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 プロファイルの設定について，1 ページ
- 電話セキュリティ プロファイルの設定のヒント，2 ページ
- 電話セキュリティ プロファイルの検索，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
- 電話セキュリティ プロファイルの設定項目，5 ページ
- 電話セキュリティ プロファイルの適用，15 ページ
- 電話セキュリティ プロファイルと電話機の同期，16 ページ
- 電話セキュリティ プロファイルの削除，16 ページ
- 電話セキュリティ プロファイルによる電話機の検索，17 ページ
- セキュリティ プロファイルの参考情報，18 ページ

電話セキュリティ プロファイルの設定について

Cisco Unified Communications Manager の管理ページでは、電話機タイプおよびプロトコルに対するセキュリティ関連の設定がセキュリティ プロファイルとしてまとめられ、1 つのセキュリティ プロファイルを複数の電話機に割り当てることができます。 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、一部の CAPF 設定などがあります。 [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ことで、構成済み設定を電話機に適用します。

Cisco Unified Communications Manager をインストールすると、自動登録用の事前定義済み非セキュア セキュリティ プロファイルのセットが提供されます。 電話機のセキュリティ機能を使用可能にするには、デバイスタイプとプロトコルに対応した新しいセキュリティプロファイルを設定して電話機に適用する必要があります。

選択したデバイスおよびプロトコルがサポートするセキュリティ機能だけが、セキュリティ プロファイル設定ウィンドウに表示されます。

電話セキュリティ プロファイルの設定のヒント

Cisco Unified Communications Manager の管理ページで電話セキュリティ プロファイルを設定する場合は、次の点を考慮してください。

- 電話機を設定する場合は、[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 プロファイルを適用します。
- 事前定義済みの非セキュア プロファイルは、削除することも変更することもできません。
- 現在デバイスに割り当てられているセキュリティ プロファイルを削除することはできません。
- 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、再構成した設定が、そ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。 古い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。
- 電話セキュリティ プロファイルの CAPF 設定（認証モードおよびキー サイズ）は、[電話の設定(Phone Configuration)] ウィンドウにも表示されます。 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）に関連する証明書操作の CAPF 設定項目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、これら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)] ウィンドウで設定が更新されます。
  - [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見つかった場合、Cisco Unified Communications Manager は一致するプロファイルを電話機に適用します。
  - [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見つからなかった場合、Cisco Unified Communications Manager は新しいプロファイルを作成して電話機に適用します。
- Cisco Unified Communications Manager 5.0 以降へのアップグレード前にデバイス セキュリティ モードを設定した場合は、Cisco Unified Communications Manager が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。
- 製造元でインストールされる証明書（MIC）は、LSC のインストールでのみ使用することをお勧めします。 シスコでは、Cisco Unified Communications Manager との TLS 接続の認証用に LSC 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

用またはその他の目的のためにMICを使用するように電話機を設定するお客様は、ご自身の責任で行ってください。 MIC が侵害されてもシスコは責任を負いかねます。

- シスコは、Cisco Unified IP Phones をアップグレードして Cisco Unified Communications Manager との TLS 接続で LSC を使用すること、および MIC ルート証明書を CallManager 信頼ストアから削除して今後の互換性の問題を回避することをお勧めします。

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

ステップ 1 Cisco Unified Communications Manager の管理ページで、[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)] の順に選択します。
[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 Profile)] ウィンドウが表示されます。 ウィンドウには、アクティブな（前の）クエリーのレコードが表示される場合もあります。

ステップ 2 データベース内のすべてのレコードを検索するには、ダイアログボックスが空になっていることを確認し、ステップ 3, （3 ページ） に進みます。
レコードをフィルタリング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 番めのドロップダウン 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） 別の検索条件を追加するには、[+] ボタンをクリックします。 条件を追加した場合は、指定したすべての条件に一致す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)] ボタンをクリックして、追加されたすべての検索条件を削除します。

ステップ 3 [検索(Find)] をクリックします。
一致するすべてのレコードが表示されます。 [ページあたりの行数(Rows per Page)] ドロップダウン リスト ボックスから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 4 表示されたレコード リストから、目的のレコード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矢印または下矢印をクリックします（使用可能な場合）。

選択した項目がウィンドウに表示されます。

関連トピック

セキュリティ プロファイルの参考情報, （18 ページ）

電話セキュリティ プロファイルの設定

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 Cisco Unified Communications Manager の管理ページで、[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)] の順に選択します。

