Microsoft Lync サーバを使用した、IM and Presence Service on Cisco Unified Communications Manager リリース 11.0(1) のリモート通話コントロール

初版：2015 年 06 月 08 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

はじめに

この章では、リモート通話コントロールのために IM and Presence サービスと Microsoft Lync サーバを統合する手順を説明します。

Microsoft Lync サーバについて

Microsoft Lync サーバは、中小規模の組織配置での使用向けに設計されています。サーバは、単一システム内で SIP レジストラ、および SIP プロキシとして動作します。サーバ機能は、IM and Presence サービスや Cisco Unified Communications Manager プラットフォームなどのゲートウェイへのリモート通話コントロールの音声機能を提供します。

Microsoft Lync Server 2010 Standard Edition は、ユーザや設定システム データのデータ ストレージとしてMicrosoft SQL Server 2008 Express データベースを同じサーバにインストールします。Microsoft Lync Server 2010 Enterprise Edition は、Microsoft SQL Server 2008 Express データベースを別のサーバにインストールします。Lync Server 管理シェルから入力されたコマンドは、SQL データベースに読み込まれます。

（注） IM and Presence サービスは、Microsoft Lync サーバ スタンダード エディションまたは Enterprise Edition の 2010 および 2013 との統合をサポートします。

詳細情報

IM and Presence サービス

その他の IM and Presence サービスのドキュメントについては、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

Cisco Unified Communications Manager

Cisco Unified Communications Manager のドキュメントについては、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 Lync

Microsoft Lync のドキュメントについては、次の URL を参照してください。

- http://technet.microsoft.com/en-us/library/gg558664.aspx
- http://office.microsoft.com/en-us/lync/

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

リモート通話コントロールについて

リモート通話コントロール（RCC）を使用すると、企業ユーザが Microsoft Lync（サードパーティ製デスクトップ インスタント メッセージング（IM）アプリケーション）経由で Cisco Unified IP Phone または Cisco IP Communicator を制御できるようになります。ユーザが Microsoft Lync クライアントにサインインすると、Lync サーバは IM and Presence サービス ノードを通じて Cisco Unified Communications Manager へ、Lync クライアントでのユーザのアクションに応じた通話機能のセットアップ、終了、保持を指示します。

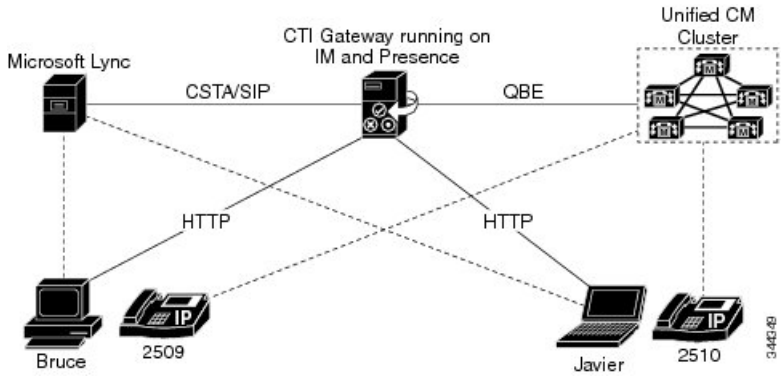
統合の概要

IM and Presence サービスを使用すると、企業ユーザが Microsoft Lync（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 または Cisco IP Communicator Phone を制御できるようになります。

次の図に示すように、Microsoft Lync はセッション開始要求を IM and Presence サービスのコンピュータ テレフォニー インターフェイス（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 または Cisco IP Communicator Phones を制御します。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 Lync アプリケーションに返します。

図 *1*：統合の概要



Microsoft Lync が IM and Presence サービスに要求を送信

Microsoft Lync がセッション開始要求を IM and Presence サービスに送信します。このような要求は、IM and Presence サービスに設定された CTI 接続アドレスにルーティングされます。

（注） IM and Presence サービスは、最大 8 つの Cisco Unified Communications Manager ノードで CTI 接続をサポートします。

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。デュアル ノード IM and Presence サービス クラスタでは、ロード バランサを使用して、Microsoft Lync 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ライバ IM and Presence サービス ノードにラウンドロビンできます。

CTI Gateway による Microsoft Lync ユーザのサインインの CTI 接続アドレスの監視

IM and Presence サービス上の 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 Lync ユーザがサインインすると、Microsoft Lync サーバは、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 または Cisco IP Communicator Phone を監視します。CTI ゲートウェイは、その Microsoft Lync 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 セッションの確立

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

Lync 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。

いずれかの CTI マネージャへの接続が失敗した場合は、接続が使用可能になるまで、Microsoft Lync 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、接続を監視します。この場合、Microsoft Lync 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 Lync は、新規 SIP INVITE メッセージを送信しますが、Microsoft Lync ユーザは再度サインインする必要はありません。

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、IM and Presence サービスでは、Microsoft Lync クライアント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。

Microsoft Office Communicator の通話コントロール機能のために IM and Presence サービスと Microsoft OCS を統合する設定手順の詳細については、『*Microsoft Office Communicator Call Control with Microsoft OCS for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

第 2 章

統合要件

（注） IP Phone のコール転送設定：ソフトキー ボタンまたは Cisco UCM の電話の設定ページを使用した Cisco IP Phone でのコール転送設定は、Microsoft Lync Client には反映されません。ただし、Micorsoft Lync でのコール転送設定は、Cisco IP Phone に反映されます。

Microsoft Lync クライアントは、IP Phone で設定されたコール転送設定を上書きできます。IP Phone は、Microsoft Lync クライアントで設定されたコール転送設定を上書きできます。

ソフトウェア要件

IM and Presence サービスと Microsoft Lync サーバの統合には、次のソフトウェアが必要です。

- IM and Presence サービス、現在のリリース
- IM and Presence サービス Lync Remote Call Control プラグイン
- Cisco Unified Communications Manager、現在のリリース
- Microsoft Lync Server 2010 または 2013 リリース 4.x（スタンダード エディションまたは Enterprise Edition）
  - Lync Server コントロール パネル
  - Lync Server 展開ウィザード
  - Lync Server ログ ツール
  - Lync Server 管理シェル

- Lync Server トポロジ ビルダー

- Microsoft 2010 Lync クライアント、または、Microsoft 2013 Lync クライアント
- （オプション）Cisco CSS 11500 コンテント サービス スイッチ
- Microsoft ドメイン コントローラ
- Microsoft Active Directory
- DNS
- Certificate Authority

事前設定チェックリスト

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。

- IM and Presence サービス ノードが、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』での説明に従って設定されている。IM and Presence サービス ノードが、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』の説明に従って Cisco Unified Communications Manager（Unified Communications Manager）サーバとともに正しく導入されている。
- Microsoft 社のドキュメントに定義されている要件に従って、Microsoft Lync サーバ をセットアップし、設定している。
- Microsoft 社のドキュメントに定義されている要件に従って、Microsoft Lync クライアントをセットアップし、設定している。

設定タスクの開始前に、次の事前設定チェックリストを確認することを推奨します。

1. Microsoft Lync サーバで、すべてのサービスが動作していることを確認します。
2. Microsoft Lync サーバのインストール手順に従い、Microsoft Lync サーバをサポートする DNS のすべての SRV レコードを更新したことを確認します。
3. Microsoft Lync クライアントがインストールされているコンピュータが、Microsoft Lync サーバの FQDN を解決できることを確認します。Microsoft Lync クライアント コンピュータから NSLOOKUP コマンドを実行して確認できます。
4. IM and Presence サービス ノード、Cisco Unified Communications Manager ノード、および Microsoft Lync サーバが DNS に追加され、各サーバが自身の FQDN を解決していることを確認します。ドメイン内の別のリソースから NSLOOKUP コマンドを実行して確認できます。
5. AD と Cisco Unified Communications Manager サーバとの間で LDAP 同期を使用している場合、接続が正しく同期されていることを確認します。

統合ライセンス要件

Microsoft Lync Remote Call Control（RCC）の各ユーザに IM and Presence サービス を割り当てる必要があります。IM and Presence サービス機能は、User Connect Licensing（UCL）と Cisco Unified Workspace Licensing（CUWL）の両方に含まれています。詳細は、『*Cisco Unified Communications Manager Enterprise License Manager User Guide*』を参照してください。

IM and Presence サービスを Cisco Unified Communications Manager の [エンド ユーザの設定（End User Configuration）] ウィンドウのユーザに割り当てることができます。詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

次の作業

Cisco Unified Communications Manager サーバ設定, （9 ページ）

第 3 章

Cisco Unified Communications Manager サーバ設定

（注） Cisco Unified Communications Manager のリリースにより、メニュー オプションとパラメータが異なるため、リリースごとの Cisco Unified Communications Manager のドキュメントを参照してください。

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

Microsoft Lync 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 Communications Manager Administration] > [デバイス（Device）] > [電話（Phone）] > [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 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 Communications Manager Administration] > [デバイス（Device）] > [電話（Phone）]

次の作業

標準 CCM アクセス コントロール グループへのユーザの追加, （10 ページ）

関連トピック

ライン アピアランス, （4 ページ）

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

標準 CCM アクセス コントロール グループへのユーザの追加

はじめる前に

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 Communications Manager Administration] > [ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [アクセス コントロール グループ（Access Control 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 CCM エンド ユーザ（Standard CCM End Users）] を選択します。

ステップ 4 [グループにエンド ユーザを追加（Add End Users to Group）] を選択します。

ステップ 5 標準 CCM アクセス コントロール グループに追加するエンド 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。

次の作業

CTI ゲートウェイ アプリケーション ユーザの設定, （11 ページ）

関連トピック

Cisco Unified Communications Manager のユーザおよびデバイスの設定, （9 ページ）

CTI ゲートウェイ アプリケーション ユーザの設定

次の手順を実行し、CTI ゲートウェイのアプリケーション ユーザを設定します。

手順

ステップ 1 [Cisco Unified 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 ユーザ名を入力します。

