



## Cisco Unity Connection の Cisco Unified Communications Manager SIP 統合ガイドのリリース 14

最終更新：2024 年 9 月 5 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/>





## 目次

---

### 第 1 章

#### 統合の説明 1

- 統合の説明 1
- はじめに 1
- 統合機能 1
- 複数の電話システムとの連動 2
- 集中型ボイスメッセージ 2

---

### 第 2 章

#### Cisco Unity Connection でボイスメッセージングポートを計画する 3

- Cisco Unity Connection でボイスメッセージングポートを計画する 3
  - ポート設定を計画する 3
  - ボイスメッセージングポート数を決定する 4
    - インストールするボイスメッセージングポート 4
    - コールに応答するボイスメッセージングポート 5
    - 発信するボイスメッセージングポート 5
  - Unity Connection クラスタに関する考慮事項 6
    - 両方の Unity Connection サーバーが機能している場合 6
    - 1つの Unity Connection サーバーのみが機能している場合 7

---

### 第 3 章

#### Cisco Unified Communications Manager SIP トランク統合を設定する 9

- 前提条件 10
- セキュア SIP コールで Tomcat 証明書を使用する 14
- 統合タスク 14
- SIP トランク セキュリティ プロファイルを作成する 16
- SIP プロファイルを作成する 18

SIP トランクを作成する	18
ルートパターンを作成する	21
ルートグループを作成する	22
ルートリストを作成する	22
ボイスメールパイロットを作成する	23
ボイスメールプロファイルを設定する	24
ボイスメールサーバーのサービスパラメータを設定する	25
(オプション) SIP ダイジェスト認証を設定する	26
(オプション) アプリケーションユーザーを作成する	26
(オプション) AXL サーバーを設定する	28
Cisco Unity Connection の統合を設定する	30
統合を作成する	31
Next Generation Security Over SIP 統合を有効にする	39
証明書を生成、アップロードする	39
RSA キーベースの証明書を設定する	39
EC キーベースの証明書を設定する	41
セキュリティモードを設定する	43
TLS 暗号の設定	44
SRTP 暗号の設定	46

---

**第 4 章**

<b>統合をテストする</b>	<b>49</b>
テレフォニー統合をテストする	49
テスト設定をセットアップする	50
リリース転送を使用した外線コールをテストする	51
メッセージを再生する	52
管理された転送を設定する	52
管理された転送をテストする	53
テストユーザーを削除する	53
Cisco Unified CM の認証と暗号化をテストする	54

## 付録 A :

**Cisco Unified Communications Manager 統合へ Cisco Unified Communications Manager Express を追加する 55**

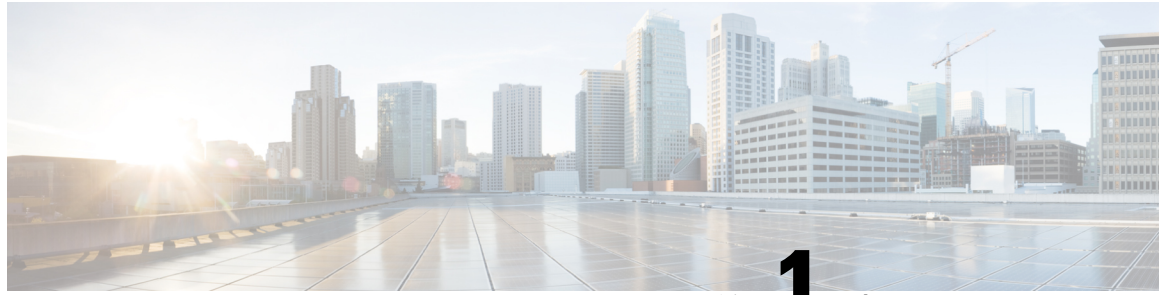
Cisco Unified Communications Manager 統合へ Cisco Unified Communications Manager Express を追加する 55

Cisco Unified CM 電話システム統合へ Cisco Unified CM Express サーバーを追加する 56

Cisco Unified Survivable Remote Site Telephony (SRST) ルータを使用する 57

AAR を経由したルーティングされたボイスメールコールにおける RDNIS の送信不能の影響 58





# 第 1 章

## 統合の説明

---

- [統合の説明 \(1 ページ\)](#)

### 統合の説明

#### はじめに

SIP トランク統合は、SIP プロトコルを使用して Unity Connection と Cisco Unified CM 間の通信を確立する方法です。

SIP トランクを介して Cisco Unity Connection と統合できる Cisco Unified CM のサポート対象バージョンのリストについては、<http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-device-support-tables-list.html>にある『Cisco Unity Connection の互換性マトリクス』を参照してください。

#### 統合機能

Cisco Unity Connection と Cisco Unified CM SIP トランクの統合は、次の機能を提供します。

- 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（ユーザーは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ーを識別します。パスワードが必要になる場合があります）
- 識別されたユーザーのメッセージ（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ーを、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）

## 複数の電話システムとの連動

Unity Connection は、同時に 2 つ以上の電話システムと連動できます。サポートされる最大の組み合わせと、Unity Connection を複数の電話システムと連動させる手順については、[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/15/integration/multiple/b\\_cuc15intmultiple.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/integration/multiple/b_cuc15intmultiple.html)にある『Cisco Unity Connection 複数電話システム統合ガイドリリース 15』を参照してください。

## 集中型ボイスメッセージ

Cisco Unity Connection は、電話システムを使用した集中型ボイスメッセージをサポートしており、Avaya DCS、Nortel MCDN、Siemens CorNet などの専用プロトコルや、QSIG または DPNSS などの規格ベースのプロトコルなど、さまざまな電話システム間ネットワークプロトコルをサポートしています。集中型ボイスメッセージは電話システムとそのインターフォンシステムネットワークの機能であり、ボイスメールではないことに注意してください。Unity Connection では、電話システムとそのインターフォンシステム ネットワーキングが正しく設定されている場合に、集中型ボイスメッセージをサポートします。詳細については、[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/15/design/guide/b\\_15cucdg.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/design/guide/b_15cucdg.html)にある『Cisco Unity Connection 設計ガイド、リリース 15』の「Cisco Unity Connection を電話システムに統合する」の章の「集中型ボイスメッセージ」の項を参照してください。





## 第 2 章

# Cisco Unity Connection でボイスメッセージングポートを計画する

- [Cisco Unity Connection でボイスメッセージングポートを計画する \(3 ページ\)](#)

## Cisco Unity Connection でボイスメッセージングポートを計画する

### ポート設定を計画する

電話システムをプログラミングする前に、Cisco Unity Connection によるボイスメッセージポートの使用方法を計画する必要があります。次の考慮事項は、電話システムのプログラミングに影響します（たとえば、ボイスメッセージポートのハントグループまたはコール転送の設定）。

- インストールされているボイスメッセージポートの数。

Unity Connection クラスタの場合、各 Unity Connection サーバーは、他のサーバーが機能しなくなった場合に備えて、すべてのボイスメッセージトラフィックを処理するのに十分なポートを持つ必要があります。

- コールに応答するボイスメッセージポートの数。
- たとえば、メッセージ通知の送信、メッセージ受信インジケータ（MWI）の設定、電話の録音および再生（TRAP）接続を行うためにダイヤルアウトするだけのボイスメッセージポートの数。

次の表では、Cisco Unity Connection Administration の [テレフォニー統合（Telephony Integrations）] > [ポート（Port）] で設定できる Unity Connection のボイスメッセージポート設定について説明します。

表 1:ボイスメッセージポートの設定

フィールド	説明
有効 (Enabled)	このチェックボックスをオンにします。
サーバー (Server)	(Unity Connection クラスタが設定されている場合) このポートを処理する Unity Connection サーバーの名前を選択します。  ボイスメッセージトラフィックを均等に共有するように、同じ数の応答およびダイヤルアウトボイスメッセージングポートを Unity Connection サーバーに割り当てます。
コールに回答 (Answer Calls)	このチェックボックスをオンにします。  Cisco Unified CM サーバーに接続するすべてのボイスメッセージポートで、[コールに回答 (Answer Calls)] チェックボックスをオンにする必要があります。そうしないと、Unity Connection へのコールに回答できない場合があります。
メッセージ通知を実行する (Perform Message Notification)	ポートをユーザーに対するメッセージ通知用に指定するには、このチェックボックスをオンにします。
MWI リクエストを送信する (Send MWI Requests)	ポートでの MWI のオン/オフを指定するには、このチェックボックスをオンにします。
TRAP接続を許可する (Allow TRAP Connections)	このチェックボックスをオンにすると、ユーザーは Cisco Unity Connection の web アプリケーションで電話から録音または再生用のポートを使用できます。

## ボイスメッセージングポート数を決定する

次のタスクでは、Cisco Unity Connection がインストールし、コールに回答し、コールをダイヤルアウトするためのボイスメッセージングポートの数を決定するプロセスについて説明します。

### インストールするボイスメッセージングポート

インストールするボイスメッセージングポートの数は、次のようなさまざまな要因によって異なります。

- コールトラフィックがピークのときに Unity Connection が応答するコールの数。
- 発信者が録音し、ユーザーが聞く各メッセージの予想される長さ。
- ユーザーの数。
- ダイヤルアウト専用設定されているポートの数。

- メッセージ通知のために発信されたコールの数。
- コールトラフィックがピークのときにアクティブ化される MWI の数。
- コールトラフィックがピークのときに必要な TRAP 接続の数。（TRAP 接続は、電話で再生および録音するために Unity Connection Web アプリケーションによって使用されます。）
- コールトラフィックがピークのときに自動アテンダントとコールハンドラを使用するコールの数。
- Unity Connection クラスタが設定されているかどうか。考慮事項については、[Unity Connection クラスタに関する考慮事項](#)のセクションを参照してください。

システムリソースが未使用のポートに割り当てられないように、必要な数のボイスメッセージポートだけをインストールすることをお勧めします。

## コールに回答するボイスメッセージングポート

ボイスメッセージポートが回答するコールは、身元不明発信者またはユーザーからの着信コールである可能性があります。通常、コールに回答するボイスメッセージポートが最もビジーです。

ボイスメッセージポートは、コールへの応答とダイヤルアウト（メッセージ通知の送信など）の両方に設定できます。ただし、ボイスメッセージポートが複数の機能を実行し、非常にアクティブな場合（多数のコールへの応答など）、ボイスメッセージポートが解放されるまで他の機能が遅延することがあります（たとえば、応答するコールが少なくなります）。最適なパフォーマンスを得るには、特定のボイスメッセージポートを着信コールの応答専用にし、他のポートをダイヤルアウト専用にします。これらのポート機能を分離することで、Unity Connection がダイヤルアウトのためにポートをオフフックにするのと同時に、着信コールがポートに着信するという衝突の可能性を排除します。

システムが Unity Connection クラスタ用に設定されている場合は、[Unity Connection クラスタに関する考慮事項](#)を参照してください。

## 発信するボイスメッセージングポート

ダイヤルアウトのみを行い、コールに回答しないポートは、次の 1 つ以上を実行できます。

- 着信メッセージを電話、ポケットベル、または電子メールでユーザーに通知します。
- ユーザー内線の MWI をオンまたはオフにします。
- ユーザーが Unity Connection Web アプリケーションで電話機を録音および再生デバイスとして使用できるように、TRAP 接続を確立します。

通常、これらのボイスメッセージポートは、最もビジーでないポートです。

システムが Cisco Unity Connection クラスタ用に設定されている場合は、[Unity Connection クラスタに関する考慮事項](#)を参照してください。



**注意** 電話システムのプログラミングでは、コールに回答できない Cisco Unity Connection のボイスメッセージポート ([コールに回答 (Answer Calls)] に設定されていないボイスメッセージポート) にコールを送信しないでください。たとえば、ボイスメッセージポートが [MWI 要求の送信 (Send MWI Requests)] だけに設定されている場合は、そのポートにコールを送信しないでください。

## Unity Connection クラスタに関する考慮事項

システムが Unity Connection クラスタ用に設定されている場合は、要件が次のシナリオでどのように変わるかを検討してください。

### 両方の Unity Connection サーバーが機能している場合

- ハントグループは、最初にサブスクリバサーバーに着信コールを送信し、サブスクリバサーバーで応答ポートが使用できない場合はパブリッシャサーバーに送信するように設定されます。
- 両方の Unity Connection サーバーがアクティブで、システムのボイスメッセージトラフィックを処理します。
- Cisco Unity Connection Administration では、各 Unity Connection サーバーに同じ数のボイスメッセージポートが割り当てられるように、ボイスメッセージポートが設定されます。このガイドでは、適切なタイミングでボイスメッセージポートを特定のサーバーに割り当てるように指示します。
- 1 つの Unity Connection サーバーに割り当てられるボイスメッセージポートの数は、他の Unity Connection サーバーが機能を停止したときに、システムのすべてのボイスメッセージトラフィック (コールへの応答とダイヤルアウト) を処理するのに十分な数である必要があります。

ボイスメッセージトラフィックを処理するために両方の Unity Connection サーバーが機能している必要がある場合、一方のサーバーが機能を停止すると、システムのキャパシティが不足します。

- 各 Unity Connection サーバーには、ボイスメッセージポートの総数の半分が割り当てられます。

すべてのボイスメッセージポートが 1 つの Unity Connection サーバーに割り当てられている場合、他の Unity Connection サーバーはコールに回答したり、ダイヤルアウトしたりできません。

- 各 Unity Connection サーバーには、コールに回答し、(たとえば、MWI を設定するために) ダイヤルできるボイスメッセージポートが必要です。

## 1 つの Unity Connection サーバーのみが機能している場合

- 電話システムのハントグループは、機能している Unity Connection サーバーにすべてのコールを送信します。
- 機能している Unity Connection サーバーは、システムのすべてのボイスメッセージングトラフィックを受信します。
- 機能している Unity Connection サーバーに割り当てられるボイスメッセージポートの数は、システムのすべてのボイスメッセージトラフィック（コールへの応答およびダイヤルアウト）を処理するのに十分な数である必要があります。
- 機能している Unity Connection サーバーには、コールに応答し、（たとえば、MWI を設定するために）ダイヤルできるボイスメッセージポートが必要です。

機能している Unity Connection サーバーに、コールに応答するためのボイスメッセージポートがない場合、システムは着信コールに応答できません。同様に、機能している Unity Connection サーバーにダイヤルアウト用のボイスメッセージポートがない場合、システムはダイヤルできません（たとえば、MWI の設定）。

