Cisco Jabber for Android Release 9.x アドミニストレーション ガイド

初版：2012 年 8 月 16 日

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

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

目 次

第 1 章

Cisco Jabber for Android

Cisco Jabber for Android を使用すると、社内 Wi-Fi ネットワークに接続した状態でエンタープライズ VoIP による発信および社内ディレクトリへのアクセスが可能になります。

Cisco Jabber for Android では次のことができます。

- Cisco Unified Communications Manager（Unified CM）を介し、モバイルデバイスを使用して社内の電話番号で VoIP コールを発信および受信できます。
- 新規メッセージが存在する場合は、Cisco Jabber for Android のホーム画面またはステータスバーからボイスメールにアクセスできます。

  Visual Voicemail 機能を有効にすると、メッセージのリストを表示してリストからメッセージを再生できます。
- SIP ダイジェスト認証を使用して Unified CM でデバイスを認証できます。
- Android のネイティブの電話アプリケーションを使用して、[キーパッド（Keypad）]、[履歴（Logs）]、[お気に入り（Favorites）]、または [連絡帳（Contacts）] タブから業務上のコールを発信できます。
- 最大 2 つの VoIP コールを実行できます（コール ウェイティング、新しいコールの追加、アクティブ コール間の切り替え）。
- 保留、転送、会議など、Unified CM が提供する標準の通話機能の多くを使用できます。
- Cisco Jabber for Android のアクティブな VoIP コールをモバイル ボイス ネットワークに転送できます。
- Cisco Jabber for Android のアクティブな VoIP コールをデバイスからデスクフォンに転送できます。
- 社内ディレクトリを検索できます。
- オフィスの電話番号に残された新規のボイス メッセージがあることをメッセージ インジケータで確認できます。
- Cisco Jabber for Android をバックグラウンドで実行している間は、業務用の電話番号宛のコールを受信できます。 Cisco Jabber for Android は使用可能になると自動的に Unified CM に登録されます。

- VPN クライアントに接続してセキュアなリモート アクセスを行う場合は、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社内の電話番号で VoIP コールを発信および受信できます。

（注） ユーザがリモートの場所から社内の Wi-Fi ネットワークに接続できるようにするには、VPN をサポートするようシステムをセットアップする必要があります。 Cisco Jabber for Android と Cisco AnyConnect Secure Mobility Client の組み合わせがサポートされます。 他の VPN クライアントは正式にはサポートされませんが、他の VPN クライアントも Cisco Jabber for Android で使用できる可能性があります。

- 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 for Android マニュアルは、Cisco Jabber for Android ユーザ ガイド一覧から入手できます。
- 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

次の一般的な手順では、Cisco Jabber の導入方法を説明します。

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。 詳細については、Cisco Jabber for Android のリリース ノートを参照してください。

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, （27 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, （23 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。 Cisco Jabber for Android ユーザ ガイド一覧の『*FAQ*』をユーザに示します。

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 Release 8.5* 以前で必要なファイル

ファイル	このファイルの入手方法の参照先
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 Android 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。 Cisco UC Integration for Microsoft Office Communicator の [ソフトウェアのダウンロード（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。

表 2：*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	Cisco Jabber for Android の [ソフトウェアのダウンロード（Software Downloads）] ページを開きます。 `cmterm-android_9.0.1v24.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	デバイスで Google Play アプリケーション（以前は Google Android Market と呼ばれていました）を使用して、Cisco Jabber for Android アプリケーションを取得します。 Google Play で「Jabber」を検索します。

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）
デバイス COP ファイルのバージョンの確認, （6 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。

（注） Unified CM をリリース 8.6 にアップグレードする前に、最新の COP ファイルを前のリリースの Unified CM にインストールする必要があります。 正しい COP ファイルがあるかどうかを確認するには、「デバイス COP ファイルのバージョンの確認」を参照してください。

Unified CM をアップグレードした後、COP ファイルを再インストールする必要が生じる場合があります。

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。 このプロセスには、時間がかかる場合があります。

i) 使用率が低い時間帯に、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

この手順を使用して、正しいデバイス COP ファイルのバージョンがご使用の Unified CM リリースにすでにインストールされているかどうかを確認します。

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 [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 Android] 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、[SIP ダイジェスト認証の有効化（Enable SIP Digest Authentication）] ドロップダウン リストが表示されることを確認します。
[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。

ダイヤル ルール セットアップ

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、オフィス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。

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 [ソフトウェアのダウンロード（Software Downloads）] ページを開きます。

（注） Cisco Jabber for Android 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：
`AppDialRules.xml`

`DirLookupDialRules.xml`（Cisco Jabber for iPhone 用）

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

VoIP 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。

専用の 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 for Android をバックグラウンドで実行中に、Cisco Jabber for Android を Unified CM に接続したままにすることができます。

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 新規 SIP プロファイルを作成するか、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「120」
- [レジスタのタイムアウト値（Timer Register Expires）] に「720」
- [キープアライブのタイムアウト値（Timer Keep Alive Expires）] に「720」
- [サブスクライブのタイムアウト値（Timer Subscribe Expires）] に「720」

- [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 変更内容を保存します。

ステップ 5 [デバイス（Device）] > [電話（Phone）] の順にアクセスし、設定するデバイスを選択します。

ステップ 6 [プロトコル固有情報（Protocol Specific Information）] セクションで、SIP プロファイルを先程作成したプロファイルに変更します。

ステップ 7 [保存（Save）] を選択してから [適用（Apply）] を選択します。

ステップ 8 [OK] をクリックします。

次の作業

Cisco Jabber for Android を実行するすべての Cisco Dual Mode for Android デバイスに対して、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 および電話機能が、Cisco Jabber for Android から独立して設定され、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セットアップされ、動作している。
  - 保留/復帰
  - コール待機
  - 通話の追加
  - 電話会議
  - 転送
  - RFC 2833、Key Press Markup Language（KPML）、および IVR コール ルーティングのデュアル トーン多重周波数（DTMF）を処理する機能。これにより、ユーザはキーパッドを使用して正しい内線番号または部門にルーティングできます。
- 会議機能がセットアップされ、機能している。 この機能は、システムのセットアップによって異なります。
  - ソフトウェア ベースの会議ブリッジを使用する場合、参加するすべてのエンドポイントは G.711 を使用する必要があります。

- デジタル シグナル プロセッサ（DSP）を使用するハードウェア ベースの会議ブリッジを使用する場合、参加者はG.711またはG.729のいずれかを使用できます。 ハードウェア ベースの会議ブリッジでは、トランスコーダでこの機能を提供する必要はありません。

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	• 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
無効	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」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. 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」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

- どのデバイスにも適用できる標準的な手順に従って、このデバイスに割り当てる拡張機能としてボイスメールをセットアップしてテストします。 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 for Android デバイスに割り当てる予定のデバイス プールに、G.711 コーデックのサポートを含む領域が関連付けられていることを確認します。
- 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 新規の Cisco Dual Mode for Android 電話デバイスを次のように追加します。

a) [デバイス（Device）] > [電話（Phone）] の順に選択します。
b) [新規追加（Add New）] をクリックします。
c) [電話のタイプ（Phone Type）] ドロップダウン リストで、[Cisco Dual Mode for Android] を選択します。

ステップ 3 [デバイス情報（Device Information）] に設定値を入力します。

（注） これらの値には、Cisco Jabber for Android だけを対象とするわけではない制約および要件が適用される可能性があります。 デバイス設定ページ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。

a) デバイス名を入力します。
次のようにデバイス名を指定します。

- BOT 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 文字まで使用できます
- 使用できる文字は、A ～ Z、0 ～ 9、ダッシュ（-）、または下線（_）のみです