ステップ 2 次のいずれかの手順を実行します。

a) 新しいプロファイルを追加するには、[検索(Find)] ウィンドウの [新規追加(Add New)] をクリックし、電話セキュリティ プロファイルの設定, （1 ページ） に進みます。

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て、コピーするセキュリティプロファイルの横に表示されている [コピー(Copy)] ボタンをクリックし、電話セキュリティ プロファイルの設定, （1 ページ） に進みます。

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、電話セキュリティ プロファイルの設定, （1 ページ） に進みます。

[新規追加(Add New)] をクリックすると、各フィールドのデフォルト設定を示し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、コピーした設定を含む設定ウィンドウが表示されます。

ステップ 3 SCCP を実行する電話機の場合は 表 1：SCCP を実行している電話機のセキュリティ プロファイル , （5 ページ）、SIP を実行する電話機の場合は 表 2：SIP を実行している電話機のセキュリティ プロファイル, （9 ページ）の説明に従い、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。

次の作業

セキュリティ プロファイルを作成した後、電話セキュリティ プロファイルの適用, （15 ページ）の説明に従い、電話機に適用します。

SIP を実行する電話機の電話セキュリティ プロファイルでダイジェスト認証を設定した場合は、[エンドユーザの設定(End User Configuration)] ウィンドウでダイジェスト信用証明書を設定する必要があります。 その後、[電話の設定(Phone Configuration)] ウィンドウの [ダイジェストユーザ(Digest User)] 設定を使用して、ユーザを電話機に関連付ける必要があります。

関連トピック

電話セキュリティ プロファイルの検索, （3 ページ）
セキュリティ プロファイルの参考情報, （18 ページ）

電話セキュリティ プロファイルの設定項目

次の表に、SCCP を実行する電話機のセキュリティ プロファイルの設定項目の説明を示します。

選択した電話機タイプおよびプロトコルがサポートしている設定だけが表示されます。

表 *1*：*SCCP* を実行している電話機のセキュリティ プロファイル

設定項目	説明
[名前(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 [電話の設定(Phone Configuration)] ウィンドウの [デバイス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 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、プロファイルを検索または更新する場合の適切なプロファイルの検出に役立ちます。
[説明(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。
[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、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)]**：電話機では、イメージ認証、ファイル認証、またはデバイス認証以外のセキュリティ機能を使用できません。 TCP 接続が Cisco Unified Communications Manager に対して開きます。 • **[認証済(Authenticated)]**：Cisco Unified Communications Manager は電話の整合性と認証を提供します。 シグナリング用に、NULL/SHA を使用する TLS 接続を開始します。 • **[暗号化済(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。 シグナリング用に AES128/SHA を使用する TLS 接続を開始し、すべての電話機コールのメディアを SRTP で搬送します。

設定項目	説明
[TFTP暗号化設定(TFTP Encrypted Config)]	このチェックボックスをオンにすると、Cisco 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。

設定項目	説明
[認証モード(Authentication Mode)]	

設定項目	説明
	このフィールドでは、CAPF 証明書の処理中に電話機が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、次のオプションのいずれかを選択します。 • [認証ストリング(By Authentication String)]：ユーザが電話機に CAPF 認証文字列を入力した場合だけ、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。 • [Nullストリング(By Null String)]：ユーザが介入することなく、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。 このオプションは、セキュリティを提供しません。このオプションは、閉じた安全な環境だけで選択することを強くお勧めします。 • [既存の証明書(LSCの優先)(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）が電話機に存在する場合、LSC 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。 LSC が電話機内に存在する場合は、MIC が電話機内に存在するかどうかにかかわらず、LSC を通じて認証が実行されます。 MIC および LSC が電話機内に存在する場合、認証は LSC を通じて実行されます。 LSC が電話機内に存在せず、MIC が存在する場合、認証は MIC を通じて実行されます。 このオプションを選択する前に、電話機内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、電話機内に証明書が存在しない場合、処理は失敗します。 MIC と LSC が電話機内に同時に存在する場合でも、電話機は常に 1 つの証明書だけを使用して CAPF に対して認証します。 何らかの原因により優先されるプライマリ証明書の信頼性が低下した場合、または他の証明書を通じて認証する場合は、認証モードを更新する必要があります。 • [既存の証明書(MICを優先)(By Existing Certificate (Precedence to MIC))]：LSC または MIC が電話機に存在する場合、LSC 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。 MIC が電話機内に存在する場合は、LSC が電話機内に存在するかどうかにかかわらず、MIC を通じて認証が実行されます。 LSC が電話機内に存在し、MIC が存在しない場合、認証は LSC を通じて実行されます。 このオプションを選択する前に、電話機内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、電話機内

