Cisco License On-Prem Installation Guide

Version 10 Release 202606

First Published: 6/2/2026
Last Modified: 6/2/2026

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

Table of Contents

Chapter 1 Purpose

This guide provides comprehensive step-by-step instructions for the initial deployment and boot-up configuration of Cisco License On-Prem. It is designed for IT administrators and technical personnel responsible for setting up the foundational infrastructure for Cisco License On-Prem, ensuring it is correctly installed and ready for subsequent application-level configuration.

Objectives

Upon completing this guide, you will be able to:

- Understand Pre-requisites
- Deploy Cisco License On-Prem
- Configure Initial System Settings
- Verify Basic Functionality
- Prepare for Next Steps

About Cisco License On-Prem

Cisco License 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 License-enabled product instances to Cisco Smart Software Manager hosted on cisco.com.

Chapter 2 Prepare your installation environment

Cisco License 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 requirements and prerequisites

Cisco License On-Prem application requirements

Cisco Smart Account access

Before you can perform any of the tasks described in the Cisco License On-Prem guide (such as configuring or managing licenses), you need to make sure you have access to your organization's Cisco Smart Account. This account is required for tasks like registering devices, managing licenses, and synchronizing license information between Cisco License Central and your local Cisco License On-Prem system.

Web browser requirements
To access Cisco License On-Prem:

- Use one of the supported browsers:
    - Chrome 137.0.7151.69 or later
    - Firefox 139.0.4 or later
    - Microsoft Edge 137.0.3296.68 or later
- Enable JavaScript in your browser

Restrictions related to third-party tools and applications

Caution:	Do not install any third-party tools or applications on the Cisco License On-Prem machine. The system is built to run in a controlled environment with only validated and optimized components to ensure stability, performance, and security. Installing unapproved software may: ○ Modify critical files, configurations, or dependencies. ○ Cause unexpected errors or system incompatibilities. ○ Prevent system recovery in case of failure. These issues could make it challenging or even impossible to diagnose and recover the system without complete re-installation, potentially resulting in downtime or loss of data. If additional functionality or tools are required, consult with the Cisco Licensing On-Prem support team to determine the best course of action while maintaining system integrity.

System limits and scalability

Product and user scalability:

- Up to 500 On-Prem Accounts
- Up to 1,000 Virtual Accounts
- Scales up to a total of 300,000 devices with a maximum capacity of 25,000 devices 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 is under heavy SL load, it may take about 6 hours for the system to relax and for the UI to be usable after the upgrade.

Supported installation modes

Cisco License On-Prem supports installation in the following modes. Use this table to determine the Cisco License On-Prem version required for each. Starting with Cisco License On-Prem release **10-202606**, installation is supported on **AMD-based CPUs** in addition to Intel-based processors.

Installation Mode	Platform Version	Supported Cisco License On-Prem version	Notes
VMware ESXi	8.0 Update 3	10-202606 and above	Secure Boot is not supported in ESXi 8 and above. It is advised to disable Secure Boot.
AWS	EC2 (latest supported)	10-202606 and above	
Azure	Latest supported	10-202606 and above	
Hyper-V	Windows Server 2022	10-202606 and above	
Nutanix	Version 7.0.x onwards NCC Version: 5.1.1 LCM Version: 3.2	10-202606 and above	
KVM (Ubuntu-based)	ubuntu-24.04.desktop-amd64.iso.	10-202606 and above	
KVM (RHEL-based)	rhel-9.6-x86_64-dvd.iso	10-202606 and above	
OpneShift Virtualization	UCS M7	10-202606 and above	

Virtual Machine-based deployment requirements

Refer to the Supported installation modes section to identify the Cisco License On-Prem version required for VMware deployment.

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 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 on 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 Cisco License On-Prem " section of the *Cisco License On-Prem User Guide*)
- Perform a new Cisco License 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 Cisco License On-Prem " section of the *Cisco License On-Prem User Guide*)
- Shut down the Cisco License On-Prem with the older version.

Capacity limitations

Deployment (Devices)	Small (SL and SLP*)	Medium (SL and SLP*)	Large (SL and SLP*)	Maximum (SL Only)
Products	100,000	150,000	500,000	700,000
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

* SLP devices with Smart agent version 5.3 and above

Cisco License On-Prem deployment scenarios

Deployment Scale	Total Supported Devices	Sample Tenant Configuration
Small	100,000 **Total Device Mix:** 80,000 SL & 20,000 SLP*	Up to 17,000 devices per tenant, for 6 tenants. **Per-Tenant Mix**: Approx. 13,000 SL & 3,300 SLP*
Medium	150,000 **Total Device Mix:** 115,000 SL & 37,000 SLP*	Up to 25,000 devices per tenant, for 6 tenants. **Per-Tenant Mix:** Approx. 19,000 SL & 6,000 SLP*
Large	500,000 **Total Device Mix:** 375,000 SL & 125,000 SLP*	Up to 83,000 devices per tenant, for 6 tenants. **Per-Tenant Mix:** Approx. 62,500 SL & 20,500 SLP*

**SLP devices require Smart Agent version 5.3 or higher.*

Note: The deployment scale metrics provided reflect Device-to-CLP performance. Comprehensive end-to-end scalability data, including CLP-to-CLC throughput, is currently undergoing validation and will be available in an upcoming update.

Supported VMware features and operations

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

- UEFI
- BIOS

Cisco License On-Prem supports **only UEFI mode for installation**, BIOS mode is a legacy option and is not supported. For UEFI installation, the 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 Cisco License On-Prem, but may still be used or performed on non-supported versions, though doing so risks encountering dropped packets, dropped connections, and other error statistics.:

- Cloning
- Migration

Chapter 3 Install and deploying Cisco License On-Prem

Overview of fresh installation sequence

This Installation Guide provides end-to-end instructions for deploying the Cisco License On-Prem application. Its sole focus is on the system-level setup, from initial planning to verifying that the application is online and accessible.

This guide is structured into four distinct phases to walk you through the entire deployment. Upon completion, you will have a fully installed and running Cisco License On-Prem instance, ready for the application-level configuration detailed in the *Cisco License On-Prem User Guide*.

Installation Phases

1. **Preparation and Planning:** This initial phase ensures you have all the necessary software, information, and resources before starting the technical deployment. Key actions include downloading the correct .iso file and gathering essential network details (IP, DNS, NTP).
2. **Platform Deployment and OS Installation:** In this phase, you will create the virtual machine (or cloud instance) and install the Cisco License On-Prem operating system by booting from the downloaded .iso file.
3. **Initial System Configuration (Kickstart):** This critical, one-time configuration step sets the system's identity and network connectivity through the console. You will configure the hostname, network parameters, and a secure SSH password.
4. **System Verification and Final Hand-off:** The final phase of installation involves verifying that the system is online and accessible, confirming successful deployment. This ensures the instance is ready for the next stage of configuration.

1. Preparation and planning

Cisco License On-Prem (Enhanced Edition 9-202510 and later) has a new architecture and completely new user interface from previous versions.

(Refer to the *Cisco License On-Prem User Guide* to understand how the new system architecture, user interface, accounts, setup, and operations have changed.)

Before you begin

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

1. Download 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 a 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 successful installation.

Cisco License On-Prem deployment and activation workflow

To ensure a successful deployment, you must complete the following five phases in the specified order. The first two phases are covered in detail within this **Installation Guide**, while the subsequent application-level setup is covered in the **Cisco License On-Prem User Guide**.

1. **Install the Cisco License On-Prem application:** This is the foundational step where the Cisco License On-Prem software is deployed onto your chosen platform. This guide provides detailed, platform-specific instructions for installing the application using the .iso file on VMware ESXi.
2. **Perform initial system configuration:** Immediately following the installation, you will perform a one-time system configuration via the console. This involves:
    a. Configure the Common Name on Cisco License On-Prem (**Security Widget > Certificates**).
    b. Synchronize the NTP server (**Settings Widget > Time Settings**).

Note: This concludes the steps covered in this *Installation Guide.* For all subsequent steps, refer to the *Cisco License On-Prem User Guide.*

3. **Perform initial application setup (GUI):** Log in to the Cisco License On-Prem web interface for the first time to complete the initial application setup. This includes:
    - changing the default administrator password,
    - verifying the Common Name, and
    - configuring the NTP server to ensure correct time synchronization.
4. **Register and approve a Local Account:** Create a new On-Prem Account within Cisco License On-Prem. This account must then be approved and registered to establish the connection between your on-premises instance and your corresponding Cisco Smart Account and Virtual Account on Cisco.com.
5. **Synchronize with Cisco.com:** Perform a full synchronization for the newly registered account. This critical step downloads all your purchased license entitlements from the Cisco Smart Software Manager cloud to your local Cisco License On-Prem instance, making them available for your products.

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

2. Platform-specific installation procedures

Download and Prepare the Cisco License On-Prem Installation Package

Before proceeding with any environment-specific installation, follow these steps to obtain and prepare the necessary software.

Download and prepare the software

Download the installation package

Step	Action
Step 1	Navigate to the Cisco Software Download page.

Step 2	Search for **Smart Software Manager**.
Step 3	Under the latest release, download the appropriate file for a new installation: • Cisco License On-Prem-[version].iso: The direct installation image. • Cisco License On-Prem-[version]_Full.zip: A package containing the install file, upgrade file, and documentation.
Step 4	**Prepare the ISO File** • If you downloaded the .zip file, extract the Cisco License On-Prem-[version].iso file from the archive. • Copy the .iso software package to a VMware Datastore accessible by your ESXi host.

Manually installing on a VM using the .iso file (VMware ESXi)

While the following procedure provides general guidance for deploying Cisco License 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.

This section is structured into three clear stages to walk you through the installations: **Preparation**, **VM Creation**, and **Hardware Configuration and Finalization**.

Preparation

Download and Prepare the Cisco License On-Prem Installation Package:

- Before proceeding, ensure you have downloaded and prepared the Cisco License On-Prem installation package as described in the "Download and Prepare the Cisco License On-Prem Installation Package" section above.
- For VMware, ensure the .iso software package is copied to a VMware Datastore accessible by your ESXi host.

Create the new Virtual Machine

Launch the New VM Wizard

Step	Action
Step 1	Log in to vSphere and navigate to **VMs and Templates**.
Step 2	Right-click your target folder and select **New Virtual Machine**.
Step 3	Follow the wizard prompts to: • Enter a **Name** for the virtual machine. • Select a compute resource and storage location.

Configure compatibility and guest OS

Step	Action
Step 1	On the Compatibility screen, select **ESXi 8.0 update 3 or later**.
Step 2	On the Guest OS screen, configure the following: • Guest OS Family: Linux • Guest OS Version: Other 5.x or later Linux (64-bit) (If unavailable, choose the next highest available 64-bit version, such as 4.x).

Hardware configuration and finalization

Customize hardware settings

Step	Action
Step 1	On the **Customize Hardware** screen, configure the virtual machine resources according to the disk size based on your deployment size. (These values are for a **small** deployment.)

Component	Setting
vCPU	4 vCPU. Configure as 4 sockets with 1 core per socket.
Memory	16 GB
Hard Disk 1	250 GB. Ensure the provisioning is set to Thin Provision
Network Adapter 1	Adapter Type: VMXNET 3 (or E1000) **Configuration:** Check Connect at Power On.
CD/DVD Drive 1	Select Datastore ISO File, browse to the .iso file you uploaded, and check Connect at Power On.
VM Options > Boot Options	Firmware: EFI **Note**: For ESXi 8.0 and above, you must disable Secure Boot.