シスコは、覚えやすいようにデバイス名にユーザ名を含めることをお勧めします。

例：
ユーザ jsmith の場合にお勧めするデバイス名は BOTJSMITH です。

b) [電話ボタン テンプレート（Phone Button Template）] には、[Standard Dual Mode for Android] を選択します。

c) ユーザがコールを保留にした場合に相手側に保留音が聞こえるように保留音をセットアップします。 この手順により、相手側を混乱させずにすみます。

- メディア リソース グループ リスト（Media Resource Group List）
- 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）

これらの設定は、このデバイスだけ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。

d) ユーザがデスクフォンを所有している場合は[プライマリ電話回線（Primary Phone）]にデスクフォンを選択します。

ステップ 4 [プロトコル固有の情報（Protocol Specific Information）] に設定値を入力します。

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

（注） 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。

b) [SIP プロファイル（SIP Profile）] ドロップダウン リストで適切な SIP プロファイルを選択します。
専用の SIP プロファイルの作成 を参照してください。

このマニュアルでは、[プロトコル固有情報（Protocol Specific Information）] セクションのうち、Cisco Jabber for Android に固有の値についてのみ説明します。 場合によっては、デバイスが正しく動作するために、Cisco Jabber for Android に固有というわけではない、他のプロトコル固有値を入力する必要があります。

ステップ 5 [プロダクト固有の設定（Product Specific Configuration Layout）] セクションに設定値を入力します。

a) [Cisco Usage and Error Tracking] ドロップダウン リストで適切なレベルの使用状況トラッキングを選択します。
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。

b) [アプリケーション ダイヤル ルール URL（Application Dial Rules URL）] フィールドは次のようにします。

- Unified CM Release 8.6 以降の場合、このフィールドはブランクのままにします。

  Unified CM 8.6 以降の場合、[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）] の順に選択してアプリケーション ダイヤル ルールを設定します。 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。

- Unified CM Release 8.5 以前のリリースを使用している場合、Cisco Jabber for Android デバイスでアプリケーション ダイヤル ルールを適用するためには、それらのダイヤル ルール ファイルへのパスをファイル名を含めて指定する必要があります。

  次のフォーマットを使用します：tftp://*TFTP* サーバの *IP* アドレス/*XML* ファイルのパス名/*XML* ファイル名

c) ディレクトリ サーバで認証が必要な場合は、LDAP のユーザ名およびパスワードを入力します。そうでない場合、これらのフィールドはブランクのままにします。
全ユーザに対して単一の読み取り専用アカウントのLDAP資格情報をセットアップすることができます。 これらの資格情報は、TFTP ファイルのプレーンテキストでクライアントに送信されます。 そのため、LDAPディレクトリの管理者には、他の権限を一切持たないディレクトリ クエリ アカウントを生成することを強く推奨します。 そのアカウントは、資格情報が確実にセミパブリック（ローカル ネットワーク上のすべてのユーザが使用可能）になるような低い値で作成してください。

d) [緊急時電話番号（Emergency Numbers）] フィールドに、指定の緊急時電話番号を入力します。このユーザに変わって必ず直接ダイヤルされる追加の緊急時電話番号をコンマ区切りのリストにして入力できます。 これらの番号に、数値以外を含めてはいけません。 スペース、ダッシュ、およびその他の文字も許可されません。

   デバイスに対して定義した緊急時電話番号は、モバイル ネットワークを使用して（エンタープライズ VoIP を使用してダイヤルするのではなく）必ず直接ダイヤルされます。これにより、救急サービスの隊員に発信者の場所を自動的に送信できます（そのようなサービスが利用可能な場合）。 直接ダイヤルされる番号は、次のような状況で便利です。

   - モバイル ネットワーク プロバイダーがある国以外の国にユーザがよく行く
   - 緊急時電話番号が各ユーザの場所によって異なる
   - 会社に専用のセキュリティ番号がある

e) [システム（System）] > [サーバ（Server）] の Unified CM Administration の設定値が、ドメイン名を含まないホスト名である場合は、[ドメイン名（Domain Name）] フィールドにドメインを入力します。

   例：
   `cisco.com`

f) [設定済みの Wi-Fi ネットワーク（Preset Wi-Fi Networks）] フィールドに、最大 3 つの SSID をスラッシュ（/）で区切ったリストを入力します。
ここにリストした SSID またはクライアントでユーザが選択した SSID にモバイルデバイスが接続した後にのみ、Cisco Jabber for Android は Unified CM への接続を試みます。 これらの SSID に接続した場合に Cisco Jabber for Android は Unified CM に到達できなければなりません。 通常、これらは社内の Wi-Fi SSID です。 SSID は最大 32 文字で、大文字小文字の区別があります。

ステップ 6 [保存（Save）] を選択します。

ステップ 7 [設定の適用（Apply Config）] を選択します。

ステップ 8 [[回線 *number*] - 新規 DN を追加（[Line number] - Add a new DN）] を選択します。

ステップ 9 このデバイスの電話番号（DN）を入力します。
この DN は新しいものにすることができます。これと同じ DN を持つデスクフォンは不要です。

ステップ 10 （オプション）デバイスの発信者 ID 設定を入力します。

a) [電話番号情報（Directory Number Information）] セクションの [ルート パーティション（Route Partition）] ドロップダウン リストで、電話番号が属するルート パーティションを選択します。
b) （オプション）[説明（Description）] フィールドに、電話番号とルート パーティションの説明を入力します。
c) [呼び出し表示（Alerting Name）] フィールドに、発信者 ID に対して表示する名前または電話番号を入力します。
d) [ASCII 呼び出し表示（ASCII Alerting Name）] フィールドに、[呼び出し表示（Alerting Name）] フィールドと同じ情報を入力します。ただし、入力は ASCII 文字に限られます。
e) [デバイス *device name* の回線 *number*（Line number on Device device name）] の [表示（発信者 ID）（Display (Caller ID)）] フィールドに、発信者 ID に対して表示する名前または電話番号を入力します。
f) [ASCII 表示（発信者 ID）（ASCII Display (Caller ID)）] フィールドに [表示（発信者 ID）（Display (Caller ID)）] フィールドと同じ情報を入力します。ただし、入力は ASCII 文字に限られます。
g) 必要に応じて [外線電話番号マスク（External Phone Number Mask）] フィールドに、この回線からコールを発信するときに発信者 ID 情報の送信に使用する電話番号（またはマスク）を入力します。
h) コール転送時に発信者名を表示するには、[デバイス *device name* における、転送呼の情報表示（Forwarded Call Information Display on Device device name）] で、[発信者名（Caller Name）] チェックボックスをオンにします。
i) コール転送時に最初にダイヤルされた番号を表示するには、[ダイヤル番号（Dialed Number）] チェックボックスをオンにします。

ステップ 11 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 を共有しない）の場合は、[コール転送とコール ピックアップの設定（Call Forward and Call Pickup Setting）] 領域で次を設定して、Cisco Jabber for Android が非実行中でネットワークに接続していないときにはコール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、Unified CM のオンライン ヘルプで [不在転送（Forward All）] などの設定を参照してください。

ステップ 12 [無応答時の呼び出し時間（No Answer Ring Duration）] 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 for Android が呼び出し音を鳴らす時間を持てるようにします。
Unified CM のオンライン ヘルプで、一般的な制限について参照してください。

ステップ 13 [保存（Save）] を選択します。

ステップ 14 ユーザの [エンド ユーザ（End User）] ページに移動します。

ステップ 15 このユーザ用に作成した Cisco Dual Mode for Android デバイスを関連付けます。
デバイスを関連付けた後、[制御するデバイス（Controlled Devices）] ボックスの [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）] セクションのいずれかに表示されます（Unified CM のリリースによって異なる）。

