Cisco Jabber Video for iPad 9.3.4 アドミニストレーション ガイド

初版：2013 年 11 月 21 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

はじめる前に

Cisco Jabber Video for iPad の設定を開始する前に、次の項目を確認します。

Cisco Jabber Video for iPad とは

Cisco Jabber Video for iPad は、インスタント メッセージ（IM）、ビデオ コールや音声コール、社内ディレクトリ検索、プレゼンス ステータス、およびボイスメールを提供する Unified Communications アプリケーションです。 基盤となる技術は次のとおりです。

- Cisco WebEx Messenger
- Cisco Unified Presence
- Cisco Unified Communications Manager
- Cisco TelePresence Video Communication Server
- Cisco Jabber Video for TelePresence（旧称無料 Jabber Video サービス）
- Cisco WebEx TelePresence（旧称有料 Jabber Video サービス）

（注） コールのビデオ品質および音声品質は、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。 ユーザがクライアントを 3G または 4G モバイル データ ネットワーク上で使用している場合、あるいは Cisco AnyConnect Secure Mobility Client などのアプリケーションによる VPN 接続を利用して社外の Wi-Fi ネットワーク上で使用している場合、シスコでは接続に関する問題をトラブルシューティングしません。

（注） Cisco Jabber Video for TelePresence および Cisco WebEx TelePresence サービスには、両方とも **Jabber Video for TelePresence** ログインを使用します。

このマニュアルの使用方法

このマニュアルは、組織固有のテクノロジーがユーザ デバイス上で正しく機能するように、それらのテクノロジーの設定に役立つ情報を提供しています。 次の表を確認して、必要なコンテンツにすばやく移動できます。

設定内容	参照する章
ドメイン ネーム サーバのサービス レコード	DNS SRV を使用した簡易サイン インのセットアップ，（7 ページ）
Cisco WebEx Messenger のみ	Cisco WebEx Messenger の設定，（17 ページ）
Cisco Unified Presence のみ	Cisco Unified Presence の設定，（21 ページ）
Cisco Unified Communications Manager のみ	Cisco Unified Communications Manager 8.x の設定，（39 ページ）
Cisco TelePresence Video Communication Server のみ	Cisco TelePresence Video Communication Server の設定，（95 ページ）
Cisco WebEx Messenger および Cisco Unified Communications Manager	Cisco WebEx Messenger および Cisco Unified Communications Manager の設定
Cisco WebEx Messenger および Cisco TelePresence Video Communication Server	Cisco WebEx Messenger および Cisco TelePresence Video Communication Server の設定
Cisco Unified Presence および Cisco Unified Communications Manager	Cisco Unified Presence および Cisco Unified Communications Manager の設定

（注） ドメイン ネーム サーバのサーバ レコード（DNS SRV）のセットアップは、Cisco Jabber Video for iPad の導入設定で最初の手順にする必要があります。

（注） Cisco Jabber Video for TelePresence および Cisco WebEx TelePresence の管理設定は必要ありません。 ユーザから質問があった場合は、次のサポート サイトに誘導してください。

- https://www.ciscojabbervideo.com/support
- http://telepresence.webex.com

Cisco Jabber Video for iPad のダウンロードとインストール

Cisco Jabber Video for iPad は、iTunes 内または iPad デバイス上で App Store からダウンロードし、インストールできるアプリケーションです。

Connect On Demand VPN

Cisco Jabber Video for iPad には Connect on Demand VPN 機能が含まれています。 Connect on Demand VPN 機能により、アプリケーションでは必要なときに自動的に VPN 接続を確立することができます。エンドユーザによる追加操作は必要ありません。 Connect On Demand VPN 機能を使用するには、ユーザが App Store から Cisco AnyConnect Secure Mobility Client をダウンロードしてインストールする必要があります。

Connect on Demand VPN 機能を Cisco Jabber Video for iPad で提供するためには、Cisco AnyConnect Secure Mobility Client で証明書認証を設定する必要があります。 この設定の情報および手順については、『*Cisco AnyConnect Secure Mobility Client Administrator Guide*』を参照してください。 『*Cisco AnyConnect Secure Mobility Client Administrator Guide*』の最新バージョンは、http://www.cisco.com/en/US/products/ps10884/products_installation_and_configuration_guides_list.html から入手できます:。

特定のネットワーク展開では、追加の Cisco Unified Communications Manager 設定が必要な場合があります。 詳細については、Connect On Demand VPN の設定, （62 ページ）を参照してください。

（注） Cisco Jabber Video for iPad では、Connect on Demand VPN 機能の有効/無効の切り替え以外の設定はありません。 この機能は、アプリケーションがインストールされると、デフォルトでオンになります。

Cisco Jabber Video for iPad の相互起動

Cisco Jabber Video for iPad は Safari などのブラウザから起動して、次のいずれかのタスクを実行できます。

- 電話番号の呼び出し
- チャット セッションの開始
- ビデオ コールの発信

次の表に、サード パーティ アプリケーションが Cisco Jabber Video for iPad の機能を利用するために使用できる相互起動の URL を示します。

機能	相互起動 URL	前提条件
電話番号の呼び出し	ciscotel://<phone_number>	Cisco Unified Communications Manager のアカウント
チャット セッションの開始	xmpp://<instant_message_id>	• Cisco WebEx Messenger のアカウント • Cisco Unified Presence のアカウント
ビデオ コールの発信	• movi://<phone_number> • movi://<URI> • sip://<phone_number> • sip://<URI>	• MOVi の Cisco TelePresence Video Communication Server アカウント: URL • SIP の Cisco Unified Communications Manager または Cisco TelePresence Video Communication Server アカウント: URL
インスタント メッセージの送信	ciscojabber://goim?screenname=<contact_id>& message=<message_tx>	• Cisco WebEx Messenger のアカウント • Cisco Unified Presence のアカウント

機能	相互起動 URL	前提条件
VoIP またはビデオ コールの発信	ciscojabber://call?address=<user_address>&type=<call_type> コール タイプ： • 0：ポイントツーポイント • 1：Cisco Unified Communications Manager • 2：Cisco TelePresence Video Communication Server • 3：Cisco Jabber Video for TelePresence / Cisco WebEx TelePresence • 4：アクティブなアカウントのタイプを判定、そのタイプでコールを発信。 （注） URL が値 1、2、3 を使用し、かつそのアカウント タイプが存在しない場合、その URL は無視されます。	• Cisco Unified Communications Manager のアカウント • Cisco TelePresence Video Communication Server アカウント • Cisco Jabber Video for TelePresence / Cisco WebEx TelePresence アカウント
担当者の追加	ciscojabber://addbuddy?screenname=<user_name>	
プロファイルの表示	ciscojabber://goprofile?screenname=<user_name>	
Cisco Jabber Video for iPad へのサインイン	ciscojabber://login?type=<account_type>&username=<user_name>&token=<login_token>&primaryserver=<primary_login_server>&secondaryserver=<secondary_login_server>&sipdomain=<sip_domain>&devicename=<ucm_device> アカウント タイプ： • 1：Cisco WebEx Messenger • 2：Cisco WebEx Messenger シングル サインオン • 3：Cisco Unified Presence • 4：Cisco Unified Communications Manager • 5：Cisco TelePresence Video Communication Server • 6：Cisco Jabber Video for TelePresence / Cisco WebEx TelePresence	• Cisco WebEx Messenger のアカウント • Cisco Unified Presence のアカウント • Cisco Unified Communications Manager のアカウント • Cisco TelePresence Video Communication Server アカウント • Cisco Jabber Video for TelePresence / Cisco WebEx TelePresence アカウント

Apple iOS のサポートに関する情報

シスコでは、最新のメジャー iOS リリースでのみ Cisco Jabber の各リリースをサポートします。 Apple は iOS を管理し、無料の iOS アップデートを提供し、アクティブにユーザに新しい iOS リリースにアップグレードすることを推奨しています。 企業のお客様が新しいメジャー iOS アップデートに移行しやすくするため、シスコのサポート担当者は、新しいリリースが発表されてから 3 か月間は、前のメジャー リリースの最後のドットのリリースをサポートします。

緊急コールに関する重要な注意事項

iPad を電話として使用すると、911、999、112 などの緊急コールで最新のまたは正確なロケーションデータが提供されない場合があります。 不適切な緊急応答センターにコールが発信されたり、緊急応答センターで正確な位置が把握できない場合があります。 緊急時には、他に連絡手段がない場合にのみ、お使いのデバイスを電話としてご使用ください。 シスコは、発生したエラーまたは遅延の責任を負いません。

第 2 章

DNS SRV を使用した簡易サイン インのセットアップ

ドメイン ネーム サーバのサービス レコード（DNS SRV）を使用して、簡易サイン インをセットアップできます。 DNS SRV によって自動検出メカニズムが追加されるため、多くの配置で手動アカウント設定を行う必要がなくなります。 DNS SRV は、Unified Communications サーバ アドレスを自動的に Cisco Jabber Video for iPad のクライアントに戻すことを可能にする、標準ベースの機能です。 DNS SRV レコードが設定されていない場合、クライアントは手動プロビジョニング ウィザードに戻します。

クライアントと併用する場合、DNS SRV には 2 つの導入モデルがあります。

1 **単一のサービス**

単一サービス導入モデルでは、インスタント メッセージおよびプレゼンス、または Unified Communications が企業ネットワークに導入されます。両方は導入されません。 これは、Cisco WebEx Messenger または Cisco Unified Presence だけが、インスタント メッセージおよびプレゼンスのために導入されるか、Cisco Unified Communications または Cisco TelePresence Video Communication Server がビデオ コールおよび音声コールのために導入されることを意味する場合があります。 1 つのサービスだけが導入される場合、管理者はサービスと DNS SRV マッピング テーブルに従って DNS SRV レコードを設定する必要があります。 単一のサービスに複数のサーバを導入することを予定している場合、管理者は複数のレコードを追加する必要があります。 各レコードには、適切なプライオリティおよび重み付けの情報を含める必要があります。 DNS SRV レコードのポート番号はクライアントによって使用されませんが、デフォルト値に設定する必要があります。

クライアントは、DNS SRV レコードで検出したプライオリティと重み付けに基づいてサーバ リストを生成します。 クライアントはこのサーバ リストを順に参照して各サーバへの接続を試み、到達可能なサーバへの接続が確立されたときに停止します。 クライアントは、当該サーバへの認証が成功したかどうかに関係なく、停止します。

2 **複数のサービス**

複数サービスの導入は、インスタント メッセージおよびプレゼンスと Unified Communications サービスの組み合わせで構成されます。 管理者はサービスと DNS SRV マッピング テーブルに従って DNS SRV レコードを設定する必要があります。 Unified Communications サービスと

インスタント メッセージおよびプレゼンス サービスを統合する場合は、管理者は Cisco WebEx Messenger または Cisco Unified Presence での Unified Communications の統合を有効にする必要があります。ユーザがインスタント メッセージおよびプレゼンスのアカウントにサインインした後、クライアントは自動的に Unified Communication のアカウントにサイン インしません。 任意の単一のサービスに複数のサーバを導入することを予定している場合、管理者は複数のレコードを追加する必要があります。 各レコードには、適切なプライオリティおよび重み付けの情報を含める必要があります。 DNS SRV レコードのポート番号はクライアントによって使用されませんが、デフォルト値に設定する必要があります。

クライアントには DNS TXT レコードによってカスタマイズできるサービス プライオリティ リストが含まれます。 これらのレコードの設定の詳細については、検出および自動設定のカスタマイズ，（13 ページ）を参照してください。 クライアントは、各サービスの最初のサーバに接続を試行します。 そのサービスに接続できない場合は、同じサービスの次のサーバが試行されます。 サーバで認証されない場合は、当該サービスのその他のサーバを無視し、次のサービスの最初のサーバにサイン インを試みます。 検出したすべてのサーバで認証に失敗した場合は、エンド ユーザにエラー メッセージが表示されます。

クライアントは正常に接続できたサーバを記憶し、アプリケーションの次回起動時にそれらに対して認証を試みます。 認証が失敗した場合、クライアントは自動的にサービス検出を実行し、現在のクレデンシャルでサイン インします。

シスコでは、管理者が集中型 TFTP サーバをセット アップして複数クラスタの Cisco Unified Communications Manager 導入に対してのみ DNS SRV を有効にするよう要求しています。 詳細については、集中型 TFTP サーバのセットアップ，（12 ページ）を参照してください。

この項では、この機能と、企業でのクライアントの導入に際しての設定方法について説明します。

（注） ここで示す手順はこの機能に特化しています。 サービス導入には、他のセクションに記述した他の手順も必要です。 どのセクションが特定の導入に該当するかについては、このマニュアルの使用方法，（2 ページ）を参照してください。

クライアントのログインおよび自動検出

クライアントの初回起動時、ドメイン ネーム サーバ（DNS）が照会されます。 ユーザが自分のアカウント（username@example.com）を入力すると、クライアントが指定されたアカウントのドメイン部分に対応する DNS SRV レコードを照会します（この場合、*example.com*）。 クライアントはDNSサーバからの応答を予期し、その応答によってクライアントは設定作業を完了し、サービスがユーザに提供されます。 指定されたアカウントは、電子メール アドレスまたは <*username*>@<*domain*> 形式を使用する他のクレデンシャルである場合があります。 システム管理者は、ユーザが Cisco Jabber Video for iPad にログインするときに必要なクレデンシャルを認識できるようにする必要があります。

管理者は、企業が実装したサービスのタイプごとに新しい DNS SRV レコードを作成します。 クライアントでは次のサービスがサポートされています。

- **インスタント メッセージおよびプレゼンス**
  - Cisco Unified Communications Manager のインスタント メッセージとプレゼンス（旧 Cisco Unified Presence）
  - Cisco WebEx Messenger（旧 Cisco WebEx Connect）
- **Unified Communications**
  - Cisco Unified Communications Manager
  - Cisco TelePresence Video Communication Server
  - Cisco Jabber Video for TelePresence
  - Cisco WebEx TelePresence

インスタント メッセージおよびプレゼンスと Unified Communications サービス（Cisco WebEx Messenger および Cisco Unified Communications Manager など）が配置されると、クライアントは DNS SRV レコードを使用して提供された Unified Communication サーバではなく、インスタント メッセージングおよびプレゼンス サービス（Cisco WebEx Messenger または Cisco Unified Presence）で設定された Unified Communications サーバを使用します。

DNS SRV レコード

DNS SRV レコードはクライアント固有のドメインで利用可能なサービスに関する情報を提供します。 クライアントはサーバを選択し、それを使用して、展開したサービスまたはサーバに接続します。 ここでは、DNS SRV レコードの形式とフォーマットについて説明します。 DNS SRV レコードに関するその他の技術情報については、RFC 2782 を参照してください。

クライアントはネットワーク上で、ユーザ指定の電子メール アドレスのドメイン部分に対応する、想定されるすべてのサービスを照会します。 次に、DNS SRV レコードの結果によって検出されたサービスに基づいて接続を試みます。 複数のサービスが検出された場合、クライアントは次の順序でサービスに接続します。

1. Cisco WebEx Messenger
2. Cisco Unified Presence
3. Cisco Unified Communications Manager
4. Cisco TelePresence Video Communication Server
5. Cisco Jabber Video for TelePresence
6. Cisco WebEx TelePresence

管理者は、このデフォルトの順序をオーバーライドできます。 変更の詳細については、検出および自動設定のカスタマイズ, （13 ページ）を参照してください。

DNS SRV レコードのセット アップ

DNS レコードは、サーバ名をネットワーク環境の単一の IP アドレスと照合する一連のエントリで構成されます。 DNS SRV レコードはこれとは異なり、サービスをネットワーク環境の単一のサーバまたは一連のサーバと照合します。 このため、DNS SRV によってクライアントは実際のサーバではなく、求めているサービス タイプを認識しているだけで済みます。 これにより、ほとんどのネットワーク環境には特定のサービスのニーズに合わせて負荷分散された複数のサーバがあるため、配置、サーバ管理、サービス フェイルオーバーが容易になります。

複数のサーバが 1 つのサービス用に設定されている場合、クライアントは、最初のエントリに接続できない場合、次のサーバに接続を試みます。 指定したサービスへの認証に失敗した場合、クライアントはこのサービスに接続を試みるのを中止し、エラー メッセージを表示します。

次の表では、クライアントの DNS SRV レコードのタイプを示します。

サービス	DNS SRV レコード
Cisco WebEx Messenger	`_xmpp-client._tcp`
Cisco Unified Presence	`_cuplogin._tcp`
Cisco Unified Communications Manager TFTP	`_cisco-phone-tftp._tcp`
Cisco Unified Communications Manager CCMCIP	`_cisco-phone-http._tcp`
Cisco TelePresence Video Communication Server（内部）	`_sip._tcp.internal`
Cisco TelePresence Video Communication Server（外部）	`_sip._tcp.external`
Cisco Jabber Video for TelePresence	`_ciscowtp._tcp`
Cisco WebEx TelePresence	`_ciscowtp._tcp`

次の表では、このマニュアルで説明する導入モデルで使用されている DNS SRV レコードの完全な例を示します。

展開モデル	完全な DNS SRV レコードの例
Cisco WebEx Messenger Cisco WebEx Messenger および Cisco Unified Communications Manager Cisco WebEx Messenger および Cisco TelePresence Video Communication Server Cisco WebEx Messenger および Cisco Jabber Video for TelePresence	`_xmpp-client._tcp.example.com SRV 0 5222 c2s.example.com.webexconnect.com`
Cisco Unified Presence Cisco Unified Presence および Cisco Unified Communications Manager	`_cuplogin._tcp.example.com SRV 0 1 8443 cup.example.com`
Cisco Unified Communications Manager	`_cisco-phone-tftp._tcp.example.com SRV 0 0 69 cucm.example.com` `_cisco-phone-http._tcp.example.com SRV 0 0 80 cucm.example.com`
Cisco TelePresence Video Communication Server	`_sip._tcp.internal.example.com SRV 0 0 5060 vcsc.example.com` `_sip._tcp.external.example.com SRV 0 0 5060 vcse.example.com`
Cisco Jabber Video for TelePresence	`_ciscowtp._tcp.jabber.com SRV 0 0 443 boot.ciscojabbervideo.com`
Cisco WebEx TelePresence	`_ciscowtp._tcp.webex.com SRV 0 0 443 boot.telepresence.webex.com`

（注） 管理者は、Cisco Jabber Video for TelePresence や Cisco WebEx TelePresence 用に DNS SRV レコードを設定する必要はありません。 それらはすでに設定されており、インターネット経由で入手可能です。

次に、クライアントが使用する Cisco Unified Presence サーバ アドレスを提供することにより検出要求に応答する、単一の DNS SRV レコードの例を示します。

```
_cuplogin._tcp.example.com SRV 0 1 8443 cup.example.com
```

（注） SRV レコードで提供されるポート番号は、クライアントでは使用されません。 ただし、レコードは提供されたデフォルト値に設定する必要があります。

（注） 重み付けおよびプライオリティは、同じ DNS SRV レコード タイプにおいてサポートされます。 重み付けは、同じプライオリティを持つ SRV レコードに対してのみ適用されます。

この例では、クライアントは想定されるすべてのサービスをネットワークで照会し、定義済みの Cisco Unified Presence サーバの応答を取得します。 これにより、クライアントが他のサービスのクレデンシャルではなく Cisco Unified Presence のクレデンシャルとして提供されたクレデンシャルを使用してこのサーバに接続するように指示します。

次の一般的な手順を使用して、新しい DNS SRV レコードを作成します。

手順

ステップ 1 提供されるネットワーク サービスで情報を編集します。
ステップ 2 複数のサーバの場合は、各サーバに割り当てる重み付けおよびプライオリティを設定します。
ステップ 3 新しい DNS SRV レコードを作成します。
ステップ 4 新しいレコードをネットワークの DNS 設定に配置します。

集中型 TFTP サーバのセットアップ

同じ企業ドメインに複数の Cisco Unified Communications Manager クラスタがある場合は、集中型 TFTP サーバをセットアップします。 また、このサーバが検出できるように、DNS SRV レコードを追加する必要があります。 次に、そのようなレコードが示される例を示します。 レコードの項目は次の順序で表示されます。

- SRV レコード
- プライオリティ
- 重み付け
- ポート
- A レコード

```
cisco-phone-tftp._tcp.example.com 0 0 69 cftp.example.com
```

集中型 TFTP サーバを示すために、`cisco-phone-tftp` レコード タイプが使用されます。 この例では、クライアントがサーバ `ctftp.example.com` を検出し、デバイス設定を直接ダウンロードできるようにします。

（注） デバイスおよびデバイス コンフィギュレーション ファイルについては、次の事項に注意してください。

- すべてのデバイス名に適格性がある必要があります。 デバイス名の最初の 3 文字は **TAB** であり、その後にデバイスに関連付けられたユーザのユーザ名を続ける必要があります。 John Smith のユーザ名が **jsmith** である場合、適切なデバイス名の例は **TABJSMITH** です。 このデバイス名の全体の長さが 15 文字を超えることはできません。
- シスコでは、管理者がすべてのクラスタのタブレット デバイスごとに SIP 認証を有効にすることを強く推奨します。
- 集中型 TFTP サーバが検出されるようにするため、管理者は企業ドメインに **cisco-phone-http** レコードを追加してはなりません。

