Cisco Smart Software Manager On-Prem

Release Notes

Version 7 Release 201910

Release Date: 10/31/2019

The 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.

Finding the Cisco Software Release

Download the image from https://software.cisco.com/download/home by searching for the Product Name "Smart Software Manager satellite". From the Smart Software Manager satellite download page expand the 'All Release' then 'Enhanced Edition'. You will find the Version 7 build 201910. If you hover over the green .iso image a pop-up will have the links to all the relevant documentation

Access the Cisco Smart Software Manager On-Prem via a web browser by entering its IP address followed by the port number.

For example, if the IP address is 172.16.0.1, enter:

http://172.16.0.1:8443/admin

After logging into the admin portal, you will see the release of the Cisco Smart Software Manager On-Prem software that is running in the System Health section.

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

Patching/ Upgrading a Standalone System

Complete these steps to download the appropriate patch to your system (release 6.x-7). Set up setup

NOTE: For both patches you must go through the On-Prem Console.

Step	Action
Step 1	From the CLI, **Ssh as admin to your server IP address**, and then to open the console, type the following command: `onprem-console` **Hint**: You can use tab completion to complete the command.

Step 2	Use the copy command to **scp the patch** and the **sha256 signing key** to your patches folder.
	You are prompted for your password.
	These are two examples of the copy command.
	`copy prefix:filename user@domain.com:/path`
	`copy user@domain.com:/path/SSM_On-Prem_7-201910.sh.sha256 patches:`
	NOTE: prefix include: backup, patches, log

Step 3	From your patches folder, use the following command: `upgrade patches:filename` You are required to have an existing corresponding signature file.

Once the installation is complete the system is operational.

Patching/Upgrading a High Availability (HA) Cluster

Complete these steps to install a patch or upgrade to a HA cluster.

Step	Action
Step 1	Make sure your HA cluster is **running** and identify the **version** of SSM you are running (6.x-7).
Step 2	Identify the Primary and Standby **IP addresses**.
Step 3	Download the **appropriate version patch** and **respective sha256 signing key** from software.cisco.com. Using the onprem console's copy command to copy the same patch to both the

Step	Action

	Active (Node 1) and the Standby (Node 2).
	`copy prefix:filename/user@domain.com:/patches:`
	`copy user@domain.com:/path/filename patches:`
	`copy user@domain.com:/path/SSM_On-Prem_7-201910.sh.sha256 patches:`

Step 4	Power off the **Standby** node (Node 2).

Step 5	In the primary node (Node 1), using **admin**:
	ssh in and type:
	`onprem-console`
	Upgrade by running the upgrade command pointed to the patch script that was downloaded in Step 2.
	`Upgrade patches:filename`

Step 6	Once the installation is complete: Power off the **Active node**. (Making sure both nodes are offline to prevent failover.)
Step 7	Power on the **standby node** (Node 2) ssh into the **Standby node** (Node 2) and wait for all the resources to begin running. **NOTE**: You can watch the PCS status to monitor the startup process by issuing the following command: `ha_status`
Step 8	Install the **patch** on the **Standby node** (Node 2). as described in Step 5.
Step 9	Once the installation is complete, power down the **Standby node** (Node 2). **CAUTION**: Make sure the standby node is completely powered down before proceeding to the next step.
Step 10	Turn on the **Primary node** (Node 1) and wait until all the resources are running. **NOTE**: You can watch the PCS status to monitor the startup process.
Step 11	Turn on the **Standby node** (Node 1).
Step 12	Use the onprem-console **ha_status command** to confirm that the cluster is functioning properly. Once complete, you can now navigate to the VIP to

Step	Action
	access your Onprem instance.

The HA Cluster patch/upgrade process is complete, and the system is operational.

Cisco SSM On-Prem Releases

Refer to the *Cisco Smart Software On-Prem User Guide* for how to use Version 7 Release 201910 features. See Finding Cisco Software Release section.

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 work flow

  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 Build 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 6.3.0

New Features

Version 6.3.0 has the following new features:

- Scheduled Sync now always sync

  As part of this release, the 30-day default check will no longer performed during the maintenance window set for by the **Scheduled Sync** feature. All local Accounts which are enabled for synchronization will be synced without consideration of their last sync time.
- Account Re-Registration support

  The **Account Re-Registration** feature allow for the ability to re-register a local Account without losing the existing Users associated with the Account or having to re-register product which have been previously registered. This process can be done either in connect or disconnected mode.
- SSM satellite High Availability (HA) ** Limited Deployment

  High Availability provides protection for licensing operations using dual virtual machines (VM) or physical servers. This offers a redundant server which increases network availability. The feature establishes one of the SSM satellite 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.

NOTE: Version 6.3 introduces High Availability as an optional component of SSM satellite Enhanced Edition is currently being offered in "Limited Deployment". If you are interested in deploying this feature for early deployment, contact the SSM satellite Program for onboarding and configuration guide via the email cs-cssm-satellite-ha@cisco.com

Resolved Common Vulnerabilities and Exposures

Version 6.3.0 resolves the following CentOS security vulnerabilities:

- CESA-2018:0805
- CESA-2019:0368
- CESA-2019:0194
- CESA-2019:0163
- CESA-2019:0230

Version 6.2.0

New Features

Version 6.2.0 has the following new features:

- DLC (Device-Led Conversion)
- 3rd party integration (Apple Push Notification and Text-To-Speech)
- Max Use Tokens
- The Cisco.com API endpoint changed from api.cisco.com to swapi.cisco.com

Resolved Common Vulnerabilities and Exposures

Version 6.2 resolves the following CentOS security vulnerabilities:

- CentOS 7 : kernel (CESA-2018:1062)
- CentOS 7 : dhcp (CESA-2018:0483)
- CentOS 7 : dhcp (CESA-2018:1453)
- CentOS 7 : glibc (CESA-2018:0805)
- CentOS 7 : gnupg2 (CESA-2018:2181)
- CentOS 7 : kernel (CESA-2018:1318)
- CentOS 7 : procps-ng (CESA-2018:1700)
- CentOS 7 : ruby (CESA-2018:0378)
- CentOS 6 / 7 : jasper (CESA-2017:1208)
- CentOS 6 / 7 : libgcrypt (CESA-2016:2674)
- CentOS 6 / 7 : openssl (CESA-2017:0286)
- CentOS 6 / 7 : vim (CESA-2016:2972)
- CentOS 7 : authconfig (CESA-2017:2285)
- CentOS 7 : curl (CESA-2017:3263)
- CentOS 7 : dhcp (CESA-2018:0158)
- CentOS 7 : emacs (CESA-2017:2771)
- CentOS 7 : git (CESA-2018:1957)
- CentOS 7 : java-1.8.0-openjdk (CESA-2018:1191)
- CentOS 7 : kernel (CESA-2018:0395)
- CentOS 7 : kernel (CESA-2018:1852)
- CentOS 7 : krb5 (CESA-2018:0666)
- CentOS 7 : mariadb (CESA-2017:2192)
- CentOS 7 : ntp (CESA-2018:0855)
- CentOS 7 : openldap (CESA-2017:1852)
- CentOS 7 : openssl (CESA-2018:0998)
- CentOS 7 : patch (CESA-2018:1200)
- CentOS 7 : pcs (CESA-2018:1060)
- CentOS 7 : php (CESA-2017:3221)
- CentOS 7 : php (CESA-2018:0406)
- CentOS 7 : python (CESA-2017:1868)

- CentOS 7 : python (CESA-2018:2123
- CentOS 7 : systemd (CESA-2018:0260
- CentOS 7 : util-linux (CESA-2017:0907)
- CentOS 7 : wpa_supplicant (CESA-2017:2907) (KRACK)
- CentOS 6 / 7 : microcode_ctl (CESA-2018:0093) (Spectre)
- CentOS 7 : java-1.8.0-openjdk (CESA-2018:1649) (Spectre)
- CentOS 7 : kernel (CESA-2018:1629) (Spectre)
- CentOS 7 : kernel (CESA-2018:1965) (Spectre)
- CentOS 7 : linux-firmware (CESA-2018:0014) (Spectre)
- CentOS 7 : linux-firmware (CESA-2018:0094) (Spectre)
- CentOS 7 : microcode_ctl (CESA-2018:0012) (Spectre)

Version 6.1.0

New Features

Version 6.1.0 has the following new features:

- Improved Bulk operation
- LDAP Group Support
- User Groups
- Virtual Account Tags
- License Tags
- API Support
- Application Redundancy

NOTE: Features in satellite Classic 5.0.1 such are DLC (Device-Led Conversion), 3rd party integration (Apple Push Notification and Text-To-Speech), Utility billing, Backup/Restore, High Availability are NOT available in release 6.1.0. They will be available in the future releases.

Resolved Common Vulnerabilities and Exposures

Version 6.1.0 resolves the following CentOS security vulnerabilities:

- CentOS 6 / 7 : mutt (CESA-2018:2526) (Removed)
- CentOS 7 : bind (CESA-2018:2570)
- CentOS 7 : kernel (CESA-2018:2748)
- CentOS 7 : nss (CESA-2018:2768)

Version 6.0.0

Version 6.0.0 is the initial release of Cisco Smart Software Manager satellite Enhanced Edition. Migration from Cisco Smart Software Manager satellite will be made available at a future date.

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

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

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
   ```

Obtaining Support

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 provides the following types of support:

Follow these steps these steps to open a support ticket:

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 Products & Services tab screen opens.
Step 3	On the right section of the tab screen, click **Open Case**.
Step 4	Make sure the Request Type is set to **Diagnose and Fix**, and then scroll down the screen to the **Bypass Entitlement** field.
Step 5	In the Bypass Entitlement field, select **Software Licensing Issue** from the drop-down list.
Step 6	Click **Next**.
Step 7	In the Describe Problem screen, select the appropriate **Severity level** based on the impact to you.
Step 8	Enter the **Title** and **Description** and all **pertinent information**.
Step 9	Review the information you entered, and then click **Submit**. You license query has been submitted.

Opening a Case with TAC

Cisco Technical Assistance Center (TAC) provides unparalleled technical support service to Cisco customers, partners, and resellers. When you need help from the TAC, you have three options for opening a case with the TAC:

1. Web Access

   The TAC Service Request Tool automates the process of opening a case with TAC. The Service Request Tool is available around-the-clock at the following URL: http://tools.cisco.com/ServiceRequestTool/create/launch.do

The TAC Service Request Tool automatically suggests solutions during the case open process. This provides the opportunity for you to resolve your issue before you actually open a case. If you must open a case, the TAC Service Request Tool allows you to check its status and add updates.

You can also use Technical Documentation and Support web site, a detailed collection of tools and technical documents written by TAC engineers, to analyze common issues and provide solutions that is available at the following URL: http://www.cisco.com/en/US/support/index.html

2. Email Access

   A case may also be opened via email by sending a message to tac@cisco.com.

3. Phone Access

   There are several different phone numbers to use when calling the TAC depending on your location in the world.

Opening a Case with Global Licensing Operations (GLO)

Traditional Licensing

Go to the License Registration Portal to either generate, resend, or re-host your existing PAK-based licenses. From this portal:

- Select **Manage > Devices > Add device** (if not already added)
- Click the device to select it, then select **Actions** and then select the **required function**.

Smart Software Licensing

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

- Under **"License Conversion"**, 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.