Cisco Meeting Management

Cisco Meeting Management 3.6

管理者向けユーザーガイド

2022 年 8 月 23 日

Cisco Systems, Inc. www.cisco.com

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
2022-08-23	ドキュメントを公開。

1 はじめに

このガイドは、Cisco Meeting Management の管理者を対象としています。

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
- 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会議の表示
- 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。

1.1 3.6 の新機能

新機能と変更の全体の概要については、リリースノートを参照してください。このリリースでは、次のセクションを更新しました。

- Meeting Management での PCAP ファイルのキャプチャ：Meeting Management は、パケット キャプチャをサポートするようになりました。

1.2 ソフトウェア

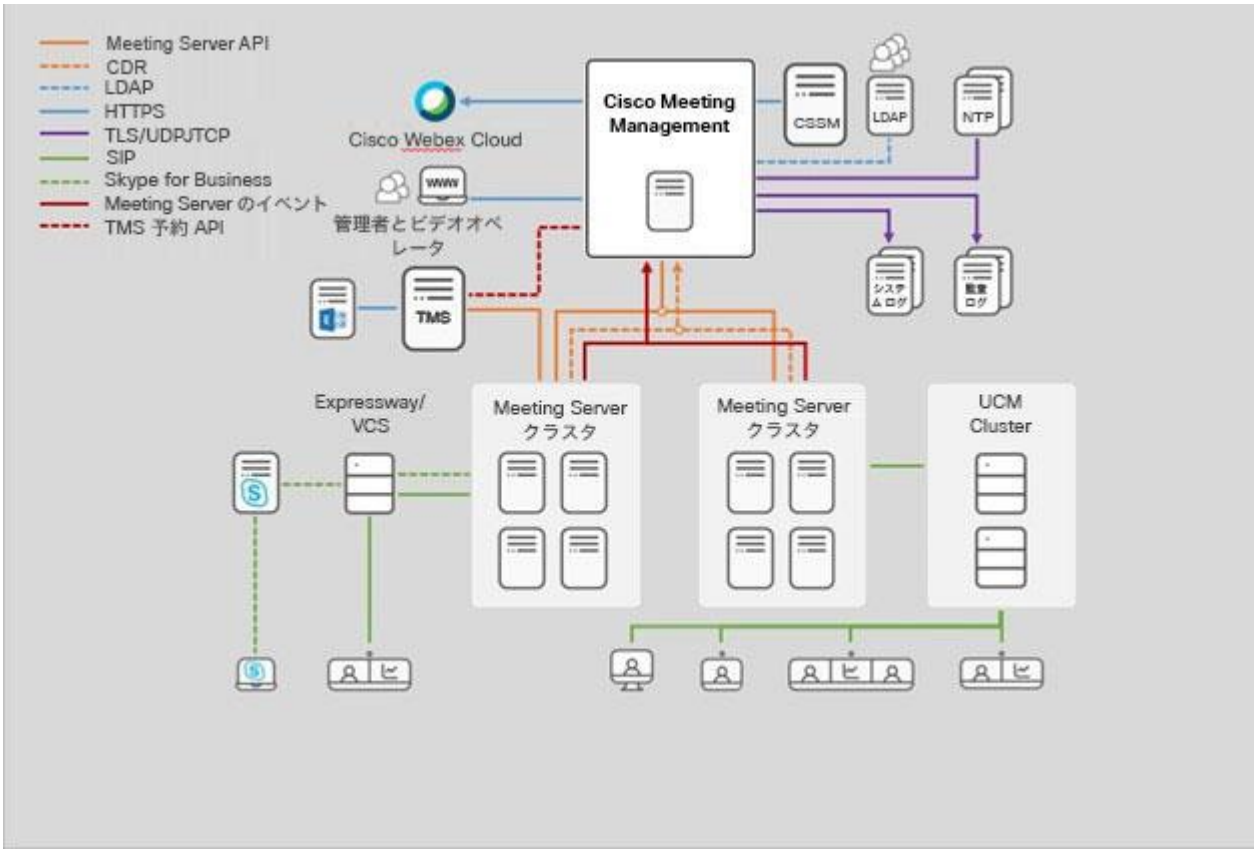
Meeting Management は仮想化されたアプライアンスです。VM（仮想マシン）の仕様は、Meeting Management が実行またはモニタリングする必要のある同時アクションの数によって異なります。仕様と要件については、管理している Call Bridge の数に関連するサイジングの見積もりを含め、『*インストールおよび構成ガイド*』を参照してください。

セキュリティのため、最初の実行後はコンソールにユーザアクセスできません。インストールプロセスを除き、Meeting Management はすべてブラウザ インターフェイスを介して使用します。

2 環境の概要

Meeting Management の 1 つのインスタンスは、以下に示すように、単一の Call Bridge のみを持つ小規模な Meeting Server 展開、または複数の Call Bridge クラスタを持つ大規模な Meeting Server 展開を管理できます。

図 1：Meeting Server 展開内の単一の Meeting Management



Meeting Management は、Call Bridge API を介して Meeting Server に接続します。アクティブな会議に関する情報を取得するために、各 Call Bridge において、CDR （コール詳細レコード）の受信側、そしてイベントクライアントとしてインストールすることで、API 要求、CDR、および Meeting Server イベントを介したアクティブな会議に関する情報を取得します。

注：クラスタのライセンスとプロビジョニングに Meeting Management のみを使用することを選択した場合、Meeting Management は、そのクラスタの Call Bridge の CDR の受信側またはイベント クライアントとして機能しません。

信頼性と正確性を高めるために、複数の NTP サーバーを構成できます。Meeting Management は、最大 5 つの NTP サーバーをサポートします。すべての Meeting Server と Meeting Management のすべてのインスタンスを同じ NTP サーバーに接続することをお勧めします。

2.1 ユーザの認証

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** は Meeting Management の [**ユーザ**（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 サーバー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 サーバーを使用して、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：すべてのユーザは、管理者またはビデオオペレータのいずれかになります。それらのアクセス許可は、ローカルで管理されているか LDAP 経由で管理されているかではなく、ロールのみに依存します。

2.2 セキュリティおよび監査

Meeting Management は、Web インターフェイスおよび接続されたサーバーへの安全な接続のために TLS 1.2 をサポートします。

バックアップ ファイルは、ユーザが指定したパスワードで保護されます。

アクティブな会議と最近の会議のイベント ログは、Meeting Management で利用できます。監査ログとシステム ログは、外部の syslog サーバーに送信できます。

また、特定の設定が必要な場合、高度なセキュリティ設定を組織のセキュリティポリシーに準拠させます。

2.3 診断とトラブルシューティング

Meeting Management は、限られた量のシステム ログをローカルに保存します。すべての監査ログとシステム ログは、外部サーバーに送信できます。

クラッシュ ログとログ バンドルは、サポート目的で利用できます。

Call Bridge の詳細、ローカル ユーザ アカウント、およびパスフレーズ ディクショナリは、他の設定の詳細とは別に復元できます。

2.4 Cisco TelePresence Management Suite（TMS）との統合

Cisco Meeting Management は TMS と統合できるため、Meeting Management を使用して会議を監視および管理しながら、TMS スケジューリング、エンドポイント管理、および電話帳機能を使用できます。

Meeting Management は予約 API を介して TMS に接続し、5 分ごとに電話帳にアクセスできることを確認し、スケジュールされた会議に関する情報を更新します。今後の会議は、スケジュールされた開始時刻の最大 24 時間前に Meeting Management に表示されます。

Meeting Management と TMS 間のよりシームレスな管理のために、スケジュールされた各会議には、Meeting Management の会議の詳細から TMS の編集ページへの直接リンクがあります。

2.5 Meeting Server のライセンス

ライセンスの目的での Meeting Server 3.0 以降では、Meeting Management が必須です。スマート ライセンスを使用している場合は、Cisco Smart Software Manager に接続する必要があります。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、ライセンス予約を導入しました。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。詳細については「ライセンス」セクションを参照してください。

注：Cisco スマート ライセンス ポータルルート CA は 2023 年 2 月に更新されます。スマート ライセンス（オンライン、SLR、または PLR）を使用している場合は、新しいライセンスの追加、Call Bridge の追加、または手動同期の実行中に、3.6 以降にアップグレードすることをお勧めします。

2.6 スマート ライセンスのための Cisco Smart Software Manager への接続

Meeting Management を使用して、Cisco Meeting Server の展開で購入したライセンスよりも多くのライセンスが使用されているかどうかをモニタリングできます。

Meeting Management は、Smart Agent を使用して Cisco Smart Software Manager（Cisco SSM）と通信します。Meeting Management は、毎日の使用状況レポートを Cisco SSM に送信し、Cisco SSM は、展開が準拠しているかどうかを報告します。

注：たとえば、復元力を追加するために、同じ Meeting Server クラスタに複数の Meeting Management のインスタンスが接続されている場合は、Meeting Management の 1 つのインスタンスのみを Cisco Smart Software Manager に接続する必要があります。両方のインスタンスを接続すると、報告された使用量は 2 回カウントされます。

2.7 電子メールまたは Webex Teams 通知用の Cisco Meeting Server Cloud Connector

Webex Control Hub に接続して、Webex Control Hub インターフェイスから Meeting Management 展開のステータスを確認し、電子メールまたは Webex Teams アラートを設定できます。

Cloud Connector は、製品を改善できるようにシスコにも統計を送信します。送信される情報については、Cisco Meeting Server Cloud Connector オンライン ヘルプを参照してください。

2.8 Meeting Server クラスタでのユーザのプロビジョニングとスペース テンプレートの作成

Meeting Management を使用して、1 つ以上の LDAP サーバーから接続された Meeting Server クラスタにユーザをインポートすることにより、Cisco Meeting Server Web アプリケーション ユーザをプロビジョニングできます。Web アプリのユーザが新しいスペースを作成するために使用できる事前構成済みのスペース設定であるスペース テンプレートを作成することもできます。

Meeting Management は、この目的のために LDAP サーバーと直接通信していないことに注意してください。代わりに、LDAP サーバーの詳細とフィルタ設定が Meeting Server に送信され、Meeting Server は LDAP 同期がトリガーされたときにその詳細を使用してユーザをプロビジョニングします。

注：セキュリティと監査上の理由から、各それぞれの LDAP サーバーの Meeting Server クラスタ用に、個別のバインドユーザアカウントを作成することを推奨します。

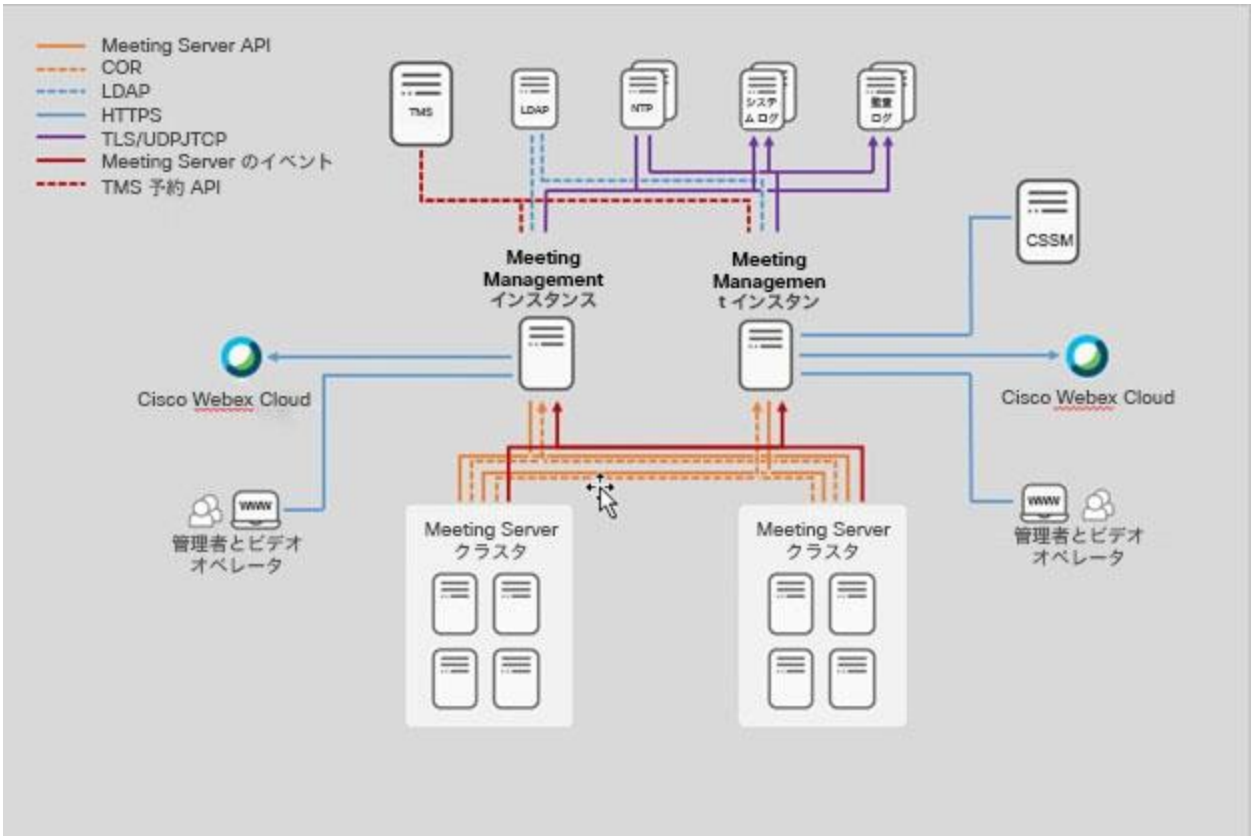
2.9 復元力

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。これらは個別に設定する必要があります。どちらも接続されている Call Bridge および TMS サーバー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一度に影響を与える可能性があります。

