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。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すべてのデバイスの認証に OAuth 更新トークンを使用できます。この機能により、Unified Communications Managerのセキュリティが強化されます。

Unified Communications Managerは、エンドポイントによって提示されたトークンを検証し、許可されたものにのみ構成ファイルを提供します。Unified Communications Managerクラスタおよびその他のシスコのデバイスで 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。

以下で、SIP 登録の OAuth サポートが拡張されました

- CiscoUnified Communications Manager12.5リリース以降の Cisco Jabber デバイス
- CiscoUnified Communications Managerリリース 14 以降の SIP 電話

（注） デフォルトでは、SIP OAUth が有効になっている場合、TFTP は SIP 電話に対して安全です。TFTP ファイルのダウンロードは、認証された電話に対してのみ、セキュリティで保護されたチャネルを介して行われます。SIP OAuth は、オンプレミスおよび MRA を介して CAPF を使用せずに、エンドツーエンドの安全なシグナリングとメディア暗号化を提供します。

次に、OAuth 用に設定できる電話セキュリティプロファイルのタイプを示します。

- 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）
- Cisco 8811
- Cisco 8841
- Cisco 8851
- Cisco 8851NR
- Cisco 8861
- Cisco 7811
- Cisco 7821
- Cisco 7841
- Cisco 7861
- Cisco 8845
- Cisco 8865
- Cisco 8865NR
- Cisco 7832
- Cisco 8832
- Cisco 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ていること、および接続がユニファイドコミュニケーションマネージャとエクスプレス Sway の間で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。
- クライアントファームウェアが SIPOAuth をサポートし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	Phone Edge TrustへのCA証明書のアップロード	トークンを取得するには、CA 証明書を電話エッジトラストにアップロードします。この手順は、Cisco Jabber デバイスには適用されません。
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	電話セキュリティプロファイルでデバイスセキュリティモードを設定する	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。

Phone Edge TrustへのCA証明書のアップロード

この手順を使用して、Tomcat 署名付き証明書のルート証明書を Phone EdgeTrust にアップロードします。

（注） この手順は Cisco Phone に対してのみ実行され、Cisco Jabber には適用されません。

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

ステップ 2 [Upload Certificate/Certificate chain] をクリックします。

ステップ 3 **[証明書/証明書チェーンのアップロード]** ウィンドウで、**[証明書の目的]** ドロップダウンリストから **[電話-エッジ-信頼]** を選択します。

ステップ 4 **[ファイルのアップロード]** フィールドで、**[参照]** をクリックして証明書をアップロードします。

ステップ 5 [アップロード（Upload）] 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。

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（Save）]** 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。

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 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、ユニファイド CM は、SIP モバイルリモートアクセスポート (デフォルトは 5091) を使用して、 mTLS を介して Jabber からの 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。

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（Save）]** 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。

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。

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。

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。

電話セキュリティプロファイルでデバイスセキュリティモードを設定する

この手順を使用して、電話機のセキュリティプロファイルで**デバイスセキュリティモード（Device Security Mode）**を設定します。これは、その電話機の**[電話機のセキュリティプロファイル（Phone Security Profile）]**内でデバイスセキュリティモードを**[暗号化（Encrypted）]**に設定している場合にのみ必要です。

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、**[システム（System）]** > **[セキュリティ（Security）]** > **[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 次のいずれかを実行します。

- 既存の電話セキュリティプロファイルを検索する
- [新規追加（Add New）] をクリックします。

ステップ 3 [電話セキュリティプロファイル情報（Phone Security Profile Information）] セクションの **[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から、**[暗号化（Encrypted）]** を選択します。

ステップ 4 **[転送タイプ（Transport type）]** ドロップダウンリストで、**[TLS]** を選択します。

ステップ 5 [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 6 **[保存（Save）]** をクリックします。

ステップ 7 電話セキュリティプロファイルを電話に関連付けます。電話セキュリティ電話を適用する方法の詳細については、Cisco Unified Communications Manager セキュリティガイドの「セキュリティプロファイルを電話に適用する」セクションを参照してください。

（注） 変更を有効にするには、スマートフォンをリセットしてください。

（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。電話機は、**https(6971)**を介して TFTP 設定ファイルを安全にダウンロードし、認証にトークンを使用します。

SIPOAuth 登録済み電話を MRA モード用に構成する

この手順を使用して、SIPOAuth 登録済み電話を MRA モードに構成します。

始める前に

電話機がアクティベーションコードを使用するように設定されていることを確認してください。詳細については、Cisco Unified Communications Manager システム設定ガイドの「アクティベーションコードを使用するための登録方法の設定」セクションを参照してください。

（注） SIP OAuth over MRA を使用する場合、ユーザーはログインにユーザー名/パスワードを使用できませんが、オンボーディングに基づくアクティベーションコードを使用する必要があります

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（Device）]** > **[電話（Phone）]**。

ステップ 2 **[検索]** をクリックして、オフプレミスモード用に構成するデバイスを選択します。

ステップ 3 **[デバイス情報]** セクションで、次の手順を実行します。

- **[MRA経由でアクティベーションコードを許可する（Allow Activation Code via MRA）]** チェックボックスをオンにします。
- **[アクティベーションコードMRAサービスドメイン]** ドロップダウンリストから、必要な MRA サービスドメインを選択します。MRA サービスドメインを設定する方法の詳細については、Cisco Unified Communications Manager システム設定ガイドの「*MRA* サービスドメインの設定」セクションを参照してください。

（注） SIP OAuth over MRA モードの場合、アクティベーションコードのみを使用し、ユーザー名/パスワードベースのログインは使用しないでください。

ステップ 4 **[プロトコル固有の情報]** セクションで、**[デバイスセキュリティプロファイル]** ドロップダウンリストから OAuth 対応の SIP プロファイルを選択します。電話機が OAuth ファームウェアをサポートしていることを確認してください。セキュリティプロファイルの作成方法の詳細については、Cisco Unified Communications Manager システム設定ガイドの「電話セキュリティプロファイルの設定」セクションを参照してください。

ステップ 5 **[保存（Save）]** と **[構成の適用（Apply Configuration）]** をクリックします。

（注） 電話機は MRA モードに切り替わり、Expressway との通信を開始します。内部ネットワークでオンプレミスからのライン Sway との通信が許可されていない場合、電話機は登録されませんが、オフプレミスの電源がオンになっているときには、その電話機に接続する準備ができています。