UCS Centralのサードパーティ証明書の設定

内容

はじめに

このドキュメントでは、Cisco Unified Computing System(UCS)Central Software(UCS Central)でサードパーティ証明書を設定するベストプラクティス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。

- Cisco UCS Central
- 認証局（CA）
- OpenSSL

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

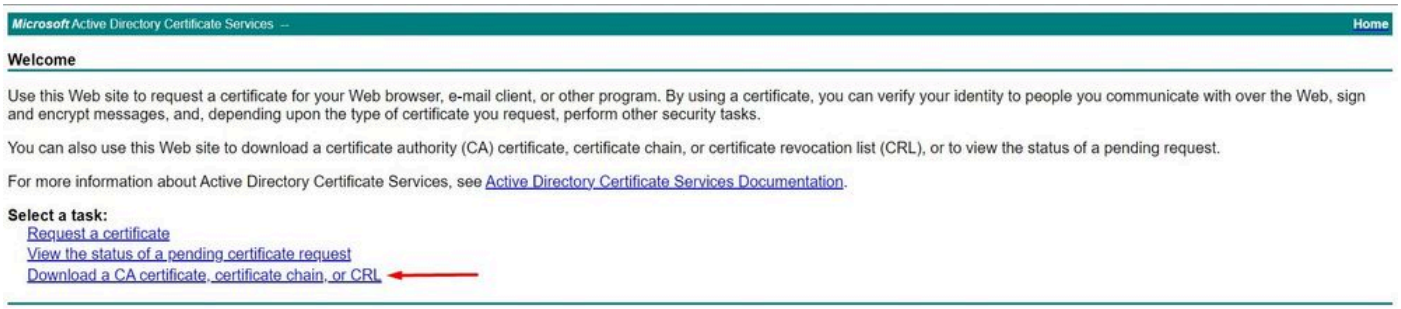
- UCS Central 2.0(1q)
- Microsoft Active Directory証明書サービス
- Windows 11 Pro N
- OpenSSL 3.1.0

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

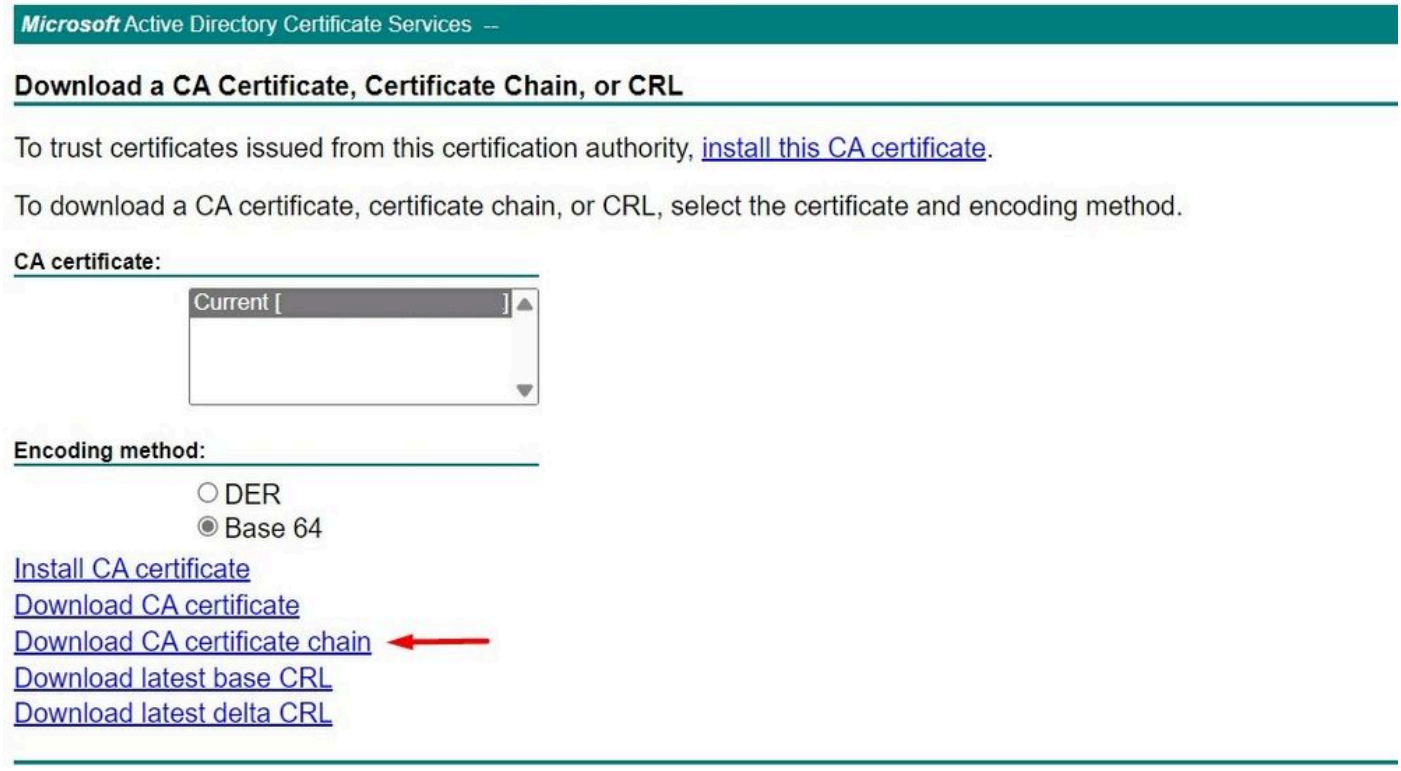
認証局から証明書チェーンをダウンロードします。

1. 認証局(CA)から証明書チェーンをダウンロードします。



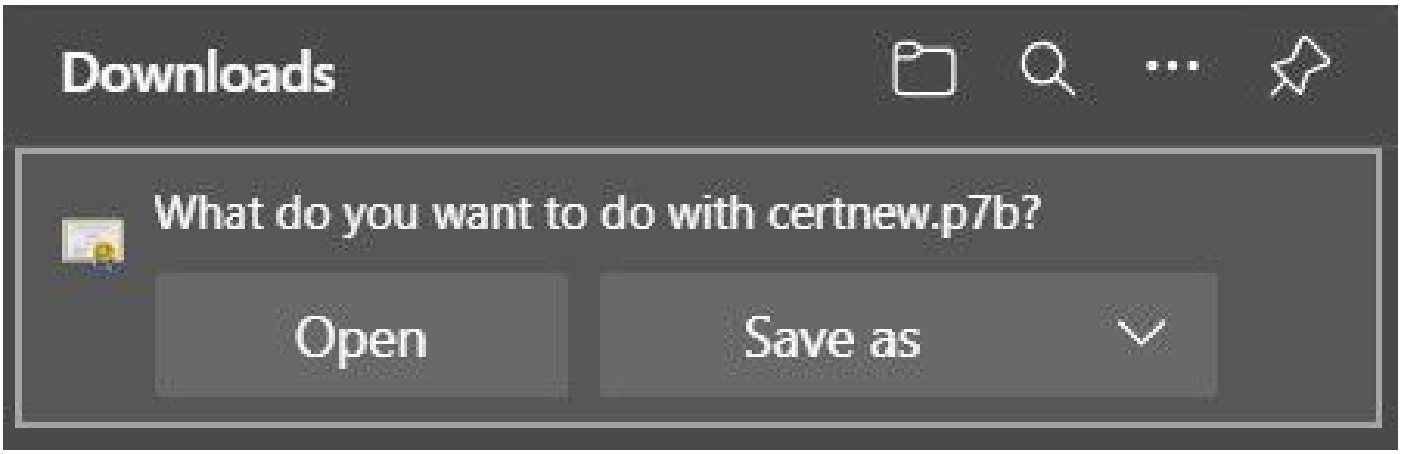
CAからの証明書チェーンのダウンロード

2. エンコーディングをBase 64に設定し、CA証明書チェーンをダウンロードします。



エンコーディングをBase 64に設定し、CA証明書チェーンをダウンロードします

3. CA証明書チェーンはPB7形式であることに注意してください。



証明書はPB7形式です

4. 証明書は、OpenSSLツールを使用してPEM形式に変換する必要があります。Open SSLがWindowsにインストールされているかどうかを確認するには、openssl versionコマンドを使用します。

```
C:\Program Files\OpenSSL-Win64\bin>openssl version
OpenSSL 3.1.0 14 Mar 2023 (Library: OpenSSL 3.1.0 14 Mar 2023)
```

