Installez un certificat de CA de tiers dans ISE 2.0

Contenu

Introduction

Ce document décrit installer un certificat signé du tiers CA dans le Logiciel Cisco Identity Services Engine.

Le processus est identique indépendamment du rôle final de certificat (authentification EAP, portail, admin et pxGrid).

Conditions requises

La connaissance de base d'infrastructure de clé publique.

Composants utilisés

Les informations dans ce document sont basées sur le matériel et les versions de logiciel suivants :

- Version 2.0 du Logiciel Cisco Identity Services Engine (ISE). La même configuration s'applique aux versions 1.3 et à 1.4.

Configurez

Générer la demande de signature de certificat (CSR) :

Pour générer le CSR allez à la gestion > aux Certificats > aux demandes de signature de certificat et choisi générez les demandes de signature de certificat (CSR).

- Sous la section d'utilisation sélectionnez le rôle à utiliser du menu de baisse vers le bas. Si le certificat sera utilisé pour de plusieurs rôles vous pouvez sélectionner la Multi-utilisation. Une fois le certificat est généré les rôles peut être changé s'il y a lieu.
- Sélectionnez le noeud pour lequel le certificat sera généré.
- Complétez les informations en tant que nécessaire (unité organisationnelle, organisation, ville, état et pays).

Note: Sous le nom commun (NC) le champ ISE automatique remplira nom de domaine complet du noeud (FQDN).

Masques :

- Si le but est de générer un contrôle de certificat de masque la case « permettez de masque Certificats ».
- Si le certificat sera utilisé pour des authentifications EAP « * » le symbole ne devrait pas être dans le domaine NC de sujet car les suppliants de Windows rejetteront le certificat de serveur.
- Même lorsque « validez le serveur que l'identité » est désactivée sur le suppliant, la prise de contact SSL peut échouer quand « * » est dans le domaine NC.
- Au lieu de cela, un FQDN générique peut être utilisé dans le domaine NC, et alors le « *.domain.com » peut être utilisé sur le champ alternatif soumis de nom DNS du nom (SAN).

Note: Quelques autorités de certification (CA) peuvent ajouter le masque (*) dans la NC du certificat automatiquement même si il pas présent dans le CSR. Dans ce scénario, une demande spéciale aura besoin de moi a fait pour empêcher cette action.

Exemple individuel CSR de certificat de serveur :

Exemple CSR de masque :

Note: L'adresse IP de chaque noeud de déploiement peut être ajoutée au champ SAN pour éviter un avertissement de certificat quand vous accédez au serveur par l'intermédiaire de l'adresse IP.

Une fois que le CSR a été créé, ISE affichera une fenêtre d'afficher avec l'option de l'exporter. Une fois qu'exporté, ce fichier devrait être envoyé au CA pour la signature.

Importer la nouvelle chaîne de certificat :

L'autorité de certification renverra le certificat de serveur signé avec la pleine chaîne de signature (racine/intermédiaire). Une fois que reçu, suivez les étapes ci-dessous pour importer les Certificats dans votre serveur ISE.

1. Importez tous les racine et (ou) Certificats intermédiaires fournis par le CA en allant à la gestion > aux Certificats > les Certificats de confiance.
2. Importez le certificat de serveur en allant à la gestion >> aux Certificats >> aux demandes de signature de certificat.
3. Sélectionnez le CSR précédemment créé et cliquez sur en fonction le certificat de grippage.
4. Sélectionnez le nouvel emplacement de certificat et ISE liera le certificat à la clé privée créée et enregistrée dans la base de données.

Note: Si le rôle d'admin a été sélectionné pour ce certificat, ISE redémarrera des services.

Vérifiez

Si le rôle d'admin était sélectionné pendant l'importation de certificat vous pouvez vérifier le nouveau certificat est en place en chargeant la page d'admin dans le navigateur. Le navigateur devrait faire confiance au nouveau certificat d'admin tant que la chaîne a été construite correctement et si la chaîne de certificat est de confiance par le navigateur.

