Cisco Jabber for iPhone Release 9.1(1) アドミニストレーション ガイド

初版：2013 年 2 月 1 日

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

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

目 次

第 1 章

概要

Cisco Jabber for iPhone は、エンタープライズ コール、ビジュアル ボイスメール、および iOS デバイスから直接の企業ディレクトリへのアクセスをユーザに提供します。

（注） VoIP 通話の音声品質は、Wi-Fi またはモバイル データ ネットワーク接続によって異なります。Cisco AnyConnect Secure Mobility Client を利用した Cisco Jabber への接続にモバイル データ ネットワークまたは社外 Wi-Fi ネットワークを使用する場合、Cisco Technical Assistance Center（TAC）では音声品質のトラブルシューティングは行えません。

Cisco Jabber for iPhone では、次のことを実行できます。

- Cisco Unified Communications Manager（Unified CM）を介し、iOS デバイスを使用して社内の電話番号でコールを発信および受信する。 VoIP またはモバイル ボイス ネットワークを使用して、コールを発信できます。

  （注） Cisco Jabber はモバイル デバイス ネットワーク環境において、Dial via Office Reverse（DVO-R）機能を用いることで、会社の電話番号を用いた発信が可能です。 DVO-R 機能には以下が必要です。

  - Cisco Jabber for iPhone client, Release 9.1(1) 以降。
  - Unified CM 9.1(1a)（2013 年 2 月リリース）。

- Cisco Jabber が実行されていないか、企業ネットワークに接続されていないときに、一般の携帯電話番号で通話を受信する。
- 複数の VoIP コール（コール ウェイティング、新しい通話の追加、アクティブ コール間の切り替え）。
- Unified CM が提供する通話中の機能の多くを使用する。 通話中の機能には、保留、転送、会議などがあります。

- アクティブな Cisco Jabber VoIP コールをデバイスからデスク フォンに、またはその逆に転送する。
- アクティブな Cisco Jabber VoIP コールをモバイル ネットワークに転送する。
- iPhone を耳に当て、通話相手の名前を発音することで、その番号にダイヤルする（日本語には対応していません）。
- 社内ディレクトリを検索する。
- ビジュアルなボイスメールのリストからそれぞれのメッセージにアクセスする。
- 自動セットアップ リンクにセカンダリまたはバックアップ TFTP サーバを設定する。
- アプリケーションは Cisco Jabber によってバックグラウンドで実行され、Unified CM が利用可能な場合は自動的に登録され、会社の電話番号へのコールを受信できる状態を保つ。
- 別の Unified CM または Cisco Unified Survival Remote Site Telephony（SRST）でサービスのバックアップをする。
- Cisco Jabber for iPhone を Cisco Jabber IM for iPhone アプリケーションと連携して使用するときに、Cisco Jabber の連絡先との IM セッションを開始する。
- サポートされる iPhone デバイスで Bluetooth ヘッドセットを使用する。
- 安全なリモート アクセスのための VPN クライアントは次の目的に使用できます。
  - 社外の Wi-Fi またはモバイル データ ネットワークを使用して、社内の電話番号から VoIP コールを発信および受信する。
  - モバイル ボイス ネットワークを経由して社内の電話番号から Dial via Office コールを発信する。 これらのコールは社外の Wi-Fi またはモバイル データ ネットワークを使用して呼のセットアップを行います。

- 関連資料，2 ページ

関連資料

次の資料には Cisco Jabber に関連した情報が記載されています。

- ユーザ向けの Cisco Jabber マニュアルは、次の Web サイトで入手できます。http://www.cisco.com/en/US/products/ps11596/products_user_guide_list.html
- 本製品固有の技術情報は、『*Solutions Reference Network Design (SRND)*』にあります。これは、Unified CM の設計ガイド一覧から入手できます。
- 管理者向けの Unified CM マニュアルは、Unified CM ドキュメント ホーム ページで入手できます。

第 2 章

はじめる前に

Cisco Jabber の導入

Cisco Jabber の一般的な導入手順を説明します。

手順

ステップ 1 最適な音声品質とコール メンテナンスに必要なネットワーク要件など、システム要件を確認します。 この製品のリリース ノートは次の Web サイトで入手できます。http://www.cisco.com/en/US/products/ps11596/prod_release_notes_list.html

ステップ 2 必要なファイルのリストを確認します。
必要なファイルをあらかじめ用意するか、このマニュアルの手順で必要になるたびに用意してください。 必要なファイル，（4 ページ）を参照してください。

ステップ 3 システムをセットアップします。
はじめる前に，（3 ページ）を参照してください。

ステップ 4 テスト デバイスを追加します。

管理, （17 ページ）を参照してください。

ステップ 5 次のようにして、必要な機能をセットアップします。

a) 前提条件をすべて満たしていることを確認します。
b) 配置する特性および機能に対するシステム レベルの設定をセットアップします。
c) 必要なすべてのユーザ レベルの設定をセットアップします。
d) Cisco Unified Communications Manager（Unified CM）にデバイスをセットアップします。
e) 機能ごとに設定をテストします。

機能ごとの説明は、機能の設定, （33 ページ）にリストされています。

ステップ 6 正常に機能する設定をテンプレートとして使用し、ユーザに合わせてデバイスをセットアップします。
一括設定, （25 ページ）を参照してください。

ステップ 7 ユーザが Cisco Jabber を設定するために必要な情報を電子メールで送信します。

Unified CM のデバイス ページで入力した設定が、自動的にデバイス上のアプリケーションに入力されます。ユーザは、必要に応じてパスワードを入力します。ユーザ向けのマニュアルは、次の Web サイトで入手できます。http://www.cisco.com/en/US/products/ps11596/products_user_guide_list.html

必要なファイル

Cisco Jabber を設定および使用するには、次のファイルが必要です。 あらかじめすべてのファイルを用意するか、必要になるごとに入手してください。

表 *1*：*Cisco Unified Communications Manager* のすべてのリリースで必要なファイル

ファイル	このファイルの入手方法の参照先
デバイス COP ファイル	ソフトウェア ダウンロード サイト http://www.cisco.com/go/jabber_iphone_cop を開きます。 cmterm-iphone-install-130129.cop.sgn を探してダウンロードします。
使用中のデバイスに対応した Cisco Jabber アプリケーション	iOS デバイスで iTunes から App Store にアクセスするか、App Store アプリケーションを使用します。 Cisco Jabber を検索するときに、Cisco Jabber と Cisco Jabber IM の区別に注意してください。

表 *2*：*Cisco Unified Communications Manager Release 8.5* 以前で必要な追加のファイル

ファイル	このファイルの入手方法の参照先
Cisco Jabber でアプリケーション ダイヤル ルールを使用可能にするために必要な Cisco Options Package（COP）ファイル （注） このファイルは、Unified CM 8.5 以前に必要です。 Unified CM 8.6 以降では、アプリケーション ダイヤル ルールがアプリケーションに統合されたため、該当のフィールドを表示するために追加の COP ファイルをインストールする必要はありません。	Cisco Jabber for iPhone では、アプリケーション ダイヤル ルールを使用可能にするために、Cisco UC Integration for Microsoft Office Lync と同じ COP ファイルを使用します。 Cisco UC Integration for Microsoft Office Communicator の [Software Downloads] ページを開きます。 Administration Toolkit バンドルをダウンロードして解凍します。 このバンドル内で必要なのは、ファイル cmterm-cupc-dialrule-wizard-0.1.cop だけです。

関連トピック

デバイス用の Cisco Options Package ファイルのインストール，（5 ページ）
ダイヤル ルールの COP ファイルの取得，（9 ページ）

デバイス用のCiscoOptionsPackageファイルのインストール

Cisco Jabber を Unified CM 内でデバイスとして使用できるようにするには、デバイス固有の Cisco Options Package（COP）ファイルをすべての Unified CM サーバに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情報については、メンテナンス ガイドのリストにある、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。
必要なファイル，（4 ページ）を参照してください。
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 Unified CM サーバからアクセスできる FTP または SFTP サーバに COP ファイルを置きます。

ステップ 3 この COP ファイルを Unified CM クラスタ内のパブリッシャ サーバ上にインストールします。

a) [Unified CM の管理（Unified CM Administration）] ポータルの右上にある [ナビゲーション（Navigation）] リスト ボックスから、[Cisco Unified OS の管理（Cisco Unified OS Administration）] を選択し、[移動（Go）] を選択します。

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。 この処理には時間がかかることがあります。

i) 使用率が低い時間帯に、Unified CM 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、各サーバのサービスがアクティブな状態に戻ったのを確認してから、次のサーバでのこの手順の実行を開始するようにしてください。

ステップ 4 クラスタのサブスクライバ サーバそれぞれに COP ファイルをインストールします。
パブリッシャと同様に、サーバの再起動などの手順を実行します。

デバイス COP ファイルのバージョンの確認

このリリースの Cisco Jabber に正しいデバイス COP ファイルを使用していることを確認するには、次の手順を使用します。

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

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

ステップ 3 [新規追加（Add New）] をクリックします。

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、[Cisco Dual Mode for iPhone] を選択します。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [プロダクト固有の設定（Product Specific Configuration Layout）] セクションまでスクロール ダウンし、[Dial via Office] ドロップダウン リストが表示されることを確認します。
[Dial via Office] ドロップダウン リストが表示された場合、COP ファイルはご使用のシステムにすでにインストールされています。

[Dial via Office] ドロップダウン リストが表示されない場合は、正しい COP ファイルを探してダウンロードします。 詳細については、必要なファイル，（4 ページ）を参照してください。

ダイヤル ルール

Cisco Jabber for iPhone は、iPhone から電話番号をダイヤルすることを容易にするための 2 つのダイヤル ルールを使用します。

- アプリケーション ダイヤル ルール（`AppDialRules.xml`）
- ディレクトリ検索ダイヤル ルール（`DirLookupDialRules.xml`）

Unified CM は、Cisco Options Package（COP）ファイルがインストールされたときに、これらのファイルを生成します。

ディレクトリ検索ダイヤル ルールは、Microsoft Active Directory を使用して発信者を識別します。Cisco Jabber は、Unified CM や Microsoft Active Directory から提供される名前ではなく、iPad のメインのアドレス帳にある発信者 ID を表示します。

アプリケーション ダイヤル ルール

携帯電話とデスクフォンでは、発信時にダイヤルする番号が異なることが一般的であるため、携帯電話ユーザが異なるダイヤル パターンでダイヤルできるよう、Unified CM を設定するようにしてください。

Unified CM では、これらのルールをすべての通話およびデバイスに適用されるように作成することもできれば、後述する方法で XML ファイルを編集して、Cisco Jabber のユーザだけに適用されるようにしたり、国コードまたは市外局番ごとにデバイスに異なるルールが適用されるようにしたりすることもできます。

たとえば、ユーザは次のように番号をダイヤルする場合があります。

- モバイル デバイス ユーザは、社外の電話番号をダイヤルする前に、9 をダイヤルする習慣がない。
- モバイルデバイス番号の市外局番が、デスクフォンの番号と異なっている場合、ユーザはモバイルデバイスの使用時は地域コードをダイヤルするが、会社の電話からダイヤルするときは地域コードをダイヤルしない。または、その逆になることがある。
- 国際電話をダイヤルするモバイル デバイス ユーザは、ダイヤルする番号をプラス記号（+）で始める場合がある。

アプリケーション ダイヤル ルールを設定すると、これらの例で示したタイプのコールに正常に接続することができます。

アプリケーション ダイヤル ルールの設定の詳細については、Unified CM のオンライン ヘルプを参照してください。

Cisco Jabber でのダイヤル ルールの使用

この一連の手順を実行すると、既存のすべてのダイヤル ルールを Cisco Jabber で使用できるようになります。

（注） この手順は、Unified CM Release 8.5 以前のリリースにのみ該当する手順です。 Unified CM 8.6 以降では、アプリケーション ダイヤル ルールがアプリケーションに統合されたため、該当のフィールドを表示するために追加の COP ファイルをインストールする必要はありません。 Unified CM 8.6 以降でアプリケーション ダイヤル ルールにアクセスするには、[コール ルーティング（Call Routing）] > [ダイヤル ルール（Dial Rules）] > [アプリケーション ダイヤル ルール（Application Dial Rules）] の順に選択します。 アプリケーション ダイヤル ルールのセットアップについては、ご使用のリリースの『Cisco Unified Communications Manager Administration Guide』（Unified CM メンテナンス ガイド一覧から入手可能）で関連する章を参照してください。

（注） ダイヤル ルールで使用する COP ファイルは、このマニュアルの他の箇所で説明しているデバイス COP ファイルとは別のものです。

他のシスコ製品のダイヤル ルールにも、この同じ COP ファイルを使用できます。

この一連の手順では、Unified CM TFTP サーバのルート レベルにある `CUPC` というフォルダに、必要な XML ファイルをインストールします。 Cisco Jabber に必要なルールが、このファイルを使用する他のクライアントに必要なルールとは異なる場合は、オプションの手順によって XML ファイルをコピーして編集し、Cisco Jabber 専用のファイルを作成してください。

他のシスコのテレフォニー クライアントをセットアップして統合している場合、この一連の手順はすでに実行済みである可能性があります。

（注） Unified CM でダイヤル ルールを更新するたびに、この一連の手順を繰り返して Cisco Jabber を含む各クライアントに変更を反映させる必要があります。

次の手順を順序どおりに実行してください。

1 ダイヤル ルールの COP ファイルの取得, （9 ページ）
2 ダイヤル ルールのコピー, （9 ページ）
3 ダイヤル ルールのコピーの確認, （10 ページ）
4 ダイヤル ルールの修正, （10 ページ）
5 TFTP サービスの再起動, （12 ページ）

ダイヤル ルールの COP ファイルの取得

手順

ステップ 1 Cisco UC Integration for Microsoft Office Communicator の [Software Downloads] ページを開きます。
（注） Cisco Jabber for iPhone では、アプリケーション ダイヤル ルールを使用可能にするために、Cisco UC Integration for Microsoft Office Communicator と同じ COP ファイルを使用します。

ステップ 2 Administration Toolkit バンドルの横の [ダウンロード（Download）] をクリックします。

ステップ 3 画面に表示される指示に従います。

ステップ 4 ダウンロードされたファイルを解凍します。

ステップ 5 CUCM フォルダで、次のダイヤル ルール COP ファイルを探します。
`cmterm-cupc-dialrule-wizard-0.1.cop.sgn`
このダウンロードに含まれる他のファイルは必要ありません。

ステップ 6 ダイヤル ルールの COP ファイルを、FTP または SFTP でアクセスできるサーバ上に置きます。

ダイヤル ルールのコピー

Unified CM アプリケーションでダイヤル ルールのコピーを作成するには、次の手順を実行します。

手順

ステップ 1 Unified CM クラスタ内のパブリッシャ サーバにサインインします。

ステップ 2 [Unified CM の管理（Unified CM Administration）] ポータルの右上で、[Cisco Unified OS の管理（Cisco Unified OS Administration）] を選択し、[移動（Go）] を選択します。

ステップ 3 [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。

ステップ 4 [ソフトウェアのインストール/アップグレード（Software Installation/Upgrade）] ウィンドウで、ダイヤル ルール COP ファイルの場所を指定します。

ステップ 5 [次へ（Next）] を選択します。

ステップ 6 [使用可能なソフトウェア（Available Software）] ドロップダウン リストから COP ファイルを選択します。

ステップ 7 [次へ（Next）] を選択します。

ステップ 8 [インストール（Install）] を選択します。

ステップ 9 TFTP サーバが稼働する Unified CM サーバごとに、この手順を繰り返します。

ダイヤル ルールのコピーの確認

手順

ステップ 1 [Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）] ポータルで、[ソフトウェア アップグレード（Software Upgrades）] > [TFTP ファイルの管理（TFTP File Management）]を選択します。

ステップ 2 [TFTP ファイルの管理（TFTP File Management）] ウィンドウで、CUPC から始まるディレクトリを探します。

ステップ 3 ダイヤル ルールがあることを確認します。

例：
```
DirLookupDialRules.xml
```

ダイヤル ルールの修正

このオプションの手順は、Cisco Jabber で使用するために、ダイヤル ファイルを修正する場合にのみ使用します。 次に、例を示します。

- Cisco Jabber に固有で、他のクライアントには使用されないルールが必要な場合。

- 複数のファイルを作成して、各ユーザの Cisco Jabber デバイスについて異なるルールを割り当てる場合。たとえば、ユーザが所有しているモバイルデバイスが異なる国コードまたは市外局番で発行され、既存のルールではユーザがモバイルデバイスから複数の国コードや市外局番に基づいて番号をダイヤルする方法に対応していない場合。

はじめる前に

- アプリケーション ダイヤル ルール, （7 ページ）のガイドラインを使用して、必要なアプリケーション ダイヤル ルールを決定します。
- Unified CM で TFTP サーバを使用する方法がわからない場合は、Unified CM メンテナンス ガイド一覧を参照して、ご使用のリリースに対応した次のマニュアルを探してください。
  - 『*Cisco Unified Communications Manager Operating System Administration Guide*』。「Software Upgrades」の章の、TFTP サーバ ファイルを管理する操作手順を参照してください。
  - 『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』。

手順

ステップ 1 Unified CM TFTP サーバのルート レベルにある `CUPC` フォルダに移動します。

ステップ 2 Cisco Jabber 用に修正するルール ファイルをコピーします。

例：
PC または Mac 上で組み込みの TFTP クライアントを使用して、次のコマンドを入力します。

```
tftp server-name
get CUPC/AppDialRules.xml
```

ステップ 3 必要に応じて、ファイルの名前を変更します。

例：

```
AppDialRulesFrance.xml
```

ステップ 4 テキスト エディタでこのファイルを開きます。

ステップ 5 既存ルールの例に従いながら、必要に応じてルールを修正または追加します。

ステップ 6 変更を保存します。

ステップ 7 修正したファイルをアップロードします。

重要 パスとファイル名を記録します。この情報は、後で必要になります。

a) ウィンドウの右上にあるドロップダウン リストから、[Cisco Unified OS の管理（Cisco Unified OS Administration）] を選択します。
b) [ソフトウェア アップグレード（Software Upgrade）] > [TFTP ファイルの管理（TFTP File Management）] の順に選択します。
c) ハード ドライブ上のファイルを選択します。
d) TFTP サーバ上のフォルダを指定します。
例：ciscojabber

e) [アップロード（Upload）] を選択します。

ステップ 8 カスタマイズする必要のある他のすべてのルール ファイルについて、この手順を繰り返します。

次の作業

必要なすべてのカスタム ダイヤル ルール ファイルの編集を完了して、ファイルをアップロードし終えたら、この項の次の手順に進みます。

Unified CM Release 8.5 以前を使用していて、Cisco Jabber デバイスにアプリケーション ダイヤル ルールを適用するには、ファイル名を含めてこれらのダイヤル ルール ファイルのパスを指定する必要があります。 これらのファイルを移動または名前変更した場合は、各配置済みデバイスの設定ページの [アプリケーション ダイヤル ルールの URL（Application Dial Rules URL）] フィールドで、このパスを更新するのを忘れないでください。

TFTP サービスの再起動

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。

詳細については、メンテナンス ガイド一覧から入手できる、『*Cisco Unified Serviceability Administration Guide*』の「Starting, Stopping, Restarting, and Refreshing Status of Services in Control Center」を参照してください。

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルの右上で [Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] を選択し、[移動（Go）] を選択します。

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

ステップ 3 サーバを選択し、[移動（Go）] を選択します。

ステップ 4 [Cisco TFTP] を選択します。

ステップ 5 [リスタート（Restart）] を選択します。

ステップ 6 このアプリケーション ダイヤル ルールの COP ファイルを実行したすべてのサーバで、この手順を繰り返します。

[SIP デュアル モード アラート タイマー（SIP Dual Mode Alert Timer）] 値の増加

[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

勤務先コールを受信するには、Cisco Jabber が実行されている必要があります。

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

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 サーバを選択します。

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 4500 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。 推奨される最小値は、4500 ミリ秒です。

専用 SIP プロファイルの作成

専用の SIP プロファイルを作成すると、Cisco Jabber をバックグラウンドで実行中に、Cisco Jabber を Unified CM に接続したままにすることができます。

Unified CM の特定のバージョンのみがこの機能をサポートします。 次の Web サイトの *Cisco Jabber for iPhone* のリリース ノートで「System Requirements」の章を参照してください。 http://www.cisco.com/en/US/products/ps11596/prod_release_notes_list.html

（注） このデバイスの設定は、Cisco Jabber 8.0 クライアントには影響しません。

手順

ステップ 1 Unified CM で、[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 2 新しい SIP プロファイルを「iPhone SIP profile」などの名前で作成するか、または既存の SIP プロファイルをコピーします。

ステップ 3 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「60」
- [レジスタのタイムアウト値（Timer Register Expires）] に「660」
- [キープアライブのタイムアウト値（Timer Keep Alive Expires）] に「660」
- [サブスクライブのタイムアウト値（Timer Subscribe Expires）] に「660」
- [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 4 [保存（Save）] を選択します。