ステップ 16 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 17 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。

ステップ 18 [保存（Save）] を選択します。

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。

- モバイル デバイスが企業ネットワークに接続されていることを確認します。 デバイスのブラウザを使用して社内イントラネット上の Web ページにアクセスできることを確認します。
- Cisco Jabber for Android を起動して、セットアップ ウィザードを完了します。 TFTP サーバの IP アドレス（通常は、Unified CM サーバの IP アドレス）と先程追加したデバイスのデバイス名（BOTXXXX）を入力します。 セットアップ ウィザードの実行方法については、エンド ユーザ向けの FAQ を参照してください。
- デバイスが登録されたことを示す通知が出されるまで待ちます。 Unified CM にデバイスが接続すると、ステータス バーの Cisco Jabber のアイコンが黒になります。
- コールの発信、保留、転送など、Cisco Jabber for Android の基本的なテレフォニー機能をテストします。

ユーザ デバイスへの変更

[Unified CM の管理（Unified CM Administration）] ページの設定（LDAP、コール制御、ダイヤル プランなど）を変更すると、[保存（Save）] をクリックして [設定の適用（Apply Config）] をクリックした後、Cisco Jabber for Android はそれらを登録します。 このアプリケーションの再登録は 30 秒後に行われます。 アプリケーションが登録するときにユーザがコール中である場合、そのコールはドロップされ、アプリケーションは自動的に再起動します。 変更を適用するときにデバイスが対応範囲外にある場合、アプリケーションは後で Unified CM に登録するときにアプリケーションを更新します。

Unified CM からデバイスを削除すると、Cisco Jabber for Android はアクティブなすべてのコールをドロップし、登録を数回試行した後、ユーザは接続できないことを知らせるエラー メッセージを受け取ります。 クライアントの情報は、デバイスから消去されません。 すべてのクライアント情

報を削除するには（たとえば、従業員が退職する場合など）、Microsoft ActiveSync などの適切なデバイス管理ソリューションを使用してください。

デバイスを削除するには、該当するリリースの『*Cisco Unified Communications Manager Administration Guide*』にあるトピック「Deleting a Phone」を参照してください。これは、メンテナンス ガイド一覧から入手できます。

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。

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。

- 企業 Wi-Fi ネットワークにモバイル デバイスを接続するための操作手順。 この手順は、Cisco Jabber for Android とは関係ありません。
- Cisco Jabber for Android を設定するための手順を含むユーザ用の資料。FAQ から入手できます。

重要 ユーザが最初に Cisco Jabber for Android を設定するときに社内ネットワークの外にいるときは、社内ネットワークへの VPN 接続を使用する必要があります。 ユーザは Cisco Jabber for Android を使用する前に、この VPN 接続を設定する必要があります。

- Google Play（以前は Google Android Market と呼ばれていました）から Cisco Jabber for Android をダウンロードおよびインストールするための手順。
- たとえば BOTJSMITH など、ユーザの Cisco Dual Mode for Android デバイスのデバイス名。
- TFTP サーバの IP アドレス。

- （該当する場合）ユーザが SIP ダイジェスト認証に必要な資格情報。 [SIP ダイジェスト認証（SIP Digest Authentication）] を有効にし、Unified CM に手動で認証するようにユーザを設定している場合、これらの資格情報を提供する必要があります。
- （該当する場合）Visual Voicemail にアクセスするためにユーザが必要な資格情報。
- （該当する場合）社内ディレクトリにアクセスするためにユーザが必要な資格情報。 推奨されるユーザ名の形式は、userid@company.com または DN の完全な形式 cn=userid,ou=organization,dc=company,dc=com のいずれかです。
- （該当する場合）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。

  Cisco AnyConnect Secure Mobility Client を使用するようにシステムをセットアップしている場合、ユーザは、ユーザ ガイド一覧の最新の『*Android User Guide for Cisco AnyConnect Secure Mobility Client*』から、Android デバイスでクライアント アプリケーションをインストールおよび使用する方法についての情報を入手できます。

  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、Google Play から無料で Cisco AnyConnect Secure Mobility Client および Cisco Jabber for Android 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内部 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。

- ユーザが問題レポート（トラブルシューティング ログ）を送信する際の宛先となる電子メール アドレス。

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 *4* : ***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
インターネット通話	TFTP	UDP	69	該当なし
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。
ディレクトリ	LDAP	TCP	389	LDAP（オプションで TLS を使用）
Unity Connection ボイスメール	VMREST	TCP	143	該当なし
Unity Connection ボイスメール	VMREST	TCP	7993	IMAP（SSL/TLS を使用）

第 4 章

機能の設定

モバイル コネクトとモバイル ID の追加

モバイル コネクト（以前のシングル ナンバー リーチ（SNR））は、Cisco Jabber が利用できないときに誰かがオフィスの番号にコールした場合に、ネイティブな携帯電話番号が鳴ることを可能にします。

Cisco Jabber が実行中で、企業のネットワークに接続されており、そのため VoIP コールを受信できる場合は、モバイル コネクトは自動的に非アクティブになります。

ユーザは、Cisco Jabber VoIP コールをモバイル ボイス ネットワークに転送するためのモバイル ID を必要とします。

（注） Cisco Jabber for Android のコールをモバイル ボイス ネットワークに移動するオプションは、ユーザが VPN を使用してモバイル データ ネットワークまたは社外 Wi-Fi ネットワーク経由で社内ネットワークに接続している場合は使用できません。

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バイル 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) [プライマリ ユーザ デバイス（Primary User Device）] 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。
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）	Unified CM にカスタム パーティションおよび複数のコーリング サーチスペースがある場合は、携帯電話番号に適用するパーティションが含まれた [コーリング サーチ スペースの再ルーティング（Rerouting Calling Search Space）] を選択します。 この携帯電話番号をモバイル ID として入力します（この手順で後述します）。

b) [保存（Save）] を選択します。

ステップ 5 携帯電話番号の新しいモバイル ID を追加します。

a) 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。

b) [新しいモバイル ID の追加（Add a New Mobile Identity）] を選択します。

c) [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。

d) 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、ネイティブなデバイス 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 この値は、モバイル コールの比較的長いコール セットアップ時間特性に対応できます。

e) [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。
f) 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。
g) [保存（Save）] を選択します。

次の作業

設定をテストします。

1 モバイル デバイスで Cisco Jabber を終了します。 手順については、ユーザ ガイド一覧から『*FAQ*』を参照してください。
2 別の電話から Cisco Jabber の内線にコールします。
3 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。

VoIP からモバイル ボイス ネットワークにアクティブなコールを転送できるようにする

ユーザが社内 Wi-Fi ネットワークの中にいる場合、アクティブな VoIP コールを Cisco Jabber for Android からモバイル ボイス ネットワーク上の携帯電話に転送できます。 この機能は、ユーザが通話しながら社内 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 for Android のこの機能を「モバイル ネットワークを使用」と呼びます。

（注） Cisco Jabber for Android のコールをモバイル ボイス ネットワークに移動するオプションは、ユーザが VPN を使用してモバイル データ ネットワークまたは社外 Wi-Fi ネットワーク経由で社内ネットワークに接続している場合は使用できません。

