为ISE管理配置基于证书或智能卡的身份验证

目录

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：

- 密码和证书身份验证的ISE配置。
- 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：

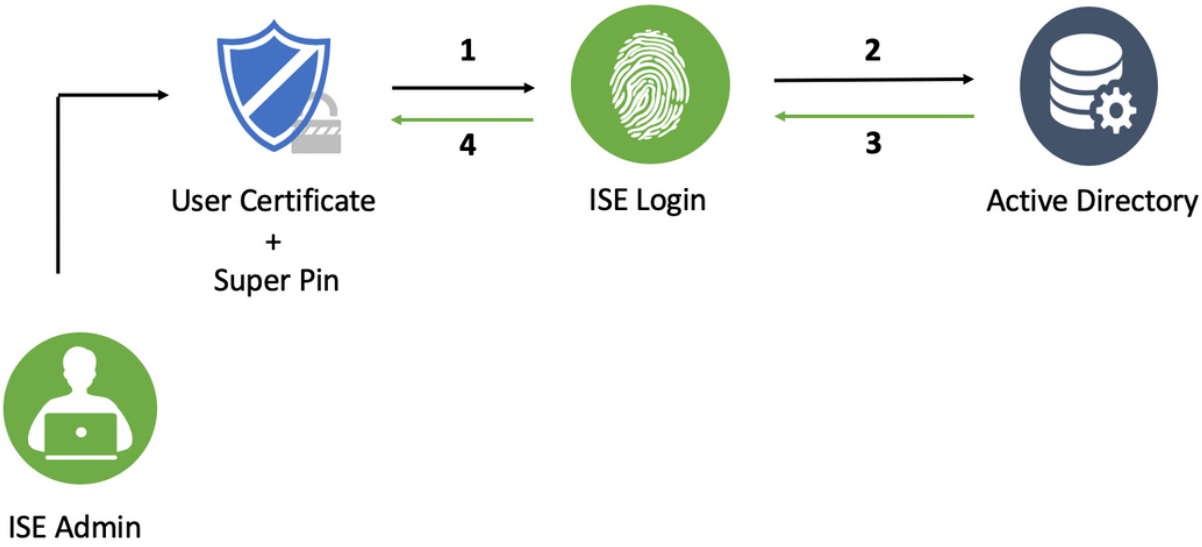
- 思科身份服务引擎(ISE)版本2.6
- Windows Active Directory(AD)Server 2008版本2
- 证书

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

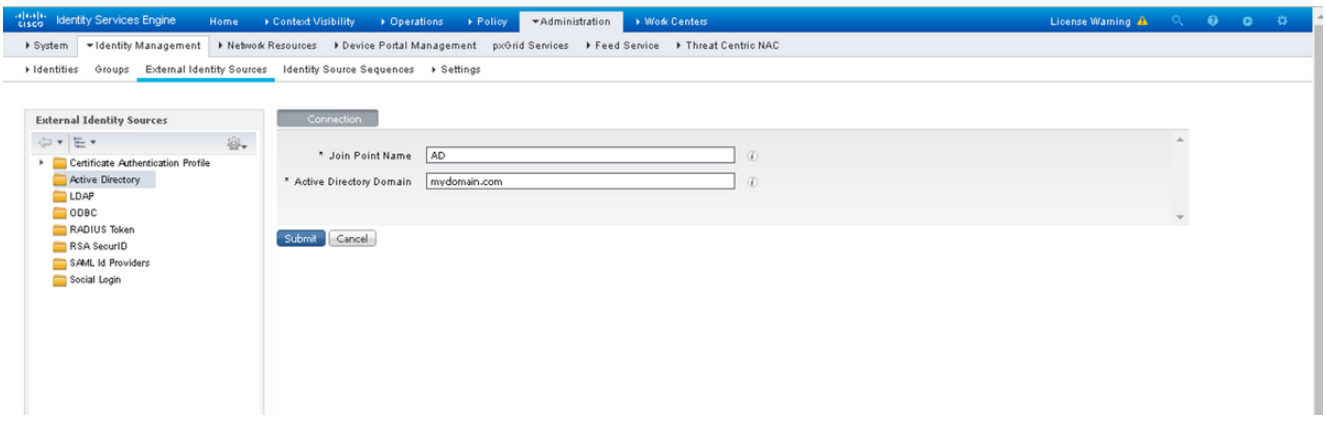
使用此部分将客户端证书或智能卡配置为外部身份，用于管理访问思科ISE管理GUI。

