Cisco Meeting Server

Cisco Meeting Server リリース 3.8

MMP コマンドライン リファレンス

2023 年 9 月 7 日

目次

変更履歴

日付	変更点
2023 年 9 月 7 日	Cisco Meeting Server 3.8 ソフトウェアの新しいバージョン。「MMP の 追加および変更の概要」を参照。
2023 年 3 月 16 日	Cisco Meeting Server 3.7 ソフトウェアの新しいバージョン。「MMP の追加および変更の概要」を参照。
2022 年 10 月 19 日	マイナー修正。
2022 年 8 月 23 日	Meeting Server 3.6 ソフトウェアの新しいバージョン。「MMP の追加および変更の概要」を参照。
2022 年 4 月 20 日	Meeting Server 3.5 ソフトウェアの新しいバージョン。「MMP の追加および変更の概要」を参照。
2021 年 12 月 21 日	「TLS 証明書検証」セクションのコマンド説明のリンクを更新。
2021 年 12 月 15 日	Meeting Server 3.4 ソフトウェアの新しいバージョン。「MMP の追加および変更の概要」を参照。
2021 年 8 月 24 日	Meeting Server 3.3 ソフトウェアの新しいバージョン。
2021 年 5 月 19 日	中規模 OVA Expressway の推奨事項に関するドキュメントを更新。
2021 年 4 月 16 日	セクション 2.1「ネットワーク インターフェイス（iface）コマンド」のインターフェイスコマンドの MTU を移動。MTU 情報に関する注記を更新。
2021 年 4 月 9 日	Meeting Server 3.2 ソフトウェアの新しいバージョン。
2021 年 3 月 16 日	Meeting Server の短期的なログイン情報が完全にサポートされる機能としてドキュメントを更新。
2020 年 12 月 4 日	pcap セクションに注記を追加
2020 年 11 月 30 日	バージョン 3.1 ソフトウェアの新しいバージョン。
2020 年 10 月 15 日	明確化のための注記を再追加。MTU 情報。 その他のマイナー修正。
2020 年 9 月 11 日	軽微な修正。
2020 年 8 月 21 日	軽微な修正。
2020 年 7 月 29 日	バージョン 3.0 ソフトウェアの新しいバージョン。

1 はじめに

Cisco Meeting Server ソフトウェアは、シスコ ユニファイド コンピューティング サーバー（UCS）技術に基づく特定のサーバー、または仕様に基づく VM サーバーでホストできます。本書では、Cisco Meeting Server を Meeting Server と呼びます。

注：Cisco Meeting Server ソフトウェアバージョン 3.0 以降では、X シリーズサーバーをサポートしません。

Cisco Meeting Server ソフトウェアには、プラットフォームとアプリケーションの 2 つのレイヤがあります。プラットフォームは、メインボード管理プロセッサ（MMP）で構成されます。アプリケーションは、この管理型プラットフォーム上で実行し、独自の設定インターフェイスを持ちます。

MMP は、低レベルのブートストラップと設定のために使用されます。コマンド ライン インターフェイスを提供します。Cisco Meeting Server 2000 では、MMP コマンド ライン インターフェイスは Serial Over LAN 接続を介してアクセスされます。仮想化された展開（Cisco Meeting Server 1000、および仕様ベースの VM サーバ）では、MMP は仮想インターフェイス A でアクセスされます。

アプリケーションレベルの管理（コールおよびメディア管理）は、API を介して実行されるか、または簡単な展開の場合は、使用可能なイーサネット インターフェイスのいずれかで実行するように設定できる Web Admin インターフェイスを介して実行されます。

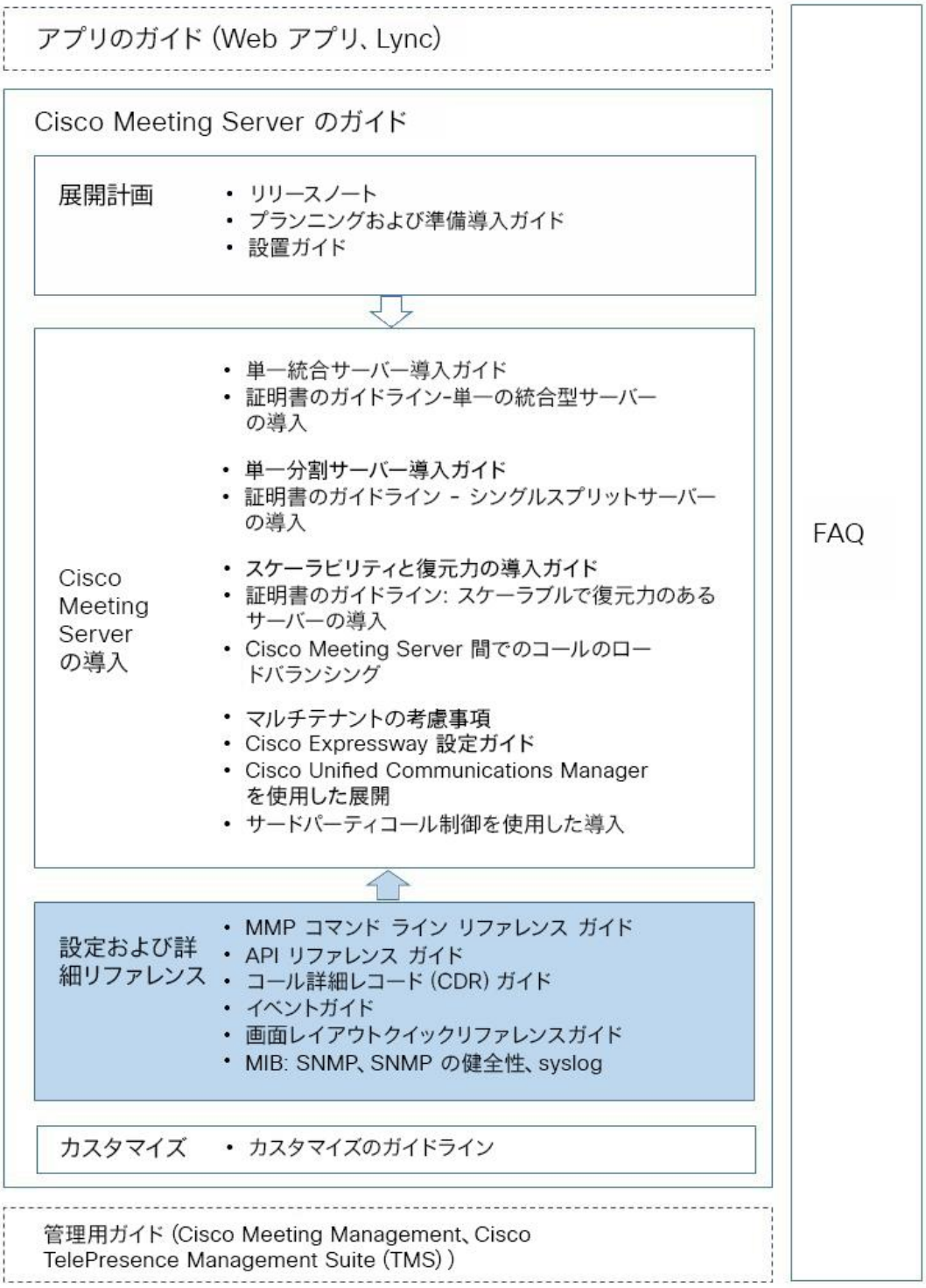
注：このガイドでは、Cisco Meeting Server ソフトウェアを Meeting Server と呼びます。

1.1 このドキュメントの使用方法

このガイドでは MMP について説明します。特に明記されていない限り、情報は Cisco Meeting Server 2000、Cisco Meeting Server 1000、および仮想化展開に等しく適用されます。

これらのドキュメントは、 cisco.com から入手できます。

図 1：バージョン 3.7 の Cisco Meeting Server のドキュメント



1.2 MMP へのアクセス

1.2.1 Cisco Meeting Server 2000

MMP コマンド ライン インターフェイスには、Cisco Meeting Server 2000 の Serial Over LAN 接続を介してアクセスします。MMP を使用する前に、Serial Over LAN 接続を IP アドレスとログイン情報で設定する必要があります。Serial Over LAN 接続の設定の詳細については、『Cisco Meeting Server 2000 設置ガイド』を参照してください。

初期設定後、SSH クライアントを使用して Serial Over LAN 接続の IP アドレスに接続し、設定された管理者アカウントのログイン情報を使用して MMP にログインします。

1.2.2 仮想化展開（Cisco Meeting Server 1000 および仕様ベースの VM サーバ）

仮想化展開では、MMP は VSphere コンソールタブ（仮想インターフェイス A 上）からアクセスされ、MMP 管理ユーザのログイン情報が必要です（「MMP ユーザアカウントコマンド」を参照）。これらは、インストール手順の一部として設定されます。『Cisco Meeting Server Installation Guide for Virtualized Deployments』を参照してください。

1.2.3 Cisco Meeting Server プラットフォーム間の特定のコマンドの違い

Cisco Meeting Server 2000 の実行は、仮想化された Cisco Meeting Server と比べるといくつかの違いがあります。

コマンド	Cisco Meeting Server 2000 上	Cisco Meeting Server 1000 上、および仮想化された Cisco Meeting Server 上
shutdown	MMP では利用できません。ブレードサーバの電源を切断するには、まず Cisco UCS Manager 上で電源を切断します。	VSphere の電源ボタンは使用しないでください。代わりに、**shutdown** コマンドを使用します。
health	MMP では利用できません。Cisco UCS Manager を使用します。	利用不可
serial	サーバのシリアル番号を返します。	利用不可
dns	インターフェイスは指定しないでください。 例： **dns add forwardzone <domain-name> <server ip>**	インターフェイスは指定しないでください。 例： **dns add forwardzone <domain-name> <server ip>**
user evict	バージョン 2.9 から利用可能	利用可能

1.3 MMP との間でのファイルの転送

ファイルは、Secure File Transfer Protocol（SFTP）を使用して MMP との間で転送できます。Windows では、WinSCP（http://winscp.net/eng/index.php）をお勧めしますが、任意のクライアントを使用できます。SFTP は、次のファイルの転送に使用されます。

- ソフトウェア アップグレードのイメージ
- 設定スナップショット
- セキュリティ証明書
- ライセンス ファイル
- システムログファイル（Cisco サポートの指示による）
- クラッシュ診断ファイル（Cisco サポートの指示による）

SFTP クライアントを、ipv4 MMP または ipv6 MMP コマンド（必要に応じて）を使用して検出できる MMP の IP アドレスに接続します。 MMP の admin ユーザのログイン情報を使用してログインします（「MMP ユーザ アカウント コマンド」を参照）。

1.3.1 SFTP クライアントに表示されるファイル

設定後、SFTP を使用して MMP にアクセスすると、次のファイルが表示されます（license.dat 以外のすべての名前が異なる場合があることに注意してください。ただし、以下は、設置ガイドおよび導入ガイドで使用されているファイル名の例です）。

- Server.crt、webbridge.crt
- license.dat（必須名）
- boot.json と live.json
- server.key、webbridge.key
- cacert.pem、privkey.pem、server.pem

1.4 使用可能な MMP コマンド

使用可能なコマンドとパラメータのリストを表示するには：

```
help
```

1 つのコマンドタイプに関する詳細を表示するには：

```
help <command name>
```

これらのコマンドについては、次の各項で説明します。すべてのコマンドは、MMP コマンドライン インターフェイス プロンプトに対して入力します。例：

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

ここで

() はオプションの選択肢を示し、そのうちの 1 つを使用します（括弧は入力しません）。

<> は、適切な値を入力する必要があるパラメータを示します。[ ] は、

オプションのパラメータを示します。

一部のコマンドの後には、同じテーブルセル内で青色で 1 つ以上の例が続きます。

コマンド/例	説明/注意事項
`iface (a|b|c|d)`	指定されたインターフェイスのネットワーク インターフェイス設定を表示します。 A、B、C、および D インターフェイスは、全二重自動ネゴシエーションに制限されていることに注意してください。

1.5 MMP コマンドの作成と完了

MMP コマンドでは、次の機能を使用できます。

- Tab：コマンドをオートコンプリートするには、Tab キーを押します。たとえば、**`help ti`** と入力して Tab キーを押すと、**`help timezone`** と入力されます。ただし、使用可能なコマンドが複数ある場合、Tab タブを 2 回押しても代替候補は表示されません。たとえば、help we の後に Tab を押すと、**`help webadmin`** が表示され、もう一度押しても、**`help webbridge`** は表示されません。
- 左右の矢印キーは、入力したコマンドの行に沿ってカーソルを移動します。
- 上下の矢印キーは、コマンド履歴を循環します
- 引用符：複数単語の引数を入力するには、たとえば次のように ”” を使用します。

  ```
  pki csr demo CN:"callbridge.example.com" OU:"Cisco Support" O:Cisco L:"New York" ST:NY C:US
  ```

キーボードショートカットを使用できます。

- CTRL-p：前のコマンドを表示します。

- CTRL-n：コマンド履歴の次のコマンドを表示します。
- CTRL-d：カーソルの下の文字を削除するか、空の行で使用すると終了します。
- CTRL-c：現在実行中のコマンドを中止します。
- CTRL-a：行頭にジャンプします。
- CTRL-e：行末にジャンプします。
- CTRL-l：端末をクリアします。
- CTRL-k：カーソルの位置から行末まで削除します。
- CTRL-m：Return キーと同じです。
- CTRL-w：カーソルから左の単語を削除します。
- CTRL-u：現在の行を削除します。
- CTRL-f：文字を前方に移動します。
- CTRL-b：文字を後方に移動します。
- CTRL-t：現在の文字を前の文字と入れ替えます。

1.6 予約済みポート

ポート 8081 は、webadmin が有効な場合、ループバックで予約されますが、webadmin が無効な場合は予約されません。ポート 8080 は常に開いています。

ポート 5060 は常に開いていますが、ポート 5061 は、証明書が Call Bridge に適用されている場合にのみ開いています。

1.7 MMP の追加および変更の概要

バージョン 3.8 では、このセクションで説明する MMP の追加をサポートしています。

Meeting Server と Cisco Unified Communications Manager/IMP **サーバー間のセキュアな通信を実現**

Meeting Server と Cisco Unified Communications Manager/IMP サーバー間の TLS 検証に使用するコマンドを以下に示します。

コマンド/例	説明
callbridge ucm certs <cert-bundle>	Cisco Unified Communications Manager の CA の信頼できる証明書を追加します。
callbridge ucm verify <enable/disable>	Meeting Server と Cisco Unified Communications Manager 間の TLS 検証を有効または無効にします。
callbridge ucm certs none	Meeting Server と Cisco Unified Communications Manager 間の TLS 検証用に追加された証明書を削除します。
callbridge imps certs <cert-bundle>	IMP サーバーに CA の信頼できる証明書を追加します。
callbridge imps verify <enable/disable>	Meeting Server と IMP サーバー間の TLS 検証を有効または無効にします。
callbridge imps certs none	Meeting Server と IMP サーバー間の TLS 検証用に追加された証明書を削除します。

Web アプリケーション セッション タイムアウトの設定

管理者は、次のコマンドを使用して、Web アプリケーション セッションのタイムアウトを時間単位で設定できます。

コマンド/例	説明
callbridge wc3jwt expiry <expiry time in hours>	Web アプリケーションのセッションタイムアウト（時間）を設定します。1 ～ 24 の整数を指定できます。設定しない場合のデフォルトは 24 です。 **注：** 変更を適用するには、Call Bridge を再起動します。

2 ネットワークコマンド

2.1 ネットワーク インターフェイス（iface）コマンド

コマンド/例	説明/注意事項
iface (a|b|c|d)	指定されたインターフェイスのネットワーク インターフェイス設定を表示します。 A、B、C、および D インターフェイスは、全二重自動ネゴシエーションに制限されていることに注意してください。
iface <interface> mtu <value> **iface a mtu 1400**	インターフェイスの最大伝送単位（MTU）のサイズをバイト単位で設定します。 **注：**すべての Meeting Server 2000 展開と、VMWare バージョン 6.7U2 以降を実行する VM および Meeting Server 1000 展開では、MTU は着信パケットと発信パケットの両方に適用されます。設定された MTU よりも大きい受信パケットはインターフェイスによってドロップされ、パケット損失と低品質の原因となり、まれに接続問題が発生します。6.7U2 より前のバージョンの VMWare を実行している VM および Meeting Server 1000 展開では、MTU は発信パケットにのみ適用され、設定された MTU よりも大きいパケットもインターフェイスで受信できます。 デフォルトの MTU は 1500 バイトです。 これらの MTU 制限が原因でパケットがインターフェイスによってドロップされないようにするには、ネットワーク上で MTU を設定する必要があります。

2.2 IP コマンド

2.2.1 IPv4 コマンド

コマンド/例	説明/注意事項
ipv4 (a|b|c|d)	設定および観測されたネットワーク値を一覧表示します。
ipv4 (a|b|c|d) dhcp	指定されたインターフェイスで dhcp を有効にします。
ipv4 (a|b|c|d) (enable|disable)	指定されたインターフェイスを有効/無効にします。 注：このコマンドは設定をクリアするのではなく、無効にするだけです。

