SIP トランク セキュリティ プロファイルの設定

この章では、SIP トランク セキュリティ プロファイルのセットアップについて説明します。

SIP トランク セキュリティ プロファイルの設定について

Unified Communications Manager Administration では、単一のセキュリティ プロファイルを複数の SIP トランクに割り当てることができるよう、SIP トランクのセキュリティ関連の設定項目をグループ化しています。セキュリティ関連の設定には、デバイス 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があります。[Trunk Configuration] ウィンドウでセキュリティプロファイルを選択する際に、構成済みの設定を SIP トランクに適用します。

Unified Communications Manager をインストールすると、自動登録用の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 プロファイルが提供されます。SIP トランクのセキュリティ機能を有効にするには、新しいセキュリティ プロファイルを設定して、SIP トランクに適用します。トランクがセキュリティをサポートしない場合は、非セキュアプロファイルを選択してください。

セキュリティ プロファイルの設定ウィンドウに表示されるのは、SIP トランクでサポートされるセキュリティ機能だけです。

SIP トランク セキュリティ プロファイルの設定のヒント

[Unified Communications Manager Administration] で SIP トランク セキュリティ プロファイルを設定する際には以下の情報を考慮してください。

- SIP トランクを設定するときは、[Trunk Configuration] ウィンドウでセキュリティ プロファイルを選択する必要があります。デバイスがセキュリティをサポートしていない場合は、非セキュア プロファイルを選択します。
- 現在デバイスに割り当てられているセキュリティ プロファイルは削除できません。
- SIP トランクに割り当てられているセキュリティ プロファイルの設定を変更すると、再設定された設定が、そのプロファイルが割り当てられているすべての SIP トランクに適用されます。
- デバイスに割り当てられているセキュリティ ファイルの名前を変更できます。古いプロファイル名および設定が割り当てられている SIP トランクは、新しいプロファイル名および設定を受け入れます。
- Unified Communications Manager 5.0 以降のアップグレード前にデバイス セキュリティ モードを設定していた場合、Unified Communications Manager は SIP トランクのプロファイルを作成し、そのプロファイルをデバイスに適用します。

SIP トランク セキュリティ プロファイルの検索

SIP トランク セキュリティ プロファイルを検索するには、次の手順を実行します。

手順

ステップ 1 **[System]** > **[Security Profile]** > **[SIP Trunk Security Profile]** の順に選択します。

[Find and List] ウィンドウが表示されます。このウィンドウには、アクティブな（以前の）照会のレコードも表示されることがあります。

ステップ 2 データベース内のレコードをすべて表示するには、ダイアログボックスを空欄のままにして、ステップ 3 （3 ページ） に進みます。

レコードをフィルタまたは検索するには、次の手順を実行します。

a) ドロップダウン リスト ボックスで検索パラメータを選択します。
b) 次に、ドロップダウン リスト ボックスで検索パターンを選択します。
c) 必要に応じて、適切な検索テキストを指定します。

（注） 検索条件をさらに追加するには、[+] ボタンをクリックします。 条件を追加すると、指定した条件をすべて満たしているレコードが検索されます。条件を削除する場合、最後に追加した条件を削除するには、[-]ボタンをクリックします。追加した検索条件をすべて削除するには、[Clear Filter] ボタンをクリックします。

ステップ 3 [検索（Find）] をクリックします。

条件を満たしているレコードがすべて表示されます。1 ページあたりの項目の表示件数を変更するには、[Rows per Page] ドロップダウン リスト ボックスで別の値を選択します。

ステップ 4 表示されるレコードのリストから、表示するレコードへのリンクをクリックします。

（注） ソート順を逆にするには、リストのヘッダーにある上向き矢印または下向き矢印をクリックします。

ウィンドウに選択した項目が表示されます。

SIP トランク セキュリティ プロファイルの設定

SIP トランク セキュリティ プロファイルを追加、更新、またはコピーするには、次の手順を実行します。

手順

ステップ 1 [Unified Communications Manager Administration] で、**[System]** > **[Security Profile]** > **[SIP Trunk Security Profile]** 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。

a) 新しいプロファイルを追加するには、[Find] ウィンドウで [Add New] をクリックします

（プロファイルを表示してから、[Add New] をクリックすることもできます）。

各フィールドにデフォルト設定が取り込まれた設定ウィンドウが表示されます。

b) 既存のセキュリティ プロファイルをコピーするには、適切なプロファイルを見つけ、[Copy] 列内にあるそのレコード用の [Copy] アイコンをクリックします

