証明書の設定

証明書の概要

アイデンティティを保護し、IM and Presence Serviceと別のシステム間の信頼関係を構築するために証明書が使用されます。証明書を使用すると、IM and Presence Service を Cisco Jabber クライアント、または任意の外部サーバに接続することが可能です。証明書がなければ、不正な DNS サーバが使用されていないか、または別のサーバにルーティングされていないかを判断することはできません。

IM and Presence Service が使用できる証明書には、以下の 2 つの主要なクラスがあります。

- 自己署名証明書：自己署名証明書は、証明書を発行したサーバと同じサーバによって署名されます。企業内では、セキュアでないネットワークに接続している接続がない場合は、自己署名付きの証明書を使用して、別の内部システムに接続することができます。たとえば、IM and Presence Service は、Cisco Unified Communications Manager への内部接続に、自己署名証明書を生成する場合があります。

- CA 署名付き証明書：CA 署名付き証明書は、サードパーティ認証局 (CA) によって署名された証明書です。CA 署名付き証明書は、サーバあるいはサービス証明書の有効性を制御するパブリック CA（Verisign、Entrust、または Digicert）あるいはサーバ（Windows 2003、Linux、Unix、IOS など）によって署名されている場合があります。CA 署名付き証明書は、自己署名証明書よりも安全であり、通常、WAN 接続に使用されます。たとえば、別の企業または WAN 接続を使用したクラスタ間ピア構成では、外部システムとの信頼関係を構築するために CA 署名付きの証明書が必要となります。

CA 署名付き証明書は、自己署名証明書よりも安全です。通常、自己署名付き証明書は内部接続では十分であると見なされますが、パブリック インターネット経由あるいは WAN 経由で接続する場合は、CA 署名付き証明書を使用する必要があります。

マルチサーバ証明書

IM and Presence Service は、いくつかのシステム サービスのマルチサーバ SAN 証明書もサポートしています。複数のサーバ証明書の証明書署名要求（CSR）を生成すると、証明書がアップロードされる際、結果として得られるマルチサーバ証明書とその証明書のチェーンは、すべてのクラスタ ノードに自動的に配布されます。

IM and Presence Services の証明書タイプ

IM and Presence Service 内のさまざまなシステム コンポーネントには、さまざまな種類の証明書が必要です。以下のテーブルでは、IM and Presence Service のクライアントおよびサービスで必要とされるさまざまな証明書について説明します。

（注） 証明書名が -ECDSA で終わる場合、その 証明書/キー タイプは楕円曲線（EC）です。それ以外の場合は、RSA です。

表 *1*: 証明書タイプおよびサービス

証明書タイプ	サービス	証明書信頼ストア	マルチサーバ サポート	注記
tomcat tomcat-ECDSA	Cisco Client Profile Agent Cisco AXL Web Service Cisco Tomcat	tomcat- trust	はい	IM and Presence Service のクライアント認証の一部として Cisco Jabber クライアントに提示されます。 Cisco Unified CM IM およびプレゼンス管理ユーザインターフェイスを移動するときに、Web ブラウザに表示されます。 関連する信頼ストアを使用し、ユーザのクレデンシャルを認証するために、IM and Presence Service が確立した設定済みの LDAP サーバとの 接続を確認します。
IPSec		ipsec-trust	非対応	IPSec ポリシーが有効になっている場合に使用します。

証明書タイプ	サービス	証明書信頼ストア	マルチサーバ サポート	注記
CUP cup-ECDSA	Cisco SIP Proxy Cisco Presence Engine	cup-trust	非対応	Expressway-C に証明書を提示して、SIP フェデレーションユーザ用の IM and Presence を取得します。IM and Presence プロキシは、クライアントとサーバの両方として動作します。 プレゼンスエンジンは、これらの証明書を Exchange/Office 365 との通信に使用してカレンダープレゼンスを取得します。プレゼンスエンジンは、クライアントとしてのみ動作します。
cup-xmpp cup-xmpp-ECDSA	Cisco XCP Connection Manager Cisco XCP Web Connection Manager Cisco XCP Directory サービス Cisco XCP Router サービス	cup-xmpp-trust	はい	XMPP セッションの作成中に、Cisco Jabber クライアント、サードパーティ製 XMPP クライアント、または CAXL ベースのアプリケーションに提示されます。 関連する信頼ストアを使用して、サードパーティ製 XMPP クライアントの LDAP 検索操作を実行中に Cisco XCP Directory サービスが確立した接続を確認します。 ルーティング通信タイプがルータ間に設定されている場合に、IM and Presence Service サーバ間にセキュアな接続を確立するときに Cisco XCP Router によって関連する信頼ストアが使用されます。
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Cisco XCP XMPP Federation Connection Manager	cup-xmpp-trust	はい	外部フェデレーション XMPP への接続時に XMPP ドメイン間フェデレーションを行うために提示されます。

