FinesseとCTIサーバ間のセキュアな通信の設定

内容

概要

このドキュメントでは、Cisco Contact Center Enterprise(CCE)ソリューションのCisco FinesseとComputer Telephony Integration(CTI) Server間に認証局(CA)署名付き証明書を実装する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- CCEリリース12.0(1)
- Finesseリリース12.0(1)
- CTI サーバ

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Packaged CCE(PCCE)12.0(1)
- Finesse 12.0(1)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

CCEバージョン11.5で、シスコはTransport Layer Security(TLS)バージョン1.2のサポートを開始しました。これにより、Session Initiation Protocol(SIP)およびReal-time Transport Protocol(RTP)メッセージをTLS 1.2経由でで安全にににできます。シスコは、コンタクトセンターのほとんどのコールフローでTLS 1.2のサポートを開始しました。インバウンドおよびアウトバウンド音声、マルチチャネル、および外部データベースdip。このドキュメントでは、インバウンド音声、特にFinesseとCTIサーバ間の通信に焦点を当てています。

CTIサーバは、次の接続モードをサポートしています。

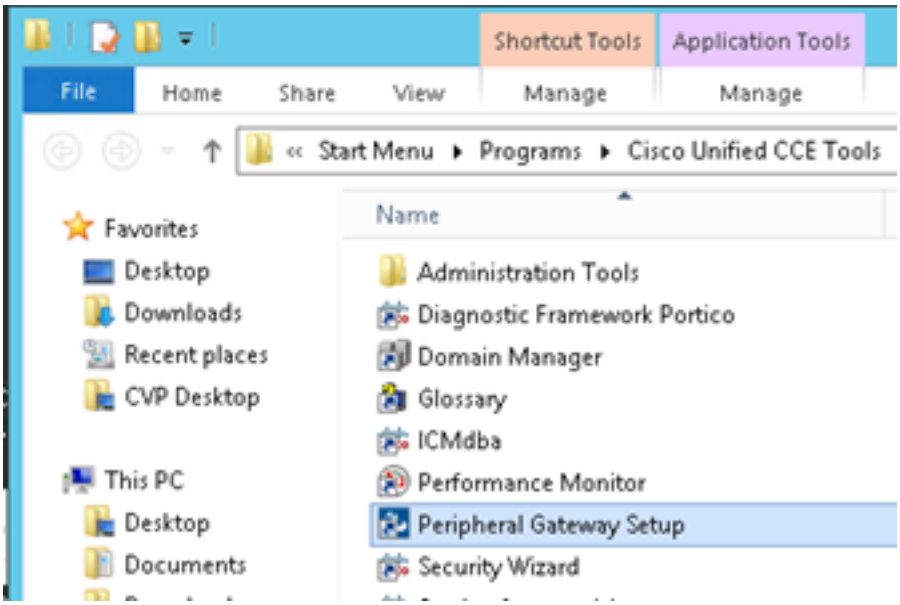
- **セキュリティで保護された専用接続**:CTIサーバとCTIクライアント（Finesse、ダイヤラ、CTIOS、およびctitest）間のセキュアな接続を許可します。
- **セキュア接続と非セキュア接続（混合モード）**:CTIサーバとCTIクライアント間のセキュアでない接続だけでなく、セキュリティ保護も可能です。これはデフォルトの接続モードです。このモードは、以前のリリースをCCE 12.0(1)にアップグレードするときに設定されます。

  注：非セキュア専用モードはサポートされていません。

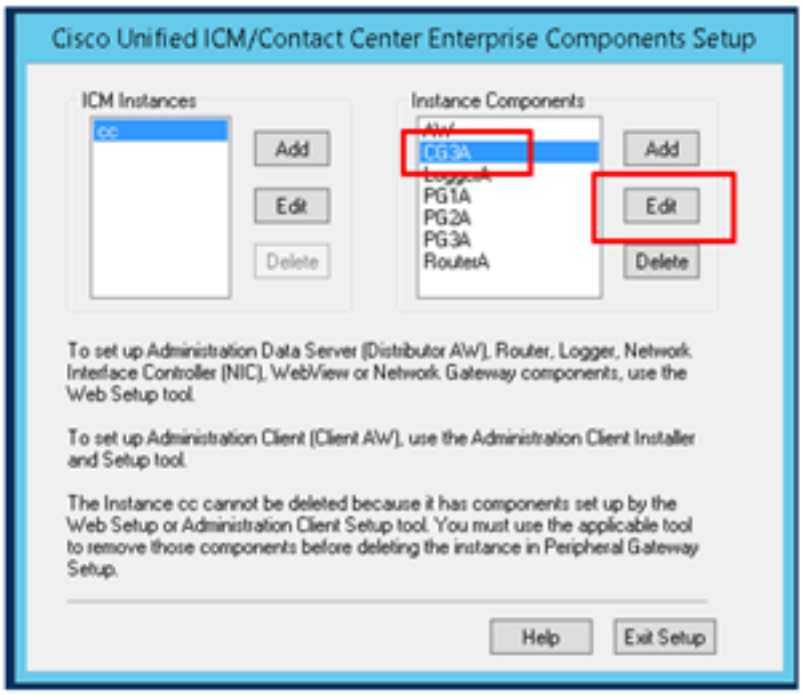
設定

CCE CTIサーバセキュア

ステップ1:PCCEアドミニストレーティブワークステーション(AW)で、**Unified CCE Toolsフォルダを開き、Peripheral Gateway Setup**をダブルクリックします。

