Configurar autenticação baseada em certificado ou cartão inteligente para administração do ISE

Contents

Introduction

Este documento descreve como configurar a autenticação baseada em certificado do cliente para o acesso de gerenciamento do Identity Services Engine (ISE). Neste exemplo, o administrador do ISE se autentica em relação ao certificado do usuário para obter acesso de administrador à GUI de gerenciamento do Cisco Identity Services Engine (ISE).

Prerequisites

Requirements

A Cisco recomenda ter conhecimento destes tópicos:

- Configuração do ISE para autenticação de senha e certificado.
- Microsoft Ative Diretory (AD)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

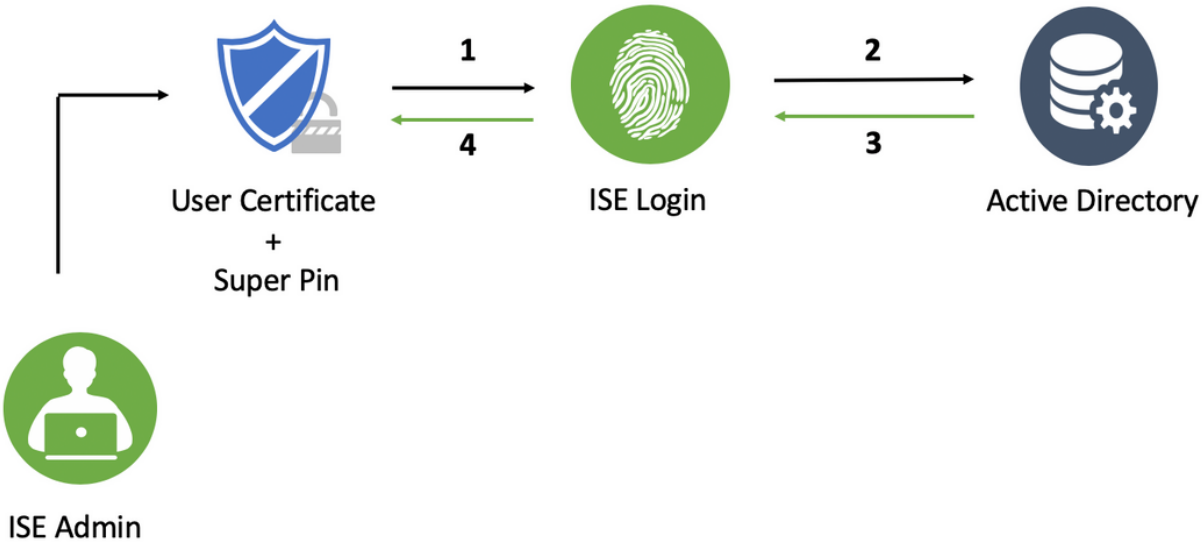
- Cisco Identity Services Engine (ISE) versão 2.6
- Windows Ative Diretory (AD) Server 2008 versão 2
- Certificado

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. Se a rede estiver ativa, certifique-se de entender o impacto potencial de qualquer configuração.

Configurar

Use esta seção para configurar o certificado do cliente ou o Smart Card como uma identidade externa para acesso administrativo à GUI de gerenciamento do Cisco ISE.

