



Cisco Unified Presence 導入ガイド

Release 6.0(1)

【注意】この文書はお客様の便宜のために作成された参考和訳であり、お客様とシスコシステムズとの間の契約を構成するものではありません。正式な契約条件は、弊社担当者、または弊社販売パートナーにご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。見当たらない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB (University of California, Berkeley) パブリック ドメイン パーミッションとして、UCB が開発したプログラムを最適化したものです。All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、すべてのマニュアルおよび上記各社のソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記各社は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取り引きによって発生する、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコまたは代理店に知らされていても、それらに対する責任を一切負いかねます。

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. 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. (0705R)

このドキュメントで使用しているインターネット プロトコル (IP) アドレスは、実在のアドレスではありません。ドキュメント中で示される例、コマンドの画面出力、および図は、いずれも視覚的な説明のみを目的としています。実在する IP アドレスが例示されていた場合、それらは意図して使用したものではありません。

Cisco Unified Presence 導入ガイド
Copyright © 2007 Cisco Systems, Inc.
All rights reserved.



CONTENTS

このマニュアルについて	vii
目的	vii
対象読者	viii
マニュアルの構成	viii
関連資料	viii
表記法	ix
技術情報の入手方法、サポートの利用方法、およびセキュリティ ガイドライン	x
シスコ製品のセキュリティの概要	x

CHAPTER 1

概要	1-1
Microsoft 製品との統合	1-2
関連資料	1-4

CHAPTER 2

Cisco Unified Communications Manager の設定の概要	2-1
サービス パラメータの設定	2-2
アプリケーション サーバとしての Cisco Unified Presence の設定	2-2
エンド ユーザへの機能の割り当て	2-3
各電話機のプライマリ内線の関連付け	2-4
ユーザへのデバイスの関連付け	2-5
IP Phone Messenger の設定およびアプリケーション ユーザとしての PhoneMessenger の追加	2-6
ユーザ グループへのエンド ユーザの割り当て	2-7
Cisco IP PhoneMessenger の IP Phone サービスの設定	2-8
Cisco IP PhoneMessenger サービスへの電話機の登録	2-9
SIP トランク セキュリティ プロファイルの設定	2-10
標準 AXL アクセス権限が有効になっているアプリケーション ユーザの追加	2-11
各 Cisco Unified Presence サーバの SIP トランクの設定	2-13
必要なサービスが実行されていることの確認	2-14
エンド ユーザとライン アピアランスの関連付け	2-15
CTI ゲートウェイの設定チェックリスト	2-16

CHAPTER 3

Cisco Unified Presence の設定の概要	3-1
ライセンス ファイルのアップロード	3-2
オプションのセカンダリ Cisco Unified Presence ノードの追加	3-3
Cisco IP Phone Messenger の設定	3-4
MOC 機能の割り当て	3-4
プレゼンス ゲートウェイの設定	3-5
着信アクセス コントロール リストの設定	3-6
プライバシー アクセス コントロール リストの設定	3-7
プロキシ サーバの設定	3-7
サービスの有効化	3-8

CHAPTER 4

Microsoft 製品との統合の概要	4-1
Microsoft Office Live Communications Server 2005 (SP 1) の設定	4-2
Microsoft LCS の設定の概要	4-2
Microsoft Active Directory の設定の概要	4-3
Exchange 予定表との統合の設定	4-5
Exchange Server での Receive As アカウントの作成	4-5
新しいアカウントの作成	4-5
ユーザ アカウントの作成	4-6
アカウントへの Exchange 参照のみ可としての制御の委任	4-6
アカウントへの Receive As 権限の追加	4-7
Cisco Unified Presence サーバでのプレゼンス ゲートウェイの設定	4-8
Cisco Unified Presence サーバでのセキュリティ証明書の設定	4-9
CA サービスのインストール	4-10
ルート証明書のダウンロード	4-10
Cisco Unified Presence サーバへのルート証明書のアップロード	4-11
IIS での CSR の生成	4-12
CSR への署名	4-13
署名済み証明書のダウンロード	4-14
IIS での署名済み証明書のアップロード	4-14
TLS ルートの設定チェックリスト	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	4-17
Microsoft Office Communicator 2005 の設定チェックリスト	4-18

CHAPTER 5

IBM Lotus Sametime 用 Cisco Click-to Call プラグインの設定の概要	5-1
前提条件	5-1
Cisco Click-to-Call プラグインのインストール	5-2
Cisco Click-to-Call プラグインの設定	5-3
Cisco Click-to-Call 用の Lotus Sametime Server の設定	5-6

Cisco Click-to-Call 用の Cisco Unified Communications Manager の設定	5-7
SIP トランク セキュリティ プロファイルの設定	5-7
Lotus Sametime Server 用の SIP トランクの設定	5-7
SIP トランクでのダイジェスト認証の設定	5-8
ユーザ名とパスワードの設定	5-9



このマニュアルについて

ここでは、『Cisco Unified Presence 導入ガイド』の概要について説明します。



(注)

このマニュアルは、ご利用可能な最新のシスコ製品情報を示していない場合があります。次の URL に記述されている、シスコ製品の英文マニュアルのページにアクセスすることにより、最新資料を入手できます。

<http://www.cisco.com/univercd/home/home.htm>

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

<http://www.cisco.com/jp>

この章は、次の内容で構成されています。

- 目的 (P. vii)
- 対象読者 (P. viii)
- マニュアルの構成 (P. viii)
- 表記法 (P. ix)
- 技術情報の入手方法、サポートの利用方法、およびセキュリティ ガイドライン (P. x)

目的

このマニュアルでは、Cisco Unified Presence 6.0(1) を設定し、Cisco Unified Communications Manager 6.0(1) および必要な Microsoft サーバや製品と統合するための設定チェックリストおよび手順について説明します。次の Microsoft サーバおよび製品が含まれます。

- Microsoft Office Live Communications Server 2005 Service Pack 1 (SP1)
- Microsoft Windows Server 2000 または 2003 Active Directory
- Microsoft Exchange Server 2003
- Microsoft Office Communicator 2005

また、このマニュアルは Cisco plug-in for IBM Lotus Sametime 7.5 のインストールおよび設定の手順について説明しています。

対象読者

『Cisco Unified Presence 導入ガイド』は Cisco Unified Presence および Cisco Unified Communications Manager の管理を担当するネットワーク管理者に情報を提供します。Microsoft および IBM の製品に関するさまざまな知識とともに、テレフォニーおよび IP ネットワーキングテクノロジーに関する知識が必要です。

マニュアルの構成

次の表は、このマニュアルの構成を示しています。

章番号	説明
第 1 章「概要」	Cisco Unified Presence の導入の概要を紹介しています。
第 2 章「Cisco Unified Communications Manager の設定の概要」	Cisco Unified Presence を導入するときに実行しなければならない Cisco Unified Communications Manager の設定タスクの概要を紹介しています。
第 3 章「Cisco Unified Presence の設定の概要」	Cisco Unified Presence Server 上で実行しなければならない設定タスクの概要を紹介しています。
第 4 章「Microsoft 製品との統合の概要」	Microsoft の環境における Cisco Unified Presence の導入の概要を紹介しています。
第 5 章「IBM Lotus Sametime 用 Cisco Click-to-Call プラグインの設定の概要」	Cisco Click-to-Call plug-in for Lotus SameTime のインストールおよび設定の手順を紹介しています。

関連資料

Cisco Unified Communications Manager の関連マニュアルについては、次の URL から『Documentation Guide for Cisco Unified Presence Release 6.0 (1)』を参照してください。

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

表記法

このマニュアルは、次の表記法を使用しています。

表記法	説明
太字	コマンドおよびキーワードは、 太字 で示しています。
イタリック体	ユーザが値を指定する引数は、 <i>イタリック体</i> で示しています。
[]	角カッコの中の要素は、省略可能です。
{ x y z }	必ずどれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x y z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
ストリング	引用符を付けない一組の文字。ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。
screen フォント	システムが表示する端末セッションおよび情報は、 <code>screen</code> フォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、 太字の screen フォントで示しています。
イタリック体の screen フォント	ユーザが値を指定する引数は、 <i>イタリック体の screen</i> フォントで示しています。
→	例の中で重要なテキストを強調しています。
^	^ 記号は、Ctrl キーを表します。たとえば、画面に表示される ^D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。

(注) は、次のように表しています。



(注) 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ワンポイント アドバイスは、次のように表しています。



ワンポイント・アドバイス

時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。

ヒントは、次のように表しています。



ヒント

便利なヒントです。

注意は、次のように表しています。

**注意**

「**要注意**」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告は、次のように表しています。

**警告**

「**危険**」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策をとるよう努めてください。

技術情報の入手方法、サポートの利用方法、およびセキュリティ ガイドライン

技術情報の入手、サポートの利用、技術情報に関するフィードバックの提供、セキュリティ ガイドライン、推奨するエイリアスおよび一般的なシスコのマニュアルに関する情報は、月刊の『*What's New in Cisco Product Documentation*』を参照してください。ここでは、新規および改訂版のシスコの技術マニュアルもすべて記載されています。次の URL からアクセスできます。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

