



統合ガイド



Microsoft OCS が統合された Cisco Unified Presence Release 8.0 で Microsoft Office Communicator の通話コントロール機能を使用するための設定

Configuring Cisco Unified Presence Release 8.0 with Microsoft OCS for Microsoft Office Communicator Call Control

【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、米国シスコシステムズ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。

- 1 この統合の要件
- 2 この統合の概要
- 3 この統合のライセンス要件
- 4 Microsoft OCS と統合するための Cisco Unified Communications Manager の設定方法
- 5 Microsoft OCS と統合するための Cisco Unified Presence の設定方法

- 6 Cisco Unified Presence と統合するための Microsoft コンポーネントの設定方法
- 7 Microsoft Active Directory で正規化規則を設定する方法
- 8 Cisco Unified Presence のセキュリティ証明書を設定する方法
- 9 Cisco Unified Presence と Microsoft OCS との間のセキュリティを設定する方法
- 10 この統合の冗長性の設定
- 11 Phone Selection プラグインを配置する方法
- 12 詳細情報の入手

1 この統合の要件

この章では、Cisco Unified Presence を Microsoft Office Communications Server または Microsoft Live Communications Server と統合して Microsoft Office Communicator (MOC) の通話コントロール機能を使用するために必要となる、設定の手順について説明します。



(注) この章では、Cisco Unified Presence を Microsoft Office Communications Server (OCS) と統合する手順について説明します。Cisco Unified Presence と Microsoft Live Communications Server (LCS) との間で同様の統合を設定する場合にも、この章をガイドとして参照できます。

ソフトウェア要件

- Cisco Unified Presence Server (Release 6.X または Release 7.X)
- Cisco Unified Communications Manager Server バージョン 6.X
- Microsoft Office Communications (OCS) 2007 または 2007 R2 Server, Standard または Enterprise
- Microsoft Live Communications (LCS) 2005 Server, Standard または Enterprise
- Microsoft Office Communicator (MOC)
- Microsoft Windows Server
- (オプション) Cisco CSS 11500 Content Services Switch

この統合では、インストールおよび設定を次のように行っていることを前提としています。

- Cisco Unified Presence サーバを、『*Deployment Guide for Cisco Unified Presence*』の説明に従ってセットアップし、設定している。
- Cisco Unified Presence サーバを、『*Deployment Guide for Cisco Unified Presence*』の説明に従って Cisco Unified Communications Manager (CUCM) サーバとともに正しく配置している。
- Microsoft 社のマニュアルに定義されている要件に従って、Microsoft OCS サーバまたは LCS サーバをセットアップし、設定している。

2 この統合の概要

- 「この統合の仕組み」(P.3)
- 「ラインアピアランス」(P.4)

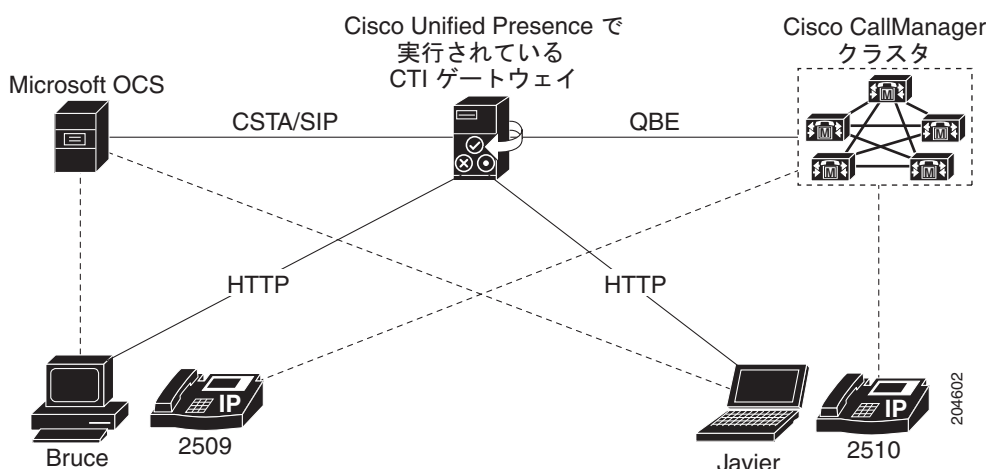
この統合の仕組み

Cisco Unified Presence を使用すると、企業ユーザが Microsoft Office Communicator (サードパーティ製デスクトップ IM アプリケーション) 経由で Cisco Unified IP Phone を制御できるようになります。この統合に使用する Microsoft Office Communicator クライアントは、Microsoft Live Communications Server (LCS) 2005 または Microsoft Office Communications Server (OCS) 2007 で実行できます。

Microsoft Office Communicator は、セッション開始要求を Cisco Unified Presence の CTI ゲートウェイに送信し、Cisco Unified Communications Manager に登録された Cisco Unified IP Phone を制御します (図 1 を参照)。CTI ゲートウェイは、要求を Cisco Unified Communications Manager 上の CTI マネージャに転送します。

Cisco Unified Communications Manager は、同じパスを反対方向に使用して、イベントを Microsoft Office Communicator アプリケーションに返します。

図 1 統合の概要



Cisco Unified Presence は、最大 8 つの Cisco Unified Communications Manager ノードで CTI 接続をサポートします。つまり、Cisco Unified Presence に最大 8 つの CTI 接続アドレスを設定できます。

Microsoft Office Communicator は、セッション開始要求を Cisco Unified Presence に送信します。このような要求は、Cisco Unified Presence に設定された CTI 接続アドレスにルーティングされます。要求は、これらの CTI 接続アドレスにラウンドロビン順に配布されます。たとえば、最初の要求は最初の CTI ノードにルーティングされ、2 番目の要求は次の CTI ノードにルーティングされるという具合です。CTI 接続アドレスにはその設定順にプライオリティが割り当てられます。デュアル ノード Cisco Unified Presence クラスタでは、ロード バランサを使用して、Microsoft Office Communicator クライアントから送信されたセッション開始要求をパブリッシャおよびサブスクリバ Cisco Unified Presence ノードにラウンドロビンできます。

Cisco Unified Presence 上の CTI ゲートウェイは、起動すると、設定済みリストに記載されたすべての CTI 接続アドレスに接続し、定期的にハートビート メッセージを送信してそれぞれの接続をモニタします。Microsoft Office Communicator ユーザがサインインすると、Microsoft OCS は、CSTA ボディを含めた SIP INVITE 要求を CTI ゲートウェイに送信してユーザの Cisco Unified IP Phone をモニタします。CTI ゲートウェイは、その Microsoft Office Communicator ユーザ用のセッションを確立し、ロード バランシング メカニズムを使用して、そのユーザからのセッション開始要求を任意の CTI 接続アドレスに送信します。

CSTA アプリケーション セッションが確立されると、デバイスの監視、コールの発信、コールの転送、デバイス制御のステータスの変更など、さまざまなアクティビティのために、Microsoft Office Communicator と CTI ゲートウェイが一連の SIP INFO メッセージを交換します。このメッセージ交換は、最初のセッション確立に使用したのと同じ CTI 接続アドレスで送信されます。

各 CTI マネージャへの接続がいずれも失敗した場合は、接続が使用可能になるまで、Microsoft Office Communicator からの発信コール要求が返送されます。Cisco Unified Communications Manager ノードがダウンしている場合は、CTI ゲートウェイが定期的にそのノードとの再接続を試みます。Cisco Unified Communications Manager ノードが使用可能になると、CTI ゲートウェイがそのノードに再接続し、接続をモニタします。この場合、Microsoft OCS が (セッション中に) SIP INFO 要求を送信する

と、新規接続となるため、CTI ゲートウェイの CTI マネージャ接続 ID は異なるものになります。
Microsoft Office Communicator は、新規 SIP INVITE メッセージを送信しますが、Microsoft Office Communicator ユーザは再度サインインする必要はありません。

関連項目

- 「ライン アピアランス」 (P.4)
- 「この統合の冗長性の設定」 (P.30)

ライン アピアランス

リモート通話コントロール機能を使用する電話機をユーザが選択すると、Cisco Unified Presence では、Microsoft Office Communicator から制御するライン アピアランスも選択されることになります。ライン アピアランスとは、回線とデバイスとの関連付けのことです。Cisco Unified Communications Manager では、管理者は、1 つのデバイスを複数の回線に関連付けたり、1 つの回線を複数のデバイスに関連付けたりできます。一般に、相互に関連付ける回線やデバイスを指定してライン アピアランスを設定するという作業は、Cisco Unified Communications Manager 管理者の役割です。

関連項目

- 「Cisco Unified Communications Manager でのユーザおよびデバイスの設定」 (P.5)

3 この統合のライセンス要件

表 1 に、Cisco Unified Presence MOC の通話コントロール機能のユーザ ライセンスおよびサーバ ライセンスの要件を示します。

表 1 Cisco Unified Presence ライセンス要件

ライセンス要件	説明
Cisco Unified Presence ユーザ機能ライセンス	MOC の通話コントロール機能を使用するユーザごとに、Cisco Unified Presence ユーザライセンスが必要です。これは、Cisco Unified Communications Manager Device License Unit (DLU; デバイス ライセンス ユニット) を 1 つ消費します。 Cisco Unified Communications Manager で、ユーザ DLU をアップロードし、ユーザの Cisco Unified Presence 機能を割り当てる必要があります。
Cisco Unified Presence サーバライセンス	Cisco Unified Presence サーバのプロキシサーバライセンスが 1 つ必要です。このライセンスをパブリッシャ Cisco Unified Presence サーバにアップロードする必要があります。

Cisco Unified Presence のライセンス要件の設定の詳細については、『*Deployment Guide for Cisco Unified Presence*』を参照してください。

関連項目

- 『*Deployment Guide for Cisco Unified Presence*』
http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

4 Microsoft OCS と統合するための Cisco Unified Communications Manager の設定方法



(注) Cisco Unified Communications Manager のリリースによってメニュー オプションおよびパラメータが異なる場合があるため、使用中のリリースに対応した Cisco Unified Communications Manager のマニュアルを参照してください。

