Smart Software Manager On-Prem Installation Guide

Version 7 Release 201910

First Published: 02/16/2015
Last Modified: 11/22/2019

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

The Java logo is a trademark or registered trademark of Sun Microsystems, Inc. in the U.S. or other countries

CONTENTS

Preface

This section describes the objectives and organization of this document and explains how to find additional information on related products and services. This preface contains these sections.

Objectives

This document provides an overview of software functionality that is specific to the Cisco Smart Software Manager On-Prem (SSM On-Prem). It is not intended as a comprehensive guide to all the software features that can be run, but only the software aspects that are specific to this application.

Related Documentation

This section refers you to other documentation that also might be useful as you configure your SSM On-Prem. This document covers important information for the SSM On-Prem and is available online.

Listed below are other guides, references, and release notes associated with Cisco Smart Software On-Prem.

- Cisco Smart Software On-Prem Quick Start Guide
- Cisco Smart Software On-Prem Installation Guide
- Cisco Smart Software On-Prem Console Reference Guide
- Cisco Smart Software On-Prem Release Notes (Version 7 Release 201910)

Document Conventions

This documentation uses the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords used in one or more step(s).
Italic	Italic text indicates arguments for which the user supplies the values or a citation from another document
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.

Convention	Description
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
variable	Indicates a variable for which you supply a value, in context where italics cannot be used.
string	A non-quoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples for the following conventions:

Convention	Description
screen font	Terminal sessions and information the switch displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following call out conventions:

✎

NOTE Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

⚠

CAUTION Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the *What's New in Cisco Product Documentation RSS feed*.

NOTE: RSS feeds are a free service.

Introduction to Smart Software Manager On-Prem

Cisco Smart Software Manager On-Prem (SSM On-Prem) is a Smart Licensing solution that 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.

Software Packaging

Your installation package of the universal ISO for SSM On-Prem consists of the following component:

- SSM On-Prem

NOTE: This universal ISO format allows it to be exported to various install media types. Exporting of the ISO image to other image types is the responsibility of the customer and is not supported by Cisco.

System Limits and Scalability

Product and User Scalability:

- Up to 500 local Accounts
- Up to 1,000 local Virtual Accounts
- Scales up to a total 50,000 product instances with a maximum capacity of 25,000 PI per account using one license each.

Supported Web Browsers

The following web browsers are supported:

- Chrome 36.0 and later versions
- Firefox 30.0 and later versions
- Internet Explorer 11.0 and later versions

NOTE: JavaScript must be enabled in your browser.

System Requirements

Cisco Smart Account Access

Ensure that you have access to a Cisco Smart Account, and have the role of either Smart Account Admin, or Virtual Account Admin, before you proceed with the tasks mentioned in this section.

Hardware Based Deployment Requirements

The SSM On-Prem can be deployed on physical servers, such as the Cisco UCS C220 M3 Rack Server, or on a hardware based server which meet the following requirements:

Minimum	Recommended
100 GB Hard Disk	200 GB Hard Disk
8 GB RAM	8 GB RAM
x86 Dual Core	x86 Quad Core
1 Ethernet NIC	2 Ethernet NICs

Virtual Machine Based Deployment Requirements

The SSM On-Prem supports the following versions of VMware vSphere Web Client:

- VMware vSphere Web Client 5.5 thru 6.5

When creating the Virtual Machine for deployment, ensure the OS type is set to "Linux" and the Guest-OS is set to either "CentOS 7 64 bit" or "Linux Other 64 bit". The configuration of the virtual machine must meet the following configuration requirements as listed in the table below.

Minimum	Recommended
100 GB Hard Disk	200 GB Hard Disk
8 GB RAM	8 GB RAM
2 vCPUs	4 vCPUs
1 vNIC - VMXNET3 or vertio.	2 vNICs - VMXNET3 or vertio.

Supported VMware Features and Operations

NOTE: There are two firmware options in VMWare to install an application:

- UEFI
- BIOS

SSM On-Prem **only supports the BIOS option** for installation. If you have to use EFI for security reasons to install applications using EFI, then it is not possible to install the SSM.

VMware supports various features and operations that allow you to manage your virtual applications and perform operations such as cloning, migration, shutdown and resume.