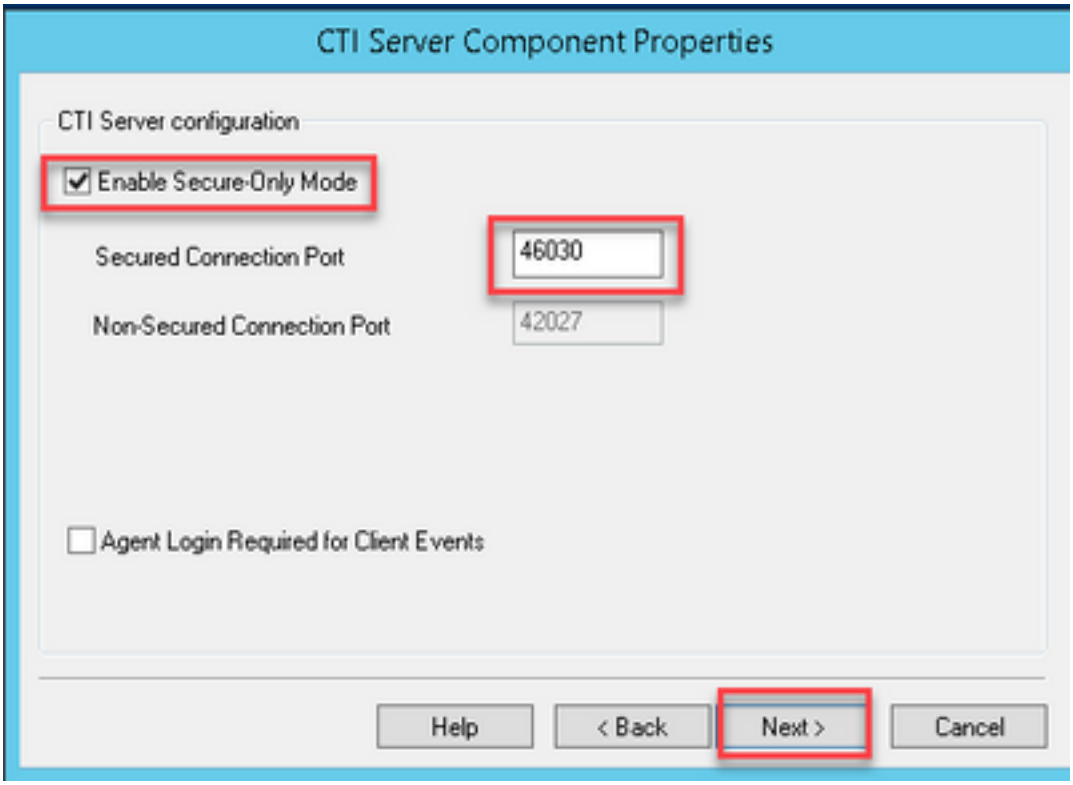


ステップ2:CG3Aを選択し、Editをクリックします。



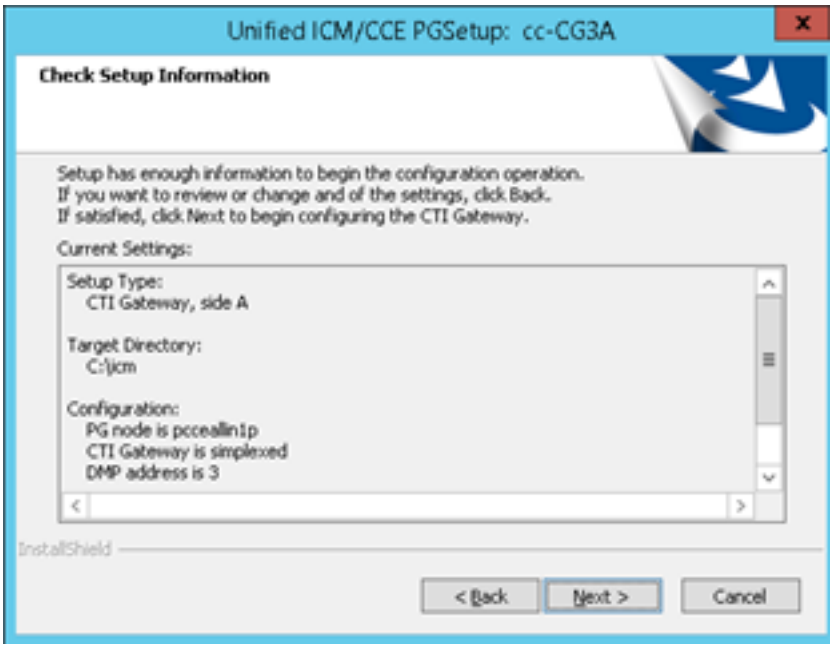
ステップ3:CTIサーバのプロパティで、[Next]をクリックします。CG3Aサービスの停止に関するセットアップに関する質問で、[はい]を選択します。

ステップ4:[CTI Server Components Properties]で、[Enable Secured-only mode]を選択します。次の演習では、Finesseで同じポートを設定する必要があるため、[Secured Connection Port (46030)]に注意してください。[next] をクリックします。

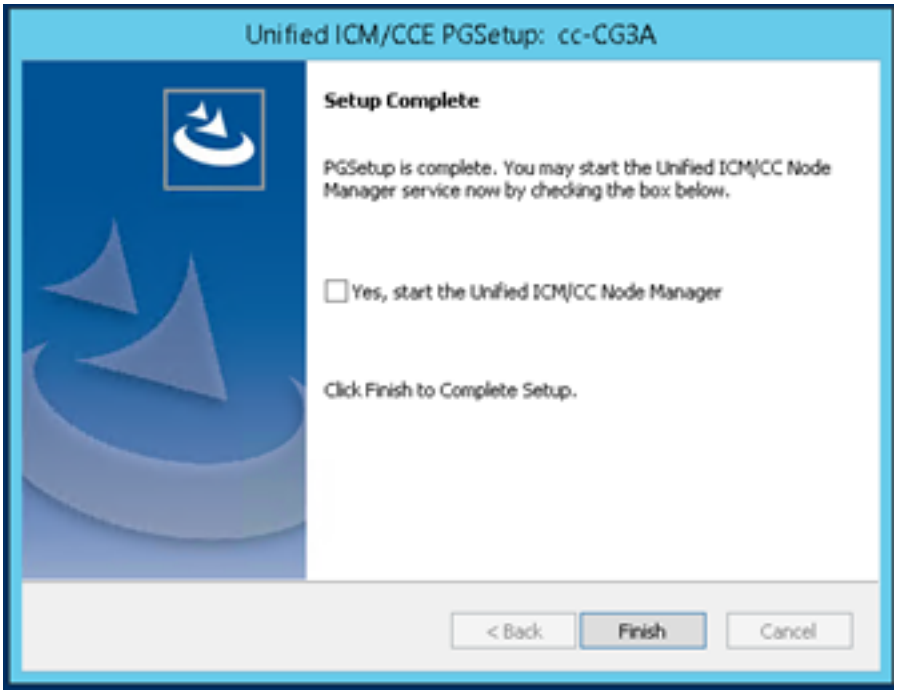


注：デフォルトのセキュアな通信は42030ですが、このドキュメントで使用する実習は40630です。ポート番号は、ICMシステムIDを含む式の一部です。システムIDが1(CG1a)の場合、デフォルトのポート番号は通常42030です。ラボのシステムIDが3(CG3a)であるため、デフォルトのポート番号は46030です。

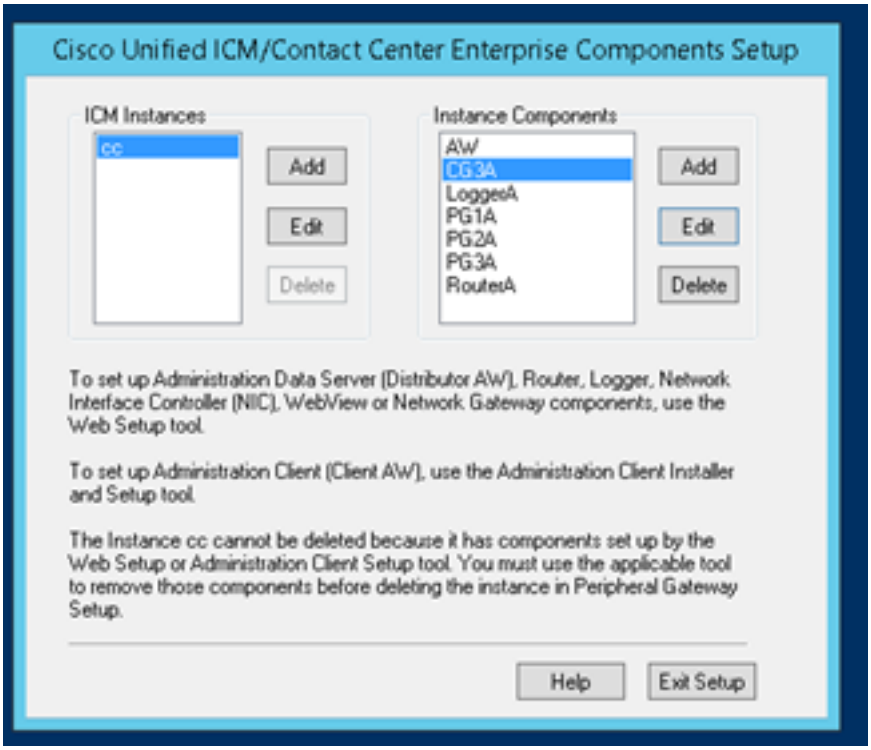
ステップ5:[CTI Network **Interface Properties]で**[Next]をクリック**します。**[Setup Information]をオン**にして、[Next]**をクリック**します。**



ステップ6：図に示すように、[Finish]をクリックします。



ステップ7:[Exit Setup]をクリックし、図に示すようにセットアップウィンドウが閉じるまで待ちます。



ステップ8:PCCEAllin1デスクトップで、[**Unified CCE service Control**]をダブル**クリックします。**

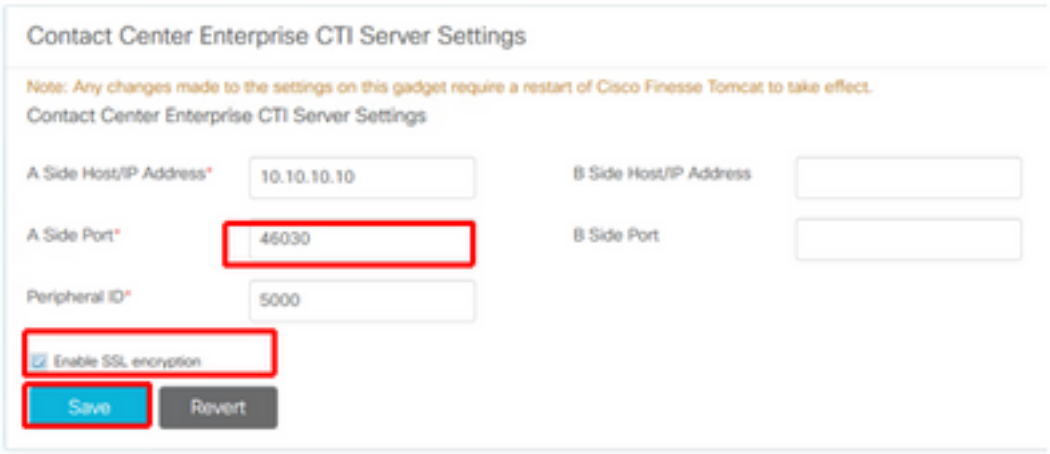
ステップ9:[Cisco ICM cc CG3A]を選択し、[Start]をクリ**ックします。**

