6 provides support only for the SSM On-Prem version 9-202507 and above. For SSM On-Prem version 9-202504, the three-node High Availability (HA) is supported only by IPv4.

Enhanced Alert Messages for License Exchange Operation on SSM On-Prem

Enhanced alert messages have been introduced in SSM On-Prem as part of the license exchange operation. These alerts notify users when the transaction source of a license is changed after a license exchange. This feature ensures that users are well-informed about device license mapping changes and provides guidance on the next steps.

The alerts are displayed across different tabs in the SSM On-Prem interface, as outlined below:

- Alerts on the Activity Log Tab

  Navigation Path: On-Prem License Workspace > Smart Licensing > Activity > Event Log
  Alert Message:
  The device <device name> has been mapped to a different transaction source after the exchange operation. Please synchronize with Cisco CSSM to get updated transaction information.

- Alerts on Product Instances and SL Using Policy Tab
  Navigation Path: On-Prem License Workspace > Smart Licensing > Inventory > Product Instances
  Alert Message:
  The device <device name> has been mapped to a different transaction source after the exchange operation. Please synchronize with Cisco CSSM to get updated transaction information.

- Alerts on the Inventory - Event Log Tab
  Navigation Path: On-Prem License Workspace > Smart Licensing > Inventory > Event Log
  Alert Message:

The <device name> has been mapped to a different transaction source after the exchange operation. Please synchronize with Cisco CSSM to get updated transaction information.

Association Between Managed Product with Source Entitlement is Ensured in SSM On-Prem

This release introduces a feature in SSM On-Prem that ensures the retention of the initial association of Managed Products with their Transaction Source. The association will persist unless explicitly changed through user specific actions or predefined conditions (the license reaches the end of term and is removed). This ensures consistency and control over license allocation and management.
Managed Products (e.g., APs) will retain their initial transaction source association unless:

- The User manually releases the association via the UI.
- The license is removed from the Virtual Account (VA) by the user.
- The license reaches the end of its term and is automatically removed.

Exclusions:
Transaction source persistence will not apply if a RUM report contains APs from a different Virtual Account (VA) (e.g., a different Wireless LAN Controller (WLC).
Acknowledgment Updates:
The acknowledgment (ACK) file will reflect changes to the transaction source association only after user-led actions or when the specified conditions are met.

Enhancements in ACK (Acknowledgment) File to Smart Agent for SSM On-Prem

This release introduces enhancements to the ACK (acknowledgment) file sent from SSM On-Prem to the Smart Agent. These enhancements allow the inclusion of transaction source association details, authorized and out-of-compliance counts, and subscription term details. Additionally, specific accommodations are made for devices using legacy licensing mechanisms.

Key Features:

1. The ACK (acknowledgment) file is enhanced with the following inclusions-

Entitlement Status: Indicates compliance (OK) or out-of-compliance (OOC).

Details for Out-of-Compliance:

- Total license count.
- Optional list of non-compliant managed products.
- Reason for non-compliance (noLicense, notEnough, or termExpired).

Details for Authorized:

- Total authorized license count.
- Optional list of managed products.

Subscription information:

- subRefId (subscription ID).
- Start and end dates.
- Authorized count for each subscription.

2. Support for the legacy devices is extended as follows - SL Devices: Receive a simple "In-compliance" or "Out-of-compliance" status.

SLP Devices: Receive acknowledgment of RUM (Report Usage Message) receipt.

3. SSM On-Prem and CSLU are updated to handle the new ACK file format for products using the UNX platform.

The new ACK file structure has been integrated into SSM On-Prem and CSLU to accommodate products running on the UNX platform.

SSM On-Prem Allows Exchange Consumption

In this release the SSM On-Prem allows exchange consumption between the transaction source of an associated license and the customer preferred transaction. This enhancement allows licenses which have no transaction source associated with them to be included in exchange.

Enablement of Product Analytics in SSM On-Prem

SSM On-Prem now supports Product Analytics (PA) an enhancement of the device telemetry feature. PA collects and synchronizes product usage data with CSSM, providing improved visibility into device behavior and license usage patterns.

A product analytics drop-down is introduced in the CSSM (Cloud). Product Analytics (PA) for your Smart Account can only be enabled/disabled in CSSM (Cloud) UI.

In CSSM (Cloud), go to **Preferences> Product Analytics** to change the PA flag for your Smart Account.

After enabling PA on CSSM (Cloud), perform a full synchronization between SSM On-Prem and CSSM (Network/Manual) before requesting data from devices. Users can view the PA enabled/disabled status in the Sync request. This ensures the updated PA status is applied to SSM On-Prem and data collection can begin.

SSM On-Prem has no control over the PA flag. It can only be enabled or disabled in CSSM.

NOTE: **Exclusions:**

- The older 'device telemetry' feature is not supported. SSM On-Prem, and CSSM in connected mode will not accept device telemetry. The On-Prem, CSLU and CSSM will not set the telemetry capability in any response. As a result, a product with device telemetry enabled will have it disabled.
- If the smart agent supports Product Analytics (PA) and the SSM On-Prem supports device telemetry, the smart agent will disable PA because the On-Prem does not support in this configuration.

Idle Timeout Mechanism for Command Line Interface (CLI) Sessions

In the 9-202507 release of SSM On-Prem, an idle timeout mechanism was introduced for command line interface (CLI) sessions to enhance security and usability. If no activity is detected and a session remains idle (inactive) for **10 minutes**, the session is automatically terminated.

This ensures that unattended CLI sessions don’t remain open for an indefinite period, hence reducing the potential security risks.

A termination notification is displayed to the user after the timeout.

Support for Multiple Syslog Servers

Cisco Smart Software Manager On-Prem now supports sending logs to **multiple syslog servers** simultaneously. Previously, logs could only be routed to a single syslog server.

This new support extends usability and enables the users to configure multiple syslog endpoints via the graphic user interface (GUI), ensuring that the logs are routed to all specified destinations. With multiple syslog servers, if one is offline, logs continue to flow to the other servers and ensures uninterrupted monitoring.

For configuration details, please refer to the Syslog tab in the user guide.

(Refer to the 'Syslog Tab under the Settings Widget section' from the '*Cisco Smart Software Manager On-Prem User Guide*' for further information).

NOTE: Upgrades to version 9-202504 are now supported from all 9.x versions of SSM On-Prem.

Accessibility Enhancements

This release includes accessibility improvements, focusing on enhanced keyboard navigation, clearer error notifications, improved information structure, and optimized component design for better usability and inclusivity.

Nutanix Platform Support for SSM On-Prem

Cisco Smart Software Manager On-Prem now supports installation on Nutanix infrastructure. This enhancement expands platform compatibility beyond AWS, VMware ESXi, and Microsoft Hyper-V, offering users greater flexibility to deploy SSM On-Prem Nutanix-based virtual environments.

(Refer to section 'Installing on a VM using the .iso file [Nutanix]' from the '*Cisco Smart Software Manager On-Prem Installation Guide*' for further information).

KVM (Ubuntu-based) Installation Support

Starting with release **9-202507,** SSM On-Prem can be installed on **KVM (Ubuntu-based)** environments. This provides an additional deployment option for customers who prefer KVM virtualization.

Qualified KVM version: Installation is supported only with **ubuntu-24.04.desktop-amd64.iso.**

Azure Platform Support for SSM On-Prem

Cisco Smart Software Manager On-Prem now supports 3-node High Availability (HA) deployment on Microsoft Azure. With this addition, customers can deploy SSM On-Prem in Azure-based virtual environments, ensuring seamless setup and reliable license management.

(Refer to section *'3-Node High Availability (HA) Deployment for Azure'* from the '*Cisco Smart Software Manager On-Prem Installation Guide*' for further information).

AWS 3- Node HA Deployment Support for SSM On-Prem

Cisco Smart Software Manager On-Prem now supports **3-node High Availability (HA) deployment on AWS.** This enhancement extends existing AWS support by introducing Elastic IP (EIP) for VIP management, ensuring robust failover handling and improved reliability for AWS-based environments.

(Refer to section *'3-Node High Availability (HA) Deployment for AWS'* from the '*Cisco Smart Software Manager On-Prem Installation Guide*' for further information).

Fixes

This release introduces the following fixes.

Bug ID	Description
CSCwe18517	**Clicking 'cancel' in Request Account Detail window results in unexpected error message** The unexpected error message that appeared upon clicking the 'cancel' button in the Request Account Detail window is fixed and the cancel button is functioning without triggering any unexpected error message.
CSCwf11244	**Incorrect display and report handling in Product Instance Report** The product instance report exhibited the following issues: 1. Display of incorrect number of devices and virtual accounts 2. The product type report window didn't close automatically after running the report 3. The product instance report was downloaded with the file name 'null'. Now, the product instance report seamlessly displays the correct data and is working as expected.
CSCwh92602	**Incorrect sizing of 'Actions for Selected' and 'Export/Import All' buttons in SL Using Policy Tab** These buttons were not aligned with the required UI specifications. The buttons are disproportional sized compared to other elements on the tab, affecting the visual consistency of the interface. The issue is resolved, and the consistent height and width parameters of these buttons are ensured to align them to the interface design guidelines.
CSCwm90507	**Visual distortion in Event Log of Network widget** The event log displayed within the network widget appeared visually squished, resulting in poor readability and an impact on the overall user experience. The log now displays in a clean, readable format, consistent with the rest of the interface design.
CSCwq46449	**'Save' button not enabled on changing remote logging under Syslog tab in Settings** In the **Settings** section, under the **Syslog** tab, it was observed that the 'Save' button fails to get enabled upon enabling and disabling remote logging. Normally, when a user modifies any settings, the system should detect the change and activate the Save button. Now, after every change detected on syslog settings save button is automatically enabled.
CSCwo95295	**UD file download failed due to nil value in 'managed by' field after upgrade** Resolved a defect that prevented users from exporting the usage data (UD) files after upgrading from 9-202407 to 9-202412. The system previously displayed an error stating "Error exporting data to offline file as there are no devices added," even when devices were present. This

	issue has been fixed, and UD file export functions correctly after upgrade.
CSCwp20187	**HSEC connected mode not working on 5.1 and 5.3 and above devices when Instant Auth is off** Fixed an issue where HSEC connected mode failed to initialize on devices running version 5.3 and above when instant authentication was disabled. The root cause of the issue was that On-Prem was unable to correctly process the auth Key requests from said devices and get the required auth codes. It is now ensured that authcode is installed on devices operating in connected mode enabling the system to send auth_key requests to CSSM; HSEC licenses are reserved restoring the functionality.
CSCwp28688	**SSM On-Prem: 9-202504 upgrade stuck on Linux/macOS** During the upgrade to SSM On-Prem 9-202504, some users experienced the upgrade process getting stuck with the message "waiting for frontend." This was initially addressed with a supplementary patch to work around the issue. In this release, the issue has been fully resolved, eliminating the need for the supplementary patch and ensuring smooth, uninterrupted upgrades across all supported systems.
CSCwq47151	**Device trust request included in usage export to CSSM** Fixed an issue where usage exports from SSM On-Prem to CSSM did not include the required device trust request. This prevented devices from being validated in CSSM. The export now correctly includes the trust request ensuring devices appear and sync as expected.

Known Issues

Bug ID	Description
CSCwq46453	**Syslog logging fails with IPv6 configuration** When configuring remote syslog logging using an IPv6 address, logs are not forwarded as expected. Logs do not appear on the configured syslog server if an IPv6 address is used.
CSCwq47153	**ARP command in SSM On-Prem console is not working** ARP (Address Resolution Protocol) is a Layer 2 protocol used in IPv4 networks to map IP addresses to physical MAC addresses on a local network segment. It can be used to display IP addresses and delete an entry from the ARP cache. **ARP protocol is supported only for IPv4 entries.** Therefore, the **ARP command will not display or manage entries for SSM On-Prem deployed through IPv6 configuration.** The SSM On-Prem console provides an option for displaying IP address resolution and control through ARP.
CSCwq46443	**The list of product instances is not displayed under the license tab** The list of product instances is not displayed as expected, upon clicking the 'In Use' count under the license tab. This issue is specific to

	scenarios with wireless LAN Controller (WLC) devices and associated Access Points (APs) with instances of removed Access Points. The issue that has been identified is under investigation for resolution.
CSCwq44278	**TLS cipher mismatch between three-node and single-node IPv4 setups** During TLS regression testing a mismatch is observed between three-node and single node IPv4 setups where the TLS regression testing is failing on the three-node cluster, while the same tests are successful on the single-node IPv4 setup. This issue is acknowledged and is being investigated for a fix.
CSCwq26278	**TLS 1.1 protocol or obsolete ciphers being unexpectedly enabled** In some cases, during upgrades or fresh deployments of version 9-202507, you might encounter TLS 1.1 protocol or obsolete ciphers being unexpectedly enabled. This issue is under investigation. The following steps circumvent the issue - 1. Navigate to Admin Workspace > Security 2. Toggle the following settings ON, then OFF (ensure clicking Save each time after you turn the toggle ON and OFF): - Enable obsolete ciphers - Enable TLS 1.1 protocol SSM On-Prem supports TLS 1.2 and TLS 1.3 protocols by default, using the following strong cipher suites: TLS 1.3 Ciphers: - TLS_AES_256_GCM_SHA384 - TLS_AES_128_GCM_SHA256 TLS 1.2 Ciphers: - ECDHE-RSA-AES128-GCM-SHA256 - ECDHE-RSA-AES256-GCM-SHA384

Resolved Vulnerabilities and Exposures

CVE-2024-41184, CVE-2025-22871, CVE-2024-12797, CVE-2025-0395, CVE-2024-24791, CVE-2024-52616, CVE-2025-21605, CVE-2025-21966, CVE-2024-4741, CVE-2024-5535, CVE-2025-26465, CVE-2023-4752, CVE-2024-58069, CVE-2025-4802, CVE-2025-21633, CVE-2025-21993, CVE-2024-58007, CVE-2025-22055, CVE-2025-37749, CVE-2024-53150, CVE-2025-21756, CVE-2025-37785, CVE-2024-55549, CVE-2025-21920, CVE-2025-21997, CVE-2025-21964, CVE-2024-4603, CVE-2024-24788, CVE-2025-21926, CVE-2024-58005, CVE-2024-2511, CVE-2024-31449, CVE-2023-45145, CVE-2024-8176, CVE-2025-37943, CVE-2025-21927

NOTE: SSM On-Prem does not use OpenSSH. Instead, it uses CiscoSSH internally. Therefore, some of the reported CVEs related to OpenSSH have been identified as false positives.

These CVEs do not impact system security and required no further action:

CVE-2023-25136, CVE-2023-28756, CVE-2023-38408, CVE-2023-48795, CVE-2023-51385, CVE-2024-6387, CVE-2024-6409, CVE-2023-29483, CVE-2023-29483

NOTE: After successfully upgrading the SSM On-Prem, a **Full Synchronization** of all SSM On-Prem accounts must be performed.

Version 9 Release 202504

Release Date: 23/05/2025

New Features

Version 9 Release 202504 introduces the following new features:

Three-Node High Availability (HA) Cluster

With this release, three-node architecture is now also available in addition to two-node architecture.

It ensures enhanced performance, robust failover capabilities, continuous service availability, and reliability compared to the current two-node HA setup. A **three-node (Active-Active) HA cluste**r consists of three nodes that are all simultaneously active and participate in handling workloads. All three nodes work in parallel to distribute the load, increase throughput, and ensure high availability.

NOTE: In SSM On-Prem version 9-202504, three-node High Availability (HA) is supported over IPV4; it is not supported over IPV6. This functionality is planned for the next release.

The current release continues to support IPv6 for two-node HA configurations and IPv6 stand-alone SSM On-Prem deployments.

NOTE: Upgrades to version 9-202504 are now supported from all 9.x versions of SSM On-Prem.

Seamless Failover without Downtime for SSM On-Prem High Availability Cluster

In the 9-202504 release of SSM On-Prem, the failover times are improved for a two-node HA active-standby cluster as well. However, since the three-node HA operates in an active-active configuration, the failovers are significantly more seamless, with zero downtime for the virtual IP.

The standby takeover process in the three-node high availability setup has been optimized to significantly minimize downtime. In the event of a failure of one active node, the remaining two active nodes seamlessly maintain cluster functionality without any interruption to the service.

