



Cisco Meeting Management

リリース 3.11

管理者向けユーザガイド

2025 年 4 月 30 日

目次

ドキュメントの改訂履歴	7
1 はじめに	8
1.1 3.11 の新機能	8
1.2 ソフトウェア	9
2 展開の概要	10
2.1 ユーザの認証	11
2.2 セキュリティと監査	11
2.3 診断とトラブルシューティング	11
2.4 Cisco TelePresence Management Suite (TMS) との統合	12
2.5 ミーティングサーバのライセンス	12
2.6 スマート ライセンス用の Cisco Smart Software Manager への接続	12
2.7 電子メールまたは Webex Teams 通知用の Cisco Meeting Server クラウド コネクタ	13
2.8 Meeting Server クラスタでのユーザのプロビジョニングとスペース テン プレートの作成	13
2.9 レジリエンス	13
2.10 会議数が多い場合の容量制限	14
2.11 Cisco Meeting Server API またはサードパーティのツールを使用している場合	14
3 概要 - 通知、Cloud Connector のステータス、ライセンスのステータスを表示します	15
4 会議 - 会議の監視と管理	16
5 スペース - スペース管理とブラストダイヤルの設定	17
5.1 スペース管理	17
5.1.1 スペースを作成する	17
5.1.2 スペースを表示する	18
5.1.3 スペースの編集	18
5.1.4 スペースの削除	19
5.1.5 参加情報	19
5.1.6 アクセスロールの編集	19
5.2 ブラストダイヤルの設定	19
5.2.1 設定	20

5.2.2	ダイヤルアウト連絡先の追加.....	20
6	ユーザー - ユーザーを追加またはユーザー設定を編集する.....	22
6.1	ユーザーについて.....	22
6.2	LDAP サーバの詳細を編集する.....	23
6.3	ビデオオペレータにスペースを割り当てる.....	23
6.4	LDAP グループの追加.....	24
6.4.1	LDAP ユーザグループの追加.....	24
6.5	ローカルユーザのセキュリティポリシーを設定する.....	25
6.6	ローカルユーザを追加する.....	28
7	サーバ - サーバを追加または編集する.....	30
7.1	設定したサーバーの追加.....	30
7.2	新しいサーバーを設定する.....	34
7.2.1	ステージング.....	34
7.2.2	新規ミーティングサーバの追加.....	34
8	証明書.....	38
8.1	CA 署名付き証明書.....	38
8.1.1	CSR による新しい証明書.....	38
8.1.2	既存の証明書とキーを使用.....	40
8.2	自己署名証明書.....	41
9	ネットワーク.....	42
9.1	DNS または NTP サーバの削除.....	42
10	Call Bridge.....	44
11	Web Bridge.....	45
12	電話会議ユーザー.....	46
12.1	LDAP 検索とユーザ マッピングをカスタマイズする.....	48
13	安全.....	51
14	プッシュ構成.....	52
14.1	SSH 機能.....	52
15	クラスターの会議管理を無効にする.....	53
16	プロビジョニング.....	54
16.1	スペースとは?.....	54

16.2	スペース テンプレートとは何ですか?	54
16.3	プロビジョニング手順	54
16.4	プロビジョニング - 始める前に	55
16.4.1	サポートされている LDAP 実装	55
16.4.2	LDAP サーバの詳細	56
16.4.3	ユーザのインポートの詳細	56
16.5	プロビジョニング - LDAP サーバ	57
16.5.1	LDAP サーバを追加する方法	57
16.6	プロビジョニング - ユーザのインポート	58
16.6.1	ユーザインポートを追加する方法	58
16.7	プロビジョニング - スペースを自動的に作成	60
16.7.1	スペースを自動的に作成するためのルールを追加する	60
16.8	プロビジョニング - ユーザーがスペースを作成できるようにする	64
16.8.1	制約事項	64
16.8.2	特定のウェブアプリユーザにスペーステンプレートを割り当てる方法	65
16.9	プロビジョニング - レビューとコミット	68
16.10	プロビジョニング - LDAP 同期	69
17	ログ - ログ、クラッシュレポート、 詳細なトレース	70
17.1	会議管理ログ	70
17.1.1	ログバンドル	70
17.1.2	システムログサーバ	70
17.1.3	監査ログサーバ	71
17.1.4	クラッシュレポート	71
17.1.5	詳細なトレース	72
17.1.6	90 日間のライセンスレポート	72
17.2	Meeting Server ログ	72
17.2.1	ログバンドル	72
17.2.2	詳細なトレース	73
17.3	ログサーバを追加または編集する	73
18	ライセンス	76
19	ライセンス状況と適用	78
19.1	利用可能なトライアル	79
19.2	試用中および試用後のライセンスステータス	81
19.3	実行と警告	81

20	ブラストダイヤル監視	83
21	設定 - 会議管理を構成する	84
21.1	ネットワーク詳細の編集	84
21.2	証明書のアップロード	84
21.3	CDR 受信者アドレスを編集する	85
21.4	TMS に接続.....	85
21.4.1	クラスターを TMS に関連付ける	86
21.4.2	TMS 電話帳にアクセスする.....	87
21.5	NTP ステータスの確認、または NTP サーバの追加.....	88
21.6	ライセンス.....	89
21.6.1	スマート ライセンスを有効にする方法	90
21.6.2	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....	91
21.6.3	ライセンス予約.....	92
21.6.3.1	ライセンス予約	93
21.6.3.2	予約済みライセンスの更新	96
21.6.3.3	予約済みライセンスの返却	98
21.6.3.4	スマートライセンスへの移行時に考慮すべき事項.....	99
21.7	Cisco Meeting Server クラウド コネクタ	100
21.7.1	Cisco Meeting Server クラウド コネクタのステータス.....	100
21.8	ユーザがログインしたときにメッセージを表示する.....	100
21.9	高度なセキュリティ設定を構成する.....	102
21.9.1	サインイン試行のレート制限.....	102
21.9.2	アイドル セッションのタイムアウト	103
21.9.3	Meeting Server のパスワードをリセット	103
21.9.4	TLS 設定.....	103
21.10	バックアップと復元.....	104
21.10.1	バックアップを作成する	104
21.10.2	バックアップを復元する	105
21.11	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.....	106
21.12	ミーティング管理の再起動	107
付録 A	セキュリティ強化	108
	アクセシビリティ通知.....	109
B	アクセシビリティサポート機能.....	110
B.1	キーボード ナビゲーション	110

B.2 スクリーンリーダーのサポート	110
Cisco の法的情報.....	111
Cisco の商標または登録商標.....	112

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
2025-04-30	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
- 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。

1.1 3.11 の新機能

新しい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。

このリリースでは、次のセクションが更新されました。

- [ローカルユーザーに対してセキュリティポリシーをセットアップする](#) - 初回ログイン時のパスワード変更に関する情報を含むセクションを追加し、パスワード有効期限の適用を強化して、必須である次回のパスワード変更に関してユーザーに送信する警告とエラー通知を含む情報を含めるようにしました。
- [高度なセキュリティ設定を構成する](#) - 「サインイン試行のレート制限」項を更新し、レート制限が有効になっていない場合に許可されるサインイン試行の最大失敗回数に関する情報を含めました。
- [ライセンス](#) - Cisco Smart Licensing 輸出コンプライアンス ポリシーに従い、カテゴリ C および D に該当する国向けに通話暗号化用の単一ライセンスを予約するための情報を追加しました。

1.2 ソフトウェア

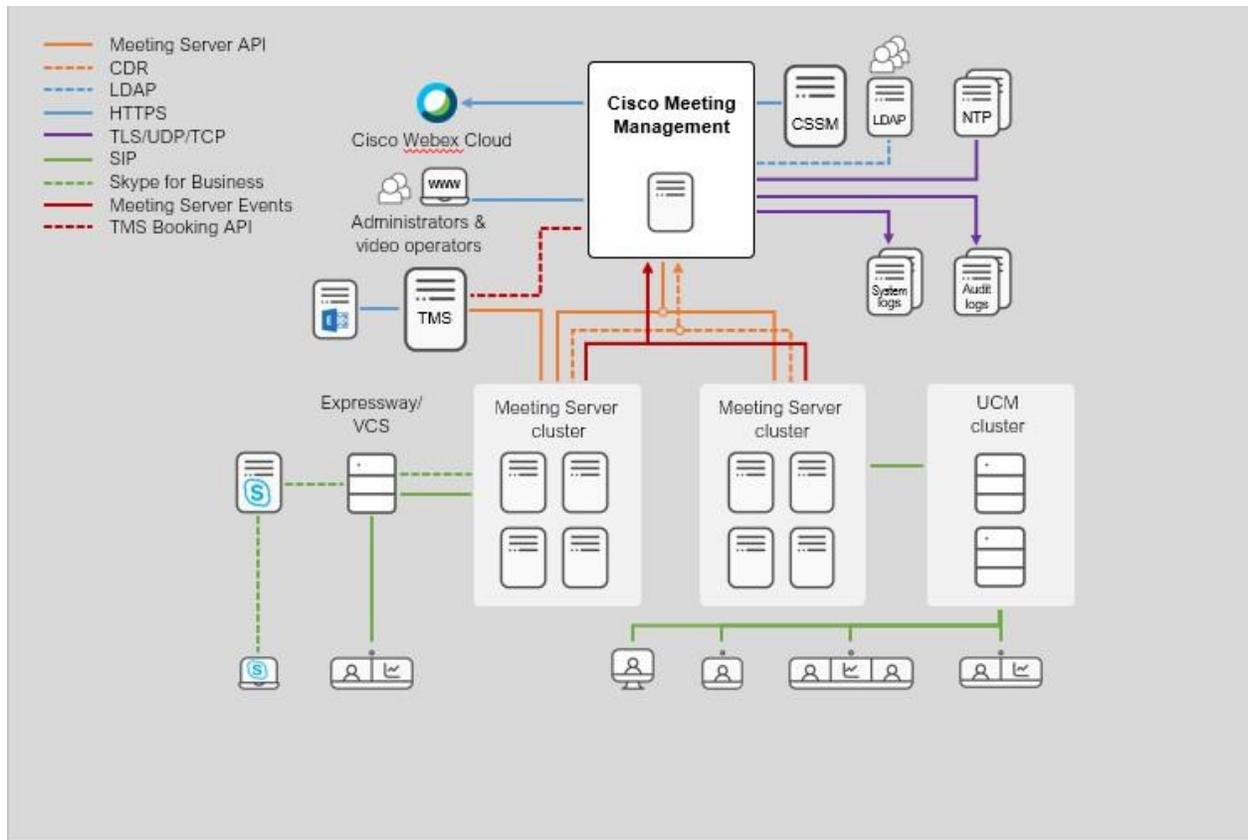
会議管理は仮想化されたアプライアンスです。VM (仮想マシン) の仕様は、会議管理で同時に実行または監視する必要があるアクションの数によって異なります。管理する Call Bridge の数に関連したサイズの見積もりを含む仕様と要件については、[インストールおよび構成ガイド](#)を参照してください。

セキュリティ上の理由から、初回実行後はユーザはコンソールにアクセスできません。インストール プロセスを除き、Meeting Management のすべての使用はブラウザー インターフェイスを介して行われます。

2 展開の概要

1 つの Meeting Management インスタンスで、単一の Call Bridge のみを含む小規模な Meeting Server 展開、または次に示すように複数の Call Bridge クラスタを含む大規模な Meeting Server 展開を管理できます。

図 1: Meeting Server 導入内の単一の Meeting Management



会議管理は、Call Bridge API を介して会議サーバに接続します。会議作業に関する情報を取得するため、各 Call Bridge に、CDR（通話詳細記録）レシーバーおよびイベントクライアントとして自身をインストールし、API リクエスト、CDR、Meeting Server イベント経由でアクティブな会議の情報を取得します。

注: クラスタのライセンスとプロビジョニングにのみ Meeting Management を使用することを選択した場合、Meeting Management はそのクラスタ内の Call Bridge の CDR レシーバーまたはイベントクライアントとして機能しません。

信頼性と精度を高めるために、複数の NTP サーバを設定できます。Meeting Management は最大 5 台の NTP サーバをサポートします。すべての Meeting Server と Meeting Management のすべてのインスタンスを同じ NTP サーバに接続することをお勧めします。

2.1 ユーザの認証

Meeting Management は、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。ローカルユーザーは、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ーを認証し、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ー 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 経由でユーザーを認証することを推奨します。

注: すべてのユーザーは、管理者またはビデオ オペレータのいずれかになることができます。権限はロールのみによって決まり、ローカルで管理されるか、LDAP 経由で管理されるかは関係ありません。

