



## Microsoft 製品との統合の概要

---

この章では、Microsoft 環境に Cisco Unified Presence を導入するために実行する必要がある設定タスクの概要を示します。

この章は、次の内容で構成されています。

- [Microsoft Office Live Communications Server 2005 \(SP 1\) の設定 \(P.4-2\)](#)
- [Microsoft Active Directory の設定の概要 \(P.4-3\)](#)
- [Exchange 予定表との統合の設定 \(P.4-5\)](#)
- [TLS ルートの設定チェックリスト \(P.4-16\)](#)
- [FIPS 準拠のセキュリティ アルゴリズムの設定チェックリスト \(P.4-17\)](#)
- [Microsoft Office Communicator 2005 の設定チェックリスト \(P.4-18\)](#)

## Microsoft Office Live Communications Server 2005 (SP 1) の設定

この項では、Cisco Unified Presence と統合する Microsoft Live Communications Server 2005 Service Pack 1 の設定に必要なタスクを示します。

Microsoft Office Live Communications Server (LCS) 2005 アプリケーション ウィンドウから、次の手順を実行します。

詳細については、各設定タスクに対応した Microsoft マニュアルを参照してください。



(注)

すべての Microsoft ソフトウェア パッチが、LCS、および Microsoft Office Communicator クライアントを実行しているすべての PC に適用されていることを確認してください。

### Microsoft LCS の設定の概要



(注)

Live Communications Server 2005 の詳細については、次の URL で参照できます。

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

#### 手順

- ステップ 1** Microsoft Office LCS が適切にインストールされアクティブであることを確認します。
- ステップ 2** [認証プロトコル] で NTLM を選択するか、サイトに適切な認証プロトコルを選択します。
- ステップ 3** この LCS に関連付けられている Cisco Unified Presence ごとに、スタティック ルートを設定します。  
ドメインは、完全修飾ドメイン名を入力します。



(注)

ここで入力するスタティック ルート ドメイン URI は、Active Directory でリモート コール制御を設定したときに入力した SIP URI と一致する必要があります。詳細については、P.4-3 の「Microsoft Active Directory の設定の概要」を参照してください。

スタティック ルートの設定方法の詳細については、「Live Communications Server 2005 オンライン ヘルプ」を参照してください。

- ステップ 4** この LCS に関連付けられている Cisco Unified Presence ごとに、認証済みのホスト レコードを追加します。



ヒント

認証済みホストには、IP アドレスまたは完全修飾ネットワーク アドレスのいずれかを入力できます。

## Microsoft Active Directory の設定の概要

この項では、Cisco Unified Presence と統合する Microsoft Windows Server Active Directory の設定に必要なタスクを示します。

Microsoft Active Directory アプリケーション ウィンドウから、次の手順を実行します。



(注)

Active Directory の設定方法の詳細については、「Active Directory オンライン ヘルプ」を参照してください。Microsoft Windows Server Active Directory の詳細については、次の URL も参照できます。  
<http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.mspx>

### 手順

**ステップ 1** 特定のユーザに関連付けられているユーザ名と電話番号を追加します。

Active Directory で設定されているユーザ名が、Cisco Unified Communications Manager で設定されているユーザ名と同じであることを確認してください。



注意

統合システムが適切に動作するように、Active Directory と Cisco Unified Communications Manager でユーザ名が同じであることを確認してください。

**ステップ 2** 追加したユーザについて、[プロパティ] ウィンドウでライブ コミュニケーションを有効にします。

**ステップ 3** SIP URI、および LCS 名または LCS プールを入力します。



注意

LCS 名または LCS プール名にアンダースコア文字が含まれていないことを確認してください。

**ステップ 4** リモート ユーザ アクセスおよびリモート コール制御を有効にします。

**ステップ 5** TEL URI を入力します。

TEL URI には次の形式を使用するようにお勧めします。

```
tel:xxxx;phone-context=dialstring
```

各部の説明は以下のとおりです。

- `xxxx` には、コールの発信時に CTI Manager が発呼番号または着信番号として Cisco Unified Presence に報告する電話番号を指定します。
- `phone-context=dialstring` と入力すると、MOC クライアントは電話番号に関連付けられているデバイスの 1 つを制御できます。

デバイス ID を入力した場合、MOC クライアントはその特定のデバイスだけを制御します。次に例を示します。

```
tel:xxxx;phone-context=dialstring;device=SEP0002FD3BB5C5
```

