Cisco Jabber 12.8 オンプレミス展開ガイド

初版：2020 年 1 月 22 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次

新規および変更情報

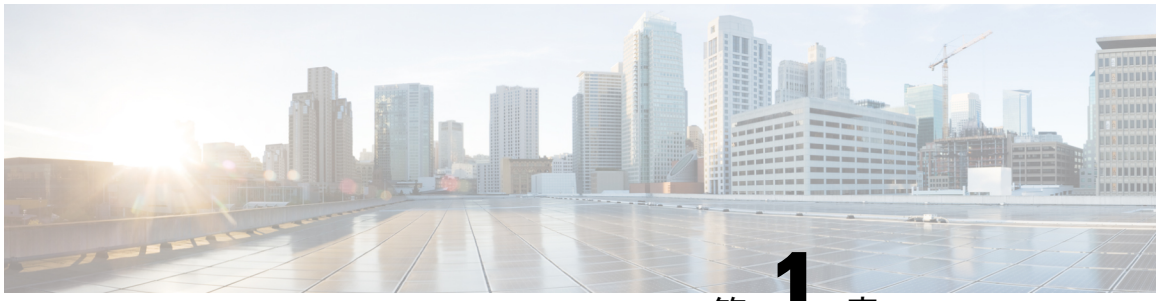
新規および変更情報

日付	ステータス	説明	場所（Location）
2020 年 1 月		ドキュメントの初公開	
	更新されました	H-264 高プロファイルサポートの追加	サポートされるコーデック

新規および変更情報

第 I 部

概要



第 1 章

Cisco Jabber の概要

このマニュアルの目的

Cisco Jabber 展開およびインストール ガイドには、Cisco Jabber の展開とインストールに必要な次のタスクベースの情報が記載されています。

- オンプレミス展開を設定してインストールするためのプロセスの概要を示す設定とインストールのワークフロー。
- IM and Presence サービス、音声およびビデオ通信、ビジュアル ボイスメール、会議など、Cisco Jabber クライアントと相互作用するさまざまなサービスの設定方法。
- ディレクトリ統合、証明書検証、およびサービス ディスカバリの設定方法。
- クライアントのインストール方法。

Cisco Jabber を展開してインストールする前に、http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html で『*Cisco Jabber Planning Guide*』を参照して、ビジネス ニーズに最適な展開オプションを決定してください。

Cisco Jabber について

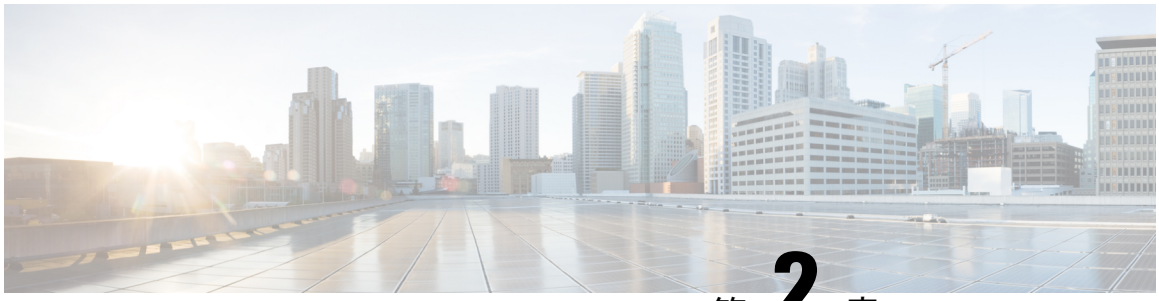
Cisco Jabber は、あらゆる場所から連絡先とのシームレスな対話を実現する Unified Communications アプリケーション スイートです。Cisco Jabber は、IM、プレゼンス、音声およびビデオ通話、ボイスメール、および会議を提供します。

Cisco Jabber 製品ファミリには、次のようなアプリケーションが含まれています。

- Cisco Jabber for Windows
- Cisco Jabber for Mac
- Cisco Jabber for iPhone and iPad

- Cisco Jabber for Android
- Cisco Jabber Softphone for VDI

Cisco Jabber 製品スイートの詳細については、https://www.cisco.com/go/jabberまたは https://www.cisco.com/c/en/us/products/unified-communications/jabber-softphone-for-vdi/index.html を参照してください。



第 2 章

設定およびインストールのワークフロー

設定ワークフローの目的

オンプレミス展開を設定してインストールするためのプロセスの概要を示す設定とインストールのワークフロー。Cisco Jabber を展開してインストールする前に、『Install and Upgrade Guides』で『Cisco Jabber Planning Guide』を参照して、ビジネスニーズに最適な展開オプションを決定してください。

前提条件

- サーバのインストールが開始され、アクティブである必要があります。
- 必須サービスの有効化と開始 （3 ページ）
- デバイス用の Cisco Options Package ファイルのインストール （4 ページ）

必須サービスの有効化と開始

必須サービスにより、サーバ間の通信が可能になり、クライアントにさまざまな機能が提供されます。

手順

ステップ 1 [Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Servicability）] インターフェイスを開きます。

ステップ 2 **[ツール（Tools）]>[コントロール センターの機能サービス（Control Center - Feature Services）]** を選択します。

ステップ 3 [サーバ（Server）] ドロップダウン リストから適切なサーバを選択します。

ステップ 4 次の各サービスが開始され、かつ有効になっていることを確認します。

- **Cisco SIP Proxy**
- **Cisco Sync Agent**
- **Cisco XCP Authentication Service**
- **Cisco XCP Connection Manager**
- **Cisco XCP Text Conference Manager**
- **Cisco Presence Engine**

ステップ 5 **[ツール（Tools）]>[コントロール センターのネットワーク サービス（Control Center - Network Services）]** を選択します。

ステップ 6 [サーバ（Server）] ドロップダウン リストから適切なサーバを選択します。

ステップ 7 **Cisco XCP Router Service** が実行されていることを確認します。

デバイス用の Cisco Options Package ファイルのインストール

Cisco Unified Communications Manager で Cisco Jabber をデバイスとして使用できるようにするには、ご使用のすべての Cisco Unified Communications Manager ノードにデバイス固有の Cisco Options Package (COP) ファイルをインストールする必要があります。

サービスが中断されないように、この手順は使用率が低い時間帯に行ってください。

COP ファイルのインストールに関する一般的な情報については、お使いのリリースに対応した『*Cisco Unified Communications Operating System Administration Guide*』の「Software Upgrades」の章を参照してください。

手順

ステップ 1 デバイスの COP ファイルをダウンロードします。

a) デバイスの COP ファイルを配置します。

- ソフトウェア ダウンロード サイトに移動します。
- ご使用のリリースに対応したデバイスの COP ファイルを配置します。

b) [今すぐダウンロード（Download Now）] をクリックします。

c) MD5 チェックサムを書き留めます。

この情報は、後で必要になります。

d) [ダウンロードを進める（Proceed with Download）] をクリックして、手順に従います。

ステップ 2 Cisco Unified Communications Manager ノードからアクセス可能な FTP または SFTP サーバに COP ファイルを配置します。

ステップ 3 Cisco Unified Communications Manager クラスタ内のパブリッシャ ノードにこの COP ファイルをインストールします。

a) [Cisco Unified OS の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

b) **[ソフトウェアアップグレード（Software Upgrades）] > [インストール/アップグレード（Install/Upgrade）]** を選択します。

c) COP ファイルの場所を指定し、必要な情報を入力します。

詳細については、オンライン ヘルプを参照してください。

d) [次へ（Next）] を選択します。

e) デバイス COP ファイルを選択します。

f) [次へ（Next）] を選択します。

g) 画面に表示される指示に従います。

h) [次へ（Next）] を選択します。

処理が完了するまで待ちます。このプロセスには、時間がかかる場合があります。

i) 使用率が低いときに Cisco Unified Communications Manager をリブートします。

j) システムが完全にサービスに復帰するまで待機します。

（注） サービスの中断を避けるために、各ノードのサービスがアクティブな状態に戻ったことを確認してから、次のサーバでのこの手順を実行するようにしてください。

ステップ 4 クラスタ内の各サブスクライバ ノードに COP ファイルをインストールします。

パブリッシャ ノードのときと同じ方法で、ノードのリブートなどの手順を実行します。

展開およびインストールのワークフロー

UC の完全な展開

手順

	コマンドまたはアクション	目的
ステップ 1	http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html で『Cisco Jabber Planning Guide』を参照してください。	• 展開シナリオを選択します。 • 要件を検証して、それらが満たされていることを確認します。 • 連絡先ソースを確認して、使用する連絡先ソースを決定します。
ステップ 2	デフォルトサービスプロファイルの作成 （13 ページ）	サービスを追加するためのサービスプロファイルを作成します。
ステップ 3	連絡先ソース （15 ページ）	ユーザの連絡先ソースを設定します。
ステップ 4	インスタントメッセージングとプレゼンス サービスの設定 （25 ページ）	Cisco Unified Communications IM & プレゼンスサービスを設定します。
ステップ 5	ボイスメールの設定 （31 ページ）	ユーザのボイスメールを設定します。
ステップ 6	Webex 会議の設定 （39 ページ）	Cisco Webex Meetingsサーバを使用して会議を設定します。
ステップ 7	CTI サービスの設定 （43 ページ）	CTIサービスを設定し、Jabber にユーザーに関連付けられているデバイスを提供します。
ステップ 8	ユーザ（Users） （47 ページ）	Jabber のユーザを設定します。
ステップ 9	ソフトフォンの設定 （63 ページ）	ユーザ用のソフトフォンデバイスを設定します。
ステップ 10	デスクフォン制御の設定 （75 ページ）	デスクフォンデバイスを作成し、機能を有効にします。
ステップ 11	拡張および接続機能の設定 （83 ページ）	ユーザのオプションを設定し、リモート デバイスへの通話を拡張します。
ステップ 12	サービス ディスカバリの設定 （91 ページ）	ユーザのサービス ディスカバリ オプションを選択します。
ステップ 13	証明書検証の設定 （103 ページ）	各サーバの必要な証明書を設定します。
ステップ 14	クライアントの設定 （107 ページ）	クライアント設定ファイルに含める機能を選択します。

	コマンドまたはアクション	目的
ステップ 15	Cisco Jabber アプリケーションおよび Jabber ソフトフォンの VDI 用の展開 （121 ページ）	ユーザのためのクライアントのインストール方法を選択します。

Jabber IM のみの展開

手順

	コマンドまたはアクション	目的
ステップ 1	http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html で『Cisco Jabber Planning Guide』を参照してください。	• 展開シナリオを選択します。 • 要件を検証して、それらが満たされていることを確認します。 • 連絡先ソースを確認して、使用する連絡先ソースを決定します。
ステップ 2	デフォルトサービスプロファイルの作成 （13 ページ）	サービスを追加するためのサービスプロファイルを作成します。
ステップ 3	連絡先ソース （15 ページ）	ユーザの連絡先ソースを設定します。
ステップ 4	インスタントメッセージングとプレゼンス サービスの設定 （25 ページ）	Cisco Unified Communications IM & プレゼンスサービスを設定します。
ステップ 5	Webex 会議の設定 （39 ページ）	Cisco Webex Meetingsサーバを使用して会議を設定します。
ステップ 6	ユーザ（Users） （47 ページ）	Jabber のユーザを設定します。
ステップ 7	サービス ディスカバリの設定 （91 ページ）	ユーザのサービス ディスカバリ オプションを選択します。
ステップ 8	証明書検証の設定 （103 ページ）	各サーバの必要な証明書を設定します。
ステップ 9	クライアントの設定 （107 ページ）	クライアント設定ファイルに含める機能を選択します。
ステップ 10	Cisco Jabber アプリケーションおよび Jabber ソフトフォンの VDI 用の展開 （121 ページ）	ユーザのためのクライアントのインストール方法を選択します。

電話専用モードの展開

手順

	コマンドまたはアクション	目的
ステップ 1	http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html で『Cisco Jabber Planning Guide』を参照してください。	• 展開シナリオを選択します。 • 要件を検証して、それらが満たされていることを確認します。 • 連絡先ソースを確認して、使用する連絡先ソースを決定します。
ステップ 2	デフォルトサービスプロファイルの作成 （13 ページ）	サービスを追加するためのサービスプロファイルを作成します。
ステップ 3	ボイスメールの設定 （31 ページ）	ユーザのボイスメールを設定します。
ステップ 4	Webex 会議の設定 （39 ページ）	Cisco Webex Meetingsサーバを使用して会議を設定します。
ステップ 5	CTI サービスの設定 （43 ページ）	CTIサービスを設定し、Jabber にユーザーに関連付けられているデバイスを提供します。
ステップ 6	ユーザ（Users） （47 ページ）	Jabber のユーザを設定します。
ステップ 7	ソフトフォンの設定 （63 ページ）	ユーザ用のソフトフォンデバイスを設定します。
ステップ 8	サービス ディスカバリの設定 （91 ページ）	ユーザのサービス ディスカバリ オプションを選択します。
ステップ 9	証明書検証の設定 （103 ページ）	証明書は、Jabber クライアントが接続するサービスごとに必要です。
ステップ 10	クライアントの設定 （107 ページ）	クライアント設定ファイルに含める機能を選択します。
ステップ 11	Cisco Jabber アプリケーションおよび Jabber ソフトフォンの VDI 用の展開 （121 ページ）	ユーザのためのクライアントのインストール方法を選択します。

電話モードの展開（連絡先を使用）

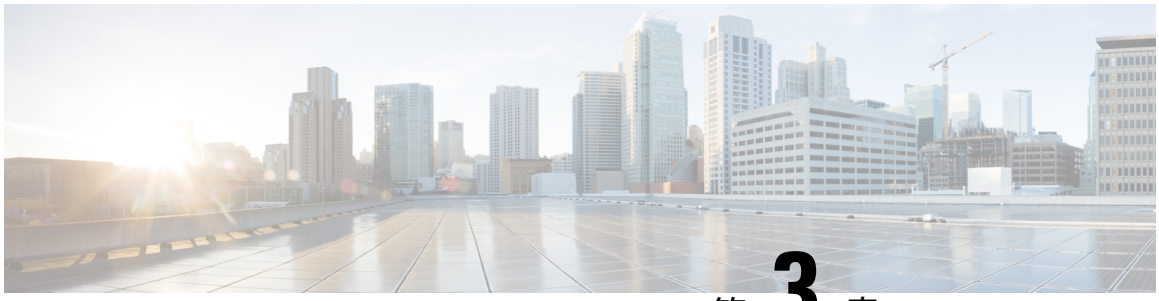
手順

	コマンドまたはアクション	目的
ステップ 1	http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html で『Cisco Jabber Planning Guide』を参照してください。	• 要件を満たしていることを確認 • 用する連絡先ソースを決定します。
ステップ 2	デフォルトサービスプロファイルの作成 （13 ページ）	サービスを追加するためのサービスプロファイルを作成します。
ステップ 3	連絡先ソース （15 ページ）	ユーザの連絡先ソースを設定します。
ステップ 4	Q&A の管理プレゼンスの設定 （30 ページ）	ユーザがクライアントにプレゼンスを持つかどうかを選択します。
ステップ 5	インスタントメッセージの設定の無効化 （29 ページ）	連絡先の展開により、この電話モードのインスタントメッセージを削除します。
ステップ 6	ボイスメールの設定 （31 ページ）	ユーザのボイスメールを設定します。
ステップ 7	Webex 会議の設定 （39 ページ）	Cisco Webex Meetingsサーバを使用して会議を設定します。
ステップ 8	CTI サービスの設定 （43 ページ）	CTIサービスを設定し、Jabber にユーザーに関連付けられているデバイスを提供します。
ステップ 9	ユーザ（Users） （47 ページ）	Jabber のユーザを設定します。
ステップ 10	ソフトフォンの設定 （63 ページ）	ユーザ用のソフトフォンデバイスを設定します。
ステップ 11	デスクフォン制御の設定 （75ページ）	デスクフォンデバイスを作成し、機能を有効にします。
ステップ 12	拡張および接続機能の設定 （83 ページ）	リモートデバイスへのコールを拡張するためにユーザにオプションを設定します。
ステップ 13	サービス ディスカバリの設定 （91 ページ）	ユーザのサービス ディスカバリ オプションを選択します。
ステップ 14	証明書検証の設定 （103 ページ）	各サーバの必要な証明書を設定します。

	コマンドまたはアクション	目的
ステップ 15	クライアントの設定 （107 ページ）	クライアント設定ファイルに含める機能を選択します。
ステップ 16	Cisco Jabber アプリケーションおよび Jabber ソフトフォンの VDI 用の展開 （121 ページ）	ユーザのためのクライアントのインストール方法を選択します。

第 II 部

サービス

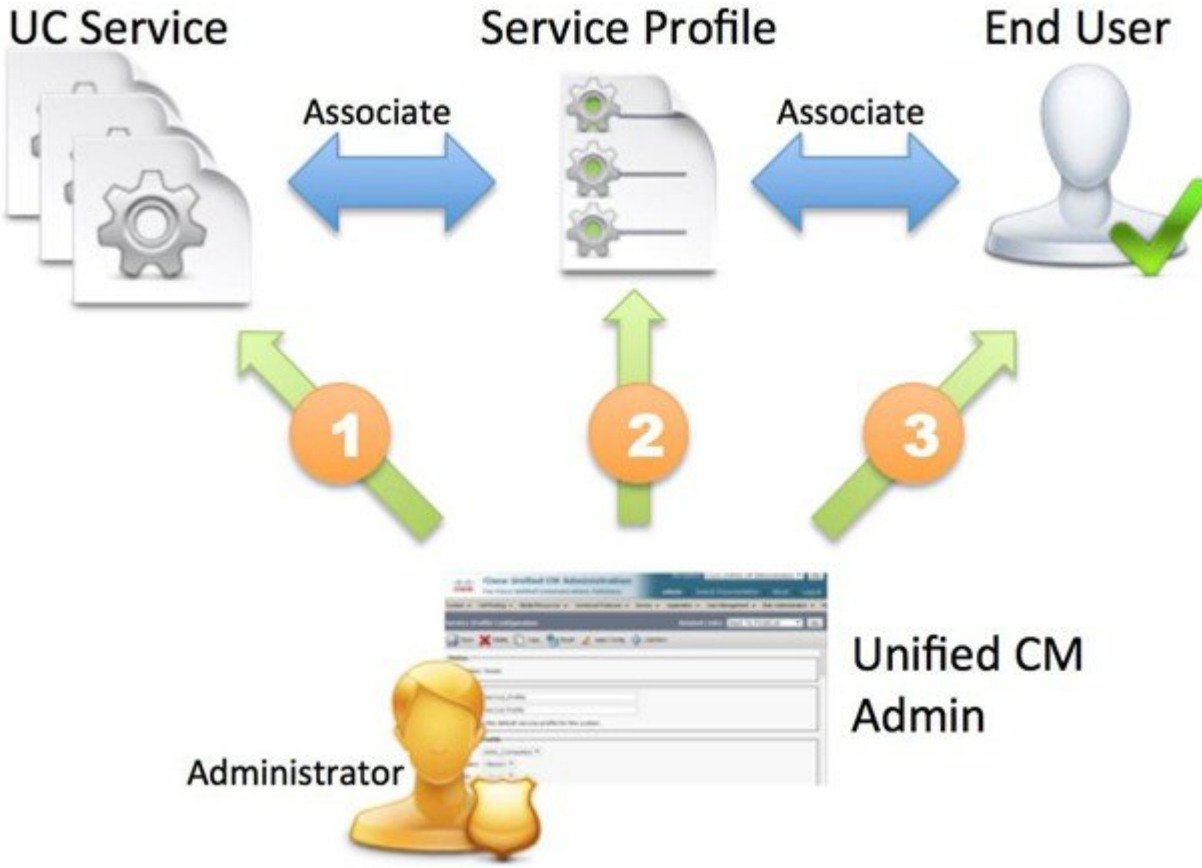


第 3 章

デフォルトサービス プロファイルの作成

サービス プロファイルの概要

図 *1:* サービス プロファイルのワークフロー



1. UC サービスの作成します。
2. UC サービスをサービス プロファイルに関連付けます。
3. ユーザをサービス プロファイルに関連付けます。

デフォルトサービス プロファイルの作成

UC サービスを追加するためのサービス プロファイルを作成します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[ユーザ管理（User Management）][> ユーザ設定（User Settings） >][サービス プロファイル（Service Profile）]** の順に選択します。
[**サービス プロファイルの検索と一覧表示（Find and List Service Profiles**）] ウィンドウが開きます。

ステップ 3 [**新規追加（Add New**）] を選択します。
[**サービス プロファイルの設定（Service Profile Configuration**）] ウィンドウが開きます。

ステップ 4 [**名前（Name**）] フィールドにサービス プロファイルの名前を入力します。

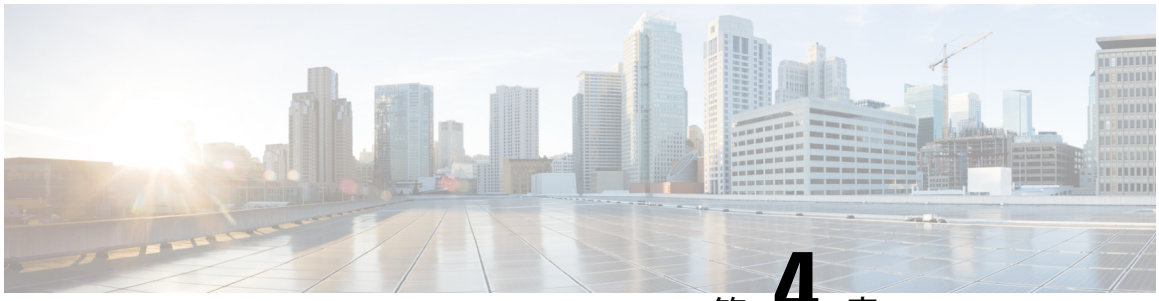
ステップ 5 サービス プロファイルをクラスタのデフォルトにする場合は、[**システム デフォルトのサービス プロファイルに設定（Make this the default service profile for the system**）] を選択します。

（注） Cisco Unified Communications Manager リリース 9.x のみ、IM 専用ユーザはデフォルトサービス プロファイルを使用する必要があります。このため、[デフォルトを使用（Use default）] を選択します。

ステップ 6 [**保存（Save**）] を選択します。

次のタスク

展開用の UC サービスを作成します。



第 4 章

連絡先ソース

連絡先ソースの設定のワークフロー

手順

	コマンドまたはアクション	目的
ステップ 1	ディレクトリ統合の設定： • サービス プロファイルでのディレクトリ統合の設定 （16 ページ） • コンフィギュレーション ファイルでのディレクトリ統合の詳細設定 （22 ページ）	Cisco Unified Communications Manager を使用してサービスプロファイル経由で、またはコンフィギュレーション ファイルを使用して、ディレクトリ統合を設定します。
ステップ 2	オプション： 写真の設定 （22 ページ）	ユーザの写真を設定するオプションについて確認します。
ステップ 3	オプション： CDI のイントラドメイン フェデレーションの設定 （23 ページ）	Cisco Jabber ユーザは、別のシステム上でプロビジョニングされたユーザや Cisco Jabber 以外のクライアント アプリケーションを使用しているユーザと通信できます。

ディレクトリ統合のためのクライアント設定

Cisco Unified Communications Manager リリース 9 以降を使用してサービス プロファイル経由で、コンフィギュレーション ファイルを使用して、ディレクトリ統合を設定できます。ここでは、ディレクトリ統合のためにクライアントを設定する方法について説明します。

次の表は、サービス プロファイルとコンフィギュレーション ファイルの両方が存在する場合に優先されるパラメータ値を示しています。

サービス プロファイル	設定ファイル	優先されるパラメータ値
パラメータ値が設定済み	パラメータ値が設定済み	サービス プロファイル
パラメータ値が設定済み	パラメータ値が空白	サービス プロファイル
パラメータ値が空白	パラメータ値が設定済み	設定ファイル
パラメータ値が空白	パラメータ値が空白	サービス プロファイルの空白（デフォルト）値

サービス プロファイルでのディレクトリ統合の設定

Cisco Unified Communications Manager リリース 9 以降では、サービス プロファイルを使用してユーザをプロビジョニングし、内部ドメイン サーバ上に `_cisco-uds` SRV レコードを展開できます。そうすれば、クライアントが自動的に Cisco Unified Communications Manager を検出して、サービス プロファイルを受け取り、ディレクトリ統合設定を取得できます。

手順

	コマンドまたはアクション	目的
ステップ 1	ディレクトリ サービスを追加する （16 ページ）	ディレクトリ UC サービスを作成します。
ステップ 2	サービス プロファイルへのディレクトリ サービスの適用 （17 ページ）	サービス プロファイルにディレクトリ UC サービスを追加します。

ディレクトリ サービスを追加する

手順

ステップ 1 **[Cisco Unified CM の管理（Cisco Unified CM Administration）]** インターフェイスを開きます。

ステップ 2 **[ユーザ管理（User Management）] > ユーザ設定（User Settings）] > UC サービス（UC Service）]** を選択します。

[**UC サービスの検索と一覧表示（Find and List UC Services**）] ウィンドウが開きます。

ステップ 3 [**新規追加（Add New**）] を選択します。
[**UC サービスの設定（UC Service Configuration**）] ウィンドウが開きます。

ステップ 4 [**UC サービス タイプ（UC Service Type**）] メニューから [**ディレクトリ（Directory**）] を選択し、[**次へ（Next**）] を選択します。

ステップ 5 ディレクトリ サービスに対して適切な値を設定します。

グローバル カタログで Cisco Jabber ディレクトリ検索を設定するには、次の値を追加します。

- [**ポート（Port**）]：3268
- [**プロトコル（Protocol**）]：TCP

ステップ 6 [**保存（Save**）] を選択します。

次のタスク

ディレクトリ サービスを適用します。

サービス プロファイルへのディレクトリ サービスの適用

手順

ステップ 1 **[ユーザ管理（User Management）][** > **ユーザ設定（User Settings）][** > **サービス プロファイル（Service Profile）]** の順に選択します。
[**サービス プロファイルの検索と一覧表示（Find and List Service Profiles**）] ウィンドウが開きます。

ステップ 2 [**新規追加（Add New**）] を選択します。
[**サービス プロファイルの設定（Service Profile Configuration**）] ウィンドウが開きます。

ステップ 3 ディレクトリ プロファイルにディレクトリ サービスを追加します。ディレクトリ プロファイルに必要な特定の設定については、「ディレクトリ プロファイル パラメータ」の項を参照してください。

ステップ 4 [**保存（Save**）] を選択します。

ディレクトリ プロファイル パラメータ

次の表は、ディレクトリ プロファイルで設定できる設定パラメータを示します。

ディレクトリ サービスの設定	説明
プライマリ サーバ（Primary server）	プライマリ ディレクトリ サーバのアドレスを指定します。 このパラメータは、クライアントが自動的にディレクトリ サーバを検出できない手動接続に必要です。
セカンダリ サーバ	バックアップ ディレクトリ サーバのアドレスを指定します。
コンタクト解決に UDS を使用（Use UDS for Contact Resolution）	クライアントが UDS を連絡先ソースとして使用するかどうかを指定します。 **True（デフォルト）** UDS を連絡先ソースとして使用します。このオプションが選択されている場合は、この表の次のパラメータが使用されません。 **いいえ（False）** CDI を連絡先ソースとして使用します。 次のパラメータはLDAPサーバへの接続に使用されます。 デフォルトで、ユーザが Expressway for Mobile and Remote Access 経由で社内ネットワークに接続するときに、UDS が連絡先解決を提供します。

ディレクトリ サービスの設定	説明
ログインしたユーザのクレデンシャルを使用（Use Logged On User Credential）	LDAPによる連絡先解決で、クライアントがログインしているユーザ名とパスワードを使用するかどうかを指定します。 Active Directory（AD）SSO を設定している場合、この設定よりも優先されます。 **True（デフォルト）** ログインしたユーザのクレデンシャルを使用します。これは、LDAP_UseCredentialsFrom パラメータの値として CUCM を使用する場合と同様です。 **いいえ（False）** ログインしたユーザのクレデンシャルを使用しないでください。 SSO が設定されている場合、Jabber は ConnectionUsername パラメータと ConnectionPassword パラメータを使用する前に、これらのクレデンシャルを使用します。 次のパラメータを使用して、ログオンユーザのクレデンシャルを指定する必要があります。 • ConnectionUsername • ConnectionPassword
Username	アントがディレククライトリ サーバで認証するために使用される共有ユーザ名を手動で指定することができます。 デフォルトでは、Cisco Jabber デスクトップ クライアントは Kerberos またはクライアント証明書認証を使用します。 このパラメータは、Kerberos またはクライアント証明書認証を使用してディレクトリ サーバで認証できない展開でのみ使用する必要があります。 読み取り専用権限を持っているアカウントの既知のまたは公開されているクレデンシャルのセットのみを使用します。

ディレクトリ サービスの設定	説明
パスワード	ディレクトリ サーバでの認証にクライアントが使用できる共有パスワードを手動で指定できるようにします。 デフォルトでは、Cisco Jabber デスクトップ クライアントは Kerberos またはクライアント証明書認証を使用します。 このパラメータは、Kerberos またはクライアント証明書認証を使用してディレクトリ サーバで認証できない展開でのみ使用する必要があります。 読み取り専用権限を持っているアカウントの既知のまたは公開されているクレデンシャルのセットのみを使用します。
検索ベース 1（Search Base 1） **検索ベース 2（Search Base 2）** **検索ベース 3（Search Base 3）** **検索ベース 4（Search Base 3）** **検索ベース 5（Search Base 3）**	検索が開始されるディレクトリ サーバの場所を指定します。つまり、検索ベースはクライアントが検索を実行するルートです。 デフォルトの場合、クライアントはディレクトリ ツリーのルートから検索を行います。デフォルトの動作を上書きする場合は、最大 3 つの検索ベースの値を OU に指定することができます。 Active Directory は、通常、検索ベースを必要としません。特定のパフォーマンス要件がある場合にのみ、Active Directory の検索ベースを指定します。 ディレクトリ内の特定の場所へのバインディングを作成するには、Active Directory 以外のディレクトリ サーバの検索ベースを指定します。 **ヒント** OU を指定すると、検索対象を特定のユーザ グループに制限することができます。 たとえば、ユーザのサブセットにはインスタント メッセージング機能だけがあります。これらのユーザを OU に含め、この OU を検索ベースとして指定します。

ディレクトリ サービスの設定	説明
すべての検索ベースで再帰検索（Recursive Search on All Search Bases）	検索ベースから始まるディレクトリの再帰検索を実行するには、このオプションを選択します。再帰検索を使用して、Cisco Jabber クライアントの連絡先検索クエリーが指定された検索コンテキスト（検索ベース）からの LDAP ディレクトリ ツリーすべてを検索できるようにします。これは、LDAP 検索と共通のオプションです。 必須フィールドです。 デフォルト値は True です。
検索タイムアウト（Search Timeout）	ディレクトリ クエリーのタイムアウト時間を秒数で指定します。 デフォルト値は 5 です。
[基本フィルタ（Base Filter）]	Active Directory クエリーの基本フィルタを指定します。 ディレクトリのサブキー名のみを指定し、ディレクトリへのクエリーの実行時にユーザ オブジェクト以外のオブジェクトを取得します。 デフォルト値は `(&(&(objectCategory=person)(objectClass=user)` です。
予測検索フィルタ（Predictive Search Filter）	予測検索クエリーに適用するフィルタを定義します。 検索クエリーをフィルタするために、複数のカンマ区切り値を定義できます。 デフォルト値は `ANR` です。 Cisco Jabber が予測検索を実行するときに、Ambiguous Name Resolution（ANR）を使用してクエリーを発行します。このクエリーにより、検索文字列が明確化され、ディレクトリ サーバ上で ANR に対して設定された属性に合致する結果が返されます。 **重要** クライアントに ANR の属性を検索させる場合は、その属性を設定するようにディレクトリ サーバを設定します。

属性のマッピング

サービス プロファイルでデフォルトの属性マッピングを変更することはできません。デフォルトの属性マッピングを変更するには、クライアントの設定ファイルで必要なマッピングを定義しなければなりません。

写真の設定

Cisco Jabber は、次の方法を使用してユーザの写真を設定します。

- **Active Directory のバイナリ オブジェクト**：設定は不要です。Cisco Jabber は thumbnailPhoto 属性からバイナリ写真を取得します。
- **PhotoURL 属性**：jabber-config.xmlファイルで PhotoSource パラメータを使用し、ディレクトリの属性を指定します。クライアントは属性を取得し、URL またはバイナリ データであるかどうかを判断し、いずれかのソースの写真を表示します。

  CDI パラメータ：PhotoSource

  例：

  ```
  <Directory>
   <PhotoSource>url</PhotoSource>
  </Directory>
  ```

- **URI 代替**：ディレクトリ サーバ タイプに対しては、jabber-config.xml ファイルで次のパラメータを使用します。

  CDI パラメータ：

  - PhotoUriSubstitutionEnabled
  - PhotoUriWithToken
  - PhotoUriSubstitutionToken

  例：

  ```
  <PhotoUriSubstitutionEnabled>True</PhotoUriSubstitutionEnabled>
  <PhotoUriSubstitutionToken>sAMAccountName</PhotoUriSubstitutionToken>
  <PhotoUriWithToken>http://example.com/photo/sAMAccountName.jpg</PhotoUriWithToken>
  ```

  UDS パラメータ：

  - UdsPhotoUriSubstitutionEnabled
  - UdsPhotoUriWithToken
  - UdsPhotoUriSubstitutionToken

  例：

  ```
  <UDSPhotoUriSubstitutionEnabled>True</UDSPhotoUriSubstitutionEnabled>
  <UDSPhotoUriSubstitutionToken>sAMAccountName</UDSPhotoUriSubstitutionToken>
  <UDSPhotoUriWithToken>http://example.com/photo/sAMAccountName.jpg</UDSPhotoUriWithToken>
  ```

コンフィギュレーション ファイルでのディレクトリ統合の詳細設定

Cisco Jabber コンフィギュレーション ファイルでディレクトリ統合を設定できます。詳細については、『*Parameters Reference Guide for Cisco Jabber*』の「*Directory*」の章を参照してください。

重要 サービス プロファイルとコンフィギュレーション ファイルが存在する場合は、常に、サービス プロファイル内の設定が優先されます。

フェデレーション

フェデレーションを使用すれば、Cisco Jabber ユーザは、別のシステム上でプロビジョニングされたユーザや Cisco Jabber 以外のクライアント アプリケーションを使用しているユーザと通信できます。

CDI のイントラドメイン フェデレーションの設定

プレゼンス サーバでのイントラドメイン フェデレーションの設定に加えて、Cisco Jabber コンフィギュレーション ファイルでいくつかの設定が必要になる場合があります。

連絡先の検索時に連絡先を解決したり、ディレクトリから連絡先情報を取得したりするには、Cisco Jabber で各ユーザの連絡先 ID が必要です。Cisco Unified Communications Manager IM & Presence サーバでは、特定の形式を使用して連絡先情報を解決しますが、この形式は、Microsoft Office Communications Server や Microsoft Live Communications Server などの他のプレゼンス サーバの形式と常に一致するわけではありません。

手順

ステップ 1 UseSIPURIToResolveContacts パラメータの値を true に設定します。

ステップ 2 クライアントが連絡先情報を取得するために使用する Cisco Jabber 連絡先 ID を含む属性を指定します。デフォルト値は `msRTCSIP-PrimaryUserAddress` です。また、SipUri パラメータで別の属性を指定することもできます。

（注） イントラドメインフェデレーションを展開して、クライアントがファイアウォールの外側から Expressway for Mobile and Remote Access に接続しているときは、次のいずれかの形式が連絡先 ID に使用されている場合にのみ連絡先検索がサポートされます。

- sAMAccountName@domain
- UserPrincipleName(UPN)@domain
- EmailAddress@domain
- employeeNumber@domain
- phoneNumber@domain

ステップ 3 UriPrefix パラメータで、SipUri パラメータ内の連絡先 ID の前に付けるプレフィックス テキストを指定します。

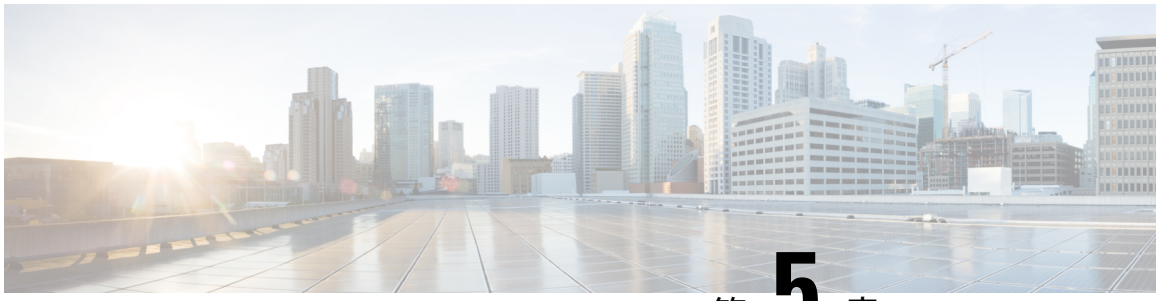
例：

たとえば、SipUri の値として msRTCSIP-PrimaryUserAddress を指定します。ディレクトリにおける各ユーザの msRTCSIP-PrimaryUserAddress の値は、sip:*username@domain* の形式になります。

例

次の XML スニペットに、設定の例を示します。

```
<Directory>
  <UseSIPURIToResolveContacts>true</UseSIPURIToResolveContacts>
  <SipUri>non-default-attribute</SipUri>
  <UriPrefix>sip:</UriPrefix>
</Directory>
```



第 5 章

インスタント メッセージングとプレゼンス サービスの設定

Cisco Unified Communications Manager リリース 10.5 以降を使用した IM and Presence サービス ワークフロー

手順

	コマンドまたはアクション	目的
ステップ 1	IM アドレス スキームの設定 （28 ページ）	ユーザの IM アドレスを設定します。
ステップ 2	メッセージの設定の有効化 （29 ページ）	Cisco Unified Communications IM and Presence サービスで、インスタント メッセージとロギングを有効にするオプションを設定します。

Cisco Unified Communications Manager リリース 9.x 以降を使用した IM and Presence サービス ワークフロー

手順

	コマンドまたはアクション	目的
ステップ 1	メッセージの設定の有効化 （29 ページ）	Cisco Unified Communications IM and Presence サービスで、インスタントメッセージとロギングを有効にするオプションを設定します。
ステップ 2	IM and Presence サービスの追加 （26 ページ）	IM and Presence UC サービスを作成します。
ステップ 3	IM and Presence サービスの適用 （27 ページ）	サービス プロファイルに IM and Presence UC サービスを追加します。

IM and Presence サービスの追加

IM and Presence サービス機能をユーザに提供します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [UC サービス（UC Service）]** を選択します。

[UC サービスの検索と一覧表示（Find and List UC Services）] ウィンドウが開きます。

ステップ 3 [新規追加（Add New）] を選択します。

[UC サービスの設定（UC Service Configuration）] ウィンドウが開きます。

ステップ 4 [UC サービスの追加（Add a UC Service）] セクションで、[UC サービス タイプ（UC Service Type）] ドロップダウン リストから [IM および Presence（IM and Presence）] を選択します。