- 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) [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。
  b) [デバイス（Device）] > [デバイス設定（Device Settings）] > [ソフトキー テンプレート（Softkey Template）] の順に選択します。
  c) 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。
  d) 右上の [関連リンク（Related Links）] ドロップダウン リストで、[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。
  e) コール状態のドロップダウン リストで [接続中（Connected）] 状態を選択し、選択されているソフトキーのリストに [モビリティ（Mobility）] キーが入っていることを確認します。
  f) コール状態のドロップダウンリストで[オンフック（On-hook）]状態を選択し、選択されているソフトキーのリストに [モビリティ（Mobility）] キーが入っていることを確認します。
- Cisco Unified Communications Manager のユーザ単位およびデバイス単位の設定で、特定のデバイスからコールをモバイルボイス ネットワークに転送するときに[モビリティ（Mobility）] ソフトキーを使用するように設定します。 モバイルデバイスに対してモバイル ID およびモバイル コネクトの両方をセットアップしていることを確認します。 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。
  a) [Unified CM の管理（Unified CM Administration）] ポータルにサインインします。
  b) Cisco Dual Mode for Android デバイスの [電話の設定（Phone Configuration）] 画面で [オーナーのユーザ ID（Owner User ID）] を選択します。
  c) [モビリティ ユーザ ID（Mobility User ID）] を選択します。
  通常、この値は [オーナーのユーザ ID（Owner User ID）] と同じです。
  d) [プロダクト固有の設定（Product Specific Configuration Layout）] セクションの [モバイル ネットワークへの転送（Transfer to Mobile Network）] ドロップダウン リストで、[モビリティ ソフトキーの使用（Use Mobility Softkey）] を選択します。

次の作業

VoIP からアクティブなコールをモバイル ネットワークに転送して、設定をテストします。

関連トピック

モバイル コネクトとモバイル ID の追加, （27 ページ）

ユーザ デバイスの追加, （18 ページ）

デスクフォンからモバイルデバイスへのアクティブコール転送の有効化

はじめる前に

- デスクフォンと Cisco Dual Mode for Android（BOTXXXX）デバイスを設定したことを確認します。
- BOTXXXX デバイスにモバイル コネクト機能を設定したことを確認します。 「モバイル コネクトとモバイル ID の追加」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 BOTXXXX デバイスの [電話の設定（Phone Configuration）] 画面に移動します。

ステップ 3 [デバイス情報（Device Information）] セクションで、[モビリティ ユーザ ID（Mobility User ID）] の値を確認します。

ステップ 4 関連付けられたデスクフォンの [電話設定（Phone Configuration）] 画面に移動します。

ステップ 5 [デバイス情報（Device Information）] セクションで、デスクフォンの [オーナーのユーザ ID（Owner User ID）] の値が、BOTXXXX デバイスの [モビリティ ユーザ ID（Mobility User ID）] の値と一致することを確認します。

ステップ 6 [デバイス情報（Device Information）] セクションの [ソフトキー テンプレート（Softkey Template）] ドロップダウン リストから、[モビリティ（Mobility）] を選択します。

（注） [モビリティ（Mobility）] オプションが表示されない場合、モビリティ ソフトキーを設定する必要があります。 『Cisco Unified Communications Manager Features and Services Guide, Release 7.0(1)』の章「Cisco Unified Mobility」にある「Mobility Softkey Configuration」の項を参照してください。

次の作業

設定をテストします。 コールをモバイルデバイスに移動する手順は、デスクフォンのモデルによって異なる場合があります。 手順の一例を次に示します。

1. デスクフォンの [モビリティ（Mobility）] ソフトキーを押します。
   場合によっては、[モビリティ（Mobility）] ソフトキーが表示されるまで、[その他（More）] を数回押す必要があることがあります。
2. [携帯電話へコールを送信（Send call to Mobile）] を選択します。
3. モバイルデバイスでコールに応答します。

関連トピック

モバイル コネクトとモバイル ID の追加, （27 ページ）
ユーザ デバイスの追加, （18 ページ）

Dial Via Office の設定

重要 この機能は、Unified CM Release 8.6 以降でのみ使用できます。

Dial Via Office（DVO）機能を使用すると、ユーザはデバイスの音声計画を使用して、勤務先番号で Cisco Jabber 発信コールを開始できます。 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。

- [常に DVO を使用（Always use DVO）]：このオプションを選択した場合、着信コールはモバイル コネクトを使用します（以前はシングル ナンバー リーチ [SNR] と呼ばれていました）。モバイル コネクトを使用すると、Cisco Jabber を使用できない状態で勤務先番号に電話がかかってきたときに、ネイティブの携帯電話番号で呼び出し音を鳴らすことができます。 これらの着信コールは、モバイル ボイス ネットワークで受信されます。
- [自動的に選択（Automatically select）]：このオプションを選択した場合、Cisco Jabber は、Wi-Fi またはユーザのインターネットのモバイル データ プランを使用して、勤務先番号への着信コールに対してインターネット電話機として機能します。

Dial Via Office（DVO）機能を設定するには、次の手順を実行します。

1 DVO をサポートするように Unified CM を設定します。 DVO をサポートするための Unified CM の設定, （32 ページ）を参照してください。

2 各 Cisco Dual Mode for Android 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, （34 ページ）を参照してください。

DVO をサポートするための Unified CM の設定

DVO 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, （33 ページ）
- モビリティ プロファイルの設定, （33 ページ）

2 デバイス COP ファイルのバージョンの確認, （34 ページ）

エンタープライズ機能アクセス番号の設定

すべての Dial via Office コールに対してエンタープライズ機能アクセス番号を設定するには、次の手順を使用します。

Dial via Office のリバース コールバック コールの場合、エンタープライズ機能アクセス番号は、Cisco Unified Communications Manager が携帯電話および着信番号をコールするの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として使用するダイヤルイン方式（DID）番号を予約します。
- 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）。

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。

国際電話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。

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。

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 リバースを設定できます。モビリティプロファイルを設定した後、ユーザまたはユーザのグループ（ある地域または場所のユーザなど）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 リバース 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

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 Android] 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 デバイスに対して Dial Via Office を設定するには、次の手順を使用します。

1 モバイル コネクトとモバイル ID の追加

2 各デバイス上での Dial Via Office の有効化

モバイル コネクトとモバイル ID の追加

モバイル コネクト（以前のシングル ナンバー リーチ（SNR））は、Cisco Jabber が利用できないときに誰かがオフィスの番号にコールした場合に、ネイティブな携帯電話番号が鳴ることを可能にします。

Cisco Jabber が実行中で、企業のネットワークに接続されており、そのため VoIP コールを受信できる場合は、モバイル コネクトは自動的に非アクティブになります。

ユーザは、Cisco Jabber VoIP コールをモバイル ボイス ネットワークに転送するためのモバイル ID を必要とします。

（注） Cisco Jabber for Android のコールをモバイル ボイス ネットワークに移動するオプションは、ユーザが VPN を使用してモバイル データ ネットワークまたは社外 Wi-Fi ネットワーク経由で社内ネットワークに接続している場合は使用できません。

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バイル 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) [プライマリ ユーザ デバイス（Primary User Device）] 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。
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。

設定	情報
再ルーティング用コーリング サーチ スペース（Rerouting Calling Search Space）	Unified CM にカスタム パーティションおよび複数のコーリング サーチ スペースがある場合は、携帯電話番号に適用するパーティションが含まれた [コーリング サーチ スペースの再ルーティング（Rerouting Calling Search Space）] を選択します。 この携帯電話番号をモバイル ID として入力します（この手順で後述します）。

b) [保存（Save）] を選択します。

ステップ 5 携帯電話番号の新しいモバイル ID を追加します。

a) 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。
b) [新しいモバイル ID の追加（Add a New Mobile Identity）] を選択します。
c) [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。
d) 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、ネイティブなデバイス 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 この値は、モバイル コールの比較的長いコール セットアップ時間特性に対応できます。

e) [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。
f) 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。
g) [保存（Save）] を選択します。

次の作業

設定をテストします。

1. モバイル デバイスで Cisco Jabber を終了します。 手順については、ユーザ ガイド一覧から『*FAQ*』を参照してください。
2. 別の電話から Cisco Jabber の内線にコールします。
3. 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。