Once the failed node recovers, it automatically rejoins the cluster and resumes normal operations within five minutes.

Even if two out of the three nodes go down, the cluster continues to operate without any disruption. Upon recovery, both nodes rejoin the cluster and restore full functionality within five minutes.

Hyper V Platform Support for SSM On-Prem

In addition to AWS and VMware ESXi, Cisco Smart Software Manager On-Prem now supports installation on Microsoft Hyper-V. This new support extends platform compatibility, allowing deployment of SSM On-Prem in Windows-based virtual environments, ensuring seamless setup and enhanced management.

Accessibility Enhancements

This release includes accessibility improvements, focusing on enhanced keyboard navigation, clearer error notifications, improved information structure, and optimized component design for better usability and inclusivity.

Fixes

This release introduces the following fixes.

Bug ID	Description
CSCwh46438	**Device fails to renew the id after a switchover, in a device HA setup** In a device HA setup, the switchover from device A to device B is accompanied by a renewal of an id which should be automatically renewed with device B. The device fails to renew this id. Now, after setting up the device HA cluster, when the device HA switches the HA role from device A to B, the id is successfully renewed.
CSCwm65570	**Issue with generation of License Subscriptions and Product Instance Report** This issue was affecting the generation of reports for the selected virtual account of license subscription details and product instance. Now, the report for a selected virtual account of license subscription details is seamlessly displayed, and the product instance report correctly reflects the product type and corresponding device counts for the selected virtual account.
CSCwo20255	**Issue with License transfer option between local virtual accounts** Following the upgrade of the SSM On-Prem server to version 9-202502, license transfer option between local virtual accounts was not visible, and the transfer count column was disabled. The license transfer option is visible now, and the transfer count column is enabled.
CSCwm98996	**Unable to uncheck the box for export-controlled functionality while creating a registration token in smart licensing** This issue prevented users from unchecking the box that allows export-controlled functionality on the registered products, while creating a new registration token under the general tab in smart licensing. This functionality is now working well and allows users to successfully uncheck the option during token creation.

CSCwn61644	**Mismatch in available to use licenses between SSM On-Prem and CSSM** In this issue (which is limited to rare scenarios) it was identified that SSM On-Prem was not displaying the correct number of licenses, resulting in a mismatch of license data specifically for **'Available to Use'** licenses between SSM On-Prem and CSSM. This issue is resolved, and the correct number of licenses is reflected in the system.

Known Issues

Bug ID	Description
CSCwp20187	**Installation of High-Security (HSEC) Licenses fails on devices running Cisco IOS 17.09+(Smart Agent 5.3 or above) when instant auth is disabled** The installation of High-Security (HSEC) licenses fails on devices running Cisco IOS version 17.09 or later (Smart Agent version 5.3 or above), when the Instant Authorization feature is disabled from the Admin Workspace. This issue has been observed exclusively in Smart Software Manager (SSM) On-Prem deployments operating in **connected mode**, where network connectivity to the Cisco Smart Software Manager is established.
CSCwp28688	**Fail to upgrade SSM On-Prem from version 9-202406 or 9-202502 to version 9-202504 and when installing the version 9-202504** Affected Versions: • Upgrades from 9-202406 and 9-202502 to 9-202504 • Fresh install of 9-202504 **Issue Description:** Users may face the following issues: • When upgrading from 9-202406 or 9-202502 to 9-202504 using SSM_On-Prem-9-202504_Upgrade.sh, the process may stop at the following message: *“Waiting for frontend...”* • After a fresh installation of 9-202504, the On-Prem GUI does not come up, and no progress is observed. • After successful upgrade or installation, excessive logging in may occur, leading to disk space issues. **Workaround:** Applying the Supplementary Patch is required for all upgrades to, or fresh installations of, version 9-202504 regardless of whether the upgrade or installation completes successfully. For detailed instructions, refer to the **Supplementary Patch Guide**.

Resolved Vulnerabilities and Exposures

CVE-2020-15778, CVE-2024-45018, CVE-2024-43854, CVE-2024-41014, CVE-2024-41013, CVE-2024-41005, CVE-2024-40998, CVE-2024-40995, CVE-2024-40977, CVE-2024-40972, CVE-2024-40960, CVE-2024-40931, CVE-2024-40904, CVE-2024-39504, CVE-2024-39472, CVE-2024-36244, CVE-2024-26961, CVE-2024-26935, CVE-2024-26923, CVE-2024-26826, CVE-2024-26640, CVE-2024-2201, CVE-2021-47383, CVE-2021-33621, CVE-2023-28755, CVE-2023-28756, CVE-2024-27280, CVE-2024-27281, CVE-2024-27282, CVE-1999-0524.

NOTE: After successfully upgrading the SSM On-Prem, a **Full Synchronization** of all SSM On-Prem accounts must be performed.

Version 9 Release 202502

Release Date: 14/02/2025

New Features

Accessibility Enhancements

This release includes significant accessibility improvements, focusing on enhanced keyboard navigation, clearer error notifications, improved information structure, and optimized component design for better usability and inclusivity.

Fixes

This release introduces the following fixes.

Bug ID	Description
CSCwf11854	**Lack of user experience when oauth token is invalid when trying to SLPs** Resolved an issue where users were not prompted to reauthenticate when OAuth tokens were missing, expired, or invalid during instant SLP synchronization. Now, users are prompted to enter CCO credentials, ensuring a seamless authentication process similar to Network Sync. Additionally, an alert is displayed if the refresh token has less than 30 days of validity.
CSCwj58181	**Alert is not getting changed for SLP devices of SA version 5.1 post-upload** Fixed an issue where alerts were not updating correctly for certain SLP devices (ISR4321/K9, VG450/K9, C8200L-1N-4T, ISR4431/K9, VG400) after importing the acknowledgment archive from CSSM. Now, the **is_sent** status updates correctly post-usage report download, and the alert message changes to **Acknowledgement received from CSSM** in both the database and UI.
CSCwk63542	**On-Prem 9-202406 System Health tab data (Uptime, RAM, Disk, CPU) unreliable** Resolved an issue where Uptime, RAM, Disk, and CPU usage in the System Health tab were not updated correctly in the Admin workspace.

	Uptime could become stuck at a random value, and memory usage remained constant regardless of system load. The metrics now update accurately and reflect real-time system performance.
CSCwn70316	**Certificate failing when Verify Server Certificate checked** Fixed an issue were enabling the **Verify Server Certificate** option in **Admin Workspace > Access Management > LDAP or OAuth2** caused login failures. Even after adding new CA certificates, authentication failed upon system reboot due to certificates not persisting in the backend. The issue has been addressed to ensure certificates remain intact and authentication functions correctly with verification enabled.
CSCwn77998	**Both network and manual sync are failing after upgrading to version 9-202412** Resolved an issue where both **network sync** and **manual sync** failed after upgrading to **version 9-202412**. Manual sync displayed an invalid synchronization response file error, while network sync failed due to a missing translation key. The issue has been fixed to ensure seamless synchronization after the upgrade.
CSCwn81730	**Exchange should be greyed out for non-unx devices during a transfer** Fixed an issue where the **Exchange** option was incorrectly available for non-UNX devices during a transfer. Now, the **Exchange** option is **greyed out** for unsupported devices, improving user experience and preventing unintended actions.
CSCwn22463	**SLP HA sync requests were not removed after manual SLP sync** During SLP sync, when the acknowledgement (ACK) file was uploaded to the SSM On-Prem, the sync requests were not removed. As a result, the reports were downloaded repeatedly, eventually increasing the size of the downloaded file (this file is downloaded during manual SLP Sync from SSM On-Prem to CSSM). This issue was observed even after the device polled On-Prem and successfully received the acknowledgement on the device. The way older reports are handled during manual Smart Licensing using Policy (SLP) synchronizations is now improved. Previously, uncleared reports could lead to "Report already processed" errors in CSSM and unnecessarily large file sizes. This update ensures that older reports are now properly processed and removed, preventing these issues and optimizing file size.

Known Issues

Bug ID	Description
CSCwn61644	**Duplicate Transaction IDs Not Accepted in On-Prem, Causing License Mismatch** On-Prem is not accepting duplicate transaction IDs with different license quantities, leading to mismatched license counts between CSSM and On-Prem. Even after CSSM reprocessed the licenses, some quantities were not reflected correctly in On-Prem.

Resolved Vulnerabilities and Exposures

No Vulnerabilities.

Version 9 Release 202501

Release Date: 24/01/2025

New Features

Accessibility Enhancements

This release includes significant accessibility improvements, focusing on enhanced keyboard navigation, clearer error notifications, improved information structure, and optimized component design for better usability and inclusivity.

Fixes

This release introduces the following fixes.

Bug ID	Description
CSCwc84431	**SSM On-Prem account license page stops loading when PoolEntitlementSummary has charge type nil value** Resolved an issue where the SSM On-Prem licenses page under Inventory would crash when encountering a null value in the **Billing Type** field. The front end has been updated to handle null values gracefully, ensuring uninterrupted page functionality. Backend changes ensure that the `charge_type` value will no longer be null.
CSCwb68754	**TGCert's expiry date is not getting updated on sync with CSSM** Resolved an issue where the product certificate (TGCert) was not updating during sync with CSSM, causing it to expire after a year and potentially impacting operations.

Known Issues

Bug ID	Description
CSCwn70316	Certificate failing when Verify Server Certificate checked.

Resolved Vulnerabilities and Exposures

No Vulnerabilities.

Version 9 Release 202412

Release Date: 20/12/2024

New Features

Version 9 Release 202412 introduces the following features:

Exploring New Flexibilities and WLC Device Support

The latest version of SSM On-Prem enhances support for Wireless LAN Controller (WLC) devices and associated Access Points (APs). This includes advanced features such as Exchange License Transaction Source, which enables seamless exchange of licenses source transactions or product instances under the Licenses or Product Instances tabs using an intuitive stepper interface. Additionally, this version introduces support for Wi-Fi 7 wireless devices using Cisco Networking Licenses.

The High Availability (HA) feature, previously available for other device types, has now been extended to support WLC devices. In HA configurations, licenses are dynamically managed to ensure only the active controller consumes licenses, maintaining accurate device classifications for active, standby, and non-reporting roles. This provides real-time compliance updates and efficient license management for WLCs and APs in HA mode.

Support for Deploying SSM On-Prem on AWS

SSM On-Prem now supports deployment on AWS cloud platforms, enabling customers to reduce hardware costs by leveraging their existing cloud infrastructure. This allows seamless deployment using Amazon Machine Images (AMI) with compliance with DISA STIG guidelines and IL6 certification. Key enhancements include VMDK to AMI conversion, AWS-specific networking configurations, and high-availability (HA) setup support. For more details, refer to the "Deploying SSM On-Prem on AWS" section in the SSM On-Prem Installation Guide.

Accessibility Enhancements

This release includes significant accessibility improvements, focusing on enhanced keyboard navigation, clearer error notifications, improved information structure, and optimized component design for better usability and inclusivity.

Fixes

This release introduces the following fixes.

Bug ID	Description
CSCwi28251	**Device HA support for SLP** SSM On-Prem now includes enhanced support for Device High Availability (HA) in SLP mode. This feature ensures accurate license consumption tracking for ACTIVE devices in a stack while seamlessly handling failover and switchover scenarios. Updates include processing reports from stacked devices, distinguishing ACTIVE, STANDBY, and MEMBER roles, and generating consolidated ACKs for usage reports. Additionally, the user interface now provides a detailed view of the stack, displaying device roles and the hostname of the ACTIVE device for better clarity. **Note:** Pull mode is not supported for SLP Device HA in Smart Agent versions 5.1 to 5.3>.

Known Issues

No Known Issues.

Resolved Vulnerabilities and Exposures

CVE-2023-20584, CVE-2023-31356, CVE-2022-24805, CVE-2022-24806, CVE-2022-24807, CVE-2022-24809, CVE-2022-24810, CVE-2022-24808, CVE-2021-47383, CVE-2024-2201, CVE-2024-26640, CVE-2024-26826, CVE-2024-26923, CVE-2024-26935, CVE-2024-26961, CVE-2024-36244, CVE-2024-39472, CVE-2024-39504, CVE-2024-40904, CVE-2024-40931, CVE-2024-40960, CVE-2024-40972, CVE-2024-40977, CVE-2024-40995, CVE-2024-40998, CVE-2024-41005, CVE-2024-41013, CVE-2024-41014, CVE-2024-43854, CVE-2024-45018, CVE-2024-6232, CVE-2024-26929, CVE-2024-36899, CVE-2023-52439, CVE-2024-38573, CVE-2024-38570, CVE-2024-36016, CVE-2024-26991, CVE-2024-38562, CVE-2024-27022, CVE-2024-38615, CVE-2024-41071, CVE-2024-35895, CVE-2024-42225, CVE-2024-26930, CVE-2024-38601, CVE-2023-52884, CVE-2024-42246, CVE-2024-26739, CVE-2024-26931, CVE-2024-26947, CVE-2024-40984, CVE-2024-26720, CVE-2024-36000, CVE-2024-35791, CVE-2024-42082, CVE-2024-38559, CVE-2024-36883, CVE-2024-40936, CVE-2023-52463, CVE-2024-38619, CVE-2024-36979, CVE-2024-35797, CVE-2024-42096, CVE-2023-52801, CVE-2024-40927, CVE-2024-26886, CVE-2024-35875, CVE-2024-41055, CVE-2024-41073, CVE-2024-42102, CVE-2024-36019, CVE-2024-41044, CVE-2024-26629, CVE-2024-41096, CVE-2024-26630, CVE-2024-42131, CVE-2024-41040, CVE-2024-26946, CVE-2024-42284, CVE-2021-47385, CVE-2024-35989, CVE-2024-27403, CVE-2024-36889, CVE-2024-36978, CVE-2024-39502, CVE-2024-38556, CVE-2024-42272, CVE-2024-39483, CVE-2023-52658, CVE-2024-42079, CVE-2024-40959, CVE-2024-6119

Version 9 Release 202410

Release Date: 31/10/2024

New Features

Version 9 Release 202410 introduces the following features:

SSM On-Prem APIs for adding and editing SLP devices

The 2 newly added SSM On-Prem APIs are designed to streamline the management of SLP product instances. These APIs allow users to effortlessly add and edit device details, just as easily as can be achieved through the user interface. This enhancement ensures a more efficient and intuitive experience for managing Smart License Using Policy devices (Refer to section 'Using smart software manager On-Prem APIs' from the '*Cisco Smart Software Manager On-Prem User Guide'* for further information).

SSM On-Prem API for License Usage and Device Details Retrieval for SLP Mode

The newly added API is designed to retrieve License Usage and Device Details for a specific product instance as opposed to all product instances on On-Prem account level. Users can search based on seven unique device identifiers, including *udi_pid, udi_serial_number, suvi, uuid, udi_vid, mac_address,* and *host_identifier*, providing more precise control over results. This API streamlines access to detailed data, supports filtering by virtual accounts, and offers pagination for organized results. Enhanced error messages for unmatched or invalid records improve the experience, making license and device management in Smart Accounts easier and more efficient. (Refer to section 'Using smart software manager On-Prem APIs' from the '*Cisco Smart Software Manager On-Prem User Guide'* for further information).

Automated Database Backup Configuration via CLI

This feature introduces an automated database backup option in the SSM On-Prem system, allowing users to configure remote servers, set backup frequencies, and automate the backup processes. Administrators can set up backups via new CLI commands, view configured frequencies, and manage backup rotations with a limit of three backups. The system checks disk space availability before each backup and logs errors when space is insufficient. Additionally, high-availability setups ensure backups run only on the active node, and a help command is available for guidance on backup configurations. (Refer to section 'Automated Database Backup Configuration' from the '*Cisco Smart Software Manager On-Prem User Guide'* for further information).

Custom SSH User Creation for Enhanced Security

This feature enhances security by allowing users to disable SSH access for the default admin user on the On-Prem CLI and create a custom "last-resort" user for secure SSH access. Once created, this custom user uses key-based or password less authentication and cannot be deleted or rolled back to the default admin account. For high-availability environments, users will need to repeat this setup on standby nodes. This feature maintains flexibility for administrators by allowing TACACS users to retain access, supporting enhanced security and streamlined user management.

