XMPP フェデレーションに使用するセキュリティ証明書の設定

XMPP フェデレーション用のセキュリティを設定するためには、以下のような操作を行う必要があります。

1 XMPP 証明書のドメインを設定します。

2 次のいずれかのタイプの証明書を作成します。

- XMPP フェデレーション用の自己署名証明書
- XMPP フェデレーション用の CA 署名付き証明書

3 ルート CA 証明書をインポートします。

まだ信頼していない CA を使用する企業とのフェデレーションを新たに設定するたびに、この操作を繰り返します。 同様に、フェデレーションを新たに設定する企業が自己署名証明書を使用している場合もこの操作を行う必要があります。この場合、ルート CA 証明書の代わりに自己署名証明書がアップロードされます。

XMPP 証明書用のドメインを設定する

XMPP フェデレーションの場合、証明書の Subject Common Name（CN）には、IM and Presence サーバのドメインを含める必要があります。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [セキュリティ（Security）] > [設定（Settings）] を選択します。

ステップ 2 [XMPP サーバツーサーバ証明書件名 CN のドメイン名（Domain name for XMPP Server-to-Server certificate Subject Common name）] に、IM and Presence サーバのドメイン名を入力します。

ヒント ここではワイルドカードのドメインを設定できます。たとえば、IM and Presence でチャット機能を配置し、チャット コンポーネントが親ドメインのサブドメインである場合は「*.example.net」と設定します。

ステップ 3 汎用の XMPP 証明書に XMPP サーバツーサーバ証明書と同じドメイン名を使用するには、[XMPP 証明書件名 CN にドメイン名を使用（Use Domain Name for XMPP Certificate Subject Common Name）] をオンにします。

ステップ 4 [保存（Save）] を選択します。

次の作業

次の手順のいずれかを使用した場合は、証明書を作成します。

- XMPP フェデレーションに自己署名証明書を使用する, （2 ページ）
- XMPP フェデレーションへの CA 署名付き証明書の使用, （3 ページ）
  トラブルシューティングのヒント
- この設定のいずれかを変更した場合は、Cisco XCP ルータ サービスを再起動する必要があります。 [Cisco Unified IM and Presence サービスアビリティ（Cisco Unified IM and Presence Serviceability）]>[ツール（Tools）]>[コントロール センタのネットワーク サービス（Control Center - Network Services）] を選択して、このサービスを再起動します。
- サーバツーサーバ ドメイン名の値を変更する場合、影響を受ける XMPP S2S 証明書を再生成してから、Cisco XCP ルータ サービスを再起動する必要があります。

XMPP フェデレーションに自己署名証明書を使用する

ここでは、XMPP フェデレーションに自己署名証明書を使用する方法について説明します。 CA 署名付き証明書の使用方法については、XMPP フェデレーションへの CA 署名付き証明書の使用, （3 ページ）を参照してください。

手順

ステップ 1 [Cisco Unified IM and Presence オペレーティング システムの管理（Cisco Unified IM and Presence Operating System Administration）] > [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 [新規作成（Generate New）] を選択します。

ステップ 3 [証明書の名前（Certificate Name）] ドロップダウン リストから [cup-xmpp-s2s] を選択し、[生成（Generate）] を選択します。

ステップ 4 Cisco XCP ルータ サービスを再起動します。 [Cisco Unified IM and Presence サービスアビリティ（Cisco Unified IM and Presence Serviceability）] > [ツール（Tools）] > [コントロール センタのネットワーク サービス（Control Center - Network Services）] を選択して、このサービスを再起動します。

ステップ 5 証明書をダウンロードして別のエンタープライズに送信して、XMPP サーバの信頼できる証明書として追加できます。 これは IM and Presence サーバまたは別の XMPP サーバにすることができます。