Diagrama de Rede

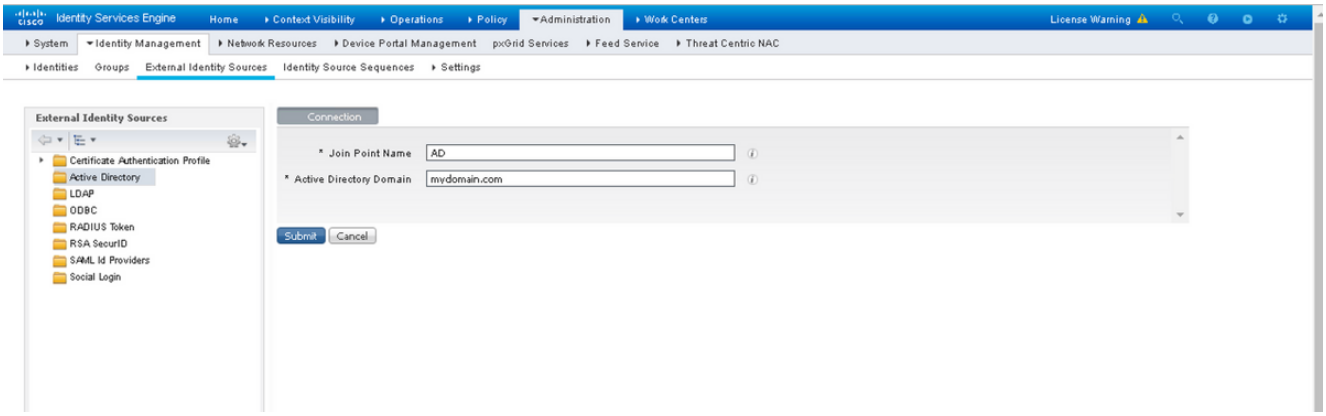


Ingressar no ISE no Ative Diretory

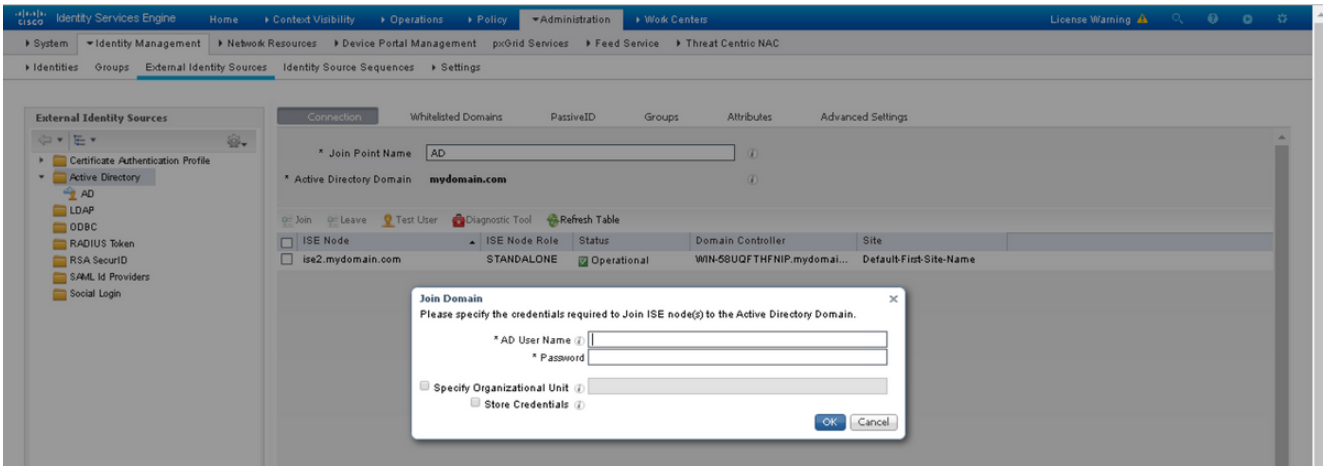
1. Escolha **Administração > Identity Management > External Identity Sources > Ative Diretory.**

2. Crie uma instância do Ative Diretory com o **nome do ponto de junção** e o **domínio do AD** no Cisco ISE.

3. Clique em Submit.



4. Junte-se a todos os nós com o **Nome de usuário** e **Senha** apropriados no prompt.



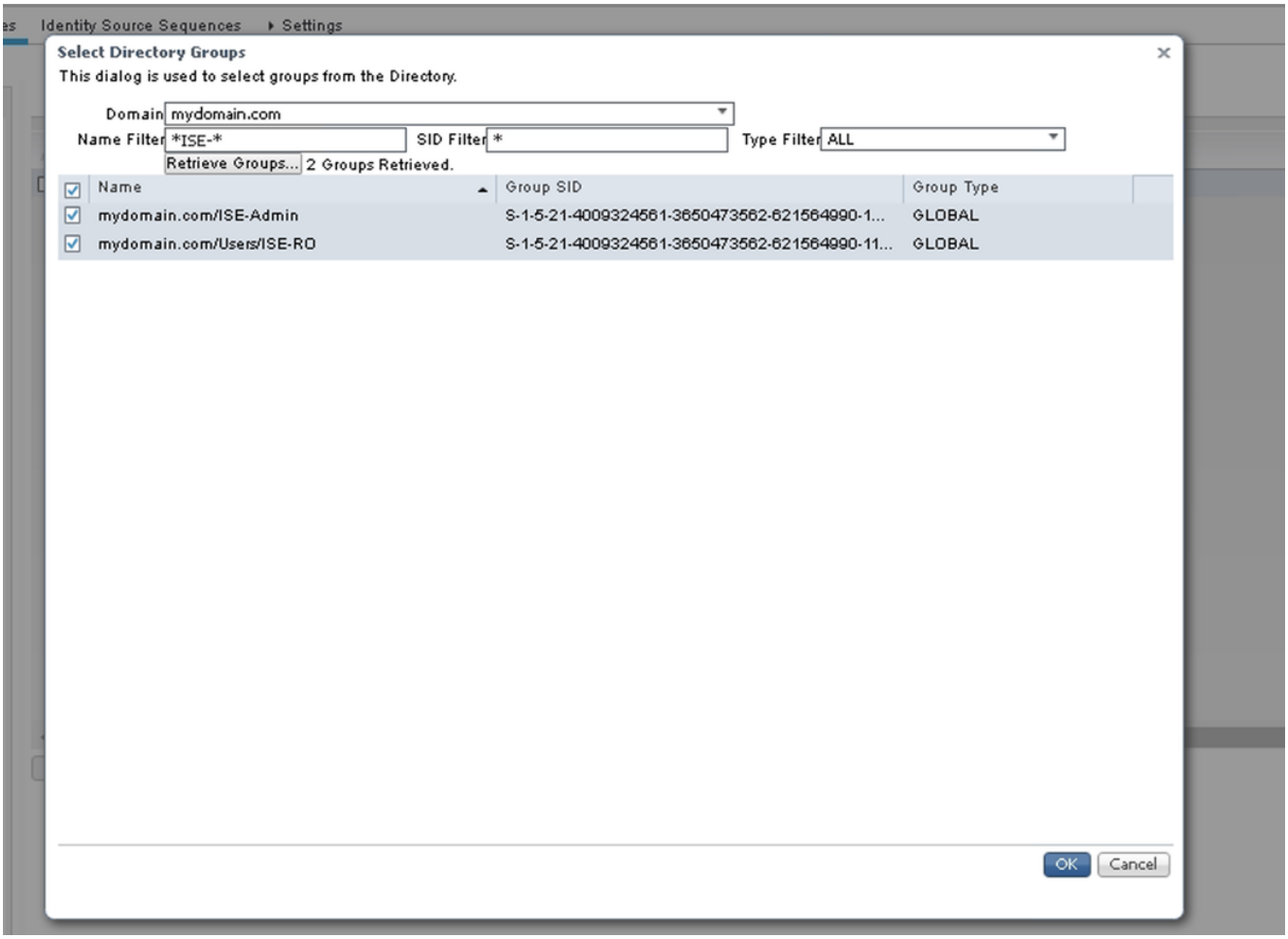
5. Click **Save**.

