証明書

証明書の管理

証明書管理機能は、さまざまな証明書タイプ、証明書の管理に関連するタスク、および証明書をモニタおよび失効させる方法の概要を提供します。

証明書概要

証明書は、導入でセキュアな接続を確立するために不可欠です。ネットワーク上で個人、コンピュータ、および他のサービスを認証します。適切な証明書管理を実施することで、適切なレベルの保護を実現し、かつ複雑さを軽減できます。

証明書は、証明書所有者のアイデンティティを証明するファイルであり、次の情報が含まれます。

- 証明書所有者の名前
- 公開キー
- 証明書を発行する認証局のデジタル署名

Unified Communications Managerは、暗号化を有効にし、サーバとクライアントのアイデンティティを検証するために、Public Key Infrastructure（PKI）を使用する証明書を使用します。適切な信頼ストアに一致する証明書がある場合を除き、他のシステムは信頼されず、アクセスが拒否されます。

ルート証明書は、デバイスやアプリケーションユーザなど、ユーザとホスト間のセキュアな接続を確保します。証明書は、クライアントとサーバのアイデンティティの安全性を確保し、これらをルート信頼ストアに追加します。

管理者は、サーバ証明書のフィンガープリントを表示し、自己署名証明書を再生成して、Unified Communications Manager インターフェイスから信頼証明書を削除できます。また、CLI を使用して自己署名証明書を再生成して表示することもできます。

Unified Communications Manager 信頼ストアを更新して証明書を管理する方法 の詳細については、Cisco Unified Communications Manager アドミニストレーション ガイドを参照してください。

Note Unified Communications Manager は、PEM（.pem）形式および DER（.der）形式の証明書のみサポートします。DER あるいは PEM の証明書のサポートされる最大サイズは 4096 ビットです。

2 つの証明書をアップロードする場合は、これらの名前と有効期間は同じであるが、シリアル番号と署名アルゴリズムが異なっていることを確認してください。

例：

`27:20:41:0c:5b:08:69:80:42:62:4f:13:bd:16:06:6a` シリアル番号と SHA-1 アルゴリズムを持つルート CA が Unified Communications Manager tomcat-trust に存在します。

`7b:35:33:71:0b:7c:08:b2:47:b3:aa:f9:5c:0d:ca:e4` シリアル番号と SHA-256 アルゴリズムの証明書をアップロードしようとすると、証明書管理は次の処理を実行します。

- 着信証明書の有効性を確認します。
- tomcatTomcat 信頼フォルダ内にある同じ名前の証明書を検索します
- Tomcat 信頼フォルダにある既存の証明書のシリアル番号と、アップロードされている着信証明書のシリアル番号を比較します。

それらのシリアル番号が異なる場合は、両方の証明書の有効期限開始日を確認します。新しい着信証明書の開始タイムスタンプが最新の場合は、既存の証明書は置き換えられ、そうでない場合はアップロードされません。

SHA-1 と SHA-256 のアルゴリズムでは、件名または共通名が同じであれば、同じエンティティに属していることを意味しています。この Unified Communications Manager フレームワークは、Unified Communications Manager サーバ上でこれら両方のアルゴリズムを同時にサポートしません。特定の信頼フォルダ内では、署名アルゴリズムが何であれ、いずれかのエンティティに属する 1 つの証明書のみがサポートされます。

証明書タイプ

このセクションでは、さまざまな種類の証明書と証明書署名要求、キーの用途拡張の概要を説明します。

電話機の証明書タイプ

電話機証明書は、電話機を認証するための一意の識別子です。これは、IP 攻撃に対するセキュリティにとって重要です。

電話機の証明書は次のとおりです。

Table 1:

電話機の証明書	説明
製造元でインストールされる証明書（MIC）	MIC は Cisco Manufacturing CA によって署名され、署名された証明書はサポートされている Cisco Unified IP Phone に自動的にインストールされます。 MIC は、ローカルで有効な証明書（LSC）のインストールまたは暗号化された設定ファイルのダウンロードに対して、シスコ認証局プロキシ機能（CAPF）で認証します。管理者は証明書を変更、削除、または無効にできないため、有効期限が切れた後は使用できません。
ローカルで有効な証明書（LSC）	Cisco Unified IP Phone は、セキュアモードで動作するために LSC を必要とし、認証と暗号化に使用されます。これらは CAPF、オンラインまたはオフライン CA により署名され、MIC よりも優先されます。 CAPF に関連付けられている必要なタスクを実行すると、サポートされている電話機にこの証明書がインストールされます。認証または暗号化を使用するようにデバイス セキュリティ モードを設定した後に、LSC により、Unified Communications Manager と電話機間の接続のセキュリティが確保されます。

