Cisco Meeting Server

Cisco Meeting Server 4.0

Installation Guide for Cisco Meeting Server Small/1000 and Virtualized Deployments

November 24, 2026

Contents

Change History 5

1 Introduction 6
- 1.1 Overview of virtualized platforms 7
- 1.2 How to use this Guide 7
- 1.3 Differences in specific MMP commands 9
- 1.4 Differences in components enabled on the different platforms 9

2 Installation 11
- 2.1 Before You Start 11
  - 2.1.1 About the Cisco Meeting Server software 11
  - 2.1.2 Host requirements for the Cisco Meeting Server as a VM deployment 11
- 2.2 Installing via VMware on a specification-based server 13
- 2.3 Deploying Meeting Server 14
  - 2.3.1 Deploying Meeting Server from the OVA file with ESXi Web Client 14
  - 2.3.2 Deploying Meeting Server on Nutanix Cluster 18
  - 2.3.3 Deploying Meeting Server Using NFVIS 24
- 2.4 Installing and initial configuration of Cisco Meeting Server Small/1000 35
  - 2.4.1 Before You Start 35
  - 2.4.2 Task 1 – Unpacking and initial startup 35
  - 2.4.3 Task 2 – Configuring VMware Network Management 37
  - 2.4.4 Task 3 – Retrieving and activating VMware Licenses 38
  - 2.4.5 Task 4 – Accessing the Cisco Meeting Server Small/1000 Console 39

3 Configuration 40
- 3.1 Creating your own Cisco Meeting Server Administrator Account 40
- 3.2 Setting up the Network Interface for IPv4 40
- 3.3 Adding Additional Network Interface(s) 42
- 3.4 Configuring the Call Bridge 42
- 3.5 Configuring the Web Admin Interface 43
  - 3.5.1 Creating the certificate for the Web Admin Interface 43
  - 3.5.2 Configuring the Web Admin Interface for HTTPS Access 44
  - 3.5.3 Useful information to help configure Web Bridge 3 46
  - 3.5.4 Enabling the Web Bridge 3 Service 48
  - 3.5.5 Configure Call Bridge with Web Bridge Addresses 50

Appendix A Technical specifications for Cisco Meeting Server 1000/Small 52

A.1 Physical specifications: 52
A.2 Environmental specifications 52
A.3 Electrical specifications 52
A.4 Video and audio specifications: 52

Appendix B Cisco licensing 54
B.1 Smart Account and Virtual Account information 54
B.2 How Smart licenses work in Meeting Server – overview 54
B.3 Expired license feature enforcement actions 56
B.4 How to retrieve licensing information (Smart Licensing) 57
B.5 Cisco Meeting Server licensing 57
B.5.1 Personal Multiparty plus licensing 58
B.5.2 Shared Multiparty plus licensing 59
B.6 Smart Licensing registration process 59
B.7 Assigning Personal Multiparty licenses to users 60
B.7.1 To determine whether a specific user has a license: 60
B.8 How Cisco Multiparty licenses are assigned 61
B.9 Determining Cisco Multiparty licensing usage 61
B.10 Calculating SMP Plus license usage 62
B.11 Retrieving license usage snapshots from a Meeting Server 63
B.12 License reporting 63
B.13 Legacy licensing file method 63
B.13.1 Getting and Entering a License File 63
B.13.2 Obtaining Cisco user licenses using the traditional licensing method 65

Appendix C Branding 67

Appendix D Sizing a VM 68
D.1 Call Bridge VM 70
D.2 Web Edge VM 71
D.2.1 Edge server configurations 71
D.2.2 Deployment considerations 73
D.3 Database VM 73
D.4 Recorder and Streamer VM 74
D.4.1 VM sizing for the new internal SIP recorder component 74
D.4.2 VM sizing for the new internal SIP streamer component 74
D.5 Web Scheduler 75
D.6 MeetingApps 75

Appendix E Additional information on VMWare 77
E.1 VMWare 77
Appendix F Creating a certificate signed by a local Certificate Authority 79
Cisco Legal Information 83
Cisco Trademark 84

Change History

Date	Change Summary
September ... 2026	New document for 4..0. Added section for Meeting Server deployment using NFVIS.

1 Introduction

The Cisco Meeting Server is a scalable software platform for voice, video and web content, which integrates with a wide variety of third-party kit from Microsoft, Avaya and other vendors. With the Cisco Meeting Server, people connect regardless of location, device, or technology.

The Cisco Meeting Server software runs as a virtualized deployment with:

- ESXi Web Client
- Nutanix cluster deployment

ESXi

The Cisco Meeting Server software runs as a virtualized deployment using VMware ESXi 8.0 with virtual hardware vmx-1x loaded onto the following platforms:

- Cisco Meeting Server 1000, /Meeting Server Small (a preconfigured Cisco UCS C220 rack server).
- specification-based VM platforms.

The table below indicates the ESXi versions supported by the current versions of Cisco Meeting Server software.

Table 1: ESXi version support

Cisco Meeting Server version	ESXi version

Nutanix

Meeting Server supports deployment on Nutanix clusters. This configuration is supported on 220 M7+ HCI nodes.

- Required AHV Version: 10.3.1.2
- Required AOS Version: 7.3.1.2

Customers often use virtualized deployments of the Cisco Meeting Server as the edge server in a split deployment and in scalable deployments.

The functionality, and user experience for participants, is identical across all platforms running the same software version. However, deployments are not interchangeable between the virtualized deployments and physical deployments (Cisco Meeting Server 2000). For example, it is not possible to create a backup from a virtualized deployment and roll it back on a Cisco Meeting Server 2000 or vice versa.

Note: Meeting Management and connected Meeting Servers must run the same software version. Meeting Management handles the product registration and interaction with your Smart Account for Smart Licensing support.

1.1 Overview of virtualized platforms

CAUTION: Irrespective of which virtualized platform is running the Cisco Meeting Server software, ensure the platform is up to date with the latest patches. Failure to maintain the platform may compromise the security of your Cisco Meeting Server.

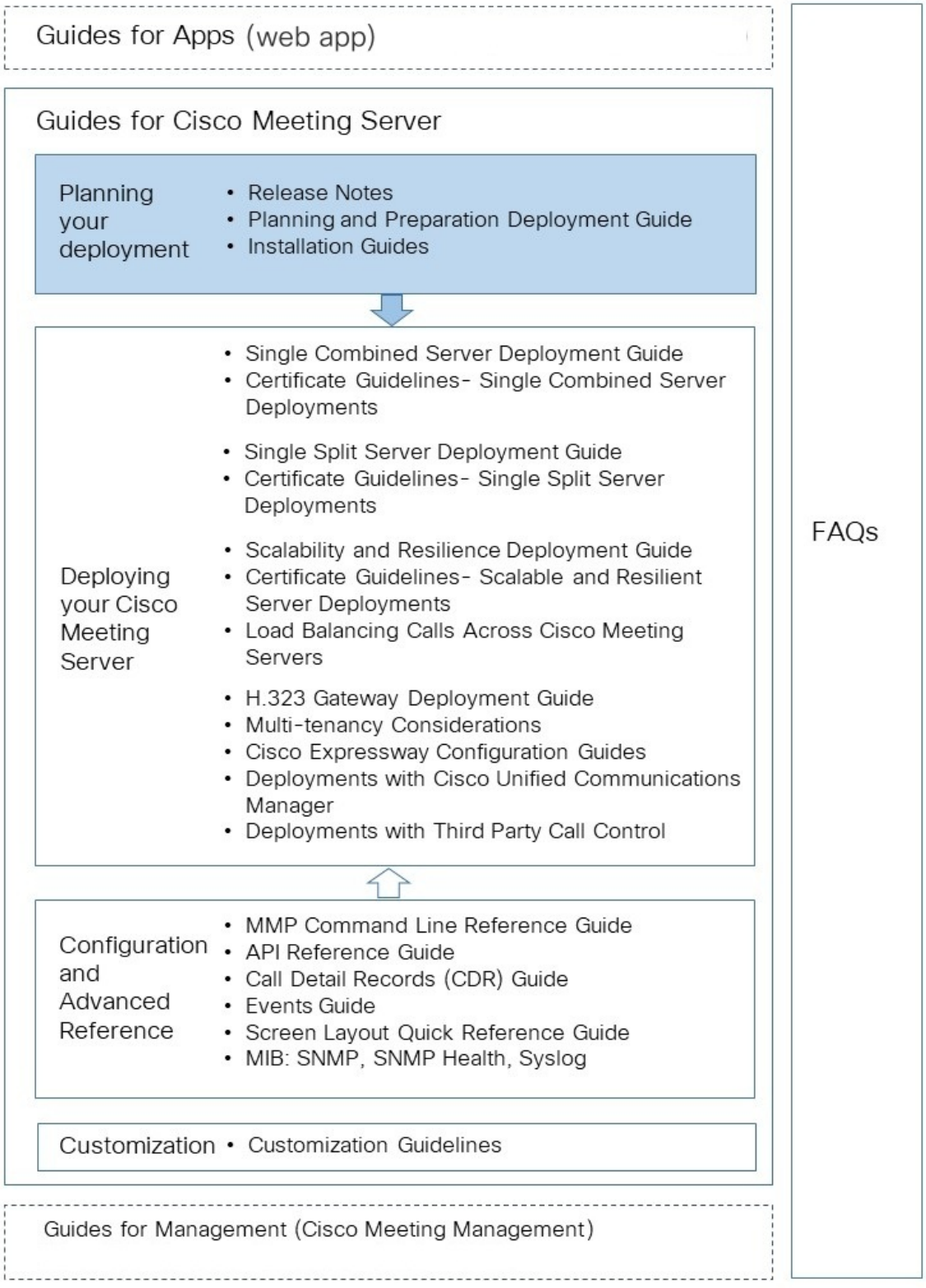
specification-based VM platforms: if you are upgrading the server from a previous virtualized Cisco Meeting Server installation, then follow the instructions in the Cisco Meeting Server release notes. If this is a new installation, then follow this guide to create a VM and install the Cisco Meeting Server software.

1.2 How to use this Guide

This guide covers the installation of the Cisco Meeting Server 1000/Small and specification-based VM deployments.

After configuring the Cisco Meeting Server and applying the license, use the Planning and Preparation Deployment Guide to guide you on deciding the appropriate deployment, and then follow the deployment and certificate guides that are most relevant to your targeted deployment, see Figure 1. These documents can be found on cisco.com.

Figure 1: Cisco Meeting Server installation and deployment documentation



Note: The address ranges we use in Cisco user documentation are those defined in RFC 5737 which are explicitly reserved for documentation purposes. IP addresses in Meeting Server user documentation should be replaced with correct IP addresses routable in your network, unless otherwise stated.

1.3 Differences in specific MMP commands

The MMP Command Reference details the full set of MMP commands. There are a few differences running a Cisco Meeting Server 2000 compared to a virtualized Cisco Meeting Server.

Command	on Cisco Meeting Server 2000	on Cisco Meeting Server 1000 /Cisco Meeting Server Small and virtualized Cisco Meeting Server
shutdown	Not available through MMP. Use Cisco UCS Manager to power down blade servers before removing power.	Do not use the vSphere power button. Use the **shutdown** command instead.
health	Not available through MMP. Use Cisco UCS Manager.	Not available
serial	Returns serial number of server.	Not available
dns	Do not specify an interface. For example **dns add forwardzone <domain-name> <server ip>**	Do not specify an interface. For example **dns add forwardzone <domain-name> <server ip>**
user evict	Available	Available

1.4 Differences in components enabled on the different platforms

The table below list the components available on the different Cisco Meeting Server platforms. If a component is not available on a platform, then the MMP and API commands specific to the component will not be available. For instance, the MMP and API commands for the TURN Server are not available on the Cisco Meeting Server 2000.

Component	on Cisco Meeting Server 2000	on Cisco Meeting Server1000/ Small and virtualized Cisco Meeting Server
Call Bridge	Available	Available
Web Bridge 3	Available	Available

Component	on Cisco Meeting Server 2000	on Cisco Meeting Server1000/ Small and virtualized Cisco Meeting Server
Database	Available	Available
Scheduler	Available	Available
TURN server	Not available	Available
Recorder	Not available	Available
Uploader	Not available	Available
Streamer	Not available	Available
SNMP MIB	Not currently available	Available

2 Installation

This chapter applies to deployments on specification-based VM platforms and Cisco Meeting Server 1000/Small.

2.1 Before You Start

2.1.1 About the Cisco Meeting Server software

The Cisco Meeting Server software is provided as an .ova file for VMware users. This is a template that sets up a new VM with a single network interface and a virtual disk containing the Cisco Meeting Server application.

After installation a fully functioning Cisco Meeting Server is available, which can be run as:

- a complete solution with all components enabled on a single server (single combined server deployment model),
- a split deployment with some components enabled on a Core server deployed on the internal network, and other components enabled on an Edge server deployed in the DMZ (single split server deployment model),
- a scalable and resilient deployment with multiple Call Bridges and databases, clustered together to support growth in usage and minimize downtime.

The same .ova file is used to install all deployments.

To upgrade the Cisco Meeting Server software follow the procedure in the release notes published for the software version.

Note:

- To avoid issues with Smart Licensing where Meeting Management is required, install a new Meeting Server every time instead of cloning the Meeting Server. Or, do a full factory reset to be able to reassign a new identical host id for the VM Meeting Servers that are already cloned.
- Meeting Server does not support secure boot.

2.1.2 Host requirements for the Cisco Meeting Server as a VM deployment

The Cisco Meeting Server runs on a broad range of standard Cisco servers as a VM deployment. Refer to this link for VM configuration requirements and UCS tested reference configurations for different deployments.

The Cisco Meeting Server also runs on third party servers including systems from Dell and HP containing Intel processors. Small form factor and ruggedized systems such as Klas VoyagerVM and DTECH LABS M3-SE-SVR2 are also supported. The software can be deployed on VMware ESXi as well as cloud services.

Table 2: Host requirements for the Cisco Meeting Server running on third party servers

	Minimum	Recommended
Server manufacturer	Any	Any
Processor type	Intel Nehalem microarchitecture microarchitecture	Intel Xeon 2600 v2 or newer
Processor frequency	2.0GHz	2.5Ghz
RAM	1GB per logical core*	1GB per logical core*
Storage	100GB	100GB

* additional memory should be available on the system for use by the hypervisor and any other VMs on the host.

Note: Meeting Server supports single and dual socket servers only.

Table 3: Recommended Core VM configurations

720p30 call legs	CPU configuration	RAM configuration	Example systems
50	Dual Intel E5-2680v2	32 GB (8x4GB)	Cisco UCS C220 M3 Dell R620 HP DL380p Gen8
40	Dual Intel E5-2650v2	32 GB (8x4GB)	Cisco UCS C220 M3 Dell R620 HP DL380p Gen8
25	Single Intel E5-2680v2	16 GB (4x4GB)	Cisco UCS C220 M3 Dell R620 HP DL380p Gen8
15	Single Intel E5-2640v2	8 GB (4x2GB)	Cisco UCS C220 M3 Dell R620 HP DL380p Gen8

In addition:

- All memory channels should be populated to maximize available memory bandwidth. There are no special requirements for NUMA systems.
- Out-of-band management systems should not be configured to share a network port with the VM. Internal testing has shown that they can cause bursts of packet loss and degraded voice and video quality. Out-of-band management should either be configured to use a dedicated network port or disabled.
- Where available, hyperthreading should be enabled on the host, without this there is capacity reduction of up to 30%.
- Cisco does not test or support AMD processor for virtual Meeting Server. It is recommended to use Intel processors for production deployments.
- The CPUs used by the Cisco Meeting Server must be dedicated for its use. This is achieved by:
  - only running a single VM on the host, or
  - pinning of all VMs on the host to specific cores and giving the Cisco Meeting Server sole use of the assigned cores, and in addition, leaving a physical core with no VMs pinned to it for the Hypervisor.
  - following the co-residency requirements for Unified Communication in a Virtualized Environment. Click on Cisco Meeting Server below the Meeting heading.
- If a VMWare Hypervisor with EVC mode enabled is used, the EVC must be set to one of the following modes or higher:

  "L2"/Intel® Nehalem generation (formerly Intel® Xeon Core™ i7)

  EVC modes which enforce compatibility with older CPUs than those listed above, are not supported as they will disable SSE 4.2; SSE4.2 is required.
- An activation key for the Call Bridge is required for media calls. To obtain the activation key, you need the MAC address of your virtual server. See Appendix B for information on licensing.

2.2 Installing via VMware on a specification-based server

Note: For every release of the Cisco Meeting Server for virtualized deployments, there will be an .ova file for a new deployment, and an upgrade image (.img) for upgrading to the latest release.

For a new installation follow this section; for an upgrade follow the release notes.

- If a VMWare Hypervisor with EVC mode enabled is used, the EVC must be set to one of the following modes or higher:

  "L2"/Intel® Nehalem generation (formerly Intel® Xeon Core™ i7)
  EVC modes which enforce compatibility with older CPUs than those listed above, are not supported as they will disable SSE 4.2; SSE4.2 is required.
- An activation key for the Call Bridge is required for media calls. To obtain the activation key, you need the MAC address of your virtual server. See Chapter 1 and Appendix B for information on licensing.
- When uploading OVA to Vcenter and deploying, the Publisher field should show (Trusted certificate). If you see a warning for an invalid certificate and not-trusted cert when importing the OVA, see this article: https://kb.vmware.com/s/article/84240. You may have to add the intermediate and root certifcates corresponding to the certificate used to sign the OVA, to the VECS Store. To procure intermediate or root certificates or any other issues, contact Cisco Technical Support.

2.3 Deploying Meeting Server

Meeting Server can be deployed:

- with ESXi Web Client
- Nutanix cluster deployment
- Using NFVIS

2.3.1 Deploying Meeting Server from the OVA file with ESXi Web Client

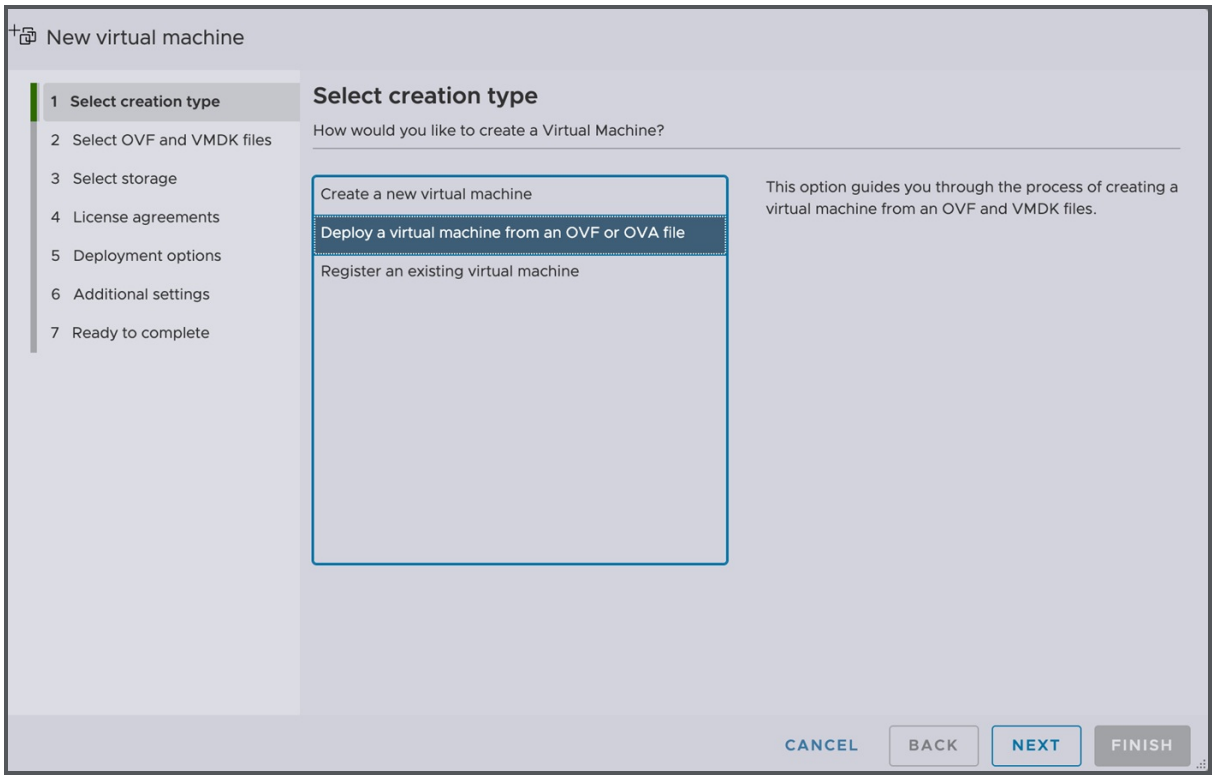
Cisco Meeting Server 1000/Small is shipped without any pre-loaded software. Follow the instructions in the section below to install the Meeting Server software.

For every release of the Cisco Meeting Server for virtualized deployments, there will be an .ova file for a new deployment, and an upgrade image (.img) for upgrading to the latest release.

Note: During the OVA installation for version 4.0, you may encounter a certificate expiry warning. Select Ignore to proceed with the deployment.

For a new installation follow this section; for an upgrade follow the release notes.

1. Download the .ova file from the Cisco website.
2. In the vSphere Client go to the host in the **Navigator** tab on the left and select **Create/Register VM.**
3. For **Select creation type**, select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.



