# Cisco Meeting Server

## インストール アシスタント 2.9

### インストールと設定

2020 年 5 月 27 日

# 目次


変更履歴 4

導入 5

前提条件 6
- クライアントコンピュータの要件 6
- Cisco Meeting Server の要件 7
- 外部依存関係 7

インストール 8
- ソフトウェアのインストール 8

ソフトウェアの実行 9
- ユーティリティの実行 9
- ユーティリティの終了 9
- ファイルの永続的な保管 9

インストール アシスタントを使用した Meeting Server の設定 10
- ステージング 10
  - 新規の Meeting Server インスタンス 10
  - 既存の Meeting Server インスタンス 10
  - ライセンス ファイル 11
  - Meeting Server DNS エントリ 11
- サーバの設定 11
- 設定のプッシュ後 13
- ツールを複数回実行 14
- トラブルシューティング 14
- インストール アシスタントの終了 14
- ソフトウェアのアンインストール 14

パネル リファレンス 15
- 証明書 15
  - CA 署名済み証明書 15
  - 既存の証明書とキーの使用 17
  - 自己署名証明書 19
- ライセンス 19
  - ライセンスのアップロード 19

ネットワーク 20
DNS または NTP サーバの削除 21
コール ブリッジ 21
会議ユーザ 21
LDAP 検索およびユーザ マッピングのカスタマイズ 23
Web ブリッジ 25
セキュリティ 25
プッシュの設定 26
Cisco 法律情報 28
Cisco 商標 29
2 用語集 30

# 変更履歴

**表 1：変更履歴**

| 日付 | 変更内容 | 理由 |
| --- | --- | --- |
| 2020 年 5 月 27 日 | ソフトウェアのリリース | バージョン 2.9 |

# はじめに

インストール アシスタントは、デモンストレーション、ラボ環境、または基本的なインストールの開始点として Cisco Meeting Server の簡単なインストールの作成を簡略化するためのツールです。このツールでは、『Cisco Meeting Server Single Server Simplified Deployment guide（Cisco Meeting Server シングル サーバ シンプル導入ガイド）』に記載されている導入のベスト プラクティスに基づいて、Meeting Server を設定します。このツールは、ブラウザ インターフェイスを使用して設定に関する情報を収集し、その設定をサーバにプッシュするスタンドアロン ツールであり、API、SFTP、または Meeting Server のコマンドライン インターフェイスにアクセスするためのユーティリティを使用する必要はありません。

インストール アシスタントは、コールを発信および受信できる SIP MCU として Meeting Server を設定します。必要に応じて、Web ベースの Cisco ミーティング アプリケーションを有効にできます。このアプリでは、ユーザはブラウザのみを使用して会議に参加できます。

---

**注**：Cisco ミーティング アプリケーションの場合、ゲスト アクセスのみを有効にすることも、オプションで、インポートした LDAP ユーザも有効にすることもできます。

---

インストール アシスタントは、空で未設定の Meeting Server 上で使用することを目的としています。これは、Meeting Server の管理ツールではありません。また、既存の Meeting Server のインストールを再設定することもできません。このツールは、Meeting Server 2.9 仮 想マシンのみを設定するために作成されています。X シリーズ製品または Cisco Meeting Server 2000 プラットフォームで使用するためのものではありません。

# 前提条件

## クライアント コンピュータの要件

インストール アシスタントは、Meeting Server から分離されたコンピューター上で実行する必要があります。

**表 2：クライアント コンピューターのソフトウェア要件**

| オペレーティング システム | ブラウザ | ディスク容量 | 備考 |
|---|---|---|---|
| Windows 10<br>Windows Server 2012/2016/2019 | Edge、Chrome および Firefox | 150 MB | Microsoft C++ 2017/2019 ランタイム配布用のインストールが必要です。Microsoft のリンク https://support.microsoft.com/en-us/help/2977003/the-latest-supported-visual-c-downloads からダウンロードしてください。[英語]<br>Windows 10 コンピューターの場合、C++ ランタイム エンジンをすでに有効にしておく必要はありますが、別途インストールする必要はありません。インストール アシスタント ツールが起動時にクラッシュする場合は、その再頒布可能パッケージがコンピューター上にあることを確認します。 |
| Apple OSX Mojave<br>Apple OSX Catalina | Safari、Chrome および Firefox | 150 MB | 適用外 |

さらに、

- クライアント コンピュータには、ローカルで実行されている TCP ポート 8000 と競合するサービスを持たせないようにしてください。
- クライアント コンピューターは、次のポートを使用して、ネットワークを介して Meeting Server にアクセス可能にする必要があります。
    - TCP 22
    - TCP 443
    - Webadmin 用に設定される TCP ポート（推奨 445）

## Cisco Meeting Server の要件

- Meeting Server は、Cisco Meeting Server 1000 または仮想マシンのインスタンスである必要があります。インストール アシスタントは、Cisco Meeting Server 2000 または Acano プラットフォームとは互換性がありません。
- Meeting Server はソフトウェア 2.9.x（任意のメンテナンスリリースの 2.9）を実行している必要があります。新しいバージョンまたは古いバージョンは、インストール アシスタント 2.9 ではサポートされていません。
- Meeting Server は、ネットワーク アドレスと管理者アカウント以外の設定が済んでいないデフォルト設定である必要があります。

