Cisco Smart Software Manager On-Prem Installation Guide

Version 9 Release 202406

First Published: 02/16/2015
Last Modified: 6/26/2024

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

Cisco Confidential

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

Cisco Confidential

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 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 Manager On-Prem Quick Start Guide
- Cisco Smart Software Manager On-Prem User Guide
- Cisco Smart Software Manager On-Prem Console Reference Guide
- Cisco Smart Software Manager On-Prem Migration Guide
- Cisco Smart Software Manager On-Prem Release Notes

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.

Cisco Confidential

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.

Cisco Confidential

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.

Downloading the Software

Cisco SSM On-Prem is available as a free download from Cisco and is provided as a New Installation package or an upgrade package for in-place upgrades from previous versions.

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 300,000 product instances with a maximum capacity of 25,000 Products per account using one license each. To reach 300,000 products, the products must be spread over 12 or more accounts.

NOTE: When the server under heavy SL load, it will take about 6hrs for the system to relax and for the UI to be usable after upgrade.

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.

Cisco Confidential

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.

Virtual Machine-Based Deployment Requirements

The SSM On-Prem supports VMware ESXi 6.0 through 7.0 Update 3. **The SSM On-Prem version 8-202401 and above supports ESXi 8.0 Update 2.**

NOTE:	Secure Boot option is not supported in **ESXi 8** and above versions and should be disabled.

When creating the Virtual Machine for deployment, ensure the OS type is set to “Linux” and the Guest-OS is set to “**Other 5.x or later Linux (64 bit)**”, (if this option is not available, choose **Other 4.x** or **Other 3.x** as per availability).

The configuration of the virtual machine must meet the following configuration requirements as listed in the table below.

NOTE:	The numbers listed in the table below are only supported with new installations. Resizing an existing installation, or during an upgrade, is not supported. To achieve the numbers in the table below with an existing installation: • Upgrade to the latest version without changing any configurations. • Take a DB backup. (See the "Backing Up the SSM On-Prem Release 8" section of the *Cisco Smart Software Manager On-Prem User Guide*.) • Perform a new SSM On-prem installation with the configurations listed in the table below and then restore the DB backup on the new installation. (See the "Restoring the SSM On-Prem Release 8" section of the *Cisco Smart Software Manager On-Prem User Guide*.) • Shutdown the SSM On-Prem with the older version.

Cisco Confidential

Capacity Limitations

Deployment (Devices)	Small (SL and SLP)	Medium (SL and SLP)	Large (SL and SLP)	Maximum (SL Only)
Products	10,000*	15,000	100,000	300,000
Hard Disk	250 Gigabyte	300 Gigabyte	500 Gigabyte	500 Gigabyte
Memory	16 Gigabyte	16 Gigabyte	32 Gigabyte	32 Gigabyte
vCPU	4 vCPU	6 vCPU	8 vCPU	8 vCPU

* 8000 SL and 2000 SLP devices.

NOTE: The above numbers are applicable to total number of SL and SLP devices on single On-Prem Server. The numbers hold good when majority of SL devices are used. Also, you cannot use more than 500 SLP devices per tenant.

For example:

- In large scale deployments, 15000 to 18000 SL devices are deployed and 3000 SLP devices are deployed over 6 tenants(500/tenant).
- In small scale deployments, 3000 SL devices and 500 SLP devices are deployed.
- Cisco recommends not more than 15000 to 18000 SL devices/tenant, and 500 SLP devices/tenant, regardless of deployment size.

Supported VMware Features and Operations

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

- UEFI
- BIOS

SSM On-Prem supports **only UEFI mode for installation**, BIOS mode is a legacy option and is not supported. For UEFI installation, secure boot option should be disabled for ESXi 8 and above versions.

The following VMware features and operations are not supported in all versions of 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

Cisco Confidential

Installing and Deploying Cisco Smart Software Manager On-Prem

NOTE: Concise directions for deploying and installing SSM On-Prem are outlined in the *Cisco Smart Software Manager 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 of Deployment Sequence

Before You Start

Before you begin the installation and deployment of SSM On-Prem, make sure you have the following resources available:

1. Downloaded the ISO image from software.cisco.com.
2. A dedicated IP address (or addresses if you are deploying a High Availability cluster).
3. An established Netmask.
4. A DNS (Domain Name Server) Address.
5. A password that is a minimum of 15 characters using mixture of: upper case, lower case, number, and special character (for example CiscoAdmin!2345).
6. A Network Time Protocol (NTP) Server Address.

The following five steps must be completed (in the order listed) to ensure a successful installation.

Installation Steps

1. **Manually Installing on a VM Using the .iso File**: See the “Manually Installing on a VM Using the .iso File (VMware ESXi)” section for steps on how to deploy the On-Prem via the installation procedure.
2. **SSM On-Prem Configuration**: 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)

Cisco Confidential

3. **Register a new Local Account**: Once a Local Account has been setup, you will need to create at least one Local Account for On-Prem to connect and synchronize with your Smart Account and register it with Cisco. This is accomplished by navigating to the On-Prem Administration workspace **Account** widget > **Account** > **New Account** (see the *Cisco Smart Software Manager On-Prem User Guide*). An alternative method is to request a new Local Account after logging into the Licensing workspace.
4. **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 *Cisco Smart Software Manager On-Prem User Guide*).
5. **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.

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

While the following procedure provides general guidance for deploying SSM On-Prem, 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 the supported versions of VMware ESXi (See Virtual Machine Based Deployment Requirements for supported versions). Please refer to your VMware user guide for specific installation steps needed for your VMware deployment.

