a 

Cisco Smart Software Manager On-Prem

Release Notes

Version 8 Release 202010

Release Date: 11/15/2020

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

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

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

https://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.

Downloading the latest Cisco Software Release

Download the image from https://software.cisco.com/download/home by searching for the Product Name **Smart Software Manager**. Select the Smart Software Manager On-Prem link. From the Smart Software Manager On-Prem download page expand the **Latest Release**. You will find the Version 8 build 202008. If you hover over the green .iso image a pop-up will have the links to all the relevant documentation.

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

Upgrading a System that is Prior to Version 7

If you are patching or upgrading an SSMS system that is prior to Version 8 (SSM On-Prem) 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 the *Cisco Smart Software On-Prem 8 Installation Guide Appendix 5 Upgrading a High Availability (HA) Cluster Version 8*.

Cisco SSM On-Prem Releases

Refer to the *Cisco Smart Software On-Prem User Guide* for how to use Version 8 Release 202008 features. See Finding Cisco Software Release section.

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.

Version 8 Release 202010 Includes these Important Fixes from Previous Releases

- 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 Common 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 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 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 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
2	CUCM ID Renew Fails–There is a compatibility issue in this release with products that use Java Agent with version less than 3.0.13. Below is the list of products affected: • Cisco Emergency Responder (CER): Java 2.1.6 • Cisco HyperFlex Systems: Java 1.3.2 • Cisco IoT Field Network Director (FND) –(No Release Number) • Cisco Policy Suite – CPS: Java 1.2 • Cisco SON Suite: Java 1.3.6 • Cisco WebEx Meeting Server (CWMS): Java 2.1.4 • Cisco Wide Area Application Services (WAAS/vWAAS): 2.0.6 • Cisco Unity Connection: Java 2.1.6 • Cisco Unity Express Virtual (vCue): Java 2.0.10 • CloudCenter Suite: Java 2.1.4 • Data Center Network Manager (DCNM): Java 2.1 • Edge and Fog Module (EFM): Java 2.0.13 • Evolved Programmable Network Manager (EPN-M): Java 1.2 • Identity Services Engine (ISE): Java 1.2 • Industrial Networking Director (IND): Java 1.2 • Prime Collaboration Provisioning (PCP) Java 1.3.6 • Prime Infrastructure: Java 1.1 • Prime Infrastructure Operations Center Java – (No release number) • Session Management Edition (SME): Java 2.1.6 • Stealthwatch Learning Network (SLN) Java 1.2 • Unified Communications Manager (CUCM) Java 2.1.6 • Video Surveillance Manager (VSM) Java jret1.8-11.9.0_192-fcs.x86_64	CSCvs39279

	• Cisco Unified SIP Proxy (CUSP) Java 1.0 and Java 2.0.9	

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

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
   ```

Getting Support with 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.