Cisco Meeting Management

リリース 3.9

インストール/コンフィギュレーション ガイド

2024 年 3 月 5 日

目次

マニュアルの変更履歴

表 1 : マニュアルの変更履歴

日付	説明
2024- 03- 05	ドキュメントを公開。

1 はじめに

このガイドは、Cisco Meeting Management の管理者向けで、Cisco Meeting Management のインストールと設定方法を説明しています。

Cisco Meeting Management は、シスコのオンプレミスのビデオ会議プラットフォーム Cisco Meeting Server 用の管理ツールです。ライセンスを管理し、Meeting Server に対して使いやすいインターフェイスを提供します。

Meeting Management の管理者は、次の操作を実行できます。

- Meeting Management のインストールと設定
- Meeting Server のライセンス設定の編集
- Meeting Server 上でのスペーステンプレートと Web アプリのユーザのプロビジョニング
- スペースの作成と管理設定および短縮ダイヤルの構成
- ビデオオペレータとしての機能

ビデオオペレータは、次の操作を実行できます。

- アクティブな会議と、1 週間以内に終了した会議のすべての表示
- Cisco TMS（TelePresence Management Suite）を使用して予定されているミーティングの表示
- アクティブな会議の管理
- Meeting Server の現在のライセンスステータスの確認

Cisco Meeting Management 3.0 以降は Meeting Server 3.0 以降では必須であり、追加のライセンスは必要ではありません。

2 3.9 の新機能

新機能と変更の概要については、リリースノートを参照してください。

2.1 このガイドの 3.8 以降の変更

- Meeting Management VM のハイパーバイザの要件が更新されました。
- 一般的に使用される単語、繰り返しまたは連続する文字を含むディクショナリを基に、パスフレーズ検証を使用して、ユーザーパスワードの品質をチェックする手順を追加しました。

3 ご使用になる前に

開始する前に、環境が Meeting Management の要件を満たしていることを確認する必要があります。また、ネットワーク設定の詳細など、いくつかの情報を準備する必要があります。

Meeting Management は、単一の Call Bridge から複数のクラスタ展開まで、何でも管理できます。VM の要件は、展開サイズによって異なります。展開サイズを決定するには、以下のキャパシティの表を参照してください。

3.1 キャパシティ

	小規模から中規模の展開	大規模な展開
Call Bridge	Cisco Meeting Server 1000 で 1 ～ 8 件の Call Bridge を実行 **または** Cisco Meeting Server 2000 で 1 件の Call Bridge を実行	Cisco Meeting Server 1000 で 9 ～ 24 件の Call Bridge を実行 **または** Cisco Meeting Server 2000 で 2 ～ 3 件の Call Bridge を実行
開始したコールレッグ数（ピーク時にすべての Call Bridge を横断）	1 秒あたり 10 件のコールレッグを開始	1 秒あたり 20 件のコールレッグを開始
Meeting Management に同時にログインしたユーザ数	15 人の同時ユーザ	25 人の同時ユーザ
1 週間のミーティング数（すべての Call Bridge を横断）	10,000	10,000

注：リストされている Call Bridge 数は、予想されるコール量に基づいています。接続されているクラスタすべてが Meeting Management 機能を無効にしている場合、小規模な展開環境の VM の要件は、どの展開サイズでも十分です。

3.2 Meeting Management VM の要件

VM 環境が、展開サイズに必要な仕様を提供できるかを確認します。

要件	中小規模の環境	大規模な展開
サーバのメーカー	すべて	すべて
プロセッサ タイプ	Intel / AMD	Intel / AMD
プロセッサの周波数	2.0 GHz	2.0 GHz
vCPU	4 コア	8 コア
ストレージ	100 GB *シックプロビジョニングとイーガーゼロ化を推奨します。*	100 GB *シックプロビジョニングとイーガーゼロ化を推奨します。*
RAM	4 GB の予約済みメモリ	8 GB の予約済みメモリ
ハイパーバイザ	ESXi 7.0 U3o	ESXi 7.0 U3o
ネットワーク インターフェイス	1	1

注：VM は、中小規模の環境用に設定されています。大規模な環境の場合は、セットアップ中にサイジングを手動で変更する必要があります。

注：中規模の環境で、後でキャパシティを大きくする必要がある可能性がある場合は、大規模な環境用に VM を設定します。

3.3 復元力

Meeting Management 展開に復元力を追加するには、最大 2 つの Meeting Management インスタンスを同じ Meeting Server 展開に接続できます。

Meeting Management のインスタンスを 1 つまたは 2 つセットアップするか決定します。これらは個別に設定する必要があります。各インスタンスは、接続されている Call Bridge および TMS から情報を直接取得します。Call Bridge と TMS 間で情報は交換されません。Meeting Management の 2 つのインスタンスを異なる場所に配置することを推奨します。停電や接続の問題など、両方のインスタンスが同時に影響を与える可能性があります。

また、Meeting Management の適切なインスタンスにユーザーを指示する方法を決定します。

次のオプションがあります。

a. **ユーザーは特定のインスタンスに手動でサインインします。**各インスタンスのアドレス（FQDN）を定義して、ユーザにサインインを求めます。問題が発生した場合は、他のインスタンスにサインインして、管理者に通知する必要があります。

b. **ユーザートラフィックがリダイレクトされます。**各インスタンスのアドレス（FQDN）を定義するのに加えて、ユーザが使用する 3 つ目のアドレスを作成して、1 つのインスタンスにリダイレクトします。ユーザには、常にユーザが使用するアドレスにサインインするよう求めます。問題がある場合は、管理者がリダイレクトを変更する必要があります。

注：ユーザがいつも 1 つのアドレスを使用している場合でも、Meeting Management の各インスタンスには固有の CDR 受信者アドレスが必要です。

注：Meeting Management の各インスタンスに対して証明書を作成することを推奨します。各証明書には、ユーザが使用しているアドレスと、固有の CDR 受信者アドレスの両方を含める必要があります。「Meeting Management の証明書」を参照してください。

3.4 ネットワークの詳細、CDR 受信者、および NTP

ネットワーク上で Meeting Management をセットアップする前に、次の詳細を知る必要があります（端末の設定）。

- Meeting Management のホスト名
- IPv4 または IPv6 アドレス

  手動で入力するか、[DHCP/SLAAC] を選択できます
- デフォルトゲートウェイ（DHCP/SLAAC を使用しない場合）
- 必要に応じて、1 DNS サーバーの IP アドレス

その他の詳細は、初回のセットアップの完了時に追加できます。

- CDR 受信者アドレス

  CDR 受信者アドレスは、Meeting Management が、CDR（コール詳細レコード）を送信するために Call Bridge に通知する FQDN です。Meeting Management に会議の情報を表示するには、CDR 受信者アドレスを正しく設定する必要があります。

注：Meeting Management の DNS レコードがセットアップされていないことを確認します。また、Call Bridge 用にファイアウォールが開いていて、CDR 受信者アドレスとして Meeting Management に設定した FQDN に到達できるか確認します。

注：すべてのクラスタの Meeting Management を無効にした場合は、CDR 受信者アドレ

スは不要ですが、Meeting Management にはエラー通知が表示されます。

- 最大 5 つの NTP サーバーの IP または FQDN、および対応する NTPv3 対称キー

  Meeting Management には、接続されている Call Bridge および TMS サーバに使用するのと同じ NTP サーバを使用することを推奨します。

- オプション：追加の DNS サーバーの IP

3.5 ユーザ

Meeting Management は、LDAP を介したローカル管理ユーザおよびユーザ認証をサポートしています。ローカルユーザのみ、LDAP ユーザのみ、または両方を選択できます。

- **[ローカルユーザー（Local users）] は Meeting Management の** [ユーザー（Users）] **ページでローカルで追加および管理されます。** これらのユーザは、Meeting Management によって直接認証されます。

  インストール中に 1 人のローカル管理者ユーザが生成され、初めてサインインした後にさらにユーザを追加できます。ローカルユーザは、セットアップとテストを行い、Meeting Management からロックアウトされなくても LDAP を変更する場合に役立ちます。

- **LDAP ユーザ** は、LDAP サーバ上の既存のグループへのマッピングを介して追加されます。Meeting Management は、LDAP サーバを使用して、サインイン時にグループメンバーシップを確認することで、これらのユーザを認証します。

  LDAP を介した認証は、一般的な使用と管理に推奨されています。

少なくとも 1 つのローカル管理者ユーザアカウントを登録することを推奨します。LDAP に問題がある場合でも Meeting Management にアクセスできるようにするためです。実稼働で一般的に使用する場合は、ユーザは LDAP 経由で認証することを推奨します。

注：実稼働環境では LDAP を使用することを推奨しているため、LDAP が設定されていない場合は、Meeting Management に常に警告が表示されます。

ユーザは、次の 2 つの役割を担います。

- **管理者は Meeting Management に完全にアクセスできます。** 通常、管理者は Meeting Management を設定し、構成を変更し、ユーザを追加し、システムを監視および保守します。管理者は、ビデオオペレータを特定のスペースにタグ付けして、それらのスペースに関連付けられた会議にのみアクセスできるようにすることができます。

- **ビデオオペレータは、[会議（Meetings）] および [概要（Overview）] ページにのみアクセスできます。** ビデオオペレータは、会議をモニタリングおよび管理し、進行中の会議に関する基本的なトラブルシューティングを実行します。たとえば、切断された参加者に電話をしたり、音声に問題がある場合は通話統計を確認することができます。ビデオオペレータには、管理者によって割り当てられたスペースで開催されるミーティングに関連するタスクを実行する権限があります。

ローカルユーザの場合、ロールはユーザプロファイルに割り当てられます。

LDAP ユーザーの場合、ロールは属する LDAP グループに割り当てられます。1 人のユーザが異なるロールを持つ複数のグループに含まれる場合、そのユーザに管理者ロールが割り当てられます。

3.6 LDAP 経由のユーザーアクセス

Meeting Management の一般的な使用と管理については、LDAP 経由でユーザーを認証することを推奨します。そのため、必要な LDAP グループを使用して LDAP サーバーを設定する必要があります。管理者用に少なくとも 1 つのグループとビデオオペレータ用のグループを作成することを推奨します。

注：Meeting Management は、ネストグループをサポートしていません。マップされたグループに他のグループが含まれている場合、ネストグループのメンバーは Meeting Management にアクセスできません。

サポートされている LDAP 実装は次のとおりです。

- Microsoft Active Directory（AD）
- OpenLDAP

  注：OpenLDAP に対して memberOf のオーバーレイを有効にする必要があります

LDAP サーバーに接続するには、次の手順が必要です。

- プロトコル（LDAP/ LDAPS）
- LDAP サーバーアドレス
- LDAP サーバーポート番号
- LDAP サーバー証明書（LDAPS 証明書の要件

  を使用している場合）

  - *証明書チェーンには、証明書に署名した CA の証明書に加えて、ルート CA 証明書を含む証明書チェーン内の上位の証明書を含める必要があります。*
  - *LDAP サーバーのアドレスを証明書に含める必要があります。*
- LDAP バインドユーザーのログイン情報

  セキュリティと監査上の理由から、Meeting Management 用に、個別のバインドユーザーアカウントを作成することを推奨します。
- 基本識別名（DN）
- 属性の検索

  これは、ユーザがサインインするときにユーザー名として入力する LDAP 属性です。

グループを追加するには、次の情報が必要です。

- 各グループの識別名

3.7 ローカルユーザーアクセス

LDAP の設定に問題がある場合でもサインインを行えるよう、少なくとも 1 人のローカル管理者ユーザーを配置することを推奨します。また、テスト目的や LDAP 設定の変更に対してローカルユーザを使用できます。

注：実稼働で一般的に使用する場合は、管理者とビデオオペレータの両方を含むすべてのユーザを LDAP 経由で認証することを推奨します。

インストール中に、Meeting Management はローカル管理者のユーザアカウントを作成し、Web インターフェイスにサインインして設定を完了できます。ネットワーク上で Meeting Management を設定している場合、ユーザ名と生成されたパスワードが VM コンソールに表示されます。

注：Web インターフェイスに初めてサインインすると、生成されたログイン情報は Meeting Management を初めて再起動するまでコンソールにのみ表示されます。サインイン後すぐにパスワードを変更することを推奨します。

より多くのローカルユーザを設定するには、次の手順が必要です。

- 各ユーザのユーザー名

  注：ユーザープロファイルを保存した後は、ユーザー名を変更できません。

- オプション：各ユーザの名
- オプション：各ユーザの姓
- 各ユーザのロール
- 必要に応じて、各ユーザのパスワード

  パスワードを自分で定義する代わりに、組み込みのパスフレーズ生成機能の使用を選択できます。

  ユーザはサインイン後にパスワードを変更できます。

3.8 ローカルユーザーのセキュリティポリシー設定

ローカルユーザーに対して以下のセキュリティポリシーを設定できます。

- 最小パスワード長が必要

  これは、選択するまで無効になります。デフォルトの最小長は 8 文字です

- 組み込みのパスフレーズ生成機能を有効にする

  組み込みのパスフレーズ生成機能は、ディクショナリの単語を組み合わせ、新しいパスワードを提案します。パスフレーズ内のデフォルトの単語数は 5 で、1 ~ 8 の任意の数を選択できます。

  組み込みのパスフレーズ生成機能を使用する場合は、ディクショナリを提供する必要があります。ディクショナリの要件：

  - *ディクショナリは、各行に 1 つの単語を含むテキストファイルである必要があります。*
  - *文字は UTF-8 でエンコードされている必要があります。*
  - *ファイルに Null 文字を含めることはできません。*
  - *ファイルの最大サイズは 10 MB です。*

- パスワードの再使用を制限する

  これは、選択するまで無効になります。入力フィールドは、値を入力するまで空白です。

3.9 サポートされるブラウザ

Cisco Meeting Management は、以下のブラウザの最新リリースバージョンでサポートされています。

- Microsoft Internet Explorer
- Microsoft Edge
- Google Chrome
- Mozilla Firefox
- Safari

次のテクノロジーを有効にする必要があります。

- WebSocket
- HTML5
- JavaScript

注：Internet Explorer では更新は強制されませんので、最新バージョンを手動で確認することをお勧めします。

3.10 システムログサーバー

Meeting Management でのログの保存は制限されています。ただし、syslog レコードはリモートロケーションに送信できます。システムログを収集するために、最大 5 つの外部 syslog サーバーを設定できます。

外部システムログサーバーを設定することを強く推奨します。トラブルシューティングとサポートにはシステムログが必要です。

ログサーバーを Meeting Management に接続するには、次の情報が必要です。

- サーバーアドレスとポート番号
- プロトコル（UDP/ TCP/ TLS）
- TLS を使用している場合、証明書

注：TLS 接続は TLS 1.2 をサポートする必要があります

注：すべてのメッセージを全長で表示する場合は、最大 8192 バイトのメッセージを受信および表示できるシステムログサーバを使用する必要があります。

3.11 監査ログサーバー

サインイン、Meeting Management の設定の変更、ビデオオペレータのアクションの実行など、Meeting Management でのユーザのアクションに関する情報が監査ログに記録されます。

Meeting Management ではログの保存が制限されています。ローカルに保存されている監査ログは、ローカルのシステムログでのみ使用できます。ただし、別個の監査ログを syslog レコードとしてリモートの場所に送信することもできます。監査ログを収集するために、最大 5 つの外部 syslog サーバを設定できます。

監査ログサーバはオプションですが、組織内で必要になる場合があります。

ログサーバーを Meeting Management に接続するには、次の情報が必要です。

- サーバーアドレスとポート番号
- プロトコル（UDP/ TCP/ TLS）
- TLS を使用している場合、証明書

注：TLS 接続は TLS 1.2 をサポートする必要があります

注：すべてのメッセージを全長で表示する場合は、最大 8192 バイトのメッセージを受信および表示できるシステムログサーバを使用する必要があります。

syslog サーバー固有のハードウェアまたは VM の要件は、Meeting Server の展開と Meeting Management の使用状況によって異なります。

3.12 Meeting Server のライセンス

Meeting Server はライセンス用の Meeting Management に依存しています。Meeting Server 3.0 以降では Meeting Management が必須です。

Meeting Management の各インスタンスに対して、スマートライセンスまたはライセンスなしを選択できます。

復元力のある展開の場合は、使用状況の二重レポートを避けるために、ライセンス用に Meeting Management のインスタンスを 1 回だけ使用します。インスタンスのライセンスモードをスマートライセンスに設定し、もう 1 つのインスタンスにはライセンスなしを設定します。

注：すべての Meeting Server クラスタは、ライセンスが有効な Meeting Management インスタンスに接続している必要があります。Meeting Management の 1 つのインスタンスのライセンスは、復元力のある展開の場合で、もう 1 つの Meeting Management のライセンスが有効になっている場合にのみ無効にしてください。

スマートライセンスでは、次の情報が必要です。

- Meeting Management の 1 つのインスタンスだけで使用する専用のバーチャルアカウントを持つ企業のスマートアカウントが必要です。

  アカウントを要求するには、シスコのアカウントチームに問い合せるか、Cisco Software Central に移動します。

- Meeting Management で使用する適切なライセンスをバーチャルアカウントに割り当てる必要があります。

  1 つのバーチャル アカウントを Meeting Management の 1 つのインスタンスに接続できます。また、1 つのバーチャルアカウントのすべてのライセンスは、Meeting Management で接続されているすべてのクラスタ間で共有されます。