Tip MIC は LSC のインストール時にのみ使用することを推奨します。シスコでは、Unified Communications Manager との TLS 接続の認証用に LSC をサポートしています。電話の設定で TLS 認証などの目的で MIC を使用した場合、MIC ルート証明書は容易に侵害されるため、当社は何ら責任を負いません

Unified Communications Manager への TLS 接続に LSC を使用するには、Cisco Unified IP Phone 6900、7900、8900、および 9900 シリーズをアップグレードします。今後の互換性の問題を回避するために、Unified Communications Manager 信頼ストアから MIC ルート証明書を削除します。

Note Unified Communications Manager への TLS 接続に MIC を使用する一部の電話機モデルは、登録できない場合があります。

管理者は Unified Communications Manager 信頼ストアから次の MIC ルート証明書を削除する必要があります。

- CAP-RTP-001
- CAP-RTP-002
- Cisco_Manufacturing_CA
- Cisco_Root_CA_2048
- Cisco_Manufacturing_CA_SHA2

- Cisco_Root_CA_M2
- ACT2_SUDI_CA

CAPF 信頼ストアに残された MIC ルート証明書は、証明書のアップグレードに使用されます。Unified Communications Manager 信頼ストアの更新と証明書の管理については、Cisco Unified Communications Manager アドミニストレーション ガイドを参照してください。

Note Unified Communications Manager リリース 12.5.1SU2 以前では、Cisco Manufacturing 証明書を CallManger 信頼ストアから削除すると、電話機の製造元でインストールされた証明書（MIC）を検証できないため、セキュアオンボーディング機能は動作しません。ただし、Unified Communications Manager リリース 12.5.1SU3 以降では、CAPF 信頼ストアを使用して電話機の MIC を検証するため、この機能は動作します。

サーバ証明書のタイプ

サーバ証明書は、基本的にサーバを識別するための証明書です。サーバ証明書は、コンテンツを暗号化および復号化する論拠の役目を果たします。

Unified Communications Manager サーバ内の自己署名証明書（所有）証明書タイプは次のとおりです。

Unified Communications Manager は次の証明書タイプを Unified Communications Manager 信頼ストアにインポートします。

Table 2: 証明書タイプと説明

証明書タイプ	説明
Cisco Unity サーバまたは Cisco Unity Connection 証明書	Cisco Unity と Cisco Unity Connection は、この自己署名ルート証明書を使用して、Cisco Unity SCCP および Cisco Unity Connection SCCP デバイス証明書に署名します。Cisco unityの場合、 Cisco Unity TELEPHONY Integration Manager (UTIM) はこの証明書を管理します。Cisco Unity Connection の場合は、Cisco Unity Connection の管理機能がこの証明書を管理します。
Cisco Unity および Cisco Unity Connection SCCP デバイス証明書	Cisco Unity および Cisco Unity Connection SCCP デバイスはこの署名証明書を使用して、Unified Communications Manager との TLS 接続を確立します。
SIP プロキシサーバ証明書	CallManager 信頼ストアに SIP ユーザエージェント証明書が含まれ、SIP ユーザエージェントの信頼ストアに Unified Communications Manager 証明書が含まれている場合、SIP トランク経由で接続する SIP ユーザエージェントは、Unified Communications Manager に対して認証されます。

Note 証明書名は、ボイスメールサーバ名に基づく証明書のサブジェクト名のハッシュを表します。すべてのデバイス (またはポート) は、ルート証明書をルートとする証明書を発行します。

次の追加の信頼ストアが存在します。

- tomcat および web アプリケーションの共通信頼ストア
- IPSec-trust
- CAPF-trust
- Userlicensing-trust
- TVS-trust
- Phone-SAST-trust
- Phone-CTL-trust

Cisco Unity Connection の CA 信頼証明書の詳細については、Cisco Unified Communications Manager アドミニストレーション ガイドを参照してください。これらの信頼証明書は、電子メール、予定表情報、連絡先を取得するための Exchange または Meeting Place Express へのセキュアな接続を確保します。

