証明書の設定

証明書の概要

証明書は ID を保護し、IM and Presence サービスと他のシステムとの間に信頼関係を構築するために使用されます。証明書を使用して、IM and Presence サービスを Cisco Unified Communications Manager、Cisco Jabber クライアント、または任意の外部サーバに接続できます。証明書がないと、不正な DNS サーバが使用されていたのか、それとも他のサーバにルーティングされていたのかを知ることは不可能です。

IM and Presence サービスが使用できる証明書には、主に 2 つのクラスがあります。

- 自己署名証明書 - 自己署名証明書は、証明書を発行したのと同じサーバによって署名されます。企業内では、自己署名証明書を使用して他の内部システムに接続することができます。ただし、それらの接続が安全でないネットワークを経由していない場合に限ります。たとえば、IM and Presence サービスは、Cisco Unified Communications Manager への内部接続用の自己署名証明書を生成します。

- CA 署名付き証明書 - サードパーティの認証局（CA）によって署名された証明書です。これらは、公的な CA（Verisign、Entrust、Digicert など）またはサーバ（Windows 2003、Linux、Unix、IOS など）によって署名され、サーバ/サービス証明書の有効性を管理できます。CA 署名付き証明書は自己署名証明書よりも安全であり、通常はあらゆる WAN 接続に使用されます。たとえば、他の企業とのフェデレーション接続または WAN 接続を使用するクラスタ間ピア設定では、外部システムとの信頼関係を構築するために CA 署名付き証明書が必要になります。

CA 署名付き証明書は自己署名証明書よりも安全です。一般に、自己署名証明書は内部接続に適していますが、WAN 接続または公衆インターネットを経由する接続には CA 署名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 サービスは、一部のシステムサービスに対してマルチサーバ SAN 証明書もサポートしています。マルチサーバ証明書の証明書署名要求（CSR）を生成すると、証明書がいずれかのクラスターノードにアップロードされると、結果として得られるマルチサーバ証明書とそれに関連付けられた署名証明書のチェーンが自動的にすべてのクラスターノードに配布されます。

IM and Presence Services の証明書タイプ

IM and Presence サービス内では、さまざまなシステムコンポーネントにさまざまな種類の証明書が必要です。ここでは、IM and Presence Service のクライアントとサービスに必要な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	あり	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	なし	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	なし	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 service、 Cisco XCP Router サービス	cup-xmpp-trust	あり	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	あり	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 プロファイルの設定
- 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 との証明書の交換

Cisco Unified Communications Manager との証明書の交換には以下のタスクを完了します。

（注） Cisco Unified Communications Manager と IM and Presence サービス間の証明書交換は、インストールプロセス中に自動的に処理されます。ただし、証明書交換を手動で完了する必要がある場合は、これらの作業を完了してください。

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 からの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。次の各証明書を 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 証明書を Cisco Unified Communications Manager にインポート （6 ページ）	証明書の交換を完了するには、IM and Presence サービス証明書を Cisco Unified Communications Manager の Callmanager-trust ストアにアップロードします。

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

この手順を使用して IM and Presence サービスに Cisco Unified Communications Manager からの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 の管理（Cisco Unified CM IM and Presence Administration）]** で、**[システム（System）]** > **[セキュリティ（Security）]** > **[証明書インポート ツール（Certificate Import Tool）]**を選択します。

ステップ 2 [証明書信頼ストア（Certificate Trust Store）] メニューから [IM and Presence（IM/P）サービス信頼（IM and Presence（IM/P）Service Trust）] 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 プロキシ サービスを再起動します。

a) IM and Presence サービスで [Cisco Unified IM and Presence サービサビリティ（Cisco Unified IM and Presence Serviceability）]から、**[ツール（Tools）]** > **[コントロール センター - 機能サービス（Control Center - Feature Services）]** を選択します。

b) **[サーバ（Server）]** ドロップダウンリストから [IM and Presence Service] ノードを選択し、**[移動（Go）]** をクリックします。

c) **Cisco SIP Proxy**を選択し、**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