Immediate Authorization Code Delivery for HSEC Activation

This feature enhances HSEC activation by delivering authorization codes to devices immediately upon first communication with SSM On-Prem. This improvement allows for faster activation by sending the authorization code during the initial communication, eliminating delays that previously required waiting for a polling response. Devices in pull mode can now receive the authorization code instantly upon manual synchronization, ensuring faster and more efficient activation across different configurations and throughput levels. Existing workflows without prior SLAC uploads remain unaffected.

Fixes

This release introduces the following fixes.

Bug ID	Description
CSCwk27983	**SLP Device Registration Issues Due to IP Address Conflicts** The SLP device registration issue caused by conflicting IP addresses in On-Prem has been resolved. Devices can now register without conflicts, ensuring seamless synchronization and accurate device management in the On-Prem GUI.
CSCwk97347	**Improved workflow for RENEW requests** Resolved an issue where SSM On-Prem did not handle situations where a Smart License device failed to send an acknowledgment for a successful RENEW request. This fix ensures proper synchronization of certificates and prevents certificate validation errors.
CSCwm36660	Addressing CVE-1999-0511 and CVE-2008-5161 Vulnerabilities in SSM On-Prem Version 9-202407
CSCwm13071	Multiple vulnerabilities reported in 9-202407
CSCwm35042	Multiple vulnerabilities reported in 9-202407

Known Issues

Bug ID	Description
CSCwn06659	Whilst using tacacs+ CLI functionality, when systemadmin logs in through CLI, systemuser priveleges are assigned.

Resolved Vulnerabilities and Exposures

CVE-2008-5161, CVE-2021-33621, CVE-2023-28755, CVE-2023-28756, CVE-2023-36617, CVE-2024-24806, CVE-2024-27280, CVE-2024-27281, CVE-2024-27282, CVE-2024-35235, CVE-2024-4032, CVE-2024-4076, CVE-2024-1737, CVE-2024-1975, CVE-2024-6923, CVE-2024-37370, CVE-2024-37371, CVE-2024-34397, CVE-2024-45491, CVE-2024-45490, CVE-2024-45492, CVE-2024-37891

Version 9 Release 202407

Release Date: 08/07/2024

New Features

Version 9 Release 202407 introduces the following features:

Enhanced LDAP Group Authentication support for nested LDAP groups:

A significant improvement has been made to how SSM On-Prem handles user authentication. Previously, users in nested LDAP sub-groups could not log in, and the system did not support queries for these nested groups. With this new feature, SSM On-Prem can query both primary and nested sub-groups for authentication. This means that users in nested LDAP sub-groups can now log in seamlessly.

This enhancement is designed to support large-scale enterprise customers, making it easier for organizations with complex group structures to adopt and benefit from SSM On-Prem.

Oracle OpenLDAP Support for Enhanced Authentication:

This new feature enhances our LDAP support in SSM On-Prem. Previously, the SSM On-Prem LDAP interface had issues working with **Oracle OpenLDAP** deployments. With this update, we are adding support for “groupOfUniqueNames” to the LDAP interface in SSM On-Prem. This means that users who are using Oracle OpenLDAP can now be authenticated seamlessly in SSM On-Prem.

This improvement ensures a smoother and more reliable authentication process for organizations using Oracle OpenLDAP.

Fixes

This release introduces the following fixes.

Bug ID	Description
CSCwi49341	**Reduced unnecessary logins to PULL mode devices:** This issue where SSM On-Prem would frequently log into devices configured in PULL

Bug ID	Description
	mode, even after successfully pulling reports. This issue affected all connection methods, including Netconf and RESTconf. With this fix, SSM On-Prem will now only log in as needed, reducing unnecessary logins and improving overall system efficiency.
CSCwh46095	**Stability Improvement for Large Manual Usage Reports:** This issue that caused SSM On-Prem to crash when generating large manual usage reports is resolved. Previously, when loading more than 300 devices and 100,000+ RUM reports, the system used to consume all available RAM, causing delays of 30-45 minutes before crashing and restarting. This issue prevented the creation of bulk RUM zip files. With this fix, SSM On-Prem can now handle large manual usage reports more efficiently, ensuring stability and reliability even with extensive data. This improvement allows for smoother and faster report generation, enhancing your overall experience.
CSCwk62288	**Remote Unauthenticated Code Execution Vulnerability in OpenSSH Server (regreSSHion): CVE-2024-6387**, A signal handler race condition was found in sshd, where a client does not authenticate within LoginGraceTime seconds (120 by default, 600 in old OpenSSH versions), then the sshd SIGALRM handler is called asynchronously. However, this signal handler calls various functions that are not async-signal-safe, for example, syslog().

Known Issues

Bug ID	Description
CSCwf66111	HA Replication Issue after Failover: This issue prevents the Secondary On-Prem from replicating the data from the Primary after a failover. If this issue is encountered, reach out to TAC support for further details and workaround.

Resolved Vulnerabilities and Exposures

CVE-2024-6387, CVE-2023-28531, CVE-2023-52160, CVE-2024-1048, CVE-2023-48795, CVE-2024-22365, CVE-2023-50868, CVE-2023-40546, CVE-2024-28834, CVE-2023-3618, CVE-2023-7008, CVE-2023-2975, CVE-2023-40548, CVE-2023-4692, CVE-2023-3446, CVE-2023-46218, CVE-2023-5517, CVE-2023-43786, CVE-2024-28182, CVE-2023-52425, CVE-2021-40153, CVE-2024-25629, CVE-2023-38408, CVE-2023-25136, CVE-2023-25193, CVE-2024-2961, CVE-2023-38471, CVE-2023-38473, CVE-2024-0450, CVE-2024-33601, CVE-2024-26146, CVE-2023-40550, CVE-2023-51385, CVE-2022-48554, CVE-2022-40090, CVE-2023-6237, CVE-2023-6004, CVE-2024-28835, CVE-2023-6597, CVE-2023-3758, CVE-2023-46316, CVE-2024-32487, CVE-2023-50387, CVE-2024-25062, CVE-2023-4408, CVE-2023-40547, CVE-2023-6228, CVE-2024-0727, CVE-2023-43787, CVE-2023-5679, CVE-2023-4693, CVE-2024-33599, CVE-2023-40745, CVE-2021-29390, CVE-2023-5678, CVE-2023-6129, CVE-2024-26141, CVE-2023-47038, CVE-2024-28757, CVE-2023-38470, CVE-2024-33602, CVE-2023-38472, CVE-2023-43785, CVE-2024-33600, CVE-2023-6918, CVE-2023-3817, CVE-2021-41043, CVE-2023-38469, CVE-2022-48622, CVE-2023-40551, CVE-2022-48624, CVE-2023-6516, CVE-2024-25126

Version 9 Release 202406

Release Date: 06/15/2024

New Features

There are no new features in Version 9 Release 202406. This version of On-Prem is a migration release and not a direct upgrade.

At present the SSM On-Prem is a virtual deployment supported on ESXi7.x and ESXi8.x and the underlying Operating System is CentOS. **CentOS is going End of Life**, so the newer version of SSM On-Prem application is built on new Operating System AlmaLinux 9. You need to install On-Prem on a separate Virtual Machine (VM) and utilize the migration script to migrate data and configuration from 8-202404 to 9-202406. The migration tool along with scripts and necessary steps will be provided as part of **On-Prem Migration Guide (***Migrating Cisco SSM On-Prem 8 (CentOS) to SSM On-Prem 9 (Alma Linux)***).**

The new host operating system is AlmaLinux 9. The required configurations such as RAM, CPU and Storage space remains identical to that of SSM On-Prem 8-202404.

Fixes

This release introduces the following critical fixes, along with a few other high and medium fixes:

Bug ID	Description
CSCwe28198	**SLUP Tab does not update on switching accounts:** When there are two or more On-Prem accounts containing SLP devices, the SLUP tab is not updating, upon switching between accounts.
CSCwi31145	**Unable to Import Authorization code before SLP devices are discovered:** On-Prem does not give the ability for customers to upload CSV files containing Authorization (Auth) codes before the devices are connected.

Known Issues

Bug ID	Description

No Known Issues.

Version 8 Release 202404

Release Date: 04/30/2024

New Features

Version 8 Release 202404 introduces the following features:

Enhancing the Cipher Management in SSM On-Prem Application

In this new feature, the SSM On-Prem cipher management is enhanced to support the most secure and up to date **TLS 1.2** and **TLS 1.3** ciphers.

It is important for SSM On-Prem to keep up to date with the changes in cryptographic algorithms. Cipher suites can get outdated and pose security threats over time. To avoid these security threats, we have analyzed currently supported cipher suites, and updated them to support only the most up to date and secure ciphers.

Obsolete and weaker ciphers can still be enabled as per requirement (Refer '**Account Tab**' section under '**Security Widget**' of *Cisco SSM On-Prem User Guide*).

Provide capability to export member distinguished names (DNs) for LDAP groups

The new feature allows customers to generate and download a report of an LDAP group. The report consists of all member DNs which are part of an LDAP group. Furthermore, in the user interface, the customer will see the total number of member DNs.

Prevent LDAP user without access to an LDAP group from logging into SSM On-Prem

This feature will enhance on the current LDAP implementation permitting login to SSM On-Prem application to only LDAP users who are part of an LDAP group.

Fixes

This release introduces the following critical fixes, along with a few other high and medium fixes:

Bug ID	Description
CSCwf38271	**Export usage to Cisco is broken**
CSCwi92889	**Export Usage:** Failed to export usage for Push devices when the account has both Pull and Push devices.
CSCwf38806	**Support for Enhanced security ciphers in SSM On-Prem:** This new feature is an enhancement to SSM On-Prem supporting the most secure and up to date TLS 1.2 and TLS 1.3 ciphers.

Known Issues

Bug ID	Description
CSCwh46438	During device HA setup, after performing a switchover, device fails id renew.

Resolved Vulnerabilities and Exposures

HIGH

- CVE-2022-28733

MEDIUM

- CVE-2023-20592
- CVE-2023-48795
- CVE-2023-51385

Not affected by

- CVE-2023-51384

Version 8 Release 202401

Release Date: 03/15/2024

New Features

Version 8 Release 202401 introduces the following features:

SLP Compliance

Re-introduced the enforcement modes (entitlement status) used in SL mode into SLP mode for entitlement tags.

- This includes Authorized, Out Of Compliance, Not Authorized.
- These will apply to all entitlement tag types, (Non-enforced, enforced, export)
- Evaluation mode & Authorization expired will NOT be supported.

Filter syslogs based on severity

Added an option in *Admin workspace -> Setting ->Syslog*, to select between syslog levels based on the priority level, all syslogs from that severity level or higher will be forwarded to the server.

Syslog categories are ranked as:

1. Level 1 **ALERT**: major error log
2. Level 2 **WARN**: minor error and warning log
3. Level 3 **INFO**: informational log

Rate limiting

Depending on the computing resources, you will either drop the request or process it. The device will retry the dropped messages. These updates help in reducing the traffic load and thereby managing the Cisco SSM On-Prem CPU and RAM spike issues.

Fixes

This release introduces the following critical fixes, along with a few other high and medium fixes:

Bug ID	Description
CSCwi89642	AppHA - onPrem no longer acknowledges pairs - incorrect entitlement cons
CSCwi92791	Vulnerabilities reported by tenable scan
CSCwi65731	Need to fix vulnerability CVE-2023-38408 on On-Prem 8-202304
CSCwi48205	Unnecessary call made to /cslu/v1/core/conf
CSCwi43173	SSM-Onprem Importing HSEC ACK from CSSM using "Import from Cisco" puts the data in the wrong table

Bug ID	Description
CSCwi37443	is_sent flag never changes in offline mode for SA == 5.1
CSCwi34955	Vulnerabilities for Smart Software Manager On-Pre
CSCwi34854	Seeing duplicate entries in cslu_poll_udi_mappings table
CSCwi33250	Getting error while doing collect usage for PULL Mode
CSCwi33133	Vulnerabilities reported for 8-202308 through tenable
CSCwj82075	While exporting the UD file. On-Prem application is not downloading any rum reports until and unless the Trust sync request is purged.
CSCwh89867	"Synchronization Failed" - Error downloading data with CSSM connector API
CSCwh89754	Schedule Sync Runs For Inactive Accounts
CSCwh84585	Java agent registration fails when provided with an unresolvable IP addr
CSCwh79009	OnPrem not clearing old records in table prod_inst_ent_summaries causing DB size to grow
CSCwh60668	Remove global variable from CSLU and Typhaon repos
CSCwh46338	Ack not being sent to device for all report ids
CSCwh33422	Smart Licensing and Manage Account Tabs remain active despite absence of
CSCwi46050	Proxy password visible unencoded in OnPrem logs
CSCwa10785	Local Acc deletion in SSM that's holding PIs causing checkmate for user from using the VAs in CSSM
CSCwf37909	When LDAP secondary authentication is disabled, customer should not have a LDAPGroupImportWorker running in background.
CSCwf80985	Improving sorting user group data
CSCwh14482	Proxy pwd in the clear
CSCwh24247	"OK_TRY_AGAIN" channel is full that is causing the failure of transactions in Onprem server
CSCwh38013	Unable to check input pattern because the pattern is not a valid regexp: invalid character in class in regular expression
CSCwh40448	Forgot password option is not working for all the users
CSCwh82990	Multiple 'WARNING' messages in logs for 'piconnector/piconnector.go': Unsupported connect method, skipping

Bug ID	Description
CSCwh84585	Java agent registration fails when provided with an unresolvable IP address
CSCwh89867	“Synchronization Failed - Error downloading data with CSSM connector API" alert is displaying at system level instead of account level
CSCwf66111	**SSM On-Prem HA recovermaster resource failed to start after primary or secondary fail:** When the SSM On-Prem primary server goes down, the application switches over to secondary node. Both of the HA paired servers are disconnected without syncing. After the primary server comes back online, it tries to validate its data and quorum on HA, and attempts to switch to standby as **recovermaster,** but fails with error message.

Known Issues

There are no new known issues in this release.

Resolved Vulnerabilities and Exposures

There are no new resolved vulnerabilities or exposures in this release.

Version 8 Release 202308

Release Date: 10/27/2023

New Features

Accessibility

Made significant accessibility improvements to color contrast, focus order, labels and instruction, information, structure, and relationships conveyed.

Fixes

Version 8 Release 202308 introduces the following critical fixes, along with a few other high and medium bugs:

Bug ID	Description
CSCwb03174	Deletion of SSMS Account fails with error constraint violation on table
CSCwc21507	SSM On-Prem cannot register to account with leading/trailing space in its name
CSCwe18578	Licenses are transferred to VA as per alphabetical order (can be seen under Manage Virtual Accounts)
CSCwe21218	Cannot Transfer SLP Devices with /api/v1/device/transfer
CSCwe28175	Reporting entitlement tags are populated with entitlement_type:STANDARD

Bug ID	Description
CSCwf18773	Unable to turn Oauth2 off
CSCwf31838	SSM On-Prem with NAT enabled CSLU setup still shows UDI as display_name for 17.9.1 running platform
CSCwf38271	Export usage to cisco is broken
CSCwf71439	SSM On-Prem 8-202212 and higher version sending wrong ACK data to Rum Report requests
CSCwh03209	SSM OnPrem: No Id cert found during AUTH RENEW
CSCwh66667	Local Acc deletion in SSM that's holding PIs causing checkmate for user from using the VAs in CSSM
CSCwh84585	Java agent registration fails when provided with an unresolvable IP address
CSCvz39919	Cert issue "\xC3" from ASCII-8BIT to UTF-8
CSCvz95905	OnPrem API does not return correct value for "total records" in a VA
None	The Product Instance Usage API response now includes SLP devices
None	Implemented better protection for GUI and CLI passwords

NOTE: After upgrading your SSM On-Prem server to Release 8-202308, you must synchronize your accounts with CSSM Cloud. For information about synchronizing your SSM On-Prem with the CSSM Cloud, see the *Smart Software Manager On-Prem User Guide*.