2.2 セキュリティと監査

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

バックアップ ファイルは、ユーザーが指定したパスワードで保護されます。

アクティブな会議と最近の会議のイベント ログは、会議管理で確認できます。監査ログとシステム ログを外部の syslog サーバに送信できます。

また、高度なセキュリティ設定により、特定の設定が必要な場合に組織のセキュリティ ポリシーに準拠できます。

2.3 診断とトラブルシューティング

会議管理では、限られた量のシステム ログがローカルに保存されます。すべての監査ログとシステム ログは外部サーバに送信できます。

クラッシュ ログと [ログバンドル](#) はサポート目的で利用できます。

Call Bridge の詳細、ローカル ユーザー アカウント、およびパスフレーズ辞書は、他の構成の詳細とは別に復元できます。

2.4 Cisco TelePresence Management Suite (TMS) との統合

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

会議管理は予約 API を介して TMS に接続し、5 分ごとに電話帳にアクセスできるかどうかを確認し、スケジュールされた会議の情報を更新します。今後の会議は、予定された開始時刻の 24 時間前まで会議管理に表示されます。

Meeting Management と TMS でよりシームレスに管理するため、スケジュールされた各会議に、Meeting Management の会議詳細から TMS の編集ページへの直接リンクを配置する必要があります。

2.5 ミーティングサーバのライセンス

Meeting Management はライセンスの目的で、Meeting Server 3.0 以降では必須です。スマートライセンスを使用している場合は、Cisco Smart Software Manager に接続する必要があります。会議管理では、ローカルライセンスファイル (従来のライセンスモード) のサポートが廃止され、ライセンス予約が導入されました。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。詳細については、[ライセンス](#) セクションを参照してください。

注: Cisco Smart Licensing Portal のルート CA は、2023 年 2 月に更新されます。Smart Licensing (オンライン、SLR、または PLR) を使用している場合は、新しいライセンスの追加、コールブリッジの追加、または手動同期の実行中に、3.6 以上にアップグレードすることをお勧めします。

2.6 スマートライセンス用の Cisco Smart Software Manager への接続

会議管理を使用すると、Cisco Meeting Server の展開で購入したライセンスよりも多くのライセンスが使用されているかどうかを監視できます。

会議管理は、Smart Agent を使用して Cisco Smart Software Manager (Cisco SSM) と通信します。会議管理は毎日の使用状況レポートを Cisco SSM に送信し、Cisco SSM は展開が準備しているかどうかを報告します。

注: 復元力を追加するなど、同じ Meeting Server クラスタに複数の Meeting Management インスタンスが接続されている場合は、Cisco Smart Software Manager に接続する Meeting Management インスタンスは 1 つだけにする必要があります。両方のインスタンスを接続すると、報告される使用量は 2 回カウントされます。

2.7 電子メールまたは Webex Teams 通知用の Cisco Meeting Server クラウド コネクタ

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

Cloud Connector は、製品の改善に役立てるために統計情報を Cisco に送信します。送信される情報を確認するには、Cisco Meeting Server Cloud Connector のオンライン ヘルプ を参照してください。

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

Meeting Management を使用すると、1 つ以上の LDAP サーバーから接続された Meeting Server クラスタにユーザーをインポートすることで、Cisco Meeting Server Web アプリユーザーをプロビジョニングできます。また、Web アプリ ユーザが新しいスペースを作成するために使用できる、事前構成されたスペース設定であるスペース テンプレートを作成することもできます。

会議管理は、この目的で LDAP サーバと直接通信していないことに注意してください。代わりに、LDAP サーバの詳細とフィルター設定が Meeting Server に送信され、LDAP 同期がトリガーされたときに Meeting Server はその詳細を使用してユーザをプロビジョニングします。

注: セキュリティと監査上の理由から、各 LDAP サーバ上の各 Meeting Server クラスタごとに個別のバインド ユーザ アカウントを作成することをお勧めします。

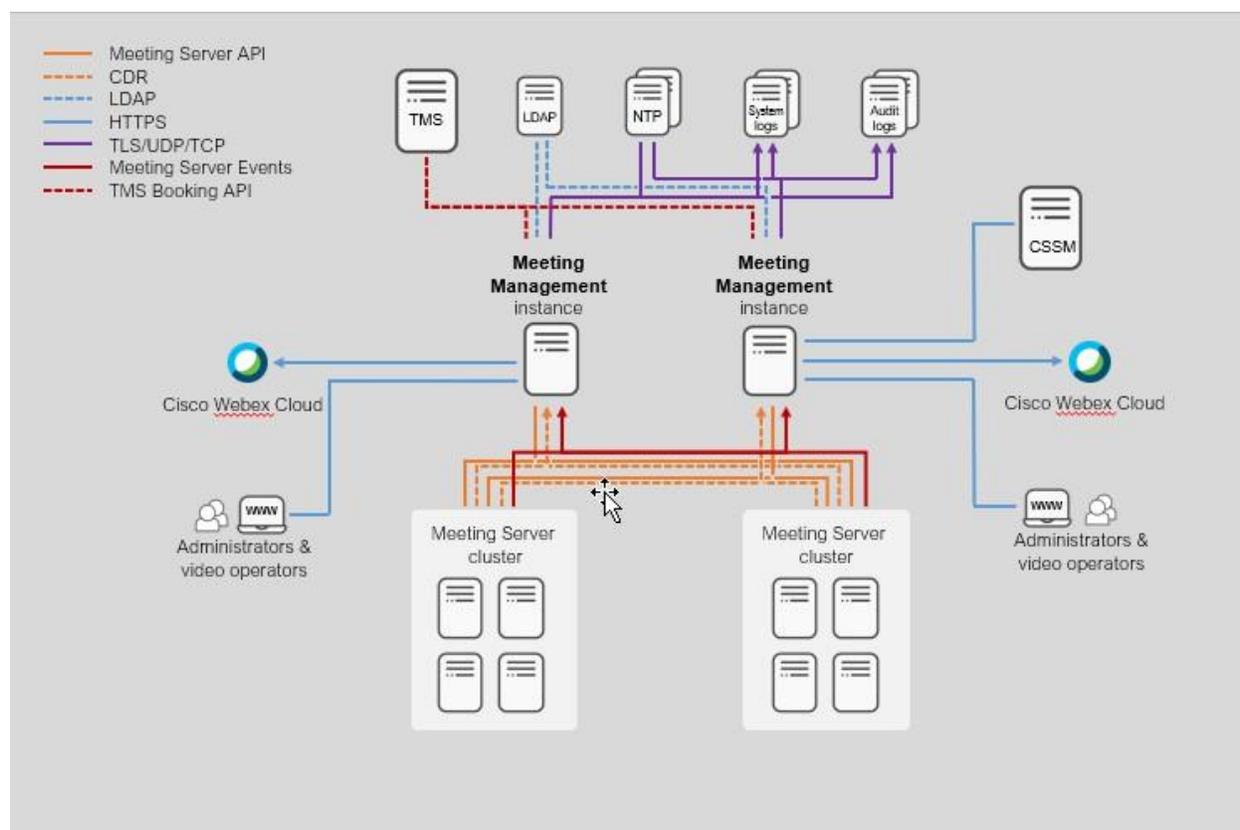
2.9 レジリエンス

会議管理の展開に回復力を追加するには、同じ会議サーバ展開に最大 2 つの会議管理インスタンスを接続できます。これらは個別に設定する必要があります。両方とも、接続された Call Bridge と TMS サーバ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。Meeting Management の 2 つのインスタンスを別の場所に配置することをお勧めします。これにより、停電や接続の問題が両方のインスタンスに同時に影響を与えないようにします。

フェイルオーバーはありません。両方のインスタンスは常にアクティブであり、会議をリストの先頭に固定するなど、Meeting Management にローカルな設定は、設定された Meeting Management のインスタンスにのみ表示されます。

注意: 回復力のある展開の場合、レポートの重複を避けるために、ライセンスには Meeting Management のインスタンスを 1 つだけ使用してください。 [「ライセンス」](#) を参照してください。

図 2: 回復力のある会議管理の展開



2.10 会議数が多い場合の容量制限

会議管理機能のパフォーマンスは、接続されている Call Bridge 上の会議の量によって異なります。容量の制限については、『インストールおよび構成ガイド』の「開始する前に」セクションの容量表を参照してください。大規模な展開の容量を超える展開がある場合は、会議管理機能を無効にする必要があります。接続されているクラスターごとに個別にこれを実行できます。

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

会議管理を使用して会議を監視または管理しているときに、アクティブな会議を管理するために API または API を使用するサードパーティ ツールを使用しないことを強くお勧めします。

3 概要 - 通知、Cloud Connector のステータス、ライセンスのステータスを表示します

概要 ページでは、いつでもシステム通知と Webex Edge のステータスを確認できます。

通知は **概要** ページに常に表示され、上部のバーのカウンターに現在通知があるかどうかが表示されます。

通知には 3 つの重大度レベルがあります。

- **エラー:** 重大な問題
- **警告:** 会議管理を継続するために対処する必要がある問題
- **情報:** 役に立つ情報または軽微な問題

ログインしている Meeting Management のインスタンスでライセンスが有効になっている場合は、Cisco Meeting Server の [ライセンス ステータス](#) も表示されます。

Meeting Management が Smart Licensing を使用している場合、ライセンス状況は、接続済みのすべてのクラスターで同じになります。青い Smart Licensing の見出しをクリックすると、[[ライセンス \(Licenses\)](#)] ページに移動します。ここでは、詳細を表示したり、編集したりできます。

The screenshot shows the Cisco Meeting Management Overview page. The top navigation bar includes the Cisco logo, 'Cisco Meeting Management', a 'Notifications' counter (3), and the user 'LDAP/Sally Wood Administrator'. The main content area is divided into three sections:

- Notifications:** A list of three notifications:
 - Error:** 'The credentials provided for server Server 1 are incorrect' (17/03/2021 12:35:08)
 - Warning:** 'Events communications with server Server 2 have been disrupted' (17/03/2021 12:35:08)
 - Information:** 'The server Server 3 is attempting to synchronize so meeting and participant details may be incomplete' (17/03/2021 12:35:08)
- License status:** A section for 'Smart Licensing' with three status indicators:
 - Meetings: **In compliance** (green)
 - Recording or Streaming: **In compliance** (green)
 - Customization: **Unlicensed** (grey)
- Cloud Connected Cisco Meeting Server Status:** A section showing 'Cloud Connector registered; cloud notifications and usage metrics enabled' with a green checkmark.

注: 上部バーの通知の数は 30 秒ごとに更新されるため、**概要** ページに表示される数と一時的に異なる場合があります。

4 会議 - 会議の監視と管理

会議 ページでは、ビデオ オペレータとして会議を監視および管理できます。手順については、[ビデオオペレータ向けユーザガイド](#)、[オンラインヘルプ](#)、および [ナレッジベース](#) の記事を参照してください。

5 スペース - スペース管理とブラストダイヤルの設定

会議管理では、スペースの作成とブラストダイヤルの構成をサポートし、ユーザグループとの会議を迅速に開催できます。

ブラストダイヤルを設定するスペースに、事前に決定した参加者のリストを追加できます。いずれかの参加者がスペースにダイヤルインすると、他のすべての参加者が同時にダイヤルアウトされます。

参加者は、DTMF 数字 1 を押して会議に参加し、* を押して通話を拒否することができます。参加者が* を押すと、通話が拒否され、Meeting Managementは、参加者への再ダイヤルを停止します。[辞退 (Decline)] ボタンまたは[拒否 (Reject)] ボタンを押しても通話を拒否できます。

注意: その他の DTMF 数字は無視され、参加者が 1 または * を押すまで、会議管理は参加者に再度ダイヤルし続けます。

5.1 スペース管理

会議管理では、管理者はスペースを作成および管理できます。Meeting Server クラスタ上でスペースを作成、表示、編集、削除したり、ブラストダイヤルを設定したりできます。

ビデオ オペレータは、会議管理を使用してスペースを作成および編集し、それらのスペースにタグを割り当てることもできます。これらのタグはビデオ オペレータに割り当てることができ、特定のスペースと、そのスペースに関連付けられた会議のみにアクセスできるようになります。

5.1.1 スペースを作成する

会議管理でスペースを作成するには、次の手順に従います。

1. [スペース] ページで、[スペースの作成] ボタンをクリックして、[スペースの作成] ポップアップ ウィンドウを起動します。
2. ドロップダウン メニューから Meeting Server クラスタを選択します。
3. スペース名にスペースの一意の名前を入力します。最大文字数は 200 文字です。
4. [スペースタグ (Space tag)] ドロップダウンで [スペースタグ (Space tag)] を選択します。ドロップダウンには、ビデオ オペレータに割り当てられているすべてのタグが一覧表示されます。

