# ISE 2.0 でのサードパーティ CA 証明書のインストール

## 目次



## 概要

この資料は Cisco Identity Services Engine（ISE）でサード パーティ CA 署名入り認証のインストールを記述したものです。 プロセスは最終的な証明書役割（EAP 認証、ポータル、Admin および pxGrid）に関係なく同じです。

## 前提条件

### 要件

Cisco は基本のナレッジが Public Key Infrastructure（PKI）あることを推奨します。

### 使用するコンポーネント

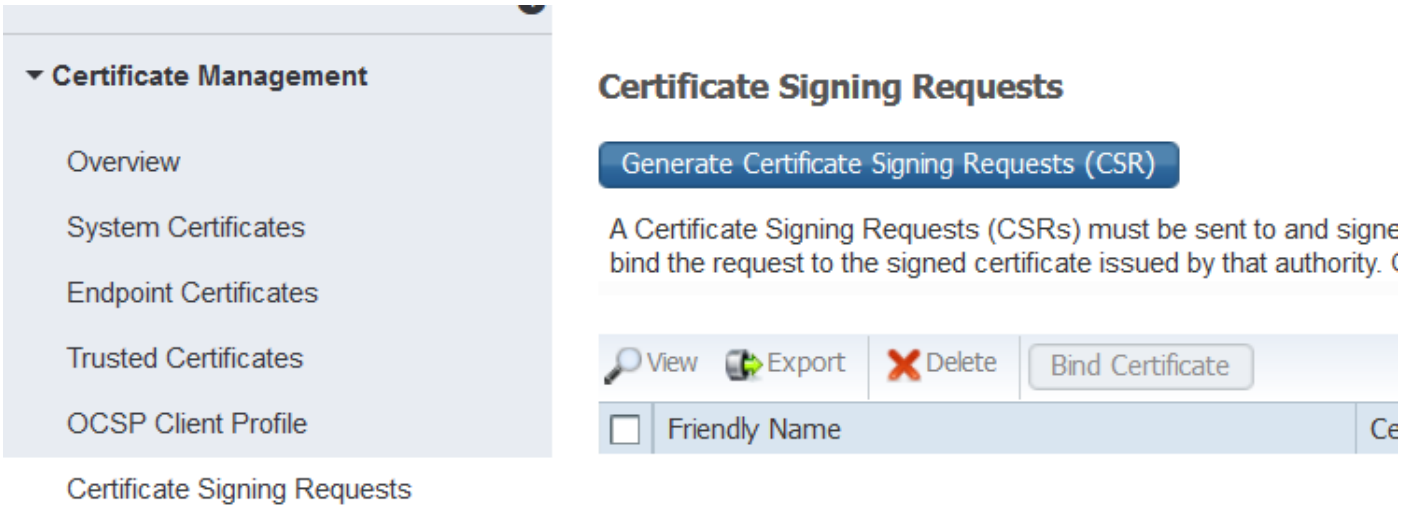
この 文書に記載されている 情報は on Cisco 基づいた Identity Services Engine（ISE）リリース 2.0 です。 リリース 1.3 および 1.4 にも同じ設定が適用されます。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

## 設定

### ステップ 1.生成する 証明書署名要求（CSR）。

CSR を生成するために、**Administration > 証明書 > 証明書署名要求**にナビゲート し、**Certificate Signing Requests （ CSR ）を**『Generate』 をクリック して下さい。




1. 使用方法 セクションの下で、ロールをドロップダウン メニューから使用されるために選択して下さい。 証明書が複数の役割のために使用されればマルチユースを選択できます。 証明書が生成されてからも、必要に応じてロールを変更できます。