  クラスタを個別にライセンスする場合は、クラスタを別の Meeting Management 展開とバーチャルアカウントに接続します。

- Cisco Smart Software Manager に直接接続できるかどうか、またはプロキシが必要かどうかを判断する必要があります。独自のプロキシサーバーを使用するか、Cisco Transport Gateway を使用できます。

  プロキシサーバーを使用している場合は、[トランスポート設定の編集（Edit Transport Settings）] ができるよう、アドレス、ポート番号、および証明書を利用可能にする必要があります。

- オプション：純粋なオンプレミスの環境では、特定の時間にのみ接続してデータを交換する Cisco Smart Software Manager オンプレミス（SSM オンプレミス）を使用できます。Meeting Management は、バージョン 8- 202008 以降をサポートしています。

  注：Cisco Smart Software Manager オンプレミス に接続しようとして Meeting Management の承認を拒否する場合は、SSM オンプレミスにログインして 、**Active Call Bridge Node** ライセンスによって認証が失敗するかどうかを確認します。はいの場合、スマートアカウントに SSM オンプレミス で再同期すると、問題は修正されます。

  Smart Software Manager オンプレミス（サテライト）を使用している場合は、[トランスポート設定の編集（Edit Transport Settings）] ができるよう、アドレス、ポート番号、および証明書を利用可能にする必要があります。ゲートウェイアドレスには、http:// の形式を使用します。 <SSM onprem address>/ SmartTransport または https:// <SSM onprem address>/ SmartTransport は設定に依存します。

3.13 Meeting Management の証明書

Meeting Management は、証明書を使用してブラウザと Call Bridge に対して自己識別します。

設定中に Meeting Management は自己署名証明書を生成し、初期構成時に使用できます。実稼働環境では、自己署名証明書を CA（認証局）によって署名された証明書に置き換える必要があります。組織内の要件に応じて、内部または外部 CA を使用できます。

証明書の要件：

- 証明書チェーンには、証明書に署名した CA の証明書に加えて、ルート CA 証明書を含む証明書チェーン内の上位の証明書を含める必要があります。
- CDR 受信者アドレスと、ユーザがブラウザインターフェイスで使用するアドレスは、証明書に記入される必要があります。より多くのアドレスが必要な場合は、証明書の SAN（サブジェクト代替名）フィールドを使用できます。

  注：SAN フィールドを使用する場合、Meeting Management では共通名は確認されません。SAN フィールドに、CDR 受信者アドレスを含める必要があります。

注：Meeting Management には、証明書署名要求を作成する機能はありません。OpenSSL ツールキットなどの専用ツールを使用して、秘密キーと証明書署名要求を作成します。

注：Meeting Management のインスタンスを 2 つ設定する場合は、各インスタンスに証明書を用意することを推奨します

3.14 Call Bridge またはクラスタの前提条件

Meeting Management をインストールして設定する前に、展開が次の前提条件を満たしていることを確認します。

- **Meeting Server API のユーザーアカウント**。Meeting Management は、API を介して Cisco Meeting Server に接続します。セキュリティと監査上の理由から、Meeting Management 用に、個別のアカウントを設定することを推奨します。複数のインスタンスを使用している場合は、Meeting Management の各インスタンスに対して個別のアカウントが必要です。

  アカウントの設定方法については、『Cisco Meeting Server API リファレンスガイド』の「API へのアクセス」を参照してください。これは、cisco.com の『プログラミングガイド』のページにあります。

- **CDR キャパシティ。ミーティング アクティビティに関する情報を取得するため、Meeting Management は各 Call Bridge の場合に、それ自体が CDR（コール詳細レコード）の受信者として設定されます。**Call Bridge が Meeting Management の各インスタンスに適したキャパシティを確保できるようにします。

  注：クラスタのライセンスとプロビジョニングにのみ Meeting Management を使用する場合は、そのクラスタの Call Bridge の CDR キャパシティは不要です。

- **NTP サーバ**。Call Bridge と Meeting Management が同期されていることを確認するために、展開内の Meeting Server ごとにタイムサーバーを設定する必要があります。Meeting Management と Meeting Server の展開には、同じ NTP サーバを使用することを推奨します。NTP サーバのキーも必要な場合があります。
- **オプション：レコーダー**。Meeting Management を使用して録音を開始および停止する場合は、展開内の Meeting Server でレコーダーを設定する必要があります。
- **オプション：ストリーマ**。Meeting Management を使用してストリーミングを開始および停止する場合は、展開内の Meeting Server でストリーマを設定する必要があります。
- **オプション：参加者を移動するために必要な設定です**。会議間で参加者を移動する場合は、Meeting Server 展開で特定の要件があります。特に、SIP エンドポイントを使用している参加者は、Cisco Expressway を介してプロビジョニングされている場合は移動できません。また、Meeting Server で負荷分散を設定する必要があります。

  詳細については、*『Cisco Meeting Server 管理者クイックリファレンスガイド：API を使用した会議間で参加者を移動する』*の「参加者を移動する際の制限事項」を参照してください

Meeting Management を設定する際、Call Bridge ごとに次の情報が必要です。

- Web 管理インターフェイスの IP アドレスまたは FQDN
- Web 管理インターフェイスのポート番号
- Meeting Management で使用するために設定した API ユーザアカウントのユーザ名とパスワード
- 検証の際に信頼された証明書を使用する場合は、Web 管理インターフェイスの CA 証明書が必要です。

注：MMP コマンド「shutdown」を使用して VM をシャットダウンする必要があります。これにより、Meeting Server は、ミーティングおよび Meeting Management の参加者を含む、接続されているすべてのデバイスに適切な切断メッセージを送信します。

アクティブなミーティング中に Meeting Server VM が突然オフまたはシャットダウンされた場合、参加者は切断されますが、参加者は接続されているように見えます。
[音声/ビデオのミュート（Audio/ Video Mute）] ボタンは、Meeting Server への接続が復元されるまでロード状態のままになります。

3.15 サポートされている Cisco Meeting Server バージョン

Meeting Server のバージョンが Meeting Management でサポートされていることを確認します。Meeting Management 3.7 は、Cisco Meeting Server バージョン 3.7 でのみサポートされます。

3.16 サポートされている TMS バージョン

推奨	最小
15.10 以降	15.9 以降

3.17 TMS 前提条件

Meeting Management をインストールして設定する前に、展開が次の要件を満たしていることを確認します。

- **TMS に接続されている Call Bridge**。すべての Meeting Server クラスタが TMS に接続されている必要があります。

  手順については、『Cisco Meeting Server（Acano）/TMS 統合およびスケジュール設定 API ガイド』を参照してください。Cisco Meeting Server マニュアルページの「設定例およびテクニカルノート」で確認できます。

- **サイト管理者のユーザアカウント**。セキュリティ、トラブルシューティング、監査上の理由から、Meeting Management 用に、個別のアカウントを設定することを推奨します。Meeting Management のインスタンスを複数使用している場合は、それぞれのインスタンスに対して別個のアカウントを作成します。

  手順については、TMS API のマニュアル、『Cisco TelePresence Management Suite Extension Booking API プログラミング リファレンス ガイド』を参照してください。

  注：同じアカウントを使用して、TMS の電話帳にアクセスし、スケジュールされたミーティングの情報を取得します。

- **NTP サーバ**。Call Bridge と TMS サーバが同期されていることを確認するために、TMS サーバのタイムサーバを設定する必要があります。Meeting Management と TMS には同じ NTP サーバーを使用することを推奨します。
- **オプション：自動 MCU フェールオーバーを無効にする。**失敗した場合は、**自動 MCU フェールオーバー**によって、スケジュールされたミーティングが TMS 内の 1 つのシステムから別のシステムに移動します。これは、Meeting Server 展開によって異なる場合がありますが、MCU など、別のタイプのシステムである場合があります。

  そのため、ミーティングは Meeting Management にスケジュールされた通りに表示される場合がありますが、アクティブになることは決してありません。また、ビデオオペレータは Meeting Management を使用してミーティングをモニタしたり管理したりできません。

  手順については、TMS のオンラインヘルプを参照してください。
- **オプション：TMS および Meeting Management 内のクラスタに対して同じ名前を使用します**。管理者の場合、Meeting Management のクラスタ表示名として使用するのと同じ名前を Meeting Server 展開の TMS で使用すると便利です。オペレータの場合、Meeting Management のプライマリ Call Bridge の名前を、TMS の Meeting Server 展開の名前に簡単に関連付けられると便利です。
- **オプション：サポートされているプロトコルを使用する電話帳の連絡先。**Meeting Management で TMS の電話帳を使用する場合は、Meeting Management に割り当てる電話帳のすべての連絡先が、Meeting Server からアクセスできるようにする必要があります。

Meeting Management から TMS に接続するために、追加の TMS ライセンスは必要ありません。

注意：Meeting Management が TMS に統合され、多数のスケジュール済みミーティングがある場合、TMS でパフォーマンスの問題が発生する可能性があります。たとえば、通知電子メールが遅れるか、ミーティングが若干遅く始まる可能性があります。

この影響は、1 週間にスケジュールを設定するミーティングの数と手動で同期する頻度、および TMS とその SQL データベースサーバーのサイジングによって異なります。

TMS を Meeting Management に接続する場合は、次の情報が必要です。

- TMS booking API サーバーの IP アドレスまたは FQDN
- 必要に応じて、TMS の CA 証明書
- TMS の Meeting Management に設定したサイト管理者ユーザーアカウントのログイン情報

Cisco Meeting Server の展開ごとに、TMS から次の情報が必要です。

- **TMS システム ID**：TMS が接続されている Cisco Meeting Server 展開に割り当てる識別子。

  *TMS システム ID を確認するには、次の手順を実行します。 TMS で展開に移動し、その **[設定（Settings）]** タブ、**[ビュー設定（View Settings）]**、**[全般（General）]** エリアに移動します。*
- **プライマリ Call Bridge**：TMS が接続するクラスタ内の Call Bridge。

  *どの Call Bridge に TMS が接続されているのかを確認するには、展開に移動して **[設定（Settings）]** タブに移動し、**[設定の表示（View Settings）]**、**[全般（General）]** エリアに移動します。**ネットワークアドレス**は、接続されている Call Bridge の IP アドレスです。*

3.18 ポート情報

表 2：Meeting Management からの発信通信用のポート

目的	プロトコル	宛先のポート
Syslog	TCP、UDP	514（または設定先）
Syslog	TLS	6514（または設定先）
LDAP	LDAP	389（または設定先）
LDAP	LDAPS	636（または設定先）
LDAP グローバルカタログ（基本 DN が DC レベルにのみ指定されている場合）	LDAP	3268（または設定先）
LDAP グローバルカタログ（基本 DN が DC レベルにのみ指定されている場合）	LDAPS	3269（または設定先）
同期時刻（NTP）	UDP	123
名前解決（DNS）	UDP	53
TMS 予約 API	HTTP	80
TMS 予約 API	HTTPS	443
証明書配布ポイント	HTTP	80
スマート ライセンシング ダイレクト	HTTPS	443
自分のプロキシ経由のスマートライセンス	HTTPS	443（または設定先）
Cisco Transport Gateway	HTTPS	443
Webex クラウドと Control Hub	HTTPS	443（または設定先）

表 3：Meeting Management への着信通信用のポート

目的	プロトコル	宛先のポート
Web インターフェイス	HTTPS	443

表 4：Meeting Management への着信通信と発信通信の両方のポート

目的	プロトコル	宛先のポート
Cisco Meeting Server API Cisco Meeting Server CDR Meeting Server のイベント	HTTPS	443（またはMeeting Server の MMP の設定先）

4 初回セットアップの概要

Meeting Management の設定を開始する前に、「ご使用になる前に」を参照して、準備ができていることを確認してください。

Meeting Management は、Cisco Meeting Server サポート契約を cisco.com すべての顧客に対する OVA ファイルとして使用できます。

初回のセットアップ中は、次の手順を実行します。

1. OVA を展開します。
2. ネットワーク上で Meeting Management を設定します。
3. 生成されたログイン情報でサインインし、パスワードを変更します。
4. 設定を編集します。
    a. ネットワーク設定を編集します。
    b. 証明書をアップロードします。
    c. CDR 受信者アドレスを入力します。
    d. オプション：TMS に接続します。
    e. NTP サーバーを追加します。
    f. オプション：サインインメッセージを追加する。
    g. オプション：高度なセキュリティ設定を構成します。
5. ログサーバを追加します。
6. Meeting Management を再起動して、Call Bridge を追加する前に CDR 受信者アドレスと、オプションで TMS の詳細情報を保存します。
7. Call Bridge を追加します。
    a. 既存の Meeting Server を追加する
    b. 新しい Meeting Server を構成して追加する
8. ライセンスモードを選択します
9. オプション：クラスタを TMS に関連付ける
10. オプション：TMS 電話帳にアクセス。
11. ユーザを追加するには、以下を行います。
    a. LDAP サーバーの詳細をセットアップします。
    b. LDAP グループを追加します。
    c. オプション：ローカルユーザのセキュリティポリシーを設定

d. オプション：ローカルユーザを追加

12. Meeting Management を再起動すると、すべての設定が保存されます。
13. バックアップを作成します。

5 OVA の展開

注：vCenter サーバーリリースが 6.5.0b 未満の場合は、HTML5 クライアントでは[OVF テンプレートの展開（Deploy OVF Template）] を利用できません。この場合、この手順には Flash クライアントを使用する必要があります。

注：手順は、Flash クライアントに基づいています。vSphere クライアントは、以下に説明する内容と若干異なる場合があります。

OVA を導入するには、次の手順を実行します。

1. VMware 環境にサインインします。
2. **[アクション（Actions）] > [OVF テンプレートの展開（Deploy OVF Template…）] の順に選択します。**
3. **[ローカルファイル（Local file）]** を選択し、cisco.com からダウンロードした OVA を参照します。
4. ウィザードを続行して、名前と場所、リソース、ストレージ、ネットワークの詳細を選択します。

   注：

   - IP 割り当ての設定が求められた場合は、空白のままにします。Meeting Management は独自の構成を持つため、この情報を使用しません。
   - OVA を vCenter にアップロードしてデプロイすると、[発行元（Publisher）] フィールドに [Trusted certificate（信頼できる証明書）] と表示されます。OVA のインポート時に、無効な証明書と信頼できない証明書に関する警告が表示される場合は、次の記事を参照してください。https://kb.vmware.com/s/article/84240. OVA への署名に使用された証明書に対応する中間証明書とルート証明書を VECS ストアに追加する必要がある場合があります。中間証明書またはルート証明書の取得、またはその他の問題については、シスコ テクニカルサポートにお問い合わせください。
5. VM のメモリが予約済みであることを確認してください。
   a. **[設定（Configure）]** タブに移動します。
   b. **[設定（Settings）]** ドロップダウンから、**[VM ハードウェア（VM Hardware）]** を選択します。
   c. **[編集（Edit）]** をクリックします。
   d. **[メモリ（Memory）]** タブで、**[すべてのゲストメモリを予約（すべてロック）（Reserve all**

guest memory (All locked)）] をオンにします。

6. 展開環境が大きい場合（キャパシティの表を参照）、VM のハードウェア設定を変更します。
    a. **[設定（Configure）]** タブに移動します。
    b. **[設定（Settings）]** ドロップダウンから、**[VM ハードウェア（VM Hardware）]** を選択します。
    c. **[編集（Edit）]** をクリックします。
    d. **[CPU]** を 4 から 8 に変更します。
    e. **[メモリ（Memory）]** を 4 GB から 8 GB に変更します。
7. 新しい Meeting Management VM が展開された後、電源をオンにします。

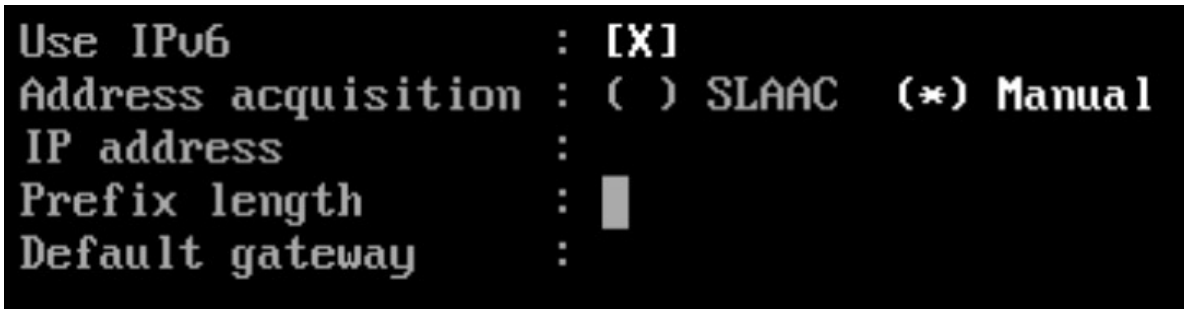
6 ネットワーク上で Meeting Management を設定します。

注：端末を介したネットワークのセットアップ中に、Meeting Management は入力が適切なフォーマットであるかを確認しますが、完全な検証は実行しません。入力した詳細を慎重に確認してください。

注：端末は米国のキーボードレイアウトを想定しています。特殊文字を入力する場合は、注意してください。たとえば、UK キーボードを使用している場合は、SHIFT+2 を押して @ と入力します。

