Configurer l'authentification basée sur un certificat ou une carte à puce pour l'administration ISE

Contenu

Introduction

Ce document décrit comment configurer l'authentification basée sur le certificat client pour l'accès de gestion ISE (Identity Services Engine). Dans cet exemple, l'administrateur ISE s'authentifie auprès du certificat utilisateur pour obtenir l'accès administrateur à l'interface utilisateur graphique de gestion de Cisco ISE (Identity Services Engine).

Conditions préalables

Conditions requises

Cisco recommande de connaître ces sujets :

- Configuration ISE pour l'authentification par mot de passe et certificat.
- Microsoft Active Directory (AD)

Components Used

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

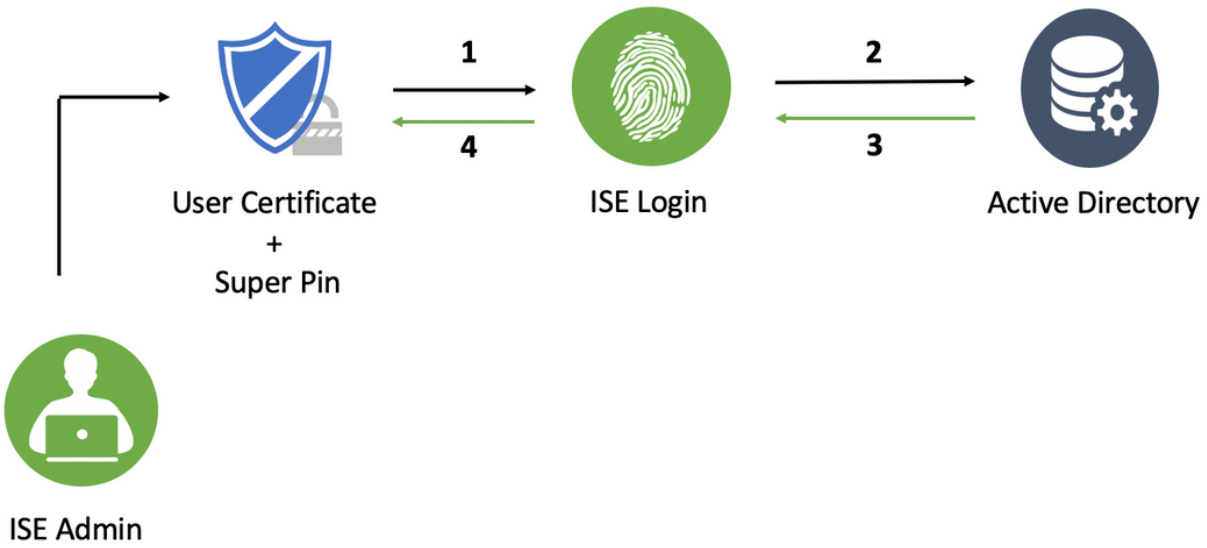
- Cisco Identity Services Engine (ISE) version 2.6
- Windows Active Directory (AD) Server 2008 version 2
- Certificat

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 le réseau est actif, assurez-vous de comprendre l'impact potentiel de toute configuration.

Configuration

Utilisez cette section pour configurer le certificat client ou la carte à puce en tant qu'identité externe pour l'accès administratif à l'interface utilisateur graphique de gestion de Cisco ISE.