コマンド/例	説明/注意事項
ipv4 (a|b|c|d) add <server IP address>/<Prefix Length> <Default Gateway> **ipv4 a add 10.1.2.3/16 10.1.1.1**	指定されたプレフィックス長の ipv4 アドレスと出力パケットのデフォルトゲートウェイを使用してインターフェイスを設定します。この例では、サブネット 10.1.0.0/16 のアドレス 10.1.2.3 で A を設定します。これ以上特定のルートがない場合、A 経由で送信されるパケットは、ゲートウェイ 10.1.1.1 経由で送信されます。
ipv4 (a|b|c|d) del <server IP address>	指定されたインターフェイスの IPv4 アドレスを削除します。
ipv4 (a|b|c|d) default	アウトバウンド接続のラスト リゾート インターフェイスを選択します。リモートホストに接続する場合、コンテキストからどのインターフェイスを使用すべきかが常にわかるわけではありません。これに対して、リモートホストによって開始された接続への応答では、接続が受け入れられたインターフェイスが使用されます。これは、強力な IP モデルと呼ばれることもあります。
ipv4 (a|b|c|d) route add <address>/<prefix length> **ipv4 (a|b|c|d) route del <address>/<prefix> length>**	特定のインターフェイスから特定のサブネットをルーティングできるように、静的ルートを追加します。これは、複数のインターフェイスが有効になっていて、特定のサブネット向けのトラフィックがその特定のインターフェイスのゲートウェイに確実にルーティングされるようにする一意ルーティングシナリオ用です。 注：通常、デフォルトルートを手動で設定する必要はなく、問題が発生する可能性があります。
ipv4 b route add 192.168.100.0/24	192.168.100.x 宛てのすべてのトラフィックは、インターフェイス b からインターフェイス b のゲートウェイに送信されます。

2.2.2 IPv6 コマンド

Meeting Server は、インターフェイスごとに複数の IPv6 アドレスをサポートし、自動的に設定されたアドレスと静的アドレスをサポートします。

コマンド/例	説明/注意事項
ipv6 (a|b|c|d)	設定および観測されたネットワーク値を一覧表示します。

コマンド/例	説明/注意事項
ipv6 (a|b|c|d) enable	指定された IPv6 インターフェイスの自動設定を開始します。リンクローカルアドレスが生成されます。重複アドレス検出（DAD）が完了すると、ルータ要請が送信されます。ルータ広告が受信された場合、 - アドバタイズされたプレフィックスが、グローバルアドレスの構築に使用されます。 - DNS の設定には、任意の RDDNS オプションが使用されます - ”managed” または ”other” フラグが設定された場合、DHCPv6 が開始されます。ルータ広告で ”managed” または "other" ビットがセットされていない場合、DHCPv6 は使用されません。 ルータ要請が 3 回送信されてもルーター広告が受信されない場合、DHCPv6 が開始されます。
ipv6 (a|b|c|d) disable	指定されたインターフェイスの IPv6 を無効にします。
ipv6 <interface> slaac (enable|disable)	SLAAC を有効/無効にします。
ipv6 (a|b|c|d) add <address>/<prefix> length> **ipv6 a add 2001::2/64**	SLAAC が無効になっている場合は、静的アドレスと静的ルータアドレスを追加する必要があります。静的ルータを追加するには、SLAAC で検出されたアドレスとルーターが静的に設定されたアドレスと共存できることに注意してください。 Meeting Server は、自動的に設定されたアドレスと静的アドレスをサポートしています。指定されたインターフェイスで IPv6 アドレスを静的に設定するには、次のコマンドを使用します。
ipv6 (a|b|c|d) del <address> **ipv6 a del 2001::2/64**	IPv6 アドレスを削除します。
ipv6 <interface> router add|del <address>	

2.3 ネットワーク診断コマンド

2.3.1 IPv4 ネットワーク診断コマンド

IPv4 を有効にすると、次のコマンドを使用できます。

コマンド/例	説明/注意事項
ping <target address|hostname>	Meeting Server からターゲット IP アドレスまたはホスト名に ping を打ちます。
traceroute <target address|hostname>	Meeting Server からターゲット IP アドレスまたはホスト名への traceroute を実行するには

2.3.2 IPv6 ネットワーク診断コマンド

IPv6 を有効にすると、次のコマンドを使用できます。

コマンド/例	説明/注意事項
ping6 <target address|hostname>	Meeting Server からターゲット IPv6 アドレスまたはホスト名に ping を打ちます。
traceroute6 <target address|hostname>	Meeting Server からターゲット IPv6 アドレスまたはホスト名への traceroute を実行するには

2.3.3 パケットキャプチャ

注：Meeting Server ではパケットをキャプチャすることができますが 、Meeting Server が動作するパケットレートが高い場合、コールの処理における Meeting Server の通常の動作を妨害するのではなく、パケットキャプチャからパケットをドロップする場合があります。パケットキャプチャのパケット損失を回避するために、Cisco は、Meeting Server ではなくネットワークスイッチでパケットをキャプチャすることをお勧めします。

コマンド/例	説明/注意事項
pcap (a|b|c|d)	指定されたインターフェイスでパケットキャプチャをただちに開始し、Ctrl-C を押すと停止します。pcap ファイルの名前が表示されます。このファイルは、SFTP 経由でダウンロードできます。 **pcap** コマンドは、複数のファイルにローテーションでパケットをキャプチャします。pcap ファイルのサイズが 500MB を超えると、パケットは新しいファイルにキャプチャされます。ミーティングサーバは、常に最大 4 つの pcap ファイルを保存し、合計最大ファイルサイズの制限は 2GB です。4 番目の pcap ファイルのサイズが 500MB を超えると、最も古い pcap ファイルが削除され、新しいファイルでパケットのキャプチャが続行されます。

コマンド/例	説明/注意事項
pcap (a|b|c|d|any) [snaplen <n>] [filter <pcap-filter-expression>]	**any** は、複数のインターフェイス、つまり有効な任意のインターフェイスでのパケットキャプチャを許可します（有効になっていないインターフェイスはスキップされます）。 **注：**複数のインターフェイスからキャプチャする場合は、各インターフェイスが別の一時的なファイルにキャプチャされ、キャプチャが停止された時にファイルが統合されるなど、ディスク領域が追加される必要があります 。したがって、複数のインターフェイスでキャプチャするときに使用できるストレージは、単一のインターフェイスでキャプチャするときに使用できるストレージの半分です。 **snaplen** は、キャプチャされた各パケットがそれより長い場合、最大バイト数（n）に切り捨てます。その結果、より多くのパケットが同じファイルサイズの制限に収まる可能性があります。 **filter** は、文字列内の条件に一致するパケットのみを選択します。これによりキャプチャが関心のあるパケットだけに減り、他のパケットのディスク容量を節約できます。この文字列の解析とパケットフィルタリングは、tcpdumpで使用されるものとまったく同じ基本ライブラリを使用して実行されるため、これはまったく同じ表現力とパフォーマンスを備えています。フィルタ式は、必要に応じて最大約 4080 文字長にすることができます。 **snaplen**オプションと **filter**オプションは、バージョン 3.1 から追加されました。

2.4 QoS/DSCP コマンド

Meeting Server は、DSCP Hex（TOS ではない）の QoS/DSCP 値をサポートします。すべての値が標準ではない場合でも、下位互換性のために 0 ～ 63 の DSCP 値を許可するという米国連邦政府機関の要件に従います。

10 進数、16 進数（大文字と小文字を区別しない）、および 8 進数としての入力をサポートしています。46、0x2E（または 0x2e）、または 056 をそれぞれ入力すると、同じ結果になります。

たとえば、EF オーディオ、AF31 シグナリング/データ、AF41 ビデオは次のとおりです。

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

DSCP 設定は、IPv4 と IPv6 について個別の値で定義できます。たとえば、oa&m を IPv4 の場合は 0x4、IPv6 の場合は 0x6 に設定すると、SSH トラフィックは IPv4 接続の場合は 0x4、IPv6 接続の場合は 0x6 でマークされます。

注：変更を有効にするには、サービスを再起動する必要があります。コアサーバを再起動することをお勧めします。

コマンド/例	説明/注意事項
dscp (4|6) <traffic type> (<DSCP value>|none)	DSCP トラフィックを設定します。DSCP トラフィックカテゴリとそれらのカテゴリ内のトラフィックタイプは次のとおりです。 ▪ signaling（SIP、AS-SIP シグナリング） ▪ assured-voice（AS-SIP の任意のオーディオ） ▪ voice（その他の音声） ▪ assured-multimedia（AS-SIP のビデオ） ▪ multimedia（その他のビデオ） ▪ multimedia-streaming（webbridge メディア）（現在は使用されていません） ▪ low-latency（現在使用されていません） ▪ oa&m（webadmin、LDAP、SSH、SFTP） （oa&m = operations、administration、management）
dscp 4 voice 0x2E **dscp 4 voice 46**	
dscp 4 oa&m 0x22	IPv4 の oa&m を設定します。
dscp 4 oa&m none	設定を削除します。
dscp assured (true|false)	”voice" および "multimedia" トラフィックタイプに対して、保証された DSCP 値と保証されていない DSCP 値の両方を設定することができます。上記を参照してください。このコマンドを使用して、保証値または非保証値の使用を強制します。
dscp assured true	たとえば、すべての音声およびビデオデータに対して assured-voice および assured-multimedia DSCP 値の使用を強制するには、このコマンドを使用します。

3 DNS コマンド

コマンド/例	説明/注意事項
dns	現在の DNS 設定の詳細を表示します。
dns add forwardzone <domain-name> <server ip> **dns add forwardzone example.org 192.168.0.1**	フォワードゾーンを設定します。 フォワードゾーンは、ドメイン名と少なくとも 1 つのサーバアドレスで構成されるペアです。ある名前が DNS 階層内の特定のドメイン名の下にある場合、DNS リゾルバでその特定のサーバーに問い合わせることができます。ロードバランシングとフェイルオーバーを可能にするには、特定のドメイン名に対して複数のサーバーを指定します。一般的には、ドメイン名として「.」を指定します。これは DNS 階層のルートであり、すべてのドメイン名と一致します。
dns del forwardzone <domain-name> <server ip>	指定されたフォワードゾーンを削除します。
dns add trustanchor <anchor> **dnsadd trustanchor. "IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5"**	ドメイン ネーム システム セキュリティ拡張（DNSSEC）のトラストアンカーを追加します。 トラストアンカーは、DNS リソースレコードフォームで引用符で囲んで指定する必要があります。例を参照してください。詳細については [1] を参照してください。
dns del trustanchor <zonename> **dns del trustanchor**	トラストアンカーを削除します。 zonename は、アンカーを表すリソースレコード（RR）内のドメイン名です。この例では、上記の例でインストールされたトラストアンカーを削除します。

コマンド/例	説明/注意事項
dns add rr <DNS RR> **dns add rr "sipserver.local. IN A 172.16.48.1"** **dns add rr "_sip._tcp.example.com. 86400 IN SRV 0 5 5060 sipserver.local."**	外部 DNS サーバで設定されていないか、上書きする必要がある値を返す DNS リゾルバを設定するには、外部 DNS サーバに照会する代わりに返されるカスタムリソースレコード（RR）を設定できます。 引用符で囲まれた、次の形式の RR を受け入れます。 **OWNER <OPTIONAL TTL> CLASS TYPE TYPE-SPECIFIC-DATA** 例： A は sipserver.local を記録します。IN A 172.16.48.1 AAAA は example.com を記録します。aaaa 3ffe:1900:4545:2:02d0:09ff:fef7:6d2c SRV は _sip._tcp.example.com を記録します。86400 IN SRV 0 5 5060 sipserver.local 注：1 つのレコードタイプに対して複数の RR を作成する場合は、外部 DNS サーバを使用してそれらを作成する必要があります。Meeting Server は、1 つのレコードタイプに対して複数の RR をサポートしておらず、最新の RR のみを保存します。たとえば、Meeting Server は 1 つの SRV レコードのみを _sipinternaltls._tcp, etc...it will not save 2 different RRs for _sipinternaltls._tcp.
dns del rr <owner-name> <type> **dns del rr _sip._tcp.example.com. SRV** **dns del rr sipserver.local. A**	
dns lookup <a|aaaa|srv> <hostname> **dns lookup srv _sip._tcp.example.com**	lookup は、SRV の結果を「ドリル」します。つまり、SRV レコードがドメイン名を返す場合、これは A および AAAA ルックアップによって解決されます。
dns flush	これは、Meeting Server の DNS キャッシュをフラッシュします。

4 ファイアウォールコマンド

MMP は、メディアインターフェイス用のシンプルなファイアウォールルールの作成をサポートします。インターフェイスでファイアウォールルールを設定した後、そのインターフェイスでファイアウォールを有効にしてください。

注：これは、完全なスタンドアロン ファイアウォール ソリューションに代わるものではありません。

ファイアウォールルールは、インターフェイスごとに個別に指定する必要があります。

インターフェイスの各ファイアウォールルールはタグで識別されます。これらは、ステータス出力で確認できます。次に例を示します。

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

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

注意：SSH を使用すると、ルールにエラーが発生した場合に SSH ポートがアクセス不能になるため、シリアルコンソール（使用可能な場合）を使用してファイアウォールを設定することをお勧めします。

コマンド/例	説明/注意事項
firewall <iface> default (allow|deny) **firewall a default deny**	インターフェイスでファイアウォールを有効にする前に、このコマンドを使用してデフォルトポリシーを設定する必要があります。 許可ポリシーは、どのルールにも一致しないすべてのパケットを許可し、拒否ポリシーは、どのルールにも一致しないすべてのパケットを破棄します ルールが設定されていない場合、インターフェイス a のすべてのパケットがドロップされます。
firewall <iface> enable **firewall <iface> disable**	指定されたインターフェイスのファイアウォールを有効にします。 指定されたインターフェイスのファイアウォールを無効にします。
firewall <iface> **firewall a**	指定されたインターフェイスの現在のファイアウォール設定を表示します。 インターフェイス a のステータスとルールセットを表示します。

コマンド/例	説明/注意事項
firewall <iface> allow <port> [/<proto>] [from <host>[/<prefix>]] **firewall <iface> deny <port> [/<proto>] [from <host>[/<prefix>]]**	これらのコマンドでルールを追加します。 <port> 引数は、数値（「80」など）または IANA サービス名レジストリからのサービス名（「http」など）として指定できます。 protocol 引数は、tcp または udp のいずれかです。省略した場合、ルールは TCP パケットと UDP パケットの両方に一致します。
firewall a allow http/tcp	インターフェイス A のポート 80 で TCP パケットを許可します。
firewall a deny 678	メディアインターフェイス A のポート 678 ですべてのパケットをドロップします。
firewall a allow ssh from 192.168.1.0/28	オプションの **from**句は、ルールが適用されるホストを制限します。これは、IPv4 または IPv6 アドレスとして指定されます。 オプションの prefix は、サブネットを示します。 192.168.1.0 から 192.168.1.255 までの 256 個の IPv4 アドレスからインターフェイス a への SSH アクセスを許可します。
firewall <iface> delete <tag> **firewall a delete 0**	ルールを削除するには、このコマンドでタグを使用します。 このテーブルの上にある単一のルールを削除します。

5 LDAP コマンド

新しい **ldap** オプションが **user add** MMP コマンドに追加され、LDAP サーバ、ディレクトリ検索パラメータ、TLS 設定の詳細を設定し、LDAP 認証を有効または無効にできるようになりました。

LDAP ユーザの追加を有効にするために、新しいオプション［**ldap**］がコマンドに追加されました。

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

注：Meeting Server API は、LDAP 認証によるユーザへのアクセスをサポートしていません。

`help ldap` **コマンドの出力は次のとおりです。**

cms> help ldap

MMP ユーザ用の LDAP クライアント

構成：

ldap
ldap server <hostname|address> <port>
ldap protocol (ldap|ldaps)
ldap binddn <username>
ldap basedn <base DN>
ldap login_attr <attribute>
ldap filter <filter>
ldap remove <binddn|filter|trust>
ldap trust <crt bundle>
ldap verify (enable|disable)
ldap min-tls-version <minimum version string>
ldap enable
ldap disable
ldap status

注：
user list MMP コマンドが拡張され、ログインした LDAP ユーザが含まれるようになりました。LDAP ユーザに適用される **user rule** パラメータは、max_failed_logins、max_idle、および max_sessions のみです。このコマンドの他のパラメータは、LDAP ユーザには適用されません。**user expire** MMP コマンドは、LDAP ユーザについてはサポートされていません。

コマンド/例	説明/注意事項
ldap	LDAP 情報を表示します。
ldap server <hostname|address> <port>	LDAP サーバ ホスト名または IP アドレスおよびポート番号を指定します。これは必須です。
ldap protocol (ldap|ldaps)	使用する LDAP プロトコルを指定します。LDAP サーバーへの安全な接続を使用するには、ldaps を使用する必要があります。プロトコルの指定は必須です。
ldap binddn <username> **ldap binddn cn=binduser,oi=user,dc=domain,dc=com** **ldap binddn "cn=bind user,o=My Company,dc=domain,dc=com"** **ldap binddn domain\\username**	検索のためにディレクトリ サーバーにバインドする識別名を追加します。bindn パラメータはオプションです。指定しない場合、匿名バインド要求が使用されます。 バインド ユーザは、ディレクトリ内の検索権限を持っている必要があります。このコマンドは、オプションのバインド パスワードの入力を求めます。 引数にスペースが含まれている場合は、引数を引用符で囲む必要があります。バックスラッシュが含まれている場合は、前にバックスラッシュを付けてエスケープする必要があります。
ldap basedn <base DN>	検索ベースに使用する基本識別名（DN）を指定します。basedn の指定は必須です。 引数にスペースが含まれている場合は、引数を引用符で囲む必要があります。バックスラッシュが含まれている場合は、前にバックスラッシュを付けてエスケープする必要があります。
ldap login_attr <attribute>	ユーザを一意に識別する、uid、userPrincipalName、sAMAccountName などの LDAP 属性名を指定します。ログインを成功させるには、属性値が事前構成された MMP ユーザー名と一致している必要があります。属性の指定は必須です。
ldap filter <filter> **ldap filter (&(objectClass=*) (memberOf=CN=admins,DC=example,DC=com))**	LDAP 検索フィルタを設定します。フィルタの指定はオプションです。フィルタが指定されていない場合、デフォルト値（objectClass=*）が使用されます。 有効な LDAP フィルタ構文を使用する必要があり、括弧で囲む必要があります。
ldap remove (binddn|filter|trust)	以前に設定された binddn、filter、または trust パラメータを削除します。

