Configure Certificate or Smartcard Based authentication for ISE Administration

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Configure](#)
[Network Diagram](#)
[Join ISE to Active Directory](#)
[Select Directory Groups](#)
[Enable Active Directory Password-Based Authentication for Administrative Access](#)
[Map External Identity Groups to Admin Groups](#)
[Import Trusted Certificate](#)
[Configure Certificate Authentication Profile](#)
[Enable Client Certificate-based Authentication](#)
[Verify](#)
[Troubleshoot](#)

Introduction

This document describes how to configure Client Certificate-based authentication for Identity Services Engine (ISE) management access. In this example, the ISE administrator authenticates against the User certificate to gain Admin access to the Cisco Identity Services Engine (ISE) management GUI.

Prerequisites

Requirements

Cisco recommends to have knowledge of these topics:

- ISE configuration for password and certificate authentication.
- Microsoft Active Directory (AD)

Components Used

The information in this document is based on these software and hardware versions:

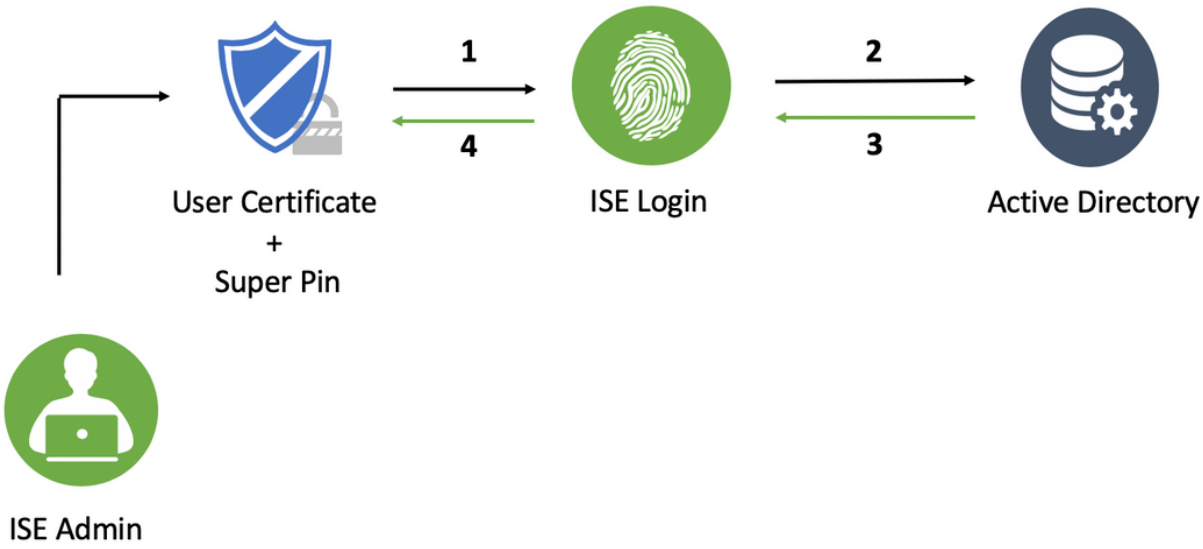
- Cisco Identity Services Engine (ISE) Version 2.6
- Windows Active Directory (AD) Server 2008 Release 2
- Certificate

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. If the network is live, make sure to understand the potential impact of any configuration.

Configure

Use this section to configure the Client certificate or Smart Card as an external identity for administrative access to the Cisco ISE management GUI.