ステップ 5 [次へ（Next）] を選択します。

ステップ 6 次のように IM and Presence サービスの詳細を入力します。

a) [製品のタイプ（Product Type）] ドロップダウン リストから [Unified CM (IM および Presence)（Unified CM (IM and Presence)）] を選択します。

b) [名前（Name）] フィールドにサービスの名前を入力します。

入力した名前は、プロファイルにサービスを追加する際に表示されます。入力する名前は必ず、一意的でわかりやすく、かつ意味が通じるものにしてください。

c) 必要であれば、[説明（Description）] フィールドに説明を入力します。

d) [ホスト名/IP アドレス（Host Name/IP Address）] フィールドに、インスタント メッセージ/プレゼンス サービスのアドレスを入力します。

重要 サービスのアドレスは完全修飾ドメイン名またはIPアドレスである必要があります。

ステップ 7 [保存（Save）] を選択します。

IM and Presence サービスの適用

Cisco Unified Communications Manager で IM and Presence サービスを追加したら、クライアントが設定を取得できるようにそのサービスをサービス プロファイルに適用する必要があります。

始める前に

IM and Presence サービスの追加 （26 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [サービス プロファイル（Service Profile）]** の順に選択します。

[サービス プロファイルの検索と一覧表示（Find and List Service Profiles）] ウィンドウが開きます。

ステップ 3 目的のサービス プロファイルを検索し、それを選択します。

[サービス プロファイルの設定（Service Profile Configuration）] ウィンドウが開きます。

ステップ 4 [IM/プレゼンス プロファイル（IM and Presence Profile）] セクションで、次のドロップダウン リストから、サービスを最大 3 つ選択します。

- **Primary**
- **セカンダリ**
- **ターシャリ（Tertiary）**

ステップ 5 **保存**をクリックします。

IM アドレス スキームの設定

この機能は、Cisco Unified Communications Manager IM and Presence サービス リリース 10.x 以降でサポートされます。Cisco Unified Communications Manager IM and Presence サービス リリース 9.x 以前のバージョンで使用されるデフォルト IM アドレス スキームは、UserID@[Default Domain] です。

手順

ステップ 1 [IM アドレス スキーム（IM Address Scheme）] を選択します。

a) [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] を開きます。

b) **[プレゼンス（Presence）] > [設定（Settings）] > [詳細設定（Advanced Configuration）]** を選択します。
[プレゼンスの詳細設定（Advanced Presence Settings）] ウィンドウが開きます。

c) [IM アドレス スキーム（IM Address Scheme）] を選択し、リストから次のいずれかを選択します。

- UserID@[Default Domain]

  ユーザ ID を使用する場合は、デフォルト ドメインが設定されていることを確認します。たとえば、サービスには `cups` ではなく、`cups.com` という名前を付ける必要があります。

- Directory URI

ステップ 2 必要なマッピングを選択します。

a) [Cisco Unified CM の管理（Cisco Unified CM Administration）] を開きます。

b) **[システム（System）] > [LDAP] > [LDAP ディレクトリ（LDAP Directory）]** を選択します。
[LDAP ディレクトリの検索と一覧表示（Find and List LDAP Directories）] ウィンドウが開きます。

c) リストからディレクトリを検索して選択します。
[LDAP ディレクトリ（LDAP Directory）] ウィンドウが開きます。

d) [同期対象の標準ユーザ フィールド（Standard User Fields To Be Synchronized）] セクションで、マッピングを選択します。

- LDAP フィールドにマッピングされるユーザ ID。デフォルトは **sAMAccountName** です。

- **mail** と **msRTCSIP-primaryuseraddress** のどちらかにマッピングされるディレクトリ URI。

メッセージの設定の有効化

インスタント メッセージング機能を有効にし、設定します。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] インターフェイスを開きます。

ステップ 2 **[メッセージング（Messaging）]** > **[設定（Settings）]** の順に選択します。

ステップ 3 次のオプションを選択します。

- **インスタント メッセージを有効にする（Enable instant messaging）**
- **クライアントでのインスタント メッセージ履歴のログ記録を可能にする（Allow clients to log instant message history）**
- **インスタント メッセージでの切り取り/貼り付けを可能にする（Allow cut & paste in instant messages）**

ステップ 4 他のメッセージング設定も適切に選択します。

ステップ 5 [保存（Save）] を選択します。

重要 Cisco Jabber は、Cisco Unified Communications Manager IM and Presence サービス リリース 9.0.x の [プレゼンスの設定（Presence Settings）] ウィンドウで次の設定をサポートしません。

- **[ユーザの通話中に DND ステータスを使用する（Use DND status when user is on the phone）]**
- **[ユーザがミーティングに参加しているときに DND ステータスを使用する（Use DND status when user is in a meeting）]**

次のタスク

- Cisco Unified Communications Manager IM and Presence サービス リリース 9.x 以降を使用している場合は、IM and Presence サービスの追加 （26 ページ）。

インスタントメッセージの設定の無効化

連絡先を展開する電話モードでは、インスタントメッセージが電話モードでの展開に適用されないため、ユーザのインスタント メッセージをオフにすることができます。

手順

ステップ 1 [**Cisco Unified CM IMおよびプレゼンス管理（Cisco Unified CM IM and Presence Administration**）] から、**[メッセージ（Messaging**）**] [** > **設定（Settings**）**]**に移動します。

ステップ 2 [**インスタント メッセージを有効にする（Enable instant messaging**）] をオフにし[**保存（Save**）] をクリックします。

次のタスク

Cisco XCP Router サービスを再起動します。

Q&A の管理プレゼンスの設定

ユーザのプレゼンス設定は、デフォルトで有効になっています。ただし、連絡先展開を使用した電話モードでは、プレゼンス設定を無効にしても、そのユーザはクライアントに表示されません。

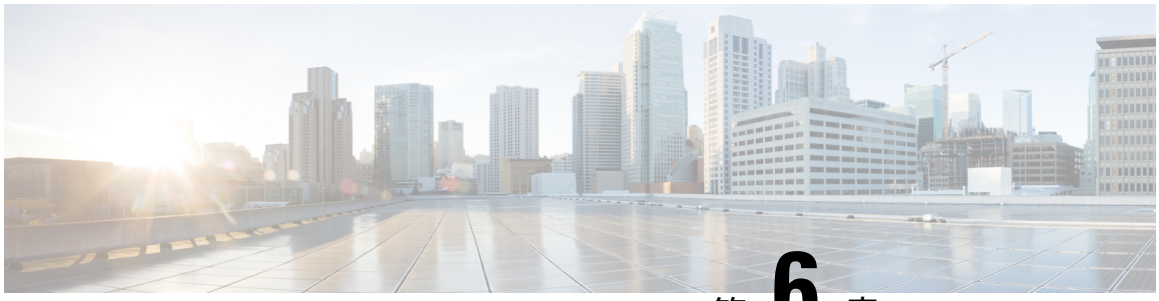
手順

ステップ 1 [**Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration**）] から、 **[プレゼンス（Presence**）**][** > **設定（Settings**）**][** > **標準設定（Standard Configuration**）**]** に移動します。

ステップ 2 [**プレゼンス ステータスの共有を有効にする（Enable availability sharing**）] をオフにして[**保存（Save**）]をクリックします。

次のタスク

Cisco XCP Router サービスを再起動します。



第 6 章

ボイスメールの設定

ボイスメール ワークフローの設定

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Jabber で使用する Cisco Unity Connection の設定 （32 ページ）	Cisco Jabber がボイスメール サービスにアクセスできるように、Cisco Unity Connection を設定します。
ステップ 2	取得とリダイレクションの設定 （33 ページ）	ユーザがボイスメール メッセージにアクセスできるように、取得を設定します。ユーザが着信コールをボイスメールに送信できるようにするために、リダイレクションを設定します。
ステップ 3	ボイスメール サービスを追加する （35 ページ）	ボイスメール UC サービスを追加します。Jabber はこの情報を使ってボイスメール サーバに接続します。
ステップ 4	ボイスメール サービスの適用 （36 ページ）	サービス プロファイルにボイスメール UC サービスを適用します。
ステップ 5	ボイスメールのクレデンシャル ソースの設定 （37 ページ）	ボイスメール サーバに接続するためのクレデンシャルを設定します。

Cisco Jabber で使用する Cisco Unity Connection の設定

Cisco Jabber がボイスメール サービスにアクセスできるように、Cisco Unity Connection を設定するための特定の手順を実行する必要があります。ユーザ、パスワードの作成、ユーザへのボイスメール アクセスのプロビジョニングなどの一般タスクの手順については、Cisco Unity Connection のマニュアルを参照してください。

メモ　Cisco Jabber は、REST インターフェイスを介してボイスメール サービスに接続し、Cisco Unity Connection リリース 8.5 以降をサポートします。

手順

ステップ 1　[Connection Jetty] および [Connection REST Service] サービスが開始していることを確認します。

a) [Cisco Unity Connection のサービスアビリティ（Cisco Unity Connection Serviceability）] インターフェイスを開きます。
b) **[ツール（Tools）] > [サービスの管理（Service Management）]** を選択します。
c) [オプションのサービス（Optional Services）] セクションで、次のサービスを検索します。
   - **[Connection Jetty]**
   - **[Connection REST Service]**
d) 必要に応じて、サービスを開始します。

ステップ 2　[Cisco Unity Connection の管理（Cisco Unity Connection Administration）] インターフェイスを開きます。

ステップ 3　ユーザのパスワード設定を編集します。

a) **[ユーザ（Users）]** を選択します。
b) 適切なユーザを選択します。
c) **[編集（Edit）] > [パスワードの設定（Password Settings）]** を選択します。
d) [パスワードの選択（Choose Password）] メニューから [Web アプリケーション（Web Application）] を選択します。
e) [次回サインイン時に、ユーザによる変更が必要（User Must Change at Next Sign-In）] をオフにします。
f) [保存（Save）] を選択します。

ステップ 4　ユーザに Web Inbox へのアクセスを付与します。

a) [サービス クラス（Class of Service）] を選択します。

   [サービス クラスの検索（Search Class of Service）] ウィンドウが開きます。

b) 適切なサービス クラスを選択するか、サービスの新しいクラスを追加します。

c) [Web Inbox と RSS フィードの使用をユーザに許可する（Allow Users to Use the Web Inbox and RSS Feeds）] を選択します。
d) [機能（Features）] セクションで、[ボイスメールへのアクセスに Unified Client の使用をユーザに許可する（Allow Users to Use Unified Client to Access Voice Mail）] を選択します。
e) 必要に応じて、その他のすべてのオプションを選択します。
f) [保存（Save）] を選択します。

ステップ 5 [API の設定（API configuration）] を選択します。

a) **[システム設定（System Settings）] > [詳細設定（Advanced）] > [API 設定（API Settings）]** を選択します。

[API の設定（API Configuration）] ウィンドウが開きます。

b) 次のオプションを選択します。

- **CUMI を介したセキュア メッセージ録音へのアクセスを許可する（Allow Access to Secure Message Recordings through CUMI）**
- **[CUMIを介してセキュアメッセージのメッセージヘッダー情報を表示する（Display Message Header Information of Secure Messages through CUMI）]**
- **CUMI 経由のメッセージ添付ファイルを許可する（Allow Message Attachments through CUMI）**

c) [保存（Save）] を選択します。

次のタスク

Cisco Unified Communications Manager リリース 9.x 以降を使用している場合は、ボイスメール サービスを追加する （35 ページ）。

取得とリダイレクションの設定

ユーザがクライアント インターフェイスでボイスメール メッセージにアクセスできるように取得を設定します。ユーザが着信コールをボイスメールに送信できるようにするために、リダイレクションを設定します。Cisco Unified Communications Manager で取得とリダイレクションを設定します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 ボイスメール パイロットを設定します。

a) **[拡張機能（Advanced Features）] > [ボイスメール（Voice Mail）] > [ボイスメール パイロット（Voice Mail Pilot）]** の順に選択します。

[ボイスメール パイロットの検索と一覧表示（Find and List Voice Mail Pilots）] ウィンドウが開きます。

b) [新規追加（Add New）] を選択します。

[ボイスメール パイロットの設定（Voice Mail Pilot Configuration）] ウィンドウが開きます。

c) [ボイスメール パイロットの設定（Voice Mail Pilot Configuration）] ウィンドウで必要な詳細情報を指定します。

d) [保存（Save）] を選択します。

ステップ 3 ボイスメール パイロットをボイスメール プロファイルに追加します。

a) **[拡張機能（Advanced Features）] > [ボイスメール（Voice Mail）] > [ボイスメール プロファイル（Voice Mail Profile）]** の順に選択します。

[ボイスメールプロファイルの検索/一覧表示（Find and List Voicemail Profiles）] ウィンドウが開きます。

b) [次のボイスメール プロファイル名でボイスメール プロファイルを検索（Find Voice Mail Profile where Voice Mail Profile Name）] フィールドに適切なフィルタを指定し、[検索（Find）] を選択してプロファイルの一覧を取得します。

c) 対象のプロファイルを一覧から選択します。

[ボイスメール パイロットの設定（Voice Mail Pilot Configuration）] ウィンドウが開きます。

d) [ボイスメール パイロット（Voice Mail Pilot）] ドロップダウン リストでボイスメール パイロットを選択します。

e) [保存（Save）] を選択します。

ステップ 4 電話番号設定でボイスメール プロファイルを指定します。

a) **[デバイス（Device）] > [電話（Phone）]** の順に選択します。

[電話の検索と一覧表示（Find and List Phones）] ウィンドウが開きます。

b) [電話を次の条件で検索（Find Phone where）] フィールドに適切なフィルタを指定し、[検索（Find）] を選択してデバイスの一覧を取得します。

c) 対象のデバイスを一覧から選択します。

[電話の設定（Phone Configuration）] ウィンドウが開きます。

d) [割り当て情報（Association Information）] セクションを探します。

e) 適切なデバイス番号を選択します。

[電話番号設定（Directory Number Configuration）] ウィンドウが開きます。

f) [電話番号の設定（Directory Number Settings）] セクションを探します。

g) [ボイスメール プロファイル（Voice Mail Profile）] ドロップダウン リストからボイスメール プロファイルを選択します。

h) [保存（Save）] を選択します。

次のタスク

ボイスメールのクレデンシャル ソースの設定 （37 ページ）

ボイスメール サービスを追加する

ボイスメール サービスを追加して、ユーザがボイス メッセージを受信できるようにします。

始める前に

Cisco Jabber で使用する Cisco Unity Connection の設定 （32 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [UC サービス（UC Service）]** を選択します。
[UC サービスの検索と一覧表示（Find and List UC Services）] ウィンドウが開きます。

ステップ 3 [UCサービスの検索/一覧表示（Find and List UC Services）] ウィンドウで、[新規追加（Add New）] を選択します。
[UC サービスの設定（UC Service Configuration）] ウィンドウが開きます。

ステップ 4 [UCサービスの追加（Add a UC Service）] セクションで、[UCサービスタイプ（UC Service Type）] ドロップダウン リストから [ボイスメール（Voicemail）] を選択して、[次へ（Next）] を選択します。

ステップ 5 ボイスメール サービスの詳細を次のように指定します。

- [製品タイプ（Product Type）]：[Unity Connection] を選択します。
- [名前（Name）]：PrimaryVoicemailServer などのサーバの記述名を入力します。
- [ホスト名/IPアドレス（Hostname/IP Address）]：ボイスメール サーバの IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。
- [ポート（Port）]：ポート番号を指定する必要はありません。 デフォルトでは、クライアントは常にポート 443 を使用して、ボイスメール サーバに接続します。そのため、ユーザが指定する値は有効になりません。
- [プロトコルタイプ（Protocol Type）]：値を指定する必要はありません。デフォルトでは、クライアントは常に HTTPS を使用して、ボイスメール サーバに接続します。そのため、ユーザが指定する値は有効になりません。

ステップ 6 [保存（Save）] を選択します。

次のタスク

ボイスメール サービスの適用 （36 ページ）

ボイスメール サービスの適用

Cisco Unified Communications Manager でボイスメール サービスを追加した後、クライアントがその設定を取得できるようにするために、そのボイスメール サービスをサービス プロファイルに適用します。

（注） Cisco Jabber は、電話モードのみで展開している場合はボイスメール UC サービス プロファイルを読み取りません。

Cisco Jabber がボイスメール サーバ情報を取得できるようにするには、`jabber-config.xml` ファイルをボイスメール パラメータで更新します。

```
<Voicemail>
<VoicemailService_UseCredentialsFrom>phone</VoicemailService_UseCredentialsFrom>
<VoicemailPrimaryServer>X.X.X.X</VoicemailPrimaryServer>
</Voicemail>
```

更新が完了したら、すべての Cisco Unified Communications Manager TFTP サーバに `jabber-config.xml` ファイルをアップロードし、TFTP サーバ ノードで TFTP サービスを再起動します。Jabber クライアントをリセットします。

始める前に

ボイスメール サービスを追加する （35 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [サービス プロファイル（Service Profile）]** の順に選択します。

[サービス プロファイルの検索と一覧表示（Find and List Service Profiles）] ウィンドウが開きます。

ステップ 3 目的のサービス プロファイルを検索し、それを選択します。

[サービス プロファイルの設定（Service Profile Configuration）] ウィンドウが開きます。

ステップ 4 [ボイスメール プロファイル（Voicemail Profile）] セクションで、以下のような設定を行います。

a) 次のドロップダウン リストから、サービスを最大 3 つ選択します。

- **Primary**
- セカンダリ
- ターシャリ（**Tertiary**）

b) [ボイスメールサービスのクレデンシャルソース（Credentials source for voicemail service）] で、次のいずれかを選択します。

- [Unified CM - IM and Presence（Unified CM - IM and Presence）]：インスタント メッセージおよびプレゼンスのクレデンシャルを使用してボイスメール サービスにサインインします。このため、ユーザはクライアントでボイスメール サービスのクレデンシャルを入力する必要ありません。
- [Web会議（Web conferencing）]：会議クレデンシャルを使用してボイスメール サービスにサインインする、このオプションはサポートされません。現時点では、会議クレデンシャルとは同期できません。
- [未設定（Not set）]：このオプションは、電話モード展開の場合に選択されます。

ステップ 5 **保存**をクリックします。

ボイスメールのクレデンシャル ソースの設定

ユーザのボイスメールのクレデンシャル ソースを指定できます。

ヒント ハイブリッド クラウドベース展開では、VoiceMailService_UseCredentialsForm パラメータを使用して、コンフィギュレーション ファイルの一部としてボイスメールのクレデンシャル ソースを設定できます。

始める前に

取得とリダイレクションの設定 （33 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [サービス プロファイル（Service Profile）]** の順に選択します。

ステップ 3 適切なサービス プロファイルを選択し、[サービス プロファイルの設定（Service Profile Configuration）] ウィンドウを開きます。

ステップ 4 [ボイスメールのプロファイル（Voicemail Profile）] セクションの [ボイスメール サービスの認証情報ソース（Credentials source for voicemail service）] ドロップダウン リストから、[Unified CM - IM およびプレゼンス（Unified CM - IM and Presence）] を選択します。

（注） [ボイスメール サービスの認証情報ソース（Credentials source for voicemail service）] ドロップダウン リストから [Web カンファレンシング（Web Conferencing）] を選択しないでください。ボイスメール サービスのクレデンシャル ソースとして会議のクレデンシャルは現時点では使用できません。

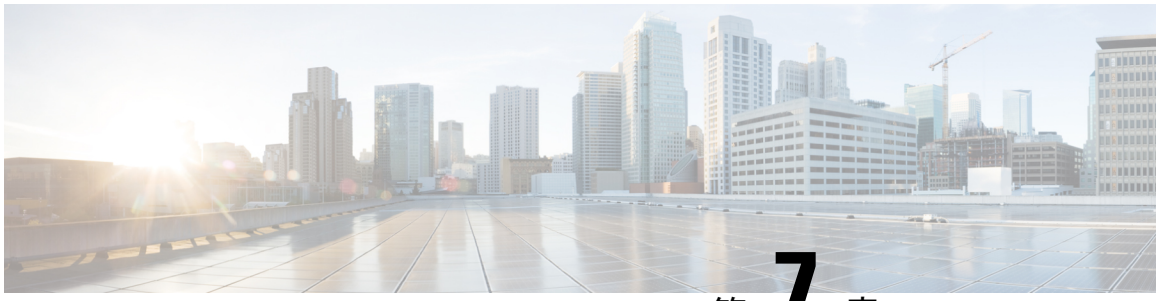
ユーザのインスタントメッセージングおよびプレゼンスのクレデンシャルは、ユーザのボイスメールクレデンシャルに一致します。このため、ユーザは、クライアントユーザインターフェイスでボイスメール クレデンシャルを指定する必要はありません。

次のタスク

重要 サーバ間でクレデンシャルを同期するメカニズムはありません。クレデンシャル ソースを指定する場合、それらのクレデンシャルがユーザのボイスメール クレデンシャルに一致することを確認する必要があります。

たとえば、ユーザのインスタント メッセージおよびプレゼンスのクレデンシャルとユーザの Cisco Unity Connection クレデンシャルが一致するように指定します。ユーザのインスタント メッセージおよびプレゼンスの各クレデンシャルが変更されたとします。この場合、そのユーザの Cisco Unity Connection クレデンシャルは、変更内容に合わせて更新する必要があります。

クラウド ベースの展開では、設定ファイルのパラメータ VoicemailService_UseCredentialsFrom を使用できます。Cisco Unified Communications Manager クレデンシャルを使用して Cisco Unity Connection にサインインするには、このパラメータの値を `phone` に設定します。



第 7 章

Webex 会議の設定

オンプレミス展開用の会議の設定

Cisco Jabber 用のオンプレミス展開を実装すると、Cisco Webex Meetings サーバを使用したオンプレミス、またはCisco Webex Meetings センターでのクラウドによる会議を設定できます。

Webex Meetings サーバを使用したオンプレミス会議の設定

手順

	コマンドまたはアクション	目的
ステップ 1	認証 Cisco Webex Meetings サーバ （40 ページ）。	
ステップ 2	ServerCisco Unified Communications Manager 上でのCisco Webex Meetingsサーバの追加 （40 ページ）。	

認証 Cisco Webex Meetings サーバ

手順

Cisco Webex Meetings サーバを使用して認証するには、次のオプションのいずれかを完了します。

- Cisco Webex Meetings サーバを使用したシングル サインオン（SSO）を SSO 環境に統合するように設定します。この場合は、Cisco Webex Meetings サーバを使用して認証するためのユーザのクレデンシャルを指定する必要がありません。
- Cisco Unified Communications Manager 上にクレデンシャル ソースを設定します。Cisco Webex Meetings サーバ用のユーザ クレデンシャルが Cisco Unified Communications Manager IM and Presence サービスまたは Cisco Unity Connection 用のクレデンシャルと一致する場合は、クレデンシャル ソースを設定できます。その後、クライアントはユーザのクレデンシャルのソースを使用してCisco Webex Meetings サーバで自動的に認証を受けます。
- ユーザにはクライアントでクレデンシャルを手動で入力するように指示します。

次のタスク

ServerCisco Unified Communications Manager 上でのCisco Webex Meetingsサーバの追加 （40 ページ）

ServerCisco Unified Communications Manager 上でのCisco Webex Meetingsサーバの追加

Cisco Unified Communications Manager で会議を設定するには、Cisco Webex Meetingsサーバを追加する必要があります。

始める前に

Cisco Webex Meetingsサーバでの認証

手順

ステップ 1 **Cisco Unified CM の管理**インターフェイスを開いて、**[ユーザ管理（User Management）]** > **[ユーザ設定（User Settings）]** > **[USサービス（UC Service）]** の順に選択します。
[UC サービスの検索と一覧表示（Find and List UC Services）] ウィンドウが開きます。

ステップ 2 [新規追加（Add New）] を選択します。

ステップ 3 [UCサービスの追加（Add a UC Service）] セクションで、[UCサービスタイプ（UC Service Type）] ドロップダウン リストから、[会議（Conferencing）] を選択してから、[次へ（Next）] を選択します。

ステップ 4 次のフィールドに入力します。

- [**製品タイプ（Product Type）**] : [Webex**(会議)（(Conferencing)）**] を選択します。
- [名前（Name）] : 設定の名前を入力します。 指定した名前は、プロファイルにサービスを追加するときに表示されます。入力する名前は必ず、一意的でわかりやすく、かつ意味が通じるものにしてください。
- [**ホスト名/IPアドレス（Hostname/IP Address）**] : Cisco Webex Meetingsサーバのサイト URL を入力します。この URL は大文字と小文字が区別され、Cisco Webex Meetingsサーバでサイト URL に設定されたケースと一致する必要があります。
- [ポート（Port）] : デフォルト値のままにします。
- [プロトコル（Protocol）] : [HTTPS] を選択します。

ステップ 5 Cisco Webexをシングル サインオン（SSO）アイデンティティ プロバイダーとして使用するには、[**SSO IDプロバイダーとしてのユーザWeb会議サーバ（User web conference server as SSO identity provider**）] をオンにします。

（注） このフィールドは、[**製品のタイプ（Product Type**）] ドロップダウン リストから [Webex（**会議**）（**(Conferencing)**）] を選択した場合にのみ有効です。

ステップ 6 [保存（Save）] を選択します。

次のタスク

サービス プロファイルに Cisco Webex Meetings サーバを追加する （41 ページ）

サービス プロファイルに Cisco Webex Meetings サーバを追加する

Cisco Webex Meetingsサーバを追加して、それをサービス プロファイルに追加すると、クライアントが会議機能にアクセスできるようになります。

始める前に

サービス プロファイルを作成します。

ServerCisco Unified Communications Manager 上でのCisco Webex Meetingsサーバの追加 （40 ページ）

手順

ステップ 1 **Cisco Unified CM** の管理インターフェイスを開いて、**[ユーザ管理（User Management）]** > **[ユーザ設定（User Settings）]** > **[サービスプロファイル（Service Profile）]** の順に選択します。

ステップ 2 目的のサービス プロファイルを検索し、それを選択します。

ステップ 3 [**会議プロファイル（Conferencing Profile**）] セクションで、[**プライマリ（Primary**）]、[**セカンダリ（Secondary**）]、および [**ターシャリ（Tertiary**）] の各ドロップダウン リストから、最大3つのCisco Webex Meetingsサーバのインスタンスを選択します。

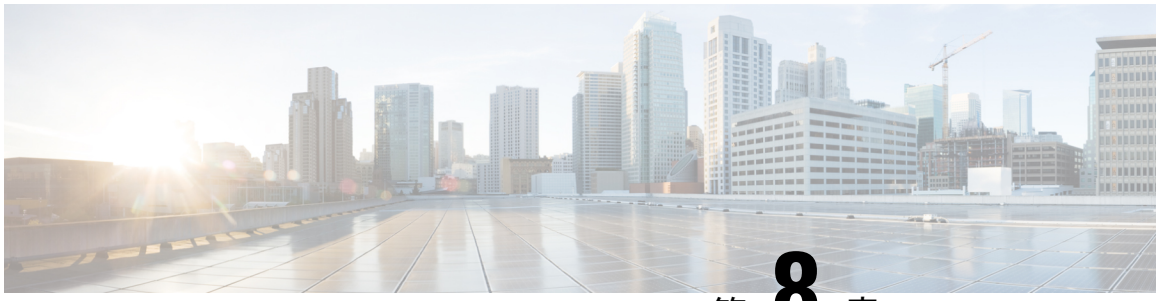
ステップ 4 [サーバ証明書の確認（Server Certificate Verification）] ドロップダウン リストから、該当する値を選択します。

ステップ 5 [Web会議サービスの資格情報ソース（Credentials source for web conference service）] ドロップダウン リストから、次のいずれかを選択します。

- [**未設定（Not set**）]：このオプションは、ユーザがCisco Webex Meetingsサーバ クレデンシャルと一致するクレデンシャル ソースを持っていない場合、または会議サイトで SSO が使用されている場合に選択します。
- [**Unified CM - IM and Presence**]：このオプションは、ユーザの Cisco Unified Communications Manager IM and Presence サービス クレデンシャルがCisco Webex Meetingsサーバ クレデンシャルと一致する場合に選択します。
- [**ボイスメール（Voicemail**）]：このオプションは、ユーザの Cisco Unity Connection クレデンシャルがCisco Webex Meetingsサーバ クレデンシャルと一致する場合に選択します。

（注） Cisco Unified Communications Manager で指定するクレデンシャルとCisco Webex Meetings サーバで指定するクレデンシャルを同期させることはできません。たとえば、あるユーザのインスタント メッセージおよびプレゼンスのクレデンシャルをそのCisco Webex Meetingsサーバ クレデンシャルと同期させるように指定した場合は、ユーザのインスタントメッセージおよびプレゼンスのクレデンシャルが変更されます。その変更に合わせてそのユーザのCisco Webex Meetingsサーバ クレデンシャルを更新する必要があります。

ステップ 6 [保存（Save）] を選択します。



第 8 章

CTI サービスの設定

CTI サービス ワークフローの設定

CTI サービスは、Jabber に UDS デバイス サービスの場所を提供します。UDS デバイス サービスは、たとえばソフトフォンやデスクフォンデバイスなどの、ユーザに関連付けられているデバイスのリストを Jabber に提供します。

手順

	コマンドまたはアクション	目的
ステップ 1	CTI サービスを追加する （43 ページ）	Jabber に CTI サービスの場所を提供する CTI UC サービスを作成します。
ステップ 2	CTI サービスの適用 （44 ページ）	サービス プロファイルに CTI UC サービスを適用します。

CTI サービスを追加する

CTI サービスは、Jabber に UDS デバイス サービスのアドレスを提供します。UDS デバイス サービスは、ユーザに関連付けられているデバイスのリストを提供します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [UC サービス（UC Service）]** を選択します。

[UC サービスの検索と一覧表示（Find and List UC Services）] ウィンドウが開きます。

ステップ 3 [新規追加（Add New）] を選択します。

[UC サービスの設定（UC Service Configuration）] ウィンドウが開きます。

ステップ 4 [UC サービスの追加（Add a UC Service）] セクションで、[UC サービス タイプ（UC Service Type）] ドロップダウン リストから [CTI] を選択します。

ステップ 5 [次へ（Next）] を選択します。

ステップ 6 次の手順に従って、CTI サービスの詳細情報を設定します。

a) [名前（Name）] フィールドにサービスの名前を入力します。

入力した名前は、プロファイルにサービスを追加する際に表示されます。入力する名前は必ず、一意的でわかりやすく、かつ意味が通じるものにしてください。

b) [ホスト名/IP アドレス（Host Name/IP Address）] フィールドに、CTI サービスのアドレスを入力します。

ホスト名、IPアドレス、または完全修飾ドメイン名（FQDN）の形式でアドレスを入力します。この値は、CTI Manager サービスを実行している Unified CM の発行者に対応しています。サブスクライバーに対して2つ目のサービスを作成します。

c) [ポート（Port）] フィールドに、CTI サービスに使用するポート番号を入力します。

ステップ 7 [保存（Save）] を選択します。

次のタスク

Unified CM サブスクライバーに対して2つ目の CTI サービスを作成します。

サービス プロファイルに CTI サービスを追加します。

CTI サービスの適用

Cisco Unified Communications Manager で CTI サービスを追加した後、クライアントがその設定を取得できるようにするために、その CTI サービスをサービス プロファイルに適用する必要があります。

始める前に

- まだ存在していないか、CTI 用に別のサービス プロファイルが必要な場合は、サービス プロファイルを作成します。
- Unified CM のパブリッシャーおよびサブスクライバーの CTI サービスを追加します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

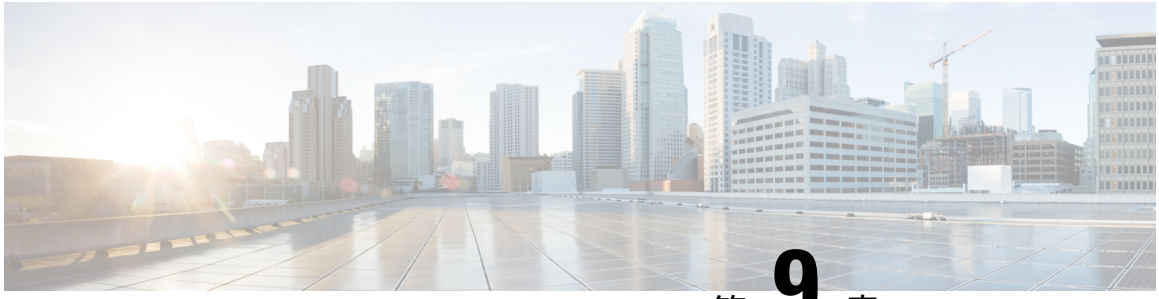
ステップ 2 **[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [サービス プロファイル（Service Profile）]** の順に選択します。
[**サービス プロファイルの検索/一覧表示（Find and List Service Profiles**）] ウィンドウが開きます。

ステップ 3 目的のサービス プロファイルを検索し、それを選択します。
[サービス プロファイルの設定（Service Profile Configuration）] ウィンドウが開きます。

ステップ 4 [CTI プロファイル（CTI Profile）] セクションに移動して、次のドロップダウン リストから、サービスを 3 つまで選択します。

- **Primary**
- **セカンダリ**
- **ターシャリ（Tertiary）**

ステップ 5 [保存（Save）] を選択します。



第 9 章

ユーザ（Users）

LDAP 同期の概要

Lightweight Directory Access Protocol（LDAP）の同期は、システムのエンドユーザのプロビジョニングと設定を支援します。LDAP の同期中、システムは外部 LDAP ディレクトリから Cisco Unified Communications Manager データベースにユーザのリストと関連するユーザ データをインポートします。また、従業員のデータの変更を漏らさずに記録するため、定期的な同期スケジュールを設定できます。

ユーザ ID とディレクトリ URI

LDAP ディレクトリ サーバと Cisco Unified Communications Manager を同期させると、次の値を含む属性を使用して、Cisco Unified Communications Manager データベースと Cisco Unified Communications Manager IM and Presence サービス データベースの両方でエンドユーザ設定テーブルを生成できます。

- **ユーザ ID**：Cisco Unified Communications Manager でユーザ ID の値を指定する必要があります。この値はデフォルトの IM アドレス スキームおよびユーザのログインに必要です。デフォルト値は `sAMAccountName` です。

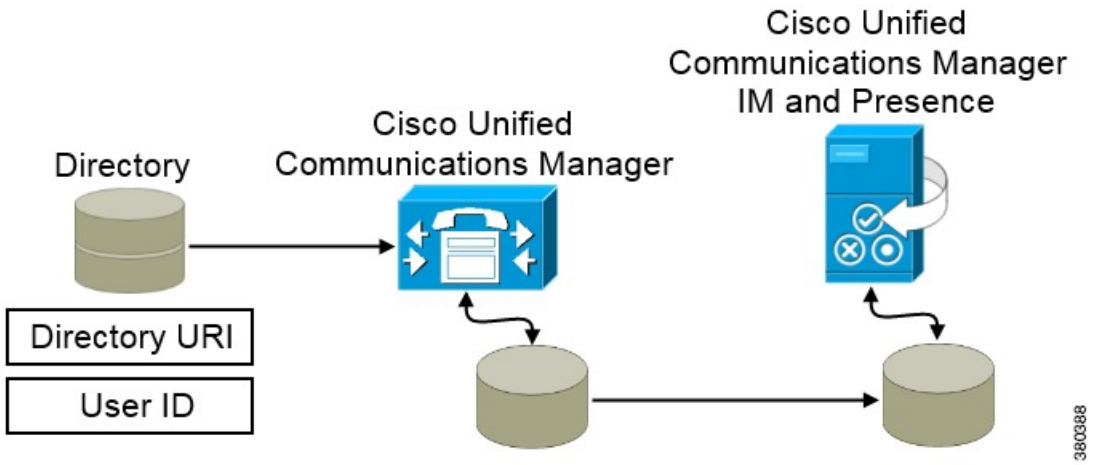
重要 ユーザ ID の属性が `sAMAccountName` 以外の場合で、Cisco Unified Communications Manager IM and Presence サービスでデフォルトの IM アドレス方式が使用されている場合は、次のようにクライアント コンフィギュレーション ファイルでパラメータの値として属性を指定する必要があります。

CDI パラメータは `UserAccountName` です。

```
<UserAccountName>attribute-name</UserAccountName>
```

設定で属性を指定せず、属性が `sAMAccountName` 以外の場合、クライアントはディレクトリ内の連絡先を解決できません。この結果、ユーザはプレゼンスを取得せず、インスタントメッセージを送信または受信できません。

- **ディレクトリ URI**：以下を予定している場合は、ディレクトリ URI の値を指定する必要があります。
  - Cisco Jabber で URI ダイヤルを有効にする。
  - Cisco Unified Communications Manager IM and Presence サービス バージョン 10 以降でディレクトリ URI アドレス スキームを使用する。



Cisco Unified Communications Manager がディレクトリ ソースと同期すると、ディレクトリ URI とユーザ ID の値を取得して、それらを Cisco Unified Communications Manager データベースのエンド ユーザ設定テーブルに入力します。

その後で、Cisco Unified Communications Manager データベースが Cisco Unified Communications Manager IM and Presence サービス データベースと同期します。その結果、ディレクトリ URI とユーザ ID の値が Cisco Unified Communications Manager IM and Presence サービス データベースのエンド ユーザ設定テーブルに入力されます。

ユーザ ワークフローの設定

手順

	コマンドまたはアクション	目的
ステップ 1	サービスのアクティブ化 （49 ページ）	ユーザ設定を LDAP ディレクトリから Cisco Unified Communications Manager と IM and Presence サービスへ同期するために必要なサービスをオンにします。
ステップ 2	LDAP ディレクトリの同期化の有効化 （50 ページ）	Cisco Unified Communications Manager が LDAP ディレクトリからユーザ設定を同期できるようにします。**ユーザ ID** について Cisco Unified Communications Manager を同期させる LDAP ディレクトリから属性を選択します。
ステップ 3	LDAP ディレクトリの同期の設定 （51 ページ）	LDAP ディレクトリと同期するよう、Cisco Unified Communications Manager を設定します。自動同期スケジュールを設定し、標準ユーザ フィールドをマップして、アクセス コントロール グループにインポートされたユーザを割り当てます。
ステップ 4	認証オプション （53 ページ）	認証オプションを選択します。 • クライアント内の SAML SSO を有効にします。 • LDAP サーバで認証します。
ステップ 5	同期の実行 （57 ページ）	Cisco Unified Communications Manager とディレクトリ サーバを同期します。
ステップ 6	ユーザへのサービス プロファイルの関連付け （57 ページ）	サービス プロファイルをユーザに関連付けます。
ステップ 7	連絡先リストの一括事前入力 （59 ページ）	ユーザの連絡先リストにデータを挿入します。

サービスのアクティブ化

社内 LDAP サーバを統合する前に、次のサービスをアクティブにする必要があります。

- Cisco DirSync サービス：社内 LDAP ディレクトリでエンドユーザの設定を同期するにはこのサービスをアクティブにする必要があります。
- （Cisco Unified Communications Manager IM and Presence サービス）Cisco Sync Agent サービス：このサービスは IM and Presence サービス ノードと Cisco Unified Communications Manager の間でデータの同期を維持します。ディレクトリ サーバとの同期を実行すると、Cisco Unified Communications Manager は次に IM and Presence サービスとデータを同期します。

