Cisco Jabber 11.5 用のオンプレミス展開

初版：2015 年 12 月 22 日

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

【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

第 1 章

Cisco Jabber の概要

このマニュアルの目的

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

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

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

Cisco Jabber について

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

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

- Cisco Jabber for Android
- Cisco Jabber for iPhone and iPad

- Cisco Jabber for Mac
- Cisco Jabber for Windows

Cisco Jabber 製品スイートの詳細については、http://www.cisco.com/go/jabber を参照してください。

第 2 章

設定およびインストールのワークフロー

設定ワークフローの目的

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

前提条件

- サーバのインストールが開始され、アクティブである必要があります。
- BFCP 機能用 COP ファイルの適用，（3 ページ）
- 必須サービスの有効化と開始，（4 ページ）
- デバイス用の Cisco Options Package ファイルのインストール，（5 ページ）

BFCP 機能用 COP ファイルの適用

Cisco Unified Communications Manager リリース 8.6.2 以降でビデオ デスクトップ共有を設定するには `cmterm-bfcp-e.8-6-2.cop.sgn` を適用する必要があります。この COP ファイルにより、CSF デバイスで BFCP を有効にするオプションが追加されます。

（注）

- アップグレードするたびにCOPファイルをインストールする必要があります。たとえば、Cisco Unified Communications Manager リリース 8.6.2 .20000-1 でビデオ デスクトップ共有を設定してから、Cisco Unified Communications Manager リリース 8.6.2 .20000-2 をアップグレードした場合は、Cisco Unified Communications Manager リリース 8.6.2 .20000-2 で COP ファイルを適用します。
- Cisco Unified Communications Manager リリース 8.6.1 でビデオ デスクトップ共有を設定してから、Cisco Unified Communications Manager リリース 8.6.2 をアップグレードした場合は、Cisco Unified Communications Manager リリース 8.6.2 上に COP ファイルを適用しなければ、ビデオ デスクトップ共有を設定できません。

手順

ステップ 1 Cisco.com 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 `cmterm-bfcp-e.8-6-2.cop.sgn` をコピーします。

ステップ 3 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] インターフェイスを開きます。

ステップ 4 `cmterm-bfcp-e.8-6-2.cop.sgn` をアップロードし、適用します。

ステップ 5 次のようにサーバを再起動します。

a) [Cisco Unified OS の管理（Cisco Unified CM Administration）] インターフェイスを開きます。
b) [設定（Settings）] > [バージョン（Version）] の順で選択します。
c) [リスタート（Restart）] を選択します。
d) この手順をクラスタの各ノードで繰り返します。最初にプレゼンテーション サーバで実行します。

COP により、CSF デバイスの [電話の設定（Phone Configuration）] ウィンドウの [プロトコル固有情報（Protocol Specific Information）] セクションに [BFCP を使用するプレゼンテーション共有を許可（Allow Presentation Sharing using BFCP）] フィールドが追加されます。

必須サービスの有効化と開始

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

手順

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

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

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

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

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

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

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

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

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

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

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

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

手順

ステップ 1 デバイスの COP ファイルをダウンロードします。

a) デバイスの COP ファイルを配置します。

- ソフトウェア ダウンロード サイトに移動します。

- ご使用のリリースに対応したデバイスの COP ファイルを配置します。

b) [今すぐダウンロード（Download Now）] をクリックします。
c) MD5 チェックサムを書き留めます。
この情報は、後で必要になります。
d) [ダウンロードを進める（Proceed with Download）] をクリックして、手順に従います。

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

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

a) [Cisco Unified OS の管理（Cisco Unified CM Administration）] インターフェイスを開きます。
b) [ソフトウェアアップグレード（Software Upgrades）] > [インストール/アップグレード（Install/Upgrade）] を選択します。
c) COP ファイルの場所を指定し、必要な情報を入力します。
詳細については、オンライン ヘルプを参照してください。
d) [次へ（Next）] を選択します。
e) デバイス COP ファイルを選択します。
f) [次へ（Next）] を選択します。
g) 画面に表示される指示に従います。
h) [次へ（Next）] を選択します。
処理が完了するまで待ちます。このプロセスには、時間がかかる場合があります。
i) 使用率が低いときに Cisco Unified Communications Manager をリブートします。
j) システムが完全にサービスに復帰するまで待機します。
（注） サービスの中断を避けるために、各ノードのサービスがアクティブな状態に戻ったことを確認してから、次のサーバでのこの手順を実行するようにしてください。

ステップ 4 クラスタ内の各サブスクライバ ノードに COP ファイルをインストールします。
パブリッシャ ノードのときと同じ方法で、ノードのリブートなどの手順を実行します。

オンプレミス展開に関する展開およびインストールワークフロー

完全 UC モードの展開

手順

	コマンドまたはアクション	目的
ステップ 1	http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html で『Cisco Jabber Planning Guide』を参照してください。	• 展開シナリオを選択します。 • 要件を検証して、それらが満たされていることを確認します。 • 連絡先ソースを確認して、使用する連絡先ソースを決定します。
ステップ 2	ユーザ, （11 ページ）	
ステップ 3	連絡先ソース, （19 ページ）	
ステップ 4	インスタント メッセージングとプレゼンス サービスの設定, （31 ページ）	
ステップ 5	ボイスメールの設定, （41 ページ）	
ステップ 6	WebEx 会議の設定, （49 ページ）	
ステップ 7	デスクフォン制御の設定, （53 ページ）	
ステップ 8	ソフトフォンの設定, （63 ページ）	
ステップ 9	拡張および接続機能の設定, （81 ページ）	
ステップ 10	サービス プロファイルの設定, （87 ページ）	
ステップ 11	サービス ディスカバリの設定, （95 ページ）	
ステップ 12	証明書検証の設定, （107 ページ）	
ステップ 13	クライアントの設定, （111 ページ）	
ステップ 14	Cisco Jabber アプリケーションの展開, （123 ページ）	

Jabber IM 専用モードの展開

手順

	コマンドまたはアクション	目的
ステップ 1	http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html で『Cisco Jabber Planning Guide』を参照してください。	• 展開シナリオを選択します。 • 要件を検証して、それらが満たされていることを確認します。 • 連絡先ソースを確認して、使用する連絡先ソースを決定します。
ステップ 2	ユーザ, （11 ページ）	
ステップ 3	連絡先ソース, （19 ページ）	
ステップ 4	インスタントメッセージングとプレゼンスサービスの設定, （31 ページ）	
ステップ 5	WebEx 会議の設定, （49 ページ）	
ステップ 6	サービス プロファイルの設定, （87 ページ）	
ステップ 7	サービス ディスカバリの設定, （95 ページ）	
ステップ 8	証明書検証の設定, （107 ページ）	
ステップ 9	クライアントの設定, （111 ページ）	
ステップ 10	Cisco Jabber アプリケーションの展開, （123 ページ）	

電話モードの展開

手順

	コマンドまたはアクション	目的
ステップ 1	http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/	• 展開シナリオを選択します。

	コマンドまたはアクション	目的
	products-installation-guides-list.html で『Cisco Jabber Planning Guide』を参照してください。	• 要件を検証して、それらが満たされていることを確認します。 • 連絡先ソースを確認して、使用する連絡先ソースを決定します。
ステップ 2	ユーザ, （11 ページ）。	
ステップ 3	証明書検証の設定, （107 ページ）。	証明書は、Jabber クライアントが接続するサービスごとに必要です。
ステップ 4	サービス ディスカバリの設定, （95 ページ）。	
ステップ 5	サービス プロファイルの設定, （87 ページ）。	
ステップ 6	ソフトフォンの設定, （63 ページ）。	
ステップ 7	ボイスメールの設定, （41 ページ）。	
ステップ 8	WebEx 会議の設定, （49 ページ）。	
ステップ 9	クライアントの設定, （111 ページ）。	
ステップ 10	Cisco Jabber アプリケーションの展開, （123 ページ）。	

第 3 章

ユーザ

ユーザの設定を行う

手順

	コマンドまたはアクション	目的
ステップ 1	同期の有効化，（11 ページ）	
ステップ 2	ユーザ ID とディレクトリ URI の入力，（12 ページ）	
ステップ 3	同期の実行，（14 ページ）	
ステップ 4	ロールとグループの割り当て，（15 ページ）	
ステップ 5	認証オプション，（16 ページ）	

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。

手順

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

ステップ 2 [システム（System）] > [LDAP] > [LDAP 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。

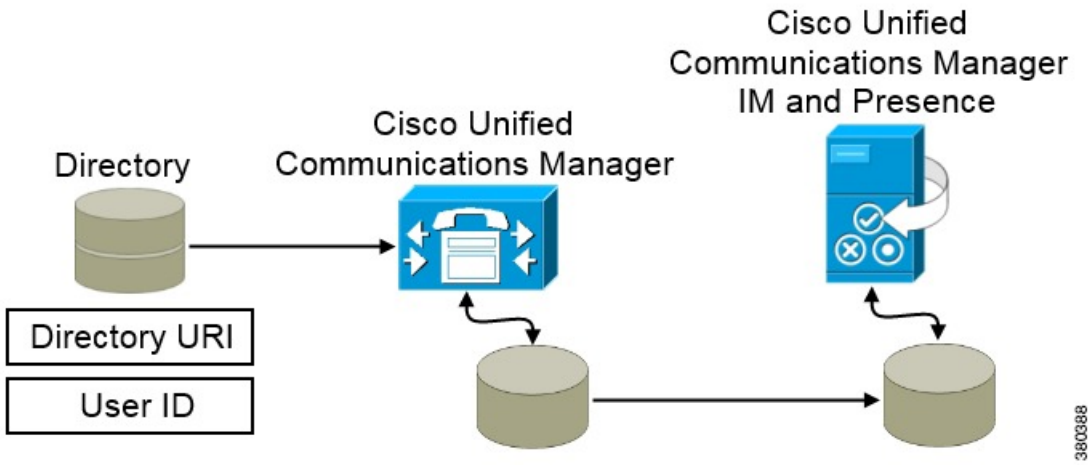
次の作業

ユーザ ID の LDAP 属性を指定します。

ユーザ ID とディレクトリ URI の入力

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

- ユーザ ID：Cisco Unified Communications Manager でユーザ ID の値を指定する必要があります。この値はデフォルトの IM アドレス スキームおよびユーザのログインに必要です。デフォルト値は `sAMAccountName` です。
- ディレクトリ URI：以下を予定している場合は、ディレクトリ URI の値を指定する必要があります。
  - Cisco Jabber で URI ダイヤルを有効にする。
  - Cisco Unified Communications Manager IM and Presence サービス バージョン 10 以降でディレクトリ URI アドレス スキームを使用する。



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

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

ユーザ 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。

手順

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 サービス 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。

EDI パラメータは `UserAccountName` です。

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

BDI パラメータは `BDIUserAccountName` です。

```
<BDIUserAccountName>attribute-name</BDIUserAccountName>
```

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 の 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。

はじめる前に

同期の有効化します。

手順

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

ステップ 2 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 アドレス

ステップ 5 [保存（Save）] を選択します。

同期の実行

ディレクトリ サーバを追加し、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。

はじめる前に

ご使用の環境にプレゼンスサーバが含まれる場合は、ディレクトリ サーバと同期する前に次の機能サービスがアクティブになっていて、開始されていることを確認する必要があります。

- Cisco Unified Communications Manager IM and Presence サービス：Cisco Sync Agent

このサービスは、プレゼンス サーバと Cisco Unified Communications Manager 間で同期されたデータを維持します。ディレクトリ サーバとの同期を実行すると、Cisco Unified Communications Manager は次にプレゼンス サーバとデータを同期します。ただし、[Cisco Sync Agent] サービスがアクティブになっていて、開始されている必要があります。

手順

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

ステップ 2 [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。

手順

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

ステップ 2 [ユーザ管理（User Management）] > [エンドユーザ（End User）] を選択します。
[ユーザの検索と一覧表示（Find and List Users）] ウィンドウが開きます。

ステップ 3 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。

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

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

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

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

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

はじめる前に

- Cisco WebEx Messenger を使用しない場合は、Cisco Unified Communications Applications 10.5.1 Service Update 1 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、『*SAML SSO Deployment Guide for Cisco Unified Communications Applications, Release 10.5*（*Cisco Unified Communications* アプリケーション リリース *10.5 SAML SSO* 導入ガイド）』を参照してください。
- Cisco Unity Connection バージョン 10.5 で SSO を有効にします。このサービス上での SAML SSO の有効化方法については、『*Managing SAML SSO in Cisco Unity Connection*』を参照してください。
- Cisco WebEx Messenger を使用する場合は、Cisco WebEx Messenger サービスで SSO を有効にして Cisco Unified Communications アプリケーションと 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、『*Cisco WebEx Messenger Administrator's Guide*（*Cisco WebEx Messenger* 管理者ガイド）』の「*Single Sign-On*（シングル サインオン）」を参照してください。

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

手順

ステップ 1 Web ブラウザで証明書を検証できるように、すべてのサーバに証明書を配布してください。これを行わない場合、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、「*Configure Service Discovery for Remote Access*（リモート アクセス用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、Cookie およびトークン値で構成されます。通常、Cookie はトークンより長く残ります。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。

関連トピック

Single Sign-On
Managing SAML SSO in Cisco Unity Connection
SAML SSO Deployment Guide for Cisco Unified Communications Applications

LDAP サーバでの認証

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

手順

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

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

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

ステップ 4 必要に応じて、LDAP クレデンシャルとユーザ検索ベースを指定します。
[LDAP認証（LDAP Authentication）] ウィンドウ上のフィールドの詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

ステップ 5 [保存（Save）] を選択します。

第 4 章

連絡先ソース

連絡先ソースの設定のワークフロー

手順

	コマンドまたはアクション	目的
ステップ 1	ディレクトリ統合の設定： • サービスプロファイルでのディレクトリ統合の設定，（20 ページ） • コンフィギュレーションファイルでのディレクトリ統合の詳細設定，（27 ページ）	Cisco Unified Communications Manager を使用してサービスプロファイル経由で、またはコンフィギュレーションファイルを使用して、ディレクトリ統合を設定します。
ステップ 2	オプション： 写真の設定，（26 ページ）	ユーザの写真を設定するオプションについて確認します。
ステップ 3	オプション： BDI または EDI のイントラドメイン フェデレーションの設定，（27 ページ）	Cisco Jabber ユーザは、別のシステム上でプロビジョニングされたユーザや Cisco Jabber 以外のクライアントアプリケーションを使用しているユーザと通信できます。

ディレクトリ統合のためのクライアント設定

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

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

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

サービス プロファイルでのディレクトリ統合の設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	ディレクトリ サービスを追加する，（21 ページ）	ディレクトリ UC サービスを作成します。
ステップ 2	サービス プロファイルへのディレクトリ サービスの適用，（25 ページ）	サービス プロファイルにディレクトリ UC サービスを追加します。

ディレクトリ サービスを追加する

手順

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

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

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

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

ステップ 5 ディレクトリ サービスに対して適切な値を設定します。
グローバル カタログで Cisco Jabber ディレクトリ検索を設定するには、次の値を追加します。

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

ステップ 6 [保存（Save）] を選択します。

次の作業

ディレクトリ サービスを適用します。

ディレクトリ プロファイル パラメータ

次の表は、ディレクトリ プロファイルで設定できる設定パラメータを示します。

ディレクトリ サービスの設定	説明
プライマリ サーバ（Primary server）	プライマリ ディレクトリ サーバのアドレスを指定します。 このパラメータは、クライアントが自動的にディレクトリ サーバを検出できない手動接続に必要です。
セカンダリ サーバ（Secondary server）	バックアップディレクトリ サーバのアドレスを指定します。
ターシャリ サーバ（Tertiary Server）	Cisco Jabber for Windows にのみ適用されます。 ターシャリ ディレクトリ サーバのアドレスを指定します。

ディレクトリ サービスの設定	説明
コンタクト解決に UDS を使用（Use UDS for Contact Resolution）	クライアントが UDS を連絡先ソースとして使用するかどうかを指定します。 **重要**（注） このオプションが選択されている場合は、この表の次のパラメータが使用されません。 デフォルトで、ユーザが Expressway for Mobile and Remote Access 経由で社内ネットワークに接続するときに、UDS が連絡先解決を提供します。
ログインしたユーザのクレデンシャルを使用（Use Logged On User Credential）	クライアントがログオンしているユーザ名とパスワードを使用するかどうかを指定します。 **[はい（True）]** クレデンシャルを使用します。これがデフォルト値です。 **[いいえ（False）]** クレデンシャルを使用しません。 次のパラメータを使用してクレデンシャルを指定します。 • EDI ◦ ConnectionUsername ◦ ConnectionPassword • BDI ◦ BDIConnectionUsername ◦ BDIConnectionPassword

ディレクトリ サービスの設定	説明
ユーザ名（Username）	ディレクトリ サーバでの認証にクライアントが使用できる共有ユーザ名を手動で指定できるようにします。 デフォルトで、Cisco Jabber for Windows は、ディレクトリ サーバに接続するときに統合 Windows 認証を使用します。 このパラメータは、Microsoft Windows クレデンシャルを使用してディレクトリ サーバで認証できない展開でのみ使用する必要があります。 読み取り専用権限を持っているアカウントの既知のまたは公開されているクレデンシャルのセットのみを使用します。
パスワード（Password）	ディレクトリ サーバでの認証にクライアントが使用できる共有パスワードを手動で指定できるようにします。 デフォルトで、Cisco Jabber for Windows は、ディレクトリ サーバに接続するときに統合 Windows 認証を使用します。 このパラメータは、Microsoft Windows クレデンシャルを使用してディレクトリ サーバで認証できない展開でのみ使用する必要があります。 読み取り専用権限を持っているアカウントの既知のまたは公開されているクレデンシャルのセットのみを使用します。

ディレクトリ サービスの設定	説明
検索ベース 1（Search Base 1） 次のパラメータは、Cisco Jabber for Windows だけに適用されます。 検索ベース 2（Search Base 2） 検索ベース 3（Search Base 3）	検索が開始されるディレクトリ サーバの場所を指定します。つまり、検索ベースはクライアントが検索を実行するルートです。 デフォルトの場合、クライアントはディレクトリ ツリーのルートから検索を行います。デフォルトの動作を上書きする場合は、最大 3 つの検索ベースの値を OU に指定することができます。 Active Directory は、通常、検索ベースを必要としません。特定のパフォーマンス要件がある場合にのみ、Active Directory の検索ベースを指定します。 ディレクトリ内の特定の場所へのバインディングを作成するには、Active Directory 以外のディレクトリ サーバの検索ベースを指定します。 **ヒント** OU を指定すると、検索対象を特定のユーザ グループに制限することができます。 たとえば、ユーザのサブセットがインスタント メッセージの機能だけを持っているとします。これらのユーザを OU に含め、この OU を検索ベースとして指定します。
すべての検索ベースで再帰検索（Recursive Search on All Search Bases）	検索ベースから始まるディレクトリの再帰検索を実行するには、このオプションを選択します。再帰検索を使用して、Cisco Jabber クライアントの連絡先検索クエリーが指定された検索コンテキスト（検索ベース）からの LDAP ディレクトリ ツリーすべてを検索できるようにします。これは、LDAP 検索と共通のオプションです。 必須フィールドです。 デフォルト値は True です。
基本フィルタ（Base Filter）	Active Directory クエリーの基本フィルタを指定します。 ディレクトリのサブキー名のみを指定し、ディレクトリへのクエリーの実行時にユーザ オブジェクト以外のオブジェクトを取得します。 デフォルト値は `(&(objectCategory=person)(objectClass=user)` です。