Diagramme du réseau

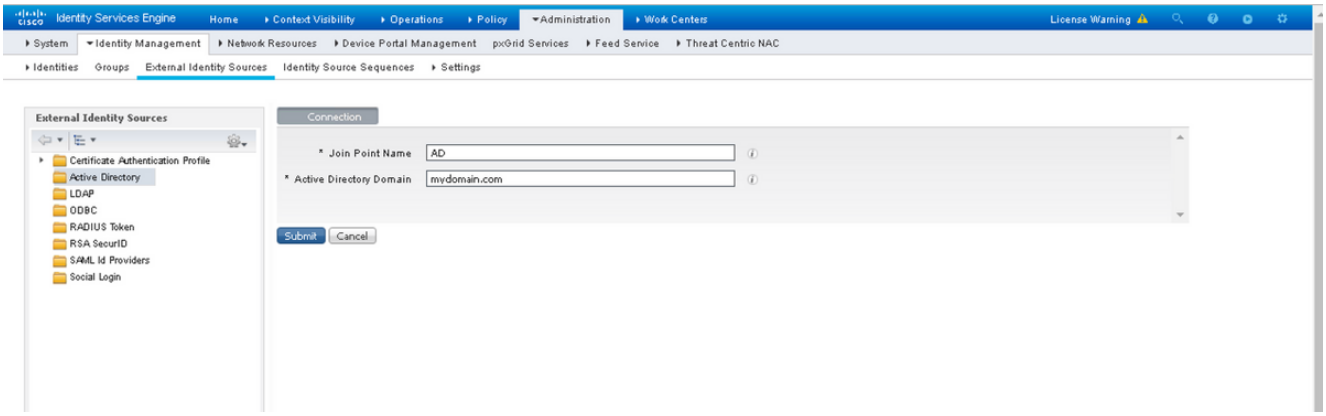


Rejoindre ISE à Active Directory

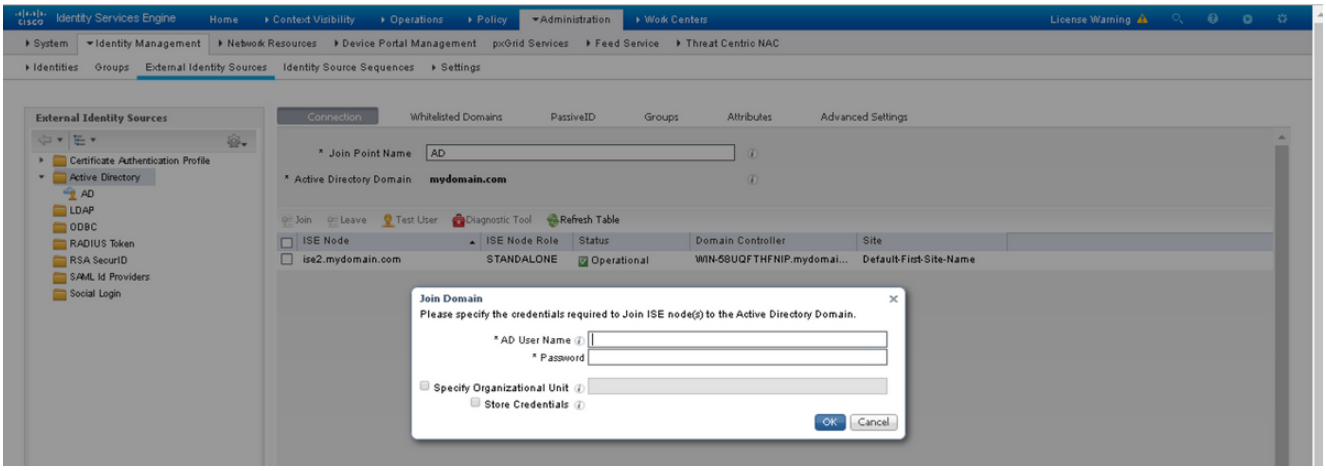
1. Sélectionnez **Administration > Gestion des identités > Sources d'identité externes > Active Directory.**

2. Créez une instance Active Directory avec le **nom du point de jointure** et le **domaine AD** dans Cisco ISE.

3. Cliquez sur Submit.



4. Rejoignez tous les noeuds avec le **nom d'utilisateur** et le **mot de passe** appropriés dans l'invite.



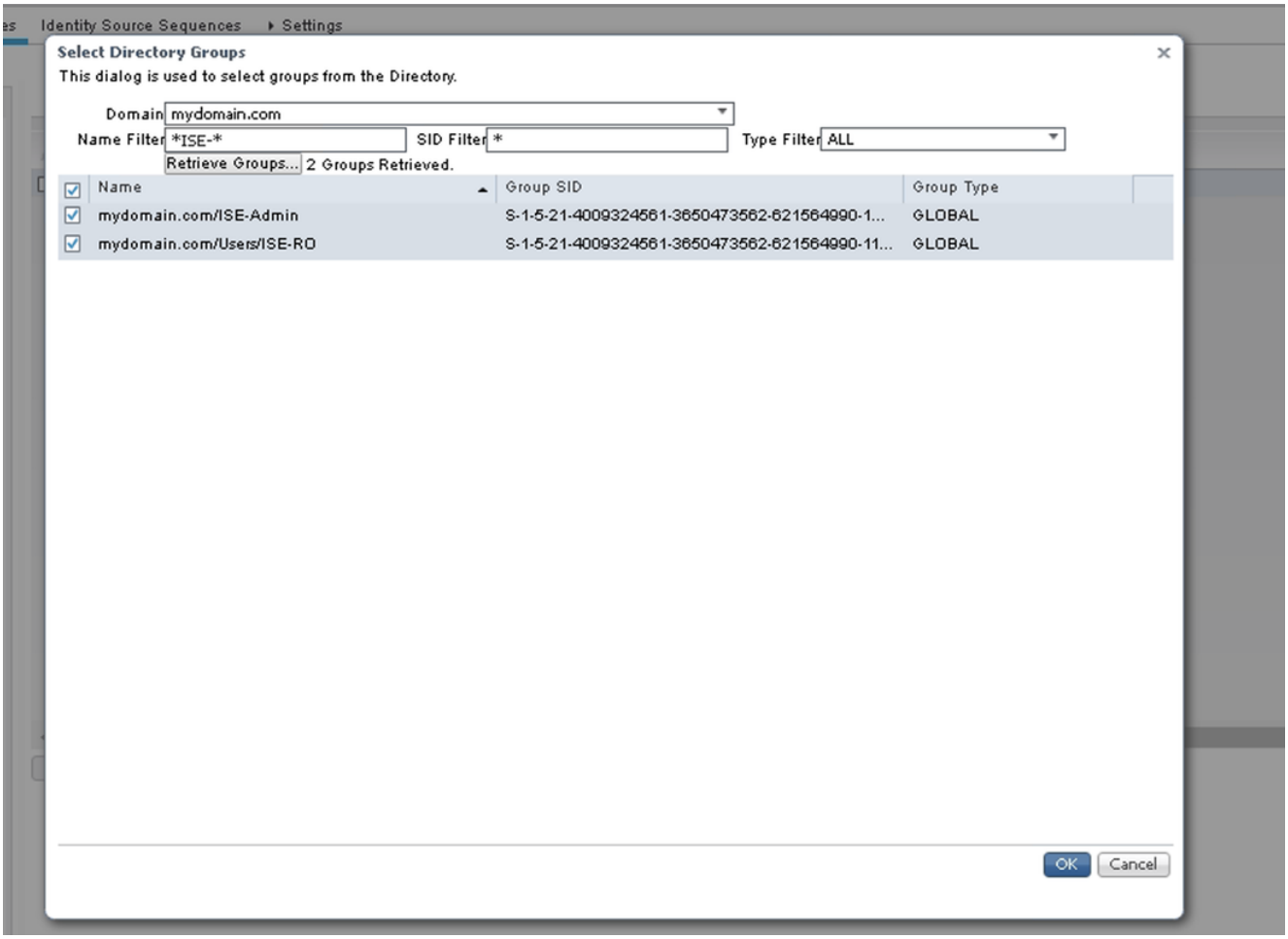
5. Click **Save**.