Some of these operations cause the runtime state of the VM to be saved and then restored upon restarting. If the runtime state includes traffic-related state, then on resumption or replaying the runtime state, additional errors, statistics, or messages are displayed on the user console. If the saved state is just configuration driven, you can use these features and operations without a problem.

The following VMware features and operations are not supported in all versions of the Cisco Cloud Service Router (CSR) 1000v, (which is the product instance used with SSM On-Prem) but can still be used or performed on non-supported versions at the risk of encountering dropped packets, dropped connections, and other error statistics:

- Cloning
- Migration

Increasing Performance on VMware ESXi Configurations

You can improve performance on VMware ESXi configurations by performing the following:

- Disable VMware ESXi power management.
- Choose the High-Performance setting to disable power management in VMware ESXi.

For more information, see the VMware Documentation.

Deploying Cisco Smart Software Manager On-Prem

NOTE: Concise directions for deploying and installing SSM On-Prem are outlined in the *Cisco Smart Software On-Prem Quick Start Guide*.

SSM On-Prem (Enhanced Edition 6.x and later) has a new architecture and completely new user interface from previous versions (Classic Edition up to 5.x). It provides:

- Access to the Licensing workspace via https://<ip-address>:8443
- Access to the Administration workspace via https://<ip-address>:8443/admin

It has new registration and synchronization procedures, new system roles and Role Based Access Control (RBAC) for license management, external authentication, syslog, proxy, and other functions. Cisco recommends that you review the *Cisco Smart Software Manager On-Prem User Guide* to understand how the new system architecture, user interface, accounts, setup, and operations have changed.

Overview

The following three phases need to be completed (in the listed order) to get your SSM On-Prem operational and to access Smart Licensing functions:

1. **Media Installation**: Follow the installation guide to deploy the On-Prem via the installation procedure (see below).
2. **Register SSM On-Prem**: In this phase, perform the following:
   a. Configure the Common Name on SSM On-Prem (Security Widget > Certificates)
   b. Synchronize the NTP server (Settings Widget > Time Settings)
   c. Register a new local Account (**Accounts > New Account**) see the *Smart Software Manager On-Prem User Guide*). An alternative method is to request a new local Account after logging into the Licensing workspace.
3. **Approve a new local Account**: Once a new local Account has been requested, it will be listed in the On-Prem Administration workspace **Account** widget under the **Account Request** tab. Next, you will need to select the appropriate method to complete the registration of your local Account with your Cisco Smart Software Manager Virtual Account which is with your Smart Account (see the *Smart Software Manager On-Prem User Guide*).
4. **Synchronize Accounts** (Synchronization Widget)

When this process is finished, you can begin using Smart Licensing features such as registering products, creating local Virtual Accounts or users, viewing/transferring product and license status, etc.

Media Installation

To begin the installation, you must download the **ISO file** on the Cisco Smart Software Manager On-Prem software package. See the Cisco software downloads link and search for Smart Software Manger to obtain the package.

Manually Deploying on Hardware Using the .iso File (USB)

Complete these steps to manually deploy the **ISO file using a USB drive**.

Step	Action
Step 1	Make a bootable USB-drive by transferring the **downloaded iso file** to USB (example using the Linux dd command)
Step 2	Insert the **installation USB** into the server to begin installing the system.
Step 3	Wait for the media to complete and proceed to the **SSM On-Prem Kickstart Installation.**

Manually Creating a VM Using the .iso File (VMware ESXi)

While the following procedure provides general guidance for deploying the Cisco CSR 1000v, the exact steps that you need to perform can vary depending on the characteristics of your VMware environment and setup. The steps and screens in this procedure are based on VMware ESXi 5.0.

Complete these steps to create a VM using the VMware ESXi.

Step	Action
Step 1	Copy the **software package** onto the VMware Datastore.
Step 2	In the VSphere client, select the **Create a New Virtual Machine** option.
Step 3	Under Configuration, select the **create a Custom configuration**, and then click **Next.** Under Name and Location, specify the **name** for the VM and then click **Next.**
Step 4	Under Storage, select the **datastore** to use for the VM and then click **Next.**
Step 5	Under Virtual Machine Version, select **Virtual Machine Version 8.** Click **Next.**
Step 6	Under Guest Operating System, select **Linux** and the **Other Linux (64-bit) setting** from the drop-down menu and then Click **Next.**
Step 7	Under CPUs, select the following settings: **2** or **4 Cores** **NOTE**: The number of cores per socket should always be set to 1 regardless of the