Step	Action
Step 1	Navigate to: https://software.cisco.com/download/home
Step 2	In the Select a Product field, search for **Smart Software Manager**.
Step 3	On the left-hand column under Latest Release, select **9-202406**, and select the appropriate version: • SSM_On-Prem-9-202406_Migration.zip Used to upgrade an existing SSM On-Prem license server to this version.
Step 4	When the download is complete, navigate to the **directory where the zip file was saved** and then right-click the **file** and select **unzip image**.
Step 5	Copy the **software package** onto the VMware Datastore.
Step 6	Log into V-sphere and click **VMs and Templates**.
Step 7	Next, create a **new folder** by right-clicking and selecting **New Folder** from the drop-

Cisco Confidential

Step	Action
	down menu and then **name the folder**.
Step 8	Right-click on the folder and select **New Virtual Machine** and then click **Next**.
Step 9	Enter a **Name** for the Virtual Machine (VM) and then click **Next**.
Step 10	Select **Storage**, and then click **Next**.
Step 11	Under Virtual Machine Version, select **Virtual Machine Version 8** and then click **Next**.
Step 12	Select a **compute resource** and then click **Next**.
Step 13	Select **Storage** and then click **Next**.
Step 14	Select **Compatibility** and click **Next**.
Step 15	Select either **ESXi 6.0 or later versions.**
Step 16	Select a **Guest OS** and then click **Next**.
Step 17	When Guest OS is selected, select **Linux** for the family and for Guest OS version, select a 64-bit version: **Other 5.x or later Linux (64 bit),** (if this option is not available, choose **Other 4.x** or **Other 3.x** as per availability).
Step 18	Under CPUs, select the following settings: **4 Cores**. The actual vCPU setting will vary depending on your scale requirements. **NOTE**: The number of cores per socket should always be set to 1 regardless of the number of virtual sockets selected. For example, a 4 vCPU configuration should be configured as 4 sockets and 1 core per socket.
Step 19	Select the following configuration options: a. CPUs: **4** b. Number of cores per socket: **1** c. Memory: **16 GB** d. New Hard Disk: **250GB** and **verify provisioning** are set to **Thin Provision**. e. New Network: Select **E1000 adapter type** (or VMXNET 3) and select **Connect at Power On**. f. Click **Add New Device** (for adding an extra network device) and add another **Network Adapter** (ensure that you use the same configuration for the new device described in step 15e).

Cisco Confidential

Step	Action
	g. New CD/DVD Drive: Select **DataStore ISO** from the list, then select **uploaded iso** and **connect at power on**. h. Select firmware as **EFI** in Boot Options in the **VM Options** tab. **Note:** Disable Secure boot if ESXi version is 8 or above.
Step 20	Click **Next**.
Step 21	Review the configuration and click **Finish**.

Deploying Cisco Software Manager On-Prem

NOTE: Refer to the Before You Start section for information required for deploying SSM On-Prem.

After you boot the media, you will be presented with the *Kickstart Screen* that requires you to enter your initial configuration (such as what disk to assign before installation and enabling support for USB devices) before being able to install the SSM On-Prem. To complete this part of the deployment, you will need the following information:

- The server hostname you plan to use
- The security profile

NOTE: For standard security features, we recommend the standard profile. For more security, choose the DISA STIG profile. For more information about the system profiles, see Selecting a System Profile.

- Your IP Address information
- Netmask or Prefix that matches your network subnet
- Gateway IP Address
- DNS Server IP Address
- Your choice of a SSH Shell password (minimum of 15 characters using mixture of: upper case, lower case, number, and special character for example CiscoAdmin!2345).

Complete the following steps for installing an ISO image.

Step	Action
Step 1	Enter the following information requested on the Cisco SSM On-Prem Quick Start Installation UI:

Cisco Confidential

Step	Action
	• Setup Hostname • System Classification: The options are default Unclassified, Confidential, Secret, Top Secret. If you choose the option, this classification shows up on the console Message of the Day banner • FIPS 140-2 Mode: Not changeable
Step 2	Select System Profile to either: (See Selecting a System Profile for details.) • Standard Profile • DISA STIG Profile which enables the OS (AlmaLinux 9) to go into STIG Mode
Step 3	Enter **IPv4** and/or **IPv6** network values per your network environment. Required values are: • Address • Netmask / Prefix • Gateway
Step 4	Configure the **DNS**.
Step 5	Click **OK**.
Once the network settings are entered, you are now ready to complete the installation of SSM On-Prem. Proceed to step 8.	
Step 6	The Popup for **Configure System Password** displays. Enter a secure **Linux SSH password** for SHELL access. **NOTE**: This is different than the UI admin password. Please keep this password in a safe location as there is no password recovery option.
Step 7	Re-enter the **Password**.
Step 8	Click **OK**. The initial setup is now complete, wait for the installation to complete (approximately **10-15** mins) before opening the application.

NOTE: It is recommended that you dismount the ISO image from the system after installation and reboot the server. SSM On-Prem will automatically boot up on restart, and you can proceed to login to the web interface.

Cisco Confidential

Configuring Secondary Authentication systems

Configuring the On-Prem Server for LDAP Authentication

ATTENTION: LDAP has undergone a major change in version 8-202102 to allow for simpler and more complete integration into an organization's Access Management controls. On-Prem now only supports the addition of LDAP Groups being added to On-Prem, and not users. If you previously used On-Prem with LDAP Users being added directly to Accounts, before upgrading to v8-202102 you must create LDAP Groups and assign any existing users to groups to provide them access to On-Prem.

Configuring the On-Prem Server for TACACS+ from CLI

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

Complete these steps to configure your On-Prem server for TACACS+ authentication using the CLI.

NOTE: The tacacs_config command requires administrator (sudo) privilege to invoke it.

