Cisco Meeting Server

Cisco Meeting Server 2.0+

Installation Guide for Virtualized Deployments

January 06, 2017

Contents

1 Introduction

The 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 Meeting Server, people connect regardless of location, device, or technology.

The Cisco Meeting Server software runs as a virtualized deployment using either VMWare ESXi version 6.0 with virtual hardware vmx-11, or Microsoft Hyper-V version 2.1, loaded onto the following platforms:

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

It also runs on Acano X-Series servers as a physical deployment.

Customers often use the Acano X-Series server for core functionality and deploy the edge services on a VM for geographic distribution.

Note: For platforms with fewer than 64 virtual cores, ESXi5.1 (and virtual hardware vmx-09) is recommended, see Section 1.3.2.

The functionality, and user experience for participants, is identical across all platforms. However, deployments are not interchangeable between the virtualized deployments and the Acano X-Series server. 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 platforms

Cisco Meeting Server 1000: ships with VMWare ESXi version 6.0 and Cisco Meeting Server pre-installed. You need to install the license file before deploying the server. Follow the instructions in the Cisco Meeting Server release notes.

Note: If you upload Acano server R1.9 or earlier to the Cisco Meeting Server 1000 then you will experience reduced performance, as R1.9 does not support ESXi 6.0.

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.

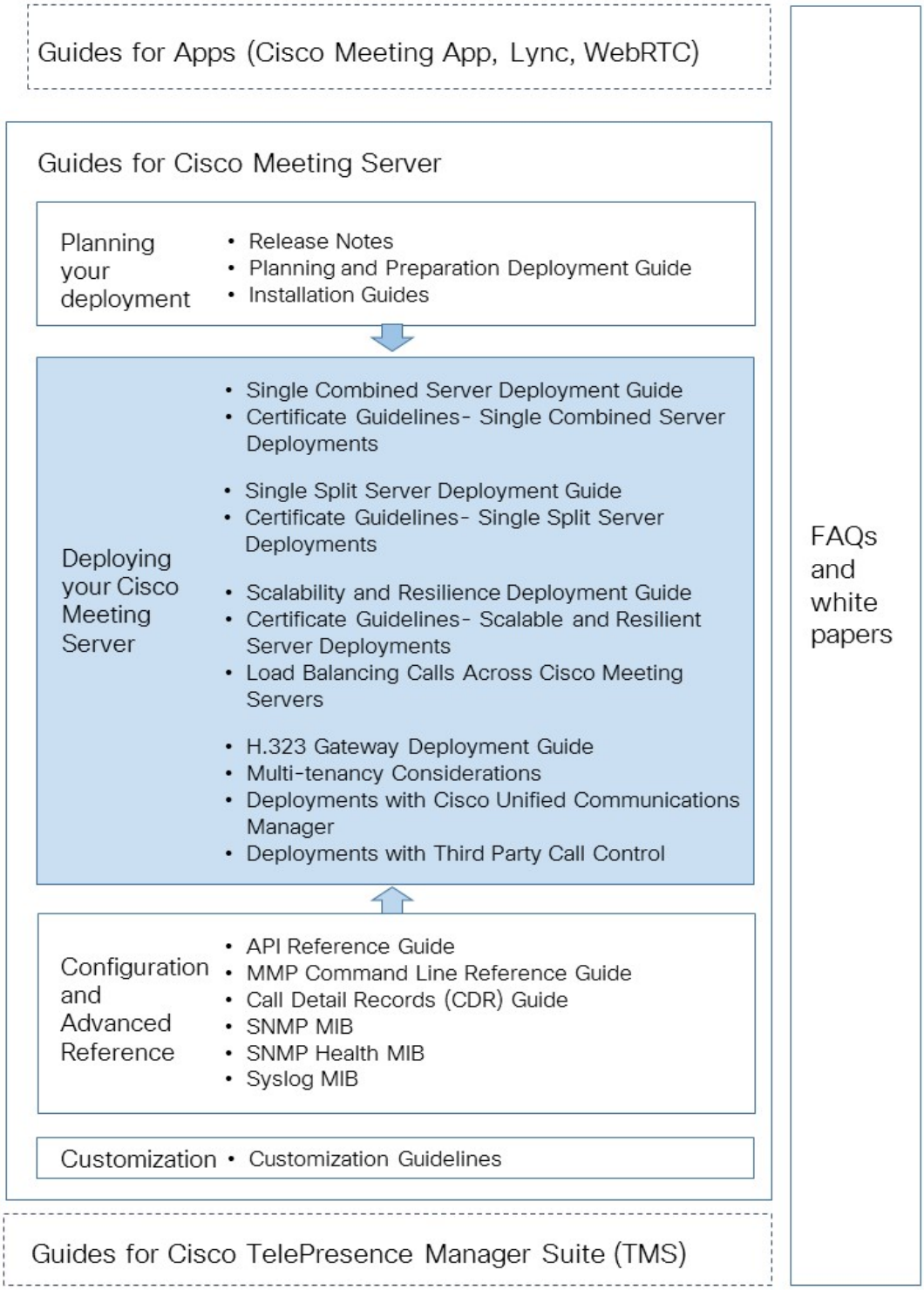
specification-based VM platforms: if you are upgrading the server from a virtualized Acano server, then follow the instructions in the Cisco Meeting Server release notes. If this is a new installation, then follow this guide to create a VM and install the Cisco Meeting Server software.