Known Issues

1.	**Device HA: ID Renew fails to find sudi/signature failure after switchover**

Resolved Vulnerabilities and Exposures

CRITICAL

- CVE-2022-30123

HIGH

- CVE-2020-14372
- CVE-2020-25632

- CVE-2020-25647
- CVE-2020-27779
- CVE-2021-20233
- CVE-2022-24903
- CVE-2022-28733
- CentOS 7 : kernel (CESA-2023:4151)
  CVE-2022-3564
- CentOS 7 : emacs (CESA-2023:3481)
  CVE-2022-48339
- CentOS 7 : python (CESA-2023:3555)
  CVE-2023-24329
- CentOS 7 : bind (CESA-2023:4152)
  CVE-2023-2828
- CVE-2023-32233

MEDIUM

- CVE-2019-11358
- CVE-2020-27749
- CVE-2021-20225
- CVE-2022-43750

LOW

- CentOS 7 : open-vm-tools (CESA-2023:3944)
  CVE-2023-20867

Version 8 Release 202304

Release Date: 07/11/2023

New Features

Version 8 Release 202304 introduces the following features:

- **Polling**

  Updated Cisco SSM On-Prem polling to reduce the traffic load, which aids in managing the Cisco SSM On-Prem CPU and RAM spike issue. The updates include the following:

  - Cisco SSM On-Prem now sends "COMPLETE" as a status notification in response to fulfilled device requests. This cancels the corresponding Poll Ids, which prevents devices from sending requests that have already been processed.
  - Cisco SSM On-Prem now generates and uses only one Poll Id per device. Prior to Release 8-202304, Cisco SSM On-Prem responded with a unique Poll Id for every usage report sent from a device.
  - Cisco SSM On-Prem retry intervals are now dynamically generated based on the scheduled synchronization to the CSSM Cloud. Prior to Release 8-202304, the retry interval was set to 5 minutes.
  - The poll interval duration is now determined by the scheduled sync and the offset. The offset is a time period determined by how busy the Cisco SSM On-Prem is. The

offset time can range from 5 minutes to 48 hours. Starting in Release 8-202304, the poll interval duration is as follows:

  - If no sync is scheduled for the next 24 hours, the poll interval is the maximum duration, which is 24 hours plus the offset.
  - If a sync is scheduled within the next 24 hours, the poll interval is the sync time plus 2 hours, for the sync to finish, plus the offset.
  - If a sync is currently active, the poll interval is 2 hours plus the offset.

- **Event Log Record Retention Range**

  Changed the number of days that event logs are retained in the **On-Prem Admin Workspace > Settings Widget** > **Event Log Settings** tab. The number of days must be between 7 and 30.

- **Virtual Machine-Based Deployment Requirements**

  Beginning with version 9-202406, SSM On-Prem can be installed on ESXi 8.0 update 3. For more information, see the *Cisco Smart Software Manager On-Prem 9 Installation Guide*.

- **Transport Layer Security 1.2 Legacy Ciphers**

  Added the **Enable TLS 1.2 legacy ciphers** option to the **On-Prem Admin Workspace > Security Widget** > **Account** tab. When enabled, this option allows legacy Cisco products, such as Cisco Unity Connection and Cisco HCM-F, to communicate with Cisco SSM On-Prem. This option is disabled by default post upgrade.

- **Instant authorization request to CSSM**

  Added the **Instant authorization request to CSSM** option to **On-Prem Admin Workspace > Settings Widget** > **CSLU** tab. When enabled, this option permits immediate communication with the Cisco Smart Software Manager Cloud (CSSM Cloud). This communication is required for newly connected devices and is only applicable when online access to the CSSM Cloud is possible. When disabled, this communication is performed only during the scheduled synchronization, which results in a delay from when a device is connected and when the configured features can function.

NOTE:

- CSSM Cloud includes reserved licenses in the total number of licenses used. SSM On-Prem, however, does not. This causes CSSM Cloud and SSM-On Prem to show a different number of licenses in use after sending multiple SLAC requests.
- The Instant authorization will only be applicable for the devices with Smart Agent version greater than 5.3, and IOS versions greater than 17.9.

Fixes

Version 8 Release 202304 introduces the following critical fixes, along with a few other high and medium bugs:

Bug ID	Description
CSCwa57745	Forgot Password option is disabled and it still works
CSCwd94495	SSM On-Prem responds with message "completed" to poll_id requests without ACK data

Bug ID	Description
CSCwe01642	SSM On-Prem crashes when receive "ENDPOINT" report requests from inactive/removed device
CSCwe06889	Cisco SSM /var/log directory is 100% full
CSCwe11850	Product Instance Report not possible to run report for SLP devices
CSCwe12294	OnPrem goes through all the SyncPolls even when the status is Complete resulting in a large number of duplicate SyncResponses
CSCwe12296	ON-PREM sync error with CSSM-cloud. "Synchronization Failed - Error downloading data with CSSM connector API"
CSCwe12297	Can't able to download all event records from Event log tab
CSCwe12399	SLUP: Before real contact PI Last contact always 1901-Jan-01 00:00:00
CSCwe14671	BULK_RUM_REPORT response message is not having signature
CSCwe16847	SLUP OnPrem: 9410 REST API Pull intermittently see Device operation failed
CSCwe17497	Upon 'EXPORT USAGE TO CISCO', it throws an error in exporting data to offline file when there is no device added
CSCwe19469	Product Instance Registration Tokens is not refreshed
CSCwe19522	Not able to transfer Product Instance from Product Instance dialogue popup
CSCwe25173	Need To Implement an Export Option Under Custom Tags
CSCwe26640	SSM OnPrem: Pull-Mode stores device credentials in cleartext
CSCwe26829	Remove Redis#exists(key) from logs
CSCwe36855	SSM OnPrem: (UI) Licensing Workspace - Inventory - generating token - visualization issue in Firefox
CSCwe39737	No Validation on Syslog server address
CSCwe55698	OnPrem sending Usage response to ASAv more than the buffer size
CSCwe63124	SSM OnPrem: Prevent excessive DB growth if smart-agent mis-behaves
CSCwe64090	SSM On-Prem 8-202212 allows renew of CERTID despite of device removed from server
CSCwe66222	Enable legacy TLS 1.2 ciphers on onprem
CSCwe74613	CMM device deletion failure in SSM On-Prem with internal error

Bug ID	Description
CSCwe74794	Vulnerabilities reported by tenable in SSM On-Prem 8-202302
CSCwe84702	Should not process ID Renew request if PI is not valid
CSCwe84703	Several issues in PULL mode configured using RESTAPI, NETCONF, RESTCONF
CSCwe88106	Subject Alternative name is not added to product cert when we add or change the SAN **NOTE:** If you are using ASR with a version earlier than IOS XR: 7.3.3, then to register to SSM On-Prem, you will have to register using FQDN in the hostname. In order to register using an IP address, the device will have to be upgraded to IOS XR 7.3.3 or later. And before performing the registration to SSM On-Prem, the following device configuration change must be added: **crypto ca fqdn-check ip-address allow** Reference: https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-6/system-security/configuration/guide/b-system-security-cg-asr9000-76x/implementing-certification-authority-interoperability.html
CSCwe99217	Evaluation of Smart Manager Smart Licensing for CVE-2021-25220 (BIND)
CSCwe99226	Evaluation of Smart Manager Smart Licensing for CVE-2021-3177 (python)
CSCwe99235	Evaluation of Smart Manager Smart Licensing for CVE-2021-26401 (redhat)
CSCwe99241	Evaluation of Smart Manager Smart Licensing for CVE-2009-4487 (nginx)
CSCwe99252	Evaluation of Smart Manager Smart Licensing for CVE-2022-21125 (redhat)
CSCwe99258	Evaluation of Smart Manager Smart Licensing for CVE-2022-21166 (redhat)
CSCwe99268	Evaluation of Smart Manager Smart Licensing for CVE-2022-21123 (redhat)
CSCwe99286	Evaluation of Smart Manager Smart Licensing for CVE-2022-2795 (DNS)
CSCwe99296	Evaluation of Smart Manager Smart Licensing for CVE-2023-22809 (Sudo)
CSCwe99304	Evaluation of Smart Manager Smart Licensing for CVE-2022-2964 (redhat)
CSCwf01745	No Validation on CSLU URL

Bug ID	Description
CSCwf35227	Add pagination to Activity Tab Event Log
CSCwf44028	Export Control Fails with Invalid PID

Known Issues

1.	**User failed to remove PI from on prem after export return keys complete.**
2.	The REST API does not work with the Instant authorization request to CSSM feature. For more information about this feature, see *New Features*.
3.	**Standby Node Name is not displayed properly on Active node under Product Instance tab**
4.	**License count displayed incorrectly under Product Instance Tab in License Modal for AppHA cluster**
5.	**RAM spikes when exporting logs with a large number of records (150k+)**
6.	**Missing export control alerts after upgrading to 8-202304**
7.	**SSM On-prem direct inline upgrade from 6.x/7.x to latest 8-202302 patch fails**
8.	**SSM On-prem fails to complete account registration if there are 2 or more requestor mail addresses**
9.	**SSM On-prem direct inline upgrade from 6.x/7.x to latest 8-202302 patch fails**
10.	**SSM On-prem fails to complete account registration if there are 2 or more requestor mail addresses**
11.	**The Syslog is not transmitted to the syslog server when HA is formed.**
12.	**Postgres fails while running stats collector throwing continuous errors.**
13.	**Deletion of SSM On-Prem Account fails with error constraint violation.**
14.	**HA failure logs are missing when VM is powered off.**
15.	**Reporting license always get moved to default VA during partial sync**
16.	**SSM On-prem HA recovermaster resouce failed to start after primary or secondary fail under certain conditions.**
17.	**Timestamps missing for Alerts**
18.	**Adding ACI devices in SLP mode fails in On-Prem configured with**

	single/dual stack HA deployment
19.	**SSM 8-202302 send wrong DLC response data to smart agent**
20.	**Unable to turn Oauth2 off**
21.	**SSM On-Prem cannot register to account with leading/trailing space in its name**
22.	**Sidekiq URL is exposed for SSM On-Prem.**
23.	**SSM On-Prem with NAT enabled SLP setup still shows UDI as display_name for 17.9.1 running platform**
24.	**SSM On-prem 8-202212 and higher version sending wrong ACK data to Rum Report requests**
25.	**Alert not getting changed for all the devices when do bulk sync with CSSM**
26.	On-Prem does not honor old Poll ids after 8-202304 upgrade Workaround: Force send a report or wait for the device to send a report. On receiving a new report, SSM On-Prem will generate a new poll id and normal functioning will resume.

Resolved Vulnerabilities and Exposures

- CentOS 7: kernel (CESA-2023:1091)

  CVE-2022-42703

  CVE-2022-4378
- CentOS 7: zlib (CESA-2023:1095)

  CVE-2022-37434
- CentOS 7: samba (CESA-2023:1090)

  CVE-2022-38023
- CentOS 7: openssl (CESA-2023:1335)

  CVE-2023-0286
- CentOS 7: nss (CESA-2023:1332)

  CVE-2023-0767

Version 8 Release 202303

Release Date: 16/05/2023

Release 8-202303 is a special patch release for resolved vulnerabilities. Download the image here:
https://software.cisco.com/download/specialrelease/3fcebb5fe58bdb60ca3850dcfbdee30f

New Features

There are no new features in this release.

Fixes

Version 8 Release 202303 introduces the following critical fixes, along with few other high and medium bugs:

Bug ID	Description
CSCwe14951	Cisco Smart Software Manager SQL Injection Vulnerability

Resolved Vulnerabilities and Exposures

HIGH

- CentOS 7 : sudo (CESA-2023:0291)

  CVE-2023-22809
- CentOS 7 : kernel (CESA-2023:0399)

  CVE-2022-2964

MEDIUM

- CentOS 7 : kernel (CESA-2023:0399)

  CVE-2017-5715

  CVE-2021-26401
- CentOS 7 : bind (CESA-2023:0402)

  CVE-2021-25220

  CVE-2022-2795
- Cisco Smart Software Manager On-Prem SQL Injection Vulnerability

  CVE-2023-20110

Version 8 Release 202302

Release Date: 02/24/2023

NOTE: As part of SSM On-Prem upgrade, stale data is cleaned up from older releases. This process might take several hours, SSM On-Prem upgrade will not complete until this clean up is complete. SSH session will be timed out, you will be logged out of the terminal and On-Prem won’t respond (both GUI port and product port) until upgrade completes.

Fixes

Version 8 Release 202302 introduces the following critical fixes, along with few other high and medium bugs:

Bug ID	Description
CSCwd93767	OnPrem: SLP DLC Ack not coming back to device
CSCwe13534	Duplicate sync response cleaner
CSCwe14672	Upload CSV file function is not working in Firefox browser.
CSCwe19603	Helios-UI: Requested Account Details model - Not able to enter message in the Message to Creator field
CSCwe19800	Licenses tab: Displaying Checkbox when there is no license added
CSCwe21127	Purge duplicate SyncRequest
CSCwe35205	Helios-ui: Upon Export to CSV, the Banner updated logs are misaligned
CSCwe42886	Need a break (split) between Syslog Server Address and UDP port fields of Syslog tab in Settings widget.
CSCwe42889	Could be able to create a token with number of uses as 2147483647.

Resolved Vulnerabilities and Exposures

HIGH

- CentOS 7: krb5 (CESA-2022:8640)

  CVE-2022-42898
- CentOS 7: device-mapper-multipath (CESA-2022:7186)

  CVE-2022-41974
- libexpat before 2.4.9 has a use-after-free in the doContent function in xmlparse.c.

  CVE-2022-40674

Version 8 Release 202212

Release Date: 12/20/2022

NOTE: After performing an upgrade, the browser pages might not reflect the latest changes. Clear your browser's cache so that your browser pages are up to date.

New Features

Version 8 Release 202212 introduces the following features:

- **Smart Account Policy Details API**
  Smart Account Policy Details API will fetch the account policy details of the OnPrem application for both connected and disconnected mode.
- **Product Instance Removal API**

  Enhanced the Product Instance removal API feature to remove SLP devices consuming reporting entitlement.
- **Product Instance Search API**

  Enhanced the Product Instance Search API feature to list SLP devices along with SL devices.
- **Create Token API**

  Updated the Create Token API by including the attributes "Expire After" and "number of Users".
- **IPv4 TTL/IPv6 Hop Limit to 255**

  Increased IPv4 TTL/IPv6 Hop Limit to 255 from 64 (Linux Default value).
- **Subject Alternative Name**

  The **Subject Alternative Name** (SAN) is an extension to the Host Common Name that allows users to specify additional host names for a single SSL certificate. This provides the ability to configure SAN for the product certificate, so products can register either by using IP Address or the FQDN in the Smart Transport URL or the CSLU Transport URL.
- **Transport Layer Security TLS 1.3**

  Upgraded SSM On-Prem to support TLS 1.3

Fixes

Version 8 Release 202212 introduces the following critical fixes, along with few other high and medium bugs:

Bug ID	Description
CSCwd08124	SSM On-Prem 8-202206 does not load alert despite of Alert in open status.
CSCvv04648	ENH: Support for adding SAN in the Product Certificate on On-Prem
CSCvx79548	Error opening licenses tab due to expiring licenses.
CSCwa89408	Scheduled sync for SLP devices doesn't work.
CSCwb86202	Removing SLP device consuming REPORTING entitlement throws error.
CSCwc15916	Cisco Smart Software Manager On-Prem Improper Authentication Vulnerability.

Bug ID	Description
CSCwc55997	Sync failure when transaction id is empty within License Transaction.
CSCwc75637	+if cu is using proxy, port number gets disabled while upgrading On-Prem to 8-202206.
CSCwc75737	Port is missing in the CSLU Configs table, but still able to receive the ACKS having proxy enabled.
CSCwc75739	Cannot transfer device consuming REPORTING entitlement.
CSCwc78195	SSM On-Prem takes more than 1 min to load first 10 devices in Product Instance tab.
CSCwc81826	GUI time zone setting is not reflecting on the event logs.
CSCwc84431	SSM On-Prem account license page stops loading when Pool Entitlement Summary has charge type nil value.
CSCwc91400	OnPrem: "backoff" scalability optimization for SL enabled devices.
CSCwc93877	8-202206 - Event log under Activity tab in On-Prem workspace doesn't display timestamp.
CSCwd04505	Delay when parsing through Product Instance list from Product Instance tab.
CSCwd08301	SSMS Password reset via email feature revert CN value of Product Certificate back to old value.
CSCwd20510	Details to be provided: Account enumeration issue reported by VISA.
CSCwd23268	SLP sync issue due to an error in processing the SLP DLC data on On-Prem which causes the sync to fail.
CSCwd34116	Cisco SSM licensing server vulnerabilities in version 8-202206.
CSCwd52197	Evaluate Smart Software Manager On-Prem for CVE-2022-31676.
None	The OK_TRY_AGAIN The large deployment of products run into an issue where a lot of requests are being dropped/rejected by SSM OnPrem. The load on the SSM OnPrem server leads to the unresponsiveness on SSM OnPrem resulting in returning 503 or communication failure error to the products. A new message response has been added to be sent to devices when the On-Prem is loaded with many requests and determined to be too busy in processing the device message. This response will notify the device to re-try its request at a certain time interval. As the request load increases, the interval will become longer to smooth out the request load on SSM On-Prem server.
None	CPU and RAM spike In our previous releases, we have RAM and CPU spikes observed for couple of scenarios which were caused by certain processes. In this release 8-

Bug ID	Description
	202212, we have addressed them; Couple of things that the user can perform to handle this situation is to upgrade the OnPrem application to version 8-202212 which would aid in resolving the RAM and CPU spikes. Another way to mitigate the RAM and CPU spikes is by having sufficient number of licenses in your OnPrem application so that the traditional SL devices are all in Incompliance. Please note, for certain processes, like SL and SLP Synchronization with Cisco, it is normal for the RAM to spike for the runtime of the process, but it should go back to normal once the process is done. If you see sustained high RAM or CPU, please contact TAC.