フェイルオーバーはありません。両方のインスタンスは常にアクティブであり、リストの一番上に会議を固定するなど、Meeting Management にローカルな設定は、それらが設定された Meeting Management のインスタンスでのみ表示されます。

注：復元力のある展開の場合は、レポートの重複を避けるために、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。「ライセンス」を参照してください。

図 2：復元力のある Meeting Management の展開



2.10 大量の会議がある場合のキャパシティ制限

Meeting Management 機能のパフォーマンスは、接続された Call Bridge での会議の量によって異なります。キャパシティの制限については、『*Installation and Configuration Guide*』の「始める前に」セクションの容量表を参照してください。大規模な展開のキャパシティを超える展開がある場合は、Meeting Management 機能を無効にする必要があります。これは、接続されたクラスタごとに個別に実行できます。

2.11 Cisco Meeting Server API またはサードパーティ ツールを使用している場合

Meeting Management を使用して会議をモニタリングまたは管理すると同時に、API（または API を使用するサードパーティ ツール）を使用してアクティブな会議を管理しないことを強くお勧めします。

3 概要 - 通知、Cloud Connector ステータス、およびライセンス ステータスの表示

[**概要**（Overview）] ページでは、システム通知と Webex Edge ステータスをいつでも確認できます。

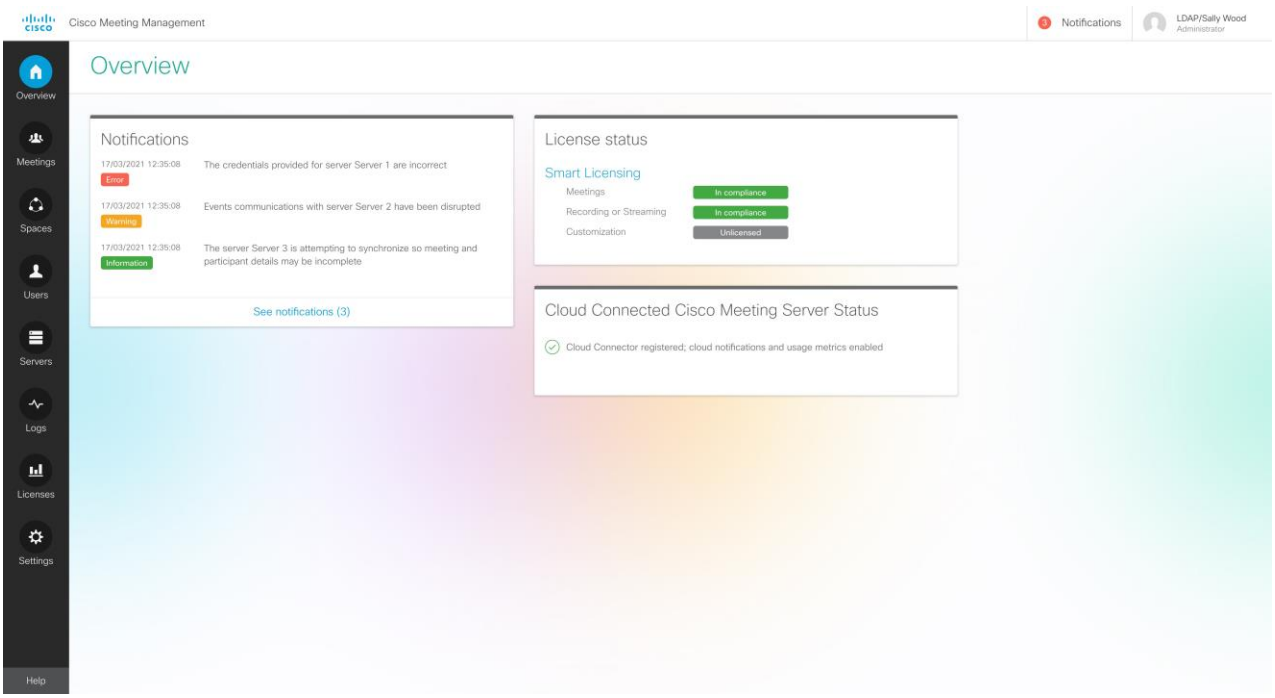
通知は常に [**概要**（Overview）] ページに表示され、トップ バーのカウンターは、現在の通知があるかどうかを示します。

通知には、3 段階のシビラティ（重大度）があります。

- **エラー**（Error）：重大レベルの問題
- **警告**（Warning）：Meeting Management の実行を継続するために対処する必要がある問題
- **情報**（Information）：有用な情報または軽微な問題

サインインしている Meeting Management のインスタンスでライセンスが有効になっている場合は、Cisco Meeting Server のライセンス ステータスも表示されます。

Meeting Management がスマートライセンスを使用している場合、ライセンスステータスは接続されているすべてのクラスタで同じです。青い**スマートライセンス**の見出しをクリックすると、詳細を表示および編集できる [**ライセンス**（Licenses）] ページに移動します。



注：トップバーの通知数は 30 秒ごとに更新されるため、[**概要**（Overview）] ページに表示される数と一時的に異なる場合があります。

4 会議 - 会議のモニタリングと管理

*[**会議**（Meetings）]* ページでは、ビデオオペレータとして会議を監視および管理することができます。手順については、*ビデオオペレータのユーザーガイド*、 オンライン ヘルプ、および ナレッジ ベースの記事*を参照してください。*

5 ブラストダイヤル - スペース管理とブラスト ダイヤル構成

Meeting Management はブラスト ダイヤルをサポートしており、ユーザグループとの会議をすばやく開催できます。

ブラストダイヤルを設定するスペースに、あらかじめ決められた参加者のリストを追加できます。参加者がスペースにダイヤルインすると、他のすべての参加者が同時にダイヤルアウトします。

参加者は DTMF の数字 1 を押して会議に参加し、* を押して通話を拒否できます。参加者が * を押して通話を拒否すると、Meeting Management は参加者の再ダイヤルを停止します。参加者は、[**却下**（Decline）] または [**拒否**（Reject）] ボタンを押して通話を拒否することもできます。

注：他の DMTF 番号はすべて無視され、Meeting Management は参加者が 1 または * を押すまで、参加者に再ダイヤルし続けます。

5.1 スペースの管理

Meeting Management には、クラスタ上のスペースを表示し、ブラストダイヤルを構成できるスペースが含まれています。これらは、Web アプリまたはプロビジョニングを使用して作成されたスペースです。Meeting Management では、スペースを作成したり参加者を招待したりすることはできませんが、ブラストダイヤルを設定するためのプラットフォームが提供されます。

5.1.1 スペースの表示

管理者は、クラスタ内のすべてのスペースの一覧を表示できます。スペース名をクリックすると、そのスペースの [参加情報（Join Information）] ページに移動します。検索バーを使用して、探しているスペースを絞り込みます。

5.1.2 参加情報

[参加情報（Join information）] タブには、会議の詳細 (可視性、会議 ID、パスコード、ビデオ アドレス) が表示されます。

5.2 ブラストダイヤル構成

ブラスト ダイヤルは、そのクラスタで会議を管理するように Meeting Management が設定されているクラスタに対してのみ設定できます。

- クラスタが Meeting Management によって管理されていない場合は、次のメッセージが表示されます。

  この Meeting Management はこのクラスタ上の会議を管理しないため、ブラストダイヤルをこのスペースに設定することはできません。これを変更するには、サーバーにアクセスしてこのクラスタを編集します。

  ［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。

- ブラスト ダイヤル モニタリングがオフになっている場合は、次のメッセージが表示されます。

  この Meeting Management ではブラストダイヤルの監視がオフになっているため、このスペースではブラストダイヤルを設定できません。これを変更するには、[設定（Settings）] > [ブラスト ダイヤル モニタリング（Blast dial monitoring）] にアクセスします。

  [設定（Settings）] に移動し、[ブラスト ダイヤル モニタリング（Blast dial monitoring）] で設定を変更します。

5.2.1 設定

ランディングページでは、次の構成を設定できます。

- **オン/オフ**：ブラスト ダイヤル設定のランディングページで、ブラスト ダイヤル機能をオンまたはオフにすることができます。オンにすると、他の設定オプションが表示されます。
- **再試行**：この設定では、連絡先が最初に通話に接続しなかった場合の再試行の試行を構成できます。
  - **再試行回数**：連絡先が通話に接続できなかった場合に、システムが連絡先へのダイヤル アウトを試行する最大回数。
  - **再試行失敗後の時間**：連絡先へのダイヤルアウトを再試行する前にシステムが待機する最小時間。デフォルト値は 180 秒です。

- **ブラスト ダイヤル参加者の自動参加 ：**グローバル レベルと参加者レベルの両方でオーディオ プロンプトをオンまたはオフにすることができます。オーディオ プロンプトが無効になっている場合、オーディオ プロンプト「Press 1 to enter the meeting or * to hang up」は再生されず、参加者は、通話を受け入れるときに DTMF 番号を押して会議に参加する必要はありません。管理者は、会議の特定の参加者の音声プロンプトを無効にすることもできます

  各参加者に利用可能な 📣 アイコンを使用します。

注：グローバルレベルで音声プロンプトを有効または無効にすると、参加者レベルの設定が上書きされます。

5.2.2 ダイヤルアウト連絡先の追加

ブラストダイヤル連絡先のリストに参加者を追加するには、2 つの方法があります。[**連絡先を追加**（Add contact）] ボタンを使用して一度に 1 つずつ手動で追加するか、CSV オプションを使用して、名前やビデオ アドレスなどの連絡先の詳細を含む CSV ファイルをアップロードすることができます。

連絡先の追加

担当者を追加するには、次の手順に従います。

1. [**連絡先の追加**（Add Contact）] をクリックします。[**ダイヤルアウト連絡先の追加**（Add dial-out contact）] ウィンドウが開きます。
2. 連絡先の名前と住所を入力します。
3. [**参加者の接続にプロンプトが必要**（Require prompt to connect participant）] を使用して、オーディオ プロンプト オプションを有効または無効にします。
4. [**完了**（Done）] をクリックします。連絡先の詳細が連絡先のリストに追加されます。関連するボタンを使用して、リストから連絡先を編集または削除できます。

CSV **をアップロード**

CSV ファイルのアップロードする方法は次のとおりです。

1. CSV ドロップダウンをクリックして、連絡先の名前、住所、音声プロンプト オプションを含む .csv ファイルをアップロードします。

ヒント：空の CSV テンプレートをダウンロードし、そのファイルを使用して、連絡先と対応する音声プロンプト オプションを追加できます。

---

2. [CSV **をアップロード**（Upload CSV）] オプションを使用して .csv ファイルをアップロードします。

   注：いずれかのオプションを使用して連絡先を既に追加している場合、追加された連絡先は上書きされ、新しくアップロードされた CSV 連絡先のみが追加されます。

3. ファイルがアップロードされると、[CSV **のダウンロード**（Download CSV）] オプションが有効になります。[CSV] ドロップダウンで、[CSV **のダウンロード**（Download CSV）] を選択して、既存の CSV をダウンロードし、コンテンツを編集して、再度アップロードすることができます。

