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

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Configurer
  - Diagramme du réseau
  - Rejoindre ISE à Active Directory
  - Sélectionner des groupes de répertoires
  - Activer l'authentification par mot de passe Active Directory pour l'accès administratif
  - Mapper les groupes d'identités externes aux groupes d'administrateurs
  - Importer un certificat sécurisé
  - Configurer le profil d'authentification du certificat
  - Activer l'authentification basée sur les certificats clients
- Vérifier
- Dépannage

Introduction

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

Conditions préalables

Exigences

Cisco recommande d'avoir connaissance de ces sujets :

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

Composants utilisés

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

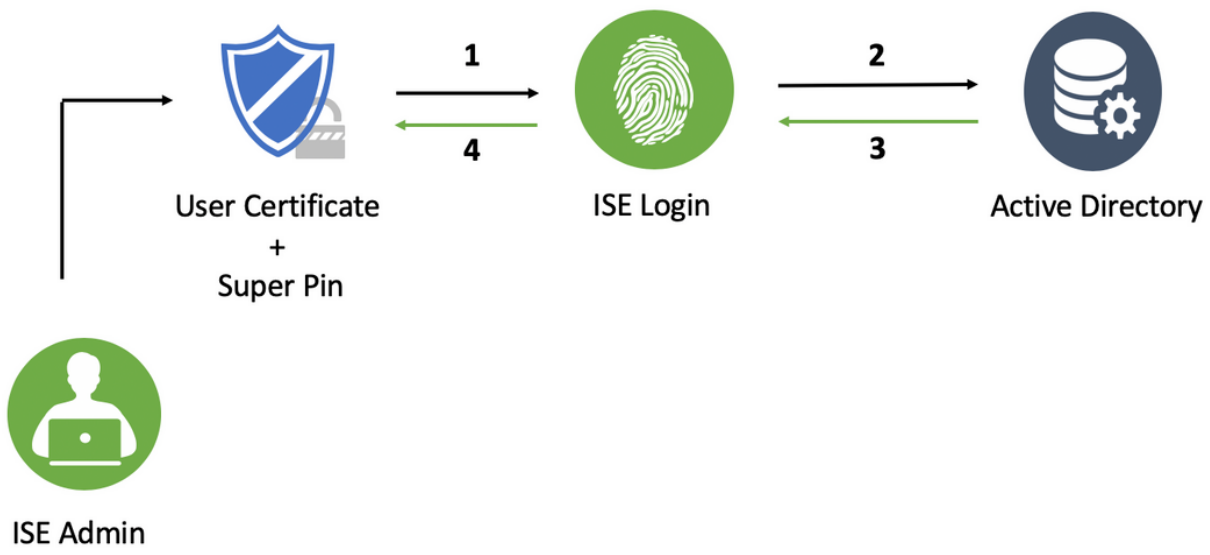
- Cisco Identity Services Engine (ISE) version 2.6
- Windows Active Directory (AD) Server 2008 version 2
- Certificat

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.

Configurer

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 Cisco ISE.

