Cisco Jabber 14.1 の Webex Messenger 導入

初版：2022 年 2 月 24 日

最終更新：2024 年 4 月 1 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

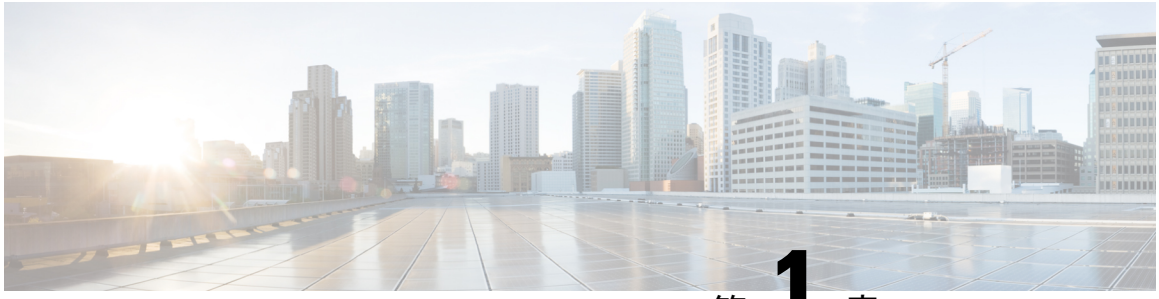
目 次

変更履歴

新規および変更情報

日付（Date）	説明	Location
2022 年 7 月	Rosetta を使用せずに、Apple M1 Mac で Jabber を実行するためのサポートが追加されました。	Mac 版 Cisco Jabber のインストーラ
2022 年 2 月	Initial Publication	

変更履歴



第 1 章

Jabber の概要

このマニュアルの目的

このガイドには、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。

- クラウドまたはハイブリッド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、https://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

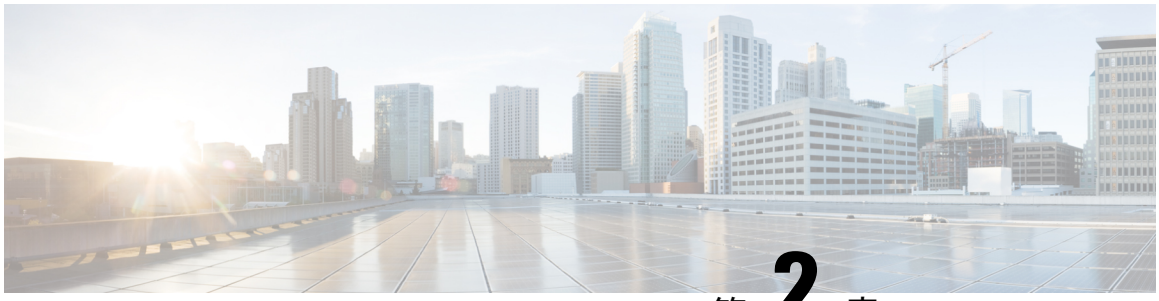
Cisco Jabber は、あらゆる場所から連絡先とのシームレスな対話を実現する Unified Communications アプリケーションスイートです。Cisco Jabber は、IM、プレゼンス、音声およびビデオ通話、ボイスメール、および会議を提供します。

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

- Android 版 Cisco Jabber
- 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

クラウドおよびハイブリッド展開のワークフロー

Cisco Webex Messenger を使用したクラウド導入のワークフロー

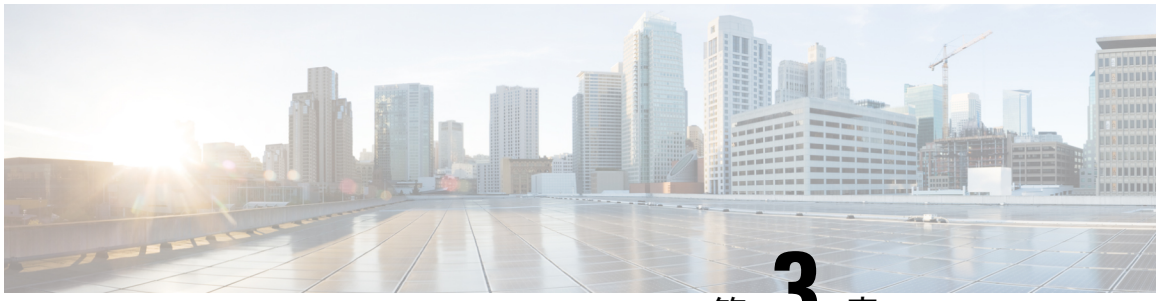
手順

	コマンドまたはアクション	目的
ステップ 1	ポリシーの設定 （5 ページ）	
ステップ 2	クラウド展開のユーザの作成 （15 ページ）	
ステップ 3	証明書の検証設定 （57 ページ）	
ステップ 4	クライアントの設定 （59 ページ）	
ステップ 5	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 （73 ページ）	

Webex Messenger を使用したハイブリッド導入のワークフロー

手順

	コマンドまたはアクション	目的
ステップ 1	ポリシーの設定 （5 ページ）	
ステップ 2	クラスタの設定 （11 ページ）	
ステップ 3	Unified Communications Manager のユーザの作成 （23 ページ）	
ステップ 4	ソフトフォンの設定 （37 ページ）	
ステップ 5	デスクフォン制御の設定 （29 ページ）	
ステップ 6	拡張および接続機能の設定 （49 ページ）	
ステップ 7	Remote Access のためのサービス検出の設定 （55 ページ）	
ステップ 8	証明書の検証設定 （57 ページ）	
ステップ 9	クライアントの設定 （59 ページ）	
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 （73 ページ）	
ステップ 11	Remote Access （125 ページ）	



第 3 章

ポリシーの設定

ポリシーの追加

ステップ 1 [ポリシー エディタ（Policy Editor）]タブを選択します。
[ポリシー（Policy）] 画面の左側に **[ポリシーリスト（Policy List）]**、右側に **[アクションリスト（Action List）]** が表示されます。

ステップ 2 [ポリシー リスト（Policy List）]で [追加（Add）]を選択します。
既存のポリシーのリストの最上部に新しいポリシーが表示されます。

ステップ 3 ポリシーの一意の名前を入力します。

次のタスク

このポリシーにアクションを追加するには、次を参照してください。 ポリシーへのアクションの追加 （5 ページ）

ポリシーへのアクションの追加

ステップ 1 [ポリシー エディタ（Policy Editor）]タブを選択します。
[ポリシーエディタ（Policy Editor）] 画面の左側に **[ポリシーリスト（Policy List）]**、右側に **[アクションリスト（Action List）]** が表示されます。

ステップ 2 [ポリシー名（Policy Name）]で、アクションを追加するポリシーを選択します。

ステップ 3 アクションを追加するには、画面の右側の **[アクションリスト（Action List）]** の下にある **[追加（Add）]** を選択します。

[アクション エディタ（Action Editor）]画面が表示されます。

ステップ 4 [アクション タグ名（Action Tag Name）]リストからポリシー アクションを選択します。

ステップ 5 **保存**を選択します。

ステップ 6 すべてのポリシーにアクションが割り当てられるまで、ステップ 3 ～ 5 を繰り返します。

ポリシー アクション Webex

デフォルトでは、新規にプロビジョニングされた Webex の組織に対し、ユーザに付与されたすべての機能が備えられています。

（注） デフォルトでは、エンドツーエンドの暗号化ポリシーは有効になっていません。組織の管理者はこのポリシーを有効にすることができます。管理者は、すべてのユーザまたは特定のユーザグループの一部の機能を無効にする必要がある場合に、ポリシーを作成できます。

ポリシー アクションは、サードパーティ製の XMPP IM アプリケーションを使用しているユーザには適用できません。

VoIP 会議の参加者が 10 人未満であれば、同じ VoIP 会議に同時に接続できます。

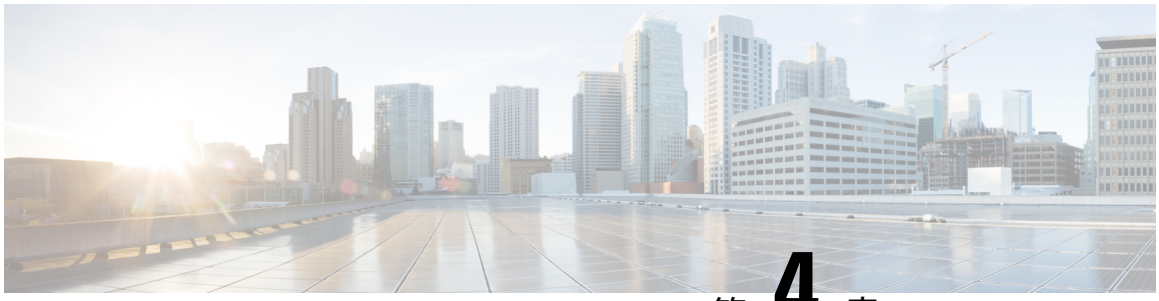
外部ユーザとは、Webex に組織に属していないユーザのことです。 これらのユーザも Webex を使用して、Webex の組織に属しているユーザと通信することができます。

ポリシー アクション	説明	影響
外部ファイル転送（External File Transfer）	組織のユーザと組織外のユーザ間の IM セッションでのファイル転送を制御します。	[無効（Disabled）]：組織の止します。 これには、1 人以ンが含まれます。
内部ファイル転送（Internal File Transfer）	組織内のユーザ間の IM セッションでのファイル転送を制御します。	[無効（Disabled）]：すべて [有効（Enabled）]：組織内きます。
外部 IM（External IM）	組織内のユーザと組織外のユーザ間の IM セッションを制御します。	[無効（Disabled）]：組織内止します。 これによって、ビスがすべて停止します。
外部 VoIP（External VoIP）	組織内のユーザと組織外のユーザ間の IM セッションでの VoIP 通信を制御します。	[無効（Disabled）]：組織内すべての VoIP 通信を停止やファイル転送のような他

ポリシー アクション	説明	影響
内部 VoIP（Internal VoIP）	組織内のユーザ間の IM セッションでの VoIP 通信を制御します。	[無効（Disabled）]：組織 信を停止します。 ただし ような他のサービスは使 [有効（Enabled）]：組織 用できます。
外部ビデオ（External Video）	組織内のユーザと組織外のユーザ間の IM セッションでのビデオ サービスを制御します。	[無効（Disabled）]：組織 すべてのビデオ サービス ションやファイル転送の
内部ビデオ（Internal Video）	組織内のユーザ間の IM セッションでのビデオ サービスを制御します。	[無効（Disabled）]：組織 サービスを停止します。 転送のような他のサービ [有効（Enabled）]：組織 使用できます。
ローカル アーカイブ（Local Archive）	ユーザがローカルで IM テキスト メッセージをアーカイブする機能を制御します。	
外部デスクトップ共有（External Desktop Share）	組織内のユーザが自身のデスクトップを組織外のユーザと共有する機能を制御します。	[無効（Disabled）]：組織 外のユーザと共有できな [有効（Enabled）]：ユー ザと共有できます。
内部デスクトップ共有（Internal Desktop share）	組織内のユーザが自身のデスクトップを組織内の他のユーザと共有する機能を制御します。	[無効（Disabled）]：組織 ザと共有できません。 [有効（Enabled）]：ユー できます。
IM のエンドツーエンドの暗号化のサポート（Support End-to-End Encryption For IM）	IM セッションのエンドツーエンドの暗号化のサポートを指定します。	[有効（Enabled）]：IM セ す。 エンドツーエンドの暗号 れません。
符号化されていない IM のサポート（Support NO Encoding For IM）	エンドツーエンドの暗号化に対応しているアプリケーションが、エンドツーエンドの暗号化に対応していないアプリケーションやエンドツーエンドの暗号化をサポートしていないサードパーティ製アプリケーションとの IM セッションを開始できるかを制御します。	[無効（Disabled）]：エン ンがエンドツーエンドの サードパーティ製アプリ ます。 [有効（Enabled）]：ネゴ する最高のレベルになり