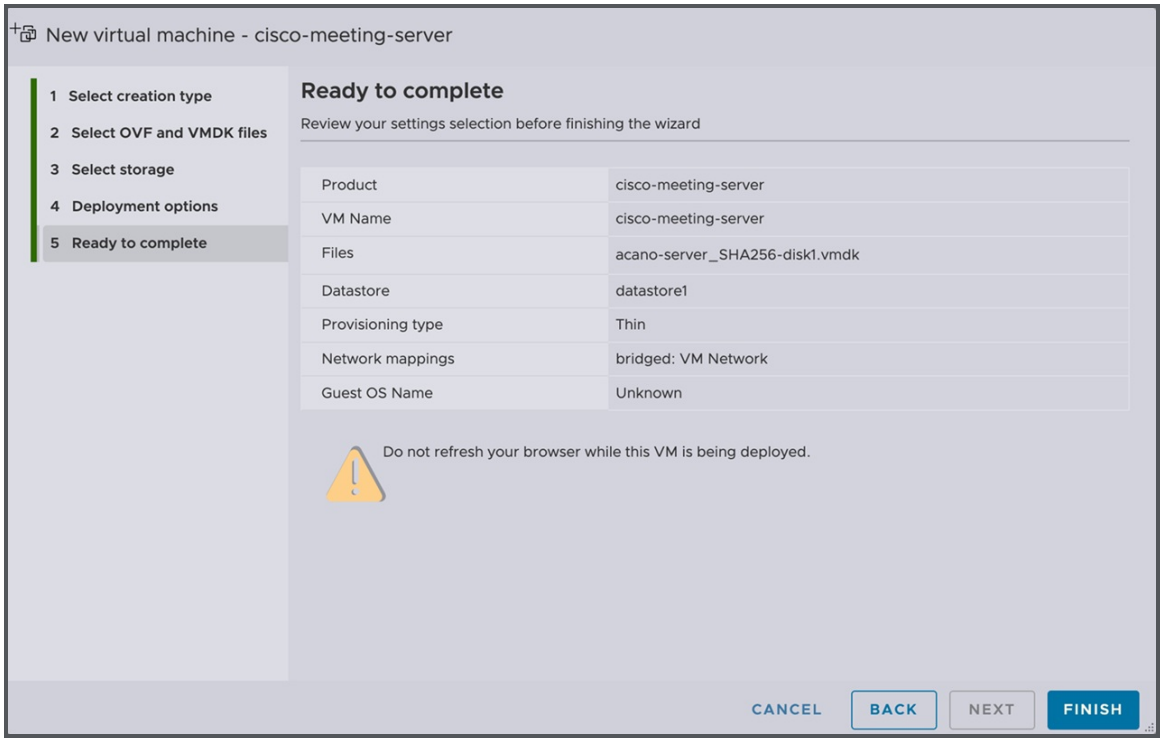
4. Enter the desired name for the virtual machine and browse or drop the .ova file (downloaded in step 1) to select it.
5. Follow the wizard instructions. The settings that must be selected are:
   a. Select the datastore to store the VM configuration and disk files.
   b. Select the network mapping you would like the VM to be connected to.
   c. Set Disk provisioning to **Thick**.
   d. Ensure **Power On After Deployment** is not selected.
   e. Click **Finish**.

Note: Depending on how your virtual host is set up, some of the wizard settings may not

---

be displayed or may not be selectable.

f.



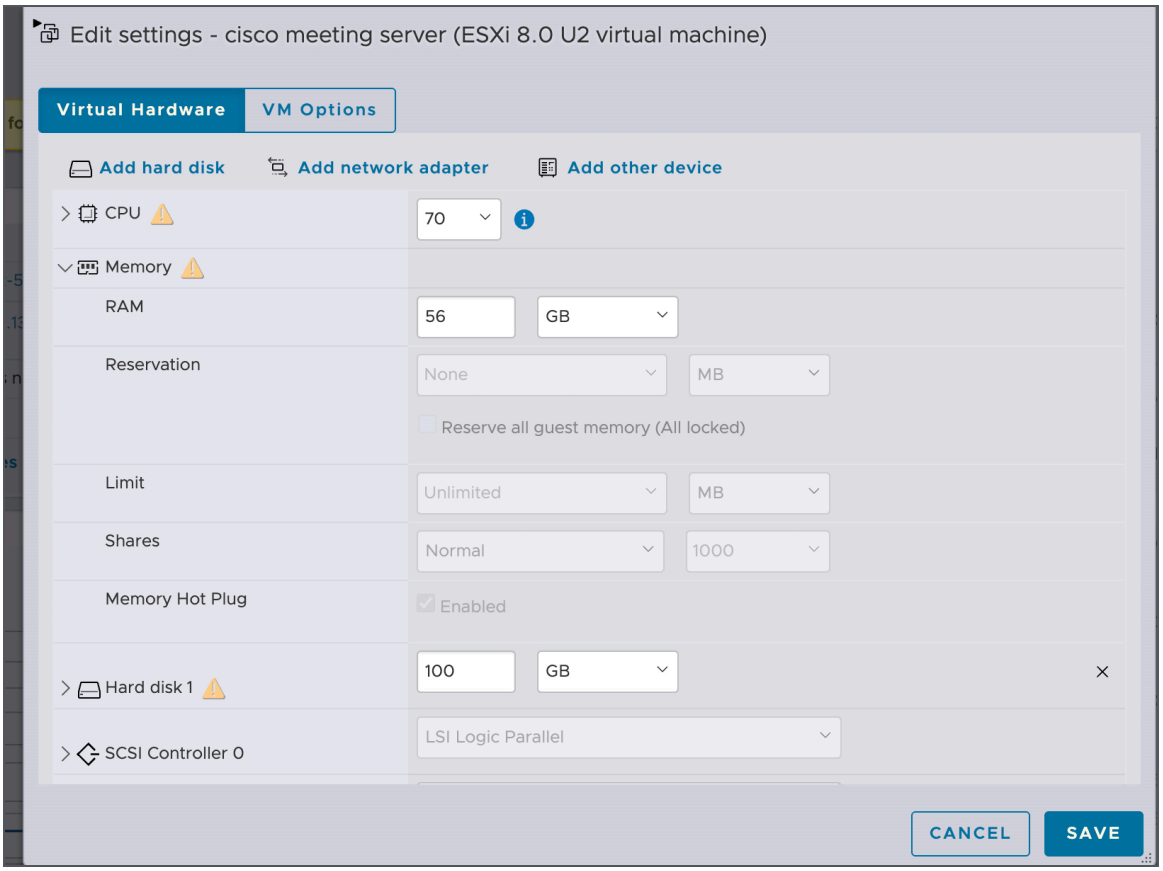
6. Once completed, the new Cisco Meeting Server VM should now be listed in your **Virtual Machines**.
7. Select the Cisco Meeting Server VM from your list of VMs.
8. From the **Actions** button, select **Edit Settings...**.
   a. Edit **VM settings** and click **CPUs**. Set **Number of CPUs** to the desired number (where 4 is the minimum). See the deployment guide for scaling details. For more information on VM configuration requirements, see https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-meeting-server.html and Appendix D.
   b. Set **Number of Cores per Socket** to one of the following:
      - On a dual processor host with hyperthreading, set **Number of Cores per Socket** to the number of logical cores minus 2.
      - On a dual processor host without hyperthreading, set **Number of Cores per Socket** to the number of logical cores minus 1.
      - On a single processor host, set **Number of Cores per Socket** to the number of logical cores.

We recommend that you configure the number of sockets to mirror underlying hardware.

Note: The number of logical cores can be found on the vSphere Web Client, by clicking **Manage > Settings > Processors**. For more information, see: https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/8-0/esxi-installation-and-setup-8-0.html.

---

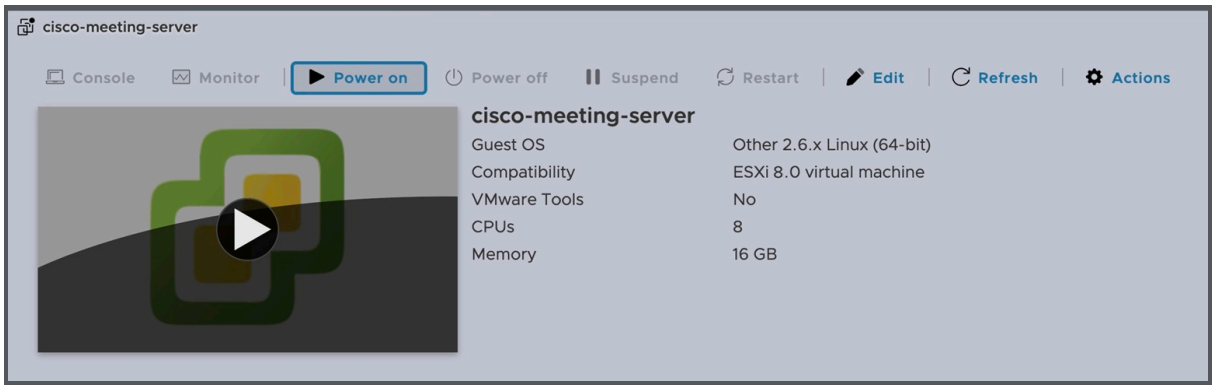
c. Click Memory and ensure the RAM is set to a minimum of 4GB.



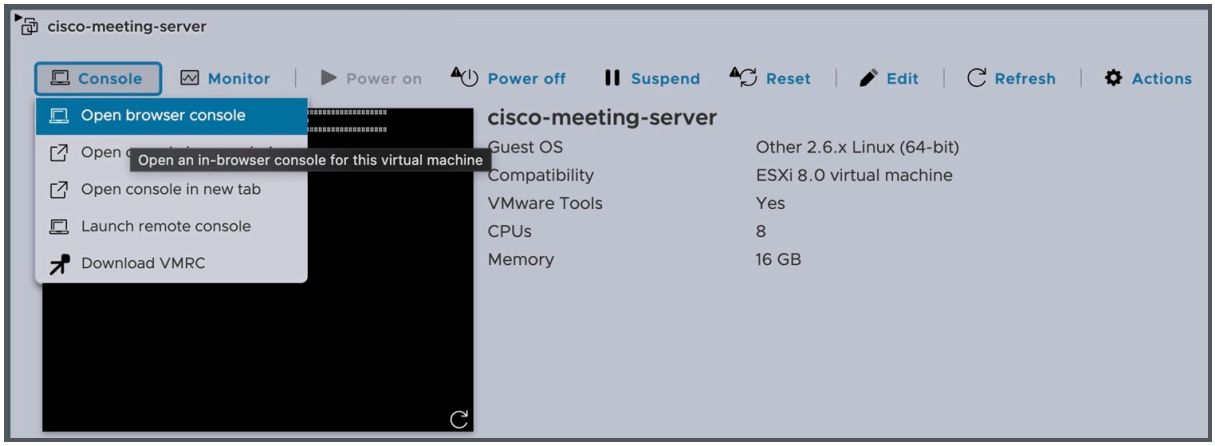
i. Select the **Reserve all guest memory (All locked)** checkbox.

d. Set the disk space to 100GB.

9. Click **Power on.**



10. Click the **Console** tab and open the browser console (or remote console if VMware Remote Console is installed).



11. Log in with the user name “admin” and press the “Enter” key to skip the password field. You will be asked to change the admin password. You are now logged into the MMP.

2.3.2 Deploying Meeting Server on Nutanix Cluster

The following section provides details about deploying Meeting Server on Nutanix cluster. Nutanix is supported on 220 M7+ HCI Nodes.

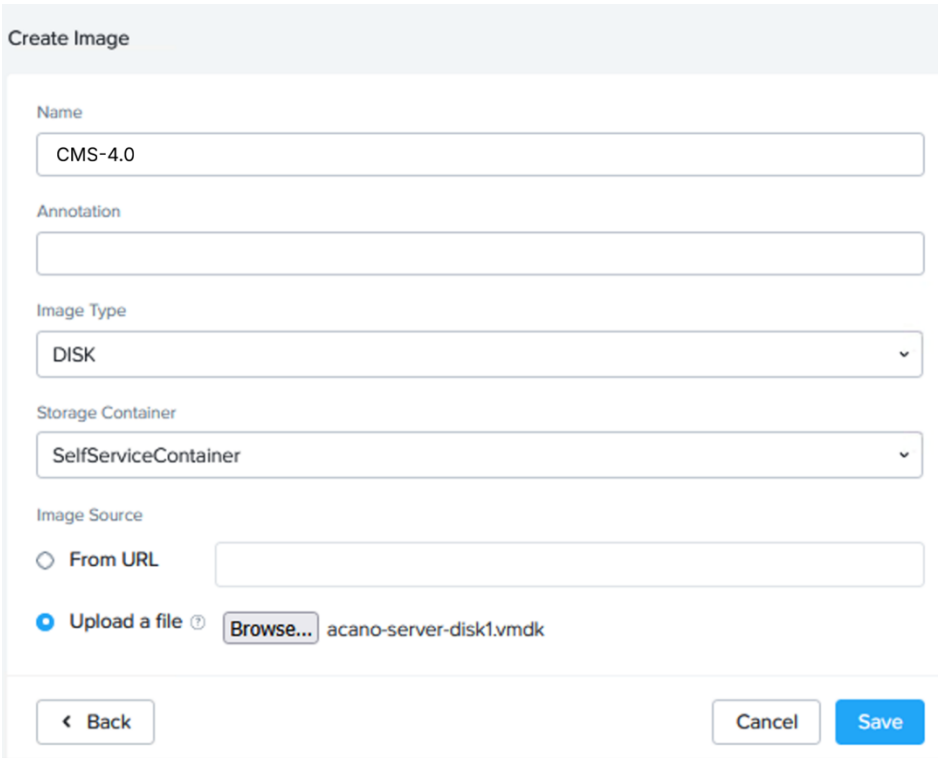
Prerequisites:

1. Nutanix Cluster(AHV: 10.3.1.2, AOS: 7.3.1.2) setup and Prism Element login is accessible.
2. Download and Extract the Meeting Server OVA file
   a. Navigate to the Cisco Connection Online CCO page and download the OVA file : (ie. Cisco_Meeting_Server_4_0.ova)
   b. Extract the downloaded OVA file to obtain the VMDK file : (ie. acano-server-disk1.vmdk)

Note: Meeting Server support on Nutanix is limited to fresh installations. Direct migration of Meeting Server virtual machines from ESXi to Nutanix is not supported; however, existing Meeting Server Virtual Machines in-line to 3.13 version on ESXi can be moved to Nutanix deployments using the backup/restore feature.

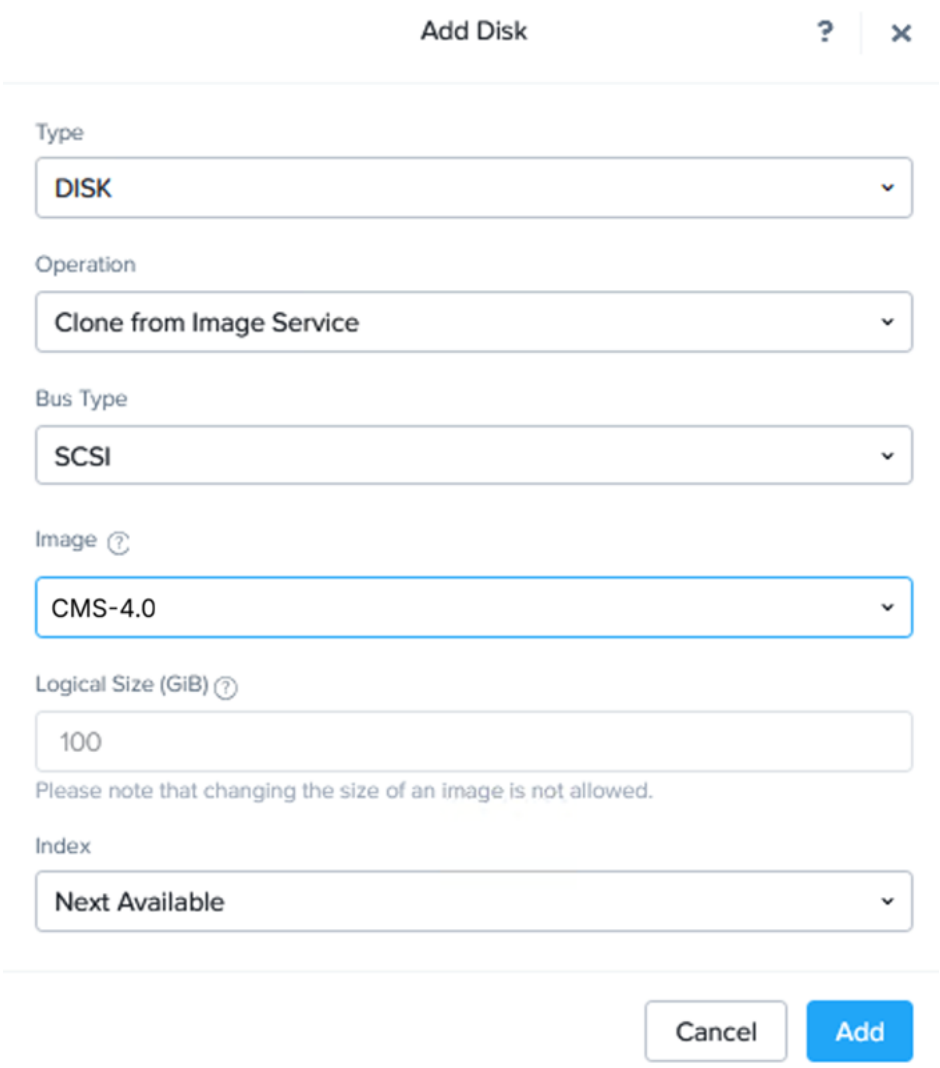
Installation steps:

1. Configure Image
    a. Login to Prism Element and go to **Settings** page and navigate to **Image Configuration**. Click **Upload Image** and provide following details,
        - **Image Name**: Enter a name for the image.
        - **Image Type**: Select Disk from the drop-down list.
        - **Storage Container**: This will be automatically selected based on the cluster configuration.
    b. Select **Upload a file** and upload the extracted VMDK file in the **Image Configuration** settings of Prism Element (refer prerequisites step 2).
    c. Click **Save** to create an Image.



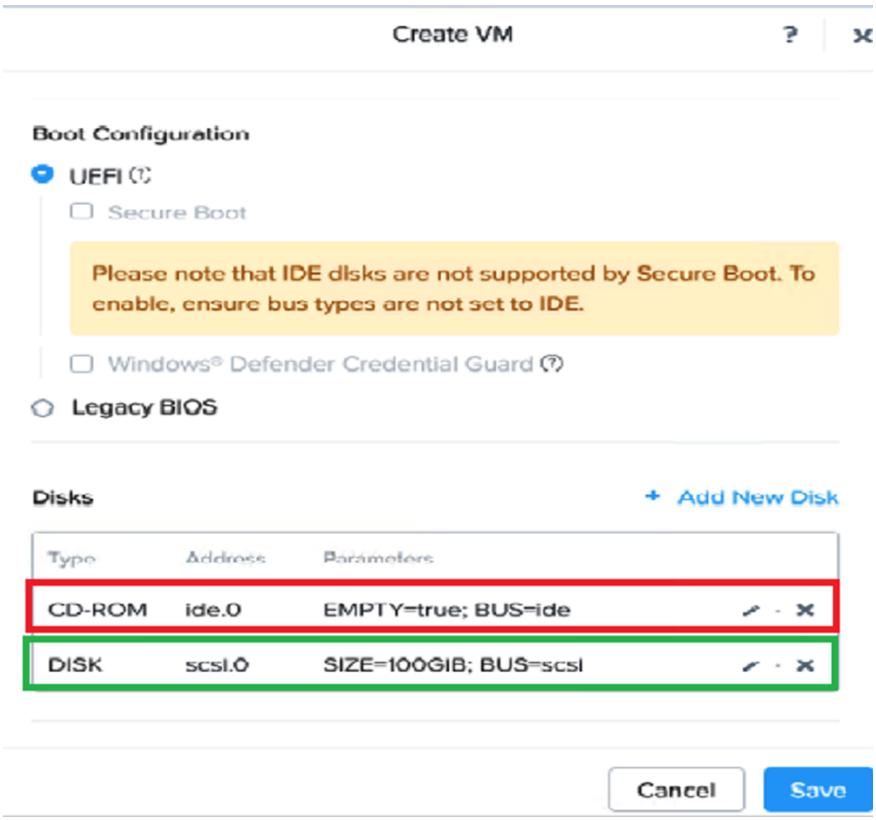
2. Deploy the Meeting Server Virtual Machine
    a. Navigate to the **VM** tab under **Settings**. Click **Create VM** on the top-right corner of the screen.

b. Configure the VM settings:
    - **General Configuration**: Specify General Configuration details.
        - **Name**: Specify VM name
        - **Description**: (Optional)
        - **Time Zone**: Click and select required time zone.
    - **Compute Details**: Specify Compute details.
        - **vCPU**: 8.
        - **Number of cores per vCPU**: 1.
        - **Memory**: 16 GB.
c. Select **UEFI** for **Boot configuration** (ensure Secure Boot is disabled).
d. Under **Add Disk**:
    - In the **Disks** section, click **Add New Disk**.
    - **Type**: select **Disk** from the drop-down list.
    - **Operation**: select **Clone from Image Service** from the drop-down list.
    - **Bus Type**: select **SCSI** from the drop-down list.



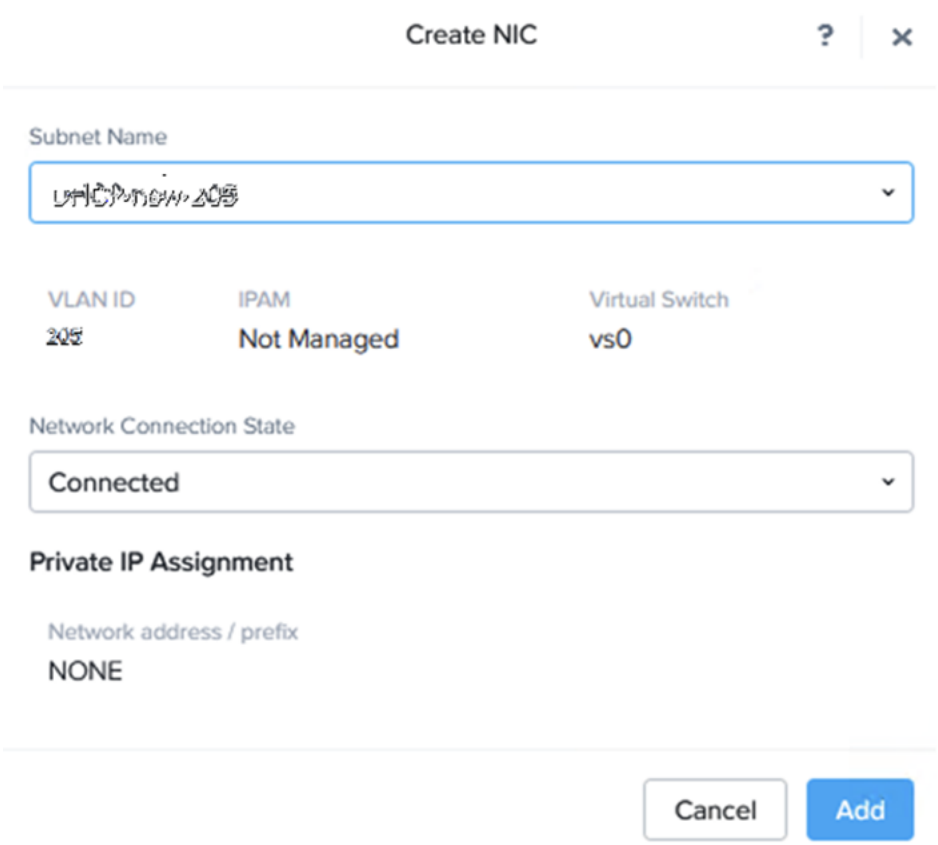
- Under **Image**, select the image created in the previous step from the drop-down list (If multiple images exist, choose the appropriate one).
- Note that **size** value gets auto assigned based on corresponding image file
- **Index** will be automatically selected as **Next Available**.