Network Diagram

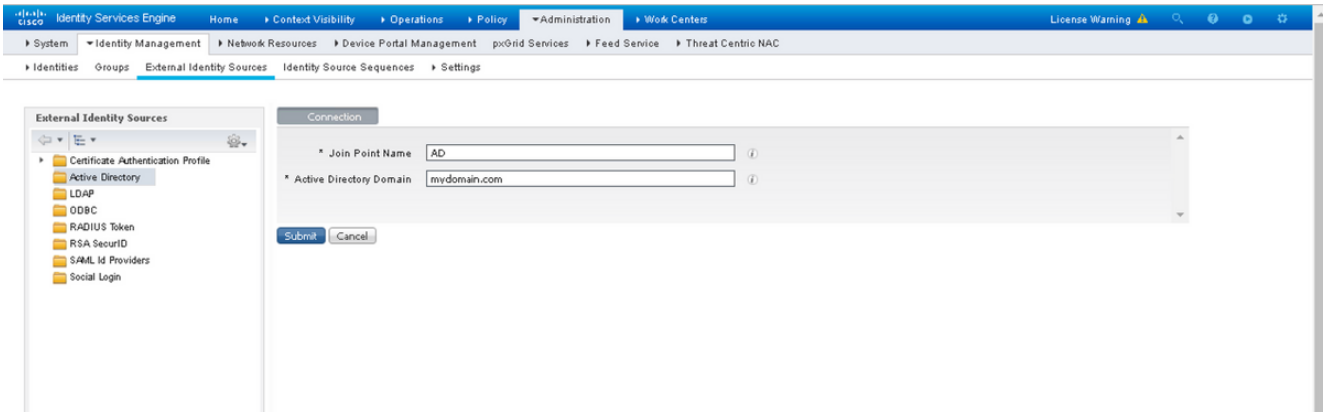


Join ISE to Active Directory

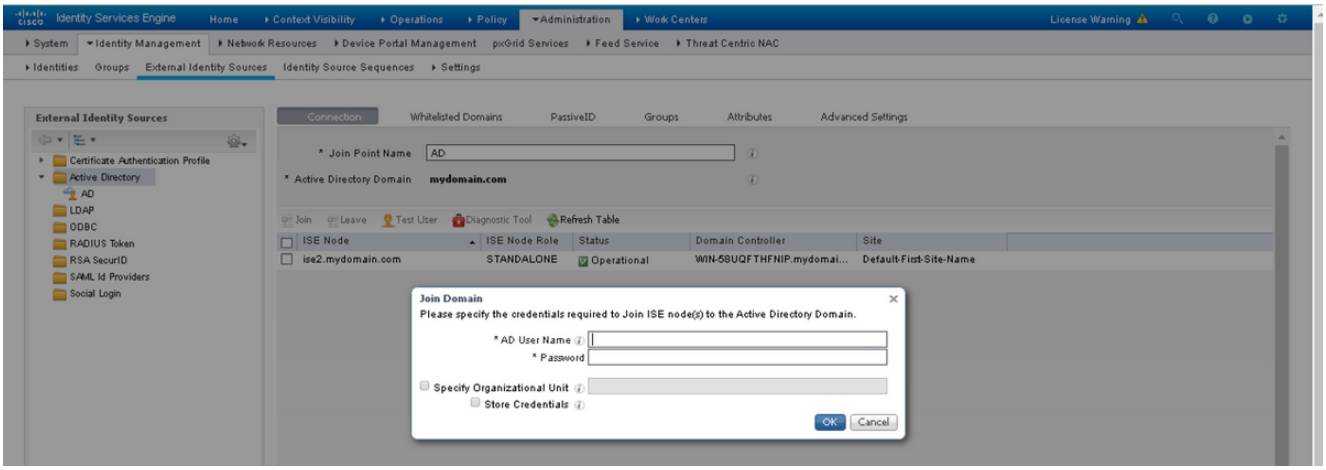
1. Choose **Administration** > **Identity Management > External Identity Sources > Active Directory.**

2. Create an Active Directory instance with **Join Point name** and **AD domain** in Cisco ISE.

3. Click **Submit**.



4. Join all the nodes with the appropriate **Username** and **Password** in the prompt.



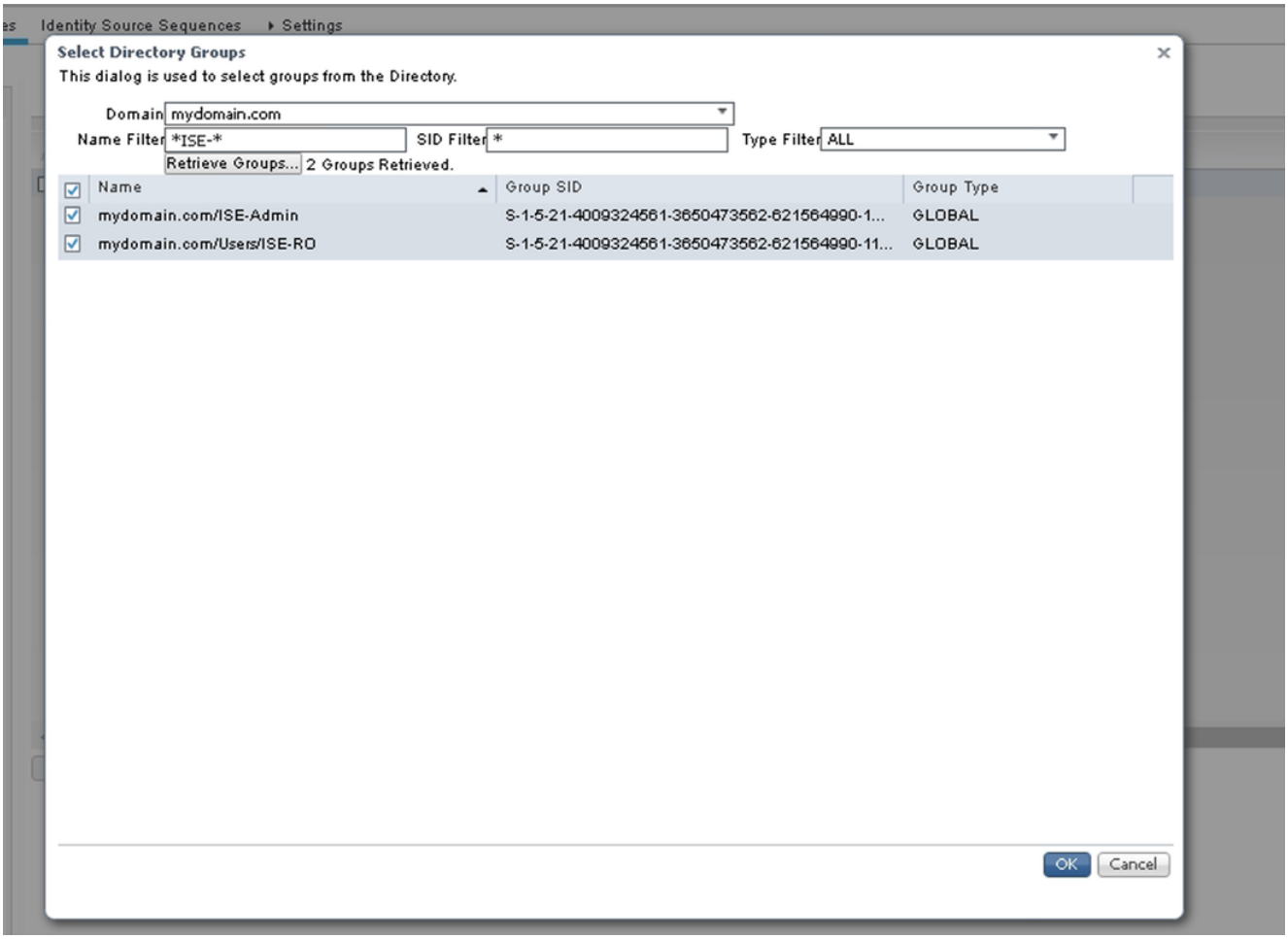
5. Click **Save**.

