Cisco Meeting Server

Cisco Meeting Server 2.0+

Installation Guide for Cisco Meeting Server 1000 and Virtualized Deployments

March 20, 2018

Contents

Change History

Date	Change Summary
March 19, 2018	Added information for: call bridge configuration, Recorder and Streamer sizing and other miscellaneous improvements.
December 20, 2017	Added support for ESXi 6.5 and ESXi 6.0 Update 3 from Cisco Meeting Server version 2.3.
November 27, 2017	Added Cisco Meeting Server 1000 additional installation detail. Removed AWS references.

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 using VMware ESXi version 6.0 with virtual hardware vmx-11loaded onto the following platforms:

- Cisco Meeting Server 1000
- Cisco Multiparty Media 400v, 410v and 410vb
- specification-based VM platforms.

Note: From version 2.3, the Cisco Meeting Server supports ESXi 6.5 and ESX 6.0 Update 3. Both ESXi 6.5 and ESX 6.0 Update 3 allow you to disable TLS 1.0 and TLS 1.1 from communicating with ESXi.

Note: The Cisco Meeting Server software also runs as a virtualized deployment using Microsoft Hyper-V version 2.1. From version 2.4 of the Cisco Meeting Server software, Hyper-V will no longer be supported.

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 and Acano X-Series servers). For example, it is not possible to create a backup from a virtualized deployment and roll it back on an Acano X-series server or vice versa.

1.1 Overview of virtualized platforms

Cisco Meeting Server 1000: ships with VMWare ESXi version 6.0 and Cisco Meeting Server pre-installed. However, this may not be the latest version of Cisco Meeting Server software available. Follow the instructions in this guide to configure the Cisco Meeting Server 1000 and apply the license. Once the Cisco Meeting Server is operational, check the version of software installed using the MMP command **`version`**. The latest software is available here. To upgrade the software installed on the Cisco Meeting Server 1000, follow the instructions in the release notes for that software version.

Note: The default Cisco UCS ESXi credentials for the Cisco Meeting Server 1000 are: login as **root** with a password of **password**. You are advised to change this login admin account. Be aware that when you change the password, Cisco UCS ESXi will require a complex password.

Cisco Multiparty Media 400v, 410v and 410vb: if you purchased VMware license VMW-VS6-410-K9 with the 410v or 410vb then this can be used when you migrate the 410v/410vb to hosting the Cisco Meeting Server. Otherwise you will need to purchase a VMware license. You do not need to delete the TelePresence Server VM providing you have sufficient RAM to also hold the Cisco Meeting Server application. Simply use the **shutdown** command to turn off the TelePresence Server, before following the steps in this guide and installing the Cisco Meeting Server software.

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 and specification-based VM deployments.

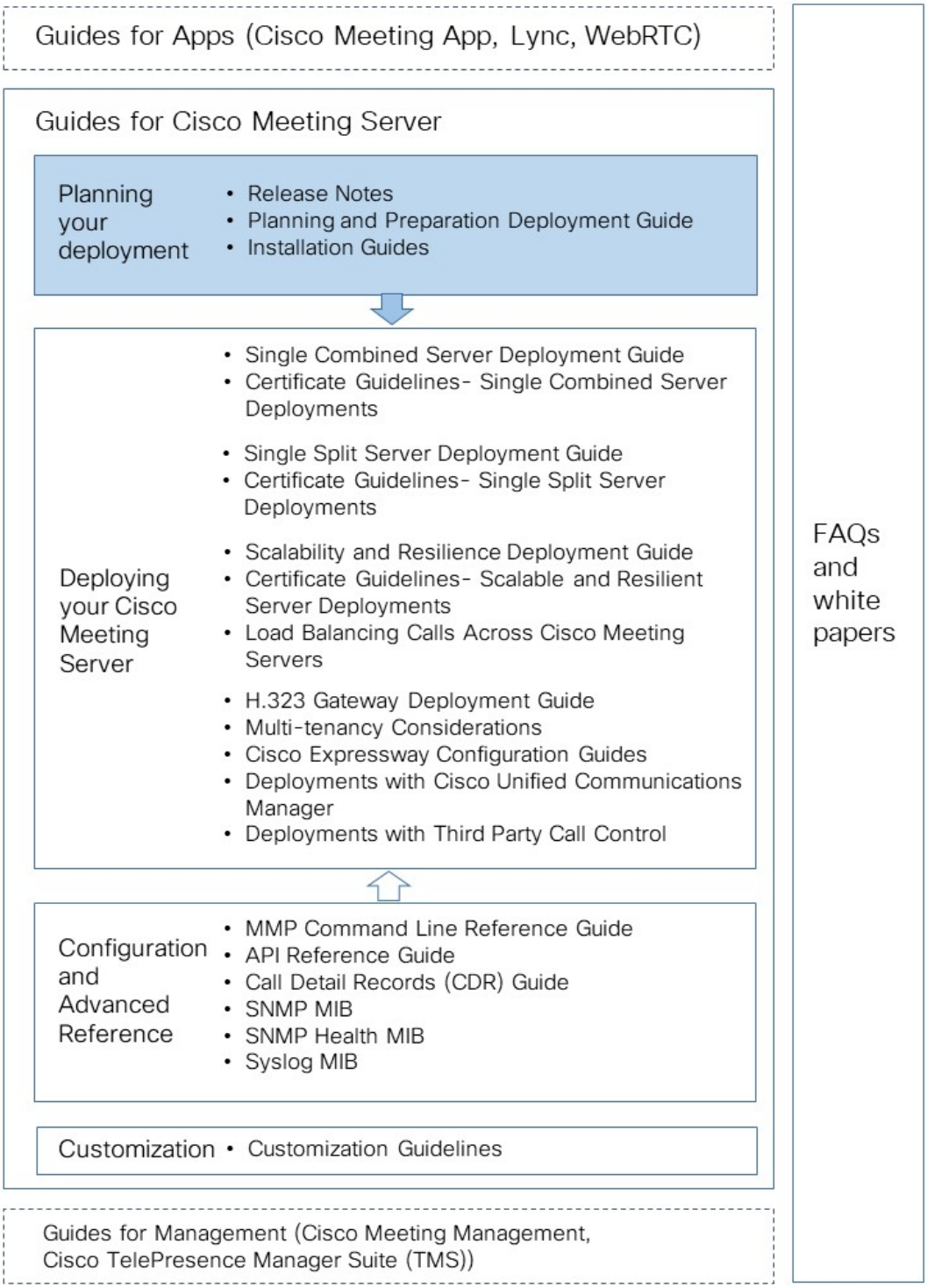
The Cisco Meeting Server 1000 is shipped with the software pre-installed. Go to Section 2.4 before going to Chapter 3 of this guide to start configuring the Cisco Meeting Server 1000.

Note: The Cisco Meeting Server 1000 has different settings to the specification-based VM server, the settings are pre-configured, do not change the settings.