注意: スペース タグ ドロップダウンはビデオ オペレータのみが使用でき、管理者は表示できません。

5. テンプレートから適切なスペース テンプレートを選択します。テンプレートが利用できない場合は、Meeting Server から作成する必要があります。
6. **作成** ボタンをクリックします。

作成されたスペースは **スペース ページ**に表示されます。進行中またはアクティブな会議があるスペース

が  アイコンと一緒に表示されます。ここで、アイコン上の数字は会議に参加する参加者の総数を表します。アイコンの上にマウスを置くと、この場合は「**4人の参加者によるアクティブな会議**」というメッセージが表示されます。

5.1.2 スペースを表示する

クラスター内のすべてのスペースを表示できます。検索バーを使用して、探しているスペースを絞り込みます。スペース名をクリックすると、そのスペースの **参加情報** ページに移動します。

注：

- 会議管理で作成されたスペースは、Web アプリには表示されません。
- ウェブアプリで作成されたスペースは表示専用モードとなり、会議管理で編集または削除することはできません。
- スペースの名前が変更されると、元のスペースが古い名前を使用しなくなっても、Meeting Management は古い名前を使用して新しいスペースを作成することを防ぎます。

5.1.3 スペースの編集

会議管理を使用して管理者またはビデオ オペレータによって作成されたスペースのみを編集できます。スペース名は、 編集アイコンを使用して変更できます。

ビデオ オペレータは、自分が作成したスペースや自分がタグ付けされたスペースを編集できます。ただし、管理者はビデオ オペレータが作成したスペースを編集できます。

次の表は、会議管理で作成されたスペースのタグ付きおよびタグなしのビデオ オペレータに対して有効になっているすべてのアクセスを説明しています。

表 2: Meeting Management で作成されたスペースのタグ付きおよびタグなしのビデオオペレータに有効なアクセス

[ユーザ (Users)]	タグ付けされたスペース	タグなしスペース
タグ付きビデオオペレーター	表示、編集、削除へのアクセス	アクセス不可
タグなしビデオオペレーター	アクセス不可	表示、編集、削除へのアクセス

メンバーがスペースにアクセスするために使用する参加情報を変更するには:

1. 編集アイコンをクリックし、[アクセスロールを編集 (Edit access role)]ポップアップウィンドウを起動します。
2. 必要に応じて、パスコード、可視性、ビデオアドレスを変更します。

注:

- 入力する新しいパスコードは整数値で、少なくともスペース テンプレートのダイヤルイン セキュリティ プロファイルで定義された長さ。
 - 入力したビデオアドレスがすでに Meeting Server に存在する場合、管理者は別のビデオアドレスを入力するように求められます。
-

3. [保存 (Save)] ボタンをクリックします。

5.1.4 スペースの削除

管理者は、会議管理で作成されたスペースのみを削除できます。ビデオオペレータは、自分が作成したスペース、または Meeting Management でタグ付けされたスペースのみを削除できます。

管理。スペース名の横にある削除アイコンを使用すると、スペースを削除できます。

5.1.5 参加情報

参加情報 タブには、会議の詳細（可視性、会議 ID、パスコード、ビデオ アドレス）が表示されます。参加情報は、E メールテンプレートとして取得できます。各ロールの横にあるアイコンを使用して参加情報をコピーすることで、その情報を参加者に共有できます。

注:

- 管理者は、ビデオオペレータが作成したスペースを表示、編集、削除できます。
 - 会議管理では、会議サーバにポートが設定されている場合にのみ参加リンクが表示されます。
-

5.1.6 アクセスロールの編集

この情報を編集し、[表示 (Visibility)] ドロップダウンの次のオプションのいずれかを選択すると、スペース表示に関する基本設定を設定できます。

- パブリックディレクトリでは、すべてのスペースメンバーと通話参加者に表示されます
- 通話参加者とスペースメンバー全員
- すべてのスペースメンバー
- スペースオーナーのみ

5.2 ブラストダイヤルの設定

ブラスト ダイヤルは、そのクラスター上の会議を管理するために会議管理が設定されているクラスターに対してのみ構成できます。

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

この会議管理ではこのクラスタ上の会議を管理しないため、このスペースでブラストダイヤルを構成することはできません。これを変更するには、「サーバ」にアクセスしてこのクラスタを編集します。

[[サーバー設定 \(Server settings\)](#)] に移動し、[[クラスタを編集 \(Edit Cluster\)](#)] で、このクラスタの [Meeting Management を使用して会議を管理する (Use Meeting Management to manage meetings)] チェックボックスをオンにします。

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

この会議管理ではブラストダイヤルの監視がオフになっているため、このスペースでブラストダイヤルを構成することはできません。これを変更するには、[[設定](#)] > [[ブラストダイヤルモニタリング](#)] にアクセスします。

[[設定 \(Settings\)](#)] に移動し、[[ブラストダイヤル監視 \(Blast dial monitoring\)](#)] で設定を変更します。

5.2.1 設定

ランディング ページでは次の構成を設定できます。

- **オン / オフ:** ブラストダイヤル構成ランディング ページで、ブラストダイヤル機能をオンまたはオフにすることができます。オンにすると、他の設定オプションが表示されます。
- **再試行:** この設定では、連絡先が最初に通話に接続できなかった場合に再試行を設定できます。
 - **再試行回数:** 通話に接続できなかった場合に、システムが連絡先へのダイヤルアウトを試行する最大回数。
 - **再試行失敗後の時間:** 連絡先へのダイヤルアウトを再試行する前にシステムが待機する最小時間。デフォルトは 180 秒です。
- **ブラストダイヤル参加者を自動参加:** 音声プロンプトは、全体レベルと参加者レベルの両方で、オン/オフに切り替えることができます。オーディオ プロンプトが無効になっている場合、オーディオ プロンプト 「**会議に参加するには 1 を押すか、電話を切るには * を押してください。**」は再生されず、参加者は通話を受け入れるときに DTMF 数字を押して会議に参加する必要はありません。管理者は、会議の特定の参加者の音声プロンプトを無効にすることもできます。

各参加者に用意されている  アイコンを使用します。

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

5.2.2 ダイヤルアウト連絡先の追加

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

連絡先を追加

連絡先を追加するには:

1. **連絡先を追加**をクリックします。 **ダイヤルアウト連絡先の追加** ウィンドウが開きます。
2. 連絡先の名前と住所を入力します。
3. 音声プロンプトオプションを有効または無効にするには、[**参加者接続にプロンプトを要求 (Require prompt to connect participant)**] を使用します。
4. **完了**をクリックします。 連絡先の詳細が連絡先リストに追加されます。 関連するボタンを使用して、リストから連絡先を編集または削除できます。

CSV をアップロード

CSV ファイルをアップロードするには:

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

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

2. CSV ファイルをアップロードするには、[**CSVをアップロード (Upload CSV)**] オプションを使用します。

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

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

注:

- ・ CSV ファイルに無効な文字が含まれている場合、ファイル形式が間違っている場合、最大ファイル サイズを超えている場合、または許可された連絡先数を超える場合は、提案された解決策を示すエラー メッセージが表示されます。 メッセージの指示に従ってエラーを修正し、ファイルをアップロードしてください。
- ・ .csv ファイルで提供される音声プロンプト値は大文字と小文字が区別され、無効な値が入力されたり空白のままになったりすると、デフォルトで無効になります。

6 ユーザー - ユーザーを追加またはユーザー設定を編集する

6.1 ユーザーについて

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。ローカルユーザーは、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ーを認証し、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ー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 経由でユーザーを認証することを推奨します。

注意: LDAP 属性名では大文字と小文字が区別されます。

ユーザーは 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、ユーザーの追加、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。

ローカルユーザーの場合、ロールはユーザープロファイルに割り当てられます。

LDAP ユーザーの場合、ロールは属する LDAP グループに割り当てられます。1 人のユーザー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、このユーザーには管理者ロールが割り当てられます。

6.2 LDAP サーバの詳細を編集する

LDAP サーバの詳細はインストール プロセス中に入力されます。 詳細については、 [インストールおよび構成ガイド](#)を参照してください。

LDAP サーバの詳細を編集したり、証明書を置き換えたりする必要がある場合は、ローカル管理者ユーザとしてログインすることをお勧めします。 これは、詳細に問題があった場合でもログインできるようにするためです。

LDAP サーバの詳細を編集するには:

1. ローカル管理者としてサインインします。
2. 関連する変更を加えます。
要件と詳細な手順については、インストール ガイドを参照してください。
3. **承認** セクションまで下にスクロールし、LDAP バインド ユーザのパスワードを入力します。
4. **変更を保存して、[会議管理を再起動します](#)**。

メモ：今すぐ再起動するか、設定が完了するまで待ってください。

6.3 ビデオオペレータにスペースを割り当てる

会議管理管理者は、ビデオ オペレータを特定のスペースにタグ付けして、それらのスペースに関連付けられた会議へのアクセス権のみを付与できます。 管理者は、ビデオ オペレータを作成または変更するときにタグを追加することで、すべてのスペースと会議へのビデオ オペレータのアクセスを制限できるようになりました。 これにより、会議をより効果的に管理および監視できるようになります。

会議管理管理者は、それぞれ **[会議]** タブまたは **[スペース]** タブを使用して、すべての会議とスペース (タグ付きまたはタグなし) を表示できます。 タグはビデオオペレータにのみ追加できます。

タグは、Meeting Server の管理者のみが coSpace API を使用して作成できます。 詳細については、 [Meeting Server API ガイド](#) を参照してください。 スペースタグは、新規および既存のビデオオペレーターの両方に追加できます。

この機能では、

- 複数のタグを割り当てることで、ビデオ オペレータに複数のスペースと会議へのアクセス権を付与できます。 ビデオ オペレータには最大 10 個のタグを割り当てることができます。
- セッション中にスペース/ビデオ オペレータに追加または変更されたタグは、ビデオ オペレータが次のセッションにサインインした後にのみ反映されます。
- ビデオ オペレータには、管理者によって割り当てられたスペースで開催される会議でタスクを実行する権限があります。
- 管理者とビデオオペレータのユーザ名は一意である必要があります。

- タグが誤って割り当てられるのを避けるために、ローカルユーザーグループと LDAP ユーザーグループの両方に異なるユーザー名を使用することをお勧めします。
- Meeting Management から LDAP ユーザーグループを削除/切断し、再度追加すると、Meeting Management は管理者がその LDAP ユーザーグループに割り当てたタグを保持し続けます。

6.4 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。

6.4.1 LDAP ユーザーグループの追加

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 オペレータにタグを割り当て、タグ付けされた会議のみにアクセスできるようにすることができます。
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、設定が完了するまで待ってください。

6.5 ローカルユーザのセキュリティポリシーを設定する

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。

注意: 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有効になります。

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、Meeting Management は、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するときに、新しいパスワードを作成するように通知します。

パスワードの有効期限が 7 日未満になると、[通知 (Notifications)] に警告メッセージが表示され、ローカルユーザーに対して次回パスワードの変更が必須であることが通知されます。ただし、パスワードの有効期限が 24 時間以内に切れる場合は、エラーメッセージが表示され、パスワードをすぐに更新する必要があります。パスワードの有効期限が 7 日以下に設定されている場合は、エラーメッセージのみが表示され、警告メッセージ機能は無効になります。

通知を受信した後もパスワードが変更されない場合、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するときに、Meeting Management はユーザに新しいパスワードを作成するように通知します。

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. 下にスクロールして **パスワードの有効期限を強制する** を選択し、**パスワードの有効期限を強制する** チェックボックスをオンにします。
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。

- **初回ログイン時にパスワードの変更を強制** して、ユーザに初回ログイン時にパスワードの変更を求めることで、安全なアクセスを確保します。

ユーザが初めてログインするか、管理者がパスワードをリセットすると、Meeting Management は「**今すぐ自分のパスワードを設定してください。**」というメッセージを表示して、ユーザに新しいパスワードを設定するように要求します。ユーザは、意図したパスワードが正しく設定されていることを確認するために、新しいパスワードを 2 回入力する必要があります。

6.6 ローカルユーザを追加する

[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 ページで [ローカル] 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、タグ付けされた会議のみにアクセスできるようにすることができます。

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 [ユーザープロフィール (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。

7 サーバ - サーバを追加または編集する

[[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。

サーバの展開が成功すると、[\[構成されたサーバ\]](#) タブで、正常に構成されたすべてのサーバを表示できます。展開ステータスが失敗または保留中のサーバは、[\[部分的に構成されたサーバ\]](#) タブに表示されます。

[Meeting Managementを無効にするかどうか](#)など、クラスタの詳細を編集したり、削除したりできます。各クラスタでは、[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](#)したり、[クラスタを TMS に関連付けて](#) 会議管理で今後の会議を確認したりすることができます。自分または他のユーザがすでに会議管理を使用してプロビジョニングを設定しているが、変更をコミットしていない場合は、クラスタの通知バナーが表示され、そのリンクをクリックすると、クラスタの [\[プロビジョニング\]](#) ページの [\[確認とコミット\]](#) タブに移動します。