パーティションを入力した場合、MOC クライアントは電話番号のパーティションを指定します。次に例を示します。

```
tel:XXXX;phone-context=dialstring;device=SEP0002FD3BB5C5;partition=myPartition
```

TEL URI にデバイス ID を入力しないと、CTI ゲートウェイは回線電話番号に関連付けられているデバイスを判別します。回線 DN に 1 つのデバイスだけが関連付けられている場合、CTI ゲートウェイはそのデバイスを使用します。

TEL URI にデバイス ID を入力せず、回線 DN に 2 つのデバイスが関連付けられている場合（共有回線）、CTI ゲートウェイは次のルールを使用してデバイスを選択します。

- 片方のデバイスが Cisco IP Communicator でステータスが登録済みの場合、CTI ゲートウェイはそのデバイスを使用します。
- 片方のデバイスが Cisco IP Communicator でステータスが未登録の場合、CTI ゲートウェイは代替ハードデバイスを使用します。
- 2 つのハードデバイスが共有回線に存在する場合、CTI ゲートウェイは、共有回線でコールを発信するときに 2 つのデバイスを監視します。ユーザが応答すると、CTI ゲートウェイはそのデバイスを監視します。

3 つ以上のデバイスが回線 DN に関連付けられている場合、希望するデバイスを TEL URI に指定する必要があります。

#### ステップ 6 リモート コール制御 SIP URI を次のように入力します。

```
sip:8000@my-cups.my-domain.com
```

ここで、my-cups.my-domain.com には、設定済みの Cisco Unified Presence の完全修飾ドメイン名を指定します。



**(注)** ここで入力する SIP URI は、Microsoft Office Live Communications Server 2005 でスタティック ルートの設定で入力したスタティック ルート URI と一致する必要があります。詳細については、[P.4-2 の「Microsoft Office Live Communications Server 2005 \(SP 1\) の設定」](#)を参照してください。

## Exchange 予定表との統合の設定

Exchange 予定表との統合を設定するには、次のタスクを実行する必要があります。

- Exchange Server で Receive As アカウントを作成する。
- Cisco Unified Presence サーバでプレゼンス ゲートウェイを設定する。
- Cisco Unified Presence サーバでセキュリティ証明書を設定する。



**(注)** Exchange Server に設定されている管理者アカウントをすでに持っている場合もありますが、デフォルトの管理者設定では、他のユーザ アカウントにログインできないことがあります。Exchange 予定表との統合用に別の管理者アカウントを作成するようにお勧めします。

この項は、次の内容で構成されています。

- [Exchange Server での Receive As アカウントの作成 \(P.4-5\)](#)
- [ユーザ アカウントの作成 \(P.4-6\)](#)
- [アカウントへの Exchange 参照のみ可としての制御の委任 \(P.4-6\)](#)
- [アカウントへの Receive As 権限の追加 \(P.4-7\)](#)
- [Cisco Unified Presence サーバでのプレゼンス ゲートウェイの設定 \(P.4-8\)](#)
- [Cisco Unified Presence サーバでのセキュリティ証明書の設定 \(P.4-9\)](#)

### Exchange Server での Receive As アカウントの作成

この項では、サーバで Receive As アカウントを作成するために実行する必要があるタスクを示します。

#### 新しいアカウントの作成



**(注)** これらの手順を Microsoft Exchange Server で実行します。

#### 手順

**ステップ 1** Exchange Server で新しいアカウントを作成します。

**ステップ 2** [Delegate Control] で [Exchange View-Only] を設定します。



**(注)** 管理グループの表示が有効でない場合は、[Exchange] を右クリックし、[Display Administrative Groups] チェックボックスをオンにします。

**ステップ 3** アカウントに [Receive Permissions] を追加します。



(注) Microsoft Exchange Server の詳細については、次の URL で参照できます。  
<http://www.microsoft.com/exchange/default.mspx>

## ユーザ アカウントの作成

次の手順を使用して、ユーザ アカウントを作成します。

### 手順

- ステップ 1** Exchange Server で **[Active Directory Users and Computers]** (ADUC) を起動します。
- ステップ 2** **[Users]** コンテナを右クリックし、**[New | User]** を選択します。  
  
[New Object User] ダイアログボックスが表示されます。
- ステップ 3** ユーザ アカウントの名前情報を入力します。
- ステップ 4** **[Next]** をクリックします。  
  