Step	Action
Step 1	Log into the CLI by typing the Linux administrator's command **ssh**. Then use the On-Prem-console command.
Step 2	Once in the On-Prem console to configure the TACACS+ server, type the command **tacacs_config**. and then, when prompted, enter in the **password**.
Step 4	Select option **#1** (server details) to configure the primary TACACS server. **NOTE**: To configure a secondary server, select **option #2** and complete steps 5-9 a second time. **NOTE**: Option **#5** (Enable/Disable TACACS provides a means of disabling a configured server (primary or secondary) without deleting the configuration. You can enable a disabled server by selecting **Option #5**. The server is enabled without having to reconfigure it. (Option #5 changes functionality according to the state of the server. If a server is disabled using Option #5, you can enable it by selecting Option #5 again.)
Step 5	Enter the **ip/hostname** (IP Address or Hostname) for the primary server.
Step 6	Enter the **shared secret** for connecting to the TACACS primary server. **NOTE**: When you create the shared secret, you cannot use these three characters. The system will give you an error message. • Space: " " • Hash sign: "#"

Cisco Confidential

Step	Action
	• Backslash: "\"
Step 7	Select the authentication method (PAP, CHAP, ASCII) for connecting to the TACACS primary server. Enter **yes** to proceed with the configuration process. **NOTE**: Once the configuration is confirmed, the configuration saved is successful. **NOTE**: At this point, you can select option **#3** to display the configuration parameters for the server.
Step 8	Next, select option **#4** (User management) for user management. **NOTE**: When you select option #4, a banner opens on the screen that Linux requires a local linux user account that matches the tacacs+ username for all required users.
Step 9	Next, select **option #1** (Add local TACACS users). You can add multiple users by separating each user with a **comma** (**,**). After entering all the users, press **Enter** to complete the user management process. To return back to the main menu, select **option #4** (back).
Step 10	When the configuration process has completed, select **option #6** to quit the on-prem console. Then you can logout of the On-Prem server. **NOTE**: At this point, you can log into the server as a TACACS user and access the functionality of On-Prem based on your authorization level, configured on TACACS server.
Step 11	If you are configured as a TACACS admin (privilege level 15) in the TACACS server, you can utilize all the functionality of on-prem. However, if you are configured as a normal TACACS user (privilege level < 15) in TACACS server, you can utilize the on-prem console functionality that does not require sudo permission.

Selecting a System Profile

SSM On-Prem provides two profiles.

- **Standard Profile**: You will be prompted with the default AlmaLinux shell with the option to use the On-Prem console. This profile provides the standard security features usually required by non-defense organizations. These features include:
  - Sha 256 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. LDAP forces correct configuration of the host, port, bind dn, and password. If these parameters are incorrect or not entered you will receive an error message.
  - Additional security features include:
    - Forcing the Administrator to update the system password during installation.
    - Disallow changing the admin password back to the default password.

Cisco Confidential

  - Adding/Deleting a User is now recorded in the Event Log.
  - Automatically logging Users out of the system when they have been idle for 10 minutes.

- **DISA STIG Profile**: When you ssh into the shell, you are placed into the white listed console which will prevent root access and limit you to using only the white listed console commands in the On-Prem console. Select this security profile at installation if STIG compliance is required. This profile selection enables security features required for Department of Defense security systems. In addition, the features enabled with this profile selection are compliant with Security Technical Implementation Guide) STIG standards. STIG features include:
  - Browser certs management where the browser certificate and framework are enabled. This feature allows the customer to import their own cert through the browser on their local directory.
  - Password management that allows the User to set password strength and password rest/recovery workflow. New tabs have been added in the Security Widget for setting password expiration parameters along with specific password settings to create greater password strength capability.
  - ADFS: OAuth ADFS adds OAuth Active Directory Federation Services support for LDAP.
  - Active directory (OAUTH2): Adds Active Directory Federation Services support in addition to Active Directory support to LDAP group import.

NOTE: SCP/WinSCP file transfer to SSM On- Prem is not possible in DISA STIG profile. You must use the SSM On-Prem console COPY command for copying **to/from** the SSM On-Prem console.

Post-Installation Configuration

After you have setup SSM On-Prem, the next step is to log into the SSM **On-Prem Web interface and complete the post installation steps**.

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

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

Login using the following credentials:

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

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

NOTE: For security reasons, you will be required to immediately change the **admin password** or disable the account after you create a new administrative local account. The password must meet complexity requirements with a minimum of 15

Cisco Confidential

characters consisting of an upper case, lower case, number, and special character. (For example: **CiscoAdmin!23456**.)

Initial Login Procedure

After initially logging into SSM On-Prem with your username and password, you will be prompted by a Wizard asking you to:

- Set the default language
- Reset your password
- Check your Common Name
- Review all your selections before logging into the application.

Complete these steps when you perform your initial login.

Step	Action
Step 1	Log into SSM On-Prem for the first time with your: • **Userid** • **Password** The Wizard opens asking you to select your default language. **NOTE**: At any point you can click **Back** to return to the previous page.
Step 2	Select the **default** language (English, French, Japanese, Chinese, Korean).
Step 3	Enter your **new password**.
Step 4	Confirm your **new password**.
Step 5	Enter or confirm your **Common Name**.
Step 6	Review your **changes**. If they are correct, click **Next**. The Wizard returns you to the Login screen. Where you can log into SSM On-Prem using your new password. If they are incorrect, click **Back**, you are returned to the previous screen.

Configuring the NTP Server

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.