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。

7.1 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. 注: これは、クラスタ設定を編集することで、後で変更できます、詳細については、**[「クラスタの Meeting Management を無効にする」](#)** を参照してください。
-
10. 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。
-
11. **[追加 (Add)]** をクリックします。
12. オプション: **クラスタを編集して**、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 Node を編集するには:
 1. 編集する Call Bridge または Edge Node までスクロールして  をクリックするか、行内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。

7.2 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。

7.2.1 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 アプリ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イスのセットアップ** 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 インストールガイド](#)』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。

7.2.2 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。
- 証明書付きサーバを設定する場合（推奨）、Meeting Server に対して FQDN を指定し、DNS サーバ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:

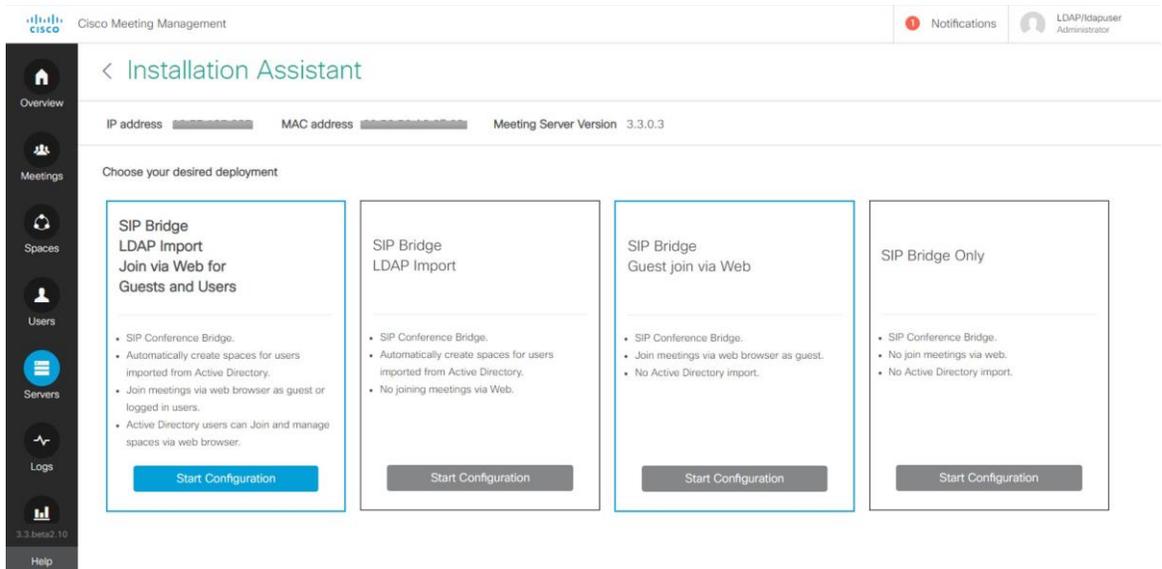
1. [インストールアシスタント (Installation Assistant)] ページで、Meeting Server のサーバアドレスを入力します。
2. ミーティング サーバで設定された **ユーザ名** を入力します。

注: デフォルトでは、ユーザ名として「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、準備ができたなら、[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。

8 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。インストールアシスタントは、認証局によって署名された証明書と自己署名証明書の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を選択に基づいて、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。Meeting Server での証明書の使用方法とその要件の詳細については、『[Cisco Meeting Server、証明書ガイドライン単一統合サーバーの導入ガイド](#)』を参照してください。

8.1 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。

8.1.1 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ーの設定を行います。

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 3: 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ます、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。

8.1.2 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ます、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ます、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 (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:

- 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。

8.2 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。

9 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ります。

1. 以下を構成します。

表 4: ネットワーク設定を構成するために入力するフィールドの説明

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	サーバー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ー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。

9.1 DNS または NTP サーバの削除

1.  をクリックし、DNS/NTP サーバを削除します。

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。

10 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。

表 5: Call Bridge サービスの設定に必要なフィールドの説明

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。

11 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。

12 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 6: LDAP 接続の設定

フィールド名	説明	入力
サーバーアドレス	接続先の LDAP サーバーのネットワークアドレスです。	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。

12.1 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 7: 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。

フィールド名	説明	入力
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: <code>\$cn\$ ミーティングスペース</code>
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: <code>\$cn\$.space</code>
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ー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: <code>\$cn\$.room</code>
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: <code>\$userPrincipalName\$</code>

[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。

13 安全

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ccount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、ユーザー名 を admin にすることはできません。

3. [次へ (Next)] ボタンが有効になります。[次へ (Next)] をクリックし、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:

- 入力されたユーザー名が間違っている場合。 解決方法: 有効なユーザー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。

14 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。

14.1 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。

15 クラスターの会議管理を無効にする

ライセンスとプロビジョニングにのみ会議管理を使用する場合は、個々のクラスターの会議管理を無効にすることができます。これは、CDR 容量を他のツール用に解放したい場合、クラスターにテナントがある場合、またはクラスターで大量の会議がホストされている場合に役立ちます。Meeting Management の容量については、「インストールと設定ガイド」を参照してください。

クラスターの会議管理を無効にするには:

1. サーバーページに移動します
2. クラスターの編集をクリック
3. [会議管理を使用してこのクラスター上の会議を管理する] チェックボックスをオフにします。

会議管理は、クラスター内の Call Bridge 上の CDR 受信者およびイベント クライアントではなくなり、クラスター内の Call Bridge でホストされている会議に関する情報の要求を停止します。

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

16 プロビジョニング

会議管理を使用すると、接続された会議サーバ上でユーザとスペース テンプレートをプロビジョニングできます。

プロビジョニング設定には、サーバ ページからアクセスできます。プロビジョニングを設定するクラスターの場合は、[[プロビジョニングの設定](#)] をクリックして、プロビジョニング設定を構成できるページに移動します。

16.1 スペースとは？

スペースとは、参加者がダイヤルインして音声会議やビデオ会議を行うことができる仮想会議室です。スペースのすべてのメンバーはスペースにアクセスでき、自分のアプリでスペースを確認できます。これは、すべてのメンバーがキーを持ち、必要なときに部屋に入ることができる共有会議室に似ています。スペースのメンバーは他のユーザを会議に招待できます。

スペースの概要とアプリの動作については、「[Web アプリユーザーガイド](#)」および「[表示の「使用方法」ガイド](#)」および「[重要情報](#)に関するドキュメント」を参照してください。

16.2 スペース テンプレートとは何ですか？

スペース テンプレートは、新しいスペースを作成するために使用できる事前構成された設定の組み合わせです。最も基本的な設定は参加者に関係します。

- スペースにはどのような参加者ロールが存在し、各ロールにはどのような権限があるか
たとえば、一部の参加者は、ホストまたはリーダーの役割を持ち、参加者の追加や削除、録画の開始、他の参加者のミュートなどのすべての権限を持ちますが、他の参加者はゲストまたはスタッフの役割を持ち、権限が制限されています。すべてのメンバーに同じ権限が与えられる、1つのロールのみを持つスペースを作成することもできます。
- 参加者ロールをパスワードで区別する必要があるか、それぞれに固有の URI と会議 ID がある必要があるか

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

16.3 プロビジョニング手順

プロビジョニングの設定は、LDAP フィルターの設定、スペース テンプレートとその他のいくつかの設定の定義、および変更のコミットで構成されます。

1. 始める前に、準備をしておきましょう。
2. クラスターを LDAP サーバに接続します。
3. インポートするユーザを定義します。
4. スペースを自動的に作成する。
5. ユーザがスペースを作成できるようにする。
6. 設定を確認して確定する。
7. プロビジョニングを実行するには、LDAP 同期を開始します。

16.4 プロビジョニング - 始める前に

16.4.1 サポートされている LDAP 実装

ミーティング サーバは、次の LDAP 実装をサポートしています。

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

各バージョンの Meeting Server を使用してテストされたバージョンについては、「相互運用性データベース」を参照してください。

注意： Meeting ServerWeb 管理インターフェイス経由で LDAP を設定した場合、Meeting Management 経由のプロビジョニングは機能しません。 Meeting Management でプロビジョニングをセットアップする前に、Web 管理インターフェイスにサインインし、[構成 (Configuration)]、[Active Directory] ページの順に選択し、すべての入力フィールドを空欄にして、[送信 (Submit)] をクリックします。ユーザがロックアウトされないようにするには、Meeting Management でプロビジョニングの設定が完了するまで同期しないでください。

16.4.2 LDAP サーバの詳細

Meeting Server クラスタを接続する LDAP サーバごとに、次のものがが必要です。

- プロトコル (LDAP/LDAPS)
LDAPS を使用することをお勧めします。
- LDAP サーバアドレス
- LDAP サーバのポート番号
デフォルトは、LDAP の場合は 389、LDAPS の場合は 636 です。ポート 636 で LDAPS を使用することをお勧めします。
証明書検証を使用する場合: LDAP サーバ証明書が Meeting Server にアップロードされ、TLS 証明書の検証が有効になっています。
- 証明書検証を使用することをお勧めします。方法については、FAQ 記事の [「LDAP サーバ証明書検証を有効にするにはどうしたらよいですか?」](#) を参照してください。
- 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、Cisco Meeting Server 用に別のバインド ユーザアカウントを作成することをお勧めします。

16.4.3 ユーザのインポートの詳細

インポートするユーザ グループごとに、次のものがが必要です。

- ベース識別名 (DN)
- LDAP 検索フィルター
- サインインユーザ名のマッピング
*LDAP サーバを Meeting Management に接続する際に、**検索属性**と呼ばれるものに相当します。これは、Meeting Server Web アプリのユーザがアプリにログインするために使用するユーザ名として使用する LDAP 属性を定義します。
\$sAMAccountName\$@example.com のような形式である必要があり、属性はユーザごとに一意である必要があります。*
- 表示名のマッピング
アプリユーザの表示名として使用する LDAP 属性を定義します。\$cn\$のような形式にする必要があります。

- 十分な PMP Plus ライセンス

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

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

Cisco Meeting Server でLDAPを使用する方法の詳細については、適切な [Meeting Server 導入ガイド](#)を参照してください。LDAP構成に関するセクションと、LDAPフィールドマッピングに関する詳細情報を含む付録があります。

16.5 プロビジョニング - LDAP サーバ

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

プロビジョニング ページのLDAPサーバタブで、クラスターがLDAPサーバに接続するために使用する詳細を入力できます。

16.5.1 LDAP サーバを追加する方法

クラスターをLDAPサーバに接続するには:

1. 会議管理で、**サーバ** ページに移動し、**プロビジョニングの設定**をクリックします。
2. LDAP **サーバ** タブで、LDAP **サーバの追加**をクリックします。
3. オプション: 自分や他の Meeting Management 管理者に分かりやすいサーバー名を入力します。
4. プロトコルを選択します。

LDAP は暗号化されていないTCP接続用です。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。

5. 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

注意: 会議管理経由で証明書をアップロードすることはできません。LDAPS 接続を完全に安全にするには、Meeting Server で証明書の検証を有効にし、信頼ストアに証明書をアップロードする必要があります。手順については、[「LDAP サーバ証明書の検証を有効にするにはどうすればいいですか?」](#)を参照してください。

6. LDAP サーバーのバインド DN およびパスワードを入力します。

これらは、Meeting Server クラスタを LDAP サーバにバインド (認証) するユーザ アカウントの資格情報です。

7. Meeting Server が 1 回の操作でデータベース全体を検索するのではなく、LDAP ライブラリのページに対応するチャンクで検索結果を受信させる場合は、[LDAP ページの結果制御を使用する (Use LDAP paged results control)] を選択します。

Oracle Internet Directory を使用していない限り、ページングされた結果を使用することをお勧めします。

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

注意: 変更はコミットするまで適用されません。変更をコミットすると、テンプレート設定がすぐに有効になります。LDAP サーバの詳細に対する変更とユーザに影響する変更は、次回 Meeting Server が LDAP サーバと同期されたときに有効になります。

注意: 変更がコミットされる前に Meeting Management を再起動すると、Meeting Management で入力したプロビジョニング設定の変更はすべて失われます。

16.6 プロビジョニング - ユーザのインポート

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

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

16.6.1 ユーザインポートを追加する方法

ユーザのインポートは好きなだけ追加できます。各ユーザのインポートごとに、特定の LDAP サーバからインポートするユーザのサブセットを定義し、ユーザ名と表示名の作成方法を決定し、PMP Plus ライセンスを割り当てるかどうかを決定します。

