为ISE管理配置基于证书或智能卡的身份验证

目录

简介

先决条件

- 要求
- 使用的组件

配置

- 网络图
- 将ISE加入Active Directory
- 选择目录组
- 为管理访问启用Active Directory基于密码的身份验证
- 将外部身份组映射到管理员组
- 导入受信任证书
- 配置证书身份验证配置文件
- 启用基于客户端证书的身份验证

验证

故障排除

简介

本文档介绍如何为身份服务引擎(ISE)管理访问配置基于客户端证书的身份验证。在本示例中，ISE管理员根据用户证书进行身份验证，以获得对思科身份服务引擎(ISE)管理GUI的管理员访问权限。

先决条件

要求

思科建议了解以下主题：

- ISE配置密码和证书身份验证。
- Microsoft Active Directory(AD)

使用的组件

本文档中的信息基于以下软件和硬件版本：

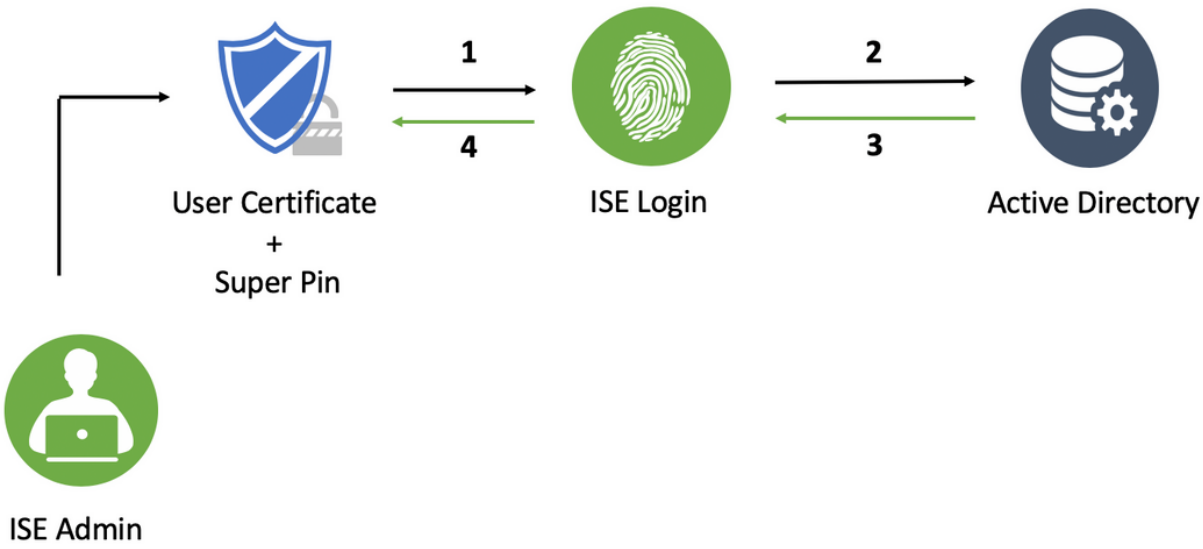
- 思科身份服务引擎(ISE)版本2.6
- Windows Active Directory(AD)Server 2008版本2
- 证书

