ボイス メッセージング ポートのセキュリティ設定

この章では、ボイスメッセージングポートのセキュリティ設定について説明します。

ボイスメッセージングセキュリティ

Unified Communications Manager ボイス メッセージング ポートおよび SCCP を実行している Cisco Unity デバイス、または SCCP を実行している Cisco Unity Connection デバイスでセキュリティを設定するには、ポートのセキュアなデバイス セキュリティ モードを選択します。認証済みのボイス メール ポートを選択すると TLS 接続が開始され、相互証明書交換を使用してデバイスが認証されます（各デバイスが他のデバイスの証明書を受け入れます）。暗号化されたボイス メール ポートを選択すると、システムはまずデバイスを認証し、デバイス間で暗号化された音声ストリームを送信します。

Cisco Unity Connection 2.0 以降では、TLS ポート経由で Unified Communications Manager に接続します。デバイス セキュリティ モードが非セキュアになると、Cisco Unity Connection は、SCCP ポート経由で Unified Communications Manager に接続します。

（注） この章で使用されている用語「サーバ」は、Unified Communications Manager サーバを示します。「ボイス メールサーバ」は Cisco Unity サーバまたは Cisco Unity Connection サーバを示します。

ボイスメッセージングセキュリティの設定のヒント

セキュリティを設定する前に、次の情報を考慮してください。

- Cisco Unity では、Cisco Unity Telephony Integration Manager (UTIM) を使用してセキュリティ タスクを実行する必要があります。Cisco Unity Connection では、Cisco Unity Connection Administration を使用してセキュリティ タスクを実行する必要があります。これらのタスクの実行方法については、Cisco Unity 向け、または Cisco Unity Connection 向けの『Unified Communications Manager integration guide』を参照してください。
- Cisco Unity 証明書を信頼ストアに保存するには、この章で説明している手順に加え、Unified Communications Manager の証明書の管理機能を使用する必要があります。

  詳細については、以下の URL にある『*Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection*』の「To Add Voice Messaging Ports in Cisco Unity Connection Administration」の手順を参照してください。

  http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/integration/guide/cucm_sccp/guide/cucintcucmskinny230.html

  証明書をコピーした後、クラスタ内の各 Unified Communications Manager サーバで CiscoCallManager サービスを再起動する必要があります。
- Cisco Unity 証明書が期限切れになったか、何らかの理由で変更された場合は、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』の証明書の管理機能を使用して信頼ストアの証明書を更新します。証明書が一致しないと TLS 認証が失敗し、ボイス メッセージングが機能しません。これは、ボイス メッセージング機能が Unified Communications Manager に登録できないためです。
- ボイスメール サーバのポートを設定するときには、デバイス セキュリティ モードを選択する必要があります。
- Cisco Unity Telephony Integration Manager (UTIM) または Cisco Unity Connection Administration で指定する設定は、Unified Communications Manager Administration で設定されているボイス メッセージング ポートのデバイス セキュリティ モードと一致する必要があります。Cisco Unity Connection Administration の [Voice Mail Port Configuration] ウィンドウ（または [Voice Mail Port] ウィザード）で、ボイス メッセージング ポートにデバイス セキュリティ モードを適用します。

ヒント デバイス セキュリティ モードの設定が一致しないと、Unified Communications Manager でのボイスメール サーバ ポートの登録は失敗し、ボイスメール サーバは登録が失敗したポートへのコールに対応できません。

- ポートのセキュリティ プロファイルを変更するには、Unified Communications Manager デバイスのリセットとボイスメール サーバ ソフトウェアの再起動が必要です。Unified Communications Manager Administration で以前と異なるデバイス セキュリティ モードを使

用するセキュリティ プロファイルを適用するには、ボイスメール サーバの設定を変更する必要があります。

- [VoiceMail Port] ウィザードで既存のボイスメール サーバのデバイス セキュリティ モードを変更することはできません。既存のボイス メール サーバにポートを追加すると、現在プロファイルに設定されているデバイス セキュリティ モードは自動的に新しいポートに適用されます。