シスコ製品のセキュリティの概要

本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国での法律を順守するものとします。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意する必要があります。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

シスコの暗号化製品に適用される米国の法律の概要については、次の URL で参照できます。

<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

何かご不明な点があれば、export@cisco.com まで電子メールを送信してください。



概要

このマニュアルでは、Cisco Unified Presence を導入して設定するプロセスの概要について説明します。次の主な設定要件について説明します。

- Cisco Unified Communications Manager の設定。
- Cisco Unified Presence の設定 (CTI ゲートウェイを含む)。
- Microsoft 製品との統合。次の Microsoft 製品の設定チェックリストが含まれます。
 - Microsoft Office Live Communications Server (LCS)
 - Microsoft Active Directory (AD)
 - Microsoft Office Communicator (MOC)

Microsoft 製品との統合

CTI ゲートウェイである Cisco Unified Presence アプリケーション モジュールを使用すると、Microsoft Office Communicator と Cisco Unified Communications Manager が連携し、Click to Dial や Phone Control サービスなどの Microsoft Office Communicator 機能がサポートされます。Microsoft Live Communications Server では、Cisco Unified Communications Manager と連携するように、Computer Supported Telecommunications Applications (CSTA) XML インターフェイスを使用します。

図 1-1 は、Microsoft プレゼンス システム アーキテクチャの全体図を示しています。

図 1-1 Microsoft プレゼンス アーキテクチャの全体図

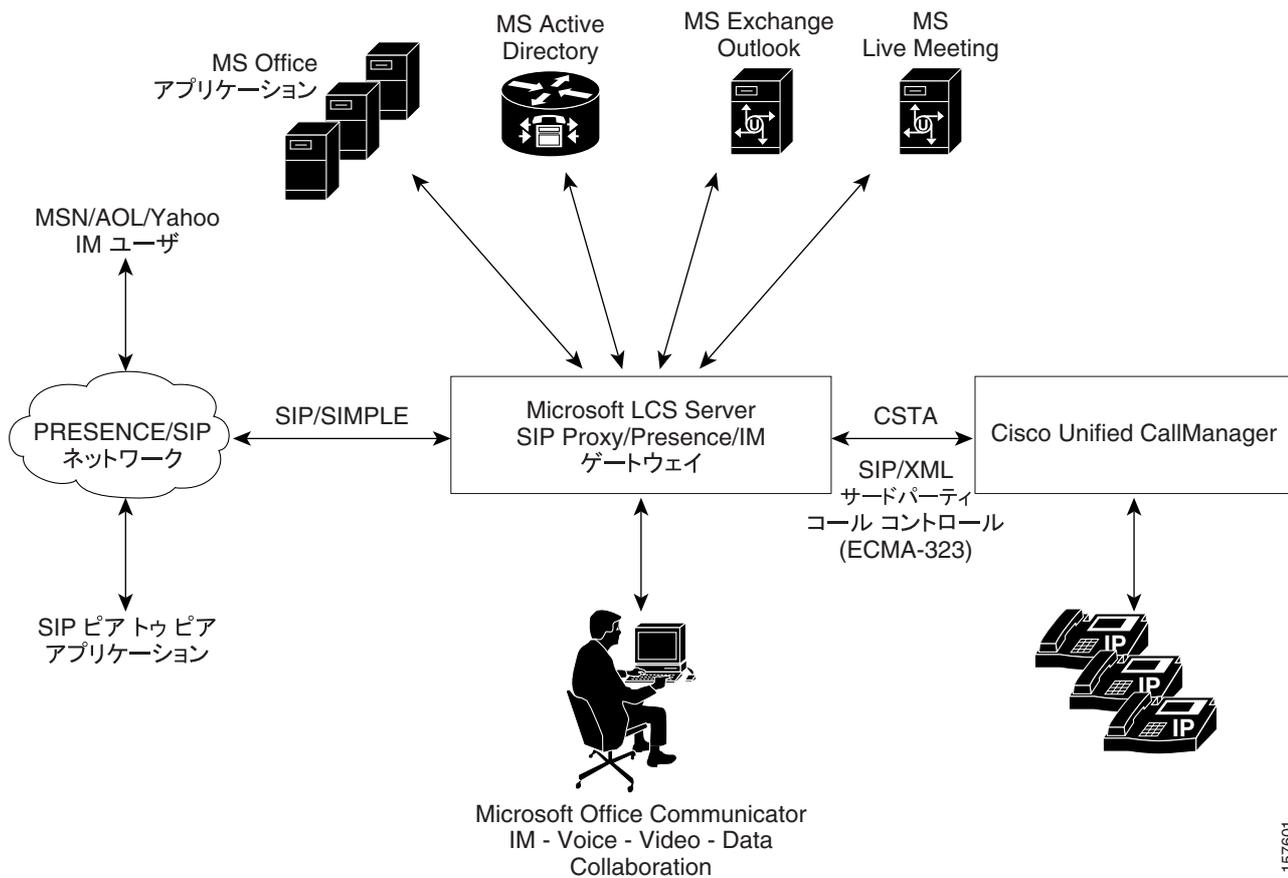


図 1-2 は、ソフトクライアント (Microsoft Office Communicator) と CTI ゲートウェイの間のメッセージフローを示しています。

図 1-2 ソフトクライアントと CTI ゲートウェイの間のメッセージフロー

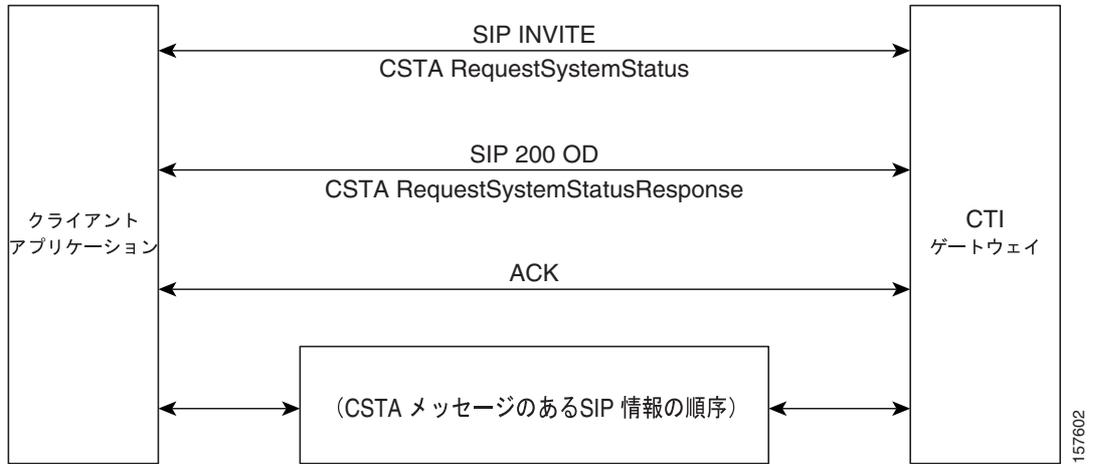
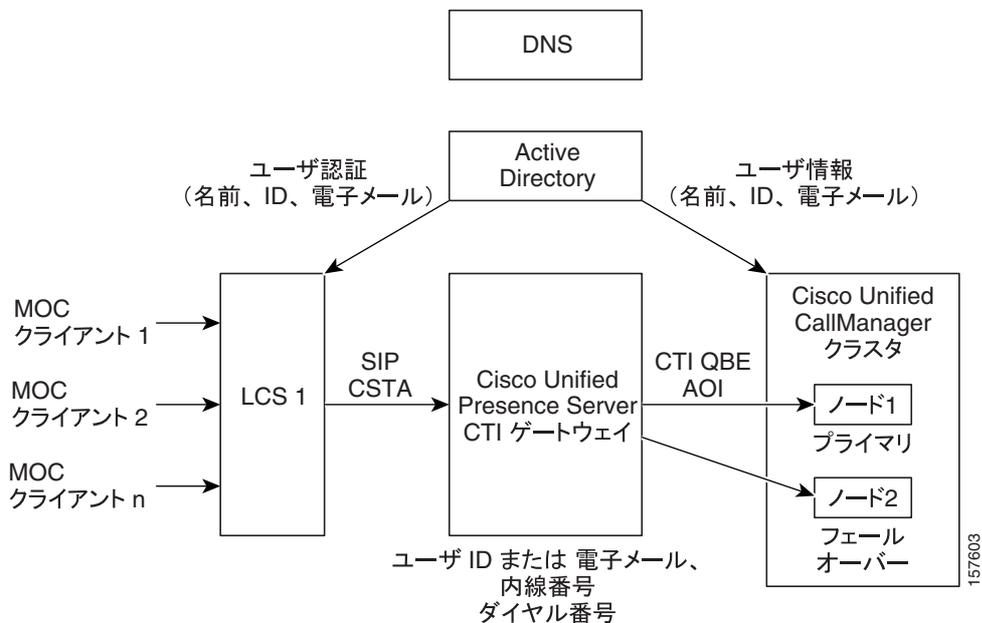