検出および自動設定のカスタマイズ

デフォルトのサービス検出順序は次のとおりです。

1. Cisco WebEx Messenger
2. Cisco Unified Presence
3. Cisco Unified Communications Manager
4. Cisco TelePresence Video Communication Server
5. Cisco Jabber Video for TelePresence

システム管理者は DNS TXT レコードを使用してサービス検出のプライオリティをカスタマイズできます。 サービス検出のプライオリティのカスタマイズは、複数のサービスを提供するネットワーク環境で必要になる場合があります。 DNS TXT レコードは RFC 1035 で定義されています。 DNS TXT の使用例は、RFC 4408（Sender Policy Framework）および RFC 5672（DomainKeys Identified Mail）で確認できます。

DNS TXT レコードを配置してサービスのプライオリティをカスタマイズしている管理者は、Jabber Simple Configuration Priority（JSCP）レコードと呼ばれる、典型的なレコードのカスタム フォームを使用する必要があります。 典型的な DNS TXT レコードは次の形式になります。

```
name ttl class TXT text
```

Jabber Simple Configuration Priority レコードはこれとは少し異なります。

```
name ttl class TXT JSCP-specific-text
```

`JSCP-specific-text` パラメータによってカスタム サービスのプライオリティが定義されます。 このパラメータには引用符付きのテキストが次の形式で含まれます。

```
"v=jscpv1 <dns-srv-name>; <dns-srv-name>; ..."
```

各サービスは、DNS SRV レコードで定義されたコードを使用して定義されます。プライオリティは、サービス リストでの表示位置に応じてサービスに割り当てられます。 リストの最初にあるサービスのプライオリティが最も高く、後ろのエントリほどプライオリティが低くなります。

（注） Cisco WebEx Messenger の導入でシングル サインオン（SSO）を使用する場合、Cisco WebEx Messenger サービスは、リストの最初のサービスである必要があります。

DNS TXT レコードを使用してサービスのプライオリティをカスタマイズする場合は、次のようになります。

- DNS TXT レコードのプライオリティは、常にデフォルトのプライオリティ リストよりも優先されます。
- DNS TXT レコードの DNS SRV 名は、追加レコードが存在する場合でもクライアントによって認識されます。
- 対応する DNS SRV レコードがない DNS SRV 名は無視され、エラーは出力されません。
- DNS TXT レコードに誤った形式が使用されているか空である場合、デフォルトのプライオリティ リストが使用され、エラーがログに記録されます。
- DNS TXT レコードがない場合、デフォルトのプライオリティ リストが使用されます。

次に、DNS SRV レコードを含み、JSCP 形式のレコードを使用する DNS TXT レコードの例を示します。

```
; UC DNS SRV records

_xmpp-client._tcp.example.com 86400 IN SRV 0 5 5222 xmppserver.example.com

_cisco-phone-tftp._tcp.example.com 86400 IN SRV 0 5 6970 cucm8xserver.example.com

_sip._tcp.internal.example.com 86400 IN SRV 0 5 5060 sipserver.example.com

; JSCP TXT RR example - WebEx Messenger サービスを無視し、CUCM サービス上の集中型 tftp での VCS サービスを優先

cisco.com 30 IN TXT "v=jscpv1 _sip._tcp.internal.example.com;
_cisco-phone-tftp._tcp.example.com; "

cisco.com 30 IN TXT "v=jscpv1 _cisco-phone-tftp._tcp.example.com"
```

この例は、クライアントが Cisco WebEx Messenger サービスを無視し、Cisco Unified Communications Manager サービス上の集中型 TFTP を伴う Cisco Telepresence Video Communications Server サービスを優先するように構築されています。

これらの一般的な手順に従って、新しい DNS SRV レコードおよび DNS TXT レコードを作成してください。

手順

ステップ 1 提供されるネットワーク サービスで情報を編集します。
ステップ 2 複数のサーバの場合は、各サーバに割り当てる重み付けおよびプライオリティを設定します。
ステップ 3 サービス検出の順序を決定します。
ステップ 4 新しい DNS SRV レコードを作成します。
ステップ 5 ステップ 3 に基づいて、DNS TXT レコードを作成します。
ステップ 6 ネットワーク内の DNS サーバに新しい DNS SRV レコードと DNS TXT レコードを配置します。

トラブルシューティング

トラブルシューティングの際、次の情報を使用します。

- ネットワーク接続デバイスから DNS 設定のトラブルシューティングを行います。 Microsoft Windows 環境でコマンド プロンプトから `NSLOOKUP` コマンドを使用します。 このコマンドの詳細については、http://support.microsoft.com/kb/816587 を参照してください。
- [設定（Settings）] > [ヘルプ（Help）] > [サービス検出（Service Discovery）]を選択して、手動サービス検出を実行します。 手動サービス検出は、システム管理者が指導してください。手動サービス検出を実行すると、現在のクライアントのアカウントからログアウトし、サービス検出を実行し、自動的に現在のユーザ クレデンシャルを使用して、検出されたサービスにログインします。

（注） 手動サービス検出を実行する前に、システム管理者に連絡してください。サービス検出を実行すると現在のアカウントからログアウトするため、既存のアカウント設定が削除される可能性があります。

第 3 章

Cisco WebEx Messenger の設定

Cisco WebEx Messenger Administration Tool を使用することにより、クラウド環境で Cisco Jabber Video for iPad を設定できます。 このツールの使用方法については、http://www.webex.com/webexconnect/orgadmin/help/index.htm にある『Cisco WebEx Messenger Administration Guide』を参照してください。

このマニュアルの PDF をダウンロードすることもできます。

Cisco WebEx Messenger Administration Tool を使用した設定

Cisco WebEx Messenger Administration Tool により、インスタント メッセージ（IM）、プレゼンス ステータス、および Cisco Unified Communications Manager との統合の設定を指定することができます。 このツールの使用方法については、http://www.webex.com/webexconnect/orgadmin/help/index.htm にある『Cisco WebEx Messenger Administration Guide』を参照してください。

次の順序でタスクを実行することを推奨します。

（注） このリストは各タスクの概略を示したものであり、設定の詳細がすべて含まれているとは限りません。 詳細については、個々のリンクを参照してください。

ユーザがすでにデスクトップ アプリケーションで Cisco WebEx Messenger と Cisco Unified Communications Manager を両方とも設定している場合、その設定は自動的に Cisco Jabber Video for iPad で有効になります。

手順

ステップ 1 組織情報を指定します。
http://www.webex.com/webexconnect/orgadmin/help/index.htm?toc.htm?17382.htm に進みます。

ステップ 2 ユーザを作成し、プロビジョニングします。
http://www.webex.com/webexconnect/orgadmin/help/index.htm?toc.htm?cs_user.htm に進みます。

ステップ 3 IM およびプレゼンス ステータスを設定します。
http://www.webex.com/webexconnect/orgadmin/help/index.htm?toc.htm?17169.htm に進みます。

ステップ 4 テレフォニー サービスを設定します。
http://www.webex.com/webexconnect/orgadmin/help/index.htm?toc.htm?18648.htm に進みます。

（注） シスコでは、テレフォニー サービスを設定する場合に、完全修飾ドメイン名（FQDN）で Cisco Unified Communications Manager を展開することを推奨します。 テレフォニー サービスを設定するときに、IP アドレスで Cisco Unified Communications Manager を展開する場合、Connect On Demand VPN 機能をイネーブルにするには追加設定が必要です。FQDN の使用の詳細については、該当する Cisco Unified Communications Manager のマニュアルを参照してください。

ステップ 5 ボイスメールを設定します。
http://www.webex.com/webexconnect/orgadmin/help/index.htm?toc.htm?cs_visual_voicemail.htm に進みます。

（注） ボイスメールのパラメータが Cisco WebEx Messenger Administration Tool と Cisco Unified Communications Manager の製品固有の設定の両方で設定されている場合、Cisco Jabber Video for iPad は Cisco Unified Communications Manager の設定を使用し、Cisco WebEx Messenger Administration Tool のボイスメール設定を無視します。

ステップ 6 会議を設定します。
http://www.webex.com/webexconnect/orgadmin/help/index.htm?toc.htm?17386.htm に進みます。

組み合わせ導入時の Cisco Unified Communications Manager の設定

Cisco WebEx Messenger と Cisco Unified Communications Manager を組み合わせて導入する場合、Cisco Unified Communications Manager の設定には、Cisco Unified Communications Manager のみの導入に関する章で説明しているのと同じ手順を使用します。 「Cisco Unified Communications Manager 9.x の設定」を参照してください。

組み合わせ導入時の VCS の設定

Cisco WebEx Messenger と VCS を組み合わせて導入する場合、Cisco TelePresence Video Communication Server（VCS）の設定には、VCS のみの導入に関する章で説明しているのと同じ手順を使用します。「Cisco TelePresence Video Communication Server の設定」を参照してください。

第 4 章

Cisco Unified Presence の設定

この章では、Cisco Unified Presence を使用した Cisco Jabber Video for iPad の設定方法について説明します。

必須サービスの起動

すべてのクラスタ内のすべての Cisco Unified Presence ノード上で次の Cisco Unified Presence Extensible Communication Platform（XCP）サービスを起動します。

- Cisco Unified Presence XCP Authentication Service
- Cisco Unified Presence XCP Connection Manager

また、使用可能にする機能に応じて次の Unified Presence XCP サービスもすべてのクラスタ内のすべての Unified Presence ノード上で起動します。

- Cisco Unified Presence XCP Text Conference Manager（グループ チャット用）
- Cisco Unified Presence XCP SIP Federation Connection Manager（SIP を使用するサードパーティ製アプリケーションとのフェデレーション サービスをサポートする場合）

- Cisco Unified Presence XCP XMPP Federation Connection Manager（XMPP を使用するサードパーティ製アプリケーションとのフェデレーション サービスをサポートする場合）
- Cisco Unified Presence XCP Counter Aggregator（システム管理者が XMPP コンポーネントに関する統計データを表示できるようにする場合）
- Cisco Unified Presence XCP Message Archiver（すべてのインスタント メッセージを自動アーカイブする場合）

（注） 関連サービスを有効にする前に、設定中の各機能のマニュアルをお読みください。 追加の作業が必要な場合があります。

ファイアウォールの要件

ポートがアプリケーションのトラフィックを伝送するようにハードウェア ファイアウォールを設定します。ハードウェアファイアウォールは、望まないトラフィックからの保護を組織レベルで実現するネットワーク デバイスです。 次の表に、Cisco Unified Communications Manager と Cisco Unified Presence の導入に必要なポートを示します。 これらのポートは、アプリケーションが正常に機能するために、すべてのファイアウォール上で開いておく必要があります。

ポート	プロトコル	説明
着信		
16384 ～ 32766	UDP	ビデオおよびオーディオ用の Real-Time Transport Protocol（RTP）メディア ストリームを受信します。 これらのポートは、Cisco Unified Communications Manager で設定します。
発信		
69	TFTP	Trivial File Transfer Protocol（TFTP）ファイルをダウンロードするために TFTP サーバに接続します

ポート	プロトコル	説明
80 および 6970	HTTP	会議用の Cisco WebEx Messenger やボイスメール機能用の Cisco Unity Connection などのサービスに接続します TFTP サーバアドレスにポートが指定されていない場合、Cisco Jabber for iPad は、ポート 6970 を使用して、電話設定ファイルとダイヤル ルール ファイルを取得しようとします。
5060	UDP/TCP	Session Initiation Protocol（SIP）コール シグナリングを提供します
5061	TCP	セキュアな SIP コール シグナリングを提供します
8443	TCP	Cisco Unified Communications Manager IP Phone（CCMCIP）サーバに接続し、現在割り当てられているデバイスのリストを取得します
16384 ～ 32766	UDP	UDP でビデオとオーディオの RTP メディア ストリームを送信します
389	TCP	連絡先を検索するために LDAP サーバに接続します
443 7080	VMRest HTTPS	Cisco Unity Connection に接続して、ボイス メッセージの取得と管理を行います
8443	HTTPS	Cisco Unified Communications Manager で連絡先を検索するために User Data Services（UDS）に接続します
636	LDAPS	連絡先を検索するためにセキュア LDAP サーバに接続します

ディレクトリ検索、IM、およびプレゼンスステータスの設定

以下のトピックを確認して、IM とプレゼンス ステータスを設定します。

はじめる前に

管理者は、Cisco Unified Presence 8.5 以上を使用する場合 **JABBERIPAD** クライアント タイプを設定する必要があります。 Cisco Unified Presence のメニューから [Cisco Unified Presence の管理（Cisco Unified Presence Administration）]>[アプリケーション（Application）]>[クライアントタイプ（Client Types）] を選択し、**JABBERIPAD** が含まれていることを確認します。 このオプションが使用可能でない場合、補足説明 CSCtq15767 の回避策一覧を参照してください。

LDAP サーバの設定

Cisco Unified Presence で次のタスクを実行します。

はじめる前に

次の手順を実行します。

- LDAP 属性マップの設定
- LDAP ディレクトリのホスト名または IP アドレスを取得します。

手順

ステップ 1 [Cisco Unified Presence の管理（Cisco Unified Presence Administration）] > [アプリケーション（Application）] > [Cisco Unified Personal Communicator] > [LDAP サーバ（LDAP Server）] を選択します。

（注） LDAP サーバの設定は、リリース 9.0 以降の Cisco Unified Communications Manager で実行します。

ステップ 2 [新規追加（Add New）] を選択します。

ステップ 3 LDAP サーバ名を入力します。

ステップ 4 LDAP サーバの IP アドレスまたは FQDN（完全修飾ドメイン名）を入力します。

ステップ 5 LDAP サーバが使用するポート番号を指定します。 デフォルトは、次のとおりです。

- TCP：389
- TLS：636

この情報については、LDAP ディレクトリのマニュアルまたは LDAP ディレクトリの設定を確認してください。

ステップ 6 プロトコル タイプに [TCP] または [TLS] を選択します。

ステップ 7 [保存（Save）] を選択します。

LDAP プロファイルの作成およびユーザの追加

Cisco Jabber Video for iPad は、検索のたびに LDAP サーバに接続します。 プライマリ サーバへの接続が失敗した場合、アプリケーションは最初のバックアップ LDAP サーバへの接続を試みます。それが使用できない場合は、2 番目のバックアップ サーバを試します。 また、アプリケーションは定期的にプライマリ LDAP サーバに復帰しようとします。 システムのフェールオーバー中に処理中の LDAP クエリーがあると、その LDAP クエリーは次に使用可能なサーバで完了します。

はじめる前に

次の手順を実行します。

- LDAP サーバ名およびアドレスを指定します。
- Cisco Jabber Video for iPad ユーザをプロファイルに追加するには、まず LDAP プロファイルを作成する必要があります。

手順

ステップ 1 [Cisco Unified Presence の管理（Cisco Unified Presence Administration）] > [アプリケーション（Application）] > [Cisco Unified Personal Communicator] > [LDAP プロファイル（LDAP Profile）] を選択します。

（注） LDAP プロファイルの設定は、リリース 9.0 以降の Cisco Unified Communications Manager で実行します。

ステップ 2 [新規追加（Add New）] を選択します。

ステップ 3 フィールドに情報を入力します。

フィールド	設定
名前（Name）	プロファイル名を 128 文字内で入力します。
説明（Description）	これはオプションです。 説明を 128 文字内で入力します。
バインド識別名（Bind Distinguished Name）	これはオプションです。 管理者レベルのアカウント情報を 128 文字内で入力します。 これは、バインドの認証のためにバインドしている識別名です。 このフィールドの構文は、展開する LDAP サーバのタイプによって異なります。 詳細については、LDAP サーバのドキュメンテーションを参照してください。

フィールド	設定
匿名バインド（Anonymous Bind）	これはオプションです。 ユーザ クレデンシャルを使用してこのLDAPサーバにサインインするには、このオプションをオフにします。 Anonymous以外のバインド操作の場合、Cisco Jabber Video for iPadは一組の資格情報を受け取ります。 設定している場合、これらのクレデンシャルは、バックアップLDAPサーバで有効にする必要があります。 （注） [匿名バインド（Anonymous Bind）] をオンにすると、ユーザはこのLDAPサーバに読み取り専用アクセスで匿名ログインできます。 匿名アクセスは、ディレクトリ サーバで許可しても構いませんが、推奨しません。 その代わりに、検索対象のユーザが配置されているのと同じディレクトリに対して読み取り専用権限を持つユーザを作成します。 アプリケーションが使用できるように、Cisco Unified Presenceにディレクトリ番号およびパスワードを指定します。
パスワード（Password）	これはオプションです。 LDAP バインドのパスワードを 128 文字内で入力します。 これは、ユーザにこのLDAPサーバへのアクセスを許可する [バインド識別名（Bind Distinguished Name）] フィールドに指定した管理者レベルのアカウントのパスワードです。
パスワードの確認（Confirm Password）	[パスワード（Password）] に入力したパスワードを再入力します。
検索コンテキスト（Search Context）	これはオプションです。 LDAPユーザ全員が設定されている場所を入力します。 この場所はコンテナまたはディレクトリです。 その名前を256文字内で入力します。 1つのOU/LDAP検索コンテキストだけを使用します。
再帰検索（Recursive Search）	これはオプションです。 検索ベースから始まるディレクトリの再帰検索を実行するにはオンにします。
[プライマリ LDAP サーバ（Primary LDAP Server）] および [バックアップ LDAP サーバ（Backup LDAP Server）]	プライマリ LDAP サーバおよびオプションのバックアップ サーバを選択します。

フィールド	設定
プロファイルにユーザを追加（Add Users to Profile）	[ユーザの検索/一覧表示（Find and List Users）] ウィンドウを終了するには、このボタンを選択します。 [検索（Find）] を選択して検索結果フィールドに値を入力します。 または、特定のユーザを検索してから [検索（Find）] をクリックします。 ユーザをこのプロファイルに追加するには、ユーザを選択し、[選択項目の追加（Add Selected）] を選択します。

ステップ 4 [保存（Save）] を選択します。

LDAP 属性マップの設定

はじめる前に

使用中の環境の LDAP 属性を入力し、所定の Cisco Jabber Video for iPad 属性にマップする、Cisco Unified Presence 上の LDAP 属性を設定します。

従業員のプロファイル写真を保存するために LDAP を使用する場合は、LDAP サーバに写真ファイルをアップロードするためのサードパーティ拡張を使用するか、他の手段で LDAP ディレクトリ サーバ スキーマを拡張して LDAP サーバが画像に関連付けることができる属性を作成します。

Cisco Jabber Video for iPad の場合、プロファイル写真を表示するには、LDAP 属性マップで、[写真（Photo）] の値を適切な LDAP 属性にマップします。

（注）
- 連絡先の写真は、Cisco Jabber Video for iPad で表示されたときにクロップされる場合があります。
- LDAP 属性マップの UPC UserID 設定は、Cisco Unified Communications Manager ユーザ ID と一致する必要があります。 このマッピングにより、ユーザは LDAP から Cisco Jabber Video for iPad の連絡先リストに連絡先を追加できます。 このフィールドは、LDAP ユーザを Cisco Unified Communications Manager および Cisco Unified Presence 上の対応するユーザと関連付けます。
- LDAP フィールドは、ただ 1 つのフィールドにだけマッピングできます。

手順

ステップ 1 [Cisco Unified Presence の管理（Cisco Unified Presence Administration）] > [アプリケーション（Application）] > [Cisco Unified Personal Communicator] > [設定（Settings）] を選択します。

リリース 9.0 を使用する場合は、[Cisco Unified CM IM/Presence（Cisco Unified CM IM and Presence）] >[アプリケーション（Application）]>[レガシー クライアント（Legacy Clients）]>[設定（Settings）] を選択します。

ステップ 2 [ディレクトリ サーバのタイプ（Directory Server Type）] からサポート対象の LDAP サーバを選択します。
LDAP サーバは、LDAP 属性マップに Cisco Jabber ユーザ フィールドおよび LDAP ユーザ フィールドを入力します。

ステップ 3 必要に応じて、特定の LDAP ディレクトリと一致するように LDAP フィールドに変更を加えます。
値はどの LDAP サーバ ホストにも共通になります。 次の LDAP ディレクトリ製品マッピングに注意してください。

製品	LastName マッピング	UserID マッピング
Microsoft Active Directory	SN	sAMAccountName
OpenLDAP	SN	uid

ステップ 4 [保存（Save）] を選択します。
ヒント 現在の属性マッピングを使用するのを止めて、工場出荷時のデフォルト設定を使用するには、[デフォルトに戻す（Restore Defaults）] を選択します。

Active Directory 属性のインデックス作成

次の Active Directory 属性のインデックスを作成します。

- sAMAccountName
- displayName
- mail
- msRTCSIP-PrimaryUserAddress

さらに、連絡先解決に使用される属性のインデックスも作成します。 たとえば、次の属性のインデックスを作成しなければならない場合があります。

- telephoneNumber
- 連絡先を見つけるために使用されるその他のディレクトリ電話番号属性（DisableSecondaryNumberLookups キーの値に依存）
- ipPhone（この属性が環境内で使用されている場合）

IM ポリシーのオン/オフ

この手順では、Cisco Unified Presence クラスタ内のすべての IM アプリケーションの IM 機能をオンまたはオフにする方法について説明します。 Cisco Unified Presence で IM 機能はデフォルトでオンになります。

