Cisco Meeting Server

Cisco Meeting Server Release 3.11

Installation Guide for Cisco Meeting Server 2000

October 31, 2025

Contents

What's changed 5

1 Introduction 6
1.1 Cisco Meeting Server 2000 overview 7
1.1.1 Interface and Management 9
1.2 How to use this Guide 10
1.2.1 Commands 10

2 Installing the server 12
2.1 Overview 12
2.2 Installing the chassis in a rack system 12
2.3 What you'll need to connect the Cisco Meeting Server 2000 to the network 13
2.4 Connecting cabling 13
2.5 Powering on/off 14
2.6 Next Steps 14

3 Configuring the Fabric Interconnect modules 15
3.1 Changing the default admin password for the Fabric Interconnect modules 16
3.2 Assigning new IP addresses for the Fabric Interconnect modules 17
3.3 Changing the default admin password for the MMP Serial over LAN account 17
3.3.1 Creating a new user account for SoL access 18
3.3.2 Deleting the mmp user account for SoL access 19
3.4 Assigning a new IP address to access the MMP Serial over LAN connection 19
3.5 Changing the UCS Manager system name 20
3.6 Configuring DNS for UCS Manager 20
3.7 Configuring the Timezone 21
3.8 Configuring NTP 22
3.9 Configuring the uplink speed of Port 1 22
3.10 Powering on the blade servers 23
3.11 Checking the health of the Cisco Meeting Server 24
3.12 Applying certificates to the Fabric Interconnect modules 25
3.13 Next steps 25

4 Configuring the Cisco Meeting Server 2000 through the MMP 26
4.1 Logging into the MMP CLI via Serial over LAN 26
4.2 Creating your own Cisco Meeting Server administrator account 26
4.3 Setting up the network interface for the Cisco Meeting Server 27

4.3.1 Configuring an IP address for Port A using DHCP 27
4.3.2 Configuring a static IP address for Port A 27
4.3.3 Setting the DNS configuration 28
4.4 Checking the installed software 28
4.5 Configuring the Web Admin Interface 29
4.5.1 Creating the certificate for the Web Admin Interface 29
4.5.2 Configuring the Web Admin Interface for HTTPS Access 30
4.6 Configuring the Email server for Scheduler 31
4.6.1 Scheduler Email configuration with SMTP 32
4.6.2 Scheduler SMTP with Auth Login configuration 32
4.6.3 Scheduler SMTP and STARTTLS configuration 33
4.6.4 Scheduler SMTP with Auth Login via STARTTLS configuration 34
4.6.5 Scheduler SMTPS configuration 35
4.6.6 Scheduler SMTPS with Auth Login configuration 36
4.6.7 Scheduler detailed logging 37

5 Planning your Cisco Meeting Server deployment 39

Appendix A Technical specifications 40
A.1 Physical specifications: 40
A.2 Environmental specifications 40
A.3 Electrical specifications 40
A.4 Video and audio specifications: 40
A.5 Number of users supported on Cisco Meeting Server 41
A.6 Bandwidth requirements: 41
A.7 Driver specifications 42

Appendix B Cisco licensing 43
B.1 Smart Account and Virtual Account information 43
B.2 How Smart licenses work in Meeting Server – overview 43
B.3 Expired license feature enforcement actions 45
B.4 How to retrieve licensing information (Smart Licensing) 46
B.5 Cisco Meeting Server licensing 46
B.5.1 Personal Multiparty plus licensing 47
B.5.2 Shared Multiparty plus licensing 48
B.6 Smart Licensing registration process 48
B.7 Assigning Personal Multiparty licenses to users 49
B.7.1 To determine whether a specific user has a license: 49

B.8 How Cisco Multiparty licenses are assigned 50
B.9 Determining Cisco Multiparty licensing usage 50
B.10 Calculating SMP Plus license usage 51
B.11 Retrieving license usage snapshots from a Meeting Server 52
B.12 License reporting 52
B.13 Legacy licensing file method 52
B.13.1 Applying a license file 52
B.13.2 Obtaining Cisco user licenses using the traditional licensing method 53

Appendix C Branding 55

Appendix D MMP and API differences between the Cisco Meeting Server 2000 and virtualized deployments 56
D.1 Differences in specific MMP commands 56
D.2 Differences in components enabled on the different platforms 56

Appendix E Creating a certificate signed by a local Certificate Authority 58

Appendix F Upgrading the UCS Manager 62
F.1 Upgrading to Cisco UCS Manager Firmware 4.0(x), 4.1(x), 4.2(x), 4.3(x) 62
F.2 Updating the Host Firmware Package for the CMS2000-FW policy 62
F.2.1 Updating CMS2000-FW policy using the CLI 62
F.2.2 Updating CMS2000-FW policy using the GUI 63

Appendix G Additional Cisco UCS Manager Commands 64
G.1 Powering down the blade servers 64
G.2 Swapping a blade server between slots 65
G.3 Disabling Serial over LAN (optional) 66
G.3.1 Re-enabling Serial over LAN after disabling 66

Cisco Legal Information 67

Cisco Trademark 68

What's changed

Version date	Change
October 31, 2025	Updated for version 3.12.

1 Introduction

The Cisco Meeting Server 2000 is a high performance, scalable platform for voice, video and web content, it interoperates with a wide variety of third-party products from Microsoft, Avaya and other vendors. With the Cisco Meeting Server 2000, people connect regardless of location, device, or technology.

The Cisco Meeting Server 2000 is based on Cisco UCS technology running Cisco Meeting Server software as a physical deployment, not as a virtualized deployment. This gives better performance and utilizes the high performance capabilities of the UCS platform.

The Cisco Meeting Server 2000 is a core network device designed to handle a large number of calls. To support this capability only the Call Bridge, and Web Bridge components are available for configuration. The Cisco Meeting Server 2000 is not suitable as an Edge server in a split Meeting Server deployment, because the TURN server edge component is not available. Deployments that need firewall traversal support for Cisco Meeting Server web app users must deploy the TURN server on a separate Cisco Meeting Server 1000 or specification-based VM server.

In addition, the Recorder and Streamer components are not available on the Cisco Meeting Server 2000, as they are more suited to the lower capacity Cisco Meeting Server 1000 and specification-based VM servers.

The Cisco Meeting Server 2000 can be deployed as a single server on the internal network, as the core server in a single split server deployment, or one of multiple core nodes of a scalable deployment. It can be part of a deployment that includes Cisco Meeting Server 1000s, and specification-based VM servers, providing they are all running the same software version. The functionality, and user experience for participants, is identical across all platforms running the same software version.

Note:

- It is not possible to create a backup from a virtualized deployment and to roll it back on a Cisco Meeting Server 2000, or vice versa.
- Meeting Server does not support secure boot.

Note: From around August 2019, Fabric Interconnect failover should be enabled by default on new Cisco Meeting Server 2000s. However, If you need to manually configure your device to enable failover, see here for more information.

Note: Meeting Server 3.0 introduced a mandatory requirement to have Cisco Meeting Management 3.0 (or later). Meeting Management handles the product registration and interaction with your Smart Account (if set up) for Smart Licensing support.

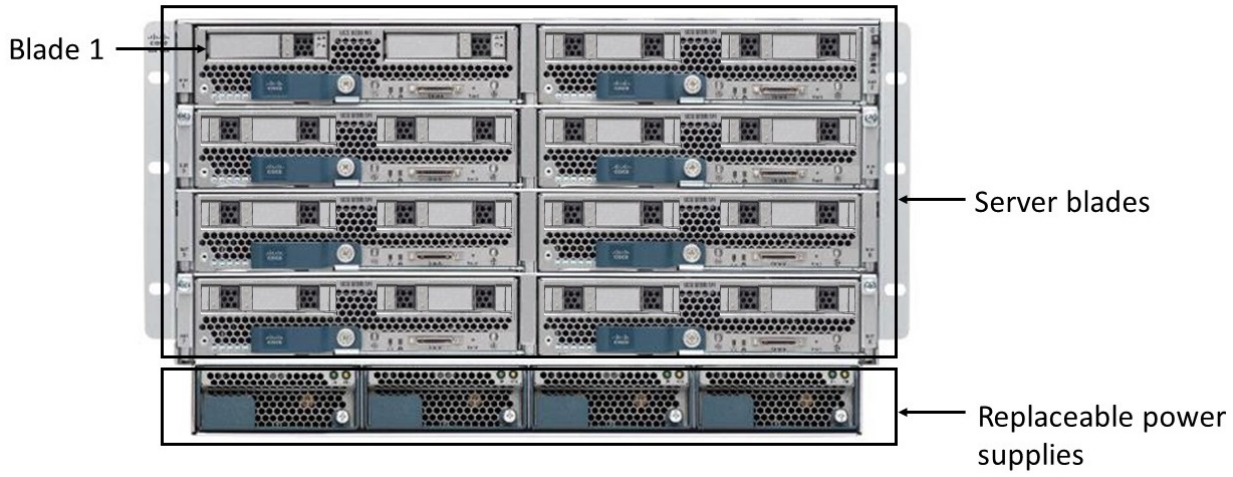
1.1 Cisco Meeting Server 2000 overview

The Cisco Meeting Server 2000 is based on Cisco UCS technology, and consists of:

- a Cisco UCS 5108 Blade Server Chassis. The Chassis is 6 RU high, and weighs approximately 115+ kg (254+ lbs) when the blades are fitted.
- two Cisco UCS 6324 Fabric Interconnect modules, providing redundancy if one fails. Both Fabric Interconnect modules host and run Cisco UCS Manager, which enables configuration of the modules. Each Fabric Interconnect module has:
    - 4 x 10 Gbps SFP+ network ports. Port 1 on both Fabric Interconnects are configured as "Uplink Ports" and mapped to Port A for the Cisco Meeting Server. Both Fabric Interconnects are configured to support failover, if one of the Fabric Interconnects fails the Cisco Meeting Server 2000 fails over to using the other one. If Ethernet Port 1 fails on either Fabric Interconnect then network traffic is moved to the other Ethernet Port 1. Port 4 on both Fabric Interconnects are reserved for internal use. Ports 2 and 3 are not used.
    - a console port to connect to a serial terminal, for configuring the Fabric Interconnect modules through Cisco UCS Manager. You can also use it to configure and control the chassis via Cisco UCS Manager command line interface (CLI) commands.
    - out-of-band 100/1000 Mbps Management port (labeled MGMT) to configure and control the chassis using the UCS Manager command line and graphical interfaces. This port also provides out-of-band access to the MMP serial console, see Section 1.1.1. For further information on using this port, see the Cisco UCS Manager GUI configuration guide.
    - USB port not currently used.
- eight Cisco UCS B200 Blade Servers (M5 or M4). The blade server fitted in slot 1 has 2 hard drives configured as a RAID 1 mirror. Blade Server 1 acts as the control blade or MMP for the Cisco Meeting Server application, it is configured through the MMP command line interface. The other seven blade servers do not have a hard drive and are used for media processing, they require no configuration.
- four hot-swappable power supplies.
- eight hot-swappable fan modules, providing cooling for the whole chassis.