この手順を使用して IM and Presence Service から証明書をダウンロードします。次の各証明書を 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 IM and Presence サービスで、**[Cisco Unified IM and Presence OS の管理（Cisco Unified IM and Presence 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 [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.pem` を選択することもできます。

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 証明書を Cisco Unified Communications Manager にインポート （6 ページ）

IM and Presence 証明書を Cisco Unified Communications Manager にインポート

証明書の交換を完了するには、IM and Presence サービス証明書を Cisco Unified Communications Manager の Callmanager-trust ストアにアップロードします。

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（Security）] > [証明書管理（Certificate Management）]** を選択します。

ステップ 3 [証明書のアップロード] をクリックします。

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

ステップ 5 IM and Presence サービスから以前にダウンロードした証明書を**閲覧**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 サービスを再起動します。

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（Server）]**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、**[Go（移動）]** をクリックします。
c) **Cisco CallManager** サービスを選択して**[再起動（Restart）]**をクリックします。

IM and Presence サービスに認証局（CA）をインストールする

IM and Presence サービスでサードパーティの認証局（CA）によって署名された証明書を使用するには、まずその CA のルート証明書信頼チェーンを IM and Presence サービスに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をアップロードする （7 ページ）	この手順を使用して、CA のルート証明書チェーンをサードパーティの認証局から IM and Presence サービスに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）	証明書をアップロードしたら、Cisco Intercluster Sync Agent サービスを再起動します。
ステップ 3	他のクラスタとの CA 証明書の同期の検証 （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たことを確認します。

CA ルート証明書チェーンをアップロードする

この手順を使用して、署名している認証局（CA）から IM and Presence データベースパブリッシャノードに証明書チェーンをアップロードします。チェーンはチェーン内の複数の証明書で構成され、各証明書は後続の証明書に署名します。

- 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 Administration] にログインします。

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

ステップ 3 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）] をクリックします。

ステップ 4 **[証明書名（Certificate Name）]** ドロップダウン リストから、以下のいずれか 1 つを選択します。

- CA 署名付きの tomact 証明書をアップロードする場合は、**トムキャット信頼**を選択します。
- CA 署名の cup-xmpp 証明書または CA 署名の cup-xmpp-s2s をアップロードする場合は、**cup-xmpp-trust**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 **[参照（Browse）]** 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（Upload File）]** をクリックします。

ステップ 8 **[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）]** ウィンドウを使用して、各中間証明書を同じ方法でアップロードします。中間証明書ごとに、チェーン内の前の証明書の名前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。このサービスの再起動することにより、ただちに CA 証明書が他のすべてのクラスタに同期されます。

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（Server）]** ドロップダウン リスト ボックスから、証明書をインポートする先の [IM and Presence Service] ノードを選択し、**[移動（Go）]** をクリックします。

（注） Command Line Interface から、`utils service restart Cisco Intercluster Sync Agent` コマンドで Cisco Intercluster Sync Agent サービスを再起動することも可能です。

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

クラスタ間同期の検証 （12 ページ）

他のクラスタとの CA 証明書の同期の検証

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 Administration** で、**[診断（Diagnostics）] > [システムトラブルシューティング（System Troubleshooter）]** を選択します。

ステップ 2 **[クラスタ間トラブルシューティング（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 トラブルシューティング（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 [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 ～ 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 に証明書をアップロードします。

次のタスクを実行して、IM and Presence サービスに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できます。

始める前に

サードパーティの認証局（CA）によって署名された CA 署名付き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 IM and Presence サービスにインストールしておく必要があります。詳細は、IM and Presence サービスに認証局（CA）をインストールする （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	クラスタ間同期の検証 （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）	証明書を cup-xmpp ストアにアップロードした場合は、すべてのクラスタノードで Cisco XMP Router を再起動してください。
ステップ 5	Cisco XCP XMPP Federation Connection Manager サービスの再起動 （14 ページ）	(XMPP フェデレーションのみ)。XMPP フェデレーション用に cup-xmpp ストアに証明書をアップロードした場合は、Cisco XCPXMPP フェデレーション接続

	コマンドまたはアクション	目的
		マネージャサービスを再起動してください。
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証明書を cup-xmpp ストアにアップロードした場合は、XMPP セキュリティ証明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）