NOTE: Memory and disk requirements vary based on deployment size. Refer to Capacity limitations section to determine the appropriate values.

Step 2	Review the configuration on the summary screen.
Step 3	Click Finish to create the virtual machine.
Step 4	Power on the newly created VM. The system will boot from the attached .iso file and launch the Cisco License On-Prem Kickstart installer.

Manually installing on a VM using the .iso file (Hyper-V)

While the following procedure provides general guidance for deploying Cisco License On-Prem, the exact steps may vary depending on your Hyper-V environment and configuration. The steps and screens in this procedure are based on supported versions of Hyper-V (see Supported Installation Modes for supported versions). For specific installation steps for your Hyper-V deployment, refer to the Hyper-V user guide.

This section is structured into three clear stages to walk you through the installations: **Preparation**, **VM Creation**, and **Hardware Configuration and Finalization**.

Preparation

Prerequisites

Ensure that your Hyper-V host is provisioned with these resources before beginning installation:

- Cisco License On-Prem ISO
- Windows Server 2022
- Minimum of 6 vCPUs for the Hyper-V host

Download and Prepare the Cisco License On-Prem Installation Package:

- Before proceeding, ensure you have downloaded and prepared the Cisco License On-Prem installation package as described in the "Download and Prepare the Cisco License On-Prem Installation Package" section above.

Create the new Virtual Machine

Launch the New VM Wizard

Step	Action
Step 1	Launch Hyper-V Manager on your Windows server.
Step 2	In the Actions pane on the right, select New > Virtual Machine.
Step 3	You should see the New Virtual Machine Wizard screen. Enter a Name for the virtual machine (VM) then click Next.

Configure compatibility and guest OS

Step	Action
Step 1	On the Specify Generation screen, select Generation 1, and then click Next.
Step 2	On the Assign Memory screen, enter the memory value based on your deployment size. Caution: Do not select the Use Dynamic Memory for this virtual machine check box. Enabling this option may affect overall system performance.
Step 3	On the Configure Networking screen, select the appropriate connection method, then click Next.
Step 4	On the Connect Virtual Hard Disk screen, select Create a virtual hard disk. Set the disk size based on your deployment size. Note: Memory and disk requirements vary based on deployment size. Refer to Capacity limitations section to determine the appropriate values.
Step 5	On the Installation Options screen: • Select Install an operating system from a bootable CD/DVD-ROM. • Choose Image file (.iso). • Browse and select the Cisco License On-Prem ISO file. • Click Next.
Step 6	Review the configuration summary, and then click Finish.

Hardware Configuration and Finalization

Customize hardware settings and finalize VM creation

Step	Action
Step 1	In Hyper-V Manager, select the newly created VM.
Step 2	In the Actions pane, click Start.
Step 3	Double-click the VM to launch the console.
Step 4	Follow the on-screen instructions to complete the Cisco License On-Prem installation. Wait for the installation to be completed. This process typically takes 10 – 15 minutes.

System verification and initial access

Step	Action
Step 1	After installation, open a terminal and run the following command to check the docker status: `docker ps` If no containers are running, execute: `systemctl restart satellite` Run the command `docker ps` again to verify the container status.
Step 2	Confirm that all containers are up and running.
Step 3	Open a web browser and enter the application URL to verify that the UI is accessible.

Installing on a VM using the .iso file (Nutanix)

While the following procedure provides general guidance for deploying Cisco License On-Prem, the exact steps may vary depending on your Nutanix environment and configuration. The steps and screens in this procedure are based on supported versions of Nutanix (see Supported Installation Modes for supported versions).

This section is structured into three clear stages to walk you through the installations: Preparation, VM Creation, and Hardware Configuration and Finalization.

Preparation

Prerequisites

Ensure that your Nutanix environment meets these requirements before beginning installation:

- Cisco License On-Prem ISO
- Nutanix Platform Version 7.0.1
- NCC Version: 5.1.1
- LCM Version: 3.2

Download and Prepare the Cisco License On-Prem Installation Package

Before proceeding, ensure you have downloaded and prepared the Cisco License On-Prem installation package as described in the "Download and Prepare the Cisco License On-Prem Installation Package" section above.

Upload the ISO Image to Nutanix

Step	Action
Step 1	Navigate to the Nutanix UI. Enter your CEC email address (not just username) and CEC password.
Step 2	**Upload the ISO Image:** • From the top navigation banner, click Home. • Click Settings > Image Configuration. • Click Upload Image. • Enter the required details, select the Cisco License On-Prem ISO file, and click Save. • Wait for the ISO image to upload. This may take up to 45 minutes.

VM Creation

Launch the New VM Wizard

Step	Action
Step 1	After the upload completes, begin the VM creation process. In the left panel, click **VM**.
Step 2	On the General Configuration, Enter the required VM details. **Note:** Memory and disk requirements vary based on deployment size. Refer to Capacity limitations section to determine the appropriate values.

Configure settings

Step	Action
Step 1	To update Disks, follow these steps: • Click the pencil icon to edit the disk configuration. • Set the Operation field to Clone from the Image Service. • In the Image field, select the uploaded ISO. • Click Update to confirm changes.
Step 2	Click Add New Disk and enter the logical disk size as per deployment needs.
Step 3	Click **Add New NIC** to add a network interface.
Step 4	Select the network from the drop-down list. Click **Save**. A toast message will confirm that the VM creation process has started.
Step 5	Locate the newly created VM under Recent Tasks.

	Open the VM. Scroll down to the VM details section. (This is typically where the VM power button and console options are displayed.)

Hardware Configuration and Finalization

Power-On and Launch Console

Step	Action
Step 1	Click Power On to start the VM.
Step 2	Once the VM is running, click Launch Console.
Step 3	Follow the on-screen prompts to continue the installation and wait for the installation to complete.

Deploying Cisco License On-Prem on KVM (RHEL and Ubuntu based)

While the following procedure provides general guidance for deploying Cisco License On-Prem, the exact steps may vary depending on your KVM environment and configuration. The steps and screens in this procedure are based on supported versions of KVM (see Supported Installation Modes for supported versions).

Prerequisites:

1. Cisco License On-Prem ISO
2. KVM

- RHEL based Platform Version - rhel-9.6-x86_64-dvd.iso
- Ubuntu based Platform Version - ubuntu-24.04.desktop-amd64.iso.

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 **9-2026041**, and select the appropriate version: SSM_On-Prem-9-202601.iso Used to perform a new install of the SSM On-Prem license server. SSM_On-Prem-9-202601_Full.zip Contains the install file, the upgrade file, and all documentation relevant to this version of the SSM On-Prem license server.
Step 4	Sign in to the **KVM either on RHEL or Ubuntu.**

Step	Action
	Open the Applications menu on the RHEL host and search for Virtual Machine Manager. Launch the application.
Step 5	Verify that the Virtual Machine Manager window opens and displays the local QEMU/KVM connection.
Step 6	Click Create a new virtual machine
Step 7	Select Local install media (ISO image or CD-ROM). Click Forward.
Step 8	Click Browse and select the SSM On-Prem ISO file (for example: 9-202507). Click Forward.
Step 9	Enter the required values for: • Memory (RAM) • CPUs (minimum 4 CPUs) • Click Forward.
	Note: Memory and disk requirements vary based on deployment size. Refer to Capacity limitations section to determine the appropriate values.
Step 10	Set the disk size to 250 GB. Click Forward.
Step 11	Verify the virtual machine configuration details. Click Finish to create the virtual machine.
Step 12	• Allow the virtual machine to boot automatically from the ISO file. • Wait for the installer screen to appear. • Allow the installation process to continue without interruption. • Wait for the installation to complete. • The process takes approximately 10–15 minutes.
Step 13	After installation completes, open the VM terminal and run: • `docker ps` • If no containers are running, execute: • `systemctl restart satellite` • Run `docker ps` again and verify that all containers are running.
Step 14	Confirm that the system is running and ready for access.

Deploying Cisco License On-Prem on Openshift Virtualization

This section describes the procedure to deploy Cisco License On-Prem on Openshift virtualization. The deployment process uses a guided wizard that allows users to configure all necessary parameters, including compute, networking, and storage options.

Before you begin

Be sure that:

- OpenShift ISO and pull secret are available
- UCS M7 (or equivalent) with:

1. Minimum 64 CPU cores
2. Minimum 512 GB RAM
3. 1 TB SSD and 1 TB NVMe

- DHCP-enabled network with available IP pool
- No additional virtualization layer

Deployment

Step	Action
Step 1	Go to Red Hat OpenShift Virtualization Assisted Installer and select **Disconnected** / **Air-gapped environment**. Download • OpenShift Virtualization ISO image • Pull secret
Step 2	**Prepare host system** • Log in to the UCS server and launch the KVM console. • Mount a Linux ISO (for example, Fedora). • Restart the system. • Press F6 and boot from the mounted ISO. • Install the Linux OS on the host.
Step 3	**Configure networking** • Assign a static IP to the host. • Configure bridge networking. • Set up a DHCP server for cluster communication.
Step 4	**Set up virtualization on host** • Install and configure KVM. • Mount NVMe storage for distributed storage. • Copy OpenShift Virtualization ISO to the host
Step 5	**Create OpenShift Virtualization nodes (VMs)** Create the following VMs: • 1 agent node (rendezvous node) • 3 control plane nodes **For agent node** • Boot the VM using OpenShift Virtualization ISO. • Add kernel parameter: `console=ttyS0`

Step	Action
	• Wait for DHCP assignment. • Select Rendezvous node. • Assign the detected IP. **For control plane nodes** • Boot each VM. • Enter the rendezvous node IP. • Save and continue.
Step 6	Be sure that all VMs are running and confirm all nodes appear in Ready state in installer UI.
Step 7	**Install OpenShift Virtualization cluster** 1. Open the installer UI from browser. 2. Enter: • Cluster name • Domain • Pull secret 3. Select Virtualization Operator 4. Assign roles: All nodes → Control Plane 5. Verify storage is attached and ready. 6. Configure networking: • API IP • Ingress IP 7. Download: • `Kubeconfig` • `kubeadmin-password` 8. Click Install Cluster.
Step 8	**Manage node reboots** 1. Monitor node states. 2. When nodes shut down, restart manually: `virsh start <vm-name>` 3. Repeat until installation completes.
Step 9	**Access OpenShift Virtualization cluster** Choose one method: Option 1: DNS • Add required DNS records Option 2: Local hosts file

Step	Action
	• Update `/etc/hosts` • Access UI: https://console-openshift-console.apps.<cluster-domain>
Step 10	**Install required tools** Install: • `Kubectl/oc` • `Virtctl` Place `kubeconfig` in: `~/ .kube/`
Step 11	Enable connectivity to Red Hat console. Apply required cluster configuration updates.
Step 12	Navigate to **Virtualization** > **Settings** Disable Automatic image download.
Step 13	**To install storage (ODF)** 1. Navigate to Operators > OperatorHub 2. Install OpenShift Virtualization Data Foundation. 3. Create a Storage System. 4. Verify storage classes are available.
Step 14	**To create project for SSM On-Prem** **1.** Navigate to: **Home > Projects** 2. Create a new project (for example: ssm-onprem-kubevirt). **3. Set context:** **`oc project <project-name>`**
Step 15	**Upload SSM On-Prem ISO** **1.** Navigate to **Virtualization > Bootable Volumes** 2. Upload ISO. 3. Verify it appears under PersistentVolumeClaims.
Step 16	**Create VM template** **1.** Navigate to: Virtualization > Templates **2.** Create a template using YAML.
Step 17	**Deploy SSM On-Prem VM** **1.** Navigate to: Virtualization > Virtual Machines **2.** Create VM using the template. **3.** Attach the uploaded ISO.

