Cisco Meeting Server

Cisco Meeting Server Release 2.3

MMP Command Line Reference

January 17, 2018

Contents

Change History 5

1 Introduction 6
- 1.1 How to use this Document 6
- 1.2 Accessing the MMP 8
  - 1.2.1 Virtualized depolyments (Cisco Meeting Server 1000 and specification based VM servers) 8
  - 1.2.2 Acano X-Series Servers 8
- 1.3 Transferring files to and from the MMP 8
  - 1.3.1 Which files you see in the SFTP client 8
- 1.4 What MMP Commands are Available? 9
- 1.5 Writing and Completing MMP Commands 10

2 Network Commands 11
- 2.1 Network Interface (iface) Commands 11
- 2.2 IP Commands 11
  - 2.2.1 IPv4 commands 11
  - 2.2.2 IPv6 commands 12
- 2.3 Network Diagnostic Commands 13
  - 2.3.1 IPv4 network diagnostic commands 14
  - 2.3.2 IPv6 network diagnostic commands 14
  - 2.3.3 Packet capture 14
- 2.4 QoS/DSCP Commands 14

3 DNS Commands 16

4 Firewall Commands 18

5 Provisioning with Certificates 20
- 5.1 TLS Certificate Verification 22

6 Commands for Configuring the Cisco Meeting Server 25
- 6.1 Federal Information Processing Standard 28
- 6.2 MTU for an Interface 28

7 MMP User Account Commands 29
- 7.1 Password Rules 30

7.2 Common Access Card (CAC) Integration 32
7.2.1 SSH login configuration 34

8 Application Configuration Commands 35
8.1 XMPP Server Commands 35
8.2 Commands for the Core to Edge Trunk 36
8.2.1 Load Balancer commands 36
8.2.2 Trunk commands 37
8.3 Supporting XMPP multi-domains 38
8.4 XMPP resiliency commands 39
8.5 Web Bridge Commands 40
8.6 TURN Server Commands 41
8.7 SIP Edge Commands (BETA feature) 42
8.8 Web Admin Interface Commands 43
8.9 Database Clustering Commands 44
8.10 Recorder Commands 46
8.11 Uploader Commands (BETA feature) 47
8.12 Streamer Commands 48

9 H.323 Commands 50

10 Miscellaneous Commands 52
10.1 Model 52
10.2 Meeting Server's Serial Number 52
10.3 Message of the Day 52
10.4 Pre-login Legal Warning Banner 52
10.5 SNMP Commands 53
10.5.1 General information 53
10.5.2 SNMP v1/2c commands 53
10.5.3 SNMP v3 commands 54
10.5.4 SNMP trap receiver configuration 55
10.6 Downloading the System Logs 55
10.7 Downloading the Log Bundle 55
10.8 Disk Space Usage 56
10.9 Backup and Restore System Configuration 56
10.10 Upgrading the Meeting Server 56
10.11 Resetting the Meeting Server 57
10.12 Password Recovery/First Boot for the Acano X-Series Server 57

Cisco Legal Information 59

Cisco Trademark 60

Change History

Date	Change Summary
August 03, 2016	Rebranded for Cisco Meeting Server 2.0
December 20, 2016	Updated for version 2.1, added commands for the Streamer
May 03, 2017	No additions for Cisco Meeting Server 2.2
July, 2017	Change to ciphers supported for tls
August 23, 2017	Miscellaneous corrections
November 01, 2017	Miscellaneous corrections
December 19, 2017	Updated for Cisco Meeting Server 2.3, changed TLS default cipher string and added two new TLS commands.
January 17, 2018	Minor addition regarding HTTPS services in section 5.1

1 Introduction

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

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 Acano X-Series Servers, the MMP can be accessed via the serial Console port or SSH on the Ethernet interface labeled Admin. In virtualized deployments (the Cisco Meeting Server 1000, and specification based VM servers) the MMP is accessed on virtual interface A.

