ISEでのサードパーティCA署名付き証明書のインストール

内容

はじめに

このドキュメントでは、サードパーティの認証局(CA)によって署名された証明書をCisco Identity Services Engine(ISE)にインストールする方法について説明します。

前提条件

要件

Basic Public Key Infrastructureに関する基本的な知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、Cisco Identity Services Engine(ISE)リリース3.0に基づくものです。同じ設定がリリース2.Xにも適用されます

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。

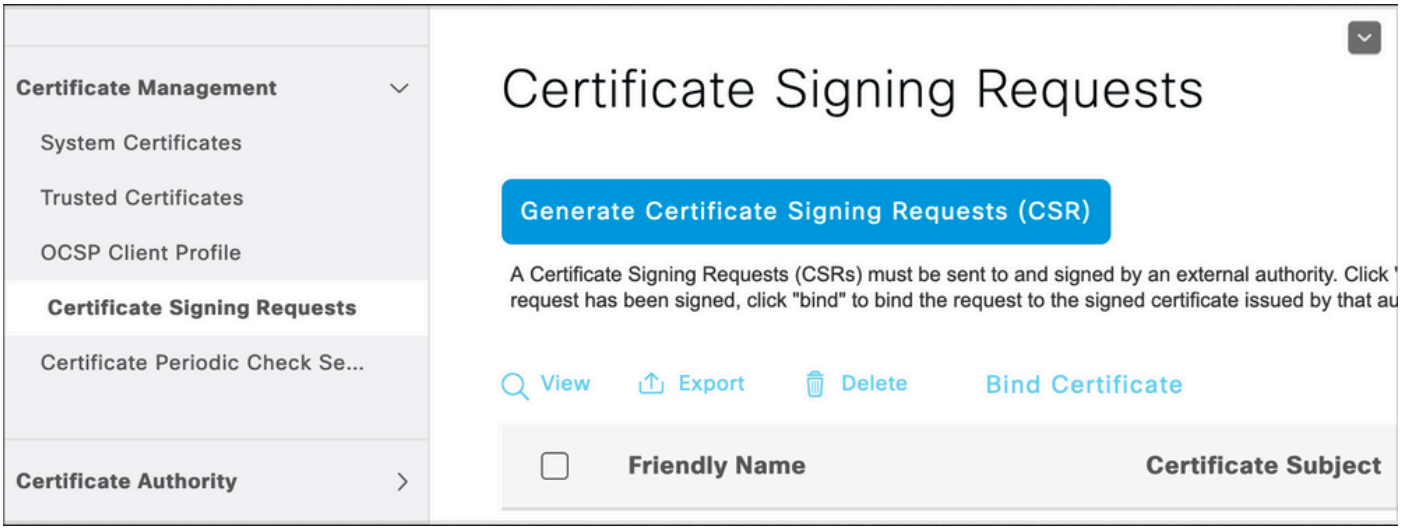
背景説明

このプロセスは、最終的な証明書ロール（EAP認証、ポータル、管理者、およびpxGrid）に関係なく同じです。

設定

ステップ 1：証明書署名要求(CSR)の生成

CSRを生成するには、Administration > Certificates > Certificate Signing Requestsの順に移動し、Generate Certificate Signing Requests (CSR)をクリックします。



1. Usageセクションで、ドロップダウンメニューから使用するロールを選択します。証明書が複数のロールに使用されている場合は、[多用途]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. 証明書を生成できる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)フィールドで、ISEはノードの完全修飾ドメイン名(FQDN)を自動的に入力します。