図 1-3 は、Microsoft Office Communicator と Cisco Unified Communications Manager Phone の統合が連携するように設定するシステム コンポーネントを示しています。

図 1-3 Microsoft Office Communicator と Cisco Unified Communications Manager Phone の統合



この導入ガイドは、サーバに Cisco Unified Presence ソフトウェアがすでにインストールされていることを前提としています。インストールの手順については、『Cisco Unified Presence インストレーションガイド』を参照してください。

関連資料

関連する Cisco IP テレフォニー アプリケーションおよび製品の詳細については、次のマニュアルを参照してください。

- *Cisco Unified Presence インストールガイド*
パブリッシャ データベースおよびサブスクリバ サーバに Cisco Unified Presence をインストールする手順が記載されています。
- *Cisco Unified Presence アドミニストレーションガイド*
Cisco Unified Presence Voice over IP ネットワークの設定、保守、および管理について、順を追って説明しています。
- *Cisco Unified Serviceability アドミニストレーションガイド for Cisco Unified Presence*
このマニュアルは、Cisco Unified Presence のサービスアビリティおよびリモート サービスアビリティのアラーム設定、トレース設定、およびその他のレポートの設定について順を追って説明しています。
- *Cisco Unified Communications Operating System アドミニストレーションガイド for Cisco Unified Presence*
Cisco Unified Communications Platform のグラフィカル ユーザ インターフェイス (GUI) および コマンドライン インターフェイス (CLI) を使用して、一般的なシステム関連タスクやネットワーク関連タスクを実行する手順が記載されています。
- *Disaster Recovery System ガイド for Cisco Unified Presence*
障害復旧システムの概要、およびバックアップと復元に関連したさまざまなタスクを実行する手順が記載されています。



Cisco Unified Communications Manager の設定の概要

この章では、Cisco Unified Communications Manager 6.0(1) の設定タスクについて説明します。これらの手順を、[Cisco Unified Communications Manager の管理] ウィンドウから実行します。

この章は、次の内容で構成されています。

- サービスパラメータの設定 (P.2-2)
- アプリケーションサーバとしての Cisco Unified Presence の設定 (P.2-2)
- エンドユーザへの機能の割り当て (P.2-3)
- 各電話機のプライマリ内線の関連付け (P.2-4)
- ユーザへのデバイスの関連付け (P.2-5)
- IP Phone Messenger の設定およびアプリケーションユーザとしての PhoneMessenger の追加 (P.2-6)
- ユーザグループへのエンドユーザの割り当て (P.2-7)
- Cisco IP PhoneMessenger の IP Phone サービスの設定 (P.2-8)
- Cisco IP PhoneMessenger サービスへの電話機の登録 (P.2-9)
- SIP トランクセキュリティプロファイルの設定 (P.2-10)
- 標準 AXL アクセス権限が有効になっているアプリケーションユーザの追加 (P.2-11)
- 各 Cisco Unified Presence サーバの SIP トランクの設定 (P.2-13)
- 必要なサービスが実行されていることの確認 (P.2-14)
- エンドユーザとラインアピアランスの関連付け (P.2-15)
- CTI ゲートウェイの設定チェックリスト (P.2-16)

サービスパラメータの設定

手順

-
- ステップ 1** [システム]>[サービスパラメータ]を選択します。
- ステップ 2** [サービスパラメータ設定 (Service Parameter Configuration)] ウィンドウで、ドロップダウン リストから Cisco Unified Communications Manager Server を選択します。
- ステップ 3** [サービス (Service)] から [Cisco Communications Manager] を選択します。
- ステップ 4** [Clusterwide Parameters (System - Presence)] セクションの [Default Inter-Presence Group Subscription] で、[Allow Subscription] を選択します。
- ステップ 5** [保存] をクリックします。



(注) 詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』の「サービスパラメータの設定」の章を参照してください。

アプリケーションサーバとしての Cisco Unified Presence の設定

手順

-
- ステップ 1** [システム]>[アプリケーションサーバ]を選択します。
- ステップ 2** [アプリケーションサーバの検索と一覧表示 (Find and List Application Servers)] ウィンドウで、[新規追加] をクリックします。
- [アプリケーションサーバの設定 (Application Server Configuration)] ウィンドウが表示されます。
- ステップ 3** [アプリケーションサーバタイプ (Application Server Type)] から [Cisco Unified Presence] を選択し、[次へ] をクリックします。
- ステップ 4** [名前] フィールドに、Cisco Unified Presence のホスト名を入力します。
- ステップ 5** [保存] をクリックします。



(注) 詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』の「アプリケーションサーバの設定」の章を参照してください。

エンドユーザへの機能の割り当て

手順

ステップ 1 [システム]>[ライセンス]>[機能割り当て]を選択します。

[機能割り当ての検索と一覧表示 (Find and List Capabilities Assignments)] ウィンドウが表示されます。

ステップ 2 すべてのユーザのリストを表示するには、[検索]をクリックします。

ステップ 3 [検索結果]セクションでユーザリンクをクリックし、[機能割り当ての設定 (Capabilities Assignment Configuration)] ウィンドウを表示します。



ヒント 複数のユーザに機能を割り当てる場合は、複数のユーザのチェックボックスをオンにして [一括割り当て] をクリックします。

ステップ 4 ウィンドウが表示されたら、[CUP (Cisco Unified Presence) を有効にする] チェックボックスをオンにします。

ステップ 5 [CUPC (Cisco Unified Personal Communicator) を有効にする] チェックボックスをオンにして、CUPC を利用可能に設定します。

ステップ 6 [保存] をクリックします。



(注) Cisco Unified Personal Communicator の詳細については、『Cisco Unified Personal Communicator インストールガイド』を参照してください。

各電話機のプライマリ内線の関連付け

手順

ステップ 1 [デバイス] > [電話] を選択します。

ステップ 2 [電話の検索と一覧表示 (Find and List Phones)] ウィンドウで、[新規追加] をクリックして新規電話デバイスを追加します。

[新規電話を追加 (Add a New Phone)] ウィンドウが表示されます。

ステップ 3 [電話のタイプ (Phone Type)]: ドロップダウン リストからデバイスを選択し、[次へ] をクリックします。

ステップ 4 [デバイスプロトコルの選択 (Select the device protocol)]: ドロップダウン リストからプロトコルを選択し、[次へ] をクリックします。

[電話の設定 (Phone Configuration)] ウィンドウで、次のフィールドに項目を入力するか選択します。

- [MAC アドレス (MAC Address)]: 電話機の MAC アドレスを入力します。
- [デバイスプール (Device Pool)]: [**Default**] を選択します。
- [電話ボタンテンプレート (Phone Button Template)]: **デフォルト** を選択します。
- [SCCP 電話セキュリティプロファイル (SCCP Phone Security Profile)] (または [SIP 電話セキュリティプロファイル (SIP Phone Security Profile)]): [**Standard SCCP Profile for Auto Registration**] (または [**Standard SIP Profile for Auto Registration**]) を選択します。

ステップ 5 [保存] をクリックします。

ステップ 6 左側の [割り当て情報 (Association Information)] セクションで、[新規 DN を追加] リンクをクリックします。

ステップ 7 [電話番号の設定 (Directory Number Configuration)] ウィンドウに、各電話機の電話番号を入力します。

ステップ 8 [保存] をクリックします。



(注) 詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』の「Cisco Unified IP Phone の設定」の章を参照してください。

ユーザへのデバイスの関連付け

手順

-
- ステップ 1** [ユーザ管理]>[エンドユーザ]を選択します。
 - ステップ 2** [ユーザの検索と一覧表示 (Find and List Users)] ウィンドウで、ユーザがすでにデータベースに格納されている場合はユーザを検索し、新規ユーザを追加する場合は[新規追加]をクリックします。
 - ステップ 3** [エンドユーザの設定 (End User Configuration)] ウィンドウで、必須フィールド (アスタリスク付き) に情報を入力します。PIN が数値であることを確認します。
 - ステップ 4** ウィンドウの下部にある [プライマリ内線 (Primary Extension)] で、各ユーザの内線を選択します。
 - ステップ 5** [保存] をクリックします。
 - ステップ 6** ウィンドウが再表示されたら、[デバイスの割り当て] をクリックします。
 - ステップ 7** [ユーザデバイス割り当て (User Device Association)] ウィンドウで、関連付けるデバイスを選択して [選択 / 変更の保存] をクリックします。
 - ステップ 8** [エンドユーザの設定 (End User Configuration)] ウィンドウに戻り ([ユーザ管理]>[エンドユーザ] を選択)、[デバイスの割り当て (Device Associations)] セクションで、デバイスがユーザに関連付けられていることを確認します。



