

与AD凭证配置示例的ISE管理门户访问

目录

[简介](#)

[先决条件](#)

[Componenets使用了](#)

[配置](#)

[加入ISE对AD](#)

[选择目录组](#)

[启用AD的管理访问](#)

[配置Admin_group对AD组映射](#)

[设置Admin_group的RBAC权限](#)

[访问与AD凭证的ISE](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文描述配置示例为使用Microsoft Active Directory (AD)作为管理访问的外部标识存储对思科身份服务引擎(ISE)管理GUI。

先决条件

Cisco 建议您了解以下主题：

- Cisco ISE版本1.1.x或以上的配置
- Microsoft AD

Componenets使用了

本文档中的信息基于以下软件和硬件版本：

- Cisco ISE版本1.1.x
- Windows服务器2008版本2

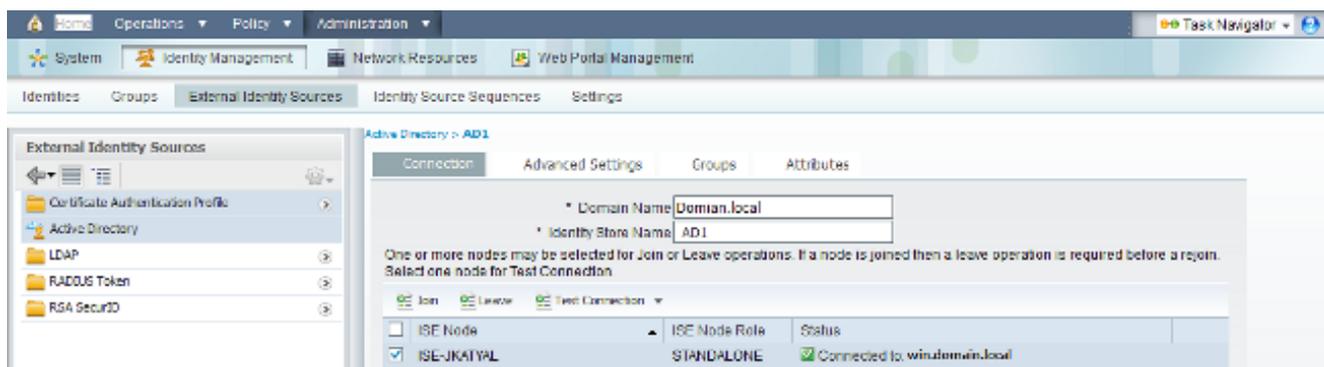
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

请使用此部分为了配置为使用Microsoft AD作为管理访问的外部标识存储对思科ISE管理GUI。

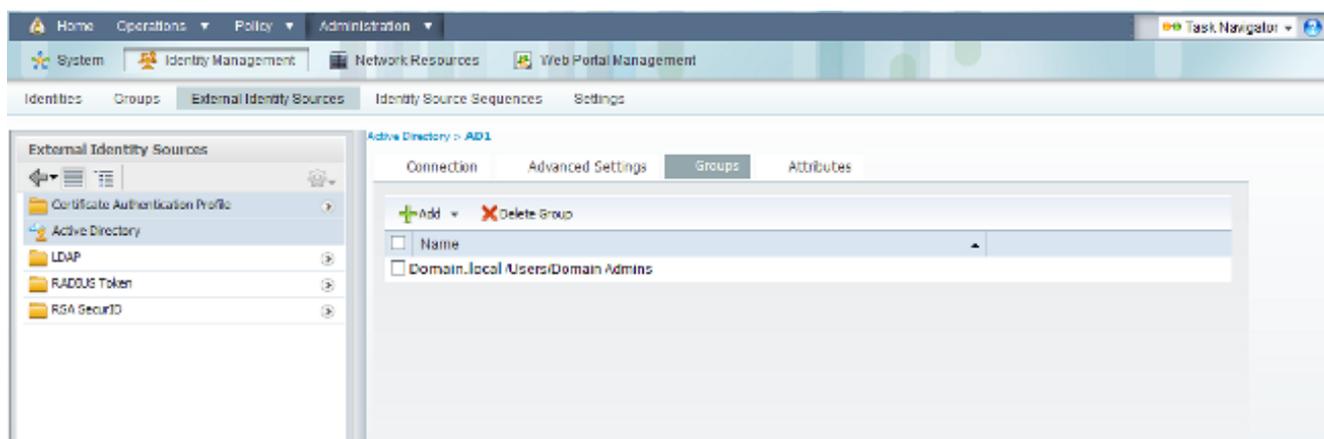
加入ISE对AD

1. 导航对**Administration > 身份管理 > 外部标识来源 > 活动目录**。
2. 输入AD域名和标识存储名称，并且点击**加入**。
3. 进入能添加和做对计算机对象的变动AD帐户的凭证，并且点击**保存配置**。