If you are installing a specification-based VM deployment, check Sizing a VM then go to Chapter 2, before proceeding to Chapter 3 to configure the VM. Note that Chapter 2 is written for experienced VMware and Hyper-V administrators.

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



1.3 MMP differences between virtualized deployments and the Acano X-Series server

The MMP Command Reference details the full set of MMP commands. There are a few differences for a Cisco Meeting Server running as a virtualized deployment compared to running on an Acano X-Series server :

- There is a **`shutdown`** command that must be used to shutdown the VM, rather than using vSphere power button.
- The concept of a serial number does not apply to a virtualized solution; therefore the MMP **`serial`** command will not return a serial number.
- Similarly the **`health`** command is not available in the virtualized deployment.
- Other commands such as **`dns`** do not require an interface for virtualized deployments, and cannot take “mmp” as the interface.

2 Installation

This chapter applies to deployments on specification-based VM platforms and Cisco Meeting Server 1000. Follow Section 2.2 to deploy a VMware host, and Section 2.3 to deploy a Microsoft Hyper-V host. Follow Section 2.4 to deploy a Cisco Meeting Server 1000. If you need to check VM sizing information, see Appendix C.

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, and a VHD disk image is provided for Microsoft Hyper-V users. These are templates that set up a new VM with a single network interface, 16GB RAM 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 or .vhd disk image 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.

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 both Intel and AMD 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 and Microsoft Hyper-V as well as cloud services.

Table 1: Host requirements for the Cisco Meeting Server running on third party servers

	Minimum	Recommended
Server manufacturer	Any	Any
Processor type	Intel Nehalem microarchitecture AMD Bulldozer microarchitecture	Intel Xeon 2600 v2 or newer
Processor frequency	2.0GHz	2.5Ghz
RAM	1GB per core*	1GB per core*
Storage	100GB	100GB
Hypervisor	For up to 32 virtual cores use: VMware ESXi 5.0 Update 3 with virtual hardware vsm-08, or Hyper-V 2012	If your server supports upto 128 virtual cores then use: VMware ESXi 6.0 with virtual hardware vsm-11 or Hyper-V 2012 R2 If your server supports up to 64 virtual cores, use: VMware ESXi 5.1 Update 2 with virtual hardware vsm-09 or ESXi 5.5 Update 1 with virtual hardware vsm-10, or Hyper-V 2012 R2 **Note:** Refer to the VMware documentation for further information.

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

Table 2: 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.
- When comparing AMD and Intel processors, the number of AMD "Modules" (a pair of "cores" sharing resources) should be compared to Intel "cores" (which execute a pair of "hyperthreads"). In internal testing we have found that AMD processors provide 60-70% capacity of an equivalent Intel processor. For this reason Intel processors are recommended 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 Conferencing heading.
- If a VMWare Hypervisor with EVC mode enabled is used, the EVC must be set to one of the following modes or higher:
  "B1"/AMD Opteron™ Generation 4
  "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.
- For Hyper-V, the "Processor Compatibility Mode" MUST NOT be enabled as it disables CPU extensions, in addition SSE 4.2 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 4 and 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. This differs from the Acano Server releases which provided an ovf folder and associated files.

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

1. Download the .ova file from the Cisco web site.
2. In the vSphere Client go to **File > Deploy ovf Template**.
3. Browse to the .ova file and select it.
4. Follow the wizard instructions. The settings that must be selected are:
   a. Name the new VM.
   b. Select a Virtual disk storage folder to hold the VM disk.
   c. Ensure **Power On After Deployment** is not selected.

   Note: Depending on how your virtual host is set up, some of the wizard settings may not be displayed or may not be selectable.
5. When you see the message " Completed successfully" , click **Close**.

   The new Cisco Meeting Server VM is listed in the vSphere client.
6. Select the Cisco Meeting Server VM
7. From the **Getting Started** tab, select **Edit Virtual Machine** settings and **CPUs**.
   a. Edit VM settings and choose CPUs. Set Number of Virtual Sockets to 1.
   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.

      The number of logical cores can be found in the vSphere Client, ESXi Summary page. For the 40 call leg configuration above (Dual Intel E5-2650v2) the value will be 30.
8. Click **Power on.**
9. Open the vSphere **Console** tab.

When the process is complete, you see the `cms login` prompt.

10. Log in with the user name “admin” and the password “admin”. You will be asked to change the admin password.

    You are now logged into the MMP. Go on to Chapter 3.

2.3 Installing via Hyper-V on a specification-based server

Note: For every release of the Cisco Meeting Server for virtualized deployments, there will be a virtual hard drive image (.vhd) for new deployments and an upgrade image (.img) for upgrading existing deployment to the latest release. For a new Hyper-V deployment follow this section, for upgrade see the Release notes.

Note: Note: Microsoft Hyper-V will no longer be supported from version 2.4 of the Meeting Server software.

1. Download the .vhd file from the Cisco web site and upload it to your Hyper-V datastore.
2. In Hyper-V Manager, select the host you want to home this VM on, then from the **Action** pane/menu, create a new VM using **New > Virtual Machine**.
3. Follow the wizard instructions. The settings that must be selected are:
   a. Name the new VM.
   b. Select **Use an Existing Virtual Hard Disk**, and browse to the .vhd file above.
4. Click **Finish**

   The new Cisco Meeting Server virtual machine is created and listed.
5. Select the Cisco Meeting Server virtual machine, and configure its **Settings** from the **Action** pane/menu.
6. Select **Processor** to configure it.
   a. Set the Number of Virtual Processors 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.

      For the 40-call leg configuration above (Dual Intel E5-2650v2) the value will be 30.
   b. In Resource Control, configure:

i. Virtual machine reserve (percentage) to 100.

ii. Virtual machine limit (percentage) to 100.

iii. Relative weight to 100.

7. Select **Memory** and ensure that startup RAM is configured to the recommended requirements above.
8. Click **Apply** and **Start the Cisco Meeting Server VM**.
9. Select the Cisco Meeting Server VM and click **Connect**.

   When the process is complete, you see the `cms login` prompt.
10. Log in with the user name “admin” and the password “admin”. You will be asked to change the admin password.

CAUTION: Passwords expire after 6 months.

You are now logged into the MMP. Go on to Chapter 3.

2.4 Installing and initial configuration of Cisco Meeting Server 1000

2.4.1 Before You Start

You need the following to complete your installation:

- PAK license number
- VMware license activation codes or customer-supplied VMware license keys
- Internet and email access to complete the license retrieval steps
- A Windows computer running vSphere Client 6.0 or the permisssions to install vSphere client on the computer
- A console, either:
  - A monitor with a VGA connector and USB keyboard
    or
  - A PC with a serial adaptor, Cisco serial cable, and terminal program, and network connection with Internet Explorer or Firefox with JAVA installed and enabled

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 Cisco UCS C220 M4 Installation Guide https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C220M4/install/C220M4.pdf

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.