Select Directory Groups

1. Create an external Administrator group and map it to the active directory group.

2. Choose **Administration >Identity Management > External Identity Sources > Active Directory > Groups > Select Groups from Directory.**

3. Retrieve at least one AD Group to which the administrator belongs.

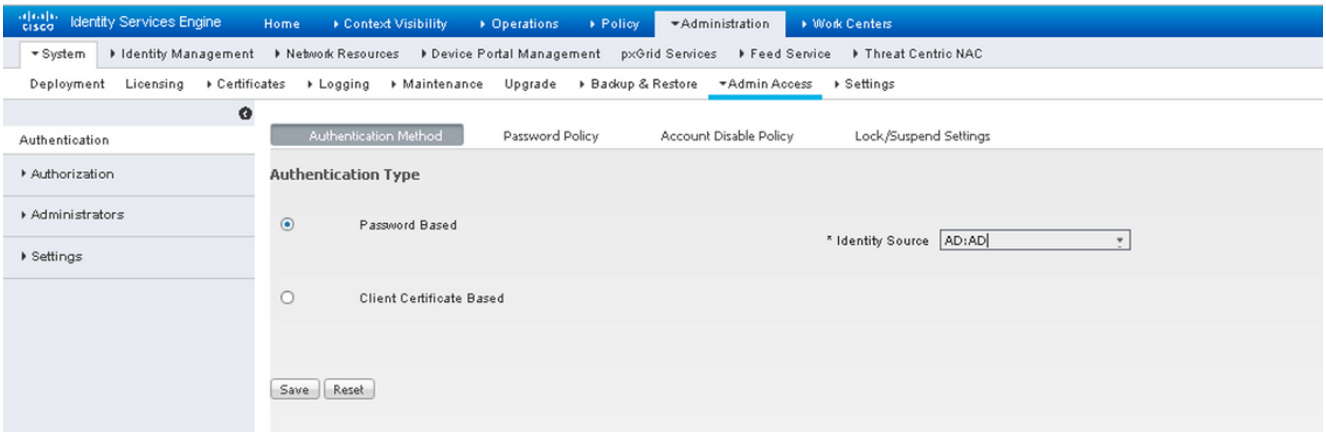


4. Click **Save**.

Enable Active Directory Password-Based Authentication for Administrative Access

1. Enable active directory instance as Password-based authentication method which has joined ISE earlier.

2. Choose **Administration** > **System > Admin access > Authentication**, as shown in the image.



3. Click **Save**.

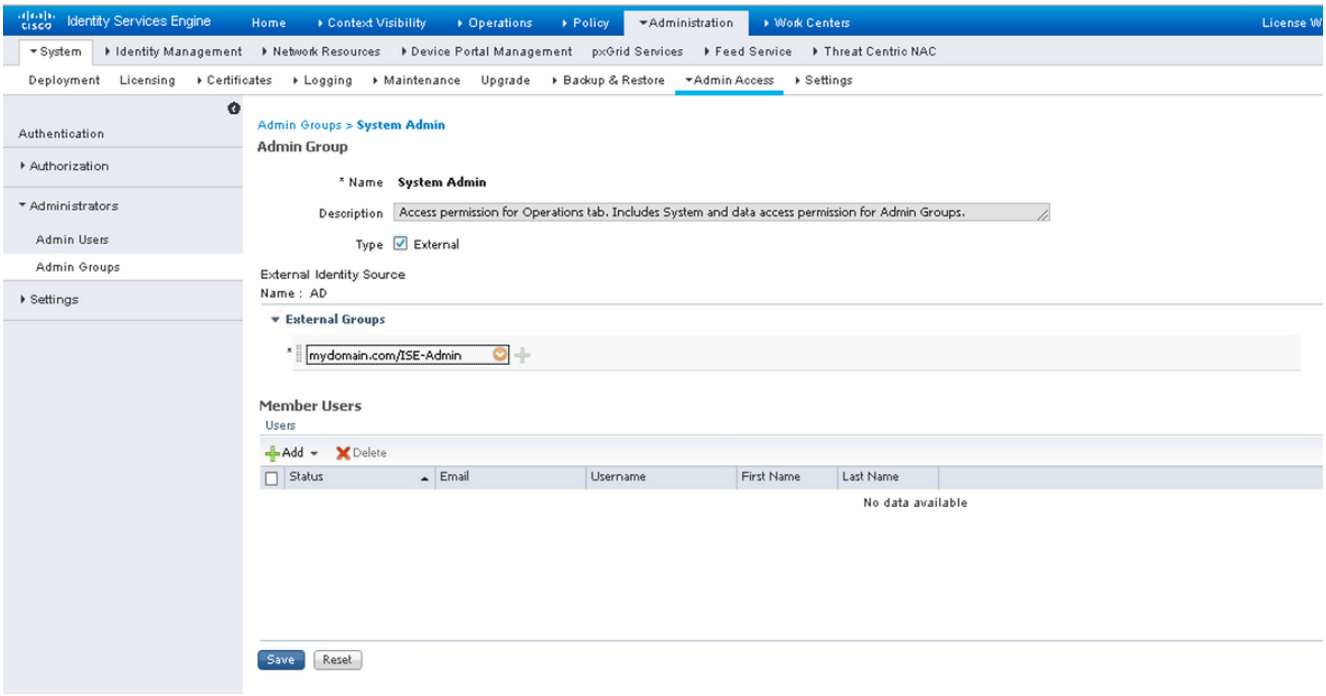
Note: Password-Based authentication configuration is required to enable Certificate-Based authentication. This configuration should be reverted after a successful configuration of Certificate-Based authentication.

