UCSMでのサードパーティ証明書の作成と使用

内容

はじめに

このドキュメントでは、セキュアな通信のためにUnified Computing System(UCS)でサードパーティ証明書を作成して使用する手順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。

- CA認証局へのアクセス
- UCSM 3.1

使用するコンポーネント

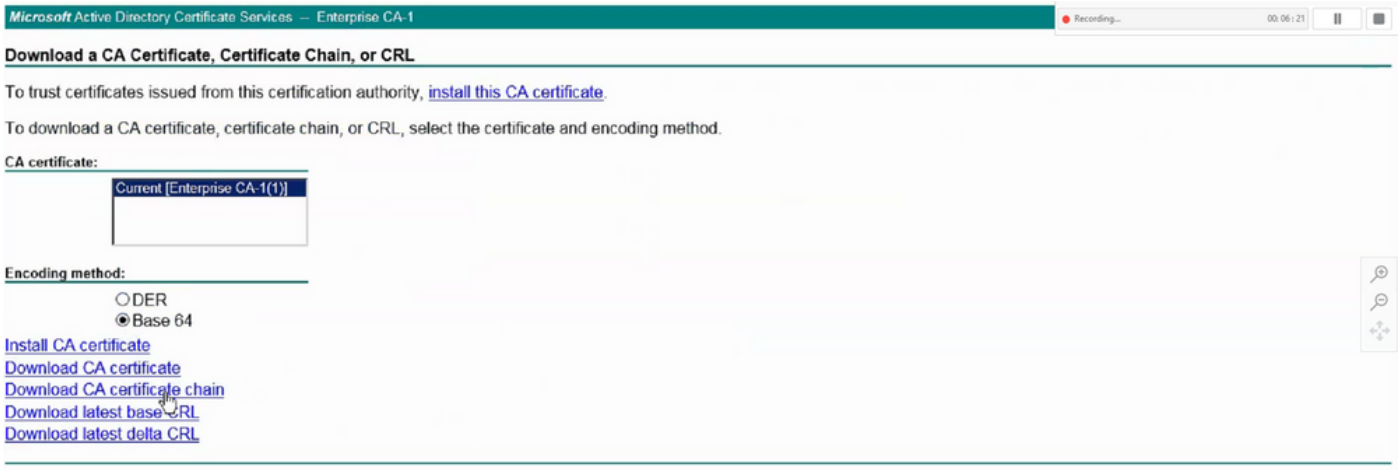
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定手順

トラストポイントの設定

手順 1

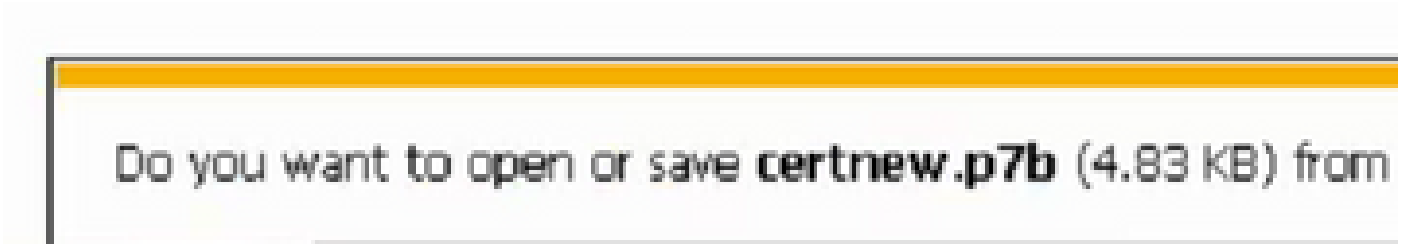
- CA認証局から証明書チェーンをダウンロードして、トラストポイントを作成します。証明書サーバ内のhttp://localhost/certsrv/Default.aspを参照してください。
- encodingがBase 64に設定されていることを確認します。