次の作業

Cisco Jabber を実行するすべての Cisco Dual Mode for iPhone デバイスに、この SIP プロファイルを選択します。

システム レベルの前提条件

お使いのシステムが次の前提条件を満たしていることを確認してください。

- 次のような標準 SIP 機能および電話機能が設定され、Cisco Jabber から独立して動作している。
  - 保留音
  - ネットワーク保留音
- 次のようなコール中の機能が設定されます。
  - 保留/復帰
  - コール待機
  - 通話の追加
  - 電話会議
  - 転送

- 次のようなシステムのコール パークが設定されます。
  - 通話中にユーザが誤って Cisco Jabber を終了しても、通話が切断されないこと。
  - ユーザが標準のコール パーク機能を使用できること。

  詳細については、『*Cisco Unified Communications Manager Features and Services Guide*』の「Call Park」の章を参照してください。このマニュアルは、http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html から入手できます。
- トランスコーディングが利用可能でない限り、電話会議にはすべての参加エンドポイントに G.711 が必要です。 G.729a だけが Cisco Jabber でサポートされている場合は、電話機の G.729a から会議ブリッジの G.711 にトランスコーディングを許可するように外部トランスコーダを設定する必要があります。

使用状況とエラーのトラッキング

Cisco Jabber は、欠陥の検出と製品パフォーマンスの向上のためにシスコが使用する使用状況の集計とエラー追跡データの収集と生成を、サード パーティ サービスの Google Analytics に依存しています。 シスコは、Google Analytics の個人情報の方針に従い、個人を特定できる情報については、これを保存しません。

Google Analytics が保存および収集するすべての情報は、機密情報として扱われます。 この情報にアクセスできるのはシスコのみです。 この機能は現在、管理者用のレポート ツールとしては使用できません。

Unified CM で各 Cisco Jabber デバイスを設定するときに、各ユーザの使用状況レポートを有効または無効にできます。

この設定に応じて、シスコは次の情報を収集します。

表 *3*：使用状況とエラーのトラッキング

使用状況とエラーのトラッキング設定	収集される情報
有効（Enabled）	• エラーおよび警告 • Cisco Jabber の画面表示（たとえば、ユーザが自分のボイス メッセージ リストを表示する頻度） • 機能のアクティビティ（たとえば、ユーザが連絡先を追加する頻度） • Cisco Jabber が接続する TFTP サーバの IP アドレス • モバイル サービス プロバイダーのアクティビティに基づいた、およその地理的位置

使用状況とエラーのトラッキング設定	収集される情報
詳細（Detailed）	[有効（Enabled）] を選択した場合に収集されるのと同じ情報
無効（Disabled）	なし

ユーザが Cisco Jabber を最初に起動したときに、シスコがデータを収集することに対する許諾契約が表示されます。 使用状況トラッキング機能が現在有効になっているかどうかにかかわらず、ユーザがこれに同意しないとアプリケーションを使用できません。

レポート ツールに関する詳細については、以下を参照してください。

- Google Analytics
- プライバシー ポリシー

第 3 章

管理

Cisco Jabber の設定

この一連の手順を実行して、Unified CM 上ですべての Cisco Jabber 機能を設定し、デバイス上で Cisco Jabber を設定する方法をユーザに説明します。

次の手順を順序どおりに実行してください。

1 基本テレフォニー機能を設定したテスト デバイスを追加します。

ユーザ デバイスの追加，（18 ページ）を参照してください。

2 テスト デバイス上で追加機能を設定します。 これらの機能はオプションです。

「機能の設定」を参照してください。

3 テストデバイス上ですべての機能が動作することを確認したら、個別のユーザとデバイスを一括で設定します。

「一括設定」を参照してください。

4 （任意）自動セットアップ リンクを準備することでユーザ向けに Cisco Jabber セットアップを最適化します。

自動セットアップ リンクの準備（任意），（27 ページ）を参照してください。

5 （任意）Cisco Jabber を相互起動するために他のアプリケーションをセットアップすることでユーザの操作性をカスタマイズします。

他のアプリケーションからの Cisco Jabber の相互起動（任意），（28 ページ）を参照してください。

6 ユーザに Cisco Jabber クライアントの設定方法を説明します。

ユーザへの指示，（28 ページ）を参照してください。

ユーザ デバイスの追加

はじめる前に

- すべてのデバイスに対する標準の操作手順に従って、このデバイスに割り当てる内線のボイスメールをセットアップしてテストします。 ユーザがエンタープライズ VoIP またはモバイル コールを使用してボイスメール システムに接続できるように、ボイスメール番号は必ず通常の電話番号としてセットアップします。
- Cisco Jabber デバイスに割り当てるデバイス プールが、サポート対象のすべての音声コーデックをサポートしているリージョンに関連付けられていることを確認します。 サポートされるコーデックについては、http://www.cisco.com/en/US/products/ps11596/prod_release_notes_list.html にあるこの製品のリリース ノートを参照してください。
- 各ユーザについて、使用状況およびエラーのトラッキングを無効にするか、それとも有効にするかを決定します。 詳細については、使用状況とエラーのトラッキング，（15 ページ）を参照してください。

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

ステップ 2 [デバイス（Device）] > [電話（Phone）] を選択して、[新規追加（Add New）] をクリックして、[電話のタイプ（Phone Type）] に [Cisco Dual Mode for iPhone] を選択して新しい電話デバイスを追加します。

ステップ 3 デバイスに必要な設定を入力します。 詳細については、「表 4：パラメータの説明」を参照してください。
これらの値には、Cisco Jabber に固有ではない制限および要件が適用される可能性があります。デバイス設定ウィンドウのオプションに関する詳細情報が必要な場合は、Unified CM のオンライン ヘルプを参照してください。

ステップ 4 [保存（Save）] を選択します。

ステップ 5 [設定の適用（Apply Config）] を選択します。

ステップ 6 [回線 [*n*] - 新規 DN を追加（[Line n] - Add a new DN）] を選択します。

ステップ 7 このデバイスのディレクトリ番号を入力します。
これは、新しい DN にできます。同じ DN のデスクフォンは必要ではありません。

ステップ 8 このデバイスがスタンドアロン デバイス（デスクフォンと DN を共有していない）の場合は、次の設定を行ってCisco Jabberが実行されておらずネットワークに接続されていないときに電話を転送するようにします。こうすると、発信者がエラー メッセージを受け取らずにすみます。

a) 未登録内線の不在転送（Forward Unregistered Internal）

b) 未登録外線の不在転送（Forward Unregistered External）

これらの設定の詳細については、同じウィンドウの [不在転送（Forward All）] やその他の設定に関する、Unified CM のオンライン ヘルプを参照してください。

ステップ 9 [無応答時の呼び出し時間（秒）（No Answer Ring Duration (seconds)）] を 24 秒に設定して、コールをボイスメールに転送する前にCisco Jabberが呼び出し音を鳴らす時間を持てるようにします。

（注） Cisco Jabber for iPhone ユーザがデバイスに PIN を設定している場合は、コールがボイスメールに転送される前にユーザが PIN を入力してコールに応答するための十分な時間を確保するために、[無応答時の呼び出し時間（秒）（No Answer Ring Duration (seconds)）] の設定値を増やすことが必要な場合があります。

[無応答時の呼び出し時間（秒）（No Answer Ring Duration (seconds)）]を増加する場合は、この設定に関連する警告について、Unified CM のオンライン ヘルプで参照してください。

ステップ 10 [ビジー トリガー(Busy Trigger)] フィールドの [デバイス<デバイス名>の複数コール/コール待機設定（Multiple Call/Call Waiting Settings on Device *device name*）] セクションで、値が 2 以上に設定されていることを確認します。

ステップ 11 環境に応じて、その他の設定を設定します。 Cisco Jabber には特定の値は必要ありません。

ステップ 12 [保存（Save）] を選択します。

ステップ 13 ユーザの [エンド ユーザ（End User）] ウィンドウに移動します。

ステップ 14 このユーザ用に作成した Cisco Dual Mode for iPhone デバイスを関連付けます。
使用している Unified CM のリリースによっては、ここでデバイスが [デバイス情報（Device Information）] セクションまたは [デバイスの割り当て（Device Associations）] セクションの [制御するデバイス（Controlled Devices）] ボックスに表示されます。

ステップ 15 このユーザがデスクフォンを所有している場合は、そのデスクフォンをプライマリ ユーザ デバイスとして選択します。

ステップ 16 関連するデスクフォンなしで動作するスタンドアロン デバイスの場合は、システム内のすべてのデバイスで標準となっている他の情報の入力が必要になることがあります。

次の作業

次のようにして、設定が動作することを確認します。

- 電話機が企業のネットワークに接続されていることを確認します。 電話のブラウザを使用して企業のイントラネット上の Web ウィンドウにアクセスできることを確認します。
- Cisco Jabber を起動して、セットアップ ウィザードを完了させます。 新しく追加したデバイスの TFTP サーバのデバイス名（TCTXXXX）と IP アドレス（通常は Unified CM サーバの IP アドレス）を入力します。

- コールの発信、保留、転送など、Cisco Jabber の VoIP コールを発信し、テレフォニー機能をテストします。

エンドユーザによる設定の編集を許可していた場合は、既存の設定に変更を加えたら、デバイス上の電話機サービス アカウントをいったん削除して、セットアップし直します。

表 *4*：パラメータの説明

パラメータ	説明
デバイス情報	
デバイス名（Device Name）	次のようにデバイス名を指定します。 • 1 つのデバイスだけを表すことができます。 単一のユーザが複数のデバイス（iPhone や iPad Touch など）に Cisco Jabber を持つ場合は、Unified CM 内でそれぞれに別々の Cisco Dual Mode for iPhone デバイスを設定します。 • **TCT** で始まらなければなりません。 • すべて大文字でなければなりません。 • 最大 15 文字です。 • 使用できる文字は、A ～ Z、0 ～ 9、ドット（.）、ダッシュ（-）、または下線（_）のみです。
電話ボタン テンプレート（Phone button Template）	[Standard Dual Mode for iPhone] を選択します。
メディア リソース グループ リスト（Media Resource Group List）	これらの項目はユーザが保留状態の際に流す保留音を設定します。 これらの設定はこのデバイスに限った設定ではありません。 詳細については、Unified CM documentation を参照してください。
ユーザ保留 MOH 音源（User Hold MOH Audio Source）	
ネットワーク保留 MOH 音源（Network Hold MOH Audio Source）	
プライマリ Phone（Primary Phone）	このユーザがデスクフォンを持つ場合は、デスクフォンを選択します。 プライマリ電話機を選択すると、このデバイスはライセンス上 Adjunct として設定されます。

パラメータ	説明
Cisco Unified Mobile Communicator の有効化（Enable Cisco Unified Mobile Communicator）	このオプションは、Cisco Unified Communications Manager Release 6.1.5 では使用できません。 Cisco Unified Communications Manager Release 7.1.5 の場合、次のように行います。 Cisco Unified Mobility Advantage サーバと連携して実行される Cisco Jabber アプリケーションがこの iPhone にもインストールされている場合は、両方のアプリケーションの全機能が動作できるようにするために、このオプションを選択します。 それ以外の場合や、他の Cisco Unified Communications Manager リリースでは、このオプションを選択しません。
プロトコル固有情報	
デバイスのセキュリティ プロファイル（Device Security Profile）	[Cisco Dual Mode for iPhone - 標準 SIP 非セキュア プロファイル（Cisco Dual Mode for iPhone - Standard SIP Non-Secure Profile）] を選択します。 このプロファイルではSIP ダイジェスト認証は無効になっています。
SIP プロファイル（SIP Profile）	「専用 SIP プロファイルの作成」で作成した SIP プロファイルを選択します。
上記セクションの他の設定	導入に応じて設定します。 このマニュアルで説明されていない値は Cisco Jabber に固有ではありませんが、デバイスが正しく動作するようにするために入力する必要があります。
プロダクト固有の設定 このセクションの情報は初期設定時に iOS デバイスにダウンロードされ、Cisco Jabber が自動設定されます。	

パラメータ	説明
エンド ユーザによる設定の編集を許可する（Allow End User Configuration Editing）	ユーザがどうしても個別に設定を変更できる必要がある場合を除いて、この設定には [無効（Disable）] を選択します。 このマニュアルの説明は、[エンド ユーザによる設定の編集を許可する（Allow End User Configuration Editing）] が無効にされていることを前提にしています。 この設定を無効にした場合、次のようになります。 • ユーザがこのウィンドウの [プロダクト固有の設定（Product Specific Configuration Layout）] セクションで行ったすべての変更内容が、Cisco Jabber を起動するたびに次の例外を除いて自動的に更新されます。 • 例外：ユーザは常にパスワードを手動で入力できます。 この設定を有効にした場合、次のようになります。 • このウィンドウで加えた変更が自動的にクライアントに渡されることはありません。 • このウィンドウの設定を変更した場合、ユーザは自分のアカウント設定を Cisco Jabber から削除してから、Cisco Jabber を最初から設定し直し、変更を有効にする必要があります。 • 例外：次の設定は、起動するたびに Cisco Jabber で更新されます。 ◦ シスコの使用状況およびエラー追跡（Cisco Usage and Error Tracking） ◦ オンデマンド VPN の URL（On Demand VPN URL） [非許可（Restricted）] を選択した場合、[無効（Disabled）] と同じ制限が適用されますが、デフォルトの着信音の設定は変更できます。
iPhone の国番号（iPhone Country Code）	このユーザがいる国の E.164 国際ダイヤル コードです。 このパラメータは、発信者 ID 名の判定に役立ちます。 この情報が設定されるのは、Cisco Jabber の初期設定時だけです。 既存のユーザでこの情報を変更する必要がある場合は、そのユーザが Cisco Jabber からすべてのアカウント情報を削除し、再入力する必要があります。

パラメータ	説明
シスコの使用状況およびエラー追跡（Cisco Usage and Error Tracking）	シスコが入手できるようにする使用状況情報のレベルを選択します。 詳細については、使用状況とエラーのトラッキング，（15 ページ）を参照してください。
Shake To Lock を許可しない（Disallow Shake To Lock）	（Cisco Mobile 8.1、Cisco Jabber 8.6） Shake to Lock は、このリリースでは使用できず、必要もありません。 （Cisco Mobile 8.0） Cisco Mobile の実行中に iPhone を振ることで、Cisco Mobile が開いている間に iPhone がスリープ状態になることを防ぐことができ、Cisco Mobile が着信コールを受信できるようになります。 iPhone がスリープ状態にならないようにすると、電話機を使用していないときに iPhone のネイティブの PIN ロックがオンにならなくなり、バッテリの寿命に影響を与える可能性があります。 [はい（Yes）] を選択した場合、ユーザは Shake to Lock を使用できなくなります。 [いいえ（No）] を選択した場合、ユーザは Shake to Lock を有効にするかどうかを設定できます。
サインイン機能（Sign In Feature）	ユーザがエクステンション モビリティを使用してログインできるようにする場合は [有効（Enabled）] を選択します。

パラメータ	説明
ディレクトリ ルックアップ ルール URL（Directory Lookup Rules URL）とアプリケーション ダイヤル ルール URL（Application Dial Rules URL）	「ダイヤル ルール」の手順で生成したファイルを移動または名前を変更する場合は、そのファイルのパスを入力します。 次の形式を使用します。 `tftp://<ip address of TFTP server>/<pathname to the XMLfile>/<XML filename>` （注） このフィールドの情報を入力または変更した場合は、[設定の適用（Apply Config）] を選択して、Unified CM の設定を完了してから、クライアントアプリケーションを終了し、再起動します。 それ以外の場合は、この設定を空白のままにします。 （注） Unified CM リリース 8.6 以降では、ダイヤル ルールはクライアントではなく Unified CM によって適用されます。
LDAP ユーザ認証の有効化（Enable LDAP User Authentication）	企業の画像を統合するために LDAP を使用します。 詳細については、LDAP サーバからの社内ディレクトリの画像の統合，（64 ページ）を参照してください。
LDAP ユーザ名（LDAP Username）	
LDAP パスワード（LDAP Password）	
LDAP サーバ（LDAP Server）	
LDAP SSL の有効化（Enable LDAP SSL）	
LDAP 検索ベース（LDAP Search Base）	
LDAP フィールドマッピング（LDAP Field Mappings）	
LDAP 画像の場所（LDAP Photo Location）	
緊急電話番号（Emergency Numbers）	iPhone でダイヤルした場合、デバイスのネイティブの電話アプリケーションおよびモバイル ネットワークを使用して接続する番号です。 iPod でダイヤルすると、これらの番号は VoIP コールを使用して接続します。 たとえば、911、999、112 などです。 これらの数値はあらかじめ入力されています。 必要に応じて更新してください。

パラメータ	説明
プリセット Wi-Fi ネットワーク（Preset Wi-Fi Networks）	Wi-Fi ネットワーク向け SSID です。 ユーザがこのフィールドにリストされた Wi-Fi ネットワーク上にいない場合、またはモバイルデータ ネットワーク上にいる場合、Cisco Jabber は AnyConnect への Connect on Demand をトリガーします。 複数の SSID はスラッシュ（/）で区切ります。 例：SalesOffice1/CorporateWiFi
デフォルトの着信音（Default Ringtone）	[大（Loud）] または [中（Normal）] を選択します。 エンドユーザによる [設定の編集を許可する（Allow End User Configuration Editing）] 設定値に [非許可（Restricted）] を選択した場合、ユーザは [デフォルトの着信音（Default Ringtone）] の設定だけを変更できます。 [無効（Disabled）] を選択した場合、ユーザはすべての設定を変更できません。
このセクションの他の設定	次の設定は、このリリースでサポートされていません。設定を空白のままにしてください。 • 標準モード コーデック（Normal Mode Codecs） • 低帯域幅コーデック（Low Bandwidth Codecs） • MeetingPlace 番号（MeetingPlace Numbers） • WebEx 番号（WebEx Numbers） • 連絡先（Contacts） • XML オプション（XML Options） • ビデオ機能（Video Capabilities） これ以外の設定は、他の機能の設定時にあとから入力します。

一括設定

このマニュアルに記載された情報を使用して、テスト ユーザおよびデバイスを個別に設定し、それを基礎にユーザとデバイスを設定するための一括管理テンプレートを作成してください。

一括処理の準備ができたら、ご使用の Unified CM リリースに対応する『*Bulk Administration Guide*』の指示に従ってください。これは、メンテナンス ガイド一覧から入手できます。

（注） デバイス構成ページの [プロダクト固有の設定（Product Specific Configuration Layout）] セクションにある設定は、エクスポートされたスプレッドシートで個別の列としては扱われません。 これらすべての設定、およびそこに含まれた情報は、デバイスごとに 1 つのセルの XML コードとして出力されます。 このセルにあるユーザ固有の情報を編集する場合は、慎重に行ってください。

重要 一括変更をするとき、変更がデバイスにプッシュされるように、次のメソッドを使用する2つのバッチ ジョブを作成し、実行することを推奨します。

1 ユーザをログアウトさせ、変更を適用する最初のバッチ ジョブを次のように作成します。

a [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

b [一括管理（Bulk Administration）] > [電話（Phones）] > [電話の更新（Update Phones）] > [クエリー（Query）] の順に選択します。

c 更新するデバイスを検索し、[次へ（Next）] を選択します。

d デバイスで変更する値を更新します。

注意：自動的に一括変更を Cisco Jabber for iPhone アプリケーションに伝搬させるには、Cisco Dual Mode for iPhone デバイスの [プロダクト固有の設定（Product Specific Configuration Layout）]セクションに移動し、[エンドユーザの設定変更を許可（Allow End User Configuration Editing）] パラメータを [無効（Disabled）] または [非許可（Restricted）] に設定します。

[エンド ユーザの設定変更を許可（Allow End User Configuration Editing）] パラメータを [有効（Enabled）] に設定した場合、変更を有効にするには、Cisco Jabber for iPhone アプリケーションを再度プロビジョニングする必要があります。

e [ログアウト/リセット/リスタート（Logout/Reset/Restart）] セクションで、[更新前にユーザをログアウト（Logout Users Before Update）] チェックボックスをオンにして、[設定の適用（Apply Config）] オプション ボタンを選択します。

f [ジョブ情報（Job Information）] セクションで、バッチ ジョブをすぐに実行するか、後で実行するかを選択します。

最初のバッチ ジョブは、2 番目のバッチ ジョブを実行する前に実行を終了している必要があります。 後で実行するようにバッチ ジョブをスケジュールする場合は、2 番目のジョブを実行する前に Unified CM が最初のジョブを完了させることができるように、十分な時間を取ってください。 ジョブのスケジューリングの詳細については、「Scheduling Jobs」を参照してください。

2 すべての Cisco Dual Mode for iPhone デバイスをリセットする 2 番目のバッチ ジョブを次のように作成します。

a [一括管理（Bulk Administration）] > [電話（Phones）] > [電話の更新（Update Phones）] > [クエリー（Query）] の順に選択します。

b 更新するデバイスを検索し、[次へ（Next）] を選択します。

c デバイスで変更する値を更新します。

d [ログアウト/リセット/リスタート（Logout/Reset/Restart）] セクションで、[更新前にユーザをログアウト（Logout Users Before Update）] チェックボックスがオフであることを確認して、[電話のリセット（Reset Phone）] オプション ボタンを選択します。

e [ジョブ情報（Job Information）] セクションで、バッチ ジョブをすぐに実行するか、後で実行するかを選択します。

自動セットアップ リンクの準備（任意）

設定を Cisco Jabber に手動入力するのではなく、電子メール メッセージのリンクをタップすることで、Cisco Jabber に設定を自動入力できるようにすると、ユーザの設定プロセスを簡略化できます。