ワイルドカード：

- ワイルドカード証明書を生成する場合は、Allow Wildcard Certificatesボックスにチェックマークを入れます。

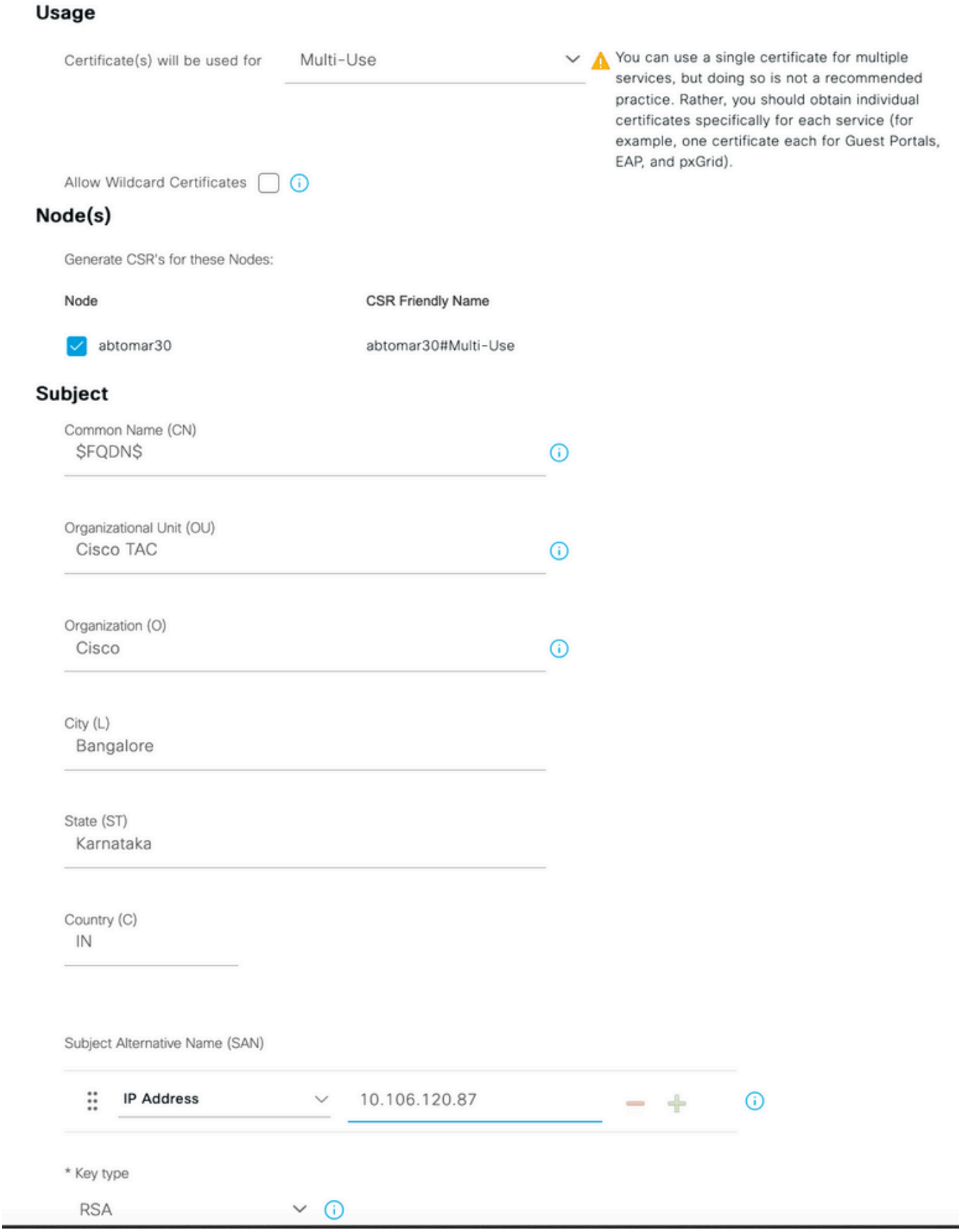
- 証明書がEAP認証に使用される場合、Windowsサプリカントはサーバ証明書を拒否するため、サブジェクトCNフィールドに*記号を入れないでください。

- サプリカントでValidate Server Identityが無効になっている場合でも、CNフィールドに*があると、SSLハンドシェイクが失敗する可能性があります。

