デフォルトのセキュリティ

デフォルトのセキュリティの概要

デフォルトのセキュリティ機能は、追加の設定要件を必要とせずに、サポートされている Cisco Unified IP 電話 に対して基本レベルのセキュリティを提供します。

この機能は、サポートされている IP 電話に次のデフォルト セキュリティを提供します。

- TFTP のデフォルト認証
- オプションの暗号化
- 証明書の検証

デフォルトのセキュリティは以下のコンポーネントを使用して、安全ではない環境で基本的なセキュリティを提供します。

- Identity Trust List（ITL）：このファイルは TFTP サービスがクラスタのインストール時に有効化された後にのみ作成され、信頼を確立するために Cisco Unified IP 電話 により使用されます。
- 信頼検証サービス：このサービスはすべての Unified Communications Manager ノードで実行され、Cisco Unified IP 電話 の証明書の認証を行います。 TVS 証明書は他のいくつかの重要な証明書と共に ITL ファイルにバンドルされています。

初期信頼リスト

初期セキュリティには初期信頼リスト（ITL）ファイルが使用され、エンドポイントが Unified Communications Manager を信頼できるようになります。 ITL では、セキュリティ機能を明示的に有効にする必要はありません。 TFTP サービスが有効になり、クラスターがインストールさ

れると、ITL ファイルが自動的に作成されます。 Unified Communications Managerの TFTP サーバの秘密鍵は ITL ファイルへの署名に使用されます。

Unified Communications Manager クラスタまたはサーバがノンセキュアモードの場合、ITL ファイルはサポートされている Cisco Unified IP 電話毎にダウンロードされます。 CLI コマンド **admin:show itl**を使用して、ITL ファイルのコンテンツを表示できます。

Cisco Unified IP 電話 は、次のタスクを実行するために ITL ファイルを必要とします。

- CAPF との安全な通信、これは設定ファイルの暗号化をサポートするための前提条件です。
- 構成ファイルの署名を認証する
- TVS を使用して HTTPS を確立する際に、EM サービス、ディレクトリ、MIDlet などのアプリケーションサーバを認証します。

Cisco IP 電話に既存の CTL ファイルがない場合、最初の ITL ファイルが自動的に信頼されます。 TVS は署名者に対応する証明書を返すことができなければなりません。

Cisco IP 電話に既存の CTL ファイルがある場合、その CTL ファイルを使用して ITL ファイルの署名を認証します。

（注） SHA-1 または MD5 アルゴリズムの値は、Initial Trust List (ITL) ファイルの値が変更された場合にのみ変更されます。 ITL ファイルのチェックサム値を使用して、Cisco IP 電話の ITL ファイルと Unified Communications Manager クラスタ間の違いを識別することができます。 ITL ファイルのチェックサム値は、ITL ファイルを変更した場合にのみ変更されます。

初期信頼リスト (ITL) ファイルの形式は CTL ファイルと同じです。 しかし、それはより小さく、無駄のないバージョンです。

次の属性が ITL ファイルに適用されます。

- TFTP サービスがアクティブで、クラスタをインストールすると、システムは ITL ファイルを自動的に構築します。 コンテンツが変更されると、ITL ファイルは自動的に更新されます。
- ITL ファイルは eToken を必要としません。 ソフト eToken (TFTP サーバの CallManager 証明書に関連する秘密鍵) を使用します。
- Cisco Unified IP 電話 は、リセット中、再起動中、または CTL ファイルのダウンロード後に、ITL ファイルをダウンロードします。

ITL ファイルには次の証明書が含まれます:

- ITLRecovery 証明書 - この証明書は ITL ファイルに署名します。
- TFTP サーバの CallManager 証明書—この証明書により、ITL ファイルの署名および電話構成ファイルの署名を認証することができます。
- クラスターで使用可能なすべての TVS 証明書 - これらの証明書により、電話は TVS と安全に通信し、証明書による認証を要求できます。

- CAPF 証明書：この証明書は設定ファイルの暗号化をサポートします。 CAPF 証明書は ITL ファイルで必要ではありませんが (TVS はそれを認証できます)、CAPF への接続を簡素化します。

ITL ファイルには各証明書のレコードが含まれています。各レコードには以下の内容が含まれています。

- 証明書
- Cisco IP 電話で簡単に検索できる事前抽出証明書フィールド
- 証明書の役割（TFTP、CUCM、TFTP+CCM、CAPF、TVS、SAST）

TFTP サーバの CallManager 証明書は、2 つの異なるロールを持つ 2 つの ITL レコードに存在します。

- TFTP または TFTP と CCM ロール：設定ファイルの署名を認証します。
- SAST ロール：ITL ファイルの署名を認証します。

ITLRecovery証明書のための証明書管理の変更

- ITLRecovery の有効期間が 5 年から 20 年に延長され、ITLRecovery 証明書がより長期間同じ状態を維持できるようになりました。

（注） ITLRecovery 証明書のデフォルトの有効期間は 5 年です。 しかし、ITLRecovery 証明書の有効期間を 5、10、15、または 20 年に設定することもできます。 Unified Communications Manager のアップグレード中に、ITLRecovery 証明書が新しいリリースにコピーされます。

- ITLRecovery 証明書を再生成する前に、CLI と GUI の両方に警告メッセージが表示されます。 この警告メッセージは、トークンなしの CTL を使用する場合、および CallManager 証明書を再生成する場合は、CTL ファイルに更新された CallManager 証明書が含まれていること、およびその証明書がエンドポイントに更新されていることを確認するために表示されます。

ITLRecovery 証明書

ITLRecovery 証明書機能では、新しいドロップダウンリスト [**ITL ファイルの状況**] を使用して、管理者は古い ITL を持つ電話を識別し、これらの電話に対して必要なアクションを実行できるようにすることができます。

一部の電話は最新の ITL ファイルを取得せず、ITL ファイルが更新されたときに古いものを保持します (CM 証明書の更新など)。 システムは、ユーザ インターフェイスに、一致しない ITL ファイルを持つ電話の一元化されたレポートを表示します。

以下は、さまざまな ITLRecovery シナリオです。

TFTP サービスのアクティベーション:

- TFTP サービスがアクティブになると、生成された ITL ファイルのハッシュとサーバのホスト名が DB に保存されます。 TFTP コードで ITL 更新が行われるたびに更新されます。
- TFTP ホスト名がすでにテーブルに存在する場合、生成された ITL ハッシュが保存されている値と比較されます。
  - ITL ハッシュが同じでない場合、新しい ITL ハッシュは DB で更新されます。
  - ITL ハッシュが同じである場合、TFTP ログは「TFTP ITL ハッシュが変更されていません」を示します。

デバイスの登録と ITLFile のダウンロード

- 電話が Unified Communications Managerで登録する際に、サーバに存在する ITLFile の詳細 (サーバのホスト名、ハッシュ、タイムスタンプ) が DB に存在しない場合に挿入されます。
- 電話が Unified Communications Manager に登録されると、その電話に適用されている ITL ファイルの詳細を含むSIPアラームが送信されます。 これは、データベースに保存されている ITL ファイルのハッシュと比較されます。
  - ITLハッシュが同じ場合、デバイスハッシュ情報は新しいタイムスタンプで更新されます。
  - ITL ハッシュが同じでない場合、報告された ITL ハッシュとタイムスタンプがデバイスに対して更新されます。
- 電話の登録を解除すると、そのデバイスの信頼ハッシュ情報は削除されます。

連携動作と制限事項

ある Unified Communications Manager クラスタに 39 個を超える証明書がある場合、Cisco IP 電話上の ITL ファイルサイズは 64KB を超えます。 ITL ファイルサイズの増加は、電話での ITL の適切な読み込みに影響を与え、その結果、Unified Communications Managerに登録する際に電話の登録が失敗することがあります。

信頼検証サービス

ネットワークには多数の電話が接続されており、これらの電話のメモリ容量は限られています。 Cisco Unified IP 電話 このため、 Unified Communications Manager はTVSを通じてリモートの信頼ストアとして機能し、証明書の信頼ストアを各電話に配置する必要がなくなります。 Cisco Unified IP 電話（電話）は CTL または ITL ファイルを通じて署名または証明書を確認できないため、確認のために TVS サーバと通信します。 このように、すべての Cisco Unified IP 電話（電話）にトラストストアがあるよりも、中央のトラストストアにある方が管理が容易です。