2. 証明書を生成する対象のノードを選択します。

3. 必要な情報を入力します（組織単位、組織、市区町村、都道府県、国）。

   **注:** Common Name （ CN ） フィールドの下で ISE はノードの完全修飾ドメイン名（ FQDN ）を自動読み込みます。

ワイルドカード：

- 目的が**割り当てワイルドカード 証明書** ボックス ワイルドカード 証明書 チェックを生成することなら。

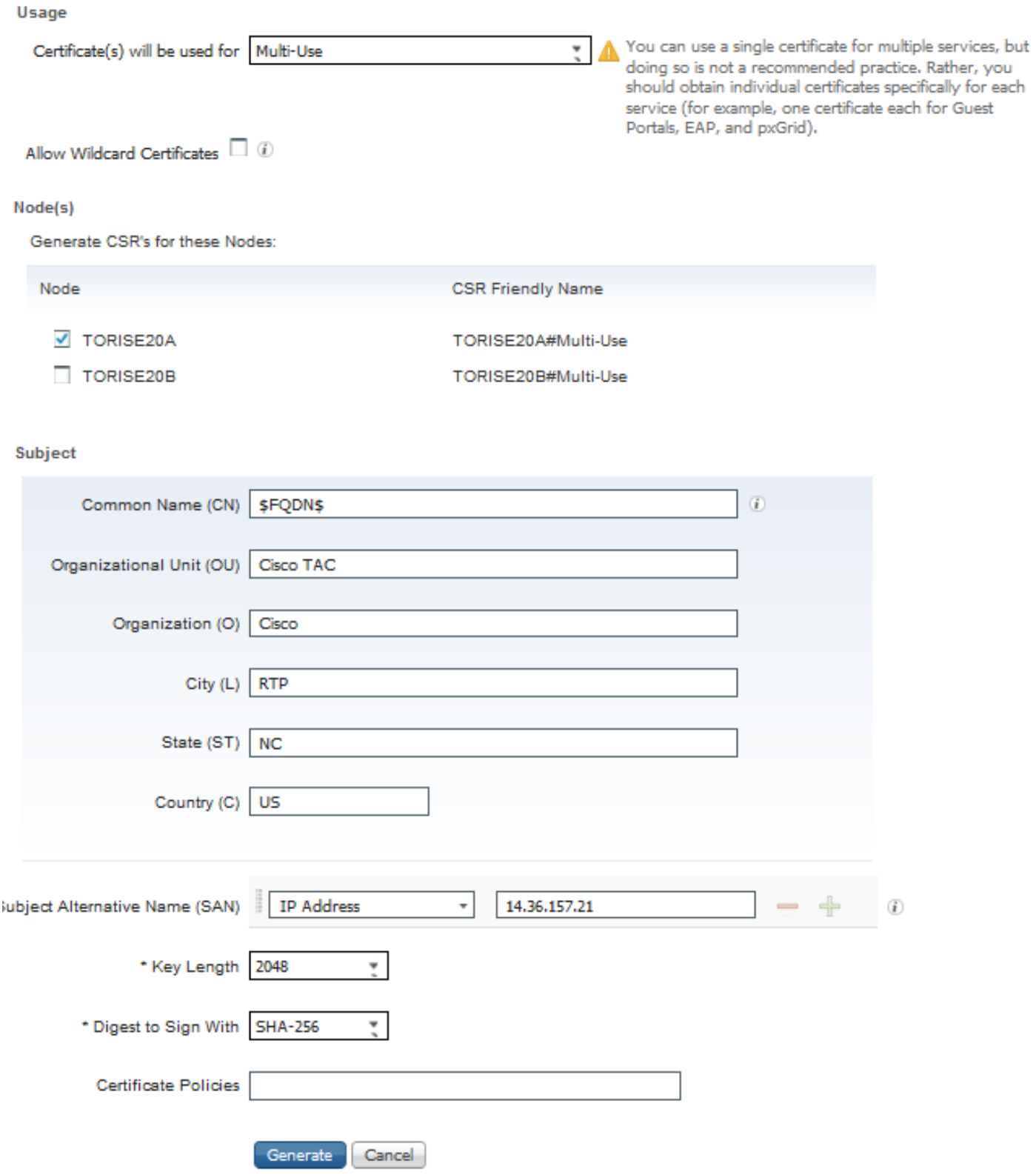
- 証明書が EAP 認証のために使用されれば*シンボルはサブジェクト CN フィールドに Windows 要求元がサーバ証明を拒否すると同時にないはずです。

- **検証しなさい**時でさえ**サーバ識別は**サプリカントで、SSL ハンドシェイク失敗するかもしれませんとき無効に なります* CN フィールドにあります。