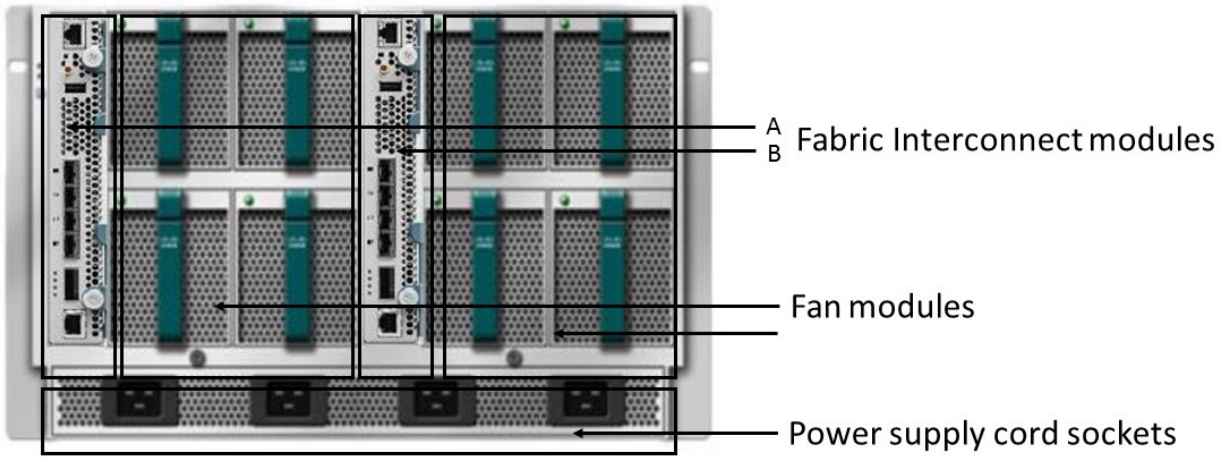
The blade servers and power supplies are installed from the front of the unit, see Figure 1.

Figure 1: Front of unit showing the 8 server modules and four replaceable power supplies



The Fabric Interconnect modules and fan modules are fitted from the rear of the unit above the power supply cord sockets, see Figure 2

Figure 2: Rear of unit showing the Fabric Interconnect modules, eight fan modules and four power supply cord sockets



Notes about redundancy features: The Cisco Meeting Server 2000 supports all of the redundancy features provided by the Cisco UCS-B platform, this includes: fans, power supplies, Fabric Interconnect failover, server blade failure, and network failover.

- Fabric Interconnect failover - Ethernet Port 1 on each Fabric Interconnect is configured to support failover.If one of the Fabric Interconnects fails the Cisco Meeting Server 2000 fails over to using the other one. If Ethernet Port 1 fails on either Fabric Interconnect then network traffic is moved to the other Ethernet Port 1.
- Seven media blades (numbered 2 through 8) used for media processing. If any of these blades are offline or removed, the Cisco Meeting Server 2000 will continue to run, but at a reduced capacity. The blade server in slot 1 is critical as the MMP and Application of the Cisco Meeting Server will not function if that blade is offline or faulty.
- Four hot-swappable power supplies. While the server can safely operate on 3 power supplies, we recommend that you replace faulty powers supplies as soon as possible.
- Eight hot-swappable fan modules, providing cooling for the whole chassis. The fan controller uses temperature sensors to decide whether to spin the remaining fans at a faster rate when there are fan failures or a fan module is removed.

1.1.1 Interface and Management

There are three layers to the Cisco Meeting Server 2000: the Cisco Meeting Server platform and application layers, and the physical hardware platform underneath the Cisco Meeting Server software.

- The Cisco Meeting Server‘s platform layer is configured through the Mainboard Management Processor (MMP) command line interface. The MMP is used for low level bootstrapping, and configuration of Cisco Meeting Server components (Call Bridge, Web Bridge, database). In the Cisco Meeting Server 2000, Blade 1 acts as the MMP for the server. A Serial over LAN (SoL) connection is provided to give access to the MMP; using SoL means that you do not need phyical access to the chassis. Before accessing the MMP you need to configure the network settings for the Fabric Interconnect modules, see Section 3. Once the Fabric Interconnect modules are configured, you can use SSH to log in to the MMP.
- The Cisco Meeting Server application layer runs on top of this management platform with its own configuration interfaces. The application level administration (call and media management) is done through the Cisco Meeting Server Web Admin Interface, and/or REST API; the API is routed through the Web Admin Interface. During the initial configuration of the MMP, the administrator defines a network interface and assigns it an IP address (labeled the ‘A’ network interface). This MMP network interface is used for accessing the application layer and its management interfaces (Web Admin and REST API). In a Cisco Meeting Server

2000, this 'A' network interface is a virtual connection that is connected to the external network through uplinks configured on Port 1 of the Fabric Interconnect modules.

Note: Cisco Meeting Server 2000 platform does not support more than one interface (i.e. configuring 'ipv4 b| c | d' is not supported on Cisco Meeting Server 2000 platform).

- The hardware platform hosts the Cisco Meeting Server software. For the Cisco Meeting Server 2000, this is the UCS chassis managed through UCS Manager. UCS Manager runs on the clustered pair of Fabric Interconnect modules installed in the chassis and is self-contained. When configuring the hardware, or the virtual elements it provides, administration is done through UCS Manager's command line interface or web interface. UCS Manager interfaces are accessed via the serial console or out-of-band 100/1000 Mbps Management ports on the Fabric Interconnect modules.

  CAUTION: Ensure the platform (UCS chassis and modules managed by UCS Manager) is up to date with the latest patches, follow the instructions in the Cisco UCS Manager Firmware Management Guide. Failure to maintain the platform may compromise the security of your Cisco Meeting Server.

Tip: When configuring the Cisco Meeting Server 2000, it is important to understand which layer to use for the configuration task you wish to undertake, and use the appropriate network connection.

1.2 How to use this Guide

This guide is part of the documentation set provided for Cisco Meeting Server 2000 and Cisco Meeting Server software, see Figure 3.

The guide covers:

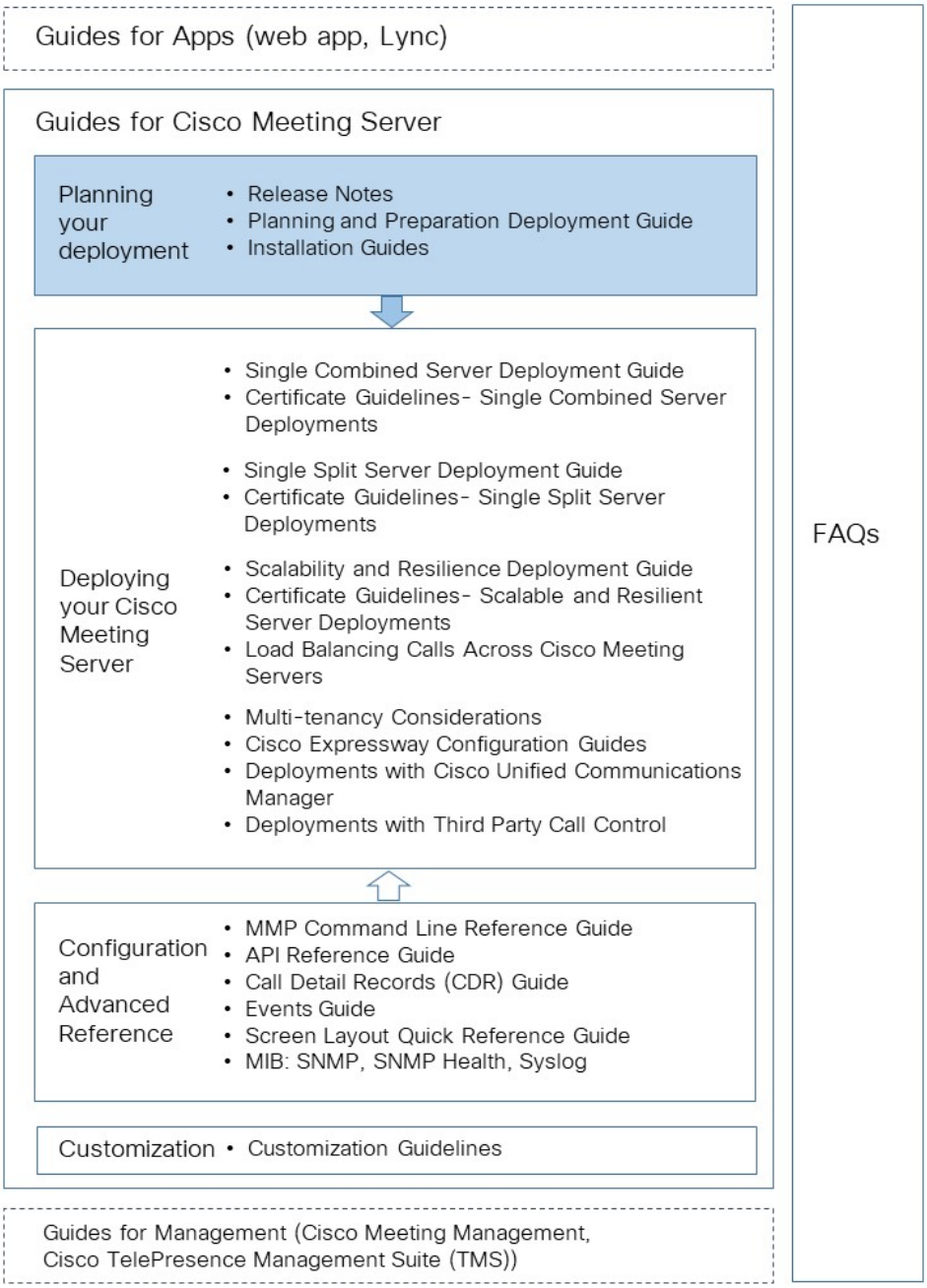
- the physical installation of your Cisco Meeting Server 2000, see Chapter 2.
- configuration of the Fabric Interconnect modules, see Chapter 3.
- setting up access to the MMP and configuring the Call Bridge, see Chapter 4.
- uploading purchased licenses and activation codes to the Call Bridge, see Chapter 1.

You then need to configure the Cisco Meeting Server for your particular deployment, see the deployment guides in Figure 3 for guidance.

1.2.1 Commands

In this document, commands are shown in black and must be entered as given—replacing any parameters in <> brackets with your appropriate values. Examples are shown in `blue` and must be adapted to your deployment.

Figure 3: Cisco Meeting Server installation and deployment documentation



2 Installing the server

2.1 Overview

This chapter covers:

- installing the Cisco Meeting Server 2000 in a 19" racking system.
- connecting cabling and power supply.