Cisco Confidential

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 and perform these steps. a. Set the **Manually Set Time** switch to **On**. b. Select the **Date** (default is current date). c. Set the current time.
Step 4	If you want to Synchronize with an NTP Server, enable Synchronize with NTP Server by: a. Enable the **Synchronize with NTP Server** switch. b. For Server Address 1, enter a **valid IP Address** or fully qualified domain name (FQDN). c. Enter a valid **Port** for Port 1. d. (Optional) If you have a second NTP Server, enter the **IP Address** or **FQDN**, and **Port** for Server Address 2. **NOTE**: When you save the NTP server address configuration, SSM On-Prem checks to see if the IP Address is correct. If the system cannot connect to the Time Server 1, the server will stop checking and show an error for server 1 (in red). If an error is listed for server 1, SSM On-Prem will **not** check to see if it can connect to Server 2 even though it may be able to do so. Conversely, if the system can connect to Server 1, it will attempt to connect to Server 2 and if it cannot connect to it, it will send back an error for Server 2.
Step 5	To use NTP/Chrony Authentication for one or both servers, complete these steps: a. Enable **Use NTP/Chrony Authentication for Server 1** by sliding the selector to the right, then select the **NTP Key Type** from the drop-down list. The choices are: SHA1, SHA256, SHA384, SHA512. **NOTE**: For security reasons, it is strongly recommended that you select SHA256, SHA384, or SHA512. (SHA1 is no longer considered to be secure.) b. Enter a unique **Key ID** and **Key.** (If you use Hexadecimal keys, select the **HEX** check box.) **NOTE**: The tooltip provides information on what HEX values must be used for SHA1, SHA256, or SHA512 as well as the range for an ASCII Key.

Cisco Confidential

Step	Action
	NOTE: For multiple NTP/Chrony servers, use Server Address 2, Port 2, and if authentication is used, Key Type 2, Key ID 2, Key 2, for the second address.
Step 6	Click **Apply**. **NOTE**: Click **Reset** if you need to reset the time settings. **NOTE**: Synchronize Time Now is enabled after the configuration has been saved or upon loading the dialog, but it is usually unnecessary, since synchronization occurs when saving the NTP configuration parameters. In addition, like other NTP clients, the SSM On-Prem NTP client automatically polls the NTP server to maintain server time.

Registering a Local Account in SSM On-Prem

Once all installation and configuration steps are completed, You must next register SSM On-Prem to your Smart Account on Cisco Smart Software Manager (https://software.cisco.com) in order to synchronize and manage your Smart Licenses and devices on SSM On-Prem.

Since On-Prem synchronizes with your Smart Account at a Virtual Account level, a Local Account must exist or be created on SSM On-Prem, which maps to the Virtual Account on your Smart Account.

To complete this process, you will need the following:

- A Cisco Smart Account
- A valid CCO User ID and Password which has access to the Smart Account or Virtual Account.
- A Virtual Account (with no products currently registered to it)

First, complete these steps to register (request) a Local Account on SSM On-Prem.

Step	Action
Step 1	Navigate to the **SSM On-Prem Administration Workspace** **https://<ip-address>:8443/admin** **NOTE**: Where the IP-address is the value used during installation. If it is part of an HA cluster, this will be the virtual IP address.
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. Each Local Account must be associated to a unique Cisco Virtual account. The Cisco Virtual Account must not have a product, or another Local Account,

Cisco Confidential

Step	Action
	registered to it.
Step 4	Click **Submit**.
Step 5	The Account request then is listed on the **Account Requests** tab in the **Accounts Widget**.
Step 6	Approve the Local Account by following the procedure in the Approving a New Local Account.

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**.
Step 5	On the account Registration pop-up, verify the information present. **NOTE**: If the Cisco Smart Account, or Cisco Virtual Account is shown in Black text, they exist and can be used. If the Cisco Smart Account, or Cisco Virtual Account is shown in red text, it is not usable. Choose a new value from the dropdown, or manually type a new value. If the Cisco Virtual Account is shown in blue text, it does not exist at Cisco and will be

Cisco Confidential

Step	Action
	created.
Step 6	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 7	Verify that the Local Account is listed as **Active** under the **Accounts** tab.

Cisco Confidential

Local Account Approval (Manual Mode)

You can also manually register the Local Account to Cisco SSM (CSSM). 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 **NOTE**: You must have access to a Smart Account for this link to be functional.
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.

Cisco Confidential

Step	Action
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 13	In the On-Prem Accounts 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 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 your Smart Account on Cisco Smart Software Manager to retrieve the list of available licenses for use with the devices that will be connected to it.

Proceed to the **Synchronization Widget** and perform a synchronization. To perform a synch by clicking the Actions column and selecting Full Synch (for first time).

Cisco Confidential

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

Registering Product Instances

To register product instances to the SSM On-Prem, see "Registering Product Instances to On-Prem" 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)
    - Account Registration: cloudsso.cisco.com
  - cloudsso.cisco.com

Troubleshooting

The following five 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 Cisco Smart Software Manager
  - Logout and then log back into the Licensing workspace and your Local Account will show up on the upper right-hand side
- Cannot add a user
  - Verify that you have the appropriate authentication method configured in the Administration workspace
  - If you are using LDAP, Adding users is no longer permitted. To add a User, you must add the LDAP Group to the required level of permissions, and add the user to the LDAP Group using the existing method your company uses for adding users to Groups (Active Directory Users & Groups, or LDAP Add Users)

Cisco Confidential

- 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 (6.3 and later)
    - IPv4: 146.112.59.25
    - IPv6: 2a04:e4c7:fffe::4

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

Cisco Confidential

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 (6.3 and later)
    - IPv4: 146.112.59.25
    - IPv6: 2a04:e4c7:fffe::4
- Verify that the SSM On-Prem can reach the configured DNS server.
- Verify that the time on the SSM On-Prem is correct.