Sélectionner des groupes de répertoires

1. Créez un groupe Administrateur externe et associez-le au groupe Active Directory.

2. Sélectionnez **Administration >Gestion des identités > Sources d'identité externes > Active Directory > Groupes > Sélectionner des groupes dans le répertoire.**

3. Récupérez au moins un groupe AD auquel appartient l'administrateur.

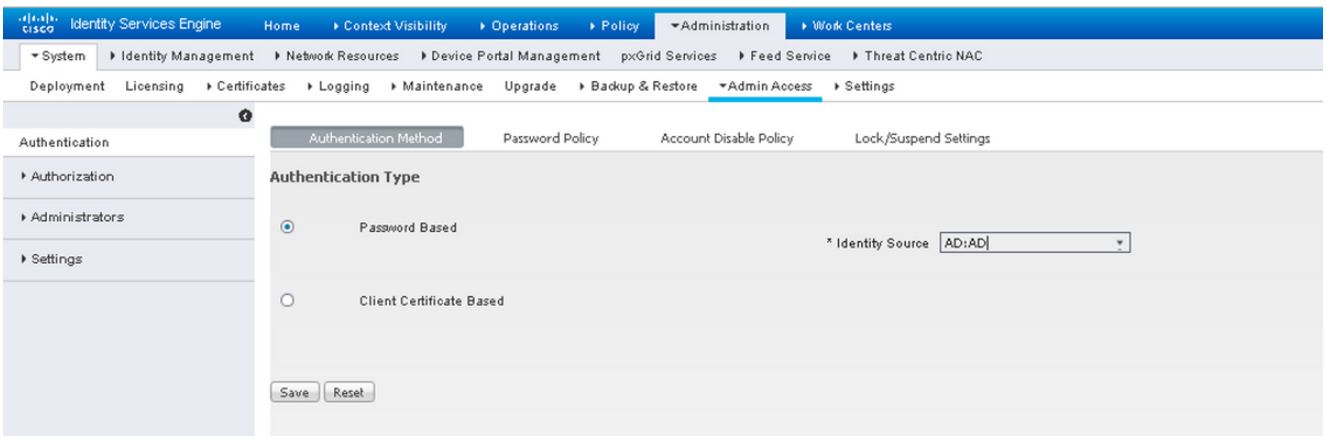


4. Click **Save**.

Activer l'authentification par mot de passe Active Directory pour l'accès administratif

1. Activez l'instance active directory comme méthode d'authentification basée sur le mot de passe qui a rejoint ISE précédemment.

2. Choisissez **Administration > System > Admin access > Authentication**, comme l'illustre l'image.



3. Click **Save**.

Note: La configuration de l'authentification basée sur le mot de passe est requise pour

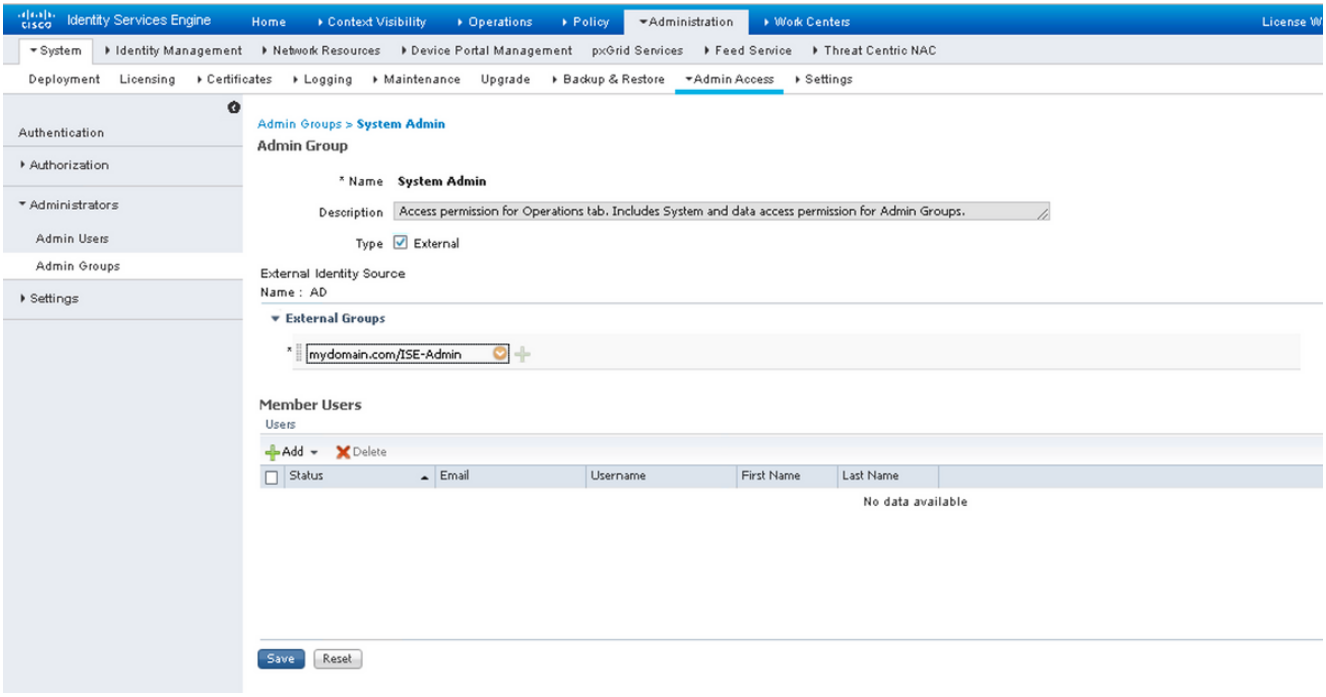
activer l'authentification basée sur le certificat. Cette configuration doit être restaurée après une configuration réussie de l'authentification basée sur les certificats.