ポリシー アクション	説明	影響
内部IM（ホワイト リストに記載されたドメインを含む）（Internal IM（including White Listed domains））	組織内のユーザとホワイト リスト上の特定ドメイン間の IM 通信を制御します。	[無効（Disabled）]：組織内の の IM ユーザになれないよう IM を開始できます。 また、 る他のサービスは無効になり
アップロード ウィジェット（Upload Widgets）		
ユーザによるプロファイルの編集を許可（Allow user to edit profile）	ユーザの自身のプロファイル情報の編集機能を制御します。	[無効（Disabled）]：ユーザは このポリシー アクションは、 イルの設定（Profile Settings）
ユーザによる表示プロファイル設定の編集を許可（Allow user to edit the view profile setting）	ユーザのグループが、ユーザ プロファイルの表示設定の変更を制限できる機能を制御します。	[無効（Disabled）]：ユーザは ません。 このポリシーアクションは、 **イルの設定（Profile Settings）** **の変更を許可（Allow users t** クスに影響します。 [ユーザによるプロファイル表 profile view settings）]チェッ ん。
内部スクリーン キャプチャ（Internal Screen Capture）	組織内のユーザのスクリーン キャプチャ送信機能を制御します。	[無効（Disabled）]：組織内の きないようにします。
外部スクリーン キャプチャ（External Screen Capture）	ユーザが組織外のユーザにスクリーン キャプチャを送信する機能を制御します。	[無効（Disabled）]：組織内の きないようにします。
内部ブロードキャスト メッセージの送信（Send Internal Broadcast Message）	ユーザが組織内のユーザにブロードキャスト メッセージを送信する機能を制御します。	[無効（Disabled）]：組織内の 送信できないようにします。
外部ブロードキャスト メッセージの送信（Send External Broadcast Message）	ユーザが組織外のユーザにブロードキャスト メッセージを送信する機能を制御します。	[無効（Disabled）]：組織内の 送信できないようにします。

ポリシー アクション	説明	影響
ユーザによるディレクトリ グループへのブロードキャストの送信を許可（Allow user to send broadcast to a directory group）	ユーザが組織内のディレクトリ グループにブロードキャスト メッセージを送信する機能を制御します。	[無効（Disabled）]：組織内 ドキャスト メッセージを
HD ビデオ（HD Video）	外部ビデオ ポリシーまたは内部ビデオ ポリシーが有効になっている場合に、コンピュータ コールに対するコンピュータ上の HD ビデオ機能を制御します。	[無効（Disabled）]：コン ビデオを停止させます。



第 4 章

クラスタの設定

ビジュアル ボイスメールの設定

ステップ 1 ビジュアル ボイスメールを設定するには、**[設定（Configuration）] タブ** > **[Unified Communications]** を選択します。
[Unified Communications]ウィンドウが開きます。

ステップ 2 [ボイスメール（Voicemail）]を選択して [CUCI 用のビジュアル ボイスメールのデフォルト設定（Default settings for Visual Voicemail for CUCI）]を選択します。

Unity Connection のお客様は、[ボイスメール サーバ（Voicemail Server）] フィールドまたは [メールストア サーバ（Mailstore Server）] フィールドに Unity Connection サーバの IP アドレスもしくは DNS 名を入力する必要があります。 その他のすべての設定はデフォルトのままにしておくことを推奨します。

ステップ 3 ビジュアル ボイスメールを有効にするには、[ビジュアル ボイスメールの有効化（Enable Visual Voicemail）] を選択します。

ステップ 4 ビジュアル ボイスメールの設定を手動で入力する場合は、[ユーザによる手動設定の入力を許可（Allow user to enter manual settings）]を選択します。

ステップ 5 次の情報を入力します。

- **ボイスメール サーバ**：Webex アプリケーションがボイスメールを取得する際に通信する必要のあるビジュアル ボイスメール サーバ名。
- [ボイスメールプロトコル（Voicemail Protocol）]：ビジュアル ボイスメール サーバとの通信に使用するプロトコル。 [HTTP] または [HTTPS] を選択できます。
- [ボイスメールポート（Voicemail Port）]：ビジュアル ボイスメール サーバに関連付けられたポート。

次のメールストア パラメータのオプションはサポートされていません。 Webex 管理ツールには値が必要です。メールストア サーバのフィールドには `10.0.0.0` を入力し、残りのフィールドにはデフォルトの値を使用します。

- [メールストアサーバ（Mailstore Server）]：メールストア サーバ名。
- [メールストアプロトコル（Mailstore Protocol）]：メールストア サーバが使用するプロトコル。 [TLS] または [プレーン（Plain）] を選択できます。
- [メールストアポート（Mailstore Port）]：メールストア サーバに関連付けられたポート。
- [IMAPアイドル期限時間（IMAP IDLE Expire Time）]：サーバのボイスメールの確認が自動的に停止する期限までの時間（分単位）。
- [メールストアの受信トレイ フォルダ名（Mailstore Inbox Folder Name）]：メールストア サーバで設定されている受信トレイ フォルダの名前。
- [メールストアのごみ箱フォルダ名（MailstoreTrash Folder Name）]：メールストア サーバで設定されているごみ箱フォルダ（通常は削除済み項目フォルダ）の名前。

ステップ 6 **保存**を選択します。

Cisco Unified Communications Manager の統合の設定

ステップ 1 **[設定（Configuration）] タブ > [追加のサービス（Additional Services）] > [Unified Communications]** を選択します。

ステップ 2 [クラスタ（Clusters）]タブを選択し、[追加（Add）]を選択します。

ステップ 3 [Messenger サービス クライアントと Cisco UC Manager の統合の有効化（Enable Cisco UC Manager integration with Messenger Service Client）]を選択します。

ステップ 4 [ユーザによる手動設定の入力を許可（Allow user to enter manual settings）]を選択すると、ユーザは基本モードのプライマリ サーバの値か、または拡張モードの TFTP/CTI/CCMCIP サーバの値を変更できます。

（注） このオプションを有効にすると、ユーザが入力した設定で Webex 組織に対して指定したデフォルトまたはグローバルの Cisco Unified Communications Manager の設定が上書きされます。

ステップ 5 [Cisco Unified Communications Manager サーバの設定（Cisco Unified Communications Manager Server Settings）] で、次のように選択します。

- [基本的なサーバ設定（BasicServer Settings）]：Cisco Unified Communications Manager サーバの基本的な設定を入力します。
- [詳細なサーバ設定（AdvancedServer Settings）]：Cisco Unified Communications Manager サーバの詳細設定を入力します。

（注） サーバ設定のオプションは、基本か詳細かによって変わります。

ステップ 6 [基本的なサーバ設定（Basic Server Settings）]に次の値を入力します。

- [プライマリサーバ（Primary Server）]：プライマリの Cisco Unified Communications Manager サーバの IP アドレスを入力します。 このサーバは、TFTP、CTI、CCMCIP で設定されます。
- [バックアップサーバ（Backup Server）]：バックアップの Cisco Unified Communications Manager サーバの IP アドレスを入力します。 このサーバは、TFTP、CTI、CCMCIP で設定され、プライマリの Unified Communications Manager サーバに障害が発生した場合のフェールオーバー サポートを提供します。

ステップ 7 [詳細なサーバ設定（AdvancedServer Settings）] を選択した場合は、TFTP（Trivial File Transfer Protocol）サーバ、CTI（コンピュータ テレフォニー インテグレーション）サーバ、CCMCIP（Cisco Unified Communications Manager IP フォン）サーバの各設定を指定します。

ステップ 8 次のサーバのそれぞれに、IP アドレスを入力します。

（注） TFTP サーバには最大 2 つのバックアップ サーバを、CTI サーバと CCMCIP サーバにはそれぞれ 1 つのバックアップ サーバを指定できます。 各バックアップ サーバに適切な IP アドレスを入力します。

- **[TFTP Server]**
- **[CTI Server]**
- **CCMCIP サーバ（CCMCIP Server）**：これは、Cisco Unified Communications Manager（UDS）サーバのアドレスです。

リストされたサーバはユーザのホーム クラスタ内に存在する必要があります。

ステップ 9 [ボイスメールのパイロット番号（Voicemail Pilot Number）]ボックスに、Cisco Unified Communications サーバのボイス メッセージ サービスの番号を入力します。

通常は、組織の管理者が Webex の組織全体のデフォルトのボイス メッセージ番号を入力します。 ただし、[ユーザによる手動設定の入力を許可（Allow user to enter manual settings）]チェックボクスを選択すると、クラスタのユーザがこのデフォルトのボイス メッセージ番号を上書きできるようにすることができます。

ステップ 10 [ボイスメール（Voicemail）]を選択します。

ステップ 11 [ビジュアル ボイスメールの有効化（Enable Visual Voicemail）]を選択します。

ここで入力したビジュアル ボイスメールの設定は、このクラスタに属しているユーザのみに適用されます。

ステップ 12 [クラスタ（Clusters）]タブで、[このクラスタに固有のボイスメール サーバ（Specific voicemail server for this cluster）]を選択してボイスメール サーバを指定します。このサーバは、組織全体に提供されるボイスメール サーバの設定とは異なります。

ステップ 13 [ユーザによる手動設定の入力を許可（Allow user to enter manual settings）]を選択して、ユーザがこのクラスタのビジュアル ボイスメール設定を手動で入力できるようにします。

ステップ 14 次の情報を入力します。

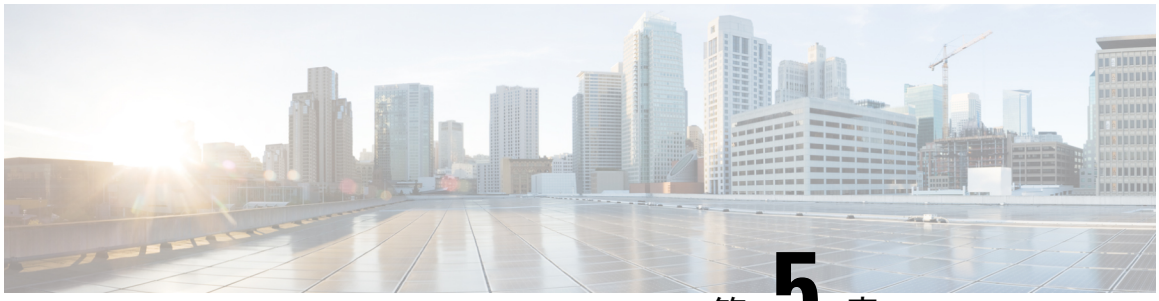
[ボイスメール サーバ（Voicemail Server）]	ボイスメール サーバの IP アドレスまたは FQDN を入力します。

