Renouvellement de certificat sur le guide de configuration de Logiciel Cisco Identity Services Engine

Contenu

Introduction

Ce document décrit des pratiques recommandées et des procédures proactives de renouveler des Certificats sur le Logiciel Cisco Identity Services Engine (ISE). Il passe en revue également comment installer des alarmes et des notifications ainsi des administrateurs sont avertis des événements à venir tels que l'expiration de certificat.

> **Note**: Ce document n'est pas destiné pour être un guide de dépannage pour des Certificats.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Certificats X509
- Configuration de Cisco ISE avec des Certificats

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 1.2.0.899 de Cisco ISE
- Appliance ou VMware

Informations générales

En tant qu'administrateur ISE, vous rencontrerez par la suite le fait que les Certificats ISE expirent. Si votre serveur ISE a un certificat expiré, les sérieux problème pourraient surgir à moins que vous remplaciez le certificat expiré par un nouveau, valide certificat.

> **Note**: Si le certificat qui est utilisé pour le Protocole EAP (Extensible Authentication Protocol) expire, toutes les authentifications pourraient échouer parce que les clients ne font plus confiance au certificat ISE. Si le certificat de protocole HTTPS expire, le risque est encore plus grand : un administrateur ne pourrait pas pouvoir ouvrir une session à l'ISE plus, et le déploiement distribué pourrait cesser de fonctionner et répliquer.

Dans cet exemple, l'ISE a un certificat installé d'un serveur d'Autorité de certification (CA) qui expirera dans un mois. L'administrateur ISE devrait installer un nouveau, valide certificat sur l'ISE avant que le vieux certificat expire. Cette approche proactive empêche ou réduit le temps d'arrêt et évite une incidence sur vos utilisateurs finaux. Une fois le délai prévu du certificat nouvellement installé commence, vous pouvez activer le protocole d'EAP et/ou HTTPS relatif au nouveau certificat.

Vous pouvez configurer l'ISE de sorte qu'il génère des alarmes et informe l'administrateur d'installer de nouveaux Certificats avant que les vieux Certificats expirent.

> **Note**: Ce document emploie HTTPS avec un certificat auto-signé afin d'expliquer l'incidence du renouvellement de certificat, mais cette approche n'est pas recommandée pour un système vivant. Il vaut mieux d'utiliser un certificat de CA pour les protocoles d'EAP et HTTPS.

Configurez

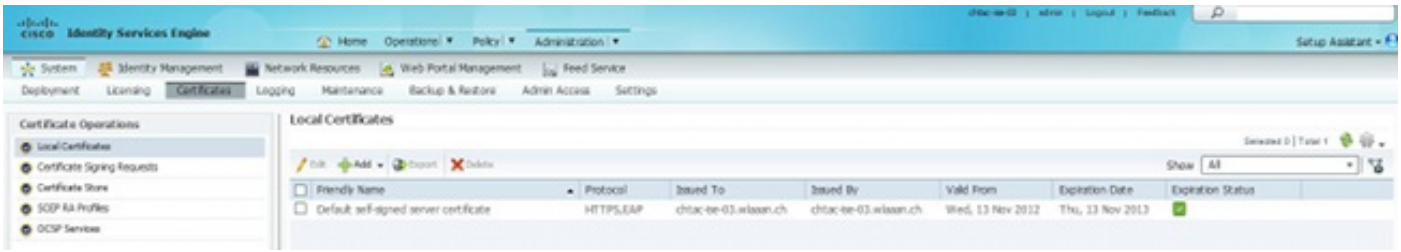
Certificats Auto-signés par ISE de vue

Quand l'ISE est installé, il génère un certificat auto-signé. Le certificat auto-signé est utilisé pour l'accès de gestion et pour la transmission dans le déploiement distribué (HTTPS) aussi bien que pour l'authentification de l'utilisateur (EAP). Dans un système vivant, utilisez un certificat de CA au lieu d'un certificat auto-signé.

> **Conseil** : Référez-vous à la Gestion de certificat dans la section de Cisco ISE du guide d'installation du matériel de Logiciel Cisco Identity Services Engine, version 1.2 pour des informations supplémentaires.

Le format pour un certificat ISE doit être le Privacy Enhanced Mail (PEM) ou les règles distinguées de codage (DER).

Afin de visualiser l'initiale auto-a signé le certificat, naviguent vers la **gestion** > le **System> délivre un certificat** > les **Certificats locaux** dans la console ISE :



Si vous installez un certificat de serveur sur l'ISE par l'intermédiaire d'une demande de signature de certificat (CSR) et changez le certificat pour le protocole HTTPS ou d'EAP, le certificat de serveur auto-signé est encore présent mais n'est plus utilisé.

> **Attention** : Pour HTTPS le protocole change, une reprise des services ISE est exigé, qui crée quelque compte rendu de temps d'arrêt. Les modifications de protocole d'EAP ne déclenchent pas une reprise des services ISE et n'entraînent pas le temps d'arrêt.

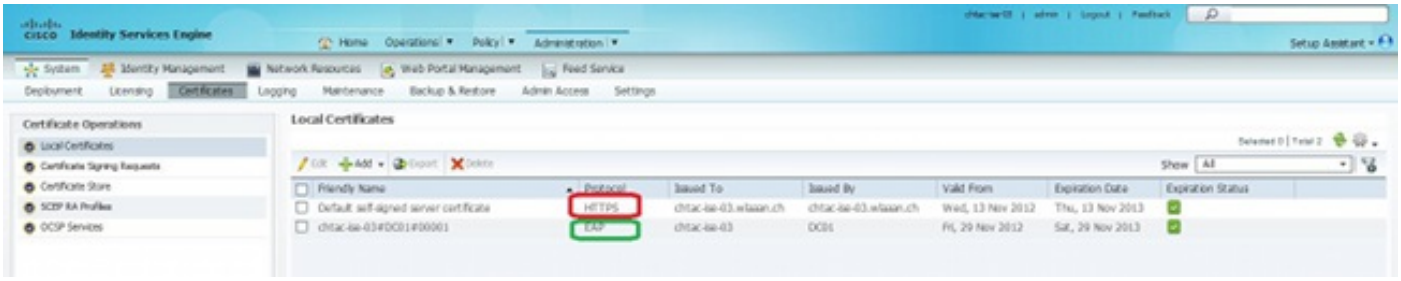
Déterminez quand changer le certificat

Supposez que le certificat installé expire bientôt. Est-il pour permettre mieux le certificat d'expirer avant que vous le renouveliez ou de changer le certificat avant expiration ? Vous devriez changer le certificat avant expiration de sorte que vous ayez le temps pour prévoir l'échange de certificat et pour gérer n'importe quel temps d'arrêt provoqué par l'échange.