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果网络处于活动状态，请确保了解任何配置的潜在影响。

配置

使用此部分将客户端证书或智能卡配置为外部身份以管理访问思科ISE管理GUI。

网络图

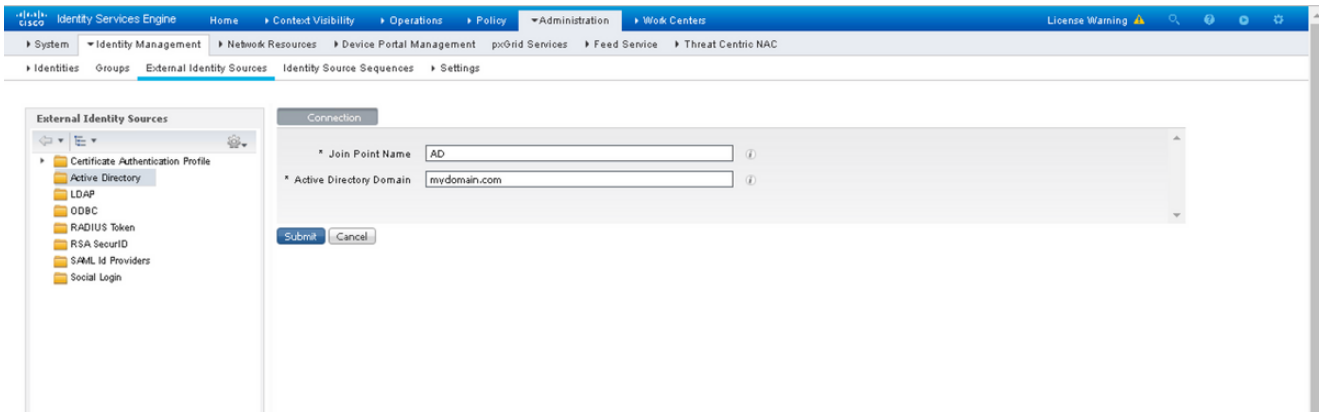


将ISE加入Active Directory

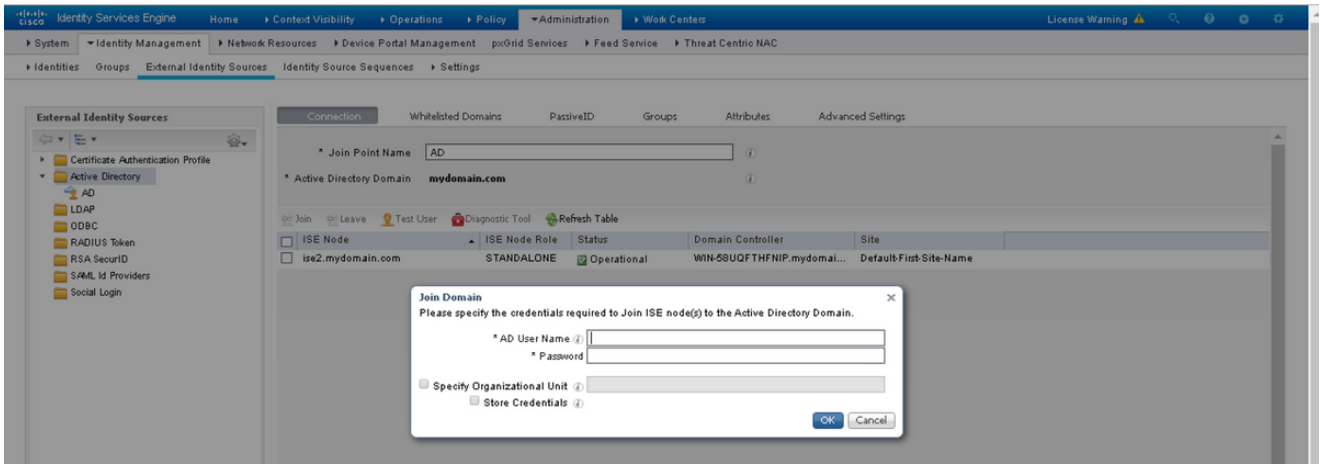
1. 选择Administration > 身份管理(Identity Management)>外部身份源(External Identity Sources)> Active Directory。

2. 在Cisco ISE中创建具有加入点名称和AD域的Active Directory实例。

3. 单击 submit。



4. 在提示符中使用适当的用户名和密码加入所有节点。



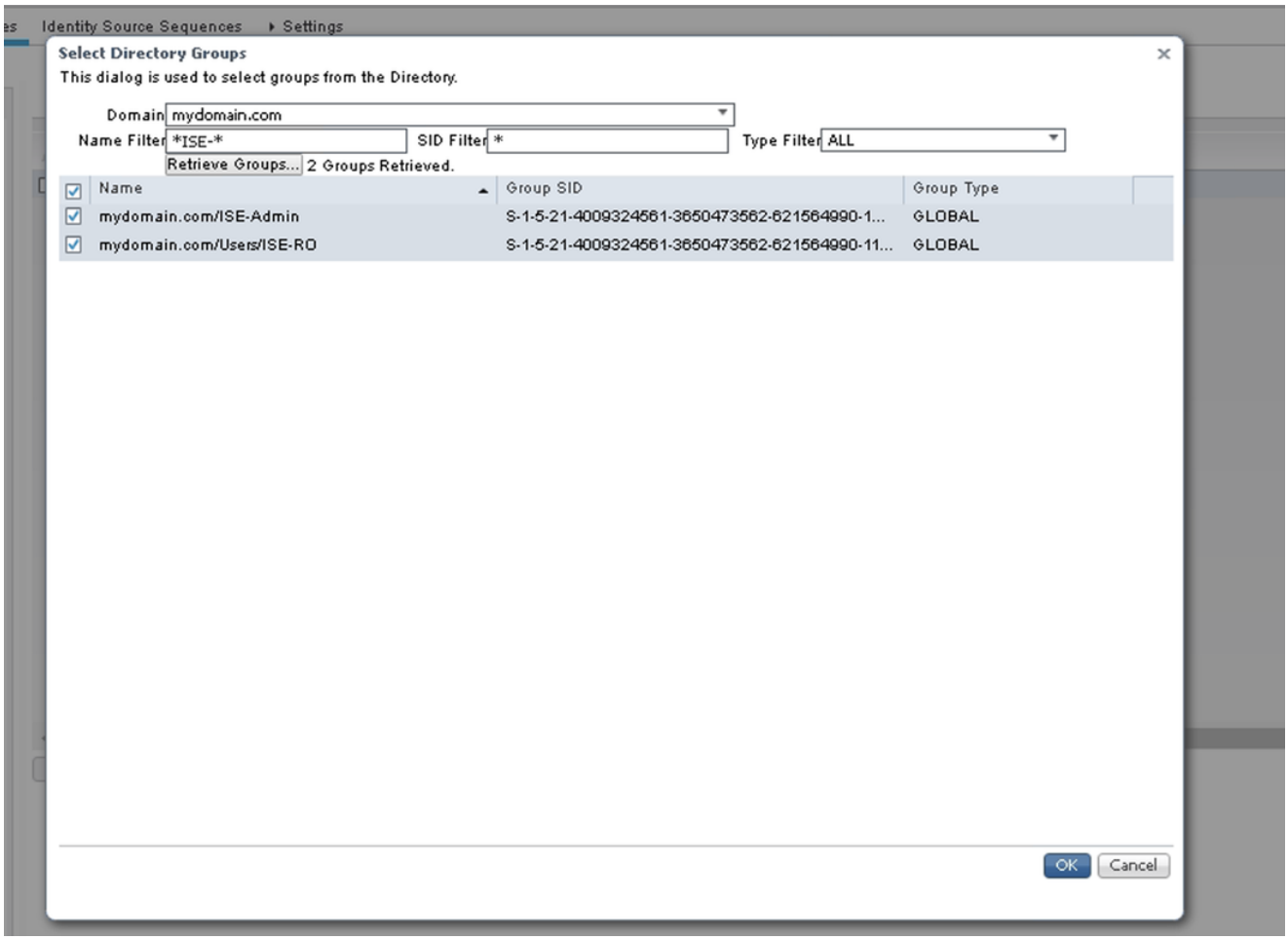
5. Click Save.