Known Issues

1.	**SSM On-Prem ISO allows to deploy server without meeting minimum system requirement.** SSMS installation completes without meeting minimum system requirement and filesystem partition is not a standard SSMS and that of CENTOS based. This would cause abnormality on SWAP memory allocation and other process ongoing.
2.	**Product Instance Report not possible to run report for SLP devices.**
3.	**PI edit info is not saved in NAT enabled mode.** Please make sure to add all the required SUDI (*Secure Unique Device Identifier*) information while creating a product. Otherwise, you would have to remove and reregister the device.
4.	Make sure the devices are configured with single IP otherwise there will be unpredictable results.
5.	**Reservation license is not consumed on OnPrem UI; but device has the AUTH code installed.**
6.	**SSM On-Prem CSLU module must not allow duplicate device addition with different host address.**
7.	**SSM On-Prem CSLU module must not allow multiple devices with same host address.**
8.	**SSM On-Prem SLUP PULL Method using Rest API call does not process license for ASR1K**
9.	**DLC issue - device is not getting acknowledgement from On-Prem**
10.	**OnPrem: Synchronization Failed - Error downloading data with CUSTOM connector API.**
11.	**/var/log/ 100% disk usage causing inline upgrade failure for SSM On-Prem**

12.	**Username and Password does not get saved on Email tab under Settings**
13.	**SSMS 8-202206 does not show device details in-use due to missing entry in sku Entitlement Map**
14.	**Not able to transfer Product Instance from Product Instance dialogue popup**
15.	**SSM On-Prem NAT enabled setup does consolidate all device reports into single file on manual export**
16.	**Can't able to download all event records from Event log tab.**
17.	**SSM On-Prem does not sync with CSSM with CCO id enabled with federated service**
18.	**OnPrem Licenses usage increments on synchronization and causes cosmetic issue.**
19.	**SSMSV6 deployed single stack server failed to send syslog message to dual-stack syslog server**

Resolved Vulnerabilities and Exposures

CRITICAL

- Python 3.x through 3.9.1 has a buffer overflow in PyCArg_repr in _ctypes/callproc.c.

  CVE-2021-3177

- This issue occurs due to the on_stream_io() function and dns_stream_complete() function in 'resolved-dns-stream.c' not incrementing the reference counting for the DnsStream object.

  CVE-2022-2526

- CentOS 7 : expat (CESA-2022:6834)
- OpenSSH < 9.1 Multiple Vulnerabilities

HIGH

- CentOS 7 : kernel (CESA-2022:0620)

  CVE-2021-4155, CVE-2021-0920, CVE-2022-22942, CVE-2020-0466, CVE-2021-3573, CVE-2021-3752, CVE-2022-0330, CVE-2021-3564, CVE-2020-0465

- A vulnerability was found in the Linux kernel’s cgroup_release_agent_write in the kernel/cgroup/cgroup-v1.c function.

  CVE-2022-0492

- An arbitrary file write vulnerability was found in GNU gzip's zgrep utility.

  CVE-2022-1271

- net/netfilter/nf_tables_api.c in the Linux kernel through 5.18.1 allows a local user (able to create user/net namespaces) to escalate privileges to root because an incorrect NFT_STATEFUL_EXPR check leads to a use-after-free.

  CVE-2022-32250

- A race condition was found the Linux kernel in perf_event_open() which can be exploited by an unprivileged user to gain root privileges.

  CVE-2022-1729

- http.client in Python 3.x before 3.5.10, 3.6.x before 3.6.12, 3.7.x before 3.7.9, and 3.8.x before 3.8.5 allows CRLF injection.

  CVE-2020-26116

- VMware Tools (12.0.0, 11.x.y and 10.x.y) contains a local privilege escalation vulnerability.

  CVE-2022-31676

- CentOS Security Update for python (CESA-2022:5235)
- CentOS 7 : systemd (CESA-2022:6160)
- CentOS 7 : xz (CESA-2022:5052)
- CentOS 7 : bind (CESA-2022:6765)
- According to its Server response header, the installed version of nginx is 1.0.x prior to 1.22.1 or 1.1.x prior to 1.23.2.

  CVE-2022-41741, CVE-2022-41742

MEDIUM

- CentOS 7 : openldap (CESA-2022:0621)

  CVE-2020-25710, CVE-2020-25709

- urllib3 before 1.25.9 allows CRLF injection.

  CVE-2020-26137

- CentOS 7 : cyrus-sasl (CESA-2022:0666)

  CVE-2022-24407

- CentOS 7 : kernel (CESA-2022:5232)
- CentOS 7 : gzip (CESA-2022:2191)

Version 8 Release 202206

Release Date: 07/20/2022

New Features

Version 8 Release 202206 introduces the following features:

- **TACACS PHASE 2**

  This feature allows the local Virtual account users to authenticate/authorize SSM On-Prem login, after TACACS+ is configured to the TACACS server. Removed dropdown “**Initial role of new user**” from TACACS+ configuration tab. **System role** dropdown and **actions** menu is set to greyed out for TACACS users on the user screen of user widget, so that system role change is only possible on the server end.

- **MSLA support in SLP**

  Incorporate MSLA usage billing functionality for SLP devices.
- **SLP Hostname enhancements**

  For SLP device having Smart Agent version less than 5.5 then UID details will be displayed in the name field, if UID details are not available then IP address will be displayed. For SLP devices having Smart Agent version greater than or equal to 5.5 only Host name will be displayed.

  NOTE: For SLP devices having Smart Agent version greater than or equal to 5.5 the host name cannot be created by using any special characters and spaces.
- **SDWAN features vManage integration with On-Prem**

  This feature focuses on the requirements to integration of vManage with SSM On-Prem license, by providing necessary Application Programming Interface (API) for vManage for usage reporting purposes. vManage license summary API and vManage account details API are developed to properly handle such calls.
- **Future dated licenses**

  The Future Dated license feature is integrated into On-Prem and enables customers to have the license which has the start date in future. The Future Dated license will be processed when the start date < current date, so that Future-dated licenses will not be consumed until the start date become current. The purchase count will only be reflected based on license transactions that have a present start date.

NOTE: SSM On-Prem does not support the CCO id enabled with federated service (Redirect to id.cisco.com) yet.

Fixes

Version 8 Release 202206 introduces the following critical fixes, other than these fixes, some other high and medium bugs have also been fixed:

Bug ID	Description
CSCvu89468	IPTables default policies are still in place.
CSCvy62936	SSM On-Prem: 8-202102: GUI Needs to have TACACS attributes to fully auto.
CSCvy94330	Device's renewal is failed when configuring language to Japanese on SSM.
CSCwa06345	License count mismatch issue in GUI SSMS and the report in the SSM.
CSCwa31053	Error when scheduling sync for customers in UTC+14 timezone.
CSCwa42681	Authorization renewal fails when configuring language to Japanese on SSM
CSCwa56683	Send RUM reports, Licenses are not being consumed on OnPrem.

Bug ID	Description
CSCwa56684	After upgrade the proxy settings in SLP DB are not persisted.
CSCwa56689	Editing CSLU product in PULL mode may result in breaking Collect Usage.
CSCwa75363	SSM On-Prem license reports for UC products - Export to Excel and CSV - Incorrect balances.
CSCwa75786	In Use Quantity not shown for selected license in On-Prem graph.
CSCwa92002	SSM OnPrem: The search function under Product Instances Inventory panel.
CSCwa94904	Enabling NAT feature in OnPrem disables the proxy setting and vice-versa. **NOTE:** NAT/proxy must be turned On, which was toggled off previously due to this bug.
CSCwa95039	CSSM processing failure of accumulated un-acknowledged rum reports.
CSCwa96336	SSM OnPrem: Incorrect Product Instance deletion in OnPrem inventory UI.
CSCwb05285	Product Instances removed from OnPrem after a year of registration.
CSCwb06331	SSM On-Prem: Smart license Alerts can't be dismissed.
CSCwb16510	CSLU device consuming reporting licenses causes duplicated license entries.
CSCwb16858	Unable to open PI by clicking on "In Use" licenses.
CSCwb23940	Display a spinner on all the screens where data is loaded.
CSCwb30211	SLP network sync fails when proxy with DNS name is configured.
CSCwb32134	Account users not showing in manage account section of onprem.
CSCwb55507	Username and Password does not get saved on Email tab under Settings.
CSCwb80668	Sidekiq jobs get stuck in development.
CSCwb98281	Cisco Smart Software Manager On-Prem version 8-202112 Privilege Escalation Vulnerability.
CSCwc09667	MLSA devices receive OOC when prepaid license of same type has OOC alert.
CSCwc12764	**When On-Prem is bombarded with multiple auth renew requests DB fills up.**
CSCwc21609	OnPrem: automate proxy setting flap after an upgrade.
None	**Postgres version has been upgraded to 13.5.**

Known Issues

1.	**CSSM <==> OnPrem (8-202201) license count inconsistencies.** SSM On-Prem showing incorrect license usage counts. Upon clicking on the in-use number of licenses, even though the number shows > 0, nevertheless nothing is being populated.
2.	Few of the SSM On-Prem APIs will not support for SLP enabled devices.
3.	**SSM On-Prem ISO allows to deploy server without meeting minimum system requirement.** SSMS installation completes without meeting minimum system requirement and filesystem partition is not a standard SSMS and that of CENTOS based. This would cause abnormality on SWAP memory allocation and other process ongoing.
4.	**Removing SLP device consuming REPORTING entitlement throws error.**
5.	**TGCert's expiry date not getting updated on sync with CSSM.**
6.	**Product Instance Report not possible to run report for SLP devices.**
7.	**LDAP Scheduled sync job does not run due to SSL certificate verify failure.** The LDAP scheduled sync which runs every 24 hours, certificates uploaded are not being updated. Due to this, the scheduled sync fails with error. New groups that are added since last sync are not updated in OnPrem resulting in no access to users in that group.
8.	**+Self signed browser certificate is not renewed by itself.**
9.	**OnPrem: Synchronization Failed - Error downloading data with CUSTOM connector API.**
10.	**PI edit info is not saved in NAT enabled mode.** Please make sure to add all the required SUDI (*Secure Unique Device Identifier*) information while creating a product. Otherwise, you would have to remove and reregister the device.
11.	Make sure the devices are configured with single IP otherwise there will be unpredictable results.
12.	**Product Instance Report not possible to run report for SLP devices**
13.	**Reservation license is not consumed on OnPrem UI; but device has the authcode installed.**
14.	**Incorrect Count when license borrowed to lower tiers.**
15.	**SSM On-Prem CSLU module must not allow duplicate device addition with different host address.**

16.	**SSM On-Prem CSLU module must not allow multiple devices with same host address.**
17.	**Cisco Smart Software Manager On-Prem version 8-202112 Privilege Escalation Vulnerability**.

Resolved Vulnerabilities and Exposures

HIGH

- CentOS 7 : samba (CESA-2021:5192)

  CVE-2016-2124, CVE-2020-25717
- CentOS 7 : polkit (CESA-2022:0274)

  CVE-2021-4034
- The request phase of the OmniAuth Ruby gem (1.9.1 and earlier)

  CVE-2015-9284
- An issue was discovered in the Linux kernel before 5.10.

  CVE-2020-36385
- An issue was discovered in Linux: KVM through Improper handling of VM_IO|VM_PFNMAP vmas in KVM can bypass RO checks and can lead to pages being freed while still accessible by the VMM and guest.

  CVE-2021-22543
- A heap out-of-bounds write affecting Linux since v2.6.19-rc1 was discovered in net/netfilter/x_tables.c.

  CVE-2021-22555
- BPF JIT compilers in the Linux kernel through 5.11.12 have incorrect computation of branch displacements, allowing them to execute arbitrary code within the kernel context.

  CVE-2021-29154
- net/bluetooth/hci_request.c in the Linux kernel through 5.12.2 has a race condition for removal of the HCI controller.

  CVE-2021-32399
- Redis is an open source, in-memory database that persists on disk.

  CVE-2021-32675, CVE-2021-32762
- arch/powerpc/kvm/book3s_rtas.c in the Linux kernel through 5.13.5 on the powerpc platform allows KVM guest OS users to cause host OS memory corruption via rtas_args.nargs, aka CID-f62f3c20647e.

  CVE-2021-37576

MEDIUM

- OpenSSH 8.2 < 8.5

  CVE-2021-28041
- CentOS 7 : openssl (CESA-2021:3798)

  CVE-2021-23840, CVE-2021-23841

- CentOS 7 : rpm (CESA-2021:4785)

  CVE-2021-20271
- CentOS 7 : krb5 (CESA-2021:4788)

  CVE-2021-37750
- CentOS 7 : kernel (CESA-2022:0063)

  CVE-2020-25704, CVE-2020-36322, CVE-2021-42739
- Sidekiq through 5.1.3 and 6.x through 6.2.0 allows XSS via the queue name of the live-poll feature when Internet Explorer is used.
  CVE-2021-30151
- A flaw was found in the way RTAS handled memory accesses in userspace to kernel communication.

  CVE-2020-27777
- An issue was discovered in the Linux kernel before 5.11.11.

  CVE-2021-29650
- A flaw was found in the KVM's AMD code for supporting SVM nested virtualization.

  CVE-2021-3653, CVE-2021-3656

Version 8 Release 202201

Release Date: 02/04/2022

Fixes

Version 8 Release 202201 introduces the following fixes:

Synchronization fails after upgrade to 202112
Network synchronization fails when upgrading to 202112. Scenario that causes it:

1. *Have CSLU device which consumes LH license in version prior to 202112 i.e., 202108*
2. *Perform upgrade to 202112*
3. *Do full synchronization*
4. *Sync with fail showing “translation missing error”*

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa58669

Other minor fixes

Version 8 Release 202201 introduces the following minor fixes as well:

Bug ID	Description
CSCwa55809	On-Prem to CSSM synchronization failure for SLU devices - ERROR_POLL_ID(NAT)
CSCwa60443	Inline upgrade from 8-202108 to 8-202112 fails with database migration
CSCwa62164	On-Prem to CSSM synchronization failure for SLU devices - ERROR_POLL_ID

Bug ID	Description
CSCwa68845	CSLU 'EXPORT USAGE TO CISCO' FAILS IN 8-202108
CSCwa75049	Unable to save LDAP configs when multiple LDAP groups are present
CSCwa77416	Unexpected Substitution Counts In Upgraded Versions < 8-202010 **NOTE:** Please perform full sync if there is a license count mismatch for LH items.
CSCwa82690	SLP device state stuck in ACK received from CSSM

Known Issues

There has been no change in terms of the known issues, these remain the same as in version 8-202112.

Scheduled Sync for SLP:
Please make sure to perform network sync from the admin portal before scheduling the synchronization for the SLP devices on the licensing portal under “Reports”.

How to perform network sync from admin portal-

1. Go to admin workspace.
2. Open “Synchronization” widget
3. Click on “Actions” on the right side of your On-Prem Account.
4. Select Full or Standard Network Synchronization.
5. Make sure that Synchronization is successful.

Resolved Vulnerabilities and Exposures

Nothing to report in this release.