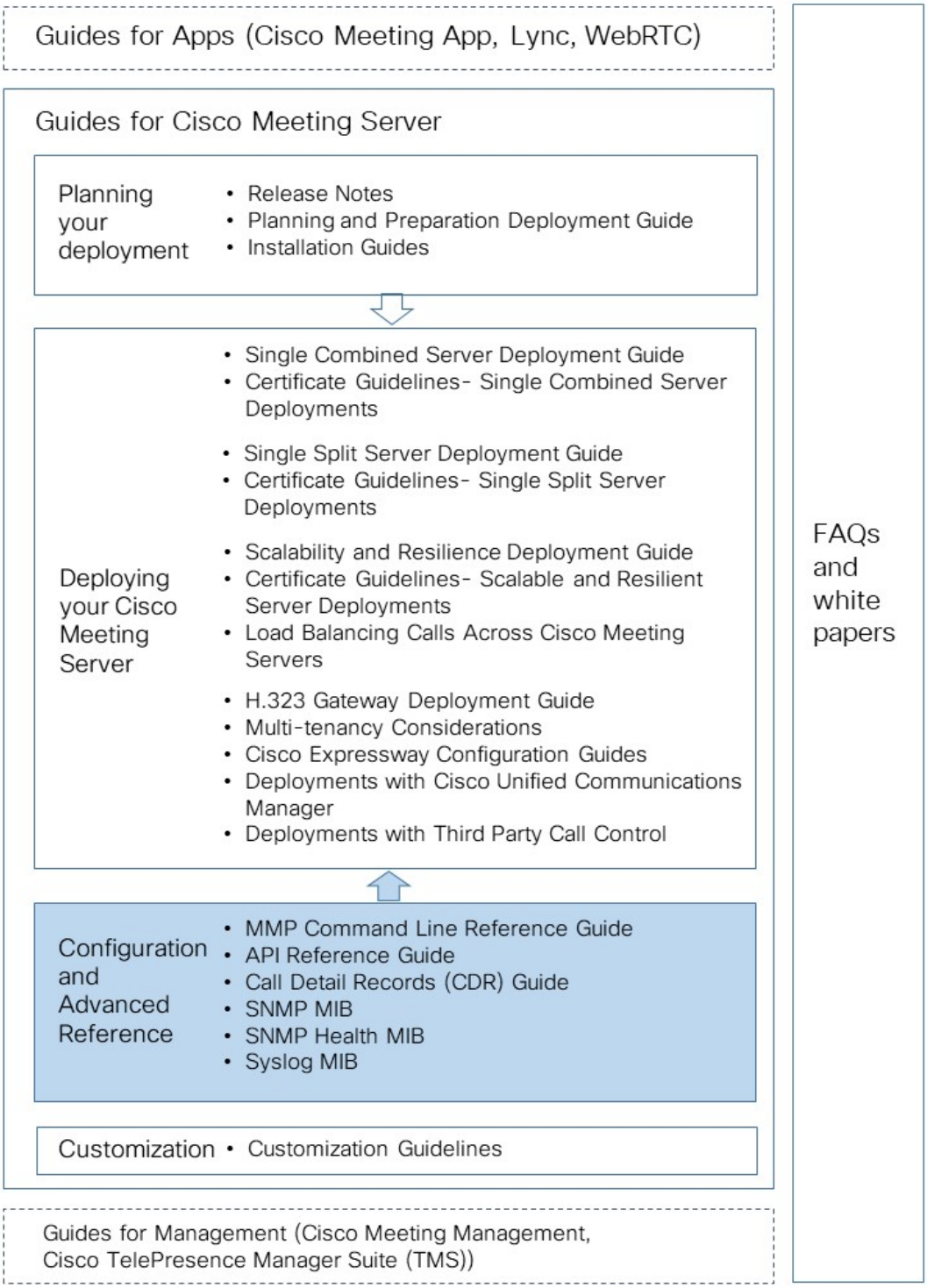
Application level administration (call and media management) is undertaken via the API, or for straightforward deployments, via the Web Admin Interface which can be configured to run on any one of the available Ethernet interfaces.

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 1000, the Acano X-Series Server and virtualized deployments.

Figure 1: Cisco Meeting Server documentation for version 2.1



1.2 Accessing the MMP

1.2.1 Virtualized depolyments (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.

1.2.2 Acano X-Series Servers

On Acano X-Series Servers, the MMP can be accessed via the serial Console port on the server or SSH on the Ethernet interface labeled Admin, which requires an SSH client; no other interfaces can be used. For Windows users puTTy is a popular choice. Access using the Console port does not require SSH; but both methods require 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 Acano X-Series Server Installation Guide.

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 and xmpp.crt
- license.dat (required name)
- boot.json and live.json
- server.key, webbridge.key and xmpp.key
- cacert.pem, privkey.pem, server.pem and xmpp.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 (admin|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 mmp	Displays the network interface configuration
iface (admin|a|b|c|d)	Displays the network interface configuration for the specified interface Sets the MMP properties to 1GE, full duplex
iface (admin|a|b|c|d) <speed> (full|on|off) **iface admin 1000 full**	Sets the network interface speed, duplex and auto-negotiation parameters
iface (admin|a|b|c|d) autoneg (on|off) **iface admin autoneg <on>**	Enables auto negotiation 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

2 Network Commands

2.1 Network Interface (iface) Commands

Command/Examples	Description/Notes
iface mmp	Displays the network interface configuration
iface (admin|a|b|c|d)	Displays the network interface configuration for the specified interface Sets the MMP properties to 1GE, full duplex
iface (admin|a|b|c|d) <speed> (full|on|off) **iface admin 1000 full**	Sets the network interface speed, duplex and auto-negotiation parameters
iface (admin|a|b|c|d) autoneg (on|off) **iface admin autoneg <on>**	Enables auto negotiation Note that the A, B, C and D interfaces are restricted to full duplex auto negotiation.

2.2 IP Commands

2.2.1 IPv4 commands

Note: In the virtualized deployment, there is no admin interface and therefore admin is not a valid entry in the following commands; select from A, B, C or D.

