



基本的なセキュリティの設定

- [セキュリティの設定について \(1 ページ\)](#)
- [セキュリティ設定のタスク \(1 ページ\)](#)

セキュリティの設定について

ここでは、Cisco Unified Communications Manager を設定するために実行する必要がある基本的なセキュリティ設定タスクについて説明します。

セキュリティ設定のタスク

基本的なセキュリティ設定をセットアップするには、次のタスクを実行します。

- [クラスタの混合モードの有効化 \(1 ページ\)](#)
- [証明書のダウンロード \(2 ページ\)](#)
- [証明書署名要求の生成 \(2 ページ\)](#)
- [証明書署名要求のダウンロード \(3 ページ\)](#)
- [サードパーティの認証局のルート証明書のアップロード \(3 ページ\)](#)
- [最小 TLS バージョンの設定 \(4 ページ\)](#)
- [TLS 暗号化の設定 \(5 ページ\)](#)

クラスタの混合モードの有効化

クラスタ内で混合モードを有効にするには、次の手順を実行します。

手順

-
- Step 1** パブリッシュ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。
- Step 2** **utils ctl set-cluster mixed-mode** CLI コマンドを実行します。

(注) 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、および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で輸出制御機能の許可が有効になっており、そのトークンがこのクラスタに登録されていることを確認します。

証明書のダウンロード

CSR 要求を送信する場合は、ダウンロード証明書タスクを使用して証明書のコピーを作成するか、証明書をアップロードします。

手順

-
- Step 1** [Cisco Unified OS Administration] から [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。
- Step 2** 検索情報を指定し、[検索 (Find)] をクリックします。
- Step 3** 必要なファイル名を選択し、[ダウンロード (Download)] をクリックします。
-

証明書署名要求の生成

証明書署名要求 (CSR) を生成します。これは、公開キー、組織名、共通名、地域、および国などの証明書申請情報を含む暗号化されたテキストのブロックです。認証局はこの CSR を使用して、ご使用のシステムの信頼できる証明書を生成します。



(注) 新しい CSR を生成すると、既存の CSR は上書きされます。

手順

-
- Step 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。
- Step 2** [CSR の作成 (Generate CSR)] をクリックします。

- Step 3** [証明書署名要求の作成 (Generate Certificate Signing Request)] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、オンラインヘルプを参照してください。
- Step 4** [生成 (Generate)] をクリックします。

証明書署名要求のダウンロード

CSR を生成した後にダウンロードし、認証局に提出する準備をします。

手順

- Step 1** [Cisco Unified OS Administration] から [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。
- Step 2** [CSR のダウンロード (Download CSR)] をクリックします。
- Step 3** [証明書の用途 (Certificate Purpose)] ドロップダウンリストで、証明書名を選択します。
- Step 4** [CSR のダウンロード (Download CSR)] をクリックします。
- Step 5** (任意) プロンプトが表示されたら、[保存 (Save)] をクリックします。

サードパーティの認証局のルート証明書のアップロード

CA ルート証明書を CAPF 信頼ストアと Unified Communications Manager 信頼ストアにアップロードし、外部 CA を使用して LSC 証明書に署名します。



(注) LSC の署名にサードパーティ CA を使用しない場合は、このタスクをスキップします。

手順

- Step 1** [Cisco Unified OS Administration] から [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。
- Step 2** [証明書/証明書チェーンのアップロード (Upload Certificate/Certificate chain)] をクリックします。
- Step 3** [証明書の目的 (Certificate Purpose)] ドロップダウンリストで、[CAPF 信頼 (CAPF-trust)] を選択します。
- Step 4** 証明書の説明を [説明 (Description)] に入力します。たとえば、外部 LSC 署名 CA の証明書のよう指定します。
- Step 5** [参照 (Browse)] をクリックしてファイルに移動してから、[開く (Open)] をクリックします。
- Step 6** [アップロード (Upload)] をクリックします。

- Step 7** このタスクを繰り返し、[証明書の用途 (Certificate Purpose)] を [CallManager 信頼 (callmanager-trust)] として証明書をアップロードします。

TLS の前提条件

最低 TLS バージョンを設定する前に、ネットワーク デバイスとアプリケーションの両方でその TLS バージョンがサポートされていることを確認します。また、それらが、ユニファイド コミュニケーション マネージャ IM およびプレゼンスサービス で設定する TLS で有効になっていることを確認します。次の製品のいずれかが展開されているなら、最低限の TLS 要件を満たしていることを確認します。この要件を満たしていない場合は、それらの製品をアップグレードします。

- Skinny Client Control Protocol (SCCP) Conference Bridge
- トランスコーダ (Transcoder)
- ハードウェア メディア ターミネーション ポイント (MTP)
- SIP ゲートウェイ
- Cisco Prime Collaboration Assurance
- Cisco Prime Collaboration Provisioning
- Cisco Prime Collaboration Deployment
- Cisco Unified Border Element (CUBE)
- Cisco Expressway
- Cisco TelePresence Conductor

会議ブリッジ、メディアターミネーションポイント (MTP)、Xcoder、Prime Collaboration Assurance および Prime Collaboration Provisioning をアップグレードすることはできません。



- (注) ユニファイド コミュニケーション マネージャ の旧リリースからアップグレードする場合は、上位のバージョンの TLS を設定する前に、すべてのデバイスとアプリケーションでそのバージョンがサポートされていることを確認します。たとえば、ユニファイド コミュニケーション マネージャ IM およびプレゼンスサービスのリリース 9.x でサポートされるのは、TLS 1.0 のみです。

最小 TLS バージョンの設定

デフォルトでは、Unified Communications Manager において、最小 TLS バージョンとして 1.0 がサポートされています。Unified Communications Manager および IM and Presence Service の最低サポート TLS バージョンを 1.1 または 1.2 などの上位バージョンにリセットするには、次の手順を使用します。

設定対象の TLS バージョンが、ネットワーク内のデバイスとアプリケーションでサポートされていることを確認します。詳細については、「[TLS の前提条件（4 ページ）](#)」を参照してください。

手順

-
- Step 1** コマンドライン インターフェイスにログインします。
- Step 2** 既存の TLS のバージョンを確認するには、**show tls min-version** CLI コマンドを実行します。
- Step 3** **set tls min-version <minimum>** CLI コマンドを実行します。ここで、<minimum> は TLS のバージョンを示します。
- たとえば、最低 TLS バージョンを 1.2 に設定するには、**set tls min-version 1.2** を実行します。
- Step 4** すべての Unified Communications Manager と IM and Presence Service クラスタノードで、手順 3 を実行します。
-

TLS 暗号化の設定

SIP インターフェイスで使用可能な最強の暗号方式を選択することで、弱い暗号を無効にすることができます。TLS 接続を確立するために Unified Communications Manager でサポートされる暗号化を設定するには、この手順を使用します。

手順

-
- Step 1** Cisco Unified CM Administration から、[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。
- Step 2** [セキュリティ パラメータ (Security Parameters)] で、[TLS 暗号化 (TLS Ciphers)] エンタープライズパラメータの値を設定します。使用可能なオプションについては、エンタープライズパラメータのオンラインヘルプを参照してください。
- Step 3** [保存 (Save)] をクリックします。
- (注) すべての TLS 暗号は、クライアントの暗号設定に基づいてネゴシエートされます。
-

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。