1つの Unity Connection サーバーのみが機能している場合



## 第 3 章

# Cisco Unified Communications Manager SIP トランク統合を設定する

この章では、Cisco Unified Communications Manager SIP トランクと Cisco Unity Connection の統合を設定する手順について説明します。このドキュメントは、Unity Connection が Cisco Unified CM と同じサーバー上に Cisco Business Edition としてインストールされている設定には適用されません。



(注) 分散型電話システムのトランク間で MWI リレーを設定する場合は、Cisco Unified CM のマニュアルで要件と手順を確認する必要があります。トランク間での MWI リレーの設定には、Unity Connection の設定は含まれません。

Cisco Unified CM SIP トランク統合の監視転送中は、Cisco Unified CM 保留音 (MOH) 機能を使用できません。

- [前提条件 \(10 ページ\)](#)
- [セキュア SIP コールで Tomcat 証明書を使用する \(14 ページ\)](#)
- [統合タスク \(14 ページ\)](#)
- [SIP トランク セキュリティ プロファイルを作成する \(16 ページ\)](#)
- [SIP プロファイルを作成する \(18 ページ\)](#)
- [SIP トランクを作成する \(18 ページ\)](#)
- [ルートパターンを作成する \(21 ページ\)](#)
- [ルートグループを作成する \(22 ページ\)](#)
- [ルートリストを作成する \(22 ページ\)](#)
- [ボイスメールパイロットを作成する \(23 ページ\)](#)
- [ボイスメールプロファイルを設定する \(24 ページ\)](#)
- [ボイスメールサーバーのサービスパラメータを設定する \(25 ページ\)](#)
- [\(オプション\) SIP ダイジェスト認証を設定する \(26 ページ\)](#)
- [\(オプション\) アプリケーションユーザーを作成する \(26 ページ\)](#)
- [\(オプション\) AXL サーバーを設定する \(28 ページ\)](#)
- [Cisco Unity Connection の統合を設定する \(30 ページ\)](#)

- [Next Generation Security Over SIP 統合を有効にする \(39 ページ\)](#)

## 前提条件

Cisco Unified CM と Unity Connection 間の SIP 統合を開始する前に、実行するタスクと統合に必要なコンポーネントを理解する必要があります。次の表に、統合を成功させるために考慮する必要がある前提条件のリストを示します。

前提条件	特記事項
該当するバージョンの Cisco Unified CM をインストールします。	<ul style="list-style-type: none"> <li>• Cisco Unified CM の互換性のあるバージョンについては、<a href="http://www.cisco.com/c/en/us/unified-communications/unity-connection/products-device-support-tables-list.html">http://www.cisco.com/c/en/us/unified-communications/unity-connection/products-device-support-tables-list.html</a> にある『リクス : Cisco Unity Connection』を参照してください。</li> </ul>
該当する数のボイスメッセージングポートを有効にするライセンスを使用して、該当するバージョンの Unity Connection をインストールします。	<ul style="list-style-type: none"> <li>• Unity Connection の互換性のあるバージョンの詳細については、<a href="http://www.cisco.com/c/en/us/unified-communications/unity-connection/products-device-support-tables-list.html">http://www.cisco.com/c/en/us/unified-communications/unity-connection/products-device-support-tables-list.html</a> にある『Unity Connection の互換性マトリクス』を参照してください。</li> <li>• インストールタスクの詳細については、<a href="https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/install_upgrade/guide/b_15.html">https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/install_upgrade/guide/b_15.html</a> にある『Cisco Unity Connection のインストール、アップグレード、およびメンテナンス リリース 15』の「Cisco Unity Connection をインストールする」の章を参照してください。</li> </ul>



<p>SCCP 統合でサポートされている電話システムは次のとおりです。</p> <ul style="list-style-type: none"><li>• Cisco Unified CM 拡張の IP 電話のみ。</li><li>• Cisco Unified CM の内線番号用の IP 電話と SIP 電話の両方 (Cisco Unified CM サーバーにメディアターミネーションポイント (MTP) はなし)。</li></ul>	<ul style="list-style-type: none"><li>• 該当する電話機をネットワークに接続する各場所の LAN 接続が必要です。</li><li>• Cisco Unified CM クラスタが複数ある場合に、ユーザーがトランクアクセスコーフィックスをダイヤルすることなく、別の Cisco Unified CM クラスタの内線番号きる機能。</li></ul>
---	---



Unity Connection が IPv6 またはデュアルモード (IPv4 および IPv6) を使用して Cisco Unified CM と通信する場合は、次のサブタスクを実行します。

1. Unity Connection サーバーで IPv6 を有効にします。
2. Cisco Unity Connection Administration の [システム設定 (System Settings) ] > [一般設定 (General Configuration) ] ページで、Unity Connection が着信トラフィックをリッスンする場所を制御する IP アドレスングモードのオプションを選択します。 [IPv4]、 [IPv6]、または [IPv4 および IPv6 (IPv4 and IPv6) ] を

選択できません。設定のデフォルトは [IPv4] です。

## セキュア SIP コールで Tomcat 証明書を使用する

Cisco Unity Connection は、SIP 証明書の代わりにセキュアコールを設定するために、RSA キーベースの Tomcat 証明書の使用をサポートしています。これにより、SIP セキュアコールに自己署名証明書とサードパーティ CA 署名証明書の両方を使用できます。

## 統合タスク

SIP トランクを介してスタンドアロンモードまたはクラスタモードで Cisco Unified CM と Unity Connection を統合するには、次の表に示すタスクを実行します。

表 2: 統合タスク

統合のシナリオ	統合タスク
Cisco Unified CM と Unity Connection との統合 (スタンドアロン)	<ul style="list-style-type: none"> <li>• <a href="#">Cisco Unity Connection</a> でボイスメッセージングポートを計画する (3 ページ)</li> <li>• 統合に向けて Cisco Unified CM を設定する <ul style="list-style-type: none"> <li>• <a href="#">SIP トランク セキュリティ プロファイル</a> を作成する</li> <li>• <a href="#">SIP プロファイル</a> を作成する</li> <li>• <a href="#">SIP トランク</a> を作成する</li> <li>• <a href="#">ルートパターン</a> を作成する</li> <li>• <a href="#">ボイスメールパイロット</a> を作成する</li> <li>• <a href="#">ボイスメールプロファイル</a> を設定する</li> <li>• <a href="#">ボイスメールサーバーのサービスパラメータ</a> を設定する</li> </ul> </li> <li>• <a href="#">Cisco Unity Connection</a> の統合を設定する</li> <li>• <a href="#">統合をテストする</a> (49 ページ)</li> <li>• オプションタスク <ul style="list-style-type: none"> <li>• (オプション) <a href="#">SIP ダイジェスト認証</a> を設定する</li> <li>• (オプション) <a href="#">アプリケーションユーザー</a> を作成する</li> </ul> </li> </ul>

統合のシナリオ	統合タスク
Cisco Unified CM と Unity Connection との統合 (クラストモード)	<ul style="list-style-type: none"> <li>• Cisco Unity Connection でボイスメッセージングポートを計画する (3 ページ)</li> <li>• 統合に向けて Cisco Unified CM を設定する <ul style="list-style-type: none"> <li>• SIP トランク セキュリティ プロファイルを作成する</li> <li>• SIP プロファイルを作成する</li> <li>• SIP トランクを作成する</li> <li>• ルートパターンを作成する</li> <li>• ルートリストを作成する</li> <li>• ルートパターンを作成する</li> <li>• ボイスメールパイロットを作成する</li> <li>• ボイスメールプロファイルを設定する</li> <li>• ボイスメールサーバーのサービスパラメータを設定する</li> </ul> </li> <li>• Cisco Unity Connection の統合を設定する</li> <li>• 統合をテストする (49 ページ)</li> <li>• オプション タスク <ul style="list-style-type: none"> <li>• (オプション) SIP ダイジェスト認証を設定する</li> <li>• (オプション) アプリケーションユーザーを作成する</li> <li>• (オプション) AXL サーバーを設定する (28 ページ)</li> </ul> </li> </ul>



- (注) これが最初の連動の場合、最初の電話システムがデフォルト ユーザー テンプレートで自動的に選択されます。電話システム連動の作成後に追加したユーザーは、デフォルトでこの電話システムに割り当てられます。ただし、後続の統合ごとに、新しい電話システムに適用可能な新しいユーザーテンプレートを追加します。新しいユーザーテンプレートの追加、または新しいユーザーを追加する際のユーザーテンプレートの選択の詳細については、[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/15/administration/guide/b\\_15cucsag.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/administration/guide/b_15cucsag.html) にある『Cisco Unity Connection システム アドミネストレーション ガイド』の「ユーザー属性」の章の「ユーザーテンプレート」セクションを参照してください。

## SIP トランク セキュリティ プロファイルを作成する

すべてのユーザー電話（電話番号）によって使用されている1つのコーリングサーチスペース（CSS）が存在している必要があります。それぞれのポート数が適切でない場合、連動が正常に機能しません。コーリングサーチスペースを設定し、ユーザーの電話を割り当てる手順については、Cisco Unified CM のヘルプを参照してください。

- ステップ 1** Cisco Unified CM Administration の [システム (System) ]メニューで、[セキュリティ (Security) ]> に移動し、>[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** [SIP トランク セキュリティ プロファイルの検索と一覧表示 (Find and List SIP Trunk Security Profiles) ]ページで、[新規追加 (Add New) ]を選択します。
- 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) ]ページの [SIP トランク セキュリティ プロファイル情報 (SIP Trunk Security Profile Information) ]で、次の設定を入力します。

表 3: SIP トランク セキュリティ プロファイル設定ページの設定

フィールド	設定
名前 (Name)	[Unity Connection SIP トランク セキュリティ プロファイル (Unity Connection SIP Trunk Security Profile) ]または別の名前を入力します。
説明 (Description)	[Cisco Unity Connection の SIP トランク セキュリティ プロファイル (SIP trunk security profile for Cisco Unity Connection) ]または別の説明を入力します。

フィールド	設定
デバイスセキュリティモード (Device Security Mode)	<p>Cisco Unified CM の認証と暗号化を有効にできない場合は、デフォルトの <b>[非セキュア (Non Secure)]</b> を受け入れます。</p> <p>Cisco Unified CM の認証または暗号化を有効にする場合は、<b>[認証済み (Authenticated)]</b> または <b>[暗号化 (Encrypted)]</b> を選択します。Cisco Unified CM サーバーの次の要件に注意してください。</p> <ul style="list-style-type: none"> <li>• TFTPサーバーを設定する必要があります。</li> <li>• Cisco Unified CM サーバーは、セキュアなシグナリングとメディア用に設定する必要があります。詳細については、<a href="https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/12_5_1/cucm_b_security-guide-1251.html">https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/12_5_1/cucm_b_security-guide-1251.html</a> にある『Cisco Unified Communications Manager セキュリティガイド、リリース 12.』の「デフォルトのセキュリティ設定」の章の「デフォルトのセキュリティ機能」の項を参照してください。</li> <li>• Cisco Unified CM サーバーの [デバイスセキュリティモード (Device Security Mode)] 設定は、Unity Connection サーバーの [セキュリティモード (Security Mode)] 設定 ([認証済み (Authenticated)] または [暗号化 (Encrypted)]) と一致している必要があります。</li> </ul> <p>(注) Cisco Unity Connection で Next Generation Encryption が有効になっている場合は、Cisco Unified CM サーバーで <b>[暗号化 (Encrypted)]</b> を選択する必要があります。</p>
X.509 のサブジェクト名 (X.509 Subject Name)	<p>Cisco Unified CM の認証と暗号化を有効にできない場合は、このフィールドを空のままにします。</p> <p>Cisco Unified CM の認証と暗号化を有効にする場合は、<b>[接続 (Connection)]</b> または別の名前を入力します。この名前は、Unity Connection サーバーの SIP 証明書の [サブジェクト名 (Subject Name)] フィールドと一致する必要があります。</p> <p>(注) X.509 サブジェクト名は Unity Connection サーバーの FQDN と一致する必要があります。</p>
ダイアログ外 EFER 要求の受け入れ (Accept Out-of-Dialog REFER)	このチェックボックスをオンにします。
Unsolicited NOTIFY の許可 (Accept Unsolicited Notification)	このチェックボックスをオンにします。

フィールド	設定
ヘッダー置き換えの許可 (Accept Replaces Header)	このチェックボックスをオンにします。

ステップ 4 [保存 (Save)] を選択します。

## SIP プロファイルを作成する

ステップ 1 [デバイス (Device)] メニューから、[デバイスの設定 (Device Settings)] > に移動し、> [SIP プロファイル (SIP Profile)] を選択します。

ステップ 2 [SIP プロファイルの検索と一覧表示 (Find and List SIP Profiles)] ページで、[検索 (Find)] を選択します。

ステップ 3 コピーする SIP プロファイルの右側にある [コピー (Copy)] を選択します。

ステップ 4 [SIP プロファイルの設定 (SIP Profile Configuration)] ページの [SIP プロファイル情報 (SIP Profile Information)] で、次の設定を入力します。

表 4: SIP プロファイル設定ページの設定

フィールド	設定
名前 (Name)	[Unity Connection SIP プロファイル (Unity Connection SIP Profile)] または別の名前を入力します。
説明	[Unity Connection の SIP プロファイル (SIP profile for Unity Connection)] またはその他の説明を入力します。

ステップ 5 Unity Connection が Cisco Unified CM との通信に IPv6 または IPv4/IPv6 デュアルスタックを使用する場合は、[ANAT を有効化 (Enable ANAT)] チェックボックスをオンにします。IPv6 またはデュアルスタック環境で発信者が正しく処理されるようにするには、この手順を実行する必要があります。

ステップ 6 [保存 (Save)] を選択します。

## SIP トランクを作成する

ステップ 1 [デバイス (Device)] メニューで、[トランク (Trunk)] を選択します。

ステップ 2 [トランクの検索と一覧表示 (Find and List Trunks)] ページで、[新規追加 (Add New)] を選択します。



- ステップ 3** [トランクの設定 (Trunk Configuration) ] ページの [トランクタイプ (Trunk Type) ] フィールドで、**[SIP トランク (SIP Trunk) ]** を選択します。
- ステップ 4** [デバイスプロトコル (Device Protocol) ] フィールドで、**[SIP]** を選択し、**[次へ (Next) ]** を選択します。
- ステップ 5** [デバイス情報 (Device Information) ] で、次の情報を入力します。

