Cisco Meeting Management

Cisco Meeting Management 3.2

インストール/コンフィギュレーション ガイド

2021 年 4 月 19 日

Cisco Systems, Inc. www.cisco.com

目次

更新履歴 5

1 はじめに 6

2 3.2 の新機能 7

2.1 3.1 以降のこのガイドの変更 7

3. ご使用になる前に 8

3.1 キャパシティ 8

3.2 Meeting Management VM の要件 9

3.3 復元力 9

3.4 ネットワークの詳細、CDR 受信者、および NTP 10

3.5 ユーザ 11

3.6 LDAP 経由のユーザアクセス 12

3.7 ローカルユーザアクセス 13

3.8 ローカルユーザのセキュリティポリシー設定 14

3.9 対応ブラウザ 14

3.10 システムログサーバ 15

3.11 監査ログサーバ 15

3.12 Meeting Server のライセンス 16

3.13 Meeting Management の証明書 17

3.14 Call Bridge またはクラスタの前提条件 18

3.15 サポートされている Cisco Meeting Server バージョン 19

3.16 サポートされている TMS バージョン 19

3.17 TMS 前提条件 19

3.18 ポート情報 22

4 初回セットアップの概要 23

5 OVA の展開 24

6 ネットワーク上での Meeting Management の設定 25

7 Web インターフェイスへのサインインとパスワードの変更 27

8 ネットワークの詳細の編集 28

9 証明書のアップロード 29

10 CDR 受信者アドレスの入力 30
11 オプション：TMS への接続 31
12 NTP サーバの追加 33
13 オプション：ユーザがログインするときに表示するメッセージの追加 34
14 オプション：高度なセキュリティ設定の構成 35
14.1 レート制限のサインイン試行 35
14.2 アイドル セッション タイムアウト 35
14.3 TLS 設定 36
15 ログサーバの追加 37
16 Call Bridge の追加 40
17 ライセンスモードの選択 43
17.1 従来のライセンスを有効にする方法 44
17.2 スマートライセンスを有効にする方法 44
17.3 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 45
18 オプション：クラスタと TMS の関連付け 46
19 オプション：TMS 電話帳へのアクセス 47
20 LDAP サーバの設定 49
20.1 LDAP サーバの設定 49
21 LDAP グループの追加 52
21.1 LDAP ユーザグループの追加 52
22 オプション：ローカルユーザのセキュリティポリシーの設定 53
23 オプション：ローカルユーザの追加 54
24 確認、保存、およびバックアップ 55
25 バックアップと復元 56
25.1 バックアップの作成 56
25.2 バックアップの復元 56
26 Meeting Management の再起動 58
アクセシビリティ通知 59

Cisco の法的情報 60
Cisco の商標 61

更新履歴

表 1：更新履歴

日付	説明
2021-04-19	SSM のアップグレードを開始する前に、オンプレミスバージョンがサポートされています。
2021-04-07	ドキュメントを公開。

1 はじめに

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

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

Meeting Management の管理者は、次の操作を実行できます。

- Meeting Management のインストールと設定
- Meeting Server のライセンス設定の編集
- Meeting Server 上でのスペーステンプレートと Web アプリのユーザのプロビジョニング
- スペースの表示と短縮ダイヤルの設定
- 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。

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

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

2 3.2 の新機能

新機能と変更の概要については、リリースノートを参照してください。

2.1 3.1 以降のこのガイドの変更

「ご使用になる前に」セクションに以下の変更を行いました。

- Smart Software Manager オンプレミス（衛星）を使用している間にゲートウェイのアドレスを設定するために使用する形式が追加されました。
- Cisco Smart Software Manager オンプレミスに接続する際の承認の問題の解決が追加されました。
- Meeting Management VM のハイパーバイザの要件が更新されました。