Note: keep only above added disk and remove if any other default disks (example: remove disks CD-ROM).



e. Add Network Adapter (NIC)

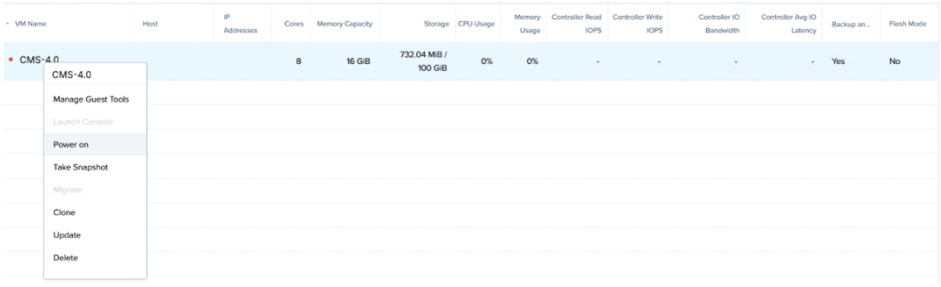
- In the **Network Adapters** section, click **Add New NIC**.
- Select desired **Subnet**.
- Click **ADD** to add new NIC.
- Click **Save**.



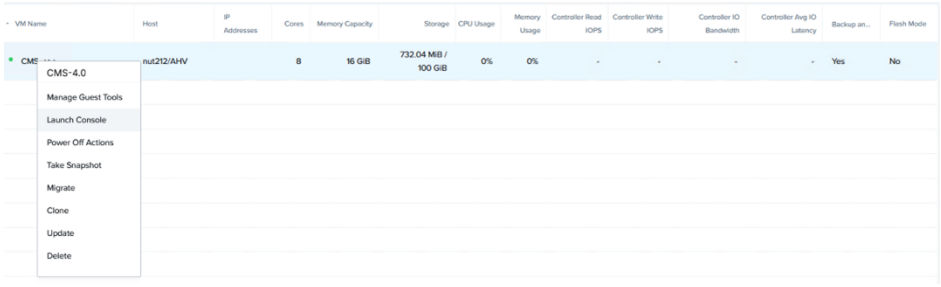
f. Ensure successful status



3. From VM page, select and right click on the installed VM and choose **Power On**.



4. After the VM is powered-on and connection is established, select and right click on the VM and choose **Launch Console**.



5. Login with the username "**admin**" and press "Enter" key to skip the password field (for freshly deployed vm), subsequently new password requirements need to be completed and then Meeting Server VM is all set for further configurations(Webadmin, Webbridge3, Callbridge, etc) and usage.

2.3.3 Deploying Meeting Server Using NFVIS

Starting with version 4.0, Cisco Network Function Virtualization Infrastructure Software (NFVIS) provides the virtualization platform for hosting and managing Cisco Meeting Server virtual instances. It delivers a streamlined and reliable foundation for the meeting environment.

Components	Version
NFVIS Version	26.2.1-FC1
Server Model	BE7K(BE7M-M7-K9)
CMS Version	4.0

For the detailed instructions about installing NFVIS and starting the management portal, refer to the Cisco Network Function Virtualization Infrastructure Software Getting Started Guide, Release 26.x and Later - Install Cisco Enterprise NFVIS Using CIMC [Cisco Enterprise NFV Infrastructure Software] - Cisco

Note: Use the following URL to access the NFVIS environment.

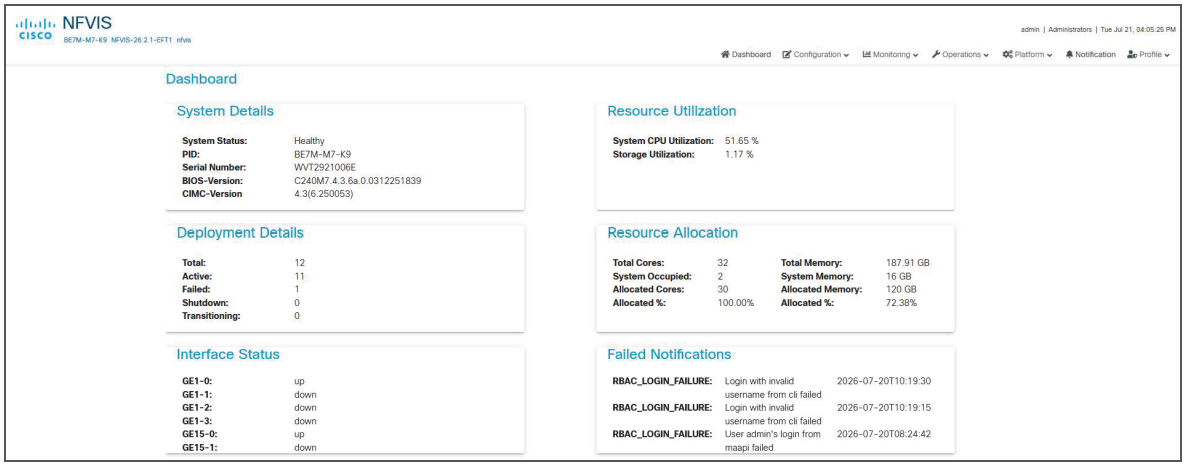
Components	Version
NFVIS Mgmt	Portal URL: https://<NFVIS-mgmtip>
Credentials	username :admin , Password :< configured-password>

1. Log in and verify NFVIS health
   a. Open a browser and navigate to **https://<NFVIS-management-IP>**
   b. Log in using the following credentials:
      i. **Username**: admin
      ii. **Password**: <configured-password>

c. After you log in, the **Dashboard** page appears. Confirm that:

   i. The system status is **Healthy.**

   ii. The displayed **PID** matches the expected product ID.

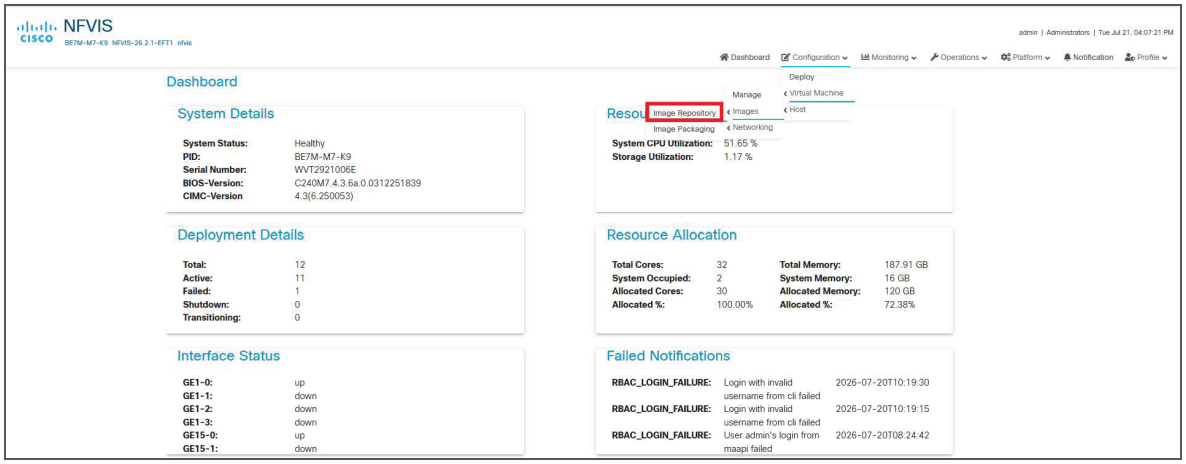


2. Upload the Image to the **Image Repository**

   2.1 Navigate to the Image Repository

   a. From the top menu bar, choose **Configuration > Image Repository**.

   b. Verify that the **Images** page opens and displays the **Image Upload and Information** section.



   2.2 Upload the **Image**

   a. Click the **LOCAL** tab to upload the image from your local computer.

   b. Click **Select File**, browse to the **CMS** image, and select .ova file.

   c. Configure the required upload parameters.

d. Add the boot mode property:

   i. Click **Add Property**.

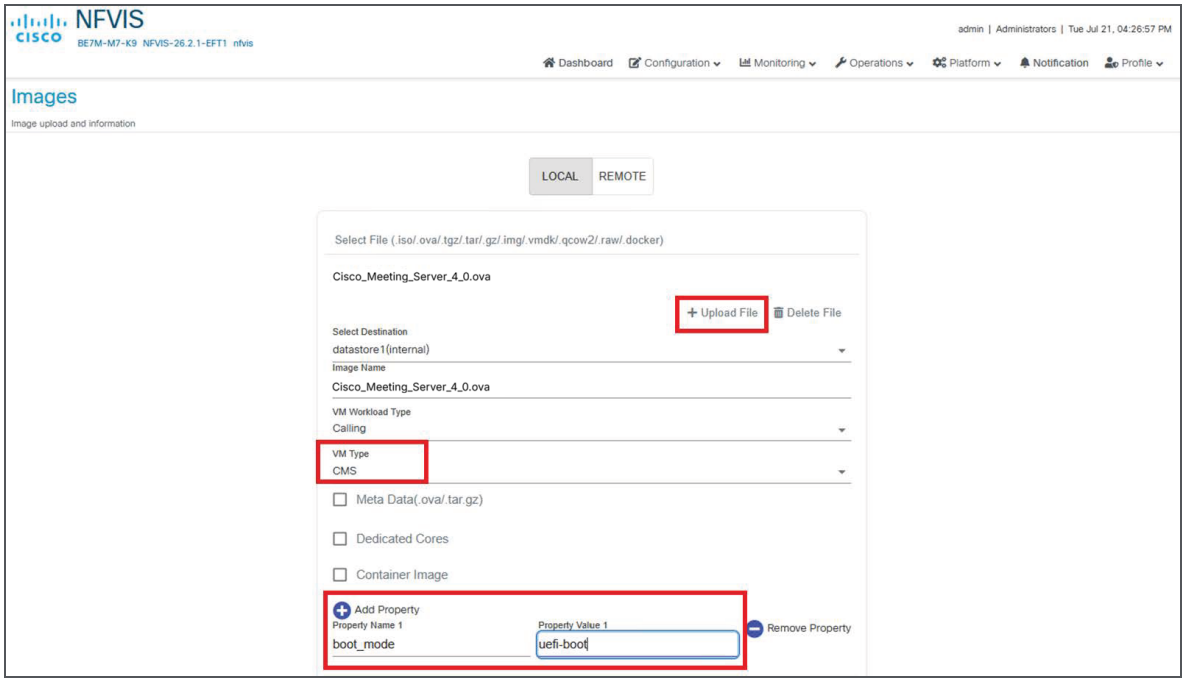
   ii. In **Property Name**, enter boot_mode.

   iii. In **Property Value**, enter uefi-boot.

Note: Adding the **boot_mode** property is required for the Meeting Server deployment. This is the key difference between the Meeting Server and Meeting Management deployment procedures.

Field	Value
Select Destination	datastore1 (internal)
Image Name	Cisco_Meeting_Server_4_0.ova
VM Workload Type	Calling
VM Type (from drop-down)	CMS
Property Name	boot_mode
Property Value	uefi-boot

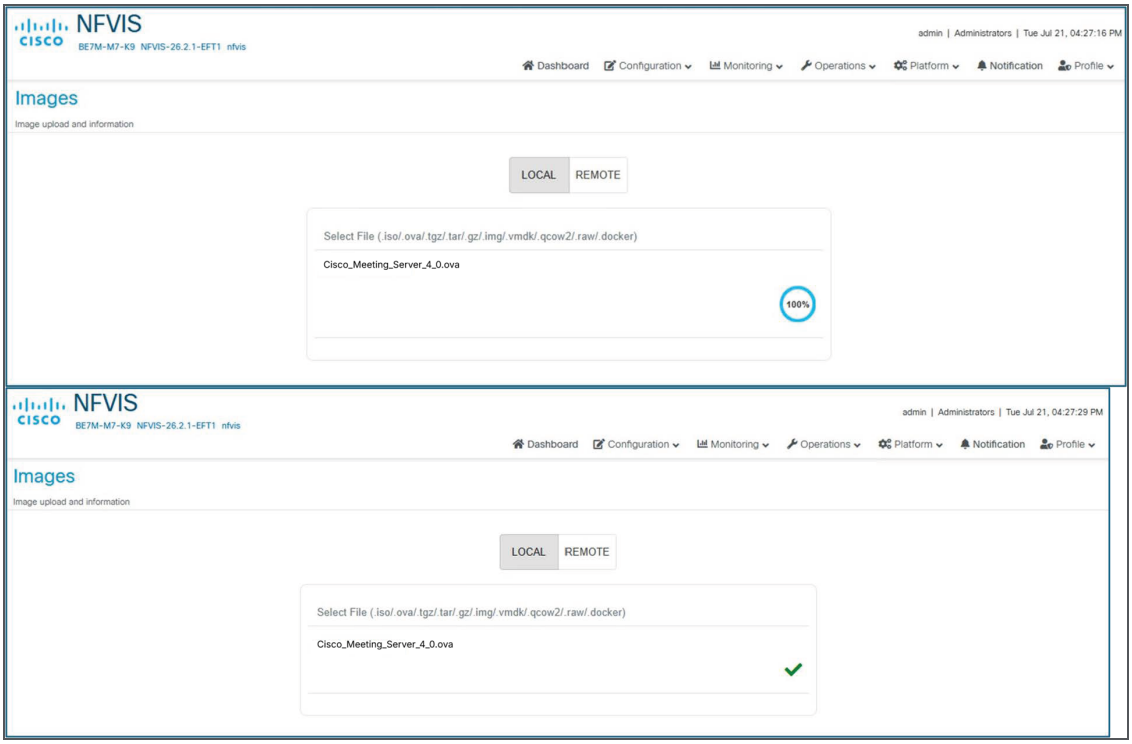
e. After adding the required property, click **+ Upload File** to begin uploading the image.



2.3 Monitor the **Upload** Progress

a. Verify that the **Image Upload Started** notification banner appears and monitor the upload progress percentage.

b. Wait for the upload to complete. A **green check mark** appears to confirm that the image was uploaded successfully.



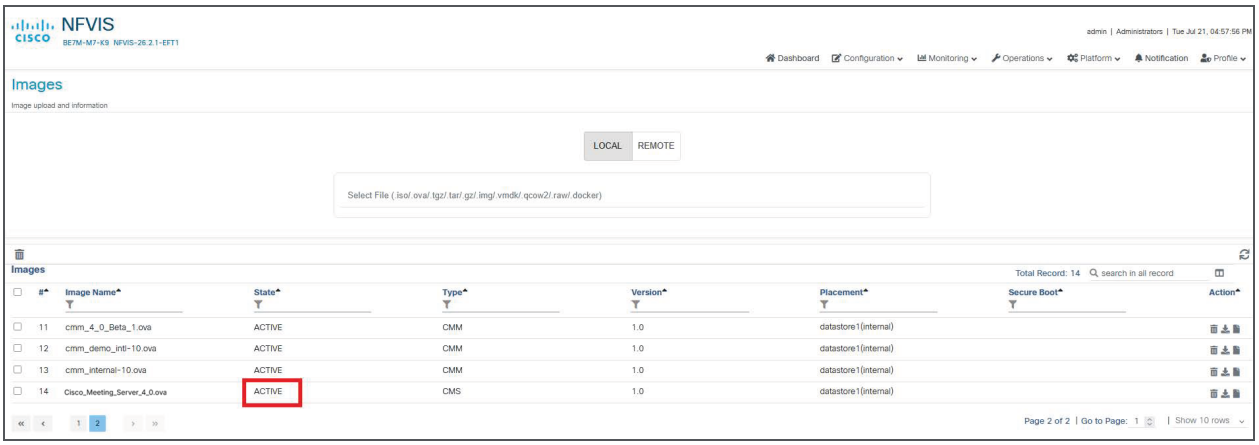
2.4 Verify the **Uploaded** Image

a. Verify that the uploaded image appears in the **Images** table.

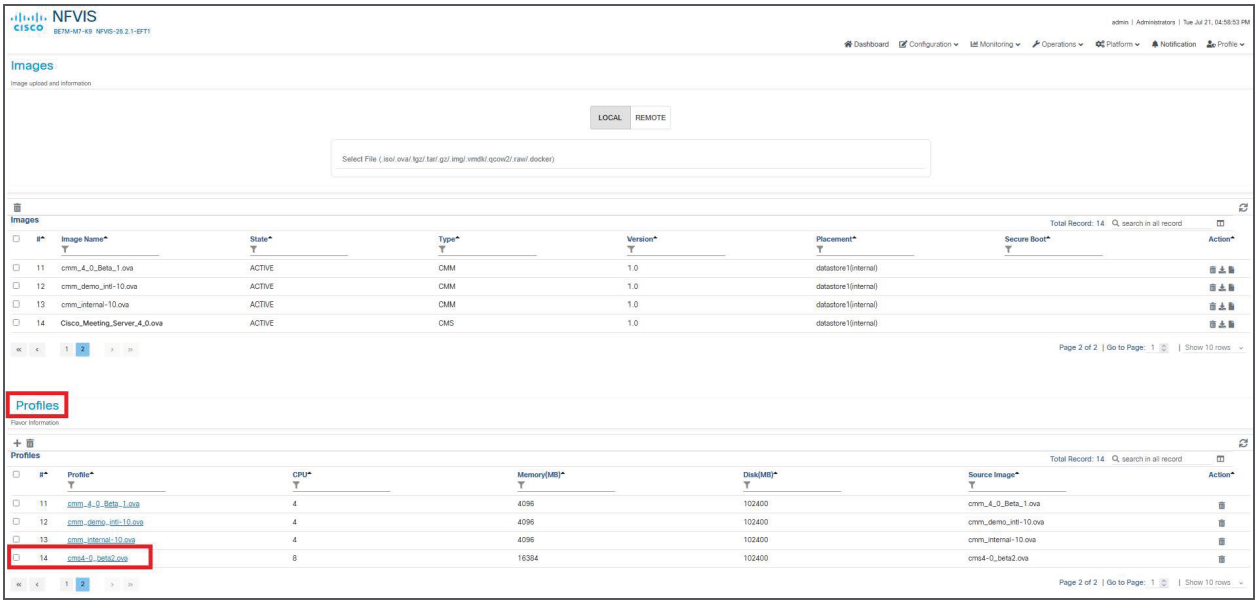
b. Confirm that the image state transitions from **CREATE** to **ACTIVE.**

c. Confirm that a profile has been created for the **image**.

Note: Do not proceed with the deployment until the image state is **ACTIVE**.



d. After the image has been uploaded successfully and verified in the Images list, confirm that the associated **VM profile** has been created.



3 Install Cisco Meeting Server

3.1 Navigate to the **Deployment Page**

a. From the top menu bar, choose **Configuration > Deploy Virtual Machine**.

b. Verify that the deployment page displays the following sections:

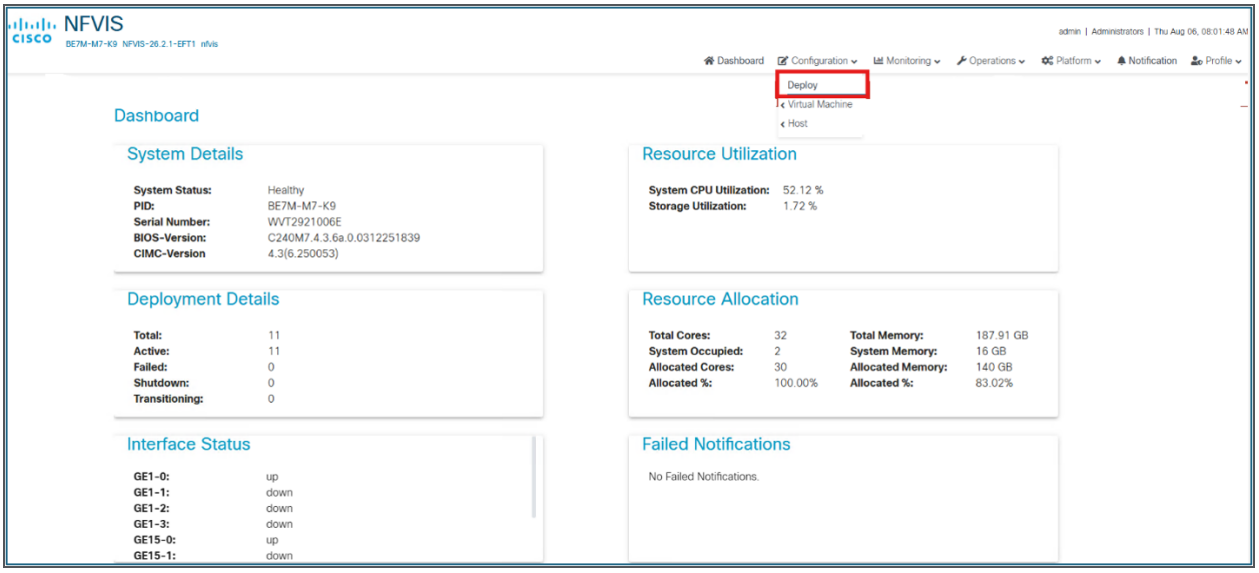
   i. **Left panel:** Network topology showing the existing VMs and network ports: GE15-0, GE1-1, GE1-2, GE1-3, GE3-0, GE3-1, GE3-2, and GE3-3.