設定項目	説明
	に証明書が存在しない場合、処理は失敗します。 （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 設定値は、[電話の設定(Phone Configuration)] ウィンドウで設定される CAPF パラメータと相互に関係があります。 [電話の設定(Phone Configuration)] ウィンドウで CAPF の設定項目を設定する方法については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』を参照してください。
[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 ボックスから認証のキー 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も大きいキー サイズを選択した場合、キーの生成に必要なエントロピーを生成するために長い時間がかかります。キー生成の優先順位を低く設定すると、処理中に電話機を動作させることができます。 電話機のモデルによっては、キー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 設定値は、[電話の設定(Phone Configuration)] ウィンドウで設定される CAPF パラメータと相互に関係があります。 [電話の設定(Phone Configuration)] ウィンドウで CAPF の設定項目を設定する方法については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』を参照してください。

次の表に、SIP を実行する電話機のセキュリティ プロファイルの設定項目の説明を示します。

表 *2*：*SIP* を実行している電話機のセキュリティ プロファイル

設定項目	説明
[名前(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 [電話の設定(Phone Configuration)] ウィンドウの [デバイス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 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、プロファイルを検索または更新する場合の適切なプロファイルの検出に役立ちます。
[説明(Description)]	セキュリティ プロファイルの説明を入力します。

設定項目	説明
[ナンス確認時間(Nonce Validity Time)]	ナンス値が有効な時間を秒単位で入力します。 デフォルト値は 600（10 分）です。 この期限が切れると、Cisco 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ランダム値で、ダイジェスト認証パスワードの MD5 ハッシュの計算に使用されます。
[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、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)]：電話機では、イメージ認証、ファイル認証、またはデバイス認証以外のセキュリティ機能を使用できません。 TCP 接続が Cisco Unified Communications Manager に対して開きます。 • [認証済(Authenticated)]：Cisco Unified Communications Manager は電話の整合性と認証を提供します。 シグナリング用に、NULL/SHA を使用する TLS 接続を開始します。 • [暗号化済(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。 シグナリング用に AES128/SHA を使用する TLS 接続を開始し、すべての SRTP 対応ホップ上のすべての電話機コールのメディアを SRTP で搬送します。

設定項目	説明
[転送タイプ(Transport Type)]	[デバイスセキュリティモード(Device Security Mode)] が [非セキュア(Non Secure)] である場合は、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（表示されないオプションもあります）。 • [TCP]：パケットを送信された順に受信するには、Transmission Control Protocol を選択します。 このプロトコルは、パケットがドロップされないことを保証しますが、セキュリティは提供されません。 • [UDP]：パケットを高速に受信するには、User Datagram Protocol を選択します。 このプロトコルは、パケットをドロップすることがあり、送信された順に受信するとは限りません。 セキュリティは提供されません。 • [TCP + UDP]：TCP と UDP を組み合わせて使用するには、このオプションを選択します。 このオプションでは、セキュリティは提供されません。 [デバイスセキュリティモード(Device Security Mode)] が [認証のみ(Authenticated)] または [暗号化(Encrypted)] である場合、[TLS] が転送タイプとなります。 TLS では、SIP 電話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暗号化（暗号化モードのみ）が提供されます。 プロファイルでデバイスセキュリティモードを設定できない場合、転送タイプは UDP になります。
[ダイジェスト認証を有効化(Enable Digest Authentication)]	このチェックボックスをオンにすると、Cisco 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、および信頼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 [認証のみ(Authenticated)] または [暗号化(Encrypted)] を選択します。
[TFTP暗号化設定(TFTP Encrypted Config)]	このチェックボックスをオンにすると、Cisco 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、シスコ製電話機専用です。 **ヒント** このオプションを有効にして、対称キーを設定し、ダイジェスト信用証明書と管理者パスワードを保護することをお勧めします。
[設定ファイル内のダイジェスト信用証明書を除外(Exclude Digest Credentials in Configuration File)]	このボックスをオンにすると、Cisco Unified Communications Manager は TFTP サーバからの電話のダウンロードのダイジェスト信用証明書を除外します。 このオプションは、Cisco Unified IP Phone 7905G、7912G、7940G、および 7960G（SIP のみ）用です。