同じユーザが 1 回のユーザ インポートにのみ含まれるようにすることをお勧めします。PMP Plus ライセンスが 1 つのユーザ インポート経由で割り当てられ、別のユーザ インポート経由では割り当てられていない場合、ユーザが両方のユーザ インポートの LDAP 検索フィルターに一致すると、そのユーザに PMP Plus ライセンスが割り当てられる場合と割り当てられない場合があります。

注意: 同じユーザが2つの異なるユーザ インポートに含まれている場合、会議管理では、どのユーザ インポートにユーザが関連付けられるかを制御できません。つまり、PMP Plus ライセンスをユーザに割り当てるユーザ インポートにユーザが含まれ、ライセンスを割り当てないユーザ インポートにもユーザが含まれた場合、そのユーザにライセンスを割り当てるかどうかを制御することはできません。

インポートするユーザのサブセットを定義するには:

1. サーバ ページに移動し、**プロビジョニングの設定をクリック**します。
2. [ユーザーをインポート (Import users)]タブで、[ユーザーインポートを追加 (Add user import)]をクリックします。
3. ユーザーインポートの**名前**を追加します。

自分や他の管理者がこのユーザーインポートを他のユーザーインポートと簡単に区別できるような名前を選択することをお勧めします。フィールドを空白のままにすると、Meeting Management では以下の設定に基づいて名前が作成されます。

4. ドロップダウンから、このユーザ インポート フィルターを設定する LDAP サーバを選択します。
5. **ベース識別名**を入力します。
6. LDAP **検索フィルター**を入力します。

ベース識別名はディレクトリ検索の開始点です。ミーティング サーバは、このノードと、LDAP ツリー内のその下にあるすべてのノードでLDAP グループを検索します。

このフィルターは、インポートするユーザのサブセットを定義します。フィルター フィールドの構文は、rfc4515 で説明されています。

注: Active Directory を使用している場合は、ユーザ オブジェクトのみを含むフィルターを入力してください。

7. **ログインユーザー名マッピング**を入力します。

これは、Meeting Server Web アプリのユーザがアプリにログインするために使用するユーザ名として使用する LDAP 属性を定義します。次のような形式である必要があります \$sAMAccountName\$@example.com、属性はユーザごとに一意である必要があります。

注意: LDAP 属性名では大文字と小文字が区別されます。

8. **表示名マッピング**を入力します。

これは、会議や各 Web アプリ ユーザのホーム画面で参加者名として使用する LDAP 属性です。\$cn\$ に似た形式である必要があります。

注意: LDAP 属性名では大文字と小文字が区別されます。

9. これらのフィルター設定に基づいてインポートされたユーザに PMP Plus ライセンスを割り当てる場合は、**[インポートされたユーザに Personal Multiparty Plus (PMP+) ライセンスを割り当てる]** チェックボックスをオンにします。

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

注意: 変更はコミットするまで適用されません。変更をコミットすると、テンプレート設定がすぐに有効になります。LDAP サーバの詳細に対する変更とユーザに影響する変更は、次回 Meeting Server が LDAP サーバと同期されたときに有効になります。

注意: 変更がコミットされる前に Meeting Management を再起動すると、Meeting Management で入力したプロビジョニング設定の変更はすべて失われます。

16.7 プロビジョニング - スペースを自動的に作成

プロビジョニングの一環として、ユーザ用のスペースを作成できます。

[**スペースを自動作成 (Automatically create spaces)**] タブでは、定義済みのすべてのスペーステンプレートと各テンプレートを使用して作成されたスペースを持つユーザーのサブセットを表示できます。

また、新しいスペーステンプレートを作成し、スペースを自動構築するために使用するスペーステンプレートを定義できます。これを実行するには、スペース名とビデオアドレスの生成方法の詳細とともに、ユーザーグループをスペーステンプレートにマッピングするルールを設定します。

16.7.1 スペースを自動的に作成するためのルールを追加する

ルールを定義するには:

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

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

4. スペース名マッピングを定義します。

これは、スペース名が生成される方法のルールを定義します。例えば、次のように入力すると \$cn\$ のスペースで、ユーザの共通名が Sally Wood の場合、このユーザのスペースの名前は Sally Wood のスペースになります。

注意: LDAP 属性名では大文字と小文字が区別されます。

5. URI ユーザ部分マッピングを定義します。

これは、スペースの URI を定義するルールです。例えば、次のように入力すると \$sAMAccountName\$ で、ユーザの SAM アカウント名が swood、ユーザのドメインが example.com の場合、ロールの一意的 URI ジェネレーターの定義方法に応じて、URI は swood@example.com、swood.host@example.com、などになります。

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

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

注意: Meeting Server は属性値を小文字に変換します。（スペースを含むその他の文字は削除または変更されません）。そのため、URI ユーザー部分のマッピングによって、すべてのユーザーが使用できる URI が生成されることを確認してください。

6. [スペーステンプレートを選択 (Choose a space template)] で、[テンプレートを新規作成 (Create new template)] を選択するか、既存のテンプレートを選択します。

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

新しいテンプレートの作成 を選択した場合は、**スペース テンプレートの作成** をクリックして手順 7 に進みます。

7. テンプレート名を定義します。

注: この名前は、Cisco Meeting Server Web アプリでもユーザーに表示されます。通常のアプリユーザにとって意味のある名前を選択するようにしてください。

8. スペーステンプレートの説明を記入します。

注: この説明は Web アプリにも表示され、この説明に基づいてスペース テンプレートが選択されます。一般的なアプリユーザが理解しやすい説明を必ず書いてください。

9. 異なる役割をパスコードで区別するか、役割ごとに固有の URI と会議 ID を持つかを決定します。
10. [**ロールを追加 (Add role)**] をクリックします
11. **ロール名**を入力します。

注: アプリ ユーザが名前からこのロールが何であることを推測できるように、わかりやすい名前を付けてください。

12. [**可視性 (Visibility)**] ドロップダウンで、テンプレートの可視範囲を選択します。
13. **一意の URI ジェネレーター** を入力して、この役割を持つ参加者がスペースにアクセスするために使用する URI を Meeting Server が生成する方法のルールを定義します。

URI は、URI ユーザ部分マッピング、URI ジェネレーター、およびドメインに基づいて作成されます。たとえば、\$.host を入力すると、URI ユーザー部分のマッピングが \$givenName\$.space の場合、ドメイン example.com に作成された Sally という名前のユーザのスペースの URI は `sally.space.host@example.com` になります。

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

14. パスコードの最小長を定義します。

この設定を無視すると、会議管理ではシステムのデフォルトを使用することになります。パスコードを要求しない場合は、0 を入力します。

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

注意: すべてのロールに同じ URI と数値 ID を使用することを選択し、ロールが複数ある場合は、パスコードなしに設定できるのは 1 つのロールのみです。複数のロールに対してパスコードなしを設定すると、Meeting Server はそれらの設定を無視し、4 文字のパスコードを提供します。

15. [**次へ (Next)**] をクリックします。
16. このロールを保有する参加者をアクティベータにするには、[**ロールをアクティベータにする (Make role and Activator)**] チェックボックスをオンにします。

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

17. ロールの権限を定義します。

設定にシステム値を使用するには、**[上書き]** チェックボックスをオフのままにします。

新しい設定を定義するには、**[上書き]** チェックボックスをオンにし、次のオプションから必要な値を選択します。

表 8: ロールの権限を定義する際に利用可能なオプション

フィールド名	説明
最大参加者数	会議のアクティブな参加者の最大数を設定します。
録画モード	次のいずれかのオプションを選択します: 無効: 記録は無効になります 手動: ユーザは録画を開始および停止できます 自動: スペース内のすべての会議が記録されます
デフォルトでロックされています	このスペース内のすべての会議をロックされた状態で開始するかどうかを設定します。
パスコードのタイムアウト (秒)	パスコードの入力を求められた場合、ミーティング サーバが参加者にパスコードを入力するのを待機する秒数を設定します。この秒数が過ぎると、パスコードなしのロールに戻ります。タイムアウトを無効にするには、値 0 を入力します。
許可されたビデオ	このスペースでの会議で参加者のビデオを許可するかどうかを設定します。プレゼンテーション ビデオの共有は、音声のみの会議の場合でも常に許可されます。
デフォルトのビデオレイアウト	この会議の参加者に表示されるデフォルトのビデオ レイアウトを設定します。
最後のアクティベータが退出するときの動作	最後のアクティベーターが退席した後の会議の残りの参加者の体験。
役割の変更を許可する	この権限を持つ参加者は役割を変更できます

18. **[次へ (Next)]** をクリックします。
19. このスペーステンプレートに必要なすべてのロールを追加するまで、手順 10 ~ 18 を繰り返します。
20. **ダイヤルアウトのデフォルト** を使用して、会議中にダイヤルアウトする参加者のデフォルトの役割を選択します。
21. **[次へ (Next)]** をクリックします。
22. スペースのデフォルト設定を定義します。
- 設定にシステム値を使用するには、**[上書き]** チェックボックスをオフのままにします。
- 新しい設定を定義するには、**[上書き]** チェックボックスをオンにして、必要な値を選択します。
23. **[完了 (Done)]** をクリックします。

注意: 変更はコミットするまで適用されません。変更をコミットすると、テンプレート設定がすぐに有効になります。LDAP サーバーの詳細に対する変更とユーザーに影響する変更は、次回 Meeting Server が LDAP サーバーと同期されたときに有効になります。

注意: 変更がコミットされる前に Meeting Management を再起動すると、Meeting Management で入力したプロビジョニング設定の変更はすべて失われます。

16.8 プロビジョニング - ユーザーがスペースを作成できるようにする

プロビジョニングの一環として、どの Web アプリユーザーがどのタイプのスペースを作成できるかを決定できます。これは、スペース テンプレートを特定のユーザ インポートに割り当てるか、ユーザ インポート内のグループに割り当てることによって行われます。

[**プロビジョニング (Provisioning)**] ページの [**ユーザーがスペースを作成できるようにする (Allow users to create spaces)**] タブでは、スペーステンプレートを作成し、それらを Web アプリユーザーの特定のグループに割り当てることができます。

16.8.1 制約事項

- スペースを作成したユーザには、会議管理で定義したロールは割り当てられません。スペース作成者 (スペース所有者でもある) は、スペースのデフォルトのコール レッグ プロファイルを受け取ります。
- スペースを作成したユーザは、そのスペースのメンバーになります。
- スペースのすべてのメンバーは、スペースを作成したユーザと同じコール レッグ プロファイルを取得します。
- テンプレートに変更を加えても、すべての変更が既存のスペースに適用されるわけではありません。

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

既存のスペースに変更を加えたい場合は、API 経由で手動で行うことができます。

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

- Web アプリでは、テンプレートが変更されたかどうかはユーザに通知されません。
すでに使用されているテンプレートに大幅な変更を加える場合は、名前または説明を更新することをお勧めします。

- 会議管理では、可能なスペース設定の小さなサブセットが提供されます。
Meeting Management を使用して作成したスペーステンプレートに追加設定を構成する場合は、Meeting Server API を使用できます。『[Cisco Meeting Server API リファレンス ガイド](#)』を参照してください。
- API を使用して作成または編集したテンプレートは Meeting Management に表示されますが、Meeting Management で編集できる設定のサブセットのみが表示されます。
- Meeting Management の一部の設定は、複数の API 設定の組み合わせです。
テンプレートの設定を簡単にするために、いくつかの設定を組み合わせました。
- 会議管理を使用して構成した設定は、コミットすると既存の設定に置き換えられます。
これは、構成した特定の設定にのみ影響します。たとえば、スペースのストリーミング URI を定義した場合、これは会議管理から構成できる設定の影響を受けません。

16.8.2 特定のウェブアプリユーザにスペーステンプレートを割り当てる方法

スペース テンプレートを作成するには:

1. サーバーページに移動し、[プロビジョニングを設定 (Set up provisioning)] をクリックします。
2. プロビジョニングページの [ユーザーがスペースを作成できるようにする (Allow users to create spaces)] タブで、[ルールを追加 (Add Rule)] をクリックします。
3. ユーザのインポートを選択します。
4. オプション: フィルターを追加します。
5. [スペーステンプレートを選択 (Chose space template)] ドロップダウンで、既存のテンプレートを選択するか、[テンプレートを新規作成 (Create new template)] を選択します。
6. 既存のテンプレートを選択した場合は、[完了] をクリックし、次の手順を無視します。
新しいテンプレートを作成することを選択した場合は、[スペース テンプレートの作成] をクリックし、次の手順に進みます。
7. スペース テンプレート名を入力してください。

これは、ユーザが作成するスペースの種類を選択したときに Web アプリに表示されるテンプレート名です。

注意: テンプレート名に特殊文字を使用すると、ステータス メッセージでの表示が異なり、代わりにエスケープ文字が表示されることがあります。名前は Web アプリでは正しく表示されます。