Step	Action
	4. Start the VM.
Step 18	**Install SSM On-Prem** 1. Open VM console. 2. Complete installation. 3. Power off VM after installation. 4. Detach boot ISO.
Step 19	**Configure VM networking** 1. Log in to VM console. 2. Configure network interface for OpenShift-managed networking. 3. Restart the VM.
Step 20	**Configure external access (MetalLB)** 1. Install MetalLB Operator: Operators > OperatorHub 2. Create: • IP address pool • L2 advertisement • MetalLB instance 3. Create a LoadBalancer Service.
Step 21	**Access SSM On-Prem** • Get assigned external IP from: Networking > Services • Open the IP in browser.

Deploying Cisco License On-Prem on AWS

This section provides instructions for deploying Cisco License On-Prem on Amazon Web Services (AWS).

Prerequisites

Before starting the deployment, ensure you have:

- **AWS Account**: An active AWS account with permissions to manage EC2 instances, S3 buckets, and create Amazon Machine Images (AMIs).
- **AWS Command Line Interface (CLI)**: Installed and configured on your local machine. Refer to the AWS CLI User Guide for installation and configuration instructions.

Deployment

Follow the step-by-step instructions:

Step	Action

Step 1	**Launch an EC2 Instance Using the AMI**
	• In the AWS Management Console, navigate to the EC2 service.
	• Click **Launch Instance** and select you AMI from this link.
	• Choose an appropriate instance type based on your performance requirements (For more details refer to "Capacity Limitation" Section).
	• Configure instance details:
	  ○ Set the **Number of Instances** to **2** (for HA configurations; 1 for standalone deployment).
	  ○ Assign the instances to an appropriate VPC and subnet.
	  ○ Enable a public IP if external access is required.
	• Configure storage and add tags to identify the instances as "Primary" and "Standby" (for HA).
	• Configure the security group rules to allow inbound traffic on:
	  ○ Port **8443** for HTTPS access to the Cisco License On-Prem web interface.
	  ○ Port **22** for SSH access (if required).
	• Review and launch the instances.

Step 2	**Access the Cisco License On-Prem Web Interface** • Once the instance is running, obtain its public DNS or IP address. • Open a web browser and navigate to: `https://<instance-public-dns-or-ip>:8443/` • Proceed with the initial configuration as prompted.

To deploy High Availability Configuration for AWS, click here.

Deploying Cisco License On-Prem on Azure

This section describes the procedure to deploy Cisco License On-Prem on Microsoft Azure on Azure Marketplace. The deployment process uses a guided wizard that allows users to configure all necessary parameters, including compute, networking, and storage options.

Deployment

Step	Action
Step 1	Go to the **Microsoft Azure Marketplace**.
Step 2	Click **Get it now.**

Step	Action
Step 3	Confirm your plan Cisco License On-Prem. Select **Get it now**
Step 4	Confirm your subscription and plan. Click **Create.**
Step 5	Follow On-screen instructions and complete all configuration tabs (**Basics, Discs, Networking, Management, Monitoring, and Advanced)** according to your deployment requirements.
Step 6	Click **Review + Create** to initiate the deployment.

To deploy High Availability Configuration for Azure, click here.

3. Initial system configuration (Kickstart Screen)

After you have set up Cisco License On-Prem, the next step is to log into the Cisco License On-Prem **Web interface and complete the post-installation steps**.

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

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

Log in using the following credentials:

- Admin User id: **admin**
- Admin Initial Password: **CiscoAdmin!2345**

You will be prompted to **type in a new password** for the admin and then asked to log in 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 characters consisting of an upper case, lower case, number, and special character.

4. System verification and final hand-off

The final phase of installation involves verifying that the system is online and accessible, confirming successful deployment. This ensures the instance is ready for the next stage of configuration.

- **Dismount ISO and reboot:** It is recommended that you dismount the ISO image from the system after installation and reboot the server. Cisco License On-Prem will automatically boot up on restart.
- **Verify docker status (recommended for all VM installs):** After the system has restarted, open a terminal and run the following command:
  - To check the docker status: `docker ps`
  - If no containers are running, execute:
    systemctl restart satellite.
  - Run `docker ps` again to verify the container status.
  - Confirm that all containers are up and running.

- **Access web interface:** Open a web browser and enter the application URL to verify that the UI is accessible. The URL will be https://<VM_IP_Address>:8443/.

The system is now ready for the post-installation configuration steps detailed in the next section.

Overview of upgrading to Cisco License On-Prem

This section outlines the process for upgrading an existing Cisco License On-Prem system to a newer version. The upgrade process is designed to retain existing licenses, devices, and configuration data.

Preparing to upgrade a Cisco License On-Prem System

Upgrading your Cisco License On-Prem system is an important process that ensures your deployment remains secure, reliable, and benefits from the latest features and fixes. This section guides you through the necessary preparations to ensure a smooth upgrade experience, including obtaining the correct upgrade files and reviewing critical pre-upgrade considerations.

Before you begin

- The upgrade / migrate from Cisco Smart Software Manager (SSM) On-Prem to Cisco License Portal is supported by below versions.

Direct Upgrade from SSM On-Prem	Direct Migrate from SSM On-Prem
9-202601	8-202404 (*Refer to Cisco License On-Prem Migration Guide).*
9-202510	

  Note: If you are using an earlier Cisco Smart Software Manager On-Prem (SSM On-Prem) version, first upgrade to one of the supported versions listed in the table before you upgrade or migrate to Cisco License On-Prem.

- Before performing an upgrade, you have a backup of your database (if you are using a VM). (refer to Manage backup and restoration from Cisco License On-Prem User Guide)
- If an account requires re-registration, complete the re-registration before you upgrade from Cisco Smart Software Manager On-Prem (SSM On-Prem) to Cisco License On-Prem (CLP). During the upgrade, accounts that require re-registration may not be retained.
- Make sure to upgrade to the latest version to have new features and fix a few critical issues and security vulnerabilities.
- After performing an upgrade, the browser pages might not reflect the latest changes. Clear your browser's cache so that your browser pages are up to date.

Note: As part of the Cisco License On-Prem upgrade, stale data is cleaned up from older releases. This process might take several hours, Cisco License On-Prem upgrade will not be complete until this clean-up is complete. SSH session will be timed out, you will be logged out of the terminal and On-Prem won't respond (both GUI port and product port) until the upgrade completes.

Procedure

Step	Action

Step 1	Navigate to: software.cisco.com/download/home.
Step 2	In the Select a Product field, enter Smart Software Manager satellite.
Step 3	On the Latest Release panel (left column), select the appropriate version based on your current deployment then click the Download Icon located on the right side of the screen.
Step 4	When the download is complete, navigate to the directory where the zip file resides right-click the file and select unzip image.

Upgrade Procedure for Standalone Systems

Once the preparation steps are complete and you have obtained the necessary upgrade files, you are ready to proceed with upgrading your Cisco License On-Prem system. This section provides step-by-step instructions for performing the upgrade through the On-Prem Console, ensuring minimal disruption and successful completion of the process.

Procedure

Step	Action
Step 1	Complete the steps in "Preparing to upgrade an Cisco License On-Prem system" to obtain the files needed for upgrading the On-Prem server.
Step 2	Using Linux 'ssh' command connect to the On-Prem server as admin: `ssh admin@<your ip address>`
Step 3	Start the On-Prem Console using this command: **`onprem-console`**

Step 4	In the On-Prem Console, use the copy command shown in these two examples.
	NOTE: You can only use the on-prem copy command when you are in the on-prem console itself. The on-prem copy command copies files **from** a remote host **to** your local on-prem machine and only works with the SCP protocol.
	`copy <your username>@<your remote host.com>:/path/CLP-9-202510_Upgrade.sh patches:`
	
	`copy <your username>@<your remote host.com>:/path/CLP-9-202510_Upgrade.sh.sha256 patches:`
	Here is a specific example of the copy command:
	`copy user@domain.com:/path/CLP-9-202510_Upgrade.sh patches:`
	Note: For more information about the copy command, see the *Cisco Smart Software Manager On-Prem Console Reference Guide*.

Step 5	After the copy command, use this upgrade command: `upgrade patches:CLP-On-Prem-10-202510_Upgrade.sh` You are required to have an existing corresponding signature file.
Step 6	After the system has completed the upgrade (approximately 5-15 minutes), you are notified that the process is complete.
Step 7	After the Cisco License On-Prem upgrade is complete, **perform a synchronization** on the system. **Note:** After performing an upgrade, your browser's pages might not reflect the latest changes. Clear your browser's cache so that your browser's pages are up to date.

Post Upgrade Configuration

After upgrading from a supported Cisco Smart Software Manager (SSM) On-Prem release, the user interface is updated to the Cisco License On-Prem UI.

After the upgrade is complete, perform the post-upgrade configuration steps.

Step	Action
Step 1	Access the Cisco License On-Prem.
Step 2	Authenticate using your administrator credentials.
Step 3	Complete the one-time authentication process when prompted.
Step 4	Review and confirm the following system information: • Hostname • Network settings • DNS settings • NTP configuration Verify the system profile: • Standard Profile • DISA STIG Profile

Step 5	Perform synchronization by navigating to **Admin Workspace> Synchronization > On-Prem Accounts.** *(Refer to Synchronization settings section from Cisco License On-Prem User Guide)*
Step 6	Schedule the synchronization by navigating to **Admin Workspace > Synchronization >** Select **Schedule sync.** *(Refer to Synchronization settings section from Cisco License On-Prem User Guide)*

Chapter 4 Post-installation configuration of Cisco License On-Prem

Essential system configuration

After booting the media, you will be presented with the Kickstart Screen for initial configuration.

1. **Enter information:**
    - Setup Hostname: The server hostname you plan to use.
    - System Classification: Default Unclassified, Confidential, Secret, or Top Secret.
    - FIPS 140-2 Mode: Not changeable.
2. **Select system profile:** Choose either Standard Profile or DISA STIG Profile.
    - **Standard profile:** Provides standard security features (Sha 256 signing, LDAP Secure, password management, idle timeout).
    - **DISA STIG profile:** Enables STIG compliance features, restricts CLI access to a white-listed console.

    NOTE: SCP/WinSCP file transfer is not possible in DISA STIG profile; use the COPY command.
3. **Enter network values:** IPv4 and/or IPv6 network values (Address, Netmask/Prefix, Gateway, DNS).
4. **Set SSH shell password:** Enter a secure Linux SSH password (minimum 15 characters, mixed case, number, special character). This is different from the UI admin password and has no recovery option.
5. **Complete:** Click OK. Wait for installation (approx. 10-15 mins).
6. Dismount the ISO image from the system after installation and reboot the server.