手順

ステップ 1 Cisco Unified Serviceability から、**[ツール（Tools）] > [サービスの有効化（Service Activation）]** を選択します。

ステップ 2 [**サーバ（Server**）] ドロップダウン リスト ボックスからパブリッシャ ノードを選択します。

ステップ 3 [**ディレクトリ サービス（Directory Services**）] の下の [**Cisco DirSync**] オプション ボタンをクリックします。

ステップ 4 **[保存（Save）]**をクリックします。

ステップ 5 **[ツール（Tools）] > [コントロール センタのネットワーク サービス（Control Center - Network Services）]** を選択します。

ステップ 6 [サーバ（Server）] ドロップダウン リスト ボックスから、[IM and Presence サービス（IM and Presence Service）] ノードを選択します。

ステップ 7 [**IM and Presence サービス（IM and Presence Services**）] で、[**Cisco 同期エージェント（Cisco Sync Agent**）] オプション ボタンをクリックします。

ステップ 8 [**保存（Save**）]をクリックします。

LDAP ディレクトリの同期化の有効化

エンドユーザの設定を社内 LDAP ディレクトリから同期するように Cisco Unified Communications Manager を設定するには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、**[システム（System）] > [LDAP] > [LDAP システム（LDAP System）]** を選択します。

[LDAP システムの設定（LDAP System Configuration）] ウィンドウが開きます。

ステップ 2 Cisco Unified Communications Manager が LDAP ディレクトリからユーザをインポートすることを許可するには、[LDAP サーバからの同期を有効にする（Enable Synchronizing from LDAP Server）] チェックボックスをオンにします。

ステップ 3 [LDAP サーバ タイプ（LDAP Server Type）] ドロップダウン リスト ボックスから、会社が使用する LDAP ディレクトリ サーバのタイプを選択します。

ステップ 4 [ユーザ ID の LDAP 属性（LDAP Attribute for User ID）] ドロップダウン リスト ボックスから、[エンドユーザ設定（End User Configuration）] ウィンドウの [ユーザ ID（User ID）] フィールドの値について、Cisco Unified Communications Manager を同期させる社内 LDAP ディレクトリの属性を選択します。

この値はデフォルトの IM アドレス スキームおよびユーザのログインに必要です。デフォルト値は `sAMAccountName` です。

設定で属性を指定せず、属性が `sAMAccountName` 以外の場合、クライアントはディレクトリ内の連絡先を解決できません。この結果、ユーザはプレゼンスを取得せず、インスタント メッセージを送信または受信できません。

ステップ 5 [**保存（Save）**]をクリックします。

LDAP ディレクトリの同期の設定

LDAP ディレクトリと同期するよう Cisco Unified Communications Manager を設定するには、次の手順を使用します。LDAP ディレクトリの同期により、[**エンド ユーザの設定（End User Configuration**）] ウィンドウに表示されるエンドユーザのデータを外部の LDAP ディレクトリより Cisco Unified Communications Manager データベースへインポートできます。定期的に LDAP ディレクトリの更新が Cisco Unified Communications Manager に伝達されるよう、同期スケジュールをセットアップできます。

フィールドとその説明を含むヘルプは、オンライン ヘルプを参照してください。

手順

ステップ 1 Cisco Unified CM の管理で、**[システム（System）] > [LDAP（LADP）][> LDAP ディレクトリ（LDAP Directory）]** を選択します。

ステップ 2 次のいずれかの手順を実行します。

- [**検索（Find**）] をクリックし、既存の LDAP ディレクトリを選択します。
- [**新規追加（Add New**）] をクリックして、新しい LDAP ディレクトリを作成します。

ステップ 3 [**LDAP 構成名（LDAP Configuration Name**）] テキスト ボックスで、LDAP ディレクトリの一意の名前を指定します。

ステップ 4 [**LDAP マネージャ識別名（LDAP Manager Distinguished Name**）] フィールドに、LDAP ディレクトリ サーバにアクセスできるユーザ ID を入力します。

ステップ 5 パスワードの詳細を入力し、確認します。

ステップ 6 [LDAP ディレクトリ同期スケジュール（LDAP Directory Synchronization Schedule）] フィールドに、外部 LDAP ディレクトリとデータ同期を行うために Cisco Unified Communications Manager が使用するスケジュールを作成します。

ステップ 7 [**同期対象の標準ユーザ フィールド（Standard User Fields To Be Synchronized**）] セクションを記入します。各エンドユーザのフィールドで、それぞれLDAP属性を選択します。同期プロセスは LDAP 属性の値を Cisco Unified Communications Manager のエンドユーザ フィールドに割り当てます。

a) [**ディレクトリURI（Directory URI**）] ドロップダウン リストで、次の LDAP 属性のいずれかを選択します。

- **msRTCSIP-primaryuseraddress**：この属性は、Microsoft Lync または Microsoft OCS が使用されている場合に AD 内で生成されます。これがデフォルト属性です。
- **メール**

ステップ 8 インポートされたすべてのエンドユーザに共通するアクセス コントロール グループにインポートしたエンドユーザを割り当てるには、次の手順を実行してください。

a) [**アクセス コントロール グループに追加（Add to Access Control Group**）] をクリックします。

b) ポップアップ ウィンドウで、インポートしたユーザに割り当てるアクセス コントロール グループごとに、対応するチェックボックスをオンにします。

c) [**選択項目の追加（Add Selected**）] をクリックします。

ユーザを、少なくとも次のアクセス コントロール グループに割り当てる必要があります。

- **[標準 CCM エンドユーザ（Standard CCM End Users）]**
- [**標準 CTI を有効にする（Standard CTI Enabled**）]：このオプションは、デスク フォンを制御するために使用します。

セキュア電話機能をユーザにプロビジョニングする場合、**Standard CTI Secure Connection** グループにユーザを割り当てないでください。

電話機のモデルによっては、次のコントロール グループが追加で必要となります。

- Cisco Unified IP Phone 9900、8900、8800 シリーズ、または DX シリーズでは、[**標準 CTI による接続時の転送および会議をサポートする電話の制御（Standard CTI Allow Control of Phones supporting Connected Xfer and conf**）] を選択します。
- Cisco Unified IP Phone 6900 シリーズでは、[**標準 CTI によるロールオーバー モードをサポートする電話の制御（Standard CTI Allow Control of Phones supporting Rollover Mode**）] を選択します。

（注） Cisco Unified Communications Manager 9.x では、[**エンドユーザの設定（End User Configuration**）] ウィンドウ（[**ユーザ管理（User Management**）] > [**エンドユーザ（End User**）]）のアクセス コントロール グループにエンドユーザを割り当てる必要があります。

ステップ 9 [**LDAP サーバ情報（LDAP Server Information**）] エリアで、LDAP サーバのホスト名または IP アドレスを入力します。

ステップ 10 LDAP サーバへのセキュアな接続を作成するには、[**TLS を使用（Use TLS**）] チェックボックスをオンにします。

ステップ 11 [**保存（Save**）]をクリックします。

認証オプション

LDAP サーバでの認証

LDAP 認証を有効にして、会社の LDAP ディレクトリに割り当てられているパスワードに対してエンドユーザのパスワードが認証されるようにするには、この手順を実行します。LDAP 認証により、システム管理者は会社のすべてのアプリケーションに対してエンドユーザの 1 つのパスワードを割り当てることができます。この設定は、エンドユーザのパスワードにのみ適用され、エンドユーザの PIN またはアプリケーション ユーザのパスワードには適用されません。ユーザがクライアントにサインインすると、プレゼンス サービスがその認証を Cisco Unified Communications Manager にルーティングします。その後で、Cisco Unified Communications Manager がその認証をディレクトリ サーバに送信します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[システム（System）] > [LDAP] > [LDAP 認証（LDAP Authentication）]** を選択します。

ステップ 3 [エンドユーザ用 LDAP 認証の使用（Use LDAP Authentication for End Users）] を選択します。

ステップ 4 必要に応じて、LDAP クレデンシャルとユーザ検索ベースを指定します。

[LDAP認証（LDAP Authentication）] ウィンドウ上のフィールドの詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

ステップ 5 [保存（Save）] を選択します。

クライアントの LDAP サーバ認証のための設定

LDAP クレデンシャルを使用するための認証の設定では、クライアントも設定する必要があります。

手順

ステップ 1 LDAP_UseCredentialsFrom パラメータで `jabber-config.xml` ファイルを更新します。

例：

<LDAP_UseCredentialsFrom>*CUCM*</LDAP_UseCredentialsFrom>

ステップ 2 Cisco Unified Communications Manager IM and Presence サービスおよび Cisco Unified Communications Manager が展開されているドメインとは別のドメインに LDAP サーバが展開されている場合は、LDAPUserDomain パラメータを設定します。このパラメータを設定しない限り、必須のパラメータである PresenceDomain の値がデフォルトで使用されます。

例：

<LdapUserDomain>*example.com*</LdapUserDomain>

匿名バインドでの認証

LDAP サーバのユーザ認証の手段として、匿名バインドを設定できます。匿名バインドを使用することにより、Jabber の [オプション（Options）] メニューの [アカウント（Accounts）] タブでのクレデンシャル入力を不要にできます。

手順

jabber-config.xml ファイルで、LdapAnonymousBinding パラメータに true または false の値を設定します。

例：

<LdapAnonymousBinding>true</LdapAnonymousBinding>

このパラメータの設定の詳細は、『*Cisco Jabber* パラメータ リファレンス ガイド（*Parameters Reference Guide for Cisco Jabber*）』を参照してください。

手動ユーザ認証

ユーザが必要とするサービスで Jabber クライアントにユーザ自身のクレデンシャルを手動で入力するサービス認証をセットアップできます。

サービス認証が（たとえば、サービスプロファイルまたは LDAP サーバに）設定されていない場合は、ユーザが自分のクレデンシャルを手動で入力するよう求められます。

ユーザのクレデンシャルは Jabber の [**オプション（Option**）] メニューの [**アカウント（Accounts**）] タブに入力します。

クライアント内の SAML SSO の有効化

始める前に

- Cisco Unified Communications Applications 10.5.1 Service Update 1 での SSO の有効化：このサービスで SAML SSO を有効化する方法については、『*SAML SSO Deployment Guide for Cisco Unified Communications Applications, Release 10.5*』を参照してください。
- Cisco Unity Connection バージョン 10.5 で SSO を有効にします。このサービス上での SAML SSO の有効化方法については、『*Managing SAML SSO in Cisco Unity Connection*』を参照してください。

手順

ステップ 1 Webブラウザで証明書を検証できるように、すべてのサーバに証明書を配布してください。これを行わないと、無効な証明書に関する警告メッセージが表示されます。証明書の検証に関する詳細については、「証明書の検証」を参照してください。

ステップ 2 クライアントの SAML SSO のサービス検出を確認します。クライアントは、標準サービス検出を使用してクライアントの SAML SSO を有効化します。設定パラメータ ServicesDomain、VoiceServicesDomain、および ServiceDiscoveryExcludedServices を使用して、サービス検出を有効化します。サービス検出を有効にする方法の詳細については、「リモートアクセスのためのサービス検出の設定」を参照してください。

ステップ 3 セッションの継続時間を定義します。

セッションは、クッキーおよびトークン値で構成されます。cookie は通常トークンより長く継続します。cookie の寿命はアイデンティティプロバイダーで定義され、トークンの期間はサービスで定義されます。

ステップ 4 SSO を有効にすると、デフォルトで、すべての Cisco Jabber ユーザが SSO を使用してサインインします。管理者は、特定のユーザが SSO を使用する代わりに、Cisco Jabber ユーザ名とパスワードを使用してサインインするようにユーザ単位でこの設定を変更できます。Cisco Jabber ユーザの SSO を無効にするには、SSO_Enabled パラメータの値を FALSE に設定します。

ユーザに電子メールアドレスを尋ねないように Cisco Jabber を設定した場合は、ユーザの Cisco Jabber への最初のサインインが非 SSO になることがあります。展開によっては、パラメータの ServicesDomainSsoEmailPrompt を ON に設定する必要があります。これによって、Cisco Jabber は初めて SSO サインインを実行する際の必要な情報を得ることができます。ユーザが以前 Cisco Jabber にサインインしたことがある場合は、必要な情報が取得済みであるため、このプロンプトは必要ありません。

モバイル クライアントの証明書ベース SSO 認証

この設定は、Cisco Jabber for iPhone および iPad にのみ必要です。Cisco Jabber for Android には、同様の設定は必要ありません。

この機能を有効にするには、Cisco Unified Communications Manager と Cisco Unity Connection の両方で [iOS での SSO ログイン動作（SSO Login Behavior for iOS）] の設定を同じにします。

Expressway for Mobile and Remote Access により、VCS Expressway 管理コンソールで組み込み Safari ブラウザを使用するように Jabber for iPhone and iPad クライアントを設定します。詳細については、https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-guides-list.htmlのCisco Expresswayインストールガイドを参照してください。

Webex Messenger では共通アイデンティティ（CI）を有効にできません。組み込まれている Safari が、Cisco Jabber for iPhone and iPad でクライアント証明書ベースの SSL 認証を使用してボイスメールに接続できるようにするには、CIを無効にする必要があります。

Cisco Unified Communications Manager での証明書ベース SSO 認証の設定

この設定は Cisco Unified Communications Manager 11.5 以降でのみサポートされます。

手順

ステップ 1 Cisco Unified CM の管理で、**[システム（System）]** > **[エンタープライズ パラメータ（Enterprise Parameters）]** に移動します。

ステップ 2 [SSO 設定（SSO Configuration）] セクションで、[iOS での SSO ログイン動作（SSO Login Behavior for iOS）] までスクロールし、[ネイティブ ブラウザを使用（Use native browser）] を選択します。

ステップ 3 [保存（Save）] を選択します。

Cisco Unity Connection での証明書ベース SSO 認証の設定

手順

ステップ 1 Cisco Unity Connection Administration で、**[システム設定（System Setting）]** > **[エンタープライズ パラメータ（Enterprise Parameters）]** と進みます。

ステップ 2 [SSO 設定（SSO Configuration）] セクションで、[iOS での SSO ログイン動作（SSO Login Behavior for iOS）] までスクロールし、[ネイティブ ブラウザを使用（Use native browser）] を選択します。

ステップ 3 [保存（Save）] を選択します。

同期の実行

ディレクトリ サーバを追加し、認証方法を指定した後、Cisco Unified Communications Manager をディレクトリ サーバと同期できます。

手順

ステップ 1 **[システム（System）] > [LDAP] > [LDAP ディレクトリ（LDAP Directory）]** を選択します。

ステップ 2 [検索（Find）] をクリックし、設定した LDAP ディレクトリを選択します。

[LDAP ディレクトリ（LDAP Directory）] ウィンドウが開きます。

ステップ 3 [今すぐ完全同期を実行する（Perform Full Sync Now）] を選択します。

（注） 同期プロセスの完了までに要する時間は、ディレクトリ内のユーザの数によって異なります。ユーザ数が数千にもなる大規模なディレクトリの同期を実施する場合、そのプロセスにはある程度の時間がかかると予想されます。

ディレクトリ サーバからのユーザ データが Cisco Unified Communications Manager データベースに同期されます。その後で、Cisco Unified Communications Manager が IM and Presence サービス データベースにユーザ データを同期します。

ユーザへのサービス プロファイルの関連付け

個別ユーザへのサービス プロファイルの関連付け

サービス プロファイルを個別ユーザへ関連付けます。

手順

ステップ 1 **[Cisco Unified CM の管理（Cisco Unified CM Administration）]** インターフェイスを開きます。

ステップ 2 **[ユーザ管理（User Management）] > [エンド ユーザ（End User）]** を選択します。

[ユーザの検索と一覧表示（Find and List Users）] ウィンドウが開きます。

ステップ 3 [ユーザを次の条件で検索（Find User where）] フィールドで適切なフィルタを指定した後、[検索（Find）] を選択してユーザのリストを取得します。

ステップ 4 対象のユーザ名をリストから選択します。

[エンド ユーザの設定（End User Configuration）] ウィンドウが表示されます。

ステップ 5 [サービスの設定（Service Settings）] セクションを探します。

ステップ 6 [ホーム クラスタ（Home Cluster）] を選択します。

ステップ 7 電話モード展開では、[Unified CM IM and Presence のユーザを有効化（関連付けられている UC サービス プロファイルで IM and Presence を設定）（Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)）] オプションが選択されていないことを確認します。

他のすべての展開では、[Unified CM IM and Presenceの ユーザを有効化（関連付けられている UC サービス プロファイルで IM and Presence を設定）（Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)）] チェックボックスをオンにします。

ステップ 8 [UC サービス プロファイル（UC Service Profile）] ドロップダウン リストからサービス プロファイルを選択します。

重要 Cisco Unified Communications Manager リリース 9.x のみ：ユーザがインスタント メッセージおよびプレゼンスの機能しか使用しない（IM 専用）場合は、[デフォルトの使用（Use Default）] を選択する必要があります。Cisco Unified Communications Manager リリース 9.x は、[UC サービス プロファイル（UC Service Profile）] ドロップダウン リストから選択された項目に関係なく、デフォルト サービス プロファイルを適用します。

ステップ 9 [保存（Save）] を選択します。

ユーザへのサービス プロファイルの一括関連付け

サービス プロファイルを複数のユーザに追加します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[一括管理（Bulk Administration）] > [ユーザ（Users）] > [ユーザの更新（Update Users）] > [クエリー（Query）]** を選択します。

[更新するユーザの検索と一覧表示（Find and List Users To Update）] ウィンドウが表示されます。

ステップ 3 [ユーザを次の条件で検索（Find User where）] フィールドで適切なフィルタを指定した後、[検索（Find）] を選択してユーザのリストを取得します。

ステップ 4 [次へ（Next）] を選択します。

[ユーザの更新（Update Users Configuration）] ウィンドウが開きます。

ステップ 5 電話機モードの展開では、インスタント メッセージとプレゼンスを無効にし、[Unified CM IM and Presence のユーザを有効化（Enable User for Unified CM IM and Presence）] チェックボックスを 1 つオンにします。

他のすべての展開では、[Unified CM IM and Presence のユーザを有効化（Enable User for Unified CM IM and Presence）] チェックボックスの両方をオンにします。

ステップ 6 [UC サービス プロファイル（UC Service Profile）] チェックボックスをオンにし、そのドロップダウン リストからサービス プロファイルを選択します。

重要 Cisco Unified Communications Manager リリース 9.x のみ：ユーザがインスタント メッセージおよびプレゼンスの機能しか使用していない（IM 専用）場合は、[デフォルトの使用（Use Default）] を選択する必要があります。

IM 専用ユーザの場合：Cisco Unified Communications Manager リリース 9.x は、[**UC サービスプロファイル（UC Service Profile**）] ドロップダウン リストで選択された項目に関係なく、常に、デフォルト サービス プロファイルを適用します。

ステップ 7 [**ジョブ情報（Job Information**）] セクションで、ジョブをただちに実行するか後で実行するかを指定します。

ステップ 8 [**送信（Submit**）] を選択します。

連絡先リストの一括事前入力

一括管理ツール（BAT）を使用してユーザの連絡先リストを事前に入力することもできます。

これにより、ユーザの連絡先リストを事前に入力して、クライアントの最初の起動後にユーザが連絡先のセットを自動的に入手できるようにします。

Cisco Jabber はクライアント連絡先リストで最大 300 件の連絡先をサポートします。

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザに提供する連絡先リストを定義した CSV ファイルを作成します。	連絡先リストのインポートのための CSV 作成 （59 ページ）
ステップ 2	BAT を使用して一連のユーザに連絡先リストを一括でインポートします。	BAT を使用した連絡先リストのアップロード （61 ページ）

連絡先リストのインポートのための CSV 作成

CSV ファイルの構造

CSV ファイルは、次の形式である必要があります。

<User ID>, <User Domain>, <Contact ID>, <Contact Domain>, <Nickname>, <Group Name>

CSV ファイル エントリの例は、次のとおりです。

```
userA,example.com,userB,example.com,buddyB,General
```

表 *1:* 入力ファイルのパラメータの説明

パラメータ	説明
[ユーザID（ User ID）]	必須パラメータです。IM and Presence Service ユーザのユーザ ID。これには、最大 132 文字を使用できます。
ユーザのドメイン名（User Domain）	必須パラメータです。IM and Presence Service ユーザのプレゼンス ドメイン。これには、最大 128 文字を使用できます。
コンタクト ID（Contact ID）	必須パラメータです。連絡先リスト エントリのユーザ ID。これには、最大 132 文字を使用できます。
Contact Domain（連絡先ドメイン）	必須パラメータです。連絡先リスト エントリのプレゼンス ドメイン。次の制限は、ドメイン名の形式に適用されます。 • 長さは 128 文字以下である必要があります • 数字、大文字と小文字、およびハイフン（-）だけ含めます • ハイフン（-）で開始または終了してはいけません • ラベルの長さは63 文字以下である必要があります • トップ レベル ドメインは文字だけで、少なくとも 2 文字にする必要があります
ニックネーム（Nickname）	連絡先リスト エントリのニックネーム。これには、最大 255 文字を使用できます。
グループ名（Group Name）	必須パラメータです。連絡先リスト エントリが追加されるグループの名前。これには、最大 255 文字を使用できます。

BAT を使用した連絡先リストのアップロード

始める前に

連絡先が入った CSV ファイルを作成します。

手順

ステップ 1 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）]** インターフェイスを開きます。

ステップ 2 **[一括管理（Bulk Administration）] [> ファイルのアップロード/ダウンロード（Upload/Download Files）]** の順に選択します。

ステップ 3 **[新規追加（Add New）]** を選択します。

ステップ 4 **[ファイル選択（Choose File）]** を選択して、CSV ファイルを検索し選択します。

ステップ 5 ターゲットとして **[連絡先リスト（Contact Lists）]** を選択します。

ステップ 6 トランザクション タイプとして **[ユーザの連絡先のインポート - カスタム ファイル（Import Users' Contacts – Custom File）]** を選択します。

ステップ 7 **[保存（Save）]** を選択してファイルをアップロードします。

UDS 連絡先検索のための認証設定

Cisco Jabber は連絡先を検索する際に認証されたディレクトリ クエリーをサポートします。認証は、Cisco Unified Communications Manager リリース 11.5 以降で設定されます。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 **utils contactsearchauthentication status** コマンドを実行し、このノードの連絡先検索の認証の設定を確認します。

ステップ 3 連絡先検索の認証の設定が必要な場合、

- 認証を有効にするには、**utils contactsearchauthentication enable** コマンドを実行します。
- 認証を無効にするには、**utils contactsearchauthentication disable** コマンドを実行します。

ステップ 4 すべての Unified Communications Manager クラスタ ノードでこの手順を繰り返します。

（注） 変更を有効にするには、電話をリセットする必要があります。

拡張 UDS 連絡先ソースの有効化

始める前に

拡張 UDS の連絡先の検索は、Cisco Unified Communications Manager リリース 11.5(1) 以降でのみ使用可能です。

手順

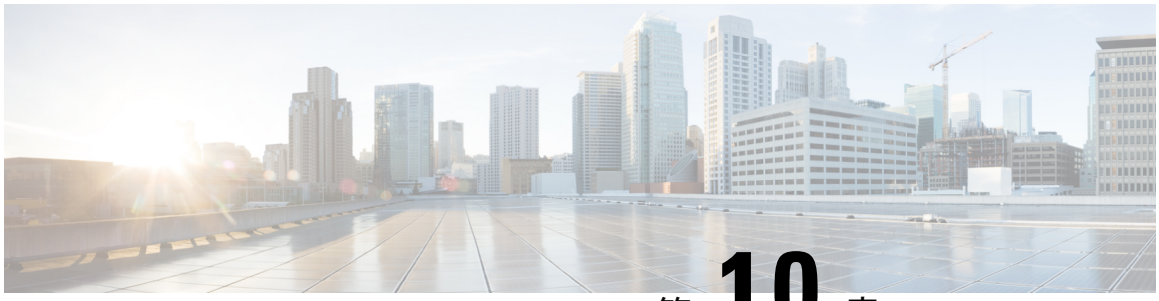
ステップ 1 [**Cisco Unified CM の管理（Cisco Unified CM Administration**）]インターフェイスを開きます。

ステップ 2 **[システム（System）][> LDAP][> LDAP 検索（LDAP Search）]** を選択します。

ステップ 3 エンタープライズLDAPディレクトリ サーバを使用してユーザ検索を実行するには、**[エンタープライズ ディレクトリ サーバのユーザ検索を有効にする（Enable user search to Enterprise Directory Server**）] チェックボックスをオンにします。

ステップ 4 [**LDAP 検索の設定（LDAP Search Configuration**）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 5 [**保存（Save**）] を選択します。



第 10 章

ソフトフォンの設定

ソフトフォン ワークフローの作成

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Jabber デバイスの作成と設定 （64 ページ）	Cisco Jabber にアクセスするユーザごとに 1 つ以上のデバイスを作成します。ユーザに提供する認証文字列を生成します。
ステップ 2	デバイスに電話番号を追加する （68 ページ）	作成した各デバイスについて、ディレクトリ番号を追加します。
ステップ 3	ユーザとデバイスの関連付け （69 ページ）	ユーザとデバイスを関連付けます。
ステップ 4	モバイル SIP プロファイルの作成 （70 ページ） を選択します。	この作業は、Cisco Unified Communications Manager リリース 9 を使用して、デバイスをモバイル クライアント用に設定する場合に実行します。
ステップ 5	電話セキュリティ プロファイルの設定 （71 ページ）	この作業は、すべてのデバイスのセキュアな電話機能をセットアップするために実行します。

Cisco Jabber デバイスの作成と設定

Cisco Jabber にアクセスするユーザごとに 1 つ以上のデバイスを作成します。ユーザは複数のデバイスを所有することができます。

（注） ユーザは、ソフトフォン（CSF）デバイスを使用して通話する場合のみ、電話会議から参加者を削除できます。

始める前に

- COP ファイルをインストールします。
- Cisco Unified Communications Manager リリース 9 以前を使用してモバイル クライアント用のデバイスを設定する場合は、SIP プロファイルを作成します。
- すべてのデバイスにセキュアな電話機能を設定する場合は、電話セキュリティ プロファイルを作成します。
- Cisco Unified Communications Manager リリース 10 以降で、CAPF エンロールメントを使用している場合は、**[エンドポイントへの証明書発行者（Certificate Issuer to Endpoint）]**の Cisco Certificate Authority Proxy Function（CAPF）サービス パラメータの値が **[Cisco Certificate Authority Proxy Function]**に設定されていることを確認します。これは、Cisco Jabber でサポートされている唯一のオプションです。CAPF サービス パラメータの設定については、『Cisco Unified Communications Manager Security Guides』の「*Update CAPF Service Parameters*」のトピックを参照してください。
- モバイル ユーザの Cisco Jabber 用の TCT デバイス、BOT デバイス、または TAB デバイスを作成する前に、組織の最上位ドメイン名を指定して、Cisco Jabber と Cisco Unified Communications Manager 間の登録をサポートします。[Unified CM の管理（Unified CM Administration）] インターフェイスで、**[システム（System）]** > **[エンタープライズ パラメータ（Enterprise Parameters）]** を選択します。[クラスタ全体のドメイン設定（Clusterwide Domain Configuration）]セクションで組織の最上位ドメイン名を入力します。例：cisco.com この最上位ドメイン名は、電話登録用の Cisco Unified Communications Manager サーバの DNS ドメインとして Jabber で使用します。たとえば、CUCMServer1@cisco.com となります。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスにログインします。

ステップ 2 **[デバイス（Device）]** > **[電話（Phone）]** の順に選択します。
[電話の検索/一覧表示（Find and List Phones）] ウィンドウが開きます。

ステップ 3 [新規追加（Add New）] を選択します。

ステップ 4 [電話のタイプ（Phone Type）] ドロップダウン リストで、設定しているデバイス タイプに適したオプションを選択してから、[次へ（Next）] を選択します。

Jabber のユーザには、ユーザごとに複数のデバイスを作成できますが、デバイスのタイプはユーザ 1 人あたり 1 つに限られます。たとえば、タブレット デバイス 1 つと CSF デバイス 1 つを作成できますが、CSF デバイスを 2 つ作成することはできません。

- [Cisco Unified Client Services Framework]：このオプションは、Cisco Jabber for Mac または Cisco Jabber for Windows 用の CSF デバイスを作成する場合に選択します。
- [Cisco Dual Mode for iPhone]：このオプションは、iPhone 用の TFT デバイスを作成する場合に選択します。
- **[Cisco Jabber for Tablet]**：このオプションは、iPad または Android タブレットまたは Chromebooks用の TAB デバイスを作成する場合に選択します。
- [Cisco Dual Mode for Android]：このオプションは、Android デバイス用の BOT デバイスを作成する場合に選択します。

ステップ 5 [オーナーのユーザ ID（Owner User ID）] ドロップダウン リストで、デバイスを作成するユーザを選択します。

電話モード展開での [Cisco Unified Client Services Framework] オプションの場合は、[ユーザ（User）] が選択されていることを確認します。

ステップ 6 [デバイス名（Device Name）] フィールドで、適切な形式を使用してデバイスの名前を指定します。

選択肢	必要な形式
Cisco Unified Client Services Framework	• 有効な文字：a ~ z、A ~ Z、0 ～ 9。 • 文字数の上限は 15 文字です。
Cisco Dual Mode for iPhone	• デバイス名は *TCT* から始める必要があります。 たとえば、ユーザ名が tadams であるユーザ Tanya Adams の TCT デバイスを作成する場合は、「**TCTTADAMS**」と入力します。 • すべて大文字でなければなりません。 • 有効な文字：A ～ Z、0 ～ 9、ピリオド（.）、アンダースコア（_）、ハイフン（-）。 • 文字数の上限は 15 文字です。

選択肢	必要な形式
Cisco Jabber for Tablet	• デバイス名は *TAB* から始める必要があります。 たとえば、ユーザ名が tadams であるユーザ Tanya Adams の TAB デバイスを作成する場合は、「**TABTADAMS**」と入力します。 • すべて大文字でなければなりません。 • 有効な文字：A ～ Z、0 ～ 9、ピリオド（.）、アンダースコア（_）、ハイフン（-）。 • 文字数の上限は 15 文字です。
[Cisco Dual Mode for Android]	• デバイス名は *BOT* から始める必要があります。 たとえば、ユーザ名が tadams であるユーザ Tanya Adams の BOT デバイスを作成する場合は、「**BOTTADAMS**」と入力します。 • すべて大文字でなければなりません。 • 有効な文字：A ～ Z、0 ～ 9、ピリオド（.）、アンダースコア（_）、ハイフン（-）。 • 文字数の上限は 15 文字です。

ステップ 7 CAPF 登録を使用している場合は、次の手順を実行して認証文字列を生成します。

1. ユーザが自分のデバイスにアクセスして、安全に Cisco Unified Communications Manager に登録できるようにするための認証文字列を生成することができ、**[Certification Authority Proxy Function（CAPF）の情報（Certification Authority Proxy Function (CAPF) Information）]** セクションに移動することができます。
2. [証明書の操作（Certificate Operation）] ドロップダウン リストで、[インストール/アップグレード（Install/Upgrade）] を選択します。
3. [認証モード（Authentication Mode）] ドロップダウン リストで、[認証ストリング（By Authentication String）] または [Null ストリング（By Null String）] を選択します。JVDI および Jabber for Windows CSF デバイスでの CAPF 認証モード [**Null ストリング（By Null String**）] の使用は、サポートされていません。使用すると、Cisco Unified Communications Manager（CUCM）への Jabber 登録が失敗します。

4. [文字列を生成（Generate String）] をクリックします。[認証文字列（Authentication String）] に文字列値が自動的に入力されます。これがエンド ユーザに提供する文字列です。
5. [キーのサイズ（ビット）（Key Size (Bits)）] ドロップダウン リストで、電話セキュリティ プロファイルで設定したものと同じキー サイズを選択します。
6. [操作の完了期限（Operation Completes By）] フィールドで、認証文字列の有効期限値を指定するか、デフォルトのままにします。
7. グループ設定ファイルを使用している場合は、[デスクトップ クライアントの設定（Desktop Client Settings）] の [シスコ サポート フィールド（Cisco Support Field）] にそれを指定します。[デスクトップ クライアントの設定（Desktop Client Settings）] で利用できる設定のうち、それ以外のものは、Cisco Jabber では使用されません。

ステップ 8 [保存（Save）] を選択します。

ステップ 9 [設定の適用（Apply Config）] をクリックします。

次のタスク

デバイスに電話番号を追加します。

ユーザへの認証文字列の提供

CAPF 登録を使用してセキュアな電話機を設定している場合は、ユーザに認証文字列を提供する必要があります。ユーザは、クライアントインターフェイスで認証文字列を指定してデバイスにアクセスし、Cisco Unified Communications Manager に安全に登録する必要があります。

ユーザがクライアントインターフェイスで認証文字列を入力すると、CAPF 登録プロセスが開始されます。

（注） 登録プロセスが完了するまでにかかる時間は、ユーザのコンピュータまたはモバイル デバイス、および Cisco Unified Communications Manager の現在の負荷によって異なります。クライアントが CAPF 登録プロセスを完了するまでに、最大 1 分間かかる場合があります。

次の場合、クライアントはエラーを表示します。

- ユーザが誤った認証文字列を入力した場合。

  ユーザは、CAPF 登録を完了するために、認証文字列の入力をもう一度試行できます。ただし、ユーザが連続して誤った認証文字列を入力すると、文字列が正しい場合でも、クライアントはユーザが入力した文字列を拒否する場合があります。その場合は、ユーザのデバイスに対して新しい認証文字列を生成し、それをユーザに提供する必要があります。

- [操作の完了期限（Operation Completes By）] フィールドに設定した有効期限が過ぎた後、ユーザが認証文字列を入力した場合。

その場合は、ユーザのデバイスに対して新しい認証文字列を生成する必要があります。ユーザは、有効期間内にその認証文字列を入力する必要があります。

重要 Cisco Unified Communications Manager でエンドユーザを設定する場合、次のユーザ グループに追加する必要があります。

- **標準CCMエンドユーザ（Standard CCM End Users）**
- **標準CTIを有効にする（Standard CTI Enabled）**

ユーザは Standard CTI Secure Connection ユーザ グループに属していてはなりません。

デバイスに電話番号を追加する

各デバイスを作成して設定したら、そのデバイスに電話番号を追加する必要があります。ここでは、**[デバイス（Device）] > [電話機（Phone）]** メニュー オプションを使用して、電話番号を追加する手順について説明します。

始める前に

デバイスを作成します。

手順

ステップ 1 [電話の設定（Phone Configuration）] ウィンドウの [割り当て情報（Association Information）] セクションに移動します。

ステップ 2 [新規 DN を追加（Add a new DN）] をクリックします。

ステップ 3 [電話番号（Directory Number）] フィールドで、電話番号を指定します。

ステップ 4 [回線に関連付けられているユーザ（Users Associated with Line）] セクションで、[エンドユーザの関連付け（Associate End Users）] をクリックします。

ステップ 5 [ユーザの検索（Find User where）] フィールドで、適切なフィルタを指定してから、[検索（Find）] をクリックします。

ステップ 6 表示されたリストから、該当するユーザを選択して、[選択項目の追加（Add Selected）] をクリックします。

ステップ 7 その他に必要な設定があれば、それらをすべて指定します。

ステップ 8 [Apply Config] を選択します。

ステップ 9 [保存（Save）] を選択します。

ユーザとデバイスの関連付け

Cisco Unified Communications Manager バージョン 9.x では、クライアントがユーザのサービス プロファイルを取得しようとすると、最初に、Cisco Unified Communications Manager からデバイス コンフィギュレーション ファイルが取得されます。その後、クライアントはデバイス構成を使用してユーザに適用されたサービス プロファイルを取得します。

たとえば、Adam McKenzie に `CSFAKenzi` という名前の CSF デバイスをプロビジョニングしたとします。Adam がサインインすると、クライアントは Cisco Unified Communications Manager から `CSFAKenzi.cnf.xml` を取得します。次に、クライアントは `CSFAKenzi.cnf.xml` で次の内容を検索します。

```
<userId  serviceProfileFile="identifier.cnf.xml">amckenzi</userId>
```

そのため、 Cisco Unified Communications Manager バージョン 9.x を使用している場合は、クライアントがユーザに適用されるサービスプロファイルを正常に取得できることを保証するために、次の手順を実行する必要があります。

- ユーザとデバイスを関連付けます。
- デバイス構成の [ユーザのオーナー ID（User Owner ID）] フィールドを適切なユーザに設定します。この値が設定されていない場合、クライアントはデフォルトのサービス プロファイルを取得します。

始める前に

（注） ユーザごとに別々のサービス プロファイルを使用する場合は、CSF を複数のユーザに関連付けないでください。

手順

ステップ 1 ユーザとデバイスを関連付けます。

a) [Unified CM の管理（Unified CM Administration）] インターフェイスを開きます。
b) **[ユーザ管理（User Management）]** > **[エンド ユーザ（End User）]** を選択します。
c) 適切なユーザを探して選択します。
   [エンド ユーザの設定（End User Configuration）] ウィンドウが表示されます。
d) [デバイス情報（Device Information）] セクションで [デバイスの割り当て（Device Association）] を選択します。
e) 必要に応じて、ユーザとデバイスを関連付けます。
f) [エンド ユーザの設定（End User Configuration）] ウィンドウに戻り、[保存（Save）] を選択します。

ステップ 2 デバイス構成で [ユーザのオーナー ID（User Owner ID）] フィールドを設定します。

a) **[デバイス（Device）] > [電話（Phone）]** の順に選択します。
b) 適切なデバイスを探して選択します。
[電話の設定（Phone Configuration）] ウィンドウが開きます。
c) [デバイス情報（Device Information）] セクションを探します。
d) [ユーザ（User）] を [オーナー（Owner）] フィールドの値として選択します。
e) [オーナーのユーザ ID（Owner User ID）] フィールドから適切なユーザ ID を選択します。
f) [保存（Save）] を選択します。

モバイル SIP プロファイルの作成

この手順は、Cisco Unified Communications Manager リリース 9 を使用していて、デバイスをモバイル クライアント用に設定している場合にのみ必要です。デスクトップ クライアント用に提供されているデフォルトのSIPプロファイルを使用してください。モバイルクライアント用にデバイスを作成および設定する前に、Cisco Unified Communication Manager に接続した状態でCisco Jabberをバックグラウンドで実行させるSIPプロファイルを作成する必要があります。

Cisco Unified Communications Manager リリース 10 を使用する場合は、モバイル クライアント用にデバイスを作成および設定するときに、**[モバイル デバイス用標準 SIP プロファイル（Standard SIP Profile for Mobile Device）]** デフォルト プロファイルを選択します。

手順

ステップ 1 **[Cisco Unified CM の管理（Cisco Unified CM Administration）]** インターフェイスを開きます。

ステップ 2 **[デバイス（Device）] > [デバイス設定（Device Settings）] > [SIP プロファイル（SIP Profile）]** を選択します。

[SIP プロファイルの検索と一覧表示（Find and List SIP Profiles）] ウィンドウが開きます。

ステップ 3 次のいずれかを実行し、新規 SIP プロファイルを作成します。

- デフォルトの SIP プロファイルを検索し、編集可能なコピーを作成します。
- **[新規追加（Add New）]** を選択し、新規 SIP プロファイルを作成します。