表 5: トランク設定ページでのデバイス情報の設定

フィールド	設定
デバイス名 (Device Name)	<b>Unity_Connection_SIP_Trunk</b> または別の名前を入力します。
説明 (Description)	<b>Unity Connection の SIP トランク</b> または別の説明を入力します。
S RTP 許可 (SRTP Allowed)	Cisco Unified CM の認証と暗号化を有効にする場合は、このチェックボックスをオンにします。

- ステップ 6** ユーザーの電話がコーリングサーチスペースに含まれている場合は、**[着信コール (Inbound Calls) ]** で次の設定を入力します。制限しない場合は、[ステップ 7](#) に進みます。

表 6: トランク設定ページでの着信コールの設定

フィールド	設定
コーリングサーチスペース (Calling Search Space)	ユーザーの電話機を含むコーリングサーチスペースの名前を選択します。
Diversionヘッダー配信のリダイレクト - インバウンド (Redirecting Diversion Header Delivery - Inbound)	このチェックボックスをオンにします。

- ステップ 7** ユーザーの電話がコーリングサーチスペースに含まれている場合は、**[アウトバウンドコール (Outbound Calls) ]** で次の設定を入力します。

フィールド	設定
Diversionヘッダー配信のリダイレクト - アウトバウンド (Redirecting Diversion Header Delivery - Outbound)	このチェックボックスをオンにします。

## SIP トランクを作成する

フィールド	設定
接続されたパーティでのみ DN を配信 (Deliver DN only in connected party)	発信 SIP メッセージでは、Unity Connection 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。これがデフォルトの設定です。
接続されたパーティでのみ URI を配信 (Deliver URI only in connected party)	発信 SIP メッセージでは、Unity Connection 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 が利用できない場合、Unity Connection は電話番号を挿入します。
接続されたパーティで URI と DN を配信 (Deliver URI and DN in connected party)	発信 SIP メッセージでは、Unity Connection は SIP の連絡先ヘッダーに発信側のディレクトリ URI と電話番号を含む混合アドレスを挿入します。ディレクトリ URI が利用できない場合、Unity Connection は電話番号だけを含まれます。

トランク設定ページでの発信コールの設定

**ステップ 8** [SIP 情報 (SIP Information)] で、次の設定を入力します。

表 7: トランク設定ページでの SIP 情報の設定

フィールド	設定
接続先アドレス (Destination Address)	Cisco Unified CM の接続先となる Unity Connection SIP ポートの IP アドレスを入力します。
宛先アドレス IPv6 (Destination Address IPv6)	Cisco Unified CM の接続先となる Unity Connection SIP ポートの IPv6 アドレスを入力します。  IPv6 アドレスは、IPv6 アドレス テキスト表現の「RFC 5952」標準で提案されている正規のテキスト表現形式である必要があります。  (注) IPv6 は、Unity Connection と Cisco Unified CM の間の SIP インテグレーションに対応しています。
接続先ポート (Destination Port)	デフォルト値の <b>5060</b> を使用することを推奨します。
SIP トランクセキュリティ プロファイル (SIP Trunk Security Profile)	[SIP トランク セキュリティ プロファイルの検索と一覧表示 (Find and List SIP Trunk Security Profiles)] ページで、 <a href="#">SIP トランク セキュリティ プロファイルを作成する</a> の手順で作成した SIP トランク セキュリティ プロファイルを選択します。例えば、「Unity Connection SIP トランク セキュリティ プロファイル」を選択します。

フィールド	設定
再ルーティング用コーリングサーチスペース (Rerouting Calling Search Space)	ユーザーの電話機で使用されるコーリングサーチスペースの名前を選択します。
アウトオブダイアログ REFER コーリングサーチスペース (Out-of-Dialog Refer Calling Search Space)	ユーザーの電話機で使用されるコーリングサーチスペースの名前を選択します。
SIP プロファイル (SIP Profile)	<a href="#">SIP プロファイルを作成する</a> の手順で作成した SIP プロファイルの名前を選択します。例えば、「Unity Connection SIP トランクプロファイル」を選択します。

ステップ 9 サイトに必要なその他の設定を調整します。

ステップ 10 [保存 (Save)] を選択します。

## ルートパターンを作成する

ステップ 1 [コールルーティング (Call Routing)] メニューで、[ルート/ハント (Route/Hunt)] > に移動し、> [ルートパターン (Route Pattern)] を選択します。

ステップ 2 [ルートパターンの検索と一覧表示 (Find and List Route Patterns)] ページで、[新規追加 (Add New)] を選択します。

ステップ 3 [ルートパターンの設定 (Route Pattern Configuration)] ページで、次の設定を入力します。

表 8: ルートパターンの設定ページの設定

フィールド	設定
ルートパターン (Route Pattern)	Unity Connection のボイスメールのパイロット番号を入力します。
ゲートウェイ/ルートリスト (Gateway/Route List)	<a href="#">SIP トランクを作成する</a> で作成した SIP トランクの名前を選択します。例えば、「Unity_Connection_SIP_Trunk」を選択します。

ステップ 4 [保存 (Save)] を選択します。

## ルートグループを作成する

**ステップ 1** [コールルーティング (Call Routing) ]メニューで、[ルート/ハント (Route/Hunt) ]> に移動し、>[ルートグループ (Route Group) ]を選択します。

**ステップ 2** [ルートグループの検索と一覧表示 (Find and List Route Groups) ]ページで、[新規追加 (Add New) ]を選択します。

**ステップ 3** [ルートグループの設定 (Route Group Configuration) ]ページで、次の設定を入力します。

表 9: ルートグループの設定ページの設定

フィールド	設定
ルートグループ名 (Route Group Name)	SIP_Trunk_Route_Group または別の名前を入力します。
分配アルゴリズム (Distribution Algorithm)	[トップダウン (Top Down) ]を選択します。

**ステップ 4** 両方の SIP トランクが [使用可能なデバイス (Available Devices) ]フィールドに表示されることを確認します。それ以外の場合は、[検索 (Find) ]を選択します。

**ステップ 5** [ルートグループに追加 (Add to Route Group) ]を選択します。

**ステップ 6** [現在のルートグループメンバー (Current Route Group Members) ]で、サブスクリバサーバーに接続する SIP トランクがリストの最初に表示されることを確認します。

上向き矢印または下向き矢印をクリックして SIP トランクの順序を変更できます。

**ステップ 7** [保存 (Save) ]を選択します。

## ルートリストを作成する

**ステップ 1** [コールルーティング (Call Routing) ]メニューで、[ルート/ハント (Route/Hunt) ]> に移動し、>[ルートリスト (Route List) ]を選択します。

**ステップ 2** [ルートリストの検索と一覧表示 (Find and List Route Lists) ]ページで、[新規追加 (Add New) ]を選択します。

**ステップ 3** [ルートリストの設定 (Route List Configuration) ]ページで、次の設定を入力します。

表 10: ルートリストの設定ページの設定

フィールド	設定
名前 (Name)	<b>SIP_Trunk_Route_List</b> または別の名前を入力します。
説明 (Description)	[ <b>SIP</b> トランクルートリスト ( <b>SIP Trunk Route List</b> )] または別の説明を入力します。
Cisco Unified Communications Manager グループ (Cisco Unified Communications Manager Group)	[ <b>デフォルト (Default)</b> ] を選択します。

ステップ 4 [保存 (Save)] を選択します。

ステップ 5 [このルートリストを有効にする (Enable This Route List)] 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。

ステップ 6 [ルートリストメンバー情報 (Route List Member Information)] で、[ルートグループの追加 (Add Route Group)] を選択します。

ステップ 7 [ルートリストの詳細設定 (Route List Detail Configuration)] ページの [ルートグループ (Route Group)] フィールドで、[Cisco Unity Connection の統合を設定する](#) の手順で作成したルートグループを選択し、[保存 (Save)] を選択します。

ステップ 8 ルートリスト設定が保存されることが示されたら、[OK] をクリックします。

ステップ 9 [ルートリストの設定 (Route List Configuration)] ページで、[リセット (Reset)] を選択します。

ステップ 10 ルートリストのリセットを確認するように求められた場合は、[リセット (Reset)] をクリックします。

ステップ 11 [閉じる (Close)] を選択します。

## ボイスメールパイロットを作成する

ステップ 1 [高度な機能 (Advanced Features)] メニューで、[ボイスメール (Voice Mail)] > に移動し、> [ボイスメールパイロット (Voice Mail Pilot)] を選択します。

ステップ 2 [ボイスメールパイロットの検索と一覧表示 (Find and List Voice Mail Pilots)] ページで、[新規追加 (Add New)] を選択します。

ステップ 3 [ボイスメールパイロットの設定 (Voice Mail Pilot Configuration)] ページで、次のボイスメールパイロット番号の設定を入力します。

表 11: ボイスメールパイロット設定ページの設定

フィールド	設定
ボイスメールパイロット番号 (Voice Mail Pilot Number)	ユーザーが自分のボイスメッセージを聞くためにダイヤルするボイスメールパイロット番号を入力します。この番号は、 <a href="#">ルートパターンを作成する</a> の手順で入力したルートパターンと一致している必要があります。
コーリングサーチスペース (Calling Search Space)	ユーザー電話を含むパーティションと、ボイスメールのパイロット番号用に設定したパーティションを含む通話検索スペースを選択します。
説明	<b>[Unity Connection パイロット (Unity Connection Pilot)]</b> またはその他の説明を入力します。
システムのデフォルトボイスメールパイロットに設定 (Make This the Default Voice Mail Pilot for the System)	このチェックボックスをオンにします。このチェックボックスをオンにすると、現在のデフォルトのパイロット番号がこのボイスメールパイロット番号に置き換えられます。

ステップ 4 [保存 (Save)] を選択します。

## ボイスメールプロファイルを設定する

ステップ 1 [高度な機能 (Advanced Features)] メニューで、[ボイスメール (Voice Mail)] > に移動し、> [ボイスメールプロファイル (Voice Mail Profile)] を選択します。

ステップ 2 [ボイスメールプロファイルの検索と一覧表示 (Find and List Voice Mail Profiles)] ページで、[新規追加 (Add New)] を選択します。

ステップ 3 [ボイスメールプロファイルの設定 (Voice Mail Profile Configuration)] ページで、次のボイスメールプロファイル設定を入力します。

表 12: ボイスメールパイロット設定ページの設定

フィールド	設定
ボイスメールプロファイル名 (Voice Mail Profile Name)	<b>[Unity Connection プロファイル (Unity Connection Profile)]</b> またはボイスメールプロファイルを識別するための別の名前を入力します。
説明 (Description)	<b>[Unity Connection のプロファイル (Profile for Unity Connection)]</b> またはその他の説明を入力します。

フィールド	設定
ボイスメールパイロット (Voice Mail Pilot)	<a href="#">ボイスメールパイロットを作成する</a> で定義したボイスメールパイロットを選択します。
ボイスメールボックスのマスク (Voice Mail Box Mask)	Cisco Unified CM でマルチテナントサービスを有効にしていない場合は、このフィールドを空白のままにします。  マルチテナントサービスを有効にしている場合、各テナントは自身のボイスメールプロファイルを使用し、他のテナントと共有するパーティションごとに内線番号（電話番号）を識別するためのマスクを作成する必要があります。たとえば、あるテナントは972813XXXXというマスクを使用し、別のテナントは214333XXXXというマスクを使用することができます。また、それぞれのテナントはMWI用に独自のトランスレーションパターンを使用します。
このボイスメールプロファイルをシステムのデフォルトにする (Make This the Default Voice Mail Profile for the System)	このボイスメールプロファイルをデフォルトにするには、このチェックボックスをオンにします。  このチェックボックスをオンにすると、現在のデフォルトのボイスメールプロファイルが、このボイスメールプロファイルに置き換えられます。

ステップ4 [保存 (Save)] を選択します。

## ボイスメールサーバーのサービスパラメータを設定する

SIP ダイジェスト認証を設定しない場合は、[Cisco Unity Connection の統合を設定する](#)に進みます。

- ステップ1 Cisco Unified CM Administration で、[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の設定 (Service Parameters Configuration)] ページの [サーバー (Server)] フィールドで、Cisco Unified CM サーバーの名前を選択します。
- ステップ3 [サービス (Service)] リストから、[Cisco CallManager] を選択します。パラメータのリストが表示されません。
- ステップ4 [クラスタ全体のパラメータ (機能 - 全般) (Clusterwide Parameters (Feature - General))] で、[マルチテナント MWI モード (Multiple Tenant MWI Modes)] パラメータを見つけます。
- ステップ5 複数のテナント MWI 通知を使用する場合は、[はい (True)] を選択します。

このパラメータを [はい (True)] に設定すると、Cisco Unified CM は、MWI がオンまたはオフにされたときに、任意の設定済みトランスレーションパターンを使用して、ボイスメールの内線番号を電話番号に変換します。

ステップ6 いずれかの設定を変更した場合は、[保存 (Save)] を選択します。次に、Cisco Unified CM サーバーをシャットダウンして再起動します。

## (オプション) SIP ダイジェスト認証を設定する

- ステップ1 [システム (System)] メニューから、[セキュリティ (Security)] > に移動し、> [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 [SIP トランク セキュリティ プロファイルの検索と一覧表示 (Find and List SIP Trunk Security Profiles)] ページで、[SIP トランク セキュリティ プロファイルを作成する](#)の手順で作成した SIP トランク セキュリティ プロファイルを選択します。
- 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)] ページで、[ダイジェスト認証を有効化 (Enable Digest Authentication)] チェック ボックスをオンにします。
- ステップ4 [保存 (Save)] を選択します。

## (オプション) アプリケーションユーザーを作成する

- ステップ1 [ユーザー管理 (User Management)] メニューで、[アプリケーションユーザー (Application User)] を選択します。
- ステップ2 [アプリケーションユーザーの検索/一覧表示 (Find and List Application Users)] ページで、[新規追加 (Add New)] を選択します。
- ステップ3 [アプリケーションユーザーの設定 (Application User Configuration)] ページで、次の設定を入力します。