网络图

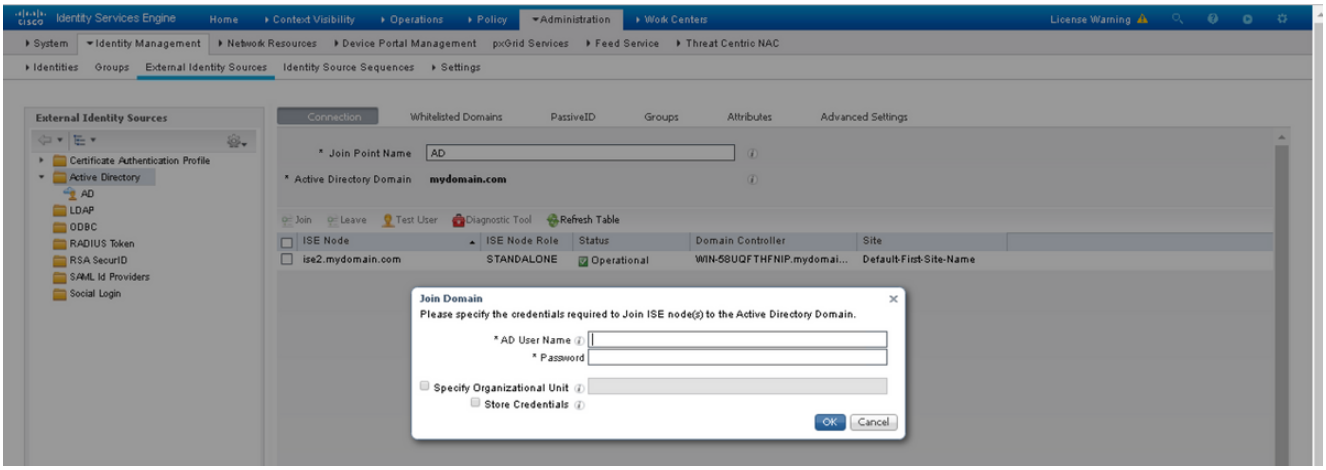


将ISE加入Active Directory

1. 选择**管理> 身份管理>外部身份源>** 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”。



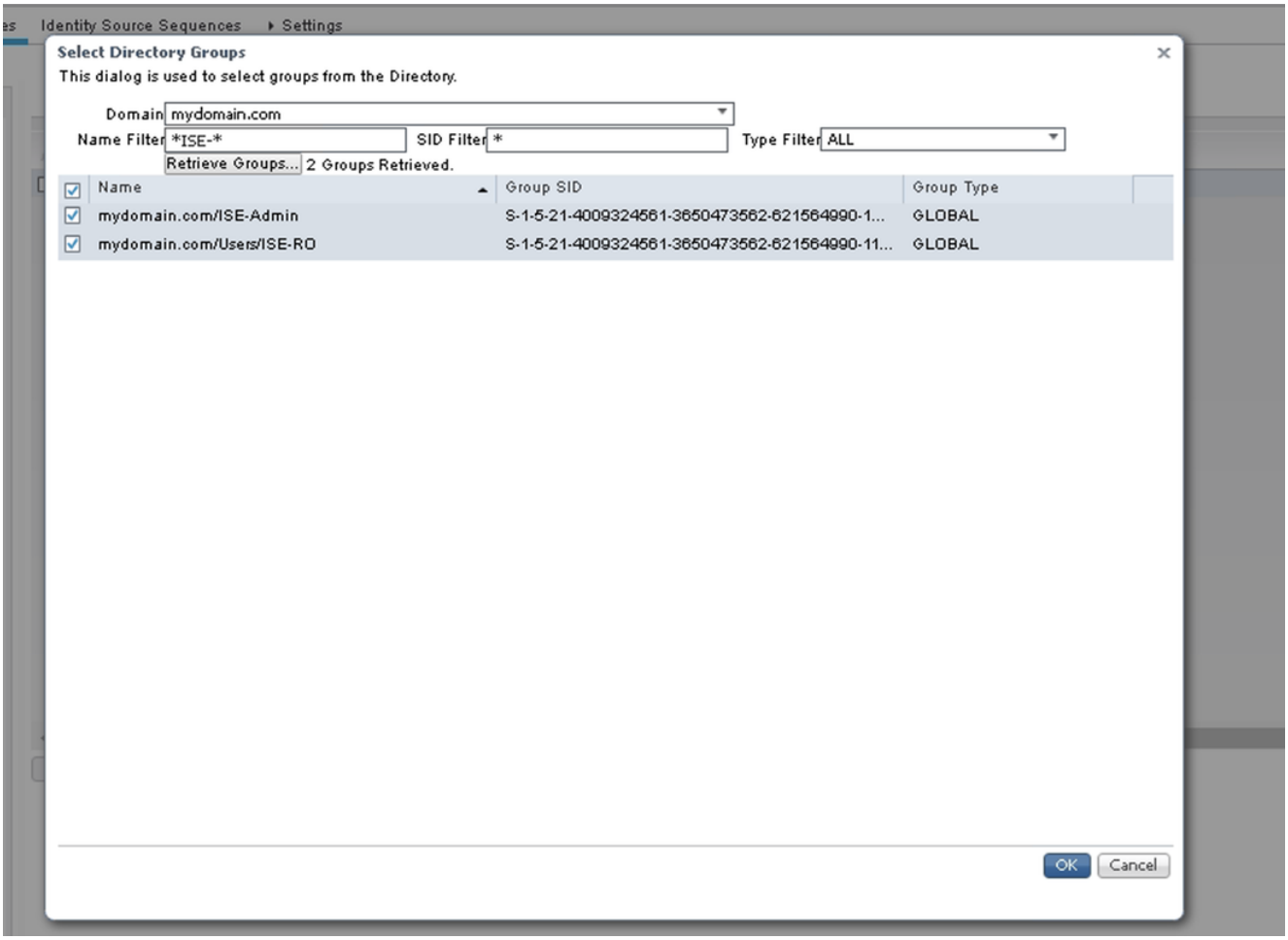
4. 在提示符中使用适当的**用户名**和**密**码加入所有节点。



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>外部身份源> Active Directory >组>从目录选择组。**
3. 至少检索一个管理员所属的AD组。