次の作業

XMPP フェデレーションのルート CA 証明書をインポートする，（6 ページ）

XMPP フェデレーションへの CA 署名付き証明書の使用

ここでは、CA 署名付き証明書を使用する方法について説明します。 自己署名付き証明書の使用方法については、XMPP フェデレーションに自己署名証明書を使用する，（2 ページ）を参照してください。

XMPP フェデレーションの証明書署名要求を生成する

ここでは、Microsoft Certificate Services CA の証明書署名要求（CSR）を生成する方法について説明します。

（注） この手順では Microsoft Certificate Services CA の CSR を生成しますが、任意の認証局の証明書を要求する場合は、CSR を生成する手順（手順 1 ～ 3）が適用されます。

はじめる前に

XMPP 証明書のドメインを設定します。XMPP 証明書用のドメインを設定する，（1 ページ）を参照してください。

手順

ステップ 1 IM and Presence で [Cisco Unified IM and Presence オペレーティングシステムの管理（Cisco Unified IM and Presence Operating System Administration）] > [セキュリティ（Security）] > [証明書の管理（Certificate Management）] の順に選択します。

ステップ 2 CSR を生成するには、次の手順を実行します。

a) [CSR の作成（Generate CSR）] を選択します。
b) 証明書名に [cup-xmpp-s2s] を選択します。
c) [CSR の作成（Generate CSR）] を選択します。
d) [閉じる（Close）] を選択し、メインの証明書ウィンドウに戻ります。

ステップ 3 .csr ファイルをローカル マシンにダウンロードするには：

a) [CSR のダウンロード（Download CSR）] を選択します。
b) [証明書署名要求のダウンロード(Download Certificate Signing Request)] ウィンドウのメニューで [cup-xmpp-s2s.csr] ファイルを選択します。
c) [CSR のダウンロード（Download CSR）] を選択して、そのファイルをローカル マシンにダウンロードします。

ステップ 4 テキスト エディタを使用して cup-xmpp-s2s.csr ファイルを開きます。

ステップ 5 CSR ファイルの内容をコピーします。
次の行から

- BEGIN CERTIFICATE REQUEST

次の行までの情報をすべてコピーします。

END CERTIFICATE REQUEST -

ステップ 6 インターネット ブラウザで CA サーバを参照します。次に例を示します。http://<name of your Issuing CA Server>/certsrv

ステップ 7 [証明書の要求（Request a certificate）] を選択します。

ステップ 8 [証明書の要求の詳細設定（Advanced certificate request）] を選択します。

ステップ 9 [Base 64 エンコード CMC または PKCS #10 ファイルを使用して証明書の要求を送信する（Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file）] を選択するか、Base 64 でエンコードした PKCS #7 ファイルを使用して更新の要求を送信します。

ステップ 10 手順 5 でコピーした CSR ファイルの内容を [保存した要求（Saved Request）] フィールドに貼り付けます。

ステップ 11 [送信（Submit）] を選択します。

ステップ 12 インターネット ブラウザで、次の URL に戻ります。http://<name of your Issuing CA Server>/certsrv

ステップ 13 [保留中の証明書の要求の状態（View the status of a pending certificate request）] を選択します。

ステップ 14 前の項で発行した証明書の要求をクリックします。

ステップ 15 [Base 64 エンコード（Base 64 encoded）] を選択します。

ステップ 16 [証明書のダウンロード（Download certificate）] を選択します。

ステップ 17 証明書をローカル マシンに保存します。

a) 証明書ファイル名 **cup-xmpp-s2s.pem** を指定します。

b) 証明書を**セキュリティ証明書**として保存します。

次の作業

XMPP フェデレーションの CA 署名付き証明書をアップロードする，（5 ページ）

トラブルシューティングのヒント

- この設定のいずれかを変更した場合は、Cisco XCP ルータ サービスを再起動する必要があります。 [Cisco Unified IM and Presence サービスアビリティ（Cisco Unified IM and Presence Serviceability）]>[ツール（Tools）]>[コントロール センタのネットワーク サービス（Control Center - Network Services）] を選択して、このサービスを再起動します。
- サーバツーサーバ ドメイン名の値を変更する場合、影響を受ける XMPP S2S 証明書を再生成してから、Cisco XCP ルータ サービスを再起動する必要があります。