CA認証局からの証明書チェーンのダウンロード

手順 2

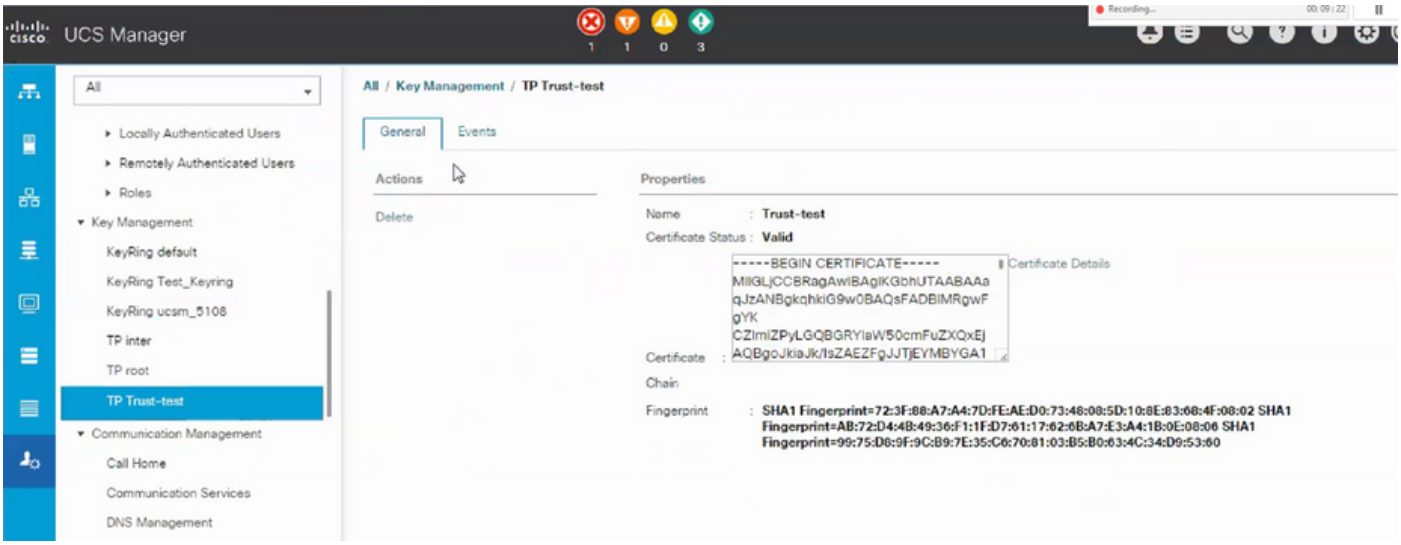
- ダウンロードされた証明書チェーンはPB7形式です。



- OpenSSLツールで.pb7ファイルをPEM形式に変換します。
- たとえば、Linuxでは、変換を実行するためにターミナルで次のコマンドを実行できます：openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem。

手順 3

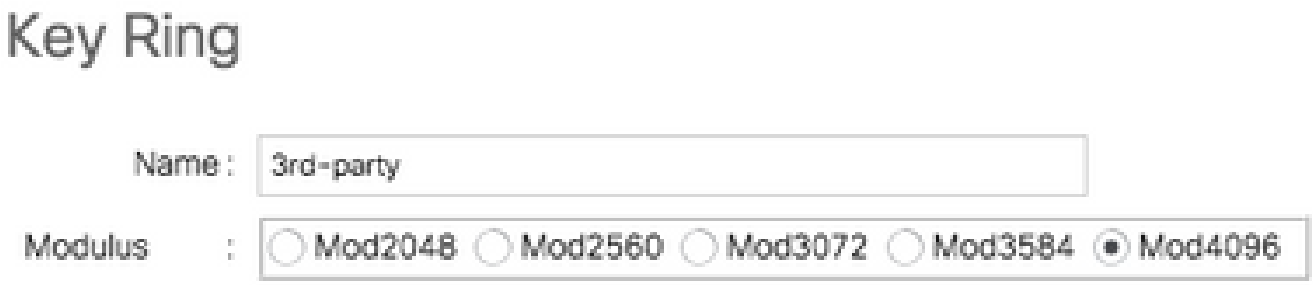
- UCSMでトラストポイントを作成します。
- Admin > Key Management > Trustpointの順に移動します。
- トラストポイントを作成するときに、このセクションのステップ2で作成した.PEMファイルの完全な内容を証明書の詳細スペースに貼り付けます。