注：
- CSV ファイルに無効な文字が含まれている場合、ファイル形式が正しくない場合、最大ファイル サイズを超えている場合、または許可されている連絡先の数を超えている場合は、推奨される解決策を示すエラー メッセージが表示されます。メッセージ内の手順に従って、エラーを修正し、ファイルをアップロードします。
- .csv ファイルで提供されるオーディオ プロンプトの値は大文字と小文字が区別され、無効な値が入力されるか空白のままになっていると、デフォルトで無効になります。

6 ユーザ - ユーザの追加またはユーザ設定の編集

6.1 ユーザについて

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 は** Meeting Management **の** [ユーザ（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 サーバー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 サーバーを使用して、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：LDAP 属性名は、大文字、小文字を区別します。

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。
- **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。

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。

6.2 LDAP サーバーの詳細の編集

LDAP サーバーの詳細は、インストール プロセス中に入力されます。詳細については、*インストールおよびコンフィギュレーション ガイド [英語]* を参照してください。

LDAP サーバーの詳細を編集するか、証明書を置き換える必要がある場合は、ローカル管理者ユーザとしてサインインすることをお勧めします。これは、詳細に問題がある場合にサインインできることを確認するためです。

LDAP サーバーの詳細の編集方法は次のとおりです。

1. ローカル管理者としてサインインします。
2. 関連する変更を行います。

   要件と詳細な手順については、インストール ガイドを参照してください。
3. [**認証**（Authorization）] セクションまで下にスクロールし、LDAP バインド ユーザのパスワードを入力します。
4. **変更を保存**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。

6.3 LDAP グループの追加

LDAP ユーザグループは 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。

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

6.3.1 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。

1. [**ユーザ**（Users）] ページで、[LDAP **ユーザグループ**（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. [次へ（Next）] をクリックします。
8. オプション：**リンクをコピーして**ユーザに送信できます。

   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。
9. [**完了**（Done）] をクリックします。
10. Meeting Management の**再起動**

    注：今すぐ再起動するか、設定が完了するまで待ちます。

6.4 ローカルユーザのセキュリティポリシーの設定

ローカルユーザのセキュリティポリシーは、[**ユーザ**（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。

注：**パスワードポリシーの強制**と**パスワードの再使用ポリシーの強制**は、ユーザ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。

6.5 ローカルユーザの追加

[**ユーザ**（Users）]ページの [**ローカル**（Local）] タブで、ローカルユーザアカウントを追加、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**（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：ユーザー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。

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**（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。

7 サーバー - サーバーの追加または編集

[**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。

サーバーの展開が成功すると、正常に構成されたすべてのサーバーが [**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サーバーは、[**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、ユーザのプロビジョニングを設定し、スペーステンプレートを 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。

7.1 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**と**パスワード**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**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**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。

9. 注：これは、後でクラスタ設定を編集することで変更できます。 クラスタの Meeting Management を無効にするを参照してください。

10. 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 [会議（Meetings）] ページには表示されません。

11. [**追加**（Add）] をクリックします。
12. オプション：**クラスタを編集**して、ユーザだけでなく他のすべてのユーザ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. 詳細を編集します。
3. [**完了**（Done）] をクリックします。

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。

7.2 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。

7.2.1 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。サーバーのリセット方法

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ログインし、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。

7.2.2 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

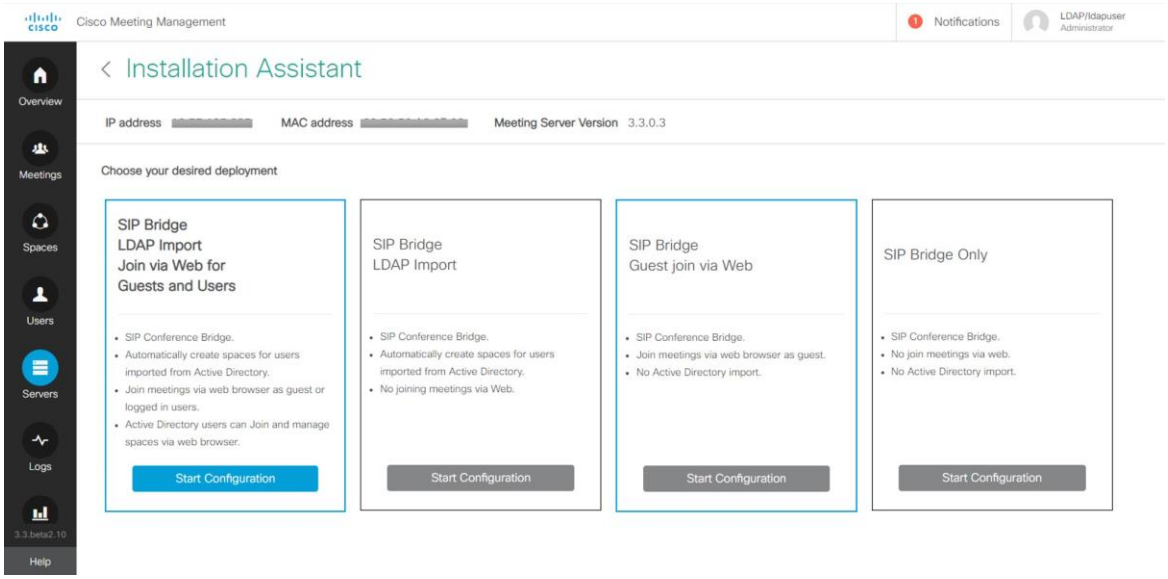
- ユーザのインポートを設定する場合は、ネットワークの LDAP ディレクトリに対して、場所、ログイン情報、LDAP ユーザの場所の詳細など、接続に関する詳細情報が必要になります。
- 証明書を使用してサーバーを設定する場合（推奨）、Meeting Server 用の FQDN を選択し、DNS サーバ ーレコードで定義する必要があります。
- 証明書を使用してサーバーを設定する場合（推奨）、認証局によって証明書要求が署名されている必要があります。インストール アシスタントは、証明書要求の生成に役立てることができます。また、既存の証明書とキー ペアを使用することもできます。

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**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、構成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、会議ユーザを除く構成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
   - 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、[**プッシュ構成**（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。

---

8 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（Cisco Meeting Server, Certificate Guidelines Single Combined Server Deployments Guide）』を参照してください。

8.1 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。

8.1.1 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**として CA **署名**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 2：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	サブドメインの使用を推奨します。	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。

8.1.2 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**として CA **署名**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。

8.2 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。

自己署名入りの証明書を使用する手順は次のとおりです。

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。

9 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.以下を設定します。

フィールド名	説明	アクション
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。	[**サーバーの追加**（Add Server）] をクリックします。NTP サーバーのアドレスが Cisco Meeting Server に追加されます。
タイム ゾーン（Time zone）	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 サーバーのアドレスが 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 ブリッジ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。

9.1 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。

10 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。

11 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。

---

12 会議ユーザ

会議ユーザパネルでは、LDAP ユーザをインポートして Cisco Meeting Web App にログインできます。

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 3：LDAP 接続の設定

フィールド名	説明	入力
サーバーアドレス（Server address）	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（Username）	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。

12.1 LDAP 検索とユーザ 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 4：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。
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**

フィールド名	説明	入力
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。

13 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。

14 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。

14.1 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。

15 クラスタの Meeting Management を無効にする

ライセンスとプロビジョニングのみに Meeting Management を使用する場合は、個々のクラスタの Meeting Management を無効にすることができます。これは、他のツールのために CDR 容量を解放したい場合、クラスタにテナントがある場合、またはクラスタが大量の会議をホストしている場合に役立ちます。Meeting Management の容量については『*インストールおよび設定ガイド*』を参照してください。

クラスタの Meeting Management を無効にする方法は次のとおりです。

1. [サーバー（Servers）] ページに移動します
2. [クラスタの編集（Edit Cluster）] をクリックします。
3. [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

   Meeting Management は、クラスタ内の Call Bridge 上の CDR レシーバおよびイベント クライアントではなくなり、クラスタ内の Call Bridge でホストされる会議に関する情報の要求を停止します。

   注：新しいクラスタの場合、クラスタに最初の Call Bridge を追加する際にこれを設定できます。

   ---

16 プロビジョニング

Meeting Management を使用して、接続された Meeting Server にユーザとスペース テンプレートをプロビジョニングできます。

[**サーバー**（Servers）] ページからプロビジョニング設定にアクセスできます。プロビジョニングを設定するクラスタについて、[**プロビジョニングの設定**（Set up provisioning）] をクリックして、プロビジョニング設定を構成できるページに移動できます。

16.1 スペースとは？

スペースは、参加者が電話またはビデオ会議を行うためにダイヤルできる仮想会議室です。スペースのすべてのメンバーは、スペースにアクセスしてアプリで表示できます。これは、すべてのメンバーが鍵を持ち、いつでも入室できる共有の会議室に似ています。スペースのメンバーは、他の人を会議に招待することができます。

スペースとは何か、アプリがどのように機能するかの詳細については、Web アプリのユーザーガイドとビジュアル「ハウツー」ガイドおよび重要事項のドキュメントを参照してください。

16.2 スペース テンプレートとは？

スペース テンプレートは、新規のスペースの作成に使用できる事前設定の組み合わせです。最も基本的な設定は参加者に関連しています。

- スペースに存在する参加者のロールと、各役割が持つ権限

  たとえば、一部の参加者は主催者またはリーダーのロールを持ち、人の追加または削除、録画の開始、他の人のミュートなどの完全な権限を持つことができ、他の参加者は制限付きの権限を持つゲストまたはスタッフのロールを持つことができます。すべてのメンバーが同じ権限を持った 1 つのロールのみのスペースを使用することもできます。

- 参加者の役割をパスコードで区別する必要があるかどうか、それぞれに一意の URI と会議 ID があるかどうか

また、デフォルトのレイアウト、会議を自動録画するかどうか、参加者に制限があるかどうかなど、スペースで開催される会議の動作に関連する設定もあります。

16.3 プロビジョニング手順

プロビジョニングの設定には、LDAP フィルタの設定、スペース テンプレートとその他のいくつかの設定の定義、および変更のコミットが含まれます。

1. 始める前に、準備を整えておきましょう。
2. クラスタを LDAP サーバーに接続します。
3. インポートするユーザを定義します。
4. 自動的にスペースを作成します。
5. ユーザのスペース作成を許可します。
6. 設定を確認してコミットします。
7. プロビジョニングを実行するには、LDAP 同期を開始します。

16.4 プロビジョニング - 始める前に

16.4.1 サポートされている LDAP 実装

Meeting Server は、次の LDAP 実装をサポートしています。

- Microsoft Active Directory（AD）
- OpenLDAP
- Oracle Internet Directory（LDAP バージョン 3）

Meeting Server の各バージョンでテストされたバージョンについては、相互運用性データベースを参照してください。

注意：Meeting Server の Web 管理インターフェースを介して LDAP を設定している場合、Meeting Management を介したプロビジョニングは機能しません。Meeting Management でプロビジョニングを設定する前に、Web 管理インターフェイスにサインインし、[**構成**（Configuration）]、[Active Directory] ページに移動し、すべての入力フィールドを空にしてから、[**送信**（Submit）] をクリックします。ユーザのロックアウトを避けるため、Meeting Management でのプロビジョニングの設定が完了するまでは同期しないでください。

16.4.2 LDAP サーバーの詳細

Meeting Server クラスタを接続する LDAP サーバーごとに、以下が必要です。

- プロトコル（LDAP/LDAPS）

  LDAPS を使用することをお勧めします。

- LDAP サーバー アドレス
- LDAP サーバーポート番号

デフォルトは LDAP の場合は 389、LDAPS の場合は 636 です。ポート 636 で LDAPS を使用することをお勧めします。

証明書の検証を使用する場合：Meeting Server に LDAP サーバー証明書をアップロードし、TLS 証明書の検証を有効にします。

- *証明書の検証を使用することをお勧めします。これを行う方法については、FAQ 記事「LDAP サーバー証明書の検証を有効にするにはどうすればよいですか？」を参照してください。*
- LDAP バインドユーザのログイン情報