Pour la vérification supplémentaire sélectionnez le symbole de verrouillage dans le navigateur et sous le chemin de certificat vérifiez la pleine chaîne est présent et fait confiance par l'ordinateur. Ce n'est pas un indicateur direct que la pleine chaîne a été passée vers le bas correctement par le serveur mais un indicateur du navigateur capable faire confiance au certificat de serveur basé sur sa mémoire locale de confiance.

Dépannez

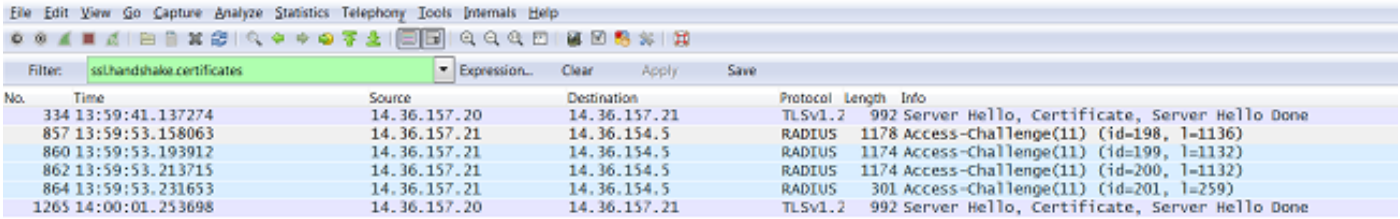
Le suppliant ne fait pas confiance au certificat de serveur local ISE pendant une authentification de dot1x.

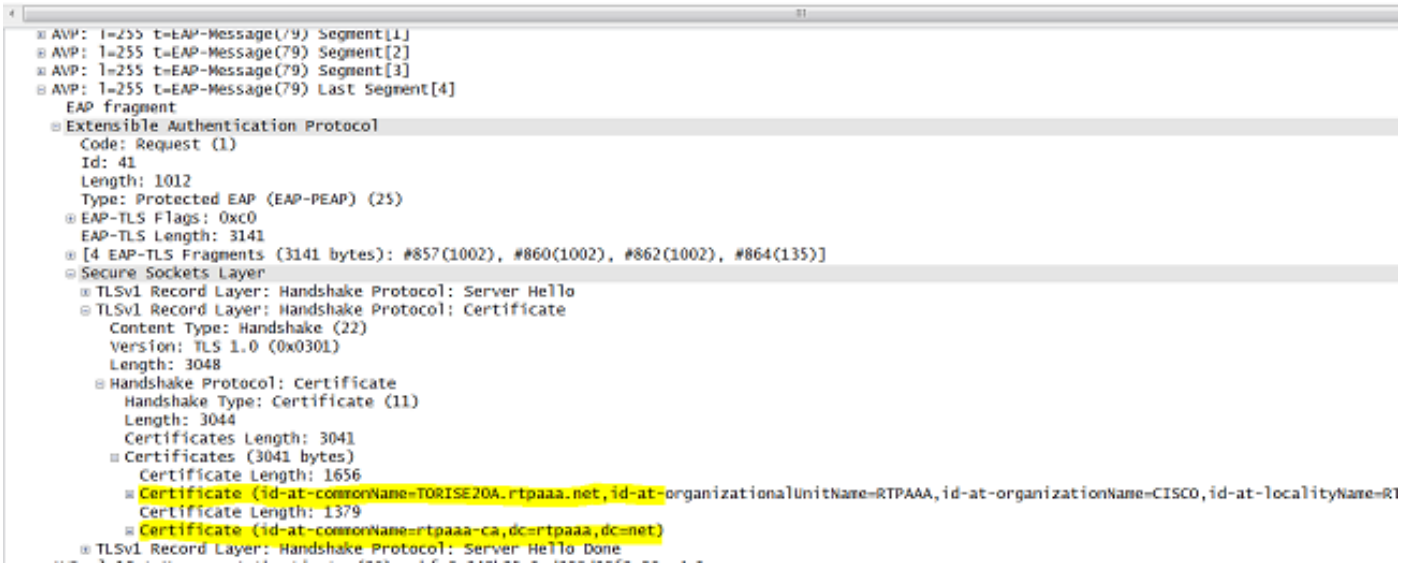
Vérifiez ISE passe la pleine chaîne de certificat pendant le processus de prise de contact SSL.