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

Command/Examples	Description/Notes
ipv4 (admin|a|b|c|d) add <server IP address>/<Prefix Length> <Default Gateway> **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 (admin|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 (admin|a|b|c|d) route add <address>/<prefix length> **ipv4 (admin|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 quite specific routing scenarios whereby 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
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.

Note: In the virtualized deployment, there is no admin interface and therefore admin is not a valid entry in the following commands; select from A, B, C or D.

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

Command/Examples	Description/Notes
ipv6 (admin|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 • any advertised prefixes are used to construct global addresses • any RDDNS options are used to configure DNS • 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 If no Router Advertisement is received after three Router Solicitations are sent, then DHCPv6 will start.
ipv6 (admin|a|b|c|d) disable	Disables IPv6 for the specified interface
ipv6 <interface> slaac (enable|disable)	Enables/disables SLAAC
ipv6 (admin|a|b|c|d) add <address>/<prefix length> **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. The Meeting Server supports automatically configured addresses and static addresses. To statically configure an IPv6 address on the specified interface use this command
ipv6 (admin|a|b|c|d) del <address> **ipv6 a del 2001::2/64**	Removes the IPv6 address
ipv6 <interface> router add|del <address>	

2.3 Network Diagnostic Commands

These commands help with network diagnostics.

Note: In a virtualized deployment, there is no admin interface so **<mmp|app>** is not required. For example, in an Acano X-Series Server deployment use:

ping (mmp|app) <target address|hostname>

but in a virtualized deployment use:

ping <target address|hostname>

2.3.1 IPv4 network diagnostic commands

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

Command/Examples	Description/Notes
`ping (mmp|app) <target address|hostname>`	Ping from the MMP or the application interfaces to the target IP address or hostname
`traceroute (mmp|app) <target address|hostname>`	To traceroute from the MMP interface or application interfaces 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 (mmp|app) <target address|hostname>`	Ping from the MMP or the application interfaces to the target IPv6 address or hostname
`traceroute6 (mmp|app) <target address|hostname>`	To traceroute from the MMP interface or application interfaces to the target IPv6 address or hostname

2.3.3 Packet capture

Command/Examples	Description/Notes
`pcap (admin|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.

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: ■ signaling (SIP, AS-SIP signaling) ■ assured-voice (any audio for AS-SIP) ■ voice (any other audio) ■ assured-multimedia (video for AS-SIP) ■ multimedia (any other video) ■ multimedia-streaming (webbridge media) ■ low-latency (XMPP) ■ oa&m (webadmin, LDAP, SSH, SFTP) (oa&m = operations, administration and management)
dscp 4 voice 0x2E **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.
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

Note: In a virtualized deployment, there is no admin interface so **<mmp|app>** is not required. For example, in an Acano X-Series Server deployment use:

dns (mmp|app) add forwardzone <domain-name> <server ip>

but in a virtualized deployment use:

dns add forwardzone <domain-name> <server ip>

Command/Examples	Description/Notes
dns	Displays the current DNS configuration details
dns (mmp|app) add forwardzone <domain-name> <server ip> **dns app add forwardzone example.org 192.168.0.1**	Configures a forward zone. 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. Note: Application and MMP DNS needs to be set separately, but application DNS does not need to be set separately for A, B, C and D.
dns (mmp|app) del forwardzone <domain-name> <server ip>	Deletes a specified forward zone
dns (mmp|app) add trustanchor <anchor> **dns mmp add trustanchor ". IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5"**	Adds a trust anchor for Domain Name System Security Extensions (DNSSEC). Trust anchors should be specified in DNS Resource Record form inside quotation marks – see the example. See [1] for details.
dns (mmp|app) del trustanchor <zonename> **dns mmp del trustanchor**	Removes a trust anchor. 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 (mmp|app) add rr <DNS RR> **dns app add rr "sipserver.local. IN A 172.16.48.1"** **dns app 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. We accept RR records in quotation marks with the following format: **OWNER <OPTIONAL TTL> CLASS TYPE TYPE-SPECIFIC-DATA** For example, A records sipserver.local. IN A 172.16.48.1 AAAA records example.com. aaaa 3ffe:1900:4545:2:02d0:09ff:fef7:6d2c SRV records _sip._tcp.example.com. 86400 IN SRV 0 5 5060 sipserver.local
dns (mmp|app) del rr <owner-name> <type> **dns app del rr _sip._tcp.example.com. SRV** **dns app del rr sipserver.local. A**	
dns (mmp|app) lookup <a|aaaa|srv> <hostname> **dns mmp lookup srv _xmpp-client._tcp.example.com**	Does name "lookups" of type A, AAAA or SRV from the perspective of either the MMP or the application. The lookup "drills" through SRV results. That is, when an SRV record returns a domain name this is resolved by A and AAAA lookups. Note: If the application modules are not operational (e.g. during booting or rebooting), then DNS lookups for "app" will return no results.
dns (mmp|app) flush	This flushes the DNS cache of either the MMP or the application layer (API) of the Meeting Server.
dns flush	The equivalent command on a virtualized deployment.