[ボイスメール プロトコル（Voicemail Protocol）]	[HTTP] または [HTTPS] を選択します。
[ボイスメール ポート（Voicemail Port）]	ポート番号を入力します。

メールストア サーバ情報はサポートされていませんが、Webex 管理ツールでは、このフィールドに値のあることが想定されているため、`10.0.0.0` と入力します。 メールストアの [プロトコル（Protocol）] フィールド、[ポート（Port）] フィールド、[IMAP のアイドル期限時間（IMAP IDLE Expire Time）] フィールドはサポートされていません。これらのフィールドからデフォルト値を削除しないでください。

[メールストア受信トレイ フォルダ名（Mailstore Inbox Folder Name）]	メールストア サーバで設定された受信トレイ フォルダの名前。
[メールストアのごみ箱フォルダ名（Mailstore Trash Folder Name）]	メールストア サーバで設定されたごみ箱フォルダまたは削除済み項目フォルダの名前。

ステップ 15 [Save]を選択します。



第 5 章

クラウド展開のユーザの作成

ユーザ ワークフローの作成

Webex 管理ツールでは、さまざまな方法で組織のユーザを作成できます。

手順

	コマンドまたはアクション	目的
ステップ 1	次のいずれかの方法を使用して、Webex 管理ツールにユーザを作成します。 • Webex 管理ツールを使用してユーザを個別に追加できます。 新しいユーザの作成 （16 ページ） • ユーザが Webex アカウントを自己登録するための電子メールによる案内を生成できます。 ユーザ プロビジョニング情報 （17 ページ） • ユーザ情報を使用して CSV ファイルを作成し、インポートします。 CSV ファイルの作成とインポート （18 ページ）	
ステップ 2	ユーザをポリシー グループに割り当てます。 ポリシーへのユーザの割り当て （21 ページ）	

新しいユーザの作成

ステップ 1 新しいユーザや管理者を作成するには、**[ユーザ（User）]** > **[追加（Add）]** を選択します。

ステップ 2 各フィールドに情報を入力します。 デフォルトの [ロール（Role）] は [ユーザ（管理者以外）（User (non-administrator)）] です。

（注） [勤務先電子メール（Business Email）] が [ユーザ名（Username）] になります。 [ユーザ名（Username）] は編集できません。

ステップ 3 （オプション）ユーザにポリシー グループを割り当てるには、[ポリシー グループの割り当て（Policy Group Assignment）]タブを選択します。

ステップ 4 Webex Messenger の組織に対して IM のアーカイブが有効になっている場合は、**[ユーザーの追加（Add User）]** ダイアログボックスに **[IM のアーカイブ（Archive IMs）]** チェックボックスが表示されます。 アーカイブを目的に、このユーザの IM をログに記録するには、[IM のアーカイブ（Archive IMs）]チェックボックスをオンにします。

ステップ 5 エンドポイントを変更するには、ドロップダウン リストから別のエンドポイントを選択します。 [デフォルト（Default）]を選択すると、[IM のアーカイブ（IM Archiving）]画面でデフォルトのエンドポイントとして事前に設定したエンドポイントがユーザに割り当てられます。

ステップ 6 このユーザをアップグレード サイトに割り当てるには、[アップグレード サイト（Upgrade Site）] ドロップダウン リストからサイトを選択します。

ステップ 7 Webex Messenger の組織が Cisco Unified Communications で有効になっている場合は、[ユーザの追加（Add User）] ダイアログ ボックスに [Unified Communications] タブが表示されます。 Cisco Unified Communications で使用可能な設定を表示するには、[Unified Communications]タブを選択します。

ステップ 8 [クラスタ（Cluster）]で、このユーザに追加する適切な Cisco Unified Communications クラスタを選択します。

ステップ 9 Webex Messenger の組織が Webex Meeting Center の統合で有効になっている場合は、[ユーザの追加（Add User）] ダイアログボックスが表示されます。 組織管理者ロールをユーザに割り当てるには、[組織管理者（Organization Administrator）]チェックボックスをオンにします。

（注）
- **[会議（Meetings）]** ページの **[新しいユーザーの作成時に会議アカウントを自動的に有効にする（Automatically enable Meeting account when creating a new user）]** を有効にしている場合は、**[会議アカウント（Meeting Account）]** チェックボックスがデフォルトで選択されます。 このような場合、[会議アカウント（Meeting Account）] のチェックボックスをクリアすることはできません。
- **[会議アカウント（Meeting Account）]**チェックボックスを選択すると、このユーザに対応する Webex Meeting Center アカウントが作成されます。

ステップ 10 [保存（Save）]を選択します。

Webex Messenger 管理ツールのウェルカム電子メール テンプレートに基づいて新しいユーザにウェルカム電子メールが送信されます。

ステップ 11 上記のステップを繰り返し、新しいユーザの追加を続行します。

ユーザ プロビジョニング情報

ユーザのプロビジョニングには、登録などのユーザプロビジョニング情報の指定や、ユーザのプロファイルを作成するときに必要なフィールドの指定が含まれています。 ここで行う設定は、Webex メッセンジャーの組織にユーザをプロビジョニングするタイミングに影響します。たとえば、特定のフィールドをここで必須に指定すると、ユーザがユーザプロファイルを作成する際に、それらのフィールドへの入力が強制されます。

Webex メッセンジャー お客様は、SAML またはディレクトリ統合が有効になっていない場合は、セルフ登録を有効にすることができます。 このような場合、組織管理者は登録 URL を指定する必要はありません。 登録が有効になっていない場合は、お客様がカスタム Web ページを指定できます。 お客様のドメインに一致する電子メール アドレスでユーザが登録しようとすると、カスタム Web ページにリダイレクトされます。 お客様はこの Web ページを使用して、新しい Webex メッセンジャー アカウントの作成に必要な内部プロセスに関する情報を表示できます。

次に例を示します。

```
Cisco Webex Messenger サービスを取得するには、ithelpdesk@mycompany.com 宛に電子メールをお送りいただくか、または +1 800 555 5555 までお電話でご連絡ください。
```

ユーザ プロビジョニング情報の入力

ステップ 1 ユーザ プロビジョニング情報を入力するには、[設定（Configuration）]タブで、**[システム設定（System Settings）]** > **[ユーザ プロビジョニング（User Provisioning）]** を選択します。

ステップ 2 ユーザによるCisco Jabberアプリケーションでのアカウントのセルフ登録を有効にするには、**登録ページを使用したユーザのセルフ**Webex**登録の有効化を選択します**。

セルフ登録ページの URL は www.webex.com/go/wc です。通常、この URL は Webex メッセンジャー 組織管理者から提供されます。

（注） Webex 登録ページを使用したユーザのセルフ登録の有効を選択しなかった場合は、[カスタム登録 URL（Custom Registration URL）] フィールドと [カスタム メッセージ（Custom Message）] ボックスが表示されます。 この場合は、カスタム ユーザ登録ページの URL を入力する必要があります。

ステップ 3 [カスタム登録 URL（Custom Registration URL）]フィールドに、カスタマイズされたセルフ登録ページの URL を入力します。

カスタム URL を入力しなかった場合は、セルフ登録ページ（デフォルト）の URL である www.webex.com/go/wc が表示されます。

ステップ 4 [カスタム メッセージ（Custom Message）]ボックスにカスタム セルフ登録ページの説明を入力します。

ステップ 5 セルフ登録ページを使用してユーザが登録するたびに、電子メールで組織管理者に通知するには、[ユーザが Cisco Webex 登録ページを使用してセルフ登録したときに通知を管理者に送信する（Send notification to Administrator when users self register using Cisco Webex registration page）]を選択します。

ステップ 6 [ユーザ プロファイルの必須フィールドの設定（Set mandatory fields for user profile）]で、ユーザのプロファイルを作成または表示するたびに強制的に表示するフィールドを選択します。 これらのフィールドは、次を実行する際に常に表示されます。

- 新規ユーザの作成
- 既存のユーザ プロファイルの編集
- CSV ファイルからのユーザのインポート

ステップ 7 **保存**を選択します。

CSV ファイルの作成とインポート

カンマ区切り値（CSV）ファイルから、多数のユーザを Webex メッセンジャー の組織に簡単にインポートできます。 同様に、CSVファイルにユーザをエクスポートすることもできます。インポートは、多数のユーザを組織に簡単に追加して、各ユーザを手動で追加する手間を省く上で、有効な方法です。

インポートが完了すると、インポートを開始した組織管理者にはインポートのステータスを通知する電子メールが届きます。 この電子メールには、インポートが成功、失敗、または終了したかが記載されています。

CSV ファイルがインポートされると、[ユーザ（User）]タブにユーザが表示されます。

CSV フィールド

注：CSV のインポート プロセスを使用して組織管理者とユーザ管理者を作成することはできません。

Webex にユーザをインポートする前に、次のフィールド（順不同）を CSV ファイルに含める必要があります。 一部のフィールドは必須項目で、情報を入力する必要があります。また、オプションのフィールドもあります。

注：フィールドに情報を入力しない場合は、文字「-」を入力します。この文字は空のフィールドとしてデータベースにインポートされます。 これはオプション フィールドに対してのみ行えます。「-」を必須フィールドに入力すると、インポート時にエラーが報告されます。 N/A 値は使用しないでください。

フィールド名	説明
employeeID	必須（*SSO* の有効時のみ）ユーザの ID を入力します。

フィールド名	説明
displayName	オプション ユーザの表示名を入力します。
firstName	必須 ユーザの名を入力します。
lastName	必須 ユーザの姓を入力します。
email	必須 ユーザの電子メール アドレスを入力します。
userName	必須 ユーザのユーザ名を user@email.com の形式で入力しま
jobTitle	オプション ユーザの役職名または担当名を入力します。
address1	オプション ユーザの住所の最初の行を入力します。 組織管
address2	オプション ユーザの住所の 2 行目を入力します。 組織管理
city	オプション ユーザの居住地の市町村を入力します。 組織管
state	オプション ユーザの居住地の都道府県を入力します。 組織 す。
zipCode	オプション ユーザの郵便番号を入力します。 組織管理者に
ISOcountry	オプション ユーザが居住する国の 2 文字の国コード（IN、 http://www.iso.org/iso/country_codes/iso_3166_code_lists/countr このフィールドをユーザに必須となるように設定できます。
phoneBusinessISOCountry	オプション ユーザの勤務先電話番号の国コード（IN、US、 必須となるように設定できます。
phoneBusinessNumber	オプション ユーザの勤務先電話番号を入力します。 組織管
phoneMobileISOCountry	オプション ユーザの携帯電話番号の国コード（IN、US、C 須となるように設定できます。
phoneMobileNumber	オプション ユーザの携帯電話番号を入力します。 組織管理
ファクス	オプション ユーザのファクス番号を入力します。
policyGroupName	オプション ユーザが属しているデフォルトのポリシー グル
userProfilePhotoURL	オプション ユーザのプロフィール写真にアクセスできる U
activeConnect	オプション ユーザーのステータスが **アクティブ** かどうかを **いいえ** を入力して **非アクティブ** ステータスを示します。
center	オプション Cisco Jabber アプリケーション ユーザのセンター す。 センターは 1 つのみ指定できます。