Mapper les groupes d'identités externes aux groupes d'administration

Dans cet exemple, le groupe AD externe est mappé au groupe Admin par défaut.

1. Choisissez **Administration > System > Admin Access >Administrators >Groupes d'administrateurs > Super administrateur.**

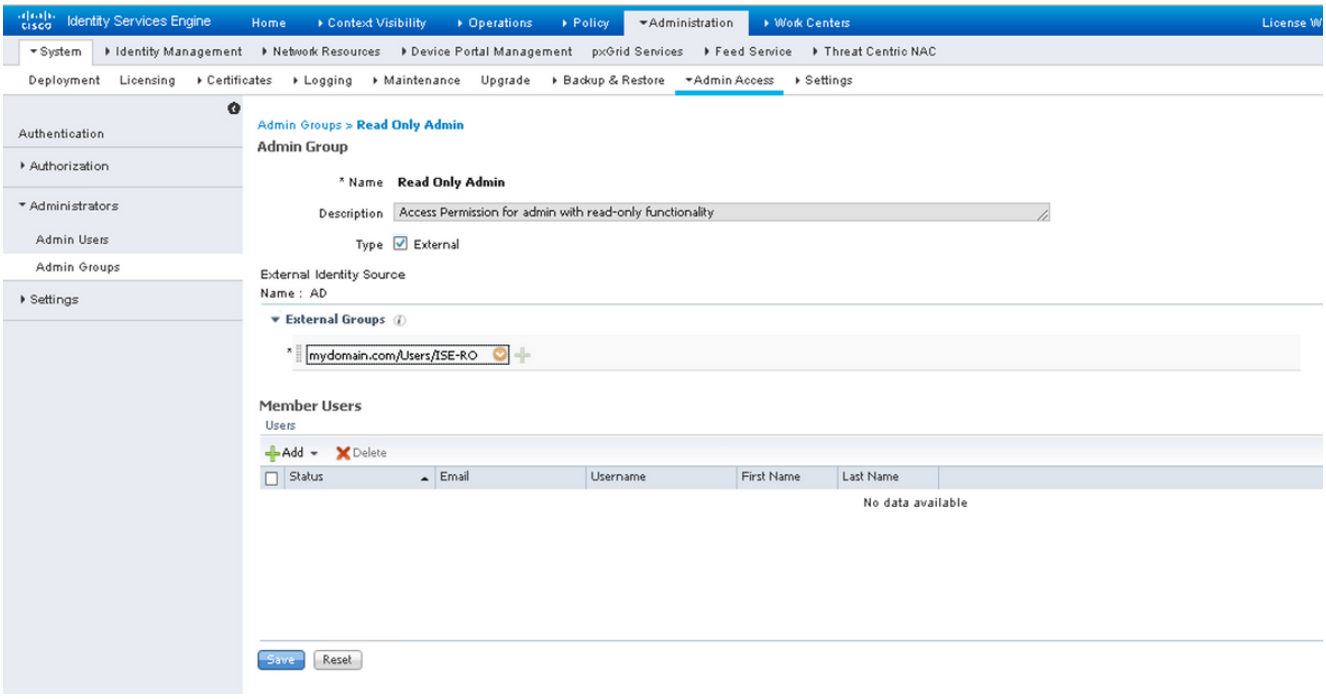
2. Cochez la case Type en tant que **Externe** et sélectionnez le groupe AD sous **Groupes externes**.



3. Click **Save**.

4. Choisissez **Administration > System > Admin Access > Administrators > Admin Groups > Read Only Admin**.

5. Cochez la case Type comme **Externe** et sélectionnez le groupe AD sous **Groupes externes**, comme illustré dans l'image.