例：
CtiGW

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 対応アクセス コントロール グループへのアプリケーション ユーザの追加, （11 ページ）

CTI 対応アクセス コントロール グループへのアプリケーション ユーザの追加

次の手順を実行し、CTI 対応アクセス コントロール グループへアプリケーション ユーザを追加します。

はじめる前に

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 Communications Manager Administration] > [ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [アクセス コントロール グループ（Access Control 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 App 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。

次の作業

アプリケーション ユーザへの CTI デバイス コントロールの割り当て, （12 ページ）

関連トピック

CTI ゲートウェイ アプリケーション ユーザの設定, （11 ページ）

アプリケーション ユーザへの CTI デバイス コントロールの割り当て

次の手順を実行し、CTI デバイス コントロールをアプリケーション ユーザに割り当てます。

注意 デバイスをコントロール対象デバイスとしてアプリケーション ユーザに追加しないでください。ロールの [標準 CTI によるすべてのデバイスの制御（Standard CTI Allow Control of All Devices）] により、アプリケーション ユーザは、すべての Cisco Unified Communications Manager デバイスをコントロールするのに十分な権限を付与されます。デバイスをコントロール対象デバイスとしてアプリケーション ユーザに追加すると、Cisco Unified Communications Manager のパフォーマンスに悪影響がおよびます。これは、Cisco Unified Communications Manager が、この方法で多数のデバイスをコントロールするシングルユーザをサポートしていないためです。

はじめる前に

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 Communications Manager Administration] > [ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [アクセス コントロール グループ（Access Control 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。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 4 [グループにアプリケーション ユーザを追加（Add App 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。

関連トピック

CTI ゲートウェイ アプリケーション ユーザの設定, （11 ページ）
CTI 対応アクセス コントロール グループへのアプリケーション ユーザの追加, （11 ページ）

ダイヤル ルールの設定

Lync サーバから送られる「+」接頭辞を取り除くには、ダイヤル ルールの設定が必要です。ダイヤル ルールが設定されていない場合、Cisco Unified Communications Manager から回線 URI が見つけられず、コール発信が失敗します。

（注） ユーザが E.164 形式の番号をプロビジョニングしている場合のみ、次の設定が必要となります。ユーザと IP 電話の両方で E.164 形式の番号がプロビジョニングされている場合、「+」接頭辞を取り除くためにアプリケーションのダイヤル ルールを設定する必要はありません。

手順

ステップ 1 [Cisco Unified Communications Manager Administration] > [コール ルーティング（Call Routing）] > [ダイヤル ルール（Dial Rules）] > [アプリケーション ダイヤル ルール（Application Dial Rules）] > [新規追加（Add New）] を選択します。

ステップ 2 ダイヤル ルールの名前と説明を入力します。

ステップ 3 [開始番号（Number Begins With）] フィールドに、+ と入力します。

ステップ 4 番号形式 xxx-xxx-xxxx をサポートするために、[桁数（Number of Digits）] フィールドに 12 と入力します。

ステップ 5 [削除する合計桁数（Total Digits to be Removed）] フィールドに、1 と入力します。
桁は常に左から右へと削除されるため、「+」接頭辞が取り除かれます。

ステップ 6 [保存（Save）] を選択します。

次の作業

IM and Presence サービス ノードの設定, （15 ページ）

第 4 章

IM and Presence サービス ノードの設定

サービス パラメータの設定

IM and Presence サービスから Microsoft Lync への SIP メッセージ ルーティングは、Microsoft Lync 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。IM and Presence サービスは、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 Lync クライアントにルーティングします。

また、IM and Presence サービスの転送タイプは、Microsoft Lync に設定された IM and Presence サービス ルートの転送タイプと同じである必要があります。

手順

ステップ 1 [Cisco Unified CM IM and 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 IM and Presence サーバを選択します。

ステップ 3 サービス [Cisco SIP プロキシ（Cisco 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。

a) 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 IM and Presence サービス 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。

b) [レコード ルート ヘッダを追加（Add Record-Route Header）] パラメータを有効にします。

c) [レコード ルート ヘッダでトランスポートを使用（Use Transport in Record-Route Header）] パラメータを有効にします。

d) パラメータ値の [SIP ルート ヘッダ トランスポート タイプ（SIP Route Header Transport Type）] を、Microsoft Lync で IM and Presence サービス ルート用に Microsoft Lync 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

発着信のアクセス コントロール リストの設定, （16 ページ）

発着信のアクセス コントロール リストの設定

この手順では、次の 4 つのアクセス コントロール リスト（ACL）のエントリを追加します。

- 着信 ACL の Lync サーバの FQDN
- 着信 ACL の Lync サーバの IP アドレス
- 発信 ACL の Lync サーバの FQDN
- 発信 ACL の Lync サーバの IP アドレス

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] > [システム（System）] > [セキュリティ（Security）] > [着信 ACL（Incoming ACL）] > [新規追加（Add New）] を選択します。

ステップ 2 着信 ACL の説明（Lync Standard Server など）を入力します。

ステップ 3 [アドレス パターン（Address Pattern）] フィールドに Lync サーバの FQDN を入力し、[保存（Save）] を選択します。

ヒント 新規の着信 ACL エントリを表示するには、ウィンドウの右上の [移動（Go）] を選択します。設定済みのすべての着信 ACL のリストが表示されます。

ステップ 4 [新規追加（Add New）] を選択します。

ステップ 5 着信 ACL の説明（Lync Standard Server など）を入力します。

ステップ 6 [アドレス パターン（Address Pattern）] フィールドに Lync サーバの IP アドレスを入力し、[保存（Save）] を選択します。

ステップ 7 [Cisco Unified CM IM and Presence Administration] > [システム（System）] > [セキュリティ（Security）] > [発信 ACL（Outgoing ACL）] > [新規追加（Add New）] を選択します。

ステップ 8 発信 ACL の説明（Lync Standard Server など）を入力します。

ステップ 9 [アドレス パターン（Address Pattern）] フィールドに Lync サーバの FQDN を入力し、[保存（Save）] を選択します。

ヒント　新規の発信 ACL エントリを表示するには、ウィンドウの右上の [移動（Go）] を選択します。設定済みのすべての発信 ACL のリストが表示されます。

ステップ 10　[新規追加（Add New）] を選択します。

ステップ 11　発信 ACL の説明（Lync Standard Server など）を入力します。

ステップ 12　[アドレス パターン（Address Pattern）] フィールドに Lync サーバの IP アドレスを入力し、[保存（Save）] を選択します。

次の作業

ルーティング設定の設定, （17 ページ）

ルーティング設定の設定

次の手順を実行し、ルーティング設定を設定します。

手順

ステップ 1　[Cisco Unified CM IM and 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、[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 4　[保存（Save）] を選択します。

次の作業

リモート通話コントロールの設定, （17 ページ）

リモート通話コントロールの設定

IM and Presence サービス CTI 接続の設定

次の手順を実行し、IM and Presence サービスで CTI 接続を設定します。

はじめる前に

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 CM IM and Presence Administration] > [アプリケーション（Application）] > [Microsoft RCC] > [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 IM and Presence サービスから Cisco Unified Communications Manager ノードに送信されるハートビート メッセージの間隔です。

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 Lync 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。

（注） Microsoft Lync を統合するには、[MOC サーバ OCS（MOC server OCS）] を選択する必要があります。

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。

重要 [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 Lync クライアントに IM and Presence サービス Lync Remote Call Control プラグインをインストールする必要があります。IM and Presence サービス Lync Remote Call Control プラグインをインストールすると、Microsoft Lync クライアントにメニュー アイテムが追加されて、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。

次の作業

ユーザの機能の割り当て，（19 ページ）

関連トピック

CTI ゲートウェイ アプリケーション ユーザの設定，（11 ページ）
Lync Remote Call Control のインストール，（59 ページ）
Microsoft RCC トラブルシュータの実行，（19 ページ）

ユーザの機能の割り当て

次の手順を実行し、ユーザにMicrosoftリモート通話コントロール（RCC）機能を割り当てます。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] > [アプリケーション（Application）] > [Microsoft RCC] > [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 リモート通話コントロール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 [Microsoft RCC の割り当て（Microsoft RCC Assignment）] ウィンドウで、[Microsoft RCC を有効にする（Enable Microsoft RCC）] をオンにします。

ステップ 6 [保存（Save）] を選択します。

重要 リモート通話コントロール機能を各 Microsoft Lync ユーザに割り当てたことを確認します。

次の作業

Microsoft RCC トラブルシュータの実行, （19 ページ）

関連トピック

IM and Presence サービス CTI 接続の設定, （17 ページ）
Microsoft RCC トラブルシュータの実行, （19 ページ）

Microsoft RCC トラブルシュータの実行

Microsoft RCC トラブルシュータは、Microsoft Lync クライアントと IM and Presence サービス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 CM IM and Presence Administration] > [診断（Diagnostics）] > [Microsoft RCC トラブルシュータ（Microsoft RCC 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 Lync のサーバ アドレスを入力します。

ステップ 4 [送信（Submit）] を選択します。

次の作業

IM and Presence サービスのための Microsoft コンポーネント統合の設定, （21 ページ）

第 5 章

IM and Presence サービスのための Microsoft コンポーネント統合の設定

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。ここで、
  - 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 IM and Presence サービスに報告する、ディレクトリ番号を指定します。
  - phone-context=dialstring を指定すると、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 Microsoft Lync クライアントが制御できるようになります。

（注） E.164 形式の番号を使用している場合、phone-context=dialstring を含めないでください。Microsoft Lync クライアントでエラーになります。E.164 形式の番号使用時の Lync のエラー，（68 ページ）を参照してください。

- デバイス ID を設定する場合、Microsoft Lync 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 Lync 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 Lync ユーザがサインインするときだけ有効になります。
- 最初のサインインの後に、Microsoft Lync ユーザは Cisco Unified Communications Manager IM and Presence サービス Lync Remote Call Control プラグインを通じて制御するライン 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ディレクトリ番号（DN）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。