証明書の前提条件

Cisco Unified Communications Manager で次の項目を設定します。

- IM and Presence サービスの SIP トランク セキュリティ プロファイルを設定します。
- IM and Presence Service の SIP トランクを設定します。
  - SIP トランクにセキュリティ プロファイルを関連付けます。

- IM and Presence Service 証明書のサブジェクト共通名（CN）を SIP トランクに設定します。

Cisco Unified Communications Manager との証明書交換

これらのタスクを完了して、Cisco Unified Communications Manager と交換を行います。

（注） Cisco Unified Communications Manager と IM and Presence Service の間の証明書の交換は、インストールの過程で自動的に処理されます。ただし、証明書交換を手動で行う必要がある場合は、このタスクを実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	IM and Presence サービスへの Cisco Unified Communications Manager 証明書のインポート （4 ページ）	IM and Presence サービスに Cisco Unified Communications Manager 証明書をインポートします。
ステップ 2	IM and Presence サービスからの証明書のダウンロード （5 ページ）	IM and Presence Service から証明書をダウンロードします。証明書は Cisco Unified Communications Manager にインポートする必要があります。
ステップ 3	IM and Presence への Cisco Unified Communications Manager 証明書のインポート （6 ページ）	証明書の交換を完了するには、IM and Presence Service の証明書を Cisco Unified Communications Manager の Callmanager-trust にインポートします。

IM and Presence サービスへの Cisco Unified Communications Manager 証明書のインポート

この手順で、IM and Presence Service に Cisco Unified Communications Manager 証明書をインポートします。

手順

ステップ 1 **Cisco Unified CM IM and Presence 管理**で、**システム** > **セキュリティ** > **証明書インポート ツール**を選択します。

ステップ 2 **[Certificate Trust Store（証明書信頼ストア）]** メニューから **[IM and Presence（IM/P）Service Trust（IM and Presence（IM/P）サービス信頼）]** を選択します。

ステップ 3 Cisco Unified Communications Manager ノードの IP アドレス、ホスト名、または FQDN を入力します。

ステップ 4 Cisco Unified Communications Manager ノードと通信するポート番号を入力します。

ステップ 5 [送信（Submit）] をクリックします。

（注） 証明書インポート ツールのインポート操作が完了すると、Cisco Unified Communications Manager に正常に接続したかどうか、また、Cisco Unified Communications Manager から証明書が正常にダウンロードされたかどうかが報告されます。証明書インポート ツールで障害が報告された場合、推奨処置についてはオンライン ヘルプを参照してください。**[Cisco Unified IM and Presence OS の管理（Cisco Unified IM and Presence OS Administration）]** > **[セキュリティ（Security）]** > **[証明書の管理（Certificate Management）]** を選択して、手動で証明書をインポートすることもできます。

（注） ネゴシエートされる TLS 暗号方式に応じて、証明書インポート ツールにより、RSA ベースの証明書または ECDSA ベースの証明書のいずれかがダウンロードされます。

ステップ 6 Cisco SIP Proxy サービスを再起動します。

a) Cisco Unified IM and Presence Serviceabilityから、IM and Presence Service に **ツール** > **コントロール センター - 機能サービス**を選択します。

b) **サーバ** ドロップダウン リスト ボックスで、IM and Presence Service クラスタ ノードを選択し、**移動**をクリックします。

c) **Cisco SIP プロキシ**を選択して、**再起動**をクリックします。

次のタスク

IM and Presence サービスからの証明書のダウンロード （5 ページ）

IM and Presence サービスからの証明書のダウンロード

この手順で、IM and Presence Service から証明書をダウンロードします。証明書を Cisco Unified Communications Manager にインポートする必要があります。

手順

ステップ 1 **Cisco Unified IM and Presence OS 管理**から、IM and Presence Service で**セキュリティ** > **証明書管理**を選択します。

ステップ 2 [検索（Find）] をクリックします。

ステップ 3 `cup.pem` ファイルを選択します。

（注） cup-ECDSAは、使用可能なオプションでもあります。

ステップ 4 [ダウンロード] をクリックして、ローカル コンピュータにファイルを保存します。

ヒント IM and Presence サービスが表示する cup.csr ファイルへのアクセスに関するすべてのエラーを無視してください。Cisco Unified Communications Manager と交換する証明書に CA（認証局）が署名する必要はありません。

次のタスク

IM and Presence への Cisco Unified Communications Manager 証明書のインポート （6 ページ）

IM and Presence への Cisco Unified Communications Manager 証明書のインポート

証明書の交換を完了するには、IM and Presence Service の証明書を Cisco Unified Communications Manager の Callmanager-trust にインポートします。

