



## **Cisco UC Integration for Cisco WebEx Connect C7 コンフィギュレーション ガイド**

**Configuration Guide for Cisco UC Integration for Cisco WebEx  
Connect C7**

2011 年 2 月 13 日

**【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/](http://www.cisco.com/jp/go/safety_warning/))をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。  
リンク情報につきましては、日本語版掲載時点で、英語版にアップ  
デートがあり、リンク先のページが移動/変更されている場合があ  
りますことをご了承ください。  
あくまでも参考和訳となりますので、正式な内容については米国サ  
イトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊  
社担当者にご確認ください。

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。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. 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、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコシステムズおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、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、シスコシステムズおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコシステムズまたはその供給者に知らされていても、それらに対する責任は一切負わないものとします。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned 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. (1005R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

*Cisco UC Integration for Cisco WebEx Connect C7 コンフィギュレーション ガイド*

© 2011 Cisco Systems, Inc.

All rights reserved.

Copyright © 2011, シスコシステムズ合同会社.

All rights reserved.



## CONTENTS

---

### CHAPTER 1

はじめに	1-1
サポートされるサーババージョン	1-2
Cisco Unified クライアント サービス フレームワークで発信トラフィックに使用されるポート	1-2
クライアント コンピュータの要件	1-2
Cisco UC Integration for Cisco WebEx Connect のハードウェア要件	1-2
Cisco UC Integration for Cisco WebEx Connect のソフトウェア要件	1-3
サポートされる Cisco Unified IP Phone	1-3
テスト済みのオーディオ デバイス	1-4
音声の品質	1-5
特記事項	1-6

---

### CHAPTER 2

<b>Cisco Unified Communications Manager でのデバイス タイプの設定</b>	<b>2-1</b>
Cisco Unified Communications Manager の準備	2-1
ユーザのデバイスおよび電話番号の作成	2-2
Windows Vista の QoS パケットマーキング	2-12

---

### CHAPTER 3

<b>ダイヤリング ルールの設定とインストール</b>	<b>3-1</b>
ダイヤリング ルールの設定	3-1
ダイヤリング ルールのインストール	3-2
ダイヤリング ルールのインストールの確認	3-2
TFTP サービスの再起動	3-2

---

### CHAPTER 4

<b>Standard CTI ユーザ グループへのユーザの追加</b>	<b>4-1</b>
ユーザの新規作成	4-1

---

### CHAPTER 5

<b>Cisco UC Integration for Cisco WebEx Connect のインストールと設定</b>	<b>5-1</b>
インストール パッケージの内容	5-1
Cisco UC Integration for Cisco WebEx Connect の設定	5-1

---

### CHAPTER 6

<b>Cisco Unity と Unity Connection Server の設定</b>	<b>6-1</b>
Cisco Unity Server	6-1
Cisco Unity Connection Server	6-3

Cisco Unity を使用した導入のための Microsoft Exchange の IMAP セキュリティ 設定の確  
認 6-5

---

CHAPTER 7

**Cisco Unified Communications Manager の設定とボイスメールの要件 7-1**

DTMF アクセス コードに関する重要な情報 7-1

ボイスメールの要件 7-1

---

CHAPTER 8

**マニュアルの入手方法およびテクニカル サポート 8-1**

マニュアルの検索 8-1



# CHAPTER 1

## はじめに

---

Cisco UC Integration for Cisco WebEx Connect C7 は Cisco WebEx Connect に電話機タブを追加します。この新しいスペースによってユーザのコンピュータはフル機能の電話機に変わり、コールの発信、受信、管理を行うことができます。

Cisco UC Integration for Cisco WebEx Connect C7 は、コール制御サービス、コール履歴、メッセージ待機インジケータ、メディアなどを提供するクライアント サービス フレームワークの統合を基盤としています。

クラウド内の Cisco WebEx Connect サービスは、残りのサービス（インスタント メッセージング、プレゼンス、スペースなど）を提供します。電話機タブから実行できる操作は次のとおりです。

- コールを発信および受信する。
- 音声メッセージ サービスを呼び出す。
- 通信履歴を表示する。
- 通信ペインのオプションを設定する。
- 電話機モードを切り替える。コンピュータからデスクフォンを制御するか、コンピュータ上の音声とマイクを使用して通話を処理するかを選択できます。これらのオプションを簡単に切り替えることが可能です。

## サポートされるサーババージョン

製品	サポートされるバージョン
Cisco Unified Communications Manager	CUCM 7.1(3)
	CUCM 7.1(5)
	CUCM 8.0(1)
	CUCM 8.5
Cisco Unity with Microsoft Exchange 2003 または Microsoft Exchange 2007	Unity 8.0
Cisco Unity Connection	Unity Connection 8.0
	Unity Connection 8.5

## Cisco Unified クライアント サービス フレームワークで発信トラフィックに使用されるポート

ポート	プロトコル	説明
69	UDP	Trivial File Transfer Protocol (TFTP) ファイルをダウンロードするために TFTP サーバに接続する。
2748	TCP	Cisco Unified Communications Manager の CTIManager コンポーネントである CTI ゲートウェイに接続する。
5060	UDP/TCP	Session Initiation Protocol (SIP; セッション開始プロトコル) コールシグナリングを提供する。
5061	TCP	セキュアな SIP コールシグナリングを提供する。
8443	TCP	Cisco Unified Communications Manager IP Phone (CCMCIP) サーバに接続し、現在割り当てられているデバイスのリストを取得する。
16384-32766	UCP	オーディオ用の RTP メディア ストリームを送信する。
16384-32766	UDP	オーディオおよびビデオ用の Receives Real-Time Transport Protocol (RTP) メディア ストリームを受信する。これらのポートは、Cisco Unified Communications Manager で設定されます。

## クライアント コンピュータの要件

### Cisco UC Integration for Cisco WebEx Connect のハードウェア要件

項目	説明
メモリ	Microsoft Windows 7 : 2 GB
	Microsoft Windows Vista : 2 GB
	Microsoft Windows XP : 1 GB
使用可能なディスク領域	200 MB

項目	説明
接続	ダウンロード帯域幅：80 Kbps アップロード帯域幅：80 Kbps
プロセッサ	
デスクトップ	2.4 GHz
ラップトップ	1.8 GHz

## Cisco UC Integration for Cisco WebEx Connect のソフトウェア要件

項目	説明
オペレーティング システム	Windows 7 Professional または Ultimate、32 ビットまたは 64 ビット (WOW モード)  Windows Vista SP2 Business または Ultimate、DirectX 10 対応、32 ビットまたは 64 ビット (WOW モード)  Windows XP SP3、DirectX 9.0c 対応、32 ビットのみ 最小ディスク領域は 80MB

## サポートされる Cisco Unified IP Phone

次の表に、Cisco UC Integration for Cisco WebEx Connect C7 でサポートされる Cisco Unified IP Phone モデルおよび Skinny Call Control Protocol (SCCP) と Session Initiation Protocol (SIP) がサポートされているかどうかを示します。

電話機	SCCP	SIP
Cisco IP Communicator	○	○
9971 (ビデオあり/なし)	×	○
9951	×	○
8961	×	○
7985G	○	×
7975G	○	○
7971G	○	○
7970G	○	○
7965G	○	○
7962G	○	○
7961G-GE	○	○
7961G	○	○
7960G	○	×
7945G	○	○
7942G	○	○
7941G-GE	○	○
7941G	○	○

電話機	SCCP	SIP
7940G	○	×
7931G	○	×
7925G	○	×
7921G	○	×
7920G	○	×
7912G	○	×
7911G	○	○
7910G	○	×
7906G	○	○
7905G	○	×
7902G	○	×
6961	○	×
6941	○	×
6921	○	×

## テスト済みのオーディオ デバイス

Cisco UC Integration for Cisco WebEx Connect でテスト済みのオーディオ ヘッドセットを次に示します。

- Polycom Speakerphone USB
- ClearOne CHAT 50 USB
- Jabra GN8110 USB
- Jabra GN8120 USB
- Jabra GN9120
- Jabra Advantage Plus
- Plantronics CS50
- Plantronics CS60
- Plantronics DA60 USB
- Plantronics DSP-400
- Plantronics DA55 USB
- Plantronics Voyager 510 Bluetooth
- Clarisys i750
- Futiro USB
- Sonic EV-87
- PLANTRONICS Blackwire C620
- Logitech USB H330
- Logitech960 USB
- SONIC DT-301

- Lenonvo
- PLANTRONICS WG200
- PLANTRONICS W430

Cisco IP Phone の詳細については、言語、電話機モデル、Cisco Unified Communications Manager リリース固有のマニュアルを参照してください。次の URL から入手できます。

<http://www.cisco.com/cisco/web/psa/maintain.html?mode=prod&level0=278875240>



(注)

7931G 電話機を Cisco UC Integration for Cisco WebEx Connect で正しく機能させるためには、Cisco Unified Communications Manager の [Outbound Call Rollover to] フィールドの値を [No Rollover] に設定する必要があります。

## 音声の品質

Cisco UC Integration for Cisco WebEx Connect は、さまざまな条件下で最高品質の音声を提供できるように設計されています。状況によって、音声伝送の中断や音声の一時的な歪み（「アーティファクト」）が発生する場合がありますが、これらはアプリケーションの通常の動作と見なされます。ただし、次のような場合は、このようなアーティファクトが発生することはほとんどなく、発生しても一時的です。

- Cisco UC Integration for Cisco WebEx Connect が推奨される設定の要件を満たすワークステーションにインストールされている。
- Cisco Unified Communication ソリューションリファレンス デザインのドキュメントで推奨されている品質基準を満たすネットワークを使用している。