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、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 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（CUCM 8.6 以降）] ドロップダウン リストを [有効（Enabled）] に設定します。

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。

Visual Voicemail のセットアップ

Visual Voicemail 機能は、基本ボイス メール サービスの代替機能の 1 つです。

Visual Voicemail を使用すると、ボイス メールボックスにダイヤルインしなくても、メッセージのリストを表示できます。 このリストから、次を行うことができます。

- メッセージの再生および一時停止
- メッセージの音声テキスト変換の表示（使用可能な場合）
- メッセージの削除
- メッセージを送信した連絡先へのコール バック
- 連絡先の追加

Visual Voicemail をセットアップするには、次の手順を実行します。

1. Voicemail Representational State Transfer（VMREST）サービスが Cisco Unity Connection にセットアップされていることを確認します。 VMREST サービスの確認, （38 ページ）を参照してください。
2. Cisco Unity Connection でセキュア メッセージングの設定を有効にします。 セキュア メッセージングの設定の有効化, （38 ページ）を参照してください。
3. Unified CM に Visual Voicemail をセットアップします。 Unified CM での Visual Voicemail のセットアップ, （39 ページ）を参照してください。

VMREST サービスの確認

ご使用の Cisco Unity Connection が正しい VMREST サービスでセットアップされ、Visual Voicemail を Cisco Jabber for Android でサポートしていることを確認するには、次の手順を実行します。

手順

ステップ 1 Cisco Unity Connection Administration にサインインします。

ステップ 2 [ナビゲーション（Navigation）] ドロップダウン リストから、[Cisco Unity Connection のサービスアビリティ（Cisco Unity Connection Serviceability）] を選択します。

ステップ 3 [移動（Go）] を選択します。

ステップ 4 [ツール（Tools）] > [サービス管理（Service Management）] を選択します。

ステップ 5 [オプション サービス（Optional Services）] セクションで、次のサービスがアクティブで実行中であることを確認します。

- Connection Jetty
- Connection REST Service

セキュア メッセージングの設定の有効化

Cisco Jabber for Android でのセキュアなボイス メッセージの再生をサポートするように Cisco Unity Connection をセットアップするには、この手順を使用します。

手順

ステップ 1 Cisco Unity Connection Administration にサインインします。

ステップ 2 [ナビゲーション（Navigation）] ドロップダウン リストで [Cisco Unity Connection Administration] を選択します。

ステップ 3 [移動（Go）] を選択します。

ステップ 4 左ペインで、[システム設定（System Settings）] > [詳細設定（Advanced）] > [API 設定（API Settings）] の順に移動します。

ステップ 5 次の 3 つのチェックボックスをオンにします。

a) CUMI を介したセキュア メッセージ録音へのアクセスを許可する（Allow Access to Secure Message Recordings through CUMI）

b) CUMI を介してセキュア メッセージのメッセージ ヘッダー情報を表示する（Display Message Header Information of Secure Messages through CUMI）

c) CUMI 経由のメッセージ添付ファイルを許可する（Allow Message Attachments through CUMI）

ステップ 6 [保存（Save）] を選択します。

Unified CM での Visual Voicemail のセットアップ

はじめる前に

- 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、完全修飾ドメイン名または IP アドレスを入力します。 *Servername.YourCompany.com:portnumber* の形式を使用します。

設定	説明
ボイスメール メッセージ ストアのユーザ名（Voicemail Message Store Username）	このフィールドは空欄のままにします。 Android用のCisco Jabberでは、このフィールドが使用されません。 このフィールドは、Cisco Unityをサポートしているデバイスで使用されます。
ボイスメール メッセージ ストア（Voicemail Message Store）	このフィールドは空欄のままにします。 Android用のCisco Jabberでは、このフィールドが使用されません。 このフィールドは、Cisco Unityをサポートしているデバイスで使用されます。

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 [リセット（Reset）] を選択します。
ステップ 7 Cisco Jabber を再起動します。
ステップ 8 ボイスメール画面が表示されるまで、セットアップ ウィザードの手順に従います。
ステップ 9 ボイスメールのパスワードを入力します。
ステップ 10 [検証（Verify）] を選択します。
ステップ 11 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。

拡張メッセージ受信インジケータの有効化

メッセージ受信インジケータは、新規ボイスメッセージがあることをユーザに知らせます。拡張メッセージ受信インジケータは、この機能をサポートするシステム上で未再生メッセージの数を示します。 ユーザは、ボイス メッセージング システムに電話してメッセージを取得できます。

（注） 基本的なメッセージ受信インジケータを有効にするには、使用するリリース用のCisco Unified Communications Managerのマニュアルに記載されている手順に従ってください。 このクライアントに固有の設定はありません。

導入環境で拡張メッセージ受信インジケータがサポートされる場合は、このオプションを Cisco Unity Connection Administration ポータルで有効にします。

手順

ステップ 1 Cisco Unity Connection Administration にサインインします。

ステップ 2 左ペインで、[テレフォニー統合（Telephony Integrations）] > [電話システム（Phone System）] に移動します。

ステップ 3 目的の電話システムのリンクを選択します。

ステップ 4 [メッセージ受信インジケータ（Message Waiting Indicators）] セクションで、[送信メッセージ数（Send Message Counts）] にチェックを入れます。

ステップ 5 [保存（Save）] を選択します。

ディレクトリ検索設定値の指定

この手順を使用すると、ディレクトリ サーバに接続するときに Cisco Jabber で使用する設定値を指定できます。 これらの設定値は、ユーザが Cisco Jabber をセットアップしたときに自動的に設定されます。

（注） Cisco Jabber for Android は、Open LDAP を使用する場合はレポート構造機能をサポートしません。 この機能は、Microsoft Active Directory を使用する場合にのみサポートされます。

レポート構造をセットアップするには、Cisco Jabber for Android で、マネージャ（Manager）、ダイレクト レポート（Direct reports）、役職（Title）、および部署（Department）という要素を使用します。

はじめる前に

社内のディレクトリ スキーマで、アプリケーションのデフォルトとは異なる属性、または追加された属性を特定します。 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。

次のテーブルを使用してディレクトリの値を確認してください。

- 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名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名を書き留めてください。

表 *5*：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）	ID	distinguishedName	distinguishedName	
表示名（Display Name）	displayName	displayName	cn	
E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	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			
自宅の電話番号（予備）（Second home phone number）	homePhoneNumber2			
携帯電話番号（Mobile Phone Number）	mobilePhoneNumber			
携帯電話番号（予備）（Second mobile phone number）	mobilePhoneNumber2			

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
ボイスメール直通電話番号（Direct to voicemail phone number）	voicemailPhoneNumber	voicemail		
ファクス番号（Fax number）	faxPhoneNumber	facsimileTelephoneNumber		
その他の電話番号（Other phone number）	otherPhoneNumber			
マネージャ	manager	manager		
ダイレクト レポート（Direct reports）	directReports	directReports		
タイトル	title	title		
部門	department	department		

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、[LDAP ユーザ認証の有効化（Enable LDAP User Authentication）] の設定値を設定します。

- ユーザがディレクトリ サービスへアクセスするときに資格情報の入力が必要ない場合は、[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 4 [LDAP サーバ（LDAP Server）] フィールドに、LDAP サーバの IP アドレスまたはホスト名を入力します。

- Cisco Jabber for Android にディレクトリ検索を導入しない場合、このフィールドはブランクのままにします。
- そうでない場合は、ディレクトリ サーバの IP アドレスまたはホスト名、およびポート番号を入力します。