Appendix 1. Managing a High Availability (HA) Cluster in Your System

From SSM On-Prem v7 Release 201907, Cisco introduced High Availability allowing customers to run 2 SSM On-Prem servers in the form of an Active-Standby cluster.

Cisco Confidential

SSM On-Prem Enhanced High Availability support is provided by Pacemaker and Corosync. These applications are provided as part of the ISO package to simplify the installation and configuration of High Availability.

Prerequisites Needed for Deploying a High Availability Cluster

- Hostnames must be unique on each node of the high availability (HA) cluster. For example, Host 1 and Host 2. If the nodes have the same name, the HA deployment will fail! Use the On-Prem 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.

NOTE: The Host Common Name for HA Cluster must match the value that the user plans to use it for the product destination URL, either as the FQDN or the virtual IP address.

NOTE: It's important to first ensure SSM On-Prem is situated properly in your network before deploying the cluster. See Appendix 6. Resolving Network Conflicts Using the docker_network_config Command.

- The virtual IP Address must be **an unassigned** (not in use) **IP address**, because the IP address will be used as a floating IP address across the cluster.
- When deploying SSM On-Prem in a HA cluster, both nodes must be running the same version. Running HA across different versions of SSM On-Prem is not supported.
- Both nodes must have IP addresses on the same subnet and are accessible by each node. The Virtual IP address must also be unused and on the same subnet for the provisioning to be successful.
- The Private IP addresses in your network need to be unused and MUST be different than the physical IP's (Node IP Addresses).

Cisco Confidential

- In addition, because these addresses are only used for the SSH Tunnel between the nodes, they should not be routable. (See Using Private IP Addresses in an HA Cluster.)
- The standby server should be a **new**, **fresh installation** of SSM On-Prem (no data). Once the HA solution is deployed, the Active server data are replicated to the Standby server.
- You must configure NTP on both nodes before deploying HA.

Deploying the HA Cluster

(Updated for SSM On-Prem 8 Release 202006)

HA deployment is only conducted through the On-Prem CLI console using specific commands. For help commands, see the *Cisco Smart Software Manager On-Prem Console Guide* for more information. 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 Manager 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, ssh into the SSM On-Prem server and at the bash prompt issue the command <onprem-console> to open the console. scp/winscp to On-Prem server is not possible in DISA STIG profile. You must use the On-prem console COPY command for copying **to** the On-Prem Console as well as **from** the On-Prem console).

To facilitate the deployment of a HA Cluster, the process has been divided into three major steps (described below) with each step focusing on a specific phase of the deployment.

NOTE: In the deployment procedure the terms Active and Standby Server are used. In the teardown sequence the terms Primary and Secondary Node are used. Listed here is the Server/Node terminology:

Active server = Primary node

Standby server = Secondary node

NOTE: HA networks are only certified to use one Network Interface Card (NIC).

Cisco Confidential

Using Private IP in Your HA Cluster

When entering private IP Addresses in your HA cluster, please read this **Caution** statement.

CAUTION: Verify that the private addresses are **NOT** in use in your network. Verify this via a ping command on SSM On-Prem **prior to using the addresses**.

If the default IP addresses recommended for use on SSM On-Prem, are to be used, you must verify that they are not in use by using the ping command <-c>: Ping Count and <-t>: Ping timeout.)

Shown here is the expected result of the ping command verifying the proposed Private IP addresses are **NOT** in use.:

```
>> ping -c 5 -t 5 169.254.0.1
PING 169.254.0.1 (169.254.0.1) 56(84) bytes of data.
--- 169.254.0.1 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time
4000ms >>

>> ping -c 5 -t 5 169.254.0.2
PING 169.254.0.2 (169.254.0.2) 56(84) bytes of data.
--- 169.254.0.2 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time
4000ms >>
```

Sequence for Deploying a HA Cluster

Listed here are the three major steps in deploying an HA cluster. Each step is explained in detail in their own section.

Step 1: Focuses on generating keys for the Primary node. These keys are the User and Setup SSH keys that establish a secure channel of communication between the Primary and Secondary nodes.

Step 2: Focuses on the deployment of the Standby server.

Step 3: Focuses on the deployment of the Active server.

First Step: Generating User and Its SSH Keys

Complete the actions in Step 1 to generate the user named sshtunnel and ssh keys for establishing a secure channel of communication between the Primary and Secondary nodes (Active and Standby servers).

NOTE: It is recommended to take snapshots after the successful deployment when you are able to navigate between each node (IP address).

Cisco Confidential

Step	Action
Step 1	To enter into the console as an Administrator, `ssh` into the **Primary** node. **NOTE**: If you are in DISA STIG mode, you are placed in the On-Prem Console by default, but scp/winscp to On-Prem server is not possible in DISA STIG profile. Therefore, you must use the oprem console COPY command for copying **to** the On-Prem console as well as **from** the On-Prem console). If you are not in the DISA STIG mode, type this command to open the On-Prem console: **onprem-console**. Press **enter**. The console opens.

Step 2	To initiate the setup of the sshtunnel, type this command:
	ha_generatekeys
	Press **enter**.
	
	Next, there is a **prompt for your admin password** to continue.
	
	NOTE: This password provides you with the proper permission to execute ha_ commands such as ha_ generatekeys.
	
	NOTE: You can use special characters such as: !@#$%^&*()-=[];:",.<>?|
	
	You **cannot** use spaces in the HA cluster (sshtunnel) passwords.
	
	Type your **admin password**.
	Press **Enter**.
	
	Shown here is the ha_generatekeys command and the expected output.
	