シスコで採用しているオペレーティング システムとのインターフェイス方法により、システム上で実行している他のアプリケーションがソフトフォンの音声やビデオの品質に悪影響を及ぼす可能性は少なくなります。ただし、これらの製品を実行するシステム環境に共通する特性は Cisco IP Phone などの閉鎖された環境と非常に異なるため、同等のパフォーマンスを実現できるという保証はありません。

アーティファクトの原因となりうる条件を次に示します。

- アプリケーションやシステム プロセスの起動、または、他のアプリケーションの実行中にシステム処理が発生することに起因する PC の CPU 使用率のスパイク（CPU 使用率が 75 ~ 100% に達する場合）。
- システムで使用できる物理メモリが不足している。
- 他のアプリケーションがネットワーク ワークステーションとのやり取りで大量の帯域幅を使用している。
- 他のネットワーク帯域幅に障害がある。
- 電源管理ポリシーにより CPU クロック速度が大幅に低減する（電池で稼動しているラップトップなど）、または断熱システムにより負荷の非常に高い状態で CPU が実行される。
- サードパーティ製ソフトウェアからの干渉など、アプリケーションがネットワークや音声システムにタイミングよくアクセスできない原因となるその他の条件。

上記の条件を回避または回復することにより、音声の歪みに関するアーティファクトを最小限に抑えることができます。

## 特記事項



### 警告

重要なお知らせ - 必読：緊急時、たとえば 911 番などにコールする場合、ソフトフォン テクノロジーでは適時かつ正確な位置データを提供できない可能性があります。不適切な緊急応答センターにコールが発信されたり、緊急応答センターで正確な位置が把握できない場合があります。緊急時には、自己の責任においてソフトフォンをお使いください。シスコは、発生したエラーまたは遅延の責任を負いません。



## CHAPTER 2

# Cisco Unified Communications Manager でのデバイス タイプの設定

Cisco UC Integration for Cisco WebEx Connect に関する Cisco Unified Communications Manager での設定作業は、デバイス タイプを Cisco Unified Communications Manager に追加することと、電話番号を設定することです。作業を始める前に、Cisco Unified Communications で次のサービスを有効にして、その設定が適切に機能することを確認する必要があります。

- Cisco Unified Communications Manager サービス。Cisco Unified Communications Manager サービスの詳細については、次の URL にある資料を参照してください。

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd\\_products\\_support\\_general\\_information.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_general_information.html)

- Cisco Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) サービス。Cisco TFTP サービスの詳細については、次の URL にある『Cisco Unified Communications Manager System Guide』を参照してください。

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html)

- Cisco CTIManager サービス。Cisco CTIManager サービスの詳細については、次の URL にある『Cisco Unified Communications Manager System Guide』を参照してください。

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html)

- Cisco Unified Communications Manager IP Phone (CCMCIP) サービス。



(注)

管理者は CCMCIP サービスを制御しません。これはデフォルトでオンにされているため、管理者は、クライアントで CCMCIP サービスに CUCM ユーザを使用するように設定する必要があります。

## Cisco Unified Communications Manager の準備

Cisco UC Integration for Cisco WebEx Connect には、Client Services Framework という新しい Cisco Unified Communications Manager デバイス タイプが必要です。Cisco Unified Communications システムにインストールされている Cisco Unified Communications Manager のリリースによっては、Cisco Options Package (COP) ファイルを使用して Cisco Unified Communications Manager にパッチを適用する必要があります。

Cisco Unified Communications Manager に Client Services Framework デバイス タイプが存在しない場合は、COP ファイルを実行する必要があります。COP ファイルは Cisco Unified Communications Manager パブリッシャ サーバで実行します。COP ファイルを適用した後、Cisco Unified Communications Manager パブリッシャ サーバを再起動し、続いてその他すべてのサーバを再起動する必要があります。

COP ファイルは Administration Toolkit から入手できます。Administration Toolkit にアクセスするには、次の URL にある [Download Software] ページから [Cisco UC Integration for Cisco WebEx Connect] に移動します。

[http://www.cisco.com/cisco/software/release.html?mdfid=282811017&flowid=5464&softwareid=282888767&release=7.1\(6\)&rellifecycle=&relind=AVAILABLE&reltype=latest](http://www.cisco.com/cisco/software/release.html?mdfid=282811017&flowid=5464&softwareid=282888767&release=7.1(6)&rellifecycle=&relind=AVAILABLE&reltype=latest)

詳細については、Cisco Unified Communications Manager のリリース ノートを参照してください。

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cucm/rel\\_notes/7\\_0\\_1/cucm-rel\\_notes-701.html#wp684478](http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/rel_notes/7_0_1/cucm-rel_notes-701.html#wp684478)

## ユーザのデバイスおよび電話番号の作成

### 手順

- ステップ 1 Cisco Unified Communications Manager Administration で [Device] > [Phone] を選択します。
- ステップ 2 [Add New] を選択します。
- ステップ 3 [Phone Type] ドロップ ダウン ボックスから、[Cisco Unified Client Services Framework] を選択します。
- ステップ 4 [Next] を選択します。
- ステップ 5 [Phone Configuration] ウィンドウで、次のように電話機の情報を入力します。

フィールド	説明
<b>Device Information</b>	
Device Name	Cisco Unified Client Services Framework デバイスを識別する名前を入力します。名前には、英数字、ピリオド、ハイフン、下線を使用できます。デバイス名は、ユーザのユーザ ID に関連付ける必要はありません。
Description	(オプション) デバイスの説明を入力します。
Device Pool	電話機を割り当てるデバイス プールを選択します。デバイス プールでは、地域、日時グループ、ソフトキー テンプレート、および Multilevel Precedence and Preemption (MLPP) 情報など、デバイスに共通する特性のセットを定義します。
Common Device Configuration	(オプション) このデバイスに割り当てる共通デバイス設定を選択します。共通デバイス設定には、特定のユーザに関連付けられる属性 (サービスまたは機能) が含まれます。
Phone Button Template	適切な電話ボタン テンプレートを選択します。電話ボタン テンプレートによって電話機のボタンの設定が決定され、各ボタンで使用される機能 (回線、短縮ダイヤルなど) が特定されます。
Common Phone Profile	電話プロファイルを特定する名前を選択します。
Calling Search Space	(オプション) パーティションのリストから選択します。コーリングサーチ スペースは、この電話番号からコールを発信できる番号を検索するための、パーティションのリストで構成されます。選択した値は、この電話番号を使用するすべてのデバイスに適用されます。
Media Resource Group List	(オプション) このウィンドウには、メディア リソース グループが一覧表示されます。このリストには、以前に定義されたメディア リソース グループのみが含まれ、最高から最低の優先順に一覧表示されます。

フィールド	説明
User Hold MOH Audio Source	(オプション) ユーザが保留操作を起動したときに再生するサウンドを選択します。
Network Hold MOH Audio Source	(オプション) ネットワークが保留操作を起動したときに再生するサウンドを選択します。
Location	RSVP ポリシー設定を変更する場所を選択します。
User Locale	(オプション) エンドユーザをサポートする、言語とフォントを含む一連の詳細情報を選択して指定します。
Network Locale	(オプション) ゲートウェイに関連付けられるロケールを選択します。ネットワーク ロケールは、特定の場所のハードウェアをサポートするための一連の詳細情報を識別します。ネットワーク ロケールには、特定の地理的領域のデバイスが使用するトーンと音の周期の定義が含まれます。 <b>注:</b> すでにインストールされ、関連付けられたデバイスによってサポートされるネットワーク ロケールのみを選択してください。リストには、この設定に使用可能なすべてのネットワーク ロケールが表示されますが、すべてをインストールする必要はありません。デバイスが、ファームウェアでサポートされていないネットワーク ロケールに関連付けられている場合、そのデバイスは起動に失敗します。
Device Mobility Mode	このデバイスのデバイス モビリティ機能をオンまたはオフにするか、デフォルトのデバイス モビリティ モードを使用する場合は、[Default] を選択します。デフォルトの設定では、デバイスの Device Mobility Mode サービス パラメータの値を使用します。
Owner User ID	(オプション) 割り当てられた電話機ユーザのユーザ ID を選択します。ユーザ ID は、Call Detail Record (CDR; 呼詳細レコード) で、このデバイスから発信されるすべてのコールに対して記録されます。 <b>注:</b> エクステンション モビリティを使用する場合は、このフィールドを設定しないでください。エクステンション モビリティでは、デバイスのオーナーはサポートされていません。 <b>注:</b> オーナー ユーザ ID とモビリティ ユーザ ID は異なっていてもかまいません。
Mobility User ID	(オプション) このデュアルモード フォンを割り当てるユーザのユーザ ID を選択します。 <b>注:</b> モバイル ユーザ ID 設定は、デュアルモード フォンのモバイル コネクト機能とモバイル ボイス アクセス機能に使用されます。 <b>注:</b> オーナー ユーザ ID とモビリティ ユーザ ID は異なっていてもかまいません。
Primary Phone	(オプション) IP Communicator や Cisco Unified Communications Integration に関連付ける物理的電話機を選択します。プライマリ電話機を選択すると、アプリケーションが使用するデバイス ライセンスユニットが少なくなり、「付属」ライセンス (プライマリ電話機に対して) と見なされます。