TVSにより、HTTPSを確立する際に、EMサービス、ディレクトリ、MIDletなどのアプリケーションサーバをCisco Unified IP 電話 （電話）で認証できるようになります。

TVS は以下の機能を提供します。

- スケーラビリティ - Cisco Unified IP 電話 （電話）のリソースは信頼する証明書の数に影響されません。
- 柔軟性—信頼できる証明書の追加または削除は、システムに自動的に反映されます。
- デフォルトでのセキュリティ - 非メディアおよびシグナリングセキュリティ機能は既定のインストールに含まれており、ユーザの介入を必要としません。

（注） セキュアなシグナリングとメディアを有効にする場合、CTLファイルを作成し、クラスタを混合モードに設定します。 CTLファイルを作成し、クラスタを混合モードに設定するには、CLIコマンド **utils ctl set-cluster 混合モード**を使用します。

以下は、TVS を説明する基本概念です。

- TVS は Unified Communications Manager サーバ上で動作し、Cisco IP Phoneの代わりに証明書の認証を行います。
- Cisco Unified IP 電話 すべての信頼できる証明書をダウンロードする代わりに、TVS のみを信頼する必要があります。
- ITL ファイルはユーザの介入なしで自動的に生成されます。 ITL ファイルは Cisco Unified IP 電話 によりダウンロードされ、そこから信頼が流れます。

認証、完全性、および認可

整合性と認証により、次の脅威から保護します。

- TFTP ファイル改ざん (整合性)
- Unified Communications Manager と電話間のコール処理シグナリングの変更 (認証)
- 中間者攻撃 (認証) です。 頭字語 セクションに定義されています。
- 電話およびサーバでのなりすまし (認証)
- リプレイ攻撃 (ダイジェスト認証)

承認では、認証されたユーザ、サービス、またはアプリケーションが実行できることを指定します。 単一のセッションで複数の認証および認可方法を実装できます。

イメージ認証（Image authentication）

このプロセスにより、IP電話にロードする前に、ファームウェア ロードであるバイナリ イメージの改ざんが防止されます。イメージが改ざんされると、電話機は認証プロセスに失敗し、新

しいイメージを拒否します。 画像認証は、ユニファイドコミュニケーションズマネージャ のインストール時に自動的にインストールされる、署名されたバイナリファイルを通じて行われます。 同様に、ウェブからダウンロードしたファームウェア更新も署名済みバイナリイメージを提供します。

デバイス認証

このプロセスにより、通信デバイスの ID を検証し、エンティティが要求されているとおりのものであることを確認します。

Unified Communications Manager サーバとサポートされている Cisco Unified IP Phone 、SIP トランク、または JTAPI/TAPI/CTI アプリケーションの間で端末認証が行われる (サポートされている場合)。 認証された接続は、各エンティティが他のエンティティの証明書を受け入れる場合にのみ、これらのエンティティ間で発生します。 相互認証は、この相互証明書交換のプロセスを説明します。

端末認証は、CiscoCTL ファイル（ Unified Communications Manager サーバノードとアプリケーションの認証用）と証明書機関プロキシ機能（端末と JTAPI/TAPI/CTI アプリケーションの認証用）の作成に依存しています。

ヒント SIP トランク経由で接続する SIP ユーザエージェントは、CallManager 信頼ストアに SIP ユーザエージェント証明書が含まれており、SIP ユーザエージェントが Unified Communications Manager 証明書を信頼ストアに含んでいる場合、 Unified Communications Manager で認証します。 CallManager トラストストアの更新についての詳細は、この *Unified Communications Manager* リリースをサポートする『 Cisco Unified Communications オペレーティングシステム管理ガイド』を参照してください。

ファイル認証

このプロセスでは、電話がダウンロードしたデジタル署名されたファイルを検証します。たとえば、設定、着信音リスト、ロケール、および CTL ファイルです。 電話機は、ファイル作成後にファイルの改ざんが行われていないことを確認するために、署名を検証します。 対応端末については、 「対応電話モデル」をご覧ください。

混合モードでクラスターを設定する場合、TFTP サーバは、着信音リスト、ローカライズ、default.cnf.xml、着信音リスト wav ファイルなどの静的ファイルに.sgn 形式で署名します。 TFTP サーバは、ファイルにデータ変更があったことを確認するたびに、<device name>.cnf.xml 形式のファイルに署名します。

キャッシュが無効になっている場合、TFTP サーバは署名済みファイルをディスクに書き込みます。 TFTP サーバは保存されたファイルが変更されたことを確認すると、ファイルに再署名します。ディスク上の新しいファイルは、保存されたファイルを削除されると上書きします。電話が新しいファイルをダウンロードする前に、管理者は影響を受けるデバイスを Unified Communications Manager で再起動する必要があります。

TFTPサーバからファイルを受信した後、電話機はファイルの署名を検証することにより、ファイルの整合性を確認します。 電話が認証された接続を確立するには、次の条件が満たされている必要があります。

- 証明書が電話に存在している必要があります。
- CTLファイルが電話機上に存在している必要があり、さらにUnified Communications Managerのエントリと証明書がCTLファイル中に存在している必要があります。
- デバイスの認証または暗号化を構成しました。

シグナリング認証（Signaling Authentication）

シグナリング整合性とも呼ばれるこのプロセスは、TLSプロトコルを使用して、送信中にシグナリング パケットに改ざんが発生していないことを検証します。

シグナリング認証は、証明書信頼リスト (CTL) ファイルの作成に依存しています。

ダイジェスト認証

SIP トランクと電話に対するこのプロセスにより、Unified Communications Managerは、Unified Communications Managerに接続するデバイスの身元を問い詰めることができます。 要求されると、デバイスは確認のため、ユーザ名とパスワードのようなダイジェスト資格情報をUnified Communications Managerに提示します。 提示された資格情報がその端末のデータベースで構成されているものと一致する場合、ダイジェスト認証が成功し、Unified Communications Managerが SIP リクエストを処理します。

（注） クラスタ セキュリティ モードはダイジェスト認証には影響しないことに注意してください。

（注） デバイスのダイジェスト認証を有効にすると、デバイスを登録するための一意のダイジェストユーザ ID とパスワードが要求されます。

Unified Communications Manager データベース内の電話ユーザーまたはアプリケーションユーザー用に SIP ダイジェスト認証情報を設定します。

- アプリケーションの場合は、[アプリケーションユーザーの設定（Application User Configuration）] ウィンドウでダイジェスト認証情報を指定します。
- SIP を実行している電話の場合、[エンドユーザ] ウィンドウでダイジェスト認証資格情報を指定します。 ユーザを設定した後で電話に資格情報を関連付けるには、[電話の設定] ウィンドウで [ダイジェスト ユーザ] とエンド ユーザを選択します。 電話をリセットすると、TFTP サーバーが電話に提供する電話設定ファイルに認証情報が含まれるようになります。 TFTP ダウンロードでダイジェスト認証情報が平文で送信されないようにするには、暗号化された電話設定ファイルのセットアップに関するトピックを参照してください。

- SIP トランクで受信したチャレンジについては、領域ユーザー名（デバイスまたはアプリケーションユーザー）とダイジェスト認証情報を指定する SIP 領域を設定します。

SIP を実行している外部電話またはトランクのダイジェスト認証を有効にし、ダイジェスト認証情報を設定すると、Unified Communications Manager は、ユーザー名、パスワード、および領域のハッシュ値を含む認証情報のチェックサムを計算します。 システムは MD5 ハッシュを計算するために、乱数であるナンス値を使用します。 Unified Communications Manager は値を暗号化し、ユーザ名とチェックサムをデータベースに保存します。

チャレンジを開始するために、Unified Communications Manager は SIP 401（未承認）メッセージを使用します。このメッセージには、ヘッダーにナンスとレルムが含まれます。 電話またはトランクの SIP デバイス セキュリティ プロファイルで、ナンスの有効時間を設定します。 ナンスの有効時間は、ナンスの値が有効である時間を分単位で指定します。 この時間間隔が終了すると、 Unified Communications Manager は外部デバイスを拒否し、新しい番号を生成します。