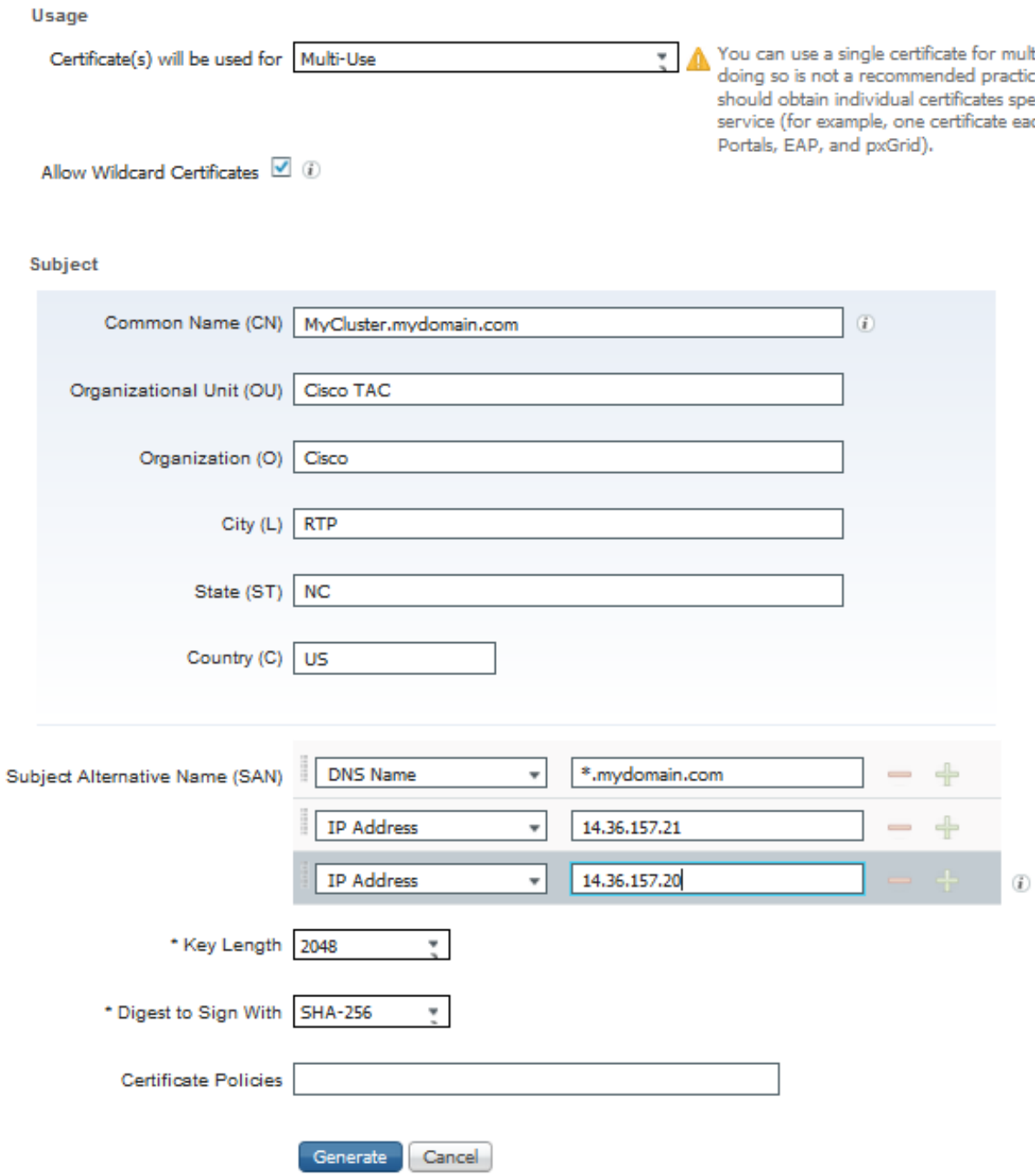
- その代り、ジェネリック FQDN は CN フィールドで使用しそれから ***.domain.com は**認証対象代替名（ SAN ） DNS名 フィールドで使用する**ことができます**。

  **注:** 一部の認証局（ CA ）は、CSR にワイルドカードが含まれていないとしても、証明書の CN に自動的にワイルドカード（ * ）を追加することがあります。 このシナリオではこの操作を防ぐために、特別な要求が上がるように必要となります。