ユーザ アカウントのデフォルトのメールボックス設定が表示されます。
- ステップ 5** **[Next]** をクリックします。  
  
概要のウィンドウが表示されます。
- ステップ 6** ユーザ アカウントの作成を完了するには、**[Finish]** をクリックします。

## アカウントへの Exchange 参照のみ可としての制御の委任

Receive As アカウントを作成するには、アカウントをメールボックス管理に追加する必要があります。

### 手順

- ステップ 1** Exchange Server で、**[Exchange System Manager]** を開きます。
- ステップ 2** [管理グループ] フォルダに進みます。
- ステップ 3** 作成したアカウントを追加する管理グループを選択します。
- ステップ 4** グループを右クリックし、ポップアップメニューから **[Delegate Control]** を選択します。  
  
[Exchange Administration Delegation Wizard] ウィンドウが表示されます。

- ステップ 5** [Next] をクリックします。
- ステップ 6** [Add] をクリックします。
- [Delegate Control] ウィンドウが表示されます。
- ステップ 7** [Browse] をクリックし、作成したユーザ アカウントを選択します。
- ステップ 8** [role] : [Exchange View-Only Administrator] を選択します。
- ステップ 9** [OK] をクリックします。
- ステップ 10** 概要のウィンドウで [Finish] をクリックし、変更内容を保存します。
- 

## アカウントへの Receive As 権限の追加

### 手順

---

- ステップ 1** Exchange Server で、[Exchange System Manager] を開きます。
- ステップ 2** [Administrative Groups] > [First Administrative Group] > [Servers] > [First Server] > [Mailbox Store] に進みます。
- ステップ 3** メールボックス ストアを右クリックし、[Properties] を選択します。
- [Properties] ウィンドウが表示されます。
- ステップ 4** [Security] タブを選択し、[Add] をクリックします。
- ステップ 5** [Enter the object name to select] フィールドに、使用するアカウントの名前を入力します。
- ステップ 6** [Receive As] を選択し、予定表情報にアクセスする必要があるすべてのメールボックス ストアで、この管理者アカウントに Receive As 権限を付与します。
- ステップ 7** [OK] をクリックします。

ここで設定したアカウントが、メールボックス ストアにログインするための完全な権限を持つこととなります。

- ステップ 8** Receive As アカウントを正しく設定したことを確認するには、次の URL でユーザの Outlook for Web Access (OWA) にログインしてみます。

`http://exchange.domain/Exchange/user/Calendar`

各部の説明は以下のとおりです。

- `exchange.domain` は、Exchange Server の名前とドメインです。
- `user` は、予定表サービスへのバックエンドサブスクリプションを作成しようとしている任意のユーザです。

- ステップ9** ログインできない場合は、アカウントが正しく設定されていないため、この項の手順を使用してアカウントを再度作成する必要があります。

## Cisco Unified Presence サーバでのプレゼンス ゲートウェイの設定



**(注)** Cisco Unified Presence の管理ページから次の手順を実行します。詳細については、『Cisco Unified Presence アドミニストレーションガイド』を参照してください。

### 手順

- ステップ1** [Cisco Unified Presence] > [プレゼンスエンジン] > [プレゼンスゲートウェイ] を選択します。
- [プレゼンスゲートウェイの検索と一覧表示 (Find and List Presence Gateways)] ウィンドウが表示されます。
- ステップ2** [新規追加] をクリックします。
- [プレゼンスゲートウェイの設定 (Presence Gateway Configuration)] ウィンドウが表示されます。
- ステップ3** [プレゼンスゲートウェイタイプ (Presence Gateway Type)] で、[Outlook] を選択します。
- ステップ4** 表 4-1 の説明に従って、残りのパラメータに適切な値を入力します。

表 4-1 プレゼンス ゲートウェイの設定値

フィールド	説明
プレゼンスゲートウェイタイプ (Presence Gateway Type)	ド롭ダウンリストから、ゲートウェイ タイプを指定します。 <ul style="list-style-type: none"> <li>[CUCM] : Cisco Unified Communications Manager ゲートウェイ</li> <li>[Outlook]: Outlook 予定表用の Microsoft Exchange ゲートウェイ</li> </ul>  <p><b>(注)</b> Cisco Unified Presence の管理機能によって、選択したゲートウェイ タイプに適切なフィールドが表示されます。</p>
説明 (Description)	このパラメータでは、このプレゼンス ゲートウェイの説明を指定します。 最大文字数 : 255
プレゼンスゲートウェイ (Presence Gateway)	このパラメータでは、関連するゲートウェイの完全修飾ドメイン名または IP アドレスを指定します。  <p><b>(注)</b> このパラメータは、Exchange Server 上の IIS 証明書のサブジェクト CN と同じである必要があります。</p>