フィールド	説明
Use Trusted Relay Point	<p>Cisco Unified Communications Manager は、このメディア エンドポイントによって Trusted Relay Point (TRP; 信頼できるリレーポイント) デバイスを挿入するかどうかをイネーブルまたはディセーブルにします。次のいずれかの値を選択します。</p> <ul style="list-style-type: none"> <li>• <b>Default</b> : この値を選択した場合、デバイスはこのデバイスが関連付けられている共通デバイス設定の [Use Trusted Relay Point] 設定を使用します。</li> <li>• <b>Off</b> : このデバイスで、TRP の使用をディセーブルにする場合にこの値を選択します。この設定によって、このデバイスが関連付けられている共通デバイス設定の [Use Trusted Relay Point] 設定が上書きされます。</li> <li>• <b>On</b> : このデバイスで、TRP の使用をイネーブルにする場合にこの値を選択します。この設定によって、このデバイスが関連付けられている共通デバイス設定の [Use Trusted Relay Point] 設定が上書きされます。</li> </ul> <p>信頼できるリレーポイント (TRP) デバイスは信頼できるリレーポイントとしてラベル付けされている MTP またはトランスコーダ デバイスを指定します。</p>
Always Use Prime Line	<p>次のいずれかのオプションをイネーブルまたはディセーブルにします。</p> <ul style="list-style-type: none"> <li>• <b>Default</b> : Cisco Unified Communications Manager は Cisco CallManager サービスをサポートする Always Use Prime Line サービス パラメータの設定を使用します。</li> <li>• <b>Off</b> : 電話機がアイドルで、いずれかの回線でコールを受信すると、電話のユーザは、コールを受信した回線からのコールに応答できません。</li> <li>• <b>On</b> : 電話機がアイドル (オフフック) で、いずれかの回線でコールを受信すると、そのコールにプライマリ回線が選択されます。他の回線のコールは鳴り続け、電話機ユーザはそれらの他の回線を選択して、これらのコールに応答する必要があります。</li> </ul>
Always Use Prime Line for Voice Message	<p>次のいずれかのオプションをイネーブルまたはディセーブルにします。</p> <ul style="list-style-type: none"> <li>• <b>On</b> : 電話機がアイドルの場合、電話機のユーザが電話機の [Messages] ボタンを押すと、ボイスメッセージを受信するために電話のプライマリ回線がアクティブ回線になります。</li> <li>• <b>Off</b> : 電話機がアイドルの場合、電話機の [Messages] ボタンを押すと、ボイスメッセージのある回線から、ボイスメッセージシステムを自動的にダイヤルします。Cisco Unified Communications Manager は常にボイスメッセージのある最初の回線を選択します。電話機のユーザが [Messages] ボタンを押したときに、ボイスメッセージがある回線がない場合、プライマリ回線が使われます。</li> <li>• <b>Default</b> : Cisco Unified Communications Manager は、Cisco CallManager サービスをサポートする Always Use Prime Line for Voice Message サービス パラメータの設定を使用します。</li> </ul>

フィールド	説明
Calling Party Transformation CSS	<p>(オプション) この設定により、デバイスの発信者番号をローカライズできます。選択する発信側変換 CSS に、このデバイスに割り当てる発信側変換パターンが含まれていることを確認してください。</p> <p><b>ヒント:</b> コールが行われる前に、デバイスは番号分析を使用して、変換を適用する必要があります。[Calling Party Transformation CSS] を [None] に設定した場合、変換は一致せず、適用されません。発信側変換パターンをルーティングに使用されていない Null 以外のパーティションに設定していることを確認してください。</p>
Geolocation	<p>(オプション) このデバイスを位置情報に関連付けないことを指定する未指定の位置情報を選択します。</p>
Use Device Pool Calling Party Transformation CSS	<p>このデバイスに割り当てられているデバイス プールに設定されている発信側変換 CSS を使用する場合は、このボックスをオンにします。このチェックボックスを選択しない場合、デバイスは [Phone Configuration] ウィンドウで選択した発信側変換 CSS を使用します。</p>
Ignore Presentation Indicators (internal calls only)	<p>コール単位でコール表示制限を設定する場合に、このボックスをオンにします。このチェックボックスをオンにすると、Cisco Unified Communications Manager は内部コールに対して受信したすべての表示制限を無視します。</p>
Allow Control of Device from CTI	<p>Computer Telephony Integration (CTI; コンピュータ テレフォニー インテグレーション) サーバを使用して、ユーザのデスクフォンを Cisco UC Integration for Cisco WebEx Connect で制御およびモニタする場合は、このオプションを選択します。</p> <p>ユーザが Standard CTI Enabled ユーザ グループに追加されるようにしてください。</p>
Logged Into Hunt Group	<p>電話機が現在ハント リスト (グループ) にログインしていることを示す場合はこのボックスをオンにします。電話機をハント リストに追加したら、管理者はこのチェックボックスをオン (またはオフ) にすることによって、ユーザをログインまたはログアウトさせることができます。</p> <p>ユーザは電話機のソフトキーを使用して、電話機をハント リストにログインまたはログアウトします。</p>
Remote Device	<p>SCCP パイプで、リモート サイトへの接続時間の遅延が発生している場合に、このボックスをオンにします。このチェックボックスをオンにすると、Cisco Unified Communications Manager に、電話デバイスの登録時にバッファを割り当て、SCCP メッセージを電話機にバンドルするように指示します。</p> <p><b>ヒント:</b> この機能はリソースを消費するため、SCCP を実行している電話機で、シグナルの遅延が発生している場合にのみ、このチェックボックスをオンにしてください。ほとんどのユーザにこのオプションは必要ありません。</p>

フィールド	説明
<b>Protocol Specific Information</b>	
Packet Capture Mode	<p>この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケット キャプチャを実行すると、CPU の使用率が上昇して、コール処理が妨げられる可能性があります。ドロップダウン リストボックスで、次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> <li>• <b>None</b> : このオプションは、パケット キャプチャが発生しないことを示します (デフォルト設定)。パケット キャプチャが完了したら、この設定を設定します。</li> <li>• <b>Batch Processing Mode</b> : Cisco Unified Communications Manager は復号化されたメッセージまたは暗号化されていないメッセージをファイルに書き込み、システムが各ファイルを暗号化します。システムは、毎日新しい暗号キーを使用して、新しいファイルを作成します。Cisco Unified Communications Manager はファイルを 7 日間保管し、ファイルを暗号化するキーも安全な場所に格納します。Cisco Unified Communications Manager は PktCap 仮想ディレクトリにファイルを保存します。1 つのファイルの中に、タイムスタンプ、送信元 IP アドレス、送信元 IP ポート、宛先 IP アドレス、パケットのprotocols、メッセージの長さ、およびメッセージが保持されます。TAC のデバッグ ツールでは、HTTPS、管理者のユーザ名とパスワード、および指定された日付を使用して、キャプチャされたパケットを保持している暗号化済みファイルを 1 つだけ要求します。同様に、暗号化されているファイルを復号化するためのキー情報も要求します。</li> </ul>
Packet Capture Duration	<p>(オプション) この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケット キャプチャを実行すると、CPU の使用率が上昇して、コール処理が妨げられる可能性があります。</p> <p>このフィールドには、1 つのパケット キャプチャセッションに割り当てる時間の上限 (分単位) を指定します。デフォルト設定は 0 で、範囲は 0 ~ 300 分です。</p> <p>パケット キャプチャを開始するには、このフィールドに 0 以外の値を入力します。パケット キャプチャが完了すると、値 0 が表示されます。</p>
Presence Group	<p>エンド ユーザのプレゼンス グループを選択します。選択したグループは、この電話番号をモニタできるデバイス、エンド ユーザ、アプリケーション ユーザを指定します。</p> <p>プレゼンス グループのデフォルト値は、Standard Presence グループを指定し、インストール時に設定されます。Cisco Unified Communications Manager Administration に設定されたプレゼンス グループはドロップダウン リストボックスにも表示されます。</p>
SIP Dial Rules	<p>(オプション) 適切な SIP ダイアル ルールを選択します。SIP ダイアル ルールは、Cisco Unified IP Phone 7905、7912、7940、7960 のローカル ダイアル プランを提供するため、ユーザは、コールが処理される前に、キーを押したり、タイマーを待機したりする必要はありません。</p> <p>SIP を実行している IP 電話にダイアル ルールを適用しない場合は、[SIP Dial Rules] フィールドを [&lt;None&gt;] に設定したままにします。これは、コールが処理される前に、ユーザがダイアル ソフトキーを使用するか、タイマーが切れるまで待つ必要があることを示します。</p>

フィールド	説明
MTP Preferred Originating Codec	(オプション) SIP コールにメディア ターミネーション ポイントが必要な場合に使用するコーデックを選択します。
Device Security Profile	電話機に必要とするセキュリティ プロファイルを選択します。 Client Services Framework- Standard SIP Secure Profile を選択する場合は、次の手順に従います。 <b>1.</b> [Certification Authority Proxy Function (CAPF) Information] セクションに、証明書および認証情報を入力します。 <b>2.</b> [Generate String] を選択します。 <b>3.</b> [Authentication String] フィールドの内容を、ユーザに電子メールで送信します。
Rerouting Calling Search Space	(オプション) 再ルーティングに使用するコーリング サーチ スペースを選択します。 参照元の再ルーティング コーリング サーチ スペースを使用して、参照先へのルートが検索されます。再ルーティング コーリング サーチ スペースが原因で参照が失敗すると、Refer Primitive は「405 Method Not Allowed」メッセージによって要求を拒否します。 リダイレクト (3xx) プリミティブおよび転送機能も再ルーティング コーリング サーチ スペースを使用して、リダイレクト先または転送先を検索します。
SUBSCRIBE Calling Search Space	(オプション) ドロップダウン リスト ボックスから、電話機のプレゼンス要求に使用する SUBSCRIBE コーリング サーチ スペースを選択します。Cisco Unified Communications Manager Administration で設定するすべてのコーリング サーチ スペースが [SUBSCRIBE Calling Search Space] ドロップダウン リスト ボックスに表示されます。 ドロップダウン リストから、エンド ユーザに別のコーリング サーチ スペースを選択しない場合、SUBSCRIBE コーリング サーチ スペースのデフォルトは [None] に設定されます。 この目的で明示的に SUBSCRIBE コーリング サーチ スペースを設定するには、すべてのコーリング サーチ スペースを設定する場合と同じようにコーリング サーチ スペースを設定します。 プレゼンス機能でサポートされる SUBSCRIBE コーリング サーチ スペースは、Cisco Unified Communications Manager が電話機から発信されたプレゼンス要求をルーティングする方法を決定します。この設定では、電話機のプレゼンス (SUBSCRIBE) 要求のコール処理検索 スペースと別にコーリング サーチ スペースを適用できます。
SIP Profile	デフォルトの SIP プロファイルまたは以前に作成された特定のプロファイルを選択します。SIP プロファイルでは、登録タイマーおよびキープアライブ タイマー、メディア ポート、Do Not Disturb (サイレント) 制御など、電話機の特定の SIP 情報を提供します。
Digest User	(オプション) デフォルトの SIP プロファイルまたは以前に作成された特定のプロファイルを選択します。SIP プロファイルでは、登録タイマーおよびキープアライブ タイマー、メディア ポート、Do Not Disturb (サイレント) 制御など、電話機の特定の SIP 情報を提供します。