ステップ 4 新しい SIP プロファイルに次の値を設定します。

- [レジスタの再送間隔の調整値（Timer Register Delta）] に「120」
- [レジスタのタイムアウト値（Timer Register Expires）] に「720」
- [キープアライブのタイムアウト値（Timer Keep Alive Expires）] に「720」
- [サブスクライブのタイムアウト値 (Timer Subscribe Expires)] に「21600」
- [サブスクライブの調整値 (Timer Subscribe Delta)]に「15」

ステップ 5 [保存（Save）] を選択します。

システムの SIP パラメータの設定

狭帯域ネットワークに接続しており、モバイルデバイスで着信コールの受信が困難な場合は、システム SIP パラメータを設定して状況を改善できます。[SIP デュアル モード アラート タイマー（SIP Dual Mode Alert Timer）] の値を大きくして、Cisco Jabber 内線へのコールがモバイル ネットワーク電話番号に途中でルーティングされないようにします。

始める前に

この設定は、モバイル クライアント専用です。

ビジネス通話を受信するには、Cisco Jabber が実行されている必要があります。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[システム（System）] > [サービス パラメータ（Service Parameters）]** の順に選択します。

ステップ 3 ノードを選択します。

ステップ 4 [Cisco CallManager（アクティブ）（Cisco CallManager (Active)）] サービスを選択します。

ステップ 5 [クラスタ全体のパラメータ（システム - モビリティ）（Clusterwide Parameters (System - Mobility)）] セクションまでスクロールします。

ステップ 6 [SIP デュアル モード アラート タイマー（SIP Dual Mode Alert Timer）] の値を 10000 ミリ秒まで増やします。

ステップ 7 [保存（Save）] を選択します。

（注） [SIP デュアル モード アラート タイマー（SIP Dual Mode Alert Timer）] の値を増やしても、Cisco Jabber に到着する着信コールが引き続き切断され、モバイル コネクトを使用して転送される場合は、[SIP デュアル モード アラート タイマー（SIP Dual Mode Alert Timer）] の値を 500 ミリ秒単位でさらに増やします。

電話セキュリティ プロファイルの設定

オプションで、すべてのデバイスに対してセキュアな電話機能をセットアップできます。セキュア電話機能により、セキュア SIP シグナリング、セキュア メディア ストリーム、および暗号化デバイス設定ファイルが提供されます。

ユーザのセキュアな電話機能を有効にした場合は、Cisco Unified Communications Manager へのデバイス接続がセキュアになります。ただし、他のデバイスとのコールは、両方のデバイスがセキュアな接続を備えている場合にのみセキュアになります。

始める前に

- Cisco CTL クライアントを使用して Cisco Unified Communications Manager のセキュリティモードを設定します。最低限、混合モード セキュリティを選択する必要があります。

  Cisco CTL クライアントを使用した混合モードの設定方法については、『Cisco Unified Communications Manager Security Guide』を参照してください。

- 電話会議の場合は、会議ブリッジがセキュアな電話機能をサポートしていることを確認します。会議ブリッジがセキュア電話機能をサポートしていない場合、そのブリッジへのコールは安全ではありません。同様に、クライアントが電話会議でメディアを暗号化できるようにするために、すべての参加者が共通の暗号化アルゴリズムをサポートしている必要があります。

- 導入でユニファイドコミュニケーションマネージャーリリース 12.5 以降を使用している場合は、SIP OAuth を Cisco Jabber と共に使用することを推奨します。詳細については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html で *Feature Configuration Guide for Cisco Unified Communications Manager*の「SIP OAuth」の章を参照してください。

手順

ステップ 1 **Cisco Unified Communications Manager** で、**[システム（System）]**>**[セキュリティ（Security）]**>**[電話セキュリティプロファイル（Phone Security Profile）]** の順に選択します。

ステップ 2 [新規追加（Add New）] を選択します。

ステップ 3 [電話のタイプ（Phone Type）] ドロップダウン リストで、設定しているデバイス タイプに適したオプションを選択してから、[次へ（Next）] を選択します。

- [Cisco Unified Client Services Framework]：このオプションは、Cisco Jabber for Mac または Cisco Jabber for Windows 用の CSF デバイスを作成する場合に選択します。
- [Cisco Dual Mode for iPhone]：このオプションは、iPhone 用の TFT デバイスを作成する場合に選択します。
- **[Cisco Jabber for Tablet]**：このオプションは、iPad または Android タブレットまたは Chromebooks用の TAB デバイスを作成する場合に選択します。
- [Cisco Dual Mode for Android]：このオプションは、Android デバイス用の BOT デバイスを作成する場合に選択します。
- [CTI リモートデバイス（CTI Remote Device）]：このオプションは、CTI リモート デバイスを作成する場合に選択します。

  CTI リモートデバイスは、ユーザのリモート接続先をモニタリングし、通話を制御する仮想デバイスです。

ステップ 4 [電話セキュリティプロファイルの設定（Phone Security Profile Configuration）] ウィンドウの [名前（Name）] フィールドで、電話セキュリティ プロファイルの名前を指定します。

ステップ 5 [デバイスセキュリティモード（Device Security Mode）] で、次のオプションのいずれかを選択します。

- [認証済み（Authenticated）]：SIP 接続が NULL-SHA 暗号化を使用した TLS 経由になります。
- [暗号化済み（Encrypted）]：SIP 接続が AES 128/SHA 暗号化を使用した TLS 経由になります。クライアントは、Secure Real-time Transport Protocol（SRTP）を使用して、暗号化されたメディア ストリームを提供します。

ステップ 6 [転送タイプ（Transport Type）] は、**TLS** のデフォルト値のままにします。

ステップ 7 TFTP サーバ上に存在するデバイス コンフィギュレーション ファイルを暗号化するには、[TFTP 暗号化（TFTP Encrypted Config）] チェックボックスをオンにします。

（注） TCT/BOT/タブレット デバイスの場合、ここでは [TFTP 暗号化（TFTP Encrypted Config）] チェックボックスをオンにしないでください。[認証モード（Authentication Mode）] で、[認証ストリング（By Authentication String）] または [Null ストリング（Null String）] を選択します。

ステップ 8 [認証モード（Authentication Mode）] で、[認証ストリング（By Authentication String）] または [Null ストリング（By Null String）] を選択します。

（注） VXME および Jabber for Windows CSF デバイスでの CAPF 認証モード **[Null ストリング（By Null String）]** の使用は、サポートされていません。使用すると、Cisco Unified Communications Manager（CUCM）への Jabber 登録が失敗します。

ステップ 9 [キーサイズ（ビット）（Key Size (Bits)）] で、証明書に適したキー サイズを選択します。キー サイズは、CAPF 登録プロセス中にクライアントが生成する公開キーと秘密キーのビット長を示します。

Cisco Jabber クライアントは 1024 ビット長のキーを含む認証文字列を使用してテストされています。Cisco Jabber クライアントが 1024 ビット長のキーではなく 2048 ビット長のキーを生成するには、より長い時間が必要になります。このため、2048 を選択した場合、CAPF 登録プロセスを完了するためにより多くの時間がかかります。

ステップ 10 [SIP 電話ポート（SIP Phone Port）] は、デフォルト値のままにします。

このフィールドで指定したポートは、[デバイスセキュリティモード（Device Security Mode）] の値として [非セキュア（Non Secure）] を選択した場合にのみ有効になります。

ステップ 11 **保存**をクリックします。

第 11 章

デスクフォン制御の設定

前提条件

Cisco CTIManager サービスが Cisco Unified Communications Manager クラスタで実行されている必要があります。

デスクフォン制御ワークフローの設定

手順

	コマンドまたはアクション	目的
ステップ 1	デスクフォン デバイスの作成 （76 ページ）	デスクフォン デバイスを作成します。
ステップ 2	CTI 用のデバイスの有効化 （77 ページ）	Cisco Jabber デスクトップ クライアントがユーザのデスクフォンを制御することを可能にします。
ステップ 3	デスクフォン ビデオの設定 （78 ページ） を選択します。	ユーザがクライアントを介してコンピュータ上のデスクフォン デバイスに転送されたビデオを受信することを可能にします。

	コマンドまたはアクション	目的
ステップ 4	デスクトップ アプリケーション用デバイスへの電話番号の追加 （80 ページ）を選択します。	デバイスにディレクトリ番号を割り当てます。
ステップ 5	ビデオ レート アダプテーションの有効化 （81 ページ）	クライアントはビデオ レート アダプテーションを利用し、最適なビデオ品質をネゴシエートします。

デスクフォン デバイスの作成

ユーザは、自分のコンピュータのデスクフォンを操作して音声コールを発信できます。

始める前に

ソフトフォン デバイスの作成

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[デバイス（Device）] > [電話（Phone）]** の順に選択します。

[電話の検索と一覧表示（Find and List Phones）] ウィンドウが開きます。

ステップ 3 [新規追加（Add New）] を選択します。

ステップ 4 [電話のタイプ（Phone Type）] ドロップダウン リストから適切なデバイスを選択し、続いて [次へ（Next）] を選択します。

[電話の設定（Phone Configuration）] ウィンドウが開きます。

ステップ 5 [デバイス情報（Device Information）] セクションで次の手順を実行します。

a) [説明（Description）] フィールドに分かりやすい説明を入力します。

クライアントにより、デバイスの説明がユーザに表示されます。ユーザが同じモデルのデバイスを複数所有している場合、説明によって複数のデバイスを区別できます。

b) [CTI からデバイスを制御可能（Allow Control of Device from CTI）] を選択します。

[CTI からデバイスを制御可能（Allow Control of Device from CTI）] を選択しない場合は、ユーザはデスクフォンを制御できません。

ステップ 6 [オーナーのユーザ ID（Owner User ID）] フィールドを適切なユーザに設定します。

重要 Cisco Unified Communications Manager バージョン 9.x では、クライアントは [オーナーのユーザ ID（Owner User ID）] フィールドを使用してユーザのサービス プロファイルを取得します。そのため、それぞれのユーザがデバイスを所有し、[オーナーのユーザ ID（Owner User ID）] フィールドがユーザと関連付けられている必要があります。

ユーザとデバイスを関連付けて [オーナーのユーザ ID（Owner User ID）] フィールドを適切なユーザに設定しないと、クライアントはユーザに適用するサービスプロファイルを取得できません。

ステップ 7 次の手順を実行し、デスクフォンのビデオ機能を有効にします。

a) [プロダクト固有の設定（Product Specific Configuration Layout）] セクションを探します。
b) [ビデオ機能（Video Capabilities）] ドロップダウン リストから [有効（Enabled）] を選択します。

（注） 可能であれば、デバイス設定でデスクフォンのビデオ機能を有効にします。ただし、一部の電話機モデルにはデバイス設定レベルでの [ビデオ機能（Video Capabilities）] ドロップダウン リストは含まれていません。この場合、[共通の電話プロファイルの設定（Common Phone Profile Configuration）] ウィンドウを開き、次に [ビデオ コール（Video Calling）] ドロップダウン リストから [有効（Enabled）] を選択する必要があります。

デスクフォンのビデオの詳細については、「デスクフォン ビデオの設定」を参照してください。

ステップ 8 必要に応じて、[電話の設定（Phone Configuration）] ウィンドウのその他の設定も指定します。

[電話の設定（Phone Configuration）] ウィンドウの設定の詳細については、Cisco Unified Communications Managerのマニュアルを参照してください。

ステップ 9 [保存（Save）] を選択します。

デバイスが正常に追加されたとのメッセージが表示されます。[電話の設定（Phone Configuration）] ウィンドウで [割り当て情報（Association Information）] セクションが利用可能になります。

次のタスク

デバイスに電話番号を追加し、設定を適用します。

CTI 用のデバイスの有効化

Cisco Jabberデスクトップ クライアントでユーザのデスクフォンを制御できるようにするには、ユーザのデバイスを作成するときに **[CTI からのデバイスの制御を許可（Allow Control of Device from CTI）]** オプションを選択する必要があります。

手順

ステップ 1 In Cisco Unified CM Administration で、**[デバイス（Device）] > [電話（Phone）]** をクリックし、電話機を検索します。

ステップ 2 [デバイス情報（Device Information）] セクションで、[CTI からのデバイスの制御を許可（Allow Control of Device from CTI）] にマークを付けます。

ステップ 3 **保存**をクリックします。

デスクフォン ビデオの設定

デスクフォンのビデオ機能を使用すると、デスクフォンでのビデオ信号をラップトップに受信し、音声信号を受信することができます。クライアントが Jabber クライアントとの接続を確立するために、コンピュータ ポート経由でコンピュータをデスク フォンに物理的に接続します。この機能は、デスクフォンへのワイヤレス接続と共に使用することはできません。

（注） ワイヤレス接続と有線接続の両方を使用できる場合、ワイヤレス接続が有線接続よりも優先されないように Microsoft Windows を設定します。詳細については、Microsoft の『*An explanation of the Automatic Metric feature for Internet Protocol routes*』を参照してください。

まず、Cisco.com から Jabber デスクフォン ビデオ サービス インターフェイスをダウンロードし、インストールする必要があります。Jabber デスクフォン ビデオ サービス インターフェイスによって Cisco Discover Protocol（CDP）ドライバを提供します。CDP では、クライアントが次のことを実行できます。

- デスクフォンを検出します。
- Cisco Audio Session Tunnel (CAST) プロトコルを使用してデスクフォンへの接続を確立して維持します。

デスクフォン ビデオでの考慮事項

デスクフォン ビデオ機能を設定する前に、以下の考慮事項および制限事項を確認してください。

- CAST を使用して複数のビデオデバイスを接続することはできません。この機能では、組み込みのカメラと一緒にデスク フォンを使用することはできません。デスク フォンにローカル USB カメラがある場合は、この機能を使用する前に削除してください。
- CTI をサポートしていないデバイスでは、この機能を使用できません。
- BFCP プロトコルおよびデスクフォンのビデオを使用して、ビデオスクリーンの共有を両方使用することはできません。

- SCCP を使用するエンドポイントでビデオの受信のみを行うことはできません。SCCP エンドポイントでは、ビデオの送信と受信を行う必要があります。SCCP エンドポイントからビデオが送信されないインスタンスでは、コールが音声のみとなります。
- 7900 シリーズ電話機は、デスクフォンのビデオ機能に SCCP を使用する必要があります。7900 シリーズ電話機は、デスクフォンのビデオ機能に SIP を使用できません。
- デスクフォンのキーパッドからコールを開始した場合、コールはデスクフォンの音声コールとして開始されます。Jabber は、次にコールをビデオにエスカレーションします。したがって、エスカレーションをサポートしない H.323 エンドポイントなどのデバイスにはビデオ コールは発信できません。エスカレーションをサポートしていないデバイスでこの機能を使用するには、Jabber クライアントからのコールを開始します。
- ファームウェア バージョン SCCP45.9-2-1S を使用する Cisco Unified IP Phone には、互換性の問題があります。ファームウェアをバージョン SCCP 45.9-3-1 にアップグレードして、この機能を使用します。
- Symantec EndPoint Protection など、一部のアンチウイルスまたはファイアウォール アプリケーションによって受信 CDP パケットがブロックされます。このブロックは、デスクフォンのビデオを無効にします。受信 CDP パケットを許可するようにアンチウイルスまたはファイアウォール アプリケーションを設定します。

  この問題の詳細については、Symantec の技術文書『*Cisco IP Phone version 7970 and Cisco Unified Video Advantage is Blocked by Network Threat Protection*』を参照してください。
- Cisco Unified Communications Manager (Unified CM) の SIP トランク設定で [メディア ターミネーション ポイントが必須（Media Termination Point Required）] チェックボックスを選択しないでください。この設定では、デスクフォンのビデオが無効になります。

手順

ステップ 1 コンピュータをデスクフォン上のコンピュータ ポートへ物理的に接続します。
ステップ 2 Unified CM でデスクフォンのビデオ機能を有効にします。
ステップ 3 Jabberデスクフォン ビデオ サービス インターフェイスをコンピュータにインストールします。

デスクフォン ビデオのトラブルシューティング

デスクフォンのビデオ機能を使用できない、またはデスクフォンデバイスが不明であることを示すエラーが発生した場合は、次の手順を実行します。

1. Cisco Unified Communications Manager でビデオのデスクフォン デバイスが有効になっていることを確認します。
2. デスクフォン自体をリセットします。
3. クライアントを終了します。

4. クライアントをインストール済みのコンピュータで services.msc を実行します。
5. Windows のタスクマネージャの [サービス（Service）] タブから、Jabber デスク フォン ビデオ サービス インターフェイスを再起動します。
6. クライアントを再起動します。

デスクトップアプリケーション用デバイスへの電話番号の追加

Cisco Unified Communications Manager で、デバイスに電話番号を追加する必要があります。このトピックでは、デバイスの作成後に **[デバイス（Device）]** > **[電話（Phone）]** メニュー オプションを使用して電話番号を追加する手順について説明します。このメニュー オプションから表示されるのは、電話機モデルまたは CTI ルート ポイントに適用される設定のみです。電話番号を設定するためのさまざまなオプションについては、Cisco Unified Communications Manager のマニュアルを参照してください。

手順

ステップ 1 [電話の設定（Phone Configuration）] ウィンドウで、[割り当て情報（Association Information）] セクションに移動します。

ステップ 2 [新規 DN を追加（Add a new DN）] を選択します。

ステップ 3 [電話番号（Directory Number）] フィールドで、電話番号を指定します。

ステップ 4 その他に必要な設定があれば、それらをすべて指定します。

ステップ 5 次の手順に従って、エンド ユーザに電話番号を関連付けます。

a) [回線に関連付けられているユーザ（Users Associated with Line）] セクションに移動します。
b) [エンド ユーザの関連付け（Associate End Users）] を選択します。
c) [ユーザを次の条件で検索（Find User where）] フィールドで適切なフィルタを指定した後、[検索（Find）] を選択してユーザのリストを取得します。
d) 対象のユーザをリストから選択します。
e) [選択項目の追加（Add Selected）] を選択します。

選択されたユーザがボイスメール プロファイルに追加されます。

ステップ 6 [保存（Save）] を選択します。

ステップ 7 [設定の適用（Apply Config）] を選択します。

ステップ 8 [設定の適用（Apply Configuration）] ウィンドウに表示されるプロンプトに従って設定を適用します。

ビデオ レート アダプテーションの有効化

クライアントはビデオ レート アダプテーションを利用し、最適なビデオ品質をネゴシエートします。ビデオ レート アダプテーションは、ネットワークの状態に合わせてビデオ品質を動的に向上または低下させます。

ビデオ レート アダプテーションを使用するには、Cisco Unified Communications Manager で Real-Time Transport Control Protocol（RTCP）を有効にする必要があります。

（注） ソフトフォンデバイスでは、デフォルトでRTCPが有効になっています。ただし、デスクフォン デバイスでは RTCP を有効にする必要があります。

共通の電話プロファイルに対する RTCP の有効化

共通の電話プロファイルでRTCPを有効にし、そのプロファイルを使用するすべてのデバイスでビデオ レート アダプテーションを有効にできます。

（注） RTCP は Jabber テレフォニー サービスの統合コンポーネントです。Jabber は無効にされても RTCP パケットを送信し続けます。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[デバイス（Device）] > [デバイスの設定（Device Settings）] > [共通の電話プロファイル（Common Phone Profile）]** の順に選択します。

[共通の電話プロファイルの検索と一覧表示（Find and List Common Phone Profiles）] ウィンドウが開きます。

ステップ 3 [共通の電話プロファイルを次の条件で検索（Find Common Phone Profile where）] フィールドで対象のフィルタを指定し、[検索（Find）] を選択してプロファイルの一覧を取得します。

ステップ 4 対象のプロファイルを一覧から選択します。

[共通の電話プロファイルの設定（Find and List Common Phone Profiles）] ウィンドウが開きます。

ステップ 5 [プロダクト固有の設定（Product Specific Configuration Layout）] セクションを探します。

ステップ 6 [RTCP] ドロップダウン リストから [有効（Enabled）] を選択します。

ステップ 7 [保存（Save）] を選択します。

デバイス設定に対する RTCP の有効化

共通の電話プロファイルの代わりに、特定のデバイス設定でRTCP を有効化できます。共通の電話プロファイルで指定したすべての設定は、特定のデバイス設定で上書きされます。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[デバイス（Device）] > [電話（Phone）]** の順に選択します。

[電話の検索と一覧表示（Find and List Phones）] ウィンドウが開きます。

ステップ 3 [電話を次の条件で検索（Find Phone where）] フィールドに適切なフィルタを指定し、[検索（Find）] を選択して電話の一覧を取得します。

ステップ 4 対象の電話を一覧から選択します。

[電話の設定（Phone Configuration）] ウィンドウが開きます。

ステップ 5 [プロダクト固有の設定（Product Specific Configuration Layout）] セクションを探します。

ステップ 6 [RTCP] ドロップダウン リストから [有効（Enabled）] を選択します。

ステップ 7 [保存（Save）] を選択します。

第 12 章

拡張および接続機能の設定

拡張および接続機能の設定のワークフロー

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザ モビリティの有効化 （83 ページ）	ユーザのモビリティを有効にし、ユーザを CTI リモート デバイスの所有者として割り当てることができます。
ステップ 2	CTI リモート デバイスの作成 （84 ページ）	CTI リモート デバイス、仮想デバイス モニタを作成し、ユーザのリモート接続先の通話を制御します。
ステップ 3	リモート接続先の追加 （85 ページ）	（オプション）専用 CTI リモート デバイスをユーザにプロビジョニングする場合は、Cisco Unified Communications Manager にリモート接続先を追加します。

ユーザ モビリティの有効化

この作業は、デスクトップ クライアント専用です。

CTI リモート デバイスをプロビジョニングするには、ユーザ モビリティを有効にする必要があります。ユーザのモビリティが有効でない場合、そのユーザを CTI リモート デバイスの所有者として割り当てることはできません。

始める前に

この作業は、次の場合にのみ該当します。

- CTI リモート デバイスに Cisco Jabber for Mac または Cisco Jabber for Windows のユーザを割り当てる予定である。
- Cisco Unified Communications Manager リリース 9.x 以降である。

手順

ステップ 1 **[ユーザ管理（User Management）] > [エンド ユーザ（End User）]** を選択します。

[ユーザの検索と一覧表示（Find and List Users）] ウィンドウが開きます。

ステップ 2 [ユーザを次の条件で検索（Find Users where）] フィールドで適切なフィルタを指定した後、[検索（Find）] を選択してユーザのリストを取得します。

ステップ 3 ユーザを一覧から選択します。

[エンド ユーザの設定（End User Configuration）] ウィンドウが表示されます。

ステップ 4 [モビリティ情報（Mobility Information）] セクションを探します。

ステップ 5 **[モビリティの有効化(Enable Mobility)]** を選択します。

ステップ 6 [保存（Save）] を選択します。

CTI リモート デバイスの作成

CTI リモートデバイスは、ユーザのリモート接続先をモニタリングし、通話を制御する仮想デバイスです。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[デバイス（Device）] > [電話（Phone）]** の順に選択します。

[電話の検索と一覧表示（Find and List Phones）] ウィンドウが開きます。

ステップ 3 [新規追加（Add New）] を選択します。

ステップ 4 [電話のタイプ（Phone Type）] ドロップダウン リストから[CTI リモート デバイス（CTI Remote Device）] を選択します。続いて [次へ（Next）] を選択します。

[電話の設定（Phone Configuration）] ウィンドウが開きます。

ステップ 5 [オーナーのユーザ ID（Owner User ID）] ドロップダウン リストから対象のユーザ ID を選択します。

（注） [オーナーのユーザ ID（Owner User ID）] ドロップダウン リストには、モビリティの有効化が利用可能なユーザのみが表示されます。詳細については、「クライアントでの *SAML SSO* の有効化」を参照してください。

Cisco Unified Communications Manager は [デバイス名（Device Name）] フィールドをユーザ ID と [CTIRD] 接頭辞から生成します。例としては、[CTRID ユーザ名（CTIRDusername）] となります。

ステップ 6 必要に応じて、[デバイス名（Device Name）] フィールドのデフォルト値を編集します。

ステップ 7 [プロトコル固有情報（Protocol Specific Information）] セクションの [再ルーティング コーリング サーチ スペース（Rerouting Calling Search Space）] ドロップダウン リストから、適切なオプションを選択してください。

[再ルーティング コーリング サーチ スペース（Rerouting Calling Search Space）] ドロップダウン リストは、再ルーティングのコーリング サーチ スペースを定義します。これにより、ユーザは CTI リモート デバイスからコールを発信および受信できるようになります。

ステップ 8 必要に応じて、[電話の設定（Phone Configuration）] ウィンドウのその他の設定も指定します。

詳細については、『System Configuration Guide for Cisco Unified Communications Manager』の「*CTI remote device setup*」のトピックを参照してください。

ステップ 9 [保存（Save）] を選択します。

電話番号を関連付け、リモート接続先を追加するには、[電話の設定（Phone Configuration）] ウィンドウのフィールドから設定します。

リモート接続先の追加

リモート接続先とは、ユーザが利用できる CTI 制御可能デバイスです。

ユーザに専用 CTI リモート デバイスをプロビジョニングする場合、**Cisco Unified CM Administration** インターフェイスを使用してリモート接続先を追加する必要があります。このタスクにより、クライアントの起動時に、ユーザは自動的に電話を制御し、コールを発信できます。

ユーザにソフトフォン デバイスおよびデスクフォン デバイスとともに CTI リモート デバイスをプロビジョニングする場合、[Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを使用してリモート接続先を追加しないでください。ユーザは、クライアント インターフェイスを使用してリモート接続先を入力できます。

（注）
- ユーザ 1 人につき 1 つのリモート接続先を作成する必要があります。ユーザに対して複数のリモート接続先を追加しないでください。
- Cisco Unified Communications Manager は、**Cisco Unified CM Administration** インターフェイスで追加したリモート接続先がルーティング可能かどうかを確認しません。そのため、追加するリモート接続先を Cisco Unified Communications Manager がルーティングできることを確認する必要があります。
- Cisco Unified Communications Manager は、自動的に CTI リモート デバイスのすべてのリモート接続先番号にアプリケーション ダイヤル ルールを適用します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[デバイス（Device）] > [電話（Phone）]** の順に選択します。

[電話の検索と一覧表示（Find and List Phones）] ウィンドウが開きます。

ステップ 3 [電話を次の条件で検索（Find Phone where）] フィールドに適切なフィルタを指定し、[検索（Find）] を選択して電話の一覧を取得します。

ステップ 4 一覧から CTI リモート デバイスを選択します。

[電話の設定（Phone Configuration）] ウィンドウが開きます。

ステップ 5 [関連付けられたリモート接続先（Associated Remote Destinations）] セクションを探します。

ステップ 6 [新規リモート接続先の追加（Add a New Remote Destination）] を選択します。

[リモート接続先情報（Remote Destination Information）] ウィンドウが開きます。

ステップ 7 JabberRD を [名前（Name）] フィールドに指定します。

制約事項 [名前（Name）] フィールドに JabberRD を指定する必要があります。クライアントは JabberRD リモート接続先のみ使用します。JabberRD 以外の名前を指定した場合、ユーザはそのリモート接続先にアクセスできません。

ユーザがクライアントインターフェイスを使用してリモート接続先を追加すると、クライアントは JabberRD 名を自動的に設定します。

ステップ 8 [接続先番号（Destination Number）] フィールドに接続先番号を入力します。

ステップ 9 必要に応じて他の値をすべて指定します。

ステップ 10 [保存（Save）] を選択します。

次のタスク

次の手順を実行してリモート接続先を確認し、CTI リモート デバイスに設定を適用します。

1. 手順を繰り返し、CTI リモート デバイスの [電話の設定（Phone Configuration）] ウィンドウを開きます。
2. [関連付けられたリモート接続先（Associated Remote Destinations）]セクションを探します。
3. リモート接続先が利用可能であることを確認します。
4. [設定の適用（Apply Config）] を選択します。

（注） [電話の設定（Phone Configuration）] ウィンドウの [デバイス情報（Device Information）] セクションには、[アクティブなリモート接続先（Active Remote Destination）] フィールドが含まれています。

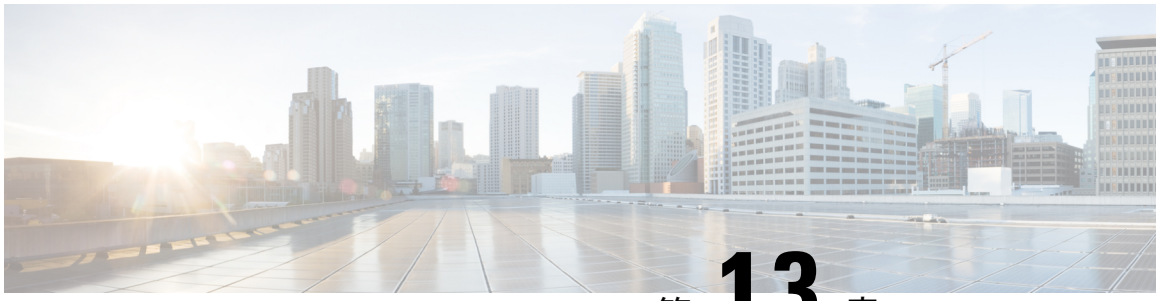
ユーザがクライアントでリモート接続先を選択すると、そのリモート接続先は [アクティブなリモート接続先（Active Remote Destination）] の値として表示されます。

次の場合、[アクティブなリモート接続先（Active Remote Destination）] の値として [none] が表示されます。

- ユーザがクライアントでリモート接続先を選択しない場合。
- ユーザが退出した場合、またはクライアントにサインインしていない場合。

第 III 部

設定（Configuration）



第 13 章

サービス ディスカバリの設定

サービス ディスカバリのオプション

サービスディスカバリにより、クライアントは自動的に企業のネットワークでサービスを検出することができます。次のいずれかのオプションを使用してサービスディスカバリを設定できます。

オプション	説明
DNS SRV レコードの確認 （92 ページ）	クライアントはサービスを自動的に検出して接続します。 これは推奨オプションです。
カスタマイゼーション （93 ページ）	インストール パラメータ、URL の設定、または企業モビリティ管理を使用してサービス検出をカスタマイズできます。
手動接続設定 （100 ページ）	手動接続設定は、サービス ディスカバリが使用されていない場合にフォールバック メカニズムを提供します。

DNS SRV レコードの確認

始める前に

『*Planning Guide for Cisco Jabber*』の「*Service Discovery*」の章で、SRV レコードの要件を確認してください。

手順

展開用のSRV レコードの作成：

オプション	説明
_cisco-uds	Cisco Unified Communications Managerの場所を提供します。クライアントは Cisco Unified Communications Manager からサービス プロファイルを取得してオーセンティケータを特定できます。
_collab-edge	Cisco VCS Expressway または Cisco Expressway-E の場所を提供します。クライアントは Cisco Unified Communications Manager からサービス プロファイルを取得してオーセンティケータを特定できます。

SRV レコードの例

```
_cisco-uds._tcp.DOMAIN service location:
priority = 0
weight = 0
port = 8443
svr hostname=_cisco-uds._tcp.example.com
```

次のタスク

SRV レコードのテスト （92 ページ）

SRV レコードのテスト

SRV レコードを作成したら、それらがアクセス可能かどうかを確認するためにテストします。

ヒント　Webベースのオプションをご希望の場合は、コラボレーションソリューションアナライザーサイトの SRV チェックツールを使用することもできます。

手順

ステップ 1 コマンド プロンプトを開きます。

ステップ 2 **nslookup** と入力します。

デフォルトの DNS サーバおよびアドレスが表示されます。これが想定された DNS サーバであることを確認してください。

ステップ 3 **set type=SRV** と入力します。

ステップ 4 各 SRV レコードの名前を入力します。

例：`_cisco-uds.exampledomain`

- サーバとアドレスが表示される：SRV レコードにアクセスできます。
- 「`_cisco-uds.exampledomain: Non-existent domain`」と表示される：SRV レコードに関する問題が存在します。

カスタマイゼーション

Windows のカスタマイゼーション

インストーラ スイッチ :Cisco Jabber for Windows

Cisco Jabber をインストールすると、オーセンティケータおよびサーバ アドレスを指定できます。インストーラは、ブートストラップ ファイルにこれらの詳細を保存します。ユーザがクライアントを初めて起動した際に、ブートストラップ ファイルを読み取ります。サービス ディスカバリが展開されている場合は、ブートストラップ ファイルが優先されます。

ブートストラップ ファイルは、サービス ディスカバリが展開されていない場合やユーザに手動で自分の接続設定を指定させたくない場合に、サービス ディスカバリのフォールバック メカニズムを提供します。

クライアントは、最初に起動したときのみ、ブートストラップ ファイルを読み取ります。クライアントは、最初の起動後にサーバ アドレスと設定をキャッシュし、以降の起動ではキャッシュからロードします。

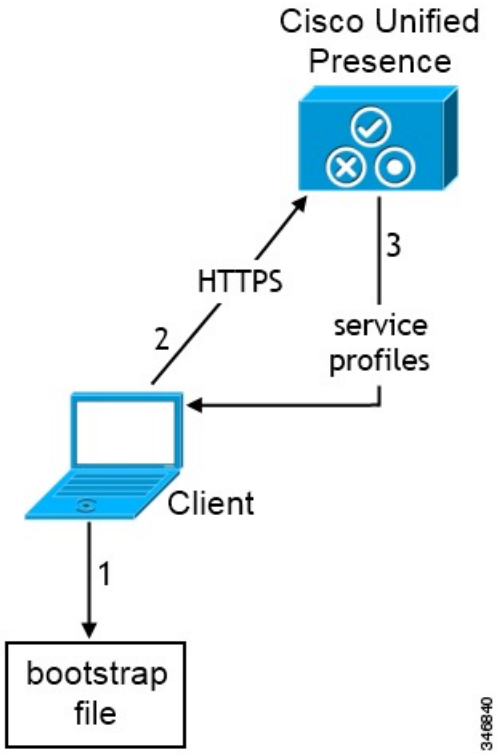
Cisco Unified Communications Managerリリース 9.x 以降を使用したオンプレミス展開では、ブートストラップ ファイルを使用せず、代わりに、サービス ディスカバリを使用することをお勧めします。

オンプレミスでの展開のブートストラップの設定

次の表は、さまざまな展開タイプの引数値を示します。

製品モード	サーバのリリース	引数値
フル UC（デフォルト モード）	リリース 9 以降： • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	次のインストーラ スイッチと値を使用する。 • AUTHENTICATOR=CUP • CUP_ADDRESS= <presence_server_address>
IM 専用（デフォルト モード）	リリース 9 以降： Cisco Unified Communications Manager IM and Presence Service	次のインストーラ スイッチと値を使用する。 • AUTHENTICATOR=CUP • CUP_ADDRESS= <presence_server_address>

次の図は、クライアントがオンプレミスでの展開の場合、ブートストラップ設定の使用法を示しています。



ユーザがクライアントを初めて起動する際に、次が実行されます。

1. クライアントは、ブートストラップ ファイルから設定を取得します。

   クライアントが、デフォルト モードで起動して、Cisco Unified Communications Manager IM and Presence サービスがオーセンティケータであると判断します。クライアントは、サー

ビス ディスカバリの結果により、その他の指示がなされない限り、プレゼンス サーバのアドレスを取得します。

2. クライアントが Cisco Unified Communications Manager IM and Presence サービスから認証され、設定を取得します。
3. クライアントは、プレゼンス サーバからサービス プロファイルを取得します。

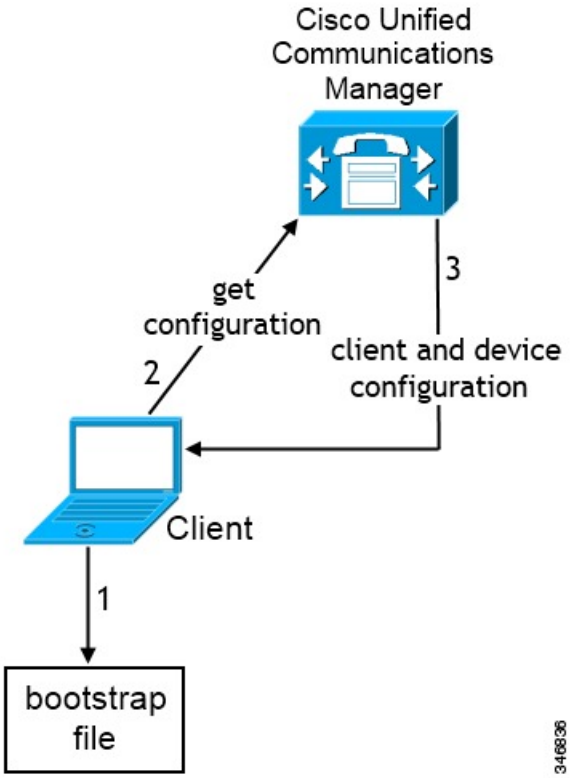
電話モードのオンプレミスの展開におけるブートストラップの設定

インストール中に、次のように引数の値を設定します。

- AUTHENTICATOR の値として `CUCM` を設定します。
- PRODUCT_MODE の値として `phone_mode` を設定します。
- TFTP の値として TFTP サーバ アドレスを設定します。
- CTI の値として CTI サーバ アドレスを設定します。
- CCMCIP の値として CCMCIP サーバ アドレスを設定します。

  Cisco Unified Communications Manager リリース 9.x 以前：Cisco Extension Mobility を有効にする場合は、CCMCIP に使用される Cisco Unified Communications Manager ノードで `Cisco Extension Mobility` サービスをアクティブにする必要があります。Cisco Extension Mobility の詳細については、使用している Cisco Unified Communications Manager のリリースに応じた『*Feature and Services*』ガイドを参照してください。

次の図は、電話モードの展開において、クライアントがブートストラップ設定をどのように使用できるかを示したものです。



ユーザがクライアントを初めて起動する際に、次プロセスが実行されます。

1. クライアントは、ブートストラップ ファイルから設定を取得します。

   クライアントが電話モードで起動して、Cisco Unified Communications Manager がオーセンティケータであると判断します。クライアントは、サービスディスカバリの結果が定まらない場合に、TFTP サーバ（および Jabber for Windows と Jabber for Mac の場合の CTI サーバ）のアドレスも取得します。

2. クライアントが Cisco Unified Communications Manager から認証され、設定を取得します。
3. クライアントは、デバイスおよびクライアント設定を取得します。

Mac およびモバイル のカスタマイゼーション

構成 URL ワークフロー

手順

	コマンドまたはアクション	目的
ステップ 1	構成 URL （97 ページ）	

	コマンドまたはアクション	目的
ステップ 2	Web サイトからの構成 URL のユーザへの提供 （99 ページ）	

構成 URL

ユーザが手動でサービス ディスカバリ情報を入力しなくても Cisco Jabber を起動できるようにするには、構成 URL を作成してユーザに配布します。

電子メールで直接、ユーザにリンクを送信するか、Web サイトにリンクを掲載することで、ユーザに構成 URL リンクを提供できます。

URL に次のパラメータを含めます。

- ServicesDomain：必須。すべての構成 URL に Cisco Jabber でのサービス ディスカバリに必要な IM and Presence サーバのドメインを含める必要があります。
- VoiceServiceDomain：IM and Presence サーバのドメインが音声サーバのドメインと異なるハイブリッド クラウドベースのアーキテクチャを展開する場合にのみ必要です。Cisco Jabber が音声サービスを検出できるようにするために、このパラメータを設定します。
- ServiceDiscoveryExcludedServices：任意。サービス ディスカバリ プロセスから次のサービスを除外できます。
  - Webexこの値を設定すると、クライアントは次のように動作します。
    - CAS 検索を実行しません。
    - 検索：
      - `_cisco-uds`
      - `_cuplogin`
      - `_collab-edge`
  - CUCM：この値を設定すると、クライアントは次のように動作します。
    - `_cisco-uds` を検索しません。
    - 検索：
      - `_cuplogin`
      - `_collab-edge`
  - CUP：この値を設定すると、クライアントは次のように動作します。
    - `_cuplogin` を検索しません。
    - 検索：
      - `_cisco-uds`

