ライブ データの証明書

Finesse および Cisco Unified Intelligence Center で HTTPS を使用する場合、Finesse および Cisco Unified Intelligence Center で提供される自己署名証明書を使用して、サードパーティ ベンダーから CA 証明書を取得してインストールするか、内部で CA 証明書を作成する必要があります。 この付録の手順は、自己署名証明書を使用する方法、または CA 証明書を作成してアップロードする方法について説明します。

ライブ データの自己署名証明書の追加

Finesse および Cisco Unified Intelligence Center の両方が、自己署名証明書を使用してインストールされます。 次の手順では、これらの自己署名証明書を使用します。 ただし、自己署名証明書を使用する場合、ライブ データ ガジェットを使用する前に、エージェントはサインインの際に Finesse デスクトップの証明書を受け入れる必要があります。 この要件を回避するために、CA 証明書を提供できます。 サードパーティ証明書のベンダーから CA 証明書を取得するか、組織に対して内部で CA 証明書を作成できます。

手順

ステップ 1 Cisco Unified Intelligence Center の Cisco Unified Operating System Administration にサインインします（http://*Cisco Unified Intelligence Center* サーバのホスト名/cmplatform）。

ステップ 2 [セキュリティ（Security）] メニューから、[証明書の管理（Certificate Management）] を選択します。

ステップ 3 [検索（Find）] をクリックします。

ステップ 4 [tomcat.pem] をクリックします。
tomcat.pem がリストにない場合は、[新規作成（Generate New）] をクリックして、[証明書の名前（Certificate Name）] ドロップダウン リストから [tomcat] を選択します。

ステップ 5 [ダウンロード（Download）] をクリックして、デスクトップにファイルを保存します。
Cisco Unified Intelligence Center パブリッシャと Cisco Unified Intelligence Center サブスクライバのホスト名を含む証明書をダウンロードする必要があります。

ステップ 6 プライマリ Finesse サーバの Cisco Unified Operating System Administration にサインインします（http://*Finesse* サーバのホスト名/cmplatform）。

ステップ 7 [セキュリティ（Security）] メニューから、[証明書の管理（Certificate Management）] を選択します。

ステップ 8 [証明書のアップロード（Upload Certificate）] をクリックします。

ステップ 9 [証明書の名前（Certificate Name）] ドロップダウン リストから、[tomcat-trust] を選択します。

ステップ 10 [Choose file] をクリックして、tomcat.pem ファイル（Cisco Unified Intelligence Center のパブリッシャとサブスクライバの証明書）のロケーションを参照してください。

ステップ 11 [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 12 Cisco Tomcat を再起動します。

ライブ データの CA 証明書の取得およびアップロード

Cisco Unified Intelligence Center パブリッシャ サーバおよび Finesse プライマリ サーバの両方で、次の手順を実行する必要があります。 Cisco Unified Communications オペレーティング システムの管理から Certificate Management ユーティリティを使用します。

[Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] を開いて、ブラウザに次の URL を入力します。

https://*Finesse* または *Cisco Unified Intelligence Center* サーバのホスト名/cmplatform

手順

ステップ 1 CSR を作成します。

a) [セキュリティ（Security）] > [証明書の管理（Certificate Management）] > [CSR の作成（Generate CSR）] を選択します。
b) [証明書の名前（Certificate Name）] ドロップダウン リストで、[tomcat] を選択します。
c) [CSR の作成（Generate CSR）] をクリックします。

ステップ 2 CSR をダウンロードします。
a) [セキュリティ（Security）] > [証明書の管理（Certificate Management）] > [CSR のダウンロード（Download CSR）] を選択します。
b) [証明書の名前（Certificate Name）] ドロップダウン リストで、[tomcat] を選択します。
c) [CSR のダウンロード（Download CSR）] をクリックします。

ステップ 3 CSR を使用して、認証局から署名付きアプリケーション証明書と CA ルート証明書を取得します。

ステップ 4 証明書を受け取ったら、[セキュリティ（Security）]> [証明書の管理（Certificate Management）] > [証明書のアップロード（Upload Certificate）] を選択します。