フィールド名	説明
storageAllocated	オプション ユーザに割り当てられたストレージをメガバイト単 数値を使用する必要があります。
CUCMClusterName	オプション ユーザが属している Cisco Unified Communications
businessUnit	オプション ユーザの部門または部署を入力します。 組織管理
IMLoggingEnable	オプション IM ロギングがこのユーザに対して有効にされてい すには **[はい（True）]** を、**[無効（disabled）]** な状況であるこ
endpointName	オプション IM の記録用に設定されたエンドポイントの名前を
autoUpgradeSiteName	オプション アップグレード サイト名を入力します。

（注） タブ区切りまたはカンマ区切りの CSV ファイルを使用できます。 CSV ファイルが、UTF-8 形式または UTF16-LE 形式で符号化されていることを確認します。

エンコード形式としての UTF-8 の選択

ステップ 1 Microsoft Excel で [ファイル（File）]> [名前を付けて保存（Save As）] を選択します。

ステップ 2 [名前を付けて保存（Save As）]ダイアログボックスで、[ツールと Web オプション（Tools and Web Options）] を選択します。

ステップ 3 [Web オプション（Web Options）]ダイアログボックスで、[エンコーディング（Encoding）]タブを選択します。

ステップ 4 [このドキュメントの保存形式（Save this document as）]リストで、[UTF-8]を選択します。

ステップ 5 [OK]をクリックして [名前を付けて保存（Save As）]ダイアログボックスに戻ります。

ステップ 6 [ファイルの種類（Save as type）]リストから、[CSV（カンマ区切り）（*.csv）（CSV (Comma delimited) (*.csv)）]を選択します。

ステップ 7 [ファイル名（File Name）]フィールドに、CSV ファイルの名前を入力し、[保存（Save）]を選択します。

ユーザのインポートとエクスポート

ステップ 1 CSV ファイルからユーザをインポートするには、Webex メッセンジャー 管理ツールで **[ユーザ（User）]** タブ > **[その他の操作（More Actions）]** > **[インポート/エクスポート（Import/Export）]** を選択します。

ステップ 2 [参照（Browse）]を選択し、インポートするユーザのリストが含まれている CSV ファイルを選択します。

ステップ 3 [インポート（Import）]を選択し、インポート プロセスを開始します。

ステップ 4 ユーザーをエクスポートするには、**[ユーザーのインポート/エクスポート（Import/Export User）]** ダイアログボックスの **[エクスポート（Export）]** を選択します。

進捗メッセージにエクスポート プロセスの進捗が表示されます。

ステップ 5 エクスポートされたユーザが含まれている CSV ファイルを表示するには、エクスポート メッセージのタイム スタンプを選択します。
確認のプロンプトが表示されます。 `Last export: 2009-06-24 09:02:01` のようなメッセージになります。

ステップ 6 [開く（Open）]を選択し、Messengerの組織のユーザが含まれているCSVファイルを表示します。 または、[保存（Save）]を選択し CSV ファイルをローカル コンピュータに保存します。

ポリシーへのユーザの割り当て

ステップ 1 ポリシー グループにユーザを割り当てるには、[ユーザ（User）]タブを選択します。

ステップ 2 新しいユーザにポリシー グループを割り当てる場合は、まず、[追加（Add）]を選択して新しいユーザを作成します。

ステップ 3 既存のユーザにポリシー グループを割り当てるには、そのユーザを検索します。

ステップ 4 検索結果で、該当するユーザの名前をダブルクリックして [ユーザの編集（Edit User）]ダイアログ ボックスを開きます。

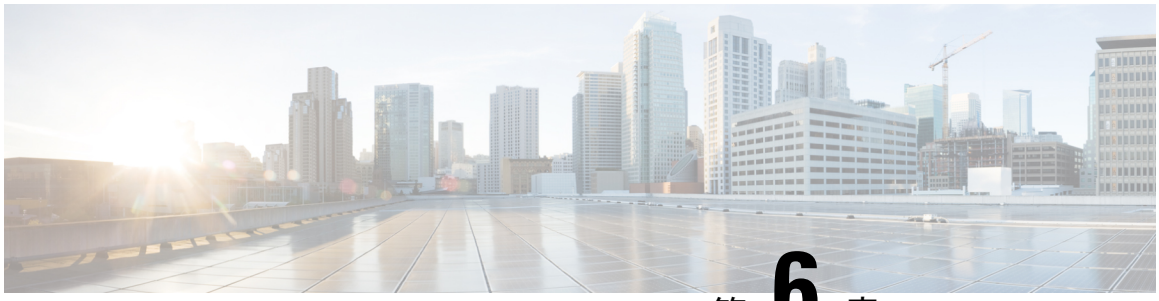
ステップ 5 [ポリシー グループの割り当て（Policy Group Assignment）]タブを選択して [ポリシー グループの割り当て（Policy Group Assignment）]ダイアログ ボックスを開きます。

ステップ 6 [検索（Search）]フィールドで、検索してこのユーザに割り当てるポリシー グループ名を 1 文字以上入力します。

ステップ 7 [検索（Search）]を選択します。

ステップ 8 [検索結果（Search Result）]ウィンドウで、該当するポリシー グループを選択し、[割り当て（Assign）]を選択してこのユーザにポリシーを割り当てます。

ステップ 9 [保存（Save）]を選択してポリシー グループの割り当てを保存し、[ユーザ（User）]タブに戻ります。



第 6 章

Unified Communications Manager のユーザの作成

同期の有効化

ディレクトリ サーバ内の連絡先データが Cisco Unified Communications Manager に複製されていることを確認するには、ディレクトリ サーバと同期する必要があります。 ディレクトリ サーバと同期する前に、同期を有効にする必要があります。

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 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 3 [LDAP システム情報（LDAP System Information）]セクションに移動します。

ステップ 4 [LDAP サーバからの同期を有効にする（Enable Synchronizing from LDAP Server）]を選択します。

ステップ 5 [LDAP サーバ タイプ（LDAP Server Type）]ドロップダウン リストから、データの同期元となるディレクトリ サーバのタイプを選択します。

次のタスク

ユーザ ID の LDAP 属性を指定します。

ユーザ ID の LDAP 属性の指定

ユーザをディレクトリ ソースから Cisco Unified Communications Manager に同期する場合は、ディレクトリ内の属性からユーザ ID を生成できます。 ユーザ ID を保持するデフォルトの属性は、sAMAccountName です。

ステップ 1 [LDAP システムの設定（LDAP System Configuration）]ウィンドウで[ユーザ ID 用 LDAP 属性（LDAP Attribute for User ID）]ドロップダウン リストを探します。

ステップ 2 必要に応じて、ユーザ ID の属性を指定し、[保存（Save）]を選択します。

重要 ユーザ ID の属性が sAMAccountName 以外の場合で、Cisco Unified Communications Manager IM and Presence Service でデフォルトの IM アドレス スキーム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 に対する LDAP 属性の指定

Cisco Unified Communications Manager リリース 9.0(1) 以降では、ディレクトリ内の属性からディレクトリ URI を生成できます。

始める前に

同期の有効化。

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 適切な LDAP ディレクトリを選択するか、[新規追加（Add New）]を選択して LDAP ディレクトリを追加します。

ステップ 3 [同期対象の標準ユーザ フィールド（Standard User Fields To Be Synchronized）]セクションを探します。

ステップ 4 [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 5 **保存**を選択します。

同期の実行

ディレクトリ サーバを追加し、必要なパラメータを指定した後、Cisco Unified Communications Manager をディレクトリ サーバと同期できます。

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 [新規追加（Add New）] 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 [LDAP ディレクトリ（LDAP Directory）] ウィンドウで必要な詳細情報を指定します。

指定可能な値と形式の詳細については、『Cisco Unified Communications Manager Administration Guide』を参照してください。

ステップ 4 情報が定期的に同期されることを保証するには、LDAP ディレクトリ同期スケジュールを作成します。

ステップ 5 [保存（Save）] を選択します。

ステップ 6 [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 がプレゼンス サーバ データベースにユーザ データを同期します。

ロールとグループの割り当て

どのタイプの展開でも、ユーザを [標準 CCM エンドユーザ（Standard CCM End Users）]グループに割り当てます。

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）]** の順に選択します。
[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 一覧から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。

ステップ 4 [権限情報（Permission Information）]セクションを探します。

ステップ 5 [アクセス コントロール グループに追加（Add to Access Control Group）]を選択します。
[アクセス コントロール グループの検索と一覧表示（Find and List Access Control Groups）]ダイアログボックスが開きます。

ステップ 6 ユーザのアクセス コントロール グループを選択します。

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。

- **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。

ステップ 7 **[選択項目の追加（Add Selected）]** を選択します。
[アクセス コントロール グループの検索と一覧表示（Find and List Access Control Groups）] ウィンドウが終了します。

ステップ 8 **[エンドユーザーの設定（End User Configuration）]** ウィンドウで **[保存（Save）]** を選択します。

認証オプション

クライアント内の SAML SSO の有効化

始める前に

- 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。
- Webex メッセンジャー のサービスの SSO を有効にすると、Cisco Unified Communications Manager と Cisco Unity Connection をサポートします。

  このサービス上での SAML SSO の有効化方法については、『*Webex* メッセンジャー *Administrator's Guide*』の「Single Sign-On」を参照してください。

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。これを行わない場合、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、「*Remote Access* 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。

Webex Teams を使用して 1 つの資格情報セットを使用して Webex Teams をログインする方法の詳細については、『*Cisco SSO Communications Deployment Guide*』を参照してください。

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 ユーザー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 ユーザー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。

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。

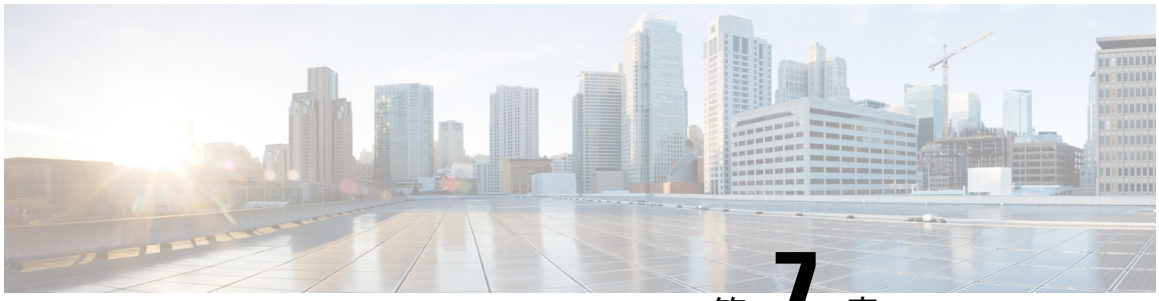
ステップ 2 **[システム（System）]** > **[LDAP]** > **[LDAP 認証（LDAP Authentication）]** を選択します。

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**を選択します。



第 7 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。

デスクフォン制御タスクフローの設定

手順

	コマンドまたはアクション	目的
ステップ 1	CTI 用のデバイスの有効化 （30 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 2	デスクフォン ビデオの設定 （30 ページ）.	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。
ステップ 3	ビデオ レート アダプテーションの有効化 （32 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。
ステップ 4	ユーザの関連付けに関する設定 （33 ページ）	ユーザとデバイスを関連付け、ユーザをアクセス コントロール グループに割り当てます。