ネットワーク上での Meeting Management を設定するには、次の手順を実行します。

1. 展開したばかりの VM のコンソールを開きます。
2. セットアップを入力するには、**[次へ（Next）]** を選択します。
3. Meeting Mangement のホスト名を入力します。
4. IPv4 を使用するかどうかを選択します。
5. **[DHCP]** または **[手動（Manual）]** アドレス取得のどちらを使用するかを選択します。
6. [手動（Manual）] を選択した場合は、[IP アドレス（IP address）]、[サブネットマスク（Subnet mask）]、および [デフォルトゲートウェイ（Default gateway）] を入力します。
7. IPv6 を使用するかどうかを選択します。
8. **[SLAAC]** または **[手動（Manual）]** アドレス取得のどちらを使うかを選択します。
9. SLAAC を使用しないことを選択した場合は、**[IP アドレス（IP address）]**、**[プレフィックス長（Prefix length）]**、および **[デフォルトゲートウェイ（Default gateway）] を入力します。**



注：IPv6 アドレスの角カッコは、これらのフィールドでは使用できません。

10. ネットワークで必要な場合は、DNS サーバーの IP アドレスを入力します。

このセットアップ中に追加できる DNS サーバーは 1 つのみですが、ブラウザインターフェイスから後でもう 1 つ追加できます。

注：IPv6 アドレスの角カッコは、このフィールドでは使用できません。

11. **[完了（Done）]** に移動し、Enter キーを押します。Meeting Management が開始するまで待ちます。

    コンソールには、1 つ以上の IP アドレス、生成されたログイン情報、および自己署名証明書用のフィンガープリントが表示されます。

    注：Meeting Management で Web インターフェイスにサインインする準備が整うまで数分かかる場合があります。

    注：Web インターフェイスに初めてサインインすると、生成されたログイン情報は Meeting Management を初めて再起動するまでコンソールにのみ表示されます。サインイン後すぐにパスワードを変更することを推奨します。

7 Web インターフェイスへのサインインとパスワードの変更

生成されたログイン情報を活用して Meeting Management にサインインします。サインインプロセス中に、パスワードを変更できます。

最初に表示される画面は、通知の概要ページです。構成を完了すると、最初にサインインするときに表示される通知は消えます。

注：**[同期された NTP ソースがありません（There are no synchronized NTP sources）]**の警告は、通常は表示されませんが、Meeting Management がデフォルトの NTP サーバーと同期されるまではしばらく表示される可能性があります

。

---

8 ネットワークの詳細の編集

基本的なネットワークの詳細はすでにセットアップ済みですが、DNS サーバを追加したり、構成を編集したりすることもできます。

ネットワーク設定を編集するには、次の手順を実行します。

1. [設定（Settings）] ページの [ネットワーク（Network）] タブに移動します。
2. 関連する詳細を入力します。

   注：IPv6 アドレスを入力する場合、ここに角カッコを使用しないでください。

3. 詳細を保存するには、Meeting Management を再起動します。

   注：今すぐ再起動するか、CDR 受信アドレスと TMS への接続の設定が完了するまで待ちます。

9 証明書のアップロード

自己署名証明書は、CA（認証局）によって署名された証明書に置き換える必要があります。

注：Meeting Management には、証明書署名要求を作成する機能はありません。OpenSSL ツールキットなどの別のツールを使用して、秘密キーと証明書署名要求を作成します。

証明書を置き換えるには、次の手順を実行します。

1. **[設定（Settings）] ページ の** [証明書（Certificate）] タブに移動します。
2. **自己署名証明書と置き換える証明書をアップロードします。**
3. **キーをアップロードします。**
4. **詳細を保存**し、Meeting Management を再起動します。

   注：今すぐ再起動するか、CDR 受信アドレスと TMS への接続の設定が完了するまで待ちます。

証明書の要件：

- *証明書チェーンには、証明書に署名した CA の証明書に加えて、ルート CA 証明書を含む証明書チェーン内の上位の証明書を含める必要があります。*
- *CDR 受信者アドレスと、ユーザがブラウザインターフェイスで使用するアドレスは、証明書に記入される必要があります。*

  注：SAN フィールドを使用する場合、Meeting Management では共通名は確認されません。SAN フィールドに、CDR 受信者アドレスを含める必要があります。

10 CDR 受信者アドレスの入力

CDR 受信者アドレスは、Meeting Management が、CDR（コール詳細レコード）を送信するために Call Bridge に通知するアドレスです。会議の情報を Meeting Management に表示するには、CDR 受信者アドレスが正しく設定されていることを確認することが非常に重要です。

注：IP アドレスが変更される可能性があるため、FQDN の使用を強く推奨します。[CDR 受信者アドレス（CDR Receiver address）] フィールドは、Meeting Management が Call Bridge に使用を指示する情報のみを構成し、Meeting Management がより広範なネットワークにどのように表示されるかは設定しません。解決可能で Call Bridge から到達可能なネットワークに設定されているアドレスを入力する必要があります。

CDR 受信者アドレスを入力するには、次の手順を実行します。

1. [設定（Settings）] ページの [CDR] **タブに移動し、CDR 受信者アドレス**を入力します。
2. **[保存（Save）]** をクリックして、Meeting Management を再起動します。

   注：今すぐ再起動するか、設定が完了するまで待ちます。

11 オプション：TMS への接続

スケジュールされたミーティングを開始する前に確認したり、参加者を追加したときに TMS の電話帳を使用して連絡先を検索したりするには、TMS を Meeting Management に接続する必要があります。

注：TMS に接続する前に、Call Bridge が TMS 予約 API に接続されている必要があります。詳細については、「ご使用になる前に」セクションを参照してください。

Meeting Management を TMS に接続するには、次の手順を実行します。

1. [設定（Settings）] ページの **[TMS]** タブに移動します。
2. **[Meeting Management で TMS を使用する（Use TMS with Meeting Management）]** チェックボックスをオンにします。
3. TMS サーバの IP アドレスまたは FQDN を入力します。
4. HTTP または HTTPS を選択します。
5. **オプション：証明書を**使用することを選択し、証明書が無効であり Meeting Management で接続を拒否する場合は、証明書失効リスト（**CRL**）に対して証明書**を確認します。**

   チェーン内の証明書が無効またはアクセスできない CRL がある場合、Meeting Management は接続をブロックします。

   可能な場合はこれを有効にすることを推奨します。

   注：HTTP 証明書配布ポイント（CDP）を備えた証明書のみがサポートされています。CRL チェックを使用し、証明書に CDP がない場合、または CDP が HTTP 経由で到達できない場合、接続は拒否されます。

   また、Meeting Management が HTTP 経由で外部アドレスに接続できるよう、ネットワークを構成する必要があります。

   ---

6. HTTPS を使用している場合は、TMS の証明書をアップロードします。

   証明書の要件は、次のとおりです。

   - *証明書はチェーンで、TMS 証明書に署名した CA の証明書に加えて、ルート CA 証明書を含む証明書チェーン内の上位の証明書を含める必要があります。*
   - *TMS サーバーに入力したサーバーアドレスは、TMS サーバ証明書に含める必要があります。*

     注：SAN フィールドを使用する場合、Meeting Management では共通名は確認されません。TMS FQDN を SAN フィールドに含める必要があります。

7. **TMS** に [ユーザー名（Username）] と [パスワード（Password）] を入力します。
8. 保存 して Meeting Management を再起動します。

注：クラスタを TMS に関連付ける前に、TMS から 情報を受信できません。

12 NTP サーバーの追加

Meeting Management が常に Meeting Server Call Bridge と同期することが重要ですので、Meeting Management では Meeting Server の展開と同じ NTP サーバを使用することを推奨します。Meeting Management には最大 5 つの NTP サーバーを接続できます。また、**[設定（Settings）] ページの** [NTP] タブでそれらのステータスをモニタリングできます。

注：表示される時間は Meeting Management サーバの時間であり、コンピュータの時刻設定と異なる場合があります。表示されるオフセットは、接続されている各 NTP サーバと Meeting Management サーバ間の値です。

NTP サーバーを追加するには、次の手順を実行します。

1. **[設定（Settings）]** ページの **[NTP]** タブに移動します。
2. **NTP サーバを追加します。**

   注：IPv6 アドレスを入力する場合、ここに角カッコを使用しないでください。

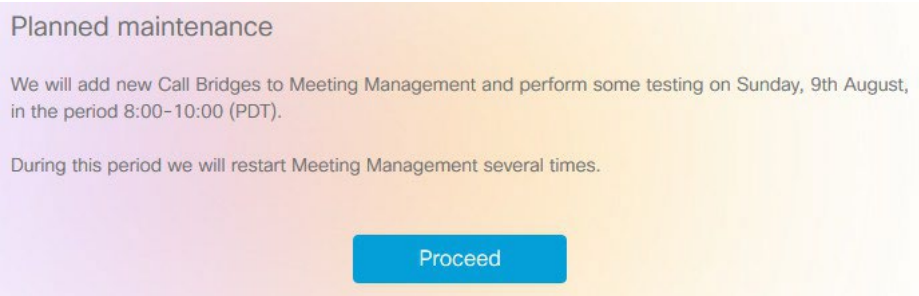
3. 変更を保存するには、Meeting Management を再起動します。

   注：今すぐ再起動するか、設定が完了するまで待ちます。

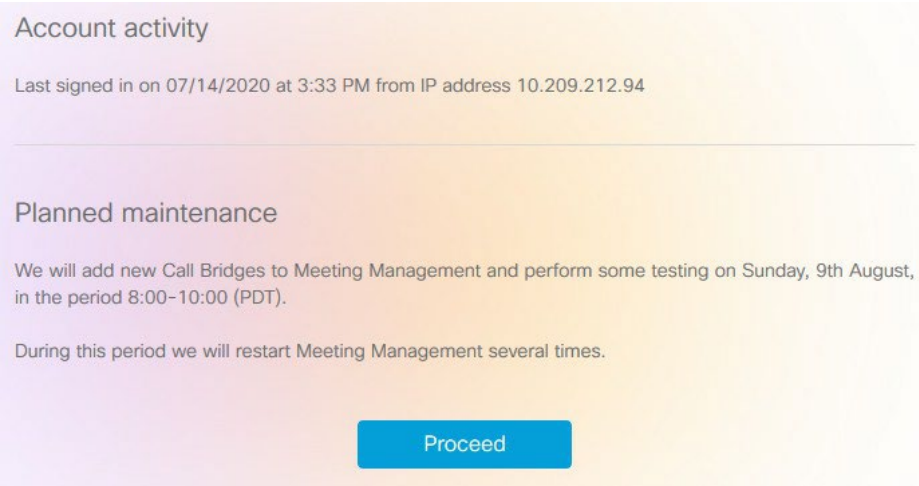
13 オプション：ユーザがログインするときに表示するメッセージの追加

サインインページの前または後にユーザーへのメッセージを含むページを挿入できます。たとえば、サインイン前のメッセージとして法的な警告や、サインイン後のメッセージとしてメンテナンスの予定を通知できます。

入力したメッセージがページに表示され、次の例のように **[続行（Proceed）]** ボタンが表示されます。



[サインイン後にアカウントアクティビティを表示する（Display account activity after sign-in）] チェックボックスをオンにすると、サインイン後にアカウントアクティビティが表示されます。以下のスクリーンショットは、アカウントアクティビティとサインイン後のメッセージの両方が表示される例を示しています。



注：変更はすぐに有効になります。

14 オプション：高度なセキュリティ設定を構成

[設定（Settings）] ページの [高度なセキュリティ（Advanced security）] タブで、高度なセキュリティ設定を構成できます。デフォルト設定では Meeting Management が機能し、安全な状態を維持します。ほとんどの環境に適しています。組織のローカル セキュリティ ポリシーで特定の設定が必要な場合にのみ、高度なセキュリティ設定を変更することを推奨します。

注：すべてのセキュリティ設定を適用するには、再起動が必要です。初回のセットアップの一環として高度なセキュリティ設定をセットアップした場合は、再起動する前に **[設定（Settings）]** ページと **[ログ（Logs）]** ページですべての構成を完了できます。

14.1 レート制限のサインイン試行

ユーザが一定の間隔でサインインを試行できる回数を制限できます。レート制限を有効にした場合、ここで構成されている設定は、LDAP ユーザとローカルユーザの両方に対して有効になります。

サインイン試行が許可された回数はトークンで測定されます。各ユーザは、定義したトークンの最大数で開始します。サインイン試行が失敗する度に 1 つのトークンを失い、再び利用可能なトークンの最大数になるまで、各間隔の最後に 1 つずつ取得します。

2 つの設定があります。

- **1 つのトークンがバケットに追加される速度（秒）**

  これは各間隔の長さ（秒）で測定されます。デフォルトは 300 秒です。

- **バケットに保持されているトークンの最大数**

  これは、指定された間隔内にユーザが許可できるサインイン試行の最大数です。デフォルトは 3 トークンです。

つまり、ユーザが最初の間隔のうちにすべてのトークンを使用した場合、2 番目の間隔のうちにサインインを試行できる回数は 1 回のみです。ユーザがすべてのトークンを使用した後にサインインしようとすると、次のメッセージが表示されます。**サインイン試行の回数が多すぎます。後ほど試してください**。これは、ログイン情報が正しい場合でも発生します。

14.2 アイドル セッション タイムアウト

Meeting Management を構成すると、一定の期間に渡って非アクティブなユーザをサインアウトできます。Meeting Management は、ユーザがマウスを移動したり、ボタンをクリックしたり、テキストを入力フィールドに入力したりすると、ユーザがアクティブであると定義します。

アイドル セッション タイムアウトを有効にする場合、デフォルトのタイムアウトは 3600 秒

（1 時間）です。最小値は 60 秒で、最大 86400 秒（24 時間）です。

注：Meeting Management はステータスを 30 秒ごとにチェックします。つまり、タイムアウトは設定された制限時間プラス最大 30 秒間に設定できます。

注：アイドル セッション タイムアウトを有効にしても、ユーザはサインインから 24 時間後に、アクティブかどうかにかかわらずサインアウトされます。

14.3 Meeting Server のパスワードをリセット

以前のパスワードを検証せずに、Meeting Server のパスワードをリセットできます。ユーザがパスワードを忘れた場合、以前のパスワードを検証せずにパスワードをリセットするオプションがあります。このオプションを有効にすると、[Call Bridge の編集（Edit Call Bridge）] ページの [パスワードのリセット（Reset password ）] ボタンを使用してパスワードをリセットしているときに、以前のパスワードの入力を求めるプロンプトは表示されません（「構成済みサーバーの追加」セクションを参照）。

以下の設定が表示されます。

以前のパスワードを検証せずにパスワードをリセット - このチェックボックスをオンにすると、以前のパスワードを検証せずにパスワードをリセットできます。このオプションは、デフォルトではオフになっています。

14.4 TLS 設定

Meeting Management との間の接続を有効にする TLS 暗号スイートを選択できます。

ここで構成した設定は、すべての TLS 接続で有効になります。そのため、Meeting Management が次に対してどのように接続するのかに影響します。

- ブラウザ
- LDAP サーバー
- Call Bridge
- システムログサーバー
- 監査ログサーバー
- TMS
- Cisco Smart Software Manager

接続されているブラウザおよびサーバーはすべて、さまざまな暗号スイートをサポートしています。接続されたユニットが Meeting Management で有効になっている暗号スイートを 1 つ以上サポートしている場合、Meeting Management はリストの一番上に最も近い暗号スイートを使用します。

デフォルトでは、次の暗号スイートは無効になっています。

- AES256- SHA

注意：特定のブラウザまたはサーバでサポートされているすべての暗号スイートを無効にした場合 、Meeting Management に接続できなくなります。

特に、優先するブラウザと LDAP サーバでサポートされている暗号スイートが有効になっているか確認してください。お使いのブラウザが Meeting Management に接続できない場合や、Meeting Management が LDAP サーバに接続できない場合は、Meeting Management からロックアウトされている可能性があります。

15 ログサーバの追加

システムログには、少なくとも 1 つの syslog サーバをセットアップすることを強く推奨します。これは、サポートチームが効率的なサポートを提供できるようにするために必要です。

注：最新のシステムログはローカルに保存されますが、制限は 500 MB のシステムログです。制限に達すると、最も古い 100 MB のログが削除されます。

システムログサーバを追加するには、次の手順を実行します。

1. **[ログ（Logs）] ページで、**[システムログサーバー（System log servers）] を選択します。
2. **[ログ サーバの追加（Add log server）]** をクリックします。
3. サーバアドレスとポート番号を入力します。

   デフォルトポートは次のとおりです。

   - *UDP：514*
   - *TCP：514*
   - *TLS：6514*

   注：IPv6 アドレスを入力する場合、ここに角カッコを使用しないでください。

4. プロトコルを選択します。
5. **オプション：証明書を**使用することを選択し、証明書が無効であり Meeting Management で接続を拒否する場合は、証明書失効リスト（**CRL**）に対して証明書**を確認します。**

   チェーン内の証明書が無効またはアクセスできない CRL がある場合、Meeting Management は接続をブロックします。

   可能な場合はこれを有効にすることを推奨します。

   注：HTTP 証明書配布ポイント（CDP）を備えた証明書のみがサポートされています。CRL チェックを使用し、証明書に CDP がない場合、または CDP が HTTP 経由で到達できない場合、接続は拒否されます。