注意 Cisco Unified Presence で IM 機能をオフにした場合、すべてのグループ チャット機能（アドホックおよび永続的なチャット）は Cisco Unified Presence で機能しません。 Cisco UP XCP Text Conference サービスをオンにしない、または Cisco Unified Presence での永続的なチャット用に外部データベースを設定することを推奨します。

手順

ステップ 1 [Cisco Unified Presence の管理（Cisco Unified Presence Administration）] > [メッセージング（Messaging）] > [設定（Settings）] を選択します。

ステップ 2 [インスタントメッセージを有効にする（Enable instant messaging）] を選択します。

（注）
- この設定をオンにした場合、ユーザは IM を送受信できます。
- この設定をオフにした場合、ユーザはIMを送受信できません。ユーザはプレゼンス ステータスおよび電話操作についてのみ IM を使用できます。

ステップ 3 [保存（Save）] を選択します。

ステップ 4 Cisco UP XCP Router サービスを再起動します。

IM ポリシー設定の指定

次の手順に従って IM ポリシー設定を指定できます。

手順

ステップ 1 [Cisco Unified Presence の管理（Cisco Unified Presence Administration）] > [プレゼンス（Presence）] > [設定（Settings）] を選択します。

ステップ 2 プレゼンス ステータスを表示するには、自動許可をオンまたはオフにします。

項目	手順
ローカル企業内のユーザから受信するすべてのプレゼンス ステータス登録を Unified Presence が自動的に許可するようにするには、自動許可をオンにします。	[確認プロンプトなしで、ユーザが他のユーザのプレゼンス ステータスを表示できるようにする（Allow users to view the availability of other users without being prompted for approval）] をオンにします。
登録の許可または拒否のプロンプトのユーザへの表示先に Unified Presence がすべてのプレゼンス ステータス登録を送信するようにするには、自動許可をオフにします。	[確認プロンプトなしで、ユーザが他のユーザのプレゼンス ステータスを表示できるようにする（Allow users to view the availability of other users without being prompted for approval）] をオフにします。

ステップ 3 [Cisco Unified Presence の管理（Cisco Unified Presence Administration）] > [メッセージング（Messaging）] > [設定（Settings）] を選択します。

ステップ 4 これらのグローバル設定をオンまたはオフにします。

項目	手順
インスタント メッセージング サービスをグローバルにオフにする	[インスタント メッセージを有効にする（Enable instant messaging）] をオフにします。
オフライン インスタント メッセージングをグローバルにオンにする	[オフライン中の相手へのインスタント メッセージの送信を無効にする（Suppress Offline Instant Messaging）] をオフにします。

ステップ 5 [保存（Save）] を選択します。

ステップ 6 Cisco UP XCP Router サービスを再起動します。

Web サーバから連絡先画像をフェッチするための URL 文字列の設定

Cisco Jabber Video for iPad が LDAP サーバではなく Web サーバから画像をフェッチできるように、LDAP 属性マップの [写真（Photo）] フィールドにパラメータ化された URL 文字列を設定できます。 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。 シスコは、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。

置換文字列として `%%<userID>%%` を使用することを推奨します。 例：

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

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 Video for iPad 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 クエリーの結果に置き換えます。

たとえば、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 Video for iPad は画像をフェッチしようとします。

この置換技術が機能するのは、Cisco Jabber Video for iPad がクエリー結果を使用でき、それを前記のテンプレートに挿入して、JPG 画像をフェッチする有効な 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。

（注）
- URL の長さは 50 文字に制限されます。
- Cisco Jabber Video for iPad は、このクエリに対する認証をサポートしません。画像は、資格情報なしで Web サーバから取得可能である必要があります。

CCMCIP プロファイルのセットアップ

手順

ステップ 1 [Cisco Unified Presence の管理（Cisco Unified Presence Administration）] > [アプリケーション（Application）] > [Cisco Unified Personal Communicator] > [CCMCIP プロファイル（CCMCIP Profile）] を選択します。
リリース 9.0 を使用する場合は、[Cisco Unified CM IM and Presence] > [アプリケーション（Application）] > [レガシー クライアント（Legacy Clients）] > [CCMCIP プロファイル（CCMCIP Profile）] を選択します。

ステップ 2 [CCMCIP ゲートウェイ プロファイルの検索と一覧表示（Find and List CCMCIP Gateway Profiles）] ウィンドウで CTI プロファイルを検索します。
CCMCIP プロファイルが見つかった場合、これ以上のアクションは不要です。

ステップ 3 CCMCIP プロファイルが見つからない場合は、[新規追加（Add New）] を選択します。

ステップ 4 フィールドに必要な情報を入力します。

フィールド	設定
名前（Name）	プロファイル名を入力します。
説明（Description）	プロファイルの説明を入力します。

フィールド	設定
[プライマリ CCMCIP ホスト（Primary CCMCIP Host）] および [バックアップ CCMCIP ホスト（Backup CCMCIP Host）]	プライマリ サーバおよびバックアップ サーバを選択します。
これをシステムのデフォルト CCMCIP プロファイルに設定(Make This the Default LDAP Profile for the System)	システムに新規に追加されたユーザがこのデフォルト プロファイルに自動的に追加されるようにする場合は、このオプションをオンにします。 Unified Communications Manager から Unified Presence にすでに同期化されているユーザは、このデフォルト プロファイルに追加されません。 ただし、デフォルト プロファイルを作成した場合は、その後で同期化されたユーザがすべてそのデフォルト プロファイルに追加されることになります。

ステップ 5 [プロファイルにユーザを追加（Add Users to Profile）] を選択します。

ステップ 6 [ユーザの検索/一覧表示（Find and List Users）] ウィンドウを使用してユーザの検索と選択を行います。

ステップ 7 [選択項目の追加（Add Selected）] をクリックして、プロファイルにユーザを追加します。

ステップ 8 メイン [CCMCIP プロファイル（CTI Profile）] ウィンドウで [保存（Save）] を選択します。

プロキシ リスナーおよび TFTP アドレスの設定

プロキシ サーバとの通信には TCP を使用することを推奨します。 プロキシ サーバとの通信に UDP を使用する場合、連絡先リストが大きくなると Cisco Jabber Video for iPad の連絡先のプレゼンス ステータス情報が使用できなくなることがあります。

はじめる前に

TFTP サーバのホスト名または IP アドレスを取得します。

手順

ステップ 1 [Cisco Unified Presence の管理（Cisco Unified Presence Administration）] > [アプリケーション（Application）] > [Cisco Unified Personal Communicator] > [設定（Settings）] を選択します。

（注） リリース 9.0 を使用する場合は、[Cisco Unified CM IM/Presence（Cisco Unified CM IM and Presence）] > [アプリケーション（Application）] > [レガシー クライアント（Legacy Client）] > [設定（Settings）] を選択します。

ステップ 2 プロキシ リスナーの [デフォルト Cisco SIP プロキシ TCP リスナー（Default Cisco SIP Proxy TCP Listener）] を選択します。

ステップ 3 プライマリ（必須）およびバックアップ（任意）の TFTP サーバのアドレスをそれぞれ所定のフィールドに割り当てます。 IP アドレスまたは FQDN（完全修飾ドメイン名）を入力できます。

ステップ 4 [保存（Save）] を選択します。

Cisco Unified Presence でのボイスメール サーバ名およびアドレスの設定

Cisco Jabber Video for iPad が Cisco Unity Connection 上のボイス メッセージ Web サービス（VMWS）を操作できるように、Cisco Unified Presence でボイスメール設定を設定する必要があります。 VMWS サービスを使用すると、アプリケーションは削除済のボイスメール メッセージを正しい場所に移動できるようになります。 また、このサービスは安全なメッセージ機能をサポートするメッセージ暗号化機能も備えています。

はじめる前に

次のタスクを実行します。

- ボイスメール サーバが設定されていることを確認します。
- ボイスメール サーバのホスト名または IP アドレスを取得します。 使用中の環境でユーザ数に関するサービスを提供する場合には、複数のホスト名の指定が必要となることがあります。

手順

ステップ 1 [Cisco Unified Presence の管理（Cisco Unified Presence Administration）] > [アプリケーション（Application）] > [Cisco Unified Personal Communicator] > [ボイスメール サーバ（Voicemail Server）] を選択します。

（注） ボイスメール サーバの設定は、リリース 9.0 以降の Cisco Unified Communications Manager で実行します。

ステップ 2 [新規追加（Add New）] を選択します。

ステップ 3 [サーバ タイプ（Server Type）] メニューから [Unity Connection] を選択します。

ステップ 4 Cisco Unity Connection サーバ名を入力します。

ステップ 5 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。

ステップ 6 [Web サービス ポート（Web Service Port）] に 443 と入力します。

ステップ 7 [Web サービス プロトコル（Web Service Protocol）] メニューで [HTTPS] を選択します。

ステップ 8 [保存（Save）] を選択します。

Cisco Unified Presence でのメールストア サーバ名およびアドレスの設定

Cisco Jabber Video for iPad がメールストアに接続できるように、メールストア情報で Cisco Unified Presence を設定します。

Cisco Unity Connection は、通常、メールストアを備えており、同じサーバでそのメールストアのホストとなります。

はじめる前に

次のタスクを実行します。

- メールストア サーバのホスト名または IP アドレスを取得します。
- メールストア サーバをプロビジョニングしてから、そのサーバをボイスメール プロファイルに追加します。

手順

ステップ 1 [Cisco Unified Presence の管理（Cisco Unified Presence Administration）] > [アプリケーション（Application）] > [Cisco Unified Personal Communicator] > [メールストア（Mailstore）] を選択します。

（注） メールストアの設定は、リリース 9.0 以降の Cisco Unified Communications Manager で実行します。

ステップ 2 [新規追加（Add New）] を選択します。

ステップ 3 メールストア サーバ名を入力します。

ステップ 4 メールストア サーバのホスト名または IP アドレスを入力します。

ステップ 5 サーバに設定されているポート番号、および Cisco Jabber Video for iPad がこのサーバに問い合わせるときに使用する対応するプロトコルを指定します。

ステップ 6 [保存（Save）] を選択します。

Cisco Unified Presence でのボイスメール プロファイルの作成

ユーザをプロファイルに追加するには、ボイスメール プロファイルを作成します。

作成するボイスメール プロファイルごとにこの手順を繰り返します。

はじめる前に

次のタスクを実行します。

- ボイスメール サーバの名前とアドレスを指定します。
- メールストア サーバの名前とアドレスを指定します。

手順

ステップ 1 [Cisco Unified Presence の管理（Cisco Unified Presence Administration）] > [アプリケーション（Application）] > [Cisco Unified Personal Communicator] > [ボイスメール プロファイル（Voicemail Profile）] を選択します。

（注） ボイスメール プロファイルの設定は、リリース 9.0 以降の Cisco Unified Communications Manager で実行します

ステップ 2 [新規追加（Add New）] を選択します。

ステップ 3 プロファイルの名前と説明を入力します。

ステップ 4 次の情報を入力します。

フィールド	説明
音声メッセージング パイロット（Voice Messaging Pilot）	ボイスメール パイロット番号は、ユーザが各自のボイス メッセージにアクセスするためにダイヤルするディレクトリ番号です。 パイロット番号はそれぞれ異なるボイス メッセージ システムに所属させることができます。 次のオプションのいずれか 1 つを選択します。 • 番号：システムのボイスメール パイロット番号を選択します。 これは、Cisco Unified Communications Manager Administration の [ボイスメール（Voice Mail）] > [ボイスメール パイロット（Voice Mail Pilot）] メニューで指定した番号と同じものです。 • [ボイスメールなし（No Voice Mail）]：応答されなかった着信コールをボイスメールに送信する必要がない場合は、このオプションを選択します。
プライマリ ボイスメール サーバ（Primary Voicemail Server）	プライマリ サーバを選択します。 指定したボイスメール サーバのいずれかを選択します。
バックアップ ボイスメール サーバ（Backup Voicemail Server）	バックアップ ボイスメール サーバの名前を入力します。 バックアップ ボイスメール サーバが必要ない場合は、[なし（None）] を選択します。
プライマリ メールストア（Primary Mailstore）	プライマリ メールストア サーバを選択します。 指定したメールストア サーバのいずれかを選択します。

フィールド	説明
バックアップ メールストア（Backup Mailstore）	バックアップ メールストア サーバの名前を入力します。 バックアップボイスメールサーバが必要ない場合は、[なし（None）] を選択します。
これをシステムのデフォルト ボイスメール プロファイルに設定（Make this the default Voicemail Profile for the system）	新規ユーザを自動的にデフォルト プロファイルに追加する場合は、このオプションをオンにします。 Cisco Unified CM から Cisco Unified Presence にすでに同期化されているユーザは、このデフォルト プロファイルに追加されません。 ただし、デフォルト プロファイルの作成後に同期化されるユーザはデフォルト プロファイルに追加されます。

ステップ 5 次の情報を入力します。

フィールド	説明
Inbox フォルダ（Inbox Folder）	新しいメッセージが保存されるメールストア サーバ上のフォルダの名前を入力します。 この値は、メールストア サーバがデフォルト フォルダとは異なるフォルダ名を使用する場合のみ変更してください。 デフォルト フォルダ：INBOX
ごみ箱フォルダ（Trash Folder）	削除したメッセージが保存されるメールストア サーバ上のフォルダの名前を入力します。 この値は、メールストア サーバがデフォルト フォルダとは異なるフォルダ名を使用する場合のみ変更してください。 デフォルト フォルダ：Deleted Items
デュアル フォルダ モードを使用可能にする（Allow dual folder mode）	UIDPLUS がサポートされていないことがわかっている場合、およびシステムでシングル フォルダ モードを強制的に使用する場合は、この設定をオフにします。 デフォルト設定：[オン（On）] （注） Microsoft Exchange 2007 サーバは、UIDPLUS 拡張をサポートしていません。

ステップ 6 [プロファイルにユーザを追加（Add Users to Profile）] を選択します。

ステップ 7 [ユーザの検索/一覧表示（Find and List Users）] ウィンドウを使用してユーザの検索と選択を行い、[選択項目の追加（Add Selected）] を選択してユーザをプロファイルに追加します。

ステップ 8 [保存（Save）] を選択します。

（注） Cisco Unified Communications Manager の製品固有の設定でボイスメール パラメータを設定している場合、Cisco Jabber Video for iPad はその設定を使用し、Cisco Unified Presence サーバのボイスメール設定を無視します。

第 5 章

Cisco Unified Communications Manager 8.x の設定

この章では、Cisco Unified Communications Manager 8.x を使用した Cisco Jabber Video for iPad の設定方法について説明します。

システムおよびネットワークの要件

Cisco Jabber Video for iPad のシステムとネットワークの要件については、このセクションを参照してください。

ファイアウォールの要件

ポートがアプリケーションのトラフィックを伝送するようにハードウェア ファイアウォールを設定します。ハードウェアファイアウォールは、望まないトラフィックからの保護を組織レベルで実現するネットワーク デバイスです。 次の表に、Cisco Unified Communications Manager と Cisco Unified Presence の導入に必要なポートを示します。 これらのポートは、アプリケーションが正常に機能するために、すべてのファイアウォール上で開いておく必要があります。

ポート	プロトコル	説明
着信		
16384 ～ 32766	UDP	ビデオおよびオーディオ用の Real-Time Transport Protocol（RTP）メディア ストリームを受信します。 これらのポートは、Cisco Unified Communications Manager で設定します。
発信		
69	TFTP	Trivial File Transfer Protocol（TFTP）ファイルをダウンロードするために TFTP サーバに接続します
80 および 6970	HTTP	会議用の Cisco WebEx Messenger やボイスメール機能用の Cisco Unity Connection などのサービスに接続します TFTP サーバ アドレスにポートが指定されていない場合、Cisco Jabber for iPad は、ポート 6970 を使用して、電話設定ファイルとダイヤル ルール ファイルを取得しようとします。
5060	UDP/TCP	Session Initiation Protocol（SIP）コール シグナリングを提供します

ポート	プロトコル	説明
5061	TCP	セキュアな SIP コール シグナリングを提供します
8443	TCP	Cisco Unified Communications Manager IP Phone（CCMCIP）サーバに接続し、現在割り当てられているデバイスのリストを取得します
16384 ～ 32766	UDP	UDP でビデオとオーディオの RTP メディア ストリームを送信します
389	TCP	連絡先を検索するために LDAP サーバに接続します
443 7080	VMRest HTTPS	Cisco Unity Connection に接続して、ボイス メッセージの取得と管理を行います
8443	HTTPS	Cisco Unified Communications Manager で連絡先を検索するために User Data Services（UDS）に接続します
636	LDAPS	連絡先を検索するためにセキュア LDAP サーバに接続します

ファイアウォールの要件

ポートがアプリケーションのトラフィックを伝送するようにハードウェア ファイアウォールを設定します。ハードウェア ファイアウォールは、望まないトラフィックからの保護を組織レベルで実現するネットワーク デバイスです。 次の表に、Cisco Unified Communications Manager と Cisco Unified Presence の導入に必要なポートを示します。 これらのポートは、アプリケーションが正常に機能するために、すべてのファイアウォール上で開いておく必要があります。

ポート	プロトコル	説明
着信		

ポート	プロトコル	説明
16384 ～ 32766	UDP	ビデオおよびオーディオ用の Real-Time Transport Protocol（RTP）メディア ストリームを受信します。 これらのポートは、Cisco Unified Communications Manager で設定します。
発信		
69	TFTP	Trivial File Transfer Protocol（TFTP）ファイルをダウンロードするために TFTP サーバに接続します
80 および 6970	HTTP	会議用の Cisco WebEx Messenger やボイスメール機能用の Cisco Unity Connection などのサービスに接続します TFTP サーバ アドレスにポートが指定されていない場合、Cisco Jabber for iPad は、ポート 6970 を使用して、電話設定ファイルとダイヤル ルール ファイルを取得しようとします。
5060	UDP/TCP	Session Initiation Protocol（SIP）コール シグナリングを提供します
5061	TCP	セキュアな SIP コール シグナリングを提供します
8443	TCP	Cisco Unified Communications Manager IP Phone（CCMCIP）サーバに接続し、現在割り当てられているデバイスのリストを取得します
16384 ～ 32766	UDP	UDP でビデオとオーディオの RTP メディア ストリームを送信します
389	TCP	連絡先を検索するために LDAP サーバに接続します

ポート	プロトコル	説明
443 7080	VMRest HTTPS	Cisco Unity Connection に接続して、ボイス メッセージの取得と管理を行います
8443	HTTPS	Cisco Unified Communications Manager で連絡先を検索するために User Data Services（UDS）に接続します
636	LDAPS	連絡先を検索するためにセキュア LDAP サーバに接続します

帯域幅のパフォーマンス期待値

優れた VGA ビデオ品質を実現するには、最低でも 256 ～ 384 kbps のアップロード帯域幅が必要です。 512 kbps 以上のアップロード帯域幅では、20 fps で 480 x 360 の発信ビデオ解像度と 30 fps で 640 x 480 の最大着信ビデオの解像度を実現できます。 VPN を使用するとペイロード サイズが増加するため、帯域幅の使用量が増加します。 ビデオ解像度とフレーム レートは、VPN 接続を使用した場合は、ここに示す値ほど高くならない場合があります。

ビデオ レート適応

Cisco Jabber for iPad はビデオ レートの適応を使用して、ネットワークの状態に基づいた最適なビデオ品質をネゴシエートします。 ビデオ転送が開始すると、ビデオ レートの適応によりビデオ品質が動的に変化します。

Cisco Jabber for iPad は使用可能な帯域幅に合わせてビデオを自動的に適応させます。 ユーザがビデオ コールを発信すると、アプリケーションはビット レートおよび解像度を急速かつ段階的に向上させ、最適な設定を実現します。 低い解像度のビデオ コールは、短期間の間に高解像度に向上すると予想されます。 アプリケーションは、後続のビデオ コールが最適な解像度で開始されるように、履歴を保存します。 ただし、最適な解像度が実現するまで、ビデオ転送が多少変動したり変化することが想定されます。

ファイアウォールの要件

ポートがアプリケーションのトラフィックを伝送するようにハードウェア ファイアウォールを設定します。 ハードウェア ファイアウォールは、望まないトラフィックからの保護を組織レベルで実現するネットワーク デバイスです。 次の表に、Cisco Unified Communications Manager と Cisco Unified Presence の導入に必要なポートを示します。 これらのポートは、アプリケーションが正常に機能するために、すべてのファイアウォール上で開いておく必要があります。

ポート	プロトコル	説明
着信		
16384 ～ 32766	UDP	ビデオおよびオーディオ用の Real-Time Transport Protocol（RTP）メディア ストリームを受信します。 これらのポートは、Cisco Unified Communications Manager で設定します。
発信		
69	TFTP	Trivial File Transfer Protocol（TFTP）ファイルをダウンロードするために TFTP サーバに接続します
80 および 6970	HTTP	会議用の Cisco WebEx Messenger やボイスメール機能用の Cisco Unity Connection などのサービスに接続します TFTP サーバ アドレスにポートが指定されていない場合、Cisco Jabber for iPad は、ポート 6970 を使用して、電話設定ファイルとダイヤル ルール ファイルを取得しようとします。
5060	UDP/TCP	Session Initiation Protocol（SIP）コール シグナリングを提供します
5061	TCP	セキュアな SIP コール シグナリングを提供します
8443	TCP	Cisco Unified Communications Manager IP Phone（CCMCIP）サーバに接続し、現在割り当てられているデバイスのリストを取得します
16384 ～ 32766	UDP	UDP でビデオとオーディオの RTP メディア ストリームを送信します
389	TCP	連絡先を検索するために LDAP サーバに接続します