OpenSSLがインストールされているかどうかを確認する

注:OpenSSLのインストールについては、この記事では扱いません。

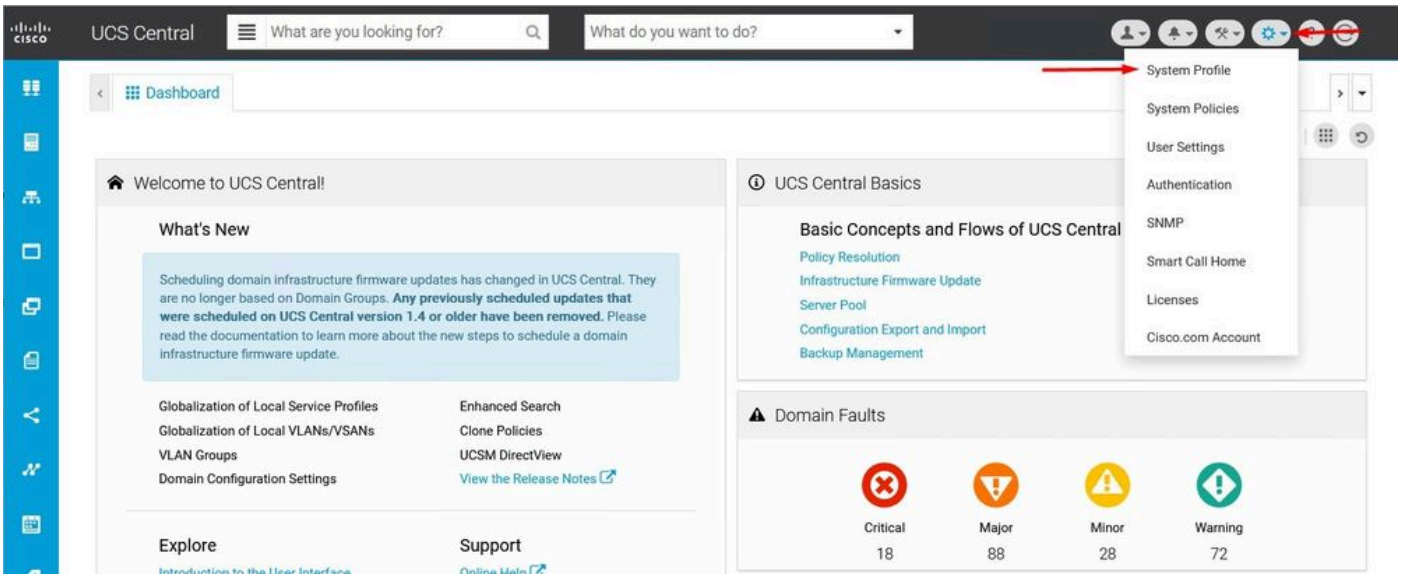
5. OpenSSLがインストールされている場合、コマンドopenssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pemを実行して変換を行います。証明書が保存されたパスを使用していることを確認します。

```
C:\Program Files\OpenSSL-Win64\bin>openssl pkcs7 -print_certs -in C://Users/[redacted]/Desktop/certnew.p7b -out C://Users/
[redacted]/Desktop/certnew.pem
```