   また、Meeting Management が HTTP 経由で外部アドレスに接続できるよう、ネットワークを構成する必要があります。

6. TLS を選択した場合は、証明書を**アップロード**します。

   証明書チェーンの要件は次のとおりです。

   - *ルート CA 証明書を含む完全な証明書チェーンを含める必要があります。*
   - *証明書にリストされているアドレスは、ログサーバに入力したアドレスと同じである必要があります。*

7. **[追加（Add）]** をクリックします。
8. 必要なログサーバが追加されるまで、この操作を繰り返します。
9. Meeting Management を再起動します。

   注：今すぐ再起動するか、設定が完了するまで待ちます。

オプション：組織内で必要な場合は、監査ログに syslog サーバを追加します。

監査ログサーバを追加するには、次の手順を実行します。

1. **[ログ（Logs）] ページで、[監査ログサーバー（Audit log servers）]** を選択します。
2. **[ログ サーバの追加（Add log server）]** をクリックします。
3. サーバアドレスとポート番号を入力します。デフォルトポートは次のとおりです。

   - UDP：514
   - TCP：514
   - TLS：6514

   注：IPv6 アドレスを入力する場合、ここに角カッコを使用しないでください。

4. プロトコルを選択します。

5. **オプション：証明書を**使用することを選択し、証明書が無効であり Meeting Management で接続を拒否する場合は、証明書失効リスト（**CRL**）に対して証明書**を確認します。**

   チェーン内の証明書が無効またはアクセスできない CRL がある場合、Meeting Management は接続をブロックします。

   可能な場合はこれを有効にすることを推奨します。

   注：HTTP 証明書配布ポイント（CDP）を備えた証明書のみがサポートされています。CRL チェックを使用し、証明書に CDP がない場合、または CDP が HTTP 経由で到達できない場合、接続は拒否されます。

   また、Meeting Management が HTTP 経由で外部アドレスに接続できるよう、ネットワークを構成する必要があります。

   ---

6. TLS を選択した場合は、証明書を**アップロード**します。

   証明書チェーンの要件は次のとおりです。

   - *ルート CA 証明書を含む完全な証明書チェーンを含める必要があります。*
   - *証明書にリストされているアドレスは、ログサーバに入力したアドレスと同じである必要があります。*

7. **[追加（Add）]** をクリックします。
8. Meeting Management を再起動します。

   注：今すぐ再起動するか、設定が完了するまで待ちます。

   ---

16 サーバーを追加

[サーバー（Servers）] ページで、接続されている Meeting Server Call Bridge とエッジノードのすべてを表示および編集できます。新しい Call Bridge を追加することもできます。

Meeting Server の展開が成功すると、正常に構成されたすべての Meeting Server が **[構成済みサーバー（Configured Servers）]** タブに表示されます。展開ステータスが失敗または保留中の Meeting Server は、**[部分的に構成されたサーバー（Partial Configured Servers）]** タブに表示されます。

Meeting Management を無効にするかどうかなどのクラスタの詳細を編集したり削除したりできます。クラスタごとに、ユーザーのプロビジョニングを設定し、space テンプレートを作成することができます。そのクラスタを TMS に関連付けて、Meeting Management で予定されている会議を確認できます。自分または別のユーザーがすでに Meeting Management を使用してプロビジョニングを設定しているが、変更をコミットしなかった場合、クラスタの **[プロビジョニング（Provisioning）]** ページ、**[レビューとコミット（Review and commit）]** タブにユーザーを送信するリンクを含むクラスタの通知バナーが表示されます。

Meeting Management は、Call Bridge API を介して Meeting Server に接続します。Meeting Management の各 Call Bridge で API ユーザアカウントを設定しなかった場合は、続行する前に設定してください。手順については、*『Cisco Meeting Server API リファレンスガイド』*の「API へのアクセス」を参照してください。これは、cisco.com の『プログラミングガイド』のページにあります。

また、CDR 受信者アドレスが正しく設定されていない場合、Meeting Management は有効なミーティングに関するすべての関連情報を受信できません。この情報は、Meeting Management 機能を有効にする場合に必要です。

Call Bridge やエッジノードを追加するには、次の手順を実行します。

1. **[サーバー（Servers）]** ページで、**[サーバーの追加（Add Server）]** をクリックします。
2. 次のいずれかを実行します。
    a. 構成済みサーバーの追加
    b. 新しいサーバーの構成
3. **[OK]**をクリックします。

16.1 構成済みサーバーの追加

ライセンスおよびその他のサービスを管理するためにすでに構成されている Call Bridge サーバーを追加するか、既存の Meeting Server エッジ ノードを追加できます。

[サーバーの追加（Add Server）] を選択し、既存の **Meeting Server Call Bridge** またはエッジ

ノードサーバーを追加する場合は、このセクションの手順に従います。Cisco Meeting Server 接続設定の情報を入力します。

1. **[サーバーアドレス（Server address）]** フィールドに、**Call Bridge** またはエッジノードサーバーの **IP** アドレスまたは **FQDN**（完全修飾ドメイン名）を入力します。

   これは Web 管理インターフェイスのアドレスと同じです。

   注：IPv6 アドレスを入力する場合は、角カッコを使用します。

2. **[ポート（Port）]** フィールドに、Call Bridge またはエッジノードサーバーのポート番号を入力します。

   注：このフィールドを空のままにすると、Meeting Management はポート 443 を使用します。

3. MMP 管理者の [ユーザー名（Username）] と [パスワード（Password）]を入力して、Call Bridge またはエッジ ノード サーバーを追加します。

   注：セキュリティと監査上の理由から、Meeting Management 用に、管理専用アカウントを使用することを強く推奨します。

4. **[表示名（Display name）]** を入力します。

   表示名は任意に選択できます。他の管理者やビデオオペレータには意味があるものにする必要があります。

5. オプション：証明書を使用する場合は、**[信頼された証明書チェーンを使用（Use a trusted certificate chain）]** します。

6. オプション：証明書を使用することを選択し、証明書が無効な場合は Meeting Management で接続を拒否する場合は、**[証明書失効リスト（CRL）に対して証明書（Certificates against certificate revocation lists (CRLs)）]** を確認します。

   チェーン内の証明書が無効またはアクセスできない CRL がある場合、Meeting Management は接続をブロックします。

   可能な場合はこれを有効にすることを推奨します。

   注：HTTP 証明書配布ポイント（CDP）を備えた証明書のみがサポートされています。CRL チェックを使用し、証明書に CDP がない場合、または CDP が HTTP 経由で到達できない場合、接続は拒否されます。

   また、Meeting Management は、HTTP 経由で外部アドレスに接続できるよう設定する必要があります。

7. オプション：証明書のセキュリティを使用することを選択した場合は、**証明書をアップロードします。**

   証明書の要件：

   - *証明書チェーンには、Web 管理インターフェイスの証明書に署名した CA の証明書に加えて、ルート CA 証明書を含む証明書チェーン内の上位の証明書を含める必要があります。*
   - *Call Bridge またはエッジノード用に入力したサーバアドレスは、Web 管理インターフェイス証明書に含める必要があります。*

   注：SAN（サブジェクトの代替名）フィールドを使用する場合は、Meeting Management は共通名を確認しません。そのため、サーバアドレスが SAN フィールドに追加されていることを確認してください。

8. **オプション：ライセンスとプロビジョニングにのみ Meeting Management を使用する場合は、[Meeting Management を使用してこのクラスタ上のミーティングを管理する（Use Meeting Management to manage meetings on this cluster）] チェックボックスをオフにします。**

   注：クラスタ設定を編集することで、後でこれを変更できます。*『管理者向けユーザガイド』*の手順を参照してください。

   注：ビデオオペレータに対して、1 つ以上のクラスタの Meeting Management が無効にされたと知らせる情報は [ミーティング（Meetings）] ページには表示されません。

9. **[追加（Add）]** をクリックします。
10. オプション：**[クラスタを編集（Edit cluster）]** して、ユーザだけでなく他のすべてのユーザーに合った表示名を付け加える。

追加した Call Bridge またはエッジノードがクラスタの一部である場合、クラスタ内の他の Call Bridge またはエッジノードは自動検出され、簡単に追加できるよう下に表示されます。

自動検出された Call Bridge やエッジノードを追加するには、次の手順を実行します。

1. **[表示（Show）]** をクリックします。
2. **[アクション（Action）]** ＋ 列で、をクリックします。
3. 該当する場合、Call Bridge またはエッジノードの詳細を入力し、証明書をアップロードします。
4. クラスタにすべての Call Bridge またはエッジノードが追加されるまで続行します。

Call Bridge やエッジノードを編集するには、次の手順を実行します。

1. 編集する Call Bridge またはエッジノードまでスクロールし、 をクリックするか、行の任意の場所をクリックします。

2. その他の詳細を編集します。
3. パスワードをリセットするには、[パスワードのリセット（Reset password）] **ボタンをクリックして、[パスワードのリセット（Reset password）]**
   ポップアップウィンドウを起動します。次のフィールドが表示されます。
   a. **ユーザー名** – MMP 管理者のユーザー名が表示されます。
   b. **現在のパスワード – 現在設定されているパスワードを入力します。[高度なセキュリティ（Advance security）]** タブの [CMS パスワードリセット（CMC password reset）] **オプションがチェックされている場合、このフィールドは表示されません。**
   c. **新しいパスワード – ミーティングサーバーの新しいパスワードを入力します。** Meeting Management は、Meeting Server で定義された基準に対して新しいパスワードを検証し、無効なエントリがある場合はエラーメッセージを表示します。
   d. **新しいパスワードを確認 - 新しいパスワードを再入力します。**
4. **[完了（Done）]** をクリックします。

注: システムは、パスワードのリセット ポップアップ ウィンドウに入力されたすべてのフィールドを検証します。管理者は、パスワードをリセットするために有効なエントリを 3 回入力する必要があります。失敗した場合は、2 時間以内に再試行できます。

既存のクラスタの Meeting Management 機能を無効または有効にするには、次の手順を実行します。

1. **[クラスタの編集（Edit Cluster）]** をクリックします。
2. **[Meeting Management を使用してこのクラスタ上のミーティングを管理する（Use Meeting Management to manage meetings on this cluster）] チェックボックスをオン**
   またはオフにします
3. **[完了（Done）]** をクリックします。

16.2 新しいサーバーの構成

[サーバーの追加（Add Server）] を選択し、[新しい Meeting Server（Call Bridge）の構成と追加（Configure and add a new Meeting Server (Call Bridge)）] を選択すると、**Meeting Management コンソールでインストール アシスタントが開きます。**

16.2.1 準備中

新しい Meeting Server を設定するには、次の要素に対応していることを確認してください。

- Meeting Server が空である
- Meeting Server の DNS エントリを設定する

新規の Meeting Server インスタンス

Meeting Server では、仮想マシンを展開して実行し、管理者アカウントを有効にする必要があります。さらに、IPv4「a」インターフェイスが設定されている必要があります。他の設定は実行されません。『Cisco Meeting server 1000 および仮想化導入ガイド（Installation Guide for Cisco Meeting Server 1000 and Virtualized Deployments）』では、Meeting Server のインスタンスを導入する方法と Cisco Meeting Server の 1000 アプライアンスを設定する方法について説明しています。このガイドの「**IPv4 用のネットワーク インターフェイスの設定**」の章では、サーバーの設定について説明しています。「a」インターフェースを構成する手順を超えないでください。

既存の Meeting Server インスタンス

Meeting Server のインスタンスが以前に設定されているか、インストール アシスタント ツールで使用されていても設定が正常に完了していない場合は、リセットし、新しいサーバとして設定してから、インストール アシスタントで使用することができます。以前の設定の上では、インストール アシスタントを使用できません。サーバのリセット方法

1. Meeting Server の MMP インターフェイスに管理者アカウントを使用してログインし、コマンド **factory_reset full** を実行して、プロンプトが表示されたら確認します。サーバーは、デフォルト設定にリセットされ、再起動します。
2. Meeting Server の MMP インターフェイスに、ユーザー名 **admin**、パスワード admin **でログインします。**
3. プロンプトが表示されたら、新しい管理者パスワードを設定します。
4. 「a」インターフェイスの IPv4 設定を構成します。『Cisco Meeting Server 1000 と仮想化導入の設置ガイド』を参照してください。

注：上記ガイドの設定手順を実行する場合は、「a」インターフェイスの設定だけにしてください。

16.2.2 新しい Meeting Server の追加

サーバー構成タスクを完了するには、以下も必要です。

- ネットワークの DNS および NTP サーバーのアドレス
- Meeting Server で使用する SIP プロキシのアドレス
- Meeting Server で使用する選択された SIP ドメイン
- ユーザのインポートを設定する場合は、ネットワークの LDAP ディレクトリに対して、場所、ログイン情報、LDAP ユーザの場所の詳細など、接続に関する詳細情報が必要になります。
- 証明書を使用してサーバを設定する場合（推奨）、Meeting Server 用の FQDN を選択し、DNS サーバ レコードで定義する必要があります。
- 証明書を使用してサーバーを設定する場合（推奨）、認証局によって証明書要求が署名されている必要があります。インストール アシスタントは、証明書要求の生成に役立てることができます。また、既存の証明書とキー ペアを使用することもできます。

新しい Meeting Server を設定するための主な手順は次のとおりです。

1. **[インストール アシスタント（Installation Assistant）]** ページで、Meeting Server の**サーバーアドレス**を入力します。
2. Meeting Server に設定されている **[ユーザー名（Username）]** を入力します。

   注：デフォルトでは、「**admin**」がユーザー名として使用されます。

3. Meeting Server に設定されている**パスワード**を入力します。
4. [接続（Connect）] をクリックします。

   注：**[接続 （Connect）]** ボタンは、サーバーアドレス、ユーザー名、およびパスワードの詳細を指定した後にのみ有効になります。

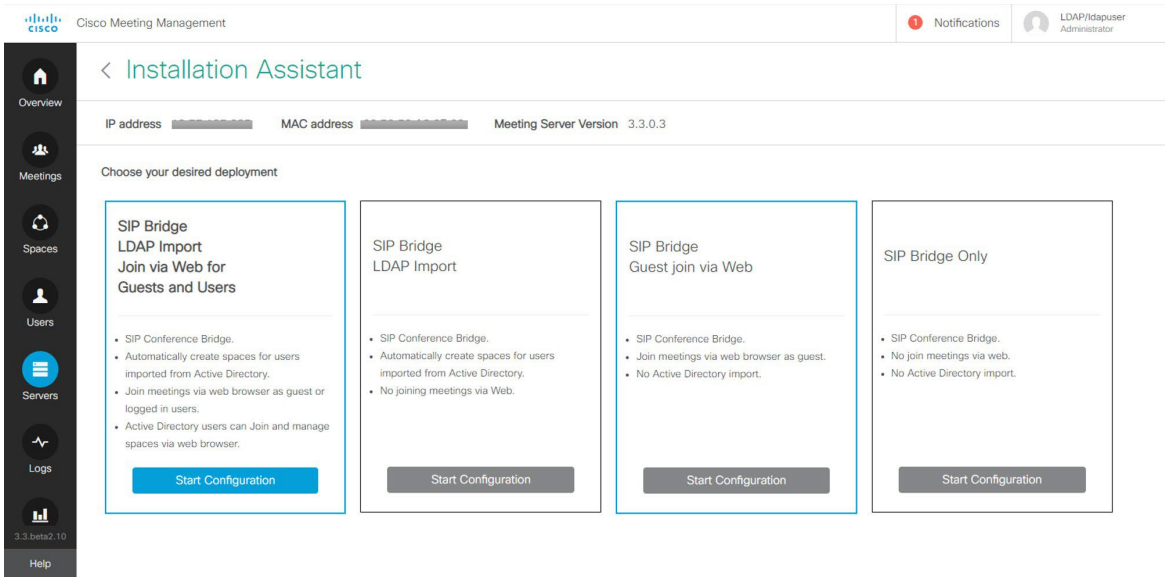
5. 次のオプションから目的の展開を選択し、**[構成の開始（Start Configuration）]** をクリックします。選択した展開タイプに基づいて、サーバーを構成するためのウィザードベースのインターフェイスが定義および表示されます。

   a. **ゲストおよびユーザの Web 経由での SIP ブリッジ LDAP インポート参加：ウィザードは、設定のすべての手順をナビゲートします。**

   b. **SIP ブリッジ LDAP インポート**：ウィザードは、Web Bridge を除く構成のすべての手順をナビゲートします。

   c. **Web 経由での SIP Bridge ゲスト参加：ウィザードは、会議ユーザを除く設定のすべての手順をナビゲートします。**

   d. **SIP ブリッジのみ：ウィザードは、Web Bridge と会議ユーザを除く構成のすべての手順をナビゲートします。**



6. プロンプトに従って必要な情報を入力して、ウィザードをナビゲートします。すべてのフィールドが検証されると、**[次へ（Next）]** ボタンが有効になります。

7. ウィザードは、選択した展開の種類に応じて、次のページのすべてまたは一部をナビゲートします。

   - 証明書
   - ネットワーク
   - Call Bridge
   - Web Bridge
   - 会議ユーザー
   - セキュリティ
   - プッシュ構成

8. **設定を確認し、準備ができたら、**[プッシュ設定（Push Configuration）] **をクリックして設定を Meeting Server にプッシュします。**

注：サーバーへの構成のプッシュに問題がある場合は、**[ログ（Logs）]** タブに移動し、**[ログ バンドルのダウンロード（Download Log Bundle）]** を使用して Meeting Management ログをダウンロードして問題を診断できます。