选择目录组

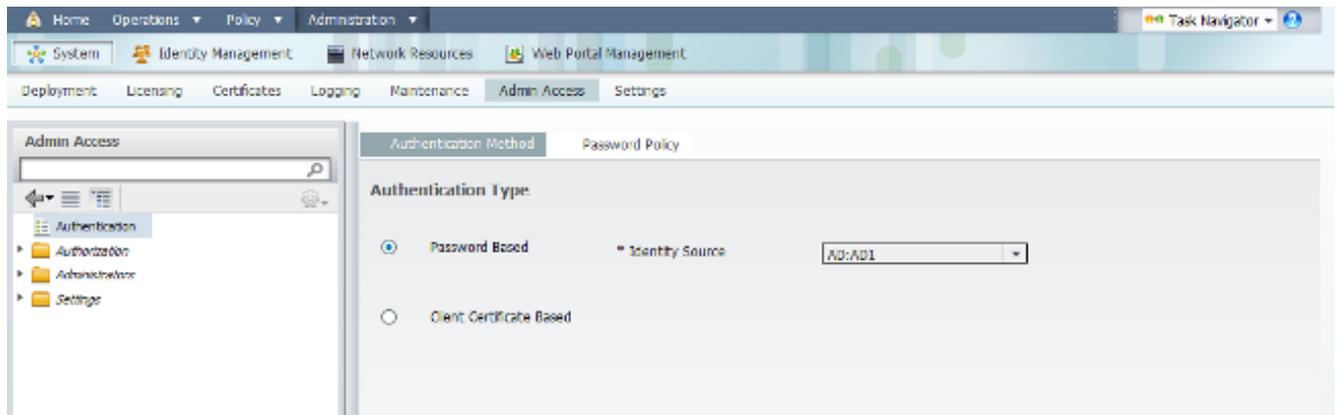
1. 导航对**Administration > 身份管理 > 外部标识来源 > 活动目录 > Groups > Add > 挑选组表目录**。
2. 导入您的管理员属于至少的一AD组。



启用AD的管理访问

完成这些步骤为了启用AD的基于密码的验证：

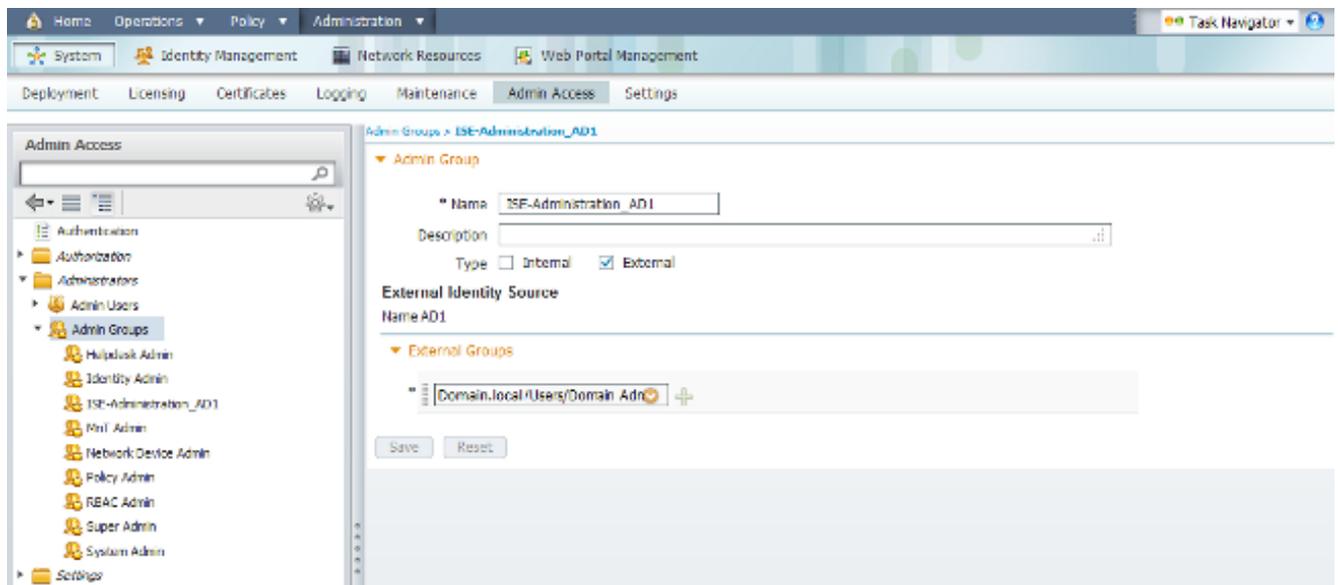
1. 导航对**管理 > System > Admin访问 > 验证**。
2. 从**认证方法**选项卡，请选择**根据的密码**选项。
3. 选择从**标识来源**下拉菜单的**AD**。
4. 点击**Save Changes**。