Quand devriez-vous changer le certificat ? Obtenez un nouveau certificat avec une date de début qui précède la date d'expiration du vieux certificat. Le délai prévu entre ces deux dates est la fenêtre de modification.

> **Attention** : Si vous activez HTTPS, il entraîne une reprise de service sur le serveur ISE, et vous éprouvez quelque compte rendu de temps d'arrêt.

Cette image dépeint les informations pour un certificat qui est délivré par un CA et expire le 29 novembre 2013 :



Générez la demande de signature de certificat

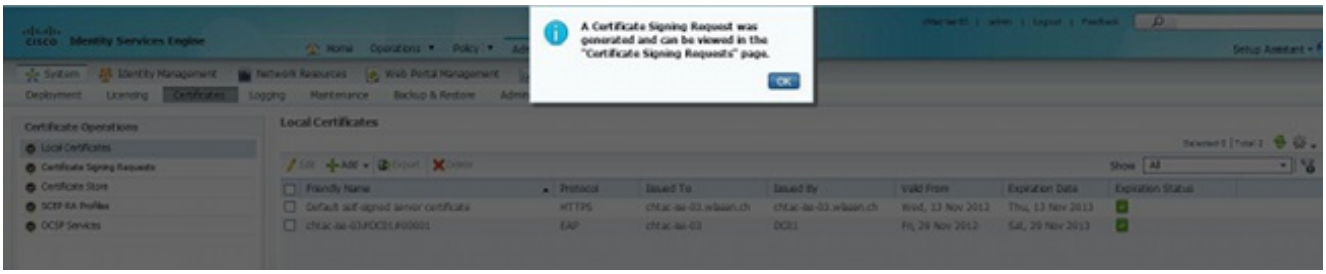
Cette procédure décrit comment renouveler le certificat par un CSR :

1. Dans la console ISE, naviguez **pour ajouter > génèrent la demande de signature de certificat**.

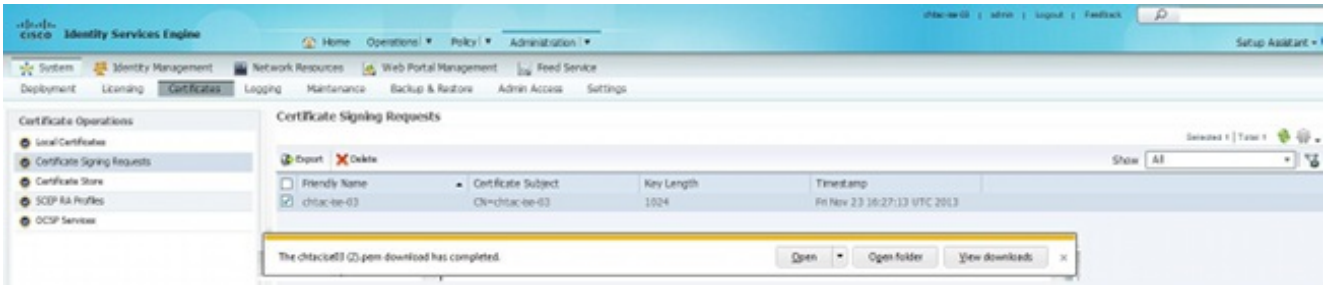
2. Les informations minimum que vous devez écrire dans le champ texte de **sujet de certificat** sont CN=ISEfqdn, où *ISEfqdn* est le nom de domaine complet (FQDN) de l'ISE. Ajoutez les champs supplémentaires tels qu'O (organisation), OU (unité organisationnelle), ou C (pays) dans le sujet de certificat avec l'utilisation des virgules :

3. Une des lignes de champ texte **alternatives soumises du nom (SAN)** doit répéter le FQDN ISE. Vous pouvez ajouter un deuxième champ SAN si vous voulez utiliser des noms alternatifs ou un certificat de masque.

4. Une fenêtre contextuelle indique si les champs CSR sont terminés correctement :



5. Afin d'exporter le CSR, des **demandes de signature de certificat de** clic dans le panneau gauche, sélectionner votre CSR, et **exportation de** clic :