（注） Unified Communications Manager は、回線側の電話またはデバイスから発信された SIP 通話のユーザー エージェント サーバー（UAS）、SIP トランクへの発信コールのユーザー エージェント クライアント（UAC）、または回線間またはトランク間接続のバックツーバック ユーザー エージェント（B2BUA）として機能します。 ほとんどの環境で、 Unified Communications Manager は主に SCCP と SIP エンドポイントを接続する B2BUA として機能します。 (SIP ユーザ エージェントは SIP メッセージを発信するデバイスまたはアプリケーションを表します。)

ヒント ダイジェスト認証は完全性や機密性を提供しません。デバイスの整合性と機密性を確保するには、デバイスが TLS をサポートしている場合、デバイスの TLS プロトコルを構成します。 デバイスが暗号化をサポートしている場合、デバイス セキュリティ モードを暗号化として構成します。デバイスが暗号化された電話構成ファイルをサポートしている場合、ファイルの暗号化を構成します。

電話のダイジェスト認証

電話のダイジェスト認証を有効にすると、Unified Communications Manager は、キープアライブメッセージを除く、SIP を実行している電話に対するすべての要求に認証を要求します。 Unified Communications Manager は、回線側の電話からのチャレンジには応答しません。

レスポンスを受信した後、Unified Communications Manager はデータベースに保存されているユーザー名のチェックサムを、レスポンスヘッダーの資格情報と照合します。

SIP を実行する電話機は、Unified Communications Manager 領域にあります。これは、Unified Communications Manager Administration のインストール時に定義されます。 SIP ステーション領域のサービス パラメータを使用して、電話に対するチャレンジのための SIP 領域を設定します。 各ダイジェストユーザーは、領域ごとに 1 セットのダイジェスト資格情報を持つことができます。

ヒント　エンドユーザのダイジェスト認証を有効にしているが、ダイジェストクレデンシャルを設定していない場合、電話は登録に失敗します。クラスタモードがノンセキュアで、ダイジェスト認証を有効にしてダイジェストクレデンシャルを設定している場合、ダイジェストクレデンシャルが電話に送信され、 Unified Communications Manager は引き続きチャレンジを開始します。

トランクのダイジェスト認証

トランクのダイジェスト認証を有効にすると、Unified Communications Manager は、SIP トランク経由で接続する SIP デバイスおよびアプリケーションからの SIP トランクリクエストをチャレンジします。 システムは、チャレンジ メッセージで Cluster ID エンタープライズ パラメータを使用します。 SIP トランクを通じて接続する SIP ユーザーエージェントは、 Unified Communications Manager でデバイスまたはアプリケーションに対して設定した固有のダイジェスト認証情報で応答します。

Unified Communications Manager が SIP トランクリクエストを開始すると、SIP トランクを通して接続する SIP ユーザーエージェントは、 Unified Communications Manager のアイデンティティをチャレンジすることができます。 これらの着信チャレンジの場合、ユーザに要求された資格情報を提供するように SIP レルムを構成します。 Unified Communications Manager が SIP 401（未承認）または SIP 407（プロキシ認証が必要）メッセージを受信すると、 Unified Communications Manager は、トランク経由で接続する領域の暗号化パスワードと、チャレンジメッセージで指定されているユーザー名を検索します。 Unified Communications Manager はパスワードを解読し、ダイジェストを計算してレスポンスメッセージで提示します。

ヒント　領域は xyz.com などの SIP トランクを介して接続するドメインを表し、リクエストの送信元を特定するのに役立ちます。

SIP 領域を設定するには、SIP トランクのダイジェスト認証に関するトピックを参照してください。 Unified Communications Manager でチャレンジする Unified Communications Manager のユーザーエージェントごとに、SIP 領域、ユーザー名とパスワードを設定する必要があります。各トユーザーエージェントは、領域ごとに 1 セットのダイジェスト資格情報を持つことができます。

認証

Unified Communications Manager は、認可プロセスを使用して、SIP を実行している電話、SIP トランク、SIP トランク上の SIP アプリケーション要求からの特定のカテゴリのメッセージを制限します。

- SIP INVITE メッセージ、ダイアログ内メッセージ、および SIP を実行している電話の場合、Unified Communications Manager は、コーリングサーチスペースとパーティションを使用した認可を行います。

- 電話からの SIP SUBSCRIBE 要求の場合、 Unified Communications Manager は、ユーザがプレゼンスグループにアクセスするための認証を提供します。
- SIP トランク Unified Communications Manager は、プレゼンスサブスクリプションと特定の非 INVITE SIP メッセージの認証を行います。たとえば、ダイヤル外の REFER、一方的な通知、replaces ヘッダーを持つ SIP 要求などです。 ウィンドウで許可された SIP リクエストにチェックを入れて、[SIP トランクセキュリティプロファイルの設定（SIP Trunk Security Profile Configuration）] ウィンドウでの権限を指定します。

SIP トランクアプリケーションの認証を有効にするには、[SIP トランクセキュリティプロファイル] ウィンドウで [アプリケーションレベル認証を有効にする] と [ダイジェスト認証] チェックボックスを選択します。次に、[アプリケーションユーザの構成] ウィンドウで、許可された SIP 要求のチェックボックスをオンにします。

SIP トランク認証とアプリケーションレベル認証の両方を有効にした場合、認証はまず SIP トランクに対して行われ、次に SIP アプリケーションユーザに対して行われます。 トランク Unified Communications Manager はトランクのアクセスコントロールリスト (ACL) 情報をダウンロードしてキャッシュします。 ACL 情報が着信 SIP リクエストに適用されます。 ACL が SIP 要求を許可しない場合、通話は 403 Forbidden メッセージで失敗します。

ACL で SIP リクエストが許可されている場合、 Unified Communications Manager は SIP トランクセキュリティプロファイルでダイジェスト認証が有効になっているかどうかを確認します。ダイジェスト認証およびアプリケーションレベル認証が有効ではない場合、 Unified Communications Manager がリクエストを処理します。 ダイジェスト認証が有効な場合、Unified Communications Manager は受信リクエストに認証ヘッダーが存在することを確認し、ダイジェスト認証を使用してソースアプリケーションを識別します。 ヘッダーが存在しない場合、Unified Communications Manager は 401 メッセージでデバイスにチャレンジを行います。

アプリケーションレベルの ACL が適用される前に、 Unified Communications Manager はダイジェスト認証でSIP トランクユーザエージェントを認証します。そのため、アプリケーションレベルの承認を行う前に、SIP トランクセキュリティプロファイルでダイジェスト認証を有効にしておく必要があります。

NMAP スキャン操作

脆弱性スキャンを実行するために、Windows または Linux プラットフォームでネットワークマッパー (NMAP) スキャンプログラムを実行できます。 NMAP は、ネットワーク探索またはセキュリティ監査のための無料のオープン ソース ユーティリティです。

（注） NMAP DP スキャンは、完了までに最大 18 時間かかる場合があります。

構文

nmap-n-vv-sU-p<*port_range*><*ccm_ip_address*>

引数の説明

-n: DNS 解決を行いません。 見つけたアクティブな IP アドレスで逆 DNS 解決を行わないように NMAP に指示します。 DNS は NMAP ビルトイン並列スタブリソルバーを使用しても遅い場合があるため、このオプションによりスキャン時間を大幅に短縮できます。

-v: 冗長レベルを上げます。これにより NMAP は進行中のスキャンに関する詳細情報を出力します。 システムは、開いているポートが見つかると表示し、スキャンに数分以上かかると NMAP が予測した場合は、完了時間の予測を提供します。 このオプションを 2 回以上使用すると、冗長性がさらに高まります。

-sU: UDP ポートスキャンを指定します。

-p: スキャンするポートを指定し、デフォルトを上書きします。 個別のポート番号や、ハイフンで区切られた範囲のポート番号(たとえば、1-1023)も使用可能であることに注意してください。

ccm_ip_address: Cisco Unified Communications ManagerのIPアドレス

自動登録

システムは、混在モードとノンセキュアモードの両方で自動登録をサポートしています。既定の構成ファイルも署名されます。デフォルトでのセキュリティをサポートしないCisco IP 電話には、署名されていないデフォルトの構成ファイルが提供されます。

Cisco Unified Communications Manager および ITL ファイルを含むクラスタ間で IP 電話を移行する

Unified Communications Manager 8.0 (1) 以降では、新しいデフォルトによるセキュリティと初期信頼リスト (ITL) ファイルの使用が導入されています。 この新機能により、異なる Unified CM クラスタ間で電話を移動する場合は注意が必要です。また、適切な移行手順に従うようにしてください。