Acano X-Series servers: follow the upgrade instructions in the Cisco Meeting Server release notes to upgrade to Cisco Meeting Server software.

1.2 How to use this Guide

This guide is written for experienced VMWare and Hyper-V administrators. Follow this guide to install the Cisco Meeting Server as a virtual deployment running Release 2.0 software. After installing the Cisco Meeting Server you need to configure the server for your particular deployment. For further configuration information refer to the Deployment Guide that is most appropriate to your targeted deployment, see Figure 1.

Figure 1: Cisco Meeting Server installation and deployment documentation



1.3 Before You Start

1.3.1 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.

1.3.2 Host requirements for the Cisco Meeting Server

The Meeting Server runs on a broad range of standard Cisco servers as a VM deployment, and also 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 such as Amazon AWS.

Table 1: Host requirements for the Cisco Meeting Server

	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

	Minimum	Recommended
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 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 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 A for information on licensing.

1.3.3 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

The Cisco Meeting Server 1000 is shipped with the software pre-installed. Follow chapter 3 of this guide to start configuring the Cisco Meeting Server 1000, and chapter 4 for information on obtaining and applying a license file. Use the Planning and Preparation Deployment Guide to guide you on deciding the appropriate configuration of the Cisco Meeting Server 1000, and then follow the appropriate deployment and certificate guides.

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.

This chapter only applies to manual deployments on specification-based VM platforms. Follow Section 2.1 to deploy a VMware host, and Section 2.2 to deploy a Microsoft Hyper-V host.

2.1 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.

2.2 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.

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.

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

3 Configuration

3.1 Creating your own Administrator Account

For security, create at least one new admin account with the following MMP command (see the MMP Command Reference for details).

```
user add <name> admin
```

You will be prompted for a password which you must enter twice. Log in with the new account - you will be asked to change your password.

Note: You must have at least two admin level accounts at all times: then if you lose the password for one account you can still log in with the other one and reset the lost password. We recommend that you create two new accounts and then delete the default "admin" account; because the username "admin" is not very secure.

Note: Any MMP user account at the admin level can also be used to log into the Web Admin Interface, you cannot create users through the Web Admin Interface command.

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.

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 Creating the Web Admin Interface Certificate

The Web Admin is only accessible through HTTPS, you need to create a security certificate to install onto the Cisco Meeting Server so you can enable the Web Admin Interface and be able to log into it.

The information in step 1 below assumes that you trust Cisco to meet requirements for the generation of a private key. 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 uploading the key/certificate pair, go to Section 3.5.

Note: if testing your Cisco Meeting Server in a lab environment, you can generate a key and a self-signed certificate on the server. Self-signed certificates are not recommended for use in real deployments (see http://en.wikipedia.org/wiki/Self-signed_certificate). 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). Then go to Section 3.5

---

1. Follow this step if you trust that Cisco meets the requirements for generation of private key material. This step explains how to generate a private key and the associated Certificate Signing Request with the MMP **pki csr** command, export them for signing by a CA, and then copying the signed certificate file on to the Cisco Meeting Server.
   a. Log in to the MMP and generate the private key and certificate signing request:

      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"
```

b. Send the CSR to one of the following:

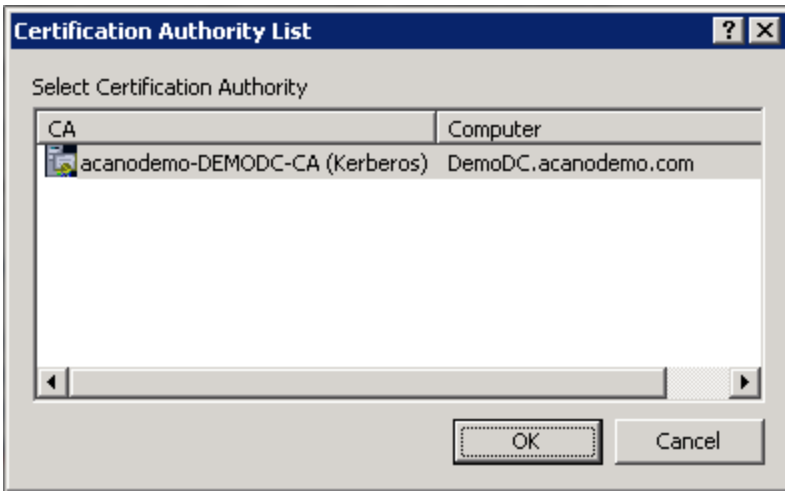
- To a Certificate Authority (CA), such as Verisign who will verify the identity of the requestor and issue a signed certificate.
- To a local or organizational Certificate Authority, such as an Active Directory server with the Active Directory Certificate Services Role installed.

  i. Transfer the file to the CA.

  ii. 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
  ```

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

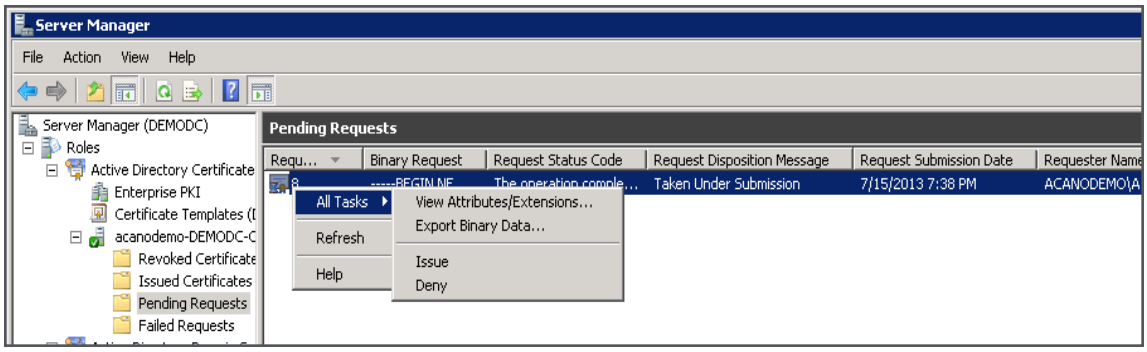


iv. Do one of the following:

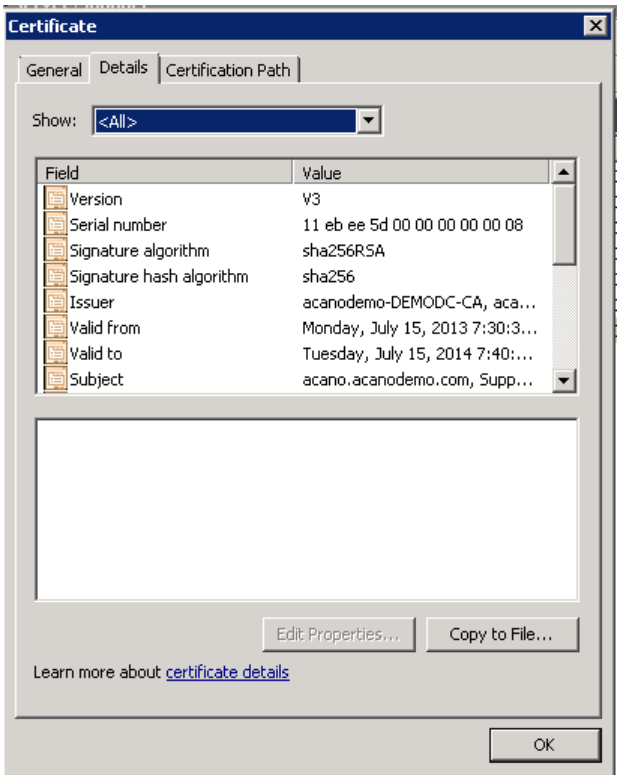
- If your Windows account has permissions to issue certificates, you are prompted to save the resulting certificate, for example as webadmin.crt. Go on to step c below.
- If you do not see a prompt to issue the resulting certificate, but instead see a message on the command prompt window that the 'Certificate 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.

v. Using the Server Manager page on the CA, locate the Pending Requests folder under the CA Role.

vi. Right-click on the pending request that matches the Request ID given in CMD window and select **All Tasks > Issue**.