ディレクトリ サービスの設定	説明
予測検索フィルタ（Predictive Search Filter）	予測検索クエリーに適用するフィルタを定義します。 検索クエリーをフィルタするために、複数のカンマ区切り値を定義できます。 デフォルト値は Ambiguous Name Resolution（ANR）です。 Cisco Jabber for Windows が予測検索を実行するときに、Ambiguous Name Resolution（ANR）を使用してクエリーを発行します。このクエリーにより、検索文字列が明確化され、ディレクトリ サーバ上で ANR に対して設定された属性に合致する結果が返されます。 **重要** クライアントにANRの属性を検索させる場合は、その属性を設定するようにディレクトリ サーバを設定します。

サービス ディスカバリは、[連絡先の解決にUDSを使用する（Use UDS for Contact Resolution）] が選択されている場合に UDS 検索を使用します。そうでない場合は、BDI または EDI 検索を使用します。サービス ディスカバリでは、ディレクトリ プロファイル内の Username、Password、SearchBase1、PrimaryServerName、ServerPort1、UriPrefix、UseJabberCredentials、BaseFilter、PredictiveSearchFilter、および DirectoryServerType を使用して LDAP サーバに接続して連絡先が検索されます。

手動サインオンでは、ディレクトリ プロファイルからの Username と Password を使用して LDAP サーバに接続して連絡先が検索されます。

属性のマッピング

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

サービス プロファイルへのディレクトリ サービスの適用

手順

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

ステップ 2 [新規追加（Add New）] を選択します。

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

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

ステップ 4 [保存（Save）] を選択します。

写真の設定

Cisco Jabber は、次の方法を使用してユーザの写真を設定します。

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

  EDI パラメータ：PhotoSource

  例：

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

  BDI パラメータ：BDIPhotoSource

  ```
  <Directory>
   <BDIPhotoSource>url</BDIPhotoSource>
  </Directory>
  ```

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

  EDI パラメータ：

  - PhotoUriSubstitutionEnabled
  - PhotoUriWithToken
  - PhotoUriSubstitutionToken

  例：

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

  BDI パラメータ：

  - BDIPhotoUriSubstitutionEnabled
  - BDIPhotoUriWithToken
  - BDIPhotoUriSubstitutionToken

例：

```
<BDIPhotoUriSubstitutionEnabled>True</BDIPhotoUriSubstitutionEnabled>
<BDIPhotoUriSubstitutionToken>sAMAccountName</BDIPhotoUriSubstitutionToken>
<BDIPhotoUriWithToken>http://example.com/photo/sAMAccountName.jpg</BDIPhotoUriWithToken>
```

UDS パラメータ：

- UdsPhotoUriSubstitutionEnabled
- UdsPhotoUriWithToken
- UdsPhotoUriSubstitutionToken

例：

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

コンフィギュレーション ファイルでのディレクトリ統合の詳細設定

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

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

フェデレーション

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

BDI または EDI のイントラドメイン フェデレーションの設定

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

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

イントラドメイン フェデレーションの設定に使用されるパラメータは、拡張ディレクトリ統合（EDI）と基本ディレクトリ統合（BDI）のどちらを使用するかによって異なります。EDI は、ネイティブな Microsoft Windows API を使用してディレクトリ サービスから連絡先データを取得し、Cisco Jabber for Windows でのみ使用されます。BDI の場合は、クライアントがディレクトリ サー

ビスから連絡先データを取得し、Cisco Jabber for Mac、Cisco Jabber for Android、および Cisco Jabber for iPhone and iPad で使用されます。

手順

ステップ 1 関連パラメータの値を true に設定します。

- BDI の場合：BDIUseSipUriToResolveContacts
- EDI の場合：UseSIPURIToResolveContacts

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

- BDI の場合：BDISipUri
- EDI の場合：SipUri

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

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

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

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

- BDI の場合：BDIUriPrefix
- EDI の場合：UriPrefix

次の XML スニペットは、BDI 用の最終的な設定例を示しています。

```
<Directory>
  <BDIUseSIPURIToResolveContacts>true</BDIUseSIPURIToResolveContacts>
  <BDISipUri>non-default-attribute</BDISipUri>
  <BDIUriPrefix>sip:</BDIUriPrefix>
</Directory>
```

次の XML スニペットは、EDI 用の最終的な設定例を示しています。

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

第 5 章

インスタント メッセージングとプレゼンス サービスの設定

Cisco Unified Communications Manager リリース 10.5 以降を使用したオンプレミス展開に関する IM and Presence サービス ワークフロー

手順

	コマンドまたはアクション	目的
ステップ 1	IM アドレス スキームの設定，（34 ページ）	
ステップ 2	メッセージの設定の有効化，（35 ページ）	

	コマンドまたはアクション	目的
ステップ 3	連絡先リストの一括事前入力, （36 ページ）	
ステップ 4	IM and Presence サービスでのユーザの設定, （36 ページ）	
ステップ 5	ユーザと回線の関連付け , （38 ページ）	この手順は任意です。

Cisco Unified Communications Manager リリース 9.x 以降を使用したオンプレミス展開に関する IM and Presence サービス ワークフロー

手順

	コマンドまたはアクション	目的
ステップ 1	IM and Presence サービスの追加, （32 ページ）	
ステップ 2	IM and Presence サービスの適用, （33 ページ）	
ステップ 3	IM アドレス スキームの設定, （34 ページ）	
ステップ 4	メッセージの設定の有効化, （35 ページ）	
ステップ 5	連絡先リストの一括事前入力, （36 ページ）	
ステップ 6	IM and Presence サービスでのユーザの設定, （36 ページ）	

IM and Presence サービスの追加

IM and Presence サービス機能をユーザに提供します。

手順

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

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

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

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

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

ステップ 5 [次へ（Next）] を選択します。

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

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

b) [名前（Name）] フィールドにサービスの名前を入力します。
入力した名前は、プロファイルにサービスを追加する際に表示されます。入力する名前は必ず、一意的でわかりやすく、かつ意味が通じるものにしてください。

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

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

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

ステップ 7 [保存（Save）] を選択します。

IM and Presence サービスの適用

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

はじめる前に

IM and Presence サービスの追加, （32 ページ）

手順

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

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

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

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

- [プライマリ（Primary）]
- [セカンダリ（Secondary）]
- [ターシャリ（Tertiary）]

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 ユーザをサービス プロファイルに追加します。

a) [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）] ダイアログボックスが開きます。

b) [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）] を選択してユーザを検索します。

c) リスト内のユーザをクリックします。
[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) [サービスの設定（Service Settings）] 領域で [ホーム クラスタ（Home Cluster）] チェックボックスをオンにします。

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

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

ステップ 7 [保存（Save）] をクリックします。

IM アドレス スキームの設定

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

手順

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

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

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

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

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

ステップ 2 必要なマッピングを選択します。

a) [Cisco Unified CM の管理（Cisco Unified CM Administration）] を開きます。
b) [システム（System）] > [LDAP] > [LDAP ディレクトリ（LDAP Directory）] を選択します。
[LDAP ディレクトリの検索と一覧表示（Find and List LDAP Directories）] ウィンドウが開きます。
c) リストからディレクトリを検索して選択します。
[LDAP ディレクトリ（LDAP Directory）] ウィンドウが開きます。
d) [同期対象の標準ユーザ フィールド（Standard User Fields To Be Synchronized）] セクションで、マッピングを選択します。

- LDAP フィールドにマッピングされるユーザ ID。デフォルトは sAMAccountName です。
- mail と msRTCSIP-primaryuseraddress のどちらかにマッピングされるディレクトリ URI。

メッセージの設定の有効化

インスタント メッセージング機能を有効にし、設定します。

はじめる前に

連絡先リストの一括事前入力, （36 ページ）。

手順

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

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

ステップ 3 次のオプションを選択します。

- インスタント メッセージを有効にする（Enable instant messaging）
- クライアントでのインスタント メッセージ履歴のログ記録を可能にする（Allow clients to log instant message history）

ステップ 4 他のメッセージング設定も適切に選択します。

ステップ 5 [保存（Save）] を選択します。

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

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

次の作業

- Cisco Unified Communications Manager IM and Presence サービス リリース 9.x 以降を使用している場合は、IM and Presence サービスの追加, （32 ページ）。

連絡先リストの一括事前入力

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

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザに提供する連絡先リストを定義した CSV ファイルを作成します。	
ステップ 2	BAT を使用して一連のユーザに連絡先リストを一括でインポートします。	BAT の使用方法と CSV ファイルの形式については、ご使用のリリースの『*Deployment Guide for Cisco Unified Communications Manager IM & Presence*』を参照してください。

IM and Presence サービスでのユーザの設定

IM and Presence に対してユーザを有効にすることができます。

ユーザの設定を個別に行う

インスタント メッセージおよびプレゼンス サービスを有効にし、個々のユーザにサービス プロファイルを追加します。

手順

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

ステップ 2 [ユーザ管理（User Management）] > [エンド ユーザ（End User）] を選択します。
[ユーザの検索と一覧表示（Find and List Users）] ウィンドウが開きます。

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

ステップ 4 対象のユーザ名をリストから選択します。
[エンド ユーザの設定（End User Configuration）] ウィンドウが表示されます。

ステップ 5 [サービスの設定（Service Settings）] セクションに移動し、以下の操作を行います。

a) [ホーム クラスタ（Home Cluster）] を選択します。

b) [ユーザに対して Unified CM IM and Presence を有効にする（Enable User for Unified CU IM and Presence）] を選択します。

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

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

ステップ 6 [保存（Save）] を選択します。

複数ユーザの設定を一括で行う

インスタントメッセージおよびプレゼンスを有効にし、複数のユーザにサービスプロファイルを追加します。

手順

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

ステップ 2 [一括管理（Bulk Administration）] > [ユーザ（Users）] > [ユーザの更新（Update Users）] > [クエリー（Query）] を選択します。
[更新するユーザの検索と一覧表示（Find and List Users To Update）] ウィンドウが表示されます。

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

ステップ 4 [次へ（Next）] を選択します。
[ユーザの更新（Update Users Configuration）] ウィンドウが開きます。

ステップ 5 2 つある [ユーザに対して Unified CM IM and Presence を有効にする（Enable User for Unified CU IM and Presence）] チェックボックスをどちらもオンにします。

重要 [ユーザに対して Unified CM IM and Presence を有効にする（Enable User for Unified CU IM and Presence）] チェックボックスは 2 つあります。インスタント メッセージおよびプレゼンスを無効にする場合は、いずれか一方のチェックボックスを選択します。インスタント メッセージおよびプレゼンスを有効にする場合は、両方のチェックボックスを選択します。

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

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

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

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

ステップ 8 [送信（Submit）] を選択します。

ユーザと回線の関連付け

ユーザの存在が [サイレント（Do Not Disturb）] として設定されるとユーザは IM 通知を受信しませんが、これによりユーザが [回線（Line）] に関連付けられることを避けるため、ユーザはコールの通知を受信することができます。

この設定は、モバイル クライアントに適用されます。

手順

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

ステップ 2 [デバイス（Device）] > [電話（Phone）] に移動します。

ステップ 3 ユーザ デバイスを選択します。
たとえば、BOTuser か TABuser を選択します。

ステップ 4 [電話の設定（Phone Configuration）] スクリーンで、[関連付け（Association）] の下にあるこのユーザ デバイス用に設定された、[電話番号（Directory Number）] または [回線（Line）] を選択します。

ステップ 5 [電話番号の設定（Directory Number Configuration）] スクリーンで、[回線に関連付けられているユーザ（Users Associated with Line）] の下のユーザを関連付けます。

第 6 章

ボイスメールの設定

Cisco Unified Communications Manager リリース 9.x 以降を使用したオンプレミス展開用のボイスメールの設定

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Jabber で使用する Cisco Unity Connection の設定，（42 ページ）	Cisco Jabber がボイスメール サービスにアクセスできるように、Cisco Unity Connection を設定します。
ステップ 2	取得とリダイレクションの設定，（43 ページ）	ユーザがボイスメールメッセージにアクセスできるように、取得を設定します。ユーザが着信コールをボイスメールに送信できるようにするために、リダイレクションを設定します。
ステップ 3	ボイスメールサービスを追加する，（45 ページ）	

	コマンドまたはアクション	目的
ステップ 4	ボイスメール サービスの適用，（46 ページ）	ボイスメールサービスを追加した後、クライアントがその設定を取得できるようにするために、そのボイスメールサービスをサービスプロファイルに適用する必要があります。
ステップ 5	ボイスメールのクレデンシャルソースの設定，（47 ページ）	

Cisco Jabber で使用する Cisco Unity Connection の設定

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

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

手順

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

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

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

ステップ 3　ユーザのパスワード設定を編集します。

a) [ユーザ（Users）] を選択します。
b) 適切なユーザを選択します。
c) [編集（Edit）] > [パスワードの設定（Password Settings）] を選択します。

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

ステップ 4 ユーザに Web Inbox へのアクセスを付与します。

a) [サービス クラス（Class of Service）] を選択します。
[サービス クラスの検索（Search Class of Service）] ウィンドウが開きます。
b) 適切なサービス クラスを選択するか、サービスの新しいクラスを追加します。
c) [Web Inbox と RSS フィードの使用をユーザに許可する（Allow Users to Use the Web Inbox and RSS Feeds）] を選択します。
d) [機能（Features）] セクションで、[ボイスメールへのアクセスに Unified Client の使用をユーザに許可する（Allow Users to Use Unified Client to Access Voice Mail）] を選択します。
e) 必要に応じて、その他のすべてのオプションを選択します。
f) [保存（Save）] を選択します。

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

a) [システム設定（System Settings）] > [詳細設定（Advanced）] > [API 設定（API Settings）] を選択します。
[API の設定（API Configuration）] ウィンドウが開きます。
b) 次のオプションを選択します。
- [CUMIを介したセキュアメッセージ録音へのアクセスを許可する（Allow Access to Secure Message Recordings through CUMI）]
- [CUMIを介してセキュアメッセージのメッセージヘッダー情報を表示する（Display Message Header Information of Secure Messages through CUMI）]
- [CUMI経由のメッセージ添付ファイルを許可する（Allow Message Attachments through CUMI）]

c) [保存（Save）] を選択します。

次の作業

Cisco Unified Communications Manager リリース 9.x 以降を使用している場合は、ボイスメール サービスを追加する，（45 ページ）。

取得とリダイレクションの設定

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

ションを設定します。Cisco Unified Communications Manager で取得とリダイレクションを設定します。

手順

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

ステップ 2 ボイスメール パイロットを設定します。

a) [拡張機能（Advanced Features）] > [ボイスメール（Voice Mail）] > [ボイスメール パイロット（Voice Mail Pilot）] の順に選択します。
[ボイスメール パイロットの検索と一覧表示（Find and List Voice Mail Pilots）] ウィンドウが開きます。

b) [新規追加（Add New）] を選択します。
[ボイスメール パイロットの設定（Voice Mail Pilot Configuration）] ウィンドウが開きます。

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

d) [保存（Save）] を選択します。

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

a) [拡張機能（Advanced Features）] > [ボイスメール（Voice Mail）] > [ボイスメール プロファイル（Voice Mail Profile）] の順に選択します。
[ボイスメールプロファイルの検索/一覧表示（Find and List Voicemail Profiles）] ウィンドウが開きます。

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

c) 対象のプロファイルを一覧から選択します。
[ボイスメール パイロットの設定（Voice Mail Pilot Configuration）] ウィンドウが開きます。

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

e) [保存（Save）] を選択します。

ステップ 4 電話番号設定でボイスメール プロファイルを指定します。

a) [デバイス（Device）] > [電話（Phone）] の順に選択します。
[電話の検索と一覧表示（Find and List Phones）] ウィンドウが開きます。

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

c) 対象のデバイスを一覧から選択します。
[電話の設定（Phone Configuration）] ウィンドウが開きます。

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

e) 適切なデバイス番号を選択します。
[電話番号設定（Directory Number Configuration）] ウィンドウが開きます。

f) [電話番号の設定（Directory Number Settings）] セクションを探します。
g) [ボイスメール プロファイル（Voice Mail Profile）] ドロップダウン リストからボイスメール プロファイルを選択します。
h) [保存（Save）] を選択します。

次の作業

ボイスメールのクレデンシャル ソースの設定, （47 ページ）

ボイスメール サービスを追加する

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

はじめる前に

Cisco Jabber で使用する Cisco Unity Connection の設定, （42 ページ）

手順

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

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

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

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

ステップ 5 ボイスメール サービスの詳細を次のように指定します。

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

ステップ 6 [保存（Save）] を選択します。

次の作業

ボイスメール サービスの適用, （46 ページ）

ボイスメール サービスの適用

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

はじめる前に

ボイスメール サービスを追加する, （45 ページ）

手順

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

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

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

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

a) 次のドロップダウン リストから、サービスを最大 3 つ選択します。

- [プライマリ（Primary）]
- [セカンダリ（Secondary）]
- [ターシャリ（Tertiary）]

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

- [Unified CM - IM and Presence（Unified CM - IM and Presence）]：インスタント メッセージおよびプレゼンスのクレデンシャルを使用してボイスメール サービスにサインインします。このため、ユーザはクライアントでボイスメール サービスのクレデンシャルを入力する必要ありません。
- [Web会議（Web conferencing）]：会議クレデンシャルを使用してボイスメール サービスにサインインする、このオプションはサポートされません。現時点では、会議クレデンシャルとは同期できません。

- [未設定（Not set）]：このオプションは、電話モード展開の場合に選択されます。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 ユーザをサービス プロファイルに追加します。

a) [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。

b) [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）] を選択してユーザを検索します。

c) リスト内のユーザをクリックします。
[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) [サービスの設定（Service Settings）] エリアで、[ホームクラスタ（Home Cluster）] チェックボックスをオンにします。

e) 電話モード展開では、[Unified CM IM and Presence のユーザを有効化（関連付けられている UC サービス プロファイルで IM and Presence を設定）（Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)）] オプションが選択されていないことを確認します。
他のすべての展開では、[Unified CM IM and Presenceの ユーザを有効化（関連付けられている UC サービス プロファイルで IM and Presence を設定）（Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)）] チェックボックスをオンにします。

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

g) [保存（Save）] をクリックします。

ボイスメールのクレデンシャル ソースの設定

ユーザのボイスメールのクレデンシャル ソースを指定できます。

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

はじめる前に

取得とリダイレクションの設定, （43 ページ）

手順

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

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

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

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

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

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

次の作業

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

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

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

第 7 章

WebEx 会議の設定

オンプレミス展開用の会議の設定

Cisco Jabber 用のオンプレミス展開を実装すると、Cisco WebEx Meetings Server を使用してオンプレミスで会議を設定するか、または Cisco WebEx Meetings Center を使用してクラウドで会議を設定できます。