Step	Action
	number of virtual sockets selected. For example, a 4 vCPU configuration should be configured as 4 sockets and 1 core per socket.
Step 8	Under Memory, configure the **supported memory size** (8 gigabytes are recommended) for your deployment.
Step 9	Under **New Hard Disk**, configure 200 gigabytes (recommended).
Step 10	Under Network, allocate at least **1 virtual network interface** card (vNICs).
Step 11	Under SCSI Controller, select **LSI Logic Parallel.**
Step 12	Under New CD/DVD Drive, select **Datastore ISO file.**
Step 13	Mount the software package from the location used in **Step 2** and then check the box for **Connect.**
Step 14	Finalize the **Virtual Machine** configuration.
Step 15	Once completed, right-click on the **machine name** and select **power on.**

Registering a Local Account in Smart Software Manager On-Prem

After you have setup SSM On-Prem, the next step is to log into your SSM **On-Prem Administration Workspace** and register your first account.

Complete these following steps to register SSM On-Prem with Cisco Smart Account to enable access to Smart Licensing functions:

Open the Cisco SSM On-Prem **Administration** workspace using the following URL:

https://<*ip-address*>:8443/admin/

When the login screen displays, login using these credentials:

- Admin Userid: **admin**
- Admin Initial Password: **CiscoAdmin!2345**

You are prompted to **type in a new password** for the admin, then asked to login using the **new password** you just created.

CAUTION: For security reasons, you will be required to immediately change the **admin password** or disable the account after you create a new local account to be used for administration.

Configuring Your Common Name

Complete these steps to configure your common name.

Step	Action
Step 1	Navigate to the **SSM On-Prem Administration Workspace** https://<ip-address>:8443/admin **NOTE**: Where IP-address is the value used during installation. If part of an HA cluster, the virtual IP address should be used.
Step 2	Open the **Security Widget.**
Step 3	In the Certificates tab, enter the **Host Common Name** (IP address).
Step 4	Click **Save.**

NOTE: The SSM ON-PREM-URL is the Common Name (CN). The Common Name (CN is set in the Administration Workspace within the Security Widget, and is entered in the form of a Fully Qualified Domain Name (FQDN), hostname, or IP address of the

SSM On-Prem.

The common name must match what is used on the product as part of the call-home configuration.

Configuring the NTP Server

Currently, you can set the time manually or allow it to synchronize with NTP. The time zone for your SSM On-Prem system can also be set with UTC+0 which allows for all the timestamps to be displayed in UTC time. UTC+offset enables the timestamp to be displayed in the system's local time.

NOTE:

When you change the time setting, all scheduled background jobs will also be rescheduled to reflect the changed time.

Complete these steps to configure Time Settings.

Step	Action
Step 1	Navigate to the **SSM On-Prem Administration Workspace** https://<ip-address>:8443/admin **NOTE**: Where IP-address is the value used during installation. If part of an HA cluster, the virtual IP address should be used.
Step 2	Open the Settings Widget, and then select the **Time Settings** tab.
Step 3	Select **Time Zone** from the drop down menu.
Step 4	To Synchronize with an NTP Server: a. Turn on **Synchronize with NTP Server**. b. (Required) Enter the **NTP Server Address**. c. Click **Synchronize Time Now**.
Step 5	Click **Apply**. **NOTE**: Click **Reset** if you need to reset the time settings to the default settings.

Requesting a New Local Account

It is necessary to register with Cisco Smart Software Manager (https://software.cisco.com) to use the Smart Software Manager On-Prem. To complete this process, ensure you meet the following requirements:

- Access to a Smart Account.
- A valid CCO User ID and Password to access the Smart Account.
- Either Smart Account or Virtual Account access to a Cisco Smart Account.
- Either an eligible existing or new Cisco Virtual Account.

With these requirements met, you will be able to proceed with the registration process by completing these steps to register (request) a local Account.