Initial system setup

As a first-time System User, System Operator, or System Administrator, you need to complete this task to access the Cisco License On-Prem user interface and set up your initial credentials.

This section covers:

- Initial login procedure
- Synchronize with NTP Server
- Request a new On-Prem account
- Configure CLI user access and disabling default admin user (optional)
- Manage pending account request (approve, reject, or register manually)
- Synchronize Cisco License On-Prem
- Register devices

Initial login procedure

As a first-time System User, System Operator, or System Administrator, you need to complete this task to access the Cisco License On-Prem user interface and set up your initial credentials.

Eligible roles for this task

System administrator, system operator, system user

Procedure

Step	Action
Step 1	Go to the Cisco License On-Prem login page.
Step 2	Enter the default Username and Password: • Username: admin • Password: CiscoAdmin!2345 The Initial Setup Wizard opens.
Step 3	In the Initial Setup Wizard: Select your preferred language (English, French, Japanese, Chinese, or Korean).
Step 4	Enter a new password and confirm it.
Step 5	Confirm the Host Common Name. This value is pre-populated based on your system setup. You can update it if needed. The Common Name must match the host portion of the destination URL. Example: Fully Qualified Domain Name (FQDN) or IP address.
Step 6	Review your selection: • If everything is correct, click **Next.** • If you need to make changes, click **Back** to return to the previous page. • Once you complete these steps, click Done. After logging in with your updated information, the system displays the default landing page.

Synchronize with NTP Server

This task ensures your Cisco License On-Prem system's time is accurate and synchronized, which is crucial for product registration, license validation, and synchronization with Cisco License Central.

Eligible roles for this task

System Administrator, System Operator

Procedure

Step	Action
Step 1	From the Cisco License On-Prem Admin Workspace, click Settings Widget.
Step 2	Navigate to Time Settings Tab.
Step 3	Set the radio button for Synchronize with NTP Server.
Step 4	(Optional) Click on Synchronize Time Now to trigger an immediate sync.
Step 5	In the form fields, enter details for each NTP servers: Server Address Port
Step 6	(Optional) To use authentication, check Use NTP/Chrony Authentication for either server.
Step 7	Click Apply to save your changes or click Reset to discard them.

Note:

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

Request a new On-Prem Account

This task involves requesting a new On-Prem account within Cisco License On-Prem, which will then be mapped to a Cisco Smart Account and Virtual Account in Cisco License Central. This is the first step in making your on-premises licensing operational.

Eligible roles for this task

System Administrator, System Operator, System User

Procedure

Create a Cisco License On-Prem local account to manage products instances and licenses.

Users can request a new Account from two locations:

- **Licensing workspace > Accounts overview (Default landing page) > Actions > Request New On-Prem Account**
- **Admin workspace > On-Prem accounts > Request New On-Prem Account** (Only System Administrator and System Operators can perform this action from this page)

When you select **Request New On-Prem Account,** a drawer opens. Follow the steps below to complete the request:

Step	Action
Step 1	In the form that appears, enter the fields: • On-Prem Account Name • Smart Account

	• Virtual Account • Primary Contact Email Address
Note: While creating the On-Prem account, be sure that: The On-Prem account is mapped to a Cisco Smart Account and a Cisco Virtual Account in Cisco License Central. This mapping should be unique and should not be changed after creation. Changing the Cisco Virtual Account mapping may cause license synchronization issues, as license information continues to be shared with the originally configured Cisco Virtual Account.	
Step 2	Review your details and click **Request On-Prem Account.**

Configure CLI user access and disabling default admin user (optional)

This optional task enhances security by disabling the default CLI admin user and creating a custom "last resort" user with equivalent privileges, allowing secure, password-less SSH access while limiting exposure to the default account.

Eligible roles for this task

System Administrator, System Operator

Before you begin

- SSH Access: Ensure SSH access to the On-Prem CLI as the default admin.
- Key-Based Authentication: Have SSH keys available for password-less authentication.

Procedure

Step	Action
Step 1	Log in to the Cisco License On-Prem CLI: ssh admin@<onprem-ip>
Step 2	Disable the Default Admin User: Use the following command to disable the default admin user and start the last resort user creation process: disable_default_user This command will prompt for a new last-resort user with custom authentication credentials.
Step 3	Create a Last Resort User: Follow the prompts to set a username and configure SSH access (key-based authentication or password-less login). Once the user is created, you will see a confirmation message: “Default admin user has been disabled. New last resort user <username> created successfully.”

NOTE:

- This feature is only accessible once. Any attempts to disable the last resort user will trigger the error: "`Error: Last resort user cannot be disabled.`"
- In a High Availability (HA) deployment, this process must be repeated on each node independently. The last resort user does not replicate across nodes.
- If you attempt to disable an already-disabled admin, you will see: "`Error: Default admin has already been disabled.`"

Manage pending account request (approve, reject, or register manually)

After accounts are requested, they need to be approved to be used in Cisco License On-Prem.

Eligible roles for this task

A user with a System Administrator or System Operator role can perform this task.

Procedure

To approve or reject an account request, follow these steps:

Step	Action
Step 1	In the Administration Workspace, open the **On-Prem Accounts** Widget from the left panel.
Step 2	Select Pending Account Requests tab.
Step 3	In the list of pending requests, locate the account request you want to manage.
Step 4	Click on the inline action menu (…) against the account you wish to manage.
Step 5	Choose one of the following actions: • **Approve:** Approves the account request and activates the account. 4. Review the account requests. **Note:** If the name of the Cisco Smart Account or Cisco Virtual Account appears red, then click on the drop-down to change the account name. 5. Click **Next**. 6. If prompted, enter your Cisco SSO ID credentials and click Submit. Upon successful registration, a message pop-up opens stating that the account was created successfully, and the local account is registered as Active under the Accounts tab. • **Reject:** Denies the request and moves it to the rejected list. 1. Enter a reason for rejection. 2. Click **Reject.** • **Register Manually:** Initiates manual registration for the account, allowing the admin to complete the process directly. This option is used when there is no direct internet connection. 1. Click the Generate Registration File link to generate a registration file. 2. Log in to Cisco License Central and go to the On-Prem Accounts section. 3. Go to the On-Prem Accounts section and select "New account".

	4. Upload the account registration file. 5. An account authorization file will be generated. Download it to your local computer. 6. Click Browse button to locate the file. **7.** Click Upload to upload the file.
Step 6	Confirm your action.

Synchronize Cisco License On-Prem

This task ensures that your local Cisco License On-Prem instance has the most up-to-date license and account information from Cisco License Central Cloud. This is a critical step after initial account registration.

Eligible roles for this task

System Administrator, System Operator

Procedure

Step	Action
Step 1	Go to the Admin Workspace and open the Synchronization widget from the left panel.
Step 2	Select Accounts Synchronization tab.
Step 3	Locate the account on the table.
Step 4	Choose Initiate network (online) sync from the inline action menu (…).
Step 5	Select either: • Standard Sync (Synchronizes only since the latest sync) • Full Sync (Performs a complete refresh of all licenses, accounts, and device)
Step 6	Confirm to start synchronization
Step 7	The dynamic processing symbol appears, and the Alerts column shows the status of the synchronization as it progresses.

Note:

After 181 days, automatic synchronization will fail due to the expiration date of the access token, so manual online synchronization is required. If an "Access Token not found Synchronization cannot proceed" error message is displayed, perform a standard or full synchronization, and you will be prompted to enter your login credentials. Once you log in, the synchronization process will proceed during the next scheduled interval.

Register devices

Once your Cisco License On-Prem is installed, configured, and synchronized with Cisco License Central, the next step is to enable your Cisco products (devices) to communicate with it. This involves configuring each device to point to your Cisco License On-Prem server.

Eligible roles for this task

System Administrator, System Operator

Before you begin

- **Cisco License On-Prem URL:** Devices must be configured with the Cisco License On-Prem URL. This URL corresponds to the Host Common Name configured during the initial setup (or found in **Admin Workspace > Security > Certificates** tab). It can be an IP address or a Fully Qualified Domain Name (FQDN).
- **Transport Method:** The method your device uses to communicate with Cisco License On-Prem (e.g., Smart Transport, Smart Call-Home, CSLU Transport) dictates how the URL should be configured. Refer to your device's product documentation for specific transport configuration commands.
- **Strict SSL Cert Checking:** Products supporting Strict SSL Cert Checking require the configured URL to match the Cisco License On-Prem Common Name or Subject Alternative Name.

Procedure

Step	Action
Step 1	Identify the Cisco License On-Prem URL: Navigate to Admin Workspace > Security > Certificates tab in your Cisco License On-Prem UI to find the Host Common Name (and Subject Alternative Name, if applicable). This is the URL your devices use to register and communicate with Cisco License On-Prem.
Step 2	Determine device transport method: Consult your Cisco device's product documentation to identify the supported licensing transport method (e.g., Smart Call-Home, CSLU Transport).
Step 3	Configure the Device URL: Access your Cisco device's CLI or GUI and configure the licensing transport URL to point to the Cisco License On-Prem URL identified in Step 1. Example (Generic): `device# license smart url <Cisco_License_On-Prem_URL>` For specific commands and syntax, refer to your product's configuration guide.
Step 4	**Proceed with Device Registration:** Once the device is configured to communicate with Cisco License On-Prem, you can proceed with generating registration tokens and completing the device registration process. For detailed, step-by-step instructions on generating registration tokens and registering specific Smart Licensing or Smart Licensing Using Policy devices, refer to the "**Initialize**" chapter of the **Cisco License On-Prem User Guide**.

Provision 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: **`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**

Step	Action
	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, tap 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.

High Availability (HA) Cluster

This section provides instructions for deploying and managing High Availability (HA) clusters for Cisco License On-Prem. HA ensures continuous operation and data redundancy by distributing services across multiple nodes. Cisco License On-Prem supports both two-node (Active-Standby) and three-node (Active-Active) HA architectures.

Introduction to High Availability (HA)

Cisco License On-Prem Enhanced High Availability is supported by Pacemaker and Corosync, which are included in the installation package.

- **Two-Node HA (Active-Standby):** Consists of an Active node that handles all client requests and a Standby node that monitors the Active node. In case of Active node failure, the Standby node automatically takes over, ensuring service continuity with minimal disruption.
- **Three-Node HA (Active-Active):** Consists of three nodes that are all simultaneously active, participating in handling workloads, distributing the load, and increasing throughput. This architecture offers enhanced performance and improved failover capabilities.

High Availability Prerequisites

Before deploying any HA cluster, ensure the following conditions are met for all participating nodes:

- C**ommon Name (FQDN/VIP):** The Host Common Name configured for the HA Cluster must match the value you plan to use for the product destination URL (either as a Fully Qualified Domain Name or the Virtual IP address).
- **Unused Virtual IP (VIP):** The Virtual IP address must be an unassigned IP address within the same subnet as the physical node IPs. This IP will float across the cluster and be used for client access.
- **Cisco License On-Prem Version:** All nodes in the HA cluster must be running the exact same version of Cisco License On-Prem.
- **Network Subnet:** All nodes must have IP addresses on the same subnet and be mutually accessible.
- Private IP Addresses:
    - You will need two unused private IP addresses for internal SSH tunnel communication between nodes. These IPs should be different from the physical node IPs and preferably non-routable.
    - **Caution:** Verify that these private IP addresses are **NOT** in use in your network using a ping command (ping -c 5 -t 5 <IP_Address>) on Cisco License On-Prem before using them. Expected output for an unused IP shows 100% packet loss.
- **NTP Configuration:** Configure NTP on all nodes before deploying HA to ensure time synchronization.
- **Standby/Follower Node State:** Any node intended to be a Standby (for two-node HA) or a Follower (for three-node HA) should be a new, fresh installation of Cisco License On-Prem with no existing data. The Active/Source node's data will be replicated to it during deployment.
- **Network Interface Card (NIC):** HA networks are only certified to use one Network Interface Card (NIC).

