Installer un certificat tiers signé par une autorité de certification dans ISE

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Configurer

- Étape 1. Générer une demande de signature de certificat (CSR).
- Étape 2. Importer une nouvelle chaîne de certificats.

Vérifier

Dépannage

- Le demandeur n'approuve pas le certificat du serveur local ISE pendant une authentification dot1x
- La chaîne de certificats ISE est correcte, mais le terminal rejette le certificat du serveur ISE pendant l'authentification

Informations connexes

Introduction

Ce document décrit comment installer un certificat signé par une autorité de certification (CA) tierce dans Cisco Identity Services Engine (ISE).

Conditions préalables

Exigences

Cisco vous recommande de connaître l'infrastructure à clé publique de base.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Identity Services Engine (ISE) version 3.0. La même configuration s'applique aux versions 2.X

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

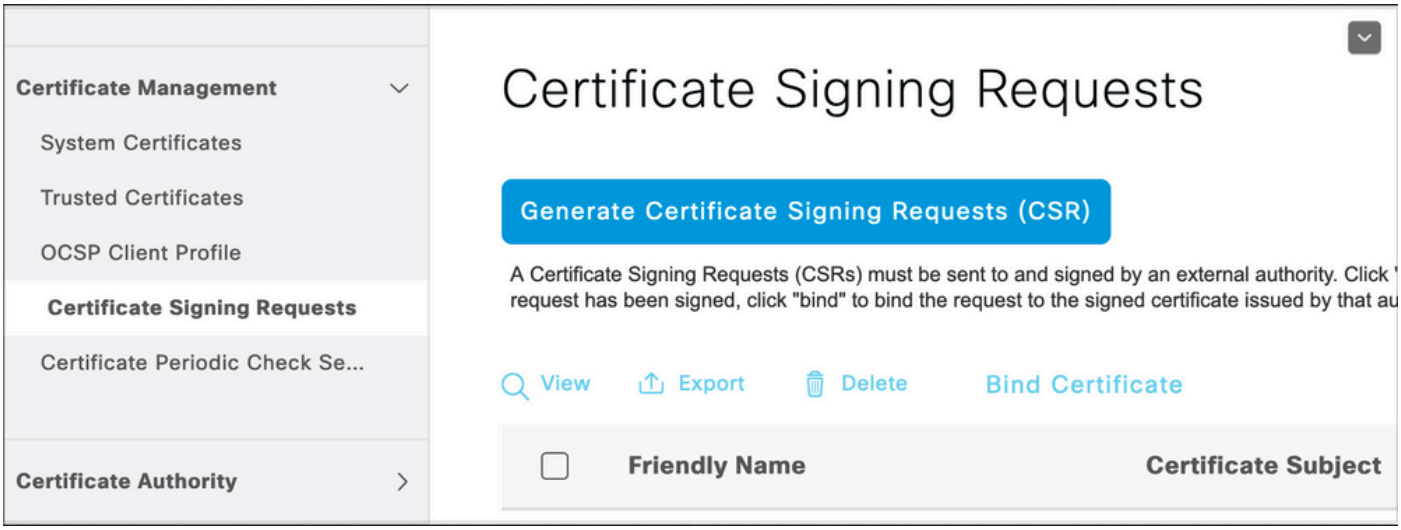
Informations générales

Ce processus est le même quel que soit le rôle de certificat final (authentification EAP, Portal, Admin et pxGrid).

Configurer

Étape 1. Générer une demande de signature de certificat (CSR).

Afin de générer le CSR, accédez à Administration > Certificates > Certificate Signing Requests et cliquez sur Generate Certificate Signing Requests (CSR).



1. Dans la section Utilisation, sélectionnez le rôle à utiliser dans le menu déroulant. Si le certificat est utilisé pour plusieurs rôles, vous pouvez sélectionner Multi-use. Une fois le certificat généré, les rôles peuvent être modifiés si nécessaire.

2. Sélectionnez le noeud pour lequel le certificat peut être généré.

3. Renseignez les informations nécessaires (Unité organisationnelle, Organisation, Ville, État et Pays).

Remarque : dans le champ Common Name (CN), ISE renseigne automatiquement le nom de domaine complet (FQDN) du noeud.

Caractères génériques :

- Si l'objectif est de générer un certificat générique, cochez la case Allow Wildcard Certificates.