2.2 Installing the chassis in a rack system

The Cisco Meeting Server 2000 is shipped with all eight blade servers installed, and weighs approximately 115+ kg (254+ lbs). You are advised to carefully remove the blade servers from their slots, **making a note of which slot each server was shipped in**, and store the blades in a safe location while you install the chassis in an industry standard 19" rack system. The chassis requires 6 RU of space.

Tip: Label each blade with the slot number it was shipped in, so you can be sure of which slot to reinstall it in after the chassis is installed in the rack. Failure to note which blade goes in which slot will result in additional time and configuration necessary to complete the installation.

WARNING: Have at least 2 adults lift and install the chassis into the racking system. The chassis is too heavy for a single adult to lift safely.

Once the chassis is installed, carefully reinsert each blade in the chassis, making sure that the blade server that has two hard disks is inserted in slot 1. You are advised to insert the other blades back into the same slots that they were shipped in, if not you will need to follow the steps in *Swapping a blade server between slots* on page 65.

Follow the instructions in the Cisco UCS 5108 Blade Server Chassis Installation Guide for:

- ambient temperature range required external to the chassis,
- how to move the chassis,
- installing rails on the chassis,
- installing the chassis in the rack,
- and connecting the power supply.

For information on:

- removing a Blade Server from the chassis,
- installing a Blade Server,
- the meaning of the LEDs on the front panel of the blade servers,
- using the Reset button,
- technical specifications of the Blade Server.

follow the instructions in the Cisco UCS B200 M5 Blade Server Installation and Service Note or Cisco UCS B200 M4 Blade Servers Installation and Service Note as appropriate.

2.3 What you'll need to connect the Cisco Meeting Server 2000 to the network

- 2 x 100/1000 switch ports to connect to the Management ports on the Fabric Interconnect modules.
- 2 x 10 Gbps switch ports to connect to Port 1 on each Fabric Interconnect module.
- Five IP addresses:
  - Three static IP addresses, one per Management (MGMT) port on each Fabric Interconnect, and a shared address. These IP addresses should be on your management VLAN. See Section 3.2.
  - One static IP address to access the MMP serial console on Blade Server 1 using Serial over LAN (SoL). This IP addresses should be on your management VLAN, as SoL access is via the MGMT port on the Fabric Interconnect modules. See Section 3.4
  - One static IP address to access the Cisco Meeting Server application through port 1 (Port A) on both Fabric Interconnect modules. This IP address should be on a different VLAN to the management VLAN. See Section 4.3.

2.4 Connecting cabling

On Fabric Interconnect A, connect the following:

- the management port to a 100/1000Mbps switch port on your management network,
- install an appropriate 10Gbps SFP+ transceiver module in port 1 and connect the port to a 10Gbps switch port on your network, **note that this must be a switch port and not configured as a trunk**.
- the serial console port to a console terminal to configure the Fabric Interconnect module.
- Ports 2 and 3 are not currently used.

Repeat the connections for Fabric Interconnect B.

Note: Do not install SFP+ transceivers in port 4 of Fabric Interconnect A or B, nor connect either port 4 to the network. Port 4 is for internal use only.

2.5 Powering on/off

Fit the power supply cords to the power supply sockets at the rear of the unit. Once power is supplied to the chassis, the Fabric Interconnect modules will begin to boot up. The blade servers will remain in standby mode (yellow LED on) until powered on, see Section 3.10. Once powered on, the blade server LED will go green.

Before removing power to the chassis, the blade servers must be put into standby mode, see Appendix G.1.

2.6 Next Steps

After the physical installation of the Cisco Meeting Server 2000 you need to configure the Fabric Interconnect modules so that the server connects to your network. See Chapter 3.

3 Configuring the Fabric Interconnect modules

This chapter details the initial configuration of the Fabric Interconnect modules, so that the server connects to your network.

This chapter covers:

- changing the default admin password assigned to both Fabric Interconnect modules.
- assigning new static IP addresses to manage the Fabric Interconnects over SSH. This includes defining a shared address to manage the Fabric Interconnect modules as a cluster.
- changing the default admin password to access the MMP layer of the Cisco Meeting Server using Serial over LAN (SoL). SoL is used to connect to the serial port on one of the Fabric Interconnect modules in the chassis, this will give access to the MMP of the Cisco Meeting Server.
- assigning a new static IP address to access the MMP via SoL.
- changing the system name.
- configuring DNS for the Meeting Server.
- configuring the timezone of the Meeting Server.
- configuring NTP for the Meeting Server.
- configuring the uplink speed of Port 1.
- powering on the blade servers.
- using UCS Manager to check the operation of the blades.
- installing certificates for the Fabric Interconnect modules.

You will need to supply the following information during the initial setup:

- password for the admin account for the Fabric Interconnect modules. Choose a strong password that meets the guidelines for Cisco UCS Manager passwords.
- new IPv4 (or IPv6) address, subnet mask, and default gateway for each Fabric Interconnect module and a shared IP address. All IP addresses need to be on the management network VLAN.
- admin password to access the MMP serial console using SoL.
- new IPv4 (or IPv6) address to access the MMP command line over the SoL connection.
- system name.
- IPv4 address (or IPv6 address) of the DNS server on your management VLAN.
- the timezone used by the Fabric Interconnect modules.
- MAC address of the MMP network port.

After completing the tasks in this chapter, you will be ready to log into the MMP of the Cisco Meeting Server 2000 and configure the Meeting Server components (Call Bridge, Web Bridge etc.), see Chapter 4.

3.1 Changing the default admin password for the Fabric Interconnect modules

To undertake the initial configuration you need to connect a serial terminal to the console port of each Fabric Interconnect module.

1. Connect a serial terminal to the console port of Fabric Interconnect A.
2. Set the parameters of the serial terminal to 9600 baud, 8 data bits, no parity, 1 stop bit.
3. Login as “admin” using the default password for UCS Manager of “C1sc0123”
4. Using the commands shown in the example below, change the password for the admin account.

Note: You do not need to repeat these steps for Fabric Interconnect B, as the Fabric Interconnect modules are clustered.

For example:

```
Cisco UCS Mini 6324 Series Fabric Interconnect
UCS-A login: admin
Password: C1sc0123
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac  Copyright (c) 2009, Cisco Systems, Inc.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

UCS-A# scope security
UCS-A /security # set password
Enter new password:
Confirm new password:
UCS-A /security* # commit-buffer
UCS-A /security # exit
UCS-A#
```

3.2 Assigning new IP addresses for the Fabric Interconnect modules

Assign a new static IP address to each Fabric Interconnect module, and assign another address that is shared by both modules. The shared IP address is used to access the UCS Manager running on the clustered Fabric Interconnect modules.

All three IP addresses need to be changed simultaneously, and need to be on the same subnet, such as your management VLAN subnet.

Configuring the addresses can be done through one of the Fabric Interconnect modules.

For example, if using IPv4:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # set out-of-band ip 10.1.1.111 netmask
255.255.255.0 gw 10.1.1.110
UCS-A /fabric-interconnect* # scope fabric-interconnect b
UCS-A /fabric-interconnect* # set out-of-band ip 10.1.1.112 netmask
255.255.255.0 gw 10.1.1.110
UCS-A /fabric-interconnect* # scope system
UCS-A /system* # set virtual-ip 10.1.1.113
UCS-A /system* # commit-buffer
UCS-A /system # exit
UCS-A#
```

For example, if using IPv6:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # scope ipv6-config
UCS-A /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001:10::157
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6-gw 2001:10::1
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6-prefix 64
UCS-A /fabric-interconnect/ipv6-config* # scope fabric-interconnect b
UCS-A /fabric-interconnect* # scope ipv6-config
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6 2001:10::158
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6-gw 2001:10::1
UCS-A /fabric-interconnect/ipv6-config* #set out-of-band ipv6-prefix 64
UCS-A /fabric-interconnect/ipv6-config* # scope system
UCS-A /system* # set virtual-ip ipv6 2001:10::156
UCS-A /system* # commit-buffer
UCS-A /system # exit
UCS-A#
```

3.3 Changing the default admin password for the MMP Serial over LAN account

The MMP (Mainboard Management Processor) is accessed using the SoL connection. When you connect to this virtual serial port, you will be prompted for a username and password

specific to the SoL interface before being passed to the Cisco Meeting Server console. A default account and password is set at the factory, for security you need to change this default password. You can also create a new admin account if you prefer not to use the default of mmp, see Section 3.3.1.

1. While logged into the command line interface of one of the Fabric Interconnect modules, change the admin password for the MMP SoL account from the default of c1sco1234.

For example:

```
UCS-A# scope org /CMS
UCS-A /org/ # enter ipmi-access-profile CMS2000-IPMI
UCS-A /org/ipmi-access-profile # enter ipmi-user mmp
UCS-A /org/ipmi-access-profile/ipmi-user # set password
Enter a password:
Confirm the password:
UCS-A /org/ipmi-access-profile/ipmi-user* # commit-buffer
UCS-A /org/ipmi-access-profile/ipmi-user # exit
UCS-A /org/ipmi-access-profile # exit
UCS-A /org # exit
UCS-A#
```

3.3.1 Creating a new user account for SoL access

If you decide to create a new user for SOL access, rather than use the default mmp account, then follow these steps replacing the name **fred** with an appropriate user name:

Note: The `show ipmi-user` line and response are optional.

```
UCS-A# scope org /CMS
UCS-A /org # enter ipmi-access-profile CMS2000-IPMI
UCS-A /org/ipmi-access-profile # create ipmi-user fred
UCS-A /org/ipmi-access-profile/ipmi-user* # set privilege admin
UCS-A /org/ipmi-access-profile/ipmi-user* # set password
Enter a password:
Confirm the password:
UCS-A /org/ipmi-access-profile/ipmi-user* # commit-buffer
UCS-A /org/ipmi-access-profile/ipmi-user # exit
UCS-A /org/ipmi-access-profile # show ipmi-user

IPMI user:
      User Name     End point user privilege   Password     Description
      ----------    ------------------------   ----------   -----------
      fred          Admin                      ****
      mmp           Admin                      ****
```

```
UCS-A /org/ipmi-access-profile # exit
UCS-A /org # exit
UCS-A#
```

3.3.2 Deleting the mmp user account for SoL access

After creating a new user account for SoL access, delete the default mmp account.

```
UCS-A# scope org /CMS
UCS-A /org # enter ipmi-access-profile CMS2000-IPMI
UCS-A /org/ipmi-access-profile # delete ipmi-user mmp
UCS-A /org/ipmi-access-profile* # commit-buffer
UCS-A /org/ipmi-access-profile # exit
UCS-A /org # exit
UCS-A#
```

3.4 Assigning a new IP address to access the MMP Serial over LAN connection

Assigning an IP address to access the Serial Over LAN connection is achieved by creating an IP address block consisting of a single IP address, and then assigning DNS servers for primary use and secondary use.