コマンド/例	説明/注意事項
ldap trust <crt bundle>	特定の証明書のバンドルを使用して証明書を検証するようにシステムを構成します。 LDAP サーバーへの安全な接続を使用するには、信頼できる CA を使用してこれを構成する必要があります。
ldap verify (enable|disable)	LDAP サーバーへの接続の証明書検証を有効または無効にします。 LDAP サーバーへの安全な接続を使用するには、証明書の検証を有効にする必要があります。無効にすると、Meeting Server は信頼証明書を要求または確認しません。
ldap min-tls-version <minimum version string>	システムが使用する最小の TLS バージョンを構成します。可能な値は 1.0、1.1、および 1.2 です。デフォルトはバージョン 1.2 です。
ldap enable	LDAP サービスを有効にします。
ldap disable	LDAP サービスを無効にします。
ldap status	ldap サービスのステータスを次のように表示します。「実行中」：サービスが実行中であることを示します。 「実行されていません」：サービスは有効になっていますが、実行されていません。詳細についてはログを確認してください。 「無効」：サービスは無効になっています

6 スケジューラコマンド

会議のスケジュールは、新しいスケジューラコンポーネントによって有効にされ、新しい **scheduler** MMP コマンドによって設定できます。

電子メールサーバの設定の詳細は、以下にリストされている新しい **scheduler** MMP コマンドを介して提供されます。

コマンド/例	説明/注意事項
scheduler **scheduler status**	スケジューラの現在のステータスを表示します。
scheduler (enable | disable)	スケジューラを有効または無効にします。
scheduler restart	スケジューラを再起動します。
scheduler https listen <interface> <port>	スケジューラがリッスンする interface:port ペアを設定します。
scheduler https listen none	スケジューラの管理 API インターフェイスを無効にします。
scheduler https certs <key-file> <crt- fullchain-file>	管理 API で使用されるサーバー証明書だけでなく、アウトバウンド接続を行うときに使用される証明書も構成します。（例：c2w リンクまたは Call Bridge への API 呼び出し）
scheduler https certs none	管理 API の証明書の設定を削除します。
scheduler c2w certs <key-file> <crt- fullchain-file>	Web Bridge 3 に提示される証明書バンドルを構成します。
scheduler c2w certs none	Web Bridge 3 への TLS 接続の証明書構成を削除します。
scheduler c2w trust <crt-bundle>	Web Bridge への接続を検証するためのトラスト バンドルを構成します。
scheduler c2w trust none	スケジューラのトラスト ストアから Web Bridge 3 の証明書バンドルを削除します。
scheduler email server <hostname | address> <port>	スケジューラが電子メールを送信する SMTP サーバーを構成します。
scheduler email server none	スケジューラから電子メール サーバー構成を削除します。
scheduler email username <smtp user-name>	SMTP サーバーでの認証に使用される電子メール アカウントを構成します。このアカウントには、会議の主催者の代わりに電子メールを送信できる適切な権限が必要です。 **注：**参加者への電子メールは、このコマンドを使用して構成されたアカウントから送信されるのではなく、会議の主催者の差出人アドレスを使用して送信されます。

コマンド/例	説明/注意事項
scheduler email remove username	SMTP 認証用に構成された電子メール ユーザー名を削除します。
scheduler email protocol <smtp | smtps>	電子メール サーバーとのスケジューラの通信を次のように指定します。 smtp：プレーン テキスト TCP（smtp）経由 smtps：暗号化された TLS チャネル経由
scheduler email auth (enable | dis-able)	SMTP 認証を有効または無効にします。
scheduler email starttls (enable | dis- able)	SMTP 接続の opportunistic TLS を有効または無効にします。
scheduler email trust <bundle> | none	（オプション）電子メール サーバーのトラスト バンドルの構成を許可します。構成されている場合、構成されたバンドルを使用して電子メール サーバーの証明書の検証が行われます。 構成されていない場合、証明書の検証は行われません。
scheduler email common-address <address@mail.domain> "<Display name>"	Meeting Server での共通の電子メール アドレスと表示名を設定します。スケジューラは、共通の電子メールアドレスから参加者に会議の招待状を送信します。 空白の場合、スケジューラは主催者の電子メールアドレスから電子メール招待状を送信します。
scheduler email common-address none	設定されている共通メールアドレスと表示名を削除します。
scheduler timedLogging	時間指定ログ ステータスを取得します。
scheduler timedLogging (webBridge|ap- i|email) <time>	指定された期間のロギングをアクティブにします。

7 証明書によるプロビジョニング

次の PKI（公開キーインフラストラクチャ）コマンドを使用します。

キーファイルには、PEM または DER としてエンコードされた RSA または DSA キーが含まれている必要があり、ファイル名拡張子は .key、.pem、または .der である必要があります。証明書ファイルは、PEM または DER としてエンコードされた x509 証明書である必要があり、ファイル名拡張子は .crt、.cer、.pem、または .der である必要があります。

ファイル名には、英数字、ハイフン、アンダースコア文字を含めることができ、その後に上記のいずれかの拡張子を付けることができます。サービスごとの証明書とキーファイル名を選択できます。すべてのサービスに同じファイルのペアを使用することもできます。

秘密キーと証明書ファイルは SFTP 経由でアップロードする必要があります。

コマンド/例	説明/注意事項
PKI	現在の PKI の使用状況を表示します。
pki list	PKI ファイル、つまり秘密キー、証明書、および証明書署名要求（CSR）をリストします。
pki inspect <filename>	ファイルを検査し、ファイルが秘密キー、証明書、CSR、または不明であるかどうかを示します。証明書の場合は、さまざまな詳細が表示されます。ファイルに証明書のバンドルが含まれている場合、バンドルの各要素に関する情報が表示されます。 PEM および DER の両方の形式のファイルが処理されます。
pki match <key> <certificate>	このコマンドは、指定されたキーとシステム上の証明書が一致するかどうかを確認します。秘密キーと証明書は、1 つの使用可能な ID の 2 つの半分であり、HTTPS などのサービスに使用する場合は一致する必要があります。
pki verify <cert> <cert bundle/CA cert> [<CA cert>] **pki verify server.pem bundle.pem rootca.pem** **pki verify server.pem bundle.pem**	証明書は認証局（CA）によって署名される場合があり、CA は中間 CA 証明書の「証明書バンドル」と、場合によっては CA 証明書を独自のファイルで提供します。証明書が CA によって署名されていることと、証明書バンドルを使用してこれを表明できることを確認するには、次のコマンドを使用します。
pki unlock <key>	多くの場合、秘密キーはパスワードで保護されます。Meeting Server で使用するには、キーのロックを解除する必要があります。 このコマンドは、ターゲットファイルのロックを解除するためのパスワードの入力を求めます。ロックされた名前は、同じ名前のロック解除されたキーに置き換えられます

コマンド/例	説明/注意事項
pki csr <key/cert basename> [<attribute>:<value>] **pki csr dbserver CN:server01.db.example.com subjectAltName:server02.db.example.com**	Cisco が秘密キーマテリアルの生成要件を満たしていることをユーザーが信頼できるように、秘密キーおよび関連する証明書署名要求を生成できます。 <key/cert basename> は、新しいキーと CSR を識別する文字列です（たとえば、「new」と入力すると、「new.key」ファイルと「new.csr」ファイルが作成されます）。 CSR の属性は、属性名と値のペアをコロン（「:」）で区切って指定できます。 属性は、次のとおりです。 CN：証明書に必要な commonName。commonName は、システムの DNS 名である必要があります。 OU: 組織単位 O: 組織 L: 地方 ST: 州 C: 国 emailAddress: 電子メールアドレス CSR ファイルは SFTP でダウンロードして、署名のために認証局（CA）に渡すことができます。（または、CSR ファイルを「pki sign」コマンドで使用して、証明書をローカルで生成することもできます。) 返送時には、SFTP 経由でアップロードする必要があります。その後、証明書として使用できます。 注：**pki csr <key/cert basename> [<attribute>:<value>]** は、subjectAltName を属性として取ります。subjectAltName の IP アドレスとドメイン名は、コンマ区切りのリストでサポートされています。たとえば次のようなものです。 **pki csr test1 CN:example.exampledemo.com subjectAltName:exampledemo.com** **pki csr test2 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:Virginia subjectAltName:exampledemo.com, 192.168.1.25,server.exampledemo.com, join.exampledemo.com, test.exampledemo.com** 証明書のサイズとチェーン内の証明書の数を最小限に抑えてください。そうしないと、TLS ハンドシェイクのラウンドトリップ時間が長くなります。

コマンド/例	説明/注意事項
pki selfsigned <key/cert basename> [<attribute>:<value>] **pki selfsigned dbca CN:"my company CA" OU:"My company" O:cms L:Raleigh ST:"North Carolina" C:US**	このコマンドを使用して、自己署名証明書を生成できます。 <key/cert basename> は、生成されるキーと証明書を識別します。たとえば、「pki selfsigned new」と入力すると、new.key と new.crt（自己署名証明書）が生成されます。 証明書の属性は、属性名と値のペアをコロン（「:」）で区切って指定できます。属性は、次のとおりです。 CN: commonName。証明書がエンドエンティティ証明書として使用される場合、commonName は関連するサービスの DNS 名である必要があります。 OU: 組織単位 O: 組織 L: 地方 ST: 州 C: 国 emailAddress: 電子メールアドレス 自己署名証明書を使用して CSR に署名できます。これらは、データベースクラスタなどの内部サービスに展開するのに役立ちます。Web サービスなどの外部サービスの場合は、外部 CA を使用します。
pki sign <csr/cert basename> <CA key/cert basename> **pki sign dbserver dbca** **pki sign dbclient dbca**	このコマンドは <csr/cert basename> によって識別される CSR に署名し、<CA key/cert basename> によって識別される CA 証明書とキーで署名された、同じベース名を持つ証明書を生成します。 ファイル <csr/cert basename> および <CA key/cert basename> は、コマンド「pki csr」および「pki selfsigned」によってそれぞれ生成されている必要があります。
pki pkcs12-to-ssh <username> pki pkcs12-to-ssh john	PKCS#12 ファイルに保存されている公開 SSH キーを使用できますが、最初に処理する必要があります。このコマンドは、<username>.pub という名前でアップロードされた PKCS#12 ファイルから使用可能な公開キーを抽出します。pkcs#12 ファイルのパスワードを入力するように求められます。完了後、pkcs#12 ファイルはパスワード保護なしで使用可能なキーに置き換えられます。 注：pkcs#12 ファイルに含まれるその他のデータはすべて失われます。 このコマンドを実行することで、ユーザー john のアップロードされた PKCS#12 ファイル john.pub のキーを使用可能にすることができます。

コマンド/例	説明/注意事項
pki	現在の PKI の使用状況を表示します。
pki list	PKI ファイル、つまり秘密キー、証明書、および証明書署名要求（CSR）をリストします。
pki	現在の PKI の使用状況を表示します。
pki inspect <filename>	ファイルを検査し、ファイルが秘密キー、証明書、CSR、または不明であるかどうかを示します。証明書の場合は、さまざまな詳細が表示されます。ファイルに証明書のバンドルが含まれている場合、バンドルの各要素に関する情報が表示されます。 PEM および DER の両方の形式のファイルが処理されます。
pki match <key> <certificate>	このコマンドは、指定されたキーとシステム上の証明書が一致するかどうかを確認します。秘密キーと証明書は、1 つの使用可能な ID の 2 つの半分であり、callbridge などのサービスに使用される場合は一致する必要があります。
pki verify <cert> <cert bundle/CA cert> [<CA cert>] **pki verify server.pem bundle.pem rootca.pem** **pki verify server.pem bundle.pem**	証明書は認証局（CA）によって署名される場合があり、CA は中間 CA 証明書の「証明書バンドル」と、場合によっては CA 証明書を独自のファイルで提供します。証明書が CA によって署名されていることと、証明書バンドルを使用してこれを表明できることを確認するには、次のコマンドを使用します。
pki unlock <key>	多くの場合、秘密キーはパスワードで保護されます。Meeting Server で使用するには、キーのロックを解除する必要があります。 このコマンドは、ターゲットファイルのロックを解除するためのパスワードの入力を求めます。ロックされた名前は、同じ名前のロック解除されたキーに置き換えられます

コマンド/例	説明/注意事項
pki csr <key/cert basename> [<attribute>:<value>] **pki csr example CN:www.example.com OU:"My Desk" O:"My Office" L:"San Jose" ST:California C:US**	Cisco が秘密キーマテリアルの生成要件を満たしていることをユーザーが信頼できるように、秘密キーおよび関連する証明書署名要求を生成できます。 <key/cert basename> は、新しいキーと CSR を識別する文字列です（たとえば、「new」と入力すると、「new.key」ファイルと「new.csr」ファイルが作成されます）。 CSR の属性は、属性名と値のペアをコロン（「:」）で区切って指定できます。属性は、次のとおりです。 CN：証明書に必要な commonName。commonName は、システムの DNS 名である必要があります。 OU: 組織単位 O: 組織 L: 地方 ST: 州 C: 国 emailAddress: 電子メールアドレス CSR ファイルは SFTP でダウンロードして、署名のために認証局（CA）に渡すことができます。（または、CSR ファイルを「pki sign」コマンドで使用して、証明書をローカルで生成することもできます。) 返送時には、SFTP 経由でアップロードする必要があります。その後、証明書として使用できます。 注：1.6.11 から、**pki csr <key/cert basename> [<attribute>:<value>]** は、属性として subjectAltName を取るようになりました。subjectAltName の IP アドレスとドメイン名は、コンマ区切りのリストでサポートされています。たとえば次のようなものです。 **pki csr test1 CN:example.exampledemo.com subjectAltName:exampledemo.com** **pki csr test2 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:Virginia subjectAltName:exampledemo.com, 192.168.1.25,exampledemo.com, server.exampledemo.com,join.exampledemo.com, test.exampledemo.com** 証明書のサイズとチェーン内の証明書の数を最小限に抑えてください。そうしないと、TLS ハンドシェイクのラウンドトリップ時間が長くなります。

コマンド/例	説明/注意事項
pki selfsigned <key/cert basename> [<attribute>:<value>]	このコマンドを使用して、自己署名証明書を生成できます。 <key/cert basename> は、生成されるキーと証明書を識別します。たとえば、「pki selfsigned new」と入力すると、new.key と new.crt（自己署名証明書）が生成されます。 CSR の属性は、属性名と値のペアをコロン（「:」）で区切って指定できます。属性は、次のとおりです。 CN：証明書に必要な commonName。commonName は、システムの DNS 名である必要があります。 OU: 組織単位 O: 組織 L: 地方 ST: 州 C: 国 emailAddress: 電子メールアドレス CSR ファイルは SFTP でダウンロードして、署名のために認証局（CA）に渡すことができます。返送時には、SFTP 経由でアップロードする必要があります。その後、証明書として使用できます。 証明書のサイズとチェーン内の証明書の数を最小限に抑えてください。そうしないと、TLS ハンドシェイクのラウンドトリップ時間が長くなります。
pki sign <csr/cert basename> <CA key/cert basename>	このコマンドは <csr/cert basename> によって識別される CSR に署名し、<CA key/cert basename> によって識別される CA 証明書とキーで署名された、同じベース名を持つ証明書を生成します。 ファイル <csr/cert basename> および <CA key/cert basename> は、コマンド「pki csr」および「pki selfsigned」によってそれぞれ生成されている必要があります。
pki pkcs12-to-ssh <username> **pki pkcs12-to-ssh john**	PKCS#12 ファイルに保存されている公開 SSH キーを使用できますが、最初に処理する必要があります。このコマンドは、<username>.pub という名前でアップロードされた PKCS#12 ファイルから使用可能な公開キーを抽出します。pkcs#12 ファイルのパスワードを入力するように求められます。完了後、pkcs#12 ファイルはパスワード保護なしで使用可能なキーに置き換えられます。 注：pkcs#12 ファイルに含まれるその他のデータはすべて失われます。 このコマンドを実行することで、ユーザー john のアップロードされた PKCS#12 ファイル john.pub のキーを使用可能にすることができます。

7.1 TLS 証明書の検証

注：TLS 証明書の検証が有効になっている場合は、リモートデバイスの証明書にサーバ認証属性とクライアント認証属性の両方が定義されていることを確認してください。これにより、発信と着信の両方の TLS 接続が確実に受け入れられます。

注：LDAP サーバーがセキュアな接続で設定されている場合、MMP で **`tls ldap`** コマンドを使用して TLS 証明書の検証が設定されるまで、接続は完全にセキュアではありません。

Meeting Server は、デフォルトではすべてのサービス、つまり SIP、LDAP、SYSLOG、HTTPS（着信接続：API、Web Admin、Web Bridge 3、発信接続：CDR）および RTMPS について、TLS 1.2 および DTLS 1.2 以上を使用します。TLS 1.2 が導入されていない古いソフトウェアとの相互運用に必要な場合、プロトコルの下位バージョンを SIP、LDAP、HTTPS サービスの最小 TLS バージョンとして設定できます。以下の **`tls <service> min-tls-version <minimum version string>`** および **`tls min-dtls-version <minimum version string>`**コマンドを参照してください。

注：`tls` 設定の変更を適用するには、Call Bridge の再起動が必要です。ただし、 **`tls syslog`** 構成が変更されている場合は、syslog サービスを無効にしてから、Call Bridge の再起動後に有効にする必要があります。

注：Meeting Server の将来のバージョンでは、TLS 1.0 が完全に削除される可能性があります。

コマンド/例	説明/注意事項
`tls <service>` **`tls ldap`**	sip|ldap|syslog|dtls|webadmin|rtmps などのサービスの設定を表示します（注：RTMPS はバージョン 3.1 からサポートされます）。 LDAP の設定を表示します。
`tls <service> trust <crt bundle>` **`tls ldap trust ldap.crt`**	特定の証明書バンドルを使用してリモートサービスの証明書を検証するようにシステムを設定します。
`tls <service> verify (enable|disable|ocsp)`	サービスの証明書検証を有効/無効にします。有効にすると、Meeting Server がリモートサービスの証明書の検証に失敗した場合、接続は切断されます。 リモートサービスがステープルされた OCSP 応答を返して証明書の失効ステータスを確認するという追加の要件を使用して検証を有効にします。 システムが証明書の有効性を検証できない場合、または証明書の失効ステータスが不明または失効である場合、リモートサービスへの接続は中止されます。