---

17 証明書

[証明書 (Certificate)] パネルでは、Meeting Server に必要な x.509 証明書を指定する方法と、新しい証明書を作成するための新しい証明書要求を作成するガイド プロセスが用意されています。インストールアシスタントは、認証局によって署名された証明書と自己署名証明書の使用をサポートしています。[証明書 (certificates)] パネルでは、CA の署名付き証明書または自己署名付き証明書を使用して選択したオプションに基づいて、自動的にオプションが調整されます。

注：自己署名付き証明書は、すべての機能に対してサポートされていません。これらはセキュリティ上のリスクがあるため、推奨されません。

推奨されるパスは、組織が信頼している認証局が署名した x.509 証明書を使用することです。認証局は、社内または公共の認証局にすることができます。Meeting Server が証明書をどのように使用しているかについて詳細については、『Cisco Meeting Server 証明書ガイドライン単一結合サーバー導入ガイド』を参照してください。

17.1 CA 署名済み証明書

[CA 署名済み証明書メソッド（CA Signed Certificate method）] を選択した場合、次の 2 つの使用可能なパスがあります。

- **CSR からの新しい証明書**：インストールアシスタントは、証明機関に提供する証明書署名要求の作成手順を案内し、さらに署名付き証明書を提示します。
- **既存の証明書とキーの提供 -** 外部のインストールアシスタントに向けて準備した既存の証明書とキーペアをアップロードします。

17.1.1 CSR 経由の新規証明書

このオプションでは、証明機関に提供する証明書署名要求（CSR）を作成することによって、新しい証明書を作成する手順を示します。

このプロセスを完了するには、以下の内容が必要です。

1. インストールアシスタントに証明書の詳細を提供し、結果として得られた CSR ファイルをダウンロードします。
2. 証明機関に CSR を提供すると、署名された証明書が返されます。また、公開されている証明機関を表す公開証明書のチェーンも必要になります。
3. 作成されたファイルはインストール アシスタントにアップロードされ、提供されたファイルを使用した Meeting Server の設定を処理します。

注：インストール アシスタント ツールは、**CSR** のダウンロード後に自由に閉じることができます。認証局からの署名付き証明書を取得したら、[一部設定済みの Meeting Server（Partial Configured Meeting Server）] タブに [サーバー（Servers）] ページから移動し、**[再開（Resume）]** をクリックして、[証明書（Certificate）] パネルに戻り、証明書アップロードプロセスを完了します（以下の手順 4 を参照）。

新しい証明書要求（CSR）を作成する手順は次のとおりです。

1. 証明書パネルで、[証明書タイプ（Certificate Type）] として[CA 署名（CA Signed）] を選択します。
2. **[証明書のアップロード オプション（Certificate Upload Options）]** で、**[CSR 経由の新しい証明書（New Certificate via CSR）]** を選択します。
3. Meeting Server で使用する詳細を含むフィールドを入力します。そのフィールドについては次で説明します。完了したら、**[次へ（Next）]** ボタンをクリックして [証明書（certificate）] パネルに戻ります。**[次へ（Next）]** ボタンは、必要な詳細をすべて入力した後にのみ有効になります。

   注：既存の生成された証明書がある場合、**[CSR の再作成（Regenerate CSR）]** をクリックすると、インストール アシスタントが複数の CSR ファイルの生成を許可しないため、既存のファイルは新しい詳細と共に上書きされます。

   表 5：証明書署名要求に必要なフィールド

フィールド名	説明	値
Meeting Server 用 FQDN	証明書の CN 値であり、DNS サーバーで定義されている必要があります。	サーバーの FQDN を入力します。
Meeting Server の SIP ドメイン	サブドメインを使用することをお勧めします。	ルーティング ルールに合わせるには、サーバーの SIP ドメインを入力します。

4. 完了した CSR が [証明書（Certificate）] パネルに表示されます。**[CSR のダウンロード（Download CSR）]** をクリックして、結果の CSR をローカル ドライブ上のファイルに保存します。
5. 署名されるために、CSR に認証局への署名を行います。これらは、署名付き証明書ファイルを返します。また、認証局の証明書チェーン バンドルも必要になります。
6. 署名付きの証明書と証明書チェーンファイルを取得したら、必要に応じて [証明書（Certificate）] パネルに戻り、**[ファイルのアップロード（Upload Files）]** を選択し、証明書とバンドルをアップロードします。証明書と CA 証明書チェーンを指定するための 2 つのフィールドが示されています。「**ファイルの選択（Select File）**」リンクを使用して、ローカル コンピューター上の特定のファイルを検索します。証明書ファイルには、次のいずれかの拡張子（CER、CRT、PEM、DER）が必要であり、PEM または DER としてエンコードされている必要があります。

7. 両方のファイルを指定したら、**[次へ（Next）]** ボタンをクリックします。ファイルはインストールアシスタントに送信され、検証されます。
8. 成功すると、証明書パネルはウィザードで完了としてマークされ、ネットワーク パネルに移動します。

エラーのシナリオ

次のシナリオの場合、エラーメッセージが表示され、**[次へ（Next）]** ボタンが無効になります。

- サーバー/技術的な問題によりアップロードが失敗した場合。解決策：証明書ファイルを再アップロードする必要があります。
- 指定された証明書が正しくない場合。
  解決策：適切な証明書と CA 証明書チェーンを選択してアップロードする必要があります。
- 証明書のアップロードに失敗した場合。
  解決策：正しい FQDN/SIP ドメインまたは正しいキー使用法で証明書を再アップロードします。
- 証明書チェーンのアップロードに失敗した場合。
  解決策：正しい FQDN/SIP ドメインまたは正しいキー使用法で証明書チェーンを再アップロードします。

17.1.2 既存の証明書とキーの使用

インストール アシスタントには、ツールを使用して CSR を生成するのではなく、既存の秘密キーと署名付き証明書を Meeting Server で使用するためのオプションが用意されています。これは、**[既存の証明書とキーを提供する（Supply an existing certificate and key）]** オプションを使用して行われます。

証明書、秘密キーおよび CA 証明書チェーンを指定する必要があります。証明書ファイルには、次のいずれかの拡張子（CER、CRT、PEM、DER）が必要であり、PEM または DER としてエンコードされている必要があります。

既存の証明書を使用する手順は次のとおりです。

1. **証明書パネルで、**[証明書タイプ（Certificate Type）] として[CA 署名（CA Signed）] **を選択します。**
2. [証明書のアップロード（Certificate Upload）] オプション**で、[既存の証明書とキーの提供（Supply an existing certificate and key）] を選択します**
3. **Meeting Server の FQDN、Meeting Server の SIP ドメイン、秘密鍵、CA 証明書チェーン、および証明書を指定するための 5 つのフィールドが表示されます。「ファイルの選択（Select File）」リンクを使用して、ローカル コンピューター上の特定のファイルを検索します。証明書ファイルには、次のいずれかの拡張子（CER、CRT、PEM、DER）が必要であり、PEM または DER としてエンコードされている必要があります。**
4. **5 つのファイルをすべて指定すると、**[次へ（Next）] ボタンが有効になります。**[次へ（Next）]** をクリックすると、ファイルがインストールアシスタントに送信され、検証されます。

成功すると、証明書パネルはウィザードで完了としてマークされ、ネットワーク パネルに移動します。

エラーのシナリオ

次のシナリオの場合、エラーメッセージが表示され、**[次へ（Next）]** ボタンが無効になります。

- サーバーまたは技術的な問題が原因でアップロードが失敗した場合 解決策：証明書ファイルを再アップロードする必要があります。

- 指定された証明書が誤っている場合、**[アップロード（Upload）]** ボタンが無効になります。
  解決策：適切な証明書と CA 証明書チェーンを選択してアップロードする必要があります。
- 提供された FQDN が正しくない場合。
  解決策：有効な FQDN を入力する必要
  があります。
- 提供された SIP ドメインが正しくない場合。
  解決策：有効な SIP ドメインを入力する必
  要があります。

17.2 自己署名証明書

自己署名付き証明書は、ローカル エンティティで署名された証明書です。証明書を検証する管理権限がありません。自己署名付き証明書は有効ですが、セキュリティの欠如のため推奨されません。Meeting Server が証明書を使用する方法とその要件については、『Cisco Meeting Server 証明書ガイドライン』を参照してください。

注：自己署名入りの証明書の詳細は、このツールによって保存されないため、1 回の設定で完了することを推奨します。

注：自己署名入り証明書を使用して Meeting Server を設定している場合は、Meeting Server の時刻が現在の時刻であることを確認してください。Meeting Server の時刻が実際の時刻と同期していない場合、エラーが表示されます。date MMP コマンドを使用して、時刻を正しく設定する必要があります。デフォルトのシステム時間は UTC です。

自己署名証明書を使用する手順：

1. [証明書（Certificate）] パネルで **[自己署名（Sef signed）]** を選択します。
2. **Meeting Server 用 FQDN** を入力します。
3. **ルーティング**ルール**に合わせるには、Meeting Server の SIP ドメイン**を入力します。
4. **[次へ（Next）]** ボタンは、必要な詳細をすべて入力した後にのみ有効になります。**[次へ（Next）]** をクリックします。
   [次へ（Next）] をクリックすると、ファイルがインストールアシスタントに送信され、検証されます。
5. 成功すると、証明書パネルはウィザードで完了としてマークされ、ネットワーク パネルに移動します。

エラーのシナリオ

次のシナリオの場合、エラーメッセージが表示され、**[次へ（Next）]** ボタンが無効になります。

- 提供された FQDN が正しくない場合。
  解決策：有効な FQDN を入力する必要

があります。

- 提供された SIP ドメインが正しくない場合。
  解決策：有効な SIP ドメインを入力する必
  要があります。

18 ネットワーク

[ネットワーク（Network）] パネルでは、サーバーのコア ネットワーク設定を設定できます。

注：これらの設定のガイダンスについては、ネットワーク管理者に問い合わせる必要がある場合があります。

1.次を設定します。

フィールド名	説明	操作
NTP サーバー	FQDN または IP アドレスのいずれかを使用して、少なくとも 1 台の NTP サーバーを設定する必要があります。 注：最大 5 台の NTP サーバーを設定できます。	**[サーバの追加（Add Server）]** をクリックします。NTP サーバのアドレスが Cisco Meeting Server に追加されます。
タイム ゾーン	サーバーのローカル タイムゾーン	ご希望のタイムゾーンを選択してください
DNS サーバー	IP アドレスを使用して、少なくとも 1 台の DNS サーバーを設定する必要があります。 注：最大 5 台の DNS サーバーを設定できます。	サーバーの IP アドレスを入力して **[サーバーの追加（Add Server）]** をクリックします。DNS サーバのアドレスが Cisco Meeting Server に追加されます。
Webadmin ポート	Meeting Server Web Admin インターフェイスが受信する TCP ポート番号を設定します。 Web Bridge を含むデプロイメントを使用している場合、ポート 443 の使用は許可されていません。	ポート番号を入力します。

すべての詳細が入力されていることを確認し、[ネットワーク（Network）] パネルの構成が正常に完了していることを確認します。[次へ（Next）] ボタンが有効になり、ネットワーク設定が保存され、クリックすると、選択した展開に基づいて次のパネルに移動します。

18.1 DNS または NTP サーバーを削除

1. をクリックして DNS や NTP サーバーを削除します。

エラーのシナリオ

次のシナリオの場合、エラーメッセージが表示され、**[次へ（Next）]** ボタンが無効になります。

- 入力済みの NTP サーバー アドレスが指定されている場合。解決策：有効な IP アドレス/FQDN を指定する必要があります。
- 間違った DNS サーバー アドレスが指定されている場合。解決策：有効な IP アドレスを指定する必要があります。
- 間違ったポート番号が提供された場合。解決策：有効なポート番号を入力する必要があります。
- 入力済みの NTP サーバー アドレスが指定されている場合。解決策：別の IP アドレス/FQDN を指定する必要があります。
- 入力済みの DNS サーバーアドレスが指定されている場合。解決策：別の IP アドレスを指定する必要があります。

19 Call Bridge

[Call Bridge] パネルでは、Call Bridge サービスの設定を構成できます。

1. 次の詳細を入力します。

フィールド名	アクション
SIP Proxy	Meeting Server からの発信コールを受信する SIP プロキシの FQDN または IP アドレスを入力します。
暗号化	接続に暗号化モード（TLS）を選択します。
SIP コールのメディア暗号化	ドロップダウン リストから、必要なオプションを選択します。
ActiveControl	すべての参加者に対して ActiveControl パーミッションを有効にします。 **このオプションが有効になっている場合、デフォルトで参加者の ActiveControls を有効にするために callLegProfile および systemprofile** が作成されます。注：これらの設定は、Meeting Server ではデフォルトで有効になっていません。

2. 正しい詳細を入力すると、Call Bridge パネルの設定が正常に完了します。

注：設定の保存を成功させるために、すべての詳細が入力されていることを確認してください。

---

3. **[次へ（Next）]** ボタンが有効になり、クリックすると、選択した展開に基づいて次のパネルに移動します。

エラーのシナリオ

次のシナリオの場合、エラーメッセージが表示され、**[次へ（Next）]** ボタンが無効になります。

- 入力された SIP プロキシの詳細が正しくない場合。
  解決策：有効な IP アドレス/FQDN を指定する必要があります。

20 Web Bridge

Web Bridge パネルでは、Call Bridge が Web Bridge に接続できるようにするポートを開くことにより、Cisco Meeting Server Web App を設定できます。

1. **Call Bridge to Web Bridge（c2w）リスニングポート**を入力します。デフォルトでは、ポート番号は 9999 です。
2. 正しい詳細が提供されると、Web Bridge パネルの構成が正常に完了します。
3. **[次へ（Next）]** ボタンが有効になり、クリックすると、選択した展開に基づいて次のパネルに移動します。

エラーのシナリオ

次のシナリオの場合、エラーメッセージが表示され、**[次へ（Next）]** ボタンが無効になります。

- 入力された Call Bridge to Web Bridge（c2w）ポートの詳細が正しくない場合。解決策：有効なポート番号を指定する必要があります。

注：443 または webadmin ポートであってはなりません。

---

21 会議ユーザー

会議ユーザー パネルでは、LDAP ユーザーをインポートして Cisco Meeting Web App にログイン可能にすることができます。

ユーザーアカウントを作成するには、次のものが必要です。

- Active Directory サーバーに接続するための接続プロパティの定義デフォルトでは、LDAPS オプションが選択されています。
- Meeting Server でユーザを作成するときに使用する検索フィルタとフィールド マッピング値を定義します。インストール アシスタントには、ほとんどの環境で動作するデフォルト値がありますが、必要に応じてデフォルト値を変更することもできます。

ユーザーアカウントを作成する場合。

1. [LDAP 接続の設定（LDAP Connection Settings）] フィールドに、Active Directory コントローラに接続するための値を入力します。すべての必須フィールドの入力が完了すると、**[次へ（Next）]** ボタンが表示されます。

   各設定の詳細については、次の表を確認してください。

表 6：LDAP 接続の設定

フィールド名	説明	入力
サーバーアドレス	接続先の LDAP サーバーのネットワーク アドレス	LDAP サーバーの FQDN または IP アドレス。
ポート	接続先の LDAP サーバーの TCP ポート。	有効なポート番号 デフォルト値は、LDAPS の場合は 636、LDAP の場合は 389 です。
ユーザー名	LDAP サーバーに接続されるユーザのユーザー名。このユーザには、ディレクトリへの読み取り権限のみが必要です。	認証に使用するユーザの LDAP 識別名（DN）または UPN。 このフィールドは空白にできません
パスワード	ユーザ指定のパスワード	ユーザのパスワード。 このフィールドは空白にできません。
検索ベース	インポート検索クエリが開始される LDAP ディレクトリ内の場所。この値の詳細については、ドメイン管理者に問い合わせてください。	検索を開始するディレクトリの場所の LDAP 識別名（DN） このフィールドは空白にできません
ユーザへの PMP ライセンスの割り当て	有効にすると、インポートされたユーザは PMP+ ライセンスを受ける資格があるものとしてマークされます。インポートするすべてのユーザに対して PMP+ ライセンスを購入していない場合は、有効にしないでください。	すべてのインポートされたユーザに PMP+ の権限をタグ付けするようにします。
既定のユーザ フィルタとフィールド マッピングの詳細の上書き	インストール アシスタントは、デフォルトの LDAP 検索フィルタとユーザ フィールド マッピングを使用して、ほとんどの環境で動作することを想定しています。このオプションを有効にすると、環境に合わせてこれらの設定を表示およびカスタマイズできます。	LDAP 検索フィルタ、および LDAP ユーザ フィールド マッピングの表示やカスタマイズを有効化します。

2. **[LDAP 接続の確認（Check LDAP Connection）]** ボタンをクリックして、LDAP 接続が使用可能であることを確認します。

注：接続チェックが失敗した場合に [LDAP 接続の確認（Check LDAP Connection）] ボタンをクリックすると、次のエラーメッセージが表示されます。**「LDAP 接続に失敗しました」**

3. **LDAP** 接続が正常に確立されると、**[**次へ（Next）**]** ボタンが有効になります。**[**次へ（**Next**）**]** をクリックします。

注：設定の保存を成功させるために、すべての詳細が入力されていることを確認してください。デフォルト値を変更する場合は、マッピングに使用される有効な LDAP 式を使用するようにしてください。

エラーのシナリオ

- [LDAP 接続の確認（Check LDAP Connection）] ボタンをクリックすると、接続確認が失敗する解決策: 有効な LDAP 接続の詳細を指定する必要があります。