WebEx Meetings Server を使用したオンプレミス会議の設定

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco WebEx Meetings Server の認証，（49 ページ）。	
ステップ 2	Cisco Unified Communications Manager 上での Cisco WebEx Meetings Server の追加，（50 ページ）。	

Cisco WebEx Meetings Server の認証

手順

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

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

次の作業

Cisco Unified Communications Manager 上での Cisco WebEx Meetings Server の追加, （50 ページ）

Cisco Unified Communications Manager 上での Cisco WebEx Meetings Server の追加

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

はじめる前に

Cisco WebEx Meetings Server を使用して認証を行います。

手順

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

ステップ 2 [新規追加（Add New）] を選択します。

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

ステップ 4 次のフィールドに入力します。

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

- [プロトコル（Protocol）]：[HTTPS] を選択します。

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

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

ステップ 6 [保存（Save）] を選択します。

次の作業

サービス プロファイルへの Cisco WebEx Meetings Server の追加, （51 ページ）

サービス プロファイルへの Cisco WebEx Meetings Server の追加

Cisco WebEx Meetings Server を追加してから、さらにそのサーバをサービス プロファイルに追加すれば、クライアントが会議機能にアクセスできます。

はじめる前に

サービス プロファイルを作成します。

Cisco Unified Communications Manager 上での Cisco WebEx Meetings Server の追加, （50 ページ）

手順

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

ステップ 2 目的のサービス プロファイルを検索し、それを選択します。

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

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

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

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

- [ボイスメール（Voicemail）]：このオプションは、ユーザの Cisco Unity Connection クレデンシャルが Cisco WebEx Meetings Server クレデンシャルと一致する場合に選択します。

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

ステップ 6 [保存（Save）] を選択します。

第 8 章

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	CTI サービスを追加する，（54 ページ）	CTI UC サービスを作成します。この情報は、CTI サーバを見つけるために Jabber が使用します。

	コマンドまたはアクション	目的
ステップ 2	CTI 用のデバイスの有効化, （56 ページ）	Cisco Jabber デスクトップ クライアントがユーザのデスクフォンを制御することを可能にします。
ステップ 3	デスクフォン ビデオの設定, （56 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 4	ビデオ レート アダプテーションの有効化, （58 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 5	ユーザの関連付けに関する設定, （60 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。
ステップ 6	デバイスのリセット, （61 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 サービスを追加する

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

手順

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

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

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

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

ステップ 5 [次へ（Next）] を選択します。

ステップ 6 次の手順に従って、インスタント メッセージ/プレゼンス サービスの詳細情報を設定します。

a) [名前（Name）] フィールドにサービスの名前を入力します。
入力した名前は、プロファイルにサービスを追加する際に表示されます。入力する名前は必ず、一意的でわかりやすく、かつ意味が通じるものにしてください。

b) [ホスト名/IP アドレス（Host Name/IP Address）] フィールドに、CTI サービスのアドレスを入力します。
c) [ポート（Port）] フィールドに、CTI サービスに使用するポート番号を入力します。

ステップ 7 [保存（Save）] を選択します。

次の作業

サービス プロファイルに CTI サービスを追加します。

CTI サービスの適用

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

はじめる前に

- まだ存在していないか、CTI 用に別のサービス プロファイルが必要な場合は、サービス プロファイルを作成します。
- CTI サービスを追加します。

手順

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

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

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

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

- [プライマリ（Primary）]
- [セカンダリ（Secondary）]
- [ターシャリ（Tertiary）]

ステップ 5 [保存（Save）] を選択します。

CTI 用のデバイスの有効化

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

手順

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

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

ステップ 3 [保存（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、ユーザは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できます。

デスクフォン ビデオを設定する

デスクフォンのビデオを設定する手順は次のとおりです。

1. コンピュータをデスクフォン デバイス上のコンピュータ ポートへ物理的に接続します。

   クライアントがデスクフォンデバイスへの接続を確立できるようにするためには、そのデバイスに対してコンピュータをコンピュータ ポート経由で物理的に接続する必要があります。デスクフォンデバイスへのワイヤレス接続によりデスクフォンのビデオ機能を使用することはできません。

ヒント ワイヤレス接続と有線接続の両方を使用できる場合、ユーザは有線接続がワイヤレス接続よりも優先されるように Microsoft Windows を設定する必要があります。詳細については、『*An explanation of the Automatic Metric feature for Internet Protocol routes*』という Microsoft マニュアルを参照してください。

2. Cisco Unified Communications Manager でビデオのデスクフォン デバイスを有効化します。
3. コンピュータに Cisco メディア サービス インターフェイスをインストールします。

   Cisco メディア サービス インターフェイスによって提供される Cisco Discover Protocol（CDP）ドライバによって、クライアントは以下を行えます。

- デスクフォン デバイスを検出します。
- CAST プロトコルを使用してデスクフォン デバイスへの接続を確立して維持します。

（注） cisco.com のダウンロード サイトから Cisco メディア サービス インターフェイスのインストール プログラムをダウンロードします。

デスクフォン ビデオでの考慮事項

ユーザにデスクフォン ビデオ機能をプロビジョニングする前に、以下の考慮事項および制限事項を確認してください。

- Cisco Unified IP Phone 9971 などのデバイスにビデオ カメラが接続されていると、デバイスでデスクフォンのビデオ機能を使用できません。デバイスからビデオカメラを取り外すと、デスクフォンのビデオ機能が使用できるようになります。
- CTI をサポートしていないデバイスでは、デスクフォン ビデオ機能を使用することはできません。
- デスクフォン ビデオでは、BFCP プロトコルを使用したビデオ デスクトップ共有はサポートされていません。
- 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。
- ユーザがデスクフォン デバイス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デバイスの音声コールとして開始されます。クライアントは、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ないデバイスでデスクフォンのビデオ機能を使用するには、ユーザは、クライアントからコールを開始する必要があります。
- 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。デスクフォンのビデオ機能を使用するには、ファームウェアのバージョンを SCCP45.9-3-1 にアップグレードする必要があります。
- 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、デスクフォンのビデオ機能が無効になる場合があります。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する必要があります。

  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 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。このチェックボックスを選択すると、デスクフォンのビデオ機能を使用できなくなります。

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. Cisco メディア 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。

手順

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

ステップ 2 [デバイス（Device）]>[デバイスの設定（Device Settings）]>[共通の電話プロファイル（Common Phone Profile）] の順に選択します。
[共通の電話プロファイルの検索と一覧表示（Find and List Common Phone Profiles）] ウィンドウが開きます。

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

ステップ 4 対象のプロファイルを一覧から選択します。
[共通の電話プロファイルの設定（Find and List Common Phone Profiles）] ウィンドウが開きます。

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

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

ステップ 7 [保存（Save）] を選択します。

デバイス設定に対する RTCP の有効化

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

手順

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

ステップ 2 [デバイス（Device）] > [電話（Phone）] の順に選択します。
[電話の検索と一覧表示（Find and List Phones）] ウィンドウが開きます。

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

ステップ 4 対象の電話を一覧から選択します。
[電話の設定（Phone Configuration）] ウィンドウが開きます。

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

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

ステップ 7 [保存（Save）] を選択します。

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。

はじめる前に

Cisco Jabber デバイスを作成および設定します。

手順

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

ステップ 2 [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 [ホーム クラスタ（Home Cluster）] を選択します。

ステップ 7 [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 8 [デバイス情報（Device Information）] セクションを探します。

ステップ 9 [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 10 ユーザを割り当てるデバイスを選択します。

ステップ 11 [選択/変更の保存（Save Selected/Changes）] を選択します。

ステップ 12 [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 13 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 14 [権限情報（Permissions Information）] セクションを探します。

ステップ 15 [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 16 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。

- [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）]

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 17 [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 18 [エンド ユーザの設定（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。

手順

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

ステップ 2 [デバイス（Device）] > [電話（Phone）] の順に選択します。
[電話の検索と一覧表示（Find and List Phones）] ウィンドウが開きます。

ステップ 3 [電話を次の条件で検索（Find Phone where）] フィールドに適切なフィルタを指定し、[検索（Find）] を選択して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。
[電話番号設定（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 9 章

ソフトフォンの設定

ソフトフォン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	Cisco Jabber デバイスの作成と設定，（64 ページ）	Cisco Jabber にアクセスするユーザごとに 1 つ以上のデバイスを作成します。
ステップ 2	SIP トランクの設定，（70 ページ）	リリース 11.5(3) から、ユーザが Cisco Jabber から電話でプレゼンス表示を確認できるようにする場合は、Cisco Unified Communications Manager と IM and Presence サービス間に SIP トランクを作成する必要があります。
ステップ 3	ユーザの関連付けに関する設定，（60 ページ）	
ステップ 4	モバイル SIP プロファイルの作成，（74 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，（76 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。
ステップ 6	ユーザへの認証文字列の提供，（78 ページ）	

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。

はじめる前に

- COP ファイルをインストールします。
- CTI リモート デバイスに割り当てるユーザのモビリティを有効にします。
- 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 以降の場合は、[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。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。たとえば、cisco.com などです。この最上位ドメイン名は、電話登録用の Cisco Unified Communications Manager サーバの DNS ドメインとして Jabber で使用します。たとえば、CUCMServer1@cisco.com となります。

手順

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

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

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

ステップ 3 [新規追加（Add New）] を選択します。

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

- [Cisco Unified Client Services Framework]：このオプションは、Cisco Jabber for Mac または Cisco Jabber for Windows 用の CSF デバイスを作成する場合に選択します。
- [Cisco Dual Mode for iPhone]：このオプションは、iPhone 用の TFT デバイスを作成する場合に選択します。
- [Cisco Jabber for Tablet]：このオプションは、iPad または Android タブレット用の 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 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
[CTI リモートデバイス（CTI Remote Device）]	• [オーナーのユーザ ID（Owner User ID）] を選択すると、デバイス名フィールドに *CTIRD<owner user ID>* と入力されます。この値は変更できます。デバイス名を *CTIRD* から始める必要はありません。 • 有効な文字：a ~ z、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 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。

選択肢	必要な形式
[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。
[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 CTI リモート デバイスを作成している場合は、[プロトコル固有情報（Protocol Specific Information）] セクションで、[再ルーティング用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ます。
再ルーティング用コーリング サーチ スペースは、再ルーティング用のコーリング サーチ スペースを定義し、ユーザが CTI リモート デバイスからコールを送受信できるようにします。

ステップ 8 エンド 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には、[Certification Authority Proxy Function（CAPF）の情報（Certification Authority Proxy Function (CAPF) Information）] セクションに移動します。

ステップ 9 [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。

ステップ 10 [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。

ステップ 11 [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。

ステップ 12 [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。

ステップ 13 [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。

ステップ 14 必要に応じて、[電話の設定（Phone Configuration）] ウィンドウで残りの設定を指定します。
残りの設定の詳細については、メニュー バーで、[ヘルプ（Help）] > [このページ（This Page）] の順にクリックします。[プロダクト固有の設定（Product Specific Configuration Layout）] セクション内の設定の詳細については、疑問符アイコンをクリックします。

ステップ 15 [保存（Save）] を選択します。

ステップ 16 [設定の適用（Apply Config）] をクリックします。

次の作業

デバイスに電話番号を追加します。

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。

はじめる前に

デバイスを作成します。

手順

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

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

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

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

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

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

ステップ 7 その他に必要な設定があれば、それらをすべて指定します。

ステップ 8 [設定の適用（Apply Config）] を選択します。

ステップ 9 [保存（Save）] を選択します。

リモート接続先の追加

リモート接続先とは、ユーザが利用できる CTI 制御可能デバイスです。

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

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

（注）

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

手順

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

ステップ 2 [デバイス（Device）] > [電話（Phone）] の順に選択します。
[電話の検索と一覧表示（Find and List Phones）] ウィンドウが開きます。

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

ステップ 4 一覧から CTI リモート デバイスを選択します。
[電話の設定（Phone Configuration）] ウィンドウが開きます。

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

ステップ 6 [新規リモート接続先の追加（Add a New Remote Destination）] を選択します。
[リモート接続先情報（Remote Destination Information）] ウィンドウが開きます。

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

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

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

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

ステップ 9 必要に応じて他の値をすべて指定します。

ステップ 10 [保存（Save）] を選択します。

次の作業

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

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

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

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

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

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

SIP トランクの設定

リリース 11.5(3) から、ユーザが電話でプレゼンス表示を確認できるようにする場合は、Cisco Unified Communications Manager と IM and Presence サービス間に SIP トランクを設定する必要があります。

IM and Presence サービスの SIP トランク セキュリティ プロファイルの設定

手順

ステップ 1 Cisco Unified CM Administration から [システム（System）] > [セキュリティ（Security）] > [SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）] を選択します。

ステップ 2 [検索（Find）] をクリックします。

ステップ 3 [Non Secure SIP Trunk Profile] をクリックします。

ステップ 4 [コピー（Copy）] をクリックして、[名前（Name）] フィールドに SIP トランク プロファイルの名前を入力します。

ステップ 5 次の設定値を確認します。

- [デバイス セキュリティ モード（Device Security Mode）] = [非セキュア（Non Secure）]
- [着信トランスポート タイプ（Incoming Transport Type）] = [TCP + UDP]
- [発信トランスポート タイプ（Outgoing Transport Type）] = [TCP]

ステップ 6 次の項目を有効にする場合はオンにします。

- [プレゼンスのSUBSCRIBEの許可（Accept Presence Subscription）]
- [Out-of-Dialog REFERの許可（Accept Out-of-Dialog REFER）]

- [Unsolicited NOTIFYの許可（Accept unsolicited notification）]
- [Replacesヘッダーの許可（Accept replaces header）]

ステップ 7 [保存（Save）] をクリックします。

次の作業

IM and Presence Service の SIP トランクの設定, （71 ページ）

IM and Presence Service の SIP トランクの設定

Cisco Unified Communications Manager クラスタと IM and Presence サービス クラスタの間には、1 個の SIP トランクのみを設定します。SIP トランクの設定後、Cisco Unified Communications Manager 上で IM and Presence PUBLISH トランクとして SIP トランクを割り当てる必要があります。

[宛先アドレス（Destination Address）] フィールドで、次の形式の 1 つを使用して値を入力してください。

- ドット付き IP アドレス
- 完全修飾ドメイン名（FQDN）
- DNS SRV

ハイ アベイラビリティが IM and Presence クラスタに設定されている場合、クラスタ内の複数のノードを識別するために、複数のエントリをドット付き IP アドレスまたは FQDN で入力する必要があります。ハイ アベイラビリティを設定する場合は、DNS SRVは IM and Presence のクラスタに使用できません。

はじめる前に

IM and Presence サービスの SIP トランク セキュリティ プロファイルの設定, （70 ページ）

手順

ステップ 1 Cisco Unified CM Administration から、[デバイス（Device）]>[トランク（Trunk）] を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [トランク タイプ（Trunk Type）] メニューから [SIP トランク（SIP Trunk）] を選択します。

ステップ 4 [デバイス プロトコル（Device Protocol）] メニューから [SIP] を選択します。

ステップ 5 [トランク サービス タイプ（Trunk Service Type）] で [なし（None）] を選択します。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [デバイス名（Device Name）] に CUPS-SIP-Trunk と入力します。

ステップ 8 [デバイス プール（Device Pool）] メニューからデバイス プールを選択します。

ステップ 9 ウィンドウの下部にある [SIP 情報（SIP Information）] セクションで、次の値を設定します。

a) [宛先アドレス（Destination Address）] フィールドに、ドット付き IP アドレスまたは DNS で解決可能で、IM and Presence ノードで設定された SRV クラスタ名に一致する必要がある FQDN を入力します。

b) マルチノード展開を設定した場合は、[宛先アドレスはSRVです（Destination Address is an SRV）] をオンにします。
このシナリオでは、Cisco Unified Communications Manager は名前（たとえば、*_sip._tcp.hostname.tld*）を解決するために DNS SRV レコード クエリーを実行します。シングルノード展開を設定する場合は、このチェックボックスをオフのままにし、Cisco Unified Communications Manager は名前（たとえば、*hostname.tld*）を解決するために DNS A レコード クエリーを実行します。

DNS SRV レコードの宛先アドレスとして IM and Presence サービスのデフォルト ドメインを使用することを推奨します。

（注） DNS SRV レコードの宛先アドレスとしてドメイン値を指定できます。指定されたドメインにユーザを割り当てる必要はありません。入力したドメイン値が IM and Presence サービスのデフォルト ドメインと異なる場合、IM and Presence サービス の SRV クラスタ名である SIP Proxy サービス パラメータが DNS SRV レコードで指定するドメイン値に一致することを確認する必要がありますデフォルト ドメインを使用する場合は、SRV クラスタ名パラメータの変更は必要ありません。

いずれの場合も、Cisco Unified Communications SIP トランクの宛先アドレスは DNS によって解決し、IM and Presence のノードで設定された SRV クラスタ名に一致する必要があります。

c) [接続先ポート（Destination Port）] に「5060」と入力します。

d) [SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）] メニューから [非セキュアな SIP トランク プロファイル（Non Secure SIP Trunk Profile）] を選択します。

e) [SIP プロファイル（SIP Profile）] メニューから [標準 SIP プロファイル（Standard SIP Profile）] を選択します。

ステップ 10 [保存（Save）] をクリックします。
トラブルシューティングのヒント

ポート番号または IP アドレスを変更することで Publish SIP trunk SRV レコードの DNS エントリを修正する場合は、そのアドレスに以前にパブリッシュしたデバイスをすべて再起動し、どのデバイスも正しい IM and Presence サービスの連絡先を指していることを確認する必要があります。

次の作業

SIP パブリッシュ トランクの設定, （72 ページ）

SIP パブリッシュ トランクの設定

この手順は、Cisco Unified Communications Manager で、Cisco Unified Communications Manager for IM and Presence サービスのユーザ ライセンスに関連付けられているすべてのライン アピアランスにおいて電話でのプレゼンス表示を公開できるようにするために実行します。

はじめる前に

IM and Presence Service の SIP トランクの設定, （71 ページ）

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] で [プレゼンス（Presence）] > [設定（Settings）] > [標準設定（Standard Configuration）] を選択します。

ステップ 2 [CUCM SIP パブリッシュ トランク（CUCM SIP Publish Trunk）] ドロップダウン リストから、SIP トランクを選択します。

ステップ 3 [保存（Save）] をクリックします。

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。

はじめる前に

Cisco Jabber デバイスを作成および設定します。

手順

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

ステップ 2 [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 [ホーム クラスタ（Home Cluster）] を選択します。

ステップ 7 [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 8 [デバイス情報（Device Information）] セクションを探します。

ステップ 9 [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 10 ユーザを割り当てるデバイスを選択します。

ステップ 11 [選択/変更の保存（Save Selected/Changes）] を選択します。

ステップ 12 [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 13 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 14 [権限情報（Permissions Information）] セクションを探します。

