Configurer les renouvellements de certificats sur ISE

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Configurer

- Afficher les certificats ISE autosignés
- Déterminer quand modifier le certificat
- Générer une requête de signature de certificat
- Installer le certificat
- Configurer le système d'alerte

Vérifier

- Vérifier le système d'alerte
- Vérifier le changement de certificat
- Vérifier le certificat

Dépannage

Conclusion

Introduction

Ce document décrit les meilleures pratiques et les procédures proactives pour renouveler les certificats sur Cisco Identity Services Engine (ISE).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Certificats X509
- Configuration d'un appareil Cisco ISE avec des certificats

Composants utilisés

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

- Cisco ISE version 3.0.0.458
- Appareil ou VMware

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

Remarque : Ce document n'est pas destiné à servir de guide de diagnostic pour les certificats.

Ce document décrit les bonnes pratiques et des procédures proactives pour renouveler les certificats sur Cisco Identity Services Engine (ISE). Il indique également comment configurer des alarmes et des notifications afin que les administrateurs soient avertis d'événements imminents tels que l'expiration des certificats. En tant qu'administrateur ISE, vous finissez par rencontrer le fait que les certificats ISE expirent. Si votre serveur ISE a un certificat expiré, de graves problèmes peuvent survenir, sauf si vous remplacez le certificat expiré par un nouveau certificat valide.

Remarque : Si le certificat utilisé pour le protocole EAP (Extensible Authentication Protocol) expire, toutes les authentifications peuvent échouer car les clients ne font plus confiance au certificat ISE. Si le certificat d'administration ISE expire, le risque est encore plus grand : un administrateur ne peut plus se connecter à l'ISE et le déploiement distribué peut cesser de fonctionner et de se répliquer.

L'administrateur ISE doit installer un nouveau certificat valide sur l'ISE avant l'expiration de l'ancien certificat. Cette approche proactive prévient ou réduit les temps d’arrêt et empêche les répercussions sur vos utilisateurs finaux. Une fois que la période du certificat nouvellement installé commence, vous pouvez activer le rôle EAP/Admin ou tout autre rôle sur le nouveau certificat.

Vous pouvez configurer ISE pour qu’il génère des alertes et informe l’administrateur qu’il est temps d’installer de nouveaux certificats avant l’expiration des anciens certificats.

Remarque : Ce document utilise le certificat d'administration ISE comme certificat auto-signé afin de démontrer l'impact du renouvellement de certificat, mais cette approche n'est pas recommandée pour un système de production. Il est préférable d'utiliser un certificat CA pour les rôles EAP et Admin.

Configurer

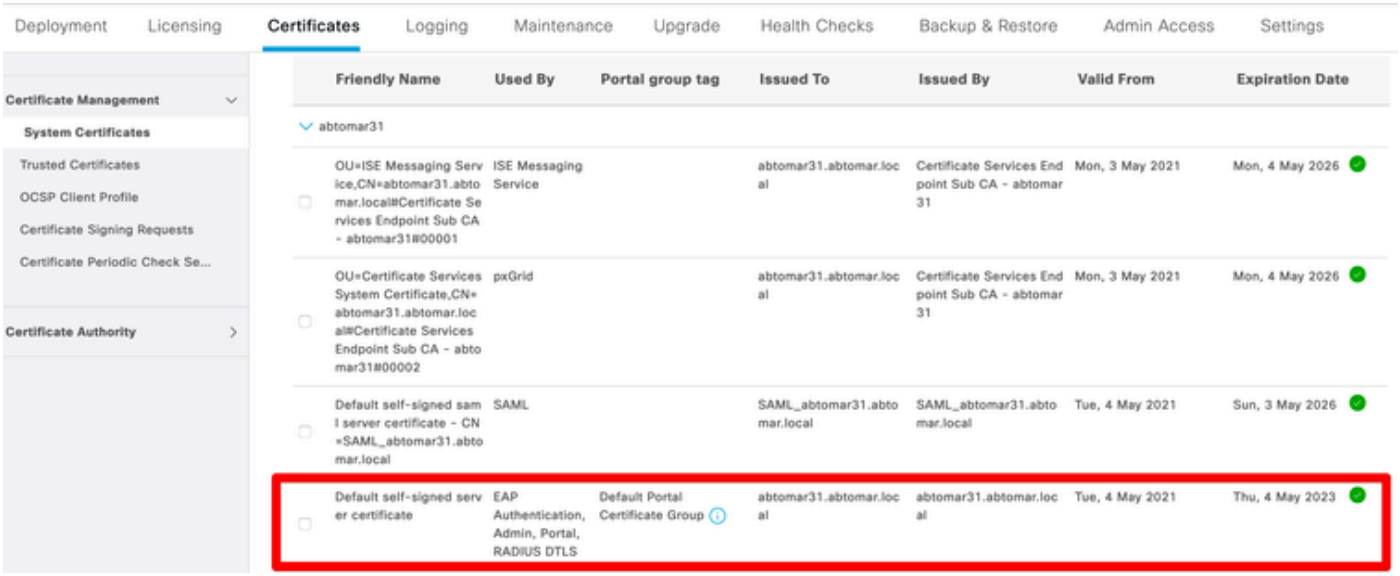
Afficher les certificats ISE autosignés

Lors de son installation, Cisco ISE génère un certificat autosigné. Le certificat autosigné est utilisé pour l'accès administratif et la communication au sein du déploiement distribué (HTTPS), ainsi que pour l'authentification des utilisateurs (EAP). Dans un système opérationnel, utilisez un certificat provenant d'une autorité de certification au lieu d'un certificat autosigné.