（注） 回線 URI では E.164 形式の番号も使用できます。ただし、Cisco Unified Communications Manager の DN が E.164 で設定されている必要があります。

関連トピック

ライン アピアランス, （4 ページ）
IM and Presence サービス ユーザ認証, （22 ページ）
Lync Remote Call Control のインストール, （59 ページ）

IM and Presence サービス ユーザ認証

Microsoft Active Directory で SIP URI を設定するときは、IM and Presence サービス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. IM and Presence サービスは、Microsoft Lync にサインインしたユーザ 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。IM and Presence サービスで一致する ID が見つからない場合は、次の処理を行います。
2. IM and Presence サービスは、Microsoft Lync ユーザの電子メールの From ヘッダが Cisco Unified Communications Manager ユーザの電子メール アドレスと一致するかどうかを確認します。IM and Presence サービスで一致する ID が見つからない場合は、次の処理を行います。
3. IM and Presence サービスは Microsoft Lync ユーザの電子メール アドレスが 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 Lync 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。

その場合、IM and Presence サービスは次の項目を確認します。

- Cisco Unified Communications Manager データベース内の、ユーザ ID「joe」の有無。このユーザ ID が存在しない場合：
- Cisco Unified Communications Manager データベース内の、電子メール アドレス「joe@someCompany.com」の有無。このメールが存在しない場合：
- Cisco Unified Communications Manager データベース内の、ocsPrimaryAddress「sip:joe@someCompany.com」の有無。

Microsoft Active Directory の設定

はじめる前に

- 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。
- IM and Presence サービス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) 追加したユーザを Microsoft Lync サーバで有効にします。
b) SIP URI を入力します。
c) Microsoft Lync のサーバ名またはプールを入力します。
注意 Microsoft Lync 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) [テレフォニー設定（Telephony Settings）] で [設定（Configure）] を選択します。
e) [リモートからのコール制御の有効化（Enable Remote call control）] をオンにします。
f) 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 IM and Presence サービス ノードの FQDN を指定します。
g) 回線 URI 値を入力します。

重要 Microsoft Active Directory で入力する SIP URI は、Microsoft Lync 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。

次の作業

Lync Server のコントロール パネルでユーザを有効にする，（24 ページ）

Lync Server のコントロール パネルでユーザを有効にする

ここでは、Lync Server のコントロール パネルで新しいユーザを有効にする方法について説明します。

手順

ステップ 1 Microsoft Lync Server がインストールされている Windows サーバにアクセスします。

ステップ 2 [スタート（Start）][すべてのプログラム（All Programs）] > [Microsoft Lync サーバ（Microsoft Lync Server）] > [Lync Server コントロール パネル（Lync Server Control Panel）] を選択します。

ステップ 3 [トップ アクション（Top Actions）] メニューで [Lync Server に対してユーザを有効にする（Enable users for Lync Server）] を選択します。

ステップ 4 [追加（Add）] を選択します。

ステップ 5 [LDAP 検索（LDAP search）] オプションを選択し、[検索（Find）] を選択します。

ステップ 6 有効にするユーザをクリックし、[OK] を選択します。

ステップ 7 [ユーザをプールに割り当て（Assign users to a pool）] ドロップダウン リストからアプリケーション プールを選択します。

ステップ 8 [SIP URI を指定する（Specify a SIP URI）] オプションを選択し、SIP URI を入力します。入力する SIP URI の例は、sip:UserA@lyncdomain.com で、UserA は追加したユーザ、lyncdomain.com は Lync サーバのドメイン名を表します。

ステップ 9 [テレフォニー（Telephony）] ドロップダウン リストから [リモート通話コントロール（Remote call control）] を選択します。

ステップ 10 回線 URI を tel:<telephone_number> の形式で入力します。<telephone_number> はユーザの追加時に入力した電話番号です。

ステップ 11 Line サーバの URI を入力します。入力する URI の例は、sip:UserA@my-cups.my-domain.com で、UserA は追加したユーザ、my-cups.my-domain.com は IM and Presence サービス ノードのドメイン名を表します。
次の点に注意してください。

a) Line サーバの URI ドメインは、スタティック ルートの MatchUri パラメータで一致する値となります。Microsoft Lync サーバのスタティック ルートの設定 , （26 ページ）を参照してください。

b) Lync サーバが IM and Presence サービスへと SIP メッセージを正しくルーティングするには、Line サーバ URI ドメインと MatchUri パラメータの値は、一致している必要があります。

c) IM and Presence サービス ノードでは、このドメインをプロキシ ドメインとして設定していなければなりません。

ステップ 12 ウィンドウ上部で [有効（Enable）] を選択し、新しいユーザを有効にします。ユーザは、[有効（Enable）] 列がオンになっている必要があります。

次の作業

Microsoft Lync Server の設定概要, （25 ページ）

関連トピック

Microsoft Active Directory での回線 URI の設定, （21 ページ）
IM and Presence サービス ユーザ認証, （22 ページ）
ライン アピアランス, （4 ページ）

Microsoft Lync Server の設定概要

（注） このトピックでは、統合のために Microsoft Lync サーバで必要な設定について簡単に説明します。Microsoft Lync の設定全体については、このドキュメントでは説明しません。詳細については、次の URL のMicrosoft Lync のドキュメントを参照してください。http://technet.microsoft.com/en-us/library/gg558664.aspx。

Microsoft Lync 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 Lync で次の項目が設定されていることを確認します。

1. 証明書設定
2. スタティック ルート
3. 認証済みホスト
4. ドメイン ネーム サーバ
5. プール プロパティ
6. サーバ プロパティ
7. プール ユーザ
8. ユーザの設定
9. Microsoft Lync クライアント設定

（注） CTI ゲートウェイが TCP を使うよう設定されている場合、Lync Server トポロジ ビルダーでゲートウェイの IP アドレスを定義する必要があります。詳細については、次の URL を参照してください。http://technet.microsoft.com/en-us/library/gg602125.aspx。http://technet.microsoft.com/en-us/library/gg602125.aspx

Lync Server 管理シェル ユーティリティを使用して Microsoft Lync Server を設定します。管理シェルユーティリティは、Lyncサーバのインストール時にデフォルトでインストールされています。Microsoft Lync server の設定時に、次の項目を設定します。

- スタティック ルート
- アプリケーション プール

- リモート通話コントロール（RCC）アプリケーション
- Lync Server の SIP リッスン ポート

Microsoft Lync Server の設定後に、トポロジを確定し、フロントエンド サービスを再起動します。

Microsoft Lync サーバのスタティック ルートの設定

Lync サーバは、受信クライアントの SIP メッセージ INVITE の URI との一致にスタティック ルートを使用します。Lync サーバは、URI 値を Line サーバの URI として参照します。

手順

ステップ 1 [スタート（Start）] > [すべてのプログラム（All Programs）] > [Microsoft Lync サーバ（Microsoft Lync Server）] > [Lync Server 管理シェル（Lync Server Management Shell）] の順に選択します。

ステップ 2 次のコマンドを実行し、現在のシステム設定を確認します。

```
Get-CsStaticRoutingConfiguration
```

ステップ 3 次のコマンドを実行し、スタティック ルートを作成します。

```
$tcpRoute = New-CsStaticRoute -TCPRoute -Destination <IP_address_CUPserver> -Port 5060
-MatchUri "<Line_Server_URI_domain>" -ReplaceHostInRequestUri $true
```

ステップ 4 プロンプトで次のコマンドを実行し、スタティック ルートを Lync サーバに読み込みます。

```
Set-CsStaticRoutingConfiguration -Route @{Add=$tcpRoute}
```

ステップ 5 ステップ 2, （26 ページ）に従い再度 Get コマンドを実行し、新しいシステム設定を確認します。

（注） スタティック ルートを変更または削除する場合は、次のコマンドを実行します。

```
Remove-CsStaticRoutingConfiguration -Identity Global
```

次の表に、Lync サーバに新しいスタティック ルートを挿入する際に使用するパラメータを示します。

表 *1*：スタティック ルートのパラメータ

パラメータ	説明
$tcpRoute	変数の名前。好きな名前をつけることができますが、$ で始まり、Set コマンドの参照に一致している必要があります。
New-CsStaticRoute	スタティック ルートから変数に設定する内部コマンド。
-TCPRoute	このパラメータはルートを TCP として設定します。
-Destination	IM and Presence サービス ノードの IP アドレス。
-Port	IM and Presence サービス ノードがリッスンするポート。TCP の場合、ポートは 5060 です。

パラメータ	説明
-MatchUri	この値は、Lync のコントロール パネルで各ユーザに指定した Line サーバの URI と比較されます。Lync Server のコントロール パネルでユーザを有効にする, （24 ページ）を参照してください。 MatchURI 値と Line サーバの URI 値の両方が、IM and Presence サービス ノードFQDNのドメインと一致する必要があります。 このパラメータの値は、二重引用符で囲む必要があります。次に例を示します。 `-MatchUri "my-cups.my-domain.com"`
-ReplaceHostInRequestUri	このパラメータは、初期値の INVITE の URI を、Destination パラメータで参照される値に置き換えます。
-CsStaticRoutingConfiguration	パラメータ値をルーティング データベースに移動するための内部コマンド。
-Route	このパラメータは、変数のパラメータを取得し、スタティック ルートを追加します。

次の作業

Microsoft Lync Server のアプリケーション プールの設定 , （27 ページ）

Microsoft Lync Server のアプリケーション プールの設定

次の手順を実行し、Lync サーバ（レジストラ）が参照するアプリケーション プールを設定します。サイトの情報をこのプールへとリンクします。

手順

ステップ 1 Lync Server 管理シェルで次のコマンドを実行し、現在のシステム設定を確認します。
```
Get-CSTrustedApplicationPool
```

ステップ 2 次のコマンドを実行し、アドレス プールを作成します。
```
New-CsTrustedApplicationpool -Identity "<IP_address_CUPserver>" -Registrar <Lync_server_FQDN>
-Site 1 -TreatAsAuthenticated $True -ThrottleAsServer $True -RequiresReplication $False
```