ステップ 15 [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 16 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。

- [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）]

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 17 [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 18 [エンド ユーザの設定（End User Configuration）] ウィンドウで [保存（Save）] を選択します。

モバイル SIP プロファイルの作成

この手順は、Cisco Unified Communications Manager リリース 9 を使用していて、デバイスをモバイルクライアント用に設定している場合にのみ必要です。デスクトップクライアント用に提供されているデフォルトの SIP プロファイルを使用してください。モバイル クライアント用にデバイ

スを作成して設定する前に、Cisco Unified Communications Manager に接続した状態で Cisco Jabber をバックグラウンドで実行させる SIP プロファイルを作成する必要があります。

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

手順

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

ステップ 2 [デバイス（Device）] > [デバイスの設定（Device Settings）] > [SIP プロファイル（SIP Profile）] の順に選択します。
[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」
- [サブスクライブの再送間隔の調整値（Timer Subscribe Delta）] に「15」

ステップ 5 [保存（Save）] を選択します。

システムの SIP パラメータの設定

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

はじめる前に

この設定は、モバイル クライアント専用です。

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

手順

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

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

ステップ 3 ノードを選択します。

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

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

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

ステップ 7 [保存（Save）] を選択します。

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

電話セキュリティ プロファイルの設定

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

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

はじめる前に

- 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。

手順

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

ステップ 2 [新規追加（Add New）] を選択します。

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

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

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（Save）] をクリックします。

ユーザへの認証文字列の提供

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。

第 10 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，（81 ページ）	
ステップ 2	CTI リモート デバイスの作成，（82 ページ）	
ステップ 3	ユーザの関連付けに関する設定，（60 ページ）	

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。

はじめる前に

この作業は、次の場合にのみ該当します。

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

手順

ステップ 1 [ユーザ管理（User Management）] > [エンド ユーザ（End User）] を選択します。
[ユーザの検索と一覧表示（Find and List Users）] ウィンドウが開きます。

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

ステップ 3 ユーザを一覧から選択します。
[エンド ユーザの設定（End User Configuration）] ウィンドウが表示されます。

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

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

ステップ 6 [保存（Save）] を選択します。

CTI リモート デバイスの作成

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

手順

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

ステップ 2 [デバイス（Device）] > [電話（Phone）] の順に選択します。
[電話の検索と一覧表示（Find and List Phones）] ウィンドウが開きます。

ステップ 3 [新規追加（Add New）] を選択します。

ステップ 4 [電話のタイプ（Phone Type）] ドロップダウン リストから[CTI リモート デバイス（CTI Remote Device）] を選択します。続いて [次へ（Next）] を選択します。
[電話の設定（Phone Configuration）] ウィンドウが開きます。

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

（注） [オーナーのユーザ ID（Owner User ID）] ドロップダウン リストには、モビリティの有効化が利用可能なユーザのみが表示されます。詳細については、「クライアント内の 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。

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。

はじめる前に

Cisco Jabber デバイスを作成および設定します。

手順

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

ステップ 2 [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 [ホーム クラスタ（Home Cluster）] を選択します。

ステップ 7 [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 8 [デバイス情報（Device Information）] セクションを探します。

ステップ 9 [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 10 ユーザを割り当てるデバイスを選択します。

ステップ 11 [選択/変更の保存（Save Selected/Changes）] を選択します。

ステップ 12 [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 13 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 14 [権限情報（Permissions Information）] セクションを探します。

ステップ 15 [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 16 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。

- [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）]

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 17 [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 18 [エンド ユーザの設定（End User Configuration）] ウィンドウで [保存（Save）] を選択します。

第 11 章

サービス プロファイルの設定

サービス プロファイル ワークフローの設定

手順

	コマンドまたはアクション	目的
ステップ 1	サービス プロファイルの設定，（87 ページ）	Cisco Unified Communications Manager バージョン 9 以降の UC サービス プロファイルで特定のクライアント設定を構成できます。
ステップ 2	サービス プロファイルのパラメータ，（88 ページ）	
ステップ 3	Cisco Unified Communications Manager サービスの追加，（91 ページ）	
ステップ 4	サービス プロファイルの作成，（92 ページ）	
ステップ 5	サービス プロファイルの適用，（92 ページ）	
ステップ 6	ユーザとデバイスの関連付け，（93 ページ）	

サービス プロファイルの設定

Cisco Unified Communications Manager バージョン 9 以降の UC サービス プロファイルで特定のクライアント設定を構成できます。

重要

- クライアントが DNS クエリーから `_cisco-uds` SRV レコードを取得する場合は、Cisco Jabber が Cisco Unified Communications Manager 上のサービス プロファイルから設定のみを取得します。

  ハイブリッド環境で、CAS URL 検索が成功した場合は、Cisco Jabber が Cisco WebEx Messenger サービスから設定を取得し、`_cisco-uds` SRV レコードは無視されます。

- 複数の Cisco Unified Communications Manager クラスタを使用した環境では、クラスタ間検索サービス（ILS）を設定できます。ILS は、クライアントがユーザのホーム クラスタを検索して、サービスを検出できるようにします。

  ILS を設定しない場合は、EMCC リモート クラスタのセットアップと同様に、リモート クラスタ情報を手動で設定する必要があります。リモート クラスタ設定の詳細については、『*Cisco Unified Communications Manager Features and Services Guide*』を参照してください。

サービス プロファイルのパラメータ

サービス プロファイルで設定できる設定パラメータについて説明します。クライアントの設定ファイルで該当する設定パラメータを確認してください。

IM and Presence サービス プロファイル

次の表に、IM and Presence サービス プロファイルで構成可能な設定パラメータを示します。

パラメータ	説明
製品のタイプ（Product type）	Cisco Jabber に認証ソースを提供し、次の値が設定されます。 • Unified CM（IM and Presence Service）：Cisco Unified Communications Manager IM and Presence サービスがオーセンティケータです。 • WebEx（IM and Presence サービス）：Cisco WebEx Messenger サービスがオーセンティケータです。 （注） このリリースでは、クライアントは、SRV レコードのクエリーに加え、HTTP クエリーを発行します。HTTP クエリーを使用すれば、クライアントは Cisco WebEx Messenger サービスの認証を受けるかどうかを決定できます。 HTTP クエリーの結果として、クライアントは `_cisco-uds` SRV レコードを取得する前に、クラウドベース展開で Cisco WebEx Messenger サービスに接続します。[製品のタイプ（Product type）] フィールドの値を [WebEx] に設定しても、WebEx サービスが CAS ルックアップによってすでに検出されている場合、実質的な効果はない可能性があります。 • 設定なし：サービス プロファイルに IM and Presence サービス設定が含まれていない場合は、オーセンティケータが Cisco Unified Communications Manager になります。

パラメータ	説明
プライマリ サーバ（Primary server）	プライマリ プレゼンス サーバのアドレスを指定します。 • オンプレミス展開：Cisco Unified Communications Manager IM and Presence サービスの完全修飾ドメイン名（FQDN）を指定する必要があります。 • クラウドベース展開：[製品のタイプ（Product type）] パラメータの値として [WebEx] が選択された場合は、クライアントが次の URL をデフォルトとして使用します。 `https://loginp.webexconnect.com/cas/auth.do` このデフォルトの URL は、設定した値を上書きします。

ボイスメール プロファイル

次の表は、ボイスメールのプロファイルで設定できる設定パラメータを示します。

パラメータ	説明
ボイスメール サーバ（Voicemail server）	ボイスメール サーバの接続設定を指定します。
ボイスメールサービスのクレデンシャル ソース（Credentials source for voicemail service）	ボイスメール サービスの認証を受けるために、クライアントがインスタント メッセージおよびプレゼンスまたは会議サービスのクレデンシャルを使用することを指定します。 設定するクレデンシャル ソースがユーザのボイスメールのクレデンシャルと一致することを確認します。このパラメータの値を設定すると、ユーザはクライアント ユーザ インターフェイスで自分のボイスメール サービスのクレデンシャルを指定できません。

会議プロファイル

次の表は、会議のプロファイルで設定できる設定パラメータを示します。

会議サービスの設定	説明
会議サーバ（Conferencing server）	会議サーバの接続設定を指定します。

会議サービスの設定	説明
Web 会議サービスのクレデンシャル ソース（Credentials source for web conference service）	会議サービスの認証を受けるために、クライアントがインスタント メッセージおよびプレゼンスまたはボイスメール サービスのクレデンシャルを使用することを指定します。 設定するクレデンシャル ソースがユーザの会議のクレデンシャルと一致することを確認します。

ディレクトリ プロファイル

サービス プロファイルでディレクトリ統合を設定する方法の詳細については、「ディレクトリ統合のためのクライアント設定」の章を参照してください。

CTI プロファイル

次の表は、CTI プロファイルで設定できる設定パラメータを示します。

CTI サービスの設定	説明
CTI サーバ（CTI server）	CTI サーバの接続設定を指定します。

Cisco Unified Communications Manager サービスの追加

IM and Presence サービス、ボイスメール、会議、ディレクトリなどのサービスのアドレス、ポート、プロトコル、およびその他の設定を指定する場合に、Cisco Unified Communications Manager サービスを追加します。

手順

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

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

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

ステップ 4 追加する UC サービスのタイプを選択し、[次へ（Next）] を選択します。

ステップ 5 必要に応じて、UC サービスを設定し、[保存（Save）] を選択します。

次の作業

UC サービスをサービス プロファイルに追加します。

サービス プロファイルの作成

Cisco Unified Communications Manager サービスを追加して設定したら、それらをサービス プロファイルに追加します。サービス プロファイルで追加の設定を適用できます。

手順

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

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

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

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

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

（注） Cisco Unified Communications Manager リリース 9.x で、インスタント メッセージング機能だけを使用しているユーザ（IM 専用）は、デフォルト サービス プロファイルを使用する必要があります。このため、IM のみのユーザにサービス プロファイルを適用する場合は、サービス プロファイルをデフォルトとして設定する必要があります。

ステップ 6 UC サービスを追加して追加の設定を適用し、[保存（Save）] を選択します。

次の作業

エンド ユーザ設定にサービス プロファイルを適用します。

サービス プロファイルの適用

UC サービスを追加してサービス プロファイルを作成したら、ユーザにサービス プロファイルを適用します。ユーザが Cisco Jabber にサインインしたら、クライアントは Cisco Unified Communications Manager からそのユーザのサービス プロファイルを取得できます。

手順

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

ステップ 2 [ユーザ管理（User Management）] > [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 既存のユーザを見つけるために適切な検索条件を入力して、リストからユーザを選択します。[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 [サービスの設定（Service Settings）] セクションを探します。

ステップ 5 [UC サービス プロファイル（UC Service Profile）] ドロップダウン リストからユーザに適用するサービス プロファイルを選択します。

重要 **Cisco Unified Communications Manager リリース 9.x のみ**：ユーザが IIM and Presence サービス機能しか使用していない（IM 専用）場合は、[デフォルトを使用（Use Default）] を選択する必要があります。IM 専用ユーザの場合は、Cisco Unified Communications Manager リリース 9.x が [UCサービスプロファイル（UC Service Profile）] ドロップダウン リストで選択された内容に関係なく、常に、デフォルト サービス プロファイルを適用します。

ステップ 6 必要に応じて、その他の設定を適用し、[保存（Save）] を選択します。

ユーザとデバイスの関連付け

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

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

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

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

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

（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ようにする必要があります。

手順

ステップ 1 ユーザとデバイスを関連付けます。

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

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

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

第 12 章

サービス ディスカバリの設定

サービス ディスカバリのオプション

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

オプション	説明
DNS SRV レコードの確認，（96 ページ）	クライアントはサービスを自動的に検出して接続します。 これは推奨オプションです。
カスタマイゼーション，（97 ページ）	インストール パラメータ、URL の設定、または企業モビリティ管理を使用してサービス検出をカスタマイズできます。
手動接続設定，（104 ページ）	手動接続設定は、サービスディスカバリが使用されていない場合にフォールバック メカニズムを提供します。

DNS SRV レコードの確認

はじめる前に

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

手順

展開用のSRV レコードの作成：

オプション	説明
_cisco_uds	Cisco Unified Communications Manager バージョン 9.0 以降の場所を提供します。クライアントは Cisco Unified Communications Manager からサービス プロファイルを取得してオーセンティケータを特定できます。
_collab-edge	Cisco VCS Expressway または Cisco Expressway-E の場所を提供します。クライアントは Cisco Unified Communications Manager からサービス プロファイルを取得してオーセンティケータを特定できます。

SRV レコードの例

```
_cisco_uds._tcp.DOMAIN service location:
priority = 0
weight = 0
port = 8443
svr hostname=192.168.0.26
```

次の作業

SRV レコードのテスト，（96 ページ）

SRV レコードのテスト

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

手順

ステップ 1 コマンド プロンプトを開きます。

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

ステップ 3 set type=SRV と入力します。

ステップ 4 各 SRV レコードの名前を入力します。

例：`_cisco-uds.exampledomain`

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

カスタマイゼーション

Windows のカスタマイゼーション

インストーラ スイッチ：Cisco Jabber for Windows

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

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

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

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

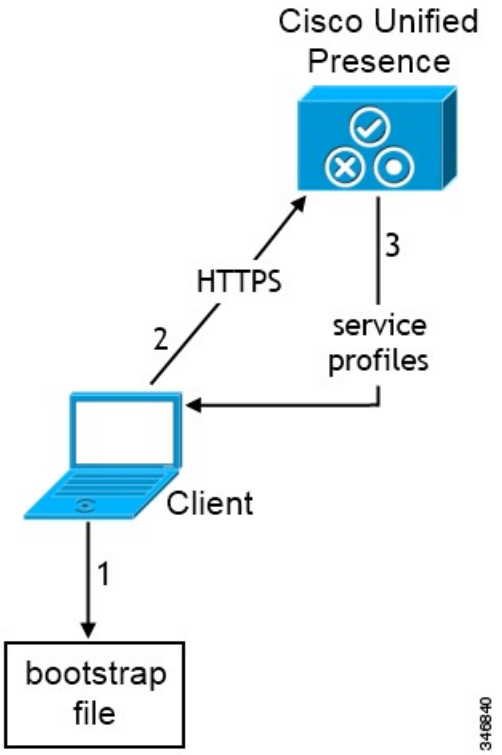
オンプレミスでの展開のブートストラップの設定

次の表は、さまざまな展開タイプの引数値を示します。

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

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

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



ユーザがクライアントを初めて起動する際に、次が実行されます。

1 クライアントは、ブートストラップ ファイルから設定を取得します。

   クライアントが、デフォルト モードで起動して、Cisco Unified Communications Manager IM and Presence サービスがオーセンティケータであると判断します。クライアントは、サービスディスカバリの結果により、その他の指示がなされない限り、プレゼンス サーバのアドレスを取得します。

2 クライアントが Cisco Unified Communications Manager IM and Presence サービスから認証され、設定を取得します。

3 クライアントは、プレゼンス サーバからサービス プロファイルを取得します。

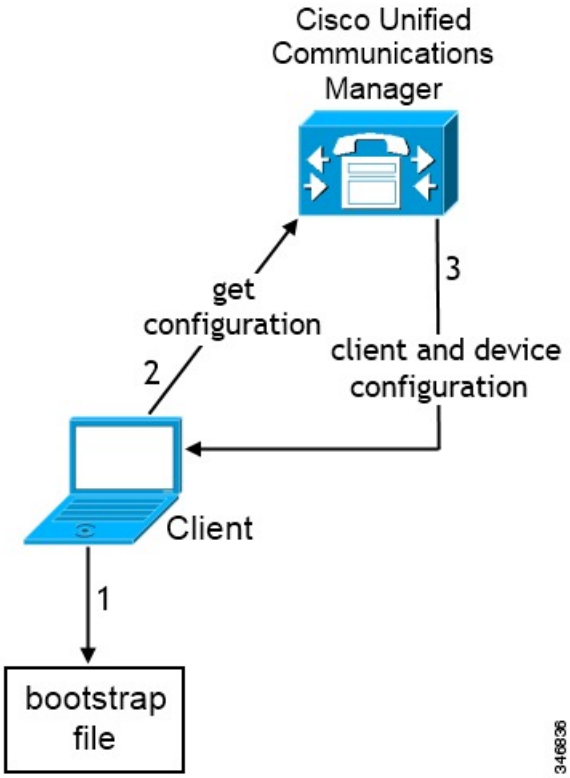
電話モードのオンプレミスの展開におけるブートストラップの設定

インストール中に、次のように引数の値を設定します。

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

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

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



ユーザがクライアントを初めて起動する際に、次プロセスが実行されます。

1 クライアントは、ブートストラップ ファイルから設定を取得します。

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

2 クライアントが Cisco Unified Communications Manager から認証され、設定を取得します。

3 クライアントは、デバイスおよびクライアント設定を取得します。

Mac およびモバイル のカスタマイゼーション

構成 URL ワークフロー

手順

	コマンドまたはアクション	目的
ステップ 1	構成 URL, （100 ページ）	
ステップ 2	Web サイトからの構成 URL のユーザへの提供, （103 ページ）	

構成 URL

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

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

URL に次のパラメータを含めます。

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

- CAS 検索を実行しません。
- 検索：
  - `_cisco-uds`
  - `_cuplogin`
  - `_collab-edge`

- CUCM：この値を設定すると、クライアントは次のように動作します。
  - `_cisco-uds` を検索しません。
  - 検索：
    - `_cuplogin`
    - `_collab-edge`

- CUP：この値を設定すると、クライアントは次のように動作します。
  - `_cuplogin` を検索しません。
  - 検索：
    - `_cisco-uds`
    - `_collab-edge`

カンマで区切った複数の値を指定して、複数のサービスを除外できます。

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

- ServicesDomainSsoEmailPrompt：任意。ユーザのホーム クラスタを決定する際に、ユーザに対して電子メール プロンプトを表示するかどうかを指定します。
  - ON
  - OFF

- EnablePRTEncryption：任意。PRT ファイルの暗号化を指定します。Cisco Jabber for Mac で使用します。
  - true
  - false

- PRTCertificateName：任意。証明書の名前を指定します。Cisco Jabber for Mac で使用します。
- InvalidCertificateBehavior：任意。無効な証明書に対するクライアントの動作を指定します。
  - RejectAndNotify：警告ダイアログが表示され、クライアントはロードされません。

- PromptPerSession：警告ダイアログが表示され、ユーザは無効な証明書を受け入れるか、または拒否できます。

- PRTCertificateUrl：信頼できるルート認証局の証明書ストアにある公開キーを含む証明書の名前を指定します。モバイル クライアント向け Cisco Jabber に適用されます。
- Telephony_Enabled：ユーザに対して電話機能を有効にするかどうかを指定します。デフォルトは true です。
  - 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。構成 URL を作成する際は、次の表記を使用する必要があります。

- `ServicesDomain`
- `VoiceServicesDomain`
- `ServiceDiscoveryExcludedServices`
- `ServicesDomainSsoEmailPrompt`
- `EnablePRTEncryption`
- `PRTCertificateURL`
- `PRTCertificateName`
- `InvalidCertificateBehavior`
- `Telephony_Enabled`
- `ForceLaunchBrowser`