個々のサーバ証明書 CSR の例

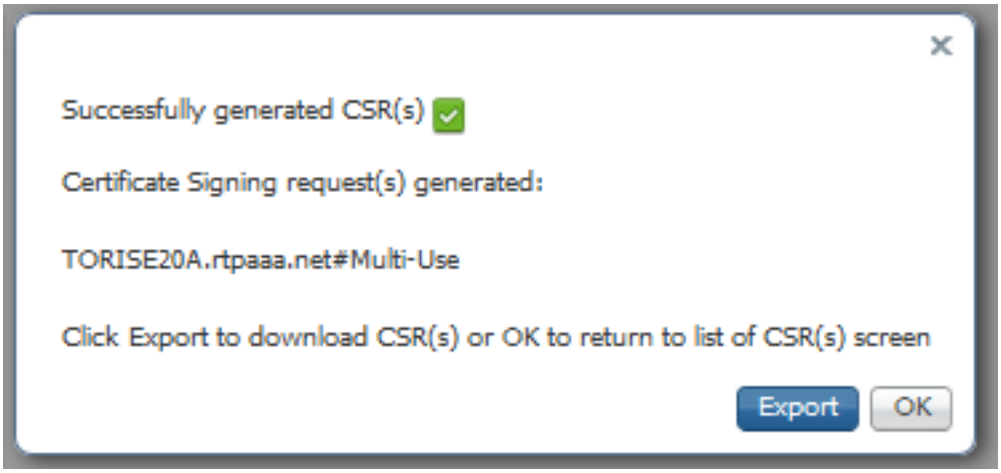



[ワイルドカード CSR の例]




**注:** 各 Deployment ノードの IP アドレスは SAN フィールドに IP アドレスによってサーバにアクセスするとき証明書警告を避けるために追加することができます。

CSR が作成されれば、ISE はそれをエクスポートするオプションのポップアップ ウィンドウを表示する。 CSR をエクスポートした後は、そのファイルを CA に送信して署名してもらう必要があります。




### ステップ 2.新しい証明書 チェーンをインポートして下さい。

認証局からは、完全な署名チェーン（ルート認証局/中間認証局）と併せて署名付きサーバ証明書が返されます。 証明書を受信した後尾は、次の手順に従って証明書を ISE サーバにインポートします。

1. CA によって提供されるルートおよび（または）中間証明書をインポートするために **Administration > 証明書 > 信頼できる証明書**にナビゲート して下さい。

2. サーバ証明をインポートするために、**Administration > 証明書 > 証明書署名要求**にナビゲート して下さい。

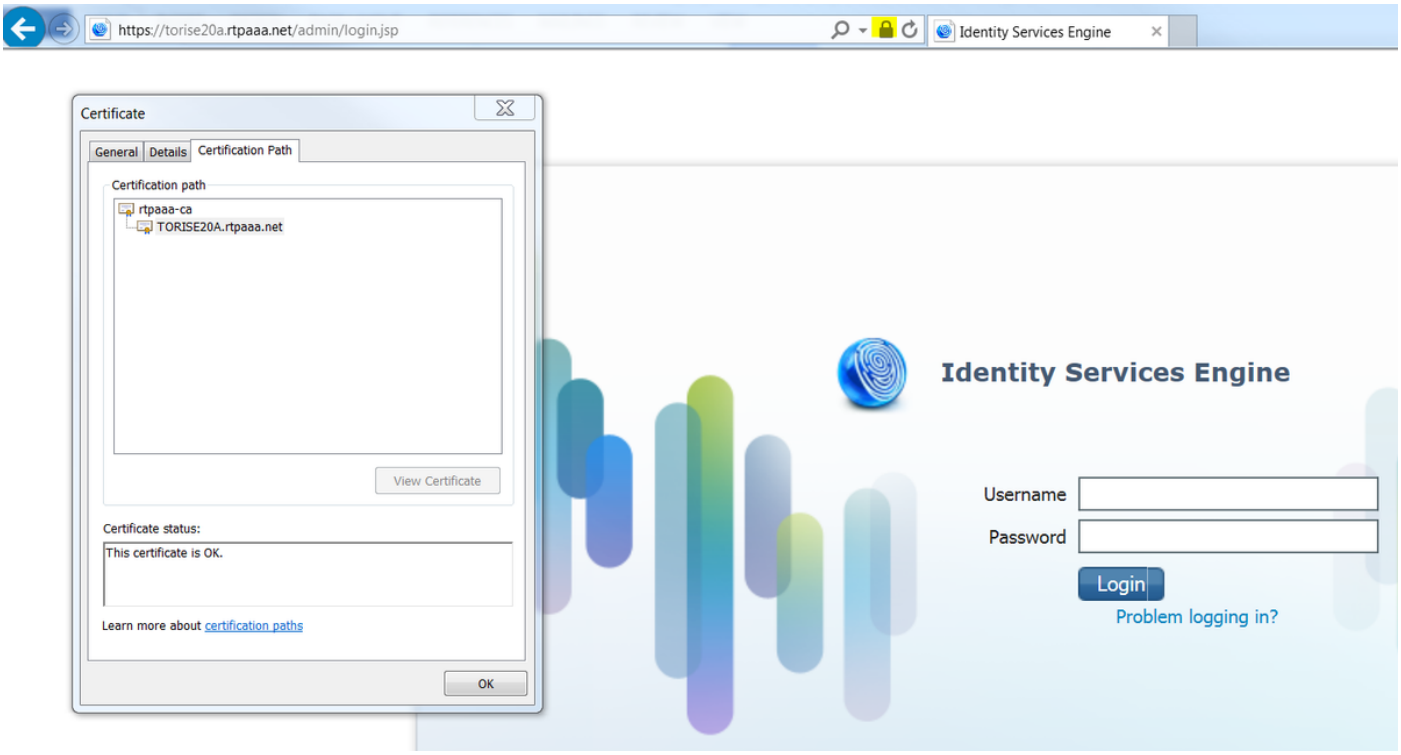
3. 前に作成した CSR を選択してから、[Bind Certificate] をクリックします。