YourDirectoryServer.YourCompany.com:portnumber という形式を使用します。 IP アドレスまたはホスト名を入力し、ポートを入力しなかった場合、クライアントはポート 389 への接続を試みます。

ステップ 5 [LDAP SSL の有効化（Enable LDAP SSL）] ドロップダウン リストが表示されます。 LDAP で SSL はサポートされないため、SSL はデフォルトで無効になっています。 [有効（Enabled）] または [無効（Disabled）] を選択しても影響はありません。

ステップ 6 次のいずれかの形式で LDAP 検索ベースを入力します。

- *OU=organization,DC=corp,DC=yourcompany,DC=com*
- *CN=users,DC=corp,DC=yourcompany,DC=com*

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ためには、ユーザ情報が格納されている社内ディレクトリのルート ノードの識別名を入力します。 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決定できるように、**Active Directory Explorer**（Microsoft 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確認してください。

ステップ 7 LDAP フィールド マッピングを入力します。 LDAP フィールド マッピングによって、ディレクトリ検索で検索して表示する情報を保持するディレクトリの属性を指定します。 「ディレクトリの要素および属性」テーブルを使用して、デフォルトと一致しないフィールド マッピングを name=value ペアとして入力します。各フィールドはセミコロン（;）で区切ります。 *name*“ ”には「要素名」列に入ってい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 8 LDAP 写真の場所に入力します。 HTTP サーバ上の画像ファイルのパス名を入力します。 必ず正しいグラフィック ファイル タイプを指定してください（jpg や png など）。 LDAP 属性を表すには、変数「%%*LDAP Attribute* %%」を使用します。

例：
`http://yourcompany.cisco.com/photo/std/%%userID%%.jpg`
文字列の中にパーセント記号を 2 つ重ねて指定する必要があります。

Cisco Jabber for Android は必要に応じて画像のサイズを自動的に調整しますが、画像が小さいほど処理は速くなります。

写真は HTTP サーバ上に保存する必要があります。ファイル名は、LDAP ディレクトリ属性内の値と同一にします（ファイル名の拡張子は除きます）。

デフォルトでは、Cisco Jabber for Android は、この手順の前に説明した「ディレクトリの要素および属性」テーブルの userid 要素にマップされる属性を使用します。 [LDAP フィールドマッピング（LDAP Field Mappings）] フィールドで別の属性を指定できます。

例：
ディレクトリのイメージ ファイルの名前が `jsmith.jpg` で、cn 属性の値が `jsmith` の場合は、[LDAP フィールドマッピング（LDAP Field Mappings）] フィールドを使用して userid 要素を LDAP ディレクトリの cn 属性にマップできます。

ステップ 9 [保存（Save）] を選択します。

ステップ 10 Cisco Jabber for Android を再起動します。

次の作業

ディレクトリ検索機能をテストします。

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。

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, （46 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
  - パスワードは保存されません。 パスワードは TFTP サーバからクリア テキストで送信されます。
  - 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, （46 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, （47 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 リストの [プロトコル固有情報（Protocol Specific Information）] セクションで [Cisco Dual Mode for Android - 標準 SIP 非セキュア プロファイル（Cisco Dual Mode for Android - 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 [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。

ステップ 7 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 Android の新しいプロファイルを作成します。

a) [新規追加（Add New）] を選択します。

b) [電話セキュリティ プロファイルのタイプ（Phone Security Profile Type）] ドロップダウン リストで、[Cisco Dual Mode for Android] を選択します。

c) [次へ（Next）] を選択します。

d) 新しい電話セキュリティ プロファイルの名前を入力します。

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

f) [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。
g) [保存（Save）] 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。

ステップ 3 [Cisco Dual Mode for Android デバイス（Cisco Dual Mode for Android device）] ページごとに、[プロファイル固有情報（Protocol 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）] ドロップダウン リストで、作成した新しいセキュア プロファイルを選択します。
b) [ダイジェスト ユーザ（Digest User）] ドロップダウン 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 [有効（Enabled）] 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 [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。

ステップ 7 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 Android の新しいプロファイルを作成します。

a) [新規追加（Add New）] を選択します。
b) [電話セキュリティ プロファイルのタイプ（Phone Security Profile Type）] ドロップダウン リストで、[Cisco Dual Mode for Android] を選択します。
c) [次へ（Next）] を選択します。
d) 新しい電話セキュリティ プロファイルの名前を入力します。

e) [ダイジェスト認証を有効化（Enable digest authentication）] を選択します。
f) [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。
g) [保存（Save）] 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 Android デバイス（Cisco Dual Mode for Android 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、作成した新しいセキュア 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。

重要 [SIP ダイジェスト認証（SIP Digest Authentication）] を有効にするには、（前の手順で概説されているように）SIP ダイジェスト認証を有効にするカスタム デバイス セキュリティ プロファイルも選択する必要があります。

このカスタム デバイス セキュリティ プロファイルを最初に選択せずに SIP ダイジェスト認証を有効にすると、次のようになります。

- Cisco Jabber は、エンド ユーザに SIP ダイジェスト認証用の資格情報の入力を求めるプロンプトを出します。
- Cisco Jabber はすべての資格情報を受け入れます。
- Unified CM は SIP ダイジェスト認証を使用してデバイスを認証しません。

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 [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。

ステップ 7 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 8 [インターネット通話の設定（Internet Calling 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。

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。

以前、セキュア接続に対応した Cisco Jabber for Android を展開していた場合は、Release Notes の「What's New」の項を参照してください。

（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, （50 ページ）
   b. VPN 接続の自動化, （50 ページ）
   c. 証明書ベースの認証の設定, （51 ページ）
   d. ASA セッション パラメータの設定, （53 ページ）
   e. トンネル ポリシーの設定, （54 ページ）
3. [設定済みの Wi-Fi ネットワーク（Preset Wi-Fi Networks）] フィールドを設定することによって、Cisco AnyConnect をサポートするように Unified CM をセットアップします。 ユーザ デバイスの追加, （18 ページ）を参照してください。

（注） Cisco Jabber for Android と Cisco AnyConnect Secure Mobility Client の組み合わせがサポートされます。 他の VPN クライアントは正式にはサポートされませんが、他の VPN クライアントも Cisco Jabber for Android で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. ユーザ デバイスの追加, （18 ページ）の手順を使用して、[設定済みの Wi-Fi ネットワーク（Preset Wi-Fi Networks）] 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。

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、『AnyConnect Administration Guide』を参照してください。

VPN 接続の自動化

ユーザが企業の Wi-Fi ネットワーク外から Cisco Jabber を開く場合、Cisco Jabber には、Cisco UC アプリケーション サーバにアクセスするための VPN 接続が必要です。 Cisco AnyConnect Secure Mobility Client が、バックグラウンドで VPN 接続を自動的に確立できるようにシステムを設定できます。これは、シームレスなユーザ エクスペリエンスの提供に役立ちます。

Trusted Network Detection のセットアップ

Trusted Network Detection 機能は、ユーザの場所を基にして VPN 接続を自動化することによって、ユーザの体感品質を向上させます。ユーザが社内 Wi-Fi ネットワークの中にいる場合、Cisco Jabber は直接 Cisco UC インフラストラクチャに到達できます。 ユーザが社内 Wi-Fi ネットワークから離れると、Cisco Jabber は、信頼ネットワークの外にいることを自動的に検出し、間接的に VPN を開始して UC インフラストラクチャへの接続を確保します。

（注） Trusted Network Detection 機能には、証明書ベース認証およびパスワード ベース認証の両方を使用できます。 ただし、証明書ベース認証の方が、よりシームレスな体感を与えることができます。

