Video Mesh の導入

Video Mesh 導入タスクのフロー

始める前に

環境の準備

手順

	コマンドまたはアクション	目的
ステップ 1	Video Mesh ノード ソフトウェアのインストールと設定 （5 ページ）	VMware ESXi または vCenter を実行しているホストサーバーに Video Mesh ノードを展開するには、次の手順に従います。ソフトウェアをオンプレミスでインストールするとノードが作成されます。その後、ネットワーク設定などの初期設定を実行します。それを後からクラウドに登録します。
ステップ 2	Video Mesh ノード コンソールへのログイン （9 ページ）	コンソールに初回サインインします。Video Mesh ノード ソフトウェアには、デフォルトのパスワードが設定されています。ノードを設定する前に、この値を変更する必要があります。
ステップ 3	コンソールでの Video Mesh ノードのネットワーク構成の設定 （10 ページ）	仮想マシン上のノードのセットアップ時に設定しなかった場合に、Video Mesh ノードのネットワーク設定を構成するには、この手順を使用します。静的 IP アドレスを設定し、FQDN/ホスト名と NTP サーバーを変更します。DHCP は現在サポートされていません。
ステップ 4	デュアルネットワークインターフェイス（デュアル NIC）展開用に外部インターフェイスを設定するには、次の手順を使用します。 • Video Mesh ノードの外部ネットワークインターフェイスの設定 （12 ページ） • 内部ルーティングルールと外部ルーティングルールを追加する （32 ページ）	ノードがオンラインに戻り、内部ネットワーク構成を確認した後、ネットワークの DMZ 内で Video Mesh ノードを展開している場合は、外部ネットワークインターフェイスを設定して、企業（内部）トラフィックを外部トラフィックから分離することができます。 また、例外を作成したり、デフォルトのルーティングルールに上書きしたりすることもできます。
ステップ 5	Webex クラウドへの Video Mesh ノードの登録 （33 ページ）	次の手順を使用して、Video Mesh ノードを Webex クラウドに登録し、追加の構成を完了します。ノードの登録に Control Hub を使用する場合は、ノードを割り当てるクラスタを作成します。クラスタには 1 つまたは複数のメディアノードがあり、それぞれ特定の地理的地域のユーザーが利用します。登録

	コマンドまたはアクション	目的
		手順では、SIP コール設定の構成、アップグレードスケジュールの設定、および電子メール通知の登録も行います。
ステップ 6	次のタスクを使用して Quality of Service（QoS）の有効化と検証を行います。 • Video Mesh ノード の Quality of Service（QoS）の有効化 （37 ページ） • ウェブインターフェイスのリフレクタツールを使用した Video Mesh ノードのポート範囲の確認 （39 ページ）	適切なサービスクラスおよび特定のメディアタイプに対する既知のポート範囲で、Video Mesh ノードが、オーディオ（EF）およびビデオ（AF41）の両方に対して個別に自動で SIP トラフィック（オンプレミス SIP 登録済みエンドポイント）をマークする場合は、QoS を有効にします。この変更により、QoS ポリシーを作成し、必要に応じてクラウドからのリターントラフィックを効果的に注釈できます。 リフレクタツールの手順を使用して、ファイアウォール上で適切なポートが開かれていることを確認します。
ステップ 7	プロキシ統合のための Video Mesh ノードの構成 （40 ページ）	Video Mesh と統合するプロキシのタイプを指定するには、次の手順を使用します。透過的なプロキシを選択した場合、ノードのインターフェイスを使用してルート証明書をアップロードおよびインストールし、プロキシを確認し、考え得る問題をトラブルシュートします。
ステップ 8	呼制御タスクフローと Video Mesh の統合 （43 ページ） に従って、呼制御、セキュリティ要件、および Video Mesh を呼制御環境と統合するかどうかに応じて、次のいずれかを選択します。 • Unified CM セキュア TLS SIP トラフィックルーティングの設定 - Video Mesh （46 ページ） （TLS） • Video Mesh 用の Unified CM TCP SIP トラフィックルーティングの設定 （50 ページ） （TCP） • Video Mesh 用の Expressway TCP SIP トラフィックルーティングの設定 （54 ページ） （TCP）	SIP デバイスは、直接到達可能性をサポートしないため、Unified CM または VCS Expressway 構成を使用して、オンプレミス登録 SIP デバイスおよび Video Mesh クラスタ間の関連性を確立する必要があります。 必要なのは、呼制御環境に応じて、Unified CM または VCS Expressway を Video Mesh ノードにトランクすることだけです。

	コマンドまたはアクション	目的
ステップ 9	Unified CM と Video Mesh ノード間での証明書チェーンの交換 （58 ページ）	このタスクでは、Unified CM および Video Mesh インターフェイスから証明書をダウンロード し、1 つを他方にアップロードします。この手順では、2 つの製品間で安全な信頼を確立し、セキュアトランクの構成と併用することで、組織内の暗号化された SIP トラフィックおよびSRTP メディアが Video Mesh ノードに定着できるようにします。
ステップ 10	組織およびVideo Meshクラスタのメディア暗号化の有効化 （61 ページ）	組織および個々のVideo Mesh クラスタのメディア暗号化をオンにする場合は、次の手順を実行します。この設定では、エンドツーエンドの TLS セットアップが強制的に実行され、Video Mesh ノードをポイントするセキュアな TLS SIP トランクが Unified CM に配置されている必要があります。
ステップ 11	Webex サイトの Video Mesh の有効化 （62 ページ）	Webex ミーティングの Video Mesh ノードに最適化されたメディアを使用して、すべての Webex アプリとデバイスに参加するには、この設定を Webex サイトで有効にする必要があります。この設定を有効化することによって、クラウドで Video Mesh およびミーティングインスタンスが一緒にリンクされ、カスケードが Video Mesh ノードで発生できるようになります。この設定が有効になっていない場合、Webex アプリとデバイスは Webex ミーティングに Video Mesh ノードを使用しません。
ステップ 12	Webex アプリ ユーザーへの Collaboration Meeting Rooms の割り当て （63 ページ）	
ステップ 13	セキュアなエンドポイントでのミーティングエクスペリエンスの確認 （63 ページ）	エンドツーエンドの TLS セットアップでメディア暗号化を使用する場合は、次の手順を使用して、エンドポイントが安全に登録され、正しいミーティングエクスペリエンスが表示されていることを確認します。

Video Mesh の一括プロビジョニングスクリプト

Video Mesh 展開で多くのノードを展開する必要がある場合、プロセスには時間がかかります。https://github.com/CiscoDevNet/webex-video-mesh-node-provisioning にあるこのスクリプトを使用して、VMWare ESXi サーバーに Video Mesh ノードをすばやく展開できます。スクリプトの使用方法については、readme ファイルを参照してください。

Video Mesh ノード ソフトウェアのインストールと設定

VMware ESXi または vCenter を実行しているホストサーバーに Video Mesh ノード を展開するには、次の手順に従います。ソフトウェアをオンプレミスでインストールするとノードが作成されます。その後、ネットワーク設定などの初期設定を実行します。それを後からクラウドに登録します。

前にダウンロードしたバージョンを使用するのではなく、Control Hub（https://admin.webex.com）からソフトウェアパッケージ（OVA）をダウンロードする必要があります。この OVA は Cisco 証明書によって署名されており、カスタマー管理者のログイン情報を使用して Control Hub にサインインした後にダウンロードできます。

始める前に

- サポートされているハードウェアプラットフォームおよび Video Mesh ノード の仕様要件については、「Video Mesh ノード ソフトウェアのシステム要件とプラットフォーム要件」を参照してください。
- 次のものを用意します。
  - 以下を備えたコンピュータ
    - VMware vSphere クライアント 6.5、6.7、または 7。

      サポートされているオペレーティングシステムの一覧は、VMware のドキュメントを参照してください。
    - Video Mesh のダウンロードされたソフトウェア OVA ファイル。

      前にダウンロードしたバージョンを使用するのではなく、Control Hub から最新の Video Mesh ソフトウェアをダウンロードします。また、このリンクからソフトウェアにアクセスすることもできます。（ファイルは約 1.5 GB です。）

（注） ソフトウェアパッケージ（OVA）の古いバージョンは、最新の Video Mesh アップグレードと互換性がありません。これにより、アプリケーションのアップグレード中に問題が発生する可能性があります。必ずこのリンクから OVA の最新バージョンをダウンロードしてください。

- VMware ESXi または vCenter 6.5、6.7、または 7 をインストールして実行しているサポート対象サーバー
- 仮想マシンのバックアップとライブマイグレーションを無効にします。Video Mesh ノードクラスタはリアルタイムシステムです。仮想マシンの一時停止によって、これらのシステムが不安定になる可能性があります。（Video Mesh ノード でメンテナンス作業を実行する場合は、Control Hub のメンテナンス モードを使用します）。

手順

ステップ 1 お使いのコンピュータから、VMware vSphere クライアントを開き、サーバー上の vCenter または ESXi システムにサインインします。

ステップ 2 **[アクション（Actions）] > [OVF テンプレートの展開（Deploy OVF Template）]** に移動します。

ステップ 3 **[OVF テンプレートの選択（Select an OVF template）]** ページで、**[ローカルファイル（Local File）]** をクリックし、**[ファイルを選択（Choose Files）]** をクリックします。**videomesh.ova** ファイルがある場所に移動し、ファイルを選択して **[次へ（Next）]** をクリックします。

注意 Video Mesh ノード のインストールを実行するたびに、前にダウンロードしたバージョンを使用するのではなく、OVA を再ダウンロードすることをお勧めします。古い OVA を展開しようとすると、Video Mesh ノード は正常に動作しないか、クラウドに登録できない場合があります。古い OVA も、アップグレード中に潜在的な問題につながります。

必ずこのリンクから OVA の新しいコピーをダウンロードしてください。

ステップ 4 **[名前とフォルダの選択（Select a name and folder）]** ページで、Video Mesh ノード の **[仮想マシン名（Virtual machine name）]**を入力し（たとえば、「Video_Mesh_Node_1」）、仮想マシンノードの展開先となる場所を選択して、**[次へ（Next）]** をクリックします。

検証チェックが実行されます。完了すると、テンプレートの詳細が表示されます。

ステップ 5 テンプレートの詳細を確認して、[次へ（Next）]をクリックします。

ステップ 6 **[設定（Configuration）]** ページで、展開設定の種類を選択し、**[次へ（Next）]** をクリックします。

- VMNLite（デフォルト）
- CMS 1000

オプションは、リソース要件の増加順にリストされています。

（注） VMNLite オプションを選択した場合は、手順を繰り返して同じホスト上で他のインスタンスを展開し、その度に同じオプションを選択する必要があります。VMNLite インスタンスと非 VMNLite インスタンスの共存はテストされておらず、サポートされていません。

ステップ 7 **[ストレージの選択（Select storage）]** ページで、デフォルトのディスク形式である **[シックプロビジョニング（Lazy Zeroed）（Thick Provision Lazy Zeroed）]** と **[データストアのデフォルト（Datastore Default）]** の VM ストレージポリシーが選択されていることを確認してから、**[次へ（Next）]** をクリックします。

ステップ 8 [ネットワークの選択（Select network）] ページで、VM に必要な接続を提供するエントリの一覧からネットワークを選択します。

- **[内部インターフェイスネットワーク（Internal Interface Network）]** については、ノードの内部 IP アドレスを選択します。
- **外部 InterfaceNetwork** の場合は、パブリックネットワークに接している外部 IP アドレスを選択します。デュアル NIC 展開を使用しない場合は、このオプションを無視します。

（注） 内部インターフェイス（トラフィックのデフォルトインターフェイス）は、CLI、SIP トランク、SIP トラフィック、およびノード管理に使用されます。外部（external）インターフェイスは、ノードからミーティングへのカスケードトラフィックとともに、HTTPS および WebSocket が Webex クラウドと通信するためのものです。

DMZ 展開の場合は、デュアル ネットワーク インターフェイス（NIC）を使用して Video Mesh ノードをセットアップできます。この導入によって、エンタープライズネットワークトラフィックを（インターボックス通信、ノードクラスタ間のカスケード、ノードの管理インターフェイスへのアクセスに使用される）外部のクラウド ネットワーク トラフィック（外部への接続に使用され、Webex にカスケード）から分離することができます。クラスタ内のすべてのノードがデュアル NIC モードになっている必要があります。シングル NIC とデュアル NIC の混在はサポートされていません。

（注） Video Mesh ノード ソフトウェアの既存のインストールでは、単一の NIC からデュアル NIC の構成にアップグレードすることはできません。この場合は、Video Mesh ノード の新規インストールを実行する必要があります。

ステップ 9 [テンプレートのカスタマイズ（Customize template）]ページで、次のネットワーク設定を行います。

- [**ホスト名（hostname**）]（オプション）：ノードの FQDN（ホスト名とドメイン）または 1 つの単語のホスト名を入力します。

  （注）
  - クラウドに問題なく登録できるように、Video Mesh ノード に設定する FQDN またはホスト名には小文字のみを使用してください。現時点では、大文字と小文字はサポートされていません。
  - FQDN またはホスト名を使用または設定する場合は、有効で解決可能なドメインを入力する必要があります。FQDN の長さは、64 文字以下にする必要があります。

- **IP アドレス**：ノードの内部インターフェイスの IP アドレスを入力します。
- **マスク**：ドット区切りの 10 進表記でサブネットを入力します。たとえば、*255.255.255.0* と入力します。

- **ゲートウェイ**：ゲートウェイの IP アドレスを入力します。ゲートウェイは、他のネットワークへの入口として機能するネットワーク ノードを表します。
- **][DNS サーバー（DNS Servers）**：ドメイン名を数値 IP アドレスに変換する処理を行う DNS サーバーのカンマ区切りのリストを入力します。（最大 4 つの DNS エントリが許可されます）。
- **[NTP サーバー（NTP Servers）]**：組織の NTP サーバまたは組織で使用可能な別の外部 NTP サーバーを入力します。また、カンマ区切りリストを使用して複数の NTP サーバーを入力することもできます。
- Video Mesh ノードは、内部 IP アドレスと解決可能な DNS 名を持っている必要があります。ノード IP アドレスは、Video Mesh ノード内部使用のために予約されている IP アドレスの範囲に属していてはなりません。デフォルトの予約済み IP アドレスの範囲は 172.17.42.0 ～ 172.17.42.63 で、後で **[診断（Diagnostic）]** メニューで設定できます。この IP アドレスの範囲は、Video Mesh ノード内、およびノードのさまざまなコンポーネント（SIP インターフェイスやメディアトランスコーディングなど）を保持するソフトウェアコンテナ間における通信のためのものです。
- すべてのノードを同じサブネットまたは VLAN に展開します。これにより、クラスタ内のすべてのノードは、ネットワーク内のクライアントのどこからでも到達可能になります。
- デュアル NIC DMZ を展開する場合は、後で、内部ネットワーク構成を保存してノードをリブートした後、ノードコンソールで外部 IP アドレスを設定することができます。

必要に応じて、ネットワーク設定の構成をスキップして、ノードにサインインした後の「コンソールでの Video Mesh ノード のネットワーク構成の設定 （10 ページ）」の手順に従うことができます。

ステップ 10 **[準備完了（Ready to Complete）]**ページで、入力したすべての設定がこの手順のガイドラインと一致していることを確認してから **[完了（Finish）]** をクリックします。

OVA の導入が完了すると、VM のリストに Video Mesh ノード が表示されます。

ステップ 11 Video Mesh ノード VM を右クリックし、**[電源（Power）] > [電源をオン（Power On）]** の順に選択します。

Video Mesh ノード ソフトウェアは、VM ホストでゲストとしてインストールされます。これで、コンソールにサインインして Video Mesh ノード を設定する準備が整いました。