- _collab-edge

カンマで区切った複数の値を指定して、複数のサービスを除外できます。

3 つのサービスをすべて除外した場合、クライアントはサービス ディスカバリを実行せず、手動で接続設定を入力することをユーザに求めます。

- ServicesDomainSsoEmailPrompt：任意。ユーザのホーム クラスタを決定する際に、ユーザに対して電子メール プロンプトを表示するかどうかを指定します。
  - オン
  - オフ
- EnablePRTEncryption：任意。PRT ファイルの暗号化を指定します。Cisco Jabber for Mac で使用します。
  - true
  - false
- PRTCertificateName：任意。証明書の名前を指定します。Cisco Jabber for Mac で使用します。
- InvalidCertificateBehavior：任意。無効な証明書に対するクライアントの動作を指定します。
  - RejectAndNotify：警告ダイアログが表示され、クライアントはロードされません。
  - PromptPerSession：警告ダイアログが表示され、ユーザは無効な証明書を受け入れるか、または拒否できます。
- PRTCertificateUrl：信頼できるルート認証局の証明書ストアにある公開キーを含む証明書の名前を指定します。モバイル クライアント向け Cisco Jabber に適用されます。
- Telephony_Enabled：ユーザに対して電話機能を有効にするかどうかを指定します。デフォルトは true です。
  - はい
  - いいえ
- ForceLaunchBrowser：ユーザに外部ブラウザの使用を強制する場合に使用します。モバイル クライアント向け Cisco Jabber に適用されます。
  - はい
  - いいえ

（注） ForceLaunchBrowser は、クライアント証明書の展開および Android OS 5.0 よりも前のデバイスに使用されます。

- IP_Mode：Jabber クライアントのネットワーク IP プロトコルを指定します。
  - IPV4 のみ：Jabber は IPv4 接続のみ試行します。
  - IPV6 のみ：Jabber は IPv6 接続のみ試行します。
  - 2 つのスタック（デフォルト）：Jabber は IPv4 または IPv6 のいずれかと接続できます。

構成 URL は次の形式で作成します。

```
ciscojabber://provision?ServicesDomain=<domain_for_service_discover>
&VoiceServicesDomain=<domain_for_voice_services>
&ServiceDiscoveryExcludedServices=<services_to_exclude_from_service_discover>
&ServicesDomainSsoEmailPrompt=<ON/OFF>
```

（注） パラメータには大文字と小文字の区別があります。

例

- `ciscojabber://provision?ServicesDomain=cisco.com`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com`
- `ciscojabber://provision?ServicesDomain=service_domain &VoiceServicesDomain=voiceservice_domain&ServiceDiscoveryExcludedServices=WEBEX`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP &ServicesDomainSsoEmailPrompt=OFF`

Web サイトからの構成 URL のユーザへの提供

電子メールで直接、ユーザにリンクを送信するか、Web サイトにリンクを掲載することで、ユーザに構成 URL リンクを提供できます。

（注） Android オペレーティング システムの制約により、Cisco Jabber for Android ユーザが Android アプリケーションから直接構成 URL を開くと、問題が発生することがあります。この問題を回避するために、Web サイトを使用して構成 URL リンクを配布することをお勧めします。

URL プロビジョニングのために Web サイト探索オプションを使用する場合は、Mozilla Firefox を使用することをお勧めします。

Web サイトからリンクを配布するには、次の手順を実行します。

手順

ステップ 1 HTML ハイパーリンクとして構成 URL を含む内部 Web ページを作成します。

ステップ 2 内部 Web ページへのリンクを電子メールでユーザに送信します。

その電子メールのメッセージで、次の手順を実行するようにユーザに指示します。

1. クライアントをインストールします。
2. 電子メール メッセージ内のリンクをクリックして、内部 Web ページを開きます。
3. 内部 Web ページ上のリンクをクリックして、クライアントを設定します。

手動接続設定

手動接続設定は、サービス ディスカバリが使用されていない場合にフォールバック メカニズムを提供します。

Cisco Jabber を起動すると、[詳細設定（Advanced settings）] ウィンドウでオーセンティケータとサーバ アドレスを指定できます。クライアントは、その後の起動時にロードするローカル アプリケーション設定にサーバ アドレスをキャッシュします。

Cisco Jabber は、次のような場合に、最初の起動時にこれらの詳細設定を入力するようにユーザに要求します。

- Cisco Unified Communications Manager リリース 9.x 以降を使用したオンプレミス：クライアントがサービス プロファイルからオーセンティケータとサーバ アドレスを取得できない場合。

ユーザが [詳細設定（Advanced settings）] ウィンドウで入力した設定は、SRV レコードやブートストラップの設定を含め、その他のソースよりも優先されます。

[Cisco IM & Presence] を選択すると、クライアントは Cisco Unified Communications Manager IM and Presence サービスから UC サービスを取得します。クライアントはサービス プロファイルまたは SSO 検出を使用しません。

（注） Cisco Jabber for Windows の場合、SRV レコードが解決されるサーバ数に関わらず、サービス検出は 20 秒後に停止します。サービス検出中に Cisco Jabber が `_cisco-uds` を検出すると、20 秒以内に最初の 2 つのサーバへの接続が試みられます。優先順位が高い 2 つのサーバに対するサービス検出の試行後は、Cisco Jabber はサーバへの接続を試みません。

ユーザは、稼働中のサーバを手動で指定するか、サービス検出の対象となる 2 つの優先順位の高いサーバのうち少なくとも 1 つのサーバを指定するように、SRV の優先順位を並べ替えることができます。

サービス ディスカバリの自動接続設定

[詳細設定（Advanced settings）] ウィンドウで [自動（Automatic）] オプションを選択することによって、サーバを自動で検出できます。

この自動オプションにより、ユーザがサービス接続の詳細を手動で設定する方法から、サービス ディスカバリを使用する方法に変更することができます。たとえば、最初の起動時に、[詳細設定（Advanced settings）] ウィンドウで、手動でオーセンティケータを設定し、サーバアドレスを指定します。

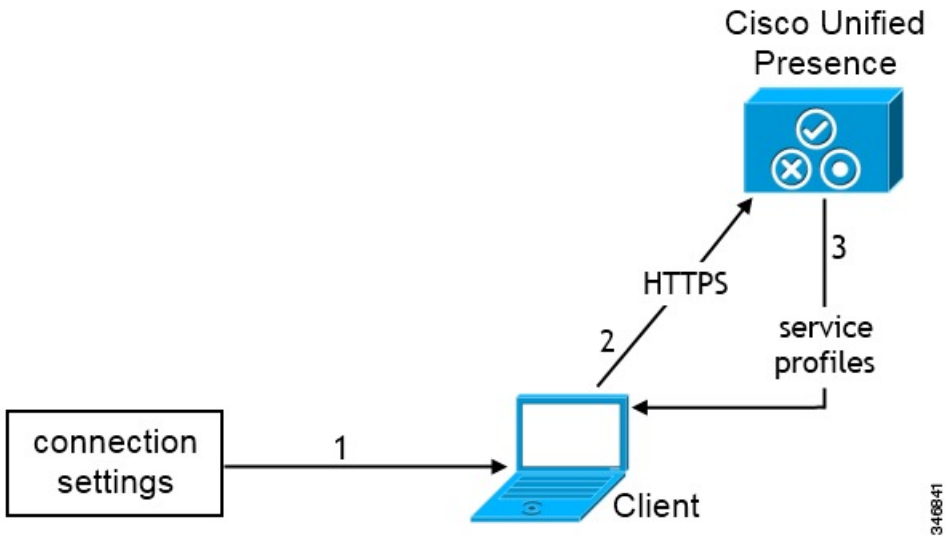
クライアントは、手動設定のキャッシュを常にチェックします。手動設定は、SRV レコードより優先され、Cisco Jabber for Windows ではブートストラップ ファイルより優先されます。したがって SRV レコードを配置し、サービス ディスカバリを使用する場合は、最初の電源投入から手動設定を上書きする必要があります。

オンプレミス展開の手動接続設定

ユーザは、[詳細設定（Advanced settings）] ウィンドウで、Cisco Unified Presence または Cisco Unified Communications Manager IM and Presence サービスをオーセンティケータとして設定し、サーバ アドレスを指定できます。

メモ `_cuplogin` SRV レコードを使用して、デフォルトのサーバアドレスを自動的に設定することもできます。

次の図は、オンプレミスの展開において、クライアントが手動接続設定をどのように使用できるかを示したものです。



1. ユーザが [詳細設定（Advanced settings）] ウィンドウで手動で接続設定を入力します。

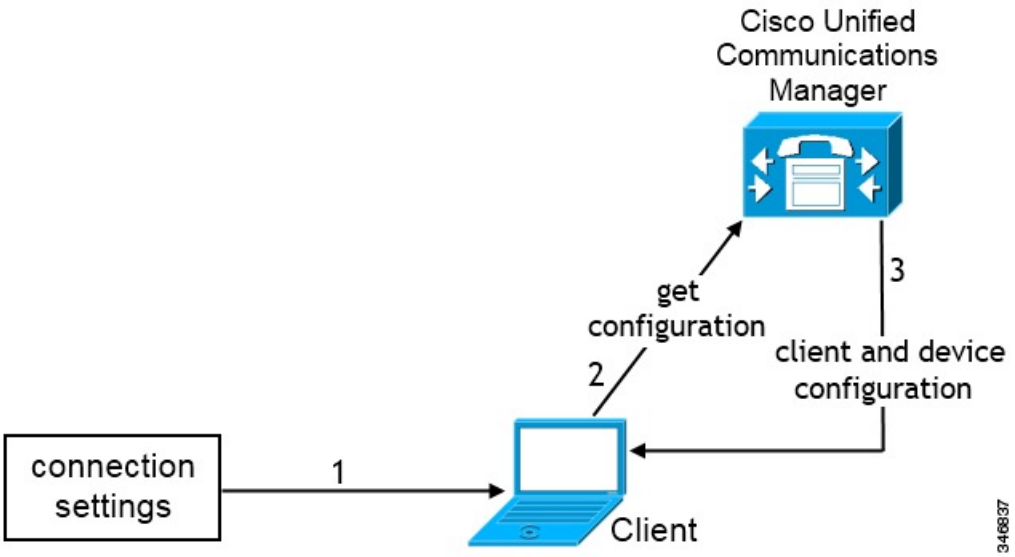
2. クライアントが Cisco Unified Presence または Cisco Unified Communications Manager IM and Presence サービスの認証を受けます。
3. クライアントは、プレゼンス サーバからサービス プロファイルを取得します。

電話モードのオンプレミスの展開における手動接続設定

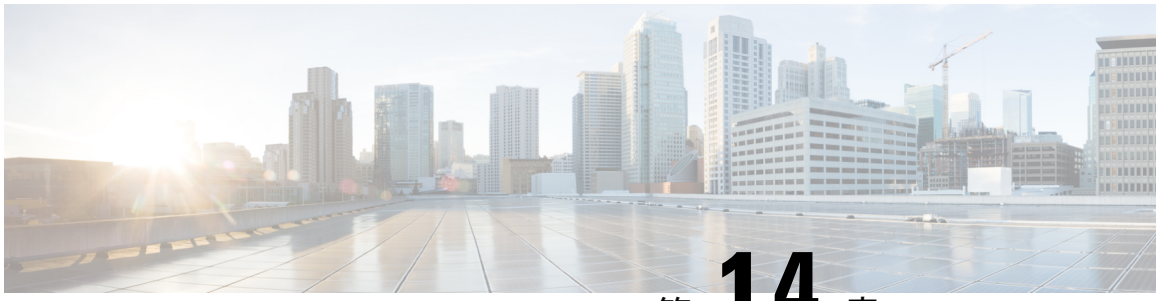
ユーザは、[**詳細設定（Advanced settings**）] ウィンドウで、Cisco Unified Communications Manager をオーセンティケータに設定し、次のサーバ アドレスを指定できます。

- TFTP サーバ
- CCMCIP サーバ
- CTI サーバ（Cisco Jabber for Windows と Cisco Jabber for Mac）

次の図は、電話モードの展開において、クライアントが手動接続設定をどのように使用できるかを示したものです。



1. ユーザが [詳細設定（Advanced settings）] ウィンドウで手動で接続設定を入力します。
2. クライアントが Cisco Unified Communications Manager から認証され、設定を取得します。
3. クライアントは、デバイスおよびクライアント設定を取得します。



第 14 章

証明書検証の設定

オンプレミス展開用の証明書の設定

証明書は、Jabber クライアントが接続するサービスごとに必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Unified Presence または Cisco Unified Communications Manager IM and Presence サービスを使用している場合は、該当する HTTP（tomcat）証明書と XMPP 証明書をダウンロードします。	詳細については、『Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager』の「*Security Configuration on IM and Presence Service*」の章を参照してください。
ステップ 2	Cisco Unified Communications Manager と Cisco Unity Connection 用の HTTPS（tomcat）証明書をダウンロードします。	詳細については、ここで『*Cisco Unified Communications Manager Security Guide*』と『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。
ステップ 3	Cisco Webex Meetings サーバ用の HTTP（tomcat）をダウンロードします。	詳細については、ここで『*Cisco Cisco Webex Meetings Server Administration Guide*』を参照してください。
ステップ 4	リモート アクセスを設定する場合は、Cisco VCS Expressway と Cisco Expressway-E のサーバ証明書をダウンロードします。このサーバ証明書は、HTTP と XMPP の両方に使用されます。	詳細については、『Configuring Certificates on Cisco VCS Expressway』を参照してください。

	コマンドまたはアクション	目的
ステップ 5	証明書署名要求（CSR）を生成します。	
ステップ 6	サービスに証明書をアップロードします。	マルチサーバ SAN を使用している場合は、クラスタと tomcat 証明書ごとに一度ずつと クラスタと XMPP 証明書ごとに一度ずつサービスに証明書をアップロードする必要があるだけです。マルチサーバ SAN を使用していない場合は、すべての Cisco Unified Communications Manager ノードのサービスに証明書をアップロードする必要があります。
ステップ 7	クライアントへの CA 証明書の展開 （104 ページ）	証明書を承認または却下するためのプロンプトを表示せずに証明書の検証が行われることを保証するには、クライアントのローカル証明書ストアに証明書を展開します。

クライアントへの CA 証明書の展開

証明書を承認または却下するためのプロンプトを表示せずに証明書検証が実施されることを保証するには、エンドポイント クライアントのローカル証明書ストアに証明書を展開します。

既存のパブリック CA を使用している場合は、CA 証明書がクライアント証明書ストアまたはキーチェーン上に存在している可能性があります。その場合は、CA 証明書をクライアントに展開する必要はありません。

CA 証明書がクライアント証明書ストアまたはキーチェーン上に存在しない場合は、CA 証明書をクライアントに展開します。

展開規模	推奨内容
ローカル マシンが多数の場合	グループ ポリシーや証明書展開管理アプリケーションなどの証明書展開ツールを使用する。
ローカル マシンが少数の場合	手動で CA 証明書を展開する。

Cisco Jabber for Windows クライアントへの CA 証明書の手動展開

手順

ステップ 1 Cisco Jabber for Windows クライアント マシンで CA 証明書を使用できるようにします。

ステップ 2 Windows マシンで、証明書ファイルを開きます。

ステップ 3 証明書をインストールしてから、[次へ（Next）] をクリックします。

ステップ 4 [証明書をすべて次のストアに配置する（Place all certificates in the following store）] を選択してから、[参照（Browse）] を選択します。

ステップ 5 [信頼されたルート証明機関（Trusted Root Certification Authorities）] ストアを選択します。ウィザードを終了すると、正常な証明書インポートを確認するためのメッセージが表示されます。

次のタスク

Windows Certificate Manager ツールを起動することによって、証明書が正しい証明書ストアにインストールされていることを確認します。**[信頼されたルート証明機関（Trusted Root Certification Authorites）] > [証明書（Certificates）]** を参照します。CA ルート証明書が証明書ストアに一覧表示されます。

Cisco Jabber for Mac クライアントへの CA 証明書の手動展開

手順

ステップ 1 Cisco Jabber for Mac クライアント マシンで CA 証明書を使用できるようにします。

ステップ 2 Mac マシンで、証明書ファイルを開きます。

ステップ 3 現在のユーザのみのログイン キーチェーンに追加して、[追加（Add）] を選択します。

次のタスク

キーチェーン アクセス ツールを開いて、[証明書（Certificates）] を選択することによって、証明書が正しいキーチェーンにインストールされていることを確認します。キーチェーン内の CA ルート証明書が一覧表示されます。

モバイル クライアントへの CA 証明書の手動展開

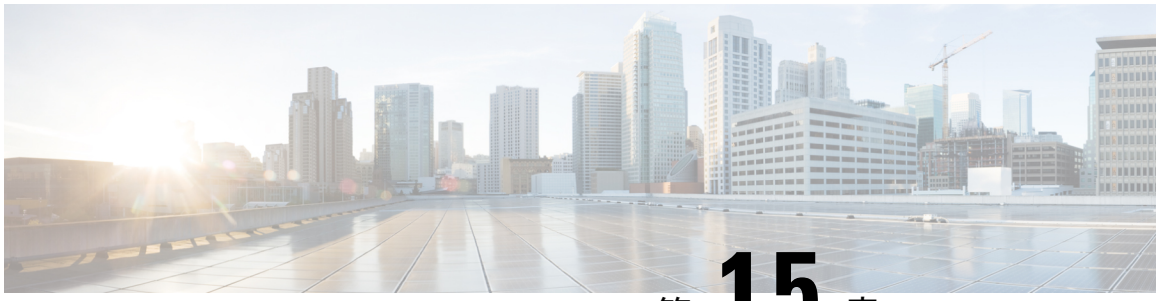
CA 証明書を iOS クライアントに展開するには、証明書展開管理アプリケーションが必要です。CA 証明書をユーザに電子メールで送信することも、ユーザがアクセス可能な Web サーバ上で証明書を公開することもできます。ユーザは証明書展開管理ツールを使用して証明書をダウンロードしてインストールできます。

ただし、Cisco Jabber for Android には証明書管理ツールが付属していないため、次の手順を実行する必要があります。

手順

ステップ 1 CA 証明書をデバイスにダウンロードします。

ステップ 2 デバイスで **[設定（Settings）] > [セキュリティ（Security）] > [デバイスストレージからインストール（Install from device storage）]** の順にタップして、画面上の指示に従います。



第 15 章

クライアントの設定

クライアント設定のワークフロー

手順

	コマンドまたはアクション	目的
ステップ 1	クライアント設定の概要	
ステップ 2	統一された *CM*(最高の優先順位) でクライアント設定パラメータを設定するか、クライアント設定ファイルを作成してホストします。	
ステップ 3	電話の設定でのパラメータの設定：デスクトップ クライアント向け	
ステップ 4	電話の設定でのパラメータの設定：モバイル クライアント向け	
ステップ 5	プロキシ設定の設定: オプション	

クライアント設定の概要

Cisco Jabber は、次のソースから設定を取得できます。

- サービス プロファイル：Cisco Unified Communications Manager リリース 9 以降の UC サービスプロファイルで一部のクライアント設定を構成できます。ユーザがクライアントを起動すると、クライアントは DNS SRV レコードを使用して Cisco Unified Communications Manager ホーム クラスタを検出し、自動的に UC サービス プロファイルから設定を取得します。
- 電話の設定：Cisco Unified Communications Manager リリース 9 以降の電話の設定で一部のクライアント設定を構成できます。クライアントは、UC サービス プロファイルの設定に加え、電話の設定から設定を取得します。
- Cisco Unified Communications Manager IM and Presence サービス：インスタント メッセージおよびプレゼンスの機能を有効にして、プレゼンス サブスクリプション要求などの特定の設定を構成できます。

  [**詳細設定（Advanced settings**）] ウィンドウで [**Cisco IM & Presence**] を選択すると、クライアントが Cisco Unified Communications Manager IM and Presence サービスから UC サービスを取得します。クライアントはサービスプロファイルまたはSSO検出を使用しません。
- クライアント設定 : ユーザがサインインしたときに適用されるクライアント設定パラメータを設定できます。次のいずれかを行います。
  - Unified CM でクライアント設定パラメータを設定します。
  - 設定パラメータを含むXMLエディタを使ってXMLファイルを作成します。その後、TFTP サーバで XML ファイルをホストします。

Unified CM でのクライアント設定パラメータの設定

クライアントの設定パラメータを設定し、Unified CM でサービス プロファイルに割り当てます。

Cisco Jabber for iPhone and iPad および Cisco Jabber for Androidについては、次のようにパラメータを設定する必要があります。

- オンプレミス展開のディレクトリ統合。
- ハイブリッドクラウド展開のボイスメール サービス クレデンシャル。

（注） ほとんどの環境で、Cisco Jabber for Windows と Cisco Jabber for Mac は、サービスに接続するための設定を必要としません。自動更新、問題報告、ユーザ ポリシーとオプションなどのカスタム コンテンツが必要な場合にのみ、設定パラメータを作成します。

手順

ステップ 1 Jabber 設定パラメータの定義 （109 ページ）

ステップ 2 サービスプロファイルへの Jabber クライアント設定の割り当て （109 ページ）

Jabber 設定パラメータの定義

統一された CM を使用すると、Jabber クライアントの設定を含む UC サービスに関する情報の追加、検索、表示、および保守を行うことができます。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [UC サービス（UC Service）]** を選択します。

ステップ 3 [新規追加（Add New）] を選択します。

ステップ 4 **UC サービス タイプ**として **Jabber クライアント設定（jabber-config.xml）**を選択します。

ステップ 5 [Next] を選択します。

ステップ 6 [**UC サービス情報 (UC Service Information)**] セクションで名前を入力します。詳細な要件については、「統一型ヘルプ」を参照してください。

ステップ 7 パラメータの詳細については、**Jabber 設定パラメータ**セクションでパラメータを入力してください。パラメータの詳細については、『*Cisco Jabber* のパラメータリファレンスガイド』の最新版を参照してください。

ステップ 8 [保存（Save）] を選択します。

サービスプロファイルへの Jabber クライアント設定の割り当て

統一 CM を使用すると、サービスプロファイルを使用して Jabber クライアント設定をユーザに割り当てることができます。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [サービス プロファイル（Service Profile）]** の順に選択します。

ステップ 3 [**新規追加** (Add New)] を選択するか、または jabber クライアントの設定に割り当てる既存のサービスプロファイルを選択します。

ステップ 4 [Jabber クライアント設定 (jabber-config)] セクションで、プロファイルに適用する設定の名前を選択します。

ステップ 5 [保存（Save）] を選択します。

クライアント設定ファイルの作成とホスト

クライアント設定ファイルを作成して、それらを Cisco Unified Communications Manager TFTP サービス上でホストします。

Cisco Jabber for iPhone and iPad と Cisco Jabber for Android では、以下をセットアップするためにグローバル コンフィギュレーション ファイルを作成する必要があります。

- オンプレミス展開のディレクトリ統合。
- ハイブリッドクラウド展開のボイスメール サービス クレデンシャル。

（注） ほとんどの環境で、Cisco Jabber for Windows と Cisco Jabber for Mac は、サービスに接続するための設定を必要としません。自動更新、問題報告、ユーザポリシーとオプションなどのカスタム コンテンツが必要な場合にのみ、コンフィギュレーション ファイルを作成します。

始める前に

次のコンフィギュレーション ファイル要件に注意してください。

- コンフィギュレーションファイル名には大文字と小文字の区別があります。エラーを回避し、クライアントが TFTP サーバからファイルを取得できるよう、ファイル名には小文字を使用してください。
- 設定ファイルには、utf-8 エンコーディングを使用してください。
- クライアントは、有効な XML 構造のない設定ファイルは読み込めません。設定ファイルの構造で終了要素をチェックし、その要素が正しくネストされていることを確認します。
- 設定ファイルでは、有効な XML 文字エンティティ参照のみが許可されます。たとえば、&の代わりに&を使用します。XML に無効な文字が含まれている場合は、クライアントは設定ファイルを解析できません。

  コンフィギュレーション ファイルを検証するには、Microsoft Internet Explorer でそのファイルを開きます。

  - Internet Explorer に XML 構造全体が表示された場合、設定ファイルは有効です。
  - Internet Explorer に XML 構造の一部しか表示されない場合は、設定ファイルに無効な文字またはエンティティが含まれている可能性があります。

手順

	コマンドまたはアクション	目的
ステップ 1	TFTP サーバ アドレスの指定 （111 ページ）	クライアントが設定ファイルにアクセスできるようにするための TFTP サーバ アドレスを指定します。
ステップ 2	グローバル設定の作成 （112 ページ）	展開でユーザ用のクライアントを設定します。
ステップ 3	グループ設定の作成 （113 ページ）	ユーザのセットごとに異なる設定を適用します。
ステップ 4	設定ファイルのホスト （114 ページ）	TFTP サーバ上でコンフィギュレーション ファイルをホストします。
ステップ 5	TFTP サーバの再起動 （114 ページ）	TFTP サーバを再起動して、クライアントがコンフィギュレーション ファイルにアクセスできるようにします。

TFTP サーバ アドレスの指定

クライアントは、TFTP サーバから設定ファイルを取得します。

手順

	コマンドまたはアクション	目的
ステップ 1	クライアントが設定ファイルにアクセスできるようにするための TFTP サーバ アドレスを指定します。	**注目** Cisco Jabber が DNS クエリーから `_cisco-uds` SRV レコードを取得すれば、自動的にユーザのホーム クラスタを特定できます。その結果、クライアントは Cisco Unified Communications Manager TFTP サービスを特定することもできます。 `_cisco-uds` SRV レコードを展開する場合は、TFTP サーバ アドレスを指定する必要はありません。

電話モードでの TFTP サーバの指定

手順

	コマンドまたはアクション	目的
ステップ 1	電話機モードでクライアントを展開する場合、TFTP サーバのアドレスを次のように指定できます。 • ユーザはクライアントの起動時に、TFTP サーバ アドレスを手動で入力します。 • TFTP 引数を使用してインストール時に TFTP サーバ アドレスを指定します。	

グローバル設定の作成

クライアントは、サインイン シーケンスの間に TFTP サーバからグローバル設定ファイルをダウンロードします。展開に含まれるすべてのユーザに対してクライアントを設定します。

始める前に

設定ファイルの構造が有効でない場合、クライアントは設定した値を読み取ることができません。詳細については、この章の XML サンプルを確認してください。

手順

ステップ 1 任意のテキスト エディタで `jabber-config.xml` という名前のファイルを作成します。

- ファイル名には小文字を使用してください。
- UTF-8 エンコーディングを使用してください。

ステップ 2 `jabber-config.xml` で必要な設定パラメータを定義します。

ステップ 3 TFTP サーバ上でグループ設定ファイルをホストします。

環境内に複数の TFTP サーバが存在する場合は、すべての TFTP サーバのコンフィギュレーション ファイルが同じであることを確認します。

グループ設定の作成

グループ コンフィギュレーション ファイルは、ユーザのサブセットに適用され、Cisco Jabber for desktop（CSF デバイス）モバイルと Cisco Jabber for mobile デバイスでサポートされます。グループ設定ファイルは、グローバル設定ファイルよりも優先されます。

CSFデバイスでユーザをプロビジョニングする場合は、デバイス設定の[シスコサポートフィールド（Cisco Support Field）] フィールドでグループ コンフィギュレーション ファイル名を指定します。ユーザがCSFデバイスを所有していない場合は、インストール中にTFTP_FILE_NAME引数を使用してグループごとに一意のコンフィギュレーション ファイル名を設定します。

始める前に

設定ファイルの構造が有効でない場合、クライアントは設定した値を読み取ることができません。詳細については、この章の XML サンプルを確認してください。

手順

ステップ 1 任意のテキスト エディタを使用して XML グループ設定ファイルを作成します。

グループ設定ファイルには、適切な名前を指定できます（例：`jabber-groupa-config.xml`）。

ステップ 2 グループ設定ファイルで必須の設定パラメータを定義します。

ステップ 3 該当する CSF デバイスにグループ コンフィギュレーション ファイルを追加します。

a) [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

b) **[デバイス（Device）] > [電話（Phone）]** の順に選択します。

c) グループ設定ファイルを適用する適切な CSF デバイスを検索して選択します。

d) [電話の設定（Phone Configuration）] ウィンドウで、**[プロダクト固有の設定（Product Specific Configuration Layout）] > [デスクトップクライアント設定（Desktop Client Settings）]** に移動します。

e) [シスコサポートフィールド（Cisco Support Field）] フィールドに、`configurationfile=group_configuration_file_name.xml` と入力します。たとえば、`configurationfile=groupa-config.xml` と入力します。

（注） TFTP サーバ上でデフォルト ディレクトリ以外の場所にあるグループ設定ファイルをホストする場合は、パスとファイル名を指定する必要があります（例：`configurationfile=/customFolder/groupa-config.xml`）。

複数のグループ設定ファイルは追加しないでください。クライアントは [シスコサポート フィールド（Cisco Support Field）] フィールドの最初のグループ設定のみを使用します。

f) [保存（Save）] を選択します。

ステップ 4 TFTP サーバ上でグループ設定ファイルをホストします。

設定ファイルのホスト

設定ファイルは任意の TFTP サーバでホストできます。ただし、デバイス設定ファイルが存在する Cisco Unified Communications Manager TFTP サーバで設定ファイルをホストすることをお勧めします。

手順

ステップ 1 Cisco Unified Communications Manager で **Cisco Unified OS の管理**インターフェイスを開きます。

ステップ 2 **[ソフトウェアのアップグレード（Software Upgrades）] > [TFTP ファイル管理（TFTP File Management）]** を選択します。

ステップ 3 [ファイルのアップロード（Upload File）] を選択します。

ステップ 4 [ファイルのアップロード（Upload File）] セクションで [参照（Browse）] を選択します。

ステップ 5 ファイル システム上の設定ファイルを選択します。

ステップ 6 [ファイルのアップロード（Upload File）] セクションの [ディレクトリ（Directory）] テキスト ボックスに値を指定しないでください。

設定ファイルが TFTP サーバのデフォルト ディレクトリに格納されるように、[ディレクトリ（Directory）] テキスト ボックスの値は空のままにします。

ステップ 7 [ファイルのアップロード（Upload File）] を選択します。

TFTP サーバの再起動

クライアントが設定ファイルにアクセスできるようにするには、その前に TFTP サーバを再起動する必要があります。

手順

ステップ 1 Cisco Unified Communications Manager で **Cisco Unified Serviceability** インターフェイスを開きます。

ステップ 2 **[ツール（Tools）] > [コントロール センターの機能サービス（Control Center - Feature Services）]** を選択します。

ステップ 3 [CM サービス（CM Services）] セクションから [Cisco Tftp] を選択します。

ステップ 4 [リスタート（Restart）] を選択します。

再起動の確認を求めるウィンドウが表示されます。

ステップ 5 [OK] を選択します。

「Cisco Tftp サービスの再起動操作が成功しました（Cisco Tftp Service Restart Operation was Successful）」というステータスが表示されます。

ステップ 6 [更新（Refresh）] を選択し、Cisco Tftp サービスが正常に起動していることを確認します。

次のタスク

設定ファイルが TFTP サーバで使用できることを確認するには、任意のブラウザで設定ファイルを開きます。通常、`http://tftp_server_address:6970/jabber-config.xml` の URL にあるグローバル設定ファイルにアクセスできます。

設定ファイル

jabber-config.xml 設定ファイルの構造、グループ要素、パラメータ、および例については、『Parameters Reference Guide for Cisco Jabber』を参照してください。

電話の設定でのパラメータの設定：デスクトップクライアント向け

クライアントは、Cisco Unified Communications Manager 上の次の場所から電話の各種設定を取得できます。

[エンタープライズ電話の設定（Enterprise Phone Configuration）]

クラスタ全体に適用されます。

（注） IM and Presence サービス機能のみを使用しているユーザ（IM 専用）の場合は、[エンタープライズ電話の設定（Enterprise Phone Configuration）] ウィンドウで電話の設定パラメータを設定する必要があります。

[共通の電話プロファイルの設定（Common Phone Profile Configuration）]

デバイスのグループに適用され、クラスタの設定よりも優先されます。

[Cisco Unified Client Services Framework（CSF）電話機の設定（Cisco Unified Client Services Framework (CSF) Phone Configuration）]

個別の CSF デバイスに適用され、グループの設定よりも優先されます。

電話の設定のパラメータ

次の表は、電話の設定の [プロダクト固有の設定（Product Specific Configuration Layout）] セクションで設定できる、およびクライアントの設定ファイルからの対応するパラメータをマッピングできる設定パラメータを示します。

デスクトップ クライアントの設定	説明
ビデオ コール（Video Calling）	ビデオ機能を有効または無効にします。 **有効（Enabled）（デフォルト）** ユーザはビデオ通話を送受信できます。 **無効（Disabled）** ユーザはビデオ通話を送受信できません。 **制約事項** このパラメータは、CSF のデバイス構成でのみ使用可能です。
ファイル転送でブロックするファイル タイプ（File Types to Block in File Transfer）	ユーザによる特定のファイル タイプの転送を制限します。 値として、`.exe` などのファイル拡張子を設定します。 複数のファイル拡張子を区切るには、セミコロンを使用します。例： `.exe;.msi;.rar;.zip`
電話制御で自動的に開始（Automatically Start in Phone Control）	クライアント初回起動時のユーザの電話タイプを設定します。初回の起動後にユーザは電話のタイプを変更できます。クライアントは、ユーザ設定を保存し、以降の起動でその設定を使用します。 **有効（Enabled）** 通話にデスクフォン デバイスを使用します。 **無効（Disabled）（デフォルト）** 通話にソフトフォン（CSF）デバイスを使用します。
Jabber For Windows ソフトウェア アップデート サーバ URL（Jabber For Windows Software Update Server URL）	クライアント アップデート情報を保持する XML 定義ファイルへの URL を指定します。クライアントは、この URL を使用して Web サーバから XML ファイルを取得します。 ハイブリッド クラウド導入環境では、Cisco Webex を使用して自動更新を設定することをお勧めします。
問題レポート サーバ URL（Problem Report Server URL）	ユーザが問題レポートを送信できるようにするカスタム スクリプトの URL を指定します。

電話の設定でのパラメータの設定：モバイルクライアント向け

クライアントは、Cisco Unified Communications Manager 上の次の場所から電話の各種設定を取得できます。

- [Cisco Dual Mode for iPhone（TCT）設定（Cisco Dual Mode for iPhone (TCT) Configuration）]：個別の TCT デバイスに適用され、グループ設定より優先されます。
- [Cisco Jabber for Tablet（TAB）設定（Cisco Jabber for Tablet (TAB) Configuration）]：個別の TAB デバイスに適用され、グループ設定より優先されます。

電話の設定のパラメータ

次の表は、電話の設定の [プロダクト固有の設定（Product Specific Configuration Layout）] セクションで設定できる、およびクライアントの設定ファイルからの対応するパラメータをマッピングできる設定パラメータを示します。

デスクトップ クライアントの設定	説明
ビデオ コール（Video Calling）	ビデオ機能を有効または無効にします。 **有効（Enabled）（デフォルト）** ユーザはビデオ通話を送受信できます。 **無効（Disabled）** ユーザはビデオ通話を送受信できません。 **制約事項** このパラメータは、CSF のデバイス構成でのみ使用可能です。
ファイル転送でブロックするファイル タイプ（File Types to Block in File Transfer）	ユーザによる特定のファイル タイプの転送を制限します。 値として、`.exe` などのファイル拡張子を設定します。 複数のファイル拡張子を区切るには、セミコロンを使用します。例： `.exe;.msi;.rar;.zip`

デスクトップ クライアントの設定	説明
電話制御で自動的に開始（Automatically Start in Phone Control）	クライアント初回起動時のユーザの電話タイプを設定します。初回の起動後にユーザは電話のタイプを変更できます。クライアントは、ユーザ設定を保存し、以降の起動でその設定を使用します。 **有効（Enabled）** 通話にデスクフォン デバイスを使用します。 **無効（Disabled）（デフォルト）** 通話にソフトフォン（CSF）デバイスを使用します。
Jabber For Windows ソフトウェア アップデート サーバ URL（Jabber For Windows Software Update Server URL）	クライアント アップデート情報を保持する XML 定義ファイルへの URL を指定します。クライアントは、この URL を使用して Web サーバから XML ファイルを取得します。
問題レポート サーバ URL（Problem Report Server URL）	ユーザが問題レポートを送信できるようにするカスタム スクリプトの URL を指定します。

任意のプロキシ設定

クライアントは、プロキシ設定を使用してサービスに接続する場合があります。

次の制限は、これらの HTTP 要求にプロキシを使用する場合に適用されます。

- プロキシ認証はサポートされていません。
- バイパス リストのワイルドカードはサポートされています。
- Cisco Jabber は、HTTP CONNECT を使用した HTTP 要求に対してプロキシをサポートしますが、HTTPS CONNECT が使用された場合はプロキシをサポートしません。
- Web プロキシの自動検出（WPAD）はサポートされていないため、無効にする必要があります。

必要に応じて、クライアント タイプの手順に従ってプロキシ設定を行います。

Cisco Jabber for Windows のプロキシ設定

インターネットプロパティのローカル エリア ネットワーク（LAN）設定での、Windows のプロキシ設定を行います。

手順

ステップ 1 [接続（Connections）] タブを選択し、[LAN の設定（LAN Settings）] を選択します。

ステップ 2 次のいずれかのオプションを使用してプロキシを設定します。

- 自動設定の場合は、.pac ファイルの URL を指定します。
- プロキシ サーバの場合は、明示的なプロキシ アドレスを指定します。

Cisco Jabber for Mac のプロキシ設定

[システム設定（System Preferences）] で Mac のプロキシ設定を行います。

手順

ステップ 1 **[システム設定（System Preferences）] > [ネットワーク（Network）]**の順に選択します。

ステップ 2 リストからネットワーク サービスを選択して、**[詳細（Advanced）] > [プロキシ（Proxies）]** の順に選択します。

ステップ 3 次のいずれかのオプションを使用してプロキシを設定します。

- 自動設定の場合は、.pac ファイルの URL を指定します。
- プロキシ サーバの場合は、明示的なプロキシ アドレスを指定します。

Cisco Jabber iPhone and iPad のプロキシ設定

iOS デバイスの Wi-Fi 設定で、次のいずれかの方法でプロキシ設定を構成します。

手順

ステップ 1 **[Wi-Fi] > [HTTP プロキシ（HTTP PROXY）] > [自動（Auto）]**の順に選択し、.pac ファイルの URL を自動設定スクリプトとして指定します。