サードパーティー CA 署名付き証明書

CA で署名された証明書は、デジタル証明書に署名および発行する信頼できるサードパーティ証明書です。

デフォルトでは、Unified Communications Manager はすべての接続に自己署名証明書を使用します。ただし、証明書に署名するようにサードパーティ CA を設定することによって、セキュリティを追加できます。サードパーティ CA を使用するには、CA ルート証明書チェーンを Cisco Unified Communications Manager Administration にインストールします。

CA で署名された証明書を発行するには、CA が証明書を発行して署名できるように証明書署名要求（CSR）を提出する必要があります。証明書をアップロード、ダウンロード、および表示する方法の詳細については、「**自己署名証明書**」セクションを参照してください。

Configuration

Unified Communications Manager に接続している別のシステムからの CA で署名された証明書を使用する場合は、 Cisco Unified Communications Manager Administration で次の手順を実行します。

- 証明書を署名した CA のルート証明書をアップロードします。
- 他のシステムから CA 署名付き証明書をアップロードします。

CA で署名された証明書を Unified Communications Manager で使用する場合は、次の手順に従います。

- Cisco Unified Communications Manager Administration で CA で署名された証明書を要求するには、CSR を完了します。
- CA ルート証明書チェーンと CA で署名された証明書の両方を次のページでダウンロードします。 Cisco Unified Communications Manager Administration
- CA ルート証明書チェーンと CA で署名された証明書の両方をアップロードします。

CA のルート証明書の取得と設定の方法の詳細については、証明機関のマニュアルを参照してください。

外部 CA からの証明書のサポート

Unified Communications Manager は、PKCS#10 Certificate Signing Request（CSR; 証明書署名要求）メカニズムを使用して、サードパーティの認証局（CA）との統合をサポートします。このメカニズムには、Unified Communications Manager の GUI でアクセスできます。

現在、サードパーティ CA を使用しているお客様は、CSR メカニズムを使用して次の証明書を発行する必要があります。

- Unified Communications Manager
- CAPF
- IPSec
- Tomcat
- 信頼検証サービス（TVS）

Note マルチサーバ（SAN）の CA 署名付き証明書は、証明書が発行元にアップロードされた場合にのみクラスタ内のノードに適用されます。新しいマルチサーバ証明書を生成します。新しいノードを追加したり、再作成するたびにクラスタにアップロードします。

システムを混合モードで実行すると、一部のエンドポイントでは、キーサイズが4096以上の CA 証明書を受け入れることができない場合があります。混合モードで CA 証明書を使用するには、次のいずれかのオプションを選択します。

- 証明書のキーサイズが 4096 未満の証明書を使用します。
- 自己署名証明書を使用します。

Note このリリースの Unified Communications Manager は SCEP インターフェイスをサポートしません。

Note サードパーティの CA 署名付き証明書をプラットフォームにアップロードした後、CTL クライアントを実行して CTL ファイルを更新する必要があります。

CTL クライアントを実行した後、該当するサービスを再起動して更新します。

次に例を示します。

- Unified Communications Manager 証明書を更新する際 に、TFTP サービスと Unified Communications Manager サービスを再起動します。
- CAPF 証明書を更新するときに CAPF を再起動します。

Unified Communications Manager または CAPF 証明書をアップロードした後に、ITL ファイルを更新するために自動的に電話がリセットされる場合があります。

プラットフォームでの証明書署名要求（CSRs）の生成方法については、Cisco Unified Communications Manager アドミニストレーション ガイドを参照してください。

証明書署名要求のキー用途拡張

次の表には、Unified Communications Manager と IM and Presence Service の CA 証明書の証明書署名要求（CSR）のキーの用途拡張が表示されています。

***Table 3: Cisco Unified Communications Manager CSR* キーの用途拡張**

	マルチサーバ	キーの拡張用途			キーの用途				
		サーバ認証 (1.3.6.1.5.5.7.3.1)	クライアント認証 (1.3.6.1.5.5.7.3.2)	IP セキュリティ末端システム (1.3.6.1.5.5.7.3.5)	デジタル署名	鍵の暗号化	データの暗号化	キー証明書署名	鍵共有
CallManager CallManager-ECDSA	Y	Y	Y		Y	Y	Y		
CAPF（パブリッシャのみ）	N	Y			Y	Y		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		
信頼検証サービス（TVS）	Y	Y	Y		Y	Y	Y		