手順

ステップ 1 ASDM を使用して、Cisco AnyConnect のクライアント プロファイルを開きます。

ステップ 2 クライアントが社内 Wi-Fi ネットワークの中にいるときにインターフェイスで受信可能な、信頼できる DNS サーバおよび信頼できる DNS ドメイン サフィックスのリストを入力します。Cisco AnyConnect クライアントは、現在のインターフェイス DNS サーバおよびドメイン サフィックスを、このプロファイルの設定と比較します。

（注） Trusted Network Detection 機能が正しく動作するためには、DNS サーバをすべて指定する必要があります。 TrustedDNSDomains と TrustedDNSServers の両方をセットアップした場合は、信頼ネットワークとして定義した両方の設定とセッションが一致する必要があります。

Trusted Network Detection をセットアップするための詳細な手順については、『Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5』の章「AnyConnect 機能の設定」で「Trusted Network Detection」の項を参照してください。

次の作業

[設定済みの Wi-Fi ネットワーク（Preset Wi-Fi Networks）] フィールドを設定することによって、Cisco AnyConnect をサポートするように Unified CM をセットアップします。ユーザ デバイスの追加, （18 ページ）を参照してください。

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 を設定する高レベルな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 Digital Certificates」の項を参照してください。

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

証明書をユーザに確実に発行できるように、システムをセットアップする必要があります。

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。

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、「Enabling Datagram Transport Layer Security (DTLS) with AnyConnect (SSL) Connections」を参照してください。

ステップ 2 セッションの永続性（自動再接続）を設定します。

a) ASDM を使用して VPN クライアント プロファイルを開きます。
b) [自動再接続の動作（Auto Reconnect Behavior）] パラメータを [復帰後に再接続（Reconnect After Resume）] に設定します。

セッションの永続性を設定する方法の詳細については、「Configuring Auto-Reconnect」を参照してください。

ステップ 3 アイドル タイムアウト値を設定します。

a) 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の詳細については、「vpn-idle-timeout」を参照してください。

ステップ 4 Dead Peer Detection（DPD）を設定します。

a) サーバ側の DPD を無効にします。
b) クライアント側の DPD を有効にします。

DPD を設定する方法の詳細については、「Enabling and Adjusting Dead Peer Detection」を参照してください。

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決定した後、「Configuring Split-Tunneling Attributes」に説明されている詳細な手順に従い、適切なトンネル ポリシーでグループ ポリシーを設定します。

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。

- 管理者のサポートなしでユーザが実行する解決法、およびアプリケーションの動作原理に関するヒントとテクニックについては、ユーザ FAQ を参照してください。
- 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，58 ページ
- アプリケーションをセットアップする前に Cisco Jabber for Android からログを取得する，58 ページ
- アプリケーションをセットアップした後に Cisco Jabber for Android からログを取得する，59 ページ
- Cisco AnyConnect からのログの取得，60 ページ
- DART からの Cisco AnyConnect トラブルシューティング データの取得，61 ページ
- 問題のトラブルシューティング，61 ページ

接続ステータスの確認

モバイルデバイスによる接続ステータスの確認

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 [メニュー（Menu）] > [設定（Settings）] の順にタップします。

ステップ 3 [アカウント（Accounts）] で、関連する機能の接続ステータスを確認します。

Cisco Jabber for Android は、次のいずれかの接続ステータス メッセージを表示します。

接続中（Connected）

機能はセットアップ済みで、適切に接続しています。

接続中（Connecting）

機能は現在接続を試行中です。

切断（Disconnected）

機能はセットアップ済みですが、現在接続していません。 たとえば、社内 Wi-Fi ネットワークが正しく接続されていなかったり、サーバがダウンしていたりすると、この接続ステータスが表示されます。

Error

機能は現在セットアップされていないか、接続していません。 たとえば、誤ったパスワードを入力するとエラーが表示されます。

アプリケーションをセットアップする前に Cisco Jabber for Android からログを取得する

ユーザがまだセットアップ ウィザードを完了していない場合は、この手順をユーザに実行させて、Cisco Jabber for Android からログを送信させます。

シスコは、ユーザが Android デバイス上の E メール アプリケーションをセットアップすることをお勧めします。

（注） ユーザがすでにセットアップ ウィザードを完了している場合、問題レポートの送信手順は異なります。

ユーザがすでにセットアップ ウィザードを完了している場合は、アプリケーションをセットアップした後に Cisco Jabber for Android からログを取得する，（59 ページ）を参照してください。

手順

ステップ 1 Cisco Jabber for Android で、[セットアップの開始（Begin Setup）] 画面にアクセスします。

ステップ 2 [メニュー（Menu）] > [ヘルプ（Help）] > [トラブルシューティング（Troubleshooting）] > [ログの送信（Send Logs）] の順にタップします。

ステップ 3 [オーディオ エンジン ログ（Audio Engine Logs）] チェックボックスがオフになっていることを確認します。

ステップ 4 すでに [インターネット設定（Internet Settings）] 画面の設定が完了している場合は、[設定ファイル（Configuration Files）] チェックボックスをオンにします。 それ以外の場合、このチェック ボックスはオフのままにします。

ステップ 5 [ログの送信（Send Logs）] をタップします。
E メール アプリケーションが開き、新規メッセージが表示されます。このメッセージには、すでに件名が設定され、ログ ファイルも添付されています。

ステップ 6 E メール メッセージの本文に問題の説明を入力し、システム管理者に送信します。

ヒント 問題が再現可能な場合は、[メニュー（Menu）] > [設定（Settings）] の順にタップして詳細ログを有効にします。 次に、[ヘルプ（Help）] で [トラブルシューティング（Troubleshooting）] をタップします。 [詳細ログ（Detailed Logging）] チェックボックスをオンにし、問題を再現してから問題レポートを送信します。

アプリケーションをセットアップした後に Cisco Jabber for Android からログを取得する

ユーザがすでにセットアップ ウィザードを完了している場合は、この手順をユーザに実行させて、Cisco Jabber for Android からログを送信させます。

シスコは、ユーザが Android デバイス上の E メール アプリケーションをセットアップすることをお勧めします。

（注） 問題レポートの送信手順は、ユーザがセットアップ ウィザードを完了しているかどうかによって異なります。

ユーザがセットアップ ウィザードを完了していない場合は、アプリケーションをセットアップする前に Cisco Jabber for Android からログを取得する，（58 ページ）を参照してください。

手順

ステップ 1 Cisco Jabber for Android で、[メニュー（Menu）] > [設定（Settings）] の順にタップします。

ステップ 2 [ヘルプ（Help）] で、[ログの送信（Send Logs）] をタップします。

ステップ 3 [オーディオ エンジン ログ（Audio Engine Logs）] チェックボックスをオンにします。

ステップ 4 [設定ファイル（Configuration Files）] チェックボックスをオンにします。

ステップ 5 [ログの送信（Send Logs）] をタップします。
E メール アプリケーションが開き、新規メッセージが表示されます。このメッセージには、すでに件名が設定され、ログ ファイルも添付されています。

ステップ 6 E メール メッセージの本文に問題の説明を入力し、システム管理者に送信します。

ヒント 問題が再現可能な場合は、[メニュー（Menu）]>[設定（Settings）] の順にタップして詳細ログを有効にします。 次に、[ヘルプ（Help）] で [トラブルシューティング（Troubleshooting）] をタップします。 [詳細ログ（Detailed Logging）] チェックボックスをオンにし、問題を再現してから問題レポートを送信します。

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 [ログの送信（Send Logs）] をタップします。

DART からの Cisco AnyConnect トラブルシューティング データの取得

Cisco AnyConnect Secure Mobility Client のインストール中および接続中に問題が発生した場合は、Diagnostic AnyConnect Reporting Tool（DART）を使用してトラブルシューティング データを収集します。

