Cisco Meeting Server

ミーティングサーバアプライアンスのセットアップガイド

Cisco Meeting Server Medium

2026 年 3 月 6 日

目次

変更履歴

日付	変更履歴	変更概要
2026 年 1 月 29 日	Medium プラットフォームのサポート	ミーティングサーバ M8 ミディアム（PID：CMS-M-M8-K9） をご紹介します。

1 はじめに

Cisco Meeting Server Medium プラットフォームは、AMD Genoa（第 4 世代）プロセッサを搭載した事前構成済みの Cisco UCS C245 M8 ラックサーバを使用して、Cisco UCS テクノロジーに基づいて構築されています。

Medium プラットフォームには、以下の利点があります。

- 高密度 CPU（384 個の vCPU）
- ハイパーバイザーを必要とせず、ベアメタル環境で動作するように最適化されたミーティングサーバアプリケーション
- 最大 40G の光ファイバーポート接続

2 Cisco Meeting Server Medium のインストールと初期設定

2.1 開梱と初期起動

1. Meeting Server、電源コード、コンソールアダプタ、およびラックキットを開梱します。
2. ミーティングサーバを配置します。詳しくは Cisco UCS C245 M8 インストールガイドを参照してください。
3. イーサネットケーブルをミーティングサーバ背面の SFP ポート（Ethernet1）に接続し、イーサネットネットワークに接続します。
4. 電源コードを各電源に接続し、電源に接続します。
5. Meeting Server 前面の電源ボタンを押します。 最初に電源をオンにした後、自動的に停止と再起動を複数回繰り返します。
6. コンソールを Meeting Server に接続して続行します。 モニタとキーボード、またはネットワーク接続上の仮想コンソールのいずれかを使用することができます。次のオプションから選択します。

2.1.1 コンソールオプション 1 - モニタとキーボード

1. Meeting Server の背面にある VGA ポート、または前面のコンソールポートに VGA 接続のモニタを接続します。
2. キーボードを Meeting Server の背面にある USB ポート、または前面のコンソールポートに接続します。
   ミーティングサーバは起動が完了すると自動的にコンソール画面に切り替わり、モニタに表示されます。

2.1.2 コンソールオプション 2 - ネットワーク経由の仮想コンソール

Meeting Server に接続するためのモニタとキーボードが利用できない場合は、この方法を使用します。

1. お使いのコンピュータのシリアルポートを、ルーターおよびスイッチに付属の標準的な青い Cisco RJ-45 DB-9 ヌルシリアルケーブルを使って Meeting Server 背面の 10101 とラベル付けされた RJ-45 ポートに接続します。

2. ターミナルプログラムを開き、シリアルポート/アダプタの COM ポートを選択し、ターミナル設定を 115200 ボー、パリティなし、8 データビット、1 ストップビットに設定します。
3. 2 つ目のイーサネット LAN ポートを、Meeting Server 背面の RJ-45 ポート（M1 とラベル付けされています）に接続します。 ネットワーク接続を 1 つ分しか確保できない場合は、Ethernet1 に接続されている LAN ケーブルを取り外し、一時的に M1 ポートに接続して、仮想機能を有効化しますコンソールに接続し、設定後に Ethernet1 に戻します。 仮想コンソールを使用するには、M1 ポートが接続され、有効な IP アドレスで構成されている必要があります。
4. Meeting Server の電源が接続されていることを確認します。 そうでない場合、CIMC 管理インターフェイスが起動するよう、数分間差し込んでいることを確認します。 CIMC が機能するために Meeting Server の電源がオンになっている必要はありませんが、電源に接続されている必要があります。 （CIMC ステータスの外部インジケータはありません。）
5. ターミナルプログラムで、**Escape と 9 のキーを同時に押して、**ポートを CIMC に切り替えます。 ユーザー名のプロンプトが表示されます。
6. デフォルトのユーザ名とパスワードを入力してください（ユーザ名：**admin**、パスワード：指定されたとおり）。
7. 初めてログインするとき、パスワードを適切なものに変更するように指示するプロンプトが表示されます。 プロンプトに従って、新しいパスワードを設定します。
8. ログインしたら、コマンドプロンプトで **scope cimc** コマンドを入力します。CIMC メニューを開いたことを反映して、コマンドプロンプトが変わります。
9. **show network detail** コマンドを入力して、管理イーサネットインタフェースの現在の設定を表示します。これには、サーバーが（ネットワーク上で利用可能な場合）DHCP 経由で取得した現在の IP アドレスも表示されます。 表示されている IPv4 アドレスをメモします (DHCP が利用できる場合)。
10. DHCP が利用できず、静的 IP を設定する必要がある場合、次のコマンドを使用し、サンプル値をネットワークに適した値に変更します。 （これらのコマンドは、ユーザーがすでに CIMC 範囲に入っていることを前提としています。）

```
scope network
set dns-use-dhcp no
set dhcp-enabled no
set v4-addr 10.1.2.3
set v4-netmask 255.255.255.0
set v4-gateway 10.1.2.1
commit
```

11. **show network detail** を入力して変更を確定します。 完了したら、コマンド **exit** を 2 回入力して、CIMC からログアウトします。