选择目录组

1. 创建外部管理员组并将其映射到Active Directory组。

2. 选择管理>身份管理(Identity Management)>外部身份源(External Identity Sources)> Active Directory > Groups > Select Groups from Directory。

3. 至少检索管理员所属的一个AD组。

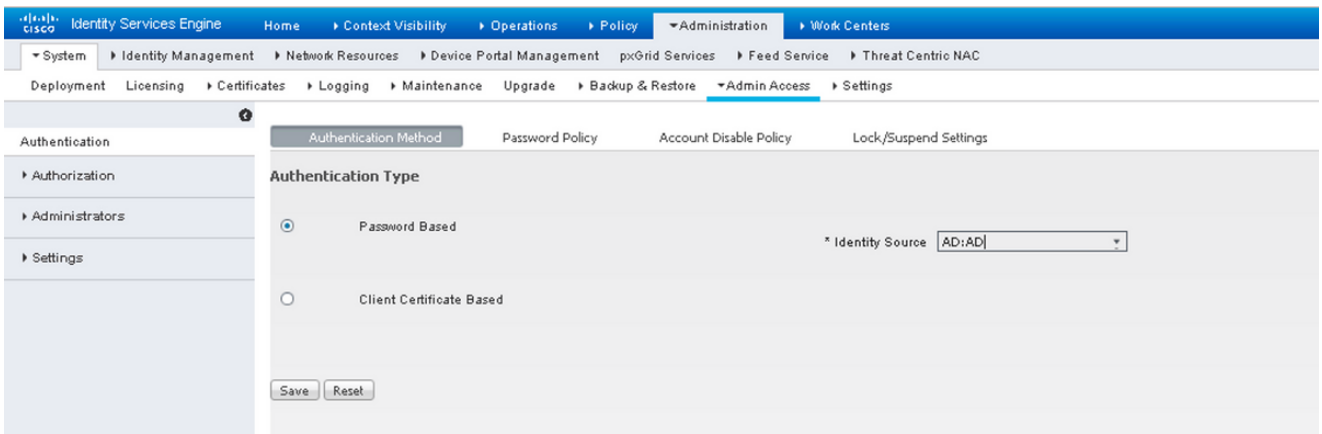


4. Click Save.

为管理访问启用Active Directory基于密码的身份验证

1. 启用Active Directory实例作为之前加入ISE的基于密码的身份验证方法。

2. 选择Administration > System > Admin access > Authentication，如图所示。



3. Click Save.

注意：需要基于密码的身份验证配置才能启用基于证书的身份验证。此配置应在基于证书的身

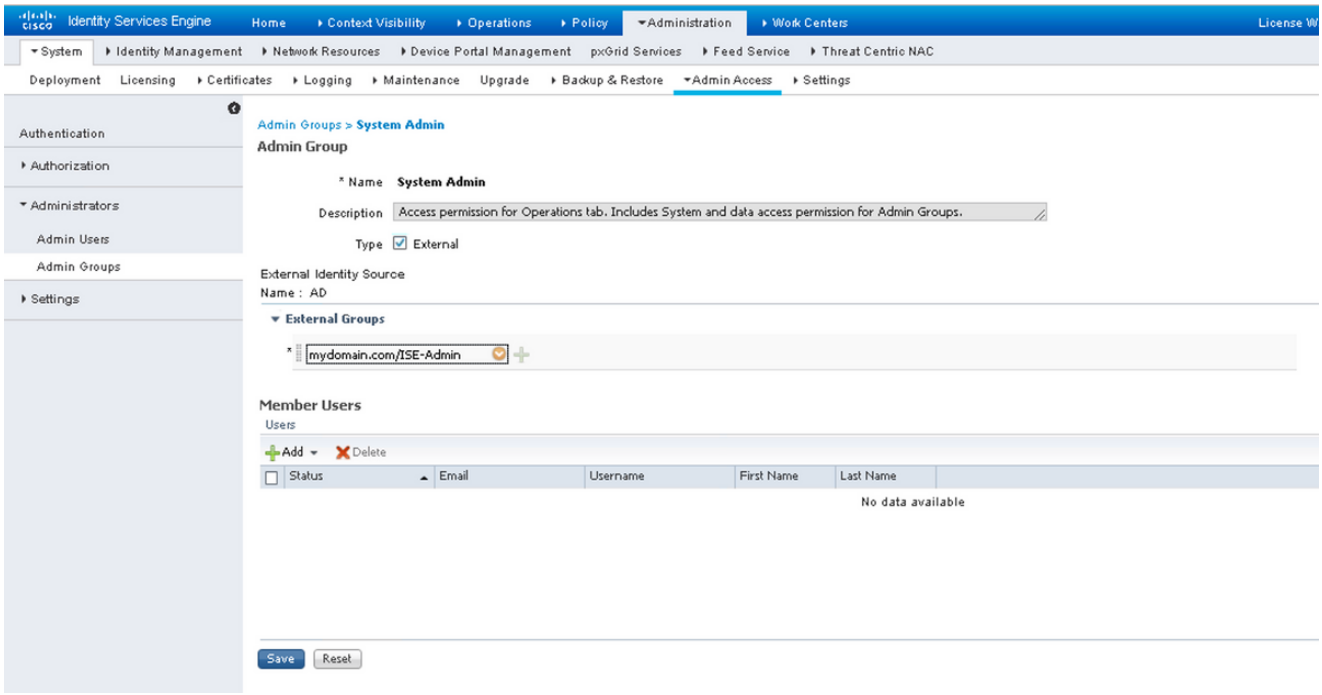
份验证配置成功后恢复。

将外部身份组映射到管理员组

在本示例中，外部AD组映射到默认管理员组。

1. 选择Administration > System > Admin Access > Administrators >Admin Groups > Super admin。