ステップ 2 **[Wi-Fi] > [HTTP プロキシ（HTTP PROXY）] > [手動（Manual）]**の順に選択し、明示的なプロキシ アドレスを指定します。

Cisco Jabber for Android のプロキシ設定

手順

Android デバイスの Wi-Fi 設定で、次のいずれかの方法でプロキシ設定を構成します。

- **[Wi-Fi]** > **[ネットワークを変更（Modify Network）]** > **[詳細オプションを表示（Show Advanced Options）]** > **[プロキシ設定（Proxy Settings）]** > **[自動（Auto）]** タブで、自動設定スクリプトとして .pac ファイルの URL を指定します。

  （注） この方法は、Android OS 5.0 以降および Cisco DX シリーズのデバイスでのみサポートされます。

- **[Wi-Fi ネットワーク（Wi-Fi Networks）]** > **[ネットワークを変更（Modify Network）]** > **[詳細オプションを表示（Show Advanced Options）]** > **[プロキシ設定（Proxy Settings）]** > **[自動（Auto）]** タブで、明示的なプロキシ アドレスを指定します。

第 16 章

Cisco Jabber アプリケーションおよび Jabber ソフトフォンの VDI 用の展開

Cisco Jabber クライアントのダウンロード

必要に応じて、そのクライアントに対応したオペレーティング システムから署名ツールを使用して、Jabber インストーラまたは Cisco Dynamic Libraries にユーザ独自のカスタマー署名を追加することができます。

（注） Cisco Jabber for Mac の場合、インストーラには製品のインストーラ ファイルが含まれています。端末ツールを使用してインストーラから pkg ファイルを解凍し、インストーラに追加する前に pkg ファイルに署名します。

手順

適切なソースからクライアントをダウンロードします。

- Cisco Software Center にアクセスして Mac 版 Cisco Jabber および Windows 版 Cisco Jabberクライアントをダウンロードします。
- Cisco Jabber for Android の場合は、Google Play からアプリケーションをダウンロードします。

- Cisco Jabber for iPhone and iPad の場合は、App Store からアプリケーションをダウンロードします。

Cisco Jabber for Windows のインストール

Cisco Jabber for Windows は、次のように使用可能な MSI インストール パッケージを提供します。

インストール オプション	説明
コマンドラインの使用 （122 ページ）	コマンドライン ウィンドウで引数を指定して、インストール プロパティを設定できます。 複数のインスタンスをインストールする場合は、このオプションを選択します。
MSI の手動による実行 （145 ページ）	クライアントの起動時に、MSI をクライアント ワークステーションのファイル システムで手動で実行し、接続プロパティを指定します。 テストまたは評価用に単一インスタンスをインストールする場合は、このオプションを選択します。
カスタム インストーラの作成 （146 ページ）	デフォルトのインストール パッケージを開き、必要なインストール プロパティを指定し、カスタム インストール パッケージを保存します。 同じインストール プロパティを持つインストール パッケージを配布する場合は、このオプションを選択します。
グループ ポリシーを使用した導入 （150 ページ）	同じドメインの複数のコンピュータにクライアントをインストールします。

始める前に

ローカル管理者権限でログインする必要があります。

コマンドラインの使用

コマンドライン ウィンドウにインストール引数を指定します。

手順

ステップ 1 コマンドライン ウィンドウを開きます。

ステップ 2 次のコマンドを入力します。

```
msiexec.exe /i CiscoJabberSetup.msi
```

ステップ 3 パラメータ = 値のペアとしてコマンドライン引数を指定します。

```
msiexec.exe /i CiscoJabberSetup.msi argument=value
```

ステップ 4 Cisco Jabber for Windows をインストールするコマンドを実行します。

インストール コマンドの例

Cisco Jabber for Windows をインストールするためのコマンド例を確認してください。

Cisco Unified Communications Manager リリース 9.x

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1
```

ここで、

CLEAR=1：既存のブートストラップ ファイルを削除します。
/quiet：サイレント インストールを指定します。

関連トピック

コマンドライン引数 （123 ページ）
言語の LCID （143 ページ）

コマンドライン引数

Cisco Jabber for Windows をインストールする際に指定可能なコマンド ライン引数を確認してください。

関連トピック

インストール コマンドの例 （123 ページ）
言語の LCID （143 ページ）

オーバーライドの引数

次の表では、過去のインストールで得た既存のブートストラップ ファイルを上書きするため、ユーザが指定する必要があるパラメータについて説明します。

引数	値	説明
CLEAR	1	クライアントが前のインストールから既存のブートストラップ ファイルを上書きするかどうかを指定します。 クライアントは、インストール中に設定した引数と値をブートストラップ ファイルに保存します。クライアントは起動時に、ブートストラップ ファイルから設定をローディングします。

CLEAR を指定した場合、インストール中に次が実行されます。

1. クライアントが既存のブートストラップ ファイルを削除する。
2. クライアントが新しいブートストラップ ファイルを作成する。

CLEAR を指定しない場合、クライアントはインストール中に既存のブートストラップ ファイルがあるかどうかをチェックします。

- ブートストラップ ファイルがない場合、インストール時に、クライアントはブートストラップ ファイルを作成します。
- ブートストラップ ファイルが見つかる場合、クライアントは、ブートストラップ ファイルを上書きせず、既存の設定を保存します。

（注） Cisco Jabber for Windows を再インストールする場合は、次の点に留意する必要があります。

- クライアントは、既存のブートストラップ ファイルからの設定を保存しません。CLEAR を指定した場合は、他のすべてのインストール引数も適切に指定する必要があります。
- クライアントは、既存のブートストラップ ファイルにインストール引数を保存しません。インストール引数の値を変更する場合、または追加のインストール引数を指定する場合は、既存の設定を上書きするために CLEAR を指定する必要があります。

既存のブートストラップ ファイルを上書きするには、コマンドラインに CLEAR を次のように指定します。

```
msiexec.exe /i CiscoJabberSetup.msi CLEAR=1
```

モード タイプの引数

次の表は、製品モードを指定するコマンドラインの引数について説明します。

引数	値	説明
PRODUCT_MODE	Phone_Mode	クライアントの製品モードを指定します。次の値を設定できます。 • Phone_Mode：Cisco Unified Communications Manager がオーセンティケータです。 基本機能としてオーディオデバイスを持つユーザをプロビジョニングする場合は、この値を選択します。

製品モードを設定する場合

電話モード展開では、Cisco Unified Communications Manager がオーセンティケータです。クライアントがオーセンティケータを取得すると、製品モードが電話機モードであることが決定されます。ただし、クライアントは最初の起動時にデフォルトの製品モードで常に開始するため、ユーザはログイン後に電話モードにして、クライアントを再起動する必要があります。

（注） Cisco Unified Communications Manager リリース 9.x 以降：インストール中に PRODUCT_MODE を設定しないでください。クライアントはサービスプロファイルからオーセンティケータを取得します。ユーザがログインすると、クライアントは、電話モードにして再起動するよう要請します。

製品モードの変更

製品モードを変更するには、クライアントのオーセンティケータを変更する必要があります。クライアントは、オーセンティケータからの製品モードを決定します。

インストール後の製品モードの変更方法は、展開に応じて異なります。

（注） すべての展開において、ユーザは [詳細設定（Advanced settings）] ウィンドウで手動でオーセンティケータを設定できます。

この場合、ユーザには、[詳細設定（Advanced settings）] ウィンドウでオーセンティケータを変更することによって、製品モードを変更するように指示します。クライアントをアンインストールし、その後に再インストールしても、手動設定を上書きすることはできません。

Cisco Unified Communications Manager バージョン 9.x 以降を使用した製品モードの変更

Cisco Unified Communications Manager バージョン 9.x 以降を使用して製品モードを変更するには、サービス プロファイルのオーセンティケータを変更します。

手順

ステップ 1 適切なユーザのサービス プロファイルでオーセンティケータを変更します。

[デフォルト モード（Default Mode）] > [電話モード（Phone Mode）] を変更します。

IM and Presence を持つユーザのプロビジョニングを行わないでください。

サービス プロファイルに IM and Presence サービスの設定が含まれていない場合は、Cisco Unified Communications Manager がオーセンティケータです。

[電話モード（Phone Mode）] > [デフォルト モード（Default Mode）] を変更します。

IM and Presence を持つユーザのプロビジョニングを行います。

IM and Presence プロファイルの [製品タイプ（Product Type）] フィールドの値を次に対して設定した場合、

- [Unified CM（IM and Presence）]：オーセンティケータは Cisco Unified Communications Manager IM and Presence サービスです。
- Webex**Webex (IM and Presence)** オーセンティケータは、Cisco Webex Messenger サービスです。

ステップ 2 ユーザにログアウトをしてから再度ログインするように指示します。

ユーザがクライアントにログインすると、サービス プロファイルの変更を取得し、オーセンティケータにユーザをログインさせます。クライアントは製品モードを決定すると、クライアントを再起動するようユーザに指示します。

ユーザがクライアントを再起動した後、製品モードの変更が完了します。

認証引数

次の表は、認証ソースの指定をユーザが設定できるコマンドライン引数を説明しています。

引数	値	説明
AUTHENTICATOR	CUP CUCM	クライアントに認証ソースを指定します。この値は、サービスディスカバリに失敗した場合に使用されます。値として次のいずれかを設定します。 • CUP：Cisco Unified Communications Manager IM and Presence サービス。デフォルトの製品モードでのオンプレミスの展開。デフォルト製品モードはフル UC または IM のみのいずれかです。 • CUCM：Cisco Unified Communications Manager。電話モードでのオンプレミスの展開。 Cisco Unified Communications Manager バージョン 9.x 以降を使用したオンプレミス展開では、`_cisco-uds` SRV レコードを展開する必要があります。クライアントは、自動的にオーセンティケータを決定することができます。
CUP_ADDRESS	IP アドレス(IP address) ホストネーム(Hostname) FQDN	Cisco Unified Communications Manager IM and Presence サービスのアドレスを指定します。値として次のいずれかを設定します。 • ホスト名（*hostname*） • IP アドレス（*123.45.254.1*） • FQDN（*hostname.domain.com*）

引数	値	説明
TFTP	IP アドレス(IP address) ホストネーム(Hostname) FQDN	TFTP サーバのアドレスを指定します。値として次のいずれかを設定します。 • ホスト名（*hostname*） • IP アドレス（*123.45.254.1*） • FQDN（*hostname.domain.com*） Cisco Unified Communications Manager がオーセンティケータとして設定されている場合に、この引数を指定する必要があります。 展開する場合： • 電話モード：クライアント コンフィギュレーションをホスティングする TFTP サーバのアドレスを指定する必要があります。 • デフォルト モード：デバイス設定をホストする Cisco Unified Communications Manager TFTPサービスのアドレスを指定できます。
CTI	IP アドレス(IP address) ホストネーム(Hostname) FQDN	CTI サーバのアドレスを設定します。 この引数を指定します。 • Cisco Unified Communications Manager をオーセンティケータとして設定する。 • ユーザは、デスク フォンデバイスを持ち、CTI サーバを必要とします。
CCMCIP	IP アドレス(IP address) ホストネーム(Hostname) FQDN	CCMCIP サーバのアドレスを設定します。 この引数を指定します。 • Cisco Unified Communications Manager をオーセンティケータとして設定する。 • CCMCIP サーバのアドレスが TFTP サーバ アドレスと同じではありません。 クライアントは両方のアドレスが同じであれば、TFTP サーバ アドレスで CCMCIP サーバを検索できます。

引数	値	説明
SERVICES_DOMAIN	Domain	サービス ディスカバリの DNS SRV レコードが存在するドメインの値を設定します。 この情報のインストーラ設定または手動設定をクライアントで使用する場合、この引数はDNS SRV レコードが存在しないドメインに設定します。この引数が指定されない場合、ユーザはサービス ドメイン情報を指示されます。
VOICE_SERVICES_DOMAIN	ドメイン	この設定が指定された場合、クライアントはサービス ディスカバリとエッジ検出の目的で、VOICE_SERVICES_DOMAIN の値を使用して次の DNS レコードを検索します。 • `_cisco-uds` • `_cuplogin` • `_collab-edge` この設定は任意です。指定しない場合、DNS は SERVICES_DOMAIN、ユーザによるメール アドレス入力、またはキャッシュされたユーザ設定から取得したサービス ドメインで照会されます。
EXCLUDED_SERVICES	次のうち1つ以上： • Webex • CUCM	Jabber がサービス ディスカバリから除外するサービスを示します。たとえば、Webexでトライアルを行い、会社のドメインがWebexに登録されているとします。ただし、JabberをWebexではなくCUCMサーバーで認証する必要があります。この場合、次のように設定します。 • EXCLUDED_SERVICES=WEBEX 使用できる値は CUCM です。 Webex すべてのサービスを除外した場合、Jabber クライアントの設定に手動設定またはブートストラップ設定を使用する必要があります。

引数	値	説明
UPN_DISCOVERY_ENABLED	true false	クライアントがサービスを検出したときに Windows セッションのユーザ プリンシパル名（UPN）を使用してユーザのユーザ ID とドメインを取得するかどうかを定義できるようにします。 • true（デフォルト）：UPN を使用して、サービス検出で使用されるユーザのユーザ ID とドメインが検索されます。UPN から検出されたユーザだけが、クライアントにログインできます。 • false：UPN はユーザのユーザ ID とドメインの検索に使用されません。ユーザは、サービス ディスカバリ用のドメインを検索するためのクレデンシャルの入力を要求されます。 インストール コマンドの例：`msiexec.exe /i CiscoJabberSetup.msi /quiet UPN_DISCOVERY_ENABLED=false`

TFTP サーバ アドレス

Cisco Jabber for Windows は、TFTP サーバから 2 つの異なるコンフィギュレーション ファイルを取得します。

- 作成したクライアント設定ファイル。
- デバイスを使用してユーザをプロビジョニングしたときに Cisco Unified Communications Manager TFTP サービスに配置されるデバイス コンフィギュレーション ファイル。

労力を最小限に抑えるには、Cisco Unified Communications Manager TFTP サービス上でクライアント コンフィギュレーション ファイルをホストする必要があります。すべての設定ファイルに対し TFTP サーバ アドレスを 1 つのみ使用します。必要な場合にそのアドレスを指定できます。

ただし、別の TFTP サーバのクライアント設定を、デバイス設定が含まれるサーバでホストできます。この場合、2 つの異なる TFTP サーバ アドレスがあります。1 つはデバイス設定をホストする TFTP サーバのアドレスであり、もう 1 つはクライアント設定ファイルをホストする TFTP サーバのアドレスです。

デフォルトの導入

この項では、プレゼンス サーバがある導入環境において、2 つの異なる TFTP サーバ アドレスを処理する方法について説明します。

以下を実行する必要があります。

1. プレゼンス サーバにあるクライアント設定をホストする TFTP サーバのアドレスを指定します。
2. インストール中に、TFTP 引数を使用して Cisco Unified Communications Manager TFTP サービスのアドレスを指定します。

クライアントは、初回起動時に以下を実行します。

1. ブートストラップ ファイルから Cisco Unified Communications Manager TFTP サービスのアドレスを取得します。
2. Cisco Unified Communications Manager TFTP サービスからデバイス設定を取得します。
3. プレゼンス サーバに接続します。
4. プレゼンス サーバからクライアント設定をホストする TFTP サービスのアドレスを取得します。
5. TFTP サーバからクライアント設定を取得します。

電話モード展開

このセクションでは、電話モード展開で 2 つの異なる TFTP サーバ アドレスを処理する方法について説明します。

以下を実行する必要があります。

1. インストール時に、TFTP 引数を使用して、クライアント設定をホストする TFTP サーバのアドレスを指定します。
2. クライアント コンフィギュレーション ファイルで TftpServer1 パラメータを使用して、デバイス設定をホストする TFTP サーバのアドレスを指定します。
3. TFTP サーバにあるクライアント設定ファイルをホストします。

クライアントが初めて起動するときには、次の処理が実行されます。

1. ブートストラップ ファイルから TFTP サーバのアドレスを取得します。
2. TFTP サーバからクライアント設定を取得します。
3. クライアント設定から Cisco Unified Communications Manager TFTP サービスのアドレスを取得します。
4. Cisco Unified Communications Manager TFTP サービスからデバイス設定を取得します。

共通のインストール引数

次の表では、共通のコマンド ライン引数を説明します。

引数	値	説明
AUTOMATIC_SIGN_IN	true false	ユーザがクライアントをインストールしたときに [Cisco Jabber の起動時にサインイン（Sign me in when Cisco Jabber starts）] チェックボックスがオンになるかどうかを指定します。 • true：ユーザがクライアントをインストールしたときに [Cisco Jabber の起動時にサインイン（Sign me in when Cisco Jabber starts）] チェックボックスがオンになります。 • false（デフォルト）：ユーザがクライアントをインストールしたときに [Cisco Jabber の起動時にサインイン（Sign me in when Cisco Jabber starts）] チェックボックスがオフになります。
CC_MODE	true false	Jabber がコモン クライテリア モードで実行されているかどうかを指定します。 デフォルト値は false です。

引数	値	説明
CLICK2X	DISABLE Click2Call	Cisco Jabber で click-to-x 機能を無効にします。 この引数をインストール中に指定すると、クライアントは click-to-x 機能のハンドラとして、オペレーティングシステムで登録しません。この引数により、クライアントはインストール中の Microsoft Windows レジストリへの書き込みができなくなります。 クライアントを再インストールし、インストール後にクライアントで click-to-x 機能を有効にするには、この引数を省略します。 （注） Windows API を使用して、jabber for Windows および Skype for Business を競合させることができます。この問題を潜在的に緩和するために、`CLICK2X = DISABLE` で Jabber をインストールすることができます。 **ブラウザの Click2Call 機能**: 新しく追加された Click2Call パラメータを使用して、Click2X パラメータを設定できるようになりました。これにより、ブラウザの Click to Call 機能だけが有効になり、Click2X 機能は無効になります。
DIAGNOSTICSTOOLENABLED	true false	Cisco Jabber for Windows ユーザに対して Cisco Jabber 診断ツールが利用可能かどうかを指定します。 • true（デフォルト）：ユーザは、Ctrl キーと Shift キーを押した状態で D キーを入力して、Cisco Jabber 診断ツールを表示できます。 • false：ユーザは Cisco Jabber 診断ツールを利用できません。

引数	値	説明
ENABLE_DPI_AWARE	true false	DPI 対応を有効にします。DPI 対応により、さまざまな画面サイズに合わせて Cisco Jabber がテキストとイメージの表示を自動的に調整することができます。 • true（デフォルト）： • Windows 8.1 および Windows 10 では、Cisco Jabber は各モニタのさまざまな DPI 設定に合わせて調整します。 • Windows 7 および Windows 8 では、Cisco Jabber はシステムの DPI 設定に応じて表示します。 • false：DPI 対応は有効になりません。 DPI 対応はデフォルトで有効になっています。DPI 対応を無効にするには、`msiexec.exe /i CiscoJabberSetup.msi CLEAR=1 ENABLE_DPI_AWARE=false` コマンドを使用します。 （注） コマンド ラインで Cisco Jabber をインストールする場合は、必ず CLEAR=1 の引数を記述します。コマンド ラインから Cisco Jabber をインストールしない場合は、jabber-bootstrap.properties ファイルを手動で削除する必要があります。

引数	値	説明
ENABLE_PRT	true false	• true（デフォルト）：クライアントの [**ヘルプ（Help）**] メニューで [**問題の報告（Report a problem**）] メニュー項目が有効になります。 • false：クライアントの [**ヘルプ（Help**）] メニューから、Jabber メニュー項目の [**問題の報告（Report a problem**）] オプションが削除されます。 このパラメータを false に設定しても、ユーザは **[スタート メニュー（Start Menu]** > **[Cisco Jabber]** ディレクトリ、または Program Files ディレクトリを使用して、問題レポート ツールを手動で起動できます。ユーザが手動で PRT を作成し、このパラメータ値が false に設定されている場合、PRT から作成された zip ファイルにはコンテンツがありません。
ENABLE_PRT_ENCRYPTION	true false	問題レポートの暗号化を有効にします。この引数は PRT_CERTIFICATE_NAME 引数と共に設定する必要があります。 • true：Jabber クライアントから送信された PRT ファイルが暗号化されます。 • false（デフォルト）：Jabber クライアントから送信された PRT ファイルは暗号化されません。 PRT の暗号化には、Cisco Jabber 問題レポートの暗号化と復号化のための公開/秘密キー ペアが必要です。

引数	値	説明
FIPS_MODE	true false	Cisco Jabber が FIPS モードであるかどうかを指定します。 Cisco Jabber は、FIPS 対応ではないオペレーティング システムでも FIPS モードにすることができます。Windows API 以外による接続のみ FIPS モードになります。 この設定を含めない場合、Cisco Jabber ではオペレーティング システムから FIPS モードが判定されます。
FORGOT_PASSWORD_URL	URL	ユーザがパスワードをなくしたり忘れたりした場合にパスワードをリセットできる URL を指定します。 この引数は任意ですが推奨されています。
FORWARD_VOICEMAIL	true false	[ボイス メッセージ（Voice Messages）] タブでボイスメールの転送を有効にします。 • true（デフォルト）：ユーザはボイスメールを連絡先へ転送できます。 • false：ボイスメールの転送は有効になりません。
INVALID_CERTIFICATE_BEHAVIOR	RejectAndNotify PromptPerSession	無効な証明書に対するクライアントの動作を指定します。 • RejectAndNotify：警告ダイアログが表示され、クライアントはロードされません。 • PromptPerSession：警告ダイアログが表示され、ユーザは無効な証明書を受け入れるか、または拒否できます。 FIPS モードの無効な証明書の場合、この引数は無視され、クライアントは警告メッセージを表示し、ロードされません。

引数	値	説明
IP_Mode	IPv4 のみ IPv6 のみ 2 つのスタック	Jabber クライアントのネットワーク IP プロトコルを指定します。 • IPV4 のみ：Jabber は IPv4 接続のみ試行します。 • IPV6 のみ：Jabber は IPv6 接続のみ試行します。 • 2 つのスタック（デフォルト）：Jabber は IPv4 または IPv6 のいずれかと接続できます。 （注） IPv6 のみのサポートは、デスクトップ デバイスのオンプレミス展開でのみ使用できます。Jabber モバイルデバイスは、すべて 2 つのスタックとして構成しなければなりません。 IPv6 の展開の詳細については、『IPv6 Deployment Guide for Cisco Collaboration Systems Release』 を参照してください。 Jabber で使用するネットワーク IP プロトコルの決定には、いくつかの要因があります。詳細については、『*Planning Guide*』の「IPv6 Requirements」の項を参照してください。

引数	値	説明
LANGUAGE	10 進数の LCID	Cisco Jabber for Windows で使用される言語のロケール ID（LCID）を 10 進数で定義します。値は、サポートされる言語に対応する、10 進数の LCID でなくてはなりません。 たとえば、次のいずれかを指定できます。 • 1033 は英語です。 • 1036 はフランス語です。 指定可能な言語の完全なリストについては、「言語の *LCID*」トピックを参照してください。 この引数は省略可能です。 値を指定しないと、Cisco Jabber for Windows が UseSystemLanguage パラメータの値をチェックします。UseSystemLanguage パラメータが true に設定されている場合は、オペレーティングシステムと同じ言語が使用されます。UseSystemLanguage パラメータが false または not defined に設定されている場合、クライアントは現在のユーザの地域言語をデフォルトとして使用します。 地域言語は、**[コントロール パネル（Control Panel）] > [地域および言語（Region and Language）] > [日付、時刻、または数字形式の変更（Change the date, time, or number format）] > [形式（Formats）] タブ > [形式（Format）]** ドロップダウンで設定します。

引数	値	説明
LOCATION_MODE	ENABLED DISABLED ENABLEDNOPROMPT	ロケーション機能を有効にするかどうか、および新しいロケーションの検出時にユーザに通知するかどうかを指定します。 • ENABLED（デフォルト）：ロケーション機能がオンになります。新しいロケーションの検出時にユーザに通知されます。 • DISABLED：ロケーション機能がオフになります。新しいロケーションの検出時にユーザに通知されません。 • ENABLEDNOPROMPT：ロケーション機能がオンになります。新しいロケーションの検出時にユーザに通知されません。
LOG_DIRECTORY	ローカル システムの絶対パス	クライアントがログファイルを書き込むディレクトリを定義します。 次の例のように、引用符記号を使用して、パスのスペース文字をエスケープします。 "C:*my_directory*\Log Directory" 指定するパスに、Windows で無効な文字を含めることはできません。 デフォルト値：%USER_PROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\Logs

引数	値	説明
LOGIN_RESOURCE	WBX MUT	複数のクライアント インスタンスへのユーザ サインインを制御します。 デフォルトで、ユーザは同時に Cisco Jabber の複数インスタンスにサインインできます。デフォルトの動作を変更するには、次のいずれかの値を設定します。 • WBX：ユーザは、一度に Cisco Jabber for Windows の 1 つのインスタンスにしかサインインできません。 Cisco Jabber for Windows は、ユーザの JID に `wbxconnect` サフィックスを付加します。ユーザは、`wbxconnect` サフィックスを使用する他の Cisco Jabber クライアントにサインインできません。 • MUT：ユーザは、一度に Cisco Jabber for Windows の 1 つのインスタンスにしかサインインできませんが、同時に他の Cisco Jabber クライアントにサインインできます。 Cisco Jabber for Windows の各インスタンスがユーザの JID に一意のサフィックスを付加します。
PRT_CERTIFICATE_NAME	証明書の名前	[エンタープライズ信頼または信頼できるルート認証局の証明書ストア（Enterprise Trust or Trusted Root Certificate Authorities certificate store）] に公開キーと共に証明書の名前を指定します。証明書の公開キーは、Jabber 問題レポートの暗号化に使用されます。この引数は ENABLE_PRT_ENCRYPTION 引数と共に設定する必要があります。

引数	値	説明
RESET_JABBER	1	ユーザのローカル プロファイル データとローミング プロファイル データをリセットします。 これらのフォルダーは削除されます。 • `%appdata%\Cisco\Unified Communications\Jabber` • `%localappdata%\Cisco\Unified Communications\Jabber`
SSO_EMAIL_PROMPT	オン オフ	ユーザのホーム クラスタを決定するために、ユーザに対して電子メール プロンプトを表示するかどうかを指定します。 電子メール プロンプトが ServicesDomainSsoEmailPrompt によって定義されている動作をするためのインストーラ要件は、次のとおりです。 • SSO_EMAIL_PROMPT=ON • UPN_DISCOVERY_ENABLED=False • VOICE_SERVICES_DOMAIN=<domain_name> • SERVICES_DOMAIN=<domain_name> 例：msiexec.exe /i CiscoJabberSetup.msi SSO_EMAIL_PROMPT=ON UPN_DISCOVERY_ENABLED=False VOICE_SERVICES_DOMAIN=example.cisco.com SERVICES_DOMAIN=example.cisco.com CLEAR=1

引数	値	説明
Telemetry_Enabled	true false	分析データを収集するかどうかを指定します。デフォルト値は true です。 ユーザエクスペリエンスと製品パフォーマンスを向上させるために、Cisco Jabber は、個人識別が不可能な利用状況とパフォーマンスに関するデータを収集してシスコに送信する場合があります。収集されたデータは、シスコによって、Jabber クライアントがどのように使用され、どのように役立っているかに関する傾向を把握するために使用されます。 Cisco Jabber が収集する分析データと、収集しない分析データの詳細については、https://www.cisco.com/web/siteassets/legal/privacy_02Jun10.html の「Cisco Jabber Supplement to Cisco's On-Line Privacy Policy」で確認できます。
TFTP_FILE_NAME	ファイル名	グループ設定ファイルの一意の名前を指定します。 値として、未修飾か完全修飾のファイル名を指定できます。この引数の値として指定するファイル名は、TFTP サーバの他の設定ファイルよりも優先されます。 この引数は省略可能です。 メモ Cisco Unified Communications Manager の CSF デバイス設定の [シスコサポートフィールド（Cisco Support Field）] で、グループ コンフィギュレーション ファイルを指定できます。

引数	値	説明
UXModel	modern classic	デスクトップクライアント版 Cisco Jabber に適用 Jabber デフォルトでは、すべての導入で最新の設計になっています。ただし、オンプレミスの展開でも古典的な設計がサポートされています。Jabberチームのメッセージングモードでは、最新の設計のみがサポートされています。 オンプレミスの展開で古典的な設計を開始する場合は、uxmodelパラメータを使用します。使用できる値は次のとおりです。 • modern (デフォルト): Jabber は最新のデザインで開始されます。 • classic: Jabber は古典的な設計で開始されます。 各ユーザは Jabber で個人設定をすることができ、これはこのパラメータよりも優先されます。

言語の LCID

次の表に、Cisco Jabber クライアントがサポートするロケール ID（LCID）または言語 ID（LangID）を示します。

サポートされる言語	Cisco Jabber for Windows	Cisco Jabber for Mac	Cisco Jabber for Android、Cisco Jabber for iPhone and iPad	LCID/LangID
アラビア語（サウジアラビア）	X		X	1025
ブルガリア語（ブルガリア）	X	X		1026
カタロニア語（スペイン）	X	X		1027
簡体字中国語（中国）	X	X	X	2052

サポートされる言語	Cisco Jabber for Windows	Cisco Jabber for Mac	Cisco Jabber for Android、Cisco Jabber for iPhone and iPad	LCID/LangID
繁体字中国語（台湾）	X	X	X	1028
クロアチア語（クロアチア）	X	X	X	1050
チェコ語（チェコ共和国）	X	X		1029
デンマーク語（デンマーク）	X	X	X	1030
オランダ語（オランダ）	X	X	X	1043
英語（米国）	X	X	X	1033
フィンランド語（フィンランド）	X	X		1035
フランス語（フランス）	X	X	X	1036
ドイツ語（ドイツ）	X	X	X	1031
ギリシャ語（ギリシャ）	X	X		1032
ヘブライ語（イスラエル）	X			1037
ハンガリー語（ハンガリー）	X	X	X	1038
イタリア語（イタリア）	X	X	X	1040
日本語（日本）	X	X	X	1041
韓国語（韓国）	X	X	X	1042
ノルウェー語（ノルウェー）	X	X		2068

サポートされる言語	Cisco Jabber for Windows	Cisco Jabber for Mac	Cisco Jabber for Android、Cisco Jabber for iPhone and iPad	LCID/LangID
ポーランド語（ポーランド）	X	X		1045
ポルトガル語（ブラジル）	X	X	X	1046
ポルトガル語（ポルトガル）	X	X		2070
ルーマニア語（ルーマニア）	X	X	X	1048
ロシア語（ロシア）	X	X	X	1049
セルビア語	X	X		1050
スロバキア語（スロバキア）	X	X	X	1051
スロベニア語（スロベニア）	X	X		1060
スペイン語（スペイン（インターナショナル ソート））	X	X	X	3082
スウェーデン語（スウェーデン）	X	X	X	5149
タイ語（タイ）	X	X		1054
Turkish	X	X	X	1055

関連トピック

インストール コマンドの例 （123 ページ）
コマンドライン引数 （123 ページ）

MSI の手動による実行

インストール プログラムを手動で実行すれば、クライアントの単一のインスタンスをインストールして、[詳細設定（Advanced settings）] ウィンドウで接続設定を指定できます。

手順

ステップ 1 CiscoJabberSetup.msi を起動します。

インストール プログラムにより、インストール プロセスのウィンドウが開きます。

ステップ 2 手順に従ってインストール プロセスを完了します。

ステップ 3 Cisco Jabber for Windows を起動します。

ステップ 4 [手動設定およびログイン（Manual setup and sign in）] を選択します。

[詳細設定（Advanced settings）] ウィンドウが開きます。

ステップ 5 接続設定プロパティの値を指定します。

ステップ 6 [保存（Save）] を選択します。

カスタム インストーラの作成

カスタム インストーラを作成するデフォルトのインストール パッケージを変換できます。

（注） カスタム インストーラは Microsoft Orca を使用して作成します。Microsoft Orca は Microsoft Windows SDK for Windows 7 と .NET Framework 4 の一部として入手できます。

Microsoft の Web サイトから、Microsoft Windows SDK for Windows 7 と .NET Framework 4 をダウンロードしてインストールします。

手順

	コマンドまたはアクション	目的
ステップ 1	デフォルト トランスフォーム ファイルの取得 （147 ページ）	Microsoft Orca でインストール パッケージを修正するためには、デフォルト トランスフォーム ファイルが必要です。
ステップ 2	カスタム トランスフォーム ファイルの作成 （147 ページ）	トランスフォームファイルは、インストーラに適用するインストール プロパティが含まれます。
ステップ 3	インストーラの変換 （148 ページ）	インストーラをカスタマイズするため、トランスフォーム ファイルを適用します。

デフォルト トランスフォーム ファイルの取得

Microsoft Orca でインストール パッケージを修正するためには、デフォルト トランスフォーム ファイルが必要です。

手順

ステップ 1 ソフトウェア ダウンロード ページから Cisco Jabber 管理パッケージをダウンロードします。

ステップ 2 Cisco Jabber 管理パッケージからファイル システムに `CiscoJabberProperties.msi` をコピーします。

次のタスク

カスタム トランスフォーム ファイルの作成 （147 ページ）

カスタム トランスフォーム ファイルの作成

カスタムインストーラを作成するには、変換ファイルを使用します。トランスフォームファイルは、インストーラに適用するインストール プロパティが含まれます。

デフォルト トランスフォーム ファイルは、インストーラを変換するとプロパティの値を指定することができます。1つのカスタムインストーラを作成する場合、デフォルト トランスフォーム ファイルを使用する必要があります。

任意でカスタム トランスフォーム ファイルを作成できます。カスタム トランスフォーム ファイルでプロパティの値を指定し、インストーラに適用します。

異なるプロパティの値を持つ複数のカスタム インストーラを必要とする場合、カスタム トランスフォーム ファイルを作成します。たとえば、デフォルト言語をフランス語に設定するトランスフォーム ファイルと、デフォルト言語をスペイン語に設定するもう1つのトランスフォーム ファイルを作成できます。インストール パッケージに各トランスフォーム ファイルを個別に適用できます。2 つのインストーラを作成したことで、各言語に 1 つのインストーラが作成されます。

始める前に

デフォルト トランスフォーム ファイルの取得 （147 ページ）

手順

ステップ 1 Microsoft Orca を起動します。

ステップ 2 `CiscoJabberSetup.msi` を開いてから、`CiscoJabberProperties.msi` を適用します。

ステップ 3 該当するインストーラ プロパティに値を指定します。

ステップ 4 トランスフォーム ファイルを生成して保存します。

a) **[トランスフォーム（Transform）] > [トランスフォームの生成（Generate Transform）]** を選択します。
b) トランスフォーム ファイルを保存するファイル システムの場所を選択します。
c) トランスフォーム ファイルの名前を指定して [保存（Save）] を選択します。

作成したトランスフォーム ファイルは、*file_name*.mst として保存されます。このトランスフォーム ファイルを適用して、CiscoJabberSetup.msi のプロパティを変更できます。

次のタスク

インストーラの変換 （148 ページ）

インストーラの変換

インストーラをカスタマイズするため、トランスフォーム ファイルを適用します。

（注） トランスフォーム ファイルを適用すると、CiscoJabberSetup.msi のデジタル署名が変更されます。CiscoJabberSetup.msi を修正したり、名前を変更しようとすると、署名が完全に削除されます。

始める前に

カスタム トランスフォーム ファイルの作成 （147 ページ）

手順

ステップ 1 Microsoft Orca を起動します。

ステップ 2 Microsoft Orca で CiscoJabberSetup.msi を開きます。

a) **[ファイル（File）] > [開く（Open）]** を選択します。
b) ファイル システム上の CiscoJabberSetup.msi の場所を参照します。
c) CiscoJabberSetup.msi を選択してから、[開く（Open）] を選択します。

Microsoft Orca でインストール パッケージが開きます。インストーラのテーブルのリストが [テーブル（Tables）] ペインに表示されます。

ステップ 3 必須: 1033（英語）以外のすべての言語コードを削除します。

制約事項 カスタム インストーラから 1033（英語）以外のすべての言語コード削除する必要があります。

Microsoft Orcaでは、デフォルト（1033）以外のいずれの言語ファイルもカスタム インストーラで保持されません。カスタムインストーラからすべての言語コードを削除しない場合、言語が英語以外のオペレーティング システムでインストーラを実行できません。

a) **[表示（View）] > [要約情報（Summary Information）]** を選択します。

[要約情報の編集（Edit Summary Information）] ウィンドウが表示されます。

b) [言語（Language）] フィールドを見つけます。
c) 1033 以外のすべての言語コードを削除します。
d) [OK] を選択します。

英語がカスタム インストーラの言語として設定されます。

ステップ 4 トランスフォーム ファイルを適用します。

a) **[トランスフォーム（Transform）] > [トランスフォームの適用（Apply Transform）]** を選択します。
b) ファイル システムのトランスフォーム ファイルの場所を参照します。
c) トランスフォーム ファイルを選択し、[開く（Open）] を選択します。

ステップ 5 [テーブル（Tables）]ペインのテーブルのリストから[プロパティ（Property）]を選択します。

`CiscoJabberSetup.msi` のプロパティのリストがアプリケーション ウィンドウの右パネルに表示されます。

ステップ 6 必要とするプロパティの値を指定します。

ヒント 値は大文字と小文字を区別します。このマニュアルの値と一致する値であることを確認します。

ヒント CLEAR の値を 1 に設定し、以前のインストールからの既存のブートストラップ ファイルを上書きします。既存のブートストラップ ファイルを上書きしない場合、カスタム インストーラで設定する値は有効ではありません。

ステップ 7 必要のないプロパティを削除します。

設定されていないプロパティを削除するのは重要です。削除しないと、設定されたプロパティが有効になりません。必要ない各プロパティを 1 つずつ削除します。

a) 削除するプロパティを右クリックします。
b) [行を削除（Drop Row）] を選択します。
c) Microsoft Orca から続行を要求されたら、[OK] を選択します。

ステップ 8 必須: カスタム インストーラで埋め込みストリームを保存できるようにします。

a) [ツール（Tools）] > [オプション（Options）] を選択します。
b) [データベース（Database）] タブを選択します。
c) [名前を付けて保存（Save As）]の選択時に埋め込みストリームをコピーする（Copy embedded streams during 'Save As'）] を選択します。
d) [適用（Apply）] を選択し、[OK] を選択します。

ステップ 9 カスタム インストーラを保存します。

a) **[ファイル（File）] > [名前を付けて変換を保存（Save Transformed As）]** を選択します。
b) ファイル システム上の場所を選択してインストーラを保存します。

c) インストーラの名前を指定してから、[保存（Save）] を選択します。

インストーラのプロパティ

次は、カスタム インストーラで変更可能なプロパティです。

- CLEAR
- PRODUCT_MODE
- AUTHENTICATOR
- CUP_ADDRESS
- TFTP
- CTI
- CCMCIP
- LANGUAGE
- TFTP_FILE_NAME
- FORGOT_PASSWORD_URL
- SSO_ORG_DOMAIN
- LOGIN_RESOURCE
- LOG_DIRECTORY
- CLICK2X
- SERVICES_DOMAIN

これらのプロパティは、インストールの引数に対応し、同じ値が設定されています。

グループ ポリシーを使用した導入

Microsoft Windows Server の Microsoft グループ ポリシー管理コンソール（GPMC）を使用して、グループ ポリシーと一緒に Cisco Jabber for Windows をインストールします。

（注） グループ ポリシーと一緒に Cisco Jabber for Windows をインストールするには、Cisco Jabber for Window の展開先となるすべてのコンピュータまたはユーザが同じドメイン内に存在している必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	言語コードの設定 （151 ページ）	MSI が何らかの形で Orca により変更されている場合のみ、この手順を使用して [言語（Language）] フィールドを 1033 に設定します。
ステップ 2	グループ ポリシーによるクライアントの展開 （152 ページ）	Cisco Jabber for Windows with Group Policy を導入します。

言語コードの設定

インストール言語の変更は、シスコが提供する MSI ファイルを使用するグループ ポリシーの配置シナリオでは必要ではありません。このような状況において、インストール言語はWindows ユーザ ロケール（形式）から決定されます。MSI が何らかの形で Orca により変更されている場合のみ、この手順を使用して [言語（Language）] フィールドを 1033 に設定します。

Jabber クライアントがサポートする言語の Locale Identifier (LCID) または Language Identifier (LangID) のリストについては、言語の LCID （143 ページ） を参照してください。

手順

ステップ 1 Microsoft Orca を起動します。

Microsoft Orca は、Microsoft の Web サイトからダウンロード可能な Microsoft Windows SDK for Windows 7 と .NET Framework 4 の一部として入手できます。

ステップ 2 `CiscoJabberSetup.msi` を開きます。

a) **[ファイル（File）] > [開く（Open）]** を選択します。
b) ファイル システム上の `CiscoJabberSetup.msi` の場所を参照します。
c) `CiscoJabberSetup.msi` を選択してから、[開く（Open）] を選択します。

ステップ 3 **[表示（View）] > [要約情報（Summary Information）]** を選択します。

ステップ 4 [言語（Language）] フィールドを見つけます。

ステップ 5 [言語（Languages）] フィールドを 1033 に設定します。

ステップ 6 [OK] を選択します。

ステップ 7 必須: カスタム インストーラで埋め込みストリームを保存できるようにします。

a) [ツール（Tools）] > [オプション（Options）] を選択します。
b) [データベース（Database）] タブを選択します。
c) [名前を付けて保存（Save As）]の選択時に埋め込みストリームをコピーする（Copy embedded streams during 'Save As'）] を選択します。
d) [適用（Apply）] を選択し、[OK] を選択します。

ステップ 8 カスタム インストーラを保存します。

a) **[ファイル（File）] > [名前を付けて変換を保存（Save Transformed As）]** を選択します。
b) ファイル システム上の場所を選択してインストーラを保存します。
c) インストーラの名前を指定してから、[保存（Save）] を選択します。

次のタスク

グループ ポリシーによるクライアントの展開 （152 ページ）

グループ ポリシーによるクライアントの展開

グループ ポリシーと Cisco Jabber for Windows を展開するには、このタスクの手順を実行します。

始める前に

言語コードの設定 （151 ページ）

手順

ステップ 1 導入のためのソフトウェア配布ポイントにインストール パッケージをコピーします。

Cisco Jabber for Windows を展開する予定のすべてのコンピュータまたはユーザは、配布ポイント上のインストール パッケージにアクセスできる必要があります。

ステップ 2 **[スタート（Start）] > [ファイル名を指定して実行（Run）]** を選択し、次のコマンドを入力します。