このリンクでは、Unified CM の [電話の設定（Phone Configuration）] ページにある [プロダクト固有の設定（Product Specific Configuration Layout）] セクションの情報が、iPhone の Cisco Jabber アプリケーションの設定に転送されます。 初回起動時に、Cisco Jabber は必要なパスワードの入力をユーザに求めます。

URL に次の情報を含めることができます。

- tu：ユーザ名
- td：デバイス ID
- ts：TFTP サーバ
- tt：セカンダリまたはバックアップ TFTP サーバ

手順

ステップ 1 ユーザごとに、固有の設定リンクを作成します。
次の形式を使用します。`tctprov://connect?tu=username&td=Cisco Dual Mode for iPhone device ID&ts=TFTP server IP address&tt=Secondary TFTP server IP address`

例：
tctprov://connect?tu=jsmith&td=TCTJSMITH&ts=192.0.2.41&tt=192.0.2.42

ステップ 2 この製品に関する必要なすべての情報をユーザに提供できるようになるまで、このリンクは隠しておきます。

ステップ 3 Unified CM でユーザのセット アップが終了したら、各ユーザに一意のリンクと使用手順をその他の必要な情報とともに送信します。

他のアプリケーションからのCiscoJabberの相互起動（任意）

この機能により、開発者はサードパーティ製のアプリケーションから Cisco Jabber を起動することができます。 URL を構築して別のアプリケーションから開くことで、アプリケーションから Cisco Jabber を起動することを可能にします。

アプリケーションから Cisco Jabber を相互起動するには、次の形式で URL を開くようにアプリケーションをセットアップします。

```
ciscotel://<phonenumber>
```

例

- `ciscotel://98255550528`
- `ciscotel://(506)555-4444`

（注） Web ページのフィールドに ciscotel 形式の URL を追加できます。 ユーザが URL をタップすると、Cisco Jabber は URL に含まれる番号を自動的にコールします。 「Notes」などの URL を開くことができるアプリケーションに、この形式で電話番号を追加することができます。

（注） どの電話番号形式をサポートするのかは、URL を開くアプリケーションによって異なります。

ユーザへの指示

Unified CM でデバイスのセットアップが完了したら、ユーザに次の情報を提供してください。

- 社内 Wi-Fi ネットワークに電話を接続するための操作手順。 この手順は、Cisco Jabber とは独立した手順です。
- Cisco Jabber のセットアップの手順を含むユーザ マニュアル。http://www.cisco.com/en/US/products/ps11596/products_user_guide_list.html から入手可能です。
- Cisco Jabber の追加設定手順。

  自動セットアップ

  自動セットアップ リンクを設定する場合は、次の手順とともに電子メールでリンクを指定してください。

（注） 複数の Cisco Dual Mode for iPhone デバイスを持つユーザについては、どの電子メール メッセージがどのデバイスに関するものかを明確にするようにしてください。

1. App Store から無料で提供されている、Cisco Jabber をダウンロードしてインストールします。
2. iPhone を再起動します。
3. 設定の電子メール メッセージを iPhone で開きます。
4. リンクをタップすると、Cisco Jabber が自動的に設定されます。

手動セットアップ

自動セットアップ リンクを作成しない場合は、ユーザに次の情報を提供してください。

- App Store から無料で提供されている Cisco Jabber をダウンロードしてインストールする手順。
- TFTP サーバの IP アドレス。
- たとえば `TCT_JSMITH` などの、ユーザの Cisco Dual Mode for iPhone デバイスの名前。

  デバイス名は、ユーザが Cisco Jabber に入力するときには、大文字と小文字は区別されません。

- （必要に応じて）社内ディレクトリにアクセスするために必要なクレデンシャル。
- （必要に応じて）SIP ダイジェストのパスワード。
- （必要に応じて）CCM ユーザのパスワード。 このパスワードは、デスクフォンの統合を有効にする場合に必要です。
- （必要に応じて）Cisco Jabber と Cisco Mobile 7.1 の両方の使用に関する詳細。 Cisco Unified Mobility Advantage（Cisco Mobile 7.1）と連携して実行される Cisco Unified Mobile Communicator アプリケーションも導入する場合は、次の点に注意します。
  - Unified CM Release 8.0 の場合：通話をダイヤルする際は、Cisco Unified Mobile Communicator の代わりに Cisco Jabber を使用する必要があります。
  - Unified CM Release 7.1.5 の場合：通話のダイヤルに、どちらのアプリケーションを使用してもかまいません。
  - すべての Unified CM リリースの場合：シスコは、ユーザがボイスメールにアクセスする際、Cisco Jabber からではなく Cisco Unified Mobile Communicator から行うことを推奨します。これは、Cisco Unified Mobile Communicator の方が、ボイスメールの機能が豊富なためです（新しいボイス メッセージの通知など）。

- （必要に応じて）ユーザが VPN を使用して社内ネットワークにリモート側からアクセスするために必要な情報。 Cisco AnyConnect Secure Mobility Client などの VPN クライアントをユーザがダウンロード、インストール、およびセットアップするのに役立つ手順を提供します。

  iPhone で Cisco AnyConnect Secure Mobility Client をインストールおよび使用する方法については、ユーザ ガイド リストにある最新の『*iPhone User Guide for Cisco AnyConnect Secure Mobility Client*』から取得できます。

  ユーザは Cisco AnyConnect Secure Mobility Client アプリケーションを次のいずれかの方法で入手できます。

  - **手動での方法**：ユーザに、Apple App Store から無料の Cisco AnyConnect Secure Mobility Client および Cisco Jabber for iPhone アプリケーションを手動でダウンロードするように依頼します。

    ヒント これらの 2 つのアプリケーションへのリンクを社内・組織内の Web ポータルにホストして、ユーザがそれらを見つけやすくなるようにします。

  - **自動化された方法**：Mobile Device Manager（MDM）ソフトウェアを使用してアプリケーションをデバイスにプッシュし、デバイスが登録後に 2 つのアプリケーションを自動的に受信するようにします。 MDM の使用方法についての詳細は、関連するサードパーティの資料を参照してください。

- Cisco Jabber による緊急番号の使用に関する詳細。 Unified CM の [緊急電話番号（Emergency Numbers）] フィールドに定義されている緊急電話番号にユーザがダイヤルする場合、Cisco Jabber はネイティブの iPhone ダイヤラを使用します。 詳細については、ユーザ デバイスの追加, （18 ページ）を参照してください。

ポートとプロトコルのリスト

次の表に、Cisco Jabber にあるポートとプロトコルを示します。 各エントリの持続期間は「エフェメラル」です。

表 *5*：*Cisco Jabber* のポートとプロトコル

機能	プロトコル	ネットワーク プロトコル	ポート	備考
Unified CM の登録	TCP	TCP	5060	Unified CM の登録の SIP ポート
電話機サービス	TFTP	UDP	69、次にエフェメラル	該当なし

機能	プロトコル	ネットワークプロトコル	ポート	備考
デスクフォンの統合	QBE	TCP	2748	該当なし
メディア	RTP	UDP	16384 ～ 32766	この範囲は、デバイス設定ファイル内で Unified CM によって指定されます。これらはデフォルトの値であり、任意の有効なポートを指定できます。
		UDP	2000 ～ 2050	簡易ファイル転送プロトコル（TFTP）サーバに接続して、TFTP ファイルのダウンロードに使用するクライアントのローカル ポート。
ディレクトリ	LDAP	TCP	389	LDAP（オプションで TLS を使用）
ディレクトリ	LDAPS	TCP	636	LDAPS
ディレクトリ	LDAP	TCP	3268	LDAP 経由の Active Directory グローバル カタログ
ディレクトリ	LDAPS	TCP	3269	LDAPS 経由の Active Directory グローバル カタログ
Unity Connection ボイスメール	IMAP	TCP	143	該当なし
Unity Connection ボイスメール	IMAP	TCP	7993	IMAP（SSL/TLS を使用）
エクステンションモビリティ			8080	クライアント

第 4 章

機能の設定

Cisco Jabber とデスクフォン間のアクティブ コール転送の有効化

はじめる前に

- ユーザのデスクフォン（プライマリ DN）の設定が完了し、内線および外線通話を発信および受信できることを確認します。

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

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

ステップ 3 デスクフォンに関連付けるユーザを検索します。

ステップ 4 ユーザ ID を選択して、[ユーザ情報（User Information）] ページを開きます。

a) [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）] を選択して、モバイル デバイスに関連付けるデスクフォンを検索します。

b) モバイル デバイスに関連付けるデバイスを選択して [選択/変更の保存（Save Selected/Changes）] を選択します。

c) [エンド ユーザ（End User）] ページに戻ります。

d) [CTI からのデバイスの制御を許可（Allow Control of Device from CTI）] チェックボックスがチェックされていることを確認します。

e) モバイル デバイスに関連付けるデスクフォンのプライマリ内線を選択します。

f) [権限情報（Permissions Information）] セクションで、ユーザ グループ リストに [標準 CTI 有効（Standard CTI Enabled）] を追加します。
8900 および 9900 シリーズ電話機の場合は、[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）] も追加します。

g) この手順であとから使用する、このユーザのユーザ ID を確認します。

h) [保存（Save）] を選択します。

ステップ 5 [デバイス（Device）] > [電話（Phone）] を選択して、モバイル デバイスに関連付けるデスクフォンを特定します。

a) [オーナーのユーザ ID（Owner User ID）] の値が正しいエンドユーザであることを確認します。

b) [CTI からのデバイスの制御を許可（Allow Control of Device from CTI）] チェックボックスがチェックされていることを確認します。
[電話の設定（Phone Configuration）] ウィンドウの [デバイス情報（Device Information）] セクションにこのオプションが表示されない場合、その電話機はこの機能をサポートしていません。

c) [保存（Save）] を選択します。

ステップ 6 [Cisco Dual Mode for iPhone] デバイスのページに移動します。

a) [オーナーのユーザ ID（Owner User ID）] の値が正しいエンドユーザであることを確認します。

b) [プロダクト固有の設定（Product Specific Configuration Layout）] セクションの [CTI 制御ユーザ名（CTI Control Username）] に、[エンド ユーザ（End User）] ページのユーザ ID を入力します。

c) [保存（Save）] を選択します。

ステップ 7 [電話番号情報（Directory Number Information）] ページに移動して、次の項目を確認します。

- [CTI からのデバイスの制御を許可（Allow Control of Device from CTI）] チェックボックスがオンになっている。

- [デバイスの関連付け（Associated Devices）] ボックスにデスクフォンとモバイル デバイスが表示されている。

ステップ 8 モバイル デバイスとデスクフォンを再起動します。

次の作業

- 次のいずれかの方法を使用してクレデンシャルを入力します。
  - Cisco Jabber を再起動して、ウィザードの手順を順番に実行します。
  - [設定（Settings）]>[電話サービス（Phone Services）]>[デスクの電話統合（CTI）（Desk Phone Integration (CTI)）] に進みます。
- エンド ユーザ設定の編集が有効な場合、電話サービス アカウントをリセットします。
  - デバイスの電話サービス アカウントを削除します。
  - アカウントをもう一度セットアップします。
- デスクフォンと Cisco Jabber の間でアクティブ コールを転送できることを確認するために設定をテストします。

重要 http://www.cisco.com/en/US/products/ps11596/products_user_guide_list.html にあるユーザ FAQ に記載されている操作手順を参照してください。

モバイル コネクトの設定

モバイル コネクト（旧称シングル ナンバー リーチ（SNR））を使用すると、次の条件で、勤務先の番号にかけた場合にネイティブの携帯電話番号が鳴るようにします。

- Cisco Jabber が使用できない。

  Cisco Jabber が再び使用できるようになり、社内ネットワークに接続されると、Unified CM はモバイル コネクトの使用ではなく、VoIP コールの発信に戻ります。
- ユーザが [常に DVO を使用（Always Use DVO）] Jabber 通話オプションを選択する。
- ユーザが [自動選択（Automatically select）] Jabber 通話オプションを選択し、このユーザが Wi-Fi ネットワークの外側にいる。

モバイル コネクトを設定するには、次の手順を実行します。

1. モバイル コネクトの有効化, （36 ページ）
2. モバイル コネクトが次の手順の 1 つまたは両方を使用して接続する 1 つまたは複数のリモート電話機の番号を指定します。

- （優先）モバイル デバイスの携帯電話番号を指定するには、モビリティ ID の追加，（37 ページ）を参照してください。
- （任意）代替電話番号を指定するには、リモート接続先の追加（任意），（39 ページ）を参照してください。

  代替番号は、自宅の電話番号、会議室の電話番号、デスクフォンの番号、2台目の携帯電話番号などの任意の電話番号のタイプです。

3 設定をテストします。

- モバイル デバイスで Cisco Jabber を終了します。 手順については、http://www.cisco.com/en/US/products/ps11596/products_user_guide_list.html の『*FAQ*』を参照してください。
- 別の電話から Cisco Jabber の内線にコールします。
- ネイティブなモバイル ネットワーク電話番号で呼び出し音が鳴り、それに応答するとコールが接続されることを確認します。

モバイル コネクトの有効化

モバイル コネクトをエンド ユーザが使用できるようにするには、次の手順を使用します。

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

ステップ 2 携帯電話番号に設定済みの、既存のリモート宛先またはモビリティ ID を探して削除します。

ステップ 3 ユーザの [エンド ユーザ（End User）] ページに移動します。

a) [モビリティ情報（Mobility Information）] セクションで、[モビリティの有効化（Enable Mobility）] チェックボックスをオンにします。
b) Unified CM Release 9.0 以前であれば、プライマリ ユーザ デバイスを指定します。
c) [保存（Save）] を選択します。

ステップ 4 Cisco Dual Mode モバイル デバイス設定のデバイス ページに移動します。

a) 次の情報を入力します。

設定	情報
ソフトキー テンプレート（Softkey Template）	[モビリティ（Mobility）] ボタンが含まれたソフトキー テンプレートを選択します。 ソフトキー テンプレートの設定については、ご使用のリリースの『*Cisco Unified Communications Manager Administration Guide*』を参照してください。 このマニュアルは、メンテナンス ガイド一覧から参照できます。

設定	情報
モビリティ ユーザ ID（Mobility User ID）	ユーザを選択します。
オーナーのユーザ ID（Owner User ID）	ユーザを選択します。 値は、モビリティ ユーザ ID と一致する必要があります。
再ルーティング用コーリング サーチ スペース（Rerouting Calling Search Space）	次の両方を含む再ルーティング用コーリング サーチ スペースを選択します。 • ユーザのデスクフォン内線のパーティション。 この要件は、ルーティング コール用ではなく、Dial via Office 機能を提供するためにシステムで使用されます。 • 携帯電話番号へのルート。携帯電話番号へのルート（つまり、ゲートウェイ/トランク パーティション）には、デバイスと関連付けられた社内内線のパーティションより高い優先順位を設定する必要があります。 Cisco Jabber を使用すると、デバイスの携帯電話番号と異なるコールバック番号を Dial via Office-Reverse コールに対して指定でき、どのコールバック番号に到達可能かが再ルーティング コーリング サーチ スペースにより制御される点に注目してください。 ユーザが代替番号を持つDVO コールバック番号を設定した場合は、代替電話番号の宛先へのルートを指定するためにトランクのコーリング サーチ スペース（CSS）を設定している必要があります。

b) [保存（Save）] を選択します。

モビリティ ID の追加

モバイル デバイスの携帯電話番号を接続先番号として指定するためにモビリティ ID を追加するには、次の手順を使用します。 この接続先番号は Dial via Office やモバイル コネクトなどの機能によって使用されます。

モビリティ ID を追加するときに指定できるのは 1 つの番号だけです。 2 台目のモバイル デバイスの携帯電話番号などの代替番号を指定する場合は、リモート接続先を設定できます。 モビリティ ID の設定の特性は、リモート接続先の設定と同一です。

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

ステップ 2 Cisco Dual Mode モバイル デバイス設定のデバイス ページに移動します。

ステップ 3 [関連付けられたモビリティ ID（Associated Mobility Identity）] セクションで [新規モビリティ ID の追加（Add a New Mobility Identity）] を選択します。

ステップ 4 [接続先番号（Destination Number）] として携帯電話番号を入力します。
この番号は、発信ゲートウェイでルーティングできる必要があります。 通常、この番号は完全な E.164 番号です。

（注） ユーザの Dial Via Office - Reverse 機能を有効にすると、ユーザのモビリティ ID の接続先番号を入力する必要があります。

Dial Via Office - Reverse を有効にして接続先番号をモビリティ ID で空にしておくと、次の状態が発生します。

- ユーザが 3G ネットワークおよび VPN を使用しているときに [自動選択（Automatically select）] Jabber 通話オプションを選択すると、電話サービスが接続できない。
- ユーザがどのタイプのネットワークでも [常に DVO を使用（Always use DVO）] Jabber 通話オプションを選択すると、電話サービスが接続できない。
- ログに電話サービスが接続できない理由が示されない。

Dial Via Office - Reverse を使用すると、接続先番号を入力した後に、更新されたユーザのモビリティ ID の接続先番号が、システムによってクライアントに自動的にプッシュされなくなります。 この問題を回避するには、ユーザに次のいずれかを実行するように依頼してください。

- Cisco Jabber for iPhone 設定で、[DVO コールバック番号（DVO Callback Number）] フィールドの電話番号を手動で更新します。
- Cisco Jabber for iPhone 設定で、[DVO コールバック番号（DVO Callback Number）] フィールドの現在の番号を削除してから Cisco Jabber for iPhone を終了し、再起動します。

iPhone 設定または Cisco Jabber for iPhone 設定の使用方法の詳細については、FAQ を参照してください。

ステップ 5 コール タイマーの初期値を入力します。
これらの値によって、モバイルデバイスのクライアントで呼び出し音を鳴らす前に、モバイルデバイス プロバイダーのボイスメールに通話がルーティングされることがなくなります。

詳細については、Unified CM のオンライン ヘルプを参照してください。

例：

設定	推奨する初期値
呼び出し開始タイマー（Answer too soon timer）	3000
呼び出し終了タイマー（Answer too late timer）	20000
呼び出し前の遅延タイマー（Delay before ringing timer）	0 （注） この設定はDVO-R のコールには適用されません。

ステップ 6 [モバイル コネクトの有効化（Enable Mobile Connect）] チェックボックスをオンにします。

ステップ 7 Dial via Office 機能を [モビリティ プロファイル（Mobility Profile）] ドロップダウン リストで設定している場合は、次のオプションのいずれか 1 つを選択します。

オプション	説明
空欄のまま	ユーザにエンタープライズ機能アクセス番号（EFAN）を使用させる場合は、このオプションを選択します。
モビリティ プロファイル（Mobility Profile）	ユーザに EFAN の代わりにモビリティ プロファイルを使用させる場合は、自分が作成したモビリティ プロファイルを選択します。

ステップ 8 携帯番号に通話をルーティングするスケジュールを設定します。

ステップ 9 [保存（Save）] を選択します。

関連トピック

エンタープライズ機能アクセス番号の設定, （47 ページ）

リモート接続先の追加（任意）

接続先番号として任意の代替番号を指定するためにリモート接続先を追加するには、次の手順を使用します。 モビリティ ID の設定の特性は、リモート接続先の設定と同一です。

代替番号は、自宅の電話番号、会議室の電話番号、デスクフォン番号、または追加のモバイル デバイス向けの複数の携帯電話番号などの任意の電話番号のタイプです。 複数のリモート接続先を追加できます。

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

ステップ 2 Cisco Dual Mode モバイル デバイス設定のデバイス ページに移動します。

ステップ 3 [関連付けられたリモート接続先（Associated Remote Destinations）] セクションで、[新規リモート接続先の追加（Add a New Remote Destination）] を選択します。

ステップ 4 [接続先番号（Destination Number）] として目的の携帯電話番号を入力します。
この番号は、発信ゲートウェイでルーティングできる必要があります。 通常、この番号は完全な E.164 番号です。

ステップ 5 コール タイマーの初期値を入力します。
これらの値によって、モバイルデバイスのクライアントで呼び出し音を鳴らす前に、モバイルデバイス プロバイダーのボイスメールに通話がルーティングされることがなくなります。

詳細については、Unified CM のオンライン ヘルプを参照してください。

例：

設定	推奨する初期値
呼び出し開始タイマー（Answer too soon timer）	3000
呼び出し終了タイマー（Answer too late timer）	20000
呼び出し前の遅延タイマー（Delay before ringing timer）	0 （注） この設定はDVO-Rのコールには適用されません。