Quand en utilisant les méthodes d'EAP qui exigent un certificat de serveur (c.-à-d. PEAP) et « validez le serveur que l'identité » est sélectionnée, le suppliant validera la chaîne de certificat utilisant les Certificats elle a dans sa mémoire locale de confiance en tant qu'élément de la procédure d'authentification. En tant qu'élément du processus de prise de contact SSL ISE présentera son certificat et également tous les racine et (ou) Certificats intermédiaires actuels dans sa chaîne. Le suppliant ne pourra pas valider l'identité de serveur si la chaîne est inachevée. Pour vérifier la chaîne de certificat est passé de nouveau à votre client, vous peut exécuter les étapes suivantes :

1. Prenez une capture d'ISE (TCPDump) pendant l'authentification. Trouvé sous des exécutions > Diagostic usine > les outils généraux > le vidage mémoire de TCP
2. Le téléchargez/ouvrez la capture et appliquez le filtre « ssl.handshake.certificates » dans Wireshark et trouvez un Access-défi.
3. Une fois que sélectionné, développez le protocole RADIUS > les paires de valeurs d'attribut > segment > l'Extensible Authentication Protocol > le Secure Sockets Layer > le certificat > les Certificats d'Eap-message le dernier

Chaîne de certificat dans la capture.

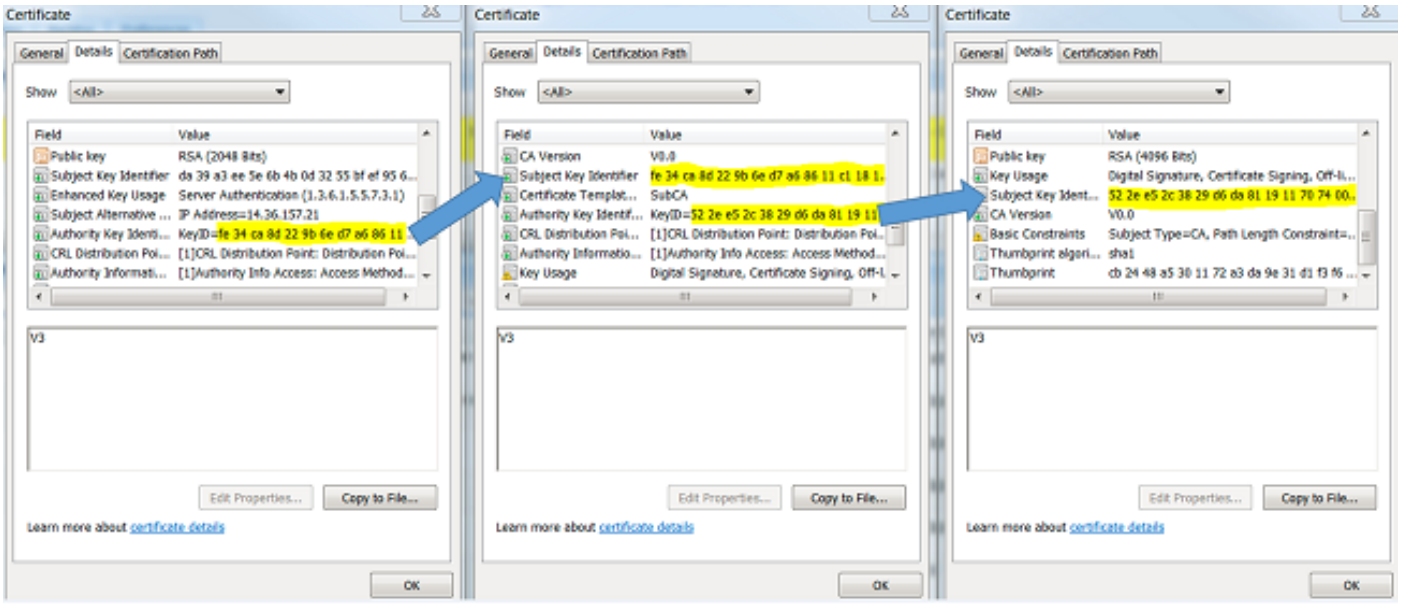




Si la chaîne n'est pas complète vous devriez aller à la gestion > aux Certificats ISE > les Certificats de confiance et vérifier que la racine et (ou) les Certificats intermédiaires sont présents. Si la chaîne de certificat est passée avec succès, la chaîne elle-même devrait être vérifiée comme valide à l'aide de la méthode tracée les grandes lignes ci-dessous.

Ouvrez chaque certificat (serveur, intermédiaire et racine) et vérifiez la chaîne de la confiance en appariant l'identifiant principal soumis (SKI) de chaque certificat à l'identifiant de clé d'autorité (AKI) du prochain certificat dans la chaîne.

Exemple de chaîne de certificat.



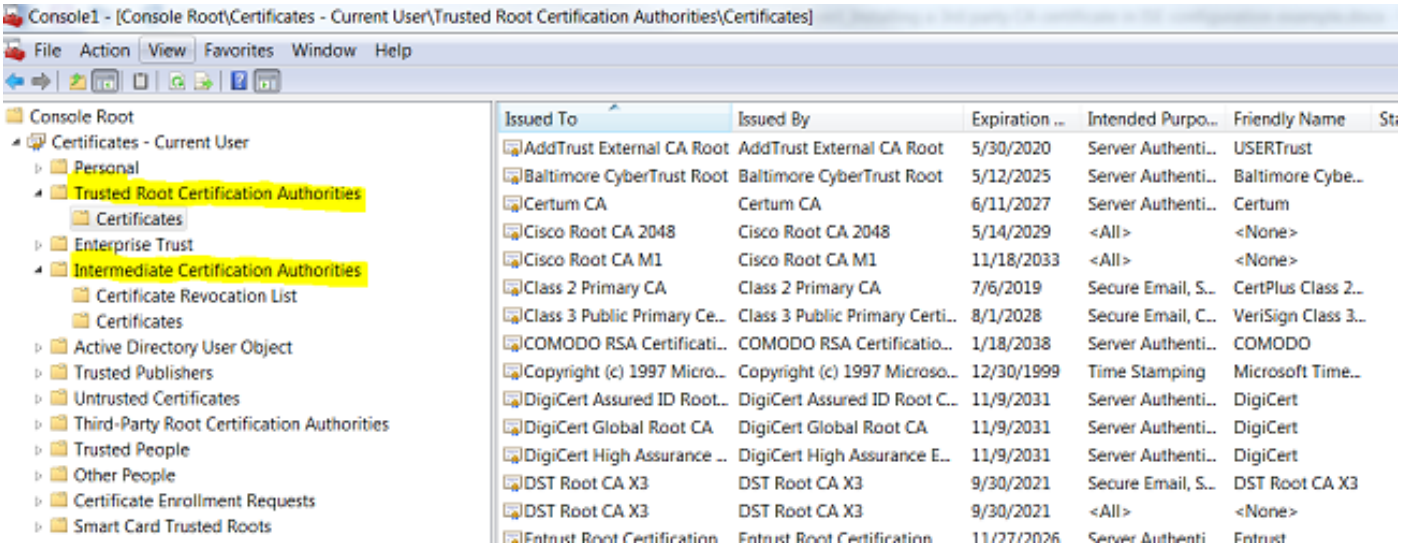
La chaîne de certificat ISE est certificat correct mais de point final des anomalies ISE de serveur pendant l'authentification.

S'ISE présente sa pleine chaîne de certificat pendant la prise de contact SSL et le suppliant rejette toujours la chaîne de certificat ; l'étape suivante est de vérifier que les Certificats intermédiaires d'and(or) de racine sont dans la mémoire locale de confiance de client.