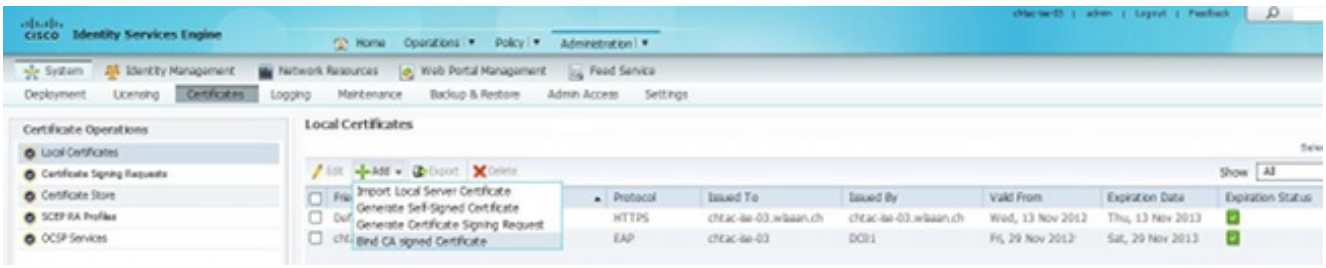


6. Le CSR est enregistré sur votre ordinateur. Soumettez-le à votre CA pour la signature.

Installez le certificat

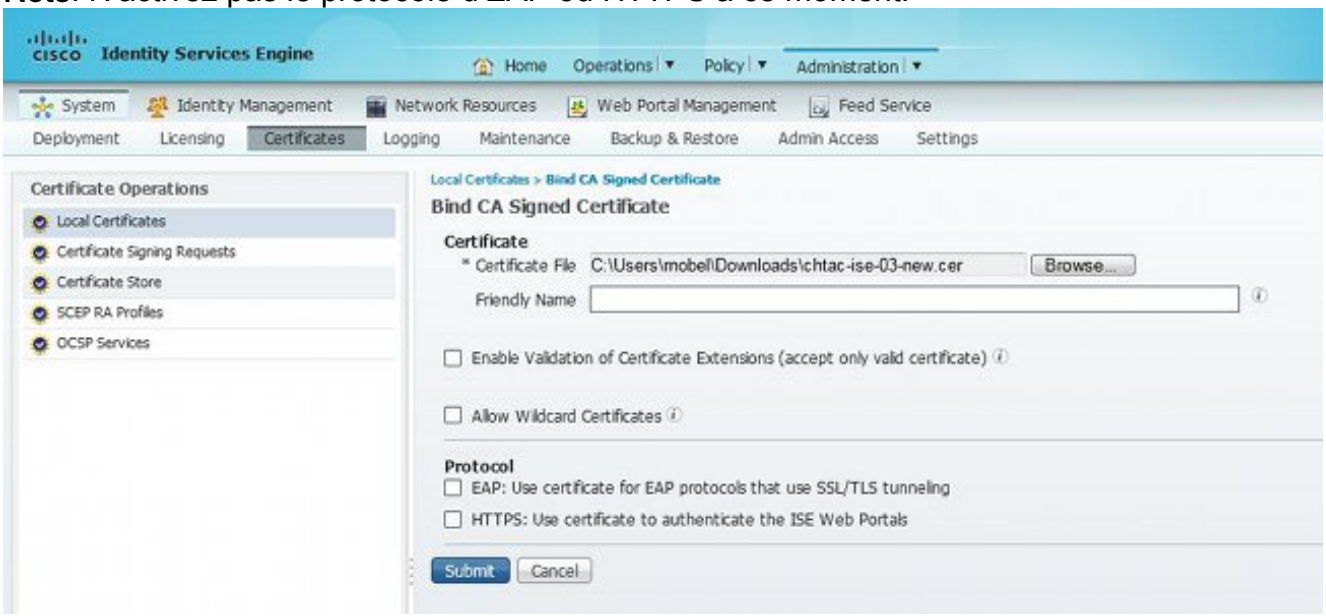
Une fois que vous recevez le certificat final de votre CA, vous devez ajouter le certificat à l'ISE :

1. Dans la console ISE, cliquez sur les **Certificats locaux** dans le panneau gauche, puis cliquez sur Add et **liez le certificat signé CA** :

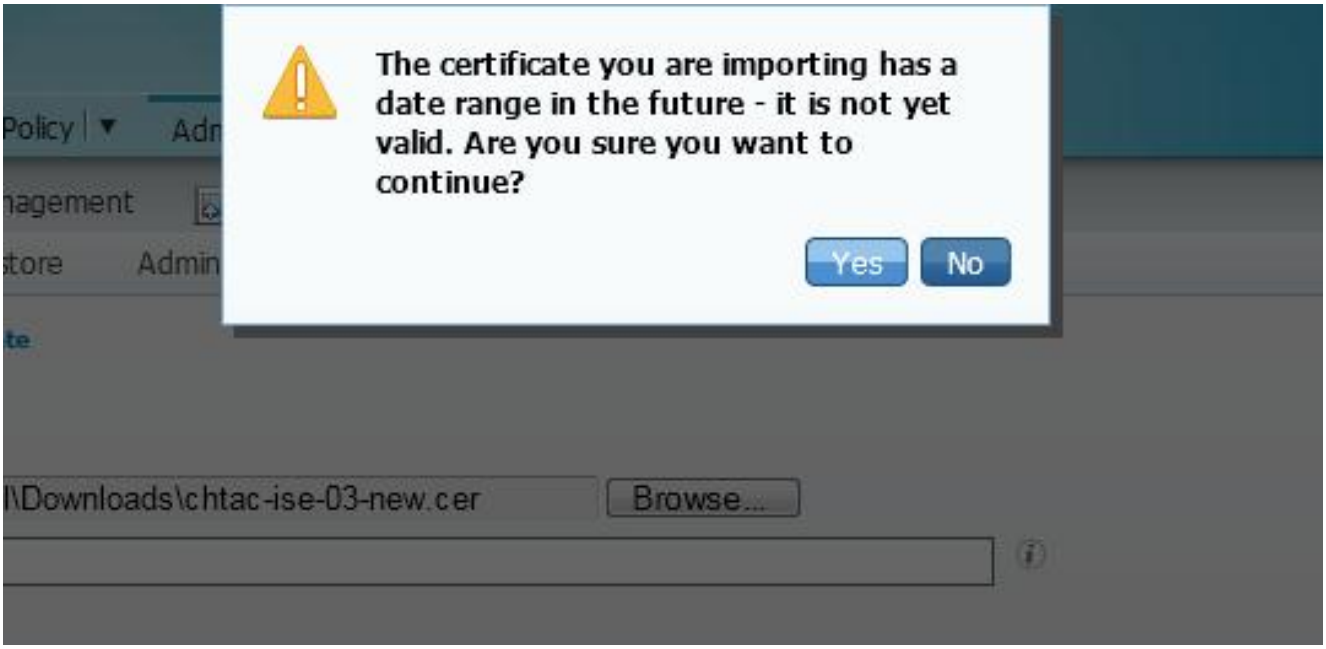


2. Écrivez une description simple et claire du certificat dans le champ texte **amical de nom** :