Selecionar grupos de diretórios

1. Crie um grupo de administradores externo e mapeie-o para o grupo de diretórios ativo.

2. Escolha **Administração >Identity Management > External Identity Sources > Ative Diretory > Groups > Select Groups from Diretory.**

3. Recupere pelo menos um grupo AD ao qual o administrador pertence.

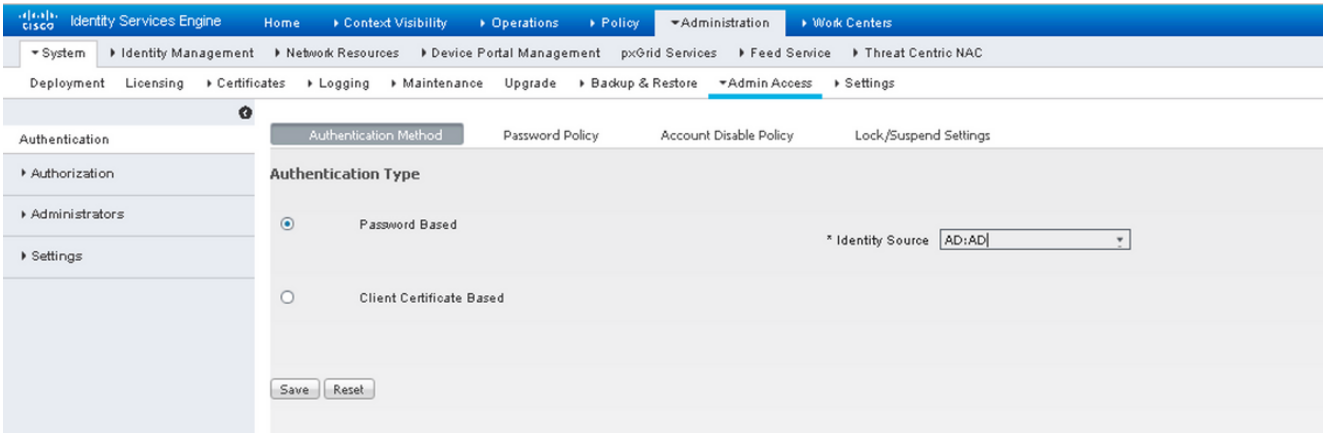


4. Click **Save**.

Ativar autenticação baseada em senha do Ative Diretory para acesso administrativo

1. Ative a instância do ative diretory como método de autenticação baseado em senha que ingressou no ISE anteriormente.

2. Escolha **Administration > System > Admin access > Authentication**, como mostrado na imagem.



3. Click **Save**.

Note: A configuração de autenticação baseada em senha é necessária para ativar a

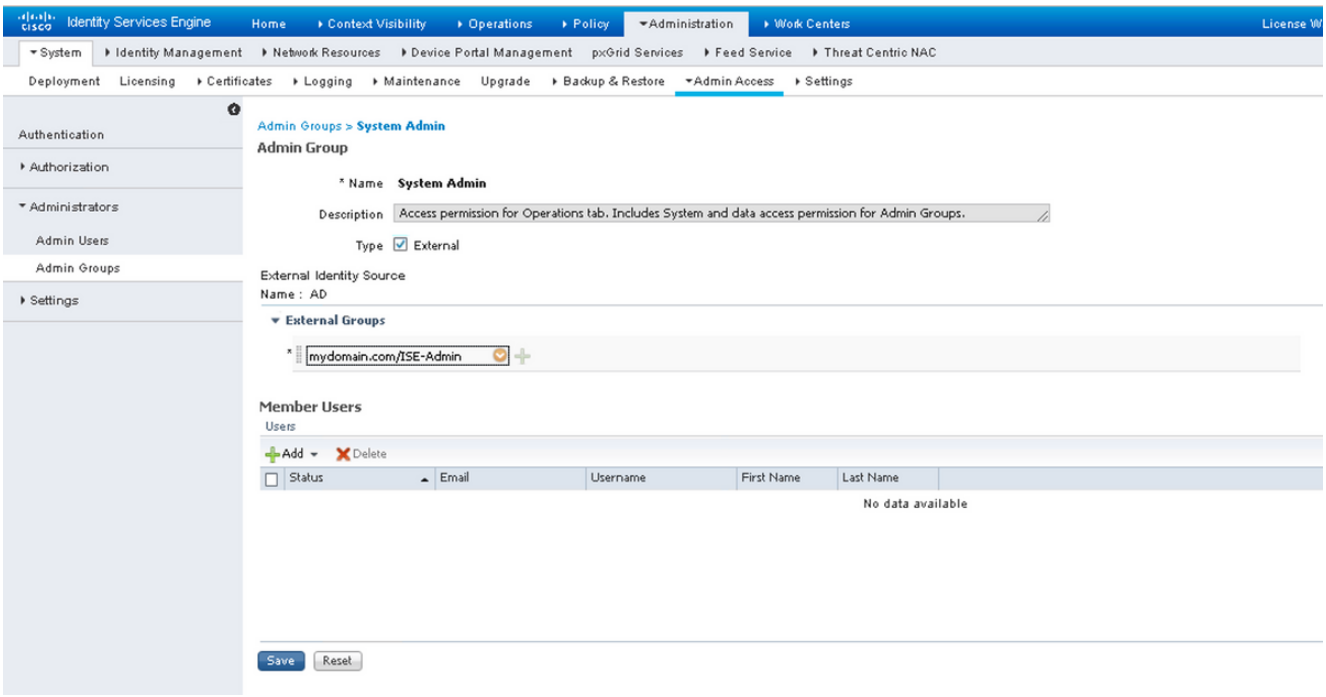
autenticação baseada em certificado. Essa configuração deve ser revertida após uma configuração bem-sucedida da autenticação baseada em certificado.