（プロファイルを表示してから、[Copy] をクリックすることもできます）。

設定ウィンドウが表示され、設定された項目が示されます。

c) 既存のプロファイルを更新するには、SIP トランク セキュリティ プロファイルの検索 （2 ページ）の説明に従い、適切なセキュリティ プロファイルを見つけて表示します。

設定ウィンドウが表示され、現在の設定が示されます。

ステップ 3 表 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） に示すように、適切な設定を入力します。

ステップ 4 **[Save]** をクリックします。

次のタスク

セキュリティ プロファイルを作成した後、それをトランクに適用します。

SIP トランクにダイジェスト認証を設定した場合は、トランクの [SIP Realm] ウィンドウと、その SIP トランクを介して接続されるアプリケーションの [Application User] ウィンドウで、ダイジェスト クレデンシャルを設定する必要があります（まだ設定していない場合）。

SIP トランクを介して接続されるアプリケーションに対してアプリケーションレベルの許可（認証）を有効にした場合は、[Application User] ウィンドウで、そのアプリケーションに許可される方式を設定する必要があります（まだ設定していない場合）。

SIP トランク セキュリティ プロファイルの設定

次の表は、SIP トランク セキュリティ プロファイルの設定を示します。

表 *1: SIP* トランク セキュリティ プロファイルの設定

設定	説明
Name	セキュリティ プロファイルの名前を入力します。新しいプロファイルを保存すると、[Trunk Configuration] ウィンドウの [SIP Trunk Security Profile] ドロップダウン リスト ボックスにその名前が表示されます。
[Description]	セキュリティ プロファイルの説明を入力します。説明には、任意の言語で最大 50 文字を指定できますが、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。

SIP トランク セキュリティ プロファイルの設定

設定	説明
[Device Security Mode]	ドロップダウン リスト ボックスから、次のいずれかのオプションを選択します。 • [Non Secure]：イメージ認証以外のセキュリティ機能は適用されません。TCP または UDP 接続が Unified Communications Manager に対して開きます。 • **[Authenticated]**：Unified Communications Manager はトランクの整合性と認証を提供します。NULL/SHA を使用する TLS 接続が開きます。 • **[Encrypted]**：Cisco Unified Communications Manager は、トランクの整合性、認証、およびシグナリング暗号化を提供しています。AES128/SHA を使用する TLS 接続がシグナリング用に開きます。 （注） [認証済み] として選択されている [デバイスのセキュリティ プロファイル (トランク)] を使用して設定した場合、Cisco ユニファイド コミュニケーション マネージャーは、NULL_SHA 暗号を使用した TLS connection (データ暗号化なし) を開始します。 これらのトランクは、通知先デバイスが NULL_SHA 暗号をサポートしていない場合は、そのデバイスを登録したり、コールを発信したりしません。 NULL_SHA 暗号をサポートしていない通知先デバイスでは、[暗号化 (Encrypted)] として選択した [デバイスのセキュリティ プロファイル (トランク)] で設定する必要があります。このデバイス セキュリティ プロファイルを使用すると、トランクは、データの暗号化を可能にする追加の TLS 暗号を提供します。

SIP トランク セキュリティ プロファイルの設定

設定	説明
[Incoming Transport Type]	[Device Security Mode] が [Non Secure] の場合、転送タイプは TCP+UDP になります。 [Device Security Mode] が [Authenticated] または [Encrypted] の場合、転送タイプは TLS になります。 （注） Transport Layer Security（TLS）プロトコルは Unified Communications Manager とトランクとの間の接続を保護します。
[Outgoing Transport Type]	ドロップダウン リスト ボックスから適切な発信転送モードを選択します。 [Device Security Mode] が [Non Secure] の場合、TCP または UDP を選択します。 [Device Security Mode] が [Authenticated] または [Encrypted] の場合、転送タイプは TLS になります。 （注） TLS により、SIP トランクのシグナリング整合性、デバイス認証、およびシグナリングの暗号化が実現します。 ヒント Unified Communications Manager システムと TCP の再使用をサポートしない IOS ゲートウェイとの間の SIP トランクを接続する場合、出力転送タイプとして UDP を使用する必要があります。