トラブルシューティングのヒント

ノードコンテナが起動するまでに、数分の遅延が発生する可能性があります。最初の起動時にコンソールにブリッジファイアウォールのメッセージが表示されます。このとき、サインインはできません。

次のタスク

Video Mesh ノード コンソールへのログイン （9 ページ）

Video Mesh ノード コンソールへのログイン

コンソールに初回サインインします。Video Mesh ノード ソフトウェアには、デフォルトのパスワードが設定されています。ノードを設定する前に、この値を変更する必要があります。

手順

ステップ 1 VMware vSphere クライアントから、Video Mesh ノード VM に移動 して、**[コンソール（Console）]** を選択し ます。

Video Mesh ノード VM が起動し、ログインプロンプトが表示されます。ログインプロンプトが表示されない場合は、**Enter** キーを押します。システムの初期化が行われていることを示す簡単なメッセージが表示される可能性があります。

ステップ 2 次のデフォルトのユーザー名とパスワードを使用して、ログインします。

a) ログイン：**admin**

b) パスワード：**cisco**

Video Mesh ノード への初回ログインであるため、管理者のパスフレーズ（パスワード）を変更する必要があります。

ステップ 3 （現在の）パスワードとして、デフォルトのパスワード（上記）を入力し、**Enter** キーを押します。

ステップ 4 [新しいパスワード（New password）]に新しいパスフレーズを入力し、**Enter** キーを押します。

ステップ 5 新しいパスワードを再入力するように求められたら、新しいパスフレーズを再入力し、**Enter** キーを押します。

「パスワードを正常に変更できました」というメッセージが表示され、最初の Video Mesh ノード 画面に、不正アクセスが禁止されたことを通知するメッセージが表示されます。

ステップ 6 **Enter** キーを押してメインメニューをロードします。

次のタスク

コンソールでの Video Mesh ノード のネットワーク構成の設定 （10 ページ）

コンソールでの Video Mesh ノードのネットワーク構成の設定

仮想マシン上のノードのセットアップ時に設定しなかった場合に、Video Mesh ノードのネットワーク設定を構成するには、この手順を使用します。静的 IP アドレスを設定し、FQDN/ホスト名と NTP サーバーを変更します。DHCP は現在サポートされていません。

OVA の展開時にネットワーク設定を構成しなかった場合、これらの手順は必須です。

（注） 内部インターフェイス（トラフィックのデフォルトインターフェイス）は、CLI、SIP トランク、SIP トラフィック、およびノード管理に使用されます。外の（外部）インターフェイスは、ノードから Webex へのカスケードトラフィックとともに、HTTPS および WebSocket が Webex クラウドと通信するためのものです。

手順

ステップ 1 VMware vSphere クライアントを通じてノードコンソールのインターフェイスを開き、管理者のログイン情報を使用してサインインします。

初めてネットワーク設定をセットアップした後、Video Meshが到達可能である場合は、セキュアシェル（SSH）を通じてノードインターフェイスにアクセスできます。

ステップ 2 Video Mesh ノードコンソールのメインメニューで、**[2 構成の編集（2 Edit Configuration）]** のオプションを選択し、**[選択（Select）]** をクリックします。

ステップ 3 Video Mesh ノードでのコールの終了を求めるプロンプトを読み、**[はい（Yes）]** をクリックします。

ステップ 4 **[静的（Static）]** をクリックして、内部インターフェイスの **[IP アドレス（IP address）]**、ネットワークの、**[マスク（Mask）]**、**[ゲートウェイ（Gateway）]**、**[DNS]** の各値を入力します。

- Video Mesh ノードは、内部 IP アドレスと解決可能な DNS 名を持っている必要があります。ノード IP アドレスは、Video Mesh ノード内部使用のために予約されている IP アドレスの範囲に属していてはなりません。デフォルトの予約済み IP アドレスの範囲は 172.17.42.0 ～ 172.17.42.63 で、**[診断（Diagnostic）]** メニューで設定できます。この IP アドレスの範囲は、Video Mesh ノード内、およびノードのさまざまなコンポーネント（SIP インターフェイスやメディアトランスコーディングなど）を保持するソフトウェアコンテナ間における通信のためのものです。
- すべてのノードを同じサブネットまたは VLAN に展開します。これにより、クラスタ内のすべてのノードは、ネットワーク内のクライアントのどこからでも到達可能になります。

- デュアル NIC DMZ を導入する場合は、内部ネットワーク構成を保存してノードをリブートした後、次の手順で外部 IP アドレスを設定することができます。

ステップ 5 組織の NTP サーバーまたは組織で使用可能な別の外部 NTP サーバーを入力します。

NTP サーバーを設定し、ネットワーク設定を保存した後は、「コンソールからの Video Mesh ノードの正常性チェック」の手順に従って、指定された NTP サーバーを介して時刻が正しく同期されていることを確認できます。

（注） 複数の NTP サーバーを設定する場合、フェールオーバーのポーリング間隔は 40 秒です。

ステップ 6 （オプション）必要に応じて、ホスト名またはドメインを変更します。

（注）
- クラウドに問題なく登録できるように、Video Mesh ノード に設定するホスト名は小文字のみを使用します。現時点では、大文字と小文字はサポートされていません。
- FQDN またはホスト名を使用または設定する場合は、有効で解決可能なドメインを入力する必要があります。FQDN の長さは、64 文字以下にする必要があります。

ステップ 7 **[保存（Save）]** をクリックし、**[変更を保存して再起動（Save Changes & Reboot）]** の順に選択します。

ドメインを指定した場合は、保存中に DNS の検証が行われます。指定された DNS サーバーアドレスを使用して FQDN（ホスト名とドメイン）を解決できない場合、警告が表示されます。警告を無視して保存を選択できますが、ノードに設定されている DNS で FQDN を解決できるまで、コールは機能しません。Video Mesh ノード リブート後、ネットワーク構成の変更が有効になります。

次のタスク

ネットワーク設定（IP アドレス、DNS、NTP など）でソフトウェアイメージをインストール、構成し、エンタープライズネットワークでアクセス可能にすると、その次の手順に移行して、セキュリティで保護されているクラウドに登録することができます。Video Mesh ノード に設定されている IP アドレスに は、エンタープライズネットワークからのみアクセスできます。セキュリティの観点からは、ノードは、カスタマーの管理者だけがノードインターフェイスにアクセスして構成を実行できるようになっています。

Video Mesh ノード の外部ネットワークインターフェイスの設定 （12 ページ）

Video Mesh ノードの外部ネットワークインターフェイスの設定

ノードがオンラインに戻り、内部ネットワーク構成を確認した後、ネットワークの DMZ 内で Video Mesh ノードを展開している場合は、外部ネットワーク インターフェイスを設定して、企業（内部）トラフィックを外部トラフィックから分離することができます。

手順

ステップ 1 Video Mesh ノード コンソールのメインメニュー で、**[5 外部 IP 構成（5 External IP Configuration）]** のオプションを選択し、**[選択（Select）]** をクリックします。

ステップ 2 **[1 有効化/無効化（1 Enable/Disable）]**、**[選択（Select）]** の順に選択したら、**[はい（Yes）]** を選択して、ノードで外部 IP アドレスオプションを有効化します。

ステップ 3 初期ネットワーク構成で行ったように、**[IP アドレス（IP Address）]**（外部）、**[マスク（Mask）]**、および **[ゲートウェイ（Gateway）]** の値を入力します。

（注） **[インターフェイス（Interface）]** フィールドには、ノードの外部インターフェイスの名前が表示されます。

ステップ 4 **[保存して再起動（Save and restart）]** をクリックします。

デュアル IP アドレスを有効にするためノードを再度リブートすると、基本的な静的ルーティングルールが自動的に設定されます。これらのルールは、プライベートクラス IP アドレス間のトラフィックが、内部インターフェイスを使用することを決定します。パブリッククラスの IP アドレス間のトラフィックには、外部インターフェイスが使用されます。後で、独自のルーティングルールを作成することができます。たとえば、内部インターフェイスからの上書きを設定し、外部ドメインへのアクセスを許可する必要がある場合などです。

（注） 特定の状況においては、既存の SSH 接続が終了する場合があります。パブリック範囲の IP アドレスを使用する組織の場合、Video Mesh ノードのパブリック IP アドレスへの SSH 接続を再確立する必要があります。

ステップ 5 内部 IP アドレスと外部 IP アドレス設定を確認するには、コンソールのメインメニューから **[4 診断（4 Diagnostics）]** に移動し て、**[Ping]** を選択し ます。

ステップ 6 **[Ping]** フィールドに、外部の宛先または内部 IP アドレスなどテストする宛先アドレスを入力し、**[OK]** をクリックします。

- cisco.com などの外部宛先をテストします。成功した場合は、外部インターフェイスから宛先にアクセスしたことが結果に示されます。
- 内部 IP アドレスをテストします。成功した場合は、内部インターフェイスからアドレスにアクセスされたことが結果に示されます。

次のタスク

Webex クラウドへの Video Mesh ノードの登録 （33 ページ）

Video Mesh ノード API

Video Mesh ノード API を使用すると、組織管理者は、Video Mesh ノードに関連するパスワード、内部および外部ネットワーク設定、メンテナンスモード、およびサーバー証明書を管理できます。これらの API は、Postman などの API ツールを介して呼び出すことも、独自のスクリプトを作成して呼び出すこともできます。ユーザーは、以下に示す情報に従って、適切なエンドポイント（ノード IP または FQDN のいずれかを使用できます）、メソッド、本文、ヘッダー、承認などを使用して API を呼び出し、希望するアクションを実行し、適切なレスポンスを取得する必要があります。

VMN 管理 API

Video Mesh 管理 API を使用すると、組織管理者はVideo Mesh ノードのメンテナンスモードと管理者アカウントパスワードを管理できます。

メンテナンスモードのステータスを受け取る

現在のメンテナンスモードのステータスを取得します（予期されるステータス：オン、オフ、保留中、またはリクエスト済み）。

[GET] https://<node_ip> /api/v1/external/maintenanceMode

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Success"
    },
    "result": {
        "isRegistered": true,
        "maintenanceMode": "pending/requested/on/off",
        "maintenanceModeLastUpdated": 1691135731847
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 401,
        "message": "login failed: incorrect password or username"
    }
}
```

サンプルレスポンス 3：

```
{
    "status": {
        "code": 429,
        "message": "Too Many Requests"
    }
}
```

メンテナンスモードを有効または無効にする

Video Mesh ノードをメンテナンスモードにすると、コールサービスのグレースフルシャットダウンを実行します（新しいコールの受け入れを停止し、既存のコールが完了するまで最大2時間待機します）。

[PUT] https://<node_ip> /api/v1/external/maintenanceMode

（注） アクティブなコールがない場合にのみ、この API を呼び出します。

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

本文：

```
{
      "maintenanceMode": "on"
}
```

- maintenanceMode：設定するメンテナンスモードのステータス（「on」または「off」）。

リクエストヘッダー：

「コンテンツ タイプ」：「application/json」

サンプルレスポンス：

サンプルレスポンス 1：

```
{
        "status": {
            "code": 200,
           "message": "Your request to enable/disable maintenance mode was successful."

    }
}
```

サンプルレスポンス 2：

```
{
      "status": {
          "code": 409,
          "message": "Maintenance Mode is already on/off"
    }
}
```

サンプルレスポンス 3：

```
{
      "status": {
          "code": 400,
          "message": "Bad Request - wrong input"
```

```
    }
}
```

admin パスワードを変更する

管理者ユーザーのパスワードを変更します。

[PUT] https://<node_ip> /api/v1/external/password

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

本文：

```
{
  "newPassword": "new"
}
```

- newPassword：Video Mesh ノードの「admin」アカウントに設定する新しいパスワード。

リクエストヘッダー：

「コンテンツ タイプ」：「application/json」

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully set the new passphrase for user admin."
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 400,
        "message": "Enter a new passphrase that wasn't used for one of the previous 3
passphrases."
    }
}
```

VMN ネットワーク API

Video Mesh ネットワーク API を使用すると、組織管理者は内部および外部のネットワーク設定を管理できます。

外部ネットワーク設定を取得する

外部ネットワークが有効か無効かを検出します。外部ネットワークが有効になっている場合は、外部 IP アドレス、外部サブネットマスク、および外部ゲートウェイも取得します。

[GET] https://<node_ip> /api/v1/external/externalNetwork

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully fetched external network configuration."
    },
    "result": {
        "ip": "1.1.1.1",
        "mask": "2.2.2.2",
        "gateway": "3.3.3.3"
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 200,
        "message": "External network not enabled."
    }
}
```

サンプルレスポンス 3：

```
{
    "status": {
        "code": 500,
        "message": "Failed to get external network configuration."
    }
}
```

外部ネットワーク設定を編集する

外部ネットワークの設定を変更します。このAPIを使用して、外部IPアドレス、外部サブネットマスク、および外部ゲートウェイを使用して外部ネットワークインターフェイスを設定または編集するとともに、外部ネットワークを有効にすることができます。また、外部ネットワークを無効にするためにも使用できます。外部ネットワーク設定を変更すると、ノードが再起動して変更が適用されます。

[PUT] https://<node_ip> /api/v1/external/externalNetwork

（注） これは、デフォルトの管理者パスワードが変更された、新しく展開された Video Mesh ノードに対してのみ設定できます。ノードを組織に登録した後は、この API を使用しないでください。

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

本文：

外部ネットワークの有効化：

```
{
  "externalNetworkEnabled": true,
  "externalIp": "1.1.1.1",
  "externalMask": "2.2.2.2",
```

```
  "externalGateway": "3.3.3.3"
}
```

外部ネットワークの無効化：

```
{
  "externalNetworkEnabled": false
}
```

- externalNetworkEnabled：外部ネットワークを有効または無効にするブール値（true または false）
- externalIp：追加する外部 IP
- externalMask：外部ネットワークのネットマスク
- externalGateway：外部ネットワークのゲートウェイ

リクエストヘッダー：

「コンテンツ タイプ」：「application/json」

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully saved the external network configuration. This node
will reboot soon to apply the changes. Please wait for a minute and relogin to the node
 to verify that all changes were applied."
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 200,
        "message": "Successfully disabled the external network. This node will reboot
soon to apply the changes. Please wait for a minute and relogin to the node to verify
that all changes were applied."
    }
}
```

サンプルレスポンス 3：

```
{
    "status": {
        "code": 400,
        "message": "One or more errors in the input: Value should be boolean for
'externalNetworkEnabled'"
    }
}
```

サンプルレスポンス 4：

```
{
    "status": {
        "code": 400,
       "message": "External network configuration has not changed; skipping save of the
 external network configuration."
```

```
    }
}
```

内部ネットワークの詳細を取得する

ネットワークモード、IPアドレス、サブネットマスク、ゲートウェイ、DNSキャッシングの詳細、DNSサーバー、NTPサーバー、内部インターフェイスMTU、ホスト名、ドメインを含む内部ネットワーク設定の詳細を取得します。

[GET] https://<node_ip> /api/v1/external/internalNetwork

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully fetched internal network details"
    },
    "result": {
        "dhcp": false,
        "ip": "1.1.1.1",
        "mask": "2.2.2.2",
        "gateway": "3.3.3.3",
        "dnsCaching": false,
        "dnsServers": [
            "4.4.4.4",
            "5.5.5.5"
        ],
        "mtu": 1500,
        "ntpServers": [
            "6.6.6.6"
        ],
        "hostName": "test-vmn",
        "domain": ""
    }
}
```

サンプルレスポンス 2：

