Cisco Unified Communications Manager システム設定ガイド, リリース 14 および SUs

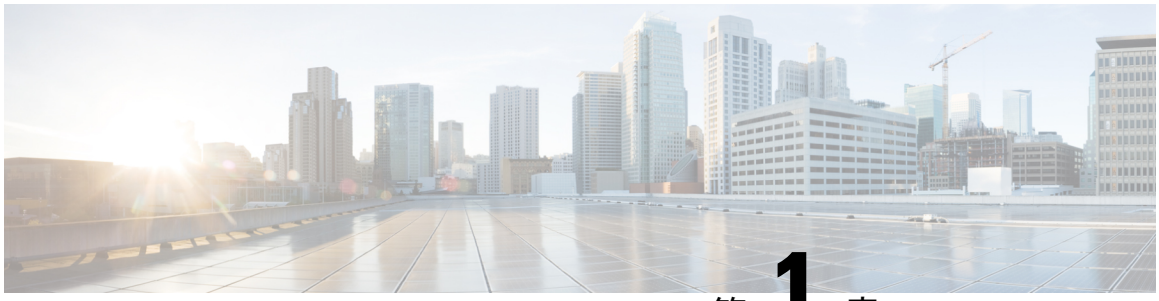
初版：2022 年 6 月 16 日

最終更新：2023 年 5 月 18 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

新規および変更情報

新規および変更情報

次の表は、この最新リリースに関するこのガイドでの機能に対する大幅な変更の概要を示したものです。ただし、このリリースに関するガイドの変更点や新機能のなかには、この表に記載されていないものもあります。

表 *1 : Unified Communications Manager* と *IM* およびプレゼンスサービスでの新機能と変更された動作

機能または変更	説明	参照先	日付（Date）
リリース 14 ドキュメントの初回リリース	—	—	2021 年 3 月 31 日
78xx および 88xx 電話機の SIP OAuth の有効化	SIP OAuth を使用すると、オンプレミスでも MRA 上でも、エンドツーエンドでのセキュアなシグナリングおよびメディア暗号化を CAPF なしでデフォルトで行うことができます。SIP OAuth が有効な場合、SIP 電話のセキュリティを TFTP で保護することができます。	• アクティベーションコードを使用する登録方法の設定（436 ページ） • アクティベーションコードの使用例 （447 ページ）	2021 年 3 月 31 日

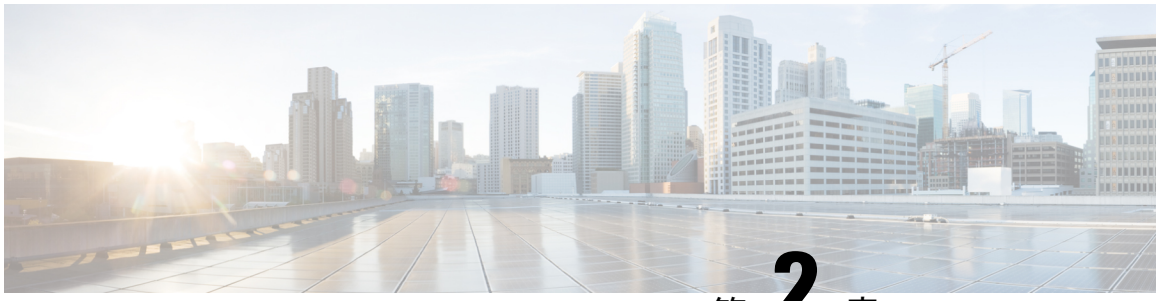
新規および変更情報

機能または変更	説明	参照先	日付（Date）
バージョンに依存しないライセンス	Unified Communications Manager は、バージョンに依存しないユーザライセンスをサポートしています。 ライセンスは、サービススタイルで、サブスクリプション期間に対して発行されます。 これらの V14 ライセンスは、Flex EA (エンタープライズ アグリーメント) または Flex NU (名前付きユーザ: プロフェッショナル、拡張、アクセス) から注文できます。	スマート ソフトウェア ライセンシング （9 ページ）	2021 年 3 月 31 日
リリース 14SU1 ドキュメントの初回リリース	—	—	2021 年 10 月 27 日
Opus コーデック トランスコーダーサポート	Unified Communications Manager には、メディアネゴシエーションを成功させるために必要な Opus オーディオコーデックのトランスコーディングをサポートする、Skinny Client Control Protocol（SCCP）で制御される iOS ベースの登録済みメディアリソースが含まれるようになりました。	Opus コーデック トランスコーダーサポート（144 ページ）	2021 年 10 月 27 日
OAuth 用の TFTP プロキシサポート	Unified Communications Manager は、TFTP プロキシを SIP OAuth の展開でサポートします。	• TFTP サーバのダイナミック設定（426 ページ） • TFTP サーバの手動設定 （427 ページ）	2021 年 10 月 27 日
リリース 14SU2 ドキュメントの初回リリース	—	—	2022 年 6 月 16 日
リリース 14SU3 ドキュメントの初回リリース	—	—	2023 年 5 月 18 日

新規および変更情報

機能または変更	説明	参照先	日付（Date）
DTMF SRTP 相互接続	現在、安全な通話と安全でない通話の両方で DTMF が一致しない場合に、Unified Communications Manager によって MTP が挿入されます。ただし、安全な通話の場合は、MTP が挿入されても、当事者のメディア間でMTPの受け渡しが行われるだけで、DTMF イベントが当事者間で送受信されることはありません。 Unified CM リリース 14SU3 よりも前のバージョンでは、DTMF 変換は安全でない通話でのみ機能し、DTMF が一致しない場合に MTP が割り当てられていました。 このリリースでは、セキュアなエンドポイント間で DTMF の不一致があった場合に、Unified CM からハードウェア MTP を（SRTP と DTMF の相互接続サポートにより）呼び出すことができます。	SRTP DTMF 相互接続 （141 ページ）	2023 年 5 月 18 日
通話用 iOS ローカルプッシュ接続機能	インターネット接続がなく、Wi-Fi 接続に制限のあるネットワーク環境（病院、クルーズ船、飛行機など）でiOSデバイスを使用する場合、Webex アプリは VoIP の着信通話の通知を受け取りません。 インターネットに接続できない場合、Apple プッシュ通知サービス（APNS）にデバイスからアクセスすることができません。 ユーザーは通話を遅延なしで受信したいと思っても、 ネットワークの速度が遅い場合は、APNS での通話に数秒の遅延が発生する場合があります。 今回のリリースで、ローカルプッシュ通知サービス（LPNS）が Apple デバイスでの通話用に導入されています。 これにより、永続的接続を使用してクライアントにプッシュメッセージが送信されるため、遅延を最小限に抑えることができます。	• 共通サービス ポート （478 ページ） • 電話機と Cisco Unified Communications Manager との間のシグナリング、メディア、およびその他の通信 （484 ページ）	2023 年 5 月 18 日

新規および変更情報



第 2 章

概要

システム設定の概要

このドキュメントには、コール制御システムのインストール後の設定に関する基本設定タスクが含まれています。このドキュメントに従って、システムパラメータ、ダイヤルプランとコール ルーティング、メディア リソースを設定し、アプリケーションの統合、エンド ユーザおよびエンドポイントのプロビジョニングを行います。このドキュメントの手順を完了すると、設定済みのダイヤル プラン、コール ルーティング、メディア リソース、帯域幅管理リソース、および基本的なセキュリティを含む基本設定ができているはずです。さらに、ユーザとエンドポイントがプロビジョニングされます。

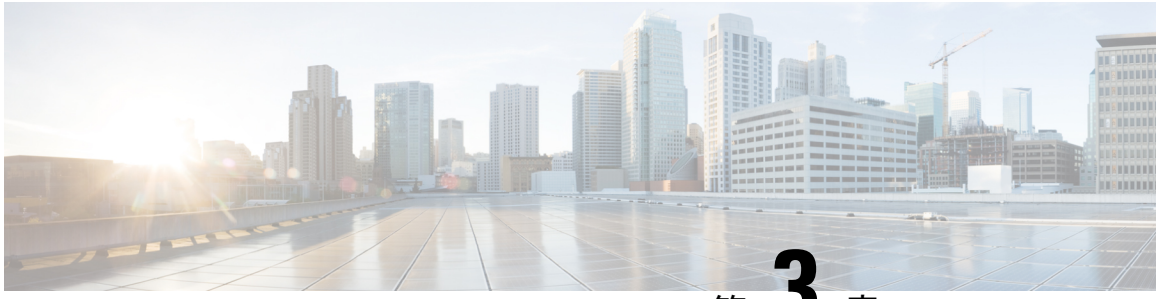
このマニュアルの構成は、次のとおりです。

- システム コンポーネント：システム ライセンス、基本的なセキュリティ、SSO、デバイス プール、トランク、ゲートウェイ、メディア リソース、およびコール アドミッション制御などの項目を設定します。
- ダイヤル プラン：ダイヤル プランとコール ルーティング要素を設定します。
- アプリケーションの統合：Cisco Emergency Responder、Cisco Unity Connection、Cisco Expressway などのアプリケーションを統合します。
- ユーザのプロビジョニング：システムにユーザを追加します。
- デバイスのプロビジョニング：ユーザ用のデバイスを登録します。

このガイドのタスクを完了すると、ご使用のシステムに、ユーザ、デバイス、基本的なセキュリティ、および SSO がセットアップされます。その後で、シスコのソリューションの設定に進むことができます。

第 部

システム コンポーネント



第 3 章

スマート ソフトウェア ライセンシング

スマート ソフトウェア ライセンシングの概要

シスコスマートソフトウェアライセンシングは、ライセンスに関する新しい考え方を提供しています。ライセンスの柔軟性が増し、企業全体のライセンスがシンプルになります。また、ライセンスの所有権および消費が可視化されます。

Ciscoスマート ソフトウェア ライセンシングを使用すると、デバイスが自己登録し、ライセンス消費を報告し、製品アクティベーションキー（PAK）が必要なくなり、ライセンスの調達、展開、管理が簡単にできるようになります。ライセンス資格を単一のアカウントにプールして、必要に応じてネットワーク経由でライセンスを自由に移動することができます。Cisco製品全体で有効化され、直接クラウドベースまたは間接導入モデルによって管理されます。

Cisco スマート ソフトウェア ライセンシング サービスでは、製品インスタンスを登録し、ライセンスの使用状況を報告し、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトから必要な認証を取得します。

スマート ライセンシングでは次のことを実行できます。

- ライセンスの使用状況とライセンス数の表示
- 各ライセンス タイプのステータスの表示
- Cisco Smart Software Manager または Cisco Smart Software Manager サテライトによる利用可能な製品ライセンスの表示
- Cisco Smart Software Manager または Cisco Smart Software Manager サテライトによるライセンス認証の更新

- ライセンス登録の更新
- Cisco Smart Software Manager または Cisco Smart Software Manager サテライトによる登録解除

（注） ライセンス承認は、30 日間に少なくとも 1 回更新することで 90 日間有効になります。Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに接続しないと、90 日後に承認の期限が切れます。

Cisco Smart Software Manager サテライトのオプションを選択する場合、このサテライトが認証を行うために、Cisco Smart Software Manager へのインターネット接続が必要になります。Cisco Smart Software Manager サテライトは、接続時間が設定可能な接続済みモードと、手動同期が必要な切断モードの 2 つのモードで動作できます。

スマート ライセンシングの導入オプションには、主に次の 2 つがあります。

- Cisco Smart Software Manager
- Cisco Smart Software Manager サテライト

Cisco Smart Software Manager

Cisco Smart Software Manager は、システムのライセンスを処理するクラウドベースのサービスです。Unified Communications Manager が直接またはプロキシ サーバ経由で、cisco.com に接続できる場合に、このオプションを使用します。Cisco Smart Software Manager によって、次のことを行うことができます。

- ライセンスの管理およびトラック
- バーチャル アカウント間でのライセンスの移動
- 登録済みの製品インスタンスの削除

オプションで、Unified Communications Manager が直接 Cisco Smart Software Manager に接続できない場合、接続を管理するプロキシ サーバを導入することができます。

Cisco Smart Software Manager の詳細については、https://software.cisco.com に進みます。

Cisco Smart Software Manager サテライト

Cisco Smart Software Manager サテライトは、セキュリティ上または可用性上の理由で、Unified Communications Manager が直接 cisco.com に接続できない場合に、ライセンスのニーズを処理できるオンプレミス導入です。このオプションを導入すると、Unified Communications Manager は、ライセンスの使用を登録し、サテライトに報告します。この際、cisco.com でホストされているバックエンドの Cisco Smart Software Managerとそのデータベースを定期的に同期します。

サテライトが cisco.com に直接接続できるかどうかに応じて、Cisco Smart Software Manager サテライトを接続または切断のいずれかのモードで導入できます。

- [接続（Connected）]：Smart Software Manager サテライトから cisco.com への直接の接続がある場合に使用されます。スマート アカウントの同期が自動的に実行されます。
- [切断（Disconnected）]：Smart Software Manager サテライトから cisco.com への接続がない場合に使用されます。Smart Account の同期を手動でアップロードおよびダウンロードする必要があります。

（注） デュアルスタックモードで実行される Unified CM は、IPv4 アドレスと IPv6 アドレスを使用して構成されたサテライトをサポートします。

Cisco Smart Software Manager サテライトの情報およびドキュメントについては、https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html に進みます。

ライセンスタイプ

ニーズをカバーするために、次のライセンスタイプを使用できます。

Cisco Unified Workspace Licensing

Cisco Unified Workspace Licensing（UWL）は、シスコ コラボレーション アプリケーションおよびサービスの最も一般的なバンドルをコスト効率の高いシンプルなパッケージで提供します。このパッケージには、ソフト クライアント、アプリケーション サーバ ソフトウェア、およびユーザごとのライセンスが含まれています。

Cisco User Connect Licensing

User Connect Licensing（UCL）は、個々の Cisco Unified Communications アプリケーションに対するユーザベースのライセンスで、アプリケーション サーバ ソフトウェア、ユーザ ライセンス、ソフト クライアントが含まれています。UCL は、必要なデバイスのタイプとデバイスの数に応じて、Essential、Basic、Enhanced、Enhanced Plus の各バージョンから選択できます。

これらのライセンスタイプと使用可能なバージョンの詳細については、http://www.cisco.com/c/en/us/products/unified-communications/unified-communications-licensing/index.html を参照してください。

Session Management Edition

Session Management Edition は、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトのいずれかに登録できます。Session Management Edition の登録には、Unified Communications Manager と同じプロセスを使用できます。Cisco Unified Communications Manager が登録されているバーチャルアカウントまたは別のバーチャルアカウントに登録し、最小のライセンス要件を満たします。

（注） 特定ライセンス予約（SLR）に登録された SME では、SLR 承認コードの生成時に最小セットのライセンスが CSSM に予約されている必要があります。

製品インスタンスの評価モード

Unified Communications Manager は、インストール後 90 日間は評価期間として実行されます。評価期間が終了すると、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録されるまで、Unified Communications Manager で新規ユーザや新規端末の追加ができなくなります。

（注） 製品が登録されると評価期間は終了します。

（注） 90 日の評価期間を使用して実行している間、セキュア SIP トランクを導入することはできません。 セキュア SIP トランクを導入するには、製品登録トークンで [エクスポート管理された機能を許可（Allow export-controlled functionality）] を選択した Smart Software Manager アカウントにシステムを登録してある必要があり ます。

システム ライセンスの前提条件

システムのライセンスプランの策定

Unified Communications（UC）のライセンス構造を確認し、把握します。詳細については、http://www.cisco.com/c/en/us/products/unified-communications/unified-communications-licensing/index.html を参照してください。

Unified Communications Manager を Smart Software Manager サービスに接続する方法を計画します。

- cisco.com の Cisco Smart Software Manager への直接接続：Unified Communications Manager は、cisco.com の Cisco Smart Software Manager に直接接続します。このオプションでは、`tools.cisco.com` を解決するように Unified Communications Manager で DNS を設定する必要があります。
- プロキシ サーバ経由で Smart Software Manager への接続：Unified Communications Manager はプロキシ サーバまたはトランスポート ゲートウェイに接続し、そこから cisco.com の Cisco Smart Software Manager サービスに接続します。Unified Communications Manager では DNS は必要ありませんが、プロキシ サーバで `tools.cisco.com` を解決できるように DNS を設定する必要があります。
- オンプレミスの Cisco Smart Software Manager サテライトへの接続：Unified Communications Manager は、オンプレミスの Smart Software Manager サテライトに接続します。Unified Communications Manager では DNS は必要ありません。接続モードを展開する場合は、サテライトサーバ上に `tools.cisco.com` を解決できる DNS が必要です。非接続モード展開の場合は、サテライトサーバで DNS を使用する必要はありません。

スマートライセンスの登録

スマートアカウントおよびバーチャル アカウントを設定します。詳細については、https://software.cisco.com/ を参照してください。

（オプション）Cisco Smart Software Manager サテライトを導入する場合は、サテライトをインストールしてセットアップします。『*Smart Software Manager* サテライト設置ガイド』などのドキュメントを参照してください。ドキュメントは https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html で入手できます。

スマート ソフトウェア ライセンシングのタスク フロー

このタスクを完了して、Unified Communications Manager のシステムライセンスを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	製品インスタンスの登録トークンの取得（13 ページ）.	仮想アカウントでの製品インスタンス登録トークンの生成は、この手順を使用します。
ステップ 2	スマートソフトウェア ライセンスへの接続の設定 （14 ページ）	Unified Communcations Manager がスマート ソフトウェア ライセンシング サービスに接続するトランスポート設定を選択します。 デフォルトでは [直接（Direct）]オプションが選択されており、製品がシスコ ライセンシング サーバに直接接続します。
ステップ 3	Cisco Smart Software Manager への登録（15 ページ）.	以下の手順で ユニファイド コミュニケーション マネージャ を Cisco スマートソフトウェア マネージャ または Cisco スマートソフトウェア マネージャ サテライトに登録します。

製品インスタンスの登録トークンの取得

始める前に

製品インスタンスを登録するには、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトから製品インスタンス登録トークンを取得します。 トークンは、エクスポート管理された機能が有効か無効かに関係なく生成できます。

手順

ステップ 1 Cisco Smart Software Manager または Cisco Smart Software Manager サテライトのいずれかでスマート アカウントにログインします。

ステップ 2 Unified Communications Manager クラスタを関連付けるバーチャル アカウントに移動します。

ステップ 3 「製品インスタンス登録トークン」を生成します。

（注） [このトークンで登録されている製品でエクスポート管理された機能を許可（Allow export-controlled functionality on the products registered with this token）]チェックボックスを選択して、このスマートアカウントで使用する製品インスタンスのトークンに対して、エクスポート管理された機能を有効にします。 このチェックボックスをオンにして条件に同意して、この登録トークンに登録されている製品の高度な暗号化を有効にします。 デフォルトでは、このチェックボックスはオンになっています。 エクスポート管理された機能をこのトークンで使用できなくするには、このチェックボックスをオフにします。

注意 このオプションは、輸出規制機能に準拠している場合のみ使用します。

（注） **[このトークンで登録されている製品の輸出規制による機能限定を許可する（Allow export-controlled functionality on the products registered with this token）]** チェックボックスは、輸出規制による機能限定の使用を許可されないスマートアカウントの場合には表示されません。

ステップ 4 トークンをコピーするか、別の場所に保存します。

詳細については、https://software.cisco.com/ を参照してください。

スマートソフトウェア ライセンスへの接続の設定

この作業を完了して、Smart Software Licensing サービスに Unified Communications Manager を接続します。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[ライセンス（Licensing）]** > **[ライセンス管理（License Management）]** を選択します。
[ライセンス管理（LicenseManagement）]ウィンドウが表示されます。

ステップ 2 [スマートソフトウェアライセンシング（Smart Software Licensing）]セクションから、[ライセンスSmart Call Home設定の表示/編集（View/Edit the Licensing Smart Call Home settings）]リンクをクリックします。
[転送設定（Transport Settings）]ダイアログ ボックスが表示されます。

ステップ 3 Smart Licensing サービスに Unified Communications Manager を接続する方法を選択します。

- [直接（Direct）]：Unified Communications Manager が cisco.com の Smart Software Manager に直接接続します。 これがデフォルトのオプションです。 このオプションでは、`tools.cisco.com` を解決できる Unified Communications Manager で DNS を導入する必要があります。
- [トランスポートゲートウェイ（Transport Gateway）]：Unified Communications Manager がオンプレミスの Cisco Smart Software Manager サテライトまたはシステム ライセンシング用のトランスポート ゲートウェイに接続します。 [URL] テキスト ボックスに、Smart Software Manager サテライトまたはトランスポート ゲートウェイのアドレスとポートを入力します。 `fqdn_of_smart_software_manager:port_number` が一例になります。 HTTPS の場合は、port 443 を使用します。
- [HTTP/HTTPSプロキシ（HTTP/HTTPS Proxy）]：Unified Communications Manager はプロキシ サーバに接続します。プロキシ サーバは、Cisco Smart Software Manager サービスと併せて、cisco.com のサテライトおよびトランスポート ゲートウェイと接続します。 プロキシ サーバの IP アドレス、ホスト名、およびポートを入力します。
  - HTTP または HTTPS プロキシで必要な認証: 認証ベースのプロキシサーバを使用して Cisco Smart Software Manager に登録する場合は、このチェックボックスをオンにします。
  - IP Address/Host Name
  - [ポート（Port）]：HTTPS の場合、port 443 を使用します。
  - ユーザ名
  - [パスワード（Password）]

ステップ 4 Unified Communications Manager が IP アドレスとホスト名を共有しないように制限するには、スマート ライセンシング登録中に [自分のホスト名またはIPアドレスをシスコと共有しません（Do not share my hostname or IP address with Cisco）]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。

Cisco Smart Software Manager への登録

製品を Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録するには、この手順を使用します。 登録するまで、製品は評価モードになっています。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[ライセンス（Licensing）]** > **[ライセンス管理（License Management）]** を選択します。
[ライセンス管理（LicenseManagement）]ウィンドウが表示されます。

ステップ 2 [スマートソフトウェアライセンシング（Smart Software Licensing）]セクションで、[登録（Register）]ボタンをクリックします。
[登録（Registration）]ウィンドウが表示されます。

ステップ 3 [製品インスタンス登録トークン（Product Instance Registration Token）]セクションで、Smart Software Manager または Smart Software Manager サテライトを使用して生成し、コピーまたは保存した「登録トークン キー」を貼り付けます。

ステップ 4 [登録（Register）]をクリックして、登録プロセスを完了します。

ステップ 5 **[閉じる（Close）]** をクリックします。 詳細については、オンライン ヘルプを参照してください。

ステップ 6 [ライセンスの使用状況レポート（License Usage Report）]セクションで、[使用状況の詳細の更新（Update Usage Details）]をクリックして、システムのライセンスの使用状況の情報を手動で更新します。

（注） 使用状況の情報は、24 時間ごとに自動的に更新されます。 詳細については、オンライン ヘルプを参照してください。

スマート ソフトウェア ライセンシングでの追加タスク

Unified Communications Manager とスマート ソフトウェア ライセンシングでは、次のオプションのタスクを実行できます。

手順

	コマンドまたはアクション	目的
ステップ 1	認証を更新 （18 ページ）	ライセンスタイプの下に表示されるすべてのライセンスのライセンス認証ステータスを手動で更新するにはこの手順を実行 h します。

	コマンドまたはアクション	目的
		（注） ライセンス認証は30日ごとに自動的に更新されます。Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに接続しないと、認証ステータスの期限は 90 日後に切れます。 Cisco Smart Software Manager サテライトのオプションを選択する場合、このサテライトが認証を行うために、Cisco Smart Software Manager へのインターネット接続が必要になります。 Cisco Smart Software Manager サテライトは、接続時間が設定可能な接続済みモードと、手動同期が必要な切断モードの 2 つのモードで動作できます。
ステップ 2	登録の更新 （19 ページ）	登録情報を手動で更新するには、以下手順を実行します。 （注） 初回登録の有効期間は 1 年です。 登録の更新は、製品を Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに接続すると、6か月ごとに自動的に行われます。
ステップ 3	登録解除 （20 ページ）	Cisco Smart Software Manager または Smart Software Manager サテライトから Unified Communications Manager クラスタを切断するには、このタスクを実行します。 製品は、評価期間の終了まで評価モードに戻ります。 製品で使用されているすべてのライセンス権限は、バーチャル アカウントにすぐにリリースされ、他の製品インスタンスで使用できるようになります。

	コマンドまたはアクション	目的
ステップ 4	Cisco Smart Software Manager でのライセンスの再登録 （21 ページ）	Unified Communications Manager を Cisco Smart Software Manager またはCisco Smart Software Manager サテライトに再登録するには、このタスクを実行します。 （注） 新しいバーチャル アカウントのトークンを使用して再登録すると、製品が異なるバーチャル アカウントに移行される場合があります。

認証を更新

この手順を使用すると、ライセンス タイプの下に表示されるすべてのライセンスのライセンス認証ステータスを手動で更新できます。

（注） ライセンス認証は 30 日ごとに自動的に更新されます。 Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに接続しないと、認証ステータスの期限は 90 日後に切れます。

Cisco Smart Software Manager サテライトのオプションを選択する場合、このサテライトが認証を行うために、Cisco Smart Software Manager へのインターネット接続が必要になります。 Cisco Smart Software Manager サテライトは、接続時間が設定可能な接続済みモードと、手動同期が必要な切断モードの 2 つのモードで動作できます。

始める前に

製品は Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録する必要があります。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [ライセンス（Licensing）] > [ライセンス管理（License Management）]** を選択します。
[ライセンス管理（LicenseManagement）]ウィンドウが表示されます。

ステップ 2 [スマートソフトウェアライセンシング（Smart Software Licensing）]セクションで、[アクション（Actions）]ドロップダウン リストをクリックします。

ステップ 3 [認証を今すぐ更新（Renew Authorization Now）]を選択します。
[認証の更新（Renew Authorization）]ウィンドウが表示されます。

ステップ 4 [OK]をクリックします。

Unified Communications Manager は、「ライセンス承認ステータス」を確認するために Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに要求を送信し、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトが Unified Communications Manager にステータスを返します。 詳細については、オンライン ヘルプを参照してください。

ステップ 5 [ライセンスの使用状況レポート（License Usage Report）]セクションで、[使用状況の詳細の更新（Update Usage Details）]をクリックして、システムのライセンスの使用状況の情報を手動で更新します。

（注） 使用状況の情報は、24 時間ごとに自動的に更新されます。 フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

登録の更新

製品を Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録する間、製品の識別にはセキュリティ アソシエーションが使用され、登録証明によってアンカーが設定されます。この有効期限（登録期間）は 1 年間です。 これは登録トークン ID の有効期限とは異なり、トークンの時間制限が有効になります。 この登録期間は 6 か月ごとに自動的に更新されます。 ただし、問題がある場合は、この登録期間を手動で更新できます。

始める前に

製品は Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録する必要があります。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [ライセンス（Licensing）] > [ライセンス管理（License Management）]** を選択します。
[ライセンス管理（LicenseManagement）]ウィンドウが表示されます。

ステップ 2 [スマートソフトウェアライセンシング（Smart Software Licensing）]セクションで、[アクション（Actions）]ドロップダウン リストをクリックします。

ステップ 3 [登録を今すぐ更新（Renew Registration Now）]を選択します。
[登録の更新（Renew Registration）]ウィンドウが表示されます。

ステップ 4 [OK]をクリックします。

Unified Communications Manager は、「登録ステータス」 を確認するために Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに要求を送信し、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトが Unified Communications Manager にステータスを返します。

ステップ 5 [ライセンスの使用状況レポート（License Usage Report）]セクションで、[使用状況の詳細の更新（Update Usage Details）]をクリックして、システムのライセンスの使用状況の情報を手動で更新します。

（注） 使用状況の情報は、24 時間ごとに自動的に更新されます。 フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

登録解除

この手順を使用すると、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトから登録を解除して、現在のバーチャルアカウントからすべてのライセンスをリリースします。この手順を実行すると、Unified Communications Manager クラスタが Cisco Smart Software Manager または Cisco Smart Software Manager サテライトから切断されます。製品で使用されているすべてのライセンス権限は、バーチャルアカウントにリリースされ、他の製品インスタンスで使用できるようになります。

（注） Unified Communications Manager が Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに接続できず、製品がまだ登録されていない場合は、警告メッセージが表示されます。このメッセージでは、製品を Cisco Smart Software Manager または Cisco Smart Software Manager サテライトから手動で削除してライセンスを解放する通知が表示されています。

始める前に

製品は Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録する必要があります。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [ライセンス（Licensing）] > [ライセンス管理（License Management）]** を選択します。
[ライセンス管理（LicenseManagement）] ウィンドウが表示されます。

ステップ 2 [スマートソフトウェアライセンシング（Smart Software Licensing）] セクションで、[アクション（Actions）] ドロップダウンリストをクリックします。

ステップ 3 [登録解除（Deregister）] を選択します。
登録解除 ウィンドウが表示されます。

ステップ 4 [OK] をクリックします。

ステップ 5 [ライセンスの使用状況レポート（License Usage Report）] セクションで、[使用状況の詳細の更新（Update Usage Details）] をクリックして、システムのライセンスの使用状況の情報を手動で更新します。

（注） 使用状況の情報は、6時間ごとに自動的に更新されます。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

（注）
- Cisco Smart Software Manager または Cisco Smart Software Manager サテライトへの登録後にデータ プレーン暗号化（混合モードの Unified Communications Manager クラスタ）が有効化され、製品が後で登録解除された場合、混合モードでは引き続き有効となります。

  Cisco Smart Software Manager または Cisco Smart Software Manager サテライトから製品が登録解除されると、SmartLicenseExportControlNotAllowedという名前の警告が管理者に送信され、クラスタが非セキュアモードに設定されます。混在モードは、再起動後も引き続き有効となります。

- この登録解除後の動作は、製品の将来のバージョンでは変更される可能性があります。CTL クライアントのセットアップに関する詳細については、「Cisco Unified Communications Managerセキュリティガイド」（http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-maintenance-guides-list.html）の「*Cisco CTL* クライアントの設定」の章を参照してください。

  トークンレス CTL の混合モードに関する詳細については、「Tokenless CTL との CUCM 混合モード」（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-tech-notes-list.html）を参照してください。

Cisco Smart Software Manager でのライセンスの再登録

この手順を使用すると、Cisco Unified Communications Manager を Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに再登録できます。

始める前に

製品インスタンスの登録トークンの取得 （13 ページ）.

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [ライセンス（Licensing）] > [ライセンス管理（License Management）]** を選択します。
[ライセンス管理（LicenseManagement）]ウィンドウが表示されます。

ステップ 2 [スマートソフトウェアライセンシング（Smart Software Licensing）]セクションで、[登録（Register）]ボタンをクリックします。
[登録（Registration）]ウィンドウが表示されます。

ステップ 3 [スマートソフトウェアライセンシング（Smart Software Licensing）]セクションで、[アクション（Actions）]ドロップダウン リストをクリックします。

ステップ 4 [登録（Reregister）]を選択します。
[登録（Reregister）]ウィンドウが表示されます。

ステップ 5 [OK]をクリックします。

ステップ 6 [製品インスタンス登録トークン（Product Instance Registration Token）]セクションで、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトを使用して生成し、コピーまたは保存した「登録トークン キー」を貼り付けます。

ステップ 7 [登録（Register）]をクリックして、登録プロセスを完了します。

ステップ 8 **[閉じる（Close）]** をクリックします。 詳細については、オンライン ヘルプを参照してください。

ステップ 9 [ライセンスの使用状況レポート（License Usage Report）]セクションで、[使用状況の詳細の更新（Update Usage Details）]をクリックして、システムのライセンスの使用状況の情報を手動で更新します。

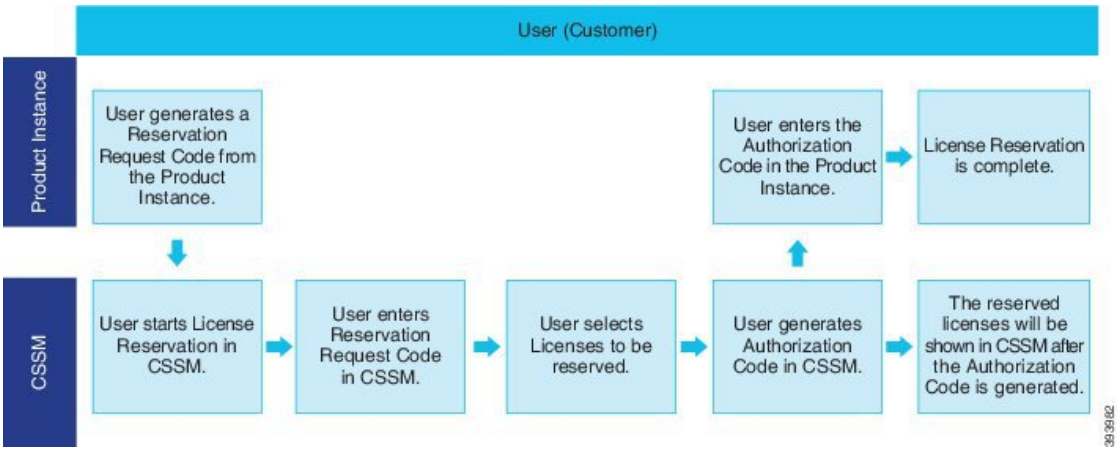
（注） 使用状況の情報は、24 時間ごとに自動的に更新されます。 フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

特定のライセンスの予約

特定ライセンス予約は、非常にセキュリティの高いネットワークで使用される機能です。 特定ライセンス予約は、使用情報を通信せずに、デバイス（製品インスタンス、Unified Communications Manager）にソフトウェアライセンスを展開する方法を提供します。

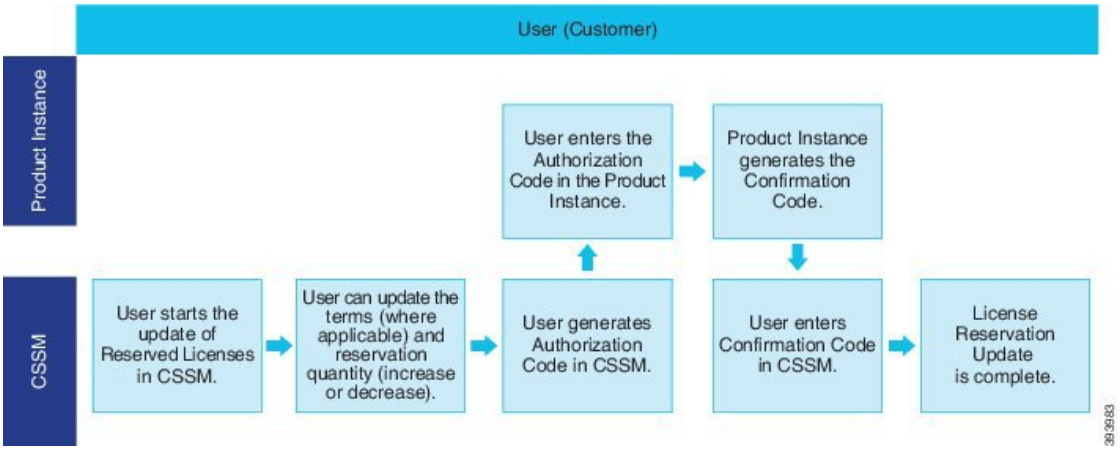
Unified Communications Manager 製品では、永久ライセンスまたは期間ベースのライセンスを指定して予約することができます。 認証コードが交換された後は、予約に変更があるまで定期的な製品の同期は必要ありません。 予約済みライセンスは、リターンコードを使用して製品からリリースされてない限り、Cisco Smart Software Manager でブロックされたままになります。

図 *1:* ライセンスの予約



予約済みライセンスの更新または変更 (増減) は、Cisco Smart Software Manager で以前に予約されたライセンスに実行できます。 新しい認証コードの製品へのインストールおよび確認コードの取得が可能です。 製品からの確認コードが Cisco Smart Software Manager にインストールされていない限り、新しい変更は送信中の状態のままになります。

図 *2:* ライセンス予約のアップデート

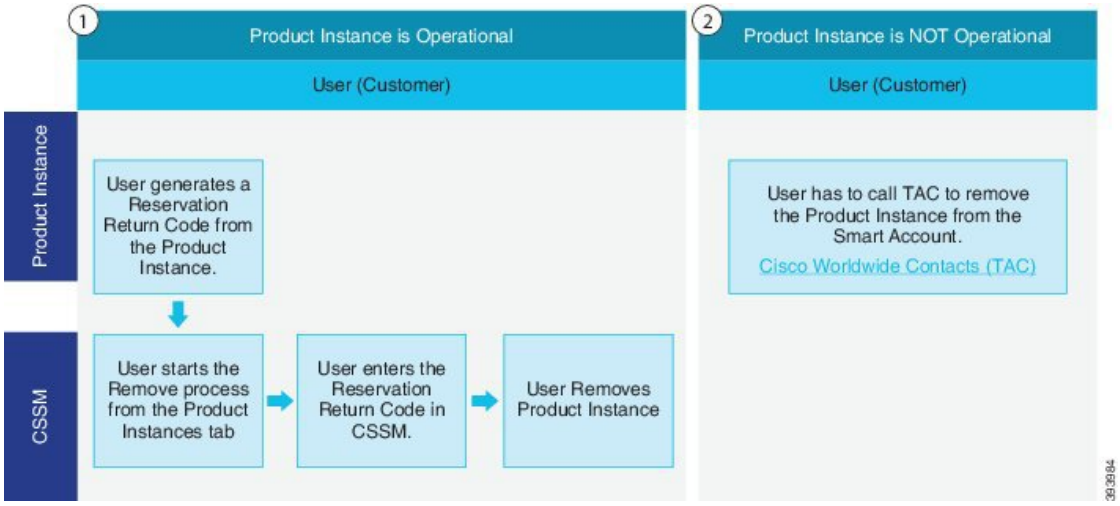


ライセンスが製品インスタンス（Unified Communications Manager）で予約されている場合、スマートアカウントから製品インスタンスを削除して、スマートアカウントからその製品インスタンス（Unified Communications Manager）に予約されているすべてのライセンスをすべてリリースするには、2 つの方法があります。

製品インスタンスは動作可能 (グレースフル削除): 製品インスタンスで（認証コードの削除）予約戻りコードを作成して、特定のライセンス予約認証をリリースすることができます。その後、CiscoSmart Software Manager に予約戻りコードを入力します。

製品インスタンスは動作不可能 (失敗または RMA による場合、または VM またはコンテナを破棄する場合): ユーザは TAC に連絡する必要があります。スマートアカウントからの製品インスタンスの削除は、TACが行います。

図 *3*: 製品インスタンスの削除: ***Unified Communications Manager***



（注） ユーザが特定のライセンス予約を有効にするには、CLI 設定のみが使用可能です。

（注） 特定ライセンス予約が Unified Communications Manager で有効化されている場合、クラウド オンボーディング用のバウチャー生成はサポートされません。

スマート アカウントでライセンス予約機能を使用できるお客様は、自身のバーチャル アカウントからライセンスを予約し、そのライセンスをデバイス UDI に関連付けて、接続していない状態で予約済みライセンスを使用してデバイスを使用することができます。 この場合、バーチャル アカウントから UDI 用の特定ライセンスと数量を予約します。 以下のオプションは、特定のライセンス予約向けの新機能および設計要素の説明です。

- license smart reservation enable
- license smart reservation disable
- license smart reservation request
- license smart reservation cancel
- ライセンス予約の更新
- license smart reservation install "<authorization-code>"
- license smart reservation install-file<url>
- license smart reservation return
- license smart reservation return-authorization "<authorization-code>"

特定のライセンスの予約タスクフロー

これらのタスクを完了して、Unified Communications Manager の特定のライセンスを予約します。

license smart reservation enable

特定のライセンスの予約を有効化するには、この手順を使用します。

始める前に

Unified Communications Manager が Cisco Smart Software Manager またはサテライトから登録解除されます。

手順

Cisco Unified CM 管理コンソールから、次の CLI コマンドを実行します。

- license smart reservation enable

license smart reservation request

Unified Communications Manager 製品から予約要求コードを生成するには、この手順を使用します。

始める前に

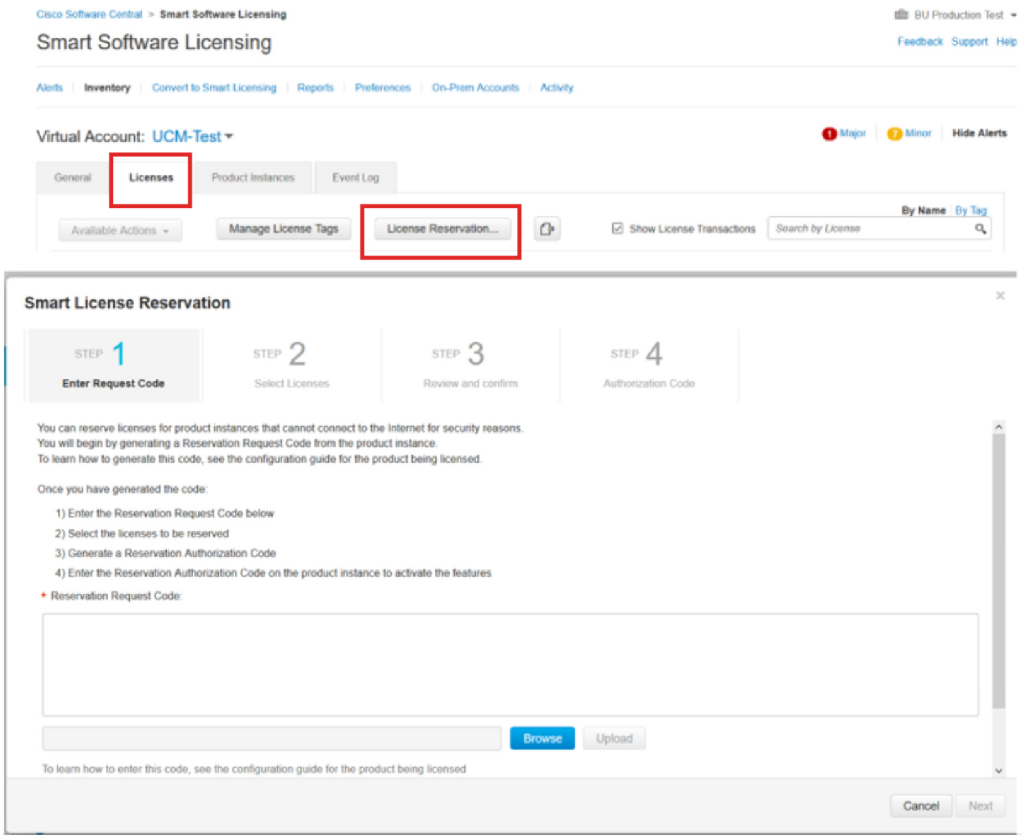
ライセンススマート予約の有効化を実行して、Unified CommunicationsManager の登録ステータスが予約中であることを確認します。

コマンド

手順

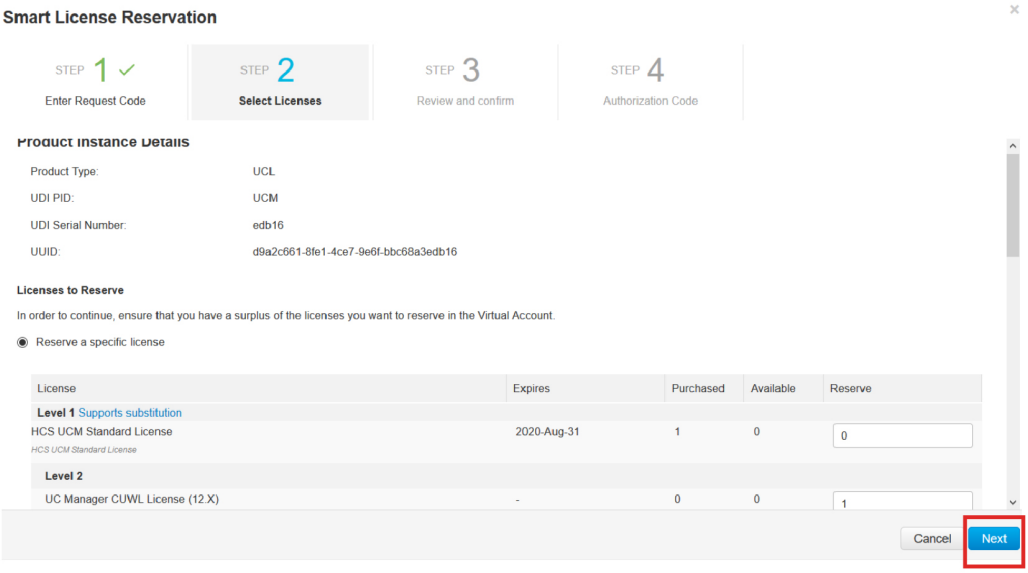
ステップ 1 Cisco Unified CM 管理コンソールから、*license smart reservation request* コマンドを実行します。

ステップ 2 CSSM [Cisco Smart Software manager] にログインし、予約リクエストコードを入力します。



450364

ステップ 3 このデバイス用に予約する必要があるライセンスを選択し、承認コードを生成します。



450365

ステップ 4 認証コードを製品インスタンスにコピーし、**license smart reservation install "<authorization-code>"** コマンドを実行してインストールします。

450366

license smart reservation install "<authorization-code>"

Cisco Smart Software Manager から生成された予約承認コードをインストールするには、この手順を使用します。

始める前に

次の順序でコマンドを実行して、Unified Communications Manager の登録ステータスが [進行中の予約（Reservation In Progress）] であることを確認します。

- **license smart reservation enable**
- **license smart reservation request**

手順

Cisco Unified CM 管理コンソールから、次の CLI コマンドを実行します。

- license smart reservation install "<authorization-code>"

license smart reservation install-file <url>

Cisco Smart Software Manager で生成されたライセンス予約承認コード ファイルをインストールするには、この手順を使用します。

始める前に

次の順序でコマンドを実行して、Unified Communications Manager の登録ステータスが [進行中の予約（Reservation In Progress）] であることを確認します。

- **license smart reservation enable**
- **license smart reservation request**

（注） URL は、SFTP サーバ上の承認コード ファイルへの必須のパスであり、次の形式で表されます。

sftp://<HostName/IP>:<port>/<Path to Authorization-Code file>

手順

Cisco Unified CM 管理コンソールから、次の CLI コマンドを実行します。

- license smart reservation install-file <url>

特定のライセンス予約に関する追加タスク

特定ライセンス予約については、Unified Communications Manager で次の追加タスクを使用できます。

license smart reservation disable

このプロセスで特定のライセンスの保留を無効にします。

始める前に

特定ライセンス予約は、Unified Communications Manager で有効化します。

手順

Cisco Unified CM 管理コンソールから、次の CLI コマンドを実行します。

- license smart reservation disable

ライセンス予約の更新

製品インスタンスのライセンス予約を更新し、新しい承認コードを取得するには、次の手順を使用します。

始める前に

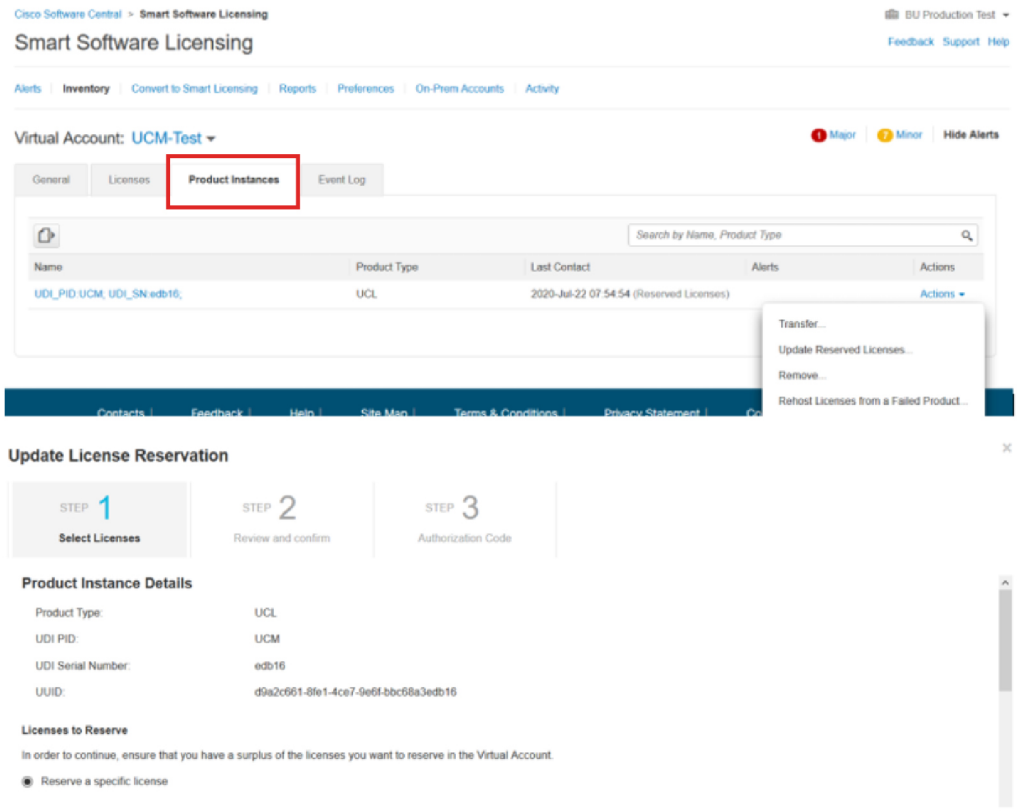
次の順序でコマンドを実行して、Unified Communcations Manger の登録ステータスが [登録済み-特定ライセンス予約] であることを確認します。

- license smart reservation enable
- license smart reservation request
- license smart reservation install "<authorization-code>"

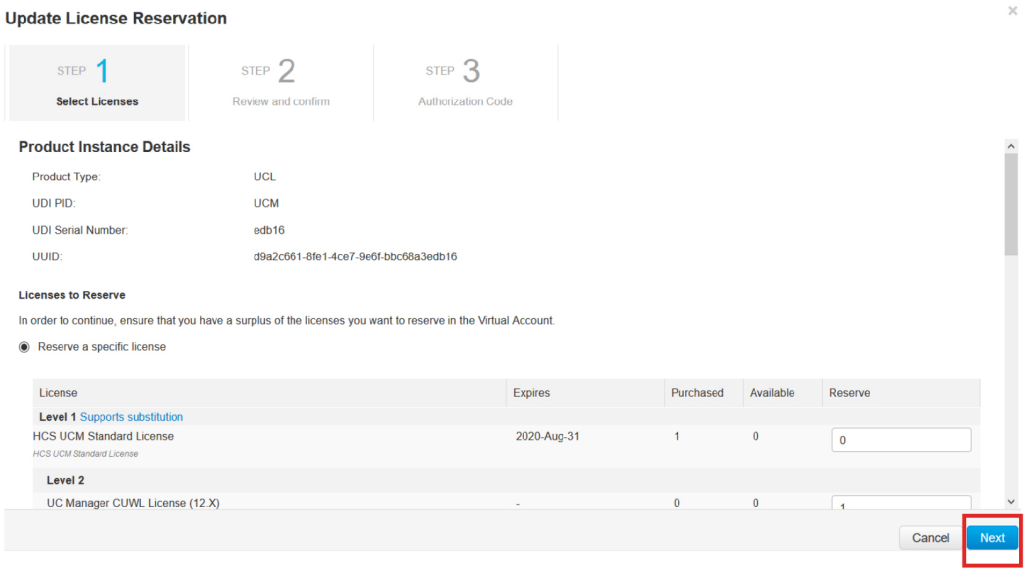
（注） Unified Communications Manager で特定のライセンス予約が有効になっている場合、上位層からライセンスを取得しても自動的には実行されません。 ライセンス予約は、Unified Communications Manager のライセンス消費/使用量に手動で更新する必要があります。

手順

ステップ 1 CSSM の予約を更新する製品インスタンスの横にある [アクションからの予約ライセンスの更新] ドロップダウン リストを選択します。

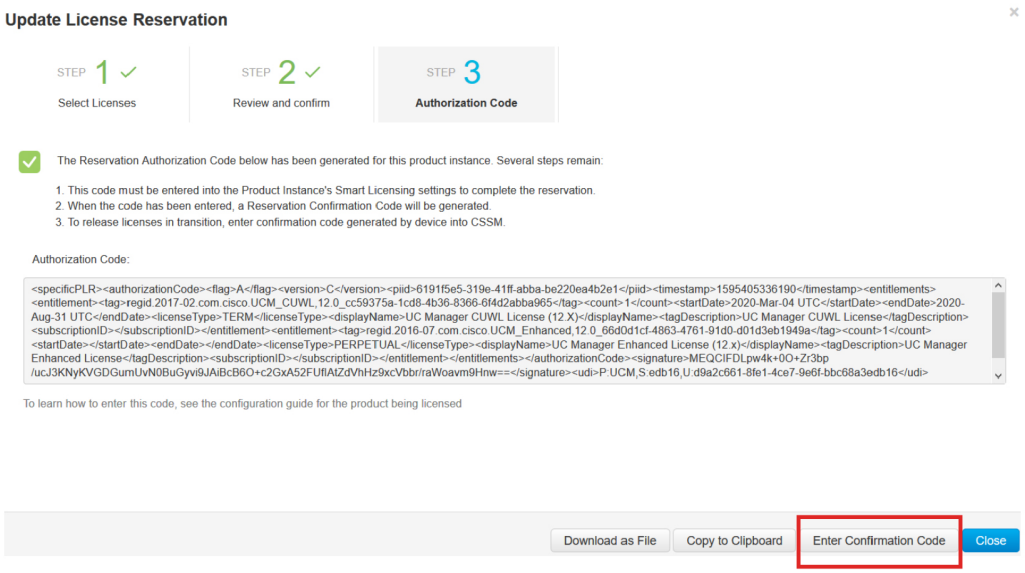


ステップ 2 予約の更新 (この製品インスタンスのライセンスの追加/削除/更新)し、承認コードを生成します。



450367

ステップ 3 認証コードを製品インスタンスにコピーし、**license smart reservation install “<authorization-code>”** コマンドを実行してインストールします。

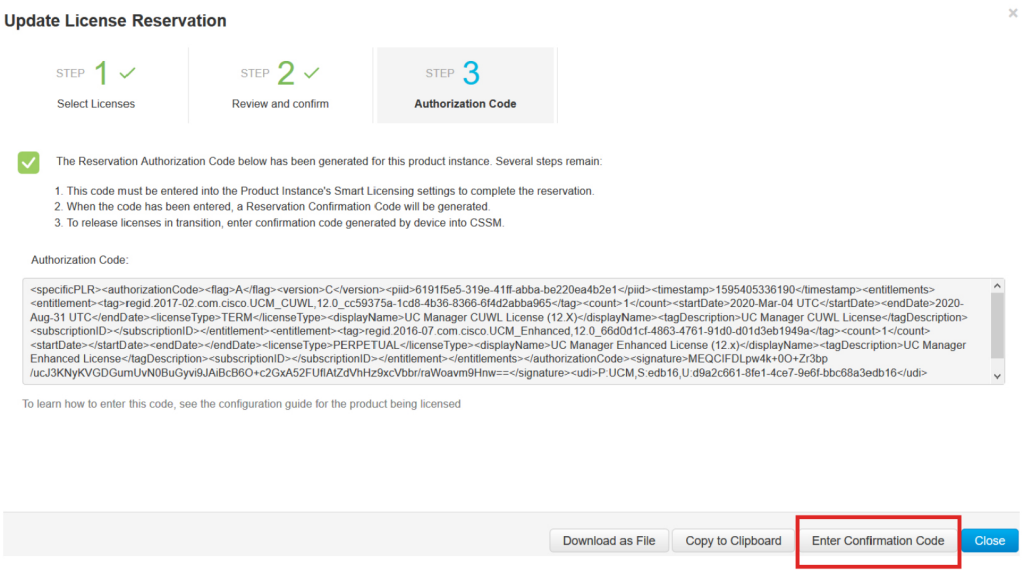


450362

ステップ 4 承認コードが正常にインストールされた後、製品に確認コードが生成されます。

450368

ステップ 5 確認コードを CSSM にコピーし、予約の更新を完了するために入力します。



license smart reservation cancel

次の手順を使用して、CUCM 要求コードに対する Cisco Smart Software Manager からの認証コードがインストールされる前に、予約プロセスをキャンセルします。

始める前に

次の順序でコマンドを実行して、Unified Communications Manager の登録ステータスが [進行中の予約（Reservation In Progress）] であることを確認します。

- **license smart reservation enable**
- **license smart reservation request**

手順

Cisco Unified CM 管理コンソールから、次の CLI コマンドを実行します。

- license smart reservation cancel

license smart reservation return

ライセンスを仮想アカウントプールに返却、CSSMから製品インスタンスを削除する際にCisco Smart Software Manager に入力する必要がある返却コードを生成するには、この手順を使用します。

始める前に

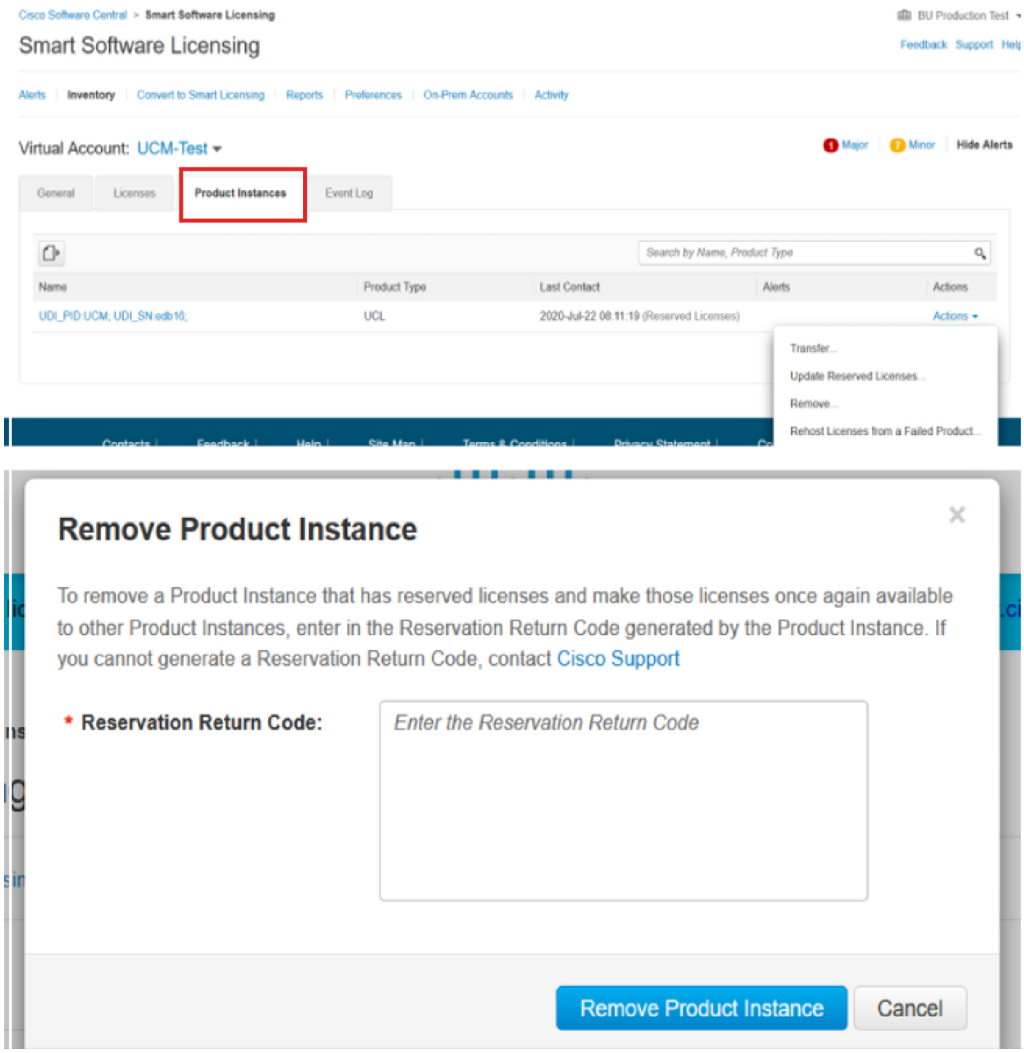
次の順序でコマンドを実行して、Unified Communcations Mangerの登録ステータスが[登録済み-特定ライセンス予約（Registered - Specific License Reservation）]であることを確認します。

- **license smart reservation enable**
- **license smart reservation request**
- **license smart reservation install "<authorization-code>"**

手順

ステップ 1 Cisco Unified CM 管理コンソールから、license smart reservation return コマンドを実行します。

ステップ 2 予約戻りコードを CSSM へコピーし、製品インスタンスを削除します。



license smart reservation return-authorization "<authorization-code>"

まだインストールされていない認証コードのリターンコードを生成するには、次の手順を使用します。 バーチャル アカウント プールにライセンスを返却して CSSM から製品インスタンスを削除するには、この返却コードを Cisco Smart Software Manager に入力する必要があります。

始める前に

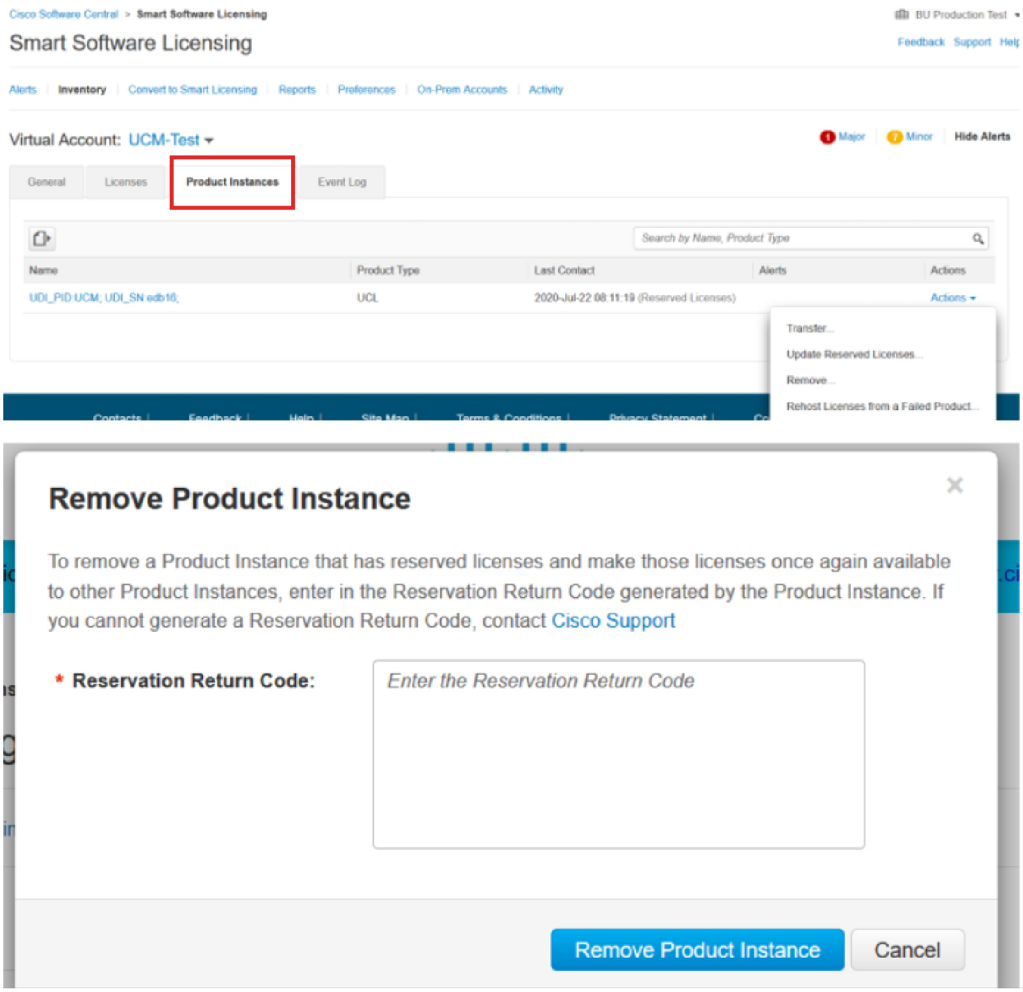
次の手順でコマンドを実行して、Unified Communcations Manager の登録ステータスが [進行中の予約（Reservation In Progress）] であることを確認します。

- **license smart reservation enable**
- **license smart reservation request**

手順

ステップ 1 Cisco Unified CM 管理コンソールから、license smart reservation return "<authorization-code>" コマンドを実行します。

ステップ 2 予約戻りコードを CSSM へコピーし、製品インスタンスを削除します。



特定ライセンス予約対応システムのバージョン14へのアップグレード

ライセンス予約が有効な 12.5 Unified Communications Manager システムをバージョン 14 にアップグレードする場合は、次のシナリオを考慮する必要があります。

1. バージョン 14 にアップグレードする前に、「license smart reservation return」コマンド (推奨) を使用して 12.x のライセンスを返します。

または

バージョン 14 にアップグレードした後、「license smart reservation return」コマンドを使用して 12.x ライセンスを返します。

2. 「license smart reservation request」コマンドを使用して要求コードを作成します。 Cisco Smart Software Manager でバージョンレス ライセンスを使用して承認コードを生成します。
3. Cisco Unified Communications Manager の license smart reservation install <auth-code> コマンドを使用して承認コードをインストールします。

バージョンに依存しないライセンス

重要 このセクションは、リリース 14 以降に適用されます。

Unified Communications Manager は、バージョンに依存しないユーザライセンスをサポートしています。ライセンスは、年間契約で、サブスクリプション期間に対して発行されます。これらの V14 ライセンスは、Flex EA（エンタープライズ アグリーメント）または Flex NU（名前付き—プロフェッショナル、拡張、アクセス）からご注文いただけます。詳細については、『注文ガイド』を参照してください。

Unified Communications Manager は、引き続きバージョン 12.X ライセンスを使用します。

ライセンスは CSSM（Cisco Smart Software Manager）で管理されます。詳細については、「スマート ソフトウェア ライセンシング （9 ページ）」を参照してください。

スマートライセンシングのエクスポートに関するコンプライアンス

スマート ライセンシングは、エクスポート制限機能をユーザが使用できるようにする手段を提供します。 接続された状態では、登録プロセスを使用して、エクスポート制限機能を使用します。 接続されていない状態では、スマート ライセンス予約を使用してエクスポート制限機能を使用します。

このエクスポート制限機能は、スマートアカウントを使用している、エクスポート制限が適用されるお客様向けのソリューションです。 この機能によってユーザは、Cisco Smart Software Manager またはサテライトで付与される規制上のエクスポート許可を要求し、エクスポート制限されている機能を Cisco Unified Communications Manager で有効化することができます。

以下のオプションでは、エクスポート制限機能に関する新しい機能と設計要素について説明しています。

- license smart export request local <exportfeaturename>

- license smart export return local <exportfeaturename>
- license smart export cancel

エクスポート制御のタスクフロー

次のタスクを実行して、Cisco Unified Communications Manager のエクスポート制限ライセンスを取得します。

license smart export request local <exportfeaturename>

このコマンドを使用すると、スマートアカウントを使用している、エクスポート制限の対象となるユーザは、Cisco Smart Software Manager またはサテライトから規制対象となるエクスポート ライセンスを要求することができます。

Cisco Smart Software Manager またはサテライトで規制対象となるエクスポート ライセンスが利用可能になると、このコマンドはエクスポート承認キーを返し、エクスポート制限の対象となる機能を製品上で有効化します。

始める前に

Cisco Unified Communications Manager は、Cisco Smart Software Manager またはサテライトを使用して登録されます。 <CUCM Export Restricted Authorization Key> ライセンスが利用可能であることを Cisco Smart Software Manager で確認してください。

手順

Cisco Unified CM 管理コンソールから、次の CLI コマンドを実行します。

- license smart export request local <exportfeaturename>

license smart export return local <exportfeaturename>

このコマンドは、以前に要求されたエクスポート制限付きライセンスを Cisco Smart Software Managerまたはサテライトに返すことを許可します。 エクスポート制限機能のエクスポート認証キーがシステムから削除されます。

始める前に

機能に対してエクスポート認証キーが生成されます。

手順

Cisco Unified CM 管理コンソールから、次の CLI コマンドを実行します。

- license smart export return local <exportfeaturename>

license smart export cancel

このコマンドを使用すると、エクスポート制限の対象となっている Smart アカウントを持つユーザは、Cisco Smart Software Manager またはサテライトからのエクスポート要求またはリターンの自動再試行のキャンセルを取り消すことができます。

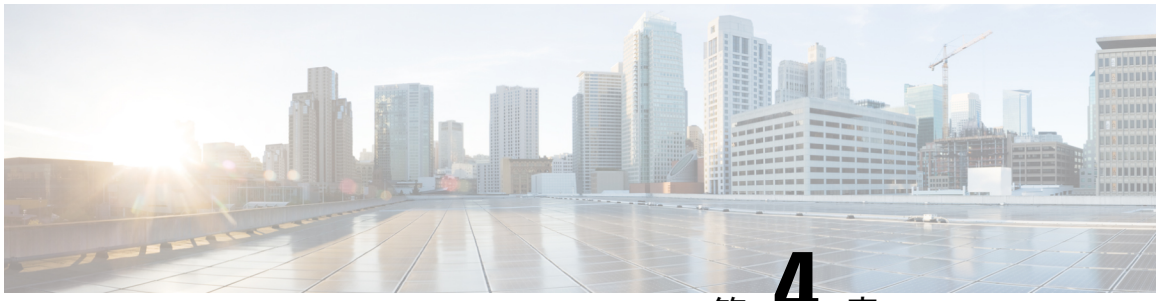
始める前に

Cisco Unified Communications Manager は、Cisco Smart Software Manager またはサテライトを使用して登録されます。

手順

Cisco Unified CM 管理コンソールから、次の CLI コマンドを実行します。

- license smart export cancel



第 4 章

エンタープライズ パラメータおよびサービスの設定

エンタープライズ パラメータの概要

エンタープライズパラメータでは、同一クラスタ内のすべてのデバイスとサービスに適用されるデフォルトの設定値を指定します クラスタは、同じデータベースを共有する Cisco Unified Communications Manager のセットで構成されます。 Cisco Unified Communications Manager の新規インストール時には、エンタープライズパラメータを使用して、デバイスのデフォルトの初期値が設定されます。

エンタープライズ パラメータに対しては、変更を加える必要がほとんどありません。 システム管理者は、変更する機能を熟知している場合、あるいは Cisco TAC から特別の指示がある場合を除いて、エンタープライズ パラメータを変更しないでください。

ほとんどの場合、推奨されるデフォルト設定で問題なく機能します。

- IP 電話のフォールバック接続モニタ期間を設定します。
- すべてのユーザに対して社内ディレクトリの検索を許可します。
- クラスタの完全修飾ディレクトリ番号（FQDN）と組織のトップレベル ドメインを設定します。
- ビデオ対応の Cisco Jabber 開始条件を設定します。
- （任意）ネットワークが IPv6 を使用している場合は、IPv6 を有効にします。
- （任意）リモート syslog サーバ名前を入力します。
- （任意）導入をトラブルシューティングするためのコール トレース ログを設定します。
- （任意）依存関係レコードを有効にします。

サービス パラメータの概要

サービス パラメータを使用すると、選択した Unified Communications Manager サーバでさまざまなサービスを設定できます。 すべてのサービスに適用されるエンタープライズ パラメータとは異なり、各サービスは個別のサービス パラメータのセットで設定されます。

サービス パラメータでは、次の 2 種類のサービスを設定できます。これらはいずれも Cisco Unified Serviceability 内で有効化できます。

- **機能サービス**：この種類のサービスは、特定のシステム機能を実行するのに使用されます。 それらを使用するためには、機能サービスをに対してオンにする必要があります。
- **ネットワーク サービス** ：ネットワーク サービスはデフォルトでオンになっていますが、トラブルシューティングの目的でネットワークサービスの停止と開始（または再起動）を選択できます。 この種類のサービスには、データベースやプラットフォームなどのシステム コンポーネントが正常に機能できるようにするサービスが含まれます。

サービス パラメータの [サービスパラメータ（service parameter）] フィールドの説明を表示するには、[サービスパラメータの設定（Service Parameter Configuration）]ウィンドウで [?] アイコンをクリックするか、パラメータの名前をクリックします。

（注） サービスを無効化すると、更新されたサービス パラメータ値は Unified Communications Manager に保持されます。 サービスを再び開始すると、Unified Communications Manager がサービス パラメータを変更後の値に設定します。

システム パラメータのタスク フロー

始める前に

Unified Communications Managerノードとポートの設定を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	エンタープライズ パラメータの設定（41 ページ）.	Unified Communications Manager ノードの初期セットアップに必要なシステム全体のパラメータを設定します。
ステップ 2	基本サービスのアクティブ化 （47 ページ）.	Cisco Unified Serviceability を使用するノードで、サービスをアクティブ化することができます。

	コマンドまたはアクション	目的
ステップ 3	サービス パラメータの設定 （50 ページ）.	クラスタ内のパブリッシャ ノードとサブスクライバ ノードのサービス パラメータを設定します。

エンタープライズ パラメータの設定

導入環境に対するエンタープライズレベルのパラメータを編集するには、この手順を使用します。 これを使用して、組織のトップレベル ドメインまたはクラスタの完全修飾ドメイン名など、エンタープライズレベルの設定を指定できます。

（注） Cisco Unified CM Administration でパラメータを編集する場合、新しい設定が Cisco Unified CM、IM and Presence Administration にも反映されます。

手順

ステップ 1 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。

[エンタープライズパラメータ（Enterprise Parameters）]ウィンドウに、エンタープライズ パラメータのリストが表示されます。

ステップ 2 パラメータ設定を編集します。

パラメータに関する説明を参照するには、GUI でパラメータ名をクリックします。 一般的なエンタープライズ パラメータの詳細については、よくある企業パラメータ （41 ページ）を参照してください。

ステップ 3 **[保存]** をクリックします。

ステップ 4 [**リセット（Reset）**]をクリックし、[**OK**]をクリックしてすべてのデバイスをリセットします。

（注） ほとんどのパラメータでは、設定を保存した後でデバイスをリセットする必要があります。デバイスが登録済みである場合は、デバイスをリセットする前に設定の変更をすべて完了させることを推奨します。

システム内のすべてのデバイスプールをリセットすることで、すべてのデバイスをリセットできます。

よくある企業パラメータ

次の表に、組織のトップレベルドメインまたはクラスタの完全修飾ドメイン名など、エンタープライズ設定に使用される共通のエンタープライズパラメータを示します。詳細なリストを参

照するには、Cisco Unified CM Administration の **[システム（System）]** > **[エンタープライズパラメータ（Enterprise Parameters）]** メニューを使用します。

表 *2 : Unified Communications Manager*の初期設定の共通企業パラメータ

パラメータ名	説明
エンタープライズ パラメータ	
Connection Monitor Duration	クラスタ内の IP 電話がセカンダリ ノードに登録された場合に、このパラメータを使用して、プライマリ ノードが使用可能になった後、それがフォールバックして再登録される前に、IP 電話が待機する時間を設定します。 このパラメータは、特定のセキュア Survivable Remote Site Telephony（SRST）ルータに対応するすべてのセキュアなデバイスに影響します。 詳細については、『*Security Guide for Cisco Unified Communications Manager*』を参照してください。 デフォルトは 120 秒です。 変更内容を反映するには、すべてのサービスを再起動してください。
CCMAdmin パラメータ	
[依存性レコードを有効化（Enable Dependency Records）]	このパラメータはトラブルシューティングに必要な依存関係の記録を表示します。 システムの初期セットアップ中は、依存関係レコードを表示すると便利な場合があります。 依存関係レコードを表示すると、CPU使用率が急激に高まり、コール処理に影響を与える可能性があります。 考えられるパフォーマンス問題を回避するために、システム設定の完了後は、このパラメータを無効にします。 負荷の低い時間帯またはメンテナンス ウィンドウの間のみに依存関係レコードを表示することを推奨します。 有効にするにはUnified Communications Manager を使用して大半の設定ウィンドウからアクセスできる **[関連リンク]** ドロップダウンリストから **[依存関係レコード]** を選択できます。 デフォルト：False
ユーザ データ サービス パラメータ	
[すべてのユーザー検索を有効にする（Enable All User Search）]	苗字、名前、またはディレクトリ番号が指定されていない場合、このパラメータは会社のディレクトリのすべてのユーザを検索することができます。 このパラメータは、[Cisco CallManager セルフ ケア（Cisco CallManager Self Care）]（CCMUser）ウィンドウでのディレクトリ検索にも適用されます。 デフォルト：[True]
クラスタ全体のドメイン設定	

パラメータ名	説明
[組織の最上位ドメイン（Organization Top Level Domain）]	このパラメータは、組織のトップレベルのドメインを定義します。例：cisco.com 最大長：255 文字 許可された値は、大文字と小文字、数字（0-9）、ハイフンとポイント（ドメインラベル区切り記号として）の有効領域を使用します。ドメイン ラベルの先頭文字をハイフンにすることはできません。 最後のラベルの先頭文字を数字にすることはできません。 たとえば、cisco.1om といったドメインは無効です。
[クラスタの完全修飾ドメイン名（Cluster Fully Qualified Domain Name）]	このパラメータに、このクラスタの1つまたは複数の完全修飾ドメイン名（FQDN）を定義します。 複数のFQDNはスペースで区切る必要があります。 アスタリスク（*）を使用して、FQDN 内でワイルドカードを指定することができます。 例：`cluster-1.cisco.com *.cisco.com` このパラメータのいずれかのFQDNに一致するホスト部分があるURLを含む要求（SIP コールなど）は、クラスタと接続されたデバイスにルーティングされます。 最大長：255 文字 有効な値：FQDNまたは*ワイルドカードを使用した部分的なFQDN。大文字と小文字、数字（0-9）、ハイフンとポイント（ドメインラベル区切り記号として）。 ドメイン ラベルの先頭文字をハイフンにすることはできません。 最後のラベルの先頭文字を数字にすることはできません。 たとえば、cisco.1om といったドメインは無効です。
IPv6	

パラメータ名	説明
IPv6 の有効化	このパラメータは、Unified Communications Manager が Internet Protocol Version 6（IPv6）をネゴシエートできるかどうか、および電話で IPv6 機能をアドバタイズできるかどうかを決定します。 このパラメータを有効化する前に、すべてのノードのプラットフォームも含め、他のすべてのネットワーク コンポーネントで IPv 6を有効にする必要があります。 それ以外の場合、システムは引き続き IPv4 専用モードで稼動します。 これは必須フィールドです。 デフォルト：False（IPv6 は無効です） IPv 6パラメータの変更を有効にするには、以下のサービスを再起動する必要があります。また、IM and Presence Serviceクラスター内の影響を受けるサービスも再起動する必要があります。 • Cisco CallManager • Cisco IP Voice Media Streaming App • Cisco CTIManager • Cisco Certificate Authority Proxy Function
Cisco Syslog Agent	
リモート Syslog サーバ名 1（Remote Syslog Server Name 1）	リモート Syslog サーバの名前または IP アドレスを入力します。 サーバ名が指定されていない場合、Cisco Unified Serviceability は Syslog メッセージを送信しません。 このパラメータは、ログ用に Syslog サーバを使用している場合にのみ必須です。 最大長：255 文字 許可された値:文字の大きさ、数字(0-9)、ハイフン、ポイントの有効なリモートSylogサーバ名を使用します。 宛先として別の Unified Communications Managerノードを指定しないでください。
Cisco Jabber	
[ビデオとともにコールを開始しない（Never Start Call with Video）]	このパラメータは、ビデオ通話の開始時に、ビデオを送信するかどうかを決定します。 すぐにビデオを送信せずにビデオ通話を開始するには、[True] を選択します。 ビデオ通話中はいつでも、ビデオの送信開始を選択できます。 このパラメータは、IM and Presence Serviceのどの設定よりも優先されます。 False に設定すると、IM and Presence Serviceで指定された設定に従ってビデオ通話が開始します。 デフォルト：False

パラメータ名	説明
SSO および OAuth の設定	
[IOS の SSO ログイン動作（SSO Login Behavior for iOS）]	このパラメータは、制御された Mobile Device Manager（MDM）導入環境で Cisco Jabber が IdP に対して証明書ベースの認証を実行できるようにする場合に必要です。 [iOS向けSSOログイン動作（SSO Login Behavior for iOS）]パラメータには次のオプションが含まれます。 • [組み込みブラウザの使用（Use Embedded Browser）]：このオプションを有効化すると、Cisco Jabber は SSO 認証に組み込みブラウザを使用します。 このオプションにより、バージョン 9 より前の iOS デバイスのネイティブ Apple Safari ブラウザで、クロス起動なしの SSO を使用できるようになります。 • [ネイティブブラウザの使用（Use Native Browser）]：このオプションを有効化すると、Cisco Jabber は、MDM 導入環境で ID プロバイダー（IdP）に対して証明書ベースの認証を実行するために、iOS デバイスで Apple Safari フレームワークを使用します。 （注） 制御された MDM 導入環境である場合を除き、ネイティブ ブラウザの使用は組み込みブラウザを使用する場合ほどセキュアではないため、このオプションの設定は推奨しません。 これは必須フィールドです。 [デフォルト（Default）]：組み込みブラウザ（WebView）を使用します。

パラメータ名	説明
[更新ログインフローを使用したOAuth（OAuth with Refresh Login Flow）]	このパラメータは、Unified Communications Manager に接続するときに、Cisco Jabber などのクライアントによって使用されるログインフローを制御します。 • [有効（Enabled）]：このオプションを有効にすると、クライアントで oAuth ベースの高速なログイン フローを使用してすばやく効率的にログインできるようになり、たとえばネットワークの変更などによってログインし直す際にユーザが入力する必要がなくなります。 このオプションを使用するためには、Expressway や Unity Connection（更新ログイン フローが有効化されている互換性のあるバージョン）など、Unified Communications ソリューションのその他のコンポーネントからのサポートが必要です。 • [無効（Disabled）]：このオプションを有効化する場合、従来の動作のままとなり、旧バージョンの他のシステム コンポーネントとの互換性が保たれます。 （注） Cisco Jabber を使用したモバイルおよびリモート アクセスの導入環境では、更新ログイン フローで oAuth をサポートする、互換性のある Expressway バージョンでのみ、このパラメータを有効化することを推奨します。 互換性のないバージョンは、Cisco Jabber の機能に影響する場合があります。 サポートされているバージョンおよび設定要件については、特定の製品のドキュメントを参照してください。 重要 この機能は、リリース 12.5(1) SU7 および 14 SU3 以降に適用されます。 パブリッシャと同様に、サブスクライバノードも要求者のノードデータベース上の更新トークンにアクセスする権限を持ち、同じものがクラスタ全体に複製されます。 これは必須フィールドです。 デフォルト：[無効(Disabled)]

パラメータ名	説明
[RTMT での SSO の使用（Use SSO for RTMT）]	このパラメータは、Real-Time Monitoring Tool（RTMT）用に SAML SSO を有効化するために設定します。 [RTMTでのSSOの使用（Use SSO for RTMT）]パラメータには、次のオプションが含まれます。 • [True]：このオプションを選択すると、RTMT は、SAML SSO ベースの IdP ログイン ウィンドウを表示します。 （注） 新規インストール時には、[RTMTでのSSOの使用（Use SSO for RTMT）]パラメータのデフォルト値は **True** になっています。 • [False]：このオプションを選択すると、RTMT は、基本認証のログイン ウィンドウを表示します。 （注） [RTMT での SSO の使用（Use SSO for RTMT）]パラメータがない Cisco Unified Communications Manager のバージョンからアップグレードする場合、新しいバージョンに表示されるこのパラメータのデフォルト値は False です。 これは必須フィールドです。 デフォルト：[True]。

基本サービスのアクティブ化

クラスタ全体でサービスをアクティブ化するには、この手順を使用します。

パブリッシャ ノードとサブスクライバ ノードで推奨されるサービスの一覧については、次のトピックを参照してください。

- パブリッシャ ノードに推奨するサービス （48 ページ）
- サブスクライバーノード用の推奨サービス （49 ページ）

手順

ステップ 1 Cisco Unified Serviceability から、**[ツール（Tools）]** > **[サービスの有効化（Service Activation）]** を選択します。

ステップ 2 ドロップダウン メニューから [サーバ（Server）]を選択して、[移動（Go）]をクリックします。

サービスと現在のステータスが表示されます。

ステップ 3 必要なサービスをアクティブ化または非アクティブ化します。

- サービスをアクティブ化するには、アクティベーションするサービスの横にあるチェックボックスをオンにします。
- サービスを非アクティブ化するには、非アクティブ化するサービスの横にあるチェックボックスをオフにします。

ステップ 4 **[保存]** をクリックします。
サービスのアクティブ化が完了するには数分かかることがあります。ステータスの変更を確認するには、ページを更新します。

パブリッシャ ノードに推奨するサービス

次の表に、専用ではない TFTP サーバを使用している場合にUnified Communications Managerパブリッシャ ノードに推奨するサービスを示します。

表 *3:* 専用ではない *TFTP* サーバの導入環境に推奨するパブリッシャ ノード サービス

タイプ（**Type**）	サービス名（**Service Name**）
CM サービス	Cisco CallManager
	Cisco Unified Mobile Voice Access Service
	Cisco IP Voice Media Streaming App
	Cisco CTIManager
	Cisco Extended Functions
	シスコ クラスタ間検索サービス
	シスコ ロケーション帯域幅マネージャ
	Cisco TFTP
CTI サービス	Cisco IP Manager Assistant
	Cisco WebDialer Web Service
CDR サービス	Cisco SOAP - CDROnDemand サービス
	Cisco CAR Web Service
データベースおよび管理者サービス	Cisco Bulk Provisioning サービス
	AXL Web Service
	Cisco URL Web Service
パフォーマンスおよびモニタリング サービス	Cisco Serviceability Reporter
	Cisco Certificate Authority Proxy Function

タイプ（Type）	サービス名（Service Name）
ディレクトリ サービス	Cisco DirSync

ヒント　以下のサービスを使用しない場合、安全にそれらを無効にできます。

- Cisco Messaging Interface
- Cisco DHCP Monitor サービス
- Cisco TAPS サービス
- Cisco Directory Number Alias Sync
- Cisco Dialed Number Analyzer Server
- Cisco Dialed Number Analyzer
- Self Provisioning IVR

サブスクライバーノード用の推奨サービス

次の表に、専用ではない TFTP サーバを使用している場合にUnified Communications Managerサブスクライバ ノードに推奨するサービスを示します。

ヒント　他のサービスを使用する予定がない場合は、そのサービスを安全に無効にすることができます。

表 *4 :* 専用の *TFTP* サーバ導入に推奨されるサブスクライバーノードサービス

タイプ（Type）	サービス名（Service Name）
CM サービス	Cisco CallManager
	Cisco IP Voice Media Streaming App
	Cisco CTIManager
	Cisco Extension Mobility
	Cisco Extended Functions
	Cisco TFTP

クラスタ内の各IM and Presence Serviceサービスノードで、次のサービスをアクティブ化する必要があります。

- Cisco SIP Proxy

- Cisco Presence Engine
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service

サービス パラメータの設定

ノードのサービス パラメータは、 Cisco Unified Communications Manager Administration を使用して設定できます。 クラスタ全体としてマークされているサービス パラメータは、クラスタ内の全ノードに影響を及ぼします。

注意 サービス パラメータの一部の変更は、システム障害の原因になることがあります。 変更しようとしている機能を完全に理解している場合と、Cisco Technical Assistance Center（TAC）から変更の指定があった場合を除いて、サービス パラメータに変更を加えないようにしてください。

始める前に

- Unified Communications Manager ノードが設定されていることを確認します。
- サービスがアクティブであることを確認します。 詳細については、基本サービスのアクティブ化 （47 ページ）を参照してください。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。は、**[システム]** > **[サービス パラメータ]** を選択します。

ステップ 2 [サーバ（Server）]ドロップダウン リストのノードを選択します。

ステップ 3 [サービス（Service）]ドロップダウン リストのサービスを選択します。

ヒント **[サービスパラメータ設定（Service Parameter Configuration）]** ウィンドウの **?** アイコンをクリックして、サービスパラメータのリストと説明を表示します。

ステップ 4 [詳細設定（Advanced）]をクリックして、すべてのパラメータのリストを表示します。

ステップ 5 サービス パラメータを変更し、[保存（Save）]をクリックします。

ウィンドウが更新され、サービス パラメータ値が更新されます。

[デフォルトに設定（Set to Default）]ボタンをクリックすると、すべてのパラメータが、[パラメータ値（Parameter Value）]フィールドの後に表示される推奨値に更新されます。 パラメータに提案値が設定されていない場合は、[デフォルトに設定（Set to Default）]ボタンをクリックしてもサービス パラメータ値は変更されません。

クラスタ全体のサービス パラメータ設定の表示

Cisco Unified Communications Manager Assistant および Cisco Unified Serviceability を使用して、クラスタ内のノードのサービスのステータスを表示できます。 サービス パラメータ設定およびパラメータの説明を表示するには、Cisco Unified Communications Manager Assistant を使用します。

手順

ステップ 1 サービスを表示し、Cisco Unified Communications Manager Assistant を使用して、ノードのサービス パラメータ設定を表示するには、次の手順を実行します。

a) **[システム]** > **[サービス パラメータ]** の順に選択します。

b) [サービスパラメータ設定（Service Parameter Configuration）]ウィンドウで、[サーバ（Server）]ドロップダウン リスト ボックスのノードを選択します。

c) [サービス（Service）]ドロップダウン ボックスのサービスを選択します。

選択したノードに適用されるすべてのパラメータが表示されます。 [クラスタ全体のパラメータ（一般）（Clusterwide Parameters（General））]セクションに表示されるパラメータは、クラスタ内の全ノードに適用されます。

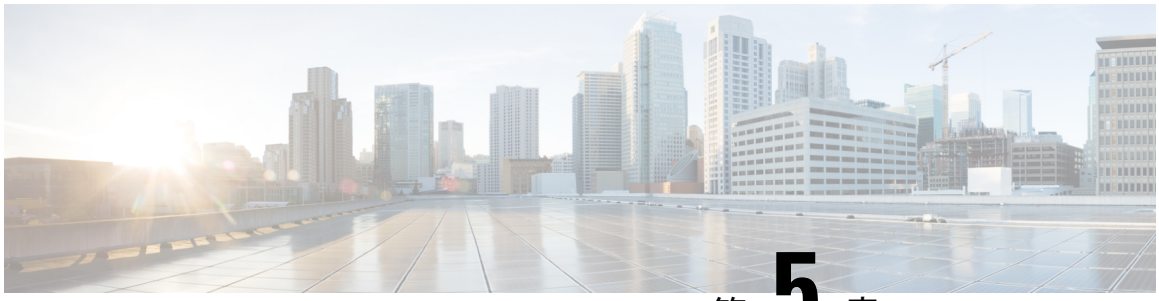
d) **[サービスパラメータ設定（Service Parameter Configuration）]** ウィンドウの（**?**）アイコンをクリックして、サービスパラメータのリストと説明を表示します。

ステップ 2 クラスタ内の全ノードに関する特定のサービスのサービスパラメータを表示するには、**[サービスパラメータ設定（Service Parameter Configuration）]** ウィンドウの **[関連リンク（Related Links）]** ドロップダウンボックスの **[すべてのサーバに対するパラメータ（Parameters for All Servers）]** を選択し、**[移動（Go）]** をクリックします。

[すべてのサーバに対するパラメータ（Parameters for All Servers）]ウィンドウが表示されます。表示されているサーバ名またはパラメータ値をクリックして、関連する [サービスパラメータ設定（Service Parameter Configuration）]ウィンドウを開くことができます。

ステップ 3 クラスタ内の全ノードに関する特定のサービスの同期外れサービスパラメータを表示するには、**[すべてのサーバに対するパラメータ（Parameters for All Servers）]** ウィンドウの **[関連リンク（Related Links）]** ドロップダウンボックスの **[すべてのサーバに対する同期外れパラメータ（Out of Sync Parameters for All Servers）]** を選択し、**[移動（Go）]** をクリックします。

[すべてのサーバに対する同期外れパラメータ（Out of Sync Parameters for All Servers）]ウィンドウが表示されます。表示されているサーバ名またはパラメータ値をクリックして、関連する [サービスパラメータ設定（Service Parameter Configuration）]ウィンドウを開くことができます。



第 5 章

IPv6 スタックの設定

IPv6 スタックの概要

IPv6 は、IPv4 アドレスが使用する 32 ビットの代わりに 128 ビットを使用する拡張 IP アドレス指定プロトコルです。 IPv6 は IPv4 よりもはるかに広い範囲の IP アドレスを提供しています。これにより、IP アドレスが枯渇するリスクが大幅に軽減されます。これは IPv4 アドレスを使用する主な懸念事項の中にあります。

デフォルトでは、Cisco Unified Communications Manager は IPv4 アドレス指定を使用するように設定されています。 ただし、IPv6 スタックをサポートするようにシステムを構成して、IPv6 のみのエンドポイントを使用して SIP ネットワークを展開できるようにすることもできます。IP アドレスが枯渇するリスクを減らすことに加えて、IPv6 は次の利点をいくつか提供しています。

- 状態なしアドレス自動設定
- 単純化されたマルチキャスト機能
- ルーティングの簡素化とルーティングテーブルの必要性の最小化
- サービスの最適化
- モビリティの適切な処理
- より優れたプライバシーと安全性

システムレベルIPv 6

IPv6 ネットワークを展開していても、Cisco Unified Communications Manager サーバは内部通信で IPv4 を使用することがあります。 これは、内部のシステムコンポーネントとアプリケーションの一部が IPv4 のみをサポートしているためです。 その結果、すべてのデバイスが IPv6 専用

モードで動作しても、Cisco Unified Communications Manager サーバはいくつかの内部通信で IPv4 を使用する必要があるため、IPv4 と IPv6 の両方のアドレスが指定されます。

（注） SIP デバイスを IPv4 と IPv6 の両方のネットワークで動作させる必要がある場合は、2 つのスタックを設定する必要があります。 この章のタスクを実行して Cisco Unified Communications Manager で IPv6 スタックを有効にする場合、2 つのスタックの SIP ネットワークも有効にする必要があります。 2 つのスタック (IPv4 および IPv6) の概要 （61 ページ） を参照してください。

デュアル スタック IPv6 の前提条件

デュアルスタックCisco Unified Communications Manager を設定する前に、IPv6 をサポートするように次のネットワークサーバとデバイスを設定する必要があります。 詳細については、デバイスのユーザ ドキュメントを参照してください。

- IPv6 がサポートされている DHCP サーバと DNS サーバをプロビジョニングします。 シスコネットワーク登録サーバは、DHCPとDNSに対するIPv 6をサポートする。
- IPv6 がサポートされている場合は、ゲートウェイ、ルータ、MTP などのネットワークデバイス用の IOS を設定します。
- IPv6 を実行するように TFTP サーバを設定します。

IPv6 の設定タスク フロー

システムのデュアル スタック IPv6 を設定するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	オペレーティング システムの IPv6 の設定 （55 ページ）	IPv6 アドレスをサポートするオペレーティング システムを設定します。
ステップ 2	IPv6 向けのサーバ設定 （56 ページ）	IPv6 アドレスを使用して、クラスタのサーバを設定します。
ステップ 3	IPv6 の有効化 （56 ページ）	IPv6 のシステムを有効にするエンタープライズ パラメータを設定します。
ステップ 4	次のいずれかの操作を行います。 • クラスタの IP アドレッシング優先順位の設定 （57 ページ）	クラスタ全体の IP アドレッシング設定を割り当てるために、エンタプライズ パラメータを設定することができます。

	コマンドまたはアクション	目的
	• デバイス用 IP アドレッシング モードの優先順位の設定 （57 ページ）	エンドポイントのグループごとに異なる設定を割り当てる必要がある場合は、共通デバイス設定でアドレッシング設定を入力します。 IP アドレッシング方式が推奨されるクラスタ設定を設定します。
ステップ 5	サービスの再起動 （59 ページ）	次のネットワーク サービスを再起動します。 • Cisco CallManager • Cisco CTIManager • Cisco IP Voice Media Streaming App • Cisco Certificate Authority Proxy Function

次のタスク

デュアル スタックのトランクを設定する方法については、SIP トランクの設定の章を参照してください。

SIP デバイスのデュアル スタックを設定する方法については、設定する SIP デバイスのセクションを参照してください。

オペレーティング システムの IPv6 の設定

Cisco Unified OS の管理でイーサネット IPv6 を設定するには、以下の手順を実行します。

（注） IPv6 DHCP サーバの設定は Windows でサポートされていないため、Cisco IOS IPv6 DHCP サーバを使用します。

手順

ステップ 1 Cisco Unified OS の管理で **設定** > **IPv6** > **イーサネット**を選択します。

ステップ 2 [Enable IPv6]チェックボックスをオンにします。

ステップ 3 **アドレス送信元** ドロップダウンリスト ボックスで、システムの IPv6 アドレス取得方法を設定します。

- **ルーターアドバタイズ**: システムは、ステートレス自動構成を使用して IPv6 アドレスを取得します。

- **DHCP**: システムは、DHCP サーバから IPv6 アドレスを取得します。
- **手動入力**: IPv6 アドレスを手動で入力する場合は、このオプションを選択します。

ステップ 4 IPv6 アドレスの取得方法に手動入力を設定する場合は、以下のフィールドに入力します。

- **IPv6 アドレス**を入力します。 たとえば、 **fd62:6:96:21e:bff:fecc:2e3a**と入力します。
- **IPv6 マスク**を入力します。たとえば、**64** と入力します。

ステップ 5 **再起動して更新する**チェックボックスをオンにして、保存後に確実にシステムが再起動するようにします。

ステップ 6 **[保存]** をクリックします。

IPv6 向けのサーバ設定

IPv6 アドレスを使用して、クラスタのサーバを設定します。

手順

ステップ 1 Cisco Unified CM Administration で、**[システム（System）]** > **[サーバ（Server）]** の順に選択します。

ステップ 2 **[IPv6 アドレス（デュアル IPv4/IPv6 の場合）]** フィールドに、次のいずれかの値を入力します。

- DNS 設定済みで、DNS サーバが IPv6 対応の場合は、サーバのホスト名を入力します。
- それ以外の場合は、非リンク ローカル IPv6 アドレスを入力します。

ステップ 3 **[保存]** をクリックします。

ステップ 4 各クラスタ ノードで上記の手順を繰り返します。

IPv6 の有効化

システムで IPv6 サポートを設定する場合、システムで IPv6 デバイスをサポートできるようにする必要があります。

手順

ステップ 1 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。

ステップ 2 [IPv6 を有効化（Enable IPv6）]エンタープライズ パラメータの値を [True（True）]に設定します。

ステップ 3 **[保存]** をクリックします。

次のタスク

クラスタ内デバイス用の IP アドレッシング設定を指定します。 クラスタ全体のエンタープライズパラメータを使用して設定を適用するか、共通デバイス設定を使用して、その設定を使用するデバイスのグループに設定を適用することができます。

- クラスタの IP アドレッシング優先順位の設定 （57 ページ）
- デバイス用 IP アドレッシング モードの優先順位の設定 （57 ページ）

クラスタの IP アドレッシング優先順位の設定

デュアル スタック IPv6 でクラスタ全体の IP アドレッシング優先順位を設定するには、この手順でエンタープライズ パラメータを使用します。 これらの設定は、これよりも優先される共通デバイス設定が特定のトランクまたはデバイスに対して適用される場合を除き、すべての SIP トランクおよびデバイスに適用されます。

（注） 共通デバイス設定での IP アドレス優先順位は、共通デバイス設定を使用するデバイスに対するクラスタ全体のエンタープライズ パラメータの設定よりも優先されます。

手順

ステップ 1 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。

ステップ 2 [メディア用のIPアドレッシングモード設定（IP Addressing Mode Preference for Media）]のエンタープライズ パラメータの値を [IPv4]または [IPv6]に設定します。

ステップ 3 [シグナリング用のIPアドレッシングモード設定（IP Addressing Mode Preference for Media）]のエンタープライズ パラメータの値を [IPv4]または [IPv6]に設定します。

ステップ 4 **[保存]** をクリックします。

デバイス用 IP アドレッシング モードの優先順位の設定

共通デバイス設定で優先順位を設定することで、個々のデバイスに IP アドレッシング モードの優先順位を設定できます。 トランク、電話、会議ブリッジ、トランスコーダなど、IPv6 アドレッシングをサポートする SIP デバイスおよび SCCP デバイスには、共通デバイス設定を適用できます。

（注） 共通デバイス設定での IP アドレス優先順位は、共通デバイス設定を使用するデバイスに対するクラスタ全体のエンタープライズ パラメータの設定よりも優先されます。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[共通デバイス設定（Common Device Configuration）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 SIP トランク、SIP 電話または SCCP 電話の場合、[IPアドレッシングモード（IP Addressing Mode）]ドロップダウン リストの値を選択します。

- [IPv4 のみ（IPv4 Only）]—デバイスはメディアやシグナリングに IPv4 アドレスだけを使用します。
- [IPv6 のみ（IPv6 Only）]—デバイスはメディアやシグナリングに IPv6 アドレスだけを使用します。
- [IPv4 および IPv6（IPv4 and IPv6）]—（デフォルト）デバイスはデュアルスタック デバイスで、利用できる IP アドレスのタイプを使用します。 両方の IP アドレスのタイプがデバイスに設定されている場合、デバイスのシグナリングには、[シグナリグ用 IP アドレッシング モード優先設定（IP Addressing Mode Preference for Signaling）]設定を使用し、メディア デバイスには、[メディア用 IP アドレッシング モード優先設定（IP Addressing Mode Preference for Media）]エンタープライズ パラメータの設定を使用します。

ステップ 4 前のステップでIPv6を設定する場合は、[シグナリング(シグナリング)] ドロップダウンリストの ip アドレス指定モードの ip アドレス設定を次のように設定します。

- [IPv4（IPv4）]—デュアル スタック デバイスでシグナリングに IPv4 アドレスを優先して使用します。
- [IPv6（IPv6）]—デュアル スタック デバイスでシグナリングに IPv6 アドレスを優先して使用します。
- [システム デフォルトを使用（Use System Default）]—デバイスは、[シグナリグ用 IP アドレッシング モード優先設定（IP Addressing Mode Preference for Signaling）]エンタープライズ パラメータの設定を使用します。

ステップ 5 **[共通デバイス構成（Common Device Configuration）]** 画面で、残りのフィールドを設定します。 フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 6 **[保存]** をクリックします。

次のタスク

IPv6 設定が完了したら、サービスの再起動 （59 ページ）を実行します。

SIP デバイスが IPv4 と IPv6 の両方のネットワークを同時にサポートするには、デバイス レベルで両方のスタックをサポートするようにシステムを設定する必要があります。詳細については、2 つのスタック (IPv4 および IPv6) の概要 （61 ページ）を参照してください。

サービスの再起動

システムの IPv6 設定したら、基本的なサービスを再起動します。

手順

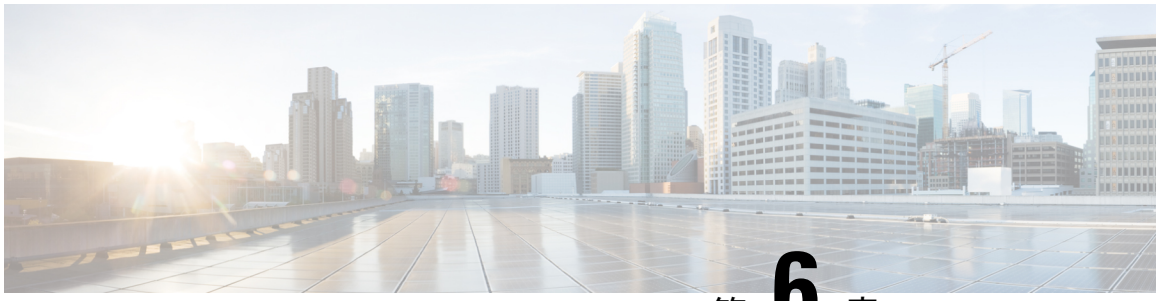
ステップ 1 Cisco Unified Serviceability にログインして、**[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）]** を選択します。

ステップ 2 次のそれぞれのサービスに対応するチェックボックスをオンにします。

- Cisco CallManager
- Cisco CTIManager
- Cisco Certificate Authority Proxy Function
- Cisco IP Voice Media Streaming App

ステップ 3 **再起動（Restart）**をクリックします。

ステップ 4 **OK**をクリックします。



第 6 章

2 つのスタック（IPv4 および IPv6）の設定

2 つのスタック (IPv4 および IPv6) の概要

SIP ネットワークが IPv4 と IPv6 の両方のスタックに設定されている場合、SIP デバイスは次の各シナリオのコールを処理できます。

- コール内のすべてのデバイスが IPv4 のみをサポートします。
- コールに含まれるすべてのデバイスは IPv6 のみに対応しています。
- コール内のすべてのデバイスは、IPv4 と IPv6 の両方のスタックをサポートしています。このシナリオでは、システムはシグナリング イベントの [シグナリングのIPアドレッシングモード設定（IP Addressing Mode Preference for Signaling）]設定とメディア イベントの [メディアのIPアドレッシングモード設定（IP Addressing Mode Preference for Media）]エンタープライズ パラメータを設定することで、IP アドレスのタイプを判別します。
- 1 つのデバイスで IPv4 のみをサポートし、他のデバイスで IPv6 のみをサポートしている。このシナリオでは、Unified Communications Manager は、2 つのアドレッシング タイプ間でシグナリングを変換するために、コール パスに MTP を挿入します。

SIP デバイスとトランクの場合は、代替ネットワーク アドレス タイプ（ANAT）を設定すると、2 つのスタック サポートを有効にできます。 ANAT が SIP デバイスまたはトランクに適用されると、IPv4 と IPv6 の両方のアドレスが使用可能な場合は、デバイスまたはトランクが送信する SIP シグナリングに両方のアドレスが含まれます。 ANAT により、エンドポイントは IPv4 専用と IPv6 専用の両方のネットワークでシームレスに相互運用できます。

2 つのスタック（IPv4 および IPv6）の前提条件

IPv6 スタックをサポートするには、まず Cisco Unified Communications Manager を設定する必要があります (デフォルトでは IPv4 が有効になっています)。 これには、メディアとシグナリングの IP アドレッシング設定の設定も含まれます。 設定の詳細については、IPv6 の設定タスク フロー （54 ページ）を参照してください。

2 つのスタック（IPv4 および IPv6）の設定タスク フロー

IPv4 と IPv6 の両方のアドレス指定を同時にサポートするように SIP デバイスとトランクを設定するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	SIP プロファイル用 ANAT の設定 （62 ページ）	IPv4 と IPv6 の両方のスタックを同時にサポートする SIP プロファイルを設定します。
ステップ 2	SIP フォンへの ANAT の適用 （63 ページ）	ANAT 対応 SIP プロファイルを SIP 電話に適用します。 これにより、SIP phone は IPv4 と IPv6 の両方のスタックを同時にサポートできます。
ステップ 3	SIP トランクへの ANAT の適用 （63 ページ）	ANAT 対応 SIP プロファイルを SIP トランクに適用します。 これにより、トランクが IPv4 と IPv6 の両方のスタックを同時にサポートできるようになります。
ステップ 4	サービスの再起動 （64 ページ）	IPv4 と IPv6 の両方のスタックを同時にサポートするようにシステムを設定した後、重要なサービスを再起動します。

SIP プロファイル用 ANAT の設定

この手順を使用すると、代替ネットワーク アドレス タイプ（ANAT）をサポートする SIP プロファイルを設定できます。 このプロファイルを使用する SIP デバイスおよびトランクは、IPv4 専用と IPv6 専用のネットワーク間でシームレスに相互運用できます。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[SIPプロファイル（SIP Profile）]** を選択します。

ステップ 2 次のいずれかを実行します。

a) 新しい SIP プロファイルを作成するには、[新規追加] をクリックします。

b) **[検索（Find）]** をクリックして、既存の SIP プロファイルを選択します。

ステップ 3 **[ANAT 有効化]** チェックボックスをオンにします。

ステップ 4 [SIPプロファイルの設定（SIP Profile Configuration）]ウィンドウで、残りのフィールドを入力します。 フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 5 **[保存]** をクリックします。

SIP プロファイル SIP 電話または SIP トランクに適用して、これらのデバイスが IPv4 と IPv6 の両方のスタックを同時にサポートできるようにする必要があります。

SIP フォンへの ANAT の適用

この手順を使用すると、SIP 電話に代替ネットワーク アドレス タイプ（ANAT）設定を適用できます。 ANAT が有効な場合は、電話は IPv4 専用と IPv6 専用の両方のネットワークと通信できます。

手順

ステップ 1 Cisco Unified CM 管理から、**[デバイス]** > **[電話機]** を選択します。

ステップ 2 既存の電話機を選択するには、[検索（Find）]をクリックします。

ステップ 3 [SIPプロファイル（SIP Profile）]ドロップダウン リスト ボックスから、ANAT を有効にした SIP プロファイルを選択します。

ステップ 4 [電話の設定（Phone Configuration）]ウィンドウで、残りのフィールドを入力します。 フィールドと設定オプションの詳細については、システムのオンラインヘルプを参照してください。

ステップ 5 **[保存]** をクリックします。

SIP トランクへの ANAT の適用

次の手順を使用して、オルタネートネットワークアドレスタイプ設定を SIP トランクに適用します。 これにより、 SIP トランクが IPv4 と IPv6 の両方のスタックを同時にサポートできるようになります。

（注） SIP トランク設定オプションの詳細については、SIP トランクの設定（106ページ）を参照してください。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [トランク（Trunk）]** を選択します。

ステップ 2 [検索（Find）]をクリックして、既存の SIP トランクを選択します。

ステップ 3 [SIPプロファイル（SIP Profile）]ドロップダウン リスト ボックスから、ANAT を有効にした SIP プロファイルを選択します。

ステップ 4 **トランク設定**ウィンドウの残りのフィールドをすべて入力します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 5 [保存]をクリックします。

サービスの再起動

IPv4 と IPv6 の両方のスタックを同時にサポートするようにシステムを設定した後、重要なサービスを再起動します。

手順

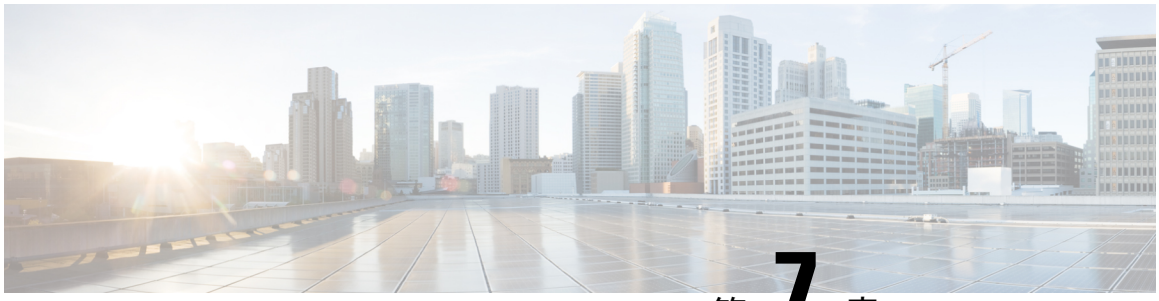
ステップ 1 Cisco Unified Serviceability にログインして、**[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）]** を選択します。

ステップ 2 次のそれぞれのサービスに対応するチェックボックスをオンにします。

- Cisco CallManager
- Cisco CTIManager
- Cisco Certificate Authority Proxy Function
- Cisco IP Voice Media Streaming App

ステップ 3 **再起動（Restart）**をクリックします。

ステップ 4 **OK**をクリックします。



第 7 章

基本的なセキュリティの設定

セキュリティの設定について

このセクションでは、Cisco Unified Communications Manager を設定するために実行する必要がある基本的なセキュリティ設定のタスクについて説明します。