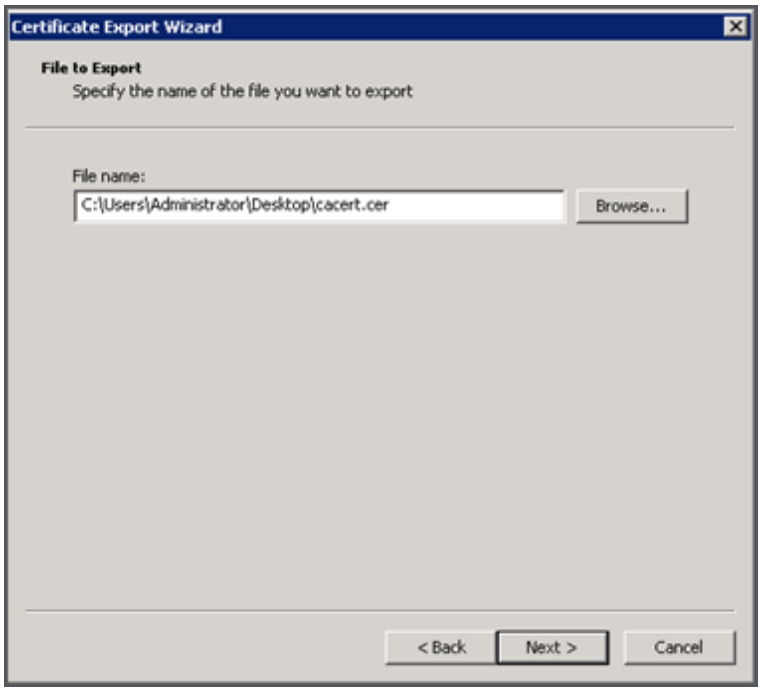
vii. The resulting signed certificate is in the Issued Certificates folder. Double-click on the certificate to open it and open the **`Details`** tab (see right).



viii. Click **Copy to File** which starts the Certificate Export Wizard.

ix. Select Base-64 encoded X.509 (.CER) and click **Next**.

x. Browse to the location in which to save the certificate, enter a name such as **`webadmin`** and click **Next**.



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

c. Transfer both the certificate (e.g. webadmin.crt) to the MMP of the Cisco Meeting Server using SFTP.

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.

3.5 Configuring the Web Admin Interface for HTTPS Access

Note: The deployment automatically sets up the Web Admin Interface to use interface A.

1. Establish a SSH connection again to the MMP and sign in.
2. If you want to use a different interface, enter the following commands to configure the Web Admin Interface:

```
webadmin certs webadmin.key webadmin.crt
webadmin listen a 443
webadmin restart
```

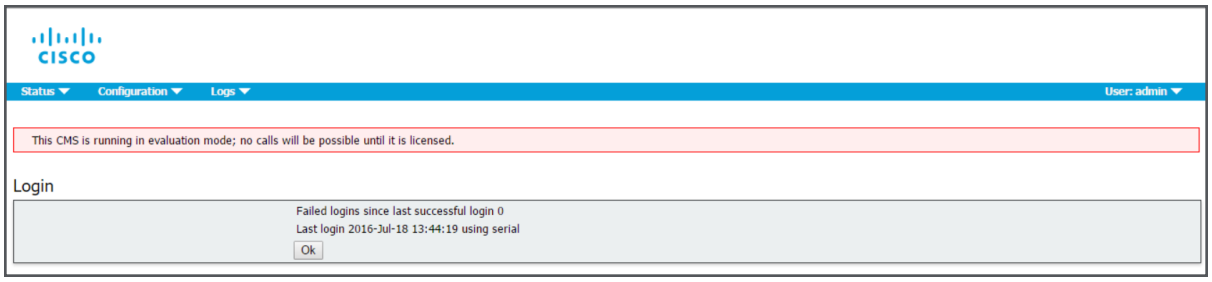
```
webadmin enable
```

Note: Be sure to use the same names as the certificates you uploaded.