Map External Identity Groups to Admin Groups

In this example, the external AD group is mapped to the default Admin group.

1. Choose **Administration >System >Admin Access >Administrators >Admin Groups > Super admin.**

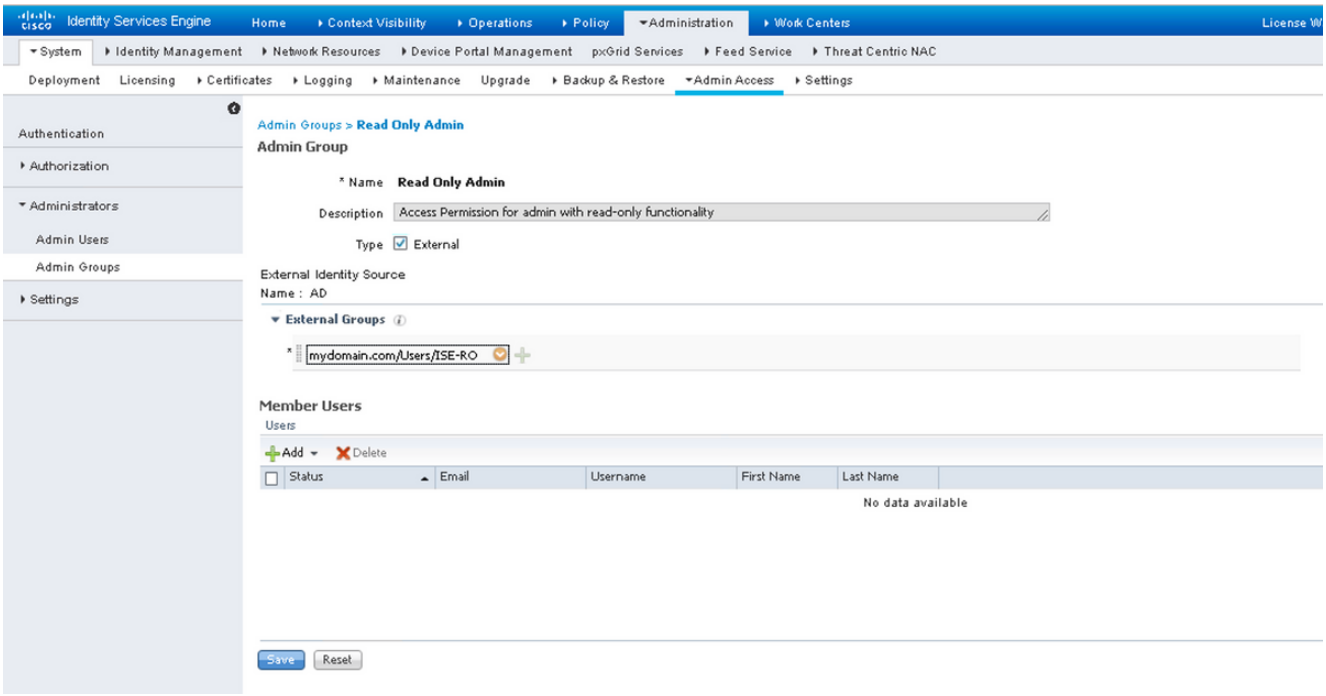
2. Check the Type as **External** and select the AD group under **External groups**.