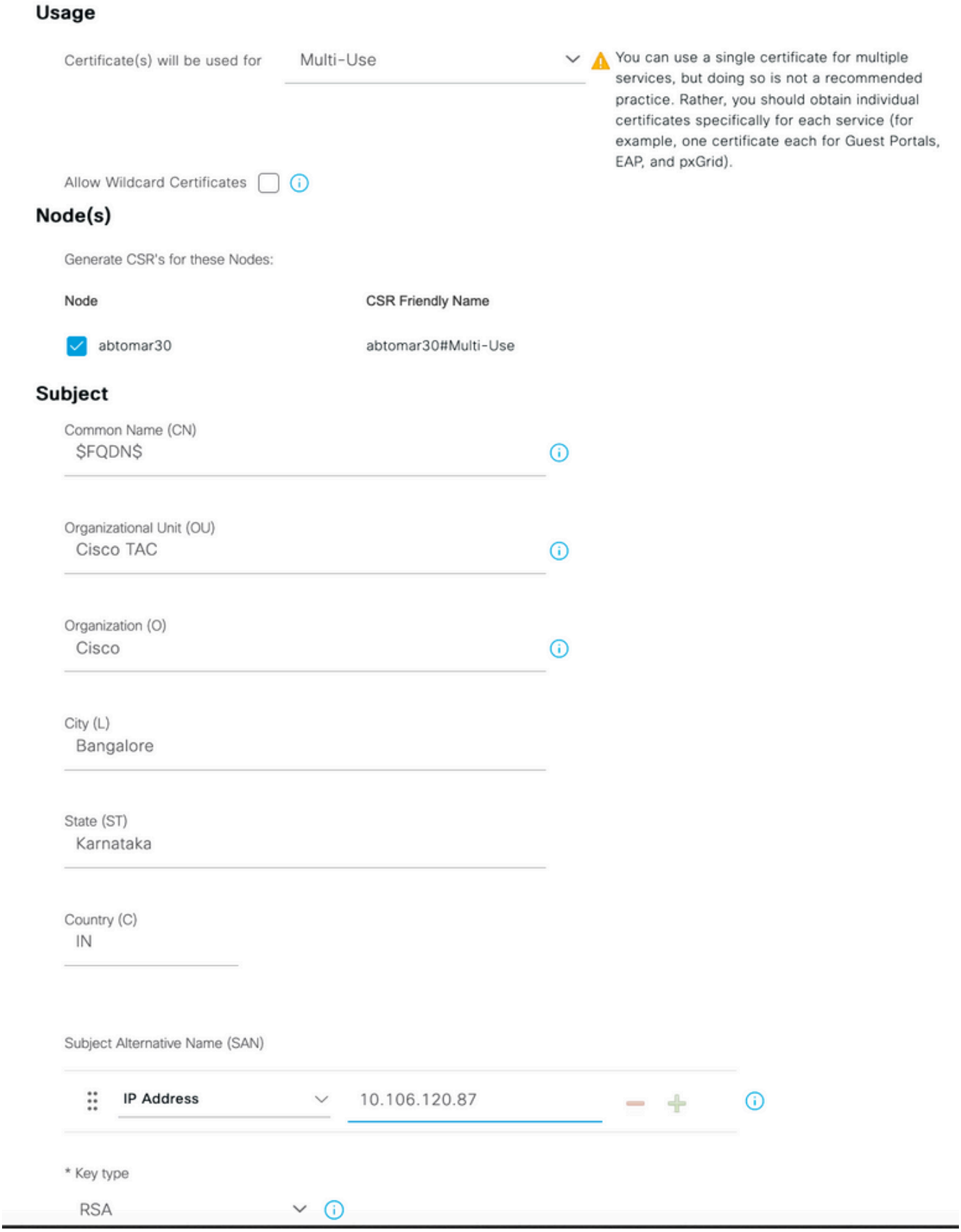
- Si le certificat est utilisé pour les authentifications EAP, le symbole * ne doit pas être dans le champ Objet CN car les demandeurs Windows rejettent le certificat du serveur.

- Même lorsque la validation de l'identité du serveur est désactivée sur le demandeur, la connexion SSL peut échouer lorsque le * est dans le champ CN.

