電話セキュリティ プロファイルの設定

この章では、セキュリティ プロファイルの設定について説明します。

- 電話セキュリティ プロファイルの概要 （1 ページ）
- 電話セキュリティ プロファイルの設定の前提条件 （1 ページ）
- 電話セキュリティ プロファイルの検索 （2 ページ）
- 電話セキュリティ プロファイルのセットアップ （3 ページ）
- 電話セキュリティ プロファイルの設定 （4 ページ）
- 電話機へのセキュリティ プロファイルの適用 （18 ページ）
- 電話セキュリティ プロファイルと電話の同期 （19 ページ）
- 電話セキュリティ プロファイルの削除 （20 ページ）
- 電話セキュリティ プロファイルによる電話の検索 （20 ページ）

電話セキュリティ プロファイルの概要

Unified Communications Manager Administration は、電話の種類およびプロトコルのセキュリティ関連設定をセキュリティ プロファイルにグループ化し、単一のセキュリティ プロファイルを複数の電話に指定できるようにします。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、いくつかの CAPF 設定などがあります。[Phone 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、構成済みの設定を電話に適用します。

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セキュリティ プロファイル一式が提供されます。電話のセキュリティ機能を有効にするには、デバイス タイプとプロトコルに応じた新しいセキュリティ プロファイルを設定し、電話に適用する必要があります。

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、選択したデバイスとプロトコルでサポートされるセキュリティ機能だけです。

電話セキュリティ プロファイルの設定の前提条件

電話セキュリティ プロファイルを設定する前に、次の点を考慮してください。

- 電話を設定するときは、[**電話の設定（Phone Configuration**）] ウィンドウでセキュリティ プロファイルを選択します。デバイスがセキュリティまたはセキュア プロファイルをサポートしていない場合は、非セキュア プロファイルを適用します。
- 定義済みの非セキュア プロファイルは削除または変更できません。
- 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。
- 電話機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、再構成した設定が、その特定のプロファイルを割り当てられているすべての電話機に適用されます。
- 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。事前にプロファイル名および設定を割り当てられている電話機は、新しいプロファイル名および設定を受け入れます。
- [**電話の設定（Phone Configuration**）] ウィンドウに、CAPF 設定、認証モード、およびキーサイズが表示されます。MIC または LSC に関連する証明書の操作には、CAPF 設定を設定する必要があります。[**電話の設定（Phone Configuration**）] ウィンドウで次のフィールドを直接更新できます。
  - セキュリティ プロファイルで CAPF 設定を更新すると、[電話の設定（Phone Configuration）] ウィンドウ上の設定も同様に更新されます。
  - [Phone Configuration] ウィンドウで CAPF 設定を更新し、一致するプロファイルが検出されると、Unified Communications Manager は、一致するプロファイルを電話に適用します。
  - [電話の設定（Phone Configuration）] ウィンドウで CAPF 設定を更新し、一致するプロファイルが検出されない場合は、Unified Communications Manager は新しいプロファイルを作成し、そのプロファイルを電話に適用します。
- アップグレード前にデバイス セキュリティ モードを設定済みの場合は、Unified Communications Manager が設定済みのモデルとプロトコルに基づいてプロファイルを作成し、デバイスにプロファイルを適用します。
- MIC は LSC のインストール時にのみ使用することを推奨します。シスコでは LSC による Cisco Unified Communications Manager との TLS 接続の認証をサポートしています。MIC ルート証明書は侵害される可能性があるため、TLS 認証またはその他の目的に MIC を使用するように電話を設定するユーザは、ご自身の責任で行ってください。MIC が侵害された場合シスコはその責任を負いません。
- TLS 接続に LSC を使用するには、Cisco IP Phone をアップグレードし、互換性の問題を回避するために MIC ルート証明書を CallManager 信頼ストアから削除することを推奨します。

電話セキュリティ プロファイルの検索

電話セキュリティ 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 [Unified Communications Manager Administration] で、**[System]** > **[Security Profile]** > **[Phone Security Profile]** を選択します。