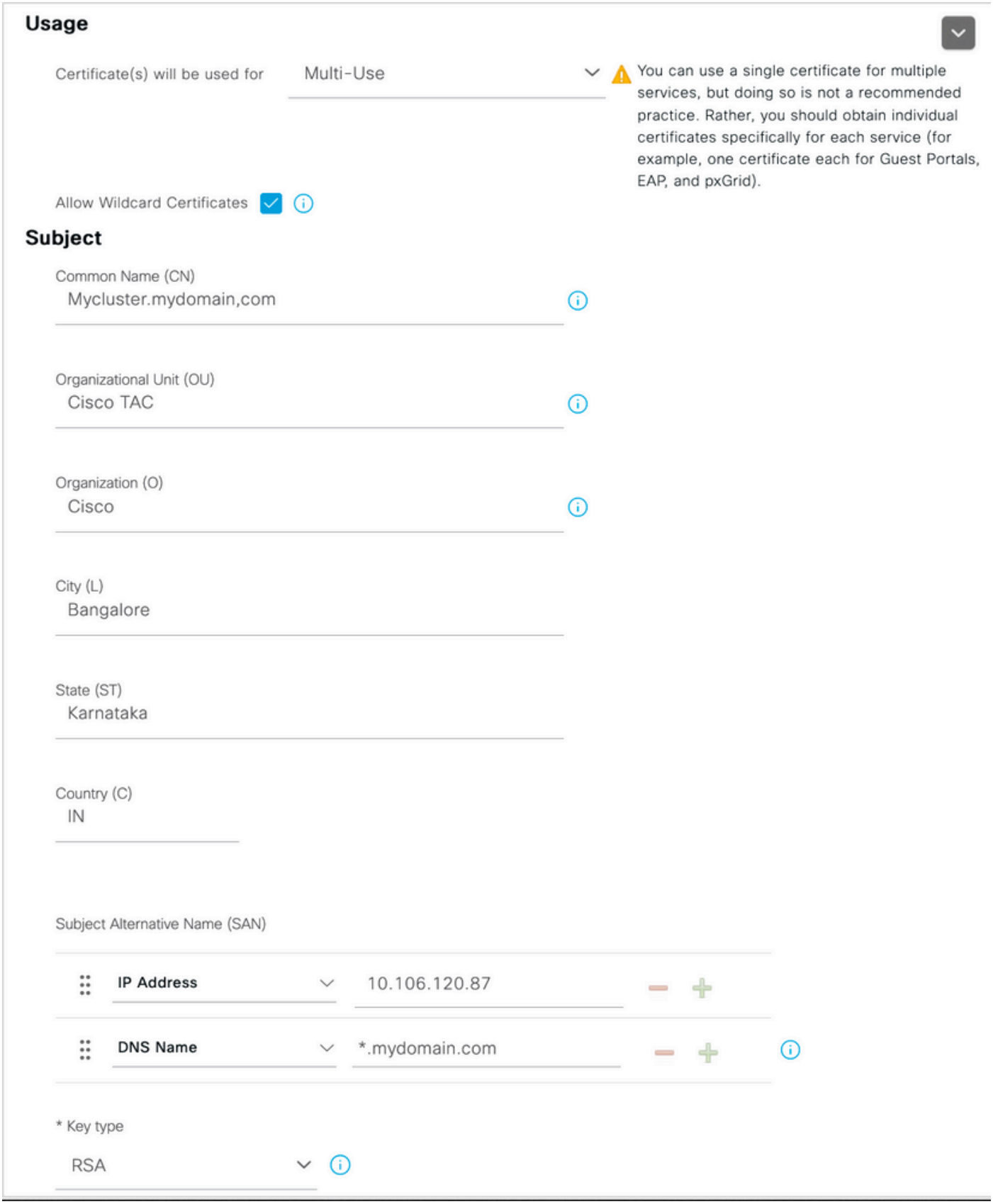
- 代わりに、汎用FQDNをCNフィールドで使用し、次にサブジェクト代替名(SAN)のDNS名フィールドでを使用すること***.domain.com**ができます。

注：一部の認証局(CA)は、CSRにワイルドカード(*)が存在しなくても、証明書のCNにワイルドカードを自動的に追加できます。このシナリオでは、このアクションを防ぐために特別な要求を発行する必要があります。