ポート	プロトコル	説明
443 7080	VMRest HTTPS	Cisco Unity Connection に接続して、ボイス メッセージの取得と管理を行います
8443	HTTPS	Cisco Unified Communications Manager で連絡先を検索するために User Data Services（UDS）に接続します
636	LDAPS	連絡先を検索するためにセキュア LDAP サーバに接続します

推奨される手順

このチェックリストでは、Cisco Unified Communications Manager を使用して Cisco Jabber Video for iPad をセットアップする一般的な手順について説明します。 実際の手順は、組織によって異なる場合があります。

1 システムの SIP パラメータの設定, （45 ページ）
2 デバイス用の Cisco Options Package（COP）ファイルのインストール, （46 ページ）
3 専用の SIP プロファイルの設定, （47 ページ）
4 Cisco Jabber Video for iPad のアプリケーション ダイヤル ルールのセットアップ, （49 ページ）
5 通話中の機能に関するシステムレベルの前提条件, （51 ページ）
6 使用状況とエラーのトラッキング, （51 ページ）
7 ユーザ デバイスの追加, （52 ページ）
8 一括設定, （59 ページ）
9 ファイアウォールの要件, （22 ページ）
10 ディレクトリ検索設定の指定, （59 ページ）
11 Connect On Demand VPN の設定, （62 ページ）
12 Cisco Unified Communications Manager, （120 ページ）

システムの SIP パラメータの設定

手順

ステップ 1 Cisco Unified CM の管理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 Parameter）] を選択します。
ステップ 3 [Cisco CallManager サービス（Cisco CallManager Service）] を選択します。

この設定は、クラスタ全体に適用されます。 [サーバ（Server）] フィールドを設定する必要はありません。

ステップ 4 SIP Trying タイマーを 1000 ms に設定します。

ステップ 5 SIP デュアル モード アラート タイマーを 4500 ms に設定します。

ステップ 6 [保存（Save）] を選択します。

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

デバイスとして Cisco Jabber Video for iPad を使用できるように、すべての Cisco Unified Communications Manager サーバにデバイス固有の Cisco Options Package（COP）ファイルをインストールします。

COP ファイルのインストールに関する一般的な情報については、http://www.cisco.com/en/us/products/sw/voicesw/ps556/prod_maintenance_guides_list.html 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。

（注） 次の Cisco Unified Communications Manager リリースには、すでにタブレット用 COP ファイルが含まれています。

- 7.1.5.35113-1 以降
- 8.5.1.16090-1 以降
- 8.6.2.23057-1 以降
- 9.0.1.11013-1-1 以降
- 9.1.1.10000-11 以降

タブレット COP ファイルのインストールは、これらのリリースには必要ではありません。

重要 サービスが中断される可能性があるため、この手順は使用率が低い時間帯に行ってください。

手順

ステップ 1 iPad 用のデバイス COP ファイルを http://www.cisco.com/cisco/software/navigator.html?mdfid=280443139&flowid=29241 からダウンロードします。

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 次の手順に従って、COP ファイルを Unified CM クラスタ内のパブリッシャ サーバにインストールします。

a) [ナビゲーション（Navigation）] ドロップダウン リストで [Cisco Unified OS の管理（Cisco Unified OS Administration）] を選択してから、[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）] の順に選択します。
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。
プロセス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) Unified CM サーバ上の Cisco Tomcat サービスを再起動します。
このステップ（Tomcat イメージ キャッシュがクリアされる）は、Unified CM のデバイス リスト ページ上でデバイス アイコンが正しく表示されるために必要です。
k) 次のコマンドを CLI から入力します。

```
utils service restart Cisco Tomcat
```

l) システムが完全にサービスに復帰するまで待機します。

重要 サービスにおける割り込みを回避するため、この手順を別のサーバで実行する場合は、事前に各サーバがサービスのアクティブな実行に復帰したことを確認します。

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、サーバの再起動を含む手順を実行します。

専用の SIP プロファイルの設定

Cisco Jabber Video for iPad がバックグラウンドで実行中も Unified Communications Manager との接続を維持できるようにする専用の SIP プロファイルを設定します。

手順

ステップ 1 Cisco Unified CM の管理にサインインします。

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

ステップ 3 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。
プロファイルに「Standard iPad SIP Profile」という名前を付けることができます。

ステップ 4 [電話で使用されるパラメータ（Parameters Used in Phone）] セクションで、次の値を入力します。

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

ステップ 5 次のフィールドにポート範囲を指定してください。

- [開始メディアポート（Start Media Port）]：メディア ストリームの開始ポートを定義します。このフィールドは、範囲の最小ポートを設定します。
- [終了メディアポート（Stop Media Port）]：メディア ストリームの開始ポートを定義します。このフィールドは、範囲の最大ポートを設定します。

（注） Cisco Jabber Video for iPad は、SIP プロファイルで設定するポート範囲を均等に区切ります。 クライアントは、次のようにポート範囲を使用します。

- ポート範囲の下半分は、オーディオ ストリーム用
- ポート範囲の上半分は、ビデオ ストリーム用

たとえば、3000 のスタート メディア ポートおよび 4000 のエンド メディア ポートを使用する場合、クライアントはポート経由で次のようにメディアを送信します。

- オーディオ ストリームのポート：3000 ～ 3501
- ビデオ ストリームのポート：3502 ～ 4000

オーディオ メディアおよびビデオ メディアのポート範囲を分割する結果として、クライアントにより識別可能なメディア ストリームが作成されます。IP パケットのヘッダー内の DSCP 値を設定することで、それらのメディア ストリームを分類し、優先させることができます。

ステップ 6 [保存（Save）] を選択します。

次の作業

Cisco Jabber Video for iPad を実行するすべてのユーザ デバイスに対してこの SIP プロファイルを選択します。

Cisco Jabber Video for iPad のアプリケーション ダイヤル ルールのセットアップ

A Cisco Options Package (COP) file must be used to set up dial rules for Cisco Unified Communications Manager 8.5 以前で Cisco Jabber Video for iPad のダイヤル ルールをセットアップするには、Cisco Options Package (COP)ファイルを使用する必要があります。 この COP ファイルは、このマニュアル内の別の項で説明しているデバイス COP ファイルとは異なります。

このトピックで説明されている一連の手順を実行して、既存のすべてのダイヤル ルールをアプリケーションから利用できるようにします。 この一連の手順では、必要な XML ファイルを Cisco Unified Communications Manager TFTP サーバのルート レベルにある CUPC という名前のフォルダにインストールする方法を説明します。

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、『*Cisco Unified Communications Manager Administration Guide*』の関連する章を参照してください。 使用している Cisco Unified Communications Manager のリリースの固有のガイドは、次の場所で入手できます。

http://www.cisco.com/en/us/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

手順

ステップ 1 ダイヤル ルール用の Cisco Options Package（COP）ファイルの取得 , （49 ページ）

ステップ 2 TFTP サービスの再起動, （50 ページ）

ダイヤル ルール用の Cisco Options Package（COP）ファイルの取得

他のシスコ製品でこの目的のために使用する COP ファイルを、ここでも使用します。

（注） この手順は、Cisco Unified Communications Manager Release 8.5 以前のバージョンにのみ適用されます。

この手順で説明する COP ファイルは、Cisco Jabber Video for iPad を Cisco Unified Communications Manager でデバイスとして使用可能にするために使用されるデバイス COP ファイルとは異なります。

手順

ステップ 1 http://www.cisco.com/cisco/software/release.html?mdfid=283665631&softwareid=283732952&release=8.6(2)&relind=AVAILABLE&rellifecycle=&reltype=latest にある Cisco UC Integration for Microsoft Office Communicator 用の [ソフトウェア ダウンロード（Software Downloads）] ページにアクセスします。

ステップ 2 使用する Cisco Unified Communications Manager のリリースに最も近いリリース番号を選択します。

ステップ 3 Administration Toolkit を含むバンドルを探します。

ステップ 4 [今すぐダウンロード（Download Now）] を選択します。

ステップ 5 画面上の指示を確認します。

ステップ 6 ダウンロードされたファイルを解凍します。

ステップ 7 CUCM フォルダ内で、ダイヤル ルールの COP ファイルを探します。
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 8 ダイヤル ルールの COP ファイルを、TFTP でアクセスできるサーバ上に置きます。

TFTP サービスの再起動

この手順は使用率が低い時間帯に行ってください。サービスが中断される可能性があります。

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『*Cisco Unified Serviceability Administration Guide*』の「Starting, Stopping, Restarting, and Refreshing Status of Services in Control Center」のトピックを参照してください。

手順

ステップ 1 [Unified CM の管理（Unified CM Administration）] で、[ナビゲーション（Navigation）] ドロップダウン リストの [Cisco Unified サービス アビリティ（Cisco Unified Serviceability）] を選択してから、[移動（Go）] を選択します。

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

ステップ 3 サーバを選択し、[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 [再起動（Restart）] を選択します。

ステップ 6 この COP ファイルを実行するすべてのサーバで、この手順を繰り返します。

通話中の機能に関するシステムレベルの前提条件

次の通話中の機能が Cisco Unified Communications Manager システムで設定されていることを確認してください。

- 保留と保留解除
- 会議とマージ
- 転送
- モバイルへの送信

（注） これらの機能の設定方法の詳細については、http://www.cisco.com/en/us/products/sw/voicesw/ps556/prod_maintenance_guides_list.html にある、お使いのリリースに対応した『*Cisco Unified Communications Manager Features and Services Guide*』を参照してください。

使用状況とエラーのトラッキング

Cisco Jabber Video for iPad 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。

収集された情報はすべて Google によって保管され、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。

Cisco Unified Communications Manager で各ユーザ デバイスを設定する際、各ユーザに対して使用状況とエラーのトラッキング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。

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 • アプリケーションの画面表示（たとえば、ユーザがボイス メッセージの一覧を表示した頻度など） • 機能アクティビティ（たとえば、ユーザが連絡先を追加した頻度など） • アプリケーションが接続した TFTP サーバ 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
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

レポート ツールに関する詳細については、次を参照してください。

- http://www.google.com/analytics/
- http://www.google.com/policies/privacy/

ユーザ デバイスの追加

ユーザ デバイスを Cisco Unified Communications Manager サーバに追加して設定を確認すること。

はじめる前に

次のタスクを実行します。

- デバイス用の Cisco Options Package（COP）ファイルのインストール, （46 ページ）
- 専用の SIP プロファイルの設定, （47 ページ）
- iPadデバイスに割り当てるデバイス プールが、サポートされるすべての音声コーデックを含んだリージョンに関連付けられていることを確認すること。 Cisco Jabber Video for iPad がサポートする音声コーデックには、G.711 mu-law または A-law および G.722.1 が含まれます。

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）] 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 ドロップダウン リストで [Cisco Jabber for Tablet] を選択してから、[次へ（Next）] をクリックします。

ステップ 5 次の表に説明されている情報を入力します。

パラメータ	説明
デバイス情報	
デバイス名（Device Name）	デバイス名は、 • 1 つのデバイスのみを表します。ユーザの複数のデバイス上に Cisco Jabber Video for iPad がある場合は、各デバイスを異なるデバイス名で設定します。 • TAB で開始し、続けて最大 15 文字の大文字または数字を入力する必要があります。 例：TABJOHND。 • ドット（.）、ダッシュ（–）、またはアンダースコア（_）を使用できます。
電話ボタンテンプレート（Phone button Template）	[標準 Jabber for iPad（Standard Jabber for iPad）] を選択します。
プロトコル固有情報	
デバイス セキュリティ プロファイル（Device Security Profile）	[Cisco Jabber for iPad – 標準 SIP 非セキュア プロファイル（Cisco Jabber for iPad – Standard SIP Non-Secure Profile）] を選択します。
SIP プロファイル（SIP Profile）	作成した SIP プロファイルを選択します。 詳細は、専用の SIP プロファイルの設定, （47 ページ）を参照してください。
プロダクト固有の設定	
LDAP ユーザ認証の有効化（Enable LDAP User Authentication）	[有効（Enabled）] を選択した場合、アプリケーションで [LDAP ユーザ認証（LDAP User Authentication）] もオンにするようユーザに指示します。

パラメータ	説明
LDAPユーザ名（LDAP Username）	アプリケーションに自動的に入力されるように、必要なLDAP設定を指定します。
LDAP パスワード（LDAP Password）	
LDAP サーバ（LDAP Server）	
LDAP 検索ベース（LDAP Search Base）	
LDAP フィールドマッピング（LDAP Field Mappings）	（注）　現時点では、このフィールドのカスタマイズはサポートされていません。
LDAP SSL の有効化（Enable LDAP SSL）	[有効（Enabled）] を選択した場合、アプリケーションで [SSL を使用（Use SSL）] もオンにするようユーザに指示します。
ボイスメールのユーザ名（Voicemail Username）	アプリケーションに自動的に入力されるように、ボイスメール設定を指定します。 詳細は、ディレクトリ検索設定の指定, （59 ページ）を参照してください。
ボイスメール サーバ（Voicemail Server）	
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（Voicemail Message Store）	
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, （51 ページ）を参照してください。
ビデオ機能（Video Capabilities）	ユーザのビデオをオンにするには、[有効（Enabled）] を選択します。
オンデマンド VPN の URL（On-Demand VPN URL）	Connect On Demand VPN 機能で使用される URL。

パラメータ	説明
プリセット Wi-Fi ネットワーク（Preset Wi-Fi Networks）	デバイスのプリセット Wi-Fi ネットワーク情報。

（注） これ以外の設定は、他の機能の設定時に入力します。

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 n] - 新規 DN を追加（[Line n] - Add a new DN）] を選択します。

ステップ 9 このデバイスのディレクトリ番号を入力します。

ステップ 10 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、アプリケーションが実行されておらず、ネットワークに接続されているときには電話を転送して、発信者がエラー メッセージを受け取らないようにするために、次の設定を指定します。

- 未登録内線の不在転送（Forward Unregistered Internal）
- 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、Cisco Unified Communications Manager のオンライン ヘルプを参照してください。

ステップ 11 [無応答時の呼び出し時間（No Answer Ring Duration）] を 24 秒間に設定し、通話をボイスメールに転送する前に、アプリケーションが呼び出し音を鳴らす時間を設定します。
Cisco Unified Communications Manager 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 12 環境に応じて、その他の設定を指定します。

ステップ 13 [保存（Save）] を選択します。

ステップ 14 次の手順に従って、作成したデバイスをユーザに関連付けます。

a) [ユーザ管理（User Management）] > [エンド ユーザ（End User）] を選択します。
b) ユーザを検索して選択します。
c) [デバイス情報（Device Information）] セクションで、[デバイスの割り当て（Device Association）] を選択します。
d) このユーザに関連付けるデバイスのチェックをオンにします。
e) [選択/変更の保存（Save Selected/Changes）] を選択します。

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。

（注） [プライマリユーザデバイス（Primary User Device）] フィールドは、Cisco Unified Communications Manager 9.0 以前のみで使用できます。 Cisco Unified Communications Manager のそれ以降のバージョンでは、このフィールドを指定する必要はありません。

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

次のタスクを実行して、設定を確認します。

- iPad デバイスが企業の Wi-Fi ネットワークに接続されていることを確認します。 デバイスのブラウザを使用して企業の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 Video for iPad を起動し、ユーザ名（または電子メール アドレス）、パスワード、および先程追加したデバイスの TFTP サーバ アドレスを入力します。
- 通話の発信、保留、転送など、Cisco Jabber Video for iPad の基本的な音声機能をテストします。

電話機としての iPad の制御の有効化

次の手順に従って、ユーザがデバイスを電話機として制御できるようにします。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、[ユーザ管理（User Management）] > [エンド ユーザ（End User）] を選択します。

ステップ 2 追加するユーザを検索して選択します。

ステップ 3 [権限情報（Permissions Information）] セクションで [ユーザ グループに追加（Add to User Group）] を選択します。

ステップ 4 [ユーザ グループの検索と一覧表示（Find and List User Groups）] ウィンドウで、「標準 CTI（Standard CTI）」 を検索します。

ステップ 5 [標準 CTI 対応（Standard CTI Enabled）] を選択します。
ユーザの電話機が Cisco Unified IP Phone 6900、8900 または 9900 シリーズ モデルの場合は、[標準 CTI による Xfer および会議をサポートする電話の制御（Standard CTI Allow Control of Phones supporting Xfer and conf）] も選択します。

ステップ 6 [選択項目の追加（Add Selected）] を選択します。

ステップ 7 [保存（Save）] を選択します。

LDAP 認証設定の指定

LDAP 認証機能を使用すると、社内 LDAP ディレクトリに対して Cisco Unified Communications Manager でユーザ パスワードを認証できます。

（注） LDAP 認証は、アプリケーション ユーザ、内部データベースの Cisco Unified Communications Manager 認証アプリケーション ユーザには適用されません。

はじめる前に

Cisco Unified Communications Manager で LDAP 同期を有効にします。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] > [システム（System）] > [LDAP] > [LDAP 認証（LDAP Authentication）] を選択します。

ステップ 2 [エンド ユーザ用 LDAP 認証の使用（Use LDAP Authentication for End Users）] をオンにします。

ステップ 3 LDAP 認証設定を指定します。

ステップ 4 LDAP サーバ ホスト名または IP アドレスおよびポート番号を指定します。

（注） Secure Socket Layer（SSL）を使用して LDAP ディレクトリと通信するには、[SSL を使用（Use SSL）] をオンにします。

ステップ 5 [保存（Save）] を選択します。

ヒント LDAP over SSL を設定する場合は、LDAP ディレクトリ証明書を Cisco Unified Communications Manager にアップロードします。

ユーザ プロビジョニングの LDAP 同期の設定

Cisco Unified Communications Manager でこのタスクを実行します。

LDAP 同期は Cisco Unified Communications Manager で Cisco Directory Synchronization（DirSync）ツールを使用して、社内 LDAP ディレクトリから情報を（手動または定期的に）同期します。DirSync サービスをオンにすると、Cisco Unified Communications Manager は社内ディレクトリからユーザを自動的にプロビジョニングします。 Cisco Unified Communications Manager ローカル データベースを引き続き使用しますが、ユーザ アカウントを作成できるようにファシリティをオフにします。LDAPディレクトリ インターフェイスを使用して、ユーザ アカウントを作成および管理します。

はじめる前に

- Cisco Unified Communications Manager で LDAP 固有の設定を試行する前に、LDAP サーバがインストールされていることを確認してください。
- LDAP 同期がアプリケーション ユーザ Cisco Unified Communications Manager に適用されないことに注意してください。 Cisco Unified Communications Manager の管理インターフェイスでアプリケーション ユーザを手動でプロビジョニングする必要があります。
- Cisco Unified Communications Manager で Cisco DirSync サービスをアクティブにし、起動します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] > [システム（System）] > [LDAP] > [LDAP システム（LDAP System）] を選択します。

ステップ 2 [新規追加（Add New）] を選択します。

ステップ 3 LDAP サーバ タイプおよび属性を設定します。

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

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] > [システム（System）] > [LDAP] > [LDAP ディレクトリ（LDAP Directory）] を選択します。

ステップ 7 [新規追加（Add New）] を選択します。

ステップ 8 次の項目を設定します。

- LDAP ディレクトリ アカウント設定
- 同期対象のユーザ属性
- 同期スケジュール
- LDAP サーバ ホスト名または IP アドレスおよびポート番号

ステップ 9 Secure Socket Layer（SSL）を使用して LDAP ディレクトリと通信するには、[SSL を使用（Use SSL）] をオンにします。

ステップ 10 [保存（Save）] をクリックします。

ヒント
- LDAP over SSL を設定するには、LDAP ディレクトリ証明書を Cisco Unified Communications Manager にアップロードします。
- 特定の LDAP 製品のアカウント同期メカニズムおよび LDAP 同期の一般的なベストプラクティスの詳細については、Cisco Unified Communications Manager SRND の LDAP ディレクトリの情報を参照してください。

一括設定

このマニュアルに記載された情報を使用して、ユーザと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、お使いの Cisco Unified Communications Manager のリリースに対応した一括管理ガイドに記載されている指示に従ってください。このガイドは http://www.cisco.com/en/us/products/sw/voicesw/ps556/prod_maintenance_guides_list.html から入手できます。

ディレクトリ検索設定の指定

はじめる前に

次のタスクを実行します。

- 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。
- この手順の表にある必須情報を収集します。
- この手順で示した表内の値について不明点がある場合は、ディレクトリ管理者にお問い合わせください。
- 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、この手順の後半でマッピングします。

要素	要素名	デフォルト ディレクトリ属性	異なる場合は、実際の値
固有識別子（Unique identifier）	identifier	distinguishedName	
表示名（Display name）	displayName	cn	
電子メール アドレス（Email address）	emailAddress	mail	
名（First name）	firstName	givenName	
姓（Last name）	lastName	sn	
ユーザ ID	userid	userPrincipalName	
メイン電話番号（Main phone number）	mainPhoneNumber	telephoneNumber	