始める前に

IM and Presence サービスからの証明書のダウンロード （5 ページ）

手順

ステップ 1 Cisco Unified OS の管理にログインします。

ステップ 2 **セキュリティ** > **証明書管理**を選択する

ステップ 3 [証明書のアップロード（Upload Certificate）] をクリックします。

ステップ 4 [証明書名]メニューから **Callmanager-trust** を選択します。

ステップ 5 IM and Presence から以前にダウンロードした証明書を**参照し**、選択します。

ステップ 6 [ファイルのアップロード（Upload File）] をクリックします。

ステップ 7 Cisco CallManager サービスの再起動：

a) Cisco Unified Serviceability から、**[ツール（Tools）]** > **[コントロール センター - 機能サービス（Control Center - Feature Services）]** の順に選択します。

b) **サーバ** ドロップダウン リスト ボックスから、Cisco Unified Communications Manager ノードを選択して、**移動**をクリックします。

c) **Cisco CallManager** サービスを選択し、**再起動**をクリックします。

IM and Presence Service での証明機関 (CA) のインストール

IM and Presence Service でサードパーティ認証局 (CA) によって署名された証明書を使用するには、まず、IM and Presence Service で信頼できるルート証明書チェーンをインストールする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	CA ルート証明書チェーンのアップロード （7 ページ）	この手段で、サードパーティ認証局から IM and Presence Service に CA ルート証明書チェーンをアップロードします。
ステップ 2	Cisco Intercluster Sync Agent サービスの再起動 （8 ページ）	証明書のアップロードが完了したら、Cisco Intercluster Sync Agent サービスを再起動します。
ステップ 3	他のクラスタに CA 証明書が同期されていることの確認 （9 ページ）	CA 証明書チェーンがすべてのピア クラスタに複製されていることを確認します。

CA ルート証明書チェーンのアップロード

この手順を使用して、署名認証局 (CA) から IM およびプレゼンス データベースのパブリッシャーノードに証明書チェーンをアップロードします。このチェーンは、チェーン内の複数の証明書で構成されており、各証明書が後続の証明書に署名している場合があります。

- ルート証明書 > 中間 1 証明書 > 中間 2 証明書

手順

ステップ 1 IM and Presence データベース パブリッシャ ノードで、Cisco Unified CM IM and Presence OS 管理 にログインします。

ステップ 2 **[Security（セキュリティ）] > [Certificate Management（証明書管理）]** を選択します。

ステップ 3 [Upload Certificate/Certificate chain] をクリックします。

ステップ 4 **証明書名** ドロップダウン リストから、以下のいずれかを選択します。

- CA 署名付きの tomact 証明書をアップロードする場合は、**tomcat-trust**を選択してください。

- CA が署名した cup-xmpp 証明書あるいは CA で署名されたcup-xmpp-s2s をアップロードする場合は、**cup-xmpp-s2s**を選択します。

ステップ 5 署名付き証明書の**説明**を入力します。

ステップ 6 **[Browse（参照）]** をクリックしてルート証明書のファイルを見つけます。

ステップ 7 **ファイルのアップロードをクリック**をクリックします。

ステップ 8 同じ方法で、**証明書および証明書チェーンのアップロード**ウィンドウを使用して、それぞれの中間証明書をアップロードします。それぞれの中間証明書について、チェーンで先行する証明書名を入力する必要があります。

次のタスク

Cisco Intercluster Sync Agent サービスの再起動 （8 ページ）

Cisco Intercluster Sync Agent サービスの再起動

IM and Presence データベース パブリッシャ ノードにルートおよび中間証明書をアップロードしたら、そのノードで Cisco Intercluster Sync Agent サービスを再起動する必要があります。この再起動で、ただちに CA 証明書が他のすべてのクラスタで同期されます。

手順

ステップ 1 [Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] から、**[ツール（Tools）]** > **[コントロールセンタ-ネットワークサービス（Control Center - Network Services）]** を選択します。

ステップ 2 **サーバ** ドロップダウン リスト ボックスで、証明書をインポートした IM and Presence Service ノードを選択して、**移動**をクリックします。

（注） CLI（コマンドライン インターフェイス）で、`utils service restart Cisco Intercluster Sync Agent` を実行して Cisco Intercluster Sync Agent サービスを再起動することもできます。

ステップ 3 **Cisco Intercluster Sync Agent** サービスを選択して、**再起動**をクリックします。

次のタスク

クラスタ間同期の確認 （12 ページ）

他のクラスタに CA 証明書が同期されていることの確認

Cisco Intercluster Sync Agent サービスが再起動した後、CA 証明書が他のクラスタに正しく同期されたことを確認する必要があります。他の IM and Presence データベース パブリッシャの各ノードで、次の手順を実行します。

