



SIP トランクの設定

- [SIP トランクの概要, 1 ページ](#)
- [SIP トランク設定の前提条件, 3 ページ](#)
- [SIP トランクの設定タスク フロー, 3 ページ](#)

SIP トランクの概要

コール制御シグナリングの SIP を展開している場合、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、リモートクラスタ、またはセッション管理エディションなどの外部デバイスに Cisco Unified Communications Manager を接続する SIP トランクを設定します。

Cisco Unified CM の管理の内部で、[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。

SIP トランクには最大 16 の異なる接続先アドレスを割り当てられます。これには、IPv4 または IPv6 アドレッシング、完全修飾ドメイン名、単一の DNS SRV レコードを使用します。

SIP トランクの次の機能を設定できます。

- 回線と名前の識別サービス
- Delayed Offer、Early Offer、Best Effort Early Offer
- シグナリング暗号化と認証
- SRTP によるメディア暗号化
- IPv6 デュアル スタックのサポート
- [ビデオ (Video)]
- BFCP と共有するプレゼンテーション
- 遠端カメラ制御
- DTMF リレー

- 発信側の正規化
- URI ダイヤル
- Q.SIG サポート
- T.38 ファックス サポート
- SIP オプション
- DTMF シグナリングの選択



(注) クラスタ A からクラスタ B で小規模 IP テレフォニー (SIPT) の Q.SIG を有効にした場合、匿名またはテキストで "INVITE" を受領しても、Cisco Unified Communications Manager は "INVITE" を Q.SIG データにエンコードしません。リーフ クラスタで同じようにデコードすると、何も表示されず、空の番号が転送されます。



(注) Q.SIG を有効にすると、URI ダイヤルが予期したとおりに応答しません。Q.SIG を無効にすると、Cisco Call Back が 2 つのクラスタ間で応答しません。

IPv6 デュアル スタックのサポート

また、一般的なデバイス設定で IP アドレッシング モードを設定することで、デュアル スタック サポートで SIP トランクを設定することもできます。詳細をここに追加します。

安全な SIP トランク

SIP トランク セキュリティ プロファイルを設定して、ダイジェスト認証、シグナリングとメディアの暗号化などのセキュリティで自分のトランクを設定することもできます。このプロファイルにはダイジェスト認証や TLS シグナリングが含まれ、そのプロファイルをネットワークの SIP トランクに関連付けます。発信メディアを暗号化するには、SRTP メディアを有効にするためにトランクを設定する必要もあります。

SIP トランクのセキュリティプロファイル概要

ネットワークの各 SIP 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る必要があります。デフォルトでは、Cisco Unified Communications Manager がすべての SIP トランクに、事前に定義された非セキュアな SIP トランク セキュリティ プロファイルを適用します。

SIP トランク セキュリティ プロファイルを使用することにより、ネットワークの SIP トランクの TLS シグナリング暗号化とダイジェスト認証のようなセキュリティを設定できます。SIP トランク セキュリティ プロファイルを設定し、そのプロファイルを SIP トランクに割り当てると、プロファイルのセキュリティの設定がトランクに適用されます。

ネットワークに異なる SIP トランクの設定がある場合に、複数の SIP トランク セキュリティ プロファイルを設定することで、さまざまなセキュリティ要件に対応できます。



(注) ネットワークにセキュリティを設定するには、CTL クライアントをセットアップし、IPSec を設定する必要もあります。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。

SIP トランク設定の前提条件

SIP トランクを設定する前に、次の手順を実行します。

- トランク接続を把握できるように、ネットワーク トポロジを計画します。
- トランクの接続先のデバイスと、それらのデバイスが SIP をどのように実装するかを確実に理解します。それらのデバイスが SIP を実装している場合は、SIP 正規化スクリプトを適用する必要が生じることがあります。
- トランクの SIP プロファイルを設定します。

さらに、SIP トランクを設定する前に、次を設定します。

- [SIP の正規化および透明性設定のタスク フロー](#)
- [SIP プロファイルの設定](#)

SIP トランクの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	SIP トランク セキュリティ プロファイルの設定 , (4 ページ)	SIP トランクに適用する任意のセキュリティ設定を使用して、SIP トランクセキュリティプロファイルを設定します。たとえば、ダイジェスト認証、デバイスセキュリティモード、および SIP シグナリングの TLS 暗号化を設定できます。 SIP トランクセキュリティプロファイルを設定しなければ、デフォルトで、Cisco Unified Communications Manager によって非セキュアな SIP トランクセキュリティプロファイルが適用されます。