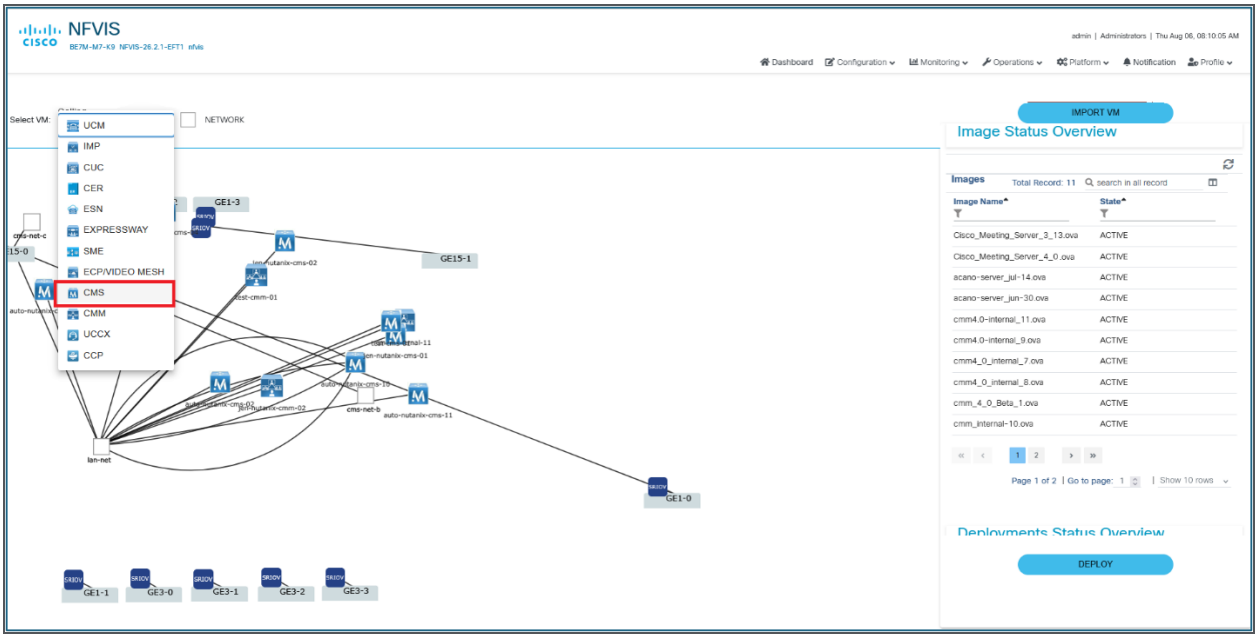
   ii. **Right panel: Image Status Overview** and **Deployments Status Overview.**

3.2 Choose the **VM Type**

a. From **VM** drop-down list in the upper-left corner, then choose **Calling** as the category.

b. From the subcategory drop-down list, choose **CMS**.





3.3 Enter the **Deployment Details**

In the **Deployment Details** panel on the right, enter the following details:

Name	CMS
Image	Cisco_Meeting_Server_4_0.ova
Group Name	(leave blank or set as needed)

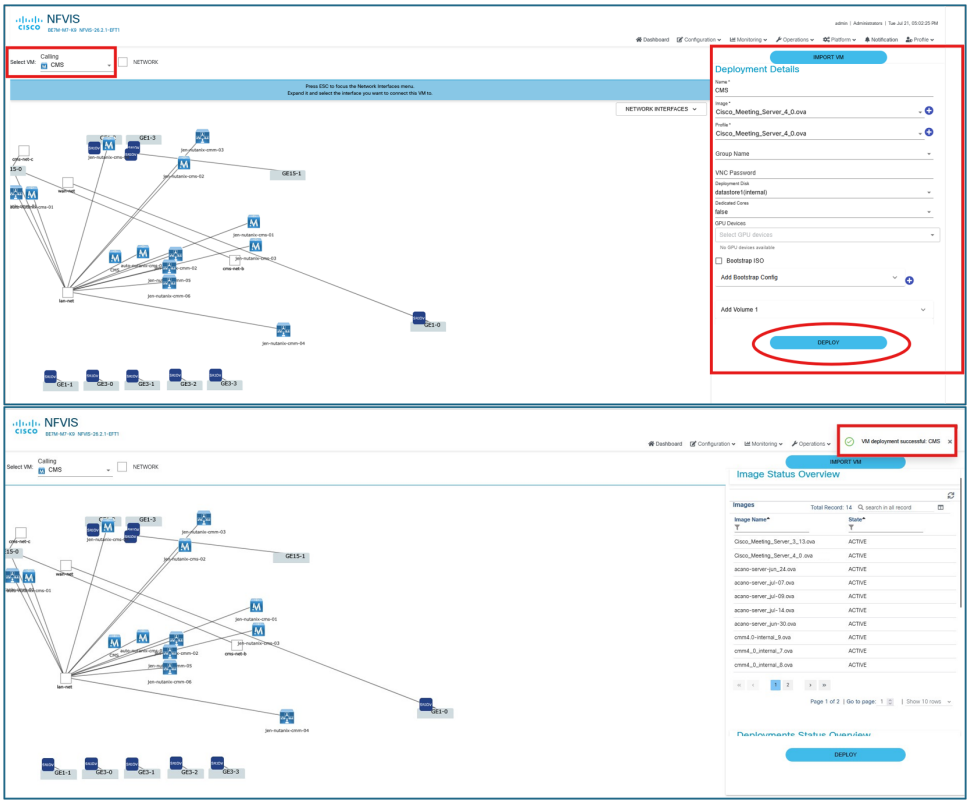
Name	CMS
VNC Password	(optional)
Deployment Disk	datastore1 (internal)
Dedicated Cores	false
GPU Devices	(none – No GPU devices available)
Bootstrap	ISO (unchecked)
Add Bootstrap Config	(optional)
Add Volume 1	(optional)

3.4 Execute the **Deployment**

a. Click **DEPLOY** at the bottom of the Deployment Details panel.

b. Wait for the following success notification to appear:

VM deployment successful: CMS

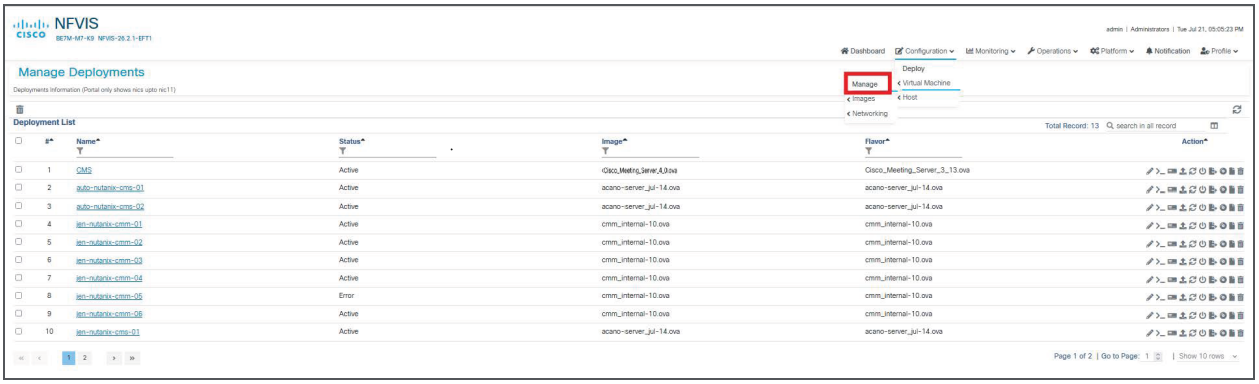


4 Verify the **Deployment Status**

4.1 Navigate to Manage Deployments

a. From the top menu bar, choose **Configuration > Manage Virtual Machine**.

b. Verify that the Manage Deployments page opens and displays all deployed VMs.



4.2 Confirm that the VM is Active

a. Verify that the newly deployed VM appears in the **Deployment List** with its status set to **Active.**



5 Configure the **VM Network**

5.1 Edit the **Deployed VM**

a. On the **Manage Deployments** page, locate the deployed **CMS** VM.

b. In the **Action** column, click the **Edit** (pencil) icon.

5.2 Assign the **Network Interface**

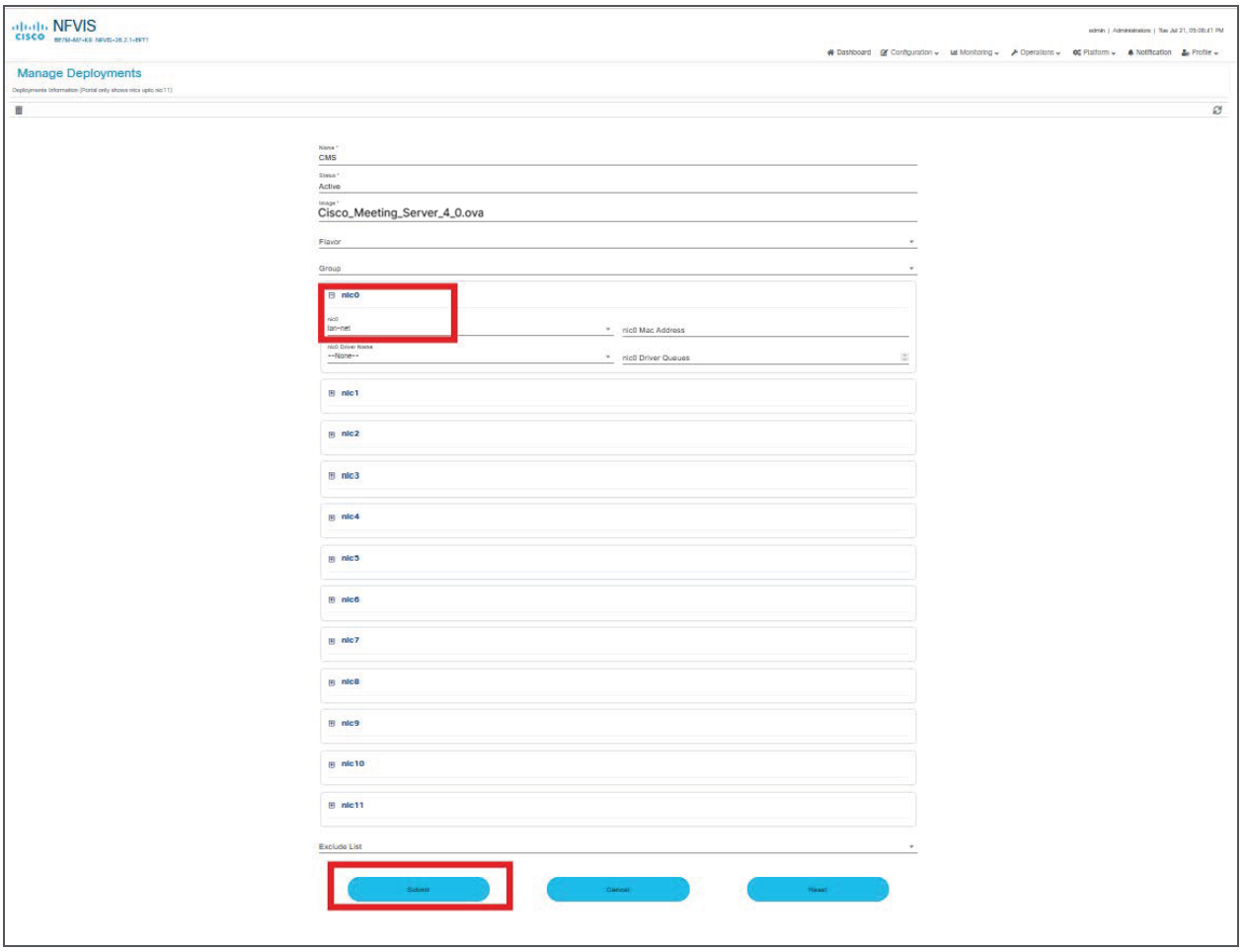
a. On the **Edit** page, configure the following network interface settings:

Name	CMS
Status	Active

Name	CMS
Image	Cisco_Meeting_Server_4_0.ova
Flavor	Cisco_Meeting_Server_4_0.ova
(select network group)	(select network group)
nic0	lan-net
nic1 – nic11	(leave default unless additional NICs are required)



b. Click **Submit** to apply the network configuration.

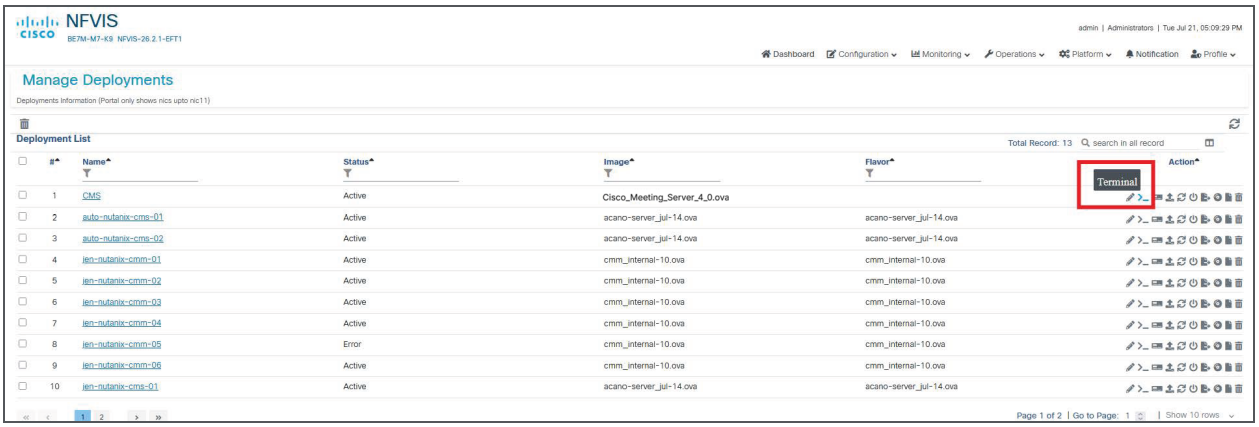


6 Access the VM Console

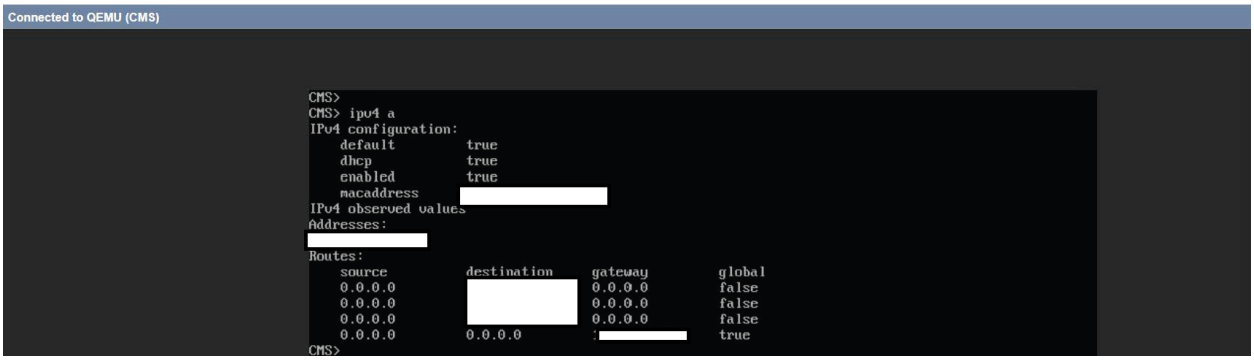
a. On the **Manage Deployments** page, locate the deployed **CMS** VM.

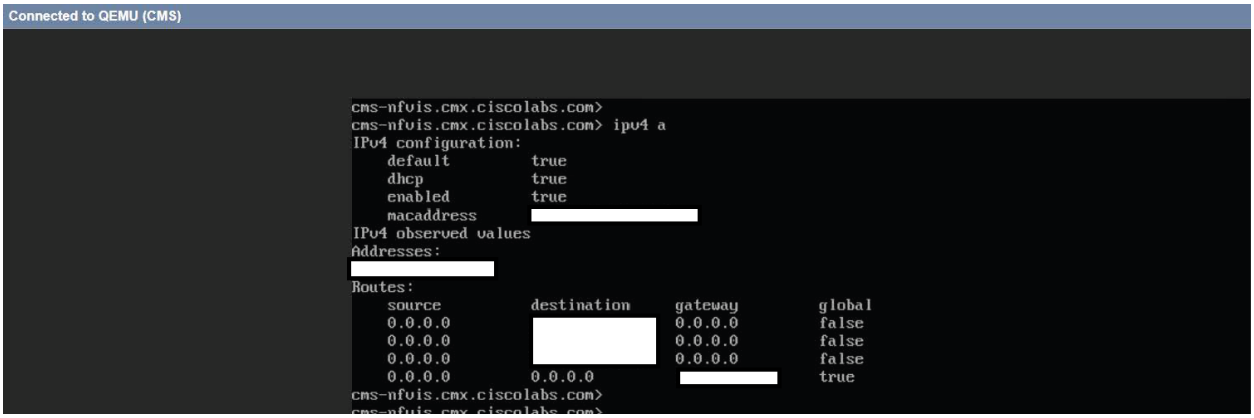
b. In the **Action** column, click the **Terminal** (console) icon.

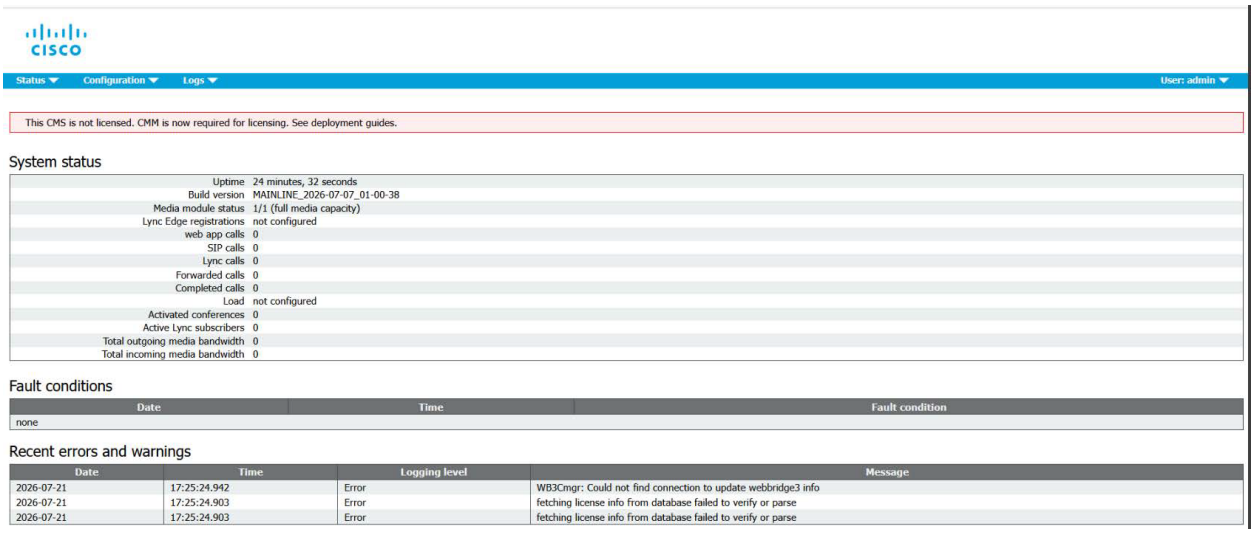
c. Verify that a terminal session opens and connects directly to the deployed VM.



d. Use the terminal session to perform the initial setup, configure the VM, or troubleshoot issues.







2.4 Installing and initial configuration of Cisco Meeting Server Small/1000

2.4.1 Before You Start

Cisco Meeting Server Small will not be shipped with VMWare pre-installed. Users must purchase ESXi and licenses from VMWare as Cisco is no longer entitled to sell VMWare licenses. Refer to ESXi installation and setup 8.0 for steps on VM ware Installation.

2.4.2 Task 1 – Unpacking and initial startup

1. Unpack the Meeting Server, power cords, console adaptor, and rack kit.
2. Position the Meeting Server or optionally rackmount – see the Cisco UCS C220 M6 Server Installation and Service Guide and Cisco UCS C220 M7 Server Installation and Service Guide for your deployment.
3. Connect the Ethernet cables to the Ethernet1 port on the rear of the Meeting Server and connect to the Ethernet network.
4. Connect the power cords to each power supply and connect to power.
5. Press the power button on the front of the Meeting Server. It will automatically stop and restart itself more than once after initial power on.
6. Connect a console to the Meeting Server to continue. You can use either a monitor and keyboard, or use a virtual console over a network connection. Select from the following options:

2.4.2.1 Console Option 1 – Monitor and keyboard

1. Attach a monitor with a VGA connection to the VGA port on the rear of the Meeting Server, or to the console port on the front.
2. Connect a keyboard to the USB ports located on the rear of the Meeting Server, or to the console port on the front.

2.4.2.2 Console Option 2 – Virtual console over network

Use this method if no monitor and keyboard are available to connect to the Meeting Server:

1. Connect your computer's serial port to the RJ-45 port on the rear of the Meeting Server labeled 10101 using the standard blue Cisco RJ-45 to DB-9 Null Serial cable provided with routers and switches.
2. Open your terminal program, select the COM port for your serial port/adaptor and set the terminal settings to 115200 baud, No Parity, 8 data bits, 1 stop bit.
3. Connect a second Ethernet LAN port to the RJ-45 port on the rear of the Meeting Server labeled M1. If you only have the resources for one network connection, remove the LAN

connected to Ethernet1 and use it for the M1 port temporarily to enable the virtual console, and move it back to Ethernet1 after configuration. The M1 port must be connected and configured with a valid IP address to use the virtual console.