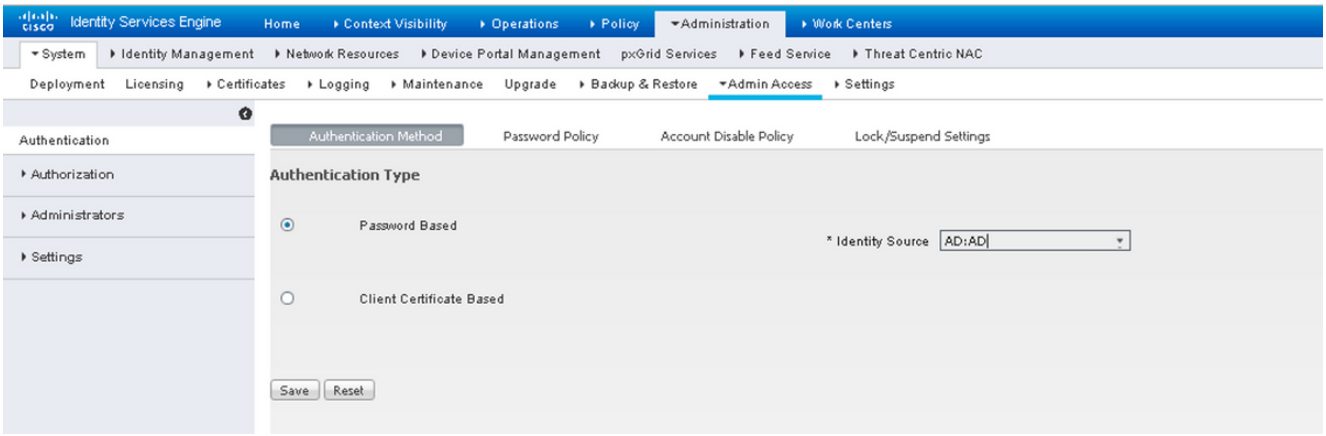


4. Click **Save**.

为管理访问启用基于密码的Active Directory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**管理>系统>管理员访问>身**份验证，如图所示。



3. Click **Save**.

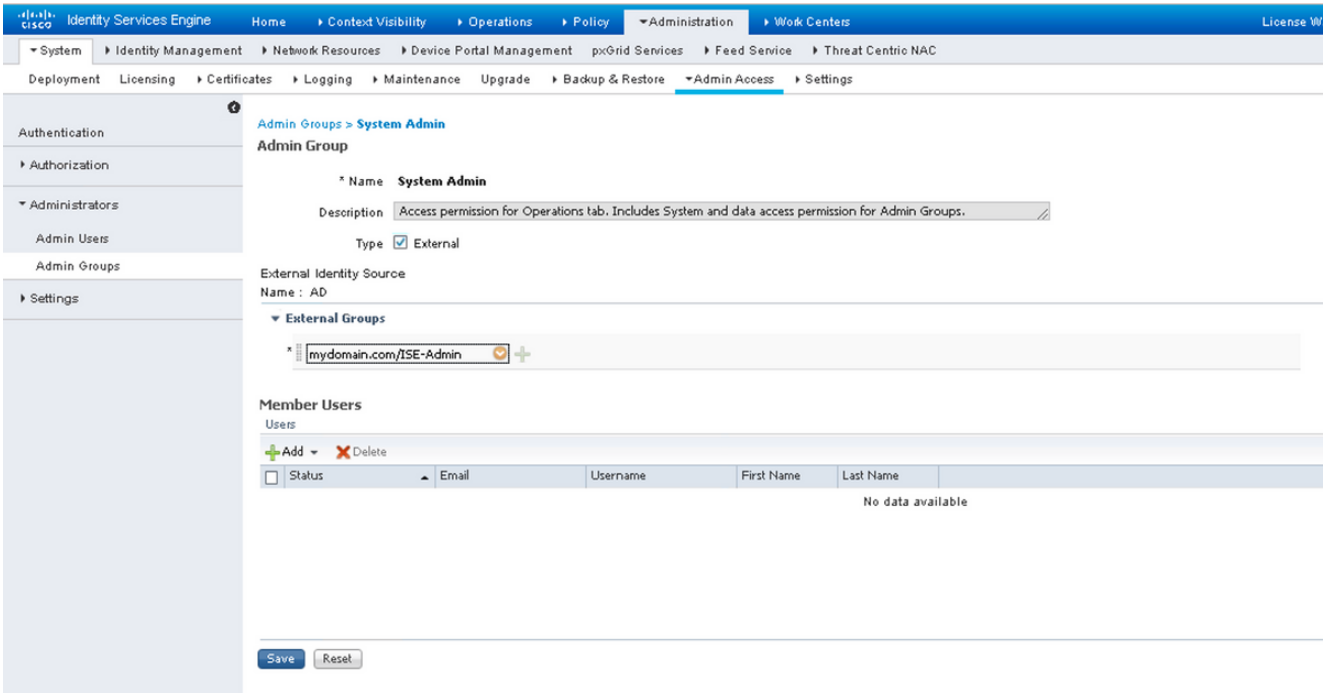
注意：启用基于证书的身份验证需要基于密码的身份验证配置。此配置应在成功配置基于证书的身份验证后恢复。