  セキュリティと監査上の理由から、Cisco Meeting Server 用に、個別のバインドユーザアカウントを作成することを推奨します。

16.4.3 ユーザーインポートの詳細

インポートするユーザのグループごとに、次のものが必要です。

- 基本識別名（DN）
- LDAP 検索フィルタ
- サインイン ユーザー名のマッピング

  *これは、LDAP サーバーを Meeting Management に接続するときの**検索属性**と呼ばれるものに対応します。これは、Meeting Server Web アプリのユーザーがアプリへのサインインに使用するユーザー名として使用する LDAP 属性を定義します。$sAMAccountName$@example.com のような形式である必要があり、属性はユーザごとに一意である必要があります。*
- 表示名のマッピング

  これは、アプリ ユーザの表示名として使用する LDAP 属性を定義します。cn のような形式にする必要があります。
- 十分な PMP Plus ライセンス

  グループのインポート設定は、グループ内のユーザに個人ライセンスを割り当てるかどうかを定義します。ユーザに個人ライセンスを割り当てる場合は、グループ内のユーザごとに 1 つの PMP Plus が必要です。

  ユーザをプロビジョニングする前にライセンスをインストールする必要はありませんが、Meeting Server の使用を開始する前にそれらをインストールする必要があります。

Cisco Meeting Server での LDAP の使用の詳細については、該当する『Meeting Server 導入ガイド』を参照してください。LDAP 設定に関するセクションと、LDAP フィールド マッピングに関する詳細情報を含む付録があります。

16.5 プロビジョニング - LDAP サーバー

ユーザとスペース テンプレートをプロビジョニングする最初の手順は、Meeting Server がユーザをインポートする 1 つ以上の LDAP サーバーに Meeting Server クラスタを接続することです。

[**プロビジョニング**（Provisioning）] ページの [LDAP **サーバー**（LDAP servers）] タブで、クラスタが LDAP サーバーへの接続に使用する詳細を入力できます。

16.5.1 LDAP サーバーの追加方法

クラスタを LDAP サーバーに接続する方法は以下のとおりです。

1. Meeting Management で、[**サーバー**（Servers）] ページに移動し、[**プロビジョニングの設定**（Set up provisioning）] をクリックします。
2. [LDAP **サーバー**（LDAP Servers）] タブで、[LDAP **サーバーの追加**（Add LDAP Server）] をクリックします。
3. オプション：自分や他の Meeting Management 管理者にとってわかりやすいサーバー名を入力します。
4. 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）。
5. 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：Meeting Management 経由で証明書をアップロードすることはできません。LDAPS 接続を完全にセキュアにするには、Meeting Serverで証明書の検証を有効にし、証明書をトラスト ストアにアップロードする必要があります。手順については、「LDAP サーバー証明書の検証を 有効にするにはどうすればよいですか?」を参照してください。

   ---
6. LDAP サーバーの**バインド** DN と**パスワード**を入力します。

   Meeting Server クラスタを LDAP サーバーにバインド（認証）するユーザアカウントのログイン情報です。

7. 1 回の操作でデータベース全体を処理するのではなく、LDAP ライブラリのページに対応するチャンクで検索結果を Meeting Server が受信するようにする場合は、[**ページングされた LDAP の結果の制御の使用**（Use LDAP paged results control）] を選択します。

   Oracle Internet Directory を使用している場合を除き、ページングされた結果を使用することをお薦めします。

   注：ページングされた結果は、Oracle Internet Directory ではサポートされていません。

注：変更は、コミットする前に適用されません。変更をコミットすると、テンプレート設定がすぐに有効になります。LDAP サーバーの詳細の変更、およびユーザに影響を与える変更は、次に Meeting Server が LDAP サーバーと同期されたときに有効になります。

注：変更がコミットされる前に Meeting Management を再起動すると、Meeting Management に入力したプロビジョニング設定へのすべての変更が失われます。

16.6 プロビジョニング - ユーザをインポート

Meeting Server クラスタでのユーザとスペース テンプレートのプロビジョニングの一環として、クラスタに接続されている LDAP サーバーからインポートするユーザを定義する必要があります。

[**プロビジョニング**（Provisioning）] ページの [**ユーザのインポート**（Import users）] タブで、ユーザのインポートを追加できます。これは、接続された LDAP サーバーの 1 つからインポートするユーザのサブセットをそれぞれ定義する LDAP フィルターとマッピングのセットです。

16.6.1 ユーザインポートを追加する方法

必要な数のユーザインポートを追加できます。ユーザインポートごとに、特定の LDAP サーバーからインポートするユーザのサブセットを定義し、ユーザー名と表示名の作成方法を決定し、ユーザに PMP Plus ライセンスを割り当てるかどうかを決定します。

同じユーザが 1 つのユーザインポートにのみ含まれていることを確認することをお勧めします。PMP Plus ライセンスが 1 つのユーザインポートで割り当てられ、別のユーザ インポートでは割り当てられず、ユーザが両方のユーザ インポートの LDAP 検索フィルタに一致する場合、そのユーザに PMP Plus ライセンスが割り当てられる場合と割り当てられない場合があります。

注：同じユーザが 2 つの異なるユーザインポートに含まれている場合、Meeting Management は、ユーザがどのユーザインポートに関連付けられるかを制御できません。これは、ユーザの PMP Plus ライセンスが割り当てられているユーザインポートの 1 つにユーザが含まれており、かつ、ライセンスが割り当てられていないユーザインポートにも含まれている場合、ユーザにライセンスが割り当てられているかどうかを制御できないことを意味します。

インポートするユーザのサブセットを定義する方法は以下のとおりです。

1. [**サーバー**（Servers）] ページに移動し、[**プロビジョニングの設定**（Set up provisioning）] をクリックします。
2. [**ユーザのインポート**（Import users）] タブで、[**ユーザインポートの追加**（Add user import）] をクリックします。
3. ユーザインポートの**名前**を追加します。

   自分や他の管理者がこのユーザインポートを他の管理者と区別しやすい名前を選択することをお勧めします。このフィールドを空白のままにすると、Meeting Management は以下で構成する設定に基づいて名前を作成します。
4. ドロップダウンから、このユーザインポート フィルタを設定する LDAP サーバーを選択します。
5. **ベース識別名**を入力します。

   ベース識別名は、ディレクトリ検索の開始点です。Meeting Server 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。
6. LDAP **検索フィルタ**を入力します。

   このフィルタは、インポートするユーザのサブセットを定義します。[フィルタ（Filter）] フィールドのシンタックスについては、rfc4515 に記載されています。

   注：Active Directory を使用している場合は、ユーザオブジェクトのみを含むフィルタを入力してください。
7. **ログインユーザー名のマッピング**を入力します。

   これは、Meeting Server Web アプリのユーザがアプリにサインインするために使用するユーザー名として使用する LDAP 属性を定義します。 これは、次の形式にする必要があります：
   $sAMAccountName$@example.com。また、属性はユーザごとに一意である必要があります。

   注：LDAP 属性名は、大文字、小文字を区別します。

8. **表示名のマッピング**を入力します。

   これは、会議および各 Web アプリ ユーザのホーム画面で参加者名として使用する LDAP 属性です。cn のような形式にする必要があります。

   注：LDAP 属性名は、大文字、小文字を区別します。

9. これらのフィルタ設定に基づいて**インポートされユーザに対する** Personal Multiparty Plus（PMP+）**ライセンスの割り当て**を行う場合は、インポートされたユーザに Personal Multiparty Plus (PMP+) ライセンスを割り当てるチェック ボックスをオンにします。

   SMP Plus ライセンスを使用する場合、またはこれらのユーザが別の所有者を持つ会議にのみ参加できるようにする場合は、このチェックボックスをオフのままにします。

注：変更は、コミットする前に適用されません。変更をコミットすると、テンプレート設定がすぐに有効になります。LDAP サーバーの詳細の変更、およびユーザに影響を与える変更は、次に Meeting Server が LDAP サーバーと同期されたときに有効になります。

注：変更がコミットされる前に Meeting Management を再起動すると、Meeting Management に入力したプロビジョニング設定へのすべての変更が失われます。

16.7 プロビジョニング - スペースを自動的に作成する

プロビジョニングの一環として、ユーザ用のスペースを作成できます。

[**スペースを自動で作成**（Automatically create spaces）] タブで、定義されているすべてのスペース テンプレートを表示し、各テンプレートで作成されたスペースを持つユーザのサブセットを確認できます。

新しいスペース テンプレートを作成したり、スペースを自動的に作成するために使用するスペース テンプレートを定義したりすることもできます。これを行うには、ユーザのグループをスペース テンプレートにマップするルールを、スペース名とビデオ アドレスの生成方法の詳細とともに設定します。

16.7.1 スペースを自動作成するためのルールを追加する

ルールの定義は以下のように実施します。

1. [**ルールを追加**（Add）] をクリックします。
2. [**ユーザインポート**（User import）] ドロップダウンからユーザインポートを選択します。
3. オプション：一部のユーザのみに同じタイプのスペースをプロビジョニングする場合は、**フィルタ**を追加して、これらのユーザのより小さなグループを指定します。

選択したサブセット内のすべてのユーザに同じタイプのスペースをプロビジョニングする場合は、フィールドを空白のままにすることができます。

4. **スペース名マッピング**を定義します。

   これにより、スペース名の生成方法に関するルールが定義されます。たとえば、cn のスペースに入り、ユーザの共通名が Sally Wood である場合、このユーザのスペースは「Sally Wood のスペース」という名前になります。

   注：LDAP 属性名は、大文字、小文字を区別します。

5. URI **ユーザ パーツ マッピング**を定義します。

   これは、スペースの URI を定義する方法のルールを定義します。たとえば、$sAMAccountName$ と入力し、ユーザの SAM のアカウント名が swood で、ユーザのドメインが example.com である場合、URI は swood@example.com、swood.host@example.com などのようになり、ロールの一意の URI ジェネレーターがどのように定義されているかによって異なります。

   注：URI ユーザパーツマッピングで使用される LDAP 属性は、ユーザに対して一意である必要があります。

   注：URI ユーザパーツマッピングでは、複数の LDAP 属性を使用できます。複数の LDAP 属性を使用する場合は、そのうちの少なくとも 1 つがユーザに対して一意であることを確認してください。

   注：Meeting Server は属性値を小文字に変換します。他の文字が削除または変更されることはありません（スペースを含む）。そのため、URI ユーザパーツマッピングが、すべてのユーザに使用できる URI になることを確認してください。

6. [**スペース テンプレートの選択**（Choose a space template）] で、[**新しいテンプレートの作成**（Create new template）] を選択するか、既存のテンプレートを選択します。

   *既存のテンプレートを選択した場合は、[**完了**（Done）] をクリックし、次の手順を無視します。*

   *[**新しいテンプレートの作成**（Create new template）] を選択した場合は、[**スペース テンプレートの作成**（Create space template）] をクリックして、ステップ 7 に進みます。*

7. **テンプレート名**を定義します。

   注：この名前は、ユーザが Cisco Meeting Server Web アプリケーションに表示するものでもあります。一般のアプリ ユーザにとって意味のある名前を選択するようにしてください。

8. スペース **テンプレートの説明**を入力します。

   注：この説明は Web アプリにも表示され、この説明に基づいてスペース テンプレートを選択します。一般のアプリユーザが理解しやすい説明を書くようにしてください。

9. さまざまな役割をパスコードで区別する必要があるかどうか、またはそれぞれに一意の URI と会議 ID を割り当てる必要があるかどうかを決定します。
10. [**ロールの追加**（Add Role）] をクリックします。
11. **ロール名**を入力します。

    注：アプリのユーザが名前からこのロールを推測できるように、名前はわかりやすいものにしてください。

12. [**可視性**（Visibility）] ドロップダウンから、テンプレートの可視性スコープを選択します。
13. **固有の** URI **ジェネレーター**を入力して、このロールを持つ参加者がスペースにアクセスするために使用する URI を Meeting Server が生成する方法のルールを定義します。

    URI は、URI ユーザパーツマッピング、URI ジェネレータ、およびドメインに基づいて作成されます。たとえば、$.host と入力し、URI ユーザパーツマッピングが $givenName$.space の場合、example.com ドメインで作成された Sally という名前の誰かのスペースの URI は ***sally.space.host@example.com*** *になります。*