Diagramme du réseau

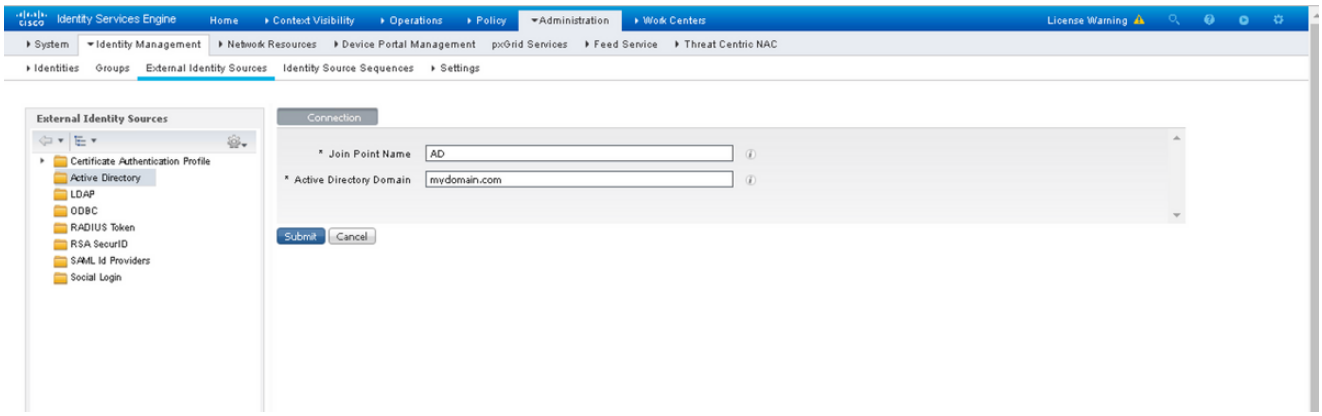


Rejoindre ISE à Active Directory

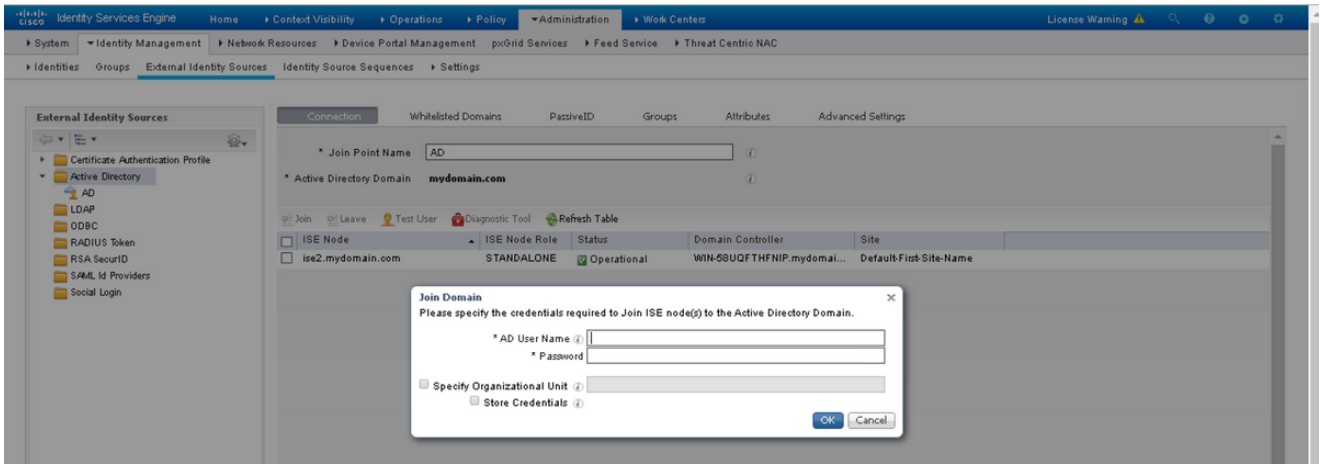
1. Sélectionnez Administration > Gestion des identités > Sources d'identités externes > Active Directory.

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

3. Cliquez sur Submit.



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



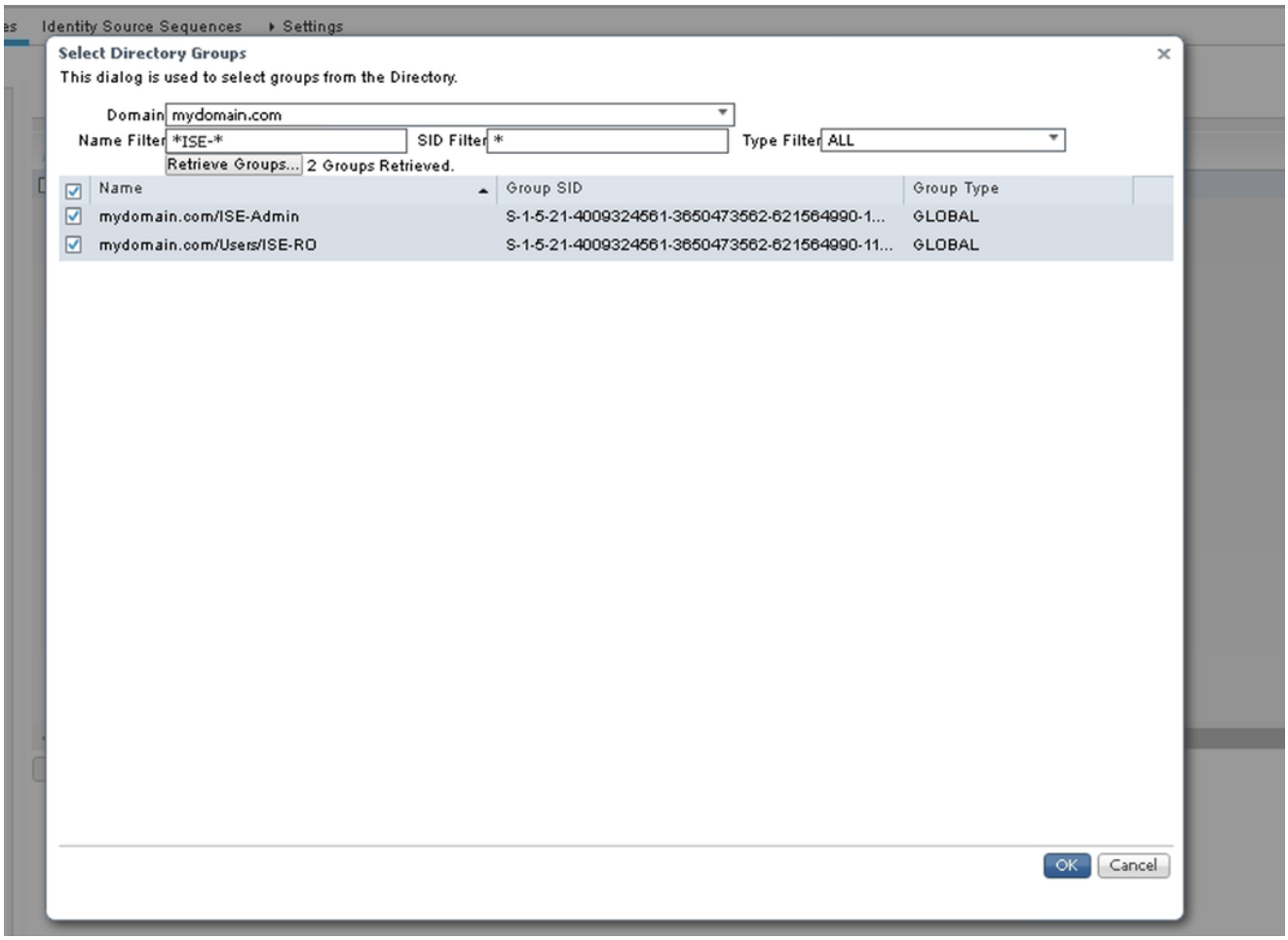
5. Cliquez sur Save.