将外部身份组映射到管理员组

在本例中，外部AD组映射到默认管理员组。

1. 选择管**理>系统>管理员访问>管理员>管理员组>超级管理员。**

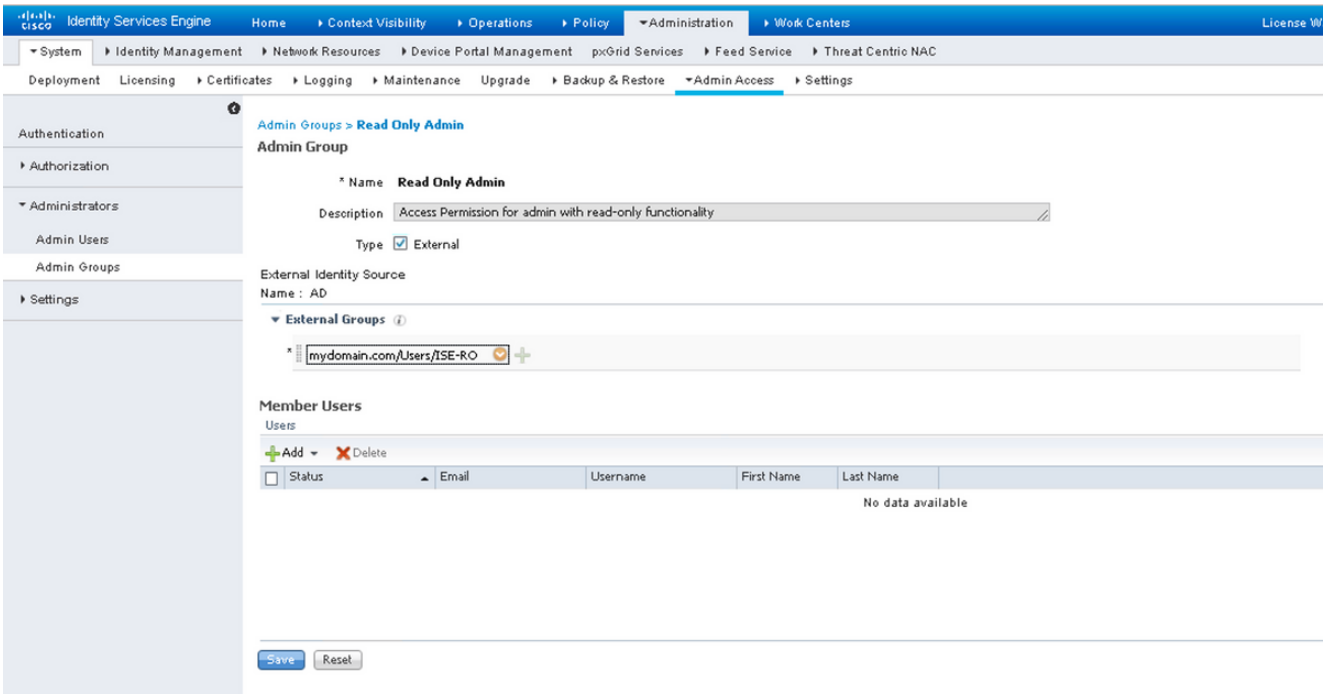
2. 选中“Type as External(类**型为**外部)”，然后在“External groups（外部组）”下**选择AD组**。