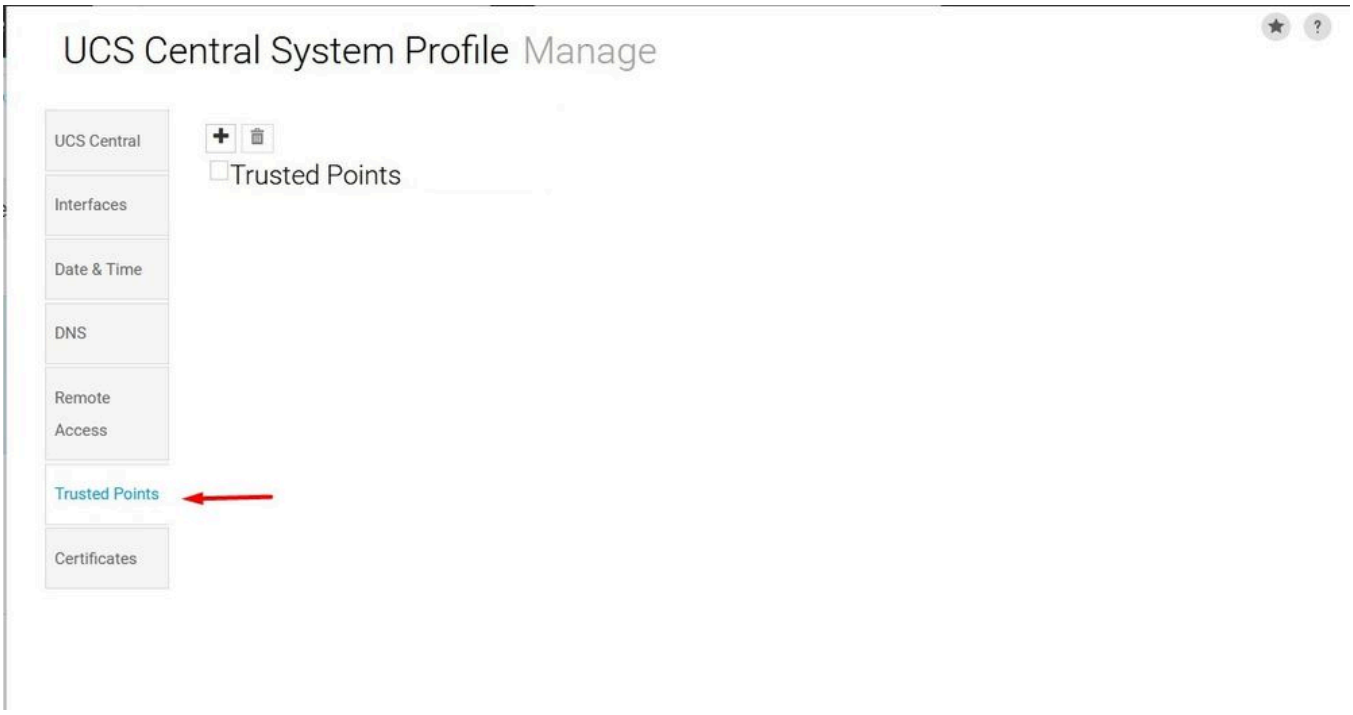
P7B証明書をPEM形式に変換する

トラステッドポイントの作成

1. System Configuration icon > System Profile > Trusted Pointsの順にクリックします。

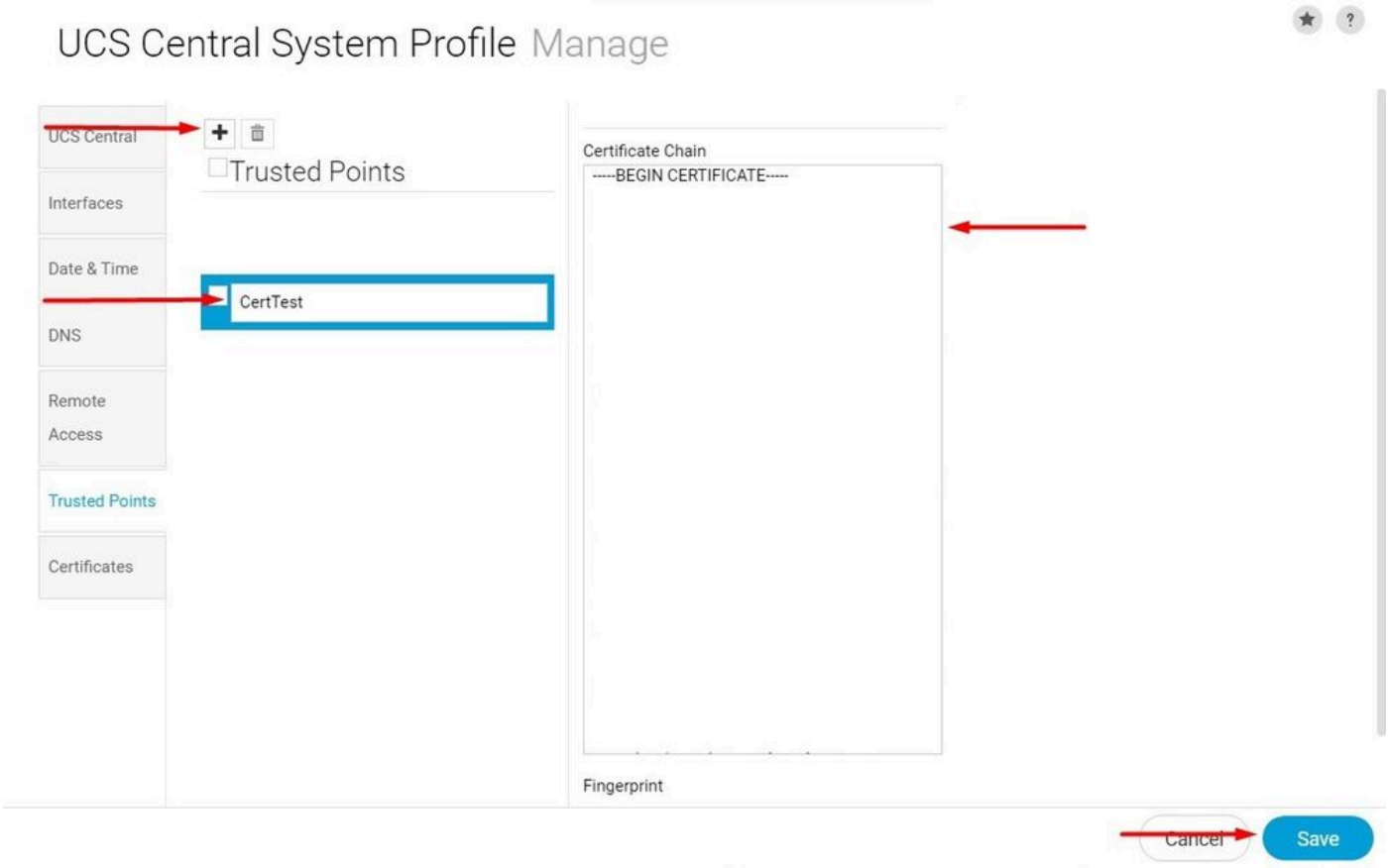


UCS Centralシステム



プロ
ファイルUCS Centralトラステッドポイント

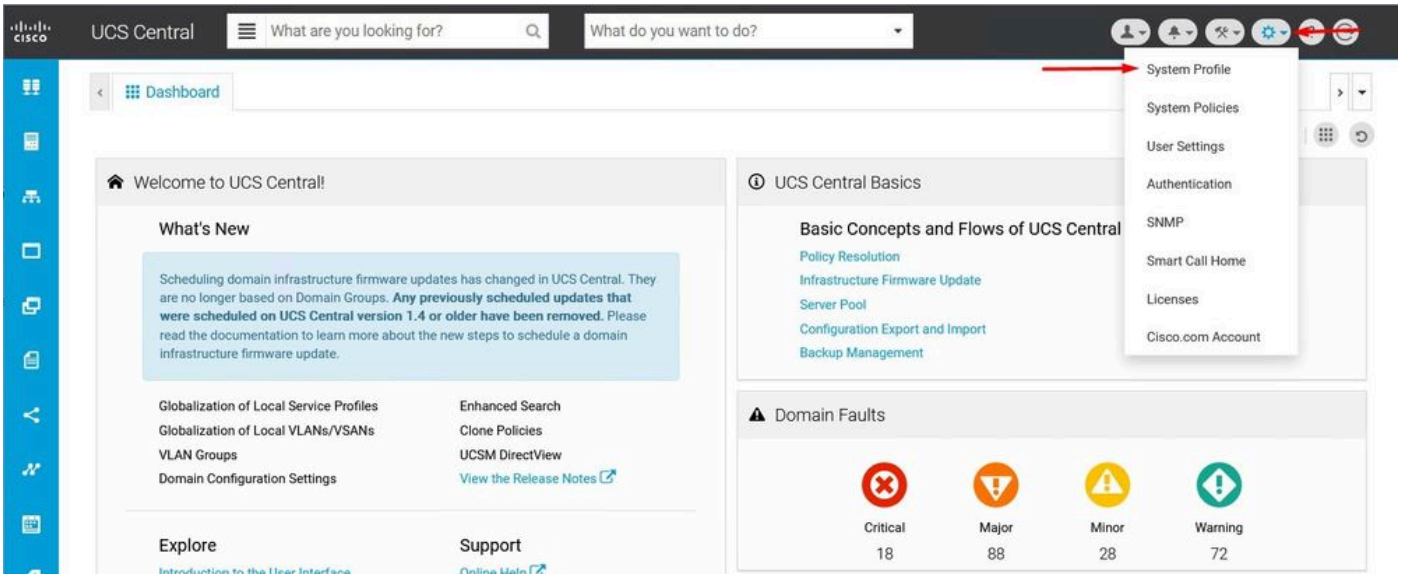
2. + (プラス) アイコンをクリックして、新しいトラステッドポイントを追加します。名前を入力し、PEM証明書の内容に貼り付けます。Saveをクリックして、変更を適用します。