ステップ 6 [モバイル コネクトの有効化（Enable Mobile Connect）] チェックボックスをオンにします。

ステップ 7 携帯番号に通話をルーティングするスケジュールを設定します。

ステップ 8 [保存（Save）] を選択します。

モバイル ネットワークへのアクティブ VoIP コールの転送

ユーザはアクティブな VoIP コールを、Cisco Jabber からモバイル ネットワーク上の自分の携帯電話番号に転送できます。 この機能は、ユーザが通話しながらWi-Fiネットワークを離れる場合（たとえば、建物を離れて車まで歩いていくときなど）や、Wi-Fiネットワークを経由すると音声品質に問題がある場合に便利です。 Cisco Jabber のこの機能は「モバイル ネットワークの使用」と呼ばれます。

この機能の実装方法は 2 種類です。 無効にすることもできます。

実装方法	説明	方法
ハンドオフ DN	iPhone は、モバイル ネットワークを使用して Unified CM にコールします。 この方法には、ダイヤルイン（DID）番号が必要です。 サービス プロバイダーは、設定する DID の値を正確に提供する必要があります。 または、H.323 または SIP を使用した Cisco OS ゲートウェイで Cisco Unified CM に通信する場合は、Cisco IOS を使用して、ゲートウェイで着信者番号を操作して、番号が Unified CM のハンドオフ番号で設定したとおりに通知するようにできます。 この実装方法を選択し、機能しなかった場合、システムは自動的にモビリティ ソフトキーを試行します。 この方法は、iPod Touch デバイスでは動作しません。	ハンドオフ DN の設定, （42 ページ）を参照してください。
モビリティ ソフトキー	Unified CM が、iPhone の PSTN モバイル サービス プロバイダーの電話番号に発信します。	VoIP からモバイル ネットワークへのアクティブ コールの転送の有効化, （44 ページ）を参照してください。
上記以外	ユーザから利用できるようにしない場合は、この機能を無効にします。	[Cisco Dual Mode for iPhone] デバイス ページの [プロダクト固有の設定（Product Specific Configuration Layout）] セクションで、[モバイル ネットワークへ転送（Transfer to Mobile Network）] オプションに対して [無効（Disabled）] を選択します。

VoIP からモバイル ネットワークへのアクティブ コールのハンドオフの有効化

ハンドオフ DN の設定

はじめる前に

必要な値を識別します。 選択する値は、ゲートウェイが渡す電話番号によって異なります（たとえば、7 桁や 10 桁など）。

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

ステップ 2 [コール ルーティング（Call Routing）] > [モビリティ（Mobility）] > [ハンドオフ設定（Handoff Configuration）] を選択します。

ステップ 3 デバイスが VoIP コールをモバイル ネットワークにハンドオフする際に使用するダイヤルイン（DID）番号のハンドオフ番号を入力します。
サービス プロバイダーは、設定する DID の値を正確に提供する必要があります。 または、H.323 または SIP を使用した Cisco IOS ゲートウェイで Cisco Unified CM に通信する場合は、Cisco IOS を使用して、ゲートウェイで着信者番号を操作して、番号が Unified CM のハンドオフ番号で設定したとおりに通知するようにできます。

（注） Unified CM で着信 DID 番号を設定されたハンドオフ DN と照合するのにトランスレーション パターンまたはその他の操作は使用できません。

ステップ 4 ハンドオフ DID の [ルート パーティション（Route Partition）] を選択します。
このパーティションは、リモート接続先インバウンド コーリング サーチ スペース（CSS）で参照するコーリング サーチ スペースで、使用できる必要があります。具体的に参照されるコーリング サーチ スペースは、ゲートウェイ、トランクの着信 CSS またはリモート接続先プロファイルの CSS です。

この機能は、このページのその他のオプションを使用しません。

ステップ 5 [保存（Save）] を選択します。

発信者 ID とモビリティ ID の一致

許可された電話機だけが外線発信できるようにするには、システム内に設定された電話機から発信されるようにする必要があります。 そのため、システムは要求元電話番号の発信者 ID と、既存のモビリティ ID との照合を試みます。 デフォルトでは、デバイスがハンドオフ機能を起動したときに、ゲートウェイから Unified CM に渡される発信者 ID が、そのデバイス用として入力したモビリティ ID 番号と完全に一致している必要があります。

ただし、システムの設定によっては、こうした番号が完全一致しない場合があります。 たとえば、モビリティ ID 番号に国番号が含まれ、発信者 ID には含まれないことがあります。 その場合は、部分一致を認識するようシステムを設定する必要があります。

異なるエリア コードまたは異なる国に、同じ電話番号が存在する可能性について考えておく必要があります。また、サービスプロバイダーが可変桁数の通話を識別する場合は、部分一致に影響があることに注意してください。 たとえば、ローカル コールは 7 桁（555 0123 など）を使用して識別されるが、エリア外コールは 10 桁（408 555 0199 など）を使用して識別されることがあります。

はじめる前に

- モビリティ ID を設定します。 モビリティ ID の追加, （37 ページ）を参照してください。
- この手順をすべて行う必要があるかどうかを確認してください。
  デバイスを使用してシステムにダイヤルインし、発信者 ID の値と、モビリティ ID の宛先番号を比較します。 値が一致しない場合は、この手順に従う必要があります。 予想されるすべてのロケールおよびエリア コード内で支給されたデバイスに対して、この手順を繰り返します。

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

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 アクティブ サーバを選択します。

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 [発信者 ID とリモート接続先の照合（Matching Caller ID with Remote Destination）] を選択し、この値に関する重要な情報を確認します。

ステップ 7 [部分一致による発信者 ID とリモート接続先の照合（Partial Match for Matching Caller ID with Remote Destination）] を選択します。

ステップ 8 [発信者 ID の部分一致の桁数（Number of Digits for Caller ID Partial Match）] を選択し、この値に関する重要な要件を確認します。

ステップ 9 部分一致に必要な桁数を入力します。

ステップ 10 [保存（Save）] を選択します。

ハンドオフのための追加のユーザおよびデバイス設定のセットアップ

はじめる前に

- Unified CM のユーザ デバイスを設定します。

- ユーザのモビリティ ID を設定します。

手順

ステップ 1 Unified CM で、[Cisco Dual Mode for iPhone] デバイス ページの [モバイル ネットワークへ転送（Transfer to Mobile Network）] オプションにある [ハンドオフ DN 機能を使用（Use Handoff DN Feature）] を選択します。
iPod Touch デバイスでは、この方法は割り当てないでください。 代わりにモビリティ ソフトキーの方法を使用します。

ステップ 2 iOS デバイスで、[設定（Settings）] > [電話（Phone）] > [発信者 ID を表示（Show My Caller ID）] をタップして、発信者 ID がオンになっていることを確認します。

ステップ 3 この機能をテストしてください。

VoIP からモバイル ネットワークへのアクティブ コールの転送の有効化

手順

ステップ 1 システム レベル設定で、電話のコール状態が「接続中（Connected）」および「オンフック（On-hook）」のときに、[モビリティ（Mobility）] ソフトキーが表示されることを確認します。

a) [デバイス（Device）]>[デバイスの設定（Device Settings）]>[ソフトキー テンプレート（Softkey Template）] で、デバイスにモバイル コネクトを設定したときに選択したソフトキー テンプレートを選択します。
b) 右上の [関連リンク（Related Links）] リスト ボックスで、[ソフトキー レイアウトの設定（Configure Softkey Layout）] を選択し、[移動（Go）] を選択します。
c) [接続時（Connected）]状態を選択し、選択されているソフトキーのリストの中にモバイル キーがあることを確認してから、[オンフック（On Hook）] 状態でも同様の手順を実行します。

ステップ 2 Unified CM のユーザごとおよびデバイスごとの設定の場合は、モバイル デバイスのモビリティ ID とモバイル コネクトの設定を確認します。
転送機能が動作するようになったら、ユーザは自分の都合に合わせて、転送機能をいじることなくモバイル コネクトを有効にしたり無効にしたりできるようになります。

デバイスが iPod Touch の場合は、代替電話番号（ユーザの携帯電話など）を使用してモビリティ ID を設定できます。

a) [Cisco Dual Mode for iPhone] デバイス ページの [オーナーのユーザ ID（Owner User ID）] を選択します。

b) [プロダクト固有の設定（Product Specific Configuration Layout）] セクションの [モバイル ネットワークへ転送（Transfer to Mobile Network）] オプションで、[モビリティ ソフトキーを使用（Use Mobility Softkey）] を選択します。

ステップ 3 デバイス ページの [デバイス（Device）] > [電話（Phone）] に移動して、TCT デバイスを見つけます。

ステップ 4 [ユーザ ロケール（User Locale）] フィールドで、[英語、アメリカ合衆国（English, United States）] を選択します。

Dial Via Office の設定

重要 DVO-R 機能には以下が必要です。

- Cisco Jabber for iPhone client, Release 9.1(1) 以降。
- Unified CM 9.1(1a)（2013 年 2 月リリース）。

Dial via Office 機能と組み合わせて使用できるユーザ制御のボイスメールの回避は、Unified CM Release 9.0 以降でのみ使用可能です。 タイマー制御のボイスメールの回避は、Unified CM Release 6.0 以降で使用できます。

Dial via Office 機能はエクステンション モビリティ機能ではサポートされません。

Dial via Office が有効になっている場合、アプリケーションは SIP ダイジェストでプロビジョニングできません。

Dial Via Office（DVO）機能を使用すると、ユーザはデバイスの番号計画を使用して、社内番号で Cisco Jabber からコールを発信できます。

Dial via Office コールには、Dial via Office - Reverse（DVO-R）と Dial via Office - Forward（DVO-F）の 2 種類があります。 Cisco Jabber は Dial via Office - Reverse（DVO-R）コールをサポートします。 DVO-R は次のように動作します。

1. ユーザが Dial via Office-Reverse コールを開始します。
2. クライアントは、携帯電話番号を Unified CM に通知します。
3. Unified CM は、携帯電話番号にコールし、接続します。
4. Unified CM はユーザがダイヤルした番号にコールし、接続します。
5. Unified CM は、2 セグメントを接続します。
6. ユーザおよび着信者は、通常のコールと同様に続けます。

着信コールは、ユーザがクライアントで設定した Jabber 通話オプションに従い、モバイル コネクトまたはインターネットを使用します。 Dial via Office では、モバイル コネクトが動作する必要

はありません。ただし、誰かが社内番号にかけた場合、ネイティブのモバイル番号で呼び出し音を鳴らすことができるようにモバイル コネクトを有効にすることを推奨します。Unified CM ユーザ ページから、モバイル コネクトを有効または無効にしたり、設定を使用してモバイル コネクトの動作を調整したりすることができます（たとえば、時間帯ルーティングや呼び出し前の遅延タイマーの設定など）。モバイル コネクトの設定の詳細については、モバイル コネクトの設定, （35 ページ）を参照してください。

次の表で、着信コールと発信コールに使用する通話メソッドについて説明します。通話メソッド（インターネット、モバイル コネクト、DVO-R、ネイティブ携帯電話コール）は、選択した Jabber 通話オプションとネットワーク接続によって異なります。

表 *6*：さまざまなネットワーク接続を経由して *Jabber* 通話オプションとともに使用する通話メソッド

<table>
<tr><th rowspan="2">接続</th><th colspan="5">コール オプション（Call Options）</th></tr>
<tr><th colspan="2">常にインターネットを使用（Always use Internet）</th><th colspan="2">常に DVO を使用（Always use DVO）</th><th>自動選択（Auto Select）</th></tr>
<tr><td rowspan="3">社内 Wi-Fi
社外 Wi-Fi
モバイル ネットワーク（3G、4G）</td><td rowspan="3">発信：インターネット</td><td rowspan="3">着信：インターネット</td><td rowspan="3">発信：DVO-R</td><td rowspan="3">着信：モバイル コネクト</td><td>発信：インターネット</td><td>着信：インターネット</td></tr>
<tr><td rowspan="2">発信：DVO-R</td><td rowspan="2">着信：モバイル コネクト</td></tr>
<tr><td colspan="2">着信：モバイル コネクト</td></tr>
<tr><td>Jabber 未登録</td><td colspan="5">発信：ネイティブの携帯電話</td></tr>
</table>

Dial via Office-Reverse（DVO-R）を設定するには、以下の手順に従ってください。

1. DVO-R をサポートするように Unified CM を設定します。DVO-R をサポートするための Unified CM の設定, （47 ページ）を参照してください。
2. 各 Cisco Dual Mode for iPhone デバイスで DVO を有効にします。各デバイスに対する Dial Via Office の設定, （49 ページ）を参照してください。

DVO-R をサポートするための Unified CM の設定

DVO-R をサポートするように Unified CM を設定するには、次の手順を実行します。

1 次の手順のいずれかまたは両方を実行します。

- エンタープライズ機能アクセス番号の設定, （47 ページ）
- モビリティ プロファイルの設定, （48 ページ）

2 デバイス COP ファイルのバージョンの確認, （6 ページ）

3 必要な場合は、モバイル ID 電話番号へのコールを発信ゲートウェイにルーティングするアプリケーション ダイヤル ルールを作成します。 モバイル ID 電話番号の形式がアプリケーション ダイヤル ルールに適合することを確認します。

詳細については、ダイヤル ルール, （7 ページ）を参照してください。

（注） DVO-R 機能には以下が必要です。

- Cisco Jabber for iPhone client, Release 9.1(1) 以降。
- Unified CM 9.1(1a)（2013 年 2 月リリース）。

エンタープライズ機能アクセス番号の設定

Dial via Office-Reverse を使用するすべての Cisco Jabber コールにエンタープライズ機能アクセス番号を設定するには、この手順を使用します。

エンタープライズ機能アクセス番号は、この目的のために別の番号がモビリティ プロファイルに設定されていない場合、Cisco Unified Communications Manager が、携帯電話およびダイヤル番号とのコールに使用する番号です。

はじめる前に

- エンタープライズ機能アクセス番号（EFAN）として使用するダイヤルイン方式（DID）番号を予約します。 モビリティ プロファイルを設定済みの場合、この手順はオプションです。
- この番号に要求される形式を決定します。 選択する正確な値は、ゲートウェイが渡す電話番号に依存します（たとえば、7桁または10桁）。 エンタープライズ機能アクセス番号はルーティング可能な番号である必要があります。

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

ステップ 2 [コール ルーティング（Call Routing）]>[モビリティ（Mobility）]>[エンタープライズ機能アクセス番号設定（Enterprise Feature Access Number Configuration）] の順に選択します。

ステップ 3 [新規追加（Add New）] を選択します。

ステップ 4 [番号（Number）] フィールドに、エンタープライズ機能アクセス番号を入力します。
システム内で一意の DID 番号を入力します。

国際番号計画をサポートするには、この番号の前に \+ を付けます。

ステップ 5 [ルート パーティション（Route Partition）] ドロップダウン リストから、エンタープライズ機能アクセスに必要な DID のパーティションを選択します。
このパーティションは、[システム（System）]>[サービス パラメータ（Service Parameters）] にある、[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)）] 中の [リモート接続先のインバウンド コーリング サーチ スペース（Inbound Calling Search Space for Remote Destination）] で指定された先のコーリング サーチ スペースから参照できるようにする必要があります。 この設定で参照するコーリング サーチ スペースは、ゲートウェイまたはトランクのインバウンドコーリング サーチ スペースか、デバイスの [電話の設定（Phone Configuration）] 画面で割り当てられたコーリング サーチ スペースです。

ユーザが代替番号を持つDVOコールバック番号を設定した場合は、代替電話番号の宛先へのルートを指定するためにトランクのコーリング サーチ スペース（CSS）を設定している必要があります。

ステップ 6 [説明（Description）] フィールドにモビリティ エンタープライズ機能アクセス番号の説明を入力します。

ステップ 7 （任意）このエンタープライズ機能アクセス番号をこのシステムのデフォルトにする場合は、[デフォルトのエンタープライズ機能アクセス番号（Default Enterprise Feature Access Number）] チェックボックスをオンにします。

ステップ 8 [保存（Save）] を選択します。

モビリティ プロファイルの設定

Cisco Jabber デバイスのモビリティ プロファイルを設定するには、次の手順を使用します。 エンタープライズ機能アクセス番号を設定済みの場合、この手順はオプションです。

モビリティ プロファイルを使用して、モバイル クライアントの Dial via Office-Reverse を設定できます。 モビリティ プロファイルを設定したら、個々のユーザや、リージョンやロケーションのユーザなどのユーザのグループに割り当てることができます。

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

ステップ 2 [コール ルーティング（Call Routing）] > [モビリティ（Mobility）] > [モビリティ プロファイル（Mobility Profile）] の順に選択します。

ステップ 3 [モビリティ プロファイル情報（Mobility Profile Information）] セクションで、[名前（Name）] フィールドにモビリティ プロファイルの説明的な名前を入力します。

ステップ 4 [Dial-via-Office-Reverse コールバック（Dial via Office-Reverse Callback）] セクションで、[コールバック発信者 ID（Callback Caller ID）] フィールドに、クライアントが Unified CM から受信するコールバック コールの発信者 ID を入力します。

ステップ 5 [保存（Save）] をクリックします。

デバイス COP ファイルのバージョンの確認

このリリースの Cisco Jabber に正しいデバイス COP ファイルを使用していることを確認するには、次の手順を使用します。

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

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

ステップ 3 [新規追加（Add New）] をクリックします。

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、[Cisco Dual Mode for iPhone] を選択します。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [プロダクト固有の設定（Product Specific Configuration Layout）] セクションまでスクロール ダウンし、[Dial via Office] ドロップダウン リストが表示されることを確認します。
[Dial via Office] ドロップダウン リストが表示された場合、COP ファイルはご使用のシステムにすでにインストールされています。

[Dial via Office] ドロップダウン リストが表示されない場合は、正しい COP ファイルを探してダウンロードします。 詳細については、必要なファイル，（4 ページ）を参照してください。

各デバイスに対する Dial Via Office の設定

各 Cisco Jabber デバイスに Dial via Office-Reverse を設定するには、次の手順を使用します。

1 各ユーザのモビリティ ID を追加します。
2 各デバイスで Dial via Office を有効にします。
3 モバイル コネクトを有効にしている場合、モバイル コネクトが動作することを確認します。デスクフォンの内線にダイヤルすると、関連付けられたモビリティ ID で指定された電話番号で呼び出し音が鳴るはずです。

モビリティ ID の追加

モバイル デバイスの携帯電話番号を接続先番号として指定するためにモビリティ ID を追加するには、次の手順を使用します。 この接続先番号は Dial via Office やモバイル コネクトなどの機能によって使用されます。

モビリティ ID を追加するときに指定できるのは 1 つの番号だけです。 2 台目のモバイル デバイスの携帯電話番号などの代替番号を指定する場合は、リモート接続先を設定できます。 モビリティ ID の設定の特性は、リモート接続先の設定と同一です。

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。
ステップ 2 Cisco Dual Mode モバイル デバイス設定のデバイス ページに移動します。
ステップ 3 [関連付けられたモビリティ ID（Associated Mobility Identity）] セクションで [新規モビリティ ID の追加（Add a New Mobility Identity）] を選択します。
ステップ 4 [接続先番号（Destination Number）] として携帯電話番号を入力します。
この番号は、発信ゲートウェイでルーティングできる必要があります。 通常、この番号は完全な E.164 番号です。

（注） ユーザの Dial Via Office - Reverse 機能を有効にすると、ユーザのモビリティ ID の接続先番号を入力する必要があります。

Dial Via Office - Reverse を有効にして接続先番号をモビリティ ID で空にしておくと、次の状態が発生します。

- ユーザが 3G ネットワークおよび VPN を使用しているときに [自動選択（Automatically select）] Jabber 通話オプションを選択すると、電話サービスが接続できない。
- ユーザがどのタイプのネットワークでも [常に DVO を使用（Always use DVO）] Jabber 通話オプションを選択すると、電話サービスが接続できない。
- ログに電話サービスが接続できない理由が示されない。

Dial Via Office - Reverse を使用すると、接続先番号を入力した後に、更新されたユーザのモビリティ ID の接続先番号が、システムによってクライアントに自動的にプッシュされなくなります。 この問題を回避するには、ユーザに次のいずれかを実行するように依頼してください。

- Cisco Jabber for iPhone 設定で、[DVO コールバック番号（DVO Callback Number）] フィールドの電話番号を手動で更新します。
- Cisco Jabber for iPhone 設定で、[DVO コールバック番号（DVO Callback Number）] フィールドの現在の番号を削除してから Cisco Jabber for iPhone を終了し、再起動します。

iPhone 設定または Cisco Jabber for iPhone 設定の使用方法の詳細については、FAQ を参照してください。

ステップ 5 コール タイマーの初期値を入力します。
これらの値によって、モバイルデバイスのクライアントで呼び出し音を鳴らす前に、モバイルデバイス プロバイダーのボイスメールに通話がルーティングされることがなくなります。

詳細については、Unified CM のオンライン ヘルプを参照してください。

例：

設定	推奨する初期値
呼び出し開始タイマー（Answer too soon timer）	3000
呼び出し終了タイマー（Answer too late timer）	20000
呼び出し前の遅延タイマー（Delay before ringing timer）	0 （注） この設定は DVO-R のコールには適用されません。