Step	Action
Step 1	Navigate to the **SSM On-Prem Administration Workspace** https://<ip-address>:8443/admin **NOTE**: Where IP-address is the value used during installation. If part of an HA cluster, the virtual IP address should be used.
Step 2	Open the **Accounts widget**.
Step 3	Click **New Account** Enter the required information: local **Account Name**, Cisco **Smart Account**, Cisco **Virtual Account**, and **Email** for notification. The required fields are labeled with * **NOTE:** The Cisco **Smart Account** must exist on Cisco Smart Software Manager. A Cisco **Virtual Account** will be created if it does not exist on Cisco Smart Software Manager. Only one SSM On-Prem can be registered to a Cisco **Virtual Account** on Cisco Smart Software Manager.
Step 4	Click **Submit**.
Step 5	The Account request then is listed on the **Account Requests** tab in the **Accounts** widget.

Approving a New Local Account

Once a new local Account has been requested, the local Account request will show up in the Administration workspace in the Accounts Widget Account Requests Tab, waiting for the System Administrator to approve, and register, the local Account to your Cisco Smart Account. As the final step in the registration procedure, you need to decide if the SSM On-Prem will be used in an online (Network Mode) or offline (Manual Mode).

Local Account Request Approval (Network Mode)

Use the Approve option to select the **Network Registration.** This method registers the local account to Cisco Smart Software Manager over your network. This method is recommended for using a registration request. Complete the following steps to register the local Account to Cisco Smart Software Manager.

Step	Action
Step 1	In the Administration Workspace for the account requesting approval in the Account Requests tab of the Accounts widget, select **Approve** under the **Actions** drop-down.
Step 2	Click **Next**.
Step 3	When prompted, enter your **CCO ID credentials** to allow Cisco Smart Account/Virtual Account access on Cisco Smart Software Manager.
Step 4	Click **Submit**. • SSM On-Prem provides a status of the registration progress. • Upon successful registration, a pop-up message “Account was created successfully” shows on the screen.
Step 5	Verify that the local Account is listed as **Active** under the **Accounts** tab.

Local Account Approval (Manual Mode)

You can also manually register the local Account to Cisco SSM. To manually register a local account, select **Manual Registration.**

NOTE: While manual registration is supported, it is not recommended because you must keep track of the specific registration request/authorization file(s) for each registration.

Complete these steps to manually register a local Account to Cisco Smart Software Manager.

Step	Action
Step 1	In the Administration workspace, for the account requesting approval in the Account Requests tab of the Accounts widget use the Actions drop-down to click **Manual Registration**.
Step 2	Click **Generate Account Registration File** to generate and save the file to your local file directory. Click outside the dialog box or press the Esc key to dismiss the dialog. **NOTE**: After this step, you are required to open a new tab in the browser and log into **Smart Software Manager** to authorize the registration file. Follow the steps 3-11 to log on and continue the process.
Step 3	Launch the **Smart Software Manager** from the URL https://software.cisco.com/#SmartLicensing-On-Prem
Step 4	Log into your **local Account** in Smart Software Manager using your local Account **username** and **password**.
Step 5	On the **Smart Software Manager** screen, click the **On-Prem Accounts** tab.
Step 6	In the **On-Prem Accounts** tab, click **New On-Prem….**
Step 7	In the **New On-Prem** dialog box, enter the **On-Prem Name**.
Step 8	Click **Choose File** to select **the registration file** that was generated in the Cisco SSM On-Prem Setup Tool.
Step 9	In the Virtual Accounts field, specify the **Cisco Virtual Account** that you want to add to the new SSM On-Prem installation.
Step 10	In the text box next to Contact Email Address field, enter your **email address**. You will be notified by email once the On-Prem file has been authorized.
Step 11	Click **Generate Authorization File** to proceed. A message is displayed stating that an authorization file is generated within 48 hours of the request and that you will receive an email notification to download the same. **NOTE**: If the authorization file is not generated within 48 hours of your request or you do not receive an email notification, you can contact Cisco support (https://www.cisco.com/tac).
Step 12	Log into **Cisco Smart Software Manager** after you receive the email notification. Navigate to the **Satellites** tab.

Step	Action
Step 13	In the Satellites tab, search the **On-Prem table** of local Accounts to locate the new **Authorization File** that you created. An alert message in the Alerts column displays: **Authorization File Ready** and a link in the Actions column displays: **Download Authorization File** for your new On-Prem install.
Step 14	Click the **Download Authorization File** link and download the authorization file to a local directory on your hard drive. **NOTE**: After this step, revert to **SSM On-Prem** and upload the authorized file. Continue with the setup process.
Step 15	In the **Smart Software Manager**, at the **Register On-Prem** step, click **Browse** and navigate to the location where the authorized SSM On-Prem file was downloaded.
Step 16	Click **Upload** to upload the authorized SSM On-Prem file.
Step 17	Click **Next** to proceed.
Step 18	Click **Next** to proceed to the **Synchronization Widget.** A periodical synchronization must happen between the On-Prem and the Cisco licensing servers to update the licenses and reauthorize any product instances.