- 「Cisco Unified Communications Manager でのユーザおよびデバイスの設定」 (P.5)
- 「標準 CCM ユーザ グループへのユーザの追加」 (P.6)
- 「CTI ゲートウェイのためのアプリケーション ユーザの設定」 (P.6)
- 「CTI 対応ユーザ グループへのアプリケーション ユーザの追加」 (P.7)
- 「アプリケーション ユーザへの CTI デバイス制御の割り当て」 (P.7)

Cisco Unified Communications Manager でのユーザおよびデバイスの設定

Microsoft OCS と統合するために Cisco Unified Communications Manager を設定する場合は、事前に Cisco Unified Communications Manager でユーザとデバイスの設定を完了しておく必要があります。電話デバイスを設定し、ユーザを設定し、各ユーザにデバイスを関連付ける必要があります。

回線をデバイスに関連付ける必要もあります。ただし、拡張モビリティ機能のユーザの場合は、回線をデバイス プロファイルに関連付けます。この関連付けがライン アピアランスとなります。ユーザをデバイスまたはデバイス プロファイルに関連付けると、ライン アピアランスがユーザに関連付けられます。

タスク	メニューパス
電話デバイスを設定し、プライマリ内線を各デバイスに関連付ける	[Cisco Unified CM の管理 (Cisco Unified Communications Manager Administration)] > [デバイス (Device)] > [電話 (Phone)]
ユーザを設定し、各ユーザにデバイスを関連付ける	[Cisco Unified CM の管理 (Cisco Unified Communications Manager Administration)] > [ユーザ管理 (User Management)] > [エンドユーザ (End User)]
ユーザをライン アピアランスに関連付ける	[Cisco Unified CM の管理 (Cisco Unified Communications Manager Administration)] > [デバイス (Device)] > [電話 (Phone)]



(注) Cisco Unified Presence Release 7.0.3 以降を実行している場合は、Cisco Unified Communications Manager で各デバイスにプライマリ内線を関連付ける必要がなくなりました。

関連項目

- 「ライン アピアランス」 (P.4)
- Cisco Unified Communications Manager のマニュアル：
http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

次の作業

[「標準 CCM ユーザ グループへのユーザの追加」 \(P.6\)](#)

標準 CCM ユーザ グループへのユーザの追加

始める前に

Cisco Unified Communications Manager で、前提条件であるユーザとデバイスの設定を完了しておきます。

手順

-
- ステップ 1** [Cisco Unified CM の管理 (Cisco Unified Communications Manager Administration)] > [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** [検索 (Find)] を選択します。
- ステップ 3** 次の手順を実行します。
- ユーザを選択して、[エンド ユーザの設定 (End User Configuration)] ウィンドウを表示します。
 - [ユーザ グループに追加 (Add to User Group)] を選択します。
 - [検索 (Find)] を選択します。
 - [標準 CCM エンド ユーザ (Standard CCM End Users)] をオンにします。
 - [選択項目の追加 (Add Selected)] を選択します。
 - [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。
- ステップ 4** ユーザ グループに追加するユーザごとにステップ 3 を繰り返します。
-

関連項目

- [「Cisco Unified Communications Manager でのユーザおよびデバイスの設定」 \(P.5\)](#)

次の作業

[「CTI ゲートウェイのためのアプリケーション ユーザの設定」 \(P.6\)](#)

CTI ゲートウェイのためのアプリケーション ユーザの設定

手順

-
- ステップ 1** [Cisco Unified CM の管理 (Cisco Unified Communications Manager Administration)] > [ユーザ管理 (User Management)] > [アプリケーション ユーザ (Application User)] 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** [ユーザ ID (User ID)] フィールドに、アプリケーション ユーザ名 (「CtiGW」など) を入力します。
- ステップ 4** このアプリケーション ユーザのパスワードを入力し、パスワードを確認します。
- ステップ 5** [保存 (Save)] を選択します。
-

次の作業

[「CTI 対応ユーザ グループへのアプリケーション ユーザの追加」 \(P.7\)](#)

CTI 対応ユーザ グループへのアプリケーション ユーザの追加

始める前に

CTI ゲートウェイを使用できるようにアプリケーション ユーザを設定します。

手順

-
- ステップ 1** [Cisco Unified CM の管理 (Cisco Unified Communications Manager Administration)] > [ユーザ管理 (User Management)] > [ユーザ グループ (User Group)] を選択します。
 - ステップ 2** [検索 (Find)] を選択します。
 - ステップ 3** [標準 CTI 対応 (Standard CTI Enabled)] を選択します。
 - ステップ 4** [グループにアプリケーション ユーザを追加 (Add Application Users to Group)] を選択します。
 - ステップ 5** CTI ゲートウェイ用に作成したアプリケーション ユーザを選択します。
 - 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。
-

関連項目

- [「CTI ゲートウェイのためのアプリケーション ユーザの設定」 \(P.6\)](#)

次の作業

[「アプリケーション ユーザへの CTI デバイス制御の割り当て」 \(P.7\)](#)

アプリケーション ユーザへの CTI デバイス制御の割り当て

始める前に

CTI ゲートウェイを使用できるようにアプリケーション ユーザを設定します。

手順

-
- ステップ 1** [Cisco Unified CM の管理 (Cisco Unified Communications Manager Administration)] > [ユーザ管理 (User Management)] > [ユーザ グループ (User Group)] を選択します。
 - ステップ 2** [検索 (Find)] を選択します。
 - ステップ 3** [標準 CTI によるすべてのデバイスの制御 (Standard CTI Allow Control of All Devices)] を選択します。
 - ステップ 4** [グループにアプリケーション ユーザを追加 (Add Application Users to Group)] を選択します。
 - ステップ 5** CTI ゲートウェイ用に作成したアプリケーション ユーザを選択します。
 - ステップ 6** Cisco Unified IP Phone の RT モデルを配置している場合は、[標準 CTI による接続時の転送および会議をサポートする電話の制御 (Standard CTI Allow Control of Phones supporting Connected Xfer and conf)] を選択します。
 - ステップ 7** [選択項目の追加 (Add Selected)] を選択します。
 - ステップ 8** [保存 (Save)] を選択します。
-

関連項目

- [「CTI ゲートウェイのためのアプリケーション ユーザの設定」 \(P.6\)](#)
- [「CTI 対応ユーザ グループへのアプリケーション ユーザの追加」 \(P.7\)](#)

5 Microsoft OCS と統合するための Cisco Unified Presence の設定方法

- 「サービス パラメータの設定」 (P.8)
- 「着信アクセス コントロール リストの設定」 (P.8)
- 「ルーティング設定の設定」 (P.9)
- 「固定電話制御設定を行う方法」 (P.9)

サービス パラメータの設定

Cisco Unified Presence から Microsoft Office Communicator への SIP メッセージルーティングは、Microsoft OCS が初期要求に追加したレコードルート ヘッダーに基づいています。Cisco Unified Presence は、レコードルート ヘッダー内のホスト名を IP アドレスに解決し、SIP メッセージを Microsoft Office Communicator クライアントにルーティングします。

また、Cisco Unified Presence の転送タイプは、Microsoft OCS に設定された Cisco Unified Presence ルートの転送タイプ (TLS または TCP) と同じである必要があります。

手順

-
- ステップ 1** [Cisco Unified Presence の管理 (Cisco Unified Presence Administration)] > [システム (System)] > [サービス パラメータ (Service Parameters)] を選択します。
- ステップ 2** Cisco Unified Presence サーバを選択します。
- ステップ 3** サービス [Cisco UP SIP プロキシ (Cisco UP SIP Proxy)] を選択します。
- ステップ 4** 次のパラメータが正しく設定されていることを確認します。
- **Proxy Domain** パラメータ値には、企業の最上位ドメイン名 (たとえば「example.com」) を定義する必要があります。このパラメータでは、この Cisco Unified Presence インストールがどの URI をローカルとして扱って処理するかを指定します。他の SIP 要求はプロキシできます。
 - **Add Record-Route Header** パラメータを有効にします。
 - **Use Transport in Record-Route Header** パラメータを有効にします。
 - **SIP Route Header Transport Type** パラメータ値を、Microsoft OCS から Cisco Unified Presence ルート用に Microsoft OCS に設定されたトランスポート パラメータと同じタイプに設定する必要があります。
- ステップ 5** [保存 (Save)] を選択します。
-

次の作業

「着信アクセス コントロール リストの設定」 (P.8)

着信アクセス コントロール リストの設定

手順

-
- ステップ 1** [Cisco Unified Presence の管理 (Cisco Unified Presence Administration)] > [システム (System)] > [セキュリティ (Security)] > [着信 ACL (Incoming ACL)] 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 [説明 (Description)] フィールドに説明を入力します。

ステップ 4 [アドレス パターン (Address Pattern)] フィールドに、関連付けられた Microsoft OCS サーバの IP アドレス、ホスト名、または Fully Qualified Domain Name (FQDN; 完全修飾ドメイン名) を入力します。

ステップ 5 [保存 (Save)] を選択します。

次の作業

[「ルーティング設定の設定」 \(P.9\)](#)

ルーティング設定の設定

手順

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

ステップ 2 [メソッド/イベント ルーティングのステータス (Method/Event Routing Status)] で [オン (On)] を選択します。

ステップ 3 優先プロキシ サーバに対して、[Default Cisco SIP Proxy TCP Listener] を選択します。

ステップ 4 [保存 (Save)] を選択します。

次の作業

[「固定電話制御設定を行う方法」 \(P.9\)](#)

固定電話制御設定を行う方法

- 「Cisco Unified Presence での CTI 接続の設定」 (P.9)
- 「ユーザの機能の割り当て」 (P.10)
- 「固定電話制御のトラブルシュータの実行」 (P.11)

Cisco Unified Presence での CTI 接続の設定

始める前に

CTI ゲートウェイに関連付けられた Cisco Unified Communications Manager サーバでアプリケーション ユーザ アカウントに対して設定した、ユーザ名およびパスワードを取得します。

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)] > [固定電話制御 (Desk Phone Control)] > [設定 (Settings)] を選択します。

