Cisco Meeting Management

リリース 3.10

インストールおよび設定ガイド

2024 年 9 月 27 日

目次

ドキュメントの改訂履歴 6

1. はじめに 7

2. 3.10 の新機能 8

2.1 3.9 以降のこのガイドの変更点 8

3. 開始する前に 9

3.1 容量 9

3.2 Meeting Management VM の要件 10

3.3 レジリエンス 10

3.4 ネットワークの詳細、CDR 受信者、NTP 11

3.5 ユーザ（Users） 12

3.6 LDAP 経由のユーザアクセス 13

3.7 ローカル ユーザ アクセス 14

3.8 ローカルユーザ用のセキュリティポリシー設定 15

3.9 サポートされるブラウザ 15

3.10 システムログサーバー 16

3.11 監査ログサーバー 16

3.12 ミーティングサーバのライセンス 17

3.13 Meeting Management の証明書 18

3.14 Call Bridge またはクラスタの前提条件 19

3.15 サポートされている Cisco ミーティングサーバのバージョン 20

3.16 サポート対象の TMS バージョン 21

3.17 TMS 前提条件 21

3.18 ポート情報 23

4. 初回セットアップの概要 24

5. OVA を展開する 26

6. ネットワーク上で Meeting Management をセットアップする....28
7. ウェブインタフェースにログインしてパスワードを変更する....30
8. ネットワーク詳細の編集....31
9. 証明書のアップロード....32
10. CDR 受信者アドレスをする....33
11. オプション: TMS に接続....34
12. NTP サーバの追加....36
13. オプション: ユーザーのサインイン時に表示するメッセージを追加する....37
14. オプション: 高度なセキュリティ設定を構成する....38
14.1 サインイン試行のレート制限....38
14.2 アイドル セッションのタイムアウト....39
14.3 Meeting Server のパスワードをリセット....39
14.4 TLS 設定....39
15. ログサーバの追加....41
16. サーバの追加....44
16.1 設定したサーバーの追加....45
16.2 新しいサーバーを設定する....48
16.2.1 ステージング....48
16.2.2 新規ミーティングサーバの追加....49
17. 証明書....51
17.1 CA 署名付き証明書....51
17.1.1 CSR による新しい証明書....51
17.1.2 既存の証明書とキーを使用....53
17.2 自己署名証明書....55
18. ネットワーク....56
18.1 DNS または NTP サーバの削除....57
19. Call Bridge....58

20. Web Bridge 59

21. 電話会議ユーザー 60

21.1 LDAP 検索とユーザ マッピングをカスタマイズする 61

22. セキュリティ 65

23. プッシュ構成 66

23.1 SSH 機能 67

24. ライセンスモードを選択する 68

24.1 スマート ライセンスを有効にする方法 69

24.2 スマートライセンスが有効になった後のスマートライセンスアクション 70

24.3 ライセンス予約 71

24.3.1 ライセンス予約 72

24.3.2 予約済みライセンスを更新する 74

24.3.3 予約済みライセンスを返却する 76

24.3.4 スマートライセンスに移行する際の考慮事項 77

25. オプション: クラスタを TMS に関連付ける 79

26. オプション: TMS 電話帳にアクセスする 80

27. LDAP サーバーのセットアップ 82

27.1 LDAP サーバーのセットアップ 82

28. LDAP グループの追加 84

28.1 LDAP ユーザグループの追加 84

29. オプション: ローカルユーザーのセキュリティポリシーをセットアップする 86

30. オプション: ローカルユーザーを追加する 89

31. 確認、保存、バックアップ 91

32. バックアップと復元 92

32.1 バックアップを作成する 92

32.2 バックアップを復元する 93

32 キーをアップロードしてアップグレードイメージを検証する 95

33 ミーティング管理の再起動 96

アクセシビリティ通知 97

34 アクセシビリティサポート機能 98
34.1 キーボード ナビゲーション 98
34.2 スクリーンリーダーのサポート 98

Cisco の法的情報 99
Cisco の商標または登録商標 100

ドキュメントの改訂履歴

表 1: ドキュメントの改訂履歴

日付	説明
2024-09-27	ドキュメントが公開されました。

1. はじめに

このガイドは Cisco Meeting Management の管理者を対象に、Cisco Meeting Management のインストールと設定の方法を説明しています。

Cisco Meeting Management は、Cisco のオンプレミス ビデオ会議プラットフォームである Cisco Meeting Server の管理ツールです。 ライセンスを管理し、Meeting Server にユーザーに分かりやすいインターフェイスを提供します。

ミーティング管理管理者は、次のことを実行できます:

- ミーティング管理をインストールして設定する
- ミーティングサーバのライセンス設定を編集する
- Meeting Server でスペーステンプレートとウェブアプリユーザーをプロビジョニングする
- スペースの作成と管理をし、ブラストダイヤルの設定をする
- ビデオ オペレータとして機能する

ビデオ オペレータは次のことを実行できます。

- すべてのアクティブなミーティング、および過去 1 週間以内に終了したミーティングを表示する
- Cisco TMS（TelePresence Management Suite）を使用してスケジュールした、開催予定のミーティングを表示する
- 進行中のミーティングを管理する
- 現在のミーティングサーバのライセンス状況を確認する

ミーティングサーバ 3.0 以降では Cisco Meeting Management 3.0 以降が必須であり、追加のライセンスは必要ありません。

2. 3.10 の新機能

新機能と変更点の概要については、リリース ノートを参照してください。

2.1 3.9 以降のこのガイドの変更点

- ミーティング管理 VM のハイパーバイザー要件を更新しました。
- パスフレーズの複雑さを使用してユーザーパスワードの強度を確認し、パスワードの有効期限を強制してパスワードが使用できる期間（日数）を設定する手順を追加しました。

3. 開始する前に

開始する前に、お使いの環境がミーティング管理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、いくつかの情報を用意しておく必要があります。

ミーティング管理では、単一の Call Bridge から複数のクラスタ展開まで、あらゆるものを管理できます。 VM の要件は、展開のサイズによって異なります。 以下の容量表を参照して、展開サイズを決定します。

3.1 容量

表 2: 導入サイズを決定するための容量表

Type	中小規模の導入	大規模導入
Call Bridge 数	1-8 Cisco Meeting Server 1000 上で実行される 1 ~ 8 の Call Bridge **または** Cisco Meeting Server 2000 上で実行される 1 つの Call Bridge	Cisco Meeting Server 1000 上で実行される 9 ~ 24 の Call Bridge **または** Cisco Meeting Server 2000 上で実行される 2 ~ 3 つの Call Bridge
開始されたコールログ（ピーク時、すべての Call Bridge 間）	毎秒 10 コールログを開始	毎秒 20 コールログを開始
ユーザーが、同時に Meeting Management にサインイン	15 人の同時ユーザ	25 人の同時ユーザ
1 週ごとのミーティング（Call Bridge 全体）	10,000	10,000

メモ: リストされている Call Bridge の数は、主に予想されるコール量に基づいています。 接続されているすべてのクラスターでミーティング管理機能が無効になっている場合、小規模な展開の VM 要件は、どの展開サイズでも十分になります。

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ことを確認してください。

表 3: Meeting Management VM **の要件**

要件	中小規模の展開	大規模な展開
サーバーの製造元	任意（Any）	任意（Any）
プロセッサタイプ	Intel / AMD	Intel / AMD
プロセッサ周波数	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 Eager Zeroing を推奨します。*	100 GB *シックプロビジョニングと Eager Zeroing を推奨します。*
RAM	4 GB の予約メモリ	8 GB の予約メモリ
ハイパーバイザー	ESXi 8.0 U3、ESXi 7.0 U3q	ESXi 8.0 U3、ESXi 7.0 U3q
ネットワークインターフェース	1	1

メモ: VM は中小規模の展開向けに構成されています。 大規模な展開の場合、セットアップ中にサイズを手動で変更する必要があります。

メモ: 中規模導入で、後でより大きなキャパシティが必要になると想定される場合は、大規模導入に VM を設定します。

3.3 レジリエンス

Meeting Management の導入にレジリエンスを追加する場合、同じ Meeting Server 導入に Meeting Management の最大 2 つのインスタンスに接続できます。

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どうかを決定します。 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、接続された Call Bridge および TMS から直接情報を取得します。 これらの間で情報が交換されることはありません。停電や接続の問題が同時に両方のインスタンスに影響を与えないように、Meeting Management の 2 つのインスタンスは異なる場所に配置することが推奨されます。

また、Meeting Management の適切なインスタンスにユーザーをダイレクトする方法を決定します。

次のオプションがあります。

a. **ユーザーは特定のインスタンスに手動でログインします。** 各インスタンスのアドレス (FQDN) を定義し、ユーザーに 1 つにログインするよう要求します。 問題が発生した場合、他のインスタンスにログインし、管理者に知らせる必要があります。

b. **ユーザートラフィックはリダイレクトされます。** 各インスタンスのアドレス（FQDN）を定義することに加えて、1 つのインスタンスにリダイレクトする 3 番目のユーザー向けアドレスを作成します。 ユーザーに、常にユーザー向けアドレスにサインインするように要求します。 問題がある場合、管理者はリダイレクトを変更する必要があります。

メモ: ユーザーが常に 1 つのユーザー向けアドレスを使用している場合でも、Meeting Management の各インスタンスは一意の CDR 受信者アドレスを持つ必要があります。

メモ: ミーティング管理の各インスタンスに対して、証明書を作成することをお勧めします。 各証明書には、ユーザ向けアドレスと固有の CDR 受信者アドレスの両方が含まれている必要があります。 「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、NTP

ネットワーク上でミーティング管理をセットアップする前に、以下の詳細を知っておく必要があります (ターミナルのセットアップ):

- お使いの Meeting Management のホスト名
- IPv4 および/または IPv6 アドレス
  手動で入力するか、または DHCP/SLAAC を選択します
- デフォルト ゲートウェイ (DHCP/SLAAC を使用しない場合)
- 1 DNS サーバの IP アドレス (必要な場合)

初回セットアップの完了時に、他の詳細を追加できます。

- CDR 受信者アドレス

  CDR 受信者アドレスは、Meeting Management が CDR（通話詳細記録）を送信するように Call Bridge に通知する FQDN です。 Meeting Management でミーティング情報を表示するには、CDR 受信者のアドレスが正しく設定されている必要があります。

メモ: ミーティング管理に DNS レコードをセットアップしていることを確認してください。 また、CDR 受信者アドレスとして Meeting Management が設定されている FQDN に到達するよう、Call Bridge にファイアウォールが開いていることを確認します。

メモ: すべてのクラスタの Meeting Management を無効にしている場合、CDR 受信者アドレスは必要ありませんが、Meeting Management はエラー通知を表示します。

- 最大 5 つの NTP サーバーの IP または FQDN、および対応する NTPv3 対称キーMeeting Management には、接続した Call Bridge および TMS サーバーに使用しているのと同じ NTP サーバーを使用することを推奨します。
- オプション: 追加の DNS サーバーの IP

3.5 ユーザ（Users）

Meeting Management は、ローカルで管理されるユーザーおよび LDAP 経由のユーザー認証をサポートしています。 ローカルユーザーのみ、LDAP ユーザーのみ、またはその両方から選択できます。

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

  インストール時に 1 人のローカル管理者ユーザーが生成されます。最初のログイン後にユーザーを追加することができます。 ローカルユーザは、セットアップやテストを行う場合や、[ミーティング管理] からロックアウトされることなく LDAP を変更する場合に役立ちます。

- LDAP **ユーザー**は、マッピング経由で LDAP サーバーの既存グループに追加されます。ミーティング管理は LDAP サーバを使用してこれらのユーザを認証し、ログイン時にグループメンバーシップを確認します。

  LDAP による認証は、一般的な使用および管理にお勧めします。

少なくとも 1 つのローカル管理者ユーザ アカウントを持っていることを推奨します。 これにより、LDAP に問題がある場合でもミーティング管理にアクセスできるようになります。 本番環境での一般的な使用では、LDAP 経由でユーザを認証することを推奨します。

メモ:本番環境では LDAP の使用を推奨しているため、LDAP が設定されていない場合は、ミーティング管理が常に警告を表示します。

ユーザは 2 つのロールを持つことができます。

- **管理者**には、Meeting Management へのフルアクセス権があります。 管理者は通常、ミーティング管理のセットアップ、構成の変更、ユーザの追加、およびシステムの監視とメンテナンスを行います。 管理者は、ビデオ オペレータを特定のスペースにタグ付けして、それらのスペースに関連付けられたミーティングのみにアクセスできるようにすることができます。
- **ビデオオペレータ**は、[**ミーティング（Meetings）**] および [**概要（Overview）**] ページへのアクセス権のみを持ちます。 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連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発信しようとしたり、音声の問題が発生している参加者に通話統計を確認したりできます。 ビデオ オペレータは、管理者によって指定された、スペースで開催されたミーティングに関連するタスクを実行する権限を持ちます。

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属している場合、このユーザには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

ミーティング管理の一般的な使用および管理については、LDAP 経由でのユーザ認証を推奨しています。そのため、必要な LDAP グループを持つ LDAP サーバをセットアップ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、ビデオ オペレータ用に 1 つのグループを作成することをお勧めします。

メモ: ミーティング管理はネストされたグループをサポートしていません。 マッピングされたグループに他のグループが含まれる場合、これらのネストされたグループのメンバーはミーティング管理にアクセスできません。

サポートされている LDAP 実装は以下のとおりです。

- Microsoft Active Directory (AD)
- OpenLDAP

  メモ: OpenLDAP では、memberOf オーバーレイが有効になっている必要があります。

LDAP サーバに接続するには、以下が必要です。

- プロトコル (LDAP/LDAPS)
- LDAP サーバアドレス
- LDAP サーバのポート番号
- LDAP サーバ証明書 (LDAPS を使用している場合) 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 証明書まで、証明書チェーンの上位にある証明書が含まれている必要があります。*
  - *LDAP サーバアドレスが証明書に含まれている必要があります。*
- LDAP バインドユーザーの資格情報

セキュリティと監査上の理由から、ミーティング管理には別のバインドユーザアカウントを作成することをお勧めします。

- ベース識別名 (DN)
- 検索属性

  これは、ユーザがログイン時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ために必要なもの:

- 各グループの識別名

3.7 ローカル ユーザ アクセス

LDAP 設定に問題がある場合にログインできるように、少なくとも 1 人のローカル管理者ユーザを用意しておくことを推奨します。 テスト目的や LDAP 設定の変更にローカルユーザを使用することもできます。

メモ: プロダクションでの一般的な使用では、すべてのユーザ (管理者とビデオ オペレータの両方) を LDAP で認証することを推奨します。

インストール中、ミーティング管理はローカル管理者ユーザアカウントを作成します。このアカウントを使ってウェブインタフェースにログインし、セットアップを完了できます。 お使いのネットワークに Meeting Management をセットアップする場合、ユーザー名と生成されたパスワードは、VM コンソールに表示されます。

メモ: ウェブインタフェースに初めてログインした後、初めてミーティング管理を再起動するまでは、生成された資格情報はコンソールにのみ表示されます。 パスワードはログインしたらすぐに変更することをお勧めします。

追加のローカルユーザをセットアップするには、以下が必要です。

- 各ユーザのユーザ名

  メモ: ユーザプロファイルを保存した後は、ユーザ名を変更することはできません。

- オプション: 各ユーザーの名
- オプション: 各ユーザーの姓
- 各ユーザの役割
- 各ユーザのパスワード (必要な場合)

組み込みのパスフレーズ ジェネレータを使用する場合、パスワードを自分で定義する代わりに、生成されたパスワードを使用できます。

ユーザはログインした後でパスワードを変更できます。

3.8 ローカルユーザ用のセキュリティポリシー設定

ローカルユーザに対して次のセキュリティポリシーをセットアップすることができます:

- パスワードの最小文字数を要求する

  これは選択するまで無効になっています。 デフォルトの最小文字数は 8 文字です

- 組み込みのパスフレーズジェネレータを有効にする

  内蔵のパスフレーズ ジェネレーターが辞書から単語を組み合わせて新しいパスワードを提案します。 パスフレーズのデフォルトの単語数は 5 で、1 ~ 8 の間で任意の数を選択できます。

  内蔵のパスフレーズ ジェネレーターを使用する場合は、辞書を提供する必要があります。

  辞書の要件:

  - *辞書は各行に 1 単語を含むテキストファイルでなければなりません。*
  - *文字は UTF-8 でエンコードされている必要があります。*
  - *このファイルには null 文字が含まれていてはなりません。*
  - *ファイルサイズの上限は 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っています。 値を入力するまで、入力フィールドは空白になっています。

3.9 サポートされるブラウザ

Cisco ミーティング管理は、以下のブラウザの最新リリース バージョンに対応しています。

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

次のテクノロジを有効にする必要があります。

- WebSocket
- HTML5
- JavaScript

メモ: Internet Explorer は更新を強制しないため、最新バージョンであることを手動で確認することをお勧めします。

3.10 システムログサーバー

ログストレージは、Meeting Management で制限されています。 しかし、syslog レコードはリモートロケーションに送信することができます。 最大 5 つの外部 syslog サーバーを構成してシステムログを収集できます。

外部システムログサーバーをセットアップすることを強くお勧めします。 トラブルシューティングとサポートにはシステムログが必要です。

ログサーバーをミーティング管理に接続するには、以下が必要です。

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

メモ: TLS 接続は TLS 1.2 をサポートしている必要があります

メモ: すべてのメッセージをフルの長さで表示する場合は、最大 8192 バイトの長さのメッセージを受け入れ、表示できるシステムログサーバーを使用する必要があります。

3.11 監査ログサーバー

監査ログには、サインイン、ミーティング管理設定の変更、ビデオオペレーターアクションの実行など、ミーティング管理でのユーザーのアクションに関する情報が含まれます。

ミーティング管理でのログストレージが制限されており、ローカルに保存された監査ログはローカルシステムログでのみ利用できます。 ただし、別の監査ログを syslog レコードとしてリモートの場所に送信できます。 監査ログを収集するために、最大 5 つの外部 syslog サーバーを構成できます。

監査ログサーバーはオプションですが、組織によっては必須になる場合があります。

ログサーバーをミーティング管理に接続するには、以下が必要です。

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

メモ: TLS 接続は TLS 1.2 をサポートしている必要があります

メモ: すべてのメッセージをフルの長さで表示する場合は、最大 8192 バイトの長さのメッセージを受け入れ、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 サーバの特定のハードウェアまたは VM の要件は、ミーティングサーバの展開とミーティング管理の使用状況によって異なります。

3.12 ミーティングサーバのライセンス

Meeting Management は Meeting Server 3.0 以降では必須です。これは、Meeting Server のライセンスが Meeting Management に依存しているためです。
Meeting Management の各インスタンスに対して、Smart Licensing またはライセンスなしを選択できます。

復元力のある展開では、使用状況の重複レポートを避けるため、ライセンスには Meeting Management のインスタンスを 1 つだけ使用します。 一方のインスタンスでライセンシングモードを Smart Licensing に設定し、もう一方のインスタンスではライセンスなしに設定します。

メモ: すべてのミーティングサーバクラスタは、ライセンスが有効になっているミーティング管理のインスタンスに接続されている必要があります。 レジリエンスのある導入があり、Meeting Management のライセンス管理が有効な場合、Meeting Management の 1 つのみのインスタンスのライセンス管理を無効にします。

スマート ライセンスの場合、以下が必要です。

- 会社のスマートアカウントと、1 つの Meeting Management のインスタンスでのみ使用される専用のバーチャルアカウントが必要です。

  アカウントを要求する場合は、Cisco アカウントチームに連絡するか、Cisco Software Central にアクセスします。

- ミーティング管理で使用するバーチャルアカウントに、適切なライセンスを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は、1 つの Meeting Management インスタンスに接続することができます。 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、ミーティング管理経由で接続されているすべてのクラスタ間で共有されることにも注意してください。

クラスタに個別にライセンスを付与する場合は、別の Meeting Management 導入およびバーチャルアカウントに接続する必要があります。

- 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 を使用することができます。

  *プロキシサーバーを使用している場合、アドレス、ポート番号、証明書が利用可能である必要があります。これにより、[**転送設定を編集（**Edit Transport Settings）] を実行できます。*

- オプション: 純粋なオンプレミス環境の場合、Cisco Smart Software Manager On-Prem (SSM On-Prem) を使用することが可能です。これは、特定の時間にのみ接続してデータを交換します。 ミーティング管理はバージョン 8-202008 以降をサポートしています。

メモ: Cisco Smart Software Manager オンプレミスに接続する際に、Meeting Management の認証が拒否される場合、SSM オンプレミスにログインし、**有効な** Call Bridge **ノード**ライセンスが原因で認証ができないのかどうかを確認します。 はいの場合、SSM On-Prem をスマート アカウントに再同期すると、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、アドレス、ポート番号、証明書が利用可能である必要があります。これにより、[**転送設定を編集（**Edit Transport Settings）] を実行できます。 ゲートウェイアドレスには、セットアップに応じて、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、ブラウザおよび Call Bridge に対してそれ自体を識別します。
セットアップ中に、Meeting Management は初期設定中に使用できる自己署名証明書を生成します。 本番環境では、自己署名証明書を CA (認証局) によって署名された証明書と置き換える必要があります。 組織の要件に応じて、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 証明書まで、証明書チェーンの上位にある証明書が含まれている必要があります。
- CDR 受信者アドレス、およびユーザがブラウザ インターフェイスに使用するアドレスは、証明書に含まれている必要があります。 さらに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。

  メモ: SAN フィールドが使用されている場合、Meeting Management は共通名を参照しません。CDR 受信者アドレスは SAN フィールドに含まれている必要があります。

メモ: Meeting Management には、証明書の署名要求を作成する機能がありません。OpenSSL ツールキットなどの専用ツールを使用して、秘密鍵と証明書署名リクエストを作成します。

メモ: Meeting Management の 2 つのインスタンスを設定する場合、各インスタンスに独自の証明書を設定することをお勧めします。

3.14 Call Bridge またはクラスタの前提条件

ミーティング管理をインストールして設定する前に、展開がこれらの前提条件を満たしていることを確認してください:

- Meeting Server API **のユーザーアカウントです** 。 ミーティング管理は API 経由で Cisco Meeting Server に接続します。 セキュリティおよび監査上の理由から、ミーティング管理には別のアカウントをセットアップすることをお勧めします。 複数のインスタンスを使用している場合、Meeting Management のインスタンスごとに個別のアカウントが必要です。

  アカウントのセットアップ方法については、『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。 プログラミングガイド ページ (cisco.com) で見つけることができます。
- CDR **容量。** 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に、ミーティング管理はそれ自体を各 Call Bridge の CDR (通話詳細レコード) 受信者として設定します。 ミーティング管理の各インスタンスに適した容量が Call Bridge にあることを確認します。

  メモ: クラスタのライセンスとプロビジョニングのみにミーティング管理を使用する場合、そのクラスタの Call Bridge に CDR 容量は必要ありません。

- NTP **サーバ。** 導入では、各 Meeting Server に対してタイムサーバーを設定し、Call Bridge と Meeting Management が同期されていることを確認する必要があります。 ミーティング管理とミーティングサーバの展開で同じ NTP サーバを使用することを推奨します。 NTP サーバーのキーも必要となる可能性があります。
- **オプション**: **レコーダー。** ミーティング管理を使用して録画を開始および停止する場合、展開内のミーティングサーバにレコーダーが設定されている必要があります。
- **オプション**: **ストリーマ。** ミーティング管理を使用してストリーミングを開始および停止する場合、展開内のミーティングサーバでストリーマが設定されている必要があります。
- **オプション**: [**参加者を移動（**Move participant**）**] **で必要な設定です。** ミーティング間で参加者を移動させたい場合は、ミーティングサーバの展開に対する特定の要件があります。 特に、SIP エンドポイントを使用する参加者は、Cisco Expressway でプロビジョニングされている場合、移動できないことに注意してください。 さらに、ミーティングサーバ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 を使用して参加者を電話会議間で移動させる』の「参加者を移動する際の制限」を参照してください。*

[ミーティング管理] を設定する場合、各 Call Bridge で以下が必要です。

- ウェブ管理インターフェイスの IP アドレスまたは FQDN
- ウェブ管理インターフェースのポート番号
- ミーティング管理で使用するためにセットアップした API ユーザアカウントのユーザ名とパスワード
- 検証に信頼できる証明書を使用する場合、ウェブ管理インターフェイスの CA 証明書が必要です。

メモ: VM は MMP コマンド「シャットダウン」を使用してシャットダウンする必要があります。これにより、ミーティングサーバは、ミーティングの参加者を含むすべての接続済みデバイスおよび Meeting Management に適切な切断メッセージを送信します。

アクティブなミーティング中に Meeting Server VM の電源が突然が切れたり、シャットダウンされたりした場合、参加者は接続が切断されますが、また、Meeting Server への接続が回復するまで、[音声/ビデオのミュート] ボタンは読み込み状態のままになります。

3.15 サポートされている Cisco ミーティングサーバのバージョン

ミーティングサーバのバージョンがミーティング管理でサポートされていることを確認してください。 ミーティング管理 3.10 は、Cisco ミーティング サーババージョン 3.10 でのみサポートされています。

3.16 サポート対象の TMS バージョン

表 4: 推奨バージョン	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、導入が次の要件を満たしていることを確認してください:

- TMS **に接続された** Call Bridges。 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 インテグレーションおよびスケジュール API ガイド』を参照してください。 Cisco ミーティングサーバのドキュメントページの [設定例とテクニカルノート] に記載されています。

- **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、および監査上の理由から、ミーティング管理には別のアカウントをセットアップすることをお勧めします。 Meeting Management で 2 つ以上のインスタンスを使用している場合は、それぞれのインスタンスに対して個別のアカウントを作成します。

  手順については、「TMS API ドキュメント」、『*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。*

  メモ: TMS 電話帳へのアクセスとスケジュール済みミーティングに関する情報の取得には、同じアカウントが使用されます。

- NTP **サーバー**。 Call Bridge と TMS サーバーが同期されるように、時刻サーバーを TMS サーバーに設定する必要があります。 ミーティング管理と TMS に同じ 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 **フェールオーバーの無効化**。 失敗した場合、**自動** MCU **フェールオーバー**が TMS 内の 1 つのシステムから別のシステムにスケジュールされたミーティングを移動します。 これは、1 つの Meeting Server 導入から別の導入への場合がありますが、MCU など、異なるタイプのシステムに対する場合もあります。

  その結果、ミーティングがミーティング管理でスケジュール通りに表示される場合がありますが、アクティブにはならず、ビデオオペレータはミーティング管理を使用してミーティングを監視または管理できません。

  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 と Meeting Management **でクラスタに同じ名前を使用する。** 管理者にとっては、ミーティング管理でクラスタ表示名として使用するのと同じ名前を、ミーティングサーバ展開の TMS で使用すると便利です。 オペレータにとっては、[ミーティング管理] のプライマリ Call Bridge の名前を TMS のミーティング サーバ展開の名前と簡単に関連付けることができると便利です。
- **オプション**: **サポートされているプロトコルを使った電話帳連絡先** ミーティング管理で TMS 電話帳を使用する場合は、ミーティング管理に指定した電話帳の連絡先全員にミーティングサーバがアクセスできることを確認してください。

ミーティング管理を 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: ミーティング管理が TMS と統合されており、多くのミーティングがスケジュールされている場合、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、通知メール

が遅延したり、ミーティングの開始が若干遅れることがありました。

影響は、週にスケジュールするミーティングの数と手動で同期する頻度、さらに TMS とその

SQL データベースサーバのサイズによって異なります。

TMS をミーティング管理に接続するには、以下の情報が必要です。

- TMS ブッキング API サーバの IP アドレスまたは FQDN
- TMS の CA 証明書 (必要な場合)
- TMS の Meeting Management 用にセットアップしたサイト管理者ユーザーアカウントのサインイン情報

各 Cisco ミーティングサーバの展開について、TMS からの以下の情報が必要です。

- TMS **システム** ID: 接続された Cisco ミーティングサーバ展開に TMS が指定する識別子です。

  *TMS システム ID を確認するには: TMS で、導入に移動し、[**設定**（Settings）] タブに移動し、[**設定の表示**（View Settings）]、[**全般**（General）] 領域の順に移動します。*

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

  *接続している Call Bridge TMS を確認する: 導入に移動し、[**設定**（Settings）] タブ、[**設定を表示**（View Settings）]、[**全般**（General）] 領域の順に選択します。 [**ネットワークアドレス**（Network Address）] は、接続された Call Bridge の IP アドレスです。*

3.18 ポート情報

表 5: Meeting Management からの発信通信用ポート

目的	Protocol（プロトコル）	宛先ポート
Syslog	TCP、UDP	514（または設定した通り）
Syslog	TLS	6514（または設定した通り）
LDAP	LDAP	389（または設定した通り）
LDAP	LDAPS	636（または設定した通り）
（ベース DN が DC レベルでのみ指定されている）LDAP グローバルカタログ	LDAP	3268（または設定した通り）
（ベース DN が DC レベルでのみ指定されている）LDAP グローバルカタログ	LDAPS	3269（または設定した通り）
時刻同期 (NTP)	UDP	123
名前解決（DNS）	UDP	53
TMS ブッキング API	HTTP	80
TMS ブッキング API	HTTPS	443
証明書配布ポイント	HTTP	80
Smart Licensing ダイレクト	HTTPS	443
プロキシ経由の Smart Licensing	HTTPS	443 (または構成済み)
Cisco Transport Gateway	HTTPS	443
Webex クラウドと Control Hub	HTTPS	443 (または構成済み)

表 6: Meeting Management への着信通信用ポート

目的	Protocol（プロトコル）	宛先ポート
ウェブインタフェース	HTTPS	443

表 7: Meeting Management への着信と発信の両方のポート

目的	Protocol（プロトコル）	宛先ポート
Cisco Meeting Server API Cisco Meeting Server CDR Meeting Server のイベント	HTTPS	443 (またはミーティングサーバの MMP での設定)

4. 初回セットアップの概要

Meeting Management のセットアップを開始する前に、「開始前に」を参照して、すべての準備が整っていることを確認します。

ミーティング管理は、Cisco Meeting Server サポート契約を結んでいるすべての顧客に対し、OVA ファイルとして cisco.com から入手できます。

初めてのセットアップでは、次の手順を実行します。

1. OVA を展開する。
2. ネットワーク上で Meeting Management をセットアップする。
3. 生成された資格情報でサインインし、パスワードを変更する。
4. 設定の編集:
    a. ネットワーク設定を編集する。
    b. 証明書をアップロードする。
    c. CDR 受信者アドレスを入力する。
    d. オプション: TMS に接続する。
    e. NTP サーバーを追加する。
    f. オプション: サインインメッセージを追加する。
    g. オプション: 高度なセキュリティ設定を設定する。
5. ログサーバを追加します。
6. 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 詳細を保存するために Meeting Management を再起動する。
7. Call Bridge を追加します。
    a. 既存のミーティングサーバを追加します
    b. 新規 Meeting Server を設定して追加する
8. ライセンスモードを選択する
9. オプション: クラスタを TMS に関連付ける
10. オプション: TMS 電話帳にアクセスする。

11. さらにユーザーを追加する:
    a. LDAP サーバーの詳細をセットアップする。
    b. LDAP グループ を追加してください。
    c. オプション: ローカルユーザーのセキュリティポリシーをセットアップする。
    d. オプション: ローカルユーザーを追加する。
12. Meeting Management を再起動して、すべての設定を保存する。
13. バックアップ を作成してください。