Finesseセキュア設定

ステップ1:Webブラウザを開き、[**Finesse** Administration]に移動**します。**

ステップ2：図に示すように、[**Contact Center Enterprise CTI Server Settings**]**セクションまで下**にスクロールします。

ステップ3：前の演習でCG3Aに設定したセキュア通信ポートのA側ポートを変更します。
46030.「Enable SSL encryption」にチェックを入れ、「Save」をクリックします。



注： 接続をテストするには、まずFinesse Tomcat Serviceを再起動するか、Finesseサーバを再起動する必要があります。

ステップ4:[Finesse Administration]ページからログアウトします。

ステップ5:FinesseでSSHセッションを開きます。

ステップ6:FINESSEA SSHセッションで、次のコマンドを実行します。

utils system restart

システムを**再起動**するかどうかを確認するメッセージが表示されたら、yesと入力します。

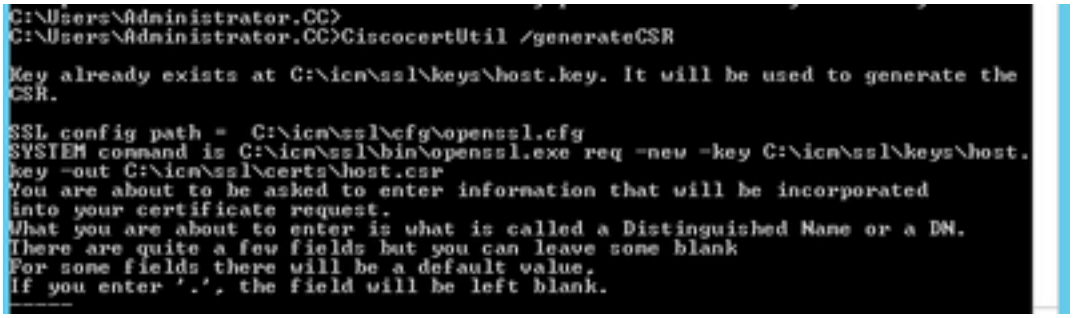
```
Using username "administrator".
Command Line Interface is starting up, please wait ...

   Welcome to the Platform Command Line Interface

VMware Installation:
        2 vCPU: Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz
        Disk 1: 146GB, Partitions aligned
        8192 Mbytes RAM

admin:utils system restart

Do you really want to restart ?

Enter (yes/no)? yes


 Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...
```

エージェントPG証明書の生成（CTIサーバ）

CiscoCertUtilsは、CCEバージョン12でリリースされた新しいツールです。このツールを使用して、着信音声のすべてのCCE証明書を管理します。このドキュメントでは、次のCiscoCertUtilsを使

用して、ペリフェラルゲートウェイ(PG)証明書署名要求(CSR)を生成します。

ステップ1：次のコマンドを実行して、CSR証明書を生成します。CiscocertUtil /generateCSR



次のように、要求された情報を入力します。

国名：JP

都道府県：MA

局所名：BXB

組織名：『シスコ

組織単位：CX

一般名：PCCEAllin1.cc.lab

[Email]：jdoe@cc.lab

チャレンジパスワード：トレイン1ng!

オプションの会社名：『シスコ

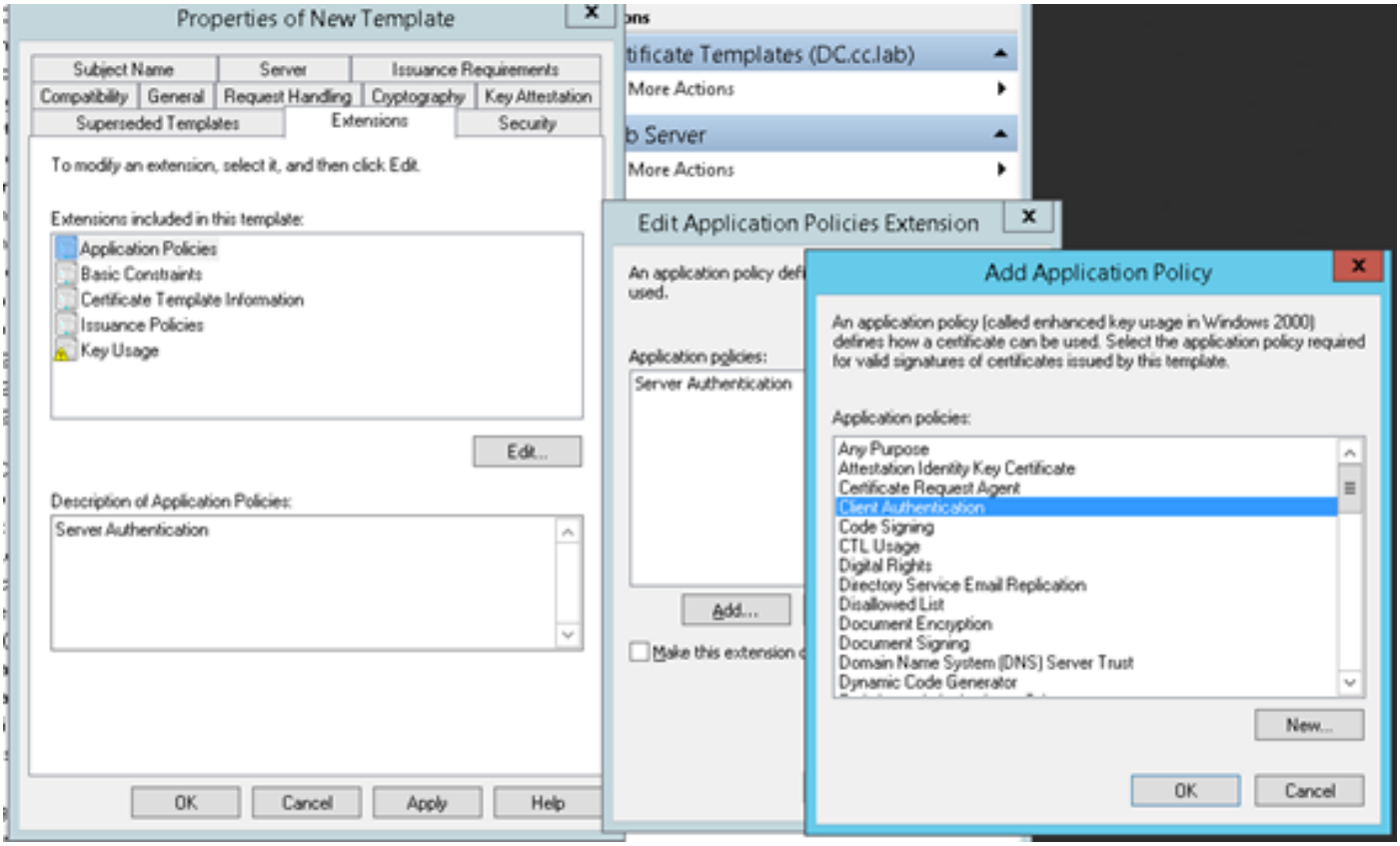
ホスト証明書とキーは、C:\icm\ssl\certsおよびC:\icm\ssl\keysに保存されます。

