# Cisco Meeting Server

## Cisco Meeting Server Release 3.3

### MMP Command Line Reference

March 27, 2024

# Contents

# Change History

| Date | Change Summary |
|---|---|
| December 21, 2021 | Updated link for command description under TLS Certificate Verification section. |
| August 24, 2021 | New version for Meeting Server 3.3 software. See Summary of MMP additions and changes |
| May 19, 2021 | Updated the document with recommendations for Medium OVA Expressway. |
| April 16, 2021 | Moved the MTU for an Interface command under section 2.1 Network Interface (iface) Commands. Updated the note regarding MTU information. |
| April 09, 2021 | New version for Meeting Server 3.2 software. |
| March 16, 2021 | Updated the document for short term credentials on the Meeting Server being a fully supported feature. |
| December 04, 2020 | Added note to pcap section |
| November 30, 2020 | New version for version 3.1 software. |
| October 15, 2020 | Clarification note added re. MTU information.<br>Other minor corrections. |
| September 11, 2020 | Minor correction. |
| August 21, 2020 | Minor correction. |
| July 29, 2020 | New version for version 3.0 software. |

# 1 Introduction

The Cisco Meeting Server software can be hosted on specific servers based on Cisco Unified Computing Server (UCS) technology or on a specification-based VM server. Cisco Meeting Server is referred to as the Meeting Server throughout this document.

**Note:** Cisco Meeting Server software version 3.0 onwards does not support X-Series servers.

There are two layers to the Cisco Meeting Server: a platform and an application. The platform is configured through the Mainboard Management Processor (MMP). The application runs on this managed platform with configuration interfaces of its own.

The MMP is used for low level bootstrapping and configuration. It presents a command line interface. On Cisco Meeting Server 2000, the MMP command line interface is accessed through the Serial Over LAN connection. In virtualized deployments (the Cisco Meeting Server 1000, and specification based VM servers) the MMP is accessed on virtual interface A.

Application level administration (call and media management) is undertaken via the API, or for straightforward deployments, via the Web Admin Interface which can be configured to run on any one of the available Ethernet interfaces.

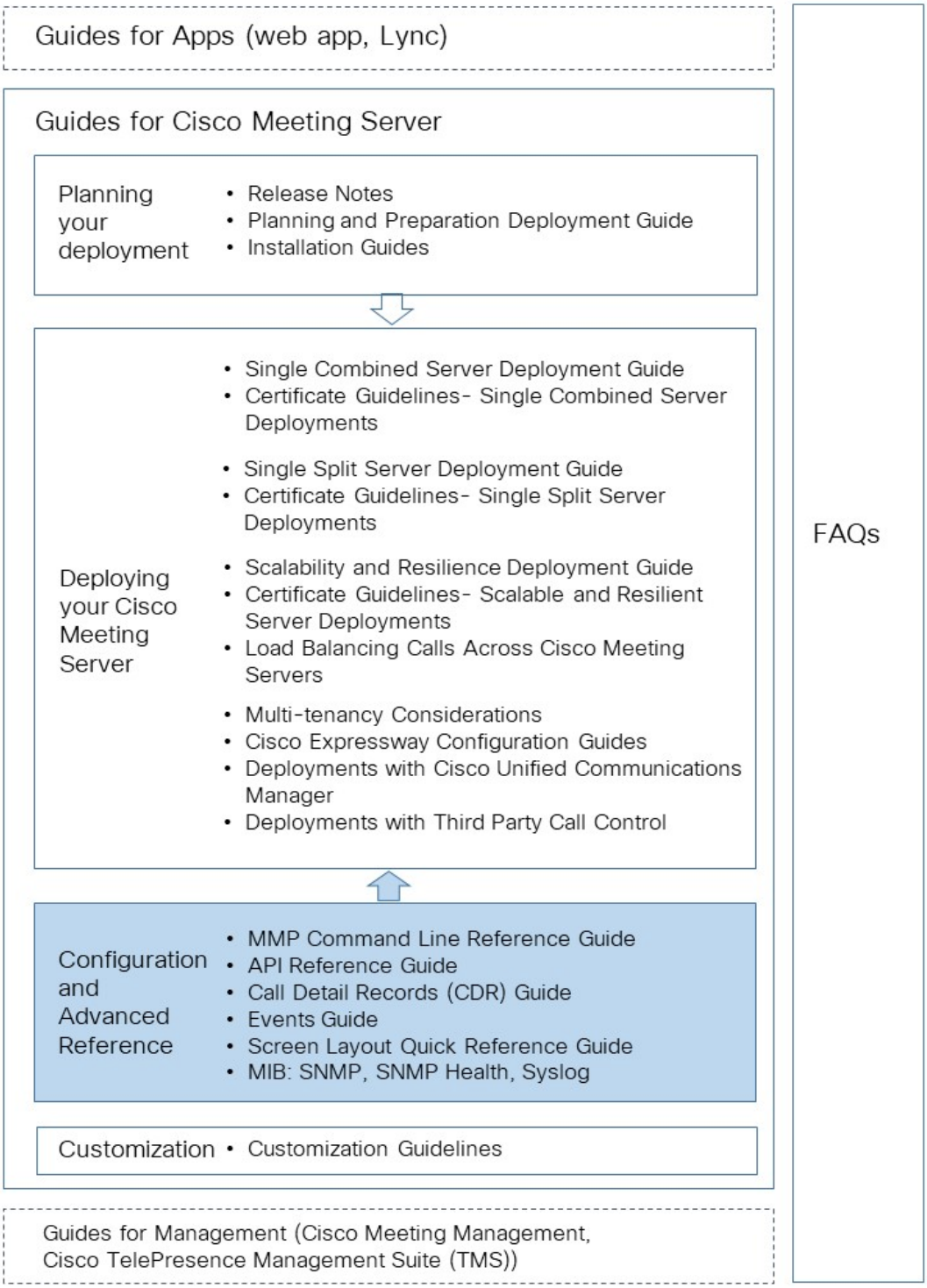
**Note:** The Cisco Meeting Server software is referred to as the Meeting Server throughout the remainder of this guide.

## 1.1 How to use this Document

This guide describes the MMP, and unless otherwise indicated, the information applies equally to the Cisco Meeting Server 2000, the Cisco Meeting Server 1000 and virtualized deployments.

These documents can be found on cisco.com.

Figure 1: Cisco Meeting Server documentation for version 3.3



## 1.2 Accessing the MMP

### 1.2.1 Cisco Meeting Server 2000

The MMP command line interface is accessed via the Serial Over LAN connection on the Cisco Meeting Server 2000. Before the MMP can be used, the Serial Over LAN connection must be configured with an IP address and credentials. Refer to the Cisco Meeting Server 2000 Installation Guide for details on configuring the Serial Over LAN connection.

After initial configuration, use an SSH client to connect to the IP address of the Serial Over LAN connection and login to the MMP using the credentials of the configured admin account.

### 1.2.2 Virtualized deployments (Cisco Meeting Server 1000 and specification based VM servers)

In virtualized deployments, the MMP is accessed through the VSphere console tab (on virtual interface A) and requires the login credentials of an MMP admin user (see MMP User Account Commands). These are set up as part of the installation procedure; see the Cisco Meeting Server Installation Guide for Virtualized Deployments.

### 1.2.3 Differences in specific commands between Cisco Meeting Server platforms

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 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.<br>For example<br>**dns add forwardzone <domain-name> <server ip>** | Do not specify an interface.<br>For example<br>**dns add forwardzone <domain-name> <server ip>** |
| **user evict** | Available from version 2.9 | Available |

## 1.3 Transferring files to and from the MMP

Files can be transferred to and from the MMP using the Secure File Transfer Protocol (SFTP). On Windows we recommend WinSCP (http://winscp.net/eng/index.php), although any client can be used. SFTP is used for transferring the following files:

- Software upgrade images
- Configuration snapshots
- Security certificates
- License files
- System log files (as directed by Cisco Support)
- Crash diagnosis files (as directed by Cisco Support)

Connect your SFTP client to the IP address of the MMP which can be found using the **ipv4** MMP or **ipv6** MMP command (as appropriate). Log in using the credentials of an MMP admin user (see MMP User Account Commands).

### 1.3.1 Which files you see in the SFTP client

After configuration you should see the following files listed when you access the MMP using SFTP (bear in mind that you may have different names for everything other than license.dat but the following are the example file names used in the installation and deployment guides):

- Server.crt, webbridge.crt
- license.dat (required name)
- boot.json and live.json
- server.key, webbridge.key
- cacert.pem, privkey.pem, server.pem

## 1.4 What MMP Commands are Available?

To see a list of commands that are available and their parameters type:

```
help
```

To see more details about one command type:

```
help <command name>
```

These commands are described in the following sections. All the commands are entered at the MMP command line interface prompt. An example is:

```
iface (a|b|c|d) <speed> (on|off)
```

where

() indicates a choice of options, use one of them – without the brackets

<> indicates a parameter that you must enter the appropriate value for

[ ] indicates an optional parameter

Some commands are followed by one or more examples in blue within the same table cell:

| Command/Examples | Description/Notes |
|---|---|
| **iface (a\|b\|c\|d)** | Displays the network interface configuration for the specified interface<br><br>Note that the A, B, C and D interfaces are restricted to full duplex auto negotiation. |

## 1.5 Writing and Completing MMP Commands

The following functionality can be used in MMP commands:

- Tab: press the Tab key to auto-complete a command. For example pressing Tab after typing **help ti** creates **help timezone**. However, if there is more than one possible command, pressing tab a second time does not provide an alternative. For example pressing Tab after **help we** provides **help webadmin** and pressing again does not provide **help webbridge**
- Left and right arrow keys move the cursor along the line of a typed command
- Up and down arrow keys cycle through the command history
- Quotation marks: to enter multiple word arguments use “” for example
  **pki csr demo CN:"callbridge.example.com" OU:"Cisco Support" O:Cisco L:"New York" ST:NY C:US**

Keyboard shortcuts can be used:

- CTRL-p: displays the previous command
- CTRL-n: displays the next command in the command history
- CTRL-d: deleted the character under cursor, or exits when used in an empty line
- CTRL-c: abort the current executing command
- CTRL-a: jumps to the beginning of the line
- CTRL-e: jumps to the end of the line
- CTRL-l: clears the terminal
- CTRL-k: deletes from the cursor position to the end of the line
- CTRL-m: equivalent to the Return key
- CTRL-w: deletes word left from cursor
- CTRL-u: deletes current line
- CTRL-f: moves forward a character

- CTRL-b: moves backward a character
- CTRL-t: swaps current character with the previous character

## 1.6 Reserved Ports

Port 8081 is reserved on loopback if the webadmin is enabled, but is not reserved if the webadmin is disabled. Port 8080 is always open.

Port 5060 is always open, while port 5061 is only open if certificates are applied to the Call Bridge.

## 1.7 Summary of MMP additions and changes

Version 3.3 supports the MMP additions described in this section.

### 1.7.1 LDAP authentication

The new **ldap** option is added to **user add** MMP command enables configuring details of an LDAP server, directory search parameters, TLS settings, and enabling or disabling LDAP authentication.

To enable adding LDAP users, a new option, [**ldap**] is added to the command:

```
user add <username> (admin|crypto|audit|appadmin|api) [ldap]
```

---

Note: Meeting Server API does not support access to users with LDAP authentication.

---

The output of the **help ldap** command is:

```
cms> help ldap
Configure LDAP client for MMP users
Usage:
    ldap
    ldap server <hostname|address> <port>
    ldap protocol (ldap|ldaps)
    ldap binddn <username>
    ldap basedn <base DN>
    ldap login_attr <attribute>
    ldap filter <filter>
    ldap remove <binddn|filter|trust>
    ldap trust <crt bundle>
```

```
ldap verify (enable|disable)
ldap min-tls-version <minimum version string>
ldap enable
ldap disable
ldap status
```

Note:
The **user list** MMP command is extended to include logged in LDAP users.
The only **user rule** parameters that apply to LDAP users are max_failed_logins, max_idle, and max_sessions. Other parameters of this command do not apply to LDAP users.
The **user expire** MMP command is not supported for LDAP users.

| Command/Examples | Description/ Notes |
|---|---|
| `ldap` | Displays information about the ldap configuration. |
| `ldap server <hostname\|address> <port>` | Specifies the LDAP server with hostname or IP address, and port number. This is mandatory. |
| `ldap protocol (ldap\|ldaps)` | Specifies the ldap protocol to use. To use a secure connection to the LDAP server, ldaps must be used. It is mandatory to specify the protocol. |
| `ldap binddn <username>`<br>`ldap binddn cn=binduser,oi=user,dc=domain,dc=com`<br>`ldap binddn "cn=bind user,o=My Company,dc=domain,dc=com"`<br>`ldap binddn domain\\username` | Adds the distinguished name with which to bind to the directory server for lookups.The binddn parameter is optional. If not specified, anonymous bind requests are used.<br>The bind user must have search permission in the directory. This command prompts for an optional bind password.<br>If spaces are included in the argument, then the argument has to be quoted. If backslashes are included, they must be escaped with a preceding backslash. |
| `ldap basedn <base DN>` | Specifies the base distinguished name to use as search base. It is mandatory to specify basedn.<br>If spaces are included in the argument, then the argument has to be quoted. If backslashes are included, they must be escaped with a preceding backslash. |

| Command/Examples | Description/ Notes |
|---|---|
| **ldap login_attr <attribute>** | Specifies the LDAP attribute name such as uid, userPrincipalName, or sAMAccountName, which uniquely identifies users. The attribute value must match the pre-configured MMP user name for successful login. Specifying an attribute is mandatory. |
| **ldap filter <filter>**<br>**ldap filter (&(objectClass=*) (memberOf=CN=admins,DC=example,DC=com))** | Sets up an LDAP search filter. Specifying a filter is optional. If no filter is specified, the default value (objectClass=*) is used.<br>A valid LDAP filter syntax must be used and it must be enclosed in parentheses. |
| **ldap remove (binddn\|filter\|trust)** | Removes binddn, filter, or trust parameters that have been set up earlier. |
| **ldap trust <crt bundle>** | Configures the system to use a particular bundle of certificates to validate the certificate.<br>To use a secure connection to the LDAP server, this must be configured with a trusted CA. |
| **ldap verify (enable\|disable)** | Enables or disables certificate verification for connection to the LDAP server.<br>To use a secure connection to the LDAP server, certificate validation must be enabled. When disabled, Meeting Server does not request or check the trust certificates. |
| **ldap min-tls-version <minimum version string>** | Configures the minimum TLS version that the system will use. Possible values are 1.0, 1.1, and 1.2. The default is version 1.2. |
| **ldap enable** | Enables the LDAP service. |
| **ldap disable** | Disables the LDAP service. |
| **ldap status** | Displays the status of the ldap service as:<br>running - indicates that the service is running<br>not running - the service is enabled but not running. Check the logs for more information.<br>disabled - the service is disabled |

### 1.7.2 SSH fingerprints verification

To verify the keys prompted by the Meeting Server against the retrieved keys before logging in, use the MMP command, **ssh server_key list.**

The output displays a list of keys along with the size, type, and fingerprints for all existing keys in the Meeting Server host, among the following keys:

- ssh_host_dsa_key.pub
- ssh_host_ecdsa_key.pub
- ssh_host_ed25519_key.pub
- ssh_host_key.pub
- ssh_host_rsa_key.pub

### 1.7.3 Scheduler configuration

The configuration details of the email server are provided via the new **`scheduler`** MMP commands listed below:

| Command / Examples | Description / Notes |
|---|---|
| **`scheduler`**<br>**`scheduler status`** | Displays current status of the Scheduler. |
| **`scheduler (enable \| disable)`** | Enables or disables the Scheduler. |
| **`scheduler restart`** | Restarts the Scheduler. |
| **`scheduler https listen <interface> <port>`** | Configures an interface:port pair for the Scheduler to listen on. |
| **`scheduler https listen none`** | Disables the Scheduler's management API interface. |
| **`scheduler https certs <key-file> <crt-fullchain-file>`** | Configures the server certs used in the management API but also the certs used when making outbound connections.For example, the c2w link or any API calls to the Call Bridge. |
| **`scheduler https certs none`** | Removes certificate configuration for the management API. |
| **`scheduler c2w certs <key-file> <crt-fullchain-file>`** | Configures the certificate bundle presented to a Web Bridge 3. |
| **`scheduler c2w certs none`** | Removes certificate configuration for the TLS connection to Web Bridge 3. |
| **`scheduler c2w trust <crt-bundle>`** | Configures the trust bundle for verifying connections to the Web Bridges. |
| **`scheduler c2w trust none`** | Removes the certificate bundle for the Web Bridge 3 from the Scheduler's trust store. |
| **`scheduler email server <hostname \| address> <port>`** | Configures the SMTP server to which the Scheduler will send emails. |
| **`scheduler email server none`** | Removes email server configuration from the Scheduler. |

| Command / Examples | Description / Notes |
|---|---|
| **scheduler email username <smtp username>** | Configures the email account used for authentication with the SMTP server. This account must have appropriate permissions to be able to send emails on behalf of the meeting organizers.<br>Note: Emails to participants will not sent from the account configured using this command, but will be sent using the From address of the meeting organizer. |
| **scheduler email remove username** | Removes the email username configured for SMTP authentication. |
| **scheduler email protocol <smtp \| smtps>** | Specifies the Scheduler's communication with the email server as:<br>smtp: over plain text TCP (smtp)<br>smtps: over an encrypted TLS channel |
| **scheduler email auth (enable \| disable)** | Enables or disables SMTP authentication. |
| **scheduler email starttls (enable \| disable)** | Enables or disables opportunistic TLS for SMTP connections. |
| **scheduler email trust <bundle> \| none** | (Optional) Allows configuration of a trust bundle for the email server. If configured, verification is done for the certificate of the email server using the configured bundle.<br>If not configured, verification of the certificate is not done. |
| **scheduler timedLogging** | Retrieves timed logging status. |
| **scheduler timedLogging (webBridge\|api\|email) <time>** | Activates logging for the specified time period. |

# 2 Network Commands

## 2.1 Network Interface (iface) Commands

| Command/Examples | Description/Notes |
|---|---|
| `iface (a\|b\|c\|d)` | Displays the network interface configuration for the specified interface<br><br>Note that the A, B, C and D interfaces are restricted to full duplex auto negotiation. |
| `iface <interface> mtu <value>`<br>`iface a mtu 1400` | Sets the maximum transmission unit size in bytes for an interface.<br><br>**Note:** In all Meeting Server 2000 deployments as well as VM and Meeting Server 1000 deployments running VMWare Version 6.7U2 and newer, the MTU applies to both incoming and outgoing packets. Packets received that are larger than the configured MTU will be dropped by the interface, causing packet loss and poor quality and in some rare cases, connection issues. In VM and Meeting Server 1000 deployments running VMWare versions prior to 6.7U2, the MTU only applies to outgoing packets, allowing packets larger than the configured MTU to still be received by the interface.<br><br>The default MTU is 1500 bytes.<br><br>MTU should be configured on the network to ensure packets are not dropped by the interface due to these MTU restrictions. |

## 2.2 IP Commands

### 2.2.1 IPv4 commands

| Command/Examples | Description/Notes |
|---|---|
| `ipv4 (a\|b\|c\|d)` | Lists configured and observed network values |
| `ipv4 (a\|b\|c\|d) dhcp` | Enables dhcp on the specified interface |
| `ipv4 (a\|b\|c\|d) (enable\|disable)` | Enables/disables the specified interface<br>Note: This command does not clear the configuration, only disables it. |

| Command/Examples | Description/Notes |
|---|---|
| **ipv4 (a\|b\|c\|d) add <server IP address>/<Prefix Length> <Default Gateway>**<br>**ipv4 a add 10.1.2.3/16 10.1.1.1** | Configures the interface with an ipv4 address with specified prefix length and default gateway for egress packets. The example configures A with address 10.1.2.3 on subnet 10.1.0.0/16. If there is no more specific route, packets exiting via A will be sent via gateway 10.1.1.1. |
| **ipv4 (a\|b\|c\|d) del <server IP address>** | Removes the IPv4 address on the specified interface |
| **ipv4 (a\|b\|c\|d) default** | Selects the interface of last resort for outbound connections. When connecting to remote hosts it is not always known from context which interface should be used. By comparison, responses to connections initiated by remote hosts will use the interface on which the connection was accepted. This is sometimes referred to as the strong IP model |
| **ipv4 (a\|b\|c\|d) route add <address>/<prefix length>**<br>**ipv4 (a\|b\|c\|d) route del <address>/<prefix length>** | Adds a static route so you can route a specific subnet out of the specific interface. This is for unique routing scenarios where multiple interfaces are enabled, and you want to ensure that traffic for a specific subnet is routed out to the gateway of that particular interface<br>Note: Generally manual configuration of a default route is not required and may cause issues. |
| **ipv4 b route add 192.168.100.0/24** | All traffic destined for 192.168.100.x will go out of interface b to interface b's gateway |

### 2.2.2 IPv6 commands

The Meeting Server supports multiple IPv6 addresses per interface, and automatically configured addresses and static addresses.

| Command/Examples | Description/Notes |
|---|---|
| **ipv6 (a\|b\|c\|d)** | Lists configured and observed network values |

| Command/Examples | Description/Notes |
|---|---|
| **ipv6 (a\|b\|c\|d) enable** | Starts auto-configuration of the specified interface for IPv6. A link-local address is generated. Duplicate Address Detection (DAD) is completed and, if SLAAC is enabled, then Router Solicitations are sent. If a Router Advertisement is received, then<br>• any advertised prefixes are used to construct global addresses<br>• any RDDNS options are used to configure DNS<br>• if the " managed" or " other" flags are set, then DHCPv6 is started. If Router Advertisements do not have the " managed" or " other" bits set, then DHCPv6 will not be used<br><br>If no Router Advertisement is received after three Router Solicitations are sent, then DHCPv6 will start. |
| **ipv6 (a\|b\|c\|d) disable** | Disables IPv6 for the specified interface |
| **ipv6 <interface> slaac (enable\|disable)** | Enables/disables SLAAC |
| **ipv6 (a\|b\|c\|d) add <address>/<prefix length>**<br>**ipv6 a add 2001::2/64** | When SLAAC is disabled, it is necessary to add static addresses and static router addresses. To add a static router, Note that SLAAC discovered addresses and routers can coexist with statically configured addresses.<br>The Meeting Server supports automatically configured addresses and static addresses. To statically configure an IPv6 address on the specified interface use this command |
| **ipv6 (a\|b\|c\|d) del <address>**<br>**ipv6 a del 2001::2/64** | Removes the IPv6 address |
| **ipv6 <interface> router add\|del <address>** | |

## 2.3 Network Diagnostic Commands

### 2.3.1 IPv4 network diagnostic commands

After you have enabled IPv4, you can you use the following commands.

| Command/Examples | Description/Notes |
|---|---|
| **ping <target address\|hostname>** | Ping from the Meeting Server to the target IP address or hostname |
| **traceroute <target address\|hostname>** | To traceroute from the Meeting Server to the target IP address or hostname |

### 2.3.2 IPv6 network diagnostic commands

After you have enabled IPv6, you can you use the following commands.

| Command/Examples | Description/Notes |
|---|---|
| **ping6 <target address\|hostname>** | Ping from the Meeting Server to the target IPv6 address or hostname |
| **traceroute6 <target address\|hostname>** | To traceroute from the Meeting Server to the target IPv6 address or hostname |

### 2.3.3 Packet capture

Note: Although packets can be captured by the Meeting Server, due to the high packet rate that the Meeting Server operates at, packets may be dropped from the packet capture rather than disturb the normal operation of the Meeting Server in handling calls. To avoid dropped packets in the packet capture, Cisco recommends capturing packets at your network switch rather than on the Meeting Server.

| Command/Examples | Description/Notes |
|---|---|
| **pcap (a\|b\|c\|d)** | Starts immediate packet capture on the specified interface and stops when you press Ctrl-C. The name of the pcap file is then displayed. This file can then be downloaded via SFTP. |
| **pcap (a\|b\|c\|d\|any) [snaplen <n>] [filter <pcap-filter-expression>]** | **any** will allow packet capture on multiple interfaces, i.e. any enabled interfaces (interfaces that are not enabled will be skipped).<br>Note: When capturing from multiple interfaces, this requires additional disk space as each interface is captured to a separate temporary file and the files are then merged when the capture is stopped. So the available storage when capture on multiple interfaces is half what is available when capturing on a single interface.<br>**snaplen** truncates each packet captured to the maximum number (n) of bytes if it is longer. As a result, more packets can fit into the same file-size limit.<br>**filter** selects only packets matching the criteria in the string. This reduces the capture to only packets of interest, and avoids wasting disk space on the others. The parsing of this string and the packet filtering are performed with exactly the same underlying libraries as used by tcpdump, so this has exactly the same expressive power and performance. The filter expression can be up to around 4080 characters long, if required<br>**snaplen** and **filter** options added from version 3.1. |

## 2.4 QoS/DSCP Commands

The Meeting Server supports QoS/DSCP values in DSCP Hex (not TOS). We follow the requirement of US Federal government institutions to allow any DSCP value between 0 and 63 for backwards compatibility even though not every value is standard.

We support input as decimal, hexadecimal (case insensitive) and octal; enter 46, 0x2E (or 0x2e), or 056, respectively, with the same result.

For example, EF Audio, AF31 Signaling/Data, AF41 Video is:

EF = 0x2E DSCP Hex, AF31 = 0x1A DSCP Hex, AF41 = 0x22 DSCP Hex

DSCP settings can be defined with independent values for IPv4 and IPv6. For example, setting oa&m to 0x4 for IPv4 and 0x6 for IPv6 results in SSH traffic being marked with 0x4 for IPv4 connections and 0x6 for IPv6 connections.

**Note:** A service restart is required for changes to take effect: we recommend rebooting the Core server.

| Command/Examples | Description/Notes |
|---|---|
| **dscp (4\|6) <traffic type> (<DSCP value>\|none)** | Sets the DSCP traffic . DSCP traffic categories and the traffic types within those categories are:<br>▪ signaling (SIP, AS-SIP signaling)<br>▪ assured-voice (any audio for AS-SIP)<br>▪ voice (any other audio)<br>▪ assured-multimedia (video for AS-SIP)<br>▪ multimedia (any other video)<br>▪ multimedia-streaming (webbridge media) (not currently used)<br>▪ low-latency (not currently used)<br>▪ oa&m (webadmin, LDAP, SSH, SFTP)<br>(oa&m = operations, administration and management) |
| **dscp 4 voice 0x2E**<br>**dscp 4 voice 46** | |
| **dscp 4 oa&m 0x22** | Sets oa&m for IPv4 |
| **dscp 4 oa&m none** | Removes the setting |
| **dscp assured (true\|false)** | It is possible to configure both assured and non-assured DSCP values for the " voice" and " multimedia" traffic types – see above. Use this command to force the use of the assured or non-assured value. |

| Command/Examples | Description/Notes |
| --- | --- |
| `dscp assured true` | For example, to force the use of the assured-voice and assured-multimedia DSCP values for all voice and video data, use this command. |

# 3 DNS Commands

| Command/Examples | Description/Notes |
|---|---|
| **dns** | Displays the current DNS configuration details |
| **dns add forwardzone <domain-name> <server ip>**<br>**dns add forwardzone example.org 192.168.0.1** | Configures a forward zone.<br>A forward zone is a pair consisting of a domain name and at least one 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 is to specify " ." as the domain name i.e. the root of the DNS hierarchy, which matches every domain name. |
| **dns del forwardzone <domain-name> <server ip>** | Deletes a specified forward zone |
| **dns add trustanchor <anchor>**<br><br>**dnsadd trustanchor ". IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A4 1855200FD2CE1CDDE32F24E8FB5"** | Adds a trust anchor for Domain Name System Security Extensions (DNSSEC).<br>Trust anchors should be specified in DNS Resource Record form inside quotation marks – see the example. See [1] for details. |
| **dns del trustanchor <zonename>**<br>**dns del trustanchor** | Removes a trust anchor.<br>The zonename is the domain name in the Resource Record (RR) representing the anchor. The example removes the trust anchor installed in the example above. |

| Command/Examples | Description/Notes |
|---|---|
| **dns add rr <DNS RR>**<br>**dns add rr "sipserver.local. IN A 172.16.48.1"**<br>**dns add rr "_sip._tcp.example.com. 86400 IN SRV 0 5 5060 sipserver.local."** | To configure the DNS resolver(s) to return values which are not configured in external DNS servers or which need to be overridden, custom Resource Records (RRs) can be configured which will be returned instead of querying external DNS servers.<br><br>We accept RRs in quotation marks with the following format:<br>**OWNER <OPTIONAL TTL> CLASS TYPE TYPE-SPECIFIC-DATA**<br><br>For example,<br>A records sipserver.local. IN A 172.16.48.1<br>AAAA records example.com. aaaa 3ffe:1900:4545:2:02d0:09ff:fef7:6d2c<br>SRV records _sip._tcp.example.com. 86400 IN SRV 0 5 5060 sipserver.local<br><br>Note: if you wish to create create multiple RRs for a single record type then you need to create them using an external DNS server. The Meeting Server does not support multiple RRs for a single record type and will only save the latest RR. For example, the Meeting Server will only save 1 SRV record for _sipinternaltls._tcp, etc...it will not save 2 different RRs for _sipinternaltls._tcp. |
| **dns del rr <owner-name> <type>**<br>**dns del rr _sip._tcp.example.com. SRV**<br>**dns del rr sipserver.local. A** | |
| **dns lookup <a\|aaaa\|srv> <hostname>**<br>**dns lookup srv _sip._tcp.example.com** | The lookup " drills" through SRV results. That is, when an SRV record returns a domain name this is resolved by A and AAAA lookups. |
| **dns flush** | This flushes the DNS cache of of the Meeting Server. |

# 4 Firewall Commands

The MMP supports the creation of simple firewall rules for the media interfaces. After setting up the firewall rule on an interface, enable the firewall on that interface.

Note: This is not intended to be a substitute for a full standalone firewall solution.