	コマンドまたはアクション	目的
ステップ 5	デバイスのリセット （35 ページ）	ユーザの関連付けを設定した後にデバイスをリセットする必要があります。

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。

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（Save）]** 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。

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。

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。

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]** ドロップダウンメニューから **[有効（Enabled）]** を選択します。

ステップ 7 **保存**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。

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。

[電話機の設定（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]** ドロップダウンメニューから **[有効（Enabled）]** を選択します。

ステップ 7 **保存**を選択します。

ユーザの関連付けに関する設定

ユーザをデバイスに関連付けると、ユーザにデバイスがプロビジョニングされます。

始める前に

Cisco Jabber デバイスを作成および設定します。

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 [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、ユーザの適切なサービス プロファイルを選択します。

ステップ 7 [デバイス情報（Device Information）]セクションを探します。

ステップ 8 [デバイスの割り当て（Device Associations）]を選択します。

[ユーザ デバイス割り当て（User Device Association）]ウィンドウが開きます。

ステップ 9 ユーザを割り当てるデバイスを選択します。 Jabber では、割り当てるソフトフォンをデバイスの種類ごとに 1 つだけサポートしています。 たとえば、ユーザ 1 人 に対して、TCT、BOT、CSF、TAB デバイスを 1 つだけ割り当てることができます。

ステップ 10 [選択/変更の保存（Save Selected/Changes）]を選択します。

ステップ 11 **[ユーザ管理（User Management）] > [エンド ユーザ（End User）]** の順に選択し、[ユーザの検索と一覧表示（Find and List Users）]ウィンドウに戻ります。

ステップ 12 一覧から同じユーザを探し、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 13 **[権限情報（Permissions Information）]** セクションを探します。

ステップ 14 [アクセス コントロール グループに追加（Add to Access Control Group）]を選択します。

[アクセス コントロール グループの検索と一覧表示（Find and List Access Control Groups）]ダイアログボックスが開きます。

ステップ 15 ユーザを割り当てるアクセス コントロール グループを選択します。

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。

- **Standard CCM End Users**
- **[標準CTIを有効にする（Standard CTI Enabled）]**

メモ 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。

ステップ 16 **[選択項目の追加（Add Selected）]** を選択します。

[アクセス コントロール グループの検索と一覧表示（Find and List Access Control Groups）] ウィンドウが終了します。

ステップ 17 **[エンドユーザーの設定（End User Configuration）]** ウィンドウで **[保存（Save）]** を選択します。

デバイスのリセット

ユーザを作成し、デバイスに関連付けた後、それらのデバイスをリセットする必要があります。

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）]を選択してデバイスの一覧を取得します。

ステップ 4 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。

ステップ 5 [割り当て情報（Association Information）]セクションを探します。

ステップ 6 対象の電話番号設定を選択します。

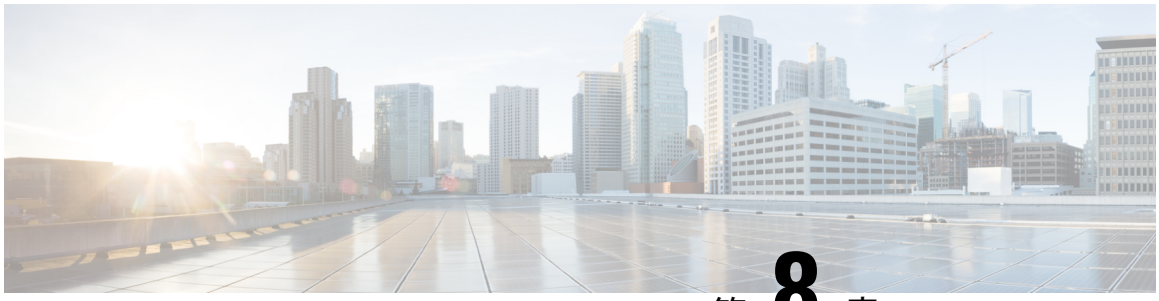
[ディレクトリ番号の設定（Directory Number Configuration）]ウィンドウが開きます。

ステップ 7 [リセット（Reset）]を選択します。

[デバイス リセット（Device Reset）]ダイアログボックスが開きます。

ステップ 8 [リセット（Reset）]を選択します。

ステップ 9 [閉じる（Close）]を選択して、[デバイス リセット（Device Reset）]ダイアログボックスを閉じます。



第 8 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 （38 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 （42 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 （42 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 （44 ページ）.	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 （45 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。

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、Mac 版 Cisco Jabber または Windows 版 Cisco Jabber 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。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。
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。

ステップ 1 **[電話機の設定（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 [設定の適用（Apply Config）]を選択します。

ステップ 9 **保存**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。

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。
[電話機の設定（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**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。

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**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。

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**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。

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、Mac 版 Cisco Jabber または Windows 版 Cisco Jabber 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。

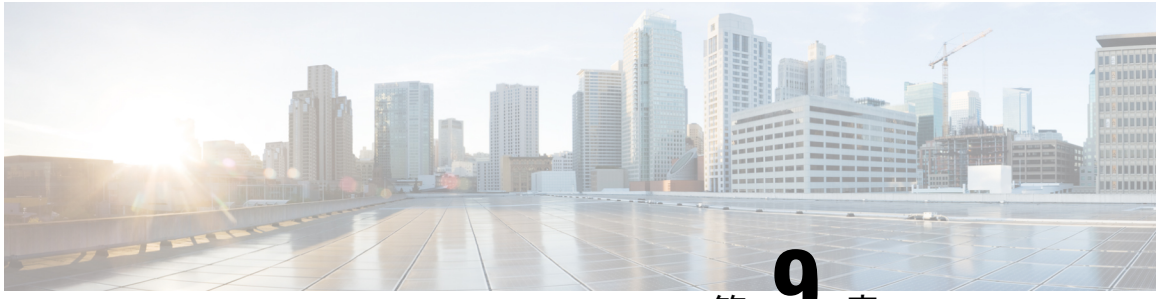
ステップ 9 [キーサイズ（ビット）（Key Size (Bits)）] で、証明書に適したキー サイズを選択します。キー サイズは、CAPF 登録プロセス中にクライアントが生成する公開キーと秘密キーのビット長を示します。

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 9 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 （49 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 （50 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 （51 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 Mac 版 Cisco Jabber または Windows 版 Cisco Jabber 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。

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**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。

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。

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。

[電話機の設定（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**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。

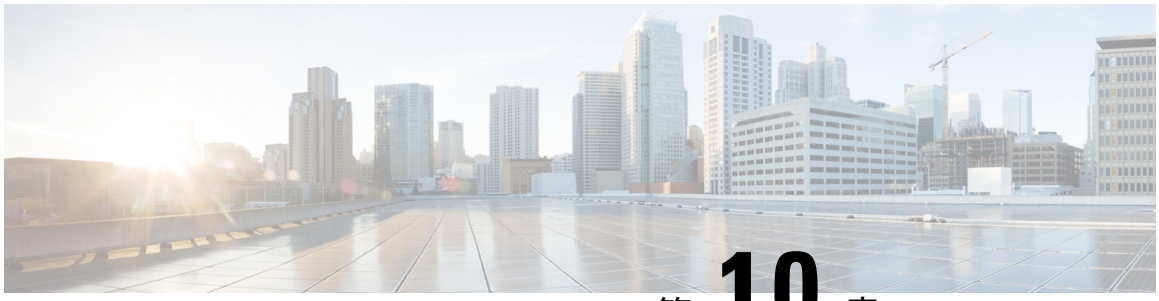
1. 手順を繰り返し、CTI リモートデバイスの [電話機の設定（Phone Configuration）]ウィンドウを開きます。
2. [**関連付けられたリモート接続先（Associated Remote Destinations**）] セクションを探します。
3. リモート接続先が利用可能であることを確認します。
4. [設定の適用（Apply Config）]を選択します。

（注） **[電話機の設定（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 10 章

Remote Access のためのサービス検出の設定

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 要件

Remote Access 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。

証明書の要件

Remote Access 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

ステップ 1 コマンド プロンプトを開きます。

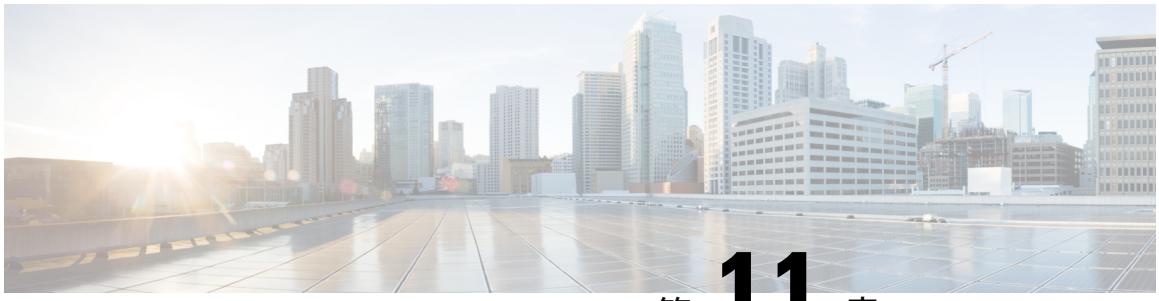
ステップ 2 **nslookup** と入力します。
デフォルトの DNS サーバおよびアドレスが表示されます。 これが想定された DNS サーバであることを確認してください。

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：`_collab-edge.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。
- 「`_collab-edge.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。



第 11 章

証明書の検証設定

クラウド展開の証明書検証

Webex メッセンジャーおよびWebex Meetingsセンターは、クライアントにデフォルトで次の証明書を提示します。

- CAS
- WAPI

（注） Webex は、証明書はパブリックな認証局（CA）によって署名されます。 Cisco Jabber はこれらの証明書を検証し、クラウドベース サービスとのセキュアな接続を確立します。

Cisco Jabber は、Webex メッセンジャーから受信した次の XMPP 証明書を検証します。 これらの証明書がオペレーティング システムに付属していない場合は、ユーザが入力する必要があります。

- VeriSign Class 3 Public Primary Certification Authority - G5：この証明書は信頼できるルート認証局に保存されます。
- VeriSign Class 3 Secure Server CA - G3：この証明書は Webex メッセンジャー サーバ ID の検証に使用され、中間認証局に保存されます。
- AddTrust 外部 CA ルート
- GoDaddy Class 2 Certification Authority Root Certificate

Windows 版 Cisco Jabber のルート証明書の詳細については、https://www.identrust.co.uk/certificates/trustid/install-nes36.htmlを参照してください。

Mac 版 Cisco Jabber のルート証明書の詳細については、https://support.apple.comを参照してください。

プロファイル写真の URL の更新

クラウド ベースの展開では、ユーザを追加またはインポートする際に、Webex により、プロファイル写真に一意の URL が割り当てられます。 Cisco Jabber は、連絡先情報を解決するときに、写真がホストされている URL の Webex からプロファイル写真を取得します。

プロファイル写真の URL は、HTTP セキュア（`https://server_name/`）を使用して、クライアントに証明書を提示します。 URL のサーバ名が次の場合：