証明書チェーンをコピーする

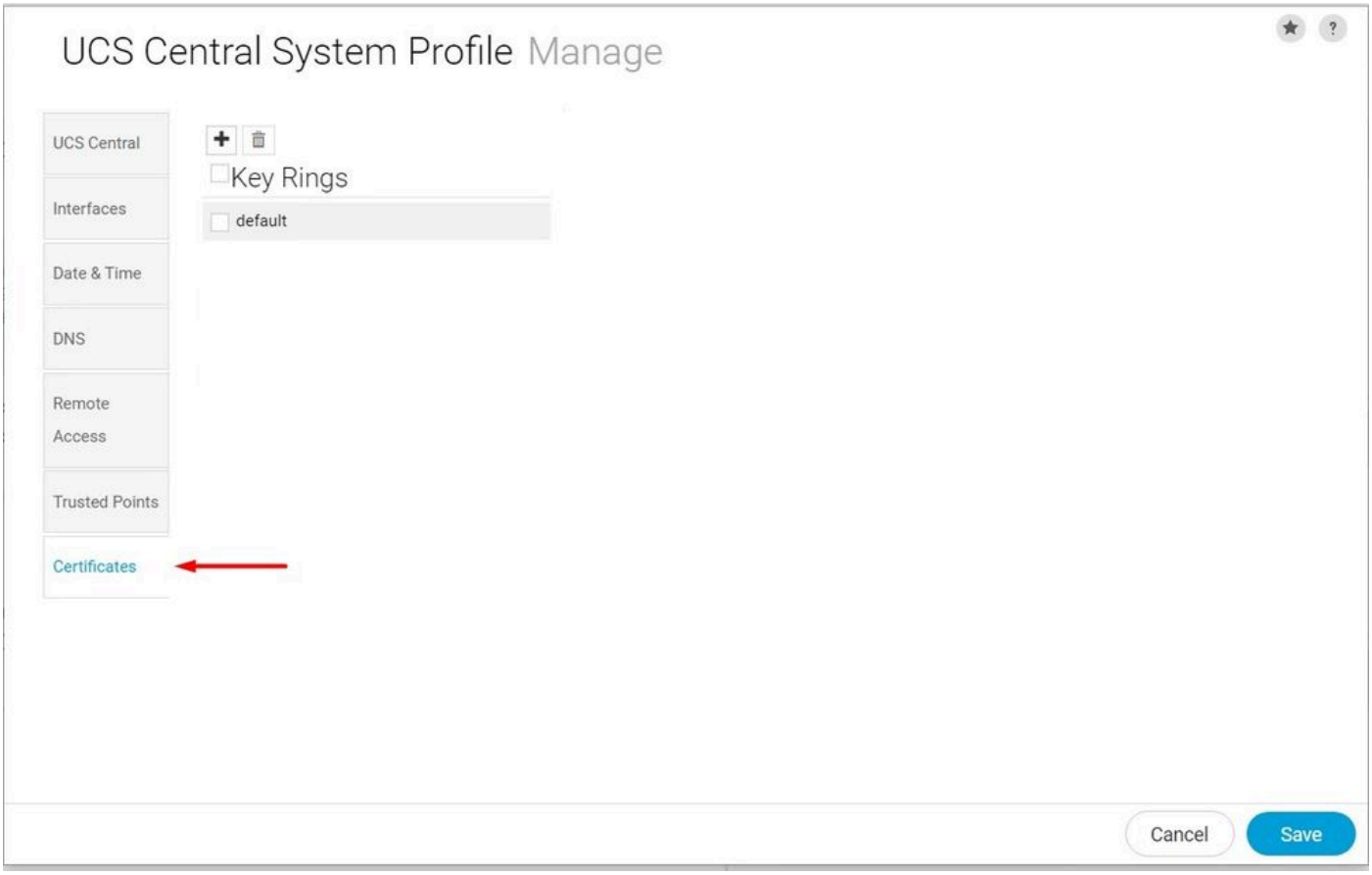
キーリングとCSRの作成

1. System Configuration icon > System Profile > Certificatesの順にクリックします。



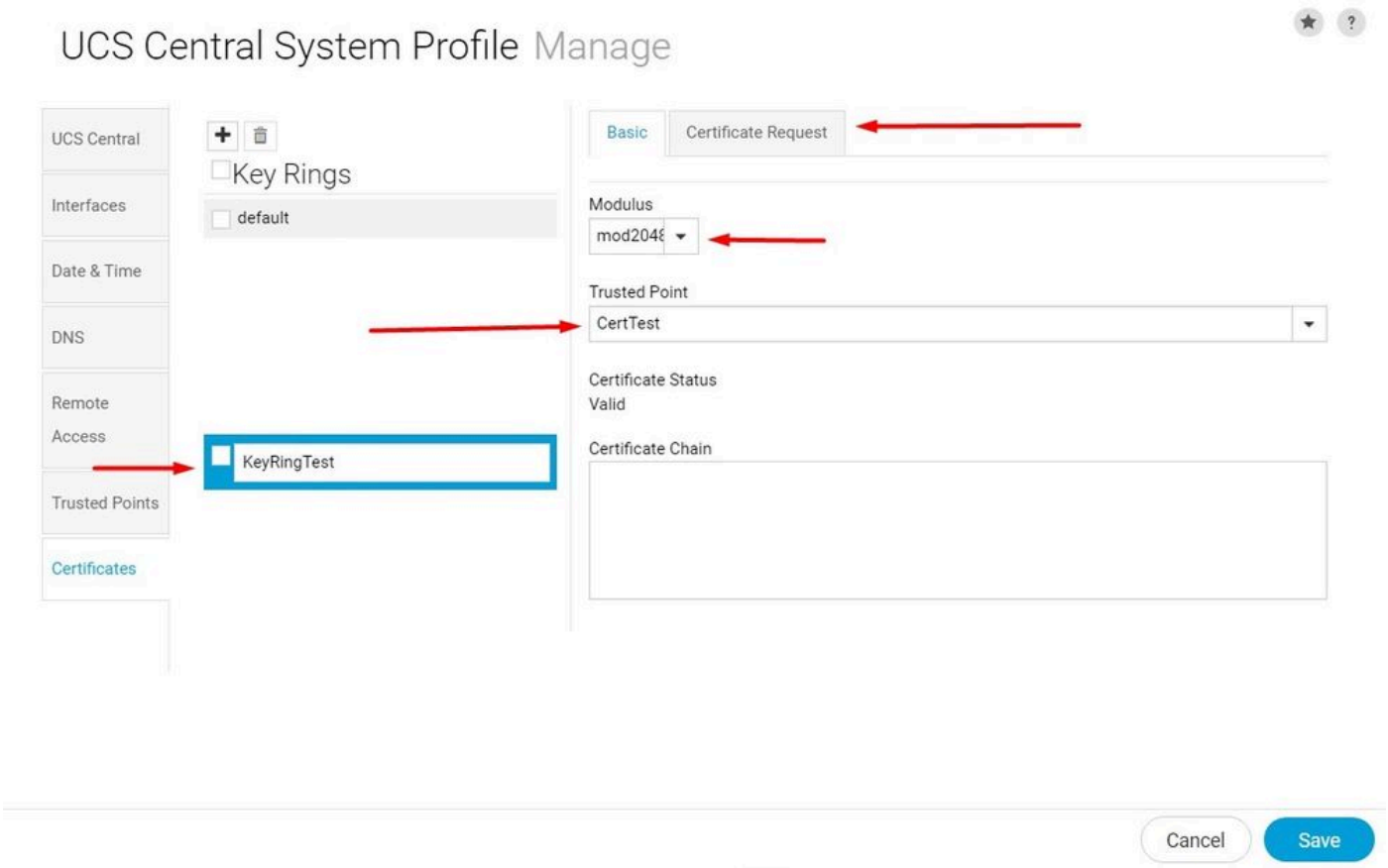
UCS Centralシステム