	`>>ha_generatekeys`
	`==========`
	
	`This step will generate a user and setup SSH keys to be used to establish a secure channel of communication between the two nodes.`
	
	`This is step 1 of 3 for deploying a HA cluster.`
	
	`The password chosen here is temporary and used only during the HA setup process. Remember this password, as you will be asked for this same password several times during the setup of the HA cluster.`
	
	`==========`
	
	`Choose an HA cluster password: <HA Cluster Password>`
	
	NOTE: The **HA Cluster Password** is synonymous with the password for the **user sshtunnel**. The terms are used interchangeably as shown in the line below.
	
	`Changing password for user sshtunnel.`
	
	`passwd: all authentication tokens updated successfully.`
	
	`Generating SSH keys...`

Cisco Confidential

Step	Action
	Operating in CiscoSSL FIPS mode. SSH keys generated successfully.
Step 3	Once the generate keys command has completed, **exit out of the On-Prem shell,** and also exit out of the ssh session. **NOTE**: The authentication token is updated and the SSH keys are generated. You are now ready for the second step of the deployment process: Provisioning the standby server.

Second Step: Provisioning the Standby Server (Secondary Node)

The next part of the deployment process is to provision the Standby server (Secondary node).

Complete these actions to provision the Standby server.

Step	Action
Step 1	ssh into the **Standby** node to enter into the console as an Administrator. **NOTE**: If you are in DISA STIG mode, you are placed in the On-Prem console by default. If you are not in the DISA STIG mode, type this command to open the On-Prem console: **onprem-console**. Press **enter**. The console opens.
Step 2	To begin the provisioning process on the Standby node, type this command: **ha_provision_standby** and then press **Enter**.
Step 3	You are prompted to enter your **admin password**.
Step 4	Now, you are notified that you are on the second main step for deploying HA, and also reminded to make sure you have completed the first step that generated the user SSHTUNNEL's SSH keys (ha_generatekeys). Next, you are prompted to enter your **Active node IP address**, **Active node private IP address**, your **Standby node IP address**, and **Standby node private IP address**. Enter these IP addresses in the following order: (See notifications below.) a. Enter **<IP address>** for the active node IP address or accept the default. Refer to Private IP section for details.

Cisco Confidential

Step	Action

	b. Enter **<private IP address>** for the Active node private IP address.
	c. Enter **<IP address>** for the Standby node IP address or accept the default.
	d. Enter **<private IP address>** for the Standby private IP address.
	e. For the HA cluster password, enter your **HA Password** (**the user sshtunnel's password**).
	NOTE: When you update IP addresses in HA, you must enter both the Active and Standby IP addresses. IP addresses **do no**t automatically replicate for each node. You must manually update each IP address for each node.
	NOTE: All IP addresses used for HA must be the same IP version. A combination of IPv4 and IPv6 addresses is not permitted.
	Shown here is the ha_provision_standby command and the expected output.
	`>> ha_provision_standby`
	`[sudo] password for admin: <`**`admin password>`**
	`Last login: Thu Mar 26 19:28:43 UTC 2020 on pts/0`
	`==========`
	`Provision SSM On-Prem server as a standby node`
	`==========`
	`This procedure will convert a stand-alone SSM On-Prem server to act as the standby node in an HA environment. Proceeding will first destroy the current database in order to begin replication from the active node.`
	`IMPORTANT: This is step 2 of 3 for deploying HA. Please ensure that you have generated SSH keys on the primary node before running this step!`
	`ALL DATABASE DATA WILL BE WIPED ON THIS NODE UNTIL REPLICATION BEGINS!`
	`==========`
	`Enter IP address of the active node:` **`<active node physical IP address>`**
	`Enter the private IP address of the active node: [169.254.0.1]:` **`<private address used for the ssh tunnel only!>`**
	`Enter IP address of the standby node:` **`<standby node physical IP address>`**
	`Enter the private IP address of the standby node: [169.254.0.2]:` **`<private address used for the ssh tunnel only!>`**
	`Enter HA cluster password:` **`<HA Cluster Password used in ha_generate>`**

Cisco Confidential

Step	Action
	HA Secondary Node Setup Confirmation Active (other node): <active node physical IP> Private Active : <active node private address used for the ssh tunnel only!> Standby (this node): <Standby node physical IP address> Private Standby : <Standby node private IP address used for the ssh tunnel only!> HA Cluster Password : <**HA Cluster Password used in ha_generate**> !!! DO NOT ABORT THIS PROCESS AFTER PROCEEDING !!! You will be prompted another time for the HA Cluster Password (user sshtunnel password). Please enter the HA Cluster password that you set previously in the initial HA setup. Proceed with the above configuration? Enter 'yes' to continue: **<yes>** Provisioning machine as a secondary node for HA cluster... Establishing SSH tunnel for both nodes... Operating in CiscoSSL FIPS mode Changing password for HA Cluster (user sshtunnel). passwd: <HA Cluster Password used in ha_generate> all authentication tokens updated successfully. Operating in CiscoSSL FIPS mode sshtunnel@<standbyIP>'s password: Operating in CiscoSSL FIPS mode Last login: Thu Mar 26 19:31:46 UTC 2020 on pts/0

Cisco Confidential

Step	Action
	Verifying SSH access to <active node> IP address ... Operating in CiscoSSL FIPS mode Last login: Thu Mar 26 19:31:50 UTC 2020 on pts/0 OK Created symlink from /etc/systemd/system/multi-user.target.wants/tunha.service to /etc/systemd/system/tunha.service. Stopping services... Removed symlink /etc/systemd/system/multi-user.target.wants/satellite.service. Starting cluster... Created symlink from /etc/systemd/system/multi-user.target.wants/pcsd.service to /usr/lib/systemd/system/pcsd.service. Changing password for user hacluster. passwd: all authentication tokens updated successfully. Last login: Thu Mar 26 19:28:44 UTC 2020 on pts/0 Setting up for data replication... (active node: <IP Address>) 5d91258862f94a54e1836dc5db7c0c9499d863433d71701e2cf80aef3cbd97e9 Standby provisioning is complete! You may now proceed with HA deployment from the active node.
Step 5	After the provisioning completes, you are finished with the second main step.