ステップ2: C:\icm\ssl\certsフォルダに移動し、host.csrファイルが生成されていることを確認します。

CSR証明書の取得 CAによる署名

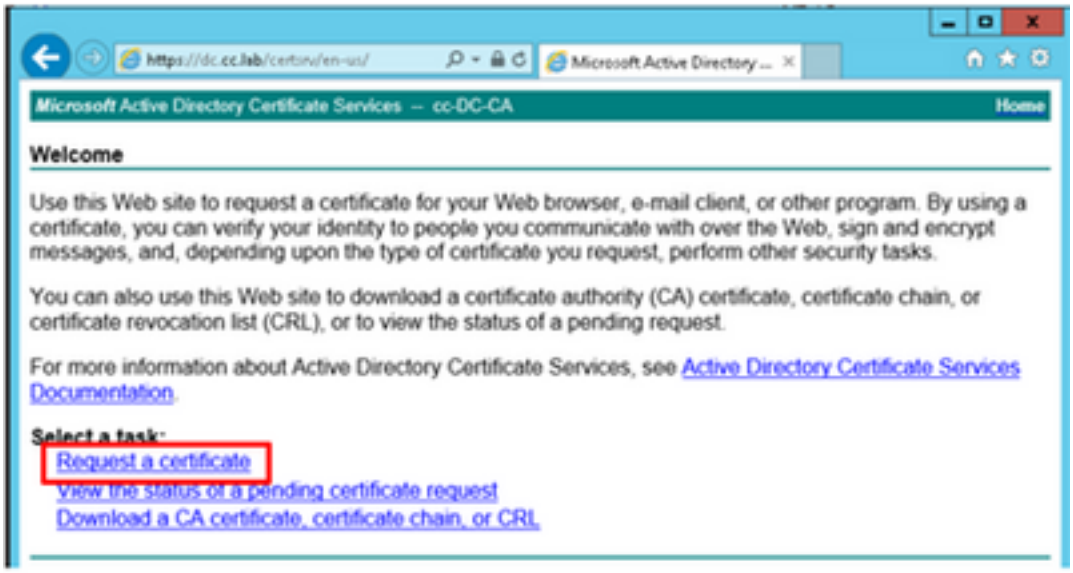
CSR証明書を生成したら、サードパーティCAによって署名される必要があります。この演習では、ドメインコントローラにインストールされたMicrosoft CAをサードパーティCAとして使用します。

Microsoft CAを使用する場合は、図に示すように、CAによって使用される証明書テンプレートにクライアント認証とサーバ認証が含まれていることを確認します。

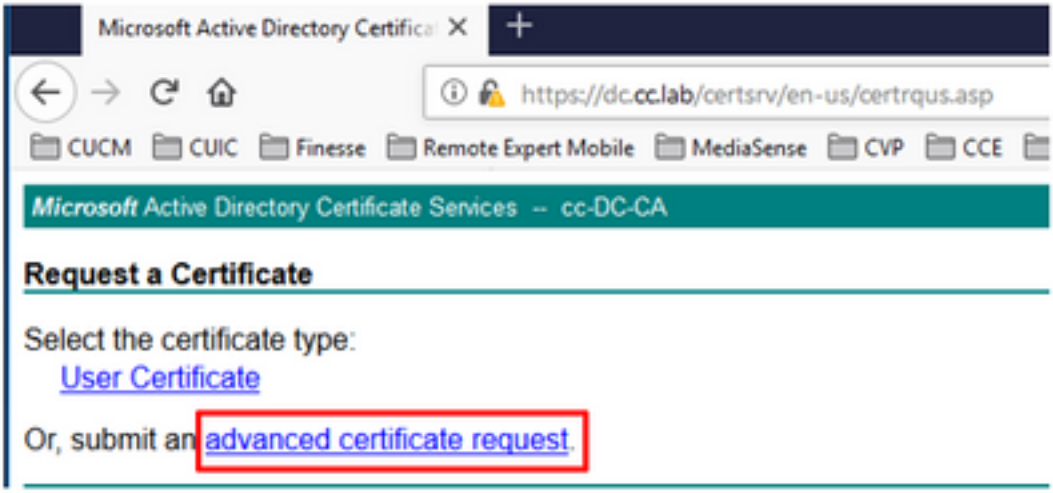


ステップ1:Webブラウザを開き、CAに移動します。

ステップ2:[Microsoft Active Directory Certificate Services]で、[Request a certificate]を選択します。

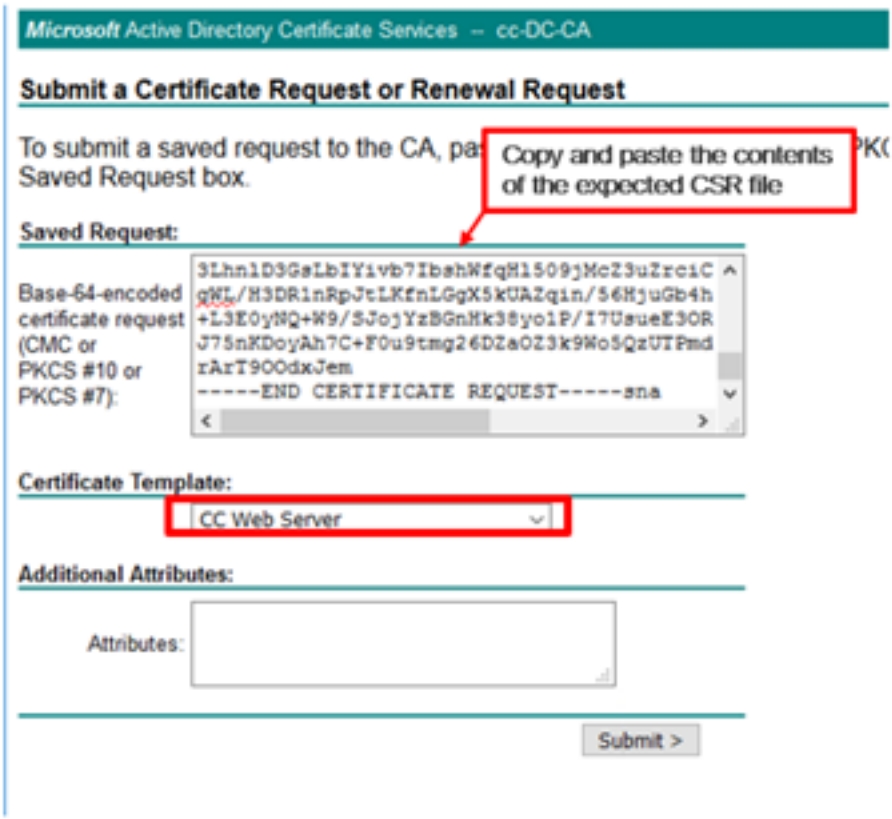


ステップ3：拡張証明書要求オプションを選択します。



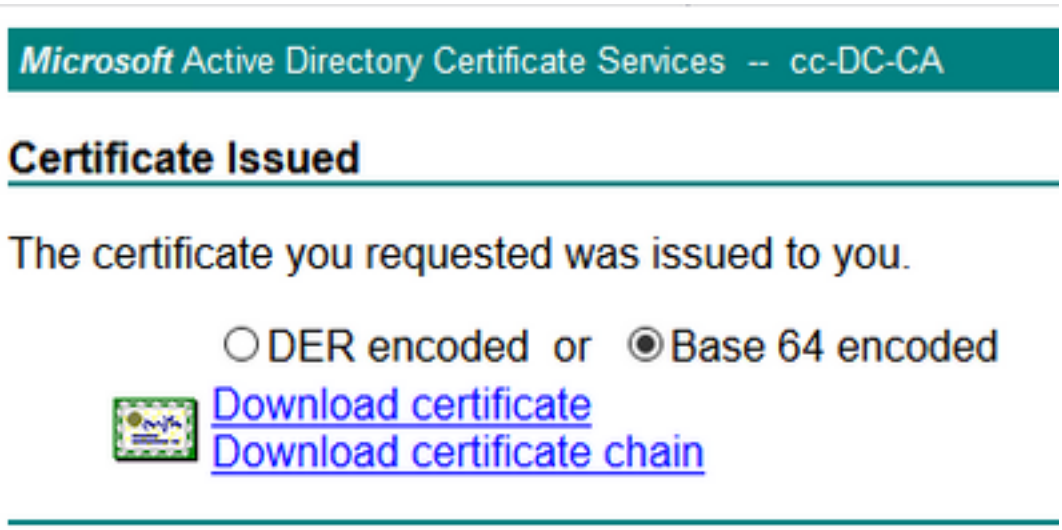
ステップ4：高度な証明書要求で、PG Agent CSR証明書の内容をコピーし、[Saved Request]ボックスに貼り付けます。