Mapear grupos de identidade externos para grupos de administradores

Neste exemplo, o grupo de AD externo é mapeado para o grupo de Admin padrão.

1. Escolha **Administração >Sistema >Acesso de Administrador > Administradores >Grupos Admin > Super administrador.**

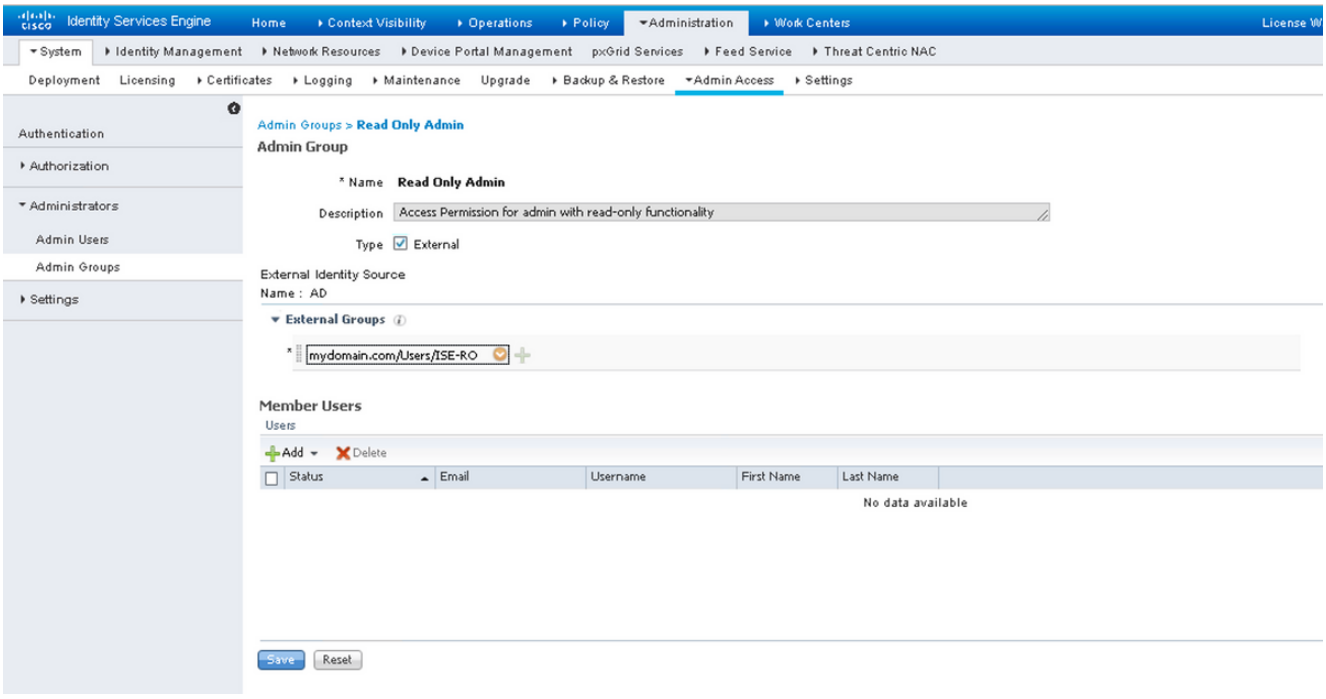
2. Marque Tipo como **Externo** e selecione o grupo AD em **Grupos externos**.



3. Click **Save**.

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

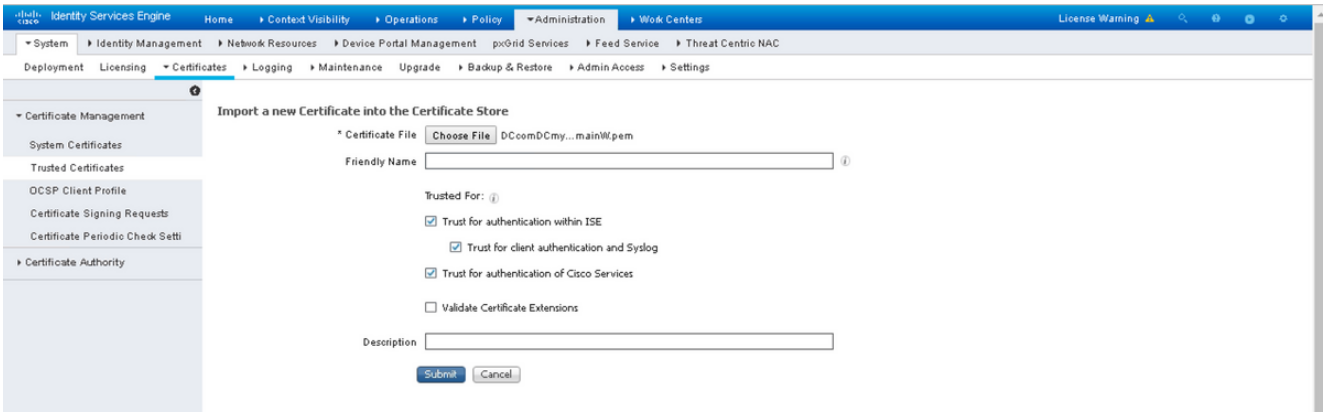
5. Marque Tipo como **Externo** e selecione o grupo AD em **Grupos externos**, como mostrado na imagem.