21.1 LDAP 検索とユーザーマッピングのカスタマイズ

インストール アシスタントは、デフォルトの LDAP 検索フィルタとユーザ フィールド マッピングを使用して、ほとんどの環境で動作することを想定しています。電子メールアドレスが定義されているユーザのデフォルトのフィルタでは、ユーザー名、Meeting Server のユーザー名を会議アドレスに設定します。

[上書き（override）] オプションを有効にすると、インポートに使用される個々の設定フィールドが表示されます。設定を表示すると、インストール アシスタントがデフォルトで使用します。**デフォルトのユーザーフィルタとフィールドマッピングの詳細の上書きが有効になっている場合、ユーザーは、環境に合わせてこれらの値をカスタマイズできます。**

ユーザ マッピング方式では、Meeting Server にインポートするときのユーザ プロパティの設定方法を定義します。この方式では変数を静的テキストとともに使用しているため、ユーザを Meeting Server 作成するときに LDAP にあるユーザのプロパティを使用できます。LDAP プロパティの使用において、ユーザごとに一意である必要があるプロパティ（ユーザー名や URI など）を重複させないように使用することが重要になります。LDAP プロパティは、$ 記号で囲まれたプロパティ名によって参照されます。例：LDAP プロパティ「mail」は、フィールド マップの式 $mail$ に参照されています。

表 7：LDAP の読み込み設定

フィールド名	説明	入力
LDAP 検索フィルタ	読み込む LDAP ユーザの条件を定義します。	LDAP 検索文字列。LDAP 検索シンタックスを使用する必要があります
表示名	ディレクトリと検索でユーザに対して表示される名前。	マッピング方式。例：cn
ユーザー名	ユーザが Cisco 会議 Web アプリケーションのログインに使用するユーザー名。 結果の値は、すべてのユーザとスペースに対して一意である必要があります。	マッピング方式。 例： **$sAMAccountName$@company.com** このフィールドは空白にすることはできず、結果は読み込まれた各ユーザに対して一意である必要

		があります。

フィールド名	説明	入力
スペース名	与えられたラベルをユーザ用のスペースに自動的に作成します。 読み込んだユーザのスペースを作成しない場合は、空白のままにします。	マッピング方式。 例：**cn Meeting space**
スペース URI	ユーザに対して自動的に作成されたスペースの URI の左側部分。 結果は、ユーザごとに一意である必要があり、ユーザー名または他のスペースと競合していない必要があります。読み込んだユーザのスペースを作成しない場合は、空白のままにします。	マッピング方式。例： **cn.space**
スペース セカンダリ URI	ユーザに対して自動的に作成されたスペースのセカンド URI の左側部分。 結果は、ユーザごとに一意である必要があり、ユーザー名または他のスペースと競合していない必要があります。オプション フィールド。読み込んだユーザのスペースを作成しない場合は、空白のままにします。	マッピング方式。例： **cn.room**
スペースコール ID	ユーザ用に自動的に作成されたスペースのコール ID を設定します。 結果は、すべてのスペースで一意である必要があります。オプション フィールド、Cisco Meeting Server では、空白の場合 ID を自動的に割り当てます。 読み込んだユーザのスペースを作成しない場合は、空白のままにします。	マッピング方式。
認証 ID マッピング	インポートされたユーザに割り当てられているマッピング プロパティ。スマートカードのログイン シナリオで使用されます。 証明書ベースのログインを特に展開しない限り、空白のままにしておきます。	マッピング方式。 例：**$userPrincipalName$**

[次へ（Next）] ボタンが有効になります。**[次へ（Next）]** をクリックすると、ログイン資格情報が作成および保存され、選択した展開に基づいて次のパネルに移動します。

注：設定の保存を成功させるために、すべての詳細が入力されていることを確認してください。

エラーのシナリオ

次のシナリオの場合、エラーメッセージが表示され、**[次へ（Next）]** ボタンが無効になります。

- 入力されたサーバーアドレスの詳細が間違っている場合。解決策：有効な IP アドレス/FQDN を指定する必要があります。

- 入力したポート番号が間違っている場合。
  解決策：正しい数値のみを指定する必要があります。

22 セキュリティ

デフォルトの管理者アカウントにアクセスできなくなった場合は、[セキュリティ（Security）] パネルを使用して、Meeting Server で別のユーザを作成することができます。

1. リカバリ アカウントを作成するには、**[バックアップユーザアカウントの作成 (Create backup user account)]** を選択します。
2. 新しいユーザー名とパスワードを作成し、パスワードを確認します。

   注：パスワードは空白にできません。また、**ユーザー名を** admin にすることはできません。

3. **[次へ（Next）]** ボタンが有効になります。**[次へ（Next）]** をクリックすると、ログイン資格情報が作成および保存され、選択した展開に基づいて次のパネルに移動します。

エラーのシナリオ

次のシナリオの場合、エラーメッセージが表示され、**[次へ（Next）]** ボタンが無効になります。

- 入力されたユーザー名が間違っている場合。
  解決策：有効なユーザー名を指定する必要があります。
  注：「admin」以外の英数字を入力してください。
- 入力したパスワードと確認パスワードが一致しません。解決策：
  両方のフィールドに同じパスワードを再入力します。
  注：英数字の値のみを指定する必要があります。

23 プッシュ構成

[プッシュ構成（Push Configuration）] パネルでは、インストール アシスタントで提供された各パネルの詳細を確認できます。

1. **[次へ（Next）]** ボタンをクリックして、提供された設定の詳細を Meeting Server にプッシュし、設定プロセスを完了します。

2. 設定が Meeting Server に正常に転送されると、インストール アシスタントに概要の詳細が表示されます。追加された Meeting Server は、**[設定済みサーバー（Configured Server）]** タブにリストされます。追加した Meeting Server は、それぞれのアイコンをクリックして編集または削除できます。

   注：追加された Meeting Server は、期限切れのライセンス状態になります。Meeting Server を Meeting Management サーバーに追加してください。

   ---

3. **［サーバー設定（Server settings）］と [クラスタの編集（Edit Cluster）] の下に移動し、**[Meeting Management を使用してこのクラスタ上の会議を管理する（Use Meeting Management to manage meetings on this cluster）] **チェックボックスをオンまたはオフにします。**

4. **表示**名を入力します。

5. **[終了（Exit）]** ボタンが有効になります。**[終了（Exit）]** をクリックして **[サーバー（Servers）]** ページに移動します。

6. 構成が失敗または不完全だった場合、考えられる次の手順は次のとおりです。

   a. **ログ：[**ログ（Logs）**] タブに移動し、[**ログバンドルのダウンロード（Download log **bundle**）**]** ボタンを使用して、インストール アシスタントのログも含む Meeting Management ログをダウンロードできます。

   b. リセット：このリンクを使用して、インストール アシスタントによってプッシュされた Meeting Server 設定を削除できます。

   c. 再開：[部分的に構成されたサーバー（Partial **Configured Server**）]**タブから Meeting Server** の構成を再開できます。

インストールアシスタントを終了すると、失敗した構成が [部分的に構成されたサーバー（Partial Configured Server）] タブに一覧表示されます。

23.1 SSH 機能

Meeting Management に追加されたエッジノードでタスクを実行するには、SSH 機能が必要で

す。管理者は、**SSH ターミナルに接続し、**[SSH ターミナル（SSH terminal）] タブを使用して、選択した Meeting Server またはエッジノードに対して MMP コマンドを実行できます。MMP 管理者の資格情報を提供することで、Call Bridge またはエッジ ノードを選択し、SSH 端末に接続できます。接続すると、選択したサーバーで MMP コマンドを実行できます。

24 ライセンスモードの選択

[設定（Settings）] ページの [ライセンス（Licensing）] タブで、ライセンスモードを選択できます。スマートライセンスを選択した場合は、ここでいくつかのスマートライセンス設定を構成することもできます。

ライセンスモードを選択する必要があります。以下の中から選択します。

- **スマートライセンス**（推奨）

  Cisco Smart Software Manager に登録してライセンス割り当てを設定するまで、ライセンス ステータスは非準拠と表示される場合があります。

  スマートライセンスを選択すると、Meeting Management は、購入したライセンスに関する情報を Cisco SSM から取得します。

  注：Meeting Management スマート ライセンシング統合用の CLI（コマンドライン インターフェイス）はありません。これは Meeting Management がグラフィックなユーザインターフェイスを提供するという設計によるものです。

- **接続された Call Bridge にアクティベーションキーをインストールする必要が**なくなりました。代わりに、Meeting Management は、従来のライセンス キーのない Call Bridge の数を Cisco Smart Software Manager に報告します。これらは、スマートアカウント**でアクティブな Call Bridge ノード**と呼ばれるライセンスタイプとして表示されます。これらのライセンスは無料で、必要な数のライセンスが自動的に付与されます。
- **ライセンスなし**

  このオプションは、復元力のある展開でのみ使用できます。復元力のある展開で、Meeting Management の他のインスタンスでスマートライセンスのいずれかを有効にしている場合は、このオプションを選択します。

注：

- **以前のバージョンの Meeting Management でこのライセンスモードを使用していたユーザーの場合、**従来のライセンス**オプションはグレー表示されます。**
- Meeting Management は、ローカル ライセンス ファイル（従来のライセンス モード）のサポートを廃止しました。スマート ライセンスに移行すると、従来のライセンス オプションはライセンス モード **ポップアップで使用できなくなります。**
- ライセンスモードを変更し、または新しいクラスタを追加した後、接続されている Meeting Servers のライセンスステータスにこの変更が適用されるまで最大で 5 分かかる場合があります。

24.1 スマートライセンスを有効にする方法

スマートライセンスを有効にするには、以下の手順を実行します。

1. Cisco SSM にサインインし、登録トークンを生成します。

   注：登録トークンを生成するときに、[製品の輸出規制機能をこのトークンに登録可能にする（Allow export-controlled functionality on the product registered with this token）] オプションを選択して、より高いレベルの製品暗号化機能を有効にしてください。詳しくは『Smart Software Manager オン プレミス ユーザーガイド』を参照してください。

2. トークンをクリップボードにコピーします。
3. ライセンスレポートに使用する Meeting Management のインスタンスを開きます。
4. **[設定（Settings）]** ページの **[ライセンス（Licensing）]** タブに移動します。
5. **[変更（Change）]** をクリックします。
6. [スマートライセンス（Smart Licensing）] を選択して、[保存（Save）] します。
7. **[登録（Register）]** ボタンをクリックします。
8. 登録トークンを貼り付けます。
9. オプション：すでに登録されている場合は、この製品インスタンス登録します

   通常、Cisco SSM では、すでに登録されている Meeting Management インスタンスを登録しません。このチェックボックスをオンにすると、Cisco SSM では、同じインスタンスを再度登録できるようになります。これは、登録解除を試みた場合や、登録解除中に Meeting Management が Cisco Smart Software Manager にアクセスできないなど、Meeting Management が登録の詳細を失った場合に役立ちます。

10. **[登録（Register）]** をクリックします。
11. 登録された場合は、バーチャルアカウントにあるライセンスの数を確認します。
12. Meeting Management で、**[ライセンス（Licenses）]** ページに移動します。
13. バーチャルアカウントにあるライセンスに関する情報を入力します。

    注：

    - 注：Meeting Management をテストする場合に、ライセンスをまだ持っていない場合は、代わりに **[トライアルの開始（Start trial）]** をクリックします。
    - 注：特定のタイプのライセンスを持っていない場合は、フィールドを空白のままにするのではなく 0 を入力します。

注：ライセンスモードを更新し、または新しいクラスタを追加した後、Meeting Management がライセンスステータスを更新するためにすべての使用情報を取得するには、時間がかかる場合があります。これには、接続の速度とデータ量に応じて、数分から 15 分を超える場合があります。

注：割り当てられたライセンスの数を変更する度に、接続されている Meeting Servers のライセンスステータスにこの変更が適用されるまで最大で 5 分かかる場合があります。

注：ライセンスの予約中に、Cisco SSM の応答時間が予想される 30 秒よりも長くかかる場合、さまざまなタイムアウト値でさらに 2 回の再試行が試行されます。Meeting Management は、2 回目と 3 回目の再試行をそれぞれ 60 秒と 90 秒待機します。3 回の再試行後にライセンスの予約が失敗した場合は、[概要（Overview）] ページに [Cisco Smart Software サーバーに到達できません（Unable to reach Cisco Smart Software Server）] と表示されます。ライセンスの予約を再開する必要があり、ライセンスが正常に予約されたことを示すメッセージがクリアされます。

24.2 スマートライセンスが有効にされた後のスマート ライセンス アクション

次を実行できます。

- **承認を今すぐ更新**：システムは UTC の午前 0 時に、毎日承認を自動的に更新します。ただし、手動で更新する場合は、ここで更新できます。これは、新しいライセンスを購入した場合、またはこの Meeting Management のバーチャルアカウントに追加のライセンスを割り当て、Meeting Management の変更をすぐに確認する場合に役立ちます。
- **登録を今すぐ更新**：システムは 6 か月ごとに登録を自動的に更新します。この Meeting Management のバーチャルアカウント間のライセンスを移動した場合や、この Meeting Management のインスタンスを別のバーチャルアカウントに移動した場合は、手動で登録を更新できます。
- **登録**：Meeting Management のこのインスタンスで別のバーチャルアカウントを使用する場合は、手動で再登録できます。
- **ライセンス予約：スマート ライセンスにより、スマート**アカウントを使用してライセンスをアクティブ化および管理できます。Cisco Smart Software Manager でトークンを生成して製品インスタンスをアクティブ化し、製品インスタンスに必要なライセンスを予約できます。スマートアカウントは、選択した製品インスタンスがすべてのデバイスで現在のライセンス要件をサポートするのに十分なライセンスに準拠し、承認されていることを保証します。詳細については、このセクションを確認してください。
- **登録解除**：バーチャルアカウントを別の展開に使用する場合や、Meeting Management の展開に復元力があり、レポートに別の会議インスタンスを使用する場合は、Meeting Management のこのインスタンスの登録を解除できます。

  注：ライセンスモードを変更すると、Meeting Management は自動的にスマートライセンスを無効にし、Cisco Smart Software Manager からの登録を解除します。

注：Meeting Management のインスタンスへの接続が切断された場合は、Cisco SSM から登録を解除することもできます。

24.3 ライセンス予約

SMART に準拠するために、Cisco 製品のユーザーはライセンス予約のサポートを必要とします。Meeting Management は、バージョン 3.4 以降のライセンス予約をサポートしています。セキュリティ上の理由で Meeting Management がインターネットに接続できない環境では、ライセンス予約を使用して機能をアクティブ化し、ライセンスを予約することができます。

この機能には、ユニバーサル（永久ライセンス予約）と 特定（特定ライセンス予約）の 2 種類あります。

- **ユニバーサル バリアント**：ユニバーサルまたは永久ライセンス予約（PLR）は、製品のすべての機能を使用できる単一のライセンスを提供します。PLR は
  軍事/防衛のお客様
- **特定のバリアント**：特定ライセンス予約（SLR）は、要件に基づいてライセンスを予約する選択肢を提供します。機能ライセンスのほか、SMP Plus や PMP Plusなどのユーザライセンスも予約できます。ライセンスの使用状況が変更された場合、この機能により、ライセンス予約を更新または変更できます。

ライセンス予約は、ユニバーサルから特定のバリアントに、またはその逆に変更できます。これには、予約の返却と製品インスタンスの再登録が含まれます。

注：ライセンス予約機能は、デフォルトでは顧客のスマート アカウントで有効になっていないため、顧客から具体的に要求され、Cisco によって承認される必要があります。どちらのタイプのライセンス予約でも、Cisco がスマート アカウントを認証する必要があります。Meeting Management の 1 つのインスタンスだけで使用する専用のバーチャルアカウントを持つ企業のスマートアカウントが必要です。アカウントを要求するには、シスコのアカウントチームに問い合せるか、Cisco Software Central に移動します。

ライセンス予約により、次のワークフローが可能になります。

- SLR/PLR ライセンス予約
- 予約済みライセンスの更新
- 予約したライセンスの返却

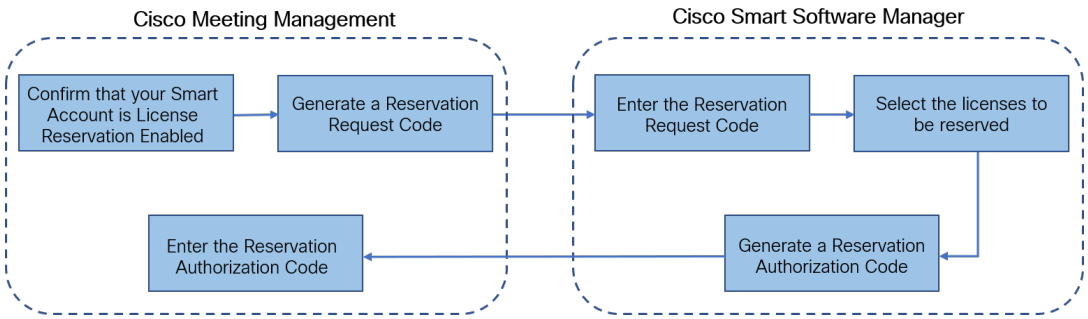
24.3.1 ライセンス予約

初期ライセンス予約のワークフローは次のとおりです。

1. スマートアカウントでライセンス予約が有効になっていることを確認します
2. Meeting Management からリクエストコードを生成します
3. Cisco SSM にコードを入力します
4. SLRの場合、予約するライセンスを選択します