- Webex ドメインを含む完全修飾ドメイン名（FQDN）：クライアントは、Webex 証明書に照らして、プロファイル写真をホストしている Web サーバを検証できます。
- IP アドレス：クライアントは、Webex 証明書に照らして、プロファイル写真をホストしている Web サーバを検証できません。 この場合、プロファイル写真の URL の IP アドレスで連絡先をルックアップする場合は常に、証明書を受け入れるようクライアントがユーザに指示します。

重要

- サーバー名として IP アドレスを含むすべてのプロファイル写真の URL を更新することをお勧めします。クライアントがユーザーに証明書の承認を求めるプロンプトを表示しないように、Webex メインを含む FQDN で IP アドレスを置き換えます。
- 写真を更新すると、クライアントで写真が更新されるまで最大 24 時間かかります。

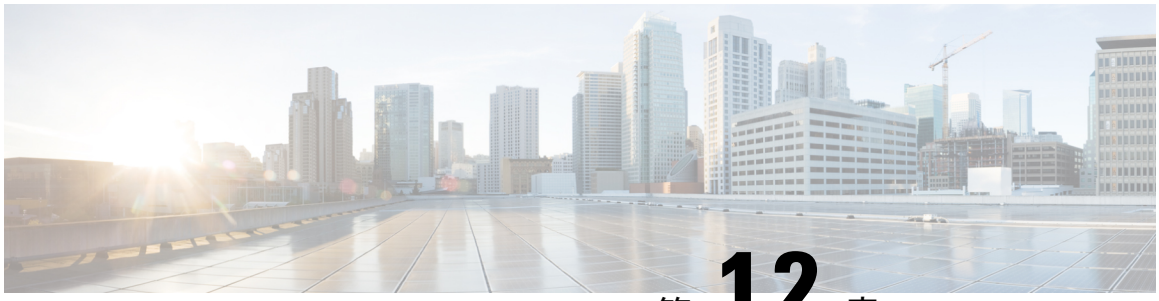
次の手順では、プロファイル写真の URL の更新方法について説明します。 詳細については、該当する Webex マニュアルを参照してください。

ステップ 1 Webex 管理ツールを使用して、ユーザ連絡先データを CSV ファイル形式でエクスポートします。

ステップ 2 [**userProfilePhotoURL**] フィールドで、Webex ドメインで IP アドレスを置き換えます。

ステップ 3 CSV ファイルを保存します。

ステップ 4 Webex 管理ツールを使用して、CSV ファイルをインポートします。



第 12 章

クライアントの設定

クライアント設定ワークフロー

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	デスクトップクライアント向けに電話機の設定でパラメータを設定する	
ステップ 4	電話機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。

- 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。
- Webex 管理ツール：Webex 管理ツールを使用して一部のクライアント設定を構成できます。

  `jabber-config.xml` クライアント設定ファイルを Webex 管理ツールにアップロードできます。 Webex メッセンジャー 管理ツール内の各グループに別個の設定ファイルを適用できます。 クライアントが Webex メッセンジャーに接続すると、XML ファイルがダウンロードされ、その設定が適用されます。

  クライアントは、次の順序で設定を行います。

  1. Webex メッセンジャー 管理ツールの設定
  2. Webex メッセンジャー 管理ツールの `jabber-config.xml` ファイルの設定。

  （注） グループ設定ファイルの設定は、Webexメッセンジャー管理ツールの設定ファイルに優先します。

  3. TFTP サーバの `jabber-config.xml` ファイルの設定。

  設定が競合する場合は、Webex 管理ツールでの設定がその設定ファイルに優先します。

Unified CM でのクライアント設定パラメータの設定

クラウドベース展開では、Webex管理ツールでクライアントを設定します。ただし、オプションで、Webex管理ツールで使用できない設定値でクライアントを設定するために設定パラメータをセットアップすることができます。

iPhone、iPad および Android 版 Cisco Jabber 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、Windows 版 Cisco Jabber と Mac 版 Cisco Jabber 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。

ステップ 1 Jabber 設定パラメータの定義 （61 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 （61 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。

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（UCService Type）]** として **[Jabber クライアント設定（Jabber Client Configuration）（jabber-config.xml）]** 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 **[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**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。

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**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

Webex 管理ツールを使用してクライアントを設定します。 ただし、オプションで、Webex 管理ツールで使用できない設定値でクライアントを設定するために TFTP サーバをセットアップすることができます。

iPhone、 iPad および Android 版 Cisco Jabber 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、Windows 版 Cisco Jabber と Mac 版 Cisco Jabber 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 （63 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 （64 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 （64 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 （65 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 （66 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。	

	コマンドまたはアクション	目的
	• 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。

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。

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) [電話機の設定（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**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。

ステップ 1 Cisco Unified Communications Manager で**Cisco Unified OS Administration** 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。

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 wasSuccessful）」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。

デスクトップクライアント向けに電話機の設定でパラメータを設定する

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機の設定(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機の設定（Enterprise Phone Configuration）]ウィンドウで電話機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** 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**）	ユーザが特定のファイル タイプを送信しないように制限します。 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）	クライアントが初めて起動するときにユーザの電話の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、次回以降の起動時にこ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、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。

電話機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。

パラメータ	説明
オンデマンド VPN の URL（On-Demand VPN URL）	オンデマンド VPN を開始するための URL です。 （注） iOS にのみ適用されます。
プリセット Wi-Fi ネットワーク（Preset Wi-fi Networks）	組織が承認する Wi-Fi ネットワークの SSID（SSID）を入力します。 SSID はスラッシュ（/）で区切ります。 入力した Wi-Fi ネットワークのいずれかに接続されている場合、デバイスはセキュア コネクトに接続しません。
デフォルトの着信音（Default Ringtone）	デフォルトの着信音を [標準（Normal）]または [大（Loud）]に設定します。
[ビデオ機能（Video Capabilities）]	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）：ユーザはビデオコールを送受信できます。 • [無効（Disabled）]：ユーザはビデオコールを送受信できません。
Dial via Office （注） TCT および BOT デバイスのみ。	Dial via Office を有効または無効にします。 • [有効（Enabled）]：ユーザはオフィス経由でダイヤルできます。 • [無効（Disabled）]（デフォルト）：ユーザはオフィス経由でダイヤルできません。

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設定します。

Windows 版 Cisco Jabber 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。

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。

Mac 版 Cisco Jabber 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。

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。

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。

Android 版 Cisco Jabber のプロキシ設定

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 13 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

アクセサリ マネージャ

アクセサリ マネージャ

Jabber デスクトップ クライアントは、アクセサリ マネージャを使用してヘッドセットなどのアクセサリとの対話を可能にします。 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。

一部の Cisco ヘッドセットおよびその他の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、通話の終了などを行います。 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。 標準ヘッドセットは API を使用してスピーカー、マイクの接続をサポートします。

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。 アクセサリ マネージャはデスクトップ電話機をサポートしていません。

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。

（注） jabber-config.xml で EnableAccessoriesManager を false に設定すると、一部のヘッドセットの通話制御ボタンが動作しません。

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:

- Logitech
- Sennheiser
- Jabra
- Plantronics

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） Mac 版 Cisco Jabber 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。

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。
- Android 版 Cisco Jabber 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。
- iPhone および iPad 版 Cisco Jabber 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。

Windows 版 Cisco Jabber のインストール

Windows 版 Cisco Jabber 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 （75 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 （96 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 （97 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 （101 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。

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 Windows 版 Cisco Jabber 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

Windows 版 Cisco Jabber 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 （76 ページ）
言語の LCID （94 ページ）

コマンドライン引数

Windows 版 Cisco Jabber 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 （76 ページ）
言語の LCID （94 ページ）

オーバーライドの引数

次の表では、これまで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ために指定する必要があるパラメータを説明します。

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。 次に、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読み込みます。

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 ファイルをすべて削除する。
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 ファイルが存在しない場合は、クライアントはインストール中にブートストラップ ファイルを作成します。
- ブートストラップ ファイルが存在する場合は、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、既存の設定を保持します。

（注） Windows 版 Cisco Jabber 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 ファイルの設定を保持しません。 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。
- クライアントはインストール引数を既存のブートストラップ ファイルに保存しません。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

次の表では、製品モードを指定するコマンド ライン引数を説明します。

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。 基本機能としてユーザに音声デバイスを提供するには、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。

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 Service です。
- Webex**Webex (IM and Presence)** オーセンティケータは、Webex メッセンジャー 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	Webex	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。 • Webex—Webex メッセンジャー サービス。クラウドベースまたはハイブリッドクラウド ベースでの展開。
CUP_ADDRESS	IP アドレス(IP address) ホストネーム(Hostname) FQDN	Cisco Unified Communications Manager IM and Presence Service 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*）
[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。

引数	値	説明
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。
SERVICES_DOMAIN	ドメイン（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。

引数	値	説明
VOICE_SERVICES_DOMAIN	ドメイン（Domain）	ハイブリッド展開では、CAS 検索を介して Webex を検出することが必要なドメインが、DNS レコードが展開されたドメインと異なる場合があります。 この場合、SERVICES_DOMAIN を Webex の検出に使用されたドメインに設定し（またはユーザにメール アドレスを入力させる）、VOICE_SERVICES_DOMAIN を DNS レコードが展開されたドメインに設定します。 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

Windows 版 Cisco Jabber 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 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

次の表は、一部の一般的なコマンド ライン引数を説明するものです:

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 が共通基準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。
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。 **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。

引数	値	説明
DIAGNOSTICSTOOLENABLED	true false	Windows 版 Cisco Jabber のユーザに対して 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。
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。 この引数はオプションですが、指定することをお勧めします。 （注） クラウドベース展開では、Webex 管理ツールを使用して、忘れたパスワードの URL を指定できます。ただし、ユーザがサインインするまで、クライアントはパスワード忘れの URL を取得できません。
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。

引数	値	説明
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。
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	Windows 版 Cisco Jabber 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、Windows 版 Cisco Jabber 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 Windows 版 Cisco Jabber の 1 つのインスタンスにしかサインインできません。 Windows 版 Cisco Jabber 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 Windows 版 Cisco Jabber 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。 Windows 版 Cisco Jabber 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移動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、Webex Messenger の導入では、従来の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。 Webex Messenger の導入を使用して古典的な設計を開始する必要がある場合は、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。 • クラシック: Jabber は従来のデザインで開始されます。 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	Windows 版 Cisco Jabber	Mac 版 Cisco Jabber	Android 版 Cisco Jabber、iPhone および iPad 版 Cisco Jabber	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	Windows 版 Cisco Jabber	Mac 版 Cisco Jabber	Android 版 Cisco Jabber、iPhone および iPad 版 Cisco Jabber	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	Windows 版 Cisco Jabber	Mac 版 Cisco Jabber	Android 版 Cisco Jabber、iPhone および iPad 版 Cisco Jabber	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
トルコ語	X	X	X	1055

関連トピック

インストール コマンドの例 （76 ページ）
コマンドライン引数 （76 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。

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 Windows 版 Cisco Jabber 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**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 （97 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 （98 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 （99 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。

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 （98 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 （97 ページ）

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 （99 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 （98 ページ）

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 は、デフォルトの 1033 を除き、カスタムインストーラ内の言語ファイルを保持しません。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と、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なくなります。