(注) 詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』の「エンドユーザの設定」の章を参照してください。

IP Phone Messenger の設定およびアプリケーション ユーザとしての PhoneMessenger の追加



(注) Microsoft Office Communicator だけを使用している場合は、この手順を実行する必要はありません。

手順

ステップ 1 [ユーザ管理] > [アプリケーションユーザ] を選択します。

ステップ 2 [アプリケーションユーザの検索と一覧表示 (Find and List Application Users)] ウィンドウで、[新規追加] をクリックします。

ステップ 3 [アプリケーションユーザの設定 (Application User Configuration)] ウィンドウで、**PhoneMessenger** のユーザ ID を使用して新規ユーザを追加します。

ステップ 4 [パスワード (Password)] および [パスワードの確認 (Confirm Password)] フィールドに、このユーザのパスワードを入力します。



(注) Cisco Unified Presence の設定で使用するため、このパスワードを記憶しておいてください。

ステップ 5 [デバイス情報 (Device Information)] の [使用可能なデバイス (Available Devices)] セクションで、Cisco IP Phone Messenger に加入するすべてのデバイスを選択し、下矢印をクリックしてそれらのデバイスを [制御するデバイス (Controlled Devices)] セクションまで移動します。

ステップ 6 [保存] をクリックします。



(注) 詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』の「アプリケーション ユーザの設定」の章を参照してください。

ユーザグループへのエンドユーザの割り当て

手順

ステップ 1 [ユーザ管理]>[ユーザグループ]を選択します。

ステップ 2 すべてのユーザグループを表示するには、[検索]をクリックします。

ステップ 3 [Standard CCM End Users] リンクをクリックします。

[ユーザグループの設定 (User Group Configuration)] ウィンドウが表示されます。

ステップ 4 [グループにエンドユーザを追加]をクリックし、ウィンドウが再表示されたら、すべての Cisco Unified Presence ユーザをこのグループに追加します。

ステップ 5 [関連リンク]メニューから [検索/リストに戻る]を選択し、[移動]を選択します。

ステップ 6 [Standard CTI Enabled] リンクをクリックします。

[ユーザグループの設定 (User Group Configuration)] ウィンドウが表示されます。

ステップ 7 [グループにエンドユーザを追加]をクリックし、ウィンドウが再表示されたら、すべての Cisco Unified Presence ユーザをこのグループに追加します。



(注) 詳細については、『Cisco Unified Communications Manager アドミニストレーションガイド』の「ユーザグループの設定」の章を参照してください。

Cisco IP PhoneMessenger の IP Phone サービスの設定



(注) Microsoft Office Communicator だけを使用している場合は、この手順を実行する必要はありません。

手順

ステップ 1 [デバイス]>[デバイスの設定]>[IP Phone サービス]を選択します。

ステップ 2 [IP Phone サービスの検索と一覧表示 (Find and List IP Phone Services)] ウィンドウで、[新規追加] をクリックします。

[IP Phone サービスの設定 (IP Phone Services Configuration)] ウィンドウが表示されます。

ステップ 3 [サービス名 (Service Name)] フィールドに、**PhoneMessenger** を入力します。

ステップ 4 [サービスの説明] フィールドに、**IP Phone Messenger** を入力します。

ステップ 5 [サービス URL (Service URL)] フィールドに、次の URL を入力します。

`http://my-cups:8081/ippm/default?name=#DEVICENAME#`

電話機で DNS が無効な場合、*my-cups* には Cisco Unified Presence の IP アドレスを指定します。

ステップ 6 [保存] をクリックします。



(注) 詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』の「Cisco Unified IP Phone サービスの設定」の章を参照してください。

Cisco IP PhoneMessenger サービスへの電話機の登録



(注) クライアントとして Microsoft Office Communicator だけを使用している場合は、この手順を実行する必要はありません。

手順

ステップ 1 [デバイス]>[電話]を選択します。

[電話の検索と一覧表示 (Find and List Phones)] ウィンドウが表示されます。

ステップ 2 デバイス リストを表示するには、[検索]をクリックします。ウィンドウが再表示されたら、電話デバイス リンクをクリックして、[電話の設定 (Phone Configuration)] ウィンドウにアクセスします。

ステップ 3 右上の [関連リンク] ナビゲーションボックスで、ドロップダウン リストから [サービスの登録 / 登録解除] を選択し、[移動] をクリックします。

ステップ 4 [登録済みの Cisco IP Phone サービス (Subscribed Cisco IP Phone Services for)] ウィンドウが表示されたら、[サービスの選択 (Select a Service)] ドロップダウン リストから [PhoneMessenger] (前回設定済み) を選択し、[次へ] をクリックします。

ステップ 5 ウィンドウが再表示されたら、[登録] をクリックします。

ステップ 6 ウィンドウが再表示されたら、[保存] をクリックします。

ステップ 7 電話機を個別に再設定するか、グループとして再設定します。



(注) 詳細については、『Cisco Unified Communications Manager アドミニストレーションガイド』の「Cisco Unified IP Phone の設定」の章を参照してください。

SIP トランク セキュリティ プロファイルの設定



(注) クライアントとして Microsoft Office Communicator だけを使用している場合は、IPPM および Cisco Unified Personal Communicator を設定するためのこの手順を実行する必要はありません。

手順

ステップ 1 [システム] > [セキュリティプロファイル] > [SIP トランクセキュリティプロファイル] を選択します。

[SIP トランクセキュリティプロファイルの検索と一覧表示 (Find and List SIP Trunk Security Profiles)] ウィンドウが表示されます。

ステップ 2 使用可能なプロファイルのリストを表示するには、[検索] をクリックします。

ステップ 3 検索結果で、[Non Secure SIP Trunk Profile] リンクをクリックします。

[SIP トランクセキュリティプロファイルの設定 (SIP Trunk Security Profile Configuration)] ウィンドウが表示されます。

ステップ 4 [デバイスセキュリティモード (Device Security Mode)] が [非セキュア] に設定されていることを確認します。

ステップ 5 [着信転送タイプ (Incoming Transport Type)] が [TCP+UDP] に設定されていることを確認します。

ステップ 6 [発信転送タイプ (Outgoing Transport Type)] が [TCP] に設定されていることを確認します。

ステップ 7 次の項目をオンにして有効にします。

- プレゼンス登録の許可 (Accept Presence Subscription)
- アウトオブダイアログ REFER の許可 (Accept Out-of-Dialog REFER)
- 未承諾 NOTIFY の許可 (Accept Unsolicited Notification)
- REPLACE ヘッダの許可 (Accept Replaces Header)

ステップ 8 [保存] をクリックします。



(注) 詳細については、『Cisco Unified Communications Manager アドミニストレーションガイド』の「SIP トランク セキュリティ プロファイルの設定」の章を参照してください。

標準 AXL アクセス権限が有効になっているアプリケーション ユーザの追加



(注) この手順はオプションです。Cisco Unified Presence のインストール中に、AXL API アクセスが有効になっているアプリケーション ユーザの AXL ユーザ ID および AXL ユーザ パスワードを入力する必要があります。

Standard AXL API Access 権限がデフォルトで有効になっている CCMAdministrator アプリケーション ユーザを使用するか、この手順に従って新規アプリケーション ユーザを作成できます。

新しいアプリケーション ユーザを作成する

ステップ 1 [ユーザ管理] > [アプリケーションユーザ] を選択します。

[アプリケーションユーザの検索と一覧表示 (Find and List Application Users)] 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。

[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウが表示されます。

ステップ 3 [ユーザ ID] フィールドに、AXLuserCUPS のように新しいアプリケーション ユーザ名を入力します。

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 使用可能なデバイスのリストから、制御対象のデバイスを選択します。

ステップ 6 [保存] をクリックします。

新規ユーザグループを作成し、アプリケーション ユーザを追加する

ステップ 7 [ユーザ管理] > [ユーザグループ] を選択します。

[ユーザグループの検索と一覧表示 (Find and List User Groups)] ウィンドウが表示されます。

ステップ 8 [新規追加] をクリックします。

ステップ 9 新規ユーザグループの名前を、group_AXLaccess のように入力し、[保存] をクリックします。

ステップ 10 [グループにアプリケーションユーザを追加] をクリックします。

ステップ 11 作成した新しいアプリケーション ユーザ名を選択し、[選択項目の追加] をクリックします。

ステップ 12 [関連リンク] ドロップダウン メニューから [ユーザグループに権限を割り当て] を選択し、[移動] を選択します。

[ユーザグループの設定 (User Group Configuration)] ウィンドウが表示されます。

ステップ 13 [Standard AXL API Access] を選択し、[選択項目の追加] をクリックします。

ステップ 14 [保存] をクリックします。

詳細については、『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の次の章を参照してください。

- アプリケーション ユーザの設定
- ユーザ グループの設定



(注) Cisco Unified Presence のインストールの詳細については、『*Installing Cisco Unified Presence, Release 1.0(2)*』を参照してください。