Follow these steps:

1. Check the existing configuration for a block of IP addresses assigned to the Serial Over LAN connection. If a block of a single IP address has been assigned and its value is suitable for your deployment, then go onto the next section. Otherwise, use the **delete block<first ip address> <last ip address>** command to unallocate the block.
2. Create a block of a single IP address . Use the **create block <first ip address> <last ip address> <gateway IP address> <subnet mask>** command. This should contain a single IP address and should be in the same management subnet as your Fabric Interconnect management IP addresses.

   Note: Cisco does not recommend using a different VLAN or subnet for the Cisco Meeting Server 2000 MMP SoL connection.

3. Specify the primary and secondary DNS IP addresses.

For example, if using IPv4:

```
UCS-A# scope org /CMS
UCS-A /org/ # enter ip-pool CMS2000-MMP-CIMC
UCS-A /org/ip-pool # show block detail
Block of IP Addresses:
From: 10.1.1.51
To: 10.1.1.51
```

```
Default Gateway: 10.1.1.1
Subnet Mask: 255.255.255.0
Primary DNS: 0.0.0.0
Secondary DNS: 0.0.0.0
UCS-A /org/ip-pool # delete block 10.1.1.51 10.1.1.51
UCS-A /org/ip-pool* # commit-buffer
UCS-A /org/ip-pool # create block 10.1.1.2 10.1.1.2 10.1.1.1 255.255.255.0
UCS-A /org/ip-pool/block* # set primary-dns 10.1.1.3 secondary-dns 10.1.1.4
UCS-A /org/ip-pool/block* # commit-buffer
UCS-A /org/ip-pool/block # exit
UCS-A /org/ip-pool # exit
UCS-A /org # exit
UCS-A#
```

3.5 Changing the UCS Manager system name

You can change the system name to reflect the location or use of the server.

For example:

```
UCS-A# scope system
UCS-A /system # set name CMS2000-London
Warning: System name modification changes FC zone name and redeploys them non-
disruptively
UCS-A /system* # commit-buffer
UCS-A /system # exit
CMS2000-London#
```

3.6 Configuring DNS for UCS Manager

You need to configure the DNS server that the Fabric Interconnect modules will use for UCS Manager.

Note: The DNS server used by UCS Manager may be different to the primary and secondary DNS servers set in Section 3.4 and used by the Cisco Integrated Management Controller (CIMC) on blade 1.

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # create dns 10.1.1.3
UCS-A /system/services* # commit-buffer
UCS-A /system/services # exit
UCS-A /system # exit
UCS-A#
```

3.7 Configuring the Timezone

You need to configure the timezone for the Cisco Meeting Server 2000.

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa          4) Arctic Ocean         7) Australia         10) Pacific
Ocean
 2) Americas        5) Asia                 8) Europe
 3) Antarctica      6) Atlantic Ocean       9) Indian Ocean

Please select a country.
1) Anguilla 19) Dominican Republic 37) Peru
2) Antigua & Barbuda 20) Ecuador 38) Puerto Rico
3) Argentina 21) El Salvador 39) St Barthelemy
4) Aruba 22) French Guiana 40) St Kitts & Nevis
5) Bahamas 23) Greenland 41) St Lucia
6) Barbados 24) Grenada 42) St Maarten (Dutch)
7) Belize 25) Guadeloupe 43) St Martin (French)
8) Bolivia 26) Guatemala 44) St Pierre & Miquelon
9) Brazil 27) Guyana 45) St Vincent
10) Canada 28) Haiti 46) Suriname
11) Caribbean NL 29) Honduras 47) Trinidad & Tobago
12) Cayman Islands 30) Jamaica 48) Turks & Caicos Is
13) Chile 31) Martinique 49) United States
14) Colombia 32) Mexico 50) Uruguay
15) Costa Rica 33) Montserrat 51) Venezuela
16) Cuba 34) Nicaragua 52) Virgin Islands (UK)
17) Curacao 35) Panama 53) Virgin Islands (US)
18) Dominica 36) Paraguay
#? 49

Please select one of the following time zone regions.
1) Eastern (most areas) 16) Central - ND (Morton rural)
2) Eastern - MI (most areas) 17) Central - ND (Mercer)
3) Eastern - KY (Louisville area) 18) Mountain (most areas)
4) Eastern - KY (Wayne) 19) Mountain - ID (south); OR (east)
5) Eastern - IN (most areas) 20) MST - Arizona (except Navajo)
6) Eastern - IN (Da, Du, K, Mn) 21) Pacific
7) Eastern - IN (Pulaski) 22) Alaska (most areas)
8) Eastern - IN (Crawford) 23) Alaska - Juneau area
9) Eastern - IN (Pike) 24) Alaska - Sitka area
10) Eastern - IN (Switzerland) 25) Alaska - Annette Island
11) Central (most areas) 26) Alaska - Yakutat
12) Central - IN (Perry) 27) Alaska (west)
13) Central - IN (Starke) 28) Aleutian Islands
14) Central - MI (Wisconsin border) 29) Hawaii
```

```
15) Central - ND (Oliver)
#? 21

The following information has been given:
United States
Pacific

Therefore timezone 'America/Los_Angeles' will be set.
Local time is now: Sat Apr 23 05:08:43 PDT 2011.
Universal Time is now: Sat Apr 23 12:08:43 UTC 2011.
Is the above information OK
1) Yes
2) No
#? 1
UCS-A /system/services* # commit-buffer
UCS-A /system/services # exit
UCS-A /system # exit
UCS-A#
```

3.8 Configuring NTP

After configuring the timezone, you need to configure the NTP server that the Fabric Interconnect modules will use.

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # create ntp-server pool.ntp.org
UCS-A /system/services* # commit-buffer
UCS-A /system/services # exit
UCS-A /system #exit
UCS-A#
```

3.9 Configuring the uplink speed of Port 1

Note: Use a 10Gbps connection for the uplink port on each Fabric Interconnect module.

For both Fabric Interconnect modules, you need to configure the speed of the uplink port.

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope interface 1 1
UCS-A /eth-uplink/fabric/interface # set speed 10gbps
UCS-A /eth-uplink/fabric/interface* #commit-buffer
UCS-A /eth-uplink/fabric/interface # exit
UCS-A /eth-uplink/fabric # exit
UCS-A /eth-uplink # scope fabric b
UCS-A /eth-uplink/fabric # scope interface 1 1
```

```
UCS-A /eth-uplink/fabric/interface # set speed 10gbps
UCS-A /eth-uplink/fabric/interface* # commit-buffer
UCS-A /eth-uplink/fabric/interface # exit
UCS-A /eth-uplink/fabric # exit
UCS-A /eth-uplink # exit
UCS-A#
```

3.10 Powering on the blade servers

Each of the eight blade servers needs to be powered on through one of the Fabric Interconnect modules.

Note: After powering on, the blade servers will remember their last power state. In the event of a power failure the blade servers will power on without you needing to rerun the commands in this section.

For example:

```
UCS-A# scope org /CMS
UCS-A /org # scope service-profile CMS2000-MMP
UCS-A /org/service-profile # power up
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA2
UCS-A /org/service-profile # power up
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA3
UCS-A /org/service-profile # power up
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA4
UCS-A /org/service-profile # power up
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA5
UCS-A /org/service-profile # power up
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA6
UCS-A /org/service-profile # power up
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA7
```

```
UCS-A /org/service-profile # power up
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA8
UCS-A /org/service-profile # power up
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # exit
UCS-A#
```

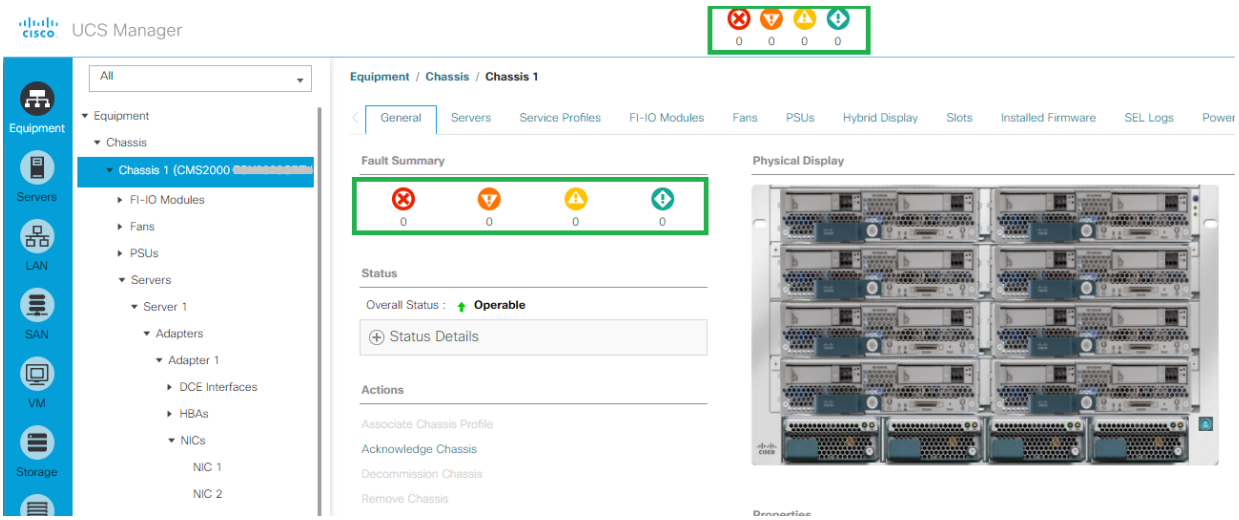
3.11 Checking the health of the Cisco Meeting Server

The Cisco UCS Manager GUI enables you to monitor the health of the Fabric Interconnect modules and the blade servers in the Cisco Meeting Server 2000 chassis. Refer to the Cisco UCS Manager System Monitoring Guide for further details.

Use the Fault Summary page (see Figure 4) to determine that the blade servers are operational. Each type of fault is represented by a different icon. The number below each icon indicates how many faults of that type have occurred in the system. If you click an icon, the Cisco UCS Manager GUI opens the Faults tab in the Work area and displays the details of all faults of that type.

If a critical alarm (red icon) is shown for any of the blade servers refer to the Cisco UCS Troubleshooting Reference Guide prior to contacting Cisco Support for advice. If one or more of blades 2 through 8 are offline or removed, the Cisco Meeting Server 2000 will continue to run, but at a reduced capacity. The blade server in slot 1 is critical as the MMP and Application of the Cisco Meeting Serverwill not function if that blade is offline or faulty.

Figure 4: UCS Manager Fault Summary page



3.12 Applying certificates to the Fabric Interconnect modules

The Cisco Meeting Server 2000 is shipped with a self-signed certificate applied to the Fabric Interconnect modules.To replace these certificates with your own, follow the instructions in the Cisco UCS Manager Administration Guide.