12. PC のブラウザに切り替え、設定した IP アドレスまたは CIMC シリアルインターフェイスから取得した IP アドレスにアクセスします。 証明書のセキュリティ警告を閉じると、Cisco ランディングページにユーザー名とパスワードのフィールドが表示されます。
13. ユーザー名：**admin** と、初めて CIMC に接続したときに設定したパスワードを使用してログインします。
14. サーバ概要ページが読み込まれたら、[アクション] の下にある [KVM の起動] リンクをクリックします。お使いのオペレーティングシステムとブラウザによっては、セキュリティ警告やダイアログが表示される場合があります。 アプリケーションがロードされるまで続行すると、サーバーに直接接続している場合と同様に、画像を監視できます。 サーバーの電源がオフの場合、**「信号がありません」**という大きな緑色のウィンドウが表示されます。
15. サーバの電源がオフになっている場合は、[アクション] タブで [電源] メニューを選択し、[電源オン] をクリックしてサーバを起動します。数分後には、ミーティングサーバのコンソール画面が表示されるはずです。

ローカルモニタとキーボードを使用して接続しているかのように、仮想コンソールを使用できます。

仮想コンソールを使用している場合に役立つ情報

- CIMC は Meeting Server 用の強力な帯域外管理インターフェイスであり、Meeting Server がラックまたはコンピュータ室に設置されている場合に使用することを推奨します。 この管理インターフェースはミーティングサーバアプリケーションでは使用されないため、接続を維持するには、M1 イーサネットポート専用の LAN 接続を確保する必要があります。 (NIC 共有オプションは、Cisco UCS Server のドキュメントにも記載されています。)
- 1 つのネットワーク接続のみで仮想コンソールを使用しており、一時的に M1 インターフェイスにそれを使用していた場合：
    a. インストールを完了するために、仮想コンソールはもう必要ありません。サーバーの M1 インタフェースからイーサネットケーブルを外し、イーサネット 1 ポートに再接続します。

b. インターフェースに DHCP を使用している場合は、イーサネットケーブルを接続した後、新しい IP アドレスを取得するためにサーバを再起動する必要があります。 再起動するには、サーバー前面の電源ボタンを短く押します。サーバーが自動シャットダウンを開始します（これには数分かかります）。 電源がオフになったら、電源ボタンを使用してオンにします。 仮想コンソールが使用していたネットワークを切断しているため、サーバーが取得した IP アドレスを確認することはできません。 IP アドレスを確認するには、DHCP 管理者に連絡して、サーバーが割り当てられている IP アドレスを確認します。 Ethernet1 インターフェースの MAC アドレスは、Cisco Meeting Server Medium の前面にある引き出し式のタブに記載されています。

これで、サーバ背面の Ethernet1 ポートにイーサネットケーブルが接続され、ミーティングサーバが使用している IP アドレスがわかるはずです。

2.2 Cisco Meeting Server Medium コンソールへのアクセス

ISO イメージが破損している、または起動できない場合は、ISO イメージの再フラッシュに関するサポートを受けるため、シスコサポートチームにお問い合わせください。

ミーティングサーバインスタンス自体には、その IP アドレスに接続するか、CIMC コンソール機能を介してアクセスできます。

1. ネットワークに DHCP がある場合は、現在の Meeting Server IP アドレス見つけるために、Meeting Server または KVM コンソールにログインし、**`IPV4 a`** コマンドを実行します。
2. 初めてログインする際は、ユーザ名とパスワードの入力を求められます。 ユーザ名「admin」でログインし、Enter キーを押してパスワードフィールドをスキップします。
3. その IP アドレスに SSH 接続することで、ミーティングサーバソフトウェアの設定を続行できます。
4. パスワードのリセットが求められます。
5. ネットワークに DHCP がない場合は、第 1 章 (または、『MMP コマンド ライン リファレンス ガイド』で説明されているとおり、KVM コンソールの仮想マシンコンソールまたは、Meeting Server MMP コマンド **`ipv4`** または **`ipv6`** を使用して、IP アドレスを VM に割り当てる必要があります。

注意：パスワードの有効期限は 6 か月です。

インストール後、完全に機能する Cisco Meeting Server が利用可能になり、次のように実行できます。

- 単一のサーバ上で有効になっているすべてのコンポーネントを備えた完全なソリューション(単一結合サーバ展開モデル)、
- 内部ネットワークに導入されたコアサーバーで一部のコンポーネントが有効になっているスプリット導入、および DMZ に導入された Edge サーバーで他のコンポーネントが有効になっているスプリット導入（シングルスプリットサーバー導入モデル）、
- クラスタ化された複数の Call Bridge とデータベースを使用した、スケーラブルでレジリエントな導入により、使用率の増加に対応し、ダウンタイムを最小限に抑えます。

2.3 インストールされているソフトウェアを確認する

Cisco Meeting Server Medium には、Cisco Meeting Server ソフトウェアがプリインストールされた状態で出荷されます。 ただし、Cisco Meeting Server ソフトウェアを設定する前に、Cisco Connection Online (CCO) で入手可能な最新バージョンの Cisco Meeting Server 3.11 にアップグレードすることをお勧めします。アップグレードするには、該当ソフトウェアバージョンのリリースノートに記載されている手順に従ってください。