4. 新しい証明書 位置を選択すれば ISE はデータベースで作成され、保存されるプライベートキーに証明書を結合 します。

   **注:** Admin 役割がこの証明書に選択される場合、ISE はサービスを再開します。

## 確認

照明書をインポートする際に管理ロールを選択した場合は、ブラウザに管理ページを読み込むことによって、新しい証明書を検証できます。 証明書チェーンが正しく構成されていて、その証明書チェーンがブラウザで信頼されている限り、ブラウザは新しい管理証明書を信頼するはずです。




さらに詳しく検証するには、ブラウザで南京錠シンボルを選択し、証明書パスに完全なチェーンが含まれていて、そのチェーンがマシンで信頼されていることを確認します。 これは、サーバが完全なチェーンを渡したことを直接示すことにはなりませんが、ブラウザがローカルの信頼ストアに基づいてサーバ証明書を信頼できることを示します。

# トラブルシューティング

## サプリカントは dot1x 認証の間に ISE ローカルサーバ 証明書を信頼しません

SSL ハンドシェーク プロセス中に ISE が完全な証明書チェーンを渡していることを確認します。

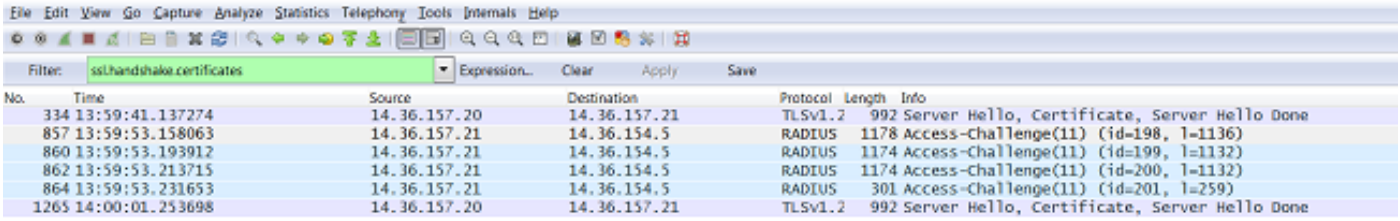
サーバ証明（すなわち PEAP）を必要とし、EAP メソッドを使用するとき ValidateServer **識別は**選択されます、サプリカントは認証プロセスの一部としてローカル信頼ストアで持っている証明書を使用して証明書 チェーンを検証します。 SSL ハンドシェイク プロセスの一部として、ISE はチェーンで現在の証明書およびまたルートおよび（または）中間証明書を示します。 チェーンが完全でないと、サプリカントはサーバ ID を検証できません。 次の手順に従うことで、証明書チェーンがクライアントに返されることを確認できます。