ステップ 6 [モバイル コネクトの有効化（Enable Mobile Connect）] チェックボックスをオンにします。

ステップ 7 Dial via Office 機能を [モビリティ プロファイル（Mobility Profile）] ドロップダウン リストで設定している場合は、次のオプションのいずれか 1 つを選択します。

オプション	説明
空欄のまま	ユーザにエンタープライズ機能アクセス番号（EFAN）を使用させる場合は、このオプションを選択します。
モビリティ プロファイル（Mobility Profile）	ユーザに EFAN の代わりにモビリティ プロファイルを使用させる場合は、自分が作成したモビリティ プロファイルを選択します。

ステップ 8 携帯番号に通話をルーティングするスケジュールを設定します。

ステップ 9 [保存（Save）] を選択します。

関連トピック

エンタープライズ機能アクセス番号の設定, （47 ページ）

各デバイス上での Dial Via Office の有効化

各デバイスで Dial Via Office を有効にするには、この手順を使用します。

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

ステップ 2 ユーザのデバイス ページに移動します。

ステップ 3 [デバイス情報（Device Information）] セクションで [Cisco Unified Mobile Communicator の有効化（Enable Cisco Unified Mobile Communicator）] チェックボックスをオンにします。

ステップ 4 ユーザのデバイス ページの [プロダクト固有の設定(Product Specific Configuration Layout)] セクションで、[Dial via Office] ドロップダウン リストを [有効(Enabled)] に設定します。

重要 DVO-R は、Unified CM Release 9.1 以降でのみサポートされています。 シスコは、Unified CM 8.6 で DVO-R を使用する Cisco Jabber をサポートするため、Service Update（SU）をまもなくリリースする予定です。 サポート対象外の Unified CM でこの設定を有効にすると、エンド ユーザには DVO 通話オプションが提示され、DVO-R コール確立の試行ができますが、そのコールは接続できません。

ステップ 5 [保存（Save）] を選択します。

ステップ 6 [設定の適用（Apply Config）] を選択します。

次の作業

この機能をテストしてください。

ボイスメール回避の設定

ボイスメール回避は、コールがモバイルサービスプロバイダーのボイスメールに応答することを防ぐ機能です。 この機能は、ユーザがモバイル デバイスの企業からモバイル コネクト コールを受信する場合に有効です。 また、着信 DVO-R コールがモバイル デバイスに発信されるときにも有効です。

次の 2 種類の方法のいずれかでボイスメール回避を設定できます。

- タイマー制御:（デフォルト）この方式では、コールがモバイル ユーザまたはモバイル サービス プロバイダーのボイスメールによって応答されるかどうかを確認するために Unified CM にタイマーを設定します。
- ユーザ制御:この方法では、コールを進める前に、DTMF トーンを生成するためにデバイスのキーパッド上の任意のキーを押すことを Unified CM に要求するように設定されます。

DVO-R を実装している場合、シスコは、ユーザ制御の音声回避を推奨します。 ユーザ制御ボイスメール回避を設定すると、この機能は DVO-R およびモバイル コネクト コールの両方に適用されます。

ボイスメール回避の詳細については、『Unified CM Features and Services Guide』の「Confirmed Answer and DVO VM detection」という項を参照してください。

タイマー制御ボイスメール回避の設定

タイマー制御のボイスメールの回避は、Unified CM Release 6.0 以降でサポートされています。

モビリティ ID またはリモート接続先で、[呼び出し開始タイマー（Answer Too Soon Timer）] および [呼び出し終了タイマー（Answer Too Late Timer）] を設定して、タイマー制御方式を設定します。 詳細については、モビリティ ID の追加, （37 ページ）またはリモート接続先の追加（任意）, （39 ページ）を参照してください。

ユーザ制御のボイスメール回避の設定

重要 ユーザ制御のボイスメールの回避は、Unified CM Release 9.0 以降で使用できます。

ユーザ制御のボイスメール回避を設定するには、次の手順を実行します。

1 Unified CM をユーザ制御のボイスメール回避をサポートするように設定する, （54 ページ）

2 次の手順のいずれか 1 つを実行して、デバイスにユーザ制御のボイスメール回避を設定します。

- モビリティ ID でのユーザ制御のボイスメール回避の有効化, （55 ページ）
- リモート接続先でのユーザ制御のボイスメール回避を有効化, （55 ページ）

重要 シスコは、エンドユーザがクライアントに設定した代替番号と DVO-R を使用する場合、ユーザ制御のボイスメール回避をサポートしません。代替番号は、ユーザがクライアントの [DVO コールバック番号（DVO Callback Number）] フィールドに入力した電話番号で、これはユーザのモビリティ ID に設定する電話番号と一致しません。

代替番号を使用してこの機能を設定する場合、Unified CM は、コールバックが誤った番号またはボイスメール システムに接続しても DVO-R コールを接続します。

Unified CM をユーザ制御のボイスメール回避をサポートするように設定する

Unified CM をユーザ制御のボイスメール回避をサポートするように設定するには、次の手順を使用します。

手順

ステップ 1 Unified CM にログインします。

ステップ 2 [ナビゲーション（Navigation）] フィールドで、[Unified CM の管理（Unified CM Administration）] を選択します。

ステップ 3 [システム（System）] > [サービス パラメータ（Service Parameters）] を選択します。

ステップ 4 [サーバ（Server）] ドロップダウン リストで、アクティブな United CM を選択します。

ステップ 5 [サービス（Service）] ドロップダウン リストで、[Cisco Call Manager（アクティブ）（Cisco Call Manager (Active)）] サービスを選択します。

ステップ 6 [クラスタ全体のパラメータ（システム - モビリティ シングル ナンバー リーチ ボイスメール）（Clusterwide Parameters (System - Mobility Single Number Reach Voicemail)）] セクションを設定します。

（注） このセクションでの設定は、Cisco Jabber に固有ではありません。 これらを設定する方法については、ご使用のリリースの『Cisco Unified Communication Manager Administrator Guide』の「Confirmed Answer and DVO VM detection」を参照してください。

ステップ 7 [保存（Save）] をクリックします。

モビリティ ID でのユーザ制御のボイスメール回避の有効化

エンド ユーザのモビリティ ID でユーザ制御のボイスメール回避を有効にするには、この手順を使用します。

はじめる前に

- Unified CM にアナンシエータを設定します。 詳細については、ご使用のリリースの『Cisco Unified Communication Manager Administrator Guide』の「Annunciator setup」の項を参照してください。
- Unified CM にメディア リソース グループを設定する場合は、メディア リソース グループにアナンシエータを設定します。 詳細については、ご使用のリリースの『Cisco Unified Communication Manager Administrator Guide』の「Media resource group setup」の項を参照してください。

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

ステップ 2 ユーザのデバイス ページに移動します。

ステップ 3 [関連付けられたモビリティ ID（Associated Mobility Identity）] セクションで、モビリティ ID のリンクをクリックします。

（注） ボイスメール回避機能が正常に動作することを確認するには、エンド ユーザが Cisco Jabber クライアントで入力する DVO コールバック番号が、モビリティ ID の [設定（Configuration）] 画面で入力する接続先番号と一致する必要があります。

ステップ 4 [シングル ナンバー リーチ ボイスメール ポリシー（Single Number Reach Voicemail Policy）] ドロップダウン リストで [ユーザ制御（User Control）] を選択します。

ステップ 5 [保存（Save）] をクリックします。

リモート接続先でのユーザ制御のボイスメール回避を有効化

エンド ユーザのリモート接続先でユーザ制御のボイスメール回避を有効にするには、この手順を使用します。

はじめる前に

- Unified CM にアナンシエータを設定します。 詳細については、ご使用のリリースの『Cisco Unified Communication Manager Administrator Guide』の「Annunciator setup」の項を参照してください。
- Unified CM にメディア リソース グループを設定する場合は、メディア リソース グループにアナンシエータを設定します。 詳細については、ご使用のリリースの『Cisco Unified

Communication Manager Administrator Guide』の「Media resource group setup」の項を参照してください。

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

ステップ 2 ユーザのデバイス ページに移動します。

ステップ 3 [関連付けられたリモート接続先（Associated Remote Destinations）] セクションで、関連付けられたリモート接続先のリンクをクリックします。

ステップ 4 [シングル ナンバー リーチ ボイスメール ポリシー（Single Number Reach Voicemail Policy）] ドロップダウン リストで [ユーザ制御（User Control）] を選択します。

ステップ 5 [保存（Save）] をクリックします。

ボイス ダイヤルのセットアップ

ボイス ダイヤルを使用すると、ユーザは社内ディレクトリにある名前を発音することで、番号をダイヤルできます（本機能は日本語には対応しておりません）。

ネットワークでボイス ダイヤルが使用可能な場合、Cisco Jabber ユーザはボイス ダイヤルのパイロット番号をダイヤルすると、どの電話機からでもボイス ダイヤル機能にいつでもアクセスできます。

次の設定のいずれかによりボイス ダイヤルを簡略化できます。

- ボイス ダイヤル モーションを有効にする（Enable Voice Dialing Motion）
- ボイス ダイヤルをお気に入りに追加する（Add Voice Dialing to Favorites）

はじめる前に

ネットワークでボイス ダイヤルが設定され、機能している必要があります。

一般使用のためにボイス ダイヤルを設定する方法については、『*System Administration Guide*』および『*Reference Guide for Cisco Unity Connection*』で、ディレクトリ ハンドラに関する説明を参照してください。これらのマニュアルは、http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html から入手できます。

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

ステップ 2 ユーザのデバイス ページに移動します。

ステップ 3 ボイス ダイヤルの設定を入力します。

設定	説明
ボイス ダイヤル モーションを有効にする（Enable Voice Dialing Motion）	ボイスダイヤルモーション機能では、モーションセンサーおよび接近センサーがアクティブになり、Cisco Jabber が実行されているときにユーザがデバイスを自分の耳に近づけ、Cisco Jabber のユーザ マニュアル（http://www.cisco.com/en/US/products/ps11596/products_user_guide_list.html）に説明のあるジェスチャーを行うと、ボイス ダイヤル パイロット番号が自動的にダイヤルされます。 この設定は、ユーザに対してボイス ダイヤル モーションを最初にオンにするかオフにするかを指定します。
ボイス ダイヤルの電話番号（Voice Dialing Phone Number）	ボイス ダイヤル機能のパイロット電話番号です。 この番号は、Cisco Jabber に一意ではありません。 詳細については、『Cisco Unity Connection Release 7.x』マニュアルの「Routing Calls to a Voice Directory Handler」の項を参照してください。
ボイス ダイヤルをお気に入りに追加する（Add Voice Dialing to Favorites）	ボイス ダイヤルの電話番号を、ユーザの Cisco Jabber のお気に入りリストに自動的に追加するかどうかを指定します。

ステップ 4 [保存（Save）] を選択します。

ステップ 5 Cisco Jabber を再起動します。

Unified CM での Visual Voicemail のセットアップ

はじめる前に

（注） ユーザが Cisco Mobile アプリケーション（Cisco Unified Mobile Communicator 7.1）を Cisco Unified Mobility Advantage と連動して実行する場合は、Cisco Jabber でボイスメールの設定をしないでください。 ユーザが最良の使用環境を得るためには、もう一方の Cisco Mobile アプリケーションのユーザが Cisco Jabber ではなく、Cisco Mobile アプリケーションを使用してボイスメールにアクセスすることを推奨します。

- IMAP が有効になっていることを確認します。
  『*System Administration Guide for Cisco Unity Connection*』の「Configuring IMAP Settings」を参照してください。このマニュアルは、http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html から入手できます。

- この手順で表に表示されている設定値を収集します。
- この項の設定値に疑問がある場合は、ボイスメール管理者に問い合わせてください。

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

ステップ 2 ユーザのデバイス ページに移動します。

ステップ 3 [プロダクト固有の設定（Product Specific Configuration Layout）] セクションに、ボイスメールの設定を入力します。

設定	説明
ボイスメールのユーザ名（Voicemail Username）	このユーザがボイスメールにアクセスするための一意のユーザ名。
ボイスメール サーバ（Voicemail Server）（ポートを含む）	ボイスメール サーバの、ホスト名または IP アドレスを入力します。 *Servername.YourCompany.com:portnumber* の形式を使用します。
ボイスメール メッセージ ストアのユーザ名（Voicemail Message Store Username）	ボイスメール メッセージ ストアのユーザ名を入力します。
ボイスメール メッセージ ストア（Voicemail Message Store）	ボイスメール メッセージ ストアの、ホスト名または IP アドレスを入力します。 これは、ボイスメール サーバと同一にすることができます。次の形式を使用します。 *YourVoiceMessageStoreServer.yourcompany.com:portnumber*

ステップ 4 [保存（Save）] を選択します。

ステップ 5 Cisco Jabber を再起動します。
エンドユーザによる設定の編集を許可していた場合は、クライアント上のボイスメール アカウントをいったん削除して、セットアップし直します。

ステップ 6 ボイスメッセージアカウントの有効化または確認のオプションが表示されるまで、ウィザードの手順に従います。

ステップ 7 [はい（Yes）] を選択します。

ステップ 8 ボイス メッセージのパスワードを入力します。

ステップ 9 [保存（Save）] を選択します。

ステップ 10 セットアップ ウィザードを完了します。

次の作業

この機能をテストしてください。

ディレクトリ検索設定値の指定

はじめる前に

- Active Directory の telephoneNumber 属性（別の属性を使用している場合は同等のもの）がインデックス化されていることを確認します。
- 社内ディレクトリ スキーマ内で、次の表に示すデフォルトとは異なる、またはこれらに追加のある属性を調べます。 変更されている属性は、この手順の後の方でマッピングする必要があります。

（注） ディレクトリ検索情報は、Unified CM からは使用できません。

制約事項 Active Directory では、次の条件が満たされている必要があります。

- 電話番号がフォーマットされていないこと。
- グローバル カタログが有効になっていること。
- Jabber がアクセスする必要のあるすべての Active Directory 属性を特定し、これらの属性をすべてのグローバル カタログ サーバに複製する必要があります。 そうしないと、Jabber はデフォルト ポートで属性情報にアクセスできません。

ディレクトリの値を確認するには、次の表を参照します。

- Active Directory サーバを使用している場合は、「デフォルトの Active Directory 属性」という列の値を参照してください。 属性が「デフォルトの Active Directory 属性」列の値と異なっている場合は、「異なる場合は、実際の値」というタイトルの列に実際の属性値を書き留めてください。
- Active Directory サーバ以外の LDAP サーバを使用している場合は、「他のすべての LDAP サーバのデフォルト属性」という列の値を参照してください。 属性が「他のすべての LDAP サーバのデフォルト属性」列の値と異なっている場合は、「異なる場合は、実際の値」というタイトルの列に実際の属性値を書き留めてください。

次の表の値について疑問がある場合は、ディレクトリ管理者に問い合わせてください。

Cisco Jabber for iPhone は、defaultNamingContext が定義されているかどうかを確認して、使用されているディレクトリ サーバのタイプを判定します。 defaultNamingContext が定義されている場合、アプリケーションは Active Directory が使用されていると判定します。 この値が定義されていない場合、アプリケーションはシステムが別の LDAP サーバを使用していると判定します。

（注） Active Directory またはその他の LDAP サーバに対するいくつかのデフォルト属性は、Cisco Jabber for iPhone と他の Cisco Jabber クライアントで異なります。 環境に複数の Cisco Jabber クライアント プラットフォームがある場合、各プラットフォームの LDAP フィールド マッピング用に別のテキストを入力する必要があります。

表 *7*：ディレクトリの要素および属性

要素	要素名	デフォルトの **Active Directory** 属性	他のすべての **LDAP** サーバのデフォルト属性	異なる場合は、実際の値
固有識別子（Unique identifier）	identifier	distinguishedName	distinguishedName	
表示名（Display name）	displayName	displayName	cn	
電子メールアドレス（Email address）	emailAddress	mail	mail	
名（First name）	firstName	givenName	givenName	
姓（Last name）	lastName	sn	sn	
ユーザ ID（User ID）	userid	sAMAccountName	uid	
メイン電話番号（Main phone number）	mainPhoneNumber	telephoneNumber	telephoneNumber	
自宅の電話番号（Home phone number）	homePhoneNumber	homeTelephoneNumber	homeTelephoneNumber	
自宅の電話番号（予備）（Second home phone number）	homePhoneNumber2	homeTelephoneNumber	homeTelephoneNumber	
携帯電話番号（Mobile phone number）	mobilePhoneNumber	mobile	mobile	
携帯電話番号（予備）（Second mobile phone number）	mobilePhoneNumber2	mobile	mobile	
ボイスメール直通電話番号（Direct to voicemail phone number）	voicemailPhoneNumber	voicemail	voicemail	

要素	要素名	デフォルトの **Active Directory** 属性	他のすべての **LDAP** サーバのデフォルト属性	異なる場合は、実際の値
FAX 番号（Fax number）	faxPhoneNumber	facsimileTelephoneNumber	facsimileTelephoneNumber	
その他の電話番号（Other phone number）	otherPhoneNumber	telexNumber	telexNumber	
ディレクトリ画像（Directory photo）	photo	jpegPhoto	jpegPhoto	
Jabber ID	jabberID	jabberID	jabberID	
役職（Job title）	jobTitle	title	title	
従業員番号（Employee number）	employeeNumber	employeeID	employeeNumber	
マネージャ ID（Manager ID）	manageruid	manager	manager	

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

ステップ 2 ユーザの Cisco Dual Mode のデバイス ページに移動します。

ステップ 3 [プロダクト固有の設定（Product Specific Configuration Layout）] セクションで、iPhone の国番号を入力します。
この情報は、発信者 ID を識別するのに役立ちます。

ステップ 4 LDAP ユーザ認証の設定を入力します。

- ディレクトリ サービスへのアクセスにクレデンシャルが不要の場合は、[無効（Disabled）] を選択します。
- ユーザがディレクトリ サービスにアクセスするときに資格情報の入力が必要である場合は、[有効（Enabled）] を選択します。

ステップ 5 LDAP ユーザ名およびパスワードを入力します。

- すべてのユーザが Active Directory のアクセスに使用する、単一の読み取り専用アカウントのクレデンシャルを入力します。 このクレデンシャルは、TFTP ファイルにクリア テキストで

送信されます。 ユーザは、ユーザ クレデンシャルを Cisco Jabber に入力する必要はありません。

- ディレクトリにアクセス可能なユーザ名を入力し、パスワードは空白のままにします。 各ユーザのパスワードを発行し、Cisco Jabber の設定にパスワードを入力するようユーザに伝えます。
- 認証が不要な場合は、この設定を空白のままにします。

デフォルトでは、LDAP ユーザ名は userPrincipalName（UPN）で、電子メール アドレスの形式（userid@example.com）になっていることがあります。

ステップ 6 LDAP サーバのアドレスを入力します。

a) Active Directory サーバのホスト名または IP アドレスおよびポート番号を入力します。

b) セキュア SSL 接続の場合はポート 3269、非セキュア接続の場合はポート 3268 を使用します。

`YourDirectoryServer.YourCompany.com:portnumber` という形式を使用します。 デフォルトでは、ポートまたは SSL 設定を入力しなかった場合、Cisco Jabber はポート 3269 で SSL 接続を試行します。

ステップ 7 「CN=users,DC=corp,DC=yourcompany,DC=com」の形式を使用して、LDAP 検索ベースを入力します。

デフォルトでは、このアプリケーションは、defaultNamingContext 属性の RootDSE 検索で見つかった検索ベースを使用します。 別の検索ベースを指定する必要がある場合は、ユーザ情報が格納された社内ディレクトリのルート ノードの Distinguished Name を入力します。 必要な名前を含んでいる最下位のノードを使用します。 上位のノードを使用すると大きな検索ベースが作成されるため、ディレクトリが非常に大規模な場合は、パフォーマンスが低下します。

（注） 最適な検索ベースを判断しやすくするには、Active Directory Explorer（Microsoft 社から入手可能）などのユーティリティを使用してデータ構造を表示してください。

ステップ 8 LDAP フィールド マッピングを入力します。

LDAP フィールド マッピングは、ディレクトリ内の属性のうち、ディレクトリ検索の検索対象および表示対象となる情報を保持しているものを指定します。

（注） マネージャ ID および従業員番号のエントリは、ディレクトリ検索結果の構造情報を報告するために必要です。 デフォルト マッピングは次の通りです。

- **Active Directory**：manageruid=manager; employeeNumber=employeeID。
- **Open LDAP**：サーバの場合 manageruid=manager; employeeNumber=employeeNumber。

マネージャに 25 以上の直接レポートがある場合、Cisco Jabber for iPhone には最初の 25 レポートだけが表示されます。

a) デフォルトに一致しないフィールド マッピングを入力する場合は、前述の表の情報を使用して、name=value pairs のように、各フィールドをセミコロン（;）で区切って入力します。 *name* には、「要素名」列に含まれる情報を入力します。 *value* には「異なる場合は、実際の値」列の情報を入力します。