## 外部依存性

インストール タスクを実行するには、次のものも必要です。

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

# インストール

## ソフトウェアのインストール

インストール アシスタントは、Meeting Server とは別のコンピュータにインストールし、そのコンピュータでローカルに使用する必要があります。6 ページの「クライアントコンピューターの要件」を参照してください。

Windows のインストール

1. お使いのオペレーティング システム用のインストール アシスタントである製品の圧縮バージョンをダウンロードし、独自のフォルダに解凍します。

Apple OSX のインストール

1. お使いのコンピュータに InstallAssistantOSX.dmg ファイルをダウンロードします。InstallAssistantOSX.dmg をダブル クリックし、ディスク イメージをマウントして開きます。
2. Cisco InstallAssistant-2.9 アイコンをアプリケーション フォルダにドラッグします。
3. アプリケーション フォルダで、InstallAssistant をダブルクリックします。
   注：Mac OS Catalina では、認証されていないため、ゲートキーパーはインストール アシスタント アプリを実行できません。
4. [セキュリティ &amプライバシー（Security & Privacy）] をクリックします。[ダウンロード元のアプリを許可（Allow apps downloaded from）] セクションで、[今すぐ開く（Open Anyway）] をクリックします。

# ソフトウェアの実行

インストール アシスタントは、ユーザ インターフェイスとして Web ブラウザを使用したスタンドアロン ユーティリティです。ソフトウェアは、ソフトウェアが実行されるアプリケーションウィンドウを使用して、Web ブラウザを自動的に開いてソフトウェアのインターフェイスを表示します。（Windows では、このアプリケーションウィンドウが端末ウィンドウになります）。

## ユーティリティの実行

Windows：抽出したインストール アシスタント ファイルのフォルダにある「server.exe」アイコンをダブルクリックします。インストール アシスタント ツールは、ユーティリティを実行するコンソール ウィンドウを開いて、https://localhost:8000 に遷移するデフォルトのブラウザを自動的に開き、ツールのインターフェイスを表示します

Apple OSX：アプリケーション フォルダーで、インストール アシスタント 2.9 のアイコンをダブルクリックします。インストール アシスタント ツールは、ユーティリティを実行するアプリケーション ウィンドウを開いて、https://localhost:8000 に遷移するデフォルトのブラウザを自動的に開き、ツールのインターフェイスを表示します

---

**注：**Catalina（10.15.3）オペレーティング システムのバージョンで開始する場合、アプリケーションを開く前に「**確認中...**」ステータスメッセージが表示され、アプリケーションの起動に時間がかかることがあります。これにより、Apple が悪意のあるソフトウェアをスキャンできないため、アプリケーションを開くことができないという例外が発生する可能性があります。この通知はソフトウェアのパッケージによるものであり、予定されています。続行するには、[Ok]をクリックして、[**セキュリティ** & **プライバシー**] コントロールパネルを開いてください。インストールアシスタントがブロックされていることを通知するメッセージが表示されたら [**今すぐ開く**] をクリックし、メッセージが表示され たら [**開く** (open)] をクリックします。

---

## ユーティリティの終了

ブラウザのウィンドウを閉じて、開いたアプリケーション ウィンドウの [閉じる (close)] アイコンをクリックします。**注：**アプリケーション ウィンドウを手動で閉じる必要があります。ブラウザを閉じるだけでは、インストール アシスタントプロセスは終了しません。

## 永続的なファイル ストレージ

インストール アシスタントは、独自の設定を行わずにスタンドアロンのユーティリティとして使用することを目的としています。ただし、後でユーティリティを終了して戻り、タスクを完了させる機能をサポートするために、証明書とライセンス ファイルの詳細は暗号化された形式でユーザのディレクトリ内のクライアントマシンに保存されます。設定が完了するか、またはインストール アシスタントを使用しない場合は、これらのファイルを削除できます。

Windows ユーザ ストレージの場所：C:\Users\<username>\InstallAssistant

Apple OSX ユーザ ストレージの場所： /Users/<username>/Library/Application Support/InstallAssistant

# インストール アシスタントを使用した Meeting Server の設定

## 準備中

インストール アシスタントは、新しい、空のサーバを設定するためだけに使用されます。Meeting Server をインストール アシスタントと一緒に使用するには、次の 3 つのタスクに対応する必要があります。

- Meeting Server が空であることを確認する
- ライセンス ファイルを入手する
- Meeting Server の DNS エントリを設定する

### 新規の Meeting Server インスタンス

Meeting Server では、仮想マシンを展開して実行し、管理者アカウントを有効にする必要があります。さらに、IPv4「a」インターフェイスが設定されている必要があります。他の設定は実行されません。『Cisco Meeting server 1000 および仮想化導入ガイド（Installation Guide for Cisco Meeting Server 1000 and Virtualized Deployments）』では、Meeting Server のインスタンスを導入する方法と Cisco Meeting Server の 1000 アプライアンスを設定する方法について説明しています。このガイドの第 3 章では、サーバの設定について説明しています。「a」インターフェイスを設定しないようにしてください（ステップ 2）。サーバは、Cisco Meeting Server ライセンスをロードできますが、必須ではありません。