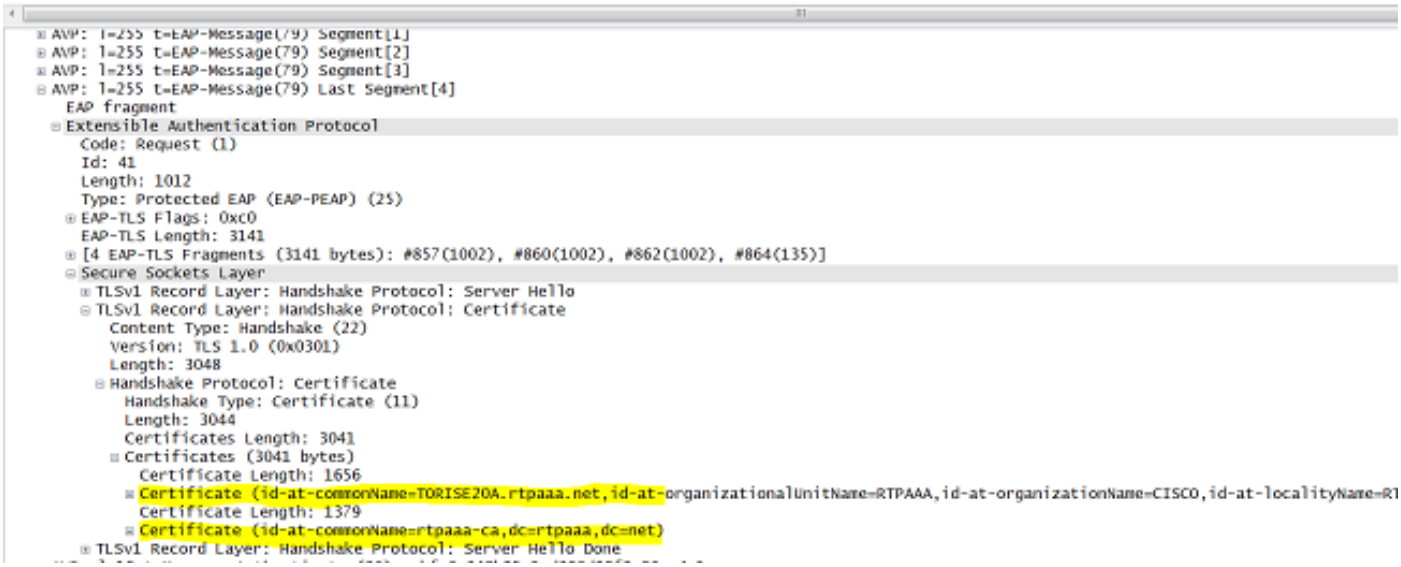
1. ISE （TCPDump）からのキャプチャを、ナビゲート **オペレーション > Diagostic ツール**に認証の間に連れて行くため **> 汎用ツール > TCP ダンプする**。

2. ダウンロードし、/キャプチャを開き、**Wireshark** のフィルタ **ssl.handshake.certificates** を適用し、アクセス チャレンジを**見つけて下さい**。

3. 選択されて **RADIUSプロトコル > 属性値ペア > EAP メッセージ最後セグメントを拡張するために、> Extensible Authentication Protocol（EAP） > Secure Sockets Layer > 証明書 > 証明書は**ナビゲート します。