Firewall rules must be specified separately for each interface.

Each firewall rule for an interface is identified by a tag. These can be seen in the status output, for example:

```
Interface      : a
Enabled        : false
Default policy : allow

Tag     Rule
---     ----
0       drop 80
```

CAUTION: We recommend using the serial console, if available, to configure the firewall, because using SSH means that an error in the rules would make the SSH port inaccessible.

| Command/Examples | Description/Notes |
|---|---|
| **firewall <iface> default (allow\|deny)**<br><br>**firewall a default deny** | Before the firewall can be enabled on an interface, a default policy must be set using this command.<br>The allow policy allows all packets that do not match any rule, and the deny policy discards all packets that do not match any rule<br>When no rules are configured this will drop every packet on interface a. |
| **firewall <iface> enable** | Enables the firewall on the specified interface. |
| **firewall <iface> disable** | Disables the firewall on the specified interface. |
| **firewall <iface>** | Displays the current firewall settings for a given interface |
| **firewall a** | Displays the status and rule set for the interface a |

| Command/Examples | Description/Notes |
|---|---|
| **firewall <iface> allow <port> [/<proto>] [from <host>[/<prefix>]]**<br><br>**firewall <iface> deny <port> [/<proto>] [from <host>[/<prefix>]]** | Add rules with these commands.<br>The <port> argument can be specified either as a number (e.g. " 80" ) or as service name from the IANA service name registry (e.g. " http" ).<br>The protocol argument is either tcp or udp. If omitted, the rule matches both TCP and UDP packets. |
| **firewall a allow http/tcp** | Allows TCP packets on port 80 on interface A |
| **firewall a deny 678** | Drops all packets on port 678 on media interface A |
| | An optional **from** clause limits the hosts to which a rule applies. This is specified as an IPv4 or IPv6 address with an optional prefix length to denote a subnet. |
| **firewall a allow ssh from 192.168.1.0/28** | Allows SSH access to interface a from the 256 IPv4 address between 192.168.1.0 and 192.168.1.255 |
| **firewall <iface> delete <tag>** | To delete a rule, use its tag with this command. |
| **firewall a delete 0** | Deletes the single rule above this table. |

# 5 LDAP Commands

The new **ldap** option is added to **user add** MMP command enables configuring details of an LDAP server, directory search parameters, TLS settings, and enabling or disabling LDAP authentication.

To enable adding LDAP users, a new option, [**ldap**] is added to the command:

```
user add <username> (admin|crypto|audit|appadmin|api) [ldap]
```

---

Note: Meeting Server API does not support access to users with LDAP authentication.

---

The output of the **help ldap** command is:

```
cms> help ldap
Configure LDAP client for MMP users
Usage:
    ldap
    ldap server <hostname|address> <port>
    ldap protocol (ldap|ldaps)
    ldap binddn <username>
    ldap basedn <base DN>
    ldap login_attr <attribute>
    ldap filter <filter>
    ldap remove <binddn|filter|trust>
    ldap trust <crt bundle>
    ldap verify (enable|disable)
    ldap min-tls-version <minimum version string>
    ldap enable
    ldap disable
    ldap status
```

---

Note:
The **user list** MMP command is extended to include logged in LDAP users.
The only **user rule** parameters that apply to LDAP users are max_failed_logins, max_idle, and max_sessions. Other parameters of this command do not apply to LDAP users.
The **user expire** MMP command is not supported for LDAP users.

---

| Command/Examples | Description/ Notes |
|---|---|
| **ldap** | Displays information about the ldap configuration. |
| **ldap server <hostname\|address> <port>** | Specifies the LDAP server with hostname or IP address, and port number. This is mandatory. |
| **ldap protocol (ldap\|ldaps)** | Specifies the ldap protocol to use. To use a secure connection to the LDAP server, ldaps must be used. It is mandatory to specify the protocol. |
| **ldap binddn <username>**<br>**ldap binddn cn=binduser,oi=user,dc=domain,dc=com**<br>**ldap binddn "cn=bind user,o=My Company,dc=domain,dc=com"**<br>**ldap binddn domain\\username** | Adds the distinguished name with which to bind to the directory server for lookups.The binddn parameter is optional. If not specified, anonymous bind requests are used.<br>The bind user must have search permission in the directory. This command prompts for an optional bind password.<br>If spaces are included in the argument, then the argument has to be quoted. If backslashes are included, they must be escaped with a preceding backslash. |
| **ldap basedn <base DN>** | Specifies the base distinguished name to use as search base. It is mandatory to specify basedn.<br>If spaces are included in the argument, then the argument has to be quoted. If backslashes are included, they must be escaped with a preceding backslash. |
| **ldap login_attr <attribute>** | Specifies the LDAP attribute name such as uid, userPrincipalName, or sAMAccountName, which uniquely identifies users. The attribute value must match the pre-configured MMP user name for successful login. Specifying an attribute is mandatory. |
| **ldap filter <filter>**<br>**ldap filter (&(objectClass=*) (memberOf=CN=admins,DC=example,DC=com))** | Sets up an LDAP search filter. Specifying a filter is optional. If no filter is specified, the default value (objectClass=*) is used.<br>A valid LDAP filter syntax must be used and it must be enclosed in parentheses. |
| **ldap remove (binddn\|filter\|trust)** | Removes binddn, filter, or trust parameters that have been set up earlier. |

| Command/Examples | Description/ Notes |
|---|---|
| **ldap trust <crt bundle>** | Configures the system to use a particular bundle of certificates to validate the certificate.<br>To use a secure connection to the LDAP server, this must be configured with a trusted CA. |
| **ldap verify (enable\|disable)** | Enables or disables certificate verification for connection to the LDAP server.<br>To use a secure connection to the LDAP server, certificate validation must be enabled. When disabled, Meeting Server does not request or check the trust certificates. |
| **ldap min-tls-version <minimum version string>** | Configures the minimum TLS version that the system will use. Possible values are 1.0, 1.1, and 1.2. The default is version 1.2. |
| **ldap enable** | Enables the LDAP service. |
| **ldap disable** | Disables the LDAP service. |
| **ldap status** | Displays the status of the ldap service as:<br>running - indicates that the service is running<br>not running - the service is enabled but not running. Check the logs for more information.<br>disabled - the service is disabled |

# 6 Scheduler Commands

Scheduling meetings is enabled by the new Scheduler component, which can be configured by the new **scheduler** MMP commands.

The configuration details of the email server are provided via the new **scheduler** MMP commands listed below:

| Command / Examples | Description / Notes |
|---|---|
| **scheduler**<br>**scheduler status** | Displays current status of the Scheduler. |
| **scheduler (enable \| disable)** | Enables or disables the Scheduler. |
| **scheduler restart** | Restarts the Scheduler. |
| **scheduler https listen <interface> <port>** | Configures an interface:port pair for the Scheduler to listen on. |
| **scheduler https listen none** | Disables the Scheduler's management API interface. |
| **scheduler https certs <key-file> <crt-fullchain-file>** | Configures the server certs used in the management API but also the certs used when making outbound connections.For example, the c2w link or any API calls to the Call Bridge. |
| **scheduler https certs none** | Removes certificate configuration for the management API. |
| **scheduler c2w certs <key-file> <crt-fullchain-file>** | Configures the certificate bundle presented to a Web Bridge 3. |
| **scheduler c2w certs none** | Removes certificate configuration for the TLS connection to Web Bridge 3. |
| **scheduler c2w trust <crt-bundle>** | Configures the trust bundle for verifying connections to the Web Bridges. |
| **scheduler c2w trust none** | Removes the certificate bundle for the Web Bridge 3 from the Scheduler's trust store. |
| **scheduler email server <hostname \| address> <port>** | Configures the SMTP server to which the Scheduler will send emails. |
| **scheduler email server none** | Removes email server configuration from the Scheduler. |
| **scheduler email username <smtp user-name>** | Configures the email account used for authentication with the SMTP server. This account must have appropriate permissions to be able to send emails on behalf of the meeting organizers.<br>**Note:** Emails to participants will not sent from the account configured using this command, but will be sent using the From address of the meeting organizer. |

| Command / Examples | Description / Notes |
|---|---|
| **scheduler email remove username** | Removes the email username configured for SMTP authentication. |
| **scheduler email protocol <smtp \| smtps>** | Specifies the Scheduler's communication with the email server as:<br>smtp: over plain text TCP (smtp)<br>smtps: over an encrypted TLS channel |
| **scheduler email auth (enable \| disable)** | Enables or disables SMTP authentication. |
| **scheduler email starttls (enable \| disable)** | Enables or disables opportunistic TLS for SMTP connections. |
| **scheduler email trust <bundle> \| none** | (Optional) Allows configuration of a trust bundle for the email server. If configured, verification is done for the certificate of the email server using the configured bundle.<br>If not configured, verification of the certificate is not done. |
| **scheduler timedLogging** | Retrieves timed logging status. |
| **scheduler timedLogging (webBridge\|api\|email) <time>** | Activates logging for the specified time period. |

# 7 Provisioning with Certificates

Use the following PKI (Public Key Infrastructure) commands.

The key file should contain an RSA or DSA key encoded as either PEM or DER with the file name extension being .key, .pem, or .der . The certificate file should be an x509 certificate encoded as PEM or DER with the file name extension being .crt, .cer, .pem, or .der.

File names can include alphanumeric characters, hyphens and underscore characters followed by one of the extensions above. You can choose the per-service certificate and key file names; even using the same pair of files for every service.

The private key and certificate files should be uploaded via SFTP.

| Command/Examples | Description/Notes |
|---|---|
| **pki** | Displays current PKI usage. |
| **pki list** | Lists PKI files i.e. private keys, certificates and certificate signing requests (CSRs). |
| **pki inspect <filename>** | Inspect a file and shows whether the file is a private key, a certificate, a CSR or unknown. In the case of certificates, various details are displayed. If the file contains a bundle of certificates, information about each element of the bundle is displayed.<br>Both PEM and DER format files are handled. |
| **pki match <key> <certificate>** | This command checks whether the specified key and a certificate on the system match. A private key and a certificate are two halves of one usable identity and must match if they are to be used for a service e.g. HTTPS. |
| **pki verify <cert> <cert bundle/CA cert> [<CA cert>]**<br><br>**pki verify server.pem bundle.pem rootca.pem**<br>**pki verify server.pem bundle.pem** | A certificate may signed by a certificate authority (CA) and the CA will provide a " certificate bundle" of intermediate CA certificates and perhaps a CA certificate in its own file. To check that the certificate is signed by the CA and that the certificate bundle can be used to assert this, use this command. |
| **pki unlock <key>** | Private keys are often provided with password-protection. To be used in the Meeting Server, the key must be unlocked.<br>This command prompts for a password to unlock the target file. The locked name will be replaced by an unlocked key with the same name |

| Command/Examples | Description/Notes |
|---|---|
| **pki csr <key/cert basename> [<attribute>:<value>]**<br><br>**pki csr dbserver CN:server01.db.example.com subjectAltName:server02.db.example.com** | For users happy to trust that Cisco meets requirements for generation of private key material, private keys and associated Certificate Signing Requests can be generated.<br><key/cert basename> is a string identifying the new key and CSR (e.g. " new" results in " new.key" and " new.csr" files)<br>Attributes for the CSR can be specified in pairs with the attribute name and value separated by a colon (" :" ).<br>Attributes are:<br>CN: commonName which should be on the certificate. The commonName should be the DNS name for the system.<br>OU: Organizational Unit<br>O: Organization<br>L: Locality<br>ST:State<br>C: Country<br>emailAddress: email address<br><br>The CSR file can be downloaded by SFTP and given to a certificate authority (CA) to be signed. (Alternatively, the CSR file can be used in the 'pki sign' command to generate a certificate locally.) On return it must be uploaded via SFTP. It can then be used as a certificate.<br>Note: **pki csr <key/cert basename> [<attribute>:<value>]** takes subjectAltName as an attribute. IP addresses and domain names are supported for subjectAltName in a comma separated list. For example:<br>**pki csr test1 CN:example.exampledemo.com subjectAltName:exampledemo.com**<br>**pki csr test2 CN:example.exampledemo.com C:US L:Purcellville O:Example OU:Support ST:Virginia subjectAltName:exampledemo.com**<br>**pki csr test3 CN:example.exampledemo.com C:US L:Purcellville O:Example OU:Support ST:Virginia subjectAltName:exampledemo.com, 192.168.1.25,server.exampledemo.com, join.exampledemo.com, test.exampledemo.com**<br>Keep the size of certificates and the number of certificates in the chain to a minimum; otherwise TLS handshake round trip times will become long. |

| Command/Examples | Description/Notes |
|---|---|
| **pki selfsigned <key/cert basename> [<attribute>:<value>]**<br>**pki selfsigned dbca CN:"my company CA" OU:"My company" O:cms L:Raleigh ST:"North Carolina" C:US** | You can use this command to generate self-signed certificates.<br><key/cert basename> identifies the key and certificate which will be generated, e.g. " pki selfsigned new" creates new.key and new.crt (which is self-signed).<br>Attributes for the certificate can be specified in pairs with the attribute name and value separated by a colon (" :" ). Attributes are:<br>CN: commonName. If the certificate is used as end-entity certificate, the commonName should be the DNS name for the relevant service..<br>OU: Organizational Unit<br>O: Organization<br>L: Locality<br>ST:State<br>C: Country<br>emailAddress: email address<br>Self-signed certificates can be used to sign CSRs. They are useful to deploy on internal services such as the database cluster. For external services such as Web services, use an external CA. |
| **pki sign <csr/cert basename> <CA key/cert basename>**<br>**pki sign dbserver dbca**<br>**pki sign dbclient dbca** | This command signs the csr identified by <csr/cert basename> and generates a certificate with the same basename, signed with the CA certificate and key identified by <CA key/cert basename>.<br>The files <csr/cert basename> and <CA key/cert basename> should have been generated by the commands 'pki csr' and 'pki selfsigned' respectively. |
| **pki pkcs12-to-ssh <username>**<br>**pki pkcs12-to-ssh john** | Public SSH keys stored in PKCS#12 files can be used but need to be processed first. This command extracts a useable public key from a PKCS#12 file uploaded with the name <username>.pub.You are prompted to enter the password for the pkcs#12 file. After completion, the pkcs#12 file is replaced with a useable key without password protection.<br>Note: Any other data contained in the pkcs#12 file is lost.<br>The key of an uploaded PKCS#12 file john.pub for user john can be made useable by executing this command |

| Command/Examples | Description/Notes |
|---|---|
| **pki** | Displays current PKI usage. |