プロ



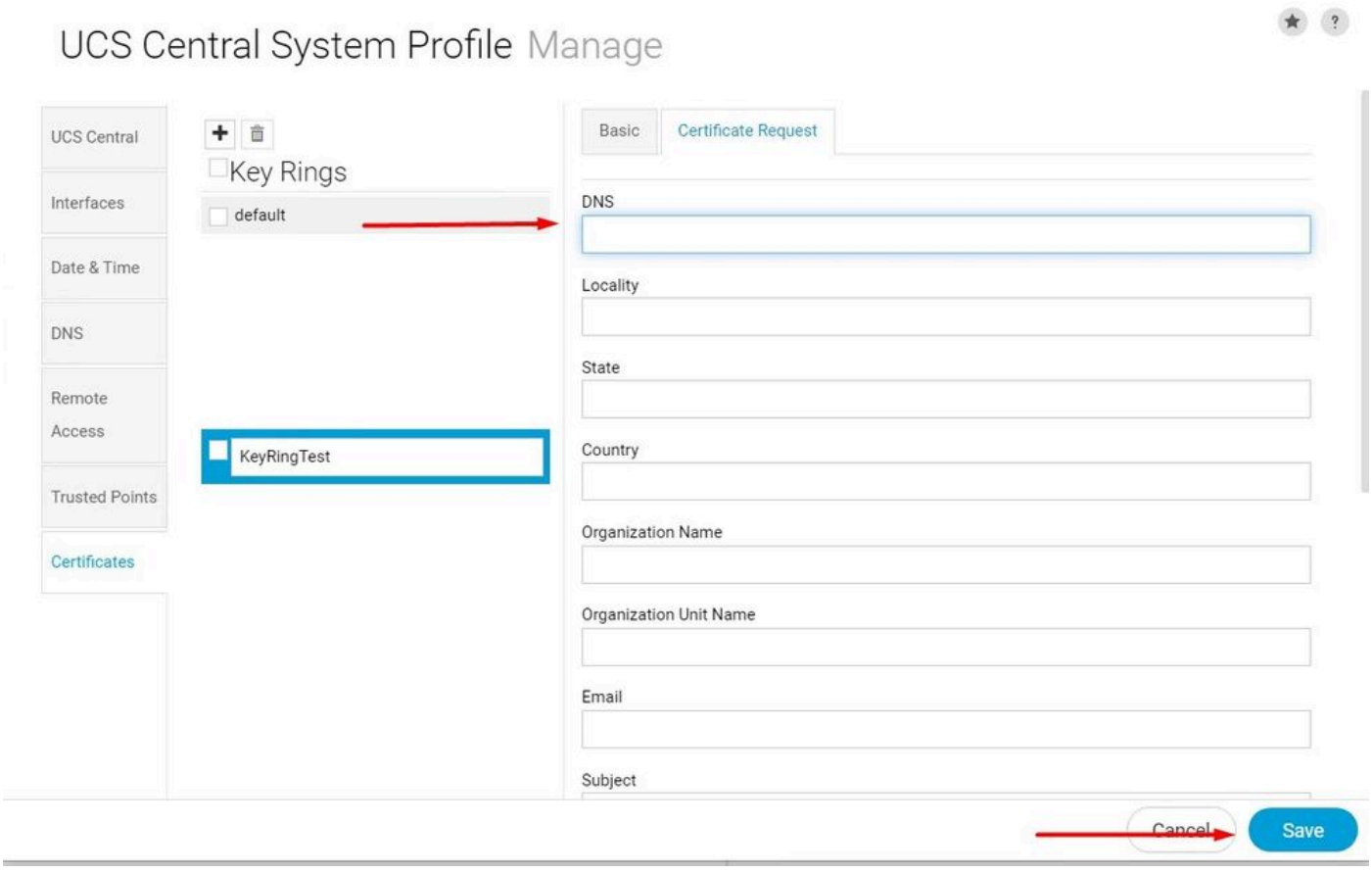
ファイルUCS Central証明書

2.プラスアイコンをクリックして、新しいキーリングを追加します。名前を入力し、モジュラスをデフォルト値のままにして（または必要に応じて変更して）、前に作成したトラステッドポイントを選択します。これらのパラメータを設定した後、証明書要求に進みます。