3. Click **Save**.

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

5. 选中“Type as External(类**型**)”，然后在“External groups(外部**组**)”下选择AD组，如图所示。



6. Click **Save**.

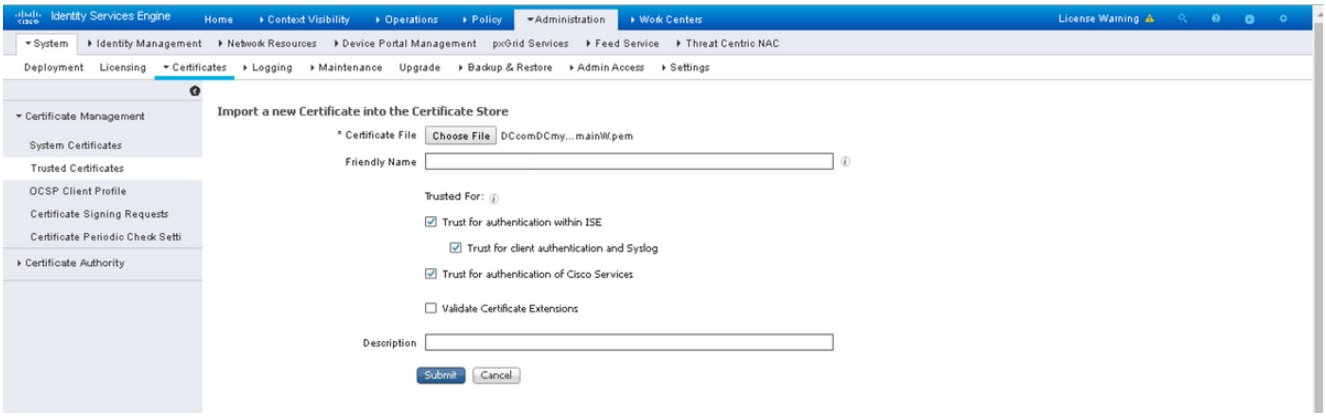
导入受信任证书

1. 导入签署客户端证书的证书颁发机构(CA)证书。

2. 选择 **管理员>系统>证书>受信任证书>导入。**

3. 点击浏览并选择CA证书。

4. 如图所示，**选中Trust for client authentication和Syslog复选**框。



5. 单击“Submit”。

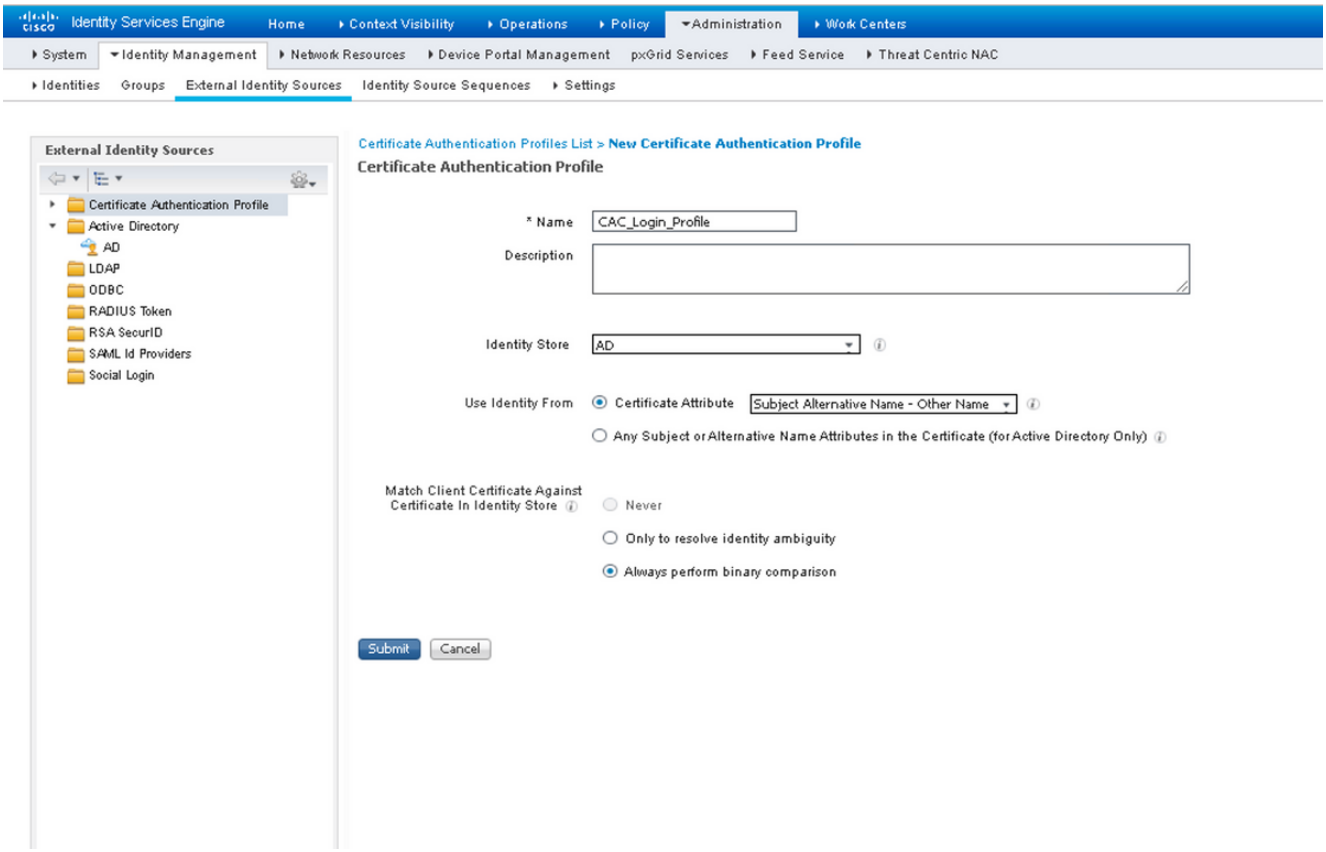
配置证书身份验证配置文件

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**管理>身份管理>外部身份源>证书身份验证配置文件>添加。**

2. 添加配置文件名称。

3. 选择在证书属性中包含管理员用户名的适当属性。

4. 如果用户的AD记录包含用户的证书，并且想将从浏览器收到的证书与AD中的证书进行比较，请选中**始终执行二进制比**较复选框，并选择之前指定的Active Directory实例名称。