SIP トランク セキュリティ プロファイルの設定

設定	説明
[Enable Digest Authentication]	ダイジェスト認証を有効にする場合に、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、Unified Communications Manager はトランクからのすべての SIP 要求に対してチャレンジを行います。 ダイジェスト認証ではデバイス認証、整合性、機密性は提供されません。これらの機能を使用するには、セキュリティ モードとして [Authenticated] または [Encrypted] を選択します。 **ヒント** TCP または UDP 転送を使用しているトランクで SIP トランク ユーザを認証するには、ダイジェスト認証を使用します。
[Nonce Validity Time]	ナンス値が有効な分数（秒単位）を入力します。デフォルト値は 600（10 分）です。この時間が経過すると、Unified Communications Manager は新しい値を生成します。 **（注）** ナンス値は、ダイジェスト認証をサポートする乱数であり、ダイジェスト認証パスワードの MD5 ハッシュを計算するときに使用されます。

SIP トランク セキュリティ プロファイルの設定

設定	説明
[Secure Certificate Subject or Subject Alternate Name]	このフィールドは、着信転送タイプおよび発信転送タイプに TLS を設定した場合に適用されます。 デバイス認証では、SIP トランク デバイスのセキュアな証明書のサブジェクトまたはサブジェクト代替名を入力します。Unified Communications Manager クラスタがある場合、または TLS ピアに SRV ルックアップを使用する場合は、単一のトランクは複数のホストに解決されることがあります。このように解決された場合、トランクに複数のセキュアな証明書のサブジェクトまたはサブジェクト代替名が設定されます。X.509 のサブジェクト名が複数存在する場合、スペース、カンマ、セミコロン、コロンのいずれかを入力して名前を区切ります。 このフィールドには、最大 4096 文字を入力できます。 **ヒント** サブジェクト名はソース接続の TLS 証明書に対応します。サブジェクト名が、サブジェクト名とポートで一意であることを確認します。異なる SIP トランクに同じサブジェクト名と着信ポートの組み合わせを割り当てることはできません。例: ポート 5061 の SIP TLS trunk1 は、セキュリティ保護された証明書の件名またはサブジェクト代替名 my_cm1, my_cm2 を持っています。ポート 5071 の SIP TLS trunk2 には、セキュリティで保護された証明書のサブジェクトまたはサブジェクト代替名 my_cm2, my_cm3 があります。ポート 5061 の SIP TLS trunk3 は、セキュリティで保護された証明書の件名またはサブジェクト代替名my_ccm4を含むことができますが、安全な証明書のサブジェクトまたはサブジェクト代替名 my_cm1 を含めることはできません。

SIP トランク セキュリティ プロファイルの設定

設定	説明
[Incoming Port]	着信ポートを選択します。0 ～ 65535 の範囲で一意のポート番号を入力します。着信 TCP および UDP SIP メッセージ用のデフォルト ポート値は 5060 です。着信 TLS メッセージ用の SIP セキュア ポートのデフォルト ポート値は 5061 です。入力した値は、このプロファイルを使用するすべての SIP トランクに適用されます。 **ヒント** TLS を使用するすべての SIP トランクは同じ着信ポートを共有できます。TCP + UDP を使用するすべての SIP トランクは同じ着信ポートを共有できます。同じポートで、SIP TLS 転送トランクと SIP 非 TLS 転送トランク タイプとを混在させることはできません。

SIP トランク セキュリティ プロファイルの設定

設定	説明
[Enable Application Level Authorization]	アプリケーション レベルの認証は、SIP トランクを介して接続されるアプリケーションに適用されます。 このチェックボックスをオンにする場合、[Enable Digest Authentication] チェックボックスもオンにして、トランクのダイジェスト認証を設定する必要があります。Unified Communications Manager は許可されているアプリケーション方式を確認する前に、SIP アプリケーション ユーザを認証します。 アプリケーション レベルの許可が有効な場合、トランク レベルの許可が最初に発生してからアプリケーション レベルの許可が発生するため、Unified Communications Manager は [Application User Configuration] ウィンドウで SIP アプリケーション ユーザに対して許可されたメソッドより先に、（このセキュリティ プロファイル内の）トランクに対して許可されたメソッドをチェックします。 **ヒント** アプリケーションのアイデンティティを信頼しないか、またはアプリケーションが特定のトランクで信頼されていない場合は、アプリケーション レベルの許可の使用を検討してください。つまり、アプリケーション要求は想定外の別のトランクから送信される場合もあります。