***Table 4: IM and Presence Service CSR* キーの用途拡張**

	マルチサーバ	キーの拡張用途			キーの用途				
		サーバ認証 **(1.3.6.1.5.5.7.3.1)**	クライアント認証 **(1.3.6.1.5.5.7.3.2)**	**IP** セキュリティ末端システム **(1.3.6.1.5.5.7.3.5)**	デジタル署名	鍵の暗号化	データの暗号化	キー証明書署名	鍵共有
cup cup-ECDSA	N	Y	Y	Y	Y	Y	Y		Y
cup-xmpp cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		Y
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		Y
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		

証明書タスク

このセクションでは、証明書を管理するすべての手順を示します。

証明書の表示

[証明書の表示（Show Certificates）] を使用して、システムに属する証明書および信頼ストアの詳細を表示します。共通名、タイプ、キー タイプ、流通、発行者、有効期限日、および証明書の説明を表示できます。

Procedure

Step 1 [Cisco Unified OSの管理（Cisco Unified OS Administration）] から、以下を選択します。 **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]**。

Step 2 [検索（Find）] をクリックします。

Step 3 証明書または信頼ストアの詳細を表示するには、証明書の共通名をクリックします。

Step 4 [閉じる（Close）] をクリックしてポップアップウィンドウを閉じ、[証明書リスト（Certificate List）] ページに戻ります。

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。

Procedure

Step 1 [Cisco Unified OSの管理（Cisco Unified OS Administration）] から、以下を選択します。 **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]**。

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。

中間証明書のインストール

中間証明書をインストールするには、まずルート証明書をインストールして、署名付き証明書をアップロードする必要があります。この手順は、認証局から 1 つの署名付き証明書と複数の証明書が証明書チェーンで提供している場合にのみ必要です。

Procedure

Step 1 Cisco Unified OS の管理で、次をクリックします。 **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]**。

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 ルート証明書をインストールするには、**[証明書の目的（Certificate Purpose）]** ドロップダウンリストから適切な信頼ストアを選択します。

Step 4 選択した証明書の目的の説明を入力します。

Step 5 次のいずれかの手順を実行して、アップロードするファイルを選択します。

- [ファイルのアップロード（Upload File）] テキスト ボックスに、ファイルへのパスを入力します。
- [参照（Browse）] をクリックしてファイルに移動し、[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 顧客証明書をインストールしたら、FQDN を使用して Cisco Unified Intelligence Center の URL にアクセスします。IP アドレスを使用して Cisco Unified Intelligence Center にアクセスすると、カスタム証明書を正常にインストールした後でも“「ここをクリックしてログインを継続します（Click here to continue）」”のメッセージが表示されます。

Note Tomcat 証明書をアップロードするときは、TFTP サービスを無効にし、その後有効にします。それ以外の場合は、TFTP は古いキャッシュの自己署名された tomcat 証明書を提供し続けます。

信頼証明書の削除

削除できる証明書は、信頼できる証明書だけです。システムで生成される自己署名証明書は削除できません。

Caution 証明書を削除すると、システムの動作に影響する場合があります。また、証明書が既存のチェーンの一部である場合、証明書チェーンが壊れることがあります。この関係は、[**証明書の一覧（Certificate List**）] ウィンドウ内の関連する証明書のユーザ名とサブジェクト名から確認します。この操作は取り消すことができません。

Procedure

Step 1 [Cisco Unified OSの管理（Cisco Unified OS Administration）] から、以下を選択します。 **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]**。

Step 2 証明書の一覧をフィルタするには、[**検索（Find**）] コントロールを使用します。

Step 3 証明書のファイル名を選択します。

Step 4 [削除（Delete）] をクリックします。

Step 5 [OK] をクリックします。

Note
- 削除する証明書が“ CAPF-trust”、“tomcat-trust”、“CallManager-trust”、または “Phone-SAST-trust” 証明書タイプの場合、証明書はクラスタ内のすべてのサーバで削除されます。
- 証明書を CAPF-trust にインポートする場合、それはその特定のノードでのみ有効になり、クラスタ全体で複製されることはありません。