ステップ 3 プロンプトで、[Y] を選択します。

ステップ 4 ステップ 1, （27 ページ）に従い再度 Get コマンドを実行し、新しいシステム設定を確認します。

ヒント　アプリケーション プールを変更または削除する場合は、次のコマンドを実行します。

```
Remove-CsTrustedApplicationPool -Identity
TrustedApplicationPool:<IP_address_CUPserver>
```

次の表に、アプリケーション プールの設定の際に使用するパラメータを示します。

表 2：アプリケーション プールのパラメータ

パラメータ	説明
New-CsTrustedApplicationPool	アプリケーション プールを追加する内部コマンド。
-Identity	プールの参照名。IM and Presence サービス ノードの IP アドレスでもあります。 このパラメータの値は、二重引用符で囲む必要があります。たとえば、`-Identity "10.0.0.1"` などです。 この値は、Microsoft Lync サーバの RCC アプリケーションの設定，（28 ページ）に従い、TrustedApplication コマンドの TrustedApplicationPoolFqdn パラメータに一致する必要があります。
-Registrar	Lync サーバの FQDN。
-Site	サイトを数値で表した値。 ヒント　Get-CsSite 管理シェル コマンドを使用してサイトの ID を検索できます。
-TreatAsAuthenticated	このパラメータの値は常に $True に設定します。
-ThrottleAsServer	このパラメータの値は常に $True に設定します。
-RequiresReplication	TCP では認証は不要なため、このパラメータの値は $False に設定する必要があります。

次の作業

Microsoft Lync サーバの RCC アプリケーションの設定，（28 ページ）

Microsoft Lync サーバの RCC アプリケーションの設定

次の手順を実行し、プールに Microsoft リモート通話コントロール（RCC）アプリケーションを追加します。

手順

ステップ 1 Lync Server 管理シェルで次のコマンドを実行し、現在のシステム設定を確認します。

```
Get-CSTrustedApplication
```

ステップ 2 次のコマンドを実行し、プールに RCC アプリケーションを追加します。

```
New-CsTrustedApplication -ApplicationID RCC -TrustedApplicationPoolFqdn
"<IP_address_CUPserver>" -Port 5060 -EnableTcp
```

ステップ 3 プロンプトで、[Y] を選択します。

ステップ 4 ステップ 1, （29 ページ）に従い再度 Get コマンドを実行し、新しいシステム設定を確認します。

ヒント アプリケーション プールを変更または削除する場合は、次のコマンドを実行します。

```
Remove-CsTrustedApplicationPool -Identity
TrustedApplicationPool:<IP_address_CUPserver>
```

次の表に、アプリケーション プールの設定の際に使用するパラメータを示します。

表 *3*：アプリケーション設定パラメータ

パラメータ	説明
New-CsTrustedApplication	RCC アプリケーションを追加する内部コマンド。
-ApplicationID	RCC などのアプリケーション名。
-TrustedApplicationPoolFQDN	IM and Presence サービス ノードの IP アドレス。 このパラメータの値は、二重引用符で囲む必要があります。たとえば、`-Identity "10.0.0.1"` などです。 この値は、Microsoft Lync Server のアプリケーション プールの設定 , （27 ページ）に従い、TrustedApplicationpool コマンドの Identity パラメータに一致する必要があります。
-Port	IM and Presence サービス ノードの SIP TCP リスニング ポート。TCP の場合、ポートは 5060 です。
-EnableTCP	このパラメータは、TCP への送信を設定します。このパラメータが含まれていない場合、送信はデフォルトで TLS となります。 （注） TLS を介した Microsoft Lync サーバの通信の詳細については、IM and Presence サービスと Microsoft Lync とのセキュリティ設定, （45 ページ）を参照してください。

次の作業

Lync サーバの SIP リッスン ポートの設定, （30 ページ）

Lync サーバの SIP リッスン ポートの設定

次の手順を実行し、Lync サーバでリッスン ポートを設定します。IM and Presence サービス ノードからの SIP トラフィックの受信で必要となります。

手順

ステップ 1 Lync Server 管理シェルで次のコマンドを実行し、現在のシステム設定を確認します。

```
Get-CSRegistrarConfiguration
```

ステップ 2 次のコマンドを実行し、Lync サーバのリッスン ポートを設定します。

```
Set-CsRegistrar registrar:<Lync_server_FQDN> -SipServerTcpPort 5060
```

ステップ 3 ステップ 1, （30 ページ）に従い再度 Get コマンドを実行し、新しいシステム設定を確認します。

ヒント アプリケーション プールを変更または削除する場合は、次のコマンドを実行します。

```
Remove-CsRegistrarConfiguration
```

次の表に、Lync サーバのリッスン ポートの設定の際に使用するパラメータを示します。

表 *4* : *Lync* サーバのリッスン ポートのパラメータ

パラメータ	説明
Set-CsRegistrar	Lync サーバのポートを設定する内部コマンド。
registrar:	Lync サーバの FQDN。
-SipServerTcpPort	Lync サーバの SIP リッスン ポート。通常、デフォルト値は 5060 です。

次の作業

Lync Server の設定の確定, （30 ページ）

Lync Server の設定の確定

ここでは、トポロジを確定し、フロントエンド サービスを再起動する方法を説明します。

手順

ステップ 1 Lync Server 管理シェルで次のコマンドを実行し、トポロジを有効にします。

```
Enable-CsTopology
```

ステップ 2 次のコマンドを実行し、トポロジを rcc.xml という XML ファイルに書き出し、ファイルを C ドライブに保存します。

```
Get-CsTopology -AsXml | Out-File C:\rcc.xml
```

（注） トポロジ情報を出力するファイルの名前と保存場所は自由に設定できます。

ステップ 3 rcc.xml ファイルを開きます。

ステップ 4 [クラスタ FQDN（Cluster Fqdn）] セクションで、IPAddress パラメータを「“<0.0.0.0>”」から IM and Presence サービス ノードの IP アドレスに変更します。

ステップ 5 rcc.xml ファイルを保存します。

ステップ 6 Lync Server 管理シェルで次のコマンドを実行します。

```
Publish-CsTopology -FileName C:\rcc.xml
```

ステップ 7 次のコマンドを実行して、フロントエンド サービスを再起動します。

```
Restart-Service RtcSrv
```

次の作業

正規化規則の設定, （33 ページ）

第 6 章

正規化規則の設定

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。

- Active Directory では、ユーザは E.164 形式の電話番号でプロビジョニングされていない
- 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であると見なし、ユーザ名が Microsoft Lync 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 Lync ユーザが発信側の名前を参照できるようにするには、Microsoft Lync 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。

はじめる前に

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 Lync の CA 署名済み証明書が Microsoft Lync 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 Lync Server で正規化が有効になっていることを確認します。それには、Lync Server 管理シェルを開き、次のコマンドを実行します。

```
Get-CsAddressBookConfiguration
```

UseNormalizationRules 値が True に設定されている場合、正規化は有効になっています。UseNormalizationRules 値が False に設定されている場合、次のコマンドを実行して正規化を有効にします。

```
Set-CsAddressBookConfiguration -UseNormalizationRules $True
```

ステップ 2 サーバの初期展開時に設定された Lync Server の共有ディレクトリ内で、ABFiles サブディレクトリを探します。[トポロジ ビルダー（Topology Builder）]>[ファイル ストア（File Stores）]を選択し、ファイル サーバの FQDN と共有名を特定します。パスは次のとおりです。`\\<Server FQDN>\<Share Folder>\1-WebServices-1\ABFiles`

ステップ 3 次のサンプル ファイルに移動します `C:\Program Files\Microsoft Lync Server 2010\WebComponents\Address Book Files\Files\Sample_Company_Phone_Number_Normalization_Rules.txt`

ステップ 4 Sample_Company_Phone_Number_Normalization_Rules.txt ファイルをコピーし、ABFiles ディレクトリ内に Company_Phone_Number_Normalization_Rules.txt として保存します。

（注） Company_Phone_Number_Normalization_Rules.txt ファイルは、実際のアドレス帳ファイルが保存されている場所ではなく、ABFiles ディレクトリに保存する必要があります。

ステップ 5 メモ帳で Company_Phone_Number_Normalization_Rules.txt ファイルを開き、 `[\s()\-\./]*` のような正規表現を削除します。Microsoft Lync Server は、テレフォニーに無関係な桁は無視し、0 ～ 9 までの連続した数字の桁のパターンのみ分析します。ただし、「+」接頭辞は認識します。

ステップ 6 Lync Server 管理シェルで次のコマンドを実行し、Company_Phone_Number_Normalization_Rules.txt ファイルに新しい設定をインポートし、アドレス帳ファイルに保存された番号に適用します。

```
Update-CsAddressBook
```

ステップ 7 5 分待ってから、Lync クライアントでアドレス帳を強制更新します。Microsoft Lync アドレス帳の更新, （35 ページ）を参照してください。

次の作業

Microsoft Lync アドレス帳の更新, （35 ページ）

サンプルの正規化規則

```
## +1 (ddd) ddd-dddd EXTddddd
#
\+1(\d{10})EXT(\d{5})
+1$1;ext=$2
#
# +1 (ddd) ddd-dddd Xdddddd
#
\+1(\d{10})[Xx]{1}(\d{5})
+1$1;ext=$2
#
```

```
# 1 (ddd) ddd-dddd
#
1(\d{10})
+1$1
#
# +1 (ddd) 70ddddd
#
\+1(\d{3})70(\d{5})
+1$170$2;ext=$2
#
# 70d-dddd Xddddd
#
70(\d{5})[Xx]{1}(\d{5})
+142570$1;ext=$2
#
# ddd-dddd Xddddd
#
(\d{7})[Xx]{1}(\d{5})
+1425$1;ext=$2
```

Microsoft Lync アドレス帳の更新

デフォルトのクライアント/サーバ設定では、アドレス帳はすぐには更新されません。Active Directory に追加された最新ユーザでアドレス帳が更新されるようにするには、サーバ側で強制的に更新し、Microsoft Lync が最新のファイルを強制的に取得し、ローカルの GalContacts.db ファイルを更新するようにしなければなりません。