```
GPMC.msc
```

[グループ ポリシー管理（Group Policy Management）] コンソールが開きます。

ステップ 3 新しいグループ ポリシー オブジェクトを作成します。

a) 左側のペインの適切なドメインを右クリックします。
b) [このドメインに GPO を作成してここにリンクする（Create a GPO in this Domain, and Link it here）] を選択します。

[新しい GPO（New GPO）] ウィンドウが開きます。

c) [名前（Name）] フィールドにグループ ポリシー オブジェクトの名前を入力します。
d) デフォルト値をそのままにするか、[発信元の開始 GPO（Source Starter GPO）] ドロップダウン リストから適切なオプションを選択し、次に [OK] を選択します。

新しいグループ ポリシーが、ドメインのグループ ポリシーのリストに表示されます。

ステップ 4 導入の範囲を設定します。

a) 左側のペインのドメインの下からグループ ポリシー オブジェクトを選択します。

グループ ポリシー オブジェクトが右側のペインに表示されます。

b) [スコープ（Scope）] タブの [セキュリティ フィルタリング（Security Filtering）] セクションで、[追加（Add）] を選択します。

[ユーザ、コンピュータ、またはグループの選択（Select User, Computer, or Group）] ウィンドウが開きます。

c) Cisco Jabber for Windows を導入するコンピュータとユーザを指定します。

ステップ 5 インストール パッケージを指定します。

a) 左側のペインのグループ ポリシー オブジェクトを右クリックして、[編集（Edit）] を選択します。

[グループ ポリシー管理エディタ（Group Policy Management Editor）] が開きます。

b) [コンピュータの設定（Computer Configuration）] を選択して、**[ポリシー（Policies）]** > **[ソフトウェアの設定（Software Settings）]** を選択します。

c) [ソフトウェアのインストール（Software Installation）] を右クリックして、**[新規（New）]** > **[パッケージ（Package）]** を選択します。

d) [ファイル名（File Name）] の横にインストール パッケージの場所を入力します（例：`\\server\software_distribution`）。

重要 インストール パッケージの場所として Uniform Naming Convention（UNC）パスを入力する必要があります。UNC パスを入力しなかった場合は、グループ ポリシーで Cisco Jabber for Windows を展開できません。

e) インストール パッケージを選択して、[開く（Open）] を選択します。

f) [ソフトウェアの導入（Deploy Software）] ダイアログボックスで、[割り当て済み（Assigned）] を選択し、[OK] を選択します。

グループ ポリシーによって、次回のコンピュータの起動時にコンピュータごとに Cisco Jabber for Windows がインストールされます。

Windows の自動更新の設定

自動更新を有効にするには、HTTP サーバ上のインストール パッケージの URL などの最新バージョンに関する情報を含む XML ファイルを作成します。ユーザがサインインしたとき、コンピュータをスリープ モードから再開したとき、または **[ヘルプ（Help）]** メニューから手動更新要求を実行したとき、クライアントは XML ファイルを取得します。

XML ファイルの構造

自動更新用の XML ファイルは次のような構造となっています。

```
<JabberUpdate>
          <App name=”JabberWin”>
               <LatestBuildNum>12345</LatestBuildNum>
               <LatestVersion>11.8.x</LatestVersion>
               <Mandatory>true</Mandatory>
               <Message>
                  <![CDATA[<b>This new version of Cisco Jabber lets you do the
```

```
                    following:</b><ul><li>Feature 1</li><li>Feature 2</li></ul>For
                    more information click <a target="_blank"
href="http://cisco.com/go/jabber">here</a>.]]>
                </Message>
              <DownloadURL>http://http_server_name/CiscoJabberSetup.msi</DownloadURL>

          </App>
        </JabberUpdate>
```

始める前に

- XML ファイルとインストール パッケージをホストするために、HTTP サーバをインストールして設定します。
- ワークステーションにソフトウェア アップデートをインストールできる権限がユーザにあることを確認します。

  ユーザがワークステーションに対する管理権限を持っていない場合は、Microsoft Windows が更新インストールを停止します。インストールを完了するには、管理者権限でログインする必要があります。

手順

ステップ 1 ご使用の HTTP サーバで更新インストール プログラムをホストします。

ステップ 2 任意のテキスト エディタを使用して更新の XML ファイルを作成します。

ステップ 3 XML で次のように値を指定します。

- `name`：`App` 要素の `name` 属性の値として次の ID を指定します。
  - JabberWin：更新は Cisco Jabber for Windows に適用されます。
- `LatestBuildNum`：更新のビルド番号。
- `LatestVersion`：更新のバージョン番号。
- `Mandatory`：（Windows クライアントのみ）True または False。画面の指示に従って、ユーザがクライアント バージョンをアップグレードする必要があるかどうかを決定します。
- `Message`：次の形式の HTML。

  ```
  <![CDATA[your_html]]>
  ```

- `DownloadURL`：HTTP サーバ上のインストール パッケージの URL。
- `AllowUpdatesViaExpressway` — Windows クライアントのみ）。False（デフォルト）または True。Expressway for Mobile and Remote Access 上で社内ネットワークに接続しているとき、Jabber が自動更新を行うか指定します。

  更新 XML ファイルがパブリック Web サーバにホストされている場合、このパラメータを false に設定します。そうしないと、Jabber には、更新ファイルが内部サーバにホストされ

ており、Expressway for Mobile and Remote Access を介してアクセスする必要があると通知されます。

ステップ 4 更新の XML ファイルを保存して閉じます。

ステップ 5 HTTP サーバ上で更新 XML ファイルをホストします。

ステップ 6 コンフィギュレーション ファイル内の UpdateUrl パラメータの値として更新 XML ファイルの URL を指定します。

Cisco Jabber for Windows のアンインストール

コマンドラインまたは Microsoft Windows のコントロールパネルを使用して Cisco Jabber for Windows をアンインストールできます。このマニュアルでは、コマンドラインを使用して Cisco Jabber for Windows をアンインストールする方法について説明します。

インストーラの使用

ファイル システムでインストーラが利用可能な場合は、それを使用して Cisco Jabber for Windows を削除します。

手順

ステップ 1 コマンドライン ウィンドウを開きます。

ステップ 2 次のコマンドを入力します。

```
msiexec.exe /x path_to_CiscoJabberSetup.msi
```

次の例を参考にしてください。

```
msiexec.exe /x C:\Windows\Installer\CiscoJabberSetup.msi /quiet
```

ここで、`/quiet` により、サイレント アンインストールが指定されます。

このコマンドは、コンピュータから Cisco Jabber for Windows を削除します。

製品コードの使用

ファイル システムでインストーラが利用できない場合は、製品コードを使用して Cisco Jabber for Windows を削除します。

手順

ステップ 1 製品コードを検索します。

a) Microsoft Windows レジストリ エディタを開きます。

b) レジストリ キー HKEY_CLASSES_ROOT\Installer\Products を見つけます。
c) **[編集（Edit）]** > **[検索（Find）]** を選択します。
d) [検索（Find）] ウィンドウの [検索（Find what）] テキスト ボックスに Cisco Jabber と入力し、[次を検索（Find Next）] を選択します。
e) **ProductIcon** キーの値を検索します。

製品コードは、**ProductIcon** キーの値（たとえば、`C:\Windows\Installer\{product_code}\ARPPRODUCTICON.exe`）です。

（注） 製品コードは Cisco Jabber for Windows のバージョンごとに異なります。

ステップ 2 コマンドライン ウィンドウを開きます。

ステップ 3 次のコマンドを入力します。

```
msiexec.exe /x product_code
```

次の例を参考にしてください。

```
msiexec.exe /x 45992224-D2DE-49BB-B085-6524845321C7 /quiet
```

ここで、`/quiet` により、サイレント アンインストールが指定されます。

このコマンドは、コンピュータから Cisco Jabber for Windows を削除します。

Cisco Jabber for Mac のインストール

Cisco Jabber for Mac のインストーラ

クライアントのインストール

クライアントをインストールするには、次のいずれかの方法を使用します。

- ユーザが手動でアプリケーションをインストールできるよう、インストーラを提供します。クライアントは `Applications` フォルダにインストールされます。クライアントの以前のバージョンを削除する必要があります。
- ユーザに自動アップデートを設定すると、インストーラは告知なしにアプリケーションを更新します。

  自動更新では、クライアントはいつも `Applications` フォルダに追加されます。

  - クライアントが別のフォルダにある場合、または `Applications` フォルダのサブフォルダにある場合は、Applications フォルダにクライアントを実行するためのリンクが作成されます。
  - ユーザが以前クライアントの名前を変更している場合は、インストーラはそれに一致するよう新しいクライアントの名前を変更します。

他の OS X インストーラのインストールと同様に、ユーザはシステムのクレデンシャルを入力するよう求められます。

告知なしのインストール：クライアントを告知なしにインストールするには、端末ツールで次の Mac OS X コマンドを使用します。

```
sudo installer -pkg /path_to/Install_Cisco-Jabber-Mac.pkg -target /
```

インストーラ コマンドの詳細は、Mac のインストーラのマニュアル ページを参照してください。

アクセサリ マネージャ

アクセサリ マネージャは、アクセサリ デバイス ベンダーにユニファイドコミュニケーション制御 API を提供するコンポーネントです。サードパーティ製デバイスは、この API を使い、デバイスで消音、通話の応答、通話の終了などのタスクを実行できます。サード パーティ ベンダーはアプリケーションによってロードされるプラグインを作成します。スピーカー、マイクに対応した標準ヘッドセットを接続できます。

特定のデバイスのみがコール制御のアクセサリ マネージャと対話します。詳細はデバイス ベンダーにお問い合わせください。デスクトップの電話機はサポートされません。

クライアント インストーラにはベンダーが提供するサードパーティのプラグインが含まれます。これらは `/Library/Cisco/Jabber/Accessories/` フォルダにインストールされます。

サポートされるサードパーティ ベンダーは、以下のとおりです。

- Logitech
- Sennheiser
- Jabra
- Plantronics

アクセサリ マネージャの機能はデフォルトで有効になっており、EnableAccessoriesManager パラメータを使用して設定されます。BlockAccessoriesManager パラメータを使用して、サードパーティのベンダーが提供する特定のアクセサリ マネージャ プラグインを無効にできます。

設定（Configuration）

クライアントへサインインするための設定情報を入力します。次のいずれかを実行します。

- オプションのサーバの情報を含む設定用 URL をユーザに提供します。詳細は、『*Cisco Jabber for Mac の URL 設定*』セクションを参照してください。
- 手動で接続するため、サーバの情報をユーザに提供します。詳細は、『手動接続設定』セクションを参照してください。
- サービス検出を使用します。詳細は、サービス検出セクションを参照してください。

インストーラの手動での実行

インストール プログラムを手動で実行すれば、クライアントの単一のインスタンスをインストールして、**[設定（Preferences）]** で接続設定を指定できます。

始める前に

クライアントの古いバージョンをすべて削除します。

手順

ステップ 1 `jabber-mac.pkg` を起動します。
インストーラにより、インストール プロセスのウィンドウが開きます。

ステップ 2 手順に従ってインストール プロセスを完了します。
インストーラはシステム クレデンシャルの入力を要求します。

ステップ 3 設定 URL を使い、またはクライアントを直接実行して、クライアントを起動します。
ユーザ クレデンシャルを入力します。

Cisco Jabber for Mac の URL 設定

ユーザが手動でサービス ディスカバリ情報を入力しなくても Cisco Jabber を起動できるようにするには、構成 URL を作成してユーザに配布します。

電子メールで直接、ユーザにリンクを送信するか、Web サイトにリンクを掲載することで、ユーザに構成 URL リンクを提供できます。

URL には次のパラメータを含めて指定できます。

- ServicesDomain：必須。すべての構成 URL に Cisco Jabber でのサービス ディスカバリに必要な IM and Presence サーバのドメインを含める必要があります。
- ServiceDiscoveryExcludedServices：任意。サービス ディスカバリ プロセスから次のサービスを除外できます。
  - Webexこの値を設定すると、クライアントは次のように動作します。
    - CAS 検索を実行しません。
    - 検索：
      - `_cisco-uds`
      - `_cuplogin`
      - `_collab-edge`
  - CUCM：この値を設定すると、クライアントは次のように動作します。

- _cisco-uds を検索しません。
- 検索：
  - _cuplogin
  - _collab-edge

- CUP：この値を設定すると、クライアントは次のように動作します。
  - _cuplogin を検索しません。
  - 検索：
    - _cisco-uds
    - _collab-edge

カンマで区切った複数の値を指定して、複数のサービスを除外できます。

3 つのサービスをすべて除外した場合、クライアントはサービス ディスカバリを実行せず、手動で接続設定を入力することをユーザに求めます。

- ServicesDomainSsoEmailPrompt：任意。ユーザのホーム クラスタを決定する際に、ユーザに対して電子メール プロンプトを表示するかどうかを指定します。
  - オン
  - オフ
- EnablePRTEncryption：任意。PRT ファイルの暗号化を指定します。Cisco Jabber for Mac で使用します。
  - true
  - false
- PRTCertificateName：任意。証明書の名前を指定します。Cisco Jabber for Mac で使用します。
- InvalidCertificateBehavior：任意。無効な証明書に対するクライアントの動作を指定します。
  - RejectAndNotify：警告ダイアログが表示され、クライアントはロードされません。
  - PromptPerSession：警告ダイアログが表示され、ユーザは無効な証明書を受け入れるか、または拒否できます。
- Telephony_Enabled：ユーザに対して電話機能を有効にするかどうかを指定します。デフォルトは true です。
  - はい
  - いいえ

- DiagnosticsToolEnabled：クライアントで診断ツールを使用できるようにするかどうかを指定します。デフォルトは true です。
  - はい
  - いいえ

構成 URL は次の形式で作成します。

```
ciscojabber://provision?ServicesDomain=<domain_for_service_discover>
&VoiceServicesDomain=<domain_for_voice_services>
&ServiceDiscoveryExcludedServices=<services_to_exclude_from_service_discover>
&ServicesDomainSsoEmailPrompt=<ON/OFF>
```

（注） パラメータには大文字と小文字の区別があります。

例

- `ciscojabber://provision?ServicesDomain=cisco.com`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com`
- `ciscojabber://provision?ServicesDomain=service_domain &VoiceServicesDomain=voiceservice_domain&ServiceDiscoveryExcludedServices=WEBEX`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP &ServicesDomainSsoEmailPrompt=OFF`

Mac の自動更新の設定

自動更新を有効にするには、HTTP サーバ上のインストールパッケージの URL などの最新バージョンに関する情報を含む XML ファイルを作成します。ユーザがサインインしたとき、コンピュータをスリープ モードから再開したとき、または [ヘルプ（Help）] メニューから手動更新要求を実行したとき、クライアントは XML ファイルを取得します。

XML ファイルの構造

以下は自動更新の XML ファイルの例です。

```
<JabberUpdate>
<App name="JabberMac">
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.6.1</LatestVersion>
  <Message><![CDATA[<b>This new version of Cisco Jabber lets you do the
following:</b><ul><li>Feature 1</li><li>Feature 2</li>
  </ul>For more information click <a target="_blank"
href="http://cisco.com/go/jabber">here</a>.]]>
  </Message>

<DownloadURL>http://http_server_name/Install_Cisco-Jabber-Mac-1.1.1-12345-MrbCdd.zip</DownloadURL>
```

```
</App>
</JabberUpdate>
```

XML ファイルの例 2

以下は自動更新の XML ファイルの例です。これは、Cisco Jabber for Windows と Cisco Jabber for Mac の両方に該当します。

```
<JabberUpdate>
 <App name="JabberMac">
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.6.1</LatestVersion>
  <Message><![CDATA[<b>This new version of Cisco Jabber lets you do the
following:</b><ul><li>Feature 1</li><li>Feature 2</li>
  </ul>For more information click <a target="_blank"
href="http://cisco.com/go/jabber">here</a>.]]>
  </Message>

<DownloadURL>http://http_server_name/Install_Cisco-Jabber-Mac-1.1.1-12345-MrbCdd.zip</DownloadURL>

 </App>
 <App name="JabberWin">
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.0</LatestVersion>
  <Message><![CDATA[<b>This new version of Cisco Jabber lets you do the
following:</b><ul><li>Feature 1</li><li>Feature 2
  </li></ul>For more information click <a target="_blank"
href="http://cisco.com/go/jabber">here</a>.]]>
  </Message>
  <DownloadURL>http://http_server_name/CiscoJabberSetup.msi
  </DownloadURL>
</App>
</JabberUpdate>
```

始める前に

XML ファイルとインストール パッケージをホストするために、HTTP サーバをインストールして設定します。

（注） DSA 署名が確実に成功するよう、Web サーバが特殊文字をエスケープする設定をしてください。たとえば、Microsoft IIS でのオプションは [2 重スペースを許可する（Allow double spacing）] です。

手順

ステップ 1 ご使用の HTTP サーバで更新インストール プログラムをホストします。

ステップ 2 任意のテキスト エディタを使用して更新の XML ファイルを作成します。

ステップ 3 XML で次のように値を指定します。

- `name`：`App` 要素の `name` 属性の値として次の ID を指定します。
  - JabberWin：更新は Cisco Jabber for Windows に適用されます。
  - JabberMac：更新は Cisco Jabber for Mac に適用されます。

- `LatestBuildNum`：更新のビルド番号。
- `LatestVersion`：更新のバージョン番号。
- `Mandatory`：TrueまたはFalse。画面の指示に従って、ユーザがクライアントバージョンをアップグレードする必要があるかどうかを決定します。
- `Message`：次の形式の HTML。

  ```
  <![CDATA[your_html]]>
  ```

- `DownloadURL`：HTTP サーバ上のインストール パッケージの URL。

  Cisco Jabber for Mac の場合、URL ファイルは次の形式にする必要があります。

  ```
  Install_Cisco-Jabber-Mac-version-size-dsaSignature.zip
  ```

ステップ 4 更新の XML ファイルを保存して閉じます。

ステップ 5 HTTP サーバ上で更新 XML ファイルをホストします。

ステップ 6 コンフィギュレーション ファイル内の UpdateUrl パラメータの値として更新 XML ファイルの URL を指定します。

Cisco Jabber モバイル クライアントのインストール

手順

ステップ 1 Cisco Jabber for Android をインストールするには、モバイル デバイスで Google Play からアプリケーションをダウンロードします。

ステップ 2 Cisco Jabber for iPhone and iPad をインストールするには、モバイル デバイスで App Store からアプリケーションをダウンロードします。

Cisco Jabber for Android、iPhone、および iPad の URL 設定

ユーザが手動でサービス ディスカバリ情報を入力しなくても Cisco Jabber を起動できるようにするには、構成 URL を作成してユーザに配布します。

電子メールで直接、ユーザにリンクを送信するか、Web サイトにリンクを掲載することで、ユーザに構成 URL リンクを提供できます。

URL には次のパラメータを含めて指定できます。

- ServicesDomain：必須。すべての構成 URL に Cisco Jabber でのサービス ディスカバリに必要な IM and Presence サーバのドメインを含める必要があります。

- ServiceDiscoveryExcludedServices：任意。サービス ディスカバリ プロセスから次のサービスを除外できます。
  - Webexこの値を設定すると、クライアントは次のように動作します。
    - CAS 検索を実行しません。
    - 検索：
      - _cisco-uds
      - _cuplogin
      - _collab-edge
  - CUCM：この値を設定すると、クライアントは次のように動作します。
    - _cisco-uds を検索しません。
    - 検索：
      - _cuplogin
      - _collab-edge
  - CUP：この値を設定すると、クライアントは次のように動作します。
    - _cuplogin を検索しません。
    - 検索：
      - _cisco-uds
      - _collab-edge

  カンマで区切った複数の値を指定して、複数のサービスを除外できます。

  3 つのサービスをすべて除外した場合、クライアントはサービス ディスカバリを実行せず、手動で接続設定を入力することをユーザに求めます。
- ServicesDomainSsoEmailPrompt：任意。ユーザのホーム クラスタを決定する際に、ユーザに対して電子メール プロンプトを表示するかどうかを指定します。
  - オン
  - オフ
- InvalidCertificateBehavior：任意。無効な証明書に対するクライアントの動作を指定します。
  - RejectAndNotify：警告ダイアログが表示され、クライアントはロードされません。
  - PromptPerSession：警告ダイアログが表示され、ユーザは無効な証明書を受け入れるか、または拒否できます。

- PRTCertificateUrl：信頼できるルート認証局の証明書ストアにある公開キーを含む証明書の名前を指定します。モバイル クライアント向け Cisco Jabber に適用されます。
- Telephony_Enabled：ユーザに対して電話機能を有効にするかどうかを指定します。デフォルトは true です。
  - はい
  - いいえ
- ForceLaunchBrowser：ユーザに外部ブラウザの使用を強制する場合に使用します。モバイル クライアント向け Cisco Jabber に適用されます。
  - はい
  - いいえ

（注） ForceLaunchBrowserは、クライアント証明書の展開およびAndroid OS 5.0 よりも前のデバイスに使用されます。

構成 URL は次の形式で作成します。

```
ciscojabber://provision?ServicesDomain=<domain_for_service_discover>
&VoiceServicesDomain=<domain_for_voice_services>
&ServiceDiscoveryExcludedServices=<services_to_exclude_from_service_discover>
&ServicesDomainSsoEmailPrompt=<ON/OFF>
```

（注） パラメータには大文字と小文字の区別があります。

例

- `ciscojabber://provision?ServicesDomain=cisco.com`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com`
- `ciscojabber://provision?ServicesDomain=service_domain &VoiceServicesDomain=voiceservice_domain&ServiceDiscoveryExcludedServices=WEBEX`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP &ServicesDomainSsoEmailPrompt=OFF`

企業モビリティ管理によるモバイルの設定

企業モビリティ管理（EMM）を使用する前に、以下を確認してください。

- EMM ベンダーが Android for Work または Apple Managed App Configuration をサポートしている。
- Android デバイスの OS が 5.0 以降

ユーザが Android 版 Cisco Jabber または iPhone および iPad 版 Cisco Jabber を起動できるように、企業モビリティ管理（EMM）を使用して Cisco Jabber を設定できます。

EMM の設定の詳細については、EMM プロバイダーから提供される管理者用の説明書を参照してください。

Jabber をマネージド デバイスでのみ実行する場合、証明書ベースの認証を展開し、EMM を使用してクライアント証明書を登録できます。

Cisco Jabber for iPhone and iPad は、Microsoft Exchange サーバからインポートされる、ローカルの連絡先のデフォルトのダイアラとして設定することができます。**Exchange ActiveSync** を使用してプロファイルを設定し、MDM 設定ファイルの [**デフォルトの音声通話アプリ**] フィールドに`com.cisco.jabberIM` 値を入力します。

EMM を使用するときは、EMM アプリケーションで AllowUrlProvisioning パラメータを **`False`** に設定し、URL 設定を無効にします。パラメータの設定の詳細は、『*AllowUrlProvisioning Parameter*』を参照してください。

EMM ベンダーは、アプリケーションの設定で様々な型の値を設定できますが、Cisco Jabber は String 型の値しか読み取りできません。EMM で次のパラメータを設定します。

- ServicesDomain
- VoiceServicesDomain
- ServiceDiscoveryExcludedServices
- ServicesDomainSsoEmailPrompt
- EnablePRTEncryption
- PRTCertificateURL
- PRTCertificateName
- InvalidCertificateBehavior
- Telephony_Enabled
- ForceLaunchBrowser
- FIPS_MODE
- CC_MODE
- LastLoadedUserProfile
- AllowUrlProvisioning
- IP_Mode
- AllowTeamsUseEmbeddedSafari: Cisco Jabber for IPhone および iPad のみ

FIPS_MODE パラメータ

EMM を使用して Cisco Jabber モバイル クライアントの FIPS モードを有効または無効にするには、このパラメータを使用します。

- *true*: Cisco Jabber を FIPS モードで実行します。
- *false*: Cisco Jabber を FIPS モードで実行できません。

例:`<FIPS_MODE> false </FIPS_MODE>`

CC_MODE パラメータ

EMM を使用して Cisco Jabber モバイル クライアントの コモン クライテリア モードを有効または無効にするには、このパラメータを使用します。

- *true*: Cisco Jabber を共通基準モードで実行します。
- *false* (デフォルト): Cisco Jabber は共通基準モードで実行されません。

例:`< CC_MODE >true</CC_MODE >`

（注） CC_MODE を有効にするには、RSA キーサイズが少なくとも 2048 ビットである必要があります。共通基準モードで Jabber が実行されるように設定する方法の詳細については、『*Cisco jabber* 12.5 のオンプレミス導入ガイド』に *cisco jabber* アプリケーションを導入する方法を参照してください。

LastLoadedUserProfile

Cisco Jabber for iPhone and iPad および Cisco Jabber for Android に適用されます。

EMM では、ユーザーがモバイル デバイスにログオンするためにパスワードを入力するだけで済むように、デバイスのユーザー名を定義します。