   The Meeting Server will automatically boot to the VMware console screen when startup is complete and should be visible on the monitor.

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 M. If you only have the resources for one network connection, remove the LAN connected to Ethernet1 and use it for the M port temporarily to enable the virtual console, and move it back to Ethernet1 after configuration. The M 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 (username: **`admin`**, password: **`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. The default username is **`root`** and the default password is **`password`**.
2. We recommend you change the default password:
   a. From the menu options, use the arrow and **Enter** keys to select **Configure Password**.
   b. Follow the prompts and set a password to use for the VMware root account.
   Note: VMware has high password complexity requirements– use a strong password including special characters, mixed case, and alpha and numeric characters.
3. From the menu options, use the arrow and Enter keys and select **Configure Management Network** and then **IPv4 Configuration**.
4. 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.
5. (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.
6. 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 M 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 M interface:
  a. You will not need the virtual console anymore to complete the install. Disconnect the Ethernet cable from the M 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 1000.

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–Configuring the VMware Instance using vSphere client

Now you connect to the VMware instance and complete the Hypervisor's initial configuration.

1. If you do not have vSphere 6.0 client installed and need to install it, follow these steps:
   a. Option 1: Download from the internet and install the client - http://vsphereclient.vmware.com/vsphereclient/VMware-viclient-all-6.0.0.exe

      or

   b. Option 2: Download from the local VMware instance:
      i. Using your Internet Browser, browse to your new server's IP, for example, **http://IPaddress**
      ii. Click the link for **Browse database in this host's inventory**
      iii. Enter the username **`root`** and password you configured in the VMware network management setup.
      iv. Navigate to **datastore1\OVA-ISO\VMware** and click the **VMware-viclient...** link to download the client installer.
      v. Once downloaded, locate the file and run the program to install the vSphere client.
2. Open vSphere client and in the connection window, enter the IP for your VMware instance, the username **`root`** and the password created during the VMware network management configuration. Click **Login** to connect to the server.
3. An SSL certificate warning appears when connecting to the server, click **Ignore** to continue. Upon connecting, you will also get a VMware evaluation notice, click **OK**.

2.4.4.1 Configuring VMware NTP

Configure the Hypervisor to have a valid NTP source so its logs will be accurate:

1. In the vSphere client, connect to the Meeting Server, and click on the Meeting Server in the left panel to select it.

2. In the right-hand panel, click the **Configuration** tab, and under **Software**, click **Time Configuration**.
3. In the resulting page, click the **Properties** link (in the top right corner).
4. In the **Properties** window, check the **NTP Client Enabled** checkbox and click the **Options** button.
5. Click **NTP Settings** from the list and click the **Add** button to add the NTP source(s) you wish to use.
6. Select **General** from the list.
7. Change the Service to **Start and Stop with the host**.
8. Click **Start** to start the service.
9. Click **OK** twice to close the time configuration pages.

2.4.5 Task 4—Retrieving and activating VMware Licenses

If you ordered VMware licenses from Cisco, the licenses will be delivered as Activation Codes in separate packaging or emails from Cisco. You require two 1-CPU licenses per Cisco Meeting Server1000. These activation codes must be converted to license keys using the VMware public website. You need internet and email access to complete this task.

2.4.5.1 Activate VMware activation keys

1. Use an internet browser (we recommend a browser other than Google Chrome for this task), go to https://www.vmware.com/oem/code.do?Name=CISCO-RESELL-AC
2. Login with a VMware account. If you do not have one, complete the steps provided on the webpage to create a new VMware profile.
3. Once logged in, enter the activation codes following your organization's policy on assigning software activation codes. After completing the steps, VMware will email the license codes to you.
4. 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. These steps are covered in detail on the VMware KB article: https://kb.vmware.com/s/article/2006973.
   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.
5. 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.

6. In the right panel, select the **Configuration** tab, then under **Software**, click on **Licensed Features**.
7. Current evaluation details display, click on the **Edit** link at the top right corner of the page.
8. In the resulting window, select **Assign a new key to this host** and click the **Enter** button to enter your license key.
9. Click **OK** close the dialog window.

Hypervisor basic setup is now complete.

2.4.6 Task 5—Accessing the Cisco Meeting Server 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 of **`root`** 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 “admin” and the password “admin”. You will be asked to change the admin password.

   CAUTION: Passwords expire after 6 months.

The rest of the configuration process follows that described in Chapter 3.

3 Configuration

3.1 Creating your own Cisco Meeting Server Administrator Account

For security purposes, you are advised to create your own adminisitrator 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, but up to 4 are supported (see the next section). The initial interface is “a”, equivalent to interface A on the Acano X-Series server. The MMP runs on this interface in the virtual deployment.

1. Configure the Network Interface speed using the following MMP commands.

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

   ```
   iface a
   ```

   To set the interface to 1GE, full duplex type:

   ```
   iface a 1000 full
   ```

   and to switch auto negotiation on or off, type:

   ```
   iface a autoneg <on|off>
   ```

We recommend that the network interface is set to auto negotiation unless you have a specific reason not to.

2. The “a” interface is initially configured to use DHCP. To view or reconfigure the IP settings:
   a. Go on to step b. if you are using static IP addresses.

      To find out the dhcp configured settings, type:

      ```
      ipv4 a
      ```

      Go on to step 3.

   b. Configure to use static IP addresses (skip this step if you are using DHCP)

      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
      ```

3. Set DNS Configuration
   a. To output the dns configuration, type:

      ```
      dns
      ```

   b. To set the application DNS server type:

      ```
      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, i.e. is the server is on IP 10.1.1.1

      ```
      dns add forwardzone . 10.1.1.33
      ```

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

      ```
      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, open the **Getting Started** tab.
2. Select **Edit Virtual Machine Settings**.
3. Add an Ethernet Adapter with type VMXNET3 in the usual way.

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

To do the same on Hyper-V.

1. In the Hyper-V Manager, select the Cisco Meeting Server VM, and select **Settings**
2. Select **Add Hardware**.
3. Add an Ethernet Adapter with type Network Adapter in the usual way.

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, seeSection 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 E.

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
   ```

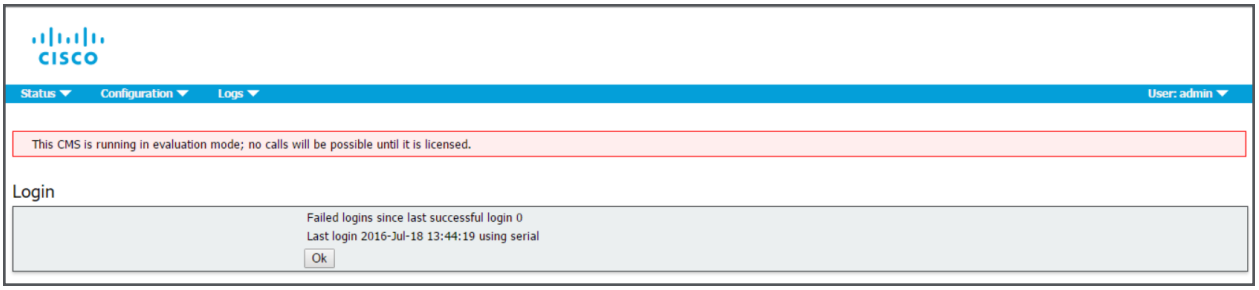
For example:

```
webadmin certs webadmin.key webadmin.crt
webadmin listen a 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.