3 ご使用になる前に

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

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

3.1 キャパシティ

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

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

3.2 Meeting Management VM の要件

VM 環境が、展開サイズに必要な仕様を提供できるかを確認します。

要件	中小規模の環境	大規模な展開
サーバのメーカー	すべて	すべて
プロセッサ タイプ	Intel / AMD	Intel / AMD
プロセッサの周波数	2.0 GHz	2.0 GHz
vCPU	4 コア	8 コア
ストレージ	100 GB *シックプロビジョニングとイーガーゼロ化を推奨します。*	100 GB *シックプロビジョニングとイーガーゼロ化を推奨します。*
RAM	4 GB の予約済みメモリ	8 GB の予約済みメモリ
ハイパーバイザ	ESXi 6.5 U3、6.7 U3、7.0 U1c	ESXi 6.5 U3、6.7 U3、7.0 U1c
ネットワーク インターフェイス	1	1

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

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

3.3 復元力

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

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

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

次のオプションがあります。

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

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

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

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

3.4 ネットワークの詳細、CDR 受信者、および NTP

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

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

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

その他の詳細は、初回のセットアップの完了時に追加できます。

- CDR 受信者アドレス

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

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

注：すべてのクラスタの Meeting Management を無効にした場合は、CDR 受信者アドレスは不要ですが、Meeting Management にはエラー通知が表示されます。

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

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

- オプション：追加の DNS サーバの IP

3.5 ユーザ

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

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

  LDAP を介した認証は、一般的な使用と管理に推奨されています。

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

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

ユーザは、次の 2 つの役割を担います。

- 管理者は Meeting Management に完全にアクセスできます。通常、管理者は Meeting Management を設定し、構成を変更し、ユーザを追加し、システムを監視および保守します。
- 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、ミーティングを監視および管理し、進行中のミーティング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。

3.6 LDAP 経由のユーザアクセス

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

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

サポートされている LDAP 実装は次のとおりです。

- Microsoft Active Directory（AD）
- OpenLDAP

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

LDAP サーバに接続するには、次の手順が必要です。

- プロトコル（LDAP/LDAPS）
- LDAP サーバ アドレス
- LDAP サーバポート番号
- LDAP サーバ証明書（LDAPS 証明書の要件を使用している場合）
  - *証明書チェーンには、証明書に署名した CA の証明書に加えて、ルート CA 証明書を含む証明書チェーン内の上位の証明書を含める必要があります。*
  - *LDAP サーバのアドレスを証明書に含める必要があります。*
- LDAP バインドユーザのログイン情報

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

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

グループを追加するには、次の情報が必要です。

- 各グループの識別名

3.7 ローカルユーザアクセス

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

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

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

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

より多くのローカルユーザを設定するには、次の手順が必要です。

- 各ユーザのユーザ名

  注：ユーザプロファイルを保存した後は、ユーザ名を変更できません。

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

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

  ユーザはサインイン後にパスワードを変更できます。

3.8 ローカルユーザのセキュリティポリシー設定

ローカルユーザに対して以下のセキュリティ ポリシーを設定できます。

- 最小パスワード長が必要

  これは、選択するまで無効になります。デフォルトの最小長は 8 文字です

- 組み込みのパスフレーズ生成機能を有効にする

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

  組み込みのパスフレーズ生成機能を使用する場合は、ディクショナリを提供する必要があります。
  ディクショナリの要件：
  - *ディクショナリは、各行に 1 つの単語を含むテキストファイルである必要があります。*
  - *文字は UTF-8 でエンコードされている必要があります。*
  - *ファイルに Null 文字を含めることはできません。*
  - *ファイルの最大サイズは 10 MB です。*

- パスワードの再使用を制限する

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

3.9 対応ブラウザ

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

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

次のテクノロジーを有効にする必要があります。

- WebSocket
- HTML5
- JavaScript

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

3.10 システムログサーバ

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

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

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

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

注：TLS 接続は TLS 1.2 をサポートする必要があります

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

3.11 監査ログサーバ

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

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

監査ログサーバはオプションですが、組織内で必要になる場合があります。

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

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

注：TLS 接続は TLS 1.2 をサポートする必要があります

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

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

3.12 Meeting Server のライセンス

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

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

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

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

従来のライセンスでは、次の情報が必要です。

- すべての Call Bridge に適切なライセンスファイルをインストールする必要があります

スマートライセンスでは、次の情報が必要です。

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

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

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

  1 つのバーチャルアカウントを Meeting Management の 1 つのインスタンスに接続できます。また、1 つのバーチャルアカウントのすべてのライセンスは、Meeting Management で接続されているすべてのクラスタ間で共有されます。これは、各クラスタが独自のライセンスを持つ従来のライセンスとは異なります。