4. Ensure Meeting Server has its power supplies connected. If not, ensure it has been plugged in for several minutes to allow the CIMC management interface to startup. Meeting Server does not have to be powered on for CIMC to function, but must be connected to power. (There is no external indicator for CIMC status.)
5. In your terminal program, press Escape and the 9 keys simultaneously to switch the port to CIMC. A username prompt displays.
6. Enter the default username and password .
7. The first time you login, you will be prompted to change the password to one of your choice. Complete the prompts to set a new password.
8. Once logged in, at the command prompt enter the command **`scope cimc`** – the command prompt changes to reflect that you are now in the CIMC menu.
9. Enter the command **`show network detail`** to show the current configuration of the management Ethernet interface, including the current IP address the server has aquired via DHCP (if available on the network). Make a note of the IPv4 address shown (if DHCP is available).
10. If DHCP is not available and you need to set a static IP, use the following commands, changing the sample values to ones appropriate for your network. (These commands assume you are already in the CIMC scope.)

```
scope network
set dns-use-dhcp no
set dhcp-enabled no
set v4-addr 10.1.2.3
set v4-netmask 255.255.255.0
set v4-gateway 10.1.2.1
commit
```

11. Enter **`show network detail`** to confirm your changes. Once complete, enter the command **`exit`** twice to log out of the CIMC.
12. Switch to your PC's browser, and browse to the IP address you configured or obtained from the CIMC serial interface. Dismiss the certificate security warnings and a Cisco landing page with username and password fields will display.
13. Login with the username of **`admin`** and the password you set when first connecting to the CIMC.
14. When the Server Summary page loads, click the Launch KVM Console link under Actions. The JAVA virtual console application loads. Depending on your Operating System and browser you may get security warnings and dialogs to acknowledge and accept.

Continue until the application loads—it will show the monitor image as if you were directly connected to the server. If the server is powered off, it will show a larger green window saying **No Signal**.

15. If the server is powered off, from the **Power** menu, select **Power On** to start the server. After a few minutes it should boot to the VMware console screen.

You can now use the virtual console the same as if you were connected using a local monitor and keyboard.

2.4.3 Task 2 – Configuring VMware Network Management

You must have console access to the server via monitor or virtual console to complete the following steps.

Ensure the server is powered on and the VMware console screen displays, offering press **F2** to configure or **F12** to shutdown.

1. Press **F2** to configure the server.
2. From the menu options, use the arrow and Enter keys and select **Configure Management Network** and then **IPv4 Configuration**.
3. Select the option for the network configuration you will use (DHCP or Static IP assignment) and configure the IPv4 Address, Mask, and Gateway as appropriate for your network.
   REMINDER: This IP address is for the VMware Hypervisior, not the Meeting Server application. The address used must be unique from the Meeting Server application.
4. (Optional) If you will access the Hypervisor management via a different VLAN from the Meeting Server application, configure the VLAN that the Management Interface should associate with.
5. Press **Escape** to return to the main menu, and **Escape** again to log out.

   The VMware management IP address displays in the bottom left of the screen.

2.4.3.1 Useful information if you are using the virtual console

- CIMC is a powerful out-of-band management interface for the Meeting Server and is recommended for use when the Meeting Server is installed in a rack or computer room. This management interface is not used by VMware or the Meeting Server application, so if you want to keep it connected, you must secure a dedicated LAN connection for the M1 Ethernet port. (NIC sharing options are also available in the Cisco UCS Server documentation.)
- If you are using the virtual console with only one network connection and had been temporarily using it for the M1 interface:

a. You will not need the virtual console anymore to complete the install. Disconnect the Ethernet cable from the M1 interface of the server and reconnect it to the Ethernet1 port.

b. If you are using DHCP for the VMware management interface, you will need to restart the server to obtain a new IP address after connecting the Ethernet cable. To restart, press the power button on the front of the server briefly and the server will initiate an automatic shutdown (this takes several minutes). After it powers off, power it back on using the power button. Because you disconnected the network that the virtual console was using, you will not be able to see the IP address the server obtained. To find the IP address, contact your DHCP administrator to find which IP address the server was assigned. The MAC address of the Ethernet1 interface can be found on the pull-out tab located on the front of the Cisco Meeting Server Small.

You should now have Ethernet connected to the Ethernet1 port on the rear of the server and know the IP address in use by the VMware management network.

2.4.4 Task 3 – Retrieving and activating VMware Licenses

Cisco does not provide VMware licenses. Users must purchase licenses from VMWare as Cisco is no longer entitled to sell VMWare licenses. You require two 1-CPU licenses per Cisco Meeting Server Small.

2.4.4.1 Activate VMware activation keys

1. Once the licenses have been added to your VMware account, the two single CPU licenses must be combined into a single, dual CPU license. This is achieved on the myVMware portal.
   TIP: You may have issues combining licenses immediately after adding them into your VMware profile. If this happens, wait 5-10 minutes and try again. If you continue to have issues, contact VMware licensing support to assist with combining the licenses.
2. Once you have the new combined license key, open the vSphere client, connect to the Meeting Server if you are not already, and click on the Meeting Server in the tree in the left panel.
3. In the right panel, select the **Configuration** tab, then under **Software**, click on **Licensed Features**.
4. Current evaluation details display, click on the **Edit** link at the top right corner of the page.
5. In the resulting window, select **Assign a new key to this host** and click the **Enter** button to enter your license key.
6. Click **OK** close the dialog window.

Hypervisor basic setup is now complete.

2.4.5 Task 4 – Accessing the Cisco Meeting Server Small/1000 Console

The Meeting Server instance itself can be accessed by connecting to its own IP address, or via the vSphere client console function.

1. Open the vSphere client and log into your Meeting Server's IP address with the username and the password you configured previously.
2. Select the Meeting Server from the left-hand panel, and use the plus sign (<) to expand the tree. A virtual machine named Cisco Meeting Server will be present and a green arrow to indicate it is powered on.
3. If your network has DHCP, to find the current Meeting Server IP address, click on the **Summary** tab while the Cisco Meeting Server VM is highlighted. The IP address the Meeting Server has obtained will be shown under the **General** section. You can ssh to that IP to continue the configuration of the Meeting Server software.
4. If your network does not have DHCP, you will have to assign an IP address to the VM using the virtual machine console in the vSphere client and the Meeting Server MMP commands **`ipv4`** or **`ipv6`** as described in Chapter 3 (or see the MMP Command Line Reference Guide).
5. To access the console, click on the **Console** tab in the vSphere client when the Meeting Server VM is selected. If the screen is blank, click within the window and press the **Enter** key. A login prompt displays.
   TIP: To regain mouse control outside the console window, press the **Control** and **Alt** keys together.
6. Log in with the user name and password.

   CAUTION: Passwords expire after 6 months.

3 Configuration

3.1 Creating your own Cisco Meeting Server Administrator Account

For security purposes, you are advised to create your own administrator accounts as username “admin” is not very secure. In addition, it is good practice to have two admin accounts in case you lose the password for one account, if you do, then you can still log in with the other account and reset the lost password.

Use the MMP command **`user add <name> admin`**, see the MMP Command Reference Guide for details. You will be prompted for a password which you must enter twice. Login with the new account, you will be asked to change the password.

CAUTION: Passwords expire after 6 months.

After creating your new admin accounts delete the default “admin” account.

Note: Any MMP user account at the admin level can also be used to log into the Web Admin Interface of the Call Bridge. You cannot create users through the Web Admin Interface.

3.2 Setting up the Network Interface for IPv4

Note: Although these steps are for IPv4, there are equivalent commands for IPv6. See the MMP Command Reference for a full description.

In the Cisco Meeting Server virtualized deployment, there is only one network interface initially, interface “a”, but up to 4 are supported (see the next section). The MMP runs on interface a in the virtual deployment.

1. To set network interface speed, duplex and auto-negotiation parameters use the **`iface`** MMP command e.g. to display the current configuration on the " a" interface, in the MMP type:

   `iface a`

   Set the network interface speed (Mbps), duplex and auto negotiation parameters using the command **`iface (a|b|c|d) <speed> (full|on|off)`**. For example, set the interface to 1GE, full duplex:

   `iface a 1000 full`

2. The “a” interface is initially configured to use DHCP. To view the existing configuration, type:

   ipv4 a

   a. If you are using DHCP IP assignment, no further IP configuration is needed, go to step 3.

   b. If you are using Static IP assignment:

      Use the **ipv4 add** command to add a static IP address to the interface with a specified subnet mask and default gateway.

      For example, to add address 10.1.2.4 with prefix length 16 (netmask 255.255.0.0) with gateway 10.1.1.1 to the interface, type:

      ipv4 a add 10.1.2.4/16 10.1.1.1

      To remove the IPv4 address, type:

      ipv4 a del <address>

3. Set DNS Configuration

   Meeting Server requires DNS lookups for many of its activities including looking up SRV records and is required for a simplified deployment. We recommend you point Meeting Server to the default DNS resolver for your network using a period " ." for the forwardzone value.

   a. To output the dns configuration, type:

      dns

   b. To set the application DNS server use the command:

      dns add forwardzone <domain name> <server IP>

      Note: A forward zone is a pair consisting of a domain name and a server address: if a name is below the given domain name in the DNS hierarchy, then the DNS resolver can query the given server. Multiple servers can be given for any particular domain name to provide load balancing and fail over. A common usage will be to specify " ." as the domain name i.e. the root of the DNS hierarchy which matches every domain name.

      ---

      for example:

      dns add forwardzone . 10.1.1.33

   c. If you need to delete a DNS entry use the command:

      dns del forwardzone <domain name> <server IP>

      for example:

      dns del forwardzone . 10.1.1.33

3.3 Adding Additional Network Interface(s)

The Cisco Meeting Server virtualized deployments support up to four interfaces (a, b, c and d).

If required, you can add a second network interface on VMWare. However, any two interfaces of the Cisco Meeting Server must not be put into the same subnet.

1. In the vSphere Client, locate your VM in the **`Hosts and Clusters`** list
2. Select **`Edit Virtual Machine Settings`**.
3. Add a Network Adapter with type VMXNET3.

Note: If you select an Ethernet Adaptor which is not VMXNET3, then you may experience network connection problems, and may invalidate your license.

Note: For more information on adding or modifying Ethernet Adapters, refer to the VMware web page Adding and Modifying Virtual Network Adapters.

---

4. After adding the new adapter, enable the interface for use on the MMP with the command **`ipv4 b enable`**, for example.
5. Reboot the VM so the addresses and gateway can be added manually or automatically picked up by DHCP (if enabled for that interface).

3.4 Configuring the Call Bridge

The Call Bridge needs a key and certificate pair that is used to establish TLS connections with SIP Call Control devices and with the Lync Front End (FE) server. If you are using Lync, this certificate will need to be trusted by the Lync FE server.

The command **`callbridge listen <interface>`** allows you to configure a listening interface (chosen from A, B, C or D). By default the Call Bridge listens on no interfaces.

1. Create and upload the certificate as described in the Certificate Guidelines.
2. Sign into the MMP and configure the Call Bridge to listen on interface A.

   ```
   callbridge listen a
   ```

   Note: the Call Bridge must be listening on a network interface that is not NAT'd to another IP address. This is because the Call Bridge is required to convey the same IP that is configured on the interface in SIP messages when talking to a remote site.

   ---

3. Configure the Call Bridge to use the certificates by using the following command so that a TLS connection can be established between the Lync FE server and the Call Bridge, for example:

   ```
   callbridge certs callbridge.key callbridge.crt
   ```

The full command and using a certificate bundle as provided by your CA, is described in the Certificate Guidelines.

4. Restart the Call Bridge interface to apply the changes.

```
callbridge restart
```

3.5 Configuring the Web Admin Interface

The Web Admin Interface acts as the interface to the Call Bridge; the API of the Cisco Meeting Server is routed through this web interface.

Configuring the Web Admin Interface involves creating a private key/certificate pair, see Section 3.5.1, and uploading the private key/certificate pair to the MMP, see Section 3.5.2.

Once the Web Admin Interface is enabled you can use either the API or the Web Admin to configure the Call Bridge.

3.5.1 Creating the certificate for the Web Admin Interface

The Web Admin Interface is only accessible through HTTPS, you need to create a security certificate and install it on the Cisco Meeting Server. Follow the steps described in the Certificate Guidelines for a production environment – this section shows how to test with a self-signed certificate in a lab environment.

Note: You need a certificate uploaded for the Web Admin Interface even if you configure the Call Bridge through the API rather than the Web Admin Interface.

The information below assumes that you trust Cisco to meet requirements for the generation of private key material. If you prefer, you can generate the private key and the certificate externally using a public Certificate Authority (CA), and then load the externally generated key/certificate pair onto the MMP of the Cisco Meeting Server using SFTP. After obtaining the signed certificate, go to Section 3.5.2.

Note: If testing your Cisco Meeting Server in a lab environment, you can generate a key and a self-signed certificate on the server. To create a self-signed certificate and private key, log in to the MMP and use the command:
`pki selfsigned <key/cert basename>`
where **`<key/cert basename>`** identifies the key and certificate which will be generated e.g. " pki selfsigned webadmin" creates webadmin.key and webadmin.crt (which is self-signed). Self-signed certificates are not recommended for use in production deployments.

The steps below explain how to generate a private key and the associated Certificate Signing Request using the MMP command **`pki csr`** , and export them for signing by a CA.

1. Log in to the MMP and generate the private key and certificate signing request (CSR):

   pki csr <key/cert basename> [<attribute>:<value>]

   where:

   <key/cert basename> is a string identifying the new key and CSR (e.g. " webadmin" results in " webadmin.key" and " webadmin.csr" files)

   and the allowed, but optional attributes are as follows and must be separated by a colon:

   - CN: the commonName which should be on the certificate. Use the FQDN defined in DNS A record as the Common Name. Failure to do this will result in browser certificate errors.
   - OU: Organizational Unit
   - O: Organization
   - L: Locality
   - ST: State
   - C: Country
   - emailAddress

   Use quotes for values that are more than one word long, for example:

   pki csr example CN:example.com "OU:Accounts UK" "O:My Company"

2. Send the CSR to one of the following:
   - To a Certificate Authority (CA), such as Verisign who will verify the identity of the requestor and issue a signed certificate.
   - To a local or organizational Certificate Authority, such as an Active Directory server with the Active Directory Certificate Services Role installed, see Appendix F.

Note: Before transferring the signed certificate and the private key to the Cisco Meeting Server, check the certificate file. If the CA has issued you a chain of certificates, you will need to extract the certificate from the chain. Open the certificate file and copy the specific certificate text including the BEGIN CERTIFICATE and END CERTIFICATE lines and paste into a text file. Save the file as your certificate with a .crt, .cer or .pem extension. Copy and paste the remaining certificate chain into a separate file, naming it clearly so you recognize it as an intermediate certificate chain and using the same extension (.crt, .cer or .pem). The intermediate certificate chain needs to be in sequence, with the certificate of the CA that issued the chain first, and the certificate of the root CA as the last in the chain.

3.5.2 Configuring the Web Admin Interface for HTTPS Access

Note: The deployment automatically sets up the Web Admin Interface to use port 443 on interface A. However, the Web Bridge also uses TCP port 443. If both the Web Admin Interface

---

and the Web Bridge use the same interface, then you need to change the port for the Web Admin Interface to a non-standard port such as 445, use the MMP command **webadmin listen <interface> <port>.**

1. Establish an SSH connection to the MMP and sign in.
2. Use SFTP to upload the private key/certificate pair and certificate bundle (optional) for the Web Admin Interface.
3. Disable the Web Admin Interface before assigning the certificate.

   webadmin disable
4. Assign the private key/certificate pair you uploaded in step 2, using the command:

   webadmin certs <keyfile> <certificatefile> [<cert-bundle>]

   where **keyfile** and **certificatefile** are the filenames of the matching private key and certificate. If your CA provides a certificate bundle then also include the bundle as a separate file to the certificate. For example:

   webadmin certs webadmin.key webadmin.crt webadminbundle.crt
5. Restart the Web Admin Interface.

   webadmin restart
6. Enable the Web Admin Interface.

   webadmin enable

For example:

```
webadmin certs webadmin.key webadmin.crt
webadmin listen b 443
webadmin restart
webadmin enable
```

Test that you can access the Web Admin Interface, i.e. enter your equivalent of https://cms-server.mycompany.com (or the IP address) in your browser and login using the MMP user account you created earlier.

Note: From version 3.0 you can use Trial Mode for a 90 day full featured period without licenses. In this instance, the Web Admin interface will display " This CMS is currently unlicensed" during this period. For information on Smart licensing and how licensing works in 3.0 see Appendix B.

- If you need to support web app clients from your internal network, you should configure Web Bridge on your main Meeting Server instance in the Core and complete the steps in this section.

- If you are using Cisco Expressway as your proxy and TURN Server for web app, Web Bridge needs to be configured on your main Meeting Server instance in the Core and you should complete the steps in this section.
- If you are using the Edge Meeting Server model, you have the option of running Web Bridge just in the Edge or running it both in the Edge and the main Internal Meeting Server instance. Enabling Web Bridge on the internal server allows clients to use web app without making connections to the Web Bridge in the DMZ. The recommendation for deployments using the Edge Meeting Server model is to run Web Bridge in both the DMZ and internal server instances. Complete the steps in this section and configure Web Bridge on the Edge instances and the main Meeting Server instance in the Core.

Note: Running Web Bridge in both the Core and Edge requires clients resolve the same Web Bridge hostname to either the internal or Edge instance as appropriate for them - this is normally referred to as 'Split-DNS' where the DNS Server resolves names to addresses based on where the client is located.

CAUTION: Important notes for Expressway users
If you are deploying Web Bridge 3 and web app you must use Expressway version X14.3 or later, earlier Expressway versions are not supported by Web Bridge 3.

Note: For more information on the web app, see Cisco Meeting Server web app Important Information.

3.5.3 Useful information to help configure Web Bridge 3

The following is useful information to help you configure Web Bridge 3 so that you can use web app:

- " Call Bridge to Web Bridge" protocol (C2W) is the link between the callbridge and webbridge3. It is an outgoing connection from the Call Bridge to the Web Bridge to establish a control channel between them. Certificates are used to authenticate and secure the C2W connection. C2W is exclusive to Call Bridge - Web Bridge traffic and is not used by users or other services.
- A C2W listening port is defined on the Web Bridge server (using **`webbridge3 c2w listen`**) to allow the Call Bridge to connect to the Web Bridge using an HTTPS connection. There is no set default value for the port number to use, but this guide uses 9999 as the example. This connection must be secured with certificates.
- We recommend you protect the C2W port from external access – it only needs to be reachable from Call Bridges.

- A Call Bridge must be able to uniquely reach the C2W interface of each Web Bridge it is configured to work with (C2W connections must use unique hostname or IP per Web Bridge 3 instance).
- Web app clients will have a single address to reach the Web Bridge so when multiple Web Bridges are used, DNS or Load Balancer solutions should be used to direct a shared name to an available Web Bridge instance. The client to Web Bridge connection is stateless for non-call activity and a session does not need to stay with a single Web Bridge.
- When establishing the TLS connection, both sides must present a certificate to verify. The Call Bridge uses the certificate set using the **`callbridge certs`** command and the Web Bridge uses the certificate set using the **`webbridge3 c2w certs`** command.
- The Web Bridge will trust certificates of Call Bridges and Schedulers that are in the Web Bridge's C2W trust store or have been signed by a certificate in the trust store, set by **`webbridge3 c2w trust`**. It is recommended to use a bundle containing the Call Bridge certificates that will connect to this Web Bridge so that only specific certificate matches will be allowed (certificate-pinning).
- The Call Bridgewill trust certificates of Web Bridges that are in the Call Bridge's C2W trust store or have been signed by a certificate in the trust store, set by **`callbridge trust c2w`**. It's recommended to use a bundle containing the Web Bridge certificates that this Call Bridge will connect so that only specific certificate matches will be allowed (certificate-pinning).
- The Scheduler trusts certificates of Web Bridges that are in the Scheduler's C2W trust store or have been signed by a certificate in the trust store, set by the command **`scheduler c2w certs <key-file> <crt-fullchain-file>`**.
- If the certificates used for C2W or Call Bridge have extended key usages defined, they must have the usages enabled to allow a Mutual TLS authentication exchange between Call Bridge and Web Bridge. If extended key usages are defined in a certificate, the Web Bridge 3 C2W certificate must include the " server authentication" extended key usage, and the Call Bridge certificate must include " client authentication" extended key usage. If no extended key usages are defined in a certificate, all usages are assumed valid.
- As the C2W connection is only between internal services, you do not explicitly need to use a certificate signed by a public authority. You can use self-signed certificates created within the MMP.
- The SAN/CN in the Web Bridge C2W certificate must match the FQDN or IP address that is used in the c2w:// url used to register the Web Bridge 3 in the Call Bridge API. If this does not match, the Call Bridge will fail the TLS negotiation, rejecting the certificate presented by the Web Bridge, and will fail to connect with the Web Bridge.

Note: If you want a certificate signed by a Public CA you will need to use the FQDN. (Certificates containing an IP address cannot be signed by a Public CA.) If you want to use an IP address in the C2W address you can create your own certificates as the C2W connection is not a public connection, therefore using Public CAs is not necessary.

- The certificate used for the Web Bridge listening interface should be signed by a certificate authority the clients will trust to avoid certificate warnings when clients connect. The FQDN the clients use to reach Web Bridge should be in the certificate CN or SAN list to avoid certificate warnings when clients connect.
- For general certificate information, see the Certificate Guidelines appropriate for your deployment.

3.5.4 Enabling the Web Bridge 3 Service

The Web Bridge service should be enabled on the Core Meeting Server instance if using the Cisco Expressway proxy or supporting web app clients who can reach the Call Bridge directly. When using the Meeting Server Edge deployment, Web Bridge 3 should run on all Edge instances and can optionally be ran on the Core Meeting Server instance where Call Bridge is running.

Complete these steps on each Meeting Server instance where Web Bridge 3 will run.

1. SSH into the MMP and log in.
2. Configure the interface and port web bridge will use for the web server with the command **`webbridge3 https listen <interface>:<port>`**.

   Using the first interface and port 443 is recommended. Example:

   ```
   webbridge3 https listen a:443
   ```
3. Set the HTTPS certificate and key pair Web Bridge will use for its web server with the command **`webbridge3 https certs <key file> <full certificate chain file>`**.

   This command requires the certificate be defined as the full certificate chain - meaning a certificate bundle that starts with the end entity certificate, includes all the intermediate signing certificate authorities, and ends with the root certificate. Example:

   ```
   webbridge3 https certs wb3-https.key wb3-https-fullchain.crt
   ```
4. Configure the interface and port for the C2W connection with the command

   `webbridge3 c2w listen <interface>:<port>` .

   Using the first interface and the default example port 9999 is recommended. Example:

   ```
   webbridge3 c2w listen a:9999
   ```
5. Configure the C2W connection certificates with the command **`webbridge3 c2w certs <key file> <full certificate chain file>.`**

   Example:

```
webbridge3 c2w certs wb3-c2w.key wb3-c2w-fullchain.crt
```

Note: This certificate must include the FQDN or IP address of the C2W interface in the CN or SAN list of the certificate. Additional information is also available in this FAQ - How do I configure connection certificates for use with Web Bridge 3?