ヒント：これでポート A が設定されました。SFTP を使用して、ポート A 経由で Cisco Meeting Server ソフトウェアのバックアップとアップグレードを行います。

残りの設定プロセスは、 第 3 章で説明されているとおりです。

3 設定

3.1 Meeting Server Medium へのデプロイメントに関する注意点

- 以下に説明する構成は、スタンドアロンノードにのみ適用されます。 クラスター展開については、 スケーラブルで回復力のある展開ガイドを参照してください。
- 複数のデータベースを混在させたデプロイメントはサポートされていません。

3.2 Cisco Meeting Server 管理者アカウントの作成

ユーザー名「admin」は安全性が低いため、セキュリティ上の理由から、独自の管理者アカウントを作成することをお勧めします。 さらに、1 つのアカウントのパスワードをなくした場合に備えて、2 つの管理者アカウントを持っておくことをお勧めします。そうした場合でも、もう一方のアカウントでログインして、なくしたパスワードをリセットできます。

MMP コマンド **`user add <name> admin`** を使用します。詳細については『MMP コマンドリファレンスガイド』を参照してください。 パスワードを 2 回入力するように指示されます。新しいアカウントでログインすると、パスワードの変更が求められます。

注意：パスワードの有効期限は 6 か月です。

新しい管理者アカウントを作成したら、デフォルトの「admin」アカウントを削除します。

メモ：管理者レベルの MMP ユーザーアカウントは、Call Bridge のウェブ管理インターフェイスにログインするためにも使用できます。 ウェブ管理インターフェイスを通じてユーザーを作成することはできません。

3.3 IPv4 用のネットワーク インターフェースをセットアップする

メモ: これらの手順は IPv4 用ですが、IPv6 用の同等のコマンドがあります。 詳細については、MMP コマンドリファレンス を参照してください。

Cisco Meeting Server の仮想化導入では、最初はインターフェイス「a」という 1 つのネットワーク インターフェイスだけですが、最大で 4 つまでサポートされます（次の項を参照）。MMP は仮想展開のインターフェイス a で実行されます。

1. ネットワークインタフェース速度、二重通信、自動ネゴシエーションのパラメータを設定するには、**iface** MMP コマンドを使用します。「a」インタフェースの現在の設定を表示するには、MMP で入力します。

   iface a

   コマンド **iface (a|b|c|d) <speed> (full|on|off)** を使用して、ネットワークインタフェース速度（Mbps）、全二重、および自動ネゴシエーションパラメータを設定します。 たとえば、インターフェイスを 1GE、全二重に設定します。

   iface a 1000 full

2. "a" インターフェイスは、最初は DHCP を使用するように構成されています。 既存の構成を表示するには、次のように入力します。

   ipv4 a

   a. DHCP IP 割り当てを使用している場合、これ以上の IP 設定は必要ありません。ステップ 3 に進みます。

   b. 静的 IP 割り当てを使用している場合:

      ipv4 add コマンドを使用して、指定されたサブネットマスクとデフォルトゲートウェイを持つインターフェースに静的 IP アドレスを追加します。

      たとえば、ゲートウェイが 10.1.1.1 でプレフィックス長が 16 のアドレス 10.1.2.4 (ネットマスク 255.255.0.0) をインターフェイスに追加するには、次のように入力します。

      ipv4 a add 10.1.2.4/16 10.1.1.1

      IPv4 アドレスを削除するには、次のように入力します。

      ipv4 a del <address>

3. DNS 構成の設定

   Meeting Server は、SRV レコードのルックアップを含むアクティビティの多くで DNS ルックアップを必要とし、簡素化された導入に必要です。 Meeting Server をネットワークのデフォルトの DNS リゾルバに指向することをお勧めします。forwardzone の値にはピリオド「.」を使用します。

   a. DNS 設定を出力するには、次のようにタイプします。

      dns

   b. アプリケーション DNS サーバーを設定するには、次のコマンドを使用します。

      dns add forwardzone <domain name> <server IP>

メモ：フォワードゾーンは、ドメイン名とサーバアドレスのペアです。名前が DNS 階層で指定のドメイン名より下にある場合、DNS リゾルバーは指定のサーバーにクエリできます。 任意の特定のドメイン名に対して複数のサーバーを指定して、ロードバランシングとフェイルオーバーを提供できます。 「.」を指定するのが一般的です。これは、すべてのドメイン名に一致する DNS 階層のルート、つまりドメイン名を意味します。

例えば：

```
dns add forwardzone。 10.1.1.33
```

c. DNS エントリを削除する必要がある場合は、次のコマンドを使用します:

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

例えば：

```
dns del forwardzone。 10.1.1.33
```

3.4 Call Bridge の設定

Call Bridge には、SIP 通話制御デバイスおよび Lync フロントエンド (FE) サーバとの TLS 接続を確立するために使用されるキーと証明書のペアが必要です。 Lync を使用している場合、この証明書は Lync FE サーバによって信頼される必要があります。

コマンド **callbridge listen <インターフェース>**を使用して、リッスンするインターフェースを設定できます（A、B、C または D から選択）。 デフォルトでは、Call Bridge はどのインターフェイスもリッスンしません。