ステップ5：クライアントおよびサーバ認証を使用したWebサーバテンプレートを選択します。ラボでは、CC Webサーバテンプレートがクライアントとサーバの認証で作成されました。



ステップ6:[Submit]をクリックします。

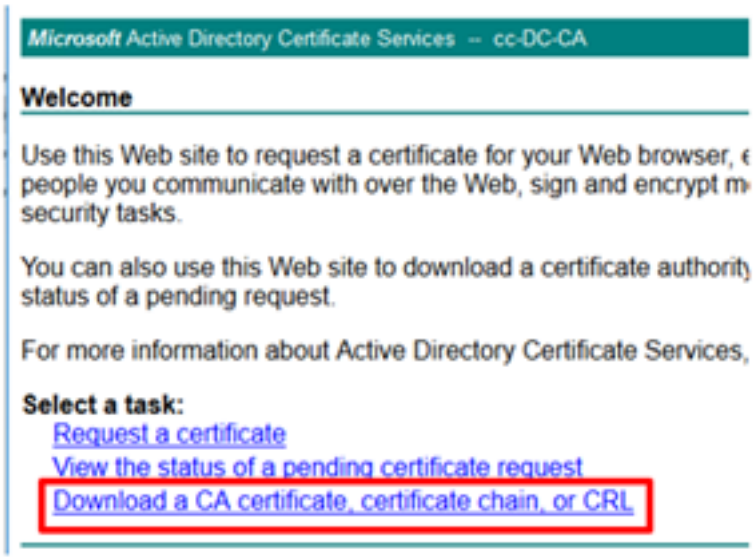
ステップ7:[Base 64 encoded]を選択し、図に示すように[Download Certificate]をクリックします。



ステップ8：ファイルを保存し、[OK]をクリックします。ファイルはDownloadsフォルダに保存されます。

ステップ9：ファイルの名前をhost.cerに変更します(オプション)。

ステップ10：ルート証明書も生成する必要があります。CA証明書ページに戻り、[Download a CA certificate, certificate chain, or CRL]を選択します。ルート証明書はすべてのサーバ（PG工ージェントとFinesse）で同じになるため、この手順を1回だけ実行する必要があります。



ステップ11:[Base 64]をクリックし、[Download CA certificate]を選択します。

ステップ12:[Save File]をクリックし、[OK]を選**択します**。ファイルはデフォルトの場所であるダウンロードに保存されます。

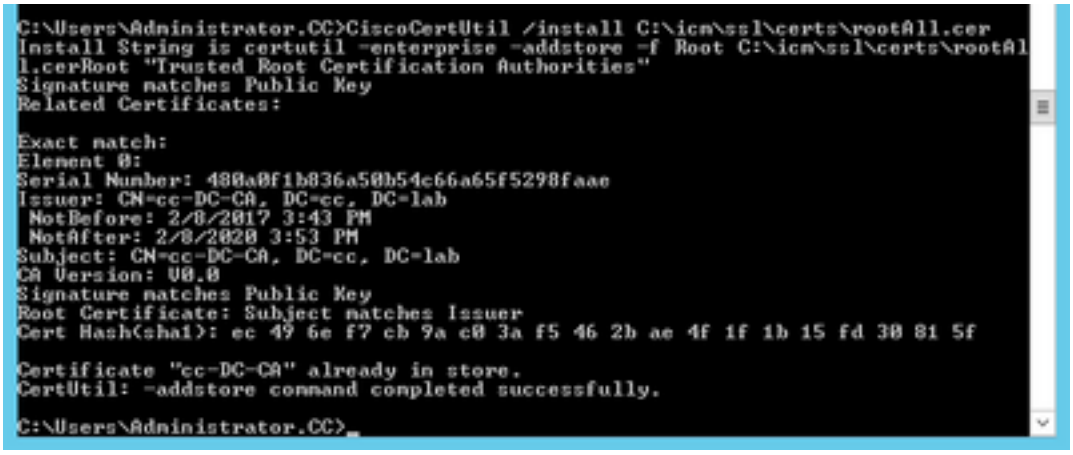
CCE PGのCA署名付き証明書のインポート

ステップ1:PGエージェントでC:\icm\ssl\certsに移動し、ルートとPGエージェントの署名**されたファ**イルをここに貼り付けます。

ステップ2:**c:\icm\ssl\certs** のhost.pem証明書の名前を**selfhost.pem**に変更します。

ステップ3:**c:\icm\ssl\certs** フォルダでhost.cerの名前をhost.pemに変更します。

ステップ4：ルート証明書をインストールします。コマンドプロンプトで、**CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer**



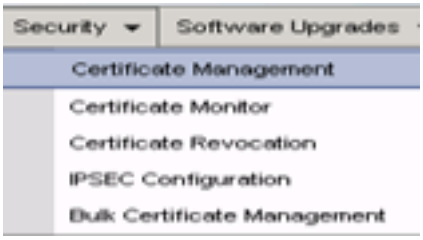
ステップ 5： 同じコマンドを実行するアプリケーション署名付き証明書をインストールします。**CiscoCertUtil /install C:\icm\ssl\certs\host.pem**

ステップ6:PGを再起動します。Unified CCE Service Controlを開き、Cisco ICM Agent PGを再起動します。

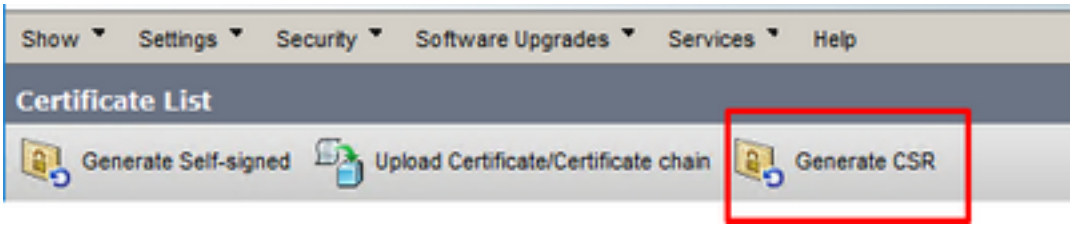
Finesse証明書の生成

ステップ1:Webブラウザを開き、[Finesse OS Admin]に移動します。

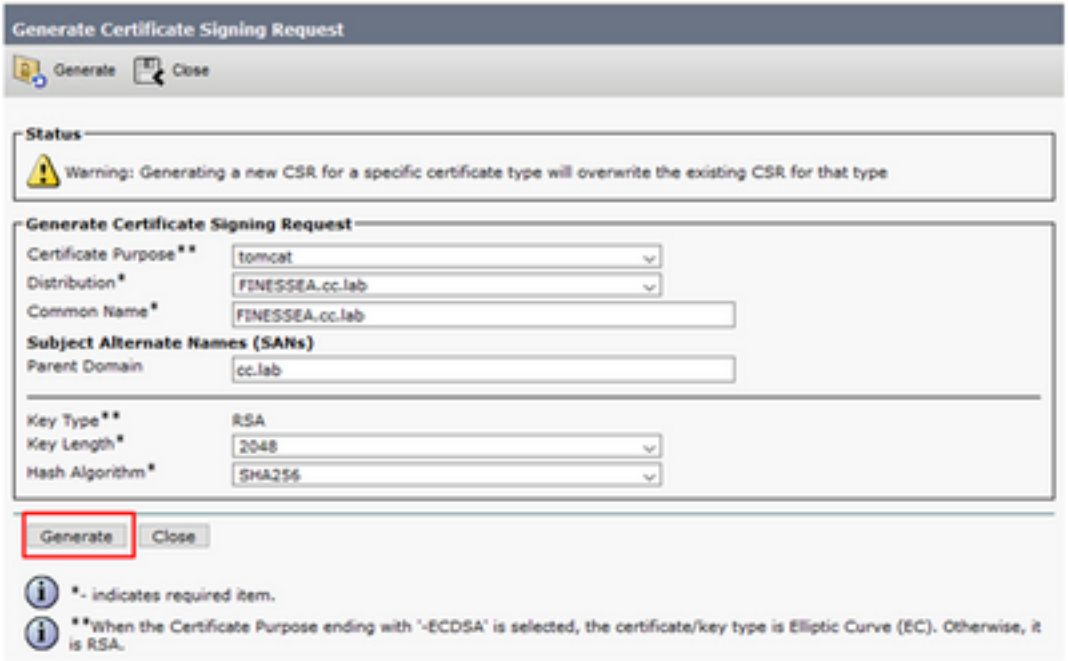
ステップ2:OS管理者クレデンシャルでログインし、図に示すように[Security] > [Certificate Management]に移動します。