    注：すべてのロールに同じ URI を使用することを選択した場合、このフィールドは無効になります。

14. 最小パスコード長を定義します。

    この設定を無視すると、Meeting Management はシステムのデフォルトを使用することを選択します。パスコードを要求しない場合は、0 を入力します。

    注：Meeting Server 管理者がシステムまたはテナントレベルで別のデフォルトを設定していない限り、システムのデフォルトは 0 です。

注：すべてのロールに同じ URI と数値 ID を使用することを選択し、複数のロールがある場合は、1 つのロールにのみパスコードを設定できません。複数の役割をパスコードなしで設定すると、Meeting Server はこれらの設定を無視し、4 文字のパスコードを提供します。

15. [次へ（Next）] をクリックします。
16. このロールを持つ参加者をアクティベータにする場合は、[**ロールとアクティベータを作成**（Make role and Activator）] チェック ボックスをオンにします。

    アクティベータは、会議を開始できる参加者です。これが関連するシナリオについては、『ビデオ オペレータ向け Cisco Meeting Management ユーザーガイド』の「会議ロビーを使用して会議をロックする」を参照してください。

17. ロールの権限を定義します。

    *設定にシステム値を使用するには、[**オーバーライド**（Override）] チェック ボックスをオフのままにします。*

    *新しい設定を定義するには、[**オーバーライド**（Override）] チェックボックスをオンにして、次のオプションから必要な値を選択します。*

フィールド名	説明
最大参加者数	会議のアクティブな参加者の最大数を設定します。
録画モード（Recording Mode）	次のいずれかのオプションを選択します。 **無効**：録画は無効になります **手動**：ユーザは録画を開始および停止できます **自動**：スペース内のすべての会議が記録されます
デフォルトでロック（Locked by default）	このスペースのすべての会議がロックを開始するかどうかを設定します。
タイムアウト（秒）（Passcode timeout (seconds)）	パスコードのないロールにフォールバックする前に、プロンプトが表示されたときに参加者がパスコードを入力するのを Meeting Server が待機する秒数を設定します。タイムアウトを無効にするには、値 0 を入力します。
ビデオを許可（Video allowed）	このスペースの会議で参加者のビデオを許可するかどうかを設定します。音声のみの会議でも、プレゼンテーション ビデオの共有は常に許可されています。
デフォルト ビデオ レイアウト（Default video layout）	この会議の参加者に表示されるデフォルトのビデオレイアウトを設定します。

最後のアクティベータが退席したときの動作（Behaviour when last activator leaves）	最後のアクティベータが退席したときの、会議の残りの参加者に対する動作。
ロールの変更を許可（Allow change role）	この権限を持つ参加者はロールを変更できます

18. [次へ（Next）] をクリックします。
19. このスペース テンプレートに必要なすべてのロールを追加するまで、手順 10 ～ 18 を繰り返します。
20. [**ダイヤルアウトのデフォルト**（Default for dial out）] を使用して、会議中のダイヤルアウト参加者のデフォルトのロールを選択します。
21. [次へ（Next）] をクリックします。
22. スペースのデフォルト設定を定義します。

    *設定にシステム値を使用するには、[**オーバーライド**（Override）] チェック ボックスをオフのままにします。*

    *新しい設定を定義するには、[**オーバーライド**（Override）] チェックボックスをオンにして、必要な値を選択します。*
23. [**完了**（Done）] をクリックします。

注：変更は、コミットする前に適用されません。変更をコミットすると、テンプレート設定がすぐに有効になります。LDAP サーバーの詳細の変更、およびユーザに影響を与える変更は、次に Meeting Server が LDAP サーバーと同期されたときに有効になります。

注：変更がコミットされる前に Meeting Management を再起動すると、Meeting Management に入力したプロビジョニング設定へのすべての変更が失われます。

16.8 プロビジョニング - ユーザのスペース作成を許可

プロビジョニングの一環として、どの Web アプリ ユーザにどのタイプのスペースの作成を許可するかを決定できます。これは、スペース テンプレートを特定のユーザインポート、またはユーザインポート内のグループに割り当てることによって行われます。

[**プロビジョニング**（Provisioning）] ページの [**ユーザのスペース作成を許可**（Allow users to create spaces）] タブで、スペース テンプレートを作成し、それらを Web アプリ ユーザの特定のグループに割り当てることができます。

16.8.1 制限事項

- スペースを作成するユーザには、Meeting Management で定義したロールが割り当てられていません。スペースの所有者でもあるスペースの作成者は、スペースのデフォルトのコール レッグ プロファイルを受け取ります。
- スペースを作成したユーザは、スペースのメンバーになります。
- スペースのすべてのメンバーは、それを作成したユーザと同じコール レッグ プロファイルを取得します。
- テンプレートを変更しても、すべての変更が既存のスペースに適用されるわけではありません。

  *新しい**参加者ロール設定**と**スペース テンプレート設定**が既存のスペースに適用されます。ロールの追加や削除などの他のテンプレートの変更は、既存のスペースには影響しません。*

  既存のスペースに変更を加える場合は、API を介して手動で行うことができます。

  注：自動的に作成されたが、ユーザによってまだアクティブ化されていないスペースは、既存のスペースとしてカウントされません。自動作成されたスペースには、ユーザがアクティブ化した時点で有効な設定が適用されます。

- Web アプリは、テンプレートが変更されたかどうかをユーザに示しません。

  既に使用されているテンプレートに大幅な変更を加えた場合は、名前または説明を更新することをお勧めします。

- Meeting Management は、可能なスペース設定の小さなサブセットを提供します。

  Meeting Management を使用して作成したスペース テンプレートに追加の設定を構成する場合は、Meeting Server API を使用できます。詳しくは『Cisco Meeting Server API Reference Guide』を参照してください。

- API を介して作成または編集したテンプレートは Meeting Management に表示されますが、Meeting Management で編集できる設定のサブセットのみを表示できます。
- Meeting Management の一部の設定は、複数の API 設定の組み合わせです。

  テンプレートを簡単に構成できるように、いくつかの設定を組み合わせました。

- Meeting Management を使用して構成した設定は、コミット時に既存の設定を置き換えます。

  これは、構成する特定の設定にのみ影響します。たとえば、スペースのストリーミング URI を定義している場合、これは Meeting Management から構成できる設定の影響を受けません。

16.8.2 特定の Web アプリ ユーザにスペース テンプレートを割り当てる方法

スペーステンプレートの作成は次のようにします。

1. [**サーバー**（Servers）] ページに移動し、[**プロビジョニングの設定**（Set up provisioning）] をクリックします。
2. [**プロビジョニング**（Provisioning）] ページの [**ユーザのスペース作成を許可**（Allow users to create spaces）] タブで、[**ルールの追加**（Add Rule）] をクリックします。
3. [**ユーザインポート**（User Import）] を選択します。
4. オプション：**フィルタ**を追加します。
5. [**スペース テンプレートを選択**（Chose space template）] ドロップダウンから、既存のテンプレートを選択するか、**新しいテンプレートを作成**します。
6. 既存のテンプレートを選択した場合は、[**完了**（Done）] をクリックし、次の手順を無視します。

   新しいテンプレートの作成を選択した場合は、[**スペース テンプレートの作成**（Create space template）] をクリックして、次の手順に進みます。
7. スペースの**テンプレート名**を入力します。

   これは、ユーザが作成するスペースのタイプを選択するときに Web アプリに表示されるテンプレート名です。

   注：テンプレート名に特殊文字を使用すると、ステータス　メッセージでの表示が異なり、代わりにエスケープ文字が表示される場合があります。名前は引き続き Web アプリに正しく表示されます。

   ---
8. スペース**テンプレートの説明**を入力します。

   これは、ユーザが作成するスペースのタイプを選択するときに Web アプリに表示されるテンプレートの説明です。
9. さまざまな役割をパスコードで区別する必要があるかどうか、またはそれぞれに一意の URI と会議 ID を割り当てる必要があるかどうかを決定します。

   URI は Web アプリではビデオ アドレスと呼ばれます。

   注：Meeting Server は、参加者のアクセス方法（Web リンクまたは URI とパスコードの一意の組み合わせのいずれか）によってロールを認識します。ロールを区別するために必要な場合、またはパスワードの最小長を設定した場合、Meeting Server は自動生成されたパスコードを追加します。 Web アプリのユーザは、スペースを管理するときにパスコードを追加または変更できます。

   ---

10. [**ロールの追加**（Add Role）] をクリックします。
11. **ロール名**を入力します。

    これは、Web アプリのユーザが他のユーザに送信する招待状の詳細を選択するときに表示される参加者ロール名です。
12. [**可視性**（Visibility）] ドロップダウンから、テンプレートの可視性スコープを選択します。
13. **固有の** URI **ジェネレーター**を入力して、このロールを持つ参加者がスペースにアクセスするために使用する URI を Meeting Server が生成する方法のルールを定義します。

    URI は、スペース名、URI ジェネレータ、およびドメインに基づいて作成されます。たとえば、$.host と入力し、ユーザがドメイン example.com に「The A team」というスペースを作成した場合、URI は ***the.a.team.host@example.com*** *になります。*

    注：すべてのロールに同じ URI を使用することを選択した場合、このフィールドは無効になります。

    ---
14. 最小パスコード長のシステム デフォルトを上書きするかどうかを決定します。

    この設定を無視すると、Meeting Management はシステムのデフォルトを使用することを選択します。
15. システムのデフォルトを上書きすることを選択した場合は、パスコードの最小長を入力します。

    デフォルトの最小長は 4 文字です。パスコードを要求しない場合は、0 を入力します。

    注：すべてのロールに同じ URI と数値 ID を使用することを選択し、複数のロールがある場合、Meeting Server は 0 を選択したことを無視します。

    ---
16. [**次へ**（Next）] をクリックします。
17. このロールを持つ参加者をアクティベータにする場合は、[**このロールをアクティベータにする**（Make this role an Activator）] チェック ボックスをオンにします。

    アクティベータは会議を開始でき、他の参加者をロビーから入れることができます。

    ホストとゲスト スペースを作成する場合は、ホストをアクティベータ、ゲストを非アクティベータにすることをお勧めします。すべての参加者に同じ役割を持たせたいチーム スペースを作成している場合は、参加者をアクティベータにする必要があります。

18. ロールのアクセス許可を構成します。

    *リストされている各設定について、デフォルトのスペース コール レッグ プロファイルに設定されている設定を上書きする場合は、[**オーバーライド**（Override）] チェックボックスをオンにします。デフォルトのコール レッグ プロファイルは、工場出荷時の設定と API を介して定義された設定の組み合わせによって定義されます。*

    *新しい設定を定義するには、[**オーバーライド**（Override）] チェックボックスをオンにして、次のオプションから必要な値を選択します。*

フィールド名	説明
最大参加者数	会議のアクティブな参加者の最大数を設定します。
録画モード（Recording Mode）	次のいずれかのオプションを選択します。 **無効**：録画は無効になります **手動**：ユーザは録画を開始および停止できます **自動**：スペース内のすべての会議が記録されます
デフォルトでロック（Locked by default）	このスペースのすべての会議がロックを開始するかどうかを設定します。
タイムアウト（秒）（Passcode timeout (seconds)）	パスコードのないロールにフォールバックする前に、プロンプトが表示されたときに参加者がパスコードを入力するのを Meeting Server が待機する秒数を設定します。タイムアウトを無効にするには、値 0 を入力します。
ビデオを許可（Video allowed）	このスペースの会議で参加者のビデオを許可するかどうかを設定します。音声のみの会議でも、プレゼンテーション ビデオの共有は常に許可されています。
デフォルト ビデオ レイアウト（Default video layout）	この会議の参加者に表示されるデフォルトのビデオレイアウトを設定します。
最後のアクティベータが退席したときの動作（Behaviour when last activator leaves）	最後のアクティベータが退席したときの、会議の残りの参加者に対する動作。
ロールの変更を許可（Allow change role）	この権限を持つ参加者はロールを変更できます

19. [**次へ**（Next）] をクリックします。
20. このスペース テンプレートに必要なすべてのロールを追加するまで、ロールの追加を繰り返します。
21. [**ダイヤルアウトのデフォルト**（Default for dial out）] を使用して、会議中のダイヤルアウト参加者のデフォルトのロールを選択します。
22. [**次へ**（Next）] をクリックします。