要素	要素名	デフォルト ディレクトリ属性	異なる場合は、実際の値
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	mobile	
携帯電話番号（予備）（Second mobile phone number）	mobilePhoneNumber2	—	
ボイスメール直通電話番号（Direct to voicemail phone number）	voicemailPhoneNumber	voicemail	
FAX 番号（Fax number）	faxPhoneNumber	facsimileTelephoneNumber	
その他の電話番号（Other phone number）	otherPhoneNumber	—	

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

- 電話番号が整形されていないこと。
- グローバル カタログが有効になっていること。

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 ユーザの iPad デバイス ページに移動します。

ステップ 3 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 4 LDAP のユーザ名とパスワードを入力します。
次のいずれかの手順を実行します。

- 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。 ユーザはアプリケーションでクレデンシャルを入力する必要がなくなります。
- 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。 各ユーザにパスワードを伝え、そのパスワードをアプリケーションで入力するようにユーザに依頼します。
- 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）であり、電子メール アドレスの形式（userid@example.com など）になっていることがあります。

ステップ 5 LDAP サーバのアドレスを入力します。

- 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次の形式で入力します。

  YourDirectoryServer.YourCompany.com:portnumber

- 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。

ポートや SSL の設定を入力しなければ、アプリケーションはデフォルトでポート 3269 への SSL 接続を試みます。

ステップ 6 「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、アプリケーションは、defaultNamingContext 属性の RootDSE 検索で見つかる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。

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 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。

デフォルトと一致しないフィールド マッピングを「name=value」ペアの形式ですべて入力します（各フィールドをセミコロン（;）で区切ります）。

例：displayName=nickname;emailAddress=email。 要素名の値を名前の値として使用します。

ステップ 8 [保存（Save）] を選択します。

次の作業

次の手順に従って、社内ディレクトリの設定をテストします。

1. Cisco Jabber for iPad の [設定（Settings）] から社内ディレクトリのアカウントを削除し（必要な場合）、アプリケーションを再起動します。
2. Cisco Unified Communications Manager のアカウントを使用してサインインし、指示に従って社内ディレクトリの設定を入力または確認します。
3. 変更を加えなかった場合も含め、[保存（Save）] をタップします。
4. ディレクトリ検索をテストします。

Connect On Demand VPN の設定

Cisco Jabber Video for iPad は、Connect on Demand VPN 機能を有効化する 2 種類の方法をサポートします。

Cisco Unified Presence と Cisco Unified Communications Manager サーバが完全修飾ドメイン名（FQDN）で設定されている場合、Connect On Demand VPN 機能は、Cisco Jabber Video for iPad を使用してイネーブルまたはディセーブルにします。 Cisco Unified Presence と Cisco Unified Communications Manager サーバが IP アドレスで設定されている場合、Connect On Demand VPN 機能をイネーブルにするようにオンデマンド VPN の URL パラメータを設定します。

（注） シスコでは、FQDN を使用して Cisco Unified Presence および Cisco Unified Communications Manager を展開することを推奨します。 FQDN を使用して展開する場合、Connect On Demand VPN 機能を使用するために Cisco Unified Presence と Cisco Unified Communications Manager を追加設定する必要はありません。

はじめる前に

- iPad 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 アクセスのセットアップについては、VPN クライアントのプロバイダーにお問い合わせください。
- Cisco Unified Presence と Cisco Unified Communications Manager サーバは、完全修飾ドメイン名または IP アドレスを使用してネットワークを識別します。
- 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 クエリーが失敗した場合は、 Cisco Jabber Video for iPad 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。

- Cisco Unified Communications Manager を、IP アドレスではなくドメイン名でアクセスできるよう設定します。 このドメイン名がファイアウォール外では解決できないことを確認します。 Cisco AnyConnect クライアント接続の Connect on Demand ドメイン リストで、このドメインを [必要に応じて接続する（Connect If Needed）] リストに追加します。
- ドメイン名を使用して Cisco Unified Communications Manager にアクセスできない場合、またはファイアウォール外からそのドメイン名の DNS 検索を失敗にできない場合、次の手順のパラメータを存在しないドメインにセットします。 存在しないドメインは、ユーザがファイアウォールの内部または外部にいるときに、DNS クエリーを失敗させます。 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。

用途	使用不可
cm8ondemand.company.com	https://cm8ondemand.company.com/vpn

手順

ステップ 1 Cisco Unified CM の管理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）] セクションに移動します。

ステップ 4 この手順の前に指定した URL を [オンデマンド VPN の URL（On-Demand VPN URL）] フィールドに入力します。

（注） URL はドメイン名のみである必要があります。 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

この機能をテストするには、次を実行します。

- 手順で指定した URL を iPad の Safari に入力し、VPN が自動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。
- iPad が VPN を使用して企業ネットワークに接続し、企業イントラネット サイトへのアクセスなどのタスクを実行できることを確認します。 接続が正常に動作しない場合、VPN プロバイダーにお問い合わせください。

社内無線ネットワークの Connect On Demand VPN をディセーブルにする

社内無線ネットワークの Connect On Demand VPN 機能をディセーブルにするには、次の手順を実行します。

はじめる前に

- 社内 Wi-Fi の SSID のリストを収集します。

手順

ステップ 1 Cisco Unified CM の管理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）] セクションに移動します。
ステップ 4 最大 3 つの社内 Wi-Fi SSID にプリセット Wi-Fi ネットワークをスラッシュで区切って設定します（/）。
ステップ 5 [保存（Save）] を選択します。

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。

（注） Cisco Jabber for Android では、オフィス経由のダイヤル - リバース機能での SIP ダイジェスト認証機能をサポートしていません。

Cisco Jabber for Android では、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, （65 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
  - 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 for Android 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, （65 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, （66 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 Jabber for Tablet - 標準 SIP 非セキュア プロファイル（Cisco Jabber for Tablet - 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 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 [システム（System）] > [セキュリティ（Security）] > [電話セキュリティ プロファイル（Phone Security Profile）] の下で、Cisco Jabber For Tablet 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 Jabber for Tablet デバイス（Cisco Jabber for Tablet 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）] 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 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 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 [システム（System）] > [セキュリティ（Security）] > [電話セキュリティ プロファイル（Phone Security Profile）] の下で、Cisco Jabber For Tablet 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 Jabber for Tablet デバイス（Cisco Jabber for Tablet 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）] 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、ウィザードの手順を再び順番に実行します。

第 6 章

Cisco Unified Communications Manager 9.x の設定

この章では、Cisco Unified Communications Manager 9.x を使用した Cisco Jabber Video for iPad の設定方法について説明します。

（注） インスタント メッセージングおよびプレゼンスが使用されていない展開では、Cisco Unified Communications Manager IM and Presence Service の設定は任意です。

必須サービスの有効化と開始

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

手順

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

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

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

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

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

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

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

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

次の作業

必要に応じて、その他のサービスも開始します。 利用可能なサービスを確認したり、現在の導入においてその他のサービスが必要かどうかを判断したりする場合は、Cisco Unified Communications Manager に関する適切なマニュアルを参照してください。

ディレクトリ統合の設定

オンプレミス展開をセット アップするときは、次の両方を実行する必要があります。

- ディレクトリ サーバと同期する。
- ディレクトリ サーバで認証する。

ディレクトリ サーバとの同期

ディレクトリ サーバとの同期により、ディレクトリ サーバ内の連絡先データが Cisco Unified Communications Manager に複製されます。

同期の有効化

ディレクトリ サーバと同期するための最初の手順は、Cisco Unified Communications Manager で同期を有効にすることです。

手順

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

ステップ 2 [システム（System）] > [LDAP] > [LDAP システム（LDAP System）] を選択します。
[LDAP システムの設定（LDAP System Configuration）] ウィンドウが開きます。

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

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

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

次の作業

ユーザ ID の LDAP 属性を指定します。

ユーザ ID の LDAP 属性の指定

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

手順

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

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

重要 ユーザ ID の属性が `sAMAccountName` でデフォルトの IM アドレス スキームを使用している場合は、次のようにクライアントの設定ファイルで UserAccountName パラメータの値として属性を指定する必要があります。

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

設定で属性を指定せず、属性が `sAMAccountName` 以外の場合、クライアントはディレクトリ内の連絡先を解決できません。 この結果、ユーザはプレゼンスを取得せず、インスタント メッセージを送信または受信できません。

同期の実行

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

はじめる前に

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

- Cisco Unified Presence：[Cisco UP Sync Agent]
- Cisco Unified Communications Manager IM and Presence Service：[Cisco Sync Agent]

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

手順

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

ステップ 2 [新規追加（Add New）] を選択します。
[LDAP ディレクトリ（LDAP Directory）] ウィンドウが開きます。

ステップ 3 [LDAP ディレクトリ（LDAP Directory）] ウィンドウで必要な詳細情報を指定します。
指定できる値およびフォーマットの詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

ステップ 4 [保存（Save）] を選択します。

ステップ 5 [完全同期を今すぐ実施（Perform Full Sync Now）] を選択します。

（注） 同期プロセスの完了までに要する時間は、ディレクトリ内のユーザの数によって異なります。 ユーザ数が数千にもなる大規模なディレクトリの同期を実施する場合、そのプロセスにはある程度の時間がかかると予想されます。

ディレクトリ サーバのユーザ データは、Cisco Unified Communications Manager データベースに同期されます。 Cisco Unified Communications Manager は、その後、プレゼンス サーバ データベースにユーザ データを同期します。

ディレクトリ サーバでの認証

ディレクトリ サーバで認証するために、Cisco Unified Communications Manager を設定する必要があります。ユーザがクライアントにログインすると、プレゼンス サーバはその認証を Cisco Unified Communications Manager にルーティングします。 Cisco Unified Communications Manager は、その後、その認証をディレクトリ サーバに委任します。

手順

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

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

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

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

ステップ 5 [保存（Save）] を選択します。

サービス プロファイルの作成

Cisco Unified Communications Manager で追加したサービスの設定を含むサービス プロファイルを作成します。 ユーザのエンド ユーザ設定にサービス プロファイルを追加します。 これにより、クライアントは、利用可能なサービスの設定をサービス プロファイルから取得できます。

手順

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

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

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

ステップ 4 [サービス プロファイルの設定（Service Profile Configuration）] ウィンドウに次のように設定を入力します。

a) [名前（Name）] フィールドにサービス プロファイルの一意な名前を指定します。
b) 必要であれば、[説明（Description）] フィールドに説明を入力します。
c) 必要に応じて、[システム デフォルトのサービス プロファイルに設定（Make this the default service profile for the system）] を選択します。

ステップ 5 [保存（Save）] を選択します。

次の作業

インスタントメッセージングとプレゼンスのセットアップ手順を実行します。インスタントメッセージングとプレゼンスを有効にするのと同時に、エンドユーザ設定にサービスプロファイルを追加できます。

インスタントメッセージングとプレゼンスのセットアップ

インスタントメッセージング機能とプレゼンス機能により、ユーザは、インスタントメッセージを送受信すること、および在席ステータスを公開および表示することができます。

インスタントメッセージングとプレゼンスをセットアップし、配置を開始します。チャットと在席ステータスの機能のセットアップに成功した後は、他のサービスを追加し、音声、ビデオ、ボイスメールなどの機能をプロビジョニングすることで、配置を構築できます。

メッセージングの設定の有効化

インスタント メッセージング機能を有効にし、設定します。

手順

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

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

ステップ 3 次のオプションを選択します。

- インスタント メッセージを有効にする（Enable instant messaging）

ステップ 4 他のメッセージング設定も適切に選択します。

ステップ 5 [保存（Save）] を選択します。

重要 Cisco Jabber Video for iPad は、Cisco Unified Communications Manager IM and Presence Service バージョン 9.0.x の [プレゼンスの設定（Presence Settings）] ウィンドウで次の設定をサポートしていません。

- ユーザの通話中に DND ステータスを使用する（Use DND status when user is on the phone）
- ユーザがミーティングに参加しているときに DND ステータスを使用する（Use DND status when user is in a meeting）
- クライアントでのインスタントメッセージ履歴のログ記録を可能にする（Allow clients to log instant message history）

プレゼンス サブスクリプション要求のプロンプト設定

社内の連絡先からのプレゼンス サブスクリプション要求のプロンプトを有効、無効のいずれかにすることができます。

クライアントは、社外の連絡先からのプレゼンス サブスクリプション要求には、ユーザに許可を求めるプロンプトを常に表示します。

手順

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

ステップ 2 [プレゼンス（Presence）] > [設定（Settings）] の順に選択します。
[プレゼンスの設定（Presence Settings）] ウィンドウが開きます。

ステップ 3 [確認プロンプトなしで、ユーザが他のユーザのプレゼンス ステータスを表示できるようにする（Allow users to view the availability of other users without being prompted for approval）] を選択し、プロンプトを無効にして、社内からのすべてのプレゼンス サブスクリプション要求を自動的に許可します。
このオプションには、次の値があります。

オン

クライアントはプレゼンス サブスクリプション要求ではユーザにプロンプトを表示しません。 クライアントはユーザにプロンプトを表示せずに、すべてのプレゼンス サブスクリプション要求を自動的に許可します。

オフ

クライアントは、プレゼンス サブスクリプション要求を許可するかどうか尋ねるプロンプトをユーザに表示します。 この設定では、ユーザの在席ステータスを社内のほかのユーザが見られる状態である必要があります。

ステップ 4 [保存（Save）] を選択します。

インスタント メッセージ/プレゼンス サービスを追加する

インスタント メッセージングとプレゼンス機能をユーザに提供します。

手順

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

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

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

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

ステップ 5 [次へ（Next）] を選択します。

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

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

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

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

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

ステップ 7 [保存（Save）] を選択します。

次の作業

サービス プロファイルにインスタント メッセージ/プレゼンス サービスを追加します。

インスタント メッセージ/プレゼンス サービスを適用する

Cisco Unified Communications Manager でインスタント メッセージおよびプレゼンス サービスを追加した後、クライアントがその設定を取得できるようにするために、そのインスタント メッセージおよびプレゼンス サービスをサービス プロファイルに適用する必要があります。

はじめる前に

サービス プロファイルを作成します。

手順

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

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

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

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

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

ステップ 5 [保存（Save）] を選択します。

ディレクトリ サービスを追加する

ディレクトリ検索機能をユーザに提供するディレクトリ サービスを追加するには、次の手順を実行します。

手順

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

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

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

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

ステップ 5 [次へ（Next）] を選択します。

ステップ 6 次の手順に従って、ディレクトリ サービスの詳細情報を設定します。

a) [製品のタイプ（Product Type）] ドロップダウン リストから、[ディレクトリ（Directory）] を選択します。

b) [名前（Name）] フィールドにサービスの名前を入力します。 入力した名前は、プロファイルにサービスを追加する際に表示されます。 入力する名前は必ず、一意的でわかりやすく、かつ意味が通じるものにしてください。
c) 必要であれば、[説明（Description）] フィールドに説明を入力します。
d) [ホスト名/IP アドレス（Host Name/IP Address）] フィールドに、CTI サービスのアドレスを入力します。
e) LDAP サーバが使用するポート番号を指定します。 デフォルトは、次のとおりです。
a) TCP：389
b) TLS：636
c) グローバル カタログ：3268/3269

ステップ 7 [保存（Save）] を選択します。

次の作業

サービス プロファイルにディレクトリ サービスを追加します。

ディレクトリ サービスの適用

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

はじめる前に

サービス プロファイルを作成します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。
ステップ 2 [ユーザ管理（User Management）]>[ユーザ設定（User Settings）]>[サービス プロファイル（Service Profile）] の順に選択します。
[サービス プロファイルの検索/一覧表示（Find and List Service Profiles）] ウィンドウが表示されます。
ステップ 3 目的のサービス プロファイルを検索し、それを選択します。
[サービス プロファイルの設定（Service Profile Configuration）] ウィンドウが開きます。
ステップ 4 [ディレクトリプロファイル（Directory Profile）] セクションで、[基本サービス（Primary service）] を選択します。
（注） 設定には 3 種類のサービス オプションが設定可能ですが、アプリケーションは [基本サービス（Primary service）] の値の使用のみをサポートします。

ステップ 5 [ログインしたユーザのクレデンシャルを使用（Use Logged On User Credential）] を選択します。

ステップ 6 LDAP サーバに対する認証アカウントを [ユーザ名（Username）] および [パスワード（Password）] フィールドで指定します。

ステップ 7 [検索ベース（Search Base）] フィールドに LDAP サーバの検索ベースを指定します。

ステップ 8 [保存（Save）] を選択します。

ユーザの設定を行う

ユーザの設定を行う場合は、インスタントメッセージおよびプレゼンスを有効にし、サービスプロファイルをユーザに追加します。

ユーザの設定を個別に行う

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

手順

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

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

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

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

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

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

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

重要 **Cisco Unified Communications Manager バージョン 9.x のみ**：インスタント メッセージとプレゼンス機能のみ（IM のみ）のユーザである場合、[デフォルトを使用（Use Default）] を選択する必要があります。

IM のみのユーザの場合、Cisco Unified Communications Manager バージョン 9.x では [UC サービス プロファイル（UC Service Profile）] ドロップダウン リストの選択内容に関係なく、常にデフォルトのサービス プロファイルが適用されます。

ステップ 6 [保存（Save）] を選択します。

複数ユーザの設定を一括で行う

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

手順

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

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

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

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

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

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

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

重要 **Cisco Unified Communications Manager バージョン 9.x のみ**：インスタント メッセージとプレゼンス機能のみ（IM のみ）のユーザである場合、[デフォルトを使用（Use Default）] を選択する必要があります。

IM のみのユーザの場合、Cisco Unified Communications Manager バージョン 9.x では [UC サービス プロファイル（UC Service Profile）] ドロップダウン リストの選択内容に関係なく、常にデフォルトのサービス プロファイルが適用されます。

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

ステップ 8 [送信（Submit）] を選択します。

音声機能およびビデオ機能のセットアップ

ユーザにソフトフォン デバイスおよびデスクフォン デバイスをプロビジョニングします。 ダイヤル プランのマッピングを設定し、音声機能およびビデオ機能をセットアップするためのその他の必須タスクを実行します。

はじめる前に

ユーザにデバイスをプロビジョニングする前に、付加ライセンスに関する情報など、Cisco Unified Communications Manager のライセンス要件を確認する必要があります。

ソフトフォン デバイスの作成

タブレット フォン デバイスの作成

iPad で使用するソフトフォン デバイスを作成するには、この手順を使用します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] インターフェイスを開きます。
[電話の検索と一覧表示（Find and List Phones）] ウィンドウが開きます。

ステップ 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）] を選択します。

ステップ 4 [電話のタイプ（Phone Type）] ドロップダウン リストで [Cisco Jabber for Tablet] を選択し、[次へ（Next）] をクリックします。
[電話の設定（Phone Configuration）] ウィンドウが開きます。

ステップ 5 デバイスの名前を [デバイス名（Device Name）] フィールドに指定します。 タブレット デバイス名には **TAB *username*** フォーマットを使用する必要があります。 たとえば、Tanya Adams という名前で、ユーザ名が tadams であるユーザのデバイスを作成するとします。 この場合、デバイス名として ***TABTADAMS*** を指定します。

（注） タブレット フォン デバイス名は大文字にする必要があります。

ステップ 6 必要に応じて、[電話の設定（Phone Configuration）] ウィンドウで設定を指定します。 このウィンドウの設定の詳細については、『Cisco Unified Communications Manager』のマニュアルの「*Phone Setup*」のトピックを参照してください。

ステップ 7 [保存（Save）] を選択します。
デバイスが正常に追加されたとのメッセージが表示されます。[電話の設定（Phone Configuration）] ウィンドウで [割り当て情報（Association Information）] セクションが利用可能になります。

デバイスに電話番号を追加する

Cisco Unified Communications Manager で、デバイスに電話番号を追加する必要があります。 このトピックでは、デバイスの作成後に [デバイス（Device）] > [電話（Phone）] メニュー オプションを使用して電話番号を追加する手順について説明します。 このメニューオプションから表示されるのは、電話機モデルまたはCTIルートポイントに適用される設定のみです。 電話番号を設定するためのさまざまなオプションについては、Cisco Unified Communications Manager のマニュアルを参照してください。

手順

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

ステップ 2 [新規 DN を追加（Add a new DN）] を選択します。
[電話番号の設定（Directory Number Configuration）] ウィンドウが開きます。

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

ステップ 4 その他に必要な設定があれば、それらをすべて指定します。

ステップ 5 次の手順に従って、エンドユーザに電話番号を関連付けます。

a) [回線に関連付けられているユーザ（Users Associated with Line）] セクションに移動します。

b) [エンドユーザの関連付け（Associate End Users）] を選択します。
[ユーザの検索と一覧表示（Find and List Users）] ダイアログボックスが開きます。

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

d) 対象のユーザをリストから選択します。

e) [選択項目の追加（Add Selected）] を選択します。
選択されたユーザがボイスメール プロファイルに追加されます。

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。
[設定の適用（Apply Configuration）] ウィンドウが開きます。