個々のサーバ証明書 CSR の例



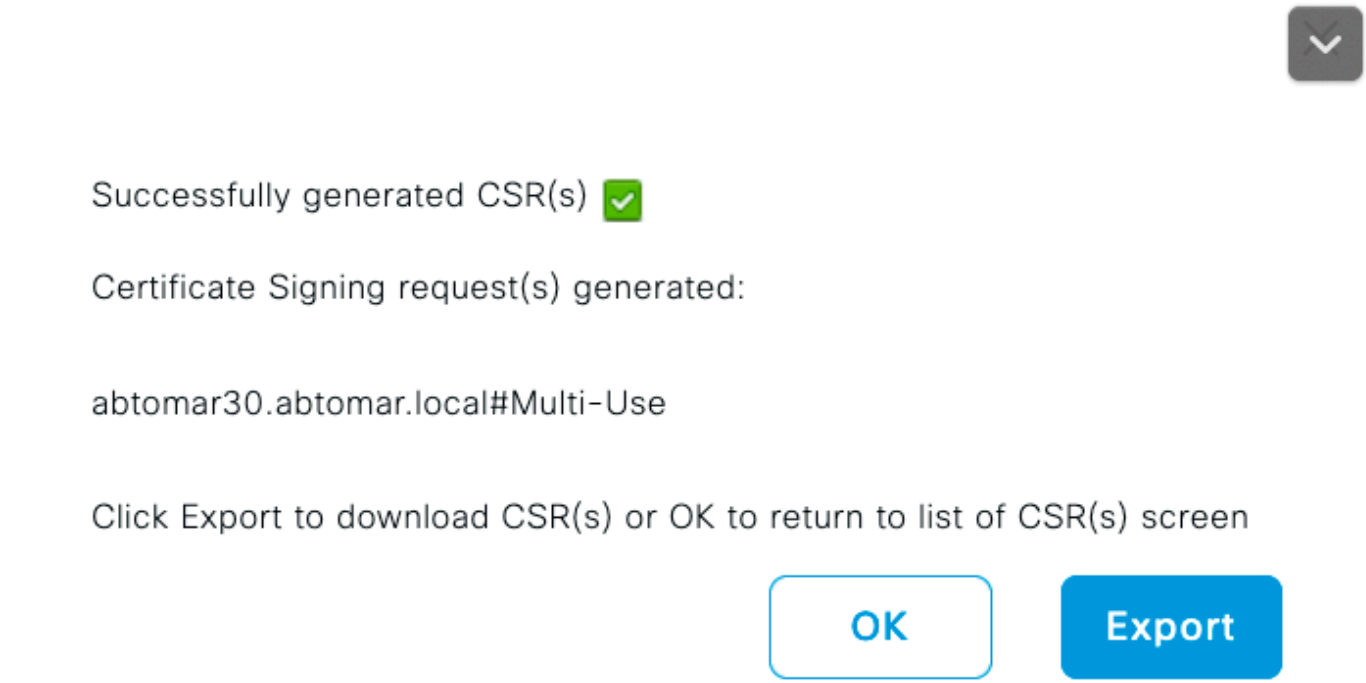
ワイルドカード CSR の例



注：各導入ノードのIPアドレスをSANフィールドに追加すると、IPアドレスを使用してサーバにアクセスする際に証明書の警告が表示されるのを回避できます。

CSRが作成されると、ISEにポップアップウィンドウが表示され、CSRをエクスポートするオプションが表示されます。 エクスポートした後、このファイルは署名のためにCAに送信する必要

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ます。

認証局(CA)は、完全な証明書チェーン（ルート/中間）とともに署名付きサーバ証明書を返します。証明書を受け取ったら、次の手順を実行して証明書をISEサーバにインポートします。

1. CAから提供されたルートおよび（または）中間証明書をインポートするには、Administration > Certificates > Trusted Certificatesの順に移動します。

2. Importをクリックし、ルート証明書または中間証明書（あるいはその両方）を選択し、送信に適用される関連するチェックボックスを選択します。
3. サーバ証明書をインポートするには、Administration > Certificates > Certificate Signing Requestsの順に移動します。