Version 8 Release 202112

Release Date: 12/22/2021

New Features

Version 8 Release 202112 introduces the following features:

- **IR1610**
  Support for the Shared Flag has been added to the SSM On-Prem. This support was already there on the CSSM cloud but not on the SSM On-Prem, hence resulting in license mismatch between SSM On-Prem and CSSM Cloud.
  If the Shared Flag is enabled, it will allow borrowing from any parent within the same hierarchy tree, else it will form the request as we do for linear hierarchy.
- **LDAP (Lightweight Directory Access Protocol) Group of Names**
  Current OnPrem implementation supports only hardcoded groups object class:
  posixGroup for OpenLDAP
  group for ActiveDirectory

Support for "**GroupOfNames**" has been added in this release.

User has possibility to use custom Groups Object Class and Group Unique Id Attribute for OpenLDAP by two fields provided in LDAP Settings.

Groups Object Class (string) - objectClass of a group that OnPrem uses in its query when importing groups. For example: groupOfNames, posixGroup.

Group Unique Id Attribute (string) - the unique attribute to track the group identity. Only groups possessing this attribute can be imported into your OnPrem. For example: gidnumber, entryUUID.

- **LDAP (Lightweight Directory Access Protocol) Enhancements**
  In this release, multiple enhancements have been added to the LDAP functionality.
  1. LDAP Users Tab: In one of our previous releases there was an ask to remove LDAP Users Tab from Access management widget. From this point, any operations could be performed only on the LDAP groups and not on a single user. However, it has not been justified by the customers' needs and we needed to bring back the functionality. So, in this release, the customers would be able to see LDAP Users Tab under Access Management widget on the Admin Portal. **The tab shows the highest system role assigned to the LDAP user.**
  2. System role assignment for LDAP Users: We would be able to see LDAP User in Users widget assign them a System Role. The widget shows individually assigned system role.
  3. Accounts role assignment for LDAP Users: We would be able to add LDAP user as "New User" in "Manage Account" view Users' tab and assign them a Role.
- **License Hierarchy support for products using Application High-Availability (AppHA)**
  High availability support for the License Hierarchy has been added in this release, it will make sure that there is no double counting when LH (License Hierarchy) is being used in a HA setup**.**

  NOTE: The On-Prem and CSSM may show different license counts in use when using the CUBE feature on Smart License Policy enabled products. This problem does not occur with products operating in traditional Smart Licensing mode. There is no business or operational impact, and the CUBE feature is working correctly. The Smart Licensing team is working with Product teams on a fix. There is no fix required in On-Prem.
- **SLP Bulk Auth Code**
  Problem: For a Product Instance running Smart Licensing Using Policy mode tries to make a request for an authorization code for export control or enforced features to the On-Prem SSM, the Smart Licensing Authorization Code (SLAC) should be download from CSSM ahead of time. This is operationally challenging and not scalable.

  Solution: In this release, feature enhancement has been added which will save the authorization requests from SLUP product instances. Once the On-Prem SSM synchronizes with cloud CSSM, the request is sent in connected or offline mode and authorization code is generated on CSSM. This authorization code is sent back to On-Prem SSM as part of the acknowledgement.
- **Product Image Security Scanning**
  To ensure the security and integrity of the SSM On-Prem license server, the product is routinely scanned for out-of-date packages as well as any know critical or high CVEs (Common Vulnerabilities and Exposures). Based on evaluating reports from various tools, several key packages have been updated. These include:

PostgreSQL
Angular
RubyOnRails
Redis

- **Accessibility (VPAT)**
  We have added a few fixes and enhancements to the existing accessibility features, please be informed VPAT (Voluntary Product Accessibility Template) is an ongoing process, and in each release, we would keep enhancing it. If you see any issue or have an idea to improve the accessibility of the SSM On-Prem, please open a bug, it will be included in the next release.

NOTE: VPAT might not work properly on Mozilla Firefox and Internet Explorer, to use VPAT without any
issues, please use Google Chrome Browser.

Fixes

Version 8 Release 202112 introduces the following critical fixes, other than these fixes, some other high and medium bugs have also been fixed:

Bug ID	Description
CSCvz12806	Unable to save LDAP Configurations.
CSCvx36137	Inability to synchronize accounts requested by System
CSCvy83324	HTTP 502 Bad Gateway when sending RUM to On-Prem
CSCvz02197	Licenses Used are always (none) in the Product Instance Report
CSCvz03547	Unable to navigate to the next page using keyboard on the Licenses tab
CSCvz14218	Labels in Smart Licensing keep changing after page refresh
CSCvz43367	On-Prem UI display partial UDI and missing UUID
CSCvz44481	Alerts status refreshes only after switching tabs
CSCvz45260	License Hierarchy Calculations mismatch between OnPrem and CSSM
CSCvz65233	SLP Device not getting deleted in CSSM
CSCvz69608	Manual and network synchronization fails after upgrade
CSCvz69609	Duplicated FTD base licenses in On-Prem licensing portal causing OOC.
CSCvz74179	Schedule Sync will not work if time zone UTC offset is not an integer
CSCwa03397	On-Prem should not be non-responsive when devices bombard with auth renew requests.
CSCwa14135	Clicking on SLUP Product Instance's IP Gives details of another device.
CSCwa15038	Partial Sync clearing Entitlement Hierarchy records.

Bug ID	Description
CSCwa36717	Cannot downgrade System role to System User when User has assigned accounts
CSCwa48579	On-Prem sending CSLU URL to SL (Smart Licensing) products and resulting in crashing of products
CSCwa52518	CSLU empty data generated during usage report generation

Known Issues

1	**Error when scheduling sync for customers in UTC+14 time zone**
2	**After upgrade the proxy settings in SLP DB are not persisted** In the case of an upgrade scenario, if the proxy is already enabled before the upgrade, after an upgrade you must disable it and enable it again to use proxy with MSLA & SLP.
3	**PI edit info is not saved in NAT-enabled mode** Please make sure to add all the required SUDI (*Secure Unique Device Identifier*) information while creating a product. Otherwise, you would have to remove and reregister the device.
4	**Send RUM reports, Licenses are not being consumed on OnPrem** When adding a new PUSH Device on SSM On-Prem UI, please make sure to add all the required SUDI information (PID and SN), else there will be no license consumption. It only applies to the product added through UI (**Add Single Product**). To add the SUDI details, click on the PI under "SL Using Policy" on Licensing Workspace, add PID & Serial Number, and save the changes.
5	**Editing CSLU product which is in PULL mode may result in breaking Collect Usage** While editing an SLP PI on UI, if password was already there for that PI, please make sure to reenter the password, else it may result in "Collect Usage" failures.
6	**USB Enable dropdown is not visible in installer** After adding four (or more) hard drives in the installation process, the **Enable USB** dropdown is moved outside screen bounds and is therefore difficult to access. As a temporary workaround, navigate to the Available Disks section and hit the Tab button the number of times equal to the number of hard drives +1 (5 Tab hits for a 4-drive setup, 6 Tab hits for a 5-drive setup, etc.) This will activate the **Enable USB** dropdown – the options will become visible on the screen and available for selection.

7	**Non-ASCII characters in the cert attributes** SSM On-Prem throws an error after fetching certificates that use non-ASCII characters in the cert attributes. Until a fix is developed for this issue, please use only ASCII characters in the cert attributes while creating a certificate.

Resolved Vulnerabilities and Exposures

Version 8 Release 202112 resolves the following security vulnerabilities:

CVE-2021-23840, CVE-2021-23841, CVE-2019-20388, CVE-2020-7595, CVE-2016-4658, CVE-2016-4658, CVE-2021-3653, CVE-2021-22543, CVE-2021-3656, CVE-2021-37576, CVE-2021-29154, CVE-2021-29650, CVE-2020-27777, CVE-2021-32399, CVE-2021-22555, CVE-2020-11668, CVE-2019-20934, CVE-2021-33909, CVE-2021-33033, CVE-2021-33034, CVE-2021-3347, CVE-2020-12364, CVE-2020-27170, CVE-2020-12363, CVE-2020-12362, CVE-2020-8648, CVE-2021-25217, CVE-2021-27219, CVE-2020-12321, CVE-2021-42574, CVE-2021-3715, CVE-2021-25214, CVE-2021-20254

Version 8 Release 202108

Release Date: 08/13/2021

New Features

Version 8 Release 202108 introduces the following features:

- **Support for proxy between On-Prem and cloud CSSM (with MSLA (Managed Service License Agreement) and SLP)**
  Enhancements have been made to both CSLU back-end go code and OnPrem MSLA go code to get proxy settings from the configuration and send messages accordingly. This allows for using the existing On-Prem UI proxy settings for MSLA and SLP.

NOTE: In the case of an upgrade scenario, if the proxy is already enabled before the upgrade, after an upgrade you must disable it and enable it again to use proxy with MSLA & SLP.

- **Deletion of SLP devices**
  This feature has been developed to make sure users can manually remove a product instance. The *Cisco Delete Product Instance* API has been enhanced to properly handle such calls.
- **Look Back**
  For products with the Look Back capability - when a product instance reports usage of license, CSSM On-Prem now compares the *past* usage value to the current purchased value for that license. If the Look Back balance is negative, the product instance may still be authorized, based on the Look Back balance logic.

  This Look Back functionality enhancement is available through additions to the “look_back_days” attribute.

- **Bulk network sync for multiple accounts**
  For improved customer experience, this feature introduces the option to select multiple/all accounts and then trigger the network sync option for all of them. This bulk synchronization option is now available in the Admin Workspace for System Admin and System Operator roles.

  Note: scheduled synchronization will take place irrespectively of the bulk sync completion.

- **Trigger sync from Licensing Portal**
  This feature has been developed with the aim of reducing dependency between users and/or business units with access to On-Prem Admin Workspace and those using On-Prem Licensing Portal. To that end, the following roles are now allowed to trigger a Standard Sync from the Licensing Portal:
  - System Admin
  - System Operator
  - Local Account Administrator
  - Local Virtual Account Administrator

- **Node Lock ID in the sync file**
  Cisco Email Security Appliance (ESA) and Cisco Web Security Appliance (WSA) products use Rest Smart agent and Node Lock ID is a part of conversion data passed from devices to CSSM/On-Prem. Node Lock ID is needed by SWIFT to identify these devices in backend for conversion of classic licenses to Smart ones.

  This enhancement has been developed to ensure the **node_lock_id** sent by the product to the SSM On-Prem is passed along to SSM Cloud in the sync file.

Fixes

Version 8 Release 202108 introduces the following fixes:

Bug ID	Description
CSCvz12806	Schedule sync failing with invalid refresh token error
CSCvy49869	Post-upgrade failure of account sync
CSCvz02208	Run report under Product Instance Report makes the page content disappear
CSCvz05241	Vulnerabilities: broken access control, business logic bypass
CSCvy56595	Fixed vulnerabilities in Centos Kernel and nss
CSCvy13189	Docker vulnerability (-userns-remap option)
CSCvy92788	Cannot change default access until after first user logged in
CSCvy92804	Provide option to delete TACACS users
CSCvy83782	Cannot add TACACS user to Local Account
CSCvy83776	Cannot find TACACS user

Bug ID	Description
CSCvy80050	TACACS user role assignment via User Widget
CSCvy92784	Time-out to be larger than 10sec (set 0-999 seconds) for TACACS
CSCvy50544	SSM On-Prem is not generating a valid CSLU Transport URL
CSCvx86234	Authorization renewal fails with "No id cert found" error
CSCvu51608	HTTP error while loading license transaction history
CSCvz06716	Cancel button on Edit User issue
CSCvz03547	Next Page navigation with keyboard issue
CSCvy73595	Next Page button in Virtual Accounts not working
CSCvy95322	Select time in negative values
CSCvy82973	Displaying different On-Prem account after page refresh
CSCvy22891	Alerts on Product Instance point to null page
CSCvx65334	Add Button in the Group Details tab issue
CSCvm52997	Pagination reset after Virtual Account deletion

Known Issues

1	**HA support for license hierarchy issue** For devices working in High Availability Cluster, there might be an issue where devices in both "active" and "standby" modes appears in *pool_ent_used_summaries* table. As a result, *entitlements_to_process(pool_id)* method of *EntitlementHierarchyService* takes into account both consumptions. **CUBE licenses being double counted in HA** In High Availability cluster, there might be an issue of CUBE licenses being double counted, with a number of licenses being "in use" and "standby" at the same time.
2	**Inability to synchronize accounts requested by System Users** In some cases, accounts requested by System Users (and approved by System Operators or System administrators) fail to synchronize with CSSM. This is due to the fact that YAML request files (originated by the On-Prem server for the faulty accounts) do not have any ID under *virtual_accounts*.

3	**Rails upgrade vulnerabilities** **Postgres update issues** Those two known issues will be fixed with the next release.
4	**PI edit info is not saved in NAT-enabled mode** Please make sure to add the all the required SUDI (*Secure Unique Device Identifier*) information while creating a product. Otherwise, you would have to remove and reregister the device.
5	**License sharing in hierarchy** This capability is required by the Data Center products, but not for Collab products. It was implemented in Production CSSM but is yet to be delivered for On-Prem (expected to be implemented in the October release ETA). Until then, hierarchy should still work on OnPrem with a smaller number of borrowed licenses, and not matching the count on CSSM and OnPrem.
6	**USB Enable dropdown is not visible in installer** After adding four (or more) hard drives in the installation process, the **Enable USB** dropdown is moved outside screen bounds and is therefore difficult to access. As a temporary workaround, navigate to the Available Disks section and hit the Tab button the number of times equal to the number of hard drives +1 (5 Tab hits for a 4-drive setup, 6 Tab hits for a 5-drive setup, etc.) This will activate the **Enable USB** dropdown – the options will become visible on the screen and available for selection.
7	**Non-ASCII characters in the cert attributes** SSM On-Prem throws an error after fetching certificates that use non-ASCII characters in the cert attributes. Until a fix is developed for this issue, please use only ASCII characters in the cert attributes while creating a certificate.

Resolved Vulnerabilities and Exposures

Version 8 Release 202108 resolves the following security vulnerabilities:

CRITICAL

CentOS 7 : nss and nspr (CESA-2020:4076)

CVE-2019-17006, CVE-2020-6829, CVE-2019-11719, CVE-2019-11727, CVE-2020-12402, CVE-2020-12401, CVE-2020-12400, CVE-2019-17023, CVE-2020-12403, CVE-2019-11756

HIGH

kernel: use-after-free in show_numa_stats function (CVE-2019-20934)

kernel: mishandles invalid descriptors in drivers/media/usb/gspca/xirlink_cit.c (CVE-2020-11668) kernel: use-after-free in cipso_v4_genopt in net/ipv4/cipso_ipv4.c (CVE-2021-33033)

kernel: use-after-free in net/bluetooth/hci_event.c when destroying an hci_chan (CVE-2021-33034)

kernel: size_t-to-int conversion vulnerability in the filesystem layer (CVE-2021-33909)

nginx 0.6.x < 1.20.1 1-Byte Memory Overwrite RCE (CVE-2021-23017)

Version 8 Release 202105

Release Date: 06/10/2021

New Features

Version 8 Release 202105 introduces the following features:

- **Bulk AuthCode Import support for devices behind NAT**
  The Cisco Smart License Utility (CSLU) functionality now supports the bulk importing of authcodes for devices behind a NAT operating in push mode. This method was not supported in 8-202102 and has been added new in this release.

  Note: At this time, CLSU is not supported through a Proxy.

Fixes

Version 8 Release 202105 introduces the following fixes:

Bug ID	Description
CSCvy48103	UC Applications and Prime infrastructure registrations fails after upgrading to SSM On-Prem version 8-202102

Known Issues

The following table lists all known open issues and bugs for Version 8 Release 202105:

1	SLP and MSLA are not supported through a proxy. Additional code changes are required to resolve this issue.
2	On-Prem SLP feature currently does not support OnPrem Account names with spaces (and other special characters). On-Prem account name doesn't affect the SA/VA names which may contain spaces and don't require any changes. There is no workaround for it. Support to be added in the next release version.

Resolved Vulnerabilities and Exposures

Nothing to report in this release.

Version 8 Release 202102

This release covers the following new features, fixes and vulnerabilities.