各 Cisco Unified Presence サーバの SIP トランクの設定



(注) IPPM および Cisco Unified Personal Communicator を設定するには、この Cisco Unified Communications Manager に関連付けられている Cisco Unified Presence Server ごとに、1 つの SIP トランクをプロビジョニングします。クライアントとして Microsoft Office Communicator だけを使用している場合は、この手順を実行する必要はありません。

ステップ 1 [デバイス] > [トランク] を選択します。

[トランクの検索と一覧表示 (Find and List Trunks)] 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。

[トランクの設定 (Trunk Configuration)] ウィンドウが表示されます。

ステップ 3 [トランクタイプ (Trunk Type)] : [SIP Trunk] を選択します。

ステップ 4 [デバイスプロトコル (Device Protocol)] : [SIP] を選択します。

ステップ 5 [次へ] をクリックします。

ステップ 6 [デバイス名 (Device Name)] : CUPS-SIP-Trunk を入力します。

ステップ 7 [デバイスプール (Device Pool)] : [Default] を選択します。

ステップ 8 [接続先ポート (Destination Port)] : 5070 と入力します。

ステップ 9 ウィンドウの下部にある [SIP 情報 (SIP Information)] セクションで、[着信先アドレス] フィールドに次のように入力します。

my-cups.sip.com

ここで、*my-cups* には、Cisco Unified Presence の完全修飾ドメイン名を指定します。

ステップ 10 [SIP トランクセキュリティプロファイル (SIP Trunk Security Profile)] : [Non Secure SIP Trunk Profile] を選択します。

ステップ 11 [SIP プロファイル (SIP Profile)] : [Standard SIP Profile] を選択します。

ステップ 12 [保存] をクリックします。



(注) 詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』の「トランクの設定」の章を参照してください。

必要なサービスが実行されていることの確認

手順

ステップ 1 [ナビゲーション]メニューから [Cisco Unified サービスアビリティ] を選択し、[移動] を選択します。

[Cisco Unified Serviceability] ウィンドウが表示されます。

ステップ 2 [Tools] > [Control Center - Feature Services] を選択します。

ステップ 3 [Control Center - Feature Services] ウィンドウで、サーバの場合は、ドロップダウン リストから Cisco Unified Communications Manager Server を選択します。

ステップ 4 [Control Center - Feature Services] ウィンドウが再表示されたら、次のサービスが実行されていることを確認します。

- Cisco Communications Manager
- Cisco TFTP
- Cisco Extension Mobility
- Cisco Communications Manager Cisco IP Phone Services
- Cisco AXL Web Service



(注) 詳細については、『Cisco Unified Serviceability アドミニストレーション ガイド for Cisco Unified Presence』の「サービスの管理」の章を参照してください。

エンドユーザとライン アピアランスの関連付け



(注) Bulk Administration を使用して、ユーザをライン アピアランスにマップすることもできます。詳細については、『Cisco Unified Communications Manager Bulk Administration ガイド』を参照してください。

手順

- ステップ 1** [Cisco Unified Communications Manager の管理] ウィンドウで、[デバイス] > [電話] を選択します。
[電話の検索と一覧表示 (Find and List Phones)] ウィンドウが表示されます。
- ステップ 2** 特定の電話機を検索するか、[検索] をクリックしてすべてのデバイスを表示します。
- ステップ 3** 設定する電話機のデバイス名をクリックします。
[電話の設定 (Phone Configuration) (Phone Configuration)] ウィンドウが表示されます。
- ステップ 4** [割り当て情報 (Association Information)] ペインで、関連付ける電話番号をクリックします。
[電話番号の設定 (Directory Number Configuration)] が表示されます。
- ステップ 5** ウィンドウの下部で、[エンドユーザの関連付け] をクリックします。
- ステップ 6** 表示されるポップアップ ウィンドウで、ライン アピアランスに関連付けるユーザを選択します。
- ステップ 7** [選択項目の追加] をクリックします。
- ステップ 8** [保存] をクリックします。

CTI ゲートウェイの設定チェックリスト

表 2-1 は、CTI ゲートウェイに必要な設定タスクを示しています。これらのタスクを、Cisco Unified Communications Manager の管理ページおよび Cisco Unified Presence の管理ページから実行します。

表 2-1 CTI ゲートウェイ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>[Cisco Unified Communications Manager の管理] ウィンドウから、アプリケーション ユーザを追加します。</p> <p>a. [ユーザ管理] > [アプリケーションユーザ] を選択します。 [アプリケーションユーザの検索と一覧表示 (Find and List Application Users)] ウィンドウが表示されます。</p> <p>b. [新規追加] をクリックします。 [アプリケーションユーザの設定 (Application User Configuration)] ウィンドウが表示されます。</p> <p>c. [ユーザ ID (User ID)] フィールドに、CtiGW のように、任意のアプリケーション ユーザ名を入力します。</p> <p>d. 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。</p> <p>e. [保存] をクリックします。</p>	<p>詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』の「アプリケーション ユーザ」の章を参照してください。</p>
ステップ 2	<p>アプリケーション ユーザを、Standard CTI Enabled ユーザ グループに追加します。</p> <p>a. [ユーザ管理] > [ユーザグループ] を選択します。 [ユーザグループの検索と一覧表示 (Find and List User Groups)] ウィンドウが表示されます。</p> <p>b. [検索] をクリックします。</p> <p>c. [Standard CTI Enabled] リンクをクリックします。 [ユーザグループの設定 (User Group Configuration)] ウィンドウが表示されます。</p> <p>d. [グループにアプリケーションユーザを追加] をクリックします。</p> <p>e. 作成したアプリケーション ユーザを選択し、[選択項目の追加] をクリックします。</p>	<p>詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』の「アプリケーション ユーザ」の章を参照してください。</p>

表 2-1 CTI ゲートウェイの設定チェックリスト (続き)

	設定手順	関連マニュアル
ステップ 3	<p>アプリケーション ユーザを、Standard CTI Allow Control of All Devices ユーザグループに追加します。</p> <ol style="list-style-type: none"> [ユーザ管理] > [ユーザグループ] を選択します。 [ユーザグループの検索と一覧表示 (Find and List User Groups)] ウィンドウが表示されます。 [検索] をクリックします。 [Standard CTI Allow Control of All Devices] リンクをクリックします。 [ユーザグループの設定 (User Group Configuration)] ウィンドウが表示されます。 [グループにアプリケーションユーザを追加] をクリックします。 作成したアプリケーション ユーザを選択し、[選択項目の追加] をクリックします。 [保存] をクリックします。 	<p>詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』の「アプリケーション ユーザ」の章を参照してください。</p>
ステップ 4	<p>Cisco Unified Presence の管理ページで、CTI ゲートウェイを設定します。</p> <ol style="list-style-type: none"> [アプリケーション] > [CTI ゲートウェイ] > [設定] を選択します。 [CTI ゲートウェイ設定 (CTI Gateway Settings)] ウィンドウが表示されます。 [アプリケーションのステータス (Application Status)] ドロップダウンメニューから [オン] を選択し、CTI ゲートウェイを有効にします。 <p> (注) CTI ゲートウェイを有効にします。デフォルトでは、[アプリケーションのステータス (Application Status)] は [オフ] に指定されています。</p> <ol style="list-style-type: none"> サイトで適切な CTI ゲートウェイ アプリケーションの設定を入力します。 [保存] をクリックします。 	<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』の「アプリケーション ユーザの設定」の章を参照してください。</p>

■ CTI ゲートウェイの設定チェックリスト



Cisco Unified Presence の設定の概要

この章では、Cisco Unified Presence で必要な設定タスクについて説明します。これらの手順を、[Cisco Unified Presence の管理] ウィンドウから実行します。

この章は、次の内容で構成されています。

- [ライセンス ファイルのアップロード \(P.3-2 \)](#)
- [オプションのセカンダリ Cisco Unified Presence ノードの追加 \(P.3-3 \)](#)
- [Cisco IP Phone Messenger の設定 \(P.3-4 \)](#)
- [MOC 機能の割り当て \(P.3-4 \)](#)
- [プレゼンス ゲートウェイの設定 \(P.3-5 \)](#)
- [着信アクセス コントロール リストの設定 \(P.3-6 \)](#)
- [プライバシー アクセス コントロール リストの設定 \(P.3-7 \)](#)
- [プロキシ サーバの設定 \(P.3-7 \)](#)
- [サービスの有効化 \(P.3-8 \)](#)

ライセンス ファイルのアップロード



(注) ライセンス ファイルをアップロードします。このファイルにより、Cisco Unified Presence アプリケーション用のライセンスが適用されます。