Conseil : Reportez-vous à la section sur la gestion des certificats dans Cisco ISE du Guide d'installation du Moteur de services de vérification des identités de Cisco (Cisco ISE), version 3.0, pour en savoir plus à ce sujet.

Un certificat ISE doit être au format Privacy Enhanced Mail (PEM) ou Distinguished Encodage Rules (DER).

Pour visualiser le certificat autosigné initial, naviguez vers Administration > System > Certificates > System Certificates (gestion > système > certificats > certificats du système) dans l'interface graphique de Cisco ISE, comme montré dans cette image.



Si vous installez un certificat de serveur sur Cisco ISE par l'intermédiaire d'une requête de signature de certificat (CSR) et que vous modifiez le certificat pour utiliser le protocole Admin ou EAP, le certificat de serveur autosigné est toujours présent, mais son état est « inutilisé ».

⚠ Mise en garde : Pour apporter des modifications au protocole Admin, un redémarrage des services ISE est nécessaire, ce qui entraîne un temps d'arrêt de quelques minutes. Les modifications apportées au protocole EAP n'entraînent pas le redémarrage des services ISE ni de temps d'arrêt.

Déterminer quand modifier le certificat

Supposons que le certificat installé expire bientôt. Est-il préférable de laisser le certificat expirer avant de le renouveler ou de modifier le certificat avant son expiration? Vous devez modifier le certificat avant l'expiration afin d'avoir le temps de planifier l'échange de certificat et de gérer les interruptions causées par l'échange.

Quand devez-vous modifier le certificat ? Obtenez un nouveau certificat dont la date de début précède la date d'expiration de l'ancien certificat. La période comprise entre ces deux dates représente la fenêtre de modification.

⚠ Mise en garde : Activer la fonction Admin provoque un redémarrage du service sur le serveur ISE, ce qui entraîne un temps d'arrêt de quelques minutes.

Cette image présente les informations d'un certificat qui expire bientôt :

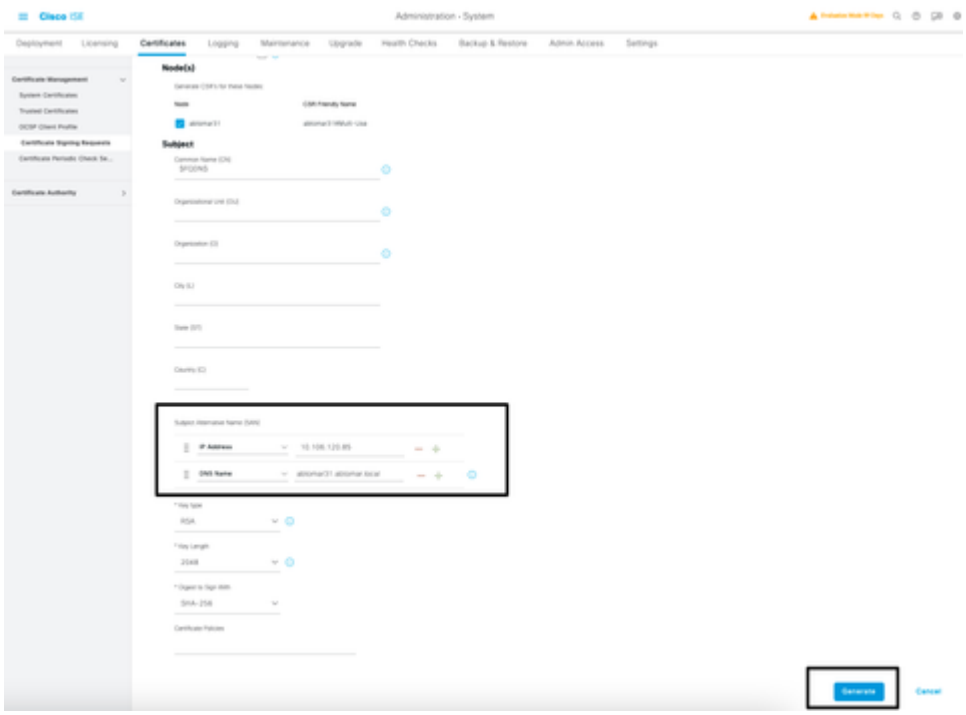


Générer une requête de signature de certificat

Cette procédure décrit comment renouveler le certificat à l'aide d'une requête de signature de certificat (CSR) :