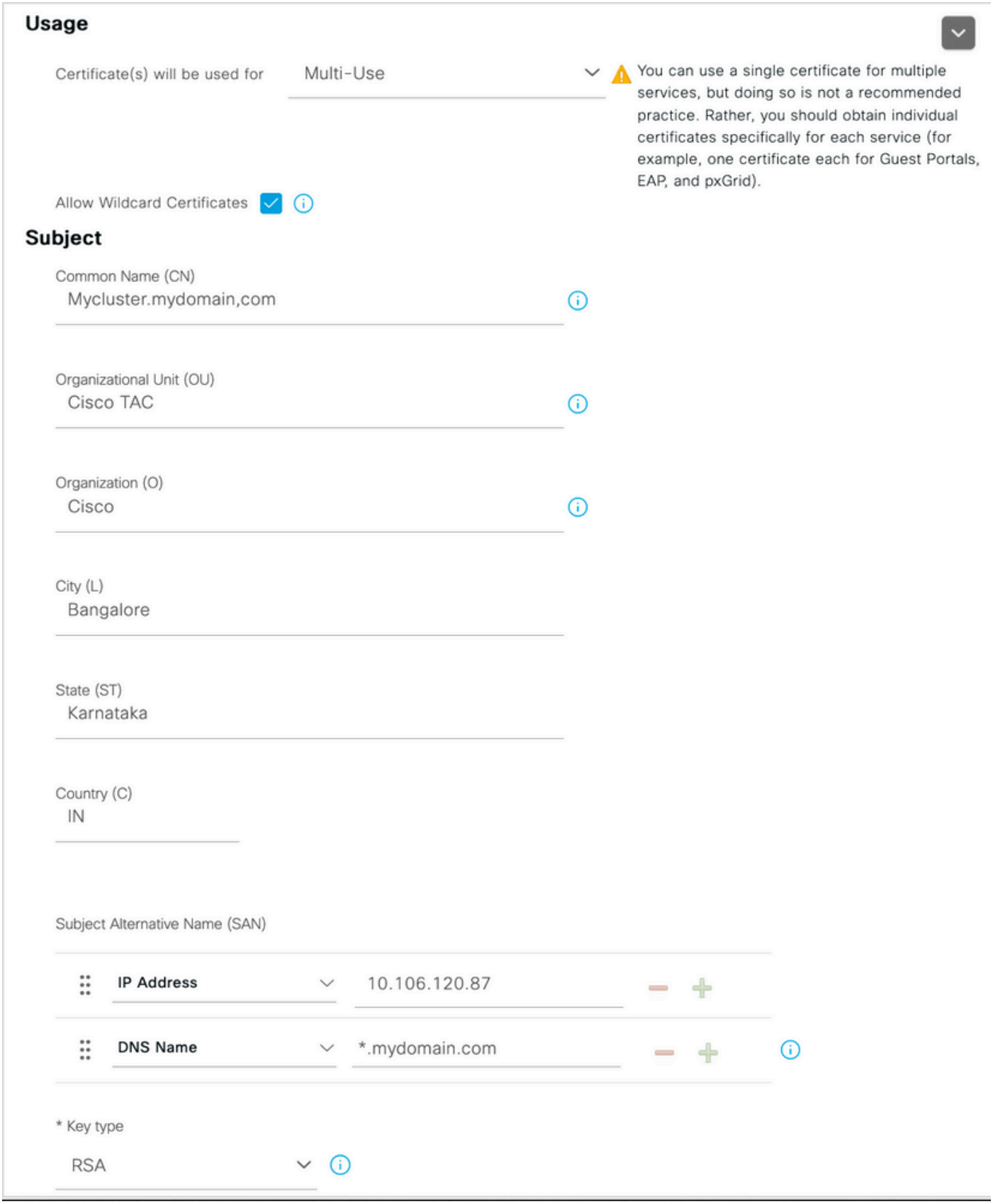
- À la place, un nom de domaine complet générique peut être utilisé dans le champ CN, puis le ***.domain.com** peut être utilisé dans le champ Nom DNS alternatif du sujet (SAN).

Remarque : certaines autorités de certification peuvent ajouter automatiquement le caractère générique (*) dans le CN du certificat, même s'il n'est pas présent dans le CSR. Dans ce scénario, une demande spéciale doit être émise pour empêcher cette action.

Exemple de certificat CSR de serveur individuel :