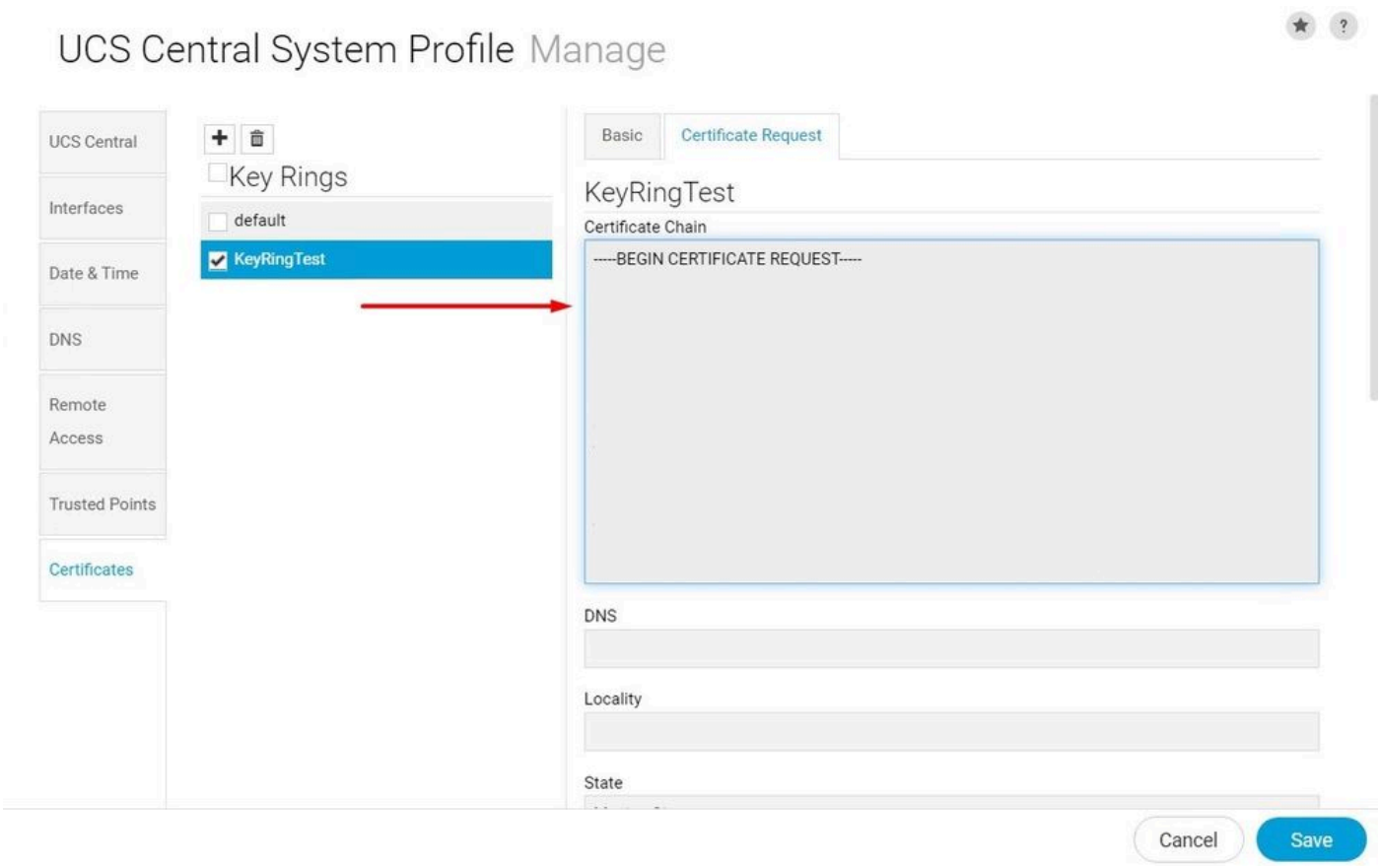
新しいキーリングの作成

3. 証明書を要求するために必要な値を入力し、「保存」をクリックします。



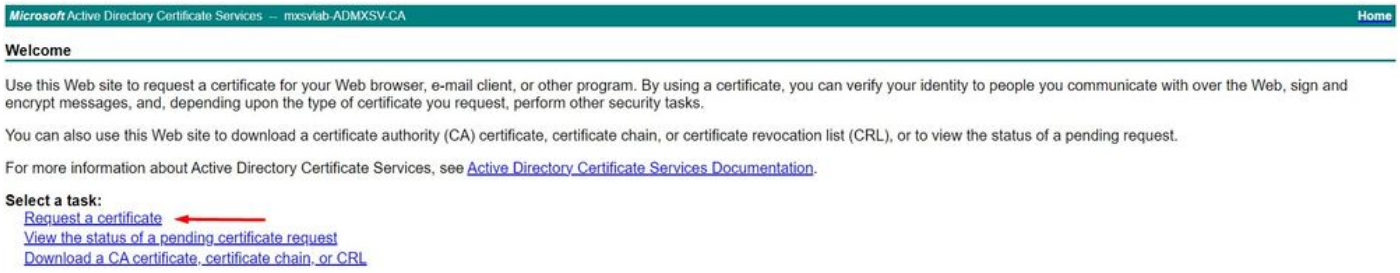
詳細を入力して証明書を生成します

4. 作成したキーリングに戻り、生成した証明書をコピーします。



生成された証明書をコピーする

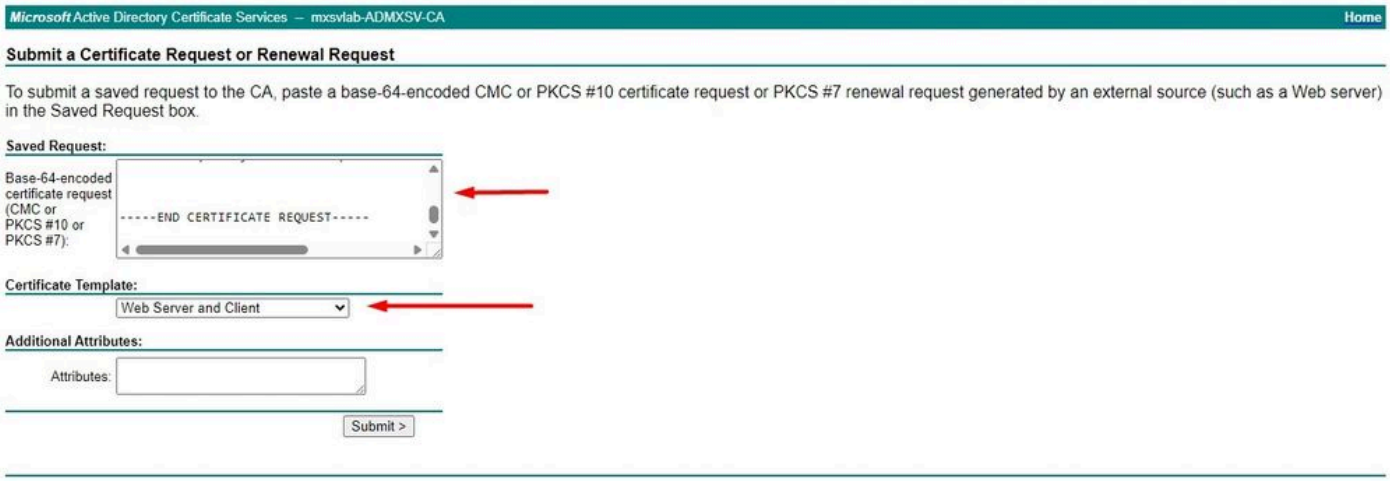
5. CAに移動し、証明書を要求します。



CAからの証明書の要求

6. UCS Centralで生成された証明書を貼り付け、CAでWebサーバとクライアントテンプレートを選択します。Submitをクリックして、証明書を生成します。

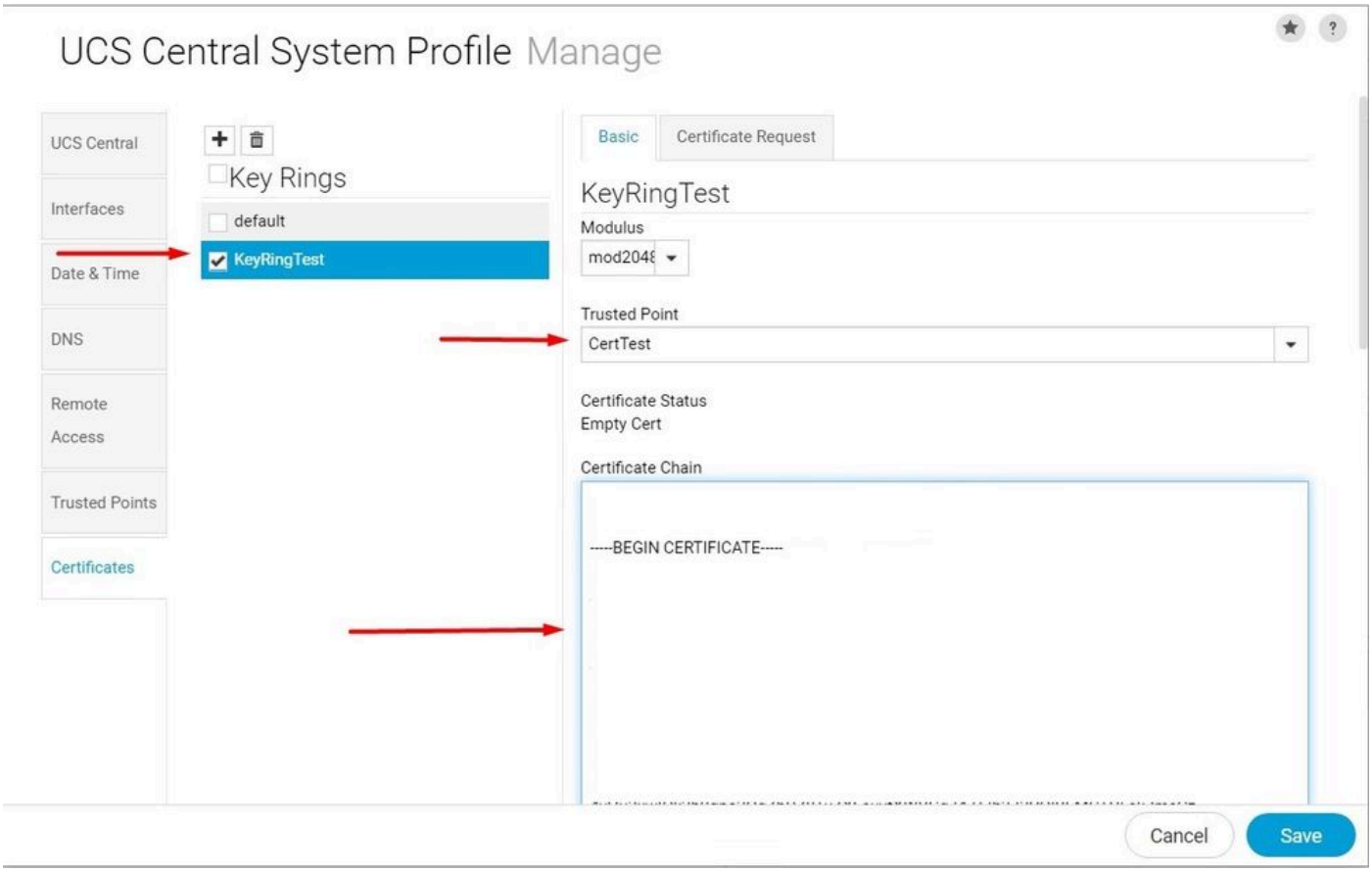
注：Cisco UCS Centralで証明書要求を生成する際、生成される証明書にSSLクライアントとサーバ認証キーの使用が含まれていることを確認してください。Microsoft Windows Enterprise CAを使用している場合、コンピュータテンプレートを使用できない場合は、コンピュータテンプレート、または両方のキー使用法を含むその他の適切なテンプレートを使用します。