```
<LastLoadedUserProfile>username@example.com<LastLoadedUserProfile>
```

AllowUrlProvisioning パラメータ

URL による設定から EMM に移行する場合、このパラメータを使用します。

このパラメータには次の値が適合します。

- true（デフォルト）：ブートストラップ設定は URL による設定により行われます。
- false：ブートストラップ設定は URL による設定では行われません。

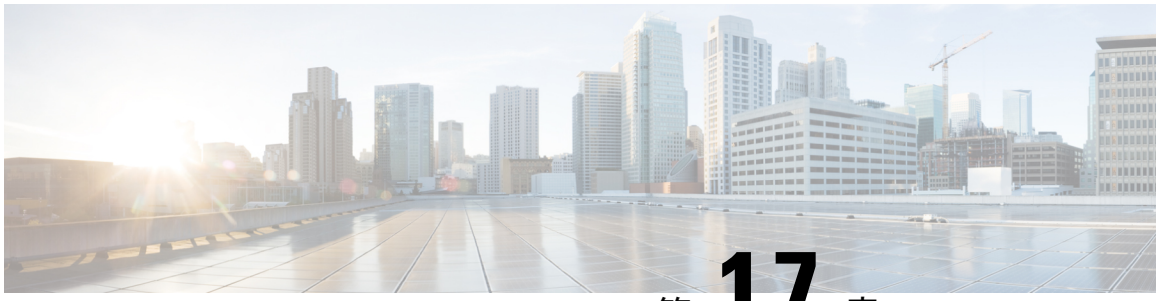
例：`<AllowURLProvisioning>false</AllowURLProvisioning>`

VDI 版 Jabber Softphone のインストール

手順

ステップ 1 Jabber の展開のワークフローを実行します。

ステップ 2 Jabber ソフトフォンの VDI をインストールするには、インストールするクライアント用の Cisco jabber ソフトフォンの展開およびインストールガイドに記載されている手順に従ってください。



第 17 章

リモート アクセス

サービス検出要件のワークフロー

手順

	コマンドまたはアクション	目的
ステップ 1	サービス検出の要件 （169 ページ）	
ステップ 2	DNS の要件 （170 ページ）	
ステップ 3	証明書の要件 （170 ページ）	
ステップ 4	_collab-edge SRV レコードのテスト （170 ページ）	

サービス検出の要件

サービスディスカバリにより、クライアントは自動的に企業のネットワークでサービスを検出することができます。Expressway for Mobile and Remote Access を使用すると、企業のネットワーク上のサービスにアクセスできます。クライアントが Expressway for Mobile and Remote Access 経由で接続し、サービスを検出するには、次の要件が満たされている必要があります。

- DNS の要件
- 証明書の要件
- 外部 SRV `_collab-edge` のテスト

DNS の要件

リモート アクセスによるサービス検出のための DNS 要件は次のとおりです。

- 外部 DNS サーバで _collab-edge DNS SRV レコードを設定します。
- 内部ネーム サーバで _cisco-uds DNS SRV レコードを設定します。
- オプションで、IM and Presenceサーバと音声サーバに異なるドメインを使用するハイブリッド クラウド ベースの展開の場合、_collab-edge レコードで DNS サーバを検索するように音声サービス ドメインを設定します。

（注） Jabber は最大3台の sso 対応サーバに接続しようとし、DNS SRV レコード(_collab-edgeと_cisco-uds) が識別するすべての sso 対応サーバからランダムに選択されます。Jabber が 3 回接続できない場合、エッジの SSO はサポートされていないと見なされます。

証明書の要件

リモート アクセスを設定する前に、Cisco VCS Expressway と Cisco Expressway-E のサーバ証明書をダウンロードします。このサーバ証明書は、HTTP と XMPP の両方に使用されます。

Cisco VCS Expressway 証明書の設定の詳細については、『Configuring Certificates on Cisco VCS Expressway』を参照してください。

_collab-edge SRV レコードのテスト

SRV レコードのテスト

SRV レコードを作成したら、それらがアクセス可能かどうかを確認するためにテストします。

ヒント Web ベースのオプションをご希望の場合は、コラボレーション ソリューション アナライザー サイトの SRV チェック ツールを使用することもできます。

手順

ステップ 1 コマンド プロンプトを開きます。

ステップ 2 **nslookup** と入力します。

デフォルトの DNS サーバおよびアドレスが表示されます。これが想定された DNS サーバであることを確認してください。

ステップ 3 **set type=SRV** と入力します。

ステップ 4 各 SRV レコードの名前を入力します。

例：`_cisco-uds.exampledomain`

- サーバとアドレスが表示される：SRV レコードにアクセスできます。
- 「`_cisco-uds.exampledomain: Non-existent domain`」と表示される：SRV レコードに関する問題が存在します。

Cisco AnyConnect 展開のワークフロー

手順

	コマンドまたはアクション	目的
ステップ 1	アプリケーション プロファイル （171 ページ）	
ステップ 2	VPN 接続の自動化 （173 ページ）	
ステップ 3	AnyConnect の参照ドキュメント （177 ページ）	
ステップ 4	セッション パラメータ （177 ページ）	

Cisco AnyConnect の導入

アプリケーション プロファイル

Cisco AnyConnect セキュア モビリティ クライアントをデバイスにダウンロードした後で、ASA はこのアプリケーションに対してコンフィギュレーション プロファイルをプロビジョニングする必要があります。

Cisco AnyConnect セキュア モビリティ クライアントのコンフィギュレーション プロファイルには、会社の ASA VPN ゲートウェイ、接続プロトコル（IPSec または SSL）、オンデマンド ポリシーなどの VPN ポリシー情報が含まれています。

次のいずれかの方法で、Cisco Jabber for iPhone and iPad のアプリケーション プロファイルをプロビジョニングすることができます。

ASDM

ASA Device Manager（ASDM）のプロファイル エディタを使用して、Cisco AnyConnect セキュア モビリティ クライアントの VPN プロファイルを定義することをお勧めします。

この方法を使用すると、Cisco AnyConnect セキュア モビリティ クライアントが初めて VPN 接続を確立した以降は、VPN プロファイルが自動的にそのクライアントにダウンロードされます。この方法は、すべてのデバイスおよび OS タイプに使用でき、VPN プロファイルを ASA で集中管理できます。

詳細については、使用しているリリースに応じた『*Cisco AnyConnect Secure Mobility Client Administrator Guide*』の「*Creating and Editing an AnyConnect Profile*」のトピックを参照してください。

iPCU

iPhone Configuration Utility（iPCU）を使用して作成する Apple コンフィギュレーション プロファイルを使用して iOS デバイスをプロビジョニングできます。Apple コンフィギュレーション プロファイルは、デバイスのセキュリティ ポリシー、VPN コンフィギュレーション情報、および Wi-Fi、メール、カレンダーの各種設定などの情報が含まれた XML ファイルです。

高レベルな手順は次のとおりです。

1. iPCU を使用して、Apple コンフィギュレーション プロファイルを作成します。

   詳細については、iPCU の資料を参照してください。

2. XML プロファイルを .mobileconfig ファイルとしてエクスポートします。
3. .mobileconfig ファイルをユーザにメールで送信します。

   ユーザがこのファイルを開くと AnyConnect VPN プロファイルと他のプロファイル設定がクライアント アプリケーションにインストールされます。

MDM

サードパーティの Mobile Device Management（MDM）ソフトウェアを使用して作成する Apple コンフィギュレーションプロファイルを使用して iOS デバイスをプロビジョニングできます。Apple コンフィギュレーション プロファイルは、デバイスのセキュリティ ポリシー、VPN コンフィギュレーション情報、および Wi-Fi、メール、カレンダーの各種設定などの情報が含まれた XML ファイルです。

高レベルな手順は次のとおりです。

1. Apple 設定プロファイルを作成するには MDM を使用します。

   MDM の使用についての詳細は Apple の資料を参照してください。

2. 登録済みデバイスに Apple 設定プロファイルをプッシュします。

Cisco Jabber for Android のアプリケーション プロファイルをプロビジョニングするには、ASA Device Manager（ASDM）のプロファイル エディタを使用して、Cisco AnyConnect セキュア モビリティ クライアントの VPN プロファイルを定義します。Cisco AnyConnect セキュア モビリティ クライアントが初めて VPN 接続を確立した以降は、VPN プロファイルが自動的にそのクライアントにダウンロードされます。この方法は、すべてのデバイスおよび OS タイプに使用でき、VPN プロファイルを ASA で集中管理できます。詳細については、使用しているリリー

スに応じた『*Cisco AnyConnect Secure Mobility Client Administrator Guide*』の「*Creating and Editing an AnyConnect Profile*」のトピックを参照してください。

VPN 接続の自動化

ユーザが企業の Wi-Fi ネットワーク外から Cisco Jabber を開く場合、Cisco Jabber には、Cisco UC アプリケーション サーバにアクセスするための VPN 接続が必要です。Cisco AnyConnect Secure Mobility Client が、バックグラウンドで VPN 接続を自動的に確立できるようにシステムを設定できます。これは、シームレスなユーザ エクスペリエンスの提供に役立ちます。

（注） VPN が自動接続に設定されていても、Expressway Mobile and Remote Access の方が接続優先順位が高いため、VPN は起動されません。

信頼ネットワーク接続のセットアップ

Trusted Network Detection 機能は、ユーザの場所を基にして VPN 接続を自動化することによって、ユーザの体感品質を向上させます。ユーザが社内 Wi-Fi ネットワークの中にいる場合、Cisco Jabber は直接 Cisco UC インフラストラクチャに到達できます。ユーザが社内 Wi-Fi ネットワークを離れると、Cisco Jabber は信頼ネットワークの外側にいることを自動的に検出します。この状況が発生すると、Cisco AnyConnect セキュア モビリティ クライアントは UC インフラストラクチャへの接続を確保するため VPN を開始します。

（注） Trusted Network Detection 機能には、証明書ベース認証およびパスワード ベース認証の両方を使用できます。ただし、証明書ベース認証の方が、よりシームレスな体感を与えることができます。

手順

ステップ 1 ASDM を使用して、Cisco AnyConnect のクライアント プロファイルを開きます。

ステップ 2 クライアントが社内 Wi-Fi ネットワークの中にいるときにインターフェイスで受信可能な、信頼できる DNS サーバおよび信頼できる DNS ドメイン サフィックスのリストを入力します。Cisco AnyConnect クライアントは、現在のインターフェイス DNS サーバおよびドメイン サフィックスを、このプロファイルの設定と比較します。

（注） Trusted Network Detection 機能が正しく動作するためには、DNS サーバをすべて指定する必要があります。TrustedDNSDomains と TrustedDNSServers の両方をセットアップした場合は、信頼ネットワークとして定義した両方の設定とセッションが一致する必要があります。

Trusted Network Detection をセットアップするための詳細な手順については、ご使用のリリースの『*Cisco AnyConnect Secure Mobility Client Administrator Guide*』の「*Configuring AnyConnect Features*」の章（リリース 2.5）または「*Configuring VPN Access*」の章（リリース 3.0 または 3.1）の「*Trusted Network Detection*」のセクションを参照してください。

Connect On Demand VPN の設定

Apple iOS Connect On Demand 機能は、ユーザのドメインに基づいて VPN 接続を自動化することにより、ユーザ エクスペリエンスを強化します。

ユーザが社内 Wi-Fi ネットワークの中にいる場合、Cisco Jabber は直接 Cisco UC インフラストラクチャに到達できます。ユーザが企業の Wi-Fi ネットワーク外に出ると、Cisco AnyConnect は、AnyConnect クライアント プロファイルで指定されたドメインに接続されているか自動的に検出します。その場合、アプリケーションはVPNを開始して、UCインフラストラクチャへの接続を確認します。Cisco Jabber を含めて、デバイス上のすべてのアプリケーションがこの機能を利用できます。

（注） Connect On Demand は、証明書で認証された接続だけをサポートします。

この機能では、次のオプションを使用できます。

- [常に接続（Always Connect）]：Apple iOS は、常にこのリスト内のドメインへの VPN 接続を開始しようとします。
- [必要に応じて接続（Connect If Needed）]：Apple iOS は、DNS を使用してアドレスを解決できない場合のみ、このリスト内のドメインへの VPN 接続を開始しようとします。
- [接続しない（Never Connect）]：Apple iOS は、このリスト内のドメインへの VPN 接続を開始しようとしません。

注目 Apple は近い将来に、[常に接続する（Always Connect）] オプションを削除する予定です。[常に接続する（Always Connect）] オプションの削除後は、ユーザは [必要に応じて接続する（Connect if Needed）] オプションを選択できます。Cisco Jabber ユーザが [必要に応じて接続（Connect if Needed）] オプションを使用したときに問題が発生する場合があります。たとえば、Cisco Unified Communications Manager のホスト名が社内ネットワークの外部で解決可能な場合は、iOS が VPN 接続をトリガーしません。ユーザは、コールを発信する前に、手動で Cisco AnyConnect セキュア モビリティ クライアントを起動することによって、この問題を回避できます。

手順

ステップ 1 ASDM プロファイル エディタ、iPCU、または MDM ソフトウェアを使用して、AnyConnect クライアント プロファイルを開きます。

ステップ 2 AnyConnect クライアント プロファイルの [必要に応じて接続する（Connect if Needed）] セクションで、オンデマンド ドメインのリストを入力します。

ドメイン リストは、ワイルドカード オプション（たとえば、cucm.cisco.com、cisco.com、および *.webex.com）を含むことができます。

Cisco Unified Communications Manager での自動 VPN アクセスのセットアップ

始める前に

- モバイル デバイスで、証明書ベースの認証での VPN へのオンデマンド アクセスが設定されている必要があります。VPN アクセスの設定については、VPN クライアントおよびヘッド エンドのプロバイダーにお問い合わせください。
- Cisco AnyConnect セキュア モビリティ クライアントと Cisco Adaptive Security Appliance の要件については、「ソフトウェア要件」のトピックを参照してください。
- Cisco AnyConnect のセットアップ方法については、『*Cisco AnyConnect VPN Client Maintain and Operate Guides*』を参照してください。

手順

ステップ 1 クライアントがオンデマンドで VPN を起動する URL を指定します。

a) 次のいずれかの方法を使用し、クライアントがオンデマンドで VPN を起動する URL を指定します。

- 必要に応じて接続する（Connect if Needed）

- Cisco Unified Communications Manager をドメイン名（IP アドレスではなく）経由でアクセスするように設定し、このドメイン名がファイアウォールの外側で解決できないことを確認します。
- Cisco AnyConnect クライアント接続の Connect on Demand ドメイン リストで、このドメインを「 必要に応じて接続（Connect If Needed）」リストに追加します。

- 常に接続する（Always Connect）
  - 存在しないドメインにステップ 4 のパラメータを設定します。存在しないドメインはユーザがファイアウォールの内部または外部にいるときに、DNS クエリーが失敗する原因となります。
  - Cisco AnyConnect クライアント接続の Connect on Demand ドメイン リストで、このドメインを「常に接続（Always Connect）」リストに追加します。

    URL は、ドメイン名だけを含む必要があります。プロトコルまたはパスは含めないでください（たとえば、「「https://cm8ondemand.company.com/vpn」」 の代わりに 「「cm8ondemand.company.com」」 を使用します）。

b) Cisco AnyConnect で URL を入力し、このドメインに対する DNS クエリーが失敗することを確認します。

ステップ 2 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 3 ユーザのデバイス ページに移動します。

ステップ 4 [プロダクト固有の設定（Product Specific Configuration Layout）] セクションの [オンデマンド VPNのURL（On-Demand VPN URL）] フィールドに、ステップ 1 で Cisco AnyConnect で特定して使用した URL を入力します。

URL は、ドメイン名だけを含む必要があります。プロトコルやパスを含まないようにしてください。

ステップ 5 [保存（Save）] を選択します。

Cisco Jabber が開くと、URL への DNS クエリーを開始します。この URL が、この手順で定義した On Demand のドメイン リストのエントリ（たとえば、cisco.com）に一致する場合、Cisco Jabber は間接的に AnyConnect VPN 接続を開始します。

次のタスク

- この機能をテストしてください。
  - この URL を iOS デバイスのインターネット ブラウザに入力し、VPN が自動的に起動することを確認します。ステータス バーに、VPN アイコンが表示されます。
  - VPN を使用して、iOS デバイスが社内ネットワークに接続できることを確認します。たとえば、社内イントラネットの Web ページにアクセスしてください。iOS デバイスが接続できない場合は、ご利用の VPN 製品のプロバイダーに問い合わせてください。

- VPN が特定のタイプのトラフィックへのアクセスを制限（管理者が電子メールと予定表のトラフィックだけが許可されるようにシステムを設定している場合など）していないことを IT 部門に確認します。

- クライアントが、社内ネットワークに直接接続されるように設定されていることを確認します。

AnyConnect の参照ドキュメント

AnyConnect の要件と展開の詳細については、次の場所にある、ご使用のリリースに対応したドキュメントを参照してください。 https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-user-guide-list.html

セッション パラメータ

セキュア接続のパフォーマンスを向上するために ASA セッション パラメータを設定できます。最良のユーザ エクスペリエンスを得るために、次の ASA セッション パラメータを設定する必要があります。

- [Datagram Transport Layer Security]（DTLS）：DTLS は、遅延とデータ消失を防ぐデータパスを提供する SSL プロトコルです。
- [自動再接続（Auto Reconnect）]：自動再接続またはセッション永続性を使用すれば、Cisco AnyConnect Secure Mobility Client はセッション中断から回復して、セッションを再確立できます。
- [セッション永続性（Session Persistence）]：このパラメータを使用すると、VPN セッションをサービス中断から回復し、接続を再確立できます。
- [アイドルタイムアウト（Idle Timeout）]：アイドル タイムアウトは、通信アクティビティが発生しない場合に、ASA がセキュア接続を切断するまでの期間を定義します。
- [デッドピア検出（Dead Peer Detection）]（DTD）：DTD は、ASA と Cisco AnyConnect Secure Mobility Client が、障害が発生した接続をすばやく検出できることを保証します。

ASA セッション パラメータの設定

Cisco AnyConnect Secure Mobility Client のエンドユーザのユーザ エクスペリエンスを最適化するために、次のように ASA セッション パラメータを設定することを推奨します。

手順

ステップ 1 DTLS を使用するように、Cisco AnyConnect を設定します。

詳細については、『*Cisco AnyConnect VPN Client Administrator Guide, Version 2.0*』の「*Configuring AnyConnect Features Using ASDM*」の章の、「*Enabling Datagram Transport Layer Security (DTLS) with AnyConnect (SSL) Connections*」のトピックを参照してください。

ステップ 2 セッションの永続性（自動再接続）を設定します。

a) ASDM を使用して VPN クライアント プロファイルを開きます。
b) [自動再接続の動作（Auto Reconnect Behavior）] パラメータを [復帰後に再接続（Reconnect After Resume）] に設定します。

詳細については、ご使用のリリースの『*Cisco AnyConnect Secure Mobility Client Administrator Guide*』の「*Configuring AnyConnect Features*」の章（リリース 2.5）または「*Configuring VPN Access*」の章（リリース 3.0 または 3.1）の「*Configuring Auto Reconnect*」のトピックを参照してください。

ステップ 3 アイドル タイムアウト値を設定します。

a) Cisco Jabber クライアントに固有のグループ ポリシーを作成します。
b) アイドル タイムアウト値を 30 分に設定します。

詳細については、ご使用のリリースの『*Cisco ASA 5580 Adaptive Security Appliance Command Reference*』の「*vpn-idle-timeout*」のセクションを参照してください。

ステップ 4 Dead Peer Detection（DPD）を設定します。

a) サーバ側の DPD を無効にします。
b) クライアント側の DPD を有効にします。

詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6*』の「*Configuring VPN*」の章の、「*Enabling and Adjusting Dead Peer Detection*」のトピックを参照してください。

ユーザプロファイルのためのモバイルおよびリモートアクセス ポリシー

ユーザーが企業ネットワークの外部で作業している場合、Cisco Unified Communications Manager にモバイルおよびリモートアクセス（MRA）アクセス ポリシーを追加して、Cisco Jabber でアクセス可能なサービスを制御できます。MRA アクセス ポリシーはユーザープロファイルに割り当てられ、組織内のユーザに異なる MRA アクセス ポリシーを割り当てることができます。

始める前に

モバイルおよびリモート アクセス ポリシーは、Cisco Unified Communications Manager Release 12.0 以降、Cisco Expressway X 8.10 以降、および OAuth 対応環境でサポートされています。

手順

ステップ 1 [**Cisco Unified CM の管理**（**Cisco Unified CM Administration**）]で, [**ユーザー管理**（**User Management**）]に移動し、[**エンドユーザー**（**End User**）]を選択します。

ステップ 2 [**検索 (Find)**] をクリックしてエンドユーザを検索し、選択します。

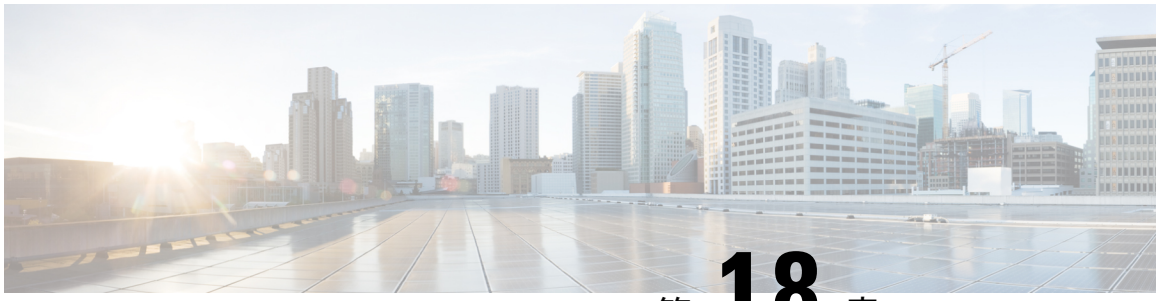
ステップ 3 [**エンドユーザの設定**（**End User Configuration**）] ウィンドウで、**ユーザプロファイル**の[**詳細表示**（**View Details**）] をクリックします。

ステップ 4 [**モバイルとリモートアクセスポリシー**（**Mobile and Remote Access Policy**）] セクションで、[**モバイルおよびリモートアクセスを有効にする**（**Enable Mobile and Remote Access**）] を選択します。

ステップ 5 [**Jabber ポリシー**（**Jabber Policies**）] ドロップダウンから、ポリシーを選択します。

- **サービスなし**: ユーザは Cisco Jabber サービスにアクセスできません。
- **IM & プレゼンスのみ**: ユーザは IM、プレゼンス、ボイスメール、および連絡先の検索にのみアクセスできます。
- **IM & プレゼンス、音声、およびビデオコール**: ユーザは、すべての Cisco Jabber サービスにアクセスできます。

ステップ 6 [**保存**（**Save**）] を選択します。



第 18 章

Quality of Service

Quality of Service オプション

Cisco Jabber の Quality of Service を設定するには、次のオプションを使用します。

オプション	説明
メディア保証の有効化 （181 ページ）	Cisco Unified Communications Manager でメディア保証を設定します。
サポートされるコーデック （183 ページ）	各クライアントのサポートされているコーデックを確認します。
SIP プロファイルでのポート範囲の定義 （184 ページ）	Cisco Unified Communications Manager でポート範囲を設定します。
Jabber-config.xml でのポート範囲の定義 （185 ページ）	jabber-config.xml ファイルでポート範囲を設定します。
DSCP 値の設定 （185 ページ）	Differentiated Services Code Point（DSCP）の値を設定します。

メディア保証の有効化

メディア保証サポートでは、低いメディア品質が原因で会議が中断されないように、すべてのネットワーク タイプでリアルタイム メディアの品質が強化されます。

始める前に

Cisco Unified Communications Manager リリース 10.x 以降のビデオと、Cisco Unified Communications Manager リリース 11.5 以降のオーディオとビデオでは、メディア保証がサポートされています。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[デバイス（Device）] > [デバイスの設定（Device Settings）] > [SIP プロファイル（SIP Profile）]** の順に選択します。

ステップ 3 選択リストからプロファイルを選択します。

ステップ 4 [**SDP 情報（SDP Information**）] セクションの [**SDP 透過性プロファイル（SDP Transparency Profile**）] で、[**不明な SDP 属性をすべて渡す（Pass all unknown SDP attributes**）] を選択します。

ステップ 5 [**設定の適用（Apply Config**）] を選択します。
このプロファイルを使用するすべての SIP デバイスは、再起動してからでなければどの変更も適用されません。

サポートされるコーデック

タイプ（Type）	コーデック	コーデック タイプ	Android 版 Cisco Jabber	iPhone および iPad 版 Cisco Jabber	Mac 版 Cisco Jabber	Windows 版 Cisco Jabber
[音声（Audio）]	G.711	A-law	○ 通常モードをサポートします。		はい	はい
		μ-law/Mu-law	○ 通常モードをサポートします。		はい	はい
	G.722		はい		はい	はい
	G.722.1	24 kb/s および 32 kb/s	○ 通常モードをサポートします。		はい	はい
	G.729		G.729 でのビジュアルボイスメールはサポートされていませんが、ユーザは G.729 と [ボイスメールに発信（Call Voicemail）] 機能を使用してボイスメッセージにアクセスできます。		不可	不可
	G.729a		○ 狭帯域幅で使用するための最小要件です。 狭帯域幅モードをサポートするコーデックだけです。 通常モードをサポートします。		はい	はい
	Opus		はい		はい	はい

タイプ（Type）	コーデック	コーデック タイプ	Android 版 Cisco Jabber	iPhone および iPad 版 Cisco Jabber	Mac 版 Cisco Jabber	Windows 版 Cisco Jabber
[ビデオ（Video）]	H.264/AVC	ベースライン プロファイル	はい		はい	はい
		高プロファイル	不可		はい	はい
[ボイスメール（Voicemail）]	G.711	A-law	はい		はい	はい
		μ-law/Mu-law（デフォルト）	はい		はい	はい
	GSM 06.10		はい		はい	はい
	PCM リニア		はい		はい	はい

Android 版 Cisco JabberまたはiPhone および iPad 版 Cisco Jabberの使用中に音声品質に問題が発生した場合は、クライアント設定で狭帯域幅モードのオンとオフを切り替えることができます。

SIP プロファイルでのポート範囲の定義

クライアントは、ポート範囲を使用して、ネットワークに RTP トラフィックを送信します。また、クライアントは、ポート範囲を均等に分割して、下半分を音声コール用に、上半分をビデオ コール用に使用します。オーディオ メディアおよびビデオ メディアのポート範囲を分割する結果として、クライアントにより識別可能なメディア ストリームが作成されます。IP パケットのヘッダー内の DSCP 値を設定することで、それらのメディア ストリームを分類し、優先させることができます。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[デバイス（Device）] > [デバイスの設定（Device Settings）] > [SIP プロファイル（SIP Profile）]** の順に選択します。

ステップ 3 適切な SIP プロファイルを検索するか、新しい SIP プロファイルを作成します。

[SIP プロファイルの設定（SIP Profile Configuration）] ウィンドウが開きます。

ステップ 4 音声とビデオのポート範囲を共通にするか分離するかを指定します。音声とビデオのポート範囲を分離する場合は、音声ポートとビデオ ポートを設定します。次のフィールドにポート範囲を指定してください。

- [開始メディアポート（Start Media Port）]：メディア ストリームの開始ポートを定義します。このフィールドは、範囲の最小ポートを設定します。
- [終了メディアポート（Stop Media Port）]：メディア ストリームの終了ポートを定義します。このフィールドは、範囲の最大ポートを設定します。

ステップ 5 [設定の適用（Apply Config）] を選択し、[OK] をクリックします。

Jabber-config.xml でのポート範囲の定義

このトピックは、Windows 版 Cisco Jabber に適用されます。

手順

ユーザがWindows版Cisco Jabberのチャット ウィンドウで画面を共有するときに使用すべきポート範囲を指定するには、『*Cisco Jabber Parameters Reference Guide*』の「SharePortRangeStart」を参照してください。

DSCP 値の設定

ネットワークを通過する Cisco Jabber トラフィックに優先順位を付ける場合に、RTP メディア パケット ヘッダーで DiffServ コード ポイント（DSCP）値を設定します。

Cisco Unified Communications Manager での DSCP 値の設定

Cisco Unified Communications Manager で音声メディアとビデオ メディアの DSCP 値を設定できます。そうすれば、Cisco Jabber は、デバイス設定から DSCP 値を取得して、それらを RTP メディア パケットの IP ヘッダーに直接適用できます。

制約事項 Microsoft Windows 7 などの新しいオペレーティング システムには、アプリケーションで IP パケット ヘッダーの DSCP 値が設定できないようにするセキュリティ機能が実装されています。そのため、Microsoft グループ ポリシーなどの DSCP 値をマーキングするための代替方式を使用する必要があります。

フレキシブル DSCP 値の設定の詳細については、『Configure Flexible DSCP Marking and Video Promotion Service Parameters』を参照してください。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。

ステップ 2 **[システム（System）] > [サービス パラメータ（Service Parameters）]** の順に選択します。

[サービス パラメータ設定（Service Parameter Configuration）] ウィンドウが開きます。

ステップ 3 適切なサーバを選択してから、[Cisco CallManager（Cisco CallManager）] サービスを選択します。

ステップ 4 [クラスタ全体のパラメータ（システム：QOS）（Clusterwide Parameters (System - QOS)）] セクションを見つけます。

ステップ 5 適切な DSCP 値を設定し、[保存（Save）] を選択します。

グループ ポリシーを用いた DSCP 値の設定

Microsoft Windows 7 などの新しいオペレーティング システム上で Cisco Jabber for Windows を展開する場合は、Microsoft グループ ポリシーを使用して DSCP 値を適用できます。

グループ ポリシーを作成するには、Microsoft サポートの記事（http://technet.microsoft.com/en-us/library/cc771283%28v=ws.10%29.aspx）の手順を実行します。

次の属性を用いて音声メディアとビデオ メディアに別々のポリシーを作成する必要があります。

属性（Attributes）	音声ポリシー	ビデオ ポリシー	シグナリング ポリシー
アプリケーション名	`CiscoJabber.exe`	`CiscoJabber.exe`	`CiscoJabber.exe`
プロトコル	UDP	UDP	TCP
ポート番号または範囲	Cisco Unified Communications Manager 上の SIP プロファイルからの対応するポート番号または範囲。	Cisco Unified Communications Manager 上の SIP プロファイルからの対応するポート番号または範囲。	SIP は 5060 安全な SIP の場合は 5061
DSCP 値	46	34	24

クライアントの DSCP 値の設定

一部の構成には、Cisco Jabber for Mac クライアントとモバイル クライアント用 Cisco Jabber のコールで Diffserv を有効にするオプションがあります。

重要 このオプションは、デフォルトで有効です。シスコは、次のシナリオで問題が発生しない限り、このオプションを無効にしないことを推奨します。

- 他の参加者の声を聞いたり、姿を確認できるが、自分の声や姿は確認されない。
- 予期しない Wi-Fi 接続問題が発生している。

通話の Diffserv を無効にすると、オーディオやビデオの品質が低下する可能性があります。

（注） EnableDSCPPacketMarking を true または false に設定すると、Cisco Jabber クライアントで [コールの Diffserv の有効化（Enable Differentiated Service for Calls）] が表示されません。

手順

ステップ 1 Cisco Jabber for Mac で、[Jabber] > [設定（Preferences）] > [コール（Calls）] > [詳細（Advanced）] に移動し、[コールの Diffserv の有効化（Enable Differentiated Service for Calls）] を選択します。

ステップ 2 モバイル クライアント用 Cisco Jabber で、[Jabber] > [設定（Settings）] > [オーディオとビデオ（Audio and Video）] に移動し、[コールの Diffserv の有効化（Enable Differentiated Service for Calls）] を選択します。

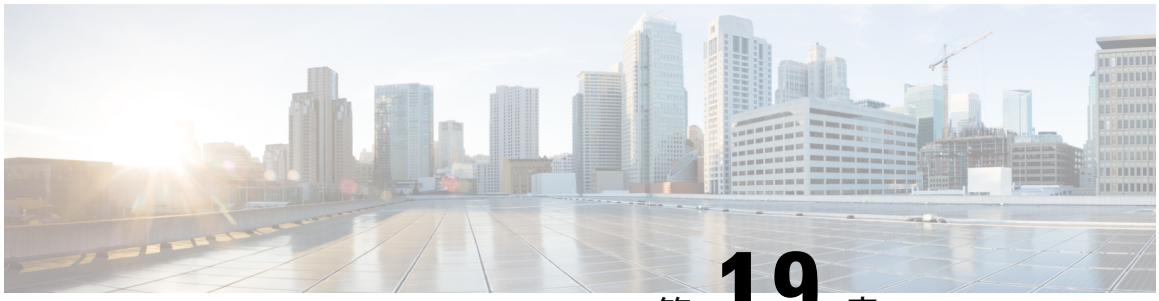
ネットワーク内の DSCP 値の設定

スイッチおよびルータを設定し、RTP メディアの IP ヘッダーで DSCP 値をマーキングします。

ネットワーク内の DSCP 値を設定するには、クライアント アプリケーションからの異なるストリームを識別する必要があります。

- メディア ストリーム：クライアントは音声ストリームとビデオ ストリームに別々のポート範囲を使用するため、それらのポート範囲に基づいて音声メディアとビデオ メディアを区別できます。SIP プロファイルのデフォルトのポート範囲を使用して、次のようにメディア パケットをマーキングする必要があります。
  - 音声メディアは、EF として、16384 ～ 24574 のポートでストリーミング
  - ビデオ メディアは、AF41 として、24575 ～ 32766 のポートでストリーミング
- シグナリング ストリーム：SIP、CTI QBE、および XMPP に必要なさまざまなポートに基づいて、クライアントとサーバ間のシグナリングを識別できます。たとえば、Cisco Jabber と Cisco Unified Communications Manager 間の SIP シグナリングはポート 5060 を介して行われます。

  AF31 としてシグナリング パケットをマーキングする必要があります。



第 19 章

Cisco Jabber のアプリケーションとの統合

Microsoft SharePoint 2010 および 2013 でのプレゼンスの設定

IMアドレスがメールアドレスと異なる状況で組織がユーザのプロファイルを定義する場合は、クライアントと Microsoft SharePoint 2010 および 2013 の間でプレゼンス統合を有効にする追加設定が必要になります。

始める前に

- Cisco Jabber for Windows クライアント専用。
- すべてのサイトが Microsoft SharePoint Central Administration（CA）と同期していることを確認します。
- Microsoft SharePoint と Active Directory 間の同期がセットアップされていることを確認します。

手順

ステップ 1 Microsoft SharePoint 2013 を使用している場合は、次の情報でユーザの SharePoint CA プロファイル ページを更新します。

a) [SIPアドレス（SIP Address）] プロファイル フィールドを空白のままにします。

b) [勤務先電子メール（Work email）] プロファイル フィールドに、ユーザ プロファイルを入力します。たとえば、**`john4mail@example.pst`** と入力します。

ステップ 2 Microsoft SharePoint 2010 を使用している場合は、次の情報でユーザの SharePoint CA プロファイル ページを更新します。

a) [SIPアドレス（SIP Address）] プロファイル フィールドに、ユーザ プロファイルを入力します。たとえば、**john4mail@example.pst** と入力します。
b) [勤務先電子メール（Work email）] プロファイル フィールドを空白のままにします。

クライアントのアベイラビリティ

ユーザは、クライアントの [オプション（Options）] ウィンドウの [ステータス（Status）] タブで自分たちがミーティング中であることを第三者に知らせるためのオプションを設定することによって、自分たちのアベイラビリティが予定表イベントに影響するかどうかを定義できます。このオプションは、予定表内のイベントとユーザのアベイラビリティを同期させます。クライアントには、サポートされている統合カレンダーの [ミーティング中（In a meeting）] アベイラビリティしか表示されません。

クライアントは、[ミーティング中（In a meeting）] アベイラビリティに関する次の 2 つのソースの使用をサポートします。

（注） モバイル クライアント向け Cisco Jabber は、Cisco Jabber 11.7 リリース以降でこのミーティング統合機能をサポートします。

- Microsoft Exchange と Cisco Unified Communication Manager IM and Presence の統合：オンプレミス展開に適用されます。Cisco Unified Presence の [マイ プレゼンス ステータスをカレンダー情報に包含する（Include Calendar information in my Presence Status）] フィールドとクライアントの [ミーティング中（In a meeting）] オプションは同じものです。両方のフィールドが Cisco Unified Communication Manager IM and Presence データベース内の同じ値を更新します。

  ユーザが両方のフィールドを別々の値で設定した場合は、最後に設定したフィールドが優先されます。クライアントが実行されている際に、ユーザが [マイ プレゼンス ステータスをカレンダー情報に包含する（Include Calendar information in my Presence Status）] フィールドの値を変更すると、ユーザはその変更を適用させるためにクライアントを再起動する必要があります。

- Cisco Jabber クライアント：オンプレミス展開とクラウドベース展開に適用されます。[ミーティング中（In a meeting）] アベイラビリティを設定するには、クライアントの Cisco Unified Communication Manager IM and Presence と Microsoft Exchange の統合を無効にする必要があります。クライアントは、Cisco Unified Communication Manager IM and Presence と Microsoft Exchange 間の統合がオンなのか、オフなのかをチェックします。また、クライアントは、統合がオフの場合にだけアベイラビリティを設定できます。

次の展開シナリオで、アベイラビリティの作成方法について説明します。

導入シナリオ	[ミーティング中（個人用のカレンダーより）（**In a meeting (according to my calendar)**）] を選択します。	[ミーティング中（個人用のカレンダーより）（**In a meeting (according to my calendar)**）] を選択しません。
Cisco Unified Communication Manager IM and Presence と Microsoft Exchange 間の統合を有効にする	Cisco Unified Communication Manager IM and Presence によってアベイラビリティ ステータスが設定されます。	アベイラビリティ ステータスは変更されません。
Cisco Unified Communication Manager IM and Presence と Microsoft Exchange 間の統合を有効にしない	クライアントにより、アベイラビリティ ステータスが設定されます。	アベイラビリティ ステータスは変更されません。
クラウドベース展開	クライアントにより、アベイラビリティ ステータスが設定されます。	アベイラビリティ ステータスは変更されません。

また、次の表に、展開シナリオ別にサポートされるアベイラビリティの説明を示します。

クライアントで有効にされたアベイラビリティ	**Cisco Unified Communication Manager IM and Presence と Microsoft Exchange の統合によって有効にされたアベイラビリティ**
[オフライン（ミーティング中）（Offline in a meeting）] アベイラビリティはサポートされません。	[オフライン（ミーティング中）（Offline in a meeting）] アベイラビリティがサポートされます。
非予定表イベントに対して [ミーティング中（In a meeting）] アベイラビリティがサポートされます。	非予定表イベントに対して [ミーティング中（In a meeting）] アベイラビリティはサポートされません。

（注） [オフライン（ミーティング中）（Offline in a meeting）] アベイラビリティは、ユーザがクライアントにログインしていないが、ユーザの予定表にイベントが存在していることを意味します。

非予定表イベントとは、インスタントミーティング、[**オフライン（Offline**）]、[**電話中（On a call**）]などのユーザの予定表に表示されないイベントを意味します。

プロトコル ハンドラ

Cisco Jabber は、次のプロトコル ハンドラをオペレーティング システムに登録し、クリックツーコールまたはクリックツー IM 機能を Web ブラウザやその他のアプリケーションから使用できるようにします。

- XMPP: または XMPP://

  Cisco Jabber でインスタント メッセージを開始し、チャット ウィンドウを開きます。

- IM: または IM://

  Cisco Jabber でインスタント メッセージを開始し、チャット ウィンドウを開きます。

- TEL: または TEL://

  Cisco Jabber で音声またはビデオ コールを開始します。

  （注） TEL は Apple 純正の電話機に登録されます。Cisco Jabber for iPhone and iPad を相互起動するために使用することはできません。

- CISCOTEL: または CISCOTEL://

  Cisco Jabber で音声またはビデオ コールを開始します。

- SIP: または SIP://

  Cisco Jabber で音声またはビデオ コールを開始します。

- CLICKTOCALL: または CLICKTOCALL://

  Cisco Jabber で音声またはビデオ コールを開始します。

プロトコル ハンドラのレジストリ エントリ

プロトコル ハンドラとして登録するために、クライアントが Microsoft Windows レジストリの次の場所に書き込みます。

- `HKEY_CLASSES_ROOT\tel\shell\open\command`
- `HKEY_CLASSES_ROOT\xmpp\shell\open\command`
- `HKEY_CLASSES_ROOT\im\shell\open\command`

2 つ以上のアプリケーションが同一プロトコルのハンドラとして登録される場合は、レジストリに最後に書き込まれたアプリケーションが優先されます。たとえば、Cisco Jabber が XMPP: のプロトコル ハンドラとして登録された後に別のアプリケーションが XMPP: のプロトコル ハンドラとして登録された場合は、別のアプリケーションの方が Cisco Jabber より優先されます。

HTML ページのプロトコル ハンドラ

HTML ページに、href 属性の一部としてプロトコル ハンドラを追加します。HTML ページに表示されるハイパーリンクをクリックすると、クライアントはプロトコルに対して適切な処理を実行します。

TEL および IM プロトコル ハンドラ

HTML ページの TEL: および IM: プロトコル ハンドラの例。

```
<html>
  <body>
    <a href="TEL:1234">Call 1234</a><br/>
    <a href="IM:msmith@domain">Send an instant message to Mary Smith</a>
  </body>
</html>
```

前の例では、ユーザがハイパーリンクをクリックして 1234 に発信すると、クライアントはその電話番号への音声コールを開始します。ユーザが Mary Smith にインスタント メッセージを送信するハイパーリンクをクリックすると、クライアントは Mary とのチャット ウィンドウを開きます。

CISCOTEL および SIP プロトコル ハンドラ

HTML ページの CISCOTEL および SIP プロトコル ハンドラの例：

```
<html>
  <body>
    <a href="CISCOTEL:1234">Call 1234</a><br/>
    <a href="SIP:msmith@domain">Call Mary</a><br/>
    <a href="CISCOTELCONF:msmith@domain;amckenzi@domain">Weekly conference call</a>
  </body>
</html>
```

上記の例では、ユーザが *1234* へコール または *Mary* にコール のハイパーリンクをクリックすると、クライアントはその電話番号への音声コールを開始します。

XMPP プロトコル ハンドラ

HTML ページの XMPP: プロトコル ハンドラを使用したグループ チャットの例。

```
<html>
  <body>
    <a href="XMPP:msmith@domain;amckenzi@domain">Create a group chat with Mary Smith and
 Adam McKenzie</a>
  </body>
</html>
```

前の例では、ユーザが Mary Smith および Adam McKenzie とのグループ チャットを作成するハイパーリンクをクリックすると、クライアントは Mary および Adam とのグループ チャット ウィンドウを開きます。

ヒント XMPP: および IM: ハンドラに連絡先リストを追加し、グループ チャットを作成します。連絡先を区切るには、次の例のようにセミコロンを使用します。

```
XMPP:user_a@domain.com;user_b@domain.com;user_c@domain.com;user_d@domain.com
```

件名と本文の追加

プロトコル ハンドラに件名と本文を追加できます。これにより、ユーザがパーソンツーパーソンまたはグループのチャットを作成するために、ハイパーリンクをクリックすると、クライアントはチャット ウィンドウを開き、前もって入力された件名と本文を表示します。

件名と本文は、次のいずれのシナリオでも追加できます。

- クライアントでインスタント メッセージング用にサポートされているプロトコル ハンドラを使用する
- パーソンツーパーソン チャットまたはグループ チャットのいずれか
- 件名と本文を含める、またはそのどちらかを含める

次の例では、ユーザが下のリンクをクリックすると、前もって入力された **I.T Desk** の本文を含む、パーソンツーパーソン チャット ウィンドウが開きます。

```
xmpp:msmith@domain?message;subject=I.T.%20Desk
```

次の例では、ユーザが下のリンクをクリックすると、[I.T Desk] のトピックを含む [グループ チャットの開始（Start Group Chat）] ダイアログボックスが開き、チャット ウィンドウの入力ボックスには「Jabber 10.5　Query」というテキストが入力されています。

```
im:user_a@domain.com;user_b@domain.com;user_c@domain.com?message;subject=I.T%20Desk;body=Jabber%2010.5%20Query
```

プロトコル ハンドラでサポートされるパラメータ

モバイル クライアントの相互起動

モバイル クライアント用 Cisco Jabber では、指定したアプリケーションに戻ることができます。たとえば、番号をダイヤルする ciscotel URI リンクを作成する場合に、パラメータとしてアプリケーション名を追加し、コールの終了時にそのアプリケーションに戻るようユーザに要求できます。

```
ciscotel://1234567?CrossLaunchBackSchema=SomeAppSchema&CrossLaunchBackAppName=SomeAppName
```

- CrossLaunchBackAppName：コール終了時に Cisco Jabber が相互起動するアプリケーションの名前を入力することをユーザに求めます。
  - none（デフォルト）：ダイアログ ボックスにアプリケーションが表示されません。
  - *app_name*：ダイアログ ボックスに表示されるアプリケーション名。
- CrossLaunchBackSchema：コールが終了したときに使用するスキーマを指定します。

- none（デフォルト）：Cisco Jabber に留まります。
- *schema*：アプリケーションの相互起動に使用されるスキーマ。

サポートされる区切り文字

HTML ページの URI リンクを作成するときに、セミコロンを使用して文字を区切ることができます。これは、SIP、Tel、CiscoTel、および ClickToCall プロトコル ハンドラでサポートされます。次の例では、2 つの番号を使用する電話会議がリンクに作成されます。

```
tel:123;123
```

IM プロトコルは、セミコロン区切り文字をサポートしています。次の例では、2 人の参加者がいるグループ チャットがリンクに作成されます。

```
im:participant1@example.com,participant2@example.com
```

DTMF サポート

IM ウィンドウでの DTMF の入力

クライアントの会話ウィンドウで、DTMF 数字を含むプロトコル ハンドラを入力すると、参加者が使用できるリンクがクライアントによって作成されます。サポートされるプロトコルは、TEL、CISCOTEL、SIP、CLICKTOCALL、CISCOIM、IM および XMPPです。サポートされるパラメータは番号または SIP URI です。

次の例では、番号が 1800123456、エントリの PIN が 5678# です。この TEL URI リンクを使用して会議リンクが作成されます。

```
tel:1800123456,,,5678#
```

アクティブ コールでの DTMF の入力

コール中、ユーザは DTMF 数字をコピーしてクライアントのコール ウィンドウに貼り付けることができます。ユーザは会議招待状の会議 ID、参加者 ID、PIN を簡単に入力できます。アクティブ コール中に英数字の文字列を入力すると、それらの文字列はキーパッドの対応する番号に解釈されます。

サポートされている DTMF 信号

ユーザが、JabberがコールしているシステムでサポートされていないDTMF信号を入力した場合、Jabber はユーザの入力を発信しません。

Cisco Jabber for Windows および mobiles では、次の DTMF 信号がサポートされています。

- 0 ～ 9
- #
- *
- A ~ D

第 IV 部

トラブルシューティング

第 20 章

トラブルシューティング

Cisco Jabber 診断ツール

Windows および Mac

Cisco Jabber 診断ツールは、次のサービスの設定と診断情報を提供します。

- サービス検出
- Webex
- Cisco Unified Communications Manager の概要
- Cisco Unified Communications Manager の設定
- ボイスメール（Voicemail）
- 証明書の検証
- Active Directory
- DNS レコード

このツールにアクセスするには、ハブ、コール、またはチャット ウィンドウにフォーカスし、**Ctrl + Shift + D** を選択する必要があります。

[**リロード（Reload）**] を選択すると、データを更新できます。また、[**保存（Save）**] を選択すると、情報を HTML ファイルに保存できます。

このツールはデフォルトで使用可能です。このツールを無効にするには、次の手順を実行します。

- Jabber for Windows の場合は、DIAGNOSTICSTOOLENABLED インストール パラメータを FALSE に設定します。

- Jabber for Mac の場合は、DiagnosticsToolEnabled パラメータを設定 URL に追加し、値を FALSE に設定します。

これらのパラメータについての詳細は、ご使用の環境に応じて『*Cisco Jabber* のオンプレミス展開』または『*Cisco Jabber* のクラウド展開とハイブリッド展開』を参照してください。

Android、iPhone、および iPad

ユーザが Cisco Jabber または Cisco Jabber IM にサインインできず、電話サービスが接続されない場合、**診断エラー** オプションを使用して、問題の原因を調べることができます。

ユーザは、[**サインイン**] ページまたは Cisco Jabber サービスに接続する際に取得した警告通知から、[**診断エラー**] オプションをタップできます。Cisco Jabber は次のことを確認します。

- ネットワークに問題があるかどうか
- Cisco Jabber サーバが到達可能かどうか
- Cisco Jabber が再接続可能であるかどうか

これらのチェックのいずれかが失敗した場合、Cisco Jabber は、考えられる解決策を含むエラーレポートを表示します。問題が引き続き発生する場合は、問題レポートを送信できます。

連絡先の解決ツール

Cisco Jabber for Windows に適用されます。

連絡先の解決ツールは、使用可能なディレクトリ ソースに関する情報と、連絡先の検索結果を表示する検索ツールを提供します。

連絡先の解決ツールにアクセスするには、ハブ、コール、またはチャット ウィンドウにフォーカスし、**Ctrl + Shift + C** を選択する必要があります。

このツールはデフォルトで使用可能であり、無効にするには ContactsDiagnosticsToolEnabled インストール パラメータを FALSE に設定します。

このツールには次の検索オプションがあります。

- [予測（Predictive）]：文字列を入力するにつれ、一致するレコードが表示されます。これは、ユーザがクライアントで連絡先を検索するときに使用される検索と同じです。
- [等価（Equivalence）]：この検索タイプには、検索文字列を解決するためさらに細かいオプションが含まれています。
  - URI または JID
  - 電話番号（Phone number）
  - SIP URI
  - E メール

検索結果として、指定した値に一致するレコードが返されます。

ContactsDiagnosticsToolEnabled インストール パラメータについての詳細は、ご使用の環境に応じて『*Cisco Jabber* のオンプレミス展開』または『*Cisco Jabber* のクラウド展開とハイブリッド展開』を参照してください。