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

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、デバイスのセキュリティ モード、ダイジェスト認証およびいくつかの CAPF 設定が含まれます。[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する際に、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。電話機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、電話機に適用する必要があります。

選択されたデバイスとプロトコルがサポートするセキュリティ機能のみが、[セキュリティ プロファイル設定（security profile settings）] ウィンドウで表示されます。

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、次の情報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。
- 事前定義された非セキュアプロファイルを削除または変更することはできません。
- デバイスに現在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。
- すでに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、その特定のプロファイルが割り当てられているすべての電話に、再設定された設定が適用されます。
- 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。以前のプロファイル名と設定で割り当てられた電話機は、新しいプロファイル名と設定を前提としています。
- CAPF 設定、認証モード、およびキーサイズは、[電話の設定 (**Phone Configuration**)] ウィンドウに表示されます。Mic または LSCs に関連する証明書操作の CAPF 設定を構成する必要があります。これらのフィールドは、[電話の**設定 (Phone Configuration**)] ウィンドウで直接更新できます。
  - セキュリティプロファイルの CAPF 設定を更新すると、[電話の設定 (Phone Configuration)] ウィンドウでも設定が更新されます。
  - [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 電話 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。

関連トピック

証明書

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

Step 1 Cisco 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。

このウィンドウには、アクティブな（以前の）クエリーのレコードも表示されることがあります。

Step 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、Step 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。条件を削除するには、**[-]** ボタンをクリックして最後に追加された条件を削除するか、または**[フィルタのクリア（Clear Filter）]** をクリックして、追加されたすべての検索条件を削除します。

Step 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、[ページあたりの行数（Rows per Page）] ドロップダウンリストで別の値を選択します。

Step 4 表示されるレコードのリストで、表示するレコードのリンクをクリックします。

（注） ソート順を反転させるには、リスト見出しの上矢印または下矢印が使用可能であればそれをクリックします。

ウィンドウに、選択したレコードが表示されます。

関連トピック

セキュリティ プロファイルに関する詳細情報の入手先

電話セキュリティプロファイルのセットアップ

電話セキュリティプロファイルを設定するには、次の手順を実行します。

手順

Step 1 Cisco 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。

Step 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。

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見つけて続行します。

[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。[コピー（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。

Step 3 SCCP または SIP を実行している電話機の適切な設定を入力します。

Step 4 [保存（Save）] をクリックします。

関連トピック

電話セキュリティプロファイルの検索, on page 3
セキュリティ プロファイルに関する詳細情報の入手先

電話セキュリティ プロファイルの設定

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

選択した電話のタイプおよびプロトコルがサポートする設定のみ表示します。

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
名前	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 [電話の設定（Phone Configuration）] ウィンドウの [デバイスのセキュリティプロファイル（Device Security Profile）] ドロップダウンリスト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。

電話セキュリティ プロファイルの設定

設定	説明
説明	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
[デバイスセキュリティモード（Device Security Mode）]	

設定	説明
	ドロップダウンリストから、次のオプションのいずれかを選択します。 • [非セキュア（Non Secure）]：イメージ、ファイル、デバイス認証を除くセキュリティ機能は電話機に存在しません。TCP 接続で Unified Communications Manager が利用できます。 • [認証済（Authenticated）]： Unified Communications Managerは電話機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。 • [暗号化（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 Communications 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` 中 - AES-256 AES-128のみ: RSA優先 （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。 • `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`

設定	説明
	（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

電話セキュリティ プロファイルの設定

設定	説明
	• TLS_RSA with AES_128_CBC_SHA1 （注） [認証済み（Authenticated）] として選択されている [デバイスセキュリティプロファイル（Device Security Profile）] を使用してトランクを設定した場合、Unified Communications Manager は、NULL_SHA 暗号を使用した TLS 接続（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がオンの場合、Unified Communications Manager は電話機が TFTP サーバからダウンロードするファイルを暗号化します。

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、電話機がCAPF証明書の操作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、閉鎖された安全な環境だけで選択することをお勧めします。 • **[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。このオプションを選択して、電話機に証明書が