例

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

Web サイトからの構成 URL のユーザへの提供

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

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

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

Web サイトからリンクを配布するには、次の手順を実行します。

手順

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

ステップ 2 内部 Web ページへのリンクを電子メールでユーザに送信します。
その電子メールのメッセージで、次の手順を実行するようにユーザに指示します。

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

企業モビリティ管理によるモバイルの設定

企業モビリティ管理（EMM）を使用する前に、以下を確認してください。

- EMM ベンダーが Android for Work または Apple Managed App Configuration をサポートしている。

- Android デバイスに Android OS 5.0 以降が搭載されているか、iOS デバイスに iOS 8.0 以降が搭載されている。

EMM を使用して、Cisco Jabber for Android や Cisco Jabber for iPhone and iPad に Cisco Jabber を設定することができます。EMM には、URL 設定に代わる方法が用意されています。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。

サポートされる EMM ソフトウェア：

- Airwatch by VMware

手動接続設定

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

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

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

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

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

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

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

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

サービス ディスカバリの自動接続設定

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

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

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

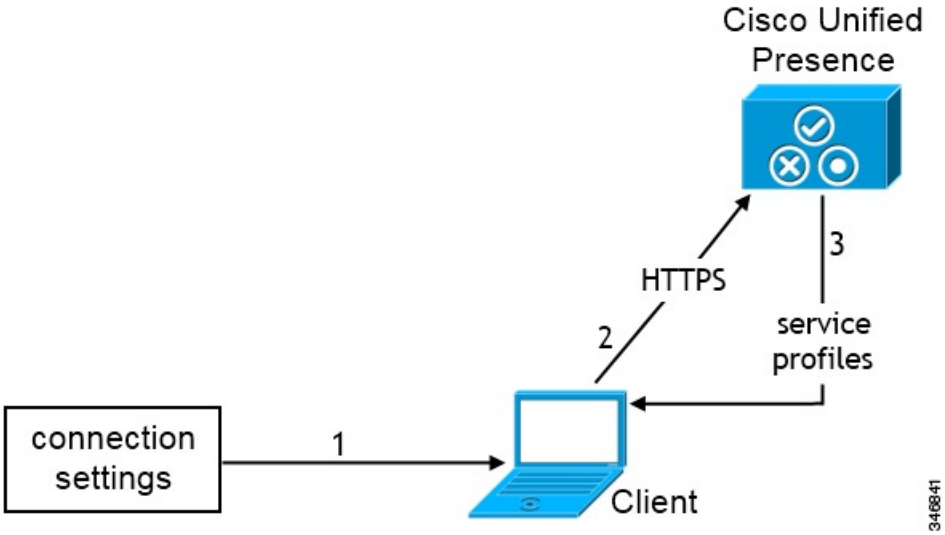
オンプレミスでの展開における手動接続設定

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

メモ

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

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



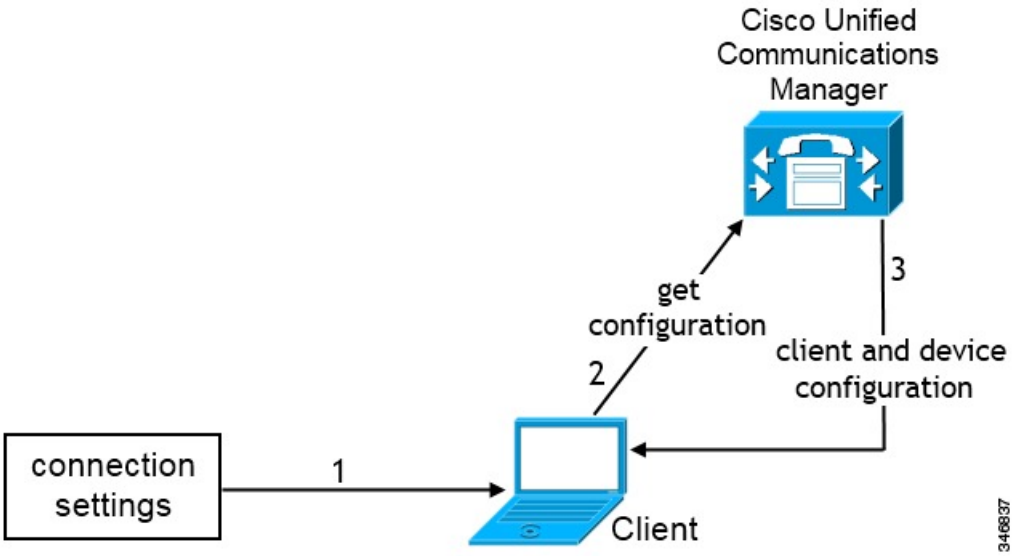
1 ユーザが [詳細設定（Advanced settings）] ウィンドウで手動で接続設定を入力します。
2 クライアントが Cisco Unified Presence または Cisco Unified Communications Manager IM and Presence サービスの認証を受けます。
3 クライアントは、プレゼンス サーバからサービス プロファイルを取得します。

電話モードのオンプレミスの展開における手動接続設定

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

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

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



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

第 13 章

証明書検証の設定

オンプレミス展開用の証明書の設定

証明書は、Jabber クライアントが接続するサービスごとに必要です。

手順

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

	コマンドまたはアクション	目的
ステップ 5	証明書署名要求（CSR）を生成します。	
ステップ 6	サービスに証明書をアップロードします。	マルチサーバSANを使用している場合は、クラスタと tomcat 証明書ごとに一度ずつと クラスタと XMPP 証明書ごとに一度ずつサービスに証明書をアップロードする必要があるだけです。マルチサーバSANを使用していない場合は、すべての Cisco Unified Communications Manager ノードのサービスに証明書をアップロードする必要があります。
ステップ 7	クライアントへの CA 証明書の展開,（108 ページ）	証明書を承認または却下するためのプロンプトを表示せずに証明書の検証が行われることを保証するには、クライアントのローカル証明書ストアに証明書を展開します。

クライアントへの CA 証明書の展開

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

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

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

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

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

手順

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

ステップ 2 Windows マシンで、証明書ファイルを開きます。

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

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

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

次の作業

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

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

手順

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

ステップ 2 Mac マシンで、証明書ファイルを開きます。

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

次の作業

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

モバイル クライアントへの CA 証明書の手動展開

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

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

手順

ステップ 1 CA 証明書をデバイスにダウンロードします。

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

第 14 章

クライアントの設定

クライアント設定のワークフロー

手順

	コマンドまたはアクション	目的
ステップ 1	クライアント設定の概要，（111 ページ）	
ステップ 2	クライアント設定ファイルの作成とホスト，（112 ページ）	
ステップ 3	電話の設定でのパラメータの設定：デスクトップ クライアント向け，（117 ページ）	
ステップ 4	電話の設定でのパラメータの設定：モバイル クライアント向け，（119 ページ）	
ステップ 5	プロキシの設定，（120 ページ）	

クライアント設定の概要

Cisco Jabber は、次のソースから設定を取得できます。

- サービス プロファイル：Cisco Unified Communications Manager リリース 9 以降の UC サービス プロファイルで一部のクライアント設定を構成できます。ユーザがクライアントを起動すると、クライアントは DNS SRV レコードを使用して Cisco Unified Communications Manager ホーム クラスタを検出し、自動的に UC サービス プロファイルから設定を取得します。

  これは、オンプレミス展開にのみ適用されます。

- 電話の設定：Cisco Unified Communications Manager リリース 9 以降の電話の設定で一部のクライアント設定を構成できます。クライアントは、UC サービスプロファイルの設定に加え、電話の設定から設定を取得します。

  これは、オンプレミス展開にのみ適用されます。

- Cisco Unified Communications Manager IM and Presence サービス：インスタント メッセージおよびプレゼンスの機能を有効にして、プレゼンス サブスクリプション要求などの特定の設定を構成できます。

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

  これは、オンプレミス展開にのみ適用されます。

- クライアント コンフィギュレーション ファイル：設定パラメータを含む XML ファイルを作成できます。その後、TFTP サーバで XML ファイルをホストします。ユーザがサインインすると、クライアントは TFTP サーバから XML ファイルを取得して設定を適用します。

  これは、オンプレミス展開およびクラウドベース展開に適用されます。

- Cisco WebEx 管理ツール：Cisco 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 Cisco WebEx 管理ツールにアップロードできます。Cisco WebEx Messenger 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 Cisco WebEx Messenger に接続すると、XML ファイルがダウンロードされ、設定ファイルが適用されます。

  クライアントは、次の順序で設定を行います。

  1. Cisco WebEx Messenger 管理ツールの設定
  2. Cisco WebEx Messenger 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、Cisco WebEx Messenger 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、Cisco 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。

  これは、クラウドベース展開にのみ適用されます。

クライアント設定ファイルの作成とホスト

オンプレミス展開とハイブリッドクラウドベース展開では、クライアントコンフィギュレーション ファイルを作成して、それらを Cisco Unified Communications Manager TFTP サービス上でホストします。

クラウドベース展開では、Cisco 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、Cisco 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。

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

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

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

はじめる前に

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は大文字と小文字が区別されます。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する必要があります。
- 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。コンフィギュレーション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。
- コンフィギュレーション 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、`&` ではなく `&` を使用してください。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は、コンフィギュレーション ファイルが有効です。
  - Internet Explorer に XML 構造の一部しか表示されない場合は、コンフィギュレーション 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, （114 ページ）	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, （115 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, （115 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	コンフィギュレーションファイルのホスティング, （116 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, （117 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。クライアントを設定する最初のステップは、クライアントが設定ファイルにアクセスできるように TFTP サーバのアドレスを指定することです。

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

電話モードでクライアントを展開する場合、TFTP サーバのアドレスを次のように指定できます。

- ユーザはクライアントの起動時に、TFTP サーバ アドレスを手動で入力します。
- TFTP 引数を使用してインストール時に TFTP サーバ アドレスを指定します。
- Microsoft Windows レジストリで 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、ログイン 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。

はじめる前に

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

手順

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

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

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

ステップ 3 TFTP サーバ上でグループ設定ファイルをホストします。
環境内に複数の TFTP サーバが存在する場合は、すべての TFTP サーバのコンフィギュレーション ファイルが同じであることを確認します。

グループ設定の作成

グループ コンフィギュレーション ファイルは、ユーザのサブセットに適用され、Cisco Jabber for desktop（CSF デバイス）上と Cisco Jabber for mobile devices 上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。

はじめる前に

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

手順

ステップ 1 任意のテキスト エディタを使用して XML グループ設定ファイルを作成します。
グループ設定ファイルには、適切な名前を指定できます（例：`jabber-groupa-config.xml`）。

ステップ 2 グループ設定ファイルで必須の設定パラメータを定義します。

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

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

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

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

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

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

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

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

f) [保存（Save）] を選択します。

ステップ 4 TFTP サーバ上でグループ設定ファイルをホストします。

コンフィギュレーション ファイルのホスティング

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 コンフィギュレーション ファイルが存在する Cisco Unified Communications Manager TFTP サーバでコンフィギュレーション ファイルをホストすることをお勧めします。

手順

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

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

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

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

ステップ 5 ファイル システム上の設定ファイルを選択します。

ステップ 6 [ファイルのアップロード（Upload File）] セクションの [ディレクトリ（Directory）] テキスト ボックスに値を指定しないでください。
コンフィギュレーション ファイルが TFTP サーバ上のデフォルト ディレクトリに存在するようにするため、[ディレクトリ（Directory）] テキストボックスには空の値を残す必要があります。

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

TFTP サーバの再起動

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

手順

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

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

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

ステップ 4 [リスタート（Restart）] を選択します。
再起動の確認を求めるウィンドウが表示されます。

ステップ 5 [OK] を選択します。
「Cisco Tftp サービスの再起動操作が成功しました（Cisco Tftp Service Restart Operation was Successful）」というステータスが表示されます。

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

次の作業

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

設定ファイル

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

電話の設定でのパラメータの設定：デスクトップ クライアント向け

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

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

クラスタ全体に適用されます。

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

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

デバイスのグループに適用され、クラスタの設定よりも優先されます。

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

個別の CSF デバイスに適用され、グループの設定よりも優先されます。

電話の設定のパラメータ

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

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

デスクトップ クライアントの設定	説明
電話制御で自動的に開始（Automatically Start in Phone Control）	クライアント初回起動時のユーザの電話タイプを設定します。初回起動後、ユーザは電話タイプを変更できます。クライアントは、ユーザ設定を保存し、以降の起動でその設定を使用します。 **[有効（Enabled）]** 通話にデスクフォン デバイスを使用します。 **[無効（Disabled）]（デフォルト）** 通話にソフトフォン（CSF）デバイスを使用します。
Jabber For Windows ソフトウェア アップデート サーバ URL（Jabber For Windows Software Update Server URL）	クライアント アップデート情報を保持する XML 定義ファイルへの URL を指定します。クライアントは、この URL を使用して Web サーバから XML ファイルを取得します。 ハイブリッドクラウドベース展開では、自動更新を設定するために Cisco WebEx 管理ツール を使用する必要があります。
問題レポート サーバ URL（Problem Report Server URL）	ユーザが問題レポートを送信できるようにするカスタム スクリプトの URL を指定します。

電話の設定でのパラメータの設定：モバイル クライアント向け

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

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

電話の設定のパラメータ

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

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。

プロキシの設定

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します。

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。

Cisco Jabber for Windows のプロキシ設定

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

手順

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

ステップ 2 次のいずれかのオプションを使用してプロキシを設定します。

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

Cisco Jabber for Mac のプロキシ設定

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

手順

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

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

ステップ 3 次のいずれかのオプションを使用してプロキシを設定します。

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

Cisco Jabber iPhone and iPad のプロキシ設定

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

手順

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

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

Cisco Jabber for Android のプロキシ設定

手順

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

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

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

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

第 15 章

Cisco Jabber アプリケーションの展開

Cisco Jabber クライアントのダウンロード

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

手順

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

Cisco Jabber for Windows のインストール

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

インストール オプション	説明
コマンドラインの使用, （124 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, （143 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, （143 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, （148 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。

はじめる前に

ローカル管理者権限でログインする必要があります。

コマンドラインの使用

コマンドライン ウィンドウにインストール引数を指定します。

手順

ステップ 1 コマンドライン ウィンドウを開きます。

ステップ 2 次のコマンドを入力します。

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

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

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

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

インストール コマンドの例

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

Cisco Unified Communications Manager リリース 9.x

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

ここで、

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

コマンドライン引数

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

オーバーライドの引数

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

引数	値	説明
CLEAR	1	クライアントが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、インストール中に引数と設定された値をブートストラップ ファイルに保存します。クライアントは起動時に、ブートストラップ ファイルから設定をローディングします。

CLEAR を指定した場合、インストール中に次が実行されます。

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

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

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

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

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

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

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

モード タイプの引数

次の表は、製品モードを指定するコマンドラインの引数について説明します。

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

製品モードを設定する場合

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

- 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、ご使用の展開により異なります。

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

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

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

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

手順

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

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

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

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

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

IM and Presence を持つユーザのプロビジョニングを行います。

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

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

ステップ 2 ユーザにログアウトをしてから再度ログインするように指示します。
ユーザがクライアントにログインすると、サービス プロファイルの変更を取得し、オーセンティケータにユーザをログインさせます。クライアントは製品モードを決定すると、クライアントを再起動するようユーザに指示します。

ユーザがクライアントを再起動した後、製品モードの変更が完了します。

認証引数

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

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

引数	値	説明
TFTP	IP アドレス ホストネーム FQDN	TFTP サーバのアドレスを指定します。値として次のいずれかを設定します。 • ホスト名（*hostname*） • IP アドレス（*123.45.254.1*） • FQDN（*hostname.domain.com*） Cisco Unified Communications Manager がオーセンティケータとして設定されている場合に、この引数を指定する必要があります。 展開する場合： • 電話モード：クライアントコンフィギュレーションをホスティングする TFTP サーバのアドレスを指定する必要があります。 • デフォルト モード：デバイス設定をホストする Cisco Unified Communications Manager TFTP サービスのアドレスを指定できます。
CTI	IP アドレス ホストネーム 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。

引数	値	説明
CCMCIP	IP アドレス ホストネーム 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。 Cisco Unified Communications Manager リリース 9.x 以前：Cisco Extension Mobility を有効にする場合は、CCMCIP に使用される Cisco Unified Communications Manager ノードで `Cisco Extension Mobility` サービスをアクティブにする必要があります。Cisco Extension Mobility の詳細については、使用している Cisco Unified Communications Manager のリリースに応じた『*Feature and Services*』ガイドを参照してください。
SERVICES_DOMAIN	ドメイン	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	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 の試験導入を実施し、会社のドメインが WebEx に登録されているが、Jabber ユーザが WebEx を使用して認証することは避けたい場合があります。Jabber は CUCM サーバで認証させることにします。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、WEBEX です。 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 が、サービス検出で使用されるユーザのユーザ ID とドメインの検索に使用されます。UPN から検出されたユーザだけが、クライアントにログインできます。 • false：UPN はユーザのユーザ ID とドメインの検索に使用されません。ユーザは、サービス ディスカバリ用のドメインを検索するためのクレデンシャルの入力を要求されます。 インストール コマンドの例：`msiexec.exe /i CiscoJabberSetup.msi /quiet UPN_DISCOVERY_ENABLED=false`

TFTP サーバ アドレス

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

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

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

ただし、デバイス設定を含む TFTP サーバとは異なる TFTP サーバでクライアント設定をホストできます。この場合、2 つの異なる TFTP サーバ アドレスを使用します。一方のアドレスは、デバイス設定をホストする TFTP サーバのアドレスで、もう一方のアドレスは、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。

デフォルトの展開

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

クライアントは、初回起動時に以下を実行します。

1. ブートストラップ ファイルから Cisco Unified Communications Manager TFTP サービスのアドレスを取得します。
2. Cisco Unified Communications Manager TFTP サービスからデバイス設定を取得します。
3. プレゼンス サーバに接続します。
4. プレゼンス サーバの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。

クライアントは、初回起動時に以下を実行します。

1. ブートストラップ ファイルから 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、すべての展開に共通のコマンドライン引数について説明します。

引数	値	説明
LANGUAGE	10 進数の LCID	Cisco Jabber for Windows で使用される言語のロケール ID（LCID）を 10 進数で定義します。値は、サポートされる言語に対応する、10 進数の LCID でなくてはなりません。 たとえば、次のいずれかを指定できます。 • 1033 は英語です。 • 1036 はフランス語です。 指定可能な言語の完全なリストについては、「言語の *LCID*」トピックを参照してください。 この引数は省略可能です。 値を指定しない場合、Cisco Jabber for Windows では現在のユーザの地域言語を使用します。 リリース 11.1(1) 以降では、値を指定しないと、Cisco Jabber for Windows が UseSystemLanguage パラメータの値をチェックします。UseSystemLanguage パラメータが true に設定されている場合は、オペレーティング システムと同じ言語が使用されます。UseSystemLanguage パラメータが false または not defined に設定されている場合、クライアントは現在のユーザの地域言語をデフォルトとして使用します。 地域言語は、[コントロール パネル（Control Panel）] > [地域および言語（Region and Language）] > [日付、時刻、または数字形式の変更（Change the date, time, or number format）] > [形式（Formats）] タブ > [形式（Format）] ドロップダウンで設定します。