ステップ 2 [アプリケーションのステータス (Application Status)] メニューから [オン (On)] を選択します。

ステップ 3 CTI ゲートウェイ アプリケーション ユーザ名とパスワードを入力します。



ヒント ユーザ名およびパスワードは大文字と小文字が区別され、Cisco Unified Communications Manager での設定に一致する必要があります。

ステップ 4 ハートビート間隔の値（秒単位）を入力します。これは、CTI 接続を監視するために、Cisco Unified Presence から Cisco Unified Communications Manager ノードに送信されるハートビート メッセージ間の時間の長さです。

ステップ 5 セッション タイマーの値（秒単位）を入力します。これは、Microsoft Office Communicator サインイン セッション用のセッション タイマーです。

ステップ 6 [Microsoft サーバ タイプ (Microsoft Server Type)] メニューから、使用している Microsoft サーバのタイプを選択します。

ステップ 7 必要に応じて、CTI 接続を確立する各 Cisco Unified Communications Manager ノードの IP アドレスを入力します。



(注) 最大 8 つの Cisco Unified Communications Manager ノードとの CTI 接続を設定できます。このようなノードはすべて、同じ Cisco Unified Communications Manager クラスターに属している必要があります。

ステップ 8 [保存 (Save)] を選択します。

トラブルシューティングのヒント

- [Microsoft サーバ タイプ (Microsoft Server Type)] として [MOC サーバ OCS (MOC server OCS)] を選択した場合は、複数のライン アピアランスを使用してリモート通話コントロールを実施するユーザのために、Microsoft Office Communicator に Phone Selection プラグインをインストールする必要があります。Phone Selection プラグインをインストールすると、Microsoft Office Communicator クライアントにタブが追加されて、制御するライン アピアランスをユーザが選択できるようになります。
- [Microsoft サーバ タイプ (Microsoft Server Type)] として [MOC サーバ LCS (MOC server LCS)] を選択した場合は、リモート通話コントロール機能によって、Cisco Unified Presence の既存のデバイス選択ロジックに基づき制御するデバイスが決定されます。

関連項目

- 「CTI ゲートウェイのためのアプリケーション ユーザの設定」 (P.6)
- 「Phone Selection プラグインを配置する方法」 (P.31)
- 「固定電話制御のトラブルシュータの実行」 (P.11)

次の作業

「ユーザの機能の割り当て」 (P.10)

ユーザの機能の割り当て

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)] > [固定電話制御 (Desk Phone Control)] > [ユーザ割り当て (User Assignment)] を選択します。

ステップ 2 [検索 (Find)] を選択します。

ステップ 3 固定電話機能を割り当てるユーザを確認します。

ステップ 4 [選択したユーザの割り当て (Assign Selected Users)] を選択します。

ステップ 5 [固定電話制御の割り当て (Desk Phone Control Assignment)] ウィンドウで [固定電話制御を有効にする (Enable Desk Phone Control)] をオンにします。

ステップ 6 [保存 (Save)] を選択します。

トラブルシューティングのヒント

- 固定電話制御機能を各 Microsoft Office Communicator ユーザに割り当てたことを確認します。
- リモート通話コントロール機能のある LCS を使用している場合は、Cisco Unified Communications Manager でユーザごとに最大 2 つのデバイスを関連付けることができます。ユーザが Extension Mobility (EM; 拡張モビリティ) デバイスにサインインしている場合、EM デバイスはユーザに関連付けることができる 2 つのデバイスのうちの 1 つであると見なされます。

次の作業

[「Cisco Unified Presence と統合するための Microsoft コンポーネントの設定方法」\(P.11\)](#)

関連項目

- [「Cisco Unified Presence での CTI 接続の設定」\(P.9\)](#)
- [「固定電話制御のトラブルシュータの実行」\(P.11\)](#)

固定電話制御のトラブルシュータの実行

固定電話制御トラブルシュータは、Microsoft Office Communicator クライアントと Cisco Unified Presence との統合をサポートする設定を検証します。

手順

ステップ 1 [Cisco Unified Presence の管理 (Cisco Unified Presence Administration)] > [診断 (Diagnostics)] > [固定電話制御トラブルシュータ (Desk Phone Control Troubleshooter)] を選択します。

ステップ 2 有効なユーザ ID を入力します。



ヒント ユーザの ID を検索するには、[検索 (Search)] を選択します。

ステップ 3 Microsoft OCS サーバアドレスを入力します。

ステップ 4 [送信 (Submit)] を選択します。

6 Cisco Unified Presence と統合するための Microsoft コンポーネントの設定方法

- [「Microsoft Active Directory での回線 URI の設定」\(P.12\)](#)
- [「Cisco Unified Presence でのユーザ認証」\(P.12\)](#)
- [「Microsoft Active Directory の設定」\(P.13\)](#)
- [「Microsoft OCS 設定の概要」\(P.14\)](#)

Microsoft Active Directory での回線 URI の設定

Microsoft Active Directory で回線 URI パラメータを設定する場合は、次の点に注意してください。

- 回線 URI には、`tel:xxxx;phone-context=dialstring` の形式を使用することを推奨します。
 - `xxxx` には、コールの発信時に CTI マネージャが発信番号または着信番号として Cisco Unified Presence に報告する、ディレクトリ番号を指定します。
 - `phone-context=dialstring` を指定すると、Microsoft Office Communicator ディレクトリ番号に関連付けられているデバイスのいずれかをクライアントが制御できるようになります。
- デバイス ID を設定する場合、Microsoft Office Communicator クライアントは最初のサインイン時にその ID に対応するデバイスを制御します。たとえば、`tel:xxxx;phone-context=dialstring;device=SEP0002FD3BB5C5` となります。
- パーティションを設定する場合、Microsoft Office Communicator クライアントはディレクトリ番号のパーティションを指定します。たとえば、`tel:xxxx;phone-context=dialstring;device=SEP0002FD3BB5C5;partition=myPartition` となります。
- 回線 URI は、Microsoft Office Communicator ユーザがサインインするときだけ有効になります。
- 初回のサインイン後、Microsoft Office Communicator ユーザは Phone Selection プラグインを使用して、制御するラインアピアランスを変更できます。
- 回線 URI でデバイス ID を設定しないと、CTI ゲートウェイが回線の Directory Number (DN; ディレクトリ番号) に関連付けられるデバイスを決定します。回線の DN にデバイスが 1 つだけ関連付けられていると、CTI ゲートウェイはそのデバイスを使用します。
- Microsoft LCS を配置し、回線 URI でデバイス ID を設定せず、2 つのデバイスを回線の DN に関連付けている場合 (共有回線)、CTI ゲートウェイは次の規則に従ってデバイスを選択します。
 - この 2 つのデバイスのいずれかが Cisco IP Communicator であり、そのステータスが登録されている場合、CTI ゲートウェイはそのデバイスを使用します。
 - この 2 つのデバイスのいずれかが Cisco IP Communicator であるものの、そのステータスが登録されていない場合、CTI ゲートウェイはもう一方のデバイスを使用します。
 - 2 つのデバイスとも Cisco IP Communicator ではない場合、Microsoft Office Communicator ユーザがサインインすると両方の電話機が鳴ります。ユーザは、電話機に応答してそのデバイスを制御する必要があります。
 - 3 つ以上のデバイスを回線の DN に関連付けている場合は、回線 URI で目的のデバイスを指定する必要があります。

関連項目

- 「ラインアピアランス」 (P.4)
- 「Cisco Unified Presence でのユーザ認証」 (P.12)
- 「Phone Selection プラグインを配置する方法」 (P.31)

Cisco Unified Presence でのユーザ認証

Microsoft Active Directory で SIP URI を設定するときは、Cisco Unified Presence がどのようにユーザ認証チェックを実行するかを考慮してください。ユーザ認証ロジックは次のとおりです。

1. Cisco Unified Presence が、Microsoft Office Communicator (サインイン) ユーザ ID が Cisco Unified Communications Manager ユーザ ID に一致するかどうかを確認します。Cisco Unified Presence が一致を検出できない場合：
2. Cisco Unified Presence が、Microsoft Office Communicator ユーザ電子メール (発信元ヘッダー) が Cisco Unified Communications Manager ユーザ電子メールに一致するかどうかを確認します。Cisco Unified Presence が一致を検出できない場合：
3. Cisco Unified Presence が、Microsoft Office Communicator ユーザ電子メールが Cisco Unified Communications Manager ユーザの `ocsPrimaryAddress` 値に一致するかどうかを確認します。

たとえば、ユーザ Joe の Microsoft Office Communicator ユーザ ID が `joe@someCompany.com` であるとします。SIP INVITE の発信元ヘッダーは `sip:joe@someCompany.com` です。

この場合、Cisco Unified Presence は次のチェックを実施します。

- Cisco Unified Communications Manager データベースにユーザ ID が「joe」であるユーザが存在するかどうか。このユーザ ID が存在しない場合：
- Cisco Unified Communications Manager データベースにメールが `joe@someCompany.com` であるユーザが存在するかどうか。このメールが存在しない場合：
- Cisco Unified Communications Manager データベースに `ocsPrimaryAddress` が「`sip:joe@someCompany.com`」であるユーザが存在するかどうか。

Microsoft Active Directory の設定

始める前に

- Microsoft Active Directory での回線 URI 設定に関するトピックに目を通します。
- Cisco Unified Presence でのユーザ認証チェックに関するトピックに目を通します。

手順

ステップ 1 Microsoft Active Directory アプリケーション ウィンドウから、各特定のユーザに関連付けるユーザ名および電話番号を追加します。

ステップ 2 追加したユーザごとに、Microsoft Active Directory で [プロパティ (Properties)] ウィンドウを開き、次のパラメータを設定します。

- a. Live Communications を有効にします。
- b. SIP URI を入力します。
- c. Microsoft OCS サーバ名またはプールを入力します。



注意

OCS サーバ名またはプール名にはアンダースコア文字が含まれていないことを確認します。

- d. [リモート ユーザ アクセス (Remote User Access)] をオンにします。
- e. [リモート通話コントロール (Remote Call Control)] をオンにします。
- f. 回線 URI 値を入力します。この値を入力するときは、次の点に注意してください。