New Features

Version 8 Build 202102 has the following features:

- **Support for Cisco Smart Licensing using Policy.**

  The Cisco Smart License Utility (CSLU) functionality has been integrated into SSM On-Prem providing support for newer devices which run Smart Licensing using Policy, providing a single platform to manage all Smart Licensing and SLP enabled devices. ***At this time, CLSU is not supported through a Proxy.***
- **Fixes and enhancements for LDAP functionality.**
  - LDAP Search fixes - When adding LDAP Users and Groups a filter can be applied to the search to overcome the 1000 record limitation affecting previous releases.
  - LDAP integration now works on Group basis versus user basis. LDAP groups are assigned to resources on OnPrem, and users are added to the groups using organization’s pre-existing access controls processes.
  - LDAP Support for Role-Based Access Control - User privileges can now be managed with user groups using RBAC policies.
- **License Hierarchy fixes**

  Resolved license hierarchy algorithm issues. Correct ratios are now shown when a Product Instance with a higher-level license (parent license) needs to share with lower-level license (child licenses). These changes will accommodate the count/ratio changes with the CSSM architecture.
- **TACACS+ Authentication integration with SSM On-Prem**

  Added functionality to allow TACACS+ to be utilized for authentication to OnPrem. This feature enables integration with a TACACS+ server so that users can be authenticated for access to both the On-Prem UI and CLI console.*

⚠

***ATTENTION**: TACACS+ uses MD5 hashing algorithm which is not FIPS compliant. If FIPS compliance is a requirement of your organization, please use an alternative secondary authentication method.

Fixes

Bug ID	Description
CSCvu32429	Product registrations fail if syslog server configuration is incorrect
CSCvv64369	SAN field doesn’t support multiple entries
CSCvv87538	Can't import wildcard certificate (browser cert)
CSCvw29893	Scheduled Sync fails with “Access Token not found” error
CSCvw79417	Scheduled sync executes on different day than desired

Bug ID	Description
CSCvx04389	Transfer Quantity Exceeds Available Quantity" error when transferring a license
CSCvy24164	Cannot transfer a license with a Subscription ID
CSCvy24164	OnPrem UI not available after upgrade

Resolved Vulnerabilities and Exposures

Version 8 Release 202102 resolves the following CentOS security vulnerabilities

CRITICAL

CentOS 7: nss and nspr (CESA-2020:4076)
CVE-2019-17006, CVE-2020-6829, CVE-2019-11719, CVE-2019-11727, CVE-2020-12402, CVE-2020-12401, CVE-2020-12400, CVE-2019-17023, CVE-2020-12403, CVE-2019-11756

HIGH

CentOS 7: kernel (CESA-2020:5023)
CVE-2019-20811, CVE-2020-14331

CentOS 7: kernel (CESA-2020:5437)
CVE-2020-14314, CVE-2020-25212, CVE-2020-25643, CVE-2020-14385, CVE-2019-18282, CVE-2020-24394, CVE-2020-10769

CentOS 7: samba (CESA-2020:5439)
CVE-2020-14323, CVE-2020-1472, CVE-2020-14318

CentOS 7: pacemaker (CESA-2020:5453)
CVE-2020-25654

CentOS 7: sudo (CESA-2021:0221)
CVE-2021-3156

CentOS 7: net-snmp (CESA-2020:5350)
CVE-2020-15862

CentOS 7: glibc (CESA-2021:0348)
CVE-2019-25013, CVE-2020-10029, CVE-2020-29573

CentOS 7: perl (CESA-2021:0343)
CVE-2020-10543, CVE-2020-12723, CVE-2020-10878

MEDIUM

CentOS 7: freetype (CESA-2020:4907)
CVE-2020-15999

CentOS 7: libcroco (CESA-2020:4072)
CVE-2020-12825

CentOS 7: python (CESA-2020:5009)
CVE-2019-20907

CentOS 7: bind (CESA-2020:5011)
CVE-2020-8622, CVE-2020-8623, CVE-2020-8624

CentOS 7: resource-agents (CESA-2020:5004)
CVE-2020-11078

CentOS 7: curl (CESA-2020:5002)
CVE-2020-8177

CentOS 7: python (CESA-2020:3911)
CVE-2019-16935

CentOS 7: libxml2 (CESA-2020:3996)
CVE-2019-19956, CVE-2019-20388, CVE-2020-7595

CentOS 7: openssl (CESA-2020:5566)
CVE-2020-1971

Known Issues

The following table lists all known open issues and bugs for Version 8 Release 202102:

1	SLP and MSLA are not supported through a proxy. Additional code changes are required to resolve this issue.
2	SLP currently does not work in Pull mode when devices are behind a NAT. This is due to the way that NAT functions and discovery is prevented since all devices currently have the same address.

Version 8 Release 202010

This release covers new features scheduled for this release. In addition, it covers the following severity levels: 1, 2, and 3.

New Features

Version 8 Build 202010 has the following new features:

There are no new features in this release.

Fixes

Bug ID	Description
CSCvu75808	ADFSv3 Configuration Fails Due to a Certificate Validation Issue
CSCvw11615	Upgrading from v8-202006 to v8-202008 Causes Synchronization to Fail

Resolved Vulnerabilities and Exposures

Version 8 Release 202010 resolves the following CentOS security vulnerabilities

HIGH

CentOS 7 : curl (CESA-2020:3916)
CVE-2019-5482

CentOS 7 : glib2 and ibus (CESA-2020:3978)
CVE-2019-12450, CVE-2019-14822C

CentOS 7 : kernel (CESA-2020:4060)
CVE-2019-19537, CVE-2019-19059, CVE-2019-19534, CVE-2020-8647, CVE-2019-18808,

CVE-2020-8649, CVE-2019-15917, CVE-2020-10732, CVE-2019-15217,
CVE-2020-1749, CVE-2020-14305, CVE-2018-20836, CVE-2019-16231, CVE-2019-19046,
CVE-2019-19063, CVE-2019-19062, CVE-2019-20636, CVE-2019-19767,
CVE-2019-9454,CVE-2017-18551, CVE-2019-16233, CVE-2019-19447, CVE-2019-19524,CVE-2019-16994, CVE-2019-19523, CVE-2020-10942, CVE-2019-20054,
CVE-2020-10742, CVE-2019-15807, CVE-2019-20095, CVE-2019-12614, CVE-2019-19807,
CVE-2020-12826, CVE-2019-9458, CVE-2020-10690, CVE-2020-12770,
CVE-2020-10751, CVE-2020-11565, CVE-2020-2732, CVE-2019-17053, CVE-2019-19055,
CVE-2019-17055, CVE-2019-19058, CVE-2019-19332, CVE-2019-19530,
CVE-2020-9383

CentOS 7 : libpng (CESA-2020:3901)
CVE-2017-12652

CentOS 7 : libvpx (CESA-2020:3876)
CVE-2019-9232, CVE-2019-9433,CVE-2017-0393, CVE-2020-0034

MEDIUM

CentOS 7 : cpio (CESA-2020:3908)
CVE-2019-14866

CentOS 7 : cups (CESA-2020:3864)
CVE-2019-8696, CVE-2017-18190, CVE-2019-8675

CentOS 7 : e2fsprogs (CESA-2020:4011)
CVE-2019-5094, CVE-2019-5188

CentOS 7 : expat (CESA-2020:3952)
CVE-2018-20843, CVE-2019-15903

CentOS 7 : libmspack (CESA-2020:3848)
CVE-2019-1010305

CentOS 7 : libssh2 (CESA-2020:3915)
CVE-2019-17498

CentOS 7 : libtiff (CESA-2020:3902)
CVE-2019-17546, CVE-2019-14973

CentOS 7 : NetworkManager (CESA-2020:4003)
CVE-2020-10754

CentOS 7 : openldap (CESA-2020:4041)
CVE-2020-12243

CentOS 7 : samba (CESA-2020:3981)
CVE-2019-14907

LOW

CentOS 7 : dbus (CESA-2020:4032)
CVE-2019-12749

CentOS 7 : glibc (CESA-2020:3861)
CVE-2019-19126

CentOS 7 : systemd (CESA-2020:4007)
CVE-2019-20386

Version 8 Release 202008

This release covers these new features. In addition, it covers fixed Severity (Sev) 1 and Severity (Sev) 2 as well as resolved vulnerabilities and exposures.

New Features

Version 8 Build 202008 has the following new features:

- **MSLA RUM Support**

  Incorporate MSLA usage billing functionality
- **Endpoint Reporting Model (ERM)**

  Ensure that each endpoint is counted as a single license consumption
- **License Hierarchy-Weights**

  Provide NXOS has weighting to help determine which device to substitute a higher tier license. Each license will be given a weight, and device sums all licenses used for the total wight to determine who has priority to borrow from the parent license first.
- **Provide audit features for Administration Workspace**

  Add audit logs to each page in Administration Workspace and improve syslogs and alerts.
- **Three new commands have been added to the On-Prem Console Guide**

  The three commands are: docker_network_config, password_policy, and tcpdump. See the Cisco Smart Software Manager *On-Prem Console Reference Guide* for more information.

Version 8 Release 202008 Includes These Important Fixes from Previous Releases

CSCvs64165 and CSCvs31532 are important fixes for access token and synchronization for Release 6.x thru Release 8

As of September 25, 2020, the new default access token life is 180 days instead of 30 days. So, when an access token is expired, you will receive an "*Access Token not found Synchronization cannot proceed*" notice when you synchronize an account.

When you receive an access token not found notice, you must select the Accounts tab > Actions, and then perform a standard or full network synchronization for that account. Before the synchronization process begins, you are prompted to enter you login credentials (CCO). Once you log in, the synchronization process will proceed during the next scheduled interval.

Bug ID	Description
CSCvs31532	On-Prem - Scheduled Sync fails after 30 days
CSCvs64165	Single Sign-On(SSO) Authentication Tokens Appear to Expire after 30 Days

Other Important Fixes from Previous Releases:

Bug ID	Description
CSCvu10501	Unable to Change Docker Network IP (internal ip-addresses used by Satellite)

Bug ID	Description
CSCvu56089	Event Log Tables inside Atlantis DB Fills up Disk Space and Makes On-Prem Unstable
CSCvu83039	CA Signed UI Cert Disappears on Release/8-202006 after Reload
CSCvu93682	LCS Cert Nil Value, On-Prem Satellite Unable to Synchronize after 8-202006
CSCvv33868	Upgrade from 6.2 to 8-202006 Fails with Table "dlc_device_migrations" Error
CSCvv60899	Browser certs do not persist after HA teardown

Resolved Common Vulnerabilities and Exposures

Version 8 Release 202008 resolves the following CentOS security vulnerabilities

CRITICAL

CVE: CVE-2020-8165

HIGH

Rails: CVE: CVE-2020-8164, CVE-2020-8162

CentOS 7: grub2 (CESA-2020:3217)

CVE-2020-14310, CVE-2020-14311, CVE-2020-15707, CVE-2020-10713, CVE-2020-14308, CVE-2020-15706, CVE-2020-14309, CVE-2020-15705

CentOS 7: kernel (CESA-2020:3220)

CentOS 7: kernel (CESA-2020:2664)

CVE-2020-12888, CVE-2019-19527, CVE-2020-12654, CVE-2020-12653, CVE-2020-10757

CentOS 7: unbound (CESA-2020:2642) REMOVED

CentOS 7: unbound (CESA-2020:2414) REMOVED

CVE: CVE-2020-10772, CVE-2020-12662, CVE-2020-12663

MEDIUM

Rails: CVE-2020-8166

CentOS 7: bind (CESA-2020:2344)

CVE: CVE-2020-8616, CVE-2020-8617

CentOS 7: dbus (CESA-2020:2894)

CVE: CVE-2020-12049

LOW

CentOS 7: microcode_ctl (CESA-2020:2432)

CVE: CVE-2020-0548, CVE-2020-0543, CVE-2020-0549

Version 8 Release 202008 Known Issues

The following table lists all known open issues and bugs for Version 8 Release 202008:

1	System level SYSLOG events are not sent to the Remote Syslog server	CSCvu94867
2	Invalid cert in db with an extra - at the endnote	CSCvu93683

Version 8 Release 202004

This release covers new features scheduled for this release. In addition, it covers fixed Sev 1 and Sev 2 as well resolved vulnerabilities and exposures.

New Features

Version 8 Build 202004 has the following new features:

- **Product support of up to 300,000 devices**

  SSM On-Prem can now support from 100,000 to 300,000 devices spread across multiple accounts (a maximum of 25,000 products with any number of licenses used for each account). Note that the total time for 300,000 products can take up to two hours.
- **Provide extended life span for tokens**

  Provide capacity to set a maximum 27-year life span (9999 days) for tokens.
- **FIPS 140-2 Compliance**

  The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government standard that defines minimum security requirements for cryptographic modules in information technology products. FIPS 14-2 Certification allows Federal customers to be FIPS compliant when deploying SSM On-Prem using a STIG Profile.
- **Provide Session Limits for concurrent users**

  Supports STIG Security Settings and Features that limit maximum concurrent user logins for both the UI and for the On-Prem Shell.
- **Capacity to utilize multiple NTP Servers and Authentication with NTP Servers**

  SSM On-Prem provides additional capacity to configure a backup NTP server that utilizes Chrony for authentication. Therefore, SSM On-Prem will support the configuration of two NTP servers where the second server acts as a fallback, if the first server becomes unresponsive.
- **Enhanced localization capability to include French**

  SSM On-Prem has expanded its localization capability to include the French language.
- **Capacity to use Customer Certificates on Proxy server**

  Increased capability for using customer certificates on a Proxy server which allows customers to upload CA used with Proxy servers.
- **Endpoint Reporting Model (ERM) Compatibility**

  Endpoint Reporting Model is an additional API to Smart Licensing used to mitigate double license count for certain controllers which provides support for Wireless LAN Controller Version 16.12.1 and later.

Version 8 Release 202004 Includes These Important Fixes from Previous Releases

Bug ID	Description
CSCvt13065	On Prem 7-202001, Proxy Does Not Work with HTTPS

Bug ID	Description
CSCvs94939	Sync Credentials are Cleared after Logging Out
CSCvs91758	Device HA Switchover Fails
CSCvs78783	Duplicate Records for Insufficient Licenses Appear in Event Log
CSCvs70622	Missing Product Details Info in On-Prem 7.2 License Page for HSEC License
CSCvo04458	Licenses Not Released from Product after 90 Days of No Communication
CSCvt03959	Force Registration Does Not Cleanup License Consumption
CSCvt35383	Third Party Auth Users Cannot Generate Bearer Tokens
CSCvt27571	Cannot Access On-Prem with Chrome
CSCvt95777	If the Customer Uploads a Weak Cipher Cert for UI Cert, the GUI No Longer is Available
CSCvt89461	Smart Software Manager On-Prem 7 Displays Inconsistent License
CSCvt29523	Failed to Set Expire Date When Attempting to Register an FP4110
CSCvu22739	On-Prem Version 7-201907 or Upgraded from 7-201907 to later Versions Count Mismatch
CSCvu32429	Product Registration Fails When Syslog Server Misconfigured

Resolved Common Vulnerabilities and Exposures

Version 8 Release 202004 resolves the following CentOS security vulnerabilities

CRITICAL

CESA-2020:0374, CESA-2020:0839, CESA-2020:1016: (CVE-2019-14895, CVE-2019-14901, CVE-2019-14898, CVE-2019-17133, CVE-2019-17666, CVE-2019-19338, CVE-2019-11487, CVE-2018-20169, CVE-2019-12382, CVE-2019-15221, CVE-2019-13233, CVE-2019-11884, CVE-2019-15916, CVE-2019-16746, CVE-2019-9503, CVE-2018-7191, CVE-2019-10207, CVE-2019-13648, CVE-2019-10639, CVE-2019-3901, CVE-2019-10638, CVE-2017-17807, CVE-2015-9289, CVE-2019-18660, CVE-2019-14283, CVE-2018-19985, CVE-2019-11190)

HIGH

CESA-2020:1113: (CVE-2019-9924)

CESA-2020:1011: (CVE-2015-2716)

CESA-2020:1138: (CVE-2018-18751)