セキュリティ設定のタスク

基本的なセキュリティ設定をセットアップするには、次のタスクを実行します。

クラスタの混合モードの有効化

クラスタで混合モードを有効化にするには、この手順を使用します。

手順

ステップ 1 パブリッシャ ノードでコマンドライン インターフェイスにログインします。

ステップ 2 **utils ctl set-cluster mixed-mode** CLI コマンドを実行します。

（注） Communications Manager が Cisco Smart Software Manager または Cisco Smart Software Managerサテライトに登録されていること、およびスマートアカウントまたはバーチャルアカウントから受信した登録トークンで輸出制御機能の許可が有効になっており、そのトークンがこのクラスタに登録されていることを確認します。

証明書のダウンロード

CSR リクエストを送信する際、ダウンロード証明書タスクを使用して証明書のコピーを作成するか、証明書をアップロードします。

手順

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

ステップ 2 検索情報を指定し、**[検索（Find）]** をクリックします。

ステップ 3 必要なファイル名を選択し、**[ダウンロード]** をクリックします。

証明書署名要求の生成

証明書署名要求（CSR）を生成します。これは、公開キー、組織名、共通名、地域、および国などの証明書申請情報を含む暗号化されたテキストのブロックです。認証局はこの CSR を使用して、ご使用のシステムの信頼できる証明書を生成します。

（注） 新しい CSR を生成すると、既存の CSR は上書きされます。

手順

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

ステップ 2 [CSR の作成（Generate CSR）]をクリックします。

ステップ 3 **[証明書署名要求の作成]** ウィンドウのフィールドを設定します。 フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [Generate]をクリックします。

証明書署名要求のダウンロード

CSR を生成した後にダウンロードし、認証局に提出する準備をします。

手順

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）]** > **[証明書の管理（Certificate Management）]** を選択します。

ステップ 2 [CSR のダウンロード（Download CSR）]をクリックします。

ステップ 3 [証明書の用途（Certificate Purpose）] ドロップダウン リストで、証明書名を選択します。

ステップ 4 [CSR のダウンロード（Download CSR）]をクリックします。

ステップ 5 （任意） プロンプトが表示されたら、[保存（Save）]をクリックします。

サードパーティの認証局のルート証明書のアップロード

CA ルート証明書を CAPF 信頼ストアと Unified Communications Manager信頼ストアにアップロードして、外部 CA を使用して LSC 証明書に署名します。

（注） サードパーティ CA を使用して LSCs に署名しない場合は、このタスクをスキップできます。

手順

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）]** > **[証明書の管理（Certificate Management）]** を選択します。

ステップ 2 **[証明書/証明書チェーンのアップロード]** をクリックします。

ステップ 3 **[証明書目的]** ドロップダウンリストで、**[CallManager 信頼]** を選択します。

ステップ 4 証明書の説明を [説明（Description）] に入力します。 たとえば、**外部 LSC 署名 CA の証明書などです。**

ステップ 5 [参照（Browse）]をクリックしてファイルに移動してから、[開く（Open）]をクリックします。

ステップ 6 [アップロード（Upload）]をクリックします。

ステップ 7 このタスクを繰り返して、証明**書の目的で**使用**される発信者管理者の信頼に証明書をアップロードします。**

TLS の前提条件

最低 TLS バージョンを設定する前に、ネットワーク デバイスとアプリケーションの両方でその TLS バージョンがサポートされていることを確認します。 また、それらが、ユニファイド コミュニケーション マネージャIM およびプレゼンスサービス で設定する TLS で有効になっていることを確認します。 次の製品のいずれかが展開されているなら、最低限の TLS 要件を満たしていることを確認します。 この要件を満たしていない場合は、それらの製品をアップグレードします。

- Skinny Client Control Protocol（SCCP）Conference Bridge
- トランスコーダ（Transcoder）
- ハードウェア メディア ターミネーション ポイント（MTP）
- SIP ゲートウェイ
- Cisco Prime Collaboration Assurance
- Cisco Prime Collaboration Provisioning
- Cisco Prime Collaboration Deployment
- Cisco Unified Border Element（CUBE）
- Cisco Expressway
- Cisco TelePresence Conductor

会議ブリッジ、メディア ターミネーション ポイント（MTP）、Xcoder、Prime Collaboration Assurance および Prime Collaboration Provisioning をアップグレードすることはできません。

（注） ユニファイド コミュニケーション マネージャの旧リリースからアップグレードする場合は、上位のバージョンの TLS を設定する前に、すべてのデバイスとアプリケーションでそのバージョンがサポートされていることを確認します。 たとえば、ユニファイド コミュニケーション マネージャIM およびプレゼンスサービス のリリース 9.x でサポートされるのは、TLS 1.0 のみです。

最小 TLS バージョンの設定

デフォルトでは、Unified Communications Manager において、最小 TLS バージョンとして 1.0 がサポートされています。 Unified Communications Manager および IM and Presence Service の最低

サポート TLS バージョンを 1.1 または 1.2 などの上位バージョンにリセットするには、次の手順を使用します。

設定対象の TLS バージョンが、ネットワーク内のデバイスとアプリケーションでサポートされていることを確認します。 詳細については、TLS の前提条件 （68 ページ）を参照してください。

手順

ステップ 1 **コマンドライン インターフェイス**にログインします。

ステップ 2 既存の TLS のバージョンを確認するには、**show tls min-version** CLI コマンドを実行します。

ステップ 3 **set tls min-version**<*minimum*> CLI コマンドを実行します。ここで、<*minimum*> は TLS のバージョンを示します。

たとえば、最低 TLS バージョンを 1.2 に設定するには、**set tls min-version 1.2** を実行します。

ステップ 4 すべてのUnified Communications ManagerおよびIM and Presence Service サービス クラスタ ノードで、ステップ 3 を実行します。

TLS 暗号化の設定

SIP インターフェイスの使用可能な最も強力な暗号化を選択することによって、弱い暗号化を無効にできます。 TLS 接続を確立するために Unified Communications Manager でサポートされる暗号化を設定するには、この手順を使用します。

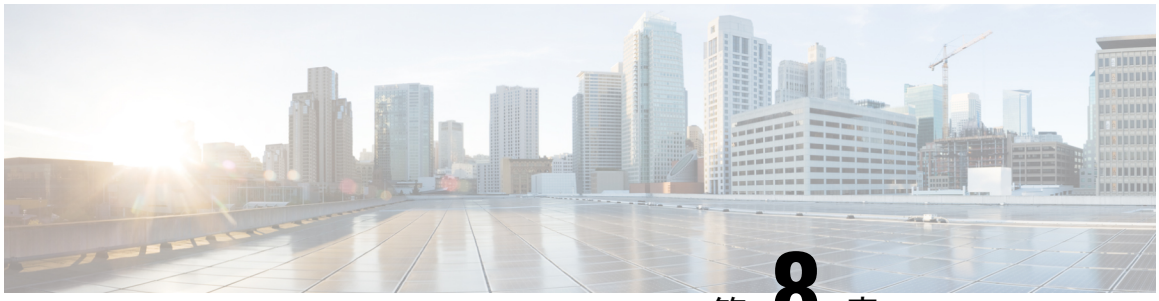
手順

ステップ 1 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。

ステップ 2 [セキュリティ パラメータ（Security Parameters）]で、[TLS 暗号化（TLS Ciphers）]エンタープライズ パラメータの値を設定します。 使用可能なオプションについては、エンタープライズ パラメータのオンラインヘルプを参照してください。

ステップ 3 **[保存]** をクリックします。

（注） すべての TLS 暗号は、クライアント暗号の設定に基づいてネゴシエートされます。



第 8 章

シングル サインオンの設定

SAML SSO ソリューションについて

重要 Cisco Jabber を Cisco Webex Meeting Server と共に導入する場合、Unified Communications Manager と Webex Meeting Server は同じドメインに存在している必要があります。

SAML は XML ベースのオープン規格のデータ形式であり、いずれかのアプリケーションにサインインした後に、管理者は定義された一連のシスコのコラボレーション アプリケーションにシームレスにアクセスできます。 SAML では、信頼できるビジネス パートナー間で、セキュリティに関連した情報交換を記述します。 これは、サービス プロバイダー（例：Unified Communications Manager）がユーザの認証に使用する認証プロトコルです。 SAML により、ID プロバイダー（IdP）とサービス プロバイダーの間で、セキュリティ認証情報を交換できます。

SAML SSO は SAML 2.0 プロトコルを使用して、シスコのコラボレーション ソリューションのドメイン間と製品間で、シングル サインオンを実現しています。 SAML 2.0 は、Cisco アプリケーション全体で SSO を有効にし、Cisco アプリケーションと IdP 間でフェデレーションを有効にします。 SAML 2.0 では、高度なセキュリティ レベルを維持しながら、シスコの管理ユーザが安全なウェブ ドメインにアクセスして、IdP とサービス プロバイダーの間でユーザー認証と承認データを交換できます。 この機能は、さまざまなアプリケーションにわたり、共通の資格情報と関連情報を使用するための安全な機構を提供します。

SAML SSO の管理者権限は、シスコのコラボレーション アプリケーションでローカルに設定されたロールベース アクセス コントロール（RBAC）に基づき認証されます。

SAML SSO は、IdP とサービス プロバイダーの間のプロビジョニング プロセスの一部として、メタデータと証明書を交換することで信頼の輪（CoT）を確立します。 サービス プロバイダーは IdP のユーザ情報を信頼しており、さまざまなサービスやアプリケーションにアクセスできるようにします。

重要　サービス プロバイダーが認証にかかわることはありません。 SAML 2.0 では、サービス プロバイダーではなく、IdP に認証を委任します。

クライアントは IdP に対する認証を行い、IdP はクライアントにアサーションを与えます。 クライアントはサービス プロバイダーにアサーションを示します。 CoT が確立されているため、サービス プロバイダーはアサーションを信頼し、クライアントにアクセス権を与えます。

SAML SSO 設定タスクフロー

SAML SSO 用にユニファイドコミュニケーションマネージャを設定するには、次のタスクを実行します。

始める前に

SAML SSO の設定では、ユニファイドコミュニケーションマネージャを設定するのと同時にアイデンティティプロバイダー(IdP)を設定する必要があります。IdP 固有の構成例については、以下を参照してください。

- Active Directory フェデレーション サービス
- Okta
- Open Access Manager
- PingFederate

（注）　上記のリンクは単なる例です。公式なマニュアルについては、IdP のマニュアルを参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Unified Communications Manager からの UC メタデータのエクスポート （73 ページ）	信頼関係を作成するには、ユニファイドコミュニケーションマネージャと IdP の間でメタデータファイルを交換する必要があります。
ステップ 2	ID プロバイダ（IdP）での SAML SSO の設定	以下のタスクを実行します。 • 信頼関係の輪を完了するために、ユニファイドコミュニケーションマネージャからエクスポートされた

	コマンドまたはアクション	目的
		UC メタデータファイルをアップロードします。 • IdP での SAML SSO の設定 • IdP メタデータファイルをエクスポートします。このファイルは、ユニファイドコミュニケーションマネージャにインポートされます。
ステップ 3	Cisco Unified Communications Manager での SAML SSO の有効化	IdP メタデータをインポートし、ユニファイドコミュニケーションマネージャで SAML SSO を有効にします。
ステップ 4	Cisco Tomcat サービスの再起動 （76 ページ）	SSO の有効化の前後には、SSO が有効になっているすべてのクラスタノードで Cisco tomcat サービスを再起動する必要があります。
ステップ 5	SAML SSO 設定の検証 （77 ページ）	SAML SSO が正常に設定されていることを確認します。

Cisco Unified Communications Manager からの UC メタデータのエクスポート

サービスプロバイダー (ユニファイドコミュニケーションマネージャ) から UC メタデータファイルをエクスポートするには、次の手順を使用します。「信頼の輪」関係を構築する目的で、メタデータ ファイルが ID プロバイダー（IdP）にインポートされます。

手順

ステップ 1 Cisco Unified CM Administration で、**[システム（System）]**>**[SAML シングル サインオン（SAML Single Sign-On）]** を選択します

ステップ 2 [SAML シングル サインオン（SAML Single Sign-On）]ウィンドウの [SSO モード（SSO Mode）] フィールドで、以下のいずれかのオプションを選択します。

- [クラスタ全体（Cluster wide）]：クラスタで 1 つの SAML 合意。

  （注） このオプションを選択する場合は、クラスタ内のすべてのノードの Tomcat サーバの証明書が同じ（マルチ サーバ SAN 証明書）であることを確認してください。

- [ノードごと（Per Node）]：それぞれのノードに個別の SAML 合意があります。

ステップ 3 [SAML シングル サインオン（SAML Single Sign-On）]ウィンドウの [証明書（Certificate）] フィールドで、以下のいずれかのオプションを選択します。

- **システムで生成された自己署名証明書の使用（Use system generated self-signed certificate）**
- **Tomcat 証明書の使用（Use Tomcat certificate）**

ステップ 4 [すべてのメタデータのエクスポート（Export All Metadata）]をクリックして、メタデータ ファイルをエクスポートします。

（注） ステップ 3 で [クラスタ全体（Cluster wide）]オプションを選択すると、クラスタ用の単一のメタデータ XML ファイルがダウンロード対象として表示されます。 一方、[ノードごと（Per Node）]オプションを選択すると、クラスタのノードごとに単一のメタデータ XML ファイルがダウンロード対象として表示されます。

次のタスク

IdP で次の作業を完了します。

- Unified Communications Manager からエクスポートされた UC メタデータ ファイルをアップロードします。
- IdP で SAML SSO を設定します。
- IdP メタデータ ファイルをエクスポートします。 「信頼の輪」関係を完成させるために、このファイルが Unified Communications Manager にインポートされます。

Cisco Unified Communications Manager での SAML SSO の有効化

サービス プロバイダー（Unified Communications Manager）で SAML SSO を有効化するには、この手順を使用します。 このプロセスには、Unified Communications Manager サーバに IdP メタデータをインポートする操作が含まれます。

重要 シスコでは、SAML SSO を有効化または無効化にした後は、Cisco Tomcat サービスを再起動することを推奨しています。

（注） SAML SSO を有効化または無効化した後は、Cisco CallManager Admin、Unified CM IM and Presence Administration、Cisco CallManager Serviceability、および Unified IM and Presence Serviceability サービスが再起動されます。

始める前に

この手順を完了する前に、次の点を確認してください。

- IdP からのエクスポート済みメタデータ ファイルが必要です。
- エンド ユーザ データが Unified Communications Manager データベースに同期されていることを確認します。
- Unified Communications Manager IM and Presence Cisco Sync Agent サービスが、正常にデータの同期を完了していることを確認します。 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] でこの検査のステータスを確認するには、**[診断（Diagnostics）] > [システム トラブルシュータ（System Troubleshooter）]** を選択します。データ同期が正常に完了した場合は[Sync Agent が関連データ（デバイス、ユーザ、ライセンス情報など）を使用して同期したことを確認する（Verify Sync Agent has sync'ed over relevant data (e.g. devices, users, licensing information)）] に [テスト合格（Test Passed）] という結果が表示されます
- Cisco Unified Administration へのアクセスを可能にするために、Standard CCM Super Users グループに少なくとも 1 人の LDAP 同期済みユーザが追加されている。 エンド ユーザ データの同期と LDAP 同期済みユーザのグループへの追加の詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』の「システムの設定」および「エンド ユーザの設定」のセクションを参照してください。

手順

ステップ 1 Cisco Unified CM の管理で、**[システム（System）] > [SAML シングル サインオン（SAML Single Sign-On）]** を選択します。

ステップ 2 [SAML SSO の有効化（Enable SAML SSO）]をクリックして、[続行（Continue）]をクリックします。

すべてのサーバ接続が再起動されることを伝える警告メッセージが示されます。

ステップ 3 [クラスタ全体（Cluster wide）]SSO モードが設定済みの場合、[マルチサーバ tomcat 証明書のテスト（Test for Multi-server tomcat certificate）]ボタンをクリックします。 それ以外の場合は、このステップを省略できます。

ステップ 4 [次へ（Next）]をクリックします。

ダイアログボックスが開き、ここで IdP メタデータをインポートできます。 IdP とサーバ間の信頼関係を設定するには、IdP から信頼メタデータ ファイルを取得し、それをすべてのサーバにインポートする必要があります。

ステップ 5 IdP からエクスポートしたメタデータ ファイルをインポートします。

a) [参照（Browse）]を使用し、エクスポート済みの IdP メタデータ ファイルを見つけて選択します。
b) [IdP メタデータのインポート(Import IdP Metadata)]をクリックします。
c) [次へ（Next）]をクリックします。
d) [サーバ メタデータをダウンロードして IdP にインストールする（Download Server Metadata and Install on IdP）]画面で、[次へ（Next）]をクリックします。

（注） **[次へ(Next)]** ボタンは、クラスタ内の 1 つ以上のノードに IdP メタデータ ファイルが正しくインポートされた場合のみ有効になります。

ステップ 6 次のように接続をテストして、設定を完了します。

a) **[エンドユーザの設定（End User Configuration）]** ウィンドウで、LDAP 同期される、**[権限情報（Permissions Information）]** リストボックスの「[標準 CCM スーパーユーザ（Standard CCM Super User）]」 権限を持つユーザを選択します。

b) [テスト実行(Run Test)]をクリックします。

IdP ログイン ウィンドウが表示されます。

（注） テストが正常に完了するまでは、SAML SSO を有効化できません。

c) 有効なユーザ名およびパスワードを入力します。

認証に成功すると、次のメッセージが表示されます。

「SSO のテストに成功しました（SSO Test Succeeded）」

このメッセージが表示されたら、ブラウザのウィンドウを閉じます。

認証に失敗するか、認証に 60 秒以上かかる場合は、[ログインに失敗しました（Login Failed）] というメッセージが IdP ログイン ウィンドウに表示されます。「」 [SAMLシングルサインオン(SAML Single Sign-On)] ウィンドウに、次のメッセージが表示されます。

「SSO メタデータのテストがタイムアウトになりました（SSO Metadata Test Timed Out）」

IdP へのログインを再試行するには、別のユーザを選択して再びテストを実行します。

d) [完了(Finish)]をクリックして、SAML SSO のセットアップを完了します。

SAML SSO が有効になり、SAML SSO に参加しているすべての Web アプリケーションが再起動されます。 Web アプリケーションの再起動には 1 ～ 2 分かかります。

Cisco Tomcat サービスの再起動

SAML シングルサインオンを有効化または無効化した前後は、シングルサインオンが実行されているすべての Unified CM クラスタノードと IM and Presence Service クラスタノードで、Cisco Tomcat サービスを再起動します。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 `utils service restart Cisco Tomcat` CLI コマンドを実行します。

ステップ 3 シングル サインオンが有効化されているすべてのクラスタ ノードで、この手順を繰り返します。

SAML SSO 設定の検証

サービス プロバイダー（Unified Communications Manager）と IdP の両方で SAML SSO を設定した後、Unified Communications Manager でこの手順に従って、設定が機能することを確認します。

始める前に

次を確認します。

- Unified CM Administration の [SAMLシングルサインオンの設定（SAML Single Sign-On Configuration）]ウィンドウに、**IdP メタデータ信頼**ファイルが正常にインポートされたことが表示されます。
- サービス プロバイダー メタデータ ファイルが IdP にインストールされます。

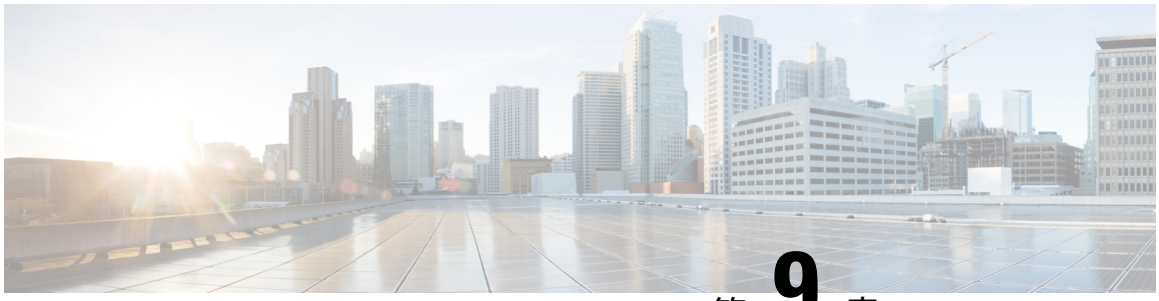
手順

ステップ 1 Cisco Unified CM Administration のユーザ インターフェイスで、**[システム（System）] > [SAML シングルサインオン（SAML Single Sign-On）]** を選択して [SAMLシングルサインオンの設定（SAML Single Sign-On Configuration）]ウィンドウを開き、[次へ（Next）]をクリックします。

ステップ 2 [有効な管理者のユーザ名（Valid Administrator Usernames）]領域から管理ユーザを選択し、[SSO テストの実行…（Run SSO Test…）]ボタンをクリックします。

（注） テスト用のユーザには管理者権限が必要であり、IdP サーバではユーザとして追加されています。 [Valid Administrator Usernames（有効な管理者のユーザ名）] 領域には、テストの実行を指示できるユーザのリストが表示されます。

テストが成功した場合は、SAML SSO が正常に設定されています。



第 9 章

デバイス プールのコア設定の設定

デバイスプールの概要

デバイスプールは、デバイスのグループに対して一連の共通設定を提供します。デバイスプールは、電話、ゲートウェイ、トランク、CTIルートポイントなどのデバイスに割り当てることができます。 デバイス プールを作成すると、各デバイスを個別に設定する代わりに、各デバイスがデバイス プールの設定を継承するように関連付けることができます。

デバイス プールを使用すると、日時グループ、リージョン、電話用 NTP リファレンスなど、ロケーションに関連した情報を割り当てることによって、デバイスをロケーションに応じて設定できます。 デバイス プールは必要なだけ作成できますが、通常はロケーションごとに 1 つです。 ただし、デバイス プールを適用することで、職務に応じて設定を適用することもできます（たとえば会社にコール センターがある場合、コール センターの電話と事務管理部門の電話を別々のデバイス プールに割り当てることが考えられます）。

このセクションでは、次のように、デバイスプールのコア設定を設定するために必要な手順について説明します。

- Network Time Protocol：電話用 NTP リファレンスを設定して、デバイス プール内の SIP デバイスに NTP サポートを提供します。
- リージョン：特定のリージョンとの間のコールに使用する帯域幅とサポートされる音声コーデックを管理します。
- Cisco Unified Communications Manager グループ：デバイスに対してコール処理の冗長性と分散コール処理を設定します。

ネットワーク タイム プロトコルの概要

NTP を使用すると、ネットワーク デバイスは、そのクロックをネットワーク タイム サーバまたはネットワーク対応のクロックと同期させることができます。NTPは、すべてのネットワークデバイスの時刻を同じにし、監査ログのタイムスタンプがネットワーク時間と一致するようにするために重要です。請求およびコール詳細レコードなどの機能は、ネットワーク上の正確なタイムスタンプに依存します。また、システム管理者は、トラブルシューティングのために監査ログに正確なタイムスタンプを必要とします。これによって、異なるシステムの監査ログを比較し、信頼できるタイムラインと一連のイベントを作成できます。

インストール時に、Unified Communications Manager パブリッシャ ノード用の NTP サーバをセットアップする必要があります。その後、サーバノードは、リリースサーバノードからそれらの時間を同期させます。

最大 5 個の NTP サーバを割り当てることができます。

電話用 NTP リファレンス

- **SIP 電話**の場合: 電話機の NTP 参照を設定し、デバイスプールを使用してそれらを割り当てる必要があります。 これらの参照により、ネットワーク時間を提供できる適切な NTP サーバに SIP 電話が送信されます。 プロビジョニングされた電話用 NTP リファレンスから SIP 電話が日時を取得できない場合、電話は Unified Communications Manager に登録したときにこの情報を受信します。
- **SCCP 電話**機の場合: 電話機の場合: 電話機は、sccp 電話機から、sccp 信号によって直接ネットワーク時間を取得できるため、電話機の NTP 参照は必要ありません。

認証済み NTP

ネットワークの NTP の領域についてネットワーク セキュリティを強化するために、認証済み NTP を設定できます。 認証済み NTP は、Cisco Unified Communications Manager パブリッシャ ノードで設定されます。サブスクライバノードと IM and Presence ノードは、Unified CM Publisher ノードからの時刻を同期します。

次の認証方法から選択できます。

- **対称キー**を使用した認証: このオプションを選択すると、ネットワーク内のデバイスは、対称キーを使用して NTP メッセージの暗号化と認証を行います。 このオプションは、RedHat などのベンダーで推奨されています。
- **Autokey (PKI ベースのインフラストラクチャ)**を使用した認証: このオプションを選択すると、ネットワーク内のデバイスは、オートキープロトコルを使用して NTP メッセージを暗号化および認証します。 この方法は、共通の条件に準拠するために必須です。
- **認証**なし:オートキー メソッドを使用した対称キーまたは認証を使用して認証を設定しない場合、NTP メッセージは認証されません。

地域の概要

リージョンは、特定のコールについて帯域幅を制限する可能性がある Unified Communications Manager のマルチサイト導入環境向けに、キャパシティ管理を提供します。 たとえば、リージョンを使用して、内部コールには高い帯域幅を維持しながら、WAN リンク経由で送信されるコールの帯域幅を制限することができます。 リージョンを使用すると、リージョン内またはリージョン間のコールの最大ビットレートを設定することにより、音声コールとビデオ通話の帯域幅を制限できます。

また、特定のコーデックのみをサポートするアプリケーションを使用している場合、システムはリージョンを使用してオーディオ コーデックの優先順位を設定します。 サポートされているオーディオコーデックの優先順位付きリストを設定し、特定のリージョンとの間のコールに適用することができます。

[リージョンの設定（Region Configuration）]ウィンドウで最大オーディオ ビットレートを設定する場合（または [サービスパラメータ設定（Service Parameter Configuration）]ウィンドウのサービスパラメータを使用して）、この設定はフィルタとして機能します。 コールでオーディオ コーデックが選択されると、Unified Communications Manager が、適合するコーデックをコール レッグの両側から選択し、設定された最大オーディオ ビットレートを超えるコーデックを除外して、リストに残ったコーデックの中から優先されるコーデックを選択します。

Unified Communications Manager は、最大 2000 のリージョンをサポートします。

サポートされているオーディオ コーデック

Unified Communications Manager は、ビデオ ストリームの暗号化および次の音声コーデックをサポートしています

オーディオ コーデック	説明
G.711	公衆電話交換網に使用される、最も広くサポートされているコーデック。
G.722	ビデオ会議でよく使用されるワイドバンド コーデック。 G.722 は無効になっていない限り、Unified Communications Manager では常に G.711 より優先されます。
G.722.1	24 および 32 kb/s で動作する低複雑度のワイドバンド コーデック。使用するビット レートはほぼ半分ですが、音声品質は G.722 の品質に近づいています。
G.728	ビデオエンドポイントがサポートする低ビットレートコーデック。
G.729	Cisco IP 電話 7900 でサポートされている 8 kb/s 圧縮を使用する低ビット レート コーデック。通常は、WAN リンクを通過するコールに使用されます。

オーディオ コーデック	説明
GSM	Global System for Mobile Communications（GSM）コーデック。 GSM を使用すると、GSM ワイヤレス ハンドセット用の MNET システムをUnified Communications Manager で動作させることができます。
L16	Advanced Audio Coding-Low Delay（AAC-LD）は、音声と音楽向けに優れた音質を提供するスーパー広帯域オーディオ コーデックです。 ビット レートが低めの場合でも、従来のコーデックと同等またはそれ以上の音質を提供します。
AAC-LD（mpeg4-generic）	SIP デバイス、特に、Cisco TelePresence Systems に対応しています。
AAC-LD（MP4A-LATM）	低オーバーヘッド MPEG-4 オーディオトランスポートマルチプレックス（LATM）は、優れたサウンドを提供するスーパーワイドバンドオーディオコーデックです。 Tandbergおよび一部のサードパーティ製エンドポイントを含むSIPデバイスで対応しています。 （注） AAC-LD（mpeg4-generic）とAAC-LD（MPA4-LATM）は互換性がありません。
Internet Speech Audio Codec（iSAC）	低および中ビットレートアプリケーションの両方で低遅延で広帯域の音質を提供するように特別に設計された、適応型広帯域オーディオコーデック。
インターネット低ビットレート コーデック（iLBC）	個別にエンコードされた音声フレームに起因する損失性ネットワークでのグレースフルな音声品質の低下を許可している間に、15.2 および 13.3 kb/s のビット レートで G.711 と G.729 の間の音声品質を提供します。iLBC は、SIP、SCCP、H323、および MGCP デバイスに対してサポートされています。 （注） H.323 アウトバウンド FastStart では、iLBC コーデックはサポートされていません。
適応マルチレート（AMR）	GSM（WDMA、EDGE、GPRS）に基づいた 2.5G/3G ワイヤレス ネットワークに必要な標準コーデック。 このコーデックは、4.75 ～ 12.2 kb/s の範囲の可変ビット レートでナローバンド（200 ～ 3400 Hz）信号をエンコードし、7.4 kb/s で始まる公衆電話交換網レベルの音声品質を提供します。 AMR は、SIP デバイスだけでサポートされます。
適応型マルチレートワイドバンド（AMR-WB）	正式には、ワイドバンドとして知られている ITU-T 標準音声コーデックである G.722.2 として体系化されており、約 16 kb/s で音声をコード化します。 このコーデックは、広い音声帯域幅（50 ～ 7000 Hz）によって、より良い音声品質を提供できるため、その他のナローバンド音声コーデック（AMR や G.711 など）より優先されます。 AMR-WB は、SIP デバイスだけでサポートされています。

オーディオ コーデック	説明
Opus	Opusコーデックは、Voice over IP、ビデオ会議、ゲーム内チャット、ライブで配信される音楽の演奏など、さまざまなインタラクティブオーディオアプリケーションを処理するために特別に設計されたインタラクティブ音声およびオーディオコーデックです。 このコーデックは、狭帯域低ビットレートから 6ー510kb / s の非常に高品質のビットレートまで拡大されます。 Opus コーデックのサポートは、すべての SIP デバイスでデフォルトで有効になっています。 [Opusコーデックの有効化（Opus Codec Enabled）]サービス パラメータを使用して Opus サポートの設置を変更できます（デフォルト設定は、[すべてのデバイスで有効（Enabled for All Devices）]です）。 このパラメータの設定を変更することで、Opus コーデックのサポートを無効化することや、非録音デバイスでのみサポートを有効化することができます。 （注） Opus は G.722 コーデックに依存しています。 SIPデバイスがOpusコーデックを使用するには、**[Enterprise Parameters Configuration]ウィンドウの[Advertise G.722 Codec]**サービスパラメータを**[Enabled]**に設定する必要があります。

Cisco Unified CM グループの概要

Unified Communications Manager グループは、デバイスが登録できる最大 3 台の冗長構成のサーバについての、優先順位付きリストです。 各グループには、1 個のプライマリ ノードと最大 2 個のバックアップ ノードが含まれます。 ノードをリストする順序によって、1 番目のノードがプライマリ ノード、2 番目のノードがバックアップ ノード、3 番目のノードが第 3 ノードとして優先順位が決定されます。 [デバイスプールの設定（Device Pool Configuration）]を使用して、Cisco Unified Communictions Manager グループにデバイスを割り当てることができます。

Unified Communications Manager グループは、システムに 2 つの重要な機能を提供します。

- コール処理の冗長性：デバイスが登録するときに、そのデバイス プールに割り当てられているグループ内のプライマリ（1 番目）Unified Communications Manager への接続を試みます。 プライマリ Unified Communications Manager が使用可能ではない場合、デバイスは最初のバックアップ ノードに接続しようとし、そのノードが使用可能ではない場合は、第 3 のノードに接続を試みます。 各デバイス プールには Unified Communications Manager グループが 1 つ割り当てられます。
- 分散コール処理：複数のデバイス プールと Unified Communications Manager グループを作成することで、デバイスの登録を複数の Unified Communications Manager に均等に分散できます。

ほとんどのシステムでは、より適切な負荷分散と冗長性を実現するために、複数のグループに対して Unified Communications Manager を割り当てます。

コール処理の冗長性

Unified Communications Manager グループは、コール処理の冗長性と回復の機能を提供します。

- フェールオーバー：グループのプライマリ Unified Communications Manager で障害が発生し、そのグループのバックアップ Unified Communications Manager にデバイスが再登録するときに実行されます。
- フォールバック：障害が発生したプライマリ Unified Communications Manager が復旧し、そのグループのデバイスがプライマリ Unified Communications Manager に再登録されるときに実行されます。

通常動作では、グループ内のプライマリ Unified Communications Manager は、電話およびゲートウェイなど、そのグループに関連付けられたすべての登録デバイスのコール処理を制御します。

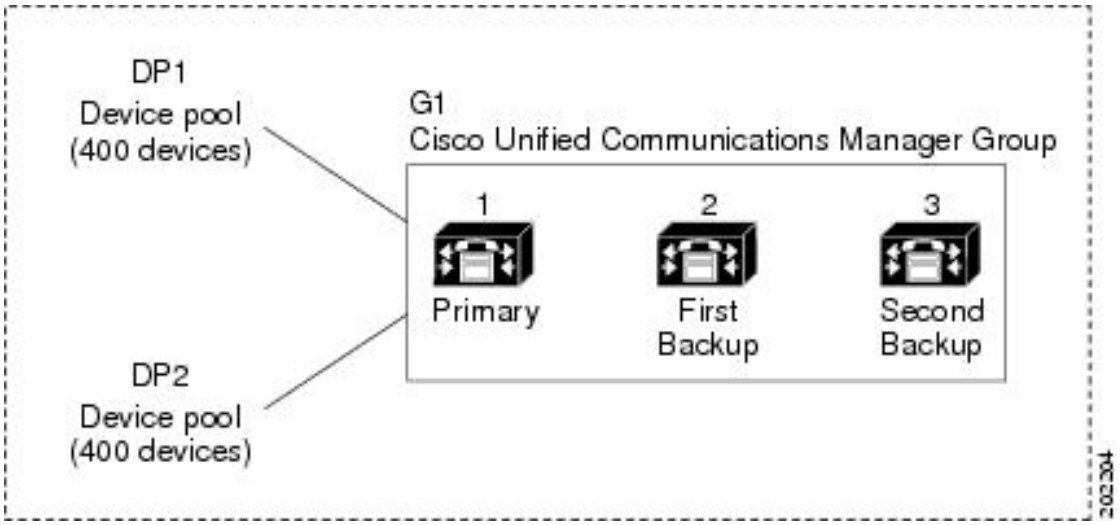
プライマリの Unified Communications Manager で何らかの理由で障害が発生した場合、グループの 1 番目のバックアップ Unified Communications Manager が、プライマリ Unified Communications Manager に登録されたデバイスを制御します。 グループに 2 番目のバックアップ Unified Communications Manager を指定する場合、プライマリと 1 番目のバックアップ両方の Unified Communications Manager で障害が発生した場合には、2 番目がデバイスを制御します。

障害が発生したプライマリ Unified Communications Manager の機能が回復すると、グループの制御が戻り、そのグループのデバイスは自動的にプライマリ Unified Communications Manager に再登録されます。

例

たとえば、次の図は 800 台のデバイスを制御する単一グループ内の 3 台の Unified Communications Manager を備えた簡単なシステムを示しています。

図 *4 : Unified Communications Manager* グループ



この図 は、2 つのデバイス プール DP1 と DP2 が割り当てられている Unified Communications Manager グループ G1 を示しています。 Unified Communications Manager 1 は、グループ G1 のプライマリ Unified Communications Manager であり、通常の動作時には、DP1 と DP2 の 800 台のデバイスをすべて制御しています。 Unified Communications Manager1 に障害が発生した場合、800 台すべてのデバイスの制御は Unified Communications Manager 2 に移ります。Unified Communications Manager 2 にも障害が発生した場合は、800 台すべてのデバイスの制御は Unified Communications Manager 3 に移ります。

この構成では、コール処理の冗長化は実現していますが、コール処理の負荷は、この例の 3 台の Unified Communications Manager 間で適切に分散されていません。 Unified Communications Managerグループとデバイス プールを使用して、クラスタ内で分散コール処理を提供する方法については、次のトピックを参照してください。

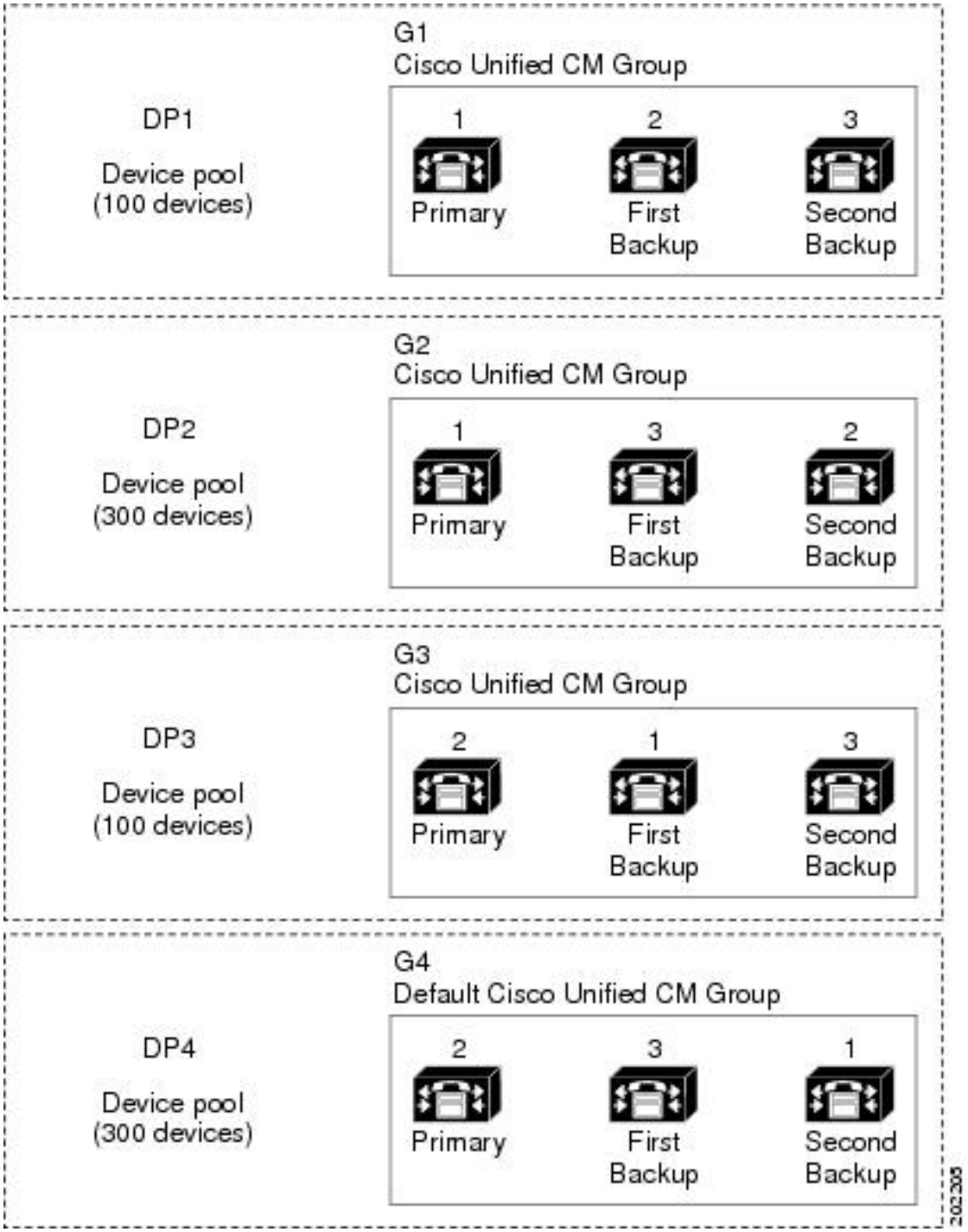
（注） 空の Unified Communications Manager グループは機能しません。

分散コール処理

Unified Communications Manager グループは、コール処理の冗長性と分散型コール処理の両方を提供します。 デバイス、デバイス プール、および Unified Communications Manager をどのようにグループに割り当てるかによって、システムの冗長性とロードバランシングのレベルが決まります。

多くの場合、グループ内の 1 台の Unified Communications Manager に障害が起きた場合に、他の Unified Communications Manager が過負荷状態にならないようにデバイスを分散する必要があります。 次の図は、3 台のと 800 台のデバイスで構成されるシステムで、分散型コール処理と冗長化の両方を実現するための グループとデバイス プールの設定例を示しています。Unified Communications ManagerUnified Communications Manager

図 *5:* 分散型コール処理と組み合わせた冗長化



上の図は、 グループの設定、デバイス プールへの割り当てを示しています。 1 は、2 つのグループ G1 と G2 でプライマリ コントローラとして機能します。Unified Communications ManagerUnified Communications ManagerUnified Communications Manager 1 で障害が発生した場合、デバイスプール DP1 の 100 台のデバイスは Unified Communications Manager 2 に再登録さ

れ、DP2 の 300 台のデバイスは Unified Communications Manager 3 に再登録されます。同様に、Unified Communications Manager 2 はグループ G3 と G4 のプライマリコントローラとして機能します。 Unified Communications Manager 2 で障害が発生した場合、DP3 の 100 台のデバイスは Unified Communications Manager 1 に再登録され、DP4 の 300 台のデバイスは Unified Communications Manager 3 に再登録されます。Unified Communications Manager 1 と Unified Communications Manager 2 の両方で障害が発生した場合は、すべてのデバイスは Unified Communications Manager 3 に再登録されます。

デバイスプールの前提条件

デバイスプールは、設定する前に、適切に計画してください。デバイスプールおよび冗長構成の Unified Communications Manager グループを設定する場合は、電話機向けにサーバの冗長性を提供すると同時に、登録を複数のクラスタに均等に分散させることを推奨します。システムについて計画を立てる際に使用できる詳細情報については、『*Cisco Collaboration* システム ソリューション リファレンス ネットワーク デザイン』（https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html）を参照してください。

Unified Communications Manager に最新のタイム ゾーン情報が含まれるようにするには、Unified Communications Manager のインストール後に、タイム ゾーン情報を更新する Cisco Options Package（COP）ファイルをインストールすることができます。大規模なタイム ゾーン変更イベント後には、最新の COP ファイルを https://software.cisco.com/download/navigator.html でダウンロードできることをお知らせします。

CMLocal の設定をローカルの日付と時刻に変更します。

デバイスプールの追加設定

この章では、Unified Communications Manager グループを使用した、電話用 NTP リファレンス、リージョン、コール処理の冗長性などの主な設定について説明します。ただし、デバイスプール設定を使用して次のオプション機能とコンポーネントをデバイスに適用することもできます。

- メディアリソース：会議ブリッジなどのメディアリソースと、保留音（MOH）を、デバイスプール内のデバイスに割り当てます。詳細については、本ドキュメントの「メディアリソース構成タスクフロー」のセクションを参照してください。
- Survivable Remote Site Telephony（SRST）：導入環境で WAN 接続を使用している場合は、SRST を設定することで、WAN が停止した場合に IP ゲートウェイが限定的なコール サポートを提供できるようになります。詳細については、本ドキュメントの「*Survivable Remote Site Telephony* の設定タスクフロー」のセクションを参照してください。
- コールルーティング情報：クラスタ間でコールをルーティングする方法の詳細については、本ドキュメントの「コールルーティングの設定タスクフロー」のセクションを参照してください。

- デバイス モビリティ：デバイス モビリティ グループを設定することで、デバイスが物理的な場所に基づいて設定を使用できるようになります。詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』の「デバイス モビリティの設定」の章を参照してください。

デバイス プールのコア設定の設定タスク フロー

デバイス プールをセットアップし、リージョン、電話用 NTP リファレンス、およびそのデバイス プールを使用するデバイスの冗長性などの設定を適用するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	Network Time Protocol の設定 （88 ページ）	このタスク フローのタスクを実行して、システムにNTPをセットアップします。電話機の NTP 参照を設定し、デバイス プールに割り当てることができる日付/時刻グループにそれらを適用します。
ステップ 2	リージョンの関係の設定 （95 ページ）	これらのタスクを実行して、システムのリージョンを設定します。 最大で2,000のリージョンを作成し、リージョンで提供できる内容に基づいて、カスタマイズしたオーディオ コーデック設定やビット レート制限など、カスタマイズした設定を指定できます。
ステップ 3	Cisco Unified CM グループの設定 （96 ページ）	コール処理の冗長性と負荷分散のための Unified Communications Manager グループを構成します。
ステップ 4	デバイス プールの設定 （97 ページ）	システム デバイスのデバイス プールを設定します。 設定された他のコア設定をデバイス プールに適用します。これらの設定をこのデバイス プールを使用するデバイスに適用します。

Network Time Protocol の設定

システムの Network Time Protocol（NTP）を設定するには、次のタスクを完了します。電話機の NTP 参照を設定し、これらの参照を日付/時刻グループに適用して、デバイスプールに適用できるようにします。

手順

	コマンドまたはアクション	目的
ステップ 1	NTP サーバの追加 （90 ページ）	（オプション）NTP サーバを追加する必要がある場合は、この手順を使用します。最大5台のNTPサーバーを追加できます。 （注） システムのインストール時に、Unified Communications Manager を 1 台の NTP サーバにポイントするように要求されました。NTP サーバを追加する場合は、この手順を使用することができます。その他の場合は、このタスクをスキップします。
ステップ 2	次のいずれかの方法を選択して、NTP メッセージを認証します。 • 対称キー経由での NTP 認証キーの設定 （90 ページ） • オートキー経由での NTP 認証キーの設定 （91 ページ）	（オプション）セキュリティを強化するには、認証済み NTP を設定します。認証を設定するには、対称キーを使用するか、またはキーを使用する必要があります。オートキー メソッドは、共通の条件に準拠するために必要です。
ステップ 3	電話用 NTP リファレンスの設定 （91 ページ）	SIP 電話では、電話用 NTP リファレンスを設定してから、日時グループとデバイスプールを介してそれらを適用する必要があります。
ステップ 4	日時グループの追加 （92 ページ）	システムに接続されているさまざまなデバイスのタイム ゾーンを定義し、設定した電話用 NTP リファレンスを適切な日時グループに割り当てます。

（注） `utils ntp*` コマンド セットなど、NTP のトラブルシューティングと設定に使用する CLI コマンドの詳細については、『コマンドライン インターフェイス リファレンス ガイド』（https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

NTP サーバの追加

NTP サーバを Unified Communications Manager に追加します。

（注） **[設定（Settings）] > [NTサーバ（NTP Servers）]** を選択して、[Cisco Unified OS Administration] ウィンドウの [NTP サーバの設定（NTP Server Configuration）] ウィンドウで NTP サーバを追加することもできます。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 パブリッシャノードが NTP サーバに到達できることを確認するには、**ユーティリティネットワーク ping <ip_address>** を実行して、ip アドレスが NTP サーバのアドレスを表すようにします。

ステップ 3 サーバにアクセス可能な場合は、`ユーティリティ ntp サーバ`を実行して、`<ip_address>` を追加し、サーバを追加します。

ステップ 4 `ユーティリティ ntp 再起動`コマンドを使用して ntp サービスを再起動します。

対称キー経由での NTP 認証キーの設定

この手順を使用して、対称キーを使用してネットワーク内の NTP メッセージを認証します。

（注） SHA1 キーは必ず 1 文字ずつ入力してください。 現在、CLI フレームワークは貼り付けられた値を読み取りません。

手順

ステップ 1 Cisco Unified Communications Manager パブリッシャノードのコマンドラインインターフェイスにログインします。

ステップ 2 [Ntp `auth-対称キーステータス` (ユーティリティ)] コマンドを実行して、現在の ntp 認証設定のステータスを確認します。

ステップ 3 次のいずれかを実行します。

- 対称キーを使用して NTP 認証を有効にするには、`ユーティリティ NTP auth` 対称キーイネーブルCLI コマンドを実行します。
- 対称キーを使用して NTP 認証を無効にするには、`ユーティリティ ntp auth`対称キーを無効にするコマンドを実行します。

ステップ 4 プロンプトに従って、NTP サーバのキー ID と対称キーを入力します。

オートキー経由での NTP 認証キーの設定

PKI ベースの自動キーを使用して NTP 認証を設定する場合は、次の手順を使用します。

（注） 対称キーを使用した NTP 認証が有効になっている場合、自動キーによる認証を有効にするには、このキーを無効にする必要があります。 対称キーを使用した NTP 認証を無効化するには、「対称キー経由での NTP 認証キーの設定 （90 ページ）」を参照してください。

始める前に

オートキー を介した NTP 認証を有効にするには、共通条件モードを有効にする必要があります。 コモン クライテリア モードを有効にする方法の詳細については、『*Cisco Unified Communications Manager* セキュリティ ガイド』の「FIPS セットアップ」の章を参照してください。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 `[Ntp 認証 (auto key status)]` コマンドを実行して、現在の ntp 認証の設定を確認します。

ステップ 3 次のいずれかを実行します。

- NTP 認証を有効にするには、**ユーティリティ用の ntp**認証自動キー有効 CLI コマンドを実行します。
- NTP認証を無効にするには、**utils ntp auth auto-key disable**コマンドラインインターフェースコマンドを実行してください。

ステップ 4 NTP 認証を有効または無効にする NTP サーバの番号を入力します。

ステップ 5 認証を有効にしている場合は、IFF クライアントキーを入力します。 NTP サーバのクライアント キーを貼り付けます。

電話用 NTP リファレンスの設定

SIP 電話に必須の電話用 NTP リファレンスを設定するには、この手順を使用します。 作成した NTP リファレンスは、日時グループを使用してデバイス プールに割り当てることができます。 このリファレンスは、ネットワーク時刻を提供できる適切な NTP サーバに SIP 電話をポイントします。 SCCP 電話機の場合、この設定は必要ありません。

（注） Unified Communications Manager は、マルチキャスト モードおよびエニーキャスト モードをサポートしていません。 これらのモードを選択した場合ではデフォルトのダイレクト ブロードキャスト モードに設定されます。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[電話用NTPリファレンス（Phone NTP Reference）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 電話機が使用するアドレス方式に従って、NTP サーバの IPv4 アドレス、または IPv6 アドレスを入力します。

（注） 電話用 NTP リファレンスの保存には、IPv4 アドレスまたは IPv6 アドレスのいずれかの入力が必要です。 IPv4 電話と IPv6 電話の両方を展開している場合、NTP サーバに、IPv4 アドレスと IPv6 アドレスの両方を設定します。

ステップ 4 [説明（Description）]フィールドに、電話用 NTP リファレンスの説明を入力します。

ステップ 5 [モード（Mode）]ドロップダウン リストから、次のオプションに従い、電話用 NTP リファレンスのモードを選択してください。

- [ユニキャスト（Unicast）]：このモードを選択すると、電話機は、指定した NTP サーバに NTP クエリ パケットを送信します。
- [ダイレクト ブロードキャスト（Directed Broadcast）]：このデフォルトの NTP モードを選択すると、電話機は任意の NTP サーバの日時情報を利用しますが、リストされている NTP サーバ（1 番目 = プライマリ、2 番目 = セカンダリ）を優先します。

（注） Cisco TelePresence および Cisco Spark デバイス タイプは、ユニキャスト モードのみをサポートします。

ステップ 6 **[保存]** をクリックします。

次のタスク

電話用 NTP リファレンスを日時グループに割り当てます。 詳細は、日時グループの追加 （92 ページ）を参照してください。

日時グループの追加

システムのタイムゾーンを定義するように、日付と時刻のグループを設定します。 構成した電話機の NTP 参照を適切なグループに割り当てます。 新しい日付/時間グループをデータベースに追加した後、デバイスプールに割り当てて設定できます。

加えた変更を適用するには、デバイスをリセットする必要があります。

ヒント　Cisco IP 電話の世界的な配布のために、各々のタイムゾーンのために日付/時間グループをつくってください。

手順

ステップ 1　Cisco Unified CM Administration から、**[システム（System）] > [日時グループ（Date/Time Group）]** の順に選択します。

ステップ 2　[新規追加] をクリックします。

ステップ 3　次のグループへの NTP 参照を割り当てます。

a) クリックして**追加電話NTP**参照
b) [**検索とリスト (Phone NTP references**リファレンス)] **ポップアップ**で、[検索 (find)] をクリックし、前のタスクで設定した電話用 ntp 参照を選択します。
c) **[選択項目の追加(Add Selected)]** をクリックします。
d) 複数の参照を追加した場合は、上下の矢印を使用して優先順位を変更します。 上部にある参照は、優先順位が高くなります。

ステップ 4　残りのフィールドを**日付と時刻**のセットウィンドウに設定します。 フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 5　**[保存]** をクリックします。

地域の設定

デバイスプールのリージョンを設定するには、次のタスクを実行します。 リージョン間の関係を設定して、より適切に帯域幅を管理します。 リージョンを使用して、特定のタイプのコール（ビデオ通話など）の最大ビット レートを制御し、特定のオーディオ コーデックに優先順位を設定することができます。

手順

	コマンドまたはアクション	目的
ステップ 1	音声コーデック設定のカスタマイズ（94 ページ）	これはオプションです。 この手順は、使用しているオーディオコーデックの優先順位をカスタマイズする場合に使用します。 このようにして、特定のオーディオコーデックを他のコーデックの先で優先することができます。 それ以外の場合は、デフォルトのオーディオコーデッ

	コマンドまたはアクション	目的
		クリストのいずれかをデバイスプールに割り当てることができます。
ステップ 2	リージョンにおけるクラスタ全体のデフォルト値の設定 （95 ページ）	リージョンにおけるクラスタ全体のデフォルト値を設定します。 [リージョンの設定（Region Configuration）] で異なる値を設定しない限り、すべてのリージョンでこのデフォルト値が使用されます。
ステップ 3	リージョンの関係の設定 （95 ページ）	新しいリージョンを設定するか、既存のリージョンの設定を編集します。 リージョン間およびリージョン内の両方のコールについて、関係を設定します。

音声コーデック設定のカスタマイズ

次の手順を実行して、使用しているオーディオコーデックの優先順位をカスタマイズします。新しい音声コーデック設定リストを作成するには、既存のリストから設定をコピーしてから、新しいリスト内の優先順位を編集します。

（注） オーディオコーデックの優先順位をカスタマイズする必要がない場合は、このタスクを省略できます。デバイスプールを設定する場合は、デフォルトの音声コーデックの優先順位リストのいずれかを割り当てることができます。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [リージョン情報（Region Information）] > [オーディオコーデックの初期設定リスト（Audio Codec Preference List）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [音声**コーデックの基本設定**] ドロップダウンリストボックスから、既存の音声コーデックの優先順位一覧のいずれかを選択します。
選択したリストに対して、優先順位の付いた音声コーデックの一覧が表示されます。

ステップ 4 [Copy]をクリックします。 コピーしたリストからのコーデックの優先順位リストが、新しく作成されたリストに適用されます。

ステップ 5 新しい音声**コーデック**リストの名前を編集します。 たとえば、コモンクライテリアのようになります。

ステップ 6 **説明**を編集します。

ステップ 7 [上 (up)] および [下 (down)] リストボックスに表示される優先順位のある順序でコーデックを移動するには、上矢印と下矢印を使用します。

ステップ 8 **[保存]** をクリックします。

新しいリストをリージョンに適用してから、そのリージョンをデバイス プールに適用する必要があります。 デバイス プール内のすべてのデバイスで、このオーディオ コーデックの初期設定リストが使用されます。

リージョンにおけるクラスタ全体のデフォルト値の設定

リージョンのデフォルト値を設定するには、次の手順を使用します。 これらの設定は、[リージョンの設定（Region Configuration）]ウィンドウ内の個々のリージョンに対してリージョンの関係を設定していない限り、デフォルトですべてのリージョンに対するコールに適用されます。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** を選択します。

ステップ 2 [サーバ（Server）]ドロップダウンリストから、Unified Communications Manager パブリッシャ ノードを選択します。

ステップ 3 [**サービス（Service**）] ドロップダウン リストから、**Cisco CallManager** サービスを選択します。
[サービスパラメータ設定（Service Parameter Configuration）]ウィンドウが表示されます。

ステップ 4 [クラスタ全体のパラメータ（システム-ロケーションとリージョン）（Clusterwide Parameters (System Location and Region)）]で、必要な新しいサービス パラメータ設定を入力します。 サービスパラメータの説明については、パラメータ名をクリックしてヘルプの説明を参照してください。

ステップ 5 **[保存]** をクリックします。

リージョンの関係の設定

リージョンを作成し、特定のリージョン間のコールにカスタム設定を割り当てるには、この手順を使用します。 優先するオーディオ コーデックおよび最大ビットレートなどの設定を編集できます。 たとえば、ネットワークの他の部分よりも帯域幅が小さいリージョンがある場合は、そのリージョンに対するビデオ通話のセッション ビットレートの最大値を編集することができます。 この値は、そのリージョンで提供可能な値にリセットすることができます。

（注） 拡張性を高めるため、また、システムが使用するリソースを少なくするために、[サービスパラメータの設定（Service Parameters Configuration）]ウィンドウでは、できるだけデフォルト値を使用することを推奨します。

手順

ステップ 1 Cisco Unified CM Administration で、**[システム（System）]** > **[リージョン情報（Region Information）]** > **[リージョン（Regions）]** を選択します。

ステップ 2 次のいずれかを実行します。

- **[検索（Find）]** をクリックします。
- **[新規追加（Add New）]**をクリックして新しいパーティションを作成します。
- リージョンの [名前（Name）]を入力します。 たとえば「NewYork」と入力します。
- **[保存]** をクリックします。

読み取り専用の [リージョンの関係（Region Relationships）] 領域には、選択したリージョンと別のリージョンの間で設定したカスタマイズ済みの設定が表示されます。

ステップ 3 このリージョンと別のリージョンの間（またはリージョン内コールの場合は同一リージョン）の設定を変更するには、[他のリージョンとの関係を変更（Modify Relationships to other Regions）] 領域の設定を編集します。

a) [リージョン（Region）]領域で、他方のリージョンを強調表示します（リージョン内コールの場合は、設定中の同じリージョンを強調表示します）。
b) 隣接するフィールドの設定を編集します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。
c) **[保存]** をクリックします。
新しい設定が、[リージョンの関係（Region Relationships）]領域にカスタム ルールとして表示されます。

（注） 一方のリージョン内でリージョンの関係を編集すると、その設定が他方のリージョンで自動的に更新されるため、他のリージョンにその設定を複製する必要はありません。 たとえば、**[リージョンの設定（Region Configuration）]** ウィンドウでリージョン 1 を開き、リージョン 2 とのカスタム関係を設定するとします。次にリージョン 2 を開くと、**[リージョンの関係（Region Relationships）]** 領域にカスタム関係が表示されます。

Cisco Unified CM グループの設定

デバイス プール内のデバイスに対して、コール処理の冗長性、ロード バランシング、およびフェールオーバーを行うための Unified Communications Manager グループを設定するには、この手順を使用します。

ヒント　クラスタノード間でデバイス登録が均等に分散される分散コール処理を提供するために、複数のグループとデバイスプールを設定して、プライマリサーバを各グループで異なるようにします。

（注）　このサーバグループは記述的ではなく、混乱を引き起こす可能性があるため、このデフォルトサーバグループは使用しないでください。

手順

ステップ 1　Cisco Unified CM Administration から、**[システム（System）] > [Cisco Unified CMグループ（Cisco Unified CM Group）]** を選択します。

ステップ 2　[Name]にグループの名前を入力します。

（注）　グループを他のユーザと簡単に区別できるように、名前に含まれるノードの順序を識別することを検討してください。 たとえば、CUCM_PUB のようになります。

ステップ 3　この Unified Communications Manager グループを、自動登録を有効化したときのデフォルトの Unified Communications Manager グループにする場合は、[自動登録のCisco Unified Communications Managerグループ（Auto-registration Cisco Unified Communications Manager Group]チェックボックスをオンにします。

ステップ 4　[使用可能なCisco Unified Communications Manager （Available Cisco Unified Communications Managers）]のリストから、このグループに追加するノードを選択し、下向き矢印をクリックして選択します。 グループには最大 3 台のサーバを追加できます。
このグループのサーバは、[選択されたCisco Unified Communications Manager（Selected Cisco Unified Communications Managers）]リスト ボックスに表示されます。 リストの 1 番上にあるサーバがプライマリ サーバです。

ステップ 5　プライマリ サーバおよびバックアップ サーバを変更するには、[選択されたCisco Unified Communications Manager（Selected Cisco Unified Communications Managers）]リスト ボックスの横にある矢印を使用します。

ステップ 6　**[保存]** をクリックします。

デバイス プールの設定

システム デバイスのデバイス プールを設定します。 設定された他のコア設定をデバイス プールに適用します。これらの設定をこのデバイス プールを使用するデバイスに適用します。 導入のニーズに合わせて、複数のデバイス プールを設定できます。

始める前に

SRST 設定を割り当てる場合は、「Survivable Remote Site Telephony の設定タスク フロー （134 ページ）」を参照してください。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[デバイスプール（Device Pool）]** を選択します。

ステップ 2 次のいずれかを実行します。

- [新規追加（Add New）]をクリックして新しいデバイス プールを作成します。
- [検索（Find）]をクリックし、既存のデバイス グループを選択します。

ステップ 3 [デバイスプール名（Device Pool Name）]フィールドに、デバイス プールの名前を入力します。

ステップ 4 [Cisco Unified Communications Managerグループ（Cisco Unified Communications Manager Group）]ドロップダウンで、コール処理の冗長性と負荷分散を処理するように設定したグループを選択します。

ステップ 5 [日時グループ（Date/Time Group）]ドロップダウン リストから、このデバイス プールを使用するデバイスの日付、時刻、および電話用 NTP リファレンスを処理するように設定したグループを選択します。

ステップ 6 [リージョン（Region）]ドロップダウン リスト ボックスから、このデバイス プールに適用するリージョンを選択します。

ステップ 7 [メディアリソースグループリスト（Media Resource Group List）]ドロップダウン リストから、このデバイス プールに適用するメディア リソースが含まれるリストを選択します。

ステップ 8 このデバイス プールに SRST 設定を適用します。

a) [SRSTリファレンス（SRST Reference）]ドロップダウン リストから、SRST リファレンスを割り当てます。

b) [接続モニタ時間（Connection Monitor Duration）]フィールドに値を割り当てます。 この設定では、電話機が SRST から登録解除して Unified Communications Manager に再登録するまでに、Unified Communications Manager との接続をモニタする時間を定義します。

ステップ 9 [デバイスプールの設定（Device Pool Configuration）]ウィンドウで、残りのフィールドに入力します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 10 **[保存]** をクリックします。

次のタスク

導入要件に応じて、複数のデバイス プールを設定します。

基本的なデバイス プール設定フィールド

表 *5:* 基本的なデバイス プール設定フィールド

フィールド	説明
[デバイスプール名（Device Pool Name）]	新しいデバイスプールの名前を入力します。 名前は最大 50 文字までで、英数字、ピリオド（.）、ハイフン（-）、アンダースコア（_）、および空白を使用できます。
[Cisco Unified CMグループ（Cisco Unified Communications Manager Group）]	このデバイス プール内のデバイスに割り当てる Cisco Unified Communications Manager グループを選択します。 Cisco Unified Communications Manager グループでは、最大 3 つの Unified Communications Manager ノードについて優先順位を設定したリストを指定します。 リストの最初のノードはそのグループのプライマリ ノードとして動作し、グループの他のメンバーは、冗長性のためのバックアップ ノードとして動作します。
Date/Time Group	このデバイス プール内のデバイスに割り当てる日時グループを選択します。 日時グループは、タイムゾーン、および日付と時刻の表示形式を指定します。
Region	このデバイス プール内のデバイスに割り当てるリージョンを選択します。 リージョンの設定値は、リージョン内および他のリージョン間でコールに使用できる音声コーデックを指定します。

通話保持

Unified Communications Manager のコール保留機能は、Unified Communications Manager で障害が発生したとき、またはコールをセットアップする Unified Communications Manager とデバイスの間の通信で障害が発生したときに、コールが中断しないようにするものです。

Unified Communications Manager は、幅広い Cisco Unified Communications デバイスに対してコール保存を完全にサポートしています。 このサポートには、Cisco Unified IP Phone、Foreign Exchange Office（FXO）（非ループスタート トランク）および Foreign Exchange Station（FXS）インターフェイスをサポートする Media Gateway Control Protocol（MGCP）ゲートウェイが含まれ、会議ブリッジ、MTP、およびトランスコーディング リソース デバイス間のコール保持もある程度含まれます。

高度なサービス パラメータ、[ピアがH.323コールを保持できるようにする（Allow Peer to Preserve H.323 Calls）] を [True] に設定することで、H.323 コール保持を有効にします。

次のデバイスおよびアプリケーションは、コール保持をサポートしています。 双方が以下のいずれかのデバイスを介して接続すると、Unified Communications Manager はコール保存を維持します。

- Cisco Unified IP 電話

- SIP トランク
- ソフトウェア会議ブリッジ
- ソフトウェア MTP
- ハードウェア会議ブリッジ（Cisco Catalyst 6000 8 Port Voice E1/T1 and Services Module、Cisco Catalyst 4000 Access Gateway Module）
- トランスコーダ（Cisco Catalyst 6000 8 Port Voice E1/T1 and Services Module、Cisco Catalyst 4000 Access Gateway Module）
- 非 IOS の MGCP ゲートウェイ（Catalyst 6000 24 Port FXS Analog Interface Module、Cisco DT24+、Cisco DE30+、Cisco VG200）
- Cisco IOS H.323 ゲートウェイ（Cisco 2800 シリーズ、Cisco 3800 シリーズなど）
- Cisco IOS MGCP ゲートウェイ（Cisco VG200、Catalyst 4000 Access Gateway Module、Cisco 2620、Cisco 3620、Cisco 3640、Cisco 3660、Cisco 3810）
- Cisco VG248 Analog Phone Gateway

次のデバイスとアプリケーションでは、コール保存をサポートしていません。

- アナンシエータ
- H.323 エンドポイント（NetMeeting またはサードパーティの H.323 エンドポイントなど）
- CTI アプリケーション
- TAPI アプリケーション
- JTAPI アプリケーション

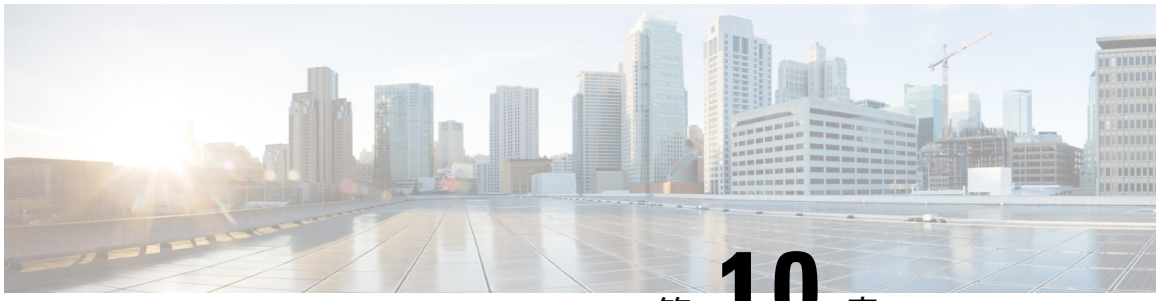
コール保持のシナリオ

次の表で、さまざまなシナリオでコール保存がどのように処理されるのかを説明します。

表 *6:* コール保持のシナリオ

シナリオ	コール保持の処理
Unified Communications Manager で障害が発生した場合。	Unified Communications Manager で障害が発生すると、障害が発生した Unified Communications Manager によってセットアップされたすべてのコールのコール処理機能が失われます。 Unified Communications Manager は、エンド ユーザがコールを終了するか、メディア接続の解放をデバイスが判別できるまで、影響を受けるアクティブなコールを維持します。 ユーザは、この障害の結果として維持されているコールに対して、コール処理機能を呼び出すことはできません。

シナリオ	コール保持の処理
Unified Communications Managerとデバイスの間で通信障害が発生した場合。	デバイスとそれを制御する Unified Communications Manager との間で通信障害が発生すると、デバイスが障害を認識し、アクティブな接続を維持します。 Unified Communications Manager が通信障害を認識し、通信が失われたデバイスでのコールに関連付けられているコール処理エンティティを消去します。 Unified Communications Manager は、影響を受けるコールに関連付けられている、障害が発生していないデバイスの制御を維持します。 Unified Communications Manager は、エンド ユーザがコールを終了するか、メディア接続の解放をデバイスが判別できるまで、影響を受けるアクティブなコールを維持します。 ユーザは、この障害の結果として維持されているコールに対して、コール処理機能を呼び出すことはできません。 （注） フェールオーバーが実行された場合、キープアライブ タイマー内で Unified CM ノードを表示すると、コールが保存モードになっていても、電話機は現在のノードに登録されたままになります。 これは、キープアライブ タイマーが有効である場合に発生する可能性があります。
デバイスの故障 （電話機、ゲートウェイ、会議ブリッジ、トランスコーダ、MTP）	デバイスに障害が発生すると、デバイス経由で存在する接続によってストリーミング メディアが停止します。 アクティブな Unified Communications Manager は、デバイスの障害を認識し、障害が発生したデバイスでのコールに関連付けられているコール処理エンティティを消去します。 Unified Communications Manager は、影響を受けるコールに関連付けられている、障害が発生していないデバイスの制御を維持します。 問題が発生していないユーザがコールを終了するか、問題が発生していないデバイスがメディア接続の解放を判別できるまで、Unified Communications Manager が、問題が発生していないデバイスに関連付けられているアクティブな接続（コール）を維持します。



第 10 章

トランクの設定

SIP トランクの概要

コール制御シグナリング用に SIP を展開する場合、SIP ゲートウェイ、SIP プロキシ サーバ、Unified Communications アプリケーション、会議ブリッジ、リモート クラスタ、または Session Management Edition などの外部デバイスに Cisco Unified Communications Manager を接続するための SIP トランクを設定します。

Cisco Unified CM Administration の内部で、[SIP Trunk Configuration] ウィンドウには、Cisco Unified Communications Manager が SIP コールの管理に使用する SIP シグナリング設定が含まれています。

1 つの SIP トランクに、IPv4 または IPv6 のアドレッシング、完全修飾ドメイン名、または単一の DNS SRV レコードを使用して、最大 16 個の異なる宛先アドレスを割り当てることができます。

SIP トランクの前提条件

SIP トランクを設定する前に、次の操作を実行してください。

- トランク接続を理解できるようにネットワークトポロジを計画します。
- トランクを接続するデバイスと、それらのデバイスが SIP を実装する方法を理解していることを確認します。

- トランク用にデバイス プールが設定されていることを確認します。
- トランクに IPv6 を展開する場合は、クラスタ全体のエンタープライズ パラメータを使用するか、トランクに適用できる共通のデバイス設定をしようして、トランクのアドレッシング設定を指定する必要があります。
- トランクを使用するアプリケーションに SIP の相互運用性の問題がある場合は、デフォルトの SIP 正規化または透過性スクリプトの使用が必要になる場合があります。デフォルトのスクリプトのいずれも要件に合わない場合は、独自のスクリプトを作成できます。カスタマイズされた SIP 正規化および透過性スクリプトの作成の詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』を参照してください。

SIP トランクの設定タスク フロー

SIP トランクをセットアップするには、この手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	SIP プロファイルの設定 （104 ページ）	SIP トランクに適用する共通の SIP 設定項目を指定します。
ステップ 2	SIP トランク セキュリティ プロファイルの設定 （105 ページ）	TLS シグナリングまたはダイジェスト認証などのセキュリティ設定を使用して、セキュリティ プロファイルを設定します。
ステップ 3	SIP トランクの設定 （106 ページ）	SIP トランクをセットアップして、そのトランクに SIP プロファイルとセキュリティ プロファイルを適用します。

SIP プロファイルの設定

共通 SIP 設定を使用して SIP プロファイルを設定するには、この手順を使用します。設定した SIP プロファイルは、このプロファイルを使用する SIP デバイスおよびトランクに割り当てることができます。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[SIPプロファイル（SIP Profile）]** を選択します。

ステップ 2 次のいずれかの手順を実行します。

- 既存のプロファイルを編集するには、**[検索（Find）]**をクリックし、SIP プロファイルを選択して既存のプロファイルを編集します。
- 新しいプロファイルを作成するには、[新規追加（Add New）]をクリックします。

ステップ 3 SIP 電話とトランクで IPv4 と IPv6 のスタックをサポートする場合は、[ANATの有効化（Enable ANAT）]チェックボックスをオンにします。

ステップ 4 SDP の相互運用性を解決するために SDP 透過性プロファイルを割り当てる場合は、[SDP透過性プロファイル（SDP Transparency Profile）]ドロップダウン リストから割り当てます。

ステップ 5 SIP の相互運用性の問題を解決するために正規化スクリプトまたは透過性スクリプトを割り当てる場合は、[正規化スクリプト（Normalization Script）]ドロップダウン リストからスクリプトを選択します。

ステップ 6 （任意） Cisco の**統合された境界要素**を越えてコールをルーティングする必要がある場合は、グローバルダイヤルプランのレプリケーション展開について、[ILS で学習した場合の通知先ルート文字列の送信] チェックボックスをオンにします。

ステップ 7 [SIPプロファイルの設定（SIP Profile Configuration）]ウィンドウで、残りのフィールドを入力します。 フィールドと設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 8 **[保存]** 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

セキュリティ設定を使用してSIP中継セキュリティプロファイルを構成し、要約アイデンティティ認証やトップドメイン名システムシグナリング暗号化などを行う。プロファイルをSIPトランクに割り当てると、トランクはセキュリティプロファイルの設定を取得します。

（注） SIP トランクに SIP トランクのセキュリティ プロファイルを割り当てない場合は、Cisco Unified Communications Manager は、デフォルトで、非セキュア プロファイルを割り当てます。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[セキュリティ（Security）]** > **[SIPトランクのセキュリティプロファイル（SIP Trunk Security Profile）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 TLS を使用した SIP シグナリング暗号化を有効化するには、次の手順を実行します。

a) [デバイスのセキュリティモード（Device Security Mode）]ドロップダウン リストから、[暗号化（Encrypted）]を選択します。

b) [着信転送タイプ（Incoming Transport Type）]および [発信転送タイプ（Outgoing Transport Type）]のドロップダウン リストから、[TLS]を選択します。

c) デバイスの認証で、[X.509 のサブジェクト名（X.509 Subject Name）]フィールドで、X.509 証明書のサブジェクト名を入力します。
d) [着信ポート（Incoming Port）]フィールドに、TLS リクエストを受信するポートを入力します。 TLS のデフォルトは 5061 です。

ステップ 4 ダイジェスト認証を有効にするには、次の内容を実行します。

a) [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。
b) システムが新しいナンスを生成するまでの時間（秒数）を[ナンス有効時間（Nonce Validity Time）]に入力します。 デフォルトは 600（10 分）です。
c) アプリケーションのダイジェスト認証を有効にするには、[アプリケーションレベル認証を有効化（Enable Application Level Authorization）]チェックボックスをオンにします。

ステップ 5 **[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）]** ウィンドウで追加フィールドを設定します。フィールドと設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 6 **[保存]** をクリックします。

（注） トランクが設定を使用するためには、**そのプロファイル**をトランク設定ウィンドウでトランクに割り当てる必要があります。

SIP トランクの設定

SIP トランクを設定するには、この手順を使用します。 1 つの SIP トランクには最大 16 個の宛先アドレスを割り当てることができます。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[トランク（Trunk）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [トランクタイプ（Trunk Type）]ドロップダウン リストから [SIP トランク（SIP Trunk）]を選択します。

ステップ 4 [プロトコルタイプ（Protocol Type）]ドロップダウン リストから、導入環境に適した SIP トランクのタイプを選択し、[次へ（Next）]をクリックします。

- **[なし（None）]（デフォルト）**
- **[Call Control Discovery（コール制御検出）]**
- **[クラスタ間のエクステンションモビリティ（Extension Mobility Cross Cluster）]**
- **[Cisco Intercompany Media Engine]**
- **[IP マルチメディア システム サービス コントロール（IP Multimedia System Service Control）]**

ステップ 5 （オプション）このトランクに**共通デバイス設定**を適用する場合は、ドロップダウン リストから設定を選択します。

ステップ 6 暗号化されたメディアをトランクを介して送信する場合は、[SRTPを許可（SRTP Allowed）] チェックボックスをオンにします。

ステップ 7 すべてのクラスタ ノードに対してトランクを有効化する場合は、[すべてのアクティブなUnified CMノードで実行（Run on All Active Unified CM Nodes）]チェックボックスをオンにします。

ステップ 8 SIP トランクの宛先アドレスを設定します。

a) [宛先アドレス（Destination Address）]テキスト ボックスに、トランクに接続するサーバまたはエンドポイントの IPv4 アドレス、完全修飾ドメイン名、または DNS SRV レコードを入力します。

b) トランクがデュアル スタック トランクの場合は、[宛先アドレス IPv6（Destination Address IPv6）]テキスト ボックスに、トランクに接続するサーバまたはエンドポイントの IPv6 アドレス、完全修飾ドメイン名、または DNS SRV レコードを入力します。

c) 宛先が DNS SRV レコードの場合は、[宛先アドレスは SRV（Destination Address is an SRV）] チェック ボックスをオンにします。

d) 接続先を追加するには、**[+]** をクリックします。

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）]** ドロップダウン リスト ボックスから、このトランクに SIP トランク セキュリティプロファイルを割り当てます。このオプションを選択しない場合は、非セキュア プロファイルが割り当てられます。

ステップ 10 [SIPプロファイル（SIP Profile）]ドロップダウン リストから、SIP プロファイルを割り当てます。

ステップ 11 （任意） この SIP トランクに正規化スクリプトを割り当てる場合は、[正規化スクリプト（Normalization Script）]ドロップダウン リストから、割り当てるスクリプトを選択します。

ステップ 12 [Trunk Configuration]ウィンドウのその他のフィールドを設定します。 フィールドと設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 13 **[保存]** をクリックします。

SIP トランクの連携動作および制限

機能	説明
複数のセキュア SIP トランクを同じ宛先に接続する	リリース 12.5(1) では、Cisco Unified Communications Manager は、同じ宛先 IP アドレスと宛先ポート番号に対する複数のセキュア SIP トランクの設定をサポートします。 これには、以下の新しい機能や利点があります。 • 帯域幅の最適化：緊急コール用に帯域幅が制限されないルートを提供します。 • 特定のリージョンまたはコーリング サーチ スペースの設定に基づく選択的ルーティング

機能	説明
Unified Communications Manager は SIP 180 Ringing の受信時に SIP-UPDATE メッセージを送信する	コールフローで「UPDATE」の値がサポートされている場合、SIP トランクは「183 Session Progress」後に「180 Ringing」を受信すると「UPDATE」SIP メッセージを送信します。
BFCP を使用したプレゼンテーション共有	シスコのエンドポイント向けにプレゼンテーション共有を導入する場合は、すべての中継 SIP トランクの SIP プロファイルで [BFCPを使用したプレゼンテーション共有を許可（Allow Presentation Sharing with BFCP）]チェックボックスがオンになっていることを確認します。 （注） サードパーティ SIP エンドポイントの場合は、[電話の設定（Phone Configuration）]ウィンドウでも同じチェックボックスがオンになっていることを確認してください。
IX チャネル	iX メディア チャネルを導入する場合は、すべての中継 SIP トランクでて使用される SIP プロファイルで [iXアプリケーションメディアを許可（Allow iX Application Media）]チェックボックスがオンになっていることを確認します。 （注） 暗号化された iX チャネルの詳細については、『*Cisco Unified Communications Manager* セキュリティ ガイド』を参照してください。
90 日間の評価ライセンス	90 日の評価期間を使用して実行している間、セキュア SIP トランクを導入することはできません。セキュア SIP トランクを導入するには、製品登録トークンで [エクスポート管理された機能を許可（Allow export-controlled functionality）] を選択した Smart Software Manager アカウントにシステムを登録してある必要があり ます。

H.323 トランクの概要

H.323 を導入している場合は、H.323 トランクがリモート クラスタと、ゲートウェイなどのその他の H.323 デバイスに接続を提供します。H.323 トランクは、Unified Communications Manager がクラスタ内通信でサポートするオーディオ コーデックおよびビデオ コーデックのほとんどをサポートします。ただし、広帯域オーディオおよび広帯域ビデオについてはサポートしません。H.323 トランクは、コール制御シグナリング用に H.225 プロトコルを使用し、メディア シグナリング用に H.245 プロトコルを使用します。

Cisco Unified CM Administration で、クラスタ間トランク（ゲートキーパー非制御）トランク タイプとプロトコル オプションを使用して H.323 トランクを設定できます。

非ゲートキーパー H.323 導入環境の場合は、Unified Communications Manager が IP WAN 経由でコールできるように、リモート クラスタ内の各デバイス プールに個別のクラスタ間トランク

を設定する必要があります。 クラスタ間トランクは、リモート デバイスの IPv4 アドレスまたはホスト名を静的に指定します。

単一のトランクには最大 16 件の宛先アドレスを設定できます。

クラスタ間トランク

2つのリモート クラスタ間にクラスタ間トランク接続を設定する場合は、一方のトランクが使用する宛先アドレスがリモート クラスタのトランクが使用するコール処理ノードと一致するように、クラスタごとにクラスタ間トランクを設定し、トランク設定を一致させる必要があります。 次に例を示します。

- リモート クラスタ トランクが [すべてのアクティブ ノードで実行（Run on all Active Nodes）] を使用する：リモート クラスタ トランクは、コール処理とロード バランシングにすべてのノードを使用します。 ローカル クラスタ内から始まるローカル クラスタ間トランクでは、リモート クラスタ内の各サーバの IP アドレスまたはホスト名を追加します。
- リモート クラスタで [すべてのアクティブノードで実行（Run on all Active Nodes）] を使用しない：リモート クラスタ トランクは、コール処理およびロード バランシング用にトランクのデバイス プールに割り当てられた Unified Communications Manager グループのサーバを使用します。 ローカルのクラスタ間トランク設定では、リモート クラスタ トランクのデバイス プールで使用される Unified Communications Manager グループから各ノードの IP アドレスまたはホスト名を追加する必要があります。

セキュアなトランク

H.323 トランクのセキュアなシグナリングを設定するには、トランクに IPSec を設定する必要があります。 詳細については、『*Cisco Unified Communications Manager* セキュリティ ガイド』を参照してください。 メディア暗号化を許可するようにトランクを設定するには、[トランクの設定（Trunk Configuration）] ウィンドウで [SRTP を許可する（SRTP allowed）] チェックボックスをオンにします。

（注） ゲートキーパーは今では広く使用されていませんが、ゲートキーパー制御のトランクを使用するようにH.323導入を設定することもできます。 ゲートキーパーが制御するトランクを設定する方法の詳細については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド リリース *10.0(1)*』を参照してください。

H.323 トランクの前提条件

「H-323」導入トポロジーを計画します。 クラスタ間のトランクについては、対応するリモートクラスタがコール処理とロードバランシングに使用されるサーバを認識していることを確認してください。 リモートクラスタ内のトランクによって使用される各コール処理サーバに接続するには、ローカルインタークラスタトランクを設定する必要があります。

トランクでのロードバランシングのためにトランクデバイスプールに割り当てられた Cisco Unified Communications Manager グループを使用している場合は、デバイス プールのコア設定の設定タスク フロー （88 ページ）の設定を実行します。

H.323 トランクの設定

次の手順を使用して、トランク導入のための設定を構成します。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[トランク（Trunk）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 **中継タイプドロップダウンリストボックス**から、**クラスタ間中継（非ゲートウェイ保護装置制御）**を選択する。

ステップ 4 **[プロトコル(Protocol)]** ドロップダウン リスト ボックスから、**[SCCP]** を選択します。

ステップ 5 [**デバイス名 (**Device Name)] テキストボックスに、トランクの一意の識別子を入力します。

ステップ 6 [**デバイスプール (**device pool)] ドロップダウンリストボックスで、このトランクに設定したデバイスプールを選択します。

ステップ 7 ローカルクラスタ内のすべてのノードをこのトランクの処理用に使用する場合は、**[すべてのアクティブな統合 CM** ノード上で実行 (Run)] チェックボックスをオンにします。

ステップ 8 トランクでの暗号化メディアを許可する場合は、[**srtp 許可** (srtp)] チェックボックスをオンにします。

ステップ 9 H. 235 パススルーを設定する場合は、**h-235 パススルーを許可**するチェックボックスをオンにします。

ステップ 10 リモート Cisco **Unified Communications Manager の情報**セクションで、このトランクの接続先のリモートサーバごとに 1 つの IP アドレスまたはホスト名を入力します。

第 11 章

ゲートウェイの設定

ゲートウェイの概要

シスコは広範な音声およびビデオ ゲートウェイを提供しています。 ゲートウェイは、Unified Communications ネットワークと外部ネットワークとの通信を可能にするインターフェイスを提供します。 従来、ゲートウェイは、PSTN、構内交換機（PBX）、またはアナログ電話や FAX 装置を含むレガシー デバイスなどのレガシー電話インターフェイスに IP ベースの Unified Communications ネットワークを接続するために使用されてきました。 最も単純な形では、音声ゲートウェイが IP インターフェイスとレガシー電話インターフェイスを備え、2 つのネットワークが通信できるようにゲートウェイが 2 つのネットワーク間でメッセージを変換します。

ゲートウェイ プロトコル

大半のシスコのゲートウェイには、複数の導入オプションがあり、多数のプロトコルのいずれかを使用して導入できます。 導入するゲートウェイに応じて、次の通信プロトコルのいずれかを使用してゲートウェイを設定できます。

- メディア ゲートウェイ コントロール プロトコル（MGCP）
- Skinny Call Control Policy（SCCP）
- Session Initiation Protocol （SIP）
- H.323

インターフェイス カード

外部ネットワークに接続インターフェイスを提供するには、ベンダーインターフェイスカード (VIC) をゲートウェイにインストールする必要があります。 ほとんどのゲートウェイには複数の VIC オプションが用意されており、各 VIC ではアナログ接続とデジタル接続に対して、さまざまなポートや接続タイプを提供できます。

ゲートウェイで提供されているプロトコル、カード、および接続については、ゲートウェイのマニュアルを参照してください。

音声ゲートウェイのセットアップ要件

ハードウェアを設置します。

Cisco Unified Communications Manager にゲートウェイを設定する前に、ゲートウェイ ハードウェアに対して次の作業を行う必要があります。

- ゲートウェイのインストールと設定
- ゲートウェイに任意のベンダーインターフェイスカード (VICs) をインストールします。
- CLI を使用して、ゲートウェイの IOS を設定します。

詳細については、ご使用のゲートウェイに付属しているハードウェアとソフトウェアのマニュアルを参照してください。

（注） 多数のゲートウェイ デバイス用のデフォルトのウェブ ページに到達するには、そのゲートウェイの IP アドレスを使用できます。 ハイパーリンクの URL を http://x.x.x.x/ にしてください。ここで、x.x.x.x は、デバイスのドット形式の IP アドレスです。 各ゲートウェイの ウェブページには、そのゲートウェイのデバイス情報とリアルタイムの状況が記載されています。

ゲートウェイの導入計画

Cisco Unified Communications Manager にゲートウェイを設定する前に、ゲートウェイに設定する接続のタイプを十分に考慮してください。 多くのゲートウェイは、MGCP、SIP、H.323、または SCCP のいずれかをゲートウェイ プロトコルとして使用して設定できます。 各導入タイプの接続タイプは、選択するプロトコルおよびゲートウェイにインストールされている VIC によって異なります。 次の点を確認してください。

- 使用ゲートウェイでサポートされているゲートウェイ プロトコル。
- ゲートウェイの VIC でサポートされているポート接続のタイプ。
- 設定予定の接続のタイプ。
- アナログ接続の場合、PSTN、レガシー PBX、またはレガシー デバイスに接続しているか。
- デジタル アクセス接続の場合、T1 CAS インターフェイスまたは PRI インターフェイスに接続しているか。
- FXO 接続の場合、着信コールをどのように転送するか。 着信コールを IVR や自動応答機能に転送しているか。

ゲートウェイの設定タスク フロー

ネットワーク ゲートウェイを Unified Communications Manager に追加するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	導入するプロトコルに応じて、次の手順のいずれかを実行します。 • MGCPゲートウェイの設定 （113 ページ） • SCCP ゲートウェイの設定 （122 ページ） • SIP ゲートウェイの設定 （126 ページ） • H.323 ゲートウェイの設定 （129 ページ）	Unified Communications Manager でゲートウェイを設定します。 多くの Cisco ゲートウェイは、ALP および SCCP、SIP、または H のいずれかを使用して展開できます。ゲートウェイプロトコルとして使用できます。 ゲートウェイのマニュアルを参照して、お使いのゲートウェイがサポートしているプロトコルと導入に最適なプロトコルを確認してください。
ステップ 2	ゲートウェイに対するクラスタ全体のコール分類の設定 （130 ページ）	（**オプション**） ネットワーク内のゲートウェイポートから着信するすべてのコールを内部 (OnNet) または 外部 (OffNet) に分類するように、クラスタ サービスのパラメータを設定します。
ステップ 3	オフネット ゲートウェイ転送のブロック （130 ページ）	（**オプション**）外部（オフネット）ゲートウェイ間のコールを Unified Communications Manager が転送しないようにブロックし、[オフネット間の転送をブロック（Block OffNet to Offnet Transfer）]パラメータを設定します。

MGCPゲートウェイの設定

MGCP 設定を使用するためにシスコのゲートウェイを設定するには、次のタスクを実行します。

始める前に

MCP ゲートウェイの Unified CM ポート接続を確認します。 Cisco Unified CM Administration から **システム** > **Cisco Unified CM** に移動し、サーバを選択して、設定されている MGCP Listen ポートと MGP Keep-alive ポートを確認します。 ほとんどの場合、デフォルトのポート設定から変更する必要はありません。

手順

	コマンドまたはアクション	目的
ステップ 1	MGCP（IOS）ゲートウェイの設定 （115 ページ）	Cisco Unified CM Administration にゲートウェイを追加し、ゲートウェイ プロトコルとして [MGCP] を選択します。 適切なスロットとベンダーのインターフェイス カード（VIC）でゲートウェイを設定します。
ステップ 2	ゲートウェイ ポート インターフェイスの設定 （115 ページ）	ゲートウェイにインストールされている VIC に接続するデバイス用のゲートウェイ ポート インターフェイスを設定します。 ほとんどの VIC には複数のポート接続とオプションがあります。したがって、いくつか別のポートのインターフェイス タイプを設定する必要がある場合があります。 **ヒント** ポート インターフェイスの設定後に、[関連リンク（Related Links）]ドロップダウン リストから [BGCP設定に戻る（Back to MGCP Configuration）]オプションを選択し、[ゲートウェイの設定（Gateway Configuration）]ウィンドウに戻ります。そのウィンドウで、別のポート インターフェイスを選択して設定できます。
ステップ 3	MGCP ゲートウェイでのデジタル アクセス T1 ポートの追加 （120 ページ）	（オプション） デジタル アクセス T1 CAS ポート インターフェイスを設定したら、ゲートウェイに T1 CAS ポートを追加します。 個別にポートを追加したり、同時にポート範囲を追加したりできます。
ステップ 4	ゲートウェイのリセット （122 ページ）	設定の変更は、ゲートウェイをリセットした後に反映されます。

MGCP（IOS）ゲートウェイの設定

Unified Communications Manager に MGCP（IOS）ゲートウェイを追加して設定するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[ゲートウェイ (Gateway)]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [ゲートウェイタイプ（Gateway Type）]ドロップダウン リストからゲートウェイを を選択して、[次へ（Next）]をクリックします。

ステップ 4 [プロトコル（Protocol）]ドロップダウン リストから [MGCP]を選択して、[次へ（Next）]をクリックします。

ステップ 5 [設定済みのスロット、VIC、およびエンドポイント（Configured Slots、VICs and Endpoints）]領域で次の手順を実行します。

a) 各[モジュール（Module）]ドロップダウン リストで、ゲートウェイにインストールされているネットワーク インターフェイス モジュール ハードウェアに対応するスロットを選択します。

b) 各[サブユニット（Subunit）]ドロップダウン リストで、ゲートウェイにインストールされている VIC を選択します。

c) **[保存]** をクリックします。
[ポート（Port）]アイコンが表示されます。 各ポート アイコンは、ゲートウェイで使用可能なポート インターフェイスに対応しています。 ポート インターフェイスを設定するには、該当するポートのアイコンをクリックします。

ステップ 6 [ゲートウェイの設定（Gateway Configuration）]ウィンドウでその他のフィールドを設定します。 フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 7 **[保存]** をクリックします。

ゲートウェイ ポート インターフェイスの設定

ゲートウェイにインストールされている VIC に接続するデバイスのポート接続を設定できます。 ほとんどの VIC には複数のポート接続とオプションがあります。したがって、いくつか別のポートのインターフェイス タイプを設定する必要がある場合があります。

設定するインターフェイスのタイプによって、次の任意のタスクを選択します。

- デジタルアクセス優先ポートの設定 （116 ページ）
- MGCP ゲートウェイのデジタル アクセス T1 ポートの設定 （116 ページ）
- FXS ポートの設定 （117 ページ）

- FXO ポートの設定 （118 ページ）
- BRI ポートの設定 （119 ページ）

デジタルアクセス優先ポートの設定

MGCP（IOS）ゲートウェイの PRI ポート インターフェイスを設定します。

始める前に

MGCP（IOS）ゲートウェイの設定 （115 ページ）

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[ゲートウェイ（Gateway）]** を選択します。

ステップ 2 PRI ポートを設定するゲートウェイを選択するには、[検索（Find）]をクリックします。

ステップ 3 [設定済みのスロット、VICおよびエンドポイント（Configured Slots, VICs, and Endpoints）]領域で、設定する BRI ポートを含むモジュールとサブユニットを見つけ、設定する BRI ポートに対応する [ポート（Port）]アイコンをクリックします。
[ゲートウェイの設定（Gateway Configuration）]ウィンドウに、BRI ポート インターフェイスが表示されます。

ステップ 4 [デバイスプール（Device Pool）]ドロップダウン リストから、デバイス プールを選択します。

ステップ 5 [ゲートウェイの設定（Gateway Configuration）]ウィンドウでその他のフィールドを設定します。 フィールドの説明については、オンライン ヘルプを参照してください。

ステップ 6 **[保存]** をクリックします。

ステップ 7 （任意） ゲートウェイ用にさらにポート インターフェイスを設定するには、[関連リンク（Related Links）]ドロップダウン リストから [MGCPの設定に戻る（Back to MGCP Configuration）]を選択し、[移動（Go）]をクリックします。

[ゲートウェイの設定（Gateway Configuration）]ウィンドウに、ゲートウェイで使用可能なポート インターフェイスが表示されます。

ポートインターフェイスの設定が完了したら、「ゲートウェイのリセット （122ページ）」を参照してください。

MGCP ゲートウェイのデジタル アクセス T1 ポートの設定

MGCP ゲートウェイで、T1 CAS ポートを T1 デジタル アクセス ポート インターフェイスに追加および設定します。

始める前に

MGCP（IOS）ゲートウェイの設定 （115 ページ）

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[ゲートウェイ（Gateway）]** を選択します。

ステップ 2 **[検索（Find）]** をクリックし、ルートクラスシグナリングを設定するゲートウェイを選択します。

ステップ 3 **設定されているスロットの Vics**とエンドポイント領域で、デジタルアクセス T1 (T1) ポートをセットアップするモジュールとサブユニットを見つけて、対応する**ポート**アイコンをクリックします。

ステップ 4 **デバイスプロトコルプル**ダウンリスト**からデジタルアクセスT 1**を選択し、**次のステップ**をクリックします。

ステップ 5 適切なゲートウェイの設定値を入力します。

フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 6 **[保存]** をクリックします。

デジタル アクセス T1 CAS ポート インターフェイスに対するポートの追加の詳細については、「MGCP ゲートウェイでのデジタル アクセス T1 ポートの追加 （120 ページ）」を参照してください。

FXS ポートの設定

MGCP ゲートウェイで Foreign Exchange Station（FXS）のポートを設定します。 FXS ポートを使用して、単純な旧式の電話サービス（POTS）の従来型の電話や、ファックス装置、スピーカーフォン、従来型のボイスメッセージング システム、自動音声応答（IVR）などの従来型のデバイスに、ゲートウェイを接続することができます。

始める前に

ポートを設定する前に、ゲートウェイを追加する必要があります。

手順

ステップ 1 Cisco Unified CM Administration で、**[デバイス（Device）]** > **[ゲートウェイ（Gateway）]** を選択します。

ステップ 2 [検索（Find）]をクリックして、FXS ポートを設定するゲートウェイを選択します。

ステップ 3 [設定済みのスロット、VIC、およびエンドポイント（Configured Slots, VICs, and Endpoints）]領域で、設定するポートに対応する [FXSポート（FXS Port）]アイコンをクリックします。[ポートの選択（Port Selection）] エリアが表示されます。

ステップ 4 [ポートタイプ（Port Type）]ドロップダウン リストから、設定する接続タイプを選択します。

- [POTS]：従来の電話機などの POTS デバイスにこのポートを接続する場合は、このオプションを選択します。
- [グラウンドスタート（Ground Start）：グランドスタート シグナリングを使用して、ファックス装置、従来型のボイスメッセージング システム、IVR などの従来型の無人デバイスにこのポートを接続する場合は、このオプションを選択します。
- [ループスタート（Loop Start）]：ループ スタート シグナリングを使用して、ファックス装置、従来型のボイスメッセージング システム、IVR などの従来型の無人デバイスにこのポートを接続する場合は、このオプションを選択します。

ステップ 5 [次へ（Next）]をクリックします。
[ポートの設定（Port Configuration）]ウィンドウには、デバイス プロトコルとしてアナログ アクセスを使用するポート インターフェイスの設定が表示されます。

ステップ 6 [デバイスプール（Device Pool）]ドロップダウン リストから、デバイス プールを選択します。

ステップ 7 [電話の設定（Phone Configuration）]ウィンドウで、残りのフィールドを入力します。

フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 8 **[保存]** をクリックします。

ステップ 9 （任意） MGCP IOS ゲートウェイでさらにポート インターフェースを設定するには、[関連リンク（Related Links）]ドロップダウン リストから [ゲートウェイに戻る（Back to Gateway）]リンクを選択し、[移動（Go）]をクリックします。

[ゲートウェイの設定]ウィンドウに、ゲートウェイで使用可能なポートが表示されます。

ポートインターフェイスの設定が完了したら、「ゲートウェイのリセット （122 ページ）」を参照してください。

FXO ポートの設定

MGCP（IOS）ゲートウェイの Foreign Exchange Office (FXO) を設定します。 FXO ポートを使用して、ゲートウェイを PSTN またはレガシー PBX に接続できます。

（注） Unified Communications Manager は、すべてのループ スタート トランクには、Positive Disconnect Supervision（確実な接続解除監視）がないものと想定します。 サーバのフェールオーバー中もアクティブなコールを維持できるように、確実な接続解除監視をグラウンドスタートに指定してトランクを設定します。

始める前に

MGCP（IOS）ゲートウェイの設定 （115 ページ）

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[ゲートウェイ（Gateway）]** を選択します。

ステップ 2 **[検索（Find）]** をクリックし、ルート クラス シグナリングを設定するゲートウェイを選択します。

ステップ 3 [設定済みのスロット、VICおよびエンドポイント（Configured Slots, VICs, and Endpoints）]領域で、FXO ポート インターフェイスをセットアップする FXO ポートを含む**モジュール**および**サブユニット**を見つけて、設定するポートに対応する [ポート（Port）]アイコンをクリックします。

ステップ 4 [ポート タイプ（Port Type）]ドロップダウンリストから、[グラウンドスタート（Ground-Start）]または [ループスタート（Loop-Start）]を選択します。

（注） VIC-2 FXO ポートを設定している場合は、サブユニット モジュールの両方のポートに同じポート タイプを選択する必要があります。

ステップ 5 [デバイスプール（Device Pool）]ドロップダウン リストから、デバイス プールを選択します。

ステップ 6 [アテンダントDN（Attendant DN）]ボックスに、このポート接続からのすべての着信コールをルーティングする電話番号を入力します。 たとえば、1 つのアテンダントの場合は、0 またはディレクトリ番号が表示されます。

ステップ 7 [ポートの設定（Port Configuration）]ウィンドウの他のフィールドに入力します。 フィールドの説明については、オンライン ヘルプを参照してください。

ステップ 8 **[保存]** をクリックします。

ステップ 9 （任意） MGCP IOS ゲートウェイでさらにポート インターフェースを設定するには、[関連リンク（Related Links）]ドロップダウン リストから [ゲートウェイに戻る（Back to Gateway）]リンクを選択し、[移動（Go）]をクリックします。

[ゲートウェイの設定] ウィンドウに、ゲートウェイで使用可能なポートが表示されます。

ポートインターフェイスの設定が完了したら、「ゲートウェイのリセット （122ページ）」を参照してください。

BRI ポートの設定

お互いの IOS ゲートウェイの BRI ポートインターフェイスを設定します。

始める前に

MGCP（IOS）ゲートウェイの設定 （115 ページ）

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[ゲートウェイ（Gateway）]** を選択します。

ステップ 2 BRI ポートを設定するゲートウェイを選択するには、[検索（Find）]をクリックします。

ステップ 3 [設定済みのスロット、VICおよびエンドポイント（Configured Slots, VICs, and Endpoints）]セクションで、BRI ポートを使用するサブユニットを探し、設定するポートに対応する [ポート（Port）]アイコンをクリックします。
[ゲートウェイの設定（Gateway Configuration）]ウィンドウに、BRI ポート インターフェイスの情報が表示されます。

ステップ 4 [デバイスプール（Device Pool）]ドロップダウン リストから、デバイス プールを選択します。

ステップ 5 適切なゲートウェイおよびポートの設定情報を入力します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 6 **[保存]** をクリックします。

ステップ 7 （任意） ゲートウェイ用にさらにポート インターフェイスを設定するには、[関連リンク（Related Links）]ドロップダウン リストから [MGCPの設定に戻る（Back to MGCP Configuration）]を選択し、[移動（Go）]をクリックします。

[ゲートウェイの設定（Gateway Configuration）]ウィンドウに、MGCP ゲートウェイで使用可能なポート インターフェイスが表示されます。

ポートインターフェイスの設定が完了したら、「ゲートウェイのリセット （122 ページ）」を参照してください。

MGCP ゲートウェイでのデジタル アクセス T1 ポートの追加

MGCP ゲートウェイで、T1 CAS ポートを T1 デジタル アクセス ポート インターフェイスに追加および設定します。 最大 24 の T1 CAS ポートを追加および設定できます。 ポートを単独に追加したり、一連のポートを追加したり構成したりすることもできます。 特定のポート範囲を入力する場合、Unified Communications Manager がそのポート範囲全体に設定を適用します。

始める前に

MGCP ゲートウェイのデジタル アクセス T1 ポートの設定 （116 ページ）

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[ゲートウェイ（Gateway）]** を選択します。

ステップ 2 [検索（Find）]をクリックし、T1 CAS ポート インターフェイスを含むゲートウェイを選択します。

ステップ 3 **[新規ポートを追加(Add a New Port)]** をクリックします。

ステップ 4 [ポートタイプ（Port Type）]ドロップダウンリストボックスから、追加するポートのタイプを選択して、[次へ（Next）]をクリックします。

ステップ 5 [開始ポート番号（Beginning Port Number）]と [終了ポート番号（Ending Port Number）]フィールドにポート番号を入力し、追加と設定を行うポート範囲を指定します。

たとえば、1 から 10 のポートを、ポートインターフェイスに同時に追加するには、1と 10を入力します。

ステップ 6 [通信の方向（Port Direction）]ドロップダウンリストボックスから、このポートを通過するコールの方向を設定します。

- [双方（Bothways）]：発着信コールの両方を許可する場合、このオプションを選択します。
- [インバウンド（Inbound）]：着信コールのみを許可する場合、このオプションを選択します。
- [アウトバウンド（Outbound）]：アウトバウンド コールのみを許可する場合、このオプションを選択します。

ステップ 7 EANDM ポートの場合、**[発信者選択]** ドロップダウン リスト ボックスから、このポートに接続されているデバイスからのアウトバウンドコールの発信者番号をどのように表示させるかを選択します。

- **[発信元(Originator)]**：発信側デバイスの電話番号を送信します。
- [最初のリダイレクト番号（First Redirect Number）]：リダイレクト側デバイスのディレクトリ番号を送信します。
- **[最後のリダイレクト番号(Last Redirect Number)]**：最後にコールをリダイレクトするデバイスの電話番号を送信します。
- [最初のリダイレクト番号（外線）（First Redirect Number (External)）]：外部電話マスクが適用されている、リダイレクトを行う最初のデバイスのディレクトリ番号を送信します。
- [最後のリダイレクト番号（外線）（First Redirect Number (External)）]：外部電話マスクが適用されている、リダイレクトを行う最後のデバイスのディレクトリ番号を送信します。

ステップ 8 **[保存]** をクリックします。

ステップ 9 MGCP ゲートウェイに追加のポートを設定するには、**[関連リンク（Related Links）]** から、**[ゲートウェイに戻る（Back to Gateway）]** を選択し、**[移動（Go）]**をクリックします。 デジタル アクセス T1 ポート インターフェイスが表示されたら、次のいずれかの手順を実行します。

- このポートインターフェイスに追加のデジタルアクセス T1 CAS ポートを追加するには、この手順のステップ 3（「**新規ポートの追加**」）に戻ります。
- ゲートウェイで追加のポートインターフェイスを設定するには、[関連リンク（Related Links）]から、[MGCP の設定に戻る（Back to MGCP Configuration）]を選択し、[移動（Go）]をクリックします。 [ゲートウェイの設定（Gateway Configuration）]ウィンドウに、ゲートウェイのサブユニット モジュールで使用可能なポートが表示されます。
- ポートインターフェイスの設定が完了したら、「ゲートウェイのリセット（122ページ）」を参照してください。

ゲートウェイのリセット

ほとんどのゲートウェイは、設定の変更が適用されるようにリセットする必要があります。 リセットを行う前に、必要なゲートウェイ設定をすべて完了することをお勧めします。

（注） H.323 ゲートウェイをリセットしても、Unified Communications Manager にロードされた設定が再初期化されるだけで、ゲートウェイの物理的な再起動やリセットは行われません。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [ゲートウェイ (Gateway)]** を選択します。

ステップ 2 [検索（Find）] をクリックして、ゲートウェイを選択します。

ステップ 3 リセットするゲートウェイの横のチェックボックスをクリックして、[リセット選択済み（Reset Selected）] をクリックします。 [デバイス リセット（Device Reset）] ダイアログ ボックスが表示されます。 次のいずれか 1 つの処理を実行します。

ステップ 4 [**リセット（Reset**）] をクリックします。

MGCP 発信者 ID の制限

FROM ヘッダーに着信 SIP 要求に特殊文字が含まれている場合、SIP-MCP/323 コールフローが影響を受け、システムがコールを切断したり、問題が表示されます。 したがって、要求が接続されている場所からUnified Communications Managerへネットワーキングノードを修正します。

次に例を示します。

- 「Per%cent」のようにアルファベットとともに存在する特殊文字が表示名に影響します。
- 「0%09%0A%01%05%0A%01%03%0A%01%04」のように存在する多くの特殊文字は、CRCX が問題を持つ可能性があるとして、リモート名が MCP 側に送信されるコールを切断する可能性があります。

SCCP ゲートウェイの設定

SCCP 設定を使用するように Cisco ゲートウェイを設定するには、このタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	ゲートウェイ プロトコルとしての SCCP の設定 （123 ページ）	ゲートウェイ プロトコルとして SCCP を使用するように、Cisco ゲートウェイを設定します。
ステップ 2	非設定アナログ 5/5 ポートの自動登録の有効化	非設定アナログ 5/5 ポートの自動登録の有効化
ステップ 3	アナログ電話の自動登録の有効化 （124 ページ）	指定したポートで自動登録を有効化にして、自動登録 DN のプールから DN を取得します。

ゲートウェイ プロトコルとしての SCCP の設定

ゲートウェイ プロトコルとして SCCP を使用するように、Cisco ゲートウェイを設定できます。この導入オプションを使用して、FXS または BRI ポートを使用して、Unified Communications Manager をアナログアクセスデバイスまたは ISDN BRI デバイスに接続できます。 SCCP ゲートウェイをデジタルアクセスの T1 トランクまたは E1 トランクに接続することはできません。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [ゲートウェイ (Gateway)]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 **[ゲートウェイ タイプ（Gateway Type）]** ドロップダウン リスト ボックスで、[Cisco VG200]を選択し、[次へ（Next）] をクリックします。

ステップ 4 [プロトコル（Protocol）] ドロップダウン リストから、[SCCP]を選択します。

ステップ 5 [設定済みのスロット、VICおよびサブユニット（Configured Slots, VICs and Subunits）]セクションで、次の手順を実行します。

a) 個々の [モジュール（Module）] ドロップダウン リストで、ゲートウェイにインストールされているネットワーク インターフェイス モジュールのハードウェアに対応するスロットを選択します。

b) 各 [サブユニット（Subunit）] で、ゲートウェイにインストールされている VIC を選択します。

ステップ 6 [ゲートウェイの設定（Gateway Configuration）]ウィンドウでその他のフィールドを設定します。

フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 7 **[保存]** をクリックします。

[ポート（Port）]アイコンは、サブユニット モジュールの横に表示されます。 各ポートのアイコンは、ゲートウェイで設定可能なポートのインターフェイスに対応します。 該当するポートのアイコンをクリックして、ポートのアナログ アクセスまたは ISDN BRI 電話を設定できます。

ステップ 8 更新を完了したときに、ゲートウェイに変更を適用します。

a) [ゲートウェイのリセット（Reset Gateway）]をクリックします。 [ゲートウェイの再起動（Restart Gateway）]ポップアップが表示されます。

b) [**リセット（Reset）**] をクリックします。

アナログ電話の自動登録の有効化

自動登録 Dn のプールから電話番号を取得するために、指定されたポートの自動登録を有効にします。デフォルトでは、ユニファイドコミュニケーションマネージャはアナログ電話の自動登録を許可しません。管理者は、SCCP プロトコルを使用して、対応するゲートウェイを介して、アナログ電話機を自動登録するようにゲートウェイモジュールを設定する必要があります。

（注） サポートされているゲートウェイタイプは、VG310、VG350、VG400、VG450、および ISR4K シリーズです。

始める前に

- 自動登録を有効化して、新しいエンドポイントがネットワークに接続している間にに割り当てられる DN の範囲を指定します。詳細については、「自動登録の有効化 （456 ページ）」の項を参照してください。
- ゲートウェイで SCCP プロトコルを使用して自動設定を有効にします。詳細については、『SCCP ゲートウェイのための CUCM 自動設定』ガイドを参照してください。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[デバイス（Device）] > [ゲートウェイ（Gateway）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 **[ゲートウェイ タイプ（Gateway Type）]** ドロップダウンリスト ボックスで、[Cisco VG200] を選択し、[次へ（Next）] をクリックします。

ステップ 4 [プロトコル（Protocol）] ドロップダウンリストから、[SCCP] を選択します。

ステップ 5 [**ゲートウェイの詳細 (Gateway Details)**] セクションで、次の手順を実行します。

a) テキストボックスに、**MAC アドレス**の最後の 10 桁を入力します。MAC アドレスを入力すると、[説明（Description）] フィールドの値が自動的に入力されます。

（注） ゲートウェイの MAC アドレスは、イーサネット MAC アドレスか、または SCCP ゲートウェイのインターフェイスで割り当てられた仮想 MAC アドレスであり、Unified Communications Manager と通信します。

MAC アドレスを指定すると、各 FXS ポートは、設定された MAC アドレスとそのポート番号からポート名を取得します。対応するアナログ電話機が自動的にこのゲートウェイに登録されます。