フィールド	説明
Media Termination Point Required	<p>このフィールドを使用して、H.323 がサポートしない機能（保留や転送など）を実装するために、メディア ターミネーション ポイントを使用するかどうかを指示します。</p> <p>機能を実装するために MTP を使用する場合は、[Media Termination Point Required] チェックボックスをオンにします。機能を実装するために MTP を使用しない場合は、[Media Termination Point Required] チェックボックスをオフにします。</p> <p>このチェックボックスは、H.323 クライアントと H.245 の機能セットをサポートしない H.323 デバイスの場合、または単一のソースから、メディア ストリーミングを終了させる場合のみ使用します。</p> <p>このチェックボックスをオンにして、MTP を必要とし、このデバイスがビデオ コールのエンドポイントになる場合、コールはオーディオのみになります。</p>
Unattended Port	このデバイスの不在ポートを指示する場合に、このチェックボックスをオンにします。
Require DTMF Reception	<p>この電話機と SIP および SCCP を実行する電話機の DTMF 受信が必要な場合に、このチェックボックスをオンにします。</p> <p><b>注：</b> Cisco Unified Mobility 機能の設定で、SIP トランク（Intercluster Trunk (ICT; クラスタ間トランク) またはゲートウェイ）経由で IP 電話のリモートの宛先としてクラスタ間 DN を使用する場合、エンタープライズ機能アクセス ミッドコール機能に重要な、DTMF 番号をアウト オブバンドで受信できるように、このチェックボックスをオンにします。</p>
<b>Certification Authority Proxy Function (CAPF) Information</b>	
Certificate Operation	<p>ドロップダウン リスト ボックスから、次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> <li>• No Pending Operation：証明書の操作が行われない場合に表示されます（デフォルトの設定）。</li> <li>• Install/Upgrade：電話機に新しい証明書をインストールするか、既存のローカルで有効な証明書をアップグレードします。</li> <li>• Delete：電話機に存在するローカルで有効な証明書を削除します。</li> <li>• Troubleshoot：Locally Significant Certificate (LSC; ローカルで有効な証明書) または Manufacture Installed Certificate (MIC; 製造元でインストールされる証明書) を取得し、CAPF トレース ファイルで証明書資格情報を表示できます。電話機に両方の証明書タイプが存在する場合、Cisco Unified Communications Manager は、証明書のタイプごとに 1 つずつ、2 つのトレース ファイルを作成します。</li> </ul> <p>[Troubleshooting] オプションを選択して、電話機に LSC または MIC が存在することを確認できます。</p>

フィールド	説明
Authentication Mode	<p>このフィールドでは、電話機が CAPF 証明書の操作時に使用する認証方法を選択できます。</p> <p>ドロップダウン リスト ボックスから、次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> <li>• <b>By Authentication String</b> : ユーザが電話機に CAPF 認証文字列を入力した場合にのみ、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。</li> <li>• <b>By Null String</b> : ユーザの介入なしで、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。 このオプションではセキュリティが確保されません。したがって、セキュアな閉じた環境の場合にだけこのオプションを選択することを強く推奨します。</li> <li>• <b>By Existing Certificate (Precedence to LSC)</b>: 電話機に <b>Manufacture Installed Certificate (MIC</b>; 製造元でインストールされる証明書) または <b>Locally Significant Certificate (LSC</b>; ローカルで有効な証明書) が存在する場合に、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に <b>LSC</b> が存在する場合、電話機に <b>MIC</b> が存在するかどうかに関係なく、<b>LSC</b> によって認証が行われます。電話機に <b>MIC</b> と <b>LSC</b> が存在する場合、<b>LSC</b> によって認証が行われます。電話機に <b>LSC</b> が存在しないが、<b>MIC</b> が存在する場合、<b>MIC</b> によって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在することを確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。 <b>MIC</b> と <b>LSC</b> が同時に電話機に存在できる場合でも、電話機が <b>CAPF</b> への認証に使用する証明書は常に 1 つだけです。優先されるプライマリ証明書が何らかの理由で破損した場合、または別の証明書を使用して認証を受ける場合は、認証モードを更新する必要があります。</li> <li>• <b>By Existing Certificate (Precedence to MIC)</b> : 電話機に <b>LSC</b> または <b>MIC</b> が存在する場合に、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に <b>MIC</b> が存在する場合、電話機に <b>LSC</b> が存在するかどうかに関係なく、<b>MIC</b> によって認証が行われます。電話機に <b>LSC</b> が存在するが、<b>MIC</b> が存在しない場合、<b>LSC</b> によって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在することを確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。</li> </ul> <p><b>注</b> : [Phone Security Profile] ウィンドウで設定される CAPF 設定は、[Phone Configuration] ウィンドウで設定される CAPF パラメータと連携します。</p>

フィールド	説明
Authentication String	<p>(オプション) [Authentication Mode] ドロップダウン リスト ボックスの [By Authentication String] オプションを選択した場合、このフィールドが適用されます。手動で文字列を入力するか、[Generate String] ボタンをクリックして、文字列を生成します。文字列には 4 桁から 10 桁含まれていることを確認します。</p> <p>ローカルで有効な証明書をインストール、アップグレード、削除、トラブルシューティングするには、電話機ユーザまたは管理者が電話機に認証文字列を入力する必要があります。</p>
Key Size (Bits)	<p>ドロップダウン リスト ボックスから証明書のキー サイズを選択します。デフォルト設定は 1024 です。その他のオプションには 512 と 2048 があります。</p> <p>デフォルトの設定より大きいキー サイズを選択すると、電話機は、キーの生成に必要なエントロピーを生成するために時間がかかります。キーの生成を低い優先順位で設定すると、操作の実行中に、電話機が機能します。電話機のモデルによっては、キーの生成が完了するまでに、30 分以上かかることがあります。</p> <p>注： [Phone Security Profile] ウィンドウで設定される CAPF 設定は、[Phone Configuration] ウィンドウで設定される CAPF パラメータと連携します。</p>
Operation Completes By	<p>(オプション) このフィールドは、[Install/Upgrade]、[Delete]、[Troubleshoot Certificate Operation] オプションをサポートし、操作を完了する必要がある日時を指定します。</p> <p>表示される値は、パブリッシャ データベース サーバに適用されます。</p>
<b>Extension Information</b>	
Enable Extension Mobility	
Log Out Profile	(オプション)
<b>MLPP Information</b>	
MLPP Domain	<p>(オプション) MLPP ドメインのドロップダウン リストから、このデバイスに関連付けられる MLPP ドメインを選択します。[None] 値のままにした場合、このデバイスはデバイスのデバイス プールに設定された値から、その MLPP ドメインを継承します。デバイス プールに MLPP ドメイン設定がない場合、このデバイスは、MLPP Domain Identifier エンタープライズ パラメータに設定された値からその MLPP ドメインを継承します。</p>
<b>Do Not Disturb</b>	
Do Not Disturb	<p>電話機の取り込み中をイネーブルにする場合は、このチェックボックスをオンにします。</p>

フィールド	説明
DND Option	<p>電話機の DND をイネーブルにすると、このパラメータによって、DND 機能の着信コールを処理する方法を指定できます。</p> <ul style="list-style-type: none"> <li>• <b>Call Reject</b> : このオプションは、着信コールの情報をユーザに提示しないことを指定します。DND Incoming Call Alert パラメータの設定に応じて、電話機はビープを再生するか、コールの点滅通知を表示します。</li> <li>• <b>Ringer Off</b> : このオプションは、呼出音をオフにしますが、着信コール情報がデバイスに表示されるため、ユーザはコールを受け付けることができます。</li> <li>• <b>Use Common Phone Profile Setting</b> : このオプションは [Common Phone Profile] ウィンドウの [DND Option] 設定をこのデバイスに使用することを指定します。</li> </ul> <p><b>注</b> : SCCP を実行している 7940/7960 電話機の場合、[Ringer Off] オプションのみを選択できます。携帯デバイスとデュアルモード電話機の場合、[Call Reject] オプションのみを選択できます。携帯デバイスまたはデュアルモード電話機で [DND Call Reject] をアクティブにすると、デバイスにコール情報が表示されません。</p>
DND Incoming Call Alert	<p>(オプション) [DND Ringer Off] または [Call Reject] オプションをイネーブルにした場合、このパラメータによってコールの表示方法を指定します。</p> <p>ドロップダウン リストから、次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> <li>• <b>None</b> : このオプションは、[Common Phone Profile] ウィンドウの [DND Incoming Call Alert] 設定をこのデバイスに使用することを指定します。</li> <li>• <b>Disable</b> : このオプションは、コールのビープと点滅通知の両方をディセーブルにしますが、[DND Ringer Off] オプションの場合、引き続き着信コール情報が表示されます。[DND Call Reject] オプションの場合、コールアラートが表示されず、デバイスに情報が送信されません。</li> <li>• <b>Beep Only</b> : 着信コールの場合、このオプションによって、電話機でビープ音のみが再生されます。</li> <li>• <b>Flash Only</b> : 着信コールの場合、このオプションによって、電話機で点滅アラートのみが表示されます。</li> </ul>



