ソフトフォンの設定

ソフトフォン ワークフローの作成

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Jabber デバイスの作成と設定 （2 ページ）	Cisco Jabber にアクセスするユーザごとに 1 つ以上のデバイスを作成します。ユーザに提供する認証文字列を生成します。
ステップ 2	デバイスに電話番号を追加する （6 ページ）	作成した各デバイスについて、ディレクトリ番号を追加します。
ステップ 3	ユーザとデバイスの関連付け （7 ページ）	ユーザとデバイスを関連付けます。
ステップ 4	モバイル SIP プロファイルの作成 （8 ページ） を選択します。	この作業は、Cisco Unified Communications Manager リリース 9 を使用して、デバイスをモバイル クライアント用に設定する場合に実行します。
ステップ 5	電話セキュリティ プロファイルの設定 （9 ページ）	この作業は、すべてのデバイスのセキュアな電話機能をセットアップするために実行します。

Cisco Jabber デバイスの作成と設定

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

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

始める前に

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

手順

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

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

ステップ 3 [新規追加（Add New）] を選択します。

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

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

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

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

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

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

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

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

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

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

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

ステップ 8 [保存（Save）] を選択します。

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

次のタスク

デバイスに電話番号を追加します。

ユーザへの認証文字列の提供

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

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

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

次の場合、クライアントはエラーを表示します。

- ユーザが誤った認証文字列を入力した場合。

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

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

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

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

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

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

デバイスに電話番号を追加する

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

始める前に

デバイスを作成します。

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**を選択します。

ユーザとデバイスの関連付け

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

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

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

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

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

始める前に

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

手順

ステップ 1 ユーザとデバイスを関連付けます。

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

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

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

モバイル SIP プロファイルの作成

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

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

手順

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

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

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

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

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

ステップ 4 新しい SIP プロファイルに次の値を設定します。

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

ステップ 5 **保存**を選択します。

システムの SIP パラメータの設定

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

始める前に

この設定は、モバイル クライアント専用です。

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

手順

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

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

ステップ 3 ノードを選択します。

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

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

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

ステップ 7 [保存（Save）] を選択します。

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

電話セキュリティ プロファイルの設定

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

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

始める前に

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

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

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

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

手順

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

ステップ 2 [新規追加（Add New）] を選択します。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ステップ 11 **[保存]** をクリックします。