⚠

注意 適切な手順に従わなかった場合、何千という電話のITLファイルを手動で削除する必要があります。

新しい ITL ファイルをサポートする Cisco IP 電話は、 Unified CM TFTP サーバからこの特別なファイルをダウンロードする必要があります。 ITL ファイルが電話機にインストールされると、以降のすべての構成ファイルとITLファイルの更新は、次のいずれかによって署名されなければなりません。

- 現在電話機にインストールされている TFTP サーバ証明書、または
- クラスターの一つのTVSサービスで検証できるTFTP証明書。 ITLファイルにリストされているクラスタ内の TVS サービスの証明書を見つけることができます。

この新しいセキュリティ機能を考慮して、電話を1つのクラスタから別のクラスタに移動するときに、3 つの問題が発生する可能性があります。

1. 新しいクラスタの ITL ファイルは現在の ITL ファイルの署名者によって署名されていないため、電話は新しい ITL ファイルまたは設定ファイルを受け入れることができません。
2. 電話の既存の ITL にリストされている TVS サーバは、電話が新しいクラスタに移動されると到達できない場合があります。
3. 証明書の検証のために TVS サーバに到達できても、古いクラスタサーバは新しいサーバ証明書を持っていない場合があります。

これら 3 つの問題のうち 1 つ以上が発生した場合、クラスタ間で移動中のすべての電話機から ITL ファイルを手動で削除することが考えられます。 しかし、これは電話の数が増えるにつれて膨大な労力を必要とするため、望ましいソリューションとは言えません。

最も望ましいオプションは、Cisco Unified CM のエンタープライズパラメータ Prepare Cluster for Rollback to pre-8.0. を利用することです。 このパラメータが True に設定されると、電話は空の TVS および TFTP 証明書セクションを含む特別な ITL ファイルをダウンロードします。

電話に空の ITL ファイルがある場合、電話は署名されていない構成ファイルを受け入れ (Unified CM 8.x 以前のクラスタへの移行用)、新しい ITL ファイルを受け入れます (別の Unified CM 8.x クラスタへの移行用)。

空の ITL ファイルは、電話で [**設定** > **セキュリティ** > **信頼リスト** > **ITL**] をチェックすることで確認できます。 古い TVS および TFTP サーバがあった場所に空のエントリが表示されます。

電話は、新しい空の ITL ファイルをダウンロードするためだけに、古い Unified CM サーバにアクセスする必要があります。

古いクラスタをオンラインのままにしておく場合は、[Prepare Cluster for Rollback to pre-8.0 Enterprise パラメーター] を無効にして、デフォルトでのセキュリティを復元してください。

暗号化（Encryption）

ヒント 暗号化機能は、Unified Communications Manager をサーバーにインストールするときに自動的にインストールされます。

この項では、Unified Communications Manager がサポートする暗号化の種類について説明します。

エンドユーザのログイン資格情報を保護する

Unified Communications Manager リリース 12.5 (1) から、すべてのエンドユーザのログイン資格情報が SHA2 でハッシュされ、セキュリティが強化されます。 Unified Communications Manager リリース 12.5 (1) より前では、すべてのエンドユーザのログイン資格情報は SHA1 のみでハッシュされていました。 Unified Communications Manager リリース 12.5 (1) には、[「時代遅れの資格情報アルゴリズムを使用する」 UCM ユーザ] レポートも含まれています。 このレポート

は Cisco Unified Reporting ページから入手できます。 このレポートは、管理者がパスワードまたは PIN が SHA1 でハッシュされたすべてのエンドユーザを一覧表示するのに役立ちます。

SHA1 でハッシュされたすべてのエンドユーザのパスワードまたは PIN は、最初のログインに成功したときに自動的に SHA2 に移行されます。 SHA1 ハッシュされた (期限切れの) 資格情報を持つエンドユーザは、次のいずれかの方法を使用して PIN またはパスワードを更新できます。

- 電話でエクステンション モビリティまたはディレクトリ アクセスにログインして PIN を更新します。
- Cisco Jabber、Cisco Unified Communications セルフケアポータル、または Cisco Unified CM の管理にログインしてパスワードを更新します。

レポートの作成方法の詳細については、 *Cisco Unified CM*の管理オンラインヘルプを参照してください。

シグナリングの暗号化

シグナリングの暗号化により、端末との間で Unified Communications Manager サーバ間で送信されるすべての SIP および SCCP シグナリングメッセージが暗号化されます。

シグナリングの暗号化により、当事者、当事者が入力する DTMF 番号、コール ステータス、メディア暗号化キーなどに関連する情報が、意図しないまたは不正なアクセスから確実に保護されます。

混合モードでクラスタを構成する場合、Cisco は Unified Communications Manager でのネットワークアドレス変換 (NAT) をサポートしません。NAT はシグナリング暗号化では機能しません。

ファイアウォールでUDP ALGを有効にして、メディアストリームファイアウォールトラバーサルを許可することができます。 UDP ALG を有効にすると、ファイアウォールの信頼された側のメディアソースは、ファイアウォールを通してメディアパケットを送信することにより、ファイアウォールを通して双方向のメディアフローを開くことができます。

ヒント ハードウェア DSP リソースはこのタイプの接続を開始することができないため、ファイアウォールの外側に存在している必要があります。

シグナリング暗号化は NAT トラバーサルをサポートしていません。 NAT を使用する代わりに、LAN 拡張 VPN の使用を検討してください。

メディア暗号化

Secure Real-Time Protocol (SRTP) を使用するメディア暗号化により、意図した受信者だけが、サポートされているデバイス間のメディアストリームを解釈できるようになります。 メディア暗号化には、デバイスのメディア マスター キー ペアの作成、デバイスへのキーの配信、およびキーの転送中の配信のセキュリティ保護が含まれます。 Unified Communications Manager は、

主に IOS ゲートウェイと Unified Communications Manager のゲートキーパー制御および非ゲートキーパー制御の H.323 トランク、そして SIP トランクに対して SRTP をサポートしています。

（注） Cisco Unified Communications Manager は、異なるデバイスやプロトコルに対して、異なる方法でメディア暗号化キーを扱います。 SCCP を実行しているすべての電話は、 Unified Communications Manager からメディア暗号化キーを取得します。これにより、TLS 暗号化シグナリングチャネルを使用して、電話へのメディア暗号化キーのダウンロードが保護されます。 SIP を実行している電話は、独自のメディア暗号化キーを生成して保存します。 Unified Communications Manager システムにより生成されるメディア暗号化キーは、H.323 および MGCP の場合は IPSec 保護リンクを介して、また SCCP および SIP の場合は暗号化された TLS リンクを介してゲートウェイに安全に送信されます。

デバイスは、SRTP を使用できるかどうかをネゴシエーションで記述する必要があります。 デバイスが同じコール内の異なるデバイスとのキャッシュされた以前のネゴシエーション SDP を使用する場合、CUCM は SRTP をサポートしません。

デバイスが SRTP をサポートしている場合、システムは SRTP 接続を使用します。 1 つ以上のデバイスが SRTP をサポートしていない場合、システムは RTP 接続を使用します。 SRTP から RTP へのフォールバックは、セキュアなデバイスから非セキュアなデバイスへの転送、トランスコーディング、保留音などで発生する可能性があります。

ほとんどのセキュリティ対応デバイスでは、認証とシグナリングの暗号化がメディア暗号化の最小要件として機能します。つまり、デバイスがシグナリングの暗号化と認証をサポートしていない場合、メディアの暗号化は実行できません。 CiscoIOS ゲートウェイとトランクは、認証なしのメディア暗号化をサポートしています。 CiscoIOS ゲートウェイおよびトランクの場合、SRTP 機能 (メディア暗号化) を有効にする場合、IPSec を設定する必要があります。

警告 ゲートウェイとトランクに SRTP またはシグナリング暗号化を設定する前に、Cisco は強く IPSec を設定することをお勧めします。CiscoIOS MGCP ゲートウェイ、H.323 ゲートウェイ、H.323/H.245/H.225 トランクは IPSec 設定に依存しているため、セキュリティ-関連情報は平文では送信されません。 Unified Communications Manager は、IPSec が正しく設定されているかどうかの確認を行いません。 IPSec を適切に設定しないと、セキュリティ関連の情報が漏えいする可能性があります。