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

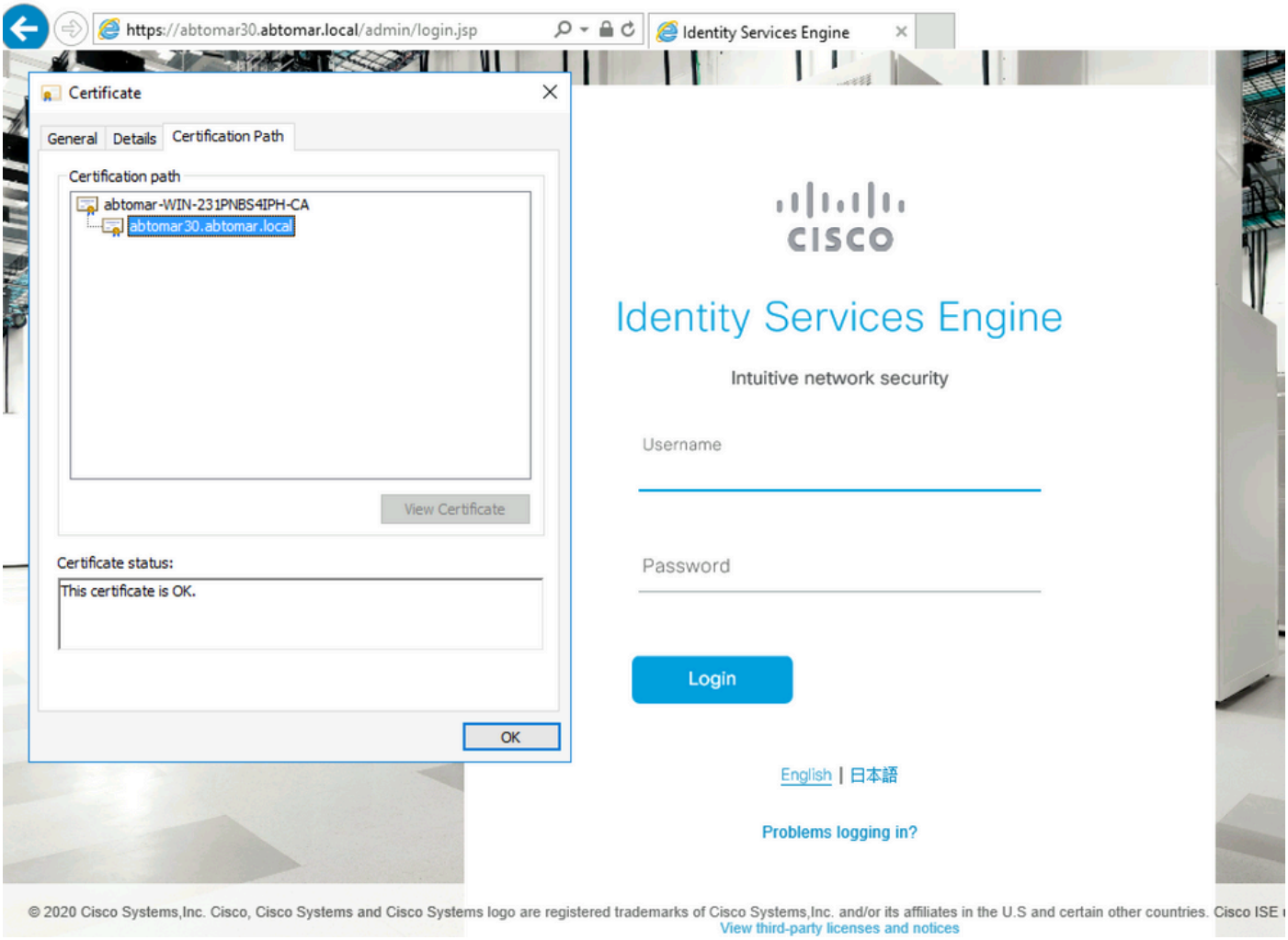
5. 新しい証明書の場所を選択すると、ISEはデータベースに作成および保存された秘密キーに証明書をバインドします。

注：この証明書に対して管理者ロールが選択されている場合、特定のISEサーバサービスが再起動します。

注意：インポートされた証明書が展開のプライマリ管理ノード用であり、管理者ロールが選択されている場合、すべてのノードのサービスが次々に再起動されます。これは予期された動作であり、このアクティビティを実行するにはダウンタイムが推奨されます。

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。チェーンが正しく構築されていて、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必要があります。



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。

トラブルシュート

dot1x認証中にサプリカントがISEローカルサーバ証明書を信頼しない

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。

サーバ証明書を必要とするEAP方式(PEAP)と[サーバIDの検証] を選択した場合、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にある証明書を使用して証明書チェーンを検証し

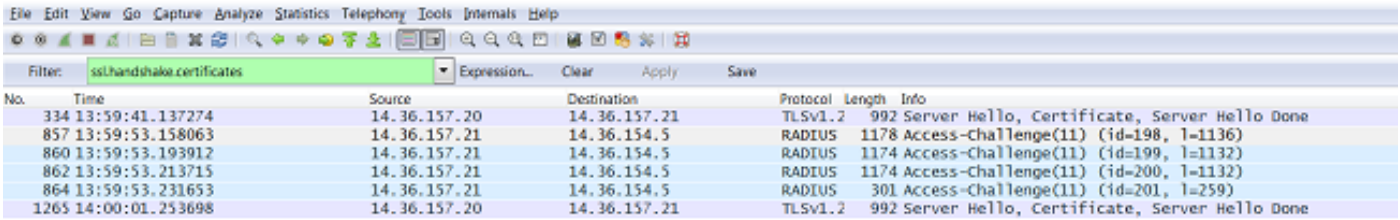
ます。SSLハンドシェイクプロセスの一部として、ISEは自身の証明書を提示し、チェーンに含まれるルート証明書や中間証明書も提示します。チェーンが完全でないと、サプリカントはサーバ ID を検証できません。証明書チェーンがクライアントに返されていることを確認するには、次の手順を実行します。