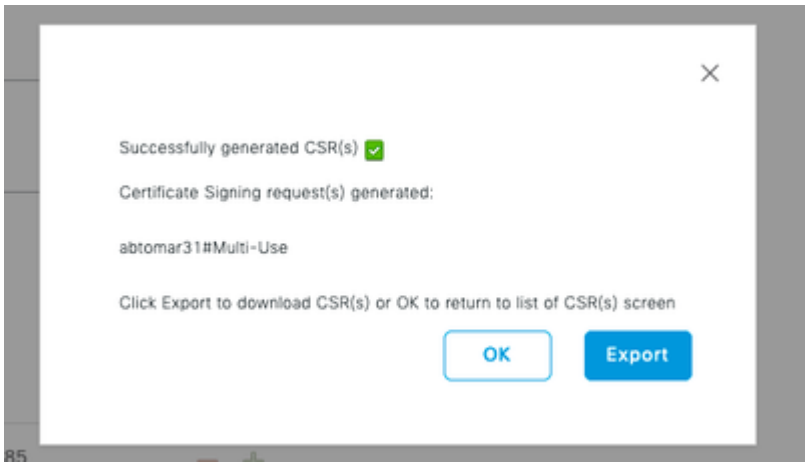
1. Dans la console ISE, accédez à Administration > System > Certificates > Certificate Signing Requests et cliquez sur Generate Certificate Signing Request :

2. Les informations minimales que vous devez saisir dans le champ de texte Certificate Subject (objet du certificat) sont CN=ISEfqdn, où ISEfqdn est le nom de domaine complet (FQDN) de Cisco ISE. Ajoutez des champs supplémentaires comme O (organisation), OU (unité organisationnelle) ou C (pays) dans l'objet du certificat à l'aide de virgules, comme suit :

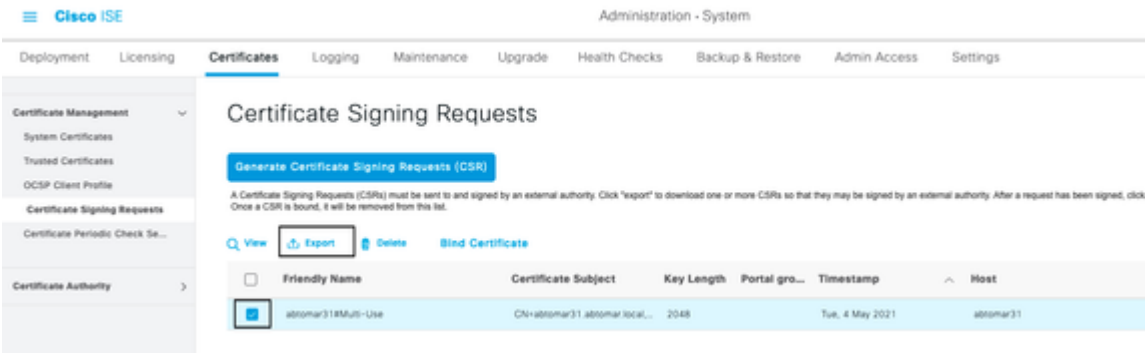


3. L'une des lignes du champ de texte Subject Alternative Name (SAN) doit répéter le nom de domaine complet de Cisco ISE. Vous pouvez ajouter un deuxième champ SAN si vous souhaitez utiliser d'autres noms ou un certificat à caractère générique.

4. Cliquez sur Generate, une fenêtre contextuelle indique si les champs CSR sont remplis correctement ou non :



5. Pour exporter la requête CSR, cliquez sur Certificate Signing Requests (requête de signature de certificat) dans le volet de gauche, sélectionnez votre requête, puis cliquez sur Export: (exporter :).

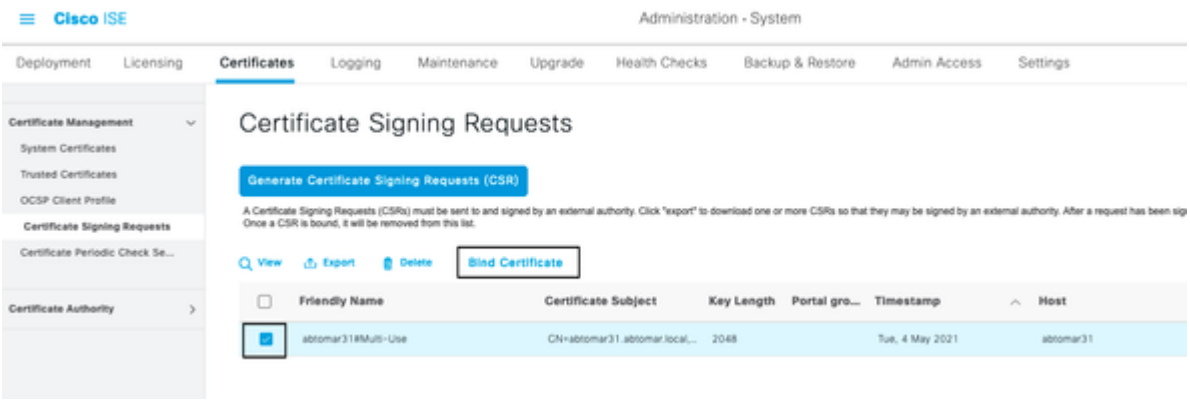


6. Le CSR est stocké sur votre ordinateur. Soumettez-la à l'autorité de certification pour obtenir une signature.

Installer le certificat

Une fois que vous avez reçu le certificat final de votre autorité de certification, vous devez l'ajouter à ISE :

1. Dans la console ISE, accédez à Administration > System > Certificates>Certificate Signing Requests, puis cochez la case sur CRS et cliquez sur Bind Certificate:



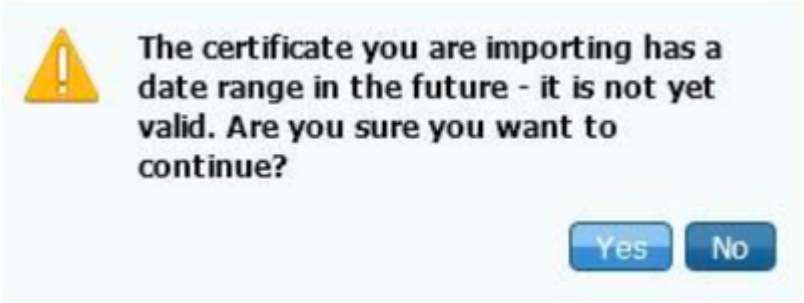
2. Entrez une description simple et claire du certificat dans le champ de texte Friendly Name (nom convivial), puis cliquez sur Submit (envoyer).

> Remarque : N'activez pas le protocole EAP ou Admin pour le moment.

3. Un nouveau certificat non utilisé s'affiche sous System Certificate (certificat du système), comme illustré ici :



4. Étant donné que le nouveau certificat est installé avant l'expiration de l'ancien, un message d'erreur signale une plage de dates future :



5. Cliquez sur Yes (oui) pour continuer. Le certificat est maintenant installé, mais n'est pas utilisé, comme indiqué en vert.



Remarque : Si vous utilisez des certificats autosignés dans un déploiement distribué, le certificat autosigné principal doit être installé dans le magasin de certificats de confiance du serveur ISE secondaire. De même, le certificat autosigné secondaire doit être installé dans le magasin de certificats de confiance du serveur ISE principal. Cela permet aux serveurs ISE de s'authentifier mutuellement. Sans cela, le déploiement peut s'interrompre. Si vous renouvelez des certificats d'une autorité de certification tierce, vérifiez si la chaîne de certificats racine a été modifiée, et assurez-vous de mettre à jour le magasin de certificats de confiance en conséquence dans ISE. Dans les deux scénarios, assurez-vous que les noeuds ISE, les systèmes de contrôle des terminaux et les demandeurs sont en mesure de valider la chaîne de certificats racine.

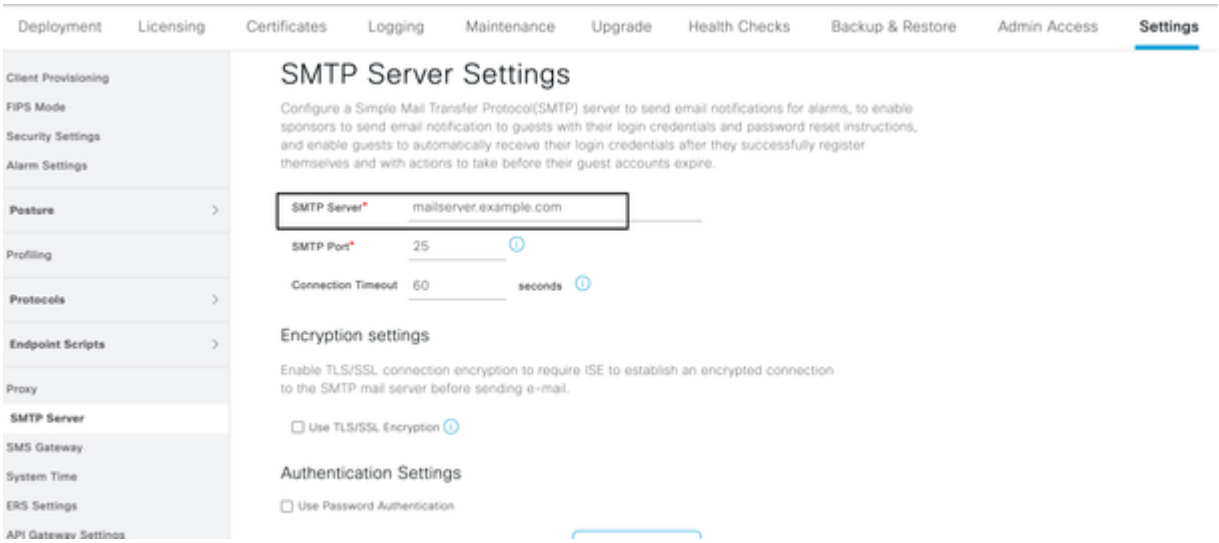
Configurer le système d'alerte

Cisco ISE vous informe lorsque la date d'expiration d'un certificat local survient dans moins de 90 jours. Une telle notification vous permet d'éviter d'atteindre l'expiration des certificats, de planifier le changement de certificat et d'éviter ou de réduire les temps d'arrêt.

La notification s'affiche de plusieurs manières :

- Des icônes d'état d'expiration de couleur sont visibles sur la page des certificats locaux.
- Des avertissements d'expiration figurent dans le rapport de diagnostics du système Cisco ISE.
- Des alertes d'expiration sont générées à 90 jours et à 60 jours, puis chaque jour au cours des 30 jours précédant l'expiration.