設定項目	説明
[認証モード(Authentication Mode)]	

設定項目	説明
	このフィールドでは、CAPF 証明書の処理中に電話機が使用する認証方法を選択できます。 このオプションは、シスコ製電話機専用です。 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。 • **[認証ストリング(By Authentication String)]**：ユーザが電話機に CAPF 認証文字列を入力した場合だけ、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。 • **[Nul文字列(By Null String)]**：ユーザが介入することなく、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。 このオプションは、セキュリティを提供しません。このオプションは、閉じた安全な環境だけで選択することを強くお勧めします。 • **[既存の証明書(LSCを優先)(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）が電話機に存在する場合、LSC 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。 LSC が電話機内に存在する場合は、MIC が電話機内に存在するかどうかにかかわらず、LSC を通じて認証が実行されます。 LSC が電話機内に存在せず、MIC が存在する場合、認証は MIC を通じて実行されます。 このオプションを選択する前に、電話機内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、電話機内に証明書が存在しない場合、処理は失敗します。 MIC と LSC が電話機内に同時に存在する場合でも、電話機は常に 1 つの証明書だけを使用して CAPF に対して認証します。 何らかの原因により優先されるプライマリ証明書の信頼性が低下した場合、または他の証明書を通じて認証する場合は、認証モードを更新する必要があります。 • **[既存の証明書(MICを優先)(By Existing Certificate (Precedence to MIC))]**：LSC または MIC が電話機に存在する場合、LSC 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。 MIC が電話機内に存在する場合は、LSC が電話機内に存在するかどうかにかかわらず、MIC を通じて認証が実行されます。 LSC が電話機内に存在し、MIC が存在しない場合、認証は LSC を通じて実行されます。 このオプションを選択する前に、電話機内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、電話機内

設定項目	説明
	に証明書が存在しない場合、処理は失敗します。 （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 設定値は、[電話の設定(Phone Configuration)] ウィンドウで設定される CAPF パラメータと相互に関係があります。 [電話の設定(Phone Configuration)] ウィンドウで CAPF の設定項目を設定する方法については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』を参照してください。
[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 ボックスから認証のキー 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も大きいキー サイズを選択した場合、キーの生成に必要なエントロピーを生成するために長い時間がかかります。キー生成の優先順位を低く設定すると、処理中に電話機を動作させることができます。 電話機のモデルによっては、キー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 設定値は、[電話の設定(Phone Configuration)] ウィンドウで設定される CAPF パラメータと相互に関係があります。 [電話の設定(Phone Configuration)] ウィンドウで CAPF の設定項目を設定する方法については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』を参照してください。
[SIP電話ポート(SIP Phone Port)]	この設定は、UDP 転送を使用し SIP を実行する電話機に適用されます。 UDP を使用する Cisco Unified IP Phone（SIP のみ）が、Cisco Unified Communications Manager からの SIP メッセージの傍受に使用する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 を使用する電話機は、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
電話セキュリティ プロファイルの設定のヒント, （2 ページ）
詳細情報

電話セキュリティ プロファイルの適用

[電話の設定(Phone Configuration)] ウィンドウで、電話セキュリティ プロファイルを電話機に適用します。

はじめる前に

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、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る証明書（MIC）が含まれていることを確認します。

電話機に証明書が含まれていない場合は、次の手順を実行します。

1. [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。
2. [電話の設定(Phone Configuration)] ウィンドウで、CAPF 設定で設定された証明書をインストールします。 この作業の実行の詳細については。
3. [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し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

ステップ 1 『*Cisco Unified Communications Manager* アドミニストレーション ガイド』の説明に従って、電話機を検索します。

ステップ 2 [電話の設定(Phone Configuration)] ウィンドウが表示されたら、[デバイスセキュリティプロファイル(Device Security Profile)] を見つけます。

ステップ 3 [デバイス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 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。 該当する電話機タイプおよびプロトコル用に設定されている電話セキュリティ プロファイルだけが表示されます。