手順

ステップ 1 Lync サーバの Lync サーバ管理シェルで、次のコマンドを実行します。

```
Update-CsAddressBook
```

このコマンドにより、Lync Server は SQL データベース内の現在の Active Directory 情報と、ダウンロード可能なクライアントとデバイスのアドレス帳ファイルとの同期を実行します。

（注） 同期プロセスが完了するまで 5 分間待機します。

ステップ 2 Microsoft Lync の管理権限で、Windows のコマンド プロンプトから次のコマンドを実行します。

```
reg add HKLM\Software\Policies\Microsoft\Communicator /v GalDownloadInitialDelay /t REG_DWORD /d 0 /f
```

このコマンドを実行すると、Microsoft Lync がアドレス帳のダウンロードをすぐに実行します。

ステップ 3 Microsoft Lync に GalContacts.db および GalContacts.db.idx ファイルが存在することを確認します。存在する場合、ユーザのプロファイル ディレクトリから削除します。

ステップ 4 Microsoft Lync 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 5 Microsoft Lync クライアントを起動し、再度サインインします。

ステップ 6 更新済みの GalContacts.db および GalContacts.db.idx ファイルがダウンロードされていることを確認します。

ステップ 7 新しいユーザを検索し、ユーザ名が Microsoft Lync に表示されることを確認します。

次の作業

IM and Presence サービスのセキュリティ証明書の設定, （37 ページ）

関連トピック

Microsoft Active Directory での正規化規則の設定, （33 ページ）

第 7 章

IM and Presence サービスのセキュリティ証明書の設定

この章は、IM and Presence サービスと Microsoft Lync との間のセキュアな接続が必要な場合のみ適用されます。

この章では、スタンドアロンの CA を使用したセキュリティ証明書の設定について説明します。企業の CA を使用している場合は、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』の、企業の CA を使用した証明書交換手順の例を参照してください。

（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

次の手順を実行し、スタンドアロン ルート CA を設定します。

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、[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 4 [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 5 [アプリケーション サーバ（Application Server）] を選択し、[Internet Information Services（IIS）] を選択します。

ステップ 6 インストール手順を完了します。

ステップ 7 [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 8 [証明書サービス（Certificate Services] を選択し、[次へ（Next）] を選択します。

ステップ 9 [スタンドアロンのルート CA（Standalone root CA）] を選択し、[次へ（Next）] を選択します。

ステップ 10 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 11 時間を、この証明書に必要な年数に変更し、[次へ（Next）] を選択してインストールを開始します。

ステップ 12 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 13 [次へ（Next）] を選択します。

ステップ 14 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 15 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、[終了（Finish）] を選択します。

次の作業

CA サーバからルート証明書をダウンロード, （38 ページ）

CA サーバからルート証明書をダウンロード

次の手順を実行し、CA サーバからルート証明書をダウンロードします。

はじめる前に

スタンドアロン ルート認証局（CA）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 をダウンロード（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 証明書をダウンロード（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。

重要 ルート証明書のサブジェクトの共通名（CN）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。

次の作業

IM and Presence サービスへのルート証明書のアップロード, （39 ページ）

関連トピック

スタンドアロン ルート認証局（CA）の設定, （37 ページ）

IM and Presence サービスへのルート証明書のアップロード

次の手順を実行し、ルート証明書を IM and Presence サービスにアップロードします。

はじめる前に

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 IM and Presence サービス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 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（Root Name）] 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、自分のコンピュータ上で certnew.cer ファイルの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 6 [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。

次の作業

IM and Presence サービスの証明書署名要求の生成, （40 ページ）

関連トピック

CA サーバからルート証明書をダウンロード, （38 ページ）
IM and Presence サービスへの署名付き証明書のアップロード, （43 ページ）

IM and Presence サービスの証明書署名要求の生成

次の手順を実行し、IM and Presence サービスの証明書署名要求（CSR）を生成します。

はじめる前に

ルート証明書を IM and Presence サービスにアップロードします。

手順

ステップ 1 [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 を作成（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 を作成（Generate CSR）] を選択します。

次の作業

IM and Presence サービスからの CSR のダウンロード, （41 ページ）

関連トピック

IM and Presence サービスへのルート証明書のアップロード, （39 ページ）

IM and Presence サービスからの CSR のダウンロード

次の手順を実行し、IM and Presence サービスから CSR をダウンロードします。

はじめる前に

IM and Presence サービスの CSR を生成します。

手順

ステップ 1 [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 をダウンロード（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 をダウンロード（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。

次の作業

CA サーバで証明書署名要求を送信, （41 ページ）

関連トピック

IM and Presence サービスの証明書署名要求の生成, （40 ページ）

CA サーバで証明書署名要求を送信

次の手順を実行し、CA サーバで CSR を送信します。

はじめる前に

IM and Presence サービスから CSR 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/certserv` 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、[証明書の要求の詳細設定（Advanced certificate request）] を選択します。

ステップ 4 [Base 64 エンコード CMC または 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。（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 5 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 6 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 7 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 8 [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 9 [管理ツール（Administrative Tools）] で [証明機関（Certificate Authority）] を開きます。
[認証局（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 10 証明書要求を右クリックし、[すべてのタスク（All Tasks）] > [発行（Issue）] を選択します。

ステップ 11 [発行済み証明書（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。

次の作業

CA サーバから署名付き証明書をダウンロード, （42 ページ）

関連トピック

IM and Presence サービスからの CSR のダウンロード, （41 ページ）

CA サーバから署名付き証明書をダウンロード

次の手順を実行し、CA サーバから署名済み証明書をダウンロードします。

はじめる前に

CA サーバで CSR 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。

次の作業

IM and Presence サービスへの署名付き証明書のアップロード, （43 ページ）

関連トピック

CA サーバで証明書署名要求を送信, （41 ページ）

IM and Presence サービスへの署名付き証明書のアップロード

次の手順を実行し、署名済み証明書を IM and Presence サービスにアップロードします。

はじめる前に

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 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、自分のコンピュータ上で署名済みの cup.pem 証明書のある場所に移動します。
ステップ 6 [ファイルのアップロード（Upload File）] を選択します。

次の作業

Lync Remote Call Control のインストール, （59 ページ）

関連トピック

CA サーバから署名付き証明書をダウンロード, （42 ページ）

第 8 章

IM and Presence サービスと Microsoft Lync とのセキュリティ設定

この章は、IM and Presence サービスと Microsoft Lync との間のセキュアな接続が必要な場合のみ適用されます。

Microsoft Lync のセキュリティ証明書の設定

CA 証明書チェーンをダウンロード

次の手順を実行し、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）] > [実行（Run）] を選択します。

ステップ 2 `http://<発行 CA サーバの名前>/certsrv` と入力し、[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 をダウンロード（Download a CA certificate, certificate chain, or CRL）] を選択します。

ステップ 4 [CA 証明書チェーンをダウンロード（Download CA certificate chain）] を選択します。

ステップ 5 [ファイルをダウンロード（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。

（注） 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 証明書チェーンをインストール, （46 ページ）

CA 証明書チェーンをインストール

次の手順を実行し、CA 証明書チェーンをインストールします。

はじめる前に

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）] > [実行（Run）] を選択します。
ステップ 2 mmc と入力し、[OK] をクリックします。
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、続いて [追加（Add）] を選択します。
ステップ 6 [コンピュータ アカウント（Computer account）] を選択し、[次へ（Next）] をクリックします。
ステップ 7 [コンピュータの選択（Select Computer）] ダイアログ ボックスで、自分のコンピュータ（このコンソールを実行中のコンピュータ）が選択されていることを確認します。
ステップ 8 [終了（Finish）] を選択し、[閉じる（Close）] を選択し、最後に [OK] を選択します。
ステップ 9 [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 10 [信頼されたルート証明機関（Trusted Root Certification Authorities）] を展開し、[証明書（Certificates）] を右クリックします。
ステップ 11 [すべてのタスク（All Tasks）] をポイントして、[インポート（Import）] を選択します。
ステップ 12 インポート ウィザードで [次へ（Next）] を選択します。
ステップ 13 [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 14 [開く（Open）] を選択し、[次へ（Next）] を選択します。
ステップ 15 [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 16 [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 17 [次へ（Next）] を選択し、[終了（Finish）] を選択します。

次の作業

CA サーバで証明書要求を送信, （47 ページ）

関連トピック

CA 証明書チェーンをダウンロード, （45 ページ）

CA サーバで証明書要求を送信

次の手順を実行し、CA サーバで証明書要求を送信します。

はじめる前に

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 [スタート（Start）] > [すべてのプログラム（All Programs）] > [Microsoft Lync サーバ（Microsoft Lync Server）] > [Lync Server 管理シェル（Lync Server Management Shell）] の順に選択します。

ステップ 2 次のコマンドを実行し、Microsoft Lync Server の証明書要求を送信します。

```
Request-CsCertificate -New -Type Default -DomainName <FQDN of Lync Server> -Output c:\cert.csr
-ClientEku $true
```

ステップ 3 Microsoft Lync Server から URL `http://<発行 CA サーバの名前>/certsrv` を入力します。

ステップ 4 [証明書を要求する（Request a certificate）] を選択し、[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 [Base 64 エンコード CMC または 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。（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 ステップ 2, （48 ページ） のファイル cert.csr を開き、ファイル内のすべての情報をクリップボードにコピーします。

ステップ 7 ファイル cert.csr の情報を認証権限サーバの [保存された要求（Saved Request）] ボックスに貼り付け、[送信（Submit）] を選択します。

次の作業

証明書を承認し、インポート, （48 ページ）

関連トピック

CA 証明書チェーンをインストール, （46 ページ）

証明書を承認し、インポート

次の手順を実行し、証明書の承認およびインポートを行います。

はじめる前に

CA サーバで証明書要求を送信します。

手順

ステップ 1 認証権限サーバで、[管理ツール（Administrative Tools）]>[証明機関（Certificate Authority）] を選択します。