ステップ 8 [設定の適用（Apply Configuration）] ウィンドウに表示されるプロンプトに従って設定を適用します。

ユーザの関連付けに関する設定

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

手順

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

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

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

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

ステップ 5 [デバイス情報（Device Information）] セクションを探します。

ステップ 6 [デバイスの割り当て（Device Association）] を選択します。
[ユーザ デバイス割り当て（User Device Association）] ウィンドウが開きます。

ステップ 7 ユーザを割り当てるデバイスを選択します。

ステップ 8 [選択/変更の保存（Save Selected/Changes）] を選択します。

ステップ 9 [ユーザ管理（User Management）] > [エンド ユーザ（End User）] の順に選択し、[ユーザの検索と一覧表示（Find and List Users）] ウィンドウに戻ります。

ステップ 10 一覧から同じユーザを探し、選択します。
[エンド ユーザの設定（End User Configuration）] ウィンドウが表示されます。

ステップ 11 [権限情報（Permissions Information）] セクションを探します。

ステップ 12 [アクセス コントロール グループに追加（Add to Access Control Group）] を選択します。
[アクセス コントロール グループの検索と一覧表示（Find and List Access Control Groups）] ダイアログボックスが開きます。

ステップ 13 ユーザを割り当てるアクセス コントロール グループを選択します。
ユーザを、少なくとも次のアクセス コントロール グループに割り当てる必要があります。

- Standard CCM End Users
- Standard CTI Enabled

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

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

ステップ 14 [選択項目の追加（Add Selected）] を選択します。

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

ステップ 15 [エンド ユーザの設定（End User Configuration）] ウィンドウで [保存（Save）] を選択します。

TFTP サーバ アドレスの指定

クライアントは TFTP サーバからデバイス設定を取得します。 そのため、ユーザにデバイスをプロビジョニングする場合、TFTP サーバ アドレスを指定する必要があります。

Cisco Unified Communications IM and Presence での TFTP サーバの指定

次の手順を実行して、Cisco Unified Communications IM and Presence で TFTP サーバのアドレスを指定します。

手順

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

ステップ 2 [アプリケーション（Application）]>[レガシー クライアント（Legacy Clients）]>[設定（Settings）] の順に選択します。
[レガシー クライアントの設定（Legacy Client Settings）] ウィンドウが開きます。

ステップ 3 [レガシー クライアントのセキュリティ設定（Legacy Client Security Settings）] セクションを探します。

ステップ 4 次のフィールドで、プライマリおよびバックアップの TFTP サーバの IP アドレスを指定します。

- プライマリ TFTP サーバ（Primary TFTP Server）

（注） TFTP の冗長性はサポートされません。

ステップ 5 [保存（Save）] を選択します。

ハイブリッド クラウドベース展開での TFTP サーバの指定

ハイブリッド クラウドベース展開では、Cisco WebEx 管理ツールで TFTP サーバ アドレスを指定できます。

手順

ステップ 1 Cisco WebEx 管理ツールを開きます。

ステップ 2 [設定（Configuration）] タブを選択します。

ステップ 3 [追加サービス（Additional Services）] セクションで [Unified Communications] を選択します。
[Unified Communications] ウィンドウが開きます。

ステップ 4 [クラスタ（Clusters）] タブを選択します。

ステップ 5 適切なクラスタをリストから選択します。
[クラスタの編集（Edit Cluster）] ウィンドウが開きます。

ステップ 6 [Cisco Unified Communications Manager サーバの設定（Cisco Unified Communications Manager Server Settings）] セクションで [サーバの詳細設定（Advanced Server Settings）] を選択します。

ステップ 7 [TFTP サーバ（TFTP Server）] フィールドでプライマリ TFTP サーバの IP アドレスを指定します。

ステップ 8 [バックアップ サーバ 1（Backup Server #1）] フィールドと [バックアップ サーバ 2（Backup Server #2）] フィールドでバックアップ TFTP サーバの IP アドレスを指定します。

ステップ 9 [保存（Save）] を選択します。
[クラスタの編集（Edit Cluster）] ウィンドウが閉じます。

ステップ 10 [Unified Communications] ウィンドウで [保存（Save）] を選択します。

デバイスのリセット

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

手順

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

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

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

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

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

ステップ 6 対象の電話番号設定を選択します。
[電話番号の設定（Directory Number Configuration）] ウィンドウが開きます。

ステップ 7 [リセット（Reset）] を選択します。

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

ステップ 8 [リセット（Reset）] を選択します。

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

CCMCIP プロファイルの作成

クライアントは、CCMCIP サーバからユーザのデバイス リストを取得します。

手順

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

ステップ 2 [アプリケーション（Application）] > [レガシー クライアント（Legacy Clients）] > [CCMCIP プロファイル（CCMCIP Profile）] の順に選択します。
[CCMCIP プロファイルの検索と一覧表示（Find and List CCMCIP Profiles）] ウィンドウが開きます。

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

ステップ 4 CCMCIP プロファイルでサービスの詳細を次のように指定します。

a) プロファイルの名前を [名前（Name）] フィールドに指定します。
b) [プライマリ CCMCIP ホスト（Primary CCMCIP Host）] フィールドで、プライマリ CCMCIP サービスのアドレスを指定します。
c) [バックアップ CCMCIP ホスト（Backup CCMCIP Host）] フィールドで、バックアップ CCMCIP サービスのホスト名または IP アドレスを指定します。
d) [サーバ証明書の確認（Server Certificate Verification）] はデフォルト値のままとします。

ステップ 5 CCMCIP プロファイルに次のようにユーザを追加します。

a) [プロファイルにユーザを追加（Add Users to Profile）] を選択します。
[ユーザの検索と一覧表示（Find and List Users）] ダイアログボックスが開きます。
b) [ユーザを次の条件で検索（Find User where）] フィールドで適切なフィルタを指定した後、[検索（Find）] を選択してユーザのリストを取得します。
c) 対象のユーザをリストから選択します。
d) [選択項目の追加（Add Selected）] を選択します。
選択されたユーザが CCMCIP プロファイルに追加されます。

ステップ 6 [保存（Save）] を選択します。

ダイヤル プランのマッピング

Cisco Unified Communications Manager のダイヤリング ルールがディレクトリのダイヤリング ルールと一致するように、ダイヤル プランのマッピングを設定します。

アプリケーション ダイヤル ルール（Application Dial Rules）

アプリケーション ダイヤル ルールにより、ユーザがダイヤルする電話番号の桁数の追加および削除が自動的に行われます。 アプリケーション ダイヤル ルールにより、ユーザがクライアントからダイヤルする番号が操作されます。

たとえば、7 桁の電話番号の先頭に自動的に 9 を追加して外線にアクセスするように、ダイヤル ルールを設定できます。

ディレクトリ検索ダイヤル ルール（Directory Lookup Dial Rules）

ディレクトリ検索ダイヤル ルールによって、発信者 ID の番号が、クライアントがディレクトリで検索できる番号に変換されます。 定義する各ディレクトリ検索ルールには、先頭の数字および番号の長さに基づいてどの数字を変換するかを指定します。

たとえば、10 桁の電話番号から市外局番と 2 桁の局番を自動的に削除するように、ディレクトリ検索ルールを作成できます。 このタイプのルールでは、たとえば、`4089023139` を `23139` に変換します。

ダイヤル ルールの発行

Cisco Unified Communications Manager バージョン 8.5 もしくはそれ以前のバージョンは、ダイヤル ルールをクライアントに自動的に発行しません。 このため、ダイヤル ルールを発行するには、COP ファイルを導入する必要があります。 この COP ファイルによって、ダイヤル ルールが Cisco Unified Communications Manager データベースから TFTP サーバ上の XML ファイルにコピーされます。 その後、クライアントは、その XML ファイルをダウンロードしてダイヤル ルールにアクセスできます。

メモ Cisco Unified Communications Manager バージョン 8.5 もしくはそれ以前のバージョンで、ダイヤル ルールを変更または修正するたびに、COP ファイルを展開する必要があります。

はじめる前に

1. Cisco Unified Communications Manager でダイヤル ルールを作成します。
2. `Cisco.com` から Cisco Jabber 管理パッケージをダウンロードします。

手順

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

ステップ 2 [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 3 [次へ（Next）] を選択します。

ステップ 4 [次へ（Next）] を選択し、[インストール（Install）] を選択します。

ステップ 5 TFTP サービスを再起動します。

ステップ 6 ブラウザでダイヤル ルールの XML ファイルを開き、TFTP サーバでそれらのファイルが利用可能であることを確認します。

a) `http://tftp_server_address:6970/CUPC/AppDialRules.xml` に移動します。

b) `http://tftp_server_address:6970/CUPC/DirLookupDialRules.xml` に移動します。

ブラウザで `AppDialRules.xml` と `DirLookupDialRules.xml` にアクセスできる場合、クライアントはダイヤル ルールをダウンロードできます。

ステップ 7 TFTP サービスを実行する Cisco Unified Communications Manager のインスタンスごとに前述の手順を繰り返します。

次の作業

Cisco Unified Communications Manager のインスタンスごとに前述の手順を繰り返した後、クライアントを再起動します。

ボイスメールのセットアップ

ボイスメールをセットアップすることで、ユーザはボイスメール メッセージを受信し、音声コールの着信をボイスメール サービスにリダイレクトできます。 ボイスメールのセットアップ タスクの一部として、メールストアを設定して、クライアントでビジュアル ボイスメールを有効にすることもできます。

Cisco Unity Connection の設定

Cisco Unity Connection を設定するには、ユーザに IMAP アクセスを提供するユーザ プロファイルを作成する必要があります。 具体的な設定作業内容については、Cisco Unity Connection のマニュアルを参照してください。

手順

ステップ 1 Cisco Unity Connection のユーザ プロファイルを作成します。

ステップ 2 ユーザに IMAP アクセスを提供します。

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

b) [サービス クラス（Class of Service）] を選択します。
[サービス クラスの編集（Edit Class of Service）] ウィンドウが開きます。

c) [ライセンスされた機能（Licensed Features）] セクションを探します。

d) [IMAP クライアントやシングル インボックスを使用したボイスメールへのアクセスをユーザに許可する（Allow Users to Access Voice Mail Using an IMAP Client and/or Single Inbox）] を選択します。

e) [メッセージ本文へのアクセスを IMAP ユーザに許可する（Allow IMAP Users to Access Message Bodies）] を選択します。

f) [保存（Save）] を選択します。

ステップ 3 セキュリティ メッセージへのアクセスを有効化します。

a) [システム設定（System Settings）] > [詳細（Advanced）] > [API 設定（API Settings）] に移動します。

b) [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）] を選択します。

ボイスメール サービスを追加する

ユーザがボイス メッセージを受信できるようにします。

手順

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

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

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

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

ステップ 5 [次へ（Next）] を選択します。

ステップ 6 ボイスメール サービスの詳細を次のように指定します。

製品のタイプ（Product Type）

[Unity Connection] を選択します。

名前（Name）

サーバのわかりやすい名前（たとえば、PrimaryVoicemailServer）を入力します。

説明（Description）

任意で説明を入力します。

ホスト名/IP アドレス（Hostname/IP Address）

次のいずれかの形式で、ボイスメール サーバのアドレスを入力します。

- ホストネーム（Hostname）
- IP アドレス（IP Address）
- FQDN

ポート（Port）

ボイスメール サーバに接続するポートを入力します。

プロトコル タイプ（Protocol Type）

適切なプロトコルを選択します。

ステップ 7 [保存（Save）] を選択します。

次の作業

サービス プロファイルにボイスメール サービスを追加します。

ボイスメール サービスを適用する

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

はじめる前に

すでに存在しないか、ボイスメール用に別のサービスプロファイルが必要な場合は、サービスプロファイルを作成します。

手順

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

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

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

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

a) 次のドロップダウン リストから、サービスを最大 3 つ選択します。

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

b) クレデンシャルとボイスメール サービスを同期させる場合は、[ボイスメール サービスのクレデンシャル ソース（Credentials source for voicemail service）] ドロップダウン リストから [Unified CM - IM/Presence] を選択します。
[Unified CM - IM/Presence] を選択した場合、ボイスメール サービスへのログインにはインスタント メッセージおよびプレゼンスのクレデンシャルが使用されます。 このため、ユーザはクライアントでボイスメール サービスのクレデンシャルを入力する必要ありません。

（注） [Web 会議（Web conferencing）] は選択しないでください。 このオプションを選択した場合、ボイスメール サービスへのログインには、会議のクレデンシャルが使用されます。 現時点では、会議クレデンシャルとは同期できません。

ステップ 5 [保存（Save）] を選択します。

メールストア サービスを追加する

メールストア サービスにより、ユーザはビジュアル ボイスメール機能を使用できます。

手順

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

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

ステップ 3 [新規追加（Add New）] を選択します。

[UC サービスの設定（UC Service Configuration）] ウィンドウが開きます。

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

ステップ 5 [次へ（Next）] を選択します。

ステップ 6 次の手順に従って、メールストア サービスの詳細情報を設定します。

名前（Name）

サーバのわかりやすい名前（たとえば、PrimaryMailStoreServer）を入力します。

説明（Description）

任意で説明を入力します。

ホスト名/IP アドレス（Hostname/IP Address）

次のいずれかの形式で、メールストア サーバのアドレスを入力します。

- ホストネーム（Hostname）
- IP アドレス（IP Address）
- FQDN

ポート（Port）

メールストア サーバに接続するポートを入力します。

プロトコル タイプ（Protocol Type）

適切なプロトコルを選択します。

ステップ 7 [保存（Save）] を選択します。

次の作業

サービス プロファイルにメールストア サービスを追加します。

メールストア サービスを適用する

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

はじめる前に

すでに存在しないか、メールストア サービス用に別のサービス プロファイルが必要な場合は、サービス プロファイルを作成します。

手順

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

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

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

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

a) 次のドロップダウン リストから、サービスを最大 3 つ選択します。

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

b) 次の各フィールドに適切な値を指定します。

- Inbox フォルダ（Inbox Folder）
- ごみ箱フォルダ（Trash Folder）
- ポーリング間隔（Polling Interval）

c) メールストアが IMAP の UIDPLUS 拡張子をサポートしている場合は、[デュアルフォルダモードを使用可能にする（Allow dual folder mode）] を選択します。

ステップ 5 [保存（Save）] を選択します。

取得とリダイレクションの設定

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

手順

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

ステップ 2 ボイスメール パイロットを設定します。

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

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

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

d) [保存（Save）] を選択します。

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

a) [拡張機能（Advanced Features）] > [ボイスメール（Voice Mail）] > [ボイスメール プロファイル（Voice Mail Profile）] の順に選択します。
[ボイスメール プロファイルの検索と一覧表示（Find and List Voice Mail Profiles）] ウィンドウが開きます。

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

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

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

e) [保存（Save）] を選択します。

ステップ 4 電話番号設定でボイスメール プロファイルを指定します。

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

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

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

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

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

f) [電話番号の設定（Directory Number Settings）] セクションを探します。

g) [ボイスメール プロファイル（Voice Mail Profile）] ドロップダウン リストからボイスメール プロファイルを選択します。

h) [保存（Save）] を選択します。

第 7 章

CiscoTelePresenceVideoCommunicationServer の設定

この章では、Cisco TelePresence Video Communication Server（VCS）を使用した Cisco Jabber Video for iPad の設定に関する総合的な情報を提供します。

前提条件

次のタスクを実行します。

- 使用する Cisco VCS および Cisco TMS（TelePresence Management Suite）のバージョンが次の要件を満たしていることを確認します。

製品	必要なバージョン
TMS	13.1 以降
VCS	6.0 以降

- NTLM 認証がネットワーク環境で必要かどうかを確認します。 その場合、VCS および Cisco Jabber Video for iPad で NTLM 認証をセットアップします。 手順については、http://www.cisco.com/en/US/products/ps11337/products_installation_and_configuration_guides_list.html で入手できる、お使いのリリースに対応した『*Cisco TelePresence Video Communication Server Authenticating Devices Deployment Guide*』を参照してください。

プロビジョニング用の TMS の設定

Cisco Jabber Video for iPad に VCS を導入するには、適切な設定でユーザ デバイスをプロビジョニングします。 必要な設定は TMS で追加および管理します。 その後、それらのデータを VCS に転送し、VCS 上で稼働しているプロビジョニング サーバを介してデバイスに配布します。

次の 2 つの必須手順を実行して、プロビジョニング用の TMS を設定します。

デバイス アドレス パターンの定義

デバイス アドレス パターンとは、TMS Provisioning Extension（TMSPE）が、プロビジョニングされたデバイスに対してアドレスを生成する際に使用するテンプレートです。 TMSPE がデバイスにユーザを接続できるように、デバイス アドレス パターンを割り当てます。

Cisco Jabber Video for iPad にデバイス アドレス パターンを指定するには、jabbertablet に属性 `{device.model}` を設定します。 必要に応じて、jabbertablet を jabber に変換するエイリアスを追加して、名前付けを簡略化します。

アドレス パターンの作成に関する詳細については、http://www.cisco.com/en/US/products/ps11472/prod_installation_guides_list.html にある『*Cisco TelePresence Management Suite Provisioning Extension Deployment Guide*』を参照してください。

テンプレートのプロビジョニングの設定およびユーザへの割り当て

Cisco Jabber Video for iPad には、特定のテンプレート、つまりアプリケーションでサポートされる、可能なすべての設定を含む XML ファイルが必要です。 テンプレートをダウンロードして TMS にアップロードすると、そのテンプレートを設定してユーザのグループに割り当てることができます。

手順の各ステップの詳細については、次の該当するマニュアルを参照してください。

- TMS バージョン 13.2 以前に含まれる TMS Agent Legacy を使用している場合は、http://www.cisco.com/en/US/products/ps11338/products_installation_and_configuration_guides_list.html に

ある『*Cisco TelePresence Management Suite Agent Legacy Deployment Guide*』を参照してください。

- TMS バージョン 13.2 以降に含まれる TMS Provisioning Extension（TMSPE）を使用している場合は、http://www.cisco.com/en/US/products/ps11472/prod_installation_guides_list.html にある『*Cisco TelePresence Management Suite Provisioning Extension Deployment Guide*』を参照してください。

手順

ステップ 1 テンプレートを http://www.cisco.com/cisco/software/navigator.html?mdfid=280443139&flowid=29241 からローカル サーバにダウンロードします。

ステップ 2 テンプレートまたはテンプレート スキーマを TMS にアップロードします。
TMSPE では「テンプレート スキーマ」という用語が使用されていますが、TMS Agent Legacy では「テンプレート」という用語が使用されています。

ステップ 3 これらのサーバ アドレス、およびその他の必要な設定をテンプレートに追加します。

- パブリック SIP サーバ アドレス（Public SIP Server Address）
- SIP サーバ アドレス（SIP Server Address）
- 電話帳サーバ URI（Phone Book Server URI）

ステップ 4 テンプレートを適切なユーザのグループに割り当てます。
グループに割り当てるテンプレートは、グループ内のすべてのユーザ、すべてのサブグループ、およびサブグループ内のすべてのユーザが継承します。 テンプレートを個別のユーザに直接割り当てることはできません。

（注） シスコでは、すべての VCS テンプレートについて、クライアントとの下位互換性を保持することを推奨します。 各 VCS の特定のデバイス タイプには複数のテンプレートを対応付けることが可能で、使用するテンプレートをプロビジョニング サーバに示すのは、クライアント登録要求です。 プロビジョニング サーバは、要求の [モデル（Model）] および [バージョン（Version）] フィールドを使用して正しいテンプレートを決定します。 要求の [バージョン（Version）] 文字列がそのモデルのすべてのインストール済みテンプレートよりも低い場合、プロビジョニング要求は失敗します。 要求の [バージョン（Version）] 文字列がそのモデルのインストールされたテンプレートより高い場合は、同等またはより低いバージョンの最も近い一致するテンプレートを検索するベストエフォートの試行が行われます。

プロビジョニング オプションの概要

プロビジョニングでは、VCS が Cisco Jabber Video for iPad をどのように使用するかを制御する設定を指定することができます。 VCS への登録後、Cisco Jabber Video for iPad は Cisco TMS Agent からプロビジョニング情報を受信し、それに基づいて機能します。

次の表には、Cisco Jabber Video for iPad に適用可能なプロビジョニング オプションの説明が示されており、それらの使用方法に関するヒントも記載されています。

フィールド	デフォルト	説明
パスワードの保存をユーザに許可する	on	このオプションでは、アカウントのパスワード ポリシーを決定します。 • [on]：ユーザがパスワードを保存することを許可します。 • [off]：ユーザがパスワードを保存することを禁止します。
自動サインアウト（Automatic Sign-out）	UseClientSetting	このオプションは、Cisco Jabber の自動サインアウト方法を指定します。 • [UseClientSetting]：自動サインアウトはクライアント設定によって制御されます。 • [NeverSignOut]：Cisco Jabber は自動サインアウトしません。 • [15Minutes]：Cisco Jabber はバックグラウンドで 15 分経過した後に自動サインアウトします。 • [30Minutes]：Cisco Jabber はバックグラウンドで 30 分経過した後に自動サインアウトします。 • [1Hour]：Cisco Jabber はバックグラウンドで 1 時間経過した後に自動サインアウトします。 • [2Hour]：Cisco Jabber はバックグラウンドで 2 時間経過した後に自動サインアウトします。 • [4Hour]：Cisco Jabber はバックグラウンドで 4 時間経過した後に自動サインアウトします。 • [8Hour]：Cisco Jabber はバックグラウンドで 8 時間経過した後に自動サインアウトします。 • [SignOutOnExit]：Cisco Jabber はバックグラウンドに移ってすぐに自動サインアウトします。