5. Cisco SSM で予約承認コードを生成します
6. Meeting Management に認証コードを入力します

図 1：ライセンス予約のワークフロー



ライセンスを予約するには、次の手順に従います。

1. [Meeting Management **設定（Meeting Management Settings）**] で、「**ライセンス**」セクションに移動します。
   a. **[登録（Register）]** ボタンをクリックして、**[スマート ソフトウェア ライセンシング登録（Smart Software Licensing Registration）]** ポップアップを開きます。
   ポップアップ
   b. ポップアップの下部にある **[ここから開始（start** here）] リンクをクリックして、ライセンス予約プロセスを開始します。
   c. **開いてるポップアップ**ウィンドウで、**[はい、自分のスマートアカウントはライセンス予約が有効になっています（Yes, My** Smart Account is License Reservation Enabled）] をクリックします。
   d. **スマートライセンス予約のポップアップで、**[生成（**Generate**）] ボタンをクリックして予約要求コード（Reservation Request Code）を生成します。
   e. 生成される予約要求コードを保存またはコピーします。
   f. **[閉じる（Close）] をクリックします。**Meeting Management の **[スマート ソフトウェア ライセンシング（Smart Software Licensing）]** ページで、**Smart Software Licensing Status** が License Reservation Pending と表示されます。

2. Smart Software Manager で、
   a. スマート アカウントで Cisco Smart Software Licensing Manager にログインします。
   b. 目的のバーチャル アカウントに移動し、**[ライセンス予約（License Reservation）]** をクリックします。

      注：ライセンス予約を使用するには、Cisco からの特別な許可が必要です。このためには、Smart Software Manager の [インベントリ（Inventory）] セクションの [ライセンス（Licenses）] タブで **[ライセンス予約（License Reservation）] ボタンが使用可能であることを確認する必要があります。**

   c. 予約要求コードを入力します。
   d. **[予約するライセンス**（Licenses to Reserve）] からライセンスを選択します。
      - PLR **の場合 -** オプション Meeting Server PLR の有効化を選択**します**
      - SLR の場合 - [特定のライセンス予約（Reserve a specific license）] **オプションを選択し、**予約する特定のライセンスを選択します。
   e. [認証**コード**の生成（**Generate Authorization** Code）] ボタンをクリックして、予約認証コードを生成します。
   f. 予約承認コードを保存またはコピーします。

      注：特定のライセンスの場合、[予約するライセンス（Licenses to Reserve）] で [特定のライセンス予約（Reserve a specific license）] **を選択すると、利用可能なライセンスのリストを表示できます。スマートアカウントで要求する際には、十分な数のライセンスを選択してください。**

3. Meeting Management で、次の手順を実行します。
   a. **[スマート ソフトウェア ライセンシング（Smart Software Licensing）]** ページで、**[予約承認コードを入力（Enter Reservation Authorization Code）]** ポップアップを開きます。
   b. 予約要求コードを表示するか、予約リクエストをキャンセルするオプションもあります
   c. **Smart Software Manager から生成された予約承認コードを入力し、[承認コード/ファイルのインストール**（Install **Authorization**

Code/File）] ボタンをクリックして予約を完了します。

4. **[ライセンス（Licensing）]** セクションで、[スマート ソフトウェア ライセンシングのステータス（Smart Software Licensing Status）] にある [登録ステータス（**Registration** status）] が以下のように変更されます。

   - 「ライセンス予約が保留中です（**License Reservation Pending**）」から「**登録済み - ライセンス予約（Registered -License Reservation**）」へ
   - 「ライセンス承認（**License authorization**）」が「**承認済み - 予約済み（Authorized - Reserved**）に変わります。

5. [ライセンス（Licenses）] ページのライセンスステータスは、次のように表示されます。
   - PLR の**予約が有効です**
   - **予約が** SLR のライセンス数とともにされています。

24.3.2 予約済みライセンスの更新

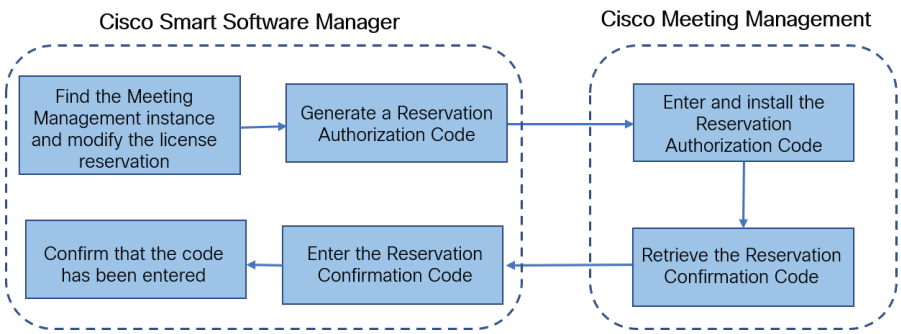
組織の変化するニーズを満たすために、特定のライセンスを更新するか、予約済みライセンスの数を変更することができます。たとえば、現在のライセンス要件が 5 で、さらに 5 ライセンスを追加する場合、ライセンス数を 10 として選択する必要があり、新しい値が以前の値を上書きします。

注：PLR を使用している場合、ライセンスの更新は適用されません。ただし、ライセンス予約のタイプを PLR から SLR に、またはその逆に変更することができます。ライセンス予約の種類を変更するには、予約済みのライセンスを返却し、製品インスタンスの登録を解除し、製品インスタンスを最初から登録し直します。予約を PLR から SLR に変更すると、SLR で選択したライセンスが PLR ライセンスを上書きします。

予約済みライセンスを更新するワークフローは次のとおりです。

1. Cisco SSM で更新するライセンス インスタンスを見つけます
2. 予約承認コードを生成します
3. Meeting Management にコードを入力してインストールします
4. 予約確認コードを生成します
5. Cisco SSM の予約確認コードを入力して確認します

図 2：ライセンス予約更新のワークフロー



予約ライセンスを更新するには、次の手順を実行します。

1. Smart Software Manager の場合
    a. 製品インスタンスで **Meeting Management インスタンスを見つけます** をクリックし、[アクション（Actions）] メニューから [ライセンス予約の更新（Update License Reservation）] を選択します。
    b. [ライセンス予約の更新（Update License Reservation）] ポップアップを使用して、予約するライセンスを変更し、新しい Reservation Authorization Code を生成します。
    c. 予約承認コードを保存またはコピーします。
2. Meeting Management 設定の場合
    a. **[ライセンス（Licensing）]** セクションに移動して、**[ライセンス予約を更新（Update License Reservation）]** をクリックします。
    をクリックするだけです。
    b. **[予約の更新（Update Reservation）]** ボタンをクリックすると開くポップアップに予約認証コードを入力します。

    注：Meeting Management インスタンスがユニバーサル ライセンスを予約している場合、ライセンス予約を更新するには、「ライセンス」**セクションの** [予約済みライセンスの返却（Return Reserved Licenses）] ボタン**を使用してこのライセンスを返却してから、製品インスタンスを再登録します。**

    ---

    c. **[認証コードのインストール（Install Authorization Code）]** ボタンをクリックして、ライセンス予約を更新し、予約確認コードを生成します。
    d. **[スマート ソフトウェア ライセンス（Smart Software Licensing）]** ページの [確認コードの表示（View confirmation code）] ボタンをクリックして、予約確認コードをコピーまたは保存します。
3. Cisco Smart Software Manager の場合
    a. **[製品インスタンス（Product Instances）]** で Cisco Meeting Management インスタンスを見つけ、**[アクション（Actions）] メニュー**から **[確認コードの入力...（Enter Confirmation Code...）]** を選択して、**[確認コードの入力（Enter Confirmation Code）]** ポップアップを起動します。
    b. **[確認コードの入力（Enter Confirmation Code）] ポップアップ**に予約確認コードを入力します。
    c. **Meeting Management** の **[スマート ソフトウェア ライセンス（Smart**

Software Licensing）] ページに戻り、**[**コードが入力されました**（Code Has Been Entered）]** ボタンをクリックして、予約認証コードのインストール後に発生したアラートを閉じます。

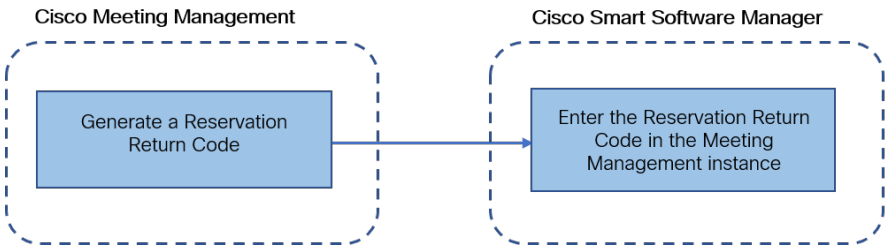
24.3.3 予約したライセンスの返却

他の製品インスタンスでライセンスを使用できるように、予約済みのライセンスをバーチャル アカウントに戻すことができます。ライセンスを返却するには、このセクションで説明されている手順に従ってください。

予約済みライセンスを返却するワークフローは次のとおりです。

1. 予約返却コード（Reservation Return Code）を生成します
2. Cisco SSM で Meeting Management インスタンスを見つけます
3. 予約返却コード（Reservation Return Code）を入力します

図 3：ライセンス予約を返却するためのワークフロー



予約済みライセンスを返却するには、次の手順に従います。

1. Meeting Management **設定**の「**ライセンス**」セクションの場合
   a. **[予約済みライセンスの返却...（Return Reserved Licenses...）]** ボタンをクリックして、**[返却ライセンスの確認（Confirm Return Licenses）]** ポップアップを起動します。
   b. **[生成（Generate）]** ボタンをクリックして、予約返却コードを生成します。
   c. [ライセンス予約返却コード（License Reservation Return Code）] ポップアップには説明テキストが表示され、ライセンス予約返却コードを含むファイルをコピーまたはダウンロードできます。
2. Smart Software Manager の場合
   a. 製品インスタンス**で Meeting Management インスタンスを見つけます**
   b. **[アクション（Actions）]** メニューから **[削除（Remove）]** を選択して、[製品インスタンスの削除（Remove Product Instance）] ポップアップを起動します。
   c. ポップアップに予約返却コードを入力して、予約済みライセンスの返却を完了します。**[ライセンス（Licensing）]** ページで、登録**ステータスが** [登録解除（Deregistered）] に変わります。

24.3.4 スマートライセンスに移行する際の考慮事項

1. 3.4 バージョンへのアップグレードには、既存の従来のライセンス ファイル（PAK ファイル）を使用できます。

2. 既存のライセンスファイル（部分的または完全に履行された PAK）をお持ちのお客様は、PAK ライセンスをスマートライセンスに変換するために、最初に購入した PAK を参照する必要があります。スマート アカウント名、ドメイン、使用中の仮想アカウントを提供して、スマート ライセンスへの手動変換を行うには、新しいグローバル ライセンス組織（GLO）リクエストを開く必要があります。

注：
- Cisco SSM を使用して PAK をスマート ライセンスに変換するセルフサービスは、新規のお客様のみが利用できます。
- 既存のライセンスからスマートライセンスへの変換は、GLO チームの助けを借りて行う必要があり、遅延が発生する可能性があります。

---

3. 90 日間の 1 回限りの試用モードを使用する必要がないように、3.4 バージョンにアップグレードする数日前にライセンスをスマートライセンスに変換する計画を立てる必要があります。
4. スマート ライセンス バーチャル アカウントに、過去 90 日間の Meeting Server の使用に十分なライセンスがあることを確認します。過度の使用の場合、Meeting Management はスマート ライセンスへの変換時に高レベルの施行を行う警告モードに入ります。高レベルの施行を行う警告モードになると、Meeting Management では 90 日間の試用が 1 回だけアラームを無音にすることができ、追加のライセンスを購入する時間を増やすことができます。
5. **バーチャルエディション CMS アクティベーション ライセンス（LIC-CMS-K9）はスマートライセンスに変換できません。代わりに、Cisco SSM は使用中の Call Bridge の数を自動的にカウントし、スマートアカウントの Call Bridge アクティブノード**の下に報告します。お客様は、使用中の Call Bridge の数を表示することしかできず、新しい Call Bridge ライセンスを追加することはできません。

25 オプション：クラスタを TMS に関連付ける

どの Call Bridgeが TMS に接続されているかを Meeting Management に通知し、その TMS システム ID を入力するには、次の手順を実行します。

1. **[サーバー（Servers）]** ページで、[クラスタと TMS の関連付け（Associate cluster with TMS）] をクリックします。
2. TMS のプライマリ Call Bridge である Call Bridge を選択します。
3. [TMS システム ID（TMS System ID）] を入力します。
4. **[完了（Done）]** をクリックして、Call Bridge の スケジュールされた会議の表示を開始します。

   Meeting Management は情報を確認し、クラスタの **[TMS に関連付けられている]** ステータスを表示し、TMS に接続されている Call Bridge は **[TMS]** というラベルを 取得します。
5. 予定されている会議を確認したいすべてのクラスタを検証するまで、この操作を繰り返します。

26 オプション：TMS 電話帳にアクセスします。

Meeting Management は TMS の電話帳にアクセスできます。そのためビデオオペレータは、参加者を会議に追加する際に連絡先を検索できます。TMS で連絡先を検索する場合と同じように検索できます。

注：TMS は、Meeting Servers で到達できない連絡先をサポートしている場合があります。Meeting Servers のアウトバウンド ダイヤル プランを更新するか、Meeting Server が到達できない電話帳のエントリを既存のダイヤルプランルールに従ってフィルタリングしてください。

ビデオオペレータが Meeting Servers からアクセスできない参加者を追加しようとすると、Meeting Management は接続を試み、失敗します。警告やエラーメッセージはありません。ビデオオペレータにはしばらくの間スピナーが表示され、その後、参加者が切断された参加者として、参加者リストに表示されます。

注：TMS では、表示される検索結果の数を構成できます。これは Meeting Management には影響を与えません。Meeting Management には常に最大 50 件の検索結果が表示されます。

ビデオオペレータが TMS の電話帳を使用するには、次の 3 つの手順を実行する必要があります。

- TMS に電話帳クライアントとして Meeting Management を追加します。

  電話帳には連絡が取れる連絡先だけが含まれるよう、まず最初に編集することを推奨します。

- TMS の Meeting Management に電話帳を割り当てます。
- Meeting Management での TMS 電話帳の使用を有効にします。

  注：これを行う前に、Meeting Management と TMS を接続する必要があります。

TMS に電話帳クライアントとして Meeting Management を追加するには、次の手順を実行します。

1. Meeting Management で、[設定（Settings）] ページ の **[TMS]** タブに移動します。
2. MAC アドレスをコピーします。
3. TMS にサインインし、[電話帳（Phone Books）] **に移動し、[Cisco Meeting Management の 電話帳（Phone Book for Cisco Meeting Management）]** に移動します。

   *Meeting Management の **[Cisco Meeting Management の電話帳（Phonebook for Cisco Meeting Management）]** リンクをクリックすると、TMS のサインイン後に正しいビューに直接移動します。*
4. **[新規（New）]** をクリックします。
5. [サーバ名（Server Name）] フィールドに、Meeting Management の名前を入力します。

   名前は、他の Meeting Management および TMS の管理者にとって意味があるものである限り、好きな名前を選択できます。
6. [MAC アドレス（MAC Address）] フィールドに、Meeting Management からコピーしたアドレスを入力します。

Meeting Management に電話帳を割り当てるには、次の手順を行います。

1. TMS で、**[電話帳（Phone Books）]** に移動し、**[Cisco Meeting Management の 電話帳（Phone Book for Cisco Meeting Management）]**に移動します。
2. TMS で Meeting Management に付けた名前をクリックします。
3. Meeting Management に使用する電話帳を選択してから、**[保存（Save）]** を 選択します。

電話帳の使用を開始するには、次の手順を実行します。

1. Meeting Management で、[設定（Settings）] ページ の **[TMS]** タブに移動します。
2. **[TMS 電話帳を使用する（Use TMS phonebook）]** チェックボックスをオンにします。
3. 上記のエリアで、Meeting Management から TMS に最初に接続した時に使用したアカウントのパスワードを入力してから**保存**し、Meeting Management を再起動します。

27 LDAP サーバーの設定

注：Meeting Management を構成して使用する前に、すべてのユーザグループを LDAP サーバー上で構成する必要があります。

27.1 LDAP サーバーの設定

LDAP サーバーを使用するように Meeting Management を設定するには、次の手順を実行します。

1. **[ユーザー（Users）]** ページで、**[LDAP サーバー（LDAP server）]** タブに移動します。
2. **[LDAP を使用する（Use LDAP）]** チェックボックスをオンにします。
3. プロトコルを選択します。

   LDAP は暗号化されていない TCP 接続用で、LDAPS はセキュアな接続用です（オプションで、認証に証明書信頼ストアを使用します）。
4. LDAP サーバーのサーバーアドレスとポート番号を入力します。

   デフォルトのポート番号：

   - *LDAP：389*
   - *LDAPS：636*

   注：AD を使用する場合で、ベース DN がドメインコンポーネント（DC）レベルにのみ設定されている場合は、デフォルトのポートを使用してグローバルカタログ（LDAPS ポート 3268、LDAPS ポート 3269）を検索します。