5. OVA を展開する

メモ:vCenter サーバのリリースが 6.5.0b 以前の場合、[OVF **テンプレートの展開**] は HTML5 クライアントでは利用できません。 この場合、このステップでは Flash クライアントを使用する必要があります。

メモ: 説明は Flash クライアントをベースにしています。 お使いの vSphere クライアントは、以下に記載されている内容と多少異なる場合があります。

OVA を展開するには:

1. VMware 環境にログインします。
2. [**アクション**（Actions）]、[OVF**テンプレートを導入...**（**Deploy OVF Template...**）] の順に選択します。
3. **ローカルファイル**を選択し、cisco.com からダウンロードした OVA を参照します。
4. ウィザードに従い、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 割り当て設定を求められた場合は、空のままにします。 Meeting Management には独自の構成があり、この情報は使用されません。
   - OVA を Vcenter にアップロードして展開するとき、発行者フィールドは「(信頼できる証明書)」を表示する必要があります。 OVA のインポート時に、無効な証明書と信頼されていない証明書に関する警告が表示される場合は、次の記事を参照してください：https://kb.vmware.com/s/article/84240 OVA に署名するために使用される証明書に対応する中間証明書およびルート証明書を VECS ストアに追加する必要がある場合があります。 中間証明書またはルート証明書を入手する場合、またはその他の問題については、Cisco テクニカルサポートに連絡してください。

5. VM のメモリが予約されていることを確認します。
    a. [**設定（**Configure）] タブに移動します。
    b. [**設定（**Settings）] ドロップダウンで、[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** タブで **ゲストメモリを予約する** (**すべてロック済み**)にチェックを入れます。
6. 導入が大きい場合は (容量表を参照)、VM 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** ドロップダウンから **仮想マシンハードウェア**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**を 4 GB から 8 GB に変更してください。
7. 新しい Meeting Management VM を導入したら、電源をオンにします。

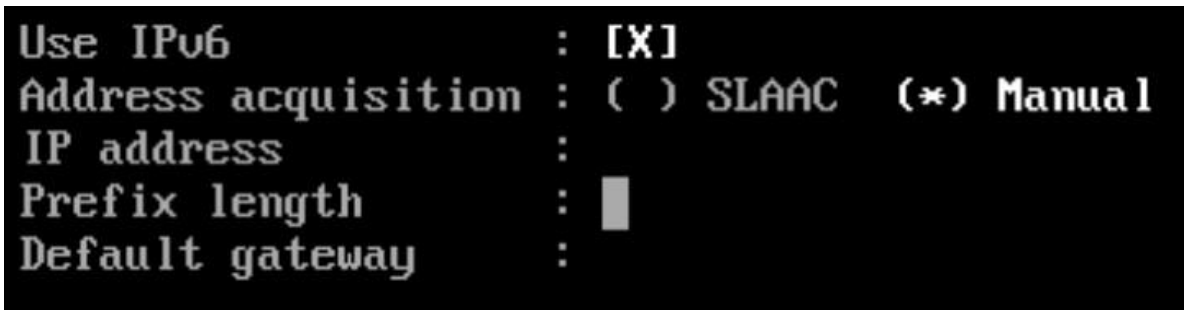
6. ネットワーク上で Meeting Management をセットアップする

メモ: ターミナルからのネットワーク設定中に、Meeting Management は入力が正しい形式であることを確認しますが、完全な確認は実行しません。 入力内容をよく確認してください。

メモ: ターミナルは US 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ときは注意してください。 たとえば、英国キーボードを使用している場合、Shift+2 キーを押して、@ を入力します。

ネットワーク上でミーティング管理をセットアップするには:

1. 導入した VM のコンソールを開きます。
2. Nextセットアップを開始するには、[**次へ**（Next）] を選択します。
3. ミーティング管理のホスト名を入力してください。
4. IPv4 を使用するかどうかを選択します。
5. DHCP または**手動による**アドレス取得を使用するかを選択します。
6. [**手動**（Manual）] を選択し、[IP**アドレス**（IP address）]、[**サブネットマスク**（Subnet mask）]、[**デフォルトゲートウェイ**（Default gateway）] を入力します。
7. IPv6 を使用するかどうかを選択します。
8. SLAAC または **手動** アドレス取得のどちらを使用するかを選択します。
9. SLAAC を使用しない場合は、[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。



メモ: IPv6 アドレスの角括弧はこれらのフィールドでは使用できません。

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

    このセットアップでは DNS サーバーを 1 つだけ追加できますが、後ほどブラウザインターフェイスからもう 1 つ追加することができます。

    メモ: IPv6 アドレスの角括弧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 を押下します。 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、生成された資格情報、自分で署名した証明書の指紋が表示されます。

    メモ: ミーティング管理でウェブインターフェイスにログインできるようになるまで数分かかることがあります。

    メモ: ウェブインタフェースに初めてログインした後、初めてミーティング管理を再起動するまでは、生成された資格情報はコンソールにのみ表示されます。 パスワードはログインしたらすぐに変更することをお勧めします。

7. ウェブインタフェースにログインしてパスワードを変更する

生成された資格情報を使用して、Meeting Management にサインインします。 サインイン中にパスワードを変更できます。

最初に表示されるのは、通知を含む概要ページです。 最初のログイン時に表示される通知は、構成が完了すると消えます。

メモ: **通常、[同期されたNTPソースがありません（**There are no synchronized NTP sources）] という警告メッセージは表示されませんが、Meeting Management がデフォルトの NTP サーバーと同期されるまで、短い期間で表示される可能性があります。

---

8. ネットワーク詳細の編集

基本ネットワークの詳細のセットアップは完了していますが、DNS サーバーの追加または設定の編集が必要な可能性があります。

ネットワーク設定を編集するには:

1. [**設定**（Settings）] ページ、[**ネットワーク**（Network）] タブの順に選択します。
2. 関連する詳細を入力します。

   メモ: IPv6 アドレスを入力する場合、ここで角括弧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。

   メモ: 今すぐ再起動するか、CDR 受信者アドレスの設定と TMS への接続が完了するまで待つことができます。

9. 証明書のアップロード

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

メモ: ミーティング管理には証明書署名リクエストを作成する機能がありません。 OpenSSL toolkit などの別のツールを使用して、秘密鍵と証明書署名リクエストを作成します。

証明書を置き換えるには:

1. [**設定**（Settings）] ページ、[**証明書**（Certificate）] タブの順に選択します。
2. **証明書をアップロード**して、自己署名証明書を置き換えます。
3. *アップロードキー。*
4. 詳細を**保存**して、Meeting Management を**再起動**します。

   メモ: 今すぐ再起動するか、CDR 受信者アドレスの設定と TMS への接続が完了するまで待つことができます。

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 証明書まで、証明書チェーンの上位にある証明書が含まれている必要があります。*
- *CDR 受信者アドレス、およびユーザがブラウザ インターフェイスに使用するアドレスは、証明書に含まれている必要があります。*

  メモ: SAN フィールドが使用されている場合、ミーティング管理は共通名を参照しません。CDR 受信者アドレスは SAN フィールドに含まれている必要があります。

10. CDR 受信者アドレスをする

CDR 受信者アドレスは、ミーティング管理が CDR (通話詳細記録) を送信するように Call Bridges に通知するアドレスです。 Meeting Management でミーティング情報を参照するには、CDR 受信者アドレスが正しく設定されていることが重要です。

メモ: IP アドレスは変更される可能性があるため、FQDN を使用することを強くお勧めします。 [CDR受信者アドレス（CDR Receiver address）] フィールドでは、Meeting Management が Call Bridge に使用するよう指示した内奥*のみ*を設定し、Meeting Management がより広いネットワークで表示される方法は設定しません。 Call Bridge から解決可能で到達可能なネットワークでセットアップされた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:

1. [**設定**（Settings）] ページ、[CDR] **タブ**の順に選択し、[CDR**受信者アドレス**（CDR receiver address）] 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。

   メモ: 今すぐ再起動するか、構成が完了するまで待ってください。

   ---

11. オプション: TMS に接続

開始前にスケジュールされたミーティングを確認したり、参加者を追加する際に TMS 電話帳を使用して連絡先を検索するには、TMS をミーティング管理に接続する必要があります。

メモ: TMS に接続する前に、Call Bridge を TMS ブッキング API に接続する必要があります。詳細については、 開始する前に のセクションを参照してください。

ミーティング管理を TMS に接続するには:

1. [**設定**] ページの [TMS] タブに移動します。
2. **ミーティング管理で** TMS **を使用する** チェックボックスを選択します。
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: 証明書を使用し、証明書が失効している場合に Meeting Management が接続を拒否するよう選択した場合、**証明書失効リスト（**CRL**）と証明書を確認します。**

   チェーンの証明書が失効しているか、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お勧めします。

   メモ: HTTP 証明書配布ポイント (CDP) を持つ証明書のみがサポートされています。 CRL チェックを使用していて、証明書に CDP が含まれていない場合、または HTTP 経由で CDP に到達できない場合、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にネットワークを設定する必要があります。

   ---

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

   証明書の要件:

   - *証明書は、TMS 証明書に署名した CA の証明書および、ルート CA 証明書まで、証明書チェーンの上位証明書を含むチェーンである必要があります。*
   - *TMS サーバー用に入力したサーバーアドレスは、TMS サーバー証明書に含まれている必要があります。*

メモ: [SAN] フィールドが使用されている場合、Meeting Management は共通名を参照しません。TMS FQDN が [SAN] フィールドに含まれている必要があります。

7. TMS の [**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。

メモ: TMS でクラスタを 関連付ける前に TMS から情報を受け取ることはありません。

12. NTP サーバの追加

ミーティング管理がミーティング サーバの Call Bridge と常に同期されていることが重要です。そのため、ミーティング管理はミーティング サーバの展開と同じ NTP サーバを使用することをお勧めします。 最大 5 つの NTP サーバーを Meeting Management に接続できます。サーバーの状況は、[**設定**（Settings）] ページ、[NTP] タブの順に選択すると確認できます。

メモ: 表示されている時間は、Meeting Management サーバーのものであり、コンピュータで設定されている時間とは異なる可能性があります。表示されているオフセットは、接続された各 NTP サーバーと Meeting Management サーバーの間の時間です。

NTP サーバを追加するには:

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

   メモ: IPv6 アドレスを入力する場合、ここで角括弧を使用しないでください。

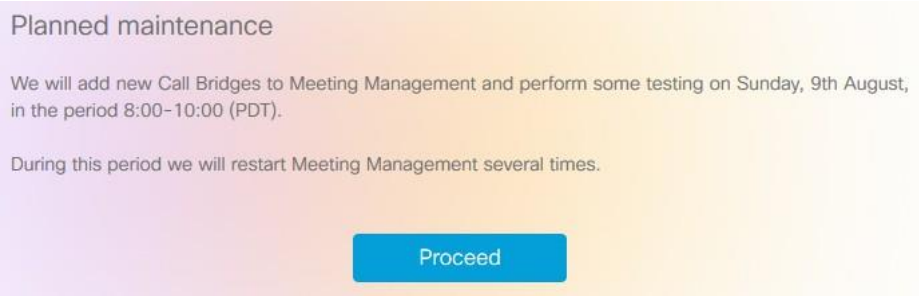
3. 変更を保存するには、Meeting Management を再起動します。

   メモ: 今すぐ再起動するか、構成が完了するまで待ってください。

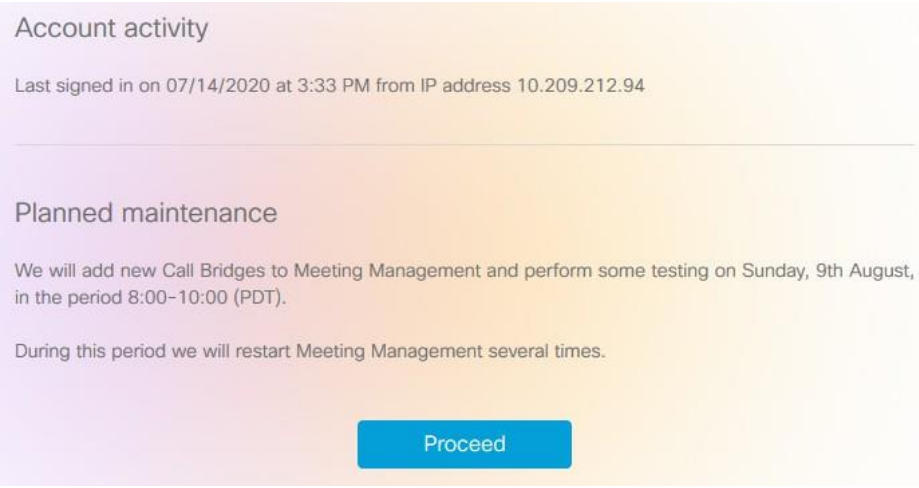
13. オプション: ユーザーのサインイン時に表示するメッセージを追加する

サインインページの前または後に、ユーザーへのメッセージページを挿入することができます。 例えば、サインイン前のメッセージに法的警告を示したり、サインイン後のメッセージを使用してメンテナンス予定を通知したりすることができます。

以下の例で示す通り、ページには、入力したメッセージと、[**続行**（Proceed）] ボタンが表示されます。



もし[**サインイン後にアカウントアクティビティを表示**（Display account activity after sign-in）] チェックボックスにチェックを入れている場合、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。



メモ: 変更はすぐに有効になります。

14. オプション: 高度なセキュリティ設定を構成する

設定ページの **高度なセキュリティ** タブで高度なセキュリティ設定を行うことができます。 デフォルト設定では、Meeting Management が機能的で安全に保たれるように設定されているため、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 ポリシーにより特定の設定が要求されている場合にのみ、高度なセキュリティ設定を変更することをお勧めします。

メモ: すべてのセキュリティ設定は、適用する前に再起動する必要があります。 初回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する場合は、再起動する前に、[**設定**（Settings）]、[**ログ**（Logs）] ページの順に選択し、すべての設定の設定を終了します。

14.1 サインイン試行のレート制限

指定された期間内にユーザーがサインインを試行できる回数を制限することができます。 レート制限を有効にすると、ここで行った設定は 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。

許可されたサインイン試行の回数はトークンで測定されます。 各ユーザーは、定義したトークンの最大数で開始します。 サインインの試行が 1 度失敗すると、1 つのトークンが失われ、利用可能なトークン最大数に再度達するまで、各間隔の終了時にトークンが 1 つ取得されます。

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レート（秒）*

  各間隔の長さを秒で示します。 デフォルトは 300 秒です。
- *バケツに保持されるトークンの最大数*

  これは、指定された時間内にユーザに許可されるサインインの最大試行回数です。 デフォルトは 3 トークンです。

これは、ユーザーが最初の間隔ですべてのトークンを消費した場合、2 番目の間隔でサインインの試行が 1 回だけとなることを意味します。 トークンを使い切った後にユーザーがサインインしようとすると、[**サインインの試行回数が多すぎます**（Too many sign in attempts）] **というメッセージが表示されます。 後ほど再度お試しください**。 これは、資格情報が正しい場合でも発生します。

14.2 アイドル セッションのタイムアウト

一定期間非アクティブなユーザをサインアウトするようにミーティング管理を設定できます。 Meeting Management は、マウスを移動したり、ボタンをクリックしたり、入力フィールドにテキストを入力したりするときに、ユーザをアクティブと定義します。

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

メモ: ミーティング管理は、30 秒ごとにステータスを確認します。つまり、設定された制限時間に最大で 30 秒を加えた値がタイムアウトになります。

メモ: アイドル セッションのタイムアウトを有効にした場合でも、ユーザはアクティブかどうかに関係なく、ログインしてから 24 時間後にサインアウトされます。

14.3 Meeting Server のパスワードをリセット

以前のパスワードを検証することなく、Meeting Server のパスワードをリセットすることができます。 ユーザがパスワードを忘れた場合、以前のパスワードを検証することなく、パスワードをリセットするオプションがあります。 このオプションが有効な場合、[Call Bridgeを編集（Edit Call Bridge）] ページの [**パスワードをリセット（**Reset password**）**] ボタンを使用してパスワードをリセットする際に、以前のパスワードの入力を求めるプロンプトは表示されません（「設定したサーバーを追加」項を参照）。