1. 『証明書のガイドライン』の説明に従って、証明書を作成してアップロードします。
2. MMP にログインし、インターフェイス A でリッスンするように Call Bridge を設定します。

```
callbridge listen a
```

メモ: Call Bridge は、別の IP アドレスに NAT されていないネットワーク インターフェイスでリッスンしている必要があります。 これは、リモート サイトと通信するときに、Call Bridge が SIP メッセージのインターフェイスで設定されたものと同じ IP を伝達する必要があるためです。

3. 次のコマンドを使用して、証明書を使用するように Call Bridge を設定します。これにより、Lync FE サーバーと Call Bridge の間で TLS 接続を確立できます。次に例を示します。

```
callbridge certs callbridge.key callbridge.crt
```

完全なコマンドと CA が提供する証明書バンドルの使用については、『証明書ガイドライン』で説明されています。

4. 変更を適用するために、Call Bridge インターフェイスを再起動します。

```
callbridge restart
```

3.5 ウェブ管理インタフェースを設定する

ウェブ管理インターフェイスは、Call Bridge へのインターフェイスとして機能します。Cisco Meeting Server の API はこのウェブインターフェイスを通してルーティングされます。

Web 管理インターフェースは HTTPS 経由でのみアクセス可能です。セキュリティ証明書を作成し、Cisco Meeting Server にインストールする必要があります。

メモ：ウェブ管理インターフェイスではなく、API を通じて Call Bridge を設定する場合でも、ウェブ管理インターフェイス用に証明書をアップロードする必要があります。

以下の情報は、Cisco が秘密鍵の生成の要件を満たしていることを信頼していることを前提としています。 ご希望であれば、秘密鍵と証明書を外部で生成することも可能です。公開認証局（CA）を使用し、外部で生成された鍵と証明書のペアを SFTP を使用して Cisco Meeting Server の MMP にロードします。

メモ：Cisco Meeting Server をラボ環境でテストする場合、サーバー上でキーと自己署名証明書を生成できます。 自己署名証明書と秘密鍵を作成するには、MMP にログインして次のコマンドを使用します。

```
pki selfsigned <key/cert basename>
```

ここで、**<key/cert basename>** は、生成されるキーと証明書を指定します。例：「pkiself signed webadmin」は、webadmin.key と webadmin.crt（自己署名）を作成します。自己署名証明書は、プロダクション環境での使用は推奨されていません。

注：署名済み証明書と秘密鍵を Cisco Meeting Server に転送する前に、証明書ファイルを確認してください。 CA が証明書のチェーンを発行している場合、チェーンから証明書を抽出する必要があります。 証明書ファイルを開き、BEGIN CERTIFICATE および END CERTIFICATE の行を含む特定の証明書テキストをコピーして、テキストファイルに貼り付けます。.crt、.cer または .pem の拡張子を持つ証明書としてファイルを保存します。残りの証明書チェーンをコピーして別のファイルに貼り付けます。中間証明書チェーンと認識できるように明確な名前を付け、同じ拡張子（.crt、.cer または .pem）を使用します。 中間証明書チェーンは順番通りである必要があります。チェーンを発行した CA の証明書が最初で、ルート CA の証明書がチェーンの最後です。

3.5.1 HTTPS アクセス用の Web 管理インターフェースの設定

注：導入時にウェブ管理者インターフェイスがインターフェイス A のポート 443 を使用するように自動的にセットアップされます。しかし、ウェブブリッジも TCP ポート 443 を使用します。ウェブ管理者インターフェイスとウェブブリッジが同じインターフェイスを使用している場合は、ウェブのポートを変更する必要があります管理インターフェイスを 445 などの非標準ポートに変更するには、MMP コマンド **`webadmin listen <interface> <port>`** を使用します。

1. MMP にログインし、以下のコマンドを使用して秘密鍵と証明書署名要求（CSR）を生成します。
   `pki csr <key/cert basename> [<attribute>:<value>]`
   ここで、

   <キー/証明書ベース名> これは、新しいキーと CSR を識別する文字列です（たとえば、「webadmin」は「webadmin.key」と「webadmin.csr」ファイルを生成します）。
2. 「証明書ガイドライン」に記載されているとおりに証明書を生成します。
3. MMP への SSH 接続を確立してログインします。
4. SFTP を使用して、秘密鍵/証明書のペアと証明書バンドル (オプション) をウェブ管理インターフェイスにアップロードします。
5. 証明書を指定する前にウェブ管理インターフェイスを無効にしてください。

   `webadmin disable`
6. 次のコマンドを使用して、ステップ 4 でアップロードした秘密鍵/証明書のペアを指定します。

   `webadmin certs <keyfile> <certificatefile> [<cert-bundle>]`

   `keyfile` と **`certificatefile`** は、一致する秘密キーと証明書のファイル名です。 CA が証明書バンドルを提供している場合は、バンドルも証明書とは別のファイルとして含めます。 次に例を示します。

   `webadmin certs webadmin.key webadmin.crt webadminBundle.crt`
7. ウェブ管理インターフェイスを再起動します。