3.13 Next steps

After configuring the Fabric Interconnect modules and powering on the blade servers, you are ready to configure components of the Cisco Meeting Server through the MMP. Chapter 4 covers the initial configuration of the Call Bridge through the MMP.

4 Configuring the Cisco Meeting Server 2000 through the MMP

This chapter details the initial configuration of the Call Bridge through the MMP. You will also need to configure other components through the MMP, however which components will depend upon your deployment. Their configuration are covered in the Cisco Meeting Server deployment guides.

4.1 Logging into the MMP CLI via Serial over LAN

To complete the initial configuration of the Cisco Meeting Server, access the MMP command line interface through the Serial Over LAN connection that was configured in Sections 3.3 and 3.4. Using a SSH client, connect to the IP address configured in Section 3.4 for the Serial Over LAN connection and log in using the credentials that were configured in Section 3.3.

For example:

```
ssh <username>@<ip address>
ssh mmp@10.1.1.2
mmp@10.1.1.2's password:
CISCO Serial Over LAN:
Close Network Connection to Exit
```

Once you successfully login, the Serial Over LAN connection will pass you to the MMP virtual console. (NOTE: To disconnect from the Serial Over LAN connection, you must close your SSH session to the server). Log in with the username “admin” and press the “Enter” key to skip the password field. You will be immediately prompted to set a new password for the “admin” account.

```
Welcome to the CMS 2000
CMS login: admin
Please enter password:
Password reset forced by administrator
Password has expired
Please enter new password:
Please enter new password again:
```

4.2 Creating your own Cisco Meeting Server administrator account

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

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

CAUTION: Passwords expire after 6 months.

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

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

4.3 Setting up the network interface for the Cisco Meeting Server

You do not need to set the network interface speed for Port A, that was done through the Fabric Interconnect modules in Section 3.9.

However, you do need to:

- configure the IP address for Port A, either using dhcp or a static address,
- set the DNS configuration.

Once the network interface and IP address of Port A are configured, the MMP can be accessed using this IP address. The MMP SoL should only need to be used in the event of Port A becoming inaccessible. SFTP can only be accessed via Port A,

4.3.1 Configuring an IP address for Port A using DHCP

To enable dhcp on Port A, type:

```
ipv4 a dhcp
```

Note: There is a similar set of commands to use if you are using IPv6. See the MMP Command Reference for a full description.

Then to find out the dhcp configured settings, type:

```
ipv4 a
```

4.3.2 Configuring a static IP address for Port A

Use the **`<ipv4|ipv6> a add`** command to add a static IP address to Port A with a specified subnet mask and default gateway.

For example, to add ipv4 address 10.1.1.6 with prefix length 16 (netmask 255.255.0.0) with gateway 10.1.1.1 to Port A, type:

```
ipv4 a add 10.1.1.6/16 10.1.1.1
```

To remove the IPv4 address, type.

```
ipv4 a del 10.1.1.6
```

4.3.3 Setting the DNS configuration

1. To output the DNS configuration, type:

   ```
   dns
   ```

2. To set the DNS configuration, 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. if the server is on IP 10.1.1.3

   ```
   dns add forwardzone . 10.1.1.3
   ```

If you need to delete a DNS entry use:

```
dns del forwardzone <domain name> <server IP>
```

for example:

```
dns del forwardzone . 10.1.1.10
```

4.4 Checking the installed software

The Cisco Meeting Server 2000 ships with the Cisco Meeting Server software pre-installed. Before configuring the Web Admin Interface for the Call Bridge, Cisco recommends checking that the latest Cisco Meeting Server software is installed:

- use the MMP command **`version`** to display the version of software installed.
- go to this link to check the latest software available. Note that the Cisco Meeting Server 2000 is a different installation file to VM deployments.

To upgrade the Cisco Meeting Server software, follow the procedure in the release notes published for the software version. Make sure you backup your configuration before upgrading.

Tip: Now that Port A is configured, use SFTP to back up and upgrade Cisco Meeting Server software via Port A.

4.5 Configuring the Web Admin Interface

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

Configuring the Web Admin Interface involves creating a private key/certificate pair, see Section 4.5.1, uploading the private key/certificate pair to the MMP, and configuring the interface to listen on Port A, see Section 4.5.2.

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

4.5.1 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.

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 4.5.2.

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 (see http://en.wikipedia.org/wiki/Self-signed_certificate)

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 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.

4.5.2 Configuring the Web Admin Interface for HTTPS Access

1. SSH to the IP address configured in Section 3.4 and access the MMP command line using the SoL connection. Log in using the admin username and password set up in Section 3.3.
2. Use SFTP to upload the private key/certificate pair and optional certificate bundle.
3. Enter the following commands to assign the uploaded files from step 2 to the Web Admin Interface and configure the interface to use Port A:

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

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

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

4.6 Configuring the Email server for Scheduler

This section describes the steps to configure the Email server for the Scheduler component. Email notifications are sent to the participants when a meeting is scheduled, canceled, or modified. Scheduler supports sending the email notifications via configuration of an SMTP email server.

The configuration of the server address and port, enabling email protocol, and configuring a username for authentication are specified via the following scheduler MMP commands:

```
scheduler email server <hostname|address> <port>
scheduler email server none
scheduler email username <smtp username>
scheduler email protocol <smtp|smtps>
scheduler email auth <enable|disable>
scheduler email starttls <enable|disable>
```

Email will not be configured on a scheduler if no server address is configured on it. At least one email server must be configured for the scheduler to send email invites. Emails can be sent from any scheduler and not necessarily from the scheduler which was used to schedule the meeting. If an email server is down, then a different scheduler sends the email.

Scheduler supports the following types of email configurations:

1. SMTP
2. SMTP with Authenticated Login (Auth Login)
3. SMTP and STARTTLS
4. SMTP with Auth Login and STARTTLS
5. SMTPS (end to end TLS Encryption for the entire SMTP transaction)
6. SMTPS with Auth Login

Note: It is recommended to use Exchange Server 2016 CU22 - 15.1.2375.7 and Exchange Server 2019 CU11 - 15.2.986.5.

Meeting invites can be sent to all the participants from a common email address. The MMP command **`scheduler email common-address <address@mail.domain> "<Display name>"`** configures the common email address and a display name on the Meeting Server. The Scheduler sends the meeting invites from the common email address to the participants.

If the common email address is left blank, the Scheduler sends the email invites from the organizer's email address.

Note: If common email address is not configured, authentication with the SMTP server requires an email address to be configured using the MMP command **`scheduler email username <smtp user-name>`**. This account configured on the MMP must have appropriate permissions to be able to send emails on behalf of web app users.

The organizer's name can also be included to appear as display name besides the email address to identify the sender. When a meeting is scheduled using web app, web app sends the name of the user scheduling the meeting as the organizer display name, to the scheduler. A name of choice can be set as display name by including the optional parameter **`organizerDisplayName`** in the scheduler API.

If the email invites fail to deliver, the Scheduler retries to send them in regular intervals. The Scheduler email queue cleaner cleans up the queued failed emails after specific expiry time.

4.6.1 Scheduler Email configuration with SMTP

To enable the Scheduler to send email notifications via the SMTP, configure the email server to listen on a specified port for the SMTP protocol.

1. Disable the Scheduler component if it is currently running:

   ```
   scheduler disable
   ```

2. Configure the email server and port:

   ```
   scheduler email server <hostname|address> <port>
   ```

   For example,

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. Enable the Scheduler:

   ```
   scheduler enable
   ```

4.6.2 Scheduler SMTP with Auth Login configuration

To enable the Scheduler to send email notifications via the SMTP with Auth Login, configure the email server to listen on a specified port for the SMTP protocol, enable the SMTP server to

support Auth Login, and configure a user account for authentication. This account configured on the MMP must have appropriate permissions to be able to send emails on behalf of web app users.

1. Disable the Scheduler component if it is currently running:

   ```
   scheduler disable
   ```

2. Configure the email server and port:

   ```
   scheduler email server <hostname|address> <port>
   ```

   For example,

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. Enable the Auth Login option:

   ```
   scheduler email auth enable
   ```

4. Set the username to be used for authentication:

   ```
   scheduler email username <username>
   ```

   Enter the password:

   ```
   scheduler email username test@test.com
   Please enter password:
   Please enter password again:
   ```

5. Enable the Scheduler:

   ```
   scheduler enable
   ```

4.6.3 Scheduler SMTP and STARTTLS configuration

To enable the Scheduler to send email notifications via the SMTP and STARTTLS, configure the email server to listen on a specified port for the SMTP protocol and enable STARTTLS.

To establish a TLS connection, the TLS handshake involves a certificate exchange between the email server and the Scheduler. By default, the Scheduler is set to trust all certificates and establishes a successful TLS connection by accepting any certificate coming from the email server. However, there is an additional option on the scheduler to configure a specific certificate. In this mode, the Scheduler accepts and trusts only the configured certificate.

1. Disable the Scheduler component if it is currently running:

   ```
   scheduler disable
   ```

2. Configure the email server and port:

   ```
   scheduler email server <hostname|address> <port>
   ```

   For example,

   ```
   scheduler email server exchange.example.com 25
   ```

```
scheduler email server 10.27.33.55 25
```

3. Enable the STARTTLS option:

   ```
   scheduler email starttls enable
   ```

4. To use a specific certificate, first import and upload the certificate to the Meeting Server VM via SFTP. Then, configure the certificate by running the command:

   ```
   scheduler email trust <cert or bundle name>
   ```

   The configured certificate must be a valid certificate. For example, the common name or SAN names must match the FQDN of the email server, the certificate must not have expired, and so on. Likewise, if the certificate is issued by a Certificate Authority or there are intermediate certificates in the chain, configure the Root CA certificate or alternatively a certificate bundle containing the root certificate, intermediate certificate 1, intermediate certificate 2 and onwards, in that order.

5. Enable the Scheduler component:

   ```
   scheduler enable
   ```

4.6.4 Scheduler SMTP with Auth Login via STARTTLS configuration

To enable the Scheduler to send email notifications via the SMTP using Auth Login and STARTTLS, configure the email server to listen on a specified port for the SMTP protocol. Additionally, enable the SMTP server to support Auth Login, configure a user account that will be used for authentication, and enable STARTTLS.

To establish a TLS connection, the TLS handshake involves a certificate exchange between the email server and the Scheduler. By default, the Scheduler is set to trust all certificates and establishes a successful TLS connection by accepting any certificate coming from the email server. However, there is an additional option on the scheduler to configure a specific certificate. In this mode, the Scheduler accepts and trusts only the configured certificate.