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

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

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

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

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

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

3.13 Meeting Management の証明書

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

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

証明書の要件

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

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

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

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

3.14 Call Bridge またはクラスタの前提条件

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

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

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

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

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

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

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

- すべての Call Bridge に含まれるすべてのライセンス（従来のライセンスの場合）。クラスタでは、すべてのユーザライセンスや、録音およびストリーミングライセンスを、各 Call Bridge のライセンスファイルに含める必要があります。これらのライセンスがすべての Call Bridge に含まれていない場合は、Meeting Management から誤ったライセンス情報とコンプライアンスステータスがレポートされる可能性があります。クラスタ内でライセンスを共有する方法については、Cisco Meeting Server の『*Scalability & Resilience Server Deployment Guide*』の付録 C を参照してください。

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

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

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

Meeting Server のバージョンが Meeting Management でサポートされていることを確認します。Meeting Management 3.2 は Cisco Meeting Server バージョン 3.2 でのみサポートされています。

3.16 サポートされている TMS バージョン

推奨	最小
15.10 以降	15.9 以降

3.17 TMS 前提条件

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

  TMS システム ID を検索するには、TMS 内で展開に移動して [設定（Settings）] タブに移動し、[設定の表示（View Settings]、[全般（General）] エリアに移動します。

- プライマリ Call Bridge：TMS が接続するクラスタ内の Call Bridge。

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

3.18 ポート情報

表 2：Meeting Management からの発信通信用のポート

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

表 3：Meeting Management への着信通信用のポート

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

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

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

4 初回セットアップの概要

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

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

初回のセットアップ中は、次の手順を実行します。

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

5 OVA の展開

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

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

OVA を導入するには、次の手順を実行します。

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

   注：IP 割り当ての設定が求められた場合は、空白のままにします。Meeting Management は独自の構成を持つため、この情報を使用しません。

5. VM のメモリが予約済みであることを確認してください。
   a. [設定（Configure）] タブに移動します。
   b. [設定（Settings）] ドロップダウンから、[VM ハードウェア（VM Hardware）] を選択します。
   c. [編集（Edit）] をクリックします。
   d. [メモリ（Memory）] タブで、[すべてのゲストメモリを予約（すべてロック）（Reserve all guest memory (All locked)）] をオンにします。
6. 展開環境が大きい場合（キャパシティの表を参照）、VM のハードウェア設定を変更します。
   a. [設定（Configure）] タブに移動します。
   b. [設定（Settings）] ドロップダウンから、[VM ハードウェア（VM Hardware）] を選択します。
   c. [編集（Edit）] をクリックします。
   d. [CPU] を 4 から 8 に変更します。
   e. [メモリ（Memory）] を 4 GB から 8 GB に変更します。
7. 新しい Meeting Management VM が展開された後、電源をオンにします。