   `webadmin restart`
8. ウェブ管理インターフェイスを有効にします。

   `webadmin enable`

例えば：

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

ウェブ管理者インタフェースにアクセスできることをテストします。たとえば、ブラウザに https://cms-server.mycompany.com（または IP アドレス）に相当するものを入力し、先ほど作成した MMP ユーザーアカウントを使用してログインします。

注： ライセンスなしで、90 日間フル機能のトライアルモードをご利用いただけます。この場合、ウェブ管理インターフェイスには、この期間中、「この CMS は現在ライセンスされていません」と表示されます。 Smart Licensing とライセンスの仕組みの詳細については、を参照してください。

3.6 Web Bridge 3 を設定する

Web Bridge 3 は、参加者がブラウザベースの Cisco ウェブアプリクライアントを使ってミーティングに参加できるようにするMeeting Server のコンポーネントです。 Web Bridge 3 は Cisco Meeting Server web app の参加者にウェブサーバーを提供し、Call Bridge および TURN サーバーコンポーネントと連携してクライアントをサポートします。 .

注: Web アプリを使用していない場合は、Web Bridge 3 を展開する必要がないため、このセクションをスキップできます。

- 内部ネットワークからウェブ アプリ クライアントをサポートする必要がある場合は、コアのメイン Meeting Server インスタンスでWeb Bridgeを設定し、この項の手順を完了する必要があります。
- ウェブアプリ用のプロキシおよび TURN Server として Cisco Expressway を使用している場合、コアのメインのMeeting Serverインスタンスで Web Bridgeを設定し、この項の手順を完了する必要があります。
- Edge Meeting Server モデルを使用している場合、Web Bridgeを Edge だけで実行するか、Edge とメインの内部Meeting Server インスタンスの両方で実行するかのオプションがあります。 内部サーバーでWeb Bridgeを有効にすると、クライアントは DMZ のWeb Bridgeに接続しなくてもウェブアプリを使用できます。 Edge Meeting Server モデルを使用した導入では、DMZ と内部サーバーインスタンスの両方で Web Bridge を実行することを推奨します。 この項の手順を完了し、Edge インスタンスでWeb Bridgeを設定し、コアでメインのMeeting Serverインスタンスを設定します。

注： Core と Edge の両方でWeb Bridgeを実行するには、クライアントが、内部インスタンスまたは Edge インスタンス (必要に応じて) に同じWeb Bridgeのホスト名を解決する必要があります。これは通常「スプリットDNS」と呼ばれ、DNS サーバーは、クライアントが配置されている場所に基づいて、名前をアドレスに解決します。

警告：Expressway ユーザーのための重要な注意点
Web Bridge 3 とウェブ アプリを展開する場合、Expressway バージョン X14.3 以降を使用する必要があります。以前の Expressway バージョンはWeb Bridge 3 ではサポートされません。

注：ウェブアプリの詳細は、「Cisco Meeting Server web app の重要な情報」 を参照してください。

3.6.1 Web Bridge 3 の設定に役立つ情報

以下は、ウェブ アプリを使用できるようにWeb Bridge 3 を設定するのに役立つ情報です。

- 「Call Bridge to Web Bridge」プロトコル（C2W）は、Call Bridge と WebBridge3 間のリンクです。 間にコントロールチャネルを確立するのは、Call BridgeからWeb Bridgeへの発信接続です。 証明書は C2W 接続の認証とセキュリティ保護に使用されます。 C2W は Call Bridge - Web Bridgeのトラフィック専用であり、ユーザや他のサービスによって使用されることはありません。
- C2W リスニングポートは、Call Bridge が HTTPS 接続を使用して Web Bridge に接続できるように、Web Bridge サーバー（**`webbridge3 c2w listen`** を使用）で定義されます。 使用するポート番号に既定値の設定はありませんが、このガイドでは例として 9999 を使用します。 この接続は証明書で保護する必要があります。
- 外部アクセスから C2W ポートを保護することを推奨します。Call Bridge からのみ到達可能である必要があります。
- Call Bridge は、連携するように設定された各 Web Bridge の C2W インターフェイスに一意に到達できる必要があります (C2W 接続では、Web Bridge 3 インスタンスごとに一意のホスト名または IP を使用する必要があります)。
- ウェブ アプリ クライアントはWeb Bridgeに到達するための単一のアドレスを持つため、複数のWeb Bridgeが使用される場合、DNS またはロード バランサ ソリューションを使用して、共有名を利用可能なWeb Bridge インスタンスに転送する必要があります。クライアントからWeb Bridgeへの接続は、通話以外のアクティビティではステートレスであり、セッションは単一のWeb Bridgeに留まる必要はありません。