1. Disable the Scheduler component if it is currently running:

   ```
   scheduler disable
   ```

2. Configure the specified email server and port:

   ```
   scheduler email server <hostname|address> <port>
   ```

   For example,

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. Enable the Auth Login option:

   ```
   scheduler email auth enable
   ```

4. Set the username to be used for authentication:

   ```
   scheduler email username <username>
   ```

Enter the password:

```
scheduler email username test@test.com
Please enter password:
Please enter password again:
```

5. Enable the STARTTLS option:

   ```
   scheduler email starttls enable
   ```

6. To use a specific certificate, first import and upload the certificate to the Meeting Server VM via SFTP. Then, configure the certificate by running the command:

   ```
   scheduler email trust <cert or bundle name>
   ```

   The configured certificate must be a valid certificate. For example, the common name or SAN names must match the FQDN of the email server, the certificate must not have expired, and so on. Likewise, if the certificate is issued by a Certificate Authority or there are intermediate certificates in the chain, configure the Root CA certificate or alternatively a certificate bundle containing the root certificate, intermediate certificate 1, intermediate certificate 2 and onwards, in that order.

7. Enable the Scheduler component:

   ```
   scheduler enable
   ```

4.6.5 Scheduler SMTPS configuration

To enable the Scheduler to send email notifications via the SMTPS, configure the email server to support end to end SMTP encryption on a specific port.

To establish a TLS connection, the TLS handshake involves a certificate exchange between the email server and the Scheduler. By default, the Scheduler is set to trust all certificates and establishes a successful TLS connection by accepting any certificate coming from the email server. However, there is an additional option on the scheduler to configure a specific certificate. In this mode, the Scheduler accepts and trusts only the configured certificate.

1. Disable the Scheduler component if it is currently running:

   ```
   scheduler disable
   ```

2. Configure the specified email server and port:

   ```
   scheduler email server <hostname|address> <port>
   ```

   For example,

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. Set the email protocol to SMTPS:

   ```
   scheduler email protcol smtps
   ```

4. To use a specific certificate, first import and upload the certificate to the Meeting Server VM via SFTP. Then, configure the certificate by running the command:

   scheduler email trust <cert or bundle name>

   The configured certificate must be a valid certificate. For example, the common name or SAN names must match the FQDN of the email server, the certificate must not have expired, and so on. Likewise, if the certificate is issued by a Certificate Authority or there are intermediate certificates in the chain, configure the Root CA certificate or alternatively a certificate bundle containing the root certificate, intermediate certificate 1, intermediate certificate 2 and onwards, in that order.

5. Enable the Scheduler component to complete the email configuration using SMTPS:

   scheduler enable

4.6.6 Scheduler SMTPS with Auth Login configuration

To enable the Scheduler to send email notifications via the SMTPS using Auth Login, configure the email server to support end to end SMTP encryption on a specific port. Additionally, enable the SMTPS server to support Auth Login and configure a user account that will be used for authentication.

To establish a TLS connection, the TLS handshake involves a certificate exchange between the email server and the Scheduler. By default, the Scheduler is set to trust all certificates and establishes a successful TLS connection by accepting any certificate coming from the email server. However, there is an additional option on the scheduler to configure a specific certificate. In this mode, the Scheduler accepts and trusts only the configured certificate.

1. Disable the Scheduler component if it is currently running:

   scheduler disable

2. Configure the specified email server and port:

   scheduler email server <hostname|address> <port>

   For example,

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. Enable the Auth Login option:

   scheduler email auth enable

4. Set the username of the user which will be used for authentication:

   scheduler email username <username>

   Enter the password:

   ```
   scheduler email username test@test.com
   Please enter password:
   ```

```
Please enter password again:
```

5. Set the email protocol to SMTPS:

   scheduler email protcol smtps

6. To use a specific certificate, first import and upload the certificate to the Meeting Server VM via SFTP. Then, configure the certificate by running the command:

   scheduler email trust <cert or bundle name>

   The configured certificate must be a valid certificate. For example, the common name or SAN names must match the FQDN of the email server, the certificate must not have expired, and so on. Likewise, if the certificate is issued by a Certificate Authority or there are intermediate certificates in the chain, configure the Root CA certificate or alternatively a certificate bundle containing the root certificate, intermediate certificate 1, intermediate certificate 2 and onwards, in that order.

7. Enable the Scheduler component to complete the email configuration using SMTPS with Auth Login:

   scheduler enable

4.6.7 Scheduler detailed logging

The Scheduler supports the option to enable detailed logging for Web Bridge connections, email notifications, and API using the scheduler timedLogging MMP command.

When timedLogging is not enabled, Meeting Server displays the following output:

```
cms-vm> scheduler timedLogging
{
"webBridge": "0",
"api": "0",
"email": "0"
}
```

To enable any of the timedLogging options, use the command:

scheduler timedLogging (webBridge|api|email) <time>

For example,

```
cms-vm> scheduler timedLogging webBridge 600
SUCCESS
```

The time variable is expressed in seconds, and enables timedLogging for the set duration.

```
cms-vm> scheduler timedLogging
{
"webBridge": "594",
```

```
"api": "0",
"email": "0"
}
```

After the set duration expires or the specific investigation or troubleshooting step is completed download the log files using SFTP.

5 Planning your Cisco Meeting Server deployment

Note: From version 3.0 you can use Trial Mode for a 90 day full featured period without licenses.

After the initial configuration, the Cisco Meeting Server 2000 is available for deployment as:

- a single server, typically suited to organizations that have one location requiring a large number of concurrent internal calls. For call capacity information, see A.4.
- a split deployment where the Cisco Meeting Server 2000 is the core node deployed on the internal network, and the edge component (TURN server) is enabled on an Edge server (Cisco Meeting Server 1000, Cisco Meeting Server specification-based VM server, Cisco Expressway) deployed in the DMZ.

  For more information on deploying the Cisco Meeting Server web edge solution, see the Deployment Guides (version 3.1 or later).
- one of multiple core nodes of a scalable and resilient deployment to support large conferences, growth in usage and minimize downtime.

Use the Planning and Preparation Deployment Guide to guide you on deciding the appropriate deployment, and then follow the deployment and certificate guides.

Appendix A Technical specifications

A.1 Physical specifications:

Chassis: Cisco UCS 5108 Blade Server Chassis

Weight: 115+ kg (254+ lbs)

Size: 6RU high

Rack requirements: 19" standard rack

A.2 Environmental specifications

Operating temperature: 10 to 35° C (50-95° F)

Operating humidity: 5 to 93% non-condensing

A.3 Electrical specifications

Maximum power:	3.36kW at 230V, 14.74A
	3.38kW at 115V, 29.48A
Power supplies	4 x 2500W Platinum AC Hot Plug Power Supply

A.4 Video and audio specifications:

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

Table 1: Call capacities across Meeting Server platforms

Type of calls	Cisco Meeting Server 1000 M6	Cisco Meeting Server Small M7	Cisco Meeting Server 2000	Cisco Meeting Server 2000 M6
Full HD calls 1080p60 video 720p30 content	40	60	175	324
Full HD calls 1080p30 video 1080p30/4K7 content	40	60	175	324

Type of calls	Cisco Meeting Server 1000 M6	Cisco Meeting Server Small M7	Cisco Meeting Server 2000	Cisco Meeting Server 2000 M6
Full HD calls 1080p30 video 720p30 content	80	120	350	648
HD calls 720p30 video 720p5 content	160	240	700	1296
SD calls 480p30 video 720p5 content	320	480	1000	1875
Audio calls (G.711)	3000	3000	3000	3200

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

A.5 Number of users supported on Cisco Meeting Server

Cisco Meeting Server cluster can support up to 300,000 users depending on the servers where the databases are located. All databases in the cluster must be on the same specification server.

Table 2: Number of users supported on Cisco Meeting Server

Cisco Meeting Server	Maximum number of users
Meeting Server 2000 M5v2	300,000
Meeting Server 2000 M5v1	200,000
Meeting Server 2000 M4, Meeting Server 1000 M4, M5v1, M5v2, and Specification based servers	75,000

Note: LDAP sync for a large number of users can cause an increase in call join times. We advise adding new users/coSpaces onto the Meeting Server during a maintenance window or during off peak hours.

A.6 Bandwidth requirements:

Cisco Meeting Server 2000 supports up to 700 simultaneous 720p HD calls. This requires between 3 and 4 Gbps network bandwidth.

A.7 Driver specifications

The table lists the driver versions supported for Cisco Meeting Server.

Driver	Version supported
Linux kernel	4.4.225
Enic driver	2.3.0.20
MegaRAID SAS	06.808.16.00-rc1

Appendix B Cisco licensing

This section covers license information for Smart licensing.

B.1 Smart Account and Virtual Account information

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

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

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

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

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

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

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

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

   ---

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

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

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

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

---

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

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

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

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

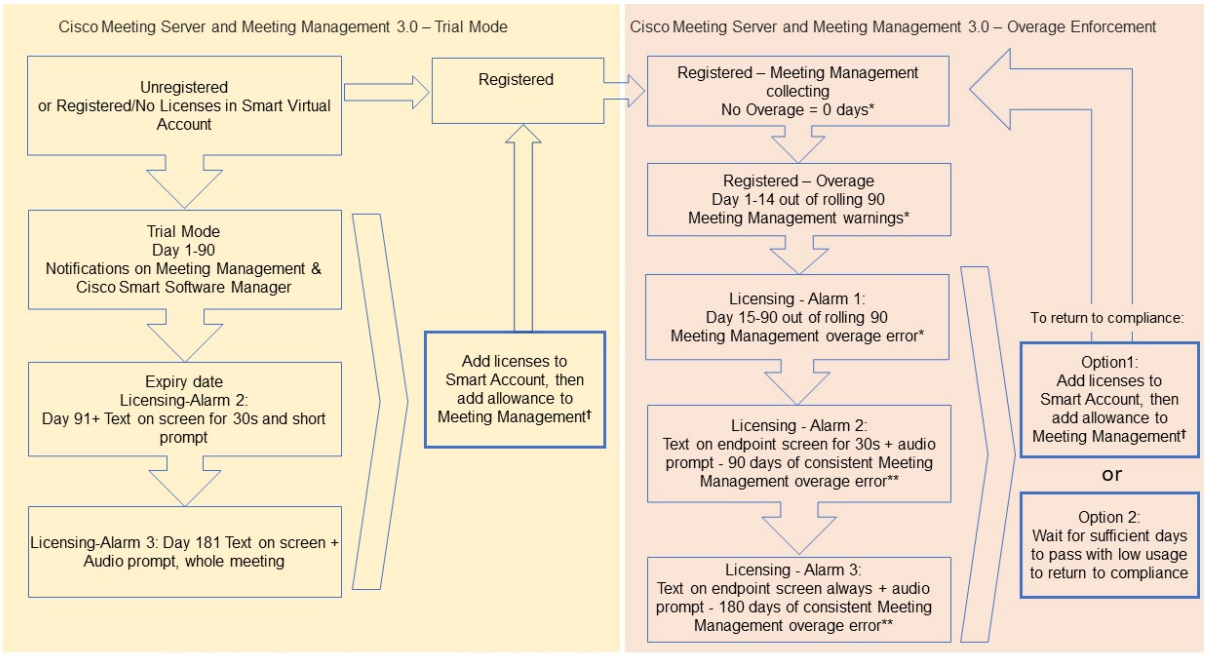
    b. If Meeting Management identifies that less than 15 out of the last 90 days are non-compliant, it will allow this and reset the Meeting Server expiry date to 90 days in the future from that point. The admin will get a visual warning to notify " Insufficient licenses" .