The banner shown in Figure 2 below will be displayed until a cms.lic license file is uploaded.

Figure 2: Cisco Meeting Server in Evaluation Mode



After you upload and apply the license file, the banner is removed. However, before you can apply the license you need to configure the port that the Call Bridge will listen on, and upload the Call Bridge certificates. This is described in the deployment guides as the type of certificates required for the Call Bridge is determined by your deployment.

Refer to Section 4 for information on obtaining and applying a license file.

4 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.

Appendix B describes the Cisco Licensing available to purchase for the Cisco Meeting Server. After purchasing the licensing, follow this chapter to apply the license to the Cisco Meeting Server.

4.1 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 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 following 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 and the MAC address of your Meeting Server.
3. You will be sent a single license file via email. Rename the license file to cms.lic either before or during transfer.
4. Transfer the license file to the MMP of your Meeting Server using SFTP.
   a. Find the IP address of the MMP using the MMP command **`iface a`**
   b. Connect your SFTP client to the IP address of the MMP and log in using the credentials of an MMP admin user.

4.2 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: 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.

You are now ready to configure the Cisco Meeting Server. See:

- 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 Deployment 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.

Appendix A Technical specifications for Cisco Meeting Server 1000

A.1 Physical specifications:

Chassis: Cisco UCS C220 M4 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 Cisco UCS C220 M4 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 3: Call capacities

Type of calls	Cisco Meeting Server 2000	Cisco Meeting Server 1000	Cisco Multiparty Media 410v	Cisco Multiparty Media 400v
1080p60	125	24	16	9
1080p30/720p60	250	48	32	18
Full HD calls (1080p30)	250	48	32	18
HD calls (720p30)	500	96	64	36

Type of calls	Cisco Meeting Server 2000	Cisco Meeting Server 1000	Cisco Multiparty Media 410v	Cisco Multiparty Media 400v
SD calls (448p30)	1000	192	128	72
Audio calls	3000	3000	2000	1000

Appendix B Cisco Licensing

You will need activation keys and licenses for the Cisco Meeting Server and Cisco user licenses. Once you have purchased your licenses from your Cisco Partner, see Section 4 for information on applying Cisco licenses.

B.1 Cisco Meeting Server Licensing and Activation Keys

The following activation keys or licenses are required to use the Cisco Meeting Server:

- Call Bridge
- Branding
- Recording
- Streaming
- XMPP license activation key, this is now included in the software

B.1.1 Call Bridge Activation keys

The activation key allows the Call Bridge to be used for media calls. Activation keys need to be installed on:

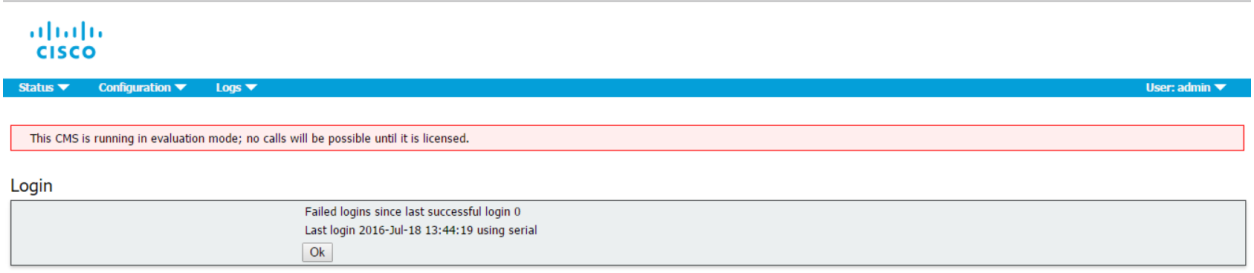
- the Cisco Meeting Server 1000,
- VM servers with Cisco Meeting Server software installed and configured as a combined server deployment (all components are on the same server),
- VM servers with Cisco Meeting Server software installed and configured as a Core server in a split server deployment.

You need to have the Call Bridge activated to create any calls, if you require demo licenses to evaluate the product then contact your Cisco sales representative.

Acano X-Series Servers do not require an activation key. VMs configured as Edge servers do not require an activation key for the Call Bridge.

To apply the license after uploading the license file, you need to restart the Call Bridge. However, you must configure the Call Bridge certificates and a port on which the Call Bridge listens before you can do this. These steps are part of the Cisco Meeting Server configuration and described in the Cisco Meeting Server deployment guides.

The banner “This CMS is running in evaluation mode; no calls will be possible until it is licensed.” is displayed in the Web Admin interface until a valid cms.lic file is uploaded. After you upload the license file, the banner is removed.



B.1.2 Branding

Customization is controlled by license keys with different keys providing different levels of customization.

The levels of customization supported are:

- No key: control of the background image and logo on the WebRTC landing page of a single Web Bridge via the Web Admin Interface; no API configuration is allowed.
- Single brand via API: only a single set of resources can be specified (1 WebRTC page, 1 set of voice prompts etc). These resources are used for all spaces, IVRs and Web Bridges.
- Multiple brand via API: different resources can be used for different spaces, IVRs and Web Bridges. These resources can be assigned at the system, tenant or space/IVR level.

To purchase branding license keys, you will need the following information:

- level of branding required (single/multiple),
- MAC address of interface A on servers hosting the Call Bridge.

B.1.3 Recording

Recording is controlled by license keys, where one license allows one simultaneous recording. The license is applied to the server hosting the Call Bridge (core server) which connects to the Recorder, not the server hosting the Recorder.

Note: The recommended deployment for production usage of the Recorder is to run it on a dedicated VM with a minimum of 4 physical cores and 4GB . In such a deployment, the Recorder should support 2 simultaneous recordings per physical core, so a maximum of 8 simultaneous recordings.

To purchase recording license keys, you will need the following information:

- number of simultaneous recordings,
- MAC address of interface A on the servers hosting the Call Bridges.

B.1.4 XMPP licenses

Customers who are using Cisco Meeting Apps require an XMPP license installed on the server(s) running the XMPP server application. The XMPP license is included in the Cisco Meeting Server software. You will also need a Call Bridge activated on the same Cisco Meeting Server as the XMPP server.

B.2 Cisco User Licensing

Cisco Multiparty licensing is the primary licensing model used for Cisco Meeting Server; Acano Capacity Units (ACUs) can still be purchased, but cannot be used on the same Call Bridge as Multiparty licenses. Contact your Cisco sales representative if you need to migrate ACUs to Multiparty licenses.