- TLS 接続を確立するとき、両側は確認のために証明書を提示する必要があります。 Call Bridge は、 **`callbridge certs`** コマンドを使用して証明書セットを使用し、Web Bridgeは、 **`webbridge3 c2w certs`** コマンドを使用して証明書セットを使用します。
- Web Bridgeは、Web BridgeのC2W トラストストアにある、または信頼ストアの **`webbridge3 c2w trust`** で設定された証明書によって署名された **`Call Bridge`** とスケジューラの証明書を信頼します。 特定の証明書の一致のみが許可されるように、このWeb Bridgeに接続する Call Bridge 証明書を含むバンドルを使用することをお勧めします (証明書ピニング)。
- Call Bridge は、Call Bridge の C2W トラストストアにある、または **`callbridge trust c2w`** で設定されたトラストストア内の証明書によって署名された Web Bridge の証明書を信頼します。 特定の証明書の一致のみが許可されるように、この Call Bridge が接続するWeb Bridgeの証明書を含むバンドルを使用することをお勧めします (証明書ピニング)。
- スケジューラは、スケジューラの C2W トラストストアにある、またはコマンド **`scheduler c2w certs <key-file> <crt-fullchain-file>`**で設定された信頼ストアの証明書によって署名されたWeb Bridgeの証明書を信頼します。
- C2W または Call Bridge に使用される証明書に拡張キー使用法が定義されている場合、Call Bridge とWeb Bridgeの間の相互 TLS 認証交換を許可するために、使用法を有効にする必要があります。 拡張キー使用法が証明書に定義されている場合、Web Bridge 3 C2W 証明書には「サーバ認証」拡張キー使用法が含まれ、Call Bridge 証明書には「クライアント認証」拡張キー使用法が含まれる必要があります。 証明書で拡張キー使用法が定義されていない場合、すべての使用法が有効であると想定されます。
- C2W 接続は内部サービス間のみであるため、公的機関によって署名された証明書を明示的に使用する必要はありません。 MMP 内で作成された自己署名証明書を使用できます。
- Web Bridge C2W 証明書の SAN/CN は、Call Bridge API でWeb Bridge 3 を登録するために使用される c2w:// URL で使用される FQDN または IP アドレスと一致する必要があります。 これが一致しない場合、Call Bridge は TLS ネゴシエーションに失敗し、Web Bridgeが提示する証明書を拒否し、Web Bridgeとの接続に失敗します。

注： パブリック CA によって署名された証明書が必要な場合は、FQDN を使用する必要があります。 (パブリック CA は、IP アドレスを含む証明書に署名できません。) C2W アドレスで IP アドレスを使用する場合、C2W 接続はパブリック接続ではないため、独自の証明書を作成できます。パブリック CA を使用する必要はありません。

- Web Bridgeのリッスン インターフェースに使用される証明書は、クライアントが信頼する認証局によって署名されている必要があります。これにより、クライアント接続時の証明書の警告が回避されます。 クライアントがWeb Bridgeに到達するために使用するFQDN は、クライアント接続時の証明書の警告を回避するために、証明書の CN または SAN リストにある必要があります。
- 証明書の一般的な情報については、導入に応じた 証明書のガイドライン を参照してください。

3.6.2 Web Bridge 3 サービスを有効にする

Cisco Expressway プロキシを使用している場合、または Call Bridge に直接到達できるウェブアプリクライアントをサポートしている場合、Web Bridgeサービスはコアメディア Serverインスタンスで有効になっている必要があります。 Meeting Serverの Edge 導入を使用する場合、Web Bridge 3 はすべての Edge インスタンスで実行する必要があり、オプションで、Call Bridge が実行されているコア Meeting Server インスタンスでも実行できます。

Web Bridge 3 が実行される各Meeting Server インスタンスでこれらの手順を完了します。

1. MMP に SSH でログインします。
2. Web Bridgeがウェブ サーバーに使用するインターフェイスとポートを次のコマンドで設定します。

   `webbridge3 https listen <interface>:<port>`.

   最初のインターフェイスとポート 443 の使用を推奨します。 例：

   `webbridge3 https listen a:443`
3. Web Bridgeがウェブ サーバーに使用する HTTPS 証明書とキー ペアを次のコマンドで設定します。 **`webbridge3 https certs <key file> <full certificate chain file>`**。

   このコマンドは、証明書が完全な証明書チェーン (エンド エンティティ証明書で始まり、すべての中間署名認証局を含み、ルート証明書で終わる証明書バンドル) として定義されることを要求します。 例：

   `webbridge3 https certs wb3-https.key wb3-https-fullchain.crt`
4. コマンドを使用して、C2W 接続のインターフェイスとポートを設定します。

   `webbridge3 c2w listen <interface>:<port>` .

   最初のインターフェイスとデフォルトのサンプル ポート 9999 を使用することを推奨します。 例：

   `webbridge3 c2w listen a:9999`

5. C2W 接続証明書をコマンド **webbridge3 c2w certs** で設定します
   <キーファイル><完全な証明書チェーンファイル>。
   例：
   webbridge3 c2w certs wb3-c2w.key wb3-c2w-fullchain.crt

   注： この証明書には、証明書の CN または SAN リストにある C2W インターフェイスの FQDN または IP アドレスが含まれている必要があります。 追加情報は、 Web Bridge 3 で使用する接続証明書を に設定するにはどうすればよいですか? も参照してください。