SIP トランクは TLS に依存して、セキュリティ関連情報が平文で送信されないようにします。

次の例では、SCCP および MGCP コールのメディア暗号化を示します。

1. メディアの暗号化と認証をサポートする端末 A と端末 B は、Unified Communications Manager に登録します。
2. デバイス A がデバイス B に発信するとき、 Unified Communications Manager はキーマネージャ関数に 2 セットのメディアセッションマスター値を要求します。

3. 両方のデバイスが 2 つのセットを受信します。1 つはメディア ストリーム用のデバイス A - デバイス B で、もう 1 つはメディア ストリーム用のセットである デバイス B - デバイス A です。
4. マスター値の最初のセットを使用して、デバイス A はメディア ストリーム、デバイス A - デバイス B を暗号化および認証するキーを取得します。
5. マスター値の 2 番目のセットを使用して、デバイス A はメディア ストリーム、デバイス B - デバイス A を認証して復号化するキーを取得します。
6. デバイス B は、逆の操作シーケンスでこれらのセットを使用します。
7. デバイスがキーを受信した後、デバイスは必要なキー導出を実行し、SRTP パケット処理が発生します。

（注） SIP および H.323 トランク/ゲートウェイを実行している電話は、独自の暗号化パラメータを生成し、それらを Unified Communications Manager に送信します。

電話会議でのメディア暗号化については、「電話会議リソースの安全性」に関連するトピックを参照してください。

セキュア ハッシュ アルゴリズム (SHA-2) に対する SCCP ゲートウェイおよびハードウェア会議ブリッジ サポート

セキュアな Skinny Client Control Protocol (SCCP) は、Transport Layer Security (TLS) および Secured Real-Time Transport Protocol (SRTP) を使用したシグナリングの整合性とメディア暗号化により、Foreign Exchange ステーション (FXS) アナログエンドポイントを強化します Unified Communications Manager。

Unified Communications Manager が、SCCP ゲートウェイ (アナログ エンドポイント) およびハードウェア コンファレンス ブリッジ (TLS および SRTP) の SHA-2 アルゴリズムのサポートを強化するようになりました。

前提条件

SCCP アナログ エンドポイントとハードウェア会議ブリッジの SHA-2 サポートは、次の Unified Communications Manager およびゲートウェイ バージョンで機能します。

- Unified CM バージョン 14 SU1 以降。
- ゲートウェイ IOS バージョン: IOS XE 17.6.1 であり、セキュアなシグナリングのために TLS V1.2 をサポートするように構成する必要があります。

（注）
- アナログ エンドポイントの場合、音声ゲートウェイで STCAPP を有効にし、Unified Communications Manager でセキュアな FXS ポートを登録するために、音声ゲートウェイで FXS ポートが使用可能であることを確認します。
- ハードウェア電話会議ブリッジの場合、電話会議用の安全な DSPFarm プロファイルが必要です。トランスコーディング セッション、MTP セッション、電話会議の同時進行の組み合わせをサポートするからです。

オーバーライド機能

Unified Communications Manager が、ゲートウェイに電話会議またはトランスコーディングサービスを要求します。ゲートウェイはリソースの空き状況に応じて、これらの要求を許可または拒否します。

Cisco Unified OS Administration ユーザーインターフェースの **[暗号管理（Cipher Management）]** ページで暗号を構成していない場合、デフォルト設定が **[エンタープライズパラメータ（Enterprise Parameters）]** > **[TLS 暗号（TLS Ciphers）]** として認識され、ネゴシエートされます。 SCCP FXS は、SCCP Cisco IP 電話との下位互換性を維持するために、SHA-1 TLS 暗号をデフォルトにします。

あなたが **すべてのサポートされている暗号** を選択した既定のオプションを **Cisco Unified CM 管理** > **システム** > **エンタープライズ パラメータ** > **TLS 暗号** フィールドで選択した場合、次の暗号が Unified CM によって認識され、TLS 接続に対して交渉されます: AEAD_AES_256_GCM, AEAD_AES_128_GCM, AES_CM_128_HMAC_SHA1_32, SHA1_80, F8_128_HMAC_SHA1_32, F8_SHA1_80。 しかし、 **Cisco Unified OS Administration** > **セキュリティ** > **暗号管理** が "AES256-GCM-SHA384:AES256- SHA256"を **すべての TLS** インターフェースに設定されている場合、すべての SIP インターフェースは「AES256-GCM-SHA384:AES256-SHA256」暗号のみをサポートし、エンタープライズパラメータ値は無視します。 詳細については、「暗号文字列の設定」および「暗号の制限」を参照してください。

次に例を示します。

1. **Cisco Unified OS Administration** > **暗号管理** は **デフォルト**、SHA-1 TLS はネゴシエートされます。
2. **Cisco Unified OS Administration** > **暗号管理** を **ALL**、SHA-2 TLS はネゴシエートされます。

安全な通話のアルゴリズム

Unified Communications Manager が強化され、追加アルゴリズムのネゴシエーションがセキュアなコールで可能になりました。 この機能強化の一環として、 Unified Communications Manager に SCCP バージョンが 23 に増加しました。

新しい SHA-2 暗号スイートのキーと Salt のサイズをサポートするために、新しい Open Receive Channel (ORC) および Start Media Transmission (SMT) バージョン 23 構造は、MAX_KEY_SIZE = 32 で実装されています。

（注） SHA-2 は SCCP 電話、H323、および MGCP ではサポートされていません。

***SCCP* 経由で登録されたアナログエンドポイントのメディアを保護するには:**

- Unified CM に登録された 2 つの安全な SCCP アナログ エンドポイント間のコールは、SHA-2 暗号 AEAD_AES_256_GCM または AEAD_AES_128_GCM のいずれかを使用してネゴシエートする必要があります。
- セキュアな SCCP アナログエンドポイントと、Unified CM に登録されている SHA-2 サポートを持つ SIP エンドポイント間の通話は、次の SHA-2 暗号 AEAD_AES_256_GCM または AEAD_AES_128_GCM のいずれかでネゴシエートされます。

電話会議がハードウェアの電話会議ブリッジで主催される場合にメディアを保護するには:

- SHA-2 をサポートする SCCP アナログ エンドポイントまたは SIP エンドポイントが SCCP ハードウェア会議ブリッジに接続されると、SHA-2 暗号がネゴシエートします: AEAD_AES_256_GCM または AEAD_AES_128_GCM。
- セキュアな電話会議中に、セキュアな SCCP 会議のエンドポイントで複数のメディア確立アルゴリズムが使用されている場合、会議ブリッジは、特定のコールレッグで対応するアルゴリズムをネゴシエートします。

TLS および SIP SRTP の AES 256 暗号化サポート

Cisco コラボレーション ソリューションは、シグナリングとメディア暗号化に Transport Layer Security (TLS) と Secure Real-time Transport Protocol (SRTP) を使用します。 現在、128 ビットの暗号化キーを持つ Advanced Encryption Standard（AES）が暗号化方式として使用されます。 AES はまた、認証方法としてハッシュベースのメッセージ認証コードセキュアハッシュアルゴリズム-1 (HMAC-SHA-1) も使用します。 これらのアルゴリズムは、必要とされる変化するセキュリティとパフォーマンスのニーズを満たすために効果的にスケールすることができません。 高まるセキュリティとパフォーマンスの要件を満たすために、Next-Generation Encryption (NGE) での暗号化、認証、デジタル署名、キー交換のアルゴリズムとプロトコルが開発されました。 また、NGE をサポートする TLS および Session Initiation Protocol (SIP) SRTP では、AES 128 の代わりに AES 256 暗号化サポートが提供されます。

TLS および SIP SRTP の AES 256 暗号化サポートが強化され、シグナリングとメディア暗号化の AES 256 暗号サポートに重視されています。 この機能は、Unified Communications Manager で実行されるアプリケーションが、SHA-2（セキュアハッシュアルゴリズム）標準に準拠し、連邦情報処理標準（FIPS）に準拠している AES-256 ベースの暗号を使用する TLS 1.2 接続をサポートするのに役立ちます。

この機能には次の要件があります。

- SIP トランクおよび SIP 回線が開始する接続。
- Unified Communications Manager が SIP 回線および SIP トランク経由の SRTP 通話に対してサポートする暗号。

（注） このリリースでは、TLS 1.2 は SIP などの一部のインターフェイスでサポートされていますが、すべてのインターフェイスではサポートされていません。 コラボレーションの展開では、TLS 1.0 および 1.1 を有効にしておくことをお勧めします。