Multiparty licensing is available in two variations: Personal Multiparty Plus (PMP Plus) licensing, which offers a named host license, and Shared Multiparty Plus (SMP Plus) licensing, which offers a shared host license. Both Personal Multiparty Plus and Shared Multiparty Plus licenses can be used on the same server.

B.2.1 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 (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: Prior to release 2.1, Ad Hoc conferences never consumed PMP+ licenses. From 2.1 the initiator of the Ad Hoc conference can be identified and if they have been assigned a PMP+ license then that is used for the conference.

B.2.2 Shared Multiparty Plus Licensing

Shared Multiparty Plus (SMP Plus) provides a concurrent license that is shared by multiple users who host video meetings infrequently. It can be purchased at a reduced price with a UCM TP Room Registration license included when purchasing room endpoints, or it can be purchased separately. Shared Multiparty Plus enables all employees who do not have Cisco UWL Meeting licenses to access video conferencing. It is ideal for customers that have room systems deployed that are shared among many employees. All employees, with or without a Cisco UWL Meeting license 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). Each Shared

Multiparty Plus license includes one Rich Media Session (RMS) license for the Cisco Expressway, which can be used to enable business-to-business (B2B) video conferencing.

B.2.3 Cisco Meeting Server Capacity Units

Acano Capacity Units (ACUs) have been renamed Cisco Meeting Server Capacity Units. Each Capacity Unit (CU) supports 12 audio ports or the following quantity of concurrent media streams to the Cisco Meeting Server software (for the CU software license terms and conditions refer here).

Table 4: Capacity Unit Licensing

Media Stream	Number of licenses per Capacity Unit	Number of licenses required per call leg
1080p30	0.5	2
720p30	1	1
480p30	2	0.5

Each CU also entitles the Licensee to content sharing in each meeting containing at least one video participant. For more information refer to the terms and conditions of the CU license.

B.3 How Cisco User Licenses are applied

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 one or more members with a Cisco PMP Plus license has joined a space, then one of their licenses will be used, if not, then
- if the person that created the space (the owner) has a Cisco PMP Plus license, then the license of that owner is assigned, 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 user with a Cisco PMP Plus license, the license of that user is assigned, if not, then
- if present a Cisco SMP Plus license is assigned.

B.4 Setting up Cisco User Licensing

The following objects and fields have been added to the API to enable Admins to determine the consumption of Multiparty licenses:

- a new /system/licensing object, enabling an Admin to determine whether components of the Cisco Meeting Server have a license and are activated,
- a new /system/multipartyLicensing object that returns the number of licenses available and in use, and
- a new /system/multipartyLicensing/activePersonalLicenses object that indicates the number of active calls that are using a Personal Multiparty Plus user license,
- new userProfile field as part of LDAP Sync
- new hasLicense field to the userProfile, this indicates if a user has a license
- new ownerId and ownerJid fields per /coSpace object. If present, the ownerId field holds the GUID of the user that owns this coSpace, and ownerJid holds the JID of the user.

Note: The owner is set using the field ownerJid when POSTing or PUTing a /coSpace object. When GETing the /coSpace both the ownerJid and ownerId are returned for the user.

Appendix C Sizing a VM

The Cisco Meeting Server is designed for maximum flexibility, it is highly scalable and allows the "mix and matching" of optimized Acano X-series servers and VM deployments, for example using VM on edge servers and Acano X-Series server 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 D provides details for the most popular virtualization technologies, including VMware, and Microsoft HyperV. 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:

- a single VM can run all components,
- a single VM can run the edge components (Web Bridge, TURN server, Load Balancer) connected to an Acano X-Series server running the Call Bridge and other core components (for instance, XMPP server, H.323 Gateway).
- one VM running edge components, connecting to a second VM running the Call Bridge and other core components.

Figure 3 illustrates the Cisco Meeting Server software components and their typical deployment. Each instance can be on a VM or Acano X-Series server.

Figure 3: Cisco Meeting Server software components and their typical deployment

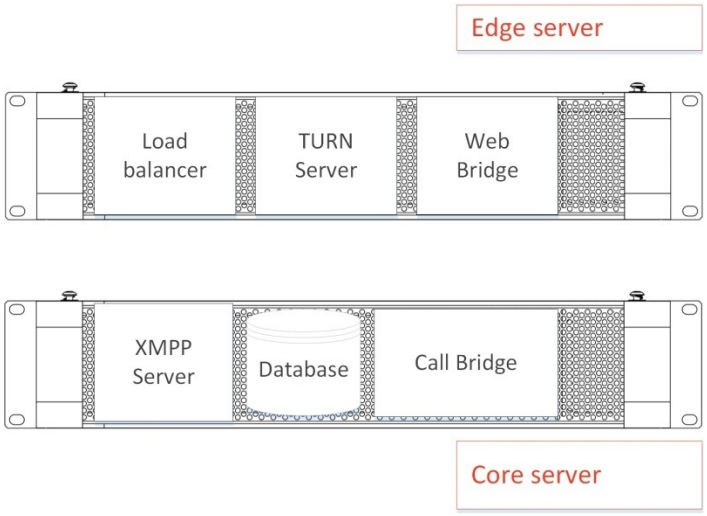
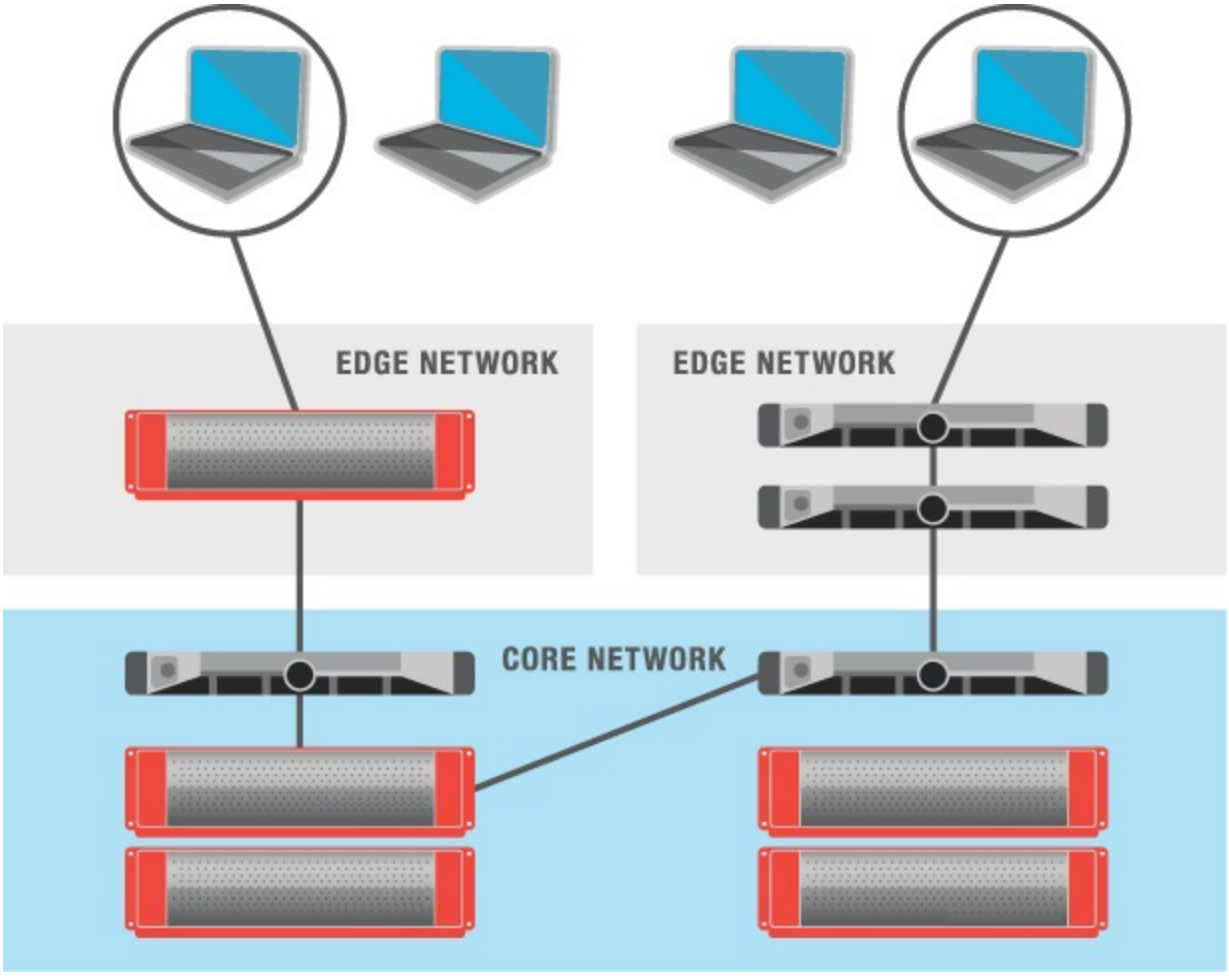