ステップ 4 [保存(Save)] をクリックします。

ステップ 5 該当する電話機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。

次の作業

SIP を実行する電話機にダイジェスト認証を設定した場合は、[エンドユーザの設定(End User Configuration)] ウィンドウで、ダイジェスト信用証明書を設定する必要があります。 次に、[電話の設定(Phone Configuration)] ウィンドウで、[ダイジェストユーザ(Digest User)] 設定を定義する必要があります。

関連トピック

セキュリティ プロファイルの参考情報, （18 ページ）

電話セキュリティ プロファイルと電話機の同期

電話機を、設定変更が行われた電話セキュリティ プロファイルと同期させるには、次の手順を実行します。この手順では、できる限り簡潔な方法で主な設定項目を適用します（たとえば、影響を受ける電話機の一部では、リセットまたは再起動する必要がない場合があります）。

手順

ステップ 1 [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)] の順に選択します。
[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電話セキュリティ プロファイルのリストが表示されます。

ステップ 4 該当する電話機と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 Profiles Configuration)] ウィンドウが表示されます。

ステップ 5 他の設定変更を行います。

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。
[設定の適用情報(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。

関連トピック

セキュリティ プロファイルの参考情報, （18 ページ）

電話セキュリティ プロファイルの削除

ここでは、Cisco 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。

はじめる前に

Cisco Unified Communications Manager の管理ページでセキュリティ 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。該当プロファイルを使用しているデバイスを検索するには、セキュリティプロ

ファイルの設定ウィンドウの [関連リンク(Related Links)] ドロップダウン リスト ボックスから [依存関係レコード(Dependency Records)] を選択して、[移動(Go)] をクリックします。

システムで依存関係レコード機能が有効になっていない場合は、[システム(System)]>[エンタープライズパラメータ設定(Enterprise Parameters Configuration)] の順に選択し、[依存関係レコードの有効化(Enable Dependency Records)] 設定を [True] に変更します。 依存関係レコード機能を使用すると、CPU 使用率が高くなるという情報を示すメッセージが表示されます。 変更内容を保存して、依存関係レコードをアクティブにします。 BFCP の詳細については、『*Cisco Unified Communications Manager System Guide*』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 プロファイルを検索します。

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、検索/一覧表示ウィンドウで、適切なチェックボックスの横に表示されているチェックボックスをオンにして、[選択項目の削除(Delete Selected)] をクリックします。 [すべて選択(Select All)] をクリックして [選択項目の削除(Delete Selected)] をクリックすると、この選択対象として設定可能なすべてのレコードを削除できます。

ステップ 3 単一のセキュリティ プロファイルを削除するには、次の作業のどちらかを実行します。

a) 検索/一覧表示ウィンドウで、適切なセキュリティ プロファイルの横に表示されているチェックボックスをオンにして、[選択項目の削除(Delete Selected)] をクリックします。

ステップ 4 削除操作の確認を要求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、[キャンセル(Cancel)] をクリックして削除操作を取り消します。

関連トピック

電話セキュリティ プロファイルの検索, （3 ページ）
セキュリティ プロファイルの参考情報, （18 ページ）

電話セキュリティ プロファイルによる電話機の検索

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

手順

ステップ 1 Cisco Unified Communications Manager の管理ページで、[デバイス(Device)] > [電話(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、検索パラメータの [セキュリティプロファイル(Security Profile)] を選択します。

a) 2 番めのドロップダウン リスト ボックスから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） 別の検索条件を追加するには、[+] ボタンをクリックします。 条件を追加した場合は、指定したすべての条件に一致す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)] ボタンをクリックして、追加されたすべての検索条件を削除します。

ステップ 3 [検索(Find)] をクリックします。
一致するすべてのレコードが表示されます。 [ページあたりの行数(Rows per Page)] ドロップダウン リスト ボックスから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 4 表示されたレコード リストから、目的のレコード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矢印または下矢印をクリックします（使用可能な場合）。
選択した項目がウィンドウに表示されます。

関連トピック

セキュリティ プロファイルの参考情報, （18 ページ）

セキュリティ プロファイルの参考情報

関連トピック

ダイジェスト認証
設定ファイルの暗号化
電話セキュリティ プロファイルの設定について, （1 ページ）
電話セキュリティ プロファイルの設定のヒント, （2 ページ）
電話セキュリティ プロファイルの設定項目, （5 ページ）