	コマンドまたはアクション	目的
ステップ 2	共通デバイス設定の実行, (5 ページ)	トランクの共通デバイス設定を実行します。デュアルスタック トランクの場合、IP アドレッシングの優先順位を設定します。
ステップ 3	SIP トランクの設定, (6 ページ)	ネットワークの SIP トランクを設定します。[トランクの設定 (Trunk Configuration)] ウィンドウで、トランクの SIP 設定を実行します。SIP プロファイル、SIP トランクセキュリティ プロファイル、および共通デバイス設定を SIP トランクに割り当てます。また、トランク接続に必要な SIP の正規化および透明性スクリプトを割り当てます。たとえば、SIP トランクが Cisco TelePresence VCS に接続する場合、 <i>vcs-interop</i> スクリプトを SIP トランクに割り当てる必要があります。

SIP トランク セキュリティ プロファイルの設定

ネットワークで SIP トランクに割り当てられる SIP トランク セキュリティ プロファイルを設定するには、次の手順を使用します。ダイジェスト認証や TLS 暗号化シグナリングのようなセキュリティ機能を設定するために、SIP トランクにプロファイルを割り当てることができます。SIP トランク セキュリティ プロファイルを設定しない場合、Cisco Unified Communications Manager により、ネットワークの SIP トランクにセキュアではないプロファイルが割り当てられます。

手順

- ステップ 1 Cisco Unified CM の管理から、[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 [新規追加 (Add New)] をクリックします。
- ステップ 3 TLS の SIP シグナリング暗号化を有効にするには、次の手順を実行します。
 - a) [デバイスセキュリティ モード (Device Security Mode)] ドロップダウン リスト ボックスから、[暗号化 (Encrypted)] を選択します。
 - b) [着信転送タイプ (Incoming Transport Type)] と [発信転送タイプ (Outgoing Transport Type)] ドロップダウン リスト ボックスから、[TLS (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。フィールドとその説明については、オンラインヘルプを参照してください。

ステップ 6 [保存 (Save)] をクリックします。
(注) ネットワーク セキュリティ セットアップの詳細については、『Cisco Unified Communications Manager セキュリティ ガイド』を参照してください。

次の作業

SIP 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るには、次の手順を使用します。

- [SIP トランクの設定, \(6 ページ\)](#)

共通デバイス設定の実行

共通デバイス設定は、ユーザ固有のサービス属性と機能属性で構成されています。デュアルスタックの電話やトランクを設定している場合、共通デバイス設定で IP アドレッシングモードの優先順位を設定できます。

手順

ステップ 1 Cisco Unified CM の管理から、[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 (Add New)] をクリックします。

ステップ 3 [共通デバイス設定 (Common Device 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 4 SIP トランクまたは SCCP 電話機では、[IP アドレッシングモード (IP Addressing Mode)] ドロップダウンリストボックスの値を選択してください。

- [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]

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 5 デュアル スタックの電話やトランクでは、[シグナリング用 IP アドレッシング モード優先設定 (IP Addressing Mode Preference for Signaling)] ドロップダウン リスト ボックスで次の IP アドレッシング モード優先設定を入力します。

- [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、[シグナリング用 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 6 [保存 (Save)] をクリックします。

SIP トランクの設定

SIP トランクの設定を行うには、次の手順を実行します。

はじめる前に

[SIP トランク セキュリティ プロファイルの設定, \(4 ページ\)](#)

手順

ステップ 1 Cisco Unified CM の管理から、[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 ボックスから、[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 ボックスから、設定する SIP トランクのタイプを選択します。

- [なし (デフォルト) (None (Default))]: トランクは、コール制御検出、Extension Mobility Cross Cluster、Intercompany Media Engine、または IP Multimedia System サービス コントロールには使用されません。
- [コール制御検出 (Call Control Discovery)]: トランクはコール制御検出機能をサポートします。

- [Extension Mobility Cross Cluster] : トランクは Extension Mobility Cross Cluster をサポートしません。
- [Cisco Intercompany Media Engine] : トランクは Intercompany Media Engine (IME) をサポートします。トランク タイプを設定する前に、IME サーバがインストールされていることを確認します。
- [IP Multimedia System サービス コントロール (IP Multimedia System Service Control)] : トランクの IP Multimedia System サービス コントロールのサポートを有効にするには、このオプションを選択します。

ステップ 5 [Next] をクリックします。

ステップ 6 このトランクに共通デバイス設定を適用する場合は、[共通デバイス設定 (Common Device Configuration)] ドロップダウン リスト ボックスから設定を選択します。

ステップ 7 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) 宛先を追加するには、[+] ボタンをクリックします。SIP トランクには最大 16 個の宛先を追加できます。

ステップ 8 [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。

ステップ 9 [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、このトランクに SIP プロファイルを割り当てます。

ステップ 10 (オプション) 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 ボックスから、割り当てるスクリプトを選択します。

ステップ 11 [トランクの設定 (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 12 [保存 (Save)] をクリックします。