表 13: アプリケーションユーザーの設定ページの設定

フィールド	設定
ユーザーID (User ID)	アプリケーションユーザーの識別名を入力します。Cisco Unified CM では、ユーザー ID の作成後の変更はできません。使用できる特殊文字は、=、+、<、>、#、;、\、,、"、および空白です。
パスワード (Password)	ダイジェスト信用証明書に使用するものと同じパスワードを入力します。
パスワードの確認 (Confirm Password)	パスワードを再度入力します。



フィールド	設定
ダイジェストクレデンシャル (Digest Credentials)	ダイジェスト信用証明書の名前を入力します。
ヘッダー置き換えの許可 (Accept Replaces Header)	このチェックボックスはオフのままにします。
使用可能なデバイス (Available Devices)	<p>このリストボックスには、このアプリケーションユーザーに関連付けることのできるデバイスが表示されます。</p> <p>デバイスをこのアプリケーションユーザーに関連付けるには、デバイスを選択し、リストボックスの下にある下矢印を選択します。</p> <p>このアプリケーションユーザーに関連付けようとするデバイスがこのペインに表示されない場合は、次のいずれかのボタンを選択して、他のデバイスを検索します。</p> <ul style="list-style-type: none"> <li>• <b>さらに電話を検索 (Find more Phones)</b> : このアプリケーションユーザーに関連付ける電話機をさらに検索するには、このボタンを選択します。[電話の検索と一覧表示 (Find and List Phones)] ウィンドウが表示され、電話機を検索できます。</li> <li>• <b>さらにルートポイントを検索 (Find More Route Points)</b> : このアプリケーションユーザーに関連付ける電話機をさらに検索するには、このボタンを選択します。[CTI ルートポイントの検索と一覧表示 (Find and List CTI Route Points)] ウィンドウが表示され、CTI ルートポイントを検索できます。</li> </ul>
割り当てられているCAPFプロファイル (Associated CAPF Profiles)	[割り当てられている CAPF プロファイル (Associated CAPF Profiles)] ペインには、そのユーザー用にアプリケーションユーザー CAPF プロファイルを設定した場合は、アプリケーションユーザー CAPF プロファイルのインスタンス ID が表示されます。プロファイルを編集するには、[インスタンス ID (Instance ID)] を選択し、[プロファイルの編集 (Edit Profile)] を選択します。[アプリケーションユーザー CAPF プロファイルの設定 (Application User CAPF Profile Configuration)] ウィンドウが表示されます。
グループ (Groups)	このリストボックスには、アプリケーションユーザーの所属先となるグループが表示されます。
ロール (Roles)	このリストボックスには、アプリケーションユーザーに割り当てられる権限が表示されます。

ステップ 4 [保存 (Save)] を選択します。

## (オプション) AXL サーバーを設定する

Unity Connection が AXL サーバーに接続する場合は、次の設定を行います。

- ステップ 1 [テレフォニー統合 (Telephony Integrations)] を展開し、[電話システム (Phone System)] を選択します。
- ステップ 2 [電話システムの検索 (Search Phone Systems)] ページで、作成した電話システムの表示名を選択します。
- ステップ 3 [電話システムの基本 (Phone System Basics)] ページの [編集 (Edit)] メニューで、[Cisco Unified Communications Manager AXL サーバー (Cisco Unified Communications Manager AXL Servers)] を選択します。

AXL サーバーへの接続は、Cisco Unified CM ユーザーのインポートや、Cisco Unity Connection の個人的なコール転送ルールのユーザーの特定の電話設定を変更するために、Unity Connection が Cisco Unified CM データベースにアクセスする必要がある場合に必要です。

(注) Cisco Unified CM ユーザーのインポートを計画している場合は、各ユーザーのエンドユーザー設定ページのプライマリ内線フィールドが入力されていることを確認してください。入力されていないと、検索でインポートするユーザーが見つかりません。

- ステップ 4 [AXL サーバーの編集 (Edit AXL Servers)] ページの [AXL サーバー (AXL Servers)] で、[新規追加 (Add New)] を選択します。
- ステップ 5 AXL サーバーの次の設定を入力し、[保存 (Save)] を選択します。

表 14: AXL サーバーの設定

フィールド	設定
順序 (Order)	AXL サーバーの優先順位を入力します。最も小さい数字はプライマリ AXL サーバーで、それよりも大きい数字はセカンダリサーバーを表します。
IP アドレス (IP Address)	AXL サーバーの IP アドレスを入力します。
ポート (Port)	Unity Connection で接続する AXL サーバーのポートを入力します。この設定は、AXL サーバーが使用するポートと同じにする必要があります。

- ステップ 6 他のすべての AXL サーバーに対して、ステップ 4 とステップ 5 を繰り返します。
- ステップ 7 [AXL サーバー設定 (AXL Server Settings)] で、次の設定を入力し、[保存 (Save)] を選択します。

表 15: AXL サーバーの設定

フィールド	設定
ユーザー名 (Username)	<p>Unity Connection で AXL サーバーにサインインするために使用するユーザー名を入力します。</p> <p>(注) このユーザーは、「標準 AXL API アクセス」ロールに割り当てられた Cisco Unified CM アプリケーションユーザーの名前と一致する必要があります。</p>
パスワード (Password)	<p>Unity Connection で AXL サーバーにサインインするために使用するユーザーのパスワードを入力します。</p> <p>(注) このパスワードは、[ユーザー名 (User Name)] フィールドに入力した Cisco Unified CM アプリケーションユーザーのパスワードと一致する必要があります。</p>
Cisco Unified Communications Manager のバージョン (Cisco Unified Communications Manager Version)	<p>以下を正確に説明する適切な設定を選択します。</p> <ul style="list-style-type: none"> <li>• Unity Connection と統合する Cisco Unified CM のバージョン。</li> <li>• AXL ポートで SSL を有効にするかどうか。</li> </ul> <p>非 SSL バージョンを選択する場合、AXL ポートは非 SSL ポート（通常はポート 80）である必要があります。SSL 対応バージョンを選択する場合、AXL ポートは SSL 対応ポート（通常はポート 443 またはポート 8443）である必要があります。</p>
プライマリ AXL サーバのエンドユーザ暗証番号同期を有効にする (Enable End User PIN Synchronization for Primary AXL Server)	<p>同じユーザー ID (Unity Connection のエイリアス) を持つユーザーに対して、Unity Connection と Cisco Unified CM 間の PIN 同期を有効にするには、このチェックボックスをオンにします。</p> <p>この機能を有効にすると、ユーザーが Cisco Unity Connection で PIN を更新するたびに、PIN は Cisco Unified CM と同期され、その逆も同様です。</p> <p>デフォルト設定：チェックボックスはオフです。</p> <p>PIN 同期の詳細については、<a href="https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/design/b_15cucsag/b_12xcucsag_appendix_010011.html">https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/design/b_15cucsag/b_12xcucsag_appendix_010011.html</a> にある『Cisco Unity Connection システム アドミニストレーション ガイド、リリース 15』の「ユーザー設定」の章にある「Unity Connection と Cisco Unified CM 間の PIN 生成」の項を参照してください。</p>

フィールド	設定
証明書エラーを無視する (Ignore Certificate Errors)	<p>AXL サーバーの証明書検証エラーを無視する場合は、チェックボックスをオンにします。このチェックボックスをオフにすると、Unity Connection は AXL サーバーの証明書を検証します。ただし、チェックボックスをオンにする前に、Cisco Unified CM の tomcat ルート証明書を Unity Connection サーバーの tomcat trust にアップロードする必要があることを確認してください。</p> <p>デフォルト設定：チェックボックスはオンです。</p> <p>証明書の詳細については、  <a href="https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/cs_administration/guide/b_15cucosagx.html">https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/cs_administration/guide/b_15cucosagx.html</a>  にある『Cisco Unified Communications オペレーティングシステムアドミニストレーションガイド、リリース 15』の「セキュリティ」の章を参照してください。</p>

- ステップ 8** 対応するアプリケーションサーバーを Cisco Unified CM に追加するには、Cisco Unified CM Administration にログインします。
- ステップ 9** Cisco Unified CM Administration で、[システム (System)] > [アプリケーションサーバー (Application Server)] ページに移動します。
- ステップ 10** [アプリケーションサーバーの検索と一覧表示 (Find and List Application Servers)] ページで、[検索 (Find)] を選択してすべてのアプリケーションサーバーを表示します。
- ステップ 11** [名前 (Name)] 列で、Cisco Unity Connection サーバーの名前を選択します。
- ステップ 12** [アプリケーションサーバーの設定 (Application Server Configuration)] ページの [使用可能なアプリケーションユーザー (Available Application User)] フィールドで、ステップ 7 で使用した Cisco Unified CM アプリケーションユーザーを選択し、下矢印を選択してそれを [選択されたアプリケーションユーザー (Selected Application User)] フィールドに移動します。
- ステップ 13** [保存 (Save)] を選択します。

## Cisco Unity Connection の統合を設定する

Unity Connection は、Cisco Unified Communications Manager との SIP トランク統合によるボイスメッセージポートの認証と暗号化に、証明書とセキュリティプロファイルを使用します。

### 前提条件

統合プロセスを開始する前に、セキュア SIP 設定を成功させるために、次の点を考慮する必要があります。

- Cisco Unity Connection は、輸出規制機能が許可されているスマートライセンスに登録する必要があります。シスコ スマート ソフトウェア ライセンシングの詳細は、  
[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/admin/12\\_0\\_1/systemConfig/cucm\\_b\\_system-configuration-guide-1201.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_0_1/systemConfig/cucm_b_system-configuration-guide-1201.html) にある『Cisco Unified Communications Manager シス

テム設定ガイド、リリース 12』の「スマート ソフトウェア ライセンシング」の章の「スマート ソフトウェア ライセンシングの概要」の項を参照してください。

- Cisco Unity Connection は制限付きバージョンを実行している必要があります。Cisco Unity Connection の制限版と無制限版の詳細については、[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/12x/security/b\\_12xcucsecx.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/security/b_12xcucsecx.html) にある『Cisco Unity Connection セキュリティガイド、リリース 12』の「Cisco Unity Connection : 制限版と無制限版」の章にある「Cisco Unity Connection : 制限版と無制限版」の項を参照してください。
- Cisco Unity Connection は、CLI コマンド「**utils cuc encryption enable**」を使用して暗号化を有効にする必要があります。CLI コマンドの詳細については、<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html> にある『Cisco Unified Solutions コマンドライン インターフェイス リファレンス ガイド』を参照してください。

Cisco Unified Communications Manager と Unity Connection が統合できる状態になっていることを確認したら、次の手順で統合を設定し、ポート設定を入力します。

## 統合を作成する

- ステップ 1** Cisco Unity Connection Administration にサインインします。
- ステップ 2** Cisco Unity Connection Administration で、[テレフォニー統合 (Telephony Integrations)] を展開し、[電話システム (Phone System)] を選択します。
- ステップ 3** [電話システムの検索 (Search Phone Systems)] ページの [表示名 (Display Name)] で、デフォルトの電話システム名をクリックします。
- ステップ 4** [電話システムの基本設定 (Phone System Basics)] ページの [電話システム名 (Phone System Name)] フィールドで、電話システムの説明的な名前を入力します。
- ステップ 5** この電話システムを TRaP 接続のデフォルトとして使用し、ボイスメールボックスを持たない管理者やユーザーが Unity Connection Web アプリケーションで電話を通じて録音および再生できるようにする場合は、[デフォルト TRAP スイッチ (Default TRAP Switch)] チェックボックスをオンにします。別の電話システムを TRaP 接続のデフォルトとして使用する場合は、このチェックボックスをオフにします。
- ステップ 6** [保存 (Save)] を選択します。
- ステップ 7** [電話システムの基本設定 (Phone System Basics)] ページの [関連リンク (Related Links)] ドロップダウンボックスで、[ポートグループの追加 (Add Port Group)] を選択して、[移動 (Go)] を選択します。
- ステップ 8** [新しいポートグループ (New Port Group)] ページで、該当する設定を入力し、[保存 (Save)] を選択します。

表 16: 新しいポートグループページの設定

フィールド	設定
電話システム (Phone System)	ドロップダウンリストから、 <b>ステップ 5</b> で入力した電話システムの名前を選択します。

フィールド	設定
作成元 (Create From)	[ <b>ポートグループテンプレート (Port Group Template)</b> ] を選択し、ドロップダウンボックスで [ <b>SIP</b> ] を選択します。
表示名 (Display Name)	ポートグループの説明的な名前を入力します。デフォルト名をそのまま使用することも、任意の名前を入力することもできます。
SIP サーバーで認証する (Authenticate with SIP Server)	Unity Connection で Cisco Unified CM サーバーを認証する場合は、このチェックボックスをオンにします。
認証ユーザー名 (Authentication User Name)	Unity Connection が Cisco Unified CM サーバーとの認証に使用する名前を入力します。
認証パスワード (Authentication Password)	Unity Connection が Cisco Unified CM サーバーでの認証に使用するパスワードを入力します。
連絡先回線名 (Contact Line Name)	ユーザーが Unity Connection に連絡するために使用し、Unity Connection が Cisco Unified CM サーバーに登録するために使用する音声メッセージング回線名 (またはパイロット番号) を入力します。
SIP セキュリティプロファイル (SIP Security Profile)	Unity Connection が使用する SIP セキュリティプロファイルを選択します。
次世代暗号化の有効化 (Enable Next Generation Encryption)	(注) (セキュアな TLS ポートが使用されている場合のみ) Unity Connection で RSA キーベースまたは EC キーベースの証明書 (自己署名証明書およびサードパーティ証明書) を使用して SIP インターフェイスで次世代暗号化サポートを提供する場合は、このチェックボックスをオンにします。詳細については、 <a href="#">Next Generation Security Over SIP 統合を有効にする</a> を参照してください。