ステップ 3 リモート通話コントロール SIP URI を、たとえば `sip:8000@my-cups.my-domain.com` のように入力します。`my-cups.my-domain.com` には、この統合のために設定した Cisco Unified Presence サーバの FQDN を指定します。

トラブルシューティングのヒント

- Microsoft Active Directory で入力する SIP URI は、Microsoft OCS でスタティック ルートを設定しているときに定義するスタティック ルート URI に一致する必要があります。

関連項目

- [「Microsoft Active Directory での回線 URI の設定」 \(P.12\)](#)
- [「Cisco Unified Presence でのユーザ認証」 \(P.12\)](#)
- [「ライン アピアランス」 \(P.4\)](#)

- Microsoft Windows Server Active Directory のマニュアル：
<http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.mspx>

次の作業

「Microsoft OCS 設定の概要」(P.14)

Microsoft OCS 設定の概要



(注) このトピックでは、この統合のために Microsoft OCS で必要になる設定について簡単に説明します。Microsoft OCS 設定の詳細な説明は、この章では触れません。Microsoft OCS のマニュアルを参照してください。

Microsoft OCS サーバが正しくインストールされてアクティブになっていることを確認します。Microsoft OCS で次の項目が設定されていることを確認します。

- 証明書設定
- スタティック ルート
- 認証済みホスト
- ドメイン ネーム サーバ
- プール プロパティ
- サーバ プロパティ
- プール ユーザ
- ユーザ設定
- Microsoft Office Communicator (MOC) 設定

関連項目

- 「Microsoft Active Directory での正規化規則の設定」(P.14)
- 「Microsoft OCS のセキュリティ証明書を設定する方法」(P.22)
- 「Microsoft OCS での Cisco Unified Presence のための TLS ルートの設定」(P.27)
- 「Microsoft OCS での認証済みホストとしての Cisco Unified Presence の設定」(P.28)
- Microsoft OCS のマニュアル：
<http://office.microsoft.com/en-us/communicationsserver/FX101729111033.aspx>

7 Microsoft Active Directory で正規化規則を設定する方法

- 「Microsoft Active Directory での正規化規則の設定」(P.14)
- 「Microsoft Office Communicator インターフェイスでのユーザ名表示の確認」(P.15)
- 「サンプルの正規化規則」(P.16)

Microsoft Active Directory での正規化規則の設定

ディレクトリ番号からユーザ名への逆ルックアップは、次の条件下では機能しません。

- Microsoft Office Communicator ユーザが Cisco Unified IP Phone を制御している
- そのユーザへの着信音声コールがある

- ユーザのディレクトリ番号が、Active Directory に E.164 として設定されている
- Active Directory 電話番号正規化規則が設定されていない

このような条件下では、アプリケーションはコールを内線番号から発信されたものと見なし、ユーザ名が Microsoft Office Communicator に表示されません。

このため、コールが発信されると表示されるポップアップ ウィンドウで Microsoft Office Communicator ユーザが発信側の名前を参照できるようにするには、Microsoft Office Communicator サーバに Active Directory アドレス帳の正しい正規化規則を設定する必要があります。



(注) 内線ダイヤリング用の正規化規則ファイルを用意する必要があります。例については、正規化規則のサンプルを取り上げているトピックを参照してください。

始める前に

証明書を正しく配布してアドレス帳の同期を取るには、Microsoft OCS の CA 署名済み証明書が Microsoft Office Communicator PC に存在する必要があります。Verisign や RSA など広く普及している CA を証明書の署名に使用している場合は、CA 証明書がすでに PC にインストールされている可能性があります。

手順

ステップ 1 正規化規則をこのファイルに追加するには、ディレクトリパス C:\Program Files\Microsoft Office Communications Server 2007\Web Components\Address Book Files\Files\Company_Phone_Number_Normalization_Rules.txt を使用します。

ステップ 2 アドレス帳サーバ (ABServer) を実行し、正規化規則を再生成するには、ディレクトリパス C:\Program Files\Microsoft Office Communications Server 2007\Server\Core>AbsServer.exe -regenUR を使用します。



(注) UR の再生成が正常に完了するまで、最大 5 分間待機することになる場合があります。

ステップ 3 ABServer を同期するには、ディレクトリパス C:\Program Files\Microsoft Office Communications Server 2007\Server\Core>ABSServer.exe -syncnow を使用します。



(注) ABServer の同期が正常に完了するまで、最大 5 分間待機することになる場合があります。

ステップ 4 同期の完了後、Microsoft OCS サーバのイベント ビューアで、同期が完了していることを確認します。

ステップ 5 電話番号 C:\Program Files\Microsoft Office Communications Server 2007\Server\Core>AbsServer.exe -testPhoneNorm <E164 phone number> で正規化規則をテストします。

関連項目

- 「サンプルの正規化規則」 (P.16)

次の作業

[「Microsoft Office Communicator インターフェイスでのユーザ名表示の確認」 \(P.15\)](#)

Microsoft Office Communicator インターフェイスでのユーザ名表示の確認

コールが発信されると表示される Microsoft Office Communicator ポップアップ ウィンドウでユーザが発信側の名前を参照できるということを、確認する必要があります。

始める前に

Microsoft Active Directory で正規化規則を設定します。

手順

-
- ステップ 1** Microsoft Office Communicator を終了します。ただし、サインアウトしないでください。
 - ステップ 2** C:\Documents and Settings\<username>\Local Settings\Application Data\Microsoft\Communicator にあるアドレス帳ファイル contacts.db を削除します。
 - ステップ 3** Microsoft Office Communicator クライアントを起動し、再度サインインします。
 - ステップ 4** galcontacts.db が作成されていることを確認します。
 - ステップ 5** 再度 Microsoft Office Communicator を終了し、サインインし、Microsoft Office Communicator にユーザ名が表示されることを確認します。
-

関連項目

- [「Microsoft Active Directory での正規化規則の設定」 \(P.14\)](#)
- [「サンプルの正規化規則」 \(P.16\)](#)

サンプルの正規化規則

```
# ++ test RTP
## PSTN:+61262637900, Extension:37XXX
# +61262637ddd
[\s()\-\.\/\+]* (61)? [\s()\-\.\/]* 0? (2) \) ? [\s()\-\.\/]* (6263) [\s()\-\.\/]* (7\d\d\d)
3$4;phone-context=dialstring
# ++ test1 RTP
## Site:, PSTN:+61388043300, Extension:33XXX
[\s()\-\.\/\+]* (61)? [\s()\-\.\/]* 0? (3) \) ? [\s()\-\.\/]* (8804) [\s()\-\.\/]* (3\d\d\d)
3$4;phone-context=dialstring
#Test input +61388043187, Test result-> tel:33187;phone-context=dialstring
# ++ test2 RTP
## PSTN:+61292929000, Extension:29XXX
[\s()\-\.\/\+]* (61)? [\s()\-\.\/]* 0? (2) \) ? [\s()\-\.\/]* (9292) [\s()\-\.\/]* (9\d\d\d)
2$4;phone-context=dialstring
# Test input +61292929761, test result-> tel:29761;phone-context=dialstring
```

内線ダイヤリング用の正規化規則ファイルを用意する必要があります。たとえば、3桁の内線ダイヤリングの正規化規則は次のようになります。

```
^(\d{3})
$1;phone-context=dialstring
```

関連項目

- [「Microsoft Active Directory での正規化規則の設定」 \(P.14\)](#)
- [「Microsoft Office Communicator インターフェイスでのユーザ名表示の確認」 \(P.15\)](#)

8 Cisco Unified Presence のセキュリティ証明書を設定する方法

このトピックを適用できるのは、Cisco Unified Presence と Microsoft OCS との間にセキュアな接続を必要とする場合だけです。



(注) SIP プロキシ証明書（所有および信頼）は、X.509 バージョン 3 に準拠する必要があります。

- 「スタンドアロン ルート認証局（CA）の設定」 (P.17)
- 「Cisco Unified Presence へのルート証明書のアップロード」 (P.18)
- 「Cisco Unified Presence の証明書署名要求の生成」 (P.19)
- 「Cisco Unified Presence からの証明書署名要求のダウンロード」 (P.20)
- 「CA サーバでの証明書署名要求の送信」 (P.20)
- 「CA サーバからの署名済み証明書のダウンロード」 (P.21)
- 「Cisco Unified Presence への署名済み証明書のアップロード」 (P.22)

スタンドアロン ルート認証局（CA）の設定

手順

- ステップ 1** ドメイン管理者権限で CA サーバにサイン インします。
- ステップ 2** Windows Server 2003 CD を挿入します。
- ステップ 3** [スタート (Start)] > [設定 (Settings)] > [コントロール パネル (Control Panel)] を選択します。
- ステップ 4** [プログラムの追加と削除 (Add or Remove Programs)] をダブルクリックします。
- ステップ 5** [Windows コンポーネントの追加と削除 (Add/Remove Windows Components)] を選択します。
- ステップ 6** [アプリケーション サーバ (Application Server)] を選択します。
- ステップ 7** [インターネット インフォメーション サービス (IIS) (Internet Information Services (IIS))] を選択します。
- ステップ 8** インストール手順を完了します。
- ステップ 9** [Windows コンポーネントの追加と削除 (Add/Remove Windows Components)] を選択します。
- ステップ 10** [証明書サービス (Certificate Services)] を選択します。
- ステップ 11** [次へ (Next)] を選択します。
- ステップ 12** [スタンドアロンのルート CA (Standalone root CA)] を選択します。
- ステップ 13** [次へ (Next)] を選択します。
- ステップ 14** CA ルートの名前を入力します。



(注) この名前は、フォレスト ルートの CA ルートをわかりやすくした名前にすることができます。

- ステップ 15** 時間をこの証明書に必要な年数に変更します。
- ステップ 16** [次へ (Next)] を選択して、インストールを開始します。
- ステップ 17** 証明書データベースおよび証明書データベース ファイルの場所を選択します。
- ステップ 18** [次へ (Next)] を選択します。
- ステップ 19** IIS を停止するように求められたら、[はい (Yes)] を選択します。