引数	値	説明
FORGOT_PASSWORD_URL	URL	ユーザが失ったパスワードまたは忘れたパスワードをリセットできる URL を指定します。 この引数は任意ですが推奨されています。 （注） クラウドベース展開では、Cisco 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。
AUTOMATIC_SIGN_IN	true false	リリース 11.1(1) 以降に適用されます。 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。

引数	値	説明
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 サーバのそ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。
LOGIN_RESOURCE	WBX MUT	複数のクライアントインスタンスへのユーザ サインインを制御します。 デフォルトで、ユーザは同時に Cisco Jabber の複数インスタンスにサインインできます。デフォルトの動作を変更するには、次のいずれかの値を設定します。 • WBX：ユーザは、一度に Cisco Jabber for Windows の 1 つのインスタンスにしかサインインできません。 Cisco Jabber for Windows は、ユーザの JID に `wbxconnect` サフィックスを付加します。ユーザは、`wbxconnect` サフィックスを使用する他の Cisco Jabber クライアントにサインインできません。 • MUT：ユーザは、一度に Cisco Jabber for Windows の 1 つのインスタンスにしかサインインできませんが、同時に他の Cisco Jabber クライアントにサインインできます。 Cisco Jabber for Windows の各インスタンスがユーザの JID に一意のサフィックスを付加します。

引数	値	説明
LOG_DIRECTORY	ローカルファイ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、パス内のスペース文字をエスケープするために引用符を使用します。 `"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`
CLICK2X	DISABLE	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。

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
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。
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。
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、http://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。

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。
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）：DPI 対応が有効になります。 • 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。

言語の LCID

次の表に、Cisco Jabber クライアントがサポートするロケール ID（LCID）または言語 ID（LangID）を示します。

サポートされる言語	Cisco Jabber for Windows	Cisco Jabber for Mac	Cisco Jabber for Android、Cisco Jabber for iPhone and iPad	LCID/LangID
アラビア語（サウジアラビア）	X		X	1025
ブルガリア語（ブルガリア）	X	X		1026
カタロニア語（スペイン）	X	X		1027
簡体字中国語（中国）	X	X	X	2052
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		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

サポートされる言語	Cisco Jabber for Windows	Cisco Jabber for Mac	Cisco Jabber for Android、Cisco Jabber for iPhone and iPad	LCID/LangID
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		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
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		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		1051
スロベニア語（スロベニア）	X	X		1060

サポートされる言語	Cisco Jabber for Windows	Cisco Jabber for Mac	Cisco Jabber for Android、Cisco Jabber for iPhone and iPad	LCID/LangID
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		1055

MSI の手動による実行

インストール プログラムを手動で実行すれば、クライアントの単一のインスタンスをインストールして、[詳細設定（Advanced settings）] ウィンドウで接続設定を指定できます。

手順

ステップ 1 `CiscoJabberSetup.msi` を起動します。
インストール プログラムにより、インストール プロセスのウィンドウが開きます。

ステップ 2 手順に従ってインストール プロセスを完了します。

ステップ 3 Cisco Jabber for Windows を起動します。

ステップ 4 [手動設定およびログイン（Manual setup and sign in）] を選択します。
[詳細設定（Advanced settings）] ウィンドウが開きます。

ステップ 5 接続設定プロパティの値を指定します。

ステップ 6 [保存（Save）] を選択します。

カスタム インストーラの作成

カスタム インストーラを作成するデフォルトのインストール パッケージを変換できます。

（注） カスタム インストーラは Microsoft Orca を使用して作成します。Microsoft Orca は Microsoft Windows SDK for Windows 7 と .NET Framework 4 の一部として入手できます。

Microsoft の Web サイトから、Microsoft Windows SDK for Windows 7 と .NET Framework 4 をダウンロードしてインストールします。

手順

	コマンドまたはアクション	目的
ステップ 1	デフォルト トランスフォーム ファイルの取得, （144 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, （144 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, （145 ページ）	インストーラをカスタマイズするため、トランスフォーム ファイルを適用します。

デフォルト トランスフォーム ファイルの取得

Microsoft Orca でインストール パッケージを修正するためには、デフォルト トランスフォーム ファイルが必要です。

手順

ステップ 1 ソフトウェア ダウンロード ページから Cisco Jabber 管理パッケージをダウンロードします。

ステップ 2 Cisco Jabber 管理パッケージからファイル システムに `CiscoJabberProperties.msi` をコピーします。

次の作業

カスタム トランスフォーム ファイルの作成, （144 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。

はじめる前に

デフォルト トランスフォーム ファイルの取得, （144 ページ）

手順

ステップ 1 Microsoft Orca を起動します。

ステップ 2 `CiscoJabberSetup.msi` を開いてから、`CiscoJabberProperties.msi` を適用します。

ステップ 3 該当するインストーラ プロパティに値を指定します。

ステップ 4 トランスフォーム ファイルを生成して保存します。

a) [トランスフォーム（Transform）] > [トランスフォームの生成（Generate Transform）] を選択します。

b) トランスフォーム ファイルを保存するファイル システムの場所を選択します。

c) トランスフォーム ファイルの名前を指定して [保存（Save）] を選択します。

作成したトランスフォーム ファイルは、*file_name*`.mst` として保存されます。このトランスフォーム ファイルを適用して、`CiscoJabberSetup.msi` のプロパティを変更できます。

次の作業

インストーラの変換, （145 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。

はじめる前に

カスタム トランスフォーム ファイルの作成, （144 ページ）

手順

ステップ 1 Microsoft Orca を起動します。

ステップ 2 Microsoft Orca で `CiscoJabberSetup.msi` を開きます。

a) [ファイル（File）] > [開く（Open）] を選択します。
b) ファイル システム上の `CiscoJabberSetup.msi` の場所を参照します。
c) `CiscoJabberSetup.msi` を選択してから、[開く（Open）] を選択します。

Microsoft Orca でインストール パッケージが開きます。インストーラのテーブルのリストが [テーブル（Tables）] ペインに表示されます。

ステップ 3 1033（英語）以外のすべての言語コードを削除します。

制約事項 カスタム インストーラから 1033（英語）以外のすべての言語コード削除する必要があります。

Microsoft Orcaでは、デフォルト（1033）以外のいずれの言語ファイルもカスタム インストーラで保持されません。カスタムインストーラからすべての言語コードを削除しない場合、言語が英語以外のオペレーティング システムでインストーラを実行できません。

a) [表示（View）] > [要約情報（Summary Information）] を選択します。
[要約情報の編集（Edit Summary Information）] ウィンドウが表示されます。
b) [言語（Language）] フィールドを見つけます。
c) 1033 以外のすべての言語コードを削除します。
d) [OK] を選択します。

英語がカスタム インストーラの言語として設定されます。

ステップ 4 トランスフォーム ファイルを適用します。

a) [トランスフォーム（Transform）] > [トランスフォームの適用（Apply Transform）] を選択します。
b) ファイル システムのトランスフォーム ファイルの場所を参照します。
c) トランスフォーム ファイルを選択し、[開く（Open）] を選択します。

ステップ 5 [テーブル（Tables）] ペインのテーブルのリストから [プロパティ（Property）] を選択します。
`CiscoJabberSetup.msi` のプロパティのリストがアプリケーション ウィンドウの右パネルに表示されます。

ステップ 6 必要とするプロパティの値を指定します。

ヒント 値は大文字と小文字を区別します。このマニュアルの値と一致する値であることを確認します。

ヒント　CLEAR の値を 1 に設定し、以前のインストールからの既存のブートストラップ ファイルを上書きします。既存のブートストラップ ファイルを上書きしない場合、カスタム インストーラで設定する値は有効ではありません。

ステップ 7　必要のないプロパティを削除します。
設定されていないプロパティを削除するのは重要です。削除しないと、設定されたプロパティが有効になりません。必要ない各プロパティを 1 つずつ削除します。

a) 削除するプロパティを右クリックします。
b) [行を削除（Drop Row）] を選択します。
c) Microsoft Orca から続行を要求されたら、[OK] を選択します。

ステップ 8　カスタム インストーラで埋め込みストリームを保存できるようにします。

a) [ツール（Tools）] > [オプション（Options）] を選択します。
b) [データベース（Database）] タブを選択します。
c) [名前を付けて保存（Save As）] の選択時に埋め込みストリームをコピーする（Copy embedded streams during 'Save As'）] を選択します。
d) [適用（Apply）] を選択し、[OK] を選択します。

ステップ 9　カスタム インストーラを保存します。

a) [ファイル（File）] > [名前を付けて変換を保存（Save Transformed As）] を選択します。
b) ファイル システム上の場所を選択してインストーラを保存します。
c) インストーラの名前を指定してから、[保存（Save）] を選択します。

インストーラのプロパティ

以下は、カスタム インストーラで変更できるプロパティです。

- CLEAR
- PRODUCT_MODE
- AUTHENTICATOR
- CUP_ADDRESS
- TFTP
- CTI
- CCMCIP
- LANGUAGE
- TFTP_FILE_NAME
- FORGOT_PASSWORD_URL
- SSO_ORG_DOMAIN
- LOGIN_RESOURCE

- LOG_DIRECTORY
- CLICK2X
- SERVICES_DOMAIN

これらのプロパティは、インストールの引数に対応し、同じ値が設定されています。

グループ ポリシーを使用した導入

Microsoft Windows Server の Microsoft グループ ポリシー管理コンソール（GPMC）を使用して、グループ ポリシーと一緒に Cisco Jabber for Windows をインストールします。

（注） グループ ポリシーと一緒に Cisco Jabber for Windows をインストールするには、Cisco Jabber for Window を展開す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する必要があります。

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, （148 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 ポリシーでのクライアントの展開, （149 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。

手順

ステップ 1 Microsoft Orca を起動します。
Microsoft Orca は、Microsoft の Web サイトからダウンロード可能な Microsoft Windows SDK for Windows 7 と .NET Framework 4 の一部として入手できます。

ステップ 2 `CiscoJabberSetup.msi` を開きます。

a) [ファイル（File）] > [開く（Open）] を選択します。
b) ファイル システム上の `CiscoJabberSetup.msi` の場所を参照します。
c) `CiscoJabberSetup.msi` を選択してから、[開く（Open）] を選択します。

ステップ 3 [表示（View）] > [要約情報（Summary Information）] を選択します。

ステップ 4 [言語（Language）] フィールドを見つけます。

ステップ 5 [言語（Languages）] フィールドを 1033 に設定します。

ステップ 6 [OK] を選択します。

ステップ 7 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。

次の作業

グループ ポリシーでのクライアントの展開, （149 ページ）

グループ ポリシーでのクライアントの展開

グループ ポリシーと Cisco Jabber for Windows を展開するには、このタスクの手順を実行します。

はじめる前に

言語コードの設定, （148 ページ）

手順

ステップ 1 導入のためのソフトウェア配布ポイントにインストール パッケージをコピーします。
Cisco Jabber for Windows を展開する予定のすべてのコンピュータまたはユーザは、配布ポイント上のインストール パッケージにアクセスできる必要があります。

ステップ 2 [スタート（Start）]>[ファイル名を指定して実行（Run）] を選択し、次のコマンドを入力します。
`GPMC.msc`

[グループ ポリシー管理（Group Policy Management）] コンソールが開きます。

ステップ 3 新しいグループ ポリシー オブジェクトを作成します。

a) 左側のペインの適切なドメインを右クリックします。

b) [このドメインに GPO を作成してここにリンクする（Create a GPO in this Domain, and Link it here）] を選択します。
[新しい GPO（New GPO）] ウィンドウが開きます。

c) [名前（Name）] フィールドにグループ ポリシー オブジェクトの名前を入力します。

d) デフォルト値をそのままにするか、[発信元の開始 GPO（Source Starter GPO）] ドロップダウンリストから適切なオプションを選択し、次に [OK] を選択します。
新しいグループ ポリシーが、ドメインのグループ ポリシーのリストに表示されます。

ステップ 4 導入の範囲を設定します。

a) 左側のペインのドメインの下からグループ ポリシー オブジェクトを選択します。
グループ ポリシー オブジェクトが右側のペインに表示されます。

b) [スコープ（Scope）] タブの [セキュリティ フィルタリング（Security Filtering）] セクションで、[追加（Add）] を選択します。
[ユーザ、コンピュータ、またはグループの選択（Select User, Computer, or Group）] ウィンドウが開きます。

c) Cisco Jabber for Windows を導入するコンピュータとユーザを指定します。

ステップ 5 インストール パッケージを指定します。

a) 左側のペインのグループ ポリシー オブジェクトを右クリックして、[編集（Edit）] を選択します。
[グループ ポリシー管理エディタ（Group Policy Management Editor）] が開きます。

b) [コンピュータの設定（Computer Configuration）] を選択して、[ポリシー（Policies）] > [ソフトウェアの設定（Software Settings）] を選択します。

c) [ソフトウェアのインストール（Software Installation）] を右クリックして、[新規（New）] > [パッケージ（Package）] を選択します。

d) [ファイル名（File Name）] の横にインストール パッケージの場所を入力します（例：`\\server\software_distribution`）。

重要 インストール パッケージの場所として Uniform Naming Convention（UNC）パスを入力する必要があります。UNC パスを入力しなかった場合は、グループ ポリシーで Cisco Jabber for Windows を展開できません。

e) インストール パッケージを選択して、[開く（Open）] を選択します。

f) [ソフトウェアの導入（Deploy Software）] ダイアログボックスで、[割り当て済み（Assigned）] を選択し、[OK] を選択します。

グループ ポリシーによって、次回のコンピュータの起動時にコンピュータごとに Cisco Jabber for Windows がインストールされます。

Cisco Media Services Interface

Cisco Jabber for Windows は、Microsoft Windows 7 以降向けの Cisco Media Services Interface バージョン 4.1.2 をサポートします。

Cisco Jabber for Mac は、Cisco Media Services Interface バージョン 4.0.2 以降をサポートします。

デスクフォン ビデオ機能

デスクフォン ビデオ機能を有効にするには、Cisco Media Services Interface をインストールする必要があります。Cisco Media Services Interface は、Cisco Jabber for Windows が以下を実行できるようにするドライバを提供します。

- デスクフォン デバイスを検出します。
- CAST プロトコルを使用してデスクフォン デバイスへの接続を確立して維持します。

Cisco Media Services Interface のインストール

手順

ステップ 1 cisco.com のダウンロード サイトから Cisco Media Services Interface インストール プログラムをダウンロードします。

ステップ 2 Cisco Jabber をインストールする各コンピュータに Cisco Media Services Interface をインストールします。
Cisco Media Services Interface のインストール方法については、該当する Cisco Medianet のマニュアルを参照してください。

Cisco Jabber for Windows のアンインストール

コマンド ラインまたは Microsoft Windows のコントロール パネルを使用して Cisco Jabber for Windows をアンインストールできます。このマニュアルでは、コマンド ラインを使用して Cisco Jabber for Windows をアンインストールする方法について説明します。

インストーラの使用

ファイル システムでインストーラが利用可能な場合は、それを使用して Cisco Jabber for Windows を削除します。

手順

ステップ 1 コマンドライン ウィンドウを開きます。

ステップ 2 次のコマンドを入力します。

```
msiexec.exe /x path_to_CiscoJabberSetup.msi
```

次の例を参考にしてください。

```
msiexec.exe /x C:\Windows\Installer\CiscoJabberSetup.msi /quiet
```

ここで、`/quiet` により、サイレント アンインストールが指定されます。

このコマンドは、コンピュータから Cisco Jabber for Windows を削除します。

製品コードの使用

ファイル システムでインストーラが利用できない場合は、製品コードを使用して Cisco Jabber for Windows を削除します。

手順

ステップ 1 製品コードを検索します。

a) Microsoft Windows レジストリ エディタを開きます。
b) レジストリ キー HKEY_CLASSES_ROOT\Installer\Products を見つけます。
c) [編集（Edit）] > [検索（Find）] を選択します。
d) [検索（Find）] ウィンドウの [検索（Find what）] テキスト ボックスに Cisco Jabber と入力し、[次を検索（Find Next）] を選択します。
e) ProductIcon キーの値を検索します。
製品コードは、ProductIcon キーの値（たとえば、`C:\Windows\Installer\{product_code}\ARPPRODUCTICON.exe`）です。

（注） 製品コードは Cisco Jabber for Windows のバージョンごとに異なります。

ステップ 2 コマンドライン ウィンドウを開きます。

ステップ 3 次のコマンドを入力します。

```
msiexec.exe /x product_code
```

次の例を参考にしてください。

```
msiexec.exe /x 45992224-D2DE-49BB-B085-6524845321C7 /quiet
```

ここで、`/quiet` により、サイレント アンインストールが指定されます。

このコマンドは、コンピュータから Cisco Jabber for Windows を削除します。

Cisco Jabber for Mac のインストール

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

- _collab-edge

カンマで区切った複数の値を指定して、複数のサービスを除外できます。

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

- ServicesDomainSsoEmailPrompt：任意。ユーザのホーム クラスタを決定する際に、ユーザに対して電子メール プロンプトを表示するかどうかを指定します。
  - ON
  - OFF
- EnablePRTEncryption：任意。PRT ファイルの暗号化を指定します。Cisco Jabber for Mac で使用します。
  - true
  - false
- PRTCertificateName：任意。証明書の名前を指定します。Cisco Jabber for Mac で使用します。
- InvalidCertificateBehavior：任意。無効な証明書に対するクライアントの動作を指定します。
  - RejectAndNotify：警告ダイアログが表示され、クライアントはロードされません。
  - PromptPerSession：警告ダイアログが表示され、ユーザは無効な証明書を受け入れるか、または拒否できます。
- Telephony_Enabled：ユーザに対して電話機能を有効にするかどうかを指定します。デフォルトは true です。
  - 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。構成 URL を作成する際は、次の表記を使用する必要があります。

- `ServicesDomain`
- `VoiceServicesDomain`
- `ServiceDiscoveryExcludedServices`
- `ServicesDomainSsoEmailPrompt`
- `EnablePRTEncryption`
- `PRTCertificateURL`
- `PRTCertificateName`
- `InvalidCertificateBehavior`
- `Telephony_Enabled`
- `ForceLaunchBrowser`

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`

Cisco Jabber モバイル クライアントのインストール

手順

ステップ 1 Cisco Jabber for Android をインストールするには、モバイル デバイスで Google Play からアプリケーションをダウンロードします。

ステップ 2 Cisco Jabber for iPhone and iPad をインストールするには、モバイル デバイスで App Store からアプリケーションをダウンロードします。