コマンド/例	説明/注意事項
tls sip ciphers <cipher string>	tls cipher コマンドを使用する必要がある場合の説明については、以下を参照してください。暗号文字列の形式は、OpenSSL（https://www.openssl.org/docs/manmaster/man1/openssl-ciphers.html#CIPHER-LIST-FORMAT）で使用される、コロンで区切られた暗号のリストです。 暗号サポートの現在のデフォルトは次のとおりです。 "ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:RSA+AES:!aNULL:!MD5:!DSS:!3DES"（バージョン 2.4.2 まで） "ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:RSA+AES:!aNULL:!MD5:!DSS:!3DES:!aDH:! aECDH"（バージョン 2.4.3 以降） ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:RSA+AES:!aNULL:!MD5:!DSS:!3DES:!aDH:!aECDH **注：**":!aDH:!aECDH:!SEED:!eNULL:!aNULL:!ARIA:!AESCCM8" は、非常に弱い暗号を禁止するために、設定された暗号文字列に自動的に追加されます。
tls <service> min-tls-version <minimum version string> **tls sip min-tls-version 1.1** **tls ldap min-tls-version 1.1**	このコマンドを使用して、Meeting Server が使用するデフォルトの TLS バージョンを変更します。（バージョン 2.3 から）。注：TLS の最小バージョンを変更する場合は、**callbridge restart** コマンドを使用して Call Bridge サービスを再起動する必要があります。 Meeting Server は、すべてのサービスに最低でも TLS 1.2 を使用します。TLS 1.2 が導入されていない古いソフトウェアとの相互運用に必要な場合、SIP、LDAP、HTTPS サービスの最小 TLS バージョンをより低いバージョンのプロトコルに設定できます。 SIP には TLS バージョン 1.1 以降を使用します。 LDAP には TLS バージョン 1.1 以降を使用します。
tls min-dtls-version <minimum version string> **tls min-dtls-version 1.1**	システムが使用する最小の DTLS バージョンを設定します。（バージョン 2.3 から）。注：DTLS の最小バージョンを変更する場合は、 **callbridge restart** コマンドを使用して Call Bridge サービスを再起動する必要があります。（バージョン 2.3 から） DTLS 1.2 を導入していない古いソフトウェアとの相互運用が必要な場合は、より低いバージョンのプロトコルを使用するように DTLS を設定します。

デフォルトでは、Meeting Server は、TCP ポート 5061 の SIP TLS を含め、すべての TLS 接続に安全な暗号のみを使用します。ただし、これは、Meeting Server が古くて安全性の低いデバイスとの間で TLS コールを実行できない可能性があることを意味する場合があります。展開に古いキットがある場合は、この tls ciphers コマンドを使用して、古いデバイスに受け入れられる暗号のリストを指定します。暗号の詳細については、『 Openssl ガイド 』を参照してください。

デバイスが安全な暗号を処理できないときの症状には、次のものがあります。

- デバイスへの SIP TLS コールが失敗する
- デバイスで HTTPS アクセスが機能しない
- ログにエラーが表示される

8 Cisco Meeting Server を設定するためのコマンド

注：Cisco Meeting Server 2000 の正常性を確認するには、Cisco UCS Manager を使用します。

コマンド/例	説明/注意事項
稼働時間	Meeting Server が最後に再起動されてからの時間を表示します。
shutdown	プロンプトに対して Y を入力すると、Meeting Server の電源がオフになります。 注：Cisco Meeting Server 2000 の MMP を介してシャットダウンすることはできません。ブレードサーバの電源を切断するには、まず Cisco UCS Manager 上で電源を切断します。
hostname <name> **hostname mybox.mydomain**	サーバのホスト名を設定します。 注：このコマンドを実行した後は、再起動が必要です。
timezone	現在設定されているタイムゾーンを表示します。
timezone <timezone name> **timezone Europe/London**	Meeting Server のタイムゾーンを設定します。Meeting Server は、標準の IANA タイムゾーンデータベースを使用します。リストについては、このリンクを参照してください。 注：このコマンドを実行した後は、再起動が必要です。
timezone list	使用可能なタイムゾーンの完全なリストを出力します。 注：GMT と時差のあるタイムゾーン（Etc/GMT<offset>）を使用することを選択した場合、offset には POSIX 形式の記号を使用します。結果として、香港のタイムゾーンは Etc/GMT-8 であり、Etc/GMT+8 ではありません。
ntp server add|del <host>	NTP サーバーを構成/削除します。<host> は名前または IP アドレスにすることができます
ntp status	NTP サーバのステータスを確認します。
ntp server list	設定済みの NTP サーバのリストを表示します。
ntp groupkey <keyfile>	オートキーサポート用の NTPv4 グループキーを追加します。
ntp autokey (enable|disable)	オートキーサポートを有効または無効にします。
ntp groupkey group.key **ntp autokey enable**	たとえば、SFTP を使用してグループキーファイルを「group.key」にアップロードし、これらのコマンドで設定できます。
date	現在のシステム時間（UTC）と現地時間を表示します。

コマンド/例	説明/注意事項
date set <date> <time> **date set 2013-08-17 13:04**	日付と時刻を設定します。このコマンドは、仮想化展開、および NTP サーバを使用しないサーバ展開でのみ必要です。 日付と時刻に使用できる形式は次のとおりです。 - ISO 8601 形式（%Y-%m-%d）と、スペースで区切られた 24 時間制の時刻。 - %m/%d/%y プラス 24 時間制の時刻。 注：NTP サーバを使用するシステムのユーザは、このコマンドを使用する必要はありません。
reboot	Meeting Server を再起動します。 注：Meeting Server を再起動すると、すべての通話が切断されます。プロセスが完了するまで数分かかります。
license	このコマンドは、仮想化サーバにのみ適用されます。 Meeting Server のライセンスステータスをチェックし、ライセンスされた機能を表示します。例： Feature: callbridge status: Activated expiry: 2014-JUl- 01 (12 days remain)
callBridge **callbridge listen (interface allowed list|none)** **callbridge listen a** **callbridge listen none** **callbridge prefer <interface>** **callbridge certs <key-file> <cert-file>[<crt-bundle>]** **callbridge certs none** **callbridge trust cluster <trusted cluster certificate bundle>**	現在のステータスを表示します。 Call Bridge がリッスンする 1 つ以上のインターフェイス（A、B、C、または D から選択）を設定します。 Call Bridge を停止し、サービスのリッスンを無効にします。ただし、Call Bridge は有効のままです。 インターフェイス許可リストから 1 つのインターフェイスを「優先」SIP インターフェイスとして選択します。このインターフェイスは、ルーティングまたはヒューリスティックを使用して一意のインターフェイスを選択できない場合に、連絡先アドレスとして使用されます。 Meeting Server とオプションで CA によって提供された CA 証明書バンドルのキーファイル名証明書ファイル名を定義します。（第 7 章も参照。） 証明書の設定を削除します。 特定の証明書バンドルを使用してクラスタ内の Call Bridge の ID を検証するように、Call Bridge を設定します。バンドルは、証明書チェーン、または信頼できる証明書の許可リストのいずれかです。（バージョン 2.4 から）。

コマンド/例	説明/注意事項
callbridge trust cluster none	Call Bridge クラスタの証明書バンドルを Call Bridge 信頼ストアから削除します。（バージョン 2.4 から）。
callbridge trust branding <trusted branding server certificate whitelist>	指定された証明書を使用してブランディングサーバ証明書を検証するように Call Bridge を設定します。（3.5 から）。 注：ブランディングサーバーが HTTPS 経由でホストされている場合、Meeting Server とブランディングサーバーの証明書は、有効な CA または同じ CA によって署名されている必要があります。ブランディングサーバーの証明書が有効な CA によって署名されていない場合、Meeting Server はブランディングサーバーとの通信に失敗することがあります。
callbridge wc3jwt expiry <expiry time in hours>	Web アプリケーションのセッションタイムアウト（時間）を設定します。1 ～ 24 の整数を指定できます。設定しない場合のデフォルトは 24 です。
callbridge restart	**注：**変更を適用するには、Call Bridge を再起動します。 コアメディアサービスを再起動します。注：Meeting Server を再起動すると、すべての通話が切断されます。プロセスが完了するまで数分かかります。
syslog server add <hostname> [<port>] **syslog server del <hostname>** **syslog server add tls:syslog.example.com 514**	Meeting Server は、TCP（UDP ではなく）を介してリモート Syslog サーバにログファイルを送信できます。 ポートのデフォルトは 514 です。 転送中の syslog データを保護するために TLS を使用する必要があることを指定するには、リモートサーバのホスト名/IP アドレスの前に「tls:」を付けます。
syslog	現在の syslog 設定を一覧表示します。
syslog enable **syslog disable**	syslog メカニズムを有効にします。
syslog audit add <hostname> **syslog audit add audit-server.example.org** **syslog audit del <hostname>**	監査ログが送信されるサーバを定義します。監査ログは、完全なシステムログのサブセットであり、セキュリティイベント（ログインなど）と設定変更に関する情報が含まれています。 注：これらの syslog audit コマンドは、監査ロールを持つユーザのみが実行できます。
audit http (enable|disable)	HTTP トランザクションの詳細な監査を有効/無効にします。
syslog tail [<number of lines>]	最新のログメッセージを表示します。デフォルトでは、これは 10 件のメッセージですが、オプションの引数で数を変更できます。
syslog page	完全なログを対話的に表示します。スペースバーを押すと、ログメッセージの次のページが表示されます。q を押して終了します。

コマンド/例	説明/注意事項
syslog follow	リアルタイムで書き込まれたログメッセージを表示します。Ctrl+C を押すと、出力を停止して、管理シェルに戻ります。
syslog search <string> **syslog search error**	特定のパターンに一致するメッセージのみを表示します。 注：現在のユーザが監査ロールを持っている場合、tail コマンドと search コマンドは監査ログメッセージを表示します。それ以外の場合は、システムログからのメッセージを表示します。システムログのダウンロードの詳細については、セクション 12.6 を参照してください。
syslog rotate <filename> **syslog rotate mylog**	ログファイルを指定されたファイル名のファイルに永続的に保存し、アクティブなシステムログを空にします。保存したファイルは SFTP を使用してダウンロードできます。
version	Meeting Server に現在インストールされているソフトウェアリリースを表示します。

8.1 連邦情報処理標準

Meeting Server は、FIPS 140-2 レベル 1 認定ソフトウェア暗号化モジュールを提供します（http://en.wikipedia.org/wiki/FIPS_140-2）。FIPS 認定の Cisco Meeting Server ソフトウェアリリースについては、このリンクをクリックしてください。

FIPS モードを有効にすると、暗号化操作がこのモジュールを使用して実行されるため、暗号化操作が FIPS で承認された暗号化アルゴリズムに制限されます。

コマンド/例	説明/注意事項
fips	FIPS モードが有効になっているかどうかを表示します。
fips enable **fips disable**	ネットワークトラフィックのすべての暗号操作について、FIPS-140-2 モード暗号化を有効または無効にします。FIPS モードを有効または無効にした後は、リブートが必要です。
fips test	組み込み FIPS テストを実行します。

9 MMP ユーザアカウントコマンド

MMP ユーザアカウントロールは次のとおりです。

- admin：MMP 管理者。すべてのタスクを行うことが許可されています。
- crypto：MMP 暗号オペレータ。暗号関連のタスクを行うことが許可されています。
- audit：監査ログを Syslog サーバに送信します（これを行う方法については、導入ガイドの「リモート Syslog サーバ」のセクションを参照してください）。
- appadmin：Web Admin インターフェイスを介してアプリケーションレベルの設定を実行できます。
- api：API を使用できます。「api」ロールは、以前は Web Admin インターフェイスを介して設定されていたことに注意してください。
- ldap：追加されたユーザは LDAP ユーザです。

注：このセクションのコマンドでセットアップされたユーザアカウントと、Active Directory を使用してセットアップされ、ユーザが Cisco Meeting App にログインして電話をかけるときのアカウントを混同しないでください。

特に明記されていない限り、以下のコマンドでは、管理者権限を持つ MMP アカウントにログインする必要があります。

コマンド/例	説明/注意事項
user add <username> (admin|crypto|audit|appadmin|api) [ldap]	指定されたタイプ（上記を参照）の新しい MMP ユーザを作成するか、作成されたユーザが LDAP ユーザです。 意図したパスワードが設定されていることを確認するために 2 回入力する必要があるユーザのパスワードの入力を求めます。 最初のログイン時に、ユーザは新しいパスワードを設定するように求められます。 **注意：**LDAP ユーザを除き、パスワードは 6 か月後に期限が切れます。
user del <username>	システムからユーザを削除します。 **注意**: **user del <username>**は、すでにログインしているを自動的にログアウトしません。**user list** を使用して、ユーザーがログインしているかどうかを確認し、ログインしている場合は、**user evict <username>**を使用して、そのユーザーのすべてのセッションを終了してから、ユーザーを削除することをお勧めします。
user list	ユーザ、ユーザのロール、パスワードの有効期限、およびログインしているかどうかのリストを表示します。

コマンド/例	説明/注意事項
user info <username>	ロール、最後のログイン、最後のログイン以降の失敗したログイン試行回数、最後にパスワードが変更された時間、パスワードの有効期限、アカウントがロックされているかどうかなど、ユーザの詳細を表示します。
user evict <username>	ユーザを MMP セッションからログアウトします。注：Web Admin セッションで現在アクティブなユーザに対してこのコマンドを使用した場合、MMP セッションがフリーズし、MMP に再ログインする必要があります。 **注：**バージョン 2.9 以降、このコマンドは Cisco Meeting Server 2000 で使用できます。
user unlock <username>	失敗したログインの最大数を超えたために発生したユーザのログインのロックを解除します。
passwd [<username>]	自分のパスワードまたは他のユーザのパスワードを変更します。指示に従ってください。 username はオプションです。これにより、管理者は別のユーザのパスワードをリセットできます。引数なしで実行すると、コマンドは現在のユーザ（自分）のパスワードを変更します。現在のユーザの認証が必要です。
user expire <username>	ユーザが次回のログイン時に新しいパスワードを設定するように強制します。 注：このコマンドはユーザタイプ「api」には適用されません。彼らのパスワードは時間の経過とともに期限切れになりますが、このコマンドを使用してパスワードの変更を強制することはできません。
user host <username> add|del <hostname> **user host bob add 192.168.1.3**	ドメイン名または IP アドレスとして指定された許可リスト内のホストからのユーザのリモートアクセスを制限します。 注：**user info**コマンドは、許可されたホスト（ある場合）の現在のリストを表示します。上記を参照してください。 bob がログインしようとしたときに、リモートホストの受け入れ可能なソースアドレスのリストに 192.168.1.3 を追加します。

コマンド/例	説明/注意事項
user duty <username> <duty hours> **user duty <username> none**	ユーザの勤務時間を制限します。 duty hours パラメータは、ユーザがシステムにアクセスできる時間を示すために使用されます。形式は、日/時間範囲のエントリのリストです。日は、Mo、Tu、We、Th、Fr、Sa、Su の 2 文字表現のシーケンスです。すべての平日（土曜日と日曜日を除く日）は Wk で表され、週末は Wd で表され、すべての曜日は Al によって表されます。繰り返される日は設定されていないことに注意してください。 MoMo = 日なし、MoWk = 月曜日を除くすべての平日。 プレフィックス「!」が付いた曜日/時間範囲は、「～を除くすべて」を示します。たとえば、!MoTu は月曜日と火曜日以外を意味します。時間範囲は、2 つの 24 時間制 HHMM をハイフン「-」で区切って、開始時刻と終了時刻を示します。終了時刻が開始時刻よりも早い場合は、勤務が翌日まで続くことを示します。 複数のルールを「または」を意味する記号「|」で組み合わせることができます。たとえば、MoTu1200-1400|We1400-1500 は、月曜日または火曜日の 12:00 ～ 14:00、または水曜日の 14:00 ～ 15:00 を意味します。
user duty bob Wk0900-1700|Sa1200-1300	平日の営業時間 (9 ～ 5) および土曜日の 12:00 ～ 13:00 の間、ボブにアクセスを許可します。

9.1 パスワードの規則

パスワードは、次の 2 つの方法で強制できます。

- 脆弱なパスワードを防ぐために、新しいパスワードをチェックする辞書をアップロードできます。新しいパスワードが辞書のエントリと一致する場合、拒否されます。
    - 辞書は、各行に 1 つの語句を含む dictionary という名前のテキストファイルである必要があります。
    - 各行は、Windows の復帰改行シーケンスではなく、単一の改行文字で終了する必要があります。
    - SFTP を使用して辞書をアップロードして、チェックを有効にします。例：