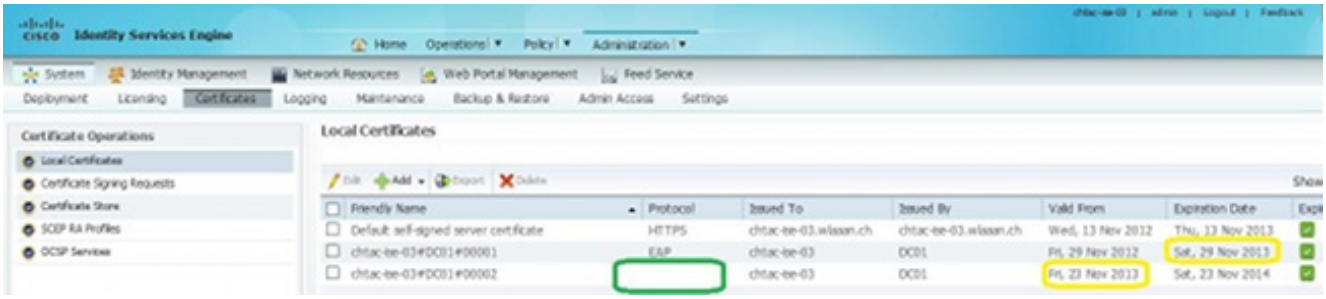
   Note: N'activez pas le protocole d'EAP ou HTTPS à ce moment.



3. Puisque vous installez le nouveau certificat avant que le vieil expire, vous voyez une erreur qui signale une plage de dates à l'avenir (23 novembre 2013 dans cet exemple).



4. Clic **oui** afin de continuer. Le certificat est maintenant installé mais non utilisable, comme mis en valeur en vert. La superposition entre la date d'expiration et la date valide est mise en valeur en jaune :



Note: Si vous utilisez les Certificats auto-signés dans un déploiement distribué, le certificat auto-signé primaire doit être installé dans le stock de certificat de confiance du serveur secondaire ISE. De même, le certificat auto-signé secondaire doit être installé dans le stock de certificat de confiance du serveur primaire ISE. Ceci permet aux serveurs ISE pour s'authentifier mutuellement. Sans ceci, le déploiement pourrait se casser. Si vous renouvelez des Certificats d'une tierce partie CA, vérifiez si la chaîne de certificat racine a changé et mettez à jour la mémoire de certificat de confiance dans l'ISE en conséquence. Dans les deux scénarios, assurez-vous que les Noeuds ISE, les systèmes d'exploitation de point final, et les suppliants peuvent valider la chaîne de certificat racine.

Configurez le système d'alerte

Cisco ISE vous informe quand la date d'expiration d'un certificat local a lieu dans les 90 jours. Une telle notification anticipée vous aide à éviter les Certificats expirés, à prévoir la modification de certificat, et à empêcher ou réduire le temps d'arrêt.

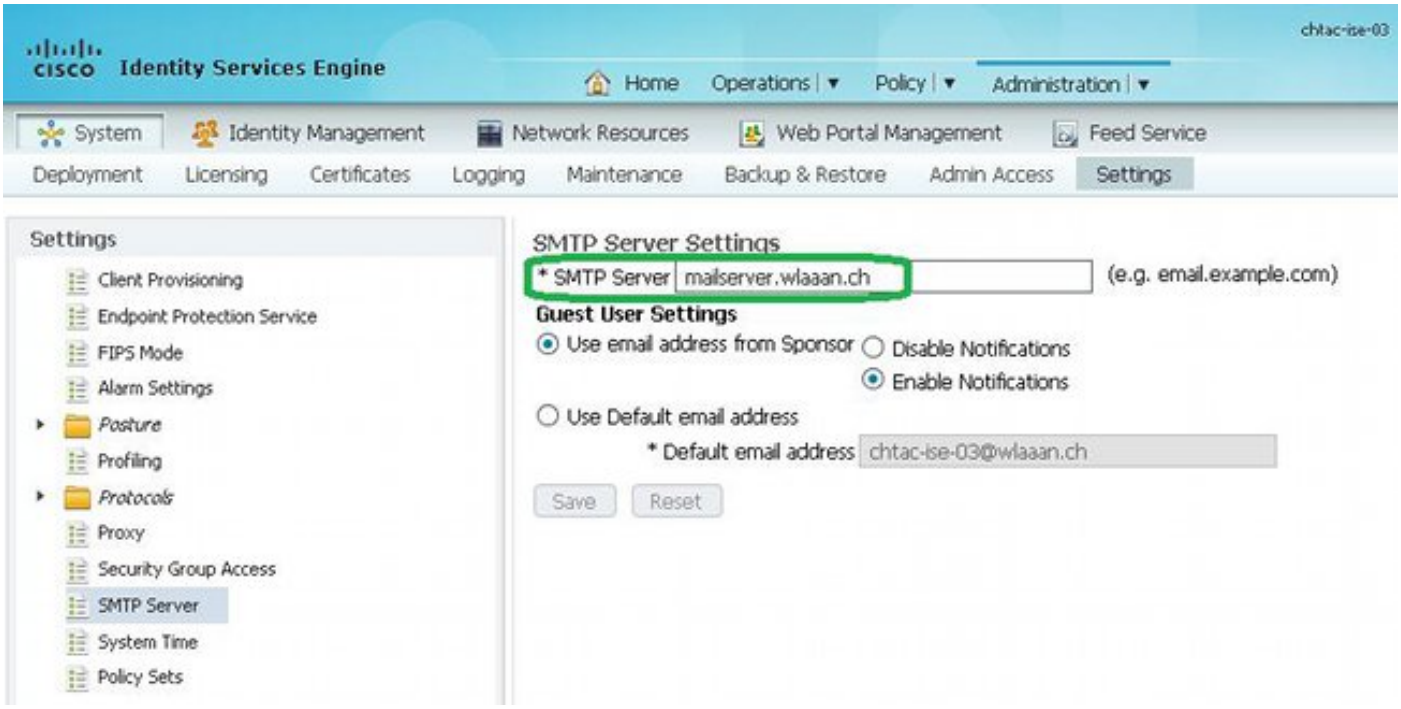
La notification apparaît de plusieurs manières :

- Les icônes d'état d'expiration de couleur apparaissent dans la page locale de Certificats.