フィールド	設定
セキュリティモード (Security Mode)	<p>(セキュアな <i>TLS</i> ポートが使用され、[次世代暗号化を有効にする (<i>Enable Next Generation Encryption</i>)] チェックボックスがオフの場合のみ) 該当するセキュリティモードを選択します。</p> <ul style="list-style-type: none"> <li>• <b>認証済み (Authenticated)</b> : コールシグナリング メッセージは、認証済み <i>TLS</i> ポートを使用して Cisco Unified CM に接続されるため、完全性が保証されます。ただし、クリア (暗号化されていない) テキストで送信されるため、コールシグナリング メッセージのプライバシーは保証されません。</li> <li>• <b>暗号化 (Encrypted)</b> : コールシグナリングメッセージは、セキュアな <i>TLS</i> ポートを使用して Cisco Unified CM に接続され、暗号化されるため、完全性とプライバシーが保証されます。</li> </ul> <p>Unity Connection サーバーの [セキュリティモード (Security Mode)] 設定は、Cisco Unified CM サーバーの [デバイスセキュリティモード (Device Security Mode)] 設定と一致している必要があります。</p>
セキュア RTP (Secure RTP)	<p>(セキュアな <i>TLS</i> ポートを使用する場合のみ) メディアストリーム (RTP) が暗号化されるように、このチェックボックスをオンにします。メディアストリームを暗号化しない場合は、チェックボックスをオフにします。</p>
SIP 転送プロトコル (SIP Transport Protocol)	<p>Unity Connection によって使用される SIP 転送プロトコルを選択します。</p>
IPv4 アドレス/ホスト名 (IPv4 Address or Host Name)	<p>Unity Connection と統合しているプライマリ Cisco Unified CM サーバーの IPv4 アドレス (または、ホスト名) を入力します。</p> <p>このフィールドに IP アドレスまたはホスト名を入力するか、[IPv6 アドレス/ホスト名 (IPv6 Address or Host Name)] フィールドに IP アドレスまたはホスト名を入力する必要があります (また、該当する場合は、両方のフィールドに情報を入力します)。両方のフィールドを空白のままにすることはできません。</p>

フィールド	設定
IPv6 アドレス/ホスト名 (IPv6 Address or Host Name)	<p>Unity Connection と統合しているプライマリ Cisco Unified CM サーバーの IPv6 アドレス（または、ホスト名）を入力します。</p> <p>IPv6 アドレスは、IPv6 アドレステキスト表現の「RFC 5952」標準で提案されている正規のテキスト表現形式である必要があります。</p> <p>このフィールドに IP アドレスまたはホスト名を入力するか、[IPv4 アドレス/ホスト名 (IPv6 Address or Host Name)] フィールドに IP アドレスまたはホスト名を入力する必要があります（また、該当する場合は、両方のフィールドに情報を入力します）。両方のフィールドを空白のままにすることはできません。</p> <p>(注) IPv6 は、Cisco Unified CM 10.0 との SIP 統合向けにサポートされています。</p>
IP アドレスまたはホスト名	Cisco Unity Connection と統合しているプライマリ Cisco Unified CM サーバーの IP アドレス（または、ホスト名）を入力します。
ポート	Unity Connection と統合しているプライマリ Cisco Unified CM サーバーの TCP ポートを入力します。デフォルト設定を使用することを推奨します。

**ステップ 9** Cisco Unified CM クラスタにセカンダリサーバーがある場合、または TFTP サーバーを追加する場合（Cisco Unified CM の認証と暗号化に必要）、[ポートグループの基本設定 (Port Group Basics)] ページで、次のサブステップを実行します。それ以外の場合は、[ステップ 11](#)に進みます。

- [編集 (Edit)] メニューで、[サーバー (Servers)] を選択します。
- セカンダリ Cisco Unified CM サーバーを追加する場合、[サーバーの編集 (Edit Servers)] ページの [SIP サーバー (SIP Servers)] で、[追加 (Add)] を選択します。それ以外の場合は、[ステップ 10e](#)に進みます。
- セカンダリ Cisco Unified CM サーバーの次の設定を入力し、[保存 (Save)] を選択します。

表 17: SIP サーバーの設定

フィールド	設定
順位 (Order)	Cisco Unified CM サーバーの優先順位を入力します。最も小さい数字はプライマリ Cisco Unified CM サーバーで、それよりも大きい数字はセカンダリサーバーを表します。



フィールド	設定
IPv4 アドレス/ホスト名 (IPv4 Address or Host Name)	<p>セカンダリ Cisco Unified CM サーバーの IPv4 アドレス (またはホスト名) を入力します。</p> <p>このフィールドに IP アドレスまたはホスト名を入力するか、[IPv6 アドレス/ホスト名 (IPv6 Address or Host Name)] フィールドに IP アドレスまたはホスト名を入力する必要があります (また、該当する場合は、両方のフィールドに情報を入力します)。両方のフィールドを空白のままにすることはできません。</p>
IPv6 アドレス/ホスト名 (IPv6 Address or Host Name)	<p>セカンダリ Cisco Unified CM サーバーの IPv6 アドレス (またはホスト名) を入力します。</p> <p>IPv6 アドレスは、IPv6 アドレステキスト表現の「RFC 5952」標準で提案されている正規のテキスト表現形式である必要があります。</p> <p>このフィールドに IP アドレスまたはホスト名を入力するか、[IPv4 アドレス/ホスト名 (IPv6 Address or Host Name)] フィールドに IP アドレスまたはホスト名を入力する必要があります (また、該当する場合は、両方のフィールドに情報を入力します)。両方のフィールドを空白のままにすることはできません。</p> <p>(注) IPv6 は、Cisco Unified CM 10.0 との SIP 統合向けにサポートされています。</p>
IP アドレスまたはホスト名 (IP Address or Host Name)	セカンダリ Cisco Unified CM サーバーの IP アドレス (またはホスト名) を入力します。
ポート (Port)	Unity Connection と統合する Cisco Unified CM サーバーの IP ポートを入力します。デフォルト設定を使用することを推奨します。
TLS ポート (TLS Port)	Unity Connection と統合する Cisco Unified CM サーバーの TLS ポートを入力します。デフォルト設定を使用することを推奨します。

- d) 必要に応じて、Cisco Unified CM クラスタ内の追加の Cisco Unified CM サーバーについてステップ 10b. とステップ 10c. を繰り返します。
- e) TFTP サーバー (Cisco Unified CM の認証と暗号化に必要) を追加する場合は、[TFTP サーバー (TFTP Servers)] で [追加 (Add)] を選択します。それ以外の場合は、ステップ 10h. に進みます。
- f) セカンダリ Cisco Unified CM サーバーの次の設定を入力し、[保存 (Save)] を選択します。

表 18: TFTP サーバーの設定

フィールド	設定
順序 (Order)	TFTP サーバーの優先順位を入力します。数値の最も小さいサーバーがプライマリ TFTP サーバーで、数値がプライマリよりも大きい場合はセカンダリサーバーです。

フィールド	設定
IPv4 アドレス/ホスト名 (IPv4 Address or Host Name)	TFTP サーバーの IPv4 アドレス (またはホスト名) を入力します。 このフィールドに IP アドレスまたはホスト名を入力するか、[IPv6 アドレス/ホスト名 (IPv6 Address or Host Name)] フィールドに IP アドレスまたはホスト名を入力する必要があります (また、該当する場合は、両方のフィールドに情報を入力します)。両方のフィールドを空白のままにすることはできません。
IPv6 アドレス/ホスト名 (IPv6 Address or Host Name)	TFTP サーバーの IPv6 アドレス (またはホスト名) を入力します。 IPv6 アドレスは、IPv6 アドレステキスト表現の「RFC 5952」標準で提案されている正規のテキスト表現形式である必要があります。 このフィールドに IP アドレスまたはホスト名を入力するか、[IPv4 アドレス/ホスト名 (IPv4 Address or Host Name)] フィールドに IP アドレスまたはホスト名を入力する必要があります (また、該当する場合は、両方のフィールドに情報を入力します)。両方のフィールドを空白のままにすることはできません。  (注) <ul style="list-style-type: none"> <li>IPv6 は、Cisco Unified CM 10.0 との SIP 統合向けにサポートされています。</li> <li>[プライマリサーバー設定 (Primary Server Settings)] で [SIP セキュリティプロファイル (SIP security profile)] ドロップダウンメニューからセキュアな SIP プロファイルを選択する場合は、DNS サーバーが IPv6 アドレスとホスト名の両方を正しく解決できることを確認します。</li> </ul>
IP アドレスまたはホスト名	TFTP サーバーの IP アドレス (またはホスト名) を入力します。

- g) 必要に応じて、追加する TFTP サーバごとに [ステップ10e](#) と [ステップ10f](#) を繰り返します。
- h) [編集 (Edit)] メニューで、[ポートグループの基本設定 (Port Group Basics)] を選択します。
- i) [ポートグループの基本設定 (Port Group Basics)] ページで、[リセット (Reset)] を選択します。

**ステップ 10** [ポートグループの基本設定 (Port Group Basics)] ページの [関連リンク (Related Links)] ドロップダウンボックスで、[ポートの追加 (Add Ports)] を選択して、[移動 (Go)] を選択します。

**ステップ 11** [新しいポート (New Port)] ページで、次の設定を入力し、[保存 (Save)] を選択します。

表 19: 新しいポートページの設定

フィールド	設定
有効 (Enabled)	このチェックボックスをオンにします。

フィールド	設定
ポート数 (Number of Ports)	このポート グループ内に作成するボイス メッセージ ポートの数を入力します。  (注) Unity Connection クラスタでは、すべての Unity Connection サーバーで使用されるボイスメッセージポートの合計数を入力する必要があります。各ポートは特定の Unity Connection サーバーに割り当てられています。
電話システム (Phone System)	ドロップダウンリストから、 <b>ステップ 5</b> で入力した電話システムの名前を選択します。
ポートグループ (Port Group)	<b>ステップ 9</b> で追加したポートグループの名前を選択します。
サーバー (Server)	Unity Connection サーバーの名前を選択します。

**ステップ 12** [ポートの検索 (Search Ports) ] ページで、この電話システム統合に対して作成した最初のボイスメッセージポートの表示名を選択します。

(注) デフォルトでは、ボイスメッセージポートの表示名は、ポートグループの表示名の後に増分番号が付加されたものになります。

**ステップ 13** [ポートの基本設定 (Port Basics) ] ページで、必要に応じてボイスメッセージポートを設定します。以下の表のフィールドを変更できます。

表 20: 個別のボイスメッセージポートの設定

フィールド	説明
有効 (Enabled)	ポートを有効にするには、チェックボックスをオンにします。ポートは通常の中に有効になります。  ポートを無効にするには、このチェックボックスをオフにします。ポートが無なっている場合、そのポートへのコールに対して、呼び出し音は鳴りますが、はありません。通常、ポートは、テスト中インストーラによってだけ無効になります。
サーバー (Server)	(Unity Connection クラスタのみ) このポートを処理する Unity Connection サーバーの名前を選択します。  ボイスメッセージングトラフィックを均等に共有するように、Cisco Unity Connection サーバーに同じ数の応答およびダイヤルアウトボイスメッセージングポートを当てます。
コールに回答 (Answer Calls)	ポートを通話への応答用に指定するには、このチェックボックスをオンにします。これらのコールは、身元不明発信者またはユーザーからの着信コールである可能性があります。

フィールド	説明
メッセージ通知を実行する (Perform Message Notification)	ポートをユーザーに対するメッセージ通知用に指定するには、このチェックボックスをオンにします。稼働率が最も低いポートに [メッセージ通知を実行する (Perform Message Notification)] を割り当てます。
MWIリクエストを送信する (Send MWI Requests)	ポートでの MWI のオン/オフを指定するには、このチェックボックスをオンにします。稼働率が最も低いポートに [MWI リクエストを送信する (Send MWI Requests)] を割り当てます。
TRAP接続を許可する (Allow TRAP Connections)	このチェックボックスをオンにすると、ユーザーは Cisco Unity Connection の web アプリケーションで電話から録音または再生用のポートを使用できます。稼働率が最も低いポートに [TRAP 接続を許可する (Allow TRAP Connections)] を割り当てます。

ステップ 14 [保存 (Save)] を選択します。

ステップ 15 [次へ (Next)] を選択します。

ステップ 16 電話システムの残りすべてのボイスメッセージポートについて、[ステップ 14](#) から [ステップ 16](#) を繰り返します。

ステップ 17 Cisco Unified CM 認証と暗号化を使用する場合は、RSA キーベースの Tomcat 証明書を生成してアップロードします。詳細については、[RSA キーベースの証明書を設定する](#)の項を参照してください。

ステップ 18 別の電話システム統合が存在する場合は、Cisco Unity Connection Administration で [テレフォニー統合 (Telephony Integrations)] を展開し、[トランク (Trunk)] を選択します。

ステップ 19 [電話システムトランクの検索 (Search Phone System Trunks)] ページの [電話システムトランク (Phone System Trunk)] メニューで、[新しい電話システムトランク (New Phone System Trunk)] を選択します。

ステップ 20 [新しい電話システムトランク (New Phone System Trunk)] ページで、電話システムトランクの次の設定を入力し、[保存 (Save)] を選択します。

表 21: 電話システムトランクの設定

フィールド	設定
電話システム元 (From Phone System)	トランクを作成する電話システムの表示名を選択します。
電話システム先 (To Phone System)	トランクが接続する既存の電話システムの表示名を選択します。
トランクアクセスコード (Trunk Access Code)	以前の既存の電話システムでゲートウェイを使用してコールを内線に転送するために Unity Connection でダイヤルする必要がある追加コードを入力します。

ステップ 21 作成する残りすべての電話システムトランクについて、[ステップ 18](#) と [ステップ 19](#) を繰り返します。

## Next Generation Security Over SIP 統合を有効にする

Unity Connection では、暗号化アルゴリズムを使用して機密性、整合性、および認証を提供する Next Generation Security over SIP インターフェイスがサポートされています。次世代暗号化により、SIP インターフェイスは TLS 1.2、SHA-2、および AES256 プロトコルに基づいて Suite B 暗号を使用するように制限されるため、より安全です。次世代暗号化には、暗号に加えて、Unity Connection と Cisco Unified CM の両方にアップロードする必要があるサードパーティ証明書も含まれています。Unity Connection と Cisco Unified CM 間の通信中に、暗号とサードパーティ証明書の両方が両端で検証されます。次に、次世代暗号化サポートの設定を示します。

### 証明書を生成、アップロードする

Unity Connection は、次世代のセキュリティのために、RSA キーベースの Tomcat 証明書と EC キーベースの Tomcat-ECDSA 証明書（自己署名およびサードパーティ）を使用します。各証明書の設定については、以降のセクションで説明します。