表 4-1 プレゼンス ゲートウェイの設定値 (続き)

フィールド	説明
アカウント名 (Account Name) (Outlook のみ)	このパラメータでは、Cisco Unified Presence が Microsoft Exchange Server への接続に使用するグローバルアカウント名を指定します。  <b>(注)</b> Exchange Server で作成した Receive As アカウントのアカウント名を入力します。
アカウントパスワード (Account Password、半角英数字のみ) (Outlook のみ)	このパラメータでは、Microsoft Exchange Server 用のアカウントパスワードを指定します。
パスワードの確認 (Confirm Password、半角英数字のみ) (Outlook のみ)	このパラメータでは、Microsoft Exchange Server 用のアカウントパスワードを確認します。アカウントパスワードのエントリと一致する必要があります。
プレゼンスゲートウェイポート (Presence Gateway Port) (Outlook のみ)	このパラメータでは、Microsoft Exchange Server 上の接続先のポートを指定します。 デフォルト値：443
信頼証明書件名 CN (Trust Certificate Subject CN) (Outlook のみ)	このパラメータでは、信頼証明書の Common Name の値を指定します。

## Cisco Unified Presence サーバでのセキュリティ証明書の設定

Cisco Unified Presence でセキュリティ証明書を設定するには、次のタスクを実行する必要があります。

- Certificate Authority (CA; 認証局) サービスをインストールする。



**(注)** Exchange Server を実行しているマシンに CA サービスをインストールしないでください。

- ルート証明書をダウンロードする。
- ルート証明書を Cisco Unified Presence サーバにアップロードする。
- Internet Information Server (IIS) で Certificate Signing Request (CSR; 証明書署名要求) を生成する。
- システム上の CA が CSR に署名するようにする。
- 署名済みの証明書をダウンロードする。
- IIS で、署名済みの証明書をアップロードする。

## CA サービスのインストール



(注) 必ず Exchange Server とは別のサーバに CA サービスをインストールしてください。

### 手順

- ステップ 1** [スタート] > [コントロールパネル] > [プログラムの追加と削除] を選択します。
- ステップ 2** [プログラムの追加と削除] ウィンドウで、[Windows コンポーネントの追加と削除] をクリックします。
- ステップ 3** [Windows コンポーネント] の下で、[証明書サービス] を選択します。
- ステップ 4** 表示される警告で、[はい] をクリックします。
- ステップ 5** [CA の種類] ウィンドウで、[スタンドアロンのルート CA] を選択し、[次へ] をクリックします。  
[CA 識別情報] ウィンドウが表示されます。
- ステップ 6** [この CA の共通名] フィールドにサーバの名前を入力し、[次へ] をクリックします。  
[証明書データベースの設定] ウィンドウが表示されます。
- ステップ 7** [証明書データベースの設定] ウィンドウでデフォルトを受け入れ、[次へ] をクリックします。
- ステップ 8** インターネット インフォメーション サービスの停止を求めるメッセージが表示されたら、[はい] をクリックします。
- ステップ 9** Active Server Pages (ASP) を有効にするよう求めるメッセージが表示されたら、[はい] をクリックします。
- ステップ 10** インストールプロセスが完了したら、[完了] をクリックします。

## ルート証明書のダウンロード

### 手順

- ステップ 1** CA サーバにログインし、Web ブラウザを開きます。
- ステップ 2** 次の URL を開きます。  
`http://127.0.0.1/crtsrv`
- 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] をクリックします。

- ステップ 4** [エンコード方式] 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] をクリックします。
- ステップ 6** 証明書、**certnew.cer** をローカル ディスクに保存します。
- 