- Les messages d'expiration apparaissent dans le rapport de diagnostic de système de Cisco ISE.

- Des alarmes d'expiration sont générées à 90 jours et à 60 jours, puis quotidiennement pendant les 30 jours finaux avant expiration.

Configurez l'ISE pour la notification électronique des alarmes d'expiration. Dans la console ISE, naviguez vers la **gestion > le système > les configurations > le serveur SMTP**, identifiez le serveur de Protocole SMTP (Simple Mail Transfer Protocol), et définissez les autres configurations de serveur de sorte que des notifications électroniques soient envoyées pour les alarmes :

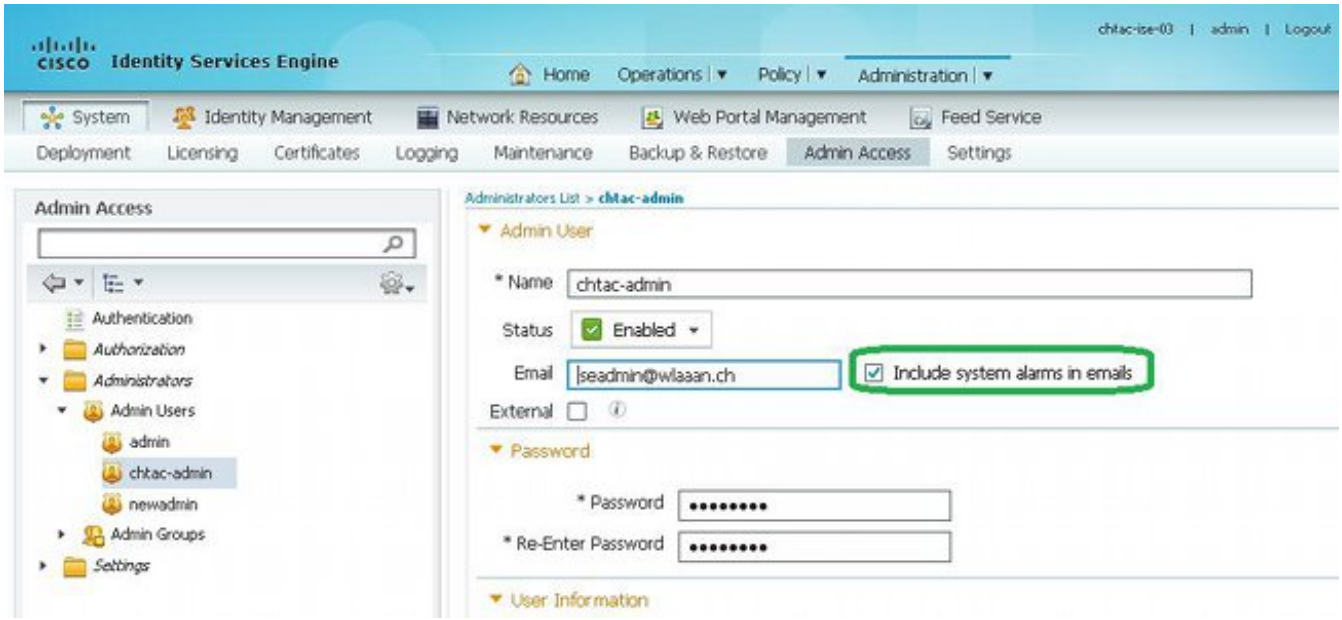


Il y a deux manières que vous pouvez installer des notifications :

- Admin Access d'utilisation afin d'informer des administrateurs :

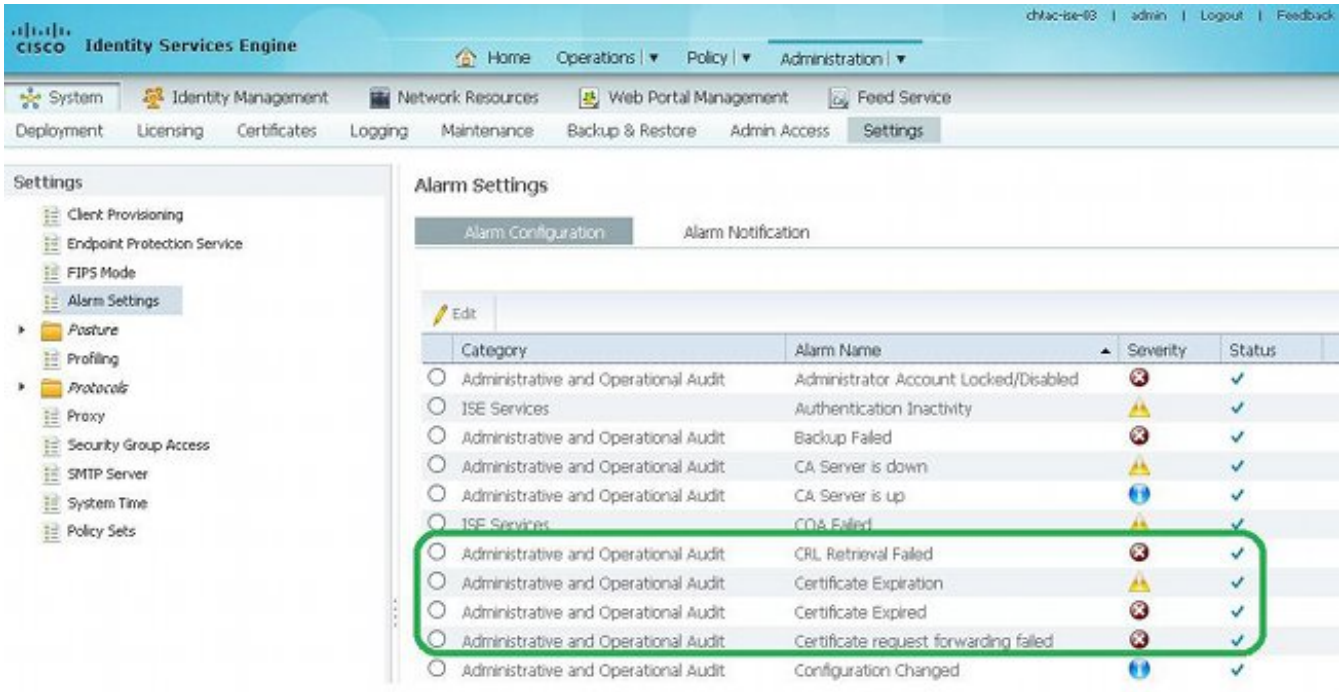
  Naviguez vers la **gestion > le système > l'admin Access > administrateurs > utilisateurs d'admin**.