ステップ3：図に示すように、[Generate CSR]をクリックします。

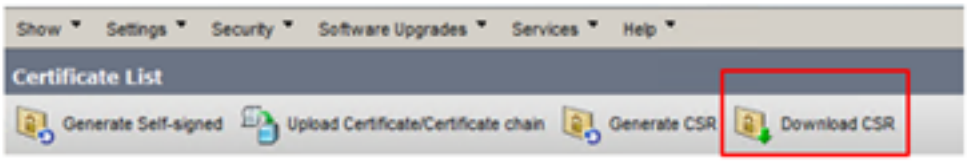


ステップ4:[Generate Certificate Signing Request]で、デフォルト値を使用し、[Generate]をクリックします。

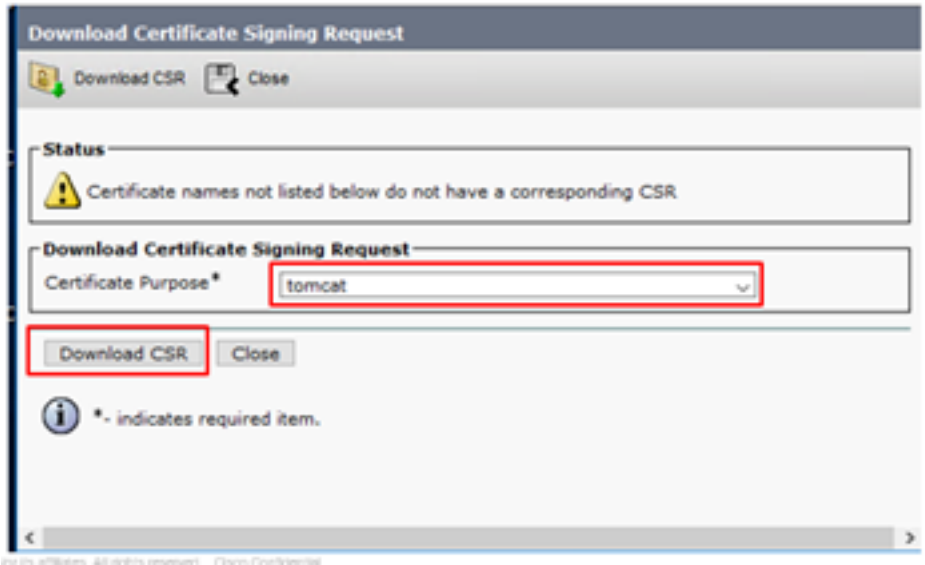


ステップ5:[Generate Certificate Signing Request]ウィンドウを閉じて、[Download CSR]を選択し

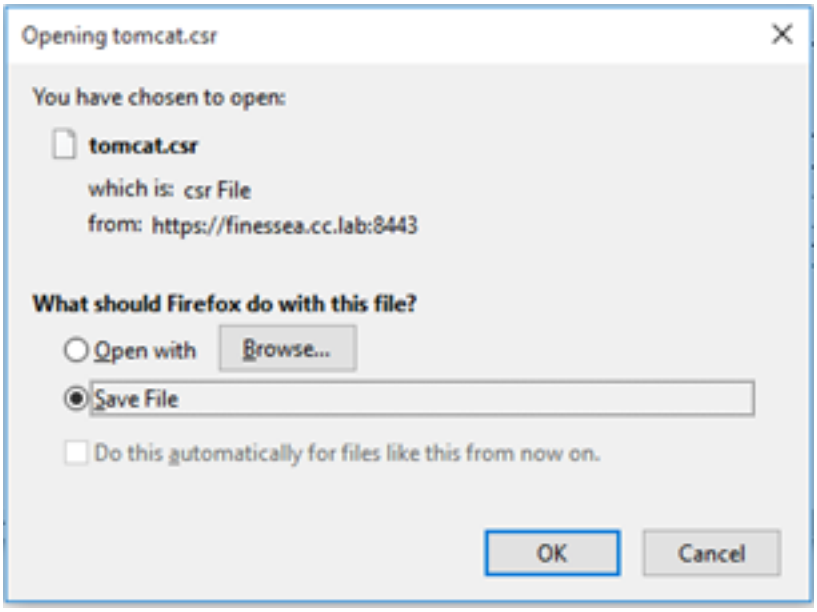
ます。



ステップ6:[Certificate Purpose]で[tomcat]を選択し、[**Download CSR**]をクリックします。



ステップ7：図に示すように、[**Save File**]を選択して[OK]をクリックします。



ステップ8:[Download **Certificate Signing Request]ウィンドウを閉**じます。証明書は既定の場所に保存されます([このPC] > [ダウンロード])。

ステップ9：エクスプローラを開き、そのフォルダに移動します。この証明書を右クリックし、名前を変更します。**finessetomcat.csr**

CAによるFinesse証明書の署名

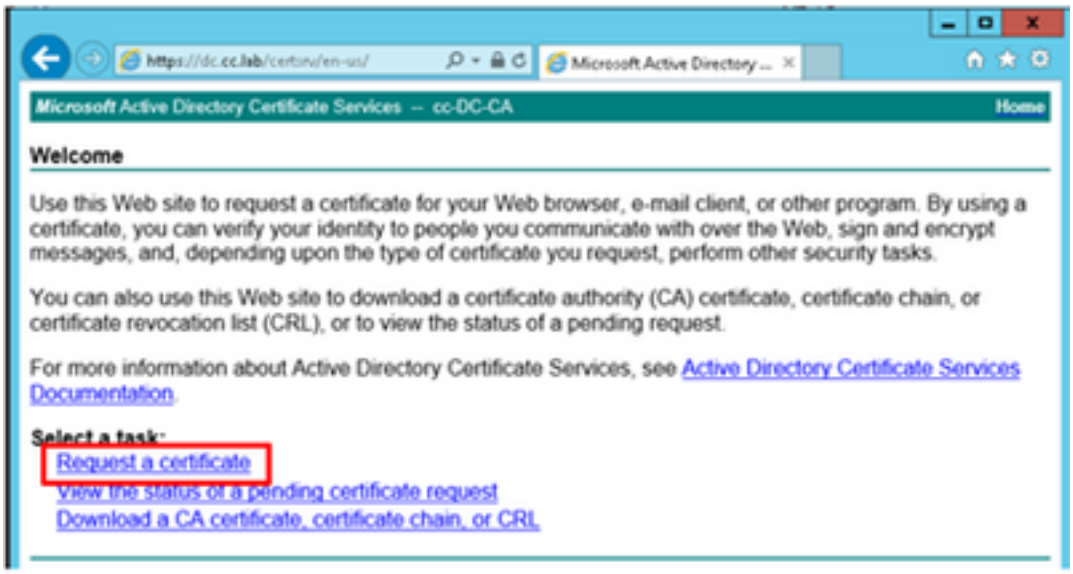
このセクションでは、前の手順で使用したのと同じMicrosoft CAがサードパーティCAとして使用

されます。

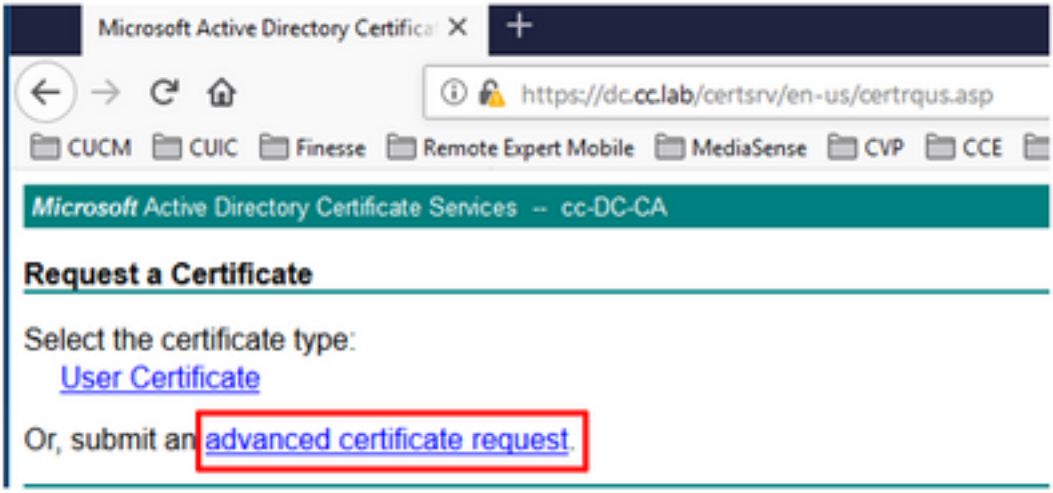
> **注：** CAによって使用される証明書テンプレートに、クライアント認証とサーバ認証が含まれていることを確認します。