(注) Cisco UC Integration for Cisco WebEx Connect では、セキュアな電話機設定はサポートされていません。

- ステップ 6** [Save] を選択します。
- ステップ 7** [Apply Config] をクリックして、設定をアクティブにします。
- ステップ 8** [OK] をクリックします。
- ステップ 9** [Phone Configuration] ウィンドウの [Association Information] セクションで [Add a new DN] (電話番号) リンクを選択します。
- ステップ 10** [Directory Number Configuration] ウィンドウで、電話番号の情報を入力します。

- ステップ 11** [Save] を選択します。
- ステップ 12** [Directory Number Configuration] ウィンドウで、[Associate End Users] を選択します。
- ステップ 13** [Find and List Users] ウィンドウでユーザを検索し、ユーザを選択して [Add Selected] を選択します。
- ステップ 14** [Save] を選択します。
- ステップ 15** Cisco Unified Communications Manager Administration で [User Management] > [End User] を選択します。
- ステップ 16** [Find and List Users] ウィンドウでユーザを検索し、ユーザを選択します。
- ステップ 17** [Device Associations] グループの [Controlled Devices] リスト ボックスに、そのユーザのデバイスが表示されていることを確認します。

## Windows Vista の QoS パケットマーキング

Quality of Service (QoS) パケット マーキングには、Active Directory 2003 ドメイン内の Windows Vista コンピュータの管理者権限が必要です。そのため、ユーザはこのオペレーティング システムの制限を克服し、Active Directory 2003 ドメイン上の Windows Vista への CSF 配備の QoS パケット マーキングをイネーブルにするために、管理者権限が必要です。

Active Directory 2008 ドメイン内の Windows Vista コンピュータの場合、次の手順に説明するように、グループ ポリシーを使用して、この制限を克服できます。

## Windows Vista での Active Directory 2008 による CSF のパケット マーキングのイネーブル化

### 手順

- ステップ 1** グループ ポリシー管理エディタ アプリケーションを起動します。
- ステップ 2** [User Configuration] ノードを展開します。
- ステップ 3** [Policies] > [Windows Settings] で、[Policy-based QoS] を右クリックし、[Create new policy] を選択します。  
たとえば、Cisco CSF UDP というポリシーを作成します。
- ステップ 4** [Specify DSCP Value] をオンにし、値として 46 と入力し、Expedited Forwarding (EF; 緊急転送) としてトラフィックをマークします。
- ステップ 5** [Next] を選択します。
- ステップ 6** [Only applications with this executable name] オプションを選択し、次の実行可能ファイル名を入力します。  
cucsf.exe
- ステップ 7** [Next] を選択します。
- ステップ 8** QoS ポリシーを任意のソース IP アドレスと宛先 IP アドレスのペアに適用することを指定します。これを実行するには、次のオプションを選択します。
- Any source IP address
  - Any destination IP address
- ステップ 9** [Next] を選択します。

**ステップ 10** QoS ポリシーを適用するプロトコルを選択し、トラフィックのソースと宛先のポートまたはポート範囲を指定します。

たとえば、UDP を選択し、[From any source port] と [To any destination port] を選択します。

**ステップ 11** [Finish] を選択します。

**ステップ 12** 作成したグループ ポリシーをクライアント コンピュータに適用します。

上の例のクライアント コンピュータに適用される設定は次のようになります。

```
[HKEY_CURRENT_USER¥Software¥Policies¥Microsoft¥Windows¥QoS¥Cisco CSF UDP]
```

```
"Version"="1.0"
```

```
"Application Name"="cucsf.exe"
```

```
"Protocol"="UDP"
```

```
"Local Port"="*"
```

```
"Local IP"="*"
```

```
"Local IP Prefix Length"="*"
```

```
"Remote Port"="*"
```

```
"Remote IP"="*"
```

```
"Remote IP Prefix Length"="*"
```

```
"DSCP Value"="46"
```

```
"Throttle Rate"="-1"
```





## CHAPTER 3

# ダイヤリング ルールの設定とインストール

ダイヤリング ルールは、ディレクトリ サービスと Cisco Unified Communications Manager の間で電話番号を変換します。

アプリケーション ダイヤリング ルールは、ユーザがダイヤルした電話番号に対して、そこから自動的に番号を除去するか、そこに番号を追加します。たとえば、外線発信する場合にはアプリケーションのダイヤル ルールにより、7 桁の電話番号の先頭に番号 9 が自動で付加されます。ディレクトリ検索ルールは、発信者の識別情報をディレクトリで検索可能な番号に変換します。

連絡先の名前解決のためにダイヤリング ルールのセットを作成する必要があります。ダイヤリング ルールが変更されるたびに、アプリケーション ダイヤリング ルールとディレクトリ検索ダイヤリング ルールを設定してエクスポートする必要があります。Cisco Unified CSF クライアントは、作成された XML ファイルをダウンロードしてその内容を解釈します。

連絡先の名前解決は、Cisco UC Integration for Cisco WebEx Connect によって提供されているすべての機能を利用するために必要となります。ユーザが各自のプロファイル設定に入力した番号は、Cisco Unified Communications Manager の設定と同期している必要があります。これらの番号は、Cisco WebEx Connect Administration Console で設定することもできます。



ヒント

これらのルールが存在し、使用可能であることは、必須の要件です。ダイヤリングに関連するほとんどの問題は、ルールが存在しない、ルールが古い、ルールが無効である、のいずれかに起因します。

## ダイヤリング ルールの設定

ダイヤリング ルールに関する概念のおよび作業ベースの詳細な情報については、Cisco Unified Communications Manager Administration のオンライン ヘルプまたは『Cisco Unified Communications Manager Administration Guide』および『Cisco Unified Communications Manager System Guide』を参照してください。

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html)

次のタイプのルールが必要です。

- アプリケーション ダイヤリング ルール
- ディレクトリ検索ダイヤリング ルール



(注)

これらのルールがすでに他のシスコ アプリケーションのために設定されている場合があります。ルールが存在する場合は、次の手順をスキップしてかまいません。

## ダイヤリング ルール のインストール

Cisco Unified Communications Manager でダイヤリング ルールを使用する場合は、Cisco UC Integration for Cisco WebEx Connect が、そのダイヤリング ルールにアクセスできるようにする必要があります。

Cisco Options Program (COP) ファイルを実行して、ダイヤリング ルールのコピーを XML 形式で生成します。Cisco UC Integration for Cisco WebEx Connect はこの XML ファイルにアクセスしてダウンロードし、その内容を解釈します。COP ファイルは Administration Toolkit から入手できます。Administration Toolkit にアクセスするには、次の URL にある [Download Software] ページから [Cisco UC Integration for Cisco WebEx Connect] に移動します。

<http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240>

### 手順

- 
- ステップ 1 Cisco Unified Operating System Administration で [Software Upgrades] > [Install/Upgrade] を選択します。
  - ステップ 2 [New install] を選択します。
  - ステップ 3 [Software Installation/Upgrade] ウィンドウで、COP ファイルのソースを指定します。
  - ステップ 4 [Next] を選択します。
  - ステップ 5 [Available Software] リスト ボックスから、適切な COP ファイルを選択します。
  - ステップ 6 [Next] を選択します。
  - ステップ 7 [Install] を選択します。
- 

## ダイヤリング ルール のインストールの確認

TFTP サーバの /usr/local/cm/tftp/CUPC ディレクトリに次のファイルがあることを確認します。

- AppDialRules.xml
- DirLookupDialRules.xml

## TFTP サービスの再起動

ダイヤリング ルールのコピーが生成されていることを確認したら、TFTP サービスを再起動します。TFTP サービスは、COP ファイルを実行した各サーバについて再起動する必要があります。

TFTP サービスの再起動方法については、次の URL の『Cisco Unified Serviceability Administration Guide』を参照してください。

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html)



## CHAPTER 4

# Standard CTI ユーザ グループへのユーザの追加

Cisco UC Integration for Cisco WebEx Connect でユーザのデスクフォンを制御できるようにするには、ユーザのデバイスを作成するときに [Allow Control of Device from CTI] オプションを選択する必要があります。また、ユーザが Standard CTI Enabled ユーザ グループに追加されるようにする必要があります。

ユーザの電話機が Cisco Unified IP Phone 6900、8900、または 9900 シリーズ モデルの場合は、Standard CTI Allow Control of Phones supporting Connected Xfer and conf ユーザ グループにもそのユーザを追加する必要があります。

### 手順

- ステップ 1** Cisco Unified Communications Manager Administration で [User Management] > [End User] を選択します。
- ステップ 2** 追加するユーザを選択します。
- ステップ 3** [End User Configuration] ウィンドウの [Permissions Information] グループにある [Add to User Group] を選択します。
- ステップ 4** [Find and List User Groups] ウィンドウで、「Standard CTI」を検索します。
- ステップ 5** [Standard CTI Enabled] ユーザ グループを選択します。  
ユーザの電話機が Cisco Unified IP Phone 6900、8900、または 9900 シリーズ モデルの場合は、[Standard CTI Allow Control of Phones supporting Connected Xfer and conf] ユーザ グループも選択します。
- ステップ 6** [Add Selected] を選択します。
- ステップ 7** [End User Configuration] ウィンドウで [Save] を選択します。