たとえば、[スロット0のモジュール（Module in Slot 0）] ドロップダウンリストで [NM-4VWIC-MBRD] が選択され、[サブユニット0（Subunit 0）] ドロップダウンリストで [VIC3-4FXS/DID-SCCP] が選択された場合、4 個の FXS ポートの値はそれぞれ [0/0/0]、[0/0/1]、[0/0/2]、[0/0/3] と表示されます。各ポートをクリックすると、[電話の設定（Phone Configuration）] ウィンドウの [説明（Description）] フィールドに、対応するポート名が表示されます。表示されるポート名は、MAC アドレスとポート値の組み合わせです。

ゲートウェイは、設定に基づいて、仮想 MAC アドレスまたはイーサネット MAC アドレスを使用して Unified Communication Manager と通信します。仮想 MACアドレスは、破損したゲートウェイを交換した場合でも使用できるため、Unified Communication Manager アプリケーションで設定を変更する必要はありません。

b) 必要な **Cisco Unified Communications Manager グループ**をドロップダウンリストから選択して、自動登録を有効化します。

ステップ 6 [設定済みのスロット、VICおよびエンドポイント（Configured Slots, VICs and Endpoints）] セクションで、次の手順を実行します。

a) 各 [モジュール（Module）] ドロップダウンリストで、ゲートウェイにインストールされているネットワーク インターフェイス モジュール ハードウェアに対応するスロットを選択し、[保存（Save）] をクリックして、それぞれの**サブユニット**を有効化します。

b) 1 つ以上のサブユニットについて、ゲートウェイにインストールされている対応する VIC を選択して、[保存（Save）] をクリックします。

（注） スロットとモジュールは、どのスロットとモジュールにFXSポートが設定されているかを示します。また、FXS ポートの数も示します。

ポートは自動登録されて自動DNを取得するため、ゲートウェイの設定は、ポートレベルまででではなくサブユニットレベルまでとします。たとえば、FXSに対してサブユニットが選択されている場合、対応する FXS ポートが自動登録 DN プールで使用可能な DN を 1 つ選択して、選択されたポートに DN を割り当てます。

ステップ 7 **[設定の適用（Apply Config）]** をクリックします。

ゲートウェイは、ポートが電話に接続されているかどうかに関係なく、FXS で設定されたすべてのポートに登録要求を送信します。

非設定アナログ 5/5 ポートの自動登録の有効化

設定されていないアナログ エフェクト ポートの自動登録を有効にするには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**システム > サービスパラメータ**

ステップ 2 **[サーバ]** ドロップダウン リスト ボックスから、稼働中の必要なサーバを選択します。

ステップ 3 **[サービス]** ドロップダウン リストから、**[Cisco CallManager (アクティブ)]** を選択します。

ステップ 4 **[クラスタワイド パラメータ (Device-PRI および MGCP ゲートウェイ)]** セクションで、**[FXS ポートの自動登録を有効にする]** の値が **[True]** に設定されているか確認してください。

（注） **[FXS ポートの自動登録を有効にする]** を **[False]** に設定して、未設定のアナログ FXS ポートの自動登録を無効にします。

ステップ 5 **[保存]** をクリックします。

トラブルシューティングのヒント

Unified Communications Manager で以下の手順を実行して、ポートが登録され、自動 DN を取得します。

1. ゲートウェイ タイプとして SCCP を設定する
2. 自動登録の有効化
3. デバイス タイプとしてアナログ電話機を選択する
4. 十分な DN が、音声ポートの数に対応するためにプールで使用可能な環境を確保します。

SIP ゲートウェイの設定

次のタスクを実行して、Unified Communications Manager で SIP ゲートウェイを設定します。多くの Cisco ゲートウェイとサードパーティゲートウェイは、SIP を使用するように設定することができます。 Unified Communications Manager には、SIP ゲートウェイ用のゲートウェイデバイスタイプが含まれていません。

始める前に

ネットワークにゲートウェイハードウェアをインストールし、Unified Communications Manager にゲートウェイを追加する前に、ゲートウェイ上で IOS ソフトウェアを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	SIP プロファイルの設定 （127 ページ）	Sip プロファイルを設定し、sip プロファイルに適用します。 トランクはこの設定を使用して SIP ゲートウェイに接続します。
ステップ 2	SIP トランク セキュリティ プロファイルの設定 （127 ページ）	SIP トランク セキュリティ プロファイルを設定して、トランクが SIP ゲートウェイに接続するためにこれを使用するようにします。 デバイスのセキュリティ モード、ダイジェスト認証、着信転送タイプや発信転送タイプの設定などのセキュリティ設定が行えます。
ステップ 3	SIP ゲートウェイ向け SIP トランクの設定 （128 ページ）	SIP ゲートウェイを指すようにすべての SIP トランクを設定する SIP トランク セキュリティ プロファイルをトランクに適用します。

SIP プロファイルの設定

SIP ゲートウェイ接続の SIP プロファイルを設定します。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [SIPプロファイル（SIP Profile）]** を選択します。

ステップ 2 次のいずれかの手順を実行します。

- 新しいプロファイルを作成するには、[新規追加（Add New）]をクリックします。
- 既存の SIP プロファイルを選択するには、**[検索（Find）]** をクリックします。

ステップ 3 [SIP プロファイルの設定（SIP Profile Configuration）]ウィンドウの各フィールドを設定します。

フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 4 **[保存]** 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 ゲートウェイに接続するトランクのセキュリティ設定とともに SIP トランク セキュリティ プロファイルを設定します。

手順

ステップ 1 Cisco Unified CM Administration で、**[システム（System）]** > **[セキュリティ（Security）]** > **[SIP トランク セキュリティプロファイル（SIP Trunk Security Profile）]** を選択します。

ステップ 2 次のいずれかの手順を実行します。

a) 既存のプロファイルを選択するには、[検索（Find）]をクリックします。

b) 新しいプロファイルを作成するには、[新規追加（Add New）]をクリックします。

ステップ 3 [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）]ウィンドウの各フィールドに入力します。

フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 4 **[保存]** をクリックします。

SIP ゲートウェイ向け SIP トランクの設定

SIP を使用するシスコまたはサードパーティのゲートウェイに Unified Communications Manager を接続するように、SIP トランクを設定します。この設定では、[**ゲートウェイの設定（gateway configuration**）] ウィンドウでゲートウェイをデバイスとして入力しないでください。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[トランク（Trunk）]** を選択します。

ステップ 2 [**新規追加**（Add new）] をクリックして新しい SIP トランクを設定します。

ステップ 3 [トランクタイプ（Trunk Type）]ドロップダウン リストから、[SIPトランク（SIP Trunk）]を選択します。

ステップ 4 **[プロトコル（Protocol）]** ドロップダウンリストから、**[SCCP]** を選択します。

ステップ 5 [SIP 情報（SIP Information）] ペインの **[接続先アドレス（Destination Address）]** フィールドに、録音サーバまたは キューブメディア の IP アドレス、完全修飾ドメイン名、または DNS SRV レコードを入力します。

ステップ 6 ドロップダウン リストから、**「SIP トランク セキュリティ プロファイル」**の手順で作成した SIP トランク セキュリティ プロファイルの名前を選択します。

ステップ 7 ドロップダウン リスト ボックスから、この **SIP トランク**に使用する SIP プロファイルを選択します。

ステップ 8 **[トランクの設定]** ウィンドウのフィールドを設定します。フィールドの説明については、オンライン ヘルプを参照してください。

ステップ 9 **[保存]** をクリックします。

H.323 ゲートウェイの設定

Unified Communications Manager で、非ゲートキーパー H.323 の導入環境に対する H.323 ゲートウェイを設定します。

（注） H.323 ゲートキーパーを導入しない場合は、ゲートキーパー制御の H.225 トランクをセットアップして、H.323 ゲートウェイを追加することもできます。 ゲートキーパーの使用率は、近年減少傾向にあるため、このシナリオは本書には記載していません。 ゲートキーパーおよびH.225 ゲートキーパーで制御されるトランクを設定する場合は、『*Cisco Unified Communications Manager* アドミニストレーション ガイド リリース *10.0(1)*』を参照してください。

（注） ゲートウェイを Unified Communications Manager に登録した後に Unified Communications Manager でゲートウェイの登録ステータスが「不明」と表示される場合があります。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [ゲートウェイ (Gateway)]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [ゲートウェイタイプ（Gateway Type）] ドロップダウン リストから、[H.323ゲートウェイ（H.323 Gateway）]を選択します。

ステップ 4 [デバイス名（Device Name）]フィールドに、ゲートウェイの IP アドレスまたはホスト名を入力します。

ステップ 5 H.235 を使用してセキュア チャネルを設定するには、[H.235 データのパススルー（H.235 Data Passthrough）]チェックボックスをオンにします。

ステップ 6 [**ゲートウェイの設定（Gateway Configuration**）] ウィンドウのフィールドを設定します。

フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 7 **[保存]** をクリックします。

ステップ 8 [リセット（Reset）]をクリックしてゲートウェイをリセットし、変更を適用します。

ほとんどのゲートウェイでは、設定の変更を適用するためにリセットする必要があります。 リセットを行う前に、必要なゲートウェイ設定をすべて完了することをお勧めします。

ゲートウェイに対するクラスタ全体のコール分類の設定

ネットワーク ゲートウェイの [コールの分類（Call Classification）]を設定します。 この設定は、システムがネットワークでゲートウェイが内部（OnNet）、または外部（OffNet）であると見なすかどうかを決定します。

[コールの分類（Call Classification）]フィールドが、個々のゲートウェイ ポート インターフェイスの設定ウィンドウに表示されます。デフォルトでは、各ゲートウェイ ポートインターフェイスはクラスタ全体のサービス パラメータの設定を使用するように設定されています。 ただし、ポートでの [コールの分類（Call Clasification）]の設定がクラスタ全体のサービス パラメータとは異なる場合、ポートでの設定がサービス パラメータの設定よりも優先されます。

手順

ステップ 1 Cisco Unified CM の管理から、**[システム（System）] > [サービス パラメータ（Service Parameters）]** の順に選択します。

ステップ 2 [サーバ（Server）]ドロップダウン リストから、Cisco CallManager サービスを実行しているサーバを選択します。

ステップ 3 [サービス（Service）] ドロップダウン リストから、[Cisco CallManager] を選択します。

ステップ 4 [クラスタ全体のパラメータ（デバイス - 概要）（Clusterwide Parameters (Device - General)）]で、[コールの分類（Call Classification）]サービス パラメータに次の値のいずれかを設定します。

- [オンネット（OnNet）] : このゲートウェイからのコールが、企業ネットワーク内から発信されているものと分類されます。
- [オフネット（OffNet）] : このゲートウェイからのコールが、企業ネットワーク外から発信されているものと分類されます。

ステップ 5 **[保存]** をクリックします。

オフネット ゲートウェイ転送のブロック

外部（オフネット）ゲートウェイ間で転送されるコールをブロックするようにシステムを設定する場合は、この手順を使用します。 デフォルトでは、ある外部ゲートウェイから別の外部ゲートウェイへの転送は許可されます。

ゲートウェイが外部（OffNet）であるか内線（OnNet）であるかどうかを判別する設定は、コール分類設定によって決定されます。 これは、クラスタ全体のサービス パラメータを使用するか、次のいずれかのポート インターフェイスを設定することで設定します。

- MGCP T1/E1 ポート インターフェイス
- MGCP FXO ポート インターフェイス
- H.323 ゲートウェイ
- SIP トランク

手順

ステップ 1 Cisco Unified CM の管理から、**[システム（System）] > [サービス パラメータ（Service Parameters）]** の順に選択します。

ステップ 2 [サーバ（Server）]ドロップダウン リストから、Cisco CallManager サービスを実行しているサーバを選択します。

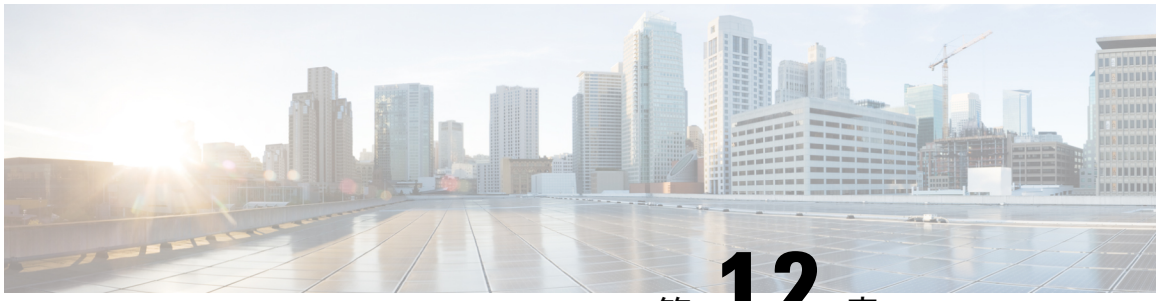
ステップ 3 [サービス（Service）] ドロップダウン リストから、[Cisco CallManager] を選択します。

ステップ 4 [オフネットからオフネットへの転送をブロック（Block OffNet to Offnet Transfer）]サービス パラメータを設定します。

- **True**：2 つの外部（オフネット）ゲートウェイ間の転送をキャンセルするには、このオプションを選択します。
- **False**：2 つの外部（オフネット）ゲートウェイ間の転送を許可するには、このオプションを選択します。 これがデフォルトのオプションです。

ステップ 5 **[保存]** をクリックします。

（注） ゲートウェイをルートパターンに関連付け、**[ルートパターンの設定（Route Pattern Configuration）]** ウィンドウで **[コールの分類（Call Classification）]** を設定することで、ゲートウェイを介してコールをオンネットまたはオフネットに分類することもできます。



第 12 章

SRST の設定

Survivable Remote Site Telephony の概要

Survivable Remote Site Telephony（SRST）は、Unified Communications Manager ノードとのワイドエリア ネットワーク（WAN）接続に依存するサイト用のオプション機能です。 SRST リファレンスは、Unified Communications Manager 管理インターフェイスで構成されています。 WAN の故障が発生した場合、IP ゲートウェイは、次のようにリモートサイトの IP 電話に限定されたテレフォニーサービスを提供することができます。

- リモート サイトの IP 電話は互いにコールできます。
- PSTN からのコールは IP 電話に到達できます。
- IP 電話からのコールは PSTN を介して外部に到達できます。

リモート サイトの電話が、関連付けられているすべての Unified Communications Manager ノードに接続できない場合、SRST リファレンスの IP ゲートウェイに接続します。 IP 電話のステータス行には、IP 電話がバックアップ SRST ゲートウェイにフェールオーバーしたことが示されます。 Unified Communications Manager への接続が復元されると、Unified Communications Manager と完全なテレフォニーサービスに再登録された IP 電話が復元されます。

SRST は、PSTN ゲートウェイ アクセスに加えて、SCCP および SIP エンドポイントが混在している可能性があるリモート サイトをサポートします。

Connection Monitor Duration

ワイドエリア ネットワーク（WAN）を介して SRST ゲートウェイに接続する IP 電話は、WAN リンクを介した Unified Communications Manager との接続を確立できると直ちに Unified Communications Manager に再接続します。 ただし、WAN リンクが不安定な場合、IP 電話は SRST に切り替えたり、 Unified Communications Manager に切り替えたりします。 このため、電話サービスが一時的に失われます（ダイヤル トーンが聞こえません）。 このような再接続

試行は、WAN リンク フラッピング問題と呼ばれ、IP 電話が Unified Communications Manager に正常に再接続するまで続きます。

Unified Communications Managerと SRST ゲートウェイの間で WAN link flapping の問題を解決するために、SRST ゲートウェイおよびレジスターから Unified Communications Manager に対して登録解除されるまで、Unified Communications Manager に対する接続を IP 電話が監視する秒数（接続監視時間）を定義できます。 IP 電話は、XML 設定ファイルに指定された接続モニタ間隔の値を受信します。

Survivable Remote Site Telephony の設定タスク フロー

始める前に

ダイヤル プランを検証します。 ダイヤル プランに 7 か 8 桁の数字があるとき、場合によりトランスレーション ルールを設定する必要があります。 トランスレーション ルールの詳細については、「トランスレーション パターンの設定 （223 ページ）」を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	SRST 参照の設定 （135 ページ）	他のすべての Unified Communications Manager ノードに到達できない場合に、制限付きのコール制御機能を提供するゲートウェイを設定します。
ステップ 2	デバイス プールへの SRST リファレンスの割り当て （135 ページ）	Unified Communications Manager が使用不可になった場合、通常デバイス プールに割当てられる SRST 参照により、発信側デバイスが発信を完了しようとするときに検索するゲートウェイが決定されます。
ステップ 3	次のいずれかの作業を実行します。 • クラスタの接続モニタ間隔の設定（136 ページ） • デバイス プールの接続モニタ間隔の設定 （136 ページ）	**任意**：接続モニタ期間を設定します。クラスタ全体のデフォルト値を適用することも、デバイス プール内のデバイスに設定を適用することもできます。
ステップ 4	SRST Gateway の SRST を有効にする（137 ページ）	ゲートウェイで SRST パラメータを設定します。

SRST 参照の設定

SRST リファレンスは、デバイスのその他すべての Cisco Unified Communications Manager ノードが到達不能の場合に、Cisco Unified Communications Manager の一部機能を利用できるゲートウェイで構成されます。

手順

ステップ 1 Cisco Unified CM Administration にログインし、**[システム（System）] > [SRST（SRST）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [SRST リファレンスの設定（SRST Reference Configuration）]ウィンドウの各フィールドを設定します。 フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 4 **[保存]** をクリックします。

デバイス プールへの SRST リファレンスの割り当て

電話機の各デバイス プールに SRST を設定できます。 デバイス プールに SRST リファレンスを割り当てると、デバイス プールのすべての電話機が、Cisco Unified Communications Manager のノードに到達できない場合、割り当てた SRST に接続を試みます。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [デバイスプール（Device Pool）]** を選択します。

ステップ 2 [検索（Find）]をクリックし、リモート IP 電話が登録されているデバイス プールを選択します。

ステップ 3 [ローミングに合わせて変化する設定（Roaming Sensitive Settings）] エリアの [SRST リファレンス（SRST Reference）] ドロップダウン リストから SRST を選択します。

[SRST リファレンス（SRST Reference）] ドロップダウン リストには次のオプションがあります。

- [無効（Disable）]：電話機は、Cisco Unified Communications Manager のいずれのノードにも到達できない場合、SRST ゲートウェイへの接続を試みません。
- [デフォルト ゲートウェイを使用（Use Default Gateway）]：電話機は、Cisco Unified Communications Manager のいずれのノードにも到達できない場合、IP ゲートウェイを SRST ゲートウェイとして接続を試みます。
- [ユーザ定義（User-Defined）]：電話が任意の Cisco Unified Communications Manager ノードに接続できない場合、SRST ゲートウェイへの接続を試みます。

ステップ 4 **[保存]** をクリックします。

クラスタの接続モニタ間隔の設定

この手順は省略可能です。 接続モニタ間隔のシステム値（エンタープライズ パラメータ）を変更する場合だけ、この手順を完了します。

手順

ステップ 1 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。

ステップ 2 [接続モニタ間隔（Connection Monitor Duration）]フィールドに値を入力します。 デフォルト値は 120 秒です。 フィールドに入力できる最大秒数は、2592000 秒です。

ステップ 3 **[保存]** をクリックします。

（注） 変更を有効にするにはすべてのサービスを再起動する必要があります。

このエンタープライズパラメータには、接続モニタ期間に対するクラスタのデフォルトを設定します。 ただし、それよりも優先される設定がデバイス プールに存在する場合、その設定が、デバイス プールを使用するデバイスのエンタープライズ パラメータ設定よりも優先されます。

デバイス プールの接続モニタ間隔の設定

この手順は省略可能です。 この操作は、次の項目に該当する場合に限り実行します。

- 接続モニタの期間について、クラスタ全体の値を使用しない場合。
- このデバイス プールの接続モニタ期間の値を個別に定義する場合。

ヒント デバイス プールの接続モニタ間隔の値を変更する場合、値は更新されるデバイス プールだけに適用されます。 その他すべてのデバイス プールは、各自の [接続モニタ間隔（Connection Monitor Duration）] フィールドの値を使用するか、[接続モニタ間隔（Connection Monitor Duration）] エンタープライズ パラメータで設定されたクラスタ全体用の値を使用します。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[デバイスプール（Device Pool）]** を選択します。

ステップ 2 [検索（Find）]をクリックし、リモート IP 電話が登録されているデバイス プールを選択します。

ステップ 3 [ローミングに合わせて変化する設定（Roaming Sensitive Settings）] エリアで、[接続モニタ間隔（Connection Monitor Duration）]フィールドに値を入力します。 フィールドに入力できる最大秒数は、2592000 秒です。

（注） この設定は、エンタープライズパラメータの接続モニタ間隔設定をオーバーライドします。

ステップ 4 **[保存]** をクリックします。

SRST Gateway の SRST を有効にする

始める前に

- デバイス プールへの SRST リファレンスの割り当て （135 ページ）
- オプションで次の作業を行うことができます。
  - クラスタの接続モニタ間隔の設定 （136 ページ）
  - デバイス プールの接続モニタ間隔の設定 （136 ページ）

手順

ステップ 1 SRST gateway (ルータ) にログインします。

ステップ 2 **Call-manager-fallback** コマンドを入力します。
このコマンドは、ルータの SRST を有効にします。

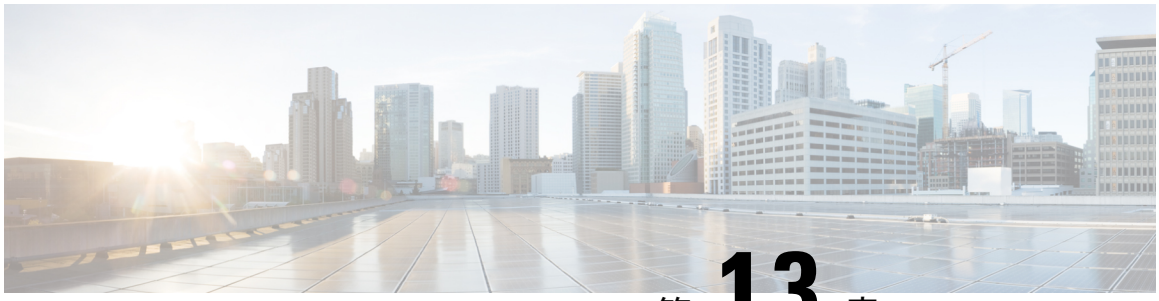
ステップ 3 **max-ephones**max-phones コマンドを入力します。ここで、max-phones は、サポート対象の Cisco IP Phone の最大数です。

ステップ 4 **max-dn**max-directory-numbers コマンドを入力します。ここで、max-directory-numbers は、ルータでサポートされているディレクトリ番号（DN）の最大数または仮想音声ポートです。

ステップ 5 **ip source-address**ip-address コマンドを入力します。ここで、ip-address は、一般的にルータのイーサネット ポートのアドレスの 1 つであるルータ IP アドレスよりも前から存在します。
このコマンドにより、SRSTルータは、指定されたIPアドレスを介してCisco IP 電話からメッセージを受信することができます。

SRST の制限

制約事項	説明
SRST 参照先の削除のヒント	デバイス プールなどの項目が使用しているSRST参照先は削除できません。 SRST リファレンスを使用しているデバイスプールを調べるには、**[SRSTリファレンスの設定（SRST Reference Configuration）]** ウィンドウから **[依存関係レコード（Dependency Records）]** リンクをクリックしてください。 システムで依存関係レコードが有効でない場合、[依存関係レコードサマリー（Dependency Records Summary）] ウィンドウにメッセージが表示されます。 使用中のSRSTリファレンスを削除しようとすると、Unified Communications Manager にエラーメッセージが表示されます。 現在使用中のSRST参照を削除する前に、以下のいずれかまたは二つのタスクを実行してください。 • 削除するSRST参照先を使用しているデバイスプールすべてに、別の SRST 参照先を割り当てます。 • 削除するSRST参照先を使用しているデバイスプールを削除します。 （注） SRST 参照先を削除するときは、削除する SRST 参照先が正しいか慎重に確認してください。 削除した SRST 参照先を元に戻すことはできません。誤って削除した場合は、その SRST 参照先を作成し直す必要があります。



第 13 章

メディア リソースの設定

メディアリソースについて

Cisco Unified Communications Manager 機能では、メディア リソースを使用する必要があります。 Cisco Unified Communications Manager には以下のようなメディアリソースも含まれます。

- アナンシエータ
- 音声自動応答（IVR）（Interactive Voice Response (IVR)）
- メディア ターミネーション ポイント（Media Termination Points）（MTP）
- トランスコーダ
- トラステッド リレー ポイント
- 会議ブリッジ
- 保留中の音楽またはビデオ

メディアリソースをメディアリソースグループの一覧に割り当て、そのリストをデバイスプールまたは個々のデバイスに割り当てることによって、電話で利用可能にすることができます。個々のデバイスのデフォルト設定では、デバイスが使用しているデバイスプールに割り当てられているメディアリソースを使用します。

（注） 保留音の設定の詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』を参照してください。

メディア ターミネーション ポイント

メディアターミネーション ポイント（MTP）は、2 つの全二重メディアストリームを受け入れ、それらのストリームをまとめてブリッジし、個別に設定と分解を行えるようにするためのエンティティです。 Cisco Unified Communications Manager は、MTP をメディアパスに挿入して、次のようなさまざまな状況を解決できます。

- 信頼されたリレー ポイント（TRP）として動作する場合
- RTP ストリームに対して IPv4 と IPv6 の変換を提供する場合
- SIP トランク経由で SIP アーリー オファーを配信する場合。
- DTMF 転送の不一致に対処する場合
- RSVP エージェントとして動作する場合

H.323 コールの MTP

メディア ターミネーション ポイントをH.323 コールのメディア パスに挿入することで、H.323 エンドポイントにコールがルーティングされた場合に通常は利用できない補完的サービス（コール保留、コール転送、コール パーク、会議など）を拡張できます。 H.323 補足サービスでMTP が必要となるのは、Empty Capability Set（ECS）または FastStart をサポートしていないエンドポイントのみです。 ECS および FastStart をサポートしているすべての Cisco および他のサードパーティ製エンドポイントでは、MTP は必要ありません。

MTP のタイプ

Cisco Unified Communications Manager は、次の MTP タイプをサポートしています。

- IOS ゲートウェイのソフトウェア MTP
- IOS ゲートウェイのハードウェア MTP
- Cisco IP Voice Media Streaming サービスが提供するソフトウェア MTP

シスコ メディア ターミネーション ポイント ソフトウェアの MTP タイプでは、ネットワークの速度とネットワーク インターフェイス カード（NIC）に応じて、デフォルトで 48 個のユーザ設定可能な MTP リソースが提供されます。 たとえば、100 MB のネットワークまたは NIC カードの場合、48 の MTP リソースをサポートできますが、10 MB の NIC カードではサポートできません。

10 MB のネットワークまたは NIC カードの場合、約 24 個の MTP リソースを提供できます。 ただし、使用可能なMTP リソースの正確な数は、PC 上の他のアプリケーションが消費しているリソース、プロセッサの速度、ネットワーク負荷、その他のさまざまな要因によって異なります。

MTP の登録

MTP デバイスは、プライマリ Cisco Unified Communications Manager が使用可能である場合は常にその Cisco Unified Communications Manager に登録され、サポートしている MTP リソースの数を Cisco Unified Communications Manager に通知します。 同じ Cisco Unified Communications Manager に複数の MTP を登録できます。 特定の Unified Communications Manager に複数の MTP が登録されている場合、その Cisco Unified Communications Manager は、MTP ごとのリソースセットを制御します。

たとえば、MTP サーバ 1 が 48 の MTP リソース用に設定され、MTP サーバ 2 は 24 のリソース用に設定されているとします。 両方の MTP が同じ Unified Communications Manager を登録する場合、その Unified Communications Manager は両方のリソース セット、つまり、合計 72 の登録済み MTP リソースを保持します。

Unified Communications Manager は、コール エンドポイントで MTP が必要であると判定すると、アクティブ ストリームが最も少ない MTP から MTP リソースを割り当てます。 その MTP リソースは、エンドポイントの代わりにコールに挿入されます。 MTP リソースの使用は、システムのユーザにも、リソースが代わりに挿入されたエンドポイントにも見えない形で行われます。 MTP リソースが必要なときに、そのリソースが使用できない場合、コールは MTP リソースを使用せずに接続されるため、そのコールは補足サービスを利用できないことになります。

SRTP DTMF 相互接続

重要 このセクションは、リリース 14SU3 以降に適用されます。

現在、安全な通話と安全でない通話の両方で DTMF が一致しない場合に、Unified CM によって MTP が挿入されます。 ただし、安全な通話の場合は、MTP が挿入されても、当事者のメディア間で MTP の受け渡しが行われるだけで、 DTMF イベントが当事者間で送受信されることはありません。 Unified CM リリース 14SU3 よりも前のバージョンでは、DTMF 変換は安全でない通話でのみ機能し、DTMF が一致しない場合に MTP が割り当てられていました。

ゲートウェイ IOS バージョン 17.10.1a 以降では、セキュアな MTP はゲートウェイ側でサポートされ、DTMF 変換が行われます。 Unified Communications Manager に登録された IOS ベースのセキュアな MTP で、SRTP と DTMF の相互接続がサポートされるようになりました。 このサポートがリリース 14SU3 以降でゲートウェイ側に追加されたため、セキュアなエンドポイント間で DTMF の不一致があった場合に、Unified CM からハードウェア MTP を（SRTP と DTMF の相互接続サポートにより）呼び出すことが可能になりました。

SRTP キーを Unified Communications Manager から MTP に、SCCP メッセージで送信できます。 MTP はこのキーを使用してインバンド DTMF イベントをアウトオブバンドイベントに復号化し、もう一方のコールレッグに送信します。 同様に、アウトオブバンド DTMF イベントの場合、Unified Communications Manager は暗号化されたインバンド DTMF イベントをもう一方のコールレッグに注入します。

重要な検討事項

- Unified Communications Manager では、リリース 14SU3 以降、以下の Cisco IOS XE 17.10.1a 以降でこの機能をサポートします。
  - Cisco 4461 サービス統合型ルーター（ISR）
  - Cisco Catalyst 8200 シリーズ エッジ プラットフォーム
  - Cisco Catalyst 8300 シリーズ エッジ プラットフォーム
  - Cisco Catalyst 8000V エッジソフトウェア

（注） この機能に必要なゲートウェイ設定の詳細については、サポートされる Cisco IOS XE 17.10.1a 以降のプラットフォームの各設定ガイドを参照してください。

- Unified Communications Manager とゲートウェイ間の TLS 1.2 接続が正常に実行されている必要があります。 TLS 1.2 の設定の詳細については、Cisco Unified Communications Manager セキュリティ ガイドを参照してください。
- この機能は、パススルーモードのハードウェア MTP（パススルーモードでの DTMF-SRTP 相互接続をサポートしている IOS ゲートウェイを使用して登録された MTP）でのみサポートされます。
- この機能は IPVMS ベースの MTP および H.323 コールフローではサポートされません。

メディア ターミネーション ポイントの連携動作と制限事項

表 7: メディア ターミネーション ポイントの連携動作と制限事項

制約事項	説明
Cisco IP 音声ストリームアプリケーション	1 台のサーバでアクティブにできる Cisco IP Voice Streaming Application は 1 つに限定されます。 追加の MTP リソースを提供するには、ネットワーク上にある他のサーバで Cisco IP Voice Streaming アプリケーションをアクティブにすることができます。 Cisco Unified Communications Manager のパフォーマンスに悪影響を与える可能性があるため、コール処理の負荷が大きい Cisco Unified Communications Manager 上では Cisco IP Voice Streaming Media Application をアクティブにしないようにすることを強くお勧めします。

制約事項	説明
Cisco Unified Communications Manager への登録	各 MTP が一度に登録できる Cisco Unified Communications Manager は 1 つに限定されます。 システム内には、設定内容に応じて、複数の MTP を存在させることができます。各 MTP は、1 つの Cisco Unified Communications Manager に登録できます。
フェールオーバーとフォールバック	ここでは、MTP デバイスが登録されている Cisco Unified Communications Manager が到達不能になったときの、MTP デバイスのフェールオーバーとフォールバックの方法について説明します。 • プライマリ Cisco Unified Communications Manager に障害が発生した場合、MTP は、MTP が属するデバイス プールに対して指定された Cisco Unified Communications Manager グループ内で、次に使用可能な Cisco Unified Communications Manager への登録を試みます。 • プライマリ Cisco Unified Communications Manager が障害後に使用可能な状態に戻り、現在まだ使用されていない場合、MTP デバイスはただちにプライマリ Cisco Unified Communications Manager に再登録されます。 • コール保存モードでアクティブだったコールまたは会議は、すべてのパーティが切断されるまで、システムによって保持されます。 システムは、補足サービスを使用可能にしません。 • MTP が新しい Cisco Unified Communications Manager への登録を試み、登録確認応答を受信しなかった場合、MTP は次の Cisco Unified Communications Manager に登録されます。 MTP デバイスは、ハード リセットまたはソフト リセット後に登録を解除し、続いて接続を解除します。 リセットが完了すると、デバイスは Cisco Unified Communications Manager に再登録されます。

トランスコーダ

トランスコーダは、あるコーデックからの入力ストリームを、別のコーデックを使用する出力ストリームに変換する、コーデック変換を実行するデバイスです。たとえば、トランスコーダは G.711 コーデックのストリームを取り込み、それを G.729 ストリームにリアルタイムで変換できます。 エンドポイントが異なる音声コーデックを使用する通話中に、Cisco Unified Communications Manager が、そのメディアパスでトランスコーダを呼び出します。 トランスコーダは、互換性のない2つのコーデック間でデータストリームを変換して、デバイス間の通信を可能にします。トランスコーダは、コールに関連するユーザまたはエンドポイントにも見えることはありません。

トランスコーダのリソースは、メディアリソースマネージャー(MRM)によって管理されます。

Opus コーデック トランスコーダーサポート

重要 このセクションは、リリース 14SU1 以降に適用されます。

Cisco Unified Communications Manager には、メディアネゴシエーションを成功させるために必要な Opus オーディオコーデックのトランスコーディングをサポートする、Skinny Client Control Protocol（SCCP）で制御される iOS ベースの登録済みメディアリソースが含まれるようになりました。

シスコのエンドポイントの大半は Opus コーデックをサポートしています。 Opus コーデックは、低帯域幅環境では G711/G729 よりも高品質で提供します。 Opus コーデック トランスコーダがサポートされている場合、Unified CM は Opus コーデックの不一致についてトランスコーダを呼び出し、Opus コーデック側では低ビットレート、リモート側ではより高いビットレートを使用できます。 ただし、Opus コーデックでサポートされているトランスコーダから Unified CM への登録は成功する必要があります。

サポートされるバージョン

Opus トランスコーディング 機能は、次のUnified Communications Managerとゲートウェイ バージョンで動作します。

- Unified CM バージョン 14 SU1 以上
- ゲートウェイ IOS バージョン IOS XE 17.6.1
- DSP ファームウェアバージョン 58.2.0 以降

設定

1. Opus コーデック トランスコーディングをサポートするサービス統合型ルータ（ISR）ゲートウェイを使用してトランスコーダを設定します。 トランスコーダプロファイルに Opus コーデックを追加する必要があります。
2. Cisco Unified Communications Manager DSPFAR プロファイルに Opus コーデックをサポートするトランスコーダを登録します。
3. トランスコーダを、トランスコーディングを要求するエンドポイントまたはトランクのメディアリソースグループリスト（MRGL）にトランスコーダを関連付け、両通話先間の地域設定を構成します。

（注） トランスコーダで構成される 2 つのコーリングパーティのデバイスプールに関連付ける場合、Unified CM はメディアネゴシエーション用の適切なトランスコーダを呼び出します。 詳細については、「トランスコーダの設定」を参照してください。

MTP 機能を使用したトランスコーダ

コーデック変換に加えて、トランスコーダは、メディアの終了点（MTP）と同じ機能を提供できます。 コーダ機能と MTP 機能が両方とも必要な場合、システムは、両方の機能セットを同時に提供できるため、トランスコーダを割り当てます。 MTP 機能のみが必要な場合は、システムはリソースプールからトランスコーダまたは MTP のいずれかを割り当てます。 リソースの選択は、メディアリソースグループによって決定されます。

[Cisco Unified CM の管理] > **[システム]** > **[サービスパラメータ]** > **[サービスパラメータの設定]** ウィンドで、**[信頼できるリレーポイントの割り当てが失敗した場合のコールの失敗]** フィールドと **[MTPの割り当てが失敗した場合のコールの失敗]** フィールドが [False] に設定されていると、ソフトウェア MTP リソースが必要なときに使用できなくなったとき、コールは MTP リソースと MTP/TRP サービスを使用せずに接続を試みます。 ハードウェア トランスコーダ機能が（あるコーデックを別のコーデックに変換するために）必要であり、トランスコーダが使用できない場合、コールは失敗します。

トランスコーダ タイプ

Cisco Unified Communications Manager の管理ページにおけるトランスコーダ タイプは次の表のとおりです。

（注） トランスコーダは、G.711 とすべてのコーデック（トランスコーダとして機能している G.711 や MTP/TRP 機能を提供している G.711 を含む）の間のトランスコーディングをサポートします。

表 *8:* トランスコーダ タイプ

トランスコーダタイプ	説明
Cisco Media Termination Point Hardware	このタイプは Cisco Catalyst 4000 WS-X4604-GWY および Cisco Catalyst 6000 WS-6608-T1 または WS-6608-E1 をサポートし、次のトランスコーディング セッション数を提供します。 Cisco Catalyst 4000 WS-X4604-GWY の場合 • G.711 へのトランスコーディング：16 の MTP トランスコーディング セッション Cisco Catalyst 6000 WS-6608-T1 または WS-6608-E1 の場合 • G.723 から G.711 へのトランスコーディング/G.729 から G.711 へのトランスコーディング：1 つの物理ポート当たり 24 の MTP トランスコーディング セッション、1 つのモジュール当たり 192 セッション

トランスコーダ タイプ	説明
Cisco IOS Media Termination Point（ハードウェア）	このタイプは Cisco 2600XM、Cisco 2691、Cisco 3725、Cisco 3745、Cisco 3660、Cisco 3640、Cisco 3620、Cisco 2600、および Cisco VG200 ゲートウェイをサポートし、次のトランスコーディング セッション数を提供します。 NM-HDV 単位 • G.711 から G.729-60 へのトランスコーディング • G.711 から GSM FR/GSM EFR へのトランスコーディング：45

トランスコーダタイプ	説明
Cisco IOS Enhanced Media Termination Point（ハードウェア）	

トランスコーダ タイプ	説明
	NM-HD 単位 このタイプは Cisco 2600XM、Cisco 2691、Cisco 3660、Cisco 3725、Cisco 3745、および Cisco 3660 アクセス ルータをサポートし、次のトランスコーディング セッション数を提供します。 • G.711 から G.729a/G.729ab/GSMFR へのトランスコーディング：24 • G.711 から G.729/G.729b/GSM EFR へのトランスコーディング：18 **NM-HDV2 単位** このタイプは Cisco 2600XM、Cisco 2691、Cisco 3725、Cisco 3745、および Cisco 3660 アクセス ルータをサポートし、次のトランスコーディング セッション数を提供します。 • G.711 から G.729a/G.729ab/GSMFR へのトランスコーディング：128 • G.711 から G.729/G.729b/GSM EFR へのトランスコーディング：96 **PVDM4** • 導入準備の PVDM4 モジュール（PVDM4-32、PVDM4-64、PVDM4-128、PVDM4-256） • T1/E1 モジュールの DSP モジュール（PVDM4-32、PVDM4-64、PVDM4-128、PVDM4-256） • DSP NIMs (NIM-PVDM4-32、NIM-PVDM4-64、NIM-PVDM4-128、NIM-PVDM4-256) これらのタイプは、ISR4K（ISR44xx、ISR43xx）、C83xx、および C82xx プラットフォームをサポートし、次のトランスコーディング セッション数を提供します。 • G.711 から G.729a/G.729ab/GSMFR へのトランスコーディング：24 • G.711 から G.729/G.729b/GSM EFR へのトランスコーディング：18 • G.711 から G.729a/G.729ab/GSMFR へのトランスコーディング：128 • G.711 から G.729/G.729b/GSM EFR へのトランスコーディング：96 • G.711/G.729/G.729ab/G.729a/G.729b から Opus へのトランスコー

トランスコーダタイプ	説明
	ディング
Cisco Media Termination Point (WS-SVC-CMM)	このタイプは、装着されているドーター カード当たり 64 のトランスコーディング セッションを提供します。1 枚のドーター カードでは 64 のトランスコーディング セッション、2 枚のドーター カードでは 128 のトランスコーディング セッション、3 枚のドーター カードでは 192 のトランスコーディング セッション、4 枚のドーター カード（最大）では 256 のトランスコーディング セッションを提供します。 このタイプは、次のコーデックの任意の組み合わせの間でトランスコーディングを提供します。 • G.711 a-law および G.711 mu-law • G.729 annex A および annex B • G.723.1 • GSM（FR） • GSM（EFR）

トランスコーダの連携動作と制限事項

トランスコーダの連携動作と制限事項

連携動作または制限事項	説明
トランスコーダの削除	メディア リソース グループに割り当てられているトランスコーダは、削除できません。 トランスコーダを使用しているメディアリソース グループを検索するには、**[トランスコーダの設定（Transcoder Configuration）]** ウィンドウの **[関連リンク（Related Links）]** ドロップダウン リスト ボックスから **[依存関係レコード（Dependency Records）]** を選択し、**[移動（Go）]** をクリックします。 [依存関係レコード要約(Dependency Records Summary)] ウィンドウに、トランスコーダを使用しているメディア リソース グループに関する情報が表示されます。 メディア リソース グループに関するより詳細な情報を見つけるには、メディア リソース グループをクリックして [依存関係レコード詳細(Dependency Records Detail)] ウィンドウを表示します。 システムで依存関係レコードが有効でない場合、[依存関係レコード サマリー（Dependency Records Summary）] ウィンドウにメッセージが表示されます。 使用中のトランスコーダを削除しようとすると、Cisco Unified Communications Manager からメッセージが表示されます。 現在使用されているトランスコーダを削除する前に、割り当てられているメディア リソース グループからトランスコーダを削除する必要があります。

連携動作または制限事項	説明
フェールオーバーとフォールバック	トランスコーダのフェールオーバーとフォールバックは以下のように動作します。 • プライマリUnified Communications Managerノードに障害が発生した場合、トランスコーダは、トランスコーダの所属するデバイスプールに対して指定されたUnified Communications Managerグループ内で、次に使用可能なノードへの登録を試みます。 • プライマリ Cisco Unified Communications Manager が使用可能な状態に戻ると、そのトランスコーダは、ただちにプライマリ Cisco Unified Communications Manager に登録されます。 • トランスコーダデバイスは、到達不能になったUnified Communications Managerノードから登録解除されます。 トランスコーディングにこのトランスコーディングプロファイルを使用していたコールは保存状態に移行し、トランスコーダは次に利用可能なノードに登録します。 ゲートウェイでは、RTP/RTCP タイムアウトを使用して、登録されている Unified Communications Manager のリソースリリースを通知します。 • トランスコーダが新しいUnified Communications Managerノードへの登録を試み、登録確認応答を受信しなかった場合、トランスコーダはリストの次のノードへの登録を行います。 トランスコーダ デバイスは、ハード リセットまたはソフト リセット後に登録を解除し、続いて接続を解除します。 リセットが完了すると、デバイスはプライマリ Cisco Unified Communications Manager ノードに再登録されます。

連携動作または制限事項	説明
Opus コーデック トランスコーダーサポート	トランスコーダプロファイルがUnified Communications Managerで登録されている場合、次のシナリオが発生します。 • ISR ゲートウェイでOpusトランスコーディングがサポートされ、Unified CM が Opus トランスコーディングをサポートしていない場合、コーデックの不一致にトランスコーダが配分されます。ただし、ISR ゲートウェイでは、必要なパラメータがこれらの S つの S 持ち込みメッセージに存在していない場合、OpenReceiveChannel (ORC) メッセージと StartMediaTransmission (SMT) SCCP メッセージが拒否されます。 • ISR ゲートウェイが Opus トランスコーディングをサポートしていない場合に、Unified CM が Opus コーデックトランスコーディングをサポートしている場合、Opus のトランスコーダ割り当て要求は失敗します。 • エンドポイントが、ファイルマルチキャストトランスポートプロトコル（FMTP）の「sprop-stereo」パラメータ値の 1 つが SDP で 1 に設定されている Opus コーデックをサポートしている場合、システムは OLC / SMT を拒否するゲートウェイへの 1 としての値「sprop-stereo」を使用してORC/SMTメッセージを送信します。最終的にコールが切断されます。

トラステッド リレー ポイントの概要

信頼されたリレーポイント (TRP) は、Cisco Unified Communications Manager がメディアストリームに挿入してコールメディアの制御ポイントとして機能するMTPまたはトランスコーダです。TRPは、ストリームに対してさらなる処理を提供し、ストリームが特定のパスに従っていることを確認できます。

コールに信頼されたリレーポイントが必要な場合、Cisco Unified Communications Manager は、TRP 機能で有効になっている MTP またはトランスコーダを割り当てます。

設定

MTP およびトランスコーダは、**[メディアの終了点の設定]** または **[トランザクションの設定]** ウィンドウの **[信頼されたリレーポイント]** チェックボックスをオンにすると、TRP機能を提供するように設定することができます。

個々のコールの TRP 要件を設定するには、次の設定ウィンドウの **[信頼されたリレーポイントを使用する]** フィールドを **[オン]** に設定します。

- 電話機設定
- [ゲートウェイの設定（Gateway Configuration）]

- [ボイスメールポート設定（Voicemail Port Configuration）]
- トランクの設定（Trunk Configuration）
- [CTIルートポイントの設定（CTI Route Point Configuration）]
- 共通デバイス設定
- [ユニバーサルデバイステンプレートの設定（Universal Device Template Configuration）]
- さまざまなメディア リソースの設定（アナンシエータ、IVR、MTP、トランスコーダ、会議ブリッジ、保留音)

トラステッド リレー ポイントの連携動作と制限事項

機能	連携動作と制限事項
Resource Reservation Protocol（RSVP）	コールでRSVPが有効になっている場合、Cisco Unified Communications Managerはまず、TRPのラベルも付いているRSVPAgentを割り当てようとします。 それ以外の場合は、別のTRPデバイスがRSVPAgentとエンドポイントの間に挿入されます。
コールのトランスコーダ	トランスコーダがコールに必要であり、それをTRPを必要とするエンドポイントと同じ側に割り当てる必要がある場合、Cisco Unified Communications Managerはまず、TRPのラベルも付いているトランスコーダを割り当てようとします。 それ以外の場合は、別のTRPデバイスがトランスコーダとエンドポイントの間に挿入されます。
エンドポイントのMTP割り当て	エンドポイント向けに、[メディアの終了点が必須（Media Termination Point Required）]チェックボックスおよび[信頼されたリレーポイントを使用（Use Trusted Relay Point）]チェックボックスをオンにすると、Cisco Unified Communications Managerは、TRPを兼ねるMTPを割り当てます。 管理者がそのようなMTPまたはTRPの割り当てに失敗すると、コールの状態が表示されます。
TRP割り当て	ほとんどの場合、TRPはユーザがコールに応答した後に割り当てられるため、TRPの割り当てに失敗したためにコールが失敗すると、ユーザがコールに応答した後に速いビジー トーンが聞こえる可能性があります （MTPが必要なSIPアウトバウンド レッグ、つまりH.323アウトバウンドFastStartは例外です）。

機能	連携動作と制限事項
エンドポイントのTRP挿入	エンドポイントまたはデバイスに関連付けられているデバイスプールのいずれかで、**[信頼されたリレーポイントを使用（Use Trusted Relay Point）]** チェックボックスをオンにした場合、Cisco Unified Communications Managerはそのエンドポイント向けにTRPを挿入する必要があります。 **[信頼されたリレーポイントの割り当てに失敗した場合コールを失敗させる（Fail Call If Trusted Relay Point Allocation Fails）]** サービスパラメータが、**True** に設定されている場合、 Cisco Unified Communications Managerが TRP の割り当てに失敗すると、コールが失敗することがあります。
TRPとリモートユーザ	TRPは、在宅勤務のリモートユーザに対するセキュアなソリューションの提供には推奨されません。 Expresswayの Mobile and Remote Accessソリューションをお勧めします。

TRP リソースが不足したときのコール動作

このセクションでは、MTP リソースの割り当てが不足したときにCisco Unified Communications Managerがコールを処理する方法の例を示します。最終的なコール動作は、これらのエンドポイントに MTP および TRP が必要かどうか、および MTP または TRPS の割り当てが失敗したときに自動的にコールを終了するようシステムが設定されているかどうかによって異なります。

MTP と TRP の両方が必要な場合

次の表に、エンドポイントで [メディアの終了点が必須（Media Termination Point Required）]と[信頼されたリレーポイントを使用（Use Trusted Relay Point）]の両方のオプションが選択されており、MTP と TRP のリソースが不足した場合に、コールが終了するかどうかを示します。

最終的なコールのステータスは、[信頼されたリレーポイントの割り当てに失敗したらコールを終了（Fail Call If Trusted Relay Point Allocation Fails）]と [MTPの割り当てに失敗したらコールを終了（Fail Call if MTP Allocation Fails）]サービス パラメータが、コールの自動終了に設定されているかどうかによって異なります。

[TRPの割り当てに失敗したらコールを終了（Fail Call If TRP Allocation Fails）] サービスパラメータ	**[MTPの割り当てに失敗したらコールを終了（Fail Call If MTP Allocation Fails）] サービスパラメータ**	**Unified CM がコー**
True	True	可
True	False	可
False	True	はい（MTP が H 合）。 いいえ（ 要な場合）
False	False	不可

MTP/TRP リソースが不足した場合のコールの自動終了が有効化されていない

次の表に、MTP または TRP のリソースが不足しており、[信頼されたリレーポイントの割り当てに失敗したらコールを終了（Fail Call If Trusted Relay Point Allocation Fails）]と [MTPの割り当てに失敗したらコールを終了（Fail Call If MTP Allocation Fails）]のサービス パラメータが [False] に設定されている場合のコール動作を示します。

MTP が必須 = はい（Yes)	TRP を使用 = はい（Yes）	リソース割り当てのステータス	コールの動作
Y	Y	TRP割り当て済み	パススルーのサポートが存在しないため、オーディオ コールのみ。
Y	Y または N	MTP のみ	オーディオ コールのみ。 TRP のサポートは存在しません。
Y	Y または N	割り当てなし	H.323 エンドポイントで [メディアの終了点が必須（Media Termination Point Required）] チェックボックスがオンになっている場合、補足サービスは無効になります。
N	Y	TRP割り当て済み	エンドポイントの機能に応じてオーディオまたはビデオ通話、およびコール アドミッション制御（CAC）。 補足サービスは引き続き機能します。
N	Y	割り当てなし	音声またはビデオ通話。 補足サービスは引き続き機能しますが、TRP のサポートは存在しません。

アナンシエータの概要

アナンシエータは、Cisco Unified Communications Manager で動作し、録音されたメッセージやトーンを Cisco IP 電話およびゲートウェイに送信することが可能な、SCCP ソフトウェアデバイスです。 そのノード上で Cisco IP Voice Media Streaming service をオンにすると、アナンシエータがクラスタノード上でアクティブ化されます。 MLPP、SIP トランク、IOS ゲートウェイ、ソフトウェア会議ブリッジなどの機能は、定義済みのメッセージを一方向のメディアストリーム経由で電話機またはゲートウェイに送信するように、アナンシエータに依存しています。 さらに、

- IPv4 と IPV6 の両方がサポートされています。 アナンシエータは、システムのプラットフォームが IPv6 に対して設定されており、IPv6 エンタープライズパラメータが有効化されている場合、自動的にデュアルモードに設定されます。
- SRTP がサポートされています

アナンシエータのスケーラビリティ

デフォルトでは、アナンシエータは 48 のメディアストリームを同時にサポートしています。追加ノードでアナンシエータをアクティブにするか、[コール数（Call Count）]サービス パラメータを使用してアナンシエータのメディア ストリームのデフォルト数を変更することで、キャパシティを増やすことができます。 ただし、当該のノードで **Cisco CallManager** サービスが非アクティブ化されていない限り、ノードでこの値を増やすことは推奨しません。

Cisco CallManager サービスが実行されていない専用のサブスクライバ ノードでアナンシエータを実行する場合、アナンシエータは最大255の同時アナウンス ストリームをサポートできます。 専用のサブスクライバーノードが 1 万ユーザの OVA バーチャルマシン設定に適合する場合、警報装置は最大 400 の同時アナウンスストリームをサポートできます。

⚠

注意 コール処理の負荷が高いUnified Communications Managerノードではアナンシエータをアクティブにしないでください。

会議ブリッジを使用したアナンシエータ

このアナンシエータは、次の条件の下で会議ブリッジに使用できます。

- アナンシエータを含むメディア リソース グループ リストが、会議ブリッジが存在するデバイス プールに割り当てられている場合。
- アナンシエータがデフォルトのメディア リソースとして設定されている場合。

メディア リソース グループ リストが会議を制御するデバイスに直接割り当てられている場合は、会議ブリッジでアナンシエータを使用できません。

会議ごとにアナウンスを1つだけサポートします。 現在のアナウンスの再生中に、システムが別のアナウンスを要求した場合は、新しいアナウンスによって再生中のアナウンスがプリエンプション処理されます。

デフォルトの警報装置アナウンスとトーン

Cisco Unified Communications Manager では Cisco IP Media Streaming Application サービスが有効になると、録音されたアナンシエータアナウンスを自動的に提供します。 アナウンスまたはトーンは、次の条件で再生されます。

- アナウンス：Cisco Multilevel Precedence and Preemption 用に設定されたデバイス向けに再生されます
- 割り込み音：参加者がアドホック会議に参加する前に聞こえます
- リングバックトーン:IOSゲートウェイを介してPSTN経由でコールを転送する場合、コールがアクティブになっていてもゲートウェイが音を再生できないため、アナンシエータがトーンを再生します。
- リングバックトーン：H.323 クラスタ間トランクを介してコールを転送するときに、トーンを再生します。

- リングバック トーン：SCCP を実行している電話機から SIP クライアントにコールを転送するとき、トーンを再生します。

デフォルトの録音されたアナンシエータアナウンスを変更したり、アナウンスを追加することはできません。 Cisco Unified Communications Manager Locale Installer がインストール済みで Cisco Unified IP Phone またはデバイス プールのロケール値を設定した場合には、アナウンスのローカリゼーションがサポートされます。ロケールインストーラとユーザおよび（対応する）ネットワーク ロケール用にインストールするファイルの詳細については、『*Installing Cisco Unified Communications Manager*（*Cisco Unified Communications Manager* のインストール）』を参照してください。ロケールインストーラをダウンロードするには、www.cisco.com のサポート ページを参照してください。

表 *9*：録音済みのアナンシエータアナウンス

条件	アナウンス
同等またはそれ以上の優先コールが進行中です。	緊急度の高い電話が使用中のため、電話をおつなぎできません。 一度電話をお切りになってから、もう一度おかけ直しください。 これは録音メッセージです。
優先順位のアクセス制限が存在します。	緊急度の高い電話が使用中のため、電話をおつなぎできません。 一度電話をお切りになってから、もう一度おかけ直しください。 これは録音メッセージです。
許可されない優先順位の使用を試みた人物がいます。	ご使用になった優先度は、回線で認証されていません。認証された優先度をお使いになるか、交換手までお問い合わせください。 これは録音メッセージです。
コールがビジー状態です。または管理者がコール待機用または優先処理用のディレクトリ番号を設定していません。	おかけになった番号は、大変込み合っており、この番号には割り込み機能が備わっておりません。 一度電話をお切りになってから、もう一度おかけ直しください。 これは録音メッセージです。
システムがコールを確立できません。	おかけになった電話番号では、正しくおつなぎできません。番号を確認してからもう一度おかけ直しいただくか、交換手までお問い合わせください。 これは録音メッセージです。
サービスが中断されました。	サービス障害のため、電話をおつなぎできません。 緊急の場合は、交換手までお電話ください。 これは録音メッセージです。

次の表に、警報機でサポートされているトーンを示します。

表 *10 :* トーンの説明

タイプ（Type）	説明
話中音	ダイヤルされた番号が使用中の場合は、ビジートーンが聞こえます。
割り込みトーン	参加者がアドホック会議に参加する前に会議割り込みトーンが聞こえます。
リングバックトーン	次のシナリオでは、アラートトーンが聞こえます。 • IOS ゲートウェイを使用して PSTN 経由でコールを転送するとき • H.323 クラスタ間トランクを介してコールを転送するとき • SCCP 電話機から SIP クライアントにコールを転送するとき

自動音声応答の概要

Interactive Voice Response（IVR）デバイスを使用すると、Cisco Unified Communications Managerは、録音済みの機能アナウンス（.wavファイル）をCisco Unified IP Phoneやゲートウェイなどのデバイスに再生できます。 これらのアナウンスは、[今すぐ会議(Conference Now)] のようなIVR アナウンスが必要な機能を使用するデバイスで再生されます。

ノードを追加すると、IVRデバイスがそのノードに自動的に追加されます。IVRデバイスは、Cisco IP Voice Media Streaming Application サービスがそのノード上で有効化されるまで、非アクティブなままです。

IVR はデフォルトで 48 人の同時発信者をサポートします。 Cisco IP Voice Media Streaming Application サービス パラメータを使用して、IVR 発信者の数を変更できます。 ただし、ノード上で 48 の IVR 発信者を超えないようにすることをお勧めします。 [今すぐ会議(Conference Now)]への参加に必要な IVR への同時コールに基づいて、IVR の発信者数を設定できます。

⚠

注意 コール処理負荷の高い Cisco Unified Communications Manager ノードでは IVR デバイスを有効化しないでください。

デフォルトの IVR アナウンスとトーン

Cisco Unified Communications Manager では Cisco IP Media ストリーミングアプリケーションサービスが有効になると、録音された一連の自動音声応答（IVR）アナウンスを自動的に提供します。 デフォルトの録音済みの IVR アナウンスを置き換えることができます。 アナウンスは、次の条件で再生されます。

表 *11* : 録音済みの *IVR* アナウンス

アナウンス	条件
ConferenceNowAccessCodeFailed アナウンス	出席者が誤ったアクセスコードを入力し最大試行回数を超えた場合に再生されます。
ConferenceNowAccessCodeInvalid アナウンス	出席者が誤ったアクセスコードを入力したときに再生されます。
ConferenceNowCFBFailed アナウンス	会議の開始中に会議ブリッジのキャパシティ制限を超える場合に再生されます。
ConferenceNowEnterAccessCode アナウンス	出席者が会議に参加しホストが出席者のアクセスコードを設定するときに再生されます。
ConferenceNowEnterPIN アナウンス	主催者または出席者がミーティングに参加しようとするときに再生されます。
ConferenceNowFailedPIN アナウンス	ホストが、正しい PIN を入力するための最大試行回数を超えた後に再生されます。
ConferenceNowGreeting アナウンス	今すぐ会議用のグリーティングプロンプトを再生します。
ConferenceNowInvalidPIN アナウンス	ホストが間違った PIN を入力したときに再生されます。
ConferenceNowNumberFailed アナウンス	ホストまたは出席者が誤ったアクセスコードを入力し最大試行回数を超えた場合に再生されます。
ConferenceNowNumberInvalid アナウンス	ホストまたは出席者が間違ったミーティング番号を入力したときに再生されます。

自動音声応答制限

機能	制約事項
ロード バランシング	自動音声応答 (IVR) は、共通のメディアデバイスドライバー経由でリアルタイムプロトコル (RTP) ストリームを使用します。 このデバイスドライバは、保留音（MOH）ソフトウェアメディアターミネーション ポイント（MTP）、ソフトウェア会議ブリッジ（CFB）、アナンシエータなどの Cisco IP Voice Media ストリーミング アプリケーションサービスが提供するその他のソフトウェアメディアデバイスによっても利用されます。 大きなコールボリュームを設定すると、システムのパフォーマンスに影響します。 これは、同じサーバノード上で CallManager サービスがアクティブになっている場合のコール処理にも影響します。
DTMF ディジット	IVR は、帯域外 (OOB) の DTMF ディジットコレクション方式のみをサポートしています。 通話デバイスと IVR の間に DTMF 機能の不一致がある場合、MTP が割り当てられます。
コーデック	IVR がサポートしているのは、G.711 (つまり、a-law と mu-law)、G.729、ワイド帯域 256 mb のみです。 発信側デバイスと IVR の間でコーデックが一致していない場合、トランスコーダが割り当てられます。

アナウンスの概要

Cisco Unified Communications Manager Administration で、メニュー パス **[メニューリソース]** > **[アナウンス（Announcements）]** を使用して、アナウンスを設定します。 アナウンスには次の 2 つの分類があります。

- [システム アナウンス（System Announcements）]：通常のコール処理で使用されるか、機能アナウンスのサンプルとして提供される、事前定義されたアナウンス。
- [機能アナウンス（Feature Announcements）]：保留音（MOH）、コール キューイングまたは外部コール制御を伴うハント パイロットなどの特定の機能で使用されます。 シスコが提供するオーディオ ファイルをアップロードするか、またはカスタムの `.wav` ファイルをアップロードすることで、機能アナウンスをカスタマイズできます。 すべてのカスタム アナウンスの `.wav` ファイルを、クラスタ内のすべてのサーバにアップロードします。

（注） トランクまたはゲートウェイ経由で接続している場合は、警告やリオーダー音などのカスタム アナウンスが再生されることがあります。 ただし、2 台の IP 電話間、または IP 電話と Jabber クライアントの間のコールでは、カスタム アナウンスは再生されません。

形式

アナウンスに推奨される形式には次の仕様が含まれます。

- 16 ビット パルス符号変調（PCM）wav ファイル
- ステレオまたはモノラル
- 48 kHz、44.1 kHz、32 kHz、16 kHz、または 8 kHz のサンプル レート

デフォルトのアナウンス

カスタムアナウンスwavファイルをアップロード、またはシステムアナウンス用にシスコが提供したファイルを変更することは可能です。ただし、アナウンス識別子を変更することはできません。たとえば、発信者が無効な番号をダイヤルすると、システムアナウンス（VCA_00121）が再生されます。 これは一般に「空席コールのアナウンス」として知られています。

表 *12 : [アナウンスの検索と一覧表示(Find and List Announcements)]* ウィンドウのアナウンス

[アナウンスID(Announcement Identifier)]	説明
Gone_00126	システム：現在使用されていない
MLPP-BNEA_00123	システム：MLPP ビジーが備わっていない
MLPP-BPA_00122	システム：MLPP 以上の優先レベル
MLPP-ICA_00120	システム：MLPP サービス障害
MLPP-PALA_00119	システム：MLPP 優先順位のアクセス制限
MLPP-UPA_00124	システム： MLPP で許可されていない優先レベル
Mobility_VMA	接続するには 1 を押してください
MonitoringWarning_00055	システム：モニタリングまたは録音中
RecordingWarning_00038	システム：録音中
TemporaryUnavailable_00125	システム：一時的に利用不可
VCA_00121	システム：欠番/無効な番号がダイヤルされた
Wait_In_Queue_Sample	ビルトイン：キューに入った発信者用の定期的な
Welcome_Greeting_Sample	ビルトイン：発信者へのグリーティング（サンプ

メディア リソースの設定タスク フロー

システムのメディア リソースを設定するには、この手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	ソフトウェア メディア リソースのアクティブ化 （163 ページ）	IPVMS サービスを有効化すると、サーバ上のソフトウェア メディア リソースがアクティブ化されます。
ステップ 2	メディア ターミネーション ポイントの設定 （163 ページ）	システムのメディア ターミネーション ポイント（MTP）を設定します。
ステップ 3	トランスコーダの設定 （164 ページ）	システムにトランスコーダ リソースを追加します。
ステップ 4	自動音声応答（IVR）の設定 （164 ページ）	システムの IVR のデフォルト設定を指定します。
ステップ 5	アナンシエータの設定 （165 ページ）	アナンシエータのシステム設定を指定します。
ステップ 6	メディア リソース グループの設定 （165 ページ）	メディア リソースをメディア リソース グループに追加します。 異なるリソースの組み合わせで複数のグループを設定します。
ステップ 7	メディア リソース グループ リストの設定 （166 ページ）	エンドポイントまたはエンドポイントのクラスに割り当てることができるメディア リソース グループのリストを作成します。
ステップ 8	デバイスまたはデバイス プールへのメディア リソースの割り当て （167 ページ）	メディア リソースをデバイスまたはデバイス プールに割り当てることで、エンドポイントがメディア リソースを使用できるようにします。
ステップ 9	アナウンスの設定 （167 ページ）	（オプション）特定のアナウンスの設定を指定します。 アナウンスは、通常の処理で使用されるほか、保留音または IVR などの機能で使用されます。
ステップ 10	カスタマイズされたアナウンスのアップロード （168 ページ）	（オプション）録音済みのアナウンスをアップロードします。 新規または既存のアナウンスにファイルを割り当てます。

ソフトウェア メディア リソースのアクティブ化

次のソフトウェア メディア リソースを有効にするには、**Cisco IP Voice Media Streaming** サービスをアクティブ化します。

- アナンシエータ
- 音声自動応答（IVR）（Interactive Voice Response (IVR)）
- メディア ターミネーション ポイント（MTP）
- ソフトウェア会議ブリッジ
- 保留音

手順

ステップ 1 Cisco Unified Serviceability から、**[ツール（Tools）] > [サービスの有効化（Service Activation）]** を選択します。

ステップ 2 [サーバ（Server）]から、Unified Communications Manager パブリッシャ ノードを選択します。

ステップ 3 [Cisco IP Voice Media Streaming Service]をオンにして [保存（Save）]をクリックします。

メディア ターミネーション ポイントの設定

ソフトウェアメディアポイント (MTP) を設定するには、次の手順を実行します。

始める前に

ソフトウェアのメディアの終了点（MTP）をアクティブにするには、Cisco IP Voice Media サービスが実行されている必要があります。

必要なMTPリソース数と、これらのリソースの提供に必要なMTPデバイス数を決定します。

手順

ステップ 1 Cisco Unified CM Administration から、**[メディアリソース（Media Resources）] > [メディアの終了点（Media Termination Point）]** を選択します。

ステップ 2 次のいずれかを実行します。

- **[検索（Find）]** をクリックし、既存の MTP を選択します。
- **[新規追加（Add New）]** をクリックし、新規 MTP を作成します。

ステップ 3 **[メディア ターミネーション ポイント名（Media Termination Point Name）]**を割り当てます。

ステップ 4 **デバイスプール**を割り当てます。

ステップ 5 このMTPを**トラステッドリレーポイント (TRP)**として指定する場合は、[トラステッドリレーポイント] チェックボックスをオンにします。

ステップ 6 **[保存]** をクリックします。

トランスコーダの設定

トランスコーダは、あるコーデックからの入力ストリームを、別のコーデックを使用し出力ストリームに変換するデバイスです。

始める前に

IVR がアクティブになるためには、Cisco IP Voice Media Streaming サービスが実行されている必要があります。

必要なトランスコーダ リソースの数とリソースの提供に必要なトランスコーダ デバイスの数を決定します。

手順

ステップ 1 Cisco Unified CM Administration にログインし、**[メディア リソース（Media Resources）] > [トランスコーダ（Transcoder）]**.を選択します。

ステップ 2 次のいずれかを実行します。

- 既存のトランスコーダを選択するには、[検索（Find）]をクリックします。
- [新規追加] をクリックします。

ステップ 3 [トランスコーダタイプ（Transcoder Type）]を選択します。

ステップ 4 トランスコーダの [MACアドレス（MAC Address）]を入力します。

ステップ 5 ドロップダウン メニューから [デバイスプール（Device Pool）]を割り当てます。

ステップ 6 このトランスコーダをトラステッド リレー ポイントとして使用する場合は、[トラステッドリレーポイント（Trusted Relay Point）]チェックボックスをオンにします。

ステップ 7 **[保存]** をクリックします。

自動音声応答（IVR）の設定

IVR の設定項目を指定するには、この手順を使用します。

始める前に

自動音声応答（IVR）がアクティブになるためには、Cisco IP Voice Media Streaming サービスが実行されている必要があります。

手順

ステップ 1 Cisco Unified CM Administration で、**[メディアリソース（Media Resources）] > [自動音声応答（Interactive Voice Response）]** を選択します。

ステップ 2 [検索（Find）]をクリックして、IVR を選択します。

ステップ 3 [Name]と [Description]を入力します。

ステップ 4 IVR コールでトラステッド リレー ポイントを使用する場合は、[信頼されたリレーポイントを使用（Use Trusted Relay Point）]ドロップダウンを [オン（On）]に設定します。

ステップ 5 [自動音声応答の設定（Interactive Voice Response Configuration）]ウィンドウで、残りのフィールドを入力します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 6 **[保存]** をクリックします。

アナンシエータの設定

アナンシエータのシステム設定を指定します。

始める前に

アナンシエータがアクティブになるためには、Cisco IP Voice Media Streaming サービスが実行されている必要があります。

手順

ステップ 1 Cisco Unified CM Administration で **[メディア リソース（Media Resources）] > [アナンシエータ（Annunciator）]** を選択します。

ステップ 2 [検索（Find）]をクリックして、アナンシエータを選択します。

ステップ 3 [Name]と [Description]を入力します。

ステップ 4 [デバイスプール（Device Pool）]を選択します。

ステップ 5 アナンシエータでトラステッド リレー ポイントを使用する場合は、[トラステッドリレーポイントを使用（Use Trusted Relay Point）]ドロップダウンを [オン（On）]に設定します。

ステップ 6 **[保存]** をクリックします。

メディア リソース グループの設定

メディアリソースグループには、エンドポイントまたはエンドポイントのグループに割り当てるメディアリソースの一覧が含まれています。

手順

ステップ 1 Cisco Unified CM Administration で、**[メディアリソース（Media Resources）]** > **[メディアリソースグループ（Media Resource Group）]** を選択します。

ステップ 2 次のいずれかを実行します。

- 既存のメディア リソース グループを選択するには、[検索（Find）]をクリックします。
- 新しいメディア リソース グループを作成するには、[新規追加（Add New）]をクリックします。

ステップ 3 [メディア リソース グループの設定（Media Resource Group Configuration）]ウィンドウで各フィールドを設定します。 フィールドとその設定オプションの詳細については、オンラインヘルプを参照してください。

ステップ 4 グループの [名前（Name）]と [説明（Description）]を入力します。

ステップ 5 [使用可能なメディアリソース（Available Media Resources）]から、このグループに追加するリソースを選択し、矢印を使用してリソースを [選択されたメディアリソース（Selected Media Resources）]に移動します。

ステップ 6 （任意）保留音オーディオにマルチキャストを使用するには、[MOHオーディオにマルチキャストを使用（Use Multi-cast for MOH Audio）]チェックボックスをオンにします。

ステップ 7 **[保存]** をクリックします。

メディア リソース グループ リストの設定

メディアリソースグループの優先順位付けされたリストの作成このリストは、個々のデバイスまたはデバイスプールに割り当てることができます。

手順

ステップ 1 Cisco Unified CM Administration で **[メディア リソース（Media Resources）]** > **[メディア リソースのグループ リスト（Media Resource Group List）]** を選択します。

ステップ 2 次のいずれかを実行します。

- 既存のリストを選択するには、[検索（Find）]をクリックします。
- 新しいリストを作成するには、[新規追加（Add New）]をクリックします。

ステップ 3 メディア リソース グループ リストの [名前（Name）]を入力します。

ステップ 4 [使用可能なメディアリソースグループ（Available Media Resource Groups）]から、追加するグループを選択し、矢印を使用して [選択されたメディアリソースグループ（Selected Media Resource Groups）]に移動させます。

ステップ 5 **[保存]** をクリックします。

（注） エンドポイントでこれらのメディアリソースを使用するには、デバイスプール、ゲートウェイポート、またはデバイスにリストを割り当てる必要があります。

デバイスまたはデバイス プールへのメディア リソースの割り当て

優先順位付きのメディア リソース グループのリストをデバイス プールまたは個別のデバイスに関連付けることで、エンドポイントにメディア リソースを割り当てます。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [電話（Phone）]** の順に選択します。

- デバイス プールにメディア リソースを追加するには、**[システム（System）] > [デバイス プール（Device Pools）]** を選択します。
- エンドポイントにメディア リソースを直接追加するには、**[デバイス（Device）] > [電話（Phone）]** を選択します。

ステップ 2 [検索（Find）]をクリックして、これらのメディアリソースを割り当てるデバイス プールまたはデバイスを選択します。

ステップ 3 **[メディアリソースグループリスト（Media Resource Group List）]**ドロップダウン リストから、リストを選択します。

ステップ 4 **[保存]** をクリックします。

ステップ 5 [選択項目への設定の適用（Apply Config to Selected）]をクリックします。
デバイス名および適切な設定変更を示した [設定の適用（Apply Configuration）]ウィンドウが表示されます。

アナウンスの設定

システムアナウンスまたは機能アナウンスとして使用できるアナウンスを設定することができます。システムアナウンスは、コール処理またはサンプル機能アナウンスを使用するために使用されますが、機能アナウンスは、ハントパイロットのコールキューまたは外部コール制御と関連付けられた特定の機能 (MOH) などに使用されます。

既存のアナウンスを変更したり、Cisco Unified Communications Manager で新しいアナウンスを設定したりすることができます。

手順

ステップ 1 Cisco Unified CM Administration から、**[メディアリソース（Media Resources）]** > **[アナウンス（Announcement）]** を選択します。

ステップ 2 次のいずれかを実行します。

- **[検索**（Find）] をクリックして、編集する既存のアナウンスを選択します。
- **[新規追加（Add New）]** をクリックして新しいアナウンスを追加します。

ステップ 3 **[アナウンスの設定]** ウィンドウのフィールドを設定します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 4 **[保存]** をクリックします。

カスタマイズされたアナウンスのアップロード

別のアナウンスを使用して、アップロードしたカスタム .wav ファイルを伴うデフォルトのアナウンスを変更することができます。 音声ソースファイルをインポートすると、Unified Communications Manager がファイルを処理し、保留音(MOH)サーバでの使用に適した形式にファイルを変換します。

（注） アナウンスはロケール（言語）で特定されます。インストールに複数の言語ロケールが使用されている場合、各カスタムアナウンスは各言語で別個の .wav ファイルとして録音し、正しいロケール指定でアップロードする必要があります。 また、米国英語以外の言語のカスタム アナウンス .wav ファイルをアップロードする前に、正しいロケール パッケージを各サーバにインストールする必要もあります。

MoH オーディオ ソースなど、アナウンスに推奨される形式には次の仕様が含まれます。

- 16 ビット PCM .wav ファイル
- ステレオまたはモノラル
- 48 kHz、44.1 kHz、32 kHz、16 kHz、または 8 kHz のサンプル レート

Unified Communications Manager の [アナウンスの検索と一覧表示（Find and List Announcements）] ウィンドウで、ハイパーリンクが設定されていないアナウンスは更新できません。 このウィンドウでハイパーリンクされた下線付きのシスコ提供のアナウンスの場合は、カスタマイズされたアナウンスを追加できます。 たとえば、MLPP-ICA_00120 と MonitoringWarning_00055 があります。

手順

ステップ 1 Cisco Unified CM Administration から、**[メディア リソース（Media Resources）] > [アナウンス（Announcement）]** を選択します。

ステップ 2 [アナウンスの検索と一覧表示（Find and List Announcements）] ウィンドウで、検索条件を入力して、[検索（Find）] をクリックし、結果リストからアナウンスのハイパーリンクをクリックします。

ステップ 3 **[アナウンスの設定（Announcement Configuration）]** ウィンドウで、**[ファイルのアップロード（Upload File）]** をクリックします。

ステップ 4 [ファイルのアップロード（Upload Files）] ポップアップ ウィンドウから、ロケールを選択し、ファイル名を入力して参照し、.wav ファイルを選択して、[ファイルのアップロード（Upload File）] をクリックします。

アップロード プロセスが始まり、処理が完了した後にステータスが更新されます。 [閉じる（Close）]を選択して [ファイルのアップロード（Upload File）] ウィンドウを閉じます。

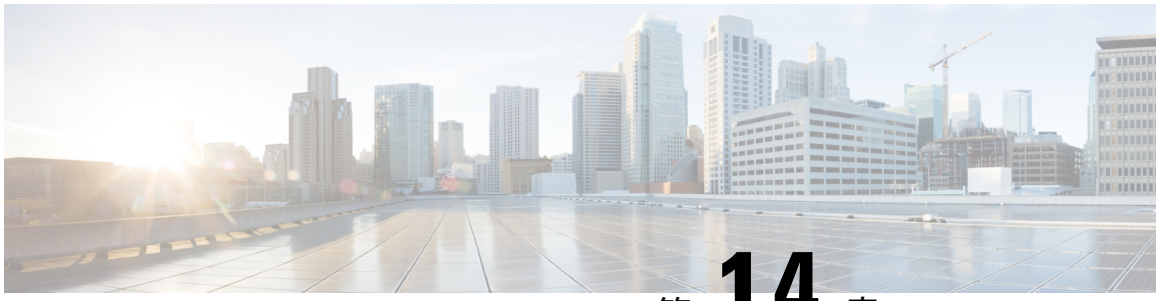
ステップ 5 （任意）Unified Communications Manager でシスコが提供するアナウンスを再生する代わりに、カスタマイズしたアナウンスを再生する場合は、**[アナウンスの設定（Announcements Configuration）]** ウィンドウの **[ロケール別のアナウンス（Announcement by Locale）]** ペインで **[有効（Enable）]** チェックボックスをオンにします。

[有効（Enable）]チェックボックスがオフになっている場合、Unified Communications Manager は、シスコが提供するアナウンスを再生します。

ステップ 6 **[保存]** をクリックします。

次のタスク

クラスタ内のサーバ間ではアナウンス ファイルが伝搬されないため、クラスタ内の各ノードにアナウンスをアップロードします。 クラスタ内の各サーバで Cisco Unified Communications Manager の管理を参照し、アップロード プロセスを繰り返します。



第 14 章

会議ブリッジの設定

会議ブリッジの概要

Cisco Unified Communications Manager の会議ブリッジは、ソフトウェアまたはハードウェアアプリケーションで、アドホックおよびミートミーの両方式の音声会議を可能にするように設計されています。 追加の会議ブリッジタイプは、ビデオ会議など、その他の会議タイプをサポートします。 どの方式の会議ブリッジも、複数の参加者による複数の会議を同時にサポートしています。 ハードウェア会議とソフトウェア会議の両方の会議ブリッジを同時にアクティブにすることができます。 ソフトウェアの会議デバイスとハードウェアの会議ブリッジでは、サポートするストリームの数とコーデックのタイプについて違いがあります。 新しいサーバを追加すると、システムによってソフトウェア会議ブリッジが自動的に追加されます。

（注） Cisco Unified Communications Managerサーバが作成されると、ソフトウェア会議ブリッジも自動的に作成され、削除できません。 Cisco Unified Communications Manager Administration に会議ブリッジソフトウェアを追加することはできません。

会議ブリッジ タイプ

Cisco Unified Communications Manager の管理ページには、次の会議ブリッジタイプが存在します。

表 *13 :* 会議ブリッジ タイプ

会議ブリッジ タイプ	説明
シスコ会議ブリッジのハードウェア	このタイプは Cisco Catalyst 4000 および 6000 音声ゲートウェイ モジュールをサポートし、次の会議セッション数をサポートします。 **Cisco Catalyst 6000** • G.711 または G.729a 会議：1 ポート当たりの参加者数 32 人、1 会議当たりの最大参加者数 6 人、1 モジュール当たりの合計参加者数 256 人、参加者数 3 人でのブリッジの数は 10。 • GSM：1 ポート当たりの参加者数 24 人、1 会議当たりの最大参加者数 6 人、1 モジュール当たりの合計参加者数 192 人。 **Cisco Catalyst 4000** G.711 会議のみ：会議参加者数 24 人。各会議の参加者が 6 人の場合、会議の最大数は 4。
Cisco Conference Bridge Software	ソフトウェア会議デバイスは、デフォルトで G.711 コーデックをサポートします。 このタイプの発信者の最大数は 256 です。256 の設定では、ソフトウェア会議ブリッジがそれぞれ 4 当事者の 64 の会議セッションをサポートできます。 会議セッションでの発信者の最大数は、**最大アドホック会議**と**最大 MeetMe 会議のユニキャスト**サービスパラメータによって指定されます。 **注意** このタイプの会議ブリッジ(SW カンファレンスブリッジ)は簡単に実装できます。 参加者の数が多い場合は、単純な合計アルゴリズムを使用している当事者を識別できないので、会議の音声品質が低下する可能性があります。
Cisco IOS Conference Bridge	• NM-HDV または NM-HDV-FARM ネットワーク モジュールを使用。 • G.711 a/mu-law、G.729、G.729a、G.729b、および G.729ab の参加者が 1 つの会議に参加可能です。 • 最大 6 人の参加者が 1 つの会議コールに参加可能です。 Cisco Unified Communications Manager は、会議リソースをコールに動的に割り当てます。 Cisco IOS Conferencing and Transcoding for Voice Gateway Router の詳細については、この製品に付属の Cisco IOS のドキュメントを参照してください。

会議ブリッジ タイプ	説明
Cisco IOS 強化ブリッジ	• Cisco 2800 シリーズおよび 3800 シリーズの音声ゲートウェイ ルータ上でオンボードの Cisco Packet Voice/Fax Digital Signal Processor Modules（PVDM2）を使用、あるいは NM-HD ネットワーク モジュールまたは NM-HDV2 ネットワーク モジュールを使用。 • G.711 a-law/mu-law、G.729、G.729a、G.729b、G.729ab、GSM FR、および GSM EFR の参加者が 1 つの会議に参加可能です。 • 最大 8 人の参加者が 1 つのコールに参加可能です。 （注） ISR4000 ルータおよび SM-X-PVDM-3000/SM-X-PVDM-2000/SM-X-PVDM-1000/SM-X-PVD では、Unified Communications Manager の最大ストリームは 4096 に制 れているため、各会議ブリッジ プロファイルで最大 512 のセッショ 登録できます。 Cisco Unified Communications Manager は、会議リソースをコールに動的に割り当てます。 Cisco IOS Enhanced Conferencing and Transcoding for Voice Gateway Router の詳細については、この製品に付属の Cisco IOS のドキュメントを参照してください。 この会議ブリッジタイプでは、ISR 4000 シリーズゲートウェイが展開されている場合に、サポートされている SIP 電話の AES_CM_128_HMAC_SHA1_80 での SRTP メディア暗号化をサポートしています。 SCCP 電話とサポートされていない SIP 電話は、AES_CM_128_HMAC_SHA1_32 暗号化にフォールバックします。 （注） ゲートウェイのロードが暗号化をサポートしていることを確認してください。 サポートの詳細については、ゲートウェイのドキュメントを参照してください。
Cisco Conference Bridge（WS-SVC-CMM）	この会議ブリッジ タイプは、Cisco Catalyst 6500 シリーズおよび Cisco 7600 シリーズの Communication Media Module（CMM）をサポートします。 これは、会議ごとに最大 8 人の参加者、ポート アダプタごとに最大 64 の会議をサポートします。 この会議ブリッジタイプでは、次のコーデックをサポートしています。この会議ブリッジタイプでは、アドホック会議をサポートしています。 • G.711 a-law/mu-law • G.729 annex A および annex B • G.723.1

会議ブリッジ タイプ	説明
Cisco Video Conference Bridge（IPVC-35xx）	Cisco Video Conference Bridge は、Cisco IP Video Phone、H.323 エンドポイント、および音声専用の Cisco Unified IP Phone にオーディオおよびビデオによる会議機能を提供します。Cisco Video Conference Bridge はビデオの H.261、H.263、および H.264 コーデックに対応しています。
Cisco IOS Heterogeneous Video Conference Bridge	第 2 世代シスコ サービス統合型ルータ（ISR G2）は、アドホック ビデオ会議とミートミー ビデオ会議をサポートする IOS ベースの会議ブリッジとして動作できます。 ルータを会議ブリッジとして機能させるには、DSP モジュールをルータに取り付ける必要があります。 異種間ビデオ会議では、すべての会議参加者が、異なるビデオフォーマット属性を使用する電話機を使用して、会議ブリッジに接続します。 異種間会議では、さまざまなフォーマット間で信号を変換するために DSP のトランスコーディング機能およびトランスサイジング機能が必要です。 異種間ビデオ会議の場合、発信側は、次のいずれかの状況の場合に、オーディオ参加者として会議に接続します。 • DSP リソースが十分でない。 • ビデオ電話機の機能をサポートするように会議ブリッジが設定されていない。 ISR G2 ルータでのビデオ会議の詳細については、ドキュメント『*Configuring Video Conferences and Video Transcoding*（ビデオ会議とビデオ トランスコーディングの設定）』を参照してください。
Cisco Guaranteed Audio Video Conference Bridge	第 2 世代シスコ サービス統合型ルータ（ISR G2）は、アドホックとミートミーの音声会議およびビデオ会議をサポートする IOS ベースの会議ブリッジとして動作できます。 ルータを会議ブリッジとして機能させるには、DSP モジュールをルータに取り付ける必要があります。 会議のオーディオ部分向けに DSP リソースが留保されますが、ビデオサービスは保証されません。 テレビ電話の発信側は、会議の開始時点で DSP リソースが使用可能であれば、ビデオ サービスを利用できます。 使用可能でない場合、発信側はオーディオ参加者として会議に接続します。 ISR G2 ルータでのビデオ会議の詳細については、ドキュメント『*Configuring Video Conferences and Video Transcoding*（ビデオ会議とビデオ トランスコーディングの設定）』を参照してください。

会議ブリッジ タイプ	説明
Cisco IOS 同種間ビデオ会議ブリッジ（Cisco IOS Homogeneous Video Conference Bridge）	第 2 世代シスコ サービス統合型ルータ（ISR G2）は、アドホック ビデオ会議とミートミー ビデオ会議をサポートする IOS ベースの会議ブリッジとして動作できます。 ルータを会議ブリッジとして機能させるには、DSP モジュールをルータに取り付ける必要があります。 Cisco IOS Homogeneous Video Conference Bridge は、同種間ビデオ会議をサポートする IOS ベースの会議ブリッジ タイプを指定します。 同種間ビデオ会議は、すべての参加者が同じビデオ フォーマット属性を使用して接続するビデオ会議です。 すべてのテレビ電話が同じビデオフォーマットをサポートし、会議ブリッジは同じデータ ストリーム フォーマットをすべてのビデオ参加者に送信します。 会議ブリッジが電話機のビデオ フォーマットをサポートするように設定されていない場合、その電話機の発信側は、オーディオのみの参加者として会議に接続します。 ISR G2 ルータでのビデオ会議の詳細については、ドキュメント『*Configuring Video Conferences and Video Transcoding*（ビデオ会議とビデオ トランスコーディングの設定）』を参照してください。

会議ブリッジ タイプ	説明
Cisco TelePresence MCU	Cisco TelePresence MCU は、Cisco Unified Communications Manager 用のハードウェア会議ブリッジのセットです。 Cisco TelePresence MCU は、高解像度（HD）のマルチポイント ビデオ会議ブリッジです。 毎秒 30 フレームで最大 1080p の性能を持ち、あらゆる会議で十分な連続表示を実現し、フルトランスコーディング機能を備えているため、マルチベンダーの HD エンドポイント環境に最適です。 Cisco TelePresence MCU では、シグナリング コール制御プロトコルとして SIP をサポートしています。 詳細に設定でき、システムおよび会議を制御およびモニタする、ビルトイン Web サーバを装備しています。 Cisco TelePresence MCU には、HTTP 通信による XML 管理 API が用意されています。 Cisco TelePresence MCU を使用すると、アドホックとミートミーの両方の音声会議とビデオ会議を実現できます。 どの方式の会議ブリッジも、複数の参加者による複数の会議を同時にサポートしています。 Cisco Unified Communications Manager は、Unified Communications Manager と Cisco TelePresence MCU の間で Binary Floor Control Protocol によるプレゼンテーション共有をサポートします。 Cisco TelePresence MCU は、ポート予約モードで設定する必要があります。 詳細については、『*Cisco TelePresence MCU* コンフィギュレーション ガイド』を参照してください。 （注） Cisco TelePresence MCU は、一般的なアウトオブバンド DTMF 方式をサポートしていません。 デフォルト設定では、Cisco Unified Communications Manager はメディア ターミネーション ポイント（MTP）を必要としません。 ただし、[メディアの終了点が必須（Media Termination Point Required）]チェックボックスがオンになっている場合は、Cisco Unified Communications Manager によって MTP が割り当てられ、SIP トランクは RFC 2833 に従って DTMF をネゴシエートします。

会議ブリッジ タイプ	説明
Cisco TelePresence Conductor	Cisco TelePresence Conductor を使用すると、会議の管理をインテリジェントに制御できます。Cisco TelePresence Conductor は、クラスタ化をサポートする、拡張性の高いデバイスで、MCU 間のロード バランシングを行い、複数のデバイスを利用可能にします。 管理者は、アプライアンスまたは VMware 上の仮想アプリケーションとして Cisco TelePresence Conductor を導入して、Cisco Unified Computing System（Cisco UCS）プラットフォームまたはサードパーティベースのプラットフォームをサポートすることができます。 Cisco TelePresence Conductor は、新しい会議ごとに最適な Cisco TelePresence リソースを動的に選択します。 アドホック、「ミートミー」、およびスケジュールされた音声およびビデオ会議は動的に拡大し、個々の MCU のキャパシティを超えることがあります。 最大 3 つの Cisco TelePresence Conductor アプライアンスまたは仮想アプリケーションをクラスタ化して、復元力をさらに高めることができます。 Cisco TelePresence Conductor アプライアンスまたは Cisco TelePresence Conductor クラスタ 1 つで、30 MCU または 2400 MCU ポートをサポートします。

会議ブリッジ タイプ	説明
Cisco Meeting Server	Cisco Meeting Server 会議ブリッジ ソリューションにより、アドホック会議、ミートミー会議、開催中の会議、ランデブー会議が可能になります。 会議ブリッジは、施設内での音声、ビデオ、ウェブ 会議を実現し、サードパーティのオンプレミス インフラストラクチャと連携します。 あらゆる規模の導入に拡張できるほか、 必要に応じて徐々に容量を増やすこともでき、組織の現在および将来のニーズに確実に対応することができます。 この会議ブリッジは高度な相互運用性を提供します。 任意の数の参加者が会議を作成し、参加することができます。 • シスコまたはサードパーティの会議室システムまたはデスクトップ ビデオ システム • Cisco Jabber クライアント • Cisco ミーティング アプリケーション（ネイティブ、または WebRTC 互換ブラウザを使用可能） • Skype for Business Cisco Meeting Server 会議ブリッジを使用するには、Cisco Meeting Server 2.0 以上のリリースが必要です。 Cisco Meeting Server は、シグナリング コール制御プロトコルとして SIP をサポートしています。 詳細に設定でき、システムおよび会議を制御およびモニタする、ビルトイン Web サーバを装備しています。 Cisco Meeting Server は、HTTP に対する XML 管理 API を提供します。 （注） Cisco Meeting Server は、H.265 ビデオ コーデックと遠端カメラ制御をサポートしていません。

会議ブリッジの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	会議ブリッジの設定 （179 ページ）	アドホック音声会議とミートミー音声会議を可能にするためにハードウェアまたはソフトウェア会議ブリッジを設定します。
ステップ 2	会議ブリッジのサービスパラメータの設定 （179 ページ）	ネットワークに Cisco IOS コンファレンスブリッジと Cisco IOS 拡張会議ブリッ

	コマンドまたはアクション	目的
		ジの両方が含まれている場合は、次の手順を実行します。
ステップ 3	会議ブリッジへの SIP トランク接続の設定 （180 ページ）	この手順を実行して、会議ブリッジへの SIP トランク接続を設定します。

会議ブリッジの設定

アドホック音声会議とミートミー音声会議を可能にするためにハードウェアまたはソフトウェア会議ブリッジを設定する必要があります。

手順

ステップ 1 Cisco Unified CM Administration から、**[メディアリソース（Media Resources）] > [会議ブリッジ（Conference Bridge）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [会議ブリッジの設定（Conference Bridge Configuration）]ウィンドウで各フィールドを設定します。 フィールドの説明の詳細については、オンライン ヘルプを参照してください。

ステップ 4 **[保存]** をクリックします。

次のタスク

ネットワークに Cisco IOS 会議ブリッジおよび Cisco IOS の拡張会議ブリッジが含まれる場合、会議ブリッジのサービスパラメータの設定 （179 ページ） を実行します。

会議ブリッジのサービスパラメータの設定

ネットワークに Cisco IOS コンファレンスブリッジと Cisco IOS 拡張会議ブリッジの両方が含まれている場合は、次の手順を実行します。

手順

ステップ 1 Cisco Unified CM の管理から、**[システム（System）] > [サービス パラメータ（Service Parameters）]** の順に選択します。

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、サーバを選択し、Cisco CallManager サービスを選択します。

ステップ 3 [クラスタ全体のパラメータ（機能 - 会議） （Clusterwide Parameters (Features - Conference)）] セクションで、次のパラメータを 6 に設定します。

- [アドホック会議の最大参加者数（Maximum Ad Hoc Conference）]

- [ミートミー会議の最大ユニキャスト数（Maximum MeetMe Conference Unicast）]

ステップ 4 **[保存]** をクリックします。

会議ブリッジへの SIP トランク接続の設定

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[トランク（Trunk）]** を選択します。

ステップ 2 次のいずれかの手順を実行します。

- 新しい SIP トランクを作成するには、[新規追加（Add New）]をクリックします。
- その接続を既存のトランクに追加するには、[検索（Find）] をクリックし、適切なトランクを選択します。

ステップ 3 [デバイスプロトコル（Device Protocol）]で、[SIP]を選択します。

ステップ 4 [トランクサービスの種類（Trunk Service Type）]で、[なし（None）]を選択します。

ステップ 5 [接続先（Destination）]領域で、会議ブリッジの IP アドレスまたはホスト名を追加して、会議ブリッジのエントリを作成します。 新しい回線が必要な場合は、**(+)** をクリックして追加することができます。

ステップ 6 [正規化スクリプト（Normalization Script）]ドロップダウン リスト ボックスから、正規化スクリプトを選択します。 たとえば、次のスクリプトは必須です。

- **cisco-telepresence-conductor-interop**：このトランクを Cisco TelePresence Conductor に接続している場合は、このスクリプトを選択します。
- **cisco-telepresence-mcu-ts-direct-interop**：このトランクを Cisco TelePresence Conductor MCU に接続している場合は、このスクリプトを選択します。
- **cisco-meeting-server-interop**：このトランクを Cisco Meeting Server に接続している場合は、このスクリプトを選択します。

ステップ 7 [トランクの設定（Trunk Configuration）] ウィンドウで、残りのフィールドを入力します。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。

ステップ 8 [保存（Save）] をクリックします。

第 15 章

拡張ロケーション コール アドミッション制御の設定

拡張ロケーション コール アドミッション制御の概要

拡張ロケーション コール アドミッション制御（CAC）を使用すると、複雑な WAN トポロジおよびクラスタ間ネットワークを介したオーディオ品質とビデオの可用性を調整できます。これには、多層ネットワークとマルチホップ ネットワークが含まれます。

ネットワーク トポロジ全体のモデルを作成して、さまざまなロケーション（LAN）と、それらのロケーションを接続する WAN リンクを示すことができます。個々のロケーションと WAN リンクについて、そのリンク経由のすべてのコールで一度に使用可能な合計帯域幅を表す、帯域幅の制限を割り当てます。特定のコールで帯域幅を使用できない場合、そのコールはビジー信号によって拒否されます。これにより、WAN リンクがオーバーサブスクライブされた結果としてオーディオとビデオの品質が劣化するのを防ぐことができます。

ロケーション帯域幅マネージャ（LBM）レプリケーション グループのクラスタ間レプリケーション機能によって、クラスタ間ネットワーク全体にロケーション設定を複製することができるため、大規模なクラスタ間ネットワークでの管理が容易になります。

拡張ロケーション CAC のコンポーネント

この機能では、次のコンポーネントを使用します。

- ロケーション：ロケーションは LAN を表します。これは、エンドポイントを含み、または単に WAN ネットワークのモデル化に対してリンク間の中継場所として機能します。Cisco Unified Communications Manager では、最大 2,000 のロケーションがサポートされます。

- リンク：2つのロケーション間の接続です。 この機能を設定するときは、個々のリンクに帯域幅の割り当てと重み付けを割り当てます。
- 重み付け：ロケーションの任意のペアの間で有効なパスを形成する、リンクの相対的な優先順位。 重み付けは、2つのロケーションの間に複数のパスが存在する場合にのみ使用されます。 重み付けは、有効なパス（累積された重み付けが最も小さいパス）を計算するために使用されます。
- 帯域幅割り当て：特定のタイプのトラフィック（オーディオ、デスクトップ ビデオ、イマーシブ ビデオ）に割り当てられた合計帯域幅。 帯域幅は、ロケーション内のコールにも割り当てることができます（デフォルト設定は [無制限（Unlimited）]）。
- ロケーション帯域幅マネージャ（LBM）：拡張ロケーション CAC が機能するためには、Cisco Unified Serviceability で機能サービスをアクティブ化する必要があります。 このサービスは、ネットワーク モデルを収集し、ロケーション間の有効なパスを算出します。これは、発信側と着信側の間のすべてのリンクとロケーションの重み付けを加算し、累積された重み付けが最も小さいパスを選択することによって算出されます。

ロケーションとリージョンの関係

拡張ロケーション コール アドミッション制御でのロケーションの設定と、リージョンを組み合わせて、コールの帯域幅を管理できます。

- リージョンの設定での帯域幅の割り当ては、2 つのリージョン間でのコールでエンドポイントが使用できる帯域幅の合計量を割り当てるものです。
- ロケーションの設定での帯域幅の割り当ては、ロケーション間でのコールで使用できる帯域幅の総量を割り当てるものです。 個別のコールについては、リージョンの設定での帯域幅は、ロケーションの設定で使用可能になっている帯域幅から差し引かれます。 たとえば、ロケーションの設定により特定のリンクで 160 kb/s の帯域幅が使用可能になっている場合、そのリンクでは、それぞれ 80 kb/s の G.711 コールを同時に 2 つサポートできます。

（注） サーバの CPU 使用率が急激に増加する可能性があるため、実稼働時間中に Location Bandwidth Manager の帯域幅またはリンク設定を変更しないでください。

Cisco Unified Communications Manager は、クラスタごとに最大 2,000 のロケーションと 2,000 のリージョンをサポートします。

クラスタ間 LBM レプリケーション

ロケーション帯域幅マネージャのハブ グループのクラスタ間レプリケーション機能を使用すると、より大規模なクラスタ間ネットワーク全体でロケーションとリンク割り当てを複製できます。 LBM を LBM ハブのロールに割り当てることで、メッシュされたクラスタ間ネットワーク全体で、ロケーションおよびリンク情報をアクティブに複製できます。 LBM ハブは、共通の接続を通じて互いを検出し、フルメッシュ型のレプリケーション ネットワークを構成しま

す。 スポークのロールが割り当てられた LBM は、そのクラスタの LBM ハブを介してクラスタ間レプリケーションに間接的に参加できます。

クラスタ間トポロジの管理

クラスタ間ネットワークを設定して管理する方法は複数あります。 次の表に、クラスタ間トポロジの設定と管理に対する 2 つのアプローチの概要を示します。

設計へのアプローチ	説明
ロケーションとリンクの管理	単一のクラスタを使用して、クラスタ間ネットワーク全体のすべてのリンクの帯域幅の割り当てを設定、管理します。 この方法では、特に、共通のロケーションが多い展開で、設定の負担が軽減されます。クラスタ間の設定方法は次のとおりです。 管理クラスタで、トポロジ全体についてすべてのロケーションとリンク（帯域幅の割り当てと重み付けを含む）を設定します。 この情報は、クラスタ間ネットワークに複製されます。 トポロジ内の他のクラスタでは、次のことを設定します。 • ローカル クラスタについてのみロケーションを設定します。 これは、デバイスをロケーションに関連付けるためだけに設定します。 • リンク情報は設定しないでください。 • ローカル クラスタ内のすべての帯域幅の割り当てを [無制限（Unlimited）]のままにします。 管理クラスタによって複製される帯域幅の割り当てがローカル クラスタでの割り当てよりも少ない場合、制限が厳しい方の設定が適用されます。
クラスタ間の Enhanced Locations CAC	このアプローチでは、次のように設定します。 • 各クラスタ内で、ローカルのロケーションと、隣接するクラスタのみに対するリンク情報を設定します。 • 隣接するクラスタに対してのみ、重み付けと帯域幅の割り当てを含め、リンク情報を割り当てます。 トポロジの残りの部分では、により複製されます。 • 各クラスタで Hub_None ロケーションの名前を変更する必要があります。そうしないと、それがクラスタ全体で共通のロケーションになります。 • 各クラスタには、一意のクラスタ ID が必要です。 （注） これは、レプリケーションですべてのクラスタにわたって一貫してクラスタ名を指定するために重要です。

拡張ロケーション CAC の前提条件

この機能を設定する前に、自社の LAN および WAN のネットワーク トポロジを把握してください。 この情報は、ロケーションとリンクに帯域幅を割り当てるために必要です。

拡張ロケーション CAC のタスク フロー

ご使用のシステムで拡張ロケーション コール アドミッション制御を設定するには、この手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	ロケーション帯域幅マネージャのアクティブ化 （185 ページ）	少なくとも 1 つのクラスタ ノードで、シスコ ロケーション帯域幅マネージャ機能サービスが実行されている必要があります。
ステップ 2	LBM グループの設定 （185 ページ）	デフォルトでは、Cisco CallManager サービスはローカルの LBM サービスと通信します。 ただし、LBM グループを使用してこの通信を管理し、冗長性のためにアクティブおよびスタンバイの LBM を提供できます。
ステップ 3	ロケーションとリンクの設定 （186 ページ）	ネットワークのロケーション（LAN）を作成し、それらのロケーションを接続する WAN リンクに帯域幅を割り当てます。
ステップ 4	LBM クラスタ間レプリケーション グループの設定 （187 ページ）	設定した CAC 情報を他のクラスタに複製するクラスタ間レプリケーション グループを作成します。
ステップ 5	SIP クラスタ間トランクの設定 （187 ページ）	ネットワーク内の SIP クラスタ間トランクに [シャドウ（Shadow）] ロケーションを割り当てます。
ステップ 6	コール アドミッション制御のサービス パラメータの設定 （188 ページ）	これはオプションです。 コール アドミッション制御のサービス パラメータの設定項目を指定します。 ほとんどの展開では、デフォルト設定で十分です。

ロケーション帯域幅マネージャのアクティブ化

拡張ロケーション コールアドミッション制御については、クラスタ内の少なくとも1つのノードでシスコ ロケーション帯域幅マネージャ機能サービスをアクティブ化する必要があります。このサービスはデフォルトでオフになっています。

手順

ステップ 1 Cisco Unified Serviceability から、**[ツール（Tools）]** > **[サービスの有効化（Service Activation）]** を選択します。

ステップ 2 [サーバ（Server）]ドロップダウン リストから、サービスを実行するクラスタ ノードを選択して [移動（Go）] をクリックします。

ステップ 3 [CMサービス（CM Services）]の下にある、[シスコ ロケーション帯域幅マネージャ（Cisco Location Bandwidth Manager）]サービスをオンにします。

ステップ 4 **[保存]** をクリックします。

ステップ 5 さらに他のノードでサービスを開始する場合は、このタスクを繰り返します。

（注） シスコでは、Cisco CallManager サービスも実行しているクラスタ内の各サブスクライバ ノードで、シスコ ロケーション帯域幅マネージャ サービスを実行することを推奨しています。

LBM グループの設定

LBM グループを設定するには、この手順を使用します。 デフォルトでは、Cisco CallManager サービスはローカルの LBM サービスと通信します。 ただし、LBM グループを使用してこの通信を管理し、冗長性のためにアクティブおよびスタンバイの LBM を提供できます。

（注） Cisco CallManager サービスが LBM を使用する順序は次のとおりです。

- LBM グループの指定
- ローカル LBM（共存）

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[ロケーション（Locations）]** > **[ロケーション帯域幅マネージャ グループ（Location Bandwidth Manager Group）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 グループに [名前（Name）]を割り当てます。

ステップ 4 [アクティブメンバー（Active Member）]ドロップダウンから、このグループのアクティブなメンバーを選択します。

ステップ 5 [スタンバイメンバー（Standby Member）]ドロップダウンから、アクティブ メンバーが使用できないときに使用することが望ましいスタンバイを選択します。

ステップ 6 **[保存]** をクリックします。

ロケーションとリンクの設定

ネットワーク内にロケーション（LAN）を作成するには、この手順を使用します。 これらのロケーション間で WAN リンクを使用するコールに、合計帯域幅と重み付けを割り当てます。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[ロケーション情報（Location Info）]** > **[ロケーション（Location）]** を選択します。

ステップ 2 [新規追加（Add New）]をクリックし、新しいロケーションを作成します。

ステップ 3 ロケーションに [名前（Name）]を割り当てます。

ステップ 4 [リンク-このロケーションと隣接ロケーション間の帯域幅（Links - Bandwidth Between This Location and Adjacent Locations）]領域で、別のロケーションに対する WAN リンクの設定項目を指定します。

a) [ロケーション（Location）]リスト ボックスから、2 つ目のロケーションを選択します。
b) 有効なパスの形成する際のこのリンクの相対的な優先順位を反映した[重み付け（Weight）]を設定します。
c) オーディオ、ビデオ、イマーシブ ビデオ（TelePresence）の各コールの合計帯域幅を設定します。
d) さらに別のロケーションに対するリンクを設定するには、この手順を繰り返します。

ステップ 5 これはオプションです。[ロケーション内-このロケーション内のデバイスの帯域幅（Intra-location - Bandwidth for Devices Within This Location）]領域を展開し、新しく作成したロケーションのロケーション内コールに対する帯域幅の割り当てを設定します。 これらのコールについては、すべてのメディア タイプでデフォルト設定は [無制限（Unlimited）]になっています。

ステップ 6 [他のロケーションの設定を変更（Modify Settings to Other Locations）]領域で、他のロケーションに対する RSVP 設定項目を指定します。

a) [ロケーション（Location）]列で、他のロケーションを選択します。
b) これらのロケーション間でのコールに関する [RSVP設定（RSVP Setting）]を選択します。
c) さらに他のロケーションとのコールについて RSVP 設定を追加するには、これらのサブステップを繰り返します。

ステップ 7 **[保存]** をクリックします。

ステップ 8 追加のロケーションを作成し、それらの新しいロケーションとの間のリンクを設定するには、この手順を繰り返します。

LBM クラスタ間レプリケーション グループの設定

LBM クラスタ間レプリケーション グループを設定するには、この手順を使用します。 これは、クラスタ間ネットワーク全体に拡張ロケーションアドミッション制御の帯域幅情報を複製するために必要です。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [ロケーション情報（Location Info）] > [ロケーション帯域幅マネージャ（LBM）のクラスタ間レプリケーション グループ（Location Bandwidth Manager (LBM) Intercluster Replication Group）]**を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [Name]にグループの名前を入力します。

ステップ 4 [ブートストラップサーバ（Bootstrap Servers）]領域で、他のハブに接続情報を複製する責任を負う LBM サーバを 1 台以上割り当てます。

ステップ 5 [ロールの割り当て（Role Assignments）]領域で、上向き矢印と下向き矢印を使用して、ハブとして機能するローカル LBM サーバと、スポークのままにする LBM サーバを選択します。

ステップ 6 **[保存]** をクリックします。

SIP クラスタ間トランクの設定

拡張ロケーションコールアドミッション制御を使用する場合、クラスタ間ネットワークのSIP クラスタ間トランクにシャドウ ロケーションを割り当てる必要があります。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [トランク（Trunks）]** を選択します。

ステップ 2 [検索（Find）]をクリックして、適切なクラスタ間トランクを選択します。

ステップ 3 [ロケーション（Location）]ドロップダウン リストから [シャドウ（Shadow）]を選択します。

ステップ 4 [トランクの設定（Trunk Confiiguration）]ウィンドウで、その他の必要なフィールドを入力します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 5 **[保存]** をクリックします。

ステップ 6 拡張ロケーション コール アドミッション制御の情報を複製するクラスタ間トランクが他にもあれば、この手順を繰り返します。

コール アドミッション制御のサービス パラメータの設定

拡張ロケーション コール アドミッション制御に関する任意指定のサービス パラメータを設定するには、この手順を使用します。

手順

ステップ 1 Cisco Unified CM の管理から、**[システム（System）] > [サービス パラメータ（Service Parameters）]** の順に選択します。

ステップ 2 [サーバ（Server）]ドロップダウン リストから、クラスタ ノードを選択します。

ステップ 3 **Cisco CallManager** サービスのサービス パラメータを設定します。

a) [サービス（Service）]ドロップダウン リストから、[Cisco CallManager]を選択します。

b) [クラスタ全体のパラメータ（コールアドミッション制御）（Clusterwide Parameters (Call Admission Control)）]領域で、任意のサービス パラメータを設定します。 パラメータに関するヘルプの説明を参照するには、GUI でパラメータの名前をクリックします。

c) **[保存]** をクリックします。

ステップ 4 **シスコ ロケーション帯域幅マネージャ** サービスの設定項目を指定します。

a) [サービス（Service）]ドロップダウン リストから、[シスコロケーション帯域幅マネージャ（Cisco Location Bandwidth Manager）]を選択します。

b) 目的のサービス パラメータを設定します。 パラメータに関するヘルプの説明を参照するには、GUI でパラメータの名前をクリックします。

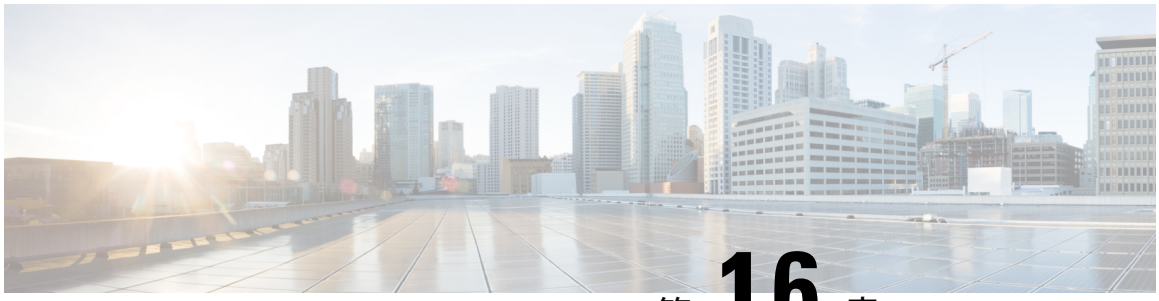
c) **[保存]** をクリックします。

拡張ロケーション CAC の連携動作の制限

次の表に、拡張ロケーション コールアドミッション制御の機能の連携動作と制限を示します。

機能	連携動作と制限事項
LBM セキュリティ モード	デフォルトでは、LBM セキュリティ モードはセキュアではありません。 この設定を、[LBMセキュリティモード（LBM Security Mode）] エンタープライズパラメータを使用して設定し直すことができます。このパラメータは、[セキュア（Secure）]、[非セキュア（Insecure）]、または [混合（Mixed）]に設定できます。 [混合（Mixed）]設定は、すべてのクラスタをセキュアにする間も通信を維持するために一時的に使用し、後で [セキュア（Secure）]に変更することができます。 このパラメータを変更した後は、設定を反映させるために、クラスタ内のすべての Cisco LBM サービス ハブをリセットする必要があります。
ビデオ通話のオーディオ帯域幅の差し引き	デフォルトでは、ビデオ通話のオーディオ部分の帯域幅はビデオ プールから差し引かれます。 [ビデオ通話のオーディオ部分をオーディオ プールから差し引く（Deduct Audio Portion from Audio Pool for Video Calls）]サービス パラメータを **True**（デフォルト設定は **False**）に設定することで、ビデオ通話のオーディオ部分をオーディオ プールから差し引くようにシステムを設定し直すことができます。
ビデオ通話の分類	Cisco TelePresence エンドポイントには、設定を変更できないビデオ通話分類である**イマーシブ**が用意されています。 その他のエンドポイントには、設定を変更できないビデオ 通話分類である**デスクトップ**が用意されています。 SIP トランクについては、関連付けられた SIP プロファイルで [ビデオ通話のトラフィッククラス（Video Call Traffic Class）]を設定することで、ビデオ分類（デスクトップ、イマーシブ、または混合）を設定できます。
メディア リソース	メディア リソースの帯域幅は、コール アドミッション制御では割り当てられません。
ロケーションの有用性	Cisco Unified Serviceability インターフェイスには、ロケーション トポロジの管理とモニタリングに使用する追加のツールが含まれます。詳細については、『*Cisco Unified Serviceability* アドミニストレーション ガイド』の「ロケーション」のトピックを参照してください。
セッション帯域幅修飾子	[SIP プロファイルの設定（SIP Profile Configuration）] ウィンドウで、SIP エンドポイントが使用するセッション帯域幅の修飾子を割り当てることができます。
帯域幅の割り当ての競合	共通のリンクまたは場所で帯域幅容量または重みの割り当てに競合がある場合、ローカル クラスタは割り当てられた値の最小値を使用します。