  Vérifiez les **alarmes de système d'inclure dans la** case à cocher d'**emails** pour les utilisateurs d'admin qui doivent recevoir des notifications d'alarme. L'adresse e-mail pour l'expéditeur des notifications d'alarme est codée en dur comme ise@hostname.

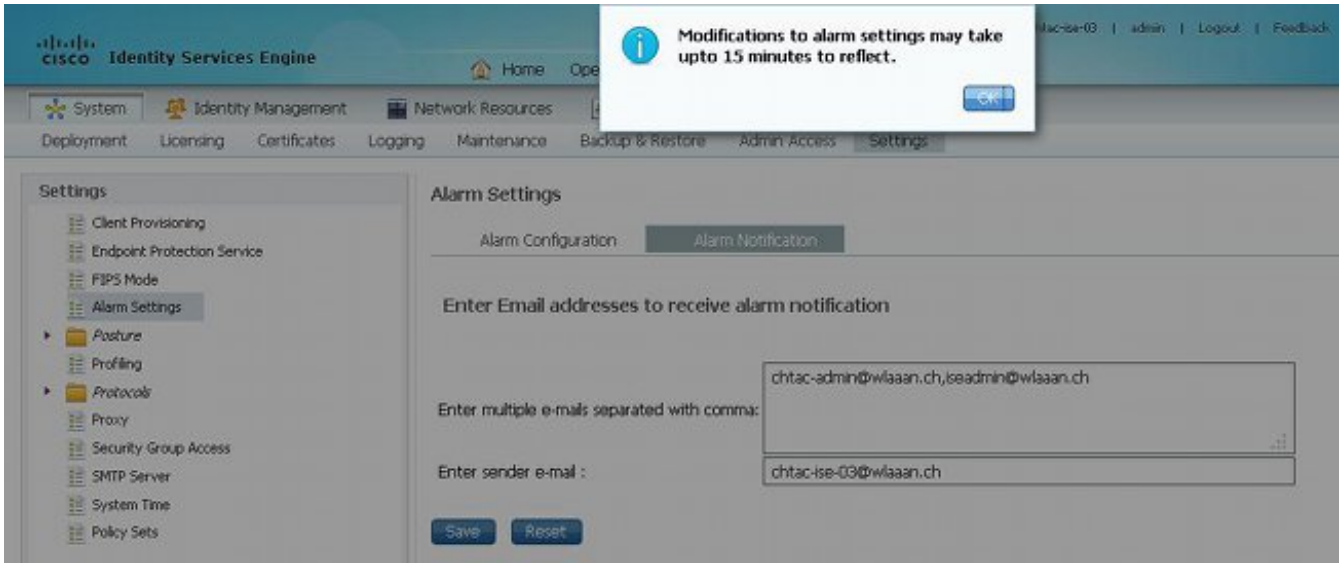


- Configurez le réglage des alarmes ISE afin d'informer des utilisateurs :

  Naviguez vers la **gestion > le système > les configurations > le réglage des alarmes > la configuration d'alarme** :



Note: Désactivez l'état pour une catégorie si vous souhaitez empêcher des alarmes de cette catégorie.Cliquez sur la **notification d'alarme,** écrivez les adresses e-mail des utilisateurs à annoncer, et sauvegardez la modification de configuration. Les modifications pourraient prendre à 15 minutes avant qu'elles sont en activité.