6. Click **Save**.

Importar certificado confiável

1. Importar o certificado da autoridade de certificação (AC) que assina o certificado do cliente.
2. Escolher **Administrador > Sistema > Certificados > Certificado Confiável > Importar.**
3. Clique em Procurar e escolha o certificado CA.
4. Marque a **caixa de seleção Confiar na autenticação do cliente e Syslog**, como mostrado na imagem.



5. Clique em Submit.

Configurar perfil de autenticação de certificado

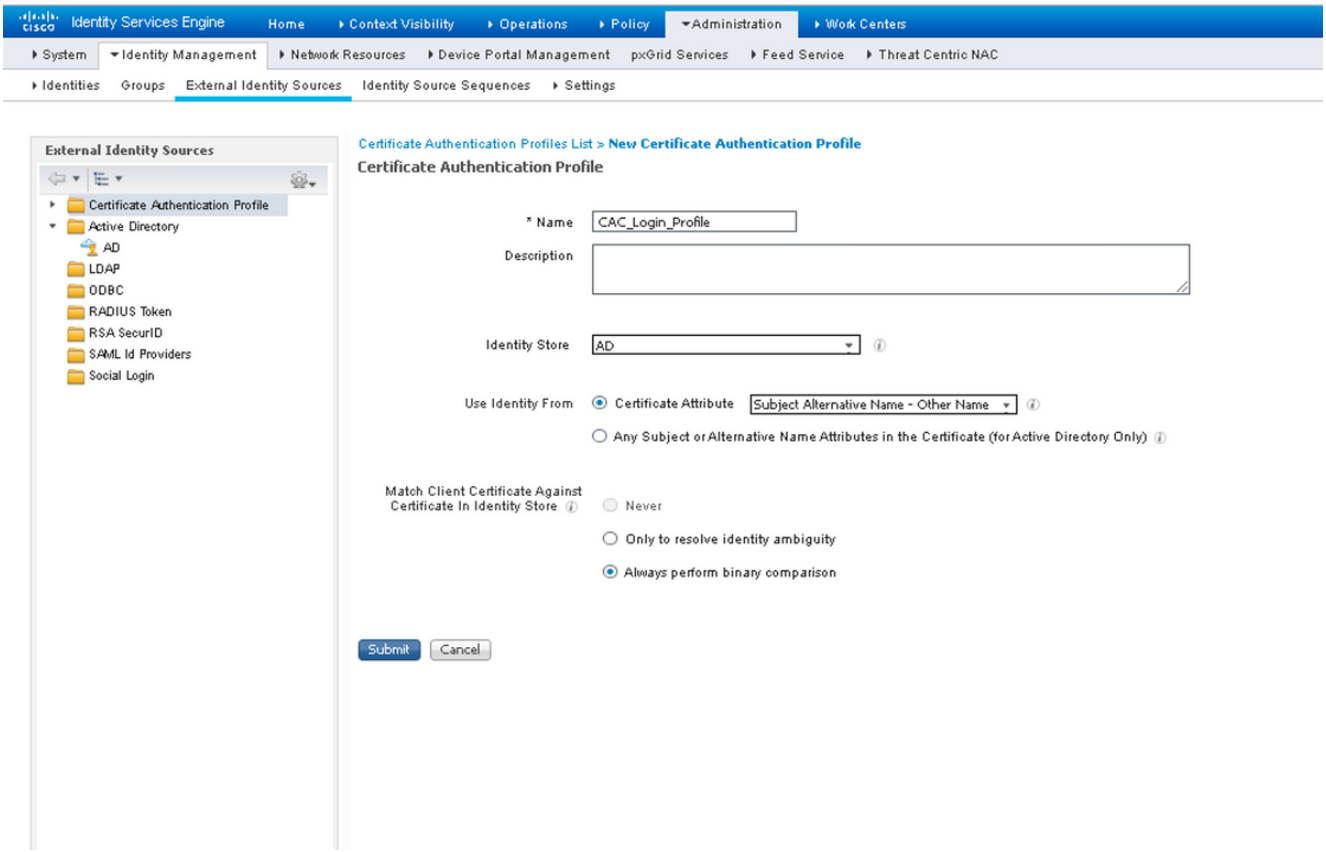
1. Para criar o perfil de autenticação de certificado para autenticação baseada em certificado do cliente, escolha **Administração >Identity Management > External Identity Source >**

Certificate Authentication Profile > Add.

2. Adicionar nome de perfil.

3. Selecione o atributo apropriado que contém o nome de usuário do administrador no atributo de certificado.

4. Se o registro do AD do usuário contiver o certificado do usuário e quiser comparar o certificado recebido do navegador com o certificado no AD, marque a caixa de seleção **Sempre executar comparação binária** e selecione o nome da instância do Ative Diretory que foi especificado anteriormente.