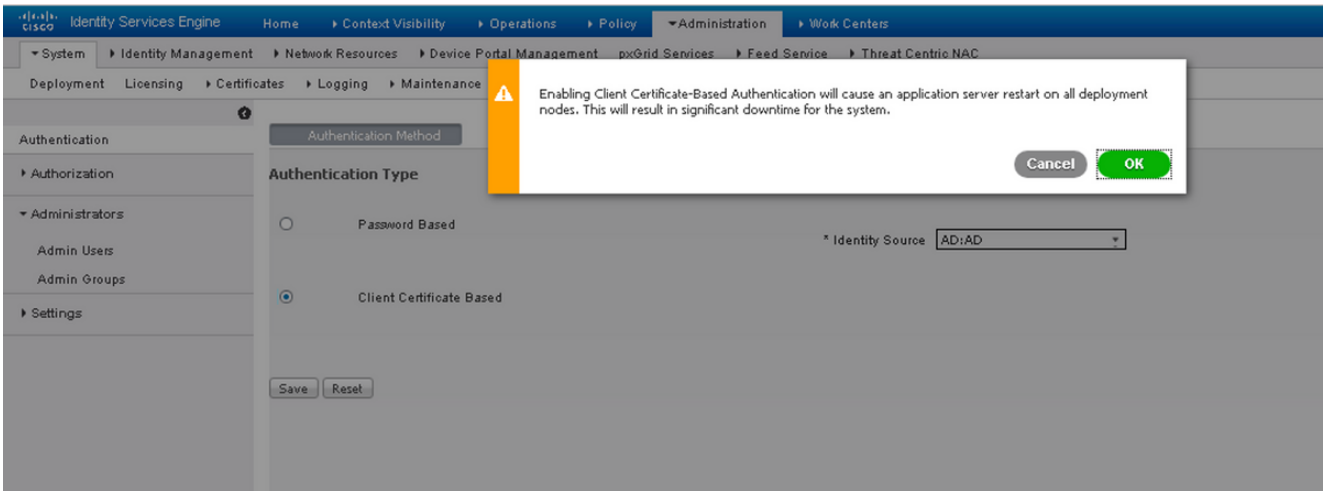


5. 单击“Submit”。

注意：也可使用相同的证书身份验证配置文件进行基于身份的终端身份验证。

启用基于客户端证书的身份验证

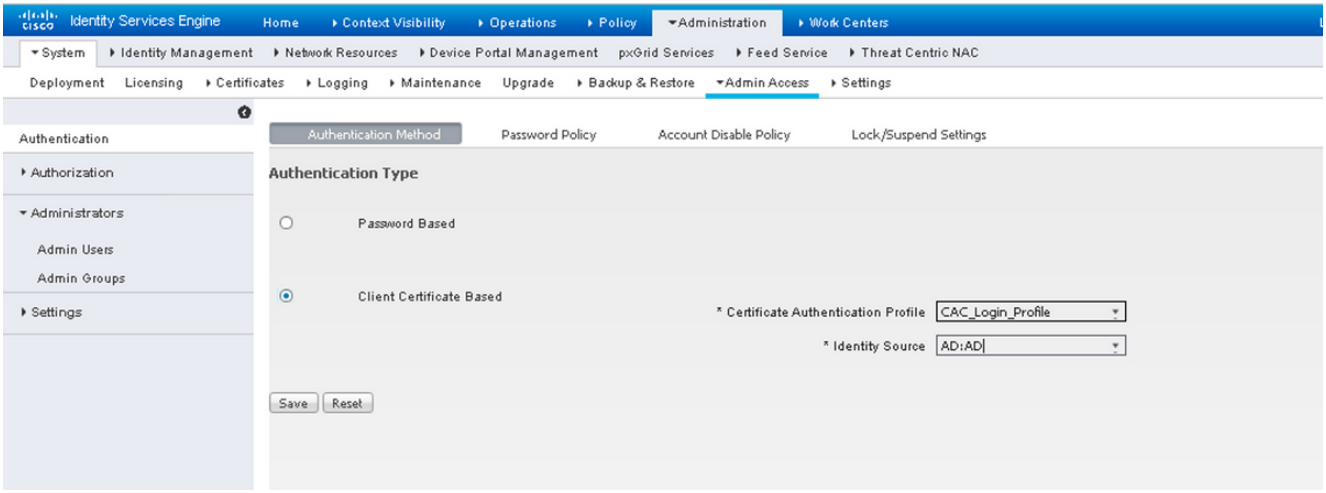
1. 选择 Administration > System > Admin Access > Authentication > Authentication Method Client Certificate Based。