3. 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. After you upload the license file (see Section 4.1), the banner is removed.

   Figure 2: Cisco Meeting Server in Evaluation Mode



Note: Any two interfaces of Cisco Meeting Server must not be put into the same subnet. The only exception is that the ADMIN interface of a physical Acano X-Series server can be on the same subnet as one of the other interfaces (A to D)—and is probably a common deployment.

Now refer to Chapter 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 A 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

For customers with a Cisco contract:

1. Purchase your activation keys and licenses through Cisco's ecommerce tool.

   You will receive an email with a “PAK” code, and the url of a web site where you need to register the PAK code with the MAC address of your Meeting Server.

2. 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.

   ---

3. Register the PAK code and the MAC address of your Meeting Server.
4. You will be sent a single license file via email. Rename the license file to cms.lic either before or during transfer.
5. 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.
6. Restart the Call Bridge.

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. These

steps were covered in Section 3.4 and Section 3.5.

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.

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

- the Single Combined Server Deployment Guide if you are deploying on a single host server
- the Single Split Server Deployment Guide if you are deploying on a split Core/Edge deployment
- the 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.

Appendix A Cisco Licensing

You will need activation keys and licenses for the Cisco Meeting Server and Cisco user licenses. For information on purchasing and applying Cisco licenses, see Section Appendix A.

A.1 Cisco Meeting Server Licensing and Activation Keys

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

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

A.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:

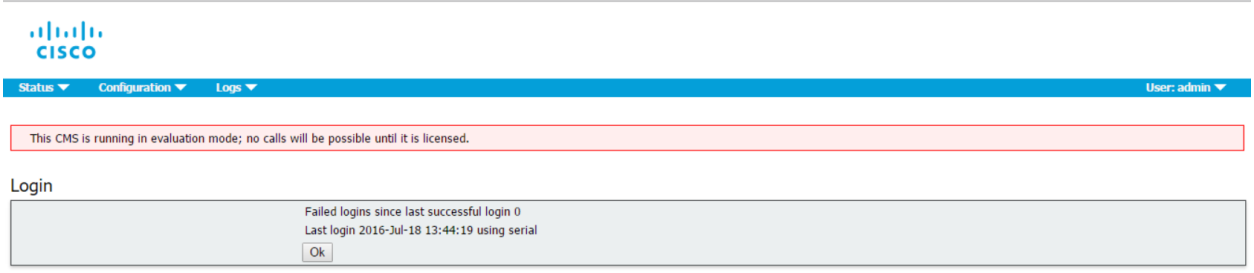
- the Cisco Meeting Server 1000,
- VM servers with Cisco Meeting Server software installed and configured as a combined server deployment (all components are on the same server),
- VM servers with Cisco Meeting Server software installed and configured as a Core server in a split server deployment.

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 or Cisco partner.

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 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.



A.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.

A.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.

A.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 Meeting Server as the XMPP server.

A.2 Cisco User Licensing

Call 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.

A.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.

A.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.

A.2.3 Cisco Meeting Server Capacity Units

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

Table 3: 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.

A.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 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 present a Cisco SMP plus license is assigned.

A.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 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 B Sizing a VM

The 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 Meeting Server software can run on. Appendix B provides details for the most popular virtualization technologies, including VMware, Microsoft HyperV and Amazon Web Services. The 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 Meeting Server or individual components of the 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 Meeting Server software components and their typical deployment. Each instance can be on a VM or Acano X-Series server.