[Find and List Phone Security Profile] 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) 最初のドロップダウン リスト ボックスで、検索パラメータを選択します。
b) 2 番目のドロップダウン 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。

電話セキュリティ プロファイルのセットアップ

手順

ステップ 1 [Unified Communications Manager Administration] で、**[System] > [Security Profile]>[Phone 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、[新規追加（Add New）] をクリックします。

[電話セキュリティ プロファイルの設定（Phone Security Profile Configuration）] ページが表示されます。

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検索し、コピーするセキュリティ プロファイルの横にある [**コピー（Copy**）] ボタンをクリックして続行します。

c) 既存のプロファイルを更新するには、適切なセキュリティプロファイルを検索し、続行します。

[Add New] をクリックすると、各フィールドにデフォルト設定が入力された設定ウィンドウが表示されます。[Copy] をクリックすると、コピーした設定が入力された設定ウィンドウが表示されます。

ステップ 3 SCCP または SIP を実行している電話機の場合は、適切な設定を入力します。

ステップ 4 **[保存 (Save)]** をクリックします。

電話セキュリティ プロファイルの設定

次の表で、SCCP を実行している電話のセキュリティ プロファイル設定について説明します。

選択された電話タイプおよびプロトコルでサポートされる設定だけが示されています。

表 *1: SCCP* を実行している電話のセキュリティ プロファイル

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、電話タイプとプロトコルの [Phone Configuration] ウィンドウの [Device 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。 **ヒント** セキュリティ プロファイル名にデバイス モデルとプロトコルを含めると、プロファイルの検索または更新時に正しいプロファイルを検索できます。
[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。

電話セキュリティ プロファイルの設定

設定	説明
[Device Security Mode]	

設定	説明
	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]：電話には、イメージ認証、ファイル認証、デバイス認証を除くセキュリティ機能が存在していません。Unified Communications Manager への TCP 接続が開かれます。 • **[Authenticated]**：Unified Communications Managerは電話の整合性と認証を提供します。NULL/SHA を使用する TLS 接続がシグナリングに対して開きます。 • **[Encrypted]**：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。 説明したように、次の暗号方式がサポートされています。 **TLS暗号方式** このパラメータは、Unified Communication Manager で SIP TLS 接続およびインバウンドの CTI Manager TLS CTI 接続を確立するためにサポートされる暗号を定義します。 最も強力：AES-256 SHA-384 のみ：RSA 優先 • `TLS_ECDHE_RSA with AES256_GCM_SHA384` • `TLS_ECDHE_RSA with AES256_GCM_SHA384` （注） パラメータ [SRTP暗号方式（SRTP Ciphers）] の値を [最も強力 - AEAD AES-256 GCM 暗号のみ（Strongest - AEAD AES-256 GCM cipher only）] に設定することを強くお勧めします。このオプションを選択すると、電話機は認証モードで登録されません。 最も強力：AES-256 SHA-384 のみ：ECDSA 優先 • `TLS_ECDHE_ECDSA with AES256_GCM_SHA384` • `TLS_ECDHE_RSA with AES256_GCM_SHA384` （注） パラメータ [SRTP暗号方式（SRTP Ciphers）] の値を [最も強力 - AEAD AES-256 GCM 暗号のみ（Strongest - AEAD AES-256 GCM cipher only）] に設定することを強くお勧めします。このオプションを選択すると、電話機は認証モードで登録されません。 中程度：AES-256 AES-128 のみ：RSA 優先 • `TLS_ECDHE_RSA with AES256_GCM_SHA384` • `TLS_ECDHE_ECDSA with AES256_GCM_SHA384` • `TLS_ECDHE_RSA with AES128_GCM_SHA256`