ステップ 2 [保留中の要求（Pending Requests）] を選択し、リスト内で新しい証明書を見つけます。

ステップ 3 新しい証明書を右クリックして、[すべてのタスク（All Tasks）]>[証明書の発行（Issue Certificate）] を選択します。

ステップ 4 Microsoft Lync Server から URL `http://<発行 CA サーバの名前>/certsrv` を入力します。

ステップ 5 [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 6 [Base 64 エンコード（Base 64 encoded）] を選択し、証明書を cer ファイル拡張子のファイルとして Microsoft Lync サーバのローカル ドライブにダウンロードします。

ステップ 7 証明書要求を作成した Microsoft Lync Server に、管理者グループのメンバーとしてサインインします。

ステップ 8 Lync Server 展開ウィザードを開始し、Lync Server システムの [インストール（Install）] または [更新（Update）] を選択します。

ステップ 9 [再実行（Run Again）] を選択します（手順 3：証明書の要求、インストール、または割り当てに加えて）。

ステップ 10 [利用可能な証明書タスク（Available Certificate Tasks）] ページで [インポート（Import）] を選択し、.p7b、.pfx または .cer ファイルから証明書をインポートします。

ステップ 11 [証明書のインポート（Import Certificate）] ページで、ステップ 6, （49 ページ） で証明機関から取得した証明書のフルパスとファイル名を入力します。または、[参照（Browse）] を選択してファイルを指定し、選択することもできます。

次の作業

インポートされた証明書の割り当て, （49 ページ）

関連トピック

CA サーバで証明書要求を送信, （47 ページ）

インポートされた証明書の割り当て

次の手順を実行し、インポート済みの証明書を割り当てます。

はじめる前に

証明書を承認し、インポートします。

手順

ステップ 1 Microsoft Lync Server で、Lync Server 展開ウィザードを開始します。

ステップ 2 Lync Server システムの [インストール（Install）] または [更新（Update）] を選択します。

ステップ 3 手順 3：証明書の要求、インストール、または割り当ての [再実行（Run Again）] を選択します。

ステップ 4 [利用可能な証明書タスク（Available Certificate Tasks）] ページで、[既存の証明書の割り当て（Assign an existing certificate）] を選択します。

ステップ 5 [証明書の割り当て（Certificate Assignment）] ページで、[次へ（Next）] を選択します。

ステップ 6 [証明書の利用詳細設定（Advanced Certificate Usages）] ページから、すべてのチェックボックスをオンにして、証明書をすべての利用に割り当てます。

ステップ 7 [証明書ストア（Certificate Store）] ページから、要求およびインポートした証明書を選択します。

ステップ 8 [証明書の割り当ての概要（Certificate Assignment Summary）] ページで設定を確認し、[次へ（Next）] を選択して証明書を割り当てます。

ステップ 9 ウィザードの終了ページで、[終了（Finish）] を選択します。

ステップ 10 各サーバで証明書スナップインを開き、[証明書（ローカル コンピュータ）（Certificates (Local Computer)）]>[個人用（Personal）]>[証明書（Certificates）] を選択し、証明書が [詳細（Details）] ウィンドウに表示されていることを確認します。

次の作業

サーバとのクライアントの認証の証明書設定の確認, （50 ページ）

関連トピック

証明書を承認し、インポート, （48 ページ）

サーバとのクライアントの認証の証明書設定の確認

次の手順を実行し、サーバとクライアントの認証の証明書が正しく設定されていることを確認します。

手順

ステップ 1 Microsoft Lync Server で、Lync Server 展開ウィザードを開始します。

ステップ 2 Lync Server システムの [インストール（Install）] または [更新（Update）] を選択します。

ステップ 3 手順 3：証明書の要求、インストール、または割り当ての [再実行（Run Again）] を選択します。

ステップ 4 [証明書ウィザード（Certificate Wizard）] ウィンドウで、デフォルトの証明書を強調表示し、[表示（View）] を選択します。

ステップ 5 [証明書の表示（View Certificate）] ウィンドウで、[証明書の詳細を表示（View Certificate Details）] を選択します。

ステップ 6 [証明書（Certificate）] ダイアログボックスで、[詳細（Details）] タブを選択します。

ステップ 7 [表示（Show）] ドロップダウン リストで、[拡張機能のみ（Extensions Only）] を選択します。

ステップ 8 [拡張キー使用（Enhanced Key Usage）] を選択し、次の情報が表示されていることを確認します。サーバ認証（1.3.6.1.5.5.7.3.1）、クライアント認証（1.3.6.1.5.5.7.3.2）。

ステップ 9 [スタート（Start）] > [すべてのプログラム（All Programs）] > [Microsoft Lync サーバ（Microsoft Lync Server）] > [Lync Server 管理シェル（Lync Server Management Shell）] の順に選択します。

ステップ 10 次のコマンドを実行し、Microsoft Lync Server からの証明書を表示します。 `Get-CsCertificate`

ステップ 11 次のようなデフォルト証明書があることを確認します。

```
Issuer    : CN=ne001a-lynccaNotAfter
NotAfter          : 6/16/2012 2:18:20 PM
NotBefore         : 6/16/2011 2:08:20 PM
SerialNumber      : 152E466D00000000000C
Subject           : CN=pool1.rcdnlync.com
AlternativeNames : {sip.rcdnlync.com, ne011a-lyncent.rcdnlync.com, pool1.rcdnlync.com}
Thumbprint        : 84BED88F2BFBB463CB4CBC328DAA6FD3A5E0677B
Use               : Default
```

次の作業

Microsoft Lync の TLS ルートの設定, （51 ページ）

Microsoft Lync の TLS ルートの設定

次のアイテムを設定し、Microsoft Lync で IM and Presence サービス の TLS ルートを設定します。

- スタティック ルート
- アプリケーション プール
- Microsoft リモート通話コントロール（RCC）アプリケーション

Microsoft Lync で、IM and Presence サービスの TLS ルートを設定した後は、トポロジを確定し、フロントエンド サービスを再起動します。

スタティック ルートの設定

次の手順を実行し、スタティック ルートを設定します。

手順

ステップ 1 [スタート（Start）] > [すべてのプログラム（All Programs）] > [Microsoft Lync サーバ（Microsoft Lync Server）] > [Lync Server 管理シェル（Lync Server Management Shell）] の順に選択します。

ステップ 2 TCP ルートが存在する場合は、次のコマンドを実行して削除します。

```
Remove-CsStaticRoutingConfiguration -Identity Global
```

ステップ 3 次のコマンドを実行し、スタティック TLS ルートを作成します。

```
$tlsRoute = New-CsStaticRoute -TLSRoute -Destination <FQDN CUP Server> -Port 5062 -MatchUri
*.rcdnlync.com -UseDefaultCertificate $true
```

ステップ 4 プロンプトで次のコマンドを実行し、スタティック ルートを Lync サーバに読み込みます。

```
Set-CsStaticRoutingConfiguration -Route @{Add=$tlsRoute}
```

ステップ 5 次のコマンドを実行し、新しいシステム設定を確認します。

```
Get-CsStaticRoutingConfiguration
```

次の表に、Lyncサーバに新しいスタティックルートを挿入する際に使用するパラメータを示します。

表 *5*：スタティック ルートのパラメータ

パラメータ	説明
$tlsRoute	変数の名前。好きな名前をつけることができますが、$ で始まり、Set コマンドの参照に一致している必要があります。
New-CsStaticRoute	スタティック ルートから変数に設定する内部コマンド。
-TLSRoute	このパラメータはルートを TLS として設定します。
-Destination	IM and Presence サービス ノードの FQDN。
-Port	IM and Presence サービス ノードがリッスンするポート。TLS の場合、ポートは 5062 です。
-MatchUri	この値はワイルドカードで、アスタリスク（*）に続いてドメインを表示します。Lyncのコントロールパネルで各ユーザに指定した Line サーバの URI と比較されます。Lync Server のコントロール パネルでユーザを有効にする，（24 ページ）を参照してください。
-UseDefaultCertificate	スタティックルートがデフォルトの証明書を使用するようにするため、この値は True に設定されています。

パラメータ	説明
-CsStaticRoutingConfiguration	パラメータ値をルーティング データベースに移動するための内部コマンド。
-Route	このパラメータは、変数のパラメータを取得し、スタティック ルートを追加します。

次の作業

アプリケーション プールの設定, （53 ページ）

アプリケーション プールの設定

次の手順を実行し、Lync サーバ（レジストラ）が参照するアプリケーション プールを設定します。サイトの情報をこのプールへとリンクします。

手順

ステップ 1 [スタート（Start）] > [すべてのプログラム（All Programs）] > [Microsoft Lync サーバ（Microsoft Lync Server）] > [Lync Server 管理シェル（Lync Server Management Shell）] の順に選択します。

ステップ 2 次のコマンドを実行し、既存の TCP アプリケーション プールを削除します。

```
Remove-CsTrustedApplicationPool -Identity TrustedApplicationPool:<IP_Address_CUPserver>
```

ステップ 3 次のコマンドを実行し、アドレス プールを作成します。

```
New-CsTrustedApplicationPool -Identity <FQDN CUP Server> -Registrar <FQDN of Pool> -site 1
-ThrottleAsServer $true -TreatAsAuthenticated $true
```

ステップ 4 プロンプトで、[Y] を選択します。

ステップ 5 次のコマンドを実行し、新しいシステム設定を確認します。

```
Get-CsTrustedApplicationPool
```

次の表に、アプリケーション プールの設定の際に使用するパラメータを示します。

表 *6*：アプリケーション プールのパラメータ

パラメータ	説明
New-CsTrustedApplicationPool	アプリケーション プールを追加する内部コマンド。
-Identity	IM and Presence サービス ノードの FQDN。
-Registrar	プールの参照名。Lync サーバの FQDN とすることもできます。

パラメータ	説明
-Site	サイトを数値で表した値。 ヒント　Get-CsSite 管理シェル コマンドを使用してサイトの ID を検索できます。
-TreatAsAuthenticated	このパラメータの値は常に `$True` に設定します。
-ThrottleAsServer	このパラメータの値は常に `$True` に設定します。