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

- より安全なパスワードの使用を強制するコマンドが多数あります。これらすべてのコマンドには、管理者レベルのアクセスが必要です。

注意：パスワードは 6 か月後に期限が切れます。

注意：他の設定で管理者ログイン情報を再利用しないでください。たとえば、TURN サーバのユーザ名とパスワードは一意である必要があります。

コマンド/例	説明/注意事項
user rule max_history <number>	そのユーザの以前のパスワード数に対して新しいパスワードをチェックすることにより、パスワードの再利用を防止します。
user rule password_age <number>	パスワードの最大有効期間を日数で強制します。
user rule min_password_age <number>	パスワードをリセットできるようになるまでの最小間隔を設定することにより、パスワード履歴制御が回避されるのを防ぎます。 注：この間隔は、管理者が "user expire <username>" コマンドを入力するとオーバーライドされます。
user rule min_length <number>	パスワードの最小長を設定します。
user rule min_special <number>	次の特殊文字の最小数を設定します。（!@#$%^&*()_ +=?><,."\/）の最小数を設定します。
user rule min_uppercase <number>	パスワードの大文字の最小数を設定します。
user rule min_lowercase <number>	パスワードの小文字の最小数を設定します。
user rule longest_digits_run <number>	パスワードで許可される最大連続数字を設定します。
user rule min_digits <number>	パスワードに含めなければならない数字の最小文字数を設定します。
user rule max_repeated_char <number>	繰り返される文字の最大回数を設定します。
user rule min_changed_ characters <number>	元のパスワードと異なる必要がある新しいパスワードの文字位置の最小数を設定します。
user rule only_ascii <true|false>	パスワードを ASCII 文字に制限します。
user rule no_username <true|false>	ユーザ名を含むパスワードが設定されないようにします。
user rule no_palindrome <true|false>	回文のパスワードが設定されるのを防ぎます。

コマンド/例	説明/注意事項
user rule max_failed_logins <attempts>	LDAP 経由で認証する MMP ユーザまたは Cisco Meeting App ユーザの 15 分間のロックアウトまでに許可されるログイン失敗回数を設定します。Meeting Server で開催される会議へのゲストアクセスは影響を受けません。0 に設定すると、このルールは有効なログイン情報を持つユーザをロックアウトします。 **user rule max_ failed_logins <attempts>**を有効にするには、Call Bridge を再起動する必要があることに注意してください。変更は MMP ユーザにはすぐに適用されます。 ロックされた MMP ユーザは MMP 管理者によってロック解除できますが、ロックアウトタイマーが期限切れになる前に LDAP ユーザのロックを解除することはできません。 ログイン失敗の最大数が設定されていない場合、MMP ユーザのロックアウトメカニズムは無効になりますが、LDAP 経由で認証するユーザのログイン試行失敗回数はデフォルトで 20 回です。
user rule max_idle <number>	アカウントがロックされるまでのアイドル状態の最大日数を設定します。最小値は 1 です。 注：アイドル時間が設定されていない場合、何も適用されません。
user rule max_sessions <number>	すべてのを同時 SSH または SFTP または Web Admin セッション数 <number> に制限します。 たとえば、最大セッション数が 5 に設定されている場合、5 つの SSH、または 5 つの Web 管理、または 5 つの SFTP セッションを同時に持つことができます。
user rule max_sessions none	セッションの制限を削除します。

9.2 共通アクセスカード（CAC）統合

共通アクセスカード（CAC）は、コンピュータ機能にアクセスするための認証トークンとして使用されます。CAC には秘密キーが含まれており、この秘密キーは抽出できませんが、カード所有者のアイデンティティを証明するためにオンカードの暗号化ハードウェアで使用できます。Meeting Server は、CAC を使用した SSH および Web 管理インターフェイスへの管理者ログインをサポートしています。

コマンド/例	説明/注意事項
cac **cac enable|disable** **cac enable strict**	現在の設定を一覧表示します。 CAC ログインを有効にするには、cac enable を実行します。 これを許可された唯一のリモートログイン方法（リカバリボタンの使用を除く）にするには、cac enable strict を使用します。このコマンドは、シリアルケーブルを使用した通常のログインを無効にします。 CAC ログインを有効にする前に、サービスが設定されていることを確認するためのチェックが行われます。「strict」オプションを指定してパスワードログインをオフにする前に、「strict」を指定せずに cac enable を使用して、設定が正しいかどうかをテストすることをお勧めします。 注：クライアントログインへの証明書ベースのアクセスの拡張はベータ機能であり、テスト環境でのみ使用し、実稼働環境では使用しないでください。 注： - cac が有効になっている場合、適切なクライアントからの証明書ベースのログインを使用できます。この方法で接続するユーザは、システムにアクセスするためにパスワードを入力する必要はありません。 - cac enable strict が適用されている場合、ユーザは Cisco Meeting App にログインする前に CAC 経由でログインする必要があります。
cac issuer <issuer cert-bundle>	CAC ユーザを検証するには、SFTP を使用して発行者証明書バンドルを MMP にアップロードする必要があります。正当なログイン情報は、暗号化され、発行者証明書の 1 つによって署名されています。そうでない場合、ログインは失敗します。詳細については、サイトの暗号化担当者にお問い合わせください。
cac ocsp enable|disable	Online Certificate Status Protocol（OCSP）：OCSP は、証明書の有効性と失効状態を確認するためのメカニズムです。MMP は OCSP を使用して、ログインに使用される CAC が有効であるかどうか、特に失効していないかどうかを調べることができます。 MMP が「厳格な」CAC モードに設定されている場合（パスワードログインは許可されません。上記を参照）、証明書を失効させることにより、MMP へのアクセスを一元的に制限できます。 OCSP は、特別な設定なしで有効にできます。このモードでは、OCSP レスポンダーの URL は、MMP に提示された CAC ログイン情報から読み取られます（存在する場合）。OCSP レスポンダーが存在しない場合、または OCSP レスポンダーが利用できない場合（ダウンしている、ルーティングできないなど）、CAC ログインは失敗します。
cac ocsp responder <URL|none>	OCSP レスポンダーの URL を設定するには、このコマンドを使用します。この URL は、CAC によって提供されるすべての URL をオーバーライドします。

cac ocsp certs <key-file> <crt-file>	一部の OCSP レスポンダーでは、リクエスターが OCSP リクエストに署名する必要があります。このコマンドは、この操作のための秘密キーと（一致する）公開証明書を指定します。 OCSP レスポンダーは、署名証明書が特定の認証局（CAC 証明書の発行者など）によって署名されていることを必要とする可能性があります。これはサイトローカルの考慮事項です。
cac ocsp certs none	証明書の設定を削除します。

9.2.1 SSH ログイン設定

X509 ベースの公開キー交換は SSH クライアントで広くサポートされていないため、CAC を使用した SSH ログインには追加の設定手順が必要です。CAC からの公開 X509 証明書を抽出して、SFTP によって、SSH 公開キーとして MMP にアップロードする必要があります。CAC からパブリック X509 証明書を取得するには、さまざまな方法があります。最も簡単な方法の 1 つは、CAC 対応の Web ブラウザを使用してキーをエクスポートすることです。

Firefox と Chrome：

Firefox または Chrome ブラウザで、 https://ca.cern.ch/ca/Help/?kbid=040111 のような URL を入力します。指示に従ってログイン情報をエクスポートします。

エクスポート後、pkcs#12 ファイルを SFTP を使用して <username>.pub MMP にアップロードします。<username> は、関連付けられたユーザーのユーザー名です。次に、上記で説明されている次のコマンドを実行します。

pki pkcs12-to-ssh <username>

Internet Explorer：

IE は、CAC（パブリック）ログイン情報を DER としてエンコードされた X509 としてエクスポートできます。これは、追加の手順なしでアップロードして使用できます（pkcs#12 を参照）。

9.3 キーベースの SSH ログイン

Meeting Server に SSH 公開キーをインストールして、キーベースの認証が成功した場合に SSH ログインがパスワード認証をバイパスするようにできます。

手順の概要：

1. 公開キーに**<username>.pub**という名前を付けます（ **<username>**は、キーベースのログインを許可する既存の Meeting Server MMP です）。
2. sftp the **<username>.pub** key to the **<CMS mmp address>**
3. **<username>@<CMS mmp address>**への SSH アクセスを試します（初回はパスワードの入力を求められる場合がありますが、その後のログインではパスワードは必要ありません）。

9.4 SSH フィンガープリント検証

取得したキーに対して Meeting Server によって要求されたキーを確認するには、MMP コマンド **ssh server_key list** を使用します。

出力には、次のキーの中で、Meeting Server ホストのすべての既存のキーのサイズ、タイプ、およびフィンガープリントとともにキーのリストが表示されます。

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

10 Jabber プレゼンスを更新するようにコールブリッジを設定するためのコマンド

jabber のユーザーステータスを更新するために、次の MMP コマンドが導入されました。

コマンド/例	説明
callbridge ucm add <host-name/IP> <axl_user> <presence_user>	Meeting Server に CUCM ノードを追加します。このコマンドは、AXL ユーザーとプレゼンスユーザーのパスワードを入力するようにユーザーに求めます。
callbridge ucm del <host- name/IP>	サーバーから CUCM を削除します。
callbridge ucm <hostname/IP> axl_service status	AXL サービスのステータスを検証します。このコマンドは、AXL ユーザーのパスワードを入力するようにユーザーに促します。
callbridge imps <hostname/IP> <presence_user> presence_service status	プレゼンスサービスのステータスを検証します。このコマンドは、ユーザーにプレゼンス ユーザーのパスワードを入力するように求めます。
callbridge ucm list	ミーティングサーバーに追加された CUCM の詳細を、そのホスト名/IP、AXL ユーザー、およびプレゼンスユーザーとともに一覧表示します。

10.1 Meeting Server と Cisco Unified Communications Manager/IMP サーバー間のセキュアな通信を実現

エンティティ間に CA 証明書バンドルをインストールして検証することで、Meeting Server と Cisco Unified Communications Manager/IMP サーバー間のセキュアな通信が可能になります。

IMP サーバーの CUPS 証明書と Cisco Unified Communications Manager の Tomcat 証明書は、ミーティング サーバーにアップロードして検証する必要があります。

Cisco Unified Communications Manager および IMPS の証明書をインストールするには、次の手順を実行します。

1. SFTP クライアントを使用して Meeting Server にログインし、認証局のバンドルファイルを Meeting Server にコピーします。
2. Meeting Server の MMP に SSH で接続します。
3. 次のコマンドを使用して、CUCM と IMPS の証明書を割り当てます。
    a. Cisco Unified Communications Manager の場合：

       callbridge ucm certs <cert-bundle>

    b. IMPS の場合：

       callbridge imps certs <cert-bundle>

IMPS の TLS 証明書を確認するには、次の手順を実行します。

次のコマンドを使用して、Cisco Unified Communications Manager および IMP サーバーの TLS 検証を有効または無効にできます。

1. Meeting Server と Cisco Unified Communications Manager 間の TLS 検証を有効または無効にするには、次のコマンドを使用します。
   callbridge ucm verify <enable/disable>
2. Meeting Server と IMPS 間の TLS 検証を有効または無効にするには、次のコマンドを使用します。
   callbridge imps verify <enable/disable>
3. Call Bridges を再起動して、コマンドを使用して変更を適用します。
   callbridgerestart
4. MMP コマンドを使用して CUCM サービスを確認できます。
   callbridge imps <hostname/IP> <presence_user> presence_service status

注：Meeting Server から Cisco Unified Communications Manager または IMPS 証明書を削除するには、MMP コマンド **callbridge ucm certsnone**または **callbridge imps certsnone** をそれぞれ使用します。

コマンド/例	説明
callbridge ucm certs <cert-bundle>	Cisco Unified Communications Manager の CA の信頼できる証明書を追加します。
callbridge ucm verify <enable/disable>	Meeting Server と Cisco Unified Communications Manager 間の TLS 検証を有効または無効にします。
callbridge ucm certs none	Meeting Server と Cisco Unified Communications Manager 間の TLS 検証用に追加された証明書を削除します。
callbridge imps certs <cert-bundle>	IMP サーバーに CA の信頼できる証明書を追加します。
callbridge imps verify <enable/disable>	Meeting Server と IMP サーバー間の TLS 検証を有効または無効にします。
callbridge imps certs none	Meeting Server と IMP サーバー間の TLS 検証用に追加された証明書を削除します。

11 アプリケーション設定コマンド

11.1 Web Bridge 3 コマンド

導入ガイドの指示に従って、Web Bridge 3 をセットアップします。このセクションでは、コマンドリファレンスのみを提供します。

注：「Call Bridge to Web Bridge」プロトコル（C2W）は、callbridge と webbridge3 の間のリンクです。

Web Bridge 3 を展開して Cisco Meeting Server Web アプリ（ユーザが会議（オーディオおよびビデオ）に参加するための Cisco Meeting Server 用の新しいブラウザベースのクライアント）を使用するための MMP コマンドを以下の表に示します。

コマンド	説明
webbridge3	Web Bridge 3 の現在の値のセットを表示します。
help webbridge3	webbridge3 のすべてのサブコマンドと共にヘルプを表示します。
webbridge3 restart	Web Bridge 3 を再起動します。
webbridge3 (enable|disable)	Web Bridge 3 を有効化または無効化します。
webbridge3 https listen <*interface*:port allowed list>	Web Bridge 3 がリッスンするインターフェイスとポートをセットアップします。コマンド **webbridge3 enable** を使用して、サービスを有効化し、リッスンを開始します。ポートのデフォルト値はなく、指定する必要があります。
webbridge3 https certs <key-file> <crt- fullchain-file>	Web Bridge 3 の HTTPS 証明書を設定します。これらは Web ブラウザに対して提示される証明書であるため、認証局（CA）による署名が必要であり、ホスト名や目的などが一致している必要があります。（証明書ファイルは、エンドエンティティの証明書で始まり、ルート証明書で終わる完全な証明書チェーンです）。
webbridge3 https certs none	HTTPS 証明書の設定を削除します。

コマンド	説明
webbridge3 https frame-ancestors <frame-ancestors space-separated string> **webbridge3 https frame-ancestors none** **webbridge3 https frame-ancestors https://*.example.com https://customdomain.example2.com:8000**	これにより、管理者は、`content-security-policy` ヘッダーで返されるカスタムの上位フレーム値を指定して、Web アプリを他の Web ページに埋め込むことができます。 クラスタのセットアップでは、このコマンドを展開のすべての Web Bridge 上で設定する必要があります。 バージョン 3.2 から追加されました。
webbridge3 http-redirect (enable [port]|disable)	（オプション）HTTP 接続のポートをセットアップすることで、HTTP リダイレクトを有効化または無効化します。このポートは、Web アプリケーションが設定されているすべての Meeting Server インターフェイスに対して開かれます。着信 HTTP 接続は、着信したインターフェイスでの一致する HTTPS ポートに自動的にリダイレクトされます。**webbridge3 http-redirect enable [port]** でポートを指定しない場合、デフォルトのポートは 80 です。
webbridge3 c2w listen <*interface*:port allowed list>	C2W 接続を設定します。Web Bridge 3 がリッスンするインターフェイスとポートをセットアップします。コマンド **webbridge3 enable** を使用して、サービスを有効化し、リッスンを開始する必要があります。このアドレスとポートは、Call Bridge からのみアクセス可能にすることを推奨します。
webbridge3 c2w certs <key-file> <crt-fullchain-file>	C2W 接続の証明書を設定：C2W 接続に使用する SSL サーバ証明書を設定する必要があります。C2W 証明書は、C2W プロトコルの接続ポートに接続する Call Bridge に対してのみ提示されます。ホスト名および目的などが一致する必要があります。（証明書ファイルは、エンドエンティティの証明書で始まり、ルート証明書で終わる完全な証明書チェーンです）。
webbridge3 c2w certs none	C2W 接続証明書の設定を削除します。
webbridge3 c2w trust <crt-bundle>	Web Bridge 3 C2W サーバが Call Bridge クライアント証明書を検証し、信頼するかどうかを決定するための信頼バンドルを設定します。
webbridge3 c2w trust none	C2W 接続の信頼バンドルの設定を削除します。

コマンド	説明
webbridge3 audiopriflag (enable|disable)	Web アプリの自動優先順位付け機能を有効または無効にします。コマンドが設定されていない場合、この機能はデフォルトで有効です。 有効にする - Web アプリは低帯域幅のシナリオでビデオとコンテンツの共有をオフにします。 無効にする - Web アプリは不安定なネットワークでアクションを実行しません。
webbridge3 options <space-separated options>	指定された機能を有効にします。複数の機能を有効にする場合は、feature_names をスペースで区切ります。このコマンドは、Cisco サポートまたは Cisco EFT からの指示がある場合にのみ使用してください。これらの機能は、実稼働での使用には適していません。この機能は、再起動しても有効なままですが、アップグレード コマンドを使用すると自動的にクリアされます。（このコマンドは現在サポートされていません）。
webbridge3 options none	Webbridge options <feature_ name> コマンドを使用して以前に有効にされたすべての機能を無効にします。Cisco サポートまたは Cisco EFT からの指示がある場合にのみ使用してください。（このコマンドは現在サポートされていません）。
webbridge3 status	Web Bridge 3 の現在の設定を表示します。

11.2 TURN サーバのコマンド

Expressway（Large OVA または CE1200）は、中規模の Web アプリの要件（つまり 800 コール以下）の導入に推奨されるソリューションです。Expressway（中規模 OVA）は、小規模の Web アプリの要件（つまり 200 コール以下）の導入に推奨されるソリューションです。ただし、Web アプリの規模を大きくする必要がある導入の場合は、バージョン 3.1 から、必要なソリューションとして Cisco Meeting Server Web Edge を推奨します。

注：TURN Server コンポーネントは、Cisco Meeting Server 2000 では使用できません。

注：TURN サーバコンポーネントは、UDP 用の標準ポート 3478 を常にサポートします。Cisco Meeting Server Web Edge を展開する場合、API ノード /turnServers の「type」パラメータを「cms」に設定する必要があります。このパラメータが設定されていない場合、デフォルトは「standard」になり、クライアントに TCP/UDP ポート 443 を使用して TURN サーバーに接続するように指示します。「type」パラメータ値の詳細については、『Cisco Meeting Server API リファレンスガイド』の「TURN サーバー*の設定と変更*」セクションを参照してください。