```
{
      "status": {
          "code": 500,
          "message": "Failed to get Network details."
    }
}
```

サンプルレスポンス 3：

```
{
      "status": {
          "code": 500,
          "message": "Failed to get host details."
    }
}
```

DNS サーバーを編集する

新しい DNS サーバーで DNS サーバーを更新します。

[PUT] https://<node_ip> /api/v1/external/internalNetwork/dns

（注） この変更を行う前に、ノードをメンテナンスモードにします。ノードをメンテナンスモードに移行する方法の詳細については、「メンテナンスモードを有効または無効にする （14 ページ）」を参照してください。

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

本文：

```
{
    "dnsServers": "1.1.1.1 2.2.2.2"
}
```

- dnsServers：更新する DNS サーバー。スペースで区切られた複数の DNS サーバーを使用できます。

リクエストヘッダー：

「コンテンツ タイプ」：「application/json」

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully saved DNS servers"
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 409,
        "message": "Requested DNS server(s) already exist."
    }
}
```

サンプルレスポンス 3：

```
{
    "status": {
        "code": 424,
        "message": "Maintenance Mode is not enabled. Kindly enable Maintenance Mode and
 try again for this node."
    }
}
```

NTP サーバーを編集する

NTP サーバーを新しいサーバーで更新します。

[PUT] https://<node_ip> /api/v1/external/internalNetwork/ntp

（注） この変更を行う前に、ノードをメンテナンスモードにします。ノードをメンテナンスモードに移行する方法の詳細については、「メンテナンスモードを有効または無効にする （14 ページ）」を参照してください。

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

本文：

```
{
    "ntpServers": "1.1.1.1 2.2.2.2"
}
```

- ntpServers：更新する NTP サーバー。スペースで区切られた複数の NTP サーバーを使用できます。

リクエストヘッダー：

「コンテンツ タイプ」：「application/json」

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully saved the NTP servers."
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 409,
        "message": "Requested NTP server(s) already exist."
    }
}
```

サンプルレスポンス 3：

```
{
    "status": {
        "code": 424,
        "message": "Maintenance Mode is not enabled. Kindly enable Maintenance Mode and
 try again for this node."
    }
}
```

ホスト名とドメインを編集する

Video Mesh ノードのホスト名とドメインを更新します。

[PUT] https://<node_ip> /api/v1/external/internalNetwork/host

（注） この変更を行う前に、ノードをメンテナンスモードにします。ノードが再起動し、変更が適用されます。ノードをメンテナンスモードに移行する方法の詳細については、「メンテナンスモードを有効または無効にする （14 ページ）」を参照してください。

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

本文：

```
{
    "hostName": "test-vmn",
    "domain": "abc.com"
}
```

- hostName：ノードの新しいホスト名。
- domain：ノードのホスト名の新しいドメイン（オプション）。

リクエストヘッダー：

「コンテンツ タイプ」：「application/json」

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
       "message": "Successfully saved the host FQDN. This node will reboot soon to apply
 the changes. Please wait for a minute and relogin to the node to verify that all changes
 were applied."
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 400,
        "message": "Unable to resolve FQDN"
    }
}
```

サンプルレスポンス 3：

```
{
    "status": {
        "code": 409,
        "message": "Entered hostname and domain already set to same."
    }
}
```

DNS キャッシングを有効または無効にする

DNS キャッシングの有効または無効にします。DNS チェックの解決に 750 ミリ秒以上かかることが多い場合、またはシスコサポートで推奨されている場合は、キャッシングを有効にすることを検討してください。

[PUT] https://<node_ip> /api/v1/external/internalNetwork/dnsCaching

（注） この変更を行う前に、ノードをメンテナンスモードにします。ノードが再起動し、変更が適用されます。ノードをメンテナンスモードに移行する方法の詳細については、「メンテナンスモードを有効または無効にする （14 ページ）」を参照してください。

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

本文：

```
{
    "dnsCaching": true
}
```

- dnsCaching：DNS キャッシング設定。ブール値（true または false）を受け入れます。

リクエストヘッダー：

「コンテンツ タイプ」：「application/json」

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully saved DNS settings changes. This node will reboot soon
 to apply the changes. Please wait for a minute and relogin to the node to verify that
all changes were applied."
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 400,
        "message": "One or more errors in the input: 'dnsCaching' field value should be
 a boolean"
    }
}
```

サンプルレスポンス 3：

```
{
    "status": {
        "code": 409,
        "message": "dnsCaching is already set to false"
    }
}
```

インターフェイス MTU を編集する

ノードのネットワーク インターフェイスの最大伝送ユニット（MTU）をデフォルト値の 1500 から変更します。1280 ～ 9000 の値を使用できます。

[PUT] https://<node_ip> /api/v1/external/internalNetwork/mtu

（注） この変更を行う前に、ノードをメンテナンスモードにします。ノードが再起動し、変更が適用されます。ノードをメンテナンスモードに移行する方法の詳細については、「メンテナンスモードを有効または無効にする （14 ページ）」を参照してください。

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

本文：

```
{
    "internalInterfaceMtu": 1500
}
```

- internalInterfaceMtu：ノードのネットワーク インターフェイスの最大伝送ユニット。値は 1280 ～ 9000 である必要があります。

リクエストヘッダー：

「コンテンツ タイプ」：「application/json」

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully saved the internal interface MTU settings. This node
will reboot soon to apply the changes. Please wait for a minute and relogin to the node
 to verify that all changes were applied."
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 400,
        "message": "One or more errors in the input: 'internalInterfaceMtu' field value
 should be a number"
    }
}
```

サンプルレスポンス 3：

```
{
    "status": {
        "code": 400,
        "message": "Please enter a number between 1280 and 9000."
    }
}
```

VMN サーバー証明書 API

Video Mesh サーバー証明書 API を使用すると、組織管理者は Video Mesh ノードに関連する証明書を作成、更新、ダウンロード、および削除できます。詳細については、「Unified CM と Video Mesh ノード間での証明書チェーンの交換 （58 ページ）」を参照してください。

CSR 証明書を作成する

指定された詳細に基づいて、CSR（証明書署名要求）証明書と秘密キーを生成します。

[POST] https://<node_ip> /api/v1/externalCertManager/generateCsr

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

本文：

```
{
    "csrInfo":
    {
         "commonName": "1.2.3.4",
         "emailAddress": "abc@xyz.com",
         "altNames": "1.1.1.1 2.2.2.2",
         "organization": "VMN",
         "organizationUnit": "IT",
         "locality": "BLR",
         "state": "KA",
         "country": "IN",
         "passphrase": "",
         "keyBitSize": 2048
    }
}
```

- commonName：共通名として指定された Video Mesh ノードの IP/FQDN。（必須）
- emailAddress：ユーザーの電子メールアドレス。（オプション）。
- altNames：サブジェクト代替名（オプション）。複数のスペースで区切られた FQDN を使用できます。指定する場合は、共通名を含める必要があります。altNames が指定されていない場合は、altNames の値として commonName を使用します。
- organization：組織/会社の名前。（オプション）。
- organizationUnit：組織単位、部署、グループ名など（任意）
- locality：市区町村。（オプション）。
- state：州/都道府県。（オプション）。
- country：国/地域。2 文字の略語。2 文字を超えて入力しないでください。（オプション）。
- passphrase：秘密キーのパスフレーズ。（オプション）。
- keyBitSize：秘密キーのビットサイズ。許容値は、デフォルトの 2048 または 4096 です。（オプション）。

リクエストヘッダー：

「コンテンツ タイプ」：「application/json」

サンプルレスポンス：

サンプルレスポンス 1：


```
{
    "status": {
        "code": 200,
        "message": "Successfully generated CSR"
    },
    "result": {
        "caCert": {},
        "caKey": {
            "fileName": "VideoMeshGeneratedPrivate.key",
            "localFileName": "CaPrivateKey.key",
            "fileLastModified": "Fri Jul 21 2023 08:12:25 GMT+0000 (Coordinated
Universal Time)",
            "uploadDate": 1689927145422,
            "size": 1678,
            "type": "application/pkcs8",
            "modulus": "S4MP1EM0DULU2"
        },
        "certInstallRequestPending": false,
        "certInstallStarted": null,
        "certInstallCompleted": null,
        "isRegistered": true,
        "caCertsInstalled": false,
        "csr": {
            "keyBitsize": 2048,
            "commonName": "1.2.3.4",
            "organization": "VMN",
            "organizationUnit": "IT",
            "locality": "BLR",
            "state": "KA",
            "country": "IN",
            "emailAddress": "abc@xyz.com",
            "altNames": [
                "1.1.1.1",
                "2.2.2.2"
            ],
            "csrContent": "-----BEGIN CERTIFICATE
REQUEST-----\nS4MP1E_C3RT_C0NT3NT\n-----END CERTIFICATE REQUEST-----"
        },
        "encryptedPassphrase": null
    }
}
```


サンプルレスポンス 2：


```
{
    "status": {
        "code": 400,
        "message": "Private key already exists. Delete it before generating new CSR."

    }
}
```


サンプルレスポンス 3：

```
{
    "status": {
        "code": 400,
        "message": "CSR certificate already exists. Delete it before generating new
CSR."
    }
}
```

サンプルレスポンス 4：

```
{
    "status": {
        "code": 400,
        "message": "CSR certificate and private key already exist. Delete them before
 generating new CSR."
    }
}
```

サンプルレスポンス 5：

```
{
    "status": {
        "code": 400,
        "message": "There were one or more errors while generating the CSR: The
\"Country\" field must contain exactly two A-Z characters."
    }
}
```

CSR 証明書をダウンロードする

生成された CSR 証明書をダウンロードします。

[GET] https://<node_ip> /api/v1/externalCertManager/csr

[送信とダウンロード（Send and Download）] オプションを使用してファイルをダウンロードすることもできます。

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

サンプルレスポンス：

サンプルレスポンス 1：

```
-----BEGIN CERTIFICATE REQUEST-----
S4MP1E_C3RT_C0NT3NT
-----END CERTIFICATE REQUEST-----
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 404,
        "message": "Could not download, CSR certificate does not exist."
    }
}
```

秘密キーをダウンロードする

CSR 証明書とともに生成された秘密キーをダウンロードします。

[GET] https://<node_ip> /api/v1/externalCertManager/key

[送信とダウンロード（Send and Download）] オプションを使用してファイルをダウンロードすることもできます。

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

サンプルレスポンス：

サンプルレスポンス 1：

```
-----BEGIN RSA PRIVATE KEY-----
S4MP1E_PR1V4T3_K3Y
-----END RSA PRIVATE KEY-----
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 404,
        "message": "Could not download, private key does not exist."
    }
}
```

CSR 証明書を削除する

既存の CSR 証明書を削除します。

[DELETE] https://<node_ip> /api/v1/externalCertManager/csr

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully deleted the CSR certificate"
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 404,
        "message": "CSR certificate does not exist."
    }
}
```

秘密キーを削除する

既存の秘密キーを削除します。

[DELETE] https://<node_ip> /api/v1/externalCertManager/key

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully deleted the private key"
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 404,
        "message": "Private key does not exist."
    }
}
```

CA 署名付き証明書と秘密キーをインストールする

提供された CA 署名付き証明書と秘密キーを Video Mesh ノードにアップロードし、ノードに証明書をインストールします。

[POST] https://<node_ip> /api/v1/externalCertManager/uploadInstallCaCert

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

本文：

「form-data」を使用して、次のファイルをアップロードします。

- 「crtFile」というキーを持つ CA 署名付き証明書（.crt）ファイル。
- 「keyFile」というキーを持つ秘密キー（.key）ファイル。

リクエストヘッダー：

Content-Type：「multipart/form-data」

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully installed certificate and key. It might take a few
seconds to reflect on the node."
```

```
},
"result": {
    "caCert": {
        "fileName": "videoMeshCsr.crt",
        "localFileName": "CaCert.crt",
        "fileLastModified": 1689931788598,
        "uploadDate": 1689931788605,
        "size": 1549,
        "type": "application/x-x509-ca-cert",
        "certStats": {
            "version": 0,
            "subject": {
                "countryName": "IN",
                "stateOrProvinceName": "KA",
                "localityName": "BLR",
                "organizationName": "VMN",
                "organizationalUnitName": "IT",
                "emailAddress": "abc@xyz.com",
                "commonName": "1.2.3.4"
            },
            "issuer": {
                "countryName": "AU",
                "stateOrProvinceName": "Some-State",
                "organizationName": "ABC"
            },
            "serial": "3X4MPL3",
            "notBefore": "2023-07-21T09:28:19.000Z",
            "notAfter": "2024-12-02T09:28:19.000Z",
            "signatureAlgorithm": "sha256WithRsaEncryption",
            "fingerPrint": "11:22:33:44:AA:BB:CC:DD",
            "publicKey": {
                "algorithm": "rsaEncryption",
                "e": 65537,
                "n": "3X4MPL3",
                "bitSize": 2048
            },
            "altNames": [],
            "extensions": {}
        }
    },
    "caKey": {
        "fileName": "VideoMeshGeneratedPrivate.key",
        "localFileName": "CaPrivateKey.key",
        "fileLastModified": 1689931788629,
        "uploadDate": 1689931788642,
        "size": 1678,
        "type": "application/pkcs8",
        "modulus": "S4MP1EM0DULU2"
    },
    "certInstallRequestPending": true,
    "certInstallStarted": null,
    "certInstallCompleted": null,
    "isRegistered": true,
    "caCertsInstalled": false,
    "csr": {
        "keyBitsize": 2048,
        "commonName": "1.2.3.4",
        "organization": "VMN",
        "organizationUnit": "IT",
        "locality": "BLR",
        "state": "KA",
        "country": "IN",
        "emailAddress": "abc@xyz.com",
```

```
            "altNames": [
                "1.1.1.1",
                "2.2.2.2"
            ],
            "csrContent": "-----BEGIN CERTIFICATE
REQUEST-----\nS4MP1E_C3RT_C0NT3NT\n-----END CERTIFICATE REQUEST-----"
        },
        "encryptedPassphrase": null
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 400,
        "message": "Could not parse the certificate file. Make sure it is a properly
 formatted certificate and try again."
    }
}
```

サンプルレスポンス 3：

```
{
    "status": {
        "code": 400,
        "message": "Private Key does not match Certificate (different modulus)"
    }
}
```

サンプルレスポンス 4：

```
{
    "status": {
        "code": 202,
        "message": "Certificate and private key PENDING installation. It might take
a few seconds to reflect on the node. If the node is in maintenance mode, it will get
 installed once it is disabled."
    }
}
```

CA 署名付き証明書をダウンロードする

ノードにインストールされている CA 署名付き証明書をダウンロードします。

[GET] https://<node_ip> /api/v1/externalCertManager/caCert

[送信とダウンロード（Send and Download）] オプションを使用してファイルをダウンロードすることもできます。

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

サンプルレスポンス：

サンプルレスポンス 1：

```
-----BEGIN CERTIFICATE-----
S4MP1E_C3RT_C0NT3NT
-----END CERTIFICATE-----
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 404,
        "message": "Could not download, CA certificate does not exist."
    }
}
```

CA 署名付き証明書を削除する

ノードにインストールされている CA 署名付き証明書を削除します。

[DELETE] https://<node_ip> /api/v1/externalCertManager/caCert

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully deleted the CA certificate."
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 404,
        "message": "CA certificate does not exist."
    }
}
```

共通 API レスポンス

上記の API のいずれかを使用しているときに発生する可能性のあるレスポンスの例を以下に示します。

レスポンス例 1：基本認証で提供されたログイン情報が正しくありません。

```
{
    "status": {
        "code": 401,
        "message": "login failed: incorrect password or username"
    }
}
```