次の作業

RCC アプリケーションの設定, （54 ページ）

RCC アプリケーションの設定

次の手順を実行し、プールに Microsoft リモート通話コントロール（RCC）アプリケーションを追加します。

手順

ステップ 1　[スタート（Start）] > [すべてのプログラム（All Programs）] > [Microsoft Lync サーバ（Microsoft Lync Server）] > [Lync Server 管理シェル（Lync Server Management Shell）] の順に選択します。

ステップ 2　次のコマンドを実行し、既存の TCP アプリケーションを削除します。

```
Remove-CsTrustedApplication -Identity <IM and Presence サーバの FQDN>/urn:application:rcc
```

ステップ 3　次のコマンドを実行し、プールに RCC アプリケーションを追加します。

```
New-CsTrustedApplication -ApplicationID RCC -TrustedApplicationPoolFqdn <IM and Presence サーバの FQDN> -Port 5062
```

ステップ 4　プロンプトで、[Y] を選択します。

ステップ 5　次のコマンドを実行し、新しいシステム設定を確認します。

```
Get-CsTrustedApplication
```

次の表に、アプリケーション プールの設定の際に使用するパラメータを示します。

表 7: アプリケーション設定パラメータ

パラメータ	説明
New-CsTrustedApplication	RCC アプリケーションを追加する内部コマンド。
-ApplicationID	RCC などのアプリケーション名。

パラメータ	説明
-TrustedApplicationPoolFQDN	IM and Presence サービス ノードの FQDN。
-Port	IM and Presence サービス ノードの SIP リスニング ポート。TLS の場合、ポートは 5062 です。

次の作業

Lync Server の設定の確定, （55 ページ）

Lync Server の設定の確定

ここでは、トポロジを確定し、フロントエンド サービスを再起動する方法を説明します。

手順

ステップ 1 Lync Server 管理シェルで次のコマンドを実行し、トポロジを有効にします。

```
Enable-CsTopology
```

ステップ 2 次のコマンドを実行し、トポロジを rcc.xml という XML ファイルに書き出し、ファイルを C ドライブに保存します。

```
Get-CsTopology -AsXml | Out-File C:\rcc.xml
```

（注） トポロジ情報を出力するファイルの名前と保存場所は自由に設定できます。

ステップ 3 rcc.xml ファイルを開きます。

ステップ 4 [クラスタ FQDN（Cluster Fqdn）] セクションで、IPAddress パラメータを「“<0.0.0.0>”」から IM and Presence サービス ノードの IP アドレスに変更します。

ステップ 5 rcc.xml ファイルを保存します。

ステップ 6 Lync Server 管理シェルで次のコマンドを実行します。

```
Publish-CsTopology -FileName C:\rcc.xml
```

ステップ 7 次のコマンドを実行して、フロントエンド サービスを再起動します。

```
Restart-Service RtcSrv
```

次の作業

TLSv1 のための Microsoft Lync の設定, （56 ページ）

TLSv1 のための Microsoft Lync の設定

IM and Presence サービスは TLSv1 のみをサポートしているため、Microsoft Lync が TLSv1 を使用するように設定する必要があります。この手順では、Microsoft Lync が TLS 暗号 TLS_RSA_WITH_3DES_EDE_CBC_SHA で TLSv1 を送信できるように、Microsoft Lync 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。

手順

ステップ 1 [スタート（Start）] > [管理ツール（Administrative Tools）] > [ローカル セキュリティ ポリシー（Local 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（Details）] 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 [OK] を選択します。

ステップ 7 Windows Server を再起動し、FIPS セキュリティ設定への変更を有効にします。

次の作業

Microsoft Lync のための新しい TLS ピア サブジェクトの作成, （56 ページ）

Microsoft Lync のための新しい TLS ピア サブジェクトの作成

次の手順を実行し、IM and Presence サービスで Microsoft Lync のための新しい TLS ピア サブジェクトを作成します。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] > [IM and 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）] フィールドで、Microsoft Lync 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 Lync 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

TLS ピア サブジェクト リストへの TLS ピアの追加, （57 ページ）

TLS ピア サブジェクト リストへの TLS ピアの追加

次の手順を実行し、IM and Presence サービスの選択した TLS ピア サブジェクトのリストに TLS ピアを追加します。

はじめる前に

IM and Presence サービスに、Microsoft Lync のための新しい TLS ピア サブジェクトを作成します。

手順

ステップ 1 [Cisco Unified CM IM and 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）] の順に選択します。

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。

次の作業

Lync Remote Call Control のインストール, （59 ページ）

第 9 章

Lync Remote Call Control のインストール

クライアント コンピュータへの IM and Presence サービス Lync Remote Call Control プラグインのインストール

Cisco Unified CM IM and Presence サービス Lync Remote Call Control プラグインは、IM and Presence サービス メニュー アイテム Microsoft Lync クライアント インターフェイスに追加し、ユーザがコントロールする電話デバイスの選択を可能にします。ユーザが複数のデバイス（回線）を持つ場合は、プラグインをインストールする必要があります。ユーザが IM and Presence サービス メニュー アイテムを選択すると、IM and Presence サービスがユーザのデフォルトの Web ブラウザで Web ページを開きます。ユーザは、コントロールする電話デバイスをこの Web ページから選択できます。

はじめる前に

- Cisco Unified Communications Manager IM and Presence サービス ユーザ オプションのユーザ名とパスワード。
- 管理者は、[標準 CCM エンド ユーザ（Standard CCM End Users）] グループにユーザを割り当てる必要があります。このグループに追加されていることを確認します。
- この手順を実行するには、addrccmenu.bat という Cisco Unified CM IM and Presence Lync Remote Call Control プラグインのバッチ ファイルが必要です。このファイルは、**Cisco Unified CM IM and Presence Administration** ユーザ インターフェイス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）] を選択して Cisco Unified Communications Manager IM and Presence Lync Remote Call Control プラグインをダウンロードします。バッチ

ファイルは zip ファイルとしてダウンロードされます。この zip ファイルを Microsoft Lync クライアント コンピュータ上に保存し、解凍する必要があります。

手順

ステップ 1 Microsoft Lync クライアント コンピュータで Windows のコマンド プロンプトを開きます。

ステップ 2 解凍した addrccmenu.bat ファイルの場所に移動します。

ステップ 3 コマンドラインで次のコマンドを実行します。*<impserveraddress>* は IM and Presence サービス ノード IP アドレス、ホスト名、または FQDN となります。

```
addrccmenu.bat impserveraddress
```

ステップ 4 regedit のセキュリティ警告が表示されても、操作を続行します。

ステップ 5 操作が完了したら、Microsoft Lync からサインアウトします。

ステップ 6 再度 Microsoft Lync クライアントにサインインし、[ツール（Tools）] メニュー オプションを選択します。新しい Cisco メニュー アイテムが見られるようになりました。

（注） IM and Presence サービス メニュー アイテムが別の IM and Presence サービス ノードを示すようにする必要がある場合、別の IM and Presence サービス ノードの IP アドレス、ホスト名または FQDN を使用して、この手順を再実行できます。

次の作業

Microsoft Lync クライアントが IM and Presence サービス メニュー アイテムにアクセスした際、IM and Presence サービス Web ページがデフォルトの Web ブラウザで開かない場合、を参照してください。 IM and Presence サービスの Web ページを、Microsoft Lync クライアントのデフォルトの Web ブラウザから開くことができません。, （67 ページ）

IM and Presence サービス Lync Remote Call Control プラグインのインストール

Cisco Unified Communications Manager IM and Presence サービス Lync Remote Call Control プラグインをアンインストールするには、IM and Presence サービス ノードの IP アドレス、ホスト名または FQDN を指定せずに、バッチ ファイルを再実行します。

手順

ステップ 1 zip ファイルを Microsoft Lync コンピュータにダウンロードし、解凍します。

ステップ 2 Windows のコマンド プロンプトを開きます。

ステップ 3 解凍した addrccmenu.bat ファイルの場所に移動します。

ステップ 4 コマンド ラインで、次のコマンドを実行します。

```
addrccmenu.bat
```

ステップ 5 regedit のセキュリティ警告が表示されても、操作を続行します。

ステップ 6 操作が完了したら、Microsoft Lync からサインアウトします。

ステップ 7 再度 Microsoft Lync クライアントにサインインし、[ツール（Tools）] メニュー オプションを選択します。Cisco メニュー アイテムが表示されなくなります。

Web ブラウザを介して電話選択にアクセスする

設定のカスタマイズ、個人応答メッセージの作成、連絡先の整理には、Cisco Unified Communications Manager IM and Presence サービス ユーザ オプション Web インターフェイスを使用します。

はじめる前に

システム管理者から次の情報を入手します。

- Cisco Unified Communications Manager IM and Presence サービス ユーザ オプションのホスト名と IP アドレス。
- Cisco Unified Communications Manager IM and Presence サービス ユーザ オプションのユーザ名とパスワード。
- Cisco Unified Communications Manager IM and Presence サービス ユーザ オプション Web インターフェイスにログインするには、管理者がユーザを [標準 CCM エンド ユーザ（Standard CCM End Users）] グループに割り当てる必要があります。

手順

ステップ 1 コンピュータ上でサポートされている Web ブラウザを開きます。

ステップ 2 Cisco Unified Communications Manager IM and Presence サービス ユーザ オプションの URL アドレスを入力します。

https://*imp_server_address*:8443/cucmuser/showHomeMini.do?mini=true

imp_server_address は、IM and Presence サービス ノードのホスト名、FQDN、または IP アドレスです。

ステップ 3 Cisco Unified Communications Manager IM and Presence サービス ユーザ オプションのユーザ名を入力します。

ステップ 4 システム管理者から提供された Cisco Unified Communications Manager IM and Presence サービス ユーザ オプションのパスワードを入力します。