例：
displayName=nickname;emailAddress=email

ステップ 9 LDAP 写真の場所に入力します。

詳細については、「LDAP サーバからの社内ディレクトリの画像の統合」を参照してください。

ステップ 10 [保存（Save）] を選択します。

ステップ 11 モバイル デバイスで Cisco Jabber を再起動します。
エンドユーザによる設定の編集を許可していた場合は、クライアント上の Directory アカウントをいったん削除して、セットアップし直します。

ステップ 12 社内ディレクトリ アカウント設定の有効化または確認のオプションが表示されるまで、ウィザードの手順に従います。

ステップ 13 社内ディレクトリ アカウント設定の有効化または確認オプションで、[はい（Yes）] をタップします。

ステップ 14 まだ入力されていない場合はパスワードを入力します。

ステップ 15 変更を加えなかった場合も、[保存（Save）] を選択します。

ステップ 16 ウィザードを完了します。

次の作業

この機能をテストしてください。

Cisco Jabber での社内ディレクトリの画像の設定

Cisco Jabber に社内ディレクトリの画像を統合するには、次の手順のいずれかを使用します。

- サイド URL を使用した社内ディレクトリの画像の統合, （63 ページ）
- LDAP サーバからの社内ディレクトリの画像の統合, （64 ページ）

サイド URL を使用した社内ディレクトリの画像の統合

Cisco Jabber が LDAP サーバではなく Web サーバから画像を取得できるように、LDAP 属性マップの [画像（Photo）] フィールドにパラメータ化された URL を設定できます。 URL の文字列には、ユーザの画像を一意に識別するデータの一部が含まれたクエリー値と LDAP 属性を含めてください。 ユーザ ID 属性を使用することを推奨します。 ただし、一意にユーザの画像を識別するデータをクエリー値に含めた LDAP 属性であればすべて使用できます。

はじめる前に

この置換技術が機能するのは、Cisco Jabber がクエリー結果を使用でき、クエリー結果をテンプレートに挿入して、JPG 画像を取得する有効な URL を生成できる場合に限られます。 社内で画像を搭載している Web サーバが、POST を必要とする場合（たとえば、ユーザの名前は URL にない場合）や、ユーザ名ではなく画像のクッキー名を使用する場合、この置換技術は機能しません。

手順

ステップ 1 Unified CM の管理にサインインします。

ステップ 2 [デバイス（Device）] > [電話（Phone）] に移動して、デバイス ID を検索します。

ステップ 3 COP ファイル フィールドの [プロダクト固有の設定（Product Specific Configuration Layout）] フィールドに移動します。

ステップ 4 [LDAP 画像の場所（LDAP Photo Location）] フィールドに移動して、画像が格納されている URL を入力します。
LDAP 属性を表すために、変数 %%*LDAP Attribute* %% を使用することを推奨します。

例：

- `http://mycompany.cisco.com/photo/std/%%uid%%.jpg`
- `http://mycompany.cisco.com/photo/std/%%sAMAccountName%%.jpg`

（注） 2 つ並んだパーセント記号は必須であり、置換する LDAP 属性の名前を囲むのに使用する必要があります。

Cisco Jabber は、パーセント記号を削除し、パーセント記号で囲んでいたパラメータを、ユーザの画像取得のために実行した LDAP クエリの結果に置き換えます。

例：
クエリー結果に値「johndoe」の属性「uid」が含まれている場合、
`http://mycompany.com/photos/%%uid%%.jpg` テンプレートによって、
`http://mycompany.com/photos/johndoe.jpg` という URL が作成されます。 Cisco Jabber は画像をフェッチしようとします。

次の作業

重要 社内画像を統合したら、[エンド ユーザによる設定の編集を許可する（Allow End User Configuration Editing）] の設定に応じて、デバイスを再プロビジョニングするかリセットします。詳細については、ユーザ デバイスの追加, （18 ページ）を参照してください。

LDAP サーバからの社内ディレクトリの画像の統合

次の手順に従って、社内ディレクトリの画像を LDAP サーバから Cisco Jabber に統合します。

（注） グローバル カタログを使用する場合は、Microsoft Active Directory の LDAP 写真フィールドの値「jpegphoto」をグローバル カタログに複製します。 詳細については、シスコに関連しないサードパーティ Web サイトに移動する次のリンクを参照してください。「グローバル カタログにレプリケートされる属性を変更する方法」

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

ステップ 2 [デバイス（Device）] > [電話（Phone）] に移動して、デバイス ID を検索します。

ステップ 3 COP ファイル フィールドの [プロダクト固有の設定（Product Specific Configuration Layout）] フィールドに移動します。

ステップ 4 [LDAP フィールド マッピング（LDAP Field Mappings）] に移動します。
デフォルト マッピングは、photo=jpegPhoto です。 カスタム マッピングが不要な場合は、その他の操作は不要です。

カスタム マッピングが必要な場合は、[LDAP フィールド マッピング（LDAP Field Mappings）] を変更します。 フィールド マッピングは property=ldapAttribute の形式で指定され、セミコロンで区切ります（例："userid=uid;photo=thumbnailPhoto"）。

次の作業

重要 社内画像を統合したら、[エンド ユーザによる設定の編集を許可する（Allow End User Configuration Editing）] の設定に応じて、デバイスを再プロビジョニングするかリセットします。詳細については、ユーザ デバイスの追加, （18 ページ）を参照してください。

SRST フェールオーバーの設定

Survivable Remote Site Telephony（SRST）は、Unified CM から別の Unified CM、Unified CM Express（Unified CME）、または SRST を実行しているルータにサービスを転送することを可能にします。

（注）
- コール パークとアドホック会議は SRST モードではサポートされません。
- Unified CME の SIP SRST 転送機能には、Unified CME 8.6 が必要です。

1. Unified CM の必須 SRST 情報を設定します。 http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.htmlを参照してください。 使用中の Cisco Unified Communications Manager のバージョンに該当する『*Administration Guide*』を選択します。
2. 次の方法のいずれか 1 つを使用してフェールオーバー デバイスを設定します。
   - Unified CME への SRST フェールオーバー。

     Unified CME で、次のパラメータを設定する必要があります。

     - registrar server expires max 1200 min 660
     - sip-ua

       timers connection aging 12

     詳細については、http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmead.pdf を参照してください。

     （注） SIP IP フォンと SIP SRST（no mode cme）を同時にプロビジョニングすることはできません。 「srst mode auto-provision」を使用してセットアップを行う SCCP SRST とは異なり、SIP SRST はデフォルトで有効になっています。

   - SRST のみにセットアップされたルータへの SRST フェールオーバー。 http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.htmlを参照してください。 使用中の Cisco Unified Communications Manager のバージョンに該当する『*Administration Guide*』を選択します。

     （注） この設定では、ルータはフェールオーバーのためにのみ設定され、ローカル SCCP または SIP IP フォンはプロビジョニングされません。

ユーザのログインおよびログアウトを許可するためのエクステンション モビリティのセットアップ

ユーザがデバイス上で Cisco Jabber にログインまたはログアウトできるように Cisco エクステンション モビリティ サービスをセットアップしてアクティブにします。

（注） エクステンション モビリティ機能は、Dial via Office 機能ではサポートされません。

はじめる前に

- エクステンション モビリティを使用したログイン機能は、Cisco Jabber ではデフォルトで無効になっています。 この機能を有効にするには、[サインイン（Sign In）] 機能のドロップダウン リストで [有効（Enabled）] を選択します。 エクステンション モビリティのセットアップに関する詳細情報については、http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_6_1/ccmfeat/fsem.html を参照してください。

（注） 外線番号マスクは、マスクをエクステンション モビリティのデバイス プロファイルに対しても設定していないと、エクステンション モビリティが有効でも表示されません。

- エクステンション モビリティは、[制御するプロファイル（Controlled Profiles）] フィールドに 1 つのプロファイルがリストされている場合にだけ機能します。
- エクステンションモビリティをエンタープライズ登録サービスとしてセットアップする場合は、エクステンション モビリティが有効になっている間、すべての Cisco Jabber ユーザが Cisco Jabber にログインまたはログアウトすることが必要です。
- エクステンション モビリティを使用するときは、[エンド ユーザによる設定の編集を許可する（Allow End User Configuration Editing）] で [無効（Disabled）] を選択します。 詳細については、ユーザ デバイスの追加, （18 ページ）を参照してください。
- エクステンション モビリティのセットアップが完了後、Cisco Jabber はユーザがログインしている場合にのみ機能します。

ユーザが自動的に Cisco Jabber からログアウトするためのタイマーの設定

Unified CM クラスタ内のすべてのエクステンション モビリティ ユーザのタイマーを設定するには、次の手順を使用します。 タイマーに関する詳細情報については、http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_6_1/ccmfeat/fsem.html#wp1178338 を参照してください。

（注） 自動のログアウト時にアクティブ コールがある場合、コールは中断されません。

手順

ステップ 1 Unified CM にログインします。

ステップ 2 [ナビゲーション（Navigation）] フィールドで、[Unified CM の管理（Unified CM Administration）] を選択します。

ステップ 3 [システム（System）] > [サービス パラメータ（Service Parameters）] を選択します。

ステップ 4 [サーバ（Server）] ドロップダウン リストで、アクティブな Unified CM を選択します。

ステップ 5 [サービス（Service）] ドロップダウン リストで、[Cisco Extenstion Mobility（アクティブ）（Cisco Extenstion Mobility (Active)）] サービスを選択します。

ステップ 6 [クラスタ内の最大ログイン時間を強制的に適用する（Enforce Intra-cluster Maximum Login Time）] フィールドで、[はい（True）] を選択します。

ステップ 7 [クラスタ内の最大ログイン時間（Intra-cluster Maximum Login Time）] フィールドに、ユーザが Cisco Jabber からログアウトするまでの経過時間を入力します。

ステップ 8 [保存（Save）] をクリックします。

他のアプリケーションからのCiscoJabberの相互起動（任意）

この機能により、開発者はサードパーティ製のアプリケーションから Cisco Jabber を起動することができます。URL を構築して別のアプリケーションから開くことで、アプリケーションから Cisco Jabber を起動することを可能にします。

アプリケーションから Cisco Jabber を相互起動するには、次の形式で URL を開くようにアプリケーションをセットアップします。

```
ciscotel://<phonenumber>
```

例

- `ciscotel://98255550528`
- `ciscotel://(506)555-4444`

（注） Web ページのフィールドに ciscotel 形式の URL を追加できます。 ユーザが URL をタップすると、Cisco Jabber は URL に含まれる番号を自動的にコールします。 「Notes」などの URL を開くことができるアプリケーションに、この形式で電話番号を追加することができます。

（注） どの電話番号形式をサポートするのかは、URL を開くアプリケーションによって異なります。

SIP ダイジェスト認証オプションのセットアップ

SIP ダイジェスト認証は、ユーザ デバイスを認証するための Unified CM のセキュリティ機能です。 詳細については、『*Cisco Unified Communications Manager Security Guide*』と『*Cisco Unified Communications Manager Administration Guide*』を参照してください。これらは、メンテナンス ガイド一覧から入手できます。

（注） Cisco Jabber は、Dial Via Office - Reverse 機能による SIP ダイジェスト認証機能をサポートしていません。

Cisco Jabber には、次の 3 つのオプションがあります。

- SIP ダイジェスト認証の無効化：実際の導入でこの機能を使用しない場合は、SIP ダイジェスト認証を無効にします。

  SIP ダイジェスト認証の無効化, （69 ページ）を参照してください。

- 自動パスワード認証を使用した SIP ダイジェスト認証の有効化
  - パスワードはクリア テキストで保存および送信されます。
  - ユーザがこのパスワードを手動で入力する必要はありません。
  - これにより、入力ミスによって Cisco Jabber が Unified CM に登録されなくなる可能性が減少します。

  自動パスワード認証を使用した SIP ダイジェスト認証の有効化, （70 ページ）を参照してください。

- 手動パスワード認証を使用した SIP ダイジェスト認証の有効化
  - パスワードが暗号化されます。
  - ユーザはこのパスワードを手動で入力する必要があります。

  手動パスワード認証を使用した SIP ダイジェスト認証の有効化, （71 ページ）を参照してください。

SIP ダイジェスト認証の無効化

Unified CM の各デバイス ページで次の手順を実行します。

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

ステップ 2 デバイスのページにナビゲートします。

ステップ 3 [デバイス セキュリティ プロファイル（Device Security Profile）] ドロップダウン リストで、[Cisco Dual Mode for iPhone - 標準 SIP 非セキュア プロファイル（Cisco Dual Mode for iPhone - Standard SIP Non-secure profile）] を選択します。

ステップ 4 [プロダクト固有の設定（Product Specific Configuration Layout）] セクションで認証の詳細を完成させます。

a) [SIP ダイジェスト認証の有効化（Enable SIP Digest Authentication）] ドロップダウン リストで [無効（Disabled）] を選択します。

b) [SIP ダイジェスト ユーザ名（SIP Digest Username）] は空白のままにしておきます。

ステップ 5 エンド ユーザ設定の編集が有効な場合、電話サービス アカウントをリセットします。

a) デバイスの電話サービス アカウントを削除します。

b) アカウントをもう一度セットアップします。

ステップ 6 Cisco Jabber を再起動します。

自動パスワード認証を使用した SIP ダイジェスト認証の有効化

手順

ステップ 1 次のようにして、[システム（System）] > [セキュリティ プロファイル（Security Profile）] > [電話セキュリティ プロファイル（Phone Security Profile）] の下で、Cisco Dual Mode for iPhone の新しい電話セキュリティ プロファイルを作成します。

a) [ダイジェスト認証を有効化（Enable digest authentication）] を選択します。

b) [設定ファイル内のダイジェスト信用証明書を除外（Exclude digest credentials in configuration file）] を選択解除します。

ステップ 2 [エンド ユーザ（End User）] ページの [ユーザ情報（User Information）] セクションで、次のタスクを実行します。

a) [ユーザ ID（User ID）] フィールドにユーザ ID が入力されていることを確認します。

b) [ダイジェスト信用証明書（Digest Credentials）] フィールドに、ダイジェスト信用証明書を入力します。

c) [ダイジェスト信用証明書の確認（Confirm Digest Credentials）] フィールドに、ダイジェスト信用証明書を再入力します。

ステップ 3 [Cisco Dual Mode for iPhone デバイス（Cisco Dual Mode for iPhone device）] ページごとに、[プロファイル固有情報（Profile Specific Information）] セクションでプロファイル情報を完成させます。

a) [デバイス セキュリティ プロファイル（Device Security Profile）] リストで、作成した電話セキュリティ プロファイルを選択します。
b) [ダイジェスト ユーザ（Digest User）] リストで、ダイジェスト ユーザを選択します。

ステップ 4 同じデバイス ページの [プロダクト固有の設定（Product Specific Configuration Layout）] セクションで、認証の詳細を完成させます。

a) [SIP ダイジェスト認証の有効化（Enable SIP Digest Authentication）] ドロップダウン リストで [無効（Disabled）] を選択します。
b) [SIP ダイジェスト ユーザ名（SIP Digest Username）] は空白のままにしておきます。

ステップ 5 エンド ユーザ設定の編集が有効な場合、電話サービス アカウントをリセットします。

a) デバイスの電話サービス アカウントを削除します。
b) アカウントをもう一度セットアップします。

ステップ 6 Cisco Jabber を再起動します。

手動パスワード認証を使用した SIP ダイジェスト認証の有効化

手順

ステップ 1 次のようにして、[システム（System）] > [セキュリティ プロファイル（Security Profile）] > [電話セキュリティ プロファイル（Phone Security Profile）] の下で、Cisco Dual Mode for iPhone の新しいプロファイルを作成します。

a) [ダイジェスト認証を有効化（Enable digest authentication）] を選択します。
b) [設定ファイル内のダイジェスト信用証明書を除外（Exclude digest credentials in configuration file）] を選択します。

ステップ 2 [エンド ユーザ（End User）] ページの [ユーザ情報（User Information）] セクションで、次のタスクを実行します。

a) [ユーザ ID（User ID）] フィールドにユーザ ID が入力されていることを確認します。
b) [ダイジェスト信用証明書（Digest Credentials）] フィールドに、ダイジェスト信用証明書を入力します。
c) [ダイジェスト信用証明書の確認（Confirm Digest Credentials）] フィールドに、ダイジェスト信用証明書を再入力します。

このパスワードを書き留めてください。 後でこのパスワードをユーザに提供します。

ステップ 3 [Cisco Dual Mode for iPhone デバイス（Cisco Dual Mode for iPhone device）] ページごとに、[プロトコル固有情報（Protocol Specific Information）] セクションで新しいプロファイル情報を入力します。

a) [デバイス セキュリティ プロファイル（Device Security Profile）] リストで、作成した電話セキュリティ プロファイルを選択します。

b) [ダイジェスト ユーザ（Digest User）] リストで、ダイジェスト ユーザを選択します。

ステップ 4 同じデバイス ページの [プロダクト固有の設定（Product Specific Configuration Layout）] セクションで、認証の詳細を完成させます。

a) [SIP ダイジェスト認証の有効化（Enable SIP Digest Authentication）] リストで [有効（Enabled）] を選択します。

b) [SIP ダイジェスト ユーザ名（SIP Digest Username）] に、作成したダイジェスト ユーザを入力します。

ステップ 5 Cisco Jabber を再起動して、セットアップ ウィザードの手順をもう一度実行します。

ステップ 6 [電話サービス（Phone Services）] 設定の確認のオプションで、[SIP ダイジェスト認証（SIP Digest Authentication）] のパスワード設定をタップし、記録しておいたパスワードを入力します。
このパスワードの大文字と小文字は区別されます。

ステップ 7 [電話サービスの設定（Phone Services Settings）] 画面で、SIP ダイジェスト認証の資格情報を入力します。
このパスワードの大文字と小文字は区別されます。

ステップ 8 エンド ユーザ設定の編集が有効な場合、電話サービス アカウントをリセットします。

a) デバイスの電話サービス アカウントを削除します。

b) アカウントをもう一度セットアップします。

Cisco AnyConnect の設定

Cisco AnyConnect Secure Mobility Client は、Cisco Jabber が Wi-Fi またはモバイル データ ネットワークを使用して、リモート ロケーションから企業ネットワークに安全に接続できるようにする VPN アプリケーションです。

（注） 企業外の Wi-Fi ネットワークまたはモバイル データ ネットワークでの音声品質は保証されません。

Cisco AnyConnect Secure Mobility Client をサポートするには、次の手順を使用してシステムを設定する必要があります。

1 Cisco Adaptive Security Appliance（ASA）をインストールして設定します。

- サポートされる Cisco Adaptive Security Appliance モデルおよびその他の要件については、Release Notes を参照してください。
- ASA のインストールおよび設定の方法については、コンフィギュレーションおよびインストレーション ガイドの一覧を参照してください。

2 Cisco AnyConnect をサポートするように ASA を設定します。

次の手順を順序どおりに実行してください。

a アプリケーション プロファイルのプロビジョニング, （73 ページ）

b VPN 接続の自動化, （75 ページ）

c 証明書ベースの認証の設定, （76 ページ）

d ASA セッション パラメータの設定, （78 ページ）

e トンネル ポリシーの設定, （80 ページ）

3 AnyConnect 用に Unified CM を設定します。 Unified CM での自動 VPN アクセスの設定, （81 ページ）を参照してください。

（注） Cisco Jabber for iPhone と Cisco AnyConnect Secure Mobility Client の組み合わせがサポートされます。 その他の VPN クライアントは公式にはサポートされませんが、その他の VPN クライアントでも Cisco Jabber for iPhone を使用できる可能性があります。 別の VPN クライアントを使用する場合は、次のように VPN を設定します。

1. 該当するサードパーティのマニュアルを使用して、VPN クライアントをインストールし、設定します。
2. Unified CM での自動 VPN アクセスの設定, （81 ページ）の手順を使用して、オンデマンド VPN を設定します。

アプリケーション プロファイルのプロビジョニング

ユーザが Cisco AnyConnect クライアントをデバイスにダウンロードした後、ASA はコンフィギュレーション プロファイルをアプリケーションにプロビジョニングする必要があります。

Cisco AnyConnect 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）、およびオンデマンド 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 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。

- ASA での VPN プロファイルのプロビジョニング
- Apple コンフィギュレーション プロファイルと iPCU を使用した iOS デバイスのプロビジョニング
- Apple コンフィギュレーション プロファイルと MDM を使用した iOS デバイスのプロビジョニング

ASA での VPN プロファイルのプロビジョニング

ASA Device Manager（ASDM）のプロファイル エディタを使用して、Cisco AnyConnect クライアントの VPN プロファイルを定義することを推奨します。

この方法を使用すると、クライアントが初めて VPN 接続を確立した後で、VPN プロファイルが自動的に Cisco AnyConnect 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。

VPN プロファイルを定義するには、次の手順に従います。

手順

ASDM で、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）] の順に選択します。 詳細については、ご使用のリリースの『*Cisco AnyConnect Secure Mobility Client Administrator Guide*』の「Deploying the AnyConnect Secure Mobility Client」の章にある「Creating and Editing an AnyConnect Client Profile Using the Integrated AnyConnect Profile Editor」の手順を参照してください。 マニュアルのバージョン一覧は http://www.cisco.com/en/US/products/ps10884 から参照できます。