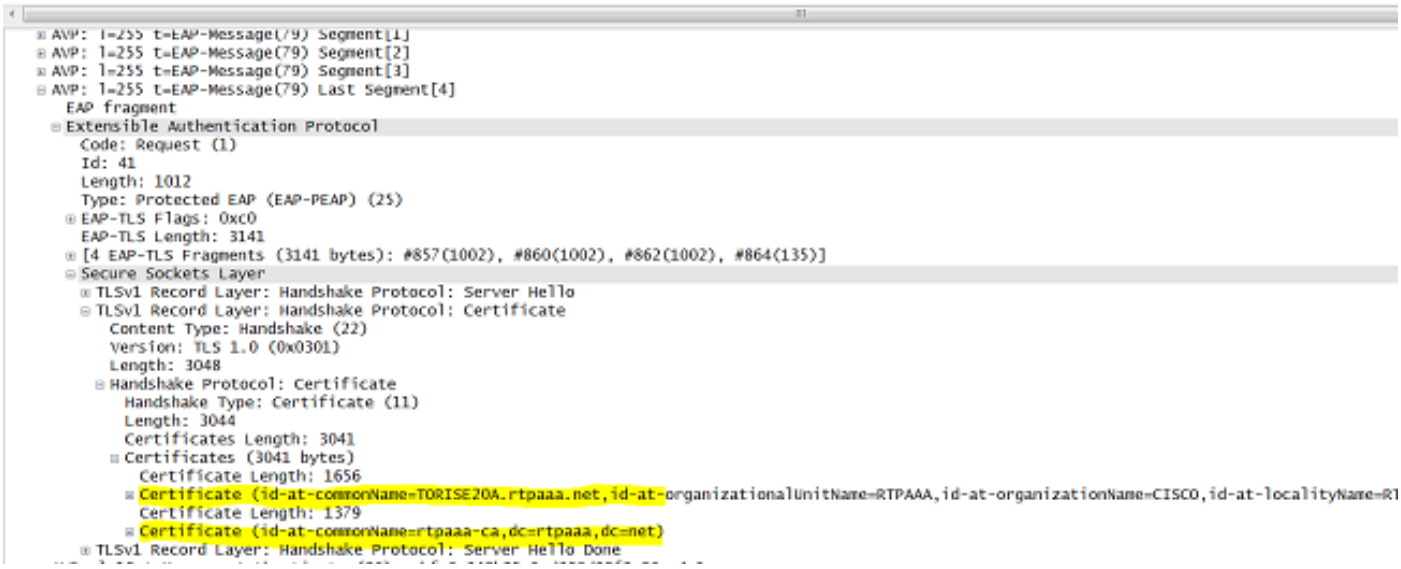
1. 認証中にISE(TCPDump)からキャプチャを取得するには、Operations > Diagnostic Tools > General Tools > TCP Dumpの順に移動します。

2. Wiresharkでキャプチャをダウンロードして開き、フィルタssl.handshake.certificatesを適用して、アクセスチャレンジを見つけます。

3. 選択したら、Expand Radius Protocol > Attribute Value Pairs > EAP-Message Last segment > Extensible Authentication Protocol > Secure Sockets Layer > Certificate > Certificatesの順に選択します。