ステップ1:Webブラウザを開き、CAに移動します。

ステップ2:[Microsoft Active Directory Certificate Services]で、[Request a certificate]を選択します。

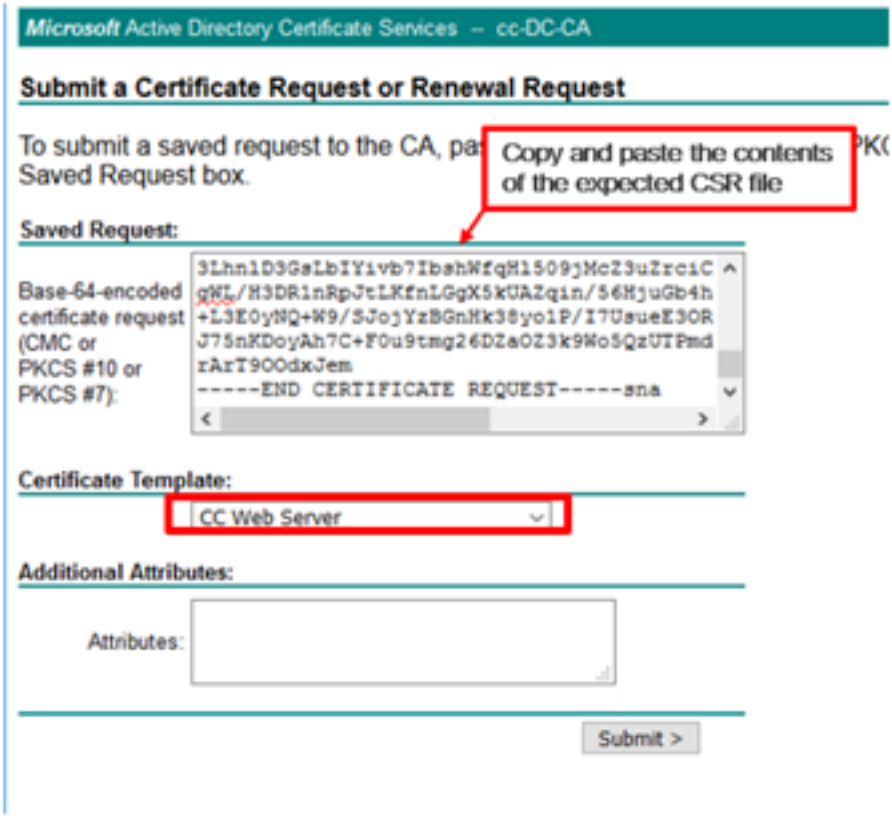


ステップ3：図に示すように、advanced certificate requestオプションを選択します。



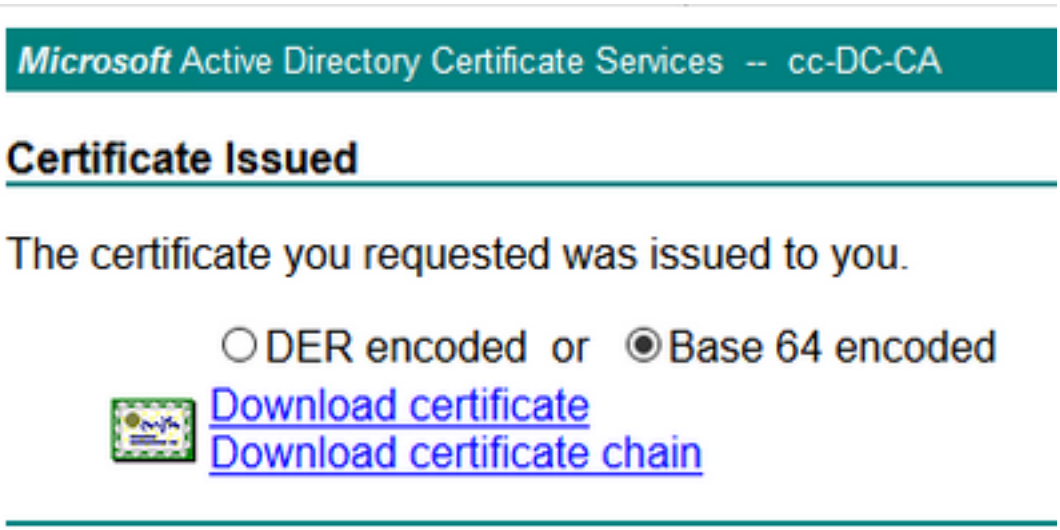
ステップ4：高度な証明書要求で、Finesse CSR証明書の内容を[Saved Request]ボックスにコピーアンドペーストします。

ステップ5：クライアントおよびサーバ認証を使用するWebサーバテンプレートを選択します。この実習では、CC Webサーバテンプレートはクライアントとサーバの認証で作成されました。



ステップ6:[Submit]をクリックします。

ステップ7:[Base 64 encoded]を選択し、図に示すように[Download certificate]をクリックします。



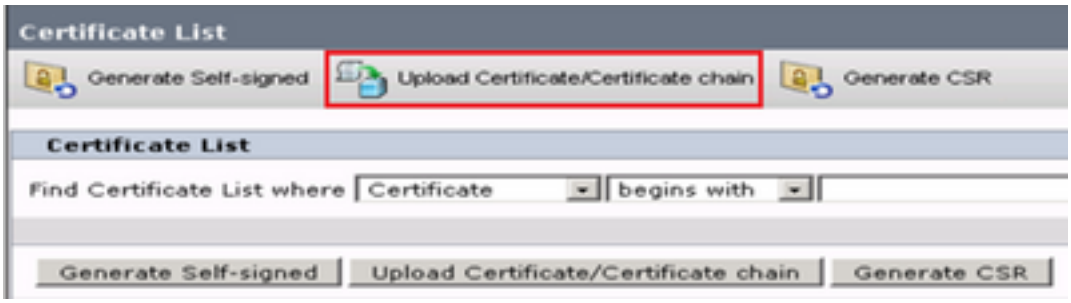
ステップ8：ファイルを保存し、[OK]をクリックします。ファイルはDownloadsフォルダに保存されます。

ステップ9：ファイル名をfinesse.cerに変更します。

Finesseアプリケーションおよびルート署名証明書のインポート

ステップ1:WebブラウザでFinesse OS Adminページを開き、[Security] > [Certificate Management]に移動します。