フィールド	デフォルト	説明
帯域幅プローブ自動スケジューリング（Bandwidth Prober Auto Scheduling）	オフ（Off）	このオプションでは、帯域幅プロービングを有効にできます。 帯域幅プロービングには、次の設定もプロビジョニングされている必要があります。 • TurnAuthPassword • TurnAuthUsername • TurnServer
帯域幅プローブ時間（Bandwidth Prober Time）	0	サインイン後、Jabber ビデオはクライアントと TURN サーバ間の帯域幅品質について TURN リレー サーバをプロービングします。 この設定により、プロービングの期間が秒単位で決定されます。 • 最小値：5 • 最大値：600 • 推奨値：30 プロビジョニングされた時間は、プロビジョニングされた最大帯域幅まで256 kb/s の間隔に分割されます。
パブリック帯域幅プローブ自動スケジューリング（Public Bandwidth Prober Auto Scheduling）	[帯域幅プローブ自動スケジューリング（Bandwidth Prober Auto Scheduling）] に設定された値を使用します。	帯域幅プロービングを有効化するには、この設定が *On* である必要があります。 帯域幅プロービングでは、次の設定もプロビジョニングする必要があることに注意してください。 • TurnAuthPassword • TurnAuthUsername • TurnServer
ClearPath	オン（On）	ClearPath は、最適ではないネットワークにおけるパケット損失の悪影響を最小限に抑える Cisco TelePresence ソリューションです。 これらのメカニズムの間ではH.264 固有のエラー回復手法、デコーダからのフィードバック、および前方誤り訂正（FEC）が使用されます。 ClearPath が有効になるためには、両方のコール参加者が、ClearPath に対応したデバイスを使用している必要があります。

フィールド	デフォルト	説明
デフォルト メディアタイプ候補（Default Mediatype Candidate）	ホスト（Host）	これは、次のときに使用するアドレスです。 • ICE ネゴシエーションの完了前。 • ICE が失敗した場合。 • リモート側が ICE に対応していない場合。 次のオプションを使用できます。 • [ホスト（Host）]：ローカル ネットワーク アドレス • [Rflx]：組織のネットワークの外側から見える企業のパブリック IP アドレス（パブリック IP） • [リレー（Relay）]：TURN リレー サーバのアドレス Cisco Jabber Video for iPad を他のほとんどのデバイスが ICE に対応していない環境に導入する場合は、[リレー（Relay）] を使用できます。
暗号化ポリシー（Encryption Policy）	自動（Auto）	アカウントの暗号化ポリシーを決定します。 このオプションは、SIP 通信（トランスポート TLS または TCP）とメディア通信（SRTP または SRTP なし）の両方に影響します。 コールを暗号化する場合、SIP 通信とメディア通信の両方が暗号化される必要があり、すべての通話者が暗号化をサポートしている必要があります。 暗号化されたメディア通信は、128 ビットの高度暗号化規格（AES）を使用した Secure Real-time Transport Protocol（SRTP）によって送信されます。 暗号化ポリシーの設定は、Cisco TMS の [システム（Systems）] > [プロビジョニング（Provisioning）] > [ディレクトリ（Directory）] の設定に従ってクライアントにプロビジョニングされます。 SIP 通信を暗号化するか（TLS）しないか（TCP）は、[TLS/TCP の使用（Force TLS/TCP）] によって定されます。 TLS バージョン 1.0。 [SRTP の使用あり/なし（Force/No Srtp）]：メディア通信が暗号化されているかいないかを決定します。 [自動（Auto）] の場合、クライアントは暗号化されたコールを試行しますが、暗号化できない場合は、暗号化されていないコールを許可します。

フィールド	デフォルト	説明
ICE	オフ（Off）	Interactive Connectivity Establishment（ICE）は、コール参加者間のメディアの伝送に最適なパスを動的に検出します。
最大受信帯域幅（Maximum In Bandwidth）	512 KB/s	指定した値により、ユーザ アカウントでデータの送受信を行うために許可される最大帯域幅が決定されます。 高い帯域幅は、良好なビデオ品質に直接結び付きます。 しかし、帯域幅を制御すれば、アプリケーションがその能力を超えてデータを受信または送信しようとするのを防ぐことができ、結果としてパケット損失、ジッター、および低いビデオ品質の発生を回避できます。
最大送信帯域幅（Maximum Out Bandwidth）	384 KB/s	
メディア ポート範囲の末尾（Media Port Range End）	21900	ビデオとオーディオの通信で使用されるポート番号の上限または下限。 セキュリティとファイアウォールに関する問題を制御するために、これらを設定できます。 10個以上のポートが含まれる範囲を指定する必要があります。そうしない場合、Cisco Jabber Video for iPad はデフォルトに戻ります。
メディア ポート範囲の始端（Media Port Range Start）	21000	
MNS モード（MNS Mode）	オフ（Off）	このオプションを有効にすると、リレー対象のメディアは、容量が保証されているプライベート HD リンク経由で常にリレーされ、ビデオの品質が確保されます。 この設定を使用するには、ICE が有効になっている必要があります。 プライベートの専用リンクは、Media Network Services などの企業から提供されます。
Multiway 参加者 URI（Multiway Participant URI）		Multiway が開始されると、参加者は、この Uniform Resource Identifier（URI）に誘導されます。
電話帳サーバ URI（Phone Book Server URI）		アカウントが Cisco TMS Agent データベース内の他のアカウントを検索できるようになります。 次の形式で URI を設定します。 phonebook@<sip_domain>.com **重要** 値を指定しなければ、Cisco Jabber Video for iPad で連絡先を検索できません。

フィールド	デフォルト	説明
プレゼンス サーバ URI（Presence Server URI）		アカウントがプレゼンス ステータスを VCS サーバに送信できるようになります。 次の形式で URI を設定します。 presence@<sip_domain>.com （注） Cisco Jabber Video for iPad は、サーバが認識されていない場合、Cisco WebEx Messenger から提供されるプレゼンス ステータスを使用します。 値を指定しなければ、Cisco Jabber Video for iPad はプレゼンス ステータスをパブリッシュできず、オフラインであると見なされます。
パブリック デフォルト メディアタイプ候補（Public Default Mediatype Candidate）	[デフォルト メディアタイプ候補（Default Mediatype Candidate）] に設定された値を使用。 動的に変化します	これは、次のときに使用するアドレスです。 • ICE ネゴシエーションの完了前。 • ICE が失敗した場合。 • リモート側が ICE に対応していない場合。 次のオプションを使用できます。 • [ホスト（Host）]：ローカル ネットワーク アドレス • [Rflx]：組織のネットワークの外側から見える企業のパブリック IP アドレス（パブリック IP） • [リレー（Relay）]：TURN リレー サーバのアドレス ユーザが組織のネットワークの外側から接続する場合は、[リレー（Relay）]を使用することを推奨します。ICE ネゴシエーションは完了するまでに数秒の時間がかかります。そのため、TURN リレーを使用すれば、コールを開始したときからメディアがファイアウォールを通過するのに役立ちます。 ICE ネゴシエーションが完了したとき、より適切なメディア パスが特定されていれば、メディアはリダイレクトされます。

フィールド	デフォルト	説明
パブリック最大受信帯域幅（Public Maximum In Bandwidth）	[最大受信帯域幅（Maximum In Bandwidth）] に設定された値を使用。 動的に変化します	指定した値により、ユーザが VCS アカウントを使用してアプリケーションにサインインした後のデータの送受信に使用できる最大帯域幅が決定されます。 この設定は、組織のネットワークの外側から接続するユーザに対して帯域幅を制御するのに役立つ場合があります。 これらのユーザは低速のネットワーク接続を使用していたり、企業はそれらのユーザの帯域幅使用量を制限したりする場合があります。
パブリック最大送信帯域幅（Public Maximum Out Bandwidth）	[最大送信帯域幅（Maximum Out Bandwidth）] に設定された値を使用。 動的に変化します	
パブリック電話帳サーバ URI（Public Phone Book Server URI）	[電話帳サーバ URI（Phone Book Server URI）] に設定された値を使用。 動的に変化します	[電話帳サーバ URI（Phone Book Server URI）] 設定を設定すれば十分です。
パブリック プレゼンス サーバ URI（Public Presence Server URI）	[プレゼンス サーバ URI（Presence Server URI）] に設定された値を使用。 動的に変化します	[プレゼンス サーバ URI（Presence Server URI）] 設定を設定すれば十分です。

フィールド	デフォルト	説明
パブリック SIP サーバ アドレス（Public SIP Server Address）	[SIP サーバ アドレス（SIP Server Address）] に設定された値を使用。 動的に変化します	ユーザが外部 VCS サーバ アドレスでサインインした後の登録要求の送信先となるサーバ アドレス 通常、この情報は、ユーザが Cisco Jabber Video for iPad で指定する外部サーバ アドレスと同じです。
解像度設定（Resolution Preferences）	高（High）	着信と発信のビデオ解像度を制限します。 Cisco Jabber Video for iPad はこの値を上書きします。 この制限は多くの要因に左右されますが、一般に次の規則に従います。 • [高（High）] では、ワイドスクリーン HD（1920x1080 または 1280x720）を上限とする可能な限り高い解像度が使用されます。 • [中（Medium）] では、ワイド CIF（512x288）以下の解像度に制限されます。 • [低（Low）] では、ワイド QCIF（256x144）以下の解像度に制限されます。
SIP サーバ アドレス（SIP Server Address）	Cisco Jabber Video for iPad がサブスクライブされている VCS サーバ	登録要求が送信されるサーバ アドレス ユーザが Cisco Jabber Video for iPad で指定する内部サーバ アドレスと同じです。
SIP 認証ユーザ名（SIP Authentication Username）		SIP 認証ユーザ名。 エンドポイントは AuthUsername および AuthPassword 値を VCS サーバでの認証に使用します。
SIP 認証パスワード（SIP Authentication Password）		SIP 認証パスワード。 エンドポイントは AuthUsername および AuthPassword 値を VCS サーバでの認証に使用します。
TurnAuthPassword		ICE を有効化するために必要な TURN サーバ設定。詳細については、ICE の有効化, （109 ページ） を参照してください。
TurnAuthUsername		
TurnServer		

VCS の設定

登録許可リストまたは検索ルールを使用する場合は、このトピックを確認してください。

ユーザ デバイスが VCS と連携するには、それらのデバイスを VCS に登録しておく必要があります。 登録 URI 内での Cisco Jabber Video for iPad ユーザのサフィックスは、`.jabbertablet` または `.jabber` です。 たとえば、ユーザの URI は、新しいサフィックスを持つ次の形式になります。 `userName.jabbertablet@DomainName` または `userName.jabber@DomainName`。 URI にサフィックスが追加されるため、次の変更が必要になる場合があります。

- 新しい URI サフィックスを許可するように、登録許可リスト（[VCS 設定（VCS configuration）] > [登録（Registration）] > [許可リスト（Allow List）]）を更新します。

  例：VCS と VCSE（VCS Expressway）の両方を導入し、許可リストを使用して外部ロケーションからの登録を制御している場合は、新しいサフィックスを許可リストに追加します。

- 新しい URI サフィックスを考慮するように、検索ルールを更新または作成します。 検索ルールの作成時には、`.+\.(jabbertablet|jabber).*@%localdomains%.*` の形式に似たパターン文字列を指定します。

  例：組織内に複数の VCS クラスタ（ゾーン）が存在する場合は、VCS ゾーンと VCSE ゾーンの間のコール ルーティングを制御するルールを更新しなければならない場合があります。

ファイアウォールの要件

ポートがアプリケーションのトラフィックを伝送するようにハードウェア ファイアウォールを設定します。ハードウェアファイアウォールは、望まないトラフィックからの保護を組織レベルで実現するネットワーク デバイスです。 次の表に、VCS の導入に必要なポートを示します。 これらのポートは、アプリケーションが正常に機能するために、すべてのファイアウォール上で開いておく必要があります。

プロトコル	ポートおよび説明
DNS	• VCS が DNS サーバにアクセスする場合、一般にポート 53 で待ち受けします。 • VCS は、どの送信元ポートから要求が送信されるかを制御しようとはしません。
SIP	• 開くようにプロビジョニングされない限り、サーバ ポートは開きません。 VCS は、5060 を開くプロビジョニングを受信すると、UDP と TCP に対して 5060 を、TLS/TCP に対して 5061 を開きます。 • 通常の使用状況では、1 つの発信 TCP 接続だけが SIP プロキシに対して確立されます。 VCS は、どの TCP 送信元ポートを使用するかを制御しようとはしません。

プロトコル	ポートおよび説明
	• VCS は、DNS SRV を使用して、SIP サーバが待ち受けしているポートを検出します。 VCS は 80 や 443 などのウェルノウン ポートを受け入れますが、通常の使用状況では、SIP のデフォルトのサーバ ポートは 5060 および 5061 です。
HTTP	• 通常の使用状況では、1 つの発信 TCP 接続だけが http または https サーバに対して確立されます。 VCS は、どの TCP 送信元ポートを使用するかを制御しようとはしません。 • アプリケーションは、DNS を使用してサーバ ポートを検出します。通常の使用状況では、80 または 443 です。
media	• VCS は、メディア（RTP/UDP）に使用できるポート範囲でプロビジョニングされます。 • 各コールについて、アプリケーションはその範囲内の 9 個のポートを開き、着信 UDP トラフィックをリッスンします。 • デフォルトのポート範囲は 21000～21900 で、アプリケーションに適切な範囲を指定する必要があります。
TURN	• アプリケーションは、ICE を使用して最適なメディア パスを検出しようとします。 • VCS は、各コールに対して TURN サーバ上に 9 個のポートを割り当てます。 • TURN の割り当てには、メディアに使用されるメディア ポート範囲が使用されます。 • アプリケーションは、DNS SRV を使用して、TURN サーバが待ち受けしているポートを検出します。 VCS は、80 や 443 などのウェルノウン ポートを受け入れます。ただし、通常の使用状況で使用されるポートは 3478 または 5349 です（TURN 標準）。 • STUN 標準と TURN 標準の規定により、アプリケーションは、各コールに対して同じポートを使用することはできません。 そのため、ポート範囲には少なくとも 100 個のポートが必要です。

主な通信タイプ

以下のトピックを確認して、Cisco Jabber Video for iPad 上で VCS に使用される主な通信タイプを把握してください。

SIP 通信

Cisco Jabber Video for iPad は、Session Initiation Protocol（SIP）を使用して VCS と通信します。 ビデオとオーディオを除き、SIP はすべての通信（加入、登録、プレゼンス ステータスのクエリー、コールの招待など）を担当します。 SIP メッセージは、プロビジョニングされた設定に従って（TLS 暗号化の有無に関係なく）TCP によって送信されます。

VCS で使用されるデフォルトの SIP リスニング ポートは次のとおりです。

- 5060（暗号化なし）
- 5061（暗号化あり）

これらのリスニング ポートを変更するには、[VCS 設定（VCS Configurations）] > [プロトコル（Protocols）] > [SIP] > [設定（Configuration）] に移動します。

（注） Jabber 本体は、これらの通信にエフェメラル TCP ポートを使用します。 これらのポートは、TCP スタックによって Cisco Jabber Video for iPad に渡されるので、設定することはできません。

H.323 が必要で、SIP をサポートしていないデバイスとの通信を有効にする場合は、Cisco VCS 上のインターワーキングを使用できます。

メディア通信

メディア データは、最大 9 本の UDP リンク（ポート）によって転送されます。 Cisco Jabber Video for iPad で使用されるメディア ストリームには、次のようなものがあります。

- 音声
- プライマリ ビデオ
- セカンダリ ビデオ（プレゼンテーション共有）

これらのストリームにはそれぞれ 2 本のリンクが必要です。1 本は RTP パケット用で、もう 1 本はRTCPパケット用です。 暗号化が有効になっている場合は、SRTPプロトコルが使用されます。

TMS でのポート範囲の変更

メディアを受信する Cisco Jabber Video for iPad のデフォルトのポート範囲は 21,000 ～ 21,900 です。 この範囲は、TMS で変更できます。

（注） 使用されるポート番号は連続していますが、指定範囲内でランダムに選択されます。

手順

ステップ 1 [システム（Systems）] > [プロビジョニング（Provisioning）] > [ディレクトリ（Directory）] に移動します。

ステップ 2 [メディア ポート範囲の先頭（Media Port Range Start）] および [メディア ポート範囲の末尾（Media Port Range End）] を使用して範囲を指定します。
最小範囲の 10 ポートを指定します。指定しなければ、デフォルトの範囲が使用されます。

VCS でのポート範囲の変更

VSC 上で使用されるデフォルトのポート範囲は 50,000 ～ 52,399 です。 これは変更できます。

（注） 使用されるポート番号は連続していますが、指定範囲内でランダムに選択されます。

手順

ステップ 1 [VCS 設定（VCS Configuration）] > [ローカル ゾーン（Local Zone）] > [トラバーサル サブゾーン（Traversal Subzone）] に移動します。

ステップ 2 [トラバーサル メディア ポートの先頭（Traversal media port start）] および [トラバーサル メディア ポートの末尾（Traversal media port end）] を使用して範囲を指定します。
最小範囲の 10 ポートを指定します。指定しなければ、デフォルトの範囲が使用されます。

メディア ルーティング

Cisco Jabber Video for iPad は、メディア ルーティングを向上させる Interactive Connectivity Establishment（ICE）をサポートしています。 コール中、ICE は、参加者全員のアプリケーションで有効になっている場合に使用されます。 詳細については、以下のトピックを確認してください。

ICE を使用しないメディア ルーティング

メディア リンクは、非トラバーサル コールでは 2 つのデバイス間に直接、トラバーサル コールでは Cisco Jabber Video for iPad と VCS の間に確立されます。 一般に、非トラバーサル コールは、同じネットワーク上に存在してインターワーキングを必要としない 2 人の参加者間のコールとして定義されます。

SIP-to-H.323 コールにはインターワーキングが必要です。 このようなコールは、デバイスが同一ネットワーク上に存在しているかどうかに関係なく、トラバーサル コールになります。 詳細については、http://www.cisco.com/en/US/products/ps11337/prod_maintenance_guides_list.html にある、お使いの VCS リリースに対応した『*Cisco TelePresence Video Communication Server Administrator Guide*』を参照してください。

ICE を使用したメディア ルーティング

ICE は、コール参加者間のメディアの伝送に最適なパスを動的に検出します。 [MNS モードの有効化（Enable MNS Mode）] プロビジョニング設定を使用することにより、メディアのルーティングを改善し、専用リンクを経路にすることができます。

ICE の有効化

ICE を起動するように Cisco VCS Expressway を設定します。

ICE を使用したメディア ルーティングには、TURN サーバが必要です。 バージョン X5.2 以降を実行中の VCS Expressway は、TURN リレー ライセンスがある場合、TURN サーバとして機能します。 TURN サーバ オプション キーが必要です。

（注） ICE プロビジョニングはデフォルトで使用できません。

手順

ステップ 1 VCS Expressway で、[VCS 設定（VCS configuration）] > [Expressway] > [TURN] に移動し、次の設定を指定します。

設定	変更
TURN サービス（TURN services）	On
ポート（Port）	3478
メディア ポート範囲の始端（Media port range start）	60000
メディア ポート範囲の末尾（Media port range end）	61399

ステップ 2 [VCS 設定（VCS configuration）] > [認証（Authentication）] > [デバイス（Devices）] > [設定（Configuration）] に移動し、[データベース タイプ（Database type）] のローカル データベースを指定します。

ステップ 3 [VCS 設定（VCS configuration）] > [認証（Authentication）] > [デバイス（Devices）] > [ローカル データベース（Local database）] に移動し、ユーザ名とパスワードを作成します。

TURN リレー ライセンスを使用するには、ユーザ名とパスワードが必要です。

ステップ 4 [システム（Systems）] > [プロビジョニング（Provisioning）] > [ディレクトリ（Directory）] > [設定（Configurations）] に移動し、次の各フィールドを次の表の値に設定します。

設定	変更後の値
ICE を有効にする（Enable NTP）	On
TurnAuthPassword	Cisco VCS Expressway を設定したときに作成されたパスワード
TurnAuthUsername	Cisco VCS Expressway を設定したときに作成されたユーザ名
TurnServer	サーバ メディアのアドレスは ICE コールでリレーされます。 通常は、Cisco VCS Expressway のアドレスです。

Cisco Jabber Video for iPad の TURN ポート

TURN ポート設定は、DNS によって制御される必要があります。 Cisco Jabber Video for iPad は、TURN の IP、優先度、重み、およびポートについて SRV 検索を実行します。 TURN は UDP 上で動作するので、検索対象は `_turn._udp.<domain>` になります。 TURN の SRV レコードが見つからない場合、Cisco Jabber Video for iPad は A レコード検索（IPv4）または AAAA 検索（IPv6）を実行しますが、ポートはデフォルトで 3478 になります。

ポートをプロビジョニングする必要がある場合は、TurnServer フィールド内の IP アドレスにポートを付加できます（例：`192.0.2.0:3478`）。