（注） この手順の情報は、-ECDSA で終わる証明書にも適用されます。

手順

ステップ 1 **Cisco Unified CM IM and Presence 管理**で、**診断** > **システムのトラブルシューティング**を選択します。

ステップ 2 **[クラスタ間トラブルシュータ（Inter-clustering Troubleshooter）]** で、**[各 TLS 対応クラスタ間ピアが正常にセキュリティ証明書を交換しました（Verify that each TLS-enabled inter-cluster peer has successfully exchanged security certificates）]** テストを検索し、テストに合格していることを確認します。

ステップ 3 テストでエラーが表示される場合は、クラスタ間ピアの IP アドレスを記録します。この IP アドレスは、CA証明書をアップロードしたクラスタを参照している必要があります。次のステップを続行し、問題を解決します。

ステップ 4 **[プレゼンス（Presence）]** > **[クラスタ間（Inter-Clustering）]** を選択し、[システム トラブルシュータ（System Troubleshooter）] ページで識別したクラスタ間ピアに関連付けられているリンクをクリックします。

ステップ 5 **[強制手動同期（Force Manual Sync）]** をクリックします。

ステップ 6 クラスタ間ピア ステータス パネルの自動リフレッシュには、60 秒かかります。

ステップ 7 **[証明書のステータス（Certificate Status）]** フィールドに「セキュアな接続です（Connection is secure）」が表示されていることを確認します。

ステップ 8 [Certificate Status（証明書のステータス）] フィールドに「Connection is secure（セキュアな接続です）」が表示されていない場合は、IM and Presence データベース パブリッシャ ノードで Cisco Intercluster Sync Agent サービスを再起動してから、ステップ 5 ～ 7 を繰り返します。

- 管理者 CLI からサービスを再起動するには、utils service restart Cisco Intercluster Sync Agent コマンドを実行します。
- また、Cisco Unified IM and Presence Serviceability の GUI からこのサービスを再起動できます。

ステップ 9 この時点で **[証明書のステータス（Certificate Status）]** フィールドに「セキュアな接続です（Connection is secure）」が表示されていることを確認します。これは、クラスタ間同期がクラスタ間で正常に確立され、アップロードした CA 証明書がほかのクラスタに同期していることを意味します。

次のタスク

各 IM and Presence Service ノードへ署名付き証明書をアップロードします。

IM and Presence Service への証明書のアップロード

以下のタスクを実行して、IM and Presence Service 用の 証明書をアップロードします。CA 署名付き証明書または自己署名証明書をアップロードすることが可能です。

始める前に

サードパーティ認証局 (CA) によって署名された CA 署名済みの証明書を使用するには、その CA のルート証明書チェーンを既に IM and Presence Service にインストールしている必要があります。詳細は、IM and Presence Service での証明機関 (CA) のインストール （7 ページ）を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	証明書のアップロード（Upload Certificates） （11 ページ）	IM and Presence Service に署名付き証明書をアップロードします。
ステップ 2	Cisco Tomcat サービスの再起動 （12 ページ）	（tomcat 証明書のみ）。Cisco Tomcat サービスを再起動します。
ステップ 3	クラスタ間同期の確認 （12 ページ）	（tomcat 証明書のみ）。Cisco Tomcat サービスがクラスタ内の影響を受けるすべてのノードに対して再起動した後、クラスタ間同期が正常に動作していることを確認する必要があります。
ステップ 4	すべてのノードで Cisco XCP ルータ サービスを再起動します。 （13 ページ）	cup-xmpp ストアに証明書をアップロードした場合は、すべてのクラスタ ノード上で Cisco XMP Router を再起動します。
ステップ 5	Cisco XCP XMPP Federation Connection Manager サービスの再起動 （13 ページ）	（XMPP フェデレーションのみ）。XMPP フェデレーション用の cup-xmpp ストアに証明書をアップロードした場合は、Cisco XCPXMPP フェデレーション サービスを再起動します。
ステップ 6	XMPP フェデレーションのセキュリティ証明書でのワイルドカードの有効化 （14 ページ）	（XMPP フェデレーションのみ）。TLS を介して XMPP フェデレーション用の cup-xmpp ストアに証明書をアップロードした場合は、XMPP セキュリティ証明

	コマンドまたはアクション	目的
		書のワイルドカードを有効にする必要があります。これはグループ チャットに必要です。

証明書のアップロード（Upload Certificates）

各 IM and Presence Service ノードに署名付き証明書をアップロードします。

（注） クラスタに必要なすべてのtomcat証明書に署名し、それらを同時にアップロードすることを推奨します。この方法を使用すると、クラスタ間通信のリカバリに要する時間が短縮されます。