23. このテンプレートから作成されるスペースの設定を定義します。

    *設定にシステム値を使用するには、[**オーバーライド**（Override）] チェック ボックスをオフのままにします。*

    *新しい設定を定義するには、[**オーバーライド**（Override）] チェックボックスをオンにして、必要な値を選択します。*

    注：ここにリストされている以外の設定を定義する場合は、Meeting Server API を介してテンプレートを調整できます。詳細については『*Cisco Meeting Server API Reference ガイド*』を参照してください。

24. [**完了**（Done）] をクリックします。

注：変更は、コミットする前に適用されません。変更をコミットすると、テンプレート設定がすぐに有効になります。LDAP サーバーの詳細の変更、およびユーザに影響を与える変更は、次に Meeting Server が LDAP サーバーと同期されたときに有効になります。

注：変更がコミットされる前に Meeting Management を再起動すると、Meeting Management に入力したプロビジョニング設定へのすべての変更が失われます。

16.9 プロビジョニング - レビューとコミット

プロビジョニングの [**レビューとコミット**（Review and commit）] タブにプロビジョニング設定が表示されます。

まだコミットされていない変更を行った場合、タブには Meeting Management にローカルな設定が表示されます。

- **変更をコミット**（Commit changes）：変更をコミットすると、ここに表示されている設定で Meeting Server の現在の設定が上書きされます。

  注：変更は、コミットする前に適用されません。変更をコミットすると、テンプレート設定がすぐに有効になります。LDAP サーバーの詳細の変更、およびユーザに影響を与える変更は、次に Meeting Server が LDAP サーバーと同期されたときに有効になります。

  注：「現在、変更をコミットできませんでした」というエラー メッセージが表示された場合は、一部の変更がコミットされている可能性があります。Meeting Management のすべてのプロビジョニング設定が正しいことを確認し、再試行してください。

- **変更を破棄**（Discard changes）：変更を破棄すると、Meeting Management は最後にコミットされた設定を Meeting Server から取得し、タブを更新してこれらを表示します。

新しい設定を構成していない場合、タブには Meeting Management が Meeting Server から取得した設定が表示され、ボタンは無効になります。設定の変更中を除き、設定は 5 分ごとに Meeting Server から取得されます。

16.10 プロビジョニング - LDAP 同期

プロビジョニングの最後の手順は、LDAP 同期を実行することです。これは、Meeting Server が LDAP サーバーからユーザをインポートし、コミットされたプロビジョニング設定を適用するために必要です。

新しいユーザなど、LDAP サーバー上の情報に変更があった場合にも、LDAP 同期を実行することをお勧めします。

[**プロビジョニング**（Provisioning）] ページの [LDAP **同期**（LDAP sync）] タブで、定期的な同期スケジュールを設定するか、手動で同期をトリガーして、最近の同期のステータスを確認できます。

スケジュールされた同期を構成する方法は以下のとおりです。

1. [**同期スケジュールの表示/編集**（View / edit sync schedule）] をクリックします。
2. アクティブな会議の中断を最小限に抑えるには、LDAP 同期を実行する Call Bridge を選択します。
3. 同期を実行する曜日を選択します。
4. 同期を実行する時刻を選択し、[OK] をクリックします。

> 注：同期スケジュールは Meeting Management で設定され、Meeting Management はスケジュールされた時刻に各同期をトリガーします。同期が実行されている Call Bridge を削除すると、スケジュールされた同期は実行されません。

LDAP 同期を手動でトリガーする方法は以下のとおりです。

1. テーブルの下にある [**今すぐ同期を実行**（Run a sync now on:）] ドロップダウンから、LDAP 同期を実行する Call Bridge を選択します。

   アクティブな会議の中断を最小限に抑えるには、他の Call Bridge よりも少ない、または重要度の低い会議をホストする Call Bridge を選択します。
2. [**今すぐ同期を実行**（Run sync now）] をクリックします。

注：Meeting Server は、接続されているすべての LDAP サーバーと同期します。

注：プロビジョニング設定を変更するたびに、設定が正しく適用されていることを確認することを強くお勧めします。Meeting Management は、同期が成功したかどうかを報告しますが、定義されたグループまたはマッピングが計画どおりに実装されたかどうかを確認することはできません。

17 ログ - ログ、クラッシュ レポート、詳細なトレース

管理者は、Meeting Management および Meeting Server のすべてのログにアクセスできます。

注：ほとんどのタイムスタンプは UTC 時間です例外は、Meeting Management 内で表示したときにブラウザのタイム ゾーンで表示されるイベント ログです。

注：特定の会議のイベント ログは、会議が終了してから最大 1 週間、[**会議**（Meetings）] ページの会議の詳細ビューに表示されます。詳細については、*ビデオオペレータ向けユーザーガイド*を参照してください。イベント ログ情報も Meeting Management システム ログに含まれますが、メッセージが属する会議別にソートされて表示されることはありません。

17.1 Meeting Management ログ

ログ バンドル、システム ログ、監査ログを含むすべての Meeting Management ログには、CMM **ログ** タブからアクセスできます。

17.1.1 ログ バンドル

[**ログ**（Logs）] ページの [CMM **ログ**（CMM logs）] タブから、[**ログ バンドルのダウンロード**（Download log bundle）] ボタンを使用して、Meeting Management のログ バンドルをダウンロードできます。ダウンロードされたログには、シスコ サポートがトラブルシューティングに必要とする情報が含まれています。

- 最新のシステムと監査ログ
- 構成の詳細（パスワードを含まないように編集）
- バージョン番号
- クラッシュレポートのリスト
- 90 日ライセンスレポート

シスコ テクニカル サポートに連絡する必要がある場合は、常にログ バンドルを含めてください。

注：メッセージの多くは Meeting Server Call Bridge から受信した情報に基づいていますが、CMM **ログ** タブでアクセスされるすべてのログは Meeting Management 用です。

17.1.2 システムログサーバー

[**システムログサーバー**（System log server）] タブで、Meeting Management がシステム ログを送信するサーバーを追加できます。システムログには、Meeting Management で発生したすべての情報が含まれています。最新のシステムログは、ログ バンドルに含まれています。最大 5 つのシステムログサーバーを構成して、Meeting Management のイベントとアクティビティを追跡できます。

最新のログのみがローカルに保存されるため、サポートに必要な場合に備えて、外部の syslog サーバーを設定して完全な履歴を保持することを強くお勧めします。

注：Meeting Management の問題をトラブルシューティングするときは、Meeting Server ログも確認する必要がある場合があります。Meeting Management のすべてのインスタンスおよびすべての Meeting Server に外部 syslog サーバーを使用することを強くお勧めします。

システムログサーバーを構成するには、次の手順を実行します。

1. [**ログサーバーの追加**（Add log server）] ボタンをクリックします
2. **サーバーアドレス**と**ポート**を入力します
3. **プロトコル**を選択します
4. [**証明書のアップロード**（Upload certificate）] ボタンを使用して証明書をアップロードします
5. [**追加**（Add）] ボタンをクリックして、ログサーバーの構成を完了します。

17.1.3 監査ログサーバー

[**監査ログサーバー**（Audit log server）] タブで、Meeting Management が監査ログを送信するサーバーを追加できます。監査ログには、Meeting Management ユーザが実行したアクションに関する情報が含まれています。たとえば、設定の変更、ログインの詳細などです。

組織で監査ログが必要な場合は、監査ログ用に外部の syslog サーバーを設定することをお勧めします。最大 5 つのシステムログーサーバーを構成して、Meeting Management のイベントとアクティビティを追跡できます。

監査ログ サーバーを構成するには、次の手順を実行します。

1. [**ログ サーバーの追加**（Add log server）] ボタンをクリックします。
2. **サーバーアドレス**と**ポート**を入力します。

3. **プロトコル**を選択します
4. [**証明書のアップロード**（Upload certificate）] ボタンを使用して証明書をアップロードします
5. [**追加**（Add）] ボタンをクリックして、ログサーバーの構成を完了します。

17.1.4 クラッシュレポート

Meeting Management のクラッシュ レポートには、[CMM **ログ**（CMM Logs）] ページの [**クラッシュ レポート**（Crash reports）] タブからアクセスできます。

17.1.5 詳細なトレース

サポートから要求された場合は、問題を再現しながら詳細なトレースを有効にして、包括的なログを収集できます。

詳細なトレースは、次の場合に利用できます。

- Meeting Server API
- Meeting Server の CDR
- Meeting Server のイベント
- TMS API
- Meeting Server Cloud Connector API

1 分、10 分、30 分、または 24 時間ごとにログをトレースするように構成できます。

17.1.6 90 日ライセンス レポート

90 日ライセンス レポートは、Webex での会議に参加することなく、サポート チームに顧客のライセンス使用状況を表示します。その後、サポート チームは 90 日ライセンス レポートを解析し、ライセンスに必要な変更があれば顧客に通知できます。

17.2 Meeting Management で PCAP ファイルをキャプチャする

[**ログ**（Logs）] ページの [CMM **ログ**（CMM logs）] タブから、[CMM PCAP] ページに移動し、パケットの継続的なキャプチャを開始して、Meeting Management でのネットワーク問題のトラブルシューティングのために pcap を処理する間の遅延を回避できます。

pcap をキャプチャするには、次の手順を実行します。

1. [CMM **ログ**（CMM logs）] タブで、[PCAP **の開始**（Start PCAP）] ボタンをクリックします。パケットは .zip ファイルにキャプチャされます。

2. キャプチャされた pcap ファイルに対してそれぞれ利用可能な ダウンロードまたは削除ボタンを使用して、PCAP ファイルをダウンロードまたは削除します。
3. [PCAP **の停止**（Stop PCAP）] ボタンをクリックして、パケット キャプチャを停止します。

開始されると、管理者が [PCAP の停止（Stop PCAP）] ボタンを使用してパケット キャプチャを停止しない限り、パケットは継続的にキャプチャされます。

パケットは、ローテーション時に複数のファイルにキャプチャされます。pcap ファイルのサイズが 500MB を超えると、パケットは新しいファイルにキャプチャされます。これにより、管理者が停止するまで、パケットを永続的にキャプチャできます。Meeting Management は、最大 4 つの pcap ファイルを保存し、最大ファイル サイズの制限は常に 2GB です。4 番目の pcap ファイルのサイズが 500MB を超えると、最も古い pcap ファイルが削除されます。

17.3 Meeting Server のログ

Meeting Management 管理者は、[**ログ**（Logs）] ページの [CMS **ログ**（CMS logs）] タブを使用して、Meeting Server およびエッジノードのログバンドルをダウンロードし、詳細なログを追跡できます。

17.3.1 ログ バンドル

Meeting Management を使用すると、管理者は、Call Bridge やエッジノードを追加した後に、それらを含むサーバーのログを収集できます。

Meeting Server のログを収集する手順は次のとおりです。

1. [**サーバーの選択**（Select server）] ボタンをクリックします
2. サーバーのリストから Call Bridges またはエッジノードを選択します。
3. [**ログバンドルの生成**（Generate log bundle）] ボタンをクリックしてログを生成します。

注：クラスタ内のすべてのノードのログバンドルを生成するには、クラスタノードを選択するときに [サーバーの選択（Select Server）] ページで、クラスタ内の各ノードを選択していることを確認します。

ログバンドルが生成されたら、選択したサーバーのログをダウンロードできます。生成されたログバンドルの名前は logbundle_<host name>_YYYY-MM-hh-mm-ss.tar.gz になります。生成されたログは、[CMS **ログ バンドル**（CMS log bundle）] ページから 24 時間以内にダウンロードできます。

17.3.2 詳細なトレース

Meeting Management を使用すると、管理者は SIP、Active Control、Active Speaker、ICE などのさまざまな Meeting Server モジュールのログをトレースできます。

詳細トレースを有効にする手順は次のとおりです。

1. [**サーバーの選択**（Select server）] ボタンをクリックします
2. サーバーのリストから [Call Bridge] を選択して、詳細なログを追跡します。
3. [**トレース**（Traces）] リストでは、さまざまな Meeting Server コンポーネントのトレースを有効または無効にすることができます。

注: ：トレース デバッグを有効にすると、選択したサーバーに過負荷がかかります。詳細トレースは、必要な場合にのみ有効にしてください。

ログをトレースする頻度を設定することもできます。たとえば、10 分または 60 分ごとにログをトレースするように構成したり、hh:mm 形式で任意の間隔を設定したりできます。

注：クラスタ内のすべてのノードのログバンドルを生成するには、クラスタノードを選択するときに [サーバーの選択（Select Server）] ページで、クラスタ内の各ノードを選択していることを確認します。

