SIP OAuth モード

SIP OAuth モードの概要

Unified Communications Manager へのセキュア登録では、CTL ファイルの更新、共通証明書信頼ストアの設定などが行われます。Cisco Jabber デバイスが、オンプレミスとオフプレミス間で切り替わる場合、セキュア登録が完了する際は毎回、LSC と Certificate Authority Proxy Function（CAPF）登録の更新処理が複雑になります。

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 以降の Cisco Jabber デバイス向けのリリースで拡張されます。

以下は、OAuth に対して設定できる 電話機のセキュリティ プロファイル タイプ です。現時点では、これは Cisco Jabber でのみサポートされています。

- Cisco Dual Mode for iPhone（TCT デバイス）
- Cisco Dual Mode For Android（BOT デバイス）
- Cisco Unified Client Services Framework（CSF デバイス）
- Cisco Jabber for Tablet（TAB デバイス）
- ユニバーサル デバイス テンプレート（Universal Device Template）

SIP 登録向けの OAuth サポートは、Cisco Unified Communications Manager 14.0 以降の以下の Cisco IP 電話シリーズ企業モデル向けのリリースで拡張されます。

- 8811
- 8841
- 8851
- 8851NR
- 8861
- 7811
- 7821
- 7841
- 7861
- 8845
- 8865
- 8865NR
- 7832
- 8832
- 8832NR

SIP OAuth モードの前提条件

この機能は、次の作業が完了していることを前提としています。

- モバイルおよびリモートアクセスが設定され、Unified Communication Manager および Expressway 間で接続が確立されていることを確認します。
- **[エクスポート制御機能を許可する（allow export-controlled）]** 機能を使用して Unified Communications Manager が Smart または Virtual アカウントに登録されていることを確認します。

SIP OAuth モードの設定タスク フロー

システムの SIP OAuth を設定するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	デバイスの OAuth アクセス トークンの有効化	Cisco IP 電話 7800 および 8800 企業シリーズでの SIP 登録の OAuth を有効に

	コマンドまたはアクション	目的
		します。この手順は Cisco Jabber デバイスには適用できません。
ステップ 2	更新ログインの設定 （4 ページ）	SIP OAuth を介してデバイスを登録するために、Unified Communications Manager で 更新ログイン フローを使用した OAuth を有効化する。
ステップ 3	OAuth ポートの設定 （4 ページ）	OAuth が登録されているノードごとに、OAuth 用のポートを割り当てます。
ステップ 4	OAuth Connection を Expressway-C に設定 （5 ページ）	手動認証された TLS 接続を Expressway-C に設定します。
ステップ 5	SIP OAuth モードの有効化 （6 ページ）	パブリッシャ ノードで CLI コマンドを使用して OAuth サービスを有効にします。
ステップ 6	Cisco CallManager サービスの再起動 （6 ページ）	OAuth が登録されているすべてのノードで、このサービスを再起動します。
ステップ 7	セキュリティ プロファイルで OAuth サポートを設定 （6 ページ）	エンドポイントに対して暗号化を展開する場合、電話セキュリティ プロファイルで、OAuth サポートを設定します。

デバイスの OAuth アクセス トークンの有効化

電話機の OAuth アクセス トークンを有効にするには、次の手順を使用します。

（注） 電話機の SIP 登録に対する OAuth サポートにのみ、このエンタープライズ パラメータを設定します。

手順

ステップ 1 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。

ステップ 2 **[SSO および OAuth の設定]** セクションで、**[デバイスの OAuth アクセス トークン]** ドロップダウン リストの値が **Implicit:Already に登録済みのデバイスに設定されます。**

（注） **デバイスの OAuthアクセストークン**の値を **Explicit:Activation Code device onboarding required**に設定して、電話のSIP登録のOAuthサポートを無効にします。

ステップ 3 **[保存]** をクリックします。

更新ログインの設定

OAuth アクセス トークンを使用して更新ログインを設定し、Cisco Jabber クライアントのトークンを更新するには、次の手順を使用します。

手順

ステップ 1 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。

ステップ 2 **[SSO および OAuth 構成（SSO and OAuth Configuration）]** で、**OAuth with Refresh Login Flow** のパラメータを **[有効（Enabled）]** にします。

ステップ 3 （任意） **[SSO および OAuth 構成（SSO and OAuth Configuration）]** セクションで、各パラメータを設定します。パラメータの説明を確認するには、パラメータ名をクリックします。

ステップ 4 **[保存]** をクリックします。

OAuth ポートの設定

SIP OAuth に使用するポートを割り当てるには、次の手順を使用します。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。, **[システム（System）]** > **[Cisco Unified CM]**。

ステップ 2 SIP OAuth を使用するサーバごとに次の操作を行います。

ステップ 3 サーバを選択します。

ステップ 4 [Cisco Unified Communications Manager（Cisco Unified Communications Manager）] の **[TCP ポートの設定（TCP Port Settings）]** で、次のフィールドに対してポート値を設定します。