| Command/Examples | Description/Notes |
|---|---|
| **pki list** | Lists PKI files i.e. private keys, certificates and certificate signing requests (CSRs). |
| **pki inspect <filename>** | Inspect a file and shows whether the file is a private key, a certificate, a CSR or unknown. In the case of certificates, various details are displayed. If the file contains a bundle of certificates, information about each element of the bundle is displayed.<br>Both PEM and DER format files are handled. |
| **pki match <key> <certificate>** | This command checks whether the specified key and a certificate on the system match. A private key and a certificate are two halves of one usable identity and must match if they are to be used for a service e.g. callbridge. |
| **pki verify <cert> <cert bundle/CA cert> [<CA cert>]**<br><br>**pki verify server.pem bundle.pem rootca.pem**<br>**pki verify server.pem bundle.pem** | A certificate may signed by a certificate authority (CA) and the CA will provide a " certificate bundle" of intermediate CA certificates and perhaps a CA certificate in its own file. To check that the certificate is signed by the CA and that the certificate bundle can be used to assert this, use this command. |
| **pki unlock <key>** | Private keys are often provided with password-protection. To be used in the Meeting Server, the key must be unlocked.<br>This command prompts for a password to unlock the target file. The locked name will be replaced by an unlocked key with the same name |

| Command/Examples | Description/Notes |
|---|---|
| **pki csr <key/cert basename> [<attribute>:<value>]**<br><br>**pki csr example CN:www.example.com OU:"My Desk" O:"My Office" L:"San Jose" ST:California C:US** | For users happy to trust that Cisco meets requirements for generation of private key material, private keys and associated Certificate Signing Requests can be generated.<br><key/cert basename> is a string identifying the new key and CSR (e.g. " new" results in " new.key" and " new.csr" files)<br>Attributes for the CSR can be specified in pairs with the attribute name and value separated by a colon (" :" ). Attributes are:<br>CN: commonName which should be on the certificate. The commonName should be the DNS name for the system.<br>OU: Organizational Unit<br>O: Organization<br>L: Locality<br>ST:State<br>C: Country<br>emailAddress: email address<br><br>The CSR file can be downloaded by SFTP and given to a certificate authority (CA) to be signed. (Alternatively, the CSR file can be used in the 'pki sign' command to generate a certificate locally.) On return it must be uploaded via SFTP. It can then be used as a certificate.<br>Note: Since 1.6.11 **pki csr <key/cert basename> [<attribute>:<value>]** now takes subjectAltName as an attribute. IP addresses and domain names are supported for subjectAltName in a comma separated list. For example:<br>**pki csr test1 CN:example.exampledemo.com subjectAltName:exampledemo.com**<br>**pki csr test2 CN:example.exampledemo.com C:US L:Purcellville O:Example OU:Support ST:Virginia subjectAltName:exampledemo.com**<br>**pki csr test3 CN:example.exampledemo.com C:US L:Purcellville O:Example OU:Support ST:Virginia subjectAltName:exampledemo.com, 192.168.1.25,exampledemo.com, server.exampledemo.com,join.exampledemo.com, test.exampledemo.com**<br>Keep the size of certificates and the number of certificates in the chain to a minimum; otherwise TLS handshake round trip times will become long. |

| Command/Examples | Description/Notes |
|---|---|
| **pki selfsigned <key/cert basename> [<attribute>:<value>]** | You can use this command to generate self-signed certificates. <key/cert basename> identifies the key and certificate which will be generated, e.g. " pki selfsigned new" creates new.key and new.crt (which is self-signed).<br>Attributes for the CSR can be specified in pairs with the attribute name and value separated by a colon (" :" ). Attributes are:<br>CN: commonName which should be on the certificate. The commonName should be the DNS name for the system.<br>OU: Organizational Unit<br>O: Organization<br>L: Locality<br>ST:State<br>C: Country<br>emailAddress: email address<br>The CSR file can be downloaded by SFTP and given to a certificate authority (CA) to be signed. On return it must be uploaded via SFTP. It can then be used as a certificate.<br>Keep the size of certificates and the number of certificates in the chain to a minimum; otherwise TLS handshake round trip times will become long. |
| **pki sign <csr/cert basename> <CA key/cert basename>** | This command signs the csr identified by <csr/cert basename> and generates a certificate with the same basename, signed with the CA certificate and key identified by <CA key/cert basename>.<br>The files <csr/cert basename> and <CA key/cert basename> should have been generated by the commands 'pki csr' and 'pki selfsigned' respectively. |
| **pki pkcs12-to-ssh <username>** | Public SSH keys stored in PKCS#12 files can be used but need to be processed first. This command extracts a useable public key from a PKCS#12 file uploaded with the name <username>.pub.You are prompted to enter the password for the pkcs#12 file. After completion, the pkcs#12 file is replaced with a useable key without password protection.<br>Note: Any other data contained in the pkcs#12 file is lost. |
| **pki pkcs12-to-ssh john** | The key of an uploaded PKCS#12 file john.pub for user john can be made useable by executing this command |

## 7.1 TLS Certificate Verification

**Note:** If TLS certificate verification is enabled, ensure that the remote device's certificate has both Server and Client Authentication attributes defined. This will ensure both outgoing and incoming TLS connections are accepted.

Note: When LDAP servers are configured with secure connection, connections are not fully secure until TLS certificate verification has been configured using the **`tls ldap`** command on the MMP.

Meeting Server uses a minimum of TLS 1.2 and DTLS 1.2 by default for all services: SIP, LDAP, HTTPS (inbound connections: API, Web Admin and Web Bridge 3; outbound connections: CDRs) and RTMPS. If needed for interop with older software that has not implemented TLS 1.2, a lower version of the protocol can be set as the minimum TLS version for the SIP, LDAP and HTTPS services. See **`tls <service> min-tls-version <minimum version string>`** and **`tls min-dtls-version <minimum version string>`** commands below.

Note: A Call Bridge restart is required for changes to the **`tls`** configuration to be applied. However if the **`tls syslog`** configuration is modified, then the syslog service must be disabled and enabled after the call bridge restart.

Note: A future version of Meeting Server may completely remove TLS 1.0.

| Com-mand/Examples | Description/Notes |
|---|---|
| **`tls <service>`**<br><br>**`tls ldap`** | Displays the configuration for a service , i.e. sip\|ldap\|dtls\|webadmin\|rtmps (Note: RTMPS support from version 3.1.)<br><br>Displays the setting for LDAP. |
| **`tls <service> trust <crt bundle>`**<br>**`tls ldap trust ldap.crt`** | Configures the system to use a particular bundle of certificates to validate the certificate of a remote service |
| **`tls <service> verify (enable\|dis-able\|ocsp)`** | Enables/disables certificate verification for a service. When enabled, if the system fails to verify the remote service's certificate, then the connection will be aborted.<br>Enables verification with the additional requirement that the remote service returns a stapled OCSP response to ascertain certificate revocation status.<br>The connection to the remote service will be aborted if either the system fails to verify the certificate validity or the certificate revocation status is unknown or revoked. |

| Com-mand/Examples | Description/Notes |
|---|---|
| **tls sip ciphers <cipher string>** | See below for an explanation of when you might need to use the tls cipher command. The cipher string format is a colon separated list of ciphers as used by OpenSSL (https://www.openssl.org/docs/manmaster/man1/openssl-ciphers.html#CIPHER-LIST-FORMAT). The current default for cipher support is:<br>" ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:RSA+AES:!aNULL:!MD5:!DSS:!3DES" (up to Version 2.4.2)<br>" ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:RSA+AES:!aNULL:!MD5:!DSS:!3DES:!aDH:!aECDH" (from version 2.4.3 onwards)<br>ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:RSA+AES:!aNULL:!MD5:!DSS:!3DES:!aDH:!aECDH<br>Note: " :!aDH:!aECDH:!SEED:!eNULL:!aNULL:!ARIA:!AESCCM8" is automatically appended to the configured cipher string to disallow very weak ciphers. |
| **tls <service> min-tls-version <minimum version string>**<br><br>**tls sip min-tls-version 1.1**<br><br>**tls ldap min-tls-version 1.1** | Use this command to change the default TLS version used by the Meeting Server. (From version 2.3). Note: When you change the minimum version of TLS, you need to restart the Call bridge service using the command **callbridge restart**.<br>The Meeting Server uses a minimum of TLS 1.2 for all services. If needed for interop with older software that has not implemented TLS 1.2, the minimum TLS version for SIP, LDAP and HTTPS can be configured to a lower version of the protocol.<br>Use TLS version 1.1 or later for SIP<br><br>Use TLS version 1.1 or later for LDAP |
| **tls min-dtls-version <minimum version string>**<br>**tls min-dtls-version 1.1** | Configures the minimum DTLS version that the system will use. (From version 2.3). Note: When you change the minimum version of DTLS, you need to restart the Call bridge service using the command **callbridge restart**. (From version 2.3)<br><br>If needed for interop with older software that has not implemented DTLS 1.2, configure DTLS to use a lower version of the protocol. |

By default, the Meeting Server only uses secure ciphers for any TLS connections, including SIP TLS on tcp port 5061. However, this may mean that the Meeting Server may be unable to make TLS calls with older, less secure devices. If your deployment has older kit, use this tls ciphers command to specify a list of ciphers that is acceptable to the older devices. See the Openssl guide for more information on ciphers.

Symptoms that a device cannot handle secure ciphers include:

- SIP TLS calls failing to the device,
- HTTPS access not working on the device,

- errors appearing in the logs.

# 8 Commands for Configuring the Cisco Meeting Server

Note: To determine the health of the Cisco Meeting Server 2000 use the Cisco UCS Manager.

| Command/Examples | Description/Notes |
|---|---|
| **uptime** | Displays the time since the Meeting Server was last rebooted |
| **shutdown** | Powers off the Meeting Server when you enter Y in response to the prompt.<br>Note: shutdown is not available through the MMP on the Cisco Meeting Server 2000. Use Cisco UCS Manager to power down blade servers before removing power.<br>The VM must be shut down using the MMP command 'shutdown'. This ensures that the Meeting Server sends an appropriate disconnect message to all connected devices including participants in a meeting and Meeting Management. |
| **hostname <name>**<br>**hostname mybox.mydomain** | Sets the hostname for the server.<br>Note: A reboot is required after issuing this command. |
| **timezone** | Displays the currently configured timezone |
| **timezone <timezone name>**<br>**timezone Europe/London** | Sets the time zone for the Meeting Server. The Meeting Server uses the standard IANA time zone database. See this link for a list.<br>Note: A reboot is required after issuing this command. |
| **timezone list** | Prints a full list of the available timezones.<br>Note: if you choose to use the timezone with offset from GMT, Etc/GMT<offset>, the offset uses POSIX-style signs. As a consequence the timezone for Hong Kong is Etc/GMT-8, and NOT Etc/GMT+8. |
| **ntp server add\|del <host>** | Configures/deletes an NTP server. <host> can be a name or IP address |
| **ntp status** | Checks the status of the NTP servers |
| **ntp server list** | Display a list of configured NTP servers |
| **ntp groupkey <keyfile>** | Adds an NTPv4 group key for autokey support |
| **ntp autokey (enable\|disable)** | Enables or disables autokey support |

| Command/Examples | Description/Notes |
|---|---|
| **ntp groupkey group.key**<br>**ntp autokey enable** | For example, a group key file can be uploaded using SFTP to " group.key" and configured with these commands. |
| **date**<br><br>**date set <date> <time>**<br><br><br><br><br><br><br><br>**date set 2013-08-17 13:04** | Displays the current system (in UTC) and local time<br><br>Sets the date and time. This command should only be necessary in virtualized deployments, and server deployments that do not use an NTP server.<br>The accepted formats for date and time are:<br>• ISO 8601 format (%Y-%m-%d) plus 24-hour time with hour separated by a space<br>• %m/%d/%y plus 24 hour time<br><br>Note: Users of systems with an NTP server should not need to use this command. |
| **reboot** | Reboots the Meeting Server.<br>Note: Rebooting the Meeting Server will disconnect any calls. The process takes some minutes to complete. |
| **license** | This command only applies on virtualized servers.<br>It checks the Meeting Server license status and displays licensed features, e.g.:<br>Feature: callbridge status: Activated expiry: 2014-JUl-01 (12 days remain) |
| **callbridge**<br><br>**callbridge listen (interface allowed list\|none)**<br>**callbridge listen a**<br><br><br>**callbridge listen none**<br><br>**callbridge prefer <interface>**<br><br><br><br>**callbridge certs <key-file> <cert-file>[<crt-bundle>]**<br><br><br>**callbridge certs none** | Displays the current status<br><br>Configures one or more interfaces (chosen from A, B, C or D) for the Call Bridge to listen on.<br><br><br><br>Stops the Call Bridge and disables listening services; however, the Call Bridge remains enabled.<br><br>Choses one interface from the interface allowed list as the " preferred" SIP interface: this interface is used as the contact address when routing or heuristics cannot be used to select a unique interface.<br><br>Defines the names of the key file name and certificate file name for the Meeting Server and, optionally, a CA certificate bundle as provided by your CA. (Also see Chapter 7.)<br><br>Removes certificate configuration |

| Command/Examples | Description/Notes |
|---|---|
| **callbridge trust cluster <trusted cluster certificate bundle>** | Configures the Call Bridge to use a particular bundle of certificates to validate the identity of the Call Bridges in the cluster. The bundle can be either a certificate chain, or an allowed list of trusted certificates. (From version 2.4). |
| **callbridge trust cluster none** | Removes the certificate bundle for the Call Bridge cluster from the Call Bridge trust store. (From version 2.4). |
| **callbridge restart** | Restarts the core media services. Note: Rebooting the Meeting Server will disconnect any calls. The process takes some minutes to complete. |
| **syslog server add <hostname> [<port>]**<br>**syslog server del <hostname>**<br>**syslog server add tls:syslog.example.com 514** | The Meeting Server can send its log files to a remote syslog server over TCP (not UDP)<br>The port defaults to 514<br>To specify that TLS should be used to protect the syslog data in transit, prefix the hostname/IP address of the remote server with " tls:" |
| **syslog** | Lists the current syslog configuration |
| **syslog enable**<br>**syslog disable** | Enables the syslog mechanism |
| **syslog audit add <hostname>**<br>**syslog audit add audit-server.example.org**<br>**syslog audit del <hostname>** | Defines the server where the audit logs will be sent. The audit log is a subset of the full system log and contains information on security events (logins, etc.) and configuration changes.<br>Note: These syslog audit commands can only be run by a user with the audit role. |
| **audit http (enable\|disable)** | Enables/disables detailed audit of HTTP transactions |
| **syslog tail [<number of lines>]** | Shows the most recent log messages. By default this is 10 messages but the number can be changed with the optional argument |
| **syslog page** | Displays the complete log interactively. Press the Space-bar to display the next page of log messages; press q to quit. |
| **syslog follow** | Displays log messages as they are written in real-time. Ctrl+C stops the output and returns you to the admin shell. |

| Command/Examples | Description/Notes |
|---|---|
| **syslog search <string>**<br>**syslog search error** | Displays only those messages that match a certain pattern<br><br>Note: If the current user has the audit role then the tail and search commands display audit log messages; otherwise they display message from the system log. See Section 11.6 for details on downloading the system logs |
| **syslog rotate <filename>**<br>**syslog rotate mylog** | Saves the log file permanently to the file with the specified filename, and empties the active system log. The saved file can be downloaded using SFTP. |
| **version** | Displays the software release currently installed on the Meeting Server. |

## 8.1 Federal Information Processing Standard

The Meeting Server provides a FIPS 140-2 level 1 certified software cryptographic module (http://en.wikipedia.org/wiki/FIPS_140-2). For information on which Cisco Meeting Server software releases are FIPS certified, click on this link.