### 既存の Meeting Server インスタンス

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

1. サーバへの SFTP で既存の Cisco Meeting Server ライセンスを取得して、サーバから cms.lic ファイルを取得することでローカルにコピーを作成します。
2. Meeting Server の MMP インターフェイスに管理者アカウントを使用してログインし、コマンド factory_reset full を実行して、プロンプトが表示されたら確認します。サーバは、デフォルト設定にリセットされ、再起動します。
3. Meeting Server の MMP インターフェイスにログインし、ユーザ名 admin パスワード admin でログインします。
4. 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。
5. 「a」インターフェイスの IPv4 設定を構成します。Cisco Meeting Server 1000 と仮想化導入の設置 ガイドを参照してください。

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

### ライセンスファイル

ライセンス ファイルは、ご注文およびお使いのバーチャルマシンの MAC アドレスから、お使いのパックの情報を使用して、Cisco ライセンスポータルを使用して履行されます。評価ライセンスやデモ ライセンスの場合は、ライセンスを圧縮されたライセンス ファイルとして直接提供します。インストール アシスタントは、ライセンスファイルを Meeting Server にロードするのに役立ちますが、ファイルを取得してツールの外部で行うことができます。ライセンス ファイルなしで Meeting Server に接続できますが、ライセンス ファイルが Meeting Server に正常にロードされるまで、設定に移動することはできません。

### Meeting Server DNS エントリ

インストール アシスタントは Meeting Server のみを設定するものであり、DNS や SIP プロキシのような外部システムは設定しません。証明書またはホスト名を Meeting Server で使用する場合は、これらの DNS エントリを DNS サーバに追加してから、インストール アシスタントを使用することを推奨します。

## サーバの設定

ここでは、サーバを設定するための主要な手順について概説します。個々のパネルまたは設定の詳細については、このガイドにあるパネル リファレンスを参照してください。

1. クライアントコンピューターでインストール アシスタント ユーティリティを開くと、ツールのインターフェイスが Web ブラウザのウィンドウに表示されます。

2. [**サーバの設定**（Configure Server）] をクリックして、Meeting Server にアドレスとログインの詳細を提供します。
    a. [**サーバの設定**（Configure Server）] 画面で、Meeting Server のアドレスを入力します。
    b. Meeting Server に設定されているユーザ名を入力します。

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

    c. Meeting Server に設定されているパスワードを入力します。
    d. インストール アシスタントが処理するファイルを安全に保存するために使用されるパスフレーズを入力します。このパスフレーズは、インストール アシスタントをいったん閉じてから再起動する場合に必要です。

    **注：**前回の試行後にツールを再度開く場合は、以前に使用したパスフレーズを再入力してください。それ以外の場合は、任意のパスフレーズを入力します。パスフレーズを忘れた場合は、ファイルを削除して再起動します。

    **注：**パスフレーズは重要になるため忘れないようにしてください。パスフレーズを忘れた場合は、次の場所から内容を削除する必要があります。
    Windows ユーザ：C:\Users\<username&gt\InstallAssistant
    MAC ユーザ：/Users/<username>/InstallAssistant
    その後、設定を新規で開始します。

3. [**接続**（Connect）] をクリックします。

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

4. このツールでは、Web Bridge の展開を選択できます。デフォルトでは、Web Bridge 3 が選択されています。
5. [Web Bridge の展開（Web Bridge deployment）] を選択し、[適用（Apply）] をクリックします。ツールの [設定（configuration）] ビューが表示されます。

    - 展開の種類を Web Bridge 3 として選択した場合、設定は Windows の電子メールアドレスに基づきます。Web Bridge 2 が選択されている場合、設定は XMPP ドメインと Windows 電子メールアドレスに基づきます。

6. 設定はパネルに分かれています。設定を行うには、関連情報を提供する必要があります。左側のメニューのリストを使用してパネル間を移動します。

   **注：**他のパネルを有効にする前に、証明書パネルとライセンス パネルを完了させる必要があります。

7. パネル間を移動して、メッセージが表示されたらフィールドに入力します。すべてのパネルが完了すると、最後のパネルである**「プッシュの設定（**Push Configuration**）」**で、指定された設定を検証する必要があります。
8. 設定を確認して検証し、準備ができたら、[**プッシュの設定（**Push Configuration**）**] をクリックして設定を サーバにプッシュします。

   **注：**サーバへのプッシュの設定時に問題が発生した場合、問題の診断を支援するログ ページが表示されます。

9. 設定が完了したら、[**終了（**Exit**）**] をクリックして、ブラウザ ウィンドウとコンソール ウィンドウを閉じて、ツールを終了できます。それ以外の場合は、コンソール ウィンドウを閉じない限り、ツールのバックグラウンド サービスは引き続き実行されます。