CESA-2020:1180: (CVE-2019-13133, CVE-2019-14981, CVE-2019-11472, CVE-2019-13297, CVE-2019-14980, CVE-2019-11470, CVE-2019-13295, CVE-2019-11597, CVE-2019-13135, CVE-2019-13454, CVE-2019-13134, CVE-2018-10805, CVE-2019-11598, CVE-2018-10804, CVE-2018-16749, CVE-2017-11166, CVE-2018-11656, CVE-2019-17540, CVE-2018-13153, CVE-2017-18273, CVE-2019-7397, CVE-2019-7398, CVE-2019-13301, CVE-2019-17541, CVE-2019-13300, CVE-2019-12975, CVE-2019-13306, CVE-2019-12976, CVE-2019-13305, CVE-2019-13304, CVE-2019-12974, CVE-2019-12979, CVE-2019-13309, CVE-2017-18271, CVE-2019-12978, CVE-2019-13307, CVE-2017-12805, CVE-2017-12806, CVE-2018-12599, CVE-2018-10177, CVE-2018-16750, CVE-2018-8804, CVE-2019-15139, CVE-2019-13311, CVE-2019-13310, CVE-2019-16708, CVE-2019-16709, CVE-2018-12600, CVE-2018-9133, CVE-2018-16328, CVE-2019-15140, CVE-2019-15141, CVE-2018-18544, CVE-2019-7175, CVE-2017-18251, CVE-2019-16710, CVE-2017-18252, CVE-2019-16711, CVE-2018-20467, CVE-2019-16712, CVE-2017-18254, CVE-2019-10131, CVE-2019-10650, CVE-2019-9956, CVE-2019-16713, CVE-2019-19948, CVE-2019-19949, CVE-2018-15607, CVE-2017-1000476, CVE-2018-14437, CVE-2018-14434, CVE-2018-14436, CVE-2018-14435)

CESA-2020:1000: (CVE-2019-17042, CVE-2019-17041)

MEDIUM

CESA-2020:1080: (CVE-2019-3890, CVE-2018-15587)

CESA-2020:1176: (CVE-2017-6519)

CESA-2020:1061: (CVE-2019-6465, CVE-2019-6477, CVE-2018-5745)

CESA-2020:1050: (CVE-2018-4180, CVE-2018-4181, CVE-2018-4700)

CESA-2020:1020: (CVE-2019-5436)

CESA-2020:1022: (CVE-2018-10360)

CESA-2020:0897: (CVE-2020-10531)

CESA-2020:1189: (CVE-2019-12779)

CESA-2020:1021: (CVE-2019-3820)

CESA-2020:1081: (CVE-2018-18066)

CESA-2020:1131: (CVE-2018-20852, CVE-2019-16056)

CESA-2020:0227: (CVE-2019-13734)

CESA-2020:0540: (CVE-2019-18634)

CESA-2020:1181: (CVE-2019-13232)

CESA-2020:1084: (CVE-20191-0197, CVE-2019-10218)

LOW

CESA-2020:1135 (CVE-2018-1116)

ADDITIONAL CONTAINER UPDATES

CVE-2014-1912, CVE-2011-1521, CVE-2012-0845, CVE-2012-1150, CVE-2011-4940, CVE-2015-7981

CVE-2019-547

CVE-2020-5249, CVE-2020-5247, CVE-2019-16770

CVE-2019-10193, CVE-2019-10192, CVE-2018-11219, CVE-2018-12326, CVE-2018-11218

CVE-2014-10077

CVE-2019-8331, CVE-2018-20676, CVE-2018-20677, CVE-2018-1404, CVE-2016-10735

Version 7 Release 202001

This release covers new features scheduled for this release. In addition, it also covers resolved vulnerabilities and exposures, fixed Sev 1 and Sev 2, and important fixes from previous releases.

New Features

Version 7 Build 202001 has the following new features:

There are no new features in this release.

Version 7 Release 202001 SEV 1 and SEV 2 Fixed

Bug ID	Description
CSCvs40521	Export Control with SmartTransport not working
CSCvs42156	Unique DB password per installation (HA/backend)
CSCvs43179	License showing out of compliance
CSCvs47442	Firepower Unable to Use Token
CSCvs56822	On-Prem 7-201910 is generating token without line break delimiter
CSCvs70622	Missing product details info in On-Prem 7.2 License page for HSEC licensed product

Resolved Common Vulnerabilities and Exposures

Version 7 Release 202001 resolves the following CentOS security vulnerabilities:

CESA-2019:3834 (CVE-2019-11135, CVE-2018-12207, CVE-2019-0154)

CESA-2019:3872 (CVE-2019-0155)

CESA-2019:3976 (CVE-2018-19519)

CESA-2019:4326 (CVE-2019-18397)

CESA-2019:3979 (CVE-2019-14821, CVE-2019-15239)

CESA-2019:4190 (CVE-2019-11729, CVE-2019-11745)

CVE-2019-5420

CVE-2019-5419

CVE-2019-5418

CVE-2019-16770

CVE-2019:10193

CVE-2019-10192

CVE-2018-12326

Version 7 Build 202001 Includes These Important Fixes from Previous Releases

CSCvr17188: Disabling IPv6 does not Disable IPv6

CSCvs40521: Do not support SmartTransport with EC

CSCvs47442: Firepower Unable to Use Token

CSCvs17220: Host Common Name in SSM On-Prem is Reset after Upgrade

CSCvr13793: SSM On-Prem HTP Missing Security Headers

CSCvs40226: Unintended r/w Access to the CSSM On-Prem Database Configured with Hard-coded Credentials

CSCvr51499: License Usage Count Increasing with Every Sync in License Hierarchy

Version 7 Release 202001 Known Issues

The following table lists all known open issues and bugs for Version 7 Release 202001:

1	Username not displayed for AD users in User Widget	CSCvs44010
2	SSO authentication tokens appear to expire after 30 days on Scheduled synch.	CSCvs64165

Version 7 Release 201910

This release covers new features scheduled for this release. In addition, it also covers resolved vulnerabilities and exposures as well as fixed Sev 1 and Sev 2.

New Features

Version 7 Build 201910 has the following new features:

- **sha256 signing key**

  Increased patch security with the addition of sha256 signing key.
- **LDAP Secure**

  SSM On-Prem supports tls (Transport Layer Security) and plain text login. Forces correct configuration of the host, port, bind dn, and password or you get an error message assuring proper configuration and security.
- **ADFS: OAuth ADFS**

  Add OAuth Active Directory Federation Services support for LDAP.
- **Active Directory** (OAUTH2)Add Active Directory Federation Services support

  This feature also adds Active Directory support to LDAP group import.
- **Browser Certs Management** Install User Browser Certificate and Framework

  This feature enables the customer to import their own cert through the browser) from their local directory.
- **Password Management** Password Strength Settings & Password reset/recovery workflow

  New tabs have been added in the Security Widget to set password expiration parameters as well as specific password settings to create greater password strength.
- **Account Management** Account Lock Out/Management Settings

  Enables an account to be locked after a specific number of incorrect login attempts. Allows System Administrator to re-set the password for the account.

NOTE: In this release, for auto lock feature to function properly, you must have **secondary authentication** configured.

- **Product Instance Engine (PIE) Integration with On-Prem**

Replace Tomcat container with Typhan Container for increased performance and scale. The changed architecture puts in place infra that allows for future increases in scale. See PIE Instance support below.

- **Product Instance Engine (PIE) Smart Transport Support**

  SSM On-Prem has expanded its support to include Smart by providing an endpoint to receive Smart Transport messages.
- **Product Instance Engine (PIE) Registration**

  Basic Product Instance Registration (no authorization)
- **Product Instance Engine (PIE) Third Party License**

  This feature provides licensing for third parties (Nuance, APNS), so they can use smart licensing to register products. It requires entitlement tags to be setup, creates “getKeys” request, all information is validated.
- **Security Widget Enhancement**

  This feature expands the Security Widget functionality to include Cert (see Browser Certs Management) and Password Enhancements (see Password Management).
- **Hardware Minimum Disk Space Requirement**

  Upgraded minimum disk requirement is 100 Gigabytes.
- **Increased maximum product instance capacity**

  Upgraded maximum product instance capacity to 50,000 with a maximum capacity of 25,000 product instances per account.

Version 7 Release 201910 SEV 1 and SEV 2 Fixed

Bug ID	Description
CSCvq99678	When request encountered comm fail, installs 4 licenses instead of 1
CSCvs17939	Database replication is broken in HA On-Prem

Resolved Common Vulnerabilities and Exposures

Version 7 Release 201910 resolves the following CentOS security vulnerabilities:

- CESA:2019:2091 (CVE-2018-16866, CVE-2018-16888, CVE-2018-15686)
- CESA:2019:2197 (CVE-2019-9516, CVE-2019-9511, CVE-2019-9513)
- CESA:2019:2027 (CVE-2018-18520, CVE-2018-18310, CVE-2018-16062, CVE-2019-7150, CVE-2018-16402, CVE-2018-16403, CVE-2019-7664, CVE-2019-7665, CVE-2018-18521, CVE-2019-7149)
- CESA:2019:2829 (CVE-2019-14835, CVE-2019-7222, CVE-2019-3460, CVE-2019-3882, CVE-2019-5489, CVE-2019-11810, CVE-2019-11599, CVE-2019-11833, CVE-2019-3900, CVE-2018-14625, CVE-2018-8087, CVE-2018-16885, CVE-2018-7755, CVE-2018-9516, CVE-2018-9517, CVE-2018-13094, CVE-2018-13095, CVE-2018-15594, CVE-2018-13053, CVE-2018-13093, CVE-2018-18281, CVE-2018-10853, CVE-2019-3459, CVE-2018-9363, CVE-2018-14734, CVE-2018-16658)
- CESA:2019-3055 (CVE-2019-3846, CVE-2018-20856, CVE-2019-10126, CVE-2019-9506)
- CESA:2019:2077 (CVE-2018-12327)
- CESA: 2019:2046 (CVE-2018-19788)
- CESA: 2019:2057 (CVE-2018-5741)

- CESA: 2019:2075 (CVE-2018-12641, CVE-2018-12697, CVE-2018-1000876)
- CESA: 2019:2181 (CVE-2018-16842)
- CESA: 2019:2060 (CVE-2019-6470)
- CESA: 2019:2118 (CVE-2016-10739)
- CESA: 2019:2047 (CVE-2018-14348)
- CESA: 2019:2049 (CVE-2018-18585, CVE-2018-18584)
- CESA: 2019:1884 (CVE-2019-3862)
- CESA: 2019:2136 (CVE-2019-3858, CVE-2019-3861)
- CESA: 2019:2237 (CVE-2018-0495, CVE-2018-12404)
- CESA: 2019:2033 (CVE-2018-6952, CVE-2016-10713)
- CESA: 2019-2964 (CVE-2018-20969, CVE-2019-13638)
- CESA: 2019:2189 (CVE-2018-1122)
- CESA: 2019:2030 (CVE-2019-9740, CVE-2018-14647, CVE-2019-5010, CVE-2019-9948, CVE-2019-9947)
- CESA: 2019:2110 (CVE-2018-16881)
- CESA: 2019:2099 (CVE-2019-3880)
- CESA: 2019:2159 (CVE-2018-18384)
- CESA: 2019:3197 (CVE-2019-1428)
- CESA: 2019:3197 (CVE-2019-1428)
- runc (CVE-2019-5736)
- nginx (CVE-2019-9516, CVE-2019-9511, CVE-2019-9513)

Version 7 Release 201910 Known Issues

The following table lists all known open issues and bugs for Version 7 Release 201910:

1	Partial Synch may does not decrement license count. Need to perform a full synchronization to correct the mismatch.	CSCvr92319
2	CUCM ID Renew Fails-There is a compatibility issue in this release with products that use Java Agent with version less than 3.0.13. Below is the list of products affected: • Cisco Emergency Responder (CER): Java 2.1.6 • Cisco HyperFlex Systems: Java 1.3.2 • Cisco IoT Field Network Director (FND) -(No Release Number) • Cisco Policy Suite – CPS: Java 1.2 • Cisco SON Suite: Java 1.3.6 • Cisco WebEx Meeting Server (CWMS): Java 2.1.4 • Cisco Wide Area Application Services (WAAS/vWAAS): 2.0.6 • Cisco Unity Connection: Java 2.1.6 • Cisco Unity Express Virtual (vCue): Java 2.0.10 • CloudCenter Suite: Java 2.1.4 • Data Center Network Manager (DCNM): Java 2.1 • Edge and Fog Module (EFM): Java 2.0.13	CSCvs39279

	• Evolved Programmable Network Manager (EPN-M): Java 1.2 • Identity Services Engine (ISE): Java 1.2 • Industrial Networking Director (IND): Java 1.2 • Prime Collaboration Provisioning (PCP) Java 1.3.6 • Prime Infrastructure: Java 1.1 • Prime Infrastructure Operations Center Java - (No release number) • Session Management Edition (SME): Java 2.1.6 • Stealthwatch Learning Network (SLN) Java 1.2 • Unified Communications Manager (CUCM) Java 2.1.6 • Video Surveillance Manager (VSM) Java jret1.8-11.9.0_192-fcs.x86_64 • Cisco Unified SIP Proxy (CUSP) Java 1.0 and Java 2.0.9	

Version 7 Release 201907

New Features

Version 7 has the following new Features:

- Rebrand from satellite to OnPrem

  Changes all occurrences of “SSM satellite Enhanced Edition” to “SSM On-Prem.”
- STIG OS Federal Compliance:

  Provide STIG OS to be shipped as application capable of running on CentOS 7.

  Provides an install option for SSM On-Prem that can be deployed and used by customers requiring STIG compliance.
- Security:

  Forces the Administrator to update the system password during installation

  Disallow changing the admin password back to the default password.

  Adding/Deleting User is now recorded in Event Log

  Automatically log users out of system when they have been idle for 10 minutes
- Migration Script:

  Migration script to support satellite 4.x/5.x to 6.3.

  Once you upgrade to 6.3 use the 7 Patch to upgrade to On-Prem 7.
- Platform Health:

  Provides ability for Admin role to edit information about a user from the Admin Portal.

  Improvements made to error handling in the process of converting PAK files licenses to Smart licenses.
- Localization:

  Localization for all text in UI for Japanese, Chinese, and Korean.
- High Availability

  General available release for active/standby High Availability.

  High Availability provides protection for licensing operations through the use of dual virtual machines (VM) or physical servers. This offers a redundant server which increases network availability. The feature establishes one of the SSM On-Prem VMs as the active processor while the other VM is designated as the standby and then synchronizing critical state information between them. Following an initial synchronization between the two VMs, High Availability dynamically maintains state information between them.

- License Hierarchy

  An enhanced SL Licensing model allows a higher-level license to be used to satisfy multiple lower-level licenses.

  Added support to allow lower-tier licenses to be satisfied by multiple higher-tier parents.

- Smart Transport Support

  Offers a new communication endpoint used by selected products. The new endpoint for Smart Transport is https://<ip.address>/SmartTransport

Resolved Common Vulnerabilities and Exposures

Version 7 201907 resolves the following CentOS security vulnerabilities:

- CESA-2019:1481
- CESA-2019:1235
- CESA-2019:1294
- CESA-2019:1619
- CESA-2019:1587

Version 7 Release 201907 Known Issues

The following table lists all known open issues and bugs for Version 7 Release 201907:

1	Loading errors on Firefox	CSCvm64119

Established Workarounds

Product Compatibility

Customers with products that use TLS 1.0 cannot use HTTPS to register. They must use HTTP for registration to satellite EE. This is due to Infosec not allowing TLS 1.0 to be used. This applies to Smart Agents before 1.5.

DNS Workaround

If DNS is configured incorrectly in kickstart, it cannot be corrected via Network Settings in **Administration** workspace. SSM satellite includes a text-based configuration tool called **nmtui** which can be used to edit the network interface configuration and correct IP on the interfaces that have the incorrect DNS entry.

To modify DNS please take the following steps:

1. Run **nmtui** with SUDO privileges.

   ```
   $ sudo nmtui
   ```

   As an alternative to **nmtui**, you can edit the network scripts directly (per interface):

   ```
   $ sudo vi /etc/sysconfig/network-scripts/ifcfg-ens3
   ```

2. Change the DNS1=“” property the correct DNS IP address.
3. Restart the network service to force NetworkManager to write out the new /etc/resolv_conf.

   ```
   $ sudo systemctl restart network
   ```

4. Restart the cerberus service to update the system database for Atlantis.

   ```
   $ sudo systemctl restart cerberus
   ```

5. SSM satellite does not explicitly indicate that LibCurl should re-resolve the DNS entries, so we must restart Atlantis.

   ```
   $ sudo systemctl restart satellite
   ```