Figure 3: Meeting Server software components and their typical deployment

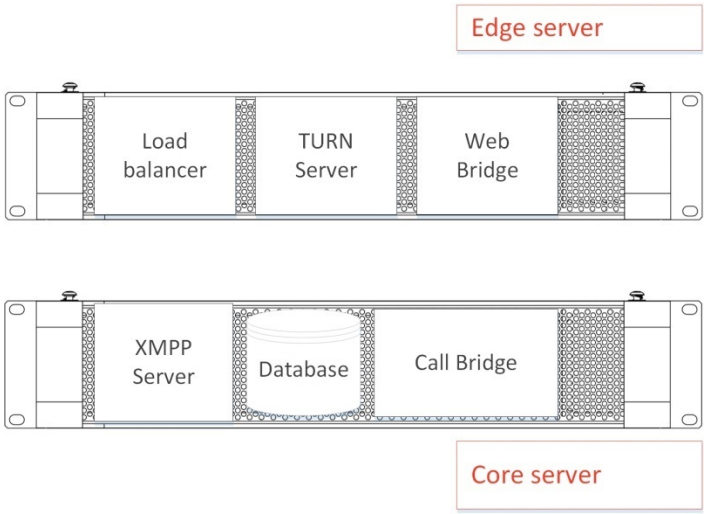
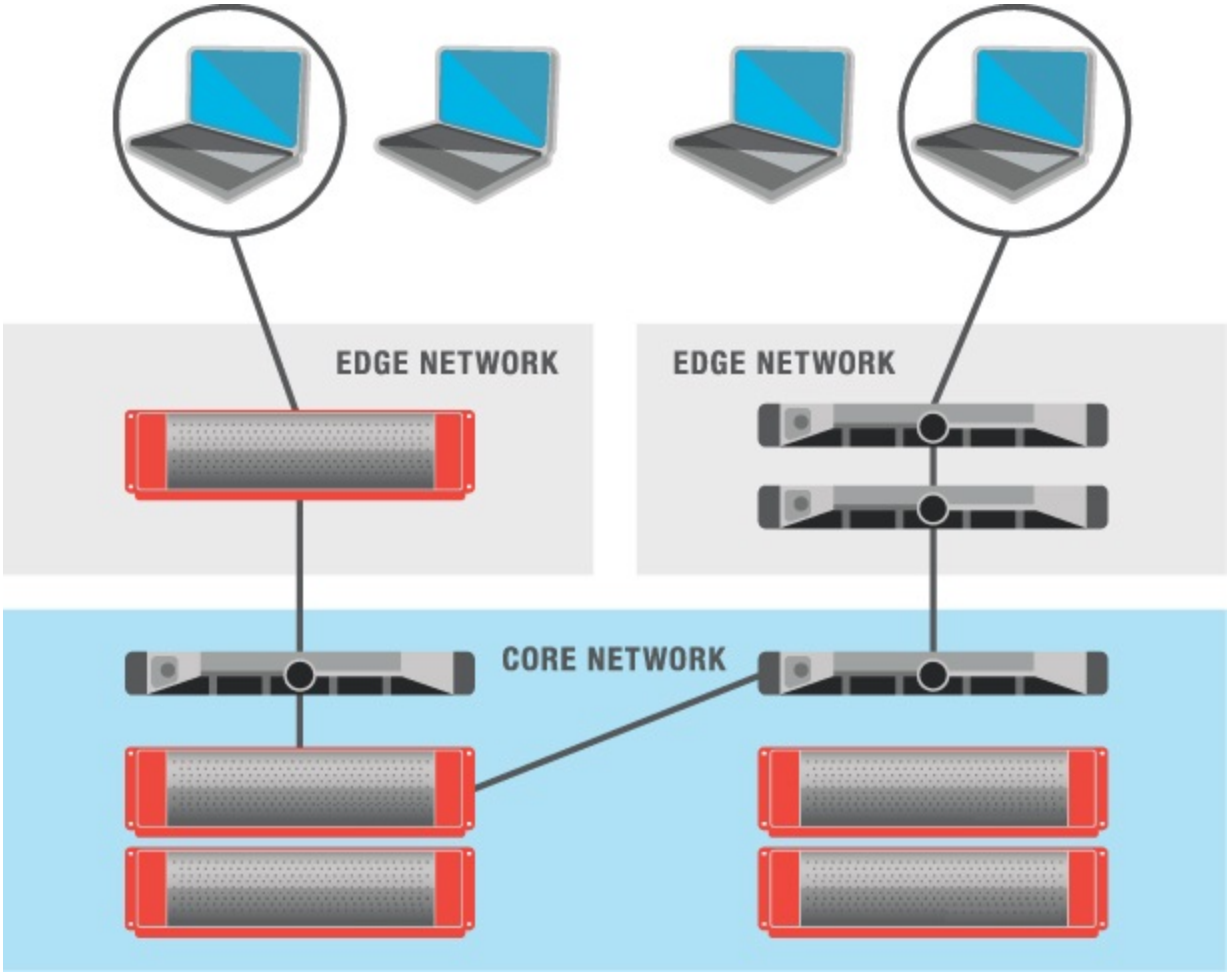


Figure 4 illustrates a distributed Meeting Server deployment using both VMs and Acano X-Series servers. Example signaling and media paths for two Cisco Meeting Apps are shown.