次の設定が表示されます。

以前のパスワードを検証せずにパスワードをリセットする - このチェックボックスにチェックを入れると、以前のパスワードを検証せずにパスワードがリセットされます。 このオプションはデフォルトで選択解除されています。

14.4 TLS 設定

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

ここでの設定はすべての TLS 接続に対して有効になり、Meeting Management が以下に接続する方法に影響します。

- ブラウザ
- LDAP サーバー

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

接続されているすべてのブラウザとサーバーは、一連の暗号スイートをサポートしています。接続されているユニットが Meeting Management で有効になっている複数の暗号スイートを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ものを使用します。

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が対応しているすべての暗号スイートを無効にすると、ミーティング管理に接続できなくなります。

優先ブラウザと 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ことを特に慎重に確認してください。 ブラウザがミーティング管理に接続できない、またはミーティング管理が LDAP サーバに接続できない場合は、ミーティング管理からロックアウトされる可能性があります。

---

15. ログサーバの追加

システムログ用に少なくとも 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するために必要です。

メモ: 最新のシステムログはローカルに保存されますが、システムログの制限は 500MB です。この制限に達すると、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:

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

   既定のポートは以下のとおりです。

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

   メモ: IPv6 アドレスを入力する場合、ここで角括弧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: 証明書を使用し、証明書が失効している場合に Meeting Management が接続を拒否するよう選択した場合、**証明書失効リスト（CRL）と証明書を確認します。**

   チェーンの証明書が失効しているか、アクセスできない CRL がある場合、ミーティング管理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お勧めします。

   メモ: HTTP 証明書配布ポイント (CDP) を持つ証明書のみがサポートされています。 CRL チェックを使用していて、証明書に CDP が含まれていない場合、または HTTP 経由で CDP に到達できない場合、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にネットワークを設定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が含まれている必要があります。*
   - *証明書に記載されているアドレスは、ログサーバ用に入力したものと同じでなければなりません。*

7. [**追加（Add）**] をクリックします。
8. 必要なログサーバを追加するまで繰り返します。
9. Meeting Management を再起動します。

メモ: 今すぐ再起動するか、構成が完了するまで待ってください。

オプション: 組織で必要な場合、監査ログ用の syslog サーバーを追加します。 監査ログサーバを追加するには:

1. [**ログ（Logs）**] ページで、[**監査ログサーバー（Audit log servers）**] を選択します。
2. [**ログサーバーの追加（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。 既定のポートは以下のとおりです。

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

メモ: IPv6 アドレスを入力する場合、ここで角括弧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: 証明書を使用し、証明書が失効している場合に Meeting Management が接続を拒否するよう選択した場合、**証明書失効リスト（CRL）と証明書を確認します。**

   チェーンの証明書が失効しているか、アクセスできない CRL がある場合、ミーティング管理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お勧めします。

メモ: HTTP 証明書配布ポイント (CDP) を持つ証明書のみがサポートされています。 CRL チェックを使用していて、証明書に CDP が含まれていない場合、または HTTP 経由で CDP に到達できない場合、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にネットワークを設定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が含まれている必要があります。*
   - *証明書に記載されているアドレスは、ログサーバ用に入力したものと同じでなければなりません。*

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

メモ: 今すぐ再起動するか、構成が完了するまで待ってください。

---

16. サーバの追加

[**サーバー（**Servers）] **ページ**では、接続されているすべての Meeting Server Call Bridge および Edge ノードを表示、編集できます。 新しい Call Bridge を追加することもできます。

Meeting Server の導入が正常に完了すると、[**設定済みサーバー（**Configured Servers）] タブで正常に設定されたすべての Meeting Server を表示できます。 失敗または保留中の導入状況の Meeting Server は、[**一部設定済みサーバー（**Partial Configured Servers）] タブに表示されます。

ミーティング管理を無効にするかどうかなど、クラスタの詳細を編集または削除できます。 各クラスタについて、ユーザーのプロビジョニングをセットアップし、スペーステンプレートを作成できます。クラスタを TMS に関連付けて、Meeting Management で今後のミーティングを確認できます。 自分や他のユーザーがすでにプロビジョニングをセットアップする Meeting Management を使用しているが、変更を確定しなかった場合は、クラスタで、リンクが記載されている通知バナーが表示されます。クラスタで、このリンクをクリックし、[**プロビジョニング（**Provisioning）] ページ、[**確認して確定（**Review and commit）] タブの順に移動します。

ミーティング管理は Call Bridge API 経由でミーティング サーバに接続します。 ミーティング管理の各 Call Bridge で API ユーザ アカウントをセットアップしていない場合は、続行する前にセットアップしてください。 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*。 プログラミングガイド ページ (cisco.com) からアクセスできます。

また、CDR 受信者アドレスが、正確に設定されていないと、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。これは、Meeting Management 機能を有効にする場合に、必要です。

Call Bridge または Edge ノードを追加する:

1. [**サーバー（**Servers）] ページで、[**サーバーを追加（**Add Server）] をクリックします。
2. 次のいずれかを実行します。
    a. 設定したサーバーを追加する:
    b. 新しいサーバーを設定する:
3. [OK] をクリックします。

16.1 設定したサーバーの追加

ライセンスおよびその他のサービスを管理するよう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。

[**サーバーを追加**（Add Server）] を選択し、既存の Meeting Server Call Bridge または Edge ノードサーバーを追加する場合は、この項の手順を実行します。 Cisco Meeting Server 接続設定の情報を入力します。

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

   これはウェブ管理インターフェイスのアドレスと同じものです。

   メモ: IPv6 アドレスを入力する場合は、角括弧を使用します。

2. [**ポート**] フィールドに Call Bridge またはエッジ ノード サーバのポート番号を入力します。

   メモ: このフィールドを空欄にしておくと、ミーティング管理はポート 443 を使用します。

3. MMP 管理者の**ユーザー名**および**パスワード**を入力して、Call Bridge または Edge ノードサーバーを追加します。

   メモ: セキュリティおよび監査上の理由から、Meeting Management には専用の管理者アカウントを使用することを強くお勧めします。

4. **表示名**を入力します。

   任意の表示名を選択できます。 他の管理者およびビデオオペレータにとって意味のあるものでなければならないことに注意してください。

5. オプション: 証明書を使用する場合は、[**信用できる証明書チェーンを使用する**（Use a trusted certificate chain to verify）] をオンにします。

6. オプション: 証明書を使用し、証明書が失効している場合に Meeting Management が接続を拒否するよう選択した場合、**証明書失効リスト**（CRL）**に対する証明書**を確認します。

   チェーンの証明書が失効しているか、アクセスできない CRL がある場合、ミーティング管理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お勧めします。

メモ: HTTP 証明書配布ポイント (CDP) を持つ証明書のみがサポートされています。 CRL チェックを使用していて、証明書に CDP が含まれていない場合、または HTTP 経由で CDP に到達できない場合、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にセットアップする必要があります。

7. オプション: 証明書によるセキュリティの使用を選択した場合は、**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 Admin インターフェイスの証明書に署名した CA の証明書および、ルート CA 証明書まで、証明書チェーンの上位証明書を含める必要があります。*
   - *Call Bridge または Edge ノード用に入力したサーバーアドレスが、ウェブ管理インターフェイスの証明書に含まれている必要があります。*

     メモ: SAN (サブジェクト代替名) フィールドが使用されている場合、Meeting Management は共通名を参照しないため、サーバーアドレスが 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: ライセンス管理とプロビジョニングに対して Meeting Management を使用する場合は、[**このクラスタでミーティングを管理するために** Meeting Management**を使用 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. メモ: これは後ほどクラスタ設定を編集することで変更できます。『*管理者用ユーザーガイド*』を参照してください。

   メモ: [ミーティング（Meetings）] ページには、Meeting Management が 1 つ以上のクラスタに対して無効になっていることをビデオオペレータに知らせる情報はありません。

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**、すべてのユーザーにとって分かりやすい表示名を付けます。

追加した Call Bridge または Edge 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 Edge ノードは自動検出され、下に表示されるため、簡単に追加できます。

自動検出された Call Bridge および Edge ノードを追加するには:

1. [**表示**（Show）] をクリックします。
2. [**アクション**（Actions）] 列で、 をクリックします。
3. Call Bridge または Edge ノードの詳細を入力し、必要に応じて証明書をアップロードします。
4. クラスター内のすべての Call Bridge または Edge ノードを追加するまで続行します。

Call Bridge または Edge ノードを編集する:

1. 編集する Call Bridge または Edge ノードまで下にスクロールして、 をクリックするか、列の任意の場所をクリックします。
2. 他の詳細を編集します。
3. [**パスワードをリセット**（Reset password）] ボタンをクリックすると、[**パスワードのリセット**（Reset Password）] ポップアップウィンドウが開きます。 以下のフィールドが表示されます。
   a. **ユーザ名** – MMP 管理者のユーザ名を表示します。
   b. **現在のパスワード** – 現在設定されているパスワードを入力します。 [高度なセキュリティ（Advance security）] タブの [CMS**パスワード**（CMS password）] リセットオプションがオンの場合、このフィールドは表示されません。
   c. **新しいパスワード** – ミーティングサーバの新しいパスワードを入力します。 Meeting Management は、Meeting Server で定義された基準に対して新しいパスワードを検証し、無効な入力がある場合はエラーメッセージを表示します。
   d. **新しいパスワードの再確認** – 新しいパスワードを再入力します。
4. [**完了**（Done）] をクリックします。

メモ: システムは、[パスワードをリセット（Reset Password）] ポップアップウィンドウに入力されたすべてのフィールドを確認します。 管理者は 3 回まで有効な入力を行ってパスワードをリセットできます。失敗した場合、管理者は 2 時間後に再試行できます。

既存のクラスタに対して Meeting Management 機能を無効または有効にする:

1. [**クラスタを編集**（Edit cluster）] をクリックします
2. [**このクラスタでミーティングを管理するために**Meeting Management**を使用する**（Use Meeting Management to manage meetings on this cluster）] をオンまたはオフにします
3. [**完了**] **をクリックします。**

16.2 新しいサーバーを設定する

[**サーバーを追加**（Add Server）]、[**新しい** Meeting Server（Call Bridge）**を設定して追加する**（Configure and add a new Meeting Server (Call Bridge)）] の順に選択すると、Meeting Management コンソールで [インストールアシスタント（Installation Assistant）] が開きます。

16.2.1 ステージング

新しい Meeting Server を設定するには、これらの要素が対処されていること確認します。

- ミーティングサーバは空です
- ミーティングサーバの DNS エントリを設定する

新しいミーティングサーバインスタンス

Meeting Server には、仮想マシンが導入されており、有効な管理者アカウントが実行されており、その 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。 他の設定は行わないでください。 『Cisco Meeting Server 1000 および仮想展開向けのインストールガイド』では、ミーティングサーバインスタンスの展開方法および Cisco Meeting Server 1000 アプライアンスの設定方法が説明されています。 サーバの設定については、 IPv4 **用ネットワークインターフェースのセットアップ** の章を参照してください。 'a' インターフェイスを設定する手順以降に進まないでください。

既存のミーティングサーバインスタンス

ミーティングサーバインスタンスが以前に構成されたか、Installation Assistant ツールで使用されたが構成が正常に完了していない場合、Installation Assistant で使用する前に、インスタンスをリセットして新しいサーバと同じ構成状態に設定する必要があります。 以前の設定の上で、[インストールアシスタント（Installation Assistant）] を使用することはできません。 サーバをリセットするには:

1. 管理者アカウントを使用して Meeting Server の MMP インターフェイスにログインし、プロンプトが表示されたら factory_reset full コマンドを発行して、確認します。 サーバは自分自身をデフォルト設定にリセットし、再起動します。
2. ユーザー名**管理者**パスワード**管理**で、Meeting Server の MMP インターフェイスにログインします。
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 および仮想化導入向け設置ガイド』を参照してください。

メモ: 上記のガイドの構成手順に従うとき、「a」インターフェイスの構成以外の作業は行わないでください。

16.2.2 新規ミーティングサーバの追加

サーバ設定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 サーバのアドレス
- ミーティングサーバで使用する SIP プロキシのアドレス
- ミーティングサーバで使用する選択済みの SIP ドメイン
- ユーザ インポートを設定する場合、ロケーション、資格情報、LDAP ユーザ ロケーションの詳細など、ネットワークの LDAP ディレクトリへの接続の詳細が必要です。
- 証明書付きサーバーを設定する場合（推奨）、Meeting Server に対して FQDN を指定し、DNS サーバーレコードで定義しておく必要があります。
- 証明書でサーバを構成する場合 (推奨)、選択した認証局によって署名された証明書要求が必要になります。 インストールアシスタントが証明書要求の生成を支援します。または、既存の証明書とキーペアを使用することもできます。

新しいミーティングサーバを設定するための主な手順は以下の通りです:

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 で設定されている**ユーザー名**を入力します。

   メモ: デフォルトでは、ユーザー名には 'admin' が使用されます。

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

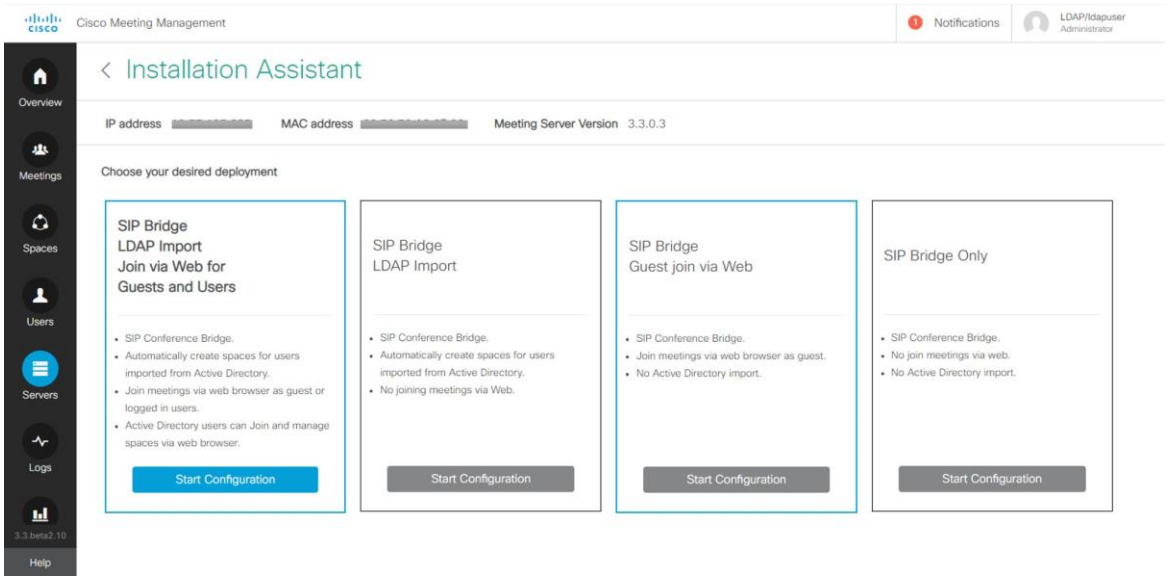
   メモ: [**接続**（Connect）] ボタンは、サーバーアドレス、ユーザー名、パスワードの詳細を入力した後でのみ有効になります。