4 Firewall Commands

The MMP supports the creation of simple firewall rules for both the media and admin 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      : admin
Enabled        : false
Default policy : allow

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

CAUTION: We recommend using the serial console to configure the firewall, because using SSH means that an error in the rules would make the SSH port inaccessible. If you must use SSH then ensure an allow ssh rule is created for the ADMIN interface before enabling the firewall.

Command/Examples	Description/Notes
firewall <iface> default (allow|deny) **firewall admin default deny**	Before the firewall can be enabled on an interface, a default policy must be set using this command. 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 When no rules are configured this will drop every packet on the admin interface.
firewall <iface> enable **firewall <iface> disable**	Enables the firewall on the specified interface. Disables the firewall on the specified interface.
firewall <iface> **firewall admin**	Displays the current firewall settings for a given interface Displays the status and rule set for the ADMIN interface

Command/Examples	Description/Notes
firewall <iface> allow <port> [/<proto>] [from <host>[/<prefix>]] **firewall <iface> deny <port> [/<proto>] [from <host>[/<prefix>]]**	Add rules with these commands. 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"). The protocol argument is either tcp or udp. If omitted, the rule matches both TCP and UDP packets.
firewall admin allow http/tcp	Allows TCP packets on port 80 on the admin interface
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 admin allow ssh from 192.168.1.0/28	Allows SSH access to the admin interface 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 admin delete 0	Deletes the single rule above this table.

5 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. 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. XMPP.
pki verify <cert> <cert bundle/CA cert> [<CA cert>] **pki verify server.pem bundle.pem rootca.pem** **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. 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>] **pki csr example CN:www.example.com OU:"My Desk" O:"My Office" L:"Round the corner" 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. <key/cert basename> is a string identifying the new key and CSR (e.g. "new" results in "new.key" and "new.csr" files) Attributes for the CSR can be specified in pairs with the attribute name and value separated by a colon (":"). Attributes are: CN: commonName which should be on the certificate. The commonName should be the DNS name for the system. OU: Organizational Unit O: Organization L: Locality ST:State C: Country emailAddress: email address 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. 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: **pki csr test1 CN:example.exampledemo.com subjectAltName:exampledemo.com** **pki csr test1 CN:example.exampledemo.com C:US L:Purcellville O:Example OU:Support ST:Virginia subjectAltName:exampledemo.com** **pki csr test3 CN:example.exampledemo.com C:US L:Purcellville O:Example OU:Support ST:VirginiasubjectAltName:exampledemo.com, 192.168.1.25,xmpp.exampledemo.com, server.exampledemo.com,join.exampledemo.com, test.exampledemo.com** 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 selfsigned <key/cert basename>	For quick testing and debugging, self-signed certificates (http://en.wikipedia.org/wiki/Self-signed_certificate) can be generated. <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).

Command/Examples	Description/Notes
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. 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

5.1 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.

Since the standardization of TLS 1.2 in 2008, continued analysis of older versions of TLS has shown significant weaknesses. This led to NIST advising in 2014 to move from TLS 1.0 to later versions of the protocol. Since then the deprecation of TLS 1.0 in products has started, with the PCI deadline for complete removal currently standing at June 2018.

Due to this, from version 2.3, the Meeting Server uses a minimum of TLS 1.2 and DTLS 1.2 for all services: SIP, LDAP, HTTPS (inbound connections: API, Web Admin and Web Bridge, outbound connections: CDRs) and XMPP. 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 future version of Meeting Server may completely remove TLS 1.0.

Command/Examples	Description/Notes
tls <service> **tls ldap**	Displays the configuration for a service , for example LDAP or SIP. Displays the setting for LDAP.
tls < service > trust <crt bundle> **tls ldap trust ldap.crt**	Configures the system to use a particular bundle of certificates to validate the certificate of a remote service

Command/Examples	Description/Notes
tls <service> verify (enable|disable)	Enables/disables certificate verification. When enabled, if the system fails to verify the remote service's certificate, then the connection will be aborted.
tls <service> verify ocsp	Enables verification with the additional requirement that the remote service returns a stapled OCSP response to ascertain certificate revocation status. 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.
tls <service> ciphers <cipher string>	See note 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/ciphers.html#CIPHER-LIST-FORMAT). The current default for cipher support is: " ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:RSA+AES:!aNULL:!MD5:!DSS:!3DES"
tls <service> min-tls-version <minimum version string>	Use this command to change the default TLS version. (From version 2.3) 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. Note: the Meeting Server only uses TLS 1.2 for XMPP services, the version cannot be changed.
tls sip min-tls-version 1.1	Use TLS version 1.1 or later for SIP
tls ldap min-tls-version 1.1	Use TLS version 1.1 or later for LDAP
tls min-dtls-version <minimum version string **tls min-dtls-version 1.1**	Configures the minimum DTLS version that the system will use. (From version 2.3) 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.