XMPP フェデレーションの CA 署名付き証明書をアップロードする

はじめる前に

XMPP フェデレーションの証明書署名要求を生成する，（3 ページ）の手順を実行します。

手順

ステップ 1 IM and Presence で [Cisco Unified IM and Presence オペレーティングシステムの管理（Cisco Unified IM and Presence Operating System Administration）]>[セキュリティ（Security）]>[証明書の管理（Certificate Management）] の順に選択します。

ステップ 2 [証明書のアップロード（Upload Certificate）] を選択します。

ステップ 3 証明書名に [cup-xmpp-s2s] を選択します。

ステップ 4 [ルート証明書（Root Certificate）] でルート証明書の名前を指定します。

ステップ 5 [ファイルのアップロード（Upload File）] を選択します。

ステップ 6 ローカル マシンに保存した CA 署名付き証明書の場所を参照します。

ステップ 7 [ファイルのアップロード（Upload File）] を選択します。

ステップ 8 Cisco XCP ルータ サービスを再起動します。 [Cisco Unified IM and Presence サービスアビリティ（Cisco Unified IM and Presence Serviceability）]>[ツール（Tools）]>[コントロール センタのネッ

トワーク サービス（Control Center - Network Services）] を選択して、このサービスを再起動します。

次の作業

XMPP フェデレーションのルート CA 証明書をインポートする，（6 ページ）

XMPP フェデレーションのルート CA 証明書をインポートする

（注） ここでは、XMPP S2S 信頼証明書を IM and Presence に手動でアップロードする方法について説明します。 また、Certificate Import Tool を使用して、XMPP S2S 信頼証明書を自動的にアップロードすることもできます。 Certificate Import Tool にアクセスするには、[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [セキュリティ（Security）] > [Certificate Import Tool] を選択します。このツールの使用方法については、オンライン ヘルプを参照してください。

IM and Presence とエンタープライズのフェデレーションを行い、共通の信頼できる認証局（CA）がエンタープライズの証明書に署名する場合、CA のルート証明書を IM and Presence サーバにアップロードする必要があります。

共通の信頼できる CA が署名した証明書ではなく、自己署名証明書を使用するエンタープライズと IM and Presence のフェデレーションを行う場合、この手順を使用して自己署名証明書をアップロードできます。

はじめる前に

ルート CA 証明書をダウンロードし、ローカル マシンに保存します。

手順

ステップ 1 IM and Presence で [Cisco Unified IM and Presence オペレーティングシステムの管理（Cisco Unified IM and Presence Operating System Administration）] > [セキュリティ（Security）] > [証明書の管理（Certificate Management）] の順に選択します。

ステップ 2 [証明書のアップロード（Upload Certificate）] を選択します。

ステップ 3 証明書名に [cup-xmpp-trust] を選択します。

（注） ルート名のフィールドは空白のままにしておきます。

ステップ 4 [参照（Browse）] を選択し、以前にダウンロードしてローカル マシンに保存したルート CA 証明書の場所を参照します。

ステップ 5 [ファイルのアップロード（Upload File）] を選択して IM and Presence サーバに証明書をアップロードします。

（注） まだ信頼していない CA を使用する企業とのフェデレーションを新たに設定するたびに、この操作を繰り返します。 同様に、フェデレーションを新たに設定する企業が自己署名証明書を使用している場合もこの操作を行う必要があります。この場合、ルート CA 証明書の代わりに自己署名証明書がアップロードされます。

トラブルシューティングのヒント

信頼証明書が自己署名の場合、XMPP フェデレーションのセキュリティ設定ウィンドウで[クライアント側の証明書が必要（Require client side certificates）] パラメータをオンにすることはできません。