TLS での AES 256 および SHA-2 のサポート

Transport Layer Security (TLS) プロトコルは、2 つのアプリケーション間の通信に認証、データ整合性、および機密性を提供します。 TLS 1.2 は Secure Sockets Layer (SSL) プロトコルバージョン 3.0 に基づいていますが、この 2 つのプロトコルには互換性がありません。 TLS は、一方がサーバとして機能し、もう一方がクライアントとして機能するクライアント/サーバモードで動作します。 SSL は、伝送制御プロトコル (TCP) レイヤーとアプリケーションの間のプロトコルレイヤーとして位置付けられ、クライアントとサーバ間の安全な接続を形成し、ネットワーク上で安全に通信できるようにします。 TLS が動作するためには、信頼できるトランスポート層プロトコルとして TCP が必要です。

Unified Communications Manager では、TLS 1.2 の AES 256 および SHA-2 (セキュア ハッシュ アルゴリズム-2) サポートは、SIP トランクと SIP 回線によって開始される接続を処理するための機能強化です。 サポートされている AES 256 および SHA-2 準拠の暗号は以下のとおりです。

- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 - 暗号文字列は ECDH-RSA-AES128-GCM-SHA256 です。
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 - 暗号文字列は ECDH-RSA-AES256-GCM-SHA384 です。

引数の説明

- Transport Layer Security（TLS）
- ECDH は楕円曲線 Diffie-Hellman アルゴリズムで、これはアルゴリズムです。
- RSA は Rivest Shamir Adleman と命名されたもので、これはアルゴリズムです。
- AES は高度暗号化標準です
- GCM はガロア/カウンター モードです

新しくサポートされた暗号に加えて、Unified Communications Manager は引き続き TLS_RSA_WITH_AES_128_CBC_SHA をサポートします。 この暗号の暗号文字列は AES128-SHA です。

（注）
- Unified Communications Manager 証明書は RSA に基づいています。
- Unified Communications Manager 10.5 (2) では、Cisco エンドポイント (電話) は上記の新しい暗号を TLS 1.2 でサポートしていません。
- Unified Communications Manager の TLS 1.2 強化での AES 256 および SHA-2 (セキュアハッシュアルゴリズム-2) サポートにより、認証局プロキシ 機能 (CAPF) のデフォルトのキーサイズが 2048 ビットに増加されました。

SRTP SIP コール シグナリングでの AES 256 サポート

Secure Real-time Transport Protocol (SRTP) は、Real-time Transport Protocol (RTP) の音声とビデオのメディア、および対応する Real-time Transport Control Protocol (RTCP) ストリームの両方に対して、機密性とデータの整合性を提供する方法を定義します。 SRTP は暗号化とメッセージ認証ヘッダーを使用してこの方法を実装します。 SRTP では、暗号化は RTP パケットのペイロードにのみ適用され、RTP ヘッダーには適用されません。 ただし、メッセージ認証は RTP ヘッダーと RTP ペイロードの両方に適用されます。 また、メッセージ認証はヘッダー内の RTP シーケンス番号に適用されるため、SRTP はリプレイ攻撃に対する保護を間接的に提供します。 SRTP は暗号化方式として 128 ビット暗号化キーを持つ Advanced Encryption Standards (AES) を使用します。 また、認証方法としてハッシュベースのメッセージ認証コードセキュアハッシュアルゴリズム-1 (HMAC-SHA-1) も使用します。

Unified Communications Manager は、SIP 回線および SIP トランクを介した SRTP 通話の暗号をサポートしています。 これらの暗号は AEAD_AES_256_GCM および AEAD_AES_128_GCM で、AEAD は Authenticated-Encryption with Associated-Data、GCM はガロア/カウンター モードです。 これらの暗号は GCM に基づいています。 これらの暗号がセッション記述プロトコル (SDP) に存在する場合、AES 128 および SHA-1 ベースの暗号と比較して、より高い優先順位で扱われます。 Cisco エンドポイント (電話) は、SRTP 用の Unified Communications Manager に追加するこれらの新しい暗号をサポートしていません。

新しくサポートされた暗号に加えて、Unified Communications Manager は引き続き次の暗号をサポートします。

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32
- F8_128_HMAC_SHA1_80

AES 256 暗号化は、次の通話でサポートされています。

- SIP 回線から SIP 回線へのコール シグナリング
- SIP 回線から SIP トランクへのシグナリング
- SIP トランクから SIP トランクへのシグナリング

Cisco Unified Communications Managerの要求

- SIP トランクおよび SIP 回線接続での TLS バージョン 1.2 のサポートが利用できます。
- TLS 1.2接続が確立されたとき、暗号サポート—TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (暗号文字列 ECDHE-RSA-AES256-GCM-SHA384) および TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (暗号文字列 ECDHE-RSA-AES128-GCM-SHA256) が利用できます。 これらの暗号は GCM に基づいており、SHA-2 カテゴリに準拠しています。
- Unified Communications Manager は TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 および TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 暗号を使用して TLS1.2 を開始します。 ピアが TLS1.2 をサポートしない場合、Unified Communications Manager は既存の AES128-SHA 暗号を使用する TLS 1.0 にフォールバックします。
- SIP 回線および SIP トランク上の SRTP 通話は、GCM ベースの AEAD_AES_256_GCM および AEAD_AES_128_GCM 暗号をサポートします。

連携動作と制限事項

- Unified Communications Manager の要件は、SIP 回線と SIP トランク、および基本的な SIP から SIP への通話のみに適用されます。
- SIP 以外のプロトコルに基づくデバイス タイプは、サポートされている暗号を使用した TLS バージョンの既存の動作を引き続きサポートします。 また、Skinny Call Control Protocol (SCCP) は、以前サポートされていた暗号の TLS 1.2 もサポートしています。
- SIP から SIP 以外への通話では、引き続き AES 128 および SHA-1 ベースの暗号が使用されます。

AES 80 ビット認証サポート

Unified Communications Manager は、保留音 (MOH)、音声自動応答 (IVR)、アナンシエータで暗号化暗号として使用される 128 ビットの暗号化キーと 80 ビットの認証タグを含む Advanced Encryption Standard (AES) をサポートします。 デフォルトでは、80 ビット認証タグをサポートする電話は、AES_CM_128_HMAC_SHA1_80暗号を使用して、MOH、IVR、アナンシエータを再生します。

電話が IP 音声メディアストリーミング（IPVMS）で安全に接続する場合、AES_CM_128_HMAC_SHA1_80 暗号が優先されます。 電話が 80 ビット認証をサポートしていない場合、AES_CM_128_HMAC_SHA1_32 暗号に戻ります。 電話が 80 ビットまたは 32 ビットの認証タグをサポートしていない場合、ネゴシエーションは Real-Time Transport Protocol (RTP) 経由で発生します。

（注） SCCP 電話は 32 ビット認証タグのみをサポートします。 そのため、電話と IPVMS 間のネゴシエーションは AES_CM_128_HMAC_SHA1_32 暗号でのみ発生します。

電話 A が AES_CM_128_HMAC_SHA1_80 をサポートし、電話 B が AES_CM_128_HMAC_SHA1_32 暗号をサポートし、ユーザー A（電話 A）がユーザー B（電話 B）にダイヤルし、コールがユーザー B によって保留にされると、電話 A は MOH に接続します。 電話 A は 80 ビット認証タグのみをサポートするため、電話 A と MOH の間のネゴシエーションは AES_CM_128_HMAC_SHA1_80 暗号を通じて発生します。

ユーザー B（電話 B）がユーザー A（電話 A）にダイヤルし、ユーザー A によりコールが保留状態になった場合、電話 B は 32 ビット認証タグのみをサポートするため、電話 B と MOH の間のネゴシエーションは AES_CM_128_HMAC_SHA1_32 暗号によって発生します。

電話が 80 ビット認証タグをサポートする場合、電話と IVR または Annunciator 間のネゴシエーションは AES_CM_128_HMAC_SHA1_80 を通じて発生します。

次の表は、電話機とその交渉暗号でサポートされている暗号を示しています。

表 *1*：電話機能と交渉暗号

電話機能	交渉暗号
AES_CM_128_HMAC_SHA1_32 および AES_CM_128_HMAC_SHA1_80	AES_CM_128_HMAC_SHA1_80
AES_CM_128_HMAC_SHA1_32	AES_CM_128_HMAC_SHA1_32
AES_CM_128_HMAC_SHA1_80	AES_CM_128_HMAC_SHA1_80
AES_CM_128_HMAC_SHA1_32 および AES_CM_128_HMAC_SHA1_80 以外	RTP に戻します。