TURN サーバのセットアップについては、導入ガイドで説明されています。このセクションでは、コマンドリファレンスを提供します。

コマンド/例	説明/注意事項
turn restart	TURN サーバを再起動します。
turn listen <interface allowed list|none> **turn listen a b** **turn listen none**	リッスンするインターフェイスの許可リストを設定します。リスニングを開始するには、コマンド turn enable でサービスを有効にする必要があります。 TURN サーバのリッスンを停止します。
turn tls <port|none>	TURN に使用する追加ポートを設定し、TURN の TCP 使用を有効にします。 注：3 つのサービスすべてについて、指定されたポートとポート 3478 で TCP トラフィックと UDP をリッスンするように TURN を設定します。このオプションは、TURN が UDP 以外の任意のサービスをリッスンするように設定し、TURN が 3478 以外のポートをリッスンするように設定する必要があります。
turn certs <keyfile> <certificate file> [<cert-bundle>]	Turn Server アプリケーションとオプションで CA によって提供された CA 証明書バンドルについて、秘密キーファイルと .crt ファイルの名前を定義します。（「証明書によるプロビジョニング」のセクションも参照してください。） このオプションは、'turn tls <port>' が使用されている場合に必要です。 **turn certs none**	証明書の設定を削除します。
turn (enable|disable)	TURN サーバを有効または無効にします。
turn credentials <username> <password> <realm> **turn credentials myusername mypassword example.com**	TURN サーバの長期ログイン情報を設定します。
turn public-ip <public ip> **turn delete public-ip**	TURN サーバのパブリック IP アドレスを設定します。 TURN サーバのパブリック IP アドレスを削除します。
turn high-capacity-mode (enable|disable)	TURN と Web アプリを実行している Meeting Server の Web アプリの規模の増加（デフォルト有効）のサポートが実装されています。これにより、Web Edge に Meeting Server を使用する場合のパケット処理量が増加します。Cisco サポートから推奨されている場合にのみ無効にします。（バージョン 3.1 以降）
turn short_term_credentials_mode (enable|disable)	TURN サーバの短期ログイン情報モードと長期ログイン情報モードを切り替えます。デフォルトは disable です。（バージョン 3.1 以降）

コマンド/例	説明/注意事項
turn short_term_credentials <shared secret> <realm> **turn short_term_credentials mysharedsecret example.com**	TURN サーバが短期的なクレデンシャルを使用するために必要な共有秘密とレルムを指定します。（バージョン 3.1 以降）

11.3 Web Admin インターフェイスコマンド

注：ポート 8081 は、webadmin が有効な場合、ループバックで予約されますが、webadmin が無効な場合は予約されません。ポート 8080 は常に開いています。

コマンド/例	説明/注意事項
webadmin	コンフィギュレーションを表示します。
webadmin restart	Web Admin インターフェイスを再起動します。
webadmin listen (a|b|c|d) [<port>] **webadmin listen a** **webadmin listen a 443**	Web Admin インターフェイスがリッスンするインターフェイスを設定します。リスニングを開始するには、コマンド **webadmin enable** でサービスを有効にする必要があります。 デフォルトはポート 443 です。
webadmin listen none	Web Admin インターフェイスのリッスンを停止します。
webadmin (enable|disable)	Web Admin インターフェイスを有効または無効にします。有効にすると、サービスを起動する前にいくつかのチェックが実行されます。リスニングインターフェイスが設定されていること、証明書が一致していること、ポートが他のサービスと衝突していないことなどです。
webadmin certs <keyfile-name> <crt filename> [<crt-bundle>] **webadmin certs none**	Web Admin インターフェイスと、オプションで CA によって提供された CA 証明書バンドルのキーファイル名と .crt ファイル名を提供します。 証明書の設定を削除します。
webadmin http-redirect (enable|disable)	Web Admin インターフェイスの HTTP リダイレクトを有効/無効にします。
webadmin status	Web Admin インターフェイスのステータスを表示します。

注：MMP ユーザアカウントは、Web Admin インターフェイスへのログインにも使用されます。

11.4 データベース クラスタリング コマンド

これらのデータベース クラスタリング コマンドについては、『スケーラビリティと復元力の導入 ガイド』と『証明書のガイドライン』で説明されています。

バージョン 2.7 以降、データベースクラスタでは、クラスタ内のデータベースに保持または接続する各 Meeting Server に設定された CA と同じ CA によって署名されたクライアント証明書およびサーバー証明書が必要になります。証明書の使用を必須にすることで、クラスタ全体の機密性と認証の両方が確保されます。

注意：証明書を必要としない旧バージョンの Meeting Server ソフトウェアを使用して、証明書を使用せずにデータベースクラスタが設定されている場合、バージョン 2.7 にアップグレードすると、データベースは停止し、証明書が設定されてデータベースクラスタが再作成されるまでアクセスできなくなります。

注：<ca_crt> は、データベースクラスタの CA 証明書バンドルです。これは信頼ストアとしても使用されるため、有効な証明書名を与えるデータベース接続と、バンドルに存在するルート証明書で終わる証明書チェーンが受け入れられます。

コマンド/例	説明/注意事項
database cluster status	このデータベース インスタンスの観点から、クラスタリングの状態を表示します。 **注：**2.7 以降、このコマンドは、設定済みの証明書がない場合に強調表示されます。
database cluster localnode <interface>	このコマンドは、新しいデータベースクラスタを初期化する前に、初期プライマリデータベースをホストするサーバで実行する必要があります。 <interface> は、次の形式で指定できます。[a|b|c|d] - インターフェイスの名前（最初の IPv6 アドレスが優先され、そうでない場合は、最初の IPv4 アドレスが選択されます）。例：database cluster localnode a ipv4:[a|b|c|d] - IPv4 に制限されたインターフェイスの名前（最初の IPv4 アドレスが選択されます）。例：database cluster localnode ipv4:a ipv6:[a|b|c|d] - IPv6 に制限されたインターフェイスの名前（最初の IPv6 アドレスが選択されます）。例：database cluster localnode ipv6:a <ipaddress> - 特定の IP アドレス。IPv4 または IPv6 にすることができます。例：database cluster localnode 10.1.3.9
database cluster initialize	このサーバの現在のデータベースの内容を唯一のデータベースインスタンス（プライマリ）として、新しいデータベースクラスタを作成します。 このコマンドは、postgres をクラスタモードに再設定します。 つまり、外部インターフェイスをリッスンし、SSL を使用します。ローカルの Call Bridge をデータベースクラスタを使用するように再設定して再起動します（有効になっている場合）。 **注：**2.7 以降、このコマンドは、有効な証明書、キー、および CA 証明書がデータベースクライアントおよびサーバにアップロードされない限り実行されません。

コマンド/例	説明/注意事項
database cluster join <hostname/IP address>	プライマリデータベースの内容をこのサーバにコピーし、そのサーバ上にあるデータベースの現在の内容を破棄して、新しいデータベースインスタンスをクラスタの一部として作成します。 <hostname/ip address> は、クラスタ内の既存のデータベースに使用できます。 データベースクラスタを使用するようにローカル Call Bridge（存在し、有効になっている場合）を再設定して再起動します。 **注：**2.7 以降、このコマンドは、有効な証明書、キー、および CA 証明書がデータベースクライアントおよびサーバにアップロードされない限り実行されません。
database cluster connect <hostname/IP address>	Call Bridge をデータベースクラスタに接続します。データベースクラスタを使用するように Call Bridge（有効になっている場合）を再設定して再起動します。ローカルデータベース（Call Bridge と同じホストサーバ上）の使用を無効にしますが、データベースの内容は保持され、このホストサーバ上でデータベースクラスタ削除コマンドが実行された後で読み取ることができます（以下を参照）。 **注：**2.7 以降、このコマンドは、有効な証明書、キー、および CA 証明書がデータベースクライアントおよびサーバにアップロードされない限り実行されません。
database cluster certs <server_key> <server_crt> <client_key> <client_crt> <ca_crt> **database cluster certs dbcluster_server.key dbcluster_server.crt dbcluster_client.key dbcluster_client.crt dbcluster_ca.crt**	データベースクラスタ内の接続を保護するために使用される証明書を設定します。 データベースクラスタを有効にする前に、証明書を設定する必要があります。
database cluster certs <client_key> <client_crt> <ca_crt> **database cluster certs dbcluster_client.key dbcluster_client.crt dbcluster_ca.crt**	Call Bridge 上に共存するデータベースがないデータベースクラスタの接続を保護するために使用される証明書を設定します。
database cluster certs none	証明書の設定を削除します。データベースクラスタを再度有効にする前に、証明書を再設定する必要があります。

コマンド/例	説明/注意事項
database cluster remove	データベースホストサーバで実行された場合は、クラスタから 1 つのデータベースを削除し、Call Bridge だけを備えたホストサーバで実行された場合は、Call Bridge を「接続解除」します。または、サーバがクラスタ化されたデータベースと Call Bridge の両方をホストしている場合は両方を実行します。
database cluster upgrade_schema	クラスタ内のデータベーススキーマのバージョンを、このノードが期待するバージョンにアップグレードします。このコマンドは、次のように実行することをお勧めします。 - プライマリデータベースで実行できますが、任意のデータベースインスタンスで実行できます。 - データベースインスタンスまたは Call Bridge をホストしているサーバで、ソフトウェアアップグレードのたびに
database cluster clear_error	スキーマのアップグレードなど、前の操作が失敗した場合（前のコマンドを参照）、このコマンドは状態を手動でリセットします。このコマンドは、Cisco サポートから指示された場合にのみ実行してください。
database cluster verifymode<full/ca>	データベース検証モードを設定します。 **full** - Meeting Server は、他の検証とともに、サーバ ID がサーバ証明書に保存されている名前と一致するかどうかを検証します。 **ca** - Meeting Server は、サーバー ID を検証せずに、証明書チェーンからルート証明書までのノードを検証します。 指定しなかった場合、検証モードはデフォルトで ca になります。

11.5 アップローダーコマンド

注：アップローダーは、Cisco Meeting Server 2000 では使用できません。

アップローダーは、ビデオコンテンツ管理のための Vbrick Rev の使用を簡素化します。このセクションでは、アップローダーのコマンドリファレンスを提供します。

コマンド	説明
uploader (enable|disable)	アップローダー コンポーネントを有効または無効にします。アップローダーを設定する前に、コンポーネントが無効になっていることを確認してください。
uploader nfs <host-name/IP>:<directory>	アップローダが監視する NFS を指定します。

コマンド	説明
uploader (cms|rev) host <host-name>	Meeting Server（cms）のホストの名前と Vbrick Rev サーバのホストの名前を使用してアップローダーを設定します。デフォルトのポートは 443 です。
uploader (cms|rev) port <port>	アップローダーに、Meeting Server（cms）への接続に使用するポートと Vbrick Rev サーバのポートを設定します。デフォルトのポートは 443 です。
uploader (cms|rev) user <user- name>	Meeting Server の API にアクセスできるユーザと Vbrick Rev サーバにアクセスできるユーザでアップローダーを設定します。
uploader (cms|rev) password	指定された Meeting Server ユーザと Vbrick Rev ユーザのパスワードを使用してアップローダーを設定します。
uploader (cms|rev) trust (<crt-bundle>|none)	指定された証明書バンドルを Meeting Server または Vbrick Rev サーバの信頼ストアにアップロードします。**none**は、指定された信頼ストアから証明書バンドルを削除します。注：アップローダーは、Meeting Server 信頼ストアと Vbrick Rev 信頼ストアに証明書バンドルがないと機能しません。
uploader edit (<uploader-team name>|none)	バージョン 2.4.0 ではサポートされていません。
uploader view (<uploader-team name>|none)	バージョン 2.4.0 ではサポートされていません。
uploader access <Private|Public|AllUsers>	ビデオ録画へのアクセス許可を設定します。
uploader cospace_member_access <view|edit|none>	スペースのメンバーがビデオ録画を表示または編集できるようにします。**none**は、スペースのメンバーの表示または編集権限を削除します。
uploader recording_owned_by_cospace_owner <true|false>	**true** は、これらのビデオ録画の単一の所有者としてスペースの所有者を選択します。
uploader fallback_owner (<user- name>|none)	スペースの所有者が VbrickRev にリストされていない場合、指定されたユーザをビデオ録画のフォールバック所有者として使用します。**none** は、フォールバック所有者を削除します。
uploader comments (enable|dis- able)	ビデオ録画へのコメントを有効または無効にします。デフォルトは無効です。
uploader ratings (enable|dis- able)	ビデオ録画の評価を有効または無効にします。デフォルトは無効です。
uploader downloads (enable|dis- able)	ダウンロード許可を設定し、ビデオ録画のダウンロードを有効または無効にします。
uploader initial_state (<active|inactive>)	最初に Vbrick Rev にアップロードされたときのビデオ録音の初期状態を設定します。デフォルトは active です。

コマンド	説明
uploader delete_after_upload (<true|false>)	アップロードの完了後にビデオ録画を NFS から削除するかどうかを選択します。デフォルトは false です。

注：**uploader debug (<true|false>)** コマンドは、バージョン 2.4 で削除され、デバッグ情報は自動的に syslog サーバーに送信されます。

11.6 レコーダーコマンド

注：レコーダーは Cisco Meeting Server 2000 では使用できません。

このセクションでは、レコーダーのコマンドリファレンスを提供します。適切な導入ガイドの指示に従って、レコーダーを展開します。

コマンド/例	説明/注意事項
recorder restart **recorder**	レコーダーを再起動します。 レコーダーの現在の設定を表示します。
recorder sip certs	SIP 証明書を設定できます。（バージョン 3.0 から追加。）
recorder sip listen <interface> <tcp-port|none> <tls-port|none>	SIP レコーダーおよびストリーマ コンポーネントでは、https 接続をリッスンする必要はなくなりましたが、SIP 接続をリッスンする必要があります。この新しい MMP コマンドは、TCP と TLS の両方を設定するために導入されました。（バージョン 3.0 から追加。）
recorder sip trace <1m|10m|30m|24h|on|off>	すべての SIP メッセージのロギングを有効にします。すべての SIP メッセージがレコーダーに記録されます。デフォルトは「off」です。「on」を使用すると、永続的または固定された期間にわたって有効にすることができます。（バージョン 3.0 から追加。）
recorder limit <value|none>	拡張性を確保するためにレコーダーの制限を設定します。これは、コール制御によって別のデバイスにフェールオーバーできるようにする、コール拒否の上限です。（バージョン 3.0 から追加。）
recorder (enable|disable)	レコーダーを有効または無効にします。
recorder nfs <hostname/IP>:<directory>	録音を保存するネットワーク ファイル サーバ（nfs）とフォルダの詳細をレコーダーに提供します。
recorder resolution <audio|720|1080>	レコーダーが会議を録音する解像度を設定します。デフォルトは 720p30 です。1080 を選択すると、レコーダーは p30 を実行できます。（バージョン 2.4 から）。

11.7 ストリーマーコマンド

注：ストリーマ–は Cisco Meeting Server 2000 では使用できません。

このセクションでは、ストリーマーのコマンドリファレンスを提供します。適切な導入ガイドの指示に従って、ストリーマーを展開します。

コマンド/例	説明/注意事項
streamer restart **streamer**	ストリーマーを再起動します。 ストリーマーの現在の設定を表示します。
streamer sip certs	SIP 証明書を設定できます。（バージョン 3.0 から追加。）
streamer limit <value|none>	拡張性を確保するためにストリーマの制限を設定します。これは、コール制御によって別のデバイスにフェールオーバーできるようにする、コール拒否の上限です。（バージョン 3.0 から追加。）
streamer sip listen <interface> <tcp-port|none> <tls-port|none>	SIP レコーダーおよびストリーマ コンポーネントでは、https 接続をリッスンする必要はなくなりましたが、SIP 接続をリッスンする必要があります。この新しい MMP コマンドは、TCP と TLS の両方を設定するために導入されました。（バージョン 3.0 から追加。）
streamer (enable|disable)	ストリーマーを有効または無効にします。設定する前にストリーマーを無効にする必要があります。設定後、ストリーマーを有効にする必要があります。

11.8 MeetingApps コマンド

MeetingApps サービスは、参加者が会議でファイルを共有できるようにするために Meeting Server に導入されています。他のサービスを使用せずに、スタンドアロンの Meeting Server ノードで設定する必要があります。Web アプリは、安全な環境で MeetingApps と通信し、ファイル共有や調査にアクセスします。

このセクションでは、MeetingApps を設定するためのコマンドをリストします。MeetingApps と Web Bridge を設定する手順は、*導入ガイド*で説明されています。

注：MeetingApps サービスは、Meeting Server 2000 では設定できません。

コマンド/例	説明
meetingapps	MeetingApps の設定済みパラメータを表示します。
meetingapps https listen <inter- face> <port>	MeetingApps がリッスンするインターフェイスとポートを設定します。

コマンド/例	説明
meetingapps https listen none	MeetingApps のインターフェイスとポートの設定を削除します。
meetingapps gen- secret	Web Bridge および MeetingApps 接続の認証に使用されるキーを生成します。
meetingapps https certs <key-file> <crt-fullchain-file>	MeetingApps の HTTPS 証明書を設定します。有効な認証局（CA）によって署名された、公的に信頼された HTTPS 証明書を使用することをお勧めします。
meetingapps https certs none	HTTPS 証明書の設定を削除します。
meetingapps (enable|disable)	MeetingApps を有効または無効にします。
meetingapps restart	MeetingApps サービスを再起動します。
meetingapps status	MeetingApps のステータスを表示します。たとえば、Running、Starting です。
webbridge3 meetingapps add <hostname> <port> <secretkey>	MeetingApps のホスト名、ポート番号、および meetingapps gensecret コマンドを使用して生成された秘密キーを設定します。
webbridge3 meetingapps add none	Web Bridge に設定されている MeetingApps をクリアします。

12 その他のコマンド

12.1 モデル

コマンド/例	説明/注意事項
model	Cisco Meeting Server の導入モデルを表示します。 仮想化された展開は CMS VM として表示されます。

12.2 Meeting Server のシリアル番号

コマンド/例	説明/注意事項
serial	Meeting Server のシリアル番号を表示します。 このコマンドは、仮想化展開には適用されないことに注意してください。