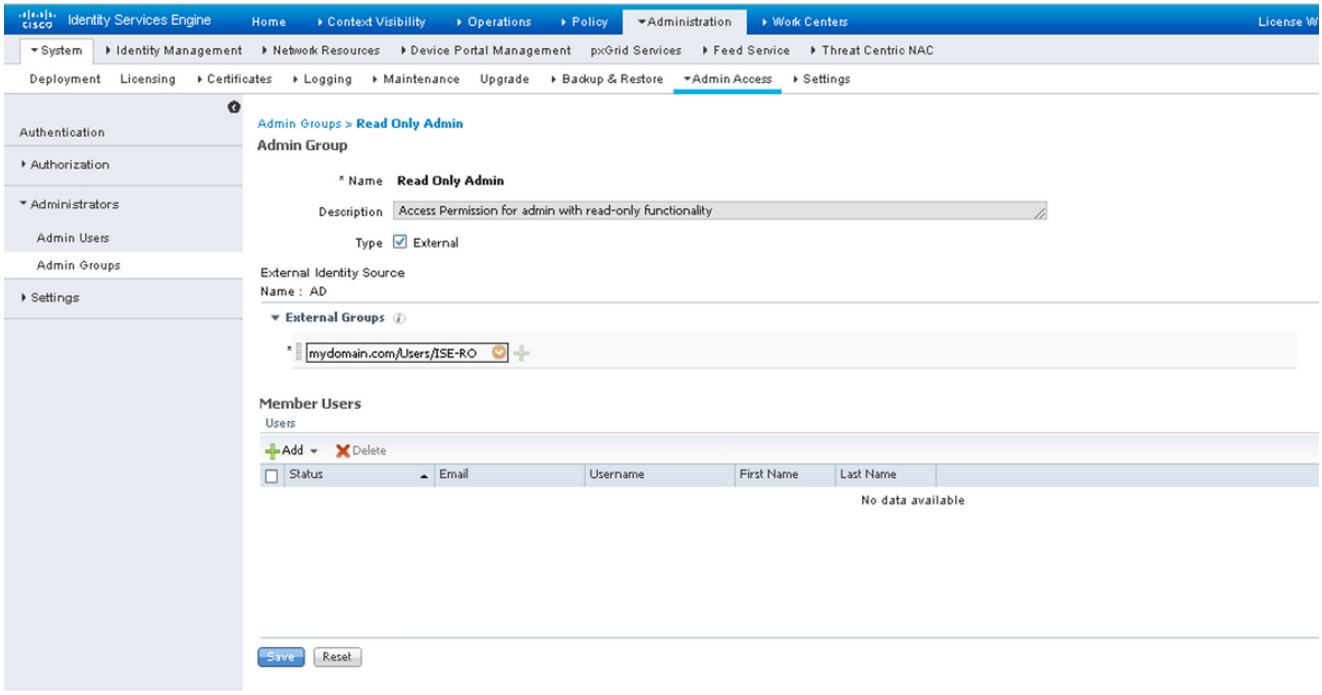
2. 选中Type as External，然后在External groups下选择AD组。



3. Click Save.

4. 选择Administration > System > Admin Access > Administrators > Admin Groups > Read Only Admin。