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 プロパティ

カスタム インストーラで修正できるプロパティは次のとおりです。

- 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 Windows 版 Cisco Jabber をインストールします。

（注） グループ ポリシーと一緒に Windows 版 Cisco Jabber をインストールするには、Windows 版 Cisco Jabber 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 （101 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 （102 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 （94 ページ） を参照してください。

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 （102 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 Windows 版 Cisco Jabber 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 （101 ページ）

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。

Windows 版 Cisco Jabber 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) Windows 版 Cisco Jabber 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 Windows 版 Cisco Jabber 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 Windows 版 Cisco Jabber 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。

（注） インスタント メッセージとプレゼンス機能のために Webex メッセンジャー サービスを使用する場合は、Webex 管理ツールを使用して自動アップデートを設定する必要があります。

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。

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 Windows 版 Cisco Jabber 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。

Windows 版 Cisco Jabber 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 Windows 版 Cisco Jabber 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 Windows 版 Cisco Jabber 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 Windows 版 Cisco Jabber を削除します。

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
```

たとえば、

```
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 Windows 版 Cisco Jabber 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 Windows 版 Cisco Jabber を削除します。

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 Windows 版 Cisco Jabber 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
```

たとえば、

```
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 Windows 版 Cisco Jabber を削除します。

Mac 版 Cisco Jabber のインストール

Mac 版 Cisco Jabber 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。 以前のバージョンのクライアント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、インストーラはいつも `Applications` フォルダにクライアントを追加します。

  - 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、インストーラは Applications フォルダにクライアントを実行するためのリンクを作成します。
  - ユーザーが以前、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。

インストーラは、インストール中にユーザーにシステム資格情報を要求します。

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。

設定

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、『*Mac* 版 *Cisco Jabber* 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。

Apple M1 Mac でネイティブに Jabber を実行する

リリース 14.1.2 以前は、Intel ベースの Mac でのみ Jabber を実行するか、Apple M1 Mac で Rosetta を使用できました。 また、Rosetta を使用せずに、Apple M1 Mac で Jabber を実行することもできるようになりました。

Jabber を Apple M1 Mac でネイティブに実行するには、**[ロゼッタで開く（Open using Rosetta）]** の **[Cisco Jabber]** をオフにします。

Jabber をどのように実行しているかは、**[アクティビティモニタ（Activity Monitor）]** で確認できます。 **[種類（Kind）]** をネイティブに起動した場合、**[Apple]** と表示されます。

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。

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。

Mac 版 Cisco Jabber 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。 Mac 版 Cisco Jabber に適用されます。
  - true
  - false
- PRTCertificateName：任意。 証明書の名前を指定します。 Mac 版 Cisco Jabber に適用されます。
- 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。
  - True
  - False

- 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。
  - True
  - False

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。

（注） インスタント メッセージとプレゼンス機能のために Webex メッセンジャー サービスを使用する場合は、Webex 管理ツールを使用して自動アップデートを設定する必要があります。

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、Windows 版 Cisco Jabber と Mac 版 Cisco Jabber 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。

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 Windows 版 Cisco Jabber に適用されます。
  - JabberMac：更新は Mac 版 Cisco Jabber 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。

  Mac 版 Cisco Jabber 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

ステップ 1 Android 版 Cisco Jabber 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 iPhone および iPad 版 Cisco Jabber 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。

Android、iPhone、および iPad 版 Cisco Jabber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。
  - True
  - False
- 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。
  - True
  - False

（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

AppConfig スタンダードを使用した Enterprise Mobility Management (EMM)

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。
- その Android デバイスには、5.0 以降の OS が搭載されています。

Enterprise Mobility Management (EMM) を使用して Cisco Jabber を設定し、Android 版 Cisco Jabber または iPhone、iPad 版 Cisco Jabber のユーザによる起動を許可します。 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。

iPhone および iPad 版 Cisco Jabber 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（Default Audio Call App）]** 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。

アプリラッピングによる EMM

EMM に対するもう 1 つのアプローチは、アプリラッピングです。 ベンダーのアプリラッピングツールを使用して Jabber をカプセル化し、ポリシーを適用して Jabber でユーザができることを制限します。 次に、カプセル化された Jabber をユーザに配布します。 新しいバージョンの Jabber にアップグレードする場合は、常にカプセル化を繰り返す必要があります。

Cisco Jabber でのアプリのラッピングを使用するには、双方向の契約に署名する必要があります。 `jabber-mobile-mam@cisco.com` の詳細については、弊社にお問い合わせください。

SDK 統合による EMM

リリース 12.8 では、EMM の別のアプローチとして Microsoft Intune および BlackBerry Dynamics のサポートが追加されました。 Microsoft および BlackBerry Sdk を使用して、アプリストアと Google Play ストアから新しいクライアントを作成しました。

- Intune 版 Jabber
- Blackberry 版 Jabber

これらのソリューションを使用して、ポータルに管理ポリシーを作成します。ユーザが新しいクライアントを使用してログインすると、クライアントはポータルと同期してポリシーを適用します。

Intune 版 Jabber を使用した EMM

導入で Intune 版 Jabber クライアントを使用する場合、管理者は Microsoft Azure で管理ポリシーを設定します。 ユーザは、アプリストアまたは Google Play ストアから新しいクライアントをダウンロードします。ユーザが新しいクライアントを実行すると、管理者が作成したポリシーを使用して同期が行われます。

注意 Intune 版 Jabber は、iOS プラットフォームで Apple Push Notification (APN) をサポートしていません。 Jabber をバックグラウンドに配置する場合、iOS デバイスがチャットメッセージやコールを受信しないことがあります。

（注） Android デバイスの場合、ユーザは最初に Intune Company Portal をインストールします。 次に、ポータルを使用してクライアントを実行します。

Intune 版 Jabber を設定するための一般的なプロセスは次のとおりです。

1. 新しい Azure AD テナントを作成します。
2. 新しい AD ユーザを作成するか、オンプレミスの AD ユーザを同期します。
3. Office 365 グループまたはセキュリティグループを作成し、ユーザを追加します。
4. Intune 版 Jabber クライアントを Microsoft Intune に追加します。
5. Microsoft Intune でポリシーを作成して展開します。
6. ユーザはクライアントにログインして、同期してポリシーを受信します。

この手順の詳細については、Microsoft のマニュアルを参照してください。

次の表は、Cisco Jabber 用のアプリ保護ポリシーでサポートされている Microsoft Intune の制限を示しています。

制約事項	Android	iPhone および iPad
他のアプリにデータを送信する	可	可
組織のデータのコピーを保存する	可	可
他のアプリへのカット、コピー、貼り付け	可	可
スクリーン キャプチャ	可	該当なし
最大 PIN 試行回数	可	可
オフラインの猶予期間	可	可
最低要件のアプリ バージョン	可	可
脱獄またはルートされるデバイスで使用する	可	可
最低要件のデバイスの OS バージョン	可	可
最低要件のパッチ バージョン	可	該当なし
職場 (または学校) のアクセス用アカウント資格情報	可	可
アクセス要件を再チェックする	可	可

Blackberry 版 Jabber を使用したEMM

導入で BlackBerry 版 Jabber クライアントを使用する場合、管理者は BlackBerry ユニファイド エンドポイントの管理 (UEM) で管理ポリシーを設定します。 ユーザは、アプリストアまたは Google Play ストアから新しいクライアントをダウンロードします。 Blackberry 版 Jabber は BlackBerry に対応していますが、BlackBerry Marketplace ではまだ入手可能ではありません。

重要 クライアントが BlackBerry を認証中であるため、貴社へのアクセスを許可する必要があります。 アクセスを受信するには、お問合せ先 (jabber-mobile-mam@cisco.com) にアクセスして、お客様の BlackBerry UEM サーバからの組織 ID をご提供ください。

新しいクライアントは BlackBerry Dynamics SDK を統合しており、ブラック UEM からポリシーを直接取得することができます。 クライアントは、接続とストレージに BlackBerry Dynamics をバイパスします。 FIPS 設定は、BlackBerry Dynamics SDK ではサポートされていません。

チャット、音声、およびビデオトラフィックは、BlackBerry インフラストラクチャをバイパスすることになります。 クライアントがオンプレミスの場合、すべてのトラフィックに対して Cisco Expressway でのモバイル & Remote Access が必要です。

注意 BlackBerry 版 Jabber は iOS プラットフォームで Apple Push Notification (APN) をサポートしていません。 Jabber をバックグラウンドに配置する場合、iOS デバイスがチャットメッセージやコールを受信しないことがあります。

（注） Android での BlackBerry 版 Jabber には Android 6.0 以降が必要です。

iOS での BlackBerry 向け Jabber には iOS 11.0 またはそれ以降が必要です。

BlackBerry Dynamics の場合、管理者は BlackBerry 版 Jabber クライアントの使用を制御するポリシーを設定します。

BlackBerry 版 Jabber を設定するための一般的なプロセスは、次のとおりです。

1. UEM にサーバを作成します。
2. BlackBerry 版 Jabber クライアントを BlackBerry Dynamics に追加します。
3. BlackBerry Dynamics でユーザを作成またはインポートします。

（注） Android ユーザの場合、必要に応じて、BlackBerry Dynamics でアクセスキーを生成できます。

4. UEM にポリシーを作成して導入します。 BlackBerry 版 Jabber アプリ設定でのこれらの設定の動作に注意してください。
   - オプションの DLP ポリシーを有効にした場合、BlackBerry は次のものを必要とします。
     - 電子メールの送信に BlackBerry Works を使用します。
     - iOS デバイスの SSO 認証には BlackBerry Access を使用してください。 Expressway とユニファイドコミュニケーションマネージャで、iOS 版**ネイティブブラウザの使用**を有効にします。 次に、**`ciscojabber`**スキームを BlackBerry UEM で BlackBerry アクセスポリシーに追加します。
   - このリストには、BlackBerry 版 Jabber 導入用のアプリ設定によって設定するのに便利な Jabber パラメータが表示されています。 これらのパラメータの詳細については、導入ガイドの *Android*、*iPhone*、*iPad* 版 *Cisco Jabber* の *URL* 設定を参照してください。

フィールド	iOS 対応	Android 対応
相互起動 Webex Meetings の無効化 [1]	可	可
サービス ドメイン	可	可

フィールド	iOS 対応	Android 対応
音声サービス ドメイン	可	可
サービス検出から除外されたサービス	可	可
サービス ドメイン SSO 電子メール プロンプト	可	可
無効な証明書の動作	可	可
テレフォニー有効	可	可
URL プロビジョニングの許可	可	可
IP モード	可	可

[1] Webex Meetings の相互起動を有効にすると、Dynamics 以外のアプリケーションを許可しない BlackBerry Dynamics コンテナで例外として実行できます。

5. ユーザはクライアントにログインします。

この手順の詳細については、BlackBerry のマニュアルを参照してください。

次の表は、Cisco Jabber 用のアプリ保護ポリシーでサポートされている BlackBerry の制限を示しています。

グループ（Group）	機能	Android	iPhone および iPad
ITポリシー	ネットワーク接続なしでデバイスをワイプします	可	可
アクティベーション	許可されたバージョン	可	可