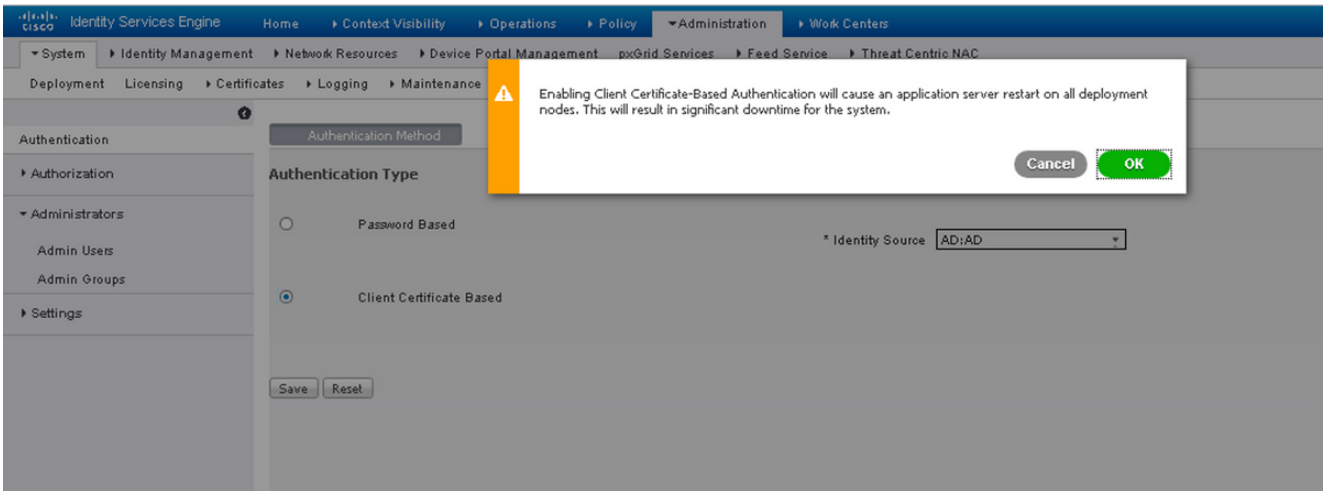


5. Clique em Submit.

Note: O mesmo perfil de autenticação de certificado também pode ser consumido para autenticação baseada em identidade de ponto final.

Ativar autenticação baseada em certificado do cliente

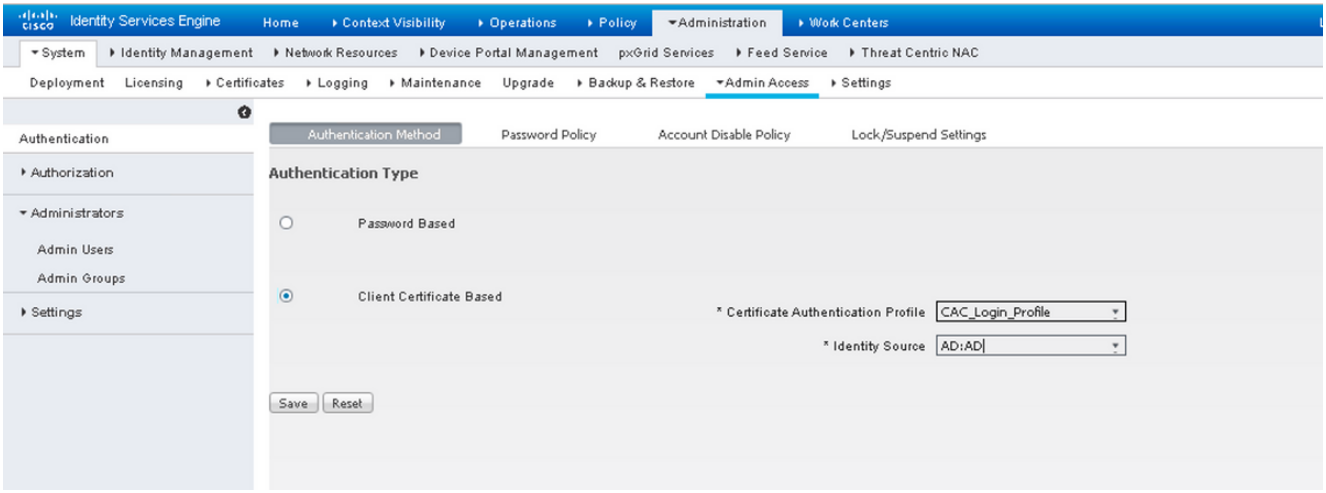
1. Escolher **Administração > Sistema > Acesso Admin > Autenticação > Método de Autenticação Baseado no Certificado do Cliente.**



2. Click **OK**.

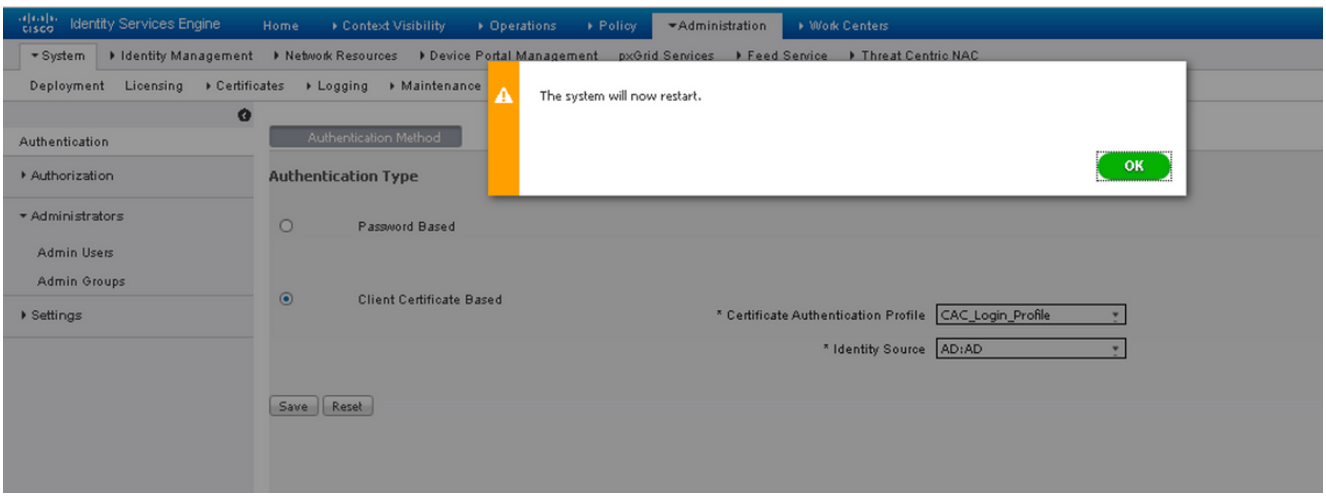
3. Escolha o **perfil de autenticação do certificado** configurado anteriormente.