By enabling FIPS mode, cryptographic operations are carried out using this module and cryptographic operations are restricted to the FIPS-approved cryptographic algorithms.

| Command/Examples | Description/Notes |
|---|---|
| **fips** | Displays whether FIPS mode is enabled |
| **fips enable**<br>**fips disable** | Enables the FIPS-140-2 mode cryptography for all cryptographic operations for network traffic.<br>After enabling or disabling FIPS mode, a reboot is required |
| **fips test** | To run the built-in FIPS test |

# 9 MMP User Account Commands

The MMP user account roles are:

- admin: MMP administrator; permitted to do all tasks
- crypto: MMP cryptography operator; permitted to do crypto-related tasks
- audit: To send audit logs to a Syslog server (refer to the Remote Syslog server section in the deployment guide for guidance on how to do this)
- appadmin: Can perform application level configuration through the Web Admin Interface
- api: Can use the API. Note that the " api" user role was previously configured through the Web Admin Interface
- ldap:The user added is a LDAP user.

---

Note: Do not confuse user accounts set up with the commands in this section, with accounts which are set up using Active Directory and which let users log in on a Cisco Meeting App and make calls.

---

Unless otherwise mentioned the following commands require you to be logged into an MMP account with admin rights.

| Command/Examples | Description/Notes |
|---|---|
| **`user add <username> (admin\|crypto\|audit\|appadmin\|api) [ldap]`** | Creates a new MMP user of the specified type (see above) or the user created is a LDAP user.<br>Prompts for a password for the user which must be entered twice to ensure that the intended password is configured.<br>On first login, the user will be asked to configure a new password.<br><br>CAUTION: User passwords expire after 6 months, except for LDAP users. |
| **`user del <username>`** | Deletes a user from the system.<br>CAUTION: **`user del <username>`** does not automatically evict users already logged in. You are advised to use **`user list`** to check whether they are logged in, and if they are then use **`user evict <username>`** to terminate all of their sessions before deleting them. |
| **`user list`** | Displays the list of users, their role, the expiry date of their password and whether or not they are logged in. |

| Command/Examples | Description/Notes |
|---|---|
| **user info <username>** | Displays user details including role, last login, number of failed login attempts since last login, last time password was changed, expiry date of password, if the account is locked or not. |
| **user evict <username>** | Logs a user out from their MMP session. Note: if you use this command on a user who is currently active in a Web Admin session, your MMP session will freeze and you will need to relogin to the MMP.<br><br>Note: From version 2.9, this command is available on the Cisco Meeting Server 2000. |
| **user unlock <username>** | Removes a lock on logins for a user caused by exceeding the maximum failed logins |
| **passwd [<username>]** | Changes your password or another users password: follow the instructions.<br>The username is optional: it allows an admin to reset another user's password. If executed with no argument, the command changes the current user's (your) password. Authentication of the current user is required. |
| **user expire <username>** | Forces a user to configure a new password on next login.<br>Note: this command does not apply to user type " api" , their passwords do expire over time, but they cannot be forced to change their password via this command. |
| **user host <username> add\|del <hostname>**<br><br>**user host bob add 192.168.1.3** | Restricts remote access for a user from hosts in an allowed list given as domain names or IP addresses.<br>Note: The **user info** command displays the current list of allowed hosts (if any) – see above<br><br>Adds 192.168.1.3 to the list of acceptable source addresses for remote hosts when bob tries to log in |

| Command/Examples | Description/Notes |
|---|---|
| **user duty <username> <duty hours>**<br>**user duty <username> none** | Restricts the duty hours of a user<br>The duty hours parameter is used to indicate the times at which a user can access the system. The format is a list of day/time-range entries. Days are a sequence of two-character representations: Mo, Tu, We, Th, Fr, Sa, Su. All weekdays (days excluding Saturday and Sunday) are represented by Wk, the weekend days by Wd and all days in the week by Al. Note that repeated days are unset MoMo = no day, and MoWk = all weekdays except Monday.<br>A day/time-range prefixed with a '!' indicates " anything but" e.g. !MoTu means anything but Monday and Tuesday.<br>The time-range is two 24-hour times HHMM, separated by a hyphen '-', to indicate the start and finish time. A finish time is earlier than the start time indicates that the duty continues into the next day.<br>Multiple rules can be combined with the '|' symbol to mean 'or' e.g. MoTu1200-1400\|We1400-1500 means Monday or Tuesday between 1200 and 1400 or Wednesday between 1400-1500. |
| **user duty bob Wk0900-1700\|Sa1200-1300** | Allows bob access during office hours (9 to 5) on weekdays and between 1200 and 1300 on a Saturday |

## 9.1 Password Rules

Passwords can be enforced in two ways:

- To prevent weak passwords you can upload a dictionary against which each new password will be checked. If the new password matches an entry in the dictionary it will be rejected:
    - The dictionary must be a text file called dictionary with one word or phrase to each line
    - Each line must end with a single line-feed character rather than the Windows carriage-return line-feed sequence
    - Upload the dictionary using SFTP to enable the checking e.g.

```
sftp>put passwordlist.txt dictionary
```

- There are a number of commands which enforce more secure password usage. All these all commands require admin level access.

CAUTION: Passwords expire after 6 months.

CAUTION: Do not reuse your admin credentials for any other configuration. For example, your TURN server username and password must be unique.

| Command/Examples | Description/Notes |
|---|---|
| **user rule max_history <number>** | Prevents password reuse by checking new passwords against that user's previous number of passwords |
| **user rule password_age <number>** | Enforces a maximum age for passwords in days |
| **user rule min_password_age <number>** | Prevents the password history controls being circumvented, by setting a minimum interval before a password can be reset.<br>Note: This interval is overridden when an admin enters the " user expire <username>" command. |
| **user rule min_length <number>** | Sets the minimum password length |
| **user rule min_special <number>** | Sets the minimum number of " special" characters: !@#$%^&*()_ +=?><,." \/ |
| **user rule min_uppercase <number>** | Sets the minimum uppercase letters in a password |
| **user rule min_lowercase <number>** | Sets the minimum lowercase letters in a password |
| **user rule longest_digits_run <number>** | Sets the maximum consecutive digits allowed in a password |
| **user rule min_digits <number>** | Sets the minimum number of digits in a password |
| **user rule max_repeated_char <number>** | Sets the maximum run of a repeated character |
| **user rule min_changed_ characters <number>** | Sets the minimum number of character positions in the new password which must differ from the old |
| **user rule only_ascii <true\|false>** | Restricts passwords to ASCII characters |
| **user rule no_username <true\|false>** | Prevents a password being set that contains the user name. |
| **user rule no_palindrome <true\|false>** | Prevents a password being set that is a palindrome |

| Command/Examples | Description/Notes |
|---|---|
| **user rule max_failed_logins <attempts>** | Sets the number of failed logins allowed, before a 15 minute lockout for MMP users or Cisco Meeting App users that authenticate via LDAP. Guest access to meetings held on the Meeting Server are unaffected. If set to 0, this rule will lock out users with valid credentials.<br><br>Note that the Call Bridge needs to be restarted for **user rule max_failed_logins <attempts>** to take effect. Changes are immediately applied to MMP users.<br><br>Locked MMP users can be unlocked by an MMP admin, but it is not possible to unlock an LDAP user before the lockout timer expires.<br><br>If no maximum number of failed logins is configured, then the lockout mechanism is disabled for MMP users, but it defaults to 20 failed login attempts for users that authenticate via LDAP. |
| **user rule max_idle <number>** | Sets the maximum number of days that an account can be idle before it is locked. The minimum value is 1.<br><br>Note: if no idle time is configured, then none is enforced. |
| **user rule max_sessions <number>** | Limits any user to <number> of simultaneous SSH or SFTP or Web Admin sessions.<br>For example, if the maximum number of sessions is configured as 5 then you can have 5 SSH, or 5 web admin, or 5 SFTP sessions simultaneously. |
| **user rule max_sessions none** | Removes session restrictions |

## 9.2 Common Access Card (CAC) Integration

The Common Access Card (CAC) is used as an authentication token to access computer facilities. The CAC contains a private key which cannot be extracted but can be used by on-card cryptographic hardware to prove the identity of the card holder. The Meeting Server supports administrative logins to the SSH and Web Admin Interface using CAC.

| Command/Examples | Description/Notes |
|---|---|
| **cac**<br>**cac enable\|disable**<br>**cac enable strict** | Lists current configuration<br>To enable CAC logins, execute cac enable<br>To make this the only allowed remote login method (excluding using the recovery button), use cac enable strict. This command disables normal logins using a serial cable.<br>Before enabling CAC logins, checks are made to ensure that the service has been configured. We recommend using cac enable without specifying "strict" to test whether the setup is correct before turning off password logins with the " strict" option.<br>NOTE: The extension of certificate based access to client logins is a beta feature, only use in a test environment, do not use in a production environment.<br>NOTE:<br>- if cac is enabled, then it is possible to use certificate based logins from suitable clients. Users connecting in this manner will not have to enter a password to access the system.<br>- if cac enable strict has been applied, then users will need to login via CAC before they are able to log in to the Cisco Meeting App. |
| **cac issuer <issuer cert-bundle>** | To validate CAC users, an issuer certificate bundle needs to be uploaded to the MMP using SFTP. Legitimate credentials will have been cryptographically signed by one of the issuer certificates; if not, then the login will fail. Contact your site cryptography officer for more information |
| **cac ocsp enable\|disable** | Online Certificate Status Protocol (OCSP) is a mechanism for checking the validity and revocation status of certificates. The MMP can use this to work out whether the CAC used for a login is valid and, in particular, has not been revoked.<br>If the MMP is configured to be in " strict" CAC mode (no password logins allowed – see above), then access to the MMP can be restricted centrally by revoking certificates.<br>OCSP can be enabled without special configuration. In this mode, the URL of the OCSP responder will be read from the CAC credentials presented to the MMP if present. If an OCSP responder is not present, or the OCSP responder is not available (is down, can't be routed to, etc.), then CAC logins fail. |
| **cac ocsp responder <URL\|none>** | To configure a URL for an OCSP responder, use this command. This URL will override any provided by the CAC. |
| **cac ocsp certs <key-file> <crt-file>** | Some OCSP responders require OCSP requests to be signed by the requestor. This command specifies a private key and (matching) public certificate for this operation:<br>It is likely that the OCSP responder will require that the signing certificate is signed by a particular authority, perhaps the issuer of the CAC certificates. This is a site-local consideration. |
| **cac ocsp certs none** | Removes the certificate configuration |

### 9.2.1 SSH login configuration

SSH login using CAC requires extra configuration steps because X509-based public key exchange is not widely supported by SSH clients. The public X509 certificate from the CAC needs to be extracted and uploaded by SFTP to the MMP as an SSH public key. There are various methods to get the public X509 certificate from the CAC; one of the easiest is to use a CAC-enabled web browser to export the key:

#### Firefox and Chrome:

In a Firefox or Chrome browser enter a url similar to https://ca.cern.ch/ca/Help/?kbid=040111. Follow the instructions to export the credentials.

After export, upload the pkcs#12 file to <username>.pub MMP using SFTP, where <username> is the username of the associated user. Then execute the following command as explained above:

```
pki pkcs12-to-ssh <username>
```

Internet Explorer:

IE can export the CAC (public) credentials as X509 encoded as DER, which can be uploaded and used without further steps (cf. pkcs#12)

## 9.3 Key-based SSH login

It is possible to install an SSH public key on Meeting Server so that SSH logins bypass password authentication if the key-based authentication is successful.

Summary steps:

1. Name your public key **<username>.pub** (where **<username>** is an existing Meeting Server MMP user who you wish to grant key based login to).
2. sftp the **<username>.pub** key to the **<CMS mmp address>**
3. Try to ssh **<username>@<CMS mmp address>** (it may ask you for a password first time, but shouldn't need a password for subsequent logins).

## 9.4 SSH fingerprint verification

To verify the keys prompted by the Meeting Server against the retrieved keys, use the MMP command, **ssh server_key list.**

The output displays a list of keys along with the size, type, and fingerprints for all existing keys in the Meeting Server host, among the following keys:

- ssh_host_dsa_key.pub
- ssh_host_ecdsa_key.pub
- ssh_host_ed25519_key.pub
- ssh_host_key.pub
- ssh_host_rsa_key.pub

.

# 10 Application Configuration Commands

## 10.1 Web Bridge 3 Commands

Follow the instructions in the Deployment Guides to set up the Web Bridge 3. This section provides a command reference only.

Note: " Call Bridge to Web Bridge" protocol (C2W) is the link between the callbridge and webbridge3.

The MMP commands to deploy Web Bridge 3 to use Cisco Meeting Server web app – the new browser-based client for Cisco Meeting Server that lets users join meetings (audio and video) – are listed in the table below.

| Command | Description |
|---|---|
| **webbridge3** | Displays the current set of values for Web Bridge 3 |
| **help webbridge3** | Displays help with all the webbridge3 subcommands |
| **webbridge3 restart** | Restarts the Web Bridge 3 |
| **webbridge3 (enable\|disable)** | Enables or disables the Web Bridge 3 |
| **webbridge3 https listen <*interface*:port allowed list>** | Sets up the interface(s) and port(s) for the Web Bridge 3 to listen on. Enable the service to start listening with the command **webbridge3 enable**. There is no default value for the port; it needs to be specified. |
| **webbridge3 https certs <key-file> <crt-fullchain-file>** | Sets the HTTPS certificates for the Web Bridge 3. These are the certificates that will be presented to web browsers so they need to be signed by a certification authority (CA) and the hostname/purpose etc needs to match. (The certificate file is the full chain of certificates that starts with the end entity certificate and finishes with the root certificate.) |
| **webbridge3 https certs none** | Removes HTTPS certificate configuration |

| Command | Description |
|---|---|
| **webbridge3 https frame-ancestors <frame-ancestors space-separated string>**<br>**webbridge3 https frame-ancestors none**<br>**webbridge3 https frame-ancestors https://*.example.com https://customdomain.example2.com:8000** | Allows administrators to specify a custom frame-ancestors value to be returned in the **content-security-policy** header allowing the web app to be embedded in other web pages.<br>In a cluster setup, this command must be configured on all Web Bridges in the deployment.<br>Added from version 3.2. |
| **webbridge3 http-redirect (enable [port]\|disable)** | (Optional) Enables/disables HTTP redirects by setting up a port for HTTP connections. This port will be opened for all Meeting Server interfaces on which the web app has been configured. Incoming HTTP connections will be automatically redirected to the matching HTTPS port for the interface they arrived on. The default port, if you don't specify one in **webbridge3 http-redirect enable [port]**, is 80. |
| **webbridge3 c2w listen <*interface*:port allowed list>** | Configures the C2W connection. Sets up the interface(s) and port(s) for the Web Bridge 3 to listen on. You must enable the service to start listening with the command **webbridge3 enable**. We recommend that you make this address/port accessible from the Call Bridge(s) only. |
| **webbridge3 c2w certs <key-file> <crt-fullchain-file>** | Configures the C2W connection certificates – you need to configure the SSL Server certificates used for the C2W connection. The C2W certificate is only presented to Call Bridges connecting to the C2W protocol connection port – the hostname/purpose etc needs to match. (The certificate file is the full chain of certificates that starts with the end entity certificate and finishes with the root certificate.) |
| **webbridge3 c2w certs none** | Removes C2W connection certificate configuration. |
| **webbridge3 c2w trust <crt-bundle>** | Sets the trust bundle that Web Bridge 3 C2W server will verify the Call Bridge client certificate against to determine whether to trust them or not. |
| **webbridge3 c2w trust none** | Removes C2W connection trust bundle configuration. |
| | |

| Command | Description |
|---|---|
| **webbridge3 options <space-separated options>** | Switches on the specified features, if more than one feature is to be enabled then separate the feature_ names with a space. Only use this command under instruction from Cisco Support or Cisco EFT. These features are not suitable for production use. The features will remain enabled across reboots, but will be automatically cleared when using the upgrade command. (This command is currently not supported.) |
| **webbridge3 options none** | Switches off all features that were previously switched on using the webbridge options <feature_ name> command. Only use under instruction from Cisco Support. (This command is currently not supported.) |
| **webbridge3 status** | Displays the current configuration for Web Bridge 3 |

## 10.2 TURN Server Commands

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

Note: The TURN Server component is not available on the Cisco Meeting Server 2000.