手順

- ステップ 1 [システム]>[ライセンス]>[ライセンスファイルのアップロード] を選択します。
[ライセンスファイルのアップロード (License File Upload)] ウィンドウが表示されます。
- ステップ 2 [ライセンスファイルのアップロード] をクリックします。
- ステップ 3 ファイルのアップロード先を参照し、[アップロード] をクリックします。



(注) 詳細については、『Cisco Unified Presence アドミニストレーションガイド』の「ライセンスファイルのアップロード」の章を参照してください。

オプションのセカンダリ Cisco Unified Presence ノードの追加



(注) この手順は、サブスクリバ ノードをインストールする前に実行してください。

手順

ステップ 1 [システム]>[サーバ]を選択します。

[サーバの検索と一覧表示 (Find and List Servers)] ウィンドウが表示されます。

ステップ 2 検索して任意のサーバをクリックします。

[サーバの設定 (Server Configuration)] ウィンドウが表示されます。

ステップ 3 ホスト名/IP アドレス: サブスクリバ ノードのホスト名または IP アドレスを入力します。このアドレスは、[Cisco Unified Communications Manager の管理]の[システム]>[アプリケーションサーバ]メニューから開いたウィンドウで入力したホスト名と一致します。

ステップ 4 [保存]をクリックします。



(注) 詳細については、『Cisco Unified Presence アドミニストレーションガイド』の「サーバの設定」の章を参照してください。

Cisco IP Phone Messenger の設定



(注) Microsoft Office Communicator だけを使用している場合は、この手順を実行する必要はありません。

手順

ステップ 1 [アプリケーション] > [IP Phone Messenger] > [設定] を選択します。

[IP Phone Messenger の設定 (IP Phone Messenger Settings)] ウィンドウが表示されます。

ステップ 2 [Cisco Unified Communications Manager の管理] ([ユーザ管理] > [アプリケーションユーザ] メニュー) で PhoneMessenger ユーザに設定したものと同一アプリケーション パスワードを設定します。



(注) [アプリケーションユーザ名 (Application Username)] と [アプリケーションパスワード (Application Password)] は、インストール中に自動的に設定されます。

ステップ 3 [保存] をクリックします。



(注) 詳細については、『Cisco Unified Presence アドミニストレーション ガイド』の「IP Phone Messenger の設定」の章を参照してください。

MOC 機能の割り当て



(注) Microsoft Office Communicator の各ユーザに、MOC 機能を割り当てたことを確認します。

手順

ステップ 1 [アプリケーション] > [CTI ゲートウェイ] > [MOC 割り当て] を選択します。

[MOC 割り当ての検索と一覧表示 (Find and List MOC Assignments)] ウィンドウが表示されます。



(注) 詳細については、『Cisco Unified Presence アドミニストレーション ガイド』の「MOC 割り当て」の章を参照してください。

プレゼンスゲートウェイの設定



(注) プレゼンス情報を受け取るためにプレゼンス エンジンが認識する必要があるゲートウェイを設定するには、プレゼンスゲートウェイを使用します。

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 表 3-1 の説明に従って、適切なパラメータ値を入力します。

ステップ 4 [保存] をクリックします。



(注) 詳細については、『Cisco Unified Presence アドミニストレーションガイド』の「プレゼンスゲートウェイ」の章を参照してください。

表 3-1 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)	ドロップダウン 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"> [CUCM]: Cisco Unified Communications Manager ゲートウェイ [Outlook]: Outlook 予定表用の Microsoft Exchange ゲートウェイ
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。
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。

表 3-1 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。

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] > [プロキシサーバ] > [着信 ACL] を選択します。

[許可されている着信ホストの検索と一覧表示 (Find and List Allowed Incoming Hosts)] 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。

[着信アクセスコントロールリストの設定 (Incoming Access Control List Configuration)] ウィンドウが表示されます。

ステップ 3 アドレスパターン (Address Pattern) : 関連付けられている Microsoft LCS の IP アドレスを入力します。

ステップ 4 [保存] をクリックします。



(注) 詳細については、『Cisco Unified Presence アドミニストレーションガイド』の「着信 ACL」の章を参照してください。

プライバシー 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] > [プロキシサーバ] > [発信 ACL] を選択します。

[許可されている宛先ホストの検索と一覧表示 (Find and List Allowed Destination Hosts)] 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。

[発信アクセスコントロールリストの設定 (Outgoing Access Control List Configuration)] ウィンドウが表示されます。

ステップ 3 アドレスパターン (Address Pattern) : 関連付けられている Microsoft LCS の IP アドレスを入力します。

ステップ 4 [保存] をクリックします。



(注) 詳細については、『Cisco Unified Presence アドミニストレーションガイド』の「発信 ACL」の章を参照してください。

プロキシ サーバの設定

手順

ステップ 1 [Cisco Unified Presence] > [プロキシサーバ] > [設定] 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)]: [オン] を選択します。

ステップ 3 [優先プロキシリスナー (Preferred Proxy Listener)]: [Default SIP Proxy TCP Listener] を選択します。

ステップ 4 [保存] をクリックします。

サービスの有効化

手順

-
- ステップ 1** [ナビゲーション] ウィンドウの右上にあるドロップダウン リストから [Cisco Unified サービスアビリティ] を選択し、[移動] をクリックします。
- ステップ 2** [Tools] > [Services Activation] を選択します。
- [Service Activation] ウィンドウが表示されます。
- ステップ 3** [Server]: ドロップダウン リストから [Cisco Unified Presence] を選択します。
- ステップ 4** [Service Activation] ウィンドウが再表示されたら、ウィンドウの下部にある [Cisco Unified Presence Services] セクションで、チェックボックスをオンにして次のサービスを有効にします。
- Cisco Enterprise SIP Proxy
 - Cisco Enterprise Presence Engine
- ステップ 5** クラスタ処理を使用している場合は、これらのサービスが 2 番目のノードで有効になっていることを確認します。
- ステップ 6** [Save] をクリックします。



(注) 詳細については、『Cisco Unified Presence Serviceability アドミニストレーション ガイド for Cisco Unified Presence』の「サービスの管理」の章を参照してください。



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になります。

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)	ドロップダウン 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"> [CUCM]: Cisco Unified Communications Manager ゲートウェイ [Outlook]: Outlook 予定表用の Microsoft Exchange ゲートウェイ  <p>(注) 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>(注) 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。  (注) 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"> [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。 [ルーティング] タブを選択し、[追加] をクリックします。 [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。 <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] > [証明書の管理] > [証明書の表示] に進み、自分の証明書および [siproxy] を選択します。</p> <ol style="list-style-type: none"> [トランスポート] で、[TLS] を選択します。 ポート [5062] を選択します。 <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"> [要求 URI 内のホストを置き換える] を選択します。 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。 	<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>http://technet2.microsoft.com/WindowsServer/en/library/49960f07-4a4c-4e04-9aef-82ab0e8efc0d1033.msp?mfr=true</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"> [ホストの承認] タブをクリックします。 Cisco Unified Presence サーバをダブルクリックします。 [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。 [OK] をクリックします。 LCS サーバを再起動し、使用可能になるまで待機します。 <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>http://technet2.microsoft.com/WindowsServer/en/library/49960f07-4a4c-4e04-9aef-82ab0e8efc0d1033.msp?mfr=true</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"> [スタート]>[管理ツール]>[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。 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。 [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。 [詳細] ペインで、[FIPS] セキュリティ設定を選択します。 セキュリティ設定を変更し、[OK] をクリックします。 	<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>http://technet2.microsoft.com/WindowsServer/en/Library/6ff574cb-30c4-4ad9-8d5e-ae697c65b9b1033.mspx</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"> Cisco Unified Presence の管理ページにログインします。 [Cisco Unified Presence]>[セキュリティ]>[TLS コンテキスト設定] に進みます。 <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"> [検索] をクリックします。 [Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context] をクリックします。 <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"> 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。 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。 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。 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。 [保存] をクリックします。 Cisco Unified Presence Serviceability Administration ページにログインします。 [Tools]>[Service Activation] に進みます。 Cisco UPS SIP Proxy サービスをリスタートします。 	<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> 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。</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>http://www.office.microsoft.com/en-us/assistance/HA011992481033.aspx#DeploymentGuide</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>http://www.office.microsoft.com/en-us/assistance/HA011992481033.aspx#DeploymentGuide</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>http://www.office.microsoft.com/en-us/assistance/HA011992481033.aspx#DeploymentGuide</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>http://www.office.microsoft.com/en-us/assistance/HA011992481033.aspx#DeploymentGuide</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>http://www.office.microsoft.com/en-us/assistance/HA011992481033.aspx#DeploymentGuide</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>http://www.office.microsoft.com/en-us/assistance/HA011992481033.aspx#DeploymentGuide</p>



IBM Lotus Sametime 用 Cisco Click-to Call プラグインの設定の概要

この章では、IBM Lotus Domino Server に Cisco Click-to-Call プラグインをインストールする手順、および Click-to-Call プラグインから発信されたコールを受け入れるように Cisco Unified Communications Manager を設定する手順について説明します。