作成したキーリングで使用する証明書を生成します。

7. コマンドopenssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pemを使用して、新しい証明書をPEMに変換します。

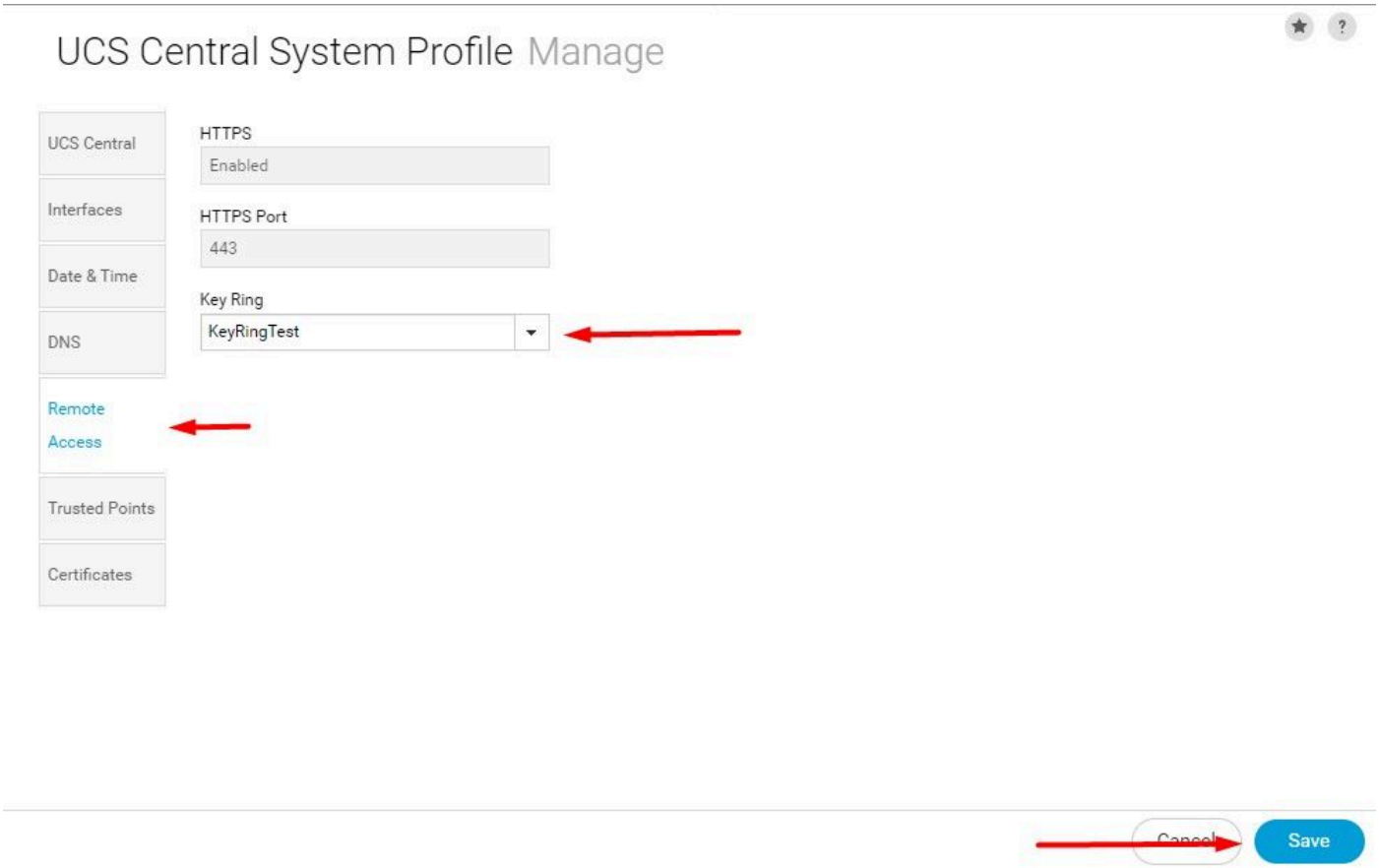
8. PEM証明書の内容をコピーし、内容を貼り付けるために作成したキーリングに移動します。作成した信頼できるポイントを選択し、設定を保存します。



要求された証明書をキーリングにペーストします。

キーリングの適用

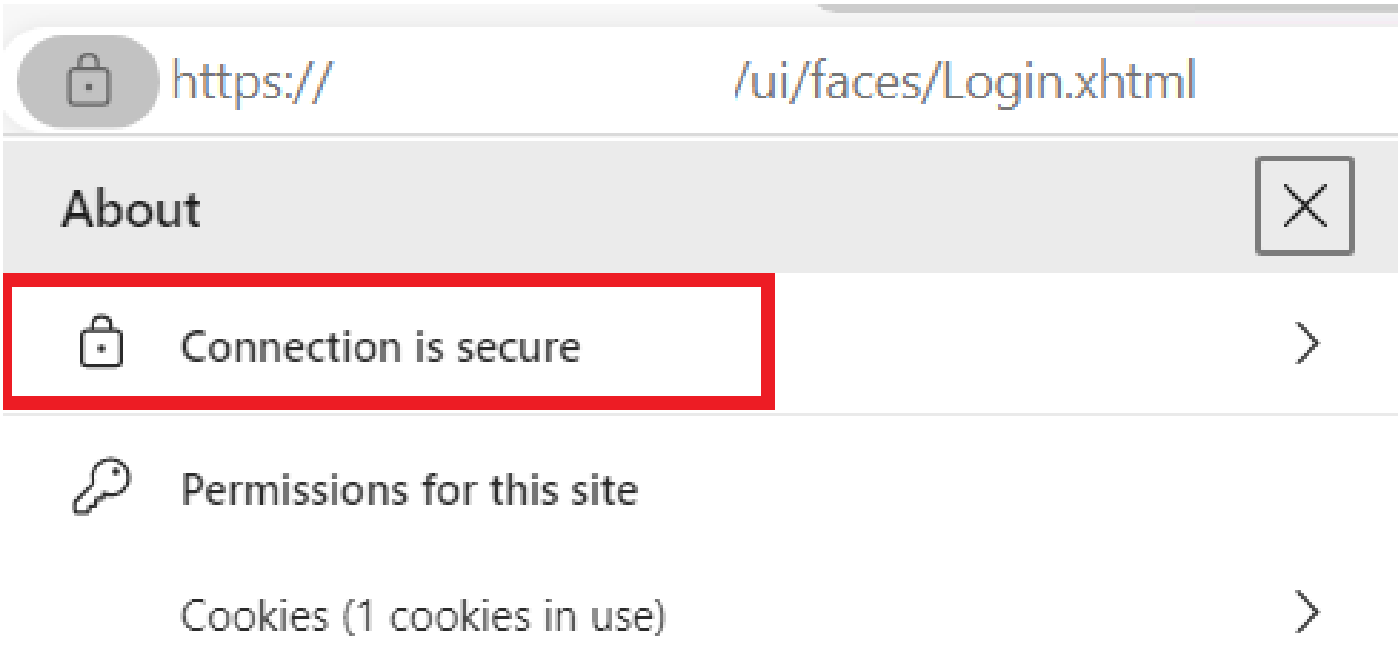
1. System Profile > Remote Access > Keyringの順に移動し、作成したキーリングを選択して、Saveをクリックします。 UCS Centralは現在のセッションを閉じます。