[**すべて無効化**（Disable all）] をクリックして、すべての Meeting Server コンポーネントの詳細トレースを無効にします。

17.4 ログサーバーの追加または編集

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**（System log servers）] を選択します。
2. [**ログ サーバーの追加**（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 の再起動

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**（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 の再起動

18 ライセンス

[**ライセンス**（Licenses）] ページには、次の情報が表示されます。

- 各機能のライセンス ステータスを表示するボックス。

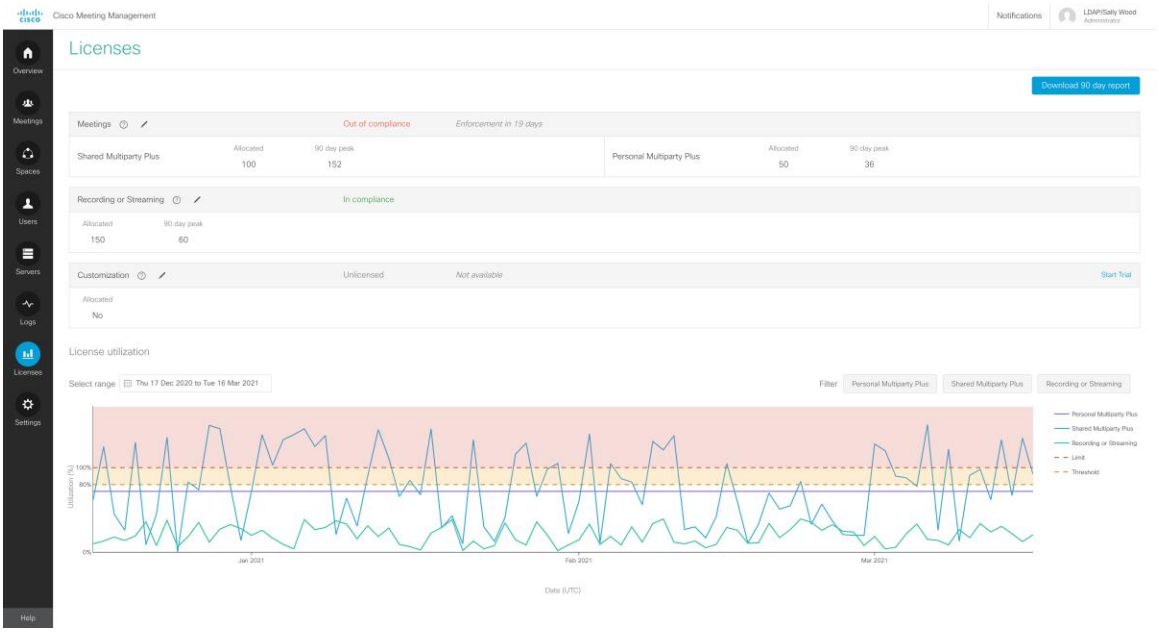
  ライセンスの状態と施行の定義を参照してください。

- 時間の経過に伴うライセンス使用率のグラフ。日付範囲を指定でき、ライセンス タイプに基づいてグラフをフィルタリングできます。

  注：1 日の日付範囲の場合、Meeting Management は 5 分ごとに 1 つのデータ ポイントを表示します。より長い日付範囲の場合、ピーク値を示す 1 日あたり 1 つのデータ ポイントがあります。

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、ライセンス予約を導入しました。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。詳細については、「ライセンス」の項を参照してください。

次のスクリーンショットは、スマート ライセンス モードの [**ライセンス**（Licenses）] ページを示しています。



各機能について、ボックスには次の情報が表示されます。

- ボックス ヘッダー：機能の名前、ライセンス ステータス、施行警告（ある場合）。
  試用版を使用していない場合は、右側に［**試用を開始**（Start trial）］ボタンもあります。

  詳細については、「ライセンスの状態と施行」のセクションを参照してください。
- **予約済み**（Reserved）：SLR ライセンス予約モードの場合に Cisco SSM で予約されたライセンスの数。
- **割り当て済み**（Allocated）：使用可能なライセンスの数

  スマートライセンスの場合、番号を入力すると、Meeting Management が Cisco Smart Software Manager で検証します。
- 90 **日間のピーク**（90-day peak）：過去 90 日間に使用されたライセンスの最大数

概要に表示される以上の詳細が必要な場合は、90 **日間のレポートをダウンロード**できます。

Meeting Management は、license-data.zip という名前の zip ファイルを提供します。このファイルには、次のファイルが含まれています。

- host-reported.csv
  このファイルには、Meeting Management がクラスタ内の個別の Call Bridge から受信した生データが含まれています。各行には以下が表示されます。
  - 特定の Call Bridge のホスト ID
  - タイムスタンプ（UTC）
  - ライセンスの種類ごとに使用されているライセンスの数。
- cluster-bins.csv
  このファイルには、Meeting Management によって計算された、5 分間隔ごとのクラスタ全体のライセンス使用量が含まれています。各行には以下が表示されます。
  - 5 分間隔の開始時刻のタイムスタンプ（UTC）
  - ライセンス タイプごとに、すべての Call Bridge に使用されるライセンスの概要。
- daily-peaks.csv
  このファイルには、Meeting Management によって計算された毎日のピークが含まれています。各行には以下が表示されます。
  - 日付（UTC）
  - ライセンス タイプごとに、3 ポイントの中央値平滑化後のその日に使用されたライセンスのピーク数

19 ライセンスの状態と施行

サインインしている Meeting Management のインスタンスでライセンスが有効になっている場合、Cisco Meeting Server 展開のライセンス ステータスを最新の状態に保つことができます。

ライセンスは機能別に分類されています。

- Meetings：これは、Call Bridge およびユーザライセンスのアクティベーションで構成されます。適切なライセンスがある場合、Call Bridge を使用できます。

  スマートライセンス用（For Smart Licensing）：アクティベーション キーは必要ありません。バーチャル アカウントで使用可能な PMP Plus または SMP Plus ライセンスがある場合は、接続されているすべての Call Bridge を使用できます。

- **録画またはストリーミング**（Recording or streaming）：このライセンスでは、録音またはストリーミングを許可します。

  スマート ライセンスの場合、録画またはストリーミング ライセンスを使用できる場合は、録画およびストリーミングがライセンスされます。

- **カスタマイズ**（Customization）このライセンスではカスタマイズされたレイアウトを許可します。

  スマートライセンスの場合、カスタマイズライセンスがある場合は、Meeting Server でカスタマイズされたレイアウトを作成できます。

Meetings ライセンス ステータスのレベルは次のとおりです。

- **準拠**（In compliance）：インストールされているライセンスの 80% 以下を使用しています。
- **ライセンスなし**（Unlicensed）：ライセンスが割り当てられていません。
- 80% **以上のしきい値**（Over 80% threshold）：ライセンス規約に準拠していますが、インストールされているライセンスの 80% 以上を使用しています。
- **ライセンス不足**（Insufficient licenses）：過去 90 日間で、1 ～ 14 日間利用可能なライセンスを多く使用しています。

  想定外のピークが生じる可能性があるため、一時的な過剰使用を許可します。ただし、使用状況データを評価し、追加のライセンスを購入する必要があるかどうかを検討することをお勧めします。

- **コンプライアンス違反**（Out of compliance）：過去 90 日間で 15 日以上、使用可能なライセンス数を超えています。

  ライセンス契約に違反しています。シスコパートナーまたはアカウントチームに連絡して、ニーズについて話し合い、追加のライセンスを購入する必要があります。

録画またはストリーミングのライセンス ステータス レベルは次のとおりです。

- **ライセンスなし**（Unlicensed）：録画またはストリーミング用のライセンスが割り当てられていません。
- **準拠**（In compliance）：インストールされているライセンスの 80% 以下を使用しています。
- 80% **以上のしきい値**（Over 80% threshold）：ライセンス規約に準拠していますが、インストールされているライセンスの 80% 以上を使用しています。
- **ライセンス不足**（Insufficient licenses）：過去 90 日間で、1 ～ 14 日間利用可能なライセンスを多く使用しています。

  想定外のピークが生じる可能性があるため、一時的な過剰使用を許可します。ただし、使用状況データを評価し、追加のライセンスを購入する必要があるかどうかを検討することをお勧めします。
- **コンプライアンス違反**（Out of compliance）：過去 90 日間で 15 日以上、使用可能なライセンス数を超えています。

  ライセンス契約に違反しています。シスコパートナーまたはアカウントチームに連絡して、ニーズについて話し合い、追加のライセンスを購入する必要があります。

カスタマイズ（Customization）のライセンス ステータスのレベルは次のとおりです。

- **ライセンス済み**（Licensed）：カスタマイズライセンスを所持しています。
- **ライセンスなし**（Unlicensed）：カスタマイズライセンスがありません。
- **コンプライアンス違反**（Out of compliance）：Meeting Management でカスタマイズをオンにしましたが、カスタマイズライセンスを持っていません。

  *これは、スマートライセンスでのみ見られます。ライセンス契約に違反しています。割り当てを [**いいえ**（No）] に変更するか、シスコ パートナーまたはアカウント チームに連絡して、ニーズについて話し合ってライセンスを購入する必要があります。*

注：Meeting Server API を使用して、ライセンスステータスを取得することもできます。これには、Meeting Server の機能コンポーネント、各コンポーネントのライセンスステータス、および有効期限が含まれます。API オブジェクト **`/clusterLicensing`** を使用すると、Meeting Server クラスタのライセンス ステータスと有効期限（該当する場合）が返されます。詳細については、『Cisco Meeting Server API Reference Guide』を参照してください。

19.1 利用可能なトライアル

トライアルには次の 3 つのタイプがあります。

- Meetings **トライアル**（Meetings trial）：このトライアルでは、90 日間、録画やストリーミング、カスタマイズを含むすべての機能のライセンスが無制限に提供されます。

  Meetings がライセンスされている場合、または以前にトライアルを使用したことがある場合、Meetings トライアルは提供されません。

- **録画またはストリーミングトライアル**（Recording or streaming trial）：この試用版トライアルでは、90 日間、録画とストリーミングを無制限に使用できます。

  すでにレコーディングまたはストリーミングのライセンスを持っている場合、または以前にトライアルを使用したことがある場合は、レコーディングまたはストリーミングのトライアルは提供されません。

- **カスタマイズトライアル**（Customization trial）：**このトライアルでは、**カスタマイズされたレイアウトを 90 日間使用できます。

  カスタマイズ ライセンスを既に持っている場合、または以前に試用版を使用したことがある場合は、カスタマイズトライアルは提供されません。

注：接続されているすべてのクラスタ間で共有される、Meeting Management の展開ごとに各タイプのトライアルを 1 つ取得します。同じタイプのトライアル中に、接続されたクラスタのいずれかが以前に Meeting Management インスタンスに接続されていた場合、Meeting Management はトライアルを提供しないため、クラスタを新しい Meeting Management デプロイメントに移動して新しいトライアルを取得することはできません。また、最初のトライアルで接続されなかった新しいクラスタを追加しても、新しいトライアルを取得することはできません。

注：試用期間が終了する前にライセンスを追加しない場合、コンプライアンス違反となり、施行が行われます。詳細は以下の表を参照してください。

19.2 試用中および試用後のライセンス状況

トライアルタイプ	トライアルに含まれるもの	試用期間中のライセンス状況	試用後のライセンス状態
Meetings	Meetings、録画とストリーミング、カスタマイズされたレイアウトを 90 日間無制限に使用	コンプライアンス（In compliance）	PMP Plus または SMP Plus のライセンスを持っている場合、会議はこれに準拠します。 PMP Plus または SMP Plus のライセンスがない場合は、ライセンスが付与されなくなり、ライセンスを追加するまで施行がアクティブになります。 録画またはストリーミングのライセンスをお持ちの場合は、録画またはストリーミングが準拠します。 録画またはストリーミングのライセンスがない場合、録画またはストリーミングはライセンスなし（Unlicensed）状態になり、使用できません。 カスタマイズ ライセンスをお持ちの場合は、カスタマイズ ライセンスが付与されます。 カスタマイズ ライセンスがない場合、カスタマイズはライセンスなし（Unlicensed）状態になり、使用できません。
録画またはストリーミング	90 日間の無制限の録画とストリーミング	コンプライアンス（In compliance）	録画またはストリーミングのライセンスがある場合、録画またはストリーミングは準拠します。 録画またはストリーミングのライセンスがない場合は、ライセンスなし（Unlicensed）状態になり、使用できません。
カスタマイズ（Customization）	90 日間のカスタマイズされたレイアウト	ライセンス済み（Licensed）	カスタマイズ ライセンスをお持ちの場合は、カスタマイズがライセンスされます。 カスタマイズ ライセンスがない場合は、ステータスがライセンスなし（Unlicensed）状態になり、使用できません。