機能	連携動作と制限事項
デバイス サポート	Unified CM と LBM は、IP 電話、ゲートウェイ、H.323 トランク接続先、および SIP トランク接続先を含む、あらゆるタイプのエンドデバイスの帯域幅を管理します。 ただし、クラスタ間拡張ロケーション CAC には、システム ロケーションのシャドウに割り当てられた SIP ICT が必要です。 他のタイプのデバイスは、一般（固定）ロケーションに割り当てられている場合にのみサポートされます。
ネットワーク障害	ネットワーク障害が発生した場合は、Unified CM が計算した帯域幅予約経路にネットワーク状態が正確に反映されない可能性があります。 このシナリオを許可する申し分のない方法はモデル内に存在しません。
同期に関する問題	システムによって作成されたモデルは常に完全に同期されるわけではありません。 保守的な帯域幅割り当てを使用して、この制約に適応できます。
WAN を介したクラスタリング	WAN 上のクラスタリングとローカル フェールオーバーを使用する導入環境では、WAN の帯域幅計算でクラスタ内 LBM トラフィックがあらかじめ計算されます。
フレキシブル DSCP マーキング	さらに QoS を高めるために、DSCP マーキングを使用して、特定のタイプの通話フローを他よりも優先するマーキングを割り当てることができます。 たとえば、ネットワークが輻輳してビデオ メディアがブロックされる場合でも基本的な通信をオーディオで続行できるように、ビデオよりもオーディオを優先することができます。 DSCP マーキングは、次の 2 つの方法で設定できます。 • サービス パラメータ：[サービスパラメータの設定（Service Parameter Configuration）]ウィンドウの [クラスタ全体のパラメータ（システム-QoS）（Clusterwide Parameters (System - QoS)）]セクションで、クラスタ全体の DSCPのデフォルト値を設定します。 • SIP プロファイル：SIP プロファイルでカスタマイズされた DSCP 設定項目を設定し、それを特定の SIP デバイスのグループに割り当てます。 この設定は、クラスタ全体のデフォルト値よりも優先されます。
APIC-EM コントローラ	APIC_EM コントローラを使用すると、外部の QoS 管理向けの SIP メディア フローを管理できます。 詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』を参照してください。



第 16 章

Resource Reservation Protocol（RSVP）の設定

RSVP コール アドミッション制御の概要

Resource Reservation Protocol（RSVP）は、IP ネットワーク内のリソースを予約するための、トランスポート レベルのリソース予約プロトコルです。 RSVP は、拡張場所のコール受付制御 (CAC) の代替として使用できます。 特定のセッションのリソースを予約します。 セッションは、特定の宛先アドレス、宛先ポート、およびプロトコル識別子（TCP または UDP）を持つフローから構成されます。

RSVP コール アドミッション制御の前提条件

IPv4 アドレッシングを使用する必要があります。 RSVP は IPv6 をサポートしていません。

RSVP 設定のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	クラスタ全体のデフォルト RSVP ポリシーの設定 （192 ページ）	クラスタ内の全ノードについて RSVP ポリシーを設定します。
ステップ 2	ロケーション ペア RSVP ポリシーの設定 （193 ページ）	これはオプションです。 ロケーション ペアにクラスタの他とは別のポリシーを

	コマンドまたはアクション	目的
		使用する場合、特定のロケーション ペアの RSVP ポリシーを設定できます。
ステップ 3	RSVP の再試行の設定 （194 ページ）	RSVP の再試行の頻度と番号を設定します。
ステップ 4	コール中 RSVP エラー処理の設定 （195 ページ）	コール中に RSVP が失敗したときにシステムがどのように応答するかを設定します。
ステップ 5	MLPP から RSVP への優先レベル マッピングの設定 （196 ページ）	これはオプションです。 複数レベルの優先順位およびプリエンプト (MLPP) を使用する場合は、発信者 MLPP 優先レベルを RSVP 優先順位にマップします。
ステップ 6	RSVP エージェントの設定	ゲートウェイ デバイスで次の IOS 手順を実行します。 RSVP エージェントの設定方法については、デバイスのドキュメントを参照してください。
ステップ 7	アプリケーション ID の設定 （197 ページ）	RSVP アプリケーション ID を設定すると、音声およびビデオ トラフィックの両方に ID が追加され、受信した ID をもとに、Cisco RSVP エージェントは、それぞれのトラフィック タイプに帯域幅の制限を設定できます。
ステップ 8	DSCP マーキングの設定 （198 ページ）	DSCP マーキングを設定して、RSVP の予約が失敗した場合、システムが RSVP エージェントまたはエンドポイント デバイスに指示してメディアの差別化サービス コントロール ポイントのマーキングをベスト エフォートに変更できるようにします。 DSCP マーキングを設定しない場合、EF マークされたメディアのパケットの超過分が、予約されているフローに対してもサービス品質（QoS）を劣化させます。

クラスタ全体のデフォルト RSVP ポリシーの設定

クラスタ内の全ノードについて RSVP ポリシーを設定します。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[システム（System）] > [サービス パラメータ（Service Parameters）]** を選択します。

ステップ 2 [サービス パラメータ設定（Service Parameter Configuration）]ウィンドウで、サーバを選択し、Cisco CallManager サービスを選択します。

ステップ 3 [クラスタ全体のパラメータ（システム-RSVP）（Clusterwide Parameters (System - RSVP)）]セクションで、Default interlocation RSVP Policy サービス パラメータを設定します。

このサービス パラメータを次の値に設定できます。

- [予約なし（No Reservation）]：どの 2 つのロケーション間にも RSVP 予約は作成されません。
- [オプション（ビデオ優先）（Optional (Video Desired)）]：オーディオ ストリームおよびビデオ ストリームの両方の予約を取得できない場合は、ベストエフォートとして、オーディオのみのコールを継続できます。 RSVP エージェントはオーディオに関する RSVP 予約を引き続き試み、予約が成功した場合は、Cisco Unified Communications Manager に通知します。
- [必須（Mandatory）]：Cisco Unified Communications Manager は、オーディオ ストリームに対する（コールがビデオ通話の場合はビデオ ストリームに対する）RSVP 予約が成功するまで、終了デバイスを呼び出しません。
- [必須（ビデオ優先）（Mandatory (Video Desired)）]：オーディオ ストリームの予約は成功したが、ビデオ ストリームの予約に失敗する場合は、音声のみでビデオ通話を行うことができます。

次のタスク

次のいずれかのオプションを選択します。

- ロケーション ペアで、残りのクラスタと異なるポリシーを使用する場合は、「ロケーション ペア RSVP ポリシーの設定 （193 ページ）」に進みます。
- クラスタ内の全ノードに同一の RSVP ポリシーを使用している場合は、「RSVP の再試行の設定 （194 ページ）」に進みます。

ロケーション ペア RSVP ポリシーの設定

ロケーション ペアにクラスタの他とは別のポリシーを使用する場合、特定のロケーション ペアの RSVP ポリシーを設定できます。 次の手順を使用するとき、ロケーション ペアに設定する RSVP ポリシーは、クラスタに設定したポリシーをオーバーライドします。

手順

ステップ 1 Cisco Unified Communications Manager の管理ページで、**[システム（System）] > [ロケーション（Location）]** メニュー オプションを選択します。

ステップ 2 ロケーション ペアの一方のロケーションを検索し、そのロケーションを選択します。

ステップ 3 選択したロケーションと別のロケーション間の RSVP ポリシーを変更するには、ロケーション ペアのもう一方のロケーションを選択します。

ステップ 4 [RSVP 設定（RSVP Settings）] ドロップダウン リストで、このロケーション ペアの RSVP ポリシーを選択します。

このフィールドに次の値を設定できます。

- [システム デフォルトを使用（Use System Default）]：ロケーション ペアの RSVP ポリシーが、クラスタ全体の RSVP ポリシーと一致します。
- **[予約なし（No Reservation）]**：どの 2 つのロケーション間にも RSVP 予約は作成されません。
- [音声優先（オプション）（Video Desired (Optional)）]：音声およびビデオ ストリームの予約を取得できない場合、ベストエフォート、音声のみのコールとして処理されます。RSVP エージェントは、音声の RSVP の予約を引き続き試行し、予約が成功すると Cisco Unified Communications Manager に通知します。 オーディオ ストリームに対する（コールがビデオ通話の場合はビデオ ストリームに対する）RSVP 予約が成功するまで、終端デバイスを呼び出しません。
- [音声優先（Video Desired）] – オーディオ ストリームの予約は成功したが、ビデオ ストリームの予約が成功しない場合、ビデオ通話は音声のみコールとして処理されます。

次のタスク

RSVP の再試行の設定 （194 ページ）

RSVP の再試行の設定

RSVP の再試行の頻度および回数を設定するには、次の手順を実行します。

始める前に

- クラスタ全体のデフォルト RSVP ポリシーの設定 （192 ページ）
- これはオプションです。 ロケーション ペア RSVP ポリシーの設定 （193 ページ）

手順

ステップ 1 Cisco Unified Communications Manager Administrationで、**[システム（System）] > [サービスパラメータ（Service Parameters）]** を選択します。

ステップ 2 [サービスパラメータ設定（Service Parameter Configuration）] ウィンドウで、サーバを選択し、Cisco CallManager サービスを選択します。

ステップ 3 [クラスタ全体のパラメータClusterwide（System - RSVP）（Clusterwide Parameters (System - RSVP)）] セクションで指定されたサービス パラメータを設定します。

これらのサービス パラメータを次の値に設定できます。

- [RSVP 再試行タイマー（RSVP Retry Timer）]：RSVP 再試行タイマーの値を秒単位で指定します。 このパラメータを 0 に設定すると、システムで RSVP の再試行が無効になります。
- [必須 RSVP ミッドコール再試行カウンタ（Mandatory RSVP Midcall Retry Counter）]：RSVP ポリシーが [必須（Mandatory）] に指定され、ミッドコール エラー処理オプションが [次の再試行カウンタを超えるとコールは失敗する（call fails following retry counter exceeds）]「」に設定されているときに、ミッドコールRSVP再試行カウンタを指定します。 デフォルト値は 1 回です。 サービス パラメータを -1 に設定すると、予約が成功するか、コールが切断されるまで、いつまでも再試行が続行されます。

次のタスク

コール中 RSVP エラー処理の設定 （195 ページ）

コール中 RSVP エラー処理の設定

コール中の RSVP エラー処理の設定には、次の手順を使用します。

始める前に

RSVP の再試行の設定 （194 ページ）

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、**[システム（System）] > [サービス パラメータ（Service Parameters）]** を選択します。

ステップ 2 [サービスパラメータ設定（Service Parameter Configuration）] ウィンドウで、サーバを選択し、Cisco CallManager サービスを選択します。

ステップ 3 [クラスタ全体のパラメータ（システム - RSVP）（Clusterwide Parameters (System - RSVP)）] セクションで、指定されたサービス パラメータを設定します。

通話中の強制 RSVP エラー処理のオプション サービス パラメータに次の値を設定できます。

- [Call becomes best effort]： コール中に RSVP が失敗した場合、コールはベスト エフォート型のコールになります。 再試行を有効にすると、RSVP の再試行が同時に開始されます。
- [Call fails following retry counter exceeded]：Mandatory RSVP Mid-call Retry Counter サービス パラメータに数値「N」を指定し、コール中に RSVP が失敗した場合、RSVP の再試行を N 回実行した後に、コールは失敗します。

次のタスク

ゲートウェイのデバイスに RSVP エージェントを設定します。 RSVP エージェントの設定方法については、デバイスのドキュメントを参照してください。 ゲートウェイで RSVP エージェントを設定した後は、Cisco Unified Communications Manager Administration に戻り、次のいずれかのオプションを選択します。

- （任意）ネットワーク内でマルチレベルの優先順位とプリエンプションを使用している場合は、「MLPP から RSVP への優先レベル マッピングの設定 （196 ページ）」に進みます。
- アプリケーション ID の設定 （197 ページ）

MLPP から RSVP への優先レベル マッピングの設定

これはオプションです。 発信者の MLPP 優先順位から RSVP 優先レベルへのマッピングを設定するには、次に示すクラスタ全体（システム - RSVP）のサービス パラメータを使用します。

- MLPP EXECUTIVE OVERRIDE To RSVP Priority Mapping
- MLPP FLASH OVERRIDE To RSVP Priority Mapping
- MLPP FLASH To RSVP Priority Mapping
- MLPP IMMEDIATE To RSVP Priority Mapping
- MLPP PL PRIORITY To RSVP Priority Mapping
- MLPP PL ROUTINE To RSVP Priority Mapping

これらのサービス パラメータを選択し、設定するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[システム（System）] > [サービス パラメータ（Service Parameters）]** を選択します。

ステップ 2 [サービスパラメータ設定（Service Parameter Configuration）] ウィンドウで、サーバを選択し、Cisco CallManager サービスを選択します。

ステップ 3 [クラスタ全体のパラメータClusterwide（System - RSVP）（Clusterwide Parameters (System - RSVP)）] セクションで指定されたサービス パラメータを設定します。

これらのサービス パラメータは、次のように機能します。

- サービス パラメータ値が高いほど、優先度を上げるという設定に基づいて RSVP 予約を開始するとき、Cisco Unified Communications Manager は発信者の優先度レベルを RSVP 優先度にマップします。
- IOS ルータは RSVP 優先度に基づいてコールをプリエンプション処理します。
- RSVP エージェントは、プリエンプションの理由を含め、RSVP 予約の失敗の理由について Cisco Unified Communications Manager に通知する必要があります。
- Cisco Unified Communications Manager は、既存の MLPP メカニズムを使用して、優先処理の対象となった発信側と着信側に優先処理に関する通知を行います。

次のタスク

ゲートウェイのデバイスに RSVP エージェントを設定します。 RSVP エージェントの設定方法については、デバイスのドキュメントを参照してください。 ゲートウェイで RSVP のエージェントを設定した後は、Cisco Unified Communications Manager Administration と「アプリケーション ID の設定 （197 ページ）」に戻ります。

アプリケーション ID の設定

RSVP アプリケーション ID を設定すると、音声およびビデオ トラフィックの両方に ID が追加され、受信した ID をもとに、Cisco RSVP エージェントは、それぞれのトラフィック タイプに帯域幅の制限を設定できます。

この手順を開始する前に、ゲートウェイ デバイスで RSVP のエージェントを設定します。 RSVP エージェントの設定方法については、デバイスのドキュメントを参照してください。

始める前に

ネットワークに RSVP アプリケーション ID を導入するには、Cisco RSVP Agent ルータで、Cisco IOS Release 12.4(6)T 以降を使用する必要があります。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[システム（System）] > [サービス パラメータ（Service Parameters）]** を選択します。

ステップ 2 [サービス パラメータ設定（Service Parameter Configuration）]ウィンドウで、サーバを選択し、Cisco CallManager サービスを選択します。

ステップ 3 [クラスタ全体のパラメータ（システム - RSVP）（Clusterwide Parameters (System - RSVP)）]セクションで、RSVP Audio Application ID サービス パラメータを設定します。

デフォルトは AudioStream です。

ステップ 4 [クラスタ全体のパラメータ（システム - RSVP）（Clusterwide Parameters (System - RSVP)）]セクションで、RSVP Video Application ID を設定します。

デフォルトは VideoStream です。

次のタスク

DSCP マーキングの設定 （198 ページ）

DSCP マーキングの設定

RSVP 予約が失敗した場合、 システムは RSVP エージェントまたはエンドポイント デバイス（RSVP エージェントの割り当てに失敗した場合）に、メディアの Differentiated Services Control Point（DSCP）マークをベストエフォート型に変更するよう指示します。 DSCP マーキングを設定しない場合、EF マークされたメディアのパケットの超過分が、予約されているフローに対してもサービス品質（QoS）を劣化させます。

始める前に

アプリケーション ID の設定 （197 ページ）

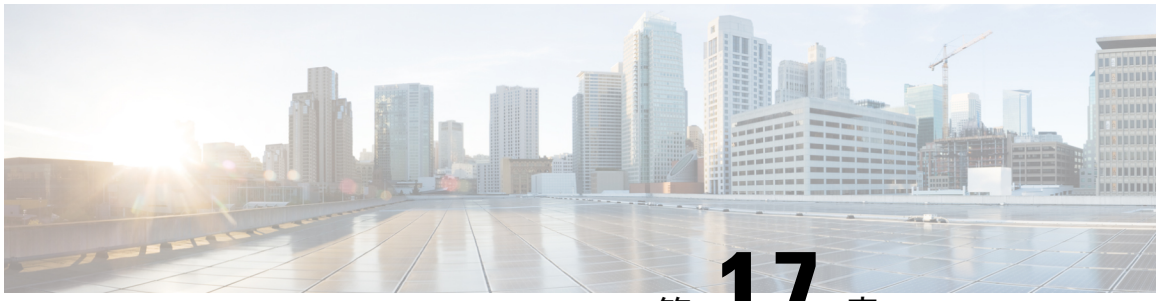
手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[システム（System）] > [サービス パラメータ（Service Parameters）]** を選択します。

ステップ 2 [サービス パラメータ設定（Service Parameter Configuration）]ウィンドウで、サーバを選択し、Cisco CallManager サービスを選択します。

ステップ 3 [クラスタ全体のパラメータ（システム - QoS）（Clusterwide Parameters (System - QoS)）]セクションで、**DSCP for Audio Calls When RSVP Fails** のサービス パラメータを設定します。

ステップ 4 [クラスタ全体のパラメータ（システム - QoS）（Clusterwide Parameters (System - QoS)）]セクションで、**DSCP for Video Calls When RSVP Fails** のサービス パラメータを設定します。



第 17 章

プッシュ通知の設定

プッシュ通知の概要

クラスタでプッシュ通知が有効になっている場合、Unified Communications Manager および IM and Presence Service は、サスペンドモード（バックグラウンドモードとも呼ばれます）で動作している Android および iOS 用 Cisco Jabber または Cisco Webex クライアントに音声通話、ビデオ通話、インスタントメッセージの通知をプッシュするために、Google と Apple のクラウドベースのプッシュ通知サービスを使用します。プッシュ通知によって、システムは Cisco Jabber または Cisco Webex と永続的な通信を維持できます。プッシュ通知は、エンタープライズネットワーク内から接続する Android および iOS 用 Cisco Jabber および Cisco Webex クライアントと、Expressway のモバイルおよびリモートアクセス機能を通じてオンプレミス展開に登録するクライアントの両方で必要となります。

プッシュ通知の動作

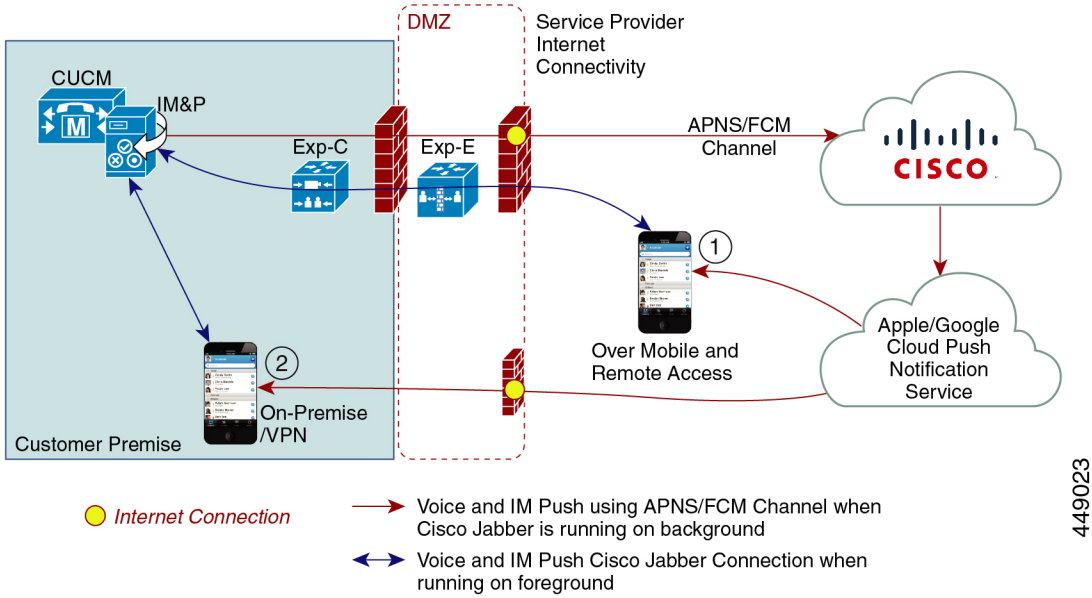
Android および iOS プラットフォームデバイスにインストールされているクライアントは、起動時に Unified Communications Manager、IM and Presence Service、および Google と Apple のクラウドに登録します。モバイルおよびリモートアクセスの展開では、クライアントは Expressway 経由でオンプレミスサーバに登録します。Cisco Jabber および Cisco Webex クライアントがフォアグラウンドモードになっている限り、Unified Communications Manager および IM and Presence Service は、コールとインスタントメッセージをクライアントに直接送信することができます。

ただし、Cisco Jabber または Cisco Webex クライアントが（たとえばバッテリ寿命を長持ちさせるために）サスペンドモードに移行すると、標準の通信チャネルは使用不可となり、Unified Communications Manager および IM and Presence Service がクライアントと直接通信することはできなくなります。プッシュ通知は、パートナークラウドを介してクライアントに到達するための別のチャネルを提供します。

（注） 次のいずれかの条件が当てはまる場合、Cisco Jabber および Cisco Webex は保留モードで動作しているとみなされます。

- Cisco Jabber または Cisco Webex アプリケーションがオフスクリーンで（つまりバックグラウンドで）実行されている
- Android または iOS デバイスがロックされている
- Android または iOS デバイスの画面がオフになっている

図 *6:* プッシュ通知のアーキテクチャ



上の図は、Android および iOS 用 Cisco Jabber または Cisco Webex クライアントが、バックグラウンドで動作している場合と停止している場合の動作を示したものです。 この図では、(1) オンプレミスの Cisco Unified Communications Manager に接続するクライアントと Expressway を介した IM and Presence サービスの展開でのモバイルおよびリモートアクセスの展開と、(2) エンタープライズネットワーク内からオンプレミス展開に直接接続する Android および iOS 用 Cisco Jabber または Cisco Webex Teams クライアントを示しています。

（注） iOS13 の Apple クライアントおよびサポートされている Android クライアントでは、音声通話とメッセージは別々のプッシュ通知チャネル（「VoIP」と「Message」）を使用して、バックグラウンドモードで動作しているクライアントに到達します。 ただし、全般的なフローはどちらのチャネルでも同じです。 iOS 12 では、音声通話とメッセージは同じチャネルを使用して配信されます。

Cisco Jabber および Cisco Webex のプッシュ通知の動作

次の表は、Unified Communications Manager および IM and Presence Service に登録された Cisco Jabber または Cisco Webex iOS クライアントの、iOS 12 および iOS 13 での動作を説明したものです。

Cisco Jabber または Cisco Webex クライアントの動作モード	Cisco Jabber が iOS12 デバイスで実行されている場合	Cisco Jabber が iOS13 デバイスまたは Android デバイスで実行されている場合
フォアグラウンドモード	音声/ビデオ通話 Unified Communications Manager 標準の SIP 通信チャネルを使用して、音声通話とビデオ通話を Cisco Jabber または Cisco Webex Teams クライアントに直接送信します。 通話の場合、Unified Communications Manager はプッシュ通知もフォアグラウンドモードの Cisco Jabber または Cisco Webex クライアントに送信します。 ただし、通話の確立には、プッシュ通知チャネルではなく標準の SIP チャネルが使用されます。 メッセージ IM and Presence Service は、標準の SIP 通信チャネルを使用してメッセージをクライアントに直接送信します。 メッセージの場合、フォアグラウンドモードのクライアントにプッシュ通知は送信されません。	動作は iOS12 の場合と同じです。

Cisco Jabber または Cisco Webex クライアントの動作モード	Cisco Jabber が iOS12 デバイスで実行されている場合	Cisco Jabber が iOS13 デバイスまたは Android デバイスで実行されている場合
サスペンドモード（バックグラウンドモード）	音声コールまたはビデオ通話 標準の通信チャネルは使用できません。Unified CM はプッシュ通知チャネルを使用します。 通知を受信すると、Cisco Jabber または Cisco Webex クライアントは自動的にフォアグラウンドモードに戻り、クライアントが呼出音を鳴らします。 メッセージング 標準の通信チャネルは使用できません。IM and Presence サービスはプッシュ通知チャネルを使用して、次のように IM 通知を送信します。 1. IM and Presence サービスは、シスコ クラウドのプッシュ REST サービスに IM 通知を送信し、その後通知は Apple クラウドに転送されます。 2. Apple クラウドは Cisco Jabber または Cisco Webex クライアントに IM 通知をプッシュし、Cisco Jabber または Cisco Webex クライアントに通知が表示されます。 3. ユーザが通知をクリックすると、Cisco Jabber または Cisco Webex クライアントは再びフォアグラウンドに移行します。 Cisco Jabber または Cisco Webex クライアントは、IM and Presence Service とのセッションを再開し、インスタントメッセージをダウンロードします。 （注） Cisco Jabber または Cisco Webex クライアントがサスペンドモードの間、ユーザのプレゼンスステータスは**「退席中」**と表示されます。	iOS13 では、コールトラフィックとメッセージトラフィックは別々のプッシュ通知チャネルに分けられます。コールには「VoIP」チャネル、メッセージングには「Message」チャネルが使用されます。 音声コールまたはビデオ通話 標準の通信チャネルは使用できません。Unified CM は「VoIP」プッシュ通知チャネルを使用します。 VoIP 通知を受け取ると、Jabber は発信者 ID を使用して CallKit を起動します。 この動作は、Cisco Jabber または Cisco Webex iOS クライアントに適用されます。 メッセージング 標準の通信チャネルは使用できません。IM and Presence Service は、「Message」プッシュ通知チャネルを使用します。 1. IM and Presence サービスは、シスコ クラウドのプッシュ REST サービスに IM 通知を送信し、その後通知は Apple クラウドに転送されます。 2. Apple クラウドは、Cisco Jabber または Cisco Webex クライアントに IM 通知をプッシュします。 3. ユーザが通知をクリックすると、Cisco Jabber または Cisco Webex クライアントはフォアグラウンドモードに移行します。 Cisco Jabber または Cisco Webex クライアントは、IM and Presence Service とのセッションを再開し、メッセージをダウンロードします。 （注） Cisco Jabber または Cisco Webex クライアントがサスペンドモードの間、ユーザのプレゼンスは**「退席中」**と表示されます。

プッシュ通知がサポートされるクライアント

クライアント	OS	プラットフォームクラウド	クラウドサービス
iPhone および iPad の Cisco Jabber	iOS	Apple 社	Apple プッシュ通知サービス（APNS）
Android の Cisco Jabber	Android	Google	Android PNS サービス
iOS の Webex	iOS	Apple 社	Apple プッシュ通知サービス（APNS）
Android の Webex	Android	Google	Android PNS サービス

プッシュ通知の設定

プッシュ通知の設定および導入の方法の詳細は、『*iPhone* および *iPad* での *Cisco Jabber* のプッシュ通知の導入』（https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html）を参照してください。

第 II 部

ダイヤル プラン

第 18 章

パーティションの設定

パーティションの概要

パーティションは、次のいずれかの論理グループです。

- ルート パターン
- ボイス メールのディレクトリ番号（DN）
- トランスレーション パターン
- トランスフォーメーション パターン
- ユニバーサル リソース識別子（URI）
- ハント パイロット

パーティションによって組織、ロケーション、コール タイプを基にルート プランを論理サブセットに分割することで、コール ルーティングが容易になります。

コーリング サーチ スペースの概要

呼び出し先の検索スペース(CSS)は、パーティションの優先順位リストです。検索スペースの呼び出しによって、発信者がコールするために使用できるコール通知先が決定されます。コール先は、発信者の呼び出し用検索スペースで利用可能なパーティションに存在する必要があります。また、発信者はその通知先を呼び出すことができません。コール検索スペースは、ディレクトリ番号と、電話やゲートウェイなどのデバイスに割り当てることができます。

発信者の電話機と発信者のディレクトリ番号の両方に、検索スペースが割り当てられている場合、システムはその 2 つを連結して、発信者のための CSS を提供します。

コール権限に従って、パーティションを使用し、検索スペースを呼び出すことによってシステムを編成できます。 たとえば、次のようにすることができます。

- 一部の従業員が長距離通話に対応しないように制限する
- ロビー電話から CEO への直接コールの発信者を制限する

サービスクラス

パーティションを使用して、検索スペース (CSS) を呼び出して、サービスのクラスを設定することができます。 次の表に、PSTN アクセスを提供するサービスクラスのために作成できる、パーティションの例と、検索スペースの発信スペースを示します。

- 緊急コール
- ローカル コール
- ナショナル コール
- 国際ダイヤル

表 *14 :* パーティションとコーリング サーチ スペース

[コーリングサーチスペース(Calling Search Space)]	ルート パーティション 1	ルート パーティション 2	ルート パーティション 3	機能
ベース_CSS	Base_PT	—	—	• 緊急 (Emergency) • オンネット
ローカル PSTN_CSS	PSTN_ローカル_PT	—	—	• 緊急 (Emergency) • オンネット • ローカル
ナショナル PSTN_CSS	PSTN_ローカル_PT	PSTN_ナショナル_PT	—	• 緊急 (Emergency) • オンネット • ローカル • 国内

[コーリングサーチスペース(Calling Search Space)]	ルート パーティション 1	ルート パーティション 2	ルート パーティション 3	機能
インターナショナルPSTN_CSS	PSTN_ローカル_PT	PSTN_ナショナル_PT	PSTN_Intl_PT	• 緊急（Emergency） • オンネット • ローカル • 国内 • 国際

デバイスは、Base_CSS のようなコール対象の検索スペースに自動的に登録されます。 すべてのデバイスはオンネットと緊急オフネット番号の両方にダイヤルできるようになります。 残りのコール検索空間は、ローカル7ビットまたはローカル10ビット、国および国際ダイヤル機能を提供するために、ユーザ機器プロファイル上のディレクトリ番号に割り当てられなければなりません。

パーティション設定のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	パーティションの設定 （209 ページ）	パーティションを設定して、到達可能性の特徴が類似したシステム リソースの論理グループを作成します。
ステップ 2	コーリング サーチ スペースの設定 （211 ページ）	コーリング サーチ スペースは、コールを完了しようとする発信側デバイスが検索するパーティションを決定します。

パーティションの設定

パーティションを設定して、到達可能性の特徴が類似したシステム リソースの論理グループを作成します。 次のいずれに対してもパーティションを作成できます。

- ルート パターン
- ボイス メールのディレクトリ番号（DN）
- トランスレーション パターン
- トランスフォーメーション パターン

- ユニバーサル リソース識別子（URI）
- ハント パイロット

パーティションを作成することで、ルート プランが組織、場所、コール タイプに基づいた論理サブセットに分割されることになり、コール ルーティングが容易になります。 複数のパーティションを設定できます。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**コール ルーティング** > **コントロールのクラス** > **パーティション**。

ステップ 2 [新規追加（Add New）]をクリックして新しいパーティションを作成します。

ステップ 3 [パーティション名、説明（Partition Name, Description）]フィールドに、ルート プランに固有のパーティション名を入力します。

パーティション名には、英数字とスペースの他にハイフン（-）とアンダースコア（_）を使用できます。 パーティション名に関するガイドラインについては、オンライン ヘルプを参照してください。

ステップ 4 パーティション名の後にカンマ（,）を入力し、パーティションの説明を同じ行に入力します。

説明にはどの言語でも最大 50 文字まで指定できますが、二重引用符（"）、パーセント記号（%）、アンパサイド（&）、バックスラッシュ（\）、山カッコ（<>）、角括弧（[]）は使用できません。

説明を入力しなかった場合は、Cisco Unified Communications Manager が、このフィールドに自動的にパーティション名を入力します。

ステップ 5 複数のパーティションを作成するには、各パーティション エントリごとに 1 行を使います。

ステップ 6 [スケジュール（Time Schedule）] ドロップダウン リストから、このパーティションに関連付けるスケジュールを選択します。

スケジュールでは、パーティションが着信コールの受信に利用可能となる時間を指定します。[なし（None）]を選択した場合は、パーティションが常にアクティブになります。

ステップ 7 次のオプション ボタンのいずれかを選択して、[タイム ゾーン（Time Zone）]を設定します。

- [発信側デバイス（Originating Device）]：このオプション ボタンを選択すると、発信側デバイスのタイムゾーンと [スケジュール（Time Schedule）]が比較され、パーティションが着信コールの受信に使用できるかどうかが判断されます。
- [特定のタイム ゾーン（Specific Time Zone）]：このオプション ボタンを選択した後、ドロップダウン リストからタイム ゾーンを選択します。 選択されたタイム ゾーンと [スケジュール（Time Schedule）]が比較され、着信コールの受信にパーティションが使用できるかどうかが判断されます。

ステップ 8 **[保存]** をクリックします。

パーティション名のガイドライン

コーリング サーチ スペースのパーティションのリストは最大 1024 文字に制限されています。つまり、CSS 内のパーティションの最大数は、パーティション名の長さによって異なります。次の表を使用して、パーティション名が固定長である場合のコーリング サーチ スペースに追加できるパーティションの最大数を決定します。

表 *15*：パーティション名のガイドライン

パーティション名の長さ	パーティションの最大数
2 文字	340
3 文字	256
4 文字	204
5 文字	172
...	...
10 文字	92
15 文字	64

コーリング サーチ スペースの設定

コーリング サーチ スペースは、通常はデバイスに割り当てられるルート パーティションの番号付きリストです。 コーリング サーチ スペースでは、発信側デバイスが電話を終了しようとする際に検索できるパーティションが決定されます。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**コール ルーティング** > **コントロールのクラス** > **コーリングサーチスペース**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [名前（Name）]フィールドに、名前を入力します。

各コーリング サーチ スペース名がシステムに固有の名前であることを確認します。 この名前には、最長 50 文字の英数字を指定することができ、スペース、ピリオド（.）、ハイフン（-）、およびアンダースコア（_）を任意に組み合わせて含めることが可能です。

ステップ 4 [説明（Description）]フィールドに、説明を入力します。

説明には、どの言語でも最大 50 文字まで指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。

ステップ 5 [使用可能なパーティション（Available Partitions）]ドロップダウン リストから、次の手順のいずれかを実施します。

- パーティションが 1 つの場合は、そのパーティションを選択します。
- パーティションが複数ある場合は、**コントロール（Ctrl）**キーを押したまま、適切なパーティションを選択します。

ステップ 6 ボックス間にある下矢印を選択し、[選択されたパーティション（Selected Partitions）]フィールドにパーティションを移動させます。

ステップ 7 （任意） [選択されたパーティション（Selected Partitions）]ボックスの右側にある矢印キーを使用して、選択したパーティションの優先順位を変更します。

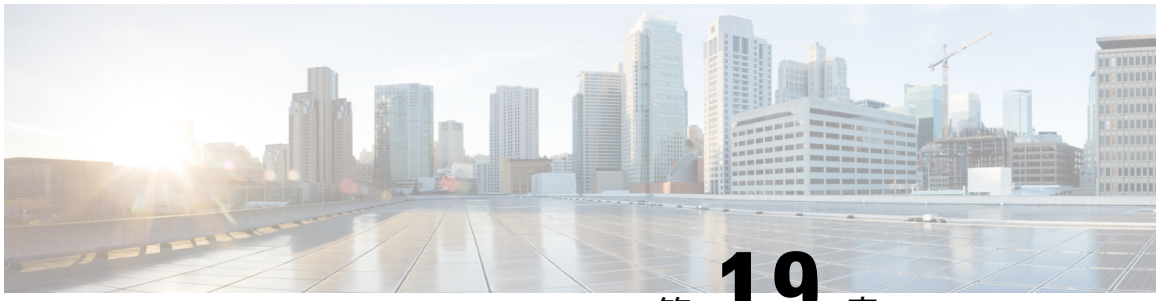
ステップ 8 **[保存]** をクリックします。

パーティションの連携動作と制限

表 *16 :* パーティション制限

機能またはアクション	制約事項
パーティションの削除	パーティションを削除する前に、次のいずれかのタスクを完了してください。 • コーリング サーチ スペース、デバイス、または削除するパーティションを使用しているその他の項目に異なるパーティションを割り当てる。 • コーリング サーチ スペース、デバイス、または削除するパーティションを使用しているその他の項目を削除する。 削除されたパーティションは取得できなくなるため、正しいパーティションを削除していることを慎重に確認してください。誤ってパーティションを削除した場合は、それを再構築する必要があります。
トランスレーション パターン	トランスレーション パターンにはディジット操作が含まれており、パーティションに割り当てられます。 コールがトランスレーション パターンと一致する場合、Unified CM が変換を実行し、そのトランスレーション パターンで指定されるコーリング サーチ スペースを使用してコールを再ルーティングします。 トランスレーション パターンの詳細については、「コール ルーティングの設定」の章を参照してください。
時間帯ルーティング	パーティションが着信コールを受け入れ可能なスケジュールを設定します。 ルーティングの時間設定の詳細については、「コール ルーティングの設定」の章を参照してください。

機能またはアクション	制約事項
論理パーティション設定	**任意**：ゲートウェイおよびトランク アクセスを使用して内部 VoIP ネットワークを外部ネットワークから分割できます。 ほとんどの導入環境では論理パーティションの使用は任意ですが、インドのように、内部ネットワークから外部へのコールをすべてローカル PSTN ゲートウェイに接続することが規制により必須となっている国では必須です。 論理パーティショニングの設定の詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』の「論理パーティション分割の設定」の項を参照してください。



第 19 章

国内の番号計画のインストール

国内番号計画の概要

Unified Communications Manager では、デフォルトで北米電話番号計画（NANP）を提供しています。設定されているダイヤル プラン要件が異なる国の場合は、シスコの国際ダイヤル プランをインストールし、それを使用して、要件特有の一意の番号計画を作成できます。

番号計画には、数字破棄命令（DDI）と、その番号計画に固有のタグが含まれています。これらの項目は、コールルーティングを設定するときに、番号計画に適したルーティングルールを作成するために使用できます。

この章では、国内番号計画をインストールする方法について説明します。国内番号計画の使用の詳細については、『*Unified Communications Manager* ダイヤルプラン導入ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

国内の番号付け計画の前提条件

北米から国外への国番号計画をインストールする場合は、現在のリリース用の国際ダイヤルプランが含まれている Cisco Option Package (COP) ファイルをダウンロードします。 COP ファイルでは、名前付けの規則 IDPv.x が使用されています。次のように、Cisco のウェブサイトから入手できます。

- https://software.cisco.com/download/navigator.html

このファイルを、Unified Communications Manager がアクセスできる外部 FTP サーバまたは SFTP サーバに配置します。

国内番号計画インストールのタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	COP ファイルのインストール （216 ページ）	（オプション） 北米以外の国の番号計画をインストールするには、現在のリリースの国際ダイヤルプランが含まれている Cisco Option Package (COP) ファイルをダウンロードします。
ステップ 2	国内の番号計画のインストール （217 ページ）	クラスタ内のそれぞれの Unified Communications Manager ノードに国内の番号計画をインストールします。 北米（システムデフォルト）以外の国における国内の番号計画をインストールしている場合にのみ、次の手順を実行します。
ステップ 3	CallManager サービスの再起動 （218 ページ）	変更は、サービスを再起動した後に有効になります。

COP ファイルのインストール

国際ダイヤル プランを含むシスコのオプション パッケージ（COP）ファイルをインストールするには、次の手順を実行します。

手順

ステップ 1 Unified Communications Manager のパブリッシャ ノードで、この手順を開始します。 Cisco Unified Communications OS 管理で、**[ソフトウェア アップグレード（Software Upgrades）] > I[インストール（nstall）]** を選択します。
[Software Installation/Upgrade]ウィンドウが表示されます。

ステップ 2 [ソース（Source）] フィールドで、[リモート ファイル システム（Remote File System）] を選択します。

ステップ 3 [ソフトウェアのインストール/アップグレード（Software Installation/Upgrade）]ウィンドウで、フィールドを設定します。 フィールドとその設定オプションの詳細については、「関連項目」を参照してください。

ステップ 4 [次へ（Next）]をクリックします。
ウィンドウが更新され、使用可能なソフトウェアのオプションとアップグレードのリストが表示されます。

ステップ 5 [オプション/アップグレード（Options/Upgrades）] ドロップダウンリストで、[DP COP] ファイルを選択して、[次へ（Next）] をクリックします。
[インストール ファイル（Installation File）] ウィンドウが開き、FTP サーバからファイルをダウンロードします。 ウィンドウにダウンロードの進捗が表示されます。

ステップ 6 [チェックサム（Checksum）] ウィンドウが表示されたら、そのチェックサムの値をダウンロードしたファイルのチェックサムの値と比較検証します。

ステップ 7 [次へ（Next）] をクリックして、ソフトウェア アップグレードに進みます。
警告メッセージとして、インストールするために選択した DP COP ファイルが表示されます。

ステップ 8 [インストール（Install）]をクリックします。
[インストール状況（Install Status）] ウィンドウが表示されます。

ステップ 9 [終了（Finish）]をクリックします。

ステップ 10 Unified Communications Manager サブスクライバ ノードで、この手順を繰り返します。 クラスタ内の全ノードに COP ファイルをインストールする必要があります。

関連トピック

COP ファイル インストールのフィールド （217 ページ）

COP ファイル インストールのフィールド

フィールド	説明
ディレクトリ（Directory）	COP ファイルが配置されているディレクトリを入力します。
[リモート サーバ（Remote Server）]	COP ファイルが配置されているサーバのホスト名または IP アドレスを入力します。
[リモート ユーザ（Remote User）]	リモート サーバのユーザ名を入力します。
[リモート パスワード（Remote Password）]	リモート サーバのパスワードを入力します。
[転送プロトコル（Transfer Protocol）]	リモート サーバと接続する場合に使用するプロトコルを選択します。

国内の番号計画のインストール

北米（システムデフォルト）以外の国における国内の番号計画をインストールしている場合にのみ、次の手順を実行します。

クラスタ内のそれぞれの Unified Communications Manager ノードに国内の番号計画をインストールします。 Unified Communications Manager publisher ノードから始めます。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[コールルーティング（Call Routing）]** > **[ダイヤルプランインストーラ（Dial Plan Installer）]** を選択します。

ステップ 2 検索条件を入力して **[検索（Find）]** をクリックします。

ステップ 3 インストールするダイヤル プランのバージョンを [利用可能なバージョン（Available Version）] ドロップダウンリストから選択します。

ステップ 4 [インストール（Install）]をクリックします。
ステータスに、ダイヤル プランがインストールされたことが表示されます。

ステップ 5 クラスターのサブスクライバ ノードごとにこの手順を繰り返します。

CallManager サービスの再起動

手順

ステップ 1 Cisco Unified Serviceability インターフェイスで、**[ツール（Tools）]** > **[コントロールセンター - 機能サービス（Control Center - Feature Services）]** を選択します。

ステップ 2 [サーバ（Servers）]ドロップダウンリストから、Cisco Unified Communications Manager サーバを選択します。
CM の [サービス（Services）] 領域で、[サービス名（Service Name）]列に Cisco CallManager が表示されます。

ステップ 3 Cisco CallManager サービスに対応するラジオ ボタンをクリックします。

ステップ 4 **再起動（Restart）**をクリックします。
サービスが再起動し、「サービスは正常に再起動しました（Service Successfully Restarted）」というメッセージが表示されます。

第 20 章

コール ルーティングの設定

コール ルーティングの概要

このシステムでは、クラスタ間でのコールのルーティング方法、およびプライベート ネットワークまたは公衆電話交換網（PSTN）に対する外部コールのルーティング方法を決定するために、ルート プランを使用します。 設定したルート プランにより、各コール タイプをルーティングするためにシステムが使用するパスが指定されます。 たとえば、オンネット コールに IP ネットワークを使用するルート プランや、ローカル PSTN コールと国際コールに別々のキャリアを使用するルート プランを作成できます。

トランスレーション パターン

変換パターンを設定して、任意のタイプのコールの数字を操作することができます。 トランスレーション パターンは、ルート パターンと同じ一般規則に従い、同じワイルドカードを使用します。 ルート パターンと同じように、トランスレーション パターンをパーティションに割り当てます。 ただし、ダイヤルされた数字がトランスレーション パターンと一致する場合、Unified CM は、ゲートウェイなどの外部エンティティにコールをルーティングしません。代わりに、まず変換を実行した後、トランスレーション パターン内で設定されたコーリング サーチ スペースを使用して、コールを再度ルーティングします。

（注） 選択したパーティション、ルートフィルタ、および番号計画の組み合わせを使用するトランスレーション パターンが固有であることを確認してください。 それには、ルート パターン/ハント パイロット、トランスレーション パターン、ディレクトリ番号、コール パーク番号、コール ピックアップ番号、またはミートミー番号の設定ウィンドウを確認して、重複するエントリがあることを示すエラーを受け取っていないかどうかを調べます。

トランスフォーメーション パターン

トランスフォーメーションパターンを使用すると、数字の破棄、プレフィックス番号の追加、発信側トランスフォーメーション マスクの追加を行えます。また、システムが電話機または PSTN にコールを送信する前に発信者番号の表示を制御することもできます。

トランスフォーメーションパターンを設定し、ルート パーティションに関連付けることによって、そのパーティションを含むコーリング サーチ スペースにパターンを割り当てます。 設定ウィンドウの [発信側トランスフォーメーションCSS（Calling Party Transformation CSS）] フィールドまたは [着信側トランスフォーメーションCSS（Called Party Transformation CSS）] フィールドを使用して、特定のデバイス、デバイス プール、ゲートウェイ、またはトランクのコール設定にパターンを割り当てることができます。

次のトランスフォーメーション パターンを設定できます。

- **発信側トランスフォーメーションパターン**：発信者番号のグローバル形式を、ゲートウェイまたはトランクなどのルート グループ デバイスに接続されているクラスタ外のネットワークで必要となるローカルの形式に適応させることができます。

  着信側トランスフォーメーションパターン：着信番号のグローバル形式を、ルート グループデバイスに接続されているクラスタ外のネットワークで必要となるローカル形式に適応させることができます。

ルート パターン

システムは、ルート プランに、次のコンポーネントを使用する 3 階層のアプローチを用います。

- **ルート パターン**：システムは、外部向けのダイヤル文字列と合致する設定済みのルート パターンを検索し、それを使用して、ゲートウェイまたはルート リストにコールを転送します。 ルート パターンは、ゲートウェイ、トランク、または 1 つ以上のルート グループを含むルート リストに割り当てることができます。
- **ルート リスト**：コールで使用可能なパスの優先順位付きリスト。
- **ルート グループ**：使用可能なパス。ルート グループは、ゲートウェイとトランクにコールを分配します。

追加のコール ルーティング

ルート プランには、次のオプションの要素も含めることができます。

- **ローカル ルート グループ**：複数のサイトがある場合は、ローカルのルート グループを使用して、ルートパターンの設定ではなくデバイス プールでの指定に従ってオフネット コールをゲートウェイにルーティングできます。 これにより、複数のロケーションに対して単一セットのルート パターンを使用できます。
- **ルートフィルタ**：ルート フィルタを作成してルート パターンまたはハント パイロットに追加することで、ユーザによるそのパターンの使用を制限できます。 ダイヤル プラン インストーラ ファイルを使用する場合は、ルート フィルターは必須ですが、手動でダイヤル プランを設定する場合は任意です。 手動設定の場合、ルート フィルタは、パターンで @ ワイルドカードを使用している場合にのみ適用されます。
- **自動代替ルーティング**：帯域幅不足のためシステムがコールをブロックしたときに、PSTN または別のネットワークを介してコールを自動的に再ルーティングします。
- **時間指定ルーティング**：特定のパーティションが着信コールを受信できる時間を指定するスケジュールを作成します。

コール ルーティングの前提条件

- パーティション設定のタスク フロー （209 ページ）の操作を実行します。
- 次の情報が用意されていることを確認してください。
  - 内部番号（内線）
  - 各ゲートウェイに転送されるコールをリストしているプラン

コールルーティングの計画の詳細については、『*Cisco Collaboration* システム ソリューション リファレンス ネットワーク デザイン』の「コール制御とルーティング」のトピックを参照してください。

コール ルーティング設定のタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	トランスレーション パターンの設定（223 ページ）	特定のパーティションでコールのディジット変換を実行する方法を指定するために、トランスレーションパターンを設定します。
ステップ 2	発信側トランスフォーメーション パターンの設定 （223 ページ）	このプロセスを使って呼び出し元の番号を変換します。 例えば、PSTNを呼び出したときに、発信者の内線番号を

	コマンドまたはアクション	目的
		オフィスのマスター番号で置き換える変換モードを設定することもできます。
ステップ 3	着信側トランスフォーメーション パターンの設定 （224 ページ）	この手順を使用して、着信側の番号を変換します。たとえば、10 桁の発信者の最後の 5 桁のみを保持するトランスフォーメーションパターンを設定できます。
ステップ 4	ローカル ルート グループの設定 （225 ページ）	（**オプション**）ローカル ルート グループを使用すると、複数のロケーションに対して 1 セットのルート パターンを使用できます。Unified CM は、ルート パターンではなく発信側デバイスのロケーションに基づいてゲートウェイを割り当てます。
ステップ 5	ルート グループの設定 （227 ページ）	（**オプション**）ゲートウェイのデバイスの選択順序を設定するようにルート グループを設定します。ルート グループには、1 つ以上のデバイスが含まれています。
ステップ 6	ルート リストの設定 （228 ページ）	（**オプション**）ルート リストには、1 つ以上のルート グループが含まれています。ルート グループの選択順序を制御するためにルート リストを設定します。
ステップ 7	ルート フィルタの設定 （229 ページ）	（**オプション**）ルート パターンが許可する特定の数字を制限するためにルーティングのフィルタを使用します。
ステップ 8	ルート パターンの設定 （233 ページ）	特定のデバイスにコールを導き、特定の数字パターンを含めるか排除するようにルート パターンを設定します。
ステップ 9	クラスタ全体の自動代替ルーティングの有効化 （238 ページ）	（**オプション**）自動代替ルーティング（AAR）を有効化すると、帯域幅不足のためにコールがブロックされたときに、システムは PSTN または別のネットワークを介してコールを再ルーティングします。

	コマンドまたはアクション	目的
ステップ 10	AAR グループの設定 （238 ページ）	（オプション）自動代替ルーティングに適用するディジット変換を含めて、AAR グループを設定します。
ステップ 11	日次ルーティングの時間の設定 （239 ページ）	（オプション）特定のパーティションが着信コールに応答可能な時間を指定するタイム スケジュールを作成します。

トランスレーション パターンの設定

ダイヤル文字列がパターンと一致したときに、コール番号と呼び出された番号に桁操作を適用するように変換パターンを設定します。 システムは数字の変換を完了してから、コールを再ルーティングします。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [トランスレーションパターン（Translation Pattern）]** を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- 新しいトランスレーション パターンを追加するには、[新規追加（Add New）]をクリックします。
- 既存のトランスレーション パターンを選択するには、[検索（Find）]をクリックします。

ステップ 3 [トランスレーションパターン（Translation Pattern）]フィールドに、このパターンを使用するダイヤル文字列と照合するパターンを入力します。

ステップ 4 [パーティション（Partition）]ドロップダウン リストから、このパターンを割り当てるパーティションを選択します。

ステップ 5 [トランスレーションパターンの設定（Translation Pattern Configuration）]ウィンドウで、残りのフィールドを入力します。 フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 6 **[保存]** をクリックします。

発信側トランスフォーメーション パターンの設定

このプロセスを使って呼び出し元の番号を変換します。 例えば、PSTNを呼び出したときに、発信者の内線番号をオフィスのマスター番号で置き換える変換モードを設定することもできます。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[Call Routing（コールルーティング）] > [トランスフォーメーション（Transformation）] > [トランスフォーメーションパターン（Transformation Pattern）] > [着信側トランスフォーメーション パターン（Calling Party Transformation Pattern）]**。

ステップ 2 次のいずれかのオプションを選択します。

- 新しい変換後のパターンを追加するには、**[新規追加（Add New）]** をクリックします。
- 既存のパターンを選択するには、[検索（Find）]をクリックします。

ステップ 3 [**パターン**（pattern）] フィールドで、発信者番号と一致させるパターンを入力します。

（注） **発信コールの場合**：

事前トランスフォーメーション発信側番号に基づいて、発信者のトランスフォーメーション マスクが選択されます。 （IP 電話に割り当てられた内線番号）。

SIP トランクで発信側トランスフォーメーションマスクを選択する間に、ルートパターンまたはグループで発信側番号が別の番号に変換された場合、発信側トランスフォーメーションマスクの選択には常に事前トランスフォーメーション発信側番号が使用されます。

Dialed Number Analyzer（DNA）に従っている限り、変換された番号を使用して発信側トランスフォーメーションマスクが選択されます。 ただし、これはDNAの動作としては正しくありません。

ステップ 4 [関係者の変換パターン**の設定**] ウィンドウで、残りのすべてのフィールドに入力します。 フィールドと設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 5 **[保存]** をクリックします。

着信側トランスフォーメーション パターンの設定

この手順を使用して、着信側の番号を変換します。 たとえば、10 桁の番号でダイヤルされたコールの最後の 5 桁のみを保持するトランスフォーメーション パターンを設定できます。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [トランスフォーメーション（Transformation）] > [トランスフォーメーションパターン（Transformation Pattern）] > [着信側トランスフォーメーション パターン（Called Party Transformation Pattern）]** を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- 新しい着信側トランスフォーメーション パターンを追加するには、[新規追加（Add New）] をクリックします。
- 既存のパターンを選択するには、[検索（Find）]をクリックします。

ステップ 3 [パターン（Pattern）]フィールドで、着信番号と一致させるパターンを入力します。

ステップ 4 **[着信側トランスフォーメーションパターンの設定（Called Party Transformation Pattern Configuration）]**ウィンドウで、残りのフィールドに入力します。 フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 5 **[保存]** をクリックします。

ローカル ルート グループの設定

（オプション） ローカル ルート グループを設定して、必要なルート リストの数を減らすことができます。 リストのポイントを、PSTN ゲートウェイのロケーションに基づいて、システムが発信をルーティングするのに使用する PSTN ゲートウェイにルーティングします。 代替として、ゲートウェイへのアクセスに使用されるルート パターンから PSTN ゲートウェイのロケーションを分離するためにローカル ルート グループを使用できます。 この設定により、異なるロケーションにある電話やその他のデバイスが単一セットのルート パターンを使用できますが、Cisco Unified Communications Manager が適切なゲートウェイを選択してコールをルーティングします。

たとえば、ローカル ルート グループを使用すると、国のすべての市で別々のダイヤル プランを持つのではなく、国全体で単一のダイヤル プランを持つことができます。 このアプローチが有効なのは、一元化されたコール導入のシナリオについてだけです。

手順

	コマンドまたはアクション	目的
ステップ 1	ローカル ルート グループの設定 （226 ページ）	**（オプション）** システムは、標準ローカル ルート グループと呼ばれるデフォルトのローカル ルート グループを提供しますが、追加のローカル ルート グループを設定できます。 追加のローカル ルート グループを指定するには、次の手順を使用します。
ステップ 2	ローカル ルート グループとデバイス プールの関連付け （226 ページ）	システムの各デバイスがそのローカル ルート グループを知るためにプロビジョニングされることを確認するためには、ローカル ルート グループをデバイス プールに関連付けます。
ステップ 3	ローカル ルート グループのルートリストへの追加 （227 ページ）	**（オプション）** ルート リストに追加できるローカル ルート グループを設定し

	コマンドまたはアクション	目的
		ます。 ローカル ルート グループを作成すると、システムはデバイス プール レベルのユーザに対して定義されたゲートウェイに発信コールをルーティングします。

ローカル ルート グループの設定

（**オプション**） システムは、標準ローカル ルート グループと呼ばれるデフォルトのローカル ルート グループを提供しますが、追加のローカル ルート グループを設定できます。 追加のローカル ルート グループを指定するには、次の手順を使用します。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートパターン（Route Pattern）]** を選択します。

ステップ 2 [行の追加（Add Row）]をクリックします。

ステップ 3 新しいローカル ルート グループの名前と説明を入力します。

ステップ 4 **[保存]** をクリックします。

ローカル ルート グループとデバイス プールの関連付け

発信側デバイスのデバイス プールの設定に基づいて、ローカル ルート グループが既存のルート グループを使用するよう割り当てることができます。 この設定により、異なるロケーションにある電話やその他のデバイスが単一セットのルートパターンを使用できますが、Unified Communications Manager が適切なゲートウェイを選択してコールをルーティングします。

システムの各デバイスがそのローカル ルート グループを知るためにプロビジョニングされることを確認するためには、ローカル ルート グループをデバイス プールに関連付けます。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [デバイスプール（Device Pool）]** を選択します。

ステップ 2 検索条件を入力し、[検索（Find）]をクリックして、結果のリストからデバイス プールを選択します。

ステップ 3 [ローカル ルート グループの設定（Local Route Group Settings）]領域で、[標準ローカル ルート グループ（Standard Local Route Group）]ドロップダウンリストからルート グループを選択します。

ステップ 4 **[保存]** をクリックします。

ローカル ルート グループのルートリストへの追加

ルート リストに追加できるローカル ルート グループを設定します。 ローカル ルート グループを作成すると、システムはデバイス プール レベルのユーザに対して定義されたゲートウェイに発信コールをルーティングします。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）]** > **[ルート/ハント（Route/Hunt）]** > **[ルートリスト（Route List）]** を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- [新規追加（Add New）]をクリックして、新しいルート リストを追加します。
- 既存のルート リストの設定を変更するには、[検索（Find）]をクリックし、結果のリストからルート リストを選択します。

[ルート リストの設定（Route List Configuration）]ウィンドウが表示されます。

ステップ 3 ルート リストにローカル ルート グループを追加するには、[ルート グループの追加（Add Route Group）]ボタンをクリックします。

ステップ 4 [ルートグループ（Route Group）]ドロップダウン リストから、ルート リストを追加するローカル ルート グループを選択します。 標準ローカル ルート グループの追加、または作成したカスタム ローカル ルート グループの追加ができます。

ステップ 5 **[保存]** をクリックします。

ステップ 6 **[設定の適用（Apply Config）]** をクリックします。

ルート グループの設定

システムが発信コール用ゲートウェイを選択するときの優先順位を示したルート グループを設定します。 グループ内の任意のゲートウェイでコールを発信できるように、同様の特性を持つゲートウェイをグループ化するには、次の手順を使用します。 ルート グループを設定したときに指定した順序で、システムは使用するゲートウェイを選択します。

1 つのデバイスを複数のルート グループに割り当てることができます。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）]** > **[ルート/ハント（Route/Hunt）]** > **[ルートグループ（Route Group）]** を選択します。

[ルートグループの設定（Route Group Configuration）]ウィンドウが表示されます。

ステップ 2 次のいずれかのオプションを選択します。

- 新しいルート グループを追加するには、[新規追加（Add New）]をクリックします。
- 既存のルート グループの設定を変更するには、[検索（Find）]をクリックし、結果のリストからルート グループを選択します。

[ルートグループの設定（Route Group Configuration）]ウィンドウが表示されます。

ステップ 3 [ルート グループの設定（Route Group Configuration）]ウィンドウで各フィールドを設定します。 フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 4 **[保存]** をクリックします。

ルート リストの設定

一連のルート グループを特定し、優先順位を付けるには、ルート リストを設定します。 Unified Communications Manager は、ルート リストの順序を使用して、発信コールに使用可能なデバイスを検索します。

ルート リストを設定すると、少なくとも 1 つのルート グループを設定する必要があります。ルート リストに含められるのは、ルート グループとローカル ルート グループだけです。

（注） 発信コールがルート リストを介して送信される場合、ルート リストのプロセスは、発信デバイスをロックして、コールが完了する前にアラートメッセージが送信されないようにします。発信デバイスがロックされた後は、ハント リストが着信コールの追跡を停止します。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）]** > **[ルート/ハント（Route/Hunt）]** > **[ルートリスト（Route List）]** を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- 新しいルート リストを作成するには、[新規追加（Add New）]をクリックします。
- 既存のルート リストの設定を変更するには、[検索（Find）]をクリックし、結果のリストからルート リストを選択します。

ステップ 3 [ルート リストの設定（Route List Configuration）]ウィンドウで各フィールドを設定します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 4 ルート グループをルート リストに追加するには、[ルートグループの追加（Add Route Group）]ボタンをクリックします。

ステップ 5 [ルート グループ（Route Group）]ドロップダウン リストから、ルート リストに追加するルート グループを選択します。

ステップ 6 **[保存]** をクリックします。

ステップ 7 **[設定の適用（Apply Config）]** をクリックします。

ルート フィルタの設定

ルート フィルタは、コールの処理方法を決定するためにダイヤル数字列を使用します。 ルート フィルタは、ワイルドカード @ を含むルート パターンを設定するときにのみ適用されます。 ルート パターンが @ ワイルドカードを含む場合、Unified Communications Manager は、この手順で指定する番号計画に従ってコールをルーティングします。

ダイヤル プラン インストーラを使用している場合、ルート フィルタは必須です。つまり、ダイヤル プラン ファイルをインストールして、その番号計画に基づいてルート パターンを設定します。 ダイヤル プランを手動で設定する場合は、ルート プランの使用は任意です。

ダイヤル プランを手動で設定すると、@ワイルドカードを含むルート パターンがあるたびにルート フィルタを設定する必要があります。 ルート パターンに@ワイルドカードが含まれていると、システムは、ルートフィルタで指定する番号計画に応じて、コールをルーティングします。

（注） コール ルーティングを設定するときは、1 つのルート フィルタを多数のルート パターンに割り当てないでください。 数百のルート パターンが関連付けられたルート フィルタを編集した場合、システム コアに発生します。 これは、ルート フィルタを使用するすべてのルート パターンのコール ルーティングの更新に新たなシステム処理が必要になるためです。 重複するルート フィルタを作成し、1 つのルート フィルタを 250 を超えるルート パターンに関連付けないようにします。

手順

ステップ 1 Cisco Unified CM Administration から、[コールルーティング（Call Routing）]>[ルートフィルタ（Route Filter）]を選択します。

ステップ 2 [番号計画（Numbering Plan）]ドロップダウン リストからダイヤル プランを選択し、[次へ（Next）]をクリックします。

ステップ 3 [ルート フィルタ名（Route Filter Name）]フィールドに名前を入力します。

各ルート フィルタ名がルート プランに一意であることを確認します。

ステップ 4 ルート フィルタのタグと演算子を選択し、データを入力して、このルート フィルタ用の句を作成します。

使用可能なルートフィルタのタグの詳細については、「ルートフィルタのタグ（230ページ）」を参照してください。

（注） EXISTS、DOES-NOT-EXIST、NOT-SELECTED の演算子を使用するタグにはルート フィルタのタグ値を入力しないでください。

ステップ 5 ルート フィルタの演算子を選択し、該当する場合は、このルート フィルタのフレーズを作成するためにデータを入力します。

使用可能なルート フィルタの演算子の詳細については、「ルート フィルタの演算子 （232 ページ）」を参照してください。

ステップ 6 **[保存]** をクリックします。

ステップ 7 **[設定の適用（Apply Config）]** をクリックします。

ルート フィルタの設定項目

ルートフィルタは、特定のルートがローカルのルートデータベースに含めるように考慮されていないプロセスです。 ルートパターンが設定されている場合にのみ適用されます。

ルートフィルタの設定に関する情報を次のトピックに示します。

ルート フィルタのタグ

タグは、ルート フィルタのコア コンポーネントです。 タグでは、ダイヤルされる数字列の一部に名前を適用しています。 たとえば、NANP 番号 972-555-1234 は、LOCAL-AREA-CODE (972)、OFFICE-CODE (555)、および SUBSCRIBER (1234) ルート フィルタ タグで構成されています。

ルート フィルタ タグには、演算子が必要であり、フィルタに掛けるコールを決定するには、その他の値も必要な場合があります。

ルート フィルタ タグ フィールドでの値には、ワイルドカード文字 X、*、#、[,]、-、^、および 0 ～ 9 の数値が使用できます。次の表の説明では、表記 [2-9] と XXXX を使用して実際の数字を表しています。 この表記では、[2 - 9] は 2 ～ 9 の範囲の任意の 1 桁の数字を表し、X は 0 ～ 9 の範囲の任意の 1 桁の数字を表します。したがって、「[2-9] XX の形式の 3 桁のエリア コード」という記述は、実際の数字 200 ～ 999、またはすべてのワイルドカード、または結果としてその範囲のパターンになる実際の数字とワイルドカードの任意の組み合わせを入力できるという意味です。

ルート フィルタ タグは、[ルートフィルタの設定(Route Filter Configuration)] ウィンドウの [番号計画(Numbering Plan)] ドロップダウン リスト ボックスで選択する番号計画によって異なります。 次の表に、北米計画番号のルート フィルタ タグを示します。

表 *17*：ルート フィルタのタグ

タグ	説明
AREA-CODE	[2-9]XX の形式のこの 3 桁のエリア コードは、長距離コールのエリア コードを指定します。
COUNTRY CODE	この 1 桁、2 桁、または 3 桁のコードは、国際コールの宛先国を指定します。
END-OF-DIALING	この 1 文字は、ダイヤルされた数字列の末尾を指定します。 NANP 内でダイヤルされる国際番号には、# 文字がダイヤル終了信号として使用されます。
INTERNATIONAL-ACCESS	この 2 桁のアクセス コードは、国際ダイヤルを指定します。 日本国内で発信するコールは、このコードに 01 を使用します。
INTERNATIONAL-DIRECT-DIAL	この 1 桁のコードは、直接ダイヤルされる国際コールを指定します。 日本国内で発信するコールは、このコードに 1 を使用します。
INTERNATIONAL-OPERATOR	この 1 桁のコードは、オペレータ経由の国際コールを指定します。 米国内で発信されるコールでは、このコードに 0 を指定します。
LOCAL-AREA-CODE	[2-9]XX の形式のこの 3 桁のローカル エリア コードは、10 桁のローカル コールのローカル エリア コードを指定します。
LOCAL-DIRECT-DIAL	この 1 桁のコードは、直接ダイヤルされるローカル コールを指定します。 NANP コールでは、このコードに 1 を使用します。
LOCAL-OPERATOR	この 1 桁のコードは、オペレータ経由のローカル コールを指定します。 NANP コールでは、このコードに 0 を使用します。
LONG-DISTANCE-DIRECT-DIAL	この 1 桁のコードは、直接ダイヤルされる長距離コールを指定します。 NANP コールでは、このコードに 1 を使用します。
LONG-DISTANCE-OPERATOR	この 1 桁または 2 桁のコードは、NANP 内のオペレータ経由の長距離コールを指定します。 オペレータ経由のコールでは、このコードに 0 を使用し、オペレータにアクセスするには 00 を使用します。
NATIONAL-NUMBER	このタグは、国際コール用の数字列の中の、各国固有の部分を指定します。
OFFICE-CODE	このタグは、7 桁のディレクトリ番号の最初の 3 桁（[2-9]XX の形式）を指定します。
SATELLITE-SERVICE	この 1 桁のコードは、国際コール用の衛星接続にアクセスできるようにします。
SERVICE	この 3 桁のコードは、緊急用の 911、修理サービス用の 611、問い合わせ用の 411 を指定します。

タグ	説明
SUBSCRIBER	このタグは、7 桁のディレクトリ番号の最後の 4 桁（XXXX の形式）を指定します。
TRANSIT-NETWORK	この 4 桁の値は、長距離通信事業者を識別します。 TRANSIT-NETWORK 値には、先行する 101 通信事業者アクセス コード接頭部を指定しないでください。 詳細については、TRANSIT-NETWORK-ESCAPE を参照してください。
TRANSIT-NETWORK-ESCAPE	この 3 桁の値は、長距離通信事業者 ID に先行します。 このフィールドの値には 101 が指定されています。TRANSIT-NETWORK-ESCAPE 値に、4 桁の通信事業者識別コードを指定しないでください。 詳細については、TRANSIT-NETWORK を参照してください。

ルート フィルタの演算子

ルート フィルタ タグの演算子は、そのタグに関連したダイヤル数字列の有無、さらに、場合によってはそのダイヤル数字列の内容に基づいて、コールがフィルタに掛けられるかどうかを決定します。 演算子 EXISTS および DOES-NOT-EXIST は、ダイヤル数字列のその部分が存在するかどうかだけをチェックします。 演算子 == は、実際にダイヤルされる数字を、指定された値またはパターンと突き合わせます。 次の表に、ルート フィルタ タグと共に使用できる演算子を示します。

表 *18* : ルート フィルタの演算子

演算子	説明
NOT-SELECTED	このタグに関連したダイヤル数字列に基づいて、コールをフィルタに掛けないことを指定します。 （注） 演算子が関連付けられるタグの有無によって、Cisco Unified Communications Manager がコールをルーティングすることが妨げられることはありません。
EXISTS	このタグに関連したダイヤル数字列が検出されたときに、コールをフィルタに掛けることを指定します。 （注） Cisco Unified Communications Manager は、タグに関連付けられている任意の数字シーケンスがダイヤル数字列に含まれる場合のみ、コールをルーティングするかブロックします。
DOES-NOT-EXIST	このタグに関連したダイヤル数字列が検出されないときに、コールをフィルタに掛けることを指定します。 （注） Cisco Unified Communications Manager は、タグに関連付けられている任意の数字シーケンスがダイヤル数字列に含まれない場合のみ、コールをルーティングするかブロックします。

演算子	説明
==	このタグに関連したダイヤル数字列が、指定された値と一致するときに、コールをフィルタに掛けることを指定します。 （注） Cisco Unified Communications Manager は、タグに関連付けられていて、関連するフィールドで指定された番号範囲内である任意の数字シーケンスがダイヤル数字列に含まれる場合のみ、コールをルーティングするかブロックします。

ルート フィルタの例

例 1：AREA-CODE と演算子 DOES-NOT-EXIST を使用するルート フィルタは、エリア コードを含まないすべてのダイヤル数字列を選択します。

例 2：AREA-CODE、演算子 ==、および項目 515 を使用するルート フィルタは、エリア コード 515 を含むすべてのダイヤル数字列を選択します。

例 3：AREA-CODE、演算子 ==、および項目 5[2-9]X を使用するルート フィルタは、520 ～ 599 の範囲のエリア コードを含むすべてのダイヤル数字列を選択します。

例 4：TRANSIT-NETWORK、演算子 ==、および項目 0288 を使用するルート フィルタは、通信事業者アクセス コード 1010288 を持つすべてのダイヤル数字列を選択します。

ルート パターンの設定

Unified Communications Manager は、ルート パターンを使用して、内部と外部のコールをルーティングまたはブロックします。 ゲートウェイ、トランク、1 つ以上のルート グループを含むルート リストにルート パターンを割り当てることができます。

（注） ルート パターンでゲートウェイを直接指定することもできますが、ルート リストおよびルート グループを設定することを推奨します。 このアプローチでは、コール ルーティングの柔軟性に加え、拡張性を最大限に発揮します。

手順

ステップ 1 Cisco Unified CM Administration から、**[コール ルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートパターン（Route Pattern）]** を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルート パターンを作成するには、[新規追加（Add New）]をクリックします。
- 既存のルート パターンを選択するには、[検索（Find）]をクリックします。

[ルートパターンの設定（Route Pattern Configuration）]ウィンドウが表示されます。

ステップ 3 [ルートパターン（ Route Pattern）]フィールドに、ダイヤル文字列が一致する必要がある番号パターンを入力します。

ステップ 4 [ゲートウェイ/ルート（Gateway/Route）]ドロップダウン リストから、このルート パターンに一致するコール送信先を選択します。

ステップ 5 [ルートパターンの設定（Route Pattern Configuration）]ウィンドウで、残りのフィールドを入力します。 フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 6 **[保存]** をクリックします。

ルート パターンの設定項目

ルート パターンは、数字列（アドレス）とルート リストへのコールまたはゲートウェイへのコールを指定する関連番号操作セットから構成されます。

設定するルートパターンの種類の例を以下に示します。

- ルート パターンのワイルドカードと特殊文字 （234 ページ）
- ドットの前の数字を削除する例 （237 ページ）
- プレフィックス番号の例 （237 ページ）
- オンネットパターンとオフネットパターンの例 （237 ページ）
- ブロックおよびルート パターンの例 （238 ページ）

ルート パターンのワイルドカードと特殊文字

ルートパターンにワイルドカードおよび特殊文字を使用すると、1 つのルートパターンで、ある電話番号（アドレス）の範囲を指定できます。 これらのワイルドカードと特殊文字を使用して、Unified Communications Manager が隣接システムに送信する前に番号を操作できるようにする指示も作成できます。

次の表に、Unified Communications Manager がサポートするワイルドカードと特殊文字を示します。

表 *19 :* ワイルドカードおよび特殊文字

文字	説明	例
@	@ 記号（@）ワイルドカードは、国別番号計画のすべての番号に一致します。 各ルート パターンで、@ ワイルドカードは 1 文字だけ使用できます。	ルート パターン 9.@ は、国別番号計画が認識するすべての電話番号をルーティングまたはブロックします。 @ ワイルドカードが含む、国別番号計画の番号のルート パターンの例を次に示します。 • 0 • 1411 • 19725551234 • 101028819725551234 • 01133123456789
X	X ワイルドカードは、0 ～ 9 の範囲にある数字の任意の 1 桁に一致します。	ルート パターン 9XXX は、9000 ～ 9999 の範囲のすべての数字をルーティングするか、またはブロックします。
!	感嘆符（!）ワイルドカードは、0 ～ 9 の範囲にある数字の 1 桁以上に一致します。	ルート パターン 91! は、910 ～ 919999999999999999999 の範囲のすべての数字をルーティングするか、またはブロックします。
?	疑問符（?）ワイルドカードは、直前の数字またはワイルドカード値の 0 回以上の繰り返しに一致します。 （注） 疑問符（??）ワイルドカードを使用した場合、2 つ目の疑問符は空の入力には一致しません。ルータパターンの例：*33X?*X?*X?#	ルート パターン 91X? は、91 ～ 919999999999999999999 の範囲のすべての数字をルーティングするか、またはブロックします。
+	プラス記号（+）ワイルドカードは、直前の数字またはワイルドカード値の 1 回以上の繰り返しに一致します。	ルート パターン 91X+ は、910 ～ 919999999999999999999 の範囲のすべての数字をルーティングするか、またはブロックします。

文字	説明	例
[ ]	角カッコ（[ ]）文字は、値の範囲を囲みます。	ルート パターン 813510[012345] は、8135100 ～ 8135105 の範囲のすべての数字をルーティングするか、またはブロックします。
-	ハイフン（-）文字は、角カッコと一緒に使用して値の範囲を示します。	ルート パターン 813510[0-5] は、8135100 ～ 8135105 の範囲のすべての数字をルーティングするか、またはブロックします。
^	ハット（^）文字は、角カッコと一緒に使用して値の範囲外を示します。 この文字は、開始角カッコ（[）の直後に配置してください。 各ルート パターンで、^ 文字は 1 文字だけ使用できます。	ルート パターン 813510[^0-5] は、8135106 ～ 8135109 の範囲のすべての数字をルーティングするか、またはブロックします。
.	デリミタとして使用されるドット（.）文字は、Cisco Unified Communications Manager のアクセス コードをディレクトリ番号から分離します。 この特殊文字を、桁を無視する指定と一緒に使用すると、隣接システムに番号を送信する前に Cisco Unified Communications Manager のアクセス コードを削除できます。 各ルート パターンで、（.）文字は 1 文字だけ使用できます。	ルート パターン 9.@ は、最初の 9 を、国別番号計画に発信する Cisco Unified Communications Manager アクセス コードとして認識します。
*	アスタリスク（*）文字は、特別な着信番号の追加の桁として利用できます。	ルート パターン *411 を設定して、内部オペレータのディレクトリ案内の利用を可能にします。
#	シャープ（#）文字は、一般にダイヤル シーケンスの終了を特定します。 #文字がパターンの最後の文字になるようにします。	ルート パターン 901181910555# は、国別番号計画内からダイヤルされる国際番号をルーティングまたはブロックします。 末尾の 5 の後の #文字は、この桁をシーケンスの最後の桁として特定します。

文字	説明	例
\+	\+ のように、バックスラッシュにプラス記号が続くと、国際番号用エスケープ文字 + の設定を示します。	\+ の使用は、国際番号用エスケープ文字 + がワイルドカードではなく、ダイヤル可能な桁であることを意味します。

ドットの前の数字を削除する例

ルートパターンでのドット単位の数字の削除を使用する1つの例は、電話機のユーザが外線に接続するためにアクセスコードをダイヤルする場合です。 北米では、通常、ユーザは9をダイヤルして外部回線にアクセスします。 次のルートパターンを使用して指定できます。

- 市内通話: **9. @**または **9.[2-9]XXXXXX**
- ナショナル コール: **9.1[2-9]XX**
- 国際 **9.011!#**

これらのパターンでは、9は外部回線のアクセスコードであり、ドット(.)は、ネットワークの内部の番号と外線番号を示すことによって、ルートパターンのフォーマットを支援する区切り文字です。 システムがダイヤルされた番号をPSTNに送信する場合は、[廃棄番号(Discard)]オプションを使用して、ダイヤルされた文字列からプレドットの数字を取り除くことにより、PSTNがコールをルーティングできるようにします。

プレフィックス番号の例

ルートパターンでの数字の接頭辞の使用の例としては、サイト間のオンネットダイヤルを設定する場合があります。 組織内のユーザが 8 + XXX-XXXX をダイヤルしてサイト間のコールにコールするように、ルートパターンを作成することができます。オフネットコールの場合は、コールを E.164 形式で PSTN にルーティングできるように、プレフィックス番号（8）を削除し、新しいプレフィックス 1<area code> を追加できます。

オンネットパターンとオフネットパターンの例

[分類の**発信 (Call 分類)**] フィールドを使用して、ルートパターンを Onnet または offnet として設定できます。 ユーザが2番目のダイヤルトーンを取得して、組織外にコールが転送されることを知らせたい場合は、コールをオフネットで分類できます。 たとえば、ユーザが外線にダイヤルする必要があるルートパターンを作成する場合、外部回線にアクセスしてオフネットパターンとして分類すると、システムは次のダイヤルトーンを提供します。

- 電話機がオフフックになっている場合のダイヤルトーン。ダイヤルした 9 の前。
- 2 番目のダイヤルトーンをダイヤルした後、そのダイヤル番号は、システムが公衆交換電話網 (PSTN) を呼び出す準備ができていることを示します。

Ensure that you deselect the **Allow Device Override** check box when you use this option.

ブロックおよびルート パターンの例

ブロックおよびルートのパターンを使用して、ルーティングされない発信または着信コールを禁止します。 ブロックパターンを

- 特定のパターンをブロックします。 たとえば、パターン 91900XXXXXXX をブロックすると、ユーザが 900 サービスにコールを配置するのを防ぐことができます。
- 特定の市外局番と場所へのコールをブロックすることによって、有料の詐欺を防止します。

クラスタ全体の自動代替ルーティングの有効化

クラスタに対して自動代替ルーティング（AAR）を有効化します。

手順

ステップ 1 Cisco Unified CM の管理から、**[システム（System）] > [サービス パラメータ（Service Parameters）]** の順に選択します。

ステップ 2 [サーバ（Server）]ドロップダウン リストでノードを選択します。

ステップ 3 [サービス（Service）]ドロップダウン リストから、[Cisco Call Manager] を選択します。

ステップ 4 [クラスタ全体のパラメータ（システム - CCM 自動代替ルーティング）（Clusterwide Parameters (System - CCM Automated Alternate Routing)）] 領域で、[自動代替ルーティングの有効化（Automated Alternate Routing Enable）]パラメータを [True]に設定します。

AAR グループの設定

自動代替ルーティング（AAR）を設定することで、ロケーションの帯域幅不足のためシステムがコールをブロックしたときに、PSTN またはその他のネットワークを通じてコールを自動的に再ルーティングすることができます。 AAR を使用すると、発信者は電話を切って着信側をダイヤルし直す必要がなくなります。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [AARグループ（AAR Group）]** を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- 新しい AAR グループを追加するには、[新規追加（Add New）]をクリックします。
- 既存の AAR グループの設定を変更するには、[検索（Find）]をクリックし、結果のリストから AAR グループを選択します。

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

ステップ 3 [名前（Name）]フィールドに、新しい AAR グループに割り当てる名前を入力します。

この名前には、最長 20 文字の英数字を指定でき、スペース、ピリオド（.）、ハイフン（-）、および下線文字（_）を任意に組み合わせることが可能です。

ウィンドウが更新され、その他のフィールドが表示されます。

ステップ 4 [AAR グループの設定（AAR Group Configuration）]ウィンドウの各フィールドを設定します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 5 **[保存]** をクリックします。

（注） **（オプション）** AAR がハント パイロットと連携できるようにするには、「ハント パイロットの設定タスク フロー （253 ページ）」を参照してください。

日次ルーティングの時間の設定

これはオプションです。 あるパーティションがいつ、着信コールの受信に利用可能かを指定するタイム スケジュールを作成します。

（注） ルーティングがメッセージ待機指示 (MWI) インターセプトに実装されていない。

手順

	コマンドまたはアクション	目的
ステップ 1	時間帯の設定 （240 ページ）	時間帯を定義するには、この手順を使用します。 開始時刻および終了時刻を定義し、さらに年次カレンダーで指定日または曜日として繰り返し間隔を指定します。
ステップ 2	タイム スケジュールの設定 （240 ページ）	スケジュールを作成するには、次の手順を実行します。 上記の手順で設定した時間帯は、このスケジュールの構成要素です。 時間帯は、複数のスケジュールに割り当てることができます。
ステップ 3	パーティションとスケジュールの関連付け （240 ページ）	特定の時間中にコールを完了しようとする場合、パーティションとスケジュールを関連付けてコーリング デバイスの検索が行われる場所を決定します。

時間帯の設定

時間帯を定義するには、この手順を使用します。 開始時刻および終了時刻を定義し、さらに年次カレンダーで指定日または曜日として繰り返し間隔を指定します。

手順

ステップ 1 Cisco Unified CM Administration から、**[コール ルーティング（Call Routing）]** > **[コントロールのクラス（Class of Control）]** > **[スケジュールの設定（Time Schedule）]** を選択します。

ステップ 2 [時間帯の設定（Time Period Configuration）]ウィンドウで各フィールドを設定します。 フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 3 **[保存]** をクリックします。

タイム スケジュールの設定

スケジュールを作成するには、次の手順を実行します。 上記の手順で設定した時間帯は、このスケジュールの構成要素です。 時間帯は、複数のスケジュールに割り当てることができます。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）]** > **[コントロールのクラス（Class of Control）]** > **[スケジュールの設定（Time Schedule）]** を選択します。

ステップ 2 [スケジュールの設定（Time Schedule）]ウィンドウのフィールドを設定します。 フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 3 **[保存]** をクリックします。

パーティションとスケジュールの関連付け

特定の時間中にコールを完了しようとする場合、パーティションとスケジュールを関連付けてコーリング デバイスの検索が行われる場所を決定します。

手順

ステップ 1 Cisco Unified CM Administration から、**[コール ルーティング（Call Routing）]** > **[コントロールのクラス（Class of Control）]** > **[パーティション（Partition）]** を選択します。

ステップ 2 [スケジュール（Time Schedule）]ドロップダウン リストから、このパーティションに関連付けるスケジュールを選択します。
スケジュールでは、パーティションが着信コールの受信に利用可能となる時間を指定します。 [なし（None）]を選択した場合は、パーティションが常にアクティブになります。

ステップ 3 **[保存]** をクリックします。

コールルーティングの制限

機能	制約事項
ルートフィルターの関連付け	コール ルーティングを設定する場合、単一ルート フィルタを多くのルート パターンに割り当てないようにしてください。 数百個のルート パターンが関連付けられているルートフィルタを編集しようとすると、システム コア クラッシュが発生する可能性があります。 これは、ルート フィルタを使用するすべてのルート パターンのコール ルーティングの更新に新たなシステム処理が必要になるためです。 発生しないようにするには、重複するルート フィルタを作成します。
外部コール制御	外部コール制御によって、アジャンクト ルート サーバは、Cisco Unified Routing Rules Interface を使用して Unified Communications Manager のコール ルーティングを決定できます。 外部コール制御を設定すると、Unified Communications Manager が、発信側および着信側の情報が入ったルート要求をアジャンクト ルート サーバに発行します。 そのサーバは、要求を受信し、適切なビジネス ロジックを適用し、コールのルーティング方法と適用すべきその他のコール処理方法をお使いのシステムに指示するルート応答を返します。 詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』の「外部コール制御」の章を参照してください。

機能	制約事項
コール制御検出	コール制御検出を使用すると、Service Advertisement Framework（SAF）と呼ばれる Cisco IOS サービス ルーティング プロトコルに登録することによって、Unified Communications Manager クラスタがホストする DN 範囲を自動的に交換できます。 SAF CCD によって、クラスタは、それぞれにホストされた DN 範囲をネットワークにアドバタイズし、ネットワーク内の他のコールエージェントによって生成されたアドバタイズメントにサブスクライブできます。 SAF CCD を使用することの主な利点は次のとおりです。 • 同じ SAF CCD ネットワークに参加するコール エージェント間でコール ルーティング情報を自動的に配布でき、したがって新しいコール エージェントが追加されたり、コール エージェントに新しい DN 範囲が追加されたりした場合に設定作業が徐々に増大することがなくなります。 • 集中型ダイヤル プラン解決コントロール ポイントに依存しなくなります。 • 複数の Unified CM クラスタが組み合わせられた場合を含め、ルーティングが変更された場合に、コール エージェント間のコール ルーティング情報が自動的に回復されます。 コール制御検出を設定するには、『*Cisco Unified Communications Manager* 機能設定ガイド』の「コール制御検出の設定」の章を参照してください。
ルート プラン レポート	詳細なルート プランは、Cisco Unified CM Administration（[コールルーティング（Call Routing）] > [ルートプランレポート（Route Plan Report）]）の [ルートプランレポート（Route Plan Report）] ウィンドウで表示できます。ルーティング計画の報告により、ルーティング計画の一部または全部のリストを確認し、レポートのモード/ディレクトリ番号、パーティションまたはルーティングの詳細情報列の項目をクリックして、直接に関連する設定ウィンドウに移動します。 さらに、ルート プラン レポートを使用してレポート データを .csv ファイルに保存し、そのファイルを他のアプリケーションにインポートすることもできます。 保存される .csv ファイルには、ウェブ ページより詳細な情報（電話機のディレクトリ番号、ルート パターン、パターン使用法、デバイス名、デバイスの説明など）が含まれます。

Dialed Number Analyzer によるトラブルシューティング

Dialed Number Analyzer は、Cisco Unified Communications Manager とともに、機能サービスの 1 つとしてインストールできます。このツールにより、Cisco Unified Communications Manager の

ダイヤルプラン設定を展開前にテストできます。また、このツールを使用して、展開後のダイヤル プランを分析することもできます。

ダイヤルプランが複雑になり、複数のデバイス、変換パターン、ルートパターン、ルートリスト、ルートグループ、発信側および着信側の変換、およびデバイスレベルの変換が関係すると、ダイヤル プランに誤りが含まれる場合があります。Dialed Number Analyzer を使用してダイヤルプランをテストするには、ダイヤルされた番号を入力に使用します。ダイヤルされた番号が分析され、コールの詳細が表示されます。その結果を使用してダイヤルプランを診断し、問題があれば特定し、ダイヤル プランを調整してから展開できます。

Dialed Number Analyzer のセットアップと使用の方法の詳細については、『*Cisco Unified Communications Manager Dialed Number Analyzer* ガイド』（https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

回線グループの設定

この章では、回線グループの追加または削除、または回線グループからの電話番号の追加または削除を行う方法について説明します。

詳細については、『*Cisco Unified Communications Manager* システム ガイド』の、ルート プランの理解に関するトピックを参照してください。

回線グループの設定の概要

Cisco Unified Communications Manager の管理ページで、**[コールルーティング(Call Routing)]** > **[ルート/ハント(Route/Hunt)]** > **[回線グループ(Line Group)]** メニュー パスを使用して、回線グループを設定します。

回線グループを使用して、電話番号を選択する順序を指定できます。 Cisco Unified Communications Manager は、コール分配アルゴリズムおよび RNA 復帰（RNAR）タイムアウト設定に基づいて、回線グループのアイドルまたは対応可能状態のメンバーに対して、コールを分配します。

（注） 回線グループに属する DN へのコールは、ダイレクト コール ピックアップ機能を使用してピックアップできません。

ヒント メンバー（ディレクトリ番号）を含まない空の回線グループを設定することは可能ですが、Cisco Unified Communications Manager では、この設定を使用してコールをルーティングすることはできません。回線グループにメンバーが含まれていない場合、空の回線グループにコールがルーティングされると、ハント リストはハントを停止します。 この状況を避けるため、回線グループには少なくとも 1 つのメンバーを必ず設定してください。

回線グループの設定のヒント

回線グループを設定する場合は、事前に少なくとも1つのディレクトリ番号を指定しておく必要があります。

回線グループを設定または更新した後で、その回線グループにメンバーを追加したり、回線グループからメンバーを削除したりできます。

回線グループの削除

1つ以上のルート/ハントリストが参照している回線グループを削除できます。 使用中の回線グループを削除しようとすると、Cisco Unified Communications Manager からエラー メッセージが表示されます。

ヒント 依存関係レコードは回線グループではサポートされていません。 ベストプラクティスとして、回線グループを削除する前に、必ず設定を確認してください。

回線グループの設定項目

フィールド	説明
[回線グループ情報(Line Group Information)]	
[回線グループ名(Line Group Name)]	この回線グループの名前を入力します。 この名前には、最長 50 文字の英数字を指定することができ、スペース、ピリオド（.）、ハイフン（-）、およびアンダースコア（_）を任意に組み合わせて使用することが可能です。 各回線グループ名が、そのルート プランに固有の名前であることを確認してください。 **ワンポイント アドバイス** 回線グループには、内容を簡潔に表す名前を使用してください。 通常、CompanynameLocationGroup の形式が、内容を簡潔に表し、回線グループをすばやくかつ簡単に識別できる方式です。 たとえば、「CiscoDallasAA1」は、Dallas にある Cisco オフィス用の Cisco Access Analog 回線グループを示します。
[RNA復帰タイムアウト（RNA Reversion Timeout）]	コールが応答されなかった場合はUnified Communications Managerがこの回線グループの次の使用可能なメンバーまたはアイドルメンバーに、次の回線グループにはコールを配信するまでの時間を秒単位で入力します。それから、ハントリストの次のグループを試して、選択されます。[RNA復帰タイムアウト(RNA Reversion Timeout)] は、回線グループ レベルで、すべてのメンバーに適用されます。

フィールド	説明
[分配アルゴリズム (Distribution Algorithm)]	ドロップダウン リスト ボックスで、回線グループ レベルで適用される次の分配アルゴリズムのオプションを選択します。 • [優先度順(Top Down)]：この分配アルゴリズムを選択すると、ライングループでアイドルまたは対応可能状態にある最初のメンバーから最後のメンバーまで、Unified Communications Manager がメンバーに対してコールを分配します。 • [循環方式（Circular）] - この配布アルゴリズムを選択した場合、Unified Communications Managerはルートグループの(n+1)番目のメンバーから始まるアイドルメンバーまたは使用可能なメンバーにコールを配布します。ここで、n番目のメンバーはアイドルまたはアイドルのいずれかです。忙しいが「ダウン」していません。 n番目のメンバーがルートグループの最後のメンバーである場合、Unified Communications Managerはそのルートグループの先頭からコールを配布します。 • 最長アイドル時間 - この分散アルゴリズムを選択した場合、Unified Communications Managerは回線グループの最長アイドルメンバーから最小アイドルメンバーまで、アイドルメンバーにのみコールを配布します。 • ブロードキャスト - この配布アルゴリズムを選択した場合、Unified Communications Managerは回線グループのすべてのアイドルまたは使用可能なメンバーに同時にコールを配布します。ブロードキャスト分配アルゴリズムを使用する場合のその他の制限事項については、[選択されたDN/ルートパーティション(Selected DN/Route Partition)] フィールドの説明にある注を参照してください。 デフォルト値は、[最長アイドル時間(Longest Idle Time)] です。
[ハントオプション(Hunt Options)]	

フィールド	説明
無応答	任意の分配アルゴリズムに対して、コールが応答しない回線グループのメンバーに配信される場合に使用するUnified Communications Managerのハントオプションを選択します。 このオプションは、メンバー レベルで適用されます。 ドロップダウン リスト ボックスから、次のオプションを選択します。 • [次のメンバへ、その後ハントリスト内の次のグループへ(Try next member; then, try next group in Hunt List)] - このハントオプションを選択した場合、Unified Communications Managerは回線グループの最初のアイドルまたは使用可能メンバーから最後のアイドルまたは使用可能メンバーまでコールをアイドルまたは使用可能メンバーに配布します。 分配に失敗した場合、Unified Communications Manager はハント リスト内の次の回線グループに対して分配を試行します。 • [次のメンバへ、ただし次のグループにはハントしない(Try next member, but do not go to next group)] - このハントオプションを選択した場合、Unified Communications Managerは回線グループの最初のアイドルメンバーまたは使用可能メンバーから最後のアイドルメンバーまたは使用可能メンバーにコールを割り当てます。 Unified Communications Managerは現在の回線グループの最後のメンバーに到達しようとするのをやめます。 • [残りのメンバにハントせず、すぐに次のグループへ(Skip remaining members, and go directly to next group)] - このハントオプションを選択した場合、最初のメンバーのRNA復帰タイムアウト値が経過したときに、Unified Communications Managerはこの回線グループの残りのメンバーをスキップします。その後、Unified Communications Managerはハントリスト内の次の行グループに直接進みます。 • [ハント中止(Stop hunting)] - このハントオプションを選択した場合、Unified Communications Managerはこの回線グループの最初のメンバーにコールを配信しようとした後にハントを停止し、メンバーはそのコールに応答しません。
無応答時のハント メンバーの自動ログアウト	このチェックボックスをオンにすると、回線のメンバーは、自動的にハント リストからログオフします。 回線メンバーを再度ログインさせるには、[HLOG] ソフトキーまたは PLK を使用します。

フィールド	説明
ビジー	任意の分配アルゴリズムに対して、通話が通話中の回線グループのメンバーに配信される場合に使用するUnified Communications Managerのハントオプションを選択します。 ドロップダウン リスト ボックスから、次のオプションを選択します。 • [次のメンバへ、その後ハントリスト内の次のグループへ(Try next member; then, try next group in Hunt List)] - このハントオプションを選択した場合、Unified Communications Managerは回線グループの最初のアイドルまたは使用可能メンバーから最後のアイドルまたは使用可能メンバーまでコールをアイドルまたは使用可能メンバーに配布します。 分配に失敗した場合、Unified Communications Manager はハント リスト内の次の回線グループに対して分配を試行します。 • [次のメンバへ、ただし次のグループにはハントしない(Try next member, but do not go to next group)] - このハントオプションを選択した場合、Unified Communications Managerは回線グループの最初のアイドルメンバーまたは使用可能メンバーから最後のアイドルメンバーまたは使用可能メンバーにコールを割り当てます。 Unified Communications Managerは現在の回線グループの最後のメンバーに到達しようとするのをやめます。 • [残りのメンバをスキップし、次のグループに直接進む(Skip remaining members, and go directly to next group)] - このハントオプションを選択した場合、Unified Communications Managerは話中メンバーに遭遇したときにこの回線グループの残りのメンバーをスキップします。 Unified Communications Managerは、ハントリストの次の行グループに直接進みます。 • [ハント中止(Stop hunting)] - このハントオプションを選択した場合、Unified Communications Managerはこの回線グループの最初のビジーメンバーにコールを配信しようとした後にハントを停止します。

フィールド	説明
なし	任意の分配アルゴリズムに対して、コールが使用できない回線グループのメンバーに配布される場合に使用するUnified Communications Managerのハントオプションを選択します。 [使用不可(Not Available)] 状態が発生するのは、該当する DN に関連付けられている電話機が、すべて未登録である場合です。 エクステンションモビリティが使用されていて、DN /ユーザがログインしていないときにも [使用不可(Not Available)] になります。ドロップダウンリストボックスのオプションから選択します。 • [次のメンバへ、その後ハントリスト内の次のグループへ(Try next member; then, try next group in Hunt List)] - このハントオプションを選択した場合、Unified Communications Managerは回線グループの最初のアイドルまたは使用可能メンバーから最後のアイドルまたは使用可能メンバーまでコールをアイドルまたは使用可能メンバーに配布します。 分配に失敗した場合、Unified Communications Manager はハント リスト内の次の回線グループに対して分配を試行します。 • [次のメンバへ、ただし次のグループにはハントしない(Try next member, but do not go to next group)] - このハントオプションを選択した場合、Unified Communications Managerは回線グループの最初のアイドルメンバーまたは使用可能メンバーから最後のアイドルメンバーまたは使用可能メンバーにコールを割り当てます。 Unified Communications Managerは現在の回線グループの最後のメンバーに到達しようとするのをやめます。 • [残りのメンバをスキップし、次のグループに直接進む(Skip remaining members, and go directly to next group)] - 残りのメンバーをスキップし、次のグループに直接移動する - このハントオプションを選択した場合、Unified Communications Managerは最初に使用不可のメンバーに遭遇したときにこの回線グループの残りのメンバーをスキップします。 Unified Communications Managerは、ハントリストの次の行グループに直接進みます。 • [ハント中止(Stop hunting)] - このハントオプションを選択した場合、Unified Communications Managerはこの回線グループの最初に使用不可のメンバにコールを配信しようとした後にハントを停止します。
[回線グループメンバ情報(Line Group Member Information)]	
[回線グループに追加する電話番号の検索(Find Directory Numbers to Add to Line Group)]	

フィールド	説明
パーティション	ドロップダウン リスト ボックスから、この回線グループのルート パーティションを選択します。 デフォルト値は <None> です。 [検索(Find)] をクリックすると、[使用可能DN/ルートパーティション(Available DN/Route Partition)] リスト ボックスに、選択されたパーティションに属する電話番号（DN）がすべて表示されます。
[次を含むディレクトリ番号(Directory Number Contains)]	検索するディレクトリ番号に含まれる文字を入力し、[検索(Find)] ボタンをクリックします。 入力した文字と一致するディレクトリ番号が [使用可能DN/ルートパーティション(Available DN/Route Partition)] ボックスに表示されます。
[使用可能DN/ルートパーティション(Available DN/Route Partition)]	[使用可能DN/ルートパーティション(Available DN/Route Partition)] リスト ボックスでディレクトリ番号を選択し、[回線グループに追加(Add to Line Group)] をクリックして、そのディレクトリ番号を [選択されたDN/ルートパーティション(Selected DN/Route Partition)] リスト ボックスに追加します。
[現在の回線グループメンバ(Current Line Group Members)]	
共有回線 DNs を使用したブロードキャストアルゴリズム	ディレクトリ番号の優先順位を変更するには、[選択されたDN/ルートパーティション(Selected DN/Route Partition)] リスト ボックス内のディレクトリ番号を選択します。 そのリスト ボックスの右側にある矢印をクリックして、リスト内でそのディレクトリ番号を上下に移動させてください。 [選択されたDN/ルートパーティション(Selected DN/Route Partition)] リスト ボックス内のディレクトリ番号の優先順位を逆転するには、[選択されたDN/ルートパーティションの順番を逆にする(Reverse Order of Selected DN/Route Partitions)] をクリックします。 （注） ブロードキャスト分配アルゴリズムを使用する回線グループに、共有回線であるDNを配置しないでください。 DNがブロードキャスト配信アルゴリズムを使用する回線グループのメンバーである場合、Unified Communications Manager は、そのDNがシェアドラインとして設定されているデバイス上のシェアドラインであるすべてのDNを表示できません。
[削除されたDN/ルートパーティション(Removed DN/Route Partition)]	[選択されたDN/ルートパーティション(Selected DN/Route Partition)] リスト ボックスでディレクトリ番号を選択し、そのディレクトリ番号を [削除されたDN/ルートパーティション(Removed DN/Route Partition)] リスト ボックスに追加します。これには、この2つのリストボックス間にある下矢印をクリックします。
ディレクトリ番号	

フィールド	説明
（この回線グループに属している DN のリスト）	所定のディレクトリ番号の [ディレクトリ番号の設定(Directory Number Configuration)] ウィンドウに移動するには、このリスト内のディレクトリ番号をクリックします。 （注） 新しい回線グループを追加する場合は、その回線グループを保存するまでこのリストは表示されません。

回線グループへのメンバーの追加

新しい回線グループまたは既存の回線グループにメンバーを追加できます。 次の手順では、既存の回線グループにメンバーを追加する方法を説明します。

始める前に

この手順を実行する前に、ディレクトリ番号を 1 つ以上定義しておく必要があります。

手順

ステップ 1 **[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [回線グループ（Line Group）]** を選択します。

ステップ 2 メンバーを追加する回線グループを見つけます。

ステップ 3 ディレクトリ番号を特定する必要がある場合は、[パーティション（Partition）] ドロップダウンリストボックスからルートパーティションを選択し、[次を含むディレクトリ番号（Directory Number Contains）] フィールドに検索文字列を入力して、[検索（Find）] をクリックします。 1つのパーティションに属するディレクトリ番号をすべて検索するには、[次を含むディレクトリ番号（Directory Number Contains）] フィールドを空白のままにして、[検索（Find）] をクリックします。

一致するディレクトリ番号のリストが [使用可能なDN/ルートパーティション(Available DN/Route Partition)] リストボックスに表示されます。

ステップ 4 [使用可能なDN/ルートパーティション（Available DN/Route Partition）] リスト ボックスで、追加するディレクトリ番号を選択し、[回線グループに追加（Add to Line Group）] をクリックして、そのディレクトリ番号を [選択されたDN/ルートパーティション（Selected DN/Route Partition）] リスト ボックスに移動します。 この回線グループに追加するメンバーごとに、この手順を繰り返します。

ステップ 5 [選択された DN/ルートパーティション (Selected DN/Route Partition)] リストボックスで、この回線グループで新しい電話番号にアクセスする順序を選択します。 順序を変更するには、ディレクトリ番号をクリックしてから、リストボックスの右側にある上向き矢印または下向き矢印を使用して、ディレクトリ番号の順序を変更します。

ステップ 6 [保存（Save）] をクリックすると、新しいディレクトリ番号が追加され、この回線グループのディレクトリ番号の順序が更新されます。

回線グループからのメンバーの削除

新しい回線グループから、または既存の回線グループからメンバーを削除できます。次の手順では、既存の回線グループからのディレクトリ番号の削除について説明します。

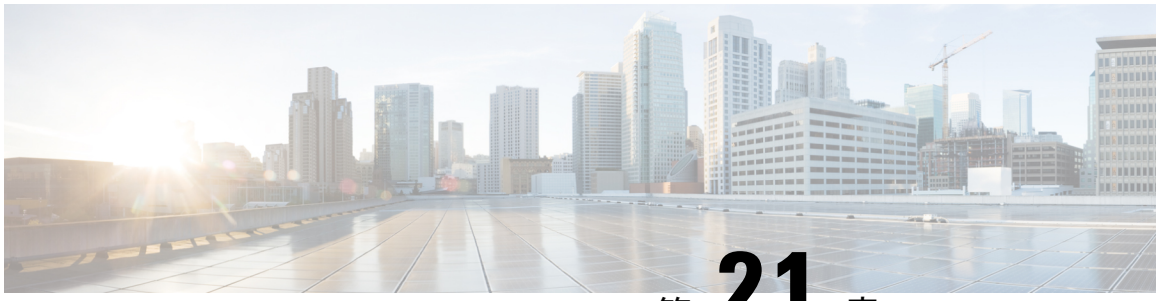
手順

ステップ 1 **[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [回線グループ（Line Group）]** を選択します。

ステップ 2 ディレクトリ番号を削除する回線グループを見つけます。

ステップ 3 [選択されたDN/ルートパーティション（Selected DN/Route Partition）] リスト ボックスで、削除するディレクトリ番号を選択し、リスト ボックスの下にある下向き矢印をクリックして、[削除されたDN/ルートパーティション（Removed DN/Route Partition）] リスト ボックスにそのディレクトリ番号を移動します。この回線グループから削除するメンバーごとに、この手順を繰り返します。

ステップ 4 メンバーを削除するには、[保存 (Save)] をクリックします。



第 21 章

ハント パイロットの設定

ハント パイロットの概要

ハントパイロットは、数値またはパターンと、回線グループ内の電話のグループまたはディレクトリ番号へのコールをルーティングできる関連付けられた一連のディジット操作で構成されています。

ハントパイロットは、着信コールの優先順位を付けられたパス(回線グループ)の優先順位リストを使用して、ハントリストと連携します。 ハントパイロットの DN にコールが発信されると、システムは、ハントリストで指定されている最初の回線グループにコールを提供します。最初の回線グループのいずれかの人がコールに応答しない場合、システムは、ハントリストで指定されている次の回線グループにコールを提供します。 回線グループは、グループ内の電話機にコールを配布する順序を制御します。 回線グループは、特定の内線番号（通常は、IP Phone 内線番号またはボイスメール ポート）を指しています。 回線グループは、コンピュータテレフォニー統合 (CTI) ポートと CTI ルートポイントをポイントできないので、ハントパイロットは、Cisco Customer Response Solution (CRS) や IP Interactive などの CTI アプリケーションによって制御されるエンドポイントにコールを配布することはできません。音声応答 (IP IVR)。

ハントパイロットは、自身の回線グループのメンバーとハントパイロットが別のパーティションに配置されている場合でも、コールを自身の回線グループのいずれかのメンバーに分配できます。 ハントパイロットが分配するコールは、すべてのパーティションおよびコーリング サーチ スペース制限を上書きします。

ハント パイロットの設定タスク フロー

これらのタスクを完了して、システムのハントパイロットを設定します。 ハントパイロットは、回線グループ内の複数の電話またはディレクトリ番号へのコールを経路指定するために使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	回線グループの設定 （254 ページ）	回線グループを作成して、複数の電話機が単一のディレクトリ番号 (DN) に送信されたコールに応答できるようにします。
ステップ 2	ハント リストの設定 （255 ページ）	回線グループの優先順位に従って、ハントリストを設定します。
ステップ 3	ハントパイロットの設定 （255ページ）	ハントパイロット番号またはシステムがハントリストへのコールを指示するために使用するパターンを設定します。

回線グループの設定

回線グループを使用すると、1 つのディレクトリ番号に送信されるコールに複数の電話で応答できます。 グループ内の電話に着信コールが分配される順序は、分配アルゴリズムが制御します。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [回線グループ（Line Group）]** を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- 新しい回線グループを作成するには、[新規追加（Add New）]をクリックします。
- 既存の回線グループを選択するには、[検索（Find）]をクリックします。

ステップ 3 [回線グループ名（Line Group Name）]を入力します。

ステップ 4 [分配アルゴリズム（Distribution Algorithm）]フィールドで、コールの分配に使用するアルゴリズムのタイプを選択します。

ステップ 5 回線グループにディレクトリ番号を追加するには、[回線グループに追加する回線グループメンバー（Line Group Members to Add to Line Group）]セクションのフィールドを設定します。

a) 追加するディレクトリ番号が存在する [パーティション（Partition）]を選択します。
b) これはオプションです。 [次を含むディレクトリ番号（Directory Number Contains）]フィールドを入力して、検索にフィルタを適用します。
c) **[検索（Find）]** をクリックします。 指定したパーティションからのディレクトリ番号のリストがボックスに表示されます。
d) [使用可能なDN/ルートパーティション（Available DN/Route Partition）]リストボックスで、グループに追加する個別のディレクトリ番号を選択し、[回線グループに追加（Add to Line Group）]をクリックします。

ステップ 6 [回線グループの設定（Line Group Configuration）]ウィンドウで、残りのフィールドを設定します。 フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 7 **[保存]** をクリックします。

ハント リストの設定

ハントリストは、回線グループの優先順位リストです。 ハントリストを介してコールをルーティングする場合、システムは、ハントリストで定義されている順序で回線グループを使用します。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）]** > **[ルート/ハント（Route/Hunt）]** > **[ハントリスト（Hunt List）]** を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- **[新規追加（Add New）]**をクリックして、新しいルート リストを作成します。
- 既存のリストを選択するには、[検索（Find）]をクリックします。

ステップ 3 ハントリスト**の**名前を入力します。

ステップ 4 ハント リストを登録する **Cisco Unified Communications Manager グループ**を選択します。

ステップ 5 [このハントリストを有効にする（Enable this Hunt List）]チェックボックスをオンにすると、[保存（Save）] をクリックしたときに即座にハント リストが有効になります。

ステップ 6 このハントリストをボイスメールに使用する場合は、**ボイスメール用**チェックボックスをオンにします。

ステップ 7 **[保存]** をクリックします。

ステップ 8 ハント リストへの回線グループの追加

a) **回線グループの追加** をクリックします。
b) **回線グループ**ドロップダウン リスト ボックスから、ハント リストに追加する回線グループを選択します。
c) **[保存]** をクリックします。
d) サイトを追加するには、これらの手順を繰り返します。

ハント パイロットの設定

回線グループに対してコールをルーティングするためにシステムが使用するハント パイロット番号またはパターンを設定します。

（注） ハント パイロットで使用できるワイルドカードと特殊文字の詳細については、「ハント パイロットのワイルドカードと特殊文字 （256 ページ）」を参照してください。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）]** > **[ルート/ハント（Route/Hunt）]** > **[ハントパイロット（Hunt Pilot）]** を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- 新しいハント パイロットを作成するには、[新規追加（Add New）]をクリックします。
- 既存のハント パイロットを選択するには、[検索（Find）]をクリックします。

ステップ 3 [ハントパイロット（Hunt Pilot）]フィールドに、コールのルーティングに使用する番号またはパターンを入力します。

ステップ 4 [ハントリスト（Hunt List）]ドロップダウンから、ハント パイロット番号に一致するコールを送信するためのハント リストを選択します。

ステップ 5 [ハントパイロットの設定（Hunt Pilot Configuration）]ウィンドウで、残りのフィールドに入力します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 6 コール キューイングを有効化する場合は、[コールをキューイング（Queue Calls）]チェックボックスをオンにし、[キューイング（Queuing）]セクションのフィールドを設定します。

ステップ 7 発信者、接続先、着信者に適用するディジット トランスフォーメーション パターンを割り当てます。

ステップ 8 **[保存]** をクリックします。

ハント パイロットのワイルドカードと特殊文字

ルート パターンおよびハント パイロットでワイルドカードおよび特殊文字を使用すると、単一ルート パターンまたはハント パイロットをある範囲の番号（アドレス）と一致させることができます。 また、これらのワイルドカードおよび特殊文字を使って指示を組み立てると、Cisco Unified Communications Manager が処理した番号を隣接システムに送信できます。