証明書の再作成

証明書が期限切れになる前に、証明書を再生成することを推奨します。RTMT（Syslog Viewer）で警告が発行され、証明書の期限が近くなると電子メールで通知が送信されます。

ただし、期限切れの証明書を再生成することもできます。電話機を再起動してサービスを再起動する必要があるため、営業時間後にこのタスクを実行します。Cisco Unified OS の管理に「cert」タイプとしてリストされている証明書のみ再作成できます。

Caution 証明書を再作成すると、システムの動作に影響する場合があります。証明書を再作成すると、サードパーティの署名付き証明書（アップロードされている場合）を含む既存の証明書が上書きされます。

Procedure

Step 1 [Cisco Unified OSの管理（Cisco Unified OS Administration）] から、以下を選択します。 **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]**。

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。すべての条件に一致したレコードが [**Certificate List**] ウィンドウに表示されます。

証明書の詳細ページで [**再生成（Regenerate**）] ボタンをクリックすると、同じキー長を持つ自己署名証明書が再生成されます。

3072 または 4096 の新しいキー長の自己署名証明書を再生成するには、[**自己署名証明書の生成（Generate Self-Signed Certificate**）] をクリックします。

Step 2 [**自己署名証明書の新規作成（Generate New Self-Signed Certificate**）] ウィンドウのフィールドを設定します。フィールドおよび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 3 [生成（Generate）] をクリックします。

Step 4 再作成された証明書の影響を受けるサービスをすべて再起動します。

Step 5 CAPF 証明書、ITLRecovery 証明書または CallManager 証明書の再作成後に CTL クライアントを再実行します（設定している場合）。

Note tomcat を再生成した場合、

- CallManager サービスを再起動します。そうしない場合、ポート 5090/5091（SIP Oauth の場合）の CallManager サービスは古い tomcat 証明書の提示を続けて、TLS で問題を引き起こします。
- TFTP サービスを非アクティブ化してアクティブ化します。そうしない場合、TFTP は古いキャッシュされた自己署名 tomcat 証明書の提供を続けます。

Note 証明書を再作成したら、システムのバックアップを実行して、最新のバックアップに再作成した証明書が含まれるようにします。バックアップに再作成した証明書が含まれていない状態でシステムの復元タスクを実行する場合は、システム内の各電話機のロックを手動で解除して、電話機を登録できるようにする必要があります。

OAuth 更新ログイン用のキーの再生成

コマンドライン インターフェイスを使用して暗号キーと署名キーの両方を再生成するには、この手順を使用します。Cisco Jabber が Unified Communications Manager との OAuth 認証に使用する暗号キーまたは署名キーが侵害された場合にのみ、この作業を実行します。署名キーは非対称で RSA ベースであるのに対し、暗号キーは対称キーです。

このタスクを完了すると、これらのキーを使用する現在のアクセス トークンと更新トークンは無効になります。

エンドユーザへの影響を最小限に抑えるために、このタスクは営業時間外に完了することを推奨します。

暗号キーは、以下の CLI を使用してのみ再生成できますが、パブリッシャノードの Cisco Unified OS の管理 GUI を使用して署名キーを再生成することもできます。選択**[セキュリティ（Security）]**>

[証明書の管理（Certificate Management）] の順に選択しで、**AUTHZ** 証明書を選択し、[再生成（Regenerate）] をクリックします。

Procedure

Step 1 Unified Communications Manager 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。

Step 2 暗号キーを再生成するには、次の手順を実行します。

a) `set key regen authz encryption` コマンドを実行します。
b) 「`yes`」と入力します。

Step 3 署名キーを再生成するには、次の手順を実行します。

a) `set key regen authz signing` コマンドを実行します。
b) 「`yes`」と入力します。
Unified Communications Manager パブリッシャ ノードがキーを再生成し、IM and Presence サービスのローカル ノードを含めたすべての Unified Communications Manager クラスタ ノードに新しいキーを複製します。

すべての UC クラスタで新しいキーを再生成して同期する必要があります。

- IM and Presence 中央クラスタ：IM and Presence 集中型展開の場合、IM and Presence ノードはテレフォニーとは別のクラスタ上で実行されています。この場合、IM and Presence Service の中央クラスタの Unified Communications Manager パブリッシャ ノードで、この手順を繰り返します。
- Cisco Expressway または Cisco Unity Connection：これらのクラスタ上でもキーを再生成します。詳細については、Cisco Expressway および Cisco Unity Connection のマニュアルを参照してください。