8. **スペーステンプレートの説明**を記入します。

これは、ユーザが作成するスペースの種類を選択したときに Web アプリで表示されるテンプレートの説明です。

9. 異なる役割をパスコードで区別するか、役割ごとに固有の URI と会議 ID を持つかを決定します。

URI は、Web アプリではビデオ アドレスと呼ばれます。

注: ミーティング サーバは、参加者のアクセス方法 (Web リンクまたは URI とパスコードの一意の組み合わせ) によって役割を認識します。 ロールを区別するために必要な場合、またはパスワードの最小長を設定している場合、Meeting Server は、自動生成パスワードを追加します。Web アプリユーザは、スペースを管理する際に、パスコードを追加または変更できます。

10. 「**ロールを追加**」をクリックします。

11. **ロール名**を入力します。

これは、Web アプリのユーザが他のユーザに送信する招待状の詳細を選択するときに表示される参加者ロール名です。

12. [**可視性 (Visibility)**] ドロップダウンで、テンプレートの可視範囲を選択します。

13. **一意の URI ジェネレーター** を入力して、この役割を持つ参加者がスペースにアクセスするために使用する URI を Meeting Server が生成する方法のルールを定義します。

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

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

14. 最小パスコードの長さに関するシステムのデフォルトを上書きするかどうかを決定します。

この設定を無視すると、会議管理ではシステムのデフォルトを使用することになります。

15. システムのデフォルトを上書きすることを選択した場合は、最小パスコードの長さを入力します。

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

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

16. [**次へ (Next)**] をクリックします。

17. この役割を持つ参加者をアクティベーターにしたい場合は、[この役割をアクティベーターにする] チェックボックスをオンにします。

アクティベーターは会議を開始し、ロビーから他の参加者を参加させることができます。

ホストとゲストのスペースを作成する場合は、ホストをアクティベーターにし、ゲストを非アクティベーターにすることをお勧めします。参加者全員に同じ役割を持たせるチームスペースを作成する場合は、参加者全員をアクティベーターにする必要があります。

18. ロールの権限を構成します。

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

新しい設定を定義するには、[上書き] チェックボックスをオンにし、次のオプションから必要な値を選択します。

表 9: ロールの権限を構成する際に利用可能なオプション

フィールド名	説明
最大参加者数	会議のアクティブな参加者の最大数を設定します。
録画モード	のいずれかのオプションを選択します: 無効: 録画は無効になります 手動: ユーザは録画を開始および停止できます 自動: スペース内のすべての会議が録画されます
デフォルトでロックされています	このスペース内のすべての会議をロックされた状態で開始するかどうかを設定します。
パスコードのタイムアウト (秒)	パスコードなしのロールにフォールバックする前に、パスコード入力を求められたときに、参加者がパスコードを入力するまで Meeting Server が待機する時間を設定します。タイムアウトを無効にするには、値 0 を入力します。
許可されたビデオ	このスペースでの会議で参加者のビデオを許可するかどうかを設定します。プレゼンテーション ビデオの共有は、音声のみの会議の場合でも常に許可されます。
デフォルトのビデオレイアウト	この会議の参加者に表示されるデフォルトのビデオ レイアウトを設定します。
最後のアクティベーターが退出するときの動作	最後のアクティベーターが退席した後の会議の残りの参加者の体験。
役割の変更を許可する	この権限を持つ参加者は役割を変更できます

19. [次へ (Next)] をクリックします。
20. このスペース テンプレートに必要なすべてのロールを追加するまで、ロールの追加を繰り返します。
21. [デフォルトのダイヤルアウト (Default for dial out)] を使用すると、会議中に参加者にダイヤルアウトするデフォルトロールを選択できます。

22. [次へ (Next)] をクリックします。

23. このテンプレートから作成されるスペースの設定を定義します。

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

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

注: ここに記載されている以外の設定を定義する場合は、Meeting Server API を介してテンプレートを調整できます。詳細については、「Cisco Meeting Server API リファレンスガイド」を参照してください。

24. [完了 (Done)] をクリックします。

注意: 変更はコミットするまで適用されません。変更をコミットすると、テンプレート設定がすぐに有効になります。LDAP サーバの詳細に対する変更とユーザに影響する変更は、次回 Meeting Server が LDAP サーバと同期されたときに有効になります。

注意: 変更がコミットされる前に Meeting Management を再起動すると、Meeting Management で入力したプロビジョニング設定の変更はすべて失われます。

16.9 プロビジョニング - レビューとコミット

プロビジョニングの **確認とコミット** タブにプロビジョニング設定が表示されます。

まだコミットされていない変更を行った場合、タブには会議管理のローカル設定が表示されます。

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

注意: 変更はコミットするまで適用されません。変更をコミットすると、テンプレート設定がすぐに有効になります。LDAP サーバの詳細に対する変更とユーザに影響する変更は、次回 Meeting Server が LDAP サーバと同期されたときに有効になります。

注意: 「現時点では変更をコミットできませんでした」というエラーメッセージが表示される場合は、一部の変更がコミットされている可能性があります。会議管理のすべてのプロビジョニング設定が正しいことを確認して、もう一度試してください。

- **変更を破棄する:** 変更を破棄すると、Meeting Management は Meeting Server から最後にコミットされた設定を取得し、タブを更新して表示します。

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

16.10 プロビジョニング - LDAP 同期

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

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

プロビジョニング ページの LDAP 同期 タブでは、定期的な同期スケジュールを設定したり、手動で同期をトリガーしたり、最近の同期のステータスを確認したりできます。

スケジュールされた同期を構成するには:

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

注: 同期スケジュールは会議管理で設定され、会議管理はスケジュールされた時間に各同期をトリガーします。同期が実行される Call Bridge を削除すると、スケジュールされた同期は実行されなくなります。

LDAP 同期を手動でトリガーするには:

1. 表の下にある **[今すぐ同期を実行:]** ドロップダウンから、LDAP 同期を実行する Call Bridge を選択します。

アクティブな会議の中断を最小限に抑えるには、他の Call Bridge よりも少ない会議または重要度の低い会議をホストする Call Bridge を選択します。

2. 「**今すぐ同期を実行**」をクリックします。

注: ミーティング サーバは、接続されているすべての LDAP サーバと同期します。

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

17 ログ - ログ、クラッシュレポート、 詳細なトレース

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

注: ほとんどのタイムスタンプは UTC です。例外は、会議管理内で表示するとブラウザのタイムゾーンで表示されるイベント ログです。

注: 特定の会議のイベント ログは、会議終了後最大 1 週間、**会議** ページの会議詳細ビューで参照できます。詳細については、「ビデオオペレータ向けユーザーガイド」を参照してください。イベント ログ情報も会議管理システム ログに含まれていますが、メッセージが属する会議別に分類されて表示されることはありません。

17.1 会議管理ログ

ログ バンドル、システム ログ、監査ログを含むすべての会議管理ログは、**CMM ログ** タブからアクセスできます。

17.1.1 ログバンドル

ログページの [CMMログ (CMM logs)] タブで、[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 のログバンドルをダウンロードできます。ダウンロードしたログには、シスコ サポートがトラブルシューティングに必要とする情報が含まれています。

- 最新のシステムおよび監査ログ
- 設定の詳細 (パスワードを含まないように編集されています)
- バージョン番号
- クラッシュレポートのリスト
- 90 日間のライセンスレポート
- ライセンスの予約の試行または再試行回数

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

注意: メッセージの多くは Meeting Server Call Bridges から受信した情報に基づいていますが、[CMM ログ (CMM logs)] タブでアクセスするすべてのログは Meeting Management 用です。

17.1.2 システムログサーバ

システム ログ サーバ タブでは、Meeting Management がシステム ログを送信するサーバを追加できます。システムログには、Meeting Management で何が起こったかに関するすべての情報が含まれています。

管理。最新のシステム ログはログ バンドルに含まれます。Meeting Management のイベントとアクティビティを追跡するために、最大 5 つのシステムログサーバを構成できます。

最新のログのみがローカルに保存されるため、サポートで必要になった場合に備えて完全な履歴を保存するために外部の syslog サーバを設定することを強くお勧めします。

注: 会議管理に関する問題をトラブルシューティングする場合は、Meeting Server のログも確認する必要がある場合があります。すべての Meeting Management インスタンスとすべての Meeting Server に外部 syslog サーバーを使用することを強くお勧めします。

システムログサーバを構成するには:

1. [ログサーバを追加 (Add log server)] ボタンをクリックします
2. サーバアドレス と ポートを入力してください
3. プロトコルを選択
4. [証明書をアップロード (Upload certificate)] ボタンを使用して証明書をアップロードします
5. **追加** ボタンをクリックして、ログサーバの設定を完了します。

17.1.3 監査ログサーバ

[**監視ログサーバ (Audit log server)**] タブで、Meeting Management が監査ログを送信するサーバを追加します。監査ログには、Meeting Management ユーザーが実行したアクションに関する情報が含まれます。たとえば、設定の変更やログインの詳細などです。

組織内で監査ログが必要な場合は、監査ログ用の外部 syslog サーバーを設定することをお勧めします。Meeting Management のイベントとアクティビティを追跡するために、最大 5 つのシステムログサーバを構成できます。

監査ログサーバを構成するには:

1. [ログサーバを追加 (Add log server)] ボタンをクリックします
2. サーバアドレス と ポートを入力してください
3. [プロトコル (Protocol)] を選択します
4. [証明書をアップロード (Upload certificate)] ボタンを使用して証明書をアップロードします
5. **追加** ボタンをクリックして、ログサーバの設定を完了します。

17.1.4 クラッシュレポート

会議管理のクラッシュレポートは、CMM ログ ページの **クラッシュレポート** タブからアクセスできます。

17.1.5 詳細なトレース

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

詳細なトレースは次の場合に利用できます：

- ミーティングサーバ API
- ミーティングサーバ CDR
- ミーティングサーバイベント
- TMS API
- ミーティング サーバ クラウド コネクタ API

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

17.1.6 90 日間のライセンスレポート

90 日間のライセンス レポートでは、顧客が Webex 会議に参加しなくても、サポート チームは顧客のライセンス使用状況を把握できます。サポート チームは、90 日間のライセンス レポートを解析し、ライセンスに必要な変更があれば顧客に通知できます。

17.2 Meeting Server ログ

Meeting Management 管理者は、ログバンドルをダウンロードし、Meeting Server と Edge ノードの詳細なログを追跡できます。これを実行するには、**ログページ**の [CMSログ (CMS logs)] タブを使用します。

17.2.1 ログバンドル

Meeting Management を使用すると、管理者は、Call Bridge や Edge ノードなどのサーバーを追加した後に、それらのログを収集できます。

会議サーバのログを収集する手順は次のとおりです。

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

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

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

17.2.2 詳細なトレース

会議管理を使用すると、管理者は SIP、アクティブ コントロール、アクティブ スピーカー、ICE などのさまざまな会議サーバ モジュールのログを追跡できます。

詳細なトレースを有効にする手順は次のとおりです。

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

注意: トレース デバッグを有効にすると、選択したサーバに負荷がかかります。詳細なトレースは必要な場合にのみ有効にしてください。

ログをトレースする頻度も設定できます。たとえば、10 分または 60 分ごとにログをトレースするように設定したり、hh:mm 形式で任意の間隔を設定したりできます。

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

すべての Meeting Server コンポーネントの詳細なトレースを無効にするには、**[すべて無効にする]** をクリックします。

17.3 ログサーバを追加または編集する

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 経路で 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 経路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一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。

オプション: 組織で必要な場合、監査ログ用の syslog サーバを追加します。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 (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。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