作成したキーリングを選択します

検証

1. UCS Centralにアクセスできるようになるまで待って、https://の横にあるロックをクリックします。サイトは安全です。



UCS Centralは安全

トラブルシューティング

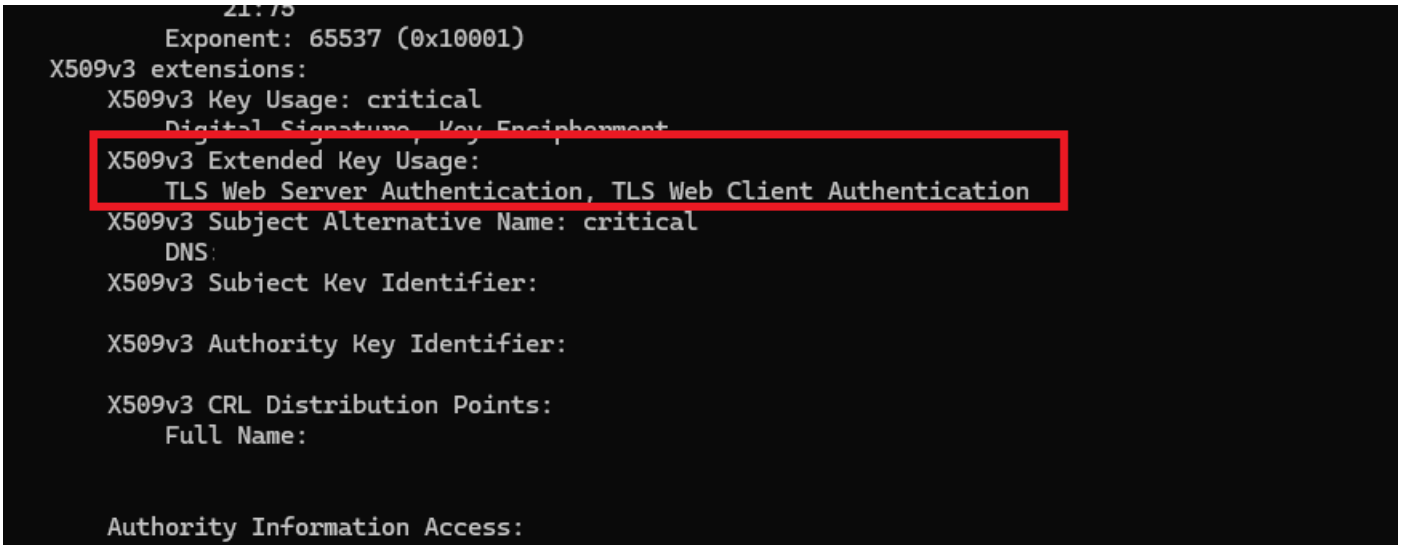
生成された証明書にSSLクライアントおよびサーバー認証キーの使用が含まれているかどうかを確認します。

CAに要求された証明書にSSLクライアントおよびサーバ認証キーが含まれていない場合、「証明書が無効です。This certificate cannot be used for TLS server authentication, check key usage extensions」が表示されます。

Invalid certificate: This certificate cannot be used for TLS server authentication, check key usage extensions.

TLSサーバ認証キーに関するエラー

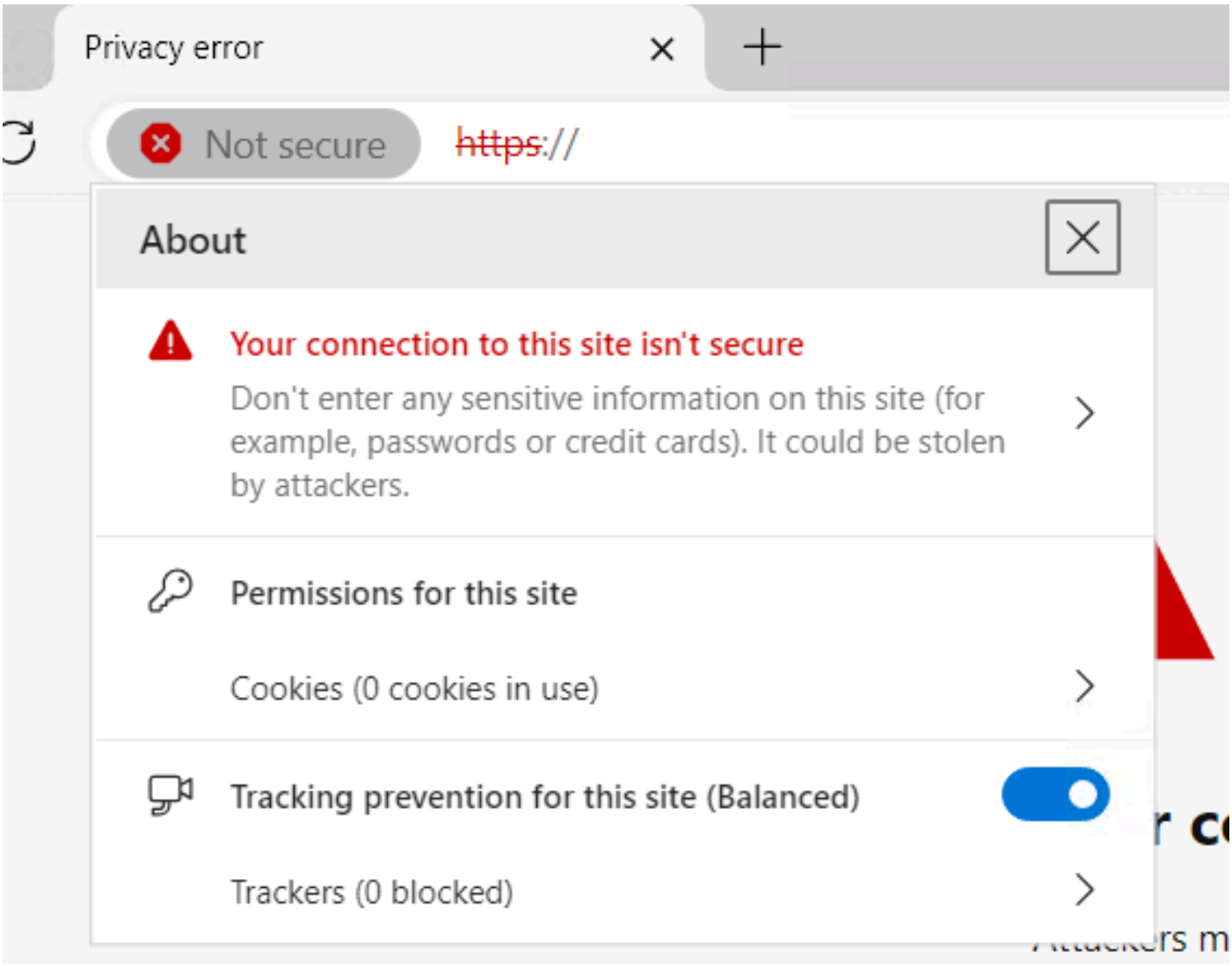
CAで選択したテンプレートから作成されたPEM形式の証明書が、正しいサーバ認証キー(PAK)の使用を使用しているかどうかを確認するには、openssl x509 -in <my_cert>.pem -text -noutコマンドを使用します。「拡張キー使用法」セクションの「Webサーバ認証」と「Webクライアント認証」が表示されている必要があります。



要求された証明書内のWebサーバとWebクライアント認証キー

UCS Centralは引き続き安全でないサイトとしてフラグが付けられます。

サードパーティ証明書を設定した後でも、ブラウザによって接続にフラグが付けられることがあります。



UCS Centralはまだ安全でないサイトです

証明書が正しく適用されているかどうかを確認するには、デバイスが認証局を信頼していることを確認します。

関連情報

- Cisco UCS Centralアドミニストレーションガイドリリース2.0
- シスコのテクニカルサポートとダウンロード

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。