グループ（Group）	機能	Android	iPhone および iPad
BlackBerry Dynamics	[パスワード（Password）]	可	可
	データ漏洩の防止: BlackBerry Dynamics アプリから BlackBerry Dynamics 以外の アプリにデータをコピーすることはできません	可	可
	データ漏洩の防止: BlackBerry Dynamics 以外のアプリから BlackBerry Dynamics アプリにデータをコピーすることはできません	可	可
	データ漏洩の防止：Android および Windows 10+ デバイスでのスクリーンキャプチャを許可しません	可	該当なし
	データ漏洩の防止: iOS デバイスで画面の録音と共有を許可しません	該当なし	可
	データ漏洩の防止: iOS デバイスのカスタムキーボードを許可しません	該当なし	可
Enterprise Management Agent のプロファイル	パーソナルアプリコレクションを許可します	可	可
コンプライアンス プロファイル	ルート OS または失敗した構成証明	可	可
	制限付き OS バージョンがインストールされています	可	可
	必要なセキュリティパッチレベルがインストールされていません	可	該当なし

BlackBerry 版 Jabber の IdP 接続

Android、iPhone および iPad 版 Jabber 導入では、クライアントが DMZ で Id プロバイダー (IdP) プロキシに接続します。 次に、プロキシは、内部ファイアウォールの背後にある IdP サーバに要求を渡します。

BlackBerry 版 Jabber では、代替パスを使用できます。 BlackBerry UEM の DLP ポリシーを有効にすると、iOS デバイスのクライアントは、安全に IdP サーバに直接トンネルできます。 このセットアップを使用するには、導入を次のように設定します。

- Expressway とユニファイド CM で、iOS 版**ネイティブブラウザの使用**を有効にします。
- **Ciscojabber**スキームを blackberry Uem の blackberry アクセスポリシーに追加します。

Android OS 上のBlackBerry 版 Jabber は、SSO のために常に IdP プロキシに接続します。

導入環境に、iOS で動作しているデバイスのみが含まれている場合、DMZ では IdP プロキシは必要ありません。 ただし、Android OS 上で動作するデバイスが導入環境に含まれている場合は、IdP プロキシが必要です。

iOS 上のアプリ トランスポート セキュリティ

iOS には、アプリ トランスポートセキュリティ（ATS）機能が含まれています。ATS では、Jabber for BlackBerry と Jabber for Intune の場合、信頼できる証明書と暗号化を使用して TLS を使用したセキュアなネットワーク接続を実現する必要があります。ATS は、X.509 デジタル証明書を持つサーバへの接続をブロックします。証明書は次のチェックを通過する必要があります。

- 無変更のデジタル署名
- 有効な有効期限
- サーバの DNS 名と一致する名前
- CA からの信頼できるアンカー証明書への有効な証明書のチェーン

（注） iOS の一部である信頼できるアンカー証明書の詳細については、https://support.apple.com/en-us/HT204132 にある「*iOS* で使用可能な信頼されたルート証明書のリスト」を参照してください。システム管理者またはユーザは、同じ要件を満たしている限り、独自の信頼できるアンカー証明書をインストールできます。

ATS の詳細については、https://developer.apple.com/documentation/security/preventing_insecure_network_connections にある「セキュアでないネットワーク接続の防止」を参照してください。

MDM 導入用の便利なパラメータ

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 では、次のパラメータが便利な場合があります。これらのパラメータの詳細については、*Android*、*iPhone*、*iPad* 版 *Cisco Jabber* の *URL* 設定を参照してください。

- ServicesDomain
- VoiceServicesDomain
- ServiceDiscoveryExcludedServices
- ServicesDomainSsoEmailPrompt
- EnablePRTEncryption
- PRTCertificateURL
- PRTCertificateName

- InvalidCertificateBehavior
- Telephony_Enabled
- ForceLaunchBrowser
- FIPS_MODE
- CC_MODE
- LastLoadedUserProfile
- AllowUrlProvisioning

  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。
- IP_Mode
- AllowTeamsUseEmbeddedSafari: iPhone および iPad 版 Cisco Jabber のみ
- AutoLoginUserName
- AutoLoginUserPassword

以降のセクションでは、MDM の導入でこれらのパラメータの一部を使用する方法について説明します。

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>`

AutoLoginUserName

iPhone および iPad 用 Cisco Jabber に適用されます。

EMM では、モバイルデバイス上のユーザ名を定義します。 このパラメータは、AutoLoginUserPassword パラメータおよび ServicesDomain パラメータとともに使用する必要があります。 これらのパラメータがまとめられているので、ユーザのサインイン情報をすでに入力している場合は、Jabber アプリをインストールすることができます。

AutoLoginUserPassword

iPhone および iPad 用 Cisco Jabber に適用されます。

EMM では、モバイルデバイスのパスワードを定義します。 このパラメータは、AutoLoginUserName パラメータおよび ServicesDomain パラメータとともに使用する必要があり

ます。 これらのパラメータがまとめられているので、ユーザのサインイン情報をすでに入力している場合は、Jabber アプリをインストールすることができます。

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。

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。

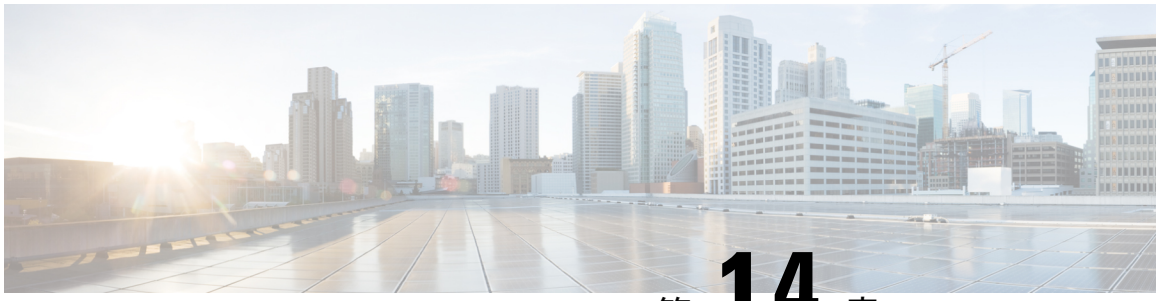
- *true*: Cisco Jabber を FIPS モードで実行します。
- *false*: Cisco Jabber を FIPS モードで実行できません。

例：`<FIPS_MODE>false</FIPS_MODE>`

VDI 版 Jabber Softphone のインストール

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 VDI 版 Cisco Jabber Softphone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 14 章

Remote Access

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 （55 ページ）	
ステップ 2	DNS 要件 （55 ページ）	
ステップ 3	証明書の要件 （55 ページ）	
ステップ 4	_collab-edge SRV レコードのテスト （126 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 要件

Remote Access 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。

証明書の要件

Remote Access 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。

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 （127 ページ）	
ステップ 2	VPN 接続の自動化 （129 ページ）	
ステップ 3	AnyConnect マニュアル リファレンス （132 ページ）	
ステップ 4	セッション パラメータ （132 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、iPhone および iPad 版 Cisco Jabber 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。

Android 版 Cisco Jabber 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。

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。

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。

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**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 マニュアル リファレンス

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（AutoReconnect）]：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（IdleTimeout）]：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（DeadPeer 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。

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*、バージョン *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。

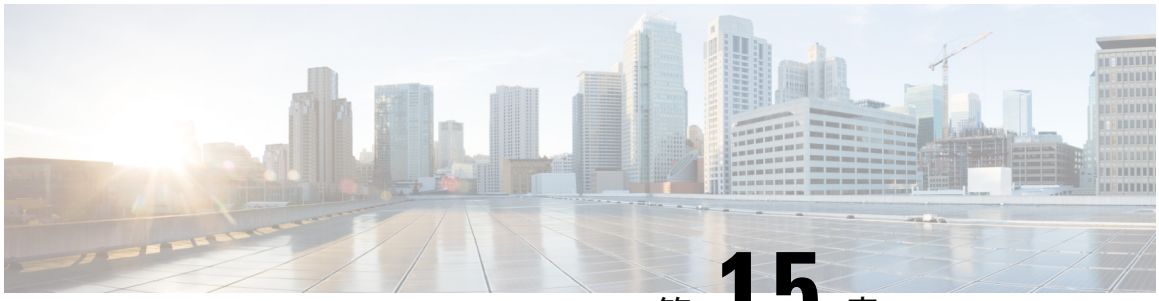
a) Cisco Jabber クライアントに固有のグループ ポリシーを作成します。
b) アイドル タイムアウト値を 30 分に設定します。

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*」の項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。



第 15 章

トラブルシューティング

Cisco Jabber ドメイン用の SSO 証明書の更新

この手順は、クラウドまたはハイブリッド展開に適用されます。 Cisco Jabber ドメイン用の更新されたシングル サインオン（SSO）証明書をアップロードするには、次の手順を使用します。

（注） 1024、2048、または 4096 暗号化ビットおよび RC4-MD5 アルゴリズムによる証明書だけがサポートされています。

始める前に

証明書は CER または CRT ファイル形式である必要があります。

ステップ 1 https://www.webex.com/go/connectadmin で Webex 組織管理ツールにログインします。

ステップ 2 管理ツールがロードされたら、[構成（Configuration）]タブをクリックします。

ステップ 3 左側のナビゲーション バーで [セキュリティの設定（Security Settings）]をクリックします。

ステップ 4 [組織の証明書の管理（Organization Certificate Management）]のリンクをクリックします。
以前にインポートされた X.509 証明書が表示されます。

ステップ 5 **[エイリアス（Alias）]**フィールドに、会社の Webex 組織を入力します。

ステップ 6 [参照（Browse）]をクリックして X.509 証明書を選択します。
証明書は CER または CRT ファイル形式である必要があります。

ステップ 7 [インポート（Import）]をクリックして証明書をインポートします。
証明書が X.509 証明書の指定された形式に従っていない場合は、エラーが表示されます。

ステップ 8 [閉じる（Close）]を 2 回クリックして [SSO 関連オプション（SSO Related Options）]画面に戻ります。

ステップ 9 [保存（Save）]をクリックしてフェデレーテッド Web シングル サインオン設定の詳細を保存します。

Cisco Jabber 診断ツール

Windows および Mac

Cisco Jabber 診断ツールは、次の機能の設定と診断情報を提供します。

- サービス ディスカバリ
- Webex
- Cisco Unified Communications Manager の概要
- Cisco Unified Communications Manager の設定
- ボイスメール
- 証明書の検証
- Active Directory
- DNS レコード

Cisco Jabber 診断ツールのウィンドウにアクセスするには、ハブ ウィンドウにフォーカスを当てて **Ctrl + Shift + D** を押します。 [リロードする（Reload）] ボタンをクリックすると、データを更新できます。 また、[保存（Save）] ボタンをクリックすると、情報を html ファイルに保存できます。

Cisco Jabber 診断ツールはデフォルトで利用可能です。 このツールを無効にするには、DIAGNOSTICS_TOOL_ENABLED インストール パラメータを FALSE に設定する必要があります。 このインストール 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。

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。

ユーザーは、**[サインイン（Sign In）]** 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（Diagnose Error）]** 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場合
- Cisco Jabber サーバが到達可能な場合
- Cisco Jabber が再接続可能である場合

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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。