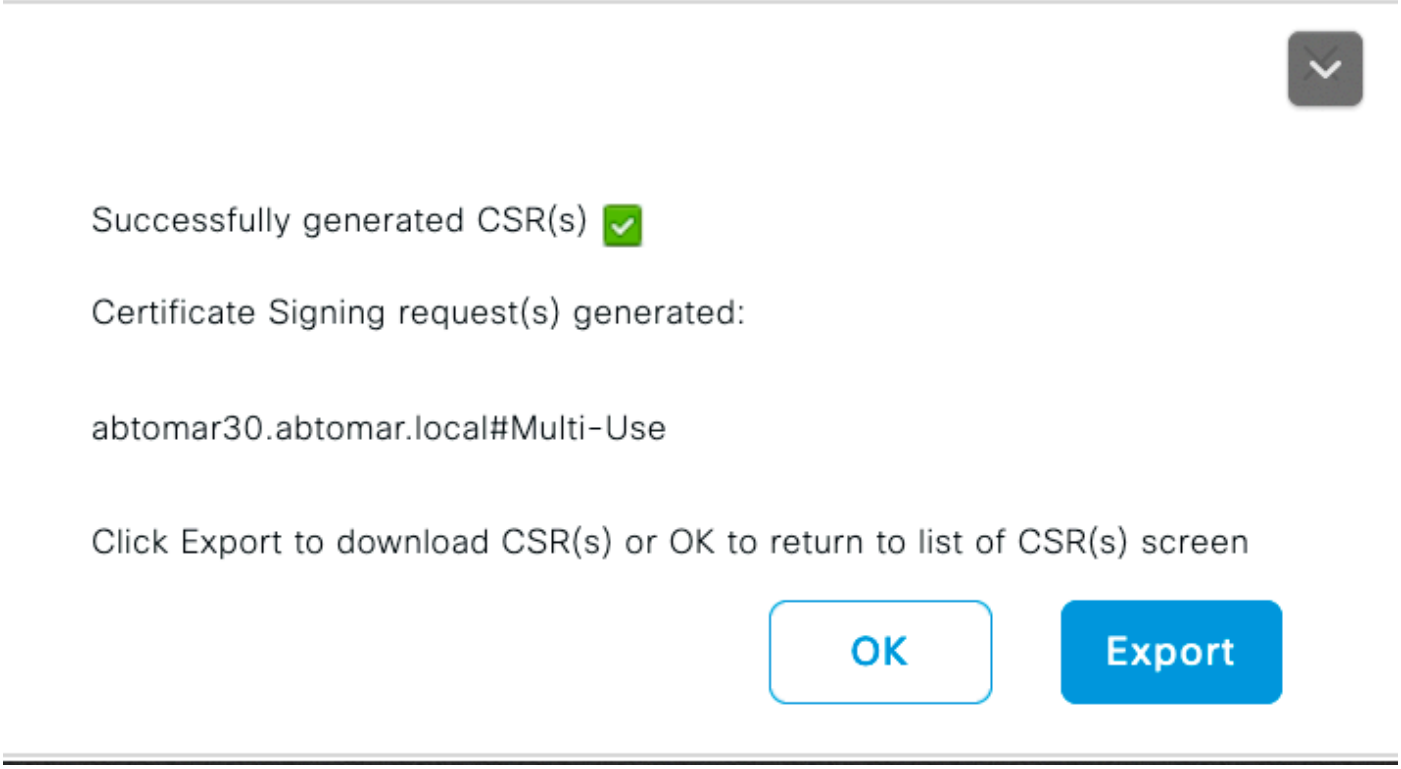


Exemple de CSR générique :



Remarque : chaque adresse IP de noeud de déploiement peut être ajoutée au champ SAN pour éviter un avertissement de certificat lorsque vous accédez au serveur via l'adresse IP.

Une fois le CSR créé, ISE affiche une fenêtre contextuelle avec l'option de l'exporter. Une fois exporté, ce fichier doit être envoyé à l'autorité de certification pour signature.



Étape 2. Importer une nouvelle chaîne de certificats.

L'autorité de certification renvoie le certificat de serveur signé avec la chaîne de certificats complète (racine/intermédiaire). Une fois reçus, procédez comme suit pour importer les certificats dans votre serveur ISE :

1. Afin d'importer tout certificat racine et (ou) intermédiaire fourni par l'autorité de certification, naviguez vers Administration > Certificates > Trusted Certificates.

2. Cliquez sur Import, puis sélectionnez le certificat racine et/ou le certificat intermédiaire et cochez les cases appropriées telles qu'elles ont été appliquées pour l'envoi.
3. Afin d'importer le certificat du serveur, naviguez à Administration > Certificates > Certificate Signing Requests.