設定	説明
	• TLS_ECDHE_ECDSA with AES128_GCM_SHA256 （注） このオプションを選択した場合、パラメータ [SRTP暗号方式（SRTP Ciphers）] の値を [最も強力 - AEAD AES-256 GCM 暗号のみ（Strongest - AEAD AES-256 GCM cipher only）] に設定することを強くお勧めします。このオプションを選択すると、電話機は認証モードで登録されません。 中程度：AES-256 AES-128 のみ：ECDSA 優先 • TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 • TLS_ECDHE_RSA with AES128_GCM_SHA256 （注） このオプションを選択した場合、パラメータ [SRTP暗号方式（SRTP Ciphers）] の値を [最も強力 - AEAD AES-256 GCM 暗号のみ（Strongest - AEAD AES-256 GCM cipher only）] に設定することを強くお勧めします。このオプションを選択すると、電話機は認証モードで登録されません。 すべての暗号方式: RSA優先 • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES128_GCM_SHA256 • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 • TLS_RSA with AES_128_CBC_SHA1 すべての暗号 ECDSA 優先 • TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 • TLS_ECDHE_RSA with AES128_GCM_SHA256

設定	説明
	• TLS_RSA with AES_128_CBC_SHA1 （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。
[TFTP Encrypted Config]	このチェックボックスをオンにすると、Unified Communications Manager は TFTP サーバからの電話のダウンロードを暗号化します。

電話セキュリティ プロファイルの設定

設定	説明
認証モード（Authentication Mode）	

設定	説明
	このフィールドでは、電話がCAPF証明書の処理時に使用する認証方法を選択できます。 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。 • **[By Authentication String]**：ユーザが電話に CAPF 認証文字列を入力した場合にのみ、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。 • **[By Null String]**：ユーザの介入なしで、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。 このオプションでは、セキュリティは提供されません。このオプションはセキュアな閉じた環境の場合にのみ選択することを強く推奨します。 • **[By Existing Certificate (Precedence to LSC)]**：製造元でインストールされる証明書（MIC）またはローカルで有効な証明書（LSC）が電話に存在する場合に、ローカルで有効な証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に LSC が存在する場合、電話機に MIC が存在するかどうかに関係なく、LSC によって認証が行われます。電話機に MIC と LSC が存在する場合、LSC によって認証が行われます。電話機にLSCが存在しないが、MICが存在する場合、MICによって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在することを確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。 MIC と LSC が同時に電話機に存在できる場合でも、電話機が CAPF への認証に使用する証明書は常に 1 つだけです。優先されるプライマリ証明書が何らかの理由で破損した場合、または別の証明書を使用して認証を受ける場合は、認証モードを更新する必要があります。 • **既存証明書（MIC に優先権）（By Existing Certificate (Precedence to MIC)）**：電話にLSCまたはMICが存在する場合に、製造元でインストールされる証明書をインストール/アップグレード、削除、またはトラブルシューティングします。電話機に LSC が存在する場合、電話機にMICが存在するかどうかに関係なく、LSCによって認証が行われます。電話機に LSC が存在するが、MIC が存在しない場合、LSC によって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在することを確認してください。電話に証明書が存在しない場合にこのオプションを選択すると、操作は失敗します。

設定	説明
	（注） [Phone Security Profile] ウィンドウで設定される CAPF 設定は、[Phone Configuration] ウィンドウで設定される CAPF パラメータと相互に関係します。
[Key Order]	このフィールドは、CAPF のキーの並び方を指定します。ドロップダウン リストから、次のいずれかの値を選択します。 • **[RSA Only]** • **[EC Only]** • **[EC Preferred, RSA Backup]** （注） **[Key Order]**、**[RSA Key Size]**、および **[EC Key Size]** フィールドの値に基づいて電話を追加すると、デバイス セキュリティ プロファイルがその電話に関連付けられます。 **[EC Only]**値 を選択し、**[EC Key Size]** の値を [256] ビットにすると、デバイス セキュリティ プロファイルには値 **EC-256** が付加されます。
[RSA Key Size (Bits)]	ドロップダウン リスト ボックスから、**[512]**、**[1024]**、**[2048]**、**[3072]**、または**4096** のいずれかの値を選択します。 （注） CallManager が **[Certificate Purpose]** で選択した RSA の **[key length]** が 2048 より大きいと、一部の電話モデルが登録に失敗する場合があります。Cisco Unified Reporting Tool（CURT）の [Unified CM Phone Feature List Report] で、3072/4096 RSA キー サイズ サポート機能をサポートする電話モデルについて確認できます。
[EC Key Size (Bits)]	ドロップダウン リスト ボックスから、**[256]**、**[384]**、または **[521]** のいずれかの値を選択します。