設定	説明
	存在しない場合、操作は失敗します。 （注） [電話セキュリティ プロファイル（Phone Security Profile）] ウィンドウで設定される CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウで設定される CAPF パラメータと連携します。
[キーの順序（Key Order）]	このフィールドは、CAPF のキーの順序を指定します。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 のみ（RSA Only）]** • **[ECのみ（EC Only）]** • **[EC 優先、RSA バックアップ（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の一覧を確認できます。
[ECキーサイズ（ビット）（EC Key Size (Bits)）]	ドロップダウンリストから、**256**、**384**、または**521**のいずれかの値を選択します。

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

電話セキュリティ プロファイルの設定

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
名前	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 [電話の設定（Phone Configuration）] ウィンドウの [デバイスのセキュリティプロファイル（Device Security Profile）] ドロップダウンリスト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。
説明	セキュリティ プロファイルの説明を入力します。
ナンス確認時間（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。

電話セキュリティ プロファイルの設定

設定	説明
[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から、次のオプションのいずれかを選択します。 • [非セキュア（Non Secure）]：イメージ、ファイル、デバイス認証を除くセキュリティ機能は電話機に存在しません。TCP 接続で Unified Communications Manager が利用できます。 • [認証済（Authenticated）]： Unified Communications Managerは電話機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。 • [暗号化（Encrypted）]： Unified Communications Managerは電話機の整合性、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（Authenticated）] として選択されている [デバイスセキュリティプロファイル（Device Security Profile）] を使用してトランクを設定した場合、Unified Communications Manager は、NULL_SHA 暗号を使用した TLS 接続（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
転送タイプ	[デバイスセキュリティモード（Device Security Mode）] が **[非セキュア（Non Secure）]** の場合は、ドロップダウンリスト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、パケットが送信したとき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場合があります。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。 [デバイスセキュリティモード（Device Security Mode）] が [認証（Authenticated）] または [暗号化（Encrypted）] の場合、TLS では [転送タイプ（Transport Type）] を指定します。TLS は、SIP 電話に対して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（暗号化モードに限る）を提供します。 プロファイルで [デバイスセキュリティモード（Device Security Mode）] を設定できない場合は、転送タイプとして UDP を指定します。
[ダイジェスト認証の有効化（Enable Digest Authentication）]	このチェックボックスをオンにすると、Unified Communications Manager は、電話機からのすべての SIP 要求で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、認証または暗号化のセキュリティモードを選択します。
TFTP 暗号化（TFTP Encrypted Config）	このチェックボックスがオンの場合、Unified Communications Manager は電話機が TFTP サーバからダウンロードするファイルを暗号化します。このオプションはシスコ製電話機に限り使用できます。 **ヒント** このオプションを有効にして、対称キーを設定し、ダイジェストログイン情報と管理者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、電話セキュリティプロファイルに関連付けられているデバイスを SIP OAuthポートに登録することが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） Unified Communications Manager リリース12.5以降、Jabber デバイスは SIP OAuth 認証に対応しています。
[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 は電話機が TFTP サーバからの電話ダウンロードのダイジェストログイン情報を削除します。このオプションは、Cisco IP 電話、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、電話機がCAPF証明書の操作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機に限り使用できます。 ドロップダウンリストから、次のオプションのいずれかを選択します。 • **[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、セキュアな閉じた環境の場合にだけこのオプションを選択することをお勧めします。 • **[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。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。 （注） [電話セキュリティ プロファイル（Phone Security Profile）] ウィ

設定	説明
	ンドウで設定される CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウで設定される CAPF パラメータと連携します。
[キー サイズ（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 サイズのもう 1 つのオプションは、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、電話機でキーの生成に必要なエントロピーを生成するのに時間がかかります。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） [電話セキュリティ プロファイル（Phone Security Profile）] ウィンドウで設定される CAPF 設定は、[電話の設定（Phone Configuration）] ウィンドウで設定される CAPF パラメータと連携します。
SIP 電話ポート（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 Unified IP 電話（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機はこの設定を無視します。

関連トピック

設定ファイルの暗号化
ダイジェスト認証
SIP 電話のダイジェスト認証の設定
暗号化された電話設定ファイルの設定
電話セキュリティプロファイルの設定の前提条件, on page 2
詳細情報の入手先