ステップ 20 Active Server Pages に関するメッセージが表示されたら [はい (Yes)] を選択します。

ステップ 21 [完了 (Finish)] を選択します。

次の作業

「CA サーバからのルート証明書のダウンロード」(P.18)。

CA サーバからのルート証明書のダウンロード

始める前に

スタンドアロン ルート Certificate Authority (CA; 認証局) を設定します。

手順

ステップ 1 CA サーバにサイン インし、Web ブラウザを開きます。

ステップ 2 URL `http://<ca_server_IP_address>/certsrv` を開きます。

ステップ 3 [CA 証明書、証明書チェーン、または CRL のダウンロード (Download a CA certificate, certificate chain, or CRL)] を選択します。

ステップ 4 [エンコード方式 (Encoding Method)] で [Base 64] を選択します。

ステップ 5 [CA 証明書のダウンロード (Download CA Certificate)] を選択します。

ステップ 6 証明書ファイル `certnew.cer` をローカル ディスクに保存します。

トラブルシューティングのヒント

ルート証明書のサブジェクトの Common Name (CN; 共通名) がわからない場合は、外部の証明書管理ツールを使用して探すことができます。Windows オペレーティング システムでは、拡張子が `.cer` の証明書ファイルを右クリックして、証明書のプロパティを開くことができます。

関連項目

- 「スタンドアロン ルート認証局 (CA) の設定」(P.17)

次の作業

「Cisco Unified Presence へのルート証明書のアップロード」(P.18)

Cisco Unified Presence へのルート証明書のアップロード

始める前に

CA サーバからルート証明書をダウンロードします。

手順

ステップ 1 Cisco Unified Presence サーバの管理に使用するローカル コンピュータに `certnew.cer` ファイルをコピーします。

ステップ 2 [Cisco Unified オペレーティング システムの管理 (Cisco Unified Operating System Administration)] > [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。

ステップ 3 [証明書のアップロード (Upload Certificate)] を選択します。

ステップ 4 [証明書の名前 (Certificate Name)] メニューから [cup-trust] を選択します。



(注) ルート名のフィールドは空白のままにしておきます。

ステップ 5 [参照 (Browse)] を選択します。

ステップ 6 ローカル コンピュータで certnew.cer ファイルがある場所に移動します。



(注) 証明書ファイルの拡張子を .pem に変更することが必要になる場合があります。

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



ヒント [証明書の管理 (Certificate Management)] の検索画面を使用して、cup-trust にアップロードした新規 CA 証明書ファイル名を書き留めます。この証明書ファイル名 (拡張子の .pem または .der 以外) が、CA 署名済み SIP プロキシ証明書をアップロードするときにルート CA のフィールドに入力する値となります。

関連項目

- 「CA サーバからのルート証明書のダウンロード」 (P.18)
- 「Cisco Unified Presence への署名済み証明書のアップロード」 (P.22)

次の作業

「Cisco Unified Presence の証明書署名要求の生成」 (P.19)

Cisco Unified Presence の証明書署名要求の生成

始める前に

Cisco Unified Presence にルート証明書をアップロードします。

手順

ステップ 1 [Cisco Unified オペレーティング システムの管理 (Cisco Unified Operating System Administration)] > [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。

ステップ 2 [CSR の作成 (Generate CSR)] を選択します。

ステップ 3 [証明書の名前 (Certificate Name)] メニューから [cup] を選択します。

ステップ 4 [CSR の作成 (Generate CSR)] を選択します。

関連項目

- 「Cisco Unified Presence へのルート証明書のアップロード」 (P.18)

次の作業

「Cisco Unified Presence からの証明書署名要求のダウンロード」 (P.20)

Cisco Unified Presence からの証明書署名要求のダウンロード

始める前に

Cisco Unified Presence の証明書署名要求を生成します。

手順

-
- ステップ 1** [Cisco Unified オペレーティング システムの管理 (Cisco Unified Operating System Administration)] > [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。
 - ステップ 2** [CSR のダウンロード (Download CSR)] を選択します。
 - ステップ 3** [証明書の名前 (Certificate Name)] メニューから [cup] を選択します。
 - ステップ 4** [CSR のダウンロード (Download CSR)] を選択します。
 - ステップ 5** [保存 (Save)] を選択して、cup.csr ファイルをローカル コンピュータに保存します。
-

関連項目

- [「Cisco Unified Presence の証明書署名要求の生成」 \(P.19\)](#)

次の作業

[「CA サーバでの証明書署名要求の送信」 \(P.20\)](#)

CA サーバでの証明書署名要求の送信

始める前に

Cisco Unified Presence から証明書署名要求をダウンロードします。

手順

-
- ステップ 1** 証明書要求ファイル cup.csr を CA サーバにコピーします。
 - ステップ 2** URL <http://local-server/certsrv> または <http://127.0.0.1/certsrv> を開きます。
 - ステップ 3** [証明書を要求する (Request a certificate)] を選択します。
 - ステップ 4** [証明書の要求の詳細設定 (Advanced certificate request)] を選択します。
 - ステップ 5** [Base64 でエンコードした CMC または PKCS #10 ファイルを使用して証明書要求を送信するか、Base64 でエンコードした PKCS #7 ファイルを使用して更新要求を送信する (Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file)] を選択します。
 - ステップ 6** メモ帳などのテキスト エディタを使用して、生成した cup 自己証明書を開きます。
 - ステップ 7** 次の行から、
-----BEGIN CERTIFICATE REQUEST
次の行までの情報をすべてコピーします。
END CERTIFICATE REQUEST-----
 - ステップ 8** 証明書要求の内容を [証明書要求 (Certificate Request)] テキスト ボックスに貼り付けます。
 - ステップ 9** [送信 (Submit)] を選択します。
要求 ID 番号が表示されます。

- ステップ 10** [管理ツール (Administrative Tools)] で [証明機関 (Certificate Authority)] を開きます。
[証明機関 (Certificate Authority)] ウィンドウの [保留中の要求 (Pending Requests)] の下に、送信したばかりの要求が表示されます。
- ステップ 11** その証明書要求を右クリックします。
- ステップ 12** [すべてのタスク (All Tasks)] > [発行 (Issue)] を選択します。
- ステップ 13** [発行した証明書 (Issued certificates)] を選択し、証明書が発行されていることを確認します。
-

関連項目

- 「[Cisco Unified Presence からの証明書署名要求のダウンロード](#)」 (P.20)

次の作業

「[CA サーバからの署名済み証明書のダウンロード](#)」 (P.21)

CA サーバからの署名済み証明書のダウンロード

始める前に

CA サーバで証明書署名要求を送信します。

手順

- ステップ 1** CA が実行されている Windows サーバで **http://<local_server>/certsrv** を開きます。
- ステップ 2** [保留中の証明書の要求の状態 (View the status of a pending certificate request)] を選択します。
- ステップ 3** 直前に送信された要求を表示するオプションを選択します。
- ステップ 4** [Base 64 エンコード (Base 64 encoded)] を選択します。
- ステップ 5** [証明書のダウンロード (Download certificate)] を選択します。
- ステップ 6** 署名済み証明書をローカル ディスクに保存します。
- ステップ 7** 証明書 **cup.pem** の名前を変更します。
- ステップ 8** cup.pem ファイルをローカル コンピュータにコピーします。
-

関連項目

- 「[CA サーバでの証明書署名要求の送信](#)」 (P.20)

次の作業

「[Cisco Unified Presence への署名済み証明書のアップロード](#)」 (P.22)

Cisco Unified Presence への署名済み証明書のアップロード

始める前に

CA サーバから署名済み証明書をダウンロードします。

手順

-
- ステップ 1** [Cisco Unified オペレーティング システムの管理 (Cisco Unified Operating System Administration)] > [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。
 - ステップ 2** [証明書のアップロード (Upload Certificate)] を選択します。
 - ステップ 3** [証明書の名前 (Certificate Name)] メニューから [cup] を選択します。
 - ステップ 4** ルート証明書の名前を指定します。ルート証明書の名前には、拡張子 .pem または .der が含まれている必要があります。
 - ステップ 5** [参照 (Browse)] を選択します。
 - ステップ 6** ローカル コンピュータで署名済みの **cup.pem** 証明書がある場所に移動します。
 - ステップ 7** [ファイルのアップロード (Upload File)] を選択します。
-

関連項目

- [「CA サーバからの署名済み証明書のダウンロード」 \(P.21\)](#)

次の作業

[「Microsoft OCS のセキュリティ証明書を設定する方法」 \(P.22\)](#)

9 Cisco Unified Presence と Microsoft OCS との間のセキュリティを設定する方法

このトピックを適用できるのは、Cisco Unified Presence と Microsoft OCS との間にセキュアな接続を必要とする場合だけです。

- [「Microsoft OCS のセキュリティ証明書を設定する方法」 \(P.22\)](#)
- [「Microsoft OCS での Cisco Unified Presence のための TLS ルートの設定」 \(P.27\)](#)
- [「Microsoft OCS での認証済みホストとしての Cisco Unified Presence の設定」 \(P.28\)](#)
- [「TLSv1 を使用するための Microsoft OCS の設定」 \(P.29\)](#)
- [「Cisco Unified Presence での Microsoft OCS の新規 TLS ピア サブジェクトの作成」 \(P.29\)](#)
- [「Cisco Unified Presence での、選択した TLS ピア サブジェクト リストへの TLS ピアの追加」 \(P.30\)](#)

Microsoft OCS のセキュリティ証明書を設定する方法

- [「CA 証明書チェーンのダウンロード」 \(P.23\)](#)
- [「CA 証明書チェーンのインストール」 \(P.23\)](#)
- [「CA サーバでの証明書要求の送信」 \(P.24\)](#)
- [「証明書の承認およびインストール」 \(P.26\)](#)
- [「インストールした証明書の設定」 \(P.27\)](#)