この章には、次の項があります。

- [前提条件 \(P.5-1\)](#)
- [Cisco Click-to-Call プラグインのインストール \(P.5-2\)](#)
- [Cisco Click-to-Call プラグインの設定 \(P.5-3\)](#)
- [Cisco Click-to-Call 用の Lotus Sametime Server の設定 \(P.5-6\)](#)
- [Cisco Click-to-Call 用の Cisco Unified Communications Manager の設定 \(P.5-7\)](#)
- [SIP トランク セキュリティ プロファイルの設定 \(P.5-7\)](#)
- [Lotus Sametime Server 用の SIP トランクの設定 \(P.5-7\)](#)
- [SIP トランクでのダイジェスト認証の設定 \(P.5-8\)](#)
- [ユーザ名とパスワードの設定 \(P.5-9\)](#)

前提条件

Click-to-Call プラグインをインストールする前に、次のソフトウェアがインストールされていることを確認します。

- IBM Lotus Domino Server 7
- IBM Sametime Server 7.5.1
- Cisco Unified Communications Manager Release 6.0(1)

IBM Lotus Domino Server をインストールまたはアップグレードする方法については、次の URL で適切なインストール マニュアルを参照してください。

<http://www-128.ibm.com/developerworks/lotus/documentation/domino/>

Lotus Sametime をインストールして設定する方法の詳細については、次の URL で適切なマニュアルを参照してください。

<http://www-128.ibm.com/developerworks/lotus/documentation/sametime/>

Cisco Unified Communications Manager Release 6.0(1) 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

Cisco Click-to-Call プラグインのインストール

Cisco Click-to-Call プラグインをインストールするには、次の手順に従います。

手順

ステップ 1 プラグインをインストールするコンピュータに Cisco Click-to-Call をダウンロードします。

ステップ 2 Click-to-Call プラグインをインストールするマシンで、Lotus Domino Server サービスを停止します。



ヒント サービスを停止する方法については、オペレーティング システムに付属のマニュアルを参照してください。

ステップ 3 InstallShield ウィザードを起動するには、オペレーティング システムに適切な Click-to-Call プラグインをダブルクリックします。

[InstallShield Wizard for Cisco Click to Call 6.0(1)] が表示されます。

ステップ 4 [次へ] をクリックします。

インストールの概要ウィンドウが表示されます。

ステップ 5 インストールの概要情報を確認したら、[インストール] をクリックしてインストールを確認します。

ウィザードによってプラグインがインストールされ、追加の概要情報が表示されます。

ステップ 6 インストールを完了するには、[完了] をクリックします。



(注) Lotus Domino Server サービスを開始する前に、Cisco Click-to-Call プラグインを設定する必要があります。P.5-3 の「Cisco Click-to-Call プラグインの設定」を参照してください。

Cisco Click-to-Call プラグインの設定

Cisco Click-to-Call プラグインを設定するには、次の手順に従います。



(注) Lotus Domino Server サービスを開始する前に、関連する Cisco Unified Communications Manager Server を少なくとも 1 つ設定する必要があります。

手順

ステップ 1 Cisco Click-to-Call プラグインをインストールしたコンピュータで、次のディレクトリに進みます。

```
\\lotus\domino
```

ステップ 2 テキスト エディタを使用して、次のファイルを開きます。

```
ClickToConfCUCM.properties
```

ステップ 3 少なくとも 1 つの関連する Cisco Unified Communications Manager Server の名前とポート番号を指定します。

ステップ 4 インストールに必要な他のパラメータ値を指定します。

例 5-1 は、Cisco Click-to-Call プラグインのプロパティ ファイルを示しています。

ステップ 5 必要な値を指定したら、ClickToConfCUCM.properties ファイルを保存します。

ステップ 6 Lotus Domino Server サービスを開始します。

ステップ 7 Lotus Domino Server サービスが実行されていることを確認します。



ヒント サービスを開始する方法については、オペレーティング システムに付属のマニュアルを参照してください。

例 5-1 Cisco Click-to-Call プラグインのプロパティ ファイル

```

#Cisco Click to Call 6.0(1) v124 (Sametime Server Plug-in) configuration file

#Note: For changes made to this file to take effect, you will need to restart the Lotus Domino Server.

#APPLICATION_NAME (optional)
#This field should be alphanumeric.
#Valid characters include alphabet(A-Z and/or a-z) and numbers(1-9) only.
#Default: c2c
APPLICATION_NAME=

#LOCAL_LISTENER_HOST (optional)
#Set the ip address/fqdn that your Sametime Server is listening on.
#Defaults to the first active ip address of the system, if left empty.
LOCAL_LISTENER_HOST=

#LOCAL_LISTENER_PORT (optional)
#Set the port that you want to listen on for SIP messages.
#It needs to be a unreserved port between 0 and 65535.
#Defaults to 5060 if left empty.
LOCAL_LISTENER_PORT=

#Call Managers (required)
#Atleast one CUCM[X]_HOST _must_ be configured
#Add as many as you like, as long as they are numbered sequentially.

#If the host is an ip address:
#      * If you do not specify a port, the port will default to 5060

#If the host is a dns name and if DNS_SRV_SUPPORT is disabled (default):
#      * If you do not specify a port, the port will default to 5060

#If the host is a dns name and if DNS_SRV_SUPPORT is enabled:
#      * Read the comments for DNS_SRV_SUPPORT.

CUCM1_HOST=
CUCM1_PORT=

CUCM2_HOST=
CUCM2_PORT=

CUCM3_HOST=
CUCM3_PORT=

CUCM4_HOST=
CUCM4_PORT=

CUCM5_HOST=
CUCM5_PORT=

CUCM6_HOST=
CUCM6_PORT=

CUCM7_HOST=
CUCM7_PORT=

CUCM8_HOST=
CUCM8_PORT=

CUCM9_HOST=
CUCM9_PORT=

CUCM10_HOST=
CUCM10_PORT=

#Application's Credentials for digest authentication (optional)
#Add as many as you like, as long as they are numbered sequentially.
REALM1=

```

```
REALM1_USERNAME=  
REALM1_PASSWORD=  
  
REALM2=  
REALM2_USERNAME=  
REALM2_PASSWORD=  
  
REALM3=  
REALM3_USERNAME=  
REALM3_PASSWORD=  
  
REALM4=  
REALM4_USERNAME=  
REALM4_PASSWORD=  
  
REALM5=  
REALM5_USERNAME=  
REALM5_PASSWORD=  
  
#MODE (optional)  
  
#Either "sequential" or "roundrobin"  
#sequential mode: Every new Click To Call request will go to the first CUCM configured. If that CUCM  
# does not respond, it will then use the sequentially next configured CUCM.  
#round robin mode: Every new Click to Call request will go to the least used CUCM. If that CUCM  
# does not respond, it will then use the next least used CUCM.  
#Default: sequential  
MODE=  
  
#DNS_SRV_SUPPORT (optional)  
#Either "true" or "false"  
  
#true: Enables DNS SRV support.  
#false: Disables DNS SRV support.  
  
#Notes: If DNS_SRV_SUPPORT is enabled:  
# * You must use fully qualified domain names for all your CUCM[X]_HOST's  
# * If you do not specify a CUCM[X]_PORT then a DNS SRV lookup will  
# be attempted for the hostname. The port is determined from the  
# SRV lookup.  
# * If you do specify a CUCM[X]_PORT, then an A lookup will be  
# attempted for the hostname provided.  
# * DNS SRV should not be used for load balancing. If you wish to load balance  
# set the MODE to "roundrobin".  
  
#Default: false  
DNS_SRV_SUPPORT=
```

Cisco Click-to-Call 用の Lotus Sametime Server の設定

Cisco Click-to-Call と連携するように Lotus Sametime Server を設定するには、次の手順を使用します。

手順

ステップ 1 Lotus Sametime Server にアクセスするには、次の URL を入力します。

`http://server-address/stcenter.nsf`

各部の説明は以下のとおりです。

`server-address` は、Lotus Sametime Server のドメイン名または IP アドレスです。

ステップ 2 表示されるウィンドウで、[**Administer the Server**] リンクをクリックします。

ステップ 3 Lotus Sametime Server にログインします。

ステップ 4 ログインした後、[**Policies**] リンクをクリックします。

ステップ 5 Cisco Click-to-Call を動作させるには、次のパラメータが有効であることを確認します。

[**Allow telephony for contact lists, instant messaging, and instant meetings**]

ステップ 6 他のポリシーがサイト用に正しく設定されていることを確認します。

Cisco Click-to-Call 用の Cisco Unified Communications Manager の設定

Cisco Click-to-Call プラグインと連携するように Cisco Unified Communications Manager を設定するには、次の手順を使用します。



(注)

Cisco Unified Communications Manager の管理ページの詳細については、『*Cisco Unified Communications Manager アドミニストレーションガイド*』を参照してください。