Configurez ISE pour recevoir des alertes d'expiration par courriel. Dans la console ISE, naviguez jusqu'à Administration > System > Settings > SMTP Server (gestion > système > paramètres > serveur SMTP), repérez le serveur SMTP (Simple Mail Transfer Protocol) et définissez les autres paramètres du serveur afin que des notifications soient envoyées par courriel pour les alertes :

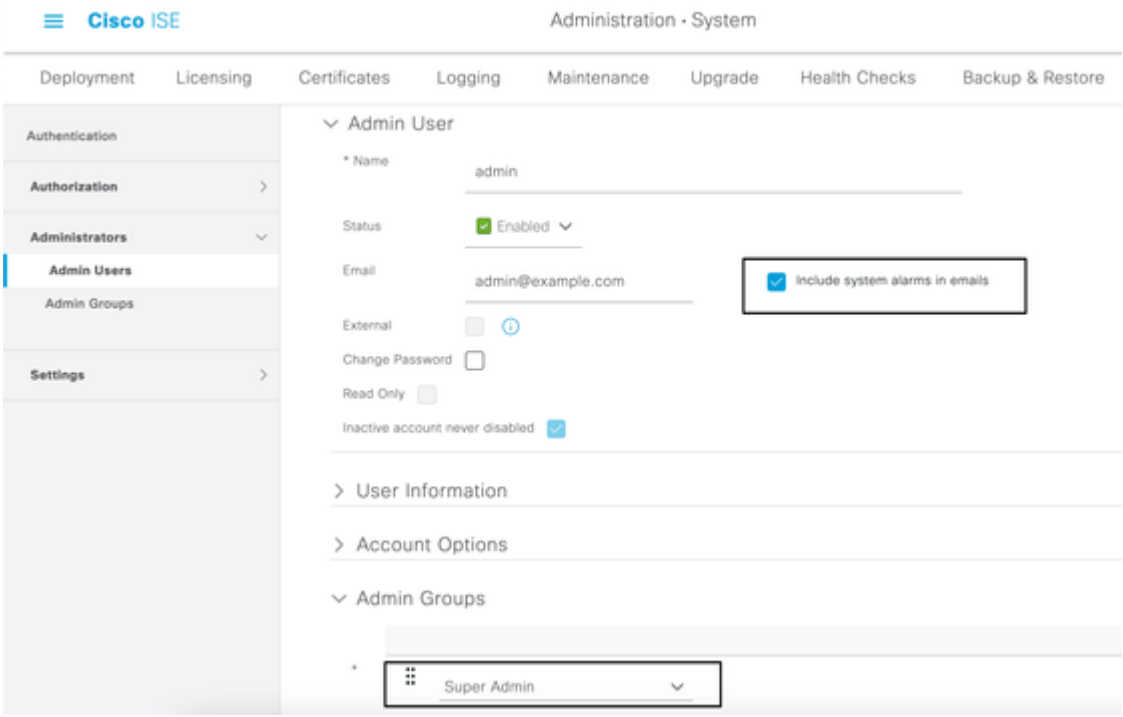


Vous pouvez configurer les notifications de deux manières :

1. Utilisez l'accès administrateur pour envoyer des notifications aux administrateurs :

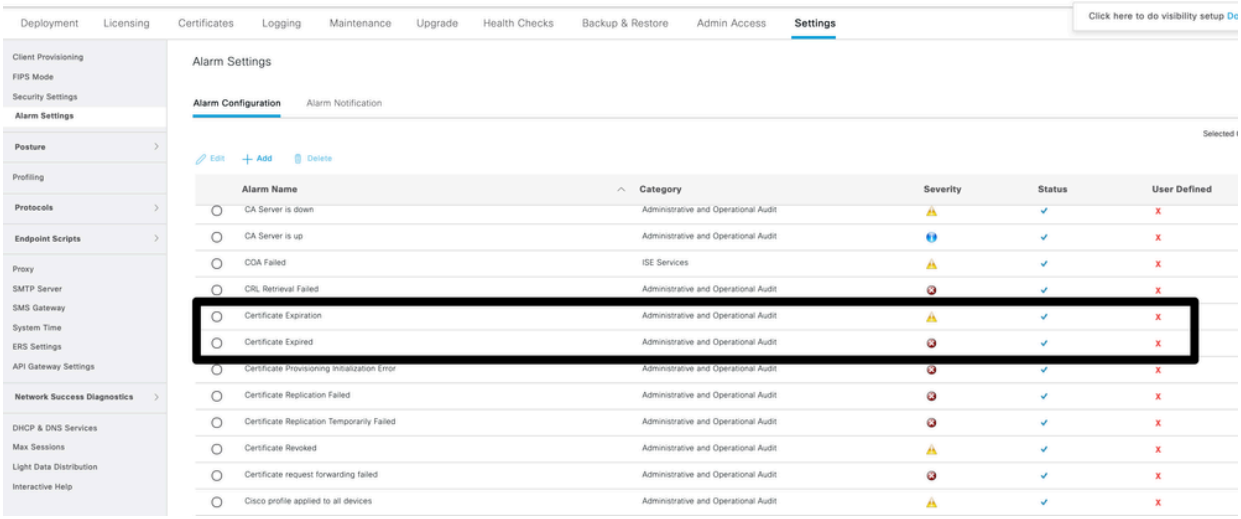
    1. Naviguez vers Administration > System > Admin Access > Administrators > Admin Users (gestion > système > accès administrateur > administrateurs > utilisateurs administrateurs).