Cisco Unified Communications Manager がサポートするワイルドカードおよび特殊文字を次の表で説明します。

表 *20 :* ワイルドカードおよび特殊文字

文字	説明	例
@	@ 記号（@）ワイルドカードは、国別番号計画のすべての番号に一致します。 各ルート パターンで、@ ワイルドカードは 1 文字だけ使用できます。	ルート パターン 9.@ は、国別番号計画が認識するすべての電話番号をルーティングまたはブロックします。 @ ワイルドカードが含む、国別番号計画の番号のルート パターンの例を次に示します。 • 0 • 1411 • 19725551234 • 101028819725551234 • 01133123456789
X	X ワイルドカードは、0 ～ 9 の範囲にある数字の任意の 1 桁に一致します。	ルート パターン 9XXX は、9000 ～ 9999 の範囲のすべての数字をルーティングするか、またはブロックします。
!	感嘆符（!）ワイルドカードは、0 ～ 9 の範囲にある数字の 1 桁以上に一致します。	ルート パターン 91! は、910 ～ 919999999999999999999 の範囲のすべての数字をルーティングするか、またはブロックします。
?	疑問符（?）ワイルドカードは、直前の数字またはワイルドカード値の 0 回以上の繰り返しに一致します。 （注） 疑問符（??）ワイルドカードを使用した場合、2 つ目の疑問符は空の入力には一致しません。ルータパターンの例：*33X?*X?*X?#	ルート パターン 91X? は、91 ～ 919999999999999999999 の範囲のすべての数字をルーティングするか、またはブロックします。
+	プラス記号（+）ワイルドカードは、直前の数字またはワイルドカード値の 1 回以上の繰り返しに一致します。	ルート パターン 91X+ は、910 ～ 919999999999999999999 の範囲のすべての数字をルーティングするか、またはブロックします。

文字	説明	例
[ ]	角カッコ（[ ]）文字は、値の範囲を囲みます。	ルート パターン 813510[012345] は、8135100 ～ 8135105 の範囲のすべての数字をルーティングするか、またはブロックします。
-	ハイフン（-）文字は、角カッコと一緒に使用して値の範囲を示します。	ルート パターン 813510[0-5] は、8135100 ～ 8135105 の範囲のすべての数字をルーティングするか、またはブロックします。
^	ハット（^）文字は、角カッコと一緒に使用して値の範囲外を示します。 この文字は、開始角カッコ（[）の直後に配置してください。 各ルート パターンで、^ 文字は 1 文字だけ使用できます。	ルート パターン 813510[^0-5] は、8135106 ～ 8135109 の範囲のすべての数字をルーティングするか、またはブロックします。
.	デリミタとして使用されるドット（.）文字は、Cisco Unified Communications Manager のアクセス コードをディレクトリ番号から分離します。 この特殊文字を、桁を無視する指定と一緒に使用すると、隣接システムに番号を送信する前に Cisco Unified Communications Manager のアクセス コードを削除できます。 各ルート パターンで、（.）文字は 1 文字だけ使用できます。	ルート パターン 9.@ は、最初の 9 を、国別番号計画に発信する Cisco Unified Communications Manager アクセス コードとして認識します。
*	アスタリスク（*）文字は、特別な着信番号の追加の桁として利用できます。	ルート パターン *411 を設定して、内部オペレータのディレクトリ案内の利用を可能にします。
#	シャープ（#）文字は、一般にダイヤル シーケンスの終了を特定します。 #文字がパターンの最後の文字になるようにします。	ルート パターン 901181910555# は、国別番号計画内からダイヤルされる国際番号をルーティングまたはブロックします。 末尾の 5 の後の #文字は、この桁をシーケンスの最後の桁として特定します。

文字	説明	例
\+	\+ のように、バックスラッシュにプラス記号が続くと、国際番号用エスケープ文字 + の設定を示します。	\+ の使用は、国際番号用エスケープ文字 + がワイルドカードではなく、ダイヤル可能な桁であることを意味します。

ハント パイロットのパフォーマンスと拡張性

次のようなパフォーマンスおよび拡張性の制限が適用されます。

- 単一の Cisco Unified Communications Manager クラスタ は、最大で 15,000 個のハント リスト デバイスをサポートします。
- 単一の Cisco Unified Communications Manager サブスクライバは、ノードごとにコール キューイングが有効にされたハント パイロットを最大で 100 個サポートします。
- ハント リスト デバイスは、各ハント リストに 10 台の IP 電話を含む 1500 のハント リスト、各ハント リストに 20 台の IP 電話を含む 750 のハント リストの組み合わせ、または同様の組み合わせにすることができます。

（注） コール カバレッジにブロードキャスト アルゴリズムを使用する場合、ハント リスト デバイスの数は、Busy Hour Call Attempts（BHCA）の数によって制限されます。ブロードキャストアルゴリズムを使用して、10 台の電話機を含むハント リストまたはハント グループを指すハント パイロットに対して 10 回の BHCA を行うことは、10 回の BHCA を行う 10 台の電話機と同じです。

- ハントパイロットの最大数は、キューで許可されている 32 の発信者で設定されている場合、コールキューが有効になっている Unified CM サブスクライバノードごとに 100 です。ノードごとのキュースロットの総数（ノード上のすべてのコールキュー対応ハントパイロットの「キューで許可される発信者の最大数」の値）は 3200 に制限されます。各ハントパイロットのキューに同時に含める発信者の最大数は 100 です。つまり、ハントパイロットごとに 100 人の発信者がキューに入ることができ、ハントパイロットの最大数は 32 に減らされます。ただしコールキューが有効になっている場合は、すべてのハントリストのメンバーの最大数は変更されません。
- 設定できる各ハントパイロットのキュー内にある最大待ち時間は、0～3600 秒（デフォルトは 900）です。 ハント リストの数が増えると、Unified Communications Manager サービスパラメータで指定するダイヤルプラン初期化タイマーを増やす必要があります。 シスコでは、1500 個のハント リストを設定している場合、ダイヤルプラン初期化タイマーを 600 秒に設定することをお勧めします。
- コールキューを使用したブロードキャストアルゴリズムを使用する場合は、1 つの回線グループに対して 35 ディレクトリ番号が含まれないようにすることを推奨します。 また、ブロードキャスト回線グループの数は、BHCC によって決まります。 Unified CM システ

ム内に複数のブロードキャスト回線グループがある場合、回線グループ内の電話番号の最大数は 35 未満にする必要があります。すべてのブロードキャスト回線グループの最頻時発呼数（BHCA）が 1 秒あたり 35 コール設定を超えないようにします。

ハント パイロットの連携動作と制限

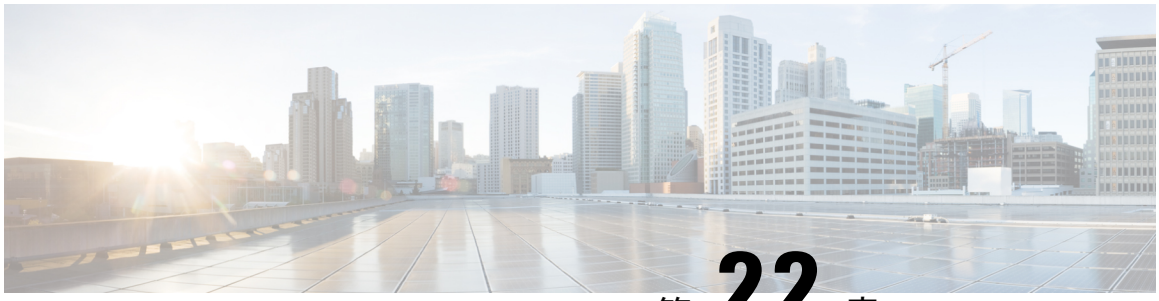
機能	連携動作と制限事項
ハント グループのシングル ナンバー リーチ	ハント グループが設定済みで、ハンド グループが指し示す 1 つ以上の電話番号でシングル ナンバー リーチ（SNR）が有効な場合には、ハント グループのすべてのデバイスがログインしない限り、SNR リモート接続先にコールが転送されません。 ハント グループ内の各デバイスについて、[電話の設定（Phone Configuration）]ウィンドウで [ハント グループにログイン（Logged into Hunt Group）]チェックボックスをオンにする必要があります。
コールキューイング	コールキューイングは、ハントパイロットのサブ機能です。 コールキューが有効になっていて、特定のハントパイロットに着信コールの要求がコールを応答するために使用可能なハントメンバーの数を超える場合、システムは、ハントメンバーが応答できるようになるまで着信コールをキューにキューに転送します。 待機中に発信者とその音楽を再生するように、保留中のアナウンスと音楽を設定することができます。 設定の詳細については、Cisco Unified Communications Manager 機能設定ガイドの「コール キューリングの設定」の章を参照してください。
Unified Mobility	ハント パイロットでの Unified Mobility デバイスの設定はお勧めしません。

配信されないコール

表 *21* : 循環アルゴリズムでコールが分配されない

制約事項	説明
BOT および TCT デバイスを含む回線グループの循環アルゴリズムで、コールが正しく配布されていません。	コールがログオフ状態にあるエージェントに拡張され、そのコールが **"Huntlogout"** タイプ以外の別の拒否タイプで拒否された場合。 次に、インデックスが 1 つ増加しないため、そのコールは前のコールに応答した同じエージェントに送られます。

制約事項	説明
回線グループの循環アルゴリズムで、コールが正しく配布されません。	循環アルゴリズムでコールを配布しているときに、エージェントが使用中の場合、そのコールは次に使用可能なエージェントに拡張されます (つまり、次のエージェントが、ビジー状態のエージェントの代わりにコールに応答します)。 （注） 複数のコールが同時に実行された場合、次に利用可能なエージェントがそのコールに応答します。



第 22 章

クラスタ間検索サービスの設定

ILS の概要

シスコ クラスタ間検索サービス（ILS）を使用すると、データを共有するリモート Cisco Unified Communications Manager クラスタで構成されるマルチクラスタ ネットワークを簡単に作成できます。

ILS を使用すると、管理者はクラスタ間の接続を手動で設定する必要がなくなります。 ハブ クラスタで ILS を設定済みであれば、新しいクラスタで ILS を有効化し、その新しいクラスタで既存のハブをポイントすることによって、新しいクラスタを接続できます。 ILS は、クラスタを自動的に接続し、両方のクラスタに大規模な ILS ネットワークのトポロジを知らせます。

ILS ネットワーク コンポーネント

ILS ネットワークは、次のコンポーネントで構成されます。

- **ハブ クラスタ**：ハブ クラスタは、自動メッシュ機能を使用して ILS ネットワークのバックボーンを形成し、他のハブ クラスタとのフル メッシュ トポロジを作成します。 ハブ クラスタは、多様な機能について、ILS ネットワーク全体で情報の中継と共有を実行します。
- **スポーク クラスタ**：スポーク クラスタはそれぞれのローカルのハブ クラスタにのみ接続し、他のハブ クラスタやスポーク クラスタに直接接続することはありません。 スポーク クラスタは、ネットワーク全体での情報の共有と中継については、それぞれのローカル ハブに依存します。
- **グローバル ダイヤル プランのインポートされたカタログ**：このオプションのコンポーネントは、グローバル ダイヤル プラン レプリケーションが設定されており、Cisco TelePresence Video Communications Server またはサードパーティのコール制御システムと相互運用している場合に適用されます。 他のシステムからエクスポートされた CSV ファイルからディレクトリ URI または +E.164 番号のカタログを手動でインポートすると、ILS ネットワーク内のユーザが別のシステムのユーザにコールできるようになります。

クラスタ ビュー

ILSのリモートクラスタビュー機能を使用して、ネットワークをマッピングすることができます。各クラスタは、ピア情報ベクターと呼ばれる更新メッセージを交換します。これは、ネットワーク内の各クラスタのステータスをリモートクラスタに通知するものです。更新メッセージには、ネットワーク内の既知のクラスタに関する次の情報が含まれます。

- クラスタ ID
- パブリッシャーのピア Id
- クラスタの説明とバージョン
- ホストの完全修飾ドメイン名（FQDN）を指定します。
- ILS がアクティブ化されているクラスタ ノードの IP アドレスとホスト名

機能のサポート

グローバル ダイヤル プラン レプリケーションおよびエクステンション モビリティ ローミングなどの機能は、クラスタがダイヤルプラン情報を共有するクラスタ間ネットワークの作成に関して、ILSに依存しています。それにより、ビデオ コール、URIダイヤリング、およびクラスタ間のモビリティを使用して、クラスタ間コール ネットワークをセットアップできます。

ILS は、IM and Presence の中央クラスタを複数のテレフォニー クラスタに接続している場合に、IM and Presence Service の集中型展開でも使用されます。ILS は、IM and Presence の中央クラスタおよびテレフォニー クラスタの間の接続を作成するのに使用されます。

ILS ネットワーキング キャパシティ

ILS ネットワークを計画する際に念頭に置くべき推奨キャパシティは以下のとおりです。

- ILS ネットワーキングは最大 10 個のハブ クラスタをサポートしており、ハブあたりのスポーク クラスタ数は 20 個であるため、合計で最大 200 個のクラスタを使用できます。ハブとスポークの組み合わせによるトポロジは、各クラスタ内で多数の TCP 接続が作成されるのを回避するために使用します。
- ハブ クラスタとスポーク クラスタを最大数まで、またはそれを超えて使用すると、パフォーマンスに影響が出る可能性があります。1 つのハブに多数のスポーク クラスタを追加すると余分な接続が作成され、メモリまたは CPU の処理量が増加する可能性があります。1 つのハブ クラスタに接続するスポーク クラスタは 20 個以下にすることを推奨します。
- ILS ネットワーキングは、追加の CPU 処理をシステムに追加します。CPU 使用率と同期時間は、クラスタ全体で同期されているレコードの数によって異なります。ハブアンドスポークトポロジを計画する場合は、ハブクラスタの CPU が負荷を処理するように設定されていることを確認します。

（注） これらの推奨事項は、システムテストに基づいており、リソース使用率を考慮しています。システムでは、これらの推奨事項を超えないようにすることはできませんが、リソースの過大な負荷にさらされるリスクがあります。最適なパフォーマンスを得るには、上記のキャパシティを推奨します。

ILS 設定のタスク フロー

ILS ネットワークをセットアップするには、この手順を実行します。

始める前に

どのクラスタをハブ クラスタにし、どのクラスタをスポーク クラスタにするのかを把握できるように、ILS トポロジを計画してください。

手順

	コマンドまたはアクション	目的
ステップ 1	クラスタ ID の設定 （265 ページ）	ILS ネットワーク内の各クラスタには、一意のクラスタ ID が必要です。
ステップ 2	ILS の設定 （266 ページ）	ネットワークのさまざまなクラスタで ILS を設定し、アクティブ化します。
ステップ 3	ILS の実行状態の確認 （267 ページ）	ILS ネットワークが実行中であることを確認します。
ステップ 4	リモート クラスタ ビューの設定 （268 ページ）	ILS ネットワークのリモート クラスタ ビューを設定します。

クラスタ ID の設定

ILS ネットワーク内の各クラスタには、一意のクラスタ ID が必要です。 リモート クラスタにクラスタ ID のデフォルトの **StandAloneCluster** 値が保持されている場合、ILS は機能しません。

手順

ステップ 1 パブリッシャ ノードで Cisco Unified CM 管理にログインします。

ステップ 2 **[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** を選択します。

ステップ 3 [クラスタID（Cluster ID）]の値を、クラスタを一意に識別する値に設定します。

ステップ 4 **[保存]** をクリックします。

ステップ 5 各クラスタのパブリッシャ ノードで、この手順を繰り返します。

ILS の設定

ネットワーク内のクラスタ間検索サービス（ILS）をアクティブ化して設定するには、この手順を実行します。

（注） 最初に設定するクラスタは、ハブ クラスタでなければなりません。

手順

ステップ 1 パブリッシャ ノードで Cisco Unified CM 管理にログインします。

ステップ 2 **[拡張機能（Advanced Features）]** > **[ILS設定（ILS Configuration）]** を選択します。

ステップ 3 [役割（Role）]ドロップダウン リスト ボックスから、設定するクラスタのタイプに応じて、[ハブクラスタ（Hub Cluster）]または [スポーククラスタ（Spoke Cluster）]を選択します。

ステップ 4 グローバル ダイヤル プラン レプリケーションを有効化する場合は、[リモートクラスタとグローバルダイヤルプランレプリケーションデータを交換（Exchange Global Dial Plan Replication Data with Remote Clusters）]チェックボックスをオンにします。

（注） URI パターン（`user@domain`）をアドバタイズするときは、[SIPプロファイルの設定（SIP Profile Configuration）]ウィンドウで、[ダイヤル文字列の解釈（Dial String Interpretation）]フィールドが [常にすべてのダイヤル文字列をURIアドレスとして処理（Always treat all dial strings as URI addresses）]に設定されていることを確認します。これは、デバイスがディレクトリ番号パターンとしてユーザセクションの数字のみを使用して URI 学習パターンにダイヤルするのを防ぐことが目的です。 その代わりに、ILS を介して、ユーザ セクションのテキスト文字列を使用して URI パターンのみをアドバタイズすることもできます。

ステップ 5 ネットワーク内のさまざまなクラスタ間で [ILS認証の詳細（ILS Authentication Details）]を設定します。

- TLS 認証の場合は、[TLS証明書の使用（Use TLS Certificates）]チェックボックスをオンにします。 このオプションを選択する場合、クラスタ内のノード間でCA 署名付き証明書も交換する必要があります。
- パスワード認証（TLS を使用するかどうかに関係なく）については、[パスワードの使用（Use Password）]チェックボックスをオンにして、パスワードの詳細を入力します。

ステップ 6 **[保存]** をクリックします。

ステップ 7 [ILSクラスタ登録（ILS Cluster Registration）]ポップアップで、登録の詳細を設定します。

a) [登録サーバ（Registration Server）]テキスト ボックスに、このクラスタに接続するハブ クラスタのパブリッシャ ノードの IP アドレスまたは FQDN を入力します。 これがネットワーク内の最初のハブ クラスタであれば、このフィールドを空白のままにしておくことができます。
b) [このクラスタにあるパブリッシャでクラスタ間検索サービスをアクティブ化（Activate the Intercluster Lookup Service on the publisher in this cluster）]チェックボックスがオンになっていることを確認します。
c) **OK**をクリックします。

ステップ 8 ILS ネットワークに追加する各クラスタのパブリッシャ ノードでこの手順を繰り返します。 新しいクラスタをハブ クラスタまたはスポーク クラスタとして追加します。

（注） 設定した同期値によっては、クラスタ情報がネットワーク全体に伝播する間に遅延が生じることがあります。

クラスタ間で Transport Layer Security（TLS）認証を使用するには、ILS ネットワークの各クラスタのパブリッシャ ノード間で、Tomcat 証明書を交換する必要があります。 Cisco Unified オペレーティング システムの管理から、証明書の一括管理機能を使用して、以下を行います。

- 証明書を各クラスタのパブリッシャ ノードから中央の場所にエクスポートします
- エクスポートされた証明書を ILS ネットワークに統合します
- ネットワークの各クラスタのパブリッシャ ノードに証明書をインポートします

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』の「Manage Certificates」の章を参照してください。

ILS の実行状態の確認

ILS ネットワークが実行中であることを確認します。

手順

ステップ 1 任意のテレフォニー クラスタでパブリッシャ ノードにログインします。
ステップ 2 Cisco Unified CM の管理から、**[詳細機能（Advanced Features）]** > **[ILS設定（ILS Configuration）]** を選択します。
ステップ 3 [ILSクラスタとグローバルダイヤルプランインポート済みカタログ（ILS Clusters and Global Dial Plan Imported Catalogs）]セクションをオンにします。 ILS ネットワーク トポロジが表示されます。

リモート クラスタ ビューの設定

ILS ネットワークのリモート クラスタ ビューを設定するには、この手順を使用します。

手順

ステップ 1 Cisco Unified CM Administration で、**[高度な機能（Advanced Features）] > [クラスタビュー（Cluster View）]** を選択します。

ステップ 2 [リモート**クラスタの検索と一覧**表示] ウィンドウで、以前作成したリモートクラスタを選択します。

ステップ 3 [リモート クラスタ サービスの設定（Remote Cluster Service Configuration）] ウィンドウから、リモート クラスタの Extension Mobility Cross Cluster、TFTP、RSVP エージェントなどのサービスを設定するには、該当するチェックボックスをオンにします。

ステップ 4 **[保存]** をクリックします。

ILS の連携動作および制限

ILS の連携動作

表 *22 : ILS* の連携動作

機能	データのやり取り
クラスタの検出	ILS のクラスタ検出を使用すると、管理者がそれらのクラスタ間の接続を手動で設定しなくても Cisco Unified Communications Manager はリモート クラスタの詳細を動的に学習できます。 ILS ネットワークの各クラスタは更新メッセージをやり取りします。これはピア情報ベクターと呼ばれ、ネットワーク内の各クラスタのステータスをリモートクラスタに知らせることを目的としています。 更新メッセージには、ネットワーク内の既知のクラスタに関する次の情報が含まれます。 • クラスタ ID • クラスタの説明とバージョン • ホストの完全修飾ドメイン名 • ILS がアクティブ化されているクラスタ ノードの IP アドレスとホスト名 **[詳細機能（Advanced Features）] > [クラスタビュー（Cluster View）]** を選択すると、ILS クラスタ検出機能が Cisco Unified CM Administration で表示できるリモート クラスタのリストを自動的に読み込みます。 このウィンドウから、リモート クラスタの Extension Mobility Cross Cluster、TFTP、RSVP エージェントなどのサービスを設定できます。 （注） [クラスタビュー（Cluster View）] に表示されるリモート クラスタの完全修飾ドメイン名には、ILS 検出で解決可能な DNS を指定する必要があります。
グローバル ダイヤル プラン レプリケーション	ILS ネットワークでグローバル ダイヤル プラン レプリケーションが有効な場合、ILS ネットワーク内のリモート クラスタは次のデータを含め、グローバル ダイヤル プラン データを共有します。 • ディレクトリURI • 代替番号 • 代替番号パターン • ルート文字列 • PSTN フェールオーバー番号

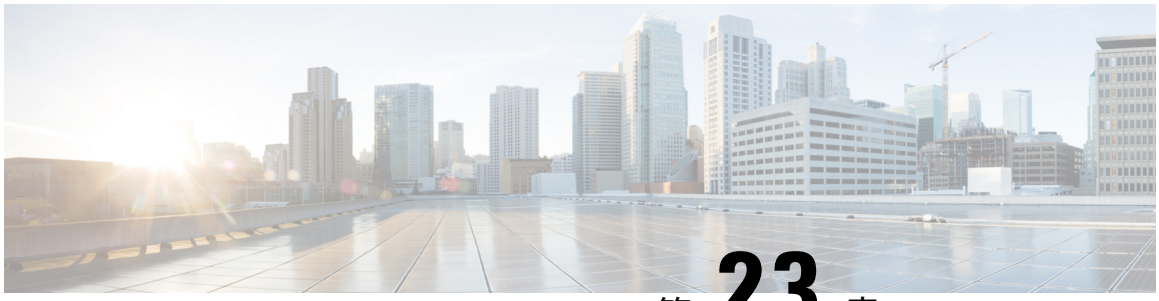
機能	データのやり取り
着信コール	ILS ベースのネットワークで、発信者番号に基づいて着信コールをブロックするには、SIP ルートパターンのパーティションを発信者の CSS に含める必要があります。 たとえば、コールが SIP トランクから発信される場合、SIP トランク受信 CSS には sip ルートパターンのパーティションが含まれている必要があります。

ILS の制限

表 *23 : ILS* の制限

制約事項	説明
ILS サービス	ILS サービスは、Unified Communications Manager のパブリッシャ ノードでのみ動作します。
クラスタ	ハブ クラスタは複数のスポークを持つことができますが、スポーク クラスタは 1 つのハブ クラスタしか持つことができません。
ILS ネットワーク	サードパーティ コール制御システムを ILS ネットワークに接続することはできません。
クラスタインポート	サードパーティのカタログは、ハブ クラスタにのみインポートできます。
重複した URI	取得した ILS クラスタに、別のリモートクラスタからの重複した Uri が含まれている場合、その URI にコールが配置されると、その uri が取得されてデータベースに挿入されているクラスタにルーティングされます。
データベースの複製ステータス	グローバルダイヤルプランデータは ILS ネットワーク上で正常に交換されますが、ILS 受信クラスタはデータベースレプリケーションステータスを完了するまで、学習した情報をデータベースに書き込みません。
インポート	インポートされたサードパーティディレクトリ Uri およびパターンの場合、[管理ウィンドウ] サンプルファイルに示されているように、CSV ファイル形式は正確なシンタックスに一致する必要があります。それ以外の場合、インポートは失敗します。

制約事項	説明
ILS ハブ	ILS ネットワークに追加のハブクラスタを追加するときは、プライマリ ILS ハブノードで、次の条件が満たされていることを確認します。 • クラスタ ID は、ILS クラスタ内のすべてのハブノードで一意です。 • 完全修飾ドメイン名（FQDN） • UDS と EM サービスは、ILS クラスタ内のすべてのハブノードで実行されています • DNS プライマリおよびリバース解決は正常に動作しています。 • すべてのハブノードから統合 Tomcat 証明書をインポートします。 あるいは、クラスタのリブートまたはエラーの修正後も [**検索とリストリモートクラスタ**] ウィンドウに「バージョン」情報が表示されることはありません。 この回避策は、ILS ネットワークからハブクラスタを削除し、上記の要件に従って、ハブクラスタを ILS ネットワークに再追加することです。



第 23 章

グローバル ダイヤル プラン レプリケーションの設定

グローバル ダイヤル プラン複製の概要

グローバル ダイヤル プラン レプリケーションを使用すると、URI ダイヤリング、エンタープライズ番号、またはE.164番号のいずれかをダイヤリングに使用するビデオ コールによって、クラスタ間 VoIP ネットワークを簡単にセットアップできます。

グローバル ダイヤル プラン レプリケーションでは、ILS ネットワーク内のリモート クラスタにグローバル ダイヤル プランのデータ要素を複製することで、シスコ クラスタ間検索サービスを活用します。 ILS ネットワーク内の各クラスタは、ホーム クラスタのルート文字列と共に、他のクラスタのグローバル ダイヤル プラン要素を学習します。

ILS 経由のグローバルなアドバタイズ

グローバル ダイヤル プラン レプリケーションでは、次のダイヤル プラン要素を ILS ネットワークにアドバタイズし、このデータをリモート クラスタに複製します。

- **ディレクトリ URI**：ローカル クラスタで、電子メール形式のディレクトリ URI（alice@cisco.com など）をプロビジョニングします。 URI ダイヤリングは、ユーザ中心型のコール発信手段を提供します。 グローバル ダイヤル プラン レプリケーションでは、ディレクトリ URI のローカル カタログを ILS ネットワーク内の他のクラスタにアドバタイズすることで、クラスタ間 URI ダイヤリングが可能になります。
- **エンタープライズ番号および E.164 代替番号**：代替番号は、付加番号命令を含むマスクを元のディレクトリ番号に適用することで作成される、元の内線番号のエイリアスです。 代替番号は、ILS ネットワーク内のどこからでもダイヤルできます。 代替番号には 2 つのタイプがあります。 ローカル クラスタで代替番号をプロビジョニングしてから各番号を ILS

ネットワークにアドバタイズするか、代替番号の範囲を要約するアドバタイズされた番号パターンを設定して、そのパターンをILSネットワークにアドバタイズすることができます。

- **アドバタイズされたパターン**：アドバタイズされたパターンは、エンタープライズ代替番号またはE.164代替番号の範囲を要約したものです。 個別の代替番号ではなくパターンをILSネットワーク全体に複製することで、リモートクラスタのデータベース領域を節約できます。アドバタイズされたパターンは、ILSネットワーク内のリモートクラスタでのみ使用されます。これらのパターンをローカル コールのルーティングに使用することはできません。

- **PSTN フェールオーバー番号**：このオプションを使用すると、エンタープライズ代替番号またはE.164 代替番号を PSTN フェールオーバー番号として割り当てることができます。VoIP チャネル経由でのグローバル ダイヤル プラン要素へのコール ルーティングが失敗した場合、フェールオーバー番号によって代替のルーティング方法が提供されます。 リモートクラスタで、適切なゲートウェイにPSTNフェールオーバーをルーティングするルートパターンを設定する必要があります。

- **ルート文字列**：各クラスタには、グローバル ダイヤル プラン カタログと共に複製されるルート文字列があります。 ルート文字列は、ディレクトリ URI または代替番号のホームクラスタを識別するものです。 クラスタ間のコール処理では、ルート文字列をホーム クラスタにルーティングするSIPルートパターンを各リモートクラスタで設定する必要があります。

- **学習されたグローバル ダイヤル プラン データ**：複製されたデータを ILS ネットワーク内のすべてのクラスタに確実に到達させるためには、各クラスタで、他のクラスタから学習したカタログと共に、ローカルでプロビジョニングされたグローバルダイヤルプランデータを複製します。

- **インポートされたグローバル ダイヤル プラン データ**：Cisco Unified Communications Manager を Cisco TelePresence Video Communications Server またはサードパーティのコール制御システムと相互運用する場合は、相手のシステムからグローバルダイヤルプランデータをcsvファイルにエクスポートし、そのcsvファイルをILSネットワーク内のハブ クラスタにインポートします。 グローバル ダイヤル プラン レプリケーションによって、インポートされたカタログがILSネットワーク内の他のクラスタに複製され、相手のシステムに登録されているディレクトリ URI および代替番号にコールを発信できるようになります。

グローバル ダイヤル プランのマッピング例

次の例は、電話の内線番号4001にマップされるグローバル ダイヤルプラン データ要素を示しています。コールルーティングが正しく設定されている場合、これらのいずれかの番号をダイヤルすると内線番号 4001 が呼び出されます。

- エンタープライズ代替番号：番号マスク 5XXXX が内線 4001 に適用され、エンタープライズ代替番号 54001 が作成されます。

- E.164 代替番号：番号マスク 1972555XXXX が内線 4001 に適用され、+E.164 代替番号 19725554001 が作成されます。

- PSTN フェールオーバー：エンタープライズ代替番号または+E.164 代替番号を PSTN フェールオーバーとして割り当て、適切なゲートウェイにコールをルーティングします。
- アドバタイズされたパターン：パターン 54XXX を使用して、54000 ～ 54999 の範囲のすべてのエンタープライズ代替番号を要約できます。 エンタープライズ代替番号と +E.164 代替番号用にパターンを作成できます。
- ディレクトリ URU：alice@cisco.com

（注） ディレクトリ URI は、ディレクトリ番号またはエンドユーザに割り当てることができます。 エンド ユーザに関連付けられているディレクトリ URI はユーザのプライマリ内線番号（ディレクトリ番号）にも関連付けられ、プライマリ内線番号が割り当てられている場合はその内線番号を呼び出します。

URI ダイヤル

URI ダイヤリングはグローバル ダイヤル プラン レプリケーションのサブ機能であり、発信者がディレクトリ URI をダイヤル文字列として使用してコールを発信できるようにします。ディレクトリ URI は、電子メール アドレスに似た英数字の文字列です（例：alice@cisco.com）。

URI は電子メール アドレスと似ていますが、ディレクトリ URI は、単独でルーティング可能なエンティティではありません。 ローカル コールの場合、ディレクトリ URI が発信者のコーリング サーチ スペース内のパーティションにある場合に限り、そのディレクトリ URI に対するコールをルーティングできます。 クラスタ間コールの場合、システムは、グローバル ダイヤル プラン レプリケーションにより複製されたクラスタ ルート文字列を取得し、SIP ルート パターンとルート文字列の照合を試みます。

ディレクトリ URI のタイプ

ディレクトリ URI には 2 つのタイプがあり、ディレクトリ URI のプロビジョニング方法によってタイプが決まります。

- ユーザベースの URI：このディレクトリ URI は、[エンドユーザの設定（End User Configuration）]でユーザに割り当てます。 これらの URI はすべて、ローカルのディレクトリ URI パーティションに自動的に割り当てられます。これは、ローカルにある削除できないパーティションです。ユーザにプライマリ内線番号も設定されている場合、URI はその内線番号のプライマリ URI として [ディレクトリ番号の設定（Directory Number Configuration）]にも表示されます。
- 回線ベースの URI：[ディレクトリ番号の設定（Directory Number Configuration）]ウィンドウで、1 つのディレクトリ番号に最大 5 個のディレクトリ URI を直接割り当てることができます。 これらの URI には、任意のローカル パーティションを割り当てることができます。

ディレクトリ URI 形式

ディレクトリ URI は、@ 記号で区切られたユーザとホスト アドレスで構成される英数字の文字列です。

Cisco Unified Communications Manager は、次の形式のディレクトリ URI をサポートします。

- user@domain（例：joe@cisco.com）
- user@ip_address（例：joe@10.10.10.1）

システムはディレクトリ URI のユーザ部分（@ 記号の前の部分）では次の形式をサポートします。

- 使用可能な文字は、a-z、A-Z、0-9、!、$、%、&、*、_、+、~、-、=、\、?、‘、,、.、/、( ) です。
- ユーザ部分の最大長は 47 文字です。
- ディレクトリ URI がデータベースに保存されている場合、Cisco Unified Communications Manager は、次の文字にパーセント エンコーディングを自動的に適用します。

  # % ^ ` { } | \ : ” < > [ ] \ ‘ およびスペース。

（注） デフォルトでは、ディレクトリ URI のユーザ部分で大文字と小文字が区別されます。 [URI検索ポリシー（URI Lookup Policy）]エンタープライズ パラメータを編集することで、ユーザの部分で大文字と小文字を区別しないように編集できます。

パーセントエンコーディングを適用すると、ディレクトリ URI の桁数が増えます。たとえば、ディレクトリ URI として「joe smith#@cisco.com」（20 文字）を入力した場合、Unified Communications Manager は、このディレクトリ URI を「joe%20smith%23@cisco.com」（24 文字）としてデータベースに保存します。 データベースの制限により、[ディレクトリURI（Directory URI）]フィールドの最大長は 254 文字となります。

Cisco Unified Communications Manager は、ディレクトリ URI のホスト部分（@ 記号の後の部分）に関して次の形式をサポートします。

- IPv4 アドレスまたは完全修飾ドメイン名がサポートされます。
- 使用可能な文字は、英数字、ハイフン（-）、ドット（.）です。
- ホスト部分をハイフン（-）で開始または終了することはできません。
- ホスト部分に、連続した 2 つのドットを含めることはできません。
- ホスト部分の最短の長さは 2 文字です。
- ホスト部分では、大文字と小文字は区別されません。

（注） **Cisco Unified Communications Manager Administration** で、一括管理を使用して、二重引用符とカンマが埋め込まれたディレクトリ URI を含む CSV ファイルをインポートする場合は、ディレクトリ URI 全体を二重引用符（"）で囲む必要があります。

URI への通話転送

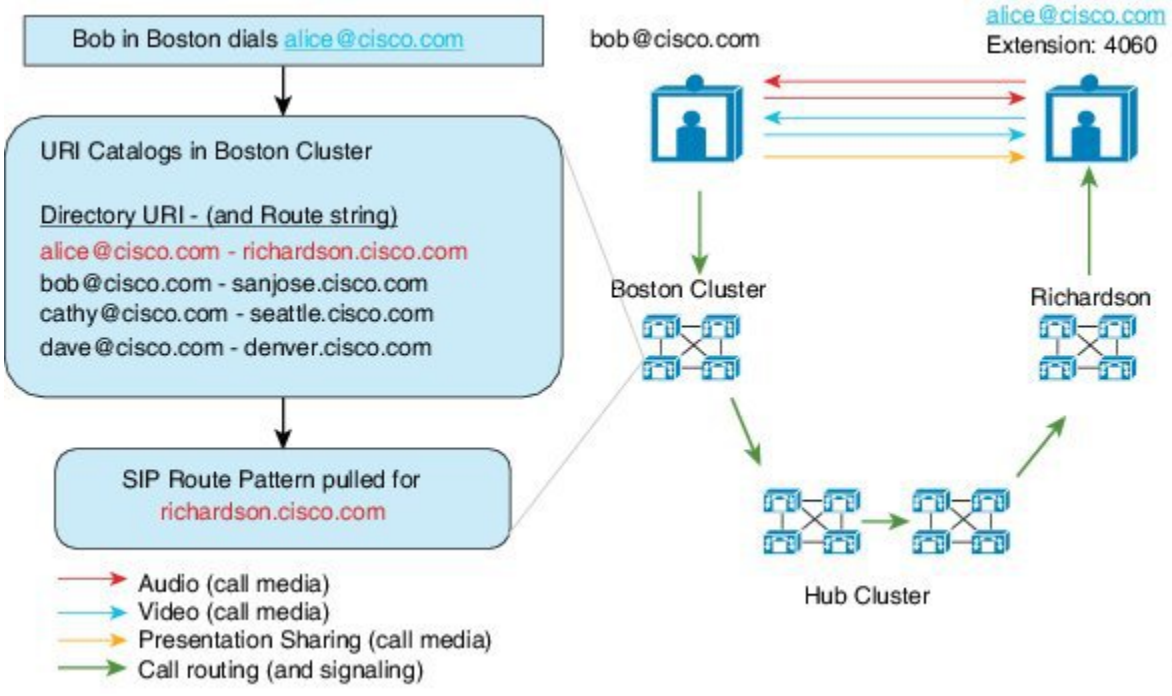
- URI への通話転送は、物理的な電話からは実行できません。
- URI への通話転送は、その URI がすでに Unified Communications Manager データベース内にある場合にのみアプリケーションを介して設定できます。 URI がデータベース内にない場合、通話転送を設定しようとしているときに、アプリケーションから「通話転送の設定に失敗しました/n新しい番号への通話転送に失敗しました（Call Forward Setting Failed /n Failed to forward calls to）」というエラーが返されます。
- 通話転送は、URI がデータベース内に存在するかどうかに関係なく Unified Communications Manager の管理ページですべての URI に対して設定できます。
- 通話転送は、データベース内に存在するかどうかに関係なく、**[Cisco Unified Communications セルフケアポータル（Cisco Unified Communications Self Care Portal）]** > **[エンドユーザ（End User）]** ページですべての URI に対して設定できます。 文字 **# % ^ ` { } | \ : ? < >[ ] \‘** を入力するときは、「パーセントエンコーディング」を使用する必要があります。 たとえば、**%3A** は**:** をメンションするために使用され、**%20** は、スペースをメンションするために使用されます。
- 通話を URI「mobile: 12345@cisco.com」に転送する必要がある場合は、**[Cisco Unified Communications セルフケアポータル（Cisco Unified Communications Self Care Portal）]** > **[エンドユーザ（End User）]** ページの [通話転送（Call-Forward）] セクションで「**mobile%3A%2012345@cisco.com**」を指定する必要があります。

グローバル ダイヤル プラン レプリケーションのコール ルーティング

クラスタ内のコールでは、グローバル ダイヤル プラン データはパーティションとコーリング サーチ スペースを介してルーティングされます。 ローカル ディレクトリ URI、エンタープライズ代替番号、または E.164 代替番号に対するコールが動作するためには、発信側で使用しているコーリング サーチ スペースにその URI または番号が存在する必要があります。

クラスタ間のコールでは、グローバル ダイヤル プラン レプリケーションがアドバタイズするクラスタ ルート文字列を使用して、着信側のホーム クラスタにコールが送信されます。 別のクラスタに所属しているディレクトリ URI または代替番号に対して発信者がコールを発信すると、システムは、関連付けられたルート文字列を取得し、ルート文字列の SIP ルート パターンと照合して、SIP ルート パターンで指定されている宛先にそのコールを送信します。 これが機能するためには、ルート文字列をそのホーム クラスタにルーティングするように、リモート クラスタの SIP ルート パターンを設定する必要があります。

コールルーティングに失敗した場合は、システムは、関連付けられたPSTNフェールオーバー番号を使用することもできます。 ただし、PSTN フェールオーバーのコールを適切なゲートウェイに送信できるように、リモートクラスタのルートパターンを設定する必要があります。



グローバル ダイヤル プラン複製の前提条件

次の作業が必要です。

- シスコ クラスタ間検索サービス（ILS）の設定
- グローバル ダイヤル プランをどのように展開するかを計画します。
  - ユーザ用のディレクトリURIをプロビジョニングすることによって、URIダイヤリングを展開する場合、 グローバル ダイヤル プラン レプリケーションを使用して、ILSネットワーク全体にディレクトリ URI を複製できます。
  - 代替番号ダイヤリングを展開する場合、エンタープライズ代替番号とE.164代替番号のどちらをを使用しますか。 PSTNフェールオーバーとしてどちらを使用しますか。
  - 代替番号を展開する場合は、番号計画を策定します。 大規模なネットワークでは、個々の代替番号ではなく番号パターンをILSネットワークにアドバタイズすることで、データベースの領域と帯域幅を節約できます。

グローバル ダイヤル プラン レプリケーションの設定タスク フロー

グローバル ダイヤル プラン レプリケーションと URI ダイヤリングを設定するには、この手順を実行します。 これらのタスクは、ILS ネットワークの各クラスタで実行する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	グローバル ダイヤル プラン複製に対する ILS サポートの有効化 （280 ページ）	ローカル クラスタでグローバル ダイヤル プラン レプリケーションのサポートを有効化します。
ステップ 2	SIP プロファイルの設定 （281 ページ）	グローバル ダイヤル プラン レプリケーションと URI ダイヤリングをサポートする SIP 設定項目を指定します。
ステップ 3	URI ダイヤリング用の SIP トランクの設定 （281 ページ）	URI ダイヤリングについては、システムが連絡先ヘッダーにディレクトリ URI、ディレクトリ番号、または混合アドレスを挿入するかどうかを設定します。
ステップ 4	SIP ルート パターンの設定 （282 ページ）	クラスタ間ルーティングについては、学習されたルート文字列をそれぞれのホーム クラスタにルーティングする SIP ルート パターンを各クラスタで設定します。
ステップ 5	学習されたデータに対するデータベース制限の設定 （283 ページ）	ILS がローカル データベースに書き込むことができるデータ量の上限を設定します。
ステップ 6	学習番号とパターンのパーティションの設定 （284 ページ）	エンタープライズ代替番号、+E.164 代替番号、および学習された番号パターンのルート パーティションを割り当てます。
ステップ 7	代替番号のアドバタイズ パターンの設定 （285 ページ）	これはオプションです。エンタープライズ代替番号または +E.164 代替番号の範囲を要約する番号パターンをアドバタイズします。

	コマンドまたはアクション	目的
ステップ 8	学習したパターンのブロック （285 ページ）	これはオプションです。特定の番号または番号パターンに対するコールをブロックするパターンを設定します。この設定はローカルで適用され、ILS ネットワークには複製されません。
ステップ 9	グローバル ダイヤル プランのデータをインポート （288 ページ）	これはオプションです。 Cisco TelePresence Video Communication Server またはサードパーティのコール制御システムと相互運用する場合は、そのシステムから ILS ネットワーク内のハブ クラスタに、ディレクトリ URI、+E.164 番号、および PSTN フェールオーバー番号のカタログをインポートします。
ステップ 10	グローバル ダイヤル プラン データのプロビジョニング （286 ページ）	ディレクトリ URI、エンタープライズ代替番号、または +E.164 代替番号を、ディレクトリ番号に割り当てます。 （注） 複数ユーザの場合は、LDAP ディレクトリ同期または一括管理を使用して、多数のユーザのグローバル ダイヤル プラン データを 1 回の操作で割り当てることができます。このガイドの「ユーザのプロビジョニング」のセクションを参照してください。

グローバル ダイヤル プラン複製に対する ILS サポートの有効化

ローカル クラスタのグローバル ダイヤル プラン レプリケーションの ILS サポートを有効にするには、次の手順に従います。

手順

ステップ 1 Cisco Unified Communications Manager のパブリッシャ ノードにログインします。

ステップ 2 Cisco Unified CM の管理から、**[詳細機能（Advanced Features）] > [ILS 設定（ILS Configuration）]** を選択します。

ステップ 3 [リモートクラスタとのグローバルダイヤルプランのレプリケーションデータの交換（Exchange Global Dial Plan Replication Data with Remote Clusters）]チェックボックスをオンにします。

ステップ 4 [アドバタイズルート文字列（Advertised Route String）]テキスト ボックスで、ローカル クラスタのルート文字列を入力します。

ステップ 5 **[保存]** をクリックします。

SIP プロファイルの設定

ネットワーク内の SIP プロファイルを編集して、グローバル ダイヤル プラン レプリケーションと URI ダイヤリングをサポートするには、この手順を使用します。

手順

ステップ 1 Cisco Unified CM Administration で、**[デバイス（Device）]**>**[デバイスの設定（Device Settings）]**>**[SIP プロファイル（SIP Profile）]** を選択します。

ステップ 2 **[検索（Find）]** をクリックして、既存の SIP プロファイルを選択します。

ステップ 3 [ダイヤル文字列の解釈（Dial String Interpretation）]ドロップダウン リストから、コールをディレクトリ URI またはディレクトリ番号としてルーティングするかどうかを決定するためにシステムが使用するポリシーを設定します。

- [常にすべてのダイヤル文字列をURIアドレスとして処理（Always treat all dial strings as URI addresses）]
- [電話番号は0～9、A～D、*、+で構成（これ以外はURIアドレスとして処理）（Phone number consists of characters 0–9, A–D, *, and + (others treated as URI addresses)）]
- [電話番号は0～9、*、+で構成（これ以外はURIアドレスとして処理）（Phone number consists of characters 0-9, *, and + (others treated as URI addresses)）]：これがデフォルトのオプションです。

ステップ 4 [SIP要求で完全修飾ドメイン名を使用（Use Fully Qualified Domain Name in SIP Requests）]チェックボックスをオンにします。

ステップ 5 これはオプションです。 Cisco Unified Border Element 全体でクラスタ間コールをルートできるようにするには、[トランク固有の設定（Trunk-Specific Configuration）]の下にある [ILS学習接続先ルート文字列を送信（Send ILS Learned Destination Route String）]チェックボックスをオンにします。

ステップ 6 **[保存]** をクリックします。

URI ダイヤリング用の SIP トランクの設定

URI ダイヤルを展開している場合は、ネットワークの SIP トランクの連絡先ヘッダーアドレス指定ポリシーを設定します。 このオプションは、Cisco Unified Communications Manager が、ディレクトリ番号、ディレクトリ URI、またはディレクトリ番号とディレクトリ URI の両方を

含む混合アドレスを、発信 SIP メッセージの SIP ID ヘッダーに挿入できるかどうかを決定します。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [トランク（Trunk）]** を選択します。

ステップ 2 [検索（Find）]をクリックして、既存の SIP トランクを選択します。

ステップ 3 [**発信コール**] 領域で、[通話および接続された**パーティ情報フォーマット**] ドロップダウンリストから次のいずれかを選択します。

- [接続された第三者の DN のみを提供する（Deliver DN only in connected party）]：発信 SIP メッセージでは、**Cisco Unity Connection** は SIP の連絡先のヘッダー情報に発信元のディレクトリ番号を挿入します。 これがデフォルト設定です。
- [接続された第三者の DN のみを提供する（Deliver DN only in connected party）]：発信 SIP メッセージでは、**ユニティコネクション**は SIP の連絡先のヘッダー情報に発信元の電話番号を挿入します。ディレクトリ URI が使用可能でない場合、Unified Communications Manager は代わりにディレクトリ番号を挿入します。
- [接続された第三者の URI と DN を提供する（Deliver URI and DN in connected party）]：発信 SIP メッセージでは、**Cisco Unity Connection** は SIP の連絡先ヘッダーに発信側のディレクトリ URI とディレクトリ番号を含む混合アドレスを挿入します。 Directory URI が使用可能でない場合、Unified Communications Manager はディレクトリ番号だけを含めます。

ステップ 4 **[保存]** をクリックします。

SIP ルート パターンの設定

グローバル ダイヤル プラン レプリケーションと URI ダイヤリングを使用するクラスタ間でのコール ルーティングについては、学習されたルート文字列がホーム クラスタに送信されるように SIP ルート パターンを設定する必要があります。

手順

ステップ 1 Cisco Unified CM Administration から、**[コールルーティング（Call Routing）] > [SIPルートパターン（SIP Route Pattern）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [パターンの使用法（Pattern Usage）]ドロップダウンから [ドメインルーティング（Domain Routing）]を選択します。

ステップ 4 IPv4 または IPv6 を展開しているかどうかに応じて、[**Ipv4 アドレス（Ipv4 address**）] または [**Ipv6 アドレス（ipv6 address**）] テキストボックスにルート文字列を入力します。

ステップ 5 [SIPトランク/ルートリスト（SIP Trunk/Route List）]の下で、ルート文字列のホーム クラスタへのルートで次のホップ クラスタにつなげる SIP トランクまたはルート リストを選択します。

ステップ 6 [SIPルートパターンの設定（SIP Route Pattern Configuration）]ウィンドウで、残りのフィールドを入力します。 フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 7 **[保存]** をクリックします。

ステップ 8 学習されたルート文字列ごとに SIP ルート パターンを作成します。

ステップ 9 ILS ネットワーク内の各クラスタに対して、この手順を繰り返します。

（注） SIP ルート パターン名にダッシュが含まれる場合、ダッシュ間に数字が含まれていないことを確認する必要があります。 ただし、ダッシュが 2 つ以上ある場合は、文字と数字の組み合わせか、文字のみを使用できます。 SIP ルート パターンの良い例と悪い例は次のとおりです。

正しいパターン：

- abc-1d-efg.xyz.com
- 123-abc-456.xyz.com

無効なパターン：

- abc-123-def.xyz.com
- 1bc-2-3ef.xyz.com

学習されたデータに対するデータベース制限の設定

データベースの制限を設定して、Unified Communications Manager がローカル データベースに書き込むことができる学習オブジェクトの数を決定します。

手順

ステップ 1 Cisco Unified CM の管理から、**[システム（System）]** > **[サービス パラメータ（Service Parameters）]** の順に選択します。

ステップ 2 [サーバ（Server）]ドロップダウン リストから、パラメータを設定するサーバを選択します。

ステップ 3 [サービス（Service）] ドロップダウンリストから、[シスコ クラスタ間検索サービス（アクティブ）（Cisco Intercluster Lookup Service (Active)）] を選択します。 サービスがアクティブと表示されていない場合は、Cisco Unified Serviceability でサービスをアクティベートしたことを確認します。

ステップ 4 [クラスタ全体のパラメータ（ILS）（Clusterwide Parameters (ILS)）]セクションで、[データベース内の学習オブジェクトの最大数（ILS Max Number of Learned Objects in Database）]サービス パラメータの上限を設定します。

ステップ 5 **[保存]** をクリックします。

（注） このサービス パラメータは、Unified Communications Manager が ILS によって学習するデータに対してデータベースに書き込むことができるエントリの最大数を決定します。 このサービス パラメータのデフォルト値は 10 万個で、最大値は 100 万個です。

このサービス パラメータを、データベースに保存されている ILS 学習エントリの現在の数より小さい値に設定した場合、Unified Communications Manager は、ILS 学習オブジェクトをそれ以上データベースに書き込みません。 ただし、既存のデータベース エントリはそのままです。

学習番号とパターンのパーティションの設定

パーティションに学習番号と学習パターンを割り当てる必要があります。 独自のパーティションを定義することも、事前定義されたデフォルトのパーティションを使用することもできます。 Unified Communications Manager は学習代替番号と番号パターンに対して、次の事前定義されたパーティションでインストールされます。

- グローバル学習エンタープライズ番号
- グローバル学習 E.164 番号
- グローバル学習エンタープライズ パターン
- グローバル学習 E.164 パターン

（注） NULL パーティションに学習番号または学習パターンを割り当てることはできません。

手順

ステップ 1 Cisco Unified CM Administration から、**[コール ルーティング（Call Routing）]** > **[グローバル ダイヤル プラン レプリケーション（Global Dial Plan Replication）]** > **[学習した番号とパターンのパーティション（Partitions for Learned Numbers and Patterns）]** を選択します。

ステップ 2 **学習番号とパターンのパーティション**の設定フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 3 **[保存]** をクリックします。

（注） また、パーティションの番号にコールを配置するために、発信者が使用する呼び出し先の検索スペースにもルートパーティションが存在する必要があります。

代替番号のアドバタイズ パターンの設定

アドバタイズされたパターンを使用して、エンタープライズの代替番号の範囲または E.i の代替番号を要約します。 このパターンをILSネットワークに通知して、クラスタ間でパターンに一致する番号への発信を可能にすることができます。

手順

ステップ 1 Cisco Unified CM Administration から、**[コール ルーティング（Call Routing）] > [グローバル ダイヤル プラン レプリケーション（Global Dial Plan Replication）] > [アドバタイズ パターン（Advertised Patterns）]** の順に選択します。

ステップ 2 [アドバタイズされたパターンの検索と一覧表示（Find and List Advertised Patterns）]ウィンドウで、次のいずれかを実行します。

- 既存のパターンを選択するには、[検索（Find）]をクリックします。
- 新しいパターンを作成するには、[新規追加（Add New）]をクリックします。

ステップ 3 [パターン（Pattern）]フィールドに、番号パターンを入力します。 たとえば、54XXX は、54000 ～ 54999 の範囲の番号を要約しています。

ステップ 4 [パターンタイプ（Pattern Type）]フィールドで、[エンタープライズ番号パターン（Enterprise Number Pattern）]または「E.164番号パターン（E.164 Number Pattern）]を選択します。

ステップ 5 ラジオボタンで、PSTN フェールオーバーを適用するかどうかを選択します。

- **[PSTNフェールオーバーを使用しない（Don't use PSTN Failover）]**
- **[パターンをPSTNフェールオーバーとして使用する（Use Pattern as PSTN Failover）]**
- [削除桁数および付加番号をパターンに適用してPSTNフェールオーバーに使用する（Apply Strip Digits and Prepend Digits to Pattern and Use for PSTN Failover）]：このオプションを選択する場合、[PSTNフェールオーバー削除桁数（PSTN Failover Strip Digits）]および [PSTNフェールオーバー付加番号（PSTN Failover Prepend Digits）]フィールドに数字を入力します。

ステップ 6 **[保存]** をクリックします。

学習したパターンのブロック

ローカル クラスタで、特定のエンタープライズ代替番号、+E.164 代替番号、または ILS を通じて学習された番号パターンに対するコール ルーティングを防止するブロッキング ルールを設定する場合は、このオプションのタスクを実行します。

コールを学習した番号または学習したパターンにルーティングする前に、ILS はローカル ブロッキング ルールがダイヤル文字列に一致するかどうかを確認します。 ブロッキング ルールと一致する場合、Unified Communications Manager はコールをルーティングしません。

手順

ステップ 1 Cisco Unified CM Administration で、**[コールルーティング（Call Routing）] > [グローバルダイヤルプランレプリケーション（Global Dial Plan Replication）] > [学習した番号とパターンのブロック（Block Learned Numbers and Patterns）]** を選択します。

ステップ 2 次のいずれかの作業を実行します。

- 既存のブロッキング ルールを選択して編集するには、[検索（Find）]をクリックして、します。
- 新しいルート パターンを作成するには、[新規追加（Add New）]をクリックします。

ステップ 3 [パターン（Pattern）]フィールドに、ブロックするパターンまたは番号を入力します。 たとえば、2065551212 へのコールをブロックするのに、206XXXXXXX というパターンを使用できます。

ステップ 4 ダイヤル文字列プリフィックスに基づいてコールをブロックする場合は、[プレフィックス（Prefix）]を入力します。

ステップ 5 コールが特定のクラスタに送信されないようにブロックする場合は、そのクラスタの **[クラスタID（Cluster ID）]**を入力します。

ステップ 6 [パターンタイプ（Pattern Type）]ドロップダウン リストから、ブロッキング ルールを適用する方法を選択します。

- [任意（Any）]：エンタープライズ番号パターンと +E.164 パターンの両方にブロッキング ルールを適用する場合は、このオプションを選択します。
- [エンタープライズパターン（Enterprise Pattern）]：エンタープライズ番号パターンにのみブロッキング ルールを適用する場合は、このオプションを選択します。
- [+E.164パターン（+E.164 Pattern）]：+E.164 番号パターンにのみブロッキング ルールを適用する場合は、このオプションを選択します。

ステップ 7 **[保存]** をクリックします。

グローバル ダイヤル プラン データのプロビジョニング

ディレクトリ URI、エンタープライズ代替番号、+E.164 代替番号、および PSTN フェールオーバー ルールをディレクトリ番号に追加するには、この手順を使用します。

（注） ユーザの数が多い場合は、ユニバーサル回線テンプレートを設定し、LDAP 同期または一括管理などのプロビジョニング ツールを使用してそれらを適用することで、多数のユーザのグローバル ダイヤル プラン データを 1 回の操作でプロビジョニングできます。 このドキュメントの「ユーザのプロビジョニング」のセクションを参照してください。

手順

ステップ 1 Cisco Unified CM Administration から、**[コール ルーティング（Call Routing）] > [ディレクトリ番号（Directory Number）]** の順に選択します。

ステップ 2 次のいずれかを実行します。

- グローバル ダイヤル プラン データを追加する既存のディレクトリ番号を選択するには、[検索（Find）]をクリックします。
- 新しいディレクトリ番号を作成するには、[新規追加（Add New）]をクリックします。

ステップ 3 新しい番号を作成する場合は、[ディレクトリ番号（Directory Number）]を入力し、[保存（Save）]をクリックします。

ステップ 4 エンタープライズ代替番号を追加するには、[エンタープライズ代替番号の追加（Add an Enterprise Alternate Number）]ボタンをクリックして、次の操作を実行します。

a) [番号マスク（Number Mask）]を入力します。たとえば、4001 の代替番号として「5XXXX」を使用します。結果として生成されたエンタープライズ代替番号（54001）が、**[代替番号（Alternate Number）]** フィールドに表示されます。

b) ローカル ルート パーティションに追加するには、[ローカルルートパーティションに追加（Add to Local Route Partition）]チェックボックスをオンにします。

c) [ルートパーティション（Route Partition）]ドロップダウンから、パーティションを選択します。

d) この代替番号を ILS ネットワークにアドバタイズする場合は、[ILS経由でグローバルにアドバタイズ（Advertise Globally via ILS）]をオンにします。

（注） エンタープライズ代替番号または+E.164 代替番号がパターンの範囲内に収まるように、アドバタイズされたパターンを設定する場合は、代替番号を個別にアドバタイズする必要はありません。

ステップ 5 +E.164 代替番号を追加するには、[+E.164代替番号の追加（Add an +E.164 Alternate Number）]をクリックして、次の操作を実行します。

a) [番号マスク（Number Mask）]を入力します。 たとえば、内線 4001 の代替番号として「1972555XXXX」と入力します。結果として生成された +E.164 代替番号（19725554001）が、**[代替番号（Alternate Number）]** フィールドに表示されます。

b) ローカル ルート パーティションに追加するには、[ローカルルートパーティションに追加（Add to Local Route Partition）]チェックボックスをオンにします。

c) [ルートパーティション（Route Partition）]ドロップダウンから、パーティションを選択します。

d) この代替番号を ILS ネットワークにアドバタイズする場合は、[ILS経由でグローバルにアドバタイズ（Advertise Globally via ILS）]をオンにします。

ステップ 6 [ディレクトリURI（Directory URIs）]セクションで、このディレクトリ番号にディレクトリ URI を追加します。

a) [URI]フィールドに、ディレクトリ URI の詳細情報を入力します。 例えば、alice@cisco.com のように入力します。

b) [パーティション（Partition）]ドロップダウンから、ディレクトリ URI をローカル パーティションに割り当てます。
c) アドバタイズされたカタログにこのディレクトリ URI を含めるには、[ILS経由でグローバルにアドバタイズ（Advertise Globally via ILS）]チェックボックスをオンにします。
d) [行を追加（Add Row）]をクリックし、ディレクトリ URI を追加します。 最大 5 個のディレクトリ URI を追加できます。

ステップ 7 [アドバタイズされたフェールオーバー番号（Advertised Failover Number）]フィールドで、エンタープライズ代替番号または +E.164 代替番号を PSTN フェールオーバーとして選択します。

ステップ 8 [ディレクトリ番号の設定（Directory Number Configuration）] ウィンドウで、残りのフィールドを設定します。 フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 9 **[保存]** をクリックします。

グローバル ダイヤル プランのデータをインポート

Cisco TelePresence Video Communications Server、サードパーティのコール制御システム、または ILS を実行していない別のシステムと相互運用する場合に、この手順を使用します。ディレクトリ URI、+E.164 パターン、および PSTN フェールオーバー ルールのカタログを、他のシステムから ILS ネットワーク内のハブ クラスタにインポートできます。 ILS が ILS ネットワーク全体にカタログを複製し、クラスタが他のシステムにコールを発信できるようになります。

始める前に

ダイヤル プラン カタログを他のシステムから CSV ファイルにエクスポートします。

手順

ステップ 1 Cisco Unified CM Administration から、**[コール ルーティング（Call Routing）]** > **[グローバル ダイヤル プラン レプリケーション（Global Dial Plan RepIication）]** > **[グローバル ダイヤル プラン レプリケーション（Imported Global Dial Plan Catalog）]** を選択します。

ステップ 2 [インポートしたグローバル ダイヤル プラン カタログの検索とリスト（Find and List Imported Global Dial Plan Catalogs）] ウィンドウで、次のいずれかのタスクを実行します。

- 結果のリストから既存のカタログを選択するには、[検索（Find）]をクリックします。
- 新しいカタログを追加するには、[新規追加（Add New）]をクリックします。

ステップ 3 [インポートしたグローバル ダイヤル プラン カタログ（Imported Global Dial Plan Catalog Settings）] ウィンドウの [名前（Name）] フィールドに、インポートするカタログを識別する一意の名前を入力します。

ステップ 4 （任意） **[説明（Description）]** フィールドに、カタログの説明を入力します。

ステップ 5 **[ルート文字列（Route String）]** フィールドで、カタログのインポート元システム用のルート文字列を作成します。

（注） ルート文字列は最大250文字長の英数字であり、ドットおよびダッシュを含めることができます。

ステップ 6 **[保存]** をクリックします。

ステップ 7 Cisco Unified CM の管理ページから、**[一括管理（Bulk Administration）]** > **[ファイルのアップロード/ダウンロード（Upload/Download Files）]** の順に選択します。

- [新規追加] をクリックします。
- **[参照（Browse）]** をクリックし、インポートするカタログ用の CSV ファイルを選択します。

（注） インポートに使用する CSV ファイルが Cisco Unified Communications Manager と互換性があることを確認します。 たとえば、バージョン 9.0(1) へのインポートをサポートする CSV ファイルは、バージョン 10.0(1) とは互換性がありません。

ステップ 8 [ターゲットを選択（Select the Target）] ドロップダウンリストで、[インポートしたディレクトリ URL とパターン（Imported Directory URIs and Patterns）] を選択します。

ステップ 9 [トランザクション タイプを選択（Select Transaction Type）] ドロップダウンリストで、[インポートしたディレクトリ URL とパターンを挿入（Insert Imported Directory URIs and Patterns）] を選択します。

ステップ 10 **[保存]** をクリックします。

ステップ 11 Cisco Unified CM Administration で、**[一括管理（Bulk Administration）]** > **[ディレクトリ URI とパターン（Directory URIs and Patterns）]** > **[インポート済みディレクトリ URI およびパターンの挿入（Insert Imported Directory URIs and Patterns）]** の順に選択します。

ステップ 12 [ファイル名（File Name）] ドロップダウンリストで、インポートするカタログを含むCSVファイルを選択します。

ステップ 13 [インポートしたディレクトリ URI カタログ（Imported Directory URI Catalog）] ドロップダウンリストで、[インポートしたグローバル ダイヤル プラン カタログ（Imported Global Dial Plan Catalog）] ウィンドウで名前を付けたカタログを選択します。

ステップ 14 **[ジョブ説明（Job Description）]** テキスト ボックスに、実行しようとしているジョブの名前を入力します。

ステップ 15 次のいずれかの手順を実行します。

- ジョブをただちに実行する場合は、[今すぐ実行（Run Immediately）] オプションを選択し、[送信（Submit）] をクリックします。
- 所定の時刻に実行するようにジョブをスケジュールするには、[後で実行（Run Later）] ラジオ ボタンをオンにして、[送信（Submit）] をクリックします。

（注） [後で実行（Run Later）] オプションを選択した場合は、ジョブの実行時刻をスケジュールするのに、一括管理ジョブ スケジューラーを使用する必要があります。

Cisco Unified Communications Manager は、インポートしたすべての +E.164 パターンを,グローバルな学習された +E.164 パターン パーティションに保存します。

（注） この手順では、すべてのローカル設定されたディレクトリ URI、+E.164 番号パターン、および関連する PSTN フェールオーバー ルールを、他のコール制御システムにインポート可能な CSV ファイル形式でエクスポートする方法について説明します。一括管理**ディレクトリ Uri およびパターン** > **のメニューを参照してください。詳細につい** > **ては、ローカルディレクトリの uri とパターンをエクスポートしてください。**

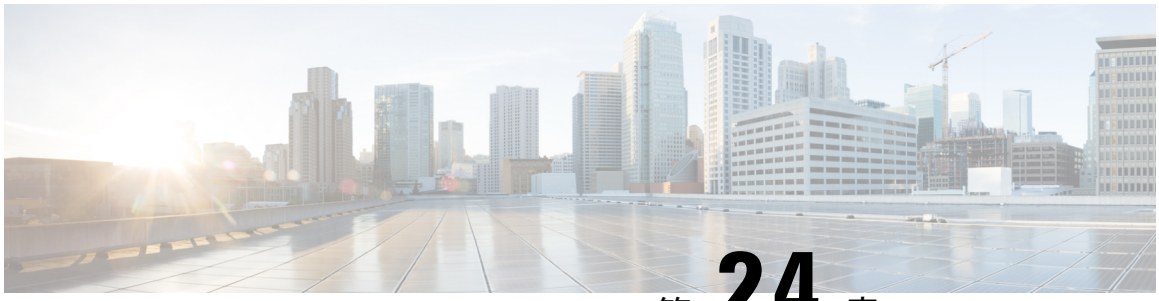
グローバル ダイヤル プラン レプリケーションの連携動作と制限

次の表に、グローバル ダイヤル プラン レプリケーションと URI ダイヤリングでの機能の連携動作の一部をまとめています。

機能	連携動作と制限事項
ディレクトリ URI と +E.164 パターンのエクスポート	ローカル クラスタで設定されているすべてのディレクトリ URI と +E.164 番号パターンを csv ファイルにエクスポートして、別のシステムにインポートすることもできます。 **1.** Cisco Unified CM Administration で、**[一括管理（Bulk Adminstration）]** > **[ディレクトリURIとパターン（Directory URIs and Patterns）]** > **[ローカルディレクトリURINEとパターンのエクスポート（Export Local Directory URIs and Patterns）]** を選択します。 **2.** 次のオプション ボタンのいずれかをクリックして、エクスポート ファイルに付加するドメイン名を定義します。 • [組織のトップレベルドメイン（Organizational Top Level Domain）]：[組織のトップレベルドメイン（Organizational Top Level Domain）] エンタープライズ パラメータの値をエクスポート ファイルのドメイン名に使用する場合は、このラジオ ボタンをクリックします。 • [ルート文字列ドメイン（Route String Domain）]：[ILSの設定（ILS Configuration）] で設定した [ルート文字列（Route String）] フィールドの値をエクスポート ファイルのドメイン名に使用する場合は、このラジオ ボタンをクリックします。 • [ユーザ定義ドメイン（User Defined Domain）]：エクスポート ファイルに付加するカスタマイズされたドメイン名を作成する場合は、このラジオ ボタンをクリックします。 このオプションを選択する場合は、[ドメイン名（Domain Name）] テキスト ボックスにドメイン名を入力します。 **3.** **[ローカルディレクトリURIとパターンのエクスポート(Export Local Directory URIs and Patterns)]** ボタンをクリックします。 **4.** CSV ファイルをローカル ドライブに保存します。

機能	連携動作と制限事項
URI ダイヤリングを使用したパーティション分割	ディレクトリ URI のパーティション分割は、ディレクトリ URI のプロビジョニング方法によって異なります。 • [エンドユーザの設定（End User Configuration）]でエンド ユーザに割り当てたユーザベースのディレクトリ URI の場合、削除できないローカルのディレクトリ URI パーティションが自動的に URI に割り当てられます。 別のパーティションを割り当てることはできませんが、[ディレクトリURIエイリアスパーティション（Directory URI Alias Partition）]エンタプライズ パラメータを設定することで、管理者が管理するパーティションをローカルディレクトリ URI パーティションのエイリアスとして使用できます。 • [ディレクトリ番号の設定（Directory Number Configuration）]で URI がディレクトリ番号に直接割り当てられている回線ベースのディレクトリ URI の場合、各 URI をローカルのパーティションに個別に割り当てることができます。 LDAP 同期や一括管理などのツールを使用してディレクトリ URI をプロビジョニングする場合は、次のようになります。 • LDAP 同期によってプロビジョニングされるディレクトリ URI はユーザベースであり、[エンドユーザの設定（End User Configuration）]でユーザに割り当てられます。 これらの URI は、ローカルのディレクトリ URI パーティションに割り当てられます。 ユーザにプライマリ内線番号が設定されている場合、この URI は、[ディレクトリ番号の設定（Directory Number Configuration）]でもプライマリ URI として表示されます。 ただし、割り当てられるパーティションはディレクトリ URI パーティションです。 • 一括管理でプロビジョニングされたディレクトリ URI の場合は、更新の適用方法によって異なります。 たとえば、`bat.xlt` スプレッドシートを使用して csv インポート ファイルを作成する場合、ディレクトリ URI を追加するのにスプレッドシートの [ユーザ（Users）]タブまたは[ユーザの更新（Update Users）]タブを使用すると、そのユーザはユーザベースの URI になります。 ただし、**[ファイル形式の作成（Create File Format）]** をクリックすると表示される **[回線フィールド（Line Fields）]** オプションを使用してディレクトリ URI を追加する場合は、その URI をディレクトリ番号に割り当て、URI ディレクトリにローカルのパーティションを割り当てることができます。

機能	連携動作と制限事項
ディレクトリ URI での大文字と小文字の区別	デフォルトでは、ディレクトリ URI のユーザ部分（@ の前の部分）では、大文字と小文字が区別されます。 [URI検索ポリシー（URI Lookup Policy）] エンタープライズ パラメータを編集することで、ユーザの部分で大文字と小文字を区別しないように設定できます。
[コーリングサーチスペース(Calling Search Space)]	ディレクトリ URI、エンタープライズ代替番号、および +E.164 代替番号がダイアル可能になるためには、発信者のコーリング サーチ スペースで使用可能なパーティションにそれらの URI または番号が存在する必要があります。
URI ダイヤリングを使用したディジット変換	ディジット変換を使用しており、クラスタ間 URI ダイヤリングを導入する場合は、電話の設定または電話が使用するデバイス プールのいずれかにディジット変換を適用します。 • 個別の電話に適用する場合は、**[リモート番号（Remote Number）]** セクションの **[発信側トランスフォーメーション CSS（Calling Party Transformation CSS）]** フィールドで変換を適用します。 • デバイスプールの場合は、**[デバイスモビリティ関連情報（Device Mobility Related Information）]** の下にある **[発信側トランスフォーメーション CSS（Calling Party Transformation CSS）]** フィールドで変換を適用することができます。 （注） ローミング用デバイスの場合は、**[電話機の設定（Phone Configuration）]** ウィンドウの **[デバイスプールの発信側トランスフォーメーション CSS を使用（Use Device Pool Calling Party Transformation CSS）]** チェックボックスがオフの場合でも、デバイスプールの設定が電話機の設定よりも優先されます。



第 24 章

発信側の正規化

発信側の正規化の概要

発信側の正規化によって電話番号のグローバル化やローカライズが可能になるため、適切な発信番号が電話機に表示されます。 発信側の正規化を使用して、一部の電話機のダイヤル機能を強化し、コールが複数の地理的ロケーションにルーティングされる場合の折返し機能を向上させます。 この機能は、電話機のコール ログ ディレクトリのディレクトリ番号を変更することなく電話機がコールバックできるよう、グローバル発信者番号をローカライズされた番号にマッピングできます。

発信者番号のグローバル化

Cisco Unified CM Administration で [発信者番号タイプ（Calling Party Number Type）] とプレフィックスを設定することで、着信側の電話に表示する発信者電話番号を、（国際国番号などのプレフィックスを含むグローバル化バージョンに）再フォーマットするように Cisco Unified Communications Manager を設定できます。それによって、世界中のどこからでもその番号をダイヤルできます。

Cisco Unified Communications Manager は、[発信者番号タイプ（Calling Party Number Type）] の値とともにルート パターンやトランスレーション パターンなどのさまざまな番号パターンを使用して、電話番号をグローバル化できます。 たとえば、Cisco Unified Communications Manager は、サブスクライバ発信者番号タイプのローカライズされたドイツの電話番号 069XXXXXXX を、ドイツの国番号と都市コードを含む +49 40 69XXXXXXX にグローバル化するように設定できます。

複数の地理的場所にルーティングされるコールの場合、各ルーティング パスに適用される異なるトランスレーション設定によって、発信者番号は各コール パスで一意にグローバル化できます。 Cisco Unified Communications Manager では、電話でローカライズされた発信者番号を電話画面に表示し、グローバル化された番号を電話の通話履歴ディレクトリに表示するように設定

することもできます。電話ユーザがコールを発信する前に、電話の通話履歴ディレクトリのエントリを編集する必要がないようにするため、グローバル発信者番号をそのローカルバージョンにマッピングします。

発信者番号のローカリゼーション

発信者番号の最終表示用に、発信者番号タイプ（国内、国際、サブスクライバ、不明）ごとに発信側トランスフォーメーションパターンを設定し、そのコールの発信者番号タイプに固有のストリップ桁数とプレフィックスの手順を適用できます。 これによって、Cisco Unified Communications Manager は、着信側の電話に表示される発信者番号が不要な国コードや国際アクセス コードを含まないローカライズされた番号となるように、発信者番号を再フォーマットできます。

たとえば、PSTN から到着した着信番号が、グローバル化された番号 +49 40 69XXXXXXX で（+49 が国番号、40 が都市コードを表す）、発信者番号タイプがサブスクライバであるとします。 Cisco Unified Communications Manager には、国番号、都市コードを取り除き、プレフィックス 0 を追加する手順とともに、発呼側トランスフォーメーション パターンを設定できます。手順が適用された後、発信者番号はダイヤルされた電話機に 069XXXXXXX として表示されます。

グローバル化された発信者番号のローカライズ バージョンへのマッピング

電話ユーザがコールを発信する前に、電話の通話履歴ディレクトリのエントリを編集する必要がないようにするため、ルート パターンと着信側トランスフォーメーション パターンを使用して、グローバル発信者番号をローカライズされたバージョンにマッピングできます。 これによって、着信側がコールを返す場合に、Cisco Unified Communications Manager は確実に正しいゲートウェイにコールをルーティングできます。

グローバル発信者番号のマッピングによって、コールバック機能が改善され、着信側は電話の通話履歴ディレクトリ内の電話番号を変更する必要なく、コールバックできます。

発信側の正規化の要件

発信側の正規化を設定する前に、Cisco Unified Serviceability で **Cisco CallManager** サービスをアクティブにする必要があります。 詳細については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

Cisco Unified Communications Manager に発信者番号タイプを判別させるには、想定するコールに一致する [発信者番号タイプ（Calling Party Number Type）]値を割り当てるパターンを設定します。 次の設定ウィンドウで、パターンを作成して適用することができます。

- ルート パターン
- ハント パイロット
- トランスレーション パターン
- 発信番号トランスフォーメーション パターン

（注） 発信者による変換は、元の発信者に対してのみ機能します。 番号をリダイレクトするために行った変更は、転送ヘッダーに対してのみ適用されます。 [SIP トランク] チャプターから設定を確認し、SIP トランク自体に転送ヘッダーを追加します。

発信側の正規化の設定タスク フロー

発信側の正規化のプレフィックスと削除桁数ルールは、Unified Communications Manager でさまざまな場面で適用できます。 たとえば、デバイス プール、ルート パターン、トランスレーション パターン、ハント パイロット、ゲートウェイ、およびトランクに桁数の変換を適用できます。 桁数の変換を適用する方法は、ダイヤル プラン、デバイス、およびトランクの導入方法に応じて変わります。 詳細については、ダイヤルプラン、ルートパターン、トランスレーション パターン、およびトランスフォーメーション パターンに関連するトピックを参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	Unified Communications Manager に発信者番号タイプを判断させる場合は、予想されるコールと合致する発信者番号タイプを作成して設定する必要があります。次の設定ウィンドウで、パターンを作成して適用することができます。 • ルート パターン • ハント パイロット • トランスレーション パターン • 発信番号トランスフォーメーション パターン	
ステップ 2	発信側番号のグローバル化 （298 ページ）	PSTN経由で受信する着信コールの場合は、発信者番号をグローバライズするための設定を構成します。
ステップ 3	コーリング サーチ スペースの設定 （299 ページ）	パーティションとコーリングサーチスペースを設定する
ステップ 4	発信側トランスフォーメーション パターンの作成 （299 ページ）	発信者番号をグローバル化されたバージョンまたはローカライズされたバージョンに変換し、各パターンをパーティションに割り当てる、通話相手の変換のパターンを作成します。

	コマンドまたはアクション	目的
ステップ 5	コーリング サーチ スペースへの発信側トランスフォーメーション パターンの適用 （300 ページ）	デバイスプール、ゲートウェイ、およびトランクのように、着信通話関係者変換 CSS をデバイスに適用します。

発信側番号のグローバル化

PSTN 経由で到達する着信コールの場合は、発信者番号をグローバル化する設定を行います。発信者番号をグローバル化し、それをデバイス プールまたは個々のデバイスに適用する設定できます。 また、クラスタ全体に、発信者番号の正規化設定を適用するサービス パラメータを設定できます。

発信者番号をグローバル化するには、次の手順を実行します。

手順

ステップ 1 発信者番号の正規化設定を特定のデバイスに適用するには、次の手順を実行します。

a) 設定を適用するデバイスの設定ウィンドウを開きます。 たとえば、デバイス プール、ゲートウェイ、電話、トランクです。

b) 設定ウィンドウの [着信コールの発信側の設定（Incoming Calling Party Settings）] セクションで、各発信者番号タイプのプレフィックスおよび削除桁数の指示を適用します。

（注） Cisco Unified Communications Manager には、コール転送、コール パーク、ボイス メッセージング、CDR データなどの補足サービスのような、すべての追加アクションの発信者番号フィールドにプレフィックスが含まれます。

ステップ 2 サービス パラメータを使用して、クラスタ全体のすべてのデバイスの発信者番号をグローバル化する場合には、次の手順を実行します。

a) Cisco Unified CM の管理から、**[システム（System）]** > **[サービス パラメータ（Service Parameters）]** の順に選択します。

b) [サーバ（Server）] ドロップダウン リストから、サービスを実行するサーバを選択します。

c) [サービス（Service）] ドロップダウン リストから、[Cisco CallManager] を選択します。

d) [詳細設定（Advanced）] をクリックします。

e) 以下のパラメータの値を設定します。この値は、クラスタ全体から電話、MGCP ゲートウェイ、H.323 ゲートウェイに適用できます。

- [発信者の国内番号プレフィックス（Incoming Calling Party National Number Prefix）]
- [発信者の国際番号プレフィックス（Incoming Calling Party International Number Prefix）]
- [発信者の不明な着信番号プレフィックス（Incoming Calling Party Unknown Number Prefix）]
- [発信者の加入者番号プレフィックス（Incoming Calling Party Subscriber Number Prefix）]

（注） Cisco Unified Communications Manager で、特定の電話のクラスタ全体のサービス パラメータ設定を適用するには、デバイスとデバイス プール レベルの両方で、その電話のプリフィックス設定をデフォルト オプションに設定する必要があります。

コーリング サーチ スペースの設定

呼び出し側の正規化機能を処理するためにコーリングサーチスペースを設定する場合は、この手順を使用します。

手順

ステップ 1 Cisco Unified CM Administration で、**[コール ルーティング（Call Routing）] > [コントロールのクラス（Class of Control）] > [パーティション（Partitions）]** の順に選択します。

ステップ 2 ネットワークのパーティションを作成します。

ステップ 3 Cisco Unified CM Administration で、**[コール ルーティング（Call Routing）] > [コントロールのクラス（Class of Control）] > [コーリング サーチ スペース（Calling Search Space）]** の順に選択します。

ステップ 4 発信側トランスフォーメーション パターンのコーリング サーチ スペースを作成します。

ステップ 5 コーリング サーチ スペースごとに、パーティションをコーリング サーチ スペースに割り当てます。

発信側トランスフォーメーション パターンの作成

発信側の正規化機能を処理するために発信側トランスフォーメーションパターンを設定している場合、次の手順を使用します。

手順

ステップ 1 Cisco Unified CM Administration で、**[コール ルーティング（Call Routing）] > [トランスフォーメーション パターン（Transformation Pattern）] > [発信側トランスフォーメーション パターン（Calling Party Transformation Pattern）]** を選択します。

ステップ 2 トランスフォーメーション パターンを作成します。

ステップ 3 作成する発信側トランスフォーメーションパターンそれぞれには、発信側番号を国際対応または国内対応するために、先頭に付加または除外している番号コマンドを割り当てます。

ステップ 4 それぞれの発信側トランスフォーメーション パターンには、コーリング サーチ スペースの 1 つに関連付けられているパーティションを割り当てます。

コーリング サーチ スペースへの発信側トランスフォーメーション パターンの適用

デバイスプール、ゲートウェイ、トランクなどのデバイスに、着信する発信側トランスフォーメーション CSS を割り当てます。

手順

ステップ 1 Cisco Unified CM Administration で、発信側トランスフォーメーションを適用するデバイスに該当する設定ウィンドウを選択します。

- [ゲートウェイ（Gateways）]
- [トランク（Trunks）]
- [デバイス プール（Device Pools）]

ステップ 2 発信者番号をローカライズするには、[コーリング サーチ スペース（Calling Search Space）] ドロップダウン リスト ボックスで、適用する発信側トランスレーション パターンを含む CSS を選択します。

（注） デバイス プールに対して CSS を設定する場合、電話機にもそのデバイス プールを適用する必要があります。

ステップ 3 発信者番号をグローバル化するには、[着信の発信者番号設定（Incoming Calling Party Settings）] セクションで、適用する発信側トランスレーション パターンを含むコーリング サーチ スペースを選択します。

発信側の正規化サービス パラメータの例

次のパラメータは、電話機、MGCP ゲートウェイ、または H.323 に対して、クラスタ全体に適用することができます。特定のデバイスでクラスタ全体パラメータを使用するためには、デバイス設定のプレフィックスをデフォルトに設定する必要があります。

- [発信者の国内番号プレフィックス（Incoming Calling Party National Number Prefix）]
- [発信者の国際番号プレフィックス（Incoming Calling Party International Number Prefix）]
- [発信者の不明な着信番号プレフィックス（Incoming Calling Party Unknown Number Prefix）]
- [発信者の加入者番号プレフィックス（Incoming Calling Party Subscriber Number Prefix）]

次の表に、プレフィックスとストリップディジットの設定の例と、これらの値を使用して、発信者番号の表示を変換する方法を示します。サービスパラメータの設定の場合、コロンの後の数字は、呼び出し者番号の先頭から除外する桁数を表し、コロンの後の数字は、発信者番号の先頭に追加されるプレフィックスを表します。

表 *24 :* 発信側の正規化のサービスパラメータ例

元の着信番号	[サービスパラメータ値(Service Parameter Value)]	説明	最終着信番号
04423452345	+:1	最初の桁を削除してから、+ のプレフィックスを追加します	+4423452345
04423452345	:2	最初の 2 桁を削除	423452345
552345	+1:6	最初の 6 桁を削除してから、+ 1 のプレフィックスを追加します。	+1
552345	+1:8	可能な桁数よりも多くの桁数が削除されているため、終了番号が空白です。	
552345	123	プレフィックス 123 の追加	123552345
空白	+1:2	電話番号が空白の場合、プレフィックスは適用されません	空白
0442345	:26	発信者の正規化は、24 桁までしかストリップできません	Cisco Unified Communications Manager ではこの設定はできません

発信側の正規化の連携動作と制限事項

発信側の正規化の連携動作

発信側の正規化機能との連携動作を次の表で説明します。

機能	連携動作
転送コール	転送機能は、発信時の更新と発信者の正規化に依存しており、各コールホップの初期コール設定が行われるため、発信者の正規化がサポートされない場合があります。次に示すのは、発信者の正規化を転送に使用する方法の一例です。 内線番号 12345、電話番号 972 500 2345 の電話機 A が、内線番号 54321、電話番号 972 500 4321 の電話機 B にコールを発信します。電話 B では、発信者番号 12345 が表示されますが、電話 B はそのコールをサンホセゲートウェイを介して電話 C に転送します。最初の転送時には、電話 C は 972 500 4321 の発信者番号が表示されますが、転送が完了した後、電話機 C は電話 A の発信者番号を 12345 として表示します。
コールの転送	転送されたコールは、発信者側番号のグローバル化およびローカル化をサポートします。たとえば、ダラスの PSTN 経由で発信者が電話機 F を使用して電話機 G にコールを発信します。電話機 G では、すべてのコールがサンノゼにある電話機 H に自動転送されます。着信するダラスゲートウェイでは、発信者番号は 555-5555/Subscriber と表示されますが、そのコールはサンノゼのゲートウェイに転送されます。ダラスからの発信コールは 972 555 5555 として表示されます。サンホセゲートウェイでの受信時には、+1 がプリフィックスされ、電話 F は +1 972 555 5555 というコール番号を表示します。
コール詳細レコード	発信側の正規化が呼詳細（CDR）と動作する方法の詳細については、『*Cisco Unified Communications Manager Call Detail Records* アドミニストレーション ガイド』を参照してください。
Cisco Unified Communications Manager Assistant	発信側の正規化機能を設定すると、Cisco Unified Communications Manager Assistant により、ローカライズおよびグローバル化されたコールが自動的にサポートされます。Cisco Unified Communications Manager Assistant は、ローカライズされた発信側番号をユーザインターフェイスに表示できます。また、マネージャに対する着信コールの場合、Cisco Unified Communications Manager Assistant は、フィルタ パターンに一致したときに、ローカライズされた発信側番号とグローバル化された発信側番号を表示できます。Cisco Unified Communications Manager Assistant の設定方法の詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html）を参照してください。

機能	連携動作
Cisco Unity Connection	Cisco Unity Connection は、国際エスケープ文字（+）をサポートしていません。このため、ボイス メッセージング機能を正常に動作させるには、Cisco Unity Connection へのコールに（+）が含まれていないことを確認する必要があります。 Cisco Unity Connection が予想どおりに動作するようにするには、このアプリケーションをデバイスとして扱い、発信側変換を設定して、このボイスメール アプリケーションに + が送信されないようにする必要があります。Cisco Unity Connection サーバで北米ベースのダイヤル プランを使用している場合は、Cisco Unity Connection で発信側番号を受信する前に、その発信側番号を NANP 形式にローカライズします。Cisco Unified Communications Manager の管理ページにはボイスメール ポート用の発信側変換 オプションがないため、ボイスメール ポートに関連付けられているデバイス プールで発信側番号変換を設定するようにしてください。発信側番号をローカライズするには、ボイスメール アプリケーションが特定の機能（Live Reply など）用の番号に容易にリダイヤルできるよう、アクセス コードにプレフィックスを付加することも検討してください。たとえば、+12225551234 を 912225551234 に変換したり、国際番号 +4423453456 に国際エスケープ コードを含めて 90114423453456 のように変換したりできます。
デバイス モビリティ	ローミング用デバイス プールの発信側変換 CSS は、[電話の設定(Phone Configuration)] ウィンドウで [デバイス プールの発信側変換 CSSを使用(Use Device Pool Calling Party Transformation CSS)] チェックボックスがオフの場合でも、同じデバイス モビリティ グループ内でローミングする電話機のデバイス レベルの設定をオーバーライドします。 次の例は、発信者側の正規化が、ホーム ロケーションはダラスだけれども、現在はサンノゼにローミングしている電話のデバイス モビリティと動作するようすを示しています。 電話機がサンノゼでローミングしているときに、ダラスの 972 500 1212 <国内> から PSTN 経由でコールを受けます。サンノゼの着信ゲートウェイでは、発信側番号がグローバル形式の + 1 408 500 1212 に変換されます。現在サンノゼにある電話機では、発信側番号は 1 972 500 1212 として表示されます。 電話機がサンノゼでローミングしているときに、サンノゼの 7 桁のダイヤル エリア内の 500 1212 <加入者> から PSTN 経由でコールを受けます。サンノゼの着信ゲートウェイでは、発信側番号がグローバル形式の + 1 408 500 1212 に変換されます。現在サンノゼにある電話機では、発信側番号は 9 500 1212 として表示されます。

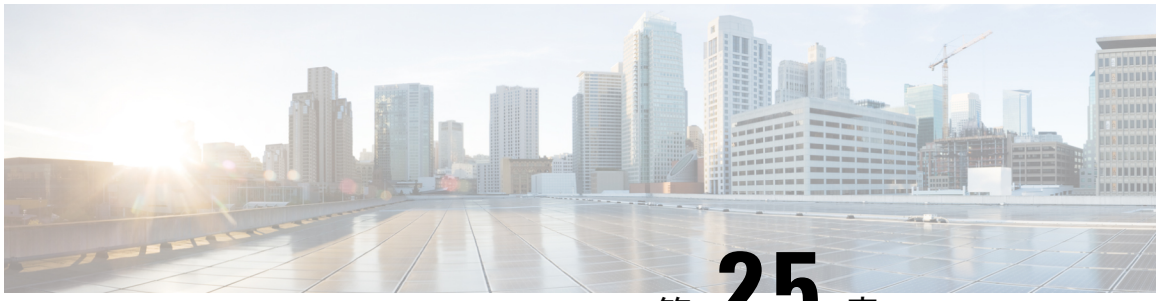
発信側の正規化の制限事項

次の表は、通話相手の正規化機能が、Cisco Unified Communications Manager の特定の機能とシステムコンポーネントを使用している場合の制限を示しています。

表 *25 :* 発信側の正規化の制限事項

機能	制限事項
共有回線	共有回線の場合に表示される発信側番号は、Cisco Unified Communications Manager 内の一連のコール制御イベントによって決まります。ローカライズされた正しくない発信側番号が共有回線で表示されるのを回避するため、特に、共有回線が地理的に異なる場所にまたがる場合は、同じ回線を共有する異なるデバイスに同じ発信側変換 CSS を設定する必要があります。
SIP トランクおよび MGCP ゲートウェイ	SIP トランクおよび MGCP ゲートウェイでは、コールごとに国際エスケープ文字（+）の送信をサポートしています。H.323 ゲートウェイは、+ をサポートしていません。QSIG トランクは、+ の送信を試みません。+ をサポートするゲートウェイ経由の発信コールの場合、Cisco Unified Communications Manager は、ダイヤルされた数字とともに + をゲートウェイに送信できます。+ をサポートしないゲートウェイ経由の発信コールの場合、Cisco Unified Communications Manager がゲートウェイにコール情報を送信すると、国際エスケープ文字 + が除去されます。
SIP	SIP は番号タイプをサポートしないため、SIP トランク経由のコールは、発信側番号の種類が不明（Unknown）である [着信番号（Incoming Number）] 設定のみをサポートします。
QSIG	QSIG 設定は、通常、均一のダイヤル プランをサポートします。QSIG を使用している場合、番号とプレフィックスの変換により機能の連携動作に問題が発生することがあります。
発信側変換 CSS	発信側番号をローカライズする場合、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。[発信側変換CSS（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。ルーティングに使用されない Null 以外のパーティションで、必ず [発信側変換パターン（Calling Party Transformation Pattern）] を設定してください。
T1-CAS および FXO ポート	発信側変換 CSS（Calling Party Transformation CSS）設定は、ゲートウェイ上の T1-CAS と FXO ポートには適用されません。

機能	制限事項
Cisco Unity Connection	Cisco Unity Connection は、国際エスケープ文字（+）をサポートしていません。このため、ボイスメッセージング機能を正常に動作させるには、Cisco Unity Connection へのコールに（+）が含まれていないことを確認する必要があります。 Cisco Unity Connection の詳細については、http://www.cisco.com/c/en/us/products/unified-communications/unity-connection/index.html を参照してください。



第 25 章

ダイヤル ルールの設定

ダイヤル ルールの概要

Unified CM は、次のタイプのダイヤルルールをサポートしています。

- **アプリケーション ダイヤル ルール**：Cisco Web Dialer や Cisco Unified Communications Manager などのアプリケーション用にダイヤルルールを追加したり優先順位を並べ替えたりするには、管理者がアプリケーション ダイヤル ルールを使用します。
- **ディレクトリ検索ダイヤル ルール**：発信者識別番号を変換したり、Cisco Unified Communications Manager Assistant などのアプリケーションでアシスタント コンソールからディレクトリ検索を実行したりするには、管理者がディレクトリ検索ダイヤルルールを使用します。
- **SIP ダイヤル ルール**：システム番号の分析とルーティングを実行するには、管理者が SIP ダイヤル ルールを使用します。 管理者は SIP ダイヤル ルールを設定し、コール処理が実行される前に、その SIP ダイヤル ルールを Cisco Unified IP Phone に追加します。

ダイヤルルールの前提条件

- SIP ダイヤルルール設定の場合は、デバイスが SIP を実行している必要があります。
- 管理者は、Cisco IP 電話 7911、7940、7941、7960、7961、7970、および 7971 とともに SIP ダイヤルルールを次のデバイスに関連付けます。

ダイヤル ルールの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	アプリケーション ダイヤル ルールの設定 （308 ページ）	Cisco Web Dialer、Cisco Unified Communications Manager Assistant などのアプリケーションのダイヤル ルールの優先順位を追加し並べ替える、アプリケーション ダイヤル ルールを設定します。
ステップ 2	ディレクトリ検索ダイヤル ルールの設定 （309 ページ）	発信者の ID 番号をディレクトリで検索可能な番号に変換するには、ディレクトリ検索ダイヤル ルールを設定します。
ステップ 3	SIP ダイヤル ルールの設定 （310 ページ）	SIP を実行している電話のダイヤル プランを設定するには、SIP ダイヤル ルールの設定を使用します。
ステップ 4	ダイヤル ルールの優先順位の変更 （313 ページ）	これはオプションです。 複数のダイヤル ルールがある場合は、[Cisco Unified Communications Manager の管理（Cisco Unified Communications Manager Administration）] ウィンドウでダイヤル ルールの優先順位を変更します。

アプリケーション ダイヤル ルールの設定

Cisco Unified Communications Manager は、アプリケーション ダイヤル ルールをサポートし、Cisco Web Dialer や Cisco Unified Communications Manager Assistant のようなアプリケーションのダイヤル ルールの優先順位の追加と並べ替えができます。 アプリケーション ダイヤル ルールを適用すると、ユーザがダイヤルする電話番号に対して数字の追加と削除が自動的に行われます。 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。

（注） Cisco Unified Communications Manager は自動的に、CTI リモート デバイスのすべてのリモート接続先番号にアプリケーション ダイヤル ルールを適用します。

新しいアプリケーション ダイヤル ルールを追加する、または既存のアプリケーション ダイヤル ルールを更新するには、次の手順を実行します。

手順

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

ステップ 2 [アプリケーション ダイヤル ルールの検索と一覧表示（Find and List Application Dial Rules）]ウィンドウで、次のいずれかの手順を実行します。

- [新規追加] をクリックします。
- [検索（Find）]をクリックし、既存のアプリケーション ダイヤル ルールを選択します。

ステップ 3 [アプリケーション ダイヤル ルールの設定（Application Dial Rule Configuration）]ウィンドウのフィールドを設定します。 フィールドの説明の詳細については、オンライン ヘルプを参照してください。

ステップ 4 **[保存]** をクリックします。

次のタスク

次の作業を行います。

- ディレクトリ検索ダイヤル ルールの設定 （309 ページ）
- SIP ダイヤル ルールの設定 （310 ページ）

ディレクトリ検索ダイヤル ルールの設定

ディレクトリ検索ダイヤルルールは、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。 各ルールでは、先頭の数字および番号の長さに基づいて、変換する数字を指定します。 たとえば、10 桁の電話番号から市外局番と 2 桁の局番を自動的に削除するディレクトリ検索ダイヤル ルールを作成できます。たとえば、4085551212 は、51212 になります。

新しいディレクトリ検索ダイヤルルールを追加するか、既存のディレクトリ検索ダイヤルルールを更新するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager Administration から、**[コール ルーティング（Call Routing）]** > **[ダイヤル ルール（Dial Rules）]** > **[ディレクトリ検索ダイヤル ルール（Directory Lookup Dial Rules）]** を選択します。

ステップ 2 [ディレクトリ検索ダイヤル ルールの検索と一覧表示（Directory Lookup Dial Rule Find and List）]ウィンドウで、以下のいずれかの手順を実行します。

- [新規追加] をクリックします。
- [検索（Find）]をクリックし、既存のディレクトリ検索ダイヤル ルールを選択します。

ステップ 3 [ディレクトリ検索ダイヤル ルール（Directory Lookup Dial Rules）]ウィンドウ内の各フィールドを設定します。 フィールドの説明の詳細については、オンライン ヘルプを参照してください。

ステップ 4 **[保存]** をクリックします。

次のタスク

SIP ダイヤル ルールの設定 （310 ページ）

SIP ダイヤル ルールの設定

SIP ダイヤル ルールによって、SIP を実行している Cisco IP 電話のローカル ダイヤル プランが提供されるため、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。 管理者が SIP ダイヤル ルールを設定し、SIP を実行している電話機に適用します。

手順

	コマンドまたはアクション	目的
ステップ 1	SIP ダイヤル ルールの設定 （311 ページ）	SIP ダイヤル ルールを設定および更新し、それらを SIP を実行している電話機と関連付けます。
ステップ 2	SIP ダイヤル ルールのリセット （312 ページ）	SIP ダイヤル ルールを更新したときに、SIP を実行している電話機をリセットまたは再起動して、電話機を新しい SIP ダイヤル ルールで更新する手順は、次のとおりです。
ステップ 3	電話機への SIP ダイヤル ルール設定の同期 （313 ページ）	設定変更された SIP ダイヤル ルールと SIP 電話を同期化するには、次の手順を行います。この手順によって、中断を最小限に抑えた方法で未処理の設定が適用されます（たとえば、影響を受ける SIP 電話の中には、リセットまたは再起動が不要なものがあります）。

関連トピック

パターンの形式 （311 ページ）

パターンの形式

表 *26 : SIP* ダイヤルルールのパターンフォーマット

ダイヤル ルール パターン	値
7940_7960_OTHER	• ピリオド（.）は、すべての文字に一致します。 • シャープ記号（#）は、終了キーとして機能します。終了が適用されるのは、マッチングで>#にヒットした後だけです。または、終了キーとしてアスタリスク(*)を使用することもできます。 （注） シャープ記号を[7940_7960_OTHER]で有効にするには、パターン フィールドにシャープ記号を設定する必要があります。 • アスタリスク (*) は 1 つ以上の文字に一致し、ワイルドカード文字として処理されます。 * の前にバックスラッシュ（\）エスケープ シーケンスを置いて* というシーケンスにすると、* を通常の文字として処理できます。 \ は電話機が自動的に削除するため、発信ダイヤル文字列には現れません。 *は、ダイヤル番号として受信された場合、ワイルドカード文字 * とピリオド（.）に一致します。 • カンマ（,）を使用すると、電話機が第 2 発信音を生成します。 たとえば、7.... は 7 で始まるすべての 4 桁の DN に一致します。8,..... は 8 に一致し、第 2 発信者（デフォルト値）を再生した後、すべての 5 桁 DN に一致します。

SIP ダイヤル ルールの設定

SIP を実行している電話機のダイヤルプランを設定します。

手順

ステップ 1 Cisco Unified Communications Manager Administration から、**[コールルーティング（Call Routing）] > [ダイヤルルール（Dial Rules）] > [SIPダイヤルルール（SIP Dial Rules）]**.を選択します。

ステップ 2 **SIPダイヤルルールの検索/一覧表示** ウィンドウが表示されます。 次のいずれかの手順を実行します。

- **[新規追加]** をクリックします。
- [**検索**] と既存の SIP ダイヤルルールを選択します。

ステップ 3 **[SIP ダイヤルルール] 設定**ウィンドウのフィールドを設定します。 フィールドの説明の詳細については、オンライン ヘルプを参照してください。

ステップ 4 **[保存]** をクリックします。

（注） Cisco Unified Communications Manager Administration で SIP ダイヤル ルールを追加または更新すると、Cisco TFTP サービスによってすべての電話機設定ファイルが再構築されます。そのため、Cisco TFTP サービスを実行するサーバ上の CPU にスパイクが発生することがあり、これは多くの電話が接続された大規模なシステムでは顕著になります。 CPU にスパイクを発生させないためには、SIP ダイヤル ルールの追加や更新をメンテナンス時間枠内で行うか、または設定変更を行う前に Cisco Unified Serviceability で Cisco TFTP サービスを一時的に停止するかしてください。Cisco TFTP サービスを停止した場合は、SIP ダイヤル ルールを追加または更新した後、必ず Cisco Unified Serviceability でサービスを再開してください。

次のタスク

SIP ダイヤル ルールのリセット （312 ページ）

関連トピック

パターンの形式 （311 ページ）

SIP ダイヤル ルールのリセット

SIP ダイヤル ルールを更新したときに、新しい SIP ダイヤル ルールで電話機が更新されるよう、次の手順を実行して SIP を実行している電話機をリセットまたは再起動します。

始める前に

SIP ダイヤル ルールの設定 （311 ページ）

手順

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

ステップ 2 [SIP ダイヤル ルールの検索と一覧表示（Find and List SIP Dial Rules）]ウィンドウで、[検索（Find）]をクリックし、リセットする既存の SIP ダイヤル ルールを選択します。

ステップ 3 [SIP ダイヤル ルールの設定（SIP Dial Rule Configuration）]ウィンドウで、[リセット（Reset）] をクリックします。

ステップ 4 [デバイス リセット（Device Reset）]ダイアログ ボックスで、次のタスクのいずれかを実行します。

- 選択したデバイスをシャットダウンせずに再起動し、Cisco Unified Communications Manager に登録するには、[再起動（Restart）]をクリックします。

- デバイスをシャットダウンしてから再起動するには、[リセット（Reset）]をクリックします。
- 操作を実行せずに [デバイス リセット（Device Reset）] ダイアログ ボックスを閉じるには、[閉じる（Close）]をクリックします。

管理者が SIP ダイヤル ルールを設定して SIP を実行している電話機に適用すると、データベースから TFTP サーバに通知が送信されます。これによって、SIP を実行している電話機の新しい設定ファイルを作成できます。 TFTP サーバは Cisco Unified Communications Manager に新しい設定ファイルについて通知し、更新された設定ファイルが電話機へ送られます。 詳細については、SIP を実行する Cisco Unified IP Phone の「**TFTP サーバの設定**」を参照してください。

次のタスク

電話機への SIP ダイヤル ルール設定の同期 （313 ページ）

電話機への SIP ダイヤル ルール設定の同期

SIP 電話機と設定が変更された SIP ダイヤル ルールを同期するには、次の手順を実行します。

始める前に

SIP ダイヤル ルールのリセット （312 ページ）

手順

ステップ 1 Cisco Unified Communications Manager Administration から、**[コールルーティング（Call Routing）] > [ダイヤルルール（Dial Rules）] > [SIPダイヤルルール（SIP Dial Rules）]**.を選択します。

ステップ 2 [SIP ダイヤル ルールの検索と一覧表示（Find and List SIP Dial Rules）]ウィンドウで、[検索（Find）]をクリックし、適切な SIP 電話機を同期する既存の SIP ダイヤル ルールを選択します。

ステップ 3 追加の設定変更を行い、**[SIPダイヤルルールの設定（SIP Dial Rule Configuration）]** で **[保存（Save）]** をクリックします。

ステップ 4 **[設定の適用（Apply Config）]** をクリックします。

ステップ 5 **OK**をクリックします。

ダイヤル ルールの優先順位の変更

[ダイヤル ルールの設定（Dial Rule Configuration）]ウィンドウでダイヤル ルールの優先順位を追加およびソートするには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager から**コールルーティング** > **ダイヤルルール**.を選択します。

ステップ 2 次のいずれかを選択します。

- **[アプリケーション ダイヤル ルール（Application Dial Rules）]**
- **[ディレクトリ検索ダイヤル ルール（Directory Lookup Dial Rules）]**
- **[SIP ダイヤル ルール（SIP Dial Rules）]**

ステップ 3 [検索と一覧表示（Find and List）] ウィンドウで、ダイヤル ルールを選択し、ダイヤル ルールの名前をクリックします。
[ダイヤル ルールの設定（Dial Rule Configuration）]ウィンドウが表示されます。

ステップ 4 上矢印と下矢印を使用して、リスト内でダイヤル ルールを上または下に移動します。

ステップ 5 順序の優先順位付けが完了したら、[保存（Save）]をクリックします。

連携動作と制限事項

SIP ダイヤル ルールの連携動作

SIP ダイヤル ルールの連携動作

Cisco Unified IP 電話	データのやり取り
SIP を実行する 7911、7941、7961、7970、および 7971。	これらの電話機は、7940_7960_OTHER ダイヤル ルール パターンを使用します。 キー プレス マークアップ言語（KPML）では、Cisco Unified Communications Manager に数字を 1 桁ごとに送信できます。 SIP ダイヤル ルールを使用すると、Cisco Unified Communications Managerに送信する前に、電話で数字のパターンをローカルに収集できます。 SIP ダイヤル ルールを設定しないと、KPML が使用されます。 Cisco Unified Communications Manager のパフォーマンスを向上させる（処理されるコールの数を増やす）には、管理者が SIP ダイヤル ルールを設定することをお勧めします。

Cisco Unified IP 電話	データのやり取り
SIP を実行している7940 および 7960	これらの電話機は 7940_7960_OTHER ダイヤル ルール パターンを使用し、KPML をサポートしていません。 これらの電話機で SIP のダイヤル プランを設定していないと、ユーザは数字が Cisco Unified Communications Manager に送信されて処理される前に、指定された時間だけ待機する必要があります。 その結果、実際のコールの処理が遅延します。

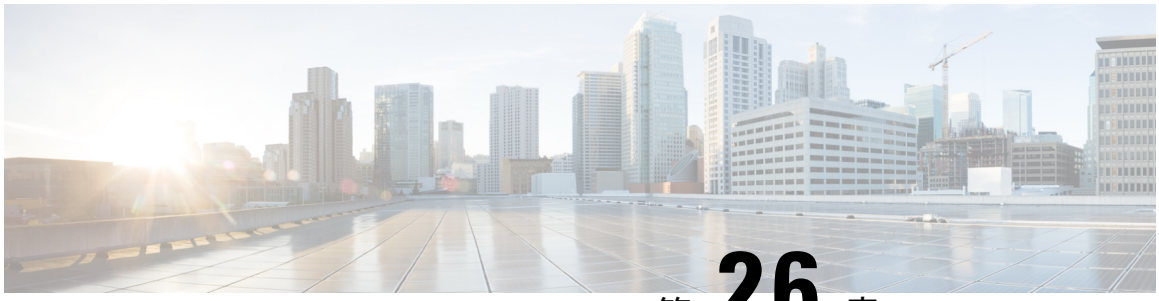
ディレクトリ検索ダイヤル ルールの制限事項

ディレクトリ検索ダイヤル ルールの制限事項

フィールド	制約事項
[開始番号（Number Begins With）]	このフィールドでは、数字と文字 +、*、# のみを使用できます。 長さは 100 文字以内でなければなりません。
[桁数（Number of Digits）]	このフィールドは数字のみをサポートします。このフィールドの値は、パターン フィールドに指定されているパターンの長さより小さくすることはできません。
[削除する合計桁数（Total Digits to be Removed）]	このフィールドは数字のみをサポートします。このフィールドの値は、[桁数（Number of Digits）]フィールドの値より大きくすることはできません。
[プレフィックス パターン（Prefix with Pattern）]	このフィールドでは、数字と文字 +、*、# のみを使用できます。 長さは 100 文字以内でなければなりません。 （注） 1 つのダイヤル ルールの [削除する合計桁数（Total Digits to be Removed）]フィールドと [プレフィックス パターン（Prefix With Pattern）]フィールドの両方を空白にすることはできません。

第 III 部

アプリケーションの統合



第 26 章

シスコ アプリケーションの統合

Cisco Unity Connection

ボイスメールとメッセージングのシステムを設定する時には、ユーザの追加、機能の有効化、Cisco Unified Communications Manager と Cisco Unity Connection との統合の各オプションに注意します。

Cisco Unity Communications Manager と統合されると、Cisco Unity Connection (ボイスメールおよびメッセージングシステム) は、AXL サービスまたは LDAP 統合を使用して手動で設定するユーザにボイスメッセージ機能を提供します。メールボックスにボイスメッセージを受信すると、ユーザの電話機にメッセージ受信のライトが点灯します。ユーザは内線または外線通話でボイスメッセージシステムにアクセスして、メッセージの取得、聞き取り、返信、転送、および削除ができます。

お客様のシステムは、直接接続されたメッセージシステムとゲートウェイベースのメッセージシステムをサポートしています。直接接続された音声メッセージシステムは、パケットプロトコルを使用してCisco Unified Communications Managerと通信します。ゲートウェイベースのボイスメッセージ システムは、シスコ ゲートウェイに接続するアナログまたはデジタル トランクを使用してCisco Unified Communications Managerに接続します。

Unified Communications Manager と Cisco Unity Connection を統合すると、ユーザに次の機能を設定できます。

- パーソナル グリーティングへの自動転送
- 通話中グリーティングへの自動転送

- 発信者 ID
- 容易なメッセージ アクセス（ユーザはIDを入力しなくてもメッセージを取得できます。Cisco Unity Connectionでは、通話発信元の内線番号に基づいてユーザを識別します。パスワードが必要になる場合があります）
- 識別されたユーザのメッセージ（Cisco Unity Connectionでは、転送された内線通話中にメッセージを残したユーザを、通話発信元の内線番号に基づいて自動的に識別します）
- メッセージ待機インジケータ（MWI）
- Cisco Unified Communications Manager と Cisco Unity Connection サーバ間のセキュアな SIP トランクの統合の設定には、Cisco Unified Communications Manager クラスタが混合モードで設定されている必要があります。

Cisco Unified Communications Manager と Cisco Unity Connection は、次のいずれかのインターフェイスを介して連携します。

- SIP トランク：SIP を使用して Cisco Unity Connection と Unified Communications Manager を統合できます。SIP は、従来の統合に含まれている複数の SCCP ポートではなく、Unity Connection サーバにつき 1 個のトランクを使用します。SIP インテグレーションでは、ボイスメールポートとメッセージ待機インジケータ (MWI) のディレクトリ番号を設定する必要がなくなります。
- SCCPプロトコル：音声メールポートを作成することで、インタフェースを直接接続された音声メッセージシステムとして構成できます。これらは、Unified CommunicationsManagerとCisco Unity Connectionとの間にリンクを確立します。

  ボイスメッセージ システムへの複数の同時コールを処理するには、複数のボイスメールポートを作成し、それらのポートを回線グループに割り当て、その回線グループをルート/ハントリストに割り当てます。

  Cisco Unified Communications Manager は、SCCP メッセージを生成します。 Cisco Unity Connection がそのメッセージを変換します。ボイスメールシステムは、メッセージ待機の on と off の番号をコールしてメッセージ受信兆候 (MWIs) を送信します。

  ボイスメール ポートやCisco Unity SCCPデバイスにセキュリティを設定すると、各デバイスが他のデバイスの証明書を受け付けた後、認証済みのデバイスに対してTLS接続（ハンドシェイク）が開きます。同様に、デバイスに暗号化を設定した場合、システムはデバイス間に SRTP ストリームを送信します。