SIP トランク セキュリティ プロファイルの設定

手順

ステップ 1 Cisco Unified Communications Manager の管理ページから、[システム]>[セキュリティプロファイル]>[SIP トランクセキュリティプロファイル]を選択します。

[SIP トランクセキュリティプロファイルの検索と一覧表示 (Find and List SIP Trunk Security Profiles)] 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。

[SIP トランクセキュリティプロファイルの設定 (SIP Trunk Security Profile Configuration)] ウィンドウが表示されます。

ステップ 3 この SIP トランク セキュリティ プロファイルの名前と説明を入力します。

ステップ 4 [アウトオブダイアログ REFER の許可 (Accept Out-of-Dialog REFER)] チェックボックスをオンにします。

ステップ 5 [保存] をクリックします。

Lotus Sametime Server 用の SIP トランクの設定

Lotus Sametime Server 用に SIP トランクを設定して、その SIP トランクを SIP トランク セキュリティ プロファイルに関連付けるには、次の手順を使用します。

手順

ステップ 1 Cisco Unified Communications Manager の管理ページで、[デバイス]>[トランク]を選択します。

[トランクの検索と一覧表示 (Find and List Trunks)] 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。

[トランクの設定 (Trunk Configuration)] ウィンドウが表示されます。

- ステップ 3** [トランクタイプ] ドロップダウン メニューから、[SIP Trunk] を選択します。
- ステップ 4** [デバイスプロトコル (Device Protocol)]: デフォルト値の [SIP] を受け入れます。
- ステップ 5** [次へ] をクリックします。
- ステップ 6** このトランクのデバイス名と説明を入力します。
- ステップ 7** [デバイスプール (Device Pool)]: [デフォルト] を選択します。
- ステップ 8** [接続先アドレス (Destination Address)]: Lotus Sametime Server の IP アドレスを入力します。
- ステップ 9** [SIP トランクセキュリティプロファイル (SIP Trunk Security Profile)]: 作成した SIP トランク セキュリティ プロファイルを選択します。
- ステップ 10** [SIP プロファイル (SIP Profile)]: [Standard SIP Profile] を選択します。
- ステップ 11** [保存] をクリックします。
- ステップ 12** 変更内容を有効にするには、[リセット] をクリックします。

SIP トランクでのダイジェスト認証の設定



(注) この項の手順を実行して、認証されたユーザだけがトランクにアクセスできることを保証できます。ただし、この項の手順はオプションであることに注意してください。

SIP トランクでダイジェスト認証を設定するには、次の手順を使用します。

手順

- ステップ 1** Cisco Unified Communications Manager の管理ページから、[システム] > [セキュリティプロファイル] > [SIP トランクセキュリティプロファイル] を選択します。
- [SIP トランクセキュリティプロファイルの検索と一覧表示 (Find and List SIP Trunk Security Profiles)] ウィンドウが表示されます。
- ステップ 2** [検索] をクリックします。
- ステップ 3** Cisco Click-to-Call 用に作成した SIP トランク セキュリティ プロファイルをクリックします。
- [SIP トランクセキュリティプロファイルの設定 (SIP Trunk Security Profile Configuration)] ウィンドウが表示されます。
- ステップ 4** [ダイジェスト認証を有効化 (Enable Digest Authentication)] チェックボックスをオンにします。

ステップ 5 [保存] をクリックします。

ステップ 6 変更内容を有効にするには、[リセット] をクリックします。

ステップ 7 レルムを設定するには、[システム] > [エンタープライズパラメータ] を選択します。

ステップ 8 [Cluster ID] フィールドに、適切な値を入力します。

ユーザ名とパスワードの設定

SIP 認証用の新しいユーザ名とパスワードを設定するには、次の手順に従います。

手順

ステップ 1 [ユーザ管理] > [アプリケーションユーザ] を選択します。

[アプリケーションユーザの検索と一覧表示 (Find and List Application Users)] 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。

[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウが表示されます。

ステップ 3 ユーザ ID、パスワード、およびダイジェスト信用証明書を入力します。

ステップ 4 [アウトオブダイアログ REFER の許可 (Accept Out-of-Dialog REFER)] チェックボックスをオンにします。

ステップ 5 [保存] をクリックします。

ステップ 6 [システム] > [セキュリティプロファイル] > [SIP トランクセキュリティプロファイル] を選択します。

[SIP トランクセキュリティプロファイルの検索と一覧表示 (Find and List SIP Trunk Security Profiles)] ウィンドウが表示されます。

ステップ 7 [検索] をクリックします。

ステップ 8 Cisco Click-to-Call 用に作成した SIP トランク セキュリティ プロファイルをクリックします。

[SIP トランクセキュリティプロファイルの設定 (SIP Trunk Security Profile Configuration)] ウィンドウが表示されます。

ステップ 9 変更内容を有効にするには、[リセット] をクリックします。



INDEX

- A**
- Active Directory
 - 設定 4-3
- C**
- Cisco Unified Communications Manager
 - AXL アクセス権限の有効化 2-11
 - Click-to-Call プラグイン 5-7
 - Click-to-Call プラグイン用の SIP トランクの設定 5-7
 - CTI ゲートウェイの設定 2-16
 - IP Phone Messenger 2-6
 - IP Phone Messenger の IP Phone サービス 2-8
 - IP Phone Messenger への電話機の登録 2-9
 - SIP トランク セキュリティ プロファイル 2-10
 - SIP トランクの設定 2-13
 - アプリケーション サーバの設定 2-2
 - アプリケーション ユーザの追加 2-11
 - エンド ユーザとライン アピアランスの関連付け 2-15
 - 機能の割り当て 2-3
 - サービス パラメータ 2-2
 - 電話機のプライマリ内線の関連付け 2-4
 - 必要なサービス 2-14
 - ユーザグループ 2-7
 - ユーザへのデバイスの関連付け 2-5
 - Cisco Unified Presence
 - 2 番目のノード 3-3
 - IP Phone Messenger の設定 3-4
 - MOC 機能 3-4
 - サービス 3-8
 - 着信アクセス コントロール リスト 3-6
 - プライバシー アクセス コントロール リスト 3-7
 - プレゼンス ゲートウェイ 3-5
 - プロキシ サーバの設定 3-7
 - ライセンス ファイル 3-2
 - Click-to-Call プラグイン
 - Cisco Unified Communications Manager 5-7
 - Lotus SameTime Sever 5-6
 - Lotus SameTime Server 用の SIP トランク 5-7
 - SIP トランク セキュリティ プロファイル 5-7
 - SIP トランクでのダイジェスト認証 5-8
 - インストール 5-2
 - 設定 5-3
 - 前提条件 5-1
 - プロパティ ファイル 5-4
 - CTI ゲートウェイ
 - 設定 2-16
- E**
- Exchange 予定表との統合
 - CA サービス 4-10
 - CSR への署名 4-13
 - Exchange 参照のみ可としての制御の委任 4-6
 - IIS での CSR の生成 4-12
 - Receive As アカウント 4-5
 - Receive As 権限 4-7
 - 署名済み証明書のアップロード 4-14
 - 署名済み証明書のダウンロード 4-14
 - セキュリティ証明書 4-9
 - 設定 4-5
 - プレゼンス ゲートウェイ 4-8
 - ユーザ アカウント 4-6
 - ルート証明書のアップロード 4-11
 - ルート証明書のダウンロード 4-10
- I**
- IP Phone Messenger
 - Cisco Unified Presence での設定 3-4
 - IP Phone サービスの設定 2-8
 - 設定 2-6

- L**
- LCS
設定 4-2
- M**
- Microsoft Office Communicator
「MOC」を参照
- Microsoft Office Live Communications Server
「LCS」を参照
- Microsoft 製品との統合
概要 1-2
- MOC
Cisco Unified Presence での機能の割り当て 3-4
設定 4-18
- R**
- Receive As アカウント
権限 4-7
作成 4-5
- S**
- SIP トランク
Click-to-Call プラグイン用の設定 5-7
Lotus SameTime Sever 5-7
セキュリティ プロファイル 2-10
設定 2-13
- T**
- TLS ルート
設定 4-16
- あ**
- アクセス コントロール リスト
着信 3-6
プライバシ 3-7
- アプリケーション サーバ
設定 2-2
- え**
- エンド ユーザ
機能の割り当て 2-3
ライン アピアランスとの関連付け 2-15
- さ**
- サービス
Cisco Unified Communications Manager 2-13
Cisco Unified Presence 3-8
- サービス パラメータ
設定 2-2
- せ**
- セキュリティ証明書
Exchange 予定表との統合用の設定 4-9
- ふ**
- プレゼンス ゲートウェイ
Exchange 予定表との統合用の設定 4-8
設定 3-5
- プロキシ サーバ
設定 3-7
- ゆ**
- ユーザ アカウント
Exchange Server での作成 4-6
- ユーザ グループ
エンド ユーザの割り当て 2-7
- ら**
- ライセンス ファイル
アップロード 3-2