# Cisco Smart Software Manager On-Prem

# Release Notes

## General Information

*Smart Software Manager On-Prem* is an on-premises asset manager which 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.

## 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*:

- *SSM On-Prem User Guide*
- *SSM On-Prem Console Guide*
- *SSM On-Prem Installation Guide*

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

- *SSM On-Prem Quick Start Guide*
- *SSM On-Prem Release Notes*

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). (*See On-Prem User Guide Appendix 1 backing up your system.)*** |

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

## Upgrading a System Prior to Version 7

If you are upgrading SSM OnPrem from a version prior to 7, please see:

*Smart Software Manager On-Prem Installation Guide (Appendix 2: Upgrading a System that is Prior to Version 7).*

## Upgrading a High Availability (HA) Cluster

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

*Cisco Smart Software On-Prem 8 Installation Guide Appendix 5 Upgrading a High Availability (HA) 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 customer's 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 then click **Submit Case**. You 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**. You 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 for access to 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.

# Release Specifications

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

## 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:

- In Use Quantity not shown for selected license in on-prem graph.

  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa75786

- Product Instances removed from OnPrem after a year of registration.

  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwb05285

- IPTables default policies are still in place.

  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvu89468

- SSM OnPrem: The search function under Product Instances Inventory panel.

  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa92002

- SSM On-Prem license reports for UC products - Export to Excel and CSV - Incorrect balances.

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa75363

- SSM On-Prem: Smart license Alerts can't be dismissed.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwb06331
- CSLU device consuming reporting licenses causes duplicated license entries.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwb16510
- Username and Password does not get saved on Email tab under Settings.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwb55507

- Sidekiq jobs get stuck in development.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwb80668
- Device's renewal is failed when configuring language to Japanese on SSM.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy94330
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa42681
- SSM OnPrem: Incorrect Product Instance deletion in OnPrem inventory UI.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa96336
- Editing CSLU product in PULL mode may result in breaking Collect Usage.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa56689
- Account users not showing in manage account section of onprem.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwb32134
- Display a spinner on all the screens where data is loaded.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwb23940
- License count mismatch issue in GUI SSMS and the report in the SSM.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa06345
- Unable to open PI by clicking on "In Use" licenses.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwb16858
- Enabling NAT feature in OnPrem disables the proxy setting and vice-versa.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa94904
  **NOTE:** NAT/proxy must be turned On, which was toggled off previously due to this bug.
- SSM On-Prem: 8-202102: GUI Needs to have TACACS attributes to fully auto.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy62936
- Send RUM reports, Licenses are not being consumed on OnPrem.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa56683
- Error when scheduling sync for customers in UTC+14 timezone.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa31053
- CSSM processing failure of accumulated un-acknowledged rum reports.

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa95039

- After upgrade the proxy settings in SLP DB are not persisted.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa56684
- OnPrem: automate proxy setting flap after an upgrade.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwc21609
- SLP network sync fails when proxy with DNS name is configured.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwb30211
- MLSA devices receive OOC when prepaid license of same type has OOC alert.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwc09667
- **When On-prem is bombarded with multiple auth renew requests DB fills up.**
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwc12764
- **Postgres version has been upgraded to 13.5.**
- Cisco Smart Software Manager On-Prem version 8-202112 Privilege Escalation Vulnerability.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwb98281

## Known Issues

| | |
|---|---|
| 1. | **CSSM <==> OnPrem (8-202201) license count inconsistencies.**<br>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.**<br>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.**<br>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.**<br>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:

- Unexpected Substitution Counts In Upgraded Versions < 8-202010
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa77416
  NOTE: Please perform full sync, if there is a license count mismatch for LH items.
- Unable to save LDAP configs when multiple LDAP groups are present
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa75049
- CSLU 'EXPORT USAGE TO CISCO' FAILS IN 8-202108
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa68845
- On-Prem to CSSM synchronization failure for SLU devices - ERROR_POLL_ID
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa62164
- Inline upgrade from 8-202108 to 8-202112 fails with database migration
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa60443
- On-Prem to CSSM synchronization failure for SLU devices - ERROR_POLL_ID(NAT)
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa55809
- SLP device state stuck in ACK received from CSSM
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa82690

## 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 and assign
them a System Role. **The widget shows individually assigned system role.**