メディア ストリーミング デバイスとの SRTP 暗号不一致

セキュアなコールが保留、IVR、または Annunciator アナウンスなどの機能を呼び出しており、リモートの発信者が打診転送を実行すると、新しいコール レッグは MOH、IVR、または Annunciator のそれとは異なる暗号機能をサポートする場合があります。 これにより暗号のミスマッチが発生し、エンドポイントの SRTP フォールバックオプションに応じて、コールは非セキュアモードにドロップされるか、または完全にドロップされます。 **Block Unencrypted Calls** サービスパラメータが **True** に設定されている場合でも、セキュアな通話がドロップされます。 **Unified Communications Manager** > **システム** > **サービスパラメータ** > **サービスパラメータ設定** ウィンドウで

Unified Communications Manager プラットフォームの新しい機能強化では、Cisco IP Voice Media Streaming (IPVMS) デバイス (MOH、IVR、Annunciator) の後の通話機能を交換するときに、すべての暗号暗号をサポートします。 SRTP フォールバックの設定がアクティブ コールに影響を与えたり、セキュリティが損なわれたりすることはありません。

（注） メディア デバイスは、SHA1_32 および SHA1_80 ビット暗号化のみをサポートします。

自己暗号化ドライブ

Unified Communications Manager は、自己暗号化ドライブ（SED）をサポートしています。これは、フル ディスク暗号化（FDE）とも呼ばれます。FDE は、ハードドライブで使用可能なすべてのデータを暗号化するために使用される暗号化方式です。このデータには、ファイル、オペレーティングシステム、およびソフトウェアプログラムが含まれます。ディスク上の使用可能なハードウェアは、すべての受信データを暗号化し、すべての送信データの暗号化を解除します。

ドライブがロックされると、暗号化キーが内部で作成され保存されます。このドライブに保存されているすべてのデータは、そのキーを使用して暗号化され、暗号化された形式で保存されます。FDE は、キー ID とセキュリティ キーで構成されます。

詳細については、『Cisco UCS C シリーズサーバー Integrated Management Controller GUI コンフィギュレーション ガイド』を参照してください。

構成ファイルの暗号化

Unified Communications Manager は、ダイジェスト資格情報や管理者パスワードなどの機密データを、TFTPサーバからダウンロードされた構成ファイルの電話機にプッシュします。

Unified Communications Manager は、データベース内でこれらの資格情報を保護するために、可逆的な暗号化を使用しています。 ダウンロード プロセス中にこのデータを保護するために、Cisco では、このオプションをサポートするすべての Cisco IP 電話に対して、暗号化構成ファイルを構成することを推奨しています。 このオプションが有効な場合、デバイス構成ファイルのみがダウンロード用に暗号化されます。

（注） 状況によっては、機密データを暗号化されていない状態で電話にダウンロードすることを選択することもできます。たとえば、電話のトラブルシューティング時。

Unified Communications Manager は暗号化キーをエンコードし、データベースに保存します。TFTP サーバは、対称暗号化キーを使用して、構成ファイルを暗号化し、解読します。

- 電話に PKI 機能がある場合、 Unified Communications Manager は電話の公開鍵を使用して、電話構成ファイルを暗号化できます。
- 電話が PKI 機能を持たない場合、 Unified Communications Manager と電話で一意の対称キーを設定する必要があります。

Unified Communications Manager Administrationの[電話セキュリティプロファイル]ウィンドウで暗号化設定ファイルを有効にします。その後、[電話の設定]ウィンドウで設定した設定を電話に適用します。

デフォルトのセキュリティ管理タスク

以下はデフォルトのセキュリティ管理タスクです。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Unified IP Phones の ITL ファイルの更新	TFTP 構成ファイルを検証します。
ステップ 2	ITL ファイル ステータスの取得	電話の ITL ファイル ステータスを取得します。
ステップ 3	Cisco Unified IP Phone サポートリストの取得	Cisco Unified IP Phone サポートリスト ページを Cisco Unified レポートを使用して取得します。
ステップ 4	クラスタを 8.0 より前のリリースにロールバックする	クラスターのロールバックを準備します。
ステップ 5	ITL ファイルの一括リセットの実行 （27 ページ）	ITL ファイルの一括リセットを実行します。
ステップ 6	CTL ローカルキーのリセット	CLI コマンドで Cisco Trust List (CTL) ファイルのリセットを実行します
ステップ 7	ITLRecovery 証明書の有効期間を表示する	ITLRecovery 証明書の有効期間を表示します。
ステップ 8	認証と暗号化のセットアップ	新規インストールに認証と暗号化を実装する。

Cisco Unified IP Phones の ITL ファイルの更新

電話に ITL ファイルがインストールされた状態で [デフォルトのセキュリティ] を使用する Unified Communication Manager による一元化された TFTP は TFTP 構成ファイルを検証しません。

リモート クラスタからの電話が集中型 TFTP 展開に追加される前に、次の手順を実行します。

ステップ 1 中央の TFTP サーバーで、エンタープライズパラメータ **Preparecluster for pre CM-8.0 ロールバック**を有効にします。

ステップ 2 TVS および TFTP を再起動します。

ステップ 3 すべての電話をリセットして、ITL 署名検証を無効にする新しい ITL ファイルがダウンロードされたことを確認します。

ステップ 4 HTTPS の代わりに HTTP を使用するようにエンタープライズ パラメータ セキュア https URL を設定します。

（注） Unified Communications Manager リリース 10.5 以降では、[**CM-8.0 以前のロールバック用にクラスタを用意する**] パラメータを有効にすると、電話が自動的にリセットされます。 中央 TFTP サーバの Unified Communications Manager バージョンおよびこのパラメータを有効にする方法については、Cisco Unified Communications Manager セキュリティガイドの「8.0 以前のリリースへのクラスタのロールバック」を参照してください。

ITL ファイル ステータスの取得

電話の ITL ファイル ステータスを取得するには、次の手順を使用します。

ステップ 1 Cisco Unified Communications Manager Administration から、**[デバイス（Device）]** > **[電話機（Phone）]** を選択します。

ステップ 2 **Find Phone where** のドロップダウンリストから ITL ファイル状況 **を選択し** 、条件を選択します。

（注） 次の表は Release 15 までのみ適用されます。

フィールド	説明
一致	サーバと電話の ITL ハッシュは同じです。
ミスマッチ	サーバの ITL ハッシュと電話のものが一致しません。
未インストール	電話は新しい CUCM サーバへの登録に失敗し、以前のサーバにバウンスバックされます。
不明	電話またはサーバの ITL ハッシュが不明です。

（注） 次の表は、リリース 15SU1 以降に適用されます。

フィールド	説明
一致	任意の TFTP サーバおよび電話の ITL ハッシュが同じです。
ミスマッチ	サーバと電話のITLハッシュが一致しない、または電話またはサーバのITLハッシュが不明です。
未インストール	電話は新しい CUCM サーバへの登録に失敗し、以前のサーバにバウンスバックされます。

ステップ 3 **[検索（Find）]** をクリックします。

Cisco Unified IP Phone サポートリストの取得

Cisco Unified Reporting ツールを使用して、デフォルトでセキュリティをサポートする Cisco エンドポイントのリストを生成します。

ステップ 1 Cisco Unified Reporting から、 **システムレポートを選択します。**

ステップ 2 **[システムレポート]** リストから、 **Unified CM 電話機能リストを選択します。**

ステップ 3 **[製品]** ドロップダウンリストから、 **デフォルトのセキュリティ** を選択します。

ステップ 4 [送信（Submit）]をクリックします。
特定の電話でサポートされている機能のリストを含むレポートが生成されます。

クラスタを 8.0 より前のリリースにロールバックする

Unified Communications Managerの 8.0 より前のリリースにクラスターをロールバックする前に、pre-8.0へのロールバックのためのクラスターの準備エンタープライズパラメータを使用して、ロールバックするクラスターを準備する必要があります。

クラスターのロールバックを準備するには、クラスター内の各サーバでこの手順に従います。

ステップ 1 Unified Communications Managerから **[システム]** > **[エンタープライズパラメータ設定]**を選択します。