### RSA キーベースの証明書を設定する

#### Unity Connection の RSA キーベースの証明書を生成する

次に、Unity Connection の RSA キーベースの証明書を生成し、Cisco Unified CM にアップロードする手順を示します。

- ステップ 1 Unity Connection で、[Cisco Unified Operating System Administration] ページにサインインします。
- ステップ 2 [セキュリティ (Security)] に移動し、[証明書の管理 (Certificate Management)] を選択します。
- ステップ 3 Unity Connection の自己署名証明書を生成する場合は、[ステップ 4](#) から [ステップ 6](#) に従います。それ以外の場合は、[ステップ 7](#) に進みます。
- ステップ 4 [証明書管理 (Certificate Management)] ページで、[自己署名の生成 (Generate Self Signed)] を選択します。
- ステップ 5 [自己署名の生成 (Generate Self-Signed)] ウィンドウで、[証明書の目的 (Certificate Purpose)] で **[Tomcat]** を選択します
- ステップ 6 [作成 (Generate)] を選択します。
- ステップ 7 RSA キーベースのサードパーティ証明書を生成するには、[証明書管理 (Certificate Management)] ページで **[CSR の生成 (Generate CSR)]** を選択します。
- ステップ 8 [証明書署名要求の生成 (Generate Certificate Signing Request)] ウィンドウで、[証明書の目的 (Certificate Purpose)] フィールドで **[tomcat]** を選択します。
- ステップ 9 [親ドメイン (Parent Domain)] フィールドに、Unity Connection の完全な FQDN を入力します。
- ステップ 10 [作成 (Generate)] を選択します。

## Cisco Unified CM の RSA ベースの証明書を作成する

- ステップ 11 [証明書リスト (Certificate List) ] ページで、[CSR のダウンロード (Download CSR) ] を選択します。これにより、Microsoft CA または Verisign であるサードパーティから Unity Connection 証明書が生成されます。
- ステップ 12 Unity Connection のリーフ証明書と認証局のルート/チェーン証明書をシステムに保存します。
- ステップ 13 [証明書一覧 (Certificate List) ] ページで、[証明書/証明書チェーンのアップロード (Upload Certificate/Certificate Chain) ] を選択します。
- ステップ 14 [証明書/証明書チェーンのアップロード (Upload Certificate/Certificate Chain) ] ウィンドウで、[証明書の目的 (Certificate Purpose) ] フィールドで [tomcat] を選択します。
- ステップ 15 [ファイルのアップロード (Upload File) ] に移動し、[参照 (Browse) ] を選択して、ステップ 12 で保存したサードパーティ CSR によって生成された Unity Connection リーフ証明書をアップロードします。
- ステップ 16 [アップロード (Upload) ] を選択します。
- ステップ 17 Cisco Unified CM で、[Cisco Unified Operating System Administration] ページにサインインします。
- ステップ 18 [セキュリティ (Security) ] に移動し、[証明書の管理 (Certificate Management) ] を選択します。
- ステップ 19 [証明書一覧 (Certificate List) ] ページで、[証明書/証明書チェーンのアップロード (Upload Certificate/Certificate Chain) ] を選択します。
- ステップ 20 [証明書/証明書チェーンのアップロード (Upload Certificate/Certificate Chain) ] ウィンドウで、[証明書の目的 (Certificate Purpose) ] フィールドで [CallManager-trust] を選択します。
- ステップ 21 [ファイルのアップロード (Upload File) ] に移動し、[参照 (Browse) ] を選択して、ステップ 6 で生成した Unity Connection 自己署名証明書をアップロードします。Unity Connection のサードパーティ証明書をアップロードするには、ステップ 12 で保存したサードパーティ認証局のルート/チェーン証明書を参照します。
- (注) Unity Connection クラスタの場合は、Cisco Unified CM の CallManager-trust でパブリッシャとサブスクライバの両方の自己署名証明書を生成してアップロードします。
- ステップ 22 [アップロード (Upload) ] を選択します。

## Cisco Unified CM の RSA ベースの証明書を作成する

Cisco Unified CM の RSA ベースの証明書を作成し、Unity Connection にアップロードする手順は次のとおりです。

- ステップ 1 Cisco Unified CM で、[Cisco Unified Operating System Administration] ページにサインインします。
- ステップ 2 [セキュリティ (Security) ] に移動し、[証明書の管理 (Certificate Management) ] を選択します。
- ステップ 3 Cisco Unified CM の自己署名証明書を生成する場合は、ステップ 4 ~ 6 に従います。それ以外の場合は、ステップ 7 に進みます。
- ステップ 4 [証明書管理 (Certificate Management) ] ページで、[自己署名の生成 (Generate Self Signed) ] を選択します。
- ステップ 5 [新しい自己署名証明書の生成 (Generate New Self Signed Certificate) ] ウィンドウで、[証明書の目的 (Certificate Purpose) ] フィールドで [CallManager] を選択します。

- ステップ 6 [作成 (Generate)] を選択します。
- ステップ 7 RSA キーベースのサードパーティ証明書を生成するには、[証明書管理 (Certificate Management)] ページで [CSR の生成 (Generate CSR)] を選択します。
- ステップ 8 [証明書署名要求の生成 (Generate Certificate Signing Request)] ウィンドウで、[証明書の目的 (Certificate Purpose)] フィールドで [CallManager] を選択します。
- ステップ 9 [親ドメイン (Parent Domain)] フィールドに、Cisco Unified CM の完全な FQDN を入力します。
- ステップ 10 [作成 (Generate)] を選択します。
- ステップ 11 [証明書リスト (Certificate List)] ページで、[CSR のダウンロード (Download CSR)] を選択します。これにより、Microsoft CA または Verisign であるサードパーティから Cisco Unified CM 証明書が生成されません。
- ステップ 12 Cisco Unified CM のリーフ証明書と認証局のルート/チェーン証明書をシステムに保存します。
- ステップ 13 [証明書一覧 (Certificate List)] ページで、[証明書/証明書チェーンのアップロード (Upload Certificate/Certificate Chain)] を選択します。
- ステップ 14 [証明書/証明書チェーンのアップロード (Upload Certificate/Certificate Chain)] ウィンドウで、[証明書の目的 (Certificate Purpose)] フィールドで [CallManager] を選択します。
- ステップ 15 [ファイルのアップロード (Upload File)] に移動し、[参照 (Browse)] を選択して、ステップ 12 で保存したサードパーティ CSR によって生成された Cisco Unified CM リーフ証明書をアップロードします。
- ステップ 16 [アップロード (Upload)] を選択します。

(注) 証明書はポートグループのリセット時に自動的にダウンロードされるため、Unity Connection で CallManager 証明書を手動でアップロードする必要はありません。ただし、サードパーティ証明書の場合は、Unity Connection の **CallManager-trust** にサードパーティ認証局のルート証明書をアップロードする必要があります。

## EC キーベースの証明書を設定する

### Unity Connection の EC キーベースの証明書を生成する

次に、Unity Connection の EC キーベースの証明書を生成し、Cisco Unified CM にアップロードする手順を示します。

- ステップ 1 Unity Connection で、[Cisco Unified Operating System Administration] ページにサインインします。
- ステップ 2 [セキュリティ (Security)] に移動し、[証明書の管理 (Certificate Management)] を選択します。
- ステップ 3 Unity Connection の自己署名証明書を生成する場合は、ステップ 4 からステップ 6 に従います。それ以外の場合は、ステップ 7 に進みます。
- ステップ 4 [証明書管理 (Certificate Management)] ページで、[自己署名の生成 (Generate Self Signed)] を選択します。
- ステップ 5 [新しい自己署名証明書の生成 (Generate New Self Signed Certificate)] ウィンドウで、[証明書の目的 (Certificate Purpose)] フィールドで [tomcat-ECDSA] を選択します。
- ステップ 6 [作成 (Generate)] を選択します。

## Cisco Unified CM の EC キーベースの証明書を生成する

- ステップ 7** EC キーベースのサードパーティ証明書を生成するには、[証明書管理 (Certificate Management)] ページで [CSR の生成 (Generate CSR)] を選択します。
- ステップ 8** [証明書署名要求の生成 (Generate Certificate Signing Request)] ウィンドウで、[証明書の目的 (Certificate Purpose)] フィールドで [tomcat-ECDSA] を選択します。
- ステップ 9** [親ドメイン (Parent Domain)] フィールドに、Unity Connection の完全な FQDN を入力します。
- ステップ 10** [作成 (Generate)] を選択します。
- ステップ 11** [証明書リスト (Certificate List)] ページで、[CSR のダウンロード (Download CSR)] を選択します。これにより、Microsoft CA または Verisign であるサードパーティから Unity Connection ECDSA 証明書が生成されます。
- ステップ 12** Unity Connection のリーフ証明書と認証局のルート/チェーン証明書をシステムに保存します。
- ステップ 13** [証明書の検索と一覧表示 (Find and List Certificates)] ページで、[証明書/証明書チェーンのアップロード (Upload Certificate/Certificate Chain)] を選択します。
- ステップ 14** [証明書/証明書チェーンのアップロード (Upload Certificate/Certificate Chain)] ウィンドウで、[証明書の目的 (Certificate Purpose)] フィールドで [tomcat-ECDSA] を選択します。
- ステップ 15** [ファイルのアップロード (Upload File)] に移動し、[参照 (Browse)] を選択して、ステップ 12 で保存したサードパーティ CSR によって生成された Unity Connection リーフ証明書をアップロードします。
- ステップ 16** [アップロード (Upload)] を選択します。
- ステップ 17** Cisco Unified CM で、[Cisco Unified Operating System Administration] ページにサインインします。
- ステップ 18** [セキュリティ (Security)] に移動し、[証明書の管理 (Certificate Management)] を選択します。
- ステップ 19** [証明書一覧 (Certificate List)] ページで、[証明書/証明書チェーンのアップロード (Upload Certificate/Certificate Chain)] を選択します。
- ステップ 20** [証明書/証明書チェーンのアップロード (Upload Certificate/Certificate Chain)] ウィンドウで、[証明書の目的 (Certificate Purpose)] フィールドで [CallManager-trust] を選択します。
- ステップ 21** [ファイルのアップロード (Upload File)] に移動し、[参照 (Browse)] を選択して、ステップ 6 で生成した Unity Connection 自己署名証明書をアップロードします。Unity Connection のサードパーティ証明書をアップロードするには、ステップ 12 で保存したサードパーティ認証局のルート/チェーン証明書を参照します。
- (注) Unity Connection クラスタの場合は、Cisco Unified CM の CallManager-trust でパブリッシャとサブスクライバの両方の自己署名証明書を生成してアップロードします。
- ステップ 22** [アップロード (Upload)] を選択します。

## Cisco Unified CM の EC キーベースの証明書を生成する

Cisco Unified CM の EC キーベースの証明書を生成し、Unity Connection にアップロードする手順は次のとおりです。

- ステップ 1** Cisco Unified CM で、[Cisco Unified Operating System Administration] ページにサインインします。
- ステップ 2** [セキュリティ (Security)] に移動し、[証明書の管理 (Certificate Management)] を選択します。



- ステップ 3** Cisco Unified CM の自己署名証明書を生成する場合は、ステップ 4～6 に従います。それ以外の場合は、ステップ 7 に進みます。
- ステップ 4** [証明書管理 (Certificate Management) ] ページで、[自己署名の生成 (Generate Self Signed) ] を選択します。
- ステップ 5** [新しい自己署名証明書の生成 (Generate New Self Signed Certificate) ] ウィンドウで、[証明書の目的 (Certificate Purpose) ] フィールドで [CallManager-ECDSA] を選択します。
- ステップ 6** [作成 (Generate) ] を選択します。
- ステップ 7** EC キーベースのサードパーティ証明書を生成するには、[証明書管理 (Certificate Management) ] ページで [CSR の生成 (Generate CSR) ] を選択します。
- ステップ 8** [証明書署名要求の生成 (Generate Certificate Signing Request) ] ウィンドウで、[証明書の目的 (Certificate Purpose) ] フィールドで [CallManager-ECDSA] を選択します。
- ステップ 9** [親ドメイン (Parent Domain) ] フィールドに、Cisco Unified CM の完全な FQDN を入力します。
- ステップ 10** [作成 (Generate) ] を選択します。
- ステップ 11** [証明書リスト (Certificate List) ] ページで、[CSR のダウンロード (Download CSR) ] を選択します。これにより、Microsoft CA または Verisign であるサードパーティから Cisco Unified CM 証明書が生成されます。
- ステップ 12** Cisco Unified CM のリーフ証明書と認証局のルート/チェーン証明書をシステムに保存します。
- ステップ 13** [証明書一覧 (Certificate List) ] ページで、[証明書/証明書チェーンのアップロード (Upload Certificate/Certificate Chain) ] を選択します。
- ステップ 14** [証明書/証明書チェーンのアップロード (Upload Certificate/Certificate Chain) ] ウィンドウで、[証明書の目的 (Certificate Purpose) ] フィールドで [CallManager-ECDSA] を選択します。
- ステップ 15** [ファイルのアップロード (Upload File) ] に移動し、[参照 (Browse) ] を選択して、ステップ 12 で保存したサードパーティ CSR によって生成された Cisco Unified CM リーフ証明書をアップロードします。
- ステップ 16** [アップロード (Upload) ] を選択します。

(注) 証明書はポートグループのリセット時に自動的にダウンロードされるため、Unity Connection で CallManager 証明書を手動でアップロードする必要はありません。ただし、サードパーティ証明書の場合は、Unity Connection の **CallManager-trust** にサードパーティ認証局のルート証明書をアップロードする必要があります。

## セキュリティモードを設定する

- ステップ 1** Cisco Unity Connection Administration にサインインします。
- ステップ 2** Cisco Unity Connection Administration で、[テレフォニー統合 (Telephony Integrations) ] を展開し、[ポートグループ (Port Group) ] を選択します。
- ステップ 3** [ポートグループの検索 (Search Port Groups) ] ページで、該当するポートグループを選択します。
- ステップ 4** [次世代暗号化の有効化 (Enable Next Generation Encryption) ] 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。

- ステップ 5 Cisco Unified CM Administration にサインインします。
- ステップ 6 [システム (System)] > [セキュリティ (Security)] に移動し、[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 7 [SIP トランク セキュリティプロファイルの検索と一覧表示 (Find and List SIP Trunk Security Profiles)] ページで、[SIP トランク セキュリティプロファイルを作成する](#)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を選択します。
- ステップ 8 [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)] ページで、**[X.509 サブジェクト名 (X.509 Subject Name)]** に入力した値が対応する Unity Connection サーバーの FQDN であることを確認します。
- ステップ 9 [TLS 暗号の設定](#)の項の説明に従って、TLS 暗号を設定します。