3. Accounts roles assignment for LDAP Users: We would be able to add LDAP user as "New User" in "Manage Account" view Users' tab and assign him 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:

- Unable to save LDAP Configurations.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz12806
- Clicking on SLUP Product Instance's IP Gives details of another device.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa14135
- Partial Sync clearing Entitlement Hierarchy records.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa15038
- On-Prem should not be non-responsive when devices bombard with auth renew requests.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa03397
- Duplicated FTD base licenses in On-Prem licensing portal causing OOC.
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz69609
- On-Prem UI display partial UDI and missing UUID
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz43367

- Alerts status refreshes only after switching tabs
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz44481
- Labels in Smart Licensing keep changing after page refresh
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz14218
- Labels in Smart Licensing keep changing after page refresh
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz14218
- On-prem sending CSLU URL to SL (Smart Licensing) products and resulting in crashing of products
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa48579
- Manual and network synchronization fails after upgrade
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz69608
- SLP Device not getting deleted in CSSM
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz65233
- Licenses Used are always (none) in the Product Instance Report
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz02197
- Inability to synchronize accounts requested by System
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvx36137
- Unable to navigate to the next page using keyboard on the Licenses tab
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz03547
- HTTP 502 Bad Gateway when sending RUM to On-Prem
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy83324
- License Hierarchy Calculations mismatch between OnPrem and CSSM
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz45260
- CSLU empty data generated during usage report generation
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa52518
- Cannot downgrade System role to System User when User has assigned accounts
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwa36717
- Schedule Sync will not work if time zone UTC offset is not an integer
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz74179

## 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**<br>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**<br>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**<br>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.<br>It only applies to the product added through UI (**Add Single Product**).<br>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**<br>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**<br>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.<br>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**<br>SSM On-Prem throws an error after fetching certificates that use non-ASCII characters in the cert attributes.<br>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:

- Schedule sync failing with invalid refresh token error
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz12806
- Post-upgrade failure of account sync
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy49869

- Run report under Product Instance Report makes the page content disappear
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz02208
- Vulnerabilities: broken access control, business logic bypass
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz05241
- Fixed vulnerabilities in Centos Kernel and nss
  https://cdetsng.cisco.com/webui/#view=CSCvy56595
- Docker vulnerability (-userns-remap option)
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy13189
- Cannot change default access until after first user logged in
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy92788
- Provide option to delete TACACS users
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy92804
- Cannot add TACACS user to Local Account
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy83782
- Cannot find TACACS user
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy83776
- TACACS user role assignment via User Widget
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy80050
- Time-out to be larger than 10sec (set 0-999 seconds) for TACACS
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy92784
- SSM On-Prem is not generating a valid CSLU Transport URL
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy50544
- Authorization renewal fails with "No id cert found" error
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvx86234
- HTTP error while loading license transaction history
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvu51608
- Cancel button on Edit User issue
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz06716
- Next Page navigation with keyboard issue
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz03547
- Next Page button in Virtual Accounts not working
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy73595
- Select time in negative values
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy95322
- Displaying different On-Prem account after page refresh
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy82973
- Alerts on Product Instance point to null page
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy22891
- Add Button in the Group Details tab issue
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvx65334
- Pagination reset after Virtual Account deletion
  https://cdetsng.cisco.com/webui/#view=CSCvm52997

## Known Issues

| | |
|---|---|
| 1 | **HA support for license hierarchy issue**<br>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.<br>As a result, *entitlements_to_process(pool_id)* method of *EntitlementHierarchyService* takes into account both consumptions.<br>**CUBE licenses being double counted in HA**<br>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**<br>In some cases, accounts requested by System Users (and approved by System Operators or System administrators) fail to synchronize with CSSM.<br>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**<br>**Postgres update issues**<br>Those two known issues will be fixed with the next release. |
| 4 | **PI edit info is not saved in NAT-enabled mode**<br>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**<br>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).<br>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**<br>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.<br>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**<br>SSM On-Prem throws an error after fetching certificates that use non-ASCII characters in the cert attributes.<br>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:

- UC Applications and Prime infrastructure registrations fails after upgrading to SSM On-Prem version 8-202102
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy48103

## 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

- Scheduled Sync fails with “Access Token not found” error
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvw29893
- Scheduled sync executes on different day than desired
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvw79417
- SAN field doesn’t support multiple entries
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvv64369
- Can't import wildcard certificate (browser cert)
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvv87538
- Product registrations fail if syslog server configuration is incorrect
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvu32429
- Cannot transfer a license with a Subscription ID
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy24164
- Transfer Quantity Exceeds Available Quantity" error when transferring a license
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvx04389
- OnPrem UI not available after upgrade
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy24164

## 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

- ADFSv3 Configuration Fails Due to a Certificate Validation Issue
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvu75808
- Upgrading from v8-202006 to v8-202008 Causes Synchronization to Fail
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvw11615

## 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 *SSM On-Prem Console 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.