18 ライセンス

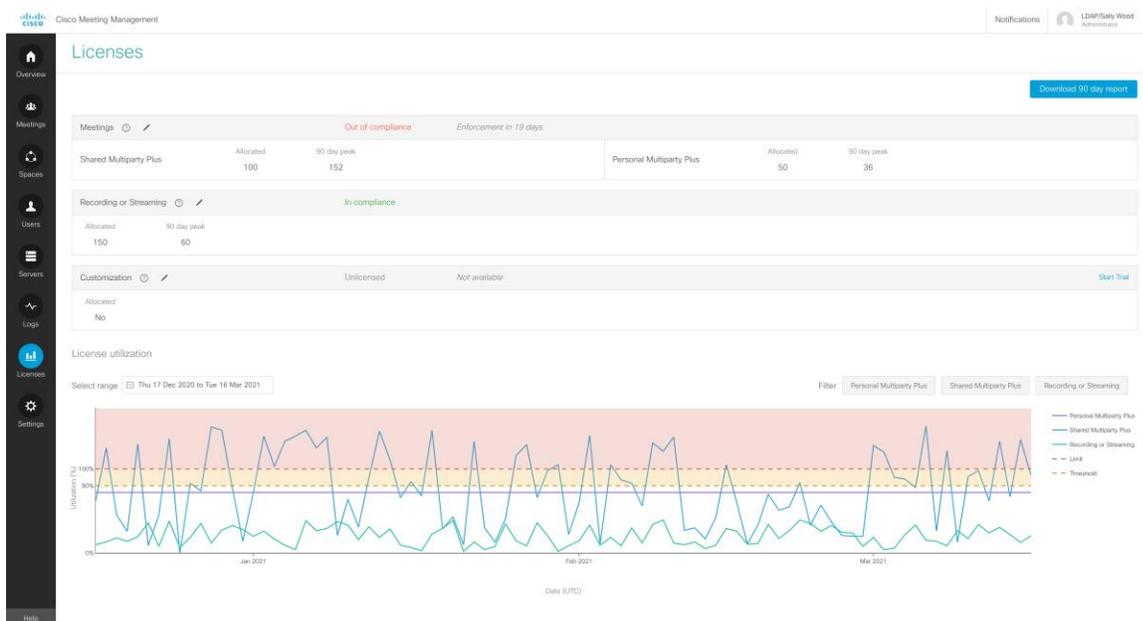
ライセンス ページには次の内容が表示されます。

- 各機能のライセンス ステータスを表示するボックス。
ステータスの定義については、[「ライセンスのステータスと適用」](#)を参照してください。
- ライセンスの使用状況の経時的グラフ。日付範囲を指定したり、ライセンスの種類に基づいてグラフをフィルタリングしたりできます。

注: 日付範囲が 1 日の場合、会議管理では 5 分ごとに 1 つのデータ ポイントが表示されます。日付範囲が長い場合は、ピーク値を示すデータ ポイントが 1 日あたり 1 つあります。

会議管理では、ローカル ライセンス ファイル (従来のライセンス モード) のサポートが廃止され、ライセンス予約が導入されました。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。詳細については、[「ライセンス」](#)項を参照してください。

以下のスクリーンショットは、Smart Licensing モードのライセンスページを示しています。



各機能について、ボックスには次の情報が表示されます。

- **ボックスヘッダー:** 機能の名前、ライセンスの状況、適用警告（該当する場合）。トライアルをまだ使用していない場合は、右側に [トライアルを開始] ボタンも表示されます。詳細については、[ライセンスのステータスと適用のセクション](#) を参照してください。
- **予約済み:** SLR ライセンス予約モードの場合に Cisco SSM で予約されているライセンスの数。
- **配置済み:** 利用可能なライセンス数
Smart Licensing の場合、番号を入力すると、*Meeting Management* が *Cisco Smart Software Manager* で確認します。
- **90 日間のピーク:** 過去 90 日間に使用されたライセンスの最大数

概要よりも詳しい情報を知りたい場合は、90 日間のレポートをダウンロードできます。

会議管理では、license-data.zip という名前の zip ファイルが提供され、このファイルには次のファイルが含まれています。

- **host-reported.csv**
このファイルには、*Meeting Management* がクラスタ内の個別の Call Bridge から受信した生データが含まれています。各行には次の内容が表示されます。
 - 特定のコールブリッジのホスト ID
 - タイムスタンプ (UTC)
 - ライセンスの種類ごとに、使用されているライセンスの数。
- **クラスタービン.csv**
このファイルには、会議管理によって計算された、5 分間隔ごとのクラスター全体のライセンス使用量が含まれています。各行には次の内容が表示されます。
 - 5 分間隔の開始時刻のタイムスタンプ (UTC)
 - ライセンス タイプごとに、すべての Call Bridge で使用されるライセンスの概要。
- **daily-peaks.csv**
このファイルには、会議管理によって計算された毎日のピークが含まれています。各行には次の内容が表示されます。
 - 日付 (UTC)
 - 各ライセンスの種類について、3 点平均平滑化後のその日に使用されたライセンスのピーク数

19 ライセンス状況と適用

ログインしている Meeting Management のインスタンスでライセンスが有効になっている場合は、Cisco Meeting Server 展開のライセンス ステータスが最新の状態に保たれます。

ライセンスは機能別に分類されます。

- **会議:** これは、Call Bridge とユーザ ライセンスのアクティベーションで構成されます。適切なライセンスをお持ちの場合は、Call Bridge を使用できます。

Smart Licensing の場合: アクティベーションキーは不要です。仮想アカウントで利用可能な PMP Plus または SMP Plus ライセンスがある場合は、接続されているすべての Call Bridge を使用できます。

- **録画またはストリーミング:** これらのライセンスでは、録画またはストリーミングが許可されます。

Smart Licensing の場合、レコーディングまたはストリーミングのライセンスが利用可能な場合に、レコーディングとストリーミングにライセンスが付与されます。

- **カスタマイズ:** このライセンスではカスタマイズされたレイアウトが許可されます。

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

会議のライセンス ステータス レベルは次のとおりです。

- **準拠中:** インストールされているライセンスの使用率は 80% 以下です。
- **ライセンスなし:** ライセンスが割り当てられていません。
- **80% を超えるしきい値:** ライセンス契約にはまだ準拠していますが、インストールされているライセンスの 80% 以上を使用しています。
- **ライセンスが不足しています:** 過去 90 日間のうち 1 ~ 14 日間に、使用可能なライセンス数を超えるライセンスを使用しました。

予期しないピークが発生する可能性があるため、一時的な超過使用を許可しています。ただし、使用状況データを評価し、追加のライセンスを購入する必要があるかどうかを検討することをお勧めします。

- **コンプライアンス違反:** 過去 90 日間のうち 15 日以上、使用可能なライセンス数を超えてライセンスを使用しています。

ライセンス契約に違反しています。ニーズについて話し合い、ライセンスをさらに購入するには、Cisco パートナーまたはアカウント チームに問い合わせてください。

録画またはストリーミングのライセンス ステータス レベルは次のとおりです。

- **ライセンスなし:** 録画またはストリーミング用のライセンスが割り当てられていません。
- **準拠中:** インストールされているライセンスの使用率は 80% 以下です。
- **80% を超えるしきい値:** ライセンス契約にはまだ準拠していますが、インストールされているライセンスの 80% 以上を使用しています。
- **ライセンスが不足しています:** 過去 90 日間のうち 1 ~ 14 日間に、使用可能なライセンス数を超えるライセンスを使用しました。

予期しないピークが発生する可能性があるため、一時的な超過使用を許可しています。ただし、使用状況データを評価し、追加のライセンスを購入する必要があるかどうかを検討することをお勧めします。

- **コンプライアンス違反:** 過去 90 日間のうち 15 日以上、使用可能なライセンス数を超えてライセンスを使用しています。

ライセンス契約に違反しています。ニーズについて話し合い、ライセンスをさらに購入するには、Cisco パートナーまたはアカウント チームに問い合わせてください。

カスタマイズのライセンス ステータス レベルは次のとおりです。

- **ライセンス済み:** カスタマイズ ライセンスがあります。
- **ライセンスなし:** カスタマイズ ライセンスがありません。
- **コンプライアンス違反:** 会議管理でカスタマイズが有効になっていますが、カスタマイズ ライセンスがありません。

これは Smart Licensing の場合にのみ表示されます。ライセンス契約に違反していません。割り当てを No に変更するか、Cisco パートナーまたはアカウントチームに連絡して、ニーズについて話し合い、ライセンスを購入します。

注: Meeting Server API は、Meeting Server の機能コンポーネント、各コンポーネントのライセンス ステータスと有効期限を含むライセンス ステータスを取得するためにも使用できます。API オブジェクト/**clusterLicensing** は、Meeting Server クラスターのライセンス ステータスと有効期限 (該当する場合) を返します。詳細については、[Cisco Meeting Server API リファレンス ガイド](#)を参照してください。

19.1 利用可能なトライアル

トライアルには 3 つの種類があります。

- **会議トライアル:** このトライアルでは、録画やストリーミング、カスタマイズなど、すべての機能のライセンスが 90 日間無制限に付与されます。

Meetings のライセンスを取得している場合、または以前に試用版を使用したことがある場合は、Meetings の試用版は提供されません。

- **録画またはストリーミングのトライアル:** このトライアルでは、90 日間録画とストリーミングを無制限にご利用いただけます。

すでに録画またはストリーミングのライセンスをお持ちの場合、または以前に試用版を使用したことがある場合は、録画またはストリーミングの試用版は提供されません。

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

カスタマイズ ライセンスをすでにお持ちの場合、または以前に試用版を使用したことがある場合は、カスタマイズ 試用版は提供されません。

注: 会議管理の展開ごとに各タイプの試用版が 1 つ提供され、接続されているすべてのクラスター間で共有されます。クラスターを新しい Meeting Management 導入に移動しても新しいトライアルを取得できません。これは、接続されているクラスターのいずれかが、以前に同じタイプのトライアル中に、Meeting Management インスタンスに以前接続されていた場合に、Meeting Management がトライアルを提供しないからです。また、最初のトライアル中に接続されなかった新しいクラスターを追加しても、新しいトライアルを取得することはできません。

注意: 試用期間が終了する前にライセンスを追加しないと、コンプライアンス違反となり、強制措置がアクティブになります。詳細は下の表をご覧ください。

19.2 試用中および試用後のライセンスステータス

トライアルの種類	トライアルに含まれるもの	試用中のライセンスステータス	試用後のライセンスステータス
ミーティング	会議、録画、ストリーミング、カスタマイズされたレイアウトを 90 日間無制限にご利用いただけます	準拠	<p>PMP Plus または SMP Plus ライセンスをお持ちの場合は、会議は準拠した状態になります。</p> <p>PMP Plus または SMP Plus ライセンスをお持ちでない場合は、ライセンスが付与されず、ライセンスを追加するまで強制がアクティブになります。</p> <p>録画またはストリーミングのライセンスをお持ちの場合は、録画またはストリーミングは準拠したものにになります。</p> <p>レコーディングまたはストリーミングのライセンスをお持ちでない場合は、レコーディングまたはストリーミングにライセンスは付与されず、利用できません。</p> <p>カスタマイズ ライセンスをお持ちの場合は、カスタマイズがライセンスされます。</p> <p>カスタマイズライセンスをお持ちでない場合は、カスタマイズにライセンスは付与されず、利用できません。</p>
録画またはストリーミング	90 日間無制限の録画とストリーミング	準拠中	<p>録画またはストリーミングのライセンスをお持ちの場合は、録画またはストリーミングは準拠したものにになります。</p> <p>レコーディングまたはストリーミングのライセンスをお持ちでない場合は、ライセンスは付与されず、利用できません。</p>
カスタマイズ	90 日間のカスタマイズされたレイアウト	ライセンス付与済み	<p>カスタマイズ ライセンスをお持ちの場合は、カスタマイズがライセンスされます。</p> <p>カスタマイズ ライセンスがない場合は、ライセンスなしのステータスとなり、利用できません。</p>

19.3 執行と警告

ライセンスページで、次回の適用に関するライセンス状況と警告の両方が表示されます。

会議に関する警告と適用:

- **<number> 日以内に適用:** これは、Alarm 1 です。コンプライアンス違反であり、Meeting Management が適用までのカウントダウンを行っています。
- **適用中、<number> 日以内に適用を強化:** これは、Alarm 2 です。つまり、適用が有効であることを示します。ミーティング参加者は、各会議の開始時に警告を見たり聞いたりします。
- **高レベルで適用中:** これは、Alarm 3 です。つまり、最高レベルの適用がアクティブであることを示します。会議の参加者には各会議の開始時に警告が聞こえ、会議中は画面上に大きな文字で警告が表示されます。

録画またはストリーミングに関する警告と強制:

- **あと <number> 日で利用可能:** Meeting Management の適用までのカウントダウンが開始されます。
- **利用できません:** 会議を録画またはストリーミングすることはできません。

カスタマイズに関する警告と強制:

- **あと <number> 日で利用可能:** Meeting Management の適用までのカウントダウンが開始されます。
- **利用できません:** カスタマイズされたレイアウトは使用できません。

20 ブラストダイヤル監視

ブラストダイヤル モニタリングを使用すると、スペースへのアクセス時に複数のダイヤルアウトを回避するために、会議管理にプライマリまたはセカンダリの役割を割り当てることができます。これは、複数の会議管理がスペース内のブラストダイヤルを監視している場合に発生する可能性があります。

- **プライマリ** - プライマリとして設定する会議管理は 1 つだけにする必要があります。これは、ほとんどの状況でブラストダイヤルをトリガーする会議管理です。
- **セカンダリ** - この会議管理は、一定時間後にブラストダイヤルをトリガーしようとしません。これは、他の会議管理がダイヤルアウトを開始していない場合にのみ実行されます。時間遅延は、「セカンダリを選択した場合の遅延 (秒)」フィールドで設定できます。
- **オフ** - この会議管理では、ブラストダイヤルはトリガーされません。