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

### 手順

---

- ステップ 1** Cisco Unified Presence サーバ の管理に使用するコンピュータに、certnew.cer 証明書ファイルをコピーするか、FTP で送信します。
- ステップ 2** [Cisco Unified Presence の管理] のログイン ウィンドウにある [ナビゲーション] メニューから、[Cisco Unified OS の管理] を選択し、[移動] をクリックします。
- ステップ 3** Cisco Unified オペレーティング システムの管理ページ用のユーザ名とパスワードを入力し、[ログイン] をクリックします。
- [Cisco Unified オペレーティングシステムの管理] ウィンドウが表示されます。
- ステップ 4** [セキュリティ] > [証明書の管理] を選択します。
- [証明書の一覧 (Certificate List)] ウィンドウが表示されます。
- ステップ 5** [証明書のアップロード] をクリックします。
- [証明書のアップロード (Upload Certificate)] ポップアップ ウィンドウが表示されます。
- ステップ 6** [証明書の名前 (Certificate Name)] ドロップダウン メニューから、[Presence Engine] を選択します。
- ステップ 7** [ルート証明書 (Root Certificate)] : 何も入力しません。
- ステップ 8** [参照] をクリックし、[certnew.cer] を選択します。
- ステップ 9** [ファイルのアップロード] をクリックします。
-

## IIS での CSR の生成



(注) CSR を生成するには、Cisco Unified Presence の管理に使用するコンピュータで次の手順を実行します。

## 手順

- 
- ステップ 1** [管理ツール] から、[インターネットインフォメーションサービス] を開きます。
- [インターネットインフォメーションサービス] ウィンドウが表示されます。
- ステップ 2** [既定の Web サイト] を右クリックし、[プロパティ] を選択します。
- 既定の Web サイトのプロパティ ダイアログボックスが表示されます。
- ステップ 3** [ディレクトリセキュリティ] タブを選択し、[サーバー証明書] をクリックします。
- [Web サーバー証明書ウィザード] ウィンドウが表示されます。
- ステップ 4** [次へ] をクリックします。
- ステップ 5** [新しい証明書の作成] を選択し、[次へ] をクリックします。
- ステップ 6** [証明書の要求を作成して後で送信する] を選択し、[次へ] をクリックします。
- ステップ 7** 証明書の適切な名前を入力し、ビット長として [1024] を選択します。
- ステップ 8** [次へ] をクリックします。
- ステップ 9** 組織と組織ユニットを入力し、[次へ] をクリックします。
- ステップ 10** [一般名] : Exchange Server の名前を入力し、[次へ] をクリックします。
- ステップ 11** 地理情報を入力し、[次へ] をクリックします。
- ステップ 12** 証明書要求の適切なファイル名を入力し、[次へ] をクリックします。
- ステップ 13** [要求ファイルの概要] ウィンドウで情報を確認し、[次へ] をクリックします。
- ステップ 14** [完了] をクリックします。
-

## CSR への署名



(注) CA サーバが証明書要求ファイルに署名するようにするには、CA サーバで次の手順を実行します。

## 手順

- 
- ステップ 1** 証明書要求ファイルを CA サーバにコピーします。
- ステップ 2** 次の URL を開きます。
- `http://local-server/certserv`
- または
- `http://127.0.0.1/certsrv`
- ステップ 3** [証明書を要求する] リンクをクリックします。
- ステップ 4** [証明書の要求の詳細設定] を選択します。
- ステップ 5** [Base 64 エンコード PKCS #10 ファイルを使用して証明書の要求を送信するか、または Base 64 エンコード PKCS #7 ファイルを使用して更新の要求を送信する] 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 CSR 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** CSR の内容を [証明書の要求] テキストボックスに貼り付けます。
- ステップ 9** [送信] をクリックします。
- 要求 ID が表示されます。
- ステップ 10** [管理ツール] で、[証明機関] を開きます。
- [証明機関] ウィンドウの [保留中の要求] の下に、直前に送信した要求が表示されます。
- ステップ 11** 要求を右クリックし、[すべてのタスク] を選択します。
- ステップ 12** [発行] をクリックします。
- ステップ 13** [発行した証明書] をクリックし、証明書が発行されたことを確認します。
-

## 署名済み証明書のダウンロード

### 手順

- 
- ステップ 1** [管理ツール] で、[証明機関] を開きます。
- 直前に発行した保留中の証明書要求が [発行した証明書] に表示されます。
- ステップ 2** 要求を右クリックし、[オープン] を選択します。
- ステップ 3** [詳細] タブをクリックします。
- ステップ 4** [ファイルへコピー] をクリックします。
- [証明書のエクスポート ウィザード] が表示されます。
- ステップ 5** [次へ] をクリックします。
- ステップ 6** [Base-64 encoded X.509] を選択し、[次へ] をクリックします。
- ステップ 7** 証明書を格納する場所を入力し、証明書名として **cert.cer** を使用します。
- ステップ 8** [次へ] をクリックします。
- ステップ 9** 概要情報を確認し、[完了] をクリックします。
- ステップ 10** Cisco Unified Presence の管理に使用するコンピュータに cert.cer をコピーします。
- 