次の表で、SIP を実行している電話のセキュリティ プロファイル設定について説明します。

表 *2: SIP* を実行している電話のセキュリティ プロファイル

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、電話タイプとプロトコルの [Phone Configuration] ウィンドウの [Device 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。 **ヒント** セキュリティ プロファイル名にデバイス モデルとプロトコルを含めると、プロファイルの検索または更新時に正しいプロファイルを検索できます。
[Description]	セキュリティ プロファイルの説明を入力します。
[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。

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]：電話には、イメージ認証、ファイル認証、デバイス認証を除くセキュリティ機能が存在していません。Unified Communications Manager への TCP 接続が開かれます。 • **[Authenticated]**：Unified Communications Managerは電話の整合性と認証を提供します。NULL/SHA を使用する TLS 接続がシグナリングに対して開きます。 • **[Encrypted]**：Cisco Unified Communications Managerは電話の整合性、認証、および暗号化を提供します。シグナリングに AES128/SHA を使用する TLS 接続が開き、SRTP はすべての SRTP 対応ホップでのすべてのコールに対してメディアを伝送します。 （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。

設定	説明
[Transport Type]	[Device Security Mode] が [Non Secure] の場合は、ドロップダウン リスト ボックスから次のオプションのいずれかを選択します（一部のオプションは表示されないことがあります）。 • [TCP]：Transmission Control Protocol を選択し、パケットが送信時と同じ順序で受信されるようにします。このプロトコルを使用すると、パケットはドロップされませんが、プロトコルはセキュリティを提供しません。 • [UDP]：User Datagram Protocol を選択し、パケットがすばやく受信されるようにします。このプロトコルはパケットをドロップする可能性があり、パケットは送信された順序で受信されないことがあります。このプロトコルはセキュリティを提供しません。 • [TCP＋UDP]：TCP と UDP を組み合わせて使用する場合は、このオプションを選択します。このオプションはセキュリティを提供しません。 [Device Security Mode] が [Authenticated] または [Encrypted] の場合、転送タイプは TLS になります。TLS によって、SIP 電話のシグナリングの整合性、デバイス認証、およびシグナリング暗号化（暗号化モードのみ）が実現されます。 プロファイルで [Device Security Mode] を設定できない場合は、転送タイプは UDP になります。
[Enable Digest Authentication]	このチェックボックスをオンにした場合、Unified Communications Manager は電話からのすべての 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。
[TFTP Encrypted Config]	このチェックボックスをオンにすると、Unified Communications Manager は TFTP サーバからの電話のダウンロードを暗号化します。このオプションはシスコ製電話専用です。 **ヒント** このオプションを有効化し、対称キーを設定してダイジェスト クレデンシャルと管理パスワードを保護することをお勧めします。