以下に、キャプチャした証明書チェーンの例を示します。

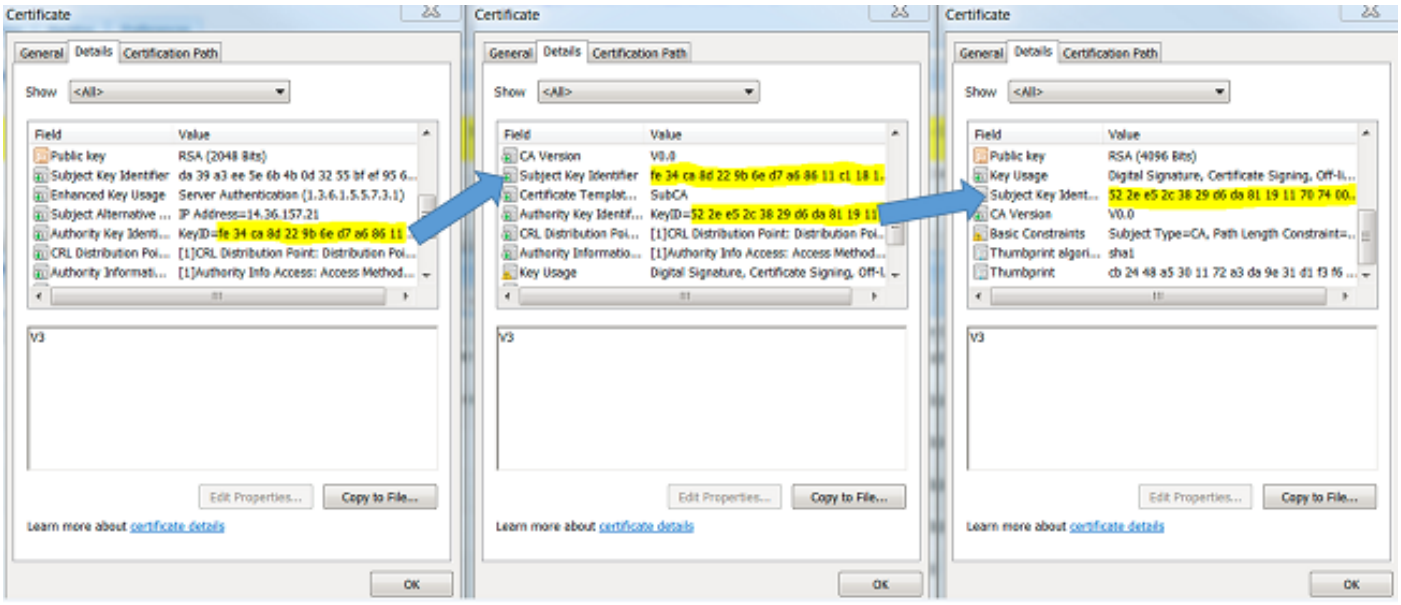




チェーンが不完全な場合は、ISE Administration > Certificates > Trusted Certificatesの順に移動し、ルート証明書および（または）中間証明書が存在することを確認します。証明書チェーンが正常に渡された場合は、ここで説明する方法を使用して、チェーン自体が有効であることを確認する必要があります。

各証明書（サーバ、中間、およびルート）を開き、各証明書のSubject Key Identifier(SKI)を、チェーン内の次の証明書のAuthority Key Identifier(AKI)と照合して、信頼のチェーンを確認します。