4. Selecione o nome da instância do Ative Diretory.



5. Click **Save**.

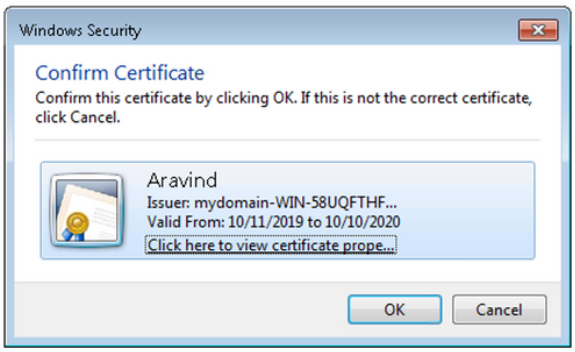
6. Os serviços ISE em todos os nós na implantação são reiniciados.

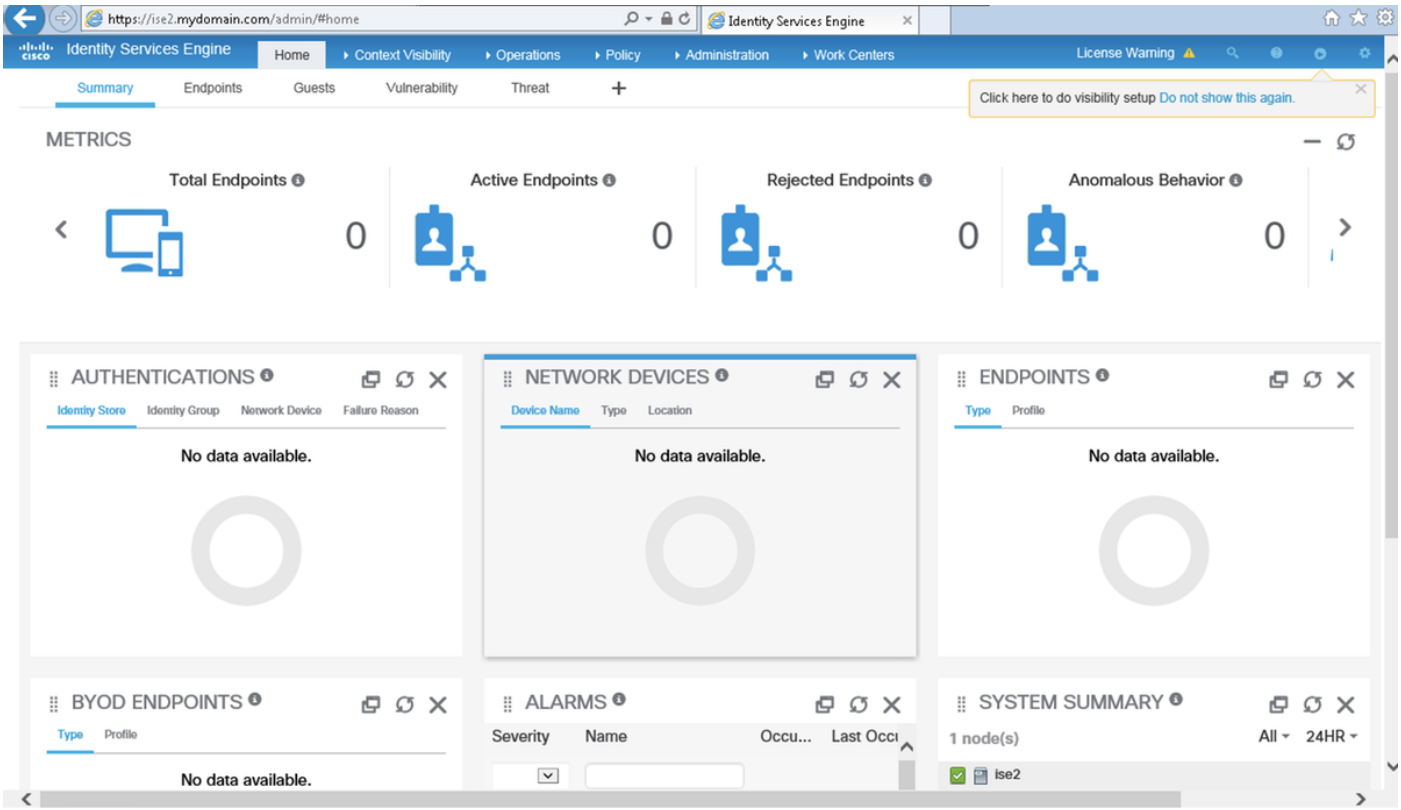


Verificar

Verifique o acesso à GUI do ISE depois que o status do serviço **do Servidor de Aplicativos** for alterado para **em execução.**

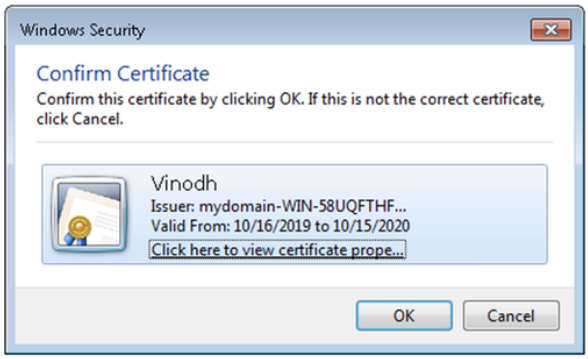
Usuário Super Admin: verifique se o usuário é solicitado a escolher um certificado para fazer login na GUI do ISE e se recebe privilégios Super Admin se o certificado for de um usuário do grupo de Identidade Externa do Super Admin.