Note: The TURN server component always supports the standard port 3478 for UDP. When deploying Cisco Meeting Server web edge, the API node **/turnServers** " type" parameter should be set to " cms" . If this parameter is unset, it defaults to " standard" , and tells the clients to use TCP/UDP port 443 to connect to the TURN server. For more information on the " type" parameter values, see the section *Setting up and modifying TURN servers* in Cisco Meeting Server API Reference Guide.

Setting up a TURN server is described in the Deployment Guides. This section provides a command reference.

| Command/Examples | Description/Notes |
|---|---|
| **turn restart** | Restarts the TURN server. |
| **turn listen <interface allowed list\|none>**<br>**turn listen a b** | Sets up an allowed list of interfaces to listen on. To start listening, you must enable the service with the command turn enable. |

| Command/Examples | Description/Notes |
|---|---|
| **turn listen none** | Stops the TURN server listening. |
| **turn tls <port\|none>** | Sets an additional port to be used for TURN, and enables TCP usage for TURN.<br>Note: Set TURN to listen for TCP traffic as well as UDP, on the port specified as well as port 3478, for all three services. This option MUST be set for TURN to listen on any service beside UDP, and for TURN to listen on any port beside 3478. |
| **turn certs <keyfile> <certificate file> [<cert-bundle>]**<br><br>**turn certs none** | Defines the name of the private key file and .crt file for the Turn Server application and, optionally, a CA certificate bundle as provided by your CA. (Also see the section Provisioning with Certificates.)<br>This option is required if 'turn tls <port>' is in use.<br>Removes certificate configuration. |
| **turn (enable\|disable)** | Enables or disables the TURN server. |
| **turn credentials <username> <password> <realm>**<br>**turn credentials myusername mypassword example.com** | Sets the long term credentials for the TURN server. |
| **turn public-ip <public ip>**<br>**turn delete public-ip** | Sets up a public IP address for the TURN server.<br>Deletes the TURN server public IP address. |
| **turn high-capacity-mode (enable\|disable)** | Implements support for increased web app scale (default enable) on the Meeting Server running TURN and web app – it allows higher packet throughput when using Meeting Server for web edge. Only disable if advised to do so by Cisco Support. (from version 3.1) |
| **turn short_term_credentials_mode (enable\|disable)** | Toggles the TURN server between short- and long-term credential mode. Default is **disable**. (from version 3.1) |
| **turn short_term_credentials <shared secret> <realm>**<br>**turn short_term_credentials mysharedsecret example.com** | Specifies the shared secret and realm required by the TURN server to use short-term credentials. (from version 3.1) |

## 10.3 Web Admin Interface Commands

Note: Port 8081 is reserved on loopback if the webadmin is enabled, but is not reserved if the webadmin is disabled. Port 8080 is always open.

| Command/Examples | Description/Notes |
|---|---|
| **webadmin** | Displays the configuration |
| **webadmin restart** | Restarts the Web Admin Interface |
| **webadmin listen (a\|b\|c\|d) [<port>]**<br>**webadmin listen a**<br>**webadmin listen a 443** | Sets up the interface for the Web Admin Interface to listen on. To start listening, you must enable the service with the command **webadmin enable**.<br>The default is port 443. |
| **webadmin listen none** | Stops the Web Admin Interface listening. |
| **webadmin (enable\|disable)** | Enables or disables the Web Admin Interface. When enabling some checks are performed before launching the service: that listening interfaces are configured, that the certificates match and that ports do not clash with other services. |
| **webadmin certs <keyfile-name> <crt filename> [<crt-bundle>]**<br><br>**webadmin certs none** | Provides the name of the key file and .crt file for the Web Admin Interface and, optionally, a CA certificate bundle as provided by your CA<br><br>Removes certificate configuration |
| **webadmin http-redirect (enable\|disable)** | Enables/disables HTTP redirects for the Web Admin Interface |
| **webadmin status** | Displays the Web Admin Interface status |

Note: MMP user accounts are also used to log in to the Web Admin Interface.

## 10.4 Database Clustering Commands

These database clustering commands are explained in the Scalability & Resilience Deployment Guide and Certificate Guidelines.

From version 2.7, database clusters require client and server certificates signed by the same CA configured in each Meeting Server holding or connecting to a database in the cluster. Enforcing the use of certificates ensures both confidentiality and authentication across the cluster.

CAUTION: If a database cluster was configured without certificates using an earlier version of Meeting Server software which did not require certificates, then on upgrading to version 2.7 the database will stop and remain unreachable until certificates are configured and the database cluster is recreated.

Note: <*ca_crt*> is the database cluster CA certificate bundle. This is also used as a trust store, so database connections that give a valid certificate name and a certificate chain that ends with a root certificate present in the bundle will be accepted.

| Command/Examples | Description/Notes |
|---|---|
| **database cluster status** | Displays the clustering status, from the perspective of this database instance.<br>Note: From 2.7 this command will highlight the lack of configured certificates. |
| **database cluster localnode <interface>** | This command must be run on the server that will host the initial primary database before initialising a new database cluster.<br>The <interface> can be in the following formats:<br>[a\|b\|c\|d] - the name of the interface (the first IPv6 address is preferred, otherwise the first IPv4 address is chosen) e.g. database cluster localnode a<br>ipv4:[a\|b\|c\|d] - the name of the interface, restricted to IPv4 (the first IPv4 address is chosen) e.g. database cluster localnode ipv4:a<br>ipv6:[a\|b\|c\|d] - the name of the interface restricted to IPv6 (the first IPv6 address is chosen) e.g. database cluster localnode ipv6:a<br><ipaddress> - a specific IP address, can be IPv4 or IPv6 e.g. database cluster localnode 10.1.3.9 |
| **database cluster initialize** | Creates a new database cluster, with this server's current database contents as the one and only database instance—the primary.<br>The command reconfigures postgres to cluster mode - i.e. listens on external interface and uses SSL<br>Reconfigures and restarts the local Call Bridge (if it is enabled) to use the database cluster.<br>Note: From 2.7 this command will not run without valid certificates, keys and CA certificates uploaded to the database clients and servers. |

| Command/Examples | Description/Notes |
|---|---|
| **database cluster join <hostname/IP address>** | Creates a new database instance as part of the cluster copying the contents of the primary database to this server and destroying the current contents of any database on it.<br><hostname/ip address> can be for any existing database in the cluster.<br>Reconfigures and restarts the local Call Bridge (if it exists and it is enabled) to use the database cluster<br>**Note:** From 2.7 this command will not run without valid certificates, keys and CA certificates uploaded to the database clients and servers. |
| **database cluster connect <hostname/IP address>** | Connects a Call Bridge to a database cluster.<br>Reconfigures and restarts the Call Bridge (if it is enabled) to use the database cluster. Disables the use of any local database (on the same host server as the Call Bridge), although the database content is preserved and can be read after a database cluster remove command is run on this host server (see below).<br>**Note:** From 2.7 this command will not run without valid certificates, keys and CA certificates uploaded to the database clients and servers. |
| **database cluster certs <server_key> <server_crt> <client_key> <client_ crt> <ca_crt>**<br>**database cluster certs dbcluster_ server.key dbcluster_server.crt dbcluster_client.key dbcluster_client.crt dbcluster_ca.crt** | Configures the certificates used to secure the connections in a database cluster.<br>Certificates must be configured before the database cluster can be enabled. |
| **database cluster certs <client_key> <client_crt> <ca_crt>**<br>**database cluster certs dbcluster_ client.key dbcluster_client.crt dbcluster_ca.crt** | Configures the certificates used to secure the connections in a database cluster where there is no co-located database on the Call Bridge. |
| **database cluster certs none** | Removes certificate configuration. Certificates will need to be configured again before the database cluster can be re-enabled. |

| Command/Examples | Description/Notes |
|---|---|
| **database cluster remove** | Removes one database from the cluster if run on a database host server, "un-connects" a Call Bridge if run on a host server with only a Call Bridge, or both if the server hosts both a clustered database and a Call Bridge. |
| **database cluster upgrade_schema** | Upgrades the database schema version in the cluster to the version this node expects. We recommend that you run this command:<br>• on the primary database, but it can be run on any database instance<br>• after every software upgrade on any server hosting a database instance or Call Bridge |
| **database cluster clear_error** | When a previous operation such as a schema upgrade failed (see the previous command), this command manually resets the state. This command should only be run when instructed to do so by Cisco support. |

## 10.5 Uploader Commands

Note: The Uploader is not available on the Cisco Meeting Server 2000.

Uploader simplifies using Vbrick Rev for video content management. This section provides a command reference for the Uploader.

| Commands | Description |
|---|---|
| **uploader (enable\|disable)** | Enables or disables the uploader component. Before configuring the Uploader, ensure the component is disabled. |
| **uploader nfs <host-name/IP>:<directory>** | Specify the NFS that the Uploader will monitor. |
| **uploader (cms\|rev) host <host-name>** | Configure the Uploader with the name of the host for the Meeting Server (cms) and the host for the Vbrick Rev server. Default port is 443. |
| **uploader (cms\|rev) port <port>** | Configure the Uploader with the port to use to connect to the Meeting Server (cms) and the port for the Vbrick Rev server. Default port is 443. |
| **uploader (cms\|rev) user <user-name>** | Configure the Uploader with the user that has access to the API of the Meeting Server and the user with access to the Vbrick Rev server. |

| Commands | Description |
|---|---|
| **uploader (cms\|rev) password** | Configure the Uploader with the password for the specified Meeting Server user and the Vbrick Rev user. |
| **uploader (cms\|rev) trust (<crt-bundle>\|none)** | Upload the specified certificate bundle to the trust store on the Meeting Server or the Vbrick Rev server. **none** removes the certificate bundle from the specified trust store. Note: the Uploader will not work without a certificate bundle in the Meeting Server trust store and the Vbrick Rev trust store. |
| **uploader edit (<uploader-team name>\|none)** | Not supported in version 2.4.0. |
| **uploader view (<uploader-team name>\|none)** | Not supported in version 2.4.0. |
| **uploader access <Private\|Public\|AllUsers>** | Set access permission to the video recordings |
| **uploader cospace_member_access <view\|edit\|none>** | Allows members of the space to view or edit the video recordings.**none** removes view or edit permissions for members of the space. |
| **uploader recording_owned_by_cospace_owner <true\|false>** | **true** selects the owner of the space as the single owner of these video recordings. |
| **uploader fallback_owner (<username>\|none)** | Use the named user as the fallback owner of the video recordings, if the owner of the space is not listed in VbrickRev.**none** removes the fallback owner. |
| **uploader comments (enable\|disable)** | Enables or disables commenting on video recordings. Default is disabled. |
| **uploader ratings (enable\|disable)** | Enables or disables video recording ratings. Default is disabled. |
| **uploader downloads (enable\|disable)** | Sets the download permission, enables or disables downloading the video recordings. |
| **uploader initial_state (<active\|inactive>)** | Set the initial state of the video recording when first uploaded to Vbrick Rev. Default is active. |
| **uploader delete_after_upload (<true\|false>)** | Selects whether to delete the video recording from the NFS after upload is complete. Default is false. |

Note: The **uploader debug (<true|false>)** command was removed in version 2.4, debugging information is automatically sent to the syslog server.

## 10.6 Recorder Commands

Note: The Recorder is not available on the Cisco Meeting Server 2000.

This section provides a command reference for the Recorder. Follow the instructions in the appropriate deployment guide to deploy the recorder.

| Command/Examples | Description/Notes |
|---|---|
| **recorder restart**<br>**recorder** | Restarts the Recorder<br>Displays the current configuration of the Recorder |
| **recorder sip certs** | Allows you to configure a SIP certificate. (Added from version 3.0.) |
| **recorder sip listen <interface> <tcp-port\|none> <tls-port\|none>** | The SIP recorder/streamer components do not need to listen for https connections, however, they do need to listen for SIP connections. This new MMP command is introduced for setting both TCP and TLS. (Added from version 3.0.) |
| **recorder sip trace <1m\|10m\|30m\|24h\|on\|off>** | Turns on logging of all SIP messages. All SIP messages will be logged on the recorder. Default is " off" . You can enable it permanently with " on" or for a fixed time period. (Added from version 3.0.) |
| **recorder limit <value\|none>** | Sets the recorder limit to allow scalability. This is the limit above which calls are rejected so that call control can fail over to another device. (Added from version 3.0). |
| **recorder (enable\|disable)** | Enables or disables the Recorder |
| **recorder nfs <hostname/IP>:<directory>** | Provides the Recorder with details of the network file server (nfs) and folder to save the recording. |
| **recorder resolution <audio\|720\|1080>** | Sets the resolution that the recorder will record meetings. The default is 720p30. Selecting 1080 allows the recorder to do p30. (From version 2.4.) |

## 10.7 Streamer Commands

**Note:** The Streamer is not available on the Cisco Meeting Server 2000.

This section provides a command reference for the Streamer. Follow the instructions in the appropriate deployment guide to deploy the streamer.

| Command/Examples | Description/Notes |
|---|---|
| **streamer restart**<br>**streamer** | Restarts the Streamer<br>Displays the current configuration of the Streamer |
| **streamer sip certs** | Allows you to configure a SIP certificate. (Added from version 3.0.) |

| Command/Examples | Description/Notes |
|---|---|
| **streamer limit <value\|none>** | Sets the streamer limit to allow scalability. This is the limit above which calls are rejected so that call control can fail over to another device. Added from version 3.0. |
| **streamer sip listen <interface> <tcp-port\|none> <tls-port\|none>** | The SIP recorder/streamer components do not need to listen for https connections, however, they do need to listen for SIP connections. This new MMP command is introduced for setting both TCP and TLS. (Added from version 3.0.) |
| **streamer (enable\|disable)** | Enables or disables the Streamer. You need to disable the Streamer before configuring it. After configuration, you need to enable the Streamer. |

# 11 Miscellaneous Commands

## 11.1 Model

| Command/Examples | Description/Notes |
|---|---|
| `model` | Displays the Cisco Meeting Server deployment model.<br><br>Virtualized deployments show as CMS VM |

## 11.2 Meeting Server's Serial Number

| Command/Examples | Description/Notes |
|---|---|
| `serial` | Displays the serial number of the Meeting Server.<br>Note that this command does not apply to the virtualized deployment. |

## 11.3 Message of the Day

MMP users with admin rights can issue the commands in this section.