CA 証明書チェーンのダウンロード

手順

- ステップ 1** [スタート (Start)] > [ファイル名を指定して実行 (Run)] を選択します。
- ステップ 2** 次の手順を実行します。
- a.** `http://<name of your Issuing CA Server>/certsrv` と入力します。
 - b.** [OK] を選択します。
- ステップ 3** [タスクの選択 (Select a task)] から [CA 証明書、証明書チェーン、または CRL のダウンロード (Download a CA certificate, certificate chain, or CRL)] をクリックします。
- ステップ 4** [CA 証明書チェーンのダウンロード (Download CA certificate chain)] を選択します。
- ステップ 5** [ファイルのダウンロード (File Download)] ダイアログボックスで [保存 (Save)] を選択します。
- ステップ 6** サーバのハードディスク ドライブにファイルを保存します。
-

トラブルシューティングのヒント

証明書ファイルの拡張子は .p7b です。この .p7b ファイルを開くと、チェーンに次の 2 つの証明書が含まれるようになります。

- スタンドアロンのルート CA 証明書の名前
- スタンドアロンの下位 CA 証明書の名前 (ある場合)

次の作業

[「CA 証明書チェーンのインストール」 \(P.23\)](#)

CA 証明書チェーンのインストール

始める前に

CA 証明書チェーンをダウンロードします。

手順

- ステップ 1** [スタート (Start)] > [ファイル名を指定して実行 (Run)] を選択します。
- ステップ 2** 次の手順を実行します。
- a.** `mmc` と入力します。
 - b.** [OK] を選択します。
- ステップ 3** [ファイル (File)] > [スナップインの追加と削除 (Add/Remove Snap-in)] を選択します。
- ステップ 4** [スナップインの追加と削除 (Add/Remove Snap-in)] ダイアログボックスで [追加 (Add)] を選択します。
- ステップ 5** [利用できるスタンドアロン スナップイン (Available Standalone Snap-ins)] のリストで [証明書 (Certificates)] を選択します。
- ステップ 6** [追加 (Add)] を選択します。
- ステップ 7** [コンピュータ アカウント (Computer account)] を選択します。
- ステップ 8** [次へ (Next)] を選択します。

- ステップ 9** [コンピュータの選択 (Select Computer)] ダイアログボックスから次の手順を実行します。
- [ローカル コンピュータ : (このコンソールを実行しているコンピュータ) (Local computer: (the computer this console is running on))] を選択します。
 - [完了 (Finish)] を選択します。
 - [閉じる (Close)] を選択します。
 - [OK] を選択します。
- ステップ 10** [証明書 (Certificates)] コンソールの左ペインで、[証明書 (ローカル コンピュータ) (Certificates (Local Computer))] を展開します。
- ステップ 11** [信頼されたルート証明機関 (Trusted Root Certification Authorities)] を展開します。
- ステップ 12** [証明書 (Certificates)] を右クリックします。
- ステップ 13** 次の手順を実行します。
- [すべてのタスク (All Tasks)] をポイントします。
 - [インポート (Import)] を選択します。
- ステップ 14** インポートウィザードで [次へ (Next)] を選択します。
- ステップ 15** [参照 (Browse)] を選択し、自分のコンピュータ上で証明書チェーンがある場所に移動します。
- ステップ 16** [開く (Open)] を選択します。
- ステップ 17** [次へ (Next)] を選択します。
- ステップ 18** [証明書をすべて次のストアに配置する (Place all certificates in the following store)] をデフォルト値のままオンにしておきます。
- ステップ 19** [証明書ストア (Certificate store)] の下に [信頼されたルート証明機関 (Trusted Root Certification Authorities)] が表示されていることを確認します。
- ステップ 20** [次へ (Next)] を選択します。
- ステップ 21** [完了 (Finish)] を選択します。
-

関連項目

- 「CA 証明書チェーンのダウンロード」 (P.23)

次の作業

「CA サーバでの証明書要求の送信」 (P.24)

CA サーバでの証明書要求の送信

始める前に

CA 証明書チェーンをインストールします。

手順

- ステップ 1** 証明書を必要とするコンピュータで、Web ブラウザを開きます。
- ステップ 2** URL `http://<name of your Issuing CA server>/certsrv` を入力します。
- ステップ 3** Enter を押します。
- ステップ 4** [証明書を要求する (Request a certificate)] を選択します。
- ステップ 5** [証明書の要求の詳細設定 (Advanced certificate request)] を選択します。
- ステップ 6** [この CA への要求を作成し、送信する。(Create and submit a request to this CA.)] を選択します。

ステップ 7 [必要な証明書の種類 (Type of Certificate Needed)] リストで [その他 (Other)] を選択します。

ステップ 8 [識別情報 (Identifying Information)] セクションの [名前 (Name)] フィールドに、**FQDN** と入力します。この名前は、Microsoft OCS の名前 (通常は FQDN) に一致する必要があります。

ステップ 9 [OID] フィールドに、OID として **1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2** と入力します。



(注) OID の中央にある 2 つの 1 をカンマで区切ります。

ステップ 10 次のいずれかの手順を実行します。

- a. Windows Certificate Authority 2003 を使用している場合は、[キーのオプション (Key Options)] の [ローカル コンピュータの証明書ストアに証明書を格納する (Store certificate in the local computer certificate store)] をオンにします。
- b. Windows Certificate Authority 2008 を使用している場合は、このトピックの「トラブルシューティングのヒント」で説明している回避策を参照してください。

ステップ 11 わかりやすい名前を入力します。

ステップ 12 [送信 (Submit)] を選択します。

ステップ 13 [潜在するスクリプト違反 (Potential Scripting Violation)] ダイアログボックスで [はい (Yes)] を選択します。

トラブルシューティングのヒント

Windows Certificate Authority 2008 を使用している場合、証明書登録ページでローカル コンピュータ ストアに証明書を保存するためのオプションがなくなりました。上記のステップ 10 の代わりに、次の回避策を実行してください。

- a. Microsoft OCS サーバからサインアウトします。
- b. ローカル ユーザとして Microsoft OCS サーバにサインインします。
- c. 証明書を作成します。
- d. CA サーバから証明書を承認します。
- e. 証明書をファイルにエクスポートします。
- f. Microsoft OCS サーバからサインアウトします。
- g. ドメイン ユーザとして Microsoft OCS サーバにサインインします。
- h. 証明書ウィザードを使用して、証明書ファイルをインポートします。証明書が、Microsoft OCS 証明書のタブに表示されます (証明書がローカル コンピュータ ストアにインストールされるためです)。

関連項目

- [「CA 証明書チェーンのインストール」 \(P.23\)](#)

次の作業

[「証明書の承認およびインストール」 \(P.26\)](#)

証明書の承認およびインストール

始める前に

CA サーバで証明書要求を送信します。

手順

-
- ステップ 1 ドメイン管理者クレデンシャルで企業の下位 CA サーバにサイン インします。
 - ステップ 2 [スタート (Start)] > [ファイル名を指定して実行 (Run)] を選択します。
 - ステップ 3 次の手順を実行します。
 - a. mmc と入力します。
 - b. Enter を押します。
 - ステップ 4 [ファイル (File)] > [スナップインの追加と削除 (Add/Remove Snap-in)] を選択します。
 - ステップ 5 [追加 (Add)] を選択します。
 - ステップ 6 [スタンドアロン スナップインの追加 (Add Standalone Snap-in)] で [証明機関 (Certification Authority)] を選択します。
 - ステップ 7 [追加 (Add)] を選択します。
 - ステップ 8 [証明機関 (Certification Authority)] で、デフォルトのオプション [ローカル コンピュータ: (このコンソールを実行しているコンピュータ) (Local computer: (the computer this console is running on))] を受け入れます。
 - ステップ 9 [完了 (Finish)] を選択します。
 - ステップ 10 [閉じる (Close)] を選択します。
 - ステップ 11 [OK] を選択します。
 - ステップ 12 MMC で、[証明機関 (Certification Authority)] を展開し、発行証明書サーバを展開します。
 - ステップ 13 [保留中の要求 (Pending Requests)] を選択します。
 - ステップ 14 詳細ウィンドウで、次の手順を実行します。
 - a. 要求 ID で識別される要求を右クリックします。
 - b. [すべてのタスク (All Tasks)] をポイントします。
 - c. [発行 (Issue)] を選択します。
 - ステップ 15 証明書の要求元のサーバで [スタート (Start)] > [ファイル名を指定して実行 (Run)] を選択します。
 - ステップ 16 `http://<name of your Issuing CA Server>/certsrv` と入力します。
 - ステップ 17 [OK] を選択します。
 - ステップ 18 [タスクの選択 (Select a task)] から、[保留中の証明書の要求の状態 (View the status of a pending certificate request)] を選択します。
 - ステップ 19 証明書要求を選択します。
 - ステップ 20 [この証明書のインストール (Install this certificate)] を選択します。
-

関連項目

- 「CA サーバでの証明書要求の送信」 (P.24)

次の作業

「インストールした証明書の設定」 (P.27)

インストールした証明書の設定

始める前に

証明書を承認し、インストールします。

手順

- ステップ 1** [スタート (Start)] > [プログラム (Programs)] > [管理ツール (Administrative Tools)] > [インターネット インフォメーション サービス (IIS) マネージャ (Internet Information Services (IIS) Manager)] を選択します。
- ステップ 2** 右側のペインで (ローカル コンピュータ) ツリーを展開します。
- ステップ 3** [既定の Web サイト (Default Web Site)] を選択します。
- ステップ 4** [プロパティ (Properties)] ダイアログボックスを右クリックして開きます。
- ステップ 5** [既定の Web サイトのプロパティ (Default Web Site Properties)] ダイアログボックスから [証明書 (Certificate)] タブを選択します。
- ステップ 6** 証明書がすでに選択されている場合は、[証明書の削除 (Delete Certificate)] を選択して、選択を解除します。
- ステップ 7** [証明書 (Certificate)] を選択して、証明書ウィザードを起動します。
- ステップ 8** 証明書ウィザードを使用して、Microsoft OCS のためにインストールした証明書を選択します。
- ステップ 9** **Microsoft Office Communications Server 2007** アプリケーションを起動します。
- ステップ 10** 右側のペインで、ローカル マシンを表すサーバを選択します。
- ステップ 11** サーバを右クリックします。
- ステップ 12** [プロパティ (Properties)] > [フロントエンドのプロパティ (Front End Properties)] を選択します。
- ステップ 13** [証明書 (Certificate)] タブを選択します。
- ステップ 14** [証明書の選択 (Select Certificate)] を選択します。
- ステップ 15** Microsoft OCS のためにインストールした証明書を検索し、選択します。