Figure 4 illustrates a distributed Cisco Meeting Server deployment using both VMs and Acano X-Series servers. Example signaling and media paths for two Cisco Meeting Apps are shown.

Figure 4: Distributed Acano deployment using both VMs and Acano Server



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.

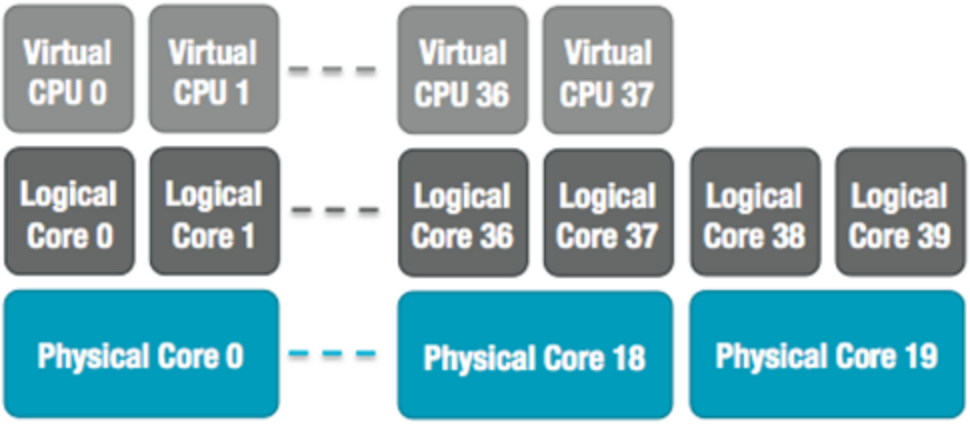
C.1 Call Bridge VM

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. If an option is available to choose both number of sockets and number of cores per socket, a single socket should be configured with all the virtual CPU cores.

Figure 5: 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. 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. For the system above, the VM should be configured with 19GB corresponding to the 19 physical CPU cores in use.

C.2 Edge VM

The requirements for other components are lower, and a VM can be used in a split core-edge deployment to provide edge functionality, for example Web Bridge, TURN server, Load Balancer on an edge VM. This edge VM can be coupled with either a core VM or an Acano X-Series server configured as a core.

A VM configured to provide edge services to an Acano X-Series server should be configured with a minimum of 8 virtual CPUs and 8 GB RAM. A VM providing edge services to a single Core VM should be configured with a minimum of 4 virtual CPUs and 4 GB RAM.

C.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:

- Eight vCPUs, 8GB 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 M4 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.

C.4 Recorder VM

Note: This section is applicable only if you choose to use a Recorder.

The recommended deployment for production usage of the Recorder is to run it on a dedicated VM with a minimum of 4 physical cores and 4GB . In such a deployment, the Recorder should support 2 recordings per physical core, so a maximum of 8 simultaneous recordings.

Table 5: Recommended Core VM configurations for Recording

Number of simultaneous recordings	CPU configuration	RAM configuration	Example systems
40	Dual Intel E5-2680v2	32 GB (8x4GB)	Cisco UCS C220 M3 Dell R620 HP DL380p Gen8
32	Dual Intel E5-2650v2	32 GB (8x4GB)	Cisco UCS C220 M3 Dell R620 HP DL380p Gen8
20	Single Intel E5-2680v2	16 GB (4x4GB)	Cisco UCS C220 M3
12	Single Intel E5-2640v2	8 GB (4x2GB)	Cisco UCS C220 M3 Dell R620 HP DL380p Gen8

In addition:

- All memory channels should be populated
- Out-of band-management systems configured to share a network port must be disabled
- Where available, hyperthreading should be enabled on the host
- The host must be dedicated to the Meeting Server VM
- If a VMWare hypervisor with EVC mode enabled is used, the EVC must be set to one of the following modes or higher:
- "B1"/AMD Opteron™ Generation 4
- "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.
- For Hyper-V, the "Processor Compatibility Mode" MUST NOT be enabled as it disables CPU extensions, in addition SSE 4.2 is required.

The Recorder uses variable bit rate, so it is not possible to accurately predict how much storage a recording will take. Our testing has shown that the size of 720p30 recordings ranges between 300MB to 800MB for 1 hour. In terms of budgeting it would be safe to assume 1GB per hour.

C.5 Streamer VM

Note: This section is applicable only if you choose to use a Streamer.

The recommended deployment for production usage of the Streamer is to run it on a separate VM. This VM should be sized with 1 vCPU and 1GB of memory per 6 concurrent streams, with a minimum of 4 vCPUs and a maximum of 32vCPUs.

Appendix D Additional information on VMWare and Microsoft Hyper-V

D.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.