4. Sélectionnez le CSR précédemment créé et cliquez sur Bind Certificate.

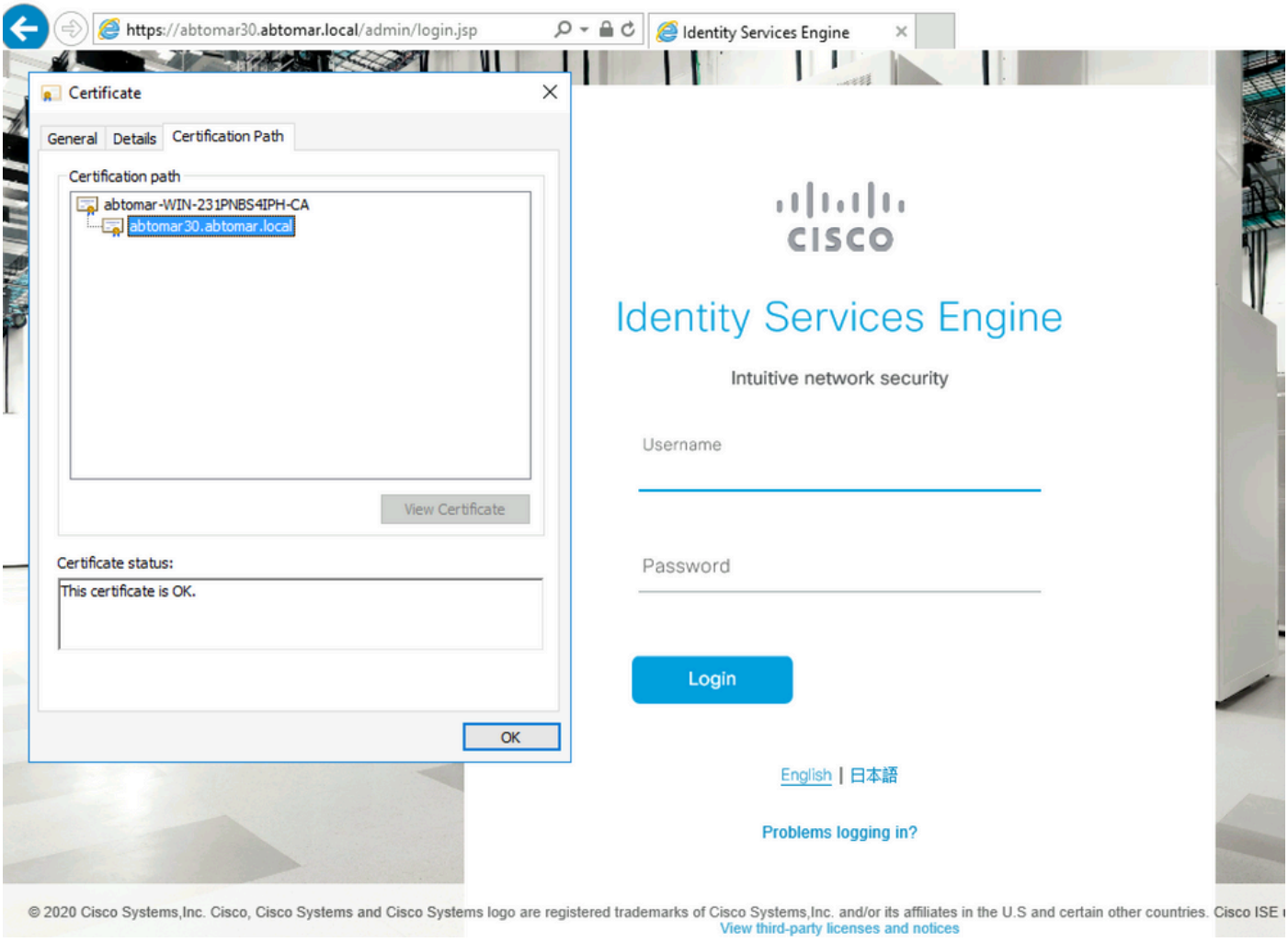
5. Sélectionnez le nouvel emplacement du certificat et ISE lie le certificat à la clé privée créée et stockée dans la base de données.

Remarque : si le rôle admin a été sélectionné pour ce certificat, les services du serveur ISE spécifiques redémarrent.

Attention : si le certificat importé est destiné au noeud d'administration principal du déploiement et si le rôle Admin est sélectionné, les services sur tous les noeuds redémarrent l'un après l'autre. Ceci est prévu et une interruption est recommandée pour effectuer cet exercice.

Vérifier

Si le rôle admin a été sélectionné lors de l'importation du certificat, vous pouvez vérifier que le nouveau certificat est en place en chargeant la page admin dans le navigateur. Le navigateur doit faire confiance au nouveau certificat d'administration tant que la chaîne a été créée correctement et si la chaîne de certificats est approuvée par le navigateur.



Pour une vérification supplémentaire, sélectionnez le symbole de verrouillage dans le navigateur et, sous le chemin d'accès du certificat, vérifiez que la chaîne complète est présente et approuvée par la machine. Il ne s'agit pas d'un indicateur direct indiquant que la chaîne complète a été transmise correctement par le serveur, mais d'un indicateur du navigateur capable d'approuver le certificat du serveur sur la base de son magasin d'approbation local.

Dépannage

Le demandeur n'approuve pas le certificat du serveur local ISE pendant une authentification dot1x

Vérifiez qu'ISE passe la chaîne de certificats complète pendant le processus d'échange SSL.