    2. Cochez la case Include system alarms in emails (inclure les alertes du système dans les courriels) pour les utilisateurs administrateurs qui doivent recevoir des notifications d'alertes. L'adresse courriel de l'expéditeur des notifications d'alertes est figée dans le code sous la forme ise@hostname (nom de l'hôte).



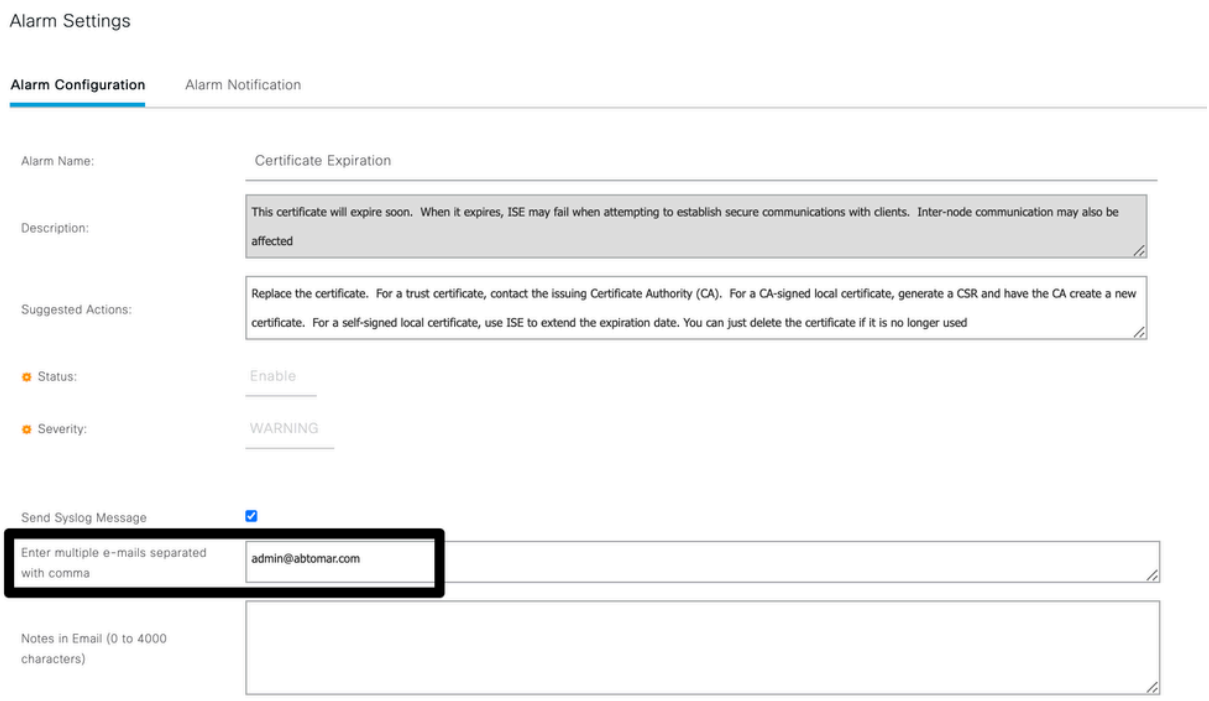
2. Configurez les paramètres d'alertes ISE afin d'informer les utilisateurs :

   1. Naviguez vers Administration > System > Settings > Alarm Settings > Alarm Configuration (gestion > système > paramètres > paramètres de l'alerte > configuration de l'alerte), comme illustré dans cette image.



> Remarque : Désactivez l'état d'une catégorie si vous souhaitez désactiver les alertes de cette catégorie.

   2. Sélectionnez Certificate Expiration, puis cliquez sur Alarm Notification. Saisissez les adresses e-mail des utilisateurs à avertir et enregistrez la modification de configuration. Les modifications peuvent prendre jusqu'à 15 minutes avant d'être actives.