この手順を使用して、各 IM and Presence Service ノードに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もインストールする必要があります。そうしないと、CA 署名付き証明書は信頼できません。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 の管理（Cisco Unified IM and Presence OS Administration）]** で、**[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 [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。

ステップ 3 **証明書の目的**を選択します。例えば、**tomcat**。

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（Upload File）] 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。

クラスタ間同期の検証

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 Administration** で、**[診断（Diagnostics）] > [システムトラブルシュータ（System Troubleshooter）]** 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（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 **[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 [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、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 サービス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 サービス 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） 任意のノード上の `cup-xmpp-s2s` または `cup-xmpp-s2s-ECDSA` 証明書を表示するには、**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、 **cup-xmpp-s2s** または **cup-xmpp-s2s-ECDSA** 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 サービス 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 の生成

この手順を使用して証明書署名要求（CSR）を生成します。CSR をサードパーティー の認証局に送信して、CAが署名した証明書を提供できるようにします。

手順

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 [CSRの生成（Generate CSR）] ボタンをクリックします。**[証明書署名要求の作成（Generate Certificate Signing Request）]** ポップアップが表示されます。

ステップ 3 **証明書の目的**ドロップダウンリストから、生成している証明書の種類を選択します。

ステップ 4 **[配信（Distribution）]** ドロップダウンから、IM and Presence サーバーを選択します。マルチサーバ証明書の場合は、**マルチサーバ（SAN）**を選択します。

ステップ 5 **キー長**および**ハッシュアルゴリズム**を入力します。

ステップ 6 残りのフィールドをすべて入力して**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 をサードパーティの認証局に送信して、CA が署名した証明書を発行できるようにします。

証明書署名要求のキー用途拡張

次の表に、Unified Communications Manager と IM and Presence Service の CA 証明書の両方に対する証明書署名要求（CSR）の主な使用法の拡張を示します。

表 *2 : Cisco Unified Communications Manager CSR* キー鍵用途拡張

	マルチサーバー	拡張キーの使用状況			キーの使途（**Key Usage**）				
		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（**Digital Signature**）]	鍵の暗号化	データの暗号化	鍵証明書サイン	鍵共有
CallManager CallManager-ECDSA	Y	Y	Y		Y	N	Y		
CAPF（パブリッシャーのみ）	N	Y	Y		Y	Y		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	N	Y		
TVS	Y	Y	Y		Y	Y	Y		

表 *3 : IM and Presence* サービスの *CSR* キーの用途の拡張

	マルチサーバー	拡張キーの使用状況			キーの使途（**Key Usage**）				
		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（**Digital Signature**）]	鍵の暗号化	データの暗号化	鍵証明書サイン	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		

自己署名証明書の生成

自己署名証明書を生成するには、次の手順を使用します。

手順

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 [自己署名証明書の作成（Generate Self-signed）] をクリックします。**新しい自己署名証明書を生成する**ポップアップが表示されます。

ステップ 3 **証明書の目的**ドロップダウンリストから、生成している証明書の種類を選択します。

ステップ 4 **分布**ドロップダウンから、サーバの名前を入力します。

ステップ 5 適切な**キーの長さ**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。例えば、SHA256 です。

ステップ 7 [Generate] をクリックします。

IM and Presence Service から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。

元の自己署名信頼証明書を CA 署名証明書に置き換えた場合、元の自己署名信頼証明書はサービス信頼ストアに残ります。この手順を使用して、Cisco Unified Communications Manager と IM and Presence サービスの両方にある自己署名証明書を削除することもできます。

始める前に

重要 CA 署名付き証明書を追加したら、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 分待機するようにします。

手順

ステップ 1 [Cisco Unified Operating System 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 **[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
- Cup および Cup-ECDSA：cup-trust
- 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（Delete）]** ボタンは、その証明書を削除する権限がある場合にのみ表示されます。

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 Operating System の管理ページ**で、**[セキュリティ(Security)]** > **[証明書の管理(Certificate Management)]**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は、**[削除（Delete）]** 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

	コマンドまたはアクション	目的
		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。
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 これはオプションです。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。