6. Web Bridge 3 の C2W トラストストアは、どの Call Bridge がこの Web Bridge に接続できるかを制御するように設定する必要があります。 信頼バンドルには、このWeb Bridge に接続するすべての Call Bridge の Call Bridge 証明書、または Call Bridge 証明書に署名した CA の証明書が含まれている必要があります。 最大限のコントロールを行うために、署名機関の証明書ではなく、バンドル中の個々の Call Bridge 証明書 (証明書ピニング) を使用することを推奨します。 Web Bridgeの c2w trust バンドルを次のコマンドで設定します: **webbridge3 c2w trust <certificate bundle>**

   webbridge3 c2w trust wb3-c2w-trust-bundle.crt

7. http リダイレクトを有効にします。 これは任意ですが、エンドユーザーの使いやすさのために推奨されています

   webbridge3 http-redirect を有効にする

8. Web Bridge サービスを有効にする

   webbridge3 enable

Web Bridgeが実行される各Meeting Serverインスタンスに対して上記の手順を繰り返し、各インスタンスで使用される証明書またはキーペアが正しいことを確認します。

C2W は、Call Bridge およびWeb Bridgeインスタンス間のコントロールインターフェイスであり、Web Bridgeが導入されている場合、Call Bridge で設定する必要があります。 Call Bridge の C2W 信頼バンドルには、この Call Bridge が接続するすべてのWeb Bridgeの C2W 証明書、またはWeb Bridgeの C2W 証明書に署名した証明書が含まれている必要があります。最大限のコントロールを行うために、署名機関の証明書ではなく、バンドル中の個々の Web Bridge C2W 証明書（証明書ピニング）を使用することを推奨します。

1. Call Bridge を実行している内部Meeting Serverの MMP インターフェイスに接続します。
2. Call Bridge リッスン インターフェイスを設定するで実行した手順で、Call Bridge に証明書がすでに設定されている必要があります。 コマンド **callbridge** を実行して確認し、[キーファイル] と [証明書ファイル] の設定が設定されていることを確認します。 そうでない場合は、先に進む前に、 Call Bridge リスニングインターフェイスを設定する の手順を繰り返します。 Call Bridge は C2W 機能の証明書で設定する必要があります。

3. コマンド **`callbridge trust c2w <certificate bundle file>`** を使用して、Web Bridge インスタンスの C2W 証明書を含む証明書バンドルで Call Bridge の C2W トラストストアを設定します。 例：

   ```
   callbridge trust c2w c2w-callbrige-trust-store.crt
   ```

   注：範囲で制限されている場合を除き、Call Bridge は、Meeting Server API で定義されているすべてのWeb Bridgeへの接続を試みます。