Third Step: Deploying the Active Server (Primary Node)

Complete these steps to deploy the Active Server (Primary Node).

Step	Action
Step 1	ssh into the **Primary** node to enter into the console as an Administrator. **NOTE**: In if you are in DISA STIG mode, you are placed in the On-Prem console by default. If you are not in the DISA STIG mode, enter this command to open the On-Prem console: **On-Prem-console**. Press **enter**.

Cisco Confidential

Step	Action
	The console opens.
Step 2	To begin the provisioning process on the primary node, by typing this command: **ha_deploy** then press **Enter**.
Step 3	You are prompted to enter your **admin password**.

Step 4	Next, you are prompted to enter the following information in the following order:
	a. Enter **<IP address>** for the Active node IP address.
	Refer to Private IP section for details.
	b. Enter **<private ip address>** for the Active node private IP address or accept the default.
	c. Enter **< IP address>** for the Standby node IP address.
	d. Enter **<private IP address>** for the Standby private IP address or accept the default.
	e. For the HA cluster password, enter your **HA Password** (the user sshtunnel's password).
	NOTE: When you update IP addresses in HA, you must enter both the active and standby node IP addresses. IP addresses **do not** automatically replicate to each node. You must manually update each IP Address on each node.
	NOTE: All IP addresses used for HA must be the same IP version. A combination of IPv4 with IPv6 addresses is not permitted.
	f. You are prompted for another confirmation.
	Type **yes** and press **Enter**.
	Once you have pressed **Enter**, the deployment process begins.
	Let the deployment process run until it completes.
	NOTE: Wait at least **1 minute** before navigating to the IP address to ensure that all services are running.
	At the end of the provisioning process your Virtual IP address will show on the command line.
	You have completed the HA deployment process and are ready to use your HA cluster.
	Shown here is the ha_deploy command and the expected output.
	`>> ha_deploy`
	`[sudo] password for admin: <admin password>`
	`==========`
	`Deploy SSM On-Prem two-node HA cluster`

Cisco Confidential

Step	Action
	========== IMPORTANT: This is step 3 of 3 for deploying a HA cluster. Be sure that you have first provisioned the standby node before running this step. ========== Enter IP address of the active node: **<Active node physical IP address>** Enter the private IP address of the Active node: [169.254.0.1]: **<private address used for the SSH tunnel only!>** Enter IP address of the standby node: **<standby node physical IP>** Enter the private IP address of the standby node: [169.254.0.2]: **<private address used for the SSH tunnel only!>** Enter virtual IP address: **<Virtual IP Address>** Enter HA cluster password: **<HA Cluster password used in ha_generate> (the user sshtunnel's password)** Verifying SSH access to <Standby Node> ... Operating in CiscoSSL FIPS mode OK High Availability Setup Confirmation Active (other node): <Active node physical IP address> Private Active : <Active node private address used for the SSH tunnel only!> Standby (this node): <Standby node physical IP address> Private Standby : <Standby node private address used for the SSH tunnel only!> Virtual IP : <Virtual IP address> HA Password : <HA Cluster Password used in ha_generate> !!! DO NOT ABORT THIS PROCESS AFTER PROCEEDING !!! NOTICE: It is strongly recommended that you perform a backup of your database before proceeding. Please see the documentation for details.

Cisco Confidential

Step	Action
	Proceed with the above configuration? Enter 'yes' to continue: **<yes>** Deploying HA cluster... Removing password for HA Cluster (user sshtunnel). passwd: Success Operating in CiscoSSL FIPS mode Operating in CiscoSSL FIPS mode Last login: Thu Mar 26 19:32:08 UTC 2020 on pts/0 Running sshtunnel post-install... Removing password for HA Cluster (user sshtunnel). passwd: Success Starting secure tunnel... Created symlink from /etc/systemd/system/multi-user.target.wants/tunha.service to /etc/systemd/system/tunha.service. Created symlink from /etc/systemd/system/multi-user.target.wants/sshtunha.service to /etc/systemd/system/sshtunha.service. Stopping services... Removed symlink /etc/systemd/system/multi-user.target.wants/satellite.service. Created symlink from /etc/systemd/system/multi-user.target.wants/pcsd.service to /usr/lib/systemd/system/pcsd.service. Changing password for user hacluster. passwd: all authentication tokens updated successfully. Last login: Thu Mar 26 19:35:50 UTC 2020 on pts/1 Authenticating cluster user... secondary-node: Authorized primary-node: Authorized

Cisco Confidential

Step	Action
	Setting up cluster... 2287b3ebcc5fa498d3d9aeb3ada3f36a3328a3ea58dbdd933ee7b6c16789fe6a Destroying cluster on nodes: primary-node, secondary-node... secondary-node: Stopping Cluster (pacemaker)... primary-node: Stopping Cluster (pacemaker)... primary-node: Successfully destroyed cluster secondary-node: Successfully destroyed cluster Sending 'pacemaker_remote authkey' to 'primary-node', 'secondary-node' primary-node: successful distribution of the file 'pacemaker_remote authkey' secondary-node: successful distribution of the file 'pacemaker_remote authkey' Sending cluster config files to the nodes... primary-node: Succeeded secondary-node: Succeeded Starting cluster on nodes: primary-node, secondary-node... primary-node: Starting Cluster (corosync)... secondary-node: Starting Cluster (corosync)... secondary-node: Starting Cluster (pacemaker)... primary-node: Starting Cluster (pacemaker)... Synchronizing pcsd certificates on nodes primary-node, secondary-node... secondary-node: Success primary-node: Success Restarting pcsd on the nodes in order to reload the certificates... secondary-node: Success primary-node: Success Waiting for node(s) to start... primary-node: Started secondary-node: Started