## IIS での署名済み証明書のアップロード



- (注) 署名済み証明書をアップロードするには、Cisco Unified Presence の管理に使用するコンピュータで次の手順を実行します。
- 

### 手順

- 
- ステップ 1** [管理ツール] で、[インターネット インフォメーションサービス] を開きます。
- [インターネット インフォメーション サービス] ウィンドウが表示されます。
- ステップ 2** [既定の Web サイト] を右クリックし、[プロパティ] を選択します。
- 既定の Web サイトのプロパティ ダイアログボックスが表示されます。
- ステップ 3** [ディレクトリ セキュリティ] タブをクリックし、[サーバー証明書] をクリックします。
- [Web サーバー証明書ウィザード] が表示されます。

**ステップ 4** [次へ] をクリックします。

**ステップ 5** [保留中の要求を処理し、証明書をインストールする] をクリックし、[次へ] をクリックします。

**ステップ 6** 証明書を選択するには、[参照] をクリックします。

**ステップ 7** [次へ] をクリックします。

**ステップ 8** [SSL ポート]: **443** と入力し、[次へ] をクリックします。

**ステップ 9** ウィザードを閉じるには、[完了] をクリックします。

---

## TLS ルートの設定チェックリスト

表 4-2 は、TLS ルート設定 (TLC) で実行するタスクを示しています。これらのタスクを Microsoft LCS で実行します。

表 4-2 TLC ルートの設定チェックリスト

	設定手順	関連マニュアル
ステップ 1	<p>スタティック ルートを追加します。</p> <ol style="list-style-type: none"> <li>[Live Communications サーバとプール] 下に表示されているサーバを右クリックし、[プロパティ] を選択します。</li> <li>[ルーティング] タブを選択し、[追加] をクリックします。</li> <li>[次ホップ] で、[ネットワーク アドレス] を選択し、Cisco Unified Presence のホスト名または FQDN を入力します。</li> </ol> <p> (注) 入力した値が、Cisco Unified Presence 証明書のサブジェクト CN と一致することを確認してください。Cisco Unified Presence 証明書のサブジェクト CN を確認するには、Cisco Unified Communications オペレーティング システムの管理ページにログインし、[セキュリティ] &gt; [証明書の管理] &gt; [証明書の表示] に進み、自分の証明書および [sipprox] を選択します。</p> <ol style="list-style-type: none"> <li>[トランスポート] で、[TLS] を選択します。</li> <li>ポート [5062] を選択します。</li> </ol> <p> (注) ポート 5062 は、デフォルトのポートを表しています。Cisco Unified Presence はこのポートでピア認証 TLS 接続をリッスンします。</p> <ol style="list-style-type: none"> <li>[要求 URI 内のホストを置き換える] を選択します。</li> <li>設定済みの LCS 証明書を選択します。入力済みの分かりやすい名前を参照して、証明書を選択できます。詳細については、P.4-9 の「Cisco Unified Presence サーバでのセキュリティ証明書の設定」を参照してください。</li> </ol>	<p>詳細については、次の URL から「Windows Server TechCenter オンライン」を参照してください。</p> <p><a href="http://technet2.microsoft.com/WindowsServer/en/library/49960f07-4a4c-4e04-9aef-82ab0e8efc0d1033.mspx?mfr=true">http://technet2.microsoft.com/WindowsServer/en/library/49960f07-4a4c-4e04-9aef-82ab0e8efc0d1033.mspx?mfr=true</a></p>
ステップ 2	<p>Cisco Unified Presence を、認証済みホストとして印を付けます。</p> <ol style="list-style-type: none"> <li>[ホストの承認] タブをクリックします。</li> <li>Cisco Unified Presence サーバをダブルクリックします。</li> <li>[サーバとして帯域を制限する] および [認証済みとして扱う] のチェックボックスをオンにします。</li> <li>[OK] をクリックします。</li> <li>LCS サーバを再起動し、使用可になるまで待機します。</li> </ol> <p>LCS サーバプールには、設定済みの発信スタティック ルートが表示されます。</p>	<p>詳細については、次の URL から「Windows Server TechCenter オンライン」を参照してください。</p> <p><a href="http://technet2.microsoft.com/WindowsServer/en/library/49960f07-4a4c-4e04-9aef-82ab0e8efc0d1033.mspx?mfr=true">http://technet2.microsoft.com/WindowsServer/en/library/49960f07-4a4c-4e04-9aef-82ab0e8efc0d1033.mspx?mfr=true</a></p>