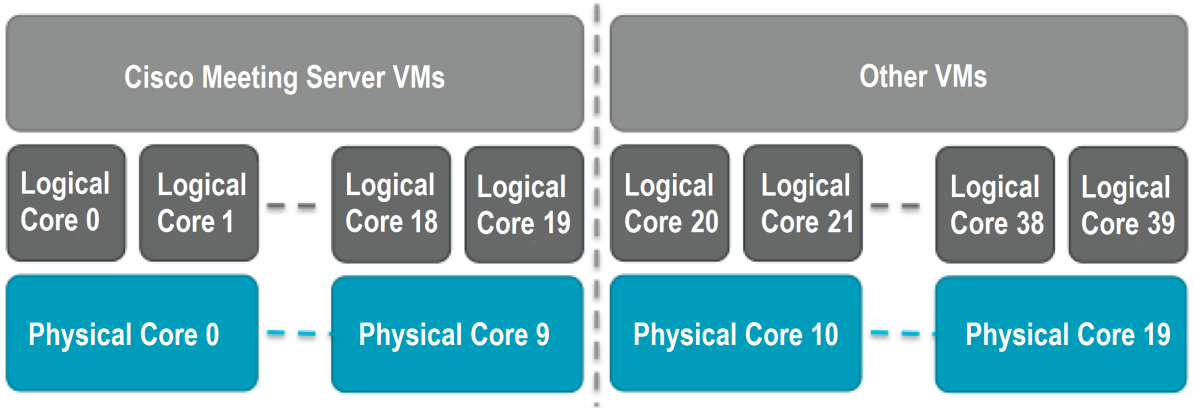
As part of internal testing we regular benchmark a variety of CPU and server configurations. During these tests synthetic calls are added over time, gradually increasing the demands on the VM and pushing it over capacity. Several internal statistics are monitored to ensure quality of user experience. In addition, ESXi statistics are monitored and diagnostic logs are collected. Since Acano is a VMware Technology Alliance Partner, these logs are submitted to VMware QA teams as part of VMware Ready certification.

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 scheduler.

Figure 6: 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 vMotion and High Availability (HA) technologies are fully supported. 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:

"B1"/AMD Opteron™ Generation 4

"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.

D.2 Microsoft Hyper-V

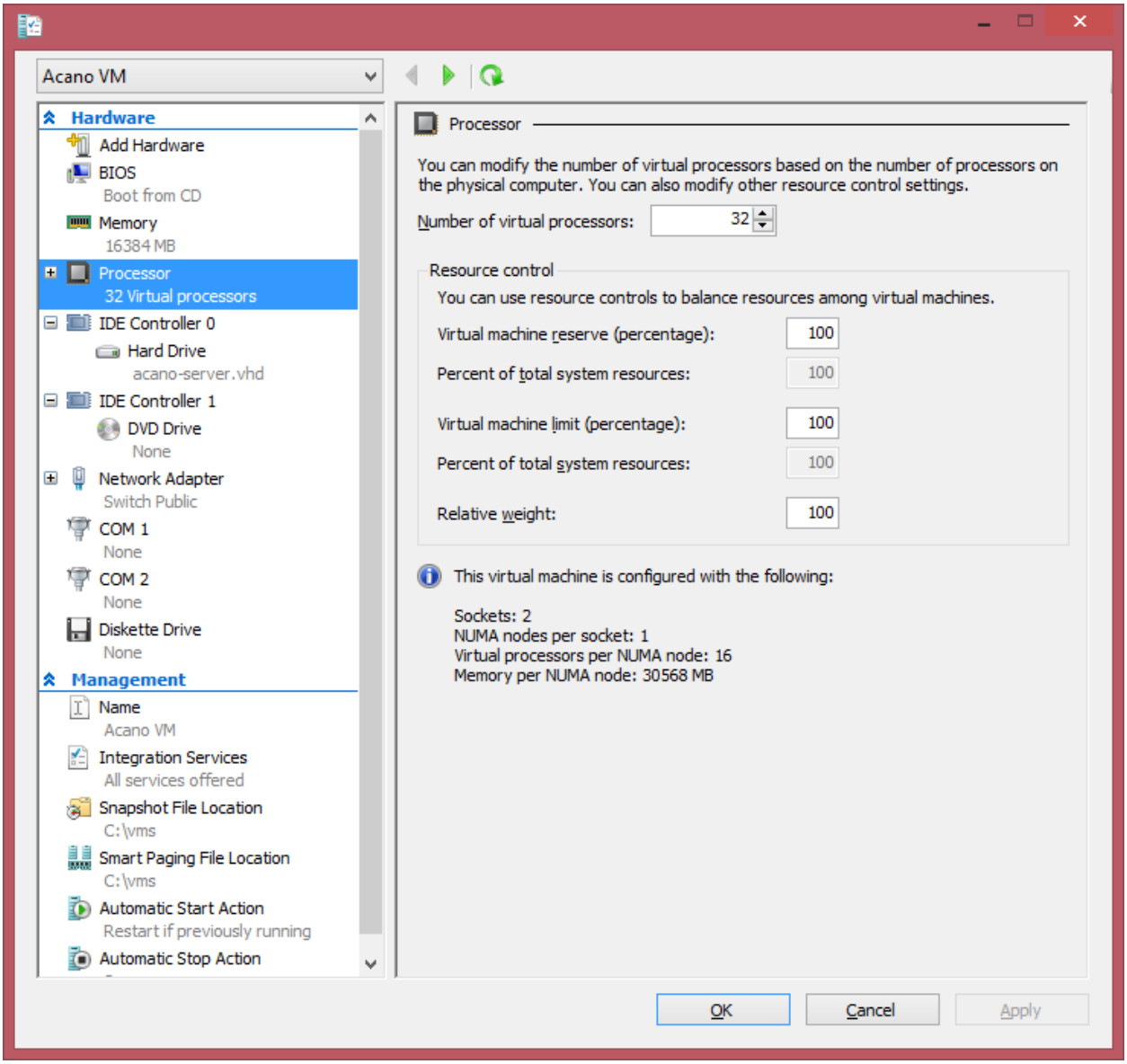
The Cisco Meeting Server supports Microsoft Hyper-V 2012 and 2012 R2. VHD disk images are created during software release and should be used for deployment. The host should be dedicated to the Cisco Meeting Server VM, leaving one physical core free for system tasks. Standard virtual network adapters are preferred, as they require fewer resources than legacy network adapters.

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. For example, a dual E5-2680v2 system has 40 virtual CPUs available, of which 38 should be allocated to the VM. Capacity will be approximately 2.5 720p30 call legs per physical CPU core for an E5-2600 or later host.

Hyper-V does not support CPU pinning. However, the "Virtual Machine reserve" option should be set to 100% to dedicate resources to the Acano VM.

Note: The "Processor Compatibility Mode" MUST NOT be enabled as it disables CPU extensions, in addition SSE 4.2 is required.