エンタープライズパラメータ設定 ウィンドウが表示されます。

Prepare Cluster for Rollback to pre-8.0 えんたーぷらいず パラメータを **True** に設定します。

（注） クラスタを Unified Communications Manager の pre-8.0 リリースにロールバックする準備をしている場合にのみ、このパラメータを有効にしてください。 このパラメータが有効になっている間、https を使用する電話サービス (エクステンション モビリティなど) は機能しません。 ただし、このパラメータが有効になっている間も、ユーザは基本的な通話を発信および受信し続けることができます。

ステップ 2 Cisco IP Phonesが自動的に再起動し、Unified Communications Manager に登録するまで 10 分間待ちます。

ステップ 3 クラスター内の各サーバを前のリリースに戻します。

クラスタを以前のバージョンに戻す方法の詳細については、 *Cisco Unified Communications Manager* 管理ガイドを参照してください 。

ステップ 4 クラスターが前のバージョンへの切り替えを完了するまで待ちます。

ステップ 5 以下のいずれかのリリースを混合モードで実行している場合、CTL クライアントを実行する必要があります。

- Unified Communications Manager720 リリース
  - 7.1(2)のすべての通常リリース
  - 712のすべてのESリリースは007.001(002.32016.001)より前です

- Unified Communications Manager リリース 7.1 (3)
  - 713のすべての通常リリースは007.001(003.21900.003) = 7.1(3a)su1aより前です
  - 712のすべてのESリリースは007.001(003.21005.001)より前です

（注） CTL クライアントの実行についての詳細は、「「CTL クライアントの設定」」の章を参照してください。

ステップ 6 [「8.0より前にロールバックするためのクラスターの準備]が[エンタープライズパラメータ]でTrueに設定されている場合、企業ディレクトリを機能させるには、次の変更を行う必要があります。」

[**デバイス] >デバイス設定 >電話サービス >企業ディレクトリ** では、サービスの URL を Application:Cisco/CorporateDirectory から http://<ipaddr>:8080/ccmcip/xmldirectoryinput.jsp に変更する必要があります。

ステップ 7 [「8.0より前にロールバックするためのクラスターの準備]が[エンタープライズパラメータ]でTrueに設定されている場合、企業ディレクトリを機能させるには、次の変更を行う必要があります。」

端末 >デバイスの設定 >電話サービス >パーソナルディレクトリ サービスの URL を、Application:Cisco/PersonalDirectory から、'http://<ipaddr>>:8080/ccmpd/pdCheckLogin.do?name=未定義に変更する必要があります。

元に戻した後にリリース 8.6 以降に切り替える

クラスタをリリース 7.x に戻した後で、リリース 8.6 以降のパーティションに戻す場合は、この手順に従ってください。

ステップ 1 クラスターを非アクティブパーティションに戻すための手順に従います。 詳細については、『*Cisco Unified Communications Manager* 管理ガイド』を参照してください 。

ステップ 2 以下のリリースのいずれかを混合モードで実行していた場合、CTL クライアントを実行する必要があります。

Cisco Unified Communications Manager リリース 7.1 (2)

- 7.1(2)のすべての通常リリース
- 712のすべてのESリリースは007.001(002.32016.001)より前です
- Unified Communications Manager リリース 7.1 (3)
  - 713のすべての通常リリースは007.001(003.21900.003) = 7.1(3a)su1aより前です
  - 712のすべてのESリリースは007.001(003.21005.001)より前です

（注） CTL クライアントの実行についての詳細は、「「CTL クライアントの設定」」の章を参照してください。

ステップ 3 Cisco 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設定 ウィンドウが表示されます。

Prepare Cluster for Rollback to pre-8.6 えんたーぷらいず パラメータを **True** に設定します。

ステップ 4 Cisco Unified IP Phone が自動的に再起動し、 Unified Communications Manager に登録するまで 10 分ほど待ちます。

ITL ファイルの一括リセットの実行

この手順は必ず Unified Communications Manager パブリッシャから実行してください。

ITL ファイルの一括リセットは、電話が ITL ファイルの署名者を信頼しなくなり、ローカルの TFTP サービスまたは TVS を使用して提供される ITL ファイルを認証できない場合に実行されます。

一括リセットを実行するには、CLI コマンド **utils itl reset** を使用します。 このコマンドは新しい ITL 回復ファイルを生成し、電話と CUCM 上の TFTP サービスの間の信頼を再確立します。

ヒント Unified Communications Manager をインストールする場合、CLI コマンド **file get tftp***ITLRecovery.p12*を使用して ITL 復旧ペアをエクスポートし、DRを通じてバックアップを実行します。SFTP サーバー（キーがエクスポートされる場所）とパスワードの入力も求められます。

ステップ 1 次のいずれかの手順を実行します。

- **utils itl reset localkey** を実行します。
- **utils itl reset remotekey** を実行します。

（注） **utils itl reset localkey** の場合、ローカルキーはパブリッシャーに存在します。 このコマンドを発行すると、ITL ファイルは ITL 回復キーがリセットされる間、CallManager キーによって一時的に署名されます。

ステップ 2 **show itl** を実行してリセットが成功したことを確認します。

ステップ 3 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 4 **[リセット（Reset）]** をクリックします。

デバイスが再起動します。 これで、CallManager キーで署名された ITL ファイルをダウンロードし、構成ファイルを受け入れる準備ができました。

ステップ 5 TFTP サービスを再起動し、すべてのデバイスを再起動します。

（注） TFTP サービスを再起動すると、ITL ファイルが ITLRecovery キーで署名され、ステップ 1 の変更がロールバックされます。

デバイスは、ITLRecovery キーで署名された ITL ファイルをダウンロードし、Unified Communications Manager に再度正しく登録します。

CTL ローカルキーのリセット

Unified Communications Manager クラスタ上のデバイスがロックされ、信頼できるステータスを失った場合、CLI コマンド **utils ctl reset localkey を使用して Cisco Trust List (CTL) ファイルのリセットを実行します。** このコマンドにより新しい CTL ファイルが生成されます。

ステップ 1 **utils ctl reset localkey** を実行します。

（注） **utils ctl reset localkey** の場合、ローカルキーはパブリッシャーに存在します。 このコマンドを発行するとき、CTL ファイルは一時的に CallManager キーによって署名されます。

ステップ 2 **show ctl** を実行してリセットが成功したことを確認してください。

ステップ 3 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。
[**エンタープライズパラメータの設定**] ページが表示されます。

ステップ 4 [**リセット**（**Reset**）] をクリックします。

デバイスが再起動します。 これで、CallManager キーで署名された CTL ファイルをダウンロードし、構成ファイルを受け入れる準備が整いました。

ステップ 5 **utils ctl update CTLFile** を実行し、必要なサービスを再起動してステップ 1 の変更をロールバックします。

デバイスが再起動します。 これで、CallManager キーで署名された CTL ファイルをダウンロードし、構成ファイルを受け入れる準備が整いました。

デバイスは、必要なキーを使用して署名された CTL ファイルをダウンロードし、再度 Unified Communications Manager に登録します。

ITLRecovery 証明書の有効期間を表示する

ITLRecovery 証明書は、電話に対して長い有効期間を持っています。 [**証明書ファイルのデータ**] ペインに移動すると、有効期間やその他の ITLRecovery 証明書の詳細を表示できます。

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 検索パラメータを入力して、証明書を検索して設定の詳細を表示します。

基準に一致する証明書の一覧が **証明書リスト** ページに表示されます。

ステップ 3 有効期間を表示するには、 **ITLRecovery** リンクをクリックしてください。

ITLRecovery 証明書の詳細は **証明書ファイルのデータ** ペインに表示されます。

有効期間は現在の年から20年間です。

認証と暗号化のセットアップ

重要 **utils ctl** CLI コマンドセットを使用して暗号化をセットアップできます。 CLI の使用の詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

以下の手順は、認証と暗号化を実装するために実行する必要があるすべてのタスクを示しています。 指定されたセキュリティ機能のために実行する必要がある作業が記載されている章の参照については、関連トピックを参照してください。

- 新規インストールに認証と暗号化を実装するには、次の表を参照してください。
- セキュアなクラスタにノードを追加するには、「インストール *Cisco Unified Communications Manager*」を参照してください。新しいノードの追加方法と新しいノードのセキュリティ設定方法について説明しています。

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。