キーリングとCSRの作成

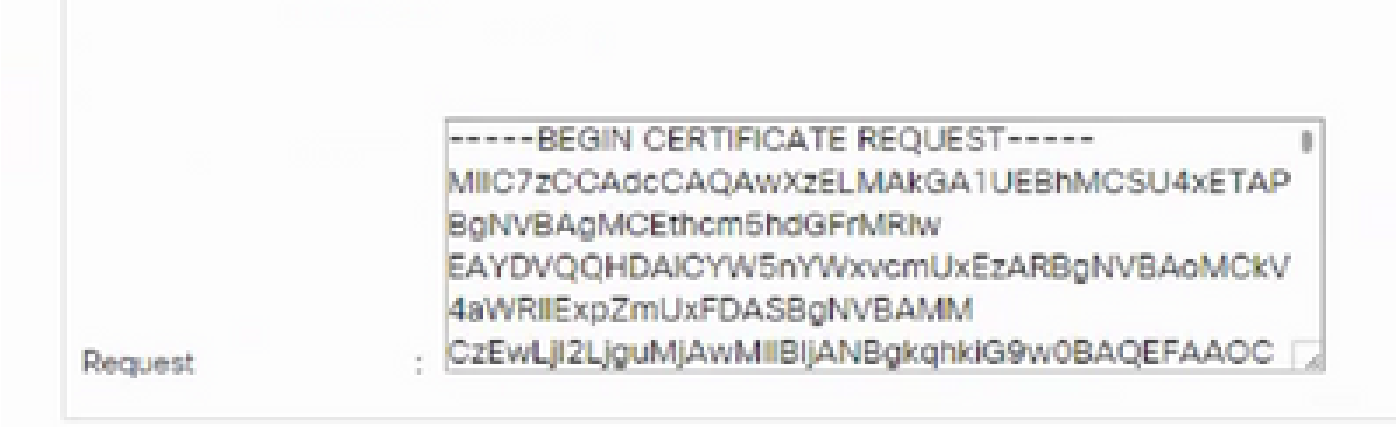
手順 1

- UCSM > Admin > Key Management > Keyringの順に移動します。
- サードパーティ証明書に必要なモジュールを選択します。



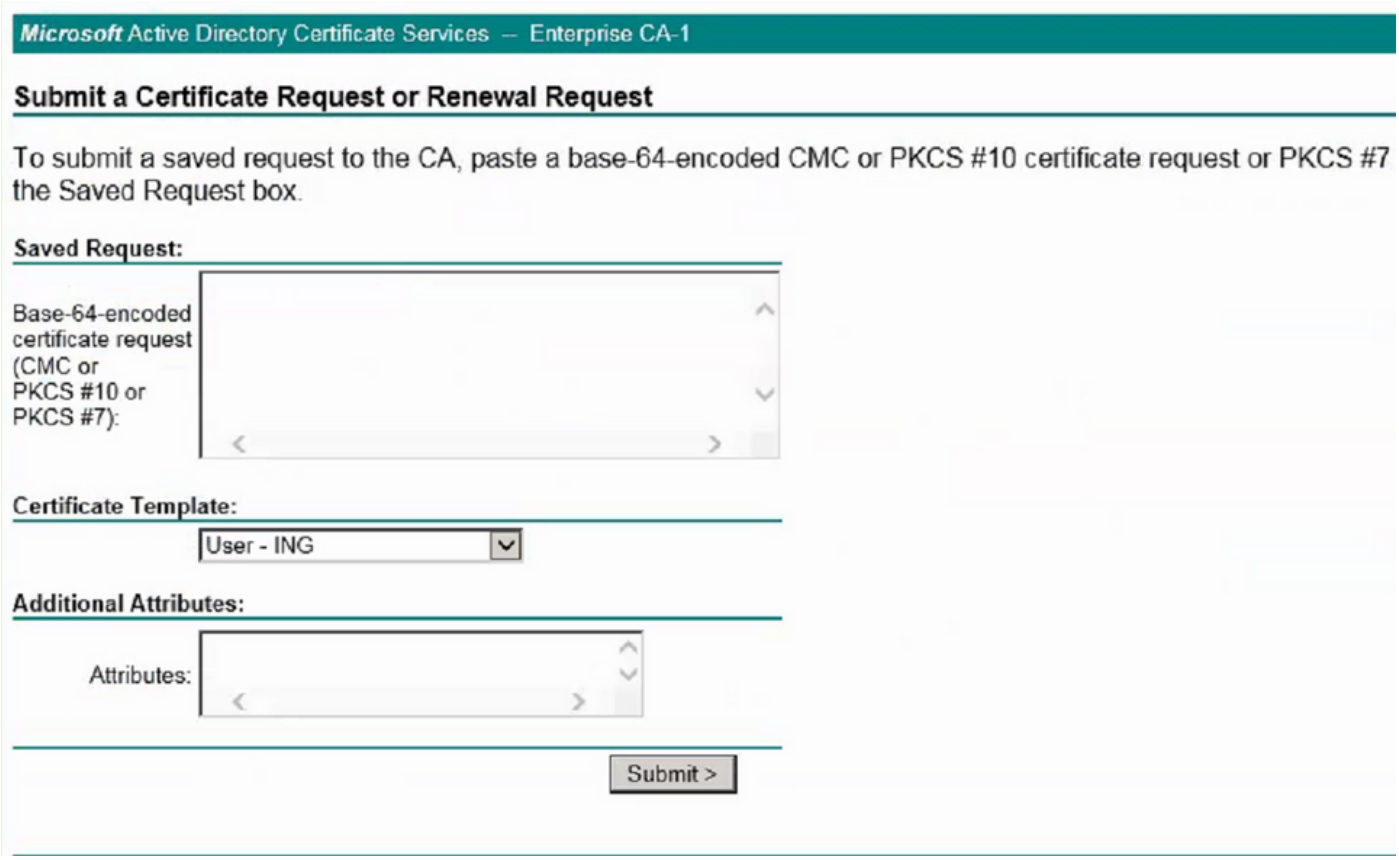
手順 2

- create certificate requestをクリックし、要求された詳細情報を入力します。