SIP トランク セキュリティ プロファイルの設定

設定	説明
[Accept Presence Subscription]	Unified Communications Manager が SIP トランク経由でのプレゼンス サブスクリプション要求を受け入れるようにするには、このチェックボックスをオンにします。 [Enable Application Level Authorization] チェックボックスをオンにしたら、[Application User Configuration] ウィンドウに移動し、この機能について許可するすべてのアプリケーション ユーザの [Accept Presence Subscription] チェックボックスをオンにします。 アプリケーション レベルの許可が有効になっている場合に、アプリケーション ユーザの [Accept Presence Subscription] チェックボックスをオンにし、トランクのこのチェックボックスをオンにしない場合、トランクに接続された SIP ユーザ エージェントに 403 エラー メッセージが送信されます。
[Accept Out-of-Dialog Refer]	Unified Communications Manager が SIP トランク経由で着信する非 INVITE、Out-of-Dialog REFER 要求を受け入れるようにするには、このチェックボックスをオンにします。 [Enable Application Level Authorization] チェックボックスをオンにしたら、[Application User Configuration] ウィンドウに移動し、このメソッドについて許可するすべてのアプリケーション ユーザの [Accept Out-of-Dialog refer] チェックボックスをオンにします。
[Accept unsolicited notification]	Unified Communications Manager が SIP トランク経由で着信する非 INVITE、Unsolicited NOTIFY メッセージを受け入れるようにするには、このチェックボックスをオンにします。 [Enable Application Level Authorization] チェックボックスをオンにしたら、[Application User Configuration] ウィンドウに移動し、このメソッドについて許可するすべてのアプリケーション ユーザの [Accept Unsolicited Notification] チェックボックスをオンにします。

SIP トランク セキュリティ プロファイルの設定

設定	説明
[Accept replaces header]	Unified Communications Manager が既存の SIP ダイアログに代わる新規の SIP ダイアログを許可するようにするには、このチェックボックスをオンにします。 [Enable Application Level Authorization] チェックボックスをオンにしたら、[Application User Configuration] ウィンドウに移動し、このメソッドについて許可するすべてのアプリケーション ユーザの [Accept Header Replacement] チェックボックスをオンにします。
[Transmit Security Status]	Unified Communications Manager が関連付けられた SIP トランクからのコールのセキュリティ アイコン ステータスを SIP ピアに送信するようにするには、この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。

SIP トランク セキュリティ プロファイルの設定

設定	説明
[SIP V.150 Outbound SDP Offer Filtering]	ドロップダウン リスト ボックスから、次のフィルタ処理オプションのいずれかを選択します。 • [Use Default Filter]：SIP トランクは [SIP V.150 Outbound SDP Offer Filtering] サービス パラメータに示されているデフォルト フィルタを使用します。このサービス パラメータを検索するには、[Unified Communications Manager Administration] で **[System]** > **[Service Parameters]** > **[Clusterwide Parameters (Device-SIP)]** に進みます。 • [No Filtering]：SIP トランクは、アウトバウンド オファーで V.150 SDP 回線のフィルタリングを行いません。 • [Remove MER V.150]：SIP トランクは、アウトバウンド オファーで V.150 MER SDP 回線を削除します。トランクが MER V.150 よりも前の Unified Communications Manager に接続する際のあいまいさを低減するには、このオプションを選択します。 • [Remove Pre-MER V.150]：SIP トランクは、アウトバウンド オファーで非 MER 対応 V.150 回線をすべて削除します。クラスタがプレ MER 回線でオファーを処理できない MER 準拠デバイスのネットワークに含まれる際のあいまいさを低減するには、このオプションを選択します。

SIP トランク セキュリティ プロファイルの設定

設定	説明
[SIP V.150 Outbound SDP Offer Filtering]	ドロップダウン リスト ボックスから、次のフィルタ処理オプションのいずれかを選択します。 • [Use Default Filter]：SIP トランクは [SIP V.150 Outbound SDP Offer Filtering] サービス パラメータに示されているデフォルト フィルタを使用します。このサービス パラメータを検索するには、[Unified Communications Manager Administration] で **[System]** > **[Service Parameters]** > **[Clusterwide Parameters (Device-SIP)]** に進みます。 • [No Filtering]：SIP トランクは、アウトバウンド オファーで V.150 SDP 回線のフィルタリングを行いません。 • [Remove MER V.150]：SIP トランクは、アウトバウンド オファーで V.150 MER SDP 回線を削除します。トランクが MER V.150 よりも前の Unified Communications Manager に接続する際のあいまいさを低減するには、このオプションを選択します。 • [Remove Pre-MER V.150]：SIP トランクは、アウトバウンド オファーで非 MER 対応 V.150 回線をすべて削除します。クラスタがプレ MER 回線でオファーを処理できない MER 準拠デバイスのネットワークに含まれる際のあいまいさを低減するには、このオプションを選択します。 （注） セキュアなコールの接続を確立するためには SIP の IOS を V.150 に設定する必要があります。IOS を Cisco Unified Communication Manager で設定する際の詳細については、http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t4/mer_cg_15_1_4M.html をご覧ください。