6. The Web Bridge 3 C2W trust store must be configured to control which Call Bridge will be allowed to connect to this Web Bridge. The trust bundle should include the Call Bridge certificate of all Call Bridges that will connect to this Web Bridge, or the certificate of the CA that signed the Call Bridge certificates. For the most control, it is recommended to use the individual Call Bridge certificates in the bundle (certificate-pinning) rather than the certificate of the signing authority. Configure the web bridge's c2w trust bundle with the command **`webbridge3 c2w trust <certificate bundle>`** Example:

   ```
   webbridge3 c2w trust wb3-c2w-trust-bundle.crt
   ```

7. Enable the http redirect. This is optional, but recommended for end-user ease of use

   ```
   webbridge3 http-redirect enable
   ```

8. Enable the web bridge service

   ```
   webbridge3 enable
   ```

Repeat the above steps for each Meeting Server instance where Web Bridge will be running and ensure the certificate or key pairs used are correct for each instance.

C2W is the control interface between the Call Bridge and Web Bridge instances and must be configured in the Call Bridge if Web Bridge is deployed. The Call Bridge's C2W trust bundle should include the Web Bridge C2W certificates of all Web Bridge that this Call Bridge will connect to, or the certificate that signed the Web Bridge C2W certificates. For the most control, it is recommended to use the individual Web Bridge C2W certificates in the bundle (certificate-pinning) rather than the certificate of the signing authority.

1. Connect to the MMP interface of the Internal Meeting Server running Call Bridge.
2. The Call Bridge should already be configured with a certificate from the steps performed in Configuring the Call Bridge listening interface. Confirm by running the command **`callbridge`** and checking that the Key File and Certificate file settings are configured. If not, repeat the steps in Configuring the Call Bridge listening interface before proceeding. The Call Bridge must be configured with certificates for C2W functionality.
3. Use the command **`callbridge trust c2w <certificate bundle file>`** to configure the Call Bridge's C2W trust store with a certificate bundle that includes the C2W certificates of the Web Bridge instances. Example:

   ```
   callbridge trust c2w c2w-callbrige-trust-store.crt
   ```

Note: Unless limited by scopes, the Call Bridge will attempt to connect to all Web Bridge that are defined in the Meeting Server API.

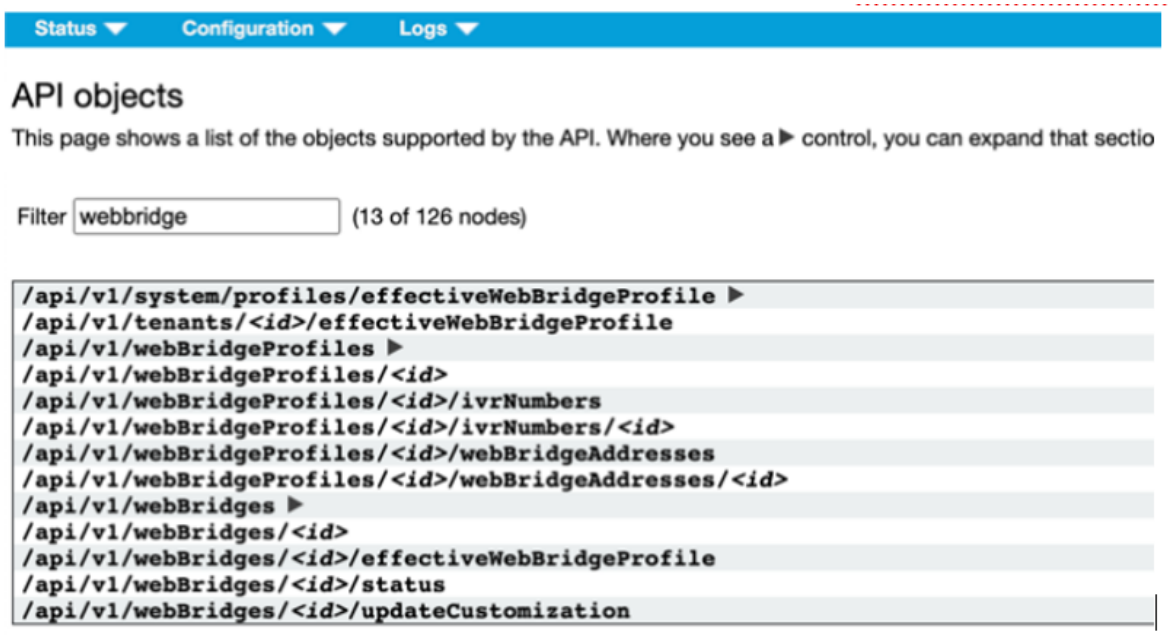
4. Restart the Call Bridge

```
callbridge restart
```

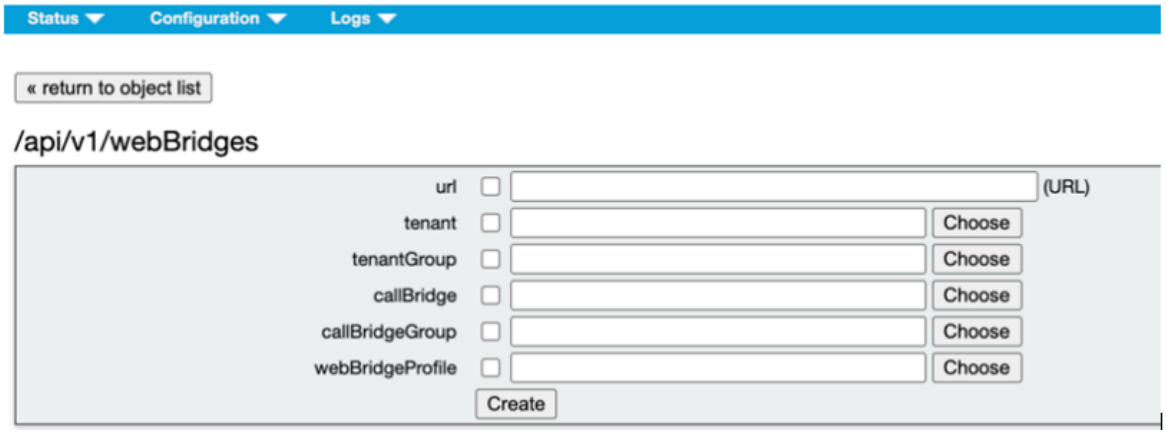
3.5.5 Configure Call Bridge with Web Bridge Addresses

The Call Bridge must be told the C2W address of each Web Bridge it will connect to (including a co-resident Web Bridge) by creating a Web Bridge entry in the Meeting Server API. This guide will use API explorer in the Web Admin interface of Meeting Server to illustrate how to complete this task.

1. Log in to the Meeting Server Web Admin interface and select **Configuration** > **API.**
2. Using the Filter input box, type **`webBridges`** to filter the list view, as shown here:



3. Locate the **`/api/v1/webBridges`** row from the resulting list and click the ▶ icon to expand it.
4. Click **Create new** to create a new Web Bridge object and the following parameter fields display as shown here:



5. Fill in the **url** field using the format *c2w://<Web Bridge FQDN>:<c2w port>* with the FQDN address of the C2W interface for Web Bridge being added. Example:

   ```
   c2w://cmsedge1.company.com:9999
   ```

   Note: The FQDN entered here must be the CN or in the list of SAN names of the certificate assigned to the C2W interface of Web Bridge 3 and must resolve to the IP of the C2W interface for the Web Bridge. IP Addresses can only be used if the C2W certificate has the IP address in the certificate's SAN or CN.

6. Click **Create** to save the new Web Bridge entry.

If you have multiple Web Bridges, repeat the above steps creating one Web Bridge object for each Web Bridge instance.

Appendix A Technical specifications for Cisco Meeting Server 1000/Small

A.1 Physical specifications:

Chassis: Cisco UCS C220 M6 Rack Server or Cisco UCS C220 M7 Rack Server

Weight: 18+ kg (40 lbs)

Size: 1RU high

Rack requirements: 19" standard rack

A.2 Environmental specifications

Operating temperature: 5 to 35° C (41-95° F)

Operating humidity: 5 to 93% non-condensing

A.3 Electrical specifications

See Power Supply Specifications in the appropriate Cisco UCS C220 Server Installation and Service Guide.

A.4 Video and audio specifications:

This table provides a comparison of the call capacities across the platforms hosting Cisco Meeting Server software.

Table 4: Call capacities across Meeting Server platforms

Type of calls	Cisco Meeting Server Small M7 (Bare metal OS)	Cisco Meeting Server Medium M8	Cisco Meeting Server Small M7 (VM deployment)	Cisco Meeting Server 1000 M6
Full HD calls 1080p60 video 720p30 content	60	150	60	40
Full HD calls 1080p30 video 1080p30/4K7 content	60	150	60	40

Type of calls	Cisco Meeting Server Small M7 (Bare metal OS)	Cisco Meeting Server Medium M8	Cisco Meeting Server Small M7 (VM deployment)	Cisco Meeting Server 1000 M6
Full HD calls 1080p30 video 720p30 content	120	225	120	80
HD calls 720p30 video 720p5 content	240	450	240	160
SD calls 480p30 video 720p5 content	480	850	480	320
Audio calls (G.711)	3000	3000	3000	3000

Note: Virtual deployments on Meeting Server Small M7 variants support a maximum of 94 vCPU and 128 GB RAM.

Appendix B Cisco licensing

This section covers license information for Smart licensing.

B.1 Smart Account and Virtual Account information

Smart Accounts can contain Virtual Accounts which allow you to organize your licenses by any designation of your choice, for example, by department. Here are some important points to note when using a Smart Virtual Account with Meeting Server and Meeting Management:

- Each Meeting Server cluster(s) to a single Meeting Management should be linked to a user-defined Smart Virtual Account.
- Each Virtual Account can only connect with a single Meeting Management server that is configured to handle Smart Licensing.
- Only configure a single Meeting Management to Smart – we recommend you do **not** configure a second redundant Meeting Management for Smart Licensing as double counting of license usage will occur.
- PMP Plus, SMP Plus, and Recording/Streaming licenses can be shared across multiple clusters with a single Meeting Management instance and Smart Licensing in a single Virtual Account.

B.2 How Smart licenses work in Meeting Server – overview

Meeting Management is mandatory for licensing to work on Meeting Server. A trust and interaction between Meeting Server and Meeting Management supports the licensing using Smart or for existing customers use of installed licensing files – it's this trusted link that enables Meeting Management to license Meeting Server.

Note: For full details on using Cisco Meeting Management to administer Smart Licensing, see the Meeting Management Administrator Guide.

A high level work flow for implementing Smart Licensing is as follows:

1. Register your Meeting Management to Smart Licensing Virtual Account.
2. When a Meeting Server first starts up it will have no license status values defined.

   Note: You can use Trial Mode for a 90 day full featured period without licenses.

   ---

3. When Meeting Server first connects to a Meeting Management instance set up to administer Smart Licensing, it checks to see if the Meeting Server has previously had a

license applied. If not, it will set the license expiry date to 90 days in the future.

The expiry date for a license is shown in Meeting Management and also returned in the clusterLicensing API, as shown in Appendix B.5.

Note: The expiry date for any feature license will only ever be up to a maximum of 90 days in the future.

---

4. Meeting Management collates Meeting Server licensing usage for the cluster and reports to your Smart Account on a daily basis to check that it has the licenses required to ensure the Meeting Server is in compliance. The Smart Account responds to Meeting Management to indicate if the Meeting Server is compliant or not. Meeting Management then sets the expiry dates as appropriate as follows:

    a. If the Meeting Management identifies that a license exists and is below entitlement for a particular feature, the expiry date will be extended to 90 days in the future.

    Note: If Meeting Server doesn't connect to Meeting Management and send usage data for a period of 90 days then the Meeting Server's license won't get refreshed and will therefore expire. For information on the enforcement actions when a license expires, see Section B.3.

    If a license usage is higher than the entitlement, or a license is not found, then enforcement occurs as follows.

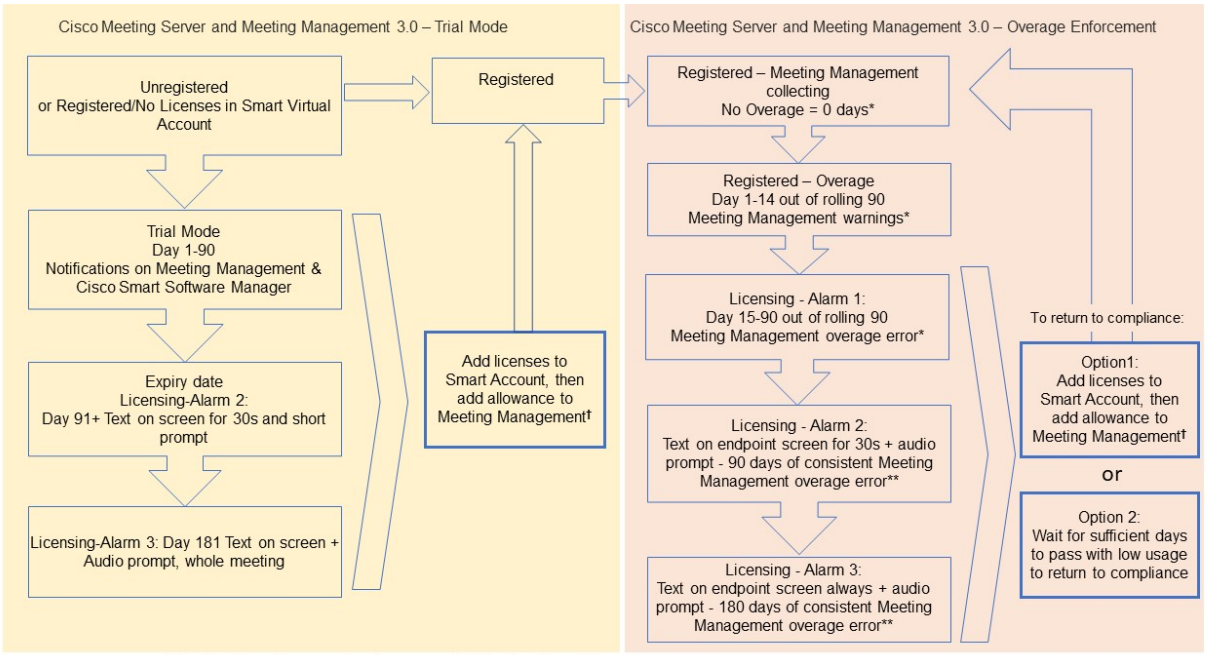
    b. If Meeting Management identifies that less than 15 out of the last 90 days are non-compliant, it will allow this and reset the Meeting Server expiry date to 90 days in the future from that point. The admin will get a visual warning to notify " Insufficient licenses" .

    c. If Meeting Management identifies that more than 15 of the last 90 days are non-compliant, the first level of enforcement (Alarm 1) will occur, i.e. out of compliance notifications on the Meeting Management interface.

    d. If overage continues, Meeting Management does not reset the 90 day clock, it gives you a countdown in xx days in which to add new licenses otherwise Alarm levels 2 and 3 will be enabled for all participants joining a meeting as shown in Appendix B.

Appendix B shows the enforcement flow from initial start up in trial mode on the left-hand side through to overage enforcement as shown on the right-hand side.

Figure 2: Cisco Meeting Server and Cisco Meeting Management Smart Licensing enforcement flow



* Counting days of overage (i.e. where usage is higher than the entitlement)
** Counting days where Meeting Management is in an error state (i.e. the state where there are 15 continuous days overage out of the last 90 days)
† To ensure accurate reporting, the administrator needs to specify within Meeting Management the number of licenses that are held in the Smart Account

B.3 Expired license feature enforcement actions

Previously, Meeting Server would evaluate its license file on restart only. From 3.0 the current status of whether a feature is licensed or not can change dynamically, for example, because a feature license expires (previously this would not have been evident until a restart), or there has been an API change. Meeting Management will calculate enforcement actions with Smart Licensing.

Note: You can use the Smart Licensing portal to enable email notifications for " insufficient licenses" .

When a license feature has expired the actions described in Table 5 will occur.

Table 5: Expired license enforcement actions

Feature	Action
callBridge	When expired: a visual text message displays on screen lasting 30 seconds and an audio prompt plays on joining a meeting for all participants/all meetings. (Alarm level 2)
callBridgeNoEncryption	When expired more than 90 days ago or no license present: the same as before but the visual message is permanent. The audio prompt plays " Your deployment is out of licensing compliance, please contact your administrator" . (Alarm level 3) . However, encrypted calls are not processed in the unlicensed state. Note: you only need callBridge or callBridgeNoEncryption to prevent the above action.
PMP/SMP	
customizations	When expired or not present, customization features will not be active during a meeting.
recording	When expired or not present you will not be able to start a new recording (regardless of whether it is a 3rd party recorder or not). This license represents recording and streaming so the same restrictions also apply to streaming.

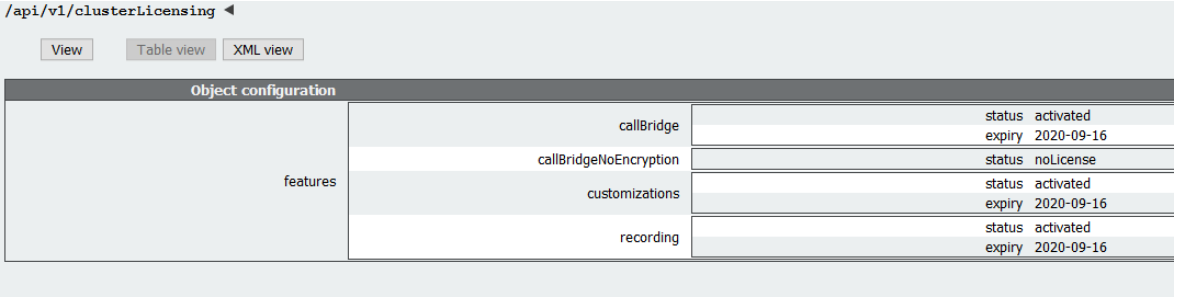
To turn off Alarms 2 and 3, simply add more licenses to your Smart Account.

B.4 How to retrieve licensing information (Smart Licensing)

To retrieve licensing information for a cluster using the Meeting Server Web Admin interface:

1. Log in to the Meeting Server Web Admin interface and select **Configuration > API**:
2. From the list of API objects, tap the ▶ after **/api/v1/clusterLicensing**
3. The current license status for the cluster is displayed as shown in this example:

Figure 3: clusterLicensing API – license status



B.5 Cisco Meeting Server licensing

The following features require a license:

- Call Bridge
- Call Bridge No Encryption
- Customizations (for custom layouts)
- Recording or Streaming

In addition to feature licenses, user licenses also need to be purchased, there are 2 different types of user licenses:

- PMP Plus,
- SMP Plus,

Note: You can use Trial Mode for a 90 day full featured period without licenses.

For information on user licensing, see Section B.7.

Note: You have the choice of purchasing an activation key with SIP media encryption enabled or SIP media encryption disabled (unencrypted SIP media) for the Cisco Meeting Server Small, Cisco Meeting Server and the VM software image. For more information on the unencrypted SIP media mode and activation key see your Deployment Guide.

B.5.1 Personal Multiparty plus licensing

Personal Multiparty Plus (PMP Plus) provides a named host license assigned to each specific user who frequently hosts video meetings. This can be purchased through Cisco UWL Meeting or Flex Meetings (which includes PMP Plus). Personal Multiparty Plus is an all-in-one licensing offer for video conferencing. It allows users to host conferences of any size (within the limits of the Cisco Meeting Server hardware deployed). Anyone can join a meeting from any endpoint, and the license supports up to full HD 1080p60 quality video, audio, and content sharing.

Note: Using Unified Communications Manager, the initiator of an Ad Hoc conference can be identified and if they have been assigned a PMP Plus license then that is used for the conference.

Note: To determine the number of active calls using the PMP Plus licence of an individual, use the parameter **`callsActive`** on API object **`/system/multipartyLicensing/activePersonalLicenses`**. We generally allow 2 calls to be active allowing for one starting and other finishing. If the call is on a cluster of Call Bridges then use the parameter **`weightedCallsActive`** on API object **`/system/multipartyLicensing/activePersonalLicenses`** for each Call Bridge in the cluster. The sum of **`weightedCallsActive`** across the cluster matches the number of distinct calls on

---

the cluster using the individual's PMP Plus license. If a PMP Plus licence is exceeded, then SMP Plus licences are assigned, see Section B.8.

B.5.2 Shared Multiparty plus licensing

Shared Multiparty Plus (SMP Plus) provides a concurrent license that is shared by multiple users who host video meetings infrequently. Shared Multiparty Plus enables all employees who do not have PMP Plus host license to access video conferencing. It is ideal for customers that have room systems deployed that are shared among many employees. All users with PMP Plus or using SMP Plus licenses have the same great experience, they can host a meeting with their space, initiate an ad-hoc meeting or schedule a future one. Each shared host license supports one concurrent video meeting of any size (within the limits of the hardware deployed).

Note: To determine the number of SMP Plus licences required, use the parameter **`callsWithoutPersonalLicense`** on API object **`/system/multipartyLicensing`**. If the calls are on a cluster of Call Bridges then use the parameter **`weightedCallsWithoutPersonalLicense`** on API object **`/system/multipartyLicensing`** for each Call Bridge in the cluster. The sum of **`weightedCallsWithoutPersonalLicense`** across the cluster matches the number of distinct calls on the cluster which require an SMP Plus license.

