アナログ エンドポイントに対する暗号化の設定

この章では、アナログ エンドポイントに対する暗号化の設定について説明します。 この機能を使用すると、アナログ電話機で Cisco VG2xx Gateway へのセキュアな SCCP 接続を作成できます。 このゲートウェイは、SCCP シグナリング通信に Cisco Unified Communications Manager で Transport Layer Security（TLS）を使用し、音声通信には SRTP を使用します。 セキュアな SCCP 通信には、証明書管理などの既存の Cisco Unified Communications Manager TLS の機能が使用されます。

- アナログ電話セキュリティ プロファイル，1 ページ
- セキュアなアナログ電話機の証明書管理，2 ページ

アナログ電話セキュリティ プロファイル

アナログ電話機で暗号化された接続を確立するには、[デバイスセキュリティモード(Device Security Mode)] パラメータを [認証のみ(Authenticated)] または [暗号化(Encryped)] に設定して、アナログ電話機用の電話セキュリティ プロファイルを作成する必要があります。 電話セキュリティ プロファイルを作成するには、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)]の順に移動します。

Cisco VG2xx ゲートウェイに接続されているアナログ電話機を設定する場合は、[デバイスセキュリティプロファイル(Device Security Profile)] パラメータに対して作成したセキュアなアナログ プロファイルを選択します。 [デバイスセキュリティプロファイル(Device Security Profile)] パラメータを設定するには、Cisco Unified Communications Manager の管理ページで [デバイス(Device)] > [電話(Phone)] にナビゲートして、設定を行う電話機の [プロトコル固有情報(Protocol Specific Information)] セクションまでスクロールします。

関連トピック

セキュアなアナログ電話機の証明書管理

セキュアなアナログ電話機の機能を利用するには、同じ CA 署名付き証明書を、Cisco VG2xx Gateway で使用する Cisco Unified Communications Manager にインポートする必要があります。 証明書のインポートの詳細については、『*Cisco Unified Communications Operating System Administration Guide*』の第 6 章「Security」を参照してください。