Synchronizing Smart Software Manager On-Prem

Now that Smart Software Manager On-Prem local Account has been registered and approved, you will need to synchronize the account with Cisco Licensing servers.

Proceed to the **Synchronization Widget** and perform a synchronization.

NOTE: A periodic synchronization must happen between the SSM On-Prem and the Cisco licensing servers to update the licenses and reauthorize any product instances.

Registering Product Instances

Register product instances to the SSM On-Prem. See the *Registering Product Instances to the On-Prem section in the Cisco Smart Software Manager On-Prem User Guide* and the documentation for your product.

- Cisco Products use the following API endpoints:
  - HTTPS(443): tools.cisco.com. (Registration/Authorization)
  - HTTP(80): **www.cisco.com**
- Smart Software Manager On-Prem uses the following API endpoints:
  - User Interface: HTTPS (8443) Only
  - Products: HTTP (80)/HTTPS(443)
  - CSSM: HTTPS (443)
    - Syncs:
      api.cisco.com. (6.2 and prior)
      swapi.cisco.com (6.3 and later)
      IPv4: 146.112.59.25
      IPv6: 2a04:e4c7:fffe::4
    - Account Registration: cloudsso.cisco.com
    - Patches and Upgrades

Troubleshooting

The following four sections describe actions to take when dealing with: Account Registration, Product Registration, Network Synchronization, and Manual Synchronization. Refer to the topics below if you have trouble in these areas.

Account Registration Issues

- The Smart Licensing and Manage local Account options are grayed out on the Licensing workspace
    - You need to request a new or access to an existing local Account
    - Register it to Smart Software Manager
    - Log back into the Licensing workspace and your local Account will show up on the upper right-hand side
    - Once a local Account is created and registered, these options are enabled
- Cannot add a user
    - Verify that you have the appropriate authentication method configured in the Administration workspace
    - If you are using LDAP, the user must log into SSM On-Prem Licensing workspace first before they can be found in the “Add User” screen
- Cannot register a product
    - Verify that you have a token which has not expired
    - Verify the URL on the product points to the proper common name or IP address for SSM On-Prem. (For details, see Filling in the Common Name.)
- When a user logs in to the Licensing workspace, they cannot see their SSM On-Prem local Account
    - Ensure the use has been assigned a role for (access to) the local Account. The available roles are local Account Administrator, local Account User, Local Virtual Account Administrator, Local Virtual Account User
- What ports are used in SSM On-Prem?

- User Interface: HTTPS (Port 8443)
- Product Registration: HTTPS (Port 443), HTTP (Port 80)
- Cisco Smart Software Manager: Ensure port 443 (HTTPS) is allowed through your firewall and ensure the following are accessible:
    - cloudsso.cisco.com
        - 173.37.144.211
        - 72.163.4.74
    - api.cisco.com (Prior to 6.2.0)
        - 173.37.145.221
        - 72.163.8.72
    - swapi.cisco.com (6.2.0 and later)

Product Registration Issues

If you experience issues with the product registration process, take the following actions:

- Ensure that the SSM On-Prem configuration is correct.
- Verify the Network Widget settings in the Administration Workspace are properly configured.
- Verify the time on the On-Prem is correct.
- Verify that the Call-Home configuration on the client points to the SSM On-Prem.
- Verify the token has been generated from the SSM On-Prem used in the call-home configuration.
- Your firewall settings should allow traffic to and from SSM On-Prem for the following:
  - 443 if using HTTPS
  - 80 if using HTTP
  - User browser to SSM On-Prem IP address uses port 8443

NOTE: Products which support Strict SSL Cert Checking require the hostname for SSM On-Prem to match the destination http URL address configured for the product.

Manual Synchronization Issues

If you experience issues with the manual synchronization process, take the following actions:

- Verify the time on the On-Prem is correct.
- Verify the licenses in the associated virtual account.
- Make sure that you are uploading and downloading the YAML (request and response) files from the correct SSM On-Prem Account. You can do this by verifying that the file names include the name of the SSM On-Prem that you are synchronizing.