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。

Note 新しい CSR を生成すると、既存の CSR は上書きされます。

Procedure

Step 1 [Cisco Unified OSの管理（Cisco Unified OS Administration）] から、以下を選択します。 **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]**。

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。

Procedure

Step 1 [Cisco Unified OSの管理（Cisco Unified OS Administration）] から、以下を選択します。 **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]**。

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 (Optional) (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。

信頼ストアへの認証局署名済み CAPF ルート証明書の追加

認証局署名済み CAPF ルート証明書を使用 する場合は、ルート証明書を Unified Communications Manager 信頼ストアに追加します。

Procedure

Step 1 [Cisco Unified OSの管理（Cisco Unified OS Administration）] から、以下を選択します。 **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]**。

Step 2 **[Upload Certificate/Certificate chain]** をクリックします。

Step 3 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）] ポップアップウィンドウで、[証明書の目的（Certificate Purpose）] ドロップダウンリストから [CallManager-trust] を選択し、認証局署名済み CAPF ルート証明書を参照します。

Step 4 [ファイルのアップロード（Upload File）] フィールドに証明書が表示されたら、[アップロード（Upload）] をクリックします。

CTL ファイルの更新

この手順を使用して、CLI コマンドを使用して CTL ファイルを更新します。混合モードが有効になっている場合は、新しい証明書をアップロードするたびに CTL ファイルを更新する必要があります。

Procedure

Step 1 Unified Communications Manager のパブリッシャノードから、**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 update CTLfile` コマンドを実行します。CTL ファイルを再生成すると、ファイルが TFTP サーバにアップロードされて、電話機に自動的に送信されます。

証明書のモニタリングと失効タスクのフロー

このセクションでは、更新が必要な証明書をモニタし、有効期限が切れた証明書を無効にできます。

証明書モニタリングの概要

管理者は、自動化されたシステムが Unified Communications Manager および IM and Presence Service サービスに含まれている場合、証明書を 追跡および更新できる必要があります。証明書モニタリングは、管理者が証明書のステータスを継続的に知り、証明書の有効期限が近づいたときに電子メールで通知を受信するのに役立ちます。

証明書モニタリングの設定

[Cisco Certificate Expiry Monitor] ネットワーク サービスを実行している必要があります。デフォルトでは、このサービスは有効ですが、次を選択して、Cisco Unified Serviceability アプリケーションでサービスが実行されているかどうかを確認することができます。 **[ツール（Tools）] > [コントロールセンター - ネットワークサービス（Control Center - Network Services）]** 次に、[Cisco Certificate Expiry Monitorサービス（Cisco Certificate Expiry Monitor Service）] のステータスが [実行中（Running）] であることを確認します。

Procedure

Step 1 [Cisco Unified OS の管理（Cisco Unified OS Administration）] から、以下を選択します。 **[セキュリティ（Security）] > [証明書モニタ（Certificate Management）]**

Step 2 設定の詳細を入力または選択します。

Step 3 [保存（**Save**）] をクリックして、設定を保存します。

Note デフォルトで、証明書モニタサービスは24時間ごとに1回実行されます。証明書モニタサービスを再起動すると、サービスが開始され、24時間後に実行する次のスケジュールが計算されます。証明書の有効期限が7日以内に近づいても、この頻度は変わりません。このサービスは、証明書の有効期限が切れる1日前から、有効期限が切れた後も1時間おきに実行します。

証明書失効の概要

このセクションでは、証明書失効について説明します。Cisco UCMは、証明書失効をモニタするためにオンライン証明書ステータスプロトコル（OCSP）をプロビジョニングします。証明書がアップロードされるたびに、スケジュールされたタイムラインで、システムはそのステータスをチェックして有効性を確認します。

コモンクライテリアモードが有効になっているFIPS展開の場合、OCSPはシステムのコモンクライテリア要件への準拠にも役立ちます。

証明書失効の設定

[有効性検証（Validation Checks）]では、Unified Communications Managerは証明書のステータスを確認し、有効性を確認します。