5. 选中Type as External，然后在External groups下选择AD组，如图所示。



6. Click Save.

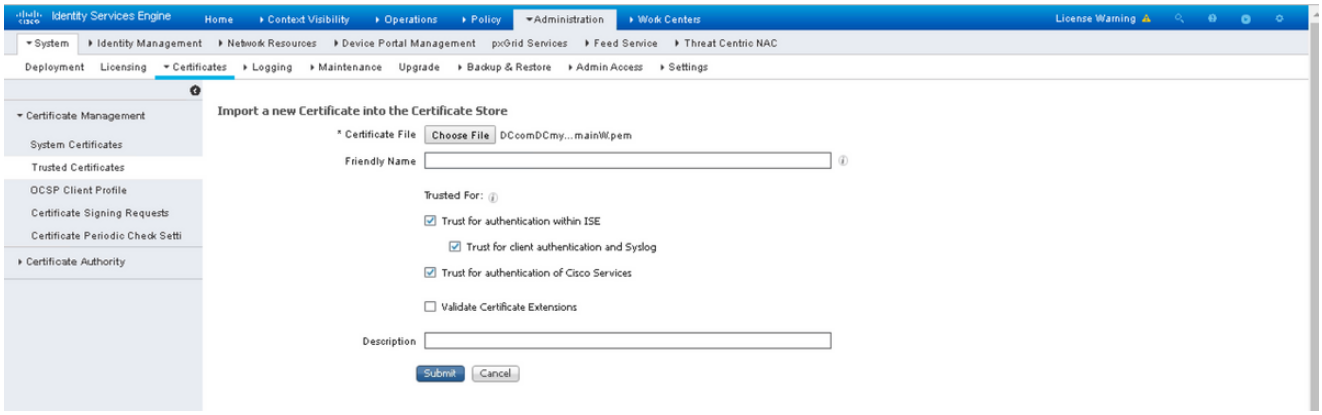
导入受信任证书

1. 导入签署客户端证书的证书颁发机构(CA)证书。

2. 选择 Administrator > System > Certificates > Trusted Certificate > Import。

3. 点击browse并选择CA证书。

4. 选中Trust for client authentication and Syslog复选框，如图所示。



5. 单击 submit。

配置证书身份验证配置文件

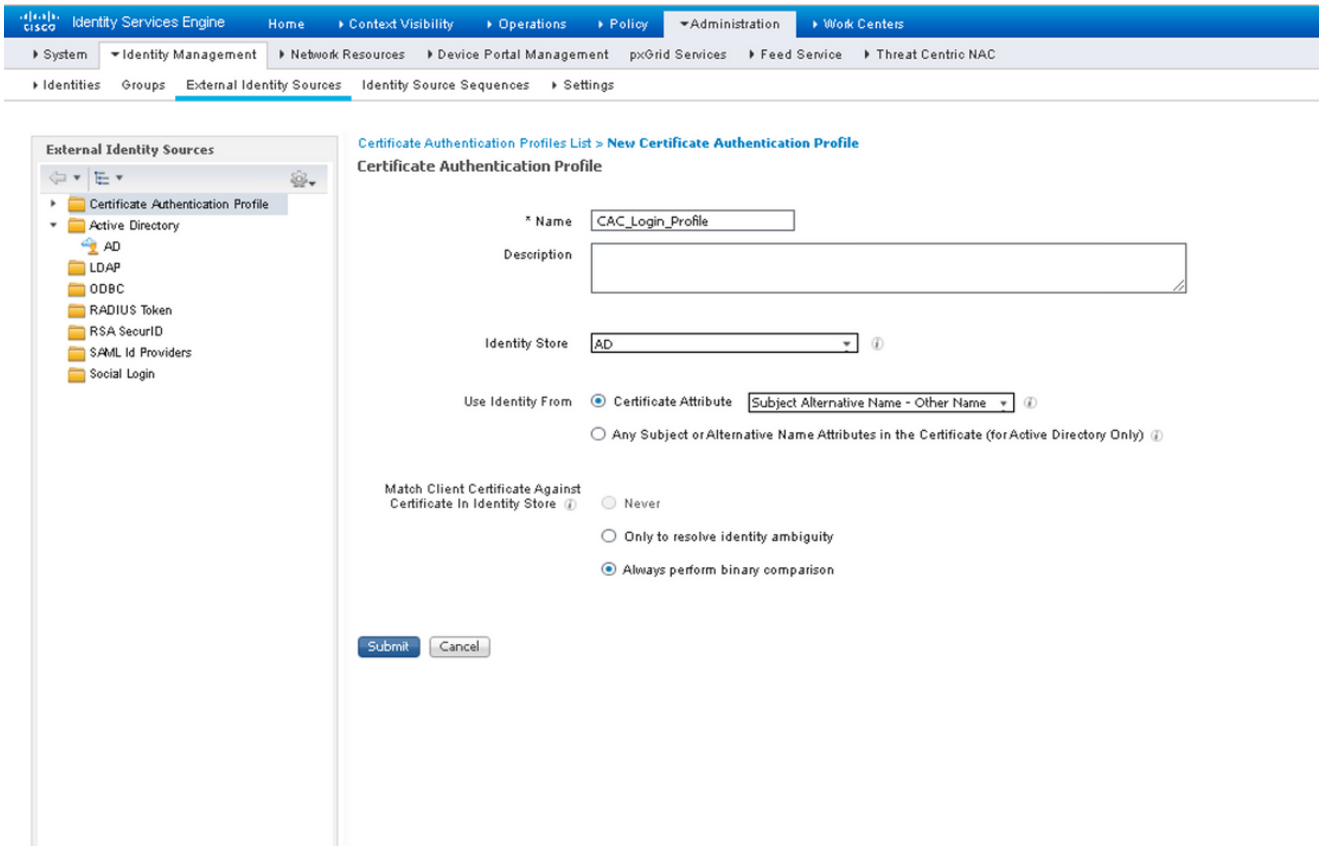
1. 要为基于客户端证书的身份验证创建证书身份验证配置文件，请选择Administration >身份管理(Identity Management)>外部身份源(External Identity Sources)>证书身份验证配置文件

(Certificate Authentication Profile)>添加(Add)。

2. 添加配置文件名称。

3. 在证书属性中选择包含管理员用户名的相应属性。

4. 如果用户的AD记录包含用户的证书，并且希望将从浏览器收到的证书与AD中的证书进行比较，请选中Always perform binary comparison复选框，并选择之前指定的Active Directory实例名称。