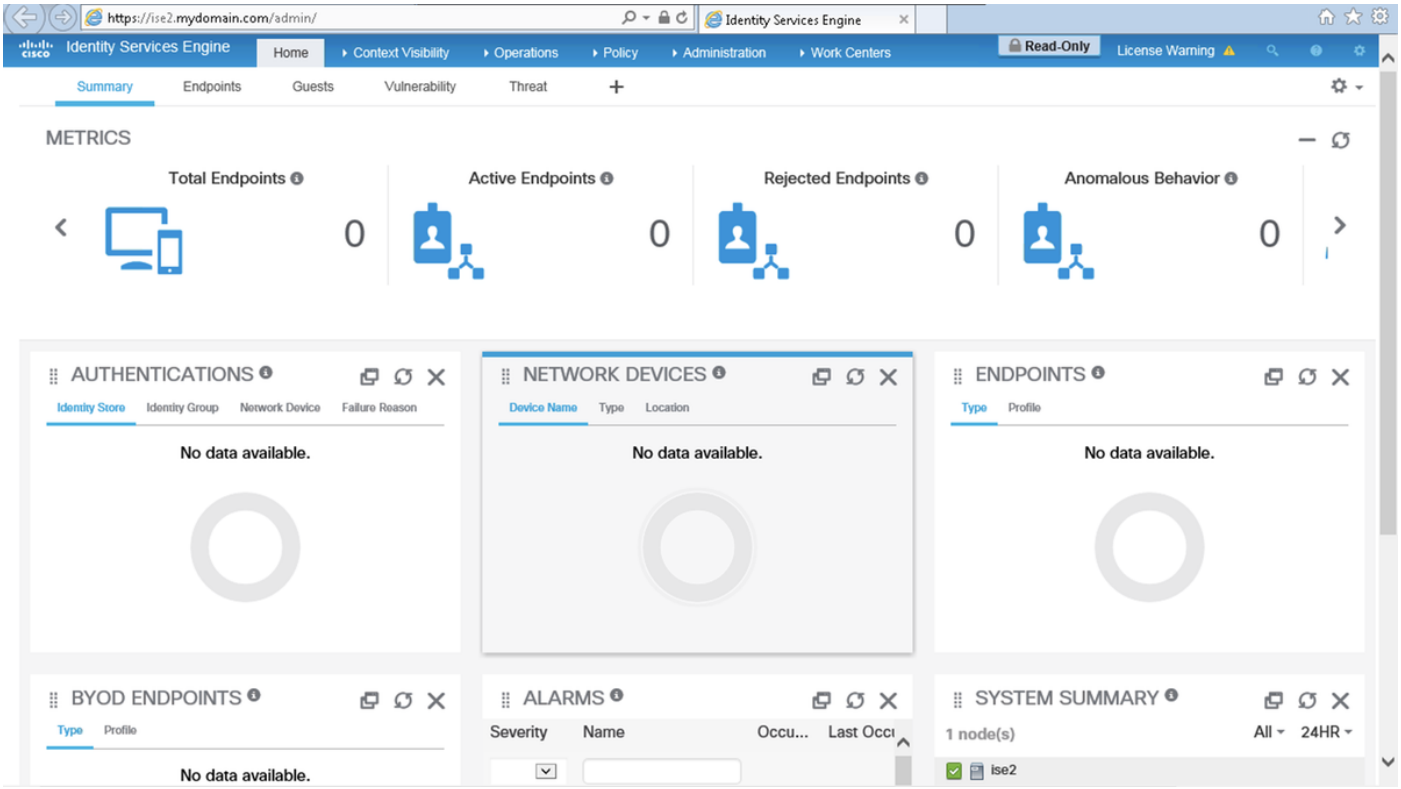




Usuário Admin Somente Leitura: Verifique se o usuário é solicitado a escolher um certificado para

fazer login na GUI do ISE e recebe privilégios Admin Somente Leitura se o certificado for de um usuário do grupo Identidade Externa Admin Somente Leitura.





Note: Se o Cartão de Acesso Comum (CAC) estiver em uso, o Smartcard apresenta o certificado do usuário ao ISE depois que o usuário digitar seu super pino válido.

Troubleshoot

1. Use o comando **application start ise safe** para iniciar o Cisco ISE em um modo seguro que

permite desativar temporariamente o controle de acesso ao portal Admin e Corrija a configuração e reinicie os serviços do ISE com o comando **application stop ise** seguido pelo **application start ise.**

2. A opção de segurança fornece um meio de recuperação se um administrador bloqueia inadvertidamente o acesso ao portal do administrador do Cisco ISE para todos os usuários. Este evento pode ocorrer se o administrador tiver configurado uma lista **de acesso IP** incorreta na **página Administração > Acesso de administrador > Configurações > Acesso**. A opção **safe** também **ignora a autenticação baseada em certificado** e reverte para a autenticação de nome de usuário e senha padrão para fazer login no portal Cisco ISE Admin.