Cisco Jabber for Android、iPhone、および iPad の URL 設定

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

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

URL には次のパラメータを含めて指定できます。

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

  カンマで区切った複数の値を指定して、複数のサービスを除外できます。

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

- ServicesDomainSsoEmailPrompt：任意。ユーザのホーム クラスタを決定する際に、ユーザに対して電子メール プロンプトを表示するかどうかを指定します。
  - ON
  - OFF
- 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。構成 URL を作成する際は、次の表記を使用します。

- `ServicesDomain`
- `VoiceServicesDomain`
- `ServiceDiscoveryExcludedServices`
- `ServicesDomainSsoEmailPrompt`
- `PRTCertificateURL`
- `InvalidCertificateBehavior`
- `Telephony_Enabled`
- `ForceLaunchBrowser`

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

ユーザが Cisco Jabber for Android または Cisco Jabber for iPhone and iPad を起動できるように、企業モビリティ管理（EMM）を使用して Cisco Jabber を設定できます。

EMM の設定の詳細については、EMM プロバイダーから提供される管理者用の説明書を参照してください。

サポートされる EMM ソフトウェア：AirWatch by VMware

第 16 章

リモート アクセス

サービス検出要件のワークフロー

手順

	コマンドまたはアクション	目的
ステップ 1	サービス検出の要件，（159 ページ）	
ステップ 2	DNS 要件，（160 ページ）	
ステップ 3	証明書の要件，（160 ページ）	
ステップ 4	_collab-edge SRV レコードのテスト，（160 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

リモート アクセスによるサービス検出のための DNS 要件は次のとおりです。

- 外部 DNS サーバで `_collab-edge` DNS SRV レコードを設定します。
- 内部ネーム サーバで `_cisco-uds` DNS SRV レコードを設定します。
- オプションで、IM and Presence サーバのドメインが音声サーバのドメインと異なるハイブリッド クラウド ベース アーキテクチャを展開する場合は、`_collab-edge` レコードを含む DNS サーバを検索するように音声サービス ドメインを設定するようにします。

証明書の要件

リモート アクセスを設定する前に、Cisco VCS Expressway と Cisco Expressway-E のサーバ証明書をダウンロードします。このサーバ証明書は、HTTP と XMPP の両方に使用されます。

Cisco VCS Expressway 証明書の設定の詳細については、『Configuring Certificates on Cisco VCS Expressway』を参照してください。

_collab-edge SRV レコードのテスト

SRV レコードのテスト

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

手順

ステップ 1 コマンド プロンプトを開きます。

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

ステップ 3 set type=SRV と入力します。

ステップ 4 各 SRV レコードの名前を入力します。
例：`_cisco-uds.exampledomain`

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

Cisco AnyConnect 展開のワークフロー

手順

	コマンドまたはアクション	目的
ステップ 1	アプリケーション プロファイル, （161 ページ）	
ステップ 2	VPN 接続の自動化, （162 ページ）	
ステップ 3	AnyConnect の参照ドキュメント, （166 ページ）	
ステップ 4	セッション パラメータ, （166 ページ）	

Cisco AnyConnect の導入

アプリケーション プロファイル

Cisco AnyConnect セキュア モビリティ クライアントをデバイスにダウンロードした後で、ASA はこのアプリケーションに対してコンフィギュレーション プロファイルをプロビジョニングする必要があります。

Cisco AnyConnect セキュア モビリティ クライアントのコンフィギュレーション プロファイルには、会社の ASA VPN ゲートウェイ、接続プロトコル（IPSec または SSL）、オンデマンド ポリシーなどの VPN ポリシー情報が含まれています。

次のいずれかの方法で、Cisco Jabber for iPhone and iPad のアプリケーション プロファイルをプロビジョニングすることができます。

ASDM

ASA Device Manager（ASDM）のプロファイル エディタを使用して、Cisco AnyConnect セキュア モビリティ クライアントの VPN プロファイルを定義することをお勧めします。

この方法を使用すると、Cisco AnyConnect セキュア モビリティ クライアントが初めて VPN 接続を確立した以降は、VPN プロファイルが自動的にそのクライアントにダウンロードされます。この方法は、すべてのデバイスおよび OS タイプに使用でき、VPN プロファイルを ASA で集中管理できます。

詳細については、ご使用のリリースの『*Cisco AnyConnect Secure Mobility Client Administrator Guide*』の「*Creating and Editing an AnyConnect Profile*」のトピックを参照してください。

iPCU

iPhone Configuration Utility（iPCU）を使用して作成する Apple コンフィギュレーション プロファイルを使用して iOS デバイスをプロビジョニングできます。Apple コンフィギュレーション プロ

ファイルは、デバイスのセキュリティ ポリシー、VPN コンフィギュレーション情報、および Wi-Fi、メール、カレンダーの各種設定などの情報が含まれた XML ファイルです。

高レベルな手順は次のとおりです。

1. iPCU を使用して、Apple コンフィギュレーション プロファイルを作成します。

   詳細については、iPCU の資料を参照してください。

2. XML プロファイルを .mobileconfig ファイルとしてエクスポートします。

3. .mobileconfig ファイルをユーザにメールで送信します。

   ユーザがこのファイルを開くと AnyConnect VPN プロファイルと他のプロファイル設定がクライアント アプリケーションにインストールされます。

MDM

サード パーティの Mobile Device Management（MDM）ソフトウェアを使用して作成する Apple コンフィギュレーションプロファイルを使用して iOS デバイスをプロビジョニングできます。Apple コンフィギュレーションプロファイルは、デバイスのセキュリティポリシー、VPN コンフィギュレーション情報、および Wi-Fi、メール、カレンダーの各種設定などの情報が含まれた XML ファイルです。

高レベルな手順は次のとおりです。

1. Apple 設定プロファイルを作成するには MDM を使用します。

   MDM の使用についての詳細は Apple の資料を参照してください。

2. 登録済みデバイスに Apple 設定プロファイルをプッシュします。

Cisco Jabber for Android のアプリケーション プロファイルをプロビジョニングするには、ASA Device Manager（ASDM）のプロファイル エディタを使用して、Cisco AnyConnect セキュア モビリティ クライアントの VPN プロファイルを定義します。Cisco AnyConnect セキュア モビリティ クライアントが初めて VPN 接続を確立した以降は、VPN プロファイルが自動的にそのクライアントにダウンロードされます。この方法は、すべてのデバイスおよび OS タイプに使用でき、VPN プロファイルを ASA で集中管理できます。詳細については、ご使用のリリースの『*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 for 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 が自動的に信頼ネットワークの外側にいることを検出します。この状況が発生すると、Cisco AnyConnect セキュア モビリティ クライアントは UC インフラストラクチャへの接続を確保するため VPN を開始します。

（注） Trusted Network Detection 機能には、証明書ベース認証およびパスワード ベース認証の両方を使用できます。ただし、証明書ベース認証の方が、よりシームレスな体感を与えることができます。

手順

ステップ 1 ASDM を使用して、Cisco AnyConnect のクライアント プロファイルを開きます。

ステップ 2 クライアントが社内 Wi-Fi ネットワークの中にいるときにインターフェイスで受信可能な、信頼できる DNS サーバおよび信頼できる DNS ドメイン サフィックスのリストを入力します。Cisco AnyConnect クライアントは、現在のインターフェイス DNS サーバおよびドメイン サフィックスを、このプロファイルの設定と比較します。

（注） Trusted Network Detection 機能が正しく動作するためには、DNS サーバをすべて指定する必要があります。TrustedDNSDomains と TrustedDNSServers の両方をセットアップした場合は、信頼ネットワークとして定義した両方の設定とセッションが一致する必要があります。

Trusted Network Detection をセットアップするための詳細な手順については、ご使用のリリースの『*Cisco AnyConnect Secure Mobility Client Administrator Guide*』の「*Configuring AnyConnect Features*」の章（リリース 2.5）または「*Configuring VPN Access*」の章（リリース 3.0 または 3.1）の「*Trusted Network Detection*」のセクションを参照してください。

Connect On Demand VPN の設定

Apple iOS Connect On Demand 機能は、ユーザのドメインに基づいて VPN 接続を自動化することにより、ユーザ エクスペリエンスを強化します。

ユーザが社内 Wi-Fi ネットワークの中にいる場合、Cisco Jabber は直接 Cisco UC インフラストラクチャに到達できます。ユーザが企業の Wi-Fi ネットワーク外に出ると、Cisco AnyConnect は、AnyConnect クライアント プロファイルで指定されたドメインに接続されているか自動的に検出します。その場合、アプリケーションは VPN を開始して、UC インフラストラクチャへの接続を確認します。Cisco Jabber を含めて、デバイス上のすべてのアプリケーションがこの機能を利用できます。

（注） Connect On Demand は、証明書で認証された接続だけをサポートします。

この機能では、次のオプションを使用できます。

- [常に接続（Always Connect）]：Apple iOS は、常にこのリスト内のドメインへの VPN 接続を開始しようとします。
- [必要に応じて接続（Connect If Needed）]：Apple iOS は、DNS を使用してアドレスを解決できない場合のみ、このリスト内のドメインへの VPN 接続を開始しようとします。
- [接続しない（Never Connect）]：Apple iOS は、このリスト内のドメインへの VPN 接続を開始しようとしません。

注目 Apple は近い将来に、[常に接続する（Always Connect）] オプションを削除する予定です。[常に接続する（Always Connect）] オプションの削除後は、ユーザは [必要に応じて接続する（Connect if Needed）] オプションを選択できます。Cisco Jabber ユーザが [必要に応じて接続（Connect if Needed）] オプションを使用したときに問題が発生する場合があります。たとえば、Cisco Unified Communications Manager のホスト名が社内ネットワークの外部で解決可能な場合は、iOS が VPN 接続をトリガーしません。ユーザは、コールを発信する前に、手動で Cisco AnyConnect セキュア モビリティ クライアントを起動することによって、この問題を回避できます。

手順

ステップ 1 ASDM プロファイル エディタ、iPCU、または MDM ソフトウェアを使用して、AnyConnect クライアント プロファイルを開きます。

ステップ 2 AnyConnect クライアント プロファイルの [必要に応じて接続する（Connect if Needed）] セクションで、オンデマンド ドメインのリストを入力します。
ドメイン リストは、ワイルドカード オプション（たとえば、cucm.cisco.com、cisco.com、および *.webex.com）を含むことができます。

Cisco Unified Communications Manager での自動 VPN アクセスのセットアップ

はじめる前に

- モバイル デバイスで、証明書ベースの認証での VPN へのオンデマンド アクセスが設定されている必要があります。VPN アクセスの設定については、VPN クライアントおよびヘッドエンドのプロバイダーにお問い合わせください。
- Cisco AnyConnect セキュア モビリティ クライアントと Cisco Adaptive Security Appliance の要件については、「ソフトウェア要件」のトピックを参照してください。
- Cisco AnyConnect のセットアップ方法については、『*Cisco AnyConnect VPN Client Maintain and Operate Guides*』を参照してください。

手順

ステップ 1 クライアントがオンデマンドで VPN を起動する URL を指定します。

a) 次のいずれかの方法を使用し、クライアントがオンデマンドで VPN を起動する URL を指定します。

- 必要に応じて接続する（Connect if Needed）
  - Cisco Unified Communications Manager をドメイン名（IP アドレスではなく）経由でアクセスするように設定し、このドメイン名がファイアウォールの外側で解決できないことを確認します。
  - Cisco AnyConnect クライアント接続の Connect on Demand ドメイン リストで、このドメインを「必要に応じて接続（Connect If Needed）」リストに追加します。
- 常に接続する（Always Connect）
  - 存在しないドメインにステップ 4 のパラメータを設定します。存在しないドメインはユーザがファイアウォールの内部または外部にいるときに、DNS クエリーが失敗する原因となります。
  - Cisco AnyConnect クライアント接続の Connect on Demand ドメイン リストで、このドメインを“常に接続（Always Connect）”リストに追加します。

    URL は、ドメイン名だけを含む必要があります。プロトコルまたはパスは含めないでください（たとえば、「https://cm8ondemand.company.com/vpn」の代わりに「cm8ondemand.company.com」を使用します）。

b) Cisco AnyConnect で URL を入力し、このドメインに対する DNS クエリーが失敗することを確認します。

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

ステップ 3 ユーザのデバイス ページに移動します。

ステップ 4 [プロダクト固有の設定（Product Specific Configuration Layout）] セクションの [オンデマンドVPNのURL（On-Demand VPN URL）] フィールドに、ステップ 1 で Cisco AnyConnect で特定して使用した URL を入力します。
URL は、ドメイン名だけを含む必要があります。プロトコルやパスを含まないようにしてください。

ステップ 5 [保存（Save）] を選択します。
Cisco Jabber が開くと、URL への DNS クエリーを開始します（たとえば、ccm-sjc-111.cisco.com）。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。

次の作業

- この機能をテストしてください。
  - この URL を iOS デバイスのインターネット ブラウザに入力し、VPN が自動的に起動することを確認します。ステータス バーに、VPN アイコンが表示されます。
  - VPNを使用して、iOSデバイスが社内ネットワークに接続できることを確認します。たとえば、社内イントラネットのWebページにアクセスしてください。iOSデバイスが接続できない場合は、ご利用の VPN 製品のプロバイダーに問い合わせてください。
  - VPNが特定のタイプのトラフィックへのアクセスを制限（管理者が電子メールと予定表のトラフィックだけが許可されるようにシステムを設定している場合など）していないことを IT 部門に確認します。
- クライアントが、社内ネットワークに直接接続されるように設定されていることを確認します。

AnyConnect の参照ドキュメント

AnyConnect の要件と展開の詳細については、次の場所にある、ご使用のリリースに対応したドキュメントを参照してください。 http://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-user-guide-list.html

セッション パラメータ

セキュア接続のパフォーマンスを向上するために ASA セッション パラメータを設定できます。最良のユーザ エクスペリエンスを得るために、次の ASA セッション パラメータを設定する必要があります。

- [Datagram Transport Layer Security]（DTLS）：DTLS は、遅延とデータ消失を防ぐデータ パスを提供する SSL プロトコルです。
- [自動再接続（Auto Reconnect）]：自動再接続またはセッション永続性を使用すれば、Cisco AnyConnect Secure Mobility Client はセッション中断から回復して、セッションを再確立できます。
- [セッション永続性（Session Persistence）]：このパラメータを使用すると、VPN セッションをサービス中断から回復し、接続を再確立できます。
- [アイドルタイムアウト（Idle Timeout）]：アイドル タイムアウトは、通信アクティビティが発生しない場合に、ASA がセキュア接続を切断するまでの期間を定義します。
- [デッドピア検出（Dead Peer Detection）]（DTD）：DTD は、ASA と Cisco AnyConnect Secure Mobility Client が、障害が発生した接続をすばやく検出できることを保証します。

ASA セッション パラメータの設定

Cisco AnyConnect Secure Mobility Client のエンドユーザのユーザ エクスペリエンスを最適化するために、次のように ASA セッション パラメータを設定することを推奨します。

手順

ステップ 1 DTLS を使用するように、Cisco AnyConnect を設定します。
詳細については、『*Cisco AnyConnect VPN Client Administrator Guide, Version 2.0*』の「*Configuring AnyConnect Features Using ASDM*」の章の、「*Enabling Datagram Transport Layer Security (DTLS) with AnyConnect (SSL) Connections*」のトピックを参照してください。

ステップ 2 セッションの永続性（自動再接続）を設定します。

a) ASDM を使用して VPN クライアント プロファイルを開きます。
b) [自動再接続の動作（Auto Reconnect Behavior）] パラメータを [復帰後に再接続（Reconnect After Resume）] に設定します。

詳細については、ご使用のリリースの『*Cisco AnyConnect Secure Mobility Client Administrator Guide*』の「*Configuring AnyConnect Features*」の章（リリース 2.5）または「*Configuring VPN Access*」の章（リリース 3.0 または 3.1）の「*Configuring Auto Reconnect*」のトピックを参照してください。

ステップ 3 アイドル タイムアウト値を設定します。

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

詳細については、ご使用のリリースの『*Cisco ASA 5580 Adaptive Security Appliance Command Reference*』の「*vpn-idle-timeout*」のセクションを参照してください。

ステップ 4 Dead Peer Detection（DPD）を設定します。

a) サーバ側の DPD を無効にします。
b) クライアント側の DPD を有効にします。

詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6*』の「*Configuring VPN*」の章の、「*Enabling and Adjusting Dead Peer Detection*」のトピックを参照してください。

第 17 章

Quality of Service

オプション

Cisco Jabber の Quality of Service を設定するには、次のオプションを使用します。

- サポートされるコーデック，（170 ページ）
- SIP プロファイルでのポート範囲の定義，（171 ページ）
- Jabber-config.xml でのポート範囲の定義，（172 ページ）
- DSCP 値の設定，（172 ページ）

サポートされるコーデック

タイプ	コーデック	コーデック タイプ	Cisco Jabber for Android	Cisco Jabber for iPhone and iPad	Cisco Jabber for Mac	Cisco Jabber for Windows
[音声（Audio）]	G.711	A-law	○ 通常モードをサポートします。		○	
		μ-law/Mu-law	○ 通常モードをサポートします。		○	
	G.722		○		○	
	G.722.1	24 kb/s および 32 kb/s	○ 通常モードをサポートします。		○	
	G.729		G.729 でのビジュアルボイスメールはサポートされていませんが、ユーザはG.729 と [ボイスメールに発信（Call Voicemail）] 機能を使用してボイスメッセージにアクセスできます。		なし	
	G.729a		○ 狭帯域幅で使用するための最小要件です。 狭帯域幅モードをサポートするコーデックだけです。 通常モードをサポートします。		○	
	Opus		○		○	

タイプ	コーデック	コーデック タイプ	Cisco Jabber for Android	Cisco Jabber for iPhone and iPad	Cisco Jabber for Mac	Cisco Jabber for Windows
[ビデオ（Video）]	H.264/AVC		○		○	
[ボイスメール（Voicemail）]	G.711	A-law	○		なし	
		μ-law/Mu-law（デフォルト）	○		なし	
	GSM 6.10		○		なし	
	PCM リニア		○		なし	

Cisco Jabber for Android または Cisco Jabber for iPhone and iPad の使用中に音声品質に問題が発生した場合は、クライアント設定で狭帯域幅モードのオンとオフを切り替えることができます。

SIP プロファイルでのポート範囲の定義

クライアントは、ポート範囲を使用して、ネットワークに RTP トラフィックを送信します。また、クライアントは、ポート範囲を均等に分割して、下半分を音声コール用に、上半分をビデオコール用に使用します。オーディオメディアおよびビデオメディアのポート範囲を分割する結果として、クライアントにより識別可能なメディア ストリームが作成されます。IP パケットのヘッダー内の DSCP 値を設定することで、それらのメディア ストリームを分類し、優先させることができます。

手順

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

ステップ 2 [デバイス（Device）] > [デバイスの設定（Device Settings）] > [SIP プロファイル（SIP Profile）] の順に選択します。

ステップ 3 適切な SIP プロファイルを検索するか、新しい SIP プロファイルを作成します。
[SIP プロファイルの設定（SIP Profile Configuration）] ウィンドウが開きます。