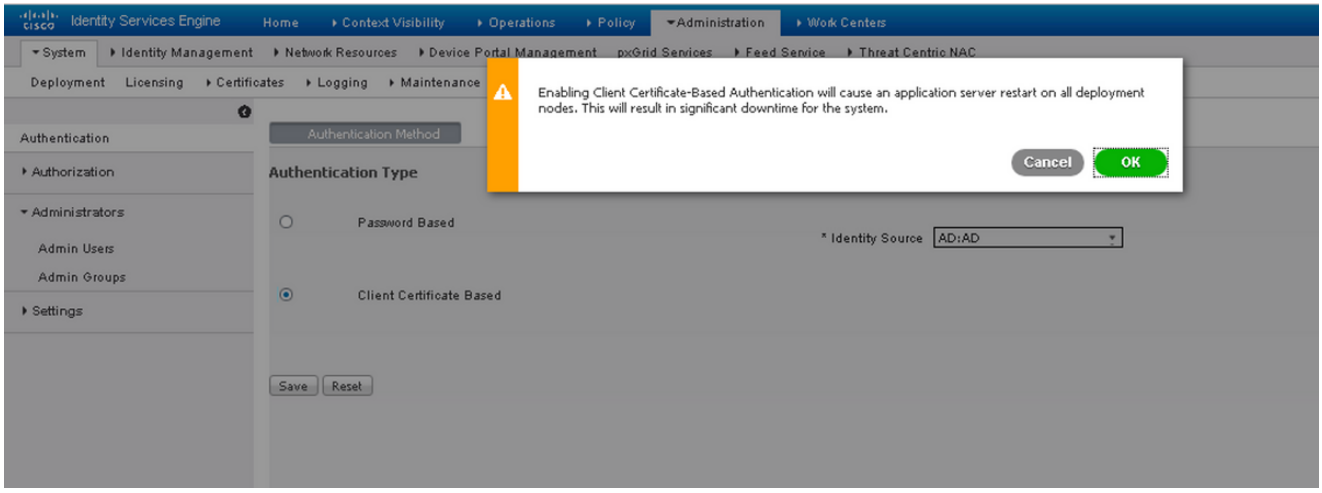


5. 单击 submit。

注意：相同的证书身份验证配置文件也可用于终端基于身份的身份验证。

启用基于客户端证书的身份验证

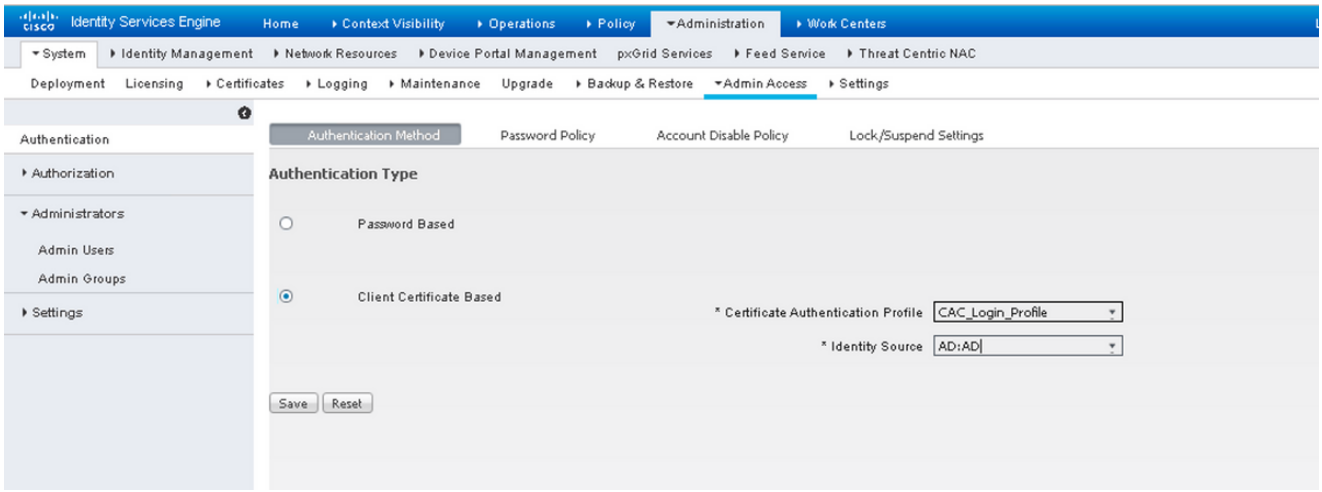
1. 选择 Administration > System > Admin Access > Authentication > Authentication Method Client Certificate Based。