- SIP 電話 OAuth ポート（SIP Phone OAuth Port）

  デフォルト値は 5090 です。設定可能な範囲は 1024 ～ 49151 です。

- SIP モバイルおよびリモートアクセス ポート（SIP Mobile and Remote Access Port）

  デフォルト値は 5091 です。設定可能な範囲は 1024 ～ 49151 です。

（注） Cisco Unified Communications Manager は、SIP Phone OAuth Port (5090) を使用して、TLS 経由の Jabber OnPremise デバイスから SIP 回線登録をリッスンします。ただし、Unified CM は、SIP モバイル Remote Access ポート（デフォルト 5091）を使用して、mLTS 経由の Expressway を介した Jabber から SIP 回線登録をリッスンします。

両方のポートは、受信 TLS/mTLS 接続に対して tomcat 証明書と tomcat 信頼を使用します。Tomcat 信頼ストアが、モバイルおよびリモートアクセスが正常に機能するように、SIP OAuth モードの Expressway-C 証明書を検証できることを確認します。

次の場合は、Expressway-C 証明書を Unified Communications Manager の tomcat 証明書にアップロードするための追加の手順を実行する必要があります。

- Expressway-C 証明書と tomcat 証明書は、同じ CA 証明書では署名されません。
- Unified CM tomcat は、CA 署名はありません。

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 SIP OAuth を使用する各サーバに対して、この手順を繰り返します。

OAuth Connection を Expressway-C に設定

Cisco Unified Communications Manager Administration に Expressway-C 接続を追加するには、次の手順を使用します。SIP OAuth を使するモバイルおよびリモートアクセス モードのデバイスには、この構成が必要です。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **デバイス** > **Expressway-C**

ステップ 2 （任意）**[Expressway-C の検索 とリスト]** ウィンドウで、**[検索]** をクリックして、Expressway-C から Unified Communications Manager にプッシュされた X.509 サブジェクト名/サブジェクト代替名を確認します。

（注） 必要に応じて値を変更できます。また、エントリが存在しない場合は、Expressway-C 情報を追加します。

ユニファイド コミュニケーション マネージャとは別のドメインを持っている場合 、管理者は Cisco Unified CM の管理ユーザインターフェイスにアクセスして、Unified CM の設定でドメインを Expressway-C に追加する必要があります。

ステップ 3 **[新規追加]** をクリックします。

ステップ 4 Expressway-C に対して、IP アドレス、ホスト名または、完全修飾ドメイン名を入力します。

ステップ 5 説明を入力します。

ステップ 6 X.509 のサブジェクト名/Expressway-C のサブジェクトの別名を、Expressway-C 証明書から入力します。

ステップ 7 **[保存]** をクリックします。

SIP OAuth モードの有効化

SIP OAut モードを有効にするには、コマンドライン インターフェイスを使用します。パブリッシャ ノードでこの機能を有効にすると、すべてのクラスタ ノードでこの機能が有効になります。

手順

ステップ 1 Unified Communications Manager のパブリッシャ ノードで、コマンドライン インターフェイスにログインします。

ステップ 2 `utils sipOAuth-mode enable` の CLI コマンドを実行します。
システムは、読み取り専用の**クラスタ SIPOAuth Mode** 企業パラメータを **[有効]** に更新します。

Cisco CallManager サービスの再起動

CLI で SIP OAuth を有効にした後に、SIP OAuth を介してエンドポイントが登録されるすべてのノードで Cisco CallManager サービスを再起動します。

手順

ステップ 1 [Cisco Unified Serviceability] から、以下を選択します。 **[ツール]** > **[コントロールセンター]** > **[機能サービス]**

ステップ 2 **[サーバ（Server）]** ドロップダウン リストからサーバを選択します。

ステップ 3 **Cisco CallManager** サービスを確認し、[再起動（Restart）] をクリックします。

セキュリティ プロファイルで OAuth サポートを設定

SIP OAuth登録をサポートする暗号化されたエンドポイントを導入している場合は、次の手順を使用して OAuth 認証を設定します。

手順

ステップ 1 [Cisco Unified CM Administration]から、**[システム（System）]** > **[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 [検索（Find）] をクリックし、電話機に使用されているセキュリティプロファイルを選択します。

ステップ 3 [デバイス セキュリティ モード（Device Security Mode）] が [暗号化（Encrypted）] であり、[転送タイプ（Transport Type）] が [TLS] であることを確認します。

ステップ 4 [OAuth 認証の有効化（Enable OAuth Authentication）]チェックボックスをオンにします。

ステップ 5 **[保存（Save）]** をクリックします。

（注） [SIP OAuth モード（SIP OAuth Mode）] が有効な場合、**[ダイジェスト認証を有効化（Enable Digest Authentication）]** および **[TFTP 暗号化設定（TFTP Encrypted Config）]** オプションはサポートされません。