セキュリティモード

セキュリティモードの概要

データや情報の改ざんを防ぐためのセキュリティメカニズムを実装するために、Unified Communications Manager は、次のセキュリティモードを提供します。

- 非セキュアモード：デフォルトモード
- セキュアモードまたは混合モード：セキュアエンドポイントと非セキュアエンドポイントをサポートします。
- SIP Auth モード：セキュアな環境での Cisco Jabber 認証に OAuth 更新トークンを使用します。

非セキュアモード（デフォルトモード）

非セキュアモードは、Unified Communications Manager を初めてインストールする場合のデフォルトのセキュリティモードです。このモードでは、Unified Communications Manager はセキュアなシグナリングやメディアサービスを提供しません。

セキュアモードの設定

セキュリティを適用するには、導入に適用するセキュリティモードを設定します。

Procedure

	Command or Action	Purpose
Step 1	混合モード	混合モードを有効にして、Cisco IP 電話および Webex デバイスのセキュリティを強化します。混合モードの有効化と確認の方法について説明します。
Step 2	SIP OAuth モード	Cisco Jabber クライアントのセキュリティを強化するには、SIP OAuth モードを設定します。

混合モード

混合モードまたはセキュアモードは、セキュアエンドポイントと非セキュアエンドポイントをサポートします。クラスタまたはサーバに Unified Communications Manager を新しくインストールすると、デフォルトでは非セキュアモードになります。ただし、セキュリティモードは非セキュアモードからセキュアモードまたは混合モードに変換できます。

クラスタを非セキュアモードから混合モード（セキュアモード）に変更するには、次の手順を実行します。

- パブリッシャ上で認証局プロキシ機能（CAPF）サービスを有効にします。
- パブリッシャ上で証明書信頼リスト（CTL）サービスを有効にします。

Note エンドポイントのセキュリティのためには、シグナリングに Transport Layer Security（TLS）を使用し、メディアに Secure RTP（SRTP）を使用します。

混合モードを有効にするには、発行元ノードのコマンドライン インターフェイスにログインし、CLI コマンド `utils ctl set-cluster mixed-mode` を実行します。

Note Unified Communications Manager が Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録されていることを確認してください。スマートアカウントまたはバーチャルアカウントから受信した登録トークンには、このクラスタへの登録中に [エクスポート制御機能を許可する（Allow Export-Controlled）] 機能が有効になっています。

セキュリティモードを非セキュアモードからセキュアモードまたは混合モードに変更した場合は、そのモードを確認できます。モードを確認するには、**[エンタープライズパラメータの設定（Enterprise Parameters Configuration）]** ページに移動して、クラスタまたはサーバが混合モードであるかどうか確認します。詳細については、「セキュリティモードの確認」トピックを参照してください。

セキュリティモードの確認

セキュリティモードを非セキュアモードからセキュアモードまたは混合モードに変更した場合は、そのモードを確認できます。モードを確認するには、**[エンタープライズパラメータの設定（Enterprise Parameters Configuration）]** ページに移動して、クラスタまたはサーバが混合モードであるかどうか確認します。

セキュリティモードを確認するには、次の手順を実行します。

Procedure

Step 1 [Unified Communications Manager Administration] で、**[システム（System）]** > **[エンタープライズパラメータ（Enterprise Parameters）]** を選択します。
[エンタープライズパラメータの設定（Enterprise Parameters Configuration）] ページが表示されます。

Step 2 [セキュリティパラメータ（Security Parameters）] ペインに移動します。
適切な値の [クラスタセキュリティモード（Cluster Security Mode）] フィールドがあります。値に 1 が表示されている場合、Unified Communications Manager は混合モードに正常に設定されています。Cisco Unified CM Administration ページでは、この値を設定できません。この値は、CLI コマンド `set utils cli` を入力した後に表示されます。

Note クラスタセキュリティモードでは、スタンドアロンサーバまたはクラスタのセキュリティ機能を設定します。

SIP OAuth モード

SIP OAuth モードでは、セキュアな環境での Cisco Jabber 認証に OAuth 更新トークンを使用できます。Unified Communications Manager の SIP 回線で OAuth をサポートすることで、CAPF なしでセキュア シグナリングとセキュア メディアが可能になります。Unified Communication Manager クラスタおよびCisco Jabberエンドポイントで OAuthベースの認証を有効にすると、SIP 登録中の OAuth トークン検証が完了します。

SIP 登録向けの OAuth サポートは、Cisco Unified Communications Manager 12.5(1) 以降の Cisco Jabber デバイス向けのリリースのみで拡張されます。SIP OAuth の詳細については、Cisco Unified Communications Manager 機能設定ガイドを参照してください。