Figure 7: Typical settings for a Cisco Meeting Server VM deployment



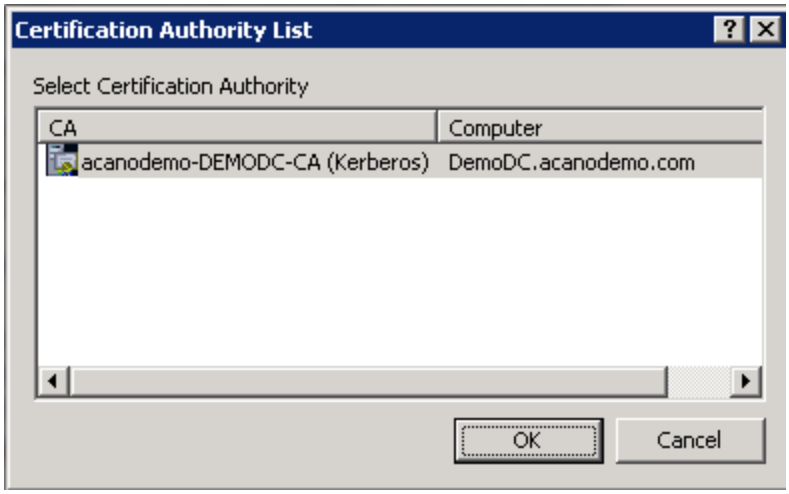
Appendix E Creating a certificate signed by a local Certificate Authority

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.

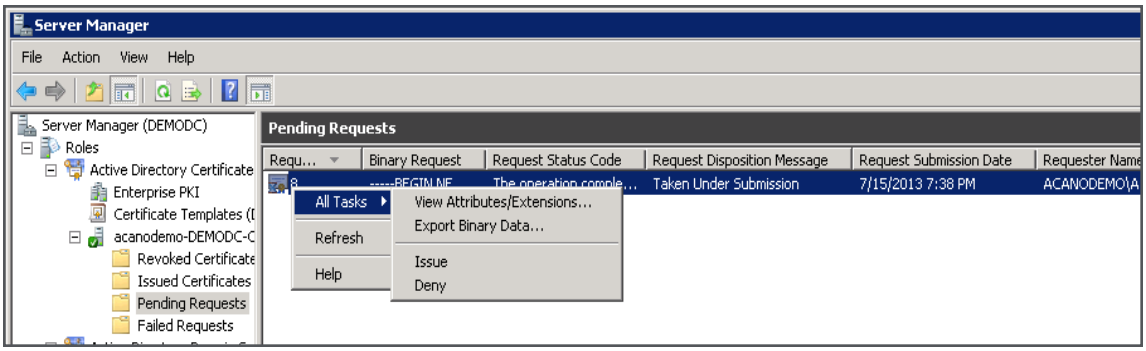


4. Do one of the following:
   - If your Windows account has permissions to issue certificates, you are prompted to save the resulting certificate, for example as webadmin.crt. Go on to step c below.
   - If you do not see a prompt to issue the resulting certificate, but instead see a message on the 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.

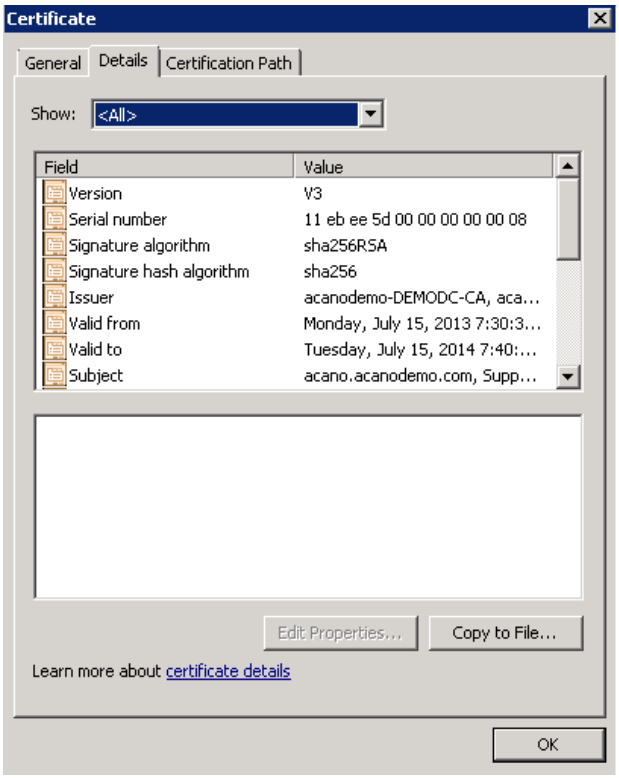
```
C:\Users\Administrator>certreq -submit -attrib "CertificateTemplate:WebServer" C
:\Users\Administrator\Desktop\demokitcsr.pem
Active Directory Enrollment Policy
  {0BD5D0B7-591F-4C77-AFEC-3C0E470F77D5}
  ldap:
RequestId: 8
RequestId: "8"
Certificate request is pending: Taken Under Submission (0)

C:\Users\Administrator>_
```

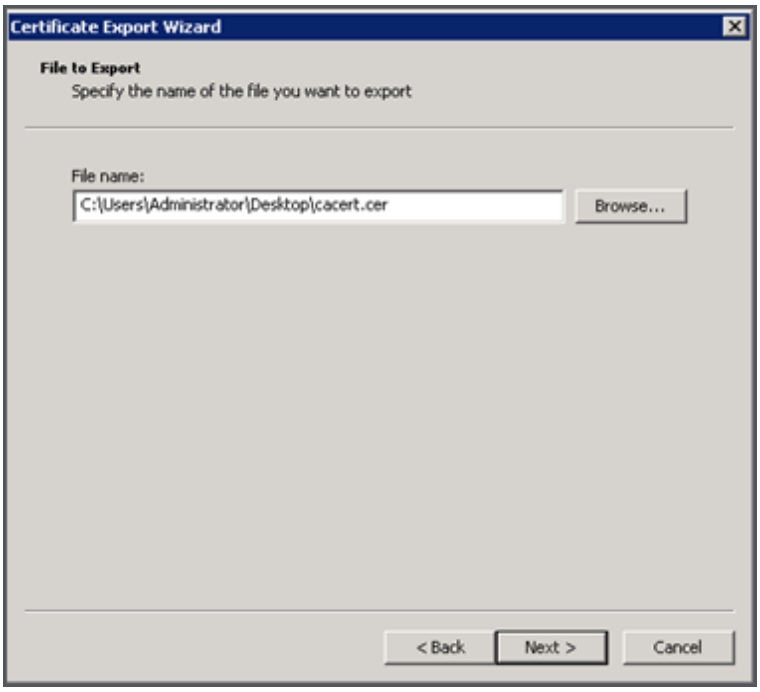
5. Using the Server Manager page on the CA, locate the Pending Requests folder under the CA Role.
6. Right-click on the pending request that matches the Request ID given in CMD window and select **All Tasks > Issue**.



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 are considered un-Controlled copies and the original on-line version should be referred to for latest version.

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

Cisco Trademark