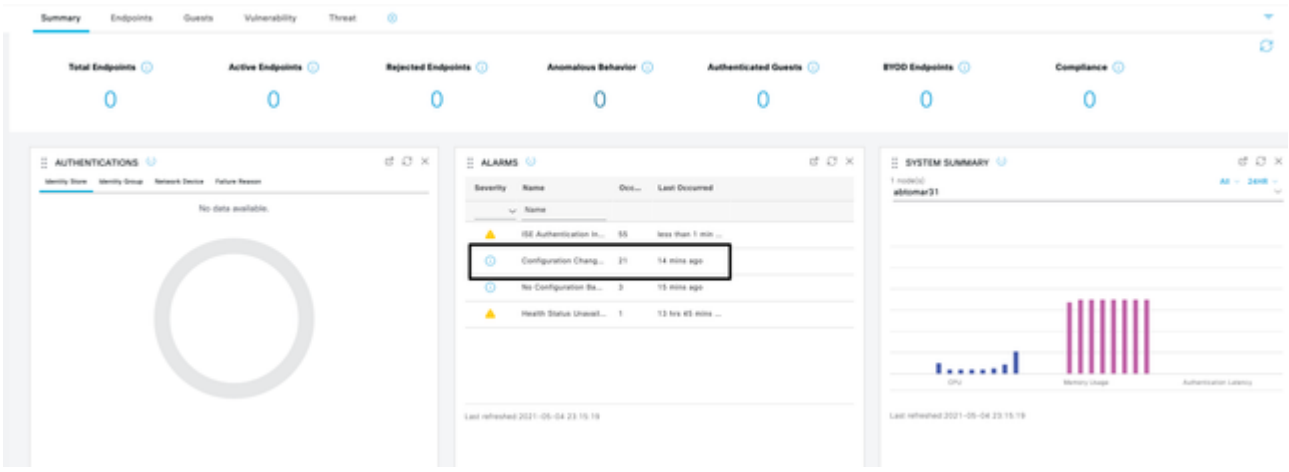


Vérifier

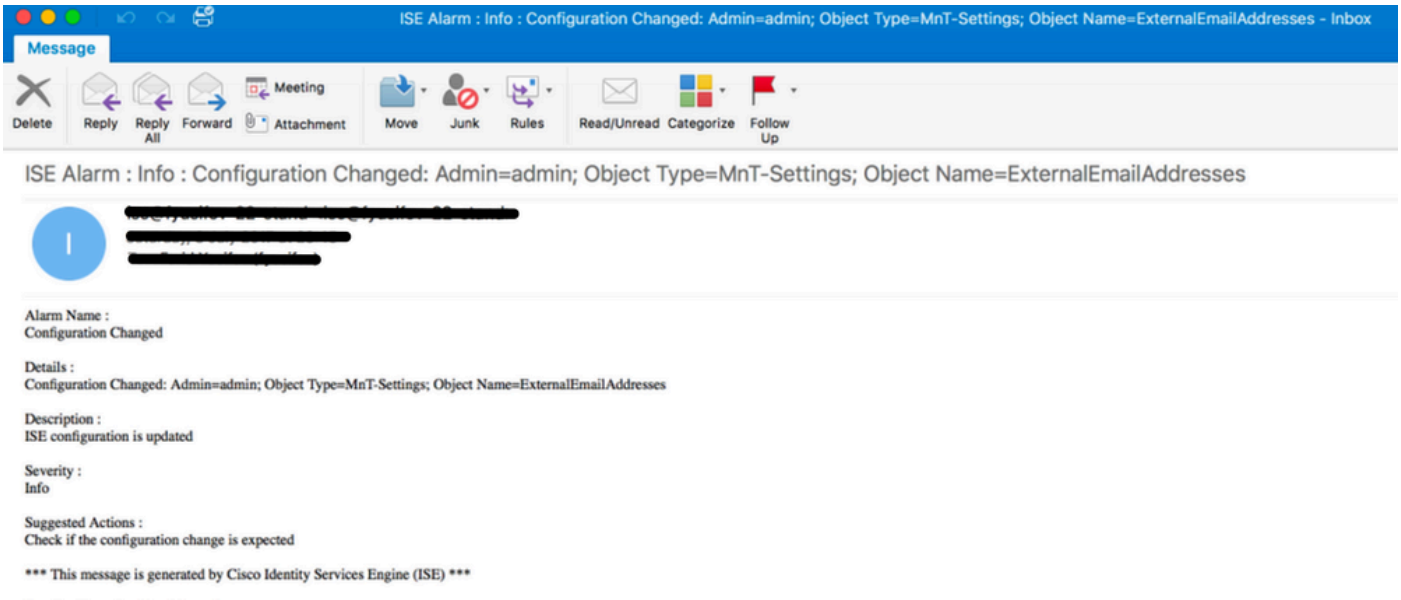
Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Vérifier le système d'alerte

Vérifiez que le système d'alerte fonctionne correctement. Dans cet exemple, une modification de la configuration génère une alerte avec un niveau de gravité Information. (Un niveau d'alerte Information est du niveau de gravité le plus faible, tandis que les expirations de certificat génèrent un niveau de gravité d'avertissement plus élevé.)



Voici un exemple d'alerte envoyée par courriel par l'ISE :