## ユーザの新規作成

### 手順

- ステップ 1** Cisco Unified Communications Manager Administration で [User Management] > [End User] を選択します。
- ステップ 2** [Add New] を選択します。

## ステップ 3 該当する場合、ユーザ資格情報を入力します。

フィールド	説明
User ID	一意のエンド ユーザ識別名を入力します。英数字および特殊文字を含む任意の文字を入力できます。このフィールドの文字の制限はありません。
Password	英数字または特殊文字を使用して、エンド ユーザのパスワードを入力します。割り当てられている資格情報ポリシーに指定されている文字数以上 (1 ~ 127 文字) を入力する必要があります。
Confirm Password	エンド ユーザ パスワードを再入力します。
PIN	エンド ユーザ PIN の数字を入力します。割り当てられている資格情報ポリシーに指定されている文字数以上 (1 ~ 127 文字) を入力する必要があります。
Confirm PIN	PIN を再入力します。
Last Name	エンド ユーザの姓を入力します。
Middle Name	エンド ユーザのミドル ネームを入力します。
First Name	エンド ユーザの名を入力します。
Telephone Number	エンド ユーザの電話番号を入力します。次の特殊文字を使用できません: (、)、-
Mail ID	エンド ユーザの電子メール アドレスを入力します。
Manager User ID	エンド ユーザ マネージャ ID のユーザ ID を入力します。  <b>ヒント:</b> 入力するマネージャ ユーザ ID は、エンド ユーザと同じクラス内に存在する必要はありません。したがって、Cisco Unified Communications Manager では、データベース内にすでに存在するユーザ ID を入力する必要はありません。
Department	エンド ユーザの部門情報 (部門番号または部門名など) を入力します。
User Locale	ドロップダウン リスト ボックスから、エンド ユーザに関連付けるロケールを選択します。ユーザ ロケールは、言語やフォントなどのエンド ユーザをサポートするための一連の詳細情報を特定します。  <b>注:</b> エンド ユーザ ロケールを選択しない場合、Cisco CallManager サービス パラメータで、デフォルト ユーザ ロケールとして指定したロケールが適用されます。
Associated PC	この必須フィールドは、Cisco IP Softphone ユーザに適用されます。
Digest Credentials	英数字の文字列を入力します。  Cisco Unified Communications Manager は、ここで指定したダイジェスト信用証明書を使用して、ダイジェスト認証時に電話機が提供する資格情報を検証します。このフィールドに入力したダイジェスト資格情報は、[Phone Configuration] ウィンドウで、ダイジェスト ユーザを選択した場合に、電話機に関連付けられます。  <b>注:</b> ダイジェスト認証の詳細については、『Cisco Unified Communications Manager Security Guide』を参照してください。
Confirm Digest Credentials	ダイジェスト資格情報の入力が入力が正しいことを確認するために、このフィールドに再度資格情報を入力します。

**ステップ 4** [Device Information] とプロフィールを選択します。

サポートされるデバイスのリストは「サポートされる Cisco Unified IP Phone」(P.1-3) を参照してください。

**ステップ 5** [Extension Mobility] パラメータを選択します。

フィールド	説明
Available Profiles	このリスト ボックスには、このエンド ユーザとの関連付けに使用可能なエクステンション モビリティ プロファイルが表示されます。 エクステンション モビリティ プロファイルを検索するには、[Find] をクリックします。表示される [Find and List Device Profiles] ウィンドウを使用して、必要なエクステンション モビリティ プロファイルを検索します。 エクステンション モビリティ プロファイルをこのエンド ユーザに関連付けるには、プロフィールを選択し、このリスト ボックスの下の下向き矢印をクリックします。
Controlled Profiles	このフィールドには、Cisco Extension Mobility に設定されているエンド ユーザに関連付けられている制御デバイス プロファイルのリストが表示されます。
Default Profile	ドロップダウン リスト ボックスから、このエンド ユーザのデフォルトのエクステンション モビリティ プロファイルを選択します。
Presence Group	プレゼンス機能でこのフィールドを設定します。 ドロップダウン リスト ボックスから、エンド ユーザのプレゼンス グループを選択します。選択したグループは、エンド ユーザがモニタ可能な宛先を指定します。 プレゼンス グループのデフォルト値は、Standard Presence グループを指定し、インストール時に設定されます。Cisco Unified Communications Manager Administration に設定されたプレゼンス グループはドロップダウン リスト ボックスにも表示されます。 プレゼンス認証はプレゼンス グループと連携し、グループ間のプレゼンス要求を許可またはブロックします。グループ間の許可の設定およびプレゼンスのエクステンション モビリティとの連携については、『Cisco Unified Communications Manager Features and Services Guide』の「Presence」の章を参照してください。
SUBSCRIBE Calling Search Space	プレゼンス機能によってサポートされる SUBSCRIBE コーリング サーチ スペースは、Cisco Unified Communications Manager がエンド ユーザから発信されたプレゼンス要求をルーティングする方法を決定します。この設定では、エンド ユーザのプレゼンス (SUBSCRIBE) 要求のコール処理サーチ スペースと別にコーリング サーチ スペースを適用できます。 ドロップダウン リスト ボックスから、エンド ユーザのプレゼンス要求に使用する SUBSCRIBE コーリング サーチ スペースを選択します。Cisco Unified Communications Manager Administration で設定するすべてのコーリング サーチ スペースが [SUBSCRIBE Calling Search Space] ドロップダウン リスト ボックスに表示されます。 ドロップダウン リスト から、エンド ユーザに別のコーリング サーチ スペースを選択しない場合、SUBSCRIBE コーリング サーチ スペースのデフォルトは [None] に設定されます。

フィールド	説明
Allow Control of Device from CTI	このチェックボックスがオンにされている場合、ユーザがデバイスにログインすると、AllowCTIControlFlag デバイス プロパティがアクティブになり、CTI アプリケーションからデバイスを制御できるようになります。ユーザがデバイスにログインするまで、この設定は無効です。 <b>注：</b> エンドユーザ設定の [Allow Control of Device from CTI] 設定によって、ユーザがログインするデバイスの AllowCTIControlFlag デバイス プロパティが上書きされます。
Enable Extension Mobility Cross Cluster	このエンドユーザが Cisco クラスタ間のエクステンションモビリティ機能を使用できるようにする場合に、このボックスをオンにします。

#### ステップ 6 電話番号の関連付けを選択します。

フィールド	説明
Primary Extension	このフィールドは、エンドユーザのプライマリ電話番号を表します。エンドユーザは、電話機に複数の回線を接続できます。  デバイスをエンドユーザに関連付ける場合、関連付けられたデバイスに設定された電話番号が、[Primary Extension] のドロップダウンリストボックスで使用できるようになります。ドロップダウンリストボックスから、このエンドユーザのプライマリ内線を選択します。  システムが Cisco Unity Connection に統合されている場合、[Related Links] メニューに [Create Cisco Unity User] リンクが表示されます。
IPCC Extension	ドロップダウンリストボックスから、このエンドユーザの IPCC 内線を選択します。 <b>注：</b> このフィールドは、IPCC Express によってインストールされたエンタープライズパラメータが [True] に設定されている場合にのみ表示されます。

ステップ 7 モビリティ情報を選択します。

フィールド	説明
Enable Mobility	<p>モバイル コネクトをアクティブにする場合に、このチェックボックスをオンにします。これにより、ユーザは、単一の電話番号を使用してコールを管理し、デスクトップフォンと携帯電話の実行中のコールをピックアップすることができます。</p> <p>このチェックボックスをオンにすると、モバイル コネクトのデバイス ライセンス ユニットを使用するライセンスがトリガーされ、[Primary User Device] ドロップダウンリスト ボックスと連携します。</p> <p>[Enable Mobility] チェックボックスをオンにし、[Primary User Device] ドロップダウンリスト ボックスから付属デバイスを選択できない場合、[License Unit Calculation] ウィンドウの [Mobility Enabled End Users] 行に示されているように、4 つの Device License Unit (DLU; デバイス ライセンス ユニット) が使われます。</p> <p>Cisco Unified Mobility をイネーブルにし、後で、[Primary User Device] ドロップダウンリスト ボックスから付属デバイスを選択すると、[License Unit Calculation] ウィンドウの [Mobility Enabled End Users] 行に示されているように、システムによって 2 つの DLU が与えられます。</p>
Primary User Device	<p>[Primary User Device] ドロップダウン リスト ボックスは、[Enable Mobility] チェックボックスと連携し、モバイル コネクトの付属デバイスに使用されるデバイス ライセンス ユニット数を制御します。</p> <p>[Enable Mobility] チェックボックスをオンにしたら、Cisco Unified Mobility のユーザに明示的に割り当てる付属デバイスを選択します。たとえば、ユーザが Cisco Unified Mobility で携帯電話に加えて使用するデスクトップフォンなどのデバイスを選択します。</p> <p>付属デバイスを選択する前に、次の情報を考慮します。</p> <ul style="list-style-type: none"> <li>• 複数の Device License Unit (DLU; デバイス ライセンス ユニット) を使用するデバイスのみがドロップダウンリスト ボックスに表示されます。</li> <li>• Cisco Unified Mobility の場合、同じデバイスを複数のユーザに割り当てることができないため、割り当て可能なデバイスのみがドロップダウンリスト ボックスに表示されます。</li> <li>• [Enable Mobility] チェックボックスをオンにし、ドロップダウンリスト ボックスからデバイスを選択すると、[Licensing Unit Calculation] ウィンドウの [Mobility Enabled End Users (Adjunct)] 行に示されているように、2 つの DLU が使われます。</li> <li>• モバイル コネクトをイネーブルにした後に、Cisco Unified Communications Manager Administration からデバイスを削除するか、割り当てを削除した場合、[License Unit Calculation] ウィンドウの [Mobility Enabled End Users] 行に示されているように、デバイスの削除または割り当ての削除後に、2 つの DLU が使われます。</li> </ul>
Enable Mobile Voice Access	<p>ユーザがモバイル ボイス アクセス Integrated Voice Response (IVR; 自動音声応答) システムにアクセスして、モバイル コネクト コールを起動し、モバイル コネクト機能をアクティブまたは非アクティブにできるようにする場合に、このチェックボックスをオンにします。</p>