レスポンス例 2：VMN は、これらの API をサポートする必要なバージョンにアップグレードされていません。

```
{
    "status": {
        "code": 421,
        "message": "Misdirected Request 1:[undefined]"
    }
}
```

レスポンス例 3：ヘッダーに誤ったリファラーが入力されました（ヘッダーが予期されなかった場合）。

```
{
    "status": {
        "code": 421,
        "message": "Misdirected Request 2:[https://x.x.x.x/setup]"
    }
}
```

レスポンス例 4：レート制限を超えています。しばらくしてから再試行してください。

```
{
    "status": {
        "code": 429,
        "message": "Too Many Requests"
    }
}
```

内部ルーティングルールと外部ルーティングルールを追加する

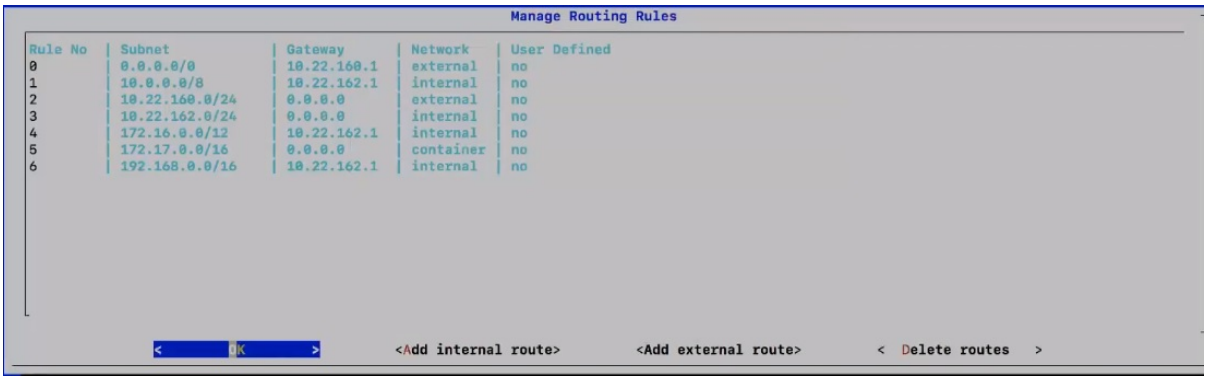
デュアルネットワークインターフェイス（NIC）の展開では、外部インターフェイスと内部インターフェイスのユーザー定義ルートルールを追加することによって、値リストコレクション作成者のルーティングを微調整することができます。デフォルトルートはノードに追加されますが、たとえば、外部サブネットまたは内部インターフェイスを介してアクセスする必要があるホストアドレス、あるいは外部インターフェイスからアクセスする必要がある内部サブネットまたはホストアドレスなど、例外を作成することができます。必要に応じて、次の手順を実行します。

手順

ステップ 1 値リストコレクション作成者インターフェイスから **[5 外部 IP 構成（5 External IP Configuration）]** を選択し、**[選択（Select）]** をクリックします。

ステップ 2 **[3 ルーティングルールの管理（3 Manage Routing Rules）]** を選択し、**[選択（Select）]** をクリックします。

このページを初めて開いたときは、デフォルトのシステムルーティングルールがリストに表示されます。デフォルトでは、すべての内部トラフィックは内部インターフェイスを通過し、外部トラフィックは外部インターフェイスを通過します。



これらのルールに手動オーバーライドを追加するには、次の手順を実行します。

ステップ 3 必要に応じて次の手順を実行します。

- **[外部ルートの追加（Add external route）]** をクリックして、外部ルートに使用する内部サブネットまたはホスト IP アドレスを入力します。
- **[内部ルートの追加（Add internal route）]** をクリックして、内部ルートに使用する内部サブネットまたはホスト IP アドレスを入力します。

各ルールを追加すると、そのルールはルーティングルールの一覧に表示され、ユーザー定義ルールとして分類されます。

（注） デフォルトルートを削除することはできませんが、設定した任意のユーザー定義オーバーライドを削除することはできます。

⚠

注意 カスタムルーティングルールは、他のルーティングと競合する可能性があります。たとえば、Video Mesh ノードインターフェイスへの SSH 接続をフリーズするルールを定義できます。このような場合は、次のいずれかを実行して、ルーティングルールを削除または変更します。

- Video Mesh ノードのパブリック IP アドレスへの SSH 接続を開きます。
- ESXi コンソールからの Video Mesh ノードへのアクセス

Webex クラウドへの Video Mesh ノードの登録

次の手順を使用して、Video Mesh ノードを Webex クラウドに登録し、追加の構成を完了します。ノードの登録に Control Hub を使用する場合は、ノードを割り当てるクラスタを作成します。クラスタには1つまたは複数のメディアノードがあり、それぞれ特定の地理的地域のユーザーが利用します。登録手順では、SIP コール設定の構成、アップグレードスケジュールの設定、および電子メール通知の登録も行います。

Before you begin

- ノードの登録を開始したら、60 分以内に登録を完了する必要があります。そうでないと、最初からやり直さなければなりません。
- ブラウザ内のポップアップブロックが無効になっていないか、または https://admin.webex.com の例外を許可しているかどうかを確認します。
- できるだけ問題が生じないように、クラスタのすべてのノードを同じデータセンターに展開します。ノードの動作とベストプラクティスについては、「Video Mesh のクラスタ」を参照してください。
- Video Mesh ノードをクラウドに登録するホストまたはマシンから、Webex クラウドと登録される Video Mesh IP アドレスに接続できる必要があります（デュアル NIC 環境内（特に Video Mesh ノードの内部 IP アドレスを含む））。

Procedure

ステップ 1 [Control Hub] にサインインします。

管理者のログイン情報を使用して Control Hub にサインインします。Control Hub 管理者機能は、Control Hub で管理者として定義されているユーザーのみが使用できます。詳細については、「顧客アカウントの役割」を参照してください。

ステップ 2 **[サービス（Services）]** > **[ハイブリッド（Hybrid）]** に移動し、次のいずれかを選択します。

- **セットアップ（Set up）**：これが登録する最初の Video Mesh ノード である場合は、このオプションを選択し、**[次へ（Next）]** をクリックします。

  Note 詳細については、「Video Mesh の前提条件の実行」を参照してください。

- **すべて表示（View all）**：すでに 1 つ以上の Video Mesh ノード を登録している場合は、このオプションを選択し、**[リソースの追加（Add Resource）]** をクリックします。

ステップ 3 Video Mesh ノード をインストールして設定していることを確認します。**[はい、登録する準備ができています（Yes, I'm ready to register...）]** をクリックし、**[次へ（Next）]** をクリックします。

ステップ 4 **[新規作成（Create a new）]** または **[クラスタの選択（select a cluster）]** で以下のいずれかを選択します。

- 新しいクラスタの場合は、Video Mesh ノードを割り当てるクラスタの名前を入力します。
- 既存のクラスタの場合は、フィールドをクリックして、新しいノードを追加する既存のクラスタを選択します。

Note クラスタには、クラスタのノードの地理的な配置場所に応じた名前を付けることを推奨します。たとえば、「San Francisco」と入力します。

ステップ 5 **[FQDN] または [IP アドレス（IP addres）]** で、Video Mesh ノード の完全修飾ドメイン名（FQDN）または内部 IP アドレスを入力して、**[次へ（Next）]** をクリックします。

- FQDN を使用する場合は、DNS によって解決できるドメインを入力します。
- IP アドレスを使用する場合は、コンソールからノードを設定するために使用したのと同じ内部 IP アドレスを入力します。

FQDN は、IP アドレスに対して直接解決する必要があります。FQDN の検証を実行して、入力ミスや一致しない構成を除外します。

Note デュアル ネットワーク インターフェイスでは、外部 IP アドレスの FQDN の指定がサポートされていません。FQDN は、内部 IP アドレスが入力されている画面でのみ追加できます。これは、同じ画面上で指定された DNS サーバーを使用するために、FQDN が解決する必要があることを示しています。

ステップ 6 **[アップグレードスケジュール（Upgrade Schedule）]** で、時間、頻度、およびタイムゾーンを選択します。

デフォルトは毎日のアップグレードスケジュールです。毎週の特定の日のスケジュールに変更できます。アップグレードが利用可能な場合は、選択した時間に Video Mesh ノード ソフトウェアが自動的にアップグレードされます。

Note アップグレードが利用可能な場合は、**[今すぐアップグレード（Upgrade Now）]** を使用して次のメンテナンスウィンドウの前にアップグレードを開始するか、**[延期（Postpone）]** して以降のウィンドウまで延期できます。

ステップ 7 **[電子メール通知（Email Notifications）]** で、管理者の電子メールアドレスを追加して、サービスアラームやソフトウェアのアップグレードに関する通知を登録します。

管理者の電子メールアドレスは自動的に追加されます。必要に応じて削除できます。

ステップ 8 **ビデオ品質**設定のオン/オフを切り替えて、1080p 30fps のビデオを有効にします。

この設定により、企業のネットワーク内に存在し、高画質の対応可能なデバイスを使用している場合、Video Mesh ノード でホストされたミーティングに参加している SIP 参加者は 1080p 30fps のビデオを使用できます。この設定は、ノードのすべてのクラスタに適用されます。

Note
- この設定がオフの場合、デフォルトは 720p です。
- Webex アプリ がサポートするビデオ解像度については、「通話とミーティングのビデオ仕様」参照してください。

ステップ 9 *[登録完了（Complete Registration）]* に表示される情報を読み、**[ノードに移動（Go to node）]** をクリックしてノードを Webex クラウドに登録します。

ノードを確認するために、ブラウザで新しいタブが開きます。この手順は、ノードの IP アドレス を使用して Video Mesh ノード をセーフリストに追加します。登録プロセス中に、Control Hub は、Video Mesh ノード にリダイレクトします。IP アドレスをセーフリストに追加する必要があります。そうでない場合、登録は失敗します。登録プロセスは、ノードがインストールされているエンタープライズ ネットワークから完了する必要があります。

ステップ 10 **[Webex Video Mesh ノードへのアクセスを許可（Allow Access to the Webex Video Mesh Node）]** をオンにして、**[続行（Continue）]** をクリックします。

ステップ 11 **[許可（Allowed）]** をクリックします。

アカウントが検証されると、Video Mesh ノードが登録され、**「登録が完了しました」**というメッセージが表示されます。これで、Video Mesh ノードが Webex に登録されました。

Video Mesh ノードは、組織の権限に基づいてマシンのログイン情報を取得します。生成されたマシンのログイン情報は定期的に期限切れになり、更新されます。

ステップ 12 ポータルリンクをクリックするか、タブを閉じて [Video Mesh] ページに戻ります。

[Video Mesh] ページに、登録した Video Mesh ノードが含まれる新しいクラスタが表示されます。

- クラスタに移動すると、新しい Video Mesh ノードが表示されます。これは最初に **[登録中（Registering）]** のステータスを示します。Webex 組織での使用準備が完了すると、ノードが **[実行中（Running）]** に変わります。
- このソフトウェアはクラウドインフラストラクチャからのサービスを含むコンテナであるため、クラウドから更新を取得してクラウドサービスと同期されるようになります。必要な更新は、ノードをクラウドに登録した後すぐにインストールされる場合があります。また、自動アップグレードスケジュールを変更することもできます。詳細については、「ハイブリッド サービス リソースの自動アップグレード」を参照してください。
- 登録したノードにデモイメージをインストールした場合は、“デモモード”の黄色ステータスのアラームが表示されます。このアラームは正常ですが、デモイメージの 90 日の猶予期間が満了する前に、完全なソフトウェアイメージをインストールすることを推奨します。

この時点で、Video Mesh ノードは、認証用に発行されたトークンを使用して、セキュリティで保護されたチャネルを介して Cisco Cloud サービスと通信する準備ができています。Video Mesh ノードは、Docker Hub（docker.com、docker.io）とも通信します。Docker は、世界中のさまざまな Video Mesh ノードに配布するためのコンテナを格納するために Video Mesh ノードによって使用されます。Docker Hub に書き込むためのログイン情報を持っているのは Cisco だけです。Video Mesh ノードは、読み取り専用のログイン情報を使用して Docker Hub に接続し、アップグレード用のコンテナをダウンロードできます。

Note イメージは、プロビジョニングデータの一部としてノードに送信されるチェックサムに基づいてダウンロードされます。Docker pull の機能の詳細については、本ドキュメントを参照してください。https://docs.docker.com/v17.09/engine/userguide/storagedriver/imagesandcontainers/#sharing-promotes-smaller-images

留意点

Video Mesh ノードに関する次の情報および Webex 組織に登録した後、どのように動作するかに注意してください。

- 新しい Video Mesh ノードを展開時、Webex アプリおよび Webex の登録は、最大 2 時間、新しいノードを認識しません。クライアントは、スタートアップ時にノードの到達可能性、ネットワークの変更、キャッシュの有効期限を確認します。2 時間の待機または、回

避策として、Webex アプリ の再起動または Webex ルームまたはデスクデバイスの再起動ができます。後で、コールアクティビティが Control Hub の Video Mesh レポートにキャプチャされます。

- Video Mesh ノードは、1 つの Webex 組織に対する登録であり、マルチテナントデバイスではありません。
- Video Mesh ノードを使用するものと使用しないものを理解するには、「Video Mesh ノードを使用するクライアントとデバイス」の表を参照してください。
- Video Mesh ノードは、お使いの Webex サイトまたは他のカスタマーまたはパートナーの Webex サイトに接続できます。たとえば、サイト A が Video Mesh ノード クラスタを展開して、それを example1.webex.com ドメインに登録したとします。サイト A のユーザーが mymeeting@example1.webex.com にダイヤルインした場合は、Video Mesh ノードを使用し、カスケードが作成できます。サイト A 内のユーザーが、yourmeeting@example2.webex.com にダイヤルする場合、サイト A のユーザーが自身のローカル Video Mesh ノードを使用して、サイト B の Webex 組織のミーティングに接続します。

What to do next

- 追加ノードを登録するには、これらの手順を繰り返します。
- アップグレードが利用可能な場合は、できるだけ早く適用することを推奨します。アップグレードするには、次の手順を実行します。

1. プロビジョニングデータは、セキュリティで保護されたチャネルを介して、Cisco 開発チームによって Webex クラウドにプッシュされます。プロビジョニングデータは署名されています。コンテナの場合、プロビジョニングデータには名前、チェックサム、バージョンなどが含まれます。また、Video Mesh ノードは、セキュリティで保護されたチャネルを介して Webex クラウドからプロビジョニングデータを取得します。
2. Video Mesh ノードによってプロビジョニングデータがいったん取得されると、ノードは読み取り専用のログイン情報で認証され、コンテナを特定のチェックサムと名前でダウンロードし、システムをアップグレードします。Video Mesh ノードで実行される各コンテナには、イメージ名とチェックサムが含まれています。これらの属性は、セキュリティで保護されたチャネルを使用して Webex クラウドにアップロードされます。

Video Mesh ノードの Quality of Service（QoS）の有効化

始める前に

- 図と表に記載されている、必要なファイアウォールポートの変更を行います。「Video Mesh で使用されるポートとプロトコル」を参照してください。

- 値リストコレクション作成者をQoSに対して有効にするには、ノードがオンラインになっている必要があります。この設定を有効にすると、メンテナンスモードまたはオフライン状態のノードは除外されます。

手順

ステップ 1 https://admin.webex.com のカスタマービューで、**[サービス（Services）]** > **[ハイブリッド（Hybrid）]** に移動し、Video Mesh カードの **[設定の編集（Edit settings）]** をクリックします。