6. Click **Save**.

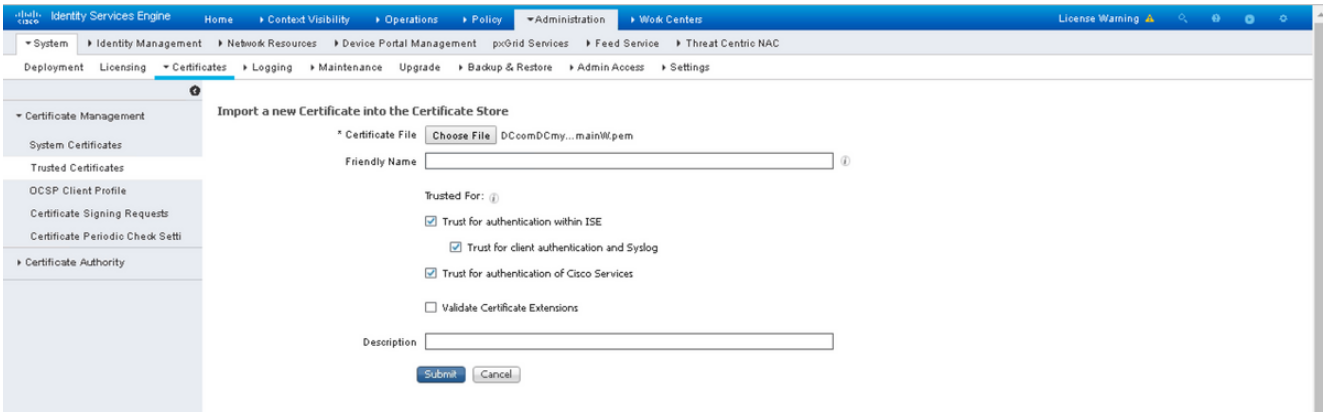
Importer un certificat approuvé

1. Importez le certificat de l'autorité de certification qui signe le certificat client.

2. Choisir **Administrateur > Système > Certificats > Certificat de confiance > Importer.**

3. Cliquez sur Parcourir et choisissez le certificat CA.

4. Cochez la **case Confiance pour l'authentification du client et Syslog**, comme indiqué dans l'image.



5. Cliquez sur Submit.

Configurer le profil d'authentification de certificat

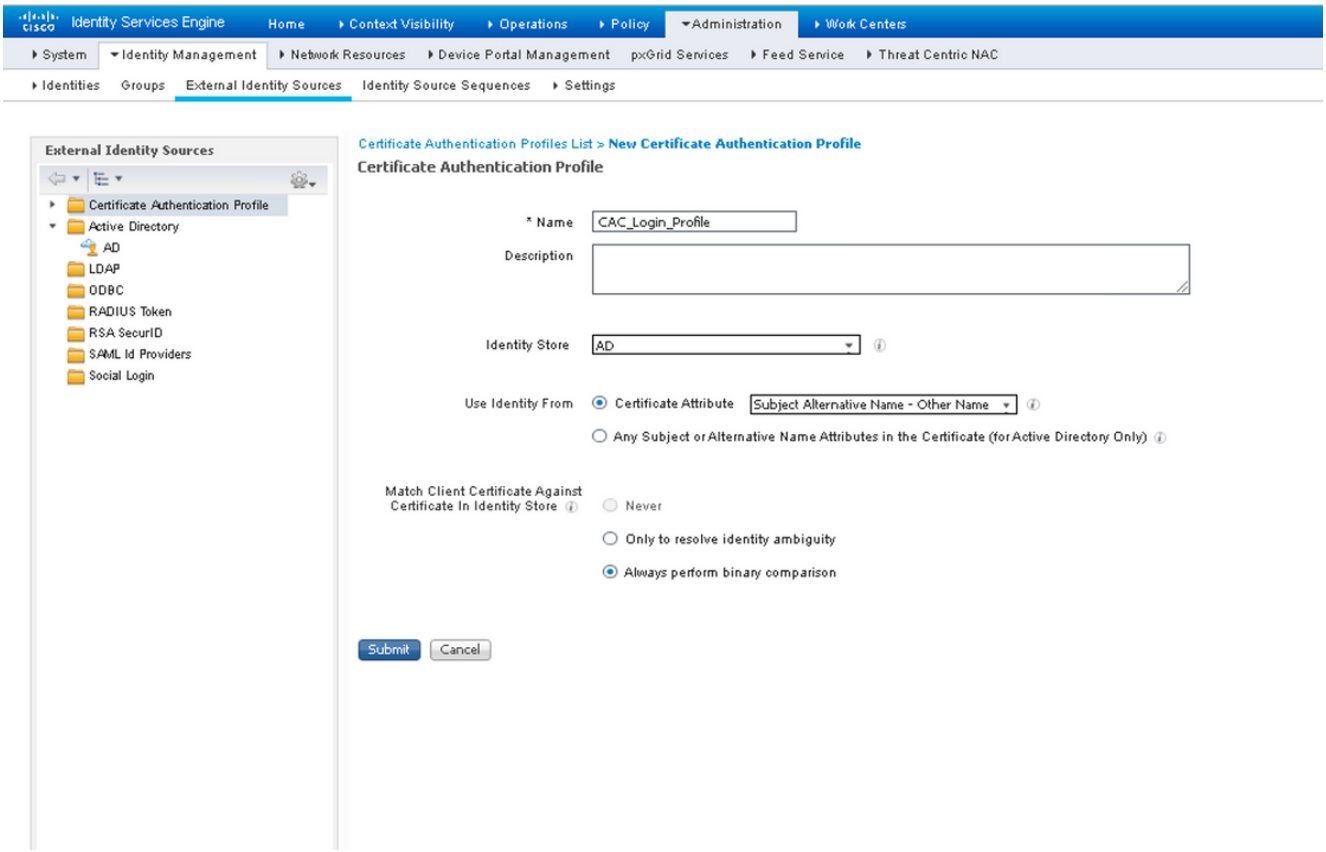
1. Afin de créer un profil d'authentification de certificat pour l'authentification basée sur le certificat client, choisissez **Administration >Gestion des identités > Sources d'identité**

externes > Profil d'authentification de certificat > Ajouter.

2. Ajouter un nom de profil.

3. Sélectionnez l'attribut approprié qui contient le nom d'utilisateur administrateur dans l'attribut de certificat.

4. Si l'enregistrement AD de l'utilisateur contient le certificat de l'utilisateur et que vous souhaitez comparer le certificat reçu du navigateur avec le certificat dans AD, cochez la case **Toujours effectuer une comparaison binaire** et activez le nom d'instance Active Directory spécifié précédemment.