  デバイスのセキュリティモードが認証または暗号化に設定されている場合、Cisco Unity TSP は、Cisco Unified Communications Manager の TLS ポートを介して Unified Communications Manager に接続します。セキュリティ モードが非セキュアの場合、Cisco Unity TSP は Cisco Unified Communications Manager の SCCP ポートを介して Unified Communications Manager に接続します。

Cisco Unity Connection をシステムに統合する設定の詳細については、『*Cisco Unity Connection* 向け *Cisco Unified Communications Manager SCCP* インテグレーション ガイド』または『*Cisco Unity Connection* 向け *Cisco Unified Communications Manager SIP* トランク インテグレーション

ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html）を参照してください。

PIN同期の有効化

PIN 同期を有効にし、エンド ユーザが、エクステンション モビリティ、開催中の会議、モバイル コネクト、および Cisco Unity Connection ボイスメールに同じ PIN を使用してログインできるようにするには、次の手順を実行します。

（注） Cisco Unified Communications Manager パブリッシャ データベース サーバが実行されており、そのデータベースのレプリケーションが完了した場合のみ、Cisco Unity Connection と Cisco Unified Communications Manager 間の PIN の同期に成功します。Cisco Unity Connection で PIN の同期に失敗すると、次のエラーメッセージが表示されます。「CUCMで暗証番号のアップデートに失敗しました。（Failed to update PIN on CUCM.）原因：PIN の取得中にエラーが発生しています。（Reason: Error getting the pin.）」

PIN 同期が有効で、エンドユーザーが PIN を変更した場合は、Cisco Unified Communications Manager で PIN を更新します。この現象は、少なくとも 1 つの構成済みの Unity Connection アプリケーション サーバで、PIN の更新が成功している場合に発生します。

（注） PIN の同期を有効にするには、機能が正常に有効化された後で、管理者がユーザに各自の PIN を変更するよう強制する必要があります。

始める前に

この手順では、すでにアプリケーションサーバが Cisco Unity Connection のセットアップに接続されていることを前提としています。使用していない場合、新しいアプリケーションサーバを追加する方法については、「関連項目」を参照してください。

PIN 同期機能を有効にするには、まず [Cisco Unified OSの管理（Cisco Unified OS Administration）] ページから Cisco Unified Communications Manager tomcat-trust に、有効な証明書をアップロードする必要があります。証明書をアップロードする方法の詳細については、「Cisco Unified Communications Manager アドミニストレーション ガイド」（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）の「セキュリティ証明書の管理」の章を参照してください。

Cisco Unity Connection サーバのユーザ ID は、Cisco Unified Communications Manager のユーザ ID と一致する必要があります。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [アプリケーションサーバ（Application Servers）]** を選択します。

ステップ 2 Cisco Unity Connection をセットアップするアプリケーション サーバを選択します。

ステップ 3 [エンドユーザのPIN同期（Enable End User PIN Synchronization）] チェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

アプリケーション サーバの設定

Cisco Expressway

Cisco Unified Communications Manager は Cisco Expressway と統合して、Cisco Unified Communications Mobile & Remote Access を提供します。Cisco Unified Communications の Mobile & Remote Access は Cisco Collaboration Edge アーキテクチャの中核を成します。Cisco Jabber などのエンドポイントが企業ネットワーク外にある場合に、Cisco Unified Communications Manager（Unified CM）への登録、呼制御、プロビジョニング、メッセージング、およびプレゼンスの機能を使用することができるようになります。Expressway は、Unified CM 登録にセキュアなファイアウォール トラバーサルと回線側サポートを提供します。

ソリューション全体で、次の機能が提供されます。

- オフプレミス アクセス：ネットワーク外で、Cisco Jabber および EX/MX/SX シリーズ クライアントに一貫性のあるエクスペリエンスを提供
- セキュリティ：セキュアな企業間（B2B）通信
- クラウドサービス：エンタープライズクラスの柔軟性と拡張性に優れたソリューションにより、Webex の統合とさまざまなサービスプロバイダーに対応
- ゲートウェイおよび相互運用性サービス：メディアおよびシグナリングの正規化、標準以外のエンドポイントのサポート。

導入の詳細については、『*Cisco Expressway* 経由の *Mobile and Remote Access* 導入ガイド』（https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html）を参照してください。

Cisco Emergency Responder

Cisco Emergency Responder（Emergency Responder）は、緊急コールに効率的に応答したり、緊急コールの処理について地方自治体の規定を順守したりできるように、テレフォニー ネット

ワークで緊急コールを管理するのに役立ちます。北米では、これらの地方条例は「Enhanced 911（E911）」と呼ばれています。同様の規定が他の国やロケールに存在します。

緊急コールに関する条例は、国、地域、州、または都市圏の中でも場所によって異なることがあるため、Emergency Responder は、特定のローカル要件に併せて緊急コール設定を指定できる柔軟性を備えています。ただし、条例は場所によって異なり、セキュリティ要件は会社によって異なるため、Emergency Responder を展開する前に、自社のセキュリティ上のニーズと法的なニーズを調査する必要があります。

Cisco Emergency Responder をインストールして Cisco Unified Communications Manager と統合する方法の詳細については、『*Cisco Emergency Responder* アドミニストレーション ガイド』（https://www.cisco.com/c/en/us/support/unified-communications/emergency-responder/products-maintenance-guides-list.html）を参照してください。

Cisco Unified Communications Manager での機能のサポート

Cisco Unified Communications Manager の次の機能は、Cisco Emergency Responder との統合をサポートしています。Cisco Unified Communications Manager でこれらの機能を設定する方法の詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』（https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html）を参照してください。

- ロケーション認識
- 緊急ハンドラ

Cisco Paging Server

Cisco Unified Communications Manager は、Cisco Paging Server と統合して Cisco IP Phone やさまざまなエンドポイントに基本的なページング サービスを提供するように設定できます。Cisco Paging Server 製品は、InformaCast 仮想アプライアンスを介して提供され、次の導入オプションを提供します。

- 基本的なページング：Cisco IP Phone に対して電話間およびグループでのライブオーディオページングを提供します。システムのすべてのユーザは、基本的なページの確立と受信に参加できます。
- 高度な通知：すべての機能を備えた緊急通知ソリューションを提供します。これにより、テキストと、ライブまたは事前に録音されたオーディオメッセージを使用して、無制限の数の電話機に到達できます。

Cisco Paging Server の詳細およびドキュメントについては、https://www.cisco.com/c/en/us/products/unified-communications/paging-server/index.html を参照してください。

構成

Cisco Unified Communications Manager の基本ページングまたは高度な通知の設定方法の詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』の「ページング」の章を参照してください。

Cisco Unified Contact Center Enterprise

Cisco Unified Contact Center Enterprise（Unified CCE）をシステムで使用して、インテリジェントコールルーティング、ネットワークとデスクトップ間のコンピュータ/テレフォニー インテグレーション（CTI）、およびIP ネットワークを介したコンタクトセンターエージェントへのマルチチャネル コンタクト管理を統合します。Unified CCE は、ソフトウェア IP の自動コール配布 (ACD) を Cisco Unified Communications と組み合わせたもので、詳細な分散型の連絡先センターを迅速に導入できます。

Unified CCE をシステムに統合するための設定方法の詳細については、『*Cisco Unified Contact Center Enterprise* 設置およびアップグレードガイド』（http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html）を参照してください。

Cisco Unified Contact Center Express

Cisco Unified Contact Center Express（Unified CCX）は、シングルまたはデュアルサーバの導入において、パッケージ化された大規模なコンタクトセンターの機能をシステムに提供します。Unified CCX は、最大 400 人の同時エージェント、42 人のスーパバイザ、150 のエージェントグループ、および150のスキルグループに対応するように拡張できます。また、電子メール、チャット、発信コール、着信コール、ワークフォース最適化、およびレポート機能が含まれています。

Unified CCX は、Unified CCX に代わってすべてのコンタクトセンターのコールを管理する Unified Communications Manager と連携します。コールがヘルプデスクに送信されると、コールシステムは、その番号が Unified CCX アプリケーションサーバを宛先としていることを認識します。この設定では、Unified CCX が着信コールを受信し、ダイヤルした内線番号に基づいて要求を処理します。スクリプトは、番号を収集し、必要に応じて、発信者からの情報を使用して適切なエージェントを選択します。割り当てられたエージェントが利用できない場合、そのコールは適切なキューに入れられ、録音されたメッセージまたは音楽が発信者にストリーミングされます。エージェントが対応可能になるとすぐに、Unified CCX はそのエージェントの電話を鳴らすように Unified Communications Manager に指示します。

エージェントが電話に出ると、関連するコールコンテキストがそのエージェントのデスクトップアプリケーションに提供されます。この手順により、顧客をサポートするための適切な情報がエージェントに表示されます。

Unified CCE をシステムに統合するための設定方法の詳細については、『*Cisco Unified CCX* アドミニストレーション ガイド』（http://www.cisco.com/c/en/us/support/customer-collaboration/

unified-contact-center-express/products-installation-and-configuration-guides-list.html）を参照してください。

高度な QoS APIC-EM コントローラ

APIC EMは、ネットワークトラフィックを集中管理するためのシステムを提供しているため、ネットワークの輻輳がある場合でも、常に通信を維持できるようになっています。 Cisco Unified Communications Manager を設定して、APIC-EM コントローラを使用し SIP メディアフローを管理するように設定すると、次のような利点がもたらされます。

- QoS 管理を一元化し、エンドポイントによる DSCP 値の割り当てが不要になります。
- メディア フローごとに異なる QoS 処理を適用できます。 たとえば、ネットワーク帯域幅が少ない場合でも、基本的な音声通信が常に維持されるように、オーディオの優先順位を付けることができます。
- SIP プロファイルの外部 QoS 設定では、APIC-EM を使用するようにユーザを設定できます。 たとえば、Cisco Jabber のユーザが、APIC-EM Ber を使用してメディアフローを管理しているときに、Cisco Unified IP 電話ユーザが Cisco Unified Communications Manager の DSCP 設定を使用している場合があります。

設定の詳細

APIC_EM コントローラと連携動作するように Cisco Unified Communications Manager を設定する方法を含め、詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』の「APIC-EM コントローラによる QoS の設定」の章を参照してください。

Cisco WebDialer サーバの設定

[WebDialersの一覧（List of WebDialers）] サービスパラメータの代わりに Cisco WebDialer アプリケーションサーバを設定して、ユーザが入力できる文字数を制限します。[アプリケーションサーバの設定（Application Server Configuration）] ウィンドウで Cisco WebDialer アプリケーションサーバを追加すると、Cisco WebDialer Web サービスの [サービスパラメータの設定（Service Parameter Configuration）] ウィンドウで、そのサーバが [WebDialersの一覧（List of WebDialers）] フィールドに表示されます。Cisco WebDialer の設定の詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html）を参照してください。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[アプリケーションサーバ（Application Server）]** を選択します。

ステップ 2 [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 サーバ タイプ**ドロップダウン リストから、**Cisco Web Dialer**を選択し、**次へ**をクリックします。

ステップ 4 **ホスト名/IP アドレス**フィールドに、サーバのホスト名またはIPアドレスを入力します。

ステップ 5 **[リダイレクタノード（Redirector Node）]** ドロップダウンリストから、**[< None >]** か、特定の Unified Communications Manager ノードを選択します。

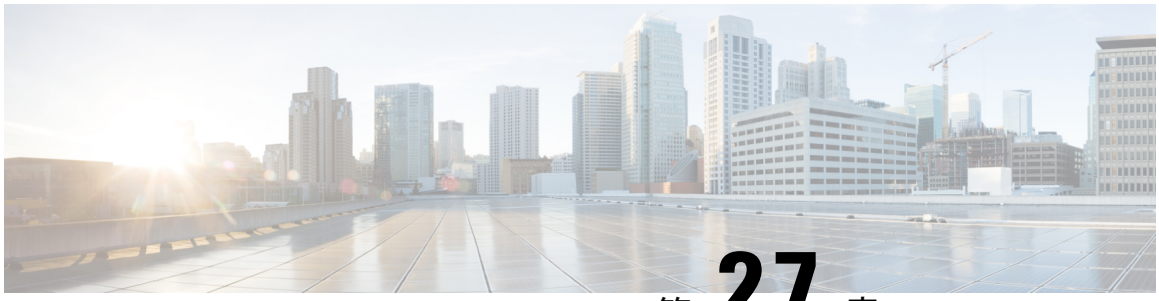
< None > を選択すると、WebDialer サーバがすべてのノードに適用されます。

ステップ 6 **[保存]** をクリックします。

ステップ 7 Cisco Unified Serviceability で**[ツール（Tools）]**>**[コントロール センター - 機能サービス（Control Center - Feature Services）]** を選択します。

ステップ 8 **Cisco WebDialer Web Service**ラジオボタンをクリックします。

ステップ 9 **再起動（Restart）**をクリックします。



第 27 章

CTI アプリケーションの設定

CTI アプリケーションの概要

コンピュータテレフォニーインテグレーション（CTI）を使用して、コンピュータ処理機能を活用しながら、電話コールの発信、受信、および管理を行うことができます。 CTIアプリケーションを使用すると、発信者 ID を使用してデータベースから顧客情報を取得したり、対話式音声自動応答 (IVR) で収集した情報を使用して、顧客のコールをその情報とともに、適切なカスタマーサービス担当者にルートすることができます。

コールのメディアをルートポイントで終端するアプリケーションは、コール単位でコールのメディアおよびポートを指定する必要があります。 CTI アプリケーションは、静的な IP アドレスまたは動的な IP アドレスとポート番号を使用して、CTI ポートおよび CTI ルートポイントでメディアを終了させることができます。

この章では、Cisco Unified Communications Manager を CTI アプリケーションとともに動作するように設定する方法について説明します。 特定のアプリケーションの設定方法については、『*Cisco Unified Communications Manager* 機能設定ガイド』を参照してください。

利用可能な Cisco CTI アプリケーションの一部を次に示します。

- デスクトップ アプリケーションである Cisco IP Communicator は、コンピュータを多機能型の電話機に変換し、コール追跡、デスクトップ コラボレーション、オンライン ディレクトリからのワンクリック ダイヤリングなどの利点を追加します。
- Cisco Unified Communications Manager 自動応答：Unified Communications Manager と連携して、特定の内線電話番号でコールを受信し、発信者が適切な内線番号を選択できるようにします。
- Cisco Web Dialer：Cisco Unified IP 電話ユーザは ウェブ およびデスクトップ アプリケーションからコールを発信できます。

- Cisco Unified Communications Manager Assistant：マネージャとそのアシスタントがより効果的に協力して作業できます。 この機能は、コール ルーティング サービス、マネージャおよびアシスタント用の電話機拡張機能、および主にアシスタントが使用するアシスタント コンソール インターフェイスから構成されています。

（注） どの Unified Communications Manager CTI アプリケーションが SIP IP Phone をサポートしているかを確認するには、アプリケーション固有のマニュアルを参照してください。

CTI ルート ポイントの概要

CTIルート ポイント仮想デバイスは、アプリケーションによって制御されるリダイレクトのための複数の同時コールを受信できます。 ユーザがアプリケーションにアクセスするためにコールできる CTI ルート ポイント上で 1 つ以上の回線を設定できます。 アプリケーションはルート ポイントでコールに応答することができ、コールを CTI ポートまたは IP Phone にリダイレクトすることもできます。 CTIアプリケーションがリダイレクト API を使用してコールをリダイレクトすることを要求した場合、Cisco Unified Communications Manager は、リダイレクト先の通話者のために回線/デバイス コーリングサーチスペースの設定を使用します。

CTI ルートポイントでは、次のことができます。

- コールに応答する
- 複数のアクティブなコールの発信および受信
- コールのリダイレクト
- コールの保留
- コールの保留解除
- コールのドロップ

Cisco Unified Communications Manager の CTI 冗長性

クラスタ内の Unified Communications Manager ノードに障害が発生した場合、CTIManager は、影響を受けた CTI ポートおよびルート ポイントを別の Unified Communications Manager ノードで開き直すことによって、これらのデバイスを回復します。 アプリケーションによって電話デバイスが開かれていた場合、その電話が別の Unified Communications Manager にフェールオーバーしたときに CTIManager がその電話を開き直します。 Cisco IP 電話が別の Unified Communications Manager にフェールオーバーしない場合、CTIManager は、その電話または電話機の回線を開くことができません。 CTIManager は、デバイス プールに割り当てられている Unified Communications Manager グループを使用して、アプリケーションによって開かれた CTI デバイスと電話を回復するのにどの Unified Communications Manager を使用するかを決定します。

CTIManager 上の CTI 冗長性

CTIManagerに障害が発生した場合、そのCTIManagerに接続されているアプリケーションは、これらのデバイスを別の CTIManager 上で再度開くことによって、影響を受けたリソースを回復できます。アプリケーションは、そのアプリケーションの設定時にプライマリとバックアップとして定義されたCTIManagerに基づいて、どのCTIManagerを使用するかを決定します（そのアプリケーションによってサポートされている場合）。アプリケーションは、新しい CTIManager に接続すると、以前に開かれたデバイスと回線を再度開くことができます。アプリケーションは、電話が新しい Unified Communications Manager にリホームする前であれば Cisco IP Phone を開き直すことができますが、リホームが完了するまではその電話を制御できません。

（注） プライマリ CTIManagerが作動状態に戻っても、アプリケーションはそのCTIManagerにリホームしません。アプリケーションがプライマリ CTIManagerにフォールバックするのは、そのアプリケーションを再起動するか、またはバックアップCTIManagerに障害が発生した場合です。

アプリケーション障害の CTI 冗長性

アプリケーション（TAPI/JTAPI、または CTIManager に直接接続されているアプリケーション）に障害が発生した場合、CTIManager はそのアプリケーションを閉じ、CTI ポートおよびルート ポイントでまだ終了していないコールを、設定された Call Forward On Failure（CFOF）番号にリダイレクトします。 CTIManager はまた、そのアプリケーションが回復してこれらのデバイスを再登録するまで、これらのCTIポートおよびルートポイントへの後続のコールを、設定された Call Forward No Answer（CFNA）番号にルーティングします。

CTI アプリケーションの前提条件

CTI アプリケーション用に Cisco Unified Communications Manager を設定する前に、デバイス プールを設定しておく必要があります。

CTI アプリケーションごとに IP Phone を追加して設定します。 IP 電話を追加して設定する方法の詳細については、「Cisco Unified IP Phone」を参照してください。

CTI アプリケーションを使用するエンド ユーザとアプリケーション ユーザを設定する

コンピュータ テレフォニー統合（CTI）では、IPv4 アドレスと IPv6 アドレスをサポートできる JTAPI および TAPI インターフェイスを通して IP アドレス情報が提供されます。 IPv6 アドレスをサポートする必要がある場合は、アプリケーションが IPv6 をサポートする JTAPI/TAPI クライアントインターフェイスバージョンを使用していることを確認してください。

CTI アプリケーション タスク フローの設定

CTI アプリケーション用に Cisco Unified Communications Manager を設定するには、次のタスクに従います。

手順

	コマンドまたはアクション	目的
ステップ 1	CTIManager サービスの有効化 （331 ページ）	アクティブになっていない場合、適切なサーバで CTIManager サービスをアクティブにします。
ステップ 2	CTIManager と Cisco Unified Communications Manager のサービス パラメータの設定 （331 ページ）	CTI のスーパー プロバイダー機能と連携して使用される CTIManager のクラスタ全体の高度サービス パラメータを設定します。
ステップ 3	CTI ルート ポイントを設定するには、次の手順を実行します。 • CTI ルート ポイントの設定 （332 ページ） • 新しいコール受け付けタイマーの設定 （333 ページ） • 同時アクティブ通話の設定 （333 ページ） • CTI ルート ポイントの同期化 （334 ページ）	アプリケーション制御のリダイレクションに複数の同時コールを受信できる 1 つ以上の CTI ルート ポイントの仮想デバイスを設定します。
ステップ 4	CTIのデバイスのディレクトリ番号を設定 （334 ページ）	CTIデバイスのディレクトリ番号を設定します。
ステップ 5	デバイスとグループの関連付け （335 ページ）	アプリケーション ユーザとエンド ユーザがアプリケーションで使用するすべてのデバイスを、適切な Cisco Unified Communications Manager グループに関連付けます（デバイス プール経由）。
ステップ 6	エンドユーザとアプリケーション ユーザの追加 （335 ページ）	Cisco Unified Communications Manager システムで Standard CTI Enabled ユーザ グループにエンドユーザとアプリケーション ユーザを追加することで設定されている CTI 制御可能なデバイスを CTI アプリケーションが制御できます。

	コマンドまたはアクション	目的
ステップ 7	（任意） アプリケーション障害に対する CTI の冗長性を設定 （337 ページ）	CTIManager が 2 つの連続した間隔内でアプリケーションからメッセージを受信することが予想されるインターバルを定義するには、次のようにします。

CTIManager サービスの有効化

手順

ステップ 1 Cisco Unified 有用性で、**[Tools]** > **[Service Activation]** の順に選択します。
ステップ 2 [サーバ（Server）]ドロップダウン リストからノードを選択します。
ステップ 3 CM Services セクションの **[Cisco CTIManager]** チェックボックスをオンにします。
ステップ 4 **[保存]** をクリックします。

CTIManager と Cisco Unified Communications Manager のサービス パラメータの設定

CTI のスーパー プロバイダー機能と連携して使用される CTIManager のクラスタ全体の高度サービス パラメータを設定します。

（注） 設定した限度を超えた場合、CTI がアラームを生成しますが、アプリケーションは追加デバイスの処理を続行します。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** の順に選択します。
ステップ 2 [サーバ（Server）]ドロップダウン リストからノードを選択します。
ステップ 3 [サービス（Service）]ドロップダウン リストから [Cisco CTIManager（アクティブ）（Cisco CTIManager（Active））] を選択します。
ステップ 4 [サービスパラメータの設定（Service Parameter Configuration）]ウィンドウで、[詳細設定（Advanced）]をクリックします。

ステップ 5 [プロバイダーあたりの最大デバイス数（Maximum Devices Per Provider）]フィールドに、単一の CTI アプリケーションが開くことのできるデバイスの最大数を入力します。 デフォルトは 2000 デバイスです。

ステップ 6 [ノードあたりの最大デバイス数（Maximum Devices Per Node）] フィールドに、Unified Communications Manager システム内の任意の CTIManager ノード上ですべての CTI アプリケーションが開くことのできるデバイスの最大数を入力します。 デフォルトは 800 デバイスです。

ステップ 7 **[保存]** をクリックします。

CTI ルート ポイントのタスク フローの設定

手順

	コマンドまたはアクション	目的
ステップ 1	CTI ルート ポイントの設定 （332 ページ）	新規の CTI ルート ポイントを追加するか、既存のポイントを変更します。
ステップ 2	新しいコール受け付けタイマーの設定 （333 ページ）	コールがルート ポイントに到着したとき、アプリケーションが指定時間内に処理（受信、応答、リダイレクト）するように新しいコール受け入れタイマーを設定します。
ステップ 3	同時アクティブ通話の設定 （333 ページ）	ルート ポイントの同時アクティブ コール数を設定します。
ステップ 4	**オプション**：CTI ルート ポイントの同期化 （334 ページ）	同期して、CTI ルート ポイントに最新の設定変更を反映させます。割り込みを最小限に抑えて、適用されていない設定を適用します （たとえば、影響を受けるデバイスの一部でリセットまたは再起動を行う必要がない場合があります）。

CTI ルート ポイントの設定

新規の CTI ルート ポイントを追加するか、既存のポイントを変更します。

手順

ステップ 1 Cisco Unified CM Administration から **[デバイス（Device）]** > **[CTIルートポイント（CTI Route Point）]** の順にクリックします。

ステップ 2 次のいずれかの作業を実行します。

- **[新規追加（Add New）]**をクリックして新しいゲートウェイを追加します。
- 既存の CTI ルートポイントの設定を変更するには、**[検索（Find）]** をクリックし、結果のリストから CTI ルートポイントを選択して、検索条件を入力します。

ステップ 3 **CTI ルートポイントの設定**ウィンドウでフィールドを設定します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 4 **[保存]** をクリックします。

新しいコール受け付けタイマーの設定

コールがルート ポイントに到着したとき、アプリケーションが指定時間内に処理（受信、応答、リダイレクト）するように新しいコール受け入れタイマーを設定します。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** を選択します。

ステップ 2 [サーバ（Server）]ドロップダウン リストからノードを選択します。

ステップ 3 [サービス（Service）] ドロップダウン リストから [Cisco CallManager（アクティブ）（Cisco CallManager (Active)）]を選択します。

ステップ 4 [CTIの新しいコール受け付けタイマー（CTI New Call Accept Timer）]フィールドで、コールの応答を許可する時間を指定します。 デフォルト値は 4 です。

ステップ 5 **[保存]** をクリックします。

同時アクティブ通話の設定

ルート ポイントの同時アクティブ コール数を設定します。

（注） TAPI アプリケーションを使用し、Cisco CallManager Telephony Service Provider（TSP）を使用して CTI ポート デバイスを制御することを計画している場合は、CTI ポート デバイスごとに 1 つの回線を設定するだけで済みます。

手順

ステップ 1 Cisco Unified CM Administration から、**[コール ルーティング（Call Routing）]** > **[ディレクトリ番号（Directory Number）]** をクリックします。

ステップ 2 [ディレクトリ番号の設定（Directory Number Configuration）] ウィンドウで、[新規追加（Add New）] をクリックします。

ステップ 3 必須フィールドに入力します。

ステップ 4 **[保存]** をクリックします。

CTI ルート ポイントの同期化

同期して、CTI ルート ポイントに最新の設定変更を反映させます。割り込みを最小限に抑えて、適用されていない設定を適用します（たとえば、影響を受けるデバイスの一部でリセットまたは再起動を行う必要がない場合があります）。

手順

ステップ 1 Cisco Unified CM Administration から **[デバイス（Device）]** > **[CTIルートポイント（CTI Route Point）]** の順にクリックします。

ステップ 2 **[CTI ルートポイントの検索と一覧表示]** ウィンドウで、**[検索（Find）]**をクリックして、CTI ルートポイントの一覧を表示します。

ステップ 3 同期させる CTI ルート ポイントの横にあるチェックボックスをオンにします。 ウィンドウ内の CTI ルート ポイントをすべて選択するには、検索結果表示のタイトルバーにあるチェックボックスをオンにします。

ステップ 4 [選択項目への設定の適用（Apply Config to Selected）]をクリックします。

ステップ 5 **OK**をクリックします。

CTIの デバイスのディレクトリ番号を設定

CTI デバイスのディレクトリ番号を設定します。

手順

ステップ 1 Cisco Unified CM Administration から、**[コール ルーティング（Call Routing）]** > **[ディレクトリ番号（Directory Number）]** の順に選択します。

ステップ 2 [ディレクトリ番号の検索と一覧表示（Find and List Directory Numbers）]ウィンドウで、[新規追加（Add New）]をクリックします。

ステップ 3 [ディレクトリ番号の設定（Directory Number Configuration）]ウィンドウで、必要なフィールドを入力します。

ステップ 4 **[保存]** をクリックします。

デバイスとグループの関連付け

アプリケーションユーザとエンドユーザがアプリケーションで使用するすべてのデバイスを、適切な Cisco Unified Communications Manager グループに関連付けます（デバイス プール経由）。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザの管理（User Management）] > [アプリケーション ユーザ（Application User）]** をクリックします。

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（Add New）]** 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 [デバイス情報（Device Information）] ペインで、[使用可能なデバイス（Available Devices）] リストから [制御するデバイス（Controlled Devices）] リストに移動して、デバイスを関連付けます。

ステップ 4 **[保存]** をクリックします。

ステップ 5 エンド ユーザのデバイスを関連付けるには、**[ユーザの管理（User Management）] > [エンド ユーザ（End User）]** をクリックします。

ステップ 6 ステップ 2 ～ 4 を繰り返します。

エンドユーザとアプリケーション ユーザの追加

Cisco Unified Communications Manager システムで Standard CTI Enabled ユーザ グループにエンド ユーザとアプリケーション ユーザを追加することで設定されている CTI 制御可能なデバイスを CTI アプリケーションが制御できます。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [アクセス制御グループ（Access Control Group）]** をクリックします。

ステップ 2 [アクセス制御グループの検索と一覧表示（Find and List Access Control Groups）]ウィンドウで、[検索（find）]をクリックして、アクセス制御グループの現在のリストを表示します。

ステップ 3 [標準 CTI を有効にする（Standard CTI Enabled）]をクリックすると、このグループの [アクセス制御グループの設定（Access Control Group Configuration）] ウィンドウが表示されます。 すべての CTI ユーザが [標準 CTI を有効にする（Standard CTI Enabled）] ユーザ グループに含まれることを確認します。使用可能なグループとその機能の完全な一覧については、「アクセス制御グループ設定のオプション」を参照してください。

ステップ 4 エンド ユーザを追加する場合は、[グループにエンド ユーザを追加（Add End Users to Group）] をクリックします。アプリケーション ユーザを追加する場合は、[アプリケーション ユーザをグループに追加（Add App Users to Group）]をクリックします。

ステップ 5 [検索（Find）]をクリックして現在のユーザの一覧を表示します。

ステップ 6 [標準 CTI を有効にする（Standard CTI Enabled）] ユーザ グループに割り当てるユーザのチェックボックスをオンにします。

ステップ 7 **[選択項目の追加(Add Selected)]** をクリックします。

アクセス制御グループの設定オプション

（注） CTI アプリケーションは、割り当て先の指定されたユーザグループをサポートしている必要があります。

（注） Standard CTI Allow Control of All Devices ユーザ グループに関連付けられているユーザは、Standard CTI Secure Connection ユーザ グループにも関連付けることをお勧めします。

（注） 次の表に示すロールをすべて適切に機能させるには、**[制御するデバイス（Controlled Devices）]** で特定のデバイスを追加する必要があります。

フィールド	説明
標準 CTI 通話モニタリング許可	このユーザ グループでは、アプリケーションがコールをモニタできます。
標準 CTI コール パーク モニタリング許可	このユーザ グループでは、コールがすべてのコール パーク ディレクトリの番号にパーク/パーク解除されるとき、アプリケーションが通知を受信できます。
標準 CTI 通話録音許可	このユーザ グループでは、アプリケーションがコールを記録できます。
標準 CTI 発信者番号の変更許可	このユーザ グループでは、サポートされている CTI アプリケーションの発信側番号をアプリケーションが変更できます。
[標準 CTI によるすべてのデバイスの制御（Standard CTI Allow Control of All Devices）]	このユーザ グループでは、システムの CTI 制御可能なデバイスをアプリケーションが制御またはモニタできます。

フィールド	説明
標準 CTI SRTP 重要素材の受信許可	このユーザ グループでは、暗号化されたメディアのストリームの復号に必要な情報をアプリケーションが受け取ることができます。 通常、このグループは記録およびモニタのために使用されます。
[標準CTIを有効にする（Standard CTI Enabled）]	すべての CTI アプリケーションに必要なこのユーザ グループでは、アプリケーションが Cisco Unified Communications Manager に接続し、CTI の機能を利用できます。
標準 CTI セキュア接続	このグループに入るためには、アプリケーションが Cisco Unified Communications Manager にセキュア（TLS）な CTI 接続が可能で、Cisco Unified Communications Manager のクラスタのセキュリティが有効になっていることが必要です。

アプリケーション障害に対する CTI の冗長性を設定

CTI Manager が 2 つの連続した間隔内でアプリケーションからメッセージを受信することが予想されるインターバルを定義するには、次のようにします。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** を選択します。

ステップ 2 [サーバ（Server）]ドロップダウン リストからノードを選択します。

ステップ 3 **[サービス（Service）]** ドロップダウンリストから **[Cisco CTI Manager（アクティブ）（Cisco CTIManager（Active））]** を選択します。

ステップ 4 [サービスパラメータの設定（Service Parameter Configuration）]ウィンドウで、[詳細設定（Advanced）]をクリックします。

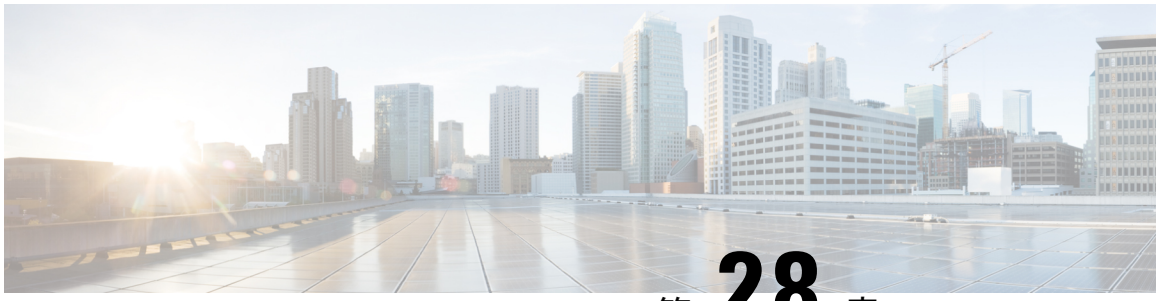
ステップ 5 [アプリケーションハートビート最小間隔（Application Heartbeat Minimum Interval）]フィールドに、最小間隔の時間を入力します。 デフォルトは 5 です。

ステップ 6 [アプリケーションハートビート最大間隔（Application Heartbeat Maximum Interval）]フィールドに、最大間隔の時間を入力します。 デフォルトは 3600 です。

ステップ 7 **[保存]** をクリックします。

第 IV 部

エンド ユーザのプロビジョニング



第 28 章

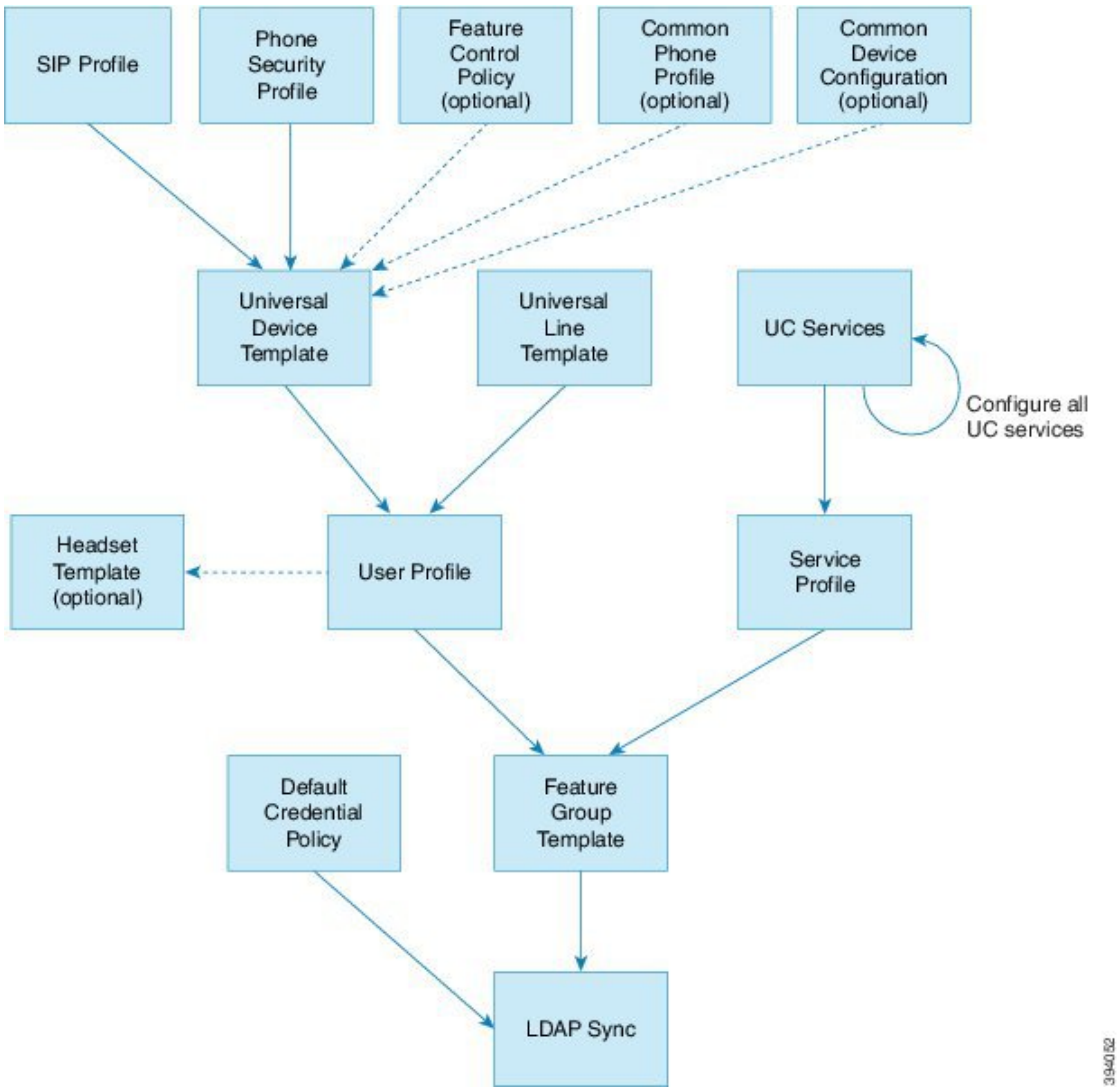
プロビジョニング プロファイルの設定

プロビジョニング プロファイルの概要

Unified Communications Manager では、新規ユーザに割り当てることができる一連のプロファイルとテンプレートが用意されています。 これらのプロファイルと共通設定をあらかじめ設定しておくと、新しいユーザをプロビジョニングしてデバイスを割り当てるときに、適用される設定に基づいてユーザとデバイスが自動的に設定されます。

ユーザをプロビジョニングするときは、必要な設定が含まれるユーザプロファイルとサービスプロファイルにそのユーザを関連付けます。 さらに、ユーザ用のデバイスを追加するときに、そのユーザのユーザプロファイルに関連付けられているユニバーサル回線テンプレートとユニバーサル デバイス テンプレートを使用して、デバイスとディレクトリ番号がすばやく設定されます。

次のプロファイルとテンプレートを使用して、ユーザのニーズに基づいて、ユーザとエンドポイントに共通の設定を適用できます。



プロビジョニング プロファイルのタスク フロー

プロビジョニングするユーザとデバイスの数が多い場合は、特定のグループ（たとえばカスタマー サポート）内のユーザに適用されるテンプレートと共通設定を使用してユーザ プロファイルとサービス プロファイルを設定することで、設定プロセスを簡略化できます。

ユーザをプロビジョニングするときは、必要な設定が含まれるユーザプロファイルとサービスプロファイルにそのユーザを関連付けます。 さらに、ユーザ用のデバイスを追加するときに、そのユーザのユーザプロファイルに関連付けられているユニバーサル回線テンプレートとユニバーサル デバイス テンプレートを使用して、デバイスとディレクトリ番号がすばやく設定されます。

次のプロファイルとテンプレートを使用して、ユーザのニーズに基づいて、ユーザとエンドポイントに共通の設定を適用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	SIP プロファイルの設定（344 ページ）	展開する SIP エンドポイントに関連付けられる共通 SIP 設定を設定します。
ステップ 2	電話機のセキュリティ プロファイルの設定（345 ページ）	プロビジョニングされたエンドポイントに割り当てるセキュリティ プロファイルを設定します。 TLS および TFTP 暗号化などの設定を割り当てます。
ステップ 3	機能管理ポリシーの作成（346ページ）	（オプション）このポリシーを使用すると、特定の機能を有効化して、電話機のソフトキーの外観を制御できます。
ステップ 4	共通の電話プロファイルの作成（347 ページ）	（オプション）このプロファイルを使用して、エンドポイントのグループに割り当てることができるプロファイルに、TFTP データおよび製品固有の設定のデフォルト値を割り当てます。
ステップ 5	共通デバイス設定の構成（348ページ）	（オプション）この設定を使用して、エンドポイントにユーザ固有の設定と IPv6 設定を割り当てます。
ステップ 6	ユニバーサル デバイス テンプレートの設定（349 ページ）	このテンプレートには、新しくプロビジョニングされた電話を設定するために使用される共通設定が含まれます。設定したプロファイルをこのテンプレートに割り当てることもできます。
ステップ 7	ユニバーサル回線テンプレートの設定（350 ページ）	このテンプレートには、新しくプロビジョニングされた内線番号を設定するために使用される共通設定が含まれます。 内線用のエンタープライズ番号および E.164 番号も設定できます。
ステップ 8	ユーザ プロファイルの設定（351 ページ）	デバイス テンプレート、回線テンプレート、および新しくプロビジョニングされるユーザの共通設定を使用して、ユーザ プロファイルを設定します。
ステップ 9	ヘッドセットテンプレートの設定（352 ページ）	（オプション）シスコ ヘッドセットを使用する場合は、ヘッドセットテンプ

	コマンドまたはアクション	目的
		レートを設定して、設定済みのユーザプロファイルに割り当てます。
ステップ 10	UC サービスの設定 （354 ページ）	IM and Presence Service およびディレクトリ サービスなどの UC サービスを設定します。
ステップ 11	サービス プロファイルの設定 （355 ページ）	プロビジョニングされたユーザに割り当てる UC サービスを含む、サービスプロファイルを作成します。
ステップ 12	機能グループテンプレートの設定 （355 ページ）	LDAP 同期の場合は、LDAP で同期されたユーザに割り当てることができる機能グループテンプレートに、ユーザプロファイルとサービスプロファイルを追加します。
ステップ 13	デフォルトのクレデンシャルポリシーの設定 （356 ページ）	新しくプロビジョニングされるユーザに割り当てるクレデンシャルポリシーを設定します。

次のタスク

- 新しいユーザをプロビジョニングするための LDAP 同期のセットアップ
- LDAP を導入していない場合は、一括管理を使用してユーザを一括でプロビジョニングできます。

SIP プロファイルの設定

共通 SIP 設定を使用して SIP プロファイルを設定するには、この手順を使用します。設定した SIP プロファイルは、SIP デバイスに割り当てることができます。

手順

ステップ 1 Cisco Unified CM Administration で、[デバイス（Device）]>[デバイスの設定（Device Settings）]>[SIPプロファイル（SIP Profile）]を選択します。

ステップ 2 次のいずれかの手順を実行します。

- 既存のプロファイルを編集するには、[検索（Find）]をクリックし、SIP プロファイルを選択します。
- 新しいプロファイルを作成するには、[新規追加] をクリックします。

ステップ 3 プロファイル名を入力します。

ステップ 4 URI ダイヤリングを展開する場合は、[ダイヤル文字列の解釈（Dial String Interpretation）]を設定して、コールをディレクトリ URI または電話番号として処理するかどうかをシステムに指示します。

ステップ 5 [電話で使用されるパラメータ（Parameters Used in Phone）]の下にある DSCP 設定項目を入力して、このプロファイルを使用するコールのタイプに対する QoS 処理を定義します。

ステップ 6 （任意）正規化スクリプトを割り当てる必要がある場合は、[正規化スクリプト（Normalization Script）] ドロップダウン リストからいずれかのデフォルト スクリプトを選択します。

（注） 独自のスクリプトを作成することもできます。 詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』を参照してください。

ステップ 7 このプロファイルで IPv4 と IPv6 の両方のスタックを同時にサポートする場合は、[ANATの有効化（Enable ANAT）]チェックボックスをオンにします。

ステップ 8 ユーザがプレゼンテーションを共有できるようにするには、[BFCP を使用するプレゼンテーションの共有を許可（Allow Presentation Sharing using BFCP）]チェックボックスをオンにします。

ステップ 9 [SIP プロファイルの設定（SIP Profile Configuration）] ウィンドウで、残りのフィールドを入力します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 10 **[保存]** をクリックします。

電話機のセキュリティ プロファイルの設定

エンドポイントの TLS シグナリング、CAPF、ダイジェスト認証の要件などのセキュリティ機能を有効にする場合は、エンドポイントに適用できる新しいセキュリティプロファイルを設定する必要があります。

（注） デフォルトでは、プロビジョニングされたデバイスに SIP phone セキュリティプロファイルを適用しない場合、デバイスは非セキュアプロファイルを使用します。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[セキュリティ（Security）]** > **[電話セキュリティ プロファイル（Phone Security Profile）]** の順に選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [電話のセキュリティプロファイルのタイプ（Phone Security Profile Type）]ドロップダウン リストから [ユニバーサルデバイステンプレート（Universal Device Template）] を選択し、デバイステンプレートを使用してプロビジョニングする際に使用できるプロファイルを作成します。

（注） 必要に応じて、特定のデバイス モデルのセキュリティ プロファイルを作成することもできます。

ステップ 4 プロトコルを選択します。

ステップ 5 [Name] フィールドにプロファイルの適切な名前を入力します。

ステップ 6 TLS シグナリングを使用してデバイスに接続する場合は、[デバイスのセキュリティモード（Device Security Mode）]を [認証済み（Authenticated）]または [暗号化（Encrypted）]に設定し、[トランスポートタイプ（Transport Type）] を [TLS]に設定します。

ステップ 7 （任意）電話でダイジェスト認証を使用する場合は、[OAuth認証の有効化（Enable OAuth Authentication）]チェックボックスをオンにします。

ステップ 8 （任意）暗号化された TFTP を使用する場合は、[TFTP暗号化設定（TFTP Encrypted Config）] チェックボックスをオンにします。

ステップ 9 [電話のセキュリティプロファイルの設定（Phone Security Profile Configuration）] ウィンドウで、残りのフィールドを入力します。 フィールドとその設定の詳細については、オンラインヘルプを参照してください。

ステップ 10 **[保存]** をクリックします。

機能管理ポリシーの作成

機能管理ポリシーを作成するには、次の手順に従います。 このポリシーを使用して、特定の機能を有効化または無効化し、電話に表示されるソフトキーの外観を制御します。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[機能管理ポリシー（Feature Control Policy）]** を選択します。

ステップ 2 次のいずれかの作業を実行します。

- 既存のポリシーの設定を変更するには、検索条件を入力して **[検索（Find）]** をクリックし、結果のリストからポリシーを選択します。
- 新しいポリシーを追加するには、**[新規追加] をクリックします。**

[機能管理ポリシーの設定（Feature Control Policy Configuration）] ウィンドウが表示されます。

ステップ 3 [名前（Name）] フィールドに機能管理ポリシーの名前を入力します。

ステップ 4 [説明（Description）] フィールドに、この機能管理ポリシーの説明を入力します。

ステップ 5 [機能管理セクション（Feature Control Section）]でリストされている各機能に対して、システムデフォルトをオーバーライドするか、次の設定を有効/無効にするかを選択します。

- デフォルトで有効な機能の設定を無効にする場合は、[デフォルトをオーバーライド（Override Default）]チェックボックスをオンにして、[設定を有効にする（Enable Setting）]チェックボックスをオフにします。
- デフォルトで無効な機能の設定を有効にする場合は、[デフォルトをオーバーライド（Override Default）]チェックボックスをオンにして、[設定を有効にする（Enable Setting）]チェックボックスをオンにします。

ステップ 6 **[保存]** をクリックします。

共通の電話プロファイルの作成

共通の電話プロファイルは、そのプロファイルを使用する電話について、TFTP データおよび製品固有の設定のデフォルト値を設定するために使用できる、オプションのプロファイルです。

手順

ステップ 1 Cisco Unified CM Administration から、[デバイス（Device）]>[デバイスの設定（Device Settings）]>[共通の電話プロファイル（Common Phone Profile）]メニューパスを選択して、共通の電話プロファイルを設定します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 プロファイル**名**を入力します。

ステップ 4 プロファイルの [**説明**] を入力します。

ステップ 5 このプロファイルを使用する電話に対して [機能管理ポリシー（Feature Control Policy）を設定する場合は、ドロップダウン リストからポリシーを選択します。

ステップ 6 [共通の電話プロファイルの設定（Common Phone Profile Configuration）]ウィンドウで、残りのフィールドを設定します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 7 [製品固有の設定レイアウト（Product-Specific Configuration Layout）] の下にあるフィールドを設定します。 フィールドの説明については、[?] をクリックして、フィールド固有のヘルプを参照してください。

ステップ 8 （任意）モバイルおよびリモートアクセス電話用に Interactive Connectivity Establishment（ICE）を有効化する場合、次の手順を実行します。

a) [ICE] ドロップダウンを [有効（Enabled）]に設定します。

b) [デフォルト候補タイプ（Default Candidate Type）]を次のいずれかに設定します。

- **[**ホスト (host)]: ホストデバイスの IP アドレスを選択することによって得られる候補。これはデフォルトです。

- **サーバ再帰**: STUN要求の送信によって取得されるIPアドレスとポートの候補。 多くの場合、これは NAT のパブリック IP アドレスを表している可能性があります。
- **中継**: TURNサーバから取得したIPアドレスとポートの候補。 IPアドレスとポートは、TURNサーバによってメディアが中継されるように、TURNサーバに常駐しています。

c) 残りの ICE フィールドを設定します。

ステップ 9 **[保存]** をクリックします。

共通デバイス設定の構成

一般的なデバイス構成は、オプションのユーザ固有特徴属性のセットを含む。 IPv6 を導入している場合は、この設定を使用して SIP トランクまたは SCCP 電話に IPv6 優先設定を割り当てることができます。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[共通デバイス設定（Common Device Configuration）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 SIP トランク、SIP 電話または SCCP 電話の場合、[IPアドレッシングモード（IP Addressing Mode）]ドロップダウン リストの値を選択します。

- [IPv4 のみ（IPv4 Only）]—デバイスはメディアやシグナリングに IPv4 アドレスだけを使用します。
- [IPv6 のみ（IPv6 Only）]—デバイスはメディアやシグナリングに IPv6 アドレスだけを使用します。
- [IPv4 および IPv6（IPv4 and IPv6）]—（デフォルト）デバイスはデュアルスタック デバイスで、利用できる IP アドレスのタイプを使用します。 両方の IP アドレスのタイプがデバイスに設定されている場合、デバイスのシグナリングには、[シグナリグ用 IP アドレッシング モード優先設定（IP Addressing Mode Preference for Signaling）]設定を使用し、メディア デバイスには、[メディア用 IP アドレッシング モード優先設定（IP Addressing Mode Preference for Media）]エンタープライズ パラメータの設定を使用します。

ステップ 4 前のステップでIPv6を設定する場合は、[シグナリング(シグナリング)] ドロップダウンリストの ip アドレス指定モードの ip アドレス設定を次のように設定します。

- [IPv4（IPv4）]—デュアル スタック デバイスでシグナリングに IPv4 アドレスを優先して使用します。
- [IPv6（IPv6）]—デュアル スタック デバイスでシグナリングに IPv6 アドレスを優先して使用します。

- [システム デフォルトを使用（Use System Default）]—デバイスは、[シグナリグ用 IP アドレッシング モード優先設定（IP Addressing Mode Preference for Signaling）]エンタープライズ パラメータの設定を使用します。

ステップ 5 **[共通デバイス構成（Common Device Configuration）]** 画面で、残りのフィールドを設定します。 フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 6 **[保存]** をクリックします。

ユニバーサル デバイス テンプレートの設定

ユニバーサル デバイス テンプレートを使用すると、新しくプロビジョニングしたデバイスに簡単に設定を適用できます。 プロビジョニングされたデバイスは、ユニバーサル デバイス テンプレートの設定を使用します。 さまざまなユーザ グループのニーズを満たすために、異なるデバイス テンプレートを設定できます。 設定したプロファイルをこのテンプレートに割り当てることもできます。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザの管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [ユニバーサル デバイス テンプレート（Universal Device Template）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 次の必須フィールドに入力します。

a) テンプレートの [デバイスの説明（Device Description）]を入力します。
b) [デバイスプールタイプ（Device Pool Type）]をドロップダウン リストから選択します。
c) [デバイスのセキュリティプロファイル（Device Security Profile）]をドロップダウン リストから選択します。
d) [SIPプロファイル（SIP Profile）]をドロップダウンリストから選択します。
e) [電話ボタンテンプレート（Phone Button Template）]をドロップダウンリストから選択します。

ステップ 4 [ユニバーサルデバイステンプレートの設定（Universal Device Template Configuration）]ウィンドウで、残りのフィールドを入力します。 フィールドの説明については、オンラインヘルプを参照してください。

ステップ 5 [電話の設定（Phone Settings）]で、次の任意指定のフィールドを入力します。

a) [共通の電話プロファイル（Common Phone Profile）]を設定した場合は、そのプロファイルを割り当てます。
b) [共通デバイス設定（Common Device Configuration）]を設定した場合は、その設定を割り当てます。

c) [機能管理ポリシー（Feature Control Policy）]を設定した場合は、そのポリシーを割り当てます。

ステップ 6 **[保存]** をクリックします。

ユニバーサル回線テンプレートの設定

ユニバーサル回線テンプレートを使用すると、新しく割り当てられたディレクトリ番号に共通の設定を簡単に適用できます。 さまざまなユーザ グループのニーズに合わせて、異なるテンプレートを設定します。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理（User Management）]** > **[ユーザ/電話の追加（User/Phone Add）]** > **[ユニバーサル回線テンプレート（Universal Line Template）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [ユニバーサル回線テンプレートの設定（Universal Line Template Configuration）]ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンラインヘルプを参照してください。

ステップ 4 代替番号を使用したグローバル ダイヤル プラン レプリケーションを展開する場合は、[エンタープライズ代替番号（Enterprise Alternate Number）]セクションと [+E.164代替番号（+E.164 Alternate Number）]セクションを展開して、次の手順を実行します。

a) [エンタープライズ代替番号の追加（Add Enterprise Alternate Number）]ボタンまたは[+E.164代替番号の追加（Add +E.164 Alternate Number）]ボタンのいずれか、または両方をクリックします。

b) 代替番号への割り当に使用する [番号マスク（Number Mask）]を追加します。 たとえば、4 桁の内線番号では、エンタープライズ番号マスク として 5 XXXX を使用し、+E.164 代替番号マスクとして 1972555XXXX を使用することが考えられます。

c) 代替番号を割り当てるパーティションを割り当てます。

d) ILS を通じてこの番号をアドバタイズする場合は、[ILS経由でグローバルにアドバタイズ（Advertise Globally via ILS）]チェックボックスをオンにします。 アドバタイズされたパターンを使用して一定の代替番号の範囲を要約している場合は、個別の代替番号をアドバタイズする必要はありません。

e) [PSTNフェールオーバー（PSTN Failover）]セクションを展開して、通常のコール ルーティングが失敗した場合に使用する PSTN フェールオーバーとして、[エンタープライズ番号（Enterprise Number）]または [+E.164代替番号（+E.164 Alternate Number）]を選択します。

ステップ 5 **[保存]** をクリックします。

ユーザ プロファイルの設定

ユーザ プロファイルを使用して、ユニバーサル回線テンプレートとユニバーサル デバイス テンプレートをユーザに割り当てます。 さまざまなユーザ グループ用に複数のユーザ プロファイルを設定します。 このサービス プロファイルを使用するユーザに対してセルフプロビジョニングを有効にすることもできます。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [ユーザプロファイル（User Profile）]**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 ユーザ プロファイルの [名前（Name）]および [説明（Description）]を入力します。

ステップ 4 ユーザの **[デスクフォン（Desk Phones）]**、**[モバイルおよびデスクトップデバイス（Mobile and Desktop Devices）]**、および **[リモート接続先/デバイスプロファイル（Remote Destination/Device Profiles）]** に、**[ユニバーサルデバイステンプレート（Universal Device Template）]** を割り当てます。

ステップ 5 [ユニバーサル回線テンプレート（Universal Line Template）]を割り当て、このユーザプロファイルのユーザの電話回線に適用します。

ステップ 6 このユーザプロファイルのユーザに自分の電話機をプロビジョニングするセルフプロビジョニング機能の使用を許可するには、次の手順を実行します

a) [エンドユーザに自分の電話のプロビジョニングを許可（Allow End User to Provision their own phones）]チェックボックスをオンにします。

b) [エンドユーザがプロビジョニングする電話機数を制限（Limit Provisioning once End User has this many phones）]フィールドに、ユーザがプロビジョニングできる電話の最大数を入力します。 最大値は 20 です。

c) このプロファイルに関連付けられたエンドユーザーに、別のユーザーがすでに所有しているデバイスを移行または再割り当てする権限があるかどうかを判断するには、**[すでに別のエンドユーザーに割り当てられた電話機のプロビジョニングを許可する（Allow Provisioning of a phone already assigned to a different End User）]** チェックボックスをオンにします。 デフォルトでは、このチェックボックスはオフになっています。

ステップ 7 このユーザープロファイルに関連付けられた Cisco Jabber ユーザーがモバイルおよびリモートアクセス機能を使用できるようにするには、**[モバイルおよびリモートアクセスの有効化（Enable Mobile and Remote Access）]** チェックボックスをオンにします。

（注）
- デフォルトでは、このチェックボックスはオンになっています。 このチェックボックスをオフにすると、**[クライアントポリシー（Client Policies）]**セクションが無効になり、サービス クライアント ポリシー オプションは、デフォルトで選択されません。
- この設定は、OAuth 更新ログインを使用している Cisco Jabber のユーザにのみ必須です。 Jabberユーザではない場合、この設定を行わずともモバイルおよびリモートアクセス機能を使用できます。 モバイルおよびリモート アクセス機能は、Jabberモバイルおよびリモートアクセスのユーザにのみ適用され、他のエンドポイントやクライアントには適用されません。

ステップ 8 このユーザプロファイルにJabberポリシーを割り当てます。**[デスクトップ クライアント ポリシー（Desktop Client Policy）]**と**[モバイル クライアント ポリシー（Mobile Client Policy）]**のドロップダウンメニューから、次のオプションのいずれかを選択します。

- サービスなし：このポリシーは、すべての Cisco Jabber サービスへのアクセスを禁止します。
- IMとプレゼンスのみ：このポリシーは、インスタントメッセージとプレゼンス機能のみを有効にします。
- IM とプレゼンス、音声とビデオ通話：このポリシーは音声やビデオ デバイスを使うすべてのユーザに対して、インスタントメッセージ、プレゼンス、ボイスメールと会議機能を有効化します。 これがデフォルトのオプションです。

（注） Jabber デスクトップクライアントには Windows 版 Cisco Jabber および Mac 版 Cisco Jabber が含まれています。 Jabber モバイルクライアントには、iPad/iPhone ユーザ用 Cisco Jabber および Android 版 Cisco Jabber が含まれています。

ステップ 9 このユーザ プロファイルのユーザが Cisco Unified Communications セルフケア ポータルで Extension Mobility または Extension Mobility Cross Cluster の最大ログイン時間を設定できるようにするには、[エンドユーザにエクステンションモビリティの最大ログイン時間の設定を許可する（Allow End User to set their Extension Mobility maximum login time）]チェックボックスをオンにします。

（注） デフォルトでは [エンドユーザにエクステンションモビリティの最大ログイン時間の設定を許可する（Allow End User to set their Extension Mobility maximum login time）] チェックボックスはオフになっています。

ステップ 10 **[保存]** をクリックします。

ヘッドセットテンプレートの設定

シスコヘッドセットに適用できるカスタマイズされた設定でヘッドセットテンプレートを設定するには、次の手順を使用します。 カスタマイズしたテンプレートを作成するか、またはシステム定義の標準デフォルトヘッドセットテンプレートを使用することができます。

（注） 標準デフォルトヘッドセット構成テンプレートは、システム定義のテンプレートです。標準デフォルトヘッドセットテンプレートに新しいユーザプロファイルを割り当てることはできますが、テンプレートを編集することはできません。デフォルトでは、すべてのユーザプロファイルがこのテンプレートに割り当てられています。このテンプレートからユーザプロファイルの関連付けを外すには、プロファイルを新しいテンプレートに割り当てる必要があります。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、**[デバイス（Device）][電話機（Phone）]** を選択します。

ステップ 2 次のいずれかを実行します。

- 既存のテンプレートを編集するには、そのテンプレートを選択します。
- 新しいテンプレートを作成するには、既存のテンプレートを選択し、**[コピー(Copy)]** をクリックします。既存の設定が新しいテンプレートに適用されます。

ステップ 3 テンプレートの**[名前（Name）]**と**[説明（Description）]**を追加します。

ステップ 4 [**モデルとファームウェアの**設定（Model and Firmware Settings）] で、カスタマイズしたヘッドセット設定をこのテンプレートに適用するように割り当てます。新しい設定を追加するには、**[**追加 (add)] ボタンをクリックして設定を構成します。

ステップ 5 上下矢印を使用して、このテンプレートに割り当てるユーザプロファイルを**割当済みユーザプロファイル**リストに移動します。これらのプロファイルに割り当てられているすべてのユーザは、このヘッドセットテンプレートにも割り当てられます。

ステップ 6 **[保存]** をクリックします。

ステップ 7 デフォルトの**テンプレート設定**に戻るには、[デフォルトに設定 (Set to Default)] ボタンを使用します。

ステップ 8 **[設定の適用（Apply Config）]** をクリックします。

標準デフォルトヘッドセット構成テンプレートの場合、**[**構成を適用 (Apply Configuration)] ボタンは次の場合有効になります。

- 割当済みユーザプロファイルリストに追加したユーザが所有するデバイス
- 匿名デバイス

カスタマイズされたヘッドセット構成テンプレートでは、**構成を適用**ボタンは、**割当済みユーザプロファイル**リストに追加したユーザが所有するデバイスでのみ有効になります。

UC サービスの設定

ユーザが使用する UC サービス接続を設定するには、次の手順を使用します。 次のUCサービスの接続を設定できます。

- ボイスメール
- メールストア（Mailstore）
- 会議
- ディレクトリ（Directory）
- IM and Presence Service
- [CTI]
- ビデオ会議スケジュールポータルの設定
- Jabberクライアント設定(jabber-config.xml)

（注） フィールドは、設定する UC サービスによって異なる場合があります。

手順

ステップ 1 Cisco Unified CMの管理から、**ユーザの管理>ユーザ設定>UCサービス**を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [UC サービスタイプ (UC Service)] ドロップダウンから、設定する UC サービスを選択し、**[次へ (Next)] をクリックします**。

ステップ 4 **製品タイプ**を選択します。

ステップ 5 [名前（Name）]にサービスの名前を入力します。

ステップ 6 サービスが存在するサーバーの**ホスト名またはIPアドレス**を入力します。

ステップ 7 ポートと**プロトコル**の情報を入力します。

ステップ 8 残りのフィールドを設定します。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。フィールドオプションは、導入しているUCサービスによって異なります。

ステップ 9 **[保存]** をクリックします。

ステップ 10 必要なすべてのUCサービスをプロビジョニングするまで、この手順を繰り返します。

（注） サービスを複数のサーバに配置する場合は、別のサーバを指す複数の UC サービス接続を設定します。 たとえば、IMとプレゼンスサービスの集中型の導入を行う場合は、別のIM ノードとプレゼンスノードをポイントするように、複数のIMおよびプレゼンスUC サービスを設定することを推奨します。 すべてのUC接続を設定した後、それらをサービスプロファイルに追加することができます。

サービス プロファイルの設定

このプロファイルを使用するエンド ユーザに割り当てる UC サービスを含む、サービス プロファイルを設定します。

始める前に

サービス プロファイルに追加する前に、Unified Communications（UC）サービスをセットアップする必要があります。

手順

ステップ 1 Cisco Unified CM の管理から、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [サービスプロファイル（Service Profile）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 選択したサービス プロファイルの設定の [名前（Name）]を入力します。

ステップ 4 選択したサービス プロファイルの設定の [説明（Description）]を入力します。

ステップ 5 このプロファイルに含める各 UC サービスに、そのサービス用の [プライマリ（Primary）]、[セカンダリ（Secondary）]、および [ターシャリ（Tertiary）] の接続を割り当てます。

ステップ 6 [サービスプロファイルの設定（Service Profile Configuration）]ウィンドウで、残りのフィールドを入力します。 フィールドの詳細については、オンライン ヘルプを参照してください。

ステップ 7 **[保存]** をクリックします。

機能グループ テンプレートの設定

機能グループテンプレートは、プロビジョニングされたユーザ用に、電話、回線、および機能をすばやく設定できるようにすることで、システムの展開をサポートします。 企業の LDAP ディレクトリからユーザを同期している場合は、ディレクトリからユーザを同期させるユーザ プロファイルおよびサービス プロファイルを使用して機能グループ テンプレートを設定します。 このテンプレートを使用して、同期されたユーザに対して IM and Presence Service を有効化することもできます。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、**[ユーザ管理（User Management）]** > **[ユーザ/電話の追加（User/Phone Add）]** > **[機能グループ テンプレート（Feature Group Template）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 機能グループ テンプレートの [名前（Name）]と [説明（Description）]を入力します。

ステップ 4 このテンプレートを使用するすべてのユーザのホーム クラスタとしてローカル クラスタを使用する場合は、[ホーム クラスタ（Home Cluster）]チェック ボックスをオンにします。

ステップ 5 このテンプレートを使用するユーザがインスタント メッセージおよびプレゼンス情報を交換できるようにするには、[Unified CM IM and Presenceのユーザを有効化（Enable User for Unified CM IM and Presence）]チェックボックスをオンにします。

ステップ 6 ドロップダウン リストから、[サービスプロファイル（Services Profile）]および [ユーザプロファイル（User Profile）]を選択します。

ステップ 7 [機能グループ テンプレートの設定（Feature Group Template Configuration）]ウィンドウの残りのフィールドに入力します。 フィールドの説明については、オンライン ヘルプを参照してください。

ステップ 8 **[保存]** をクリックします。

次のタスク

機能グループ テンプレートと LDAP ディレクトリ同期を関連付け、テンプレートの設定を同期したエンド ユーザに適用します。

デフォルトのクレデンシャル ポリシーの設定

新しくプロビジョニングされたユーザに適用されるクラスタ全体のデフォルトのクレデンシャル ポリシーを設定するには、この手順を使用します。 次の各クレデンシャル タイプに対して、個別のクレデンシャル ポリシーを適用できます。

- アプリケーション ユーザー パスワード
- エンド ユーザー パスワード
- エンド ユーザ PIN

手順

ステップ 1 クレデンシャル ポリシーの設定を入力します。

a) Cisco Unified CM Administration で、**[ユーザ管理]** > **[ユーザ設定]** > **[クレデンシャル ポリシーのデフォルト]** を選択します。

b) 次のいずれかを実行します。

- [検索（Find）] をクリックし、既存のクレデンシャル ポリシーを選択します。
- [新規追加（Add New）]をクリックして、新しいクレデンシャル ポリシーを作成します。

c) ABCD や 123456 のようなハッキングされやすいパスワードをシステムにチェックさせる場合は、[単純すぎるパスワードのチェック（Check for Trivial Passwords）]チェックボックスをオンにします。

d) [クレデンシャル ポリシーの設定（Credential Policy Configuration）]ウィンドウの各フィールドに入力します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

e) **[保存]** をクリックします。

f) 他のクレデンシャル タイプ用に別のクレデンシャル ポリシーを作成する場合は、この手順を繰り返します。

ステップ 2 次のいずれかのクレデンシャル タイプにクレデンシャル ポリシーを適用します。

a) Cisco Unified CM Administration で、**[ユーザ管理]** > **[ユーザ設定]** > **[クレデンシャル ポリシーのデフォルト]** を選択します。

b) クレデンシャル ポリシーを適用するクレデンシャル タイプを選択します。

c) [クレデンシャルポリシー（Credential Policy）]ドロップダウンから、このクレデンシャル タイプに適用するクレデンシャル ポリシーを選択します。 たとえば、作成したクレデンシャル ポリシーを選択できます。

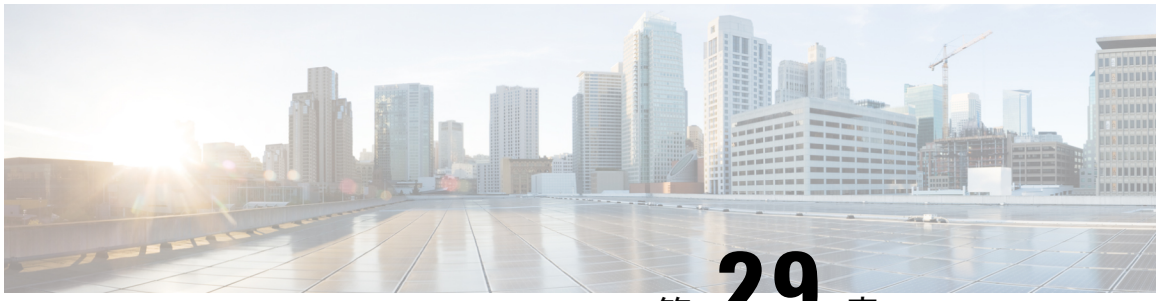
d) [クレデンシャルの変更（Change Credential）]フィールドと [クレデンシャルの確認（Confirm Credential）]フィールドの両方にデフォルトのパスワードを入力します。 ユーザが次にログインするときに、これらのパスワードを入力する必要があります。

e) [クレデンシャル ポリシーのデフォルトの設定（Credential Policy Default Configuration）] ウィンドウで、残りのフィールドを設定します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

f) **[保存]** をクリックします。

g) 他のクレデンシャル タイプにクレデンシャル ポリシーを割り当てる場合は、この手順を繰り返します。

（注） また、個々のユーザに対して、**[エンド ユーザの設定]** ウィンドウまたはそのユーザの **[アプリケーション ユーザ設定]** ウィンドウから、特定のユーザクレデンシャルにポリシーを割り当てすることもできます。 クレデンシャル タイプ (パスワードまたは PIN) の隣にある **[クレデンシャルの編集]** ボタンをクリックして、そのユーザの**クレデンシャル設定** を開きます。



第 29 章

LDAP 同期の設定

LDAP 同期の概要

Lightweight Directory Access Protocol（LDAP）の同期は、システムのエンドユーザのプロビジョニングと設定を支援します。 LDAP の同期中、システムは外部 LDAP ディレクトリから Cisco Unified Communications Manager データベースにユーザのリストと関連するユーザ データをインポートします。 インポートしている間に、エンドユーザを設定することもできます。

（注） Unified Communication Manager は、LDAPS（SSL を使用した LDAP）をサポートしますが、StartTLS を使用した LDAP はサポートしていません。 LDAP サーバ証明書を Unified Communication Manager に Tomcat-Trust 証明書としてアップロードします。

サポートされている LDAP ディレクトリの詳細については、*Cisco Unified Communications Manager と IM and Presence Service* の互換性マトリクスを参照してください。

LDAP 同期では、以下の機能がアドバタイズされます。

- **エンドユーザのインポート**：LDAP 同期を使用して、システムの初期設定時にユーザ一覧を会社の LDAP ディレクトリから Unified Communication Manager のデータベースにインポートできます。 機能グループテンプレート、ユーザプロファイル、サービスプロファイル、ユニバーサルデバイス、回線テンプレートなどの設定項目が設定されている場合は、設定をユーザに適用することができ、また、同期プロセス中に設定したディレクトリ番号とディレクトリ Uri を割り当てることができます。 LDAP同期プロセスは、ユーザーリストとユーザー固有のデータをインポートし、設定した構成テンプレートを適用します。

（注） 初期同期が実行された以降は、LDAP 同期を編集することはできません。

- **スケジュールされた更新**：Unified Communication Manager をスケジュールされた間隔で複数の LDAP ディレクトリと同期するように設定できます。これによって確実にデータベースが定期的に更新され、すべてのユーザ データを最新に保ちます。
- **エンド ユーザの認証**：LDAP 同期を使用して、システムが Cisco Unified Communications Manager データベースではなく、LDAP ディレクトリに対してエンド ユーザー パスワードを認証するように設定できます。 LDAP 認証によって、企業は、すべての企業内アプリケーションに対応する単一のパスワードをエンド ユーザに割り当てることができます。この機能は、PIN またはアプリケーション ユーザー パスワードには適用されません。
- **シスコ モバイルおよびリモート アクセスのクライアントおよびエンド ポイントのディレクトリ サーバ ユーザー検索**：社内ディレクトリ サーバが企業ファイアウォール外で運用されている場合でも検索できます。 この機能を有効にすると、ユーザ データ サービス（UDS）がプロキシとして機能し、Unified Communications Manager データベースにユーザー検索要求を送信する代わりに、それを社内ディレクトリに送信します。

LDAP 同期の前提条件

前提条件のタスク

LDAP ディレクトリからエンドユーザをインポートする前に、次のタスクを実行します。

- ユーザ アクセスを設定します。ユーザに割り当てるアクセス制御グループを決定します。ほとんどの導入環境では、デフォルトのグループで十分です。 ロールとグループをカスタマイズする必要がある場合は、アドミニストレーション ガイドの「ユーザ アクセスの管理」の章を参照してください。
- 新しくプロビジョニングされたユーザーにデフォルトで適用されるクレデンシャル ポリシーに、デフォルトのクレデンシャルを設定します。
- LDAP ディレクトリからユーザを同期する場合は、機能グループ テンプレートが設定されていることを確認してください。このテンプレートには、ユーザ プロファイル、サービス プロファイル、ユーザの電話と電話の内線に割り当てるユニバーサル回線テンプレートおよびユニバーサル デバイス テンプレートの設定が含まれます。

（注） システムにデータを同期するユーザについては、Active Directory サーバでの電子メール ID フィールドが一意のエントリであるか空白であることを確認してください。

LDAP 同期設定のタスク フロー

外部 LDAP ディレクトリからユーザ リストをプルし、Unified Communication Manager のデータベースにインポートするには、以下のタスクを使用します。

（注） LDAP ディレクトリをすでに一度同期している場合、外部 LDAP ディレクトリから新しい項目を同期することはできますが、Unified Communication Manager 内の新しい設定を LDAP ディレクトリ同期に追加することはできません。この場合、一括管理ツールと、[ユーザの更新（Update Users）]や[ユーザの挿入（Insert Users）]などのメニューを使用できます。『*Bulk Administration Guide for Cisco Unified Communications Manager*』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco DirSync サービスの有効化 （362 ページ）	Cisco Unified Serviceability にログインし、Cisco DirSync サービスを有効にします。
ステップ 2	LDAP ディレクトリ同期の有効化 （362 ページ）	Unified Communication Manager の LDAP ディレクトリ同期を有効化します。
ステップ 3	LDAP フィルタの作成 （363 ページ）	（オプション） Unified Communication Manager に社内 LDAP ディレクトリからユーザのサブセットだけを同期するには、LDAP フィルタを作成します。
ステップ 4	LDAP ディレクトリの同期の設定 （363 ページ）	アクセス制御グループ、機能グループのテンプレートとプライマリ エクステンションのフィールド設定、LDAP サーバのロケーション、同期スケジュール、および割り当てなどの LDAP ディレクトリ同期を設定します。
ステップ 5	エンタープライズ ディレクトリ ユーザー検索の設定 （366 ページ）	（オプション） エンタープライズ ディレクトリ サーバ ユーザを検索するシステムを設定します。 システムの電話機とクライアントをデータベースの代わりにエンタープライズ ディレクトリ サーバに対してユーザの検索を実行するように設定するには、次の手順に従います。
ステップ 6	LDAP 認証の設定 （367 ページ）	（オプション） エンド ユーザーパスワード認証に LDAP ディレクトリを使用するには、LDAP 認証を設定します。
ステップ 7	LDAP アグリーメント サービス パラメータのカスタマイズ （368 ページ）	（オプション） 任意指定の [LDAP同期（LDAP Synchronization）] サービス パラメータを設定します。 ほとんどの導

	コマンドまたはアクション	目的
		入の場合、デフォルト値のままで問題ありません。

Cisco DirSync サービスの有効化

Cisco DirSync サービスをアクティブにするには、Cisco Unified Serviceability で次の手順を実行します。 社内 LDAP ディレクトリでエンドユーザの設定を同期するには、このサービスをアクティブにする必要があります。

手順

ステップ 1 Cisco Unified Serviceability から、**[ツール（Tools）]** > **[サービスの有効化（Service Activation）]** を選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リストからパブリッシャ ノードを選択します。

ステップ 3 [**ディレクトリ サービス（Directory Services**）] の下の [**Cisco DirSync**] オプション ボタンをクリックします。

ステップ 4 **[保存]** をクリックします。

LDAP ディレクトリ同期の有効化

エンド ユーザの設定を社内 LDAP ディレクトリから同期させるには、以下の手順で Unified Communication Manager を設定します。

（注） LDAP ディレクトリをすでに一度同期している場合、外部 LDAP ディレクトリから新規ユーザーを同期することはできますが、Unified Communications Manager 内の新しい設定を LDAP ディレクトリ同期に追加することはできません。また、機能グループテンプレートやユーザプロファイルなどの基になる構成アイテムの編集を追加することもできません。 すでに 1 回の LDAP 同期を完了しており、別の設定でユーザを追加する場合は、ユーザの更新やユーザの挿入などの一括管理メニューを使用できます。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[LDAP]** > **[LDAPシステム（LDAP System）]** を選択します。

ステップ 2 Unified Communications Manager で、LDAP ディレクトリからユーザをインポートするには、**LDAP サーバからの同期を有効にする** チェックボックスをオンにします。

ステップ 3 **LDAP サーバ タイプ** ドロップダウン リストから、使用する LDAP ディレクトリ サーバの種類を選択します。

ステップ 4 **[ユーザ ID の LDAP 属性（LDAP Attribute for User ID）]** ドロップダウンリストで、**[エンドユーザの設定（End User Configuration）]** ウィンドウの **[ユーザ ID（User ID）]** フィールドに関して、Unified Communications Manager で同期する社内 LDAP ディレクトリから属性を選択します。

ステップ 5 **[保存]** をクリックします。

LDAP フィルタの作成

LDAP フィルタを作成することで、LDAP 同期を LDAP ディレクトリからのユーザのサブセットのみに制限することができます。 LDAP フィルタを LDAP ディレクトリに適用する場合、Unified Communications Manager は、フィルタに一致するユーザのみを LDAP ディレクトリからインポートします。

（注） LDAP フィルタを設定する場合は、RFC4515 に指定されている LDAP 検索フィルタ標準に準拠する必要があります。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、**[システム（System）]** > **[LDAP(LDAP)]** > **[LDAP フィルタ（LDAP Filter）]** を選択します。

ステップ 2 [新規追加（Add New）]をクリックして、新しい LDAP フィルタを作成します。

ステップ 3 [フィルタ名（Filter Name）]テキスト ボックスに、LDAP フィルタの名前を入力します。

ステップ 4 [フィルタ（Filter）]テキスト ボックスに、フィルタを入力します。 フィルタは、UTF-8 で最大 1024 文字まで入力できます。また、丸カッコ（ ()）で囲みます。

ステップ 5 **[保存]** をクリックします。

LDAP ディレクトリの同期の設定

LDAP ディレクトリと同期するように Unified Communications Manager を設定するには、この手順を使用します。 LDAP ディレクトリ同期により、エンドユーザのデータを外部の LDAP ディレクトリから Unified Communication Manager データベースにインポートして、エンドユーザの設定ウィンドウに表示することができます。ユニバーサル回線とデバイステンプレートを使用する機能グループテンプレートがセットアップされている場合は、新しくプロビジョニングされるユーザとその内線番号に自動的に設定を割り当てることができます。

ヒント　アクセス制御グループまたは機能グループ テンプレートを割り当てる場合は、LDAP フィルタを使用して、インポートを同じ設定要件のユーザ グループに限定できます。

手順

ステップ 1　Cisco Unified CM の管理で、**[システム（System）] > [LDAP（LADP）] > [LDAP ディレクトリ（LDAP Directory）]** を選択します。

ステップ 2　次のいずれかの手順を実行します。

- [**検索（Find**）] をクリックし、既存の LDAP ディレクトリを選択します。
- [新規追加（Add New）]をクリックして、新しい LDAP ディレクトリを作成します。

ステップ 3　[LDAPディレクトリの設定（LDAP Directory Configuration）]ウィンドウで、次のように入力します。

a) [LDAP設定名（LDAP Configuration Name）]フィールドで、LDAP ディレクトリに一意の名前を割り当てます。
b) [**LDAP マネージャ識別名（LDAP Manager Distinguished Name**）] フィールドに、LDAP ディレクトリ サーバにアクセスできるユーザー ID を入力します。
c) パスワードの詳細を入力し、確認します。
d) [LDAPユーザー検索スペース（LDAP User Search Space）]フィールドに、検索スペースの詳細を入力します。
e) [ユーザ同期用のLDAPカスタムフィルタ（LDAP Custom Filter for Users Synchronize）]フィールドで、[ユーザのみ（Users Only）]または[ユーザとグループ（Users and Groups）]を選択します。
f) （オプション）特定のプロファイルに適合するユーザのサブセットのみにインポートを限定する場合は、[グループ用LDAPカスタムフィルタ（LDAP Custom Filter for Groups）]ドロップダウン リストから LDAP フィルタを選択します。

ステップ 4　**LDAP ディレクトリ同期スケジュール** フィールドに、外部 LDAP ディレクトリとデータ同期を行うために Unified Communication Manager が使用するスケジュールを作成します。

ステップ 5　[**同期対象の標準ユーザ フィールド（Standard User Fields To Be Synchronized**）] セクションを記入します。 各エンドユーザのフィールドで、それぞれ LDAP 属性を選択します。 同期プロセスが LDAP 属性の値を Unified Communication Manager のエンドユーザ フィールドに割り当てます。

ステップ 6　URIダイヤリングを展開する場合は、ユーザのプライマリディレクトリURIアドレスに使用されるLDAP属性が割り当てられていることを確認してください。

ステップ 7　**同期するカスタム ユーザ フィールド** のセクションで、必要な LDAP 属性を持つカスタム ユーザ フィールド名を入力します。

ステップ 8　インポートしたエンド ユーザを、インポートしたすべてのエンド ユーザに共通するアクセス コントロール グループに割り当てるには、次の手順を実行します。

a) [アクセス コントロール グループに追加（Add to Access Control Group）]をクリックします。
b) ポップアップ ウィンドウで、インポートされたエンド ユーザに割り当てる各アクセス制御グループごとに、対応するチェックボックスをオンにします。
c) **[選択項目の追加(Add Selected)]** をクリックします。

ステップ 9 機能グループ テンプレートを割り当てる場合は、[機能グループテンプレート（Feature Group Template）]ドロップダウン リストからテンプレートを選択します。

（注） エンドユーザは、そのユーザが存在しない初回のみ、割り当てられた**機能グループテンプレート**と同期されます。 既存の [機能グループ テンプレート（Feature Group Template）]が変更され、関連付けられた LDAP の完全同期が実行される場合、変更点は更新されません。

ステップ 10 インポートされた電話番号にマスクを適用して、プライマリ内線番号を割り当てるには、次の手順を実行します。

a) [挿入されたユーザの新規回線を作成するために、同期された電話番号にマスクを適用する（Apply mask to synced telephone numbers to create a new line for inserted users）]チェックボックスをオンにします。
b) [マスク（Mask）]を入力します。 たとえば、インポートされた電話番号が 8889945 である場合、11XX のマスクによって 1145 のプライマリ内線番号が作成されます。

ステップ 11 ディレクトリ番号のプールからプライマリ内線番号を割り当てる場合は、次の手順を実行します。

a) [同期された LDAP 電話番号に基づいて作成されなかった場合、プール リストから新しい回線を割り当て（Assign new line from the pool list if one was not created based on a synced LDAP telephone number）]チェック ボックスをオンにします。
b) [DN プールの開始（DN Pool Start）]テキスト ボックスと [DN プールの終了（DN Pool End）] テキストボックスに、プライマリ内線番号を選択するディレクトリ番号の範囲を入力します。

ステップ 12 （オプション）Jabber デバイスを作成する必要がある場合は、[Jabber エンドポイント プロビジョニング（Jabber Endpoint Provisioning）] の項で、自動プロビジョニングに必要な Jabber デバイスを、次のドロップダウンから 1 つ選択します。

- Cisco Dual Mode for Android（BOT）
- Cisco Dual Mode for iPhone（TCT）
- Cisco Jabber for Tablet（TAB）
- Cisco Unified Client Services Framework（CSF）

（注） **[LDAP にライトバック（Write back to LDAP）]** オプションを使用すると、Unified CM から選択したプライマリ DN を LDAP サーバーにライトバックできます。 ライトバックできる LDAP 属性は **telephoneNumber**、**ipPhone**、および **mobile** です。

ステップ 13 [LDAPサーバ情報（LDAP Server Information）]セクションで、LDAP サーバのホスト名または IP アドレスを入力します。

ステップ 14 TLS を使用して LDAP サーバに対するセキュアな接続を作成する場合は、[TLSを使用（Use TLS）]チェックボックスをオンにします。

ステップ 15 **[保存]** をクリックします。

ステップ 16 LDAP同期を完了するには、**完全同期の実行**をクリックします。それ以外の場合は、スケジュールされた同期を待つことができます。

（注） LDAP で削除されたユーザは、24 時間後に Unified Communications Manager から自動的に削除されます。 また、削除されたユーザが次のデバイスのモビリティ ユーザとして設定されている場合、これらの非アクティブなデバイスも自動的に削除されます。

- リモート宛先プロファイル
- リモート接続先プロファイル テンプレート
- モバイルスマート クライアントプロファイル
- CTI リモート デバイス
- Spark リモート デバイス
- Nokia S60
- Cisco Dual Mode for iPhone
- IMS-integrated Mobile（基本）
- キャリア統合モバイル
- [Cisco Dual Mode for Android]

エンタープライズ ディレクトリ ユーザー検索の設定

データベースではなくエンタープライズ ディレクトリ サーバに対してユーザー検索を実行するように、システムの電話機とクライアントを設定するには、次の手順を使用します。

始める前に

- LDAP ユーザー検索に選択するプライマリ、セカンダリ、および第 3 サーバが Unified Communication Manager のサブスクライバ ノードに到達可能なネットワークにあることを確認します。
- **[システム（System）]** > **[LDAP]** > **[LDAP システム（LDAP System）]** を選択し、 **[LDAP システムの設定（LDAP System Configuration）]**ウィンドウの **[LDAP サーバタイプ（LDAP Server Type）]** ドロップダウンリストから LDAP サーバのタイプを設定します。

手順

ステップ 1 Cisco Unified CM の管理で、**[システム（System）] > [LDAP] > [LDAP 検索（LDAP Search）]** を選択します。

ステップ 2 エンタープライズ LDAP ディレクトリ サーバを使用してユーザー検索を実行するには、**[エンタープライズ ディレクトリ サーバのユーザ検索を有効にする（Enable user search to Enterprise Directory Server）]** チェックボックスをオンにします。

ステップ 3 **[LDAP 検索の設定（LDAP Search Configuration）]** ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 **[保存]** をクリックします。

（注） OpenLDAP サーバでルーム オブジェクトとして表される会議室を検索するには、カスタム フィルタを (|(objectClass=intOrgPerson)(objectClass=rooms)) に設定します。これにより、Cisco Jabber のクライアントがルーム名で電話会議室を検索し、ルームに関連付けられている番号をダイヤルできるようになります。

会議室は、ルーム オブジェクトの OpenLDAP サーバに、**givenName**、**sn**、**mail**、**displayName**、または **telephonenumber** の属性が設定されていると検索可能です。

LDAP 認証の設定

LDAP 認証を有効にして、会社の LDAP ディレクトリに割り当てられているパスワードに対してエンド ユーザーパスワードが認証されるようにするには、この手順を実行します。 この設定は、エンドユーザのパスワードにのみ適用され、エンドユーザの PIN またはアプリケーション ユーザーパスワードには適用されません。

手順

ステップ 1 Cisco Unified CM の管理で、**[システム（System）] > [LDAP] > [LDAP 認証（LDAP Authentication）]** を選択します。

ステップ 2 [エンド ユーザ用 LDAP 認証の使用（Use LDAP Authentication for End Users）]チェックボックスをオンにして、ユーザー認証に LDAP ディレクトリを使用します。

ステップ 3 [LDAP マネージャ識別名（LDAP Manager Distinguished Name）]フィールドに、LDAP ディレクトリにアクセス権がある LDAP マネージャのユーザー ID を入力します。

ステップ 4 [パスワードの確認（Confirm Password）]フィールドに、LDAP マネージャのパスワードを入力します。

ステップ 5 [LDAPユーザー検索ベース（LDAP User Search Base）]フィールドに、検索条件を入力します。

ステップ 6 [LDAPサーバ情報（LDAP Server Information）]セクションで、LDAP サーバのホスト名または IP アドレスを入力します。

ステップ 7 TLS を使用して LDAP サーバに対するセキュアな接続を作成する場合は、[TLSを使用（Use TLS）]チェックボックスをオンにします。

ステップ 8 **[保存]** をクリックします。

次のタスク

LDAP アグリーメント サービス パラメータのカスタマイズ （368 ページ）

LDAP アグリーメント サービス パラメータのカスタマイズ

LDAPアグリーメントのシステムレベルでの設定をカスタマイズする、任意指定のサービス パラメータを設定するには、この手順を実行します。 これらのサービス パラメータを設定しない場合、Unified Communications Manager により、LDAP ディレクトリ統合のデフォルト設定が適用されます。 パラメータの説明については、ユーザ インターフェイスでパラメータ名をクリックしてください。

サービス パラメータを使用して次の設定をカスタマイズできます。

- [最大アグリーメント数（Maximum Number of Agreements）]：デフォルト値は 20 です。
- [最大ホスト数（Maximum Number of Hosts）]：デフォルト値は 3 です。
- [ホスト障害時の再試行の遅延（秒）（Retry Delay On Host Failure (secs)）]：ホスト障害のデフォルト値は 5 です。
- [ホストリスト障害時の再試行の遅延（分）（Retry Delay On HotList failure (mins)）]：ホストリスト障害のデフォルト値は 10 です。
- [LDAP接続のタイムアウト（秒）（LDAP Connection Timeouts (secs)）]：デフォルト値は 5 です。
- [遅延同期の開始時間（分）（Delayed Sync Start time (mins)）]：デフォルト値は 5 です。
- **[ユーザカスタマーマップの監査時間（User Customer Map Audit Time）]**

手順

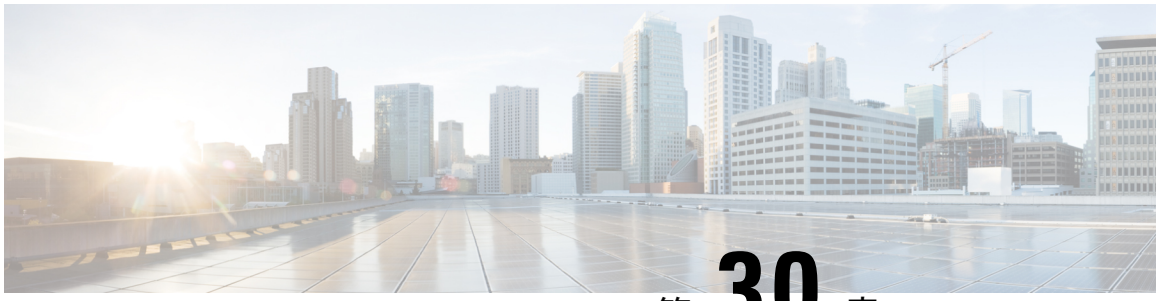
ステップ 1 Cisco Unified CM の管理から、**[システム（System）]** > **[サービス パラメータ（Service Parameters）]** の順に選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リスト ボックスからパブリッシャ ノードを選択します。

ステップ 3 [サービス（Service）]ドロップダウン リスト ボックスから、[Cisco DirSync]を選択します。

ステップ 4 Cisco DirSync サービス パラメータの値を設定します。

ステップ 5 **[保存]** をクリックします。



第 30 章

一括管理ツール使用したユーザおよびデバイスのプロビジョニング

一括管理ツールの概要

一括管理ツール（BAT）は、Unified Communications Manager データベースに対してバルク トランザクションを実行するのに使用できる Web ベースのアプリケーションです。 BAT を使用することで、類似する多数の電話、ユーザ、ポートの追加、更新、または削除を一度に実行できます。

（注） [一括管理（Bulk Administration）] メニューは、Unified Communications Manager サーバの最初のノードでのみ表示されます。

Cisco Unified CM Administration の [一括管理（Bulk Administration）] メニューから送信されたすべてのジョブは、Cisco Bulk Provisioning Service（BPS）によって管理および保守されます。このサービスは、Cisco Unified Serviceability から開始できます。 Cisco Bulk Provisioning Service は、Unified Communications Manager の最初のノード上でのみアクティブ化する必要があります。

BAT を使用して、次の処理を実行できます。

- 多数の電話の追加、更新、または削除を一括で実行する
- 新しい電話のグループを追加する共通の電話属性を定義する
- 新しい BAT 電話テンプレートを作成する
- 新規ユーザのグループを追加し、ユーザを電話やその他の IP テレフォニー デバイスに関連付ける

- BAT スプレッドシートからユーザ CSV データ ファイルを作成する
- 電話とユーザをバッチで追加するための CSV データ ファイルを作成する
- 電話機とユーザのグループを Unified Communications Manager データベースとディレクトリに追加する

一括管理ツールの前提条件

- ユーザおよびサービスのプロファイルの設定

一括管理ツールのタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	データベースへの電話機の追加 （371 ページ）	BAT を使用して、電話およびその他の IP テレフォニー デバイスを Unified Communications Manager データベースに一括で追加します。
ステップ 2	新しい BAT 電話テンプレートの作成 （372 ページ）	新しいBAT電話テンプレートを作成できます。
ステップ 3	BAT スプレッドシートを使用した電話機 CSV データ ファイルの作成 （378 ページ）	BAT で使用するよう設計された .xls 形式のスプレッドシートを使用して、新しい電話または IP テレフォニー デバイスをシステムに追加できます。
ステップ 4	テキストエディタを使用したカスタム電話機ファイル形式の作成 （381 ページ）	テキストエディタを使用して、テキストベースの CSV データ ファイル用にカスタムの電話ファイル形式を作成できます。
ステップ 5	Unified Communications Manager への電話機の挿入 （382 ページ）	電話、Cisco VGC Phone、CTI ポート、または H.323 クライアントを Unified Communications Manager データベースに追加できます。
ステップ 6	ユーザーの追加 （384 ページ）	BAT を使用して、新規ユーザのグループを追加し、ユーザを電話やその他の IP テレフォニーデバイスに関連付けることができます。

	コマンドまたはアクション	目的
ステップ 7	BAT スプレッドシートからのユーザ CSV データ ファイルの作成 （385 ページ）	Unified Communications Manager データベースに新しいユーザを追加するために詳細を BAT スプレッドシートに記述した後、それを CSV データ ファイルに変換できます。
ステップ 8	Unified Communications Manager データベースへユーザを挿入する （386 ページ）	CSV データ ファイルを使用して、ユーザのグループを Unified Communications Manager データベースに追加できます。
ステップ 9	電話機とユーザのファイル形式の追加 （388 ページ）	テキストベースの CSV データ ファイルで電話とユーザのファイル形式を追加することができます。 CSV データ ファイルを作成したら、ファイル形式をテキストベースの CSV データ ファイルに関連付ける必要があります。
ステップ 10	Unified Communications Manager へのユーザ付き電話の挿入 （389 ページ）	電話機とユーザのグループを Unified Communications Manager データベースとディレクトリに追加できます。

データベースへの電話機の追加

BAT を使用して、電話機と他の IP テレフォニー デバイスを一括して Unified Communications Manager データベースに追加する場合は、各電話機に複数の回線、サービス、およびスピードダイヤルを追加することができます。 CTI ポートと H.323 クライアントを追加することもできます。

電話機用の CSV データ ファイルを作成する方法としては、次の 2 つのオプションがあります。

- BAT スプレッドシート（BAT.xlt）を使用し、データを CSV 形式にエクスポートする。
- テキスト エディタを使用して、CSV 形式のテキスト ファイルを作成する（経験豊富なユーザ向け）。

手順

ステップ 1 **[一括管理(Bulk Administration)]** > **[電話(Phones)]** > **[電話テンプレート(Phone Template)]** の順に選択します。

[電話テンプレートの検索/一覧表示(Find and List Phone Templates)]ウィンドウが表示されます。

ステップ 2 電話テンプレートを挿入するための CSV データ ファイルを作成します。

次のいずれかの選択肢を実行します。

a) BAT スプレッドシートを使用して CSV データ ファイルを作成します。

b) 次のように、テキスト エディタを使用して CSV データ ファイルを作成します。

1. **[一括管理(Bulk Administration)]** > **[電話(Phones)]** > **[電話ファイル形式(Phone File Format)]** > **[ファイル形式の作成(Create File Format)]** の順に選択します。
2. テキスト エディタを使用して、使用するファイル形式に従った電話機用の CSV データ ファイルを作成します。
3. **[一括管理(Bulk Administration)]** > **[電話(Phones)]** > **[電話ファイル形式(Phone File Format)]** > **[ファイル形式の追加(Add File Format)]** の順に選択して、テキストベースのファイル形式と CSV データ ファイルを関連付けます。

ステップ 3 **[一括管理(Bulk Administration)]** > **[電話(Phones)]** > **[電話の確認(Validate Phones)]** の順に選択します。

ステップ 4 **[一括管理（Bulk Administration）]** > **[電話（Phones）]** > **[電話の挿入（Insert phones）]** を選択して、電話レコードを Unified Communications Manager データベースに挿入します。

新しい BAT 電話テンプレートの作成

新しい BAT 電話テンプレートを作成できます。 電話テンプレートを作成したら、回線、サービス、およびスピード ダイヤルを追加できます。

手順

ステップ 1 **[一括管理(Bulk Administration)]** > **[電話(Phones)]** > **[電話テンプレート(Phone Template)]** の順に選択します。

ステップ 2 [新規追加] をクリックします。 [新規電話テンプレートを追加(Add a New Phone Template)]ウィンドウが表示されます。

ステップ 3 [電話タイプ（Phone Type）]ドロップダウンリストから、テンプレートを作成する電話モデルを選択します。 [次へ（Next）]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、デバイス プロトコルを選択します。 [次へ（Next）]をクリックします。

[電話テンプレートの設定(Phone Template Configuration)]ウィンドウに、選択したデバイス タイプに対応するフィールドとデフォルトのエントリが表示されます。

ステップ 5 **[テンプレート名(Template Name)]** フィールドに、テンプレートの名前を入力します。

名前には、50 文字以内の英数字を指定することができます。

ステップ 6 [デバイス情報（Device Information）] 領域に、このバッチの共通の電話設定を入力します。

電話モデルとデバイス タイプによっては、一覧に示されている属性がすべて揃っていないものがあります。 すべての属性の詳細については、電話機モデルのマニュアルを参照してください。

ステップ 7 この BAT 電話テンプレートの設定値をすべて入力した後、**[保存(Save)]** をクリックします。

トランザクションが完了したことがステータスに示されたら、回線属性を追加することができます。

BAT テンプレートにおける電話回線の追加または更新

BAT テンプレートに 1 つ以上の回線を追加したり、既存の回線を更新したりすることができます。 BAT テンプレートで使用しているボタン テンプレートにより、追加または更新できる回線の数が決まります。 複数の回線を持つプライマリ電話テンプレートを作成することができます。 さらに、標準規格のテンプレートを使用して、1 回線または標準規格のテンプレートの回線数以下の複数回線を持つ電話機を追加することができます。 選択する設定値は、このバッチ内のすべての電話機またはユーザ デバイス プロファイルで使用されます。

回線テンプレートの値には、英数字を使用することをお勧めします。番号を指定すると、実際のディレクトリ番号と競合する可能性があるためです。 英数字を使用することで、コール ピックアップ グループ番号やコール パーク番号などの情報との競合も回避できます。

BAT テンプレート用に表示される最大回線数は、BAT 電話テンプレートの作成時に選択したモデルとボタン テンプレートによって決まります。 一部の CiscoUnifiedIPPhone モデルでは、CiscoUnifiedIPPhone サービスと短縮ダイヤルもテンプレートに追加できます。

手順

ステップ 1 回線を追加する電話テンプレートを検索します。

ステップ 2 **[電話テンプレートの設定（Phone Template Configuration）]** ウィンドウの **[割り当て情報（Association Information）]** 領域で、**[回線 [1] - 新規 DN を追加（Line [1] - Add a new DN）]** をクリックします。

[回線テンプレートの設定（Line Template Configuration）]ウィンドウが表示されます。

ステップ 3 回線設定値に対して適切な値を入力または選択します。

ステップ 4 **[保存]** をクリックします。

ステップ 5 その他の回線の設定値を追加するには、ステップ 2 （373 ページ） ～ステップ 4 （373 ページ）を繰り返します。

[回線テンプレートの設定（Line Template Configuration）] ウィンドウの右上隅にある **[関連リンク（Related Links）]** ドロップダウン リスト ボックスから [検索/一覧表示に戻る（Back to Find/List）] を選択すると、**[回線テンプレートの検索/一覧表示（Find and List Line Templates）]** ウィンドウが表示されます。

a) 既存の回線テンプレートを検索するには、適切な検索条件を入力して、**[検索(Find)]** をクリックします。

b) 新しい回線テンプレートを追加するには、**[新規追加(Add New)]** をクリックします。

BAT テンプレートにおける IP サービスの追加または更新

BAT テンプレートで機能を直接入力してある CiscoUnifiedIPPhone モデルに、CiscoUnifiedIPPhone サービスを登録できます。 ユーザまたは電話機を IP サービスにまとめて登録するには、IP

サービスが共通のサービス パラメータを持ち、電話テンプレートによって登録されている必要があります。 固有のサービス パラメータを持つ IP サービスをまとめて登録することはできません。 固有のサービス パラメータを持つサービスの場合は、CSV ファイルを使用します。

手順

ステップ 1 IP サービスを追加する電話テンプレートを検索します。

ステップ 2 **[電話テンプレートの設定（Phone Template Configuration）]** ウィンドウの **[割り当て情報（Association Information）]** 領域で、**[新規 SURL を追加（Add a new SURL）]** をクリックします。
ポップアップ ウィンドウが表示されます。 このウィンドウで、利用可能な CiscoUnifiedIPPhone サービスを登録できます。

ステップ 3 **[サービスの選択(Select a Service)]** ドロップダウン リスト ボックスで、すべての電話機に登録するサービスを選択します。 **[サービスの説明(Service Description)]** ボックスに、選択したサービスの詳細が表示されます。

ステップ 4 [次へ（Next）]をクリックします。

ステップ 5 必要に応じて、**[サービス名(Service Name)]** フィールドでサービスの名前を変更します。

ステップ 6 選択したサービスを関連付けるか、他のサービスをテンプレートに追加します。

a) これらの電話サービスを電話テンプレートに関連付けるには、**[保存(Save)]** をクリックします。

b) 他のサービスを追加するには、ステップ 3 （374 ページ） ～ステップ 6 （374 ページ） を繰り返します。

c) すべてのサービスをテンプレートに追加するには、**[更新(Update)]** をクリックします。

選択したテンプレートのサービスの追加または更新が完了したら、次のステップに進みます。

ステップ 7 ポップアップ ウィンドウを閉じます。

BAT テンプレートにおけるスピード ダイヤルの追加または更新

電話機ボタン テンプレートでスピード ダイヤル ボタンが設定されている場合は、電話機および Cisco VGC Phone の BAT テンプレートでスピード ダイヤルを追加または更新することができます。 BAT テンプレートで使用している電話機ボタン テンプレートによって、使用可能なスピード ダイヤル ボタンの数が決まります。

手順

ステップ 1 スピード ダイヤルを追加する電話テンプレートを検索します。

ステップ 2 [電話テンプレートの設定(Phone Template Configuration)]ウィンドウで、次のいずれかを実行します。

a) **[割り当て情報（Association Information）]** 領域で、**[新規 SD を追加（Add a new SD）]** をクリックします。

b) ウィンドウの右上隅にある **[関連リンク（Related Links）]** ドロップダウン リスト ボックスから、[短縮ダイヤルの追加/更新（Add/Update Speed Dials）] を選択します。

ポップアップ ウィンドウが表示されます。 このウィンドウで、CiscoUnifiedIPPhones および拡張モジュールに対して、スピード ダイヤル ボタンを指定できます。

ステップ 3 **[スピードダイヤル設定(Speed Dial Settings)]** 領域で、アクセス コードや長距離コードを含めて、電話番号を **[番号(Number)]** フィールドに入力します。

（注） 電話番号を入力する際、必要に応じて、電話番号の後に強制承認コード（FAC）またはクライアント識別コード（CMC）を入力できます。 電話番号、FAC、CMC は、続けて入力するか、カンマ（,）で区切って入力することができます。 スピードダイヤルには、暗証番号、パスワード、およびその他の、コールが接続された後に DTMF ディジットとして送信される数字を含めることができます。 スピードデジタルによる接続中に一時停止が必要な場合は、1 つ以上のカンマ（,）を入力してください。各カンマは、2 秒間の一時停止を表します。 DTMF ディジットは、コールが接続された後に、カンマの数に対応する時間の一時停止を挟んで送信されます。

ステップ 4 **[ラベル(Label)]** フィールドに、スピード ダイヤル番号に対応するラベルを入力します。

ステップ 5 **[短縮ダイヤル設定(Abbreviated Dial Settings)]** 領域で、該当する IP Phone モデルに短縮ダイヤルを設定することができます。 ステップ 3 （375 ページ） を繰り返します。

ステップ 6 **[保存]** をクリックします。

BAT によってテンプレートにスピード ダイヤル設定値が挿入され、ポップアップ ウィンドウが閉じます。

BAT テンプレートにおけるビジー ランプ フィールドの追加または更新

電話機ボタン テンプレートでスピード ダイヤル ボタンが設定されている場合は、電話機および Cisco VGC Phone の BAT テンプレートでビジー ランプ フィールド スピード ダイヤルを追加または更新することができます。 BATテンプレートで使用している電話機ボタンテンプレートによって、使用可能な BLF SD ボタンの数が決まります。

手順

ステップ 1 スピード ダイヤルを追加する電話テンプレートを検索します。

ステップ 2 [電話テンプレートの設定(Phone Template Configuration)]ウィンドウで、次のいずれかを実行します。

a) **[割り当て情報（Association Information）]** 領域で、**[新規 BLF SD を追加（Add a new BLF SD）]** をクリックします。

b) ウィンドウの右上隅にある **[関連リンク（Related Links）]** ドロップダウンリストから、[ビジーランプフィールド短縮ダイヤルの追加/更新（Add/Update Busy Lamp Field Speed Dials）] を選択します。

ポップアップ ウィンドウが表示されます。 このウィンドウで、CiscoUnifiedIPPhones および拡張モジュールに対して、ビジー ランプ フィールド スピード ダイヤル（BLF SD）ボタンを指定できます。

ステップ 3 [スピードダイヤル設定(Speed Dial Settings)]領域で、アクセス コードや長距離コードを含めて、電話番号を **[接続先(Destination)]** フィールドに入力します。

ステップ 4 ドロップダウン リストから、ディレクトリ番号を選択します。 **[検索(Find)]** をクリックすると、ディレクトリ番号を検索できます。

ステップ 5 **[ラベル(Label)]** フィールドに、BLF SD 番号に対応するラベルを入力します。

ステップ 6 **[保存]** をクリックします。
BAT によってテンプレートに BLF SD 設定値が挿入され、ポップアップ ウィンドウが閉じます。

BAT テンプレートにおけるビジー ランプ フィールド ダイレクト コール パークの追加または更新

電話機ボタン テンプレートでスピード ダイヤル ボタンが設定されている場合は、電話機および Cisco VGC Phone の BAT テンプレートでビジー ランプ フィールド（BLF）ダイレクト コール パークを追加または更新することができます。 この BAT テンプレートで使用している電話機ボタン テンプレートによって、使用可能な BLF ダイレクト コール パーク ボタンの数が決まります。

手順

ステップ 1 BLF スピード ダイレクト コール パークを追加する電話テンプレートを検索します。

ステップ 2 [電話テンプレートの設定(Phone Template Configuration)]ウィンドウで、次のいずれかを実行します。

a) **[割り当て情報（Association Information）]** 領域で、**[新規 BLF ダイレクトコールパークの追加（Add a new BLF Directed Call Park）]** をクリックします。

b) ウィンドウの右上隅にある **[関連リンク（Related Links）]** ドロップダウン リスト ボックスから、**[BLFダイレクトコールパークの追加/更新（Add/Update BLF Directed Call Park）]** を選択します。

ポップアップ ウィンドウが表示されます。 このウィンドウで、CiscoUnifiedIPPhones および拡張モジュールに対して、BLF ダイレクト コール パーク ボタンを指定できます。

ステップ 3 **[割り当てられていないビジーランプフィールド/ダイレクトコールパークの設定（Unassigned Busy Lamp Field/Directed Call Park Settings）]**領域で、ドロップダウン リストからディレクトリ番号を選択します。 **[検索(Find)]** をクリックすると、ディレクトリ番号を検索できます。

ステップ 4 **[ラベル(Label)]** フィールドに、BLF ダイレクト コール パーク番号に対応するラベルを入力します。

ステップ 5 **[保存]** をクリックします。

BAT によってテンプレートに BLF ダイレクト コール パーク設定が挿入され、ポップアップ ウィンドウが閉じます。

BAT テンプレートにおけるインターコム テンプレートの追加または更新

BAT テンプレートに 1 つ以上のインターコム テンプレートを追加したり、BAT テンプレートの既存のインターコム テンプレートを更新したりすることができます。BAT テンプレートで使用しているボタン テンプレートにより、追加または更新できる回線の数が決まります。 複数の回線を持つ標準規格の電話テンプレートを作成することができます。 さらに、標準規格のテンプレートを使用して、1 回線または標準規格のテンプレートの回線数以下の複数回線を持つ電話機を追加することができます。 インターコム テンプレート用に選択する設定値は、このバッチ内のすべての電話機またはユーザ デバイス プロファイルで使用されます。

インターコムテンプレートには、英数字を使用することを推奨します。番号を指定すると、実際のディレクトリ番号と競合する可能性があるためです。 英数字を使用することで、コール ピックアップ グループ番号やコール パーク番号などの情報との競合も回避できます。

BAT テンプレート用に表示される最大回線数は、BAT 電話テンプレートの作成時に選択したモデルとボタン テンプレートによって決まります。 一部の CiscoUnifiedIPPhone モデルでは、CiscoUnifiedIPPhone サービスと短縮ダイヤルもテンプレートに追加できます。

手順

ステップ 1 インターコム テンプレートを追加する電話テンプレートを検索します。

ステップ 2 **[電話テンプレートの設定（Phone Template Configuration）]** ウィンドウの **[割り当て情報（Association Information）]** 領域で、**[インターコム [1] - 新規インターコムの追加（Intercom [1] - Add a new Intercom）]** をクリックします。
[インターコムテンプレートの設定(Intercom Template Configuration)]ウィンドウが表示されます。

ステップ 3 インターコム テンプレート設定値に対して、適切な値を入力または選択します。

ステップ 4 **[保存]** をクリックします。
BAT によって、インターコム テンプレートが電話テンプレート設定に追加されます。

ステップ 5 その他のインターコムテンプレートの設定値を追加するには、ステップ 2 （377 ページ） ～ステップ 4 （377 ページ） を繰り返します。

[インターコムテンプレートの設定（Intercom Template Configuration）] ウィンドウの右上隅にある **[関連リンク（Related Links）]** ドロップダウン リスト ボックスから [検索/一覧表示に戻る（Back to Find/List）] を選択すると、**[インターコム電話番号の検索/一覧表示（Find and List Intercom Directory Numbers）]** ウィンドウが表示されます。

（注） **[インターコムテンプレートの設定（Intercom Template Configuration）]** ウィンドウの右上隅にある **[関連リンク（Related Links）]** ドロップダウン リスト ボックスから [検索/一覧表示に戻る（Back to Find/List）] を選択すると、**[インターコム電話番号の検索/一覧表示（Find and List Intercom Directory Numbers）]** ウィンドウが表示されます。

a) 既存のインターコムディレクトリ番号を検索するには、適切な検索条件を入力して、**検索(Find)** をクリックします。
b) 新しいインターコムディレクトリ番号を追加するには、**インターコム電話番号の検索/一覧表示(Find and List Intercom Directory Numbers)**ウィンドウで、**新規追加(Add New)** をクリックします。