## FIPS 準拠のセキュリティ アルゴリズムの設定チェックリスト

Federal Information Processing Standard (FIPS; 連邦情報処理標準) アルゴリズムを有効にするには、表 4-3 に示されている設定タスクに従ってください。これらのタスクを Microsoft LCS サーバおよび Cisco Unified Presence サーバで実行します。

表 4-3 FIPS 準拠のセキュリティ アルゴリズムの設定チェックリスト

	設定手順	関連マニュアル
ステップ 1	<p>TLS 暗号 TLS_RSA_WITH_3DES_EDE_CBC_SHA が設定された TLSv1 を送信するように、LCS サーバを設定します。</p> <ol style="list-style-type: none"> <li>[スタート] &gt; [管理ツール] &gt; [ドメイン コントローラ セキュリティ ポリシー] を選択します。</li> <li>コンソール ツリーで、[セキュリティ設定] をクリックします。</li> <li>[ローカル ポリシー] をクリックし、[セキュリティ設定] を選択します。</li> <li>[詳細] ペインで、[FIPS] セキュリティ設定を選択します。</li> <li>セキュリティ設定を変更し、[OK] をクリックします。</li> </ol>	<p>FIPS 準拠のアルゴリズムの設定の詳細については、次の URL から「FIPS-compliant algorithm information for Microsoft Windows Server」を参照してください。</p> <p><a href="http://technet2.microsoft.com/WindowsServer/en/Library/6ff574cb-30c4-4ad9-8d5e-ae697c65b9b1033.mspx">http://technet2.microsoft.com/WindowsServer/en/Library/6ff574cb-30c4-4ad9-8d5e-ae697c65b9b1033.mspx</a></p>
ステップ 2	<p>Cisco Unified Presence で TLS コンテキストを設定します。</p> <ol style="list-style-type: none"> <li>Cisco Unified Presence の管理ページにログインします。</li> <li>[Cisco Unified Presence] &gt; [セキュリティ] &gt; [TLS コンテキスト設定] に進みます。</li> </ol> <p>[TLS コンテキストの検索と一覧表示 (Find and List TLS Contexts)] ウィンドウが表示されます。</p> <ol style="list-style-type: none"> <li>[検索] をクリックします。</li> <li>[Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context] をクリックします。</li> </ol> <p>[TLS コンテキスト設定 (TLS Context Configuration)] ウィンドウが表示されます。</p> <ol style="list-style-type: none"> <li>使用可能な TLS 暗号のリストから、[TLS_RSA_WITH_3DES_EDE_CBC_SHA] をクリックします。</li> <li>下矢印をクリックして、[選択された TLS 暗号 (Selected TLS Ciphers)] まで移動します。</li> <li>使用可能な TLS ピア サブジェクトのリストから、設定済みの TLS ピア サブジェクトをクリックします。</li> <li>下矢印をクリックして、[選択された TLS ピアサブジェクト (Selected TLS Peer Subjects)] まで移動します。</li> <li>[保存] をクリックします。</li> <li>Cisco Unified Presence Serviceability Administration ページにログインします。</li> <li>[Tools] &gt; [Service Activation] に進みます。</li> <li>Cisco UPS SIP Proxy サービスをリスタートします。</li> </ol>	<p>詳細については、『Cisco Unified Presence アドミニストレーションガイド』を参照してください。</p>

## Microsoft Office Communicator 2005 の設定チェックリスト

表 4-4 は、Cisco Unified Presence と統合する Microsoft Office Communicator 2005 の設定に必要なタスクを示しています。

Microsoft Office Communicator 2005 アプリケーション ウィンドウから、次の手順を実行します。

詳細については、各設定タスクに対応した Microsoft マニュアルを参照してください。



(注)