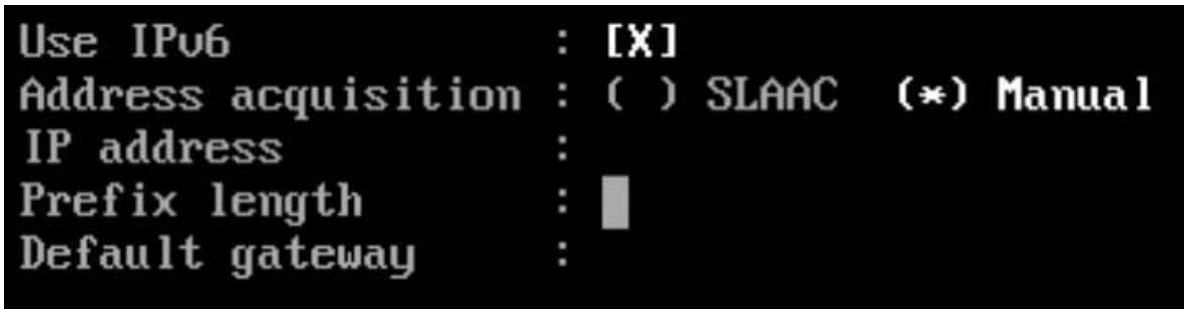
6 ネットワーク上での Meeting Management の設定

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

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

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

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



注：IPv6 アドレスの角カッコは、これらのフィールドでは使用できません。

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

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

注：IPv6 アドレスの角カッコは、このフィールドでは使用できません。

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

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

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

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

7 Web インターフェイスへのサインインとパスワードの変更

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

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

注：「同期された NTP ソースがありません」の警告は、通常は表示されませんが、Meeting Management がデフォルトの NTP サーバと同期されるまではしばらく表示される可能性があります

---

8 ネットワークの詳細の編集

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

ネットワーク設定を編集するには、次の手順を実行します。

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

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

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

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

9 証明書のアップロード

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

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

証明書を置き換えるには、次の手順を実行します。

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

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

証明書の要件

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

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

10 CDR 受信者アドレスの入力

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

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

CDR 受信者アドレスを入力するには、次の手順を実行します。

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

   注：今すぐ再起動するか、設定が完了するまで待ちます。

   ---

11 オプション：TMS への接続

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

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

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

1. [設定（Settings）] ページの [TMS] タブに移動します。
2. [Meeting Management で TMS を使用する（Use TMS with Meeting Management）] チェックボックスをオンにします。
3. TMS サーバの IP アドレスまたは FQDN を入力します。
4. HTTP または HTTPS を選択します。
5. オプション：証明書を使用することを選択し、証明書が無効な場合は 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 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 [ユーザ名（Username）] と [パスワード（Password）] を入力します。
8. 保存 して Meeting Management を**再起動**します。

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

12 NTP サーバの追加

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。表示されるオフセットは、接続されている各 NTP サーバと Meeting Management サーバ間の値です。