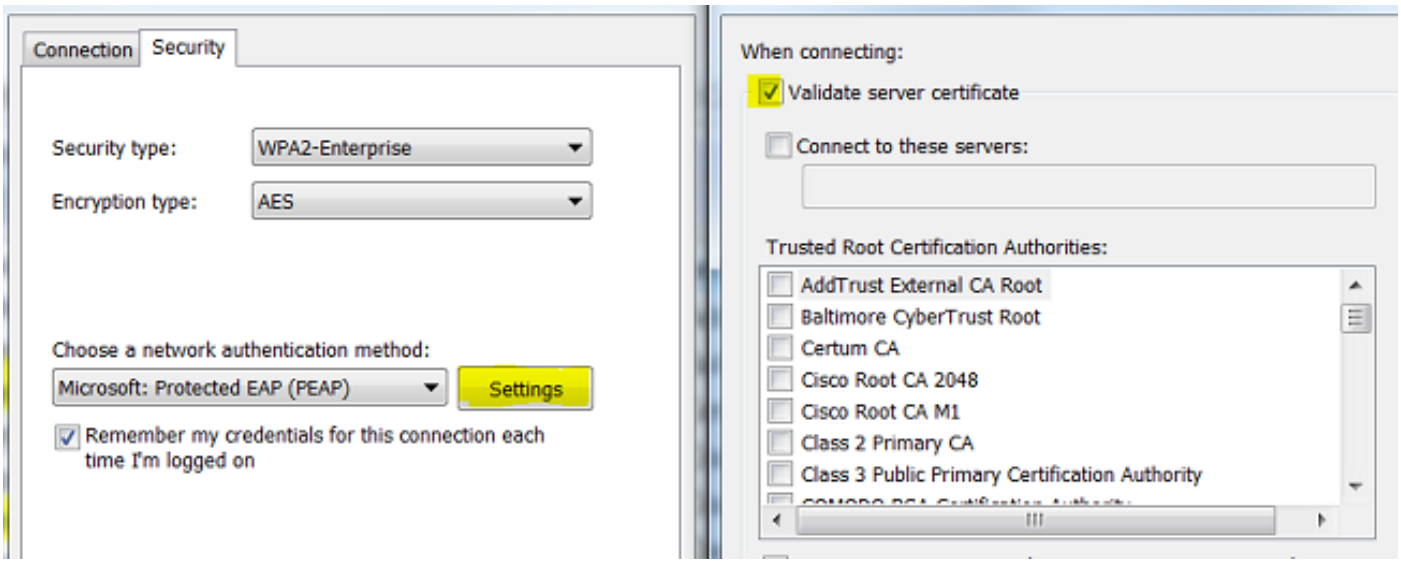
Pour vérifier ceci à partir d'un fichier ouvert du périphérique mmc.exe de Windows > Ajouter-retirez SNAP-dans > des Certificats choisis de la colonne SNAP-Institut central des statistiques disponible > ajoutent > sélectionnent « mon compte utilisateur » ou « compte d'ordinateur » selon le type d'authentification en service (utilisateur ou ordinateur). > CORRECT

Sous Autorités de certification racine approuvée » choisies de vue de console les « et « des autorités intermédiaires de certification » pour vérifier la

présence de la racine et du certificat intermédiaire dans la mémoire locale de confiance.



Une méthode facile de vérifier que c'est une question de contrôle d'identité de serveur, décochent « valident le certificat de serveur » sous la configuration de profil de suppliant et le testent de nouveau.



Note: ISE actuellement ne prend en charge pas traiter des Certificats utilisant RSASSA-PSS comme algorithme de signature. Ceci inclut le certificat de serveur, la racine, l'intermédiaire ou le certificat client (c.-à-d. EAP-TLS, PEAP (TLS), etc.). Référez-vous à la bogue CSCug22137.

Références

- Guide de l'administrateur de Logiciel Cisco Identity Services Engine, version 2.0