ステップ 2 **[サービスの品質（Quality of Service）]** までスクロールし、**[有効にする（Enable）]** をクリックします。

有効にすると、オンプレミスのSIPクライアント/エンドポイントおよび一意のDSCPマーキングがあるクラスタ間のカスケードの音声とビデオに使用される大規模な個別のポート範囲（オンプレミスの 呼制御構成によって決定）が取得されます。

- オーディオ：52500 ～ 59499 および 59500 ～ 62999 DSCP EF（Expedited Forwarding（EF; 完全優先転送））
- ビデオ/コンテンツ：63000 ～ 64667 および 64668 ～ 65500 DSCP AF41

値リストコレクション作成者からのすべてのSIPおよびカスケードトラフィックは、オーディオは、EF、ビデオは、AF41 とマークされています。個別のポート範囲は、カスケードメディアのソースポートとして、他の値リストコレクション作成者、クラウドメディアノード、さらに、SIP クライアントメディアの発信元と宛先のポートとして使用されます。Webex Teams アプリとカスケードメディアは、5004 の接続先共有ポートとポート範囲 50000 ～ 53000 を引き続き使用します。

（注） 共有ポートからのすべての Video Mesh リターン トラフィック（音声、ビデオ、コンテンツ）は、AF41 とマークされます。音声トラフィックは、発信元ポート番号に基づいて、ネットワーク内で EF と再マークされる必要があります。

QoS ポートの範囲に対して 1 つのノードがひとつづつ有効になっているかを示すステータスメッセージが表示されます。**[保留中ノードの確認（Review Pending Nodes）]** をクリック すると、QoSに対して保留状態になっているノードのリストが表示されます。ノードのコールトラフィックによっては、この設定を有効にするのに最大 2 時間かかることがあります。

ステップ 3 QoS が 2 時間以内に完全に有効になっていない場合は、さらなる調査を行うため、サポートに対してケースを開きます。

ノードがリブートし、新しいポートの範囲で更新されます。

この設定を無効にすると、音声とビデオ（34000–34999）の両方に使用される狭く整理したポート範囲を取得します。値リストコレクション作成者からのすべてのトラフィック（SIP、カスケード、クラウドトラフィックなど）は、1 つの AF41 のマーキングを取得します。

ウェブインターフェイスのリフレクタツールを使用した Video Mesh ノードのポート範囲の確認

必要な TCP/UDP ポートが Video Mesh ノードから開かれているかどうかを確認するため、リフレクタツール（Video Mesh ノードとクライアント上の Python スクリプトを使用したサーバーの組み合わせ）が使用されます。

始める前に

- https://github.com/CiscoDevNet/webex-video-mesh-reflector-client から Reflector ツールクライアント（Python スクリプト）のコピーをダウンロードします。
- スクリプトを正常に動作させるには、使用している環境で Python 2.7.10 またはそれ以降を実行していることを確認してください。
- 現在、このツールでは、Video Mesh ノードおよびクラスタ内検証に SIP エンドポイントをサポートしています。

手順

ステップ 1 https://admin.webex.com のカスタマービューで、値リストコレクション作成者のメンテナンスノードを有効にするには、次の手順に従います。

ステップ 2 ノードが Control Hub で [メンテナンス可能（Ready for maintenance）] ステータスを表示するまで待機します。

ステップ 3 Webex Video Mesh ノードインターフェイスを開きます。

この説明については、「ウェブインターフェイスからの Video Mesh ノードの管理」を参照してください。

ステップ 4 **[リフレクタツール（Reflector Tool）]** までスクロールし、使用するプロトコルに応じて **[TCP リフレクタサーバー（TCP Reflector Server）]** または **[UDP リフレクタサーバー（UDP Reflector Server）]** のいずれかを起動します。

ステップ 5 **[リフレクタサーバーの起動（Start Reflector Server）]** をクリックし、サーバーが正常に起動するまで待機します。

サーバーの起動時に通知が表示されます。

ステップ 6 Video Mesh ノードの到達先とするネットワーク上のシステム（PC など）から、次のコマンドでスクリプトを実行します。

```
$ python <local_path_to_client_script>/reflectorClient.py --ip <ip address of the server>
 --protocol <tcp or udp>
```

実行の終了時に、必要なすべてのポートが開かれている場合、クライアントは成功メッセージを表示します。

```
$ python reflectorClient.py --ip 10.22.162.102 --protocol tcp
Please wait while verifying tcp for ports: ['5004', '5060-5061'] ...
 [----------------------------->] 100.00%  Success/Failed/Total: 3/0/3

############################
No ports are blocked for tcp in ['5004', '5060-5061']
############################
Exiting Reflector Client tool...
$
```

必要なポートが開いていない場合、クライアントは、失敗した旨を通知するメッセージを示します。

```
$ python reflectorClient.py --ip 10.22.162.102 --protocol tcp --start-port 5060 --end-port 5062
Please wait while verifying tcp for port range: 5060 - 5062 ...
 [----------------------------->] 100.00%  Success/Failed/Total: 2/1/3

Failed ports in the first try:  ['5062']
Retrying(4 times) the above failed ports:
Retry number 1:
   Verifying port -> 5062
Retry number 2:
   Verifying port -> 5062
Retry number 3:
   Verifying port -> 5062
Retry number 4:
   Verifying port -> 5062
#########################
Ports which are not open for tcp are: ['5062']
#########################
Exiting Reflector Client tool...
```

ステップ 7 ファイアウォール上のポートの問題を解決してから、上記の手順を再実行します。

ステップ 8 詳細については、**--help** を使用してクライアントを実行してください。

```
$ python reflectorClient.py --help
Usage:
      --ip and --protocol are mandatory.
      If start-port is specified, end-port is considered mandatory. If no starting port is specified, default ports are verified for connectivity.
      By default, tool checks for QoS ports unless --non-qos option is specified.
      Default QoS ports include: TCP - 5004, 5060, 5061 and UDP - 5004, 52500-59499 and 63000-64667.
      Default non QoS ports include: TCP - 5004, 5060, 5061 and UDP - 5004, 34000-34999.
      To verify single port, both start and end port should be the required port to verify.
      Examples:
      Below run is to verify non-qos ports using an input port range:
        python reflectorClient.py --ip <hmn-ip-address> --protocol <udp/tcp> --start-port 52000 --end-port 52501 --non-qos
      Below run in to verify default qos ports:
        python reflectorClient.py --ip <> --protocol <udp/tcp>
$
```

プロキシ統合のための Video Mesh ノードの構成

Video Mesh と統合するプロキシのタイプを指定するには、次の手順を使用します。透過的な検査プロキシまたは明示的なプロキシを選択した場合、ノードのインターフェイスを使用してルート証明書をアップロードおよびインストールし、プロキシ接続を確認し、考え得る問題をトラブルシュートします。

始める前に

- サポートされているプロキシオプションの概要については、「Video Mesh のプロキシサポート」を参照してください。
- Video Mesh のプロキシサポートの要件

手順

ステップ 1 Web ブラウザで Video Mesh セットアップ URL `https://[IP または FQDN/setup` を入力し、ノード用にセットアップした管理者のログイン情報を入力して、**[サインイン（Sign In）]** をクリックし ます。

ステップ 2 [信頼ストアとプロキシ（Trust Store & Proxy）] に移動して、次のオプションを選択します。

- **プロキシなし（No proxy）**：プロキシを統合する前のデフォルトオプション。証明書の更新は必要ありません。
- **透過的な非検査プロキシ（Transparent Non-Inspecting Proxy）**：Video Mesh ノードは特定のプロキシサーバーアドレスを使用するように設定されないため、非検査プロキシと連動するための変更は必要ありません。証明書の更新は必要ありません。
- **透過的な検査プロキシ（Transparent Inspecting Proxy）**：Video Mesh ノードは特定のプロキシサーバーアドレスを使用するように設定されません。Video Mesh では http(s) 設定の変更は必要ありませんが、Video Mesh ノードにはプロキシを信頼するためのルート証明書が必要です。通常、IT は検査プロキシを使用して、アクセス可能な Web サイトおよび許可されないコンテンツのタイプに関するポリシーを適用します。このタイプのプロキシは、すべてのトラフィックを（https も）復号します。
- **明示的なプロキシ（Explicit Proxy）**：明示的なプロキシを使用する場合、プロキシサーバーが使用するクライアント（Video Mesh ノード）を指定します。このオプションは複数の認証タイプをサポートします。このオプションを選択した場合、以下の情報を入力する必要があります。

  1. **プロキシ IP/FQDN（Proxy IP/FQDN）**：プロキシ マシンに到達可能なアドレス。
  2. **プロキシポート（Proxy Port）**：プロキシがプロキシ経由のトラフィックをリッスンするために使用するポート番号。
  3. **プロキシプロトコル（Proxy Protocol）**：**http**（Video Mesh は、http プロキシ経由で https トラフィックをトンネル接続します）または **https**（Video Mesh ノードからプロキシへのトラフィックは、https プロトコルを使用します）を選択します。プロキシサーバーのサポート対象に応じてオプションを選択します。
  4. プロキシ環境に応じて、次の認証タイプの中から選択します。

オプション	使用方法
なし（**None**）	認証方式がない HTTP または HTTPS の明示的なプロキシを選択します。

オプション	使用方法
基本（**Basic**）	HTTP または HTTPS の明示的なプロキシで使用できます。 HTTP ユーザーエージェントが要求を行う際にユーザー名とパスワードを入力するために使用され、Base64 エンコーディングを使用します。
ダイジェスト（**Digest**）	HTTPS の明示的なプロキシでのみ使用できます。 機密情報を送信する前にアカウントを確認するために使用され、ネットワークを介して送信する前にユーザー名とパスワードにハッシュ機能を適用します。
NTLM	HTTP の明示的なプロキシでのみ使用できます。 ダイジェストと同様に、機密情報を送信する前にアカウントを確認するために使用されます。ユーザー名とパスワードではなく、Windows ログイン情報を使用します。 このオプションを選択する場合は、プロキシが **[NTLM ドメイン（NTLM Domain）]** フィールドで認証のために使用する Active Directory ドメインを入力します。**[NTLM ワークステーション（NTLM Workstation）]** フィールドで、指定された NTLM ドメイン内のプロキシワークステーション（ワークステーション アカウントまたはマシン アカウントとも呼ばれます）の名前を入力します。

透過的な検査または明示的なプロキシについては、次の手順に従います。

ステップ 3 **[ルート証明書またはエンドエンティティ証明書のアップロード（Upload a Root Certificate or End Entity Certificate）]** をクリックし、明示的または透過的な検査プロキシのルート証明書を見つけて選択します。

証明書はアップロードされますが、証明書をインストールするためにノードを再起動する必要があるため、まだインストールされません。詳細を確認するには、証明書発行者名の近くにある矢印をクリックします。または、誤りがあったために証明書を再アップロードする場合は、[**削除（Delete）**] をクリックします。

ステップ 4 透過的な検査または明示的なプロキシについては、**[プロキシ接続の確認（Check Proxy Connection）]** をクリックして、Video Mesh ノードとプロキシ間のネットワーク接続をテストします。

接続テストが失敗した場合は、失敗した理由とその問題を解決する方法を説明するエラーメッセージが表示されます。

ステップ 5 明示的なプロキシの場合、接続テストが成功した後、トグルを **[このノードからポート 443 へのすべての HTTPS リクエストを明示的なプロキシ経由でルーティングする（Route all port 443 https requests from this node through the explicit proxy）]** に切り替えます。この設定は適用されるまでに 15 秒かかります。

ステップ 6 **[すべての証明書を信頼ストアにインストール（Install All Certificates Into the Trust Store）]**（プロキシのセットアップ中にルート証明書が追加された場合は常に表示されます）または **[再起動（Reboot）]**（ルート証明書が追加されない場合は表示されます）をクリックし、プロンプトを読み、準備ができたら **[インストール（Install）]** をクリックします。

ノードは数分以内に再起動します。

ステップ 7 ノードが再起動したら、必要に応じて再度サインインして **[概要（Overview）]** ページを開き、接続チェックのステータスがすべて緑色になっていることを確認します。

プロキシ接続チェックでは、webex.com のサブドメインだけがテストされます。接続の問題がある場合、一般的な原因は、インストール手順に記載されているクラウドドメインの一部がプロキシでブロックされていることです。

呼制御タスクフローと Video Mesh の統合

Video Mesh に SIP ダイヤルインをルーティングするように、SIP トランクを設定します。SIP デバイスは、直接到達可能性をサポートしないため、Unified CM または VCS Expressway 設定を使用して、オンプレミス SIP デバイスおよび Video Mesh クラスタ間の関係を確立する必要があります。

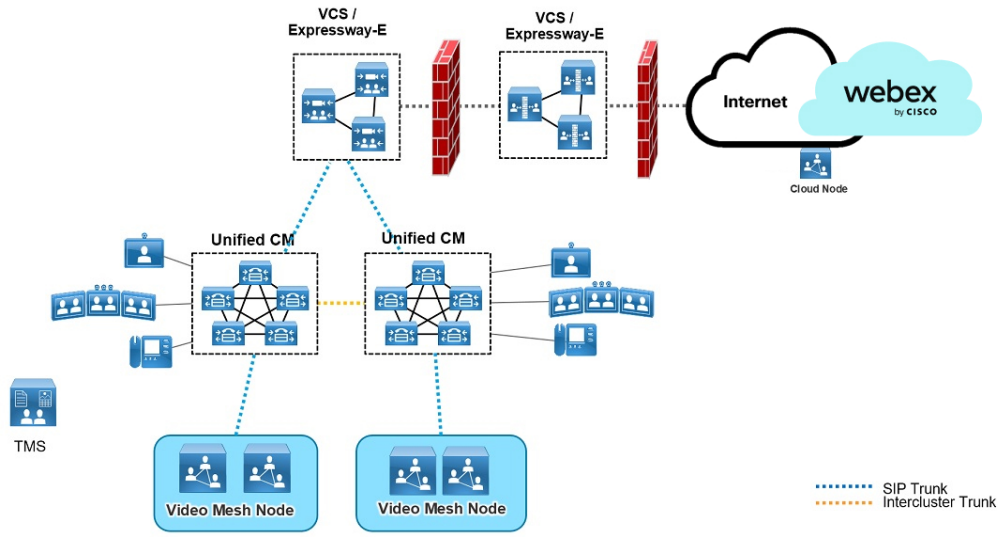
始める前に

- 一般的な導入例については、「Video Mesh と Cisco Unified Communications Manager の導入モデル」を参照してください。
- Video Mesh は、Unified CM と SIP シグナリング間の TCP または TLS のいずれかをサポートします。SIP TLS は VCS Expressway 向けにサポートされていません。
- Unified CM では、各 SIP トランクが最大 16 の Video Mesh 接続先（IP アドレス）をサポートできます。
- Unified CM では、SIP トランクセキュリティプロファイルの受信ポートは、デフォルト（非セキュア SIP トランクプロファイル）にできます。

- Video Mesh では、**webex.com**（短いビデオアドレス向け）、**sitename.webex.com**、および **meet.ciscospark.com** の 3 つのルートパターンがサポートされています。他のルートパターンはサポートされていません。

（注） 短いビデオアドレス形式（**meet@webex.com**）を使用する場合、Video Mesh ノードは常にコールを処理します。Video Mesh が有効になっていないサイトに対するコールの場合でも、ノードはコールを処理します。