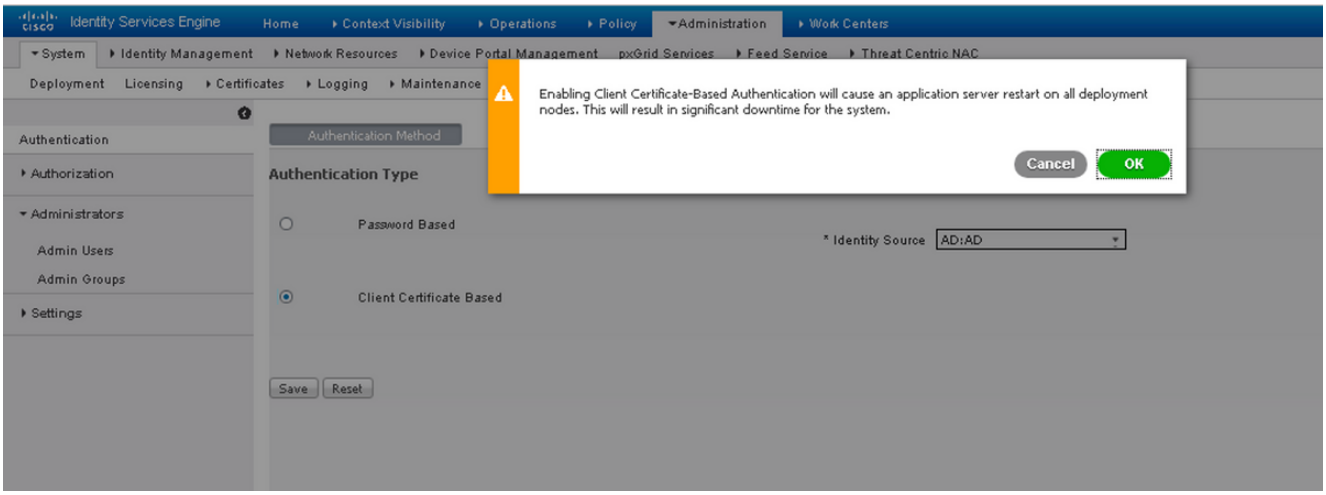


5. Cliquez sur Submit.

Note: Le même profil d'authentification de certificat peut également être utilisé pour l'authentification basée sur l'identité des points de terminaison.

Activer l'authentification basée sur le certificat client

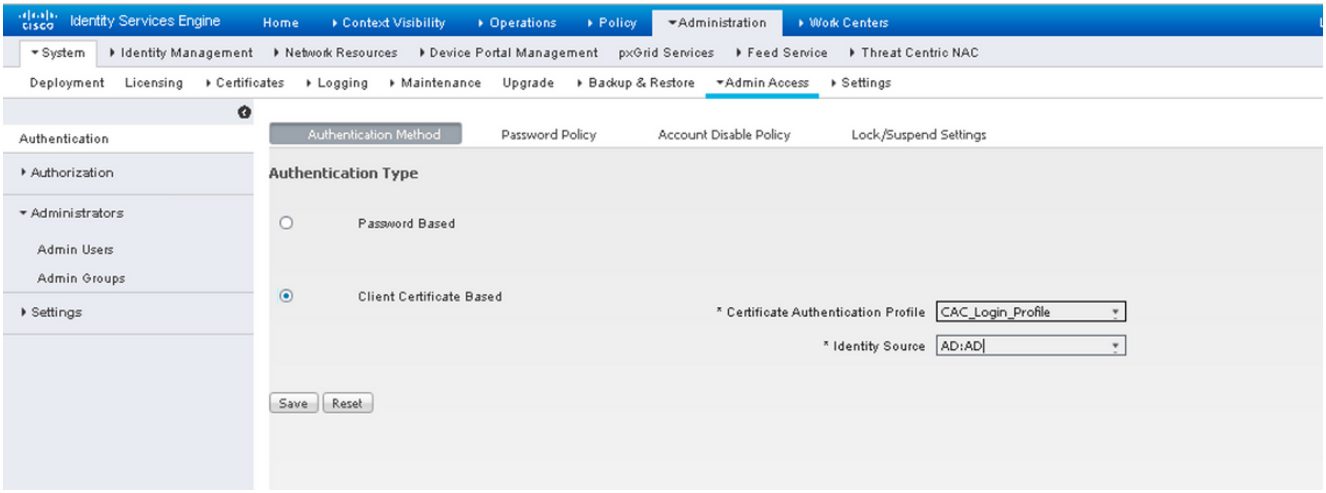
1. Choisir **Administration > System > Admin Access > Authentication > Authentication Method Client Certificate Based.**



2. Click OK.

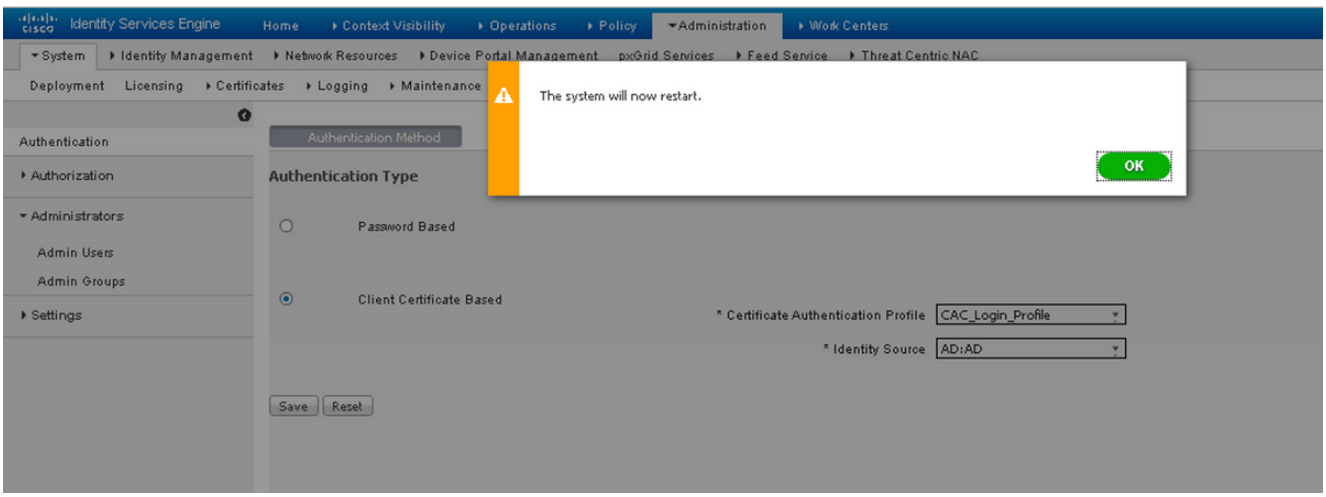
3. Choisissez le **profil d'authentification de certificat** configuré précédemment.