## 設定のプッシュ後

1. プッシュの設定に成功すると、設定を選択したサービスが設定され、有効になります。Web 管理者には、https://fqdn:<webadminport> からアクセスできます。Web Bridge が有効になっている場合は、https://fqdn **からアクセスでき、**TestCospace というテスト スペースが Meeting Server 上に作成されます。
2. サーバの Web Admin インターフェイスに接続できることを確認し、ログインします。デフォルトは https://fqdn:445 **です**。
3. コール コントロールが、設定したドメイン名を使用して Meeting Server からのコールを送受信するように設定されていることを確認します。
4. サーバ上にテスト スペースが定義されていて、Web Admin インターフェイスを介して URI を更新し、エンドポイントからダイヤルインして、テストします。
5. ユーザのインポートを有効にした場合、LDAP の変更を同期するには、Meeting Server Web Admin インターフェイスの [**今すぐ同期** (Sync Now)] を使用して手動で行う必要があります（[**設定** (Configuration**）**] > [**アクティブ ディレクトリ（**Active Directory**）**]）。
6. Web Bridge を有効にしている場合、ユーザは https://fqdn を参照してミーティングに参加できま す。

## ツールを複数回実行

サーバに設定がプッシュされた後は、サーバが工場出荷時にリセットされていない限り、設定をサーバに再度プッシュするためにインストール アシスタントを使用することはできません。ライセンス ファイル以外については、[**プッシュの設定**(Push configuration )] ボタンをクリックするまで、インストール アシスタントは Meeting Server の設定を変更しません。このため、プッシュの設定が行われていない限り、ツールの開始と停止、および同じ Meeting Server への接続ができます。

## トラブルシューティング

トラブルシューティングには、次のパスに格納されているログを使用できます。
Windows：お使いのマシンの \C:\InstallAssistantWin\InstallAssistant\portal\logs。
Apple OSX： /Users/<username>/InstallAssistant/logs
トラブルシューティング情報については、次のリンク先を参照してください。https://meeting- infohub.cisco.com/faq/category/25/cisco-meeting-server.html [英語]

## インストール アシスタントの終了

Windows : [コマンドプロンプト（command prompt）] ウィンドウを閉じます。
Apple OSX : [インストール アシスタント（Installation Assistant）] ウィンドウを閉じます。

## ソフトウェアのアンインストール

ローカル コンピュータからインストール アシスタント ソフトウェアを削除するには、次の場所から InstallAssistant ディレクトリを削除してください。

Windows ユーザ：C:\Users\<username>/ Apple

OSX ユーザ： /Users/<username>/

# パネル リファレンス

## 証明書

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

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

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

### CA 署名済み証明書

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

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

#### CSR **経由の新規証明書**

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

このプロセスを完了するには、以下の内容が必要です。

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

**注：**インストール アシスタント ツールは、CSR のダウンロード後に自由に閉じることができます。認証局からの署名付き証明書を取得したら、インストール アシスタントを再起動して、[証明書（Certificate）] パネルに戻り、アップロード プロセスを完了します（以下の手順 4 を参照）。

新しい証明書要求（CSR）を作成する手順は次のとおりです。

1. [証明書（Certificates）] パネルで証明書の種類「**署名付き** CA（CA Signed）」を選択して、[証明書のアップロードオプション] の下で [CSR **経由の新規証明書**（New Certificate via CSR）] を選択
2. [CSR **の生成**（Generate CSR）] をクリックして、Meeting Server で使用する詳細を含むフィールドを入力します。そのフィールドについては次で説明します。完了したら、[**生成**（Generate）] ボタンをクリックして [証明書（certificate）] パネルに戻ります。[生成（Generate）] ボタンは、必要な詳細をすべて入力した後にのみ有効になります。

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

**表 3：証明書署名要求に必要なフィールド**

| フィールド名 | 説明 | 値 |
|---|---|---|
| Meeting Server 用 FQDN | 証明書の CN 値であり、DNS サーバ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。 |
| Meeting Server の SIP ドメイン | サブドメインの使用を推奨します。 | ルーティング ルールに合わせるには、サーバの SIP ドメインを入力します。 |
| Web や Cisco ミーティング アプリケーション ユーザのログイン ドメイン（XMPP ドメイン） | これは、ユーザ名のドメインの一部であり、Cisco ミーティング アプリケーションの Web アプリにログインするために使用されます（Cisco ミーティング アプリケーションの Web アプリのユーザ ログインを有効にする必要がある場合にのみ必要）。別のログイン ドメイン名と SIP ドメイン名の使用を推奨します。<br>注：[Web Bridge 3 の展開（Web Bridge 3 deployment）] を選択した場合、電子メールアドレスを使用したログインが完了しているため XMPP ドメインを使用できません。 | Cisco ミーティングアプリケーションの Web アクセス（ゲストまたはユーザ）を有効にする場合にのみ、ログイン ドメインを入力します。 |