2. Click **OK**.

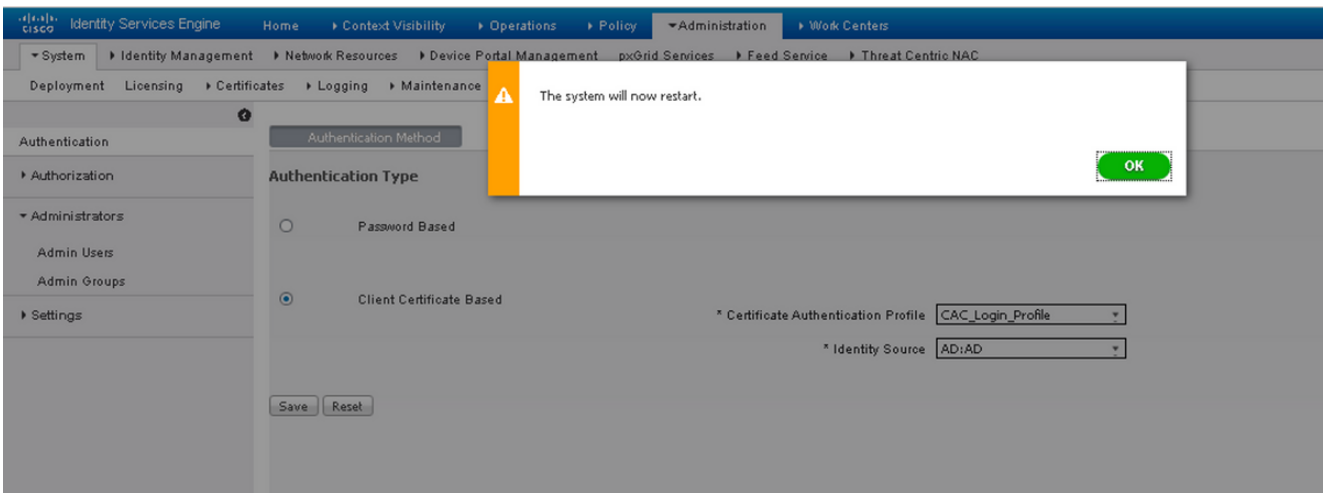
3. 选择之前**配置的证**书身份验证配置文件。

4. 选择Active Directory实例名称。



5. Click **Save**.

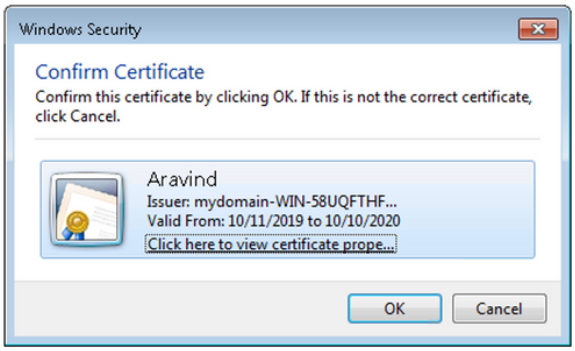
6. 部署中所有节点上的ISE服务将重新启动。

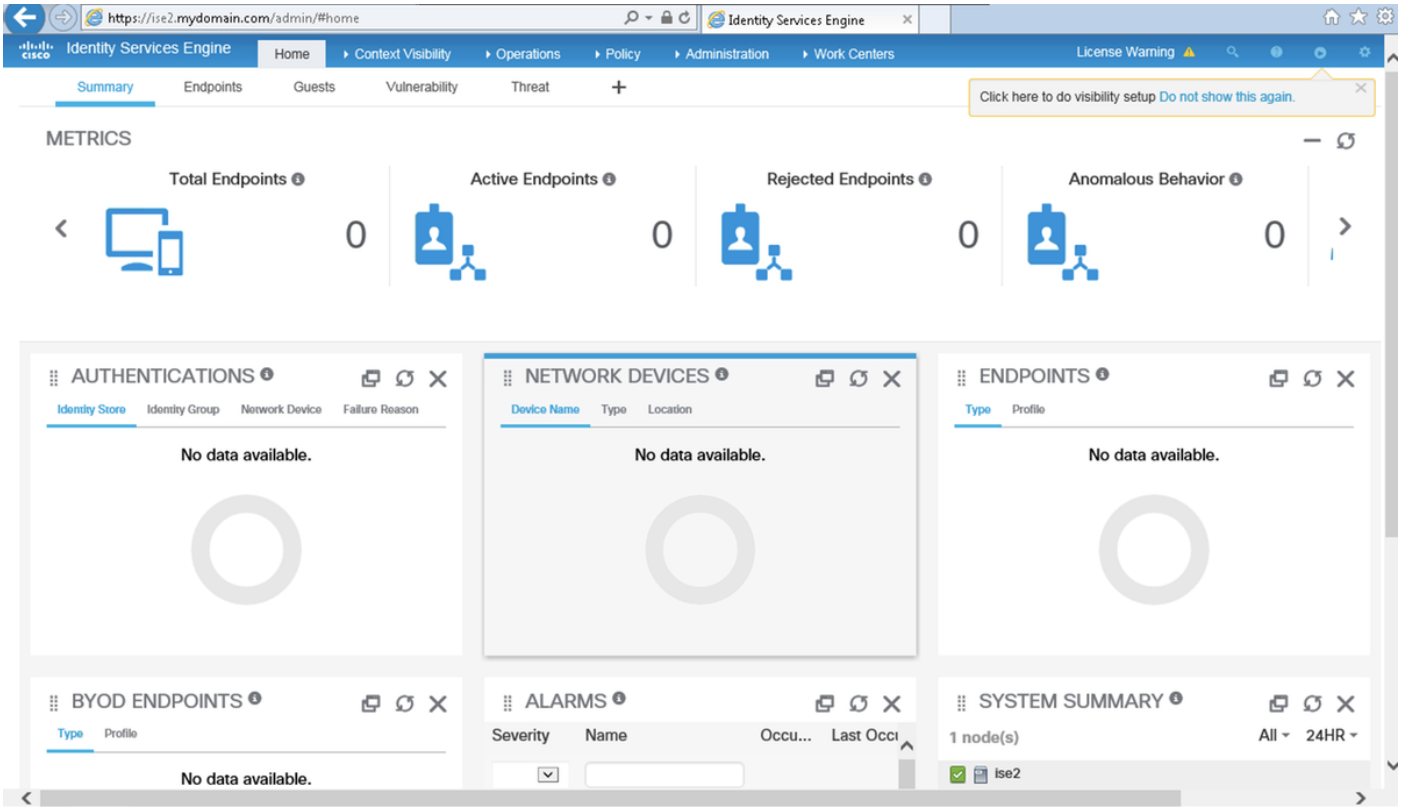


验证

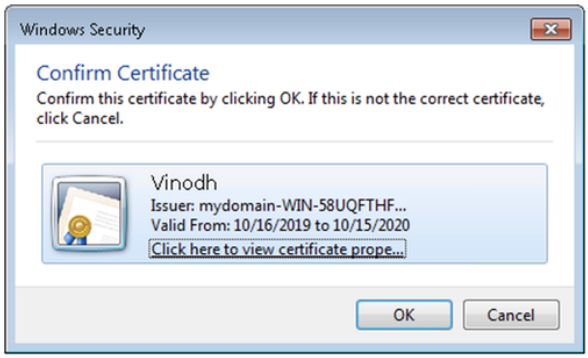
验证在应用服务器服务状态更**改为运**行后对ISE GUI的**访问。**

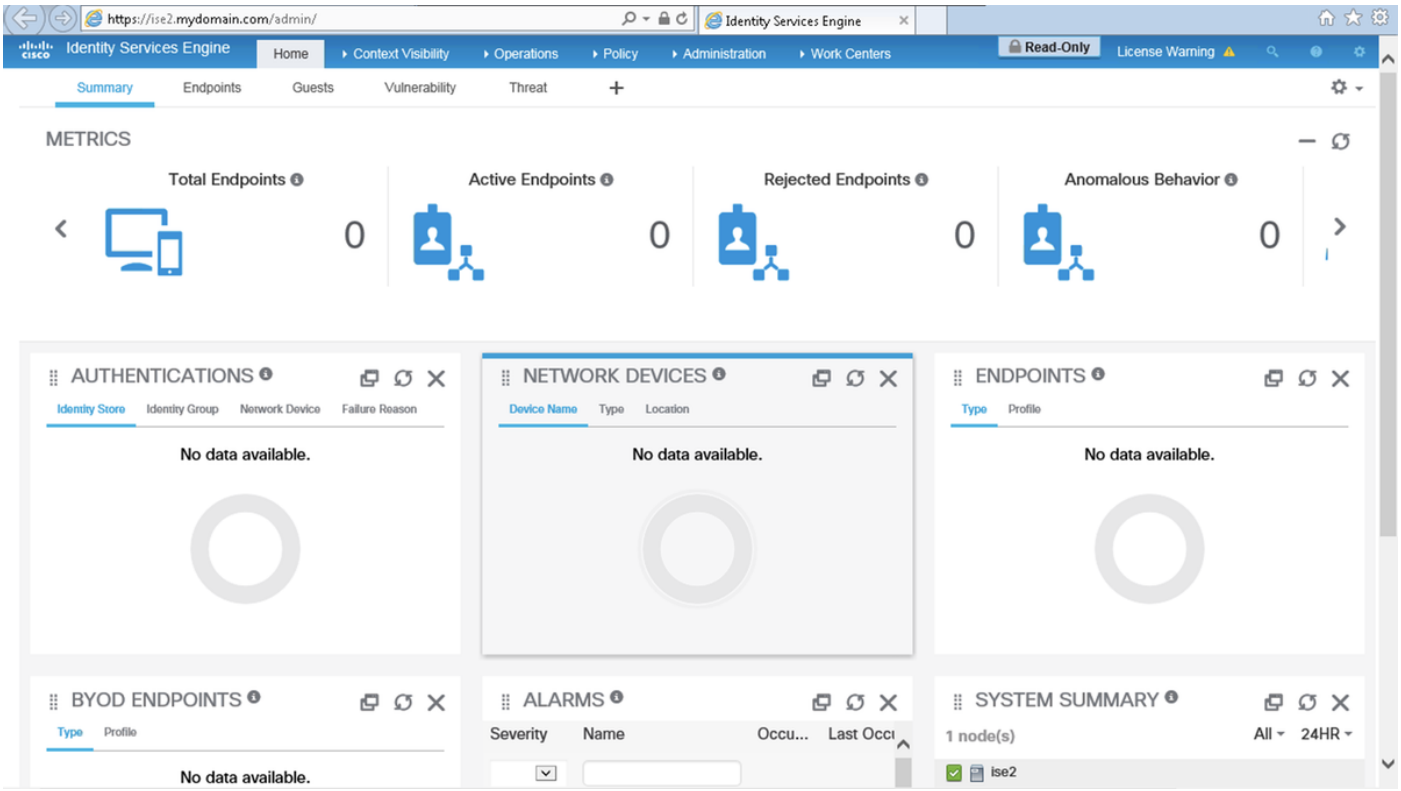
Super Admin User: Verify该用户是否被提示选择证书以登录ISE GUI，并且如果证书是Super Admin External Identity组的用户部分，则会获得Super Admin权限。





只读管理员用户：如果证书是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证书以登录ISE GUI并授予只读管理员权限。





注意：如果使用通用访问卡(CAC)，智能卡在用户输入有效超级PIN后向ISE显示用户证书。

故障排除

1. 使用**application start ise safe** 命令在安全模式下启动Cisco ISE，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和application start ise更正ISE的配置并重新启动**ISE的**服务。。
2. 如果管理员无意中锁定了所有用户对思科ISE管理员门户的访问，安全选项提供恢复方法。如

果管理员在“管理”(Administration)>“管理员访问”(Admin Access)>“设置”(Settings)>“访问”(Access)页面中配置了错误的IP访问列表，则可能会发生此事件。safe 选项还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Cisco ISE管理员门户。