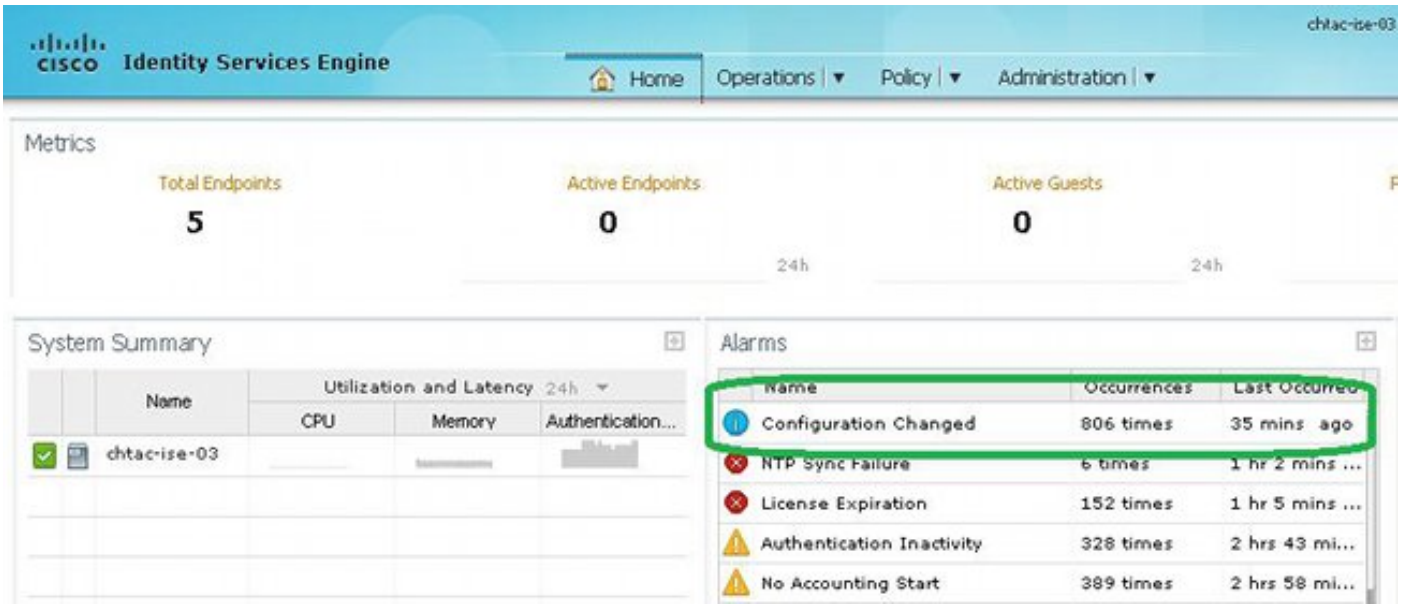


Vérifiez

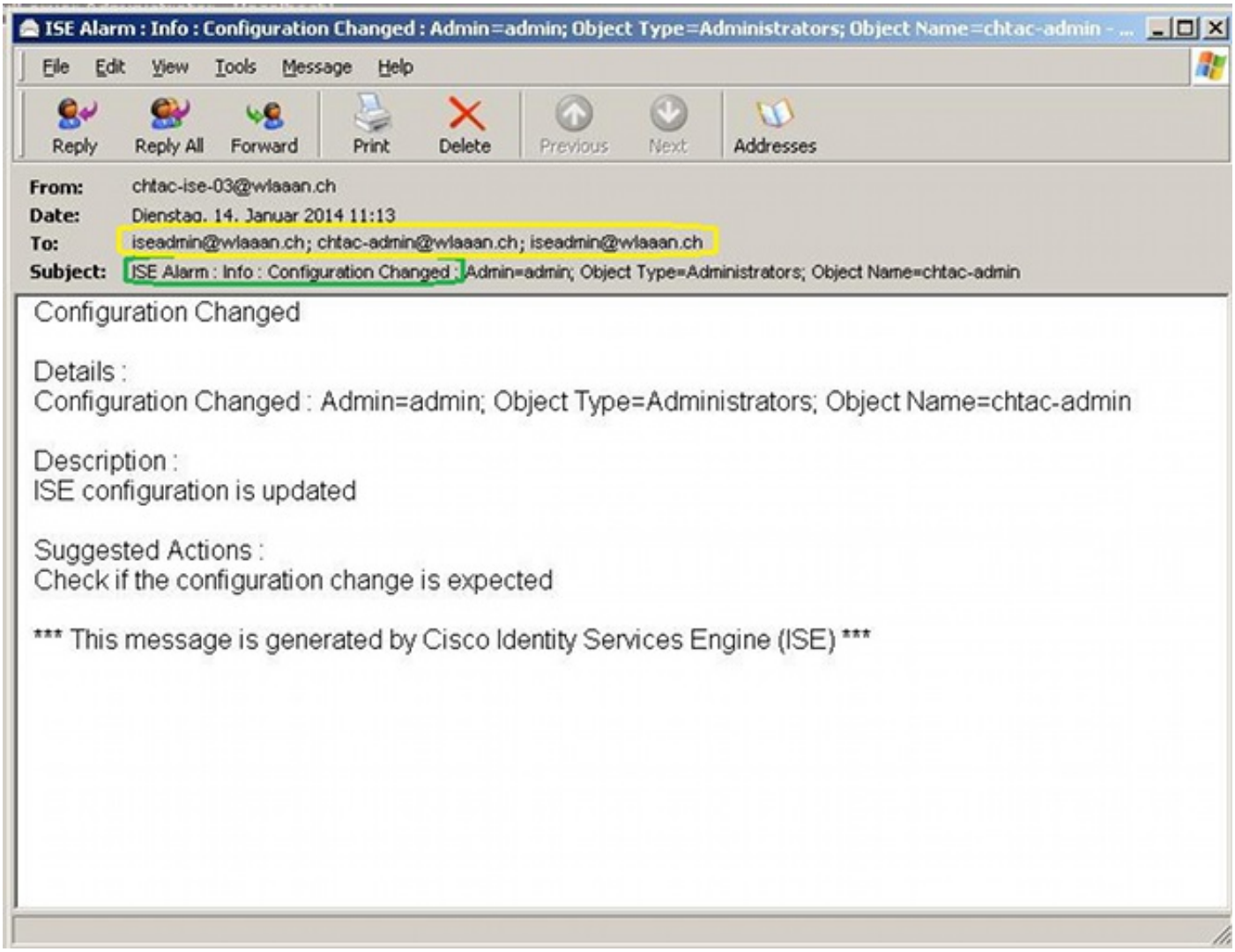
Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Vérifiez le système d'alerte

Vérifiez que le système d'alerte fonctionne correctement. Dans cet exemple, une modification de configuration génère une alerte avec un niveau d'importance des informations. (Une alarme de l'information est la plus basse sévérité, alors que les expirations de certificat génèrent un niveau d'importance plus élevé de l'avertissement.)