- (注)** Microsoft LCS を使用している場合は、上記のステップ 1 ~ 7 に従って、**Microsoft Live Communications Server 2005** アプリケーションを開きます。管理ページから、目的のサーバを右クリックして、[プロパティ (Properties)] ダイアログボックスを開きます。[セキュリティ (Security)] タブを選択し、[証明書の選択 (Select Certificate)] を選択して、新規にインストールした LCS 証明書を選択します。

関連項目

- 「証明書の承認およびインストール」 (P.26)

次の作業

「Microsoft OCS での Cisco Unified Presence のための TLS ルートの設定」 (P.27)

Microsoft OCS での Cisco Unified Presence のための TLS ルートの設定

手順

- ステップ 1** **Microsoft Office Communications Server 2007** アプリケーションを起動します。
- ステップ 2** 右側のペインで Microsoft OCS Server プールを右クリックします。
- ステップ 3** [プロパティ (Properties)] > [フロント エンドのプロパティ (Front End Properties)] を選択します。

- ステップ 4** [フロントエンドサーバーのプロパティ (Front End Server Properties)] ダイアログボックスから、[ルーティング (Routing)] タブを選択します。
- ステップ 5** [追加 (Add)] を選択します。
- ステップ 6** 次の手順を実行して、スタティック ルートを追加します。
- [ドメイン (Domain)] フィールドに Cisco Unified Presence のホスト名 /FQDN を入力します。



(注) これは、Cisco Unified Presence 証明書のサブジェクトの CN と一致する必要があります。一致しない場合、Microsoft OCS は Cisco Unified Presence との TLS 接続を確立しません。

- [転送 (Transport)] メニューから [TLS] を選択します。
- [ポート (Port)] フィールドに **5062** と入力します。ポート番号 5062 は、Cisco Unified Presence がピア認証 TLS 接続をリッスンするデフォルトのポートです。
- [要求 URI 内のホストを置き換える (Replace host in request URI)] をオンにします。
- [OK] を選択します。

トラブルシューティングのヒント

[Cisco Unified オペレーティング システムの管理 (Cisco Unified Operating System Administration)] > [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択し、証明書の一覧に登録されている証明書を選択すると、Cisco Unified Presence 証明書のサブジェクトの CN を確認できます。

次の作業

[「Microsoft OCS での認証済みホストとしての Cisco Unified Presence の設定」 \(P.28\)](#)

Microsoft OCS での認証済みホストとしての Cisco Unified Presence の設定

手順

- ステップ 1** **Microsoft Office Communications Server 2007** アプリケーションを起動します。
- ステップ 2** 右側のペインで Microsoft OCS Server プールを右クリックします。
- ステップ 3** [プロパティ (Properties)] > [フロントエンドのプロパティ (Front End Properties)] を選択します。
- ステップ 4** [ホストの承認 (Host Authorization)] タブを選択します。
- ステップ 5** [追加 (Add)] を選択します。
- ステップ 6** FQDN を選択し、証明書の記載どおりに CUP X.509 サブジェクトの共通名を入力します。
- ステップ 7** [サーバーとして帯域を制限する (Throttle as server)] をオンにします。
- ステップ 8** [認証済みとして扱う (Treat as Authenticated)] をオンにします。
- ステップ 9** [OK] を選択します。
- ステップ 10** Microsoft OCS サーバを再起動します。
- サーバが再起動すると、Microsoft OCS サーバプールに、設定したばかりの発信スタティック ルートが表示されます。

次の作業

[「TLSv1 を使用するための Microsoft OCS の設定」 \(P.29\)](#)

TLSv1 を使用するための Microsoft OCS の設定

Cisco Unified Presence は TLSv1 のみをサポートするため、TLSv1 を使用するように Microsoft OCS を設定する必要があります。この手順では、Microsoft OCS が TLS 暗号 TLS_RSA_WITH_3DES_EDE_CBC_SHA で TLSv1 を送信できるように、Microsoft OCS で FIPS 準拠のアルゴリズムを設定する方法について説明します。この手順では、Microsoft OCS がドメイン コントローラに設定されています。

手順

-
- ステップ 1** [スタート (Start)] > [管理ツール (Administrative Tools)] > [ドメイン コントローラ セキュリティ ポリシー (Domain Controller Security Policy)] を選択します。
 - ステップ 2** コンソール ツリーで [セキュリティの設定 (Security Settings)] を選択します。
 - ステップ 3** [ローカル ポリシー (Local Policies)] を選択します。
 - ステップ 4** [セキュリティ オプション (Security Options)] を選択します。
 - ステップ 5** 詳細ウィンドウで FIPS セキュリティ設定をダブルクリックします。
 - ステップ 6** セキュリティ設定を変更します。
 - ステップ 7** [OK] を選択します。
-

次の作業

[「Cisco Unified Presence での Microsoft OCS の新規 TLS ピア サブジェクトの作成」 \(P.29\)](#)

Cisco Unified Presence での Microsoft OCS の新規 TLS ピア サブジェクトの作成

手順

-
- ステップ 1** [Cisco Unified Presence の管理 (Cisco Unified Presence Administration)] > [Cisco Unified Presence] > [セキュリティ (Security)] > [TLS ピア サブジェクト (TLS Peer Subjects)] 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** [ピア サブジェクト名 (Peer Subject Name)] フィールドに、Microsoft OCS が提示する証明書のサブジェクト CN を入力します。
 - ステップ 4** [説明 (Description)] フィールドに Microsoft OCS サーバの名前を入力します。
 - ステップ 5** [保存 (Save)] を選択します。
-

次の作業

[「Cisco Unified Presence での、選択した TLS ピア サブジェクト リストへの TLS ピアの追加」 \(P.30\)](#)

Cisco Unified Presence での、選択した TLS ピア サブジェクト リストへの TLS ピアの追加

始める前に

Microsoft OCS で Cisco Unified Presence の新規 TLS ピア サブジェクトを作成します。

手順

-
- ステップ 1** [Cisco Unified Presence の管理 (Cisco Unified Presence Administration)] > [システム (System)] > [セキュリティ (Security)] > [TLS コンテキスト設定 (TLS Context Configuration)] を選択します。
 - ステップ 2** [検索 (Find)] を選択します。
 - ステップ 3** [Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context] を選択します。
[TLS コンテキスト設定 (TLS Context Configuration)] ウィンドウが表示されます。
 - ステップ 4** 使用可能な TLS 暗号のリストから、[TLS_RSA_WITH_3DES_EDE_CBC_SHA] を選択します。
 - ステップ 5** 右矢印を選択して、この暗号を [選択された TLS 暗号 (Selected TLS Ciphers)] に移動します。
 - ステップ 6** [空の TLS フラグメントの無効化 (Disable Empty TLS Fragments)] をオンにします。
 - ステップ 7** 使用可能な TLS ピア サブジェクトのリストから、設定した TLS ピア サブジェクトを選択します。
 - ステップ 8** 右矢印を選択して、[選択された TLS ピア サブジェクト (Selected TLS Peer Subjects)] に移動します。
 - ステップ 9** [保存 (Save)] を選択します。
-

関連項目

「Cisco Unified Presence での Microsoft OCS の新規 TLS ピア サブジェクトの作成」 (P.29)

10 この統合の冗長性の設定

- 「TCP でのロード バランシング」 (P.30)

TCP でのロード バランシング

このトピックでは、着信 CSTA/TCP 接続で使用できるように、Cisco Unified Presence デュアル ノード設定でロード バランサを組み込む方法について説明します。ロード バランサには、Cisco CSS 11501 Content Services Switch を推奨します。

表 2 では、この統合に合わせて Cisco CSS 11501 Content Services Switch を設定する際に必要となるタスクの概要を示します。各タスクの詳細については、次の URL で Cisco CSS 11500 Content Services Switch のマニュアルを参照してください。

http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_installation_and_configuration_guides_list.html

表 2 TCP でのロード バランシングのための Cisco CSS 11501 設定チェックリスト

タスク	追加の注意事項
各 Cisco Unified Presence サーバの SIP サービス エントリを作成する。	<ul style="list-style-type: none"> • キープアライブ ポートは、内容と同じポート（ポート 5060）である必要があります。 • キープアライブ メッセージ タイプの値は「tcp」である必要があります。
SIP 規則を作成して、内容およびこの内容を管理するサービスを定義する。	<p>内容は、ポート 5060 の SIP です。</p> <p>(各 Cisco Unified Presence サーバの) SIP サービス エントリは、規則に関連付ける必要があります。</p>
ロード バランサの仮想 IP アドレスを表示するための Network Address Translation (NAT; ネットワーク アドレス変換) 規則を作成する。	NAT 規則では、Cisco Unified Presence サーバから Microsoft OCS に戻るパケットを、(Cisco Unified Presence サーバから直接発生したものではなく) ロード バランサから発生したものとして示します。

Microsoft OCS では、次のパラメータを設定する必要があります。

- SIP メッセージのルーティングに使用するロード バランサの仮想 IP アドレスとなるネクストホップ アドレス。
- ポート 5060 でのデフォルトの TCP リスナー。

Cisco Unified Presence では、ロード バランサの仮想 IP アドレスを設定する必要があります。これは、[Cisco Unified Presence の管理 (Cisco Unified Presence Administration)] > [システム (System)] > [サービス パラメータ (Service Parameters)] > [Cisco UP SIP プロキシ (Cisco UP SIP Proxy)] > [一般的なプロキシ パラメータ (クラスタ全体) (General Proxy Parameters (Clusterwide))] にある、仮想 IP アドレスのフィールドに設定します。

11 Phone Selection プラグインを配置する方法



(注) Phone Selection プラグインを適用できるのは、Cisco Unified Presence Release 7.0.3 以降を実行している場合のみです。