NOTE: You can be notified to re-perform a full manual synchronization after a standard manual synchronization.

Network Synchronization Issues

If you experience issues with the network synchronization process, take the following actions:

- Verify that the SSM On-Prem can reach cisco.com
- Ensure port 443 (HTTPS) is allowed through your firewall and that the following can be accessed:
  - cloudsso.cisco.com
    - 173.37.144.211
    - 72.163.4.74

  - api.cisco.com (Prior to 6.2.0)
    - 173.37.145.221
    - 72.163.8.72)
  - swapi.cisco.com (6.2.0 and later)
- Verify that the SSM On-Prem can reach the configured DNS server.
- Verify that the time on the SSM On-Prem is correct.

IP Address Conflict

If you experience issues with the IP address conflict, take the following actions:

- Verify that an IP address conflict has not occurred due to using atlantis0 as a management IP address. (If this occurs, contact Cisco Support)

Appendix 1. Patching/ Upgrading a Standalone System

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

NOTE: Before performing an upgrade, it is recommended that you have a backup of your database or a snapshot of the machine (if you are using a VM).

You must install the patches 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.
	The following example is a copy command
	`>> copy user@domain.com:/path/SSM_On-Prem_7-201910.sh patches:`
	`>> copy user@domain.com:/path/SSM_On-Prem_7-201910.sh.sha256 patches:`
	NOTE: prefix includes: backup, patches, log

Step 3	From your patches folder, use the following command: `>> upgrade patches:SSM_On-Prem_7-201910.sh` 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

CAUTION!: Make sure the following conditions are met when upgrading a High Availability (HA) cluster.

1) Before performing an upgrade, it is recommended that you have a backup of your database or a snapshot of the machine (if you are using a VM).
2) In a High Availability (HA) cluster, performing a snapshot can invoke a failover, therefore it is recommended to only perform snapshots in a degraded state (the other node is completely powered off).
3) The cluster has been reverted to a standalone state (created two independent nodes by initiating the ha_teardown command on each node).

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

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`
Step 2	Identify the **IP address** for the Active node (Node 1), and using the onprem console, initiate the ha_teardown command.

Step 3	Download the **appropriate version patch** and **respective sha256 signing key** from software.cisco.com.
	Using the onprem console's copy command lines, copy this patch to the **Active node** (Node 1).
	`>> copy user@domain.com:/path/SSM_On-Prem_7-201910.sh patches:`
	`>> copy user@domain.com:/path/SSM_On-Prem_7-201910.sh.sha256 patches:`

Step 4	Identify the **IP address** for the Standby node (Node 2), and using the onprem console, initiate the ha_teardown command.

Step 5	Use the **same command lines** to copy the patch to the proposed Standby (Node 2) server.
	`>> copy user@domain.com:/path/SSM_On-Prem_7-201910.sh patches:`
	`>> copy user@domain.com:/path/SSM_On-Prem_7-201910.sh.sha256 patches:`

Step	Action

Step 6	In the Active node (Node 1) sever, using **admin**:
	ssh in and type:
	`onprem-console`
	Upgrade by running the upgrade command pointed to the patch script that was downloaded in Step 3.
	`>> upgrade patches:SSM_On-Prem_7-201910.sh`

Step 7	In the Standby node (Node 2) sever, using **admin**:
	ssh in and type:
	`onprem-console`
	Upgrade by running the upgrade command pointed to the patch script that was downloaded in Step 3.
	`>> upgrade patches:SSM_On-Prem_7-201910.sh`

Step 8	**NOTE**: This process can take several minutes, you will see a message: SSM Update Complete! Wait 10 min for all containers and processes to come to completion. Once steps 6 and 7 have completed, proceed to step 9.
Step 9	Re-deploy HA (refer to Appendix 2) on the node that was active at the time of teardown.

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

Appendix 2. Adding a High Availability (HA) Cluster to Your System

(Available on SSM On-Prem Version 7 Release 201907 and later.)

SSM On-Prem Enhanced High Availability support is provided by pacemaker and corosync. These applications are provided in the ISO packaging to simplify the install and configuration of these applications.

Prerequisites Needed for Deploying a High Availability (HA) Cluster

- Hostnames must be unique on each node of the HA cluster (for example, Host 1 and Host 2). If the nodes have the same name, the HA deployment will fail! Use the OnPrem Console hostname command to change the hostname of the machines.