Sélectionner des groupes de répertoires

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

2. Sélectionnez Administration >Gestion des identités > Sources d'identités externes > Active Directory > Groupes > Sélectionner des groupes dans l'annuaire.

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

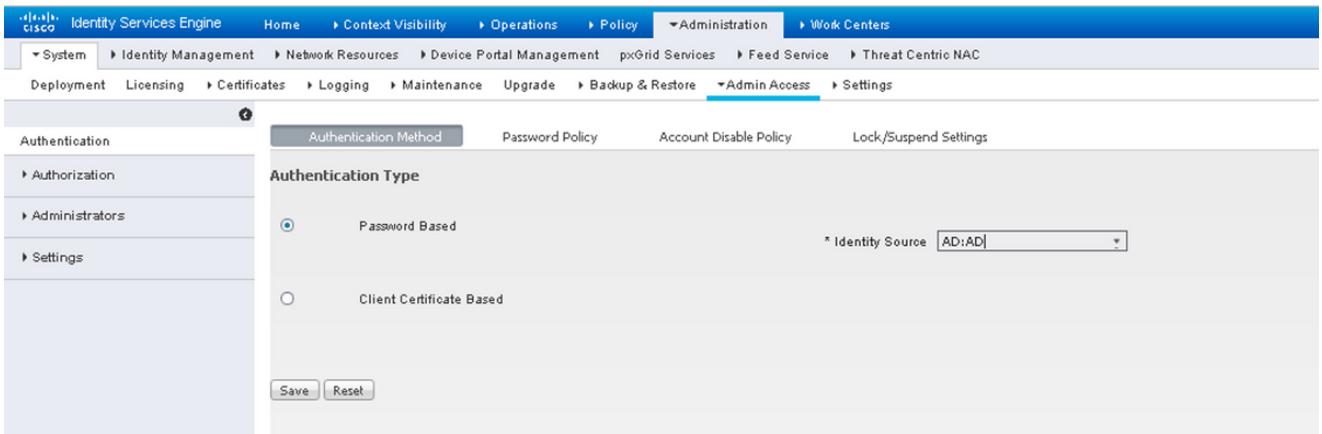


4. Cliquez sur Save.

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

1. Activez l'instance Active Directory en tant que méthode d'authentification basée sur un mot de passe qui a rejoint ISE précédemment.

2. Choisissez Administration > System > Admin access > Authentication, comme illustré dans l'image.



3. Cliquez sur Save.

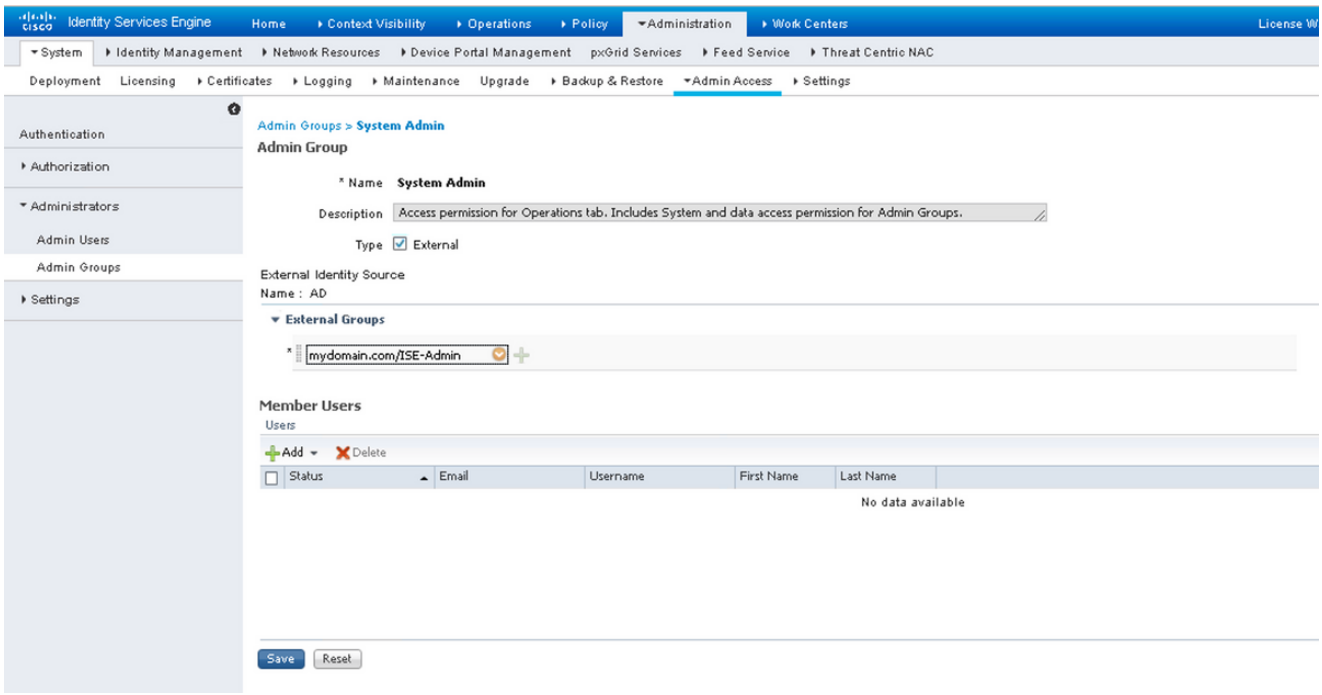
Remarque : La configuration de l'authentification basée sur un mot de passe est requise pour activer l'authentification basée sur un certificat. Cette configuration doit être rétablie après une configuration réussie de l'authentification basée sur les certificats.