配置Admin group对AD组映射

定义思科ISE Admin group并且映射它给AD组。这允许授权确定角色根据组成员的管理员的基于访问控制(RBAC)权限在AD。

1. 导航给**管理>System > Admin访问>管理员> Admin组**。
2. 单击**添加**在表报头为了查看新的Admin group配置窗格。
3. 输入名称对于新的Admin group。
4. 在Type字段，请检查**外部**复选框。
5. 从**外部组**下拉菜单，请选择您希望此Admin group映射的AD组，如对挑选目录组部分定义。
6. 点击**Save Changes**。

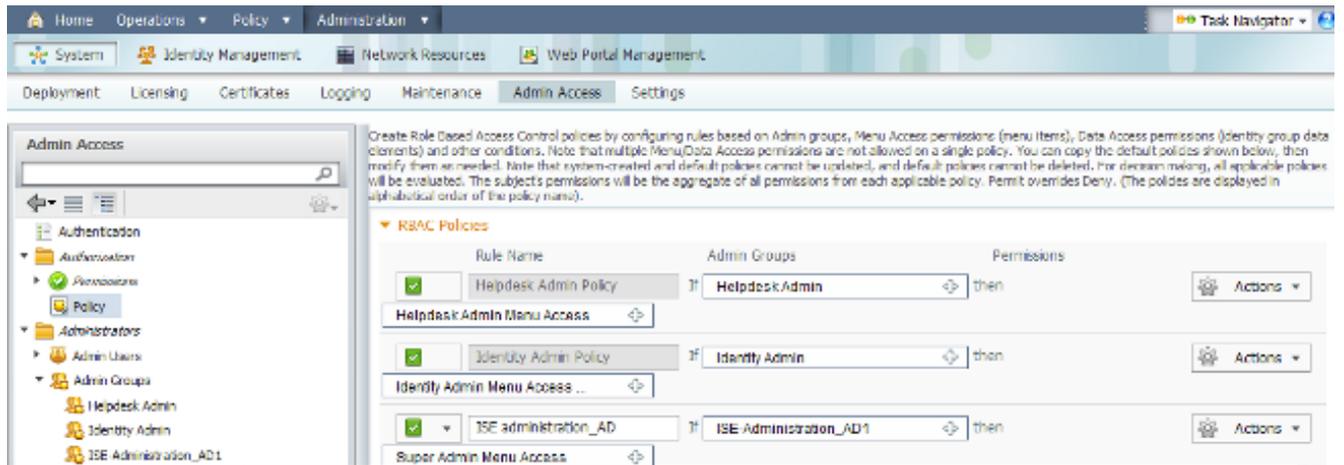


设置Admin group的RBAC权限

完成这些步骤为了分配RBAC权限到在前面部分创建的Admin组：

1. 导航对**管理>System > Admin访问>授权>Policy**。
2. 从在右边的**操作**下拉菜单，请选择**插入下面新建的策略**为了添加一项新的策略。
3. 创建呼叫**ISE_administration_AD**的新规则，映射它与在AD部分的Enable (event)管理访问定义的Admin group，并且分配它权限。**Note:**在本例中，呼叫**特级Admin**的Admin group分配，与标准的管理帐户是等同的。

4. 点击**保存更改**，并且保存的更改的确认显示在GUI的右下角。



与AD凭证的访问ISE

完成这些步骤为了访问与AD凭证的ISE：

1. 管理GUI的注销。
2. 从**标识来源**下拉菜单的挑选**AD1**。
3. 输入从AD数据库和登录的用户名和密码。



Note:对内部用户存储的ISE默认，在AD是不可得到的情况下或者使用的帐户凭证在AD不存在。这实现快速登录，如果使用内部存储，当AD为管理访问时配置。

验证

为了确认您的配置适当地工作，请验证认证的用户名在ISE GUI的角的。



故障排除

目前没有针对此配置的故障排除信息。

相关信息

- [思科身份服务引擎用户指南，版本1.1 -管理Identities和Admin访问](#)
- [技术支持和文档 - Cisco Systems](#)