3. 完了した CSR が [証明書（Certificate）] パネルに表示されます。[CSR **のダウンロード（**Download CSR**）**] をクリックして、結果の CSR をローカル ドライブ上のファイルに保存します。
4. 署名されるために、CSR に認証局への署名を行います。これらは、署名付き証明書ファイルを返します。また、認証局の証明書チェーン バンドルも必要になります。
5. 署名付きの証明書と証明書チェーンファイルを取得したら、必要に応じて [証明書（Certificate）] パネルに戻り、[**ファイルのアップロード（**Upload Files**）**] をクリックし、証明書とバンドルをアップロードします。証明書と CA 証明書チェーンを指定するための 2 つのフィールドが示されています。[**ファイルの選択（**Select File**）**] リンクを使用してお使いのローカル コンピューター上の特定のファイルを検索します。証明書ファイルには、次のいずれかの拡張子（CER、CRT、PEM、DER）が必要であり、PEM または DER としてエンコードされている必要があります。
6. 両方のファイルを指定すると、[**アップロード（**Upload**）**] ボタンが有効になります。[**アップロード（**Upload**）**] 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。
7. 成功すると、証明書とその詳細情報が [**利用可能な証明書（**Available Certificates**）**] の下に表示され、[証明書（Certificate）] パネルがナビゲーション ツリーで完了とマークされます。

**エラーのシナリオ**

- サーバまたは技術的な問題が原因でアップロードが失敗した場合は、エラー通知が表示され、証明書ファイルを再アップロードする必要があります。
- 指定された証明書が誤っている場合、エラー通知が表示され、[アップロード（Upload）] ボタンが無効になります。適切な証明書と CA 証明書チェーンを選択してアップロードする必要があります。

### 既存の証明書とキーの使用

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

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

既存の証明書を使用する手順は次のとおりです。

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

成功すると、証明書とその詳細情報が [**利用可能な証明書（**Available Certificate**）**] の下に表示され、[証明書（Certificate）] パネルがナビゲーション ツリーで完了とマークされます。

**エラーのシナリオ**

- サーバまたは技術的な問題が原因でアップロードが失敗した場合は、エラー通知が表示され、証明書ファイルを再アップロードする必要があります。
- 指定された証明書が誤っている場合、エラー通知が表示され、[**アップロード（**Upload**）**] ボタンが無効になります。適切な証明書と CA 証明書チェーンを選択してアップロードする必要があります。

### 自己署名証明書

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

**注：**現在、自己署名入りの証明書が選択されている場合、インストール アシスタントは Web Bridge や会議ユーザの設定をサポートしません。

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

自己署名入りの証明書を使用する手順は次のとおりです。

1. [証明書 (Certificate)] パネルで [**自己署名（Sef signed）**] を選択して、[**適用（Apply）**] をクリックします。ナビゲーションツリーで [証明書（Certificate）] パネルが完了済みとしてマークされます。

## License

Cisco Meeting Server の機能を設定して有効にするには、アクティブなライセンス ファイルが必要です。ライセンス ファイルは、サーバの MAC アドレスと Meeting Server の購入の PAK 情報を使用して、Cisco ライセンス ポータルから入手します。

### ライセンスのアップロード

**注：**電子メール経由で xxxx.lic ファイルを .zip 形式で受信することになります。インストール アシスタントにアップロードする前にファイルを解凍する必要があります。

[**ライセンス（License）**] パネルで、実行する必要があるアクティブなライセンスを Cisco Meeting Server でアップロードする必要があります。[ライセンスの選択（Select License）] オプションを使用すると、新しいライセンス ファイルを検索してアップロードできます。

1. [**ライセンス ファイルの選択（Select License File）**] をクリックします。
   ライセンス ファイルが選択され、ファイル形式がサポートされている形式である場合にのみ、ファイルがアップロードされます。[**ライセンスのプレビュー（Preview License）**] オプションで、新しいライセンスを表示できます。

   **注：**ライセンス ファイル名は、サポートされている形式（例：cms.lic）に自動的に名前が変更されます。

2. 利用可能なサービスの詳細を表示し、適切なファイルを入力した後に [**開く（Open）**] をクリックできます。
3. [**ライセンスのプレビュー（Preview License）**] をクリックすると、新しいライセンスファイルで利用可能なサービスが表示されます。

**注：**新しいライセンス ファイルをアップロードすると、サーバ上の以前のライセンス ファイルや、そのファイルを有効にした権限が置き換えられます。

4. [**アップロード**（Upload）] をクリックして新しいライセンス ファイルを保存するか、[**キャンセル**（Cancel）] をクリックして、現在このサーバにあるライセンスによってアクティブ化されているサービスを保持します。