Note: `motd` commands are only supported on Meeting App versions prior to version 1.9.

| Command/Examples | Description/Notes |
|---|---|
| `motd` | Displays the current message of the day, if any. |
| `motd add "<message text>"` | Displays a banner with <message> after login<br>Alternatively, a message no larger than 2048 characters can be configured by copying a file by SFTP to " motd" . |
| `motd del` | Removes the message of the day. |

## 11.4 Pre-login Legal Warning Banner

If your organization requires a legal warning prior to login, MMP users with admin rights can use the following commands:

| Command/Examples | Description/Notes |
|---|---|
| `login_warning` | Displays the current login warning message, if any. |

| Command/Examples | Description/Notes |
|---|---|
| `login_warning add "<message>"` | Displays a legal warning prior to login<br>Alternatively, a message no larger than 2048 characters can be configured by copying a file by SFTP to " login_warning" . |
| `login_warning del` | Deletes the legal warning |

## 11.5 SNMP Commands

**Note:** Meeting Server 2000 does not support SNMP, therefore the `snmp` commands will not be available.

### 11.5.1 General information

MIBs can be downloaded from any Cisco Meeting Server using SFTP.

For a virtualized deployment (Cisco Meeting Server 1000, or specification based VM server) the MIB files are:

- ACANO-MIB.txt
- ACANO-SYSLOG-MIB.txt

Place these files on your SNMP implementation's search path Te.g. ~/.snmp/mibs for Net-SNMP.

**Note:** The MIBs will be renamed in a future release to reflect the rebranding to Cisco Meeting Server.

The MMP interface only provides a minimal amount of user configuration options. To handle more complex requirements, use the MMP interface to create an initial user and then manage the user database directly - for example with snmpusm from the Net-SNMP package.

The Meeting Server supports both SNMP versions 1/2c and 3: the configuration is different for each. Be aware of the security implications of using SNMP version 1/2c: it does not support robust authentication and therefore anyone who knows the community string can query the server.

### 11.5.2 SNMP v1/2c commands

Access control for v1/2c is based on " communities" . These can be created via the MMP interface when SNMP is disabled.

| Command/Examples | Description/Notes |
|---|---|
| **snmp community add <name> [IP address/prefix]**<br>**snmp community del <name>** | Access control for v1/2c is based on " communities" . These can be created and deleted via the MMP when SNMP is disabled.<br>Note: Only use alphanumeric and underscore in the SNMP community name, other " special" characters, including dash, will return an error message. |
| **snmp community add public** | Allows access to the complete tree from anywhere using the community string " public" . |
| **snmp community add local 10.1.0.0/16** | Allows access but only from the specified subnet. |
| **snmp (enable\|disable)** | Enables/disables SNMP v1/2c |

### 11.5.3 SNMP v3 commands

Access control for v3 is based on users. These can be created from the MMP interface.

| Command/Examples | Description/Notes |
|---|---|
| **snmp user add <name> <password> (MD5\|SHA) (DES\|AES)** | Access control for v3 is based on users.<br>Creates a user with the specified password, using the " MD5" algorithm for authentication and the " DES" algorithm for encryption, with access to the complete tree.<br>Note: Only use alphanumeric and underscore in the SNMP user name, other " special" characters, including dash, will return an error message. |
| **snmp user del <name>** | Deletes an SNMP user. |
| **snmp (enable\|disable)** | Enables/disable SNMP v3. |

### 11.5.4 SNMP trap receiver configuration

| Command/Examples | Description/Notes |
|---|---|
| **snmp trap enable <hostname> <agent community string>**<br>**snmp trap disable**<br>**snmp trap enable mybox public** | Configures an SNMP trap receiver.<br><hostname> is the hostname of machine that will receive traps, and <community string> is the community string that will be used |

## 11.6 Downloading the System Logs

The system log is 100MB maximum. When this limit is reached, the oldest messages are discarded to make room for new ones. An SNMP trap is generated when the log reaches 75%

of capacity.

If log data must be retained for compliance or other reasons, and a remote syslog server is not in use, you can:

- Connect to the MMP using a SFTP tool and copy the system log file off the server to a local file store. This leaves the current contents intact
- Save the log file permanently using the **`syslog rotate <filename>`** command. The active system log is then emptied. This saved file can be downloaded using SFTP

  For example: **`syslog rotate mylog`**
- A user with the audit role can save the audit log with **`syslog audit rotate <filename>`**

## 11.7 Generating and downloading the Log Bundle

From version 2.2, the Meeting Server can produce a log bundle containing the configuration and state of various components in the Meeting Server. This log bundle includes the syslog and live.json files, the files will aid Cisco Support speed up their analysis of your issue.

If you need to contact Cisco support with an issue, follow these steps to download the log bundle from the Meeting Server.

1. Connect your SFTP client to the IP address of the MMP.
2. Log in using the credentials of an MMP admin user.
3. Copy the file logbundle.tar.gz to a local folder.
4. Rename the file, changing the logbundle part of the filename to identify which server produced the file. This is important in a multi-server deployment.
5. Send the renamed file to your Cisco Support contact for analysis.

Initial file size of the log bundle.tar.gz is 1 Kb, after transfer via SFTP the size will increase depending on the number of files and their size.

---

Note: In the event that you are not able to download the logbundle due to a slow network connection between a computer and the Meeting Server, you can download the log and live.json files to send to Cisco Support.

---

## 11.8 Disk Space Usage

| Command/Examples | Description/Notes |
|---|---|
| **`df`** | Displays disk usage for both the MMP and MODULE 0 as the percentage usage per partition and the percentage inode usage. |

## 11.9 Backup and Restore System Configuration

Note: Backup commands are also available on the virtualized solution.

| Command/Examples | Description/Notes |
|---|---|
| **backup list** | Displays a list of any backup files on the server. |
| **backup snapshot <name>** | Creates a full Meeting Server snapshot. A file <name>.bak is created for download over SFTP. We strongly recommend using this command regularly.<br><br>Note: The backup files will not contain SSO files and locally hosted branding files. |
| **backup rollback <name>** | Restores the system for the backed up server, this involves rolling back the configuration for the server. If not already on the Meeting Server the backup file must be uploaded to the Meeting Server using SFTP prior to running this rollback command.<br>Note: This command overwrites the existing configuration as well as the license.dat file and all certificates and private keys on the system and reboots the Meeting Server. Therefore it should be used with caution. If you restore this backup to another server, you must copy your existing license.dat file and certificates beforehand because they will be overwritten during the backup rollback process. The license.dat file is keyed to the servers MAC address so will fail when restored from a backup from another server and will need to be replaced after the server is back online. |

## 11.10 Upgrading the Meeting Server

| Command/Examples | Description/Notes |
|---|---|
| **upgrade [<filename>]** | Upgrades the Meeting Server. You must have uploaded the image file of the version that you want to upgrade to before issuing this command.<br>When upgrading, a full system backup is created automatically. The backup name is derived from the current software version. For example, if the upgrade is from R2.9 to R3.0, the backup will be called 2_9.bak.<br>The default filename if one is not provided is upgrade.img<br>From version 3.0 this command performs signature and integrity checks before proceeding with upgrading Meeting Server with the specified image. The checks will be carried out even if the **upgrade <name> verify** command has been previously run on that image. Updated from version 3.0. |

| Command/Examples | Description/Notes |
|---|---|
| `upgrade <filename> [no-backup]` | Use with caution. |
| `upgrade list` | To get a list of the upgrade images on the system |
| `upgrade delete <name>`<br>`upgrade delete upgrade.img` | Upgrade images persist until they are deleted using SFTP or this CLI command |
| `upgrade <filename> verify` | Carries out all the integrity and signature checks normally done during upgrade, but does not proceed with the upgrade. This command can also be used to display the image type. Added from version 3.0. |
| `authenticity` | Displays all information relating to software authenticity: how the running image was validated (key type and name), and the public keys currently loaded along with their details (type, name and source). It also displays whether the keys are trusted: if a SPECIAL key is installed, whether its signature has been verified with the MASTER key (other keys are internal and always trusted). Added from version 3.0. |
| `authenticity key add <key-file>` | Installs a SPECIAL key. Only one SPECIAL key may be installed at a time. Added from version 3.0. |
| `authenticity key none` | Removes the SPECIAL key currently installed. This command must be used to remove a key before installing another, or when the key is no longer in use. Added from version 3.0. |

## 11.11 Resetting the Meeting Server

| Command/Examples | Description/Notes |
|---|---|
| `factory_reset (full\|app)` | The " full" option removes all user configuration: any credentials installed on the system will be lost. Afterwards, you must deploy the Meeting Server again following the instructions mentioned in the Installation guide.<br>The " app" option removes Active Directory sync data and space (coSpace), Lync and SIP configuration; but MMP configuration remains. After the command completes, the system will reboot. |

# Appendix A Version 3.0 MMP command removal

All MMP commands associated with the features and components that removed from Meeting Server in 3.0 removed as follows:

- H.323 gateway commands (**h323_gateway**)
- Web Bridge 2 commands (**webbridge**)
- XMPP server commands (**xmpp**)
- XMPP multi-domains commands (**xmpp multi_domain**)
- XMPP resiliency commands (**xmpp cluster**)
- Load Balancer commands (**loadbalancer**)
- Trunk commands (**trunk**)
- SIP edge commands (**sipedge** and edge-related **callbridge**)
- Recorder and Streamer commands dependent upon XMPP
- MMP commands applicable to X-series server

Table 1: Removed commands for configuring the Meeting Server

| Command/Examples | Description/Notes |
|---|---|
| **health** | Displays temperatures, voltages and other health information about the Meeting Server.<br>Note: The health command is not available on a virtualized deployment. |
| **callbridge trust xmpp <trusted xmpp certificate allowed list** | Configures the Call Bridge to use a particular allowed list of certificates to validate the identity of the XMPP servers. (From version 2.4) |
| **callbridge trust xmpp none** | Removes the XMPP certificate allowed list from the Call Bridge trust store. (From version 2.4) |

Table 2: Removed XMPP server commands

| Command/Examples | Description/Notes |
|---|---|
| **xmpp**<br>**xmpp status** | Displays the current configuration |
| **xmpp restart** | Restarts the XMPP server |
| **xmpp domain <domain-name>** | Creates a component secret for the XMPP server |

| Command/Examples | Description/Notes |
|---|---|
| **xmpp listen <interface allowed list\|none>**<br><br>**xmpp listen a b**<br>**xmpp listen none** | Sets up an allowed list of interfaces to listen on. You must enable the service in order to start listening with the command xmpp enable<br>Stops the XMPP server listening |
| **xmpp (enable\|disable)** | Enables or disables the XMMP server |
| **xmpp certs <key-file> <crt-file> [<crt-bundle>]**<br><br>**xmpp certs none** | Defines the name of the key file and certificate file for the XMPP server, and optionally, a CA certificate bundle as provided by your CA.<br><br>Removes certificate configuration |
| **xmpp motd add <message>**<br><br>**xmpp motd del** | Configures a " message of the day" which will be displayed when Cisco Meeting App or XMPP clients log in. " "<br><br>Removes the message of the day.<br><br>Alternatively, a message no larger than 2048 characters can be configured by copying a file by SFTP to " xmpp.motd" .<br>Modifying the xmpp.motd in any way causes the XMPP server to restart.<br><br>Note: **motd** commands are only supported on Meeting App versions prior to version 1.9. |
| **xmpp max_sessions <number>**<br><br>**xmpp max_sessions none**<br><br>**xmpp max_sessions 3** | Limits the number of simultaneous XMPP sessions that an individual user can have with the XMPP server (and hence, the number of simultaneous logins). This prevents a single user from exhausting system resources.<br><br>Removes any restriction on the XMPP sessions per user.<br><br>If the expectation is that a user will have at most an iPad, iPhone and PC login, then set the maximum sessions to three. |
| **xmpp callbridge add <component name>**<br><br>**xmpp callbridge del <component name>** | These xmpp callbridge commands are explained in the Scalability & Resilience Deployment Guide<br><br>Configures the XMPP server to allow connections from a new Call Bridge. Note: a secret will be generated, this is required if you set up XMPP resiliency. Now go to the Web Admin Interface on that Call Bridge and configure it to connect to the XMPP server.<br><br>Stops a Call Bridge from accessing the XMPP server. |

| Command/Examples | Description/Notes |
|---|---|
| **xmpp callbridge list** | For each Call Bridge lists the domain, component_secret and connection status |
| **xmpp callbridge add-secret <callbridge>** | Required for XMPP resiliency. Used to add to the other nodes in the XMPP cluster, the secrets generated from connecting the Call Bridges to the first node in the cluster. |
| **xmpp reset** | Returns an XMPP server to a standalone configuration (removes any Call Bridges that have been added). Only use this command if you need to restart configuration. |

Table 3: Removed loadbalancer commands

| Command/Examples | Description/Notes |
|---|---|
| **loadbalancer list [<tag>]** | Lists the all the load balancer configurations or, if tag is provided, just that load balancer's configuration |
| **loadbalancer (enable\|disable) <tag>**<br>**loadbalancer enable exampleEdge** | Enables or disables the load balancer<br>Note that the public port (see below) is not opened until there are trunks to service connections. |
| **loadbalancer create <tag>**<br>**loadbalancer create exampleEdge** | Creates a load balancer |
| **loadbalancer trunk <tag> <iface> [:<port>]**<br>**loadbalancer trunk exampleEdge a:3999**<br>**loadbalancer public <tag> <iface> [:<port allowed list>]**<br>**loadbalancer public exampleEdge b:5222**<br>**loadbalancer public exampleEdge b:5222 lo:5222** | Configures the trunk interface and port<br><br>Configures the public interface and port (for accepting client connections)<br>In a common edge deployment, the Web Bridge is also enabled and needs to make use of a Core to Edge trunk. To allow this, configure the loopback interface as a public interface |
| **loadbalancer auth <tag> <key-file> <cert-file> <trust-bundle>**<br>**loadbalancer auth exampleEdge acano.key acano.crt trust.pem** | Configures the private key and certificate used to authenticate to the trunk, and the trusted certificates which may be presented by the trunk.<br>If a trunk presents any of the certificates in the trust bundle when creating the TLS connection and the trunk accepts the certificate that the load balancer presents, then the connection will succeed. Specifically, if the trust bundle contains a valid chain of certificates, with the presented certificate issued by a CA at the end of the chain, then authentication will succeed. Otherwise, the connection will be rejected. In particular, if self-signed certificates are used, then the public certificate can be put into the trust bundle and authentication will succeed. |
| **loadbalancer delete <tag>** | Deletes the load balancer configuration. |