C'est un exemple de l'alarme d'email qui est envoyée par l'ISE :



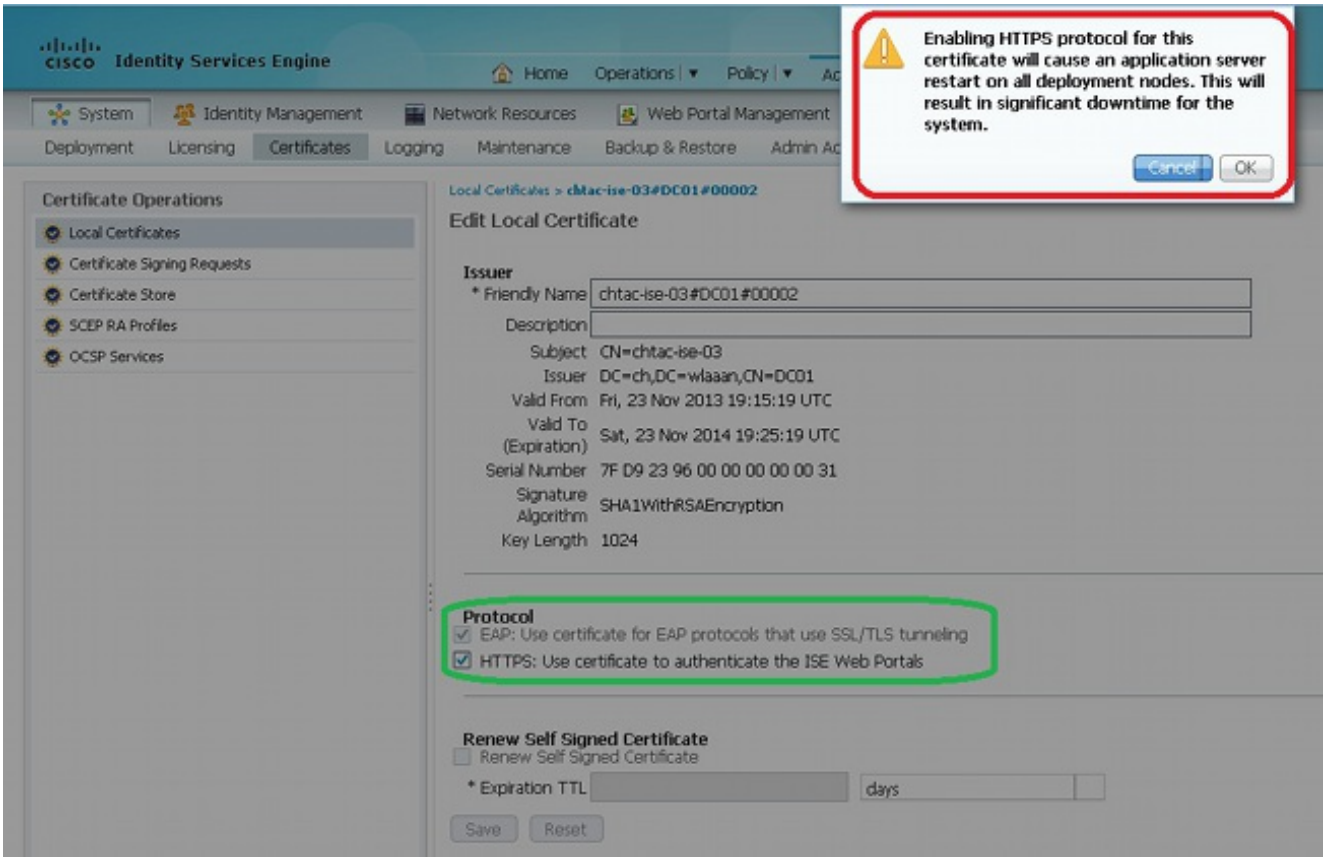
Note: Dans cet exemple, l'ISE envoie le message d'alarme d'email deux fois à iseadmin@wlaaan.ch, comme mis en valeur en jaune. Cette adresse e-mail a été installée pour recevoir des notifications par les deux méthodes expliquées dedans configurent le système d'alerte.

Vérifiez la modification de certificat

Cette procédure décrit comment vérifier que le certificat est installé correctement et comment changer les protocoles pour l'EAP et/ou le HTTPS :

1. Sur la console ISE, naviguez vers la **gestion > les Certificats > les Certificats locaux**, et sélectionnez le nouveau certificat afin de visualiser les détails.

   Attention : Si vous activez le protocole HTTPS, les reprises de service ISE, qui entraîne le temps d'arrêt de serveur.



Dans cet exemple, supposez que HTTPS redémarre le service ISE.

2. Afin de vérifier l'état de certificat sur le serveur ISE, sélectionnez cette commande dans le CLI :

```
CLI:> show application status ise
```

3. Une fois que tous les services sont en activité, tentative d'ouvrir une session en tant qu'administrateur.

4. Pour un scénario distribué de déploiement, naviguez vers la **gestion > l'état de système > de déploiement > de noeud** sur la console ISE, et vérifiez l'état de noeud.

5. Vérifiez que l'authentification d'utilisateur final est réussie. Sur la console ISE, naviguez vers des **exécutions > des authentifications**, et examinez le certificat pour l'authentification du Protected Extensible Authentication Protocol (PEAP) /EAP-Transport Layer Security (TLS).

Vérifiez le certificat

Si vous voulez vérifier le certificat extérieurement, vous pouvez utiliser les outils encastrés de Microsoft Windows ou la boîte à outils d'OpenSSL.

OpenSSL est une implémentation d'open-source du protocole de Secure Sockets Layer (SSL). Si les Certificats utilisent votre propre CA privé, vous devez placer votre certificat de CA de racine sur un ordinateur local et utiliser l'option d'OpenSSL - *CApath*. Si vous avez une intermédiaire CA, vous devez la placer dans le même répertoire aussi bien.

Afin d'obtenir les informations générales au sujet du certificat et les vérifier, utilisation :

```
openssl x509 -in certificate.pem -noout -text
openssl verify certificate.pem
```

Il pourrait également être utile de convertir les Certificats avec la boîte à outils d'OpenSSL :

```
openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem
```

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Conclusion

Puisque vous pouvez installer un nouveau certificat sur l'ISE avant qu'il soit en activité, Cisco recommande que vous installiez le nouveau certificat avant que le vieux certificat expire. Cette période de superposition entre la vieille date d'expiration de certificat et la nouvelle date de début de certificat te donne l'heure de renouveler des Certificats et de prévoir leur installation avec peu ou pas de temps d'arrêt. Une fois le nouveau certificat écrit sa plage de dates valide, active le protocole d'EAP et/ou HTTPS. Souvenez-vous, si vous activez HTTPS, il y aurez une reprise de service.