**注：**無効なライセンス ファイルをアップロードしている場合は、エラー メッセージが表示されます。正しいライセンス ファイルを .lic 形式でアップロードする必要があります。

## ネットワーク

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

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

1. 次を設定します。

| フィールド名 | 説明 | 操作 |
|---|---|---|
| Meeting Server FQDN | サーバの FQDN | 有効な FQDN を入力します。次に例を示します。<br>meetingserver.example.com |
| NTP サーバ | FQDN または IP アドレスのいずれかを使用して、少なくとも 1 台の NTP サーバを設定する必要があります。<br>注：最大 5 台の NTP サーバを設定できます。 | [サーバの追加（Add Server）] をクリックします。NTP サーバのアドレスが Cisco Meeting Server に追加されます。 |
| タイム ゾーン（Time zone） | サーバのローカル タイムゾーン | ご希望のタイムゾーンを選択してください |
| DNS サーバ（Server） | FQDN または IP アドレスのいずれかを使用して、少なくとも 1 台の DNS サーバを設定する必要があります。<br>注：最大 5 台の DNS サーバを設定できます。 | サーバの IP アドレスを入力して [サーバの追加（Add Server）] をクリックします。DNS サーバのアドレスが Cisco Meeting Server に追加されます。<br>注：正しい DNS サーバ アドレスを「10.77.89.100」形式で入力してください。 |
| Webadmin ポート | Meeting Server Web Admin インターフェイスが受信する TCP ポート番号を設定します。443 以外のポートを使用することが推奨されているため、ユーザが扱う Web インターフェイス（Web Bridge）にはデフォルトの HTTPS ポートを使用できます。 | ポート番号を入力します。 |

2. 設定を保存する前に、すべての詳細が入力されていることを確認します。[**保存**（Save）] をクリックします。その後、ネットワーク設定が保存されます。

### DNS または NTP サーバを削除

1. をクリックして DNS や NTP サーバを削除します。

## Call Bridge

[コール ブリッジ（Call Bridge）] パネルでは、コール ブリッジ サービスの設定を構成できます。

1. 次の詳細を入力します。

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

2. [**保存（Save）**] をクリックして、設定を保存します。

---

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

---

## 会議ユーザ

[会議ユーザ（Conferencing user）] パネルは、Active Directory からユーザのインポートを有効にするためのオプション設定です。ユーザをインポートすると、ユーザは Cisco Meeting アプリケーションにログインして、スペースを管理し、ミーティングに参加できるようになります。このパネルは、Web Bridge が有効になっている場合にのみ表示されます。

ユーザをインポートするには次の事項が必要です。

- Active Directory サーバに接続するための接続プロパティの定義
- ユーザがインポートされる LDAP の場所の指定

- LDAP ユーザの値を Meeting Server のユーザ値に変換するための検索フィルタとプロパティ マッピングを定義すること。インストール アシスタントには、ほとんどの環境で動作するデフォルト値がありますが、必要に応じてデフォルト値を変更することもできます。

Active Directory からユーザをインポートする場合は、次のようにします。

1. [Cisco **ミーティングアプリケーションのユーザの有効化**（Enable users for Cisco Meeting App）] の下にあるチェックボックスをオンにします。追加の構成設定が表示されます。
2. 提供されているフィールドに XMPP ドメイン名を入力します。このドメインは、x.509 証明書の SAN リストに含まれている必要があります。証明書を読み込むための [CSR **の生成**（Generate CSR）] オプションがある場合、そのパネルからの XMPP ドメインが自動的にここにコピーされます。この設定では、ユーザが Cisco ミーティングアプリケーションにログインするために使用するユーザ名のドメイン部分を構成します。
   注：[Web Bridge 3 の展開（Web Bridge 3 deployment）] を選択した場合、電子メールアドレスを使用したログインが完了しているため XMPP ドメイン フィールドを使用できません。
3. [LDAP **接続の設定**（LDAP Connection Settings）] フィールドに、Active Directory コントローラに接続するための値を入力します。すべての 必須フィールドの入力が完了すると、[**保存**（Save）] ボタンが表示されます。
   各設定の詳細については、次の表を確認してください。

**表 4：LDAP 接続の設定**

| フィールド名 | 説明 | 入力 |
|---|---|---|
| プロトコル | 接続で LDAP または TLS のある LDAP を使用する場合に設定します。<br>LDAPS 推奨 | 使用している環境に応じて LDAP または LDAPS のいずれかを選択します。 |
| サーバ アドレス（Server address） | 接続先の LDAP サーバのネットワーク アドレス | LDAP サーバの FQDN または IP アドレス。 |
| ポート | 接続先の LDAP サーバの TCP ポートLDAP のデフォルトは 389 または 3268 です。 | 有効なポート番号<br>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（Username） | LDAP サーバに接続されるユーザのユーザ名。このユーザには、ディレクトリへの読み取り権限のみが必要です。<br>注：[Web Bridge 3 展開（Web Bridge 3 deployment）] を選択した場合、デフォルトのユーザ名は「$mail$」形式になります。 | 認証に使用するユーザの LDAP 識別名（DN）または UPN<br>このフィールドは空白にできません |
| パスワード | ユーザ指定のパスワード | ユーザのパスワード。<br>このフィールドは空白にできません。 |