ステップ 5 ルート証明書をアップロードします。
a) [証明書の名前（Certificate Name）] ドロップダウン リストから、[tomcat-trust] を選択します。
b) [ファイルのアップロード（Upload File）] フィールドで、[参照（Browse）] をクリックして、ルート証明書ファイルを参照してください。
c) [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 6 アプリケーション証明書をアップロードします。
a) [証明書の名前（Certificate Name）] ドロップダウン リストで、[tomcat] を選択します。
b) [ルート証明書（Root Certificate）] フィールドに、CA ルート証明書の名前を入力します。
c) [ファイルのアップロード（Upload File）] フィールドで、[参照（Browse）] をクリックして、アプリケーションの証明書ファイルを参照してください。
d) [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 アップロードが完了したら、プライマリ Finesse サーバの CLI にアクセスします。

ステップ 8 **utils service restart Cisco Finesse Notification Service** コマンドを入力して、Cisco Finesse Notification サービスを再起動します。

ステップ 9 コマンド **utils service restart Cisco Tomcat** を入力して、Cisco Tomcat サービスを再起動します。

ステップ 10 ルート証明書とアプリケーション証明書を Cisco Unified Intelligence Center パブリッシャ サーバにアップロードします。

ステップ 11 アップロードが完了したら、Cisco Unified Intelligence Center サーバの CLI にアクセスします。

ステップ 12 **utils service restart Intelligence Center Openfire Service** コマンドを入力して、Intelligence Center Openfire サービスを再起動します。

ステップ 13 **utils service restart Intelligence Center Reporting Service** コマンドを入力して、Intelligence Center Reporting サービスを再起動します。

内部的な証明書の作成

Microsoft Certificate Server のセットアップ

この手順では、展開に Windows Server 2008 Active Directory サーバが使用されていることを前提とします。 Windows 2008 ドメイン コントローラの Active Directory 証明書サービスの役割を追加するには、次の手順を実行します。

手順

ステップ 1 [スタート（Start）] をクリックし、[コンピュータ（Computer）] を右クリックして、[管理（Manage）] を選択します。

ステップ 2 左側のペインで、[役割（Roles）] をクリックします。

ステップ 3 右側のペインで、[役割の追加（Add Roles）] をクリックします。
[役割の追加（Add Roles）] ウィザードが開きます。

ステップ 4 [サーバの役割の選択（Select Server Roles）] 画面で、[Active Directory 証明書サービス（Active Directory Certificate Services）] チェックボックスをオンにして [次へ（Next）] を選択します。

ステップ 5 [Active Directory 証明書サービスについて（Introduction to Active Directory Certificate Services）] 画面で、[次へ（Next）] をクリックします。

ステップ 6 [役割サービスの選択（Select Role Services）] 画面で、[認証局（Certification Authority）] チェックボックスをオンにして、[次へ（Next）] をクリックします。

ステップ 7 [セットアップの種類の指定（Specify Setup Type）] 画面で、[エンタープライズ（Enterprise）] を選択し、[次へ（Next）] をクリックします。

ステップ 8 [CA の種類の指定（Specify CA Type）] 画面で、[ルート CA（Root CA）] を選択し、[次へ（Next）] をクリックします。

ステップ 9 [公開キーのセットアップ（Set Up Private Key）]、[CA の暗号化を設定（Configure Cryptography for CA）]、[CA 名の設定（Configure CA Name）]、[有効期間を設定（Set Validity Period）]、および [証明書データベースの設定（Configure Certificate Database）] 画面で [次へ（Next）] をクリックして、デフォルトの値を受け入れます。

ステップ 10 [インストール時の選択を確認（Confirm Installations Selections）] 画面で、情報を確認し、[インストール（Install）] をクリックします。

CA 証明書のダウンロード

この手順は、Windows 証明書サービスを使用していることを前提としています。 次の手順を実行して、認証局からルート CA 証明書を取得します。 ルート証明書を取得した後、各ユーザは Finesse にアクセスするために使用するブラウザにインストールする必要があります。

手順

ステップ 1 Windows 2008 ドメイン コントローラで、CLI コマンド **ca.cert certutil - ca_name.cer** を実行します。

ステップ 2 ファイルを保存します。 後で検索できるように、ファイルを保存した場所のメモを残しておきます。

Internet Explorer のルート証明書の導入

グループ ポリシーが Active Directory ドメインによって適用されている環境では、ルート証明書を各ユーザの Internet Explorer に自動的に追加できます。 証明書を自動的に追加すると、設定に関するユーザ要求が簡略化されます。