以下に、キャプチャした証明書チェーンの例を示します。

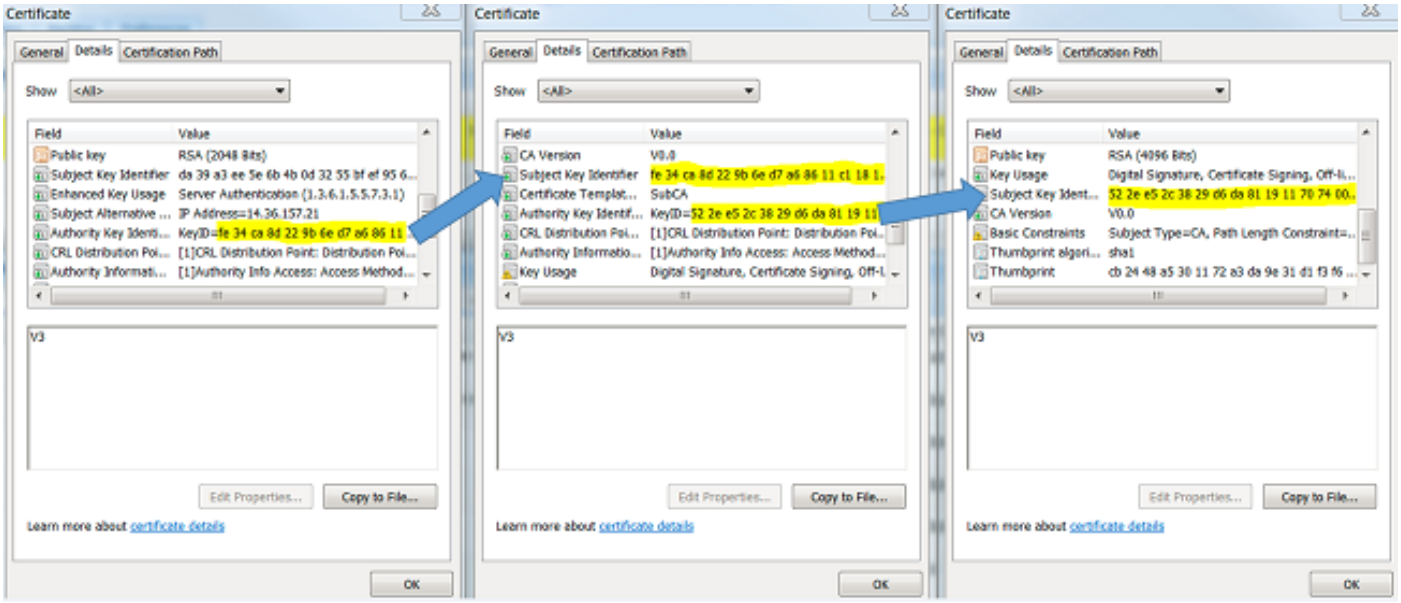



チェーンが不完全である場合、**ISE Administration > 証明書 > 信頼できる証明書**にナビゲート し、ルートおよび（または）中間証明書があることを確認して下さい。 証明書 チェーンが正常に渡される場合、チェーン自体は有効なとしてここに説明されている方式の使用によって確認する必要があります。

各証明書（サーバ、中間物およびルート）を開き、チェーンの次の証明書の権限キー 識別子（AKI）に各証明書の認証対象キー識別子（スキー）を一致させることによって信頼のチェーンを確認して下さい。