21 設定 - 会議管理を構成する

設定 ページでは、次のような会議管理の設定を構成できます。

- [会議管理のネットワーク設定](#)
- 会議管理が着信 HTTPS 接続で提示する [証明書](#)。
- 会議管理がコールブリッジから情報を受信する [CDR 受信者アドレス](#)
- [TMS](#) 設定
- [NTP](#) 設定
- [ログインメッセージ](#)
- [高度なセキュリティ](#)

ここでは、会議管理のバックアップ、復元、アップグレード、[再起動](#) も行うことができます。

21.1 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。

21.2 証明書のアップロード

会議管理証明書の有効期限が切れた場合は、新しい証明書に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期限切れの証明書を新しい証明書に置き換えます。
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。

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。

21.3 CDR 受信者アドレスを編集する

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。

21.4 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、『インストールおよび構成ガイド』の「開始する前に」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、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. 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。

注意: クラスタを TMS に関連付けるまでは、TMS から情報は受信されません。

21.4.1 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。

21.4.2 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。

21.5 NTP ステータスの確認、または NTP サーバの追加

Meeting Management が Meeting Server の Call Bridge と常に同期されていることが重要です。そのため、Meeting Management は Meeting Server の展開と同じ NTP サーバー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。

21.6 ライセンス

[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。

21.6.1 スマート ライセンスを有効にする方法

スマートライセンシングの有効化

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 (Allow export- controlled functionality on the products registered with this token)]** 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、接続されているミーティングサーバ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。

21.6.2 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 から登録を解除できます。

21.6.3 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。

- **ユニバーサルバリエーション:** 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エーションに、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。

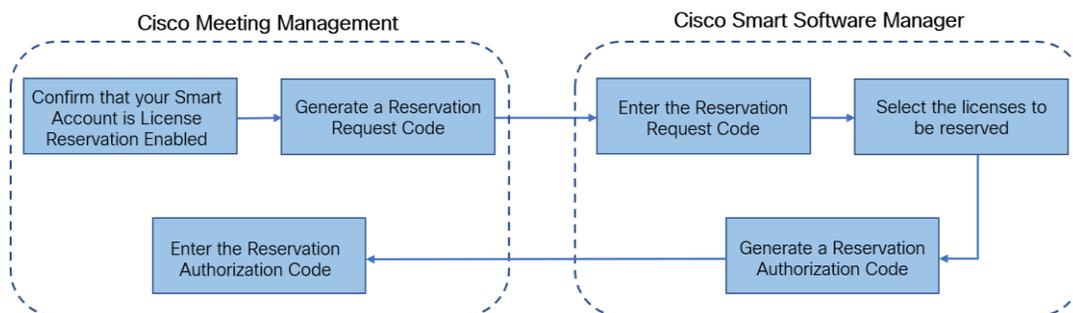
- [SLR/PLR ライセンスの予約](#)
- [予約済みライセンスを更新する](#)
- [予約済みライセンスを返却する](#)

21.6.3.1 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 3: 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スング (Smart Software Licensing)] ページで、[スマートソフトウェアライセンスング (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。

注: バージョン 3.11 からは、Cisco Smart Licensing 輸出コンプライアンス ポリシーに従って、カテゴリ C およびカテゴリ D に該当する国向けに、通話暗号化用の単一ライセンス LIC-CMS-ENCRYPT-S を予約できるようになりました。このライセンスでは、必要な場合にのみ通話の暗号化が許可されます。会議管理は、通話の暗号化を有効にするためにアクティブな LIC-CMS-ENCRYPT-S ライセンスが存在するかどうかを確認します。暗号化を有効にするには、特定のライセンスを予約しながら、単一の **CMS 暗号化** ライセンスを選択します。最初に暗号化ライセンスを持たない仮想アカウントに会議管理を登録した場合、変更を有効にするには、通話暗号化ライセンスを追加した後に再登録する必要があります。

- 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スング (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スング状況 (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**。

21.6.3.2 予約済みライセンスの更新

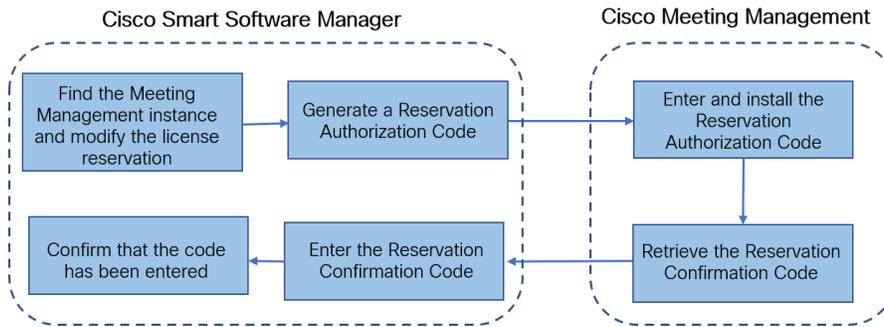
組織のニーズの変化に合わせて、特定のライセンスを更新するか、予約ライセンス数を変更できます。たとえば、現在のライセンス要件が 5 で、さらに 5 ライセンスを追加したい場合、ライセンス数として 10 を選択する必要があり、新しい値が以前の値を上書きします。

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 4: 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. 会議管理の **スマート ソフトウェア ライセンス** ページに戻り、**コードが入力されました** ボタンをクリックして、予約認証コードのインストール後に表示されたアラートを閉じます。

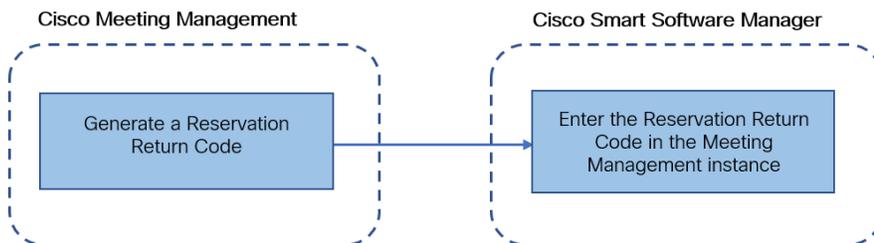
21.6.3.3 予約済みライセンスの返却

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 5: 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。ライセンスページで、[登録 (Registration)] 状況が、[登録解除 (Deregistered)] に変更されます。

21.6.3.4 スマートライセンスへの移行時に考慮すべき事項

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ます、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。

21.7 Cisco Meeting Server クラウド コネクタ

注意: 会議管理からサービスを無効にすると、会議管理から Webex クラウドへの情報の送信のみが停止されます。 Meeting Management を完全に登録解除し、サービスを無効にするには、WebexControl Hub に移動します。

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

このサービスでは次のことが可能です。

- Control Hub インターフェースで会議管理インスタンスに関する情報を確認します。
- 電子メールと Webex Teams アラートを設定すると、会議管理のエラーや警告について通知を受け取ることができます。

このサービスは、Webex Cloud にメトリックも送信します。

21.7.1 Cisco Meeting Server クラウド コネクタのステータス

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

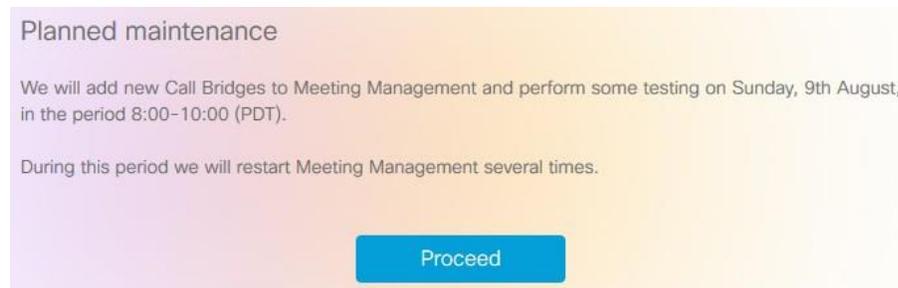
- 登録: この Meeting Management インスタンスが Webex Cloud に登録されているかどうかを示します。
- Webex Cloud サービスのアドレス: これは、Cisco Meeting Server Cloud Connector が機能するために Meeting Management がアクセスする必要があるアドレスを示します。

詳しい手順と詳細については、[クラウドコネクタのオンラインヘルプ](#)を参照してください。

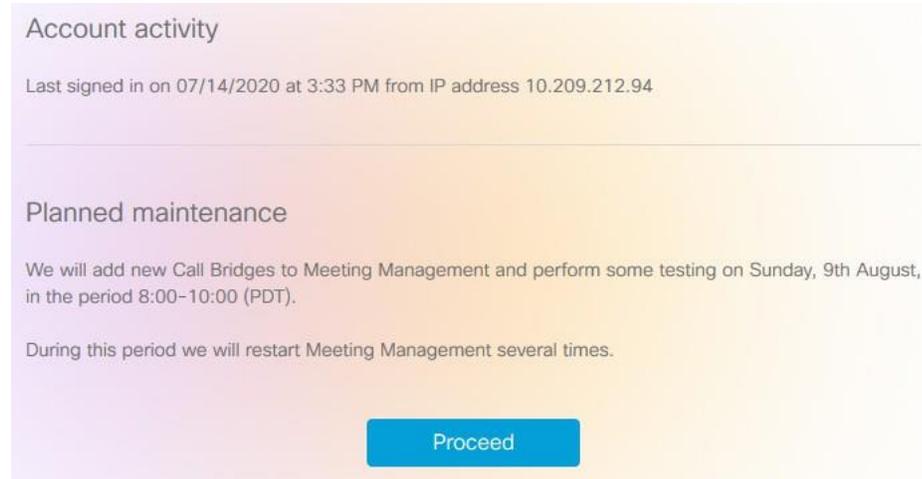
21.8 ユーザがログインしたときにメッセージを表示する

サインインページの前または後に、ユーザ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。

21.9 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完了します。

21.9.1 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。ユーザがトークンを使い切った後にログインしようとする、「ログイン試行回数が多すぎます」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。

管理者がレート制限を設定していない場合、Meeting Management ではデフォルトで、LDAP ユーザとローカルユーザの両方に対して最大 20 回のサインイン試行の失敗が許可され、それを超えると 15 分のロックアウト期間が適用されます。ユーザーが、再試行回数の制限を超えてサインインをしようとする、「ログイン試行回数が多すぎます。」というメッセージが表示されます。しばらくしてからもう一度お試しください。ローカルユーザーがロックされた場合に、管理者がアカウントを手動でロック解除するには、

 ボタンをクリックします。これは、ローカルユーザーリストの各ローカルユーザーの横にあります ([**ユーザー (Users)**] > [**ローカル (Local)**]) の順に選択)。ただし、リストには、ローカルユーザがロックアウトされているかどうかのステータスは示されません。LDAP ユーザの場合、デフォルトの 15 分間のロックアウトタイマーが期限切れになるまで、ロックアウトをバイパスすることはできません。

21.9.2 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。

21.9.3 Meeting Server のパスワードをリセット

以前のパスワードを検証せずに、Meeting Server への認証に Meeting Management が使用する Meeting Server パスワードをリセットできます。ユーザがパスワードを忘れた場合、以前のパスワードを検証することなく、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)。

注: 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。この接続には API アカウントの使用はお勧めしません。

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。

21.9.4 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、ミーティング管理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ー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。

21.10 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

これにはパズ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
 - パズフレーズ辞書

21.10.1 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](#) が必要な場合は、すべての設定を有効にするために今すぐ再起動してください。
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。

21.10.2 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
これにはパスワードジェネレータ、パスワード検証、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ィールを更新します。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。
- バックアップを作成した後、管理者とビデオ 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 オペレータは復元されたパスワードを使用して会議管理にログインでき、管理者は変更された資格情報を使用してログインできるようになります。

21.11 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。したがって、署名されていないイメージから署名されたイメージにアップグレードする場合は、手動検証が依然として推奨されます。つまり、

3.6 から 3.7 にアップグレードする場合、または以前のバージョンにダウングレードする場合でも、ハッシュを手動で検証することをお勧めします。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。

21.12 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。

付録 A セキュリティ強化

セキュリティ強化 VMware 製品を安全に導入および運用する方法については、『VMware セキュリティ強化ガイド』を参照してください。

アクセシビリティ通知

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

Cisco 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。

B アクセシビリティサポート機能

B.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。

- **Tab**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。

B.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」と表示し、スペース名を入力するように指示します。

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。

© 2025 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。シスコの商標の一覧については、www.cisco.com/jp/go/trademarks をご覧ください。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)