B.6 Smart Licensing registration process

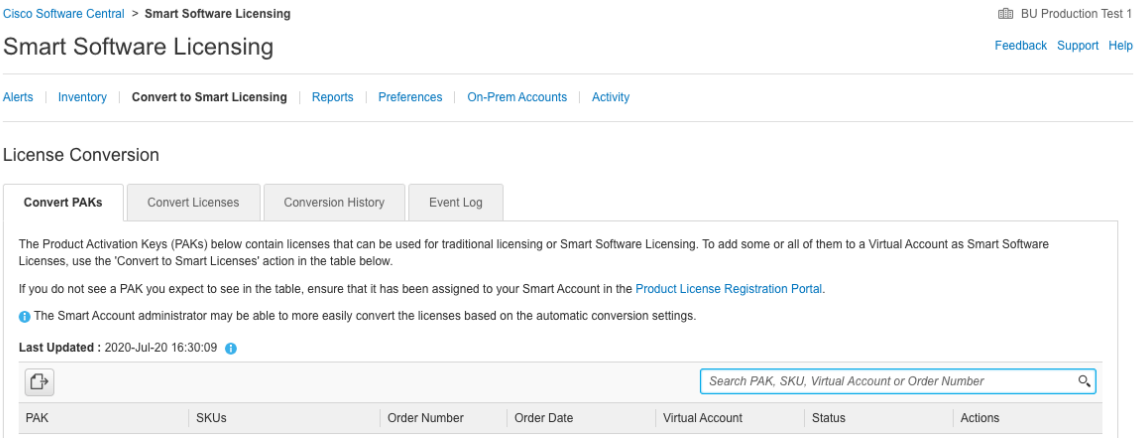
To enable Smart Licensing:

1. Sign in to Cisco Smart Software Manager (CSSM) portal and choose Virtual Account with Meeting Server Licenses.
2. Generate a registration token.
3. Copy the token to your clipboard.
4. Open the instance of Meeting Management that you want to use for license reporting.
5. Go to the **Settings** page, **Licensing** tab.
6. Click **Change**.
7. Choose **Smart Licensing** and **Save**.
8. Click **Register**.
9. Paste the registration token (this allows Meeting Management to connect to the Smart Licensing portal).
10. Click **Register**.
11. When you have registered, check how many licenses you have in your Virtual Account.
12. In Meeting Management, go to the **Licenses** page.

13. Enter the license information for the licenses you have in your Virtual Account.

    If any licenses are not shown in your Virtual Account, use the **Convert Licenses** tab, search by PAK to find them, then choose **Convert Licenses** as shown in Figure 4. (If you can't find a license(s), open a case by sending an email to licensing@cisco.com.)

    Figure 4: License conversion for Smart Licensing



B.7 Assigning Personal Multiparty licenses to users

This process requires that users are imported from a single LDAP source. See the " Provisioning – Import users" chapter in the Meeting Management Administrator Guide for full details.

B.7.1 To determine whether a specific user has a license:

1. From the list of API objects, tap the ▶ after **/users**
   a. Select the **object id** of the specific user
   b. Identify the **object id** of the **userProfile** associated with this user
2. From the list of API objects, tap the ▶ **/userProfiles**
   a. Select the **object id** of the specific userProfile
   b. Find the setting for parameter **hasLicence**. If set to **true** then the user identified in step 1 is associated with a Cisco Multiparty user license. If set to **false** the user is NOT associated with a Cisco Multiparty user license.

Note: If the userProfile is deleted, then the userProfile is unset for the ldapSource and the imported users.

B.8 How Cisco Multiparty licenses are assigned

When a meeting starts in a space, a Cisco license is assigned to the space. Which license is assigned by the Cisco Meeting Server is determined by the following rules:

- if the space owner is defined and corresponds to a Meeting Server imported LDAP user with an assigned Cisco PMP Plus license, the license of that owner is assigned irrespective of whether the person is active in the conference, if not, then
- if the meeting was created via ad hoc escalation from Cisco Unified Communications Manager, then Cisco Unified Communications Manager provides the GUID of the user escalating the meeting. If that GUID corresponds to a Meeting Server imported LDAP user with an assigned Cisco PMP Plus license, the license of that user is assigned, if not, then
- if the meeting was scheduled via Cisco TMS version 15.6 or newer, then TMS will provide the owner of the meeting. If that user corresponds to a Meeting Server imported LDAP user by user ID/email address with an assigned Cisco PMP Plus license, the license of that user is assigned to the meeting, if not then,
- a Cisco SMP Plus license is assigned.

B.9 Determining Cisco Multiparty licensing usage

We recommend you use Meeting Management to view your Multiparty licensing usage. However, the API can be used.

Table 6 below lists the API objects and parameters that can be used to determine the consumption of Multiparty licenses.

Table 6: Objects and parameters related to Multiparty license usage

API object	Parameter (s)	Use to .....
/system/licensing	personal, shared	determine whether components of the Cisco Meeting Server have a Multiparty license and are activated. Values are: noLicense, activated, grace, expired. Also provides date of expiry and number limit.
/system/multipartyLicensing	personalLicenseLimit, sharedLicenseLimit, personalLicenses, callsWithoutPersonalLicense, weightedCallsWithoutPersonalLicense	indicates the number of licenses available and in use
/system/multipartyLicensing/ activePersonalLicenses	callsActive, weightedCallsActive	indicates the number of active calls that are using a Personal Multiparty Plus user license,
/userProfiles	hasLicense	indicates whether or not a user is associated with a Cisco Multiparty user license

For more information on these additional object and fields to support Cisco Multiparty licensing, refer to the Cisco Meeting Server API Reference Guide.

B.10 Calculating SMP Plus license usage

For the following specific scenarios, the SMP Plus license consumed for a meeting is reduced to 1/6th of a full SMP Plus license:

- an audio-only conference where no attendees are using video,
- a Lync gateway call unless the Meeting Server is recording or streaming, at which point it is considered a full conference and a full SMP Plus license is consumed,
- a point to point call involving a web app and a SIP endpoint, or two web apps, unless the Meeting Server is recording or streaming, at which point it is considered a full conference and a full SMP Plus license is consumed.

A full SMP Plus license is consumed for any audio-video conference instantiated from a space with the owner property undefined, owned by an imported LDAP user without a PMP Plus license, or owned by an imported LDAP user whose PMP Plus license has already been consumed, this is irrespective of the number of participants.

Note: A point to point call is defined as:

- having no permanent space on the Meeting Server,
- two or less participants, including the recorder or streamer
- no participants hosted on the Lync AVMCU,

This includes Lync Gateway calls as well as other types of calls: point-to-point web app to web app, web app to SIP and SIP to SIP.

B.11 Retrieving license usage snapshots from a Meeting Server

An administrator can retrieve license usage from the Meeting Server. These cannot be accessed though the Web Admin Interface, instead use an API tool such as POSTMAN:

Use GET on **`/system/MPLicenseUsage/knownHosts`** to retrieve host ids of the Meeting Servers in the deployment. Supply an offset and limit if required to retrieve host ids other than those on the first page of the list.

Use GET on **`/system/MPLicenseUsage`** to retrieve license usage from the Call Bridge of the Meeting Server with the specified host id. Supply a start and end time for the snapshot. Provides information on number of personal licenses in use, number of shared licenses in use which are audio only, point to point, or neither audio or point to point, number of calls being recorded and number of streamed calls.

Note: Note: personal and shared licenses are normalized over the number of Call Bridges that the call spans.

B.12 License reporting

Meeting Management has license reporting/usage information for the last 90 days, and Cisco Smart Software Manager also contains license reporting information. The usage of recording licenses indicates the number of conferences recording concurrently, similarly the streaming license usage indicates the number of conferences streaming concurrently.

B.13 Legacy licensing file method

This section only applies if you are using the traditional licensing method. From version 3.4, the support for traditional licensing has been deprecated. The existing local licenses will still be supported until the license expires.

B.13.1 Getting and Entering a License File

All virtualized deployments of the Cisco Meeting Server require a license file; the license file is for the MAC address of your virtual server.

Note: If you are uploading Cisco Meeting Server 2.0 to an existing deployment, then you can continue to use the " acano.lic" license issued for the Acano server. However, if you want to extend your deployment then you will need to purchase a Cisco license.

After purchasing the licensing, follow this chapter to apply the license to the Cisco Meeting Server only if you are using the traditional licensing method.

B.13.1.1 Transferring the license file to the Cisco Meeting Server

This section assumes that you have already purchased the licenses that will be required for your Meeting Server from your Cisco Partner and you have received your PAK code(s).

Follow these steps to register the PAK code with the MAC address of your Meeting Server using the Cisco License Registration Portal.

1. Obtain the MAC address of your Meeting Server by logging in to the MMP of your server, and enter the MMP command: **`iface a`**

   Note: This is the MAC address of your VM, not the MAC address of the server platform that the VM is installed on.

2. Open the Cisco License Registration Portal and register the PAK code(s) and the MAC address of your Meeting Server.
3. If your PAK does not have an R-CMS-K9 activation license, you will need this PAK in addition to your feature licenses.
4. The license portal will email a zipped copy of the license file. Extract the zip file and rename the resulting xxxxx.lic file to **`cms.lic`**.
5. Using your SFTP client, log into Meeting Server and copy the **`cms.lic`** file to the Meeting Server file system.
6. Restart the Call Bridge using the MMP command **`callbridge restart`**
7. After restarting the Call Bridge, check the license status by entering the MMP command **`license`**

   The activated features and expirations will be displayed.

B.13.1.2 After transferring the license file

To apply the license you need to restart the Call Bridge. However, you must have configured the Call Bridge certificates and a port on which the Call Bridge listens, before you can do this.

After the license file has been applied, the " Call Bridge requires activation" banner will no longer appear when you sign into the Web Admin Interface.

Note: From version 3.0 you can use Trial Mode for a 90 day full featured period without licenses. In this instance, the Web Admin interface will display " This CMS is currently unlicensed" during this period. For information on Smart licensing and how licensing works in 3.0 see Appendix B.

Note: If you are deploying multiple servers (single combined or split Core or Edge servers) that you will cluster, see the Scalability & Resilience Deployment Guide Appendix entitled *Sharing Call Bridge licenses within a cluster* for more information if you are using the traditional licensing method. Otherwise, refer to the Smart Licensing section as you can now license multiple clusters with one set of Meeting Server licenses in your Smart Account and you no longer need to load the license file onto each individual Meeting Server instance as was the case prior to 3.0.

You are now ready to configure the Cisco Meeting Server. See the appropriate guide for your deployment found here:

- Single Combined Server Deployment Guide if you are deploying on a single host server
- Single Split Server Deployment Guide if you are deploying on a split Core/Edge deployment
- Scalability & Resilience Guide if you are deploying multiple servers (single combined or split Core or Edge servers) that you will cluster.

Remember to use the **`shutdown`** command rather than using the vSphere power button when you want to shut down the Cisco Meeting Server.

B.13.2 Obtaining Cisco user licenses using the traditional licensing method

This section assumes that you have already purchased the licenses that will be required for your Meeting Server from your Cisco Partner and you have received your PAK code(s).

Follow these steps to register the PAK code with the MAC address of your Meeting Server using the Cisco License Registration Portal.

1. Obtain the MAC address of your Meeting Server by logging in to the MMP of your server, and enter the MMP command: **`iface a`**

   Note: This is the MAC address of your VM, not the MAC address of the server platform that the VM is installed on.

   ---

2. Open the Cisco License Registration Portal and register the PAK code(s) and the MAC address of your Meeting Server.

3. If your PAK does not have an R-CMS-K9 activation license, you will need this PAK in addition to your feature licenses.
4. The license portal will email a zipped copy of the license file. Extract the zip file and rename the resulting xxxxx.lic file to **`cms.lic`**.
5. Using your SFTP client, log into Meeting Server and copy the **`cms.lic`** file to the Meeting Server file system.
6. Restart the Call Bridge using the MMP command **`callbridge restart`**
7. After restarting the Call Bridge, check the license status by entering the MMP command **`license`**

   The activated features and expirations will be displayed.

Appendix C Branding

Some aspects of the participant experience of meetings hosted on Meeting Servers can be branded, they include :

- the web app sign-in background image, sign-in logo, text below sign-in logo, icon, custom virtual background images in Self-view pane, and the text on the browser tab,
- IVR messages,
- SIP and Lync participant's splash screen images and all audio prompts/messages,
- text on the meeting invitation.

If you apply a single brand with only a single set of resources specified (one web app sign-in page, one set of voice prompts, one invitation text), then these resources are used for all spaces, IVRs and Web Bridges in the deployment. Multiple brandings allow different resources to be used for different spaces, IVRs and Web Bridges. Resources can be assigned at the system, tenant, space or IVR level using the API.

See the Customization Guidelines for more information on branding.

Appendix D Sizing a VM

The Cisco Meeting Server is designed for maximum flexibility, it is highly scalable and allows the "mix and matching" of Cisco Meeting Server 2000, Cisco Meeting Server 1000 and VM deployments. For example, using VMs as edge servers and Cisco Meeting Server 2000 and Cisco Meeting Server 1000 at the core for a highly scalable distributed architecture, or placing all components within a VM deployment on a single standardized server.

Maximum flexibility is also carried through into the wide range of standard servers and specifications the Cisco Meeting Server software can run on. Appendix E provides details for one of the most popular virtualization technologies: VMware. The Cisco Meeting Server software also runs effectively on an array of more specialized servers, for example for applications requiring portable and rugged form factors.

The whole Cisco Meeting Server or individual components of the Cisco Meeting Server can be run in a virtual machine (VM) deployment. For instance:

- for the purposes of testing the deployment, all of the components can run on a single VM see Figure 5.

  Note: In production networks, the Recorder and Streamer components should be enabled on a different Meeting Server to the server hosting the conferences.

- a single VM can run the Web Bridge as an edge component with the TURN server, connected to a Cisco Meeting Server 2000 or Cisco Meeting Server 1000 sitting in the core network running the Call Bridge, and another VM running the other core components.

  Note: If the Cisco Expressway is used at the edge of the network, then the TURN server component on the VM does not require enabling, and the Web Bridge should reside on the Meeting Server with the Call Bridge hosting the conferences.

- one VM running edge components, connecting to a second VM running the Call Bridge and database, and a third VM running other core components.

Figure 5 illustrates the Cisco Meeting Server software components enabled on one server. Figure 6 illustrates the Cisco Meeting Server software components deployed across an edge server and core servers.

Figure 5: Cisco Meeting Server software components enabled on one server

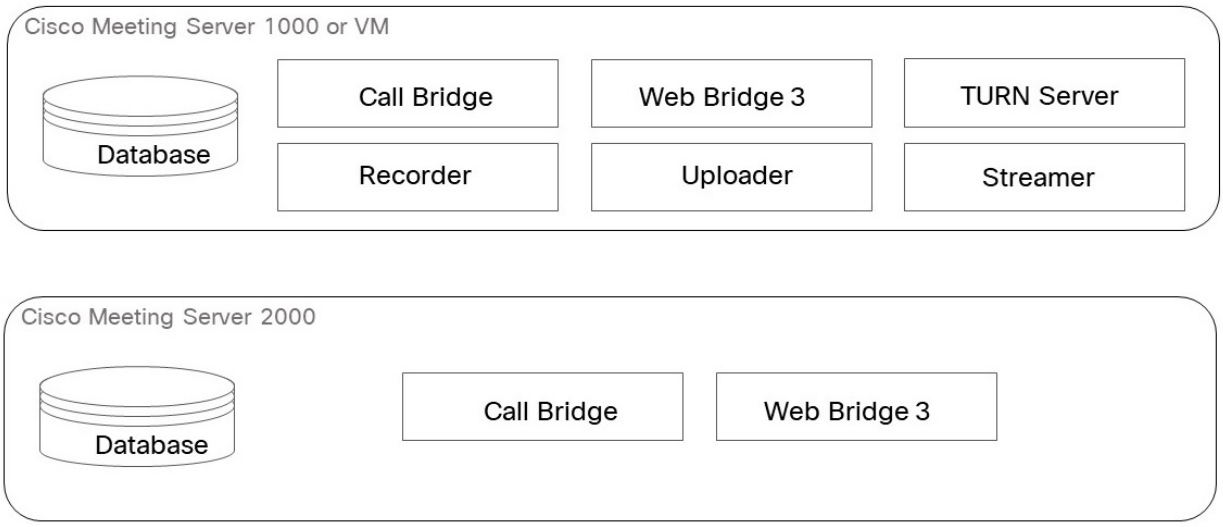
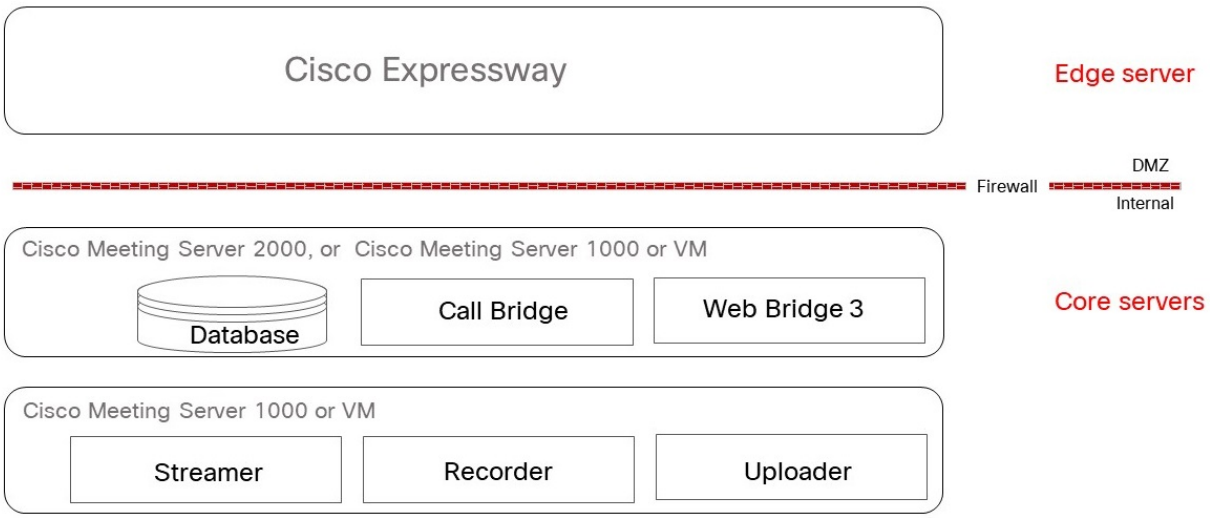


Figure 6: Cisco Meeting Server software components with the TURN server and Web Bridge 3 at the edge



When a VM is configured to run one or more Cisco Meeting Server components, Cisco recommends that the entire host is dedicated to the VM. This provides best performance for real time media applications and ensures high quality end user experience. The sizing of VMs depends on the components being used.

Note: The specification-based VM deployments support a baseline configuration of 70 vCPU and 58GB RAM.

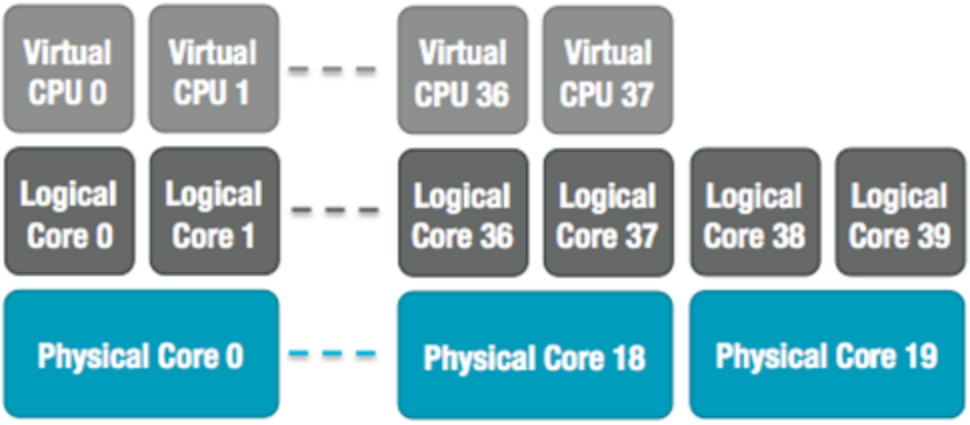
D.1 Call Bridge VM

The Call Bridge carries out the media transcoding for the Cisco Meeting Server. This component has the highest requirements of any of the components.

Each physical core of an Intel Xeon 2600 series (or later) CPU, running at 2.5GHz, is capable of approximately 2.5 720p30 H.264 call legs when hyperthreading is enabled. Capacity scales linearly with number of CPU cores and frequency, so a two socket E5-2680v2 system, which has 20 physical cores, can handle 50 concurrent 720p30 H.264 call legs.

The VM should be configured to use all but one of the host physical cores. When hyperthreading is enabled the number of available logical cores is double the number of physical cores, so in the dual E5-2680v2 system above, there are 40 virtual CPUs, of which 38 should be allocated to the VM. We recommend that you configure the number of sockets to mirror underlying hardware.

Figure 7: Virtual CPU core allocation for a dual E5-2680v2 host



Over subscription of the host, either by incorrectly setting the number of Cisco Meeting Server VM virtual CPUs or by contention for CPU resources amongst VMs, causes scheduling delays and results in degraded media quality. The recommendation to assign the number of vCPUs in excess of the number of physical cores is an overcommitment of the CPU resource. This CPU over commitment does lead to a distortion in the VM CPU utilization statistics and a higher CPU Ready time. CPU commitment is a workload specific consideration and therefore may conflict with more generic advice. This vCPU commitment is intentional for Cisco Meeting Server and is a result of empirical testing to extract peek performance from a host. A Cisco Meeting Server VM, correctly configured according to the recommendations above, will degrade gracefully by dropping frame rate and/or resolution if pushed over capacity.

1GB RAM for each underlying physical CPU core should be allocated to the VM with a minimum allocation of 4GB of RAM. For the system above, the VM should be configured with 19GB corresponding to the 19 physical CPU cores in use.

Though RAM requirements for the Call Bridge VMs are 1GB per vCPU with a minimum of 4GB of RAM, recommended minimum is 8GB. To increase cospace scale in a deployment beyond 75k cospaces, an additional 1GB of RAM per 100k cospaces is required for all Call Bridge and Database VMs. In the above Call Bridge VM example, to support 50 HD ports and 275k cospaces it would require 38GB of RAM to support the 50 HD ports plus 2GB of RAM for the 200k cospaces in excess of 75k.

D.2 Web Edge VM

Expressway (Large OVA or CE1200) is the recommended solution for deployments with medium web app scale requirements (i.e. 800 calls or less). Expressway (Medium OVA) is the recommended solution for deployments with small web app scale requirements (i.e. 200 calls or less). However, for deployments that need larger web app scale, from version 3.1 we recommend Cisco Meeting Server web edge as the required solution.

D.2.1 Edge server configurations

Two virtual machine hardware configurations are supported for the Edge server role. These configurations define the supported minimum hardware requirements and capacities they support.