## TLS 暗号の設定

次に、Unity Connection および Cisco Unified CM で TLS 暗号オプションを設定する手順を示します。

- ステップ 1 Cisco Unified CM Administration で、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] の順に選択します。
- ステップ 2 [セキュリティパラメータ (Security Parameters)] の [TLS 暗号 (TLS Ciphers)] ドロップダウンリストから適切な暗号オプションを選択します。
- ステップ 3 画面の右隅にあるナビゲーションウィンドウで、[Cisco Unified サービスアビリティ (Cisco Unified Serviceability)] を選択し、[移動 (Go)] を選択します。
- ステップ 4 [Cisco Unified サービスアビリティ (Cisco Unified Serviceability)] ページで、[ツール (Tools)] > [コントロールセンター - 機能サービス (Control Centre-Feature Services)] に移動し、[CM サービス (CM Services)] で [Cisco Call Manager] を選択します。
- ステップ 5 [再起動 (Restart)] を選択します。
- (注) Cisco Unified CM クラスタの場合は、パブリッシャサーバーとサブスクライバサーバーの両方で Cisco Call Manager サービスを再起動する必要があります。
- ステップ 6 [Cisco Unity Connection の管理 (Cisco Unity Connection Administration)] ページにサインインし、[システム設定 (System Settings)] を展開し、[全般設定 (General Configuration)] を選択します。
- ステップ 7 [TLS 暗号 (TLS Ciphers)] ドロップダウンリストから適切な暗号を選択します。
- ステップ 8 画面の右隅にあるナビゲーションウィンドウで、[Cisco Connection Serviceability] を選択し、[移動 (Go)] を選択します。
- ステップ 9 [ツール (Tools)] > [サービス管理 (Service Management)] に移動し、**Connection Conversation Manager** を停止します。Connection Conversation Manager サービスが停止したら、再度開始します。
- (注) Unity Connection クラスタの場合は、パブリッシャとサブスクライバの両方で **Connection Conversation Manager** を再起動する必要があります。

**ステップ 10** 証明書を生成、アップロードするのセクションの説明に従って、RSA および EC キーベースの証明書を生成してアップロードします。

次の表に、RSA または ECDSA 暗号の優先順に TLS 暗号オプションを示します。

表 22: TLS 暗号オプションと優先順位

TLS 暗号オプション	TLS 暗号 (優先順)
最も強力: AES-256 SHA-384 のみ: RSA 推奨	<ul style="list-style-type: none"> <li>• TLS_ECDHE_RSA_WITH_A</li> <li>• TLS_ECDHE_ECDSA_WITH</li> </ul>
強力: AES-256 SHA-384 のみ: ECDSA 推奨	<ul style="list-style-type: none"> <li>• TLS_ECDHE_ECDSA_WITH</li> <li>• TLS_ECDHE_RSA_WITH_A</li> </ul>
中: AES-256 AES-128のみ: RSA 推奨	<ul style="list-style-type: none"> <li>• TLS_ECDHE_RSA_WITH_A</li> <li>• TLS_ECDHE_ECDSA_WITH</li> <li>• TLS_ECDHE_RSA_WITH_A</li> <li>• TLS_ECDHE_ECDSA_WITH</li> </ul>
中: AES-256 AES-128 のみ: ECDSA 推奨	<ul style="list-style-type: none"> <li>• TLS_ECDHE_ECDSA_WITH</li> <li>• TLS_ECDHE_RSA_WITH_A</li> <li>• TLS_ECDHE_ECDSA_WITH</li> <li>• TLS_ECDHE_RSA_WITH_A</li> </ul>
すべての暗号方式: RSA 推奨 (デフォルト)	<ul style="list-style-type: none"> <li>• TLS_ECDHE_RSA_WITH_A</li> <li>• TLS_ECDHE_ECDSA_WITH</li> <li>• TLS_ECDHE_RSA_WITH_A</li> <li>• TLS_ECDHE_ECDSA_WITH</li> <li>• TLS_RSA_WITH_AES_128_G</li> </ul>
すべての暗号方式: ECDSA優先	<ul style="list-style-type: none"> <li>• TLS_ECDHE_ECDSA_WITH</li> <li>• TLS_ECDHE_RSA_WITH_A</li> <li>• TLS_ECDHE_ECDSA_WITH</li> <li>• TLS_ECDHE_RSA_WITH_A</li> <li>• TLS_RSA_WITH_AES_128_G</li> </ul>

Unity Connection と Cisco Unified Communications Manager 間のネゴシエーションは、次の条件の TLS 暗号設定に依存します。

- Unity Connection がサーバーとして機能する場合、TLS 暗号ネゴシエーションは、Cisco Unified CM によって選択された設定に基づきます。
  - ECDSA ベースの暗号がネゴシエートされる場合、EC キーベースの tomcat-ECDSA 証明書が SSL ハンドシェイクで使用されます。
  - RSA ベースの暗号がネゴシエートされる場合、RSA キーベースの Tomcat 証明書が SSL ハンドシェイクで使用されます。

- Unity Connection がクライアントとして機能する場合、TLS 暗号ネゴシエーションは Unity Connection によって選択された設定に基づきます。

## SRTP 暗号の設定

Next Generation Security over RTP インターフェイスを有効にするには、次のように SRTP 暗号を設定します。

- 
- ステップ 1** Cisco Unified CM Administration で、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] の順に選択します。
- ステップ 2** [セキュリティパラメータ (Security Parameters)] の [SRTP 暗号 (SRTP Ciphers)] ドロップダウンリストから適切な暗号オプションを選択します。
- ステップ 3** 画面の右隅にあるナビゲーションウィンドウで、[Cisco Unified サービスアビリティ (Cisco Unified Serviceability)] を選択し、[移動 (Go)] を選択します。
- ステップ 4** [Cisco Unified サービスアビリティ (Cisco Unified Serviceability)] ページで、[ツール (Tools)] > [コントロールセンター - 機能サービス (Control Centre-Feature Services)] に移動し、[CM サービス (CM Services)] で [Cisco Call Manager] を選択します。
- ステップ 5** [再起動 (Restart)] を選択します。
- (注) Cisco Unified CM クラスタの場合は、パブリッシャサーバーとサブスクリバサーバーの両方で Cisco Call Manager サービスを再起動する必要があります。
- ステップ 6** [Cisco Unity Connection の管理 (Cisco Unity Connection Administration)] ページにサインインし、[システム設定 (System Settings)] を展開し、[全般設定 (General Configuration)] を選択します。
- ステップ 7** [SRTP 暗号 (SRTP Ciphers)] ドロップダウンリストから適切な暗号を選択します。
- ステップ 8** 画面の右隅にあるナビゲーションウィンドウで、[Cisco Connection Serviceability] を選択し、[移動 (Go)] を選択します。
- ステップ 9** [ツール (Tools)] > [サービス管理 (Service Management)] に移動し、**Connection Conversation Manager** を停止します。Connection Conversation Manager サービスが停止したら、再度開始します。
- (注) Unity Connection クラスタの場合は、パブリッシャとサブスクリバの両方で **Connection Conversation Manager** を再起動する必要があります。
- 

次の表に、RSA または ECDSA 暗号の優先順に SRTP 暗号オプションを示します。

表 23: SRTP 暗号オプションと優先順位

SRTP 暗号オプション	優先順位の SRTP
すべてのサポートされている AES-256 および AES-128 暗号方式	<ul style="list-style-type: none"><li>• AEAD_AES_256_GCM</li><li>• AEAD_AES_128_GCM</li><li>• AES_CM_128_HMAC_SHA1_32</li><li>• AES_CM_128_HMAC_SHA1_80</li></ul>
AEAD AES-256、AES-28 GCM ベース暗号方式	<ul style="list-style-type: none"><li>• AEAD_AES_256_GCM</li><li>• AEAD_AES_128_GCM</li></ul>
AEAD AES256 GCM ベースの暗号方式のみ	AEAD_AES_256_GCM





## 第 4 章

# 統合をテストする

Cisco Unity Connection と電話システムが正しく連動しているかどうかをテストするには、次の手順を実行します。

いずれかの手順で失敗が示された場合は、必要に応じて次のドキュメントを参照してください。

- [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/15/install\\_upgrade/guide/b\\_15cuciumg.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/install_upgrade/guide/b_15cuciumg.html) にある『Cisco Unity Connection インストール、アップグレード、およびメンテナンスガイド、リリース 15』の「Unity Connection をインストールする」の章。
- [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/15/troubleshooting/guide/b\\_15cuctsg.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/troubleshooting/guide/b_15cuctsg.html) にある『Cisco Unity Connection トラブルシューティングガイド、リリース 15』
- このガイドで前述したセットアップ情報。
  - テレフォニー統合をテストする (49 ページ)
  - テスト設定をセットアップする (50 ページ)
  - リリース転送を使用した外線コールをテストする (51 ページ)
  - メッセージを再生する (52 ページ)
  - 管理された転送を設定する (52 ページ)
  - 管理された転送をテストする (53 ページ)
  - テストユーザーを削除する (53 ページ)

## テレフォニー統合をテストする

**ステップ 1** Cisco Unity Connection Administration の [テレフォニー統合 (Telephony Integrations) ] から [電話システム (Phone System) ] を選択します。

**ステップ 2** 設定をテストする必要がある電話システムをリストから選択します。

**ステップ 3** [関連リンク (Related Links) ] ドロップダウンリストで、[テレフォニー設定の確認 (Check Telephony Configuration) ] を選択し、[移動 (Go) ] を選択して電話システム統合設定を確認します。

テストが成功しなかった場合、タスク実行結果にはトラブルシューティングのステップが書かれた 1 つ以上のメッセージが表示されます。問題を解決した後に、もう一度接続をテストしてください。

**ステップ 4** [タスクの実行結果 (Task Execution Results)] ウィンドウで、[閉じる (Close)] を選択します。

## テスト設定をセットアップする

- ステップ 1** Unity Connection が接続されている同じ電話システムに 2 つのテスト内線番号 (電話機 1 と電話機 2) を設定します。
- ステップ 2** 着信に応答しない場合に Cisco Unity Connection のパイロット番号に着信を転送するように電話機 1 を設定します。
- 電話システムは、4 回以上の呼び出し音で Unity Connection パイロット番号にコールを転送する必要があります。そうしないと、テストが失敗する可能性があります。
- ステップ 3** Unity Connection Administration で、[ユーザー (Users)] を展開し、次に [ユーザー (Users)] を選択します。
- ステップ 4** [ユーザーの検索 (Search Users)] ページで、テストに使用するユーザーの表示名を選択します。このユーザーの内線は、電話機 1 の内線である必要があります。
- ステップ 5** [ユーザーの基本設定の編集 (Edit User Basics)] ページで、[次回ログイン時に自己登録を設定する (Set for Self-enrollment at Next Login)] チェックボックスをオフにします。
- ステップ 6** [音声名 (Voice Name)] フィールドに、テストユーザーの録音名を録音します。
- ステップ 7** [保存 (Save)] を選択します。
- ステップ 8** [編集 (Edit)] メニューで、[メッセージ待機インジケータ (Message Waiting Indicators)] を選択します。
- ステップ 9** [メッセージ待機インジケータ (Message Waiting Indicators)] ページで、メッセージ待機インジケータを選択します。テーブルにメッセージ待機の兆候がない場合は、[新規追加 (Add New)] を選択します。
- ステップ 10** [メッセージ待機インジケータの編集 (Edit Message Waiting Indicator)] ページで、次の設定を入力します。

表 24: MWI の編集ページの設定

フィールド	設定
有効 (Enabled)	テストユーザーの MWI を有効にするには、このチェックボックスをオンにします。
表示名 (Display Name)	デフォルトを受け入れるか、別の名前を入力します。



フィールド	設定
ユーザーの内線番号を継承 (Inherit User's Extension)	電話機 1 で MWI を有効にするには、このチェックボックスをオンにします。

- ステップ 11 [保存 (Save)] を選択します。
- ステップ 12 [編集 (Edit)] メニューで、[転送オプション (Transfer Options)] を選択します。
- ステップ 13 [転送オプション (Transfer Options)] ページで、アクティブなオプションを選択します。
- ステップ 14 [転送オプションの編集 (Edit Transfer Option)] ページの [転送アクション (Transfer Action)] で、[内線番号 (Extension)] オプションを選択し、電話機 1 の内線番号を入力します。
- ステップ 15 [転送タイプ (Transfer Type)] フィールドで、[スイッチヘリリースする (Release to Switch)] を選択します。
- ステップ 16 [保存 (Save)] を選択します。
- ステップ 17 Cisco Unity Connection Administration ウィンドウを最小化します。
- Cisco Unity Connection Administration ウィンドウは後の手順で再度使用するため、閉じないでください。
- ステップ 18 Real-Time Monitoring Tool (RTMT) にサインインします。
- ステップ 19 [Unity Connection] メニューで、[ポートモニター (Port Monitor)] を選択します。[ポートモニター (Port Monitor)] ツールが右側のペインに表示されます。
- ステップ 20 右側のペインで、[ポーリングの開始 (Start Polling)] を選択します。[ポートモニター (Port Monitor)] には、発信したコールを処理しているポートが表示されます。

## リリース転送を使用した外線コールをテストする

- ステップ 1 電話機 2 で、外線に接続するために必要なアクセスコードを入力し、外部の発信者が Unity Connection に直接ダイヤルするために使用する番号を入力します。
- ステップ 2 [ポートモニター (Port Monitor)] で、このコールを処理するポートをメモします。
- ステップ 3 ガイダンスが再生されたら、電話機 1 の内線番号を入力します。ガイダンスが再生されるということは、ポートが正しく設定されていることを意味します。
- ステップ 4 電話機 1 が鳴り、電話機 2 で呼び出し音が聞こえることを確認します。呼び出し音が聞こえるということは、Unity Connection がコールを正しくリリースし、電話機 1 に転送したことを意味します。
- ステップ 5 電話機 1 を応答しないままにして、コールを処理するポートの状態が「アイドル」に変わることを確認します。この状態は、リリース転送が成功したことを意味します。
- ステップ 6 電話システムが待機するように設定されている呼び出し回数の後で、コールが Unity Connection に転送され、テストユーザーのグリーティングが再生されることを確認します。グリーティングが再生されるということは、電話システムが未応答のコールとコール転送情報を Unity Connection に転送し、Unity Connection は情報を正しく解釈したことを意味します。