19.3 施行と警告

[**ライセンス**（Licenses）] ページでは、ライセンス ステータスと、今後の施行に関する警告の両方を確認できます。

会議（Meetings）に関する警告と施行

- <number> **日後に施行が行われます：これは警告レベル** 1 **です。**コンプライアンス違反をしているため、Meeting Management は施行までカウントダウンしています。
- **施行が行われます。**<number> **日後に高レベルの施行が行われます：これは警告レベル** 2 **であり、施行が行われることを意味します。**会議の参加者は、各会議の開始時に警告を見たり聞いたりします。
- **高レベルの施行が行われます**：これは警告レベル 3 であり、最高レベルの施行が行われることを意味します。会議の参加者には、各会議の開始時に警告が聞こえ、会議全体を通して画面上の大きなテキストで警告が表示されます。

録画またはストリーミング（Recording or streaming）に関する警告と施行

- <number> **日間利用できます**：Meeting Management が施行日までカウントダウンします。
- **利用できません**：会議を録画またはストリーミングすることはできません。

カスタマイズ（Customization）に関する警告と施行

- <number> **日間利用できます**：Meeting Management が施行日までカウントダウンします。
- **利用できません**：カスタマイズされたレイアウトは使用できません。

20 ブラスト ダイヤル モニタリング

ブラスト ダイヤル モニタリングを使用すると、プライマリ ロールまたはセカンダリ ロールを Meeting Management に割り当てて、スペースにアクセスしたときに複数のダイヤル アウトを回避できます。これは、複数の Meeting Management がスペース内のブラスト ダイヤルを監視している場合に発生する可能性があります。

- **プライマリ** – 1 つの Meeting Management のみをプライマリに設定する必要があります。これは、ほとんどの状況でブラスト ダイヤルをトリガーする Meeting Management です。
- **セカンダリ** – この Meeting Management は、時間遅延の後にブラスト ダイヤルをトリガーしようとします。これは、他の Meeting Management がダイヤルアウトを開始していない場合にのみ実行されます。時間遅延は、[**セカンダリを選択した場合の遅延（秒）**（Delay (seconds) when Secondary is chosen）] フィールドで設定できます。
- **オフ** – この Meeting Management はブラスト ダイヤルをトリガーしません。

21 設定 - Meeting Management の構成

[**設定**（Settings）] ページでは、次のような Meeting Management の設定を構成できます。

- Meeting Management のネットワーク設定
- Meeting Management が着信 HTTPS 接続で提示する証明書。
- Meeting Management が Call Bridge から情報を受信する CDR 受信者アドレス
- TMS 設定
- NTP 設定
- サインイン メッセージ
- 高度なセキュリティ

ここで、Meeting Management のバックアップ、復元、アップグレード、および再起動を行うこともできます。

21.1 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。

21.2 証明書のアップロード

Meeting Management 証明書の有効期限が切れたら、新しい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. **証明書をアップロード**して、期限切れの証明書を新しいものに置き換えます。
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。

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。

21.3 CDR 受信者アドレスの編集

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。

21.4 TMS に接続

スケジュールされた会議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、*『インストールおよびコンフィギュレーション ガイド』*[英語] の「始める前に」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 サーバに入力したサーバアドレスは、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。

21.4.1 クラスタと TMS の関連付け

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**（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。

21.4.2 TMS 電話帳へのアクセス

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、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れば、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。

21.5 NTP ステータスの表示または 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。示されているオフセットは、接続されている各 NTP サーバーと Meeting Management サーバーの間のものです。

NTP サーバを追加するには、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。

21.6 ライセンス

[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。

21.6.1 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：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。

21.6.2 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。

21.6.3 ライセンス予約

SMART に準拠するために、シスコ製品のユーザ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/防衛のお客様のみが利用できます。
- **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、シスコ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、シスコがスマート 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。

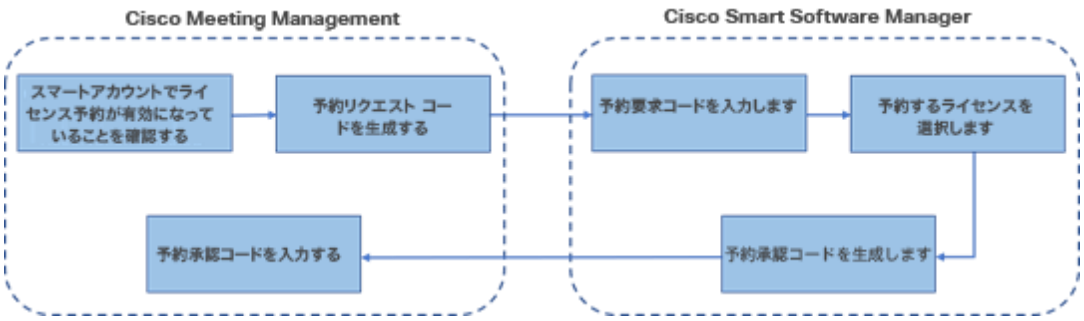
- SLR/PLR ライセンス予約
- 予約済みライセンスの更新
- 予約したライセンスの返却

21.6.3.1 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 3：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。
    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**」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、シスコ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**」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**
- SLR **のライセンス数とともに予約**されています。

21.6.3.2 予約済みライセンスの更新

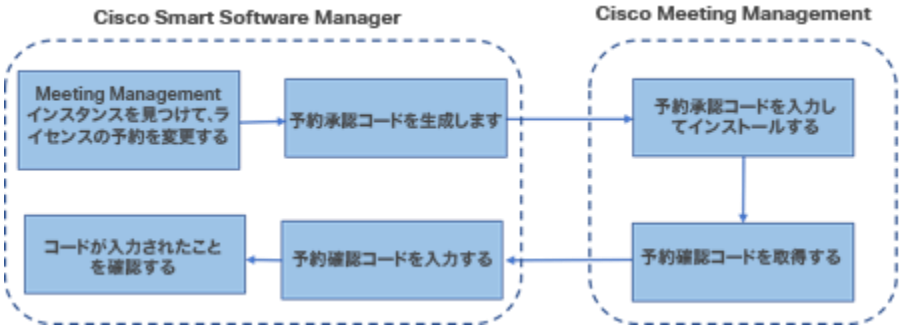
組織の変化するニーズを満たすために、特定のライセンスを更新するか、予約済みライセンスの数を変更することができます。たとえば、現在のライセンス要件が 5 で、さらに 5 ライセンスを追加する場合、ライセンス数を 10 として選択する必要があり、新しい値が以前の値を上書きします。

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 4：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**から 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 [**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**」セクションに移動し、[**予約の更新**（Update Reservation）] ボタンをクリックします。

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。

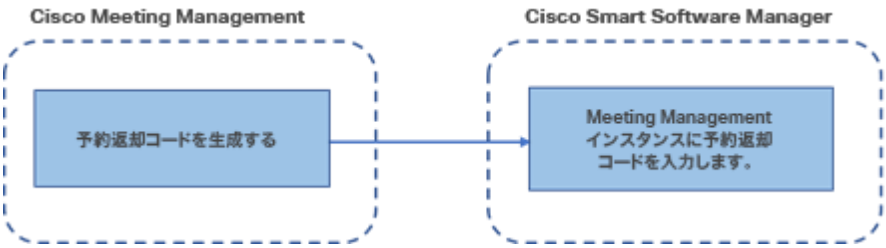
21.6.3.3 予約したライセンスの返却

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 5：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。

21.6.3.4 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。

21.7 Cisco Meeting Server Cloud Connector

注：Meeting Management からサービスを無効にすると、Meeting Management から Webex クラウドへの情報の送信のみが停止します。Meeting Management の登録を完全に解除してサービスを無効にするには、Webex Control Hub に移動します。

Cisco Meeting Server Cloud Connector は、Meeting Management の展開を Webex Control Hub および Webex クラウドに接続できるハイブリッド サービスです。

このサービスでは以下が可能になります。

- Control Hub インターフェイスの Meeting Management インスタンスに関する情報を参照する。
- メールと Webex Teams アラートを設定して、Meeting Management のエラーと警告について通知を受け取ることが可能になる。

このサービスでは、メトリクスも Webex クラウドに送信します。

21.7.1 Cisco Meeting Server Cloud Connector ステータス

[Cisco Meeting Server Cloud Connector] タブで、次のステータス情報を確認できます。

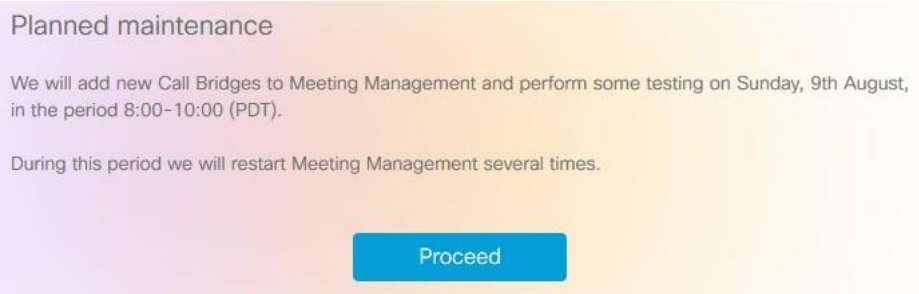
- 登録：これは、Meeting Management のこのインスタンスが Webex クラウドに登録されているかどうかを示します。
- Webex クラウドサービスのアドレス：これは、Cisco Meeting Server Cloud Connector が機能するために Meeting Management が到達する必要があるアドレスを示します。

詳細な手順と情報については、『Cloud Connector オンライン ヘルプ』を参照してください。

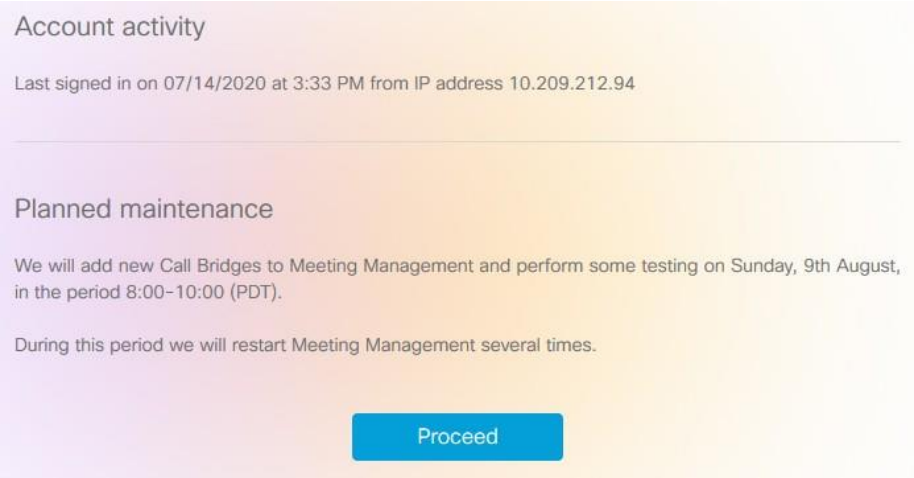
21.8 ユーザがサインインしたときにメッセージを表示する

サインインページの前または後にユーザ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。

21.9 高度なセキュリティ設定の構成

[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。

21.9.1 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。

21.9.2 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。

21.9.3 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 Bridges
- 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ー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 サーバー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 サーバー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。

21.10 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

21.10.1 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。
再展開する必要がある場合は、簡単に設定を再使用できます。

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。

21.10.2 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。

21.11 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。

付録 A セキュリティの強化

安全な方法で VMware 製品を展開し、運用するセキュリティ強化の詳細については、『VMware セキュリティ強化ガイド』を参照してください。

アクセシビリティ通知

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 Meeting Project に関する Voluntary Product Accessibility Template（VPAT）は次の場所で入手できます。

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

Cisco の法的情報

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

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

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.
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 トポロジー図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

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

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

シスコの商標