サインイン時の通信の動作

Cisco Jabber Video for iPad にサインインした後、ユーザは、内部と外部の VCS サーバ アドレスを指定します。 アプリケーションは、最初に内部アドレスに対して加入を試みます。 iPadデバイスが社外の Wi-Fi に接続されているような状況では、アプリケーションは、外部アドレスに対して加入を試みます。

内部 VCS サーバ アドレスが複数の IP アドレスに変換される DNS アドレスである場合、アプリケーションは、外部 VCS サーバ アドレスを試す前に、これらすべての IP 番号に対して接続を試みます。 DNS サーバに SRV レコードが格納されている場合、アプリケーションは、それらの IP アドレスの優先度と重みに従います。格納されていなければ、ランダムな順序でそれらを試します。

通常、VCS または TMS Agent が最初の登録メッセージをチャレンジします。 アプリケーションは、認証情報を別の SUBSCRIBE メッセージで送信することにより、このチャレンジに応答します。

登録の認証が完了した後、TMS Agentはプロビジョニング情報をアプリケーションに送信します。

アプリケーションは、TMS の [SIP サーバ URI（SIP Server URI）] または [パブリック SIP サーバ URI（Public SIP Server URI）] のプロビジョニング情報に従って VCS に登録します。 このプロビジョニング情報が、ユーザのサインイン時に指定される内部および外部の VCS サーバ アドレス（両者は同じであることが推奨されています）と同一である場合、アプリケーションは加入先と同じ VCS に登録します。 アプリケーションが登録されている間は、VCS は、メッセージをそのアプリケーションに転送することを認識しています。

初期登録後、アプリケーションは、VCS サーバの [標準登録の最長リフレッシュ（秒）（Standard registration refresh maximum (seconds)）] 設定に従って登録メッセージを VCS に送信し続けます。アプリケーションは、指定された時間間隔の 75% が経過した後にメッセージを送信します。

（注） [標準登録の最長リフレッシュ（秒）（Standard registration refresh maximum (seconds)）] 設定は、バージョン X6.0 の VCS では使用できません。

登録リフレッシュの最大時間の指定

ユーザがデバイス上で Cisco Jabber Video for iPad から一時的に離れて他の作業を実行すると、アプリケーションはバックグラウンドになり、10 分ごとに復帰するように設定されます。 アプリケーションが VCS サーバへの登録を継続できるように、標準 SIP 登録のリフレッシュ期間の最大値を 900 に設定する必要があります。

手順

ステップ 1 VCS サーバで、[VCS 設定（VCS configuration）] > [プロトコル（Protocols）] > [SIP] > [設定（Configuration）] に移動します。

ステップ 2 [登録コントロール（Registration controls）] セクションで、[標準登録の最長リフレッシュ（秒）（Standard registration refresh maximum (seconds)）] に 900 を入力します。

ステップ 3 [保存（Save）] を選択します。

サインイン後の通信の動作

ユーザが Cisco Jabber Video for iPad にサインインした後、このアプリケーションは次のタスクを継続的に実行します。

接続の確認

Cisco Jabber Video for iPad は、ユーザがアプリケーションにサインインした後、DNS を使用して TURN サーバとポートを探します。 アプリケーションは、SRV レコードで指定され、TURN サーバでサポートされている任意のポート（80（HTTP）と 443（HTTPS）を含む）を使用できます。

アプリケーションは、次の順序でポートを探します。

1. UDP
2. TCP（サポートされている場合）
3. TLS（サポートされている場合）

ポートが検出されない場合、アプリケーションはデフォルトで 3478 と 5349 のポートを使用します。

（注） この時点で VCS を TURN サーバとして使用する場合、TCP リレーを使用したファイアウォールの通過はサポートされません。

帯域幅プロービング

帯域幅プロービングがプロビジョニングされた場合、ユーザがアプリケーションにサインインした後、Cisco Jabber Video for iPad はダミー メディアを TURN サーバで折り返して戻ってくるようにルーティングします。 この機能では、TURN サーバが正常にプロビジョニングされている必要があります。

帯域幅プロービングの結果は、アプリケーションのリソースを動的に適応させるために使用されます。 この結果は、プロービング用にプロビジョニングされる時間の影響も受け、多くの場合、最悪の事態の帯域幅シナリオを表しているので、実際のコール時に使用可能な帯域幅はそれよりも大きくなる可能性があります。

ディレクトリ検索

ユーザが Cisco Jabber Video for iPad の検索フィールドに文字を入力するたびに、アプリケーションは VCS 上の TMS エージェントにクエリーを実行し、TMS エージェントは一致した結果で応答します。 検索結果が選択されると、アプリケーションは、その連絡先のプレゼンス ステータスについても VCS にクエリーします。

コール設定

コール設定は、VCS 経由の SIP メッセージで伝えられます。 コール設定時にコールの属性が決定される方法については、以下のトピックを確認してください。

暗号化

コールを暗号化する場合、SIP 通信とメディア通信の両方が暗号化される必要があり、すべての通話者が暗号化をサポートしている必要があります。 暗号化されたメディア通信は、128 ビットの高度暗号化規格（AES）を使用した Secure Real-time Transport Protocol（SRTP）によって送信されます。

TMS で [システム（Systems）] > [プロビジョニング（Provisioning）] > [電話帳（Directory）] に移動して、次の暗号化ポリシー設定を指定できます。

- [TLS/TCP の使用（Force TLS/TCP）]：SIP 通信が暗号化されているか（TLS）いないか（TCP）を決定します。 Cisco Jabber Video for iPad で現在使用される TLS バージョンは 1.0 です。
- [SRTP の使用あり/なし（Force/No Srtp）]：メディア通信が暗号化されているかいないかを決定します。
- [自動（Auto）]：Cisco Jabber Video for iPad は暗号化コールを試行します。 できない場合、アプリケーションは暗号化されないコールを許可します。

送信帯域幅と受信帯域幅

コール セットアップ中、Cisco Jabber Video for iPad は受信する最大帯域幅をサーバの設定に従ってシグナリングします。 このシグナリングが守られるかどうかは、コールの相手側のシステムに依存します。

コール中に送信される最大帯域幅とコールの開始時に送信される帯域幅の両方がコール セットアップ時に決定されます。

コール中、アプリケーションが送信できる帯域幅は増減しますが、送信される帯域幅がコール セットアップ時に決定された最大帯域幅を超えることはありません。

ビデオ解像度

プロビジョニングの [解像度設定（Resolution Preferences）] 設定により、着信ビデオと発信ビデオの両方の解像度が制御されます。 プロビジョニング オプションの概要, （98 ページ）を参照してください。 着信ビデオに対する制限は、コール内の他の参加者が使用しているシステムによって決まります。

良好なビデオ品質には多くの要因が影響します。 フレーム レート、高い画像解像度、シーンのライティング、およびカメラの光学的性能がすべて重要な要因です。

発信ビデオ解像度

Cisco Jabber Video for iPad は、ビデオ送信時の解像度を決定するときに次の基準を使用します。

- カメラのネイティブ フォーマットでの解像度
- 解像度が受信側で許可される必要があること。
- 高解像度を低帯域幅で送信すると品質が低下すること。 送信帯域幅が解像度に対して十分な大きさでなければならないこと。 次のガイドラインを参照してください。
  - 最適：640x368（768 Kbps 以上が必要）
  - 良好：480x360（512 Kbps 以上が必要）

帯域幅を増やすと、画質が向上します。 [最大送信帯域幅（Maximum Out Bandwidth）] を使用して、許可される帯域幅を指定できます。 詳細については、プロビジョニング オプションの概要, （98 ページ）を参照してください。

上の記述に従って十分な帯域幅があるにもかかわらず、高解像度が実現されない場合は、一般に次のいずれかまたは両方がその原因である可能性があります。

- ネットワーク接続に関する問題（パケット損失など）
- 高い CPU 使用率

着信ビデオ解像度

プロビジョニングで [最大受信帯域幅（Maximum In Bandwidth）] を使用して、着信ビデオに対して許可される帯域幅を指定できます。 詳細については、プロビジョニング オプションの概要, （98 ページ）を参照してください。 高解像度ビデオの着信に必要な帯域幅は、各コール参加者のデバイスの機能および制限に応じて変化します。

（注） 参加者のデバイスが高解像度ビデオの送信に対応していて、着信ビデオの帯域幅に制限を指定していない場合であっても、ネットワーク接続の問題（パケット損失など）によって着信ビデオの解像度が要求に満たない場合があります。

プレゼンテーションの解像度

共有プレゼンテーションの最大解像度は、コール参加者のデバイスで使用可能な帯域幅および機能によって異なります。 無制限の帯域幅を使用した Jabber 間のコールの場合、プレゼンテーション解像度は 448 p になります。

プレゼンテーションの解像度を変更することはできません。

ビデオと音声の標準

Cisco Jabber Video for iPad では、送信と受信の両方について次の標準がサポートされています。アプリケーションは、コール内の他の参加者のデバイスまたはアプリケーションでサポートされている、最適な標準を常に使用します。

- 音声：G.722.1 および G.711
- ビデオ：H.264

ICE ネゴシエーション

コールの接続が完了した後、コールの参加者全員が ICE を有効にし、サポートしている場合、ICE がネゴシエートされます。 ICE ネゴシエーションには、2 ～ 3 秒の時間がかかり、9 つの TURN サーバ ライセンス（メディア リンクごとに 1 つのライセンス）が必要です。

コール中の処理

コールの設定が完了した後、ユーザ操作の結果として、あるいは状態の変化に対する自動化された応答として、いくつかの操作を Cisco Jabber Video for iPad で要求される場合があります。 詳細については、以下のトピックを確認してください。

Multiway

Multiway は、ユーザがコールに参加し、複数参加者の会議をシームレスに作成する機能です。 Cisco Jabber for iPad は、Multiway を開始できません。 他の参加者が使用しているデバイスから Multiway が開始されると、そのコールは、[Multiway 参加者 URI（Multiway Participant URI）] プロビジョニング オプションに従ってマルチ会議システムにリダイレクトされます。

メディア ストリームのミュート

カメラまたはマイクロフォンがコール中にミュートにされると、Cisco Jabber Video for iPad は、その帯域幅を他のメディア リンクが使用するように割り当てます。 ユーザが 2 つのストリームに対して十分な帯域幅を確保できない場合は、一方のストリームをミュートにすることで、もう一方のストリームの品質を向上させることができます。

使用されていないリンクが（たとえばファイアウォールによって）閉じられるのを防ぐために、アプリケーションは 7 秒ごとに STUN（キープ アライブ）メッセージを送信します。

自動帯域幅適応

Cisco Jabber Video for iPad がネットワークの能力を超える帯域幅を送信または受信している状況では、パケットの損失率が高くなり、コールの品質が低下する可能性があります。 アプリケーションは、自動帯域幅適応メカニズムを使用して、そのような帯域幅に関する問題に対処します。

（注） 自動適応には時間がかかります。 ネットワークとシステムの能力に合わせてアプリケーションを設定しておくことを推奨します。

第 8 章

ユーザへの指示の作成

ここでは、アプリケーション ユーザ向けの指示の準備について説明します。

（注） DNS SRV を使用した簡易サイン インのセットアップ, （7 ページ） に説明されているように DNS SRV を設定している場合、サーバ アドレスなどの情報を提供する必要はありません。 選択した設定に関係なく、管理者はユーザ名、パスワード、電子メール アドレスなどの情報を提供する必要があります。

Cisco WebEx Messenger

ユーザが Cisco Jabber Video for iPad にサインインするために必要な情報を電子メール メッセージで送信します。 この情報には次のものがあります。

- App Store から **Cisco Jabber Video for iPad** という名前のアプリケーションをダウンロードし、インストールする手順
- ユーザのアカウント用の電子メール アドレス
- ユーザが iPad でアプリケーションを起動した後に電子メール アドレスを入力する手順

- FAQ にアクセスする手順（ユーザは [設定（Settings）] アイコン > [ヘルプ（Help）] > [FAQ（FAQs）] を選択して表示できます）
- ユーザに伝える必要のあるその他の情報

Cisco WebEx Messenger および Cisco Unified Communications Manager

ユーザが Cisco Jabber Video for iPad で Cisco WebEx Messenger および Cisco Unified Communications Manager を使用するために必要な情報を電子メール メッセージで送信します。 この情報には次のものがあります。

- App Store から **Cisco Jabber Video for iPad** という名前のアプリケーションをダウンロードし、インストールする手順
- ユーザのアカウント用のクレデンシャル：
  - Cisco WebEx Messenger アカウント用の電子メール アドレス
  - Cisco Unified Communications Manager アカウント用のユーザ名または電子メール アドレス、および TFTP サーバ アドレス
- 次の順序のアカウント設定手順：
  1. ユーザが iPad でアプリケーションを起動した後に電子メール アドレスを入力する手順。
  2. アプリケーションの [設定（Settings）] から Cisco Unified Communications Manager を設定します。

注意 ユーザが Cisco Unified Communications Manager アカウントに最初にサインインした場合、アプリケーションで Cisco WebEx Messenger を設定することはできません。

- FAQ にアクセスする手順（ユーザは [設定（Settings）] アイコン > [ヘルプ（Help）] > [FAQ（FAQs）] を選択して表示できます）
- ユーザに伝える必要のあるその他の情報

Cisco WebEx Messenger および Cisco TelePresence Video Communication Server

ユーザが Cisco Jabber Video for iPad で Cisco WebEx Messenger および VCS を使用するために必要な情報を電子メール メッセージで送信します。 VCS ユーザには、カスタマイズされた電子メール

メッセージを TMS から送信します。デフォルトの電子メールテンプレートには、簡単なメッセージ、ユーザ名、およびパスワードが含まれています。

（注） TMS からアカウント情報を送信する方法の詳細については、次の該当するマニュアルを参照してください。

- TMS Agent Legacy を使用する場合は、http://www.cisco.com/en/US/products/ps11338/products_installation_and_configuration_guides_list.html にある『*Cisco TelePresence Management Suite Agent Legacy Provisioning Guide*』を参照してください。
- TMS Provisioning Extension（TMSPE）を使用する場合は、http://www.cisco.com/en/US/products/ps11472/prod_installation_guides_list.html にある『*Cisco TelePresence Management Suite Provisioning Extension Deployment Guide*』を参照してください。

電子メール メッセージには、次の情報を含める必要があります。

- App Store から **Cisco Jabber Video for iPad** という名前のアプリケーションをダウンロードし、インストールする手順
- ユーザのアカウント用のクレデンシャル：
  - Cisco WebEx Messenger アカウント用の電子メール アドレス
  - VCS アカウント用のユーザ名、内部サーバと外部サーバのアドレス、および SIP ドメイン アドレス

    ユーザが複数の VCS クラスタに分散している場合は、正しいサーバ アドレスを別のグループのユーザに確実に伝えてください。
- 次の順序のアカウント設定手順：
  1. ユーザが iPad でアプリケーションを起動した後に電子メール アドレスを入力する手順。
  2. アプリケーションの [設定（Settings）] から VCS を設定します。

注意 ユーザは、先に VCS アカウントでサインインした場合、アプリケーションで Cisco WebEx Messenger を設定できません。

- FAQ にアクセスする手順（ユーザは [設定（Settings）] アイコン > [ヘルプ（Help）] > [FAQ（FAQs）] を選択して表示できます）
- ユーザに伝える必要のあるその他の情報

Cisco Unified Communications Manager

Cisco Unified Communications Manager の設定が完了したら、次の情報が含まれる電子メール メッセージをユーザに送信します。

- App Store から **Cisco Jabber Video for iPad** という名前のアプリケーションをダウンロードし、インストールする手順
- TFTP サーバ アドレス、ユーザのユーザ名または電子メール アドレス、およびオプションの CCMCIP サーバ アドレス
- ユーザが iPad でアプリケーションを起動した後に電子メール アドレスを入力する手順
- 企業の Wi-Fi ネットワークにデバイスを接続するための手順。 この手順は、Cisco Jabber Video for iPad とは関係ありません。
- デバイス上で VPN（バーチャル プライベート ネットワーク）アクセスを設定するための手順（VPN 接続経由での Cisco Jabber Video for iPad の使用をユーザに許可する場合）。 この手順は、Cisco Jabber Video for iPad とは関係ありません。
- ユーザがアプリケーションから [SSL を使用（Use SSL）] および [LDAP ユーザ認証（LDAP User Authentication）] を有効にする必要があるかどうかの指示

  アプリケーションに LDAP の設定が自動的に入力されるように、[Cisco Unified CM の管理（Cisco Unified CM Administration）] のユーザ デバイスの [プロダクト固有の設定（Product Specific Configuration Layout）] セクションに必要な LDAP 設定がすべて指定されていることを確認してください。 詳細は、ユーザ デバイスの追加, （52 ページ）を参照してください。
- FAQ にアクセスする手順（ユーザは [設定（Settings）] アイコン > [ヘルプ（Help）] > [FAQ（FAQs）] を選択して表示できます）
- ユーザに伝える必要のあるその他の情報

Cisco Unified Presence

Cisco Unified Presence の設定が完了したら、次の情報が含まれる電子メール メッセージをユーザに送信します。

- App Store から **Cisco Jabber Video for iPad** という名前のアプリケーションをダウンロードし、インストールする手順
- ユーザのユーザ名または電子メール アドレス
- ユーザが iPad でアプリケーションを起動した後に電子メール アドレスを入力する手順
- 企業の Wi-Fi ネットワークにデバイスを接続するための手順。 この手順は、Cisco Jabber Video for iPad とは関係ありません。

- デバイス上で VPN（バーチャル プライベート ネットワーク）アクセスを設定するための手順（VPN 接続経由での Cisco Jabber Video for iPad の使用をユーザに許可する場合）。 この手順は、Cisco Jabber Video for iPad とは関係ありません。
- FAQ にアクセスする手順（ユーザは [設定（Settings）] アイコン > [ヘルプ（Help）] > [FAQ（FAQs）] を選択して表示できます）
- ユーザに伝える必要のあるその他の情報

Cisco Unified Presence および Cisco Unified Communications Manager

ユーザが Cisco Jabber Video for iPad で Cisco Unified Presence および Cisco Unified Communications Manager を使用するために必要な情報を電子メール メッセージで送信します。 この情報には次のものがあります。

- App Store から **Cisco Jabber Video for iPad** という名前のアプリケーションをダウンロードし、インストールする手順
- ユーザのアカウント用のクレデンシャル：
  - Cisco Unified Presence アカウント用のユーザ名または電子メール アドレス、およびサーバ アドレス
  - Cisco Unified Communications Manager アカウント用のユーザ名または電子メール アドレス、および TFTP サーバ アドレス
- 次の順序のアカウント設定手順：
  1. ユーザが iPad でアプリケーションを起動した後に電子メール アドレスを入力する手順。
  2. アプリケーションの [設定（Settings）] から Cisco Unified Communications を設定します。

注意 ユーザが Cisco Unified Communications Manager アカウントに最初にサインインした場合、アプリケーションで Cisco Unified Presence を設定することはできません。

- 企業の Wi-Fi 接続にデバイスを接続するための手順。 この手順は、Cisco Jabber Video for iPad とは関係ありません。
- デバイス上で VPN（バーチャル プライベート ネットワーク）アクセスを設定するための手順（VPN 接続経由での Cisco Jabber Video for iPad の使用をユーザに許可する場合）。 この手順は、Cisco Jabber Video for iPad とは関係ありません。
- FAQ にアクセスする手順（ユーザは [設定（Settings）] アイコン > [ヘルプ（Help）] > [FAQ（FAQs）] を選択して表示できます）

- ユーザに伝える必要のあるその他の情報

Cisco TelePresence Video Communications Server

Cisco Jabber Video for iPad で VCS を使用するのに必要な情報をユーザに提供するために、カスタマイズされた電子メール メッセージを TMS からユーザに送信します。 デフォルトの電子メール テンプレートには、簡単なメッセージ、ユーザ名、およびパスワードが含まれています。

さらに、次の情報も電子メール メッセージに含めます。

- 内部および外部のサーバ アドレス。 ユーザが複数の VCS クラスタに分散している場合は、正しいサーバ アドレスを別のグループのユーザに確実に伝えてください。
- SIP ドメイン アドレス
- ユーザが iPad でアプリケーションを起動した後に電子メール アドレスを入力する手順
- App Store から **Cisco Jabber Video for iPad** という名前のアプリケーションをダウンロードし、インストールする手順
- FAQ にアクセスする手順（ユーザは [設定（Settings）] アイコン > [ヘルプ（Help）] > [FAQ（FAQs）] を選択して表示できます）
- ユーザに伝える必要のあるその他の情報

TMS からアカウント情報を送信する方法の詳細については、次の該当するマニュアルを参照してください。

- TMS Agent Legacy を使用する場合は、http://www.cisco.com/en/US/products/ps11338/products_installation_and_configuration_guides_list.html にある『*Cisco TelePresence Management Suite Agent Legacy Deployment Guide*』を参照してください。
- TMS Provisioning Extension（TMSPE）を使用する場合は、http://www.cisco.com/en/US/products/ps11472/prod_installation_guides_list.html にある『*Cisco TelePresence Management Suite Provisioning Extension Deployment Guide*』を参照してください。