| フィールド名 | 説明 | 入力 |
|---|---|---|
| 検索ベース | インポート検索クエリが開始される LDAP ディレクトリ内の場所。この値の詳細については、ドメイン管理者に問い合わせてください。 | 検索を開始するディレクトリの場所の LDAP 識別名（DN）<br>このフィールドは空白にできません |
| ユーザへの PMP ライセンスの割り当て | 有効にすると、インポートされたユーザは PMP+ ライセンスを受ける資格があるものとしてマークされます。インポートするすべてのユーザに対して PMP+ ライセンスを購入していない場合は、有効にしないでください。 | すべてのインポートされたユーザに PMP+ の権限をタグ付けするようにします。 |
| 既定のユーザ フィルタとフィールド マッピングの詳細の上書き | インストール アシスタントは、デフォルトの LDAP 検索フィルタとユーザ フィールド マッピングを使用して、ほとんどの環境で動作することを想定しています。このオプションを有効にすると、環境に合わせてこれらの設定を表示およびカスタマイズできます。 | LDAP 検索フィルタ、および LDAP ユーザ フィールド マッピングの表示やカスタマイズを有効化します。 |

### LDAP 検索とユーザ マッピングのカスタマイズ

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

<Windows ユーザ名>@<XMPP ドメイン>

[上書き（override）] オプションを有効にすると、インポートに使用される個々の設定フィールドが表示されます。設定を表示すると、インストール アシスタントがデフォルトで使用します。

上書きが有効になっている場合、ユーザは、環境に合わせてこれらの値をカスタマイズできます。

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

**表 5：LDAP の読み込み設定**

| フィールド名 | 説明 | 入力 |
|---|---|---|
| LDAP 検索フィルタ | 読み込む LDAP ユーザの条件を定義します。 | LDAP 検索文字列。LDAP 検索シンタックスを使用する必要があります |
| 表示名 | ディレクトリと検索でユーザに対して表示される名前。 | マッピング方式。例：$cn$ |

| フィールド名 | 説明 | 入力 |
|---|---|---|
| ユーザ名<br>（User name） | ユーザが Cisco ミーティングアプリケーションのログインに使用する XMPP ユーザ名。これは、インストール アシスタントの他の手順で定義されたドメイン名と一致する @<XMPP ドメイン名> および <XMPP ドメイン名>で終わるユーザ名の形式にする必要があります。<br>結果の値は、すべてのユーザとスペースに対して一意である必要があります。 | マッピング方式。<br>例：<br>$sAMAccountName$@company.com<br>このフィールドは空白にすることはできず、結果は読み込まれた各ユーザに対して一意である必要があります。 |
| スペース名 | 与えられたラベルをユーザ用のスペースに自動的に作成します。<br>読み込んだユーザのスペースを作成しない場合は、空白のままにします。 | マッピング方式。<br>例：$cn$ Meeting space |
| スペース URI | ユーザに対して自動的に作成されたスペースの URI の左側部分。<br>結果は、ユーザごとに一意である必要があり、ユーザ名または他のスペースと競合していない必要があります。読み込んだユーザのスペースを作成しない場合は、空白のままにします。 | マッピング方式。<br>例：$cn$.space |
| スペース セカンダリ URI | ユーザに対して自動的に作成されたスペースのセカンド URI の左側部分。<br>結果は、ユーザごとに一意である必要があり、ユーザ名または他のスペースと競合していない必要があります。オプション フィールド。読み込んだユーザのスペースを作成しない場合は、空白のままにします。 | マッピング方式。<br>例：$cn$.room |
| スペースのコール ID | ユーザ用に自動的に作成されたスペースのコール ID を設定します。<br>結果は、すべてのスペースで一意である必要があります。オプション フィールド、Cisco Meeting Server では、空白の場合 ID を自動的に割り当てます。<br>読み込んだユーザのスペースを作成しない場合は、空白のままにします。 | マッピング方式。 |
| 認証 ID マッピング | インポートされたユーザに割り当てられているマッピング プロパティ。スマートカードのログイン シナリオで使用されます。<br>証明書ベースのログインを特に展開しない限り、空白のままにしておきます。 | マッピング方式。<br>例：$userPrincipalName$ |

1. [**保存**（Save）] をクリックして、設定を保存します。

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

## Web Bridge

Meeting Server の Web Bridge 機能を有効にするオプションがあります。[Web Bridge] パネルの Web Bridge を有効にすると、参加者は、Web ベースの Cisco ミーティング アプリケーションを使用しているゲストとしてミーティングに参加できるようになります。Web Bridge が有効になっている場合は、ユーザを Active Directory からインポートできるようにして、ユーザが Cisco ミーティング アプリケーション Web アプリを使用してログインすることで、スペースを管理できます。認証済みユーザの有効化は、Web Bridge が有効化されている場合にのみ有効になる、[会議ユーザ（Conference User）] パネルで設定されます。

Web Bridge 機能を有効にするには、[Web Bridge] パネルで次のように入力します。

1. [Web Bridge **を有効にする（**Enable Web Bridge**）**] チェックボックスをオンにします。
2. [Web Bridge 2] を選択した場合は、[XMPP ドメイン名（XMPP domain name）] テキストフィールドに、Meeting Server で使用する XMPP ドメインを入力します。この設定は、生成された CSR ステップ（使用している場合）で設定されているログイン ドメインと一致し、Meeting Server の証明書のサブジェクト代替名（SAN）のリストに含まれている必要があります。
   または
   [Web Bridge 3] が選択されている場合、発信する必要がある Web Bridge（c2w）リスニング ポート番号にコール ブリッジを入力します。これにより、コール ブリッジを Web Bridge に接続できます（デフォルトのポート番号は 9999 です）。
3. [**保存**（Save）] をクリックします。