Apple コンフィギュレーション プロファイルと iPCU を使用した iOS デバイスのプロビジョニング

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するには、次の手順を実行します。 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。

手順

ステップ 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。

ステップ 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。

ステップ 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。

Apple コンフィギュレーション プロファイルと MDM を使用した iOS デバイスのプロビジョニング

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するには、次の手順を実行します。 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。

手順

ステップ 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。

ステップ 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。

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。

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。

- [常に接続する（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。

- [必要に応じて接続する（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 接続の開始を試行しません。

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。

ステップ 3 Unified CM で、Cisco Jabber デバイス設定の [オンデマンド VPN URL（On-Demand VPN URL）] フィールドを設定します。
手順の詳細については、Unified CM での自動 VPN アクセスの設定, （81 ページ）を参照してください。

Cisco Jabber が開くと、URL への DNS クエリを開始します（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。

証明書ベースの認証の設定

Cisco AnyConnect クライアントは、Microsoft Active Directory/LDAP パスワード、RADIUS ベースのワンタイム トークン、および証明書を含めて、多くの認証方式をサポートしています。 これらの方式のうち、クライアント証明書認証は最もシームレスな使用環境を提供します。

ASA の証明書ベースの認証用設定

ASA は、Cisco IOS CA、Microsoft Windows 2003、Windows 2008 R2、Entrust、VeriSign、RSA Keon など、さまざまな標準認証局（CA）サーバが発行した証明書をサポートします。

次の手順で、証明書ベースの認証用に ASA を設定するステップの概要を示します。 詳細については、『*Cisco ASA 5500 Series Configuration Guide using ASDM, 6.4 and 6.6*』の「Configuring Access Control」の章の「Configuring Digital Certificates」の項を参照してください。 このマニュアルは、http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html から参照できます。

手順

ステップ 1 ルート証明書を CA から ASA にインポートします。
ステップ 2 ASA の ID 証明書を生成します。
ステップ 3 SSL 認証用の ASA の ID 証明書を使用します。
ステップ 4 証明書失効リスト（CRL）または Online Certificate Status Protocol（OCSP）を設定します。
ステップ 5 認証にクライアント証明書を要求するように、ASA を設定します。

クライアント証明書の配布

次のいずれかの方法に従って、Cisco Jabber for iPhone デバイスに証明書を発行できます。

- SCEP
- Mobileconfig ファイル

SCEP を使用したクライアント証明書の配布

ASA は証明書の配布を簡略化する Simple Certificate Enrollment Protocol（SCEP）をサポートします。

ASA は SCEP を使用して、クライアント認証に使用される証明書を安全に発行および更新できます。 次に、この手順の全体的な概要を示します。

1. リモート ユーザが Cisco AnyConnect を初めて開くときに、アプリケーションは Active Directory 資格情報またはワンタイム トークン パスワードのいずれかを使用してユーザを認証します。
2. クライアントが VPN を確立したら、ASA は SCEP 要求を含むクライアント プロファイルを提供します。
3. Cisco AnyConnect クライアントから証明書要求が送信されると、認証局（CA）は自動的にその要求を受け入れるか拒否します。
4. CA が要求を受け入れると、次のことが起こります。
   a. 証明書はデバイス上のネイティブ証明書ストアにインストールされます。
   b. Cisco AnyConnect は認証に証明書を使用します。その後、VPN 接続を構築するときには、ユーザにパスワードを求めるプロンプトは出されなくなります。

手順

SCEP モジュールを Windows 2008 サーバにインストールして ASA をセットアップする方法についての詳細は、「ASA 8.X: AnyConnect SCEP Enrollment Configuration Example」を参照してください。

Mobileconfig ファイルを使用したクライアント証明書の配布

証明書を含む iPhone モバイル コンフィギュレーション ファイルを作成するには、次の手順を実行します。 このファイルを使用して、証明書をユーザに配布できます。

手順

ステップ 1 iPCU ソフトウェアを使用して mobileconfig ファイルを作成し、certificate (.pfx) ファイルを組み込みます。

ステップ 2 mobileconfig ファイルをユーザに転送します。
ユーザがこのファイルを開くと、ファイルによって証明書がデバイスにインストールされます。

ステップ 3 Cisco ISE のネイティブ サプリカント プロビジョニング プロセスを使用して、ユーザ証明書を配布します。

ステップ 4 Enterprise MDM ソフトウェアを使用して、登録済みデバイスに証明書をプロビジョニングおよびパブリッシュします。

ASA セッション パラメータの設定

VPN 接続を確立した後に ASA 上でセッション パラメータを設定して、Cisco AnyConnect Secure Mobility Client および Cisco Jabber のユーザ エクスペリエンスを定義できます。

ASA セッション パラメータには、次のものがあります。

- [DTLS]：DTLS は、UDP を使用して遅延の少ないデータ パスを提供する標準ベースの SSL プロトコルです。 DTLS により、Cisco AnyConnect クライアントは、SSL トンネルおよび DTLS トンネルの 2 つのトンネルを同時に使用して、SSL VPN 接続を確立することができます。 DTLS を使用すると、遅延と帯域幅の問題を防止して、パケットの遅延の影響を受けやすい Cisco Jabber などのリアルタイム アプリケーションのパフォーマンスを向上させることができます。 DTLS が設定済みで UDP が中断された場合、リモート ユーザの接続は自動的に DTLS から TLS にフォールバックします。 DTLS はデフォルトで有効になっています。
- [セッションの永続性（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。 たとえば、ユーザがある Wi-Fi ネットワークから別の Wi-Fi またはモバイル データ ネットワークにローミングすると、Cisco AnyConnect クライアントは自動的に VPN セッションを再開します。 また、デバイスがスタンバイ、スリープ、またはハイバネーション モードから再開した後に、VPN セッションを再確立するように Cisco AnyConnect を設定できます。
- [アイドル タイムアウト（Idle Timeout）]：アイドル タイムアウト（vpn-idle-timeout）は、通信アクティビティがない場合に ASA が VPN 接続を終了するまでの時間です。 アイドル タイムアウトの時間を非常に短くすると、VPN 接続が頻繁に中断され、コールごとに VPN を再確立する必要があります。 一方、アイドル タイムアウトの値が大きすぎると、ASA 上の

同時セッションの数が過剰になります。 [アイドル タイムアウト（Idle Timeout）] 値は、グループ ポリシーによって設定できます。

- [デッドピア検出（DPD）（Dead-Peer Detection (DPD)）]：このパラメータにより、ASA ゲートウェイまたは Cisco AnyConnect クライアントは、ピアが応答しておらず、接続に失敗した状態を素早く検出できます。 シスコでは次を推奨しています。
  - サーバ側の DPD を無効にして、デバイスが確実にスリープできるようにします（このパラメータを有効にすると、デバイスがスリープしなくなります）。
  - クライアント側の DPD を有効にします。これにより、クライアントは、ネットワーク接続が不足した場合にトンネルを終了する時期を決定できるようになります。

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。
ASA セッション パラメータの設定方法については、『*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」の項を参照してください。 このマニュアルは、http://www.cisco.com/en/US/products/ps10884/prod_maintenance_guides_list.html から参照できます。

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。

セッションの持続性の設定方法の詳細については、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」の項を参照してください。 ご使用のリリースのマニュアルは、http://www.cisco.com/en/US/products/ps10884/products_installation_and_configuration_guides_list.html から参照できます。

ステップ 3 アイドル タイムアウト値を設定します。

a) 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。

アイドル タイムアウト値を設定する方法についての詳細は、ご使用のリリースの『*Cisco ASA 5580 Adaptive Security Appliance Command Reference*』の「vpn-idle-timeout」の項を参照してください。 ご使用のリリースのマニュアルは、http://www.cisco.com/en/US/products/ps6120/prod_command_reference_list.html から参照できます。

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。

DPD を設定する方法についての詳細は、『*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」のサブセクションを参照してください。 このマニュアルは、http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html から参照できます。

トンネル ポリシーの設定

VPN トンネルでトラフィックを転送する方法を指定するトンネル ポリシーを設定するには、次の手順に従います。

トンネル ポリシーを設定するには、まず使用するトンネル ポリシーのタイプを決定する必要があります。 トンネル ポリシーには、次のものがあります。

Full-Tunnel ポリシー

これはデフォルトのトンネル ポリシーです。 Cisco Jabber および Cisco AnyConnect の展開で最もセキュアなオプションが必要な場合は、このポリシーを使用します。 Full-Tunnel の場合、デバイス上のすべてのアプリケーションからのすべてのトラフィックは、VPN トンネルを介して ASA ゲートウェイに送信されます。 オプションで、ローカル LAN アクセス機能を有効にして、ローカル印刷とローカル ネットワーク ドライブ マッピングを有効にすることができます。

Split-Tunnel ポリシー

電話機から企業ネットワークに Cisco Jabber 固有のトラフィックだけを転送する場合は、このポリシーを使用します。 このポリシーは、宛先サブネットに基づいてトラフィックを転送します。 VPN を介して（暗号化して）送信されるトラフィックと、（暗号化せずに）平文で送信されるトラフィックを指定できます。

関連付けられている機能である Split-DNS は、VPN トンネルを介して解決される DNS トラフィックと、エンドポイント DNS リゾルバによって処理される DNS トラフィックを定義します。

ネットワーク ACL での Split-Include ポリシー

このポリシーは、次の場合に使用します。

- 帯域幅の問題のため、VPN トンネルを介して送信されるトラフィックを制限する場合。
- VPN セッションを Cisco Jabber アプリケーションに制限する場合。

ASA で Split-Include ポリシーを使用すると、トラフィックの宛先 IP アドレスに基づいて VPN トンネル内で送信されるトラフィックを指定できます。

Cisco Unified CM クラスタ、ディレクトリ サーバ、および TFTP サーバの IP サブネットを含める必要があります。 Cisco Jabber は、企業 Wi-Fi ネットワーク上の IP Phone またはコンピュータ電話とのピアツーピア メディア接続を必要とします。 そのため、シスコは、Split-Include ポリシーに企業ネットワーク IP アドレス範囲を含めるよう推奨しています。この設定は、一部の展開に対して適切ではない可能性があります（たとえば、買収やその他の事情のため、会社の IP 空間が連続していない場合）。

このポリシーはすべての内部トラフィックをトンネルに転送しますが、Facebook や YouTube など、クラウドベースのサービスがトンネルに入るのを防止できます。

（注） Split-Include ポリシーで指定したアドレス範囲に転送されるすべてのアプリケーション データがトンネル化されるため、Cisco Jabber 以外のアプリケーションもトンネルにアクセスできます。他のアプリケーションが企業 Wi-Fi ネットワークを使用できないようにするには、VPN フィルタ（ネットワーク ACL）を適用して、使用可能なポートをさらに制限します。

Split-Exclude ポリシー

Split-Include ポリシーで必要なサブネット全体を定義するのが現実的でない場合は、このポリシーを使用します。 Split-Exclude ポリシーを使用すると、VPN トンネルから既知のトラフィックを除外できます。 たとえば、帯域幅に問題がある場合は、NetFlix、Hulu、YouTube などのサービスの宛先サブネットを Split-Exclude リストに追加できます。

使用するトンネル ポリシーのタイプを指定したら、『*Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6*』の「Configuring Tunnel Groups, Group Policies, and Users」の章の「Configuring Split-Tunneling Attributes」の項を参照してください。 このマニュアルは、http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html から参照できます。

Unified CM での自動 VPN アクセスの設定

次の要件を満たしている場合、Cisco Jabber は VPN を自動的に起動できます。

- ユーザが Cisco Jabber を起動したときに、企業ネットワークを直接使用できない。
- VPN を使用してデバイスを接続可能である。

- この項の要件が満たされ、手順がすべて完了している。

Apple.com で次の情報も参照してください。

- 『*iPhone OS Enterprise Deployment Guide*』に記載された情報。このマニュアルは、http://support.apple.com/manuals/#iphone から入手できます
- iPhone Configuration Utility。http://www.apple.com/downloads/macosx/apple/application_updates/iphoneconfigurationutility21forwindows.html から入手できます
- iPhone でサポートされるプロトコルおよび認証方法のリスト。http://support.apple.com/kb/HT1288 にあります
- 『*iPhone User Guide*』に記載された VPN に接続するための iPhone の設定方法。このマニュアルは、http://www.apple.com/support/country/?dest=manuals から入手できます
- 次の Web サイトで入手可能な一般情報。http://www.apple.com/support/iphone/enterprise/

はじめる前に

- iPhone 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。
- iOS 5.1.1 を実行する iPhone に対しては、Apple iOS 用の Cisco AnyConnect Secure Mobility Client を使用することを推奨します。 Cisco AnyConnect VPN ソリューションの要件は、次のとおりです。
  - Cisco Adaptive Security Appliance リリース 8.4 以降
  - Cisco AnyConnect Secure Mobility Client リリース 2.5 以降

    Cisco AnyConnect の設定の詳細については、http://www.cisco.com/en/US/products/ps8411/prod_maintenance_guides_list.html を参照してください。

（注） Cisco Jabber では、VPN クライアントのリリースが一部サポートされていません。 次の Web サイトにある Cisco Jabber のリリース ノートでシステム要件を確認してください。http://www.cisco.com/en/US/products/ps11596/prod_release_notes_list.html

- オンデマンドで VPN を起動するために設定された URL を確認します。 Cisco AnyConnect クライアントで URL を入力します。 このドメインで DNS クエリが失敗した場合は、Cisco Jabber がオンデマンドで VPN をトリガします。
  次のいずれかの方法を使用します。
  - Unified CM を（IP アドレスではなく）ドメイン名経由でアクセスするように設定します。また、ドメイン名がファイアウォールの外では解決できないようにします。
    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 [必要に応じて接続する（Connect If Needed）] リストに追加します。

- ドメイン名を使用して Unified CM にアクセスできない場合や、ファイアウォールの外からのドメイン名に対する DNS ルックアップを失敗させることができない場合は、次の手順のパラメータを存在しないドメイン（つまり、ユーザがファイアウォール内または外にいる場合に、DNS クエリを失敗させる原因となるドメイン）に設定します。 次に、AnyConnect クライアント接続の Connect on Demand ドメイン リストで、そのドメインを [常に接続する（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。 プロトコルやパスを含まないようにしてください。 詳細については、下記の例を参照してください。

表 *8*：正しい *URL* の形式

適切な例	不適切な例
“cm8ondemand.company.com”	“https://cm8ondemand.company.com/vpn”

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。

ステップ 2 ユーザの [Cisco Dual Mode for iPhone] デバイス ページに移動します。

ステップ 3 [プロダクト固有の設定（Product Specific Configuration Layout）] セクションまでスクロールします。

ステップ 4 [オンデマンド VPN URL（On-Demand VPN URL）] フィールドに、この手順の前提条件として Cisco AnyConnect で識別および使用した URL を入力します。

（注） 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。

次の作業

- エンド ユーザによる設定の編集を許可していた場合は、クライアント上の電話サービス アカウントをいったん削除して、セットアップし直します。
  これが必要なければ、クライアントを再起動します。
- この機能をテストしてください。
  - この URL を iPhone の Safari 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、iPhone が企業ネットワークに接続され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。 iPhone 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していないか（たとえば、電子メールとカレンダー操作のトラフィックだけが許可されるように、管理者がシステムを設定している場合など）IT 部門に確認します。

- Cisco Jabber が、企業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。

第 5 章

トラブルシューティング

次のリストでは、Cisco Jabber をトラブルシューティングする手順を示します。

- 管理者の援助なしにユーザが自分で実行できる解決法、およびアプリケーションの動作に関するヒントとテクニックについては、次の Web サイトで入手可能なユーザ *FAQ* を参照してください。
  http://www.cisco.com/en/US/products/ps11596/products_user_guide_list.html
- Release Notes も参照してください。
- モバイルデバイスから直接、各企業内サーバへの接続のステータスを確認します。
- この製品に固有ではない機能について（たとえば、会議、通話転送など）
  - 既存の設定済みデスクフォンでその機能をテストします。正常に動作するようなら、動作するデバイス構成を Cisco Jabber のデバイス構成と比較します。
  - Unified CM のマニュアルで、トラブルシューティングのヒントを確認します。Troubleshoot and Alerts マニュアルリストを参照してください。

- 正しい IP アドレス、ポート、パス、ユーザ名、およびパスワードを入力していることを確認します。IP アドレスではなくホスト名を入力していた場合は、代わりに IP アドレスを入力します。
- ユーザに発生した問題が解決できず、シスコのサポート担当者に問い合わせる必要がある場合は、ユーザに、その問題を取り込んだクライアントログファイルを送信してもらってください。クライアントからのログの取得については、次のトピックを参照してください。

- 接続ステータスの確認，86 ページ
- Cisco Jabber からのログの取得，86 ページ
- Cisco AnyConnect からのログの取得，90 ページ
- トラブルシューティングのヒント，91 ページ

接続ステータスの確認

ユーザは、自分のモバイルデバイスを使用して自分の接続ステータスを確認できます。

手順

ステップ 1 Cisco Jabber アイコンをタップしてアプリケーションを開きます。

ステップ 2 [設定（Settings）] > [トラブルシューティング（Troubleshooting）] > [接続ステータス（ConnectionStatus）] をタップします。

接続ステータスが表示されます。

接続されている状態（Connected）
機能は正しく設定され、接続されています。

接続中（Connecting）
Feature is currently making a connection attempt.

切断（Disconnected）
機能は設定されていますが、現在接続されていません。ユーザが Wi-Fi に正しく接続していないか、サーバが停止している可能性があります。

エラー（Error）
機能は現在設定されていないか、接続されていません。ユーザが誤ったパスワードを入力している可能性があります。

不明（Unknown）
機能の状態は不明です。この問題を修復するには、Unified CM でのアカウント設定を確認します。

Cisco Jabber からのログの取得

ユーザに、この手順に従って Cisco Jabber からログを送信してもらいます。

手順

ステップ 1 モバイルデバイスから Cisco Jabber を起動します。

ステップ 2 [設定（Settings）] > [トラブルシューティング（Troubleshooting）] をタップします。

ステップ 3 [詳細ログ（Detailed Logging）] をオンに設定します。

ステップ 4 問題の再現を試み、詳細をログに取り込みます。

ステップ 5 [設定（Settings）] > [トラブルシューティング（Troubleshooting）] > [問題レポートツール（ProblemReporting）] をタップします。
Cisco Jabber を登録できない場合は、代わりに [バージョン情報（About）] > [トラブルシューティング（Troubleshooting）] > [問題レポートツール（Problem Reporting）] をタップします。

ステップ 6　含めるファイルを選択します。
含めるファイルがわからない場合は、すべてのファイルを含めてください。

ステップ 7　[問題レポートをE メールで送信（Email Problem Report）] をタップします。

ステップ 8 自分自身など、受信者の電子メールアドレスを入力します。

（記載例）mypc-email

ステップ 9 電子メールメッセージの本文に問題の説明を入力します。

（記載例）サインインしたときにエラーが表示される。

ステップ 10 [送信（Send）] をタップします。

次の作業

不要になった場合は、[詳細ログ（Detailed Logging）] をオフにします。

Cisco AnyConnect からのログの取得

ユーザにこの手順に従って Cisco AnyConnect Secure Mobility Client からログを送信してもらいます。

手順

ステップ 1 Cisco AnyConnect のホーム画面から、[メニュー（Menu）] > [診断（Diagnostics）] の順にタップします。

ステップ 2 [ロギングおよびシステム情報（Logging and System Information）] をタップします。

ステップ 3 [ログの送信（Send Logs）] をタップします。

トラブルシューティングのヒント

セットアップの問題

Unified CM で Cisco Jabber デバイスを作成できない

問題　ユーザのデバイスタイプをオプションとして使用できない。

対処　デバイス COP ファイルをアップロードし、Unified CM を再起動したことを確認してください。デバイス用の Cisco Options Package ファイルのインストール，（5 ページ）を参照してください。

Cisco Jabber の登録が失敗する

問題　Cisco Jabber 登録が失敗またはタイムアウトする。

対処　次のリストに、登録が失敗またはタイムアウトするという状況を引き起す可能性がある、さまざまな原因と解決法を示します。

- ユーザに http://www.cisco.com/en/US/products/ps11596/products_user_guide_list.html にあるユーザ向けの FAQ でトラブルシューティングのヒントを確認してもらいます。
- モバイルデバイスが Unified CM に到達できることを確認します。モバイルデバイスのブラウザを使用して [Unified CM の管理（Unified CM Administration）] ポータルに接続します。
- 登録がエラー 503 で拒否された場合は、Unified CM の Cisco Dual Mode for iPhone のデバイスページにアクセスし、[リセット（Reset）] を選択してからもう一度実行してみます。
- TFTP サーバのアドレスとして使用している Unified CM サーバのホスト名を DNS サーバが解決できることを確認します。
- Cisco Jabber の TFTP サーバアドレスの設定に、Unified CM サーバのホスト名ではなく IP アドレスを入力します。
- 「検証がタイムアウトになりました（Verification Timed Out）」というエラーメッセージで登録が失敗する場合は、デバイス COP ファイルをインストールした後にクラスタ内の一部の Unified CM サーバを再起動していないことを示します。デバイス COP ファイルのインストール後に、すべての Unified CM サーバを再起動します。
- 導入に対応できるだけの十分なライセンスを持っていることを確認します。
- そのユーザのデバイスページで [Cisco Unified Mobile Communicator の有効化（Enable CiscoUnified Mobile Communicator）] チェックボックスがオンになっていることを確認します。詳細については、各デバイスに対する Dial Via Office の設定，（49 ページ）を参照してください。
- VPN を介した接続を行おうとしている場合：
  - デバイスが、Cisco Jabber とは独立して内部リソースに到達できることを確認します。イントラネットの Web ページ、またはファイアウォールの背後にあるその他のリソースにアクセスしてみます。