BAT スプレッドシートを使用した電話機 CSV データ ファイルの作成

BAT スプレッドシートを使用して、CSV データ ファイルを作成します。 スプレッドシート内でファイル形式を定義することができるので、BAT スプレッドシートはデータ ファイル形式を使用して CSV データ ファイルのフィールドを表示します。

（注） いずれかのフィールドにカンマを入力した場合、BAT.xlt を使用して BAT 形式にエクスポートするときに、そのフィールド エントリは二重引用符で囲まれます。

BAT スプレッドシートにブランク行を入力すると、その空の行はファイルの終わりとして扱われ、ブランク行の後に入力されているデータは BAT 形式に変換されません。

CTI ポートを追加する際に、ダミー MAC アドレス オプションを使用することができます。 このオプションを使用すると、ダミー MAC アドレスの形式で、CTI ポートごとに固有のデバイス名が指定されます。このダミー MAC アドレスは、後で、 Cisco Unified Communications Manager Administration の管理ページまたは UnifiedCM Auto-Register Phone Tool を使用して手動で更新できます。 H.323 クライアント、VGC Phone、および VGC Virtual Phone には、ダミー MAC アドレス オプションを使用しないでください。

ダミー MAC アドレス オプションでは、次の形式のダミー MAC アドレスが自動的に生成されます。

XXXXXXXXXXXX

ここで、X は任意の 12 文字の 16 進数（0 ～ 9 および A ～ F）を表します。

注目 BAT スプレッドシートで電話機に関して定義する回線およびスピード ダイヤルの数は、BAT 電話テンプレートで定義されている数を超えないようにしてください。この数を超えている場合、CSV データ ファイルおよび BAT テンプレートを挿入しようとするとエラーが発生します。

BAT スプレッドシートのすべてのフィールドの編集が完了したら、内容を CSV 形式のデータ ファイルにエクスポートできます。 エクスポートされる CSV 形式のデータ ファイルには、次のようなデフォルトのファイル名が割り当てられます。

```
<tabname>-<timestamp>.txt
```

ここで、<tabname>は、作成した入力ファイルのタイプ（たとえば、電話）を表し、<timestamp>は、ファイルが作成された正確な日時を表します。

エクスポートされたファイルをローカル ワークステーション上に保存したら、この CSV 形式のデータ ファイルの名前を変更することができます。

（注） カンマが入った CSV ファイル名（例：abcd,e.txt）は、Unified Communications Manager サーバにアップロードできません。

手順

ステップ 1 BAT.xlt ファイルを検索し、ダブルクリックして、BAT スプレッドシートを開きます。

ステップ 2 プロンプトが表示されたら、**[マクロを有効にする]**ボタンをクリックして、スプレッドシート機能を使用します。

ステップ 3 電話機オプションを表示するには、スプレッドシートの下部にある **[電話 (Phones)]** タブをクリックします。

ステップ 4 次のデバイス タイプのいずれかのオプション ボタンを選択します。

選択するデバイス タイプによってBAT スプレッドシート内のデータの検索条件が決まります。

- 電話機
- [CTIポート(CTI Port)]
- [H.323クライアント(H.323 Client)]
- [VGC Phone]
- [VGC Virtual Phone]
- [Cisco IP Communicator Phone]

スプレッドシートには、選択されたデバイスで使用可能なオプションが表示されます。 たとえば、[電話(Phones)] を選択すると、電話回線数とスピード ダイヤル数のフィールドが表示されます。

ステップ 5 各電話機の BAT スプレッドシートに表示するデバイスと回線のフィールドを選択します。 次の手順を実行します。

a) **[ファイル形式の作成(Create File Format)]** をクリックします。

b) デバイス フィールドを選択するには、**[デバイスフィールド(Device Fields)]** ボックスでデバイス フィールド名をクリックし、次に矢印をクリックしてそのフィールドを **[選択済みのデバイスフィールド(Selected Device Fields)]** ボックスに移動します。

CSV データ ファイルには、**[MACアドレス/デバイス名(MAC Address/Device Name)]** および **[説明(Description)]** を含める必要があります。したがって、これらのフィールドは常に選択された状態になっています。

ヒント　リスト内の特定範囲のフィールドを複数同時に選択するには、**Shift** キーを押しながらフィールド名をクリックします。 複数のフィールドを任意に選択するには、**Ctrl** キーを押しながらフィールド名をクリックします。

c) **[回線フィールド(Line Fields)]** ボックスで回線フィールド名をクリックしてから、矢印をクリックしてそのフィールドを **[選択済みの回線フィールド(Selected Line Fields)]** ボックスに移動します。

ヒント　**[選択されている回線(Selected Line)]** ボックスと **[デバイス(Device)]** ボックス内の項目の順序を変更するには、項目を選択し、上矢印と下矢印を使用して、リスト内でフィールドを上または下に移動します。

d) 既存の CSV 形式を上書きするかどうかを確認するメッセージが表示されます。 CSV データ ファイル形式を修正するには、**[作成(Create)]** をクリックします。

e) **OK**をクリックします。
選択したフィールド用の新しいカラムが、指定した順序で BAT スプレッドシートに表示されます。

ステップ 6　**[電話回線数(Number of Phone Lines)]** ボックスが表示されるまで右にスクロールし、電話機の回線数を入力します。

（注）　入力する回線数は、BAT テンプレートで設定した回線数を超えることはできません。

ステップ 7　電話機の **[スピードダイヤルの最大数(Maximum Number of Speed Dials)]** ボックスでスピードダイヤル ボタンの数を入力する必要があります。

（注）　入力するスピード ダイヤル数は、BAT テンプレートで設定したスピード ダイヤル数を超えることはできません。

ボタン数を入力すると、各スピード ダイヤル番号用のカラムが表示されます。

ステップ 8　**[BLFスピードダイヤルの最大数(Maximum Number of BLF Speed Dials)]** ボックスで、ビジー ランプ フィールド（BLF）スピード ダイヤル ボタンの数を入力します。
ボタン数を入力すると、各 BLF スピード ダイヤル番号用のカラムが表示されます。

ステップ 9　スプレッドシートで回線ごとに個々の電話機のデータを入力します。

すべての必須フィールド、および該当するオプション フィールドに値を入力します。 各カラムの見出しは、フィールドの長さ、およびそのフィールドが必須かオプションかを指定しています。 電話フィールドの説明については、オンライン ヘルプを参照してください。

ステップ 10　電話機ごとに MAC アドレスを入力しなかった場合は、**[ダミーMACアドレスの作成(Create Dummy MAC Address)]** チェックボックスをオンにします。

注目　H.323 クライアント、VGC Phone、および VGC Virtual Phone には、ダミー MAC アドレス オプションを使用しないでください。

ステップ 11　**[BAT形式にエクスポート(Export to BAT Format)]** をクリックして BAT Excel スプレッドシートから CSV 形式のデータ ファイルにデータを転送します。

ヒント　エクスポートされた CSV データファイルを読み取る方法の詳細については、BAT 内の **[電話の挿入（Insert Phones）]** ウィンドウで **[サンプルファイルの表示（View Sample File）]** へのリンクをクリックしてください。

このファイルは、デフォルトのファイル名（`<tabname>-<timestamp>.txt`）で、ローカルワークステーション上で選択したフォルダに保存されます。

テキスト エディタを使用したカスタム電話機ファイル形式の作成

テキスト エディタを使用して、テキストベースの CSV データ ファイル用にカスタムの電話ファイル形式を作成できます。

手順

ステップ 1　**[一括管理(Bulk Administration)]** > **[電話(Phones)]** > **[電話ファイル形式(Phone File Format)]** > **[ファイル形式の作成(Create File Format)]** の順に選択します。

ステップ 2　[新規追加] をクリックします。

ステップ 3　**[形式名(Format Name)]** フィールドに、このカスタム形式の名前を入力します。

ステップ 4　カスタム ファイル形式に表示するフィールドを選択します。 次の手順を実行します。

a) デバイス フィールドを選択するには、**[デバイスフィールド(Device Fields)]** ボックスでデバイス フィールド名をクリックし、次に矢印をクリックしてそのフィールドを **[選択済みのデバイスフィールド(Selected Device Fields)]** ボックスに移動します。

CSV データ ファイルには、**[MACアドレス/デバイス名(MAC Address/Device Name)]** および **[説明(Description)]** を含める必要があります。したがって、これらのフィールドは常に選択された状態になっています。

ヒント　リスト内の特定範囲のフィールドを複数同時に選択するには、**Shift** キーを押しながらフィールド名をクリックします。 複数のフィールドを任意に選択するには、**Ctrl** キーを押しながらフィールド名をクリックします。

b) **[回線フィールド(Line Fields)]** ボックスで回線フィールド名をクリックしてから、矢印をクリックしてそのフィールドを **[選択済みの回線フィールド(Selected Line Fields)]** ボックスに移動します。

c) **[インターコムDNフィールド(Intercom DN Fields)]** ボックスでインターコム DN フィールドの名前をクリックしてから矢印をクリックし、そのフィールドを **[選択済みのインターコムDNフィールド(Selected Intercom DN Fields)] の [順序(Order)]** ボックスに移動します。

ヒント　**[選択済みの回線フィールド(Selected Line Fields)]**、**[選択済みのデバイスフィールド(Selected Device Fields)]**、および **[選択済みのインターコムDNフィールド(Selected Intercom DN Fields)] の [順序(Order)]** ボックス内の項目の順序は変更できます。 項目を選択し、上矢印と下矢印を使用して、リスト内でフィールドを上または下に移動します。

ステップ 5 [IP Phoneサービスの最大数(IP Phone Services Maximums)]領域で、次のフィールドに最大値を入力します。

- [スピードダイヤルの最大数(Maximum Number of Speed Dials)]
- [BLFスピードダイヤルの最大数(Maximum Number of BLF Speed Dials)]
- [BLFダイレクトコールパークの最大数(Maximum Number of BLF Directed Call Parks)]
- [IP Phoneサービスの最大数(Maximum Number of IP Phone Services)]
- [IP Phoneサービスパラメータの最大数(Maximum Number of IP Phone Service Parameters)]

ステップ 6 **[保存]** をクリックします。
カスタムファイル形式の名前が、**[電話ファイル形式の検索/一覧表示（Find and List Phone File Formats）]** ウィンドウの **[ファイル形式名（File Format Names）]** リストに表示されます。

Unified Communications Manager への電話機の挿入

電話機レコードを Unified Communications Manager データベースに挿入する際は、ターゲット CSV データ ファイルと、電話機レコードの挿入方法を定義します。 次の操作の任意の組み合わせを選択して、既存の電話機レコードを上書きします。または、アップロード時にレコードを挿入することもできます。

- 新しい短縮ダイヤルを追加する前に、既存の短縮ダイヤルをすべて削除してください。
- 新しい短縮ダイヤルを追加する前に、既存のBLF短縮ダイヤルをすべて削除してください。
- 新しいコールパークを追加する前に、既存のすべてのBLFダイレクトコールパークを削除してください。
- 新しいサービスを追加する前に、既存のすべての登録サービスを削除してください。

（注） 電話機レコードを、挿入前に確認する必要があります。

（注） BAT には、次の形式の電話番号のための電話番号 URI フィールドが必要です。

ディレクトリ番号 1 では URI 1 、ディレクトリ番号 1 では URI 1 ルート パーティション、ディレクトリ番号 1 では URI 1 がプライマリです。

ダミー MAC アドレス オプションを使用することができます。 CTI ポートを追加する場合、このオプションを使用すると、ダミー MAC アドレスの形式で、CTI ポートごとに固有のデバイス名が指定されます。このダミー MAC アドレスは、後で、Unified Communications Manager の管理ページまたは UnifiedCM Auto-Register Phone Tool を使用して手動で更新できます。 H.323

クライアント、VGC Phone、および VGC Virtual Phone には、ダミー MAC アドレス オプションを使用しないでください。

ダミー MAC アドレス オプションでは、次の形式のダミー MAC アドレスが自動的に生成されます。

XXXXXXXXXXXX

ここで、X は任意の 12 文字の 16 進数（0 ～ 9 および A ～ F）を表します。

始める前に

- 追加するデバイスには、Unified Communications Manager 一括管理（BAT）電話テンプレートが必要です。 データ ファイルのアップロード先とアップロード方法を選択できます。 電話機レコードを、挿入前に確認する必要があります。
- 電話機または他の IP テレフォニー デバイスに固有の詳細を含むカンマ区切り値（CSV）形式のデータ ファイルが必要です。

手順

ステップ 1 **[一括管理(Bulk Administration)]** > **[電話(Phones)]** > **[電話の挿入(Insert Phones)]** の順に選択します。

ステップ 2 アップロードする電話機レコードのファイル形式のタイプを指定します。

a) カスタマイズされたファイル形式を使用する電話機レコードを挿入するには、**[電話固有の詳細の挿入(Insert Phones Specific Details)]** オプション ボタンをクリックして、ステップ 3 （383 ページ） と ステップ 5 （384 ページ） を続けます。

b) [すべての詳細(All Details)] オプションを使用して生成したエクスポート電話機ファイルから電話機レコードを挿入するには、**[電話のすべての詳細の挿入(Insert Phones All Details)]** オプション ボタンをクリックします。

ステップ 3 **[ファイル名(File Name)]** ドロップダウン リスト ボックスで、この特定のバルク トランザクション用に作成した CSV データ ファイルを選択します。 次に、選択したカスタムファイルで電話機を更新できるようにするには、**[カスタムファイルで電話機の更新を許可する]** チェックボックスをオンにします。

ステップ 4 **[既存の設定の上書き(Override the existing configuration)]** チェックボックスをオンにすると、既存の電話機の設定が、挿入するファイルに含まれている情報によって上書きされます。 次に、アップロード中に実行するアップロードアクションの横にあるチェックボックスをオンにします。

[既存の設定の上書き(Override the existing configuration)] チェックボックスをオンにすると、次のアップロード操作が選択可能になります。

- 新しい短縮ダイヤルを追加する前に、既存の短縮ダイヤルをすべて削除してください。
- 新しい短縮ダイヤルを追加する前に、既存のBLF短縮ダイヤルをすべて削除してください。
- 新しいコールパークを追加する前に、既存のすべてのBLFダイレクトコールパークを削除してください。

- 新しいサービスを追加する前に、既存のすべての登録サービスを削除してください。

（注） 当該のレコードをアップロード時に CSV データ ファイルの既存のレコードに追加する場合は、チェックボックスをオフにします。

ステップ 5 [固有の詳細(Specific Details)] オプションを選択した場合は、**[電話テンプレート名(Phone Template Name)]** ドロップダウン リストで、このタイプのバルク トランザクション用に作成した BAT 電話テンプレートを選択します。

注目 CSV データ ファイルに個々の MAC アドレスを入力しなかった場合は、**[ダミー MAC アドレスの作成(Create Dummy MAC Address)]** チェックボックスをオンにする必要があります。 この情報は、後で、手動で更新できます。 ステップ 8 （384 ページ）に進みます。 データ入力ファイルに MAC アドレスまたはデバイス名を指定した場合は、このオプションを選択しないでください。

ユーザに割り当てられる電話機の MAC アドレスがわからない場合には、このオプションを選択します。 電話機が接続されると、そのデバイスに対する MAC アドレスが登録されます。

ステップ 6 **[ジョブ情報(Job Information)]** 領域に、ジョブの説明を入力します。

ステップ 7 挿入の方法を選択します。 次のいずれかを実行します。

a) 電話機レコードをすぐに挿入する場合は、**[今すぐ実行(Run Immediately)]** をクリックします。

b) 後で電話レコードを挿入するには、**[後で実行(Run Later)]**をクリックします。

ステップ 8 **[送信(Submit)]** をクリックして、電話機レコードを挿入するジョブを作成します。

[ジョブの設定(Job Configuration)] ウィンドウで、このジョブのスケジュールやアクティブ化を行います。

次のタスク

挿入する電話機のタイプが Cisco Unified Mobile Communicator である場合は、挿入ジョブを完了した後でデバイスをリセットする必要があります。 電話機をリセットするには、**[一括管理(Bulk Administration)]** > **[電話(Phones)]** > **[電話のリセット/リスタート(Reset/Restart Phones)]** の順に選択します。

ユーザーの追加

BAT スプレッドシートを使用して新しい複数のユーザを Unified Communications Manager データベースに一括して追加するには、CSV データ ファイルを作成する必要があります。 ユーザに CiscoIPSoftPhone などの CTI ポートを必要とするアプリケーションがある場合、BAT を使用して CTI ポートを既存のユーザに関連付けられます。

手順

ステップ 1 カンマ区切り値（CSV）データ ファイルを作成して、追加するユーザごとに個々の値を定義します。

ステップ 2 BAT を使用して、ユーザを Unified Communications Manager データベースに挿入します。

BAT スプレッドシートからのユーザ CSV データ ファイルの作成

Unified Communications Manager データベースに新しいユーザを追加するために詳細を BAT スプレッドシートに記述した後、それを CSV データ ファイルに変換できます。

（注） BAT スプレッドシートにブランク行を入力すると、その空の行はファイルの終わりとして扱われ、ブランク行の後に入力されているデータは BAT 形式に変換されません。

BAT スプレッドシートのユーザを追加するためのフィールドの編集が完了したら、内容を CSV 形式のデータ ファイルにエクスポートできます。 エクスポートされる CSV 形式のデータ ファイルには、次のようなデフォルトのファイル名が割り当てられます。

```
<tabname>-<timestamp>.txt
```

ここで、<tabname>は、作成した入力ファイルのタイプ（たとえば、電話）を表し、<timestamp>は、ファイルが作成された正確な日時を表します。

エクスポートされたファイルをローカル ワークステーション上に保存したら、この CSV 形式のデータ ファイルの名前を変更することができます。 いずれかのフィールドにカンマを入力した場合、BAT.xlt を使用して BAT 形式にエクスポートするときに、そのフィールド エントリは二重引用符で囲まれます。

（注） カンマが入った CSV ファイル名（例：abcd,e.txt）は、Unified Communications Manager サーバにアップロードできません。

手順

ステップ 1 BAT.xlt ファイルを見つけ、ダブルクリックして、BAT スプレッドシートを開きます。

ステップ 2 プロンプトが表示されたら、**[マクロを有効にする]**ボタンをクリックして、スプレッドシート機能を使用します。

ステップ 3 ユーザを追加するには、スプレッドシートの下部にある **[ユーザ(Users)]** タブをクリックします。

ステップ 4 すべての必須フィールド、および該当するオプション フィールドに値を入力します。 各カラムの見出しは、フィールドの長さ、およびそのフィールドが必須かオプションかを指定しています。

各行に、 オンラインヘルプファイルで説明されている情報を指定します。

- ユーザが複数のデバイスを持つ場合、デバイス名フィールドは各デバイスに1つずつ設定します。
- 新しいユーザに関連付ける追加のデバイス名を入力するには、**[制御するデバイスの数(Number of Controlled Devices)]** テキスト ボックスに値を入力します。

（注） CTI ポート、ATA ポート、および H.323 クライアントなど、すべてのデバイスをユーザに関連付けることができます。

ステップ 5 新しいユーザに関連付ける追加のデバイス名を入力するには、**[制御するデバイスの数(Number of Controlled Devices)]** テキスト ボックスに値を入力します。

ステップ 6 **[BAT形式にエクスポート(Export to BAT Format)]** をクリックして BAT Excel スプレッドシートから CSV 形式のデータ ファイルにデータを転送します。

このファイルは、デフォルトのファイル名（<tabname>-<timestamp>.txt）で、C:\XLSDataFiles に保存されます。あるいは **[参照（Browse）]** を使用して別の既存フォルダに保存することもできます。

ヒント エクスポートされた CSV データファイルを読み取る方法については、BAT 内の **[ユーザの挿入（Insert Users）]** ウィンドウで、**[サンプルファイルの表示（View Sample File）]** へのリンクをクリックしてください。

次のタスク

CSV データ ファイルを Unified Communications Manager データベース サーバの最初のノードにアップロードして、BAT がデータ ファイルにアクセスできるようにする必要があります。

Unified Communications Manager データベースへユーザを挿入する

CSV データ ファイルを使用して、ユーザのグループを Unified Communications Manager データベースに追加できます。 ユーザを挿入するためにCSVファイルに入力したフィールド値によって、ユーザ テンプレートに設定された値が上書きされます。

注目 信用証明書 ポリシーが「[単純すぎるパスワードの確認(Check for Trivial Passwords)]」を有効にしていて、ユーザ テンプレートのパスワードがユーザ ID であり、ユーザー ID が単純すぎるパスワードに必要な条件を満たさない場合は、BAT を介したユーザの挿入が失敗することがあります。

ユーザは、制御するデバイスの対象として選択されたデバイスを使用せずに設定されたプライマリ内線がある BAT を使用して挿入できます。 それには、BAT を使用してユーザを挿入する前に、Unified Communications Manager で DN を事前実装する必要があります。 DN を事前に定義する手順の概要は、次のとおりです。

1. DN ページでユーザのプライマリ内線に関連付けられる DN の範囲を作成します。
2. 設定したプライマリ内線（事前実装した DN と同じになる）で BAT テンプレートを作成します。
3. 次の手順の説明に従い、BAT を使用してユーザを挿入します。

始める前に

ユーザ名、制御するデバイスの名前、およびディレクトリ番号が格納されている、UTF-8 符号化形式で保存された CSV データ ファイルが必要です。 この CSV データ ファイルは、次のいずれかの方法で作成できます。

- BAT スプレッドシートを CSV 形式に変換する。
- エクスポート ユーティリティで、ユーザ データのエクスポート ファイルを作成する。

（注） エクスポートした BAT ファイルを使用してユーザを挿入している場合、複数のファイルにエクスポートされたユーザについて、「「ユーザー ID がすでに存在しています」」というエラーが表示されることがあります。 たとえば、1 つ目の回線マネージャのリストとユーザのリストが、どちらも同じマネージャ ユーザー ID を含んでいることがあります。

手順

ステップ 1 **[一括管理(Bulk Administration)]** > **[ユーザ(Users)]** > **[ユーザの挿入(Insert Users)]** の順に選択します。

ステップ 2 **[ファイル名(File Name)]** フィールドで、このバルクトランザクション用に作成した CSV データ ファイルを選択します。

ステップ 3 エクスポート ユーティリティを使用して作成した CSV データ ファイルの場合は、**[ユーザのエクスポートで作成されたファイル(File created with Export Users)]** チェックボックスをオンにします。

ステップ 4 **[ユーザテンプレート名(User Template Name)]** ドロップダウン リストから、挿入に使用するユーザ テンプレートを選択します。

（注） ユーザ プロファイル、制御するデバイスの名前、およびディレクトリ番号は、Unified Communications Manager データベースに存在している必要があります。 制御するデバイスの完全な名前を入力する必要があります。 デバイス名に MAC アドレスしか含まれていない場合は、デバイスが存在しないことを示すエラーが BAT に表示されます。

ステップ 5 **[ジョブ情報(Job Information)]** 領域に、ジョブの説明を入力します。

ステップ 6 挿入の方法を選択します。 次のいずれかを実行します。

a) ユーザ レコードをすぐに挿入する場合は、**[今すぐ実行(Run Immediately)]** をクリックします。

b) ユーザ レコードを後で挿入する場合は、**[後で実行(Run Later)]** をクリックします。

ステップ 7 ユーザ レコードを挿入するジョブを作成するには、**[送信(Submit)]** をクリックします。

このジョブのスケジュールやアクティブ化を行うには、[一括管理(Bulk Administration)]メインメニューの [ジョブスケジューラ(Job Scheduler)]オプションを使用します。

BAT スプレッドシートを使用した電話機とユーザの追加

電話機とユーザを一括して追加するための CSV データ ファイルを作成します。

手順

ステップ 1 BAT.xlt ファイルを見つけ、ダブルクリックして、BAT スプレッドシートを開きます。

BAT.xlt ファイルをダウンロードすることができます。

ステップ 2 プロンプトが表示されたら、**[マクロを有効にする]**ボタンをクリックして、スプレッドシート機能を使用します。

ステップ 3 スプレッドシートの下部にある **[電話-ユーザ(Phones-Users)]** タブをクリックします。

ステップ 4 BAT スプレッドシートを使用した電話機 CSV データ ファイルの作成 （378 ページ）のステップ 4 ～ 10 の作業を行います。

電話機とユーザのファイル形式の追加

テキストベースの CSV データ ファイルで電話とユーザのファイル形式を追加することができます。 CSVデータ ファイルを作成したら、ファイル形式をテキストベースのCSVデータ ファイルに関連付ける必要があります。 ファイル形式を CSV ファイルに関連付けると、各フィールドの名前はCSV データ ファイルの最初のレコードとして表示されます。 この情報を使用して、各フィールドの値を正しい順序で入力してあることが確認できます。

始める前に

更新するユーザごとに個々の値を定義する CSV データ ファイルを作成する必要があります。

テキスト エディタを使用して CSV データ ファイルを作成した場合は、テキストベースのファイルに値を入力するためのファイル形式をすでに作成したということになります。 値は、ファイル形式で指定されている順序でテキスト ファイルに入力済みです。

手順

ステップ 1 **[一括管理（Bulk Administration）] > [電話とユーザ（Phones and Users）] > [電話とユーザのファイル形式（Phones & Users File Format）] > [ファイル形式の割り当て（Assign File Format）]** の順に選択します。
[ファイル形式の追加（Add File Format Configuration）]ウィンドウが表示されます。

ステップ 2 **[ファイル名（File Name）]** フィールドで、このトランザクション用に作成したテキストベースの CSV ファイルを選択します。

ステップ 3 **[形式ファイル名（Format File Name）]** フィールドで、このタイプのバルクトランザクション用に作成したファイル形式を選択します。

ステップ 4 一致するファイル形式を CSV データ ファイルに関連付けるジョブを作成するには、**[送信（Submit）]** をクリックします。

ステップ 5 このジョブのスケジュールやアクティブ化を行うには、[一括管理（Bulk Administration）]メイン メニューの [ジョブスケジューラ（Job Scheduler）] オプションを使用します。

（注） ファイル形式を追加すると、ユーザ フィールドが自動的に追加されます。

Unified Communications Manager へのユーザ付き電話の挿入

電話機とユーザのグループを Unified Communications Manager データベースとディレクトリに追加できます。

（注） 電話機レコードを、挿入前に確認する必要があります。

ダミー MAC アドレス オプションを使用することができます。 CTI ポートを追加する場合、このオプションを使用すると、ダミー MAC アドレスの形式で、CTI ポートごとに固有のデバイス名が指定されます。このダミー MAC アドレスは、後で、Unified Communications Manager の管理ページまたは UnifiedCM Auto-Register Phone Tool を使用して手動で更新できます。 H.323 クライアント、VGC Phone、および VGC Virtual Phone には、ダミー MAC アドレス オプションを使用しないでください。

ダミー MAC アドレス オプションでは、次の形式のダミー MAC アドレスが自動的に生成されます。

XXXXXXXXXXXX

ここで、X は任意の 12 文字の 16 進数（0 ～ 9 および A ～ F）を表します。

始める前に

1. カンマ区切り値（CSV）データ ファイルを作成して、挿入する電話機およびユーザごとに個々の値を定義します。 BAT スプレッドシート（BAT.xlt）を使用して CSV データ ファ

イルを作成し、電話機とユーザを追加することができます。あるいは、CSV形式のカスタムテキストファイルを作成し、電話機とユーザの組み合わせを追加することができます。

2. ファイル形式と CSV データ ファイルを関連付けます。
3. 電話機とユーザ レコードを検証します。

手順

ステップ 1 **[一括管理(Bulk Administration)]** > **[電話とユーザ(Phones & Users)]** > **[ユーザ付きの電話の挿入(Insert Phones with Users)]** の順に選択します。

ステップ 2 **[ファイル名(File Name)]** フィールドで、このバルク トランザクション用に作成した CSV データ ファイルを選択します。

ステップ 3 **[電話テンプレート名(Phone Template Name)]** フィールドで、このトランザクションに使用した BAT 電話テンプレートを選択します。

注目 CSVデータ ファイルに個々のMACアドレスを入力しなかった場合は、**[ダミーMACアドレスの作成(Create Dummy MAC Address)]** チェックボックスをオンにする必要があります。 この情報は、後で、手動で更新できます。 データ入力ファイルにMAC アドレスまたはデバイス名を指定した場合は、このオプションを選択しないでください。

ユーザに割り当てられる電話機の MAC アドレスがわからない場合には、このオプションを選択します。 電話機が接続されると、そのデバイスに対する MAC アドレスが登録されます。

ステップ 4 **[ユーザテンプレート名(User Template Name)]** フィールドで、このトランザクションに使用した BAT ユーザ テンプレートを選択します。

ステップ 5 **[ジョブ情報(Job Information)]** 領域に、ジョブの説明を入力します。

ステップ 6 挿入の方法を選択します。 次のいずれかを実行します。

a) 電話機とユーザをすぐに挿入する場合は、**[今すぐ実行(Run Immediately)]** をクリックします。

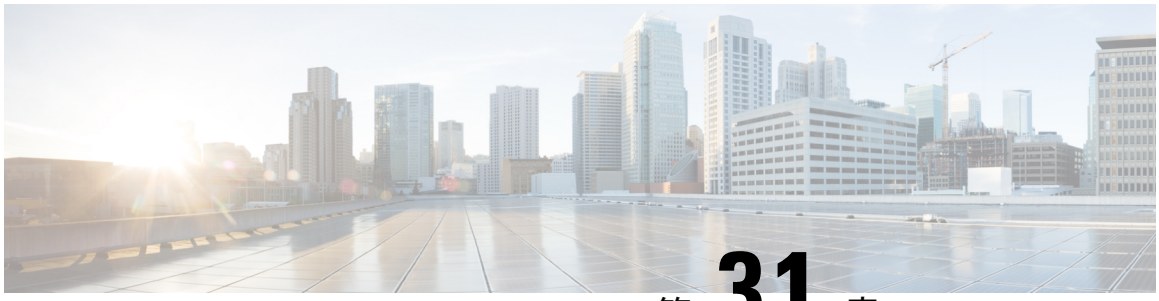
b) 電話機とユーザを後で挿入する場合は、**[後で実行(Run Later)]** をクリックします。

ステップ 7 電話機レコードとユーザ レコードを挿入するジョブを作成するには、**[送信(Submit)]** をクリックします。

このジョブのスケジュールやアクティブ化を行うには、[一括管理(Bulk Administration)]メインメニューの [ジョブスケジューラ(Job Scheduler)] オプションを使用します。

第 V 部

エンドポイントのプロビジョニング



第 31 章

エンドポイントの設定

エンドポイント プロビジョニングのデフォルト値

この項の情報を使用して、エンドポイントデバイスを設定し、エンドポイントにユーザを関連付けます。

Unified Communications Manager では、エンドポイントを追加する前にプロビジョニングできるように、デバイスの一連のデフォルト設定が用意されています。 これらのデバイスのデフォルト設定をあらかじめ設定しておくと、新しいユーザをプロビジョニングするときに、適用される設定に基づいてデバイスが自動的に設定されます。

エンドポイントのプロビジョニングに関するデフォルト設定には次の 2 つがあります。

- デバイスのデフォルト値の設定
- エンタープライズ電話設定項目の設定

エンドポイントプロビジョニングのデフォルト前提条件

エンドポイント登録用に設定されているポートを確認します。 Cisco Unified CM Administration から **システム** > **Cisco Unified CM** に移動し、サーバを選択して、設定されたポート設定を確認します。

（注） ほとんどの場合、ポートをデフォルト設定から変更する必要はありません。

エンドポイントプロビジョニングのデフォルト値のタスク フロー

システムのデバイスを設定するには、このタスク フローを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	デバイスのデフォルト値の設定 （394 ページ）	Unified Communications Manager ノードに自動登録するデバイスに適用される、デフォルト設定を変更できます。 デバイスのタイプごとに固有のデフォルト設定があります。
ステップ 2	デバイスプロファイルの設定 （398 ページ）	**（オプション）** ユーザ用の特定のデバイスに関連付けられている一連の属性で構成される、デバイス プロファイルを設定できます。
ステップ 3	デフォルトのデバイス プロファイルの設定 （395 ページ）	ユーザ デバイス プロファイルが設定されていない電話機にユーザがログインするたびに電話機が取得する、デフォルトのデバイス プロファイルを設定できます。
ステップ 4	デフォルトのデバイスプロファイルでのソフトキーテンプレートの設定 （396 ページ）	**（オプション）** ソフトキー テンプレートに追加するデフォルトのデバイス プロファイルを追加できます。
ステップ 5	エンタープライズ電話の設定 （398 ページ）	同じクラスタ内のすべての電話に適用されるエンタープライズ電話の基本設定を指定できます。

デバイスのデフォルト値の設定

デバイスのデフォルト設定の更新

デバイスのデフォルト設定を構成するには、この手順を使用します。この設定を使用するとデフォルトのファームウェア ロード、デフォルトのデバイス プール、ソフトキーテンプレート、および登録方法（自動登録またはアクティベーション コード）を割り当てることができます。

始める前に

デバイスのデフォルト設定を更新する前に、システムに適用する次のタスクを実行します。

- TFTP サーバにデバイスの新しいファームウェア ファイルを追加します。
- デバイスのデフォルトを使用して、ディレクトリに存在しないファームウェア ロードを割り当てると、それらのデバイスは割り当てられたファームウェアをロードできません。
- 新しいデバイス プールを設定します。 デバイスが電話の場合は、新しい電話テンプレートを設定します。

手順

ステップ 1 Cisco Unified CM Administration で、**[デバイス（Device）]**>**[デバイスの設定（Device Settings）]**>**[デバイスのデフォルト（Device Defaults）]** を選択します。

ステップ 2 [デバイスのデフォルト設定（Device Defaults Configuration）]ウィンドウで、更新するデバイス タイプに適用可能な設定を変更し、[保存（Save）]をクリックします。 フィールドの説明については、オンラインヘルプを参照してください。

- [ロード情報（Load Information）]
- [デバイス プール（Device Pool）]
- [電話テンプレート（Phone Template）]

ステップ 3 そのタイプのすべてのデバイスをリセットして、クラスタ内の全ノードにある該当するタイプのすべてのデバイスに新しいデフォルトをロードするには、デバイス名の左側にある [リセット（Reset）] アイコンをクリックします。

すべてのデバイスをリセットしない場合は、ノードに自動登録された新しいデバイスにだけ、更新されたデフォルト値が設定されます。

デフォルトのデバイス プロファイルの設定

ユーザがユーザ デバイス プロファイルのない電話機にログインした場合、電話機は必ずデフォルトのデバイス プロファイルを使用します。

デフォルトのデバイス プロファイルには、デバイス タイプ（電話機）、ユーザ ロケール、電話ボタン テンプレート、ソフトキー テンプレート、および MLPP 情報（Multilevel Precedence and Preemption（MLPP）Information）が含まれています。

手順

ステップ 1 Cisco Unified CM Administrationウィンドウで、**[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[デフォルトのデバイス プロファイル（Default Device Profile）]** を選択します。

ステップ 2 [デフォルトのデバイスプロファイルの設定（Default Device Profile Configuration）]ウィンドウで、[デバイスプロファイルタイプ（Device Profile Type）]ドロップダウン リストから、該当する Cisco Unified IP Phone を選択します。

ステップ 3 [次へ（Next）]をクリックします。

ステップ 4 [デバイスプロトコル（Device Protocol）]ドロップダウン リストから、適切なプロトコルを選択します。

ステップ 5 [次へ（Next）]をクリックします。

ステップ 6 [デフォルトのデバイスプロファイルの設定（Default Device Profile Configuration）]ウィンドウで、フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 7 **[保存]** をクリックします。

デフォルトのデバイスプロファイルでのソフトキーテンプレートの設定

Cisco Unified Communications Manager には、コール処理およびアプリケーション用の標準ソフトキー テンプレートが組み込まれています。 カスタム ソフトキー テンプレートを作成するときは、標準テンプレートをコピーして、必要に応じて変更します。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[ソフトキー テンプレート（Softkey Template）]**。

ステップ 2 新しいソフトキーテンプレートを作成するには、この手順を実行します。それ以外の場合は、次のステップに進みます。

a) [新規追加] をクリックします。
b) デフォルトのテンプレートを選択して、[コピー（Copy）]をクリックします。
c) [ソフトキーテンプレート名（Softkey Template Name）]フィールドに、テンプレートの新しい名前を入力します。
d) **[保存]** をクリックします。

ステップ 3 既存のテンプレートにソフトキーを追加するには、次の手順を実行します。

a) [検索（Find）]をクリックして、検索条件を入力します。
b) 必要な既存のテンプレートを選択します。

ステップ 4 [デフォルト ソフトキー テンプレート（Default Softkey Template）]チェックボックスをオンにし、このソフトキーテンプレートをデフォルトのソフトキーテンプレートとして指定します。

（注） あるソフトキー テンプレートをデフォルトのソフトキー テンプレートとして指定した場合、先にデフォルトの指定を解除してからでないと、そのテンプレートは削除することができません。

ステップ 5 右上隅にある **[関連リンク（Related Links）]** ドロップダウンリストから **[ソフトキーレイアウトの設定（Configure Softkey Layout）]** を選択し、**[移動（Go）]** をクリックします。

ステップ 6 [設定するコール状態の選択（Select a Call State to Configure）]ドロップダウン リストから、ソフトキーに表示するコール状態を選択します。

ステップ 7 [選択されていないソフトキー（Unselected Softkeys）]リストから追加するソフトキーを選択し、右矢印をクリックして [選択されたソフトキー（Selected Softkeys）]リストにそのソフトキーを移動します。新しいソフトキーの位置を変更するには、上矢印と下矢印を使用します。

ステップ 8 追加のコール状態でのソフトキーを表示するには、前述のステップを繰り返します。

ステップ 9 **[保存]** をクリックします。

ステップ 10 次のいずれかの作業を実行します。

- すでにデバイスに関連付けられているテンプレートを変更した場合は、[設定の適用（Apply Config）] をクリックしてデバイスを再起動します。
- 新しいソフトキーテンプレートを作成した場合は、そのテンプレートをデバイスに関連付けた後にデバイスを再起動します。詳細については、「共通デバイス設定へのソフトキーテンプレートの追加」と「電話機のセクションとソフトキーテンプレートの関連付け」を参照してください。

次のタスク

次のいずれかの設定ウィンドウにあるソフトキーテンプレートドロップダウンからテンプレートを選択すると、カスタマイズされたソフトキーテンプレートをデバイスに適用できます。

- 電話機設定
- ユニバーサル デバイス テンプレート（Universal Device Template）
- [BATテンプレート（BAT Template）]
- 共通デバイス設定
- [デバイスプロファイル（Device Profile）]
- [デフォルトのデバイスプロファイル（Default Device Profile）]
- [UDPプロファイル（UDP Profile）]

デバイスプロファイルの設定

デバイスプロファイルは特定のデバイスに関連付けられた属性のセットで構成されます。Cisco Extension Mobility機能を使用するために、作成したデバイスプロファイルをエンドユーザに関連付けることができます。

手順

ステップ 1 **Cisco Unified CM Administration**ウィンドで、**デバイス** > **デバイスの設定** > **デバイスプロファイル**を選択します。

ステップ 2 [デバイス プロファイルの設定（Device Profile Configuration）]ウィンドウで、[デバイス プロファイル タイプ（Device Profile Type）]ドロップダウン リストから、該当する Cisco Unified IP Phone を選択します。

ステップ 3 [次へ（Next）]をクリックします。

ステップ 4 [デバイスプロトコル（Device Protocol）]ドロップダウン リストから、適切なプロトコルを選択します。

ステップ 5 [次へ（Next）]をクリックします。

ステップ 6 [電話ボタンテンプレート（Phone Button Template）]ドロップダウン リストから、テンプレートを選択します。

ステップ 7 （任意）[ソフトキーテンプレート（Softkey Template）]ドロップダウン リストから、ソフトキー テンプレートを選択します。

ステップ 8 [デバイス プロファイルの設定（Device Profile Configuration）]ウィンドウで各フィールドを設定します。 フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 9 **[保存]** をクリックします。

（注） デバイス プロファイルを使用して Cisco Extension Mobility をセットアップする方法の詳細については、『*Cisco Unified Communications Manager* リリース *12.5(1)SU1* 機能設定ガイド』を参照してください。

エンタープライズ電話の設定

エンタープライズ電話設定項目の設定

ネットワーク内の電話で使用可能な、製品固有の設定フィールドのデフォルト値を指定するには、この手順を使用します。

このウィンドウで設定したパラメータは、[共通の電話プロファイルの設定(Common Phone Profile Configuration)] ウィンドウや各種デバイスの [電話の設定(Phone Configuration)] ウィンドウにも

表示されることがあります。 これらの同じパラメータをこれらの他のウィンドウにも設定した場合、優先される設定は、1）[電話の設定(Phone Configuration)] ウィンドウの設定、2）[共通の電話プロファイル(Common Phone Profile)] ウィンドウの設定、3）[エンタープライズ電話の設定(Enterprise Phone Configuration)] ウィンドウの設定の順に決定されます。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [エンタープライズ電話の設定（Enterprise Phone Configuration）]** を選択します。

ステップ 2 [製品固有の設定レイアウト（Product Specific Configuration Layout）]セクションの必須フィールドに入力します。

すべてのエンタープライズ電話パラメータについて説明を表示するには、 [エンタープライズ電話パラメータの設定（Enterprise Phone Parameters Configuration）] ウィンドウで [?] ボタンをクリックします。

ステップ 3 [エンタープライズ電話の設定（Enterprise Phone Configuration）] ウィンドウで、残りのフィールドを入力します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

電話の設定

Unified Communications Manager データベースに電話を手動で追加するには、この手順を実行します。 自動登録を使用している場合は、次の手順を実行する必要はありません。 自動登録を選択すると、Unified Communications Manager が自動的に電話を追加し、ディレクトリ番号を割り当てます。

手順

ステップ 1 Cisco Unified CM 管理から、**[デバイス] > [電話機]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [電話タイプ（Phone Type）]ドロップダウンリストから、該当する Cisco IP 電話モデルを選択します。

ステップ 4 [次へ（Next）]をクリックします。

ステップ 5 [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、次のいずれかを選択します。

- **SCCP**
- **SIP**

ステップ 6 [次へ（Next）]をクリックします。

ステップ 7 [電話の設定（Phone Configuration）]ウィンドウのフィールドを設定します。 フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

（注） セキュリティプロファイルで設定されている CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウに表示される Certificate Authority Proxy Function の設定に関係するものです。 製造元でインストールされる証明書（MIC）またはローカルで有効な証明書（LSC）に関連する証明書操作の CAPF 設定値を指定する必要があります。 電話の設定ウィンドウで更新する CAPF 設定がセキュリティプロファイルの CAPF 設定に与える影響の詳細については、『Cisco Unified Communications Manager セキュリティ ガイド』を参照してください。

ステップ 8 **[保存]** をクリックします。

ステップ 9 [関連付け（Association）]エリアで、[回線 [1] - 新規 DN を追加（Line [1] - Add a new DN）]をクリックします。

ステップ 10 [ディレクトリ番号（Directory Number）]フィールドに、電話に関連付ける電話番号を入力します。

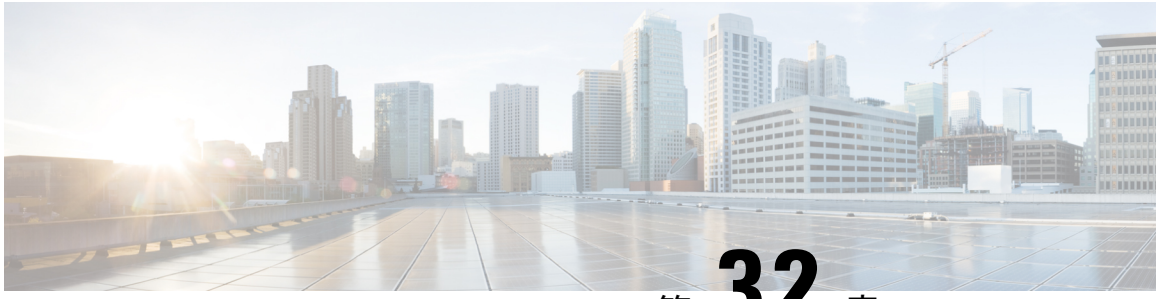
ステップ 11 **[保存]** をクリックします。

セルフケア ポータル

セルフケア ポータルは、新しい電話機のプロビジョニングと設定のための導入プロセスの一部として使用できます。

- エンド ユーザは、ポータルを使用して電話機の機能と設定をカスタマイズできます。
- デバイス アクティベーション コードの導入準備時に、ユーザはポータルを使用して電話機をアクティブにするオプションを選択できます。
- ユーザは、ポータルを使用して、自身のシングル ナンバー リーチのリモート接続先をセルフプロビジョニングすることもできます。

エンドユーザは、ポータルを使用する前に、アクセス権を持つ必要があります。 ポータルセットアップの詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』の「セルフケア ポータル」の章を参照してください。



第 32 章

CAPF の設定

認証局プロキシ機能（CAPF）の概要

Cisco Certificate Authority Proxy Function (CAPF) は、ローカルの重要な証明書 (LSCs) を発行し、Cisco エンドポイントを認証する Cisco 専有サービスです。 CAPF サービスは、ユニファイドコミュニケーションマネージャー上で実行され、次のタスクを実行します。

- サポートされる Cisco Unified IP Phone に対して LSC を発行する。
- 混合モードが有効になっている場合に、電話機を認証します。
- 電話機用の既存の LSCs をアップグレードします。
- 表示およびトラブルシューティングを行うために電話の証明書を取得する。

CAPF 実行モード

次のモードで動作するように CAPF を設定することができます。

- Cisco Authority プロキシ機能: ユニファイドコミュニケーションマネージャーの CAPF サービスは、CAPF サービス自体によって署名された LSCs を発行します。 これは、デフォルトのモードです。
- [オンライン CA (Online CA)]: 外部オンライン CA が「電話用 LSC」として署名している場合は、このオプションを使用します。 CAPF サービスは、自動的に外部 CA に接続されます。CSR が送信された場合、CA は署名して CA 署名した LSC を自動的に返します。
- オフライン CA: このオプションは、オフラインの外部 CA を使用して LSC for phone に署名する場合に使用します。 このオプションでは、LSC を手動でダウンロードして CA に提

出してから、CA 署名の証明書の準備ができてからそれらをアップロードする必要があります。

（注） シスコでは、サードパーティ CA を使用して LSC に署名する必要がある場合、**オフライン** ca の代わりにオンライン ca オプションを使用して、プロセスが自動化されていて、問題が発生する可能性が低くなることを推奨します。

CAPF サービス証明書

統合コミュニケーションマネージャがインストールされている場合、CAPF サービスが自動的にインストールされ、CAPF 固有のシステム証明書が生成されます。セキュリティが適用されると、Cisco CTL クライアントは、すべてのクラスタノードに証明書をコピーします。

電話の証明書タイプ

シスコは次の X.509v3 証明書タイプを電話で使用します。

- ローカルで有効な証明書（LSC）：このタイプの証明書は Cisco Certificate Authority Proxy Function（CAPF）に関連する必要な作業の実行後に、電話にインストールされます。 デバイス セキュリティ モードを認証または暗号化に設定した後で、LSC は Unified Communications Manager と電話の間の接続を保護します。

（注） オンライン CA の場合、LSC の有効性は CA に基づいています。また、CA が許可している限り使用できます。

- 製造元でインストールされる証明書（MIC）：Cisco Manufacturing は MIC をサポートされている電話モデルに自動的にインストールします。 製造元でインストールされる証明書は LSC インストールの Cisco Certificate Authority Proxy Function（CAPF）を認証します。 製造元でインストールされる証明書を上書きしたり、削除することはできません。

（注） 製造元でインストールされる証明書（MIC）を LSC のインストールでのみ使用することが推奨されます。 シスコでは Unified Communications Manager との TLS 接続の認証のために LSC をサポートしています。 MIC ルート証明書は侵害される可能性があるため、TLS 認証またはその他の目的に MIC を使用するように電話を設定するお客様は、ご自身の責任で行ってください。 MIC が侵害された場合シスコはその責任を負いません。

CAPF 経由の LSC 生成

CAPF を設定した後、電話機に設定されている認証文字列を追加します。 キーと証明書の交換は、電話機と CAPF の間で行われます。次のような場合があります。

- 電話機は、設定された認証方法を使用して CAPF に対して自身を認証します。
- 電話機は公開/秘密キー ペアを生成します。
- 電話機は、署名されたメッセージの中で、公開キーを CAPF に転送します。
- 秘密キーは電話に残り、外部に公開されることはありません。
- 証明書はCAPF によって署名され、署名付きメッセージによって電話に送り返されます。

（注） 電話のユーザが証明書操作の中断や、電話の動作ステータスの確認を実行できることに注意してください。

（注） キー生成の優先順位を低く設定すると、処理中に電話機を動作させることができます。 証明書生成中にも電話は正常に機能しますが、TLS トラフィックが増加することで、電話での通話の処理に最小限の中断が発生する可能性があります。 たとえば、インストールの最後に証明書がフラッシュに書き込まれると、音声信号が発生することがあります。

CAPF 前提条件

LSC 生成用の認証局のプロキシ機能を設定する前に、次の手順を実行します。

- サードパーティ CA を使用して LSCs に署名したい場合は、CA を外部に設定します。
- 電話機を認証する方法を計画します。
- LSCs を生成する前に、次のものを用意していることを確認してください。
  - Unified Communications Manager リリース 12.5 以降
  - 証明書に CAPF を使用するエンドポイント (Cisco IP 電話および Jabber を含む)。
  - Microsoft Windows Server 2012 および 2016
  - ドメイン名サービス（DNS）が設定されています
- 「CA ルートおよび HTTPS 証明書」をアップロードしてから、LSCs を生成する必要があります。 セキュア SIP connection では、HTTPS 証明書は CAPF-トラストを通過し、CA ルート証明書はCAPF 信頼でコールマネージャーの信頼をたどります。 インターネットイ

ンフォメーションサービス(IIS)は、HTTPS証明書をホストします。 CAルート証明書は、証明書署名要求(CSR)への署名に使用されます。

証明書をアップロードする必要がある場合のシナリオを次に示します。

表 *27*: 証明書のアップロードシナリオ

シナリオ	結果
CA ルートおよび HTTPS 証明書は同じです。	CA ルート証明書をアップロードする。
CA ルートと HTTPS の証明書は異なり、HTTPS 証明書は同じ CA ルート証明書によって発行されます。	CA ルート証明書をアップロードする。
中間CAとHTTPSの証明書は異なり、CAルート証明書によって発行されます。	CA ルート証明書をアップロードする。
CA ルートと HTTPS の証明書は異なり、同じ CA ルート証明書によって発行されます。	CA ルートおよび HTTPS 証明書をアップロードする。

（注） 複数の証明書を同時に生成するとコール処理中断の原因となるため、スケジュールされたメンテナンスの時間帯に CAPF を使用することを強く推奨します。

認証局プロキシ機能設定のタスクフロー

次のタスクを実行して、証明機関プロキシ機能 (CAPF) サービスがエンドポイント用 LSCs を発行するように設定します。

（注） 新しい CAPF 証明書を再生成またはアップロードした後に、CAPF サービスを再起動する必要はありません。

手順

	コマンドまたはアクション	目的
ステップ 1	サードパーティの認証局のルート証明書のアップロード	LSCにサードパーティのCA署名を適用する場合は、CAルート証明書チェーンをCAPF信頼ストアにアップロードしま

	コマンドまたはアクション	目的
		す。 それ以外の場合は、この作業をスキップできます。
ステップ 2	認証局（CA）ルート証明書のアップロード （406 ページ）	CA ルート証明書をUnified Communications Manager信頼ストアにアップロードします。
ステップ 3	オンライン認証局の設定 （407 ページ）	電話機 LSC 証明書を生成するには、次の手順を使用します。
ステップ 4	オフライン認証局の設定の設定	オフライン CA を使用して電話機 LSC 証明書を生成するには、次の手順を使用します。
ステップ 5	CAPF サービスをアクティブ化または再起動する	CAPF システム設定を構成した後に、重要な CAPF サービスをアクティブにします。
ステップ 6	次のいずれかの手順を使用して、Unified Communications Managerの CAPF 設定を構成します。 • CAPD 設定をユニバーサル デバイス テンプレートで設定します。（410 ページ） • バルク Admin による CAPF 設定の更新 （411 ページ） • 電話機の CAPF 設定の設定 （413 ページ）	次のオプションのいずれかを使用して、CAPF 設定を電話機の設定に追加します。 • まだ LDAP ディレクトリを同期していない場合、CAPF 設定をユニバーサルデバイステンプレートに追加し、初期 LDAP 同期を使用して設定を適用することができます。 • 一括管理ツールを使用すると、1 回の操作で多数の電話機に CAPF 設定を適用できます。 • CAPF 設定を電話機ごとに適用することができます。
ステップ 7	キープアライブ タイマーの設定 （414 ページ）	タイムアウトしないように、CAPF エンドポイント接続のキープアライブ値を設定します。 デフォルト値は 15 分です。

サードパーティの認証局のルート証明書のアップロード

CA ルート証明書を CAPF 信頼ストアとUnified Communications Manager信頼ストアにアップロードして、外部 CA を使用して LSC 証明書に署名します。

（注） サードパーティ CA を使用して LSCs に署名しない場合は、このタスクをスキップできます。

手順

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

ステップ 2 **[証明書/証明書チェーンのアップロード]** をクリックします。

ステップ 3 **[証明書目的]** ドロップダウンリストで、**[CallManager 信頼]** を選択します。

ステップ 4 証明書の説明を [説明（Description）] に入力します。 たとえば、**外部 LSC 署名 CA の証明書などです。**

ステップ 5 [参照（Browse）]をクリックしてファイルに移動してから、[開く（Open）]をクリックします。

ステップ 6 [アップロード（Upload）]をクリックします。

ステップ 7 このタスクを繰り返して、証明**書の目的で**使用さ**れる発信者管理者の信頼に証明書をアップロードします。**

認証局（CA）ルート証明書のアップロード

クラスタ全体の証明書をアップロードし、クラスタ内のすべてのサーバに配布します。

手順

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

ステップ 2 **[証明書/証明書チェーンのアップロード]** をクリックします。

ステップ 3 **[証明書目的（Certificate Purpose）]** ドロップダウンリストで、**[CallManager 信頼（CallManager-trust）]** を選択します。

ステップ 4 証明書の説明を [説明（Description）] に入力します。 たとえば、**外部 LSC 署名 CA の証明書などです。**

ステップ 5 [参照（Browse）]をクリックしてファイルに移動してから、[開く（Open）]をクリックします。

ステップ 6 [アップロード（Upload）]をクリックします。

重要 この注意事項は、リリース 14 SU2 以降に適用されます。

（注） ルート CA 証明書または中間 CA 証明書には、次のデフォルトの X509 拡張機能を含める必要があります。

X509v3 の基本的制約:

CA:TRUE, pathlen:0

X509v3 キーの使用法:

デジタル署名、証明書署名

これらの拡張機能が証明書に存在しない場合、TLS 接続エラーが発生します。

重要 この注意事項は、リリース 14 SU3 以降の IPsec 証明書にのみ適用されます。

（注） CA 署名付き IPsec 証明書の場合、次の拡張機能を含めることはできません。

X509v3 の基本的制約:

CA:TRUE

オンライン認証局の設定

オンライン CAPF を使用して電話機 LSC を生成するには、Unified Communications Managerにあるこの手順を使用します。

手順

ステップ 1 Cisco Unified CM の管理から、**[システム（System）]** > **[サービス パラメータ（Service Parameters）]** の順に選択します。

ステップ 2 **[サーバ]** ドロップダウン リストから、[Cisco Certificate Authority Proxy Function（アクティブ）] サービスを選択します。

ステップ 3 [サービス（Service）]ドロップダウン リストから、[Cisco Certificate Authority Proxy Function（アクティブ）（Cisco Certificate Authority Proxy Function (Active)）]を選択します。 サービス名の横に「Active」と表示されることを確認します。

ステップ 4 [エンドポイントへの証明書発行者（Certificate Issuer to Endpoint）]ドロップダウン リストから、[オンラインCA（Online CA）]を選択します。 CA 署名付き証明書では、オンライン CA を使用することを推奨しています。

ステップ 5 **[証明書の有効期間（日数）]** フィールドに、CAPF が発行した証明書が有効である日数を表す数値を、1 ～ 1825 の間で指定します。

ステップ 6 [オンラインCAパラメータ（Online CA Parameters）]画面で次のパラメータを設定し、オンライン CA セクションに対する接続を作成します。

- オンライン CA ホスト名：サブジェクト名または共通名（CN）は、HTTPS 証明書の完全修飾ドメイン名（FQDN）と同じである必要があります。

（注） 設定されているホスト名は、Microsoft CA で実行されているインターネット インフォメーションサービス（IIS）でホストされる HTTPS 証明書の共通名（CN）と同じです。

- オンライン CA ポート: オンライン CA のポート番号（443 など）を入力します。
- オンライン CA テンプレート：テンプレートの名前を入力します。 Microsoft CA がテンプレートを作成します。

  （注） このフィールドが有効になるのは、オンライン CA タイプが Microsoft CA の場合のみです。

- オンライン CA タイプ: エンドポイント証明書の自動登録には、Microsoft CA または EST でサポートされる CA を選択します。
  - Microsoft CA - CA が Microsoft CA である場合は、このオプションを使用してデジタル証明書をデバイスに割り当てます。

    （注） FIPSS 対応モードは、Microsoft CA ではサポートされていません。

    - **重要** リリース 14SU2 以降でサポートされます。

    EST サポート CA: CA が自動登録用の組み込み EST サーバモードをサポートしている場合は、このオプションを使用します。

- オンライン CA ユーザ名：CA サーバのユーザ名を入力します。
- オンライン CA パスワード：CA サーバのユーザ名のパスワードを入力します。
- 証明書登録プロファイル ラベル: EST がサポートする CA のデジタル ID を有効な文字で入力します。

  （注） このフィールドが有効になるのは、オンライン CA タイプが EST サポート CA の場合のみです。

ステップ 7 残りの CAPF サービス パラメータを完了します。 サービスパラメータのヘルプ システムを表示するには、パラメータ名をクリックします。

ステップ 8 **[保存]** をクリックします。

ステップ 9 変更内容を有効にするには、**Cisco Certificate Authority Proxy Function** サービスを再起動します。 Cisco Certificate Enrollment service を自動的に再起動します。

現在のオンライン CA の制限

- CA サーバが英語以外の言語を使用している場合、オンライン CA 機能は動作しません。CA サーバは英語でのみ応答します。
- オンライン CA 機能は、CA での mTLS 認証をサポートしていません。
- LSC 操作にオンライン CA を使用している場合、LSC 証明書に「デジタル署名」と「キー暗号化」のキー使用法が指定されていないと、デバイスのセキュア登録は失敗します。

- LSC 操作にオンライン CA を使用している場合、LSC 証明書に「デジタル署名」と「キー暗号化」が指定されていないと、デバイスのセキュア登録は失敗します。

オフライン認証局の設定の設定

オフライン CA を使用して電話機 LSC 証明書を生成することを決定した場合は、次の高度なプロセスに従うことができます。

（注） オフライン CA オプションを使用すると、オンライン CA よりも時間がかかり、手動による手順が非常に多くなります。証明書の生成および送信プロセス中に問題（たとえば、ネットワークの停止や電話機のリセットなど） が発生した場合は、プロセスを再起動する必要があります。

手順

ステップ 1 サードパーティ認証局からルート証明書チェーンをダウンロードします。

ステップ 2 ルート証明書チェーンを Unified Communications Manager 内の必要な信頼（CallManager 信頼 CAPF 信頼）にアップロードします。

ステップ 3 [エンドポイントへの証明書の発行（Certificate Issue to Endpoint）] サービスパラメータを [オフライン CA（Offline CA）] に設定して、オフライン CA を使用するように Unified Communications Manager を設定します。

ステップ 4 お使いの電話機の LSC 用に **CSR** を生成します。

ステップ 5 認証局に**CSR** を送信します。

ステップ 6 **CSR** から署名付き証明書を取得します。

オフライン CA を使用して電話機 LSC を生成する方法の詳細な例については、「CUCM サードパーティ CA 署名済み LSC の作成およびインポートの設定」を参照してください。

CAPF サービスをアクティブ化または再起動する

CAPF システムを設定した後に、重要な CAPF サービスをアクティブにします。 CAPF サービスがすでにアクティブ化されている場合は、再起動します。

手順

ステップ 1 Cisco Unified Serviceability から**[ツール]** > **[サービス アクティベーション]** を選択します。

ステップ 2 [サーバ（Server）]ドロップダウン リストからパブリッシャ ノードを選択し、[移動（Go）]をクリックします。

ステップ 3 **[セキュリティ サービス]** ペインから、次の該当するサービスを確認します。

- **Cisco Certificate Enrollment Service**: オンラインCAを使用している場合はこのサービスのチェックをオンにし、そうでない場合はチェックを外したままにします。
- **Cisco Certificate Authority プロキシ機能**: このサービスをオフ (非アクティブ) にした場合は、チェックを入れます。 サービスがすでにアクティブ化されている場合は、再起動します。

ステップ 4 いずれかの設定を変更した場合、**[保存]** をクリックします。

ステップ 5 **Cisco Certificate Authority Proxy Function** サービスがすでにチェックされている場合は（アクティブ）、再起動します。

a) **[関連リンク]**ドロップダウン リストから**[コントロールセンター-ネットワークサービス]**を選択し、**[移動]** をクリックします。

b) **[セキュリティの設定]**ペインから、**シスコ認証局プロキシ機能**サービスを確認し、**[再起動]** をクリックします。

ステップ 6 次の手順のいずれかを実行して、個々の電話機に対して CAPF 設定を構成します。

a) CAPD 設定をユニバーサル デバイス テンプレートで設定します。 （410 ページ）

b) バルク Admin による CAPF 設定の更新 （411 ページ）

c) 電話機の CAPF 設定の設定 （413 ページ）

CAPD 設定をユニバーサル デバイス テンプレートで設定します。

CAPF設定をユニバーサルデバイステンプレートに設定するには、次の手順を実行します。テンプレートは、機能グループテンプレートの設定を使用して、LDAPディレクトリ同期に適用します。テンプレートのCAPF設定が、このテンプレートを使用する同期済みのすべてのデバイスに適用されます。

（注） Universalデバイステンプレートは、まだ同期されていないLDAPディレクトリにしか追加することができません。 初期 LDAP 同期が発生した場合は、一括管理を使用して電話機を更新します。 詳細については、バルク Adminによる CAPF 設定の更新（411 ページ）を参照してください。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザの管理（User Management）]** > **[ユーザ/電話の追加（User/Phone Add）]** > **[ユニバーサルデバイステンプレート（Universal Device Template）]** を選択します。

ステップ 2 次のいずれかを実行します。

- **[検索]** をクリックし、既存のテンプレートを**選択**します。
- [新規追加] をクリックします。

ステップ 3 **認証局プロキシ機能（CAPF）の設定**領域の拡張

ステップ 4 [証明書の操作（Certificate Operation）]ドロップダウンリストで、[インストール/アップグレード（Install/Upgrade）]を選択します。

ステップ 5 **[認証モード]** ドロップダウンメニューで、デバイスを認証するオプションを選択します。

ステップ 6 認証文字列の使用を選択した場合は、**テキストボックス**に認証文字列を入力するか、**[**文字列の生成 ([文字列の生成])] をクリックして、システムによって文字列が生成されるようにします。

（注） この文字列がデバイス上で設定されていない場合、認証は失敗します。

ステップ 7 残りのフィールドで、キー情報を設定します。 フィールドの詳細については、オンライン ヘルプを参照してください。

ステップ 8 **[保存]** をクリックします。

（注） このテンプレートを使用するデバイスは、この手順で割り当てたのと同じ認証方法で構成されていることを確認してください。 それ以外の場合、デバイス認証は失敗します。 電話機の認証を設定する方法の詳細については、電話機のマニュアルを参照してください。

ステップ 9 このプロファイルを使用するデバイスにテンプレート設定を適用します。

a) ユニバーサルデバイステンプレートを Feature Group テンプレートの設定に追加します。
b) 機能グループテンプレートを、同期されていないLDAPディレクトリ設定に追加します。
c) LDAP 同期を完了します。 CAPF 設定は、同期されているすべてのデバイスに適用されます。

機能グループテンプレートとLDAP ディレクトリ同期の設定の詳細については、Cisco Unified Communications Manager システム設定ガイドの「Configure End Users」セクションを参照してください。

バルク Admin による CAPF 設定の更新

一括管理の**電話機の更新**クエリを使用して、多数の既存の電話機の CAPF 設定と lsc 証明書を 1 回の操作で構成します。

（注） まだ電話機をプロビジョニングしていない場合は、一括管理の**[電話機の挿入]**メニューを使用して、CSV ファイルからのCAPF設定で新しい電話機をプロビジョニングできます。 CSV ファイルから電話機を挿入する方法の詳細については、Cisco Unified Communications Manager 一括管理ガイドの「電話機の挿入」セクションを参照してください。

電話機は、この手順で追加する認証方法と文字列と同じように設定されていることを確認します。 それ以外の場合、お使いの電話機は CAPF に対して認証しません。 電話機で認証を設定する方法の詳細については、「電話機のマニュアル」を参照してください。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**バルク管理 > 電話機 > 電話機の更新 > クエリ**

ステップ 2 フィルタオプションを使用して、更新する電話機に検索を制限し、**[検索]**をクリックします。

たとえば、**[電話機の検索場所]** ドロップダウンを使用して、LSC が特定の日付の前期限切れになるすべての電話機またはデバイスプール内の電話機を選択することができます。

ステップ 3 [次へ（Next）]をクリックします。

ステップ 4 **ログアウト/リセット/再起動**セクションから**[設定の適用]**を選択します。 ジョブを実行すると、CAPF アップデートは更新されたすべての電話に適用されます。

ステップ 5 [**証明機関プロキシ関数（capf）]**の情報で、**[**証明書の操作（Certificate Operation）] チェックボックスをオンにします。

ステップ 6 **[証明書の操作]** ドロップダウン リストから、**[インストール /アップグレード]** を選択して、新しい LSC 証明書を電話機にインストールします。

ステップ 7 **[認証モード]** ドロップダウンから、LSC インストール時に電話機を認証する方法を選択します。

（注） 電話機で同じ認証方法を設定します。

ステップ 8 **認証モード**として**認証文字列**で選択した場合は、次の手順のいずれかを実行します。

- 各デバイスに対して一意の認証文字列を使用する場合は、**各デバイスに対して一意の認証文字列を生成する**ことを確認してください。
- すべてのデバイスに同じ認証文字列を使用する場合は、**[認証文字列]**テキストボックスに文字列を入力するか、**[文字列の生成]** をクリックします。

ステップ 9 **[電話の更新（Update Phones）]** ウィンドウで **[CAPF の情報（Certification Authority Proxy Function（CAPF）Information）]** セクションの残りのフィールドを入力します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 10 **[ジョブ情報（Job Information）]** セクションで、**[今すぐ実行（Run Immediately）]**を選択します。

（注） スケジュールされた時刻にジョブを実行する場合は、**[後で実行する]** を選択します。 ジョブのスケジュール設定の詳細については、Cisco Unified Communications Manager 一括管理ガイドの「スケジュールされたジョブの管理」セクションを参照してください。

ステップ 11 [送信（Submit）]をクリックします。

（注） この手順で**[設定の適用]**オプションを選択しなかった場合は、更新されたすべての電話機の **[電話機の設定]** ウィンドウで設定を適用します。

電話機の CAPF 設定の設定

個々の電話機の LSC 証明書の CAPF 設定を設定するには、次の手順を実行します。

（注） CAPF 設定を多数の電話機に適用するには、バルク管理または LDAP ディレクトリ同期を使用します。

電話機は、この手順で追加する認証方法と文字列と同じように設定します。 それ以外の場合、電話機は CAPF に対して自身を認証しません。 電話機で認証を設定する方法の詳細については、「電話機のマニュアル」を参照してください。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[デバイス]** > **[電話]**

ステップ 2 既存の電話機を選択するには、[検索（Find）]をクリックします。 **[電話設定]** ページが表示されます。

ステップ 3 **[認証局プロキシ機能 (CAPF) の情報]** ペインに移動します。

ステップ 4 **[証明書の操作]** ドロップダウン リストから、**[インストール /アップグレード]** を選択して、新しい LSC 証明書を電話機にインストールします。

ステップ 5 **[認証モード]** ドロップダウンから、LSC インストール時に電話機を認証する方法を選択します。

（注） 電話機は、同じ認証方法を使用するように設定されている必要があります。

ステップ 6 **[認証文字列]** で選択した場合は、テキスト文字列を入力するか、**[文字列の生成]** をクリックして、システムが文字列を生成するようにします。

ステップ 7 **[電話機の設定（Phone Configuration）]** ページで **[認証局プロキシ機能 (CAPF) の情報]** ペインの残りのフィールドに詳細を入力します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 8 **[保存]** をクリックします。

キープアライブ タイマーの設定

ファイアウォールによって接続がタイムアウトしないように、次の手順を実行して、CAPF-エンドポイント接続のクラスターワイドキープアライブタイマーを設定します。デフォルト値は15分です。 各間隔の後、CAPF サービスは電話機にキープアライブ信号を送信して、接続を開いた状態にします。

手順

ステップ 1 発行者ノードにログインするには、コマンドラインインターフェイスを使用します。
ステップ 2 `utils capt set keep_alive` CLI コマンドを実行します。
ステップ 3 5 ~ 60 (分) の間の数値を**入力**し、確定キーをクリックします。

CAPF の管理タスク

CAPF を設定し、LSC 証明書を発行した後、次のタスクを使用して LSC 証明書を継続的に管理します。

証明書ステータスのモニタリング

証明書のステータスを自動的に監視するようにシステムを設定することができます。証明書が期限切れに近づいたときにシステムから電子メールが送信され、期限切れ後に証明書が失効します。

証明書の監視の確認の設定方法の詳細については、「証明書の管理」の章の「証明書の監視と失効のタスクフロー」を参照してください。

古い LSC レポートの実行

次の手順を使用して、古い LSC レポートを Cisco Unified レポートから実行します。 古い LSCs は、エンドポイント CSR への応答として生成された証明書ですが、古くなった LSCS がインストールされる前に新しい CSR が生成されたため、インストールされませんでした。

（注） また、パブリッシャーノードで `utils capf stale-lsc list` CLI コマンドを実行することによって、古い LSC 証明書のリストを取得することもできます。

手順

ステップ 1 Cisco Unified Reporting から **[System Reports]** をクリックします。
ステップ 2 左側のナビゲーションバーで、[**古い LSCs**] を選択します。
ステップ 3 **[新規レポートの生成]** をクリックします。

保留中の CSR リストの表示

保留中の CAPF CSR ファイルのリストを表示するには、この手順を使用します。すべての CSR ファイルはタイムスタンプされます。

手順

ステップ 1 発行者ノードにログインするには、コマンドラインインターフェイスを使用します。
ステップ 2 `utils core active list` CLI コマンドを実行します。
保留中の CSR ファイルのタイムスタンプリストが表示されます。

古い LSC 証明書の削除

古い LSC 証明書をシステムから削除するには、次の手順を使用します。

手順

ステップ 1 発行者ノードにログインするには、コマンドラインインターフェイスを使用します。
ステップ 2 `[utils capf state-lsc delete all` CLI コマンド] を実行します。
古い LSC 証明書はすべてシステムから削除されます。

CAPF システムの連携動作と制限事項

機能	データのやり取り
認証文字列（Authentication String）	電話の CAPF 認証方式については、アップグレードまたはインストールの後に同じ認証文字列を電話に入力する必要があります。入力されなかった場合、操作が失敗します。 [TFTP Encrypted Config] エンタープライズ パラメータが有効な状態で認証文字列の入力に失敗した場合、電話の設定は失敗し、該当する認証文字列が電話に入力されるまで回復しません。
クラスタ サーバ クレデンシャル	CAPF が Unified Communications Manager クラスタのすべてのサーバを認証できるよう、クラスタ内のすべてのサーバで管理者のユーザ名とパスワードを同じものにする必要があります。
セキュアな電話機の移行	セキュアな電話が別のクラスタに移動されると、Unified Communications Manager はその電話が送信する LSC 証明書を信頼しなくなります。これは、その LSC 証明書が、CTL ファイル内に証明書が存在しない別の CAPF によって発行されたものであるためです。 セキュア電話を登録可能にするには、既存の CTL ファイルを削除します。 その後、[Install/Upgrade] オプションを使用して新しい CAPF により新規 LSC 証明書をインストールし、新しい CTL ファイルのために電話をリセットします（または MIC を使用します）。 [Phone Configuration] ウィンドウの [CAPF] セクションにある [Delete] オプションを使用して、電話を移動する前に既存の LSC を削除します。

機能	データのやり取り
Cisco Unified IP Phone 6900 シリーズ、7900 シリーズ、および 8900 シリーズ、および 9900	将来的な互換性の問題を回避するため、Unified Communications Manager との TLS 接続に LSC を使用するために Cisco Unified IP Phone 6900 シリーズ、7900 シリーズ、8900 シリーズ、9900 シリーズをアップグレードし、MIC ルート証明書を CallManager 信頼ストアから削除することが推奨されます。Cisco Unified Communications Manager との TLS 接続に MIC を使用する一部の電話モデルは登録できない場合があることに注意してください。 管理者は CallManager 信頼ストアから次の MIC ルート証明書を削除する必要があります。 • CAP-RTP-001 • CAP-RTP-002 • Cisco_Manufacturing_CA • Cisco_Root_CA_2048
停電	以下の情報は、通信障害や電源障害の発生時に適用されます。 • 電話での証明書インストールの実行中に通信障害が発生した場合、電話は証明書の取得を 30 秒間隔でさらに 3 回試行します。 これらの値は設定できません。 • 電話による CAPF とのセッション試行中に電源障害が発生した場合、電話はフラッシュに保存されている認証モードを使用します。つまり、電話の再起動後に TFTP サーバから新しい設定ファイルをロードできなかった場合です。 証明書操作が完了すると、システムはフラッシュの値をクリアします。
証明書の暗号化	Cisco Unified Communications Manager リリース 11.5(1)SU1 以降、CAPF サービスによって発行されるすべての LSC 証明書は、SHA-256 アルゴリズムで署名されています。 したがって、IP 電話 7900/8900/9900 シリーズのモデルは、SHA-256 署名済み LSC 証明書および外部 SHA2 アイデンティティ証明書（Tomcat、CallManager、CAPF、TVS など）をサポートします。署名の検証が必要な、その他の暗号化の操作では、SHA-1 のみがサポートされます。 （注） ソフトウェア メンテナンスが終了またはサポートが終了した電話モデルを使用する場合は、Unified Communications Manager の 11.5(1)SU1 より前のリリースの使用を強くお勧めします。

7942 および 7962 電話機を含む CAPF の例

ユーザまたは Unified Communications Manager によって電話がリセットされたときの CAPF と Cisco Unified IP Phone 7962 および 7942 とのインタラクションについては、以下の情報を考慮してください。

（注） 次の例では、LSC が電話に存在せず、CAPF 認証モードとして**既存の証明書**が選択されている場合、CAPF 証明書操作が失敗します。

例：非セキュア デバイス セキュリティ モード

この例では、[Device Security Mode] を **[Nonsecure]** に設定し、[CAPF Authentication Mode] を **[By Null String]** または **[By Existing Certificate (Precedence...)]** に設定した後、電話がリセットされます。 リセットした電話は直ちにプライマリ Unified Communications Manager に登録され、設定ファイルを受信します。 その後、電話によって LSC をダウンロードするための CAPF セッションが自動的に開始されます。 電話で LSC をインストールした後、[Device Security Mode] を [Authenticated] または [Encrypted] に設定します。

例：認証済み/暗号化済みデバイス セキュリティ モード

この例では、**[Device Security Mode]** を **[Authenticated]** または **[Encrypted]** に設定し、[CAPF Authentication Mode] を **[By Null String]** または **[By Existing Certificate (Precedence...)]** に設定した後、電話がリセットされます。CAPFセッションが終了しLSCがインストールされるまで、電話はプライマリ Unified Communications Manager に登録されません。 セッションが終了すると、電話が登録され、直ちに認証済みまたは暗号化済みモードで動作します。

この例では、電話が自動的に CAPF サーバに接続されないため、**[By Authentication String]** を設定できません。電話に有効な LSC がない場合、登録は失敗します。

IPv6 アドレッシングとの CAPF のインタラクション

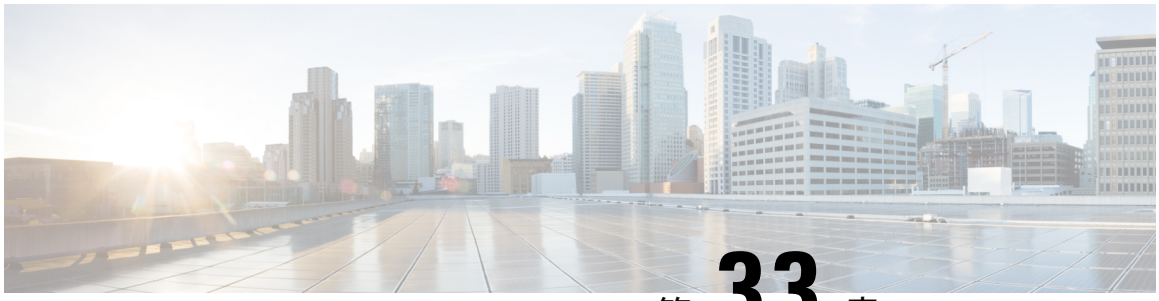
CAPF は、IPv4、IPv6、またはその両方のタイプのアドレスを使用する電話に対し、証明書の発行とアップグレードを実行できます。 IPv6 アドレスを使用する SCCP を実行する電話の証明書の発行またはアップグレードを実行するには、[Unified Communications Manager Administration] で [Enable IPv6] サービスパラメータを **[True]** に設定する必要があります。

証明書取得のために電話が CAPF に接続されると、CAPF では [Enable IPv6] エンタープライズパラメータの設定を使用して、その電話の証明書の発行またはアップグレードを実行するかどうかが決定されます。 このエンタープライズパラメータが **False** に設定された場合、CAPF は IPv6 アドレスを使用する電話からの接続を無視または拒否し、その電話は証明書を受け取りません。

IPv4、IPv6、またはその両方のタイプのアドレスを使用する電話から CAPF への接続方法について、次の表で説明します。

表 *28 : IPv6* または *IPv4* 電話から *CAPF* への接続方法

電話の IP モード	電話の IP アドレス	CAPF IP アドレス	電話から CAPF への接続方法
2 スタック	IPv4 と IPv6 が利用可能	IPv4、IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。IPv6 アドレスでは接続できない場合、電話は IPv4 アドレスを使用して接続を試みます。
2 スタック	IPv4	IPv4、IPv6	電話は IPv4 アドレスを使用して CAPF に接続します。
2 スタック	IPv6	IPv4、IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。 試行に失敗すると、電話は IPv4 アドレスを使用して CAPF に接続します。
2 スタック	IPv4	IPv4	電話は IPv4 アドレスを使用して CAPF に接続します。
2 スタック	IPv4 と IPv6 が利用可能	IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。
2 スタック	IPv4 と IPv6 が利用可能	IPv4	電話は IPv4 アドレスを使用して CAPF に接続します。
2 スタック	IPv4	IPv6	電話は CAPF に接続できません。
2 スタック	IPv6	IPv4	電話は CAPF に接続できません。
2 スタック	IPv6	IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。
IPv4 スタック	IPv4	IPv4、IPv6	電話は IPv4 アドレスを使用して CAPF に接続します。
IPv6 スタック	IPv6	IPv4、IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。
IPv4 スタック	IPv4	IPv4	電話は IPv4 アドレスを使用して CAPF に接続します。
IPv4 スタック	IPv4	IPv6	電話は CAPF に接続できません。
IPv6 スタック	IPv6	IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。
IPv6 スタック	IPv6	IPv4	電話は CAPF に接続できません。



第 33 章

TFTP サーバの設定

プロキシ TFTP 展開の概要

プロキシ簡易ファイル転送プロトコル (TFTP) サーバを使用して、ネットワークのエンドポイントに必要な設定ファイル(ダイヤルプラン、着信音ファイル、デバイス設定ファイルなど)を指定します。 展開内の任意のクラスタに TFTP サーバをインストールして、複数クラスタのエンドポイントからの要求を処理することができます。 DHCP スコープは、設定ファイルを取得するために使用するプロキシ TFTP サーバの IP アドレスを指定します。

冗長およびピア プロキシ TFTP サーバ

単一クラスタの導入では、クラスタは少なくとも 1 つのプロキシ TFTP サーバを備えている必要があります。 冗長性を確保するために、クラスタに別のプロキシ TFTP サーバを追加することができます。 2 台目のプロキシ TFTP サーバは、IPv4 のオプション 150 に追加されます。 IPv6 の場合、第 2 TFTP サーバを、DHCP スコープの TFTP サーバ アドレスサブオプションタイプ 1 に追加します。

複数のクラスタ展開では、最大 3 台のリモートプロキシ TFTP サーバをプライマリプロキシ TFTP サーバのピアクラスタとして指定できます。 これは、複数の DHCP スコープに対して 1 台のプロキシ TFTP サーバだけを設定する場合、または 1 つの DHCP スコープのみを設定する場合に便利です。 プライマリプロキシ TFTP サーバは、ネットワーク内のすべての電話機とデバイスに設定ファイルを提供します。

各リモートプロキシ TFTP サーバとプライマリプロキシ TFTP サーバの間にピア関係を作成する必要があります。

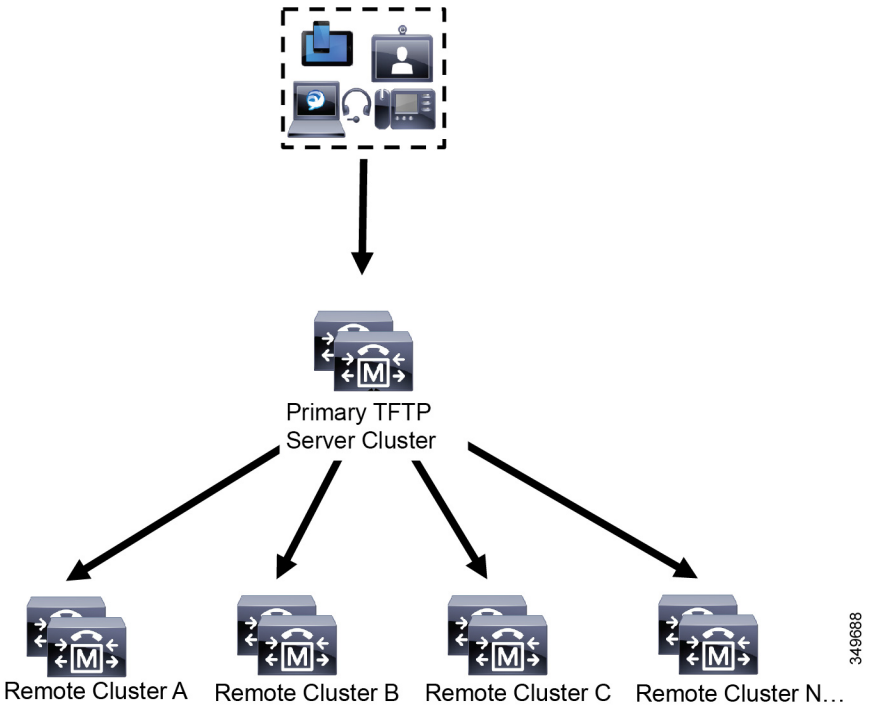
ヒント　ネットワーク内のリモートプロキシ TFTP サーバ間にピア関係を設定する場合は、関係を階層構造にしておきます。 ループの発生を回避するために、リモートクラスタ上のピアプロキシ TFTP サーバが相互にポイントしないようにします。 たとえば、プライマリノード A にノード B と C のピアリレーションシップがあるとします。ノード B と C の間にピア関係を作成しないでください。作成すると、ループが作成されます。

プロキシ TFTP

マルチクラスタ システムでは、プロキシ TFTP サービスは、1 つのプライマリ TFTP サーバを介して複数のクラスタから TFTP ファイルを提供できます。 単一のサブネットまたは VLAN に複数のクラスタからの電話機が含まれている場合や、複数のクラスタが同じ DHCP TFTP オプション（150）を共有している場合、プロキシ TFTP はそれらの状況に対する単一の TFTP 参照として機能できます。

プロキシ TFTP サービスは、図に示すように、単一レベルの階層として機能します。 より複雑な複数レベル階層はサポートされません。

図 *7:* プロキシ *TFTP* のシングル レベル階層



上の図では、デバイスのグループが構成ファイルのプライマリ TFTP サーバと通信します。 デバイスから TFTP の要求を受信すると、プライマリ TFTP は、設定ファイルだけでなく、リモートクラスタ A、B、C、N(構成されている他のリモートクラスタ)などリモートで構成された他のクラスタについて、それぞれ自身のローカルキャッシュを検索します。

プライマリ TFTP サーバ上では、任意の数のリモートクラスタを設定できます。ただし、各リモートクラスタには最大 3 個の TFTP IP アドレスしか含めることができません。 冗長性を確保するための推奨設計は、クラスタごとに 2 台の TFTP サーバを使用することです。したがって、プライマリ TFTP サーバ上のリモートクラスタあたり 2 つの IP アドレスを使用して冗長性を確保できます。

使用例とベスト プラクティス

実装でのプロキシ TFTP の使用方法とベストプラクティスを詳細に示す次のシナリオを検討します。

1. クラスタは、他の目的がない単なるプロキシ TFTP クラスタとして機能できます。 この場合、クラスタには他のクラスタとの関係がなく、コールを処理しません。 このシナリオでは、リモート クラスタ TFTP が手動で定義され、8.0 よりも前へのロールバックが推奨されます。

（注） 自動登録は、このシナリオでは動作しません。

2. クラスタは、リモートクラスタのプロキシ TFTP サーバとしても機能するリモートクラスタです。 リモート クラスタは手動で定義されるので、自動登録は有効にしないでください。

IPv4 および IPv6 デバイスに対する TFTP サポート

IPv4 の電話機とゲートウェイで DHCP カスタムオプション 150 を使用して、TFTP サーバの IP アドレスを検出することを推奨します。 オプション 150 を使用すると、ゲートウェイと電話機は TFTP サーバの IP アドレスを検出します。 詳細については、デバイスに同梱されているマニュアルを参照してください。

IPv6 ネットワークでは、Cisco ベンダー固有の DHCPv6 情報を使用して、TFTP サーバ IPv6 アドレスをエンドポイントに渡すことを推奨します。 この方式では、TFTP サーバの IP アドレスをオプション値として設定しています。

IPv4 を使用するエンドポイントと IPv6 を使用するエンドポイントがある場合は、IPv4 には DHCP カスタム オプション 150 を、IPv6 には Cisco ベンダー固有情報オプションである TFTP サーバアドレスのサブオプションタイプ 1 を使用することをお勧めします。 TFTP サーバが IPv4 を使用して要求を処理しているときに、エンドポイントが IPv6 アドレスを取得して要求を TFTP サーバに送信した場合、TFTP サーバは IPv6 スタックで要求を受信していないため、その要求を受信しません。 この場合、エンドポイントを Cisco Unified Communications Manager に登録できません。

IPv4 および IPv6 デバイスが TFTP サーバの IP アドレスを検出するために使用できる別の方法があります。 たとえば、IPv4 デバイスに DHCP オプション 066 または CiscoCM1 を使用できます。 IPv6 デバイスの場合、他の方法として、TFTP サービスのサブオプションタイプ 2 を使用する方法と、エンドポイントで TFTP サーバの IP アドレスを設定する方法があります。 こ

れらの代替手段は推奨されません。代替手段を使用する前に、シスコのサービスプロバイダーに問い合わせてください。

TFTP 展開のエンドポイントおよび設定ファイル

SCCP 電話機、SIP 電話およびゲートウェイは、初期化時に設定ファイルを要求します。 デバイス設定を変更すると、更新された設定ファイルがエンドポイントに送信されます。

設定ファイルには、Unified Communications Managerノードの優先順位リスト、これらのノードに接続するために使用される TCP ポート、さらに他の実行可能ファイルが含まれます。 一部のエンドポイント用の設定ファイルには、電話機のボタン（メッセージ、ディレクトリ、サービス、および情報）用のロケール情報および URL が保存されています。 ゲートウェイ用の設定ファイルには、デバイスが必要とする設定情報がすべて保存されています。

プロキシ TFTP のセキュリティに関する考慮事項

シスコプロキシ TFTP サーバは、署名付きの要求と署名されていない要求の両方を処理でき、セキュアでないモードと混在モードのいずれでも動作できます。 プロキシ TFTP サーバは、電話機がファイルをリクエストし、見つからない場合は、リモートクラスタにリクエストを送信するときに、ローカル ファイル システムまたはデータベースを検索します。 電話が `ringlist.xml.sgn`、ロケールファイルなどの名前の共通ファイルをサーバにリクエストすると、サーバは電話のホームクラスタからファイル自体ではなくファイルのローカルコピーを送信します。

プロキシ TFTP からファイルを受信すると、ファイルにプロキシサーバの署名があり、電話の初期信頼リスト（ITL）と一致しないことから、署名の検証に失敗するため、電話はファイルを拒否します。 この問題を解決するには、電話機のセキュリティ デフォルト (SBD) セキュリティを無効にするか、プロキシ TFTP の CallManager 証明書を新しい(リモート/ホーム) クラスタの phone-sast-trust にインポートします。 その後、電話機は Trust Verification Service (TVS) に到達し、プロキシ TFTP 認証を信頼できます。 導入で EMCC が有効になっている場合は、一括証明書の交換が必要です。

デフォルトでセキュリティを無効にするには、Cisco Unified Communications Manager セキュリティ ガイドの「Cisco Unified IP Phone の ITL ファイルの更新」セクションを参照してください。

混在モードのプロキシ TFTP

混在モードで実行されているリモートクラスタ上の TFTP サーバには、シスコ証明書信頼リスト (CTL) ファイルにプライマリ プロキシ TFTP サーバ証明書を追加する必要があります。 そうでない場合、セキュリティが有効になっているクラスタに登録されているエンドポイントは、必要なファイルをダウンロードできなくなります。 証明書の一括インポートエクスポートを実行した後、この更新 CTL ファイルを実現するには。

詳細については、IP電話をクラスタ間で移行して一括証明書のエクスポートを実行する場合、Cisco Unified Communications Manager セキュリティ ガイドの「一括証明書のエクスポート」セクションを参照してください。

プロキシ TFTP 環境内のクラスタ間での電話機の移動

プロキシ TFTP 環境のリモート クラスタ間で電話機を移動する場合は、次の手順を実行します。

1. リモート クラスタ B (宛先クラスタ) に電話機の詳細を追加します。
2. リモート クラスタ A (送信元クラスタ) から電話機の詳細を削除します。

（注） プロキシTFTPでの電話機の設定は、期限切れになるまで30分あります。ファイルが見つからない応答を避けるために、プロキシ クラスタの TFTP サービスを再起動します。

3. 電話機をリセットしてリモートクラスタBから設定ファイルをダウンロードし、リモートクラスタ B に登録します。

TFTP サーバの設定タスク フロー

クラスタに対して拡張モビリティクロスクラスタ (EMCC) が設定されている場合は、システムがプロキシTFTPサーバを動的に設定できます。そうしない場合は、TFTPサーバを設定して、セキュリティモードを手動で設定することができます。

手順

	コマンドまたはアクション	目的
ステップ 1	次のいずれかの方法を使用して、TFTP サーバをセットアップします。 • TFTP サーバのダイナミック設定 （426 ページ） • TFTP サーバの手動設定 （427 ページ）	クラスタ間ルックアップサービス (ILS) が設定されている場合は、TFTP サーバを動的に設定することができます。 EMCCが設定されていない場合は、TFTP サーバを手動でセットアップします。クラスタがセキュアであるか、あるいは非セキュアであるかを示す必要があります。 クラスタは、デフォルトでは非セキュアとして扱われます。
ステップ 2	（任意） TFTP サーバの CTL ファイルの更新 （428 ページ）	CTL クライアントプラグインをインストールし、混在モードで動作しているすべてのリモートクラスタ内のすべてのプロキシ TFTP サーバの Cisco Certificate Trust List (CTL) ファイルにプライマリプロキシ TFTP サーバを追加します。

	コマンドまたはアクション	目的
ステップ 3	（任意） エンドポイント デバイスに対応するドキュメントを参照してください。	プロキシTFTP展開にリモートクラスタがある場合は、プロキシTFTPサーバをすべてのリモートエンドポイントの信頼検証リスト (TVL) に追加する必要があります。
ステップ 4	（任意） TFTP サーバの非設定ファイルの変更 （429 ページ）	プロキシTFTPサーバからエンドポイントを要求した非設定ファイルを変更できます。
ステップ 5	（任意） TFTP サービスの停止と開始 （429 ページ）	エンドポイントの変更済みの設定されていないファイルをアップロードした場合は、プロキシ TFTP ノード上で TFTP サービスを停止して再起動します。
ステップ 6	（任意） DHCPサーバに対応するドキュメントを参照してください。	複数のクラスタに展開する場合は、プライマリプロキシ TFTP サーバの IP アドレスが含まれるように、個々のリモートノードのDHCPスコープを変更します。

TFTP サーバのダイナミック設定

ネットワークに設定されているクラスタルックアップサービス (ILS) を使用している場合は、Cisco proxy TFTP サーバを動的に設定することができます。

始める前に

ネットワークの EMCC を設定します。詳細については、『*Cisco Unified Communications Manager* 機能およびサービス ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

SIP OAuth が有効になっている場合は、オフクラスタの Tomcat 証明書のルート CA 証明書をプロキシ電話 Edge Trust にコピーする必要があります。

手順

Cisco Unified Communications Manager の管理ページで、**[拡張機能(Advanced Features)]** > **[クラスタビュー(Cluster View)]** > **[今すぐリモートクラスタを更新(Update Remote Cluster Now)]** を選択します。TFTP サーバはクラスタに対して自動的に設定されます。

次のタスク

エンドポイントの信頼検証リスト (TVL) にリモートプロキシ TFTP サーバを追加する必要があります。そうでない場合は、リモートクラスタ上のプロキシ TFTP サーバからの構成ファイルは受け入れられません。詳細については、お使いのエンドポイントデバイスに対応するマニュアルを参照してください。

TFTP サーバの手動設定

EMCC が設定されていない場合にネットワークで TFTP を設定するには、手動の手順を実行する必要があります。

[クラスタ ビュー（Cluster View）] で、プライマリ プロキシ TFTP サーバとその他の TFTP サーバ間のピア関係をセットアップします。 最大 3 台のピア TFTP サーバを追加できます。

プロキシ TFTP 導入環境の各リモート TFTP サーバには、プライマリ プロキシ TFTP サーバとのピア関係が含まれる必要があります。 ループの作成を回避するため、リモート クラスタのピア TFTP サーバが互いを指し示していないことを確認します。

始める前に

重要 リリース 14SU1 以降、SIP OAuth が有効になっている場合は、オフクラスタの Tomcat 証明書のルート CA 証明書をプロキシ電話機のエッジ信頼にコピーする必要があります。

手順

ステップ 1 リモート クラスタを作成します。 次の操作を実行します。

a) Cisco Unified CM Administration で、**[高度な機能（Advanced Features）] > [クラスタの表示（Cluster View）]** を選択します。

b) [新規追加] をクリックします。 [リモート クラスタの設定（Remote Cluster Configuration）] ウィンドウが表示されます。

c) TFTP サーバの最大 50 文字のクラスタ ID と完全修飾ドメイン名（FQDN）を入力し、[保存（Save）]をクリックします。

クラスタ ID の有効な値には、英数字、ピリオド（.）、ハイフン（-）が含まれます。FQDN の有効な値には、英数字、ピリオド（.）、ハイフン（-）、アスタリスク（*）、およびスペースが含まれます。

d) （任意） [リモート クラスタ サービスの設定（Remote Cluster Service Configuration）]ウィンドウで、リモート クラスタの最大 128 文字の説明を入力します。

二重引用符（“）、山カッコ（><）、バックスラッシュ（\）、ハイフン（-）、アンパサンド（&）、またはパーセント記号（%）は使用しないでください。

ステップ 2 リモート クラスタの TFTP を有効にするには、[TFTP]チェック ボックスをオンにします。

ステップ 3 [TFTP]をクリックします。

ステップ 4 [リモート クラスタ サービスの手動上書き設定（Remote Cluster Service Manually Override Configuration）]ウィンドウで、[リモート サービス アドレスの手動設定（Manually configure remote service addresses）]を選択します。

ステップ 5 これらの TFTP サーバとピア関係を作成するには、TFTP サーバの IP アドレスを入力します。

TFTP サーバの IP アドレスは 3 つまで入力できます。

ステップ 6 （任意） プロキシ TFTP サーバがセキュアなクラスタに展開されている場合は、[クラスタは安全です（Cluster is Secure）]チェック ボックスをオンにします。

ステップ 7 **[保存]** をクリックします。

次のタスク

エンドポイントの Trust Verification List（TVL）に、すべてのリモート TFTP サーバを追加する必要があります。追加しないと、エンドポイントがリモート クラスタにあるプロキシ TFTP サーバからの設定ファイルの受け入れが拒否されます。 詳細については、お使いのエンドポイント デバイスに対応するマニュアルを参照してください。

TFTP サーバの CTL ファイルの更新

混在モードの各クラスタで `utils ctl` を実行して、発行元ノードから CTL ファイルを更新します。 プロキシ TFTP サーバとすべてのクラスタ間で完全なセキュリティ ネットワークが作成され、プロキシとリモート クラスタ間の証明書の一括インポートとエクスポート交換が行なえるのを確認します。

CTLClient の使用中、混在モードで動作しているリモートクラスタ内のすべての TFTP サーバの Cisco Certificate Trust List (CTL) ファイルに、プライマリ TFTP サーバまたはプライマリ TFTP サーバの IP アドレスを追加する必要があります。 これは、セキュリティ対応クラスタ内のエンドポイントが設定ファイルを正常にダウンロードできるようにするために必要です。

セキュリティと Cisco CTL CLI の使用の詳細については、Cisco Unified Communications Manager セキュリティ ガイドの「Cisco CTL セットアップについて」のセクションを参照してください。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[アプリケーション] > [プラグイン]**

ステップ 2 **[検索]**をクリックして、インストール可能なすべてのプラグインのリストが表示します。

ステップ 3 Cisco CTL クライアントの**ダウンロード**リンクをクリックします。
システムは TFTP サーバ上に保管される証明書にデジタル署名をするクライアントをインストールします。

ステップ 4 TFTP サーバをリブートします。

TFTP サーバの非設定ファイルの変更

ロードファイルや `RingList.xml`など、設定されていないファイルを、プロキシ TFTP サーバからのエンドポイント要求であるように変更できます。 この手順を完了したら、変更したファイルをプロキシ TFTP サーバの TFTP ディレクトリにアップロードします。

手順

ステップ 1 Cisco Unified Communications Operating System Administration で、**[ソフトウェア アップグレード（Software Upgrades）]** > **[TFTP ファイル管理（TFTP File Management）]** を選択します。
[TFTP ファイル管理] ウィンドウが表示されます。

ステップ 2 [ファイルのアップロード（Upload File）]をクリックします。
[ファイルのアップロード] ポップアップが表示されます。

ステップ 3 次のいずれかの操作を実行します。

- **[参照]**をクリックして、アップロードするファイルのディレクトリの場所を参照します。
- 更新されたファイルの完全なディレクトリパスを**[ディレクトリ]**フィールドに貼り付けます。

ステップ 4 **[ファイルのアップロード]** をクリックするか、**[終了]**をクリックしてファイルをアップロードせずに終了します。

次のタスク

Cisco Unified 有用性管理を使用して、プロキシ TFTP ノード上の Cisco TFTP サービスを停止して再起動します。

TFTP サービスの停止と開始

次の手順に従って、プロキシ TFTP ノード上の TFTP サービスを停止して再開します。

サービスの有効化、無効化、および再起動についての詳細は、『*Cisco Unified Serviceability* アドミニストレーション ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

手順

ステップ 1 Cisco Unified Serviceability で、**[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）]** の順に選択します。

ステップ 2 [コントロール センター-機能サービス（Control Center–Feature Services）] ウィンドウで、[サーバ（Server）] ドロップダウンリストからプロキシ TFTP ノードを選択します。

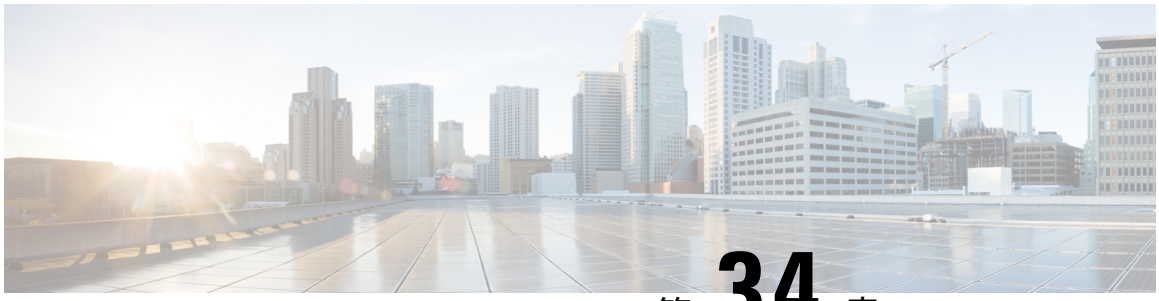
ステップ 3 [CMサービス（CM Services）] 領域で TFTP サービスを選択し、[停止（Stop）] をクリックします。

ステータスが変化し、更新されたステータスが反映されます。

ヒント サービスの最新のステータスを表示するには、[更新（Refresh）] をクリックします。

ステップ 4 [CM サービス（CM Services）] 領域で TFTP サービスを選択し、[開始（Start）] をクリックします。

ステータスが変化し、更新されたステータスが反映されます。



第 34 章

アクティベーション コードによるデバイスのオンボーディング

アクティベーション コードの概要

アクティベーションコードにより、新しくプロビジョニングされた電話機が簡単にプロビジョニングされます。 アクティベーションコードは、電話を登録する際にユーザが電話に入力する必要がある、1 回限りの 16 桁の値です。 アクティベーションコードは、管理者が各電話機の MAC アドレスを手動で収集して入力する必要なく、電話をプロビジョニングおよびオンボードする簡単な方法を提供します。 これは自動登録の代替となるシンプルな方法法であり、この方法で多数の電話機のプロビジョニング、1 台の電話機のプロビジョニング、または既存の電話機の再登録も可能です。

モバイル およびリモートアクセスに準拠したデバイスを使用して、アクティベーション コードを使用してモバイルおよびリモートアクセスから簡単かつ安全に登録することもできます。

アクティベーションコードデバイスのオンボードは、次のモードで動作します。

- オンプレミス
- Mobile Remote Access（MRA）

（注） TFTP プロキシのセットアップでは、アクティベーションコードの導入準備と TFTPA を使用したエンドポイント登録はサポートされていません。

アクティベーション コードには次の利点があります。

- アクティベーション コードを使用したオンボーディングによって、新しくプロビジョニングされた電話機または信頼されていない電話機すべてについて、それぞれの Manufacturing Installed Certificate（MIC）の評価と検証を Unified Communications Manager に実行させることができます。

（注） オンボードアクティビティを実行するには、シスコの製造ルート証明書が CallManager 信頼ストアに存在している必要があります。

- 実際の MAC アドレスを手動で入力する必要はありません。 管理者はダミーの MAC アドレスを使用することができ、電話機は登録時に実際の MAC アドレスを使用して設定を自動的に更新します。
- 電話名を BAT から SEP に変換するために、タップなどの IVR を導入する必要はありません。

電話ユーザは、セルフケアポータルを使用してアクティベーションコードを取得できます。 **[Show Phone Ready To Activate]** 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備えています。 それ以外の場合は、管理者が電話機のユーザにコードを提供する必要があります。

（注） の BAT MAC アドレスを使用してプロビジョニングすると、アクティベーション コードはその電話機モデルに関連付けられます。 BAT MAC は、「BAT」で始まるデバイス名への参照であり、その後に MAC アドレスのように見えるランダムな 12 桁の 16 進数が続きます。 空白の MAC アドレスフィールドを使用してデバイス設定ページを保存すると、この形式のランダムな名前が作成されます。電話機をアクティブにするには、電話機のモデルに一致するアクティベーションコードを入力する必要があります。

セキュリティを強化するために、電話機の実際の MAC アドレスを使用して電話機をプロビジョニングできます。 このオプションでは、管理者がプロビジョニング時に個々の電話機の MAC アドレスを収集して入力する必要があるため、設定項目が多くなりますが、ユーザが電話機の実際の MAC アドレスと一致するアクティベーション コードを入力する必要があるため、セキュリティが向上します。

技術的な制限により、アクティベーションコードを介したデバイスの導入準備はプロキシ TFTP 導入ではサポートされません。

オンプレミス モードでのオンボーディングのプロセス フロー

次に、されている場合に、アクティベーションコードを使用して新しい電話機をオンボードするプロセスフローを示します。

1. 管理者は、ユーザがオンボードのアクティベーションコードを入力するように設定を設定します。
2. 管理者が電話機をプロビジョニングして設定します。 のBAT macアドレスが使用されている場合、管理者は実際の mac アドレスを入力しません。
3. 電話機は、DHCP opt 150 を介して、または電話機の設定で設定されている代替 TFTP から TFTP の IP アドレスを取得します。 電話機は XMLDefault ファイルをダウンロードし、アクティベーションコードが使用中であることを検出します。
4. ユーザが電話機のアクティベーションコードを入力します。
5. 電話機は、アクティベーションコードと製造元でインストールされた証明書を使用して Cisco Unified Communications Manager を認証します。
6. 電話機のオンボーディングにアクティベーションコードを使用する場合、電話機にはTVS サービスが必要になります。 TVS 機能を提供する ITL ファイルには、Unified CM サーバのポート 2445 で稼働する TVS サービスの証明書が含まれています。
7. Cisco Unified Communications Manager は、実際の MAC アドレスを使用してデバイス設定を更新します。 TFTP サーバは、電話機のデバイス設定を検知し、電話機を登録できるようにします。 デバイス登録は最大で5分間可能であることに注意してください。

（注） 導入準備のアクティベーション コードために、デフォルトの通信マネージャ グループにサブスクライバを追加することをお勧めします。 デフォルトの通信マネージャ グループ内のノードがダウンした場合は、導入準備の問題が発生する可能性があります。

モバイルおよびリモートアクセスモードでの導入準備プロセスフロー

次に、モバイルおよびリモートアクセスモードを使用する場合に、アクティベーションコードを使用して新しい電話機をオンボードするプロセスフローを示します。

1. 管理者は、Cisco Cloud でアクティベーションコードのオンボードを有効にし、モバイルおよびリモートアクセスのアクティベーションドメインを指定するように、クラウド/ハイブリッド通信を設定します。
2. 必要に応じて、管理者が追加のモバイルおよびリモートアクセスのサービスドメインを設定します。
3. 管理者は、MACアドレス（BAT、AXL、GUI）を指定せずに完全なデバイス設定を作成します。 デバイス名は、ランダムな BAT MAC アドレスになります。

4. 管理者が、このデバイスのアクティベーション コードを要求します。 デバイスアクティベーションサービスは、クラウドベースのデバイスアクティベーションサービスからコードを要求します。
5. ユーザはセルフケアポータルからコードを取得できます。または、管理者がそのコードをユーザに送信することもできます。
6. ユーザが電話機の電源を投入し、アクティベーションコードを入力します。
7. 電話機はクラウドから、モバイルおよびリモートアクセス/Cisco Unified Communications Manager の場所をクラウドから学習し、認証します。
8. デバイス アクティベーション サービスが、電話機の MAC アドレスでデータベース内のデバイス設定を更新します。

   電話機が、TFTP に登録して通常のモバイルおよびリモートアクセスなどの電話機固有の設定ファイルを取得し、Cisco Unified Communications Manager に登録できるようになりました。

（注） 在宅勤務のリモートユーザにセキュアなソリューションを提供する場合は、TRP でなく Expressway の Mobile and Remote Access を提供することをお勧めします。

アクティベーションコードの前提条件

リリース 12.5(1) では、次の Cisco IP 電話モデルでアクティベーション コードによるオンボーディングがサポートされます。7811、7821、7832、7841、7861、8811、8841、8845、8851、8851NR、8861、8865、および 8865NR。

リリース 12.5 SR3 は、オンプレミスと MRA の両方の Cisco IP 電話モデルでのオンボードをサポートしています。

さらに、リリース 12.5(1)SU1 では、次の Cisco IP 電話モデルがサポートされます。8832 および 8832NR

クラウドのオンボードプロセスでは、次のドメイン名が Cisco Unified Communications Manager によって解決される必要があります。

- fos-a.wbx2.com
- idbroker.webex.com
- push.webexconnect.com
- btpush.webexconnect.com

セルフケア ポータル

ユーザにセルフケア ポータルを使用して電話をオンボードさせる場合は、ユーザがアクセスできるようにポータルを事前にセットアップする必要があります。 詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』の「セルフケア ポータル」の章を参照してください。

オンプレミス モードでのアクティベーション コードを使用したデバイスのオンボーディングのタスク フロー

アクティベーションコードを使用して新しい電話をオンボードするには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	デバイス アクティベーションサービスの有効化 （436 ページ）	シスコの**デバイスアクティベーションサービス**は、シスコの統合型の有用性で実行されている必要があります。
ステップ 2	アクティベーション コードを使用する登録方法の設定 （436 ページ）	[Device Defaults] で、サポートされている電話機モデルのアクティベーション コードを使用するようにデフォルトの登録方法を設定します。
ステップ 3	アクティベーション コードを要件とする電話機をプロビジョニングします。 プロビジョニングのオプションの例を2つ示します。 • アクティベーション コードを要件とする電話機の追加 （437ページ） • 一括管理によるアクティベーション コードを使用した電話の追加 （438 ページ）	Cisco Unified Communications Manager には、左側のオプションを含むさまざまなプロビジョニング方法があります。 どの方法を選択する場合も、その電話機の **[電話機の設定（Phone Configuration）]** で **[オンボーディングにはアクティベーションコードが必要（Requires Activation Code for Onboarding）]** チェックボックスがオンになっていることを確認してください。
ステップ 4	電話機のアクティブ化 （441 ページ）	アクティベーション コードをユーザに配布します。 電話機を使用するためには、ユーザがその電話機にコードを入力する必要があります。

デバイス アクティベーションサービスの有効化

アクティベーション コードを使用するには、Cisco Unified Serviceability で**シスコ デバイス アクティベーション サービス**が実行されている必要があります。 サービスが実行されていることを確認するには、この手順を使用します。

手順

ステップ 1 Cisco Unified Serviceability から、**[ツール（Tools）] > [サービスの有効化（Service Activation）]** を選択します。

ステップ 2 [サーバ（Server）]ドロップダウン リストから、Unified Communications Manager パブリッシャ ノードを選択して [移動（Go）]をクリックします。

ステップ 3 [**CM サービス (CM Services)**] で、 **Cisco デバイスアクティベーションサービス**の**ステータス**が**アクティブ化**されていることを確認します。

ステップ 4 サービスが実行されていない場合は、隣接するチェックボックスをオンにして、[**保存 (Save)**] をクリックします。

次のタスク

アクティベーション コードを使用する登録方法の設定 （436 ページ）

アクティベーション コードを使用する登録方法の設定

特定のモデルタイプの電話機がアクティベーションコードを使用して Unified Communications Manager に登録するようにシステムのデフォルトを設定するには、次の手順を使用します。

（注） この手順は、オンプレミスのエンドポイントの導入準備にのみ適用されます。 **[デバイスのデフォルト]** の下の導入準備メソッド設定は、アクティベーション コードを使用したモバイルおよびリモートアクセス エンドポイントの導入準備には適用されません。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [デバイスのデフォルト（Device Defaults）]** を選択します。

ステップ 2 **[デバイスのデフォルト設定]** ウィンドウで、**[デュアルバンク情報]** セクションで登録にアクティベーションコードを使用するデバイスタイプを選択し、**オンプレミス導入準備メソッド**を**自動登録**から**アクティベーションコード**に変更します。

ステップ 3 **[保存]** をクリックします。

（注） デバイスのデフォルトがアクティベーション コードに設定されている場合で、自動登録が以前に電話タイプに使用されている場合は、以降に新しい電話機を追加する場合は、アクティベーション コードの導入準備または電話機の手動設定 (MAC アドレスを使用) および登録に従う必要があります。

詳細については、アクティベーション コードを要件とする電話機の追加および一括管理によるアクティベーション コードを使用した電話の追加セクションを参照して、新しい電話機をプロビジョニングします。

アクティベーション コードを要件とする電話機の追加

アクティベーション コードを要件として新しい電話機をプロビジョニングする場合は、この手順を使用します。

始める前に

適用する設定を入力したユニバーサル デバイス テンプレートおよびユニバーサル回線テンプレートを設定することで、プロビジョニング プロセスを迅速化できます。

（注） テンプレートを使用しない場合は、新しい電話機を追加して手動で設定するか、または BAT テンプレートを使用して設定を追加することができます。 いずれの場合も、**[電話機の設定（Phone Configuration）]** ウィンドウで **[オンボーディングにはアクティベーションコードが必要（Requires Activation Code for Onboarding）]** チェックボックスをオンにする必要があります。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[デバイス]** > **[電話]**

ステップ 2 [テンプレートからの新規の追加（Add New From Template）]をクリックして、ユニバーサル回線テンプレートまたはユニバーサル デバイス テンプレートから設定を追加します。

ステップ 3 [電話のタイプ（Phone Type）]ドロップダウン メニューから、電話機モデルを選択します。

ステップ 4 [MACアドレス（MAC Address）]フィールドに、MAC アドレスを入力します。 アクティベーション コードでは、ダミーの MAC アドレスまたは電話機の実際の MAC アドレスを使用できます。

次のシナリオでは、電話機の MAC アドレスを変更できます。

- **BAT{mac}->SEP{mac}**: 保存時に **?BAT? to ?SEP?** プレフィックスを変更する正確なデバイス名を知っている必要があります 。

- **SEP{mac}->BAT{mac}**: プレフィックスを ?SEP? から ?BAT? に変更する MAC アドレスと、プレフィックスが ?BAT? の新しいデバイス名を空白にすることができます。.