4. Sélectionnez le nom de l'instance Active Directory.



5. Click **Save**.

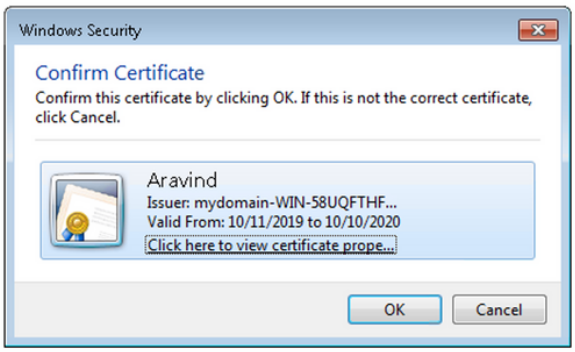
6. Les services ISE sur tous les noeuds du déploiement redémarrent.

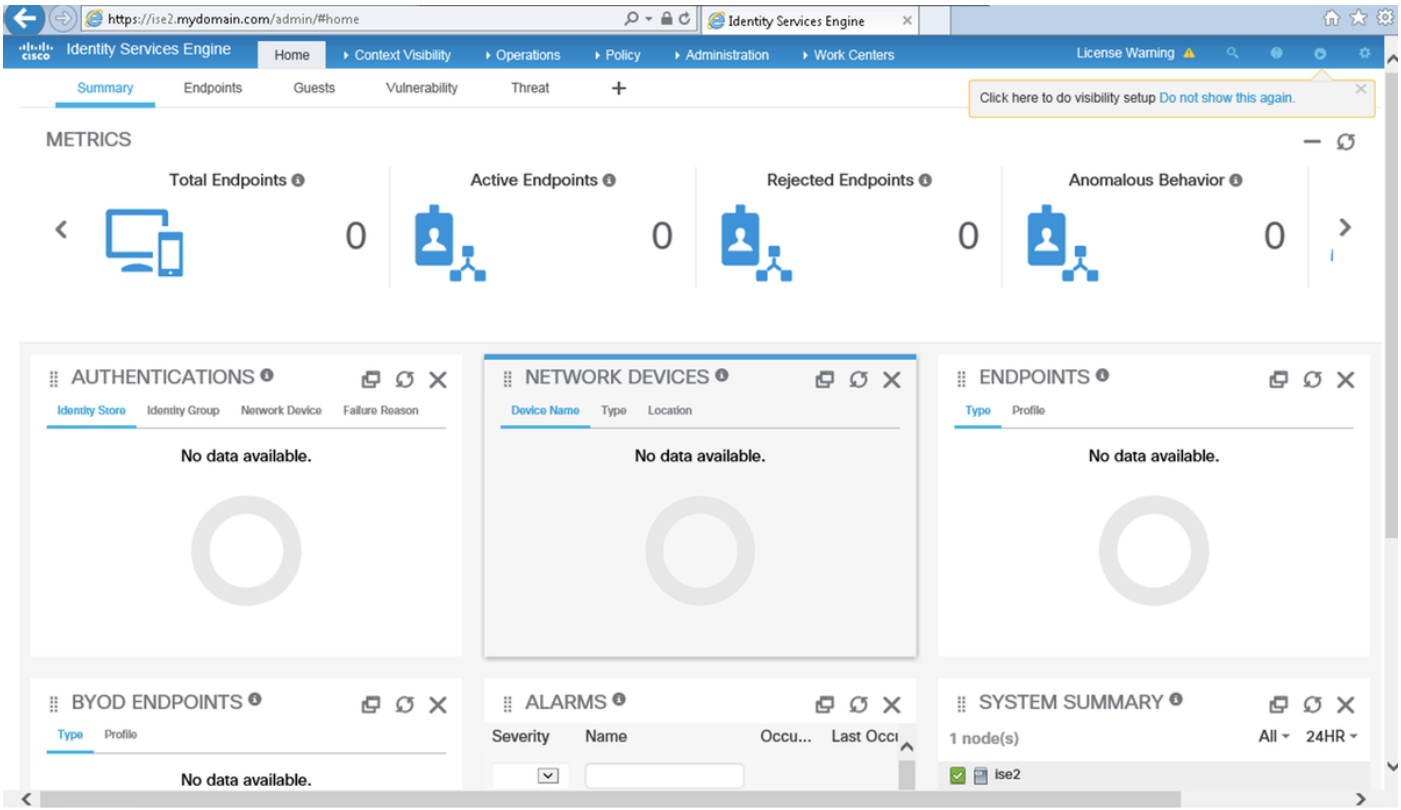


Vérification

Vérifiez l'accès à l'interface utilisateur graphique ISE après que l'état du service **Application Server** soit **en cours d'exécution.**

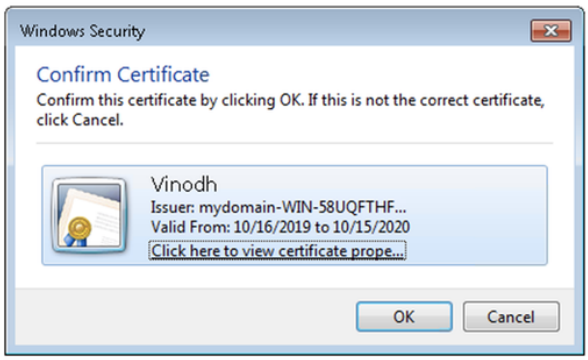
Utilisateur Super Admin : vérifiez que l'utilisateur est invité à choisir un certificat pour se connecter à l'interface utilisateur graphique ISE et qu'il bénéficie des privilèges Super Admin si le certificat appartient à un utilisateur du groupe d'identité externe Super Admin.