- デバイスが、Cisco Jabber とは独立して内部リソースに到達できることを確認します。イントラネットの Web ページ、またはファイアウォールの背後にあるその他のリソースにアクセスしてみます。
- デバイスが VPN を介して接続できない場合は、VPN 製品のプロバイダーにお問い合わせください。

- SIP ダイジェスト認証を有効にした場合は、クレデンシャルを正しく入力したことを確認します。

関連トピック

デバイス用の Cisco Options Package ファイルのインストール，（5 ページ）

Cisco Jabber が Unified CM に接続できない

次の問題は、Cisco Jabber が、Cisco Unified Mobility Advantage サーバと連携して実行される CiscoUnified Mobile Communicator クライアントと iPhone 上で共存する導入で発生する場合があります。

問題　モビリティ ID に関連付けられたデバイスプールの変更後、Cisco Jabber が Cisco Unified CM に接続できない。

対処　対処両方のクライアントアプリケーションを終了し、この Cisco Jabber アプリケーションを起動する前に、Cisco Unified Mobility Advantage サーバとともに動作するクライアントアプリケーションを再起動するようにユーザに依頼します。

ディレクトリサーバのハンドシェイクエラー

問題　クライアントがディレクトリサーバに接続しようとすると、SSL ハンドシェイクエラーで接続が失敗する。

対処　Unified CM のデバイスページで [LDAP SSL の有効化（Enable LDAP SSL）] の設定を変更し、アプリケーションを再起動します。

クライアントでのエンドユーザによる設定の編集を許可していた場合は、Cisco Jabber 内のディレクトリアカウントをいったん削除して、セットアップし直します。

デバイスページに加えた変更が反映されない

問題　Unified CM の Cisco Dual Mode for iPhone デバイスの設定ページにある [プロダクト固有の設定（Product Specific Configuration Layout）] セクションの変更がクライアントに反映されない。

次のいずれかを試してください。

- このマニュアルですでに説明した、[Cisco Dual Mode for iPhone] デバイスページの [エンドユーザによる設定の編集を許可する（Allow End User Configuration Editing）] 設定での設定変更に関する重要情報を参照してください。
- エンドユーザによる設定の編集を許可していた場合は、クライアント上の関連するアカウントをいったん削除して、セットアップし直します。

関連トピック

ユーザデバイスの追加，（18 ページ）

ダイヤルルールに加えた変更が反映されない

問題　Unified CM のアプリケーションダイヤルルールまたはディレクトリルックアップルールに加えた変更が反映されない。

対処　Unified CM Release 8.5 以前を使用する場合、Cisco Jabber で変更を使用できるようにするためにダイヤルルール COP ファイルを再実行し、TFTP サービスを再起動します。更新されたルールは、ユーザがアプリケーションを次回再起動したときに、Cisco Jabber が使用できるようになります。Cisco Jabber でのダイヤルルールの使用，（8 ページ）を参照してください。

デバイスアイコンが見つからない

問題　[Unified CM の管理（Unified CM Administration）] ページにデバイスアイコンが表示されない。

対処　次のことを試してください。

1. Tomcat サービスを再起動します。
2. ブラウザにデバイスページを再ロードします。
3. 必要に応じて、ブラウザのキャッシュをクリアします。
4. 問題が解決しない場合は、Unified CM サーバを再起動します。

デバイスの問題

コールを完了できない

問題　システムがダイヤル可能な電話番号に接続できない。ユーザには、ネットワークビジートーンが聞こえるか、エラーメッセージが送られる。

対処　次のことを試してください。

- Unified CM Release 8.5 以前を使用し、アプリケーションダイヤルルールを変更した場合は、Cisco Jabber で変更を使用できるようにするためにダイヤルルール COP ファイルを実行し、TFTP サービスを再起動したことを確認します。
- ダイヤルルールを変更して、デバイスページの [プロダクト固有の設定（Product SpecificConfiguration Layout）] セクションでダイヤルルールの代替場所を指定した場合は、TFTP サービスを再開する前にカスタムファイルを必ず更新してください。
- デバイスページで [未登録時コール転送（Call Forward Unregistered）] を必ず設定してください。

Cisco Jabber でコールを受信できない

問題　着信通話が Cisco Jabber の実行中にいったんは着信するが、コールが切断され、モバイルコネクトを使用してネイティブの携帯電話番号に転送される。

対処　[SIP デュアルモードアラートタイマー（SIP Dual Mode Alert Timer）] 値の増加，（13 ページ）で前述したように、Unified CM で [SIP デュアルモードアラートタイマー（SIP Dual Mode Alert Timer）] を設定します。

問題　Cisco Jabber が数分間アイドル状態になると、着信インターネット通話がボイスメールに直接送信され、不在履歴として表示されます。

対処　Unified CM で、SIP デュアルモードアラートタイマーが [SIP デュアルモードアラートタイマー（SIP Dual Mode Alert Timer）] 値の増加，（13 ページ）で説明しているように設定されていることを確認します。

問題　デバイス上で PIN を所有している Cisco Jabber for iPhone のユーザは、コールがボイスメールに送られるまでコールに応答できない。

対処　[無応答時の呼び出し時間（秒）（No Answer Ring Duration (seconds)）] 設定の値を大きくして、ユーザが PIN を入力する十分な時間を確保し、コールがボイスメールに送られる前に応答できるようにします。

[無応答時の呼び出し時間（秒）（No Answer Ring Duration (seconds)）] 設定を変更するには、TCT デバイスの DN に移動し、[コール転送とコールピックアップの設定（Call Forward and Call Pickup
Settings）] セクションの下にある設定を使用してください。

（注）　[無応答時の呼び出し時間（秒）（No Answer Ring Duration (seconds)）] を増加する場合は、この設定に関連する警告について、Unified CM のオンラインヘルプで参照してください。

コールが不適切にボイスメールに送信される

問題　コールがボイスメールに直接ルーティングされる。

対処　Unified CM で、[モビリティ ID（Mobility Identity）] ページのコールタイマー値を修正してください。詳細については、モビリティ ID の追加，（37 ページ）を参照してください。

問題　Cisco Jabber が数分間アイドル状態になると、着信インターネット通話がボイスメールに直接送信され、不在履歴として表示されます。

対処　Unified CM で、SIP デュアルモードアラートタイマーが [SIP デュアルモードアラートタイマー（SIP Dual Mode Alert Timer）] 値の増加，（13 ページ）で説明しているように設定されていることを確認します。

VoIP コールをモバイルネットワークに転送できない

問題　ユーザが Cisco Jabber から携帯電話番号にアクティブな VoIP コールを送信できない。

対処　次のいずれかを試してください。

- デバイスが企業 Wi-Fi ネットワークに接続されていることを確認します。デバイスが企業 Wi-Fi ネットワークに接続されていない場合は、コールをモバイルネットワークに移動するオプションがグレー表示になり、使用できなくなります。
- Cisco Jabber を終了して内線をダイヤルすることによって、モバイルコネクトが動作することを確認します。速いビジーシグナルが聞こえる場合は、モビリティ ID の電話番号がルーティング可能なフォーマットで入力されていることを確認します。
- Unified CM で、[モビリティ ID（Mobility Identity）] ページのコールタイマーを調整してください。詳細については、Unified CM のオンラインヘルプを参照してください。[プライマリ DNS（Primary DN）] ページの [無応答時の呼び出し時間（No Answer Ring Duration）] が、[モビリティ ID（Mobility Identity）] ページの [呼び出し終了タイマー（Answer Too Late Timer）] に指定した値よりも大きいことを確認してください。

（注）　呼び出し終了タイマーは、通話が受け入れられたモバイルネットワークから Unified CM が確認応答を受信したときに起動されます。一部のモバイルネットワークは、ダイヤルされた番号が呼び出し中であるという別のアラートを、それに続いて送信することがあり、その場合は Unified CM がそのアラートを受信したときに呼び出し終了タイマーが再起動されます。

実際のモバイルデバイスでこのことをテストするには、企業の電話システム上の別の電話から携帯電話の電話番号（モバイルネットワーク上のもの）をダイヤルし、最後の桁をダイヤルしてから、コールがボイスメールに転送されるまでの経過時間を調べます。

[無応答時の呼び出し時間（No Answer Ring Duration）] を増やす場合は、この設定に関連する警告について、Unified CM のオンラインヘルプで参照してください。

- Unified CM で、[SIP デュアルモードアラートタイマー（SIP Dual Mode Alert Timer）] を 5000 ミリ秒まで増やします。問題が解決しない場合は、この値を最大 10000 ミリ秒まで、500 ミリ秒単位で大きくしていきます。[SIP デュアルモードアラートタイマー（SIP Dual ModeAlert Timer）] を大きくする方法の詳細については、[SIP デュアルモードアラートタイマー（SIP Dual Mode Alert Timer）] 値の増加，（13 ページ）を参照してください。

モバイルネットワークから Cisco Jabber にコールを転送できない

問題　ユーザがモバイルネットワークから Cisco Jabber にコールを転送できない。

対処　ユーザは、Cisco Jabber からモバイルネットワークに通話を転送できますが、それ以外の方向には転送できません。

Cisco Jabber の終了後にアクティブな VoIP コールをピックアップできない

問題　アクティブな VoIP コールの途中でユーザが Cisco Jabber を終了した場合、相手がまだ通話中であれば、Cisco Jabber を再起動したときにユーザが通話を取得できるはずです。ユーザがパーク元のコールを取得できない場合、タイムアウトが生じることがあります。

対処　Unified CM で、パークのタイムアウト時間を増やします。詳細については、http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html にある『CiscoUnified Communications Manager Features and Services Guide』の「Call Park Reversion Timer」「Park Monitoring Forward No Retrieve Timer」の項を参照してください。

音声品質の問題

問題　音声品質が悪い。

対処　ネットワーク状態が変化するため、音声品質は保証されません。社外のネットワークの問題は Cisco Jabber に固有のものではなく、本製品で制御できるものでもないため、Cisco TechnicalAssistance Center（TAC）ではこれらの問題のトラブルシューティングは行いません。

それでも、次の対応を試してください。

- ユーザが取れる対処方法については、http://www.cisco.com/en/US/products/ps11596/products_ user_guide_list.html にあるユーザ向けの FAQ を参照してください。
- 企業の Wi-Fi ネットワークを音声転送に最適化する方法に関する一般的な情報については、http://www.cisco.com/en/US/products/ps11596/prod_release_notes_list.html にある Cisco Jabber のリリースノートの「Network Requirements」の項を参照してください。

コールが切断または中断される

問題　コールが予期せず切断または中断される。

（注）　Bluetooth ヘッドセットがこの問題を悪化させている可能性があります。

対処　Bluetooth 関連の問題と社外のネットワークの問題は Cisco Jabber に固有のものではなく、本製品で制御できるものでもないため、Cisco TAC ではこれらの問題のトラブルシューティングは行いません。

- ユーザが取れる対処方法については、http://www.cisco.com/en/US/products/ps11596/products_ user_guide_list.html にあるユーザ向けの FAQ を参照してください。
- ユーザが企業の構内にいるときにこの問題が頻繁に発生する場合は、Wi-Fi ネットワークが http://www.cisco.com/en/US/products/ps11596/prod_release_notes_list.html にあるリリースノートに記載されているネットワーク要件を満たしているか確認してください。

Cisco Jabber VoIP 通話中にバッテリが通常より急速に消耗する

問題　デバイスのバッテリが、Cisco Jabber VoIP の通話中、通常の携帯電話での通話中よりも急速に消耗する。

対処　VoIP 通話は、通常の携帯電話通話よりも若干多くの電力を消費する場合があります。ユーザが取れる対処方法については、http://www.cisco.com/en/US/products/ps11596/products_user_guide_list.html にあるユーザ向けの *FAQ* を参照してください。

検索の問題

ディレクトリ検索ができない

問題　ディレクトリ検索と発信者 ID が利用できない。

Unified CM のデバイスページにディレクトリサーバの IP アドレスを入力しないと、CiscoJabber はディレクトリサービスを使用しません。この情報を入力し、保存してデバイスをリセットしてから、Cisco Jabber を再起動します。

エンドユーザによる設定の編集を許可していた場合は、Cisco Jabber の Directory アカウントをいったん削除して、追加し直します。

発信者 ID が誤りまたは不明

問題　一部の発信者が正しく認識されない。

対処　次の点に注意してください。

- Microsoft Active Directory でユーザを追加、またはユーザ情報を変更した場合、Cisco Jabber の [履歴（Recents）] または [ボイスメール（Voicemail）] にある発信者 ID の修正に最大 24 時間要することがあります。この遅延により、パフォーマンスに影響を与える同期動作が最小限に抑えられます。
- 番号が、ディレクトリルックアップルールを使用する連絡先と一致しない場合、Cisco Jabber は Unified CM から渡された電話番号を表示し、ディレクトリルックアップルールで変更されることはありません。
- ディレクトリルックアップルールに変更を加えた場合は、指定された COP ファイルを実行し、変更内容を Cisco Jabber が使用できることを確認してから、TFTP サービスを再起動してください。

関連トピック

Cisco Jabber でのダイヤルルールの使用，（8 ページ）

発信者の識別に時間がかかる

問題　発信者の連絡先情報が社内ディレクトリから取得される場合、発信者、着信番号、およびボイスメッセージを識別するためのユーザエクスペリエンスが遅くなる。

対処　Unified CM の [デバイス（Device）] ページの [プロダクト固有の設定（Product Specific Configuration Layout）] セクションで、LDAP ポート設定が正しいことを確認します。

検索が遅い

問題　検索結果が遅く返される。

対処　Unified CM の [デバイス（Device）] ページの [プロダクト固有の設定（Product Specific Configuration Layout）] セクションで、LDAP ポート設定が正しいことを確認します。

検索結果が得られない

問題　ディレクトリ検索で、既知の従業員が検索されない。

ディレクトリルックアップルールに変更を加えた場合は、指定された COP ファイルを実行し、変更内容を Cisco Jabber が使用できることを確認してから、TFTP サービスを再起動してください。

関連トピック

Cisco Jabber でのダイヤルルールの使用，（8 ページ）

ボイスメールの問題

ボイスメールサーバに接続できない

問題　ユーザがボイスメールにアクセスしようとしたら、「ユーザ名またはパスワードが間違っています（Incorrect username or password）」というエラーを連続して受け取った。

対処　何度も誤ったサインインを行ったためにユーザアカウントがロックされていないか、ボイスメールサーバを調べて確認します。

Cisco AnyConnect の問題

証明書認証の失敗

問題　Cisco AnyConnect Secure Mobility Client が、証明書を使用して ASA で認証できない。

対処　次のことを確認してください。

- 証明書が引き続き有効であり、CA サーバによって証明書が取り消されていない。
- 認証に対して、正しい VPN 接続プロファイルを設定した。
- 証明書の [キー使用（Key Usage）] 設定を [TLS Web クライアント認証（TLS Web Client Authentication）] に設定した。

SCEP 登録の障害

問題　Cisco AnyConnect Secure Mobility Client が、SCEP を使用して証明書を登録できない。

対処　次のことを確認してください。

- CA サーバは、証明書を自動的に付与するように設定されています。
- ASA と CA サーバ間のクロックスキューは、30 秒未満です。
- CA サーバの登録 URL は、VPN トンネルを介して到達可能です。
- VPN クライアントプロファイルの [自動 SCEPHost（Automatic SCEPHost）] 値が接続プロファイルの [グループエイリアス（Group-Alias）] と一致しています。たとえば、グループエイリアスが certenroll に設定され、ASA アドレスが asa.example.com の場合は、SCEP 自動ホストを asa.example.com/certenroll に設定する必要があります。
- ASA で ssl certificate-authentication interface outside port 443 コマンドを有効化しました。

Cisco AnyConnect の起動に関する問題

問題　Cisco Jabber が iOS デバイスで Cisco AnyConnect Secure Mobility Client を自動的に起動しない。

対処　次のことを確認してください。

- Unified CM 内でデバイスのオンデマンド VPN URL が設定されている。
- AnyConnect プロファイルのオンデマンドドメインリストにオンデマンド VPN URL が含まれている。

Dial Via Office の問題

Dial Via Office コールが突然終了する

（注）　DVO-R 機能には以下が必要です。
- Cisco Jabber for iPhone client, Release 9.1(1) 以降。
- Unified CM 9.1(1a)（2013 年 2 月リリース）。

問題　DVO コールを発信してキーパッドで任意の番号を押すと、そのコールが通知なしで終了します。この問題は、DVO とユーザ制御のボイスメール回避を有効にしていて、ユーザがコールする個人にビジー回線があり、デスクフォンのボイスメールを設定していなかった場合に発生することがあります。

対処　次のことを試してください。

- ユーザに後からコールするように依頼します。
- ユーザ制御のボイスメールの回避の代わりにタイマーベースのボイスメール回避を使用してエンドユーザを設定します。詳細については、ボイスメール回避の設定，（53 ページ）を参照してください。

Dial via Office コールが接続できない

（注） DVO-R 機能には以下が必要です。
- Cisco Jabber for iPhone client, Release 9.1(1) 以降。
- Unified CM 9.1(1a)（2013 年 2 月リリース）。

問題　ユーザは Jabber 通話オプションを [常に DVO を使用（Always use DVO）] または [自動選択（Automatically select）] に設定しますが、DVO コールを発信しようとしたときに、コールは接続されません。

対処　この問題は、サポート対象外の Unified CM のリリースで DVO を有効にした場合に発生する可能性があります。サポート対象外の Unified CM のリリースで DVO を有効にした場合、エンドユーザは DVO の通話オプションを確認し、DVO コールの発信を試行できますが、コールは接続できません。

関連トピック

各デバイス上での Dial Via Office の有効化，（52 ページ）

Dial via Office コールがボイスメールまたは代替番号から発信される

（注） DVO-R 機能には以下が必要です。
- Cisco Jabber for iPhone client, Release 9.1(1) 以降。
- Unified CM 9.1(1a)（2013 年 2 月リリース）。

問題　個人はユーザのボイスメールシステムまたは代替電話番号からコールを受信します。

対処　次のことを試してください。

- ユーザが代替番号によってDVO コールバック番号を設定するかどうかを確認します。代替番号は、ユーザがクライアントの [DVO コールバック番号（DVO Callback Number）] フィールドに入力した電話番号で、これはUnified CM のユーザのモビリティ ID に設定する電話番号と一致しません。

  代替電話番号の接続先にルーティングするトランクコーリングサーチスペース（CSS）の設定によってこの問題を解決できます。詳細については、モバイルコネクトの有効化，（36 ページ）またはエンタープライズ機能アクセス番号の設定，（47 ページ）を参照してください。
- ユーザがDial via Office コールを発信したときにモバイルボイス接続が弱かったかどうかユーザに確認するように依頼します。この問題を回避するには、ユーザがDial via Office コールを発信する前に強力なモバイル音声接続が存在することを確認します。

問題　代替コールバック番号を使用しているときは、DVO-R コールの発信はできません。代替コールバック番号のパーティションが、発信トランクCSS（コールサーチスペース）にあることを確認します。詳細については、モバイルコネクトの有効化，（36 ページ）またはエンタープライズ機能アクセス番号の設定，（47 ページ）を参照してください。

関連トピック

モビリティ ID の追加，（37 ページ）
リモート接続先の追加（任意），（39 ページ）

DVO コールバックに関する問題

（注） DVO-R機能には以下が必要です。
- Cisco Jabber for iPhone client, Release 9.1(1) 以降。
- Unified CM 9.1(1a)（2013 年2 月リリース）。

問題　ユーザがDVO-R コールを発信した後に、コールバックがモバイルデバイスに到達しないか、ユーザがそれに応答する前に短い期間表示され、その後表示されなくなります。モバイルコネクトがユーザ向けに設定されていると、ユーザはモバイルコネクトコールを受信することがあります。

対処　Unified CM で、[SIP デュアルモードアラートタイマー（SIP Dual Mode Alert Timer）] を5000 ミリ秒まで増やします。問題が解決しない場合は、この値を最大10000 ミリ秒まで、500 ミリ秒単位で大きくしていきます。[SIP デュアルモードアラートタイマー（SIP Dual Mode Alert Timer）] を大きくする方法の詳細については、[SIP デュアルモードアラートタイマー（SIP Dual Mode Alert Timer）] 値の増加，（13 ページ）を参照してください。