NTP サーバを追加するには、次の手順を実行します。

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

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

   ---

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

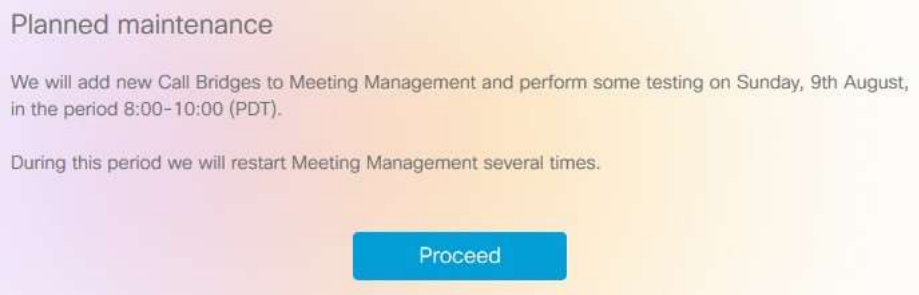
   注：今すぐ再起動するか、設定が完了するまで待ちます。

   ---

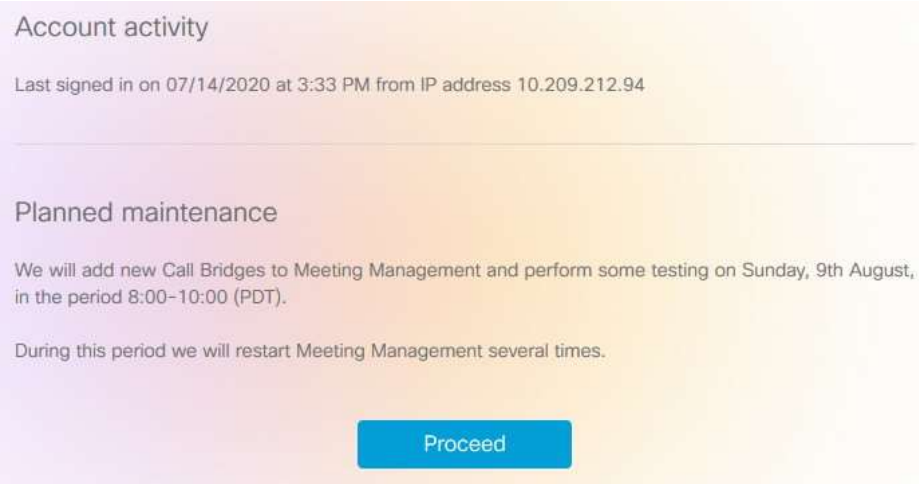
13 オプション：ユーザがログインするときに表示するメッセージの追加

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

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



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



注：変更はすぐに有効になります。

14 オプション：高度なセキュリティ設定の構成

[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。

14.1 レート制限のサインイン試行

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

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

2 つの設定があります。

- 1 つのトークンがバケットに追加される速度（秒）

  これは各間隔の長さ（秒）で測定されます。デフォルトは 300 秒です。

- バケットに保持されているトークンの最大数

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

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

14.2 アイドル セッション タイムアウト

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

アイドル セッション タイムアウトを有効にする場合、デフォルトのタイムアウトは 3600 秒（1 時間）です。最小値は 60 秒で、最大 86400 秒（24 時間）です。

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

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

14.3 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
- Call Bridge 数
- システムログサーバ
- 監査ログサーバ
- TMS
- Cisco Smart Software Manager

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

デフォルトでは、次の暗号スイートは無効になっています。

- AES256-SHA

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

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

15 ログサーバの追加

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

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

システムログサーバを追加するには、次の手順を実行します。

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

   デフォルトポートは次のとおりです。

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

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

4. プロトコルを選択します。
5. オプション：証明書を使用することを選択し、証明書が無効な場合は 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 が HTTP 経由で外部アドレスに接続できるよう、ネットワークを構成する必要があります。

6. TLS を選択した場合は、**証明書をアップロードします**。

   証明書チェーンの要件は次のとおりです。

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

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

   注：今すぐ再起動するか、設定が完了するまで待ちます。

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

監査ログサーバを追加するには、次の手順を実行します。

1. [**ログ**（Logs）] ページで、[**監査ログサーバ**（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 が HTTP 経由で外部アドレスに接続できるよう、ネットワークを構成する必要があります。

   ---

6. TLS を選択した場合は、証明書をアップロードします。

   証明書チェーンの要件は次のとおりです。

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

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

   注：今すぐ再起動するか、設定が完了するまで待ちます。

   ---

16 Call Bridge の追加

[**サーバ**（Servers）] ページで、接続されている Meeting Server Call Bridge のすべてを表示および編集できます。また、新しい Call Bridge を追加したり、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 で予定されているミーティングを確認できます。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、[確認とコミット（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 を追加するには、次の手順を実行します。

1. [サーバ（Servers）] ページで、[コールブリッジの追加（Add Call Bridge）] をクリックします。
2. [サーバアドレス（Server address）] フィールドに、Call Bridge API 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。
3. [ポート（Port）] フィールドに、Call Bridge API 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。
4. Call Bridge API の [ユーザ名（Username）] と [パスワード（Password）] を入力します。

   注：セキュリティと監査上の理由から、Meeting Management 用に、個別のユーザアカウントを使用することを強く推奨します。
5. [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。
6. 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。

7. 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。

   ---

8. 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 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。

     ---

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

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

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

10. [追加（Add）] をクリックします。
11. 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 がクラスタの一部である場合、クラスタ内の他の Call Bridge 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 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. Call Bridge の [アクション（Actions）] 列で、 をクリックします。
3. 該当する場合、Call Bridge 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 が追加されるまで続行します。

Call Bridge 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。

17 ライセンスモードの選択

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

ライセンスモードを選択する必要があります。以下の中から選択します。

- **スマートライセンス**（推奨）

  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 Smart Software Manager から取得します。