（注） この手順の情報は、-ECDSA で終わる証明書にも適用されます。

始める前に

証明書が CA によって署名されている場合は、そのCA のルート証明書チェーンがインストールされている必要があります。でないと、CA署名証明書が信頼されないものとみなされます。CA 証明書がすべてのクラスタに正しく同期されている場合は、各 IM and Presence Service ノードに適切な署名付き 証明書をアップロードできます。

手順

ステップ 1 **Cisco Unified IM and Presence OS 管理**で、**セキュリティ** > **証明書管理**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 **証明書の目的**を選択します。たとえば、**tomcat**とします。
ステップ 4 署名付き証明書の説明を入力します。
ステップ 5 アップロードするファイルを検索するには、**[参照（Browse）]** をクリックします。
ステップ 6 [ファイルのアップロード] をクリックします。
ステップ 7 各 IM and Presence Service ノードで繰り返します。

次のタスク

Cisco Tomcat サービスを再起動します。

Cisco Tomcat サービスの再起動

各 IM and Presence サービス ノードに tomcat 証明書をアップロードしたら、各ノードで Cisco Tomcat サービスを再起動する必要があります。

手順

ステップ 1 管理 CLI にログインします。
ステップ 2 次のコマンドを実行します。`utils service restart Cisco Tomcat`。
ステップ 3 各ノードで繰り返します。

次のタスク

クラスタ間同期が正常に動作していることを確認します。

クラスタ間同期の確認

Cisco Tomcat サービスがクラスタ内の影響を受けるすべてのノードに対して再起動した後、クラスタ間同期が正常に動作していることを確認する必要があります。他のクラスタの各 IM and Presence データベース パブリッシャ ノードで次の手順を実行します。

手順

ステップ 1 **Cisco Unified CM IM and Presence 管理**で、**診断** > **システムのトラブルシューティング**を選択します。
ステップ 2 **[クラスタ間トラブルシュータ（Inter-clustering Troubleshooter）]** で、**[各 TLS 対応クラスタ間ピアがセキュリティ証明書を正常に交換していることを確認する（Verify that each TLS-enabled inter-cluster peer has successfully exchanged security certificates）]** テストを検索し、テストに合格していることを確認します。
ステップ 3 テストでエラーが表示される場合は、クラスタ間ピアの IP アドレスを記録します。この IP アドレスは、CA証明書をアップロードしたクラスタを参照している必要があります。次のステップを続行し、問題を解決します。
ステップ 4 **プレゼンス**>**クラスタ間**を選択し、[システムのトラブルシューティング]ページで、識別したクラスタ間ピアに関連付けられているリンクをクリックします。
ステップ 5 **[強制手動同期（Force Manual Sync）]** をクリックします。
ステップ 6 **[ピアの Tomcat 証明書も再同期します（Also resync peer's Tomcat certificates）]** チェックボックスをオンにし、**[OK]** をクリックします。
ステップ 7 クラスタ間ピア ステータス パネルの自動リフレッシュには、60 秒かかります。
ステップ 8 **[証明書のステータス（Certificate Status）]** フィールドに「セキュアな接続です（Connection is secure）」が表示されていることを確認します。

ステップ 9 **[証明書のステータス（Certificate Status）]** フィールドに「セキュアな接続です（Connection is secure）」が表示されていない場合は、IM and Presence データベース パブリッシャ ノードで Cisco Intercluster Sync Agent サービスを再起動してから、ステップ 5 ～ 8 を繰り返します。

- 管理者 CLI からサービスを再起動するには、[utils service restart Cisco Intercluster Sync Agent] コマンドを実行します。
- また、Cisco Unified IM and Presence Serviceability の GUI からこのサービスを再起動できます。

ステップ 10 この時点で [Certificate Status（証明書のステータス）] フィールドに「Connection is secure（セキュアな接続です）」が表示されていることを確認します。これは、クラスタ間同期が、このクラスタと、証明書をアップロードしたクラスタの間で再確立されていることを意味します。

すべてのノードで Cisco XCP ルータ サービスを再起動します。

各 IM and Presence Service ノードに cup-xmpp の証明書や cup-xmpp-ECDSA の証明書をアップロードしたら、各ノードで Cisco XCP Router サービスを再起動する必要があります。

（注） また、Cisco Unified IM and Presence Serviceability GUI から Cisco XCP Router サービス を再起動できます。

手順

ステップ 1 管理 CLI にログインします。

ステップ 2 次のコマンドを実行します。[utils service restart Cisco XCP Router]

ステップ 3 各ノードで繰り返します。

Cisco XCP XMPP Federation Connection Manager サービスの再起動

各 IM and Presence サービス のフェデレーション ノードに cup-xmpp-s2s の証明書や cup-xmpp-s2s-ECDSA の証明書をアップロードしたら、各フェデレーション ノードの Cisco XCP XMPP Federation Connection Manager サービスを再起動する必要があります。