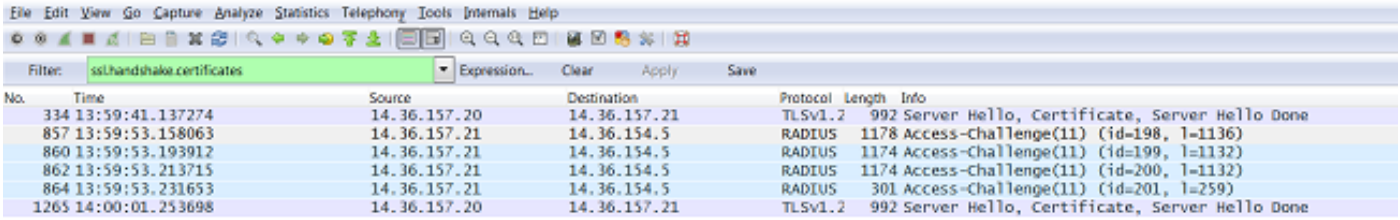
Lorsque vous utilisez des méthodes EAP qui nécessitent un certificat de serveur (c'est-à-dire, PEAP) et que l'option Valider l'identité du serveur est sélectionnée, le demandeur valide la chaîne de certificats en utilisant les certificats qu'il a dans son magasin d'approbation local dans le cadre du processus d'authentification. Dans le cadre du processus de connexion SSL, ISE présente son certificat ainsi que tous les certificats racine et (ou) intermédiaires présents dans sa chaîne. Le demandeur ne pourra pas valider l'identité du serveur si la chaîne est incomplète. Pour vérifier que la chaîne de certificats est renvoyée à votre client, vous pouvez effectuer les étapes suivantes :

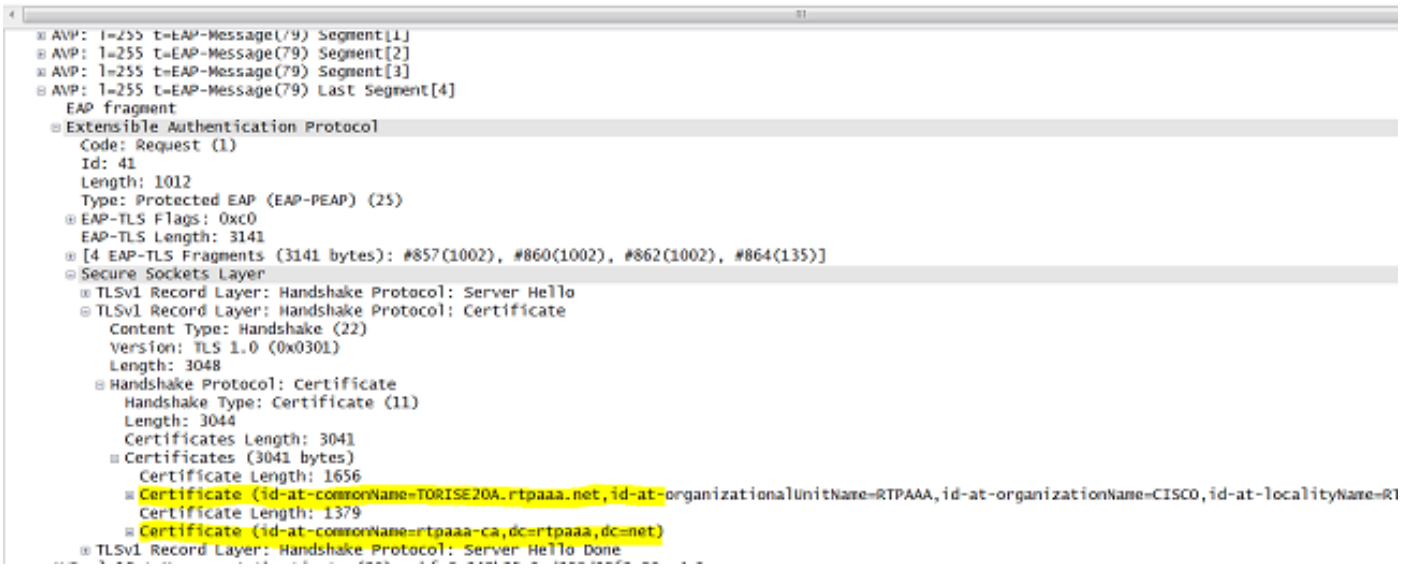
1. Afin d'effectuer une capture à partir d'ISE (TCPDump) pendant l'authentification, naviguez vers Operations > Diagnostic Tools > General Tools > TCP Dump.

2. Téléchargez/ouvrez la capture et appliquez le filtre ssl.handshake.certificates dans Wireshark et trouvez un défi d'accès.

3. Une fois la sélection effectuée, naviguez vers Expand Radius Protocol > Attribute Value Pairs > EAP-Message Last segment > Extensible Authentication Protocol > Secure Sockets Layer > Certificate > Certificates.

Chaîne de certificats dans la capture.