図 *1 :* 分散 *Unified CM* を使用した *Video Mesh* の導入例



手順

	コマンドまたはアクション	目的
ステップ 1	呼制御環境とセキュリティ要件に応じて、次のオプションのいずれかを選択します。 • Unified CM セキュア TLS SIP トラフィックルーティングの設定 - Video Mesh （46 ページ） • Video Mesh 用の Unified CM TCP SIP トラフィックルーティングの設定（50 ページ） • Video Mesh 用の Expressway TCP SIP トラフィックルーティングの設定（54 ページ）（TCP のみ）	**Unified CM に登録されている SIP デバイス（TLS または TCP）** TLS 暗号化トラフィックまたは TCP SIP トラフィックのいずれかを使用して、Video Mesh を使用して Unified CM を設定します。高い可用性を備え、デバイス障害に対応できる、クラスタ設定を反映したトランクルーティングポリシーを作成できます。Unified CM Session Management Edition（SME）を使用している場合、Session Management クラスタ内の Unified CM サーバー間でインバ

	コマンドまたはアクション	目的
		ウンドコールとアウトバウンドコールが均等に分散されるよう、Unified CM SME とリーフシステムにトランクを設定します。 通常各サイトには、関連付けられている専用の Unified CM クラスタがあります。これらのクラスタは、クラスタ間 SIP トランクを介して接続されます。各クラスタには、Video Mesh ノードのローカルサイトへのコールイントランクが含まれます。 障害やオーバーフロー状態に対応できるように設定することもできます。この構成は、停止が発生した場合や Video Mesh クラスタがキャパシティに達した場合に役立ちます。クラスタとの間で SIP 会議またはコールを確立できない場合、会議/コールはオーバーフローします。 **VCS または Expressway に登録されている SIP デバイス（TCP のみ）** ネイバーゾーンと検索ルールを設定して、Webex Meetings から Video Mesh クラスタへ SIP ダイヤルインおよびダイヤルアウトをルートします。VCS Control または Expressway-C に登録されている SIP デバイスは、直接到達可能性をサポートしないため、TCP ベースの Expressway 設定を使用して、オンプレミス SIP デバイスおよび Video Mesh クラスタ間の関係を確立する必要があります。 障害やオーバーフロー状態に対応できるように設定することもできます。この構成は、停止が発生した場合や Video Mesh クラスタがキャパシティに達した場合に役立ちます。クラスタとの間で確立できない SIP ミーティングやコールは、VCS Control/Expressway-C または

	コマンドまたはアクション	目的
		Expressway-C/Eペアを介してクラウドにオーバーフローします。

Unified CM セキュア TLS SIP トラフィックルーティングの設定 - Video Mesh

手順

ステップ 1 Video Mesh クラスタに SIP プロファイルを作成するには、次のようにします。

a) Cisco Unified CM Administration から、**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [SIPプロファイル（SIP Profile）]** の順に選択し、**[検索（Find）]** をクリックします。

b) **[Cisco VCS用の標準SIPプロファイル（Standard SIP Profile For Cisco VCS）]** を選択し、さらに **[コピー（Copy）]** をクリックします。

c) 新しいプロファイルの名前を入力します。たとえば、「**`Video Mesh SIP プロファイル`**」と入力します。

d) **[トランク固有の構成（Trunk Specific Configuration）]** で、**[音声コールとビデオ コールに対する早期オファー サポート（Early Offer support for voice and video calls）]** を**[ベストエフォート（Best Effort）]**（MTP は挿入しない）にセットします。

この設定は、（Webex サイト用に外部ドメインによってルーティングされた）Webex クラウドへの新しいSIPトランクに適用できます。この設定は、既存のSIPトランキングやコールルーティングには影響を与えません。

e) **[サービスタイプのトランクの接続先ステータスをモニタするために OPTIONS Ping を有効にする（Enable OPTIONS Ping to monitor destination status for Trunks with Service Type）]** がオンになっていることを確認します。

f) その他のフィールドはデフォルト値のままにして変更を保存します。

ステップ 2 Video Mesh クラスタの新しい SIP トランク セキュリティ プロファイルを追加します。

a) Cisco Unified CM Administration から、**[システム（System）] > [セキュリティ（Security）] > [SIPトランクセキュリティプロファイル（SIP Trunk Security Profile）]** の順に選択し、さらに **[新規追加（Add New）]** をクリックします。

b) 「**`Video Mesh Secure SIP Trunk Security Profile`**」 などのわかりやすい名前を入力します。

c) 次の設定を確認します。

フィールド	値
デバイスセキュリティモード（Device Security Mode）	**暗号化（Encrypted）**

フィールド	値
着信転送タイプ（Incoming Transport Type）	**TLS**
発信転送タイプ（Outgoing Transport Type）	**TLS**
X.509 のサブジェクト名（X.509 Subject Name） 安全な証明書の件名またはサブジェクトの別名	Video Mesh ノード証明書の共通名を入力します。
着信ポート（Incoming Port）	**5061**
SIP V.150アウトバウンド SDPオファーのフィルタリング（SIP V.150 Outbound SDP Offer Filtering）	**デフォルトのフィルタを使用（Use Default Filter）**

d) その他のフィールドはデフォルト値のままにして変更を保存します。

ステップ 3 Video Mesh クラスタをポイントする新しい SIP トランクを追加します。

- Unified CM のみの導入では、トランクを 1 つ追加します。
- SME の導入では、通常、Unified CM と SME の間にトランクが存在します。SME と Video Mesh ノードの間に別のトランクを追加します。いずれのトランクにも以下の同じ内容を設定します。

a) Cisco Unified CM Administration で、**[デバイス（Device）] > [トランク（Trunk）]** の順に選択し、さらに **[新規追加（Add New）]** をクリックします。

b) トランク タイプに **[SIP トランク（SIP Trunk）]** を選択し、他の値はそのままにして **[次へ（Next）]** をクリックします。

c) 「**`Video_Mesh_SIP_Trunk_UCMtoVMN`**」 などのわかりやすい名前を入力します。

d) **[SRTP Allowed（SRTP を許可する）]** チェックボックスをオンにします。

e) **[発呼側および接続側情報フォーマット（Calling and Connecting Party Info Format）]** として、**[接続側にのみ URI および DN を配信（使用可能な場合）（Deliver URI and DN in connected party, if available）]** をオンにします。この設定により、混合アイデンティティが有効になります。これにより、SIP トランクが企業側のパーティのディレクトリ URI を Webex に送信できるようになります。

f) **[すべてのアクティブな Unified CM ノードで実行（Run on All Active Unified CM Nodes）]** をオンにします。

g) **[SIP 情報 - 宛先（SIP Information - Destination）]** で、各 Video Mesh ノードに対して IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。

h) **[宛先ポート（Destination Port）]** に「**5061**」と入力します。

i) **SIP トランク セキュリティ プロファイル**の場合は、前の手順で作成した「**Video Mesh トランク セキュリティ プロファイル**」を選択します。（「**Video Mesh Secure SIP Trunk Security Profile**」 はその一例です。）

j) **SIP プロファイル**の場合は、前の手順で作成した「**Video Mesh SIP プロファイル**」を選択します。（たとえば、「**Video Mesh SIP プロファイル**」など）。

k) その他のフィールドはデフォルト値のままにして変更を保存します。

（注） Video Mesh コールまたは会議では、SIP コールを終了するノードだけでなく、クラスタ内の任意のノードにメディアを割り当てることができます。

ステップ 4 Webex クラウドフェールオーバー用の Expressway をポイントする SIP トランクを作成します。

注意 既存の Unified CM と Expressway の導入にすでにある SIP トランクを使用できます。別のトランクを作成し、それら Expressway で Mobile Remote Access（MRA）も実行する場合は、MRA が中断されることがあります。

a) Cisco Unified CM Administration で、**[デバイス（Device）] > [トランク（Trunk）]** の順に選択し、さらに **[新規追加（Add New）]** をクリックします。

b) トランク タイプに **[SIP トランク（SIP Trunk）]** を選択し、他の値はそのままにして **[次へ（Next）]** をクリックします。

c) 「**Video_Mesh_VCS_Trunk**」 などのわかりやすい名前を入力します。

d) **[発呼側および接続側情報フォーマット（Calling and Connecting Party Info Format）]** として、**[接続側にのみ URI および DN を配信（使用可能な場合）（Deliver URI and DN in connected party, if available）]** をオンにします。この設定により、混合アイデンティティが有効になります。これにより、SIP トランクが企業側のパーティのディレクトリ URI を Webex に送信できるようになります。

e) **[SIP 情報 - 宛先（SIP Information - Destination）]** で、各 Expressway の IP アドレス、または完全修飾ドメイン名（FQDN）を入力します。**[ポート（Port）]** に対して、「**5060**」を入力します。

f) **[SIP プロファイル（SIP Profile）]** には、**[Cisco VCS 用の標準 SIP プロファイル（Standard SIP Profile For Cisco VCS）]** を選択します。

ステップ 5 Video Mesh クラスタへのコール用の新しいルートグループを作成します。

a) Cisco Unified CM Administration で、**[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートグループ（Route Group）]** の順に選択し、**[新規追加（Add New）]** をクリックします。

b) 「**Video Mesh Node Route Group**」 などの、わかりやすい名前を入力します。

c) **分散アルゴリズム**を**トップダウン方式**に変更します。

d) **[ルートグループメンバー情報]** セクションで、**Video Mesh**と名前が付いているデバイスを見つけます。

e) **[ルートグループに追加（Add to Route Group）]** をクリックし、「**Video_Mesh_SIP_Trunk_UCMtoVMN**」 を追加します。

f) 変更を保存します。

ステップ 6 クラウドにオーバーフローできるように、コールを Expressway に渡す新しいルートグループを作成します。

a) Cisco Unified CM Administration で、**[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートグループ（Route Group）]** の順に選択し、**[新規追加（Add New）]** をクリックします。

b) 「**Video Mesh Expressway Route Group**」 などの、わかりやすい名前を入力します。

c) **分散アルゴリズム**を**トップダウン方式**に変更します。

d) **[ルートグループメンバー情報]** セクションで、**Video Mesh** と名前が付いているデバイスを見つけます。

e) **[ルートグループに追加（Add to Route Group）]** をクリックし、**「Video_Mesh_VCS_Trunk」** を追加します。

f) 変更を保存します。

ステップ 7 Video Mesh クラスタおよび Expressway にコールするための新しいルートリストを作成 します。

a) Cisco Unified CM Administration で、**[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートリスト（Route List）]** の順に選択し、**[新規追加（Add New）]** をクリックします。

b) 「**Video Mesh Node Route List**」 などの、わかりやすい名前を入力します。

c) **[Cisco Unified Communications Manager グループ（Cisco Unified Communications Manager Group）]** を **[デフォルト（Default）]** に設定するか、構成に合わせて別の値を設定します。

d) 変更を保存します。

e) **[ルートリストメンバー情報]** セクションで、**[ルートグループの追加（Add Route Group）]** をクリックして、**「Video Mesh ルート グループ」** を選択します。

f) その他の設定はデフォルトのままにし、変更内容を保存します。

g) **[ルートリストメンバー情報]** セクションで、**[ルートグループの追加（Add Route Group）]** をクリックして、**「Video Mesh エクスプレスウェイ ルート グループ」** を選択します。

h) その他の設定はデフォルトのままにし、変更内容を保存します。

ステップ 8 Webex ミーティング向けに、短いビデオアドレスのダイヤリング形式の SIP ルートパターンを作成します。

a) **[コールルーティング（Call Routing）] > [SIP ルートパターン（SIP Route Pattern）]** で、**[新規追加（Add New）]** をクリックし、「**Video Mesh Route Pattern for Webex Short URIs**」 という名前を入力します。

b) **[Pv4 パターン（IPv4 pattern）]** で、ドメインとして **webex.com** と入力します。

c) **[SIP トランク/ルートリスト（SIP Trunk/Route List）]**の場合は、Video Mesh に対して作成された [ルートリスト（Route List）] を選択します。例：**「Video Mesh ルート リスト」** など。

d) その他のフィールドはデフォルト値のままにして変更を保存します。

短いビデオアドレスダイヤリング機能により、ユーザーは、ビデオシステムを使用して Webex ミーティングまたはイベントに参加するために Webex サイト名を記憶しておく必要がなくなりました。知っておく必要があるのはミーティングまたはイベントの番号のみであるため、ミーティングにより迅速に参加できます。

ステップ 9 Webex サイトの SIP ルートパターンを作成します。

a) **[コールルーティング（Call Routing）] > [SIP ルートパターン（SIP Route Pattern）]** で、**[新規追加（Add New）]** をクリックし、「**`Video Mesh Route Pattern for Webex Sites`**」 という名前を入力します。

b) **[Pv4 パターン（IPv4 pattern）]** で、メディアを最適化する Webex サイト（例：「**examplesitename.webex.com**」）を入力します。

c) **[SIP トランク/ルートリスト（SIP Trunk/Route List）]**の場合は、Video Mesh に対して作成された [ルートリスト（Route List）] を選択します。例：「**Video Mesh ルート リスト**」など。

d) その他のフィールドはデフォルト値のままにして変更を保存します。

ステップ 10 Webex アプリ ミーティング用の SIP ルートパターンを作成し ます（下位互換性）。

a) **[コールルーティング（Call Routing）] > [SIP ルートパターン（SIP Route Pattern）]** で、**[新規追加（Add New）]** をクリックし、「**`Video Mesh Route Pattern for Teams Meetings`**」 という名前を入力します。

b) **[Pv4 パターン（IPv4 pattern）]** に、**meet.ciscospark.com** と入力します。

c) **[SIP トランク/ルートリスト（SIP Trunk/Route List）]**の場合は、Video Mesh に対して作成された [ルートリスト（Route List）] を選択します。例：「**Video Mesh ルート リスト**」など。

d) その他のフィールドはデフォルト値のままにして変更を保存します。

Video Mesh 用の Unified CM TCP SIP トラフィックルーティングの設定

Procedure

ステップ 1 Video Mesh クラスタに SIP プロファイルを作成するには、次のようにします。

a) Cisco Unified CM Administration から、**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [SIPプロファイル（SIP Profile）]** の順に選択し、**[検索（Find）]** をクリックします。

b) **[Cisco VCS用の標準SIPプロファイル（Standard SIP Profile For Cisco VCS）]** を選択し、さらに **[コピー（Copy）]** をクリックします。

c) 新しいプロファイルの名前を入力します。たとえば、“**`Video Mesh SIP プロファイル`**” と入力します。

d) **[トランク固有の構成（Trunk Specific Configuration）]** で、**[音声コールとビデオ コールに対する早期オファー サポート（Early Offer support for voice and video calls）]** を**[ベストエフォート（Best Effort）]**（MTP は挿入しない）にセットします。