ステップ 4 音声とビデオのポート範囲を共通にするか分離するかを指定します。音声とビデオのポート範囲を分離する場合は、音声ポートとビデオ ポートを設定します。次のフィールドにポート範囲を指定してください。

- [開始メディアポート（Start Media Port）]：メディア ストリームの開始ポートを定義します。このフィールドは、範囲の最小ポートを設定します。

- [終了メディアポート（Stop Media Port）]：メディア ストリームの終了ポートを定義します。このフィールドは、範囲の最大ポートを設定します。

ステップ 5 [設定の適用（Apply Config）] を選択し、[OK] をクリックします。

Jabber-config.xml でのポート範囲の定義

このトピックは、Cisco Jabber for Windows に適用されます。

手順

ユーザがCisco Jabber for Windows のチャット ウィンドウで画面を共有するときに使用すべきポート範囲を指定するには、『*Cisco Jabber Parameters Reference Guide*』の「SharePortRangeStart」を参照してください。

DSCP 値の設定

ネットワークを通過する Cisco Jabber トラフィックに優先順位を付ける場合に、RTP メディア パケット ヘッダーで DiffServ コード ポイント（DSCP）値を設定します。

Cisco Unified Communications Manager での DSCP 値の設定

Cisco Unified Communications Manager で音声メディアとビデオ メディアの DSCP 値を設定できます。そうすれば、Cisco Jabber は、デバイス設定から DSCP 値を取得して、それらを RTP メディア パケットの IP ヘッダーに直接適用できます。

制約事項 Microsoft Windows 7 などの新しいオペレーティング システムには、アプリケーションで IP パケット ヘッダーの DSCP 値が設定できないようにするセキュリティ機能が実装されています。そのため、Microsoft グループ ポリシーなどの DSCP 値をマーキングするための代替方式を使用する必要があります。

フレキシブル DSCP 値の設定の詳細については、『Configure Flexible DSCP Marking and Video Promotion Service Parameters』を参照してください。

手順

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

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

[サービス パラメータ設定（Service Parameter Configuration）] ウィンドウが開きます。

ステップ 3 適切なサーバを選択してから、[Cisco CallManager（Cisco CallManager）] サービスを選択します。

ステップ 4 [クラスタ全体のパラメータ（システム：QOS）（Clusterwide Parameters (System - QOS)）] セクションを見つけます。

ステップ 5 適切な DSCP 値を設定し、[保存（Save）] を選択します。

グループ ポリシーを用いた DSCP 値の設定

Microsoft Windows 7 などの新しいオペレーティング システム上で Cisco Jabber for Windows を展開する場合は、Microsoft グループ ポリシーを使用して DSCP 値を適用できます。

グループ ポリシーを作成するには、Microsoft 社のサポート技術情報に記載されている次の手順を実行します。 http://technet.microsoft.com/en-us/library/cc771283%28v=ws.10%29.aspx

次の属性を用いて音声メディアとビデオ メディアに別々のポリシーを作成する必要があります。

属性	音声ポリシー	ビデオ ポリシー	シグナリング ポリシー
アプリケーション名	`CiscoJabber.exe`	`CiscoJabber.exe`	`CiscoJabber.exe`
プロトコル	UDP	UDP	TCP
ポート番号または範囲	Cisco Unified Communications Manager 上の SIP プロファイルからの対応するポート番号または範囲。	Cisco Unified Communications Manager 上の SIP プロファイルからの対応するポート番号または範囲。	SIP は 5060 安全な SIP の場合は 5061
DSCP 値	46	34	24

クライアントの DSCP 値の設定

一部の構成には、Cisco Jabber for Mac クライアントとモバイル クライアント用 Cisco Jabber のコールで Diffserv を有効にするオプションがあります。

重要 このオプションは、デフォルトで有効です。シスコは、次のシナリオで問題が発生しない限り、このオプションを無効にしないことを推奨します。

- 他の参加者の声を聞いたり、姿を確認できるが、自分の声や姿は確認されない。
- 予期しない Wi-Fi 接続問題が発生している。

コールの Diffserv を無効にすると、オーディオやビデオの品質が低下する可能性があります。

（注） EnableDSCPPacketMarking を true または false に設定すると、Cisco Jabber クライアントで [コールの Diffserv の有効化（Enable Differentiated Service for Calls）] が表示されません。

手順

ステップ 1 Cisco Jabber for Mac で、[Jabber] > [設定（Preferences）] > [コール（Calls）] > [詳細（Advanced）] に移動し、[コールの Diffserv の有効化（Enable Differentiated Service for Calls）] を選択します。

ステップ 2 モバイル クライアント用 Cisco Jabber で、[Jabber] > [設定（Settings）] > [オーディオとビデオ（Audio and Video）] に移動し、[コールの Diffserv の有効化（Enable Differentiated Service for Calls）] を選択します。

ネットワーク内の DSCP 値の設定

スイッチおよびルータを設定し、RTP メディアの IP ヘッダーで DSCP 値をマーキングします。

ネットワーク内の DSCP 値を設定するには、クライアント アプリケーションからの異なるストリームを識別する必要があります。

- メディア ストリーム：クライアントは音声ストリームとビデオ ストリームに別々のポート範囲を使用するため、それらのポート範囲に基づいて音声メディアとビデオメディアを区別できます。SIP プロファイルのデフォルトのポート範囲を使用して、次のようにメディア パケットをマーキングする必要があります。
  - 音声メディアは、EF として、16384 ～ 24574 のポートでストリーミング
  - ビデオ メディアは、AF41 として、24575 ～ 32766 のポートでストリーミング
- シグナリング ストリーム：SIP、CTI QBE、および XMPP に必要なさまざまなポートに基づいて、クライアントとサーバ間のシグナリングを識別できます。たとえば、Cisco Jabber と Cisco Unified Communications Manager 間の SIP シグナリングはポート 5060 を介して行われます。

AF31 としてシグナリング パケットをマーキングする必要があります。

第 18 章

Cisco Jabber のアプリケーションとの統合

Microsoft SharePoint 2010 および 2013 でのプレゼンスの設定

IM アドレスがメール アドレスと異なる状況で組織がユーザのプロファイルを定義する場合は、クライアントと Microsoft SharePoint 2010 および 2013 の間でプレゼンス統合を有効にする追加設定が必要になります。

はじめる前に

- Cisco Jabber for Windows クライアント専用。
- すべてのサイトが Microsoft SharePoint Central Administration（CA）と同期していることを確認します。
- Microsoft SharePoint と Active Directory 間の同期がセットアップされていることを確認します。

手順

ステップ 1 Microsoft SharePoint 2013 を使用している場合は、次の情報でユーザの SharePoint CA プロファイル ページを更新します。

a) [SIPアドレス（SIP Address）] プロファイル フィールドを空白のままにします。

b) [勤務先電子メール（Work email）] プロファイル フィールドに、ユーザ プロファイルを入力します。たとえば、john4mail@example.pst と入力します。

ステップ 2 Microsoft SharePoint 2010 を使用している場合は、次の情報でユーザの SharePoint CA プロファイル ページを更新します。

a) [SIPアドレス（SIP Address）] プロファイル フィールドに、ユーザ プロファイルを入力します。たとえば、john4mail@example.pst と入力します。

b) [勤務先電子メール（Work email）] プロファイル フィールドを空白のままにします。

クライアントのアベイラビリティ

ユーザは、クライアントの [オプション（Options）] ウィンドウの [ステータス（Status）] タブで自分たちがミーティング中であることを第三者に知らせるためのオプションを設定することによって、自分たちのアベイラビリティが予定表イベントに影響するかどうかを定義できます。このオプションは、予定表内のイベントとユーザのアベイラビリティを同期させます。クライアントには、サポートされている統合カレンダーの [ミーティング中（In a meeting）] アベイラビリティしか表示されません。

クライアントは、[ミーティング中（In a meeting）] アベイラビリティに関する次の 2 つのソースの使用をサポートします。

（注） モバイル クライアント用 Cisco Jabber では、このミーティング統合はサポートされていません。

- Microsoft Exchange と Cisco Unified Communication Manager IM and Presence の統合：オンプレミス展開に適用されます。Cisco Unified Presence の [マイ プレゼンス ステータスをカレンダー情報に包含する（Include Calendar information in my Presence Status）] フィールドとクライアントの [ミーティング中（In a meeting）] オプションは同じものです。両方のフィールドが Cisco Unified Communication Manager IM and Presence データベース内の同じ値を更新します。

  ユーザが両方のフィールドを別々の値で設定した場合は、最後に設定したフィールドが優先されます。クライアントが実行されている際に、ユーザが [マイ プレゼンス ステータスをカレンダー情報に包含する（Include Calendar information in my Presence Status）] フィールドの値を変更すると、ユーザはその変更を適用させるためにクライアントを再起動する必要があります。

- Cisco Jabber クライアント：オンプレミス展開とクラウドベース展開に適用されます。[ミーティング中（In a meeting）] アベイラビリティを設定するには、クライアントの Cisco Unified Communication Manager IM and Presence と Microsoft Exchange の統合を無効にする必要があります。クライアントは、Cisco Unified Communication Manager IM and Presence と Microsoft Exchange 間の統合がオンなのか、オフなのかをチェックします。また、クライアントは、統合がオフの場合にだけアベイラビリティを設定できます。

次の展開シナリオで、アベイラビリティの作成方法について説明します。

導入シナリオ	[ミーティング中（個人用のカレンダーより）（In a meeting (according to my calendar)）] を選択します。	[ミーティング中（個人用のカレンダーより）（In a meeting (according to my calendar)）] を選択しません。
Cisco Unified Communication Manager IM and Presence と Microsoft Exchange 間の統合を有効にする	Cisco Unified Communication Manager IM and Presence によってアベイラビリティ ステータスが設定されます。	アベイラビリティ ステータスは変更されません。
Cisco Unified Communication Manager IM and Presence と Microsoft Exchange 間の統合を有効にしない	クライアントにより、アベイラビリティ ステータスが設定されます。	アベイラビリティ ステータスは変更されません。
クラウドベース展開	クライアントにより、アベイラビリティ ステータスが設定されます。	アベイラビリティ ステータスは変更されません。

また、次の表に、展開シナリオ別にサポートされるアベイラビリティの説明を示します。

クライアントで有効にされたアベイラビリティ	Cisco Unified Communication Manager IM and Presence と Microsoft Exchange の統合によって有効にされたアベイラビリティ
[オフライン（ミーティング中）（Offline in a meeting）] アベイラビリティはサポートされません。	[オフライン（ミーティング中）（Offline in a meeting）]アベイラビリティがサポートされます。
非予定表イベントに対して [ミーティング中（In a meeting）] アベイラビリティがサポートされます。	非予定表イベントに対して [ミーティング中（In a meeting）] アベイラビリティはサポートされません。
（注） [オフライン（ミーティング中）（Offline in a meeting）] アベイラビリティは、ユーザがクライアントにログインしていないが、ユーザの予定表にイベントが存在していることを意味します。 非予定表イベントとは、インスタント ミーティング、[オフライン（Offline）]、[電話中（On a call）]などのユーザの予定表に表示されないイベントを意味します。	

プロトコル ハンドラ

Cisco Jabber は、次のプロトコル ハンドラをオペレーティング システムに登録し、クリックツーコールまたはクリックツー IM 機能を Web ブラウザやその他のアプリケーションから使用できるようにします。

- XMPP: または XMPP://

  Cisco Jabber でインスタント メッセージを開始し、チャット ウィンドウを開きます。

- IM: または IM://

  Cisco Jabber でインスタント メッセージを開始し、チャット ウィンドウを開きます。

- TEL: または TEL://

  Cisco Jabber で音声またはビデオ コールを開始します。

  （注） TEL は Apple 純正の電話機に登録されます。Cisco Jabber for iPhone and iPad を相互起動するために使用することはできません。

- CISCOTEL: または CISCOTEL://

  Cisco Jabber で音声またはビデオ コールを開始します。

- SIP: または SIP://

  Cisco Jabber で音声またはビデオ コールを開始します。

- CLICKTOCALL: または CLICKTOCALL://
  Cisco Jabber で音声またはビデオ コールを開始します。

プロトコル ハンドラのレジストリ エントリ

プロトコル ハンドラとして登録するために、クライアントが Microsoft Windows レジストリの次の場所に書き込みます。

- `HKEY_CLASSES_ROOT\tel\shell\open\command`
- `HKEY_CLASSES_ROOT\xmpp\shell\open\command`
- `HKEY_CLASSES_ROOT\im\shell\open\command`

2 つ以上のアプリケーションが同一プロトコルのハンドラとして登録される場合は、レジストリに最後に書き込まれたアプリケーションが優先されます。たとえば、Cisco Jabber が XMPP: のプロトコル ハンドラとして登録された後に別のアプリケーションが XMPP: のプロトコル ハンドラとして登録された場合は、別のアプリケーションの方が Cisco Jabber より優先されます。

HTML ページのプロトコル ハンドラ

HTML ページに、href 属性の一部としてプロトコル ハンドラを追加します。HTML ページに表示されるハイパーリンクをクリックすると、クライアントはプロトコルに対して適切な処理を実行します。

TEL および IM プロトコル ハンドラ

HTML ページの TEL: および IM: プロトコル ハンドラの例。

```
<html>
  <body>
    <a href="TEL:1234">Call 1234</a><br/>
    <a href="IM:msmith@domain">Send an instant message to Mary Smith</a>
  </body>
</html>
```

上記の例では、ユーザがハイパーリンクをクリックして1234に発信すると、クライアントはその電話番号への音声コールを開始します。ユーザがMary Smithにインスタント メッセージを送信するハイパーリンクをクリックすると、クライアントはMaryとのチャット ウィンドウを開きます。

CISCOTEL および SIP プロトコル ハンドラ

HTML ページの CISCOTEL および SIP プロトコル ハンドラの例：

```
<html>
  <body>
    <a href="CISCOTEL:1234">Call 1234</a><br/>
    <a href="SIP:msmith@domain">Call Mary</a><br/>
    <a href="CISCOTELCONF:msmith@domain;amckenzi@domain">Weekly conference call</a>
  </body>
</html>
```

上記の例では、ユーザが *1234* へコール または *Mary* にコール のハイパーリンクをクリックすると、クライアントはその電話番号への音声コールを開始します。

XMPP プロトコル ハンドラ

HTML ページの XMPP: プロトコル ハンドラを使用したグループ チャットの例。

```
<html>
  <body>
    <a href="XMPP:msmith@domain;amckenzi@domain">Create a group chat with Mary Smith and
Adam McKenzie</a>
  </body>
</html>
```

上記の例では、ユーザが Mary Smith および Adam McKenzie とのグループ チャットを作成するハイパーリンクをクリックすると、クライアントは Mary および Adam とのグループ チャット ウィンドウを開きます。

ヒント XMPP: および IM: ハンドラに連絡先リストを追加し、グループ チャットを作成します。連絡先を区切るには、次の例のようにセミコロンを使用します。

```
XMPP:user_a@domain.com;user_b@domain.com;user_c@domain.com;user_d@domain.com
```

件名と本文の追加

プロトコル ハンドラに件名と本文を追加できます。これにより、ユーザがパーソンツーパーソンまたはグループのチャットを作成するために、ハイパーリンクをクリックすると、クライアントはチャット ウィンドウを開き、前もって入力された件名と本文を表示します。

件名と本文は、次のいずれのシナリオでも追加できます。

- クライアントでインスタント メッセージング用にサポートされているプロトコル ハンドラを使用する
- パーソンツーパーソン チャットまたはグループ チャットのいずれか
- 件名と本文を含める、またはそのどちらかを含める

次の例では、ユーザが下のリンクをクリックすると、前もって入力されたI.T Deskの本文を含む、パーソンツーパーソン チャット ウィンドウが開きます。

```
xmpp:msmith@domain?message;subject=I.T.%20Desk
```

次の例では、ユーザが下のリンクをクリックすると、[I.T Desk] のトピックを含む [グループチャットの開始（Start Group Chat）] ダイアログボックスが開き、チャット ウィンドウの入力ボックスには「Jabber 10.5 Query」というテキストが入力されています。

```
im:user_a@domain.com;user_b@domain.com;user_c@domain.com?message;subject=I.T%20Desk;body=Jabber%2010.5%20Query
```

プロトコル ハンドラでサポートされるパラメータ

モバイル クライアントの相互起動

モバイル クライアント用 Cisco Jabber では、指定したアプリケーションに戻ることができます。たとえば、番号をダイヤルする ciscotel URI リンクを作成する場合に、パラメータとしてアプリケーション名を追加し、コールの終了時にそのアプリケーションに戻るようユーザに要求できます。

```
ciscotel://1234567?CrossLaunchBackSchema=SomeAppSchema&CrossLaunchBackAppName=SomeAppName
```

- CrossLaunchBackAppName：コール終了時に Cisco Jabber が相互起動するアプリケーションの名前を入力することをユーザに求めます。
  - none（デフォルト）：ダイアログ ボックスにアプリケーションが表示されません。
  - *app_name*：ダイアログ ボックスに表示されるアプリケーション名。
- CrossLaunchBackSchema：コールが終了したときに使用するスキーマを指定します。
  - none（デフォルト）：Cisco Jabber に留まります。
  - *schema*：アプリケーションの相互起動に使用されるスキーマ。

サポートされる区切り文字

HTML ページの URI リンクを作成するときに、セミコロンを使用して文字を区切ることができます。これは、SIP、Tel、CiscoTel、および ClickToCall プロトコル ハンドラでサポートされます。次の例では、2 つの番号を使用する電話会議がリンクに作成されます。

```
tel:123;123
```

IM プロトコルは、カンマ区切り文字に加えてセミコロン区切り文字をサポートしています。次の例では、2 人の参加者がいるグループ チャットがリンクに作成されます。

```
im:participant1@example.com,participant2@example.com
```

DTMF サポート

IM ウィンドウでの DTMF の入力

クライアントの IM ウィンドウで、DTMF 数字を含むプロトコル ハンドラを入力すると、参加者が使用できるリンクがクライアントによって作成されます。サポートされるプロトコルは、TEL、CISCOTEL、SIP、CLICKTOCALL、CISCOIM、IM および XMPPです。サポートされるパラメータは番号または SIP URI です。次の例では、ダイヤルイン番号が 1800-123456、エントリの PIN が 5678# です。この TEL URI リンクを使用して会議リンクが作成されます。

```
tel:1800123456,,,5678#
```

アクティブ コールでの DTMF の入力

コール中、ユーザはDTMF 数字をコピーしてクライアントのコール ウィンドウに貼り付けることができます。会議招待状の会議 ID、参加者I D、PIN を簡単に入力できます。アクティブ コール中に英数字の文字列を入力すると、それらの文字列はキーパッドの対応する番号に解釈されます。

サポートされる DTMF ストリング

DTMF ストリングには次を含めることができます。

- 0 ～ 9
- #
- *
- カンマ：1 秒の遅延を意味します（複数のカンマを使用できます）。
- a ~ z、A ~ Z：これらの文字は、アクティブ コール時にサポートされません。

無効な DTMF 数字は無視されます。