**注：**Web Bridge を有効にすると、インストール アシスタントによって、必要な XMPP SRV レコードに対応するローカル DNS RR エントリが Meeting Server に作成されます。このローカル エントリは、Meeting Server によって解決可能であるというだけであり、この簡略化されたセットアップのローカル Web Bridge のみをサポートすることを目的としています。必要に応じて、DNS サーバのローカル DNS RR エントリを削除し、適切な SRV レコードに置き換えることができます。

## セキュリティ

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

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

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

3. [**保存**（Save）] をクリックします。ログイン資格情報が作成され、保存されます。

## 設定をプッシュする

[プッシュ設定（Push Configuration）] パネルでは、インストール アシスタントで設定した各パネルの詳細を確認できます。また、詳細を Cisco Meeting Server に送信して設定プロセスを完了することもできます。設定をプッシュする前に、設定を検証する必要があります。検証が正常に完了すると、[プッシュ設定（Push configuration）] ボタンが有効になります。検証が失敗した場合は、特定のパネルに移動して、競合する設定を更新します。

1. パネル設定の詳細を確認し、[**設定の検証（**Validate settings**）**] をクリックします。
2. 検証に成功すると、[**プッシュ設定（**Push configuration**）**] オプションが有効化されます。
3. [**プッシュ設定（**Push configuration **）**] ボタンをクリックして、詳細を Cisco Meeting Server に送信し、設定プロセスを完了します。

   **注：**提供された証明書にすべての必須フィールドが含まれていない場合は、次のエラーメッセージが表示されます「**検証に失敗しました。提出された証明書には、ユーザのインポートとスペースへのアクセスに必要な** XMPP **や** SIP **ドメインの詳細が含まれていません。適切な証明書をアップロードするか、**[**会議ユーザ（**Conferencing User**）**] **と** [Web Bridge] **パネルの設定を無効にしてから、設定の詳細を検証します。**'

   Web Bridge 2 を展開する場合、証明書に FQDN と SIP や XMPP のドメインが含まれている場合は、証明書の検証が確認されます

   Web Bridge 3 を展開する場合、証明書に FQDN と SIP や XMPP のドメインが含まれている場合は、証明書の検証が確認されます。さらに、このアプリケーションは、証明書に指定されている場合、[拡張キーの使用（extended key usage）] フィールドに TLS Web Server 認証と TLS Web クライアント認証の両方が含まれているかどうかを確認します。
4. 暗号化パスフレーズを入力して、秘密キーを暗号化したり復号化したりします。注：このフィールドを空にすることはできません。

インストール アシスタントは、パネルに指定されている情報を確認し、エラーを検出した場合、それらを表示します。必要な変更を加えて、設定の詳細を検証する必要があります。

5. 検証に成功した場合は、[**プッシュ設定（**Push configuration**）**] ボタンが有効になります。[**プッシュ設定（**Push configuration**）**] ボタンをクリックして、設定を開始します。

   **注：**検証に失敗した場合は、特定のパネルに戻り、競合する設定を更新します。
6. 設定が Cisco Meeting Server に正常に転送されると、インストール アシスタントに概要の詳細が表示されます。ログをダウンロードすることもできます。変更を加えずに

   ツールを終了します。このパネルは、インストール アシスタントを再度開いたときに使用できます。

**注：**Cisco Meeting Server へのプッシュ設定が失敗した場合は、詳細についてログの詳細を確認する必要があります。[**ログのダウンロード（**Download logs**）**] をクリックして、ログの詳細ファイルをダウンロードして表示します。

**注：**プッシュ設定が失敗し、設定済みのサーバでインストール アシスタントを再使用する場合は、同じサーバ上でインストール アシスタントを再度使用する前に、Meeting Server を工場出荷時の状態にリセットして、IP アドレスを再設定する必要があります。ファクトリ リセットは、サーバの MMP コマンドラインに ssh を使用してログインし、「factory_reset full」コマンドを実行することによって行われます。ファクトリ リセット コマンドを使用すると、ライセンス ファイルとネットワーク設定が削除されるため、工場出荷時にサーバをリセットする前に情報が確実に取得されるようになります。

# Cisco の法的情報

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

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

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.
ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

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

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

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

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

© 2020 Cisco Systems, Inc. All rights reserved.

# Cisco の商標

Cisco および Cisco のロゴは、米国およびその他の国における Cisco およびその関連会社の商標を示します。Cisco の商標の一覧については、www.cisco.com/go/trademarks.をご覧ください。Third-party trademarks mentioned are the property of their respective owners. 「パートナー」という用語の使用は 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）

# 2 用語集

M

**マイ用語**
マイ定義