セキュアなボイスメッセージングポートのセットアップ

次の手順では、ボイスメッセージングポートのセキュリティを設定するために使用するタスクについて説明します。

ステップ 1 **utils ctl** CLI コマンドを実行して、Unified Communications Manager が混合モードであることを確認します。

ステップ 2 電話機が認証または暗号化用に設定されていることを確認します。

ステップ 3 Cisco Unified Communications Operating System Administration の証明書管理機能を使用して Cisco Unity 証明書を Unified Communications Manager サーバの信頼ストアにコピーし、CiscoCallManager サービスを再起動します。

詳細については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』および『*Cisco Unified Serviceability Administration Guide*』を参照してください。

（注） 以下のヒントは、リリース 14SU3 以降では無効です。

ヒント クラスタにある各 Unified Communications Manager サーバの Cisco CTL Provider サービスをアクティブにします。次に、すべてのサーバで CiscoCallManager サービスを再起動します。

ステップ 4 Unified Communications Manager の管理ページで、ボイス メッセージング ポートのデバイス セキュリティ モードを設定します。

ステップ 5 Cisco Unity または Cisco Unity Connection のボイス メッセージング ポートのセキュリティ関連設定タスクを実行します。たとえば、Cisco Unity が Cisco TFTP サーバを指すように設定します。

詳細については、Cisco Unity または *Cisco Unity Connection* の『Unified Communications Manager Integration Guide』を参照してください。

ステップ 6 Unified Communications Manager の管理ページでデバイスをリセットし、Cisco Unity ソフトウェアを再起動します。

詳細については、Cisco Unity または *Cisco Unity Connection* の『Unified Communications Manager Integration Guide』を参照してください。

単一のボイスメッセージングポートへのセキュリティプロファイルの適用

単一のボイス メッセージング ポートにセキュリティ プロファイルを適用するには、次の手順を実行します。

この手順では、証明書がまだ存在していない場合に、デバイスをデータベースに追加し、電話機に証明書をインストールしたことを前提としています。セキュリティプロファイルを初めて適用した後、またはセキュリティプロファイルを変更した場合は、デバイスをリセットする必要があります。

始める前に

セキュリティプロファイルを適用する前に、ボイスメッセージングセキュリティとセキュアなボイスメッセージングポートの設定に関連するトピックを確認してください。

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、ボイス メッセージング ポートを検索します。

ステップ 2 ポートの設定ウィンドウが表示されたら、[**Device Security Mode**] 設定を見つけます。ドロップダウン リスト ボックスから、ポートに適用するセキュリティ モードを選択します。データベースでは次のオプションを予め定義しています。デフォルト値は、[Not Selected] に指定されています。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 [リセット（Reset）] をクリックします。

ボイスメールポートウィザードを使用したセキュリティプロファイルの適用

この手順を使用して、新しいボイスメールサーバの [ボイスメールポート (Voice Mail Port)] ウィザードで [デバイスセキュリティモード (Device Security Mode)] 設定を適用します。

既存のボイスメールサーバのセキュリティ設定を変更するには、単一のボイスメッセージングポートへのセキュリティプロファイルの適用に関連するトピックを参照してください。

始める前に

セキュリティプロファイルを適用する前に、ボイスメッセージングセキュリティとセキュアなボイスメッセージングポートの設定に関連するトピックを確認してください。

ステップ 1 [Unified Communications Manager Administration] で、**[Voice Mail]** > **[Cisco Voice Mail Port Wizard]** を選択します。

ステップ 2 ボイス メール サーバの名前を入力し、[Next] をクリックします。

ステップ 3 追加するポートの数を選択します。[**Next**] をクリックします。

ステップ 4 [**Cisco Voice Mail Device Information**] ウィンドウで、ドロップダウンリストボックスから**デバイスセキュリティモード**を選択します。データベースでは次のオプションを予め定義しています。デフォルト値は、[Not Selected] に指定されています。

ステップ 5 『 *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、その他のデバイス設定を行います。[次へ（Next）] をクリックします。

ステップ 6 『 *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、設定プロセスを続行します。[Summary] ウィンドウが表示されたら、[Finish] をクリックします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。