- 要求フィールドの内容をコピーします。



手順 3

証明書を生成するには、手順2でコピーした要求を次のスペースに貼り付けます。



手順 4

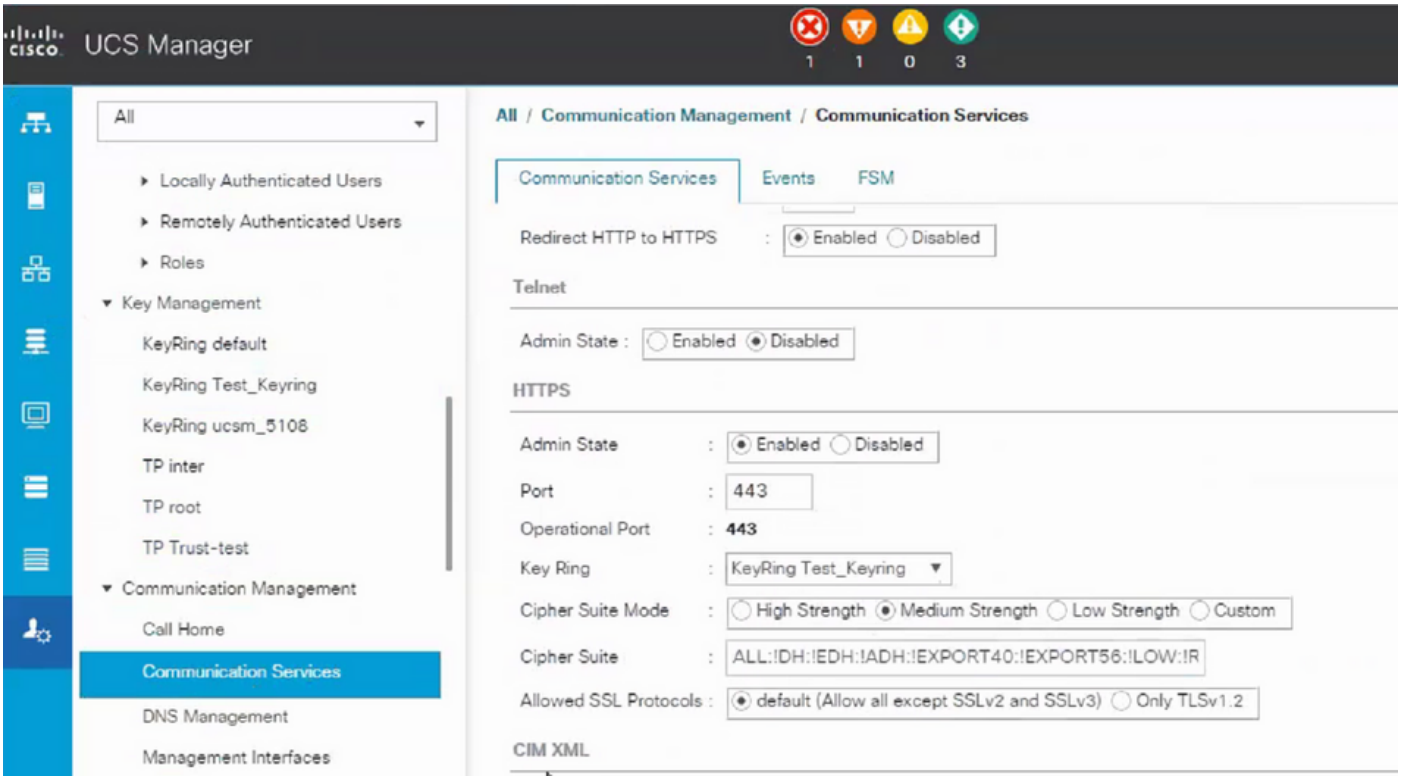
- 送信されると、新しい証明書が生成されます。ファイルを開き、このセクションのステップ1で作成したキーリングの証明書フィールドに、新しく生成した証明書のすべての内容をコピーします。