ステップ 5 [ログイン（Login）] をクリックします。
ユーザ オプション Web インターフェイスからログアウトするには、[ユーザ オプション] ウィンドウの右上隅にある [ログアウト] を選択します。セキュリティ上の理由により、非アクティブ時間が 30 分を経過すると、ユーザは自動的にユーザ オプションからログアウトされます。

第 10 章

Microsoft Lync サーバと Microsoft Lync クライアントのログ

Lync Server Logging Tool では、Lync サーバのトレースを取得し、メッセージ ログを表示できます。Microsoft Lync クライアントでも、SIP メッセージングなどのクライアント関連のログ情報を取得できます。

- トレースを取得し、Microsoft Lync サーバのログを表示，63 ページ
- Microsoft Lync クライアントのログを有効にし、表示，64 ページ

トレースを取得し、Microsoft Lync サーバのログを表示

次の手順を実行し、Microsoft Lync のトレースを取得し、メッセージ ログを表示します。

手順

ステップ 1 [スタート（Start）] > [すべてのプログラム（All Programs）] > [Microsoft Lync サーバ（Microsoft Lync Server）] > [Lync Server ロギング ツール（Lync Server Logging Tool）] の順に選択します。
ステップ 2 **[コンポーネント（Component）]** 領域で、[SIPStack] チェックボックスをオンにします。
ステップ 3 [レベル（Level）] 領域で [すべて（All）] オプションを選択します。
ステップ 4 [フラグ（Flags）] 領域で、すべてのフラグをオンにします。
ステップ 5 トレース取得の準備が整ったら、[ログの開始（Start Logging）] を選択します。
ステップ 6 トレース停止の準備が整ったら、[ログの停止（Stop Logging）] を選択します。
ステップ 7 [ログ ファイルの解析（Analyze Log Files）] を選択します。
ステップ 8 [SIPStack] および [SIPStackPerf] チェックボックスをオンにします。
ステップ 9 [解析（Analyze）] を選択します。
ステップ 10 [メッセージ（Messages）] タブを選択します。メッセージをクリックすると、内容が表示されます。

Microsoft Lync クライアントのログを有効にし、表示

次の手順を実行し、クライアントのログを有効にし、結果のログを表示します。

手順

ステップ 1 [スタート（Start）] > [すべてのプログラム（All Programs）] > [Microsoft Lync] > [Microsoft Lync サーバ（Microsoft Lync Server）] を選択します。
ステップ 2 ウィンドウの右上のドロップダウン矢印をクリックします。
ステップ 3 [ツール（Tools）] > [オプション（Options）] を選択します。
ステップ 4 左側のペインで [一般（General）] を選択します。
ステップ 5 [ログ（Logging）] 領域で [Lync でのログをオンにする（Turn on logging in Lync）] と [Lync の Windows イベント ログをオンにする（Turn on Windows Event logging for Lync）] チェックボックスをオンにします。
ステップ 6 [OK] を選択します。
ステップ 7 Lync クライアントを終了します。ただし、Lync クライアントからサイン アウトしないでください。
ステップ 8 クライアント コンピュータで `C:\Users\Administrator.NE001B-LYNCAD\Tracing>` に移動します。
ステップ 9 このディレクトリのすべてのファイルを選択し、削除します。
ステップ 10 Lync クライアントにサインインします。

ヒント　C:\Users\Administrator.NE001B-LYNCAD\Tracing> に新しいファイルが作成されています。

ステップ 11　Lync クライアントからのサインイン、またはコール試行を完了します。

ステップ 12　Lync クライアントを終了します。

ステップ 13　C:\Users\Administrator.NE001B-LYNCAD\Tracing> で Communicator-uccapi-0 ファイルを開きます。

（注）　Communicator-uccapi-0 ファイルには、SIP メッセージングのログや、その他のクライアント関連のログ情報が含まれます。

第 11 章

トラブルシューティング

IM and Presence サービスの Web ページを、Microsoft Lync クライアントのデフォルトの Web ブラウザから開くことができません。

問題 Microsoft Lync クライアント ユーザが IM and Presence サービス メニュー アイテムにアクセスする際、デフォルトの Web ブラウザが IM and Presence サービス ノードに接続できず、IM and Presence サービスの Web ページを開くことができません。

解決法 Microsoft Lync クライアント ユーザが IM and Presence サービス メニュー アイテムにアクセスする際、通常は IM and Presence サービスの Web ページがユーザのデフォルトの Web ブラウザで開きます。しかし、Web ブラウザから IM and Presence サービス ノードに接続できない場合、次の項目を確認します。

1. ブラウザの設定で JavaScript が有効になっていることを確認します。
2. Web ブラウザで次のアドレスを入力し、ブラウザから IM and Presence サービス ノードに接続できることを確認します。 https://*imp_server_address*:8443/cucmuser/showHomeMini.do?mini=true

imp_server_address は、IM and Presence サービス ノードのホスト名、FQDN、または IP アドレスです。

3 IM and Presence サービス ノードの IP アドレス、または FQDN の指定が間違っている場合、プラグインのインストール手順を再実行し、IM and Presence サービス ノードのアドレスを修正します。

4 接続に関して他に問題がある場合、次の作業が必要な場合があります。

- IM and Presence サービス ノードの Web アドレスを、Microsoft Lync クライアント コンピュータのブラウザの、信頼済み Web アドレスの一覧に追加します。Microsoft 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、信頼済みの Web アドレスの一覧に次のエントリを追加します。

  `https://<IM and Presence_server_name>`

- ドメインの HTTPS Web アドレスを IM and Presence サービス ノードのセキュリティ ゾーンに追加します。Microsoft Explorer で、[Microsoft Internet Explorer] > [インターネット オプション（Internet Options）] > [セキュリティ（Security）] > [イントラネット（Local Internet）] > [サイト（Sites）] > [詳細設定（Advanced）] を選択し、セキュリティ ゾーンの Web アドレスの一覧に次のエントリを追加します。`https://*.`<使用しているドメイン>

5 ユーザにこの機能を使用する権限がないとのエラー メッセージが表示された場合、IM and Presence サービス ノードでユーザを Microsoft Lync で有効にしなければなりません。リモート通話コントロールの設定, （17 ページ）を参照してください。

6 信頼されていないセキュリティ証明書に関するエラー メッセージ、または同様の警告が表示される場合、[続行（Continue）] を選択します。多くのブラウザでは、Web サイトのセキュリティ証明書をダウンロードし、信頼済みに設定することができます。

E.164 形式の番号使用時の Lync のエラー

解決法 Lync Server のコントロール パネルでユーザを有効にする, （24 ページ）で示すように、[回線 URI（Line URI）] フィールドに tel: 値を追加する際、E.164 形式の番号を使用している場合は `phone-context=dialstring` を追加しないでください。例をあげると、[回線 URI（Line URI）] フィールドは “`tel:+19728131000`” と設定する必要があります。
“`tel:+19728131000;phone-context=dialstring.`” とは設定しないでください。

`phone-context=dialstring` が追加された場合、Lync クライアントではエラーが発生し、サインイン処理を開始するための最初の INVITE を Lync サーバに送信しません。

Cisco Unified Communications Manager へのユーザの同期

ユーザが AD でプロビジョニングされているのに Cisco Unified Communications Manager で表示されない場合、次の手順を実行し、ユーザを Cisco Unified Communications Manager に同期します。

手順

ステップ 1 [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（AD に一致する LDAP 設定名を選択します）。

ステップ 2 設定が正しいことを確認します。

ステップ 3 [完全同期を今すぐ実行する（Perform Full Sync Now）] を選択し、プロンプトが表示されたら [OK] を選択します。

ステップ 4 [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。
ユーザはユーザ リストには表示されません。

ユーザ ID での IM and Presence の有効化

Cisco Unified Communications Manager でユーザが設定されているものの、IM and Presence サービスで表示されない場合は、次の手順を実行します。

手順

ステップ 1 [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 ユーザを検索します。

ステップ 3 ユーザを選択します。

ステップ 4 [Unified CM IM and Presence でのユーザの有効化（Enable User for Unified CM IM and Presence）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] を選択します。

Lync クライアントでのユーザの通話コントロールが有効であることを確認する

ユーザには Lync クライアントでの通話コントロールがない場合、次の手順を実行する必要があります。

手順

ステップ 1 Lync クライアントにサインインします。

ステップ 2 ウィンドウの右上のドロップダウン矢印をクリックします。

ステップ 3 [ツール（Tools）] > [オプション（Options）] > [電話（Phones）] を選択します。

ステップ 4 [電話の統合（Phone Integration）] 領域で、[電話システムとの統合を有効にする（Enable integration with your phone system）] オプションを選択します。

ステップ 5 [詳細設定（Advanced）] を選択します。

ステップ 6 [自動設定（Automatic Configuration）] オプションが選択されていることを確認します。
このオプションを使用し、クライアントは Lync サーバ データベースからの正しい情報にアクセスできます。

ステップ 7 [OK] を選択します。
問題が解決しない場合は、ユーザが Cisco Unified Communications Manager と同期しており、IM and Presence サービス ノードでユーザに対して RCC が有効になっていることを確認します。

関連トピック

ユーザの機能の割り当て，（19 ページ）

Microsoft Lync クライアントのステータス バーの、赤い X のついた電話のアイコン

解決法 ユーザが Microsoft Lync クライアントにサインインし、ウィンドウ下部のステータス バーに「通話転送設定済み（Call forwarding is“ ”on）」または「通話転送未設定（Call forwarding is“ ”off）」というテキストが表示される場合、統合設定は正常に行われています。ステータス バーに赤い X のついた電話のアイコンが表示される場合、統合が失敗しています。サインインの問題を解決するには、Lync サーバのトレースを開始して、IM and Presence サーバと Microsoft Lync サーバとの間の INVITE/INFO SIP メッセージ交換シーケンスの問題を特定します。Microsoft Lync のサーバのログと Microsoft Lync クライアントのログの詳細については、Microsoft Lync のドキュメントを参照してください。

関連トピック

詳細情報, （2 ページ）

Microsoft Lync クライアントのステータス バーの、赤い **X** のついた電話のアイコン