証明書チェーンの例。

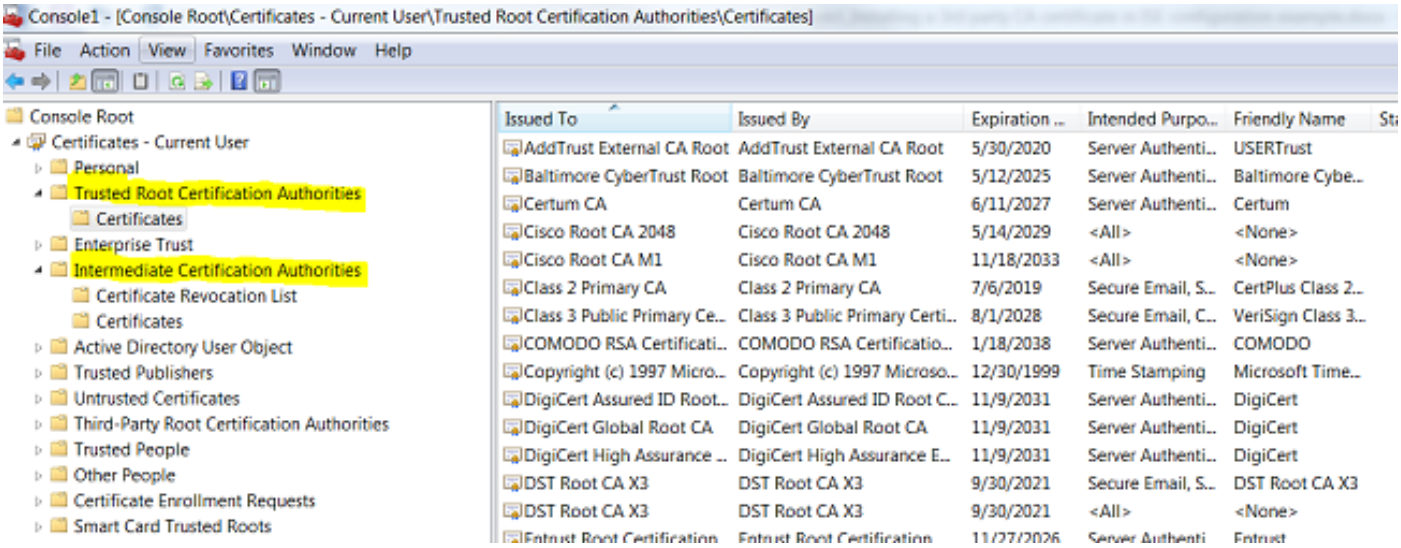


ISE証明書チェーンは正しいが、認証中にエンドポイントがISEサーバ証明書を拒否する

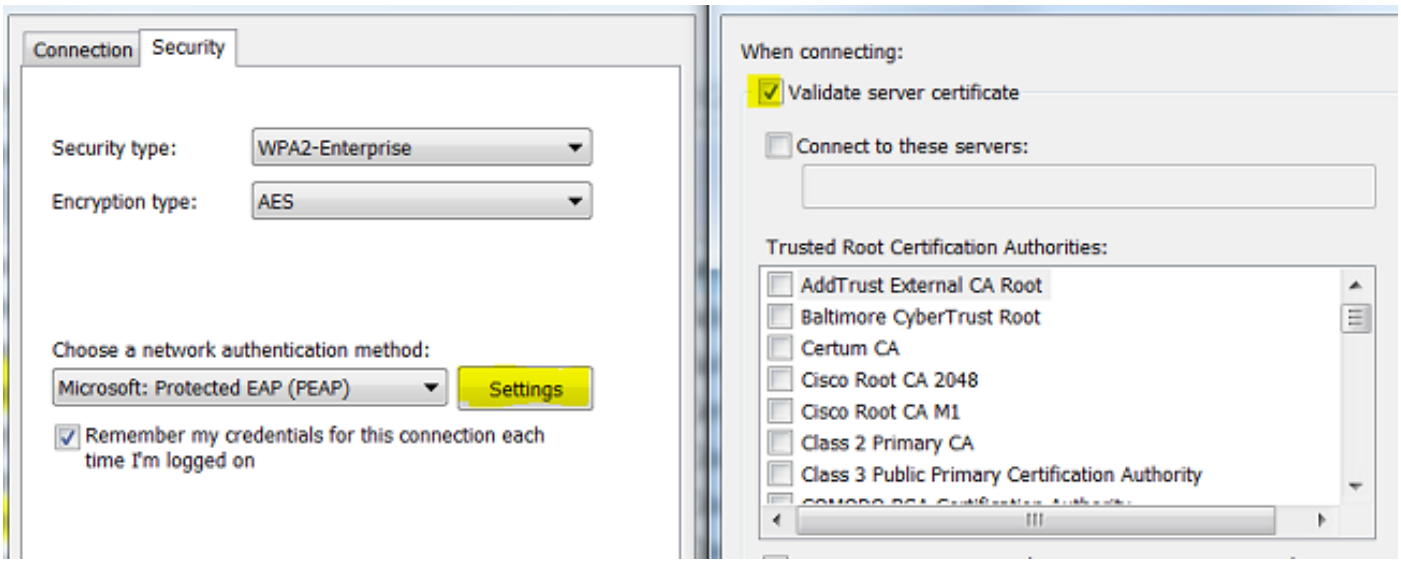
SSLハンドシェイク中にISEが完全な証明書チェーンを提示し、サプリカントが引き続き証明書チェーンを拒否する場合は、次の手順で、ルート証明書および（または）中間証明書がクライアントのローカル信頼ストアにあることを確認します。

Windowsデバイスからこれを確認するには、mmc.exe File > Add-Remove Snap-inに移動します。Available snap-ins列からCertificatesを選択し、Addをクリックします。使用している認証タイプ（ユーザまたはマシン）に応じて、My user accountまたはcomputer accountのいずれかを選択し、OKをクリックします。

コンソールビューでTrusted Root Certification AuthoritiesとIntermediate Certification Authoritiesを選択し、ローカルの信頼ストアにルート証明書と中間証明書が存在することを確認します。



これがサーバIDチェックの問題であることを確認する簡単な方法として、サプリカントプロファイル設定でValidate Server Certificateのチェックマークを外して、もう一度テストします。



関連情報

- Cisco Identity Services Engine 管理者ガイド リリース 3.0
- 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。