Using Private IP Addresses in Your HA Cluster

Private IP addresses are used for the SSH tunnel between nodes and should not be routable. You must ensure these private addresses are not in use on your network.

Verify private addresses are not in use using a ping -c 5 -t 5 <IP_Address> command before deployment. Expected output: "5 packets transmitted, 0 received, 100% packet loss".

Deploying a Two-Node HA Cluster (Active-Standby)

This section outlines the steps to deploy a two-node HA cluster, where one node is Active and the other is Standby.

Eligible roles for this task

System Administrator

Step 1: Generate SSH Keys on the Primary Node

This task establishes a secure communication channel between the Primary and Standby nodes.

Step	Action
Step 1	SSH into the Primary node as an administrator. If in Standard mode, type `onprem-console` and press Enter to open the console. (If in DISA STIG mode, you are placed in the console by default.)

Step 2	Select the ha_mode you want to deploy as follows:
	`[admin@Cisco-License-On-Prem ~]$ onprem-console`
	`CLP Console`

	>> select_ha_mode 1. Deploy Two-node HA 2. Deploy Three-node HA Enter your choice (1 or 2): 1 Two-node HA mode selected successfully.
Step 3	When prompted, enter your admin password. **Note**: You can use special characters such as: !@#$%^&*()-=[];:",.<>?| You **cannot** use spaces in the HA cluster (sshtunnel) passwords. Shown here is the ha_generatekeys command and the expected output. To initiate the setup of the SSH tunnel, type the command: ha_generatekeys and press Enter. >>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... Operating in CiscoSSL FIPS mode. SSH keys were generated successfully.
Step 4	Choose an HA cluster password (this is for the `sshtunnel` user and will be used during HA setup. **Note:** Spaces are not permitted in the HA cluster password.
Step 5	Once the keys are generated, exit the Cisco License On-Prem shell and the SSH session.

Step 2: Provision the Standby Node

This task prepares the Standby node to receive data replication from the Active node.

Step	Action

Step 1	SSH into the Standby node and open the On-Prem console: ssh admin@<standby_node_ip> onprem-console

Step 2	Begin the provisioning process:
	Select the `ha_mode` you want to deploy as follows:
	`[admin@Cisco-License-On-Prem ~]$ onprem-console`
	`CLP Console`
	`>> select_ha_mode`
	`1. Deploy Two-node HA`
	`2. Deploy Three-node HA`
	`Enter your choice (1 or 2): 1`
	`Two-node HA mode selected successfully.`
	`ha_provision_standby`

Step 3	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**, **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 the Private IP section for details.
	a. Enter **<private IP address>** for the Active node private IP address.
	b. Enter **<IP address>** for the Standby node IP address or accept the default.
	c. Enter **<private IP address>** for the Standby private IP address.
	d. 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 Cisco License On-Prem server as a standby node`

```
============================================================
======

This procedure will convert a stand-alone Cisco License
On-Prem server to act as the standby node in an HA
environment. Proceeding will first destroy the current
database 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 the 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 the 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>


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 maschine 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 were 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

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 cluster.

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>)

5d91258862f94a54e1836dc5db7c0c9499d863433d71701e2cf80aef3c
bd97e9


Standby provisioning is complete!

You may now proceed with HA deployment from the active node.
```

Step 5	Confirm the configuration by typing yes.
Step 6	The provisioning will complete, indicating it's ready for deployment from the active node.

Step 3: Deploy the Active Server (Primary Node)

This step finalizes the HA cluster deployment.

Step	Action
Step 1	SSH into the Primary node and open the On-Prem console: ssh admin@<primary_node_ip> onprem-console
Step 2	Initiate the deployment: ha_deploy
Step 3	Enter your admin password.
Step 4	Provide the following information when prompted: **CAUTION:** Do not abort this process after proceeding. • Active node IP address • Active node private IP address • Standby node IP address • Standby node private IP address • Virtual IP address • HA cluster password >> ha_deploy [sudo] password for admin: **<admin password>** ========== Deploy Cisco License On-Prem two-node HA cluster ========== 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.


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

Setting up cluster...

2287b3ebcc5fa498d3d9aeb3ada3f36a3328a3ea58dbdd933ee7b6c167
89fe6a

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
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 Cisco
License On-Prem using the virtual IP at https:// <Virutal
IP>
```

Step 5	Confirm the configuration by typing yes.
Step 6	Wait for the deployment process to complete (approximately 5-15 minutes). The Virtual IP address will be displayed upon completion.

Post-Deployment Notes:

- **Access:** Always use the Virtual IP address to access Cisco License On-Prem. Do not use individual node IP addresses for server access, except for direct host OS access.
- **Data Replication:** The Active Cisco License On-Prem automatically replicates data to the Standby node. The Standby node will be unavailable until initial data replication is complete.
- **Troubleshooting:** If HA setup fails, downgrade the cluster (see below) and retry installation.
- **Status:** Use ha_status in the Cisco License On-Prem Console to check HA status.

Forced Failover of a High Availability Cluster

A forced failover is the deliberate act of switching the active role from the Primary (Active) node to the Standby node. This action is crucial for maintaining service availability and effectively managing your HA environment.

Why is Forced Failover required?

The primary purpose of a forced failover is to allow administrators to proactively manage the HA cluster, ensuring continuous operation even when the active node requires intervention. It minimizes downtime by allowing a controlled transition of services.

Circumstances when the users need to perform this.

- **Scheduled Maintenance:** For planned maintenance on the active node (e.g., OS updates, hardware upgrades, software patching), allowing services to shift to the standby node.
- **HA Testing:** To regularly test and validate the HA setup's failover mechanism, ensuring system resilience for disaster recovery.
- **Performance Troubleshooting:** To address active node performance degradation or software glitches, shifting services to standby for troubleshooting and isolation.
- **Pre-emptive Action:** As a pre-emptive measure for impending active node issues (e.g., high resource utilization, hardware alerts) to prevent uncontrolled outages.

How to perform a forced failover:

1. **Trigger the Failover:** You must simulate a failure of the Primary (Active) node. This is typically done by stopping its virtual machine or powering off the server.
2. **Switchover Process:** Upon detecting the Primary node's unavailability, the Standby node will automatically be promoted to the Active role. This switchover process typically completes within 2 minutes.
3. **Node Roles After Failover:** The original Primary node, once it is brought back online, will automatically rejoin the cluster as the new Standby node.

Downgrading a High Availability Cluster

To convert an HA cluster back to a single standalone node:

Step	Action
Step 1	Connect to the Primary/Active Cisco License On-Prem using the On-Prem Console.
Step 2	Execute the ha_teardown command: **NOTE:** You must run ha_teardown on the Primary node first. Running it on the secondary node first can prevent ha_deploy from completing later. ha_teardown
Step 3	The Secondary/Standby server must be discarded and cannot be reused. **NOTE:** Browser certificates are deleted when ha_teardown is used and must be re-uploaded.

Deploying a Three-Node HA Cluster (Active-Active)

A three-node HA cluster consists of three simultaneously active nodes that distribute the workload.

Key Principle: 'Source of Truth'

One node serves as the 'source of truth,' containing the primary data that is replicated to the other two nodes. Data on the other two nodes will be overwritten with data from the 'source of truth' node.

Before you begin

Before upgrading a three-node HA deployment, verify that all nodes are synchronized and identify the node that contains the most current and complete data.
After tearing down the existing HA cluster, perform a validation check on all nodes and select the node with the most current data as the source of truth for the upgraded deployment.
This verification helps ensure data consistency and provides a known-good baseline when rebuilding the upgraded HA cluster.

⚠

CAUTION: The 'source of truth' should be consistent across all nodes and should remain unchanged throughout all operations in the three-node High Availability (HA) cluster. Any data from nodes that are not 'source of truth' would be deleted.

The source of truth node serves as the primary node containing the required data, which is replicated to all other nodes in the HA cluster. On the remaining two nodes of the cluster, the data is overwritten with the data from 'source of truth' node.

Step 1: Select HA Mode

Step	Action
Step 1	SSH into all of the three nodes and open the Cisco License On-Prem console.
Step 2	Execute the `>>select_ha_mode` command: `select_ha_mode`
Step 3	Choose option 2 for "`Deploy Three-node HA`". Three node HA mode selected successfully.

Step 2: Prepare the 'Source of Truth' Node

On the designated 'source of truth' node, If this is an entirely new deployment, perform the following *before* proceeding with HA formation:

- Reset the default UI password for the source node before continuing with HA formation.
- Create an On-Prem account before proceeding with HA formation. The above two activities must be performed on 'source of truth' node before deploying HA.

Note: For existing Single Node deployments converting to three Node HA, Source of truth will be the original Single node machine.

Step 3: Deploy HA (ha_deploy) on All Three Nodes

Step	Action
Step 1	On each of the three nodes, execute the following command in the Cisco License On-Prem console ha_deploy
Step 2	Provide the following information when prompted: • IP address of the current node. • Virtual IP address (vip_ip). • IP addresses of the remaining nodes in the cluster (comma-separated). • IP that is the 'source of truth' node. **Caution:** Do not abort this process after proceeding. Refer the following command structure

	>>ha_deploy ========== Deploy SSM On-Prem three-node HA cluster 1. Enter IP address of the current node: <current node physical IP address> 2. Enter if Multi Datacenter setup is required (yes/no): (choose no if you would like to setup all servers in single data center.) *(To deploy 3 node HA in multi data-center, refer to the section Deploying a Three-Node Multi-Data Center HA Cluster)* 3. Enter the virtual IP address: <vip_ip> 4. Enter the IP address of the remaining nodes in cluster (comma-separated): <physical IP address of follower node 1>,<physical IP address of follower node 2> All API addresses are valid. 5. Using dc- name for datacenter Valid datacenter name: dc-<vip_ip> The datacenter name is autogenerated based on the VIP 6. Enter the IP that is the source of the truth: < physical IP address of the source of truth node> High Availability Setup Confirmation Current node : <current node physical IP address> Cluster nodes : <physical IP addresses of the other two cluster nodes> Virtual IP : <vip_ip> Datacenter : <dc-<vip_ip> > Source of Truth : <physical IP address of the source of truth node> !!! DO NOT ABORT THIS PROCESS AFTER PROCEEEDING!!! 7.Proceed with the above configuration? Enter 'yes' to continue: yes Stopping standalone server Preparing node for HA cluster formation…… Graceful leave complete Nomad and Consul Stopped System is ready to be deployed for HA WARN: Please ensure that the other two nodes in the cluster are ready to be deployed (Step 6) for HA setup as well before proceeding.
Step 3	Confirm the configuration by typing yes.

	Enter yes to continue: yes Info: HA Cluster Configuration found, configured nodes <physical IP address of node 1>,<physical IP address of node 2> Wait for the deployment to complete.

Post-Deployment Notes

- **Synchronization Delay:** After successful HA establishment, the system requires time to synchronize the database across all three nodes. This may cause a brief delay before data (e.g., browser/product certificates) is fully propagated and reflected on the Virtual IP. This behavior is expected.
- **Access:** Access the cluster through the VIP at https://<vip_ip>.
- **Product Certificate:** Update the Common Name (CN) for the Product Certificate under 'Security > Certificates' to use the VIP.
- **Synchronization:** Perform a synchronization from the Admin Workspace to apply and propagate changes.
- On successful deployment of a three-node high availability cluster, the following message is displayed on the **leader node**:

Successful Deployment of a Three-Node Cluster on the Leader Node