電話機へのセキュリティ プロファイルの適用

電話機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、特定の電話機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た証明書 (MIC) が含まれていることを確認してください。

電話機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、電話機に適用する必要があります。ただし、電話機に証明書が含まれていない場合は、次のタスクを実行します。

- [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。
- [電話の設定 (Phone Configuration)] ウィンドウで、capf 設定を構成することによって証明書をインストールします。
- [電話の設定 (Phone Configuration)] ウィンドウで、認証または暗号化用に設定されたデバイス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

Step 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。

Step 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。
電話機タイプとプロトコルに対してのみ設定されている電話セキュリティプロファイルが表示されます。

Step 3 [保存（Save）] をクリックします。

Step 4 該当する電話に変更を適用するには、[**設定の適用 (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、[**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。

関連トピック

Certificate Authority Proxy Function
SIP 電話のダイジェスト認証の設定
セキュリティ プロファイルに関する詳細情報の入手先

電話機のセキュリティプロファイルと電話機の同期

電話セキュリティプロファイルに複数の電話を同期させるには、次の手順を実行します。

手順

Step 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。

Step 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。

Step 3 該当する電話機を同期する電話セキュリティプロファイルをクリックします。

Step 4 追加の設定変更を加えます。

Step 5 [保存（Save）] をクリックします。

Step 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。

Step 7 [OK] をクリックします。

関連トピック

セキュリティ プロファイルに関する詳細情報の入手先

電話セキュリティ プロファイルの削除

Unified Communications Managerでセキュリティプロファイルを削除する前に、別のプロファイルをデバイスに適用するか、該当プロファイルを使用するすべてのデバイスを削除してください。

プロファイルを使用するデバイスを確認するには、ステップ 1 を実行します。

手順

Step 1 [セキュリティプロファイルの設定（Security Profile Configuration）] ウィンドウで、[関連リンク（Related Links）] ドロップダウンリストから [依存関係レコード（Dependency Records）] を選択し、[移動（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になっていない場合は、**[システム] > [エンタープライズパラメータ設定 (system Enterprise Parameters Configuration)]** に移動し、[依存関係レコードの有効化 (Enable dependency Records)] 設定を **[True]** に変更依存関係レコード機能に関連する高 CPU 使用率に関する情報がメッセージに表示されます。依存関係レコードを有効にするには、変更を保存します。依存関係レコードの詳細については、次を参照してください。Cisco Unified Communications Manager システム設定ガイド

ここでは、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。

Step 2 削除するセキュリティプロファイルを検索します。

Step 3 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チェックボックスの横にあるチェックボックスをオンにします。次に、[**Delete Selected**] をクリックします。この選択で設定可能なすべてのレコードを削除するには、[すべて選択（Select All）] をクリックして、[選択項目の削除（Delete Selected）] をクリックします。

Step 4 単一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行います。

a) [**Find And List**] ウィンドウで、適切な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ます。次に、[**Delete Selected**] をクリックします。

Step 5 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。

関連トピック

電話セキュリティプロファイルの検索, on page 3
セキュリティ プロファイルに関する詳細情報の入手先

電話機のセキュリティプロファイルを使用した電話機の検索

特定のセキュリティプロファイルを使用する電話機を検索するには、次の手順を実行します。

手順

Step 1 Cisco Unified Communications Manager Administrationから、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。

Step 2 最初のドロップダウンリストから、検索パラメータ **[セキュリティプロファイル（Security Profile）]** を選択します。

a) ドロップダウンリストで、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） 追加の検索条件を追加するには、**[+]** をクリックします。条件を追加した場合、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、[-] 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] をクリックします。

Step 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、[ページあたりの行数（Rows per Page）] ドロップダウンリストで別の値を選択します。

Step 4 表示されるレコードのリストで、表示するレコードのリンクをクリックします。

（注） ソート順を反転させるには、リスト見出しの上矢印または下矢印が使用可能であればそれをクリックします。

ウィンドウに、選択したレコードが表示されます。

関連トピック

セキュリティ プロファイルに関する詳細情報の入手先