   注：LDAP サーバーアドレスがリテラルの IPv6 アドレスの場合は、角カッコで囲って入力します。

5. **オプション：証明書を**使用することを選択し、証明書が無効であり Meeting Management で接続を拒否する場合は、証明書失効リスト（**CRL**）に対して証明書**を確認します。**

   チェーン内の証明書が無効またはアクセスできない CRL がある場合、Meeting Management は接続をブロックします。

   可能な場合はこれを有効にすることを推奨します。

   注：HTTP 証明書配布ポイント（CDP）を備えた証明書のみがサポートされています。CRL チェックを使用し、証明書に CDP がない場合、または CDP が HTTP 経由で到達できない場合、接続は拒否されます。

   また、Meeting Management が HTTP 経由で外部アドレスに接続できるよう、ネットワークを構成する必要があります。

   ---

6. LDAPS を使用している場合は、[証明書のアップロード（Upload certificate）] をクリックして、LDAP サーバーの証明書チェーンを Meeting Management の信頼ストアに追加します。

   証明書の要件

   - *証明書チェーンには、LDAP サーバの証明書に署名した CA の証明書に加えて、ルート CA 証明書を含む証明書チェーン内の上位の証明書を含める必要があります。*
   - *LDAP サーバに入力したサーバアドレスは、LDAP サーバ証明書に含める必要があります。*

7. バインド DN とパスワードを入力します。

   Meeting Management を LDAP サーバーにバインド（認証）するユーザーアカウントのログイン情報です。

   注：これらのフィールドに入力する文字列はすべて、大文字と小文字が区別されます。

   ---

8. **[ベース DN（Base DN）]**（ベース識別名）を追加します。

   ベース識別名は、ディレクトリ検索の開始点です。Meeting Management は、このノード内の LDAP グループおよび LDAP ツリー内のすべてのノードを検索します。

   注：このフィールドは大文字と小文字を区別します。

   注：ベース DN がドメインコンポーネント（DC）レベルにのみ設定されている場合は、デフォルトのポートを使用してグローバルカタログ（LDAPS ポート 3268、LDAPS ポート 3269）を検索します。

   ---

9. **[検索属性（Search attribute）]** を選択します。

   検索属性は、Meeting Management にサインインするときにユーザがユーザー名として入力する LDAP 属性です。

   注：このフィールドは大文字と小文字を区別します。

10. **設定を保存して** Meeting Management **を再起動します。**

    注：今すぐ再起動するか、設定が完了するまで待ちます。

28 LDAP グループの追加

LDAP ユーザーグループは LDAP サーバー上で構成され、Meeting Management にマップされています。そのため、Meeting Management は、LDAP サーバーを使用して、サインイン時にグループのメンバーシップを確認してユーザを認証できます。

ユーザーと LDAP ユーザーグループの詳細については、「ご使用になる前に」の項を参照してください。

28.1 LDAP ユーザグループの追加

ユーザーグループを追加するには、以下を行います。

1. [ユーザー（Users）] ページで、**[LDAP ユーザーグループ（LDAP User Groups）]** タブに移動します。
2. **[LDAP グループの追加（Add LDAP group）]** をクリックします。
3. **LDAP パス**を入力します。
4. **[確認（Check）]** をクリックして、グループが見つかるか確認します。
5. グループが見つかった場合は、[ユーザーの表示（View users）] をクリックして、このグループに表示されるユーザー名が表示されたかを確認します。
6. グループのロールを選択します。
7. **起動するには、選択したユーザーに対する** [アクション（Actions）] **で使用可能な** [ユーザープロファイルの表示（View User Profile）] **ボタンをクリックし、**
   [ユーザープロファイル（User Profile）] **ポップアップウィンドウを起動します。**
8. **[タグの追加（Add Tags）]** フィールドでタグを割り当てます（オプション）。最大 10 個のタグを追加できます。

   これにより、管理者はビデオオペレータにタグを割り当て、タグ付けされたミーティングにのみアクセスできるようにすることができます。タグの追加の詳細については、『Meeting Management 管理者ガイド』を参照してください。
9. [次へ（Next）] をクリックします。
10. **オプション：[リンクをコピー（Copy link）] してユーザーに送信できます。**

    ここに表示されるリンクは、CDR 受信者アドレスです。チームがブラウザインターフェイスにアクセスするためにユーザに別のアドレスを提供する場合は、代わりにそのアドレスをユーザに与えます。
11. **[完了（Done）]** をクリックします。
12. Meeting Management を再起動します。

注：今すぐ再起動するか、設定が完了するまで待ちます。

29 オプション：ローカルユーザのセキュリティポリシーの設定

ローカルユーザーのセキュリティポリシーは、[ユーザー（Users）] ページの [ローカル設定（Local configuration）] タブで設定できます。次のポリシーを設定できます。

- [パスワードポリシーを強制（Enforce password policy）] して、最小パスワード長を要求します

  これは、選択するまで無効になります。デフォルトの最小長は 8 文字です

- パスフレーズ生成機能を使用して、組み込みのパスフレーズ生成機能を有効にします

  組み込みのパスフレーズ生成機能は、ディクショナリの単語を組み合わせ、新しいパスワードを提案します。パスフレーズ内のデフォルトの単語数は 5 で、1 ~ 8 の任意の数を選択できます。

  組み込みのパスフレーズ生成機能を使用する場合は、ディクショナリを提供する必要があります。ディクショナリの要件：

  - *ディクショナリは、各行に 1 つの単語を含むテキストファイルである必要があります。*
  - *文字は UTF-8 でエンコードされている必要があります。*
  - *ファイルに Null 文字を含めることはできません。*
  - *ファイルの最大サイズは 10 MB です。*

- パスワードの再使用ポリシーを強制して、パスワードの再使用を制限します

  これは、選択するまで無効になります。入力フィールドは、値を入力するまで空白です。

注：セキュリティポリシーの変更は、Meeting Management を再起動した後にのみ適用されます。今すぐ再起動するか、初期構成が完了するまで待ちます。

注：[パスワードポリシーの強制（Enforce password policy）]と[パスワードの再使用ポリシーの強制（Enforce password reuse policy）] **は、ユーザーが自分のパスワードを変更した場合にのみ適用されます。**

注：パスフレーズ生成機能が有効な場合、Meeting Management ではすべてのユーザのパスフレーズが提案されます。

- **パスフレーズ検証** を使用して、一般的に使用される単語、繰り返しまたは連続する文字を含むディクショナリと照合して、ユーザーパスワードの品質をチェックします。

  このリストには 、サービス名、ユーザー名、製品名、派生語などのコンテキスト固有の単語も含まれます。ユーザーが選択したパスワードがリストのいずれかに一致する場合、パスフレーズ検証機能はパスワードを拒否し、別の値を選択するようにユーザーに通知します。

  ディクショナリの要件：

  - *ディクショナリは、各行に 1 つの単語を含むテキストファイルである必要があります。*
  - *文字は UTF-8 でエンコードされている必要があります。*
  - *ファイルに Null 文字を含めることはできません。*
  - *ファイルの最大サイズは 10 MB です。*

  パスフレーズ検証を有効にするには、次の手順を実行します。

  1. [パスフレーズ検証を使用（ Use passphrase verifier）] まで下にスクロールし 、チェックボックスをオンにします。
  2. **[ディクショナリのアップロード（Upload dictionary ）] ボタンをクリックし、セキュリティ要件を満たさないパスフレーズのリストを含むテキストファイル（.txt）を選択します。**
  3. 既存のディクショナリ ファイルを削除するには、[削除（ remove）] をクリックします。

注：
• Meeting Management はデフォルトのディクショナリを提供しません。管理者は、ディクショナリを定義してアップロードする必要があります。
• Meeting Management のバックアップ時にディクショナリが存在する場合、そのディクショナリはバックアップ ファイルに含まれます。バックアップファイルが復元されると、ディクショナリも復元されます。

---

30 オプション：ローカルユーザの追加

[ユーザー（Users）]ページの **[ローカル（Local）]** タブで、ローカルユーザーアカウントを追加、削除、または編集できます。ユーザの詳細については、「ご使用になる前に」の項目を参照してください。

ローカル ユーザを追加するには、次の手順を実行します。

1. **[ユーザー（Users）]** ページで、**[ローカル（Local）]** タブに移動します。
2. **[ローカルユーザの追加（Add local user）]** をクリックします。
3. ユーザー名を入力します。

   注：ユーザ名は後で変更できませんので、詳細を保存する前に注意してください。

4. オプション：名と姓を入力します。
5. ロールを割り当てます。
6. 新しいパスワードを作成します。
7. パスワードを確認し、**[追加（Add）]** をクリックします。
8. **[タグの追加（Add Tags）]** フィールドに、タグを入力します。最大 10 個のタグを追加できます。

   これにより、管理者はビデオオペレータにタグを割り当て、タグ付けされたミーティングにのみアクセスできるようにすることができます。タグの追加の詳細については、『Meeting Management 管理者ガイド』を参照してください。

ローカル ユーザを削除するには、次の手順を実行してください。

1. **[ユーザー（Users）]** ページで、**[ローカル（Local）]** タブに移動します。
2. 削除するユーザーを見つけ、  [アクション（Actions）] 列の **をクリックします。**

注：現在サインインしている管理者アカウントは、絶対に削除できません。

ローカル管理者ユーザアカウントが 1 つだけで、それを削除する場合は、LDAP 管理者としてサインインしてからローカルアカウントを削除します。

ローカルユーザーの編集を編集するには、以下を行います。

1. **[ユーザー（Users）]** ページで、**[ローカル（Local）]** タブに移動します。
2. 削除するユーザーを見つけ、**[アクション（Actions）]** 列の **をクリックします。** 

3. 必要な変更を加えます。
4. **[完了（Done）]** をクリックします。

31 確認、保存、およびバックアップ

すべての詳細が正しく完了していることを確認してから、必要に応じて Meeting Management を再起動します。構成の保存に再起動が必要な場合は、画面の上部にバナーが表示されます。

構成のバックアップを取ります。これで Meeting Management を使用する準備が整いました。

32 バックアップと復元

Meeting Management に変更を加える前に、常に新しいバックアップを作成することを推奨します。バックアップには次が含まれます。

- **構成**：
  - ライセンス設定以外の **[設定（Settings）]** ページのすべての詳細
  - LDAP サーバーの詳細
  - すべての LDAP グループの詳細
  - ローカルユーザのセキュリティポリシー設定

これにはパスフレーズ生成機能の設定が含まれますが、ディクショナリの設定は含まれません

- **データベース**：
  - ローカルユーザの詳細（最近のパスワードのハッシュなど）
  - すべての Call Bridge の詳細（TMS システム ID を含む）
  - パスフレーズディクショナリ

32.1 バックアップの作成

Meeting Management の使用を開始する前に、バックアップを作成することを推奨します。その後、再展開する必要がある場合は、設定を簡単に再利用できます。

1. 再起動が必要な場合は、すべての設定を有効にできるよう、今すぐこれを行います。
2. **[設定（Settings）]** ページで、**[バックアップと復元（Backup and restore）]** タブに移動します。
3. **[バックアップファイルのダウンロード（Download backup file）]** をクリックします。
4. パスワードを入力し、**[ダウンロード（Download）]** をクリックします。
5. バックアップファイルとパスワードを安全な場所に保存します。

注：バックアップは暗号化されています。パスワードなしでは使用できません。

32.2 バックアップの復元

バックアップを復元する前に、次の手順を実行します。

- バックアップファイルとパスワードの準備ができていることを確認します。

パスワードは、ユーザまたは別の管理者がバックアップを作成した際に選択されました。

- すべての設定を復元するか、データベースまたは構成の詳細のいずれかだけを復元する

のかを決定します（以下の手順 4 を参照）。

- バックアップの復元中は、LDAP サーバーがオンライン上で実行されていることを確認してください。
- TMS が接続されている場合は、バックアップの復元中に TMS がオンラインであることを確認します。

注：復元中に LDAP サーバーまたは TMS がオフラインの場合、復元は失敗します。

注：LDAP の詳細を復元する場合は、ローカル管理者としてサインインしてバックアップを復元することを推奨します。

以前に保存したバックアップを復元するには、次の手順を実行します。

1. **[設定（Settings）]** ページで、**[バックアップと復元（Backup and restore）]** タブに移動します。
2. **[バックアップ ファイルのアップロード (Upload backup file)]** をクリックします。
3. バックアップファイルを選択します。
4. どちらかまたは両方のオプションを選択します。
   - **構成の復元**：
     - ライセンス設定以外の **[設定（Settings）]** ページのすべての詳細
     - LDAP サーバーの詳細
     - すべての LDAP グループの詳細
     - ローカルユーザのセキュリティポリシー設定

       これにはパスフレーズ生成機能の設定が含まれますが、ディクショナリの設定は含まれません
   - **データベースの復元**：
     - ローカルユーザの詳細（最近のパスワードのハッシュなど）
     - すべての Call Bridge の詳細（TMS システム ID を含む）
     - パスフレーズディクショナリ

   2 つのオプションのいずれかを確認しない場合は、バックアップを復元できません。
5. パスワードを入力し、**復元**します。

注：Meeting Management を復元するときにローカルユーザとしてサインインしている場合は、Meeting Management はバックアップからアカウントをリストに追加するか、バックアッププロファイルが現在の設定で更新されます。他のすべての設定は、バックアップの設定に置き換えられます。

32 アップグレードイメージを検証するためのキーのアップロード

Cisco Meeting Management は、イメージが本物か改ざんされているかを検証する署名をアップグレードイメージに埋め込みます。

イメージの署名は、署名付きイメージからアップグレードする場合にのみ検証されます。このため、署名されていないイメージから署名付きイメージにアップグレードする場合、つまり、3.6 から 3.7 へのアップグレード、または旧バージョンへのダウングレードでは、引き続き手動でハッシュを検証することを推奨します。この機能は、3.7 以降からアップグレードするときに完全に有効になります。

バージョン 3.7 から、特別なビルドにアップグレードするには、特別なキーをアップロードする必要があります。**[キーのアップロード（Upload Key）]** ボタンが導入され、管理者が公開キーをアップロードしてアップグレードイメージを確認できるようになりました。ただし、管理者は、特別なビルドにアップグレードする場合にのみ、このアクションを実行します。

公開鍵をアップロードするには:

1. [設定（Settings）] **ページの [アップグレード（Upgrade）]** タブに移動します。
2. [キーのアップロード] をクリックし、公開キーを参照して選択します。選択した公開鍵が検証され、アップロードされます。

注：署名された製品／特別なビルドから別の署名された製品ビルドへのアップグレードは、管理者からのアクションを必要としません。Meeting Management は、ハッシュを手動で検証することなく、アップグレードイメージを自動的に検証します。

---

33 Meeting Management の再起動

Meeting Management のほとんどの設定は、適用する前に再起動する必要があります。Meeting Management を再起動するには、次の手順を実行します。

1. **[設定（Settings）]** ページの [再起動（Restart）] タブに移動します。
2. **[再起動（Restart）]** をクリックします。

注：Meeting Management を再起動すると、すべてのユーザが警告なくサインアウトされ、会議に関する情報はすべて Meeting Management から削除されます。再起動後もアクティブな会議の開始時間と、引き続き接続されている参加者の参加時間は、API 要求によって元に戻されます。会議の詳細に表示される時間は正しいですが、イベントログのエントリには新しいタイムスタンプが与えられます。

アクセシビリティの注意事項

シスコは、利用しやすい製品およびテクノロジーの設計および提供に取り組んでいます。

Cisco Master Project の Voluntary Product Accessibility Template（VPAT）は、以下で入手可能です。

http://www.cisco.com/web/about/responsibility/accessibility/ legal_ regulatory/vpats.html#telepresence

アクセシビリティの詳細については、以下を参照してください。

www.cisco.com/web/about/responsibility/accessibility/ index.html

34 アクセシビリティ サポート機能

34.1 キーボード ナビゲーション

キーボードを使用して Meeting Management 内を移動できます。

- Meeting Management の領域間を移動するには、 **Tab キー**を使用します。アウトラインで囲まれた領域にフォーカスがあるることがわかります。**Shift + Tab キー**を使用すれば、前のフォーカスエリアに移動できます。
- 項目を選択するには、スペースバーまたは Enter キーを使用します。
- 矢印 キーを使用して、リストまたはドロップダウンメニューをスクロールします。
- 開いている画面/メニューを閉じるには、 **Esc キー**を使用します。

34.2 スクリーン リーダーのサポート

JAWS スクリーンリーダーバージョン 18 以降を使用できます。

スクリーンリーダーは、フォーカスされた領域/ボタン、画面に表示される通知、警告、ステータスメッセージ、および実行できるアクションなどの関連情報を読み上げます。

例：[スペースの作成（Create Space）] ボタンにフォーカスすると、スクリーンリーダーは「スペースの作成（ Create Sapce）」と読み上げるので、スペース名を入力します。

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表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。製品の利用に関するすべての責任はユーザーが負わなければなりません。

対象製品のソフトウェアライセンスと限定保証は、製品に添付された『Information Packet』に記載されており、この参照により本マニュアルに組み込まれるものとします。このソフトウェアライセンスまたは限定保証を見つけられない場合は、CISCO の代理店に連絡しコピーを入手してください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

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

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、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 IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

この文書の印刷されたハード コピーおよび複製されたソフト コピーは、すべて管理対象外と見なされます。最新版については、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