5. 次のオプションから希望する導入を選択し、[**設定を開始**（Start Configuration）] をクリックします。 選択した導入タイプに基づいて、サーバーを設定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され、表示されます。
   a. **ゲストとユーザー向けのウェブ経由の** SIP Bridge LDAP **インポート参加**: ウィザードは設定のすべて手順に移動します。

b. SIP Bridge LDAP **インポート**: ウィザードは、Web Bridge を除く設定のすべてのステップをナビゲートします。

c. **ウェブ経由の** SIP Bridge **ゲスト参加**: このウィザードは、電話会議ユーザーを除く、設定のすべて手順に移動します。

d. SIP Bridge **のみ**: このウィザードは、Web Bridge および電話会議ユーザーを除く、設定のすべて手順に移動します。



6. ウィザードの指示に従って必須情報を入力します。 すべてのフィールドの検証が完了すると、[**次へ**] ボタンが有効になります。
7. 選択した導入タイプに応じて、ウィザードは次のすべてまたは一部のページを移動できます:
   - 証明書
   - ネットワーク
   - Call Bridge
   - Web Bridge
   - 電話会議ユーザー
   - セキュリティ
   - プッシュ構成
8. 設定を確認し、準備ができたら、[**設定をプッシュ**（Push Configuration）] をクリックして、Meeting Server に設定をプッシュします。

メモ: サーバーに設定をプッシュする際に問題が発生したら、[**ログ**（Logs）] タブに移動して、[**ログバンドルをダウンロード**（Download Log Bundle）] を使用して Meeting Management をダウンロードすると、問題を診断できます。

---

17. 証明書

[証明書] パネルでは、ミーティングサーバーに必要な X.509 証明書を指定する方法を選択することができます。また、新しい証明書の作成をお探しの方には、新しい証明書を作成するためのガイド付きプロセスが提供されます。 インストレーションアシスタントは、認証局によって署名された証明書と自己署名証明書の両方をサポートしています。 証明書パネルは、CA 署名付き証明書または自己署名証明書のどちらを使用するかの選択に基づいて、表示されるオプションを自動的に調整します。

メモ: 自己署名証明書はすべての機能でサポートされているわけではありません。セキュリティ上のリスクがあるため、お勧めできません。

推奨されるパスは、組織が信頼する認証局によって署名された X.509 証明書を使用することです。 認証局には、内部または公開認証局を指定できます。 ミーティングサーバーでの証明書の使用方法とその要件についての詳細は、『Cisco Meeting Server、単一統合サーバー導入ガイド』を参照してください。

17.1 CA 署名付き証明書

CA 署名付き証明書の方法が選択されている場合、2 つの利用可能なパスがあります。

- CSR **経由の新しい証明書** – [インストールアシスタント（Installation Assistant）] が、Certificate Authority への証明書署名リクエストの作成をガイドします。これは署名済み証明書も返します。
- **既存の証明書とキーを提供** – 既存の証明書と外部で準備したキーペアをインストールアシスタントにアップロードします。

17.1.1 CSR による新しい証明書

このオプションでは、Certificate Authority に提供する証明書署名リクエスト（CSR）を作成することで、新しい証明書を作成することができます。

このプロセスを完了するには、次のものが必要です。

1. インストールアシスタントで証明書の詳細を入力し、CSR ファイルをダウンロードします。
2. 認証局に CSR を提供すると、署名済み証明書が返されます。 また、認証局を表す公開証明書のチェーンも必要になります。認証局はこれを提供します。
3. 生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ます。インストールアシスタントは、提供されたファイルを使ってミーティングサーバの設定を行います。

メモ: CSR をダウンロードした後は、Installation Assistant ツールを自由に閉じることができます。 Certificate Authority からの署名済み証明書を取得したら、[**サーバー（**Servers**）**] **ページの** [**一部設定済み** Meeting Server**（**Partial Configured Meeting Server**）**] タブに移動し、[**再開（**Resume**）**] をクリックして、[**証明書（**Certificate**）**] パネルに戻り、証明書のアップロード処理を完了します（手順 4 を参照）。

新しい証明書リクエスト（CSR）を作成するための手順:

1. [証明書（Certificate）] パネルで、[**証明書の種類（**Certificate Type**）**] に [CA **署名済み（**CA Signed**）**] を選択します。
2. [**証明書をアップロード（**Certificate Upload**）**] オプションで、[CSR **経由の新しい証明書（**New Certificate via CSR**）**] を選択します。
3. Meeting Server で使用する詳細をフィールドに入力します。 フィールドについて以下に説明します。 完了したら、[**次へ（**Next**）**] ボタンをクリックし、[証明書（Certificate）] パネルに戻ります。 [**次へ**] ボタンは、必要な情報をすべて入力した場合にのみ有効になります。

メモ: 既存の生成された証明書がある場合、[CSR**を再生成（**Regenerate CSR**）**] をクリックすると、新しい詳細で既存ファイルが上書きされます。これは、[インストールアシスタント（Installation Assistant）] で、複数の CSR ファイル生成が許可されていないためです。

表 8: **証明書署名リクエストに必要なフィールド**

フィールド名	**説明**	**値**
ミーティングサーバの FQDN	これは証明書の CN 値であり、DNS サーバで定義されている必要があります。	サーバの FQDN を入力します。
ミーティングサーバの 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 ルールに合わせてサーバの SIP ドメインを入力します。

4. 完了した CSR は [証明書] パネルに表示されます。 [CSR **のダウンロード**] をクリックして、生成された CSR をローカルドライブ上のファイルに保存します。
5. CSR を認証局に渡して署名をもらいます。 署名された証明書ファイルが返されます。 その認証局の証明書チェーン バンドルも必要になります。
6. 署名付き証明書と証明書チェーンファイルを入手したら、必要に応じて [証明書（Certificate）] パネルに戻り、[**ファイルをアップロード（**Upload Files**）**] を選択して証明書/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 2 つのフィールドが表示されます。 [**ファイルを選択（**Select File**）**] リンクを使用して、ローカルコンピュータにある特定のファイルを指定します。 証明書ファイルには次の拡張子 (CER、CRT、PEM、DER) のいずれかが付いている必要があり、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て、[**次へ（**Next**）**] ボタンをクリックすると、ファイルが、[インストールアシスタント（Installation Assistant）] に送信され、確認されます。
8. 正常に終了すると、ウィザード内で [証明書（Certificate）] パネルに完了のマークが付き、[ネットワーク（Network）] パネルに移動することができます。

エラーシナリオ

以下の場合、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/技術的な問題によりアップロードが失敗した場合。 解決方法: 証明書ファイルを再度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。
  解決方法: 正しい証明書および 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。
  解決方法: 正しい FQDN/SIP ドメインまたは正しいキーを使用して、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。
  解決方法: 正しい FQDN/SIP ドメインまたは正しいキーを使用して、証明書チェーンを再アップロードします。

17.1.2 既存の証明書とキーを使用

ツールで CSR を生成する代わりに、ミーティングサーバ用に既存の秘密鍵と署名証明書を使用するオプションがインストールアシスタントに提供されます。 これは、[**既存の証明書とキーを指定（**Supply an existing certificate and key**）**] オプションを使用して実行します。

証明書、秘密鍵、および CA 証明書チェーンを提供する必要があります。 証明書ファイルには次の拡張子 (CER、CRT、PEM、DER) のいずれかが付いている必要があり、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:

1. [証明書（Certificate）] パネルで、[**証明書の種類（**Certificate Type**）**] に [CA **署名済み（**CA Signed**）**] を選択します。
2. *[証明書をアップロード（Certificate Upload）] オプションで、[既存の証明書とキーを指定（Supply an existing certificate and key）] を選択します。*
3. [Meeting Server **の** FQDN（FQDN for Meeting Server）]、[Meeting Server **の** SIP **ドメイン（**SIP domain for Meeting Server**）**]、[**プライベートキー（**Private key**）**]、[CA**証明書チェーン（**CA certificate chain**）**] および [**証明書（**Certificate**）**] を指定するために 5 つのフィールドが表示されます。 [**ファイルを選択（**Select File**）**] リンクを使用して、ローカルコンピュータにある特定のファイルを指定します。 証明書ファイルには次の拡張子 (CER、CRT、PEM、DER) のいずれかが付いている必要があり、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 つのファイルすべてを指定すると、[**次へ**] 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。

正常に終了すると、ウィザード内で [証明書] パネルに完了のマークが付き、[ネットワーク] パネルに移動することができます。

エラーシナリオ

以下の場合、エラーメッセージが表示され、[**次へ**] 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の解決方法: 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、[**アップロード（**Upload**）**] ボタンは無効になります。
  解決方法: 正しい証明書および 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。 解決方法: 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。 解決方法: 有効な SIP ドメインを入力する必要があります。

17.2 自己署名証明書

自己署名証明書は、ローカル エンティティによって署名された証明書です。 証明書を検証する管理機関がありません。 自己署名証明書は有効ですが、セキュリティ上の理由からお勧めできません。 ミーティングサーバでの証明書の使用方法とその要件についての詳細は、 Cisco Meeting Server 証明書ガイドラインを参照してください。

メモ: 自己署名証明書の詳細はツールによって保存されないため、一度に設定を完了することが推奨されます。

メモ: Meeting Server の設定に自己署名証明書を使用している場合、Meeting Server の時間が現在時刻になっていることを確認してください。 ミーティングサーバの時間が実際の時間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、時間を正確に設定する必要があります。 デフォルトのシステム時間は UTC です。

自己署名証明書を使用する手順:

1. [証明書（Certificate）] パネルで [**自己署名（Self signed）**] を選択します。
2. ミーティングサーバの FQDN を入力します。
3. ルーティングルールに従うように Meeting Server **の** SIP **ドメイン**を入力します。
4. [**次へ**] ボタンは、必要な情報をすべて入力した場合にのみ有効になります。 [**次へ**] 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. 正常に終了すると、ウィザード内で [証明書（Certificate）] パネルに完了のマークが付き、[ネットワーク（Network）] パネルに移動することができます。

エラーシナリオ

以下の場合、エラーメッセージが表示され、[**次へ**] 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。 解決方法: 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。 解決方法: 有効な SIP ドメインを入力する必要があります。

18. ネットワーク

[ネットワーク] パネルでは、サーバのコア ネットワーク設定を構成することができます。

メモ: これらの設定に関するガイダンスについては、ネットワーク管理者に連絡する必要がある場合があります。

1. 以下を構成します。

フィールド名	説明	アクション
NTP サーバー	FQDN または IP アドレスを指定して、少なくとも 1 つの NTP サーバを構成する必要があります。 メモ: 最大 5 つの NTP サーバを設定できます。	[**サーバーの追加**（Add server）] をクリックします。 Cisco Meeting Server に NTP サーバーのアドレスが追加されます
タイムゾーン	サーバのローカルタイムゾーン	希望のタイムゾーンを選択します。
DNS サーバー	IP アドレスを指定して、少なくとも 1 つの DNS サーバを設定する必要があります。 メモ: 最大 5 つの DNS サーバを設定できます。	サーバーの IP アドレスを入力し、[**サーバーを追加**（Add server）] をクリックします。 Cisco Meeting Server に DNS サーバーのアドレスが追加されます
ウェブ管理ポート	ミーティングサーバウェブ管理インタフェースが待機する TCP ポート番号を設定します。 ウェブ ブリッジを含む展開を使用している場合は、ポート 443 の使用が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、[ネットワーク] パネルの設定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ます。このボタンをクリックすると、選択した導入に基づき、次のパネルに移動します。

18.1 DNS または NTP サーバの削除

1. をクリックし、DNS/NTP サーバーを削除します。

エラーシナリオ

以下の場合、エラーメッセージが表示され、[**次へ**] 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提供された場合。 解決方法: 有効な IP アドレス /FQDN を提供する必要があります。
- 正しくない DNS サーバーアドレスが提供された場合。 解決方法: 有効な IP アドレスを指定する必要があります。
- ポート番号が間違っている場合。 解決方法: 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 サーバアドレスが提供された場合。 解決方法: 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 サーバアドレスが提供された場合。 解決方法: 別の IP アドレスを指定する必要があります。

19. Call Bridge

[Call Bridge] パネルを使用すると、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 プロキシ	ミーティングサーバからの発信通話を受信する SIP プロキシの完全修飾ドメイン名または IP アドレスを入力します。
暗号化	接続の暗号化モード (TLS) を選択します。
SIP 通話のメディア暗号化	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 権限を有効にします。 このオプションが有効な場合、 callLegProfile と systemProfile が作成され、デフォルトで参加者の ActiveControls が有効になります。 メモ: Meeting Server では、これらの設定はデフォルトでは有効になっていません。

2. 正しい詳細を指定すると、[Call Bridge] パネルの設定が正常に完了します。

   メモ: 設定を正常に保存するために、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ます。このボタンをクリックすると、選択した導入に基づき、次のパネルに移動します。

エラーシナリオ

以下のシナリオの場合、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:

- 入力した SIP プロキシの詳細が間違っている。
  解決方法: 有効な IP アドレス/FQDN を提供する必要があります。

20. Web Bridge

[Web Bridge] パネルでは、Call Bridge が Web Bridge に接続することを許可するポートを開くことで、Cisco Meeting Server ウェブアプリを設定できます。

1. Call Bridge **から** Web Bridge (c2w) **へのリスニングポート**を入力します。 既定では、ポート番号は 9999 です。
2. 正しい詳細を指定すると、[Web Bridge] パネルの設定が正常に完了します。
3. [**次へ（**Next）] ボタンが有効になります。このボタンをクリックすると、選択した導入に基づき、次のパネルに移動します。

エラーシナリオ

以下のシナリオの場合、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:

- 入力した Call Bridge から Web Bridge (c2w) へのポートの詳細が正しくない場合。 解決方法: 有効なポート番号を指定する必要があります。

メモ: 443 または webadmin ポートは使用できません。

---

21. 電話会議ユーザー

[電話会議ユーザー（Conferencing）] パネルでは、Cisco Meeting Web App にログインする LDAP ユーザーをインポートできます。

ユーザアカウントの作成には以下が必要です。

- Active Directory サーバーに接続するための接続プロパティを定義します。 デフォルトでは LDAPS オプションが選択されています。
- 検索フィルタと Meeting Server 上に作成されるユーザーに使用されるフィールドマッピングの値を定義します。 [Installation Assistant] にはほとんどの環境で機能するデフォルト値がありますが、必要に応じてこれらのデフォルトを上書きするオプションがあります。

ユーザアカウントを作成するには:

1. [LDAP **接続設定**] 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への入力が完了すると、[**次へ**] ボタンが表示されます。

   各設定の詳細については、次の表に記載されています。

   表 9: LDAP **接続の設定**

フィールド名	説明	入力
サーバーアドレス	接続先の LDAP サーバーのネットワークアドレスです。	LDAP サーバーの完全修飾ドメイン名または IP アドレス
Port	接続する LDAP サーバーの TCP ポートです。	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。
ユーザ名	LDAP サーバーに接続するユーザーのユーザー名です。 このユーザーには、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ーの LDAP 識別名 (DN) または UPN。 このフィールドを空欄にすることはできません
パスワード	指定されたユーザーのパスワードです。	ユーザーのパスワードです。 このフィールドを空欄にすることはできません。

検索ベース	インポート検索クエリが開始する LDAP ディレクトリ内の場所です。 この値に関するサポートが必要な場合は、ドメイン管理者に連絡してください。	検索を開始するディレクトリの場所の LDAP 識別名 (DN) です。 このフィールドを空欄にすることはできません
PMP ライセンスをユーザーに割り当てる	有効になっている場合、インポートされたユーザーは PMP+ ライセンスの対象としてマークされます。 インポートされるすべてのユーザーに対して 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。	PMP+ 資格を持つインポートされた各ユーザーにタグ付けを有効にします。
既定のユーザフィルターとフィールド マッピングの詳細を上書きする	インストールアシスタントは、ほとんどの環境で機能するデフォルトの 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ます。 このオプションを有効にすると、これらの設定を表示し、環境に合わせてカスタマイズすることができます。	LDAP 検索フィルタまたは LDAP ユーザーフィールドマッピングの表示またはカスタマイズすることを有効にします。