フィールド	説明
Maximum Wait Time for Desk Pickup	携帯電話からデスクトップフォンに転送されたコールをユーザがピックアップするまでに許可する最大の時間をミリ秒単位で入力します。
Remote Destination Limit	ユーザのデスクトップフォンからコールの転送が許可される電話機の最大数を入力します。
Remote Destination Profiles	このフィールドには、このユーザに作成されたリモート接続先プロファイルが一覧表示されます。特定のリモート接続先プロファイルの詳細を表示するには、リストのリモート接続先プロファイルを選択し、[View Details] リンクをクリックします。



## CHAPTER 5

# Cisco UC Integration for Cisco WebEx Connect のインストールと設定

Cisco UC Integration for Cisco WebEx Connect をインストールする前に、システムが必要な前提条件をすべて満たしていることを確認します。次の URL にあるリリース ノートを参照し、必要な正しいバージョンのソフトウェアがすべてインストールされていることを確認してください。

[http://www.cisco.com/en/US/products/ps10627/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps10627/prod_release_notes_list.html)

[http://www.webex.com/m/connectreleasenotes\\_c6.pdf](http://www.webex.com/m/connectreleasenotes_c6.pdf)

## インストール パッケージの内容

Cisco UC Integration for Cisco WebEx Connect インストール パッケージには、次のものが含まれています。

- 実行可能ファイル。ユーザは、各自のコンピュータで実行可能ファイルを実行できます。
- Microsoft Installer (MSI) ファイル。これは、Active Directory グループ ポリシー、Microsoft System Management Server (SMS)、Altiris などのプッシュ メカニズムにおけるサイレント インストールに使用されます。

## Cisco UC Integration for Cisco WebEx Connect の設定

Cisco WebEx Connect を Cisco Unified Client Services Framework と連携して機能するように設定する 2 つの方法があります。

1. Cisco WebEx Connect Administration Console を使用する。詳細については、WebEx Connect Administration Console のオンライン ヘルプを参照してください。これは推奨される設定方法です。ヘルプは次の URL にあります。

<http://www.webex.com/webexconnect/orgadmin/help/index.htm>



**(注)** 複数の Cisco Unified CSF クライアントを使用することは、サポートされているシナリオではありません。

2. Cisco WebEx Connect の [Settings] ページにある [Unified Communications] タブに設定を入力する。この方法を使用する場合は、バックアップ サーバを設定できないことに注意してください。

3. [Settings] ページの詳細については、次の URL にある Cisco WebEx Connect のヘルプを参照してください。

<http://www.webex.com/webexconnect/help/wwhelp.htm>



## CHAPTER 6

# Cisco Unity と Unity Connection Server の設定

## Cisco Unity Server

Cisco Unity は、コールを受け、グリーティングを再生し、ボイスメールを記録および符号化します。Cisco Unity はボイスメールを受信すると、電子メールに .wav ファイルを追加し、それを設定された電子メール アカウントに送信します。Cisco Unity は、メッセージ保管用のメールストア サーバとして使用するために Microsoft Exchange サーバにユーザ メールボックスを作成します。

Cisco Unified Communications Integration for Cisco WebEx Connect ユーザがボイスメールを聞く場合、Cisco Unified Communications Integration を使用して、IMAP 経由でメールストア サーバからそれらを取得します。

Cisco Unified Communications Integration は Cisco Unity ユニファイドメッセージと Cisco Unity ボイス メッセージの両方の設定をサポートします。ユニファイド メッセージでは、Exchange Server 電子メール アカウントはボイスメールと電子メールの両方をサポートします。ボイス メッセージでは、Exchange Server 電子メール アカウントにはボイスメール メッセージだけが含まれています。

### はじめに

- Cisco Unity のサポートされるリリースをインストールし、設定します。
- Cisco Unified Communications Manager と Cisco Unity を統合します。両サーバとも、ボイスメール ポートを設定するように、インストールされ、稼動している必要があります。
- SSL を使用してメールストア サーバとのセキュアな伝送を実現する場合は、インストールまたはアップグレード時に（あるいは、インストールまたはアップグレードの完了後の任意の時点で）、SSL を使用するように Cisco Unity を設定する必要があります。認証局として機能するようにサーバを指定し、証明書要求を送信し、証明書を発行して Cisco Unity サーバにインストールする必要があります。

## 手順

**ステップ 1** IMAP 仮想サーバを使用するように Microsoft Exchange サーバを設定します。

このリリースを設定するには	操作内容
Microsoft Exchange 2003	<ol style="list-style-type: none"> <li>a. [Start] &gt; [All Programs] &gt; [Microsoft Exchange] &gt; [System Manager] を選択します。</li> <li>b. [System Manager] の左側のセクションで、[Servers] を展開します。</li> <li>c. サーバ名を選択します。</li> <li>d. [Protocols] &gt; [IMAP] を選択します。</li> <li>e. 右クリックし、[Start Server] を選択します。</li> </ol>
Microsoft Exchange 2007	<ol style="list-style-type: none"> <li>a. [Start] &gt; [Run] を選択し、「services.msc」と入力し、[OK] をクリックします。</li> <li>b. [Microsoft Exchange IMAP4] サービスを選択し、[Start] をクリックします。このサービスはデフォルトでは開始されません。</li> </ol>

**ステップ 2** ポートおよび暗号化タイプを設定します。

このサーバを設定するには	操作内容
Microsoft Exchange 2003	<ol style="list-style-type: none"> <li>a. [IMAP Virtual Server] を右クリックし、[Properties] を選択します。</li> <li>b. [Access] タブから [Authentication] をクリックします。 <ul style="list-style-type: none"> <li>- [Requires SSL/TLS Encryption] がオフで、TCP および SSL 接続を使用するようになっていることを確認します。</li> <li>- [Requires SSL/TLS Encryption] がオンで、SSL だけを使用するようになっていることを確認します。</li> </ul> </li> <li>c. [OK] を選択します。</li> </ol>
Microsoft Exchange 2007	<ol style="list-style-type: none"> <li>a. [Start] &gt; [Programs] &gt; [Microsoft Exchange Server 2007] &gt; [Exchange Management Shell] を選択します。</li> <li>b. Exchange PowerShell 経由で IMAP4 サービスを実行しているクライアントアクセスサーバの認証設定を指定します。</li> </ol> <p>注：Microsoft Exchange 2007 はデフォルトで SSL を使用します。</p> <ol style="list-style-type: none"> <li>c. 適切に設定するために次のコマンドのいずれかを実行します。 <ul style="list-style-type: none"> <li>- プレーンテキストログインの場合：<b>set-imapsettings -LoginType PlainTextLogin</b></li> <li>- SSL の場合：<b>set-imapsettings -LoginType SecureLogin</b></li> </ul> </li> </ol>

**ステップ 3** ユーザを設定します。

- ユーザが既存の Cisco Unity ユーザである場合、ユーザを Cisco Unified Communications Manager データベースと Cisco Unified Presence に追加します。

- ユーザが新規ユーザの場合、ユーザを Cisco Unified Communications Manager データベース、Cisco Unity (これはユーザを Exchange と Active Directory に追加する)、Cisco Unified Presence に追加します。

**ステップ 4** 新規および既存のユーザのメールボックスを作成します。詳細については、Exchange Server のマニュアルを参照してください。

**ステップ 5** (オプション) 次の手順に従って安全なメッセージ機能をイネーブルにします。

- a. ユーザ テンプレートに変更を加えるには、[Subscribers] > [Subscribers] > [Features] を選択します。

ここで加えた変更は、このテンプレートを使用して作成された既存のユーザ アカウントには適用されません。変更後にこのテンプレートを使用して作成されるユーザ アカウントにだけ適用されます。

- b. 安全なメッセージ機能を有効にするには、[Message Security When Sending a Message] リストからオプションを選択します。たとえば、[Encrypt All Messages] を選択します。

この設定では、ユーザがメッセージを他のユーザに送信するときにメッセージを暗号化するかどうかを指定します。

- c. [Save] を選択します。

- d. 適宜ユーザまたはユーザ テンプレートを追加するには、これらの手順を繰り返します。

**ステップ 6** (オプション) 身元不明発信者からのメッセージに対して安全なメッセージ機能を有効にします。

- a. [System] > [Configuration] > [Message Security Settings] を選択します。

- b. 身元不明発信者からのメッセージを暗号化するかどうかを指定します。リストからオプションを選択します。

- c. [Save] を選択します。

#### トラブルシューティングのヒント

Cisco Unified Communications Integration ユーザは [Cisco Unified Communications Integration Preferences] ウィンドウに Cisco Unity 資格情報を入力する必要があります。

## Cisco Unity Connection Server

Cisco Unity Connection は Cisco Unified Communications Integration for Cisco WebEx Connect ユーザに Cisco Unified Communications Integration インターフェイスから、ボイスメール メッセージを表示、再生、ソート、削除する機能を提供します。

#### はじめに

- Cisco Unity Connection のサポートされるリリースをインストールし、設定します。
- Cisco Unified Communications Manager と Cisco Unity Connection を統合します。両サーバとも、ボイスメール ポートを設定するように、インストールされ、稼動している必要があります。