```
Success! Data Written to: db/pwenv
Success! Data Written to: artifactory/data
HA cluster deployed successfully.
You can access the cluster through the VIP at: <vip_ip>
Steps to complete before product registration:
1. Update the Common Name (CN) for the Product Certificate under
s'Security > Certificates' to use the VIP (Virtual IP).
2. Perform a synchronization from Admin Workspace to apply and
propagate the changes across the cluster.
```

On successful deployment of a three-node high availability cluster, the following message is displayed on the follower nodes:

Successful Deployment of a Three-Node Cluster on the Follower Nodes

```
INFO: SymmetricDS Node properties generated.
INFO: Elected leader Cisco License-On-Prem-cef02b.global, continuing
post cluster steps on the leader node.
>>
```

Steps to tear down a three-node HA cluster

A teardown of the High Availability cluster is required when you need to completely rebuild or reconfigure it. This is typically necessary for:

- **Major architectural changes:** Such as switching between a two-node and a three-node HA setup.

- **Fundamental setup corrections:** If the initial HA deployment had critical configuration errors that cannot be easily rectified.
- **Significant version upgrades:** In some cases, a major upgrade might necessitate a fresh HA deployment rather than an in-place upgrade of the cluster.

Note: Three-node HA relies on timed consensus among the nodes; therefore, any network or time-related discrepancies can result in a failed three-node HA formation cycle. In such cases, the most effective course of action is to dismantle the partially formed cluster and reinitiate the three-node HA deployment process. Please ensure low-latency connectivity among all three nodes prior to formation.

Upgrading High Availability (HA) Cluster

Upgrading your High Availability (HA) cluster ensures that your system continues to benefit from the latest features, security enhancements, and performance improvements. This section outlines the steps required to successfully upgrade a HA cluster, highlighting important prerequisites to minimize risks and maintain service continuity.

Before You Begin

- **Database Backup:**
  Ensure you have a current backup of your database before performing an upgrade.
  Reason: Without a backup, you risk irreversible data loss if the upgrade encounters an error or fails.
- **Network Interface Card (NIC) Limitation:**
  HA networks are certified for use with only one Network Interface Card (NIC).
  Reason: Using more than one NIC can cause network inconsistencies or failures, impacting cluster stability and failover capability.

To Install an upgrade to a HA cluster, follow these steps.

Procedure

Step	Action
Step 1	Revert the existing cluster to two standalone machines by using the teardown command. For each machine type: ha_teardown **NOTE**: See uploading deleted browser certificates after HA teardown for further information.
Step 2	After each machine has been reverted to a standalone state. Follow the procedures for Preparing to Upgrade a SSM On-Prem System and then Upgrading to Cisco License On-Prem.
Step 3	After each machine has been upgraded, follow the Deploying an HA Cluster procedure.

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

Replacing Browser Certificates after HA Teardown

If you teardown a HA cluster, all the Docker containers are stopped and re-started, but the browser certificate is deleted and will have to uploaded again after tearing down an HA cluster (using the <ha_teardown command>).

If your browser certificate is deleted as part of the teardown of a HA cluster and the node is subsequently upgraded to release 8-202102, you will also need to upload your browser certificate again.

Step	Action
Step 1	On each node, execute the ha_teardown command in the Cisco License On-Prem console: ha_teardown
Step 2	Confirm by typing yes.
Step 3	Proceed with teardown on the other nodes as well.

Network Port Requirements for HA Deployment

This section details all network ports required for the proper operation of Cisco Smart Software Manager On-Prem, including its user interface, product registration, synchronization with Cisco Smart Software Manager, and internal communication for High Availability (HA) cluster deployments.

General Cisco License On-Prem Communication Ports

These ports are required for basic Cisco License On-Prem functionality and external communication.

Port	Protocol	Purpose
4646	TCP	Nomad server leader detection (required for required HA failover monitoring).
4647	TCP	Nomad client communication.
4648	TCP	Nomad HTTP API.
6680	TCP	Internal service communication.
8500	TCP	Consul HTTP API.
8300	TCP	Consul server RPC.
8301	TCP/UDP	Consul LAN gossip.
8302	TCP/UDP	Consul WAN gossip.
8600	TCP	Consul DNS
8502	TCP	Internal service ports
8503	TCP	Internal service ports
6681	TCP	Internal service ports
6682	TCP	Internal service ports

6683	TCP	Internal service ports
6684	TCP	Internal service ports
31415	TCP	Internal service ports
5432	TCP	PostgreSQL database

High Availability (HA) Configuration on AWS

To configure High Availability (HA) for Cisco License On-Prem, deploy both primary and standby instances, and configure failover and failback using AWS Lambda and CloudWatch.

Deploy Primary and Standby EC2 Instances

Step	Action
Step 1	Launch two EC2 instances using the AMI created earlier. (Refer to the deployment steps.)
Step 2	Assign tags to identify the instances as "Primary" and "Standby."
Step 3	**Allocate three Elastic IPs:** • **EIP-1** for the Primary instance. • **EIP-2** for the Standby instance. • **EIP-3 (VIP)** for user traffic, dynamically reassigned during failover.
Step 4	Once both instances are up and running, refer to the **HA Installation Section** to configure High Availability using the VIP.
Step 5	**Access the GUI** • After completing the HA configuration steps, access the Cisco License On-Prem GUI using the VIP IP. **Note:** In the On-Prem Admin HA tab, the **private IP** will be displayed as the VIP. This behavior is expected in AWS, as the private VIP is exclusively used for communication between the two nodes. • For additional details about failover and failback operations, refer to the table **"Flow of Events and IP Behavior."**

Configure Lambda for Failover and Failback

Step	Action
Step 1	Open the AWS Lambda console and click **Create Function**.
Step 2	Name the function (e.g., `HA-Failover-Failback-Function`).
Step 3	Select **Python 3.x** as the runtime.

Step 4	Create or attach an IAM role with the following permissions
	`{`
	`  "Version": "2012-10-17",`
	`  "Statement": [`
	`  {`
	`  "Effect": "Allow",`
	`  "Action": [`
	`  "ec2:DescribeInstances",`
	`  "ec2:DescribeAddresses",`

Step	Action
	"ec2:AssociateAddress", "ec2:DisassociateAddress"], "Resource": "*" }] }

Step 5	Use the following code in the Lambda function:
	import boto3
	import logging
	import time
	
	# Initialize logger
	logger = logging.getLogger()
	logger.setLevel(logging.INFO)
	
	# Initialize EC2 client
	ec2 = boto3.client('ec2')
	
	def lambda_handler(event, context):
	start_time = time.time()
	
	# Define variables
	primary_instance_id = 'xx' # Replace with your Primary instance ID
	standby_instance_id = 'xx' # Replace with your Standby instance ID
	vip_eip_allocation_id = 'xx' # Replace with your VIP Elastic IP Allocation ID
	primary_eip_allocation_id = 'xx' # Replace with your Primary instance's initial Elastic IP Allocation ID
	standby_eip_allocation_id = 'xx' # Replace with your Standby instance's initial Elastic IP Allocation ID
	
	# Log the incoming event
	logger.info(f"Received event: {event}")
	
	# Extract the instance ID and state from the event
	instance_id = event.get('detail', {}).get('instance-id')
	instance_state = event.get('detail', {}).get('state', '')
	logger.info(f"Instance ID: {instance_id}, State: {instance_state}")
	
	try:
	if instance_id == primary_instance_id:
	if instance_state in ['stopped', 'terminated']:
	logger.info("Primary instance is down. Initiating failover to Standby instance...")
	switch_vip_to_instance(standby_instance_id, vip_eip_allocation_id)
	reassign_initial_ip(primary_instance_id, primary_eip_allocation_id)
	elif instance_state == 'running':
	logger.info("Primary instance is back online, but no failback is performed.")
	elif instance_id == standby_instance_id:
	if instance_state in ['stopped', 'terminated']:
	logger.info("Standby instance is down.

Step	Action
	Initiating failback to Primary instance...") switch_vip_to_instance(primary_instance_id, vip_eip_allocation_id) reassign_initial_ip(standby_instance_id, standby_eip_allocation_id) elif instance_state == 'running': logger.info("Standby instance is back online but remains in standby mode.") except Exception as e: logger.error(f"An error occurred during the failover/failback process: {e}") end_time = time.time() logger.info(f"Total execution duration: {end_time - start_time} seconds")