2. [LDAP**接続を確認**（Check LDAP Connection）] ボタンをクリックし、LDAP 接続が利用可能かを確認します。

   メモ: [LDAP**接続を確認**（Check LDAP Connection）] ボタンをクリックすると、接続の確認ができなかった場合に、[LDAP**を接続できませんでした**（LDAP Connection Failed）] というエラーメッセージが表示されます。

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。

メモ: 設定を正常に保存するために、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、マッピングに使用される有効な LDAP 式を使用していることを確認してください。

エラーシナリオ

- [LDAP**接続を確認**（Check LDAP Connection）] ボタンをクリックすると、接続確認が失敗します。解決方法: 有効な LDAP 接続詳細を指定する必要があります。

21.1 LDAP 検索とユーザ マッピングをカスタマイズする

インストールアシスタントは、ほとんどの環境で機能するデフォルトの 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ます。 デフォルトでは、メールアドレスとユーザー名が定義されているユーザーがフィルタ処理され、Meeting Server のユーザー名がミーティングアドレスに設定されます。

上書きオプションを有効にすると、インポートに使用される個別の構成フィールドが表示され、Installation Assistant がデフォルトで使用している設定が表示されます。 [**デフォルトのユーザーフィルタとフィールドマッピング詳細をオーバーライドする**（Override default user filter and field mapping details）] が有効な場合、ユーザーは、これらの値を環境に合わせてカスタマイズできます。

ユーザマッピング式は、ミーティングサーバにユーザをインポートする際の、ユーザのプロパティの設定方法を定義します。 式は静的テキストと共に変数を使用するため、ミーティングサーバでユーザを作成するときに LDAP のユーザのプロパティを使用できます。 LDAP プロパティの使用は、ユーザごとに一意である必要があるプロパティ (ユーザ名や URI など) が重複していないことを確認するために重要です。 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、フィールドマッピング式の $mail$ により参照されます。

表 10: LDAP **インポート設定**

フィールド名	説明	入力
LDAP 検索フィルター	インポートするために照合する LDAP ユーザーの基準を定義します。	LDAP 検索文字列。 LDAP 検索構文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表示される名前。	マッピング式。 例: cn
ユーザ名	ユーザが Cisco ミーティング ウェブアプリにログインするために使用するユーザ名です。 結果として得られる値は、すべてのユーザとスペースで一意である必要があります。	マッピング式。 例： $sAMAccountName$@company.com このフィールドを空欄にすることはできません。結果はインポートされたユーザーごとに固有なものでなければなりません。
スペース名	ユーザ用に自動作成されたスペースに付けるラベルです。 インポートされたユーザ用にスペースを作成しない場合は、空白のままにします。	マッピング式。 例: cn ミーティングスペース

スペース URI	ユーザー用に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り、ユーザ名や他のスペースと競合しないようにする必要があります。 インポートされたユーザーに対してスペースが作成されない場合は、空欄にします。	マッピング式。 例: cn.space
スペースのセカンダリ URI	ユーザ用に自動的に作成されたスペースの 2 番目の URI の左側部分。 結果はユーザごとに一意であり、ユーザ名や他のスペースと競合しないようにする必要があります。 オプションのフィールドです。 インポートされたユーザ用にスペースを作成しない場合は、空白のままにします。	マッピング式。 例: cn.room
スペースコール ID	ユーザに対して自動的に作成されるスペースのコール ID を設定します。 結果はすべてのスペースで一意でなければなりません。 オプションのフィールドです。空の場合、Cisco ミーティングサーバが自動的に ID を割り当てます。 インポートされたユーザ用にスペースを作成しない場合は、空白のままにします。	マッピング式。
認証 ID のマッピング	インポートされたユーザに割り当てられたマッピングプロパティ。 スマートカード ログインのシナリオで使用されます。 特に証明書ベースのログインを展開する場合を除き、空白のままにします。	マッピング式。 例: $userPrincipalName$

[**次へ**（Next）] ボタンが有効になります。 [**次へ**] をクリックすると、ログイン情報が作成、保存されます。展開の選択内容に応じて次のパネルが表示されます。

メモ: 設定を正常に保存するために、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。

エラーシナリオ:

次の場合、エラーメッセージが表示され、[**次へ**] ボタンが無効になります:

- 入力されたサーバアドレスの詳細が正しくない場合。 解決方法: 有効な IP アドレス /FQDN を提供する必要があります。
- 入力されたポート番号が正しくない場合。
  解決方法: 正確な数値のみを入力する必要があります。

22. セキュリティ

既定の管理者アカウントへのアクセス権を失った場合、セキュリティパネルからミーティングサーバに別のユーザを作成することができます。

1. [**バックアップユーザーアカウントを作成**（Create backup user account）] を選択し、リカバリアカウントを作成します。
2. [**新しいユーザー名**（New username）]、[**パスワード**（Password）] および [**パスワードを確認**（Confirm Password）] を入力します。

   メモ: **パスワード** を空欄にすることはできません。また、 **ユーザ名** 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）] をクリックし、ログイン資格情報を作成し、保存したら、選択した導入に基づいて、次のパネルに移動します。

エラーシナリオ:

以下の場合、エラーメッセージが表示され、[**次へ**] ボタンが無効になります:

- 入力されたユーザ名が間違っている場合。 解決方法: 有効なユーザ名を入力する必要があります。
  メモ:「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用パスワードが一致しない場合。 解決方法: 両方のフィールドに同じパスワードを再入力します。
  メモ: 入力できる値は英数字のみです。

23. プッシュ構成

[プッシュ構成] パネルでは、Installation Assistant で提供した各パネルのすべての詳細を確認することができます。

1. [**次へ**] ボタンをクリックしてミーティングサーバに設定の詳細を送信し、設定を完了します。

2. 構成が Meeting Server に正常にプッシュされると、インストールアシスタントが要約の詳細を表示します。 追加されたミーティングサーバは、 **設定済みサーバ** タブに表示されます。 追加されたミーティングサーバを編集または削除するには、各アイコンをクリックします。

   メモ: 追加されたミーティングサーバは期限切れライセンス状態になります。 ミーティングサーバをミーティング管理サーバに追加してください。

   ---

3. 新しく作成された Meeting Server クラスタを使用してミーティングを管理するには、[**このクラスタで**Meeting Management**を使用して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にします。
4. 表示名 **を入力します。**
5. [**終了**] ボタンが有効になります。 [**終了**] をクリックして [**サーバ**] ページに移動してください。
6. 構成が失敗した、または不完全だった場合、以下が考えられる次のステップです。
   a. ログ: [**ログ（**Logs）] タブに移動し、[**ログバンドルをダウンロード（**Download log bundle）] ボタンを使用すると、Meeting Management ログをダウンロードできます。これには、[インストールアシスタント（Installation Assistant）] ログも含まれます。
   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りプッシュされた Meeting Server 設定を削除することができます。
   c. 再開: [**一部設定済みサーバー（**Partial Configured Server）] タブで、Meeting Server の設定を再開できます。

失敗した設定は、[インストールアシスタント（Installation Assistant）] を終了したら、[**一部設定済みサーバー（**Partial Configured Server）] タブで一覧されます。

23.1 SSH 機能

[ミーティング管理] に追加された Edge 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 Edge ノードに対して、MMP コマンドを実行できます。Call Bridge または Edge ノードを選択し、MMP 管理者資格情報を提供することで SSH ターミナルに接続できます。接続したら、選択したサーバ上で MMP コマンドを実行できます。

24. ライセンスモードを選択する

[設定] ページの [ライセンス] 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、ここでスマート ライセンス設定の一部を構成することもできます。

ライセンスモードを選択してください。 次のいずれかを選択します。

- **スマート ライセンス** (推奨)

  Cisco Smart Software Manager に登録し、ライセンスの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、ミーティング管理は Cisco SSM から購入したライセンスに関する情報を取得します。

  メモ: ミーティング管理スマート ライセンスのインテグレーションには CLI (コマンドライン インターフェイス) はありません。 これは設計によるものです。ミーティング管理は、GUI を提供するためです。

- **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 Cisco Smart Software Manager に従来のライセンスキーがない Call Bridge の数をレポートします。 これらはスマートアカウントに**アクティブ** Call Bridge **ノード**（Active Call Bridge Node）という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与えられます。
- *ライセンスなし*

  このオプションは回復力のある導入のみで利用できます。 回復力のある導入を実行し、Meeting Management のもう一方のインスタンスで Smart Licensing が有効な場合にこのオプションを選択します。

注：

- **従来のライセンス** オプションは、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に対してはグレー表示されます。
- Meeting Management では、ローカルライセンスファイルのサポートは廃止されました（従来のライセンスモード）。 Smart Licensing に移行すると、[従来のライセンス（Traditional Licensing）] オプションは、[**ライセンスモード**（Licensing Mode）] ポップアップで利用できなくなります。
- ライセンスモードを変更するか、新しいクラスタを追加した後、接続されているミーティングサーバのライセンスステータスに変更が反映されるまで最大 5 分かかる場合があります。

24.1 スマート ライセンスを有効にする方法

スマートライセンシングの有効化

1. Cisco SSM にログインし、登録トークンを生成します。

   メモ: 登録トークンの生成時に、 [**このトークンで登録された製品に輸出規制対象の機能を許可する**] オプションを選択して、より高度な製品暗号化機能を有効にしてください。詳細については、『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ミーティング管理のインスタンスを開きます。
4. **設定** ページの [**ライセンス**] タブに移動します。
5. [**変更**] をクリックします。
6. [Smart Licensing] を選択し、 [**保存**] を選択します。
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を登録します

   通常、Cisco SSM はすでに登録されているミーティング管理のインスタンスを登録させることはできません。 このチェックボックスをオンにすると、Cisco SSM は同じインスタンスを再度登録させます。 これは、ミーティング管理が登録の詳細を失った場合に役立ちます。例えば、登録解除しようとしたが、登録解除中に Meeting Management が Cisco Smart Software Manager に到達できなかった場合などです。

10. [**登録（**Register）] をクリックします。
11. 登録が済んだら、バーチャルアカウントにあるライセンス数を確認してください。
12. ミーティング管理で、 **ライセンス** ページに移動します。
13. バーチャルアカウントに所有するライセンスの情報を入力します。

    注：

    - Meeting Management をテストするが、まだライセンスを持っていない場合は、代わりに [**トライアルを開始（**Start trial）] をクリックしてください。
    - 特定のタイプのライセンスをお持ちでない場合は、フィールドを空欄にするのではなく、0 を入力してください。

メモ: ライセンスモードを更新するか、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のすべての使用情報を取得するまで、しばらく時間がかかる場合があります。 接続の速度とデータ量に応じて、これには数分から 15 分以上かかります。

メモ: 割り当てられたライセンス数を変更するたびに、接続されている Meeting Server のライセンス状況に変更が反映されるまでに最大 5 分かかる場合があります。

メモ: ライセンスの予約時に、Cisco SSM の応答に予想される 30 秒よりも長い時間がかかる場合、さまざまなタイムアウト値を指定して、さらに 2 回の再試行が行われます。 Meeting Management は 2 回目と 3 回目の再試行で、それぞれ 60 秒と 90 秒待機します。 3 回再試行してもライセンス予約に失敗すると、[**概要**（Overview）] ページに、[Cisco Smart Software Server**に到達できません**（Unable to reach Cisco Smart Software Server）] と表示されます。 ライセンスの予約を再度開始する必要があり、ライセンスが正常に予約されたことを示すメッセージが消去されます。

24.2 スマートライセンスが有効になっ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。

- **今すぐ認証を更新**: システムは、認証を日単位で午前 0 時 (UTC) に自動更新します。 手動で更新する場合は、ここで実行できます。 これは、新しいライセンスを購入した、またはこのミーティング管理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た場合に、ミーティング管理で変更をすぐに確認したい場合に便利です。
- **今すぐ登録を更新**: システムは 6 ヶ月ごとに登録を自動更新します。 この Meeting Management のバーチャルアカウント間でライセンスを移動する場合、または Meeting Management のこ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、手動で登録を更新することを検討します。
- **再登録**: 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、手動で再登録できます。

- **ライセンスの予約**: 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ベートし、管理することができます。 Cisco Smart Software Manager でトークンを生成することで製品インスタンスをアクティベートし、製品インスタンスに必要なライセンスを予約します。 スマートアカウントにより、選択した製品インスタンスがコンプライアンスを満たし、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が付与されます。 詳細については、こちらの項を参照してください。
- **登録解除**: 別の展開でバーチャルアカウントを使用する場合、または復元力のあるミーティング管理展開があり、レポートに他のインスタンスを使用する場合、このミーティング管理のインスタンスを登録解除できます。

メモ: ライセンスモードを変更すると、ミーティング管理は自動的にスマートライセンスを無効にし、Cisco Smart Software Manager から登録解除します。

メモ: Meeting Management のインスタンスへの接続が切断された場合は、Cisco SSM からも登録を解除できます。

24.3 ライセンス予約

Cisco 製品ユーザが SMART に準拠するためには、License Reservation のサポートが必要です。 ミーティング管理は、バージョン 3.4 以降のライセンスの予約をサポートしています。 セキュリティ上の理由により Meeting Management がインターネットに接続できない環境では、[ライセンスの予約] を使用して機能をアクティベートし、ライセンスを予約することができます。

この機能には、Universal (Permanent License Reservation) と Specific (Specific License Reservation) の 2 つのバリエーションがあります。

- **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の使用を有効にする単一のライセンスを提供します。 PLR は、軍事/防衛の顧客のみが利用できます。
- **特定のバージョン** : 特定のライセンス予約（SLR）は、要件に基づいてライセンスを予約するための選択肢を提供します。 機能ライセンスに加えて、SMP Plus および 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の予約を更新または変更できます。

ライセンスの予約は、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することができます。 これには、予約の取り消しと製品インスタンスの再登録が含まれます。

メモ: 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、顧客が特別に要求し、Cisco によって承認される必要があります。 どちらのタイプのライセンス予約でも、Cisco はスマートアカウントを承認する必要があります。 会社のスマートアカウントと、1 つの Meeting Management のインスタンスでのみ使用される専用のバーチャルアカウントが必要です。 アカウントを要求する場合は、Cisco アカウントチームに連絡するか、Cisco Software Central にアクセスします。

ライセンスの予約により、以下のワークフローが可能になります。

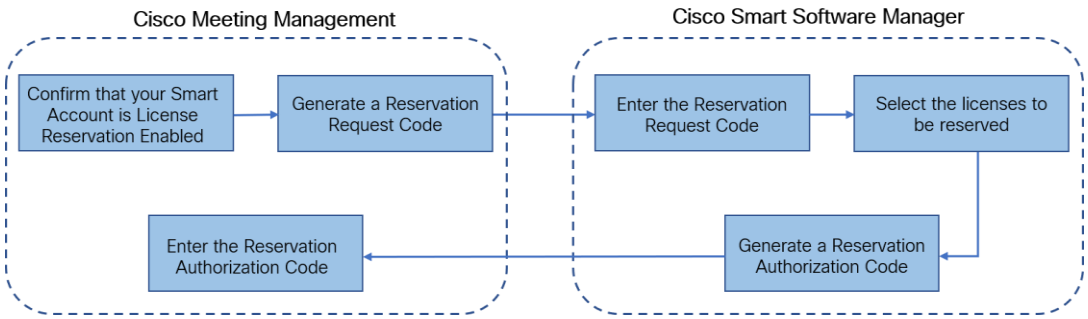
- SLR/PLR ライセンスの予約
- 予約済みライセンスを更新する
- 予約済みライセンスを返却する

24.3.1 ライセンス予約

初回ライセンス予約のワークフローは以下の通りです。

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 から予約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 で承認コードを入力します

図 1: ライセンス予約のワークフロー



ライセンスの予約は次の手順で行います:

1. Meeting Management で、[**設定**（Settings）]、[**ライセンス**（Licensing）] セクションの順に選択します。

a. [**登録**（Register）] ボタンをクリックして、[Smart Software Licensing Registration（Smart Software Licensing **登録**）] を開きます。

b. ポップアップ下部の [**ここから開始**（Start Here）] リンクをクリックし、ライセンス予約プロセスを開始します。

c. 表示されるポップアップウィンドウで、[**はい、My スマートアカウントでライセンス予約を有効にする**（Yes, My Smart Account is License Reservation Enabled）] をクリックします。

d. [**スマートライセンス予約**（Smart License Reservation）] ポップアップで、[**生成**（Generate）] ボタンをクリックして、予約リクエストコードを生成します。

e. 生成された Reservation Request Code を保存またはコピーします。

f. [**閉じる**] **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、[**スマートソフトウェアライセンシング**（Smart Software Licensing）] 状況が、[**ライセンス予約保留**（License Reservation Pending）] として表示されます。

2. Smart Software Manager

a. スマート アカウントを使用して Cisco Smart Software Licensing Manager にログインします

b. 希望のバーチャルアカウントに移動して、 [**ライセンスの予約**] **をクリックします。**

メモ: ライセンスの予約を使用するには、Cisco からの特定の許可が必要です。 これを実行するには、[Smart Software Manager] の [**在庫**（Inventory）] セクションにある [**ライセンス**（Licenses）] タブで、[**ライセンス予約**（License Reservation）] ボタンが利用可能になっていることを確認する必要があります。

---

c. 予約リクエストコードを入力します。

d. [**予約するライセンス**（Licenses to Reserve）] **で**、ライセンスを選択します。

- PLR の場合 - オプションの Meeting Server **の** PLR **有効化を選択します**
- SLR の場合 - オプションの選択**特定のライセンスを予約**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**] ボタンをクリックして、予約認証コードを生成します。

f. Reservation Authorization Code を保存またはコピーします。

メモ: 特定のライセンスの場合、[**予約するライセンス（**Licenses to Reserve）] で [**特定のライセンスを予約（**Reserve a specific license）] を選択すると、ユーザーに利用できるライセンスの一覧が表示されます。 スマートアカウントでリクエストする際に、十分な数のライセンスを選択していることを確認してください。

---

3. [ミーティング管理] 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）] ポップアップが開きます。
   b. 予約リクエストコードを表示したり、[予約リクエスト（Reservation Request）] をキャンセルすることもできます。
   c. Smart Software Manager で生成された予約承認コードを入力し、[**承認コード/ファイルをインストール（**Install Authorization Code/ File）] ボタンをクリックして、予約を完了します。
4. [**ライセンス（**Licensing）] セクションで、[**スマートソフトウェアライセンシング状況（**Smart Software Licensing Status）] の [**登録（**Registration）] 状況が、以下の通り変更されます。
   - *[ライセンス予約保留（License Reservation Pending）] から [登録済み - ライセンス予約（Registered - License Reservation）]* へ
   - *そして ライセンス認証 を 認証済み - 予約済みとして使用します。*
5. [**ライセンス（**Licenses）] ページのライセンス状況は、以下のように表示されます。
   - PLR **で有効な予約**
   - SLR のライセンス数とともに [**予約済み（**Reserved）]。

24.3.2 予約済みライセンスを更新する

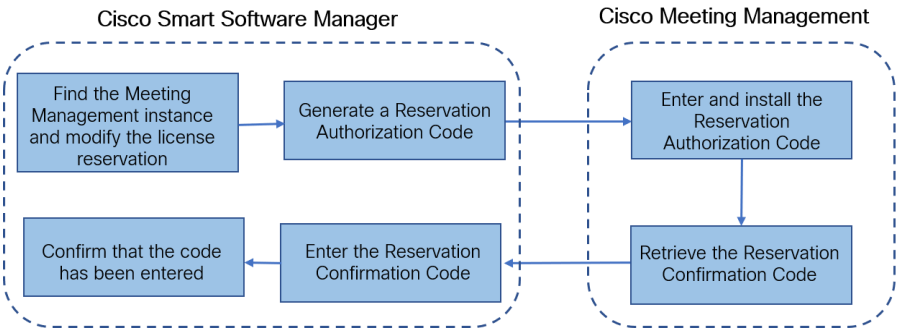
組織のニーズの変化に合わせて、特定のライセンスを更新するか、予約ライセンス数を変更できます。 たとえば、現在のライセンス要件が 5 で、さらに 5 ライセンスを追加したい場合、ライセンス数として 10 を選択する必要があり、新しい値が以前の値を上書きします。

メモ: 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、ライセンス予約タイプを PLR から SLR (またはその逆) に変更することができます。 ライセンスの予約のタイプを変更するには、予約したライセンスを返却し、製品インスタンスを登録解除し、製品インスタンスを最初から再登録します。 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ためのワークフローは以下の通りです。

1. Cisco SSM で更新するためのライセンスインスタンスを見つける
2. 予約承認コードを生成する
3. ミーティング管理でコードを入力してインストール
4. 予約確認コードを生成する
5. Cisco SSM の予約確認コードを入力して確認する

図 2: ライセンス予約更新のワークフロー



次の手順に従って予約済みライセンスを更新してください。

1. Smart Software Manager:
   a. [**製品インスタンス**（Product Instances）] から Cisco Meeting Management インスタンスを見つけて、[**ライセンスの予約を更新**（Update License Reservation）] を [**アクション**（Actions）] メニューから選択します。
   b. [**ライセンス予約を更新**（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、新しい予約承認コードを生成します。
   c. Reservation Authorization Code を保存またはコピーします。
2. Meeting Management の [**設定**（Settings）] で、
   a. [**ライセンス**（Licensing）] セクションに移動して、[**予約を更新**（Update Reservation）] ボタンをクリックします。

b. 表示されるポップアップで予約承認コードを入力し、[**予約を更新**（Update Reservation）] ボタンをクリックします。

メモ: Meeting Management インスタンスが、Universal 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**（Licensing）] セクションの [**予約済みライセンスを返却**（Return Reserved Licenses）] ボタンを使用し、このライセンスを返却し、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の予約を更新し、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シング**（Smart Software Licensing）] ページの [**確認コードを表示**（View confirmation code）] ボタンをクリックして、予約確認コードをコピーして保存します。

3. Cisco Smart Software Manager で、

a. [**製品インスタンス**（Product Instances）] で、Cisco Meeting Management インスタンスを探し、[**アクション**（Actions）] メニューの [**確認コードを入力**...（Enter Confirmation Code...）] を選択し、[**確認コードを入力**（Enter Confirmation Code）] ページを開きます。

b. [予約確認コード] を [**確認コードの入力**] ポップアップに入力します。

c. Meeting Management の [**スマートソフトウェアライセンシング**（Smart Software Licensing）] ページに戻り、[**コードが入力済み**（Code Has Been Entered）] ボタンをクリックして、予約承認コードがインストールされた後に配置された警告を無視します。

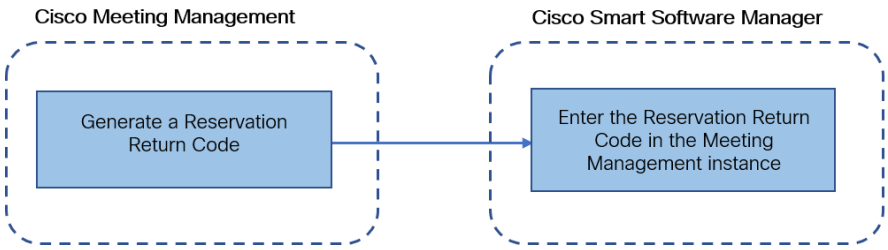
24.3.3 予約済みライセンスを返却する

予約したライセンスをバーチャルアカウントに戻すことで、他の製品インスタンスでライセンスを使用することができます。 ライセンスを返却するには、このセクションに記載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ためのワークフローは以下のとおりです。

1. Reservation リターンコードを生成します
2. Cisco SSM で、Meeting Management インスタンスを見つけます
3. 予約リターンコードを入力します

図 3: **ライセンス予約を返却するためのワークフロー**



これらの手順に従って予約済みライセンスを返却してください:

1. Meeting Management の [**ライセンス**（Licensing）] セクションの [**設定**（Settings）] で、
    a. [**予約済みライセンスを返却**...（Return Reserved Licenses...）] ボタンをクリックし、[**返却ライセンスを確認**（Confirm Return Licenses）] ポップアップを開きます。
    b. [**生成**] ボタンをクリックして予約リターン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）] ポップアップでは、指示が表示され、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 で、
    a. [**製品インスタンス**（Product Instances）] で Meeting Management インスタンスを見つけます
    b. [**アクション**（Actions）] メニューの [**削除**（Remove）] を選択し、[**製品インスタンスを削除**（Remove Product Instance）] ポップアップを開きます。
    c. ポップアップに予約返却コードを入力し、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**（Registration）] 状況が、[**登録解除済み**（Deregistered）] に変わります。

24.3.4 スマートライセンスに移行する際の考慮事項

1. 既存の従来のライセンスファイル (PAK ファイル) は、3.4 バージョンへのアップグレードに使用できます。
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) を持つ顧客は、PAK ライセンスを Smart Licensing 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。 スマートライセンスへの手動変換を行うには、新しい Global Licensing Org (GLO) リクエストを開き、使用中のスマートアカウント名、ドメイン、バーチャルアカウントを入力する必要があります。

注：
• Cisco SSM を使用して PAK を Smart Licensing に変換するセルフサービスは、新規のお客様のみ利用できます。
• 既存のライセンスから Smart ライセンスへの変換は、GLO チームの協力を得て行う必要があり、遅延が発生する場合があります。

3. 90 日間の 1 回限りのトライアルモードを使用しなくてもよいように、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 Smart Licensing に変換する計画を立てる必要があります。
4. お使いの Smart Licensing バーチャルアカウントに、過去 90 日間の Meeting Server の使用に対して十分なライセンスがあることを確認してください。 使用が多い場合、Meeting Management は、Smart Licensing への返還時に高度な強制警告モードに入ります。 高度な強制警告モードの場合、Meeting Management では 90 日間のトライアルで 1 回だけ警告を止めることができ、追加ライセンスを購入するための時間を確保できます。
5. 仮想版 CMS アクティベーションライセンス（LIC- CMS- K9）は、Smart Licensing に変換できません。代わりに、Cisco SSM が使用中の Call Bridge 数を自動的にカウントし、それをスマートアカウントの [Call Bridge**アクティブノード**（Call Bridge Active Nodes）] で報告します。 顧客は使用中の Call Bridge の数を表示することしかできません。新しい Call Bridge ライセンスを追加することはできません。

25. オプション: クラスタを TMS に関連付ける

TMS に接続されている Call Bridge を Meeting Management に通知し、その TMS システム ID を入力するには:

1. [**サーバー**（Servers）] ページで、[**クラスタを**TMS**に関連付ける**（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 を入力します。
4. [**完了**（Done）] をクリックして、Call Bridge のスケジュール済み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**（Associated with TMS）] 状況を表示します。TMS に接続されている Call Bridge には、TMS というラベルが付きます。
5. 今後のミーティングを表示するすべてのクラスタを確認するまで繰り返します。

26. オプション: TMS 電話帳にアクセスする

[ミーティング管理] は TMS 電話帳にアクセスできるため、ビデオ オペレータはミーティングに参加者を追加する際に、それらを使用して連絡先を検索できます。 検索は、TMS で連絡先を検索する場合と同様に機能します。

メモ: TMS は、ミーティングサーバが到達できない連絡先をサポートする場合があります。 ミーティングサーバの発信ダイヤルプランを更新するか、既存のダイヤルプランルールに従ってミーティングサーバが到達できない電話帳エントリをフィルターで除外してください。

ビデオオペレータがミーティングサーバから到達できない参加者を追加しようとした場合、Meeting Management は接続を試みますが失敗します。 警告やエラーメッセージは表示されません。 ビデオオペレータにはローディングアイコンがしばらく表示され、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。

メモ: TMS では、表示する検索結果の数を設定することができます。 ミーティング管理への影響はありません。 ミーティング管理には、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 電話帳を使用できるようにするには、次の 3 つの手順を実行します。

- TMS で電話帳クライアントとしてミーティング管理を追加します。

  まず、連絡が取れる連絡先だけが含まれるように電話帳を編集することが推奨されます。
- TMS の Meeting Management に電話帳を割り当てます。
- ミーティング管理で TMS 電話帳の使用を有効にします。

  メモ: これを行う前に、Meeting Management を TMS に接続する必要があります。

TMS で電話帳クライアントとして Meeting Management を追加するには:

1. Meeting Management で、[**設定**（Settings）] ページ、[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）]、[Cisco Meeting Management**の電話帳**（Phone Book for Cisco Meeting Management）] の順に選択します。

Meeting Management の *[Cisco Meeting Management**の電話帳**（Phone Book for Cisco Meeting Management）]* リンクをクリックすると、*TMS にサインインした後で適切なビューに直接移動します。*

4. [**新規作成**] をクリックします。
5. [サーバー名（Server Name）] フィールドで、Meeting Management の名前を入力します。

   他の Meeting Management および TMS 管理者にとって意味のある名前であれば、どのような名前でもかまいません。
6. [MAC アドレス] 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。

電話帳をミーティング管理に指定するには:

1. TMS で、[**電話帳**（Phone Books）]、[Cisco Meeting Management**の電話帳**（Phone Book for Cisco Meeting Management）] の順に移動します。
2. TMS でミーティング管理に付けた名前をクリックします。
3. ミーティング管理に使用する電話帳を選択し、[**保存**] を選択します。

電話帳を使い始めるには:

1. Meeting Management で、[**設定**（Settings）] ページ、[TMS] タブに移動します。
2. [TMS**電話帳を使用**（Use TMS phonebook）] チェックボックスを選択します。
3. 上の領域で、Meeting Management を TMS に初めて接続する際に使用したアカウントのパスワードを入力し、Meeting Management を**保存**して、**再起動**します。

27. LDAP サーバーのセットアップ

メモ: ユーザーグループを使用するように Meeting Management を設定する前に、LDAP サーバー上ですべてのユーザーグループを設定する必要があります。

27.1 LDAP サーバーのセットアップ

LDAP サーバーを使用するために Meeting Management をセットアップするには:

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

   LDAP は暗号化されていない TCP 接続用です。LDAPS はセキュアな接続用で、オプションで認証に証明書トラスト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。

   既定のポート番号:

   - *LDAP: 389*
   - *LDAPS: 636*

   メモ: AD を使用しており、ベース DN がドメインコンポーネント (DC) レベルのみで設定されている場合、グローバルカタログの検索にはデフォルトのポート (LDAP ポート 3268、LDAPS ポート 3269) を使用します。

   メモ: LDAP サーバアドレスが文字通りの IPv6 アドレスである場合、角括弧で囲んで入力します。
5. オプション: 証明書を使用し、証明書が失効している場合に Meeting Management が接続を拒否するよう選択した場合、**証明書失効リスト**（CRL）**と証明書を確認します。**

   チェーンの証明書が失効しているか、アクセスできない CRL がある場合、ミーティング管理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お勧めします。

メモ: HTTP 証明書配布ポイント (CDP) を持つ証明書のみがサポートされています。 CRL チェックを使用していて、証明書に CDP が含まれていない場合、または HTTP 経由で CDP に到達できない場合、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にネットワークを設定する必要があります。

6. LDAPS を使用している場合は、[**証明書のアップロード**（Upload certificate）] をクリックして、LDAP サーバーの証明書チェーンを Meeting Management トラスト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 サーバーの証明書に署名した CA の証明書および、ルート CA 証明書まで、証明書チェーンの上位証明書を含める必要があります。*
   - *LDAP サーバー用に入力したサーバーアドレスは、LDAP サーバー証明書に含まれている必要があります。*

7. バインド DN とパスワードを入力します。

   これらは、Meeting Management を LDAP サーバーにバインド（認証）するユーザーアカウントの資格情報です。

   メモ: これらのフィールドでは大文字と小文字が区別されます。

8. **ベース** 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。 ミーティング管理は、このノードと、LDAP ツリー内でその下にあるすべてのノード内の LDAP グループを検索します。