手順

ステップ 1 管理 CLI にログインします。

ステップ 2 次のコマンドを実行します。[utils service restart Cisco XCP XMPP Federation Connection Manager]

ステップ 3 各フェデレーション ノードで繰り返します。

XMPP フェデレーションのセキュリティ証明書でのワイルドカードの有効化

XMPP フェデレーションのパートナー間での TLS を介してのグループ チャットをサポートするには、XMPP セキュリティ証明書に対するワイルドカードを有効にする必要があります。

デフォルトでは、XMPP フェデレーション セキュリティ証明書の `cup-xmpp-s2s` および `cup-xmpp-s2s-ECDSA` には IM and Presence Service 展開によってホストされるすべてのドメインが含まれます。これらは、証明書内のサブジェクト代替名（SAN）エントリとして追加されます。同じ証明書内のホストされているすべてのドメインにワイルドカードを指定する必要があります。そのため、「example.com」の SAN エントリの代わりに、XMPP セキュリティ証明書には「*.example.com」の SAN エントリが含まれている必要があります。グループ チャットのサーバ エイリアスは、IM and Presence Service システムでホストされているいずれかのドメインのサブドメインであるため、ワイルドカードが必要です。例：「conference.example.com」。

（注） いずれのノードでも、`cup-xmpp-s2s` または `cup-xmpp-s2s-ECDSA` を表示するには、**Cisco Unified IM and Presence OS 管理** > **セキュリティ** > **証明書管理** を選択して、**cup-xmpp-s2s** または **cup-xmpp-s2s-ECDSA** のリンクをクリックします。

手順

ステップ 1 **[システム（System）]** > **[セキュリティの設定（Security Settings）]** を選択します。

ステップ 2 [XMPP フェデレーション セキュリティ証明書でのワイルドカードの有効化（Enable Wildcards in XMPP Federation Security Certificates）] をオンにします。

ステップ 3 [保存（Save）] をクリックします。

次のタスク

Cisco XMPP Federation Connection Manager サービスが実行しており、XMPP フェデレーションが有効になっているクラスタ内のすべてのノードで XMPP フェデレーション セキュリティ証明書を生成する必要があります。このセキュリティ設定は、すべての IM and Presence Service クラスタで有効にし、TLS を介しての XMPP フェデレーションをサポートする必要があります。

CSR を作成する

この手順で、証明書署名要求（CSR）を生成します。CSR は、サードパーティ CA に送信して、CA が署名した証明書を提供してもらう必要があります。

手順

ステップ 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。

ステップ 2 **CSRの生成** ボタンをクリックします。**証明書署名要求の生成** のポップアップ画面が表示されます。

ステップ 3 **証明書の目的** ドロップダウンから、生成する証明書のタイプを選択します。

ステップ 4 **配布** ドロップダウンから、IM and Presence サーバを選択します。マルチサーバ証明書の場合は、**マルチサーバ**を選択します。

ステップ 5 **キーの長さ**と**ハッシュ アルゴリズム**を入力します。

ステップ 6 残りのすべてのフィールドの入力を完了して、**生成**をクリックします。

ステップ 7 CSR をローカル コンピュータにダウンロードします。

a) [CSR のダウンロード（Download CSR）] をクリックします。
b) [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。
c) **CSR のダウンロード**

次のタスク

CSR をサードパーティ認証局に送信して、CA 署名付き証明書を発行してもらいます。

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。

表 *2 : 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		

	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
CAPF（パブリッシャのみ）	N	Y			Y	N		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）	N	Y	Y		Y	Y	Y		

表 *3 : 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		
cup-xmpp cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		

（注） CA 署名証明書のプロセスの一部として、「データ暗号化」ビットが変更または削除されていないことを確認します。

自己署名証明書の生成

この手順で、事故署名証明書を生成します。

手順

ステップ 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。

ステップ 2 [自己署名証明書の作成（Generate Self-signed）] をクリックします。**新しい自己署名入りの証明書の生成**のポップアップ画面が表示されます。

ステップ 3 **証明書の目的** ドロップダウンから、生成する証明書のタイプを選択します。

ステップ 4 **配布** ドロップダウンで、サーバ名を入力します。

ステップ 5 適切な**キー長**を選択します。

ステップ 6 **ハッシュ アルゴリズム**から、暗号化アルゴリズムを選択します。たとえば、SHA256 を選びます。

ステップ 7 [生成（Generate）] をクリックします。

IM and Presence Service の自己署名信頼証明書の削除

同じクラスタ内のノード間でサービスアビリティ用のクロスナビゲーションをサポートするために、IM and Presence サービスと Cisco Unified Communications Manager の間の Cisco Tomcat サービス信頼ストアが自動的に同期されます。