- 「キーリングとCSRの作成」のステップ3で作成したドロップダウンからトラストポイントを選択します。

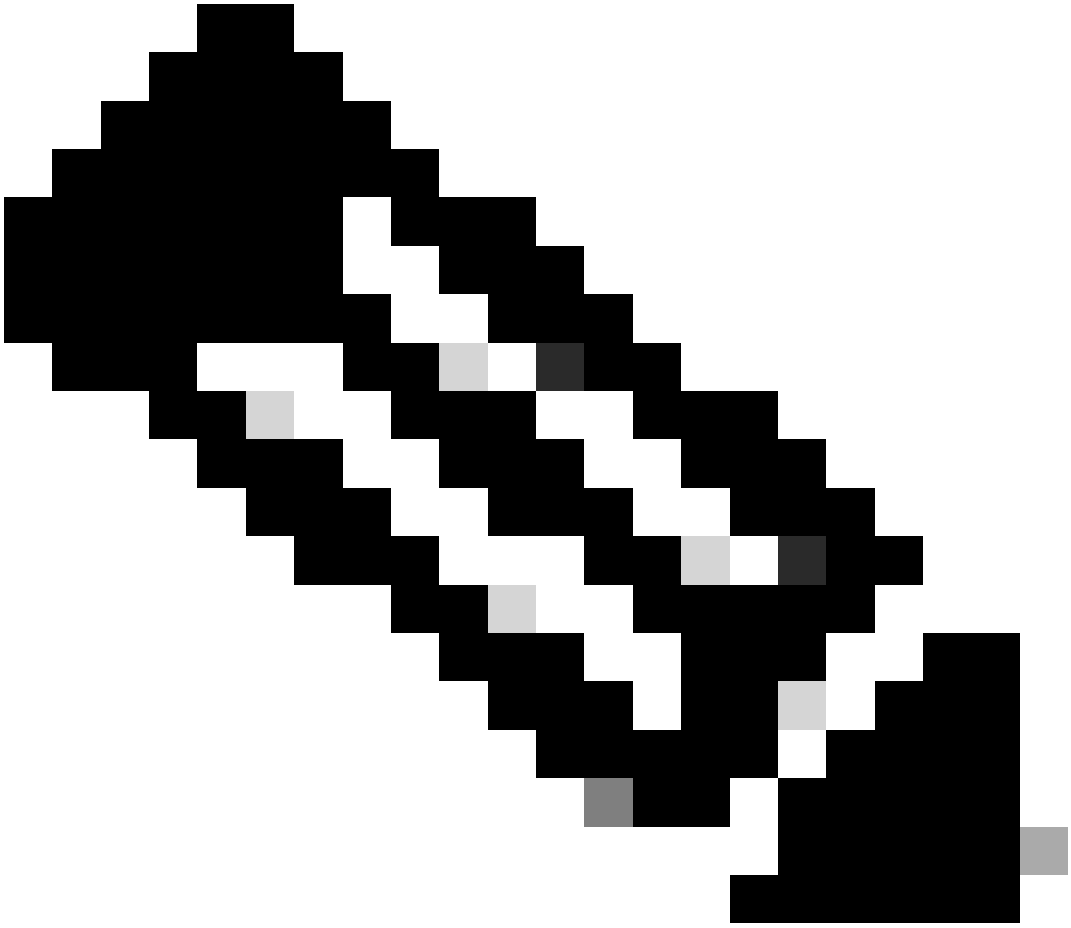
キーリングの適用

手順 1

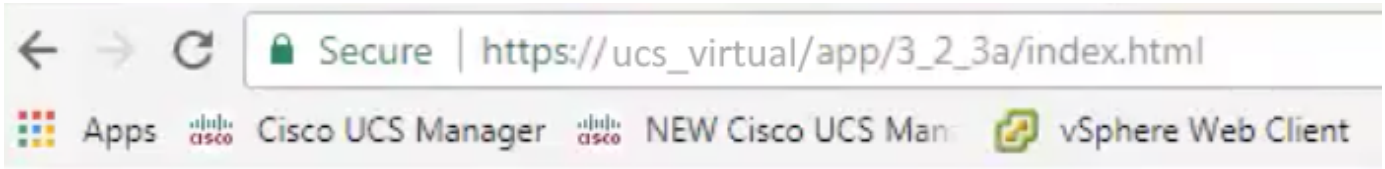
次に示すように、コミュニケーションサービスで作成したキーリングを選択します。



キーリングを変更すると、UCSMへのHTTPS接続がWebブラウザでセキュアとして表示されます。



注：これを行うには、ローカルデスクトップもUCSMと同じCA認証局からの証明書を使用する必要があります。



関連情報

- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。