  注：Meeting Management のスマートライセンスには、次の制限があります。

  - ライセンスの予約は Meeting Management ではサポートされていません。
  - 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。

- 従来のライセンス

  従来のライセンスを選択すると、Meeting Management は、接続されている Call Bridge にインストールされているライセンスファイルから購入したライセンスに関する情報を取得します。

  注：このオプションは、接続されている Call Bridge にインストールされている従来のライセンスがすでにある場合のみ使用できます。従来のライセンスは段階的に廃止され、新しい顧客には提供されません。

  注意：Call Bridge にアクティベーションキー（API では callBridge または callBridgeNoEncryption と呼ばれます）がない場合、Meeting Server の管理者がすべての Call Bridge に正しいアクティベーションキーをインストールするまで、クラスタ全体が高い強制レベルになります。

- 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または従来の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：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。

17.1 従来のライセンスを有効にする方法

接続されている Call Bridge にインストールする必要があるライセンスがある場合は、従来のライセンスモードを選択した後に何もする必要はありません。

注：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、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：Meeting Management をテストする場合に、すべての機能のライセンスを持っていない場合は、[ライセンス（Licenses）] ページでトライアルを開始できます。

17.2 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。
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。

17.3 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。
- 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、レポートに別のミーティング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。

18 オプション：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ミーティング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. 予定されているミーティング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。

19 オプション：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、参加者をミーティングに追加する際に連絡先を検索できます。TMS で連絡先を検索する場合と同じように検索できます。

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

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

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

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

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

  電話帳には連絡が取れる連絡先だけが含まれるよう、まず最初に編集することを推奨します。
- TMS の Meeting Management に電話帳を割り当てます。
- Meeting Management での TMS 電話帳の使用を有効にします。

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

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

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

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

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

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

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

電話帳の使用を開始するには、次の手順を実行します。

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

20 LDAP サーバの設定

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

20.1 LDAP サーバの設定

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

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

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

   デフォルトのポート番号：

   - *LDAP：389*
   - *LDAPS：636*

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

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

5. オプション：証明書を使用することを選択し、証明書が無効な場合は 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 が HTTP 経由で外部アドレスに接続できるよう、ネットワークを構成する必要があります。

   ---

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

   証明書の要件

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

7. バインド DN とパスワードを入力します。

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

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

   ---

8. [ベース DN（Base DN）]（ベース識別名）を追加します。

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

   注：このフィールドは大文字と小文字を区別します。

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

   ---

9. [検索属性（Search attribute）] を選択します。

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

   注：このフィールドは大文字と小文字を区別します。

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

    注：今すぐ再起動するか、設定が完了するまで待ちます。

21 LDAP グループの追加

LDAP ユーザグループは LDAP サーバ上で構成され、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。

21.1 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 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。

22 オプション：ローカルユーザのセキュリティポリシーの設定

ローカルユーザ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。今すぐ再起動するか、初期構成が完了するまで待ちます。

注：パスワードポリシーの強制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。

---

23 オプション：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. ユーザ名を入力します。

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

4. オプション：名と姓を入力します。
5. ロールを割り当てます。
6. 新しいパスワードを作成します。
7. パスワードを確認し、[追加（Add）] をクリックします。

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。

24 確認、保存、およびバックアップ

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

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

25 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

25.1 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。

25.2 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。

26 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、ミーティング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ミーティングの開始時間と、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。ミーティングの詳細に表示される時間は正しいですが、イベントログのエントリには新しいタイムスタンプが与えられます。

アクセシビリティ通知

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 ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されており、この参照により本書に組み込まれるものとします。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。全著作権所有。著作権©1981、カリフォルニア大学理事会。

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 IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

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

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

Cisco の商標

Cisco および Cisco のロゴは、米国およびその他の国における Cisco およびその関連会社の商標を示します。Cisco の商標の一覧については、www.cisco.com/go/trademarks をご覧ください。Third-party trademarks mentioned are the property of their respective owners. 「パートナー」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。（1721R）