3. Click **Save**.

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

5. Check the Type as **External** and select the AD group under **External groups**, as shown in the image.



6. Click **Save**.

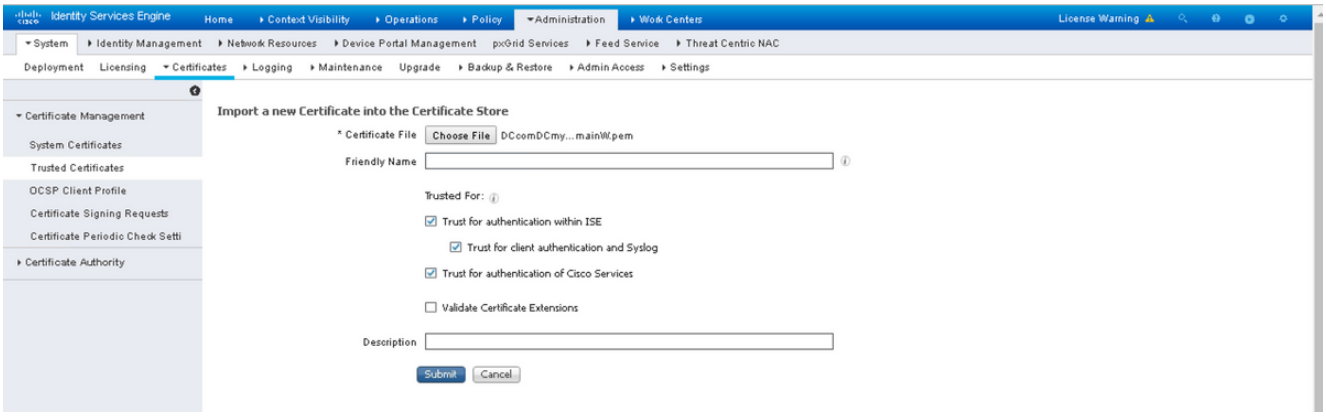
Import Trusted Certificate

1. Import the Certificate authority(CA) certificate that signs the client certificate.

2. Choose **Administrator > System > Certificates > Trusted Certificate > Import.**

3. Click browse and choose the CA certificate.

4. Check the **Trust for client authentication and Syslog checkbox**, as shown in the image.



5. Click **Submit.**

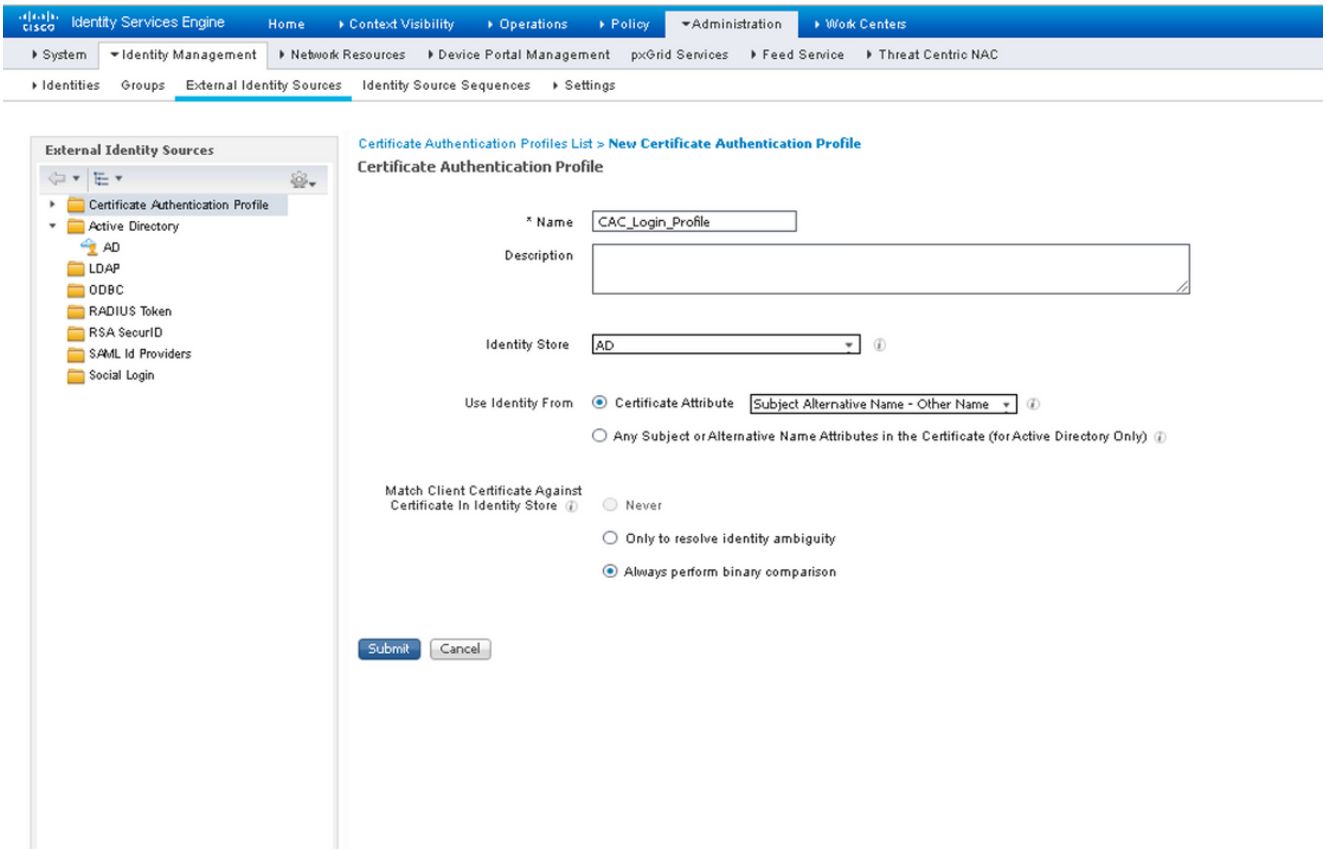
Configure Certificate Authentication Profile

1. In order to create Certificate Authentication Profile for Client certificate-based authentication, Choose **Administration >Identity Management > External Identity Sources > Certificate Authentication Profile > Add.**

2. Add profile name.

3. Select the appropriate attribute that contains the administrator username in the certificate attribute.

4. If the AD record for the user contains the user's certificate, and want to compare the certificate that is received from the browser against the certificate in AD, check **Always perform binary comparison** checkbox, and select the Active Directory instance name that was specified earlier.