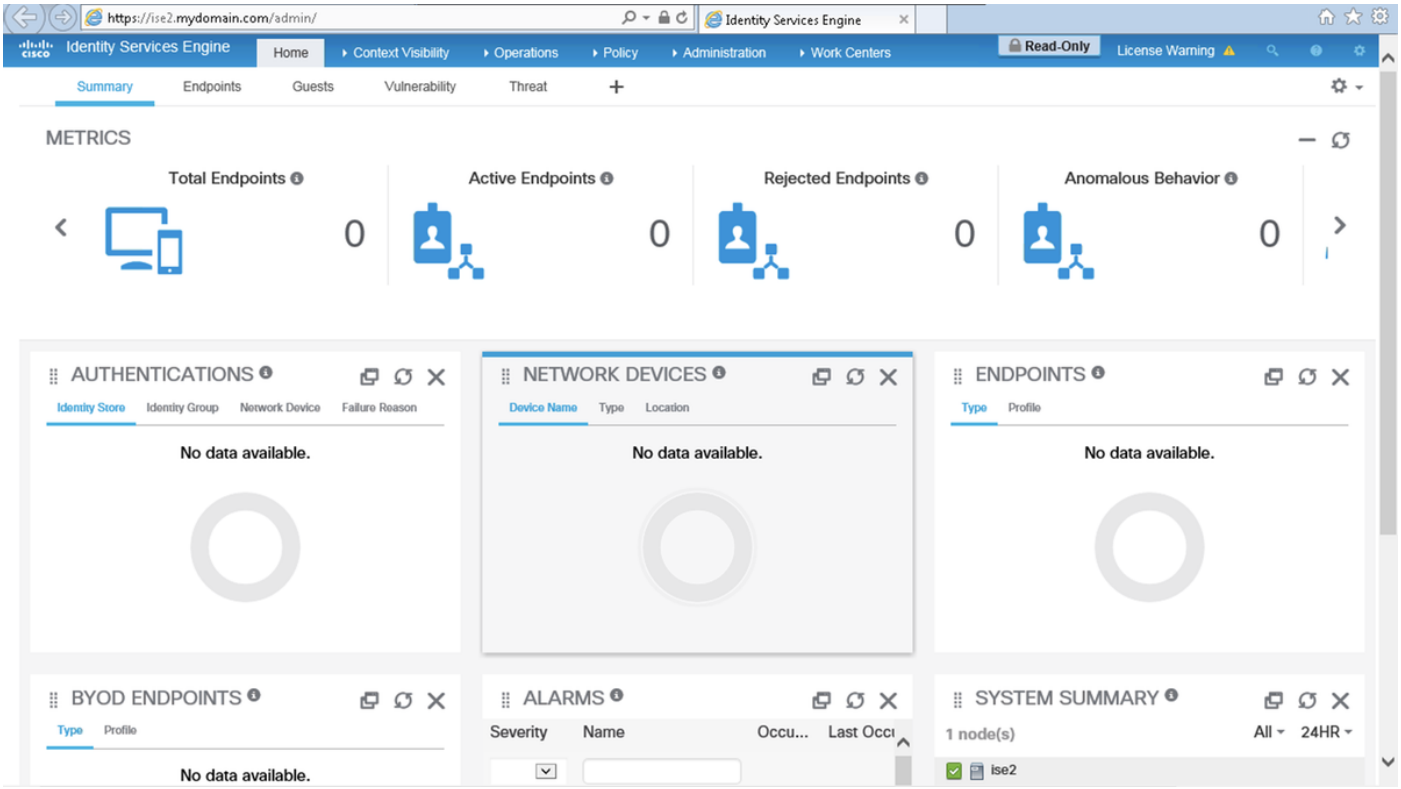




Utilisateur Admin en lecture seule : vérifiez que l'utilisateur est invité à choisir un certificat pour se

connecter à l'interface utilisateur graphique ISE et qu'il dispose de privilèges Admin en lecture seule si le certificat appartient à un utilisateur du groupe Identité externe Admin en lecture seule.





Note: Si la carte d'accès commune (CAC) est utilisée, Smartcard présente le certificat d'utilisateur à ISE une fois que l'utilisateur a entré sa super broche valide.

Dépannage

1. Utilisez la commande **application start ise safe** pour démarrer Cisco ISE en mode sans

échec qui permet de désactiver temporairement le contrôle d'accès au portail Admin et corrigez la configuration et redémarrez les services d'ISE avec la commande **application stop ise** suivie de **application start ise.**

2. L'option safe fournit un moyen de récupération si un administrateur verrouille par inadvertance l'accès au portail d'administration Cisco ISE pour tous les utilisateurs. Cet événement peut se produire si l'administrateur a configuré une liste **d'accès IP** incorrecte dans la **page Administration > Admin Access > Settings > Access**. L'option **safe** ignore également **l'authentification basée sur les certificats** et revient à l'authentification par nom d'utilisateur et mot de passe par défaut pour la connexion au portail d'administration Cisco ISE.