Table 4: Removed Trunk commands

| Command/Examples | Description/Notes |
|---|---|
| **trunk list [<tag>]** | Lists the all the Core configurations or, if tag is provided, just that Core's configuration |
| **trunk (enable\|disable) <tag>** | Enables or disables the Core |
| **trunk create <tag> <port or service name>**<br>**trunk create trunktoExampleEdge xmpp** | Creates a trunk instance for XMPP. |
| **trunk edge <tag> <edge name\|ip address>[:<port>]** | Configures the domain name or IP address of the Edge to trunk to. Note that the domain name could resolve to multiple IP addresses. In that case, a connection is attempted to all addresses. If no port is specified, it is assumed that the port can be discovered by a DNS SRV lookup of the domain name |
| **trunk auth <tag> <key-file> <cert-file> <trust-bundle>** | Configures the private key and certificate used to authenticate to the Edge server, and the trusted certificates which may be presented by the Edge server. |
| **trunk delete <tag>** | Deletes the Core configuration. |
| **trunk debug <tag>** | This command is only to be used under the guidance of Cisco Support. The diagnostics show:<br>• the DNS results for the Edge server name<br>• attempts to create the TLS connection and authenticate to each address<br>• if successful, debug information from the Core server, including:<br>  • a list of " Core" connections (trunk to Edge server connections) to the Edge server in question<br>  • the client connections currently being serviced by that Edge server<br>  • memory usage statistics for the Edge server |

Table 5: Removed commands for supporting XMPP multi-domains

| Command/Examples | Description/Notes |
|---|---|
| **xmpp multi_domain add <domain name> <key-file> <crt-file> [<crt-bundle>]** | Add another domain that the XMPP server will listen to. Specify the private key, certificate and optional certificate bundle as provided by the CA. Restart the XMPP server for this change to take effect. Note: the XMPP server will not start if the private key or certificate files are missing or invalid. |
| **xmpp multi_domain del <domain name>** | Delete the domain that the XMPP server listens to. |
| **xmpp multi_domain list** | List the domain that the XMPP server listens to. |

Table 6: Removed XMPP resiliency commands

| Command/Examples | Description/Notes |
|---|---|
| **xmpp cluster enable\|disable** | Enables/disables XMPP clustering. Enabling the XMPP cluster must be done before enabling XMPP on a node. If xmpp cluster is disabled and xmpp is started, this will start the xmpp server in standalone mode. |
| **xmpp cluster trust <trustbundle.pem>** | Specifies the bundle of certificates that will be trusted by the xmpp cluster. The <trustbundle.pem> should contain all of the certificates for the xmpp servers in the cluster. The certificates must already have been applied to the xmpp servers using the xmpp certs command. This mechanism ensures that the different xmpp nodes in the cluster trust each other, and enables the failover operation and the forwarding of traffic between nodes. |
| **xmpp cluster status** | Reports the live state of the xmpp cluster. If the cluster has failed, then this command will return the statistics of the xmpp server running on this Meeting Server only. Use this command to try and help diagnose connectivity problems. |
| **xmpp cluster initialize** | Initializes a cluster. This command will create a 1 node live xmpp cluster, you can join other nodes (xmpp servers) to this cluster. |
| **xmpp cluster join <cluster>** | Add this node to the cluster. <cluster> is the IP address of the first node in the cluster (see command xmpp cluster initialize). |
| **xmpp cluster remove** | Remove this node from the cluster. This requires the node to be running. |

| Command/Examples | Description/Notes |
|---|---|
| **xmpp cluster remove <node>** | Removes the specified node from the cluster, where <node> is either the IP address or a domain name for the node. This allows you to remove a node from the cluster if the node is unresponsive. |
| **xmpp callbridge add-secret <callbridge>**<br>**Please enter a secret: <secret>** | Add Call Bridge secret to XMPP server. Used to configure the other nodes with the secrets created when connecting the Call Bridges to the first XMPP server node in the cluster.<br>This command allows a Call Bridge to share credentials with many XMPP servers. |

Table 7: Removed Web Bridge commands (for setting up legacy Web Bridge 2)

| Command/Examples | Description/Notes |
|---|---|
| **webbridge restart** | Restarts the Web Bridge |
| **webbridge status** | Displays the current configuration |
| **webbridge listen <a\|b\|c\|d\|none [:<port>] allowed list>**<br>**webbridge listen a b** | Sets up the interface(s) and port(s) for the Web Bridge to listen on. You must enable the service to start listening with the command webbridge enable. The default for the optional port argument is 443. |
| **webbridge listen none** | Stops the Web Bridge listening. |
| **webbridge (enable\|disable)** | Enables or disables the Web Bridge |
| **webbridge certs <keyfile-name> <crt filename> [<crt-bundle>]** | Provides the name of the key file and .crt file for the Web Bridge and, optionally, a CA certificate bundle as provided by your CA |
| **webbridge certs none** | Removes certificate configuration |
| **webbridge clickonce <url\|none>** | Defines the clickonce link location. The url must be prefixed by http://, https:// or ftp:// and be a valid url. If a user follows a call invite link or coSpace web link (e.g. https://www.join.cisco.com/invited.sf?id=1234) using Internet Explorer (the only browser that we support for clickonce), then we will attempt to redirect the user to the configured clickonce location, rather than using the default. When this redirect occurs, the PC Client starts automatically (or is downloaded if it is not already installed) and the call/coSpace will be dialed. |
| **webbridge clickonce none** | Disables all clickonce redirect behavior |

| Command/Examples | Description/Notes |
|---|---|
| **webbridge msi (<url>\|none)**<br>**webbridge dmg (<url>\|none)**<br>**webbridge ios (<url>\|none)**<br>**webbridge ios none** | Configures the download locations for Windows msi, Mac OSX dmg and iOS installers which are presented to WebRTC users<br>To deconfigure, use the appropriate command with the parameter **none** |
| **webbridge trust <crt-bundle\|crt-file>**<br>**webbridge trust none** | Controls which Call Bridge instances are allowed to configure guest accounts and customizations (like background image). If the trusted Call Bridge is running on the same server as the Web Bridge, then issuing the webbridge trust command with the name of the Call Bridge public certificate/certificate bundle is sufficient. If the Call Bridge is running on another server, the public certificate/certificate bundle of the Call Bridge must first be copied to the Web Bridge server using SFTP.<br>**Note:** In clustered Call Bridge deployments, if the Call Bridges have different certificates then combine the certificates into one bundle. |
| **webbridge trust xmpp <trusted xmpp certificate allowed list>** | Configures the Web Bridge to use a particular allowed list of certificates to validate the identity of the XMPP servers. (From version 2.4) |
| **webbridge trust xmpp none** | Removes the XMPP certificate allowed list from the Web Bridge trust store. (From version 2.4) |
| **webbridge http-redirect (enable\|disable)** | Enables/disables HTTP redirects |
| **webbridge url-redirect (<url>\|none)** | Configures the URL redirect location. To deconfigure, use the command with the parameter **none** |
| **webbridge options <feature_name1 feature_name2>**<br>**webbridge options cma.webrtc.ios** | Switches on the specified features, if more than one feature is to be enabled then separate the feature_names with a space. Only use this command under instruction from Cisco Support or Cisco EFT. These features are not suitable for production use.<br>The features will remain enabled across reboots, but will be automatically cleared when using the upgrade command.<br>(From version 2.5). |
| **webbridge options none** | Switches off all features that were previously switched on using the **webbridge options <feature_name>** command. Only use under instruction from Cisco Support or Cisco EFT. (From version 2.5). |

Table 8: Removed commands to configure the SIP Edge component

| Command/Examples | Description/Notes |
|---|---|
| **callbridge add edge <ip address>:<port>** | Adds the SIP Edge for the Call Bridge to use. |
| **callbridge del edge** | Removes the SIP Edge |
| **callbridge trust edge <certificate file>** | Specify a certificate for the Call Bridge to trust for connections to and from the SIP Edge. This is the certificate of the SIP Edge. |
| **sipedge private <interface>:<port>** | Specify the internal interface and port for connections to and from the Call Bridge |
| **sipedge public <interface>:<port>** | Specify the external interface and port for connections to and from external systems |
| **sipedge public-ip <address>**<br>**sipedge public-ip none** | Configure or remove the NAT address that the SIP Edge can be reached at. |
| **sipedge certs <key-file> <crt-file> <trusted-bundle>** | Configure the private key and certificate for the SIP Edge along with a bundle of trusted certificates for the connection from the Call Bridge |
| **sipedge enable**<br>**sipedge disable** | Enables or disables the SIP Edge component |
| **sipedge restart** | Restarts the SIP Edge component. Use this command after you have changed the certificates on the SIP edge. Do not use this command when important calls are active. |

Table 9: Removed commands to configure the Meeting Server to accept and send H.323 calls

| Command/Examples | Description/Notes |
|---|---|
| **h323_gateway enable/disable/restart** | The gateway will not start unless it is configured properly. |
| **h323_gateway certs <keyfile> <certificate file> [<cert-bundle>]** | Defines the name of the private key file and .crt file for the H.323 Gateway application and, optionally, a CA certificate bundle as provided by your CA. (Also see the section Provisioning with Certificates.) |
| **h323_gateway certs none** | Removes certificate configuration |

| Command/Examples | Description/Notes |
|---|---|
| **h323_gateway h323_nexthop <host/ip>**<br>**h323_gateway del h323_nexthop** | Connect to this IP address for all outgoing H.323 calls and let the device at this IP address handle the routing. If this address is not set, only IP dialing works.<br>Typically this IP address is a Cisco VCS/Polycom DMA, and an H.323 trunk is established between the Cisco Meeting Server H.323 Gateway and the third party device (H.323 Gatekeeper). The H.323 Gateway does not register with the device, just forwards calls to them – the device will need to be configured appropriately to accept these calls. |
| **h323_gateway default_uri <uri>**<br>**h323_gateway del default_uri** | Optional. If an incoming H.323 call has no destination (normally only the case when the H.323 Gateway has been dialed by an IP address) the SIP call is made to whatever default_uri is set. The default_uri may point to an IVR, or directly into a coSpace. If it is not set, the call is rejected. |
| **h323_gateway sip_domain <uri>**<br>**h323_gateway del sip_domain <uri>** | Optional. If an incoming H.323 call is made to the gateway without a domain in the destination address, @<sip_domain> will be appended to the destination address before the SIP call to the Call Bridge is made. |
| **h323_gateway sip_domain_strip <yes/no>** | If set to " yes" and " h323_gateway sip_domain" is set, when a SIP call is made to the gateway the @<sip_domain> will be stripped from the source address (if present) before making the H.323 call. |
| **h323_gateway h323_domain <uri>**<br>**h323_gateway del h323_domain <uri>** | Optional. If an H.323 call is made to the gateway without including a domain in the source address, @<h323_domain> will be appended to the source address before the SIP call is made. |
| **h323_gateway h323_domain_strip <yes/no>** | If set to " yes" and " h323_gateway h323_domain" is set, when a SIP call is made to the gateway the @<h323_domain> will be stripped from the destination address (if present) before making the H.323 call. |
| **h323_gateway h323_interfaces <interface list>**<br>**h323_gateway sip_interfaces <interface list>** | Must be configured in order for gateway to start, but the actual setting is currently ignored. |
| **h323_gateway sip_port <port>** | Ports for the SIP side to listen on. The default is 6061.<br>Note: if you wish to change the default port from 6061, and if the H.323 Gateway and Call Bridge are on the same server, make sure you avoid port 5061 which is used by the Call Bridge.<br>Changes do not take place until the gateway is restarted.<br>The H.323 Gateway always expects TLS connections; therefore, " Encrypted" should be selected on outbound dial plan rules on the Call Bridge |

| Command/Examples | Description/Notes |
|---|---|
| **h323_gateway sip_proxy <uri>** | Set this to the IP address of the Call Bridge, or for multiple Call Bridges use the domain name (through DNS). All incoming H.323 calls will be directed to this uri<br>If the Call Bridge and the H.323 Gateway are on the same host then use IP address 127.0.0.1. If the Call Bridge and the H.323 Gateway are on different hosts then use the IP address of the Call Bridge. |
| **h323_gateway restrict_codecs <yes/no>** | If set to yes, the H.323 Gateway is limited to a safe set of codecs that are less likely to cause interoperability problems. Currently this set is G.711/G.722/G.728/H.261/H.263/ H.263+/H.264.<br>Codecs disabled by this feature are G.722.1 and AAC. |
| **h323_gateway disable_content <yes/no>** | If set to yes, H.239 content is disabled. |
| **h323_gateway trace_level <level>** | Provides additional logging to aid troubleshooting by Cisco support. You may be asked to provide traces for levels 0, 1, 2 or 3. |

Table 10: Removed XMPP recorder commands

| Command | Description |
|---|---|
| **recorder listen <a\|b\|c\|d\|lo\|none [:<port>] allowed list>**<br>**recorder listen a b** | Sets up the interface(s) and port(s) for the Recorder to listen on. You must enable the service to start listening with the command recorder enable. The default for the optional port argument is 443. |
| **recorder listen none** | Stops the Recorder listening. |
| **recorder certs <keyfile-name> <crt filename> [<crt-bundle>]** | Provides the name of the key file and .crt file for the Recorder and, optionally, a CA certificate bundle as provided by your CA |
| **streamer certs none** | Deprecated from version 3.0(Beta2).<br>Removes certificate configuration |
| **recorder certs none** | Removes certificate configuration |

| Command | Description |
|---|---|
| **streamer trust <crt-bundle\|crt-file>** | Controls which Call Bridge instances are allowed to connect to the Recorder.<br>If the trusted Call Bridge is running on the same server as the Recorder, then issuing the recorder trust command with the name of the Call Bridge public certificate/certificate bundle is sufficient. If the Call Bridge is running on another server, the public certificate/certificate bundle of the Call Bridge must first be copied to the server with the enabled Recorder using SFTP. |

Table 11: Removed XMPP streamer commands

| Command | Description |
|---|---|
| **streamer listen <a\|b\|c\|d\|lo\|none [:<port>] allowed list>**<br>**recorder listen a b** | Sets up the interface(s) and port(s) for the Streamer to listen on. You must enable the service to start listening with the command streamer enable. The default for the optional port argument is 443. |
| **streamer certs none** | Removes certificate configuration |
| **streamer certs <keyfile-name> <crt filename> [<crt-bundle>]** | Provides the name of the key file and .crt file for the Streamer and, optionally, a CA certificate bundle as provided by your CA |
| **streamer trust <crt-bundle\|crt-file>** | Controls which Call Bridge instances are allowed to connect to the streamer.<br>If the trusted Call Bridge is running on the same server as the streamer, then issuing the streamer trust command with the name of the Call Bridge public certificate/certificate bundle is sufficient. If the Call Bridge is running on another server, the public certificate/certificate bundle of the Call Bridge must first be copied to the server with the enabled streamer using SFTP. |
| **streamer trust none** | Deconfigures any trust settings. |
| **streamer listen <a\|b\|c\|d\|lo\|none [:<port>] allowed list>**<br>**recorder listen a b** | Sets up the interface(s) and port(s) for the Streamer to listen on. You must enable the service to start listening with the command streamer enable. The default for the optional port argument is 443. |

# 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