すべての Microsoft ソフトウェア パッチが、LCS、および Microsoft Office Communicator クライアントを実行しているすべての PC に適用されていることを確認してください。

表 4-4 Microsoft Office Communicator 2005 の設定チェックリスト

設定手順	関連マニュアル
<p>Microsoft Active Directory で前回設定したログイン名を入力します。詳細については、P.4-3 の「Microsoft Active Directory の設定の概要」を参照してください。</p> <p>Active Directory で設定されているユーザ名が、Cisco Unified Communications Manager で設定されているユーザ名と同じであることを確認してください。</p> <p> <b>注意</b> 統合システムが適切に動作するように、Active Directory と Cisco Unified Communications Manager でユーザ名が同じであることを確認してください。</p>	<p>Microsoft Office Communicator 2005 の設定方法の詳細については、「Microsoft Office Communicator オンラインヘルプ」を参照してください。</p> <p>Microsoft Office Communicator 2005 の詳細については、次の URL も参照できます。</p> <p><a href="http://www.office.microsoft.com/en-us/assistance/HA011992481033.aspx#DeploymentGuide">http://www.office.microsoft.com/en-us/assistance/HA011992481033.aspx#DeploymentGuide</a></p>
<p>Microsoft Live Communications Server の IP アドレスまたは FQDN を入力し、TCP を使用した接続方法を選択します。</p>	<p>Microsoft Office Communicator 2005 の設定方法の詳細については、「Microsoft Office Communicator オンラインヘルプ」を参照してください。</p> <p>Microsoft Office Communicator 2005 の詳細については、次の URL も参照できます。</p> <p><a href="http://www.office.microsoft.com/en-us/assistance/HA011992481033.aspx#DeploymentGuide">http://www.office.microsoft.com/en-us/assistance/HA011992481033.aspx#DeploymentGuide</a></p>
<p>[電話統合を有効にする] を選択します。</p>	<p>Microsoft Office Communicator 2005 の設定方法の詳細については、「Microsoft Office Communicator オンラインヘルプ」を参照してください。</p> <p>Microsoft Office Communicator 2005 の詳細については、次の URL も参照できます。</p> <p><a href="http://www.office.microsoft.com/en-us/assistance/HA011992481033.aspx#DeploymentGuide">http://www.office.microsoft.com/en-us/assistance/HA011992481033.aspx#DeploymentGuide</a></p>

表 4-4 Microsoft Office Communicator 2005 の設定チェックリスト (続き)

設定手順	関連マニュアル
<p>通常のユーザであれば、[自動構成] を選択できます。</p>	<p>Microsoft Office Communicator 2005 の設定方法の詳細については、「Microsoft Office Communicator オンラインヘルプ」を参照してください。</p> <p>Microsoft Office Communicator 2005 の詳細については、次の URL も参照できます。</p> <p><a href="http://www.office.microsoft.com/en-us/assistance/HA011992481033.aspx#DeploymentGuide">http://www.office.microsoft.com/en-us/assistance/HA011992481033.aspx#DeploymentGuide</a></p>
<p>ユーザは、ログインした後、発呼側の電話番号のデフォルトデバイスに [電話] または [コンピュータ] のいずれかを選択できます。</p> <p> (注) ユーザがデフォルトデバイスに [コンピュータ] を指定した場合、Cisco Unified Presence は LCS とは統合されません。</p>	<p>Microsoft Office Communicator 2005 の設定方法の詳細については、「Microsoft Office Communicator オンラインヘルプ」を参照してください。</p> <p>Microsoft Office Communicator 2005 の詳細については、次の URL も参照できます。</p> <p><a href="http://www.office.microsoft.com/en-us/assistance/HA011992481033.aspx#DeploymentGuide">http://www.office.microsoft.com/en-us/assistance/HA011992481033.aspx#DeploymentGuide</a></p>
<p>MOC 設定で、個人用情報マネージャに Microsoft Office Outlook (該当する場合) を選択します。</p>	<p>Microsoft Office Communicator 2005 の設定方法の詳細については、「Microsoft Office Communicator オンラインヘルプ」を参照してください。</p> <p>Microsoft Office Communicator 2005 の詳細については、次の URL も参照できます。</p> <p><a href="http://www.office.microsoft.com/en-us/assistance/HA011992481033.aspx#DeploymentGuide">http://www.office.microsoft.com/en-us/assistance/HA011992481033.aspx#DeploymentGuide</a></p>