   メモ: このフィールドでは大文字と小文字が区別されます。

   メモ: ベース DN がドメインコンポーネント (DC) レベルのみで設定されている場合、グローバルカタログの検索にはデフォルトのポート (LDAP ポート 3268、LDAPS ポート 3269) を使用します。

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

   検索属性は、ユーザがミーティング管理にログインするときにユーザ名として入力する LDAP 属性です。

   メモ: このフィールドでは大文字と小文字が区別されます。

10. 設定を**保存**して、Meeting Management を**再起動**します。

    メモ: 今すぐ再起動するか、構成が完了するまで待ってください。

28. LDAP グループの追加

LDAP ユーザーグループは LDAP サーバーで設定され、Meeting Management にマッピングされるため、Meeting Management は LDAP サーバーを使用し、ログイン時にグループメンバーシップを確認することでユーザーを認証できます。

ユーザーと LDAP ユーザーグループの詳細については、「始める前に」の記事を参照してください。

28.1 LDAP ユーザグループの追加

ユーザグループを追加するには:

1. [**ユーザー**（Users）] ページで、[LDAP**ユーザーグループ**（LDAP user groups）] タブに移動します。
2. [LDAP**グループを追加**（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、グループが検出されるかを確認します。
5. グループが見つかった場合は、[**ユーザの表示**] をクリックして、お探しのユーザ名がこのグループに表示されているかどうかを確認します。
6. グループのロールを選択します。
7. [**ユーザープロファイルの表示**（View User Profile）] ボタン (選択したユーザーに対する [**アクション**（Actions）] で利用可能) をクリックして [**ユーザープロファイル**（User Profile ）] ポップアップウィンドウを起動します。
8. **タグを追加する** フィールドでタグ (オプション) を割り当てます。 最大 10 個のタグを追加できます。

   これにより、管理者はビデオ オペレーターにタグを割り当て、タグが付けられたミーティングのみにアクセスできるようにすることができます。 タグの追加の詳細については、『ミーティング 管理者ガイド』を参照してください。
9. [**次へ**（Next）] をクリックします。

10. オプション: **リンクをコピー**すると、リンクをユーザーに送信できます。

    ここに表示されるリンクが 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の別のアドレスをユーザーに指定する場合は、そのアドレスを指定します。

11. [**完了**（Done）] をクリックします。
12. Meeting Management を**再起動**します。

    メモ: 今すぐ再起動するか、構成が完了するまで待ってください。

29. オプション: ローカルユーザーのセキュリティポリシーをセットアップする

ユーザ ページの **ローカル設定** タブでローカルユーザのセキュリティポリシーをセットアップすることができます。 次のポリシーをセットアップすることができます。

- 最小パスワード長を要求する**パスワードポリシーを適用する**

  これは選択するまで無効になっています。 デフォルトの最小文字数は 8 文字です

- **パスフレーズジェネレータを使用**して組み込みパスフレーズジェネレータを有効にする

  内蔵のパスフレーズ ジェネレーターが辞書から単語を組み合わせて新しいパスワードを提案します。 パスフレーズのデフォルトの単語数は 5 で、1 ~ 8 の間で任意の数を選択できます。

  内蔵のパスフレーズ ジェネレーターを使用する場合は、辞書を提供する必要があります。 辞書の要件:

  - *辞書は各行に 1 単語を含むテキストファイルでなければなりません。*
  - *文字は UTF-8 でエンコードされている必要があります。*
  - *このファイルには null 文字が含まれていてはなりません。*
  - *ファイルサイズの上限は 10 MB です。*

- **パスワード再利用ポリシーを強制**し、パスワードの再利用を制限する

  これは選択するまで無効になっています。 値を入力するまで、入力フィールドは空白になっています。

メモ: セキュリティポリシーの変更は、Meeting Management を**再起動**後有効になります。 今すぐ再起動するか、初期構成が完了するまで待ってください。

メモ: **パスワードポリシーを適用**および**パスワード再利用ポリシーを適用**は、ユーザーが各自のパスワードを変更した場合にのみ適用されます。

メモ: パスフレーズジェネレータが有効になっている場合、ミーティング管理はすべてのユーザのパスフレーズを提案します。

- **パスフレーズ検証ツールを使用して**一般的に使用される単語、繰り返し使用される文字、または連続する文字を含む辞書と照合して、ユーザーパスワードの品質をチェックします。

  リストには、サービス名、ユーザ名、製品名、派生語など、コンテキストに固有の単語も含まれます。ユーザが選択したパスワードがリストから一致した場合、パスフレーズ検証機能はパスワードを拒否し、ユーザに別の値を選択するよう通知します。

  辞書の要件:

  - *辞書は各行に 1 単語を含むテキストファイルでなければなりません。*
  - *文字は UTF-8 でエンコードされている必要があります。*
  - *このファイルには null 文字が含まれていてはなりません 。*
  - *ファイルサイズの上限は 10 MB です。*

  パスフレーズ検証を有効にするには:

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

  注：
  • Meeting Managementには既定の辞書が用意されていません。 管理者は辞書を定義してアップロードする必要があります。
  • ミーティング管理のバックアップ時に辞書が存在する場合、バックアップファイルにも辞書が含まれます。 バックアップファイルが復元されると、辞書も復元されます。

- [**パスワードの複雑さを強制する**（Enforce password complexity）] でパスワードの強度を確認します。 ユーザーがパスワードを作成するときに、パスワードに要求される複雑さのレベルを設定できます。

  *ローカルユーザーを追加または編集する際に、[**ローカルユーザーを追加（**Add Local User）] ポップアップウィンドウでユーザーが設定したパスワードが、管理者が設定した複雑さの基準を満たしていない場合、Meeting Management は、パスワードの強度を満たすために必要な文字を含めるようユーザーに通知します。この機能は、選択するまで無効になっています。*

*ユーザーのセキュリティポリシーを設定するときに、[**パスワードの複雑さを強制する（Enforce password complexity）**] のオプションのいずれかまたはすべてを選択します。*

- 大文字（A-Z）を含む
- 小文字（a-z）を含む
- 少なくとも 1 つの数字 (0-9) を含む
- 1 文字以上の特殊文字 (!$%^&*()_+|~-={}[]:";'<>?,/) を含む。パスワードを完全に

有効にするには、以下の手順に従います。

1. [**パスワードの複雑さを強制する（**Enforce password complexity**）**] までスクロールして、[**パスワードの複雑さを強制する（**Enforce password**）**] チェックボックスを有効にします。
2. ユーザのパスワードに必要なオプションのチェックボックスを選択します。
3. [**保存（**Save**）**] をクリックします。

- [**パスワードの有効期限を強制する（**Enforce password expiration**）**] でパスワードの使用期間を日数で設定します。 パスワードの有効期限が切れると、ミーティング管理はユーザのアクセスを無効にし、パスワードを変更するように通知します。

  有効にすると、現在のパスワードの有効期限が切れた後にユーザがログインしたときに、ミーティング管理はユーザに新しいパスワードを作成するよう通知します。

  これは選択するまで無効になっています。 入力フィールドのデフォルト値は、30 日に設定されます。

  パスワードの有効期限を有効にするには:

  1. [**パスワードの有効期限を強制する（パスワードの有効期限を強制する）**] までスクロールして、[**パスワードの有効期限を強制する（**Enforce password expiration**）**] チェックボックスを有効にします。
  2. [**最長寿命日数（**Maximum age of password (in days)**）**] フィールドに日数を入力します。
  3. [**保存（**Save**）**] をクリックします。
  4. Meeting Management を再起動します。

メモ: パスワードの有効期限が初めて有効になったとき、すべてのローカルユーザのパスワードは期限切れになり、ユーザはパスワードを変更する必要があります。

---

30. オプション: ローカルユーザーを追加する

[**ユーザ**] ページの [**ローカル**] タブでローカルユーザアカウントを追加、削除、編集できます。 ユーザーの詳細については、「始める前に」の記事を参照してください。

ローカルユーザを追加するには:

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

   メモ: ユーザ名を後から変更することはできません。保存する前に慎重に確認してください。

4. オプション: 姓名を入力します。
5. 役割を指定します。
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て、[**追加**（Add）] をクリックします。
8. [**タグを追加**（Add tags）] フィールドで、タグを入力します。 最大 10 個のタグを追加できます。

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

ローカルユーザを削除するには:

1. **ユーザ** ページで [**ローカル**] タブに移動します。
2. 削除するユーザを見つけてクリックします。 [**アクション**（Actions）] 列で。

メモ: 現在ログインに使用している管理者アカウントを削除することはできません。

ローカル管理者ユーザーアカウントが 1 つしかなく、それを削除したい場合は、LDAP 管理者としてサインインしてローカルアカウントを削除します。

ローカルユーザーを編集する:

1. [**ユーザー**（Users）] ページで、[**ローカル**（Local）] タブに移動します。
2. 編集するユーザーを見つけて、[**アクション**（Actions）] 列の [**ユーザープロファイル**（User profile）] ボタンをクリックします。
3. 必要に応じて変更を行います。
4. [**完了**（Done）] をクリックします。

31. 確認、保存、バックアップ

すべての情報が正しく入力されていることを確認したら、必要に応じて、Meeting Management を再起動します。 構成を保存するため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。

設定のバックアップを取れば、Cisco Meeting Management を使い始める準備が完了です。

32. バックアップと復元

ミーティング管理に変更を加える前に、新しいバックアップを作成しておくことをお勧めします。 バックアップには以下が含まれます:

- *設定:*
    - 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
    - ローカルユーザ用のセキュリティポリシー設定

  これにはパスフレーズジェネレータの設定が含まれますが、辞書は含まれません
- *データベース:*
    - ローカル ユーザの詳細 (最近使用したパスワードのハッシュを含む)
    - TMS システム ID を含むすべての Call Bridge の詳細
    - パスフレーズ辞書

32.1 バックアップを作成する

ミーティング管理の使用を開始する前に、バックアップを作成しておくことをお勧めします。その後、再展開が必要になった場合に、設定を簡単に再利用できます。

1. 再起動が必要な場合、今すぐこれを実行すると、すべての変更が有効になります。
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をダウンロード**（Download backup file）] をクリックします。
4. パスワードを入力して [**ダウンロード**] を選択してください。
5. 安全な場所にバックアップファイルとパスワードを保存します。

メモ: バックアップは暗号化されているため、パスワードがなければ使用できません。

32.2 バックアップを復元する

バックアップを復元する前に:

- バックアップファイルとパスワードが手元にあることを確認してください。

  パスワードはあなたまたは他の管理者がバックアップを作成した際に選択されたものです。

- すべての設定を復元するか、またはデータベースまたは構成の詳細を復元するかを決定します (ステップ 4 を参照)。
- バックアップを復元する間、LDAP サーバがオンラインになっ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、バックアップの復元中に TMS がオンラインになっていることを確認してください。

メモ: 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。

メモ: LDAP の詳細を復元する場合、ローカル管理者としてログ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:

1. [**設定**] ページで [**バックアップと復元**] 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**] をクリックします。
3. *バックアップファイル を選択してください。*
4. 1 つ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
     - ローカルユーザ用のセキュリティポリシー設定

       これにはパスフレーズジェネレータ、パスフレーズ検証、パスワードの複雑さの強制、パスワードの有効期限の強制の設定が含まれますが、辞書ファイルは含まれません。
   - ***データベースを復元する***:
     - ローカル ユーザの詳細 (最近使用したパスワードのハッシュを含む)

- TMS システム ID を含むすべての Call Bridge の詳細
- パスフレーズ辞書

2 つのオプションのいずれかをチェックしないと、バックアップを復元することができません。

5. パスワードを入力し、**復元します**。

注：

- メモ：Meeting Management を復元する際に、ローカルユーザーとしてサインインした場合、Meeting Management は、お使いのアカウントをバックアップからリストに追加するか、現在の設定を維持したままバックアップされたプロファイルを更新します。 他のすべての設定は、バックアップの設定で置き換えられます。
- バックアップの取得後に管理者およびビデオオペレータのパスワードを変更し、ダウンロードしたバックアップファイルを復元すると、ビデオオペレータは復元したパスワードを使用して Meeting Management にログインでき、管理者は変更した認証情報を使用してログインできるようになります。

---

32 キーをアップロードしてアップグレードイメージを検証する

Cisco Meeting Management は、画像が本物であるか、または改ざんされているかを確認するアップグレード画像に署名を埋め込みます。

イメージの署名は、署名されたイメージからアップグレードする場合にのみ検証されます。 そのため、未署名のイメージから署名済みのイメージにアップグレードする場合は、手動での検証が推奨されます。つまり、3.6 から 3.7 へ、またはそれ以前のバージョンへダウングレードする場合も、ハッシュを手動で確認することをお勧めいたします。 この機能は 3.7 以降からアップグレードすることで有効になります。

バージョン 3.7 から、特別なビルドへのアップグレードには特別なキーのアップロードが必要になります。 [**アップロードキー**（Upload Key）] ボタンは、有効な管理者のみに導入されます。これにより、パブリックキーをアップロードでき、アップグレード画像を確認できます。ただし、管理者は特別なビルドにアップグレードする場合にのみ、このアクションを実行します。

公開鍵をアップロードするには:

1. [**設定**（Settings）] ページの [**アップグレード**（Upgrade）] タブに移動します。
2. [**アップロードキー**（Upload Key）] をクリックし、パブリックキーを参照して選択します。 選択した公開鍵が確認され、アップロードされます。

メモ: 署名されたプロダクション/スペシャルビルドから別の署名されたプロダクションビルドへのアップグレードは、管理者からのアクションを必要としません。 ミーティング管理はハッシュの手動確認を必要とせずに、自動的にアップグレードイメージを確認します。

---

33 ミーティング管理の再起動

ミーティング管理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。 ミーティング管理を再起動するには:

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

メモ: ミーティング管理を再起動すると、すべてのユーザーは警告なしにサインアウトされ、ミーティングに関するすべての情報は Meeting Management から削除されます。 再開後もアクティブなミーティングの開始時間、および接続している参加者の参加時間は、API リクエストを介して復元されます。 ミーティングの詳細に表示される時刻は正確ですが、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 マスタープロジェクトの Voluntary Product Accessibility Template (VPAT) は、ここで入手可能です。

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

アクセシビリティの詳細については、

www.cisco.com/web/about/responsibility/accessibility/index.html で詳細情報を見つけることができます。

34 アクセシビリティサポート機能

34.1 キーボード ナビゲーション

キーボードを使って Meeting Management を操作することができます。

- **タブ**を使用すると、Meeting Management の領域を移動できます。 輪郭で囲まれた領域にフォーカスが合っていることがわかります。 Shift + Tab を使用すると、前にフォーカスしていた領域に移動できます。
- **スペースバー**または Enter キーを押して項目を選択します。
- 矢印キーを使用して、リストまたはドロップダウンリスト メニューをスクロールします。
- Esc を使用すると、開いている画面やメニューを閉じる、または解除できます。

34.2 スクリーンリーダーのサポート

JAWS スクリーンリーダーのバージョン 18 以降を使用できます。

スクリーンリーダーは、フォーカスされている領域/ボタン、通知、警告、画面に表示されるステータスメッセージなどの関連情報、および実行できるアクションを通知します。

例: [**スペースを作成**（Create Space）] ボタンにフォーカスすると、スクリーンリーダーは "スペースを作成" と読み上げ、スペース名を入力するよう指示します。

Cisco の法的情報

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

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

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

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。 CISCO およびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、CISCO 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 CISCO またはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

★定型★このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。 ★定型★マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。 説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

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

Cisco 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。

© 2024 Cisco Systems, Inc. All rights reserved.

Cisco の商標または登録商標

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。 シスコの商標のリストを表示するには、次の URL にアクセスしてください。

www.cisco.com/go/trademarks。 記載されているサードパーティの商標は、それぞれの所有者に帰属します。 「パートナー」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。 (1721R)