SIP トランク セキュリティ プロファイルの適用

[Trunk Configuration] ウィンドウでトランクに SIP トランク セキュリティ プロファイルを適用します。デバイスにセキュリティ プロファイルを適用するには、次の手順を実行します。

手順

ステップ 1 『*Administration Guide for Cisco Unified Communications Manager*』の説明に従って、トランクを検索します。

ステップ 2 [トランク設定（Trunk Configuration）] ウィンドウが表示されたら、[SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）] 設定を探します。

ステップ 3 セキュリティ プロファイルのドロップダウン リスト ボックスから、デバイスに適用するセキュリティ プロファイルを選択します。

ステップ 4 **[Save]** をクリックします。

ステップ 5 トランクをリセットするには、[Apply Config] をクリックします。

次のタスク

ダイジェスト認証を有効にしたプロファイルを SIP トランクに適用した場合は、[SIP Realm] ウィンドウでダイジェスト クレデンシャルを設定する必要があります。

アプリケーション レベルの認証を有効にしたプロファイルを適用した場合は、[Application User] ウィンドウでダイジェスト クレデンシャルと、適切な認証方法を設定する必要があります（まだ設定していない場合）。

SIP トランク セキュリティ プロファイルと SIP トランクの同期

設定変更が行われた SIP トランク セキュリティ プロファイルと SIP トランクを同期させるには、次の手順を実行します。この手順では、最小限の割り込みで未適用の設定が適用されます。（たとえば、影響を受けるデバイスの一部では、リセットまたは再起動が不要な場合があります。）

手順

ステップ 1 **[System]** > **[Security Profile]** > **[SIP Trunk Security Profile]** の順に選択します。

[Find and List SIP Trunk Security Profiles] ウィンドウが表示されます。

ステップ 2 使用する検索条件を選択します。

ステップ 3 [検索（Find）] をクリックします。

ウィンドウに検索条件と一致する SIP トランク セキュリティ プロファイルのリストが表示されます。

ステップ 4 該当する SIP トランクと同期させる SIP トランク セキュリティ プロファイルをクリックします。[SIP Trunk Security Profile Configuration] ウィンドウが表示されます。

ステップ 5 追加の設定変更を加えます。

ステップ 6 **[保存（Save）]** 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。

[Apply Configuration Information] ダイアログが表示されます。

ステップ 8 [OK] をクリックします。

SIP トランク セキュリティ プロファイルの削除

この項では、Unified Communications Manager データベースから SIP トランク セキュリティ プロファイルを削除する方法について説明します。

始める前に

[Unified Communications Manager Administration] からセキュリティ プロファイルを削除する前に、デバイスに別のプロファイルを適用するか、そのプロファイルを使用するすべてのデバイスを削除する必要があります。プロファイルを使用しているデバイスを検索するには、[SIP Trunk Security Profile Configuration] ウィンドウの [Related Links] ドロップダウン リスト ボックスで [Dependency Records] を選択し、[Go] をクリックします。

依存関係レコード機能がシステムで有効でない場合は、依存関係レコード概要ウィンドウに、依存関係レコードを有効にするために実行できる操作が表示されます。また、依存関係レコード機能に関連して CPU 負荷が高くなることについての情報も表示されます。依存関係レコードの詳細は、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

手順

ステップ 1 削除する SIP トランク セキュリティ プロファイルを探します。

ステップ 2 次のいずれかの作業を実行します。

a) 複数のセキュリティ プロファイルを削除するには、[Find and List] ウィンドウで次のいずれかの作業を実行します。

- 削除するセキュリティ プロファイルの隣にあるチェック ボックスをオンにして、[Delete Selected] をクリックします。

- [Select All] をクリックし、次に [Delete Selected] をクリックすると、設定可能なすべてのレコードが削除されます。

b) 1 つのセキュリティ プロファイルを削除するには、[Find and List] ウィンドウで次のいずれかの作業を実行します。

- 削除するセキュリティ プロファイルの隣にあるチェック ボックスをオンにして、[Delete Selected] をクリックします。
- セキュリティ プロファイルの [Name] リンクをクリックします。特定の [Security Profile Configuration] ウィンドウが表示されたら、[Delete Selected] をクリックします。

ステップ 3 削除操作を確認するプロンプトが表示されたら、[OK] をクリックして削除するか、[Cancel] をクリックして削除の操作をキャンセルします。

SIP トランク セキュリティ プロファイルに関する詳細情報の入手先

- 認証
- 連携動作
- ダイジェスト認証