2. Click OK.

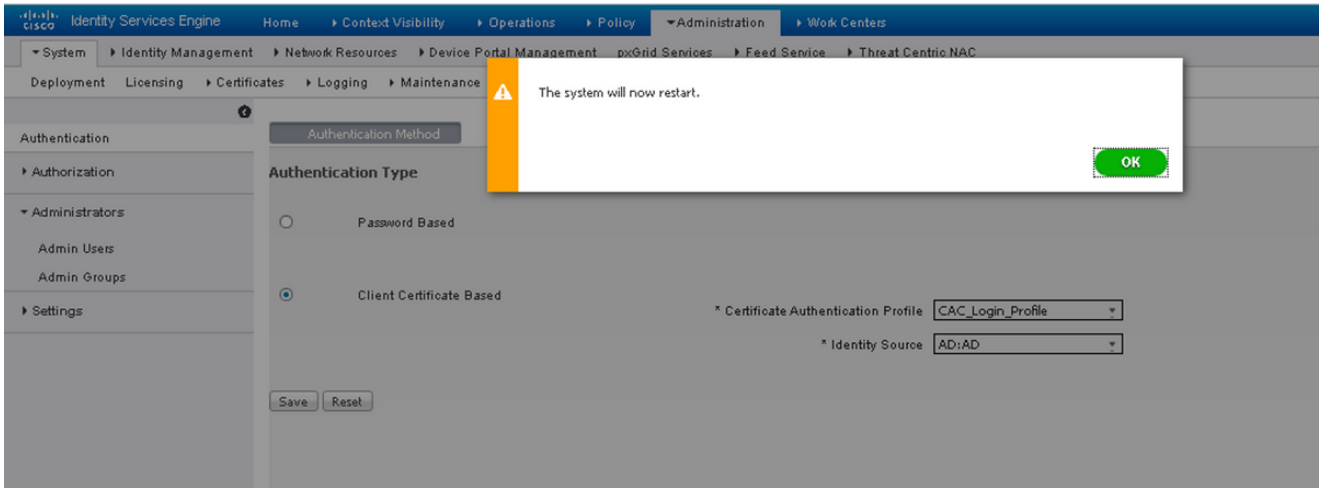
3. 选择之前配置的证书身份验证配置文件。

4. 选择Active Directory实例名称。



5. Click Save.

6. 部署中的所有节点上的ISE服务会重新启动。

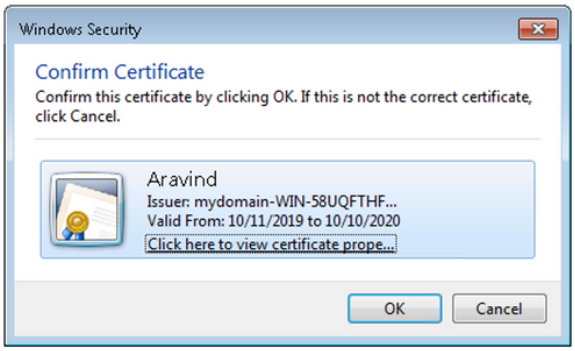


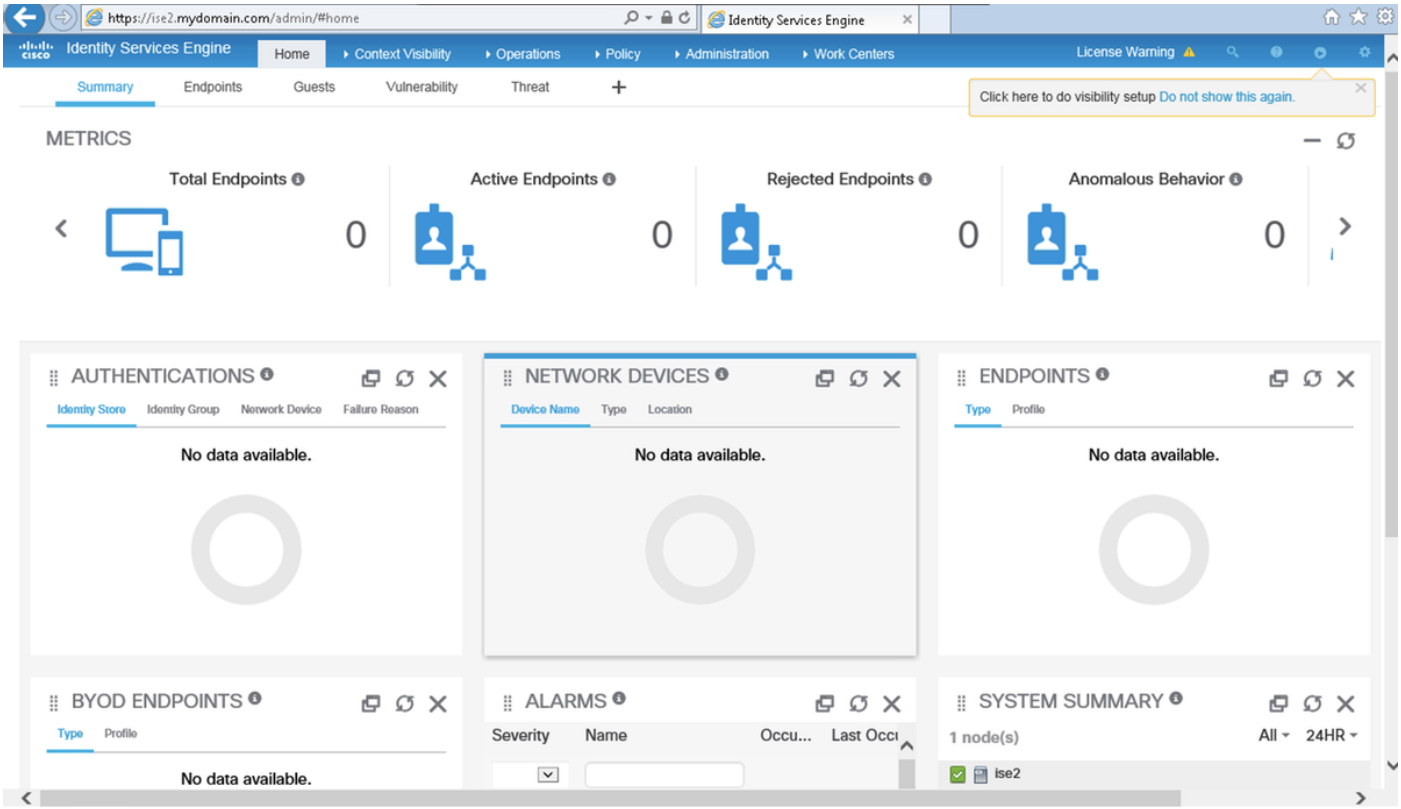
验证

在应用服务器服务状态更改为运行后，验证对ISE GUI的访问。

超级管理员用户：验证是否提示用户选择证书以登录到ISE GUI，并且如果证书属于超级管理员外部身份组的用户部分，则授予超级管理员权限。



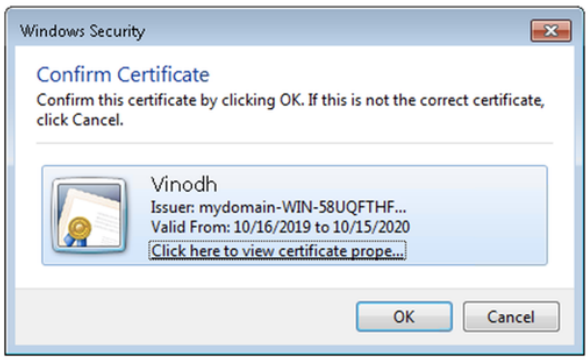


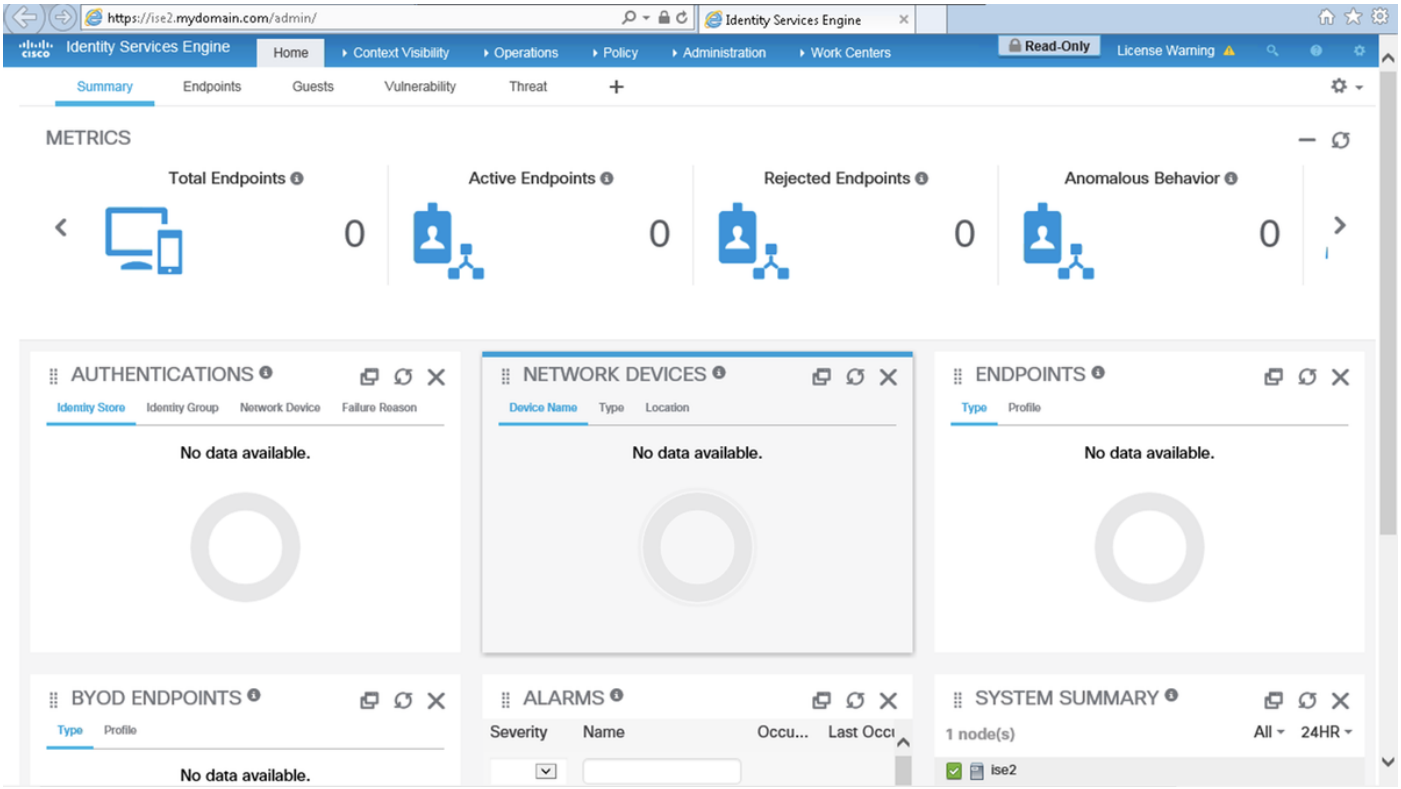


只读管理员用户：如果证书属于只读管理员外部身份组的用户部分，请验证是否提示用户选择要登

录到ISE GUI的证书并授予只读管理员权限。







注意：如果正在使用通用访问卡(CAC)，智能卡会在用户输入其有效超级PIN后向ISE提供用户证书。

故障排除

1. 使用application start ise safe命令以安全模式启动Cisco ISE，该模式允许临时禁用对管理员门户的访问控制，并使用命令application stop ise后跟application start ise更正配置并重新启动ISE的服务.
2. 如果管理员无意中阻止所有用户访问Cisco ISE管理员门户，则safe选项提供恢复方法。如果管理员在Administration > Admin Access > Settings > Access页面中配置了不正确的IP Access列表，则可能会发生此事件。safe选项还可绕过基于证书的身份验证，并恢复为默认用户名和密码身份验证，以便登录到Cisco ISE管理员门户。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。