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

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

1. Choisissez Administration > System > Admin Access > Administrators >Groupes admin > Super admin.

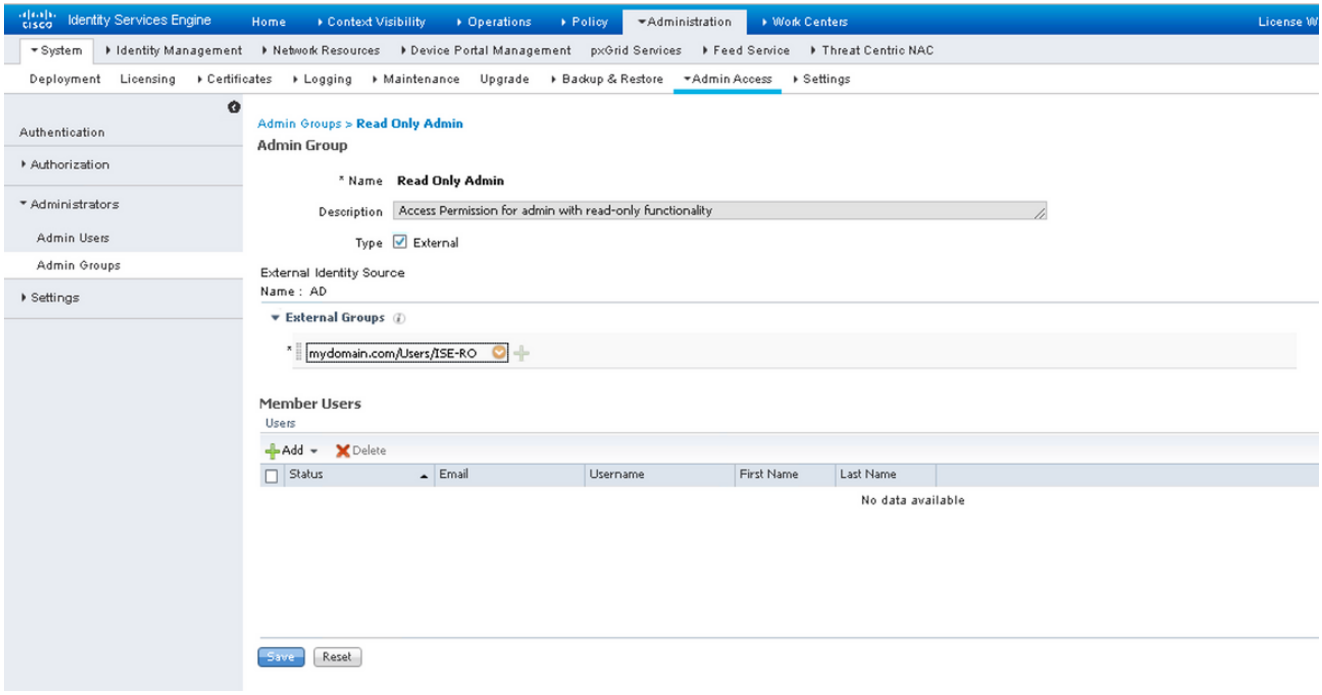
2. Cochez la case Type as External et sélectionnez le groupe AD sous External groups.



3. Cliquez sur Save.

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

5. Cochez la case Type as External et sélectionnez le groupe AD sous External groups, comme illustré dans l'image.



6. Cliquez sur Save.

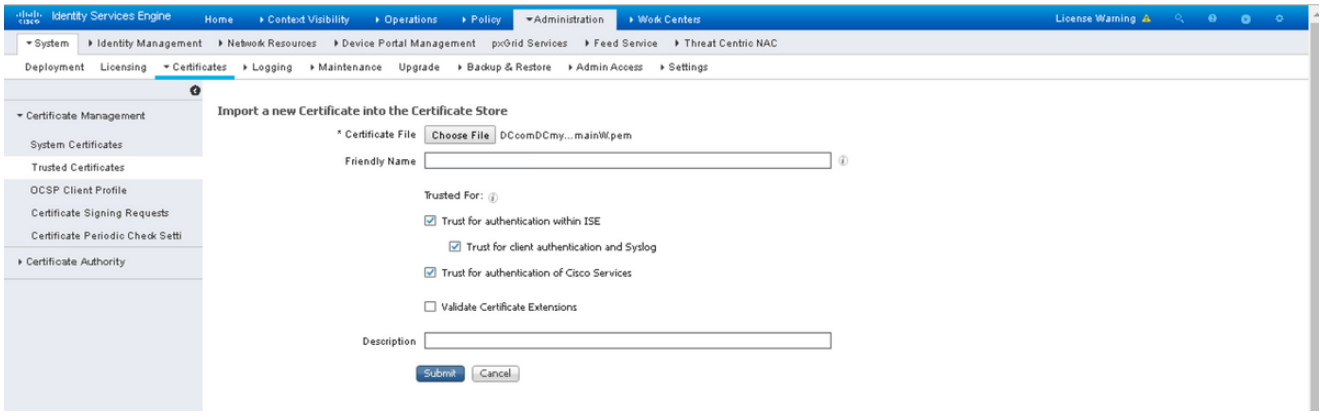
Importer un certificat sécurisé

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 sélectionnez le certificat CA.