（注） 証明書の警告を回避するために、各ユーザは Finesse サーバの完全修飾ドメイン名（FQDN）を使用してデスクトップにアクセスする必要があります。

手順

ステップ 1 Windows 2008 ドメイン コントローラで、[スタート（Start）] > [管理ツール（Administrative Tools）] > [グループ ポリシーの管理（Group Policy Management）] をクリックします。

ステップ 2 [デフォルトのドメイン ポリシー（Default Domain Policy）] を右クリックし、[編集（Edit）] を選択します。

ステップ 3 [グループ ポリシー管理コンソール（Group Policy Management Console）] で、[コンピュータ設定（Computer Configuration）] > [ポリシー（Policies）] > [ウィンドウの設定（Window Settings）] > [セキュリティ設定（Security Settings）] > [公開キー ポリシー（Public Key Policies）] に進みます。

ステップ 4 [信頼されたルート証明機関（Trusted Root Certification Authorities）] を右クリックし、[インポート（Import）] を選択します。

ステップ 5 ca_name.cer ファイルをインポートします。

ステップ 6 [コンピュータ設定（Computer Configuration）] > [ポリシー（Policies）] > [Windows 設定（Windows Settings）] > [セキュリティ設定（Security Settings）] > [公開キー ポリシー（Public Key Policies）] > [証明書サービス クライアント - 自動登録（Certificate Services Client - Auto-Enrollment）] に進みます。

ステップ 7 [設定モデル（Configuration Model）] リストから、[有効（Enabled）] を選択します。

ステップ 8 ドメインに含まれるコンピュータにユーザとしてサインインし、Internet Explorer を開きます。

ステップ 9 ユーザが証明書を持っていない場合は、ユーザのコンピュータ上で **gpupdate.exe/target:computer /force** コマンドを実行します。

Internet Explorer ブラウザの証明書のセットアップ

CA 証明書を取得してアップロードした後、すべてのユーザが証明書を受け入れるか、証明書がグループ ポリシーによって自動的にインストールされる必要があります。

ユーザがドメインに直接ログインしていないか、グループ ポリシーが使用されていない環境では、証明書を受け入れたら、システム内の Internet Explorer のすべてのユーザが次の手順を実行する必要があります。

手順

ステップ 1 Windows Explorer で、ca_name.cer ファイルをダブルクリックし、[開く（Open）] をクリックします。

ステップ 2 [Install Certificate] > [Next] > [Place all certificates in the following store] をクリックします。

ステップ 3 [参照（Browse）] をクリックし、[信頼されたルート証明機関（Trusted Root Certification Authorities）] を選択します。

ステップ 4 [OK] をクリックします。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [終了（Finish）] をクリックします。
認証局（CA）から証明書をインストールしようとしていることを示すメッセージが表示されます。

ステップ 7 [はい（Yes）] をクリックします。
インポートが正常に実行されたことを示すメッセージが表示されます。

ステップ 8 証明書がインストールされたことを確認するには、Internet Explorer を開きます。 ブラウザのメニューから、[ツール（Tools）]>[インターネット オプション（Internet Options）] を選択します。

ステップ 9 [コンテンツ（Content）] タブをクリックします。

ステップ 10 [証明書（Certificates）] をクリックします。

ステップ 11 [信頼されたルート証明機関（Trusted Root Certification Authorities）] タブをクリックします。

ステップ 12 新しい証明書がリストに表示されていることを確認します。

Firefox ブラウザの証明書のセットアップ

システム上の Firefox のすべてのユーザは、次の手順を一度実行して、証明書を受け入れる必要があります。

（注） 証明書の警告を回避するために、各ユーザは Finesse サーバの完全修飾ドメイン名（FQDN）を使用してデスクトップにアクセスする必要があります。

手順

ステップ 1 Firefox のブラウザ メニューの [オプション（Options）] を選択します。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [証明書（Certificates）] タブをクリックします。

ステップ 4 [証明書を表示（View Certificate）] をクリックします。

ステップ 5 [インポート（Import）] をクリックして、ca_name.cer ファイルを参照します。