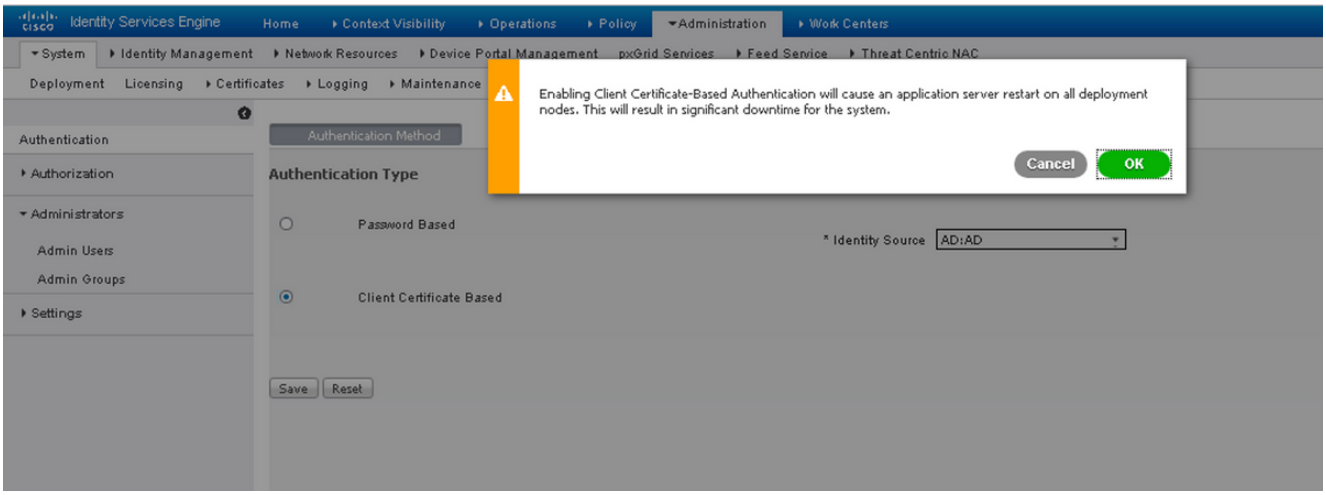


5. Click **Submit.**

Note: The same Certificate authentication profile can be consumed for endpoint Identity-based authentication also.

Enable Client Certificate-based Authentication

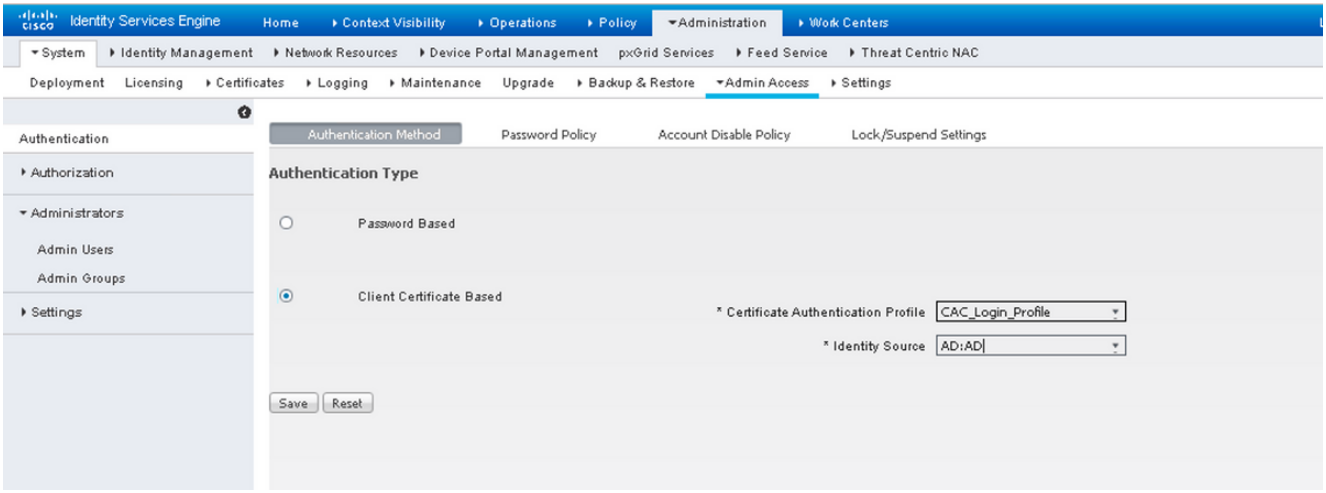
1. Choose **Administration > System > Admin Access > Authentication > Authentication Method Client Certificate Based.**



2. Click **OK**.

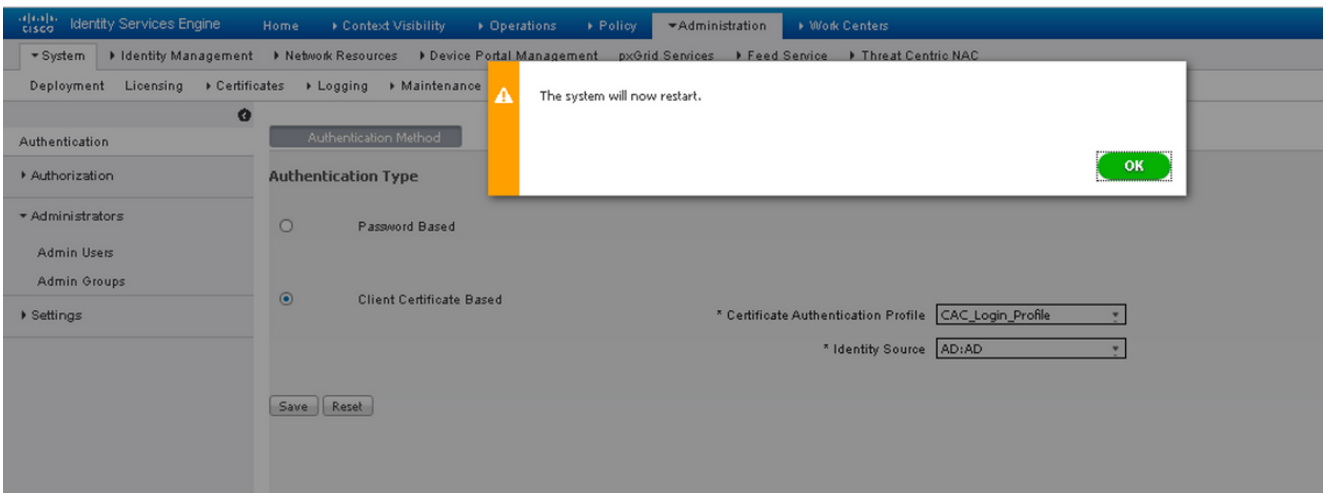
3. Choose the **Certificate Authentication Profile** that is configured earlier.