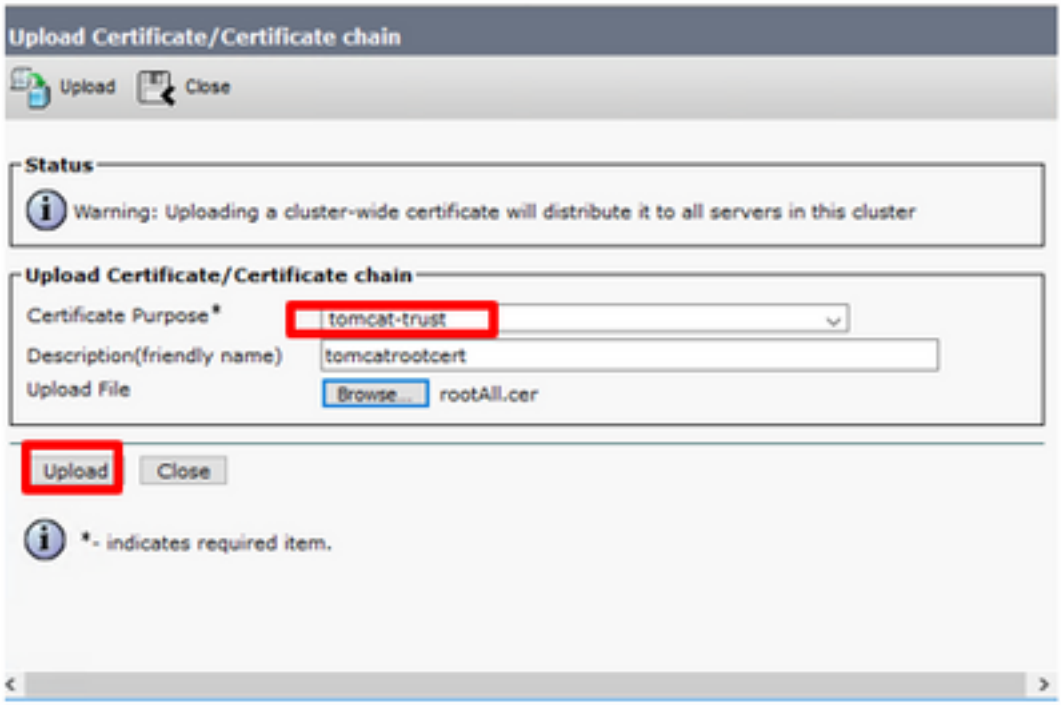
ステップ2：図に示すように、[Upload Certificate/Certificate chain]ボタンをクリックします。



ステップ3：ポップアップウィンドウで、[Certificate Purpose]**に[tomcat-trust]を選択します。**

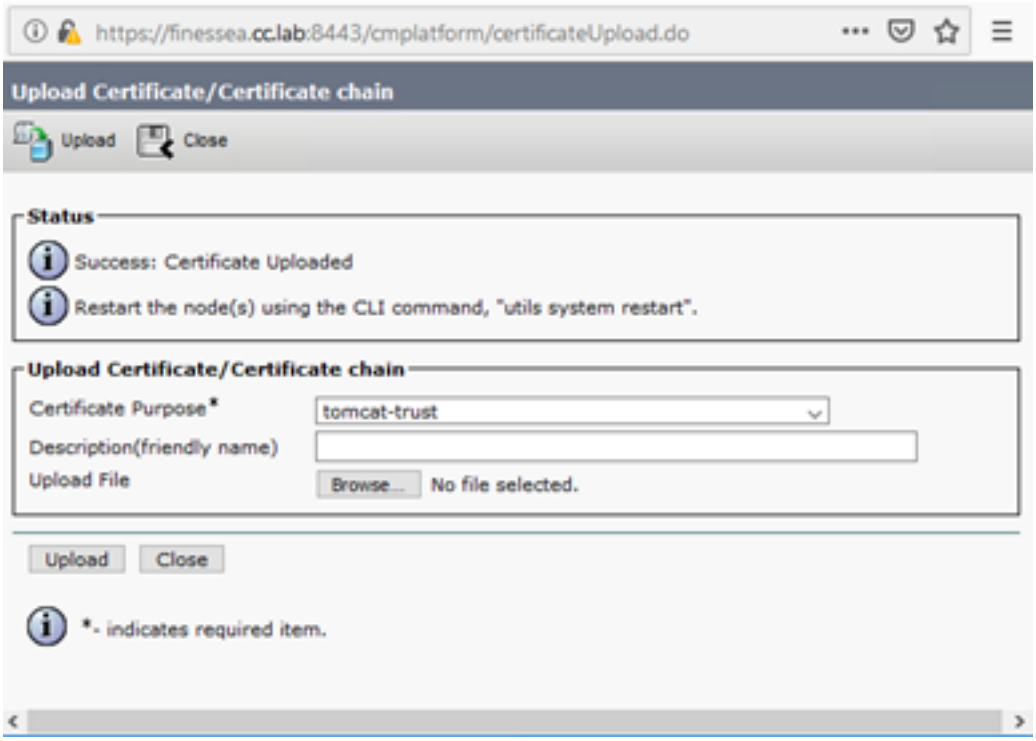
ステップ4:**[Browse...]ボタンをクリック**し、インポートするルート証明書ファイルを選択します。次に、[開く]ボタンを**クリック**します。

ステップ5：説明に**tomcatrootcert**のように書き込み、図に示すように**Upload**ボタンをクリックします。

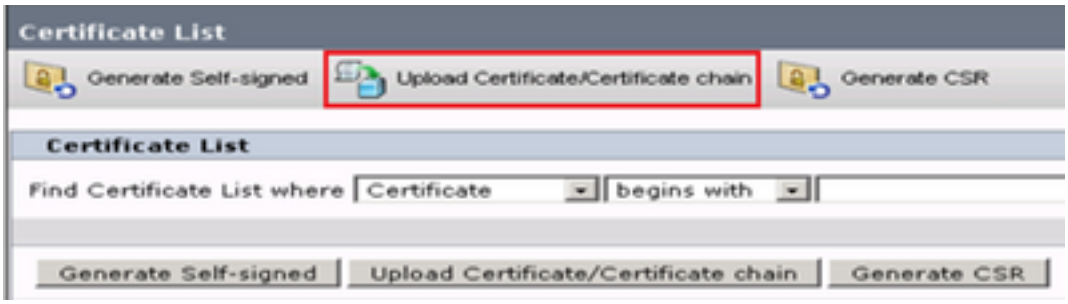


ステップ6:「Success:**Certificate Uploadedメッセージ**をクリックしてウィンドウを閉じます。

システムの再起動が要求されますが、最初にFinesseアプリケーション署名付き証明書のアップロードを続行し、システムを再起動できます。



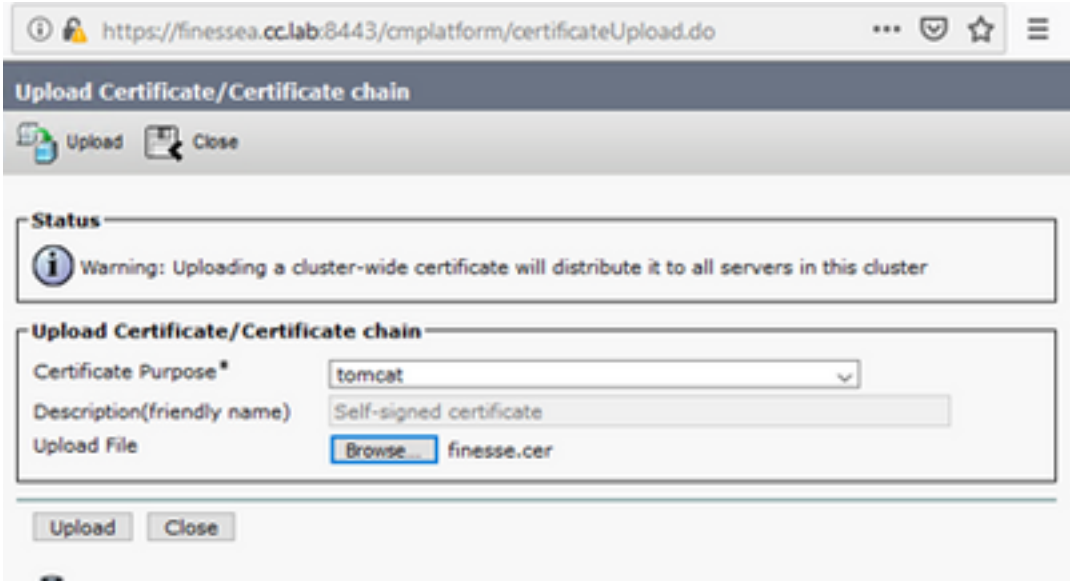
ステップ7:[**Upload Certificate/Certificate chain**]ボタンをクリックして、Finesseアプリケーション証明書をインポートします。



ステップ8：ポップアップウィンドウで、[Certificate Purpose]**に[tomcat]を選択します**。

ステップ9:[**Browse...]ボタンをクリック**し、Finesse CA署名付きファイルfinesse.cerを選択**します**。次に、[開く]ボタンを**クリック**します。

ステップ10:[Upload]ボタンを**クリック**します。



ステップ11:「Success:**証明書がアップロードされました。**

ここでも、システムの再起動が要求されます。ウィンドウを閉じて、システムの再起動を続行します。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。