Cisco Smart Software Manager On-Prem Quick Start Installation Guide

Version 8 Release 202308

First Published: 02/16/2015
Last Modified: 10/27/2023

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, such as Java, 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

Smart Software Manager On-Prem Quick Start Installation

The following steps show the SSM On-Prem installation workflow for installing an ISO image.

Step	Action
Step 1	Download the **ISO image** from CCO.
Step 2	Deploy the **ISO** per your Orchestration Environment.
Step 3	Enter the following information requested on the Cisco SSM On-Prem Quick Start Installation UI: • 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 4	Select System Profile • Standard Profile • DISA STIG Profile which enables the OS (CentOS 7.5.1804) to go into STIG Mode
Step 5	Enter **IPv4** and/or **IPv6** network values per your network environment. Required values are: • Address • Subnet mask / Prefix • Gateway
Step 6	Configure the **DNS**.
Step 7	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 8	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 9	Re-enter the **Password**.
Step 10	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. The SSM On-Prem system automatically boots up.

Selecting a System Profile

SSM On-Prem provides two profiles.

- **Standard Profile**: You will be prompted with the default centos 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.
    - 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 whitelisted console which will prevent root access and limit you to using only the whitelisted console commands in the On-Prem console. Select this security profile at installation if STIP 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.