設定	説明
[OAuth 認証の有効化（Enable OAuth Authentication）]	[**デバイス セキュリティ プロファイル**] ドロップダウンリストから **[暗号化 (Encrypted)] を選択**すると、このチェックボックスが使用可能になります。 このチェック ボックスをオンにすると、Unified Communications Manager では、この電話のセキュリティ プロファイルと関連付けられているデバイスが SIP OAuth ポートを使用して登録できるようになります。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 OAuth を有効にするには、次のようにします。 • [Transport Type] が [TLS] の場合： • [デバイス セキュリティモード（Device Security Mode）]は [暗号化（Encrypted）]です。 • ダイジェスト認証の無効化 • 暗号化設定は無効です。 （注） ユニファイドコミュニケーションマネージャーリリース 12.5 では、Jabber は SIP OAuth 認証をサポートしています。
[Exclude Digest Credentials in Configuration File]	このチェックボックスをオンにすると、Unified Communications Manager は TFTP サーバからの電話のダウンロードでダイジェスト クレデンシャルを除外します。このオプションは、Cisco IP Phone、7942、および 7962 (SIP のみ) に対応しています。

電話セキュリティ プロファイルの設定

設定	説明
認証モード（Authentication Mode）	

設定	説明
	このフィールドでは、電話がCAPF証明書の処理時に使用する認証方法を選択できます。このオプションはシスコ製電話専用です。 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。 • **[By Authentication String]**：ユーザが電話に CAPF 認証文字列を入力した場合にのみ、ローカルで有効な証明書をインストール/アップグレード、またはトラブルシューティングします。 • **[By Null String]**：ユーザの介入なしで、ローカルで有効な証明書をインストール/アップグレード、またはトラブルシューティングします。 このオプションではセキュリティが確保されません。したがって、このオプションはセキュアな閉じた環境の場合にのみ選択することを強く推奨します。 • **[By Existing Certificate (Precedence to LSC)]**：製造元でインストールされる証明書（MIC）またはローカルで有効な証明書（LSC）が電話に存在する場合に、ローカルで有効な証明書をインストール/アップグレード、またはトラブルシューティングします。電話機に LSC が存在する場合、電話機に MIC が存在するかどうかに関係なく、LSC によって認証が行われます。電話機に LSC が存在しないが、MIC が存在する場合、MIC によって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在することを確認してください。このオプションを選択して、電話機に証明書が存在しない場合、操作は失敗します。 MIC と LSC が同時に電話機に存在できる場合でも、電話機が CAPF への認証に使用する証明書は常に 1 つだけです。優先されるプライマリ証明書が何らかの理由で破損した場合、または別の証明書を使用して認証を受ける場合は、認証モードを更新する必要があります。 • **既存証明書（MIC に優先権）（By Existing Certificate (Precedence to MIC)）**：電話に LSC または MIC が存在する場合に、製造元でインストールされる証明書をインストール/アップグレード、またはトラブルシューティングします。電話機に LSC が存在する場合、電話機に MIC が存在するかどうかに関係なく、LSC によって認証が行われます。電話機に LSC が存在するが、MIC が存在しない場合、LSC によって認証が行われます。 このオプションを選択する前に、電話機に証明書が存在することを確認してください。電話に証明書が存在しない場合にこのオプションを選択すると、操作は失敗します。

設定	説明
	（注） [Phone Security Profile] ウィンドウで設定される CAPF 設定は、[Phone Configuration] ウィンドウで設定される CAPF パラメータと相互に関係します。
[Key Size]	CAPF で使用されるこの設定では、ドロップダウン リスト ボックスから証明書のキー サイズを選択します。デフォルト設定は 1024 です。キー サイズのその他のオプションは 512 です。 デフォルトの設定より大きいキー サイズを選択すると、電話がキーの生成に必要なエントロピーを生成する時間が長くなります。キーの生成を低い優先順位で設定すると、操作の実行中に、電話機が機能します。電話機のモデルによっては、キーの生成が完了するまでに、30 分以上かかることがあります。 （注） [Phone Security Profile] ウィンドウで設定される CAPF 設定は、[Phone Configuration] ウィンドウで設定される CAPF パラメータと相互に関係します。
[SIP Phone Port]	この設定は、UDP 転送を使用し SIP を実行する電話に適用されます。 UDP を使用して Unified Communications Manager からの SIP メッセージをリッスンする Cisco IP Phone（SIP のみ）のポート番号を入力します。デフォルト設定は 5060 です。 TCP または TLS を使用している電話ではこの設定が無視されます。