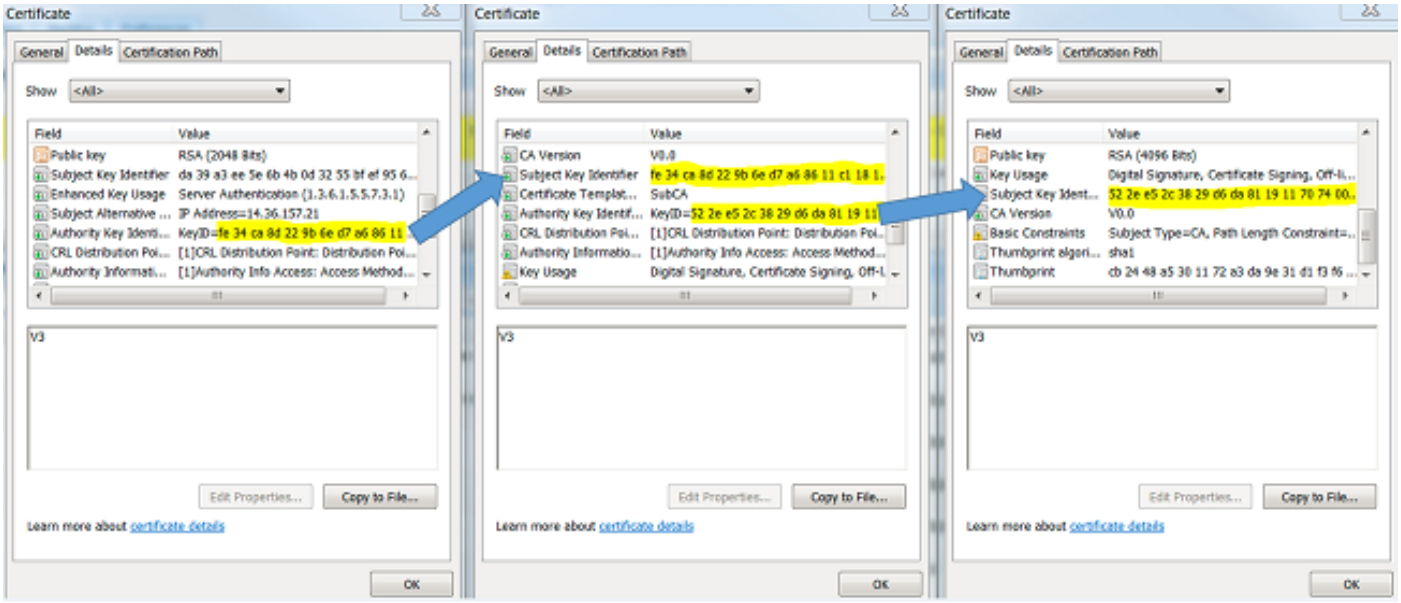


Si la chaîne est incomplète, accédez à ISE Administration > Certificates > Trusted Certificates et vérifiez que les certificats racine et (ou) Intermediate sont présents. Si la chaîne de certificats est passée avec succès, la chaîne elle-même doit être vérifiée comme étant valide à l'aide de la méthode décrite ici.

Ouvrez chaque certificat (serveur, intermédiaire et racine) et vérifiez la chaîne de confiance en faisant correspondre l'identificateur de clé de sujet (SKI) de chaque certificat à l'identificateur de

clé d'autorité (AKI) du certificat suivant dans la chaîne.

Exemple de chaîne de certificats.