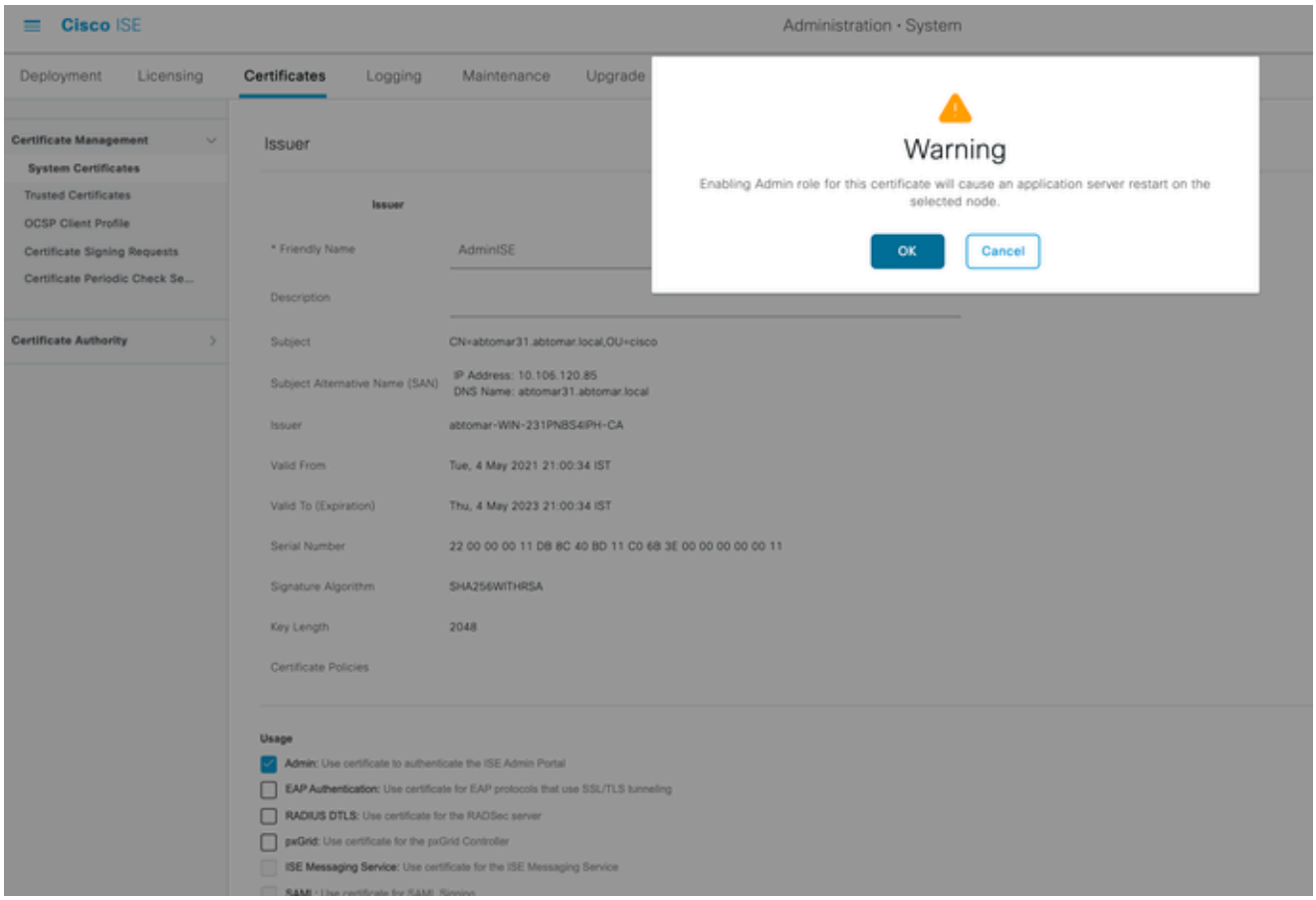


Vérifier le changement de certificat

Cette procédure décrit comment vérifier que le certificat est installé correctement et comment modifier les rôles EAP et/ou Admin :

1. Sur la console ISE, naviguez vers Administration > Certificates > System Certificates (gestion > certificats > certificats de système) et sélectionnez le nouveau certificat afin d'en afficher les détails.

> ⚠ Mise en garde : Si vous activez l'utilisation Admin, le service ISE redémarre, ce qui entraîne un temps d'arrêt du serveur.



2. Pour vérifier l'état du certificat sur le serveur ISE, entrez la commande suivante dans l'interface CLI :

<#root>

CLI:>

show application status ise

3. Une fois que tous les services sont actifs, essayez de vous connecter en tant qu'administrateur.

4. Pour un scénario de déploiement distribué, accédez à Administration > System > Deployment. Vérifiez que l'icône du noeud est verte. Placez le curseur sur l'icône pour vérifier que la légende indique Connecté.

5. Vérifiez que l'authentification de l'utilisateur final a réussi. Pour ce faire, accédez à Operations > RADIUS > Livelogs. Vous pouvez trouver une tentative d'authentification spécifique et vérifier que ces tentatives ont été authentifiées avec succès.

Vérifier le certificat

Si vous souhaitez vérifier le certificat de l’extérieur, vous pouvez utiliser les outils Microsoft Windows intégrés ou la boîte à outils OpenSSL.

OpenSSL est une implémentation libre du protocole SSL (Secure Sockets Layer). Si les certificats utilisent votre propre autorité de certification privée, vous devez placer votre certificat racine provenant d’une autorité de certification sur un ordinateur local et utiliser l’option OpenSSL - CApath. Si vous disposez d’une autorité de certification intermédiaire, vous devez également placer le certificat dans le même répertoire.

Afin d’obtenir des informations générales sur le certificat et de le vérifier, utilisez :

<#root>

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

Il peut également être utile de convertir les certificats avec la boîte à outils OpenSSL :

<#root>

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

Dépannage

Aucune information de diagnostic spécifique n'est actuellement disponible pour cette configuration.

Conclusion

Comme vous pouvez installer un nouveau certificat sur ISE avant qu’il ne soit actif, Cisco vous recommande de le faire avant l’expiration de l’ancien certificat. Cette période de chevauchement entre la date d’expiration de l’ancien certificat et la date de début du nouveau certificat vous donne le temps de renouveler les certificats et de planifier leur installation avec peu ou pas de temps d’arrêt. Une fois que la plage de dates de validité du nouveau certificat est en vigueur, activez le protocole EAP et/ou Admin. N’oubliez pas que si vous activez l’utilisation par l’administrateur, le service redémarrera.

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.