元の自己署名入りの信頼証明書を CA 署名付き証明書と置き換えた場合、元の自己署名入りの信頼証明書は、サービストラスト ストアに保持されます。この手段で、IM and Presence Service および Cisco Unified Communications Manager の自己署名証明書を削除することができます。

始める前に

重要 CA 署名付き証明書をついたした場合、指定された IM and Presence Service ノード上で Cisco Intercluster Sync Agent サービスが定期的なクリーンアップ タスクを実行するのを 30 分待機してください。

手順

ステップ 1 Cisco Unified IM and Presence OS 管理で、**セキュリティ > 証明書管理**を選択します。

ステップ 2 [検索（Find）] をクリックします。

[証明書の一覧（Certificate List）] が表示されます。

（注） 証明書の名前は、サービス名と証明書タイプの 2 つの部分で構成されています。たとえば tomcat-trust では、tomcat がサービスで trust が証明書タイプです。

削除できる自己署名付き信頼証明書は、次のとおりです。

- Tomcat および Tomcat-ECDSA：tomcat-trust
- Cup-xmpp および Cup-xmpp-ECDSA：cup-xmpp-trust
- Cup-xmpp-s2s および Cup-xmpp-s2s-ECDSA：cup-xmpp-trust
- カップとカップ-ECDSA: カップトラスト
- Ipsec：ipsec-trust

ステップ 3 削除する自己署名付き信頼証明書のリンクをクリックします。

重要 サービス信頼ストアに関連付けられているサービスに対して、CA 署名付き証明書がすでに設定されていることを確認します。

新しいウィンドウが表示され、証明書の詳細が示されます。

ステップ 4 [削除（Delete）] をクリックします。

（注） **削除** ボタンは、削除する権限が与えられている証明書に関してのみ表示されます。

ステップ 5 クラスタ内、およびでクラスタ間ピアの各 IM and Presence Service ノードに対してこの手順を繰り返し、不要な自己署名信頼証明書が展開全体で完全に削除されるようにします。

次のタスク

サービスが Tomcat である場合は、Cisco Unified Communications Manager ノード上の IM and Presence Service ノードの自己署名付き tomcat-trust 証明書を確認する必要があります。Cisco Unified Communications Manager からの自己署名 Tomcat 信頼証明書の削除 （18 ページ）を参照してください。

Cisco Unified Communications Manager からの自己署名 Tomcat 信頼証明書の削除

クラスタ内の各ノードについて、Cisco Unified Communications Manager サービス信頼ストアには 1 つの自己署名 tomcat 信頼証明書があります。Cisco Unified Communications Manager ノードから削除する対象となるのは、これらの証明書だけです。

（注） 次の手順の情報は、-EC 証明書にも適用されます。

始める前に

CA 署名付き証明書でクラスタの IM and Presence Service ノードをすでに設定し、証明書が Cisco Unified Communications Manager ノードに伝達されるよう 30 分間待機したことを確認します。

手順

ステップ 1 **Cisco Unified OS 管理**で、**セキュリティ** > **証明書管理**を選択します。

[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2 検索結果をフィルタリングするには、ドロップダウン リストから **[証明書（Certificate）]** および **[で始まる（begins with）]** を選択し、空のフィールドに tomcat-trust と入力します。[検索（Find）] をクリックします。

[証明書の一覧（Certificate List）] ウィンドウが拡張され、tomcat-trust の証明書が示されます。

ステップ 3 IM and Presence Service ノードのホスト名、または名前の FQDN が含まれているリンクを特定します。これらは、このサービスおよび IM and Presence Service ノードに関連付けられている自己署名証明書です。

ステップ 4 IM and Presence Service ノードの自己署名 tomcat-trust 証明書のリンクをクリックします。

新しいウィンドウが表示され、tomcat-trust 証明書の詳細が示されます。

ステップ 5 証明書の詳細で、Issuer Name CN= と Subject Name CN= の値が一致している、つまり自己署名の証明書であることを確認します。

ステップ 6 自己署名の証明書であることが確認され、CA 署名付き証明書が Cisco Unified Communications Manager ノードに確実に伝達されたと判断できる場合に、**削除**をクリックします。

（注） **[削除（Delete）]** ボタンは、削除する権限が与えられている証明書に関してのみ表示されます。

ステップ 7 クラスタ内の各 IM and Presence Service ノードに対して、手順 4、5、および 6 を繰り返します。

証明書モニタリング タスク フロー

次のタスクを行い、証明書ステータスと有効期限を自動的にモニタするようシステムを設定します。

- 証明書の有効期限が近づいているときは、電子メールで通知する。
- 有効期限が切れた証明書を失効させる。

手順

	コマンドまたはアクション	目的
ステップ 1	証明書モニタ通知の設定 （20 ページ）	証明書の自動モニタリングを構成します。システムは定期的に証明書ステータスをチェックし、証明書の有効期限が近づいていると電子メールで通知します。