Cisco AnyConnect クライアントを実行しているデバイス上に DART ツールをインストールする必要があります。インストールした後、DART ウィザードを実行して、デバイス上の Cisco AnyConnect ログを収集したり、ログを電子メールで送信したりできます。 DART によってログ、ステータス、および診断情報が収集され、それを Cisco Technical Assistance Center（TAC）での分析に使用できます。 DART を使用するのに管理者特権は必要ありません。

DART を使用した Cisco AnyConnect Secure Mobility Client のトラブルシューティングについては、メンテナンス ガイド一覧から入手できる、ご使用のリリースに対応した『*Cisco AnyConnect VPN Client Administrator Guide*』の「Using DART to Gather Troubleshooting Information」の項を参照してください。

問題のトラブルシューティング

アップグレードの問題

Cisco Jabber for Android をアップグレードできない

問題 ユーザが、Cisco Jabber for Android Release 8.6.x から Release 9.0(1) にアップグレードできません。

解決法 Cisco Jabber for Android Release 9.0 にアップグレードする場合、ユーザはまず、前のバージョンの製品をデバイスからアンインストールする必要があります。

セットアップの問題

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。

解決法 ダイヤル ルールの COP ファイルを再実行し、変更内容を Cisco Jabber が使用できるようにしてから、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。

Cisco Jabber for Android の登録が失敗する

問題 Cisco Jabber for Android の登録が失敗またはタイムアウトします。

解決法 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、FAQ にあるユーザに関するトラブルシューティングのヒントを確認させます。
- 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。 確認するには、デバイス上のブラウザを使用して Unified CM Administration ポータルに接続してみます。
- 登録がエラー 503 で拒否された場合は、Unified CM の Cisco Dual Mode for Android 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 for Android 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。
- 「確認がタイムアウトしました（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。 エラーを解決するために、すべての Unified CM サーバを再起動してください。
- 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 ページの [設定済みの Wi-Fi ネットワーク（Preset Wi-Fi Networks）] フィールドに、社内の Wi-Fi SSID を入力していることを確認します。 詳しくは、「ユーザデバイスの追加」を参照してください。
- そのユーザのデバイス ページで [Cisco Unified Mobile Communicator の有効化（Enable Cisco Unified 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, （34 ページ）を参照してください。
- ユーザに、社内 Wi-Fi ネットワークにデバイスが接続できるか確認させます。 ネットワークがカスタム Wi-Fi ネットワークの場合、ユーザが [カスタム Wi-Fi ネットワーク（Custom Wi-Fi Networks）] 画面で関連するチェックボックスをオンにしておかないと、Cisco Jabber for Android は登録を試行しません。
- Unified CM の [システム（System）] > [サーバ（Server）] の値が、ドメインなしのホスト名である場合は、Cisco Dual Mode for Android のデバイス ページの [ドメイン名（Domain Name）] フィールドにドメイン名を入力します。

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）

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。

解決法 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。

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します。

解決法 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。

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。

解決法 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。

デバイスの問題

Cisco Jabber 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 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。

解決法 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可能性があります。ユーザが実行できるアクションについては、ユーザ向けの FAQ を参照してください。

Cisco Jabber 登録が頻繁にドロップする

問題 ユーザ デバイスがアイドル状態のときに、Unified CM 登録が頻繁にドロップする。

解決法 [Unified CM の管理（Unified CM Administration）] の SIP プロファイル設定を確認してください。 詳細については、「専用の SIP プロファイルの作成」を参照してください。

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。

解決法 次のことを試してください。

- アプリケーション ダイヤル ルールを変更した場合は、ダイヤル ルール COP ファイルを実行して変更内容を Cisco Jabber から使用可能にしたこと、および TFTP サービスを再起動したことを確認してください。
- 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 Specific Configuration 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。

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。

解決法 Unified CM で、[モバイル ID（Mobile 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、モバイル コネクトとモバイル ID の追加, （27 ページ）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ます。

解決法 社外のネットワークの問題は、Cisco Jabber for Android で制御できるものでもなければ Cisco Jabber for Android に固有のものでもないため、Cisco Technical Assistance Center（TAC）は、このような問題をトラブルシューティングしません。 次のいずれかを試してください。

- ユーザが実行できるアクションについては、ユーザ向けの FAQ を参照してください。
- このような問題が頻繁に発生する場合は、Unified CM Administration の SIP プロファイル設定を確認します。 詳細については、「専用の SIP プロファイルの作成」を参照してください。

- ユーザが会社構内にいるときにこのような問題が頻繁に発生する場合は、Wi-Fi ネットワークが、Cisco Jabber for Android の Release Notes に規定されているネットワーク要件を満たしているか確認します。
- Unified CM Administration ページの設定を変更し、[保存（Save）] をクリックしてから、[設定の適用（Apply Config）] をクリックすると、Cisco Jabber が再登録されます。 このアプリケーションの再登録は 30 秒後に行われます。 Cisco Jabber が再登録されると、アクティブなコールが切断され、アプリケーションが自動的に再起動します。

関連トピック

ユーザ デバイスへの変更, （22 ページ）

音声品質の問題

問題 音声品質が悪い。

解決法 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 に固有のものでもなければ、本製品で制御できるものでもないため、Cisco Technical Assistance 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。

- ユーザが実行できるアクションについては、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、Cisco Jabber for Android の Release Notes にある「“Network Requirements”」の項を参照してください。

モバイル ネットワークから Cisco Jabber にコールを移動できない

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。

解決法 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 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。

解決法 [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, （12 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 Android デバイスがスリープ状態になった後、Cisco Jabber for Android ユーザがコールに応答できない。

解決法 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 7000 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, （12 ページ）を参照してください。

モバイル デバイスにコールを送信できない

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

解決法 次のいずれかを試してください。

- アクティブ コールをモバイル デバイスに転送するときに、ユーザが企業 Wi-Fi ネットワーク内にいることを確認します。 ユーザが企業 Wi-Fi ネットワーク外にいる場合は、Cisco Jabber for Android コールをモバイル ボイス ネットワークに移動するオプションを使用できません。
- 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、[モバイル ID（Mobile 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、[モバイル ID（Mobile 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、企業のコーリング 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。
- 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。

検索の問題

ディレクトリ検索ができない

問題 ディレクトリ検索を利用できません。

解決法 Unified CM のデバイス ページでディレクトリ サーバの IP アドレスを入力しないと、Cisco Jabber for Android は、導入環境にディレクトリ サービスが含まれていないものと見なします。 この情報を入力し、保存してデバイスをリセットし、Cisco Jabber for Android を再起動します。

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。

解決法 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。

解決法 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。

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。

解決法 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。

ボイスメールサーバとの接続が切断

問題 資格情報が期限切れまたは無効であるためにボイスメール サーバとの接続が失われたという通知が表示されますが、パスワードを変更できません。

解決法 ユーザは Cisco Jabber for Android でボイスメール パスワードを変更できません。 この問題を解決するには、Cisco Personal Communications Assistant（PCA）を開いて、パスワードを変更します。 Cisco PCA にアクセスするには、http://<*Cisco Unity Connection server*>/ciscopca を開きます。

SIP ダイジェスト認証の問題

SIP ダイジェスト認証の設定の問題

問題 SIP ダイジェスト認証の資格情報を入力するようにユーザにプロンプトが表示された場合に、Cisco Jabber for Android が任意のテキストを受け入れます。

解決法 設定を検査して、次を確認します。

- ダイジェスト認証を有効にしたカスタム電話セキュリティ プロファイルを作成していること。
- カスタム電話セキュリティ プロファイルを使用するようにデバイス セキュリティ プロファイルを設定していること。

関連トピック

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, （47 ページ）