6 Commands for Configuring the Cisco Meeting Server

Command/Examples	Description/Notes
health	Displays temperatures, voltages and other health information about the Meeting Server. Note: The health command is not available on a virtualized deployment.
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. After using the shutdown command, an Acano X-Series Server can then be powered off.
hostname <name> **hostname mybox.mydomain**	Sets the hostname for the server. Note: A reboot is required after issuing this command.
timezone	Displays the currently configured timezone
timezone <timezone name> **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. Note: A reboot is required after issuing this command.
timezone list	Prints a full list of the available timezones. 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
ntp groupkey group.key **ntp autokey enable**	For example, a group key file can be uploaded using SFTP to "group.key" and configured with these commands.
date	Displays the current system (in UTC) and local time

Command/Examples	Description/Notes
date set <date> <time> **date set 2013-08-17 13:04**	Sets the date and time. This command should only be necessary in virtualized deployments, and server deployments that do not use an NTP server. The accepted formats for date and time are: • ISO 8601 format (%Y-%m-%d) plus 24-hour time with hour separated by a space • %m/%d/%y plus 24 hour time Note: Users of systems with an NTP server should not need to use this command.
reboot	Reboots the Meeting Server. Note: Rebooting the Meeting Server will disconnect any calls. The process takes some minutes to complete.
license	This command only applies on virtualized servers. It checks the Meeting Server license status and displays licensed features, e.g.: Feature: callbridge status: Activated expiry: 2014-JUl-01 (12 days remain)
callbridge **callbridge listen (interface whitelist|none)** **callbridge listen a** **callbridge listen none** **callbridge prefer <interface>** **callbridge certs <key-file> <cert-file>[<crt-bundle>]** **callbridge certs none** **callbridge restart**	Displays the current status Configures one or more interfaces (chosen from A, B, C or D) for the Call Bridge to listen on. Stops the Call Bridge and disables listening services; however, the Call Bridge remains enabled. Choses one interface from the interface whitelist 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. 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 5.) Removes certificate configuration Restarts the core media services. Note: Rebooting the Meeting Server will disconnect any calls. The process takes some minutes to complete.

Command/Examples	Description/Notes
syslog server add <hostname> [<port>] **syslog server del <hostname>** **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) The port defaults to 514 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 **syslog disable**	Enables the syslog mechanism
syslog audit add <hostname> **syslog audit add audit-server.example.org** **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. 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 Spacebar 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.
syslog search <string> **syslog search error**	Displays only those messages that match a certain pattern 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 10.6 for details on downloading the system logs
syslog rotate <filename> **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.

6.1 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). 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` `fips disable`	Enables the FIPS-140-2 mode cryptography for all cryptographic operations for network traffic. After enabling or disabling FIPS mode, a reboot is required
`fips test`	To run the built-in FIPS test

6.2 MTU for an Interface

Command/Examples	Description/Notes
`iface <interface> mtu <value>` `iface a mtu 1400`	Sets the maximum transmission unit size in bytes for an interface

7 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

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)	Creates a new MMP user of the specified type (see above) Prompts for a password for the user which must be entered twice to ensure that the intended password is configured. On first login, the user will be asked to configure a new password. CAUTION: user passwords expire after 6 months.
user del <username>	Removes a user from the system
user list	Displays the list of users, their role, the expiry date of their password and whether or not they are logged in.
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.
user unlock <username>	Removes a lock on logins for a user caused by exceeding the maximum failed logins

Command/Examples	Description/Notes
passwd [<username>]	Changes your password or another users password: follow the instructions. 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. 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> **user host bob add 192.168.1.3**	Restricts remote access for a user from hosts in a whitelist given as domain names or IP addresses. Note: The **user info** command displays the current list of allowed hosts (if any) – see above Adds 192.168.1.3 to the list of acceptable source addresses for remote hosts when bob tries to log in
user duty <username> <duty hours> **user duty <username> none** **user duty bob Wk0900-1700|Sa1200-1300**	Restricts the duty hours of a user 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. A day/time-range prefixed with a '!' indicates " anything but" e.g. !MoTu means anything but Monday and Tuesday. 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. 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. Allows bob access during office hours (9 to 5) on weekdays and between 1200 and 1300 on a Saturday

7.1 Password Rules

CAUTION: Passwords expire after 6 months.

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.

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. 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

Command/Examples	Description/Notes
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
user rule max_failed_logins <attempts>	Sets the number of failed login allowed before a 15 minute lockout. Note: if no maximum number of failed logins is configured, then none is enforced.
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. Note: if no idle time is configured, then none is enforced.
user rule max_sessions <number>	Limits any user to <number> simultaneous SSH sessions, <number> simultaneous webadmin sessions and, if not an account with the webadmin role, one console session. Note: the maximum number of concurrent sessions is 3, sessions are counted across web and ssh.
user rule max_sessions none	Removes session restrictions

7.2 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 **cac enable|disable** **cac enable strict**	Lists current configuration To enable CAC logins, execute cac enable 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. 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. 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. NOTE: - 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. - 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. 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. 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: 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

7.2.1 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)

8 Application Configuration Commands

8.1 XMPP Server Commands

These commands are for setting up an XMPP server as described in the Deployment Guides.

