



ボイスメールおよびメッセージング向けの Cisco Unity Connection の設定

- [Cisco Unity Connection, 1 ページ](#)
- [Cisco Unity Connection のボイスメールとメッセージング設定タスク フロー, 3 ページ](#)

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 Unified Communications Manager に統合された Cisco Unity Connection（ボイスメールとメッセージングのシステム）は、AXL サービスまたはLDAP 統合を介して、手動で設定したユーザにボイスメッセージング機能を提供します。ユーザが、メールボックスでボイスメッセージを受信すると、ユーザの電話機のメッセージ待機ランプが点灯します。ユーザは、内部または外部コールでボイスメッセージングシステムにアクセスして、メッセージの取得、再生、応答、転送、削除ができます。

このシステムは直接接続とゲートウェイベースの両方をサポートするメッセージングシステムです。直接接続のボイスメッセージングシステムは、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ングシステムは、アナログまたはデジタルトランク経由で Cisco ゲートウェイに接続することにより 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 は、コール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）。
- 識別されているユーザのメッセージング（Cisco Unity Connection は、転送された内線コール中にメッセージを残したユーザを、コール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 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。従来の統合に必要な複数の SCCP ポートの代わりに、SIP は、各 Unity Connection サーバに1つのトランクを使用します。SIP の統合により、ボイスメールポートとボイスメールメッセージ待機インジケータ（MWI）に電話番号を設定する必要がなくなります。
- SCCP プロトコル：ボイスメールポートを作成して、直接接続するボイスメッセージングシステムとのインターフェイスを設定します。この方法により、Unified Communications Manager と Cisco Unity Connection との間のリンクが確立します。

ボイスメッセージングシステムに複数かつ同時に接続するコールを処理するためには、複数のボイスメールポートを作成して、そのポートを、回線グループおよびルート/ハントリスト内の回線グループに設定します。

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、メッセージ待機ランプの点滅設定のある番号をコールして、メッセージ待機インジケータ（MWI）を送信します。

ボイスメールポートおよび Cisco Unity SCCP デバイスのセキュリティ設定を行うと、各デバイスが他のデバイスの証明書を受け入れた後、認証済みのデバイス間で TLS 接続（ハンドシェイク）が開始されます。また、システムは、デバイス間で SRTP ストリームを送受信できるようにします。これは、デバイスに暗号化設定を行った場合の動作です。

デバイスのセキュリティモードに認証または暗号化を設定すると、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。

システムに Cisco Unity Connection を統合する設定の詳細については、<http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html> で、『Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection』または『Cisco Unified Communications Manager SIP Trunk Integration Guide for Cisco Unity Connection』を参照してください。

Cisco Unity Connection のボイスメールとメッセージング 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	Cisco Unity Connection で、ボイスメールとメッセージングを設定します。	Cisco Unity Connection を設定するには、Cisco Unity Connection 向け『Cisco Unified Communications Manager SCCP Integration Guide』または『Cisco Unified Communications Manager SIP Trunk Integration Guide for Cisco Unity Connection』を参照してください。 http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html
ステップ 2	PIN 同期の有効化 、(3 ページ)	これはオプションです。共通の PIN 同期を有効にするには、次の手順を使用します。

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 パブリッシュ データベース サーバが稼働し、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。Failed to update PIN on CUCM.Reason: Error getting the pin.



- (注) PIN の同期が有効で、エンドユーザが PIN を変更した場合は、Cisco Unified Communications Manager で PIN が更新されます。これは、設定済みの Unity Connection アプリケーション サーバの 1 台以上で PIN の更新に成功した場合のみです。

はじめる前に

この手順は、アプリケーション サーバを Cisco Unity Connection の設定にすでに接続していることを前提としています。接続していない場合は、新しいアプリケーション サーバの追加方法の詳細について、以下の「関連項目」のセクションを参照してください。

PIN 同期の機能を有効にするには、最初に、Cisco Unity Server に接続するための有効な証明書を Cisco Unified OS の管理ページから Cisco Unified Communications Manager の tomcat-trust に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』の「“Manage Security Certificates”」の章を参照してください。 <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>

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 の管理から、[システム (System)] > [アプリケーション サーバ (Application Servers)] の順に選択します。
 - ステップ 2 Cisco Unity Connection の設定を行うアプリケーション 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](#)