Phone Selection プラグインを導入すると、Microsoft Office Communicator クライアント インターフェイスに [Cisco Unified Presence] タブが追加され、制御する電話デバイスをユーザが選択できるようになります。Microsoft Office Communicator が Cisco Unified Presence サーバに接続し、図 2 に示すように、Microsoft Office Communicator の連絡先リストの下のペインに [電話の選択 (Phone Selection)] タブが表示されます。

次の場合、Phone Selection プラグインをインストールする必要があります。

- Cisco Unified Presence で、[Microsoft サーバ タイプ (Microsoft Server Type)] の値が [MOC サーバ OCS (MOC Server OCS)] になっている
- ユーザが複数のデバイス (回線) を保有している
- Microsoft OCS で、ユーザの回線 URI がライン アピアランスを一意に識別しない (たとえば、回線 URI に device= または partition= のいずれか、または両方がない)



(注) Microsoft LCS 2005 でリモート通話コントロール機能を実行している場合には、Phone Selection プラグインを使用できません。Microsoft LCS 2005 は、カスタマイズしたタブをサポートしないためです。Microsoft LCS 2005 を使用している場合は、リモート通話コントロール機能によって、Cisco Unified Presence のデバイス選択ロジックに基づき制御するデバイスが決定されます。[Cisco Unified Presence の管理 Cisco Unified Presence Administration] の GUI で、[アプリケーション (Application)] > [固定電話制御 (Deskphone Control)] > [設定 (Settings)] を選択し、[Microsoft サーバ タイプ (Microsoft Server Type)] の値として [MOC サーバ LCS (MOC Server LCS)] を選択します。

- 「クライアント PC での Phone Selection プラグインのインストール」 (P.32)
- 「Phone Selection プラグインのアンインストール」 (P.34)
- 「プラグイン関連情報のユーザへの提供」 (P.34)

クライアント PC での Phone Selection プラグインのインストール

始める前に

この手順を実行するには、Phone Selection プラグイン インストーラ ファイル **Cisco MOC RCC Plug-in.msi** が必要です。これは、[Cisco Unified Presence の管理 (Cisco Unified Presence Administration)] からダウンロードできます。[アプリケーション (Application)] > [プラグイン (Plugins)] を選択し、**Cisco Unified Presence MOC Remote Call Control** プラグインをダウンロードします。

手順

ステップ 1 クライアント PC で次のコマンドを実行します。CUPFQDN 値には、Cisco Unified Presence サーバの FQDN を指定します。

```
msiexec /I "<plug_in_filename>.msi" CUPFQDN=my-CUP.cisco.com /L*V install_log.txt
```



(注) このコマンドで Cisco Unified Presence サーバの FQDN を指定しない場合、プラグインのインストールが中断します。

ステップ 2 インストール手順に従ってインストールを進め、Phone Selection プラグインのインストールを完了します。

ステップ 3 Microsoft Office Communicator を起動し、Cisco Unified Presence タブが接続されてインターフェイスに表示されることを確認します。

トラブルシューティングのヒント

Microsoft Office Communicator クライアントが Cisco Unified Presence タブに接続できない場合は、次の点を確認してください。

- Cisco Unified Presence サーバに対して無効な IP アドレスまたは FQDN を指定した可能性があります。プラグインのインストール手順を繰り返して、ステップ 1 のコマンドで正しい Cisco Unified Presence サーバ アドレスを指定します。
- タブ接続の問題が発生した場合には、次の点に注意してください。
 - クライアント PC でブラウザを開き、信頼される Web アドレスのリストに Cisco Unified Presence サーバの Web アドレスを追加することが必要になる場合があります。Microsoft Internet Explorer で、[インターネットオプション (Internet Options)] > [セキュリティ (Security)] > [信頼済みサイト (Trusted Sites)] を選択し、Web アドレス **https://<Cisco Unified Presence_server_name>** を、信頼される Web アドレスのリストに追加します。
 - Cisco Unified Presence サーバのセキュリティ ゾーンにドメインの HTTPS Web アドレスを追加することが必要になる場合があります。Microsoft Internet Explorer で、[インターネットオプション (Internet Options)] > [セキュリティ (Security)] > [ローカルイントラネット (Local intranet)] > [サイト (Sites)] > [詳細設定 (Advanced)] を選択し、セキュリティ ゾーンの Web アドレスのリストにエントリ **https://*.your-domain** を追加します。
- この機能を使用するための権限がないことをユーザに通知するエラー メッセージが表示される場合は、Cisco Unified Presence で Microsoft Office Communicator に対してユーザを有効にする必要があります。

Microsoft Vista プラットフォームを実行しているときに、プラグインのインストールで問題が発生した場合は、クライアント PC で User Access Control (UAC; ユーザ アクセス制御) を無効にすることが必要になる場合があります。UAC を無効にするには、次の手順に従います。

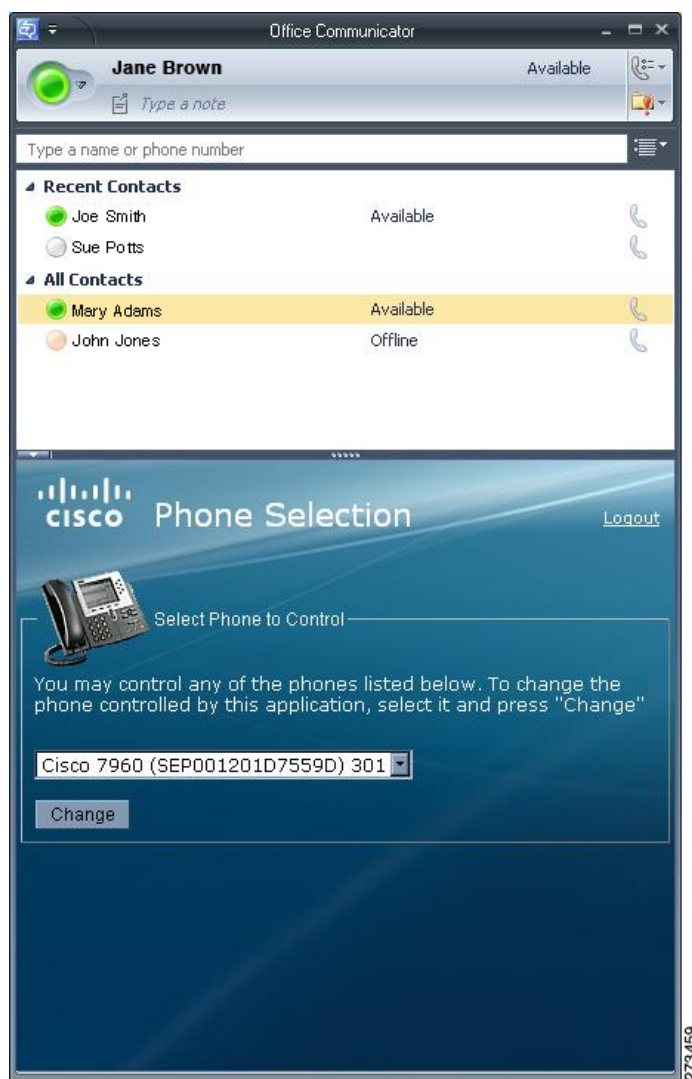
1. ローカル管理者グループのメンバーのクレデンシャルでクライアント PC にサイン インします。
2. [スタート (Start)] > [コントロール パネル (Control Panel)] > [ユーザー アカウント (User Accounts)] を選択します。

3. [ユーザー アカウント (User Accounts)] ペインで [ユーザー アカウント (User Accounts)] を選択します。
4. ユーザ アカウントの作業ペインで、[ユーザー アカウント制御の有効化または無効化 (Turn User Account Control On or Off)] を選択します。
5. UAC が現時点で管理者承認モードに設定されている場合は、ユーザ アカウント制御メッセージが表示されます。[続行 (Continue)] を選択します。
6. [ユーザー アカウント制御 (UAC) を使ってコンピュータの保護に役立たせる (Use User Account Control (UAC) to help protect your computer)] をオフにします。
7. [OK] を選択します。
8. [今すぐ再起動する (Restart Now)] を選択して変更を適用します。

関連項目

- 「[Phone Selection プラグインのアンインストール](#)」 (P.34)
- 「[プラグイン関連情報のユーザへの提供](#)」 (P.34)

図 2 [電話の選択 (Phone Selection)] タブのある Microsoft Office Communicator クライアント



Phone Selection プラグインのアンインストール

Phone Selection プラグインをアンインストールするには、クライアント PC で次のコマンドを実行します。

```
msiexec /x "<plug_in_filename>" /L*V install_log.txt
```

プラグイン関連情報のユーザへの提供

提供する情報	説明
サイン イン情報	Cisco Unified Presence インターフェイス用のユーザ名とパスワードが登録されたユーザ ベースを提供します。
Phone Selection プラグインを使用するための手順	『 <i>Quick Start Guide for the Phone Selection Plug-In for the Microsoft Office Communicator Call Control Feature for Cisco Unified Presence Release 7.03</i> 』をユーザに提供します。

12 詳細情報の入手

Cisco Unified Presence

Cisco Unified Presence の追加マニュアルについては、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6837/tsd_products_support_series_home.html

Cisco Unified Communications Manager

Cisco Unified Communications Manager のマニュアルについては、次の URL を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Microsoft Office Communications Server (OCS)

Microsoft OCS のインストール、設定、および配置の詳細については、次の URL を参照してください。

<http://office.microsoft.com/en-us/communicationsserver/FX101729111033.aspx>

Microsoft Live Communications Server (LCS)

Microsoft LCS のインストール、設定、および配置の詳細については、次の URL を参照してください。

<http://office.microsoft.com/en-us/communicationsserver/FX011526591033.aspx>

Microsoft Active Directory

Microsoft Windows Server Active Directory の詳細については、次の URL を参照してください。

<http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.mspx>

シスコは世界各国 200 箇所にオフィスを開設しています。
各オフィスの住所、電話番号、FAX 番号は当社の Web サイト (www.cisco.com/go/offices) をご覧ください。

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)

© 2010 Cisco Systems, Inc.
All rights reserved.

Copyright © 2010–2011, シスコシステムズ合同会社 .
All rights reserved.

お問い合わせは、購入された各代理店へご連絡ください。



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/>