12.3 本日のメッセージ

管理者権限を持つ MMP ユーザは、このセクションのコマンドを発行できます。

注： motdコマンドは、バージョン 1.9 より前のバージョンの Meeting App でのみサポートされています。

コマンド/例	説明/注意事項
motd	現在の今日のメッセージがあれば表示します。
motd add "<message text>"	ログイン後に <message> とともにバナーを表示 または、SFTP でファイルを「motd」にコピーすることで、2048 文字以下のメッセージを設定できます。
motd del	今日のメッセージを削除します。

12.4 ログイン前の法的警告バナー

組織がログイン前の法的警告を必要とする場合、管理者権限を持つ MMP ユーザは次のコマンドを使用できます。

コマンド/例	説明/注意事項
login_warning	現在のログイン警告メッセージがあれば表示します。

コマンド/例	説明/注意事項
login_warning add "<message>"	ログイン前の法的警告を表示します。 または、SFTP でファイルを「login_warning」にコピーすることで、2048 文字以下のメッセージを設定できます。
login_warning del	法的警告を削除します。

12.5 SNMP コマンド

注：Meeting Server 2000 は SNMP をサポートしていないため、snmp コマンドは使用できません。

12.5.1 一般情報

MIB は、SFTP を使用して任意の Cisco Meeting Server からダウンロードできます。

仮想化展開（Cisco Meeting Server 1000、または仕様ベースの VM サーバ）の場合、MIB ファイルは次のとおりです。

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

これらのファイルを SNMP 導入の検索パスに配置します。たとえば、Net- SNMP の場合、~/.snmp/mibs です。

注：MIB は、Cisco Meeting Server へのブランド変更を反映するために、将来のリリースで名前が変更されます。

MMP インターフェイスは、最小限のユーザ設定オプションのみを提供します。より複雑な要件を処理するには、MMP インターフェイスを使用して初期ユーザを作成し、ユーザデータベースを直接管理します。たとえば、Net-SNMP パッケージの snmpusm を使用します。

Meeting Server は、SNMP バージョン 1/2c と 3 の両方をサポートします。設定はそれぞれ異なります。SNMP バージョン 1/2c を使用することによるセキュリティへの影響に注意してください。これは堅牢な認証をサポートしていないため、コミュニティ文字列を知っている人なら誰でもサーバへのクエリを実行できます。

12.5.2 SNMP v1/2c コマンド

v1/2c のアクセス制御は「コミュニティ」に基づいています。これらは、SNMP が無効になっているときに MMP インターフェイスを介して作成できます。

コマンド/例	説明/注意事項
snmp community add <name> [IP address/prefix] **snmp community del <name>**	v1/2c のアクセス制御は「コミュニティ」に基づいています。これらは、SNMP が無効になっているときに MMP を介して作成および削除できます。 **注：**SNMP コミュニティ名には英数字とアンダースコアのみを使用してください。ダッシュなど、他の「特殊」文字はエラーメッセージを返します。
snmp community add public	コミュニティ文字列「public」を使用して、どこからでも完全なツリーにアクセスできます。
snmp community add local 10.1.0.0/16	アクセスを許可しますが、指定されたサブネットからのみ許可します。
snmp (enable|disable)	SNMP v1/2c を有効/無効にします。

12.5.3 SNMP v3 コマンド

v3 のアクセス制御はユーザに基づいています。これらは、MMP インターフェイスから作成できます。

コマンド/例	説明/注意事項
snmp user add <name> <password> (MD5|SHA) (DES|AES)	v3 のアクセス制御はユーザに基づいています。 認証に「MD5」アルゴリズム、暗号化に「DES」アルゴリズムを使用して、指定されたパスワードで完全なツリーにアクセスできるユーザを作成します。 **注：**SNMP ユーザ名には英数字とアンダースコアのみを使用してください。ダッシュなど、その他の「特殊」文字を使用すると、エラーメッセージが返されます。
snmp user del <name>	SNMP ユーザを削除します。
snmp (enable|disable)	SNMP v3 を有効/無効にします。

12.5.4 SNMP トラップの受信者の設定

コマンド/例	説明/注意事項
snmp trap enable <hostname> <agent community string> **snmp trap disable** **snmp trap enable mybox public**	SNMP トラップの受信者を設定します。 <hostname> は、トラップを受信するマシンのホスト名で、 <community string> は、使用されるコミュニティ文字列です

12.6 システムログのダウンロード

システムログは最大 100MB です。この限界に達すると、最も古いメッセージが破棄され、新しいメッセージのためのスペースが確保されます。ログがキャパシティの 75% に達すると、SNMP トラップが生成されます。

コンプライアンスまたはその他の理由でログデータを保持する必要があり、リモート Syslog サーバが使用されていない場合は、次のことができます。

- SFTP ツールを使用して MMP に接続し、システムログファイルをサーバからローカルファイルストアにコピーします。これにより、現在の内容がそのまま残ります。
- **`syslog rotate <filename>`**コマンドを使用して、ログファイルを永続的に保存します。その場合、アクティブなシステムログは空になります。この保存されたファイルは SFTP を使用してダウンロードできます。

  例：**`syslog rotate mylog`**
- 監査ロールを持つは、 **`syslog audit rotate <filename>`** を使用して監査ログを保存できます。

12.7 ログバンドルの生成とダウンロード

Meeting Server では、Meeting Server 内のさまざまなコンポーネントの設定と状態を含むログバンドルを生成できます。このログバンドルには、syslog ファイルと live.json ファイルが含まれます。問題についてCisco サポートに連絡する必要がある場合、これらのファイルは、分析を迅速化するのに役立ちます。

Meeting Server ログバンドルは、次の方法で生成されます。

- Meeting Server 管理者は、MMP 管理者ユーザのログイン情報を使用して SFTP クライアントを MMP IP アドレスに接続することにより、ログバンドルのダウンロードプロセスを開始できます。システムは、logbundle.tar.gz というファイル名のログバンドルを生成してダウンロードします。
- または、管理者は、**`generate_logbundle`**コマンドを使用して、ダウンロードプロセスを開始する前にログバンドルを生成できます。 generatedlogbundle.tar.gz というファイル名のログバンドルが生成されます。

コマンド/例	説明/注意事項
generate_logbundle	それぞれの会議サーバーで generatedlogbundle.tar.gz というファイル名のログバンドルを生成します。 **注：**このコマンドが実行されるたびに、以前に生成されたログバンドルが最新のログバンドルに置き換えられます。

以下の手順を使用して、ログバンドルをダウンロードします。

1. SFTP クライアントを MMP の IP アドレスに接続します。
2. MMP の admin ユーザのログイン情報を使用してログインします。
3. ログバンドルをダウンロードする必要がある場所で、次のいずれかのコマンドを実行します。
   a. **`sftp get logbundle.tar.gz`**
   b. **`sftp get generatedlogbundle.tar.gz`**
4. logbundle.tar.gz/generatedlogbundle.tar.gz ファイルをローカルフォルダにコピーします。
5. ファイルの名前を変更します。ファイル名の logbundle の部分を、ファイルを作成したサーバーを特定する名前に変更します。これは、複数サーバーの展開で重要です。
6. 分析のため、名前を変更したファイルをCisco サポートの連絡先に送信します。

log bundle.tar.gz の最初のファイルサイズは 1 Kb です。SFTP 経由で転送した後は、ファイル数とそのサイズに応じてサイズが増加します。

注：コンピュータと Meeting Server 間のネットワーク接続が遅いことが原因でログバンドルをダウンロードできない場合は、ログと live.json ファイルをダウンロードして、シスコサポートに送信できます。

12.8 ディスク領域使用率

コマンド/例	説明/注意事項
`df`	MMP と MODULE 0 の両方のディスク使用量を、パーティションごとの使用率および i ノード使用率として表示します。

12.9 システム設定のバックアップと復元

注：backup コマンドは仮想化ソリューションでも使用できます。

コマンド/例	説明/注意事項
backup list	サーバ上のバックアップファイルのリストを表示します。
backup snapshot <name>	完全な Meeting Server スナップショットを作成します。<name>.bak ファイルは、SFTP 経由でダウンロードするために作成されます。このコマンドを定期的に使用することを強くお勧めします。ファイル名の最大文字数は 256 文字です。
backup rollback <name>	バックアップされたサーバのシステムを復元します。これには、サーバの設定のロールバックが含まれます。Meeting Server 上にまだない場合は、このロールバックコマンドを実行する前に、SFTP を使用してバックアップファイルを Meeting Server にアップロードする必要があります。ファイル名の最大文字数は 256 文字です。 注：このコマンドは、既存の設定、license.dat ファイル、およびシステム上のすべての証明書と秘密キーを上書きし、Meeting Server を再起動します。したがって、注意して使用する必要があります。このバックアップを別のサーバに復元する場合は、既存の license.dat ファイルと証明書を事前にコピーしておく必要があります。これらは backup rollback プロセス中に上書きされます。license.dat ファイルはサーバの MAC アドレスに対応しているため、別のサーバからのバックアップから復元すると失敗し、サーバがオンラインに戻った後に置き換える必要があります。

12.10 Meeting Server のアップグレード

コマンド/例	説明/注意事項
upgrade [<filename>]	Meeting Server をアップグレードします。このコマンドを発行する前に、アップグレードしたいバージョンのイメージファイルをアップロードしておく必要があります。 アップグレードすると、システム全体のバックアップが自動的に作成されます。バックアップ名は、現在のソフトウェアバージョンに由来します。たとえば、R2.9 から R3.0 へのアップグレードの場合、バックアップの名前は 2_9.bak になります。指定されなかった場合のデフォルトのファイル名は upgrade.img です。 バージョン 3.0 から、このコマンドは、指定されたイメージで Meeting Server をアップグレードする前に、署名と完全性のチェックを実行します。それ以前にそのイメージに対して **upgrade <name> verify** コマンドが実行された場合でも、このチェックは実行されます。バージョン 3.0 で更新されました。 バージョン 3.7 以降、Meeting Server は、データベースクラスタがサーバー構成で有効になっているかどうかを識別し、それに応じて、アップグレードする前にノードのクラスタ化を解除するようにユーザーに通知します。ユーザーは、20 秒以内に **CTRL+C** を押すことにより、アップグレード プロセスを中止することを選択できます。
upgrade <filename> [no- backup]	注意して使用してください。
upgrade list	システム上のアップグレードイメージのリストを取得します。
upgrade delete <name> **upgrade delete upgrade.img**	アップグレードイメージは、SFTP またはこの CLI コマンドを使用して削除されるまで保持されます。
upgrade <filename> verify	通常はアップグレード中に実行される完全性と署名のチェックをすべて実行しますが、続けてアップグレードを実行しません。このコマンドを使用は、イメージ タイプを表示する目的でも使用できます。（バージョン 3.0 から追加。）
authenticity	ソフトウェアの真正性に関するすべての情報を表示します。実行中のイメージがどのように検証されたか（キーのタイプと名前）、現在ロードされている公開キーとその詳細（タイプ、名前、ソース）。また、キーが信頼されているかどうかも表示します。特別なキーがインストールされているかどうか、その署名がマスター キーで検証済みであるかどうか（それ以外のキーは内部キーであり常に信頼されます）。（バージョン 3.0 から追加。）

authenticity key add <key-file>	特別なキーをインストールします。一度にインストールできる特別なキーは 1 つだけです。（バージョン 3.0 から追加。）
authenticity key none	現在インストールされている特別なキーを削除します。別のキーをインストールする前に既存のキーを削除する場合、またはキーをそれ以降使用しない場合に、このコマンドを使用する必要があります。（バージョン 3.0 から追加。）

12.11 Meeting Server のリセット

コマンド/例	説明/注意事項
factory_reset (full|app)	「full」オプションは、すべてのユーザ設定を削除します。システムにインストールされているログイン情報はすべて失われます。その後、Meeting Server を再度展開する必要があります。 「app」オプションは、Active Directory 同期データとスペース（coSpace）、Lync および SIP 設定を削除します。ただし、MMP 設定は残ります。 コマンドが完了すると、システムが再起動します。

付録 A バージョン 3.0 MMP コマンドの削除

3.0 で Meeting Server から削除された機能とコンポーネントに関連するすべての MMP コマンドは、以下のように削除されています。

- H.323 ゲートウェイコマンド（**h323_gateway**）
- Web Bridge 2 コマンド（**webbridge**）
- XMPP サーバコマンド（**xmpp**）
- XMPP マルチドメインコマンド（**xmpp multi_domain**）
- XMPP レジリエンシコマンド（**xmpp cluster**）
- ロードバランサのコマンド（loadbalancer）
- トランクのコマンド（trunk）
- SIP エッジのコマンド（**sipedge**およびエッジ関連の **callbridge**）
- XMPP に依存していたレコーダーおよびストリーマのコマンド
- X シリーズサーバに適用可能な MMP コマンド

表 1：Meeting Server の設定に関する削除されたコマンド

コマンド/例	説明/注意事項
health	Meeting Server に関する温度、電圧、およびその他の正常性情報を表示します。 注：health コマンドは、仮想化展開では使用できません。
callbridge trust xmpp <trusted xmpp certificate allowed list	XMPP サーバの ID を検証するために、特定の証明書の許可リストを使用するように Call Bridge を設定します。（バージョン 2.4 から）
callbridge trust xmpp none	Call Bridge 信頼ストアから XMPP 証明書の許可リストを削除します。（バージョン 2.4 から）

表 2：削除された XMPP サーバコマンド

コマンド/例	説明/注意事項
xmpp **xmpp status**	現在の設定を表示します。
xmpp restart	XMPP サーバを再起動します。
xmpp domain <domain-name>	XMPP サーバのコンポーネントシークレットを作成します。

コマンド/例	説明/注意事項
xmpp listen <interface allowed list|none> **xmpp listen a b** **xmpp listen none**	リッスンするインターフェイスの許可リストを設定します。リスニングを開始するには、xmpp enable コマンドでサービスを有効にする必要があります。 XMPP サーバのリッスンを停止します。
xmpp (enable|disable)	XMMP サーバを有効または無効にします。
xmpp certs <key-file> <crt-file> [<crt-bundle>] **xmpp certs none**	XMPP サーバとオプションで CA によって提供された CA 証明書バンドルのキーファイル名と証明書ファイル名を定義します。 証明書の設定を削除します。
xmpp motd add <message> **xmpp motd del**	Cisco Meeting App または XMPP クライアントのログイン時に表示される「今日のメッセージ」を設定します。 今日のメッセージを削除します。 または、SFTP でファイルを「xmpp.motd」にコピーすることで、2048 文字以内のメッセージを設定できます。何らかの方法で xmpp.motd を変更すると、XMPP サーバが再起動します。 **注：motd** コマンドは、バージョン 1.9 より前のバージョンの Meeting App でのみサポートされています。
xmpp max_sessions <number> **xmpp max_sessions none** **xmpp max_sessions 3**	個々のユーザが XMPP サーバで使用できる同時 XMPP セッション数（したがって、同時ログイン数）を制限します。これにより、1 人のユーザがシステムリソースを使い果たすことがなくなります。 ユーザごとの XMPP セッションの制限を削除します。 ユーザが最大で iPad、iPhone、および PC のログインを持つことが予想される場合は、最大セッションを 3 に設定します。
xmpp callbridge add <component name> **xmpp callbridge del <component name>**	これらの xmpp callbridge コマンドは、『スケーラビリティと復元力の導入ガイド』で説明されています。 新しい Call Bridge からの接続を許可するように XMPP サーバを設定します。注：シークレットが生成されます。これは、XMPP のレジリエンシを設定する場合に必要です。次に、その Call Bridge の Web Admin インターフェイスに移動し、XMPP サーバに接続するように設定します。 Call Bridge が XMPP サーバにアクセスするのを停止します。

コマンド/例	説明/注意事項
xmpp callbridge list	Call Bridge ごとに、ドメイン、component_secret、および接続ステータスをリストします。
xmpp callbridge add-secret <callbridge>	XMPP のレジリエンシに必要です。クラスタ内の最初のノードに Call Bridge を接続することによって生成されたシークレットを XMPP クラスタ内の他のノードに追加するために使用されます。
xmpp reset	XMPP サーバをスタンドアロン設定に戻します（追加されたすべての Call Bridge を削除します）。このコマンドは、設定を再起動する必要がある場合にのみ使用してください。

表 3：削除されたロードバランサコマンド

コマンド/例	説明/注意事項
loadbalancer list [<tag>]	すべてのロードバランサ設定をリストします。または、tag が指定された場合は、そのロードバランサの設定のみをリストします。
loadbalancer (enable|disable) <tag> **loadbalancer enable exampleEdge**	ロードバランサを有効または無効にします。 パブリックポート（下記参照）は、接続を処理するトランクが存在するようになるまで開かれないことに注意してください。
loadbalancer create <tag> **loadbalancer create exampleEdge**	ロードバランサを作成します。
loadbalancer trunk <tag> <iface> [:<port>] **loadbalancer trunk exampleEdge a:3999** **loadbalancer public <tag> <iface> [:<port allowed list>]** **loadbalancer public exampleEdge b:5222 loadbalancer public exampleEdge b:5222 lo:5222**	トランクインターフェイスとポートを設定します。 パブリックインターフェイスとポートを設定します（クライアント接続を受け入れるため）。 一般的なエッジ展開では、Web Bridge も有効にして、コアからエッジへのトランクを利用する必要があります。これを可能にするには、ループバック インターフェイスをパブリックインターフェイスとして設定します。
loadbalancer auth <tag> <key-file> <cert-file> <trust-bundle> **loadbalancer auth exampleEdge acano.key acano.crt trust.pem**	トランクへの認証に使用される秘密キーと証明書、およびトランクによって提示される可能性のある信頼できる証明書を設定します。 TLS 接続の作成時にトランクが信頼バンドル内のいずれかの証明書を提示し、トランクがロードバランサによって提示された証明書を受け入れた場合、接続は成功します。具体的には、信頼バンドルに証明書の有効なチェーンが含まれており、提示された証明書がチェーンの最後の CA によって発行されている場合、認証は成功します。それ以外の場合、接続は拒否されます。特に、自己署名証明書が使用されている場合、公開証明書を信頼バンドルに入れることができ、認証は成功します。
loadbalancer delete <tag>	ロードバランサの設定を削除します。