#### 手順

**ステップ 1** 新規のユーザを追加します。

- a. 左側のセクションの [Users] を展開します。
- b. [New User] を選択します。
- c. [Edit] > [Password Settings] を選択します。

- d. [Choose Password] ドロップダウンボックスで、[Web Application] を選択します。
- e. [User Must Change at Next Sign-In] を選択解除します。
- f. [Save] をクリックします。
- g. [Edit] > [Change Password] を選択します。
- h. 新しいパスワードを設定します。

### ステップ 2 ユーザを設定します。

ユーザが既存の Cisco Unity Connection ユーザの場合、それらを Cisco Unified Communications Manager データベースに追加します。

ユーザが新しい Cisco Unified Communications Integration ユーザの場合、ユーザを Cisco Unified Communications Manager データベースと Cisco Unity Connection に追加します。

### ステップ 3 (オプション) 次の手順に従って、ユーザに対する不明な発信者からのメッセージのセキュリティの処理方法を指定します。

- a. 左側のセクションの [Users] を展開します。
- b. [User] を選択します。
- c. ユーザのエイリアスを選択します。
- d. [Edit] > [Message Settings] を選択します。  
[Unidentified Callers Message Security] で、[Mark Secure] チェックボックスをオンにします。

### 手順

### ステップ 1 Cisco Unity Connection Administration で新規または既存のサービス クラスをセットアップして、Internet Mail Access Protocol (IMAP) クライアントからボイス メッセージにアクセスできるようにします。

- a. 左側のセクションの [Class of Service] を展開します。
- b. [Class of Service] を選択します。
- c. [Search Class of Service] ウィンドウの [Search Results] テーブル内で適切なサービス クラスの表示名を選択します。
- d. [Features] の下にある [Allow Users to Use Unified Client to Access Voice Mail] チェックボックスをオンにします。
- e. [Licensed Features] の下にある [Allow Users to Access VoiceMail Using an IMAP Client] チェックボックスをオンにします。
- f. [Allow Users to Access Message Bodies] を選択します。
- g. [Save] を選択します。

### ステップ 2 (オプション) 次の手順に従って安全なメッセージ機能をイネーブルにします。

- a. 左側のセクションの [Class of Service] を展開します。
- b. [Class of Service] を選択します。
- c. [Message Options] セクション内の [Require Secure Messaging] のオプションを選択して、セキュアなメッセージを有効にします。

### ステップ 3 Cisco Unity Connection サーバで、Cisco Unified Communications Integration ユーザごとにボイスメールボックスを使用して、Connection ユーザ アカウントを作成します。



(注)

Cisco Unity Connection のユーザ ID は Cisco Unified Presence または Cisco Unified Communications Integration のユーザ ID と一致している必要はありません。Cisco Unified Communications Integration には独立したボイスメール ID があり、これは、アプリケーションの [Preference] ウィンドウで設定します。ただし、Cisco Unified Communications システム全体で同じユーザ ID を使うことは役に立つことがあります。

**ステップ 4** まだ存在しない場合は、Cisco Unity Connection の管理ページで適用可能なユーザ アカウントの Web アプリケーションパスワードを指定します。

#### トラブルシューティングのヒント

- ユーザは、Cisco Unified Communications Integration アプリケーションで、ボイスメール資格情報、つまり、ユーザ名とパスワードを入力する必要があります。
- サーバへの問い合わせが可能で、ユーザ資格情報が正しいにもかかわらず、ボイスメール メッセージがダウンロードされない場合は、次の手順を実行します。
  - ポート 7993 の設定をチェックします。Cisco Unity Connection がポート 7993 でリッスンしていることを確認します。
  - ファイアウォールの設定を確認します。リモート コンピュータから、Cisco Unified Communications Integration を実行しているコンピュータに Telnet を実行し、ファイアウォールに接続できることを確認します。Cisco Unified クライアント サービス フレームワーク実行可能ファイル (connect.exe) が、該当するサーバとポートで TCP、TLS、SSL を使用して、IMAP ネットワーク接続を確立することを許可します。

#### ボイスメール機能をイネーブルにする

- ステップ 1** [Class of Service] ページ > [Voicemail User COS] を開きます。
- ステップ 2** [Licensed Features] セクションで、次の 2 つのオプションをオンにします。
- ステップ 3** Allow Users to Access Voice Mail Using an IMAP Client and/or Single Inbox
- ステップ 4** Allow Users to Use the Messaging Inbox and RSS Feeds

## Cisco Unity を使用した導入のための Microsoft Exchange の IMAP セキュリティ設定の確認

### はじめに

このトピックの情報に関する質問は、Microsoft Exchange 管理者または Cisco Unity 管理者に問い合わせてください。

### 手順

- ステップ 1** IMAP がセキュアか非セキュアかを確認します。
- Microsoft Exchange 2003 の場合 :
- a. [Start] > [All Programs] > [Microsoft Exchange] > [System Manager] を選択します。
  - b. [Administrative Groups] > [First Administrative Group] > [Servers] > [<サーバ名>] > [Protocols] > [IMAP4] を選択します。

- c. [Default IMAP4 Virtual Server] を右クリックし、[Properties] を選択します。
- d. [Access Control] セクションで [Access] を選択し、[Authentication] を選択します。
- e. [Requires SSL/TLS encryption] 選択されていることを確認します。

Microsoft Exchange 2007 の場合は、[Start] > [All Programs] > [Microsoft Exchange Server 2007] > [Exchange Management Console] で、関連の設定に移動します。

**ステップ 2** Internet Information Services (IIS) のセキュリティ設定を確認します。

- a. [Start] > [Programs] > [Administrative Tools] > [Internet Information Services (IIS) Manager] を選択します。
- b. [<コンピュータ名>(local computer)] > [Web Sites] > [Default Web Site] を選択します。
- c. [Default Web Site] を右クリックし、[Properties] を選択します。
- d. [Directory Services] を選択します。
- e. [Secure Communications] セクションで、[Edit] を選択します。
- f. [Require secure channel (SSL)] が有効であるかを確認します。

#### 次の作業

IMAP がセキュアな場合、ボイスメール アダプタを設定する際に、[Transport Type] で [TLS] を選択する必要があります。それ以外の場合は [TCP] を選択します。

TLS を選択する場合

- [Trust Policy] を [Trusted Certificates] に設定したセキュリティ コンテキストを指定します。
- Exchange Server によって証明書を交換します。
- Cisco Unified Mobility Advantage との証明書の交換については、次のセキュリティに関するドキュメント モジュールを参照してください。
- [http://www.cisco.com/en/US/products/ps7270/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html)



## CHAPTER 7

# Cisco Unified Communications Manager の設定とボイスメールの要件

## DTMF アクセス コードに関する重要な情報

Cisco Unified Communications Manager で設定するすべての DTMF アクセス コードは、相互に排他的である必要があります。デフォルトのモビリティ DTMF アクセス コードが、他の通話中の DTMF アクセス コードと重複しないようにしてください。

たとえば、デフォルトで、モビリティ機能と Cisco Unity の両方で通話中の機能にアスタリスク (\*) が使用されると、両アプリケーションの DTMF 機能が正しく動作しなくなります。

これは Cisco Unified Mobility Advantage に固有の問題ではありませんが、Cisco Unified Mobile Communicator のユーザがボイスメールにアクセスする場合、または通話中の機能を使用する場合に悪影響を与えます。

DTMF アクセス コードを設定するには、ご使用のリリースの Cisco Unified Communications Manager マニュアルを参照してください。

## ボイスメールの要件

ビジュアル ボイスメールを使用するための前提条件は次のとおりです。

- サポートされるトランスコーディング プロトコルをシステムで使用できることを確認します。互換性マトリクスを参照してください。  
[http://www.cisco.com/en/US/products/ps7270/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html)
- IMAP が有効になっていることを確認します。
  - Cisco Unity の場合：  
[http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products\\_configuration\\_example09186a00809d8c91.shtml](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_configuration_example09186a00809d8c91.shtml) にある『Using IMAP4 to Access Voice Messages in Cisco Unity System with Exchange 2007』を参照してください。
  - Cisco Unity Connection を使用する場合：  
[http://www.cisco.com/en/US/products/ps6509/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html) の『System Administration Guide Cisco Unity Connection Release 7.x』の「Configuring IMAP Settings」を参照してください。
- ボイスメールにアクセスするための DTMF コードが Cisco Unified Communications Manager 内で固有であることを確認します。「[DTMF アクセス コードに関する重要な情報](#)」(P.3) を参照してください。

- 複数の Exchange サーバまたはボイスメール サーバのユーザを扱う場合は、Exchange サーバまたはボイスメール ストアごとに個別のボイスメール アダプタを作成します。



## CHAPTER 8

# マニュアルの入手方法およびテクニカルサポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『What's New in Cisco Product Documentation』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

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

『What's New in Cisco Product Documentation』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

## マニュアルの検索

- マニュアルの一覧については、  
[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cuciwex/roadmap/cuciconnect\\_map.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cuciwex/roadmap/cuciconnect_map.html) にある『*Documentation Guide for Cisco Unified Communications Integration (TM) for Cisco WebEx Connect*』を参照してください。
- Cisco WebEx Connect Administration Console :  
<http://www.webex.com/webexconnect/orgadmin/help/index.htm>
- Cisco Unified Communications Manager のマニュアル  
『Cisco Unified Communications Manager Documentation Guide』およびお使いの Cisco Unified Communications Manager リリースに対応した資料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](http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html)
- Cisco WebEx Connect オンライン ヘルプ :  
<http://www.webex.com/webexconnect/help/wwhelp.htm>