	コマンドまたはアクション	目的
ステップ 2	OCSP による証明書失効の設定 （21 ページ）	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。

証明書モニタ通知の設定

Unified Communications Manager または IM and Presence サービスの自動証明書モニタリングを設定します。システムは定期的に証明書のステータスをチェックし、証明書の有効期限が近づいていると電子メールで通知します。

（注） [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。デフォルトでこのサービスは有効化されていますが、**[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）]** を選択し、[Cisco Certificate Expiry Monitor サービス（Cisco Certificate Expiry Monitor Service）] の状態が [実行中（Running）] であることを検証して Cisco Unified Serviceability でサービスが実行中であることを確認できます。

手順

ステップ 1 （Unified Communications Manager の証明書モニタリングのために）Cisco Unified OS の管理にログインするか、（IM and Presence サービスの証明書モニタリングのために）Cisco Unified IM and Presence の管理にログインします。

ステップ 2 **[セキュリティ（Security）] > [証明書モニタ（Certificate Management）]** を選択します。

ステップ 3 [通知開始時期（Notification Start Time）] フィールドに、数値を入力します。この値は、近づきつつある有効期限の通知を、有効期限の何日前にシステムが開始するかを表します。

ステップ 4 [通知頻度（Notification Frequency）] フィールドには、通知を行う頻度を入力します。

ステップ 5 これはオプションです。[電子メール通知を有効にする（Enable E-mail notification）] チェックボックスをオンにして、近づきつつある証明書有効期限に関する電子メールアラートをシステムに送信させます。

ステップ 6 [LSC モニタリングを有効にする（Enable LSC Monitoring）] チェック ボックスをオンにして、LSC 証明書を証明書ステータス チェックに含めます。

ステップ 7 [電子メール ID（E-mail IDs）] フィールドに、システムが通知を送信する電子メール アドレスを入力します。複数の電子メールアドレスは、セミコロンで区切って入力できます。

ステップ 8 [保存（Save）] をクリックします。

（注） 証明書モニタ サービスは、デフォルトで 24 時間ごとに 1 回だけ実行します。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、この周期は変化しません。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。

次のタスク

Online Certificate Status Protocol（OCSP）を設定し、期限切れの証明書をシステムが自動的に失効させるようにします。詳細については、次を参照してください。OCSP による証明書失効の設定 （21 ページ）

OCSP による証明書失効の設定

オンライン証明書ステータスプロトコル（OCSP）を有効にして、証明書の状態を定期的にチェックし、期限切れの証明書を自動的に失効させます。

始める前に

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 応答属性を設定されているルート CA 証明書または中間 CA 証明書を使用することができます。または、tomcat-trust へアップロードされている指定された OCSP 署名証明書を使用することができます。

手順

ステップ 1 （Unified Communications Manager の証明書失効のために）Cisco Unified OS の管理にログインするか、（IM and Presence サービスの証明書失効のために）Cisco Unified IM and Presence の管理にログインします。

ステップ 2 **[セキュリティ（Security）] > [証明書失効（Certificate Revocation）]** を選択します。

ステップ 3 [OCSP の有効化（Enable OCSP）] チェック ボックスをオンにして、次のタスクのいずれかを実行します。

- OCSP チェックの OCSP レスポンダを指定する場合は、[設定済み OCSP URI を使用する（Use configured OCSP URI）] ボタンを選択し、[OCSP 設定済み URI（OCSP Configured URI）] フィールドにレスポンダの URI を入力します。
- OCSP レスポンダ URI で証明書を設定する場合、[証明書からの OCSP URI を使用する（Use OCSP URI from Certificate）] ボタンを選択します。

ステップ 4 [失効チェックを有効にする（Enable Revocation Check）] チェック ボックスをオンにします。

ステップ 5 [チェック間隔（Check Every）] フィールドに失効チェックの間隔を入力します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 （省略可）CTI、IPsec または LDAP リンクがある場合は、これらの長期性接続の 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 の管理から、**[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。

b) [証明書の失効や有効期限（Certificate Revocation and Expiry）] で、[証明書有効性チェック（Certificate Validity Check）] パラメーターを [True] に設定します。

c) [有効性チェック頻度（Validity Check Frequency）] パラメーターの値を設定します。

（注） **証明書失効**ウィンドウの [失効チェックを有効にする（Enable Revocation Check）] パラメーターの間隔値は、[有効チェック頻度（Validity Check Frequency）] エンタープライズ パラメーターの値よりも優先されます。

d) [保存（Save）] をクリックします。

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。