表 4：削除されたトランクコマンド

コマンド/例	説明/注意事項
trunk list [<tag>]	すべてのコア設定、または tag が指定された場合はそのコアの設定のみをリストします。
trunk (enable|disable) <tag>	コアを有効または無効にします。
trunk create <tag> <port or service name> **trunk create trunktoExampleEdge xmpp**	XMPP のトランクインスタンスを作成します。
trunk edge <tag> <edge name|ip address>[:<port>]	トランクの接続先のエッジのドメイン名または IP アドレスを設定します。ドメイン名は複数の IP アドレスに解決されることがあります。その場合、すべてのアドレスへの接続が試行されます。ポートが指定されなかった場合、ドメイン名の DNS SRV ルックアップによってポートを検出できると見なされます。
trunk auth <tag> <key-file> <cert-file> <trust-bundle>	エッジサーバへの認証に使用される秘密キーと証明書、およびエッジサーバによって提示される可能性のある信頼できる証明書を設定します。
trunk delete <tag>	コア設定を削除します。

trunk debug <tag>	このコマンドは、Cisco サポートの指示の下でのみ使用してください。診断には以下が示されます。
	- エッジサーバ名の DNS 結果
	- TLS 接続を作成し、各アドレスに対して認証を試みます
	- 成功した場合は、コアサーバからのデバッグ情報を表示します。これには以下が含まれます。
	  - 問題のエッジサーバへの「コア」接続（トランクからエッジサーバへの接続）のリスト
	  - そのエッジサーバによって現在処理されているクライアント接続
	  - エッジサーバのメモリ使用量の統計

表 5：XMPP マルチドメインのサポートに関して削除されたコマンド

コマンド/例	説明/注意事項
xmpp multi_domain add <domain name> <key-file> <crt-file> [<crt-bundle>]	XMPP サーバがリッスンする別のドメインを追加します。CA によって提供された秘密キー、証明書、およびオプションの証明書バンドルを指定します。この変更を有効にするには、XMPP サーバを再起動します。注：秘密キーまたは証明書ファイルがないか、無効である場合、XMPP サーバは起動しません。
xmpp multi_domain del <domain name>	XMPP サーバがリッスンするドメインを削除します。
xmpp multi_domain list	XMPP サーバがリッスンするドメインをリストします。

表 6：削除された XMPP レジリエンシコマンド

コマンド/例	説明/注意事項
xmpp cluster enable|disable	XMPP クラスタリングを有効/無効にします。ノードで XMPP を有効にする前に、XMPP クラスタを有効にする必要があります。xmpp クラスタが無効で xmpp が起動された場合、xmpp サーバはスタンドアロンモードで起動します。
xmpp cluster trust <trustbundle.pem>	xmpp クラスタによって信頼される証明書のバンドルを指定します。<trustbundle.pem>には、クラスタ内の xmpp サーバーのすべての証明書が含まれている必要があります。証明書は、xmpp certs コマンドを使用して xmpp サーバにすでに適用されている必要があります。このメカニズムにより、クラスタ内のさまざまな xmpp ノードが相互に信頼できるようになり、フェイルオーバー操作とノード間のトラフィックの転送が可能になります。
xmpp cluster status	xmpp クラスタのライブ状態を報告します。クラスタに障害が発生した場合、このコマンドは、この Meeting Server でのみ実行されている xmpp サーバの統計を返します。このコマンドを使用して、接続の問題を診断してみてください。
xmpp cluster initialize	クラスタを初期化します。このコマンドは、1 ノードのライブ xmpp クラスタを作成します。他のノード（xmpp サーバ）をこのクラスタに参加させることができます。
xmpp cluster join <cluster>	このノードをクラスタに追加します。<cluster> は、クラスタ内の最初のノードの IP アドレスです（コマンド xmpp cluster initialize を参照）。
xmpp cluster remove	このノードをクラスタから削除します。これには、ノードが実行している必要があります。

コマンド/例	説明/注意事項
xmpp cluster remove <node>	指定されたノードをクラスタから削除します。ここで、<node> は、ノードの IP アドレスまたはドメイン名です。これにより、ノードが応答しない場合にクラスタからノードを削除できます。
xmpp callbridge add-secret <callbridge> **Please enter a secret: <secret>**	Call Bridge シークレットを XMPP サーバに追加します。クラスタ内の最初の XMPP サーバノードに Call Bridge を接続するときに作成されたシークレットを使用して、他のノードを設定するために使用されます。 このコマンドにより、Call Bridge は多くの XMPP サーバとログイン情報を共有できます。

表 7：削除された Web Bridge コマンド（レガシー Web Bridge 2 の設定用）

コマンド/例	説明/注意事項
webbridge restart	Web Bridge を再起動します。
webbridge status	現在の設定を表示します。
webbridge listen <a|b|c|d|none [:><port>] allowed list> **webbridge listen a b**	Web Bridge がリッスンするインターフェイスとポートを設定します。リッスンを開始するには、コマンド webbridge enable を使用して、サービスを有効にする必要があります。オプションの port 引数のデフォルトは 443 です。
webbridge listen none	Web Bridge のリッスンを停止します。
webbridge (enable|disable)	Web Bridge を有効または無効にします。
webbridge certs <keyfile-name> <crt filename> [<crt-bundle>]	Web Bridge と、オプションで CA によって提供された CA 証明書バンドルのキーファイル名と .crt ファイル名を提供します。
webbridge certs none	証明書の設定を削除します。
webbridge clickonce <url|none>	クリックワンスリンクの場所を定義します。URL の先頭には http://、https://、または ftp:// を付け、有効な URL にする必要があります。ユーザが Internet Explorer（クリックワンスをサポートする唯一のブラウザ）を使用して、通話招待リンクまたは coSpace Web リンク（https://www.join.cisco.com/invited.sf?id=1234 など）をたどると、デフォルトを使用するのではなく、設定されたクリックワンスの場所にユーザをリダイレクトしようとします。 このリダイレクトが発生すると、PC クライアントが自動的に起動し（まだインストールされていない場合はダウンロードされ）、call/coSpace がダイヤルされます。
webbridge clickonce none	すべてのクリックワンスリダイレクト動作を無効にします。

コマンド/例	説明/注意事項
webbridge msi (<url>|none) **webbridge dmg (<url>|none)** **webbridge ios (<url>|none)** **webbridge ios none**	WebRTC ユーザに表示される Windows msi、Mac OSX dmg、および iOS インストーラのダウンロード場所を設定します。 設定を解除するには、パラメータ **none** を指定して適切なコマンドを使用します。
webbridge trust <crt-bundle|crt-file> **webbridge trust none**	ゲストアカウントとカスタマイズ（背景画像など）の設定を許可する Call Bridge インスタンスを制御します。 信頼された Call Bridge が Web Bridge と同じサーバで実行されている場合は、Call Bridge の公開証明書/証明書バンドルの名前を指定して webbridge trust コマンドを発行するだけで十分です。Call Bridge が別のサーバで実行されている場合は、まず、Call Bridge の公開証明書/証明書バンドルを SFTP を使用して Web Bridge サーバにコピーする必要があります。 **注：**クラスタ化された Call Bridge 展開で、Call Bridge に異なる証明書がある場合は、証明書を 1 つのバンドルに結合します。
webbridge trust xmpp <trusted xmpp certificate allowed list>	XMPP サーバの ID を検証するために、証明書の特定の許可リストを使用するように Web Bridge を設定します。（バージョン 2.4 から）
webbridge trust xmpp none	XMPP 証明書の許可リストを Web Bridge 信頼ストアから削除します。（バージョン 2.4 から）
webbridge http-redirect (enable|disable)	HTTP リダイレクトを有効/無効にします。
webbridge url-redirect (<url>|none)	URL リダイレクトの場所を設定します。設定を解除するには、パラメータ **none** を指定してコマンドを使用します。
webbridge options <feature_name1 feature_name2> **webbridge options cma.webrtc.ios**	指定された機能を有効にします。複数の機能を有効にする場合は、feature_names をスペースで区切ります。このコマンドは、Cisco サポートまたは Cisco EFT からの指示がある場合にのみ使用してください。これらの機能は、実稼働での使用には適していません。 この機能は、再起動しても有効なままですが、アップグレードコマンドを使用すると自動的にクリアされます。 （バージョン 2.5 から）。
webbridge options none	以前に有効にされたすべての機能を**webbridge options<feature_name>** コマンドを使用して無効にします。Cisco サポートまたは Cisco EFT からの指示がある場合にのみ使用してください。（バージョン 2.5 から）。

表 8：SIP エッジコンポーネントの設定に関して削除されたコマンド

コマンド/例	説明/注意事項
callbridge add edge <ip address>:<port>	使用する Call Bridge の SIP エッジを追加します。
callbridge del edge	SIP エッジを削除します。
callbridge trust edge <certificate file>	SIP エッジとの接続で信頼する Call Bridge の証明書を指定します。これは、SIP エッジの証明書です。
sipedge private <interface>:<port>	Call Bridge との接続のための内部インターフェイスとポートを指定します。
sipedge public <interface>:<port>	外部システムとの接続のための外部インターフェイスとポートを指定します。
sipedge public-ip <address> **sipedge public-ip none**	SIP エッジに到達できる NAT アドレスを設定または削除します。
sipedge certs <key-file> <crt-file> <trusted-bundle>	Call Bridge からの接続用の信頼できる証明書バンドルとともに、SIP エッジの秘密キーと証明書を設定します。
sipedge enable **sipedge disable**	SIP エッジコンポーネントを有効または無効にします。
sipedge restart	SIP エッジコンポーネントを再起動します。SIP エッジで証明書を変更した後に、このコマンドを使用します。重要なコールがアクティブなときは、このコマンドを使用しないでください。

表 9：H.323 コールを受け入れて送信するように Meeting Server を設定するために削除されたコマンド

コマンド/例	説明/注意事項
h323_gateway enable/disable/restart	ゲートウェイは、正しく設定されていないと起動しません。
h323_gateway certs <keyfile> <certificate file> [<cert-bundle>]	H.323 ゲートウェイ アプリケーションとオプションで CA によって 提供された CA 証明書バンドルについて、秘密キーファイルと .crt ファイルの名前を定義します。（「証明書によるプロビジョニング」のセクションも参照してください。）
h323_gateway certs none	証明書の設定を削除します。

コマンド/例	説明/注意事項
h323_gateway h323_nexthop <host/ip> **h323_gateway del h323_nexthop**	すべての発信 H.323 コールについて、この IP アドレスに接続し、この IP アドレスのデバイスにルーティングを処理させます。このアドレスが設定されていない場合、IP ダイヤルのみが機能します。 通常、この IP アドレスは Cisco VCS/Polycom DMA であり、Cisco Meeting Server H.323 ゲートウェイとサードパーティデバイス （H.323 ゲートキーパー）の間に H.323 トランクが確立されます。H.323 ゲートウェイはデバイスに登録せず、通話を転送するだけです。これらの通話を受け入れるようにデバイスを適切に設定する必要があります。
h323_gateway default_uri <uri> **h323_gateway del default_uri**	（オプション）着信 H.323 コールに宛先がない場合（通常、H.323 ゲートウェイが IP アドレスによってダイヤルされた場合のみ）、SIP コールは default_uri が設定されているものに発信されます。default_uri は、IVR を指す場合もあれば、直接 coSpace を指す場合もあります。設定されていない場合、コールは拒否されます。
h323_gateway sip_domain <uri> **h323_gateway del sip_domain <uri>**	（オプション）着信 H.323 コールが宛先アドレスにドメインなしでゲートウェイに発信された場合、@<sip_domain> は、Call Bridge への SIP コールが行われる前に宛先アドレスに追加されます。
h323_gateway sip_domain_strip <yes/no>	「yes」に設定され、「h323_gateway sip_domain」が設定された場合、SIP コールがゲートウェイに発信されると、@<sip_domain> が送信元アドレス（存在する場合）から削除されてから、H.323 コールが行われます。
h323_gateway h323_domain <uri> **h323_gateway del h323_domain <uri>**	（オプション）送信元アドレスにドメインを含めずに H.323 コールがゲートウェイに発信された場合、@<h323_domain> が送信元アドレスに追加されてから、SIP コールが行われます。
h323_gateway h323_domain_strip <yes/no>	「yes」に設定され、「h323_gateway h323_domain」が設定された場合、SIP コールがゲートウェイに発信されると、@<h323_domain> が宛先アドレス（存在する場合）から削除されてから、H.323 コールが行われます。
h323_gateway h323_interfaces <interface list> **h323_gateway sip_interfaces <interface list>**	ゲートウェイを開始するには設定する必要がありますが、実際の設定は現在無視されています。

コマンド/例	説明/注意事項
h323_gateway sip_port <port>	SIP 側がリッスンするポート。デフォルトは 6061 です。 注：デフォルトポートを 6061 から変更する場合、H.323 ゲートウェイと Call Bridge が同じサーバ上にある場合は、Call Bridge で使用されるポート 5061 を避けてください。ゲートウェイが再起動されるまで、変更は有効になりません。 H.323 ゲートウェイは常に TLS 接続を想定しています。したがって、Call Bridge のアウトバウンド ダイヤルプラン ルールで「暗号化」を選択する必要があります。
h323_gateway sip_proxy <uri>	これを Call Bridge の IP アドレスに設定するか、複数の Call Bridge でドメイン名を使用します（DNS 経由）。すべての着信 H.323 コールは、この uri に転送されます。 Call Bridge と H.323 ゲートウェイが同じホスト上にある場合は、IP アドレス 127.0.0.1 を使用します。Call Bridge と H.323 ゲートウェイが異なるホスト上にある場合は、Call Bridge の IP アドレスを使用します。
h323_gateway restrict_codecs <yes/no>	yes に設定すると、H.323 ゲートウェイは、相互運用性の問題を引き起こす可能性が低い安全なコーデックのセットに制限されます。現在、このセットは G.711/G.722/G.728/H.261/H.263/H.263+/H.264 です。 この機能によって無効にされるコーデックは、G.722.1 および AAC です。
h323_gateway disable_content <yes/no>	yes に設定すると、H.239 コンテンツが無効になります。
h323_gateway trace_level <level>	Cisco サポートによるトラブルシューティングに役立つ追加のロギングを提供します。レベル 0、1、2、または 3 のトレースを提供するように求められる場合があります。

表 10：削除された XMPP レコーダーコマンド

コマンド	説明
recorder listen <a|b|c|d|lo|none [:><port>] allowed list> **recorder listen a b**	レコーダーがリッスンするインターフェイスとポートを設定します。recorder enable コマンドでリスニングを開始するには、サービスを有効にする必要があります。オプションの port 引数のデフォルトは 443 です。
recorder listen none	レコーダーのリスニングを停止します。
recorder certs <keyfile-name> <crt filename> [<crt-bundle>]	レコーダーのキー ファイルと .crt ファイル の名前を提供します。オプションで、CA によって提供された CA 証明書バンドルの名前を提供します。

コマンド	説明
streamer certs none	バージョン 3.0（ベータ 2）から非推奨になりました。証明書の設定を削除します。
recorder certs none	証明書の設定を削除します。
streamer trust <crt-bundle|crt-file>	どの Call Bridge インスタンスにレコーダーへの接続を許可するかを制御します。 信頼された Call Bridge がレコーダーと同じサーバで実行されている場合は、Call Bridge の公開証明書/証明書バンドルの名前を指定して recorder trust コマンドを発行するだけで十分です。Call Bridge が別のサーバで実行されている場合は、まず、レコーダーを有効にしたサーバに、Call Bridge の公開証明書/証明書バンドルを SFTP を使用してコピーする必要があります。

表 11：削除された XMPP ストリーマコマンド

コマンド	説明
streamer listen <a|b|c|d|lo|none [:><port>] allowed list> **recorder listen a b**	ストリーマがリッスンするインターフェイスとポートを設定します。streamer enable コマンドでリスニングを開始するには、サービスを有効にする必要があります。オプションの port 引数のデフォルトは 443 です。
streamer certs none	証明書の設定を削除します。
streamer certs <keyfile-name> <crt filename> [<crt-bundle>]	ストリーマのキー ファイルと .crt ファイル の名前を提供します。オプションで、CA によって提供された CA 証明書バンドルの名前を提供します。
streamer trust <crt-bundle|crt-file>	どの Call Bridge インスタンスにストリーマへの接続を許可するかを制御します。 信頼された Call Bridge がストリーマと同じサーバで実行されている場合は、Call Bridge の公開証明書/証明書バンドルの名前を指定して streamer trust コマンドを発行するだけで十分です。Call Bridge が別のサーバで実行されている場合は、まず、ストリーマを有効にしたサーバに、Call Bridge の公開証明書/証明書バンドルを SFTP を使用してコピーする必要があります。
streamer trust none	すべての信頼設定をクリアします。
streamer listen <a|b|c|d|lo|none [:><port>] allowed list> **recorder listen a b**	ストリーマがリッスンするインターフェイスとポートを設定します。streamer enable コマンドでリスニングを開始するには、サービスを有効にする必要があります。オプションの port 引数のデフォルトは 443 です。

Cisco の法的情報

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されています。ソフトウェアライセンスまたは限定保証書が見つからない場合は、CISCO の代理店に連絡してコピーを入手してください。

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.
ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図などの図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

この文書の印刷されたハードコピーおよび複製されたソフトコピーは、すべて管理対象外と見なされます。最新バージョンについては、現在のオンラインバージョンを参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所と電話番号は、当社の Web サイト（http://www.cisco.com/jp/go/offices）をご覧ください。

Cisco の商標