⚠

CAUTION: If host names within the HA cluster match, then the deployment will fail requiring teardown and re-deployment.

- The virtual IP must **be an unassigned** (not in use) **IP address**; because the IP address will be used as a floating IP address across the cluster.
- SSM On-Prem must share the same SSM On-Prem version across each node. Deploying an HA cluster across different versions of SSM On-Prem is not supported.
- Both nodes must have an IP address, network mask, gateway and both nodes must be within the **same network** and must be able to communicate/ping each other.
- The standby node should be a **new**, **unregistered instance** of SSM On-Prem, because after HA is deployed, data will be replicated from the active node to the standby node.

Deploying the HA Cluster

HA deployment is only conducted through the On-Prem CLI console using specific commands. For help commands, see *Cisco SSM On-Prem Console Guide* for more information on help commands. A custom install script has been provided to simplify installation and configuration. This script is located in the On-Prem console and is initiated through the <ha_deploy> command.

NOTE: See the Cisco Smart Software On-Prem Console Reference Guide on how to use the On-Prem Console and help commands.

NOTE: If you select STIG mode at installation, when you ssh into the SSM On-Prem server you are automatically placed into the On-Prem console. If you select the Standard mode, you can ssh into the SSM On-Prem server and at the bash prompt issue the command <onprem-console> to open the console.

Complete these steps to add a standby On-Prem (HA node).

Step	Action
Step 1	(Recommended) Backup your **database** before deploying an HA Cluster.
Step 2	Provision the **standby node** for HA deployment by entering this command: ha_provision_standby
Step 3	At the prompts, supply: d. The primary node **IP Address** (Active IP) e. A **unique password** for authenticating nodes within the cluster
Step 4	Enter **ha_deploy** on the primary node and use the following parameters: a. The primary node **IP Address.** b. The standby node **IP address.** c. The **IP address** for the floating virtual IP. **NOTE**: The Virtual IP address must be free (not in use). d. Enter the **HA Password** (see step 2b)
Step 5	Wait approximately 10 minutes for the system to update. You will see a notice that the deployment was successful. Once updated, you can open the SSM On-Prem Licensing workspace by going to https://<ip-address>:8443 or the Administration workspace by going to https://<ip-address>:8443/admin/ where `ip-address` is the address of the virtual IP.

NOTE: Any data entered into the standby On-Prem database will be discarded once the HA cluster is formed, as it will begin replicating data from the active SSM On-Prem.

CAUTION: When accessing the SSM On-Prem, always use the VIP address. Do not access the server using the Service IP addresses except for direct HOST OS access.

The HA configuration ensures all data is automatically replicated between the active and standby satellite. In the event there is a loss of connectivity with the active satellite, an automatic failover occurs, and the standby satellite starts responding, enabling a non-disruptive recovery and continuous operation.

In case the HA setup is unsuccessful (seen from logs) due to connectivity issues or any other unforeseen issues, it is advisable to retry Installing an HA Cluster after performing the steps described in Downgrading a High Availability Cluster section. Downgrading will convert SSM On-Prem back to stand-alone mode.

Once in the On-Prem console, use this command to access an HA Cluster:

```
ha_status
```

NOTE: High availability clusters are accessed through the On-Prem console.

HA status and commands are used through the On-Prem Console. See Appendix 1 Console Help Commands for information and explanations of the help commands.

Once enabled, the active SSM On-Prem automatically begins the process of replicating data to the standby satellite. Until the initial data has finished replication across the nodes, the standby SSM On-Prem is unavailable.

Forced Failover of a High Availability Cluster

NOTE: This switchover from **Active** to **Standby** can take up to 2 minutes.

After a switchover occurs, the Standby is promoted to the active On-Prem and the degraded SSM On-Prem is demoted to standby when it rejoins the cluster.

Downgrading a High Availability Cluster

A Cisco Smart Manager On-Prem cluster can be directly downgraded to a single node standalone.

Use the On-Prem Console to connect to the **Primary/Active** SSM On-Prem using the <ha_teardown> command:

After verifying the SSM On-Prem's operation, the Secondary/Standby server must be discarded and cannot be reused. You will now have a standalone system instead of a cluster.

NOTE: See the Cisco Smart Software On-Prem Console Reference Guide on how to use the On-Prem Console and help commands.