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



When a VM is configured to run one or more 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.

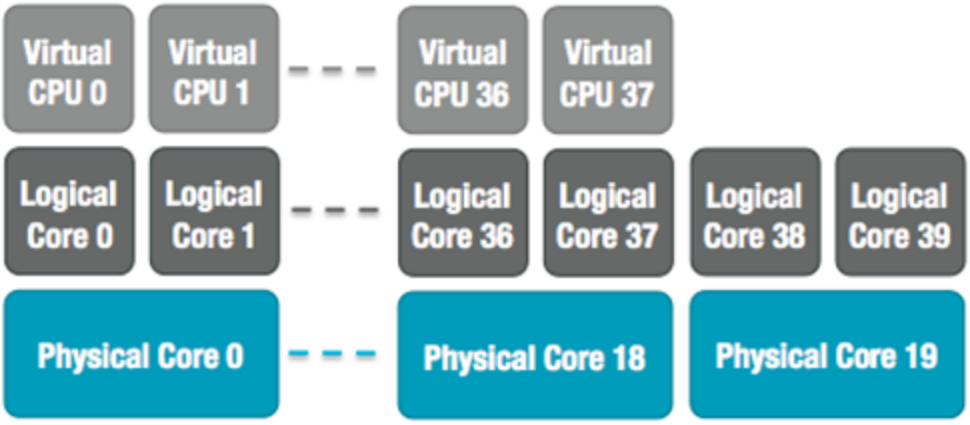
B.1 Call Bridge VM

The Call Bridge carries out the media transcoding for the 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 Meeting Server VM virtual CPUs or by contention for CPU resources amongst VMs, causes scheduling delays and results in degraded media quality. A 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.

B.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.

Appendix C Additional information on VMWare, Microsoft Hyper-V and Amazon Web Services

C.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.

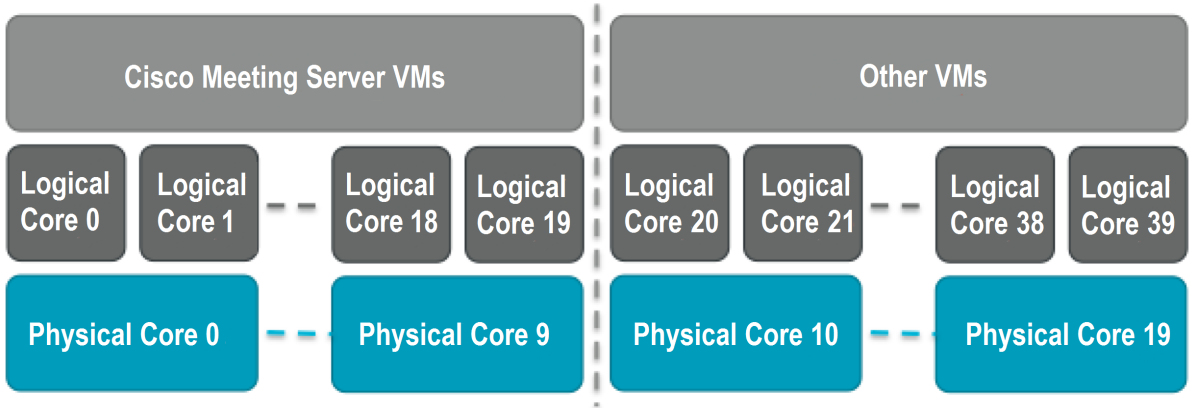
As part of internal testing we regular benchmark a variety of CPU and server configurations. During these tests synthetic calls are added over time, gradually increasing the demands on the VM and pushing it over capacity. Several internal statistics are monitored to ensure quality of user experience.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