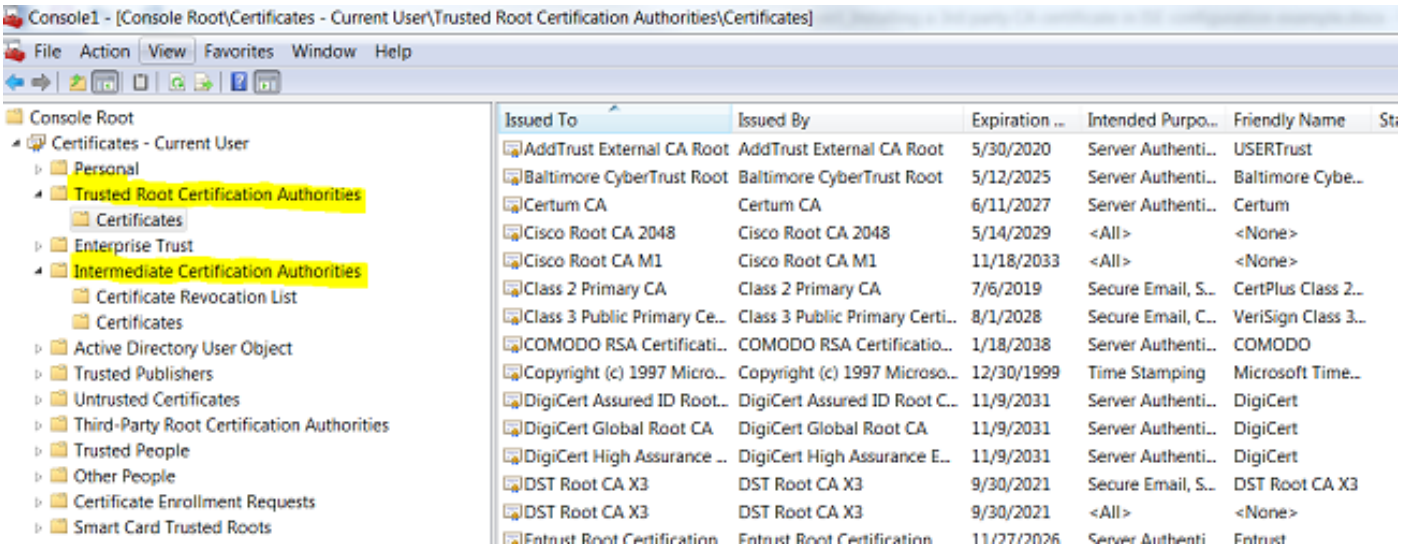


La chaîne de certificats ISE est correcte, mais le terminal rejette le certificat du serveur ISE pendant l'authentification

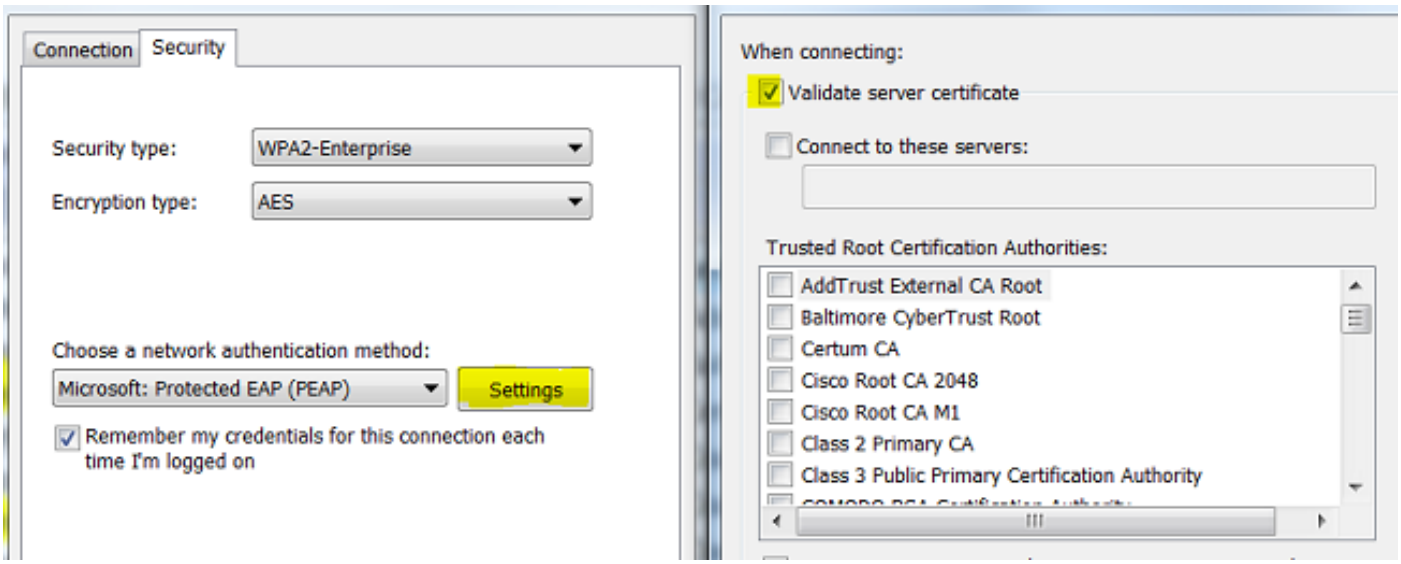
Si ISE présente sa chaîne de certificats complète lors de la connexion SSL et que le demandeur continue de rejeter la chaîne de certificats, l'étape suivante consiste à vérifier que les certificats racine et/ou intermédiaire se trouvent dans le magasin local d'approbations du client.

Afin de vérifier cela à partir d'un périphérique Windows, naviguez vers mmc.exe File > Add-Remove Snap-in. Dans la colonne Composants logiciels enfichables disponibles, sélectionnez Certificats et cliquez sur Ajouter. Sélectionnez Mon compte d'utilisateur ou Compte d'ordinateur selon le type d'authentification utilisé (Utilisateur ou Machine), puis cliquez sur OK.

Dans la vue de la console, sélectionnez Autorités de certification racines de confiance et Autorités de certification intermédiaires pour vérifier la présence des certificats racines et intermédiaires dans le magasin d'approbations local.



Pour vérifier facilement qu'il s'agit d'un problème lié à la vérification de l'identité du serveur, désactivez la case à cocher Valider le certificat du serveur dans la configuration du profil du demandeur et testez-la à nouveau.



Informations connexes

- Guide de l'administrateur de Cisco Identity Services Engine, version 3.0
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.