4. Select the Active Directory instance name.



5. Click **Save**.

6. ISE services on all the nodes in the deployment restarts.

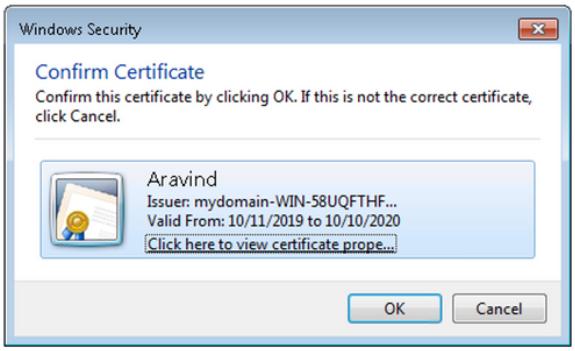


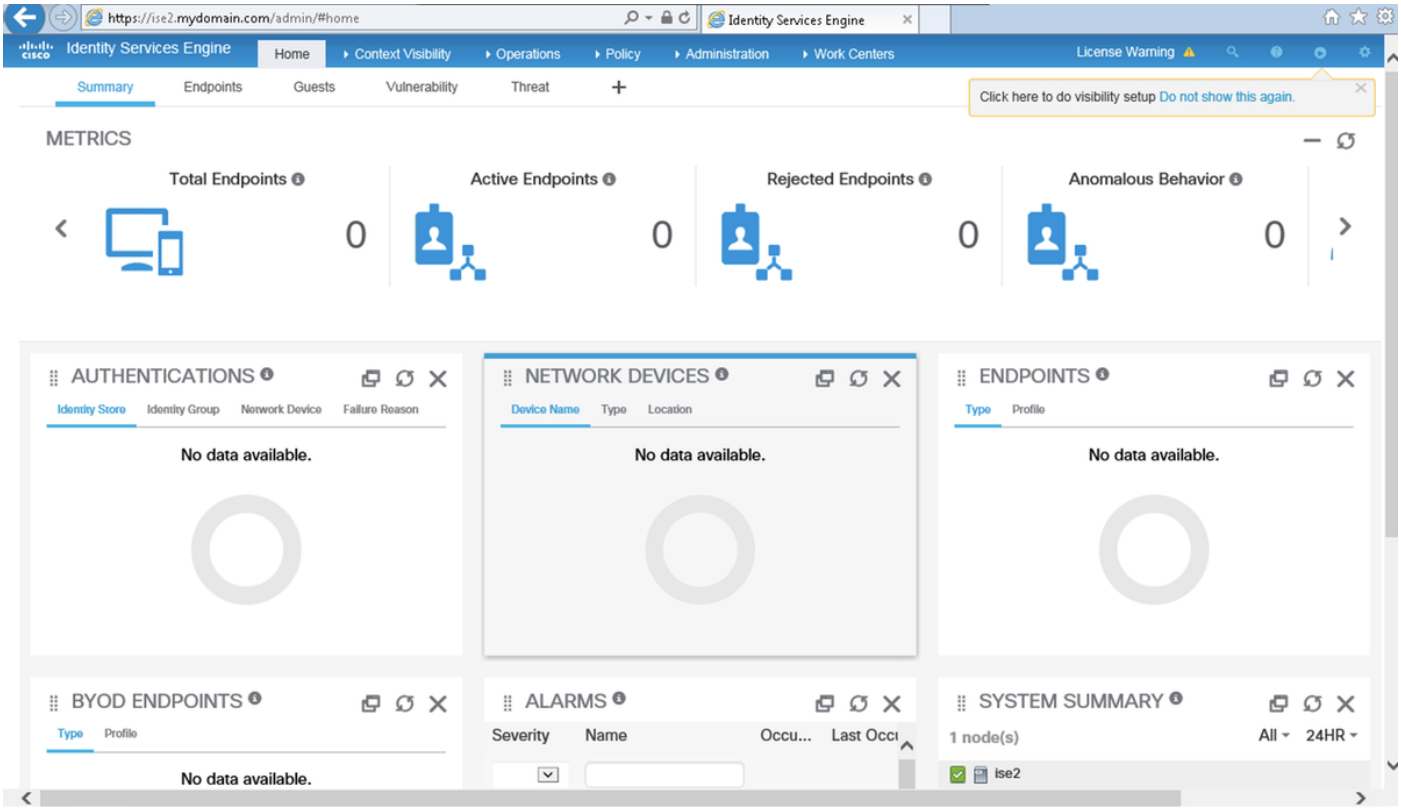
Verify

Verify access to the ISE GUI after the **Application Server** service status changes to **running.**

Super Admin User: Verify that the user is prompted to choose a certificate to login to the ISE GUI and is given Super Admin privileges if the certificate is of a user part of the Super Admin External Identity group.