アクティベーション コードが有効化されている場合、[MACアドレス（MAC Address）]フィールドは空白のままにすることができます。 ダミーの MAC アドレスが自動入力されます。

ステップ 5 [デバイステンプレート（Device Template）]ドロップダウン リストから、適用する設定が含まれる既存のユニバーサル デバイス テンプレートなどのテンプレートを選択します。

ステップ 6 [ディレクトリ番号（Directory Number）]フィールドから、既存のディレクトリ番号を選択するか、[新規（New）] をクリックして次の手順を実行します。

a) [新規内線の追加（Add New Extension）]ポップアップで、適用する設定が含まれている新しいディレクトリ番号と回線テンプレートを入力します。

b) [保存（Save）]をクリックして、さらに [閉じる（Close）]をクリックします。
新しい内線番号が [ディレクトリ番号（Directory Number）]フィールドに表示されます。

ステップ 7 これはオプションです。 [ユーザ（User）]フィールドで、この電話機に適用するユーザー ID を選択します。

ステップ 8 **[Add（追加）]** をクリックします。

ステップ 9 [オンボーディングにはアクティベーションコードが必要（Requires Activation Code for Onboarding）]チェックボックスをオンにします。 モバイルおよびリモート アクセス モードの場合は、[モバイルおよびリモートアクセスでアクティベーション コードを許可する] **チェックボックス**をオンにします。

ステップ 10 適用するその他の設定を入力します。 フィールドとその設定のヘルプについては、オンライン ヘルプを参照してください。

ステップ 11 [保存（Save）]をクリックし、[OK]をクリックします。
この電話機の設定によって新しいアクティベーション コードが生成されます。 コードを表示する場合は、[アクティベーション コードの表示（View Activation Code）]をクリックします。

次のタスク

電話機のアクティブ化 （441 ページ）

一括管理によるアクティベーション コードを使用した電話の追加

このオプションのタスク フローには、一括管理ツールの電話の挿入機能を使用して 1 回の操作で多数の電話をプロビジョニングするプロビジョニング例が含まれます。 これらの電話では、登録にアクティベーション コードを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	BAT プロビジョニングテンプレートの設定 （439 ページ）	プロビジョニングされた電話に適用する設定を含む BAT テンプレートを設定します。
ステップ 2	新しい電話機での CSV ファイルの作成（440 ページ）	追加する新しい電話を含む CSV ファイルを作成します。
ステップ 3	電話の挿入 （441 ページ）	一括管理の電話の挿入機能を使用して、新しい電話をデータベースに追加します。

BAT プロビジョニングテンプレートの設定

特定の電話機モデルの新しくプロビジョニングされた電話に対して一括管理から適用できる、共通設定を入力した電話テンプレートを作成するには、この手順を使用します。

始める前に

この手順では、ユーザがすでにシステムに展開されており、ニーズに合ったデバイス プール、SIP プロファイル、および電話セキュリティ プロファイルがすでに設定済みであることを前提としています。

手順

ステップ 1 Cisco Unified CM Administration から、**[一括管理（Bulk Administration）] > [電話（Phones）] > [電話テンプレート（Phone Template）]** を選択します。

ステップ 2 [新規追加] をクリックします。

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、テンプレートを作成する電話機モデルを選択します。

ステップ 4 [テンプレート名（Template Name）]を入力します。

ステップ 5 [オンボーディングにはアクティベーションコードが必要（Requires Activation Code for Onboarding）]チェックボックスをオンにします。 モバイルおよびリモート アクセス モードの場合は、[モバイルおよびリモートアクセスでアクティベーション コードを許可する]**チェックボックス**をオンにします。

ステップ 6 次の必須フィールドに値を入力します。

- [デバイス プール（Device Pool）]
- [電話ボタンテンプレート（Phone Button Template）]
- [オーナーのユーザID（Owner User ID）]
- デバイス セキュリティ プロファイル（Device Security Profile）
- [SIPプロファイル（SIP Profile）]

ステップ 7 [電話テンプレートの設定（Phone Template Configuration）]ウィンドウで、残りのフィールドを入力します。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。

ステップ 8 **[保存]** をクリックします。

次のタスク

新しい電話機での CSV ファイルの作成 （440 ページ）

新しい電話機での CSV ファイルの作成

新しい電話機で新しい csv ファイルを作成するには、次の手順を使用します。

（注） Csv ファイルは手動で作成することもできます。

手順

ステップ 1 Cisco Unified CM の管理ページから、**[一括管理(Bulk Administration)]** > **[ファイルのアップロード/ダウンロード(Upload/Download Files)]** の順に選択します。

ステップ 2 **[検索(Find)]** をクリックします。

ステップ 3 **Bat**のファイルシートを選択してダウンロードします。

ステップ 4 スプレッドシートを開き、[**電話 (phone)**] タブに移動します。

ステップ 5 新しい電話機の詳細をスプレッドシートに追加します。 ダミーMACアドレスを使用している場合は、[MAC アドレス (MAC Address)] フィールドを空のままにします。 **[オンボーディングにはアクティベーションコードが必要（Requires Activation Code for Onboarding）]** チェックボックスをオンにします。 モバイルおよびリモートアクセス モードの場合は、**[モバイルおよびリモートアクセスでアクティベーション コードを許可する]** チェックボックスをオンにします。

ステップ 6 完了したら、[**BAT 形式にエクスポート (Export TO BAT Format)**] をクリックします。

ステップ 7 Cisco Unified CM の管理ページから、**[一括管理(Bulk Administration)]** > **[ファイルのアップロード/ダウンロード(Upload/Download Files)]** の順に選択します。

ステップ 8 CSV ファイルをアップロードします。

a) [新規追加] をクリックします。

b) [**ファイルの選択 (Choose file)**] をクリックして、アップロードする csv ファイルを選択します。

c) ターゲットとして [電話（Phones）]を選択します。

d) [**Insert phone]:**トランザクションタイプに固有の詳細を選択します。

e) **[保存]** をクリックします。

次のタスク

電話の挿入 （441 ページ）

電話の挿入

CSV ファイルから新しい電話機を挿入するには、この手順を使用します。

手順

ステップ 1 **[一括管理（Bulk Administration）] > [電話（Phones）] > [電話の挿入（Insert Phones）]** を選択します。

ステップ 2 [ファイル名（File Name）]ドロップダウン リストから、CSV ファイルを選択します。

ステップ 3 [電話テンプレート名（Phone Template Name）]ドロップダウン リストから、作成したプロビジョニング テンプレートを選択します。

ステップ 4 [ダミーMACアドレスの作成（Create Dummy MAC Address）]チェックボックスをオンにします。

（注） セキュリティを強化するために、このCSVファイルに実際のMACアドレスを追加することで、一致するMACアドレスを持つ電話機でのみアクティベーション コードを使用できるようになります。その場合は、このチェックボックスをオフのままにします。

ステップ 5 ジョブをすぐに実行するには、[今すぐ実行（Run Immediately）]チェックボックスをオンにします。 後で実行することを選択した場合は、一括管理ツールのジョブ スケジューラでジョブのスケジュールを設定する必要があります。

ステップ 6 **[送信]** をクリックします。

次のタスク

電話機のアクティブ化 （441 ページ）

電話機のアクティブ化

プロビジョニング後に、電話機のユーザにアクティベーションコードを配布して、電話機をアクティブ化できるようにします。 アクティベーションコードを収集して配布するには、次の2つのオプションがあります。

- セルフケアポータル: 電話機のユーザは、電話機に適用されるアクティベーションコードを取得するために、セルフケアポータルにログインできます。 電話機にコードを手動で入力するか、電話機のビデオカメラを使用して、セルフケアで表示されるバーコードをスキャンすることができます。 どちらの方法でも動作します。 電話機のユーザがセルフケアを使用してアクティベーションできるようにするには、Cisco Unified Communications Manager で、**[アクティブにする準備ができているかどうかを表示]** 企業パラメータを **True**（デフォルトの設定）に設定する必要があります。

（注） セルフケア ポータルのユーザ アクセスを設定する方法の詳細については、「*Cisco Unified Communications Manager* の機能設定ガイド」の「セルフケア ポータル」の章を参照してください。

- CSV ファイル: 未処理のユーザとアクティベーションコードのリストを csv ファイルにエクスポートすることもできます。これをユーザに配布できます。手順については、「アクティベーションコードのエクスポート （442 ページ）」を参照してください。

登録プロセス

電話機のユーザは、電話機を使用するために、電話機にアクティベーションコードを入力する必要があります。 電話機のユーザが電話機で正しいアクティベーションコードを入力すると、次のことが発生します。

- 電話機は Cisco Unified Communications Manager で認証されます。
- Cisco Unified Communications Manager の電話機の設定は、電話機の実際の MAC アドレスを使用して更新されます。
- 電話機は、TFTP サーバからコンフィギュレーションファイルおよびその他の関連ファイルをダウンロードし、Cisco Unified Communications Manager に登録します。

次の作業

これで、電話機を使用できる状態になりました。

アクティベーションコードのエクスポート

アクティベーション コードとそれに対応する電話機およびユーザと共に CSV ファイルにエクスポートするには、この手順を使用します。 このファイルを使用して、アクティベーションコードをユーザに配布できます。

手順

ステップ 1 Cisco Unified CM 管理から、**[デバイス]** > **[電話機]** を選択します。

ステップ 2 [関連リンク（Related Links）]から[アクティベーションコードのエクスポート（Export Activation Codes）]を選択し、[移動（Go）]をクリックします。

デバイスオンボードタスクフロー(モバイルおよびリモートアクセス モード)

モバイルおよびリモートアクセス モードでアクティベーション コードを使用して新しい電話機のオンボーディングを実行するには、このタスクを実行します。

始める前に

シスコの**デバイスアクティベーションサービス**は、シスコの統合型の有用性で実行されている必要があります（サービスはデフォルトで実行されています）。 SXP サービスが実行していることを確認するには、デバイス アクティベーションサービスの有効化 （436 ページ）へ移動します。

手順

	コマンドまたはアクション	目的
ステップ 1	モバイルおよびリモートアクセスによる Cisco Cloud 導入準備の有効化 （444 ページ）	[クラウドオンボーディング]でバウチャーを生成し、アクティベーション コードによるオンボーディングを有効化して、モバイルおよびリモートアクセスのアクティベーション ドメインを指定します。
ステップ 2	モバイル およびリモートアクセス サービス のドメイン設定 (オプション) （444 ページ）	クラスタをクラウドに導入準備し、リモート モバイルおよびリモートアクセスのデバイスを特定のモバイルおよびリモートアクセスのアクティベーション ドメインに導入準備できます。
ステップ 3	カスタム証明書のアップロード (オプション) （445 ページ）	これはオプションです。 独自のカスタム証明書を使用する場合、リモートモバイルおよびリモートアクセス エンドポイントは、それらをクラウドからダウンロードし、Expressway に接続するために使用できます。
ステップ 4	アクティベーション コードを要件とする電話機をプロビジョニングします。プロビジョニングのオプションのサンプルを 2 つ示します。 • アクティベーション コードを要件とする電話機の追加 （437 ページ）	Unified CM データベースに電話機をプロビジョニングする必要があります。Unified CM には、次のサンプル オプションを含む、さまざまなプロビジョニング方法を使用できます。

	コマンドまたはアクション	目的
	• 一括管理によるアクティベーションコードを使用した電話の追加 （438 ページ）	
ステップ 5	電話機のアクティブ化 （441 ページ）	アクティベーション コードをユーザに配布します。 電話機を使用するためには、ユーザがその電話機にコードを入力する必要があります。

モバイルおよびリモートアクセスによるCisco Cloud導入準備の有効化

手順

ステップ 1 クラウドベースのデバイス アクティベーション サービスに接続するためにクラスタ（CCMActサービス）を認証するには、[バウチャーの生成（Generate Voucher）]ボタンをクリックしてバウチャーを生成します。

ステップ 2 モバイル およびリモートアクセス アクティベーション ドメインを指定します。 （これはもモバイルおよびリモートアクセスのサービス ドメイン リストに自動的にコピーされます。）

ステップ 3 アクティベーション コードによるオンボーディングを有効化するには、[アクティベーションコードによる導入準備を有効化]チェックボックスと[モバイルおよびリモートアクセスの導入準備を許可] チェックボックスをオンにします。 自動登録を使用したオンボーディングをデバイスのデフォルトとして設定した場合、[モバイルおよびリモートアクセスの導入準備を許可] チェックボックスが無効化され、自動的にチェックされます。この設定はモバイルおよびリモートアクセス モードの電話でのみ機能するためです。 アクティベーション コードを使用したオンボーディングをデバイスのデフォルトとして設定した場合は、両方のチェックボックスを使用できます。

ステップ 4 **[保存]** をクリックします。

モバイル およびリモートアクセス サービスのドメイン設定(オプション)

電話機のモバイルおよびリモートアクセス サービスドメインを設定するには、次の手順を実行します。

手順

ステップ 1 **[詳細機能]**>**[モバイルおよびリモートアクセス サービスドメイン]**を選択して、[モバイルおよびリモートアクセス サービスドメイン] ウィンドウにアクセスします。

ステップ 2 モバイル およびリモート アクセス サービスのドメイン名を入力します。

ステップ 3 アクティベーションに使用される入力 Sway E の SRV レコードを入力します。

ステップ 4 選択したドメインの横にある**[デフォルト]**のチェックボックスをオンにして、デフォルトのモバイルおよびリモートアクセス サービスドメインを選択します。 これは、デバイスプールレベルで [< None >] を選択した場合に使用されるドメインです。

ステップ 5 そのレコードの行にあるリンクを使用して依存関係レコードにアクセスし、依存関係の数も表示します。

カスタム証明書のアップロード(オプション)

カスタム証明書をアップロードするには、次の手順を使用します。

手順

ステップ 1 証明書をエクスプレス Sway にアップロードします。 他の証明書は削除しないでください。

ステップ 2 **[CUCM OSの管理（CUCM OS Administration）] > [証明書の管理（Certificate Management）]** のパスを使用して、新しい証明書を Unified Communications Manager にアップロードします。「電話エッジ信頼」タイプを使用します。 （Unified Communications Manager は、これらの証明書をクラウドに送信してから、Expressway にアクセスする電話機に送信します）。

ステップ 3 必要に応じて、その他の「電話エッジ信頼」タイプの証明書を削除して、カスタム証明書が使用中の証明書だけになるようにします。

アクティベーションコードの追加タスク

次の表に、アクティベーションコードに必要となる追加タスクを示します。

タスク	手順
登録済み電話機のアクティベーションコードの生成	すでに登録されている電話機のアクティベーションコードを生成するには、次のようにします。 1. Cisco Unified CM 管理から、**[デバイス] > [電話機]** を選択します。 2. アクティベーション コードを生成する電話機を検索して [電話機の設定（Phone Configuation）]を開きます。 3. [オンボーディングにはアクティベーションコードが必要（Requires Activation Code for Onboarding）]チェックボックスをオンにして、[保存（Save）]をクリックします。

タスク	手順
未登録の電話機のアクティベーション コードを生成する	未登録の電話機用に新しいアクティベーション コードを生成するには、次の手順を実行します。これは、新しい電話機のアクティベーションプロセスが失敗した場合などに必要になる可能性があります。 **1.** Cisco Unified CM 管理から、**[デバイス]** > **[電話機]** を選択します。 **2.** アクティベーション コードを生成する電話機を検索して [電話機の設定（Phone Configuation）]を開きます。 **3.** [アクティベーションコードの解放（Release Activation Code）]をクリックします。 **4.** [新しいアクティベーションコードの生成（Generate New Activation Code）]をクリックし、[保存（Save）]をクリックします。
アクティベーション コードのオプションパラメータの設定	アクティベーション コードのオプションのサービス パラメータを設定する場合は、次の手順を実行します。 **1.** Cisco Unified CM Administration から、[システム（System）]>[サービスパラメータ（Service Parameters）]を選択します。 **2.** [サーバ（Server）]ドロップダウン リストからパブリッシャ ノードを選択します。 **3.** [サービス（Service）]ドロップダウン リストから [シスコデバイスアクティベーションサービス（Cisco Device Activation Service）] を選択します。 **4.** 以下に示すオプションのサービス パラメータの値を設定します。設定の詳細については、状況依存ヘルプを参照してください。 • [アクティベーション有効期間（時間）（Activation Time to Live (Hours)）] : アクティベーション コードが有効である時間数。 デフォルトは 168 です。 • **モバイルおよびリモートアクセス アクティベーションの有効化**: モバイル およびリモート アクセス アクティベーションを有効にするには、これを True (デフォルト設定) に設定します。 • **モバイルおよびリモートアクセス アクティベーション ドメイン**: モバイルおよびリモートアクセス デバイスのアクティベーションが行なわれるドメイン。 **5.** **[保存]** をクリックします。

アクティベーション コードの使用例

次の表に、アクティベーションコードによるデバイスのオンボードの使用例を示します。

使用例	説明
既存の電話機の交換	アクティベーションコードを使用すると、既存の電話機を簡単に置き換えることができます。 たとえば、リモートワーカーには電話機が破損しているために新しい電話機が必要であるとしましょう。 • 管理者が、Unified Communications Manager で破損した電話機の[電話機の設定（Phone Configuration）]を開きます。 • 管理者は、 **MAC アドレス**を空白にし、[**Activation Code for Activation**] チェックボックスをオンにして、[**Save**] をクリックします。 • ユーザは同じ電話機モデルの新しい電話機を取得し、電話機をネットワークに接続します。 • ユーザはセルフケアにログインしてアクティベーションコードを取得し、電話機にコードを入力します。 電話機のオンボーディングが正常に終了します。 （注） このシナリオでは、ユーザは、破損した電話機と同じ電話機モデルである限り、新しい電話機をオンボードできます。 より安全な環境では、古い電話機を交換するために、管理者が交換用電話機をプロビジョニングする必要がある場合があります (以下を参照)。

使用例	説明
アクティベーションコードを使用した新しい電話機の安全な輸送	より安全な環境では、次のように、特定の MAC アドレスにアクティベーションコードを使用して、電話機の出荷プロセスが安全であることを確認できます。 • 管理者が、Unified Communications Manager で新しい電話機をプロビジョニングします。 • 新しい電話の**電話の構成**時の設定では、管理者が電話機の実際の**MAC アドレス**を入力し、[**オンボードのアクティベーションコードが必要 (Requires Activation Code for Activation)**] チェックボックスをオンにします。 • 管理者が、電話機を梱包してユーザに発送します。 • ユーザは新しい電話機をネットワークに接続します。 • ユーザがセルフケアにログインしてアクティベーションコードを取得すると、電話機にコードが入力されます。電話機のオンボーディングが正常に終了します。 （注） このシナリオでは、ユーザはその特定の電話機のみをオンボードできます。
新しい電話機の安全な輸送 (自動登録)	アクティベーションコードの代わりに、自動登録と tap を使用して、電話機をリモートワーカーに安全に輸送することもできます。 • デバイスの**デフォルト設定**では、管理者は電話機モデルの**オンボード方式**が**自動登録**であることを確認します。 • 管理者が、Unified Communications Manager で新しい電話機をプロビジョニングします。 新しい電話機の**電話機の設定**では、管理者が電話機の実際の**MAC アドレス**を空白にします。 • 管理者が、電話機を梱包してユーザに発送します。 • ユーザは新しい電話機をネットワークに接続し、自動登録を行うことができます。 • ユーザは tap を使用して、自動登録レコードを古いレコードに戻します。 （注） このシナリオでは、自動登録とタップの両方を設定する必要があります。

使用例	説明
自動登録による電話の再登録	アクティベーションコードと自動登録の間の特定の電話機モデルの導入準備方式を、**[デバイスのデフォルト設定（Device Defaults Configuration）]** ウィンドウの**オンプレミス導入準備方式**を使用して切り替えることができます。 （注） 既存の電話機を自動登録経由で再オンにする場合は、自動登録が機能するようにデータベースから既存のレコードを削除する必要があります。
モバイルおよびリモートアクセスモードで使用するためのオンプレミス電話機	電話機をオンプレミスでオンプレミスにしてから、モバイルおよびリモートアクセスモードで電話機を再度オンボードにマークして、MRA モードでの OAuth 接続によって提供されたセキュリティを活用し、ライン sway から Cisco Unified Communications Manager への信頼できる接続を利用することができます。 このシナリオでは、「モバイルおよびリモートアクセスを介してアクティベーション コードを許可する」が有効になっている状態で、電話機のオンプレミスで、受信したOAuthアクセストークンを検証し、モバイルおよびリモートアクセス モードに切り替えて、モバイルおよびリモートアクセス との通信を開始します。 内部ネットワークでオンプレミスからのライン Sway との通信が許可されていない場合、電話機は登録されませんが、オフプレミスの電源がオンになっているときには、その電話機に接続する準備ができています。 （注） 未登録のオフプレミスの電話機は、ファームウェアのロードを更新できません。このシナリオは、最新のファームウェアをダウンロードし、アクティベーションコード機能を使用するためにオンプレミスにする必要がある、すぐに設定された電話機で役立ちます。 **[MRA を介してアクティベーションコードを許可する]** チェックボックスがオンになっていて、MRA サービスドメインと OAuth トークンがある場合、電話機はMRA モードに切り替わります。
ゼロ タッチ導入準備によるオンプレミス電話機の導入準備	オンプレミスの電話機が登録され、セキュリティ プロファイルが OAuth として設定されている場合、電話機はリセットまたは再起動時にアクセス トークンを暗黙的に取得します。

第 35 章

自動登録の設定

自動登録の概要

自動登録では、新しい電話機をネットワークに接続したときに、Unified Communications Manager がそれらの電話機にディレクトリ番号を自動的に割り当てることができます。

現在、自動登録はセキュアモードで有効になっています。この拡張機能によって、新しい電話のプロビジョニング中にクラスタを保護できるため、システムのセキュリティが強化されます。また、新しい電話を登録する際にクラスタセキュリティを無効にする必要がないため、登録プロセスが簡素化されるメリットもあります。

911（緊急）および0（オペレータ）コールのみを許可するデバイスプールを作成しておくと、自動登録が有効になっている場合に許可されていないエンドポイントがネットワークに接続するのを防ぐために使用できます。新しいエンドポイントはこのプールに登録できますが、アクセスは制限されます。連続して起動しネットワークへの登録を試みる不正なデバイスによる不正アクセスは阻止されます。電話番号に影響を与えることなく、自動登録された電話を新しい場所に移動し、別のデバイスプールに割り当てることができます。

システムは、自動登録されている新しい電話機が SIP または SCCP を実行しているかどうかを認識していないため、自動登録を有効にするときにこれを指定する必要があります。SIP と SCCP の両方をサポートするデバイス（Cisco IP 電話 7911、7940、7941、7960、7961、7970、および7971 シリーズなど）は、Auto Registration Phone Protocol と呼ばれるエンタープライズパラメータで指定されたプロトコルで自動登録されます。

1 つのプロトコルのみをサポートするデバイスは、そのプロトコルを使用して自動登録されます。自動登録の電話プロトコル設定は無視されます。たとえば、SCCP のみをサポートするすべての Cisco IP 電話は、自動登録電話プロトコルパラメータが [SIP] に設定されていても、SCCP でのみ自動登録します。

ネットワークに追加する電話機が 100 に満たない場合は、自動登録機能を使用することをお勧めします。100 台を超える電話機を追加するには、一括管理ツール（BAT）を使用します。詳細については、『*Cisco Unified Communications Manager* 一括アドミニストレーション ガイド』

（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

自動登録の設定タスク フロー

自動登録を有効にすると、セキュリティ上のリスクが伴います。ネットワークに新しいエンドポイントを追加している間は、短時間の自動登録のみを有効にしてください。

手順

	コマンドまたはアクション	目的
ステップ 1	自動登録のパーティションの設定 （453 ページ）	自動登録された電話を内部コールのみに制限するために、自動登録専用に使用するルートパーティションを設定します。
ステップ 2	自動登録用コーリングサーチスペースの設定 （454 ページ）	自動登録電話を内線専用に制限するには、自動登録専用のコーリング サーチスペースを設定します。
ステップ 3	自動登録用デバイスプールの設定 （455 ページ）	自動登録用に設定されているコーリングサーチスペースを使用するデバイスプールを作成します。
ステップ 4	自動登録のデバイス プロトコル タイプの設定 （456 ページ）	自動登録する電話機のタイプに一致するように、プロトコルを SCCP または SIP に設定するには、次の手順を使用します。
ステップ 5	自動登録の有効化 （456 ページ）	ノード上の自動登録を有効にして自動登録に使用し、**自動登録Cisco Unified Communications Managerグループ**パラメータを、自動登録に使用されるCisco Unified Communications Managerグループの自動登録を有効にします。
ステップ 6	自動登録の無効化 （458 ページ）	新しいデバイスの登録が完了したらすぐに、ノードの自動登録を無効にします。
ステップ 7	自動登録番号の再利用 （459 ページ）	これはオプションです。 無効になっているデバイスの自動登録番号は再利用できます。 自動登録ディレクトリ番号の範囲をリセットした場合、開始番号から再度検索するようにシステムに強制します。 利用可能なディレクトリ番号は再利用されます。

自動登録のパーティションの設定

自動登録された電話を内部コールのみに制限するために、自動登録専用に使用するルートパーティションを設定します。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**コールルーティング** > **コントロールのクラス** > **パーティション**。

ステップ 2 [新規追加（Add New）]をクリックして新しいパーティションを作成します。

ステップ 3 [パーティション名、説明（Partition Name, Description）]フィールドに、ルート プランに固有のパーティション名を入力します。

パーティション名には、英数字とスペースの他にハイフン（-）とアンダースコア（_）を使用できます。 パーティション名に関するガイドラインについては、オンライン ヘルプを参照してください。

ステップ 4 パーティション名の後にカンマ（,）を入力し、パーティションの説明を同じ行に入力します。

説明にはどの言語でも最大 50 文字まで指定できますが、二重引用符（"）、パーセント記号（%）、アンパサイド（&）、バックスラッシュ（\）、山カッコ（<>）、角括弧（[]）は使用できません。

説明を入力しなかった場合は、Cisco Unified Communications Manager が、このフィールドに自動的にパーティション名を入力します。

ステップ 5 複数のパーティションを作成するには、各パーティション エントリごとに 1 行を使います。

ステップ 6 [スケジュール（Time Schedule）]ドロップダウン リストから、このパーティションに関連付けるスケジュールを選択します。

スケジュールでは、パーティションが着信コールの受信に利用可能となる時間を指定します。[なし（None）]を選択した場合は、パーティションが常にアクティブになります。

ステップ 7 次のオプション ボタンのいずれかを選択して、[タイム ゾーン（Time Zone）]を設定します。

- [発信側デバイス（Originating Device）]：このオプション ボタンを選択すると、発信側デバイスのタイムゾーンと [スケジュール（Time Schedule）]が比較され、パーティションが着信コールの受信に使用できるかどうかが判断されます。
- [特定のタイム ゾーン（Specific Time Zone）]：このオプション ボタンを選択した後、ドロップダウン リストからタイム ゾーンを選択します。 選択されたタイム ゾーンと [スケジュール（Time Schedule）]が比較され、着信コールの受信にパーティションが使用できるかどうかが判断されます。

ステップ 8 **[保存]** をクリックします。

次のタスク

自動登録用コーリングサーチスペースの設定 （454 ページ）

自動登録用コーリングサーチスペースの設定

自動登録電話を内線専用に制限するには、自動登録専用のコーリング サーチ スペースを設定します。

始める前に

自動登録のパーティションの設定 （453 ページ）

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**コールルーティング** > **コントロールのクラス** > **コーリングサーチスペース**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [名前（Name）]フィールドに、名前を入力します。

各コーリング サーチ スペース名がシステムに固有の名前であることを確認します。 この名前には、最長 50 文字の英数字を指定することができ、スペース、ピリオド（.）、ハイフン（-）、およびアンダースコア（_）を任意に組み合わせて含めることが可能です。

ステップ 4 [説明（Description）]フィールドに、説明を入力します。

説明には、どの言語でも最大 50 文字まで指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。

ステップ 5 [使用可能なパーティション（Available Partitions）]ドロップダウン リストから、次の手順のいずれかを実施します。

- パーティションが 1 つの場合は、そのパーティションを選択します。
- パーティションが複数ある場合は、**コントロール（Ctrl）**キーを押したまま、適切なパーティションを選択します。

ステップ 6 ボックス間にある下矢印を選択し、[選択されたパーティション（Selected Partitions）]フィールドにパーティションを移動させます。

ステップ 7 （任意） [選択されたパーティション（Selected Partitions）]ボックスの右側にある矢印キーを使用して、選択したパーティションの優先順位を変更します。

ステップ 8 **[保存]** をクリックします。

次のタスク

自動登録用デバイスプールの設定 （455 ページ）

関連トピック

サービスクラス （208 ページ）

自動登録用デバイスプールの設定

自動登録にデフォルトのデバイスプールを使用するか、SIP 用と SCCP デバイス用に自動登録に使用する個別のデバイスプールを設定することができます。

自動登録用のデフォルトのデバイスプールを設定するには、デフォルトのCisco Unified Communications Managerグループと、自動登録コーリングサーチスペース(CSS)をデフォルトのデバイス プールに割り当てます。 SIP デバイスと SCCP デバイス用に個別のデフォルトデバイスプールを設定する場合は、デフォルトのデバイスプール値を使用します。

始める前に

自動登録用コーリングサーチスペースの設定 （454 ページ）

手順

ステップ 1 Cisco Unified Communications Manager の管理ページで、**[システム(System)]** > **[デバイスプール(Device Pool)]** を選択します。

ステップ 2 自動登録のデフォルトデバイスプールを変更するには、次の操作を実行します。

a) **[検索（Find）]**をクリックし、デバイスプールのリストから **[デフォルト]** を選択します。

b) **[デバイスプールの設定]** ウィンドウで、**[自動登録の コーリングサーチスペース]** フィールドで自動登録に使用するCSS を選択し、**[保存(Save)]** をクリックします。

ステップ 3 自動登録用の新しいデバイスプールを作成するには、次の操作を実行します。

a) [新規追加] をクリックします。

b) [**デバイスプールの設定**] ウィンドウに、デバイスプールの一意の名前を入力します。

名前は最大50文字までで、英数字、ピリオド（.）、ハイフン（-）、アンダースコア（_）、および空白を使用できます。

c) 次のフィールドをデフォルトのデバイスプールと一致するように設定します。 フィールドの説明については、オンライン ヘルプを参照してください。

- **Cisco Unified Communications Manager グループ**で、**デフォルト**を選択します。
- [**日付と時刻]**グループで、**CMLocal** を選択します。
- **[リージョン（Regions）]** で、**[デフォルト（Default）]** を選択します。

d) **[自動登録のコーリングサーチスペース]** フィールドで自動登録に使用する CSS を選択し、**[保存(Save)]** をクリックします。

次のタスク

自動登録のデバイス プロトコル タイプの設定 （456 ページ）

自動登録のデバイス プロトコル タイプの設定

SIP および SCCP デバイスが自動登録されている場合は、まず自動登録の電話プロトコルパラメータを SCCP に設定し、SCCP を実行しているすべてのデバイスをインストールする必要があります。 次に、Auto Registration Phone Protocol パラメータを [SIP] に変更し、SIP を実行するすべての電話を自動登録する必要があります。

始める前に

自動登録用デバイスプールの設定 （455 ページ）

手順

ステップ 1 [Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] で、**[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** を選択します。

ステップ 2 **[エンタープライズパラメータ設定（Enterprise Parameters Configuration）]** ウィンドウで、**[Auto Registration Phone Protocol]** ドロップダウンリストから **[SCCP]** または **[SIP]** のいずれかを選択し、**[保存（Save）]** をクリックします。

次のタスク

自動登録の有効化 （456 ページ）

自動登録の有効化

自動登録が有効の場合は、ネットワークに接続する際に新しいエンドポイントに割り当てられるディレクトリ番号の範囲を指定する必要があります。 新しいエンドポイントが接続される度に、次の使用可能なディレクトリ番号が割り当てられます。 自動登録に使用できるディレクトリ番号がなくなった場合、エンドポイントを自動登録することはできません。

新しいエンドポイントは、**[自動登録 Cisco Unified CM グループ（Auto-Registration Cisco Unified Communications Manager Group）]** 設定が有効になっているグループ内の最初の Unified Communications Manager ノードを使用して、自動登録されます。 その後、デバイス タイプに基づき、自動登録された各エンドポイントがデフォルトのデバイス プールに自動で割り当てられます。

始める前に

自動登録のデバイス プロトコル タイプの設定 （456 ページ）

- デバイス プール、コーリング サーチ スペース、および内線発信のみ許可するように自動登録するデバイスのアクセスを制限するルート パーティションを作成します。
- ディレクトリ番号が自動登録範囲で利用できることを確認します。

- 新しい電話を登録するために利用できるライセンス ポイントが十分にあることを確認します。
- [デバイスのデフォルト設定（Device Defaults Configuration）]ウィンドウに、SIP および SCCP の電話イメージ名が正しく表示されていることを確認します。 共通デバイス設定ファイルのほとんどは TFTP サーバ上で利用できますが、デバイスの設定ファイルが存在することを確認します。
- シスコの TFTP サーバが起動して実行中であることと、TFTP の DHCP オプションで適切なサーバが指定されていることを確認します。

手順

ステップ 1 Cisco Unified Communications Manager Administration から、**[システム（System）]** > **[Cisco Unified CM]** を選択し、**[Cisco Unified Communications Managerの検索と一覧表示（Find and List Cisco Unified Communications Managers）]** ウィンドウの **[検索（Find）]** をクリックします。

ステップ 2 自動登録を使用するには、クラスタの [Cisco Unified Communications Manager]を選択します。

が表示されます。

ステップ 3 [Cisco Unified CM Configuration（Cisco Unified CM Configuration）]ウィンドウで、[自動登録情報（Auto-registration Information）]セクションのノードの自動登録パラメータを設定し、[保存（Save）]をクリックします。 フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

a) ユニバーサル デバイス テンプレートを選択して、ドロップダウン リストから自動登録を使用します。

自動登録用に作成されているユニバーサル デバイス テンプレートがない場合は、[デフォルトのユニバーサル デバイス テンプレート（Default Universal Device Template）]を選択します。 選択したテンプレートで、デバイス プールが指定されていることを確認します。これは、**[ユーザの管理（User Management）]** > **[ユーザ/電話の追加（User/Phone Add）]** > **[ユニバーサルデバイステンプレート（Universal Device Template）]** からの自動登録で使用されます。

b) ドロップダウン リストからの自動登録に使用するユニバーサル ライン テンプレートを選択します。

自動登録用に作成されているユニバーサル ライン テンプレートがない場合は、[デフォルトのユニバーサル ライン テンプレート（Default Universal Line Template）]を選択します。選択したテンプレートで、コーリング サーチ スペースおよびルート パーティションが指定されていることを確認します。これは、**[ユーザの管理（User Management）]** > **[ユーザ/電話の追加（User/Phone Add）]** > **[ユニバーサル回線テンプレート（Universal Line Template）]** からの自動登録で使用されます。

c) 電話番号の最初と最後を [開始ディレクトリ番号（Starting Directory Number）]および [終了ディレクトリ番号（Ending Directory Number）]フィールドに入力します。

ディレクトリ番号の最初と最後を同じ値に設定すると、自動登録は無効になります。

d) [このCisco Unified CM では自動登録は無効にする（Auto-registration Disabled on this Cisco Unified Communications Manager）]のチェックボックスをオフにして、このノードの自動登録を有効にします。

選択した Unified Communications Manager ノードでのみ自動登録を常に有効化または無効化します。 自動登録機能をクラスタ内の別のノードに切り替える場合は、使用する Unified Communications Manager ノード、デフォルトの Unified Communications Manager グループ、およびデフォルトのデバイス プールを設定し直す必要があります。

ステップ 4 **[システム（System）]** > **[Cisco Unified CM グループ（Cisco Unified CM Group）]** の順に選択し、**[Cisco Unified CM グループの検索と一覧表示（Find and List Cisco Unified Communications Manager Groups）]** ウィンドウの **[検索（Find）]** をクリックします。

ステップ 5 自動登録を有効化する Unified Communications Manager グループを選択します。

このグループ名は、ほとんどの場合 [デフォルト（Default）]になります。 別の Cisco Unified Communications Manager グループを選択することもできます。 このグループでは、最低 1 つのノードを選択する必要があります。

ステップ 6 このグループの [Cisco Unified CM Group Configuration]ウィンドウにおいて、**[自動登録（Auto-registration）] [Cisco Unified Communications Manager][グループ（Group）]** を選択して、グループの自動登録を有効にし、[保存（Save）]をクリックします。

ヒント [選択済 Cisco Unified CM（Selected Cisco Unified Communications Managers）]のリストに、自動登録用に設定したノードが含まれていることを確認します。 矢印を使用して、リストに表示するノードを移動します。 表示されている順に、Unified Communications Manager ノードが選択されます。 変更を [保存（Save）]します。

ステップ 7 自動登録するデバイスをインストールします。

（注） 自動登録された電話を再設定し、その電話を永続的なデバイス プールに割り当てます。 電話のロケーションを変更しても、電話に割り当てられているディレクトリ番号は変更されません。

（注） 別の種類の電話を登録するには、デバイスのプロトコルタイプを変更し、そのデバイスを取り付けてから自動登録を無効にします。

自動登録の無効化

新しいデバイスの登録が完了したらすぐに、ノードの自動登録を無効にします。

始める前に

自動登録の有効化 （456 ページ）

手順

ステップ 1 [Cisco Unified Communications Manager Administration] で、**[システム（System）]** > **[Cisco Unified CM]** を選択し、**[Cisco Unified CM の検索と一覧表示（Find and List Cisco Unified CM）]** ウィンドウの **[検索（Find）]** をクリックします。

ステップ 2 ノードのリストから **Cisco Unified Communications Manager**を選択します。

ステップ 3 選択したノードの **[Cisco Unified CM Configuration]** ウィンドウで、 **[この Cisco Unified Communications Manager で自動登録を無効にする]**チェックボックスにチェックし、このノードの自動登録を無効にし、**[保存（Save）]** をクリックします。

ヒント **開始ディレクトリ番号**と**終了ディレクトリ番号**フィールドに同じ番号に設定しても、自動登録が無効になります。

次のタスク

これはオプションです。 自動登録されたデバイスのディレクトリ番号を手動で変更した場合や、そのデバイスをデータベースから削除した場合は、そのディレクトリ番号を再使用することができます。 詳細については、自動登録番号の再利用 （459ページ）を参照してください。

自動登録番号の再利用

新しいデバイスがネットワークに接続されると、システムは、次に使用可能な（未使用の）自動登録ディレクトリ番号をそのデバイスに割り当てます。 自動登録されたデバイスの電話番号を手動で変更した場合や、そのデバイスをデータベースから削除した場合は、そのデバイスの自動登録されていたディレクトリ番号を再使用することができます。

デバイスが自動登録しようとすると、システムは管理者が指定した自動登録番号の範囲を検索して次に使用可能なディレクトリ番号を検出し、そのデバイスに割り当てます。 Cisco Unified Communications Manager は、最後に割り当てられた電話番号の次のディレクトリ番号から順に、検索を開始します。 範囲内の最後のディレクトリ番号に達すると、システムは範囲の開始ディレクトリ番号から検索し続けます。

自動登録のディレクトリ番号の範囲をリセットし、システムがその範囲の開始番号から検索するようにすることができます。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[システム（System）]** > **[Cisco Unified Communications Manager]** を選択します。

ステップ 2 自動登録をリセットするには、[Cisco Unified Communications Manager]を選択します。

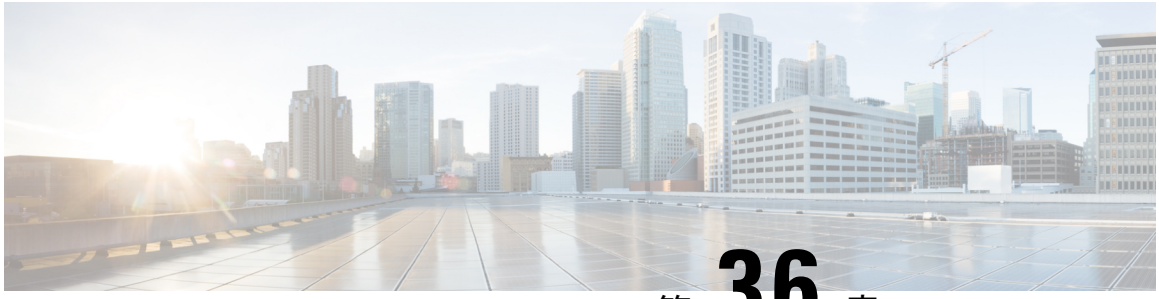
ステップ 3 現在の設定を [開始のディレクトリ番号（Starting Directory Number）] と [最後のディレクトリ番号（Ending Directory Number）] フィールドに書き留めます。

ステップ 4 [この Cisco Unified Communications Manager で自動登録を無効化（Auto-registration Disabled on this Cisco Unified Communications Manager）] をクリックしてから、[保存（Save）] をクリックします。

自動登録が無効の間、新しい電話は自動登録できません。

ステップ 5 [開始ディレクトリ番号（Starting Directory Number）] と [最後のディレクトリ番号（Ending Directory Number）] フィールドを以前の値に設定してから、[保存（Save）] をクリックします。

ヒント これらのフィールドを新しい値に設定できます。



第 36 章

セルフプロビジョニングの設定

セルフプロビジョニングの概要

セルフプロビジョニング機能は、管理者に連絡することなく自分の電話をプロビジョニングする機能をエンドユーザに提供することにより、ネットワークの電話機をプロビジョニングするのに役立ちます。 システムでセルフプロビジョニングが設定されており、個別のエンド ユーザでセルフプロビジョニングが有効化されている場合、そのエンドユーザは電話をネットワークに接続して所定のいくつかのプロンプトに従うことで、新しい電話機をプロビジョニングできます。 Cisco Unified Communications Managerは、事前設定されたテンプレートを適用することによって、電話と電話回線を設定します。

セルフプロビジョニングは、管理者がエンドユーザの代わりに電話機をプロビジョニングする際に使用するか、またはエンドユーザがセルフプロビジョニングを使用して自分の電話機をプロビジョニングするために使用することができます。

セルフプロビジョニングは、クラスタのセキュリティ設定が非セキュア モードまたは混在モードであるかどうかにかかわらずサポートされます。

セキュリティモード

次の 2 つのモードのいずれかで、セルフプロビジョニングを設定できます。

- セキュアモード:セキュアモードでは、ルフプロビジョニングにアクセスするためにはユーザまたは管理者がセ認証されている必要があります。 エンドユーザは、そのパスワードまたは暗証番号に対して認証を受けることができます。 管理者は、事前設定された認証コードを入力できます。
- 非セキュアモード:非セキュアモードでは、ユーザまたは管理者は、ユーザー ID またはセルフプロビジョニング ID を入力して、電話機をユーザアカウントに関連付けることができます。 セキュリティで保護されていないモードは、日々の使用には推奨されていません。

ユニバーサル回線とデバイステンプレートによる設定

セルフプロビジョニングは、エンドユーザに対して、プロビジョニング済みの電話機と電話回線を設定するために、ユニバーサル回線テンプレートとユニバーサルデバイステンプレートの設定を使用します。ユーザが自分の電話機をプロビジョニングすると、システムはそのユーザのユーザプロファイルを参照し、対応するユニバーサルラインテンプレートを、プロビジョニングされた電話回線に、ユニバーサルデバイステンプレートを、プロビジョニングされた電話機に適用します。

プロビジョニングされた電話

この機能を設定したら、次の手順を実行して電話をプロビジョニングできます。

- 電話機をネットワークに接続します。
- セルフプロビジョニングの IVR 拡張機能をダイヤルします。
- プロンプトに従って、電話機を設定し、電話機をエンドユーザに関連付けます。セルフプロビジョニングの設定方法に応じて、エンドユーザは、ユーザーパスワード、PIN、または管理者の認証コードを入力することができます。

ヒント　エンドユーザに代わって多数の電話をプロビジョニングしている場合、セルフプロビジョニング IVR 拡張に転送するユニバーサル デバイス テンプレートに短縮ダイヤルを設定します。

アナログ FXS ポートのセルフプロビジョニング

ユーザがセルフプロビジョニング IVR を呼び出して、関連付けられた DN をそのアナログポートに割り当てることができるように、アナログ FXS ポートでセルフプロビジョニングを有効にすることができます。さらに、プロビジョニングされた電話機では、ユーザはアナログ音声ゲートウェイポートに関連付けられている DN の割り当てを解除し、別のユーザに割り当てることができます。

手順

1. プラグインは、ゲートウェイの FXS 音声ポートのアナログ電話機です。ポートは自動登録または事前設定されている (手動で) ため、電話機は自動登録プールまたは割り当てられた DN から自動的に DN を取得します。
2. 自動登録されたアナログデバイスからのセルフプロビジョニング IVR を呼び出します。
3. セルフサービス ID と PIN を入力します。

（注）　確認時に、アナログデバイスはエンドユーザのプライマリ内線番号を使用してプロビジョニングされます。自動登録 DN がプールに解放されます。

セルフプロビジョニングの前提条件

エンドユーザがセルフプロビジョニングを使用できるようにするには、次の項目を使用してエンドユーザを設定する必要があります。

- エンドユーザには、プライマリ内線番号が必要です。
- エンドユーザは、ユニバーサルラインテンプレートのユニバーサルデバイステンプレートを含む、ユーザプロファイルまたは機能グループテンプレートに関連付けられている必要があります。 ユーザ プロファイルは、セルフプロビジョニング用に有効にする必要があります。

セルフプロビジョニングの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	セルフプロビジョニングのサービスの有効化 （464 ページ）	Cisco Unified 有用性で、**セルフプロビジョニングの IVR** および **CTI Manager** サービスをアクティブにします。
ステップ 2	セルフプロビジョニングの自動登録の有効化 （464 ページ）	セルフプロビジョニング用の自動登録パラメータを有効にします
ステップ 3	CTI ルート ポイントの設定 （465 ページ）	セルフプロビジョニングの IVR サービスを処理するために、CTI ルートポイントを設定します。
ステップ 4	CTI ルートポイントのディレクトリ番号を追加する （465 ページ）	ユーザが自動プロビジョニング IVR にアクセスするためにダイヤルインする内線番号を設定し、その内線番号を CTI ルートポイントに関連付けます。
ステップ 5	セルフプロビジョニングのアプリケーションユーザの設定 （466 ページ）	セルフプロビジョニング IVR 向けのアプリケーションユーザの設定 CTI ルートポイントをアプリケーションユーザに関連付けます。
ステップ 6	セルフプロビジョニングのシステムの設定 （467 ページ）	アプリケーションユーザと CTI ルートポイントをセルフプロビジョニングの IVR に関連付けるなど、システムのセルフプロビジョニング設定を構成します。

	コマンドまたはアクション	目的
ステップ 7	ユーザ プロファイルでのセルフプロビジョニングの有効化 （468 ページ）	ユーザが割り当てられているユーザプロファイルで電話機をセルフプロビジョニングできるようにします。

セルフプロビジョニングのサービスの有効化

セルフプロビジョニング機能をサポートするサービスをアクティブにするには、次の手順を使用します。 セルフプロビジョニング用 IVR サービスと Cisco CTI Manager サービスの両方が実行されていることを確認します。

手順

ステップ 1 Cisco Unified Serviceability から、**[ツール（Tools）] > [サービスの有効化（Service Activation）]** を選択します。

ステップ 2 [サーバ（Server）]ドロップダウン リストからパブリッシャ ノードを選択し、[移動（Go）]をクリックします。

ステップ 3 [**CM サービス**] で、**Cisco CTI Manager** を確認します。

ステップ 4 **CTI サービス**で、**セルフプロビジョニングの IVR** を確認します。

ステップ 5 **[保存]** をクリックします。

セルフプロビジョニングの自動登録の有効化

セルフプロビジョニングにこの手順を使用するためには、パブリッシャで自動登録パラメータを設定する必要があります。

手順

ステップ 1 Cisco Unified CM Administration で、**[システム（System）] > [Cisco Unified CM（Cisco Unified CM）]** を選択します。

ステップ 2 パブリッシャノードをクリックします。

ステップ 3 プロビジョニングされた電話機に適用する**ユニバーサルデバイステンプレート**を選択します。

ステップ 4 プロビジョニングされた電話機の電話回線に適用する**ユニバーサル回線テンプレート**を選択します。

ステップ 5 **開始ディレクトリ番号**と**終了ディレクトリ番号**フィールドを使用して、プロビジョニングされた電話機に適用する一連のディレクトリ番号を入力します。

ステップ 6 **[このCisco Unified CMでは自動登録は無効にする（Auto-registration Disabled on this Cisco Unified Communications Manager）]** チェックボックスをオフにします。

ステップ 7 SIP 登録に使用するポートを確認します。 ほとんどの場合、ポートをデフォルト設定から変更する必要はありません。

ステップ 8 **[保存]** をクリックします。

CTI ルート ポイントの設定

セルフプロビジョニング IVR 用の CTI ルート ポイントを設定するには、この手順を使用します。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[CTIルートポイント（CTI Route Point）]** を選択します。

ステップ 2 次のいずれかの手順を実行します。

a) [検索（Find）]をクリックし、既存の CTI ルート ポイントを選択します。
b) [新規追加（Add New）]をクリックして、新しい CTI ルート ポイントを作成します。

ステップ 3 [デバイス名（Device Name）]フィールドに、ルート ポイントを識別する一意の名前を入力します。

ステップ 4 [デバイスプール（Device Pool）]ドロップダウン リストで、このデバイスのプロパティを指定するデバイス プールを選択します。

ステップ 5 [ロケーション（Location）]ドロップダウン リストから、この CTI ルート ポイントの適切なロケーションを選択します。

ステップ 6 [トラステッド リレーポイントを使用（Use Trusted Relay Point）]ドロップダウン リストから、Unified Communications Manager がこのメディア エンドポイントを使用してトラステッド リレーポイント（TRP）デバイスを挿入するかどうかを選択します。デフォルト設定では、このデバイスに関連付けられている共通デバイス設定の設定が使用されます。

ステップ 7 [CTIルートポイントの設定（CTI Route Point Configuration）]ウィンドウで、残りのフィールドに入力します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 8 **[保存]** をクリックします。

CTI ルートポイントのディレクトリ番号を追加する

セルフプロビジョニング用の IVR にアクセスするためにユーザがダイヤルする内線番号を設定するには、この手順を使用します。 この内線を、セルフプロビジョニングに使用する CTI ルートポイントに関連付ける必要があります。

手順

ステップ 1 Cisco Unified CM 管理（Cisco Unified CM Administration）から**[デバイス（Device）]** > **[CTI ルート ポイント（CTI Route Point）]** を選択します。

ステップ 2 **[検索（Find）]** をクリックして、セルフプロビジョニング用に設定した CTI ルートポイントを選択します。

ステップ 3 **[割り当て（Association）]** で、**[回線 [1] - 新しい DN の追加（Line [2] – Add a new DN）]** をクリックします。
[電話番号の設定(Directory Number Configuration)]ウィンドウが表示されます。

ステップ 4 **[ディレクトリ番号]**フィールドで、セルフプロビジョニングの IVR サービスにアクセスするためにユーザにダイヤルする内線番号を入力します。

ステップ 5 **[保存]** をクリックします。

ステップ 6 **[ディレクトリ番号設定（Directory Number Configuration）]** ウィンドウの残りのフィールドに入力します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 7 **[保存]** をクリックします。

セルフプロビジョニングのアプリケーションユーザの設定

セルフプロビジョニング IVR 用にアプリケーション ユーザを設定し、アプリケーション ユーザに作成した CTI ルーティング ポイントを関連付ける必要があります。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザ（User）]** > **[アプリケーション ユーザ（Application User）]** を選択します。

ステップ 2 次のいずれかの手順を実行します。

a) 既存のアプリケーション ユーザを選択するには、[検索（Find）]をクリックして、アプリケーション ユーザを選択します。

b) 新しいアプリケーション ユーザを作成するには、[新規追加] をクリックします。

ステップ 3 [ユーザ ID（User ID）]テキスト ボックスに、アプリケーション ユーザの一意の名前を入力します。

ステップ 4 アプリケーション ユーザの [BLF プレゼンス グループ（BLF Presence Group）]を選択します。

ステップ 5 アプリケーション ユーザに作成した CTI ルーティング ポイントを関連付けるには、次の手順を実行します。

a) 作成した CTI ルーティング ポイントが、[使用可能なデバイス（Available Devices）]リスト ボックスに表示されない場合は、[別のルート ポイントを検索（Find More Route Points）] をクリックします。
作成した CTI ルーティング ポイントが、使用可能なデバイスとして表示されます。

b) [使用可能なデバイス（Available Devices）]リストで、セルフプロビジョニング用に作成した CTI ルート ポイントを選択し、下向き矢印をクリックします。
CTI ルート ポイントが [制御するデバイス（Controlled Devices）]リストに表示されます。

ステップ 6 [アプリケーション ユーザの設定（Application User Configuration）]ウィンドウの他のフィールドを設定します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 7 **[保存]** をクリックします。

セルフプロビジョニングのシステムの設定

システムをセルフプロビジョニング用に設定するには、次の手順を使用します。セルフプロビジョニングは、ネットワーク内のユーザが管理者に連絡をとらずにIVRシステムを介して自分のデスクフォンを追加できる機能を提供します。

（注） セルフプロビジョニング機能を使用するには、エンド ユーザのユーザ プロファイルでも該当機能を有効にする必要があります。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザ管理（User Management）] > [セルフプロビジョニング（Self-Provisioning）]** を選択します。

ステップ 2 セルフプロビジョニング IVR でエンド ユーザを認証するかどうかを設定するには、次のオプション ボタンのいずれかをクリックします。

- [認証が必要（Require Authentication）]：セルフプロビジョニング IVR を使用するには、エンドユーザが自分のパスワード、PIN、またはシステム認証コードを入力する必要があります。
- [認証は必要なし（No Authentication Required）]：エンドユーザは認証なしでセルフプロビジョニング IVR にアクセスできます。

ステップ 3 セルフプロビジョニング IVR で認証を要求するように設定されている場合、次のオプション ボタンのいずれかをクリックして、IVR がエンド ユーザを認証する方法を設定します。

- [エンド ユーザのみを認証（Allow authentication for end users only）]：エンド ユーザは自分のパスワードまたは PIN を入力する必要があります。
- [ユーザ（Password/PIN の入力）および管理者（認証コードの入力）を認証（Allow authentication for users (via Password/PIN) and Administrators (via Authentication Code)）]：エンド ユーザは認証コードを入力する必要があります。 このオプションを選択した場合、認証コードとして、0 から 20 桁までの整数を [認証コード（Authentication Code）]テキスト ボックスに入力します。

ステップ 4 [IVR 設定（IVR Settings）]のリストボックスから、矢印を使用して IVR プロンプトで使用する言語を選択します。使用可能な言語は、システムにインストールした言語パックによって異なります。 追加の言語パックをダウンロードするには、cisco.com のダウンロード セクションを参照してください。

ステップ 5 [CTIルートポイント（CTI Route Points）]ドロップダウン リストから、セルフプロビジョニング IVR 用に設定した CTI ルート ポイントを選択します。

ステップ 6 [アプリケーションユーザ（Application User）]ドロップダウン リストから、セルフプロビジョニング用に設定したアプリケーション ユーザを選択します。

ステップ 7 **[保存]** をクリックします。

ユーザ プロファイルでのセルフプロビジョニングの有効化

ユーザが電話をセルフプロビジョニングできるようにするには、その機能が割り当てられているユーザプロファイルで有効になっている必要があります。

（注） ユーザが使用しているユーザ プロファイルがわからない場合は、[エンドユーザの設定（End User Configuration）] ウィンドウでユーザの設定を開き、[ユーザプロファイル（User Profile）] フィールドで正しいプロファイルを確認できます。

手順

ステップ 1 Cisco Unified CM Administration から、[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [ユーザプロファイル（User Profile）]を選択します。

ステップ 2 **[検索（Find）]** をクリックして、ユーザが割り当てられているユーザプロファイルを選択します。

ステップ 3 そのユーザプロファイルに**ユニバーサル回線テンプレート**と**ユニバーサル デバイス テンプレート**を割り当てます。

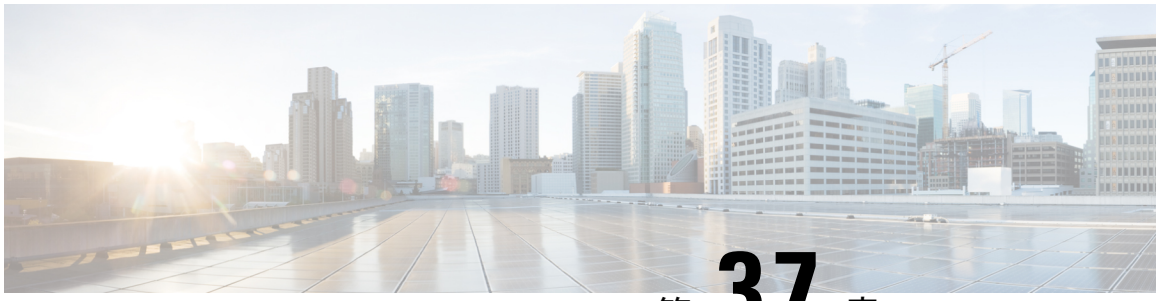
ステップ 4 セルフプロビジョニング用のユーザの設定

- [エンドユーザに自分の電話のプロビジョニングを許可（Allow End User to Provision their own phones）]チェックボックスをオンにします。
- ユーザがプロビジョニングできる電話機の数の制限を入力します。 デフォルトは 10 です。
- ユーザがセルフプロビジョニングを使用して以前に割り当てられた電話機を無効にしたい場合は、古いデバイスのエンド ユーザに関連付けられているユーザ プロファイル ページで、別のエンド ユーザに割り当てられている電話機の **[別のエンドユーザーにすでに割り当てられている電話のプロビジョニングを許可する]** 設定を確認します。 以前に割り当てられた電話機をユーザが再割り当てできるのは、古いデバイスに関連付けられているユーザプロファイル内でこのチェックボックスをオンにした場合のみです。

ステップ 5 **[保存]** をクリックします。

第 VI 部

参考情報



第 37 章

Cisco Unified Communications Manager での TCP および UDP ポートの使用

Cisco Unified Communications Manager の TCP と UDP ポートの使用に関する概要

Cisco Unified Communications Manager の TCP および UDP ポートは、次のカテゴリに整理されます。

- Cisco Unified Communications Manager サーバーがクラスタ間で使用するポート
- 共通サービス ポート
- Cisco Unified Communications Manager と LDAP ディレクトリの間のポート
- CCMAdmin または CCMUser から Cisco Unified Communications Manager への Web 要求
- Cisco Unified Communications Manager から電話機への Web 要求
- 電話機と Cisco Unified Communications Manager の間のシグナリング、メディア、およびその他の通信
- ゲートウェイと Cisco Unified Communications Manager の間のシグナリング、メディア、およびその他の通信
- アプリケーションと Cisco Unified Communications Manager の間の通信
- CTL クライアントとファイアウォールの通信
- HP サーバ上の特殊なポート

上記のそれぞれのカテゴリのポートの詳細については、「「ポートの説明」」を参照してください。

（注） シスコでは、これらのポートで想定されるすべての設定シナリオを検証しているわけではありません。この一覧を参考にした結果、設定に問題が発生した場合は、シスコのテクニカルサポートにお問い合わせください。

ポート設定は、特に Cisco Unified Communications Manager に適用されます。リリースによってポートが異なる場合があり、今後のリリースで新しくポートが追加される可能性もあります。このため、インストールされている Cisco Unified Communications Manager のバージョンに一致するバージョンのマニュアルを使用していることを確認してください。

事実上すべてのプロトコルが双方向で行われますが、セッション開始側から見た方向を記載しています。デフォルトのポート番号は、管理者が手動で変更できる場合もありますが、ベストプラクティスとしてこのような変更は推奨しません。Cisco Unified Communications Manager が内部使用に限って複数のポートを開くことに注意してください。

Cisco Unified Communications Manager ソフトウェアをインストールすると、デフォルトでは有用性のために次のネットワーク サービスが自動的にインストールされてアクティブになります。詳細については、「「Cisco Unified Communications Manager サーバの間のクラスタ内ポート」」を参照してください。

- Cisco Log Partition Monitoring（共通パーティションを監視および消去します。このサービスは、カスタム共通ポートを使用しません）
- Cisco Trace Collection Service（TCTS ポート使用）
- Cisco RIS Data Collector（RIS サーバ ポート使用）
- Cisco AMC Service（AMC ポート使用）

ファイアウォール、ACL、または QoS の設定は、トポロジ、テレフォニー デバイスおよびテレフォニー サービスの配置とネットワーク セキュリティ デバイスの配置との関係、および使用中のアプリケーションとテレフォニー拡張機能によって異なります。また、デバイスやバージョンによって、ACL のフォーマットが異なることにも注意してください。

（注） Cisco Unified Communications Manager でマルチキャスト保留音（MoH）ポートを設定することもできます。このマニュアルにはマルチキャスト MOH のポート値を記載していません。

（注） システムのエフェメラル ポートの範囲は 32768 ～ 61000 であり、電話を登録したままにするには、これらのポートを開く必要があります。詳細については、「http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html」を参照してください。

（注） ポート 22 への接続が開き、抑えられないように、ファイアウォールを設定します。IM and Presence サブスクライバ ノードのインストール中に、Cisco Unified Communications Manager パブリッシャノードに対する複数の接続が短時間に連続して開かれます。これらの接続をスロットリングすると、インストールが失敗する可能性があります。

ポート説明

Cisco Unified Communications Manager サーバ間のクラスタ間ポート

表 *29 : Cisco Unified Communications Manager* サーバ間のクラスタ間ポート

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
エンドポイント（Endpoint）	Unified Communications Manager	514 / UDP	システム ロ
Unified Communications Manager	Unified Communications Manager	443 / TCP	このポートは バノードへの のインストー クライバと発 使用されます
Unified Communications Manager	RTMT	1090、1099 / TCP	RTMT パフォ タ、データ収 およびアラー Cisco AMC サ
Unified Communications Manager（DB）	Unified Communications Manager（DB）	1500、1501 / TCP	データベース TCP はセカン
Unified Communications Manager（DB）	Unified Communications Manager（DB）	1510 / TCP	CAR IDS DB。 ジンが、クラ 接続要求を監
Unified Communications Manager（DB）	Unified Communications Manager（DB）	1511 / TCP	CAR IDS DB。 ド時に、CAR タンスをもう めに使用され
Unified Communications Manager（DB）	Unified Communications Manager（DB）	1515 / TCP	インストール のデータベー ション

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
Cisco Extended Functions（QRT）	Unified Communications Manager（DB）	2552 / TCP	Cisco Unified Co Managerデータ 知をサブスクラ きるようにしま
Unified Communications Manager	Unified Communications Manager	2551 / TCP	アクティブ/バッ 別のための Cisc Services 間のク
Unified Communications Manager（RIS）	Unified Communications Manager（RIS）	2555 / TCP	Real-time Informa （RIS）データ
Unified Communications Manager（RTMT、AMC、またはSOAP）	Unified Communications Manager（RIS）	2556 / TCP	Cisco RIS 向け R Information Servi データベース ク
Unified Communications Manager（DRS）	Unified Communications Manager（DRS）	4040 / TCP	DRS プライマリ ト
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5001 / TCP	このポートは、S がリアルタイム グ サービスに使
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5002 / TCP	このポートは、S がパフォーマン サービスに使用
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5003 / TCP	このポートは、S がコントロール サービスに使用
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5004 / TCP	このポートは、S がログ コレクシ スに使用します
標準 CCM 管理ユーザ / 管理	Unified Communications Manager	5005 / TCP	このポートは SO CDROnDemand 2 よって使用され
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5007 / TCP	SOAP モニタ

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
Unified Communications Manager（RTMT）	Unified Communications Manager（TCTS）	エフェメラル / TCP	Cisco Trace C Service（TCT Trace and Log 向けのバック ス
Unified Communications Manager（Tomcat）	Unified Communications Manager（TCTS）	7000、7001、7002 / TCP	このポートに Collection Too Cisco Trace C との通信に使
Unified Communications Manager（DB）	Unified Communications Manager（CDLM）	8001 / TCP	クライアント 変更通知
Unified Communications Manager（SDL）	Unified Communications Manager（SDL）	8002 / TCP	クラスタ間通
Unified Communications Manager（SDL）	Unified Communications Manager（SDL）	8003 / TCP	クラスタ間通 （CTI 対象）
Unified Communications Manager	CMI マネージャ	8004 / TCP	Cisco Unified Manager と C とのクラスタ
Unified Communications Manager（Tomcat）	Unified Communications Manager（Tomcat）	8005 / TCP	Tomcat シャッ リプトで使用 ニング ポー
Unified Communications Manager（Tomcat）	Unified Communications Manager（Tomcat）	8080 / TCP	診断テストの の通信
ゲートウェイ（Gateway）	Unified Communications Manager	8090	CUCM と GW ターフェイス
Unified Communications Manager	ゲートウェイ（Gateway）		Recording 機能 に使用する H
Unified Communications Manager（IPSec）	Unified Communications Manager（IPSec）	8500 / TCP および UDP	IPSec クラス よるシステム スタ間複製
Unified Communications Manager（RIS）	Unified Communications Manager（RIS）	8888 ～ 8889 / TCP	RIS サービス ステータス要
Location Bandwidth Manager（LBM）	Location Bandwidth Manager（LBM）	9004 / TCP	LBM 間のク

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
Unified Communications Manager パブリッシャ	Unified Communications Manager サブスクライバ	22 / TCP	Cisco SFTP サー スクライバを新 トールする場合 トを開く必要が
Unified Communications Manager	Unified Communications Manager	8443 / TCP	ノード間のコン ター機能とネッ ビスへのアクセ ます。

共通サービス ポート

表 *30 :* 共通サービス ポート

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
エンドポイント（Endpoint）	Unified Communications Manager	7	Internet Control Message Protocol（ICMP）。このプロトコル番号がエコー関連のトラフィックを伝送します。列見出しに示すようなポートとなるものではありません。
Unified Communications Manager	エンドポイント（Endpoint）		
Unified Communications Manager（DRS、通話詳細記録）	SFTP サーバ	22 / TCP	SFTP サーバにバックアップデータを送信します。（DRS ローカル エージェント） 通話詳細記録のデータを SFTP サーバーに送信します。
エンドポイント（Endpoint）	Unified Communications Manager（DHCP サーバ）	67 / UDP	DHCP サーバとして機能する Cisco Unified Communications Manager （注） Cisco Unified Communications Manager 上で DHCP サーバを実行することは推奨しません。

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
Unified Communications Manager	DHCP サーバ（DHCP Server）	68 / UDP	DHCP クライアントとして機能する Cisco Unified Communications Manager （注） Cisco Unified Communications Manager 上で DHCP クライアントを実行することは推奨しません。 その代わりに、Cisco Unified Communications Manager には固定 IP アドレスを設定します。
エンドポイントまたはゲートウェイ	Unified Communications Manager	69、6969、次にエフェメラル / UDP	電話機とゲートウェイに対する TFTP サービス
エンドポイントまたはゲートウェイ	Unified Communications Manager	6970 / TCP	プライマリサーバーとプロキシサーバー間の TFTP。 電話機とゲートウェイに対する TFTP サーバの HTTP サービス
Unified Communications Manager	NTP サーバ（NTP Server）	123 / UDP	ネットワーク タイム プロトコル（NTP）
SNMP サーバ	Unified Communications Manager	161 / UDP	SNMP サービス応答（管理アプリケーションからの要求）
CUCM サーバ SNMP プライマリ エージェント アプリケーション	SNMP トラップの宛先	162 / UDP	SNMP トラップ
SNMP サーバ	Unified Communications Manager	199 / TCP	SMUX サポートのための組み込み SNMP エージェント リスニングポート
Unified Communications Manager	DHCP サーバ（DHCP Server）	546 / UDP	DHCPv6。 IPv6 用の DHCP ポート。

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
Unified Communications Manager Serviceability	Location Bandwidth Manager（LBM）	5546 / TCP	Enhanced Location CAC Serviceability
Unified Communications Manager	Location Bandwidth Manager（LBM）	5547 / TCP	コール アドミッションの要求および帯域幅の縮小
Unified Communications Manager	Unified Communications Manager	6161 / UDP	プライマリエージェントとネイティブエージェント間の通信に使用され、ネイティブエージェントの MIB 要求を処理します。
Unified Communications Manager	Unified Communications Manager	6162 / UDP	プライマリエージェントとネイティブエージェント間の通信に使用され、ネイティブエージェントから生成された通知を転送します。
中央集中型 TFTP	代替 TFTP（Alternate TFTP）	6970 / TCP	中央集中型 TFTP ファイル ロケータ サービス
Unified Communications Manager	Unified Communications Manager	7161 / TCP	SNMP プライマリエージェントとサブエージェント間の通信に使用されます。
SNMP サーバ	Unified Communications Manager	7999 / TCP	Cisco Discovery Protocol（CDP）エージェントが、CDP 実行可能機器と通信します。
エンドポイント（Endpoint）	Unified Communications Manager	443、8443/TCP	Cisco ユーザ データ サービス（UDS）の要求に使用されます。
Unified Communications Manager	Unified Communications Manager	9050 / TCP	Cisco Unified Communications Manager にある TAPS を利用して CRS 要求を処理します。

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
Unified Communications Manager	Unified Communications Manager	61441 / UDP	Cisco Unified Communications Manager アプリケーションが、UDP でこのポートにアラームを送信します。 Cisco Unified Communications Manager MIB エージェントが、Cisco Unified Communications Manager MIB 定義に従って、このポートを監視し、SNMP トラップを生成します。
Unified Communications Manager	Unified Communications Manager	5060、5061 / TCP	トランクベースの SIP サービスを提供します。
Unified Communications Manager	Unified Communications Manager	7501	クラスタ間検索サービス（ILS）の証明書ベースの認証に使用されます。
Unified Communications Manager	Unified Communications Manager	7502	ILS のパスワードベース認証に使用されます。
Unified Communications Manager	Unified Communications Manager	9966	シスコのプッシュ通知サービスで、ファイアウォールが有効になっているときにクラスタ内のノード間で通信するために使用されます。
Unified Communications Manager	Unified Communications Manager	9560	ローカルプッシュ通知サービス（LPNS）で使用されます。
--	--	8000-48200	ASR および ISR G3 プラットフォームのデフォルト ポート範囲。
		16384-32766	ISR G2 プラットフォームのデフォルト ポート範囲。

Cisco Unified Communications Manager と LDAP ディレクトリとの間のポート

表 *31 : Cisco Unified Communications Manager* と *LDAP* ディレクトリとの間のポート

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
Unified Communications Manager	外部ディレクトリ	389、636、3268、3269 / TCP	外部ディレクトリ（Active Directory、Netscape Directory）への Lightweight Directory Access Protocol（LDAP）クエリ
外部ディレクトリ	Unified Communications Manager	エフェメラル	

CCMAdmin または CCMUser から Cisco Unified Communications Manager への Web 要求

表 *32 : CCMAdmin* または *CCMUser* から *Cisco Unified Communications Manager* への *Web* 要求

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
ブラウザ	Unified Communications Manager	80、8080 / TCP	ハイパーテキスコル（HTTP）
ブラウザ	Unified Communications Manager	443、8443 / TCP	Hypertext Transpo over SSL（HTTP
ブラウザ	Unified Communications Manager	9463/TCP	Hypertext Transpo over SSL（HTTP TLS1.3 の v6 のみ ます。

Cisco Unified Communications Manager から電話機への Web 要求

表 *33 : Cisco Unified Communications Manager* から電話機への *Web* 要求

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
Unified Communications Manager • QRT • RTMT • [電話の検索と一覧表示（Find and List Phones）] ページ • [電話の設定（Phone Configuration）] ページ	電話（Phone）	80/TCP	ハイパーテキコル（HTTP

電話機とCisco Unified Communications Managerとの間のシグナリング、メディア、およびその他の通信

表 *34 :* 電話機と *Cisco Unified Communications Manager* との間のシグナリング、メディア、およびその他の通信

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
電話（Phone）	DNSサーバ	53 / TCP	Session Initiation Protocol（SIP）電話機が、ドメインネーム システム（DNS）を使用して、完全修飾ドメイン名（FQDN）を解決します。 （注） デフォルトでは、一部のワイヤレス アクセス ポイントは TCP の 53 番ポートをブロックし、FQDN を使用しながら CUCM を設定しているときに、ワイヤレス SIP 電話機が登録されないようにします。
電話（Phone）	Unified Communications Manager（TFTP）	69、次にエフェメラル / UDP	ファームウェアおよび設定ファイルのダウンロードに使用される Trivial File Transfer Protocol（TFTP）
電話（Phone）	Unified Communications Manager	2000 / TCP	Skinny Client Control Protocol（SCCP）
電話（Phone）	Unified Communications Manager	2443 / TCP	Secure Skinny Client Control Protocol（SCCPS）
電話（Phone）	Unified Communications Manager	2445 / TCP	エンドポイントに信頼検証サービスを提供します。

送信元（送信者）	送信先（リスナー）	宛先ポート（Destination Port）	目的
電話（Phone）	Unified Communications Manager（CAPF）	3804 / TCP	ローカルで有効な証明書（LSC）を IP Phone に発行するための認証局プロキシ機能（CAPF）リスニング ポート
電話（Phone）	Unified Communications Manager	5060 / TCP および UDP	Session Initiation Protocol（SIP）電話機
Unified Communications Manager	電話（Phone）		
電話（Phone）	Unified Communications Manager	5061 TCP	Secure Session Initiation Protocol（SIPS）電話機
Unified Communications Manager	電話（Phone）		
電話（Phone）	Unified Communications Manager（TFTP）	6970 TCP	ファームウェアおよび設定ファイルの HTTP ベースのダウンロード
電話（Phone）	Unified Communications Manager（TFTP）	6971、6972 / TCP	TFTP への HTTPS インターフェイス。 電話機が、TFTP からセキュアな設定ファイルをダウンロードするためにこのポートを使用します。
電話（Phone）	Unified Communications Manager	8080 / TCP	電話機の XML アプリケーション、認証、ディレクトリ、サービスなどの URL。これらのポートは、サービスごとに設定できます。
電話（Phone）	Unified Communications Manager	9443 / TCP	電話機が、認証された連絡先検索にこのポートを使用します。
電話（Phone）	Unified Communications Manager	9444	電話機は、このポート番号を使用してヘッドセット管理機能を利用します。
iPhone/iPad（Webex アプリ）	Unified Communications Manager	9560/安全なウェブソケット	Webex アプリは、このポート番号を LPNS 機能に使用します。

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
IP VMS	電話（Phone）	16384 ～ 32767 / UDP	Real-Time Protocol（RTP）、Secure Real-Time Protocol（SRTP） （注） 他のデバイスは全範囲を使用しますが、Cisco Unified Communications Manager は 24576 ～ 32767 だけを使用します。
電話（Phone）	IP VMS		

ゲートウェイと Cisco Unified Communications Manager との間のシグナリング、メディア、およびその他の通信

表 *35 :* ゲートウェイと *Cisco Unified Communications Manager* との間のシグナリング、メディア、およびその他の通信

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
ゲートウェイ（Gateway）	Unified Communications Manager	47, 50, 51	Generic Routing E（GRE）、Encap Security Payload 証ヘッダー（AH のプロトコル番号 された IPSec トラ 伝送します。 列 すようなポート はありません。
Unified Communications Manager	ゲートウェイ（Gateway）		
ゲートウェイ（Gateway）	Unified Communications Manager	500 / UDP	IP Security（IPSe ル確立のための ト キー エクスチ （IKE）
Unified Communications Manager	ゲートウェイ（Gateway）		
ゲートウェイ（Gateway）	Unified Communications Manager（TFTP）	69、次にエフェメラル / UDP	Trivial File Transf （TFTP）

送信元（送信者）	送信先（リスナー）	宛先ポート（Destination Port）	目的
Cisco Intercompany Media Engine（CIME）トランクを使用した Unified Communications Manager	CIME ASA	1024 ～ 65535 / TCP	ポート マッピス。 CIME オルでのみ使用
Gatekeeper	Unified Communications Manager	1719 / UDP	ゲートキーパ RAS
ゲートウェイ（Gateway）	Unified Communications Manager	1720 / TCP	H.323 ゲート ラスタ間トラ けの H.225 シ サービス
Unified Communications Manager	ゲートウェイ（Gateway）		
ゲートウェイ（Gateway）	Unified Communications Manager	エフェメラル / TCP	ゲートキーパ 上の H.225 シ サービス
Unified Communications Manager	ゲートウェイ（Gateway）		
ゲートウェイ（Gateway）	Unified Communications Manager	エフェメラル / TCP	音声、ビデオ を確立するた ナリング サー （注） ク 種 な シ さ ホ IC イ ホ 1 て
Unified Communications Manager	ゲートウェイ（Gateway）		
ゲートウェイ（Gateway）	Unified Communications Manager	2000 / TCP	Skinny Client （SCCP）
ゲートウェイ（Gateway）	Unified Communications Manager	2001 / TCP	Cisco Unified Manager の導 6608 ゲート グレード ポー

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
ゲートウェイ（Gateway）	Unified Communications Manager	2002 / TCP	Cisco Unified Co Manager の導入 6624 ゲートウェ グレード ポート
ゲートウェイ（Gateway）	Unified Communications Manager	2427 / UDP	Media Gateway C Protocol（MGCP ウェイ コントロ
ゲートウェイ（Gateway）	Unified Communications Manager	2428 / TCP	Media Gateway C Protocol（MGCP ホール
--	--	4000 ～ 4005 / TCP	Cisco Unified Co Managerに音声、 よび D チャネル ないときには、 トがこのような ファントム Real Transport Protoco ポートおよび Re Transport Control （RTCP）ポート されます。
ゲートウェイ（Gateway）	Unified Communications Manager	5060 / TCP および UDP	Session Initiation （SIP）ゲートウ クラスタ間トラ
Unified Communications Manager	ゲートウェイ（Gateway）		
ゲートウェイ（Gateway）	Unified Communications Manager	5061 / TCP	Secure Session In Protocol（SIPS） イおよびクラス （ICT）
Unified Communications Manager	ゲートウェイ（Gateway）		

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
ゲートウェイ（Gateway）	Unified Communications Manager	16384 ～ 32767 / UDP	Real-Time Pro Secure Real-T （SRTP） （注） 他 全 ま U C M ～ 使
Unified Communications Manager	ゲートウェイ（Gateway）		

アプリケーションと Cisco Unified Communications Manager との間の通信

表 *36* : アプリケーションと *Cisco Unified Communications Manager* との間の通信

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
CTL クライアント	Unified Communications Manager CTL プロバイダー	2444 / TCP	Cisco Unified Manager の証 （CTL）プロ ニング サービ
Cisco Unified Communications アプリケーション	Unified Communications Manager	2748 / TCP	CTI アプリケ バ
Cisco Unified Communications アプリケーション	Unified Communications Manager	2749 / TCP	CTI アプリケ （JTAPI/TSP） Manager 間の
Cisco Unified Communications アプリケーション	Unified Communications Manager	2789 / TCP	JTAPI アプリ バ
Unified Communications Manager Assistant Console	Unified Communications Manager	2912 / TCP	Cisco Unified Manager Assis 前の IPMA）

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
Unified Communications Manager Attendant Console	Unified Communications Manager	1103 ～ 1129 / TCP	Cisco Unified Co Manager Attendar （AC）JAVA RM リ サーバ
Unified Communications Manager Attendant Console	Unified Communications Manager	1101 / TCP	RMI サーバは、 バック メッセー のポートを使用 ントに送信しま
Unified Communications Manager Attendant Console	Unified Communications Manager	1102 / TCP	Attendant Console サーバ バインド RMIサーバは、 トに RMI メッセ します。
Unified Communications Manager Attendant Console	Unified Communications Manager	3223 / UDP	Cisco Unified Co Manager Attendar （AC）サーバ回 トは、Attendant バから ping およ セージを受信し Console サーバに 送信します。
Unified Communications Manager Attendant Console	Unified Communications Manager	3224 / UDP	Cisco Unified Co Manager Attendar （AC）クライア 線状態情報およ 態情報のために 登録されます。
Unified Communications Manager Attendant Console	Unified Communications Manager	4321 / UDP	Cisco Unified Co Manager Attendar （AC）クライア コール制御のた バに登録されま
SAF/CCD を使用する Unified Communications Manager	SAF イメージを実行する IOS ルータ	5050 / TCP	EIGRP/SAF プロ 行するマルチサ ルータ。

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
Unified Communications Manager	Cisco Intercompany Media Engine（IME）サーバ	5620 / TCP このポートでは、ポート番号 5620 の使用を推奨しますが、CLI コマンドの add ime vapserver または set ime vapserver port を Cisco IME サーバで実行することにより、値を変更できます。	VAP プロト Intercompany サーバとの通 す。
Cisco Unified Communications アプリケーション	Unified Communications Manager	8443 / TCP	課金アプリケ テレフォニー ションなどの が、Cisco Un Communicatio タベースに対 で読み書きす る AXL/SOA

CTL クライアントとファイアウォールとの通信

表 *37 : CTL* クライアントとファイアウォールとの通信

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
CTL クライアント	TLS プロキシ サーバ	2444 / TCP	ASA ファイ 明書信頼リス バイダー リ ス

Cisco Smart Licensing Service と Cisco Smart Software Manager 間の通信

Unified Communications Manager の Cisco Smart Licensing Service は、コールホームを通じて Cisco Smart Software Manager と直接通信を行います。

表 *38 : Cisco Smart Licensing Service* と *Cisco Smart Software Manager* 間の通信

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
Unified Communications Manager（Cisco Smart Licensing Service）	Cisco Smart Software Manager（CSSM）	443 / HTTPS	スマートライセンシングサービスは、Unified CM が苦情であるかどうかを確認するために、CSSM にライセンス使用を送信します。

HP サーバ上の特殊なポート

表 *39 : HP* サーバ上の特殊なポート

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
エンドポイント（Endpoint）	HP SIM	2301 / TCP	HP エージェントポート
エンドポイント（Endpoint）	HP SIM	2381 / TCP	HP エージェントポート
エンドポイント（Endpoint）	Compaq 管理エージェント	25375、25376、25393 / UDP	COMPAQ 管理エ拡張（cmaX）
エンドポイント（Endpoint）	HP SIM	50000 ～ 50004 / TCP	HP SIM への HT

ポート参照

ファイアウォール アプリケーション インスペクション ガイド

ASA シリーズ参考情報

http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html

PIX アプリケーション Inspection Configuration Guides

http://www.cisco.com/c/en/us/support/security/pix-firewall-software/products-installation-and-configuration-guides-list.html

『FWSM 3.1 Application Inspection Configuration Guide』

http://www-author.cisco.com/c/en/us/td/docs/security/fwsm/fwsm31/configuration/guide/fwsm_cfg/inspct_f.html

IETF TCP/UDP ポート割り当てリスト

Internet Assigned Numbers Authority（IANA）IETF 割り当てポート リスト

http://www.iana.org/assignments/port-numbers

IP テレフォニー設定とポート使用に関するガイド

『Cisco CRS 4.0 (IP IVR and IPCC Express) Port Utilization Guide』

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

『Port Utilization Guide for Cisco ICM/IPCC Enterprise and Hosted Editions』

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html

Cisco Unified Communications Manager Express Security Guide to Best Practices

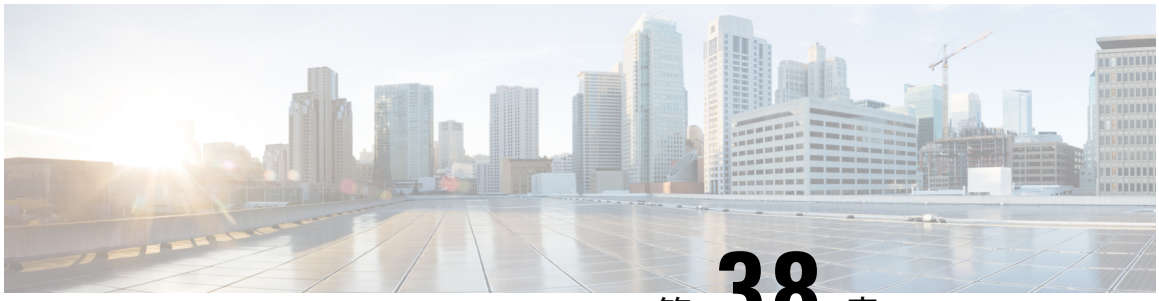
http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e30.html

Cisco Unity Express Security Guide to Best Practices

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e31.html#wp41149

VMware ポート割り当てリスト

vCenter Server、ESX ホストおよびその他のネットワーク コンポーネント管理アクセス用の TCP および UDP ポート



第 38 章

IM and Presence サービスのポートの使用情報

IM and Presence サービス ポートの使用方法の概要

このマニュアルには、IM and Presence Service が、クラスタ内接続用および、外部アプリケーションまたは外部デバイスとの通信用に使用する TCP および UDP ポートの一覧を示します。これは、IP Communications ソリューションの実装時に、ネットワークにファイアウォール、アクセス コントロール リスト（ACL）、および Quality of Service（QoS）を設定するうえで重要な情報となります。

（注） シスコでは、これらのポートで想定されるすべての設定シナリオを検証しているわけではありません。 この一覧を参考にした結果、設定に問題が発生した場合は、シスコのテクニカルサポートにお問い合わせください。

事実上すべてのプロトコルが双方向で行われますが、このマニュアルではセッション開始側から見た方向を記載しています。デフォルトのポート番号は、管理者が手動で変更できる場合もありますが、ベスト プラクティスとしてこのような変更は推奨しません。 IM and Presence Service が内部使用に限って複数のポートを開くことに注意してください。

このドキュメントのポートは、IM and Presence サービスに特別に適用されます。 リリースによってポートが異なる場合があり、今後のリリースで新しくポートが追加される可能性もあります。 このため、インストールされている IM and Presence Service のバージョンに一致する正しいバージョンのマニュアルを使用していることを確認してください。

ファイアウォール、ACL、または QoS の設定内容は、トポロジ、ネットワーク セキュリティ デバイスの配置に対するデバイスとサービスの配置、および使用するアプリケーションとテレ

フォニー拡張機能の種類に応じて異なります。 また、デバイスやバージョンによって、ACL のフォーマットが異なることにも注意してください。

テーブルで照合する情報

この表では、このドキュメントの表のそれぞれに照合する情報を定義します。

表 *40* : 表の内容

表の項目	説明
送信元（From）	ポートに要求を送信するクライアント
移行後	ポートで要求を受信するクライアント
[役割（Role）]	クライアントまたはサーバのアプリケーションまたはプロセス
プロトコル	通信の確立と終了に使用されるセッション層プロトコル、またはトランザクションの要求と応答に使用されるアプリケーション層プロトコルのどちらか。
トランスポートプロトコル	コネクション型（TCP）またはコネクションレス型（UDP）のトランスポート層プロトコル
宛先/リスナー	要求の受信に使用されるポート
ソース/送信元	要求の送信に使用されるポート

IM and Presence サービス ポート リスト

次のテーブルは、IM and Presence サービスがクラスタ内とクラスタ間のトラフィックに使用するポートを示します。

表 *41 : IM and Presence* サービス ポート：*SIP* プロキシの要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
SIP ゲートウェイ ---------- [IM and Presence]	[IM and Presence] ---------- SIP ゲートウェイ	SIP	TCP および UDP	5060	エフェメラル	デフォルトの SIP プロキシの UDP および TCP リスナー

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
SIP ゲートウェイ	[IM and Presence]	SIP	TLS	5061	エフェメラル	TLS サーバ認証のリスナー ポート
[IM and Presence]	[IM and Presence]	SIP	TLS	5062	エフェメラル	TLS 相互認証のリスナー ポート
[IM and Presence]	[IM and Presence]	SIP	UDP/TCP	5049	エフェメラル	内部ポート。 ローカルホスト トラフィック専用。
[IM and Presence]	[IM and Presence]	HTTP	[TCP]	8081	エフェメラル	設定の変更を示す設定のエージェントからの HTTP 要求に使用されます。
サードパーティ製クライアント	[IM and Presence]	HTTP	[TCP]	8082	エフェメラル	デフォルトの IM and Presence HTTPのリスナー。 サードパーティ製クライアントからの接続に使用されます。
サードパーティ製クライアント	[IM and Presence]	HTTPS	TLS/TCP	8083	エフェメラル	デフォルトの IM and Presence HTTPS リスナー。 サードパーティ製クライアントからの接続に使用されます。

表 *42 : IM and Presence* サービス ポート：*Presence* エンジンの要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	IM and Presence（Presence Engine）	SIP	UDP/TCP	5080	エフェメラル	デフォルトの SIP UDP/TCP リスナー ポート

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（Presence Engine）	IM and Presence（Presence Engine）	Livebus	UDP	50000	エフェメラル	内部ポート。 ローカルホスト トラフィック専用。 LiveBus メッセージング ポート。 IM and Presence サービスは、このポートをクラスタ通信に使用します。

表 *43 : IM and Presence* サービス ポート：シスコの *Tomcat WebRequests*

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
ブラウザ	[IM and Presence]	HTTPS	[TCP]	8080	エフェメラル	Web アクセスに使用されます。
ブラウザ	[IM and Presence]	AXL/HTTPS	TLS/TCP	8443	エフェメラル	SOAP によりデータベースおよびサービスアビリティへのアクセスを提供します。
ブラウザ	[IM and Presence]	HTTPS	TLS/TCP	8443	エフェメラル	Web 管理へのアクセスを提供します。
ブラウザ	[IM and Presence]	HTTPS	TLS/TCP	8443	エフェメラル	ユーザ オプション ページへのアクセスを提供します。
ブラウザ	[IM and Presence]	SOAP	TLS/TCP	8443	エフェメラル	SOAP により Cisco Unified Personal Communicator、Cisco Unified Mobility Advantage、およびサードパーティ製の API クライアントへのアクセスを提供します。

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
ブラウザ	[IM and Presence]	HTTPS	[TCP]	9463	エフェメラル	Hypertext Transport Protocol over SSL（HTTPS）では、TLS1.3 の v6 のみが使用できます。

表 *44 : IM and Presence* サービス ポート：外部社内ディレクトリ要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence] --- 外部社内ディレクトリ	外部社内ディレクトリ --- [IM and Presence]	LDAP	[TCP]	389 / 3268	エフェメラル	ディレクトリ プロトコルを外部社内ディレクトリと統合できるようにします。 この LDAP ポートは、統合される社内ディレクトリによって異なります（デフォルトは 389）。 Netscape Directory の場合は、別のポートで LDAP トラフィックを受信するよう設定できます。 認証用に IM&P と LDAP サーバ間の通信を LDAP に許可します。
[IM and Presence]	外部社内ディレクトリ	LDAPS	[TCP]	636	エフェメラル	ディレクトリ プロトコルを外部社内ディレクトリと統合できるようにします。 この LDAP ポートは、統合される社内ディレクトリによって異なります（デフォルトは 636）。

表 *45 : IM and Presence* サービス ポート：リクエストの設定

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（設定エージェント）	IM and Presence（設定エージェント）	[TCP]	[TCP]	8600	エフェメラル	設定エージェントのハートビート ポート

表 *46 : IM and Presence* サービス ポート：*Certificate Manager* の要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	証明書マネージャ	[TCP]	[TCP]	7070	エフェメラル	内部ポート。ローカルホスト トラフィック専用。

表 *47 : IM and Presence* サービス ポート：*IDS*データベースの要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（データベース）	IM and Presence（データベース）	[TCP]	[TCP]	1500	エフェメラル	データベース クライアント用の内部 IDS ポート。 ローカルホスト トラフィック専用。
IM and Presence（データベース）	IM and Presence（データベース）	[TCP]	[TCP]	1501	エフェメラル	内部ポート：アップグレード中に IDS の 2 次インスタンスを始動するための代替ポートです。 ローカルホスト トラフィック専用。
IM and Presence（データベース）	IM and Presence（データベース）	XML	[TCP]	1515	エフェメラル	内部ポート。 ローカルホスト トラフィック専用。 DB レプリケーション ポート。

表 *48 : IM and Presence Service* ポート：*IPSec* マネージャの要求

送信元 送信者	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（IPSec）	IM and Presence（IPSec）	専用	UDP/TCP	8500	8500	内部ポート：ipsec_mgr デーモンがプラットフォーム データ（ホスト）の証明書のクラスタ レプリケーションに使用するクラスタ マネージャ ポートです。

表 *49 : IM and Presence* サービス ポート：*DRF*にマスター エージェント サーバ要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（DRF）	IM and Presence（DRF）	[TCP]	[TCP]	4040	エフェメラル	DRF Master Agent サーバ ポート。Local Agent、GUI、および CLI からの接続を受け入れます。

表 *50 : IM and Presence* サービス ポート：*RISDC* 要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（RIS）	IM and Presence（RIS）	[TCP]	[TCP]	2555	エフェメラル	Real-time Information Services（RIS）データベース サーバ。 クラスタ内の他の RISDC サービスに接続し、クラスタ全体のリアルタイム情報を提供します。

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（RTMT/AMC/SOAP）	IM and Presence（RIS）	[TCP]	[TCP]	2556	エフェメラル	Cisco RIS 向け Real-time Information Services（RIS）データベース クライアント。RIS クライアント接続で、リアルタイム情報を取得できるようにする
IM and Presence（RIS）	IM and Presence（RIS）	[TCP]	[TCP]	8889	8888	内部ポート。 ローカルホスト トラフィック専用。 サービス ステータスの要求および応答用として、RISDC（システム アクセス）が TCP で servM にリンクするために使用します。

表 *51 : IM and Presence* サービス ポート：*SNMP* の要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
SNMP サーバ	[IM and Presence]	SNMP	UDP	161, 8161	エフェメラル	SNMPベースの管理アプリケーションにサービスを提供
[IM and Presence]	[IM and Presence]	SNMP	UDP	6162	エフェメラル	SNMP マスター エージェントから転送される要求を受信するネイティブ SNMP エージェント。
[IM and Presence]	[IM and Presence]	SNMP	UDP	6161	エフェメラル	ネイティブ SNMP エージェントからのトラップ情報を受信し、管理アプリケーションに転送する SNMP マスター エージェント。

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
SNMP サーバ	[IM and Presence]	[TCP]	[TCP]	7999	エフェメラル	CDP Agent が CDP バイナリと通信するためにソケットとして使用します。
[IM and Presence]	[IM and Presence]	[TCP]	[TCP]	7161	エフェメラル	SNMP マスターエージェントとサブエージェント間の通信に使用されます。
[IM and Presence]	SNMP トラップ モニタ	SNMP	UDP	162	エフェメラル	SNMP トラップを管理アプリケーションに送信します。
[IM and Presence]	[IM and Presence]	SNMP	UDP	設定可能	61441	内部 SNMP トラップ レシーバ

表 *52 : IM and Presence* サービス ポート：*Racoon* サーバ要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
ゲートウェイ（Gateway） ---------- [IM and Presence]	[IM and Presence] ---------- ゲートウェイ（Gateway）	Ipsec	UDP	500	エフェメラル	Internet Security Association and the KeyManagement Protocol（ISAKMP）を有効にします。

表 *53 : IM and Presence* サービス ポート：システム サービス要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（RIS）	IM and Presence（RIS）	XML	[TCP]	8888 および 8889	エフェメラル	内部ポート。 ローカルホスト トラフィック専用。 RIS サービス マネージャ（servM）と通信するクライアントを受信するために使用します。

表 *54 : IM and Presence* サービス ポート：*DNS* 要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	DNS サーバ	DNS	UDP	53	エフェメラル	DNS サーバが IM and Presence DNS 照会を受信するポート。 宛先:DNS サーバ|送信元:IM and Presence

表 *55 : IM and Presence* サービス ポート：*SSH/SFTP* 要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	エンドポイント（Endpoint）	SSH/SFTP	[TCP]	22	エフェメラル	多くのアプリケーションが、サーバへのコマンドライン アクセスを行うために使用します。 ノード間で証明書などのファイル交換（sftp）にも使用されます。

表 *56 : IM and Presence* サービスポート *- ICMP* 要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence] ---------- Cisco Unified Communications Manager	Cisco Unified Communications Manager ---------- [IM and Presence]	ICMP	IP	該当なし	エフェメラル	インターネット制御メッセージ プロトコル（ICMP）。 Cisco Unified Communications Manager サーバとの通信に使用されます。

表 *57 : IM and Presence* サービス ポート：*NTP* 要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	NTP サーバ（NTP Server）	NTP	UDP	123	エフェメラル	Cisco Unified Communications Manager は NTP サーバとして動作します。サブスクライバ ノードが、パブリッシャ ノードと時刻を同期するために使用されます。

表 *58 : IM and Presence* サービス ポート：*Microsoft Exchange* 通知要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
Microsoft Exchange	[IM and Presence]	HTTP（HTTPu）	) WebDAV：HTTP /UDP/IP 通知 2) EWS - HTTP/TCP/IP SOAP 通知	IM and Presence サーバ ポート（デフォルト 50020）	エフェメラル	Microsoft Exchange は、このポートを使用してカレンダー イベントの特定のサブスクリプション識別子に対する変更を示す通知（NOTIFY メッセージによって示される）を送信します。 ネットワーク構成内にある Exchange サーバと統合する場合に使用されます。 どちらのポートも作成されます。 送信されるメッセージの種類は、設定するカレンダー プレゼンス バックエンド ゲートウェイのタイプによって異なります。

表 *59 : IM and Presence* サービス ポート：*SOAP* サービス リクエスト

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（Tomcat）	IM and Presence（SOAP）	[TCP]	[TCP]	5007	エフェメラル	SOAP モニタ ポート

表 *60 : IM and Presence* サービス ポート：*AMC RMI* 要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	RTMT	[TCP]	[TCP]	1090	エフェメラル	AMC RMI オブジェクト ポート RTMT パフォーマンス モニタ、データ収集、ロギング、およびアラート生成用の Cisco AMC サービス。
[IM and Presence]	RTMT	[TCP]	[TCP]	1099	エフェメラル	AMC RMI レジストリ ポート RTMT パフォーマンス モニタ、データ収集、ロギング、およびアラート生成用の Cisco AMC サービス。

表 *61 : IM and Presence* サービスポート *- XCP* 要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
XMPP クライアント	[IM and Presence]	[TCP]	[TCP]	5222	エフェメラル	クライアント アクセス ポート
[IM and Presence]	[IM and Presence]	[TCP]	[TCP]	5269	エフェメラル	サーバ間接続（S2S）ポート
サードパーティ製 BOSH クライアント	[IM and Presence]	[TCP]	[TCP]	7335	エフェメラル	XCP Web Connection Manager が、BOSH を使用するサードパーティ製 API との接続に使用する HTTP リスニング ポート

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（XCP サービス）	IM and Presence（XCP ルータ	[TCP]	[TCP]	7400	エフェメラル	XCP ルータ マスター アクセス ポート。 オープン ポート設定からルータに接続する XCP サービス（XCP 認証コンポーネント サービスなど）は、通常このポートを使用して接続します。
IM and Presence（XCP ルータ	IM and Presence（XCP ルータ	UDP	UDP	5353	エフェメラル	MDNS ポート。 クラスタ内の XCP ルータはこのポートを使用してお互いを検出します。
IM and Presence（XCP ルータ	IM and Presence（XCP ルータ	[TCP]	[TCP]	7336	HTTPS	MFT ファイル転送（オンプレミスのみ）。

表 *62 : IM and Presence* サービスポート：外部データベースのリクエスト

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	PostgreSQL データベース	[TCP]	[TCP]	5432 [1]	エフェメラル	PostgreSQL データベース リスニング ポート
[IM and Presence]	Oracle データベース	[TCP]	[TCP]	1521	エフェメラル	Oracle データベース リスニング ポート
IM and Presenc	MSSQL database	[TCP]	[TCP]	1433	エフェメラル	MSSQL データベース リスニング ポート

[1] これがデフォルトのポートですが、任意のポートで受信するよう PostgreSQL データベースを設定できます。

表 *63 : IM and Presence* サービス ポート：高可用性の要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（Server Recovery Manager）	IM and Presence（Server Recovery Manager）	[TCP]	[TCP]	20075	エフェメラル	Cisco Server Recovery Manager が管理 RPC 要求を行うために使用するポート。
IM and Presence（Server Recovery Manager）	IM and Presence（Server Recovery Manager）	UDP	UDP	21999	エフェメラル	Cisco Server Recovery Manager がピアとの通信に使用するポート。

表 *64 : IM and Presence* サービス ポート：*In Memory* データベース レプリケーションのメッセージ

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	[IM and Presence]	専用	[TCP]	6603*	エフェメラル	Cisco Presence Datastore
[IM and Presence]	[IM and Presence]	専用	[TCP]	6604*	エフェメラル	Cisco Login Datastore
[IM and Presence]	[IM and Presence]	専用	[TCP]	6605*	エフェメラル	Cisco SIP Registration Datastore
[IM and Presence]	[IM and Presence]	専用	[TCP]	9003	エフェメラル	Cisco Presence Datastore デュアル ノード プレゼンス冗長グループの複製。
[IM and Presence]	[IM and Presence]	専用	[TCP]	9004	エフェメラル	Cisco Login Datastore デュアル ノード プレゼンス 冗長グループの複製。
[IM and Presence]	[IM and Presence]	専用	[TCP]	9005	エフェメラル	Cisco SIP Registration Datastore デュアル ノード プレゼンス冗長グループの複製。

* 管理 CLI 診断ユーティリティを実行するには、`utils imdb_replication status` コマンドを使用します。これらのポートは、クラスタの IM and Presence Service ノード間で設定されているすべてのファイアウォールでオープンである必要があります。 このセットアップは、通常の運用では必要ありません。

表 *65 : IM and Presence* サービス ポート：*In Memory* データベース *SQL* メッセージ

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	[IM and Presence]	専用	[TCP]	6603	エフェメラル	Cisco Presence Datastore SQL クエリ。
[IM and Presence]	[IM and Presence]	専用	[TCP]	6604	エフェメラル	Cisco Login Datastore SQL クエリ。
[IM and Presence]	[IM and Presence]	専用	[TCP]	6605	エフェメラル	Cisco SIP Registration Datastore SQL クエリ。
[IM and Presence]	[IM and Presence]	専用	[TCP]	6606	エフェメラル	Cisco Route Datastore SQL クエリ。

表 *66 : IM and Presence* サービス ポート：*In Memory* データベースの通知メッセージ

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
[IM and Presence]	[IM and Presence]	専用	[TCP]	6607	エフェメラル	Cisco Presence Datastore XML ベースの変更通知。
[IM and Presence]	[IM and Presence]	専用	[TCP]	6608	エフェメラル	Cisco Login Datastore XML ベースの変更通知。
[IM and Presence]	[IM and Presence]	専用	[TCP]	6609	エフェメラル	Cisco SIP Registration Datastore XML ベースの変更通知。
[IM and Presence]	[IM and Presence]	専用	[TCP]	6610	エフェメラル	Cisco Route Datastore XML ベースの変更通知。

表 *67 : IM and Presence Service* ポート *:* 強制手動同期*/X.509* 証明書更新要求

送信元（送信者）	送信先（リスナー）	プロトコル	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（Intercluster Sync Agent）	IM and Presence（Intercluster Sync Agent）	[TCP]	[TCP]	37239	エフェメラル	Cisco Intercluster Sync Agent サービスは、このポートを使用してコマンドを処理するためのソケット接続を確立します。

表 *68 : IM and Presence* サービス ポート：*ICMP* 要求

送信元（送信者）	送信先（リスナー）	宛先ポート（**Destination Port**）	目的
エンドポイント/IM and Presence	[IM and Presence]	7	Internet Contr Protocol（ICM トコル番号が ラフィックを 列見出しに示 となるもので
[IM and Presence]	エンドポイント/IM and Presence		

表 *69 : IM and Presence* に使用されるポート *- Cisco Unified CM* コミュニケーションおよび *IM and Presence* の発行者 *-* サブスクライバコミュニケーション

送信元（送信者）	送信先（リスナー）	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
Cisco Unified Communications Manager	IM and Presence パブリッシャ	[TCP]	1500	双方向	データベース クライアント用の内部 ID ポート。ローカルホスト トラフィック専用。
Cisco Unified Communications Manager	IM and Presence パブリッシャ	[TCP]	8443	双方向	Web 管理へのアクセスを提供します。
Cisco Unified Communications Manager	IM and Presence パブリッシャ	[TCP]	1090	双方向	AMC RMI オブジェクト ポート RTMT パフォーマンス モニタ、データ収集、ロギング、およびアラート生成用の Cisco AMC サービス。

送信元（送信者）	送信先（リスナー）	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
Cisco Unified Communications Manager	IM and Presence パブリッシャ	[TCP]	2555	双方向	Bi-directional Real-time Information Services（RIS）データベースサーバ。クラスタ内の他の RISDC サービスに接続し、クラスタ全体のリアルタイム情報を提供します。
Cisco Unified Communications Manager	IM and Presence パブリッシャ	[TCP]	8500	双方向	内部ポート：ipsec_mgr デーモンがプラットフォームデータ（ホスト）の証明書のクラスタレプリケーションに使用するクラスタマネージャポートです。
Cisco Unified Communications Manager	IM and Presence パブリッシャ	[TCP]	8600	双方向	設定エージェントのハートビート ポート
Cisco Unified Communications Manager	IM and Presence パブリッシャ	UDP	123	双方向	時間同期に使用されるネットワークタイムプロトコル（NTP）。
IM and Presence パブリッシャ	IM and Presence サブスクライバ	UDP	50000	双方向	内部ポート。ローカルホストトラフィック専用。LiveBus メッセージングポート。 IM and Presence サービスは、このポートをクラスタ通信に使用します。
IM and Presence パブリッシャ	IM and Presence サブスクライバ	UDP	21999	双方向	Cisco Server Recovery Manager がピアとの通信に使用するポート。
IM and Presence パブリッシャ	Cisco Unified Communications Manager	[TCP]	4040	双方向	DRF マスター エージェント サーバ ポートは、ローカルエージェントの GUI および CLI からの接続を受け入れます。

送信元（送信者）	送信先（リスナー）	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence パブリッシャ	Cisco Unified Communications Manager	[TCP]	8001	双方向	永続チャットの構成中に使用されます。
IM and Presence パブリッシャ	Cisco Unified Communications Manager	[TCP]	6379	双方向	マネージドファイル転送（MFT）の構成時に使用されます。
IM and Presence パブリッシャ	IM and Presence サブスクライバ	[TCP]	7	双方向	外部データベース（MSSQL）の構成中に使用されます。
IM and Presence パブリッシャ	IM and Presence サブスクライバ	[TCP]	20075	双方向	Cisco Server Recovery Manager が管理 RPC 要求を行うために使用するポート。
IM and Presence パブリッシャ	IM and Presence サブスクライバ	[TCP]	8600	双方向	設定エージェントのハートビート ポート
IM and Presence サブスクライバ	IM and Presence パブリッシャ	[TCP]	9005	双方向	Cisco SIP Registration Datastore デュアル ノード プレゼンス冗長グループの複製。
IM and Presence サブスクライバ	IM and Presence パブリッシャ	[TCP]	9003	双方向	Cisco Presence Datastore デュアル ノード プレゼンス冗長グループの複製。
IM and Presence サブスクライバ	IM and Presence パブリッシャ	[TCP]	20075	双方向	Cisco Server Recovery Manager が管理 RPC 要求を行うために使用するポート。
IM and Presence サブスクライバ	IM and Presence パブリッシャ	[TCP]	9004	双方向	Cisco Login Datastore デュアル ノード プレゼンス冗長グループの複製。
Cisco Unified Communications Manager	IM and Presence パブリッシャ	[TCP]	5070	双方向	コール設定で使用されます

送信元（送信者）	送信先（リスナー）	トランスポートプロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence パブリッシャ	IM and Presence サブスクライバ	[TCP]	44000	双方向	コール設定で使用されます

表 *70 : On-a-call_Presence*

送信元（送信者）	送信先（リスナー）	送信元ポート（**Source Port**）	宛先ポート（**Destination Port**）	プロトコル	備考
Cisco Unified Communications Manager	IM and Presence パブリッシャ	[37240 – 61000]	5070	[TCP]	
IM and Presence パブリッシャ	XMPP クライアント（Jabber）	5222	64846	[TCP]	クライアントアクセスポート
IM and Presence パブリッシャ	XMPP クライアント（Jabber）	5222	56361	[TCP]	クライアントアクセスポート

表 *71 : MS-SQL DB* の設定

送信元（送信者）	送信先（リスナー）	送信元ポート（**Source Port**）	宛先ポート（**Destination Port**）	プロトコル
IM and Presence パブリッシャ	データベース	[37240 – 61000]	7	[TCP]

表 *72 : MS-SQL* 持続チャットの設定

送信元（送信者）	送信先（リスナー）	送信元ポート（**Source Port**）	宛先ポート（**Destination Port**）	プロトコル
IM and Presence パブリッシャ	データベース	37240 – 61000	1433	[TCP]

表 *73 :* マネージドファイル転送（*MFT*）

送信元（送信者）	送信先（リスナー）	送信元ポート（**Source Port**）	宛先ポート（**Destination Port**）	プロトコル
IM and Presence パブリッシャ	外部ファイル サーバ	37240 – 61000	7	[TCP]
IM and Presence パブリッシャ	外部ファイル サーバ	37240 – 61000	22	[TCP]
IM and Presence パブリッシャ	外部ファイル サーバ	37240 – 61000	5432	[TCP]
IM and Presence パブリッシャ	データベース	54288 - 54292	5432	[TCP]

SNMP については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

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