この設定は、（Webex サイト用に外部ドメインによってルーティングされた）Webex への新しい SIP トランクに適用できます。この設定は、既存の SIP トランキングやコールルーティングには影響を与えません。

e) **[サービスタイプのトランクの接続先ステータスをモニタするために OPTIONS Ping を有効にする（Enable OPTIONS Ping to monitor destination status for Trunks with Service Type）]** がオンになっていることを確認します。

f) その他のフィールドはデフォルト値のままにして変更を保存します。

ステップ 2 Video Mesh クラスタの新しい SIP トランク セキュリティ プロファイルを追加します。

a) Cisco Unified CM Administration から、**[システム（System）] > [セキュリティ（Security）] > [SIP トランクセキュリティプロファイル（SIP Trunk Security Profile）]** の順に選択し、さらに **[新規追加（Add New）]** をクリックします。

b) "**`Video Mesh Trunk Security Profile`**" などの、わかりやすい名前を入力します。

c) 次の設定を確認します。

フィールド	値
デバイスセキュリティモード（Device Security Mode）	**非セキュア（Non Secure）**
着信転送タイプ（Incoming Transport Type）	**TCP+UDP**
発信転送タイプ（Outgoing Transport Type）	**TCP**
着信ポート（Incoming Port）	**5060**
SIP V.150アウトバウンド SDPオファーのフィルタリング（SIP V.150 Outbound SDP Offer Filtering）	**デフォルトのフィルタを使用（Use Default Filter）**

d) その他のフィールドはデフォルト値のままにして変更を保存します。

ステップ 3 Video Mesh クラスタをポイントする新しい SIP トランクを追加します。

- Unified CM のみの導入では、トランクを 1 つ追加します。
- SME の導入では、通常、Unified CM と SME の間にトランクが存在します。SME と Video Mesh ノードの間に別のトランクを追加します。いずれのトランクにも以下の同じ内容を設定します。

a) Cisco Unified CM Administration で、**[デバイス（Device）] > [トランク（Trunk）]** の順に選択し、さらに **[新規追加（Add New）]** をクリックします。

b) トランク タイプに **[SIP トランク（SIP Trunk）]** を選択し、他の値はそのままにして **[次へ（Next）]** をクリックします。

c) **"`Video_Mesh_SIP_Trunk_UCMtoVMN`"** などのわかりやすい名前を入力します。

d) **[発呼側および接続側情報フォーマット（Calling and Connecting Party Info Format）]** として、**[接続側にのみ URI および DN を配信（使用可能な場合）（Deliver URI and DN in connected party, if available）]** をオンにします。この設定により、混合アイデンティティ

が有効になります。これにより、SIP トランクが企業側のパーティのディレクトリ URI を Webex に送信できるようになります。

e) **[すべてのアクティブな Unified CM ノードで実行（Run on All Active Unified CM Nodes）]** をオンにします。

f) **[SIP 情報 - 宛先（SIP Information - Destination）]** で、各 Video Mesh ノードに対して IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。

g) **[宛先ポート（Destination Port）]** に**「5060」**と入力します。

h) **SIP トランク セキュリティ プロファイル**の場合は、前の手順で作成した**「Video Mesh トランク セキュリティ プロファイル」**を選択します。（たとえば、"**`Video Mesh トランク セキュリティ プロファイル`**"など）。

i) **SIP プロファイル**の場合は、前の手順で作成した**「Video Mesh SIP プロファイル」**を選択します。（たとえば、"**`Video Mesh SIP プロファイル`**"など）。

j) その他のフィールドはデフォルト値のままにして変更を保存します。

Note Video Mesh コールまたは会議では、SIP コールを終了するノードだけでなく、クラスタ内の任意のノードにメディアを割り当てることができます。

ステップ 4 Expressway をポイントする新しい SIP トランクを作成します。

Caution 既存の Unified CM と Expressway の導入にすでにある SIP トランクを使用できます。別のトランクを作成し、それら Expressway で Mobile Remote Access（MRA）も実行する場合は、MRA が中断されることがあります。

a) Cisco Unified CM Administration で、**[デバイス（Device）] > [トランク（Trunk）]** の順に選択し、さらに **[新規追加（Add New）]** をクリックします。

b) トランク タイプに **[SIP トランク（SIP Trunk）]** を選択し、他の値はそのままにして **[次へ（Next）]** をクリックします。

c) "**`Video_Mesh_VCS_Trunk`**" などのわかりやすい名前を入力します。

d) **[発呼側および接続側情報フォーマット（Calling and Connecting Party Info Format）]** として、**[接続側にのみ URI および DN を配信（使用可能な場合）（Deliver URI and DN in connected party, if available）]** をオンにします。この設定により、混合アイデンティティが有効になります。これにより、SIP トランクが企業側のパーティのディレクトリ URI を Webex に送信できるようになります。

e) **[SIP 情報 - 宛先（SIP Information - Destination）]** で、各 Expressway の IP アドレス、または完全修飾ドメイン名（FQDN）を入力します。**[ポート（Port）]** に対して、**「5060」**を入力します。

f) **[SIP プロファイル（SIP Profile）]** には、**[Cisco VCS 用の標準 SIP プロファイル（Standard SIP Profile For Cisco VCS）]** を選択します。

ステップ 5 Video Mesh クラスタへのコール用の新しいルートグループを作成します。

a) Cisco Unified CM Administration で、**[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートグループ（Route Group）]** の順に選択し、**[新規追加（Add New）]** をクリックします。

b) "**`Video Mesh Node Route Group`**" などの、わかりやすい名前を入力します。

c) **分散アルゴリズム**を**トップダウン方式**に変更します。

d) **[ルートグループメンバー情報]** セクションで、**Video Mesh** と名前が付いているデバイスを見つけます。
e) **[ルートグループに追加（Add to Route Group）]** をクリックし、“**Video_Mesh_SIP_Trunk_UCMtoVMN**” を追加します。
f) 変更を保存します。

ステップ 6 クラウドにオーバーフローできるように、コールを Expressway に渡す新しいルートグループを作成します。

a) Cisco Unified CM Administration で、**[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートグループ（Route Group）]** の順に選択し、**[新規追加（Add New）]** をクリックします。
b) “**Video Mesh Expressway Route Group**” などの、わかりやすい名前を入力します。
c) **分散アルゴリズム**を**トップダウン方式**に変更します。
d) **[ルートグループメンバー情報]** セクションで、**Video Mesh** と名前が付いているデバイスを見つけます。
e) **[ルートグループに追加（Add to Route Group）]** をクリックし、“Video_Mesh_VCS_Trunk” を追加します。
f) 変更を保存します。

ステップ 7 Video Mesh クラスタおよび Expressway にコールするための新しいルートリストを作成します。

a) Cisco Unified CM Administration で、**[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートリスト（Route List）]** の順に選択し、**[新規追加（Add New）]** をクリックします。
b) “**Video Mesh Node Route List**” などの、わかりやすい名前を入力します。
c) **[Cisco Unified Communications Manager グループ（Cisco Unified Communications Manager Group）]** を **[デフォルト（Default）]** に設定するか、構成に合わせて別の値を設定します。
d) 変更を保存します。
e) **[ルートリストメンバー情報]** セクションで、**[ルートグループの追加（Add Route Group）]** をクリックして、**「Video Mesh ルート グループ」**を選択します。
f) その他の設定はデフォルトのままにし、変更内容を保存します。
g) **[ルートリストメンバー情報]** セクションで、**[ルートグループの追加（Add Route Group）]** をクリックして、**「Video Mesh エクスプレスウェイ ルート グループ」**を選択します。
h) その他の設定はデフォルトのままにし、変更内容を保存します。

ステップ 8 Webex ミーティング向けに、短いビデオアドレスのダイヤリング形式の SIP ルートパターンを作成します。

a) **[コールルーティング（Call Routing）] > [SIP ルートパターン（SIP Route Pattern）]** で、**[新規追加（Add New）]** をクリックし、“**Video Mesh Route Pattern for Webex Short URIs**” という名前を入力します。
b) **[Pv4 パターン（IPv4 pattern）]** で、ドメインとして **webex.com** と入力します。
c) **[SIP トランク/ルートリスト（SIP Trunk/Route List）]**の場合は、Video Mesh に対して作成された [ルートリスト（Route List）] を選択します。例：“**Video Mesh ルート リスト**”など。
d) その他のフィールドはデフォルト値のままにして変更を保存します。

短いビデオアドレスダイヤリング機能により、ユーザーは、ビデオシステムを使用して Webex ミーティングまたはイベントに参加するために Webex サイト名を記憶しておく必要がなくなりました。知っておく必要があるのはミーティングまたはイベントの番号のみであるため、ミーティングにより迅速に参加できます。

ステップ 9 Webex サイトの SIP ルートパターンを作成します。

a) **[コールルーティング（Call Routing）] > [SIP ルートパターン（SIP Route Pattern）]** で、**[新規追加（Add New）]** をクリックし、“**Video Mesh Route Pattern for Webex Sites**” という名前を入力します。

b) **[IPv4 パターン（IPv4 pattern）]**で、メディアを最適化する Webex サイトを入力します。たとえば、“**examplesitename.webex.com**” です（**examplesitename** は実際の Webex サイトの名前）。

c) **[SIP トランク/ルートリスト（SIP Trunk/Route List）]**の場合は、Video Mesh に対して作成された [ルートリスト（Route List）] を選択します。例：“**Video Mesh ルートリスト**”など。

d) その他のフィールドはデフォルト値のままにして変更を保存します。

ステップ 10 Webex アプリ ミーティング用の SIP ルートパターンを作成し ます。

a) **[コールルーティング（Call Routing）] > [SIP ルートパターン（SIP Route Pattern）]** で、**[新規追加（Add New）]** をクリックし、“**Video Mesh Route Pattern for Teams Meetings**” という名前を入力します。

b) **[Pv4 パターン（IPv4 pattern）]** に、**meet.ciscospark.com** と入力します。

c) **[SIP トランク/ルートリスト（SIP Trunk/Route List）]**の場合は、Video Mesh に対して作成された [ルートリスト（Route List）] を選択します。例：“**Video Mesh ルートリスト**”など。

d) その他のフィールドはデフォルト値のままにして変更を保存します。

Video Mesh 用の Expressway TCP SIP トラフィックルーティングの設定

Procedure

ステップ 1 Video Mesh クラスタをポイントするゾーンを作成します。

a) VCS Control または Expressway-C から、**[設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）]** に移動し、**[新規（New）]** をクリックします。

b) 次のフィールドを設定します。

フィールド名	値
名前（Name）	**WebexVideoMeshZone** などゾーンを容易に識別するための名前を入力します。
タイプ（Type）	**ネイバー（Neighbor）**
H.323	

フィールド名	値
モード（Mode）	**オフ（Off）**
SIP	
モード（Mode）	**オン（On）**
ポート（Port）	**5060**
転送	**TCP**
ロケーション（Location）	
次の方法でピアを検索する（Look up peers by）	**アドレス（Address）**
ピア [n] アドレス	各 Video Mesh ノードの IP アドレスを入力します。

c) その他のフィールドはデフォルト設定のままにし、変更を保存します。

ステップ 2 Webex サイトの Video Mesh クラスタ用のダイヤルパターンを作成します。

a) Expressway-C から、**[設定（Configuration）]** > **[ダイヤル プラン（Dial Plan）]** > **[検索ルール（Search rules）]** に移動し、**[新規（New）]** をクリックします。

b) Webex サイト検索ルール用に次のフィールドを設定します。

フィールド名	値
ルール名（Rule Name）	検索ルールを簡単に識別するためのルール名（たとえば、**WebexVideoMesh-YourSite**）を入力します。
優先度（Priority）	デフォルトは**100**です。この数値がクラウドのフォールバックルールおよびB2Bルールよりも低いことを確認してください。
プロトコル（Protocol）	**SIP**
モード（Mode）	**エイリアスのパターンマッチ（Alias pattern match）**
パターンタイプ（Pattern type）	**Regex**

フィールド名	値
パターン文字列（Pattern string）	`.*@(YourSite\.)?webex\.com.*` **Note** このパターンは、**yoursite.webex.com** と **webex.com**（短いビデオアドレス向け）の両方の形式と一致します。短いビデオ アドレス ダイヤリング機能により、ユーザーは、ビデオシステムを使用して Webex ミーティングまたはイベントに参加するために Webex サイト名を記憶しておく必要がなくなりました。知っておく必要があるのはミーティングまたはイベントの番号のみであるため、ミーティングにより迅速に参加できます。
パターン動作（Pattern behavior）	**変更なし（Leave）**
正常に一致する場合（On successful match）	**続行（Continue）**
ターゲット（Target）	**WebexVideoMeshZone** など、作成した Video Mesh ゾーンを選択します。

c) その他のフィールドはデフォルト設定のままにし、変更を保存します。

ステップ 3 フェールオーバーのためのクラウド Expressway をポイントするトラバーサルクライアントとゾーンのペアを作成します。

a) トラバーサルクライアントとゾーンペアを作成する手順については、『*Expressway* 基本設定ガイド』を参照してください。

ステップ 4 Expressway-E をリードするトラバーサル クライアント ゾーンにフォールバック検索ルールを作成します。

a) Expressway-C から、**[設定（Configuration）]** > **[ダイヤル プラン（Dial Plan）]** > **[検索ルール（Search rules）]** に移動し、**[新規（New）]** をクリックします。

b) 次のフィールドを設定します。

フィールド名	値
ルール名（Rule Name）	検索ルールを簡単に識別するためのルール名（たとえば、**WebexVideoMesh-Failover**）を入力します。
優先度（Priority）	100 がデフォルトです。Video Mesh のダイヤルパターンおよびB2Bルールより高い数値を入力して、優先順位が低いことを確認します。
プロトコル（Protocol）	**SIP**

フィールド名	値
モード（Mode）	**Any Alias**
パターン動作（Pattern behavior）	**変更なし（Leave）**
正常に一致する場合（On successful match）	**続行（Continue）**
ターゲット（Target）	Expressway-E をリードするトラバース クライアント ゾーンを選択します。

c) その他のフィールドはデフォルト設定のままにし、変更を保存します。

ステップ 5 Expressway-E から、**[設定（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]** に移動します。**[新規（New）]** をクリックして、Webex Zone を追加します。

X8.11 より前のバージョンでは、この目的のために新しい DNS ゾーンを作成しました。

ステップ 6 クラウド Expressway のダイヤルパターンを作成します。

a) Expressway-E から、**[設定（Configuration）]** > **[ダイヤル プラン（Dial Plan）]** > **[検索ルール（Search rules）]** に移動し、**[新規（New）]** をクリックします。

b) 次のフィールドを設定します。

フィールド名	値
ルール名（Rule Name）	検索ルールを簡単に識別するためのルール名（たとえば、**WebexVideoMesh-toCloud**）を入力します。
優先度（Priority）	ローカルの Video Mesh ノードのルールより大きい値を入力してください。ノードが 100 に設定されている場合、この値を **101** に設定します。また、その値が Expressway のすべての B2B ルールより低いことも確認する必要があります。
プロトコル（Protocol）	**SIP**
ソース（Source）	**指定（Named）**
ソース名（Source Name）	**WebexVideoMeshZone** などのセキュア トラバーサル サーバー ゾーンを選択します。
モード（Mode）	**エイリアスのパターンマッチ（Alias pattern match）**
パタータイプ（Pattern type）	**Regex**
パターン文字列（Pattern string）	`.*@(YourSite\.)?webex\.com.*`

フィールド名	値
パターン動作（Pattern behavior）	**変更なし（Leave）**
正常に一致する場合（On successful match）	**停止（Stop）**
ターゲット（Target）	Webex Zone または DNS ゾーンを選択します。

ステップ 7 Expressway-C に登録されている SIP デバイスの場合、ブラウザでデバイスの IP アドレスを入力し、**[セットアップ（Setup）]** に移動し、**[SIP]** にスクロールして、**[タイプ（Type）]** ドロップダウンから **[標準（Standards）]** を選択します。

Unified CM と Video Mesh ノード間での証明書チェーンの交換

証明書交換を完了して、Unified CM と Video Mesh インターフェイス間の双方向の信頼を確立します。証明書は、安全なトランク設定を使用し、組織内の暗号化された SIP トラフィックと SRTP メディアが、信頼できる Unified CM から信頼できる Video Mesh ノードに到達することを許可します。