4. Cochez la case Trust for client authentication and Syslog, comme indiqué dans l'image.



5. Cliquez sur Submit.

Configurer le profil d'authentification du certificat

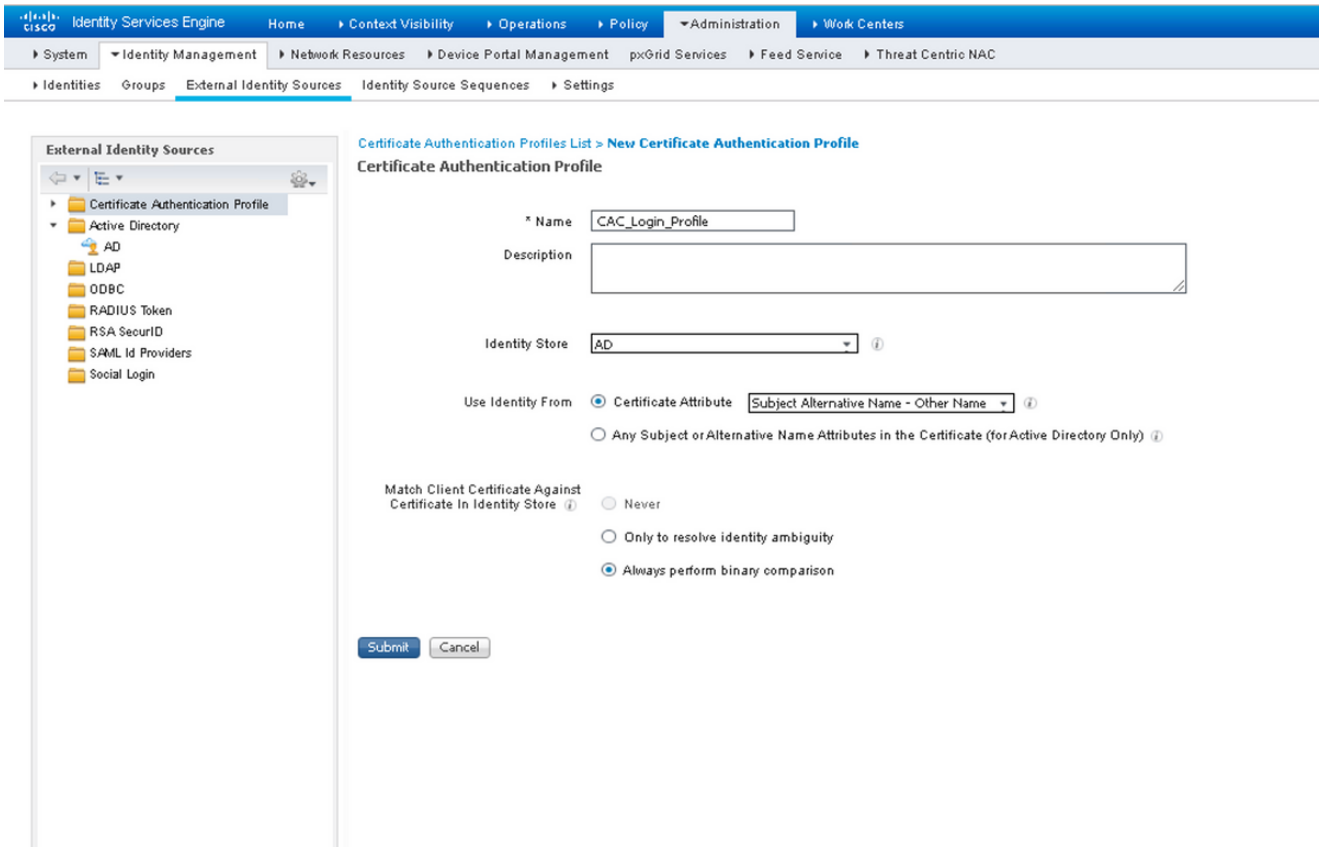
1. Afin de créer un profil d'authentification de certificat pour l'authentification basée sur certificat client, choisissez Administration >Gestion des identités > Sources d'identités externes >

Profil d'authentification du certificat > Ajouter.