- ステップ7 [ポートモニター (Port Monitor)] で、このコールを処理するポートをメモします。
- ステップ8 テストユーザーにメッセージを残して、電話機2を切ります。
- ステップ9 [ポートモニター (Port Monitor)] で、コールを処理するポートの状態が「アイドル」に変わることを確認します。この状態は、コールが終了したときにポートが正常に解放されたことを意味します。
- ステップ10 電話機1のMWIがアクティブになっていることを確認します。アクティブになったMWIは、電話システムとUnity Connectionが正常に統合され、MWIをオンにすることを意味します。

---

## メッセージを再生する

- ステップ1 電話機1から、Unity Connectionの内部パイロット番号を入力します。
- ステップ2 パスワードの入力を求められたら、テストユーザーのパスワードを入力します。パスワードのリクエストが聞こえたということは、電話システムが必要なコール情報をUnity Connectionに送信し、Unity Connectionが情報を正しく解釈したことを意味します。
- ステップ3 テストユーザーの名前の録音が再生されることを確認します（テストユーザーの名前を録音しなかった場合は、電話機1の内線番号が再生されます）。録音名が再生されるということは、Unity Connectionが内線番号によってユーザーを正しく識別したことを意味します。
- ステップ4 メッセージの再生
- ステップ5 メッセージを聞いたら、そのメッセージを削除します。
- ステップ6 電話機1のMWIが非アクティブになっていることを確認します。非アクティブになったMWIは、電話システムとCisco Unity Connectionが正常に統合され、MWIをオフにすることを意味します。
- ステップ7 電話機1を切断します。
- ステップ8 [ポートモニター (Port Monitor)] で、コールを処理するポートの状態が「アイドル」に変わることを確認します。この状態は、コールが終了したときにポートが正常に解放されたことを意味します。

---

## 管理された転送を設定する

- ステップ1 Cisco Unity Connection Administrationのテストユーザーの[転送オプションの編集 (Edit Transfer Option)] ページで、[転送タイプ (Transfer Type)] フィールドで[転送の監視 (Supervise Transfer)] を選択します。
- ステップ2 [呼び出し回数 (Rings to Wait For)] フィールドに3と入力します。
- ステップ3 [保存 (Save)] を選択します。
- ステップ4 Cisco Unity Connection Administration ウィンドウを最小化します。  
Cisco Unity Connection Administration ウィンドウは後の手順で再度使用するため、閉じないでください。

## 管理された転送をテストする

- 
- ステップ 1 電話機 2 で、外線に接続するために必要なアクセスコードを入力し、外部の発信者が Unity Connection に直接ダイヤルするために使用する番号を入力します。
  - ステップ 2 [ポートモニター (Port Monitor) ] で、このコールを処理するポートをメモします。
  - ステップ 3 ガイダンスが再生されたら、電話機 1 の内線番号を入力します。ガイダンスが再生されるということは、ポートが正しく設定されていることを意味します。
  - ステップ 4 電話機 1 が鳴り、電話機 2 で呼び出し音が聞こえないことを確認します。代わりに、電話システムがコールが保留中であることを示す通知 (音楽など) が再生されます。
  - ステップ 5 電話機 1 を応答しないままにして、コールを処理するポートの状態が「ビジー」のままであることを確認します。この状態で、保留中であるという通知が聞こえた場合は、Unity Connection が転送を監視していることを意味します。
  - ステップ 6 呼び出し音が 3 回鳴った後、テストユーザーのグリーティングが再生されることを確認します。グリーティングが再生されるということは、Cisco Unity Connection が監視転送コールを正常に呼び戻したことを意味します。
  - ステップ 7 グリーティング中に電話機 2 を切ります。
  - ステップ 8 [ポートモニター (Port Monitor) ] で、コールを処理するポートの状態が「アイドル」に変わることを確認します。この状態は、コールが終了したときにポートが正常に解放されたことを意味します。
  - ステップ 9 [ポーリングの停止 (Stop Polling) ] を選択します。
  - ステップ 10 RTMT を終了します。
- 

## テストユーザーを削除する

Unity Connection が Cisco Unified CM 認証または暗号化用に設定されている場合は、次の手順を実行します。

- 
- ステップ 1 Unity Connection Administration で、[ユーザー (Users) ] を展開し、次に [ユーザー (Users) ] を選択します。
  - ステップ 2 [ユーザーの検索 (Search Users) ] ページで、テストユーザーの左側にあるチェックボックスをオンにします。
  - ステップ 3 [選択項目の削除 (Delete Selected) ] を選択します。
-

## Cisco Unified CM の認証と暗号化をテストする

---

- ステップ1 電話機 1 から、Unity Connection の内部パイロット番号をダイヤルします。
  - ステップ2 電話機の LCD に認証アイコンや暗号化アイコンが表示されていることを確認します。
  - ステップ3 電話機 1 を切断します。
-



## 付録 **A**

# Cisco Unified Communications Manager 統合 へ Cisco Unified Communications Manager Express を追加する

Cisco Unity Connection は、Cisco Unified CM サーバーと Cisco Unified Communications Manager Express サーバーのポートグループを持つ Cisco Unified Communications Manager 電話システム統合を統合できます。通常、この設定は、WAN リンクがダウンしたときにブランチオフィスでコール処理機能を確保するために使用されます。

ただし、次の考慮事項があります。

- Cisco Unified CM Express のバージョンと Cisco Unity Connection のバージョンは、<http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-device-support-tables-list.html>にある Cisco Unity Connection の互換性マトリックスでサポートされている組み合わせである必要があります。
- Cisco Unified CM 電話システムの統合は、通常、Cisco Unified CM Express サーバーを追加する前にすでに作成されています。
- [Cisco Unified Communications Manager 統合へ Cisco Unified Communications Manager Express を追加する \(55 ページ\)](#)

## Cisco Unified Communications Manager 統合へ Cisco Unified Communications Manager Express を追加する

Cisco Unity Connection は、Cisco Unified CM サーバーと Cisco Unified Communications Manager Express サーバーのポートグループを持つ Cisco Unified Communications Manager 電話システム統合を統合できます。通常、この設定は、WAN リンクがダウンしたときにブランチオフィスでコール処理機能を確保するために使用されます。

ただし、次の考慮事項があります。

- Cisco Unified CM Express のバージョンと Cisco Unity Connection のバージョンは、<http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-device-support-tables-list.html>にある Cisco Unity Connection の互換性マトリックスでサポートされている組み合わせである必要があります。
- Cisco Unified CM 電話システムの統合は、通常、Cisco Unified CM Express サーバーを追加する前にすでに作成されています。

## Cisco Unified CM 電話システム統合へ Cisco Unified CM Express サーバーを追加する

- ステップ 1** Cisco Unity Connection Administration で、[テレフォニー統合 (Telephony Integrations)] を展開し、[ポートグループ (Port Group)] を選択します。
- ステップ 2** [ポートグループの検索 (Search Port Groups)] ページで、Cisco Unified CM サーバーのポートグループの名前を選択します。
- ステップ 3** [ポートグループの基本 (Port Group Basics)] ページの [編集 (Edit)] メニューで、[サーバー (Servers)] を選択します。
- ステップ 4** [サーバーの編集 (Edit Servers)] ページの [Cisco Unified Communications Manager] で、[追加 (Add)] を選択します。
- ステップ 5** 新しい行に、以下の設定を入力します。

表 25: Cisco Unified CM Express サーバーの設定

フィールド	設定
順位 (Order)	Cisco Unified CM サーバーよりも大きい数値を入力します。最も小さい数字はプライマリ Cisco Unified CM サーバーで、それよりも大きい数字はセカンダリサーバーを表します。
IPv4 アドレス/ホスト名 (IPv4 Address or Host Name)	Cisco Unified CM ポートグループに追加する Cisco Unified CM Express サーバーの IPv4 アドレス (またはホスト名) を入力します。
IPv6 アドレス/ホスト名 (IPv6 Address or Host Name)	Cisco Unified CM Express の統合には、このフィールドを使用しないでください。IPv6 は、Cisco Unity Connection と Cisco Unified CM Express の間ではサポートされていません。
IP アドレスまたはホスト名 (IP Address or Host Name)	Cisco Unified CM ポートグループに追加する Cisco Unified CM Express サーバーの IP アドレス (またはホスト名) を入力します。
ポート (Port)	Cisco Unified CM ポートグループに追加する Cisco Unified CM Express サーバーの TCP ポートを入力します。デフォルト設定を使用することを推奨します。

フィールド	設定
TLS ポート (TLS Port)	Cisco Unified CM ポートグループに追加する Cisco Unified CM Express サーバーの TLS ポートを入力します。デフォルト設定を使用することを推奨します。

- ステップ 6** [保存 (Save)] を選択します。
- ステップ 7** [編集 (Edit)] メニューで、[詳細設定 (Advanced Settings)] を選択します。
- ステップ 8** [詳細設定の編集 (Edit Advanced Settings)] ページの [応答後の遅延 (Delay After Answer)] フィールドに **1000** と入力し、[保存 (Save)] を選択します。
- ステップ 9** [編集 (Edit)] メニューで、[ポートグループの基本設定 (Port Group Basics)] を選択します。
- ステップ 10** [ポートグループの基本設定 (Port Group Basics)] ページで、[リセット (Reset)] を選択します。
- ステップ 11** リセットするとすべてのコールトラフィックが終了するというプロンプトが表示されたら、[OK] を選択します。
- ステップ 12** [関連リンク (Related Links)] ドロップダウンリストで、[ポートグループのテスト (Test Port Group)] を選択し、[実行 (Go)] を選択して Cisco Unified CM Express ポートグループの設定を確認します。
- ステップ 13** テストによって進行中のコールが終了することを確認するプロンプトが表示されたら、[OK] を選択します。
- テストが成功しなかった場合、タスク実行結果にはトラブルシューティングのステップが書かれた 1 つ以上のメッセージが表示されます。問題を解決した後に、もう一度接続をテストしてください。
- ステップ 14** [タスクの実行結果 (Task Execution Results)] ウィンドウで、[閉じる (Close)] を選択します。
- ステップ 15** Cisco Unity Connection Administration からサインアウトします。

## Cisco Unified Survivable Remote Site Telephony (SRST) ルータを使用する

Cisco Unified Survivable Remote Site Telephony (SRST) ルータがネットワークの一部であり、Cisco Unified SRST ルータが Cisco Unified CM からコール処理機能を引き継ぐ場合 (WAN リンクがダウンしている場合など)、ブランチオフィスの電話は、引き続き機能します。ただし、この状況では、統合機能には次の制限があります。

- **通話中グリーティングへの通話転送** : Cisco Unified SRST ルータが PSTN に対して FXO/FXS 接続を使用している状況で、分散拠点から Unity Connection に着信が転送された場合、通話中グリーティングを再生することはできません。
- **内線グリーティングへの通話転送** : Cisco Unified SRST ルータが PSTN に対して FXO/FXS 接続を使用している状況で、分散拠点から Cisco Unity Connection に着信が転送された場合、内線グリーティングを再生することはできません。PSTN は FXO 回線の発番号を提供するため、発信者はユーザとして識別されません。

- **着信転送**：PSTNに到達するにはアクセスコードが必要であるため、Unity Connection から支社への着信転送は失敗します。
- **識別されているユーザーのメッセージ**：Cisco Unified SRST ルータが PSTN に対して FXO/FXS 接続を使用し、支社のユーザーがメッセージを残したり通話を転送したりする場合、そのユーザーは識別されません。発信者は、身元不明発信者と表示されます。
- **メッセージ受信インジケータ**：MWI は支社の電話機では更新されません。そのため、新規メッセージが到着した場合や、すべてのメッセージを聞いた場合、MWI はその状況を正しく反映しません。WAN リンクが再確立された場合は、MWI を再同期化することをお勧めします。
- **ルーティング規則**：Cisco Unified SRST ルータが PSTN に対して FXO/FXS 接続を使用している状況で、分散拠点から Unity Connection に着信が到達した場合（一般の着信または転送呼）、着信サービスは失敗します。

Cisco Unified SRST ルータが PRI/BRI 接続を使用している場合、分散拠点から Unity Connection への通話の発信者 ID が PSTN によって提供される完全な番号（局番および内線）になる場合があります。そのため、Unity Connection ユーザーの内線と一致しない場合があります。その場合は、代行内線番号を使用して Unity Connection に発信者 ID を認識させることができます。

SRST を使用する場合は、Redirected Dialed Number Information Service (RDNIS) をサポートする必要があります。

Cisco Unified SRST ルータの設定については、<http://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/products-installation-and-configuration-guides-list.html> にある、該当する『Cisco Unified SRST システムアドミニストレーターガイド』の「ボイスメールと Cisco Unified SRST を統合する」の章を参照してください。

## AARを経由したルーティングされたボイスメールコールにおけるRDNISの送信不能の影響

自動代替ルーティング（AAR）を使用する場合は、RDNIS がサポートされている必要があります。

- AAR では、WAN が加入過多の状態になった場合に、PSTN を介して通話を転送できます。ただし、PSTN を介して再転送される場合は、RDNIS が影響を受けることがあります。Cisco Unity Connection がメッセージングクライアントに対してリモートである場合は、正しくない RDNIS 情報によって、AAR が PSTN を介して再ルーティングするボイスメールコールに影響が及ぶことがあります。RDNIS 情報が誤っている場合、通話はダイヤル先のユーザーのボイスメールボックスに到達せず、代わりに自動受付のプロンプトを受信します。その場合、発信者は、到達先の内線番号を再入力するように要求されることがあります。この動作は、主に、電話通信事業者がネットワークを介した RDNIS を保証できない場合の問題です。通信事業者が RDNIS の正常な送信を保証できない理由は数多くあります。通信事業者に問い合わせて、回線のエンドツーエンドで RDNIS の送信を保証しているかどうかを確認してください。オーバーサブスクリプションの状態になった WAN に対



して AAR を使用する代わりに方法は、単に、オーバーサブスクリプションの状況で発信者にリオーダー トーンが聞こえるようにすることです。



## 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。