証明書の検証手順は次のとおりです。

- Unified Communications Managerは代理信頼モデル（DTM）を使用し、OCSP署名属性のルートCAまたは中間CAをチェックします。ルートCAまたは中間CAは、OCSP証明書に署名してステータスを確認する必要があります。
- 代理信頼モデルが失敗した場合は、レスポンダの信頼モデル（TRP）に戻ります。次に、Unified Communications ManagerはOCSPサーバからの指定されたOCSP応答署名証明書を使用して証明書を検証します。

Note 証明書の失効ステータスを確認するために、OCSPレスポンダが実行されている必要があります。

期限切れの証明書が自動的に失効するようにOCSPを設定します。[証明書失効（Certificate Revocation）]ウィンドウでOCSPオプションを有効にすると、最も安全な方法でリアルタイムに証明書失効をチェックすることができます。オプションから、証明書のOCSP URIを使用するか、または設定済みのOCSP URIを使用するかを選択します。

Note syslog、FileBeat、SIP、ILS、LBMなど、TLSクライアントはOCSPからリアルタイムで失効応答を受信します。

システムに OCSP チェックに必要な証明書があることを確認します。OCSP 応答属性で設定されたルート CA 証明書または中間 CA 証明書、または tomcat-trust にアップロードされた、指定 OCSP 署名証明書を使用できます。

Procedure

Step 1 [Cisco Unified OSの管理（Cisco Unified OS Administration）] から、以下を選択します。 **[セキュリティ（Security）] > [証明書失効（Certificate Revocation）]**

Step 2 **[ANATの有効化（Enable OCSP）]** チェックボックスを選択します。

Step 3 証明書に OCSP レスポンダ URI が設定されている場合は、[証明書からの OCSP URI を使用する（Use OCSP URI from Certificate）] オプションをクリックします。

または

Step 4 OCSP チェックに OCSP レスポンダを指定する場合は、[設定された OCSP URI を使用（Use Configured OCSP URI Option）] をクリックします。

Step 5 レスポンダの [OCSP の設定済み URI] を入力します。

Step 6 失効チェックを有効にするには、[失効チェックの有効化（Enable Revocation Check）] チェックボックスをオンにします。

Step 7 失効ステータスを確認する**頻度**を入力し、[時間（Hours）] または [Days（日）] から**時間間隔**をクリックします。

Step 8 [保存（Save）] をクリックします。

Note シスコサービスのリストを再起動して、リアルタイム OCSP を有効にするように求める、アラートがポップアップ表示されます。このポップアップは、[OCSP の有効化（Enable OCSP）] チェックボックスをオンにした場合、または以降の変更を保存した場合にのみ表示されます。

OCSP レスポンダは、検証とコモンクライテリアモードがオンの場合に、次のいずれかのステータスを返します。

- [良好（Good）]：OCSP レスポンダがステータスの照会に対して肯定的な応答を送信していることを示します。証明書は失効しませんが、証明書が発行されたという意味でも、応答時間が証明書の有効期間内にあるという意味でもありません。Response 拡張機能は、発行、有効性など、証明書のステータスに関してレスポンダが行ったより多くの要求を伝えます。
- [失効（Revoked）]：証明書が永久的または一時的に失効（保留）ステータスにあることを示します。
- [不明（Unknown）]：OCSP レスポンダが要求された証明書について認識していないことを示しています。

Warning コモンクライテリアモードを有効にした場合、接続は [失効済み（Revoked）] および [不明（Unknown）] のケースで失敗します。コモンクライテリアモードを無効にすると、接続は [不明（Unknown）] のケースで成功します。

Step 9 (Optional) CTI、IPsec または LDAP リンクがある場合は、これらの長期的に中断しない接続の OCSP 失効サポートを有効にするために、上記の手順に加えて次の手順も行う必要があります。

a) [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]**。

b) [証明書失効と有効期限（Certificate Revocation and Expiry）] ペインに移動します。

c) [証明書有効性チェック（Certificate Validity Check）] パラメータを [有効（Enabled）] に設定します。

d) [有効性チェック頻度（Validity Check Frequency）] パラメータの値を入力します。

Note **[証明書失効（Certificate Revocation）]** ページの **[失効チェックの有効化（Enable Revocation Check）]** パラメータの間隔値は、**[有効性チェックの頻度（Validity Check Frequency）]** エンタープライズパラメータの値よりも優先されます。

e) [保存（Save）] をクリックします。