（注） クラスタ化された環境では、CA とサーバー証明書を各ノードにインストールする必要があります。

始める前に

セキュリティ上の理由から、ノードのデフォルトの自己署名証明書の代わりに、Video Mesh ノードで CA 署名付き証明書を使用することをお勧めします。

手順

ステップ 1 Web ブラウザで Video Mesh ノードインターフェイス（IP アドレス/セットアップ、例：`https://192.0.2.0/setup`）を開き、そのノードの管理者ログイン情報でサインインします。

ステップ 2 **[サーバー証明書（Server Certificates）]** に移動し、必要に応じて証明書とキーのペアをリクエストおよびアップロードします。

a) （オプション）認定プロバイダーから発行された証明書が必要な場合は、**[証明書署名要求の作成（Create a Certificate Signing Request）]** をクリックします。必要な情報（共通名を

含む必要があるFQDNである**サブジェクト代替名**を含む）を入力し、リクエストを作成します。CSRをダウンロードし、リクエストをプロバイダーに送信します。（リクエストは複数可能です。これらは、認証局（CA）の署名付き証明書（CSR の作成中にすでに生成された秘密キー）を返します

（注） 共通名はURLではありません。プロトコル（http://やhttps://など）、ポート番号、またはパス名は含まれません。X.509 証明書仕様の `commonName` フィールドは、共通名を表します。`https://www.example.com` の場合、正しい値は `example.com` です。

秘密キーは、CSRを生成したときにすでに配置されています。CSRの作成手順を使用しない場合、秘密キーをアップロードする必要があります。

b) 証明書とキーを有している場合、**[サーバー証明書のアップロード（.crt または .pem ファイル）（Upload a Server Certificate（.crt or .pem file））]** をクリックし、証明書ファイルを選択して、**[秘密キーのアップロード（.key ファイル）（Upload a Private Key（.key file））]** をクリックし、パスフレーズがある場合はパスフレーズを入力します。

c) 証明書を取得したら、クラスタ内の最初の Video Mesh ノードに移動し、**[サーバー証明書のインストール（Install Server Certificate）]** をクリックし、プロンプトを読み、**[インストール（Install）]** をクリックして **[OK]** をクリックします。

クラウドに登録されたVideo Meshノードは正常にシャットダウンし、通話が終了するまで最大 2 時間待機します。その後、ノードは証明書のインストールを完了します。サーバー証明書がインストールされると、プロンプトが表示されます。その後、ページをリロードして、新しい証明書とキーエントリを表示できます。

d) 証明書とキーファイルの横にある **[ダウンロード（Download）]** をクリックして、ローカルコピーを保存します。

ファイルを覚えやすい場所に保存し、ブラウザタブで、Video Meshインスタンスを開いたままにしておきます。

e) クラスタ内の次のVideo Meshノードに移動し、パスフレーズを入力して、秘密キーファイルをアップロードします。その後、**[サーバー証明書のアップロード（Upload a Server Certificate）]** をクリックし、**[サーバー証明書のインストール（Install Server Certificate）]** を選択し、プロンプトを読み、**[インストール（Install）]** をクリックして **[OK]** をクリックします。

f) 同じクラスタ内の Video Mesh ノードについて、この手順を繰り返します。

ステップ 3 別のブラウザタブで、Cisco Unified OS の管理から、**[セキュリティ（Security）]** > **[証明書の管理（Certificate Management）]** に移動します。検索条件を入力して **[検索（Find）]** をクリックし、証明書または証明書信頼リスト(CTL)のファイル名を選択して **[ダウンロード（Download）]** をクリックします。

Unified CM ファイルを覚えやすい場所に保存し、ブラウザタブで、 Unified CM インスタンスは開いたままにしておきます。

ステップ 4 Video Mesh [ノードインターフェイス（Node Interface）] タブに戻り、**[信頼ストアおよびプロキシ（Trust Store & Proxy）]** をクリックして、オプションを選択します。

- Unified CM がよく知られた組織によって署名された CA 証明書を使用する場合、Video Mesh ノードはそれを自動的に信頼します。信頼は、定期的に更新される VMN ノードのホスト OS からのルート証明書のリストに基づいています。
- Unified CM が内部の企業 CA ルート証明書で署名された CA 証明書を使用する場合、そのルート証明書をノードに追加します。このルート証明書は企業内から入手できますが、Unified CM からダウンロードできない場合があります。
- Unified CM が外部要求を処理するために使用する ECDSA 証明書と RSA 証明書の両方を追加します。これらの証明書は、自己署名証明書または CA 証明書です。
- 1 つの証明書をダウンロードした場合は、**[ルート証明書またはエンドエンティティ証明書のアップロード（.crt または .pem ファイル）（Upload a Root Certificate or End Entity Certificate（.crt or .pem file））]** をクリックし、ダウンロードした CallManager.pem 証明書ファイルを選択します。**[すべての証明書を信頼ストアにインストール（Install All Certificates into the Trust Store）]** をクリックし、プロンプトを読み、**[インストール（Install）]** をクリックして、ノードを再起動します。
- 証明書チェーンをダウンロードした場合は、ルート CA 証明書と中間 CA 証明書をアップロードし、**[すべての証明書を信頼ストアにインストール（Install All Certificates into the Trust Store）]** をクリックし、プロンプトを読んで **[インストール（Install）]** をクリックします。

クラウドに登録された Video Mesh ノードは正常にシャットダウンし、通話が終了するまで最大 2 時間待機します。CallManager.pem 証明書をインストールするには、ノードが自動的に再起動します。オンラインに戻ると、CallManager.pem 証明書が Video Mesh ノードにインストールされている場合にはプロンプトが表示されます。その後、ページをリロードして新しい証明書を表示できます。

ステップ 5 [Cisco Unified OS の管理（Cisco Unified OS Administration）] タブに戻り、**[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）]** をクリックします。**[証明書の目的（Certificate Purpose）]** ドロップダウンリストから証明書名を選択し、Video Mesh ノードインターフェイスからダウンロードしたファイルを参照して、**[開く（Open）]** をクリックします。

ステップ 6 ファイルをサーバーにアップロードするには、[ファイルのアップロード（Upload File）] をクリックします。

証明書チェーンをアップロードしている場合は、チェーン内のすべての証明書をアップロードする必要があります。

（注） 証明書をアップロードしたら、影響を受けるサービスを再起動します。サーバーが再起動したら、CCMAdmin または CCMUser GUI にアクセスして、新しく追加した証明書が使用されていることを確認できます。

（注） API を使用してサーバー証明書をインストールおよび管理できます。詳細については、「VMN サーバー証明書 API （24 ページ）」を参照してください。

組織およびVideo Meshクラスタのメディア暗号化の有効化

組織および個々のVideo Meshクラスタのメディア暗号化をオンにする場合は、次の手順を実行します。この設定では、エンドツーエンドの TLS セットアップが強制的に実行され、Video Mesh ノードをポイントするセキュアな TLS SIP トランクが Unified CM に配置されている必要があります。

設定	結果
Unified CM は安全なトランクで設定されており、このVideo Mesh Control Hub 設定は有効になっていません。	コールが失敗します。
Unified CM は安全なトランクで設定されておらず、このVideo Mesh Control Hub 設定は有効になっています。	コールは失敗しませんが、非セキュアモードにフォールバックします。

注意 シスコのエンドポイントには、エンドツーエンドの暗号化が動作するように、セキュリティプロファイルと TLS ネゴシエーションを設定する必要があります。この設定を行わない場合、TLSを使用して設定されていないエンドポイントからクラウドにコールがオーバーフローします。すべてのエンドポイントが TLS を使用するように設定できる場合にのみ、この機能を有効にすることをお勧めします。

始める前に

- Unified CM セキュア TLS SIP トラフィックルーティングの設定 - Video Mesh （46 ページ）
- Unified CM と Video Mesh ノード間での証明書チェーンの交換 （58 ページ）

手順

ステップ 1 https://admin.webex.com のカスタマービューで、**[サービス（Services）]** > **[ハイブリッド（Hybrid）]** に移動し、Video Mesh カードの **[設定（Settings）]** をクリックします。

ステップ 2 **[メディア暗号化（Media Encryption）]** までスクロールし、設定をオンに切り替えます。

この設定により、組織内の Video Mesh ノードを通過するすべてのメディアチャネルで暗号化が強制されます。コールが失敗する可能性がある状況や、エンドツーエンドの暗号化が動作するために必要な要件については、前の表および注意を参照してください。

ステップ 3 **[すべて表示（Show all）]** をクリックし、セキュアな SIP トラフィックを有効にする各 Video Mesh クラスタで、次の手順を繰り返します。

a) リストにある Video Mesh クラスタエントリを選択して、**[クラスタ設定の編集（Edit cluster settings）]** をクリックします。
b) **[SIP コール（SIP Calls）]** までスクロールし、チェックボックスをオンにします。
c) **[信頼済み SIP 送信元（Trusted SIP sources）]** で、Unified CM 証明書のサブジェクト代替名（通常は Unified CM の FQDN）に存在する共通名（CN）または FQDN を入力します。

これらのエントリは信頼済み SIP 送信元として識別され、セキュアな SIP コールを Webex Video Mesh に送信することが許可されます。

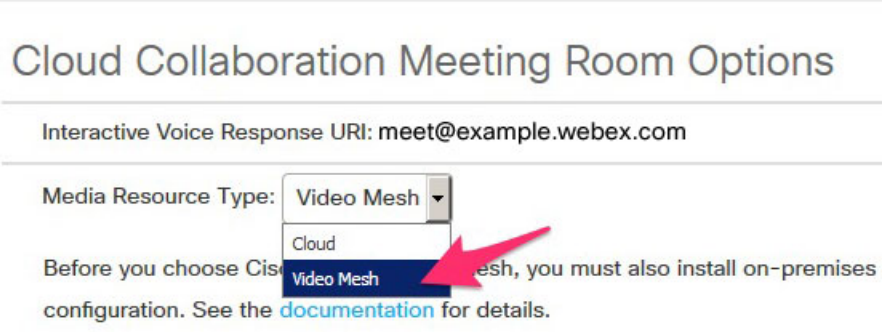
Webex サイトの Video Mesh の有効化

Webex ミーティングの Video Mesh ノードに最適化されたメディアを使用して、すべての Webex アプリとデバイスに参加するには、この設定を Webex サイトで有効にする必要があります。この設定を有効化することによって、クラウドで Video Mesh およびミーティングインスタンスが一緒にリンクされ、カスケードが Video Mesh ノードで発生できるようになります。この設定が有効になっていない場合、Webex アプリとデバイスは Webex ミーティングに Video Mesh ノードを使用しません。

手順

ステップ 1 https://admin.webex.com のカスタマービューで、**[サービス（Services）]** > **[ミーティング（Meetings）]** に移動し、ミーティングカードで Webex サイトをクリックし、**[設定（Settings）]** ⚙ をクリックすると 、Webex サイト設定オプションにアクセスできます。

ステップ 2 **[共通設定（Common Settings）]** にアクセスするには、**[サービス（Service）]** > **[ミーティング（Meeting）]** > 、**[サイト設定（Site Settings）]** の順にクリックします。**[共通設定（Common Settings）]** から、**[Cloud Collaboration Meeting Rooms（CMR）]** をクリックして、**[メディアリソースの種類（Media Resource Type）]** で **[Video Mesh]** を選択し、下部にある **[保存（Save）]** をクリックします。



この設定によって、クラウドで Video Mesh およびミーティングインスタンスが一緒にリンクされ、カスケードが Video Mesh ノードで発生できるようになります。この設定は、15 分後に

環境全体に反映されます。 この変更が反映された後に開始される Webex ミーティングでは、新しい設定が適用されます。このフィールドをデフォルトのオプションである [クラウド（Cloud）] に設定したままにすると、クラウドでホストされているすべてのミーティングおよび Video Mesh ノードは使用されなくなります。

Webex アプリ ユーザーへの Collaboration Meeting Rooms の割り当て

手順

- Control Hub を使用してサイトを管理する場合は、次のようにします。
  a) https://admin.webex.com のカスタマー ビューから、**[ユーザー（Users）] > [ユーザーの管理（Manage Users）]** に移動します。

     複数のユーザーをまとめて割り当てるには、この文書を参照してください。

  b) **Webex Collaboration Meeting Rooms** を組織内のユーザーに割り当てます。
- サイト管理者を使用してサイトを管理する場合は、次のようになります。
  a) [サイト管理（Site Admin）] から、**[ユーザーの管理（Manage Users）]** に移動します。
  b) ユーザーアカウントを編集し、Collaboration Meeting Room をオンにします。

     複数のユーザーをまとめて割り当てるには、この文書を参照してください。

セキュアなエンドポイントでのミーティングエクスペリエンスの確認

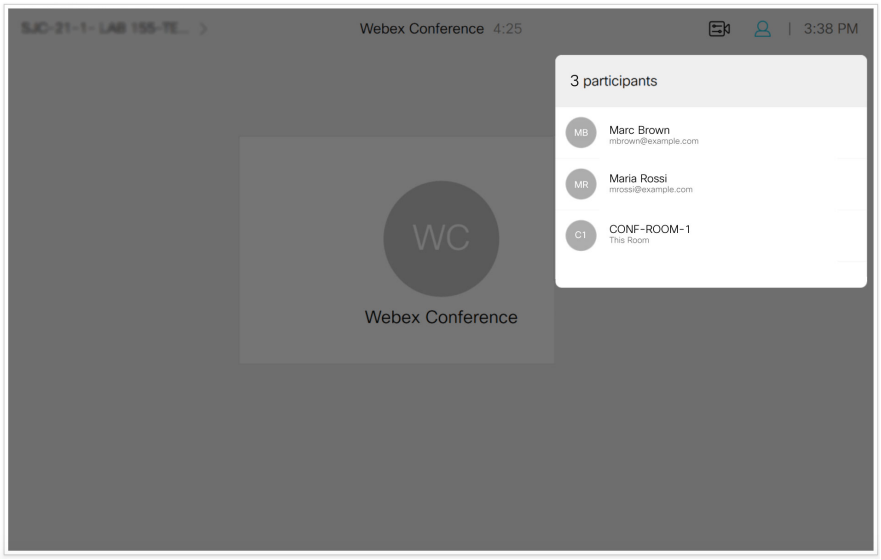
エンドポイントが安全に登録され、正しいミーティングエクスペリエンスが表示されていることを確認するには、以下の手順を実行します。

手順

ステップ 1 セキュリティ保護されたエンドポイントからミーティングに参加します。

ステップ 2 ミーティングの名簿がデバイスに表示されることを確認します。

この例は、タッチパネルを使用するエンドポイントでミーティングリストがどう見えるかを示しています。



ステップ 3 ミーティング中、**[コールの詳細（Call Details）]** から Webex Conference の情報にアクセスします。

ステップ 4 [暗号化（Encryption）] セクションで、**[タイプ（Type）]** が **[AES-128]** として表示され、**[ステータス（Status）]** が **[オン（On）]** として表示されていることを確認します。

Webex Conference

Participant(s)			Encryption	
URL	[redacted]		Type	AES-128
Call rate	6000 kbps		Status	On

Video	Transmit	Presentation	Receive	Presentation
Protocol	H264	N/A	H264	N/A
Resolution	1280x720	N/A	1280x720	N/A
Frame rate	30 fps	N/A	30 fps	N/A
Channel rate	2484 kbps	N/A	759 kbps	N/A
Total packet loss (%)	0.0%		0.0%	
Current packet loss (...	0.0%		0.0%	
Jitter	1 ms		3 ms	

Audio	Transmit	Receive
Protocol	AACLD	Opus
Channel rate	63 kbps	64 kbps
Total packet loss (%)	0.0%	0.0%
Current packet loss (...	0.0%	0.0%
Jitter	1.00 ms	4.00 ms

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。