Configure CloudWatch Event Rules for Failover and Failback

Step	Action

Step 1	**Primary Instance Down (Trigger Failover)**
	• **Purpose**: Triggers the Lambda function when the primary instance enters a "stopped" or "terminated" state.
	• **Configuration:**
	○ **Event Source**: AWS EC2
	○ **Detail Type**: EC2 Instance State-change Notification
	○ **State Filter**: `stopped` or `terminated`
	○ **Instance ID Filter**: Primary instance ID
	• **Event Pattern (JSON):**
	{
	"source": ["aws.ec2"],
	"detail-type": ["EC2 Instance State-change Notification"],
	"detail": {
	"state": ["stopped", "terminated"],
	"instance-id": ["<Primary_Instance_ID>"]
	}
	}

Step 2	**Standby Instance Down (Trigger Failback)**
	• **Purpose**: Triggers the Lambda function when the standby instance (current active) enters a "stopped" or "terminated" state, initiating failback to the original primary.
	• **Configuration**:
	○ **Event Source**: AWS EC2
	○ **Detail Type**: EC2 Instance State-change Notification
	○ **State Filter**: `stopped` or `terminated`
	○ **Instance ID Filter**: Standby instance ID
	• **Event Pattern (JSON)**:
	{
	"source": ["aws.ec2"],
	"detail-type": ["EC2 Instance State-change Notification"],
	"detail": {
	"state": ["stopped", "terminated"],
	"instance-id": ["<Standby_Instance_ID>"]

Step	Action
	} }

Total IPs to Reserve

Elastic IPs (Public)

- **EIP-1:** Primary instance public IP.
- **EIP-2:** Standby instance public IP.
- **EIP-3 (VIP):** Dynamically reassigned during failover and failback.

Floating Private IP

- This private IP functions as a shared internal Virtual IP (VIP) in high availability configuration.
- It is part of HA formation and does not require dynamic reassignment.

Flow of Events and IP Behavior

Stage	Box	Public IP (Elastic IP)	Private IP	VIP Elastic IP (EIP)	Description
Initial State	**Box-1**	Elastic IP - 1 (IP-3) → VIP	Auto (e.g., 10.0.0.1)	VIP EIP (IP-3)	Box-1 is the Primary node, handling traffic through VIP (IP-3).
	Box-2	Elastic IP - 2 (IP-2)	Auto (e.g., 10.0.0.2)	Not associated	Box-2 is the Standby node, ready to take over if Box-1 fails, but currently not handling VIP traffic.
Failover (Box-1 Down)	**Box-1**	Elastic IP - 1 (IP-1)	Auto (e.g., 10.0.0.1)	Not associated	Box-1 becomes Standby after failing. Its VIP (IP-3) is disassociated and it retains Elastic IP (IP-1) for future use.
	Box-2	Elastic IP - 3 (IP-3) → VIP	Auto (e.g., 10.0.0.2)	VIP EIP (IP-3)	Box-2 takes over as the Primary node, and VIP (IP-3) is now

Stage	Box	Public IP (Elastic IP)	Private IP	VIP Elastic IP (EIP)	Description
					associated with it to handle traffic.
Box-1 Comes Back Online	**Box-1**	Elastic IP - 1 (IP-1)	Auto (e.g., 10.0.0.1)	Not associated	Box-1 comes back online but remains in Standby mode. It retains Elastic IP (IP-1) and does not take over the VIP.
	Box-2	Elastic IP - 3 (IP-3) → VIP	Auto (e.g., 10.0.0.2)	VIP EIP (IP-3)	Box-2 continues as the Primary node, handling traffic via VIP (IP-3).
Failback (Box-2 Down)	**Box-1**	Elastic IP - 3 (IP-3) → VIP	Auto (e.g., 10.0.0.1)	VIP EIP (IP-3)	Box-1 becomes the Primary node again and handles traffic via VIP (IP-3).
	Box-2	Elastic IP - 2 (IP-2)	Auto (e.g., 10.0.0.2)	Not associated	Box-2 goes down, and Elastic IP (IP-2) remains associated for future recovery.

Test and Validate the HA Setup

Step	Action
Step 1	**Failover Testing:** • Stop the Primary instance to simulate a failure. • Verify that the Lambda function reassigns the VIP Elastic IP (EIP-3) to the Standby instance.
Step 2	**Failback Testing:** • Restart the Primary instance to simulate recovery. • Confirm that the Lambda function reassigns the VIP Elastic IP (EIP-3) back to the Primary instance.

Flow of Events and IP Behavior with Floating IP

Flow of Events

1. **Initial Setup**
    a. Primary Instance:
    Holds Elastic IP - 1 (IP-1) for public access.
    Is assigned the VIP Elastic IP (IP-3) for user traffic.
    Uses a Floating Private IP (e.g., 10.0.0.100) as the VIP in the HA setup for internal communication.
    b. Standby Instance:
    Holds Elastic IP - 2 (IP-2) for public access.
    Does not have the VIP Elastic IP (IP-3).
    The Floating Private IP (10.0.0.100) is part of the HA setup but not actively serving traffic.
2. **Failover (Primary Down)**
    a. Primary Instance:
    Retains Elastic IP - 1 (IP-1) for monitoring or recovery purposes.
    The VIP Elastic IP (IP-3) is no longer associated with this instance.
    The Floating Private IP (10.0.0.100) remains part of the HA logic but does not actively route traffic.
    b. Standby Instance:
    Becomes the active node, serving traffic through VIP Elastic IP (IP-3).
    The Floating Private IP (10.0.0.100) remains in use and is leveraged for HA logic.
3. **Failback (Primary Recovers)**
    a. Primary Instance:
    Recovers and is reassigned the VIP Elastic IP (IP-3) by the HA mechanism.
    Retakes its role as the active node, handling user traffic.
    Continues using the Floating Private IP (10.0.0.100) as part of the HA setup.
    b. Standby Instance:
    Returns to standby mode, holding only Elastic IP - 2 (IP-2) for public access.
    The VIP Elastic IP (IP-3) is no longer associated.
    Continues to be part of the HA setup with the Floating Private IP (10.0.0.100).
4. **Post-Failback**
    a. Primary Instance:
    Fully resumes its role as the active node with both VIP Elastic IP (IP-3) and Floating Private IP (10.0.0.100) for HA.
    b. Standby Instance:
    Remains passive, ready for future failover events.
    Retains its initial Elastic IP - 2 (IP-2).
    The Floating Private IP (10.0.0.100) is consistently part of the HA logic but does not serve traffic unless a failover occurs.

Key Notes

- **Elastic IPs**: EIP-1 and EIP-2 remain static for monitoring, while EIP-3 (VIP) is reassigned dynamically.
- Floating Private IP: Static internal IP consistently used for communication within the VPC.
- Compliance: Ensure the setup meets DISA STIG security guidelines.

NOTE: **Elastic IPs:**
- EIP-1: Primary instance public IP.
- EIP-2: Standby instance public IP.
- EIP-3 (VIP): Virtual IP for user traffic, dynamically reassigned during failover and

failback.

Floating Private IP:

- A static private IP used within the VPC for internal communication between instances.

Compliance:

- Ensure that the setup complies with DISA STIG guidelines for security hardening.

3-Node High Availability (HA) Deployment for AWS

Cisco License On-Prem supports a three-node High Availability (HA) deployment on Amazon Web Services (AWS). This architecture uses an Elastic IP (EIP) to provide Virtual IP (VIP) functionality and failover.

Prerequisites

Before proceeding with the deployment, ensure you have:

- An active AWS account with sufficient permissions to create VPCs, subnets, EC2 instances, Elastic IPs, Security Groups, CloudWatch Alarms, and Lambda functions.
- A Virtual IP (VIP) address that will be used by the Cisco License On-Prem cluster. This VIP must be an Elastic IP (EIP) in AWS.
- SSH client for connecting to EC2 instances.

Deployment Steps

The 3-node High Availability (HA) deployment on AWS involves the following major tasks:

1. Create a Custom VPC
2. Launch ECS Instances
3. Upgrade ISO Image
4. Configure VIP Management
5. Set Up Failover Workflow
6. Configure Security Groups
7. Validate Deployment

Create a Custom VPC

Step	Action
Step 1	Log in to your AWS Management Console
Step 2	Navigate to the VPC service. Click **Create VPC.** Choose **VPC only.**
Step 3	Provie a name and CIDR block (for example, 10.0.0.0/16).
Step 4	Create a **public subnet** (for example, 10.0.1.0/24).
Step 5	Create an **Internet Gateway (IGW)** and attach it to the VPC.
Step 6	Create a route table, associate it with the public subnet, and add a default route to the IGW (0.0.0.0/0).

Launch EC2 Instances

Step	Action
Step 1	From the **EC2 Dashboard,** launch three EC2 instances using the Cisco License On-Prem AMI from the AWS Marketplace.
Step 2	Place all instances in the same VPC and subnet.
Step 3	Assign two network interface per instance: ○ **Public Interface:** for external communication (via the public subnet) ○ **Private Interface:** for inter-node HA communication (via a private subnet, if required).

Connect to each EC2 instance using Secure Shell (SSH) and Upgrade ISO Image

- Transfer the ISO upgrade script

root mode:

scp scpuser@skywalker.cisco.com:/volume1/SharedISO/Cisco/On-Prem/9-202507/CCO/Cisco_License_On-Prem_9-202601_Upgrade/ Cisco_License_On-Prem-9-202601_Upgrade.sh /var/files/patches/

scpscpuser@skywalker.cisco.com:/volume1/SharedISO/Cisco/On-Prem/9-202507/CCO/SSM_On-Prem_9-202507_Upgrade/SSM_On-Prem-9-202507_Upgrade.sh.sha256 /var/files/patches/

- From the On-Prem console, run the following command to apply the patch and verify it with the checksum file:

```
onprem-console:
upgrade patches:SSM_On-Prem-9-202507_Upgrade.sh SSM_On-Prem-9-202507_Upgrade.sh.sha256
```

Configure VIP Management with Elastic IP (EIP)

- On-Premises deployments use keepalived with VRRP to manage the VIP.
- On AWS, this functionality is replaced with an EIP:
  - The EIP is initially associated as VIP.
  - EIP association/disassociation is managed externally using AWS services (not keepalived directly).

Configure Failover Workflow Using CloudWatch and Lambda

Step	Action
Step 1	Create a **CloudWatch** alarm to monitor EC2 instance health.
Step 2	Create an **EventBridge rule** to capture EC2 state changes (Stopped, Terminated, Pending).
Step 3	Configure a **Lambda function** to handle failover events: ○ Detect unhealthy instances. ○ Disassociate the EIP from the failed node. ○ Reassign the EIP to a healthy instance ○ Log the failover event.

Configure Security Groups

Step	Action
Step 1	In the navigation pane, under **Network & Security**, click **Security Groups**.
Step 2	Click **Create security group**.
Step 3	Add inbound rules to allow traffic on the required ports (Nomad, Consul, PostgreSQL, and other internal services). To ensure successful deployment and communication, these ports must be unblocked on the private subnet. Refer to Appendix 8. Network Port Requirements for HA Deployment for complete list of ports and protocols. **Note**: Port **4646** must be accessible by the Lambda function to determine the leader of the cluster.

Validation Procedures

Step	Action
Step 1	Verify VPC and subnet configuration in the **VPC Dashboard**.
Step 2	Test connectivity between EC2 instances.
Step 3	Confirm EIP association and reassignment logic.
Step 4	Simulate failover by stopping one EC2 instance and observing EIP reassignment.
Step 5	Validate Security Group rules with EC2 connectivity tests.

Deployment Conditions

The 3-node HA deployment process on AWS is similar to on-premises but includes AWS-specific requirements:

- **Nodes:** Three standalone EC2 instances, each with its own IP, deployed in the same subnet or network topology with full node-to-node reachability.
- **VIP:** A single Elastic IP (EIP) is used as the Virtual IP. The EIP is initially assigned to the leader node and reassigned automatically during failover.
- **Node Configuration:**
  - All three EC2 instances must be in the same VPC (custom or default).
  - Connectivity must be ensured through security groups for both internal and external communication.
- **Network Interfaces:**
  - **Public Interface (Public Subnet):** Provides dynamic public Ips for external communication.
  - **Private Interface (Private Subnet):** Provides static private IPs for inter-node HA communication. These remain persistent across reboots.

Failover Workflow

Steps	Action
Step 1	**EIP Assignment:** Associate an Elastic IP with the leader node after deployment.
Step 2	**CloudWatch EventBridge Rule:** Monitor EC2 state changes such as stopped, terminated, or failed.
Step 3	**Lambda Trigger:** Use a Lambda function to detect unhealthy nodes and reassign the EIP to a healthy leader.
Step 4	**Reassociation :** During failover, the EIP is disassociated from the failed node and reassigned to the new leader, ensuring service continuity.

NOTE:	Compared to on-premises deployments, AWS requires additional configuration steps, especially for Elastic IP (EIP) management and networking. These steps help ensure a resilient 3-node HA setup.

3-Node High Availability (HA) Deployment for Azure

Cisco License On-Prem supports a three-node High Availability (HA) architecture on Microsoft Azure. This deployment uses an **Internal Load Balancer (ILB)** to manage failovers and traffic routing across nodes.

Prerequisites

An Azure 3-Node HA deployment uses:

- **Three standalone nodes,** each with their own IP address, within the same virtual network or topology that ensures full node-to-node reachability.
- **A Virtual IP (VIP)** managed through an Azure Internal Load Balancer (ILB) for traffic routing and failover.

Node Configuration

Virtual Machine

- Deploy **three virtual machines (VMs)** from VHD in the same or different subnets within a custom Virtual Network (VNet).
- Ensure connectivity through **Network Security Groups (NSGs)** for both internal and external communication.

Network Interface

Each VM uses a single **Network Interface (NIC):**

- **Internal Communication (Private IP):**
  - Assign a static private IP address to each VM within the same VNet and subnet.
  - This private IP is used for inter-node communication (Nomad and Consul).
  - The private IP persists across VM reboots and is critical for HA cluster integrity.
- **External Communication (Optional Public IP):**
  - If external access is required (for SSH or API calls), associate a Public IP address with the VM's NIC.
  - Public Ips can be dynamic or static.
  - In HA deployment using ILB, public Ips are typically disabled to restrict access to internal clients only.

Security and Routing

- Apply **Network Security Groups (NSGs)** to NICs or subnets to control inbound and outbound traffic.
- Allow required ports for Nomad, Consul, and PostgreSQL.

VIP Management in Azure

In Azure, VIP functionality is implemented using an **Internal Load Balancer (ILB):**

- The ILB is assigned a static **private IP address,** acting as the VIP.
- The VIP is not tied to any single VM. Instead, traffic is routed to healthy nodes in the backend pool, based on health probe results.
- Failover and traffic redirection are handled automatically by the ILB. No manual reassignment or scripts are required.

Failover Workflow in Azure

1. **VIP Assignment**
   - The ILB is assigned a static private IP (VIP) for cluster communication.
   - Traffic is routed only to the active node identified by health probes.
2. **Monitoring VM State**
   - Use Azure Event Grid to subscribe to VM lifecycle events such as Stopped, Deallocated, Failed, or Restarted.
   - These events are automatically emitted when VM states change.
3. **Triggering Automation**
   - Configure an **Azure Function** as the event handler for Event Grid.
   - When a state change occurs, the function evaluates cluster health and leadership status.
4. **Backend Pool Reconfiguration**
   - The Azure Function checks which node is the Nomad/Consul leader.
   - If the ILB backend pool does not align with the current leader:
     - Remove the unhealthy node from the backend pool.
     - Add the new leader node to the backend pool to route traffic correctly.

Deployment Steps

- Create Three Virtual Machines in the same **availability** set or **virtual machine scale** to ensure high availability.
- Configure each node with required services (Nomad, Consul, PostgreSQL).

Create an Internal Load Balancer

Step	Action
Step 1	In Azure Portal, select **Create a resource > Load Balancer.**
Step 2	Choose **Internal** as the type.
Step 3	Assign a frontend IP configuration (VIP).
Step 4	Add the three VMs to the backend pool.
Step 5	Create health probes to monitor availability of each node.
Step 6	Add load balancing rules to distribute traffic.

Configure VIP Management

Step	Action
Step 1	Assign the VIP to the ILB frontend configuration**.**
Step 2	Verify that backend pool members are correctly configured to respond to health probes.

Perform Failover Test

Step	Action
Step 1	Stop one of the VMs.
Step 2	Verify that traffic is redirected to the remaining nodes.
Step 3	Monitor load balancer metrics and logs to confirm failover behavior.

Create VM Using Custom Image (Azure Marketplace)

Step	Action
Step 1	In Azure Portal, select **Create a resource > Virtual Machine.**
Step 2	In the **Basics** tab complete the required details (subscription, resource group, VM name, region).
Step 3	In the **Image** dropdown, select **Browse all public and private images.**
Step 4	Search for the required custom image from Azure Marketplace.
Step 5	Select the image and configure VM size, authentication, and inbound ports.
Step 6	Review and create the VM.

Create a Network Security Group (NSG)

Step	Action
Step 1	In Azure Portal, select **Create a resource > Network Security Group.**
Step 2	Enter the name, subscription, and resource group.
Step 3	Add inbound rules for the required ports (Nomad, Consul, PostgreSQL, and internal services).
Step 4	Refer to Appendix 8. Network Port Requirements for HA Deployment for complete list of ports and protocols. Note: Port 4646 must be accessible by the Lambda function to determine the leader of the cluster.
Step 5	Associate the NSG with the subnet or VM NICs.

Configure Internal Load Balancer (ILB)

Step	Action
Step 1	In Azure Portal, go to Load Balancers > Create.
Step 2	**Basics Tab:** ○ **Name:** ilb-ha-cluster ○ **Type:** Internal ○ **SKU:** Standard ○ **Region:** Same as VMs ○ **VNet/Subnet:** Same as VM subnet ○ **Private IP:** Static (acts as VIP, e.g., 10.0.1.100)
Step 3	**Frontend IP Configuration:** ○ Name: ilb-frontend ○ Private IP: 10.0.1.100
Step 4	**Health Probe:** ○ Protocol: TCP ○ Port: 4646 (Nomad leader detection) ○ Interval: 5 seconds
Step 5	**Load Balancing Rule:** ○ Frontend Port: 4646 ○ Backend Port: 4646 ○ Backend Pool: ha-backend-pool ○ Probe: `nomad-health-probe`

VIP Management Strategy

1. The Internal Load Balancer (ILB) is assigned a **static private IP** (for example, 10.0.1.100) that serves as the Virtual IP (VIP).
2. A health probe monitors the Nomad leader port (4646).
3. Traffic is routed only to the node that passes the health probe, ensuring that only the active leader receives traffic.
4. (Optional) You can use **Azure Function** with **Event Grid** to automate backend pool updates when leadership changes. This ensures that the ILB always directs traffic to the current leader without manual intervention.

Failover Testing

Steps	Action
Step 1	**Simulate Failure** ○ Stop the current leader VM.
Step 2	**Observe ILB Behavior** ○ Health probe detects failure. ○ Traffic reroutes to the next healthy node.
Step 3	**Verify** From a test VM in the same subnet, run: `curl http://10.0.1.100:4646/v1/status/leader`
Step 4	Confirm the new leader responds.

Next steps and application configuration

Your Cisco License On-Prem system is now successfully installed, the operating system is configured, and the initial application setup is complete. The system is ready for you to begin configuring its various features and managing your licenses and devices.

This Installation Guide has covered the foundational steps to get your Cisco License On-Prem instance online and accessible. All subsequent application-level configuration, account management, and operational tasks are detailed in the Cisco License On-Prem User Guide.

Chapter 5 Troubleshooting installation and initial access

This section provides solutions to common issues you might encounter during or immediately after the installation of Cisco License On-Prem, preventing initial system access or successful boot-up. For all other application-level troubleshooting, including account registration, synchronization, and license management issues, please refer to the ***"Troubleshoot"*** chapter in the *Cisco License On-Prem User Guide*.

Initial checks before troubleshooting

Before addressing specific scenarios, perform these general checks to rule out common installation-related problems:

- **Verify VM/Platform Requirements:** Ensure your virtual machine or cloud instance meets the minimum CPU, Memory, and Disk requirements specified in the "System Requirements and Prerequisites" section.
- **ISO Integrity:** Confirm the downloaded ISO file is not corrupted.
- **Boot Order:** Verify the VM's boot order is set to boot from the ISO image during installation.
- **Network Configuration during Kickstart:** Double-check the IP address, Netmask/Prefix, Gateway, and DNS settings entered during the initial Kickstart configuration. Incorrect network settings will prevent the system from being accessible.
- **Default Admin Password:** Ensure you are using the correct default password (CiscoAdmin!2345) for the very first login.
- **Web Browser Compatibility:** Use one of the supported web browsers listed in the "System Requirements and Prerequisites" section.

Common installation & initial access scenarios

Scenario	Cause	Solution	Reference
I cannot access the Cisco License On-Prem UI after installation.	Incorrect network configuration during Kickstart, firewall blocking access, or services not started.	1. **Verify Network Settings:** Log into the CLI via SSH (if accessible) and use network commands to confirm IP, gateway, and DNS. 2. **Check Firewall:** Ensure port 8443 (HTTPS) is open on your host firewall. 3. **Verify Services:** Log into the CLI and run `docker ps` to check if all containers are running. If not, try `systemctl` restart satellite.	• Initial System Configuration • Platform-Specific Installation Procedures
Default admin login fails (after initial password change).	Incorrect new password, or password complexity rules not met.	1. **Re-enter Password Carefully:** Ensure Caps Lock is not on and re-enter your new password. 2. **Password Reset:** If you forgot your new	• Initial Login Procedure • "Manage" chapter in Cisco License On-Prem User

		password, you may need to follow the password reset procedure.	Guide (for password reset)
System is slow or unresponsive immediately after installation.	Insufficient VM resources allocated, or services are still starting up.	1. **Verify VM Resources:** Check your VM settings against the "Capacity Limitations" in this guide. 2. **Allow Startup Time:** Give the system 5-15 minutes after reboot for all services to fully start.	• System Requirements and Prerequisites • Platform-Specific Installation Procedures
Kickstart screen is not displayed / VM does not boot from ISO.	Incorrect VM boot order, corrupted ISO, or ISO not properly attached.	1. **Check VM Boot Order:** Ensure the VM's BIOS/EFI settings prioritize booting from the CD/DVD drive (where the ISO is attached). 2. **Re-attach ISO:** Verify the .iso file is correctly attached to the VM's CD/DVD drive and "Connect at Power On" is selected. **3.** **Re-download ISO:** If issues persist, re-download the ISO to rule out corruption.	• Platform-Specific Installation Procedures • Preparing Your Installation Environment
I see Docker-related firewall warnings during installation or startup.	These messages are normal internal Docker startup sanity checks. Docker adjusts firewall rules to enable container communication, and these warnings indicate that rules are being added where none existed.	These warnings can generally be ignored. They do not affect the installation or startup of the application, and no action is required.	

Resolving network conflicts using the docker_network_config command

During installation or initial access, you may encounter network connectivity issues if the default Docker network address pool used by Cisco License On-Prem overlaps with your organization's existing network ranges. The default internal Docker subnet is 172.16.2.0/24. Overlapping subnets can cause routing conflicts, resulting in unreachable services or unexpected network behavior.

Symptom

- Network communication issues between Cisco License On-Prem containers and the broader network.

- Unreachable services due to duplicate or conflicting IP address ranges.

Cause

- The default Docker internal network (e.g., 172.16.2.0/24) overlaps with your organization's network address space.

Solution - Change the docker internal network range

To resolve network conflicts, you can reconfigure the Docker internal network address pool using the On-Prem console's docker_network_config command.

Steps:

1. **Access the On-Prem console:**
   Refer to the Cisco Smart Software Manager On-Prem Console Guide for instructions on opening the On-Prem console.
2. **Run the docker_network_config command:**
   At the On-Prem console prompt, enter:

docker_network_config

You will be prompted to specify a new network range for internal Docker communications.

3. Choose a non-overlapping subnet:
   - Select a subnet that does **not** overlap with any existing network ranges in your environment.
   - The subnet must be a contiguous range defined by a /24 mask (e.g., 192.168.0.0/24, 10.10.10.0/24).
   - For a /24 pool, you will have 256 IP addresses (253 usable for internal communications).
4. Apply the configuration:
   - The docker_network_config command will update the Docker networking settings and allocate addresses from the specified pool.