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

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

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

Figure 5: Cisco Meeting Server and Cisco Meeting Management Smart Licensing enforcement flow



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

B.3 Expired license feature enforcement actions

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

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

When a license feature has expired the actions described in Table 3 will occur.

Table 3: Expired license enforcement actions

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

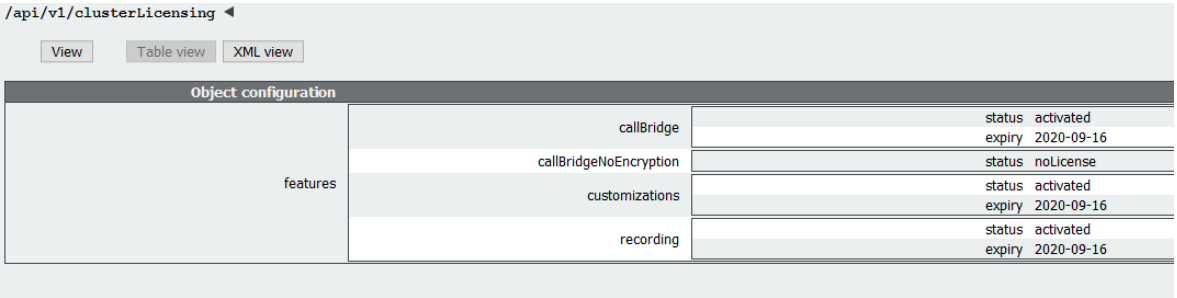
To turn off Alarms 2 and 3, simply add more licenses to your Smart Account.

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

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

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

Figure 6: clusterLicensing API – license status



B.5 Cisco Meeting Server licensing

The following features require a license:

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

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

- PMP Plus,
- SMP Plus,

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

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

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

B.5.1 Personal Multiparty plus licensing

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

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

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

---

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

B.5.2 Shared Multiparty plus licensing

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

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

B.6 Smart Licensing registration process

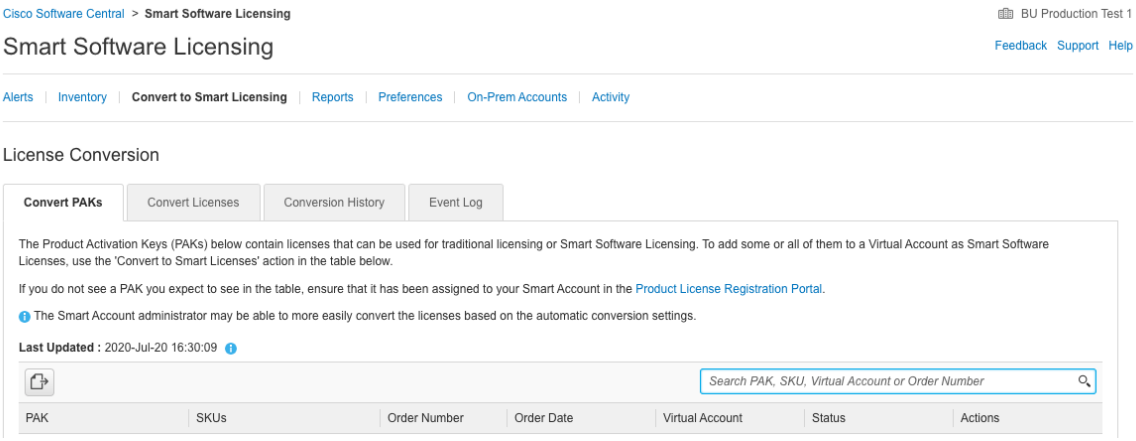
To enable Smart Licensing:

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

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

    If any licenses are not shown in your Virtual Account, use the **Convert Licenses** tab, search by PAK to find them, then choose **Convert Licenses** as shown in Figure 7. (If you can't find a license(s), open a case by sending an email to licensing@cisco.com.)

    Figure 7: License conversion for Smart Licensing



B.7 Assigning Personal Multiparty licenses to users

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

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

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

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

B.8 How Cisco Multiparty licenses are assigned

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

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

B.9 Determining Cisco Multiparty licensing usage

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

Table 4 below lists the API objects and parameters that can be used to determine the consumption of Multiparty licenses.

Table 4: Objects and parameters related to Multiparty license usage

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

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

B.10 Calculating SMP Plus license usage

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

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

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

Note: A point to point call is defined as:

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

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

B.11 Retrieving license usage snapshots from a Meeting Server

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

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

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

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

B.12 License reporting

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

B.13 Legacy licensing file method

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

B.13.1 Applying a license file

The Cisco Meeting Server 2000 requires a license file, when applied this license activates the Call Bridge so that it can create calls; the license file is tied to the MAC address assigned to Port

A.

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

B.13.1.1 Transferring the license file to the Cisco Meeting Server 2000

This section assumes that you have already configured the port that the Call Bridge will listen on, and uploaded the Call Bridge certificates.

Transfer the license file to your Meeting Server using SFTP. If you already know the IP address of Port A, then omit step 1.

1. SSH to the IP address of Port A configured in Section 3.4, log in using the admin username and password set up in Section 3.3. Use the MMP command **`ipv4 a`**or **`ipv6 a`** to find the IP address of Port A.
2. Upload the cms.lic file to the IP address of Port A using SFTP.
3. SSH to the IP address of Port A and log in using the credentials of an MMP admin user.
4. Restart the Call Bridge using the MMP command **`callbridge restart`**. This will apply the license file.
5. After restarting the Call Bridge, check the license status by entering the MMP command **`license`**

   The activated features and expirations will be displayed.

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

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

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

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

1. Obtain the MAC address of your Meeting Server by logging in to the MMP of your server, and enter the MMP command: **`iface a`**
2. Open the Cisco License Registration Portal and register the PAK code(s) and the MAC address of your Meeting Server.
3. If your PAK does not have an R-CMS-K9 activation license, you will need this PAK in addition to your feature licenses.

4. The license portal will email a zipped copy of the license file. Extract the zip file and rename the resulting xxxxx.lic file to **`cms.lic`**.
5. Using your SFTP client, log into Meeting Server and copy the **`cms.lic`** file to the Meeting Server file system.
6. Restart the Call Bridge using the MMP command **`callbridge restart`**
7. After restarting the Call Bridge, check the license status by entering the MMP command **`license`**

   The activated features and expirations will be displayed.

Appendix C Branding

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

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

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

See the Customization Guidelines for more information on branding.

Appendix D MMP and API differences between the Cisco Meeting Server 2000 and virtualized deployments

D.1 Differences in specific MMP commands

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

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

D.2 Differences in components enabled on the different platforms

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

Component	on Cisco Meeting Server 2000	on Cisco Meeting Server1000/ Small and virtualized Cisco Meeting Server
Call Bridge	Available	Available
Web Bridge 3	Available	Available
Database	Available	Available
Scheduler	Available	Available
TURN server	Not available	Available
Recorder	Not available	Available
Uploader	Not available	Available
Streamer	Not available	Available
SNMP MIB	Not currently available	Available

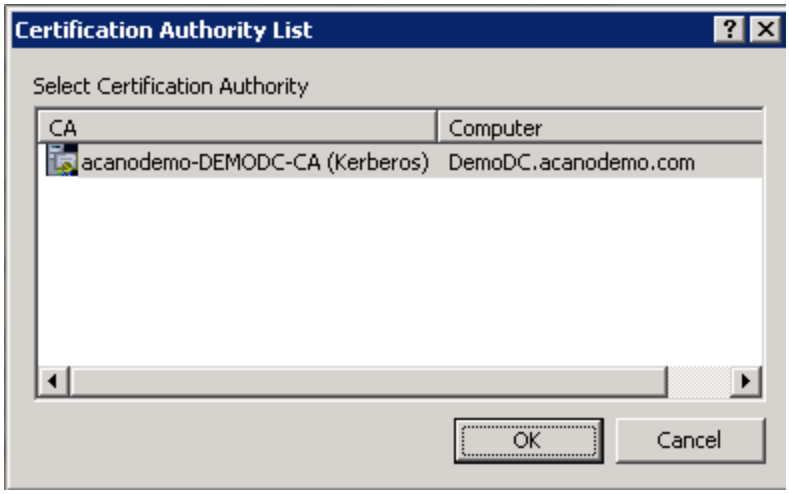
Appendix E Creating a certificate signed by a local Certificate Authority

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.

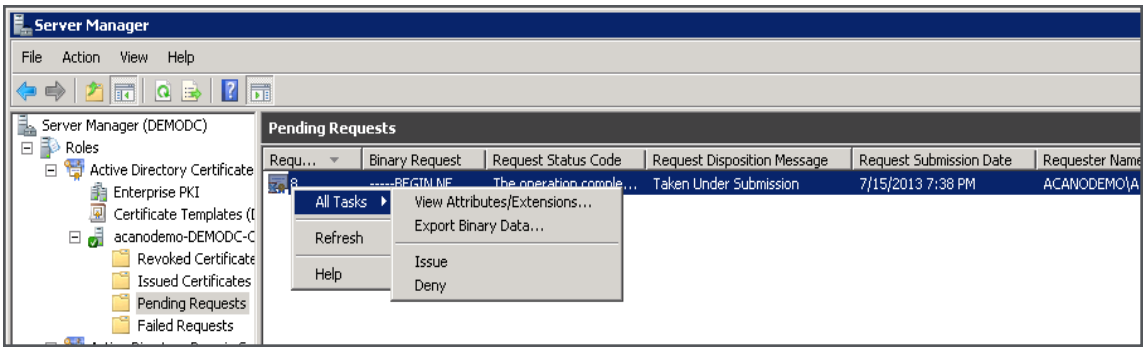


4. Do one of the following:
   - If your Windows account has permissions to issue certificates, you are prompted to save the resulting certificate, for example as webadmin.crt. Go on to step c below.
   - If you do not see a prompt to issue the resulting certificate, but instead see a message on the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