" Small" Edge Server

1 x Cisco Meeting Server VM with the following specification for supported Cisco hardware

- 4 GB RAM
- 4 vCPUs
- 1Gbps network interface

" Large" Edge Server

1 x Cisco Meeting Server VM with the following specification for supported Cisco hardware

- 8 GB RAM
- 16 vCPUs
- 10Gbps network interface

Recommended processor specifications:

We recommend processor specification such as Intel Xeon E5 2600 running at 2.5GHz or higher. We recommend 1 vCPU to 1 physical CPU.

NIC requirement:

Cisco has tested and validated Split-server deployment using single NIC configuration for the TURN Servers. Hence, from version 3.0, we recommend you configure listening ports for a TURN Server only on one interface.

Co-residency support:

The Edge server can be co-resident with other VMs. However, each 4 vCPU VM has a 1 Gbps NIC requirement and each 16 vCPU has a 10Gbps NIC requirement. The VM host will need sufficient NIC capacity for all applications.

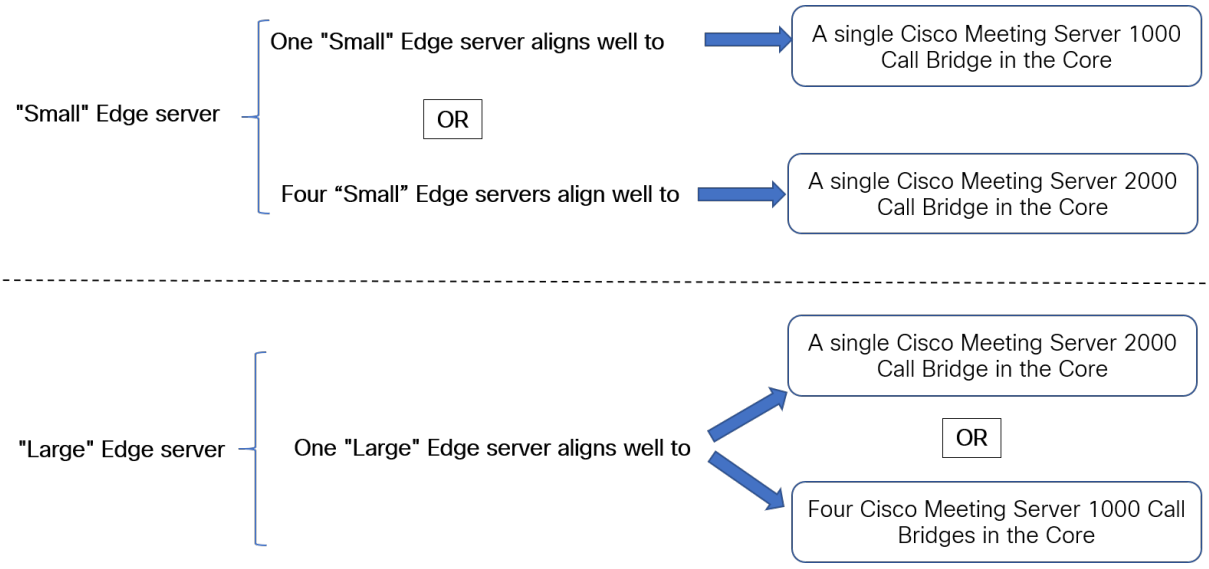
Note:

- Meeting Server M5 onwards hardware supports 10Gbps NIC.

Table 7: Edge Server web app call capacities

Type of calls	Small Edge VM Call Capacity	Large Edge VM Call Capacity
Full HD calls 1080p30 video	100	350
HD calls 720p30 video	175	700
SD calls 448p30 video	250	1000
Audio calls (G.711)	850	3000

The two Edge server configurations provide capacities that simplify matching Edge capacity to Core Call Bridge capacity when using Cisco Meeting Server appliances for Call Bridge.



Determine the number of Edge servers needed by reviewing the Call Bridge call capacity the core Call Bridge supports, and the Edge server hardware configuration being used.

D.2.2 Deployment considerations

- We recommend that all edge servers serving the same Call Bridge or Call Bridge Group be the same capacity, i.e. all 4 vCPUs or all 16 vCPUs, not a mix of both.
- For scalable or resilient deployments, we recommend that you configure Call Bridge groups. This allows you to assign a unique group of TURN servers to each Call Bridge group which is useful for helping with load balancing and keeping TURN servers sensibly geolocated with Call Bridges.
- For web app to match SIP scale (up to 24 Call Bridges per cluster), we support multiple edge servers. However, Call Bridge groups only support up to 10 Edge servers per group. For scalable or resilient deployments needing more than 10 Edge servers, more than one Call Bridge group will be necessary.
- To support the Meeting Server Edge solution, a new MMP command **`turn highcapacity-mode (enable|disable)`** is introduced that enables TURN scalability mode. This setting is enabled by default.

For more information on deploying the Cisco Meeting Server web edge solution, see the Deployment Guides (version 3.1 or later).

D.3 Database VM

Note: This section is applicable only if you choose to use one or more external databases.

The host server for a database has modest CPU requirements, but requires large storage and memory. We do not mandate a qualified VM host but recommend:

- 8 vCPUs, 8GB[1] RAM and 100GB data store

  (The OVF will be set to these parameters so that they are the defaults post-deployment)
- Sandy Bridge (or later) class Intel processors (e.g. E5-2670 or E5-2680 v2)
- The data store should reside on either a high IO per second SAN or local SSD storage
- The data must reside on the same vdisk as the OS

The Cisco UCS C220 which is currently used as the host for the Cisco Meeting Server 1000 could be used, but the VM database would only use a small percentage of the server's resources. Using this server, other VMs could be also hosted on the same server as the VM database, if desired.

[1]RAM requirements for the Database VM are 8GB plus 1GB of RAM per 100k cospaces in excess of 75k. For example a Database VM in a deployment supporting 375k cospaces will required the 8GB minimum RAM requirement plus 3GB of RAM to support the 300k cospaces in

excess of 75k.

D.4 Recorder and Streamer VM

Note: The new internal SIP recorder and streamer service cannot be used as an External recording or streaming service as the services rely on specific SIP header parameters passed by the Meeting Server Call Bridge. When calls from any other source that is not Meeting Server Call Bridge connect, the recorder/streamer will reject the call as it won't locate the specific SIP headers expected.

D.4.1 VM sizing for the new internal SIP recorder component

The recommended deployment for production usage of the recorder is to run it on a dedicated VM with a minimum of 4 vCPU cores and 4GB of RAM. The following table provides an idea of performance and resource usage for each of the recording types.

Table 8: Internal SIP recorder performance and resource usage

Recording Setting	Recordings per vCPU	RAM required per recording	Disk budget per hour	Maximum concurrent recording
720p	2	0.5GB	1GB	40
1080p	1	1GB	2GB	20
audio	16	100MB	150MB	100

Key point to note (applies to new internal recorder component only):

- Performance scales linearly adding vCPUs up to the number of host physical cores.

D.4.2 VM sizing for the new internal SIP streamer component

The recommended deployment for production usage of the streamer is to run it on a dedicated VM with a minimum of 4 vCPU cores and 4GB of RAM. The following table gives an idea of 3 recommended minimum specifications and the number of streams they can handle.

Table 9: Internal SIP streamer recommended specifications

Number of vCPUs	RAM	Number of 720p streams	Number of 1080p streams	Number of audio-only streams
4	4GB	50	37	100
4	8GB	100	75	200
8	8GB	200	150	200

Key points to note (applies to new internal streamer component only):

- Number of vCPUs should not oversubscribe the number of physical cores.
- Maximum number of 720p streams supported is 200 regardless of adding more vCPUs.
- Maximum number of 1080p streams supported is 150 regardless of adding more vCPUs.
- Maximum number of audio-only streams supported is 200 regardless of adding more vCPUs.

D.5 Web Scheduler

The Scheduler is a Meeting Server component that allows end users to schedule meetings via the web app. It is supported on Meeting Server Small,Meeting Server 2000 and Meeting Server on VM deployments. For Meeting Server on specification-based VM platforms, an additional 4 GB of RAM is required for running the scheduler component. There is no additional RAM requirement for Meeting Server Small and Meeting Server 2000. Scheduler supports sending email notifications via configuration of an SMTP email server. For more information on email server configuration, see Cisco Meeting Server Installation Guides.

One scheduler supports 150,000 meetings; two or three schedulers can be added to provide resiliency but the capacity remains at 150K scheduled meetings. Scheduled meeting data is stored in the Meeting Server database and both clustered and single box database deployments are supported.

The scheduler is deployed as a new component using the Meeting Server MMP. When the scheduler is enabled, it makes API requests to the Call Bridge over the loopback interface. It is therefore a requirement that the scheduler is deployed on a Meeting Server which is also hosting a Call Bridge. It is not possible to configure the scheduler to use a remote Call Bridge. See Cisco Meeting Server Deployment Guides for more information on how to deploy the scheduler.

D.6 MeetingApps

Web app features like File Sharing and Surveys are deployed on the MeetingApps service.The MeetingApps must be configured on a stand alone Meeting Server node without any other services. Depending on whether the participants are joining from an external or an internal network, MeetingApps can be configured on DMZ network or on internal network accordingly.

MeetingApps services cannot be configured on Meeting Server 2000. It is recommended to configure the MeetingApps only on a spec based Virtualized deployment of Meeting Server. However, you can use Meeting server 2000 or Meeting Server 1000 as a Call Bridge or Web bridge along with Meeting Apps on VM deployments with the following specification.

Number of vCPUs	RAM	Disk Space
8	16 GB	100 GB

The MeetingApps can be configured on VM deployments of Meeting Server using the MMP command **`meetingapps`**.

Appendix E Additional information on VMWare

E.1 VMWare

Core VMs should be configured to use the entire host. This ensures that a CPU core is available for the ESXi kernel to perform management and network operations.

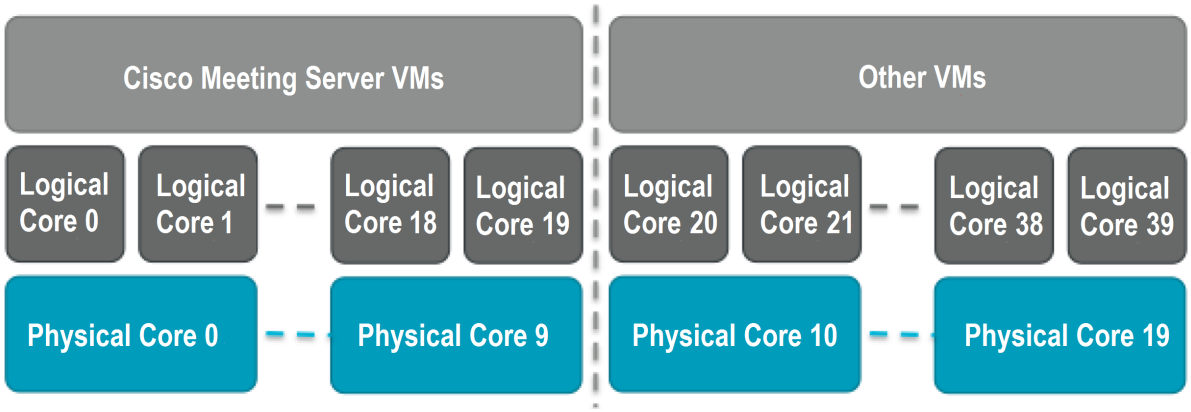
As part of internal testing we regular benchmark a variety of CPU and server configurations. During these tests synthetic calls are added over time, gradually increasing the demands on the VM and pushing it over capacity. Several internal statistics are monitored to ensure quality of user experience. In addition, ESXi statistics are monitored and diagnostic logs are collected.

Although not recommended, it is possible to run other VMs alongside the Cisco Meeting Server VM as long as CPU isolation domains are created to prevent contention. This technique is known as "anti-pinning", and involves explicitly pinning every VM to a subset of the cores. The Cisco Meeting Server VM must be the only VM pinned to its cores, and all other VMs need to be explicitly pinned to other cores.

For example, if a 20 core dual E5-2680v2 host is available, but only 25 concurrent 720p30 call legs are required, then anti-pinning can be used. Using the 2.5 calls/core ratio, 10 physical cores are required to provide this capacity. 10 cores can be used for other tasks.

With hyperthreading enabled, 40 logical cores are available and ESXi labels these logical cores by index 0-39. The Cisco Meeting Server VM should be allocated 20 virtual CPUs and configured with scheduling affinity 0-19. All other VMs running on the host must be explicitly configured with affinity 20-39 to create the pair of isolation domains. It may also be necessary to leave a physical core with no VMs pinned to it for the ESXi Hypervisor.

Figure 8: VM isolation domains created by pinning



VMXNet3 virtual network adapters are preferred as they require lower overhead than other adaptor types. All virtual network adapters should be the same type.

VMware Fault Tolerance (FT) is not supported as it is limited to single virtual core VMs. High level tools such as VMware vCenter Operations Manager are fully supported.

Note: If a VMWare hypervisor with EVC mode enabled is used, the EVC must be set to one of the following modes or higher:

"L2"/Intel® Nehalem generation (formerly Intel® Xeon Core™ i7)

EVC modes which enforce compatibility with older CPUs than those listed above, are not supported as they will disable SSE 4.2; SSE4.2 is required.

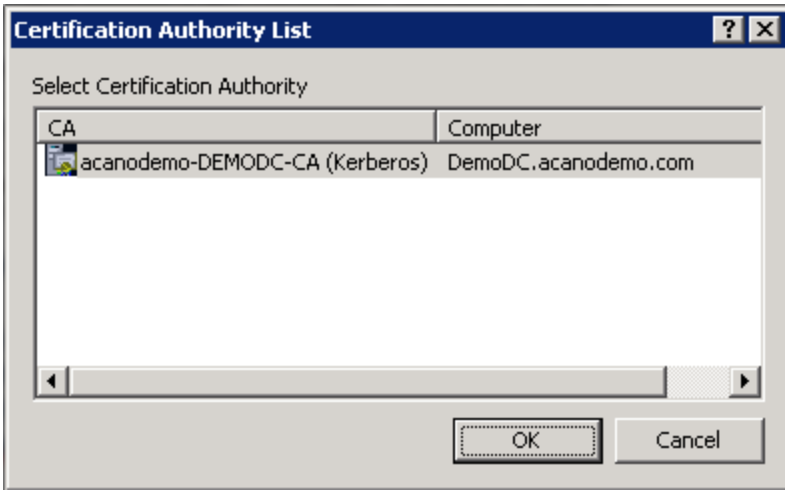
Appendix F Creating a certificate signed by a local Certificate Authority

This appendix covers the steps for signing the CSR using a local CA such as Microsoft Active Directory server with the Active Directory Certificate Services Role installed.

1. Transfer the file to the CA.
2. Issue the following command in the command line management shell on the CA server replacing the path and CSR name with your information:

   ```
   certreq -submit -attrib "CertificateTemplate:WebServer"
   C:\Users\Administrator\Desktop\webadmin.csr
   ```

3. After entering the command, a CA selection list is displayed similar to that below. Select the correct CA and click OK.

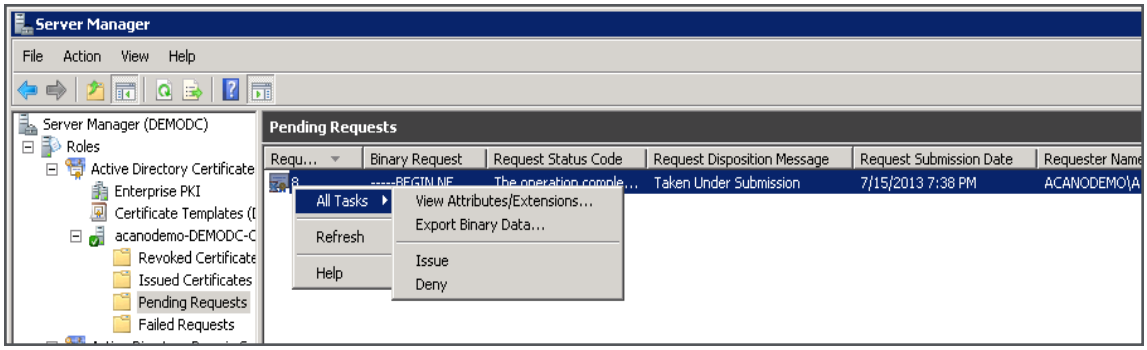


4. Do one of the following:
   - If your Windows account has permissions to issue certificates, you are prompted to save the resulting certificate, for example as webadmin.crt. Go on to step c below.
   - If you do not see a prompt to issue the resulting certificate, but instead see a message on the command prompt window that the 'Certificate request is pending: taken under submission', and listing the Request ID as follows. Note the RequestID

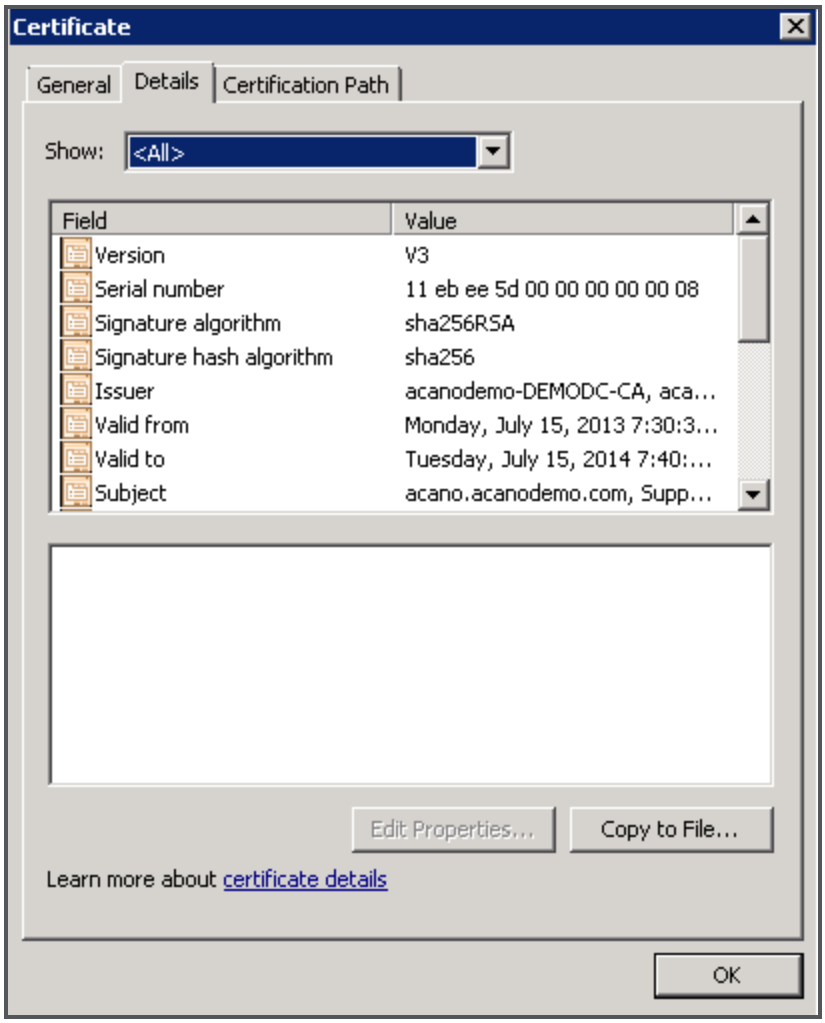
and then follow the steps below before going on to step c below.



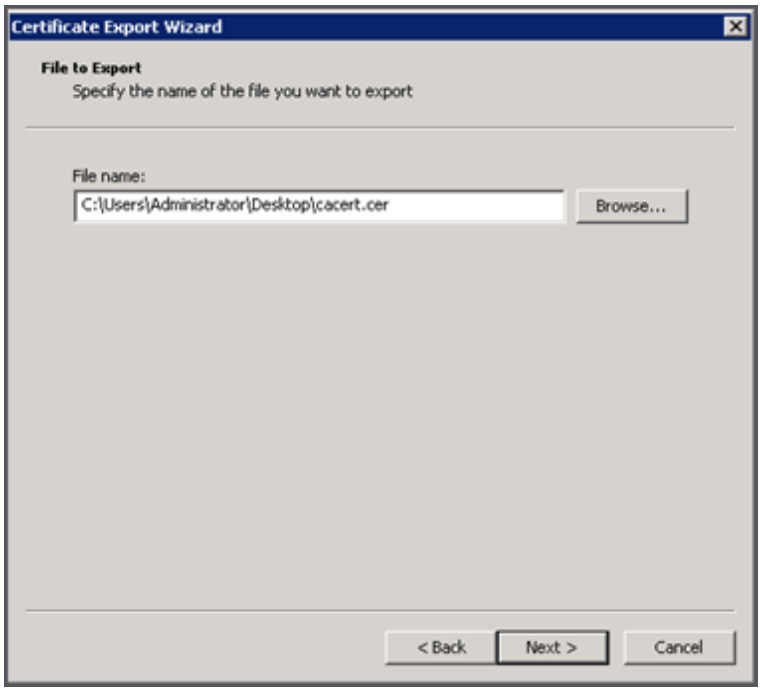
5. Using the Server Manager page on the CA, locate the Pending Requests folder under the CA Role.
6. Right-click on the pending request that matches the Request ID given in CMD window and select **All Tasks > Issue**.



7. The resulting signed certificate is in the Issued Certificates folder. Double-click on the certificate to open it and open the **`Details`** tab (see right).



8. Click **Copy to File** which starts the Certificate Export Wizard.
9. Select Base-64 encoded X.509 (.CER) and click **Next**.
10. Browse to the location in which to save the certificate, enter a name such as **`webadmin`** and click **Next**.



11. Rename the resulting certificate to **`webadmin.crt`**.

Now transfer the certificate (e.g. webadmin.crt) and private key to the MMP of the Cisco Meeting Server using SFTP, see Section 3.5.2.

CAUTION: If you are using a CA with the Web Enrolment feature installed, you may copy the CSR text including the BEGIN CERTIFICATE REQUEST and END CERTIFICATE REQUEST lines to submit. After the certificate has been issued, copy only the certificate and not the Certificate Chain. Be sure to include all text including the BEGIN CERTIFICATE and END CERTIFICATE lines and paste into a text file. Then save the file as your certificate with a .pem, .cer or .crt extension.

Cisco Legal Information

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

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

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

© 2026 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)