電話機へのセキュリティ プロファイルの適用

始める前に

電話の認証に証明書を使用するセキュリティ プロファイルを適用する前に、対象の電話にローカルで有効な証明書（LSC）または製造元でインストールされる証明書（MIC）が含まれていることを確認します。

電話のセキュリティ機能を有効にするには、デバイス タイプとプロトコルに応じた新しいセキュリティ プロファイルを設定し、電話に適用する必要があります。ただし、電話に証明書が含まれない場合は、次の作業を実行してください。

- [**電話の設定**（**Phone Configuration**）] ウィンドウで、非セキュア プロファイルを適用します。
- [Phone Configuration] ウィンドウで、CAPF 設定を行い、証明書をインストールします。
- [Phone Configuration] ウィンドウで、認証または暗号化のために設定されているデバイスのセキュリティ プロファイルを適用します。

デバイスに電話セキュリティ 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 [**電話の設定（Phone Configuration**）] ウィンドウの [**プロトコル固有情報（Protocol Specific Information**）] セクションに移動します。

ステップ 2 [Device Security Profile] ドロップダウンリストから、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。
電話のタイプおよびプロトコルに設定された電話セキュリティ プロファイルだけが表示されます。

ステップ 3 **[Save]** をクリックします。

ステップ 4 該当する電話に変更を適用するには、[Apply Config] をクリックします。

（注） セキュリティ プロファイルを削除するには、[**検索と一覧表示（Find and List**）] ウィンドウ上で該当するセキュリティ プロファイルの横にあるチェックボックスをオンにし、[**選択項目の削除（Delete Selected**）] をクリックします。

電話セキュリティ プロファイルと電話の同期

手順

ステップ 1 [Unified Communications Manager Administration] で、**[システム（System）] > [セキュリティ プロファイル（Security Profile）] > [電話セキュリティ プロファイル（Phone Security Profile）]** を選択します。
[**電話セキュリティ プロファイルの検索/一覧表示（Find and List Phone 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、[検索（Find）] をクリックします。
検索条件に一致する電話セキュリティ プロファイルの一覧がウィンドウに表示されます。

ステップ 3 該当の電話機を同期させる電話セキュリティ プロファイルをクリックします。
[**電話セキュリティ プロファイルの設定（Phone Security Profile Configuration**）] ウィンドウが表示されます。

ステップ 4 追加の設定変更を加えます。

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 [設定の適用（Apply Config）] をクリックします。
[**設定情報の適用（Apply Configuration Information**）] ダイアログボックスが表示されます。

ステップ 7 [OK] をクリックします。

電話セキュリティ プロファイルの削除

この項では、Unified Communications Manager データベースから電話セキュリティ 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確認するには、[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、**[System]** > **[Enterprise Parameters Configuration]** に移動し、[Enable Dependency Records] 設定を [True] に設定します。依存関係レコード能に関連してCPU負荷が高くなることについての情報が表示されます。依存関係レコードを有効にするため、変更を保存します。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 削除するセキュリティ プロファイルを探します。

ステップ 2 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] ウィンドウで該当するセキュリティ プロファイルの横にあるチェック ボックスをオンにし、[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。

ステップ 3 1 つのセキュリティ プロファイルを削除するには、次のいずれかの作業を実行します。

a) [Find and List] ウィンドウで、該当するセキュリティ プロファイルの横にあるチェック ボックスをオンにし、[Delete Selected] をクリックします。

ステップ 4 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。

電話セキュリティ プロファイルによる電話の検索

特定のセキュリティ プロファイルを使用している電話を検索するには、次の手順を実行します。

手順

ステップ 1 Unified Communications Manager Administrationで、**[Device]** > **[Phone]** を選択します。

ステップ 2 最初のドロップダウン リスト ボックスから、検索パラメータ [Security Profile] を選択します。

a) 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。

b) 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。