C.2 Microsoft Hyper-V

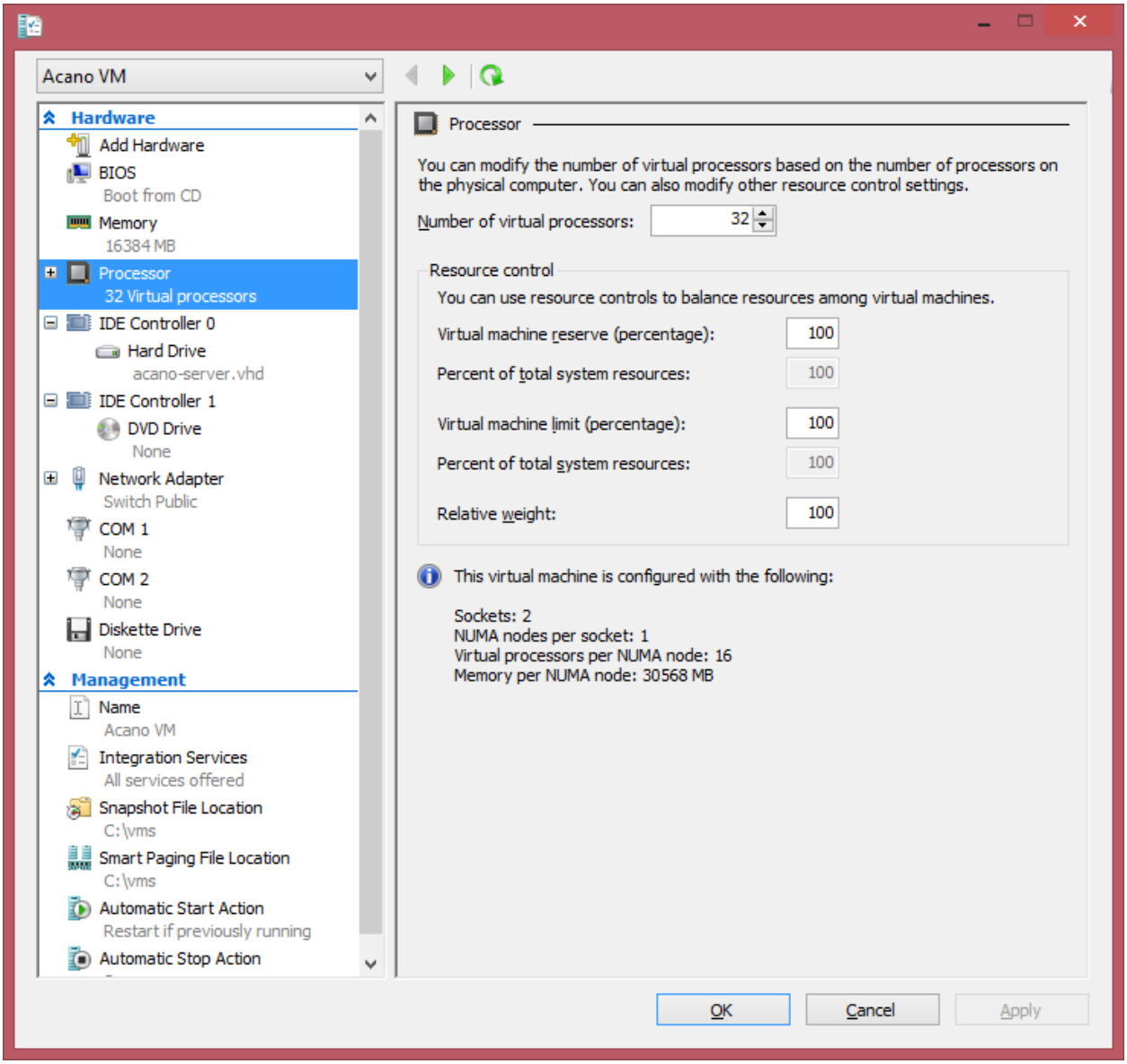
The Meeting Server supports Microsoft Hyper-V 2012 and 2012 R2. VHD disk images are created during software release and should be used for deployment. The host should be dedicated to the Meeting Server VM, leaving one physical core free for system tasks. Standard virtual network adapters are preferred,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



C.3 Amazon Web Services

The Meeting Server VM can run on Amazon EC2/VPC instances. An AMI template is available for deployment. Dedicated instances should be used to prevent contention with other VMs or AWS tenants. A security group must be associated with the Acano VM to allow control and media traffic to flow – required ports can be found in the Cisco Meeting Server Deployment Guides.

We recommend the following instance types:

Table 4: Recommended EC2 Instance Types

	Instance Type	Virtual CPUs
Edge services	c3.2xlarge	8
20 720p30 call legs	c3.4xlarge	16
40 720p30 call legs	c3.8xlarge	32

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