Cisco Confidential

Step	Action
	Configuring cluster... Adding redis backend (kind: Mandatory) (Options: first-action=start then-action=start) Adding postgres_clone_data backend (kind: Mandatory) (Options: first-action=start then-action=start) Adding gobackend central_logger (kind: Mandatory) (Options: first-action=start then-action=start) Adding backend central_logger (kind: Mandatory) (Options: first-action=start then-action=start) Adding central_logger frontend (kind: Mandatory) (Options: first-action=start then-action=start) Adding frontend recovermaster (kind: Mandatory) (Options: first-action=start then-action=start) Adding frontend promotetomaster (kind: Mandatory) (Options: first-action=start then-action=start) Adding promotetomaster virtual_ip (kind: Mandatory) (Options: first-action=start then-action=start) Warning: Defaults do not apply to resources which override them with their own defined values primary-node: Cluster Enabled secondary-node: Cluster Enabled DB replication to secondary node complete. HA cluster deployment complete! You may now access SSM On-Prem using the virtual IP at https:// **<Virutal IP>** The deployment is complete.

CAUTION: When accessing the SSM On-Prem, always use the Virtual IP 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 nodes. In the event there is a loss of connectivity with the active node, an automatic failover occurs, and the standby node starts responding, enabling a non-disruptive recovery and continuous operation.

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

Cisco Confidential

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 *Console Help Commands in the Cisco Smart Software Manager On-Prem Console Reference Guide* 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 node. Until the initial data have finished replication across the nodes, the standby SSM On-Prem is unavailable.

NOTE: The Host Common Name for HA Cluster must match the value that the user plans to use it for the product destination URL, either as the FQDN or the virtual IP address.

Forced Failover of a High Availability Cluster

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

After a switchover occurs, the Standby is promoted to the Active On-Prem node and the degraded SSM On-Prem node 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>

NOTE: If you use the <ha_teardown> command, **you must use it on the Primary node first**. If you use the <ha_teardown> command first on the secondary node, it can cause a condition that will prevent the <ha_deploy> command from successfully completing.

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

Cisco Confidential

NOTE: Browser certificates are deleted when the HA teardown command is used. To restore the deleted certificate, you will need to upload the certificate again. See uploading deleted browser certificates after HA teardown for further information.

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

Appendix 2. Resolving Network Conflicts Using the docker_network_config Command

The default setting for SSM On-Prem is to allocate a subnet from a default address pool for the Docker network. This address pool is used for internal communication between the Docker Containers. For SSM On-Prem, the default address pool allocated is 172.16.2.0/24.

If this address range overlaps with your customer network, there can be unexpected routing issues that occur due to duplicate networks on incorrect routes. To guard against overlapping network issues, you can open the On-Prem console and use the <docker_network_config> command (see the *Cisco Smart Software Manager On-Prem Console Guide* for details on opening the On-Prem console and using this command). This command will assist you in changing the internal Docker network addresses used by the Docker Containers by showing an address range **not** used anywhere in your network.

How It Works

When you run the <docker_network_config> command, you are prompted to enter a network (range?) to be designated for SSM On-Prem internal communications.

For example, you should select a network range that supports a contiguous range of addresses defined with a /24 bit mask, for example 172.16.2.0/24 or 192.168.0.0/24.

For 172.16.2.0/24 pool, the addresses available for internal communications consist of 256 IP Addresses (with 253 usable addresses). Using the <docker_network_config> command will allow the internal Docker networking function to allocate appropriate addresses from this pool.

Appendix 3. Provisioning IPv4

You can customize your IPv4 routing using the on-prem console. Complete these steps to customize an existing IPv4 route.

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:

Cisco Confidential

Step	Action
	`onprem-console` **Hint**: You can use tab completion to complete the command.
Step 2	Once in the console, type "**?**" to open the help menu.
Step 3	Once in the help menu, type in this help command: **ha_network_manager** The NetworkManager TUI opens.
Step 4	Select **Edit a connection**. Press **Enter** to open the Ethernet screen. **HINT**: Use **Tab** to navigate through the screen and **Enter** to open a command.
Step 5	From the Ethernet screen, select the **Ethernet Connection** you want to edit.
Step 6	Tab to **Edit** and press **Enter**. The Edit Connection screen opens.
Step 7	Tab to **Routing <Edit...>** and press **Enter**.
Step 8	From this screen you can edit, add, or remove a connection. To add a connection, tab to **Add** and press **Enter**. Another connection line will open. When you add or edit an ethernet connection, you must configure the following fields: • Destination/Prefix • Next Hop • Metric
Step 9	Once you have finished adding or editing an ethernet connection, tab to **OK** and press **Enter**. The system saves the changes and you are returned to the Edit Connection screen. **NOTE**: You can select **Cancel** to return to the Edit Connection screen.
Step 10	After you have customized the appropriate connections, tab to **OK** and press **Enter**, you are returned to the Ethernet screen.
Step 11	To return to the NetworkManager TUI screen, tab to **Back** and press **Enter**.
Step 12	To quit the Network_Manager application, tab to **Quit** and press **Enter**. You are returned to the On-Prem-console.

Cisco Confidential