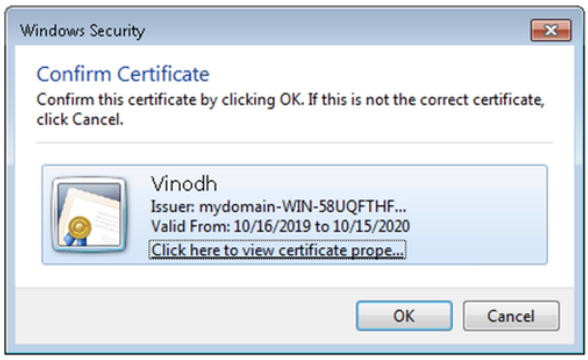


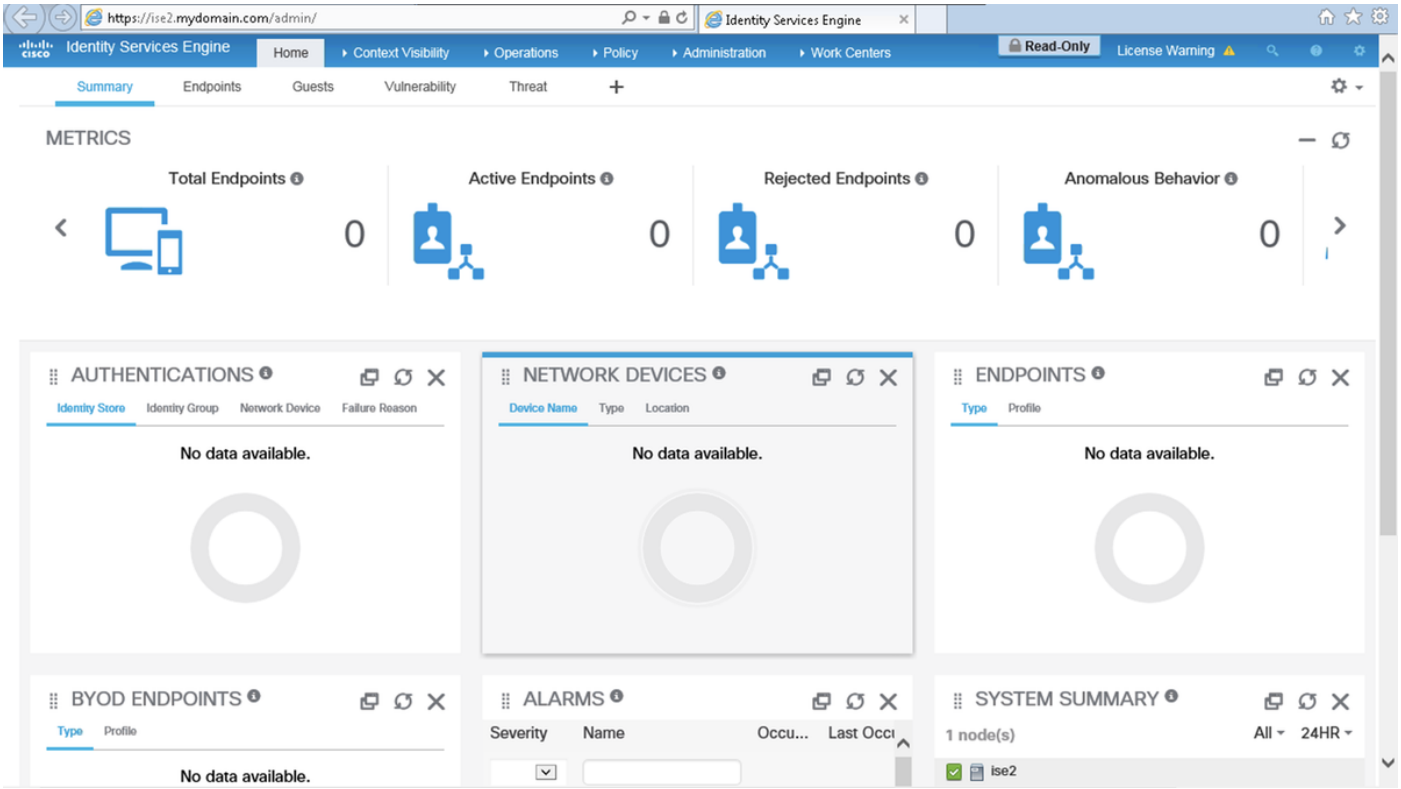


Read-only Admin User: Verify that the user is prompted to choose a certificate to login to the ISE GUI and is given Read-only Admin privileges if the certificate is of a user part of Read-only Admin

External Identity group.







Note: If Common Access Card (CAC) is in use, Smartcard presents the user certificate to ISE after the user enters their valid super pin.

Troubleshoot

1. Use the **application start ise safe** command to start Cisco ISE in a safe mode that allows to disable access control temporarily to the Admin portal and Correct the configuration and

restart the services of ISE with the command **application stop ise** followed by **application start ise*.***

2. The safe option provides a means of recovery if an administrator inadvertently locks out access to the Cisco ISE Admin portal for all users. This event can happen if the administrator configured an incorrect **IP Access** list in the **Administration > Admin Access > Settings > Access page**. The **safe** option also **bypasses certificate-based authentication** and reverts to the default username and password authentication for logging into the Cisco ISE Admin portal.