Command/Examples	Description/Notes
xmpp **xmpp status** **xmpp restart** **xmpp domain <domain-name>**	Displays the current configuration Restarts the XMPP server Creates a component secret for the XMPP server
xmpp listen <interface whitelist|none> **xmpp listen a b** **xmpp listen none**	Sets up a whitelist of interfaces to listen on. You must enable the service in order to start listening with the command xmpp enable Stops the XMPP server listening
xmpp (enable|disable)	Enables or disables the XMMP server
xmpp certs <key-file> <crt-file> [<crt-bundle>] **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. (Also see the section Provisioning with certificates.) Removes certificate configuration
xmpp motd add <message> **xmpp motd del**	Configures a " message of the day" which will be displayed when Cisco Meeting App or XMPP clients log in. " " Removes the message of the day. Alternatively, a message no larger than 2048 characters can be configured by copying a file by SFTP to " xmpp.motd" . Modifying the xmpp.motd in any way causes the XMPP server to restart.
xmpp max_sessions <number> **xmpp max_sessions none**	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. Removes any restriction on the XMPP sessions per user.

Command/Examples	Description/Notes
xmpp max_sessions 3	If the expectation is that a user will have at most an iPad, iPhone and PC login, then set the maximum sessions to three.
	These xmpp callbridge commands are explained in the Scalability & Resilience Deployment Guide
xmpp callbridge add <component name>	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.
xmpp callbridge del <component name>	Stops a Call Bridge from accessing the XMPP server.
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. See Section 8.4 for other commands to deploy XMPP resiliency.
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.

8.2 Commands for the Core to Edge Trunk

The Call Bridge needs to be accessible to clients on external networks despite sitting behind one or more firewalls and even NAT. To avoid complex configuration in split deployments, TLS trunks can be created between the Core and the Load Balancer on the Edge server.

The Core server and the Edge server mutually authenticate, and the Edge starts to listen on port 5222 for incoming client connections (XMPP).

This section describes the commands to set up this trunk; this is divided into commands that need to be run in the Edge's MMP and those that are run in the Core's MMP.

8.2.1 Load Balancer 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

Command/Examples	Description/Notes
loadbalancer (enable|disable) <tag> **loadbalancer enable exampleEdge**	Enables or disables the load balancer Note that the public port (see below) is not opened until there are trunks to service connections.
loadbalancer create <tag> **loadbalancer create exampleEdge**	Creates a load balancer
loadbalancer trunk <tag> <iface> [:<port>] **loadbalancer trunk exampleEdge a:3999** **loadbalancer public <tag> <iface> [:<port whitelist>]** **loadbalancer public exampleEdge b:5222** **loadbalancer public exampleEdge b:5222 lo:5222**	Configures the trunk interface and port Configures the public interface and port (for accepting client connections) 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> **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. 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.

8.2.2 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> **trunk create trunktoExampleEdge xmpp**	Creates a trunk instance for XMPP.

Command/Examples	Description/Notes
`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:
	• the DNS results for the Edge server name
	• attempts to create the TLS connection and authenticate to each address
	• if successful, debug information from the Core server, including:
	  • a list of "Core" connections (trunk to Edge server connections) to the Edge server in question
	  • the client connections currently being serviced by that Edge server
	  • memory usage statistics for the Edge server

8.3 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.

8.4 XMPP resiliency commands

Note: the XMPP resiliency feature is a fully released feature in Cisco Meeting Server 2.1.0, and supported for production environments.

XMPP resiliency provides fail-over protection for a client being unable to reach a specific XMPP server in multi-server deployments. Refer to the Scalability and Resilience Deployment Guide for the steps in setting up XMPP resiliency.

The MMP commands to configure the Meeting Server to deploy XMPP resiliency are listed in the table below.

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> **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. This command allows a Call Bridge to share credentials with many XMPP servers.

8.5 Web Bridge Commands

The Web Bridge only supports TLS; therefore you must follow the instructions in the Deployment Guides to set up the Web Bridge. This section provides a command reference.

Command/Examples	Description/Notes
webbridge restart **webbridge status**	Restarts the Web Bridge Displays the current configuration
webbridge listen <a|b|c|d|none [:<port>] whitelist> **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>] **webbridge certs none**	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 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.acano.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.

Command/Examples	Description/Notes
webbridge clickonce none	Disables all clickonce redirect behaviour
webbridge msi (<url>|none) **webbridge dmg (<url>|none)** **webbridge ios (<url>|none)** **webbridge ios none**	Configures the download locations for Windows msi, Mac OSX dmg and iOS installers which are presented to WebRTC users To deconfigure, use the appropriate command with the parameter none
webbridge trust <crt-bundle|crt-file> **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.
webbridge http-redirect (enable|disable)	Enables/disables HTTP redirects

8.6 TURN Server Commands

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 whitelist|none> **turn listen a b** **turn listen none**	Sets up a whitelist of interfaces to listen on. To start listening, you must enable the service with the command turn enable. Stops the TURN server listening.
turn tls <port|none>	Select the port for the TURN server to listen on Note: the Web Bridge and Turn Server cannot listen on the same interface:port combination. To run both on port 443 requires them to be run on separate servers/VMs, or on different interfaces on the same server/VM.