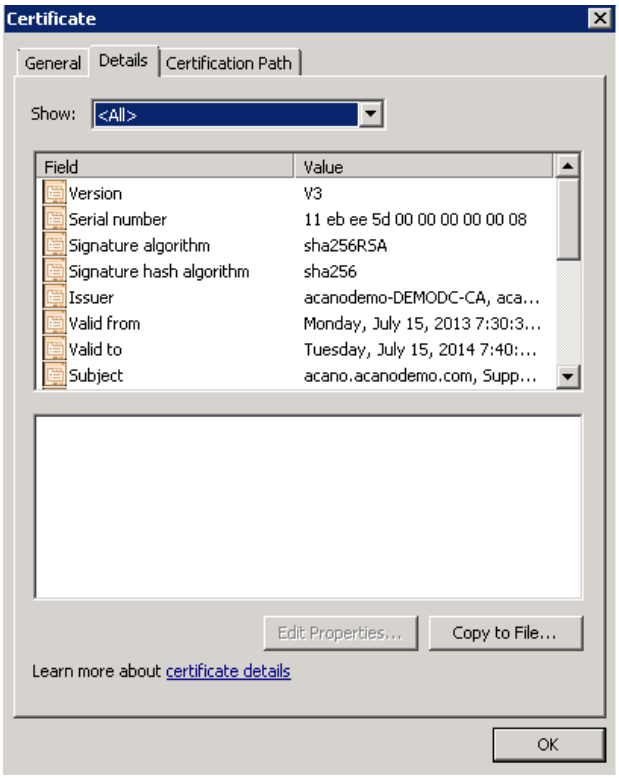
```
C:\Users\Administrator>certreq -submit -attrib "CertificateTemplate:WebServer" C
:\Users\Administrator\Desktop\demokitcsr.pem
Active Directory Enrollment Policy
  {0BD5D0B7-591F-4C77-AFEC-3C0E470F77D5}
  ldap:
RequestId: 8
RequestId: "8"
Certificate request is pending: Taken Under Submission (0)

C:\Users\Administrator>_
```

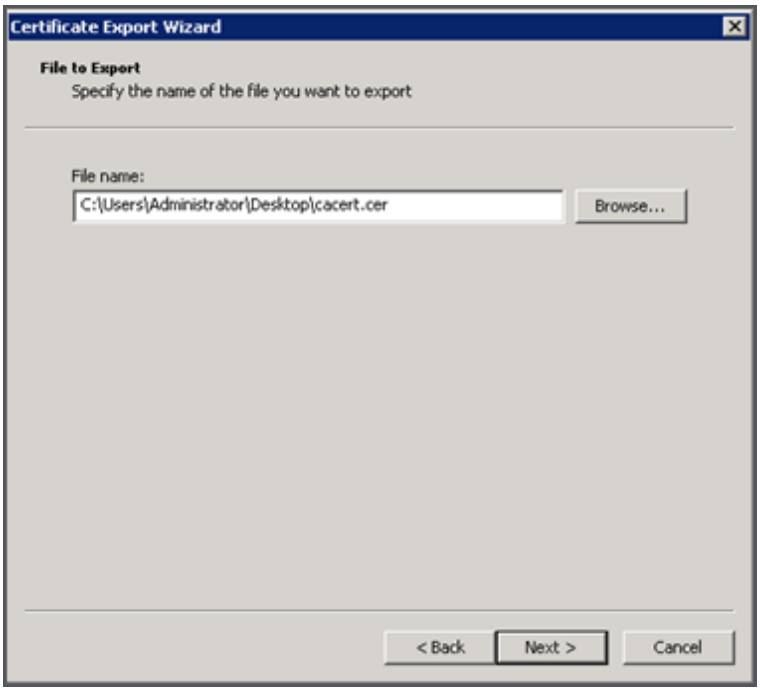
5. Using the Server Manager page on the CA, locate the Pending Requests folder under the CA Role.
6. Right-click on the pending request that matches the Request ID given in CMD window and select All Tasks > Issue.



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 4.5.2.

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.

Appendix F Upgrading the UCS Manager

Cisco Meeting Server 2000 runs on a Cisco UCS 5108 blade server chassis populated with two UCS 6324 Fabric Interconnects and eight UCS B-Series blade server compute resources.

Follow the instructions in the Cisco UCS Manager Firmware Management Guide Release 4.3 (x), 4.2(x), 4.1, or 4.0 to upgrade the firmware. Click here to view the available versions of UCS Manager that have been tested for interoperability.

This Appendix contains simplified steps required to update the CMS2000-FW policy used to set the firmware version on the blades.

F.1 Upgrading to Cisco UCS Manager Firmware 4.0(x), 4.1(x), 4.2(x), 4.3 (x)

Upgrading directly to Release 4.0(x), 4.1(x), 4.2(x), 4.3(x) is not supported from releases prior to 3.1(3) or 3.2(3). To upgrade to Release 4.0(x), 4.1(x), 4.2(x), or 4.3 (x) out the following steps in this order:

1. Upgrade the Infrastructure A bundle to Release 3.1(3) or 3.2(3).
2. Upgrade the B bundle for all servers to Release 3.1(3) or 3.2(3) by modifying the CMS2000-FW Host Firmware Package.
3. Upgrade the Infrastructure A bundle to Release 4.0(x), 4.1(x), 4.2(x), or 4.3 (x).
4. Upgrade the B bundle for all servers to Release 4.0(x), 4.1(x)4.2(x), or 4.3 (x) by modifying the CMS2000-FW Host Firmware Package.

F.2 Updating the Host Firmware Package for the CMS2000-FW policy

Prerequisites:

Ensure that the appropriate firmware is downloaded to the fabric interconnect.

F.2.1 Updating CMS2000-FW policy using the CLI

```
UCS-A# scope org CMS
UCS-A /org # scope fw-host-pack CMS2000-FW
UCS-A /org/fw-host-pack # show detail

Server Host Pack:
Name: CMS/CMS2000-FW
Mode: Staged
Description: CMS2000 Blade Server Firmware Package
Policy Owner: Local
```

```
B-Series Package Version: 3.2(3k)B
C-Series Package Version:
Service Pack Version:

UCS-A /org/fw-host-pack # set blade-vers 4.1(1d)B
UCS-A /org/fw-host-pack* # commit-buffer
UCS-A /org/fw-host-pack # top
UCS-A#
```

F.2.2 Updating CMS2000-FW policy using the GUI

1. In the Navigation pane, click **Servers**.
2. Expand **Servers > Policies**.
3. Expand the node for the **CMS** organization.
4. Expand **Host Firmware Packages** and choose the **CMS2000-FW** policy.
5. In the **Work** pane, click the **General** tab.
6. To modify the components in the host firmware package, click **Modify Package Versions**.

   The **Modify Package Versions** window displays.
7. To modify the blade package, from the **Blade Package** drop-down list, select the blade package version.
8. Click **OK**.

   Cisco UCS Manager verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS Manager updates the firmware according to the settings in the maintenance policies included in the service profiles.

Appendix G Additional Cisco UCS Manager Commands

This appendix covers a few Cisco UCS Manager commands that may be useful, but are not required in the initial set up of the Cisco Meeting Server 2000.

G.1 Powering down the blade servers

All eight blade servers need to be powered off before power is removed from the chassis.

For example:

```
UCS-A# scope org /CMS
UCS-A /org # scope service-profile CMS2000-MMP
UCS-A /org/service-profile # power down
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA2
UCS-A /org/service-profile # power down
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA3
UCS-A /org/service-profile # power down
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA4
UCS-A /org/service-profile # power down
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA5
UCS-A /org/service-profile # power down
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA6
UCS-A /org/service-profile# power down
UCS-A /org/service-profile*# commit-buffer
UCS-A /org/service-profile# exit
UCS-A /org # scope service-profile CMS2000-MEDIA7
UCS-A /org/service-profile # power down
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # scope service-profile CMS2000-MEDIA8
UCS-A /org/service-profile # power down
```

```
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # exit
UCS-A /org # exit
UCS-A#
```

G.2 Swapping a blade server between slots

If during racking, a blade is swapped between slots, it must be acknowledged before it can be used in the current slot. Check the slots using the **show server status** command and then acknowledge the slots that have a mismatch. The acknowledgment rebuilds the connections between the blade server and the Fabric Interconnect modules, it may take up to 20 minutes to complete.

Note: The blade server fitted with two hard drives must be installed in slot 1.

```
UCS-A# show server status
Server  Slot Status   Availability   Overall Status    Discovery
------- -----------   ------------   --------------    ---------
1/1     Equipped      Unavailable    Ok                Complete
1/2     Equipped      Unavailable    Ok                Complete
1/3     Equipped      Unavailable    Ok                Complete
1/4     Mismatch      Unavailable     Compute Mismatch Retry
1/5     Mismatch      Unavailable     Compute Mismatch Retry
1/6     Equipped      Unavailable    Ok                Complete
1/7     Equipped      Unavailable    Ok                Complete
1/8     Equipped      Unavailable    Ok                Complete
```

```
UCS-A# acknowledge slot 1/4
UCS-A* # acknowledge slot 1/5
UCS-A* # commit-buffer
UCS-A#
```

Wait until all blades have completed discovery before continuing.

```
UCS-A# show server status
Server  Slot Status   Availability   Overall Status    Discovery
------- -----------   ------------   --------------    ---------
1/1     Equipped      Unavailable    Ok                Complete
1/2     Equipped      Unavailable    Ok                Complete
1/3     Equipped      Unavailable    Ok                Complete
1/4     Equipped      Unavailable     Ok               Complete
1/5     Equipped      Unavailable    Ok                Complete
1/6     Equipped      Unavailable    Ok                Complete
1/7     Equipped      Unavailable    Ok                Complete
1/8     Equipped      Unavailable    Ok                Complete
```

G.3 Disabling Serial over LAN (optional)

If you do not want to use the Serial over LAN connection to access the MMP, then you can disable the SoL policy.

CAUTION: You will require SoL to complete the initial configuration of the MMP. Do not disable SoL until you have configured the Cisco Meeting Server with a network IP address.

```
UCS-A# scope org /CMS
UCS-A /org/ # scope sol-policy CMS2000-MMP-SOL
UCS-A /org/sol-policy # show detail

SOL Policy:

  Name: CMS/CMS-2000-SOL
   SOL State: Enable
   Speed:115200
   Decription:
   Policy Owner: Local

UCS-A /org/sol-policy # disable
UCS-A /org/sol-policy* # commit-buffer
UCS-A /org/sol-policy # exit
UCS-A /org # exit
UCS-A#
```

G.3.1 Re-enabling Serial over LAN after disabling

You only need to re-enable SoL if you have previously disabled it and now wish to use SoL.

```
UCS-A# scope org /CMS
UCS-A /org # scope sol-policy CMS2000-MMP-SOL
UCS-A /org/sol-policy # show detail

SOL Policy:

  Name: CMS/CMS-2000-SOL
   SOL State: Disable
   Speed:115200
   Decription:
   Policy Owner: Local

UCS-A /org/sol-policy # enable
UCS-A /org/sol-policy* # commit-buffer
UCS-A /org/sol-policy # exit
UCS-A /org # exit
UCS-A#
```

Cisco Legal Information

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

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

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

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

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

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

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

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

Cisco Trademark