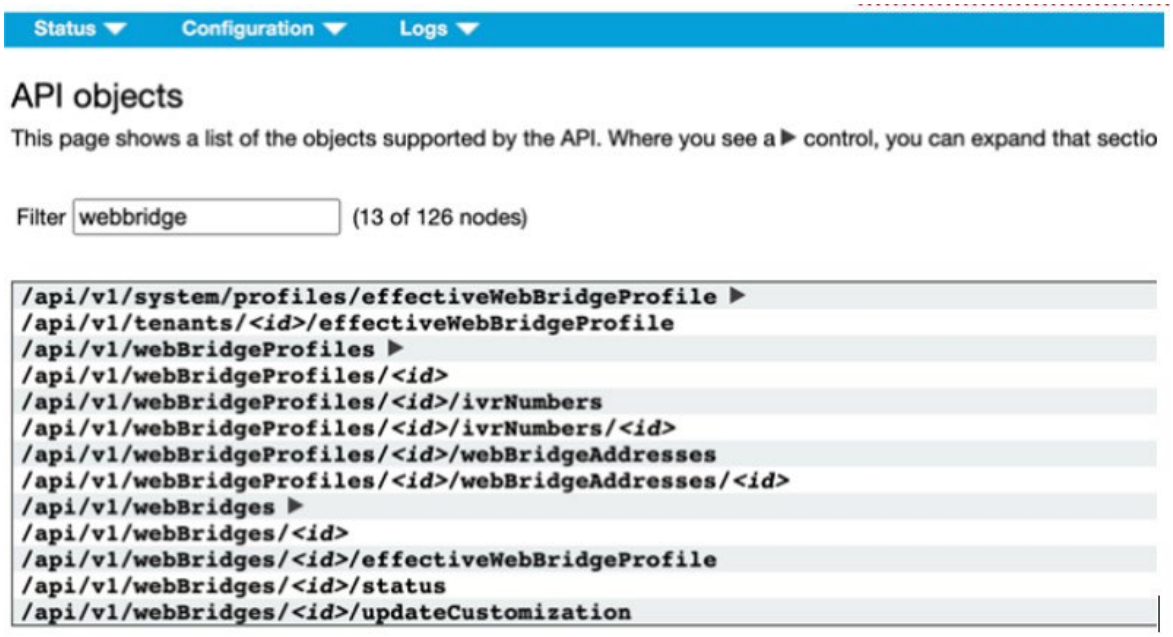
4. Call Bridge を再起動します

   ```
   callbridge restart
   ```

3.6.3 Web Bridge アドレスを使用して Call Bridge を設定する

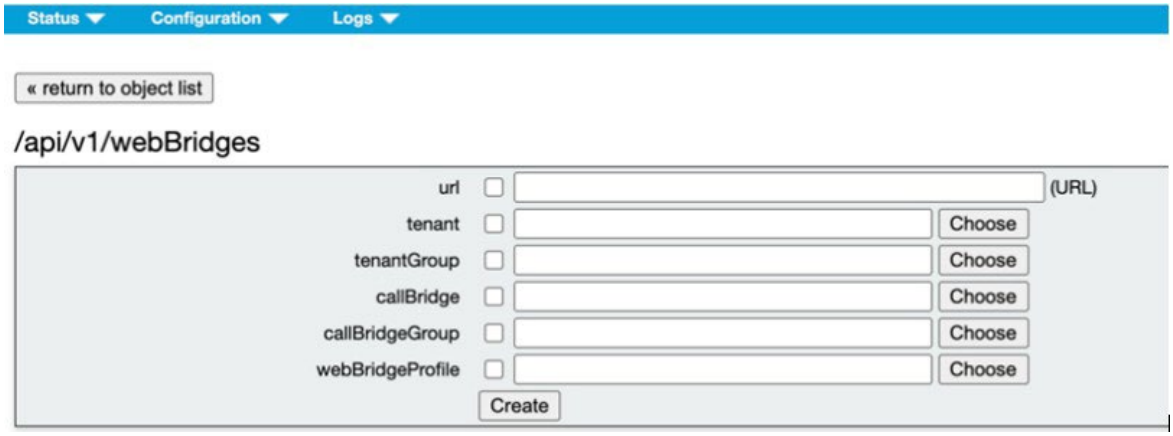
Meeting Server API でWeb Bridgeのエントリを作成することで、Call Bridge が接続する各Web Bridge (共存するWeb Bridgeを含む) の C2W アドレスを Call Bridge に通知する必要があります。 このガイドでは、Meeting Serverのウェブ管理インターフェースの API エクスプローラーを使用して、このタスクを完了する方法を説明します。

1. ミーティングサーバの Web 管理インターフェースにログインし、 **設定** > **API** を選択します。
2. [フィルタ] ボックスに「**`webBridges`**」と入力し、リストビューをフィルタリングします。ここに示すように。



3. 表示されたリストから [**`/api/v1/webBridges`**] 行を見つけ、[▶] アイコンをクリックして導入します。

4. [Create new] をクリックして新しいWeb Bridgeオブジェクトを作成します。
   次のパラメータフィールドが次のように表示されます。



5. url フィールドには、*c2w://<Web Bridge FQDN>:<c2w port>* の形式で、追加する Web Bridge の C2W インターフェースの FQDN アドレスを入力します。 例：

   c2w://cmsedge1.company.com:9999

   注： ここで入力する FQDN は、Web Bridge 3 の C2W インターフェイスに割り当てられた証明書の CN または SAN 名のリストにあり、Web Bridgeの C2W インターフェイスの IP に解決する必要があります。 IP アドレスは、C2W 証明書が証明書の SAN または CN の IP アドレスを持つ場合にのみ使用できます。

6. 新しいWeb Bridgeエントリを保存するために **作成** をクリックします。

複数のWeb Bridgeがある場合、上記の手順を繰り返し、Web Bridgeの各インスタンスに対して 1 つのWeb Bridgeオブジェクトを作成します。

付録 A Cisco Meeting Server Medium の技術仕様

A.1 物理仕様：

シャーシ: Cisco UCS C245 M8 サーバーのインストールとサービスガイド

重量: 19+ kg (40 ポンド)

サイズ：高さ 2RU

A.2 環境仕様

動作温度：5°C～35°C（41～95°F）

動作湿度：8%～90%（結露なきこと）

A.3 電気的仕様

電源仕様については、該当する Cisco UCS C245 M8 サーバインストール および サービスガイドを参照してください。

A.4 ビデオおよび音声仕様：

この表は、Cisco Meeting Server ソフトウェアをホストしているプラットフォーム間でのコールキャパシティの比較を示しています。

表 1：ミーティングサーバプラットフォーム間の通話容量

Cisco Meeting Server プラットフォーム		Cisco Meeting Server 1000 M7（ノードあたり）	Cisco Meeting Server Medium M8（ノードあたり）
個々の Meeting Server またはクラスター内のサーバ (メモ 1、2、3、および 4) と Call Bridge グループ内の Meeting Server	1080p30 720p30 SD 音声通話	120 240 480 3000	225 450 850 3000
	HD 参加者電話会議ごとサーバごと		
	web app のコールキャパシティ（内線通話 & 外線通話を呼び出しています）：		
	フル HD HD SD 音声通話	120 240 480 3000	225 450 850 3000
Call Bridge グループ内の Meeting Server	サポートされているコール タイプ		
	読み込み制限	240,000	450,000

Meeting Server M8 プラットフォームは、最大 450,000 の負荷制限をサポートしています。

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式、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、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。 添付されていない場合には、代理店にご連絡ください。

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.

本契約におけるその他の保証にかかわらず、これらのサプライヤーのすべてのドキュメント ファイルおよびソフトウェアは、すべての欠陥を含めて「現状のまま」提供されます。 CISCO およびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズ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システムズ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。

★定型★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。 ★定型★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、およびその他の図は、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。 最新版については、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 www.cisco.com/go/offices. をご覧ください。

Cisco の商標または登録商標