Command/Examples	Description/Notes
turn certs <keyfile> <certificate file> [<cert-bundle>]	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.)
turn certs none	Removes certificate configuration
turn (enable|disable)	Enables or disables the TURN server
turn credentials <username> <password> <realm> **turn credentials myusername mypassword example.com**	Sets the credentials for the TURN server
turn public-ip <public ip>	Sets up a public IP address for the TURN server
turn delete public-ip	Deletes the TURN server public IP address

8.7 SIP Edge Commands (BETA feature)

Note: SIP and Lync call traversal is a beta feature, only use in a test environment, do not use in a production environment.

The SIP Edge component provides support for traversal of local firewalls for SIP endpoints and Lync calls in split server deployments. The Call Bridge uses a TURN server within the Meeting Server to traverse the local firewall and send the SIP signal via a new SIP Edge component. Refer to the deployment guides for the steps in setting up SIP and Lync call traversal in a test environment.

The MMP commands to configure the SIP Edge component are listed in the table below.

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

Command/Examples	Description/Notes
sipedge public <interface>:<port>	Specify the external interface and port for connections to and from external systems
sipedge public-ip <address> **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 **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.

8.8 Web Admin Interface Commands

Command/Examples	Description/Notes
webadmin	Displays the configuration
webadmin restart	Restarts the Web Admin Interface
webadmin listen (admin|a|b|c|d) [<port>] **webadmin listen a** **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**. The default is port 443. Note: admin is not a valid parameter for this command in the virtualized deployment.
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>] **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 Removes certificate configuration

Command/Examples	Description/Notes
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.

8.9 Database Clustering Commands

These database clustering commands are explained in the Scalability & Resilience Deployment Guide

Command/Examples	Description/Notes
database cluster status	Displays the clustering status, from the perspective of this database instance.
database cluster localnode <interface>	This command must be run on the server that will host the initial master database before initialising a new database cluster. The <interface> can be in the following formats: [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 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 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 <ipaddress> - a specific IP address, can be IPv4 or IPv6 e.g. database cluster localnode 10.1.3.9 **Note:** Do not use the Admin interface for database clustering.
database cluster initialize	Creates a new database cluster, with this server's current database contents as the one and only database instance—the master. The command reconfigures postgres to cluster mode - i.e. listens on external interface and uses SSL Reconfigures and restarts the local Call Bridge (if it is enabled) to use the database cluster.

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 master database to this server and destroying the current contents of any database on it. <hostname/ip address> can be for any existing database in the cluster. Reconfigures and restarts the local Call Bridge (if it exists and it is enabled) to use the database cluster
database cluster connect <hostname/IP address>	Connects a Call Bridge to a database cluster. 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).
database cluster certs <server_key> <server_crt> <client_key> <client_ crt> <ca_crt> **database cluster certs dbcluster_ server.key db cluster_server.crt dbcluster_client.key db cluster_client.crt dbcluster_ca.crt**	Fully enables encryption between databases in a cluster. A database cluster can be set up in unencrypted mode and encryption enabled subsequently.
database cluster certs <client_key> <client_crt> <ca_crt> **database cluster certs dbcluster_ client.key dbcluster_client.crt dbcluster_ ca.crt** **database cluster certs none**	Enables encryption for remote connections only, with no server keys. Disables encryption between databases
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.

Command/Examples	Description/Notes
`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: • on the master database, but it can be run on any database instance • 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.

8.10 Recorder Commands

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` `recorder`	Restarts the Recorder Displays the current configuration of the Recorder
`recorder listen <a|b|c|d|lo|none [:<port>] whitelist>` `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 (enable|disable)`	Enables or disables the Recorder

`recorder certs <keyfile-name> <crt filename> [<crt-bundle>]`
 	
`recorder certs none`
	Provides the name of the key file and .crt file for the Recorder and, optionally, a CA certificate bundle as provided by your CA
	
	Removes certificate configuration

`recorder trust <crt-bundle|crt-file>` `recorder trust none`	Controls which Call Bridge instances are allowed to connect to the Recorder. 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.

Command/Examples	Description/Notes
recorder nfs <hostname/IP>:<directory>	Provides the Recorder with details of the network file server (nfs) and folder to save the recording.

8.11 Uploader Commands (BETA feature)

Version 2.3 previews the Uploader component to simplify using Vbrick Rev for video content management. This section provides a command reference for the Uploader. Follow the instructions in the version 2.3 release notes to configure 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 <hostname>	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 <username>	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.
uploader (cms|rev) pass-word	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)	Allow the named team to edit the video recordings on Vbrick Rev. If the **<uploader-team name>** includes a space then use straight quotes around the team name. **none** removes the named team, members of the team can no longer edit the video recordings.
uploader view (<uploader-team name>|none)	Allow the named team to view the video recordings on Vbrick Rev. If the **<uploader-team name>** includes a space then use straight quotes around the team name. **none** removes the named team, members of the team can no longer view the video recordings.
uploader access <Priv-ate|Public|AllUsers>	Set access permission to the video recordings

Commands	Description
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.