証明書 チェーンの例。

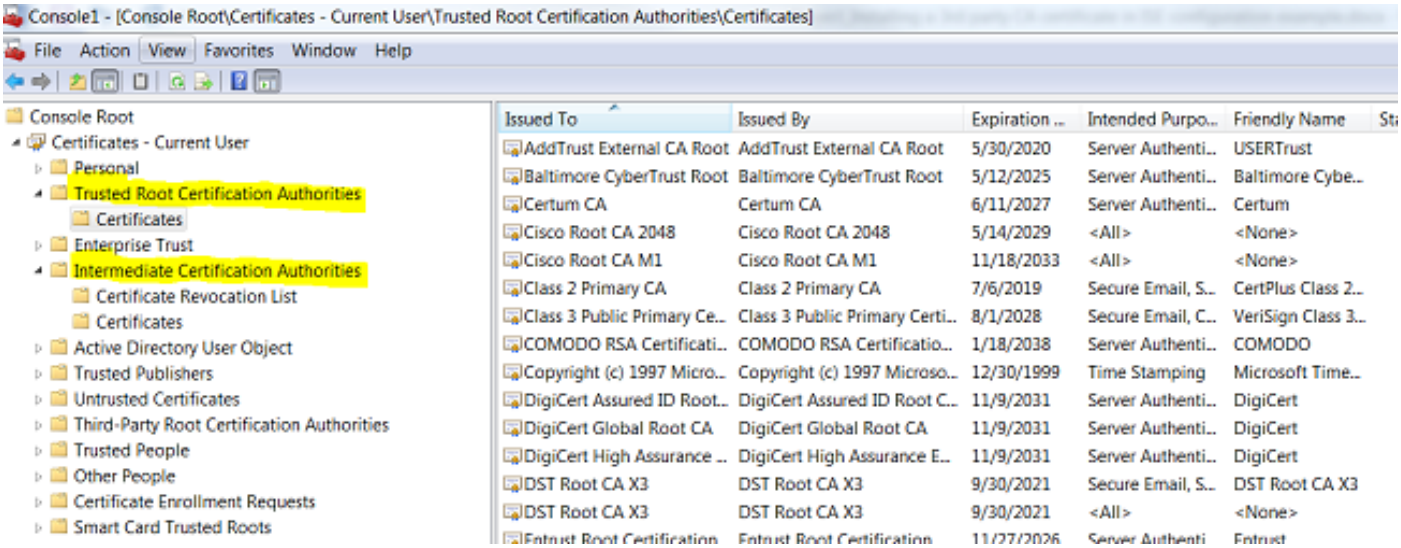



## ISE 証明書 チェーンは認証の間に正しいしかしエンドポイント リジェクト ISE サーバ証明です

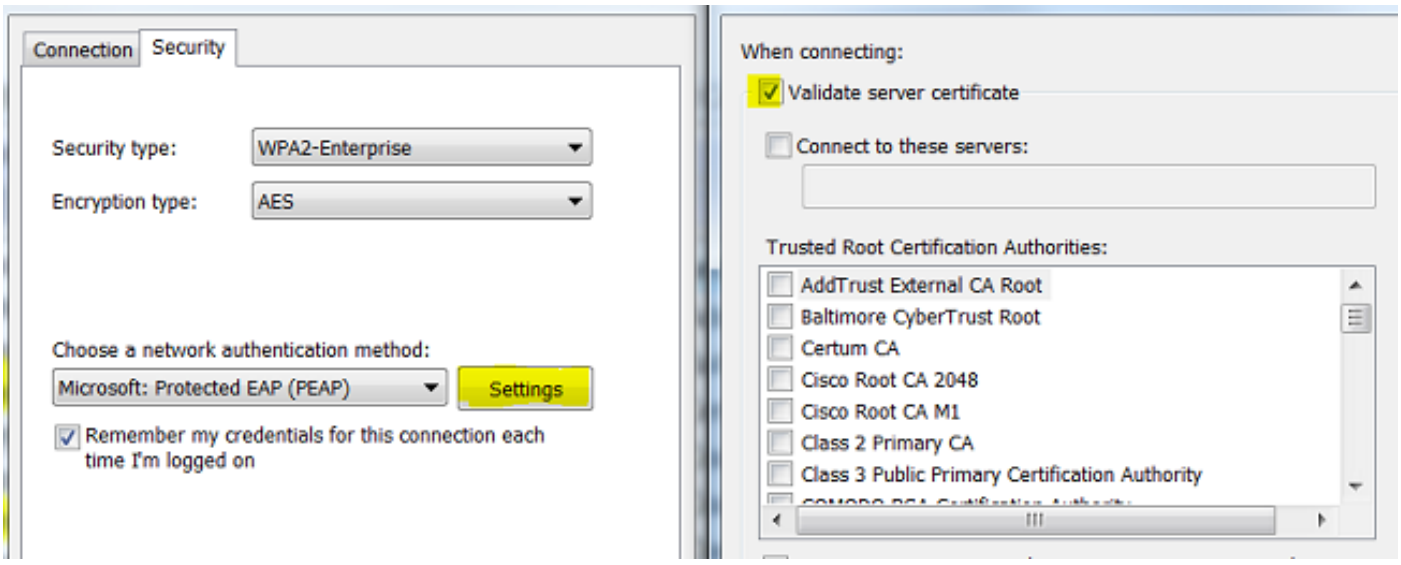
SSL ハンドシェーク中に ISE が完全な証明書チェーンを提示しているのにサプリカントがその証明書チェーンを拒否する場合は、 次のステップとして、ルート証明書と中間証明書のすべてがクライアントのローカル信頼ストアに存在することを確認します。

これを、ナビゲート **mmc.exe ファイル > Add Remove Snap-In** に Windows デバイスから確認するため。 利用可能 なスナップ ins カラム**から** Certificatesand を『Add』 をクリック します選択して下さい。 Myuser **アカウントか** computeraccount を使用中の認証種別**によって**（ユーザかマシン）**選択し、**次に『OK』 をクリック して下さい。

コンソール ビューの下で、**信頼できるルート認証機関**および**中間認証局（CA）を**ローカル信頼ストアのルートおよび中間物証明書の存在を確認するために選択して下さい。




これがサーバ識別チェック問題であることを確認する簡単な方法はサプリカント プロファイル設定の下で、**検証し、サーバ証明を**再度テストしますチェックを外します。




**注:** ISE はシグニチャ アルゴリズムとして RSASSA-PSS を使用して現在 証明書の処理をサポートしません。 これにはサーバ証明、ルート、中間物またはクライアント 認証（すなわち TLS、PEAP（TLS）、等）が含まれています。 バグ CSCug22137 を参照してください。

# 関連情報

- Cisco Identity Services Engine 管理者ガイド リリース 2.0
- テクニカル サポートとドキュメント – Cisco Systems