- Single Sign-On(SSO) Authentication Tokens Appear to Expire after 30 Days
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvs64165
- On-Prem - Scheduled Sync fails after 30 days
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvs31532

## Other Important Fixes from Previous Releases:

- Upgrade from 6.2 to 8-202006 Fails with Table "dlc_device_migrations" Error
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvv33868
- LCS Cert Nil Value, On-Prem Satellite Unable to Synchronize after 8-202006
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvu93682
- Event Log Tables inside Atlantis DB Fills up Disk Space and Makes On-Prem Unstable
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvu56089
- Unable to Change Docker Network IP (internal ip-addresses used by Satellite)
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvu10501
- Browser certs do not persist after HA teardown
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvv60899
- CA Signed UI Cert Disappears on Release/8-202006 after Reload
  https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvu83039

## 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

- On Prem 7-202001, Proxy Does Not Work with HTTPS (https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvt13065)
- Sync Credentials are Cleared after Logging Out (https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvs94939)
- Device HA Switchover Fails (https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvs91758)
- Duplicate Records for Insufficient Licenses Appear in Event Log (https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvs78783)
- Missing Product Details Info in On-Prem 7.2 License Page for HSEC License (https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvs70622)
- Licenses Not Released from Product after 90 Days of No Communication (https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvo04458)
- Force Registration Does Not Cleanup License Consumption (https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvt03959)
- Third Party Auth Users Cannot Generate Bearer Tokens (https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvt35383)
- Cannot Access On-Prem with Chrome https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvt27571
- If the Customer Uploads a Weak Cipher Cert for UI Cert, the GUI No Longer is Available https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvt95777
- Smart Software Manager On-Prem 7 Displays Inconsistent License https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvt89461
- Failed to Set Expire Date When Attempting to Register an FP4110 https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvt29523
- On-Prem Version 7-201907 or Upgraded from 7-201907 to later Versions Count Mismatch https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvu22739
- Product Registration Fails When Syslog Server Misconfigured https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvu32429

## 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

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

## 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

- When request encountered comm fail, installs 4 licenses instead of 1 (https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvq99678)
- Database replication is broken in HA On-Prem (https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvs17939)

## 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: | CSCvs39279 |

| | | |
|---|---|---|
| | • Cisco Emergency Responder (CER): Java 2.1.6<br>• Cisco HyperFlex Systems: Java 1.3.2<br>• Cisco IoT Field Network Director (FND) –(No Release Number)<br>• Cisco Policy Suite – CPS: Java 1.2<br>• Cisco SON Suite: Java 1.3.6<br>• Cisco WebEx Meeting Server (CWMS): Java 2.1.4<br>• Cisco Wide Area Application Services (WAAS/vWAAS): 2.0.6<br>• Cisco Unity Connection: Java 2.1.6<br>• Cisco Unity Express Virtual (vCue): Java 2.0.10<br>• CloudCenter Suite: Java 2.1.4<br>• Data Center Network Manager (DCNM): Java 2.1<br>• Edge and Fog Module (EFM): Java 2.0.13<br>• Evolved Programmable Network Manager (EPN-M): Java 1.2<br>• Identity Services Engine (ISE): Java 1.2<br>• Industrial Networking Director (IND): Java 1.2<br>• Prime Collaboration Provisioning (PCP) Java 1.3.6<br>• Prime Infrastructure: Java 1.1<br>• Prime Infrastructure Operations Center Java - (No release number)<br>• Session Management Edition (SME): Java 2.1.6<br>• Stealthwatch Learning Network (SLN) Java 1.2<br>• Unified Communications Manager (CUCM) Java 2.1.6<br>• Video Surveillance Manager (VSM) Java jret1.8-11.9.0_192-fcs.x86_64<br>• 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
   ```