8.12 Streamer Commands

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

streamer restart **streamer**	Restarts the Streamer Displays the current configuration of the Streamer
streamer listen <a|b|c|d|lo|none [:<port>] whitelist> **streamer 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 recorder enable. The default for the optional port argument is 443.
streamer listen none	Stops the Streamer listening.
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.
streamer certs <keyfile-name> <crt filename> [<crt-bundle>] **streamer certs none**	Provides the name of the key file and .crt file for the Streamer and, optionally, a CA certificate bundle as provided by your CA Removes certificate configuration

streamer trust <crt-bundle|crt-file>	Controls which Call Bridge instances are allowed to connect to the Streamer. 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

9 H.323 Commands

The MMP commands to configure the Meeting Server to accept and send H.323 calls are listed in this section.

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>] **h323_gateway certs none**	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.) Removes certificate configuration
h323_gateway h323_nexthop <host/ip> **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. 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> **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> **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> **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.

Command/Examples	Description/Notes
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> **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. 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. Changes do not take place until the gateway is restarted. The H.323 Gateway always expects TLS connections; therefore, " Encrypted" should be selected on outbound dial plan rules on the Call Bridge
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 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. 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.

10 Miscellaneous Commands

10.1 Model

Command/Examples	Description/Notes
`model`	Displays the Cisco Meeting Server deployment model. For an Acano X-series server the possible values are: Acano X1, Acano X2, or Acano X3. Virtualized deployments show as CMS VM

10.2 Meeting Server's Serial Number

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

10.3 Message of the Day

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

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 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.

10.4 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 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

10.5 SNMP Commands

10.5.1 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

For an Acano X-series server, the MIB files are:

- ACANO-MIB.txt
- ACANO-HEALTH-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.

10.5.2 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] **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.
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
snmpwalk -v 1 -c <community> <MMP-address> ACANO-HEALTH-MIB::acanoHealth **snmpwalk -v 1 -c public <MMP-address> ACANO-HEALTH-MIB::acanoHealth**	To test the configuration using v1/2c, use Net-SNMP's snmpwalk (http://net-snmp.sourceforge.net/) on Linux (other tools are available on Windows) – see the example on the left. Note: ACANO-HEALTH-MIB is only available on theAcano X-Series Server, it is not available on virtualized deployments.

10.5.3 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. 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.
snmp user del <name>	Deletes an SNMP user.
snmp (enable|disable)	Enables/disable SNMP v3.
snmpwalk -v 3 -u <secName> -a <authProtocol> -A <authPassword> -x <privProtocol> -X <privPassword> -l <secLevel> <MMP-address> ACANO-HEALTH-MIB::acanoHealth **snmpwalk -v 3 -u fred -a MD5 -A example123 -x DES -X exampl123 -l authPriv <MMP-address> ACANO-HEALTH-MIB::acanoHealth**	To test the configuration using v3, use Net-SNMP's snmpwalk (http://net-snmp.sourceforge.net/) on Linux (other tools are available on Windows) – see the example on the left. Note: ACANO-HEALTH-MIB is only available on the Acano X-Series Server, it is not available on virtualized deployments.

10.5.4 SNMP trap receiver configuration

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

10.6 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>**

10.7 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.

10.8 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.

10.9 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.
backup rollback <name>	Restores the system for the backup <name> (uploads the file and rolls back the configuration. 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.

10.10 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. 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 R1.9 to R2.0, the backup will be called 1_9.bak. The default filename if one is not provided is upgrade.img
upgrade <filename> [no-backup]	Use with caution.

Command/Examples	Description/Notes
`upgrade list`	To get a list of the upgrade images on the system
`upgrade delete <name>` `upgrade delete upgrade.img`	Upgrade images persist until they are deleted using SFTP or this CLI command

10.11 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. 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.

10.12 Password Recovery/First Boot for the Acano X-Series Server

Use this procedure for the first configuration of the Acano X-Series Server or if you no longer have the password of an MMP account with admin rights.

1. If necessary, plug both power units in to the mains using the appropriate power cables for your location. There are no on/off switches so the server powers up immediately.
2. Moving to the front of the X-series server you see the two power unit status LEDs and the status LED on, indicating that the server is powered and operational.
3. Connect the Console port to a terminal emulator using the serial cable supplied in the box. Use baud rate 115200, 8 data bits, no parity and 1 stop bit.
4. Using a Philips screwdriver loosen the two screws on the top front service hatch and hinge the cover upwards.

   You see the fan module on the left and a smaller area on the right with cables and connectors. In this area and behind the front grill are two small buttons: one red (labeled reset) and one black.
5. Carefully press the red (reset) button only.
6. Within four minutes of pressing this button log into the server using the terminal emulator: user account is “admin”, no password will be requested.
7. Set up your admin account using the following command.

   ```
   user add admin admin
   ```

Note: You can create multiple admin level accounts with different account names.

8. You are prompted for a password which you must enter twice.

   Note: When you log in subsequently, either via the Console port or the interface labeled Admin with the admin account created above and you will be asked for this password.

9. Close the hatch and push the screws down to secure the hatch, no screwdriver is needed.

Cisco Legal Information

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

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

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

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

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

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

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

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

Cisco Trademark