2. Ajoutez un nom de profil.

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

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

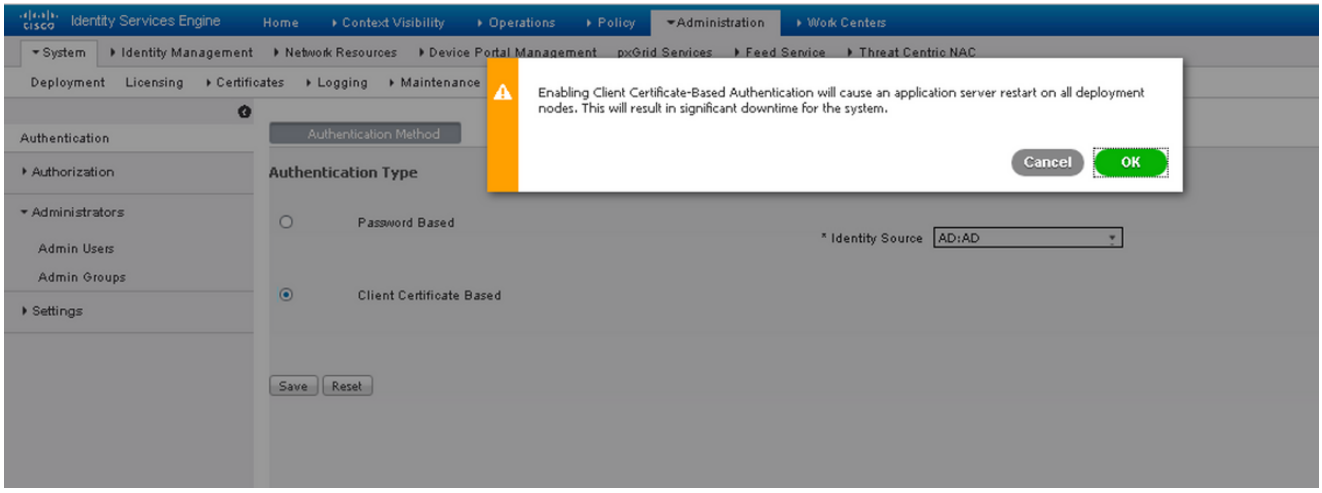


5. Cliquez sur Submit.

Remarque : Le même profil d'authentification de certificat peut également être utilisé pour l'authentification basée sur l'identité du terminal.

Activer l'authentification basée sur les certificats clients

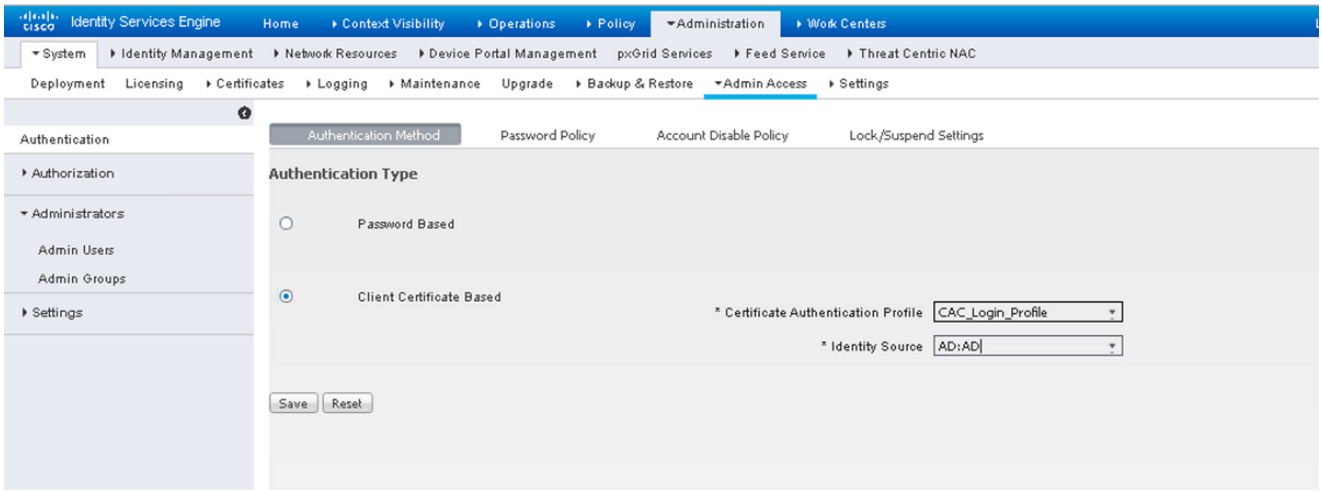
1. Choisir Administration > System > Admin Access > Authentication > Authentication Method Client Certificate Based.



2. Click OK.

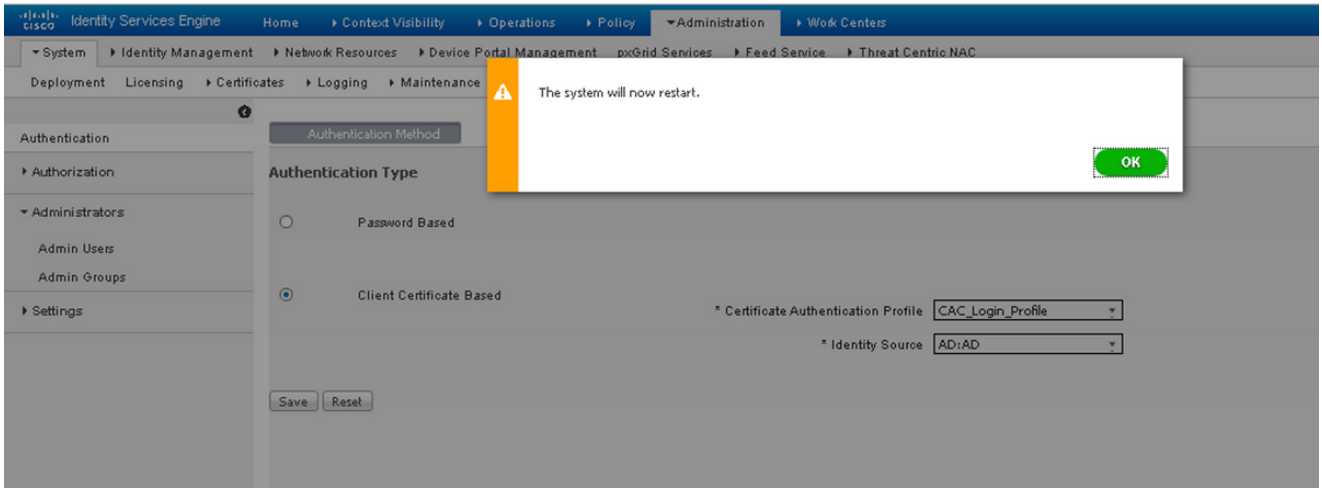
3. Sélectionnez le profil d'authentification de certificat qui est configuré précédemment.

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



5. Cliquez sur Save.

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

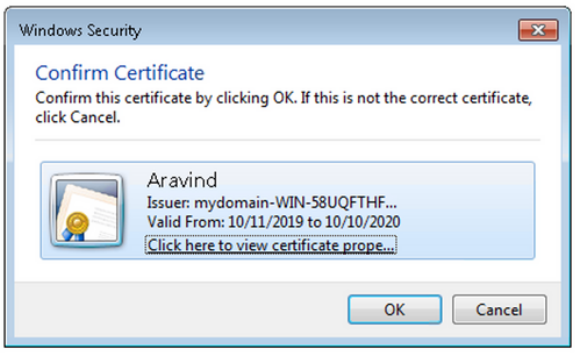


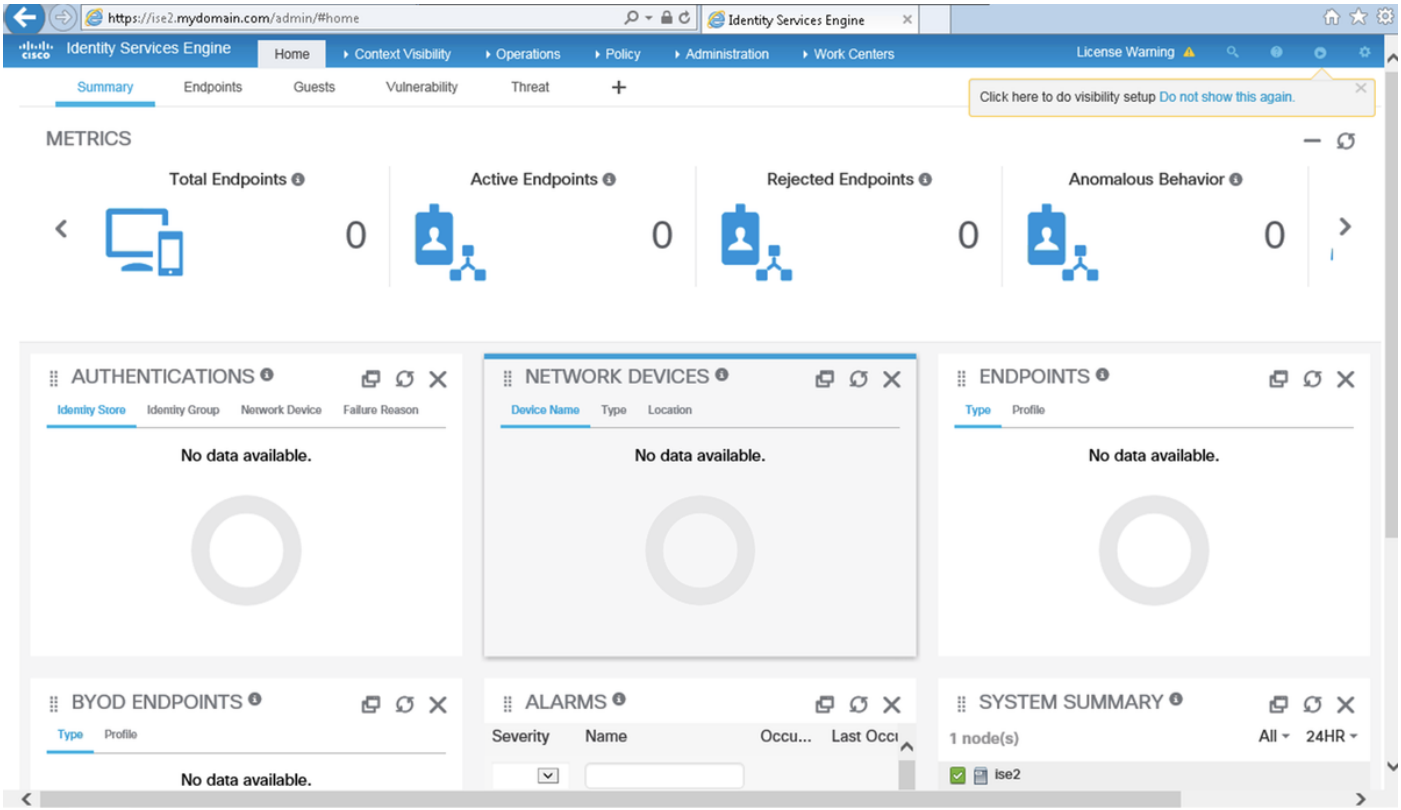
Vérifier

Vérifiez l'accès à l'interface utilisateur graphique ISE après que l'état du service Application Server passe à running.

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 dispose de privilèges Super Admin si le certificat fait partie d'un utilisateur du groupe Identité externe Super Admin.

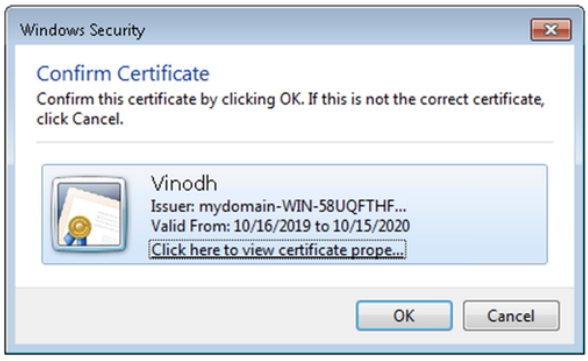


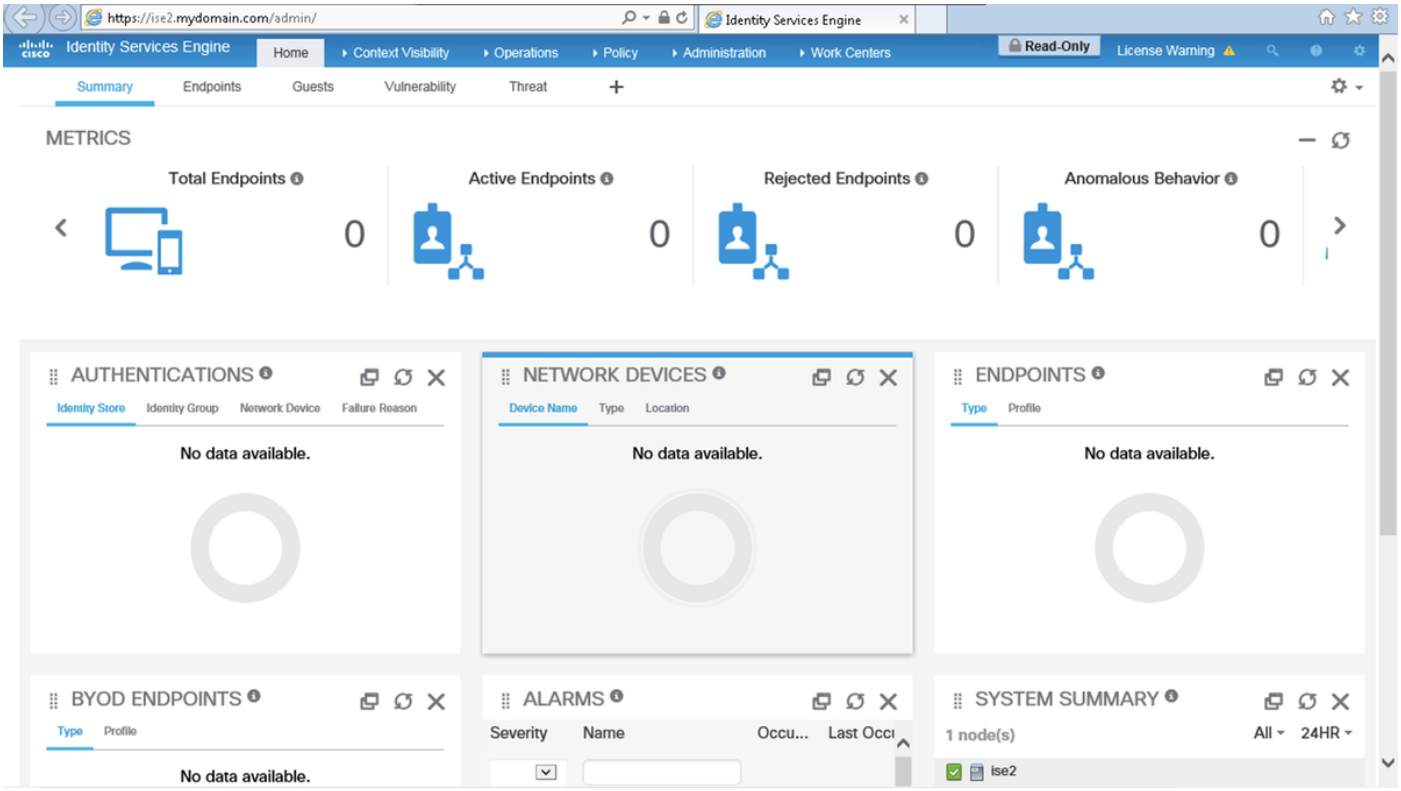




Utilisateur admin en lecture seule : vérifiez que l'utilisateur est invité à choisir un certificat pour se connecter à l'interface utilisateur graphique ISE et qu'il dispose de privilèges d'administrateur en lecture seule si le certificat fait partie d'un utilisateur du groupe d'identités externes admin en lecture seule.







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

Dépannage

1. Utilisez la commande application start ise safe pour démarrer Cisco ISE dans un mode sécurisé qui permet de désactiver temporairement le contrôle d'accès au portail Admin et de corriger la configuration et de redémarrer les services d'ISE avec la commande application stop ise suivie de application start ise.
2. L'option sécurisée permet de récupérer les données si un administrateur bloque par inadvertance l'accès au portail d'administration de 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 contourne également l'authentification